UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

SEGURIDAD EN REDES Y REDES PRIVADAS VIRTUALES SOBRE INTERNET

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

DAVID GRÁNDEZ HERZ

PROMOCIÓN

2001 - II

LIMA – PERÚ
2005

SEGURIDAD EN REDES Y REDES PRIVADAS VIRTUALES SOBRE INTERNET

A mis padres,

por su constante apoyo y motivación,

y por transmitirme el deseo de superación

SUMARIO

El presente trabajo pretende dar una visión global de los aspectos necesarios para la implementación de seguridad en redes informáticas.

El capítulo I es una introducción a la seguridad en redes. Se dan a conocer los fundamentos de seguridad y la importancia de las políticas de seguridad.

El capítulo II ofrece una visión de las amenazas a las que están sujetas las redes, clasifica a los atacantes y sus motivaciones, y detalla los diferentes tipos de ataque que existen.

El capítulo III muestra los distintos métodos disponibles para autenticación de usuarios, autorización de acceso a recursos, y contabilidad o auditoría.

Los capítulos IV y V abarcan los temas de Firewalls y de Sistemas de Detección y Prevención de Intrusos, elementos clave en la protección de una red.

El capítulo VI muestra los diferentes mecanismos para la administración de redes.

El capítulo VII se enfoca en mostrar los diferentes objetivos de ataque en una red y proporciona técnicas de defensa para protegerlos.

En el capítulo VIII se muestran las maneras de mitigar los diferentes tipos de ataque.

El capítulo IX abarca el tema de Redes Privadas Virtuales sobre Internet, mostrando las diferentes tecnologías criptográficas disponibles para su implementación.

El capítulo X muestra diferentes diseños de seguridad en redes, incluyendo redes pequeñas y medianas con o sin soporte para telefonía IP, redes wireless o inalámbricas, y redes de acceso remoto. Los diseños de seguridad para redes grandes, aquellas de proveedores y empresas muy grandes, no han sido contemplados en este trabajo.

ÍNDICE

PRÓLOGO

La seguridad en redes informáticas ha pasado de ser un requerimiento exclusivo de organizaciones gubernamentales relacionadas con la seguridad, o de instituciones financieras preocupadas por la seguridad de la información y de las transacciones de valores, a ser prácticamente un requisito para cualquier persona o entidad que requiere conectar su red con otra.

La información se ha convertido en un activo intangible, un elemento valioso para organizaciones e individuos que, por tanto, debe ser protegido. Con la difusión y la mejora en la confiabilidad de los sistemas de computadoras, la tendencia ha sido, y continúa siendo, el trasladar la información a medios digitales, accesibles a través de dichos sistemas.

La necesidad de acceder a la información desde puntos distantes motivó el desarrollo de mecanismos para interconectar los sistemas de computadoras entre sí. Sin duda, el ejemplo más claro es la expansión de la red de redes, Internet, la cual ha contribuido enormemente al

desarrollo de las comunicaciones en general, interconectando virtualmente cualquier punto del planeta con cualquier otro.

Esta red cuyo propósito siempre ha sido el de facilitar la comunicación entre redes para el intercambio de información, se creó a partir de protocolos o lenguajes de comunicación diseñados para cumplir ese mismo objetivo, sin tomar en cuenta aspectos de seguridad que hoy en día cobran cada vez más importancia. La facilidad y practicidad ofrecidas por Internet para el intercambio de información y el poco conocimiento de sus deficiencias para mantener la confidencialidad e integridad de los datos, motivó su empleo en la transmisión y puesta a disposición de todo tipo de información, desde irrelevante hasta altamente confidencial; en cualquiera de sus formatos: datos, comunicaciones de voz e incluso video.

Más aún, en un número cada vez mayor de casos la continuidad del negocio de las empresas depende de la disponibilidad de acceso que tengan sus clientes a los recursos de la empresa, vía Internet. Tal es el caso de empresas que han implementado sistemas de Comercio Electrónico, así como aquellas que ofrecen otros servicios "en línea" a sus clientes.

Personas y organizaciones con diversos fines en mente han sabido aprovechar las deficiencias de seguridad de Internet y de sus protocolos. Esto ha originado que otros grupos de personas y organizaciones vuelquen sus esfuerzos hacia la búsqueda y desarrollo de mecanismos, metodologías y tecnologías que proporcionen mayores niveles de seguridad en el mundo de las redes informáticas.

Hoy en día conectarse a Internet es cada vez más fácil y económico, pero a la vez, si no se toman las medidas de seguridad adecuadas, los sistemas conectados pueden ser víctimas de ataques, y sus usuarios víctimas de robo, destrucción o alteración de información muchas veces confidencial. A esta nueva modalidad de crimen se le ha denominado "Crimen Cibernético" o "Crimen Informático", y a su escenario, el "Ciberespacio". Se estima que hoy en día, sólo en Estados Unidos, se produce un crimen informático cada veinte minutos.

Implementar Seguridad en una red no solo consiste en usar técnicas avanzadas de cifrado, instalar un firewall, escribir una buena política de control de contraseñas, o repasar una larga lista de tareas de seguridad. Muchos de los problemas de seguridad que se presentan tienen su origen en la naturaleza humana: el desconocimiento, la confianza mal entendida, el descuido, la falta de adhesión a normas, son algunos de los causantes.

Resulta irónico que cuando se trata de seguridad en redes no se puede hablar de ofrecer seguridad al cien por ciento. No existen sistemas infalibles. Cada nueva tecnología o mecanismo de seguridad que se desarrolle siempre tendrá un punto débil. Ya sea en si mismo o debido al hecho que, al ser implementado de manera modular, si alguno de los módulos o capas es vulnerable, podrá hacer que parte o todo el sistema lo sea también. En general, siempre habrá alguien que encontrará la manera de aprovechar los puntos débiles y burlar la seguridad.

Los esfuerzos de seguridad deben centrarse, entonces, en tratar de minimizar estas vulnerabilidades, manteniéndose al día con las últimas novedades en seguridad para dificultarles la tarea a los atacantes. Es un proceso constante y arduo, en un mundo donde la única red segura es aquella que está aislada o apagada.

El presente trabajo pretende transmitir los conceptos, principios, tecnologías y consideraciones relacionadas con la implementación de seguridad en redes informáticas, incluyendo las redes virtuales privadas implementadas sobre Internet.

Dada la variedad de los temas involucrados, la profundidad de los mismos ha tenido que ser limitada a brindar la información necesaria para cumplir el objetivo planteado.

Este trabajo ha sido posible en gran medida gracias al aporte de Cisco Systems, una empresa reconocida mundialmente, que fabrica equipos para proporcionar soluciones completas de red y que colabora en el desarrollo de estándares. Actualmente, Cisco posee la mayor fuente de información tecnológica del planeta, accesible vía Internet. Cabe mencionar el aporte de empresas de seguridad como Check Point e ISS (*Internet Security Systems*), y organizaciones tales como la Agencia de Seguridad Nacional de los Estados Unidos (NSA: *National Security Agency*), CERT (*Computer Emergency Response Team*) o Equipo de Respuesta ante Emergencias de Computadoras, entre otras; además del aporte de personas cuya dedicación y experiencia en el tema de seguridad en redes ha facilitado la comprensión de diversos aspectos de seguridad involucrados, muchas veces complejos.

CAPÍTULO I

INTRODUCCIÓN A LA SEGURIDAD EN REDES

CAPÍTULO I

INTRODUCCIÓN A LA SEGURIDAD EN REDES

1.1. DEFINICIÓN DE SEGURIDAD EN REDES

Es la implementación de dispositivos de seguridad, políticas y procesos para prevenir el acceso no autorizado a recursos de red y la alteración, destrucción, divulgación o denegación de recursos o datos.

Paradoja de la Seguridad en Redes: La única red segura es aquella que está aislada o apagada.

1.2. FUNDAMENTOS DE SEGURIDAD

Los cuatro pilares o fundamentos sobre los cuales se basa la seguridad en redes son:

- **PRIVACIDAD:** La información debe ser accesible o leída solo por el emisor y el receptor.
- **AUTENTICACIÓN:** El receptor debe poder estar seguro de la identidad del emisor.

- **INTEGRIDAD:** La información debe ser recibida tal como fue transmitida, sin alteraciones.
- **NO REPUDIACIÓN:** El receptor debe ser capaz de probar que una información determinada vino de un emisor específico. A su vez, el emisor debe ser capaz de probar que envió o no cierta información.

1.3. POLÍTICAS DE SEGURIDAD: OBJETIVOS Y LINEAMIENTOS

POLITICAS DE SEGURIDAD

Una política de seguridad es un manifiesto formal que especifica un conjunto de reglas que deben seguir aquellos a los que se les ha dado acceso a bienes tecnológicos o de información dentro de una organización. Una política de seguridad no es un documento técnico, es un documento de negocios que detalla las actividades permitidas y prohibidas, así como los esfuerzos y responsabilidades relacionados con la seguridad. El negocio debe dictar el alcance y profundidad de una política de seguridad y no al revés.

Este documento debe abarcar los siguientes temas:

- Uso aceptable de los bienes corporativos: Puede referirse, por ejemplo, al uso del correo electrónico y del acceso a Internet.

- Política de Configuración de Servidores y Estaciones de Trabajo: Define qué aplicaciones deben ser configuradas en la red. Asegura que todos los sistemas en la red se adhieran a una configuración estándar, lo cual reduce el tiempo de localización de problemas.

- Política de Administración de Parches: Define cómo deben hacerse las actualizaciones (*upgrades*) de los sistemas, y cómo los parches deben ser probados antes de ser aplicados en el entorno de producción.

- Política de Infraestructura de Red: Define cómo debe ser administrada la red y quién es responsable por su mantenimiento. Debe abarcar los siguientes temas: Esquema de direccionamiento de red, Convención de nombres, Manejo de configuración y cambios, Calidad del servicio, Administración y monitoreo de sistemas, Consolidación y procesamiento de registros y capturas.

- Política de Acceso: Define los derechos y privilegios de acceso para proteger bienes contra pérdida o divulgación, especificando directivas de uso aceptable para los usuarios, personal de operaciones y administrativo. Debe proveer directivas para conexiones externas, comunicaciones de datos, conexiones de dispositivos a la red, y adición de nuevo software a los sistemas; además de especificar los mensajes de advertencia o notificación. De igual manera, debe contemplar la seguridad física, regulando el acceso físico a la información y a los dispositivos de red.

- Política de Privacidad: Define las expectativas razonables de privacidad en relación con el monitoreo del correo electrónico, registro de lo tecleado, acceso a carpetas y archivos de los usuarios.

- Política de No repudiación: Define las responsabilidades de los usuarios, personal operativo y administrativo. Debe especificar la capacidad de auditoría y proveer directivas para manejo de incidentes.

- Política de Autenticación: Establece la confianza a través de una política de contraseñas efectiva, estableciendo directivas de autenticación para sitios remotos, y el empleo de dispositivos de autenticación. Se especifican, por ejemplo, los requisitos que deben tener las contraseñas: tamaño, tiempo de validez, tipo y complejidad.

- Otras políticas pueden abarcar temas tales como respaldo (*backup*), mantenimiento, uso de cifrado, entre otras.

El equipo encargado de la creación de la política de seguridad debe incluir a miembros de la parte administrativa, legal y técnica. La política de seguridad debe poder ser ejecutada y estar amparada por las leyes y regulaciones.

OBJETIVOS DE LA POLÍTICA DE SEGURIDAD

- Guiar al personal técnico en la elección del equipamiento, mas no especificar qué equipamiento en particular elegir. La política debe definir los requerimientos mínimos que se deben cumplir.

- Guiar al personal técnico en la configuración de los equipos.

- Definir responsabilidades para usuarios y administradores.

- Definir sanciones por violar las políticas, permitiendo a los usuarios entender que existen consecuencias de sus acciones.

- Definir procedimientos de respuesta y escalamiento ante amenazas identificadas.

En resumen, una política de seguridad consiste en lineamientos a ser seguidos por los administradores para planificar los esfuerzos y procedimientos de respuesta. Se definen responsabilidades y sanciones para usuarios y administradores, así como una respuesta planificada cuando las medidas empleadas sean insuficientes.

LINEAMIENTOS DE SEGURIDAD

Para que una política de seguridad sea exitosa se debe cumplir lo siguiente:

- La gerencia debe respaldar activa y totalmente la política, de lo contrario no será efectiva.

- La política debe ser consistente en alcance y objetivos. Por ejemplo, no se debe permitir que un grupo de usuarios no use contraseñas sólo porque el gerente de ese grupo no ve la necesidad. Una política inconsistente o imprecisa está abierta a interpretación.

- La política debe ser técnicamente realizable. No debe ser tan complicada que el usuario la deje de lado.

- La política no debe ser escrita como un documento técnico. La política debe ser entendible, clara y concisa. Debe ser fácil de entender para el usuario promedio, ya que será distribuida en toda la organización. Al no ser un documento técnico, permite que los conceptos de seguridad sean propagados sin revelar los detalles y las tecnologías específicas empleadas para cumplir los objetivos. El plan de implementación es una sección de la política de seguridad donde se define la información de hardware y aplicaciones específicos. El acceso al plan de implementación debe ser restringido a personal autorizado.

- La política debe ser implementada globalmente a lo largo de la organización. Un "hueco" o deficiencia de seguridad en un punto de la organización, plantea una amenaza a toda la organización.

- La política debe definir claramente los roles y responsabilidades. Los usuarios deben estar enterados de lo que está permitido y prohibido. Los administradores deben conocer sus objetivos y responsabilidades con respecto a la seguridad.

- La política debe ser suficientemente flexible para responder a los cambios tecnológicos, de infraestructura, al crecimiento y a los nuevos objetivos de la organización. La política de seguridad es un documento "vivo" y debe ser constantemente revisado y modificado para asegurar su relevancia en la organización.

- La política debe especificar sanciones ante violaciones. Las sanciones no deben oponerse a los derechos de los empleados ni a las leyes vigentes. Por ello es muy importante que, dentro del comité de seguridad encargado de hacer la política, existan miembros del área legal y de recursos humanos.

- La política debe incluir un plan de respuesta ante incidentes relacionados con brechas de seguridad. La mayoría de las políticas diferencian las brechas que han sido originadas desde dentro de la organización de aquellas originadas desde Internet.

1.4. SEGURIDAD EN REDES COMO UN PROCESO

La seguridad es un proceso continuo, no un esfuerzo de implementación en un momento determinado. Este dinamismo permitirá que la seguridad de la red evolucione y sea mejorada constantemente a medida que nuevas amenazas aparezcan.

Cuatro pasos deben ser seguidos en la implementación de una política de seguridad:

- **Proteger:** Implementar los equipos y procesos, y asegurar las configuraciones de los sistemas para reducir la exposición de la red.

- **Monitorear / Responder:** Monitorear la red para determinar cómo los cambios han afectado a la red, buscar amenazas adicionales y responder adecuadamente ante el descubrimiento de eventos. El monitoreo debe ocurrir en todo momento.
- **Probar:** Poner a prueba la red y las configuraciones de los sistemas para determinar si existen vulnerabilidades. Las pruebas deben hacerse cada vez que ocurran cambios significativos en las redes.

- **Administrar / Mejorar:** Administrar los sistemas y procesos, y realizar mejoras continuamente a estos, así como a las políticas, basándose en los resultados obtenidos en las pruebas y en las vulnerabilidades halladas durante el monitoreo de la red.

La figura 1.1 muestra gráficamente el proceso de seguridad y su interacción con las políticas de seguridad.

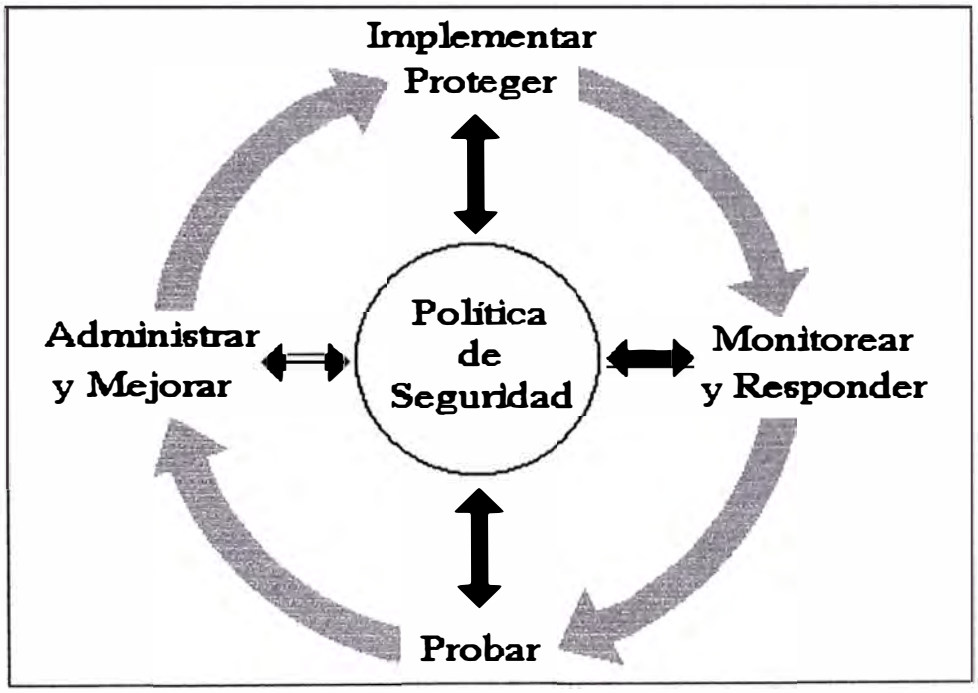

FIGURA 1.1 – La Seguridad como un Proceso

CAPÍTULO II

RIESGOS DE SEGURIDAD Y ATAQUES

CAPITULO II

RIESGOS DE SEGURIDAD Y ATAQUES

Hoy en día los sistemas de computadoras se han convertido en un componente fundamental de casi toda organización. Hasta las organizaciones más pequeñas suelen usar una computadora para mantener registros e información financiera. Ya que estos sistemas son capaces de realizar funciones de manera rápida y precisa, y debido a que facilitan la comunicación entre organizaciones, las redes de computadoras continúan creciendo y se interconectan cada vez más. Más aún, toda organización que proporciona algún tipo de acceso público a su red tiene una conexión a Internet, y este acceso no está libre de riesgo.

Las computadoras, no importa cuan avanzadas sean, siguen siendo máquinas que funcionan según un conjunto predeterminado de instrucciones. Los sistemas operativos y otros paquetes de software son solo conjuntos de instrucciones compilados que la computadora usa para transformar una entrada en una salida.

2.1. VULNERABILIDADES

Una vulnerabilidad es una falla en los procedimientos de seguridad, software, sistemas de control internos o implementación de un Sistema de Información que puede afectar la integridad, confidencialidad, la capacidad de registro y seguimiento, y/o la disponibilidad de datos o servicios.

La definición más generalizada de vulnerabilidad es: cualquier punto en un paquete de software o sistema que permite a un usuario alterar dicho software u obtener acceso al sistema, algo para lo cual no fue específicamente diseñado. Por esta razón, muchos desarrolladores de software continúan produciendo parches para sus productos a medida que las vulnerabilidades son descubiertas.

La mayoría de las redes contienen una combinación de datos públicos y privados. Un esquema de seguridad correctamente implementado protege la información en la red y sin embargo permite que cierta información sea accedida por entidades externas, usualmente sin permitir su modificación. Un ejemplo de esto puede ser una página web corporativa. Proteger adecuadamente una red asegura que no será usada como punto de ataque contra otras redes.

Los ataques pueden ser efectivos y dañar las redes por tres razones principalmente: falta de efectividad de la política de seguridad, debilidades de configuración, y debilidades tecnológicas.

FALTA DE EFECTIVIDAD DE LA POLÍTICA DE SEGURIDAD

Esta es la base de todos los esfuerzos de seguridad, y pueden resultar no efectivas por las siguientes razones:

- Políticas internas. Cuando se dan inconsistencias y se permiten excepciones a las reglas de seguridad.

- Falta de una Política Escrita. Es prácticamente como no tener una política.

- Falta de Continuidad, ante cambios de personal frecuentes, por ejemplo.

- Falta de un Plan de Recuperación ante Desastres. Debe existir un plan de contingencia ante violaciones de seguridad. La información recogida durante estos eventos debe protegerse y no debe ser eliminada por los esfuerzos de recuperación.

- Falta de Procedimientos de Actualización y Parchado de los sistemas.

- Falta de Monitoreo. La ausencia de monitoreo y análisis de los registros de eventos expone a la organización a ser atacada sin que siquiera se sepa que dicho ataque está ocurriendo.

- Falta de Control de Acceso. El acceso no autorizado se facilita cuando se implementan sistemas de control de acceso mal diseñados, contraseñas con longitudes y complejidad no apropiadas, cambios poco frecuentes de contraseñas, contraseñas escritas en notas pegadas al monitor o teclado, contraseñas compartidas.

DEBILIDADES DE CONFIGURACIÓN

- Equipos mal configurados por desconocimiento o por error.

- Contraseñas fáciles de adivinar o muy cortas. Las contraseñas deben consistir de al menos ocho caracteres y deben incluir mayúsculas, minúsculas y caracteres especiales.

- Servicios de Internet mal configurados, entre ellos: *Java Applets, Java Scripts*, opciones de seguridad de FTP o IP.

- Uso de opciones por defecto. Generalmente las opciones por defecto ayudan en la configuración como punto de partida pero no son adecuadas para poner un sistema en producción.

DEBILIDADES TECNOLÓGICAS

- Debilidades en Sistemas Operativos.

- Debilidades en los Protocolos. Algunas suites de protocolos, como TCP/IP, fueron diseñados sin poner énfasis en los aspectos de seguridad.

- Debilidades en las Aplicaciones. Muchas aplicaciones son escritas sin contemplar aspectos de seguridad, pues su propósito principal es la funcionalidad.

- Debilidades en los Equipos de Red. Cualquier sistema de cierta complejidad es propenso a tener errores de configuración o vulnerabilidades en su diseño. Es muy importante enfocarse en qué tipo de tráfico de red necesita soportarse, y asegurarse que se implementen los dispositivos adecuados en los lugares adecuados dentro de la red.

2.2. AMENAZAS DE SEGURIDAD

Hay distintas maneras de clasificar las amenazas de seguridad

2.2.1. AMENAZA ESTRUCTURADA

Es un esfuerzo organizado para atacar un objetivo específico. Debido a esto puede ser el tipo de amenaza más peligrosa. Las amenazas estructuradas

provienen de atacantes que típicamente están altamente motivados y son técnicamente competentes. Tales atacantes pueden actuar de manera independiente o en grupos para estudiar, desarrollar y usar técnicas de *hackeo* sofisticadas, burlando las medidas de seguridad y penetrando en las organizaciones. Ocasionalmente estos atacantes son contratados por organizaciones criminales, competidores industriales, u organizaciones auspiciadas por los gobiernos en la búsqueda de información de inteligencia. Existen otros grupos como los *hacktivistas*, que son *hackers* motivados por la búsqueda de un medio para expresar su punto de vista político.

2.2.2. AMENAZA NO ESTRUCTURADA

Es de lejos, la más común. Usualmente, es el resultado de escaneos en Internet en la búsqueda de objetivos de oportunidad. Existen diferentes tipos de programas de exploración o "*scripts*" disponibles para ser bajados de Internet que pueden ser usados para escanear un host o una red buscando vulnerabilidades. También existen programas para romper contraseñas, generadores de números de tarjetas de crédito, demonios o procesos que realizan llamadas, entre otros. A pesar que los atacantes en esta categoría pueden tener intenciones maliciosas, muchos están más interesados en el desafío intelectual de burlar las defensas que en hacer daño. Estos atacantes generalmente no son muy sofisticados y no están enfocados en un objetivo en particular. Si la seguridad de una red es muy fuerte para que ellos obtengan acceso, entonces

podrían utilizar técnicas de Denegación de Servicios (DoS) como última alternativa.

2.2.3. AMENAZAS INTERNAS

Las amenazas internas provienen generalmente de empleados o ex-empleados disgustados, y pueden ser estructuradas o no estructuradas. Las amenazas internas estructuradas representan un gran peligro para la red de la organización puesto que el atacante ya tiene acceso a la red. Sus acciones se enfocan en obtener privilegios de administrador.

2.2.4. AMENAZAS EXTERNAS

Son aquellas originadas desde una fuente externa, y pueden ser estructuradas o no estructuradas. Pueden tener intenciones maliciosas y destructivas, tales como robo de información, denegación distribuida de servicios (DDoS). También pueden presentarse como errores que generan un comportamiento inesperado en la red, tales como la desconfiguración del servidor de nombres de dominio (DNS), lo cual puede ocasionar, por ejemplo, que todos los correos se demoren o sean retornados al remitente.

2.3. LOS ATACANTES Y SUS MOTIVACIONES

La palabra atacante o intruso, en el contexto de este documento, hace referencia a aquella persona que intenta obtener acceso a una red o sistema de computadoras sin autorización.

Los atacantes o intrusos se pueden clasificar de la siguiente manera:

2.3.1. CRACKER

La definición generalizada de *Cracker* es la de aquel que usa conocimientos avanzados de las redes y de la Internet para comprometer la seguridad de una red sin autorización. Usualmente se les atribuye intenciones maliciosas, tales como las de destruir, alterar y/o robar la información de los sistemas en los que han irrumpido. Este término fue acuñado a mediados de los 80s por *hackers* que querían diferenciarse de aquellos cuyas intenciones, al entrar a un sistema o red, eran maliciosas.

Una definición más precisa de *Cracker* es la de aquel que busca maneras de burlar la seguridad o la protección de licencia de algún software.

2.3.2. HACKER

Persona que investiga la integridad y seguridad de una red o sistema operativo, empleando usualmente técnicas avanzadas de programación. Las motivaciones de un *hacker* no son siempre maliciosas. *Hacker Ético* es un término usado para

describir a los consultores en seguridad. Un *hacker* puede ser contratado por una compañía para poner a prueba los mecanismos de defensa de una organización y descubrir sus debilidades.

2.3.3. *SCRIPT KIDDIE*

Es un argot usado para describir a un *hacker* principiante quien se vale mucho de *scripts* y programas disponibles al público para poner a prueba la seguridad de una red en búsqueda de vulnerabilidades.

2.3.4. *PHREAKER*

Persona que investiga los sistemas telefónicos, usualmente para tratar de hacer llamadas gratuitas locales, nacionales y sobretodo internacionales. Algunos "roban" llamadas de tarjetas telefónicas de usuarios, mientras que otros "roban" llamadas de la compañía telefónica misma, adulterando tarjetas o aparatos telefónicos, o ingresando a los sistemas de dichas compañías telefónicas.

Las razones por las cuales alguien intenta acceder, alterar, o desestabilizar una red son tan diferentes como los intrusos mismos. Algunas de las motivaciones más comunes se mencionan a continuación:

- **Intrusión por Curiosidad**

  A veces la gente solo es curiosa con respecto a la información contenida en un sistema o red. Un incidente conocido asociado a este tipo de intrusión es el de un niño de catorce años quien ingresa al sistema de tarjetas de crédito de una compañía para husmear. Algunas veces, un empleado, puede intentar entrar al sistema de planillas solo para ver si está recibiendo un pago justo en relación a sus compañeros de trabajo. Alternativamente, un empleado puede tener curiosidad respecto a el estado financiero de la compañía o si hay algo interesante dentro de los registros de personal. Sea cual sea el enfoque de la curiosidad, el denominador común entre aquellos que irrumpen por curiosidad es el que usualmente se produce poco o ningún daño a la información.

- **Intrusión por Diversión y Desafío**

  Algunos disfrutan el desafío de ser capaces de burlar las medidas de seguridad de un sistema. Mientras más sofisticadas sean dichas medidas, mayor el desafío. Existen varios sitios en Internet, tales como foros y grupos de discusión donde los miembros publican sus más recientes conquistas y el desafío impuesto al irrumpir en los sistemas. Los miembros de estos grupos celebran los intentos exitosos y proporcionan guía a aquellos que no tuvieron éxito. Estos son sitios útiles de los cuales un administrador de seguridad puede obtener información acerca de las técnicas más recientes usadas para irrumpir en los sistemas.

- **Intrusión por Venganza**

  La venganza puede ser una motivación poderosa. Empleados descontentos o ex-empleados que tienen un buen entendimiento de la red y saben qué activos atacar, pueden causar problemas sustanciales a una organización. Es siempre recomendable cambiar las contraseñas y deshabilitar las cuentas siempre que personal clave deje la organización y asegurarse que se monitoree la red en busca de ataques a activos específicos.

- **Intrusión con Fines Lucrativos**

  Esta es otra motivación poderosa para irrumpir en una red. Obtener información de tarjetas de crédito, realizar transferencias no autorizadas de cuentas bancarias, o manipular la información de facturación puede ser extremamente lucrativo. Un ejemplo más subjetivo es el siguiente: En noviembre del 2002, una prominente agencia de noticias fue acusada de irrumpir en el sistema de computadoras de una compañía sueca para robar información relacionada con su desempeño financiero. La agencia de noticias fue acusada de obtener esta información para publicarla antes del anuncio oficial, ganando así a todas las otras agencias con la noticia. Esto muestra cómo un fin lucrativo no está directamente relacionado con la transferencia de fondos u obtener información de tarjetas de crédito. Por supuesto, el robo de secretos corporativos puede proporcionar a un competidor una significativa ventaja en el mercado.

- **Intrusión con Fines Políticos**

  El hecho que muchas economías dependan ampliamente de las transacciones electrónicas las hace vulnerables a interrupciones ante "*ciberataques*". La guerra electrónica (*Cyber Warfare*) existe y puede plantear una amenaza real a cualquier economía. Si se deseara desestabilizar una economía, el hacerlo por medios electrónicos sería el método elegido debido a un número de factores, entre los cuales se encuentran: la habilidad de lanzar un ataque desde virtualmente cualquier parte del mundo usando equipamiento y conectividad de bajo costo; y la posible carencia de medidas de seguridad de red necesarias para contrarrestar ataques.

  Otra forma de motivación política común es el *Hacktivismo*, que viene a ser el acto de seleccionar a una organización como objetivo y, desfigurar sus páginas o portales web con propósitos políticos, por ejemplo.

2.4. CLASIFICACIÓN GENERAL DE ATAQUES

2.4.1. ATAQUES DE RECONOCIMIENTO

El reconocimiento de una red es el acto de recolectar información acerca de dicha red como preparación para un posible ataque. Esta información puede ser obtenida de una gran variedad de fuentes, y más aún, existe información cuya difusión no puede ser controlada por el personal de administración de red. Algunos ejemplos de esta clase de información son los rangos de direcciones IP asignados a una organización, los cuales pueden ser determinados por un atacante mediante el uso de bases de datos de organizaciones como ARIN, RIPE o APNIC; y la información acerca de la propiedad de un nombre de dominio y de direcciones IP de servidores DNS, los cuales pueden ser determinados por un atacante, a partir de consultas a bases de datos de registros de red, tales como Network Solutions o Register.com.

Usualmente, después que un atacante identifica los rangos de la red objetivo, comienza la tarea de descubrir a los hosts, lo cual puede ser realizado de diversas maneras, como con barridos de paquetes de prueba (*pings*) ICMP, o escaneos de rangos de red.

Otra manera es usando escaneos TCP del tipo ciego (*blind-TCP scans*) mediante el uso de herramientas tales como Nmap. Estas herramientas exploran rangos de

red usando el protocolo TCP en lugar de ICMP, pudiendo buscar servicios comunes tales como: web, correo electrónico y FTP. A pesar de que el escaneo TCP ciego no provee una imagen completa de todos los posibles hosts que son alcanzables desde Internet, proporciona una lista suficientemente amplia de los servidores públicos disponibles. Este tipo de escaneo puede ser virtualmente invisible ante los ojos de los administradores de red, ya que busca los grupos de puertos que usualmente están abiertos.

Usualmente en un escaneo TCP ciego se completan solo dos etapas (SYN, SYN-ACK) de la negociación de tres vías de TCP (SYN, SYN-ACK, ACK). La herramienta de búsqueda puede no completar la negociación o enviar un paquete de RESET (RST) para cerrar la sesión TCP semi-abierta en el objetivo. Esto se grafica en la figura 2.1.

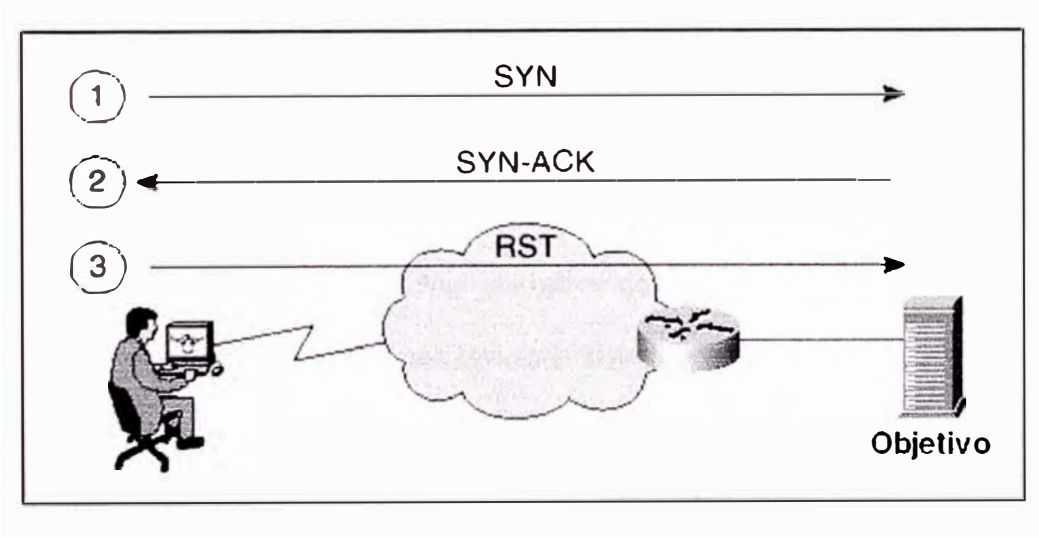

FIGURA 2.1 – Ataque de Reconocimiento: Escaneo TCP "Ciego"

Otros métodos de descubrimiento de hosts incluyen usar escaneos TCP con opciones inusuales en las banderas de los mensajes. Por ejemplo, supongamos que un atacante sospecha que los administradores de red tienen implementadas políticas o listas de control de acceso en el ruteador de borde para filtrar conexiones TCP de entrada, pero permiten flujos que son parte de conexiones ya existentes originadas desde dentro de la red. Para sortear este obstáculo, el atacante puede intentar un escaneo de tipo TCP ACK (en el cual el bit ACK en el encabezado TCP está puesto a uno) para pasar paquetes a través de las políticas o listas de control de acceso. Según está definido en el RFC 793, luego que los paquetes alcanzan su objetivo, la respuesta apropiada de un host a un paquete TCP ACK no solicitado es: enviar un paquete TCP RST de vuelta al emisor si un servicio está corriendo en el puerto en cuestión; o no responder si no hay servicio asociado con el puerto objetivo.

Una vez que el atacante ha enumerado los hosts en una red, puede pasar a identificar el sistema operativo de los hosts objetivo así como enumerar los servicios disponibles para intentar vulnerarlos. Estos ataques de reconocimiento logran determinar el sistema operativo de un host determinado, a partir de las modificaciones particulares que cada sistema operativo le hace a las banderas en los mensajes de respuesta, debido a las diferencias en las implementaciones del stack TCP/IP.

Los ataques de reconocimiento no pueden ser enteramente prevenidos. El bloquear los mensajes de Eco y los mensajes de Respuesta de Eco de ICMP en el ruteador de borde detiene los barridos PING, pero esto a expensas de sacrificar capacidades de diagnóstico importantes. Protegerse de ataques de reconocimiento de red involucra una combinación mucho más compleja de soluciones, que incluyen el filtrado ICMP, eliminar mensajes de bienvenida en los hosts, y reducir el número de servicios disponibles en los hosts.

Muchos ataques de reconocimiento han sido escritos y puestos en *scripts* que permiten a *hackers* novatos o *script kiddies* lanzar ataques a redes enteras sin mucho esfuerzo.

La siguiente lista muestra los ataques de reconocimiento más comunes:

- **Consultas DNS *Whois*:** Una consulta *whois* al DNS (servidor de nombres de dominios) proporciona al usuario no autorizado información tal como el espacio de direcciones asignado a un dominio particular y quién posee dicho dominio.

- **Barrido PING (*PING Sweep*):** El resultado de un barrido PING (*Packet InterNet Groper*) o de paquetes de prueba, puede proporcionar al usuario no autorizado el número de hosts activos en una red.

- **Escaneos Verticales:** Escanean los puertos de un único host y hacen solicitudes a diferentes servicios en cada puerto. Este método permite al usuario no autorizado determinar qué tipo de sistema operativo y qué servicios están corriendo en el host.

- **Escaneos Horizontales:** Escanean un rango de direcciones en busca de un puerto o servicio específico. Un escaneo horizontal común es el barrido FTP (*File Transfer Protocol*), el cual explora un segmento de red buscando respuestas a intentos de conexión en el puerto 21.

- **Escaneo en Bloque:** Es una combinación del escaneo vertical y horizontal, es decir, explora un segmento de red e intenta realizar conexiones en múltiples puertos de cada host del segmento.

2.4.2. ATAQUES DE DENEGACIÓN DE SERVICIOS (DoS: *Denial of Service*)

El objetivo de los ataques DoS (*Denial of Service*) no es obtener acceso a una red o a la información en una red sino más bien es hacer que un servicio o una red no esté disponible para usuarios legítimos.

Estos ataques se dividen en dos categorías generales: Ataques de Denegación No distribuida de Servicios y Ataques de Denegación Distribuida de Servicios

DENEGACIÓN NO DISTRIBUIDA DE SERVICIOS (DoS)

Estos ataques, conocidos simplemente como ataques DoS, están dirigidos contra servicios específicos tales como servicios Web, Telnet, FTP, entre otros. Son llevados a cabo abriendo y manteniendo abiertas todas las conexiones disponibles del servicio. Esto explota las debilidades en la arquitectura de red y los protocolos de red más que introducir un bug o error en un programa.

Otro método comúnmente usado en los ataques DoS es un ataque que origina que el servicio se termine —por ejemplo, a través de un *Buffer Overflow* o desborde de memoria contra un proceso BIND/DNS. Los ataques DoS incluyen el inundar al objetivo con pings lCMP o SYNs TCP, y el empleo de un ataque conocido como "Ping de la Muerte".

- **Ataque de Inundación de SYNs TCP**

  El ataque de inundación de SYNs TCP consiste en generar un gran número de conexiones semi-abiertas en el objetivo, enviando paquetes SYN, a los cuales el objetivo responde con paquetes SYN-ACK. El atacante no envía los paquetes ACK necesarios para completar la negociación de tres vías, sino que sigue enviando paquetes SYN hasta que llena la cola de SYNs TCP, y cuando esto sucede el objetivo no puede aceptar más conexiones TCP hasta que los temporizadores de algunas conexiones semi-abiertas expiren.

- **Ping de la Muerte**

  El ataque conocido como "Ping de la Muerte" consiste en enviar paquetes de prueba ICMP (*Internet Control Message Protocol*) de un tamaño determinado desde una máquina remota hacia un gran número de sistemas, ocasionando caídas de los mismos. Para comprender este tipo de ataque es necesario comprender algunos aspectos del funcionamiento de IP los que se detallan a continuación: tal como está definido en el RFC 791 los paquetes IP pueden tener una longitud máxima de 65535 (2^16 -1) bytes, lo cual incluye el encabezado IP (de típicamente 20 bytes si no hay opciones IP especificadas). Por otro lado, un mensaje ICMP de Solicitud de Eco (que se transporta en un paquete IP) tiene 8 bytes de cabecera (según RFC 792) y está seguido de un número de bytes del campo de datos. De lo anterior, el tamaño máximo de este campo es $65535 - 20 - 8 = 65507$ bytes.

Es posible enviar un paquete con más de 65507 bytes en el campo de datos de ICMP, debido a la manera como la fragmentación se realiza: para la transmisión, los paquetes IP mayores que el MTU (Unidad de Transmisión Máxima) de la capa subyacente son fragmentados en paquetes más pequeños, los cuales son reensamblados por el receptor. La fragmentación confía en el valor del campo *Offset* (posición relativa) en cada fragmento para determinar donde debe ir éste al ser reensamblado. En el último fragmento es posible combinar un número válido de *offset* con un tamaño de fragmento adecuado de tal manera que: *offset* + tamaño > 65535. Ya que típicamente los sistemas no procesan el paquete hasta que tienen todos los fragmentos y han tratado de reensamblarlo, existe la posibilidad de desbordar las variables internas de 16 bits. Esto ocasiona caídas o reinicios del sistema, volcados de memoria o del *kernel* (núcleo del Sistema Operativo) y similares.

DENEGACIÓN DISTRIBUIDA DE SERVICIOS (DDoS)

Los ataques DDoS (*Distributed Denial of Service*) buscan infligir daño, inundando la red o al host con tráfico inútil y no deseado. En este tipo de ataque, el atacante obtiene control de hosts en redes distintas de la del objetivo e instala software para controlarlos. Dichos hosts son llamados Zombies, Esclavos o Agentes. Los hosts que están entre la computadora del atacante y los Agentes se conocen como Maestros o Manejadores (*Handlers*), y son usados por los atacantes para darles un nivel adicional de protección haciendo más difícil el

rastreo. La computadora del atacante indica a los Manejadores que envíen tráfico, quienes instruyen a su vez a los Agentes para atacar un objetivo específico. Coordinando estos ataques, el atacante es capaz de incrementar el volumen de tráfico del ataque total y potencialmente sobrecargar al objetivo.

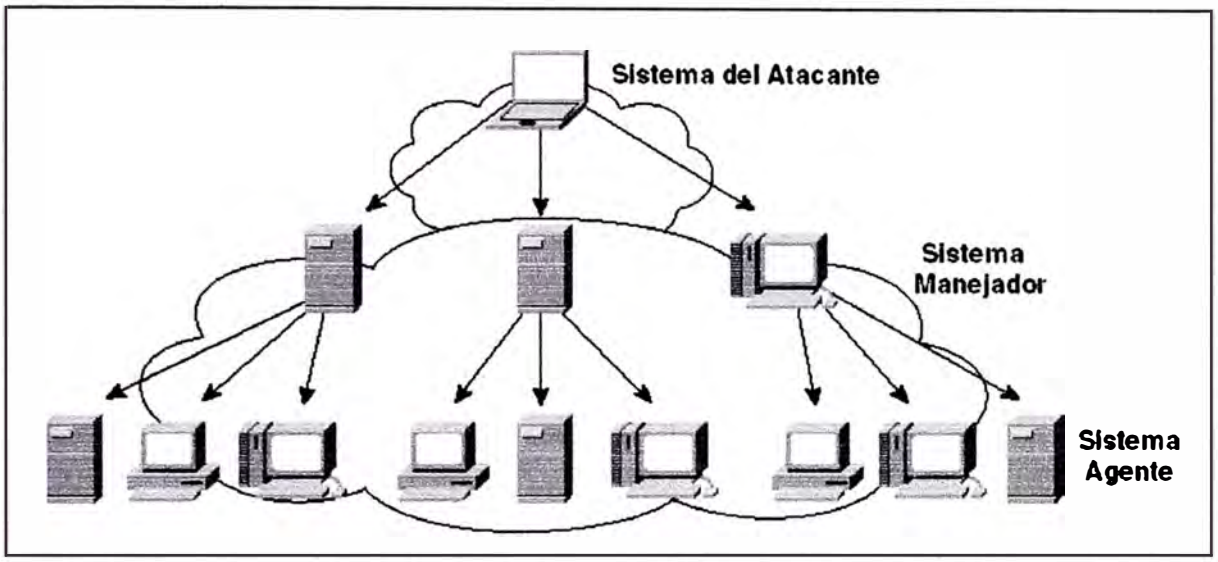

FIGURA 2.2 – Ataque DDoS o de Denegación Distribuida de Servicios

Para entender el impacto que un ataque DDoS puede tener en una red, usaremos como ejemplo una organización que tiene un enlace E1 (2 Mbps) con su proveedor de Internet, tanto para salir a Internet como para permitir acceso a su servidor web corporativo. Un atacante con 100 sistemas bajo su control inicia un ataque DDoS contra el servidor web. Asumiendo que el ancho de banda promedio de lo sistemas bajo su control es de 128 kbps, y considerando que los 100 sistemas son usados en un ataque coordinado conjunto contra el servidor

empleando todo el ancho de banda de sus respectivos enlaces, entonces el tráfico total agregado generado es de 12.8 Mbps. Esto supera en más de 6 veces el tamaño del enlace de la empresa hacia Internet.

Algunas herramientas usadas para realizar ataques DDoS son: Stacheldracht, Trin00, Tribe Flood Network (TFN), TFN2K, Mstream, y Shaft.

2.4.3. ATAQUES DE ACCESO

El objetivo de este tipo de ataque es obtener acceso a una computadora o a una red. Habiendo obtenido acceso, el atacante podrá realizar diferentes tipos de actividades, tales como:

INTERCEPCIÓN: Si el usuario no autorizado es capaz de capturar tráfico, mediante un *sniffer* por ejemplo, podrá almacenar dicha información para uso posterior. La información capturada es todo lo que circula por el segmento de red al que está conectado el atacante, y puede incluir información confidencial tal como registros personales, planillas, proyectos de investigación y desarrollo. Si circula información de administración de red, será posible capturar contraseñas para componentes específicos y tomar control de dichos equipos. Los métodos usados para interceptar tráfico varían pero usualmente requieren conectividad física con la red. Pasar de una tecnología basada en Hubs a una

basada en Switches, reduce enormemente la cantidad de tráfico que puede ser capturado por un *sniffer* de red. Sin embargo, la manera más efectiva de proteger la información sensible es almacenarla en un formato cifrado y enviarla por conexiones cifradas. Esto evitará que el atacante pueda leer la información.

MODIFICACIÓN: El acceso no autorizado a un sistema es realizado explotando una vulnerabilidad ya sea en el sistema operativo u otro paquete de software corriendo en dicho sistema. Habiendo obtenido acceso, el usuario no autorizado puede alterar los recursos del sistema. Esto no solo incluye el contenido de los archivos, sino también, las configuraciones del sistema. Por otro lado, tenemos el escalamiento no autorizado de privilegios, el cual se refiere a un usuario de una cuenta autorizada pero con bajo nivel de privilegios, que intenta obtener un mayor nivel de privilegios. Esto permite al atacante obtener mayor control del sistema o red bajo ataque.

FABRICACIÓN: Teniendo acceso al sistema atacado, el usuario no autorizado puede crear falsos objetos e introducirlos en el entorno. Esto puede incluir alterar la información o insertar vulnerabilidades empaquetadas tales como virus, gusanos, o caballos de Troya que pueden continuar atacando la red desde adentro.

- **Virus:** Los virus de computadoras varían desde molestosos hasta destructivos. Ellos consisten en código que se adhiere a software que corre en una computadora o al sector de arranque de los discos duros de la misma. De esta manera, cada vez que dicho software es ejecutado o la computadora es arrancada, el virus se reproduce y puede continuar creciendo hasta destruir el sistema de la computadora infectada.

- **Gusano o Worm:** Un gusano es un virus que explota vulnerabilidades de sistemas en una red para copiarse a sí mismo. Un gusano escanea la red buscando computadoras con una vulnerabilidad específica. Una vez que la encuentra, se copia a sí mismo en ese sistema y comienza a escanear desde allí. Los gusanos puede causar daño variable en los sistemas que infectan. Sin embargo, la actividad de propagarse dentro de una red y de una red a otra, agota los recursos del sistema infectado y consume el ancho de banda de los enlaces internos y de los enlaces hacia otras redes. Esto puede tener el efecto de aislamiento de una determinada red.

- **Troyano o Caballo de Troya:** Un caballo de Troya es un programa que usualmente aparenta realizar una función (como ser un juego, o un protector de pantalla, etc) pero hace algo completamente diferente (como corromper la información en un disco duro). Muchos tipos de caballos de Troya se adhieren a los sistemas, y sus efectos varían desde irritación menor para el

usuario a la destrucción total del sistema de archivos. Los troyanos son usados también para vulnerar los sistemas, creando cuentas que permiten a usuarios no autorizados obtener acceso o aumentar el nivel de privilegios. Algunos troyanos capturan la información del sistema y la envían a un destino que puede ser accedido por el atacante. Otros permiten al atacante tomar control total del sistema e incluso enrolarlo en un ataque DDoS.

2.5. CLASIFICACION DE ATAQUES POR SU COMPLEJIDAD

Según el nivel de complejidad, los ataques pueden ser clasificados como Rudimentarios o Sofisticados. La figura 2.3 muestra la evolución de las herramientas usadas por los *hackers* o atacantes durante las últimas décadas, indicando que éstas son cada vez más sofisticadas, mientras que el conocimiento necesario para utilizarlas es cada vez menor. Esto puede ayudar a comprender la proliferación de ataques en Internet.

2.5.1. ATAQUES RUDIMENTARIOS

ATAQUES DE RECONOCIMIENTO

Estos ataques se vieron en la sección 2.4.1.

ATAQUES DE DENEGACIÓN DE SERVICIOS (DoS)

Estos ataques se vieron en la sección 2.4.2.

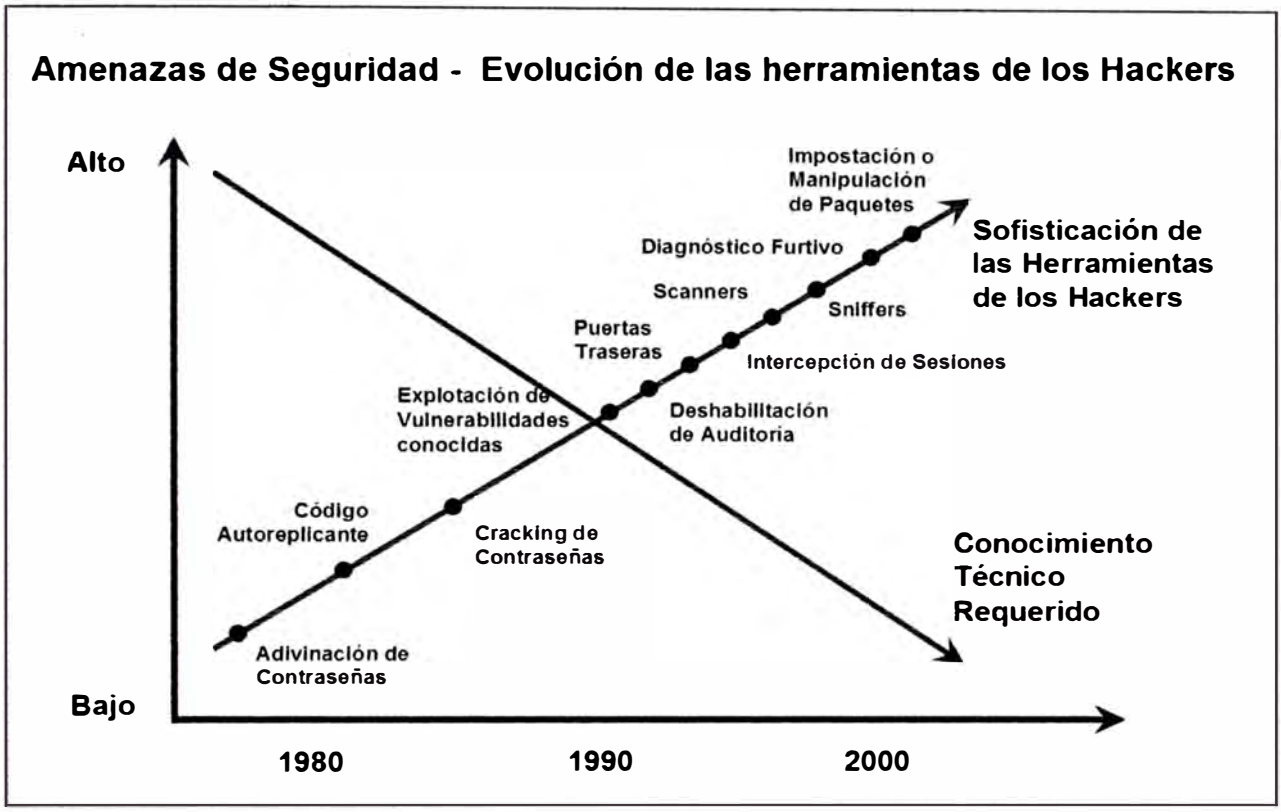

FIGURA 2.3 – Amenazas de Seguridad y Evolución de Herramientas de los *Hackers*

ATAQUES DE ACCESO NO AUTORIZADO

A pesar de que la categoría "acceso no autorizado" no está limitada a ataques específicos contra redes, cubre los tipos de ataques más comúnmente ejecutados hoy en día. Estos ataques pueden originarse tanto desde afuera de la red como dentro de ella.

Cuando los usuarios, legítimos o no, se conectan a un puerto para acceder a un servicio tal como SSH o Telnet, típicamente se encontrarán con un mensaje que advierte que el acceso no autorizado está prohibido. Si los atacantes continúan intentando acceder al sistema, sus acciones se considerarán no autorizadas. Cabe mencionar que, la ausencia de una indicación (o *banner*) de advertencia no significa que el acceso a cualquier persona sea permitido.

En esta categoría de ataque no se incluyen aquellas acciones que implican el conectarse a un puerto para ver si un servicio está activo o no; esto típicamente cae en la categoría de Reconocimiento. Esta categoría incluye cualquier intento para acceder a un sistema por parte de una persona que conscientemente sabe que no tiene permisos de acceso específicos a dicho sistema.

ATAQUES A NIVEL DE LA CAPA DE APLICACIÓN

Estos ataques apuntan a aplicaciones específicos que corren en un host, tales como servicios Web, FTP o SMTP. Los atacantes que exitosamente explotan una debilidad en la aplicación, obtienen acceso al host con el mismo nivel de privilegios que tiene la aplicación.

Algunos ejemplos de vulnerabilidades y ataques a nivel de la capa de aplicación son:

- **Vulnerabilidad IIS para traspaso de directorios o ataque UNICODE:** Uno de los blancos más conocidos para ataques a nivel de la capa de aplicación es el Internet Information Server (IIS) de Microsoft. Un atacante que explota esta vulnerabilidad del IIS, es capaz de buscar directorios en el servidor fuera del directorio raíz. Esto le permite ver archivos a los que normalmente no podría acceder. También permite al atacante ejecutar ciertos comandos y servicios para vulnerar aún más al host. Esto puede ser hecho desde un navegador de Internet típico tal como Internet Explorer o Netscape.

- **Desborde de Buffer o Buffer Overflow:** Este es otro tipo de ataque a la capa de aplicación que se puede realizar debido a la ausencia o deficiencia de chequeo de los límites de los datos ingresados en un programa. Al enviar datos, convenientemente manipulados, a un programa, el atacante es capaz de redirigir el programa para ejecutar código de su elección. Esto típicamente resulta en la creación de un intérprete de comandos o *shell* para que el atacante obtenga acceso al sistema. Estos ataques pueden ocasionar también denegación de servicios.

- **Ataques de Cadenas de Caracteres:** Estos ataques son muy similares a los de desborde de buffer, y se basan en un chequeo no apropiado de los límites en el formato de una cadena de caracteres a ser impresa por un programa. Es un ataque considerablemente más difícil de ejecutar que un desborde de

buffer, ya que se requiere inyectar apropiadamente el código del ataque en el formato de la declaración de la cadena.

ATAQUES DE EXPLOTACIÓN DE CONFIANZA (*Trust Exploitation*)

Una relación de confianza existe entre dos sistemas cuando cada sistema acuerda aceptar comunicaciones del otro sistema sin autenticar explícitamente la conexión. La confianza se establece de diversas maneras. Existen relaciones de confianza en Windows en las que un dominio puede confiar en otro dominio y proporcionar autenticación pasante. En los sistemas UNIX, existe la relación de confianza de los servicios R-. El esquema de confianza de estos difiere del de Windows en que no se necesita más autenticación que el nombre de host o dirección IP para establecer un canal de comunicación. La relación de confianza más común que existe en los sistemas UNIX es dada a través del archivo /etc/hosts/.equiv o el archivo .rhosts en la carpeta raíz (*home*) del usuario. Una solicitud de conexión es hecha sin mayor chequeo o autenticación si las tres condiciones siguientes se cumplen a la vez: una solicitud de acceso remoto es hecha usando los servicios **rlogin, rcp, rsh** o **rdist**; el nombre de la máquina origen existe en cualquiera de los archivos arriba mencionados; y el nombre de usuario usado para hacer la solicitud existe en el archivo /etc/passwd del host objetivo. Cuando estas tres condiciones se cumplen simultáneamente, la solicitud se autoriza y burla todos los mecanismos de autenticación en el host.

Otro tipo de relación de confianza puede ocurrir cuando dos o más sistemas residen en la misma subred. Se asume que por estar dentro de la misma subred, los sistemas deben ser confiables. Un sistema comprometido puede fácilmente llevar a que se comprometan otros debido a esto. Otra posibilidad existe cuando un sistema en la parte interna de un firewall confía explícitamente en un sistema en la parte externa. Un sistema externo comprometido puede llevar a que se comprometa un sistema interno.

2.5.2. ATAQUES SOFISTICADOS

IMPOSTACIÓN IP O *IP SPOOFING*

Se produce cuando un atacante, sea dentro de una red o fuera de ella, intenta obtener acceso a un recurso restringido haciendo pasar la dirección IP de su sistema por la dirección IP de otro sistema el cual tiene acceso al recurso restringido; siempre que la restricción esté basada únicamente en la dirección IP origen de la comunicación.

Típicamente, la impostación IP es llevada a cabo inyectando información dentro de un canal de comunicaciones ya existente entre dos sistemas para obtener acceso a los sistemas de computadoras. Si los atacantes no están interesados en el contenido de las respuestas del sistema objetivo, pueden usar un ataque IP *Spoofing* unidireccional o ciego en el que asumen cual será la respuesta del

objetivo y envían la información sin estar al tanto del contenido de la respuesta. Para una verdadera comunicación bidireccional, el atacante debe controlar las tablas de encaminamiento o "ruteo", para redirigir los paquetes que tienen como destino la dirección IP impostada hacia el sistema del atacante.

SNIFFERS DE PAQUETES

Un *sniffer* de paquetes es una aplicación en software que usa la tarjeta de red en modo promiscuo, siendo así capaz de recibir todos los paquetes de un segmento de red físico y entregárselos a una aplicación. Los *sniffers* de paquetes son típicamente usados para seguimiento e identificación de problemas y análisis de tráfico, pero pueden ser usados también para capturar información confidencial tal como nombres de usuario y contraseñas, ya que diversas aplicaciones, tales como Telnet, FTP, SNMP y SMTP, envían el tráfico entre cliente y servidor en texto llano, es decir, no cifrado. Si el atacante captura nombres de usuarios y contraseñas en un sistema, puede intentar usar esos mismos datos o una combinación de ellos, en otros sistemas y potencialmente obtener acceso. En el peor de los casos, el atacante podría obtener acceso a una cuenta con privilegios de administrador, emplearía dicha cuenta para crear una nueva cuenta, también con privilegios de administrador, y así podría usar esta última en cualquier momento como una puerta trasera a la red.

ATAQUES DE CONTRASEÑAS

Existen numerosas estrategias para atacar a un sistema en base a contraseñas. La estrategia más rudimentaria involucra el empleo de ataques de fuerza bruta simples mediante los cuales el atacante se conecta al sistema e intenta diversos nombres de cuentas y contraseñas comunes o por defecto. Por ejemplo, un atacante al descubrir un ruteador en una red le hará Telnet y tratará primero las contraseñas por defecto con la esperanza que eso le proporcione fácil acceso el dispositivo.

Otras vías de ataque de contraseñas incluyen Caballos de Troya instalados para capturar cuentas y contraseñas, IP *Spoofing*, y *Sniffers* de paquetes. Una vez que la información de la cuenta haya sido capturada, el atacante podrá acceder al sistema con el mismo nivel de privilegios que posee el usuario cuya cuenta ha sido comprometida. Al igual que con los *sniffers* de paquetes, si la cuenta tiene privilegios de administrador, el atacante podrá crear puertas traseras para acceder al sistema en un futuro. Adicionalmente, el atacante podría capturar los archivos /etc/passwd y /etc/shadow de un host con sistema operativo basado en UNIX o hacer un vaciado de memoria de un sistema Windows, y usar una herramienta de ataque de contraseñas, tal como L0phtCrack o John The Ripper, para romper contraseñas adicionales.

Un problema adicional con las contraseñas es que los usuarios tienden a usar las mismas contraseñas, complejas o no, en múltiples sistemas a los cuales se conectan. En consecuencia, el atacante que compromete una cuenta en un sistema puede usar esa cuenta para obtener acceso a un amplio rango de sistemas en la red.

ATAQUE DE HOMBRE EN EL MEDIO (*MAN-IN-THE-MIDDLE*)

Esta categoría cubre las situaciones en las que el atacante es capaz de interceptar paquetes que están cruzando por la red, pudiendo modificar o falsificar la información en dichos paquetes, para luego reinyectarlos. Estos ataques pueden ser usados para interceptar sesiones en curso, capturar información clasificada, crear ocurrencias DoS, corromper información transmitida, o introducir información nueva, típicamente falsa, en sesiones de red.

Un ejemplo de ataque de hombre en el medio se muestra en la figura 2.4. En el paso 1, el atacante intercepta y establece un enlace de comunicación con el cliente Web. Esto puede ser realizado impostando la dirección IP del servidor Web verdadero, en el servidor DNS del cliente. Cuando el cliente pregunte al servidor DNS por la dirección del servidor Web, el servidor DNS responderá proporcionando la dirección IP del atacante. La máquina del atacante estará corriendo un servidor Web con páginas idénticas, o casi idénticas, a las páginas Web del servidor real. El cliente se conecta al servidor Web del atacante e

ingresa su información, tal como se muestra en el paso 2. La máquina del atacante se conecta entonces con el servidor Web real, establece una conexión y pasa la información del cliente al servidor, en el paso 3. La respuesta del servidor es entregada al cliente en los pasos 4 y 5.

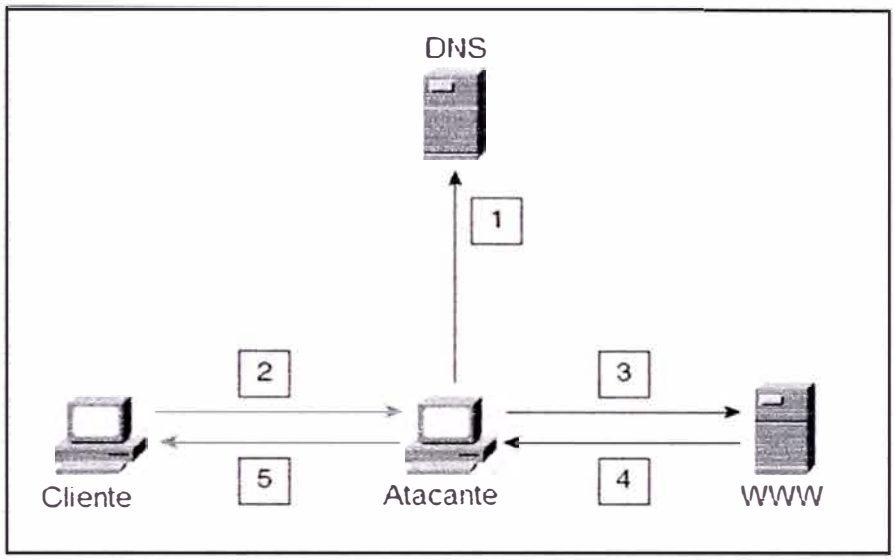

FIGURA 2.4 – Ataque de Hombre en el Medio

REDIRECCIÓN DE PUERTOS

La redirección de puertos es un caso específico de la explotación de confianza. En esencia, es un ataque de tipo túnel. En este caso, el atacante usa un host comprometido para entregar tráfico pasado a través de un puerto abierto en un firewall o en una lista de control de acceso en un ruteador, el que normalmente estaría denegado.

Esto se muestra en la figura 2.5, en donde se ha considerado un firewall con tres interfases –interna, externa, y una zona desmilitarizada (DMZ). Los hosts en la parte externa (aquellos que están en Internet) pueden llegar a los hosts en la DMZ pero no a aquellos en la parte interna. Los hosts en la parte interna (LAN) pueden llegar tanto a los hosts en la DMZ como a los de la parte externa. Los hosts en la DMZ pueden llegar a los hosts en la parte externa y a los hosts en la parte interna.

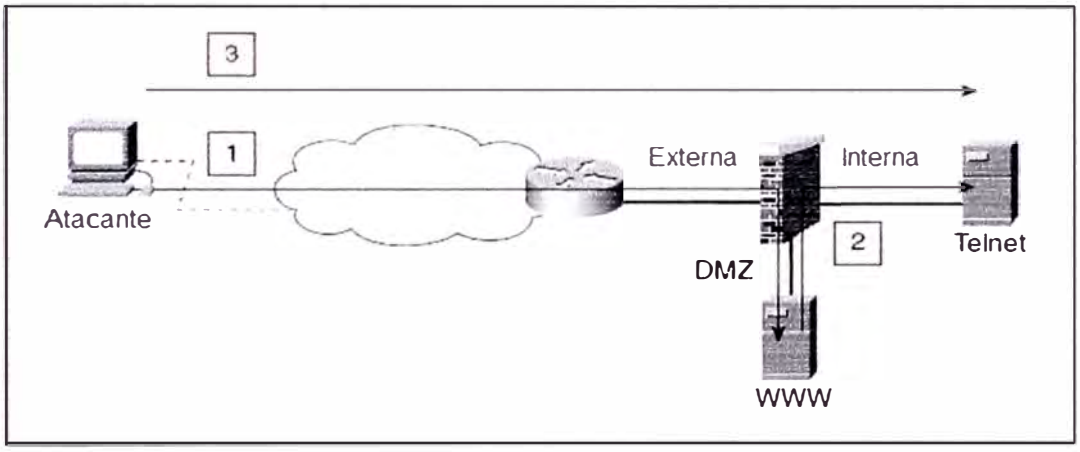

FIGURA 2.5 – Ataque de Redirección de Puertos

Un host en la DMZ cuya seguridad ha sido comprometida por un atacante, podría ser capaz de redireccionar conexiones, directamente a la LAN interna. En el paso 1 del ejemplo mostrado, un atacante compromete el servidor Web, y en el paso 2 instala un programa de redirección de puertos que toma las conexiones entrantes al puerto 80 y envía el tráfico al puerto Telnet de un host en la red

interna. El atacante simplemente se conecta al puerto Web en el host de la DMZ y es automáticamente conectado al puerto Telnet del host en la LAN interna, tal como se muestra en el paso 3. Ninguna de estas conexiones viola las políticas del firewall; sin embargo, el atacante habrá logrado conectarse a la red interna.

Ejemplos de software que puede proveer esta debilidad son: Netcat y HTTP tunnel.

VIRUS, GUSANOS, CABALLOS DE TROYA, *ADWARE*, *SPYWARE* Y MÁS

Tal como se mencionó en la sección 2.4.3, los **Virus** son pequeños pedazos de código móvil que se adhieren a otros programas o documentos y pueden infectar una computadora cuando el programa es ejecutado o el documento es abierto.

Un **Gusano (*Worm*)** es un virus que escanea las redes buscando computadoras con vulnerabilidades específicas. Una vez que encuentra una, se copia a sí mismo en ese sistema y comienza a escanear desde dicha red, con el objetivo de continuar propagándose.

Los **Caballos de Troya** son aplicaciones que aparentan ser benignas pero contienen código potencialmente malicioso que puede ser usado para atacar el sistema en el cual corren. Un ejemplo de Caballo de Troya es aquel que aparenta

ser un juego, un protector de pantalla u otra aplicación, pero que cuando se ejecuta se inserta a sí mismo en el sistema, abre uno o más puertos en el host e informa a su atacante, por medio de un correo o una sesión de chat, que el host ha sido exitosamente infectado. El atacante puede entonces conectarse al sistema desde el exterior, entrando así a la red. Como ejemplo clásico tenemos a los famosos virus Melissa y "*I Love You*", que eran *scripts* en Visual Basic adjuntados a correos electrónicos. Cuando el usuario abría el correo electrónico, el programa de correo ejecutaba el código inserto en el *script*, lo cual hacía que el virus sea enviado a cada una de las direcciones de correo que hubiera en la libreta de direcciones del usuario. Algunos Caballos de Troya, llamados RATs (*Remote Administration Tools*) o Herramientas de Administración Remota, permiten al atacante obtener acceso irrestricto a la computadora atacada siempre que esté conectada. El atacante podrá realizar todo tipo de actividades, tales como transferencia de archivos; agregar/remover programas o archivos; controlar el *mouse*, el teclado, la lectora de discos, y otros dispositivos; así como capturar todo lo que el usuario hace.

Adware es software, patrocinado por auspiciadores, que despliega anuncios cada vez que se ejecuta. Usualmente, este tipo de software está disponible para ser descargado de Internet gratuitamente, pues es la publicidad la que proporciona las ganancias a la compañía desarrolladora. A pesar de que pueden parecer inofensivos, dejando de lado la molestia que causan los *pop-ups* o anuncios

desplegados, un *Adware* puede instalar componentes en las computadoras para hacer seguimiento de información personal (incluyendo edad, género, ubicación, preferencias de compras, hábitos de navegación, etc.). Muchos programas auspiciados sólo informan que instalarán software *adware* en el sistema, en alguna línea enterrada dentro del acuerdo de licencia. En muchos casos el software no funcionará sin el componente *adware*. Algunos *adwares* pueden instalarse a sí mismos incluso si uno declina el ofrecimiento.

Los ***Spyware*** o software de monitoreo de sistemas son aplicaciones diseñadas para monitorear la actividad en las computadoras a varios niveles, pues pueden capturar virtualmente todo lo que uno haga en ellas, grabando todo lo que se teclea, las páginas web que se visitan, los correos que se reciben o envían, los diálogos de chat, y los programas que se ejecutan. Los programas de monitoreo usualmente corren en segundo plano, de tal manera que el usuario no sabe que lo monitorean. La información capturada es almacenada en la computadora en archivos de registro cifrados para su posterior recojo. Algunos programas son capaces de enviar por correo estos archivos de registro. Tradicionalmente, estos programas debían ser instalados por alguien con privilegios de administrador. Sin embargo, actualmente estas herramientas de monitoreo son disfrazadas en archivos adjuntos a los correos electrónicos o en software gratuito o *freeware*, cayendo en la categoría de Caballos de Troya.

Hay muchos otros programas sospechosos o molestosos que también pueden alojarse en las computadoras sin consentimiento expreso del usuario. Algunos pueden tener capacidades de espía (*Spyware*), mientras que otros pueden buscar molestar o afectar negativamente los recursos del sistema. Estos programas reciben muchos nombres, incluyendo: *malware*, *scumware*, parásitos, *annoyanceware*.

CAPÍTULO III

AUTENTICACIÓN, AUTORIZACIÓN Y CONTABILIDAD

CAPITULO III

AUTENTICACIÓN, AUTORIZACIÓN Y CONTABILIDAD

(AAA: *Authentication, Authorization and Accounting*)

El control de acceso es la piedra angular para asegurar la integridad, confidencialidad y disponibilidad de una red y sus recursos. El implementar la identificación y verificación de los usuarios, permitiéndoles acceso y luego auditando sus acciones proporciona una sólida armazón para la seguridad.

En una red uno necesita primero identificar y verificar la autenticidad de los usuarios, luego darles permiso de acceso sólo a algunos recursos en la red, y además tener la capacidad de auditar sus acciones dentro de la red. Estas tareas pueden ser realizadas implementando autenticación, autorización y contabilidad, o AAA (*Authentication, Authorization, Accounting*) en inglés.

Las bases de datos para autenticación, autorización y contabilidad pueden residir:

- En cada dispositivo de red al que se desea acceder, o que va a permitir el acceso a un recurso de red determinado. Esto puede ser administrativamente complejo y poco escalable.
- En servidores de seguridad especializados.

3.1. AUTENTICACIÓN

La autenticación proporciona un método para verificar la identidad de usuarios y administradores, quienes solicitan acceso a recursos de red, a través de ventanas de diálogo para ingreso de nombre de usuario y contraseña, de mecanismos de desafío y respuesta, tokens, entre otros.

En general, existen tres maneras de autenticar a un individuo:

- Algo que le pertenece: Una llave física, tarjeta de seguridad o identificación, o un generador de contraseñas válidas sólo una vez.
- Algo que conoce: Una contraseña, una llave criptográfica, o la respuesta correcta a una pregunta desafío.
- Algo que es: Alguna medida biométrica, tal como huella digital, escaneo retinal, patrón de voz, características faciales, entre otras.

Para una red, se necesita un protocolo de autenticación durante la comunicación cuando una prueba directa de autenticidad no puede ser proporcionada.

A continuación se listan diversos métodos de autenticación en redes, desde los más fuertes y complejos hasta los más débiles y sencillos:

- **Tarjetas *Token* y *Soft Tokens*:** Son dispositivos electrónicos compactos. Un PIN o código de identificación personal es proporcionado a los usuarios. El usuario se autentica con una combinación del código proporcionado por el *token* y el PIN.

- **Contraseñas válidas sólo una vez (OTP: *One-time passwords*)**: Son sistemas basados en una frase-contraseña (*pass-phrase*) secreta que genera contraseñas. Éstas son válidas sólo por una vez, y por tanto protegen de ataques de contraseñas, de ataques de interceptación de información o *eavesdropping*, y de ataques *playback*, los cuales consisten en capturar o grabar intercambios de información para luego repetirlos, haciéndose pasar por alguna de las partes.

- **Nombre de Usuario y Contraseña con fecha de expiración:** El usuario debe cambiar la contraseña cada cierto tiempo puesto que ésta expira. Usualmente se fija el tiempo para expiración en 30, 60 o 90 días.

- **Nombre de Usuario y Contraseña fijas:** La contraseña es la misma a menos que el administrador de sistemas la cambie. Este método es vulnerable a ataques con programas para romper contraseñas entre otros.

- **Sin Nombre de usuario ni Contraseña**: Esta es una invitación abierta a *hackers* que descubren el método de acceso a un sistema.

En general, se recomienda tener un sistema de Autenticación de Dos Factores (*Two-factor authentication*), el cual es un sistema que confirma la identidad de los usuarios usando dos factores o elementos distintivos – algo que ellos poseen y algo que ellos conocen. Al requerir dos formas distintas de identificación electrónica, las organizaciones mejoran la protección y confidencialidad de la información, reducen el riesgo de fraude, y se genera la sensación de que Internet puede ser un lugar seguro para hacer negocios.

Dependiendo del equipo en cuestión, se pueden definir uno o más métodos de autenticación. El hacer esto asegura la continuidad del servicio de autenticación, de fallar alguno de los métodos.

Es recomendable que el acceso a dispositivos de red, tales como ruteadores, firewalls o servidores de acceso, con propósitos de administración o gestión, sea realizado fuera de banda, es decir, por un medio distinto al que emplean los usuarios para intercambiar la

información. En general, se recomienda que todas las líneas de acceso para administración y gestión tengan implementados mecanismos de autenticación. Esto incluye los puertos de administración dedicados locales conocidos como Consolas, los puertos dedicados para acceso remoto, así como los terminales virtuales para acceso vía protocolos Telnet, SSH, entre otros.

3.2. AUTORIZACIÓN

El proceso de autorización determina los recursos de red a los cuales tiene acceso el usuario, y qué operaciones le están permitidas realizar una vez que ha sido autenticado. La información para autorización puede ser almacenada localmente en el dispositivo de red o remotamente en un servidor de seguridad. El método de autorización AAA trabaja comparando los atributos o parámetros del solicitante con aquellos almacenados en la base de datos.

3.3. CONTABILIDAD (*ACCOUNTING*)

Este servicio AAA permite registrar la actividad del usuario en la red, tal como tiempos de inicio y fin de conexión, comandos ejecutados, número de paquetes, número de bytes e identidades del usuario. La información recolectada, incluyendo la cantidad de recursos consumidos por los usuarios, puede ser usada para propósitos de facturación, auditoría y control.

3.4. SERVIDOR REMOTO DE SEGURIDAD

Una base de datos remota de seguridad proporciona políticas de seguridad uniformes para acceso remoto a través de toda la organización. Maneja todos los perfiles de usuarios remotos de manera centralizada.

A continuación, profundizaremos en tres de los protocolos para servidores de seguridad más usados: TACACS+, RADIUS y Kerberos.

3.4.1. TACACS (*Terminal Access Controller Access Control System*)

TACACS proporciona una manera centralizada de validar a los usuarios individualmente antes de que ellos puedan obtener acceso, entre otros dispositivos, a ruteadores, firewalls, y servidores de acceso, estos últimos conocidos como NAS (*Network Access Server*) o RAS (*Remote Access Server*).

TACACS fue producto del Departamento de Defensa de los Estados Unidos y está descrito en el RFC 1492. TACACS es un protocolo abierto y puede ser acomodado a la mayoría de bases de datos de usuarios y contraseñas. TACACS fue originalmente diseñado para correr en UNIX, pero actualmente corre también en Windows.

En la figura 3.1 se muestra un servidor TACACS+ atendiendo a un cliente conmutado.

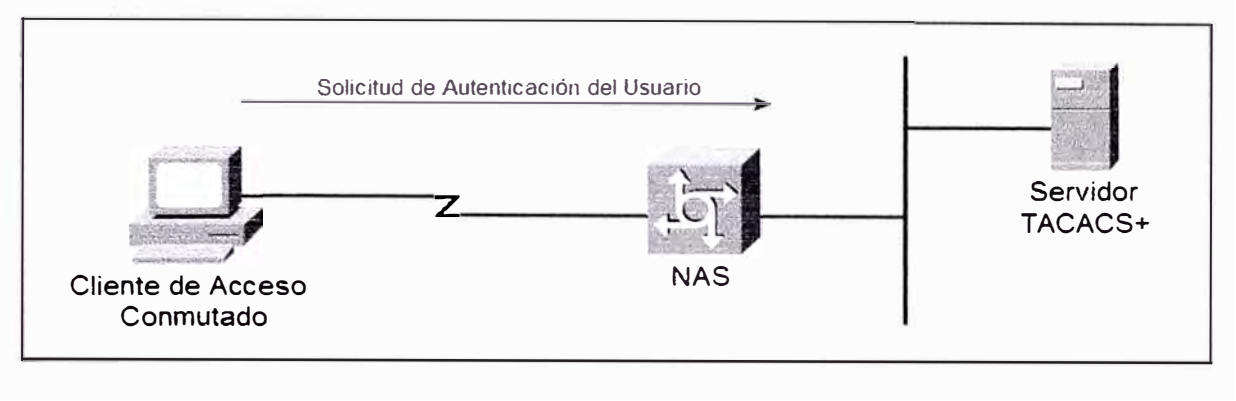

FIGURA 3.1 - Servidor TACACS+ soportando a Cliente de Acceso Conmutado

Con TACACS habilitado, el ruteador o servidor de acceso solicita al usuario un nombre de usuario y contraseña. Luego, este dispositivo pregunta al servidor TACACS acerca de la validez del nombre de usuario y contraseña proporcionados. Si la respuesta indica que los datos son válidos, entonces el acceso es permitido de acuerdo al perfil del usuario.

Las tres versiones de servidor de seguridad TACACS que existen actualmente son:

- TACACS: Un protocolo de acceso antiguo e incompatible con el nuevo protocolo TACACS+. Proporciona chequeo y autenticación de contraseñas, y notificación de las acciones del usuario para propósitos de seguridad y registro.

- XTACACS: Una extensión del antiguo protocolo TACACS, que proporcionaba funcionalidades adicionales. TACACS Extendido provee información acerca del uso del traductor de protocolos y del ruteador. Esta información es usada en archivos para auditoría y registro de UNIX.

- TACACS+: Un protocolo mejorado que proporciona información de registro detallada y control administrativo flexible sobre los procesos de autenticación y autorización.

TACACS+ proporciona mecanismos modulares separados para autenticación, autorización y contabilidad (AAA). Permite que haya un único servidor de control de acceso (el demonio TACACS+) que proporcione los servicios de autenticación, autorización y contabilidad de manera independiente. Cada servicio puede estar ligado a su propia base de datos para aprovechar otros servicios disponibles en ese servidor o en esa red, dependiendo de la capacidad del demonio.

El protocolo TACACS+ provee autenticación entre el NAS y el demonio TACACS+, y asegura la confidencialidad ya que todos los intercambios de información del protocolo entre las partes son cifrados, típicamente usando el algoritmo MD5 (*Message Digest 5*). TACACS+ puede retransmitir las contraseñas para ARA, SLIP, PAP, CHAP y telnet estándar. Por lo tanto, los

clientes pueden usar el mismo nombre de usuario y contraseña para diferentes protocolos. El puerto TCP 49 está reservado para TACACS+.

3.4.2. RADIUS (*Remote Authentication Dial-In User Service*)

RADIUS es un protocolo cliente/servidor distribuido que protege las redes de accesos no autorizados. RADIUS comprende dos elementos: un Servidor de Autenticación y Protocolos Cliente. Un NAS funciona como Cliente RADIUS. El Cliente es responsable de transmitir la información proporcionada por el usuario, a los servidores RADIUS designados, y luego actuar según la respuesta recibida. Los Servidores RADIUS son responsables de recibir solicitudes de conexión de usuarios, autenticar usuarios, y entregar toda la información de configuración necesaria para que el Cliente le proporcione el servicio al usuario. Los servidores RADIUS pueden actuar como clientes *proxy* para otras clases de servidores de autenticación. RADIUS emplea como protocolo de comunicaciones entre Cliente y Servidor, a UDP. El proceso de autenticación/autorización se realiza por el puerto 1645 (adicionalmente se usa el puerto UDP 1812).

La figura 3.2 muestra un servidor RADIUS atendiendo a un cliente conmutado.

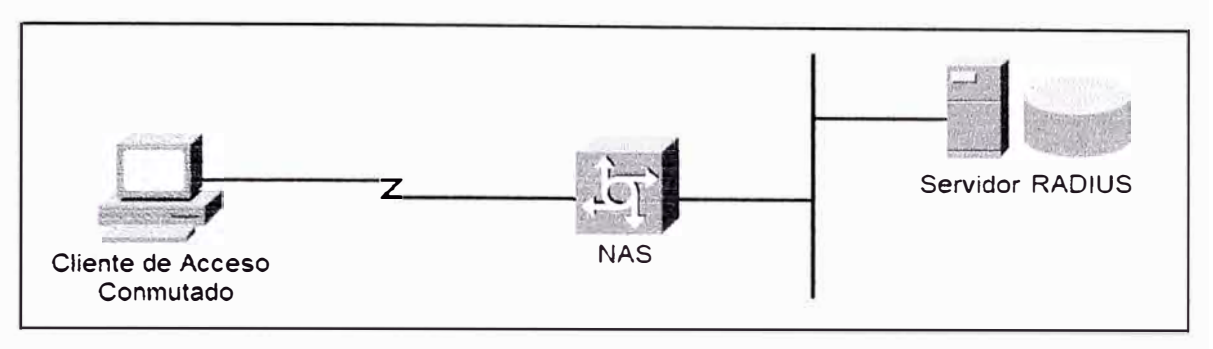

FIGURA 3.2 - Servidor RADIUS soportando a Cliente de Acceso Conmutado

RADIUS cifra sólo la contraseña en el paquete de solicitud de acceso que va del Cliente al Servidor. El resto del paquete no es cifrado. Información tal como nombre de usuario, servicios autorizados, y contabilidad podría ser capturada por un tercero.

El servidor RADIUS soporta una variedad de métodos para autenticar a los usuarios. Cuando se le proporciona el nombre de usuario y contraseña original dada por el usuario, puede soportar PPP (PAP y CHAP), *login* de UNIX, entre otros.

RADIUS combina autenticación y autorización. Los paquetes de aceptación de solicitud enviados por el servidor RADIUS al cliente contienen información de autorización. Esto hace difícil separar la autenticación de la autorización. Sin embargo, RADIUS realiza la contabilidad de manera separada, usando el puerto UDP 1646, y adicionalmente el puerto UDP 1813.

Cuando un usuario intenta acceder al sistema y autenticarse en un servidor de acceso que emplea RADIUS, se dan los siguientes pasos:

1. Se le avisa al usuario para que ingrese un nombre de usuario y contraseña.

2. El nombre de usuario y la contraseña cifrada se envían por la red hacia el servidor RADIUS.

3. El usuario recibe una de las siguientes respuestas del servidor RADIUS:
   - ACCEPT: El usuario es autenticado y validado.
   - REJECT: El usuario no es autenticado y se le avisa para que vuelva a ingresar un nombre de usuario y contraseña, o en su lugar, el acceso es denegado.
   - CHALLENGE: Se recolecta información adicional del usuario.
   - CHANGE PASSWORD: Se le pide al usuario elegir una nueva contraseña.

La respuesta ACCEPT o REJECT es enviada con información adicional que es usada para el proceso de autorización. Se debe completar la autenticación RADIUS antes de pasar a la autorización RADIUS.

3.4.3. KERBEROS

El protocolo Kerberos fue diseñado por el Instituto Tecnológico de Massachussets (MIT) con el fin de proporcionar autenticación fuerte para aplicaciones cliente/servidor usando criptografía de llave secreta. Kerberos mantiene una base de datos de sus clientes y sus llaves privadas. La llave privada es un número extenso conocido sólo por Kerberos y por el cliente al cual pertenece. En caso que el cliente sea un usuario, se trata de una contraseña cifrada. Los servicios de red que requieren autenticación se registran con Kerberos, tal como lo hacen los clientes que desean usar dichos servicios. Las llaves privadas son negociadas durante el registro.

Ya que Kerberos conoce dichas llaves privadas, puede crear mensajes que convenzan a un cliente que otro es realmente quien dice ser. Kerberos también genera llaves privadas temporales, llamadas Llaves de Sesión, las que son entregadas a dos clientes solamente. Las llaves de sesión pueden ser usadas para cifrar mensajes entre las dos partes.

Kerberos proporciona tres niveles distintos de protección. El programador de la aplicación determina cuál es el apropiado, de acuerdo con los requerimientos de la aplicación. Por ejemplo, algunas aplicaciones requieren solo que la autenticidad sea establecida en el inicio de una conexión de red y pueden asumir que mensajes posteriores de una dirección de red dada provienen de la parte

autenticada. Otras aplicaciones requieren autenticación de cada mensaje, pero no se preocupan si el contenido del mensaje es divulgado. Para este tipo de aplicaciones, Kerberos proporciona los llamados mensajes seguros. Un mayor nivel de seguridad se ofrece a través de mensajes privados, en donde cada mensaje no es solo autenticado sino también cifrado. Los mensajes privados son usados, por ejemplo, por el mismo servidor Kerberos para enviar contraseñas a través de la red.

3.5. AUTENTICACIÓN PAP, CHAP Y MS-CHAP

Tradicionalmente, los usuarios remotos conmutados se conectaban a un servidor de acceso para iniciar una sesión punto a punto PPP. PPP (*Point-to-Point Protocol*) es el protocolo de capa dos OSI estándar para el transporte de diferentes protocolos a través de conexiones seriales, conexiones a través de la Red Digital de Servicios Integrados (RDSI o ISDN en inglés), o por la Red pública de telefonía conmutada (RTC) también llamada PSTN (*Public Switched Telephone Network*) en inglés.

En la actualidad PPP soporta dos protocolos de autenticación: PPP y CHAP. Ambos son especificados en el RFC 1334 y son soportados en interfases sincrónicas y asíncronas. La autenticación vía PAP o CHAP es equivalente a teclear el nombre de usuario y contraseña cuando lo solicita el servidor. CHAP es considerado más seguro pues con él la contraseña del usuario remoto nunca es enviada a través de la conexión.

3.5.1. PAP (*Password Authentication Protocol*)

La autenticación PAP involucra un saludo de dos vías donde el nombre de usuario y la contraseña son enviadas a través del enlace en texto llano (no cifrado). Cuando se habilita PAP, el cliente remoto que intente conectarse al servidor de acceso, deberá enviar una solicitud de autenticación. Si el nombre de usuario y contraseña especificada en dicha solicitud es aceptada, el servidor de acceso enviará una aceptación de autenticación, de lo contrario enviará un mensaje de rechazo. Este proceso se muestra en la figura 3.3.

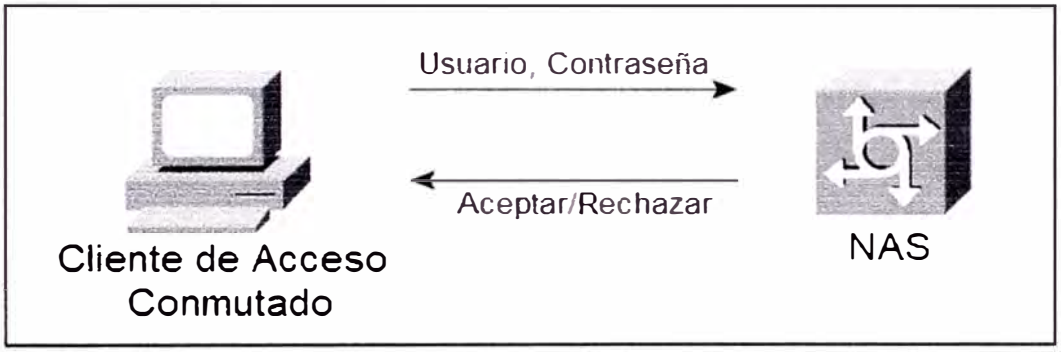

FIGURA 3.3 - Proceso de Autenticación PAP: Saludo de Dos Vías

PAP no proporciona protección contra ataques de contraseña o ataques de tipo *playback*, en los que se reenvían paquetes pertenecientes a sesiones de autenticación exitosas previas. Un analizador de protocolos podría fácilmente capturar la contraseña.

3.5.2. CHAP (*Challenge Handshake Authentication Protocol*)

CHAP es un protocolo de autenticación más seguro que PAP puesto que la contraseña nunca es enviada a través del enlace. CHAP verifica periódicamente la identidad de la contraparte usando saludos de tres vías (ver figura 3.4). Este es realizado en el establecimiento de la comunicación y puede ser repetido en cualquier momento posterior.

Una vez que la fase de establecimiento de la comunicación ha sido completada, el servidor de acceso envía un mensaje *challenge* o de desafío a la contraparte remota, quien responde con un valor calculado usando una función *hash* o unilateral (típicamente MD5). El servidor de acceso verifica la respuesta contra su propio cálculo del valor hash esperado. Si los valores coinciden, la contraparte es autenticada. De lo contrario la conexión debe ser terminada.

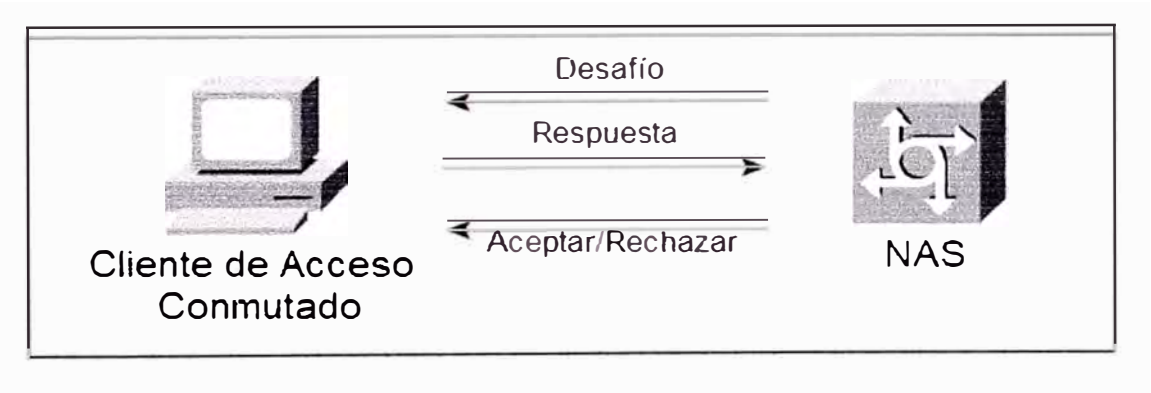

FIGURA 3.4 - Proceso de Autenticación CHAP: Saludo de Tres Vías

CHAP proporciona protección contra ataques *playback* a través del uso de un identificador que varía incrementalmente y un valor cambiante de mensaje *challenge* o de desafío. El empleo repetitivo de mensajes de desafío busca limitar el tiempo de exposición ante un ataque individual. El servidor de acceso controla la frecuencia y "temporización" de los mensajes de desafío.

Este método de autenticación depende de un valor secreto conocido solamente por el que autentica y la contraparte. El algoritmo CHAP requiere que la longitud del valor secreto sea de al menos un octeto. Sin embargo, es recomendable que el valor secreto sea de al menos la longitud del valor usado por el algoritmo de *hashing* elegido (16 octetos para MD5), para protegerse de ataques de búsqueda exhaustivos. El algoritmo de *hashing*, se elige de tal forma que no sea computacionalmente factible determinar el valor secreto del mensaje de desafío y los valores de respuesta, es decir, que sea una función unilateral.

3.5.3. MS-CHAP (*Microsoft Challenge Handshake Authentication Protocol*)

MS-CHAP es la versión CHAP de Microsoft y es una extensión del RFC 1994. Al igual que la versión estándar de CHAP, MS-CHAP es usado para autenticación PPP; pero en este caso, la autenticación se da entre la PC que usa Windows y el ruteador o servidor de acceso remoto actuando como NAS.

MS-CHAP difiere del estándar CHAP en lo siguiente:

- MS-CHAP es habilitado al negociar CHAP con el campo de algoritmo puesto a 0x80 (MS-CHAP versión 1) o 0x81 (MS-CHAP versión 2), opción 3 del protocolo de control de enlace o LCP (*Link Control Protocol*).
- El paquete de respuesta MS-CHAP tiene un formato diseñado para ser compatible con los productos Microsoft Windows, y no requiere que el autenticador almacene una contraseña en texto llano o de cifrado reversible.
- MS-CHAP provee un mecanismo de reintento de autenticación controlado por el autenticador.
- MS-CHAP provee un mecanismo de cambio de contraseña controlado por el autenticador.
- MS-CHAP define códigos de razón de falla, que se entregan como en el campo de mensaje del paquete de respuesta.

MS-CHAP versión 2 es muy similar a la versión 1 pero incompatible. En particular, ciertos campos de protocolo han sido eliminados o usados de otra manera. Adicionalmente, la versión 2 proporciona autenticación mutua.

CAPÍTULO IV

FIREWALLS

CAPITULO IV

FIREWALLS

Un firewall es un sistema diseñado para prevenir el acceso no autorizado hacia o desde una red privada. Los firewalls son frecuentemente usados para evitar que usuarios de Internet no autorizados accedan a redes privadas o Intranets que están conectadas a Internet. Todos los paquetes que entran o salen de la Intranet pasan a través del firewall, el cual examina dichos paquetes y bloquea aquellos que no cumplen un determinado criterio de seguridad.

Los firewalls pueden ser implementados en hardware, en software o en una combinación de ambos. Una de las desventajas de usar un firewall en software instalado en un servidor o cliente, es que al estar el firewall como una aplicación montada sobre un sistema operativo, las vulnerabilidades de este sistema operativo podrían afectar la operatividad y efectividad del firewall e incluso deshabilitarlo por completo.

Hoy en día, muchas empresas no toman conciencia de los riesgos de emplear un servidor firewall para varios fines tales como servidor de archivos, servidor Web, servidor de

correo, etc. Al hacer esto se abren puertos de servicios, y si la aplicación servidor o el sistema operativo son vulnerables a cierto tipo de ataque, no solo podría verse afectado el servicio en cuestión sino todos los demás, incluyendo el servicio de firewall, pudiendo desprotegerse así toda la red. Por otro lado, se pone en riesgo la confidencialidad de la información almacenada en dicho servidor, pues al tratarse de un dispositivo de borde, está constantemente expuesto a ataques provenientes de otras redes.

Después del ruteador, el firewall es considerado como la primera línea de defensa para proteger una red.

El método bajo el cual operan los firewalls puede estar basado en una de las siguientes tecnologías:

4.1. SERVIDOR PROXY FIREWALL

Un servidor *proxy* firewall es una aplicación que actúa como intermediario entre dos hosts. Esto lo logra creando y ejecutando un proceso que emula a un servicio, tal como si estuviera corriendo en el host destino. En esencia, un servidor *proxy* firewall convierte una sesión de dos partes en una sesión de cuatro partes, con el proceso intermedio emulando a los dos hosts reales. De esta manera, intercepta todos los mensajes que entran y salen de la red, escondiendo efectivamente las direcciones de red reales de los hosts. Debido a que estos firewalls operan en la capa de aplicación, se les conoce también como Firewalls de la Capa de Aplicación.

Un servicio *proxy* debe ser ejecutado para cada tipo de aplicación que el firewall soportará: Un *proxy* SMTP (*Simple Mail Transport Protocol*) para correo electrónico, un *proxy* HTTP para servicios Web, y así sucesivamente.

Debido a que los servidores *proxy* firewall centralizan toda la actividad para una aplicación en un solo servidor, representan una oportunidad ideal para realizar una variedad de funciones útiles, tales como la inspección de paquetes a profundidad. Esta es la razón por la que actualmente muchos firewalls incorporan alguna forma de arquitectura de servidor *proxy*. Por ejemplo, paquetes entrantes dirigidos a un servidor configurado estrictamente para proporcionar información (digamos, un servidor FTP), pueden ser inspeccionados para ver si contienen comandos para escritura (tales como el comando PUT). De esta manera, el servidor *proxy* podría permitir solamente conexiones con comandos para lectura.

Pros: Buen nivel de seguridad, completo conocimiento de lo que ocurre en la capa de aplicación.

Contras: Bajo desempeño, soporte limitado a ciertas aplicaciones, escalabilidad limitada.

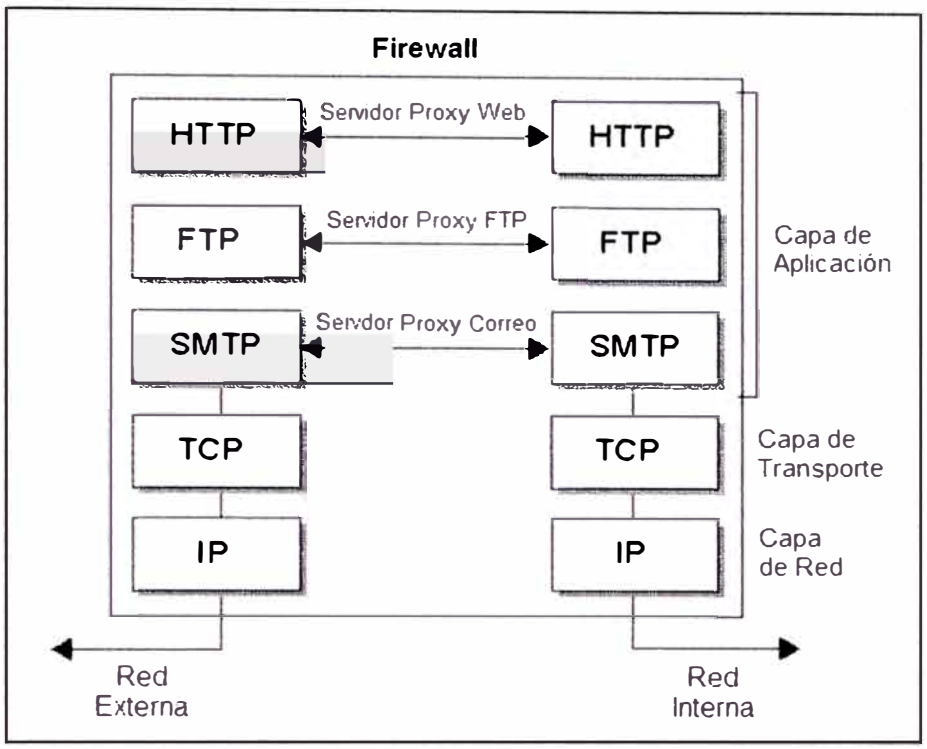

FIGURA 4.1 - Servidor *Proxy* Firewall

4.2. FIREWALL DE FILTRADO DE PAQUETES

Un firewall de filtrado de paquetes convencional, también llamado de filtrado estático, bloquea o permite direcciones origen y destino, es decir, analiza un paquete basándose en la información del encabezado IP de la capa de red, y a lo más en la información de la capa de transporte (puertos TCP y UDP). Esta técnica de filtrado es susceptible a ataques de impostación de IPs.

Pros: Independencia de las aplicaciones, alto desempeño, escalabilidad.

Contras: Bajo nivel de seguridad, no filtra por encima de la capa de red/transporte pues no maneja información que depende del contexto o del estado de las aplicaciones.

4.3. FIREWALL DE INSPECCIÓN DE ESTADOS (*STATEFUL INSPECTION*)

Un Firewall de Inspección de Estados, también conocido como de filtrado dinámico de paquetes, no se limita a examinar la información a nivel de la capa de red y transporte, sino que analiza el contenido del paquete incluyendo la información del protocolo de la capa de aplicación (tal como la información de una conexión FTP) para aprender acerca del estado de la sesión TCP o UDP. Esto permite soportar protocolos cuyo funcionamiento involucra la creación de múltiples canales como resultado de las negociaciones en el canal de control. Muchos de los protocolos multimedia, como H.323 y RealAudio, así como otros protocolos, entre ellos FTP, RPC y SQL*Net usan múltiples canales para sus comunicaciones.

Un Firewall de Inspección de Estados, hace un seguimiento y mantiene una tabla de todas las sesiones que atraviesan cada una de las interfases del firewall, asegurándose que sean válidas y no sean intervenidas. Una sesión es válida si, por ejemplo, se completan todos los pasos de la negociación o saludo de tres vías de TCP. Las sesiones no válidas serían entonces aquellas que no han completado todos estos pasos (llamadas también sesiones embrionarias), y por tanto se podrían tratar de intentos de ataques de denegación de servicios.

Adicionalmente, un Firewall con *Stateful Inspection* cierra puertos hasta que una conexión a un puerto específico sea solicitada. Por ejemplo, si un usuario en la parte interna del firewall accede a una página de un servidor Web en Internet (parte externa), los paquetes de retorno de este servidor hacia el usuario deberán ser permitidos en los puertos especificados en la sesión, y sólo durante la duración de la misma. En el caso de un firewall de filtrado de paquetes o estático, implementar este simple esquema de navegación requeriría que hubiera, todo el tiempo, un amplio rango de puertos abiertos (del puerto 1024 en adelante) para aceptar paquetes de un rango muy amplio de direcciones, lo cual implica un riesgo de seguridad.

En un firewall de inspección de estados las decisiones de filtrado se basan no solo en reglas predefinidas o estáticas sino también en el contexto que ha sido establecido por paquetes anteriores que pasaron a través del firewall.

Cabe mencionar que, a diferencia de las sesiones TCP, las sesiones UDP no están orientadas a la conexión, es decir, no existe un establecimiento de la sesión, ni verificación de la entrega de información. Esta característica hace más difícil identificar paquetes que pertenecen a la misma sesión UDP. Cada paquete UDP de solicitud permitido a través del firewall es registrado, y los paquetes UDP que viajan en dirección opuesta son verificados contra una lista de sesiones pendientes para asegurarse que cada paquete UDP esté en un contexto autorizado. Un paquete que es una respuesta genuina a

una solicitud es entregado; los demás son descartados. De igual manera, si una respuesta no llega dentro de un período de tiempo especificado, la conexión expira.

A la empresa de seguridad Check Point se le acredita el haber acuñado el término Inspección de Estados (*Stateful Inspection*) al usarlo en su software Firewall-1 por primera vez en 1993.

Pros: Buen nivel de seguridad, completo conocimiento de lo que ocurre en la capa de aplicación, alto desempeño, escalabilidad, transparencia.

CAPÍTULO V

SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS

CAPITULO V

SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS

5.1. SISTEMA DE DETECCIÓN DE INTRUSOS (IDS: *Intrusion Detection System*)

La detección de intrusos se ha convertido en una de las tecnologías de red críticas para dar una adecuada seguridad a una red.

Según el método de detección de ataques, existen dos tipos de IDSs:

- Basados en firmas o patrones predefinidos de ataque, los que hay que actualizar periódicamente. Este método es análogo al usado por muchos Antivirus.
- Basados en Anomalías o Heurísticos, que toman decisiones basados en características de comportamiento predefinidas consideradas como normales o aceptables.

De manera general, existen dos categorías de IDSs:

- IDS de red (NIDS o *Network* IDS)
- IDS basado en Host (HIDS o Host IDS)

5.1.1. IDS DE RED (NIDS: *Network Intrusion Detection System*)

Los NIDSs son dispositivos en hardware que monitorean el tráfico de red en busca de patrones de ataque distintivos de acuerdo con su base de datos, o en busca de anomalías, es decir, tráfico no considerado dentro de lo normal de acuerdo a ciertas reglas o perfiles predefinidos. Dicho tráfico podría ser un indicativo de un ataque en potencia.

Estos dispositivos se colocan en distintos segmentos de red (dominios de *broadcast*), y específicamente, en puntos estratégicos tales como puntos de acceso a otras redes (e.g. Internet, Extranets), zonas de concentración de accesos remotos, zonas desmilitarizadas (DMZ), granjas de servidores, e incluso en los segmentos de red donde están los usuarios LAN.

Cuando un NIDS detecta un ataque, puede simplemente registrar y enviar una alarma a una consola de administración, o en algunos tipos de NIDS más avanzados, terminar o bloquear dicha conexión insertando nuevas reglas en las listas de control de acceso de ruteadores y/o firewalls.

Típicamente, un NIDS se conecta a un puerto de un switch, en modo promiscuo, para escuchar todo el tráfico de un segmento de red, de una VLAN determinada, o de ciertos hosts conectados a puertos del switch pertenecientes a la misma VLAN. En este sentido el NIDS se comporta como un *sniffer* de paquetes.

En escenarios donde los switches no tienen la capacidad de permitir monitoreo de puertos, se colocan los *Network Taps*, que son dispositivos capaces de interceptar la información de enlaces de fibra y cobre, resultando esto transparente para los demás dispositivos de red.

En el caso de contar con un hub, en vez de un switch, basta conectar el NIDS a cualquier puerto, puesto que por su naturaleza un hub enviará una copia de la información recibida en un puerto a todos los demás puertos.

El monitoreo se realiza desde una interfaz específica, mientras que las alarmas son transmitidas a través de la interfaz de control.

5.1.2. IDS EN HOST (HIDS: *Host Intrusion Detection System*)

Un Host IDS es un software que se instala y ejecuta en un sistema terminal tal como un servidor, una estación de trabajo o una computadora portátil (*laptop*). La función de un HIDS es proporcionar una última línea de defensa en caso que el NIDS falle en detectar un ataque, lo cual puede ocurrir ya sea si la base de datos de firmas del NIDS está desactualizada o si el atacante es capaz de emplear una técnica de evasión para esconder un ataque ante el NIDS. Los HIDS se usan también en lugar de un NIDS en el caso que sean pocos los hosts en la red, que haya un bajo nivel de amenaza, o resulte prohibitivo a nivel de costos.

Los HIDS se sitúan entre el kernel o núcleo del Sistema Operativo y los procesos. Monitorean al host y detectan acciones no permitidas, tales como el reemplazo de un archivo crítico, la ejecución de una instrucción "ilegal" en la memoria de la computadora, o llamadas al sistema por parte de programas que no tienen autorización.

Ciertos Host IDSs (IPSs) no solo tienen la capacidad de detectar ataques y reportarlos, sino que también previenen ataques conocidos y no conocidos usando una combinación de reglas de comportamiento definidas, y una base de datos de firmas de ataques. Por ejemplo, pueden detener la ejecución de programas o archivos con código potencialmente dañino.

En la figura 5.1 se muestra una red en la que se han implementado sistemas Host IDS y *Network* IDS, y se observa su correcta ubicación dentro de la misma.

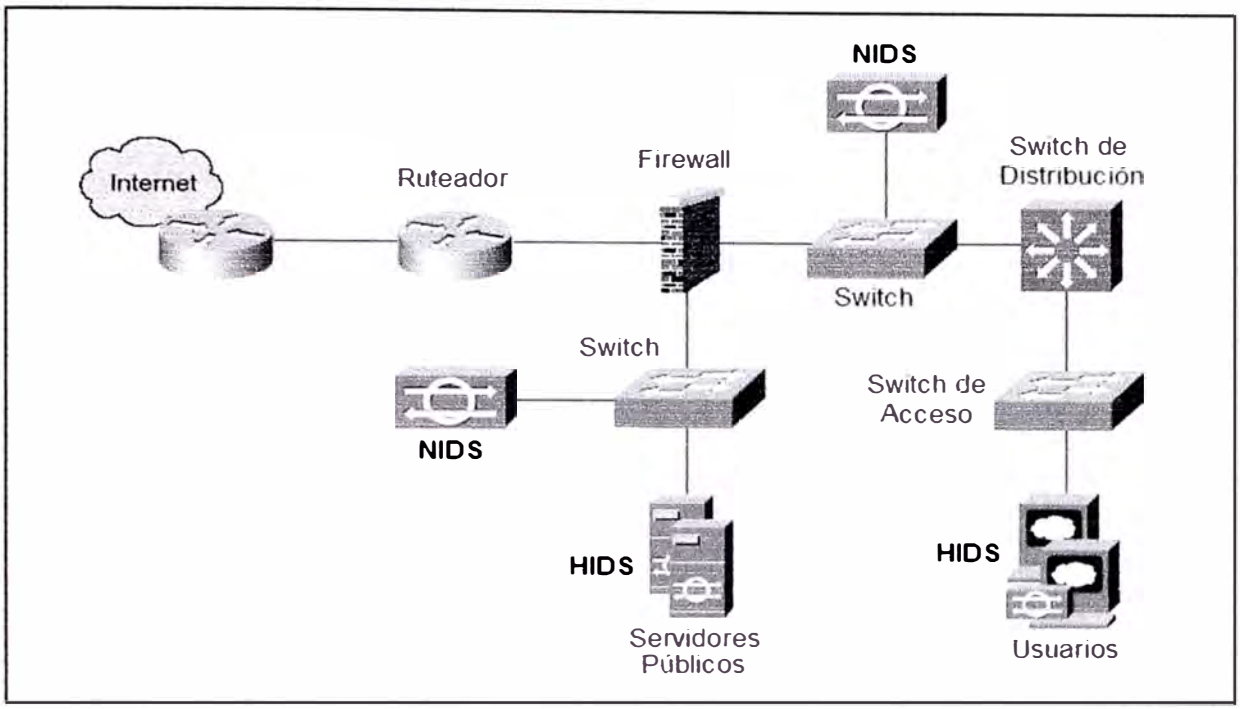

FIGURA 5.1 - Ubicación de Host IDSs y Network IDSs en una red

5.2. SISTEMA DE PREVENCIÓN DE INTRUSOS (IPS: *Intrusion Prevention System*)

Se considera a los IPSs o Sistemas de Prevención de Intrusos, la nueva raza de IDSs. Los IPSs son muy similares en funcionamiento a los IDSs. Sin embargo, existen importantes diferencias que se verán a continuación:

5.2.1. IPS DE RED (NIPS: *Network Intrusion Prevention System*)

A diferencia de los *Network* IDSs que se sitúan en un segmento de red escuchando el tráfico que circula pero que no lo atraviesa, los *Network* IPSs se sitúan en medio del tráfico que van a inspeccionar, tal como un firewall. Debido

a que el tráfico debe pasar a través de él para llegar a su destino, un NIPS no solo es capaz de alertar acerca de una posible actividad hostil, sino que también tiene la habilidad de bloquear dicho tráfico por sí mismo.

Antes de elegir un IPS de red es importante tener en consideración la capacidad efectiva de tráfico que puede manejar y tener pensado un esquema de contingencia en caso este falle.

5.2.2. IPS EN HOST (HIPS: *Host Intrusion Prevention System*)

Un Host IPS no solo detecta ataques sino que también los previene, siendo proactivos e integrándose con el firewall en el host. Así pueden, por ejemplo, bloquear paquetes maliciosos que llegan al host, a nivel de la capa de red, antes que puedan hacer daño a la aplicación a la que apuntan.

En la figura 5.2 se muestra una red en la que se han implementado sistemas Host IPS y *Network* IPS, y se observa su correcta ubicación dentro de la misma.

Sea cual sea la modalidad de IDS/IPS elegida, hay que realizar una puesta a punto del IDS/IPS antes de ponerlo en producción. De lo contrario, podría darse la situación en la que se niegue tráfico que debería ser permitido, generando así falsas alarmas o falsos positivos, y afectando el normal funcionamiento de la red o de los hosts.

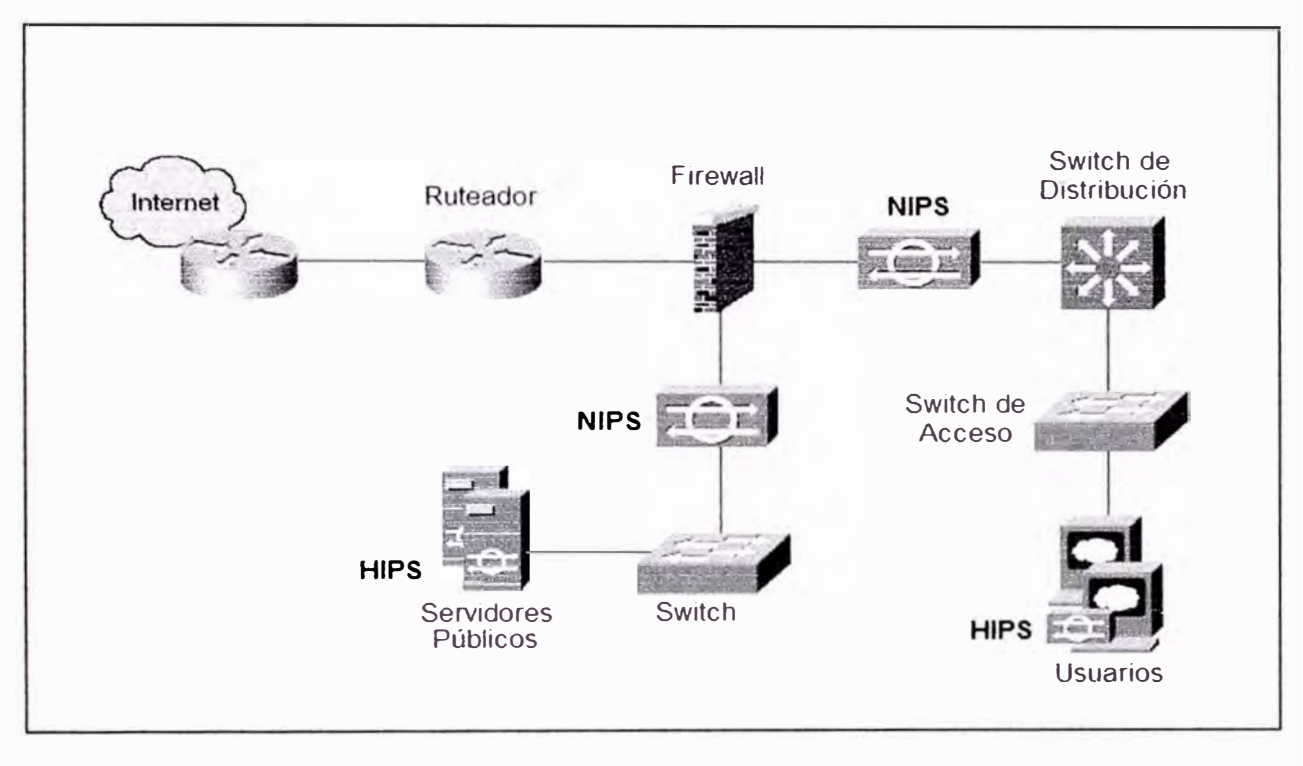

FIGURA 5.2 - Ubicación de Host IPSs y *Network* IPSs en una red

CAPÍTULO VI

ADMINISTRACIÓN DE RED

CAPITULO VI

ADMINISTRACIÓN DE RED

La administración de redes implica la ejecución de una serie de funciones para ayudar a mantener, monitorear y hacer seguimiento ante problemas relacionados con los recursos de red.

6.1. TIPOS DE ADMINISTRACIÓN DE RED

El flujo de tráfico generado por las acciones de administración puede ser de dos tipos: Dentro de la Banda (*In-band*) o Fuera de Banda (*Out-band*)

6.1.1. ADMINISTRACIÓN DENTRO DE LA BANDA

Se refiere al flujo de información de administración que sigue la misma ruta o usa los mismos medios que el tráfico convencional, y debido a esto es considerado menos seguro que la administración fuera de banda, puesto que la información de administración podría ser capturada, modificada y usada por un atacante.

Por lo tanto, uno debe tener siempre presente los posibles riesgos de seguridad que implica tener una administración de este tipo, y en lo posible, implementar técnicas tales como limitar la administración de red a sólo lectura, usar protocolos que establezcan túneles y cifren la información, o usar variantes más seguras de los protocolos de administración.

6.1.2. ADMINISTRACIÓN FUERA DE BANDA

Se refiere al flujo de información de administración que no sigue la misma ruta ni usa los mismos medios que el tráfico convencional. Usualmente, se usa una red paralela o una ruta alterna para este propósito. Esta ruta se conecta directamente a un puerto de red dedicado en el dispositivo a administrar o finaliza en otro dispositivo conocido como servidor terminal, el que a su vez tiene una conexión directa al puerto de consola del dispositivo a administrar.

Generalmente, la administración fuera de banda es considerada más segura, puesto que el segmento de red de administración es privado y, estando aislado del tráfico de red convencional, es menos propenso a ser comprometido por un atacante. Sin embargo, este tipo de administración es generalmente la menos costo-efectiva, ya que cada dispositivo requiere una conexión dedicada a la red de administración.

Mitigación de Ataques al Tráfico de Administración

Para mitigar ataques dirigidos al tráfico de administración, hay que considerar lo siguiente:

- ☑ Utilizar preferentemente administración fuera de banda para tener el nivel de seguridad más alto.
- ☑ Cuando el tráfico de administración esté dentro de la banda, deberá ponerse más énfasis en asegurar el transporte que realizan los protocolos de administración, usando por ejemplo técnicas de cifrado en túneles, tales como IPSec. Si esto no fuera posible, utilizar un protocolo de administración seguro.
- ☑ Si un dispositivo que requiere administración reside fuera de la red, se recomienda usar túneles IPSec para administrarlo. Este túnel deberá originarse en la red de administración y terminar directamente en el dispositivo.
- ☑ Cuando el tráfico de administración no pueda ser asegurado debido a limitaciones de los equipos, se debe tener en cuenta que podría existir interceptación y falsificación de la información.

6.2. PROTOCOLOS DE ADMINISTRACIÓN DE RED

Diferentes protocolos que proporcionan una gran variedad de servicios son empleados para administrar una red. Estos protocolos varían desde protocolos de administración de configuraciones, pasando por protocolos de monitoreo y registro de eventos, hasta protocolos de sincronización de tiempo.

La primera preocupación al elegir un tipo de protocolo para que logre un objetivo de administración en particular, es el nivel de seguridad que dicho protocolo provee. Inherentemente algunos protocolos de administración son mucho más seguros que otros que realizan una función similar. De igual forma, una versión diferente del mismo protocolo podría proveer un nivel mejorado de seguridad comparado con versiones anteriores.

6.2.1. PROTOCOLOS DE ACCESO REMOTO

TELNET

Telnet es un protocolo de emulación de terminal, comúnmente usado en redes basadas en TCP/IP. Telnet permite acceso remoto en texto llano a dispositivos administrados, proporcionando así, el método menos seguro de administración remota. La iniciación de una sesión Telnet requiere que el usuario acceda al dispositivo ingresando credenciales de autenticación válidas, las que normalmente consisten en un nombre de usuario y contraseña. Esta autenticación puede tomar lugar localmente en el dispositivo remoto o puede ser pasada a un servidor de autenticación, tal como un servidor RADIUS o TACACS+. Telnet usa el puerto TCP 23 para establecer sus conexiones.

SSH (*Secure Shell*)

SSH es un programa de interfaz de usuario seguro, que puede usarse para acceder a un dispositivo remoto y ejecutar comandos. Fue desarrollado por SSH Communication Security Inc., y proporciona autenticación fuerte y comunicación segura sobre enlaces no seguros.

SSH proporciona protección contra ataques DNS, ataques de impostación de IP o IP *Spoofing*, y ataques de encaminamiento o "ruteo" de IP origen. Si un atacante comprometiera la seguridad de una red, solo sería capaz de forzar la desconexión de una sesión SSH. El atacante no podría tomar control de la sesión (*hijacking*) o realizar un ataque de *playback* ya que el cifrado estaría habilitado.

La información de inicio de sesión y todo el resto del tráfico son intercambiados en texto cifrado, haciendo casi imposible que un atacante obtenga las contraseñas.

SSH usa el puerto TCP 22 para establecer sus conexiones, y los métodos de autenticación incluyen RSA, SecurID y contraseñas, que al igual que con Telnet pueden residir en el equipo o en servidores de autenticación.

SSL (*Secure Socket Layer*)

SSL es un protocolo que proporciona seguridad y privacidad en una conexión. El protocolo, desarrollado por Netscape Communications Corporation, mantiene la seguridad y la integridad de las comunicaciones usando autenticación y cifrado. SSL soporta autenticación de servidor y cliente. Cuando se inicia una sesión SSL, el servidor envía su llave pública al cliente. El cliente luego usa esta llave pública para generar una llave secreta aleatoria que es enviada de vuelta hacia el servidor, creando así un intercambio de llave secreta para la sesión. Durante el intercambio inicial, el sistema criptográfico RSA de llave pública es usado. Una vez que este intercambio inicial es exitoso, diversos cifradores están disponibles, incluyendo RC2 (*River's Cipher 2*), IDEA (*International Data Encryption Algorithm*), DES (*Data Encryption Standard*) y 3DES (*Triple-DES*). SSL usa el puerto TCP 443 para sus comunicaciones.

Recientemente, SSL ha sido fusionado por el IETF con otros protocolos y métodos de autenticación, en un nuevo protocolo conocido como TLS (*Transport Layer Security*).

6.2.2. Protocolo de Reportes y Registro de Eventos: Syslog

El protocolo Syslog es un mecanismo de transporte usado para enviar mensajes de eventos a través de una red. Estos eventos pueden ser el resultado de iniciar o

detener un proceso, algún umbral que haya sido alcanzado, o los reportes de la situación actual de alguna condición o proceso.

Toda la información de syslog es enviada en texto llano entre el dispositivo administrado y el servidor de registro o la consola de administración. Syslog no posee mecanismos para autenticación, y no se realiza un chequeo de la integridad del mensaje para asegurar que la información no haya sido manipulada en tránsito. Por lo tanto, un atacante podría alterar la información en los mensajes syslog en un intento de confundir al administrador de red o incluso disfrazar o disimular sus acciones.

Syslog usa el puerto UDP 514. Para mitigar ataques contra Syslog se deberá cifrar su tráfico dentro de un túnel IPSec, siempre que sea posible.

6.2.3. Protocolo de Monitoreo y Control: SNMP

SNMP (*Simple Network Management Protocol*) es un protocolo de monitoreo y control de red ampliamente usado. Fue desarrollado al final de los años 80s, y se ha convertido en un estándar de facto para administración inter-redes.

SNMP v1 es la versión original de SNMP y está definida en el RFC 1157. En esta versión, la seguridad está basada en cadenas de comunidad (*community strings*).

SNMP v2c es una versión experimental definida en los RFC 1901, 1905 y 1906. Usa un esquema de seguridad para cadenas de comunidad tal como se define en SNMP v1. La 'c' en SNMP v2c significa "comunidad".

SNMP versión 3 es la versión más reciente y segura de este protocolo, tradicionalmente inseguro. Soporta verificación de integridad de mensajes, autenticación y cifrado de la información de administración en la red. SNMP v3 está definido en los RFCs del 2273 hasta el 2275. Soporta autenticación por usuario, MD5, SHA y cifrado DES-56.

Un sistema SNMP contiene dos elementos principales: Administrador, y Agentes.

El Administrador es la interfaz que el administrador de red emplea para realizar las funciones de administración de red. A esta interfaz se le llama también Consola de Administración o Motor de Administración.

Los Agentes son hardware y software que reporta las actividades en cada dispositivo de red que está siendo administrado, las cuales son comunicadas al Administrador. La información que es devuelta por estos agentes está estructurada en un formato jerárquico llamado MIB (*Management Information Base*). Cada MIB define qué es lo que se obtiene del dispositivo administrado y

qué puede ser controlado en él. Los Agentes pueden responder a solicitudes específicas del Administrador SNMP o pueden ser configurados para reportar eventos mientras ocurren usando un mensaje especial llamado TRAP asíncrono.

A la información que sólo puede ser recibida del dispositivo pero no escrita en el dispositivo vía SNMP se le denomina de acceso de sólo lectura, mientras que a la información que puede ser leída y escrita en el dispositivo se le denomina de acceso de lectura-escritura. Este acceso de lectura-escritura es controlado por las cadenas de comunidad (*community strings*), las que proporcionan una forma rudimentaria de seguridad en las versiones iniciales de SNMP. En estas versiones iniciales, las cadenas de comunidad eran transmitidas en texto llano y por tanto estaban propensas a ser capturadas por un *sniffer* de paquetes. Una vez que las cadenas de comunidad son comprometidas, el atacante puede reconfigurar un dispositivo remoto, vía SNMP, si el acceso de lectura-escritura ha sido permitido. Un nivel adicional de seguridad puede ser incorporado a SNMP con el uso de políticas o listas de control de acceso, para restringir el acceso SNMP a ciertos dispositivos únicamente.

SNMP usa los puertos UDP 161 y 162. Los Agentes escuchan en el puerto UDP 161 mientras que los *traps* asíncronos son recibidos en el puerto UDP 162 por la consola de administración.

Para mitigar los ataques a SNMP, a menos que se use SNMP v3, es recomendable usar cadenas de comunidad de sólo lectura. También restringir el acceso a los dispositivos a sólo las consolas de administración a través de políticas o listas de control de acceso. Finalmente, como medida adicional de seguridad, se puede usar un protocolo de cifrado en túnel, tal como IPSec, para un transporte seguro de la información.

6.2.4. Protocolo de Administración de Archivos: TFTP

TFTP (*Trivial File Transfer Protocol*) es un protocolo de transferencia de archivos para TCP/IP usado comúnmente por diversos dispositivos de red para transferir configuraciones o archivos de sistema a través de una red. A diferencia de FTP, TFTP no maneja directorios ni contraseñas. La información es enviada en texto llano, lo cual hace a TFTP vulnerable a ataques con *sniffers* de paquetes y, consecuentemente la información sensible podría ser obtenida. Para mitigar ataques contra TFTP, se deberá cifrar el tráfico TFTP mediante túneles IPSec, siempre que sea posible.

TFTP usa el puerto UDP 69 para control y puertos UDP mayores que 1023 para el flujo de datos entre el dispositivo remoto y el servidor TFTP.

6.2.5. Protocolo de Sincronización de Tiempo: NTP

NTP (*Network Time Protocol*) es un protocolo TCP/IP que facilita la sincronización de tiempo en los dispositivos de red con una fuente de tiempo común. La sincronización precisa de los relojes de los dispositivos de red es crítica para el uso de certificados digitales y en el estampado de tiempos para eventos. Consecuentemente, la fuente de tiempo que se quiera usar para la sincronización debe ser confiable. Es normal hacer que NTP haga la sincronización con una fuente autoritativa de tiempo tal como un reloj atómico o de radio, o de un servidor de tiempo público de Internet, y que luego distribuya esta referencia a través de la red.

NTP versión 3, definido en el RFC 1305, soporta autenticación criptográfica entre las partes. Sin esta autenticación, sería posible para un atacante realizar un ataque DoS en el sistema enviando información NTP falsa. Esto podría causar que los certificados digitales expiren y sean afectados los servicios que dependen de estos. Un atacante también podría hacer que sus acciones sean difíciles de rastrear si el reloj del sistema fuera alterado.

NTP usa el puerto UDP 123 para la sincronización de tiempo. Para mitigar ataques a NTP se recomienda usar la versión 3 de NTP, que tiene autenticación criptográfica, y a la vez implementar restricciones a través de políticas o listas de control de acceso indicando las partes que participarán en el intercambio NTP.

CAPÍTULO VII

OBJETIVOS DE ATAQUE Y TÉCNICAS DE DEFENSA

CAPITULO VII

OBJETIVOS DE ATAQUE Y TÉCNICAS DE DEFENSA

7.1. LOS RUTEADORES SON OBJETIVOS

Tres funciones de los ruteadores son discutidas en esta sección. Primero, los ruteadores son dispositivos que anuncian direcciones de red a través de protocolos de ruteo. Segundo, los ruteadores pueden filtrar el tráfico de red. Tercero, los ruteadores conectan un red con otra; una función que ha hecho que los ruteadores sean un objetivo popular para intrusos. Debido a esto, el protegerlos es crítico. Las posturas de seguridad de un ruteador pueden ser mejoradas siguiendo las siguientes recomendaciones:

- **Implementar Políticas o Listas de Control de Acceso en las interfases** para tener un primer filtro de tráfico en base a direcciones IP origen, direcciones IP destino, puertos origen y puertos destino. Esto ayuda también a mitigar ataques de impostación de IPs (IP *Spoofing*).

☑ **Restringir el Acceso a los ruteadores para Administración:** Esto se puede hacer de las siguientes maneras:

- Restringiendo los protocolos usados para conectarse al ruteador con propósitos de administración.
- Usar políticas o listas de control de acceso para restringir qué direcciones IP pueden conectarse al ruteador.
- Solicitar contraseña para entrar, es decir, para iniciar una sesión.
- Asegurarse que las sesiones terminen después de un tiempo determinado de no estar siendo usadas.
- Considerar el uso de SSH (*Secure Shell*) o HTTPS (*Secure Hypertext Transfer Protocol*) en lugar de Telnet.

☑ **Asegurar el acceso SNMP en los ruteadores:** Esto puede ser logrado de la siguiente manera:

- Usar la versión 2 de SNMP como mínimo.
- Escoger los nombres de las cadenas de comunidad (*Community String*) con el mismo cuidado que con las contraseñas.
- Exigir autenticación.
- Restringir las direcciones IP que pueden conectarse al puerto SNMP en el ruteador.

- ☑ **Usar TACACS+ para controlar el acceso al ruteador:** Usar un sistema de autenticación, autorización y contabilidad (AAA: authentication, authorization, and accounting) permite la recolección de información acerca de accesos y salidas de usuarios, accesos HTTP, cambios de privilegios, comandos ejecutados y eventos similares. Las entradas de los registros AAA son enviados a servidores de autenticación usando el protocolo TACACS+ o Radius, y son grabadas por dichos servidores, típicamente en archivos de disco. Las contraseñas TACACS+ son transmitidas cifradas por lo que la amenaza del monitoreo de transmisiones (*Sniffing*) para capturar contraseñas es mitigada.

- ☑ **Desactivar Servicios que no se necesiten:** Esto incluye el servicio *finger* y pequeños servicios TCP y UDP tales como *chargen*, *discard* y *echo*. Si el protocolo NTP (*Network Time Protocol*) no es usado, considere deshabilitarlo. Si el equipo tiene activados protocolos propietarios, tales como CDP (*Cisco Discovery Protocol*) de Cisco, que no son vitales o necesarios para el funcionamiento o administración de la red, es recomendable desactivarlos.

- ☑ **Para los Protocolos de Encaminamiento o "Ruteo", considerar el uso de algún método de autenticación para asegurarse que las actualizaciones de "ruteo" (*routing updates*) sean válidas:** Usar autenticación *Message Digest (MD)* en lugar de autenticación con contraseñas en texto llano.

7.2. LOS SWITCHES SON OBJETIVOS

En principio, cabe mencionar que en un diseño de red LAN jerárquico se tienen las siguientes capas:

- **Capa de *Core* (Núcleo):** Es el *backbone* (o punto medular) de conmutación de alta velocidad, diseñado para conmutar paquetes tan rápido como sea posible entre dispositivos de la capa de distribución. Por esto se recomienda no realizar en esta capa, tareas de manipulación de paquetes, tales como filtrado. Actualmente es común que la Capa de *Core* sea un entorno de capa 3 puro, es decir, que tanto VLANs (LANs virtuales) como troncales con VLANs no estén presentes, siendo éstas finalizadas en la capa de distribución.

- **Capa de Distribución:** Separa las capas de *Core* y de Acceso. En esta capa se realiza la manipulación de paquetes. Sus funciones incluyen: filtrado, agregación de direcciones o áreas, definición de dominios de *broadcast/multicast*, encaminamiento Inter-VLAN, redistribución de rutas, encaminamiento basado en políticas, e implementación de seguridad.

- **Capa de Acceso:** El punto donde los usuarios finales se conectan a la red. Sus funciones incluyen: segmentación granular, filtrado a nivel de direcciones MAC (*Media Access Control*), y repartición o conmutación del ancho de banda.

La manera como estas capas son implementadas (si en equipos separados o no) depende de las necesidades de la organización. Sin embargo, para un funcionamiento óptimo y para propósitos de escalabilidad se debe mantener la jerarquía.

Al igual que sus contrapartes, los ruteadores, los switches están siendo cada vez más atacados. Estos ataques apuntan tanto a switches capa 2 como capa 3 y 4, y muchos de ellos son exclusivos de las funciones que realizan los switches dentro de una red. Dichos ataques incluyen el *VLAN hopping*, mediante el cual un atacante en una VLAN obtiene acceso a un host en otra VLAN a la cual normalmente no tendría acceso desde su VLAN; y otro tipo de ataque conocido como impostación de direcciones MAC (*MAC Address Spoofing*).

Las recomendaciones hechas para los ruteadores, se puede aplicar a los switches, así como las siguientes recomendaciones específicas para switches:

- ☑ **En los puertos troncales, usar un Identificador de VLAN dedicado (nativo), distinto del identificador empleado para puertos de usuario:** Esto previene los ataques del tipo *VLAN-hopping*

- ☑ **Evitar el uso de la VLAN por Defecto tanto para la operación como para la administración.** Cualquier puerto que no sea asignado a una VLAN determinada pertenece a la VLAN por Defecto. Por su característica, por defecto omnipresente

en una red de switches no configurada adecuadamente, el uso de esta VLAN no se recomienda. Pero si se usa, hay que filtrarla de los puertos troncales hacia otros switches donde no sea usada.

☑ **Configurar todos los puertos de usuario como no troncales.** Previene ataques del tipo *VLAN-hopping*, entre otros.

☑ **Establecer un número limitado de direcciones MAC (dos o tres) para puertos de usuario.** Esta implementación mitiga, entre otros, los ataques de inundación de MACs y la consecuente saturación de las tablas de conmutación de los switches. Un switch cuya tabla de conmutación ha sido saturada se comporta como un Hub, es decir que cuando reciba una trama la copiará en todos los demás puertos. Un atacante puede aprovechar esto para capturar tráfico de todo el segmento de red.

☑ **Habilitar la mitigación de ataques del protocolo *Spanning-Tree Protocol*:** Esto se logra configurando de manera perenne a un determinado switch como principal (*Root Bridge*); evitando la recepción de BPDUs (*Bridge Protocol Data Unit*) y específicamente la recepción de paquetes de cambio de topología (*Configuration/Topology Change BPDUs*) que podrían hacer que un atacante fuerce un recálculo en el algoritmo *Spanning-Tree* y se haga pasar como *Root brigde*, ejecutando así un ataque del tipo hombre en el medio al derivar todo el tráfico hacia él.

- ☑ **Deshabilitar todos los puertos no usados y ponerlos en una VLAN que no esté siendo utilizada:** Esto previene que intrusos se conecten a puertos no utilizados y se comuniquen con otros dispositivos de la red.

- ☑ **Usar autenticación de puertos en capa dos como por ejemplo 802.1X:** Este protocolo proporciona un esquema de autenticación para los usuarios que intenten conectarse a la red.

- ☑ **Usar protocolos de administración propietarios sólo cuando sea necesario:** Como ejemplo tenemos el protocolo CDP (*Cisco Discovery Protocol*) el cual ayuda en la administración de dispositivos Cisco. Sin embargo la información disponible en CDP puede proporcionarle al atacante información clave. Es recomendable limitar el uso de CDP a áreas de la red que sean consideradas suficientemente seguras.

- ☑ **En el caso de redes LAN implementadas con switches marca Cisco, usar contraseñas para el protocolo VTP:** El protocolo VTP (*VLAN Trunking Protocol*) es usado para propagar información de configuración de VLANs de un switch servidor a switches clientes. Usar autenticación en los anuncios VTP reduce la probabilidad de que estos anuncios sean impostados por un atacante.

- ☑ **Bloquear tráfico entre determinados puertos de una misma VLAN (VLANs Privadas)**: Algunas marcas de switches permiten, dentro de una VLAN determinada, configurar a ciertos puertos como protegidos o aislados, los que no podrán enviar tráfico directamente a otros puertos configurados de la misma manera. Para que este envío se realice, todo el tráfico de dichos puertos deberá pasar antes por un dispositivo de Capa 3. El envío de tráfico entre estos puertos especialmente configurados y otros no configurados de esta manera, llamados no protegidos o promiscuos, deberá proceder de manera normal. Los puertos no protegidos o promiscuos podrán comunicarse con cualquier puerto de la VLAN privada. Adicionalmente, se da la posibilidad de crear comunidades, formadas por puertos aislados que podrán comunicarse entre sí y con puertos promiscuos, mas no con puertos aislados pertenecientes a otras comunidades.

7.3. LOS HOSTS SON OBJETIVOS

Los hosts son los elementos más frecuentemente atacados en una red. Ellos representan los objetivos más visibles para un atacante y el mayor problema de seguridad para un administrador debido a que consisten en una combinación de distintas plataformas de hardware, sistemas operativos y aplicaciones, cada una con sus propias actualizaciones y parches.

Los atacantes ven a los hosts como los objetivos más valiosos debido a las aplicaciones que corren, a la información que es almacenada en ellos, y el hecho que pueden ser usados para atacar a otros destinos. Los hosts representan el elemento más exitosamente atacado en una red.

Por ejemplo, considere un servidor Web típico de una red corporativa. La aplicación servidor Web puede ser de un proveedor, el sistema operativo de otro, y el hardware de un tercero. Adicionalmente el servidor Web podría estar corriendo ciertos programas CGI disponibles gratuitamente o una aplicación comercial que haga interfaz con él, como por ejemplo, una base de datos SQL. Toda esta variedad de componentes en el host puede contener múltiples vulnerabilidades, algunas más severas que otras. Esto no quiere decir, que usar un sistema operativo y aplicaciones de un mismo fabricante sea más seguro; en algunos casos es todo lo contrario. Lo que hay que tener en cuenta es que mientras más complejo sea un sistema, mayor la probabilidad de falla.

Cuando se aplique seguridad a los hosts, se debe prestar atención a los sistemas que los componen; probar las actualizaciones y parches en sistemas de prueba antes de aplicarlos en un entorno en producción. Los parches pueden crear conflictos inesperados entre los componentes en software y dar como resultado una denegación de servicios al evitar que una aplicación o sistema funcione adecuadamente.

Adicionalmente, se recomienda desactivar los servicios no necesarios, es decir, aquellos que no se requieren para el adecuando funcionamiento y administración del sistema. Algunos sistemas vienen con servicios activados por defecto que pueden representar un objetivo potencial para atacar. Por ejemplo, si un host no es servidor FTP entonces deshabilitar el servicio FTP y si es posible remover el paquete FTP.

Otras posibles vías de ataque son el uso de cuentas por defecto y contraseñas fáciles de adivinar. Las cuentas privilegiadas en los sistemas de producción deben estar limitadas a aquellos usuarios que necesiten acceder al sistema para propósitos de administración o mantenimiento del software.

La clave para mejorar exitosamente la seguridad de un sistema es reducir al mínimo el número de posibles vías de ataque. Adicionalmente, se debe considerar el uso de software de detección/prevención de intrusos basados en hosts (Host IDS/IPS), al menos en sistemas críticos, para mejorar aún más la postura de seguridad del sistema.

Mejorar la seguridad global en un sistema no significa necesariamente que el sistema será impenetrable, pero sin duda lo hará más difícil de vulnerar.

7.4. LAS APLICACIONES SON OBJETIVOS

Al igual que los sistemas operativos de los hosts, las aplicaciones son susceptibles a errores de codificación. La magnitud del daño causado por errores de codificación puede variar desde un error menor del tipo "*HTTP 404 - File Not Found*" a algo considerablemente peor como un desborde de buffer que provee acceso interactivo directo a un host. Las aplicaciones deben mantenerse constantemente al día. Más aún, las aplicaciones de dominio público y aquellas desarrolladas a medida deben ser auditadas para asegurar que no se introduzcan vulnerabilidades potenciales al sistema con la instalación del software. Estas auditorías deben considerar los siguientes factores:

- Análisis de llamadas que la aplicación hace a otras aplicaciones y al S.O.
- Nivel de privilegios de la aplicación.
- Nivel de confianza que la aplicación tiene respecto a los sistemas que la rodean.
- Método de transporte que la aplicación usa para pasar datos a través de la red.

Este nivel de auditoría es necesario para resolver posibles vulnerabilidades que afectarían la postura de seguridad del sistema y de la red en su conjunto.

Se recomienda mantener actualizadas las aplicaciones y el sistema operativo con los últimos parches y actualizaciones de seguridad. Asimismo, el empleo de Host IDS/IPSs permitiría bloquear el uso de las aplicaciones vulnerables, para realizar acciones maliciosas.

7.5. LAS REDES SON OBJETIVOS

Defenderse de ataques a redes es quizás la tarea más difícil, ya que típicamente en estos ataques se toma ventaja de una propiedad intrínseca de la red. Esta categoría de ataques incluye los ataques a nivel de la Capa 2, ataques de Denegación Distribuida de Servicios (DDoS) y con *Sniffers* de Red.

Los ataques a nivel de la Capa 2 pueden ser mitigados aplicando las recomendaciones mencionadas anteriormente en las secciones "Los Switches son Objetivos" y "Los Ruteadores son Objetivos".

El impacto de las acciones de *sniffing* puede ser mitigado a través de la implementación de una red con switches y la aplicación de las recomendaciones ya mencionadas.

Protegerse de ataques DDoS es mucho más difícil pues, típicamente, su objetivo es el de deshabilitar una red por completo y no solo un host. El principal método para lograrlo es consumir todo el ancho de banda disponible en la red tanto de entrada como de salida. Un efecto colateral de un ataque DDoS puede ser que un sistema atacado colapse.

La cooperación entre el cliente final y su proveedor de acceso a Internet (ISP: *Internet Service Provider*) es la única manera efectiva de mitigar muchos de los efectos de un ataque DDoS. El ISP puede limitar la tasa de tráfico en la interfaz del ruteador que da

cara al enlace del usuario, cada vez que exceda una cierta cantidad predeterminada del ancho de banda total del enlace.

Dentro de las formas más comunes de ataques DDoS se encuentran los de inundación de paquetes ICMP, inundación con SYNs TCP, e inundación UDP.

Un mecanismo de defensa que se puede idear para proteger sus sistemas es seguir las recomendaciones de filtrado tal como está especificado en los RFCs 1918 y 2827.

El RFC 1918 especifica los rangos de direcciones IP que son reservados para uso privado, es decir que no deberían venir desde Internet. Los rangos privados definidos son:

- Clase A: 10.0.0.0 - 10.255.255.255
- Clase B: 172.16.0.0 - 172.31.255.255
- Clase C: 192.168.0.0 - 192.168.255.255

El RFC 2827 define el filtrado de entrada hacia la red del proveedor de acceso (filtrado de salida desde el punto de vista del cliente), previniendo que desde el cliente llegue tráfico con direcciones que no estén dentro de los rangos asignados a dicho cliente.

Cuando se implementa en el enlace WAN del lado del ISP, el filtrado ayuda a prevenir que paquetes con direcciones origen dentro de los rangos especificados por el RFC 1918

así como otro tráfico impostado, llegue al enlace del cliente. En el lado del cliente, el seguir las recomendaciones de filtrado según estos RFCs, ayuda a prevenir que los atacantes lancen ataques DDoS usando direcciones IP impostadas bloqueándolos en el ruteador de borde del cliente. A pesar de que esta estrategia no previene que los ataques DDoS ocurran, sí previene que el atacante imposte la dirección origen de los hosts atacantes.

7.6. LAS REDES DE VOZ SON OBJETIVOS

Con el advenimiento de la Telefonía IP y su rápido despliegue, se despiertan nuevas preocupaciones en torno a la seguridad de las comunicaciones de voz.

Entran en escena las nuevas centrales telefónicas IP, conocidas también como *Call-processing Managers* (Procesadores de Llamadas) o simplemente *Call Managers*. Asimismo, aparecen los teléfonos IP en hardware y software; estos últimos llamados *SoftPhones* o teléfonos IP basados en PC.

En la actualidad, no existe un estándar ampliamente adoptado o desplegado para el control de llamadas en Telefonía IP, ni para la provisión de características y funciones en los teléfonos IP. Los fabricantes emplean protocolos de control propietarios, lo cual introduce una variable adicional cuando se habla de implementar recomendaciones de seguridad.

Las redes de voz son un objetivo atractivo para un atacante, sea que desee jugar una broma impostando a alguien, tener acceso a mensajes de voz o capturar conversaciones confidenciales.

El mayor problema con las redes de voz es que generalmente son abiertas, es decir, se requiere poca o ninguna autenticación para obtener acceso a ellas. Esto debido a que el modelo de diseño para redes de telefonía IP se basó en sistemas de voz tradicionales.

A continuación se proponen una serie de recomendaciones para mejorar la seguridad en estas redes:

- ☑ Por cuestiones de calidad de servicio, escalabilidad, manejo y seguridad, el despliegue de dispositivos de telefonía IP y dispositivos de datos IP debe darse en dos segmentos de red separados lógicamente. Esto ayuda a mitigar ataques con herramientas que capturan la información de voz y la reensamblan en archivos de audio. La segmentación permite, además, usar la misma infraestructura, léase switches, de acceso, distribución y core. Tecnologías tales como LANs virtuales (VLANs), control de acceso y firewalls de inspección de estados proporcionan la segmentación en capa 3 necesaria para mantener los segmentos de voz y datos separados.

- ☑ Sin embargo, si un atacante lograra conectar una estación de trabajo al segmento de voz, podría usar una herramienta tal como *dsniff* para hacer que el switch se comporte como un hub, y así monitorear llamadas. Otro tipo de ataque consistiría en conectar en el segmento de voz un teléfono IP con una dirección MAC (*Media Access Control*) impostada, asumir la identidad del teléfono llamado e interceptar llamadas.

- ☑ Si a manera de simplificar el cableado, las estaciones de trabajo se van a conectar a los switches a través de los teléfonos IP, se recomienda emplear teléfonos IP con tecnologías avanzadas en Capa 2 tales como 802.1q que permitan implementar VLANs distintas para separar el tráfico de voz del de datos; y no solamente proporcionar simple conectividad en capa 2. Adicionalmente, se debe contar con control de acceso en capa 3, esto en la capa de distribución.

- ☑ No se recomienda el uso de teléfonos IP basados en PC, a menos que se tenga un firewall de inspección de estados como intermediario en la interacción de los segmentos de datos y voz. Por su naturaleza los teléfonos IP basados en PC residen en el segmento de datos y requieren acceso al segmento de voz para hacer llamadas, para que se realice el control de las mismas, y para dejar mensajes de voz. Las llamadas entre dispositivos IP generalmente usan puertos UDP dinámicamente asignados. Sin un firewall de inspección de estados, llevar el control de estos puertos no sería factible, y restaría permitir acceso a un gran rango de puertos UDP,

lo cual los haría más vulnerables a, por ejemplo, ataques DoS de inundación de paquetes UDP. Los teléfonos IP basados en PC son más susceptibles a ataques, puesto que no escapan de las vulnerabilidades de los sistemas operativos, de las aplicaciones, de los servicios, de virus, gusanos, etc. Los teléfonos IP en hardware por su parte, corren un sistema operativo especialmente diseñado y menos sujeto a vulnerabilidades.

☑ Se recomienda el uso de un firewall de inspección de estados en ubicaciones de la red donde se permite la interacción entre los segmentos de voz y datos. Un firewall de inspección de estados proporcionará protección contra ataques de Denegación de Servicios que busquen agotar los recursos alojados para conexiones, protección contra ataques de fragmentación de paquetes, mitigación de ataques de impostación de direcciones, habilitación de acceso dinámico granular por puerto (TCP y/o UDP), y filtrado en general. Hay múltiples flujos legítimos entre los segmentos de datos y voz que deben ser permitidos, como por ejemplo, si el Servidor de Mensajes de Voz y el *Call Manager* o Central Telefónica IP se encuentran en el segmento de datos. También, en el caso que desde los teléfonos IP se quiera navegar en Internet, se tendrá que pasar por un Servidor *Proxy* el cual accederá a Internet a través del segmento de datos. Por otro lado, los teléfonos IP basados en PC que estén en el segmento de datos, tendrán que acceder al segmento de voz si allí se encuentran el servidor de Mensajes de Voz y la Central IP.

- ☑ Se recomienda asignar direcciones IP privadas a los dispositivos telefónicos IP, según lo establecido en el RFC 1918, para reducir la probabilidad de que el tráfico de voz salga de la red. Un atacante desde Internet no podrá escanear el segmento de voz en busca de vulnerabilidades a menos que haya una mala configuración en la traducción de direcciones IP de privadas a públicas o NAT (*Network Address Translation*). Ésto sólo se debe dar de manera controlada en el servidor *Proxy* que permite navegación en Internet desde los teléfonos IP. Los dispositivos Capa 3 de la red mitigarán la impostación de direcciones IP en el segmento de voz mediante la aplicación de las recomendaciones del RFC 2827.

- ☑ Establecer mecanismos de autenticación para los teléfonos IP, empezando por la autenticación por direcciones MAC. De esta manera, y asumiendo que el proceso de registro automático haya sido deshabilitado, un teléfono con una dirección MAC no registrada no podrá obtener la configuración de la red y por lo tanto no podrá hacer ni recibir llamadas. Esta es una primera línea de defensa, que sin embargo no brindaría protección en un escenario en el que un atacante logre impostar una dirección MAC válida perteneciente a un teléfono IP. Algunos teléfonos IP permiten un nivel de autenticación básico, solicitando al usuario que ingrese su nombre de usuario y contraseña. Otros soportan características tales como solicitar un código para permitir realizar llamadas de larga distancia. El problema es que típicamente estas claves son fijas y se envían por la red sin cifrar, por lo que pueden ser capturadas. En otros casos, se solicita nombre de usuario, contraseña y un PIN o

Número de Identificación Personal. Lo ideal es que alguno de estos valores sea variable. Esquemas de autenticación similares se pueden usar para acceder a los sistemas de mensajería de voz. Ahora, a pesar de todo esto, si el usuario se autentica exitosamente y luego deja su teléfono sin supervisión sin haber salido del sistema, todas las medidas de seguridad no habrán servido.

- ☑ Se recomienda deshabilitar los puertos de los switches que no estén siendo usados, para evitar la inserción de dispositivos espías en la red.

- ☑ La asignación de direcciones IP para teléfonos IP es típicamente realizada mediante DHCP (*Dynamic Host Configuration Protocol* o Protocolo de Configuración de Host Dinámica). Es recomendable tener servidores DHCP separados para los segmentos de voz y datos. Se debe considerar la posibilidad de asignar estáticamente direcciones IP a direcciones MAC conocidas. Esto mitigará ataques DoS de agotamiento de direcciones IP.

- ☑ Implementar la funcionalidad de firewall con inspección de estados entre los segmentos de voz y datos puede ser difícil para muchas empresas. Sin embargo, los NIDSs son actualmente soportados por los switches. A pesar de que los NIDSs no incluyen firmas de ataques relacionadas con el protocolo de control de voz, si incluyen firmas para ataques DoS UDP y explotación de vulnerabilidades en HTTP las cuales se aplican a ambientes de voz.

- ☑ Se deben tomar muchas precauciones con los sistemas donde residan los servicios de correo de voz y procesamiento de llamadas (Central Telefónica IP). Éstas incluyen: deshabilitar todos los servicios y aplicaciones que no sean necesarios, parchar y mantener actualizado el sistema operativo y los servicios, deshabilitar funciones de voz no usadas, e instalar un Host IDS.

7.7. LAS REDES WIRELESS O INALÁMBRICAS SON OBJETIVOS

Hoy en día, las redes wireless o inalámbricas se han convertido en uno de los más interesantes objetivos para los atacantes. Las organizaciones están implementando tecnologías wireless a una tasa rápida, usualmente sin considerar todos los aspectos de seguridad. Muchas veces, para facilitar su implementación, los dispositivos wireless tienen deshabilitadas por defecto las características de seguridad. Los *hackers* han visto en esto no solo la oportunidad de obtener accesos gratuitos a Internet o de ocultar su identidad, sino también de penetrar en redes a las que, de otra manera, les hubiera sido difícil acceder desde Internet. A diferencia de una red cableada, una *Wireless* LAN (WLAN) envía la información usando como medio el aire y puede ser accesible desde fuera de los límites físicos de la organización. Cuando la información de la red wireless no es cifrada, los paquetes pueden ser vistos por cualquiera que esté dentro del rango de frecuencia y alcance. Por ejemplo, un atacante con una laptop, sistema operativo Linux, un adaptador wireless y un programa como TCPDUMP puede recibir, ver y almacenar todos los paquetes que circulan por una Wireless LAN determinada.

En la actualidad, los estándares de la IEEE para redes wireless son los siguientes:

- **802.11:** Con una velocidad de transmisión de 1 o 2 Mbps, trabaja en la banda de 2.4GHz y puede utilizar los esquemas de modulación FHSS (*Frequency-Hopping Spread Spectrum*), y DSSS (*Direct-Sequence Spread Spectrum*).
- **802.11a:** Velocidad de transmisión de hasta 54 Mbps. Trabaja en la banda de 5 GHz y usa modulación OFDM (*Orthogonal Frequency-Division Multiplexing*).
- **802.11b:** Velocidad de transmisión de 11 Mbps. Trabaja en la banda de 2.4 GHz y usa modulación DSSS. Fue aceptado en el año 1999, y es el estándar más difundido.
- **802.11g:** Velocidad de transmisión de hasta 54 Mbps. Trabaja en la banda de 2.4 Ghz y usa modulación OFDM. Permite compatibilidad hacia atrás con el estándar 802.11b.

7.7.1. DEBILIDADES DE LOS ESTÁNDARES 802.11 a/b/g

A continuación se mencionan algunas de las debilidades más resaltantes de los actuales estándares para redes wireless:

- **Interferencia o *Jamming*:** Resulta fácil introducir interferencia en las comunicaciones wireless, incluso haciéndolas imposibles. Basta con bombardear a un punto de acceso wireless (*Wireless Access Point*) con solicitudes de acceso, sean éstas exitosas o no. Por otro lado, otros servicios

wireless en el mismo rango de frecuencia que la WLAN pueden reducir el ancho de banda disponible.

- **Autenticación MAC:** Los puntos de acceso (AP) wireless pueden identificar cada tarjeta wireless por su dirección MAC (*Media Access Control* o Control de Acceso al Medio) la que se encuentra grabada internamente. Algunas implementaciones requieren que las MACs de las tarjetas estén registradas en los APs antes de que el servicio wireless pueda ser usado. Este escenario puede resultar complejo puesto que cada AP en la red necesitaría tener acceso a esta lista. Aún si esto fuera factible, no es una medida de seguridad suficiente si se tiene en cuenta que existen maneras de cambiar las direcciones MAC incorporadas en las tarjetas Wireless, por direcciones MAC aleatorias o impostadas deliberadamente.

- **Modo Ad Hoc versus Modo Infraestructura:** Muchas WLANs operan usando el Modo Infraestructura. En este modo, los clientes wireless se conectan contra un punto de acceso (AP) para todas sus comunicaciones. Sin embargo, se pueden implementar WLANs de tal manera que se formen redes punto-a-punto independientes. En una implementación de este tipo, conocida como WLAN Ad Hoc, los hosts equipados con adaptadores de red wireless, con la misma configuración y que estén dentro del mismo rango, pueden

compartir archivos directamente, sin pasar por un AP. Esto representa un riesgo de seguridad.

- **Denegación o Degradación de Servicios:** Los mensajes de administración de los estándares 802.11 a/b/g (los usados para redes LAN wireless), incluyendo el *beacon* (aviso intermitente), el detector de solicitud o respuesta, las asociaciones y reasociaciones de solicitud y respuesta, la disociación, y la "desautenticación" no son autenticados. Por lo tanto, una WLAN puede ser objeto de ataques de Denegación de Servicios (DoS) mediante el empleo de herramientas tales como WLAN-Jack.

- **Punto de Acceso "*Rogue*" o Fraudulento:** Es aquel accesible por los usuarios wireless de la organización pero que no es reconocido como elemento autorizado o confiable de la red. Muchos de estos dispositivos son instalados por usuarios que buscan tener acceso wireless, siendo conectados en algún puerto de switch disponible, usualmente sin habilitar medidas de seguridad. Otro tipo de AP "*rogue*" es aquel que se hace pasar por un AP confiable y engaña a los usuarios wireless quienes se asocian a él, permitiendo que el atacante manipule las tramas wireless mientras atraviesan el AP. Esto se puede prevenir o minimizar mediante políticas corporativas, seguridad física, y habilitando seguridad basada en puertos en los switches de borde a través del uso de autenticación 802.1X. La detección puede ser

realizada usando *scripts*, analizadores o *sniffers* wireless, y realizando revisiones físicas periódicas de la infraestructura wireless instalada.

- **Difusión o no difusión del SSID (*Service Set Identifier*) o Identificador de Servicios:** En una red abierta, el SSID se difunde periódicamente. En cambio, en una red cerrada, los APs no hacen difusión (*broadcast*) del SSID con cada transmisión de la señal intermitente o *beacon*, con la intención de que sólo aquellos que conozcan el SSID puedan asociarse al AP y acceder a la red. Para el usuario común tratando de conectarse de manera wireless, parecería que no hubiera un AP funcionando en el área. Sin embargo, existen tramas de administración que se intercambian entre APs y dispositivos wireless que transmiten el SSID en texto llano. Estas tramas podrían ser capturadas por un atacante, haciendo la no difusión del SSID irrelevante.

7.7.2. WEP (*Wired Equivalent Privacy*):

La seguridad tradicional usada por los estándares 802.11 a/b/g para redes LAN wireless, incluye los métodos de autenticación abierta o autenticación mediante llave compartida (PSK: *Pre-Shared Key*) que se combinan con WEP (*Wired Equivalent Privacy*) o privacidad equivalente a la de una red cableada. Estas combinaciones ofrecen un nivel de privacidad y control de acceso muy rudimentario, pues pueden ser vulneradas.

La autenticación abierta implica poco más que proporcionar el SSID (*Service Set Identifier*) o Identificador de Servicios correcto, pues en este esquema cualquier cliente wireless puede asociarse con el AP. El uso de WEP con Autenticación Abierta previene que el cliente envíe y reciba información hacia y desde el AP, a menos que tenga la llave WEP correcta.

Con autenticación de llave compartida, el cliente envía al AP una solicitud de asociación. El AP responde enviando un paquete desafío al cliente, el cual el cliente debe cifrar con la llave WEP correcta y enviar de regreso al AP. Si el cliente tiene la llave incorrecta o ninguna llave, la autenticación fallará y el cliente no podrá asociarse al AP. La autenticación de llave compartida no se considera segura ya que un atacante que capture tanto el mensaje de desafío (que está en texto llano) y el mismo desafío cifrado con una llave WEP, puede descifrar la llave WEP. Más aún, ya que la misma llave es usada tanto para la autenticación de llave compartida, como para cifrar el tráfico entre el AP y los clientes, dicho tráfico podría ser descifrado por un atacante una vez que se haya comprometido la autenticación de llave compartida. Irónicamente, la configuración más segura se obtiene usando "Autenticación Abierta", permitiendo que cualquiera se asocie con el AP, y basándose en otros métodos para manejar la seguridad.

WEP usa un algoritmo de cifrado desarrollado por Ron Rivest de RSA, llamado RC4, el cual es un cifrador de flujos. Este trabaja generando un flujo conocido como *keystream*, a partir de una llave corta, el cual es combinado con el texto llano mediante una operación XOR para generar el texto cifrado. El receptor debe tener una copia de la misma llave con la que genera el mismo *keystream*, realiza la operación de XOR con el texto cifrado y obtiene el texto llano original.

Para asegurarse que un paquete no haya sido modificado en tránsito, WEP usa un campo de chequeo de integridad en el paquete, implementado usando el *checksum* CRC-32, que va como parte del texto cifrado. Sin embargo CRC-32 es lineal, lo cual significa que un atacante podría intercambiar bits arbitrariamente en un mensaje cifrado y ajustar adecuadamente el *checksum* para que el mensaje pareciera válido.

Una llave estática WEP está compuesta de 64, 128 o hasta 256 bits, la cual debe ser definida, y luego ingresada en todos los dispositivos WLAN, es decir, en cada uno de los APs y tarjetas wireless de los usuarios. Esta es una tarea que consume tiempo. Si uno de los dispositivos que usa llaves WEP estáticas se pierde o es robado, el poseedor del dispositivo podría acceder a la WLAN, sin ser detectado como usuario no autorizado hasta y a menos que la pérdida o robo sea reportado. El administrador de red tendría entonces que cambiar la llave WEP en cada dispositivo wireless que estuviere usando la misma llave. En

organizaciones grandes, con cientos o miles de usuarios wireless, esto puede ser una tarea agobiante y desalentadora.

Para ser más precisos, la porción de llave secreta que está bajo el control del administrador tiene en realidad una longitud de 64, 128 o 256 bits menos 24 bits. Estos 24 bits, que no están bajo control del administrador. Son usados como Vector de Inicialización (IV) para aumentar el tamaño de la llave y producir una llave RC4 distinta para cada paquete. El problema es que el IV se envía en el paquete en texto llano. Además 24 bits no son suficientes para evitar una rotación del IV suficientemente espaciada. Por ejemplo, un AP ocupado, que constantemente envíe paquetes de 1500 bytes (MTU o unidad máxima de transferencia por defecto) a 11Mbps, agotaría el espacio de IVs no repetidos después de $1500\times 8/(11\times 10^6)\times 2^{24} \sim 18000$ segundos o aproximadamente 5 horas (El tiempo podría ser menor ya que muchos paquetes podrían ser menores que el MTU). Esto permitiría a un atacante capturar dos mensajes cifrados con el mismo *keystream* y realizar ataques estadísticos para recuperar el texto original, e incluso la llave. Más aún, cuando la misma llave es usada por todos los dispositivos wireless, hay más posibilidades de una "colisión" IV. Incluso existen ciertas marcas de tarjetas wireless que cada vez que son inicializadas ponen el IV en 0 y lo incrementan en uno con cada paquete. Dos o más tarjetas de estas activadas casi al mismo tiempo ocasionarían una abundancia de

colisiones IV. Sin embargo, lo peor de todo es que el estándar 802.11 especifica el cambio del IV con cada paquete como opcional.

En resumen, WEP puede ser vulnerado en todas sus variantes (64,128 o 256 bits) usando herramientas disponibles en Internet, tales como AirSnort o WEPCrack. Actualmente, se estima que en una red muy activa, las llaves WEP de 128 bits (la variante más usada) pueden ser obtenidas en tan solo 15 minutos.

Todos estos problemas de seguridad hicieron ver que era necesario adicionar elementos de seguridad o extensiones a las redes wireless. Estas extensiones usan IPSec y 802.1X/EAP.

7.7.3. EXTENSIÓN IPSEC EN REDES WIRELESS

Como se explicará con más detalle en el capítulo 9, IPSec (*Internet Protocol Security*) es una infraestructura de estándares abiertos para proporcionar comunicaciones seguras y privadas sobre redes IP.

Cuando se implementa IPSec en redes wireless, se instala un software cliente IPSec en cada dispositivo cliente wireless. El usuario a través de este cliente IPSec establecerá un túnel para enviar su información a la red. Por otro lado, se colocan filtros para permitir sólo el tráfico wireless dirigido al concentrador VPN, el servidor DHCP (*Dynamic Host Configuration Protocol*) y al servidor

DNS (*Domain Name System*). IPSec proporciona confidencialidad del tráfico IP (a través de protocolos de cifrado como DES, 3DES o AES), además de autenticación y servicios *antireplay*.

7.7.4. EXTENSIÓN 802.1X/EAP EN REDES WIRELESS

El uso del estándar IEEE 802.1X ofrece un marco efectivo para autenticar y controlar el uso del tráfico por parte de los usuarios de una red, así como variar dinámicamente las llaves de cifrado. 802.1X emplea el protocolo EAP (*Protocolo de Autenticación Extensible*) para redes cableadas y no cableadas, conocido como EAPoL (*EAP over LANs*), el cual soporta múltiples métodos de autenticación, tales como tarjetas o dispositivos *token*, Kerberos, contraseñas válidas sólo una vez (OTPs), certificados y autenticación de llave pública.

802.1X define tres roles:

- **Suplicante:** Usuario o Cliente que solicita la autenticación.
- **Servidor de Autenticación:** Servidor que proporciona la autenticación.
- **Autenticador:** El dispositivo al cual el Suplicante le solicita acceso, y el cual pasa la solicitud de acceso hacia el Servidor de Autenticación.

Funcionamiento de 802.1X aplicado a Redes Wireless:

Las comunicaciones iniciales de 802.1X se inician cuando un Suplicante (dispositivo wireless cliente) intenta conectarse con un Autenticador (un Punto

de Acceso o AP). El AP responde habilitando un puerto para pasar sólo los paquetes EAP del cliente hacia un servidor de autenticación localizado en el lado cableado del AP. Los APs bloquean cualquier otro tráfico hasta que se pueda verificar la identidad del cliente, usando un servidor de autenticación como RADIUS. Una vez autenticado, el AP abre más puertos para que el cliente pase otro tipo de tráfico.

Las siguientes interacciones ocurren cuando se emplea 802.1X:

1. El Suplicante (cliente wireless) envía un mensaje EAP de inicio.
2. El Autenticador (AP) responde con un mensaje EAP de solicitud de identidad.
3. El Suplicante envía un paquete EAP de respuesta, que contiene su identidad, para ser enviado al Servidor de Autenticación.
4. El Servidor de Autenticación emplea un algoritmo de autenticación específico para verificar la identidad del Suplicante. Esto mediante el uso de certificados digitales u otro tipo de autenticación EAP.
5. El Servidor de Autenticación enviará al Suplicante un mensaje de aceptación o uno de rechazo.
6. El Autenticador (AP) envía un paquete EAP de aceptación o rechazo al Suplicante.
7. Si el Servidor de Autenticación aceptó al Suplicante, el Autenticador (AP) permitirá que el Suplicante pase tráfico hacia la red.

Un ejemplo de este proceso se muestra en la figura 7.1.

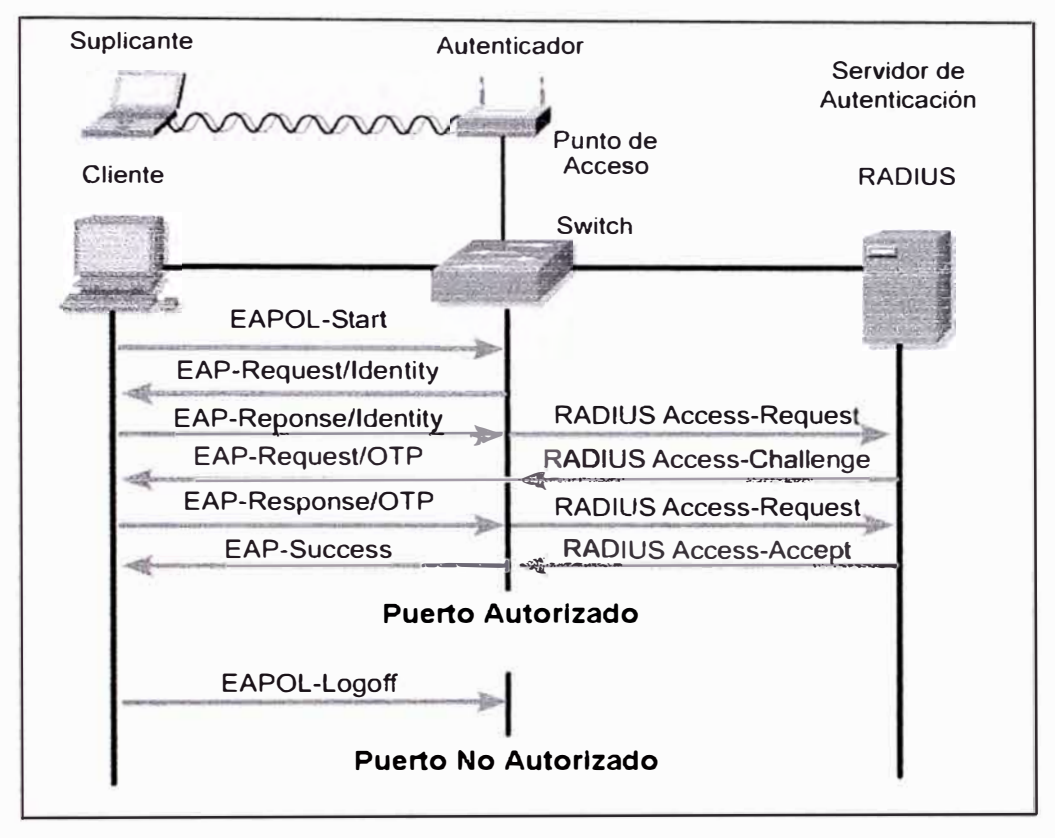

FIGURA 7.1 - Autenticación usando 802.1X/EAPoL y RADIUS

El protocolo 802.1X básico proporciona autenticación efectiva ya sea que se implemente algún tipo de cifrado 802.11 o ninguno. Si se configura para implementar intercambio de llaves, el servidor de autenticación 802.1X puede enviar llaves de sesión al Autenticador (AP) junto con el mensaje de aceptación. El AP usará estas llaves de sesión para construir, firmar y cifrar un mensaje de llave EAP que será enviado al cliente wireless después de enviar el mensaje de

éxito. El cliente podrá entonces usar el contenido del mensaje de llave para definir las llaves de cifrado aplicables. En una implementación típica con 802.1X, el cliente puede cambiar automáticamente las llaves de cifrado tan seguido como considere necesario para minimizar la posibilidad de que un atacante tenga tiempo suficiente para descifrar la llave en uso.

802.1X no es la solución completa. Es importante hacer notar que 802.1X no proporciona los mecanismos de autenticación. Se debe escoger el tipo de EAP a usar, entre ellos EAP-TLS (*EAP – Transport Layer Security*) o EAP-TTLS (*EAP Tunneled Transport Layer Security*), el cual definirá cómo la autenticación se realizará. En la figura 7.2 se observa la arquitectura EAP.

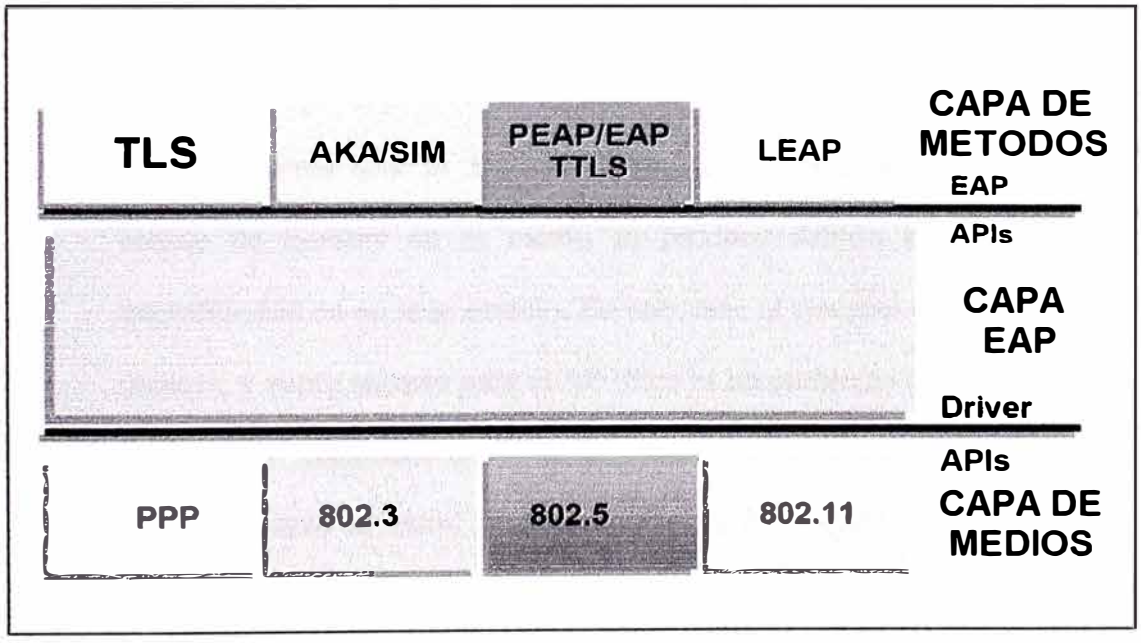

FIGURA 7.2 - Arquitectura EAP

Por otro lado, el software que soporta el tipo específico de EAP reside en el Servidor de Autenticación y en el sistema operativo o software de aplicación de los dispositivos cliente. El Autenticador (AP) actúa como dispositivo pasante de los mensajes 802.1X, lo cual significa que uno puede especificar el tipo de EAP sin realizar cambios o *upgrades* en el AP que soporte 802.1X. 802.1X es particularmente adecuado para redes LAN wireless, puesto que requiere poco procesamiento por parte del Autenticador (el punto de acceso wireless).

En el 2002, se descubrió que 802.1X era vulnerable a ataques del tipo captura de sesión (*hijacking*) y del tipo hombre en el medio. La captura de sesión se produce cuando un atacante espera que alguien se autentique exitosamente. Luego, haciéndose pasar por el AP, envía un mensaje de disociación al cliente. El cliente cree que ha sido desconectado pero el AP cree que el cliente sigue conectado. Si WEP u otro mecanismo no está presente, el atacante podrá inmediatamente usar la conexión hasta que expire la sesión. Por otro lado, el ataque de hombre en el medio se produce debido a que 802.1X realiza autenticación en un solo sentido. En este caso el atacante actúa como AP ante el usuario, y como usuario para el AP. Este es un problema en el diseño de 802.1X puesto que considera a los APs como entidades confiables, y este no es necesariamente el caso. 802.1X no es seguro cuando se usa en un medio compartido, a menos que una asociación de seguridad sea establecida. A pesar

de todo esto, y hasta que exista un protocolo más seguro es mejor usar 802.1X que no usar ningún esquema de autenticación de usuarios.

7.7.5. WPA (*Wi-Fi Protected Access*)

WPA o Acceso Protegido para Redes Wireless de Fidelidad Inalámbrica es un estándar interino de la Alianza Wi-Fi introducido en el 2003, previo al estándar 802.11i de la IEEE.

WPA tiene dos modos de operación:

- **WPA Modo Empresarial:** Requiere un servidor RADIUS para autenticación y distribución de llaves, centralizando el manejo de las credenciales de los usuarios. Para implementaciones en el hogar o pequeñas empresas esta no es una alternativa práctica.

- **WPA Modo PSK (*Pre-Shared Key*) o de llave pre-compartida:** Una llave compartida se usa para la autenticación. Es decir, las credenciales del usuario residen en los dispositivos (APs y tarjetas wireless). Este modo comparte las mismas dificultades de administración y es vulnerable a los mismos ataques que los sistemas de llave compartida, tales como ataques de diccionario.

WPA ofrece dos opciones de cifrado:

- **TKIP** (*Temporal Key Integrity Protocol*) o Protocolo de Integridad de Llave Temporal.

- **AES** (*Advanced Encryption System*) o Sistema Avanzado de Cifrado: Utiliza llaves simétricas de longitud variable para cifrado de información en bloque.

TKIP forma parte de un borrador de estándar del grupo de trabajo 802.11i de la IEEE. TKIP utiliza el cifrador de flujos RC4 con llaves de 128 bits para cifrado y llaves de 64 bits para autenticación. TKIP es una mejora con respecto a WEP pues agrega una función de mezclado de llave por cada paquete, para desasociar los vectores de inicialización (IV), que son visibles, de llaves débiles.

TKIP agrega un mecanismo dinámico de reciclado de llaves, mediante el cual comparte una llave inicial entre los dispositivos, para que luego cada dispositivo cambie la llave de cifrado para cada paquete. Además, mejora el Valor de Chequeo de Integridad (ICV) incorporando un código de integridad de mensaje (MIC: *Message Integrity Code*) para proteger tanto el encabezado como la carga útil; e implementa un contador de tramas para proteger contra ataques de tipo *playback*.

Todo esto hace a TKIP más resistente ante ataques criptográficos que involucran la reutilización de llaves. TKIP mitiga de manera significativa la vulnerabilidad de deducción de llaves que tiene WEP, pero no proporciona una solución completa a todas las debilidades.

Con WPA se puede usar autenticación mediante certificados, en la cual un servidor de una Autoridad Certificadora (CA) permitiría garantizar que los dispositivos que se conectan fueran realmente quienes dicen ser.

Ventajas de WPA:

- Agrega autenticación a WEP.
- Brinda compatibilidad hacia atrás para dispositivos que soportan WEP.
- Permite integrar servidores RADIUS para facilitar la administración, auditoría y registro.

Desventajas de WPA:

- Excepto cuando se usa WPA-PSK su instalación es complicada, y poco apropiada para hogares y negocios pequeños.
- Requiere que se realicen *upgrades* de *firmware* para algunos dispositivos. Para otros, esto no será posible por cuestiones de incompatibilidad.

- El *overhead* o información que agrega a los paquetes hace que disminuya el rendimiento. El cifrado y descifrado es más lento para dispositivos que la realizan en software y no en hardware dedicado.
- Es vulnerable a ataques de denegación de servicio.

7.7.6. 802.11i

Es un borrador de estándar de la IEEE para seguridad en redes wireless 802.11. 802.11i define una serie de nuevos estándares y se basa en otros estándares existentes.

RSN (*Robust Secure Network*)

802.11i introduce el protocolo RSN (*Robust Secure Network*) o Red Segura Robusta, para establecer comunicaciones seguras en redes wireless. RSN funciona de la siguiente manera:

1. La tarjeta wireless envía una solicitud (*Probe Request*)
2. El punto de acceso wireless (WAP) envía una respuesta (*Probe Response*) con una trama de intercambio de información (RSN *Information Element* o IE).
3. La tarjeta wireless solicita autenticación por medio de alguno de los métodos aprobados.
4. El WAP proporciona autenticación a la tarjeta wireless.

5. La tarjeta wireless envía una solicitud de asociación (*Association Request*) con una trama RSN IE.
6. El WAP envía la respuesta de la asociación (*Association Response*).

RSN hace una difusión (*broadcast*) por toda la red wireless del RSN IE (*Information Element*), el cual contiene la siguiente información:

- Todas las formas de autenticación disponibles.
- Todos los cifradores *unicast* disponibles.
- El cifrador *multicast* disponible.

802.11i también introduce los protocolos de cifrado WRAP y CCMP basados en el algoritmo de cifrado AES.

- **WRAP (*Wireless Robust Authenticated Protocol*):** WRAP o Protocolo Autenticado Robusto Inalámbrico es un protocolo de cifrado basado en el modo OCB (*Offset Codebook*) de AES. Problemas de derechos de propiedad intelectual han hecho que la IEEE introduzca CCMP en el estándar 802.11i y haga a WRAP un componente opcional de RSN.

- **CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*):** CCMP es el protocolo de cifrado preferido para el estándar 802.11i. CCMP está basado sobre el modo CCM (Contador

con CBC-MAC) del algoritmo de cifrado AES. Utiliza llaves de 128 bits, con un vector de inicialización (IV) para detección de *replay* o repetición. A diferencia de WRAP, CCMP es mandatorio en una implementación RSN. Los componentes de CCMP son:

- Componente CM (*Counter Mode* o Modo Contador) de CCMP, es el algoritmo que provee la privacidad de la información.
- Componente CBC-MAC (*Cipher Block Chaining Message Autenticación Code*), provee autenticación e integridad de la información.

802.1X, EAP-TLS y RADIUS:

802.11i RSN utiliza 802.1X/EAP para el transporte de extremo a extremo de los métodos de autenticación entre las tarjetas de red wireless y el punto de acceso wireless (Wireless AP), y para proporcionar las llaves dinámicas que ellos requieran. A pesar que EAP-TLS (*Extensible Authentication Protocol – Transport Layer Security*) no es un componente oficial del estándar 802.11i, es el protocolo de autenticación *de facto* para redes wireless 802.11i puesto que cumple todos los requerimientos. RADIUS tampoco es un componente oficial de 802.11i pero es el proveedor de autenticación *de facto*.

802.1aa

802.1aa es una revisión de 802.1X que va a corregir muchos de los problemas encontrados en este último. Su desarrollo está en coordinación con el nuevo RFC para EAP y con el objetivo de integrarse a 802.11i.

7.7.7. Recomendaciones de Seguridad para redes LAN Wireless

En el diseño estándar, se asume que los dispositivos wireless están conectados a una sola subred IP, y que la mayoría de servicios para la red cableada están también disponibles para la red wireless.

Algunas recomendaciones de seguridad en Puntos de Acceso (AP) se indican a continuación:

- ☑ Habilitar autenticación (RADIUS, TACACS+) centralizada de usuarios para la interfaz de administración.
- ☑ Elegir Cadenas de Comunidad SNMP difíciles y cambiarlas frecuentemente. Considerar usar SNMP en modo de solo lectura si la infraestructura de administración así lo permite.
- ☑ Deshabilitar cualquier protocolo de administración inseguro o no esencial provisto por el fabricante.
- ☑ Utilizar protocolos de administración seguros tales como SSH (*Secure Shell Protocol*).

- ☑ Limitar el tráfico de administración a una subred dedicada cableada (no wireless).
- ☑ Aislar el tráfico de administración del tráfico de usuarios y cifrarlo de ser posible.
- ☑ Habilitar el cifrado de tramas wireless de ser posible.
- ☑ Ubicar el punto de acceso wireless en un lugar seguro.

Las recomendaciones de seguridad para Clientes/Usuarios Wireless se indican a continuación:

- ☑ Deshabilitar el modo Ad-Hoc.
- ☑ Habilitar el cifrado de tramas wireless de ser posible.

CAPÍTULO VIII

MITIGACIÓN DE ATAQUES RUDIMENTARIOS Y SOFISTICADOS

CAPITULO VIII

MITIGACIÓN DE ATAQUES RUDIMENTARIOS Y SOFISTICADOS

8.1. MITIGACIÓN DE ATAQUES RUDIMENTARIOS

8.1.1. MITIGACIÓN DE ATAQUES DE RECONOCIMIENTO

El enfoque se centra en proteger la red de incursiones de exploración por parte de los atacantes. En realidad, no es posible evitar que los atacantes, y cualquiera en general, tenga acceso a información relacionada con rangos de direcciones, puesta a disposición por organizaciones como ARIN, APNIC y RIPE, o a información de nombres de dominio, disponible en registradores de red. Con esto en mente y siendo realistas, se debe comprender que la defensa empieza en el perímetro de la red, y que iniciar esta tarea involucra dos técnicas básicas: Reducir la visibilidad de la red y mejorar la seguridad de las aplicaciones.

Reducir la Visibilidad de la Red

Reducir la visibilidad de la red involucra reducir al mínimo el número de servicios en el segmento que da cara a la red pública. Esto significa que si servidores Web, SMTP FTP y DNS están situados en la zona desmilitarizada (DMZ) del módulo de acceso a Internet, los únicos puertos de entrada abiertos en el ruteador de borde serán para los servidores Web, SMTP, FTP y DNS. Todos los otros puertos estarán bloqueados con políticas o listas de control de acceso. Si existen otros hosts en la DMZ pero el acceso desde el exterior no es requerido, no deberá llegar tráfico a estos hosts a través del ruteador de borde.

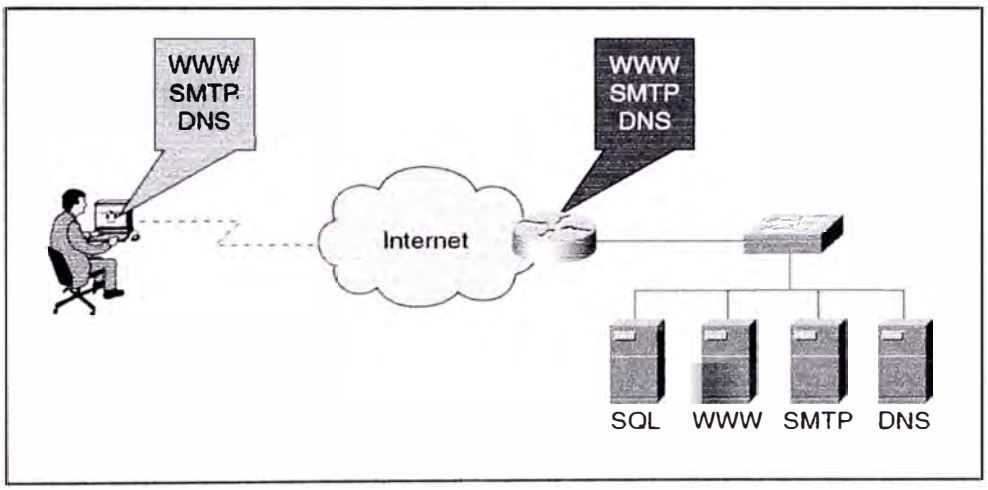

FIGURA 8.1 - Reducción de la Visibilidad de la Red

Este concepto se ilustra en la figura 8.1, en la que se consideran cuatro servidores (WWW, DNS, SMTP y SQL) detrás del ruteador. Un atacante que escanee la red solo encontrará tres servidores: WWW, DNS y SMTP. El cuarto

servidor no será visible para el atacante puesto que las políticas o listas de control de acceso en el ruteador denegarán cualquier acceso al servidor SQL.

Mejorar la Seguridad de las Aplicaciones

Esto involucra estar al día con los parches y actualizaciones para todas las aplicaciones, y reducir la información que las aplicaciones puedan proporcionar a través de mensajes de saludo o *banners*. Es posible configurar *Sendmail*, un popular agente de transporte de mensajería o MTA (*Mail Transport Agent*), de tal manera que no anuncie su versión cuando otro MTA se conecte a él. De manera similar, muchos demonios Telnet y FTP pueden ser configurados para no anunciar el tipo de sistema operativo o la versión cuando un cliente se conecte. Todo esto dificulta los ataques de reconocimiento.

8.1.2. MITIGACIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIOS

La tarea de combatir los ataques DoS o DoS Distribuidos (DDoS) comienza con la identificación de los puntos débiles en la arquitectura de red donde estos ataques pueden tener ventaja. Típicamente los puntos débiles están localizados en el ruteador de borde. Si un atacante lanza un ataque DDoS dirigido a consumir el ancho de banda disponible, detener el ataque en el ruteador de borde no ayuda mucho. Detener un ataque DDoS de gran magnitud requiere coordinación con el ISP. Defenderse de ataques DoS involucra no solo el

defenderse de ataques dirigidos específicamente, sino también el asegurarse que hosts en la red no sean fuente de ataques DoS, puesto que esto también generaría tráfico indeseable. A continuación se describen los métodos usados para mitigar ataques DoS:

Técnicas *Antispoof* o Anti-impostación

Se basan en el filtrado especificado en el RFC 2827. En resumen, a pesar que el RFC 2827 está escrito principalmente desde la perspectiva de un ISP, es de igual forma aplicable a redes de todo tamaño. Este documento recomienda que en el borde de la red del ISP, donde las redes de los clientes se conectan, el tráfico de entrada a la red sea filtrado y restringido a aquellos prefijos asignados al cliente. Por ejemplo, en la figura 8.2 el ISP ha asignado al cliente A el rango 192.168.100.0/24 y al cliente B el rango 192.168.101.0/24. Aplicando filtros en los ruteadores de borde del ISP, éste puede restringir el tráfico que llega a la red del ISP a través de dichos ruteadores, a sólo el tráfico asignado a dichos clientes.

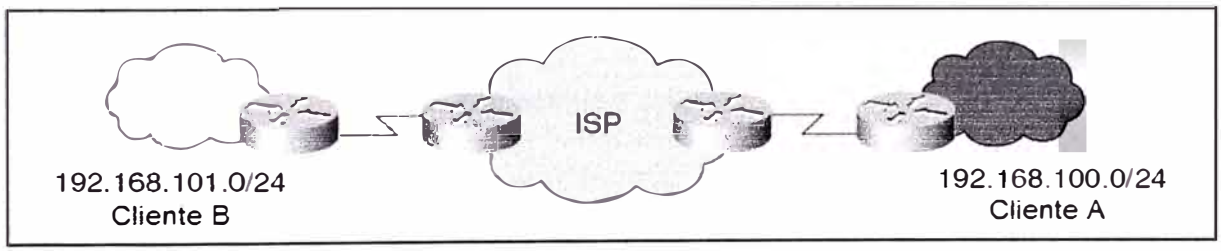

FIGURA 8.2 - Técnicas *Antispoof* o Anti-impostación

Los clientes a su vez pueden implementar filtros de egreso de acuerdo con las recomendaciones del RFC 2827 como filtros adicionales para prevenir que sus redes se conviertan en fuente de ataques DoS.

Técnicas Anti-DoS

Los firewalls pueden proporcionar mecanismos de defensa contra ataques DoS, específicamente contra inundaciones de SYNs TCP, al limitar el número de conexiones semi-abiertas permitidas por host.

Otro mecanismo de defensa es la intercepción de paquetes TCP, mediante el cual el ruteador intercepta las peticiones entrantes SYN TCP provenientes de un cliente hacia un servidor que se busca proteger. El ruteador responde a la petición SYN, enviando un paquete SYN-ACK y espera el paquete ACK TCP final del cliente para completar el saludo de tres vías de TCP. Una vez que este saludo está completo, el ruteador reproduce el saludo con el servidor, permitiendo que todo el tráfico entre el servidor y el cliente continúe. Esta capacidad protege al sistema cuya cola de SYNs TCP de entrada puede ser limitada y por tanto, susceptible a ataques.

Limitar la Tasa de Tráfico

Una organización puede implementar, en cooperación con su ISP, la limitación de tasa de tráfico, mediante la cual, al tráfico no esencial se le da una pequeña

fracción del ancho de banda total del enlace. Adicionalmente, una organización puede implementar Calidad de Servicio (QoS) para identificar el tráfico permitido y asegurar que sea manejado con la prioridad adecuada, mientras que otro tráfico, que potencialmente podría ser no autorizado, sería relegado a un manejo no prioritario. El limitar la tasa de tráfico y aplicar QoS para moldear el tráfico puede ayudar en gran medida a mitigar el impacto de los ataques DoS y DDoS.

Derivar el Tráfico

En la lucha por mitigar los efectos de ataques DoS y DDoS, empresas como Riverhead Networks (adquirida en el 2004 por Cisco Systems), han desarrollado sistemas que permiten identificar actividad de tipo DoS (ataques conocidos o no) usando algoritmos de detección basados en anomalías. Estos sistemas reportan inmediatamente estas anomalías a otro sistema, el cual a su vez envía anuncios BGP (*Border Gateway Protocol*) o de cambios de topología de red al ruteador de *upstream* (corriente arriba) más cercano. De esta manera el tráfico anómalo destinado al objetivo es derivado hacia este sistema, para ser analizado y filtrado mediante algoritmos avanzados. Los paquetes maliciosos son descartados, mientras que los paquetes legítimos son enviados al destino. Los sistemas mencionados han sido diseñados principalmente para ser implementados en redes de proveedores de servicios de Internet (ISPs) y de empresas grandes.

8.1.3. MITIGACIÓN DE ATAQUES DE ACCESO NO AUTORIZADO

En teoría, esta es una de las técnicas de mitigación de ataques más simple. Debido a que un atacante debe ser capaz de acceder a un puerto para obtener acceso a un sistema, la solución más sencilla es denegar el acceso a dicho puerto. Por ejemplo, si para que un atacante obtenga acceso a un sistema se requiere que haga Telnet a dicho sistema, entonces, el bloquear el puerto Telnet a dichos sistemas en el ruteador y firewall, mediante políticas o listas de control de acceso, sería la solución.

Sin embargo, en la práctica a veces es necesario tener habilitados puertos para el funcionamiento de determinados servicios. En dichos caso el bloquear puertos definitivamente, sería una solución extrema e inaceptable. La solución sería aplicar políticas o listas de control de acceso en ruteadores y/o firewalls, que especifiquen los sistemas y puertos a ser accedidos, y los hosts que tendrían acceso a dichos sistemas y puertos. Adicionalmente, mecanismos de autenticación con esquemas de contraseñas cambiantes mejorarían la postura de seguridad.

8.1.4. MITIGACIÓN DE ATAQUES EN LA CAPA DE APLICACIÓN

Desafortunadamente, los ataques a nivel de la capa de Aplicación no pueden ser completamente eliminados. Nuevas vulnerabilidades son descubiertas en

diversas aplicaciones, plataformas y sistemas operativos. Adicionalmente, a medida que el software se hace más y más complejo, la probabilidad de ocurrencia de una vulnerabilidad de consecuencias desastrosas se incrementa dramáticamente.

El primer paso para reducir la posibilidad de un ataque en la capa de aplicación, es seguir las recomendaciones del administrador de sistemas para la operación de los hosts y sistema operativos.

Se recomienda parchar y actualizar el software en todos los sistemas activos en la red, tanto a nivel de sistema operativo como a nivel de las aplicaciones.

Suscribirse a listas de correo, como las de Bugtraq y CERT (*Computer Emergency Response Team*), y acceder a foros que proporcionen información sobre vulnerabilidades existentes y emergentes, es una muy buena idea.

Deben revisarse las bitácoras o registros de eventos del sistema operativo y de la red, y usar las herramientas de análisis de bitácoras, disponibles, para identificar comportamiento que podría indicar intentos de explotación de vulnerabilidades.

Se recomienda, también, implementar sistemas de detección/prevención de intrusos, llamados IDS/IPS (*Intrusion Detection/Prevention System*) tanto del tipo host IDS/IPS como del tipo Network IDS/IPS o de red.

Un host IDS/IPS opera insertando agentes en los hosts. Los agentes protegen al host detectando actividad no autorizada o modificaciones de archivos y reportando e incluso respondiendo a este tipo de actividad.

Un IDS/IPS de red monitorea los paquetes que atraviesan la subred. Cuando detecta un ataque potencial, puede alertar y/o terminar la sesión e incluso reconfigurar termporal o definitivamente los equipos de borde, tales como ruteadores y firewalls, con listas o políticas de control de acceso adecuadas. Ya que los NIDS/NIPSs típicamente trabajan usando firmas de ataques conocidos, comparando el tráfico de red con estas firmas, son susceptibles a generar un alto número de falsas alarmas. Es crucial que estos dispositivos estén correctamente afinados para ser altamente efectivos en detectar ataques reales.

8.1.5. MITIGACIÓN DE ATAQUES DE EXPLOTACIÓN DE CONFIANZA

Los ataques de explotación de confianza pueden ser mitigados a través de un estricto control de acceso y estrictas restricciones en los niveles de confianza dentro de la red. Por ejemplo, los sistemas internos nunca deben confiar

totalmente en los sistemas que se encuentran en la DMZ (zona desmilitarizada) o zona donde se colocan normalmente los servidores de acceso público. Además, la relación de confianza debe estar basada en algo más que la dirección IP del host confiable.

8.2. MITIGACIÓN DE ATAQUES SOFISTICADOS

8.2.1. MITIGACIÓN DE ATAQUES IP *SPOOFING*

Las medidas de defensa contra ataques IP *Spoofing* o de impostación de IPs deben ser implementadas tanto en la red de la empresa como en la red del proveedor. A pesar que estos ataques no pueden ser completamente eliminados, la amenaza que ellos representan puede ser reducida a través del control de acceso y del filtrado según RFC 2827.

IP *Spoofing* funciona correctamente sólo cuando los dispositivos emplean, para la autenticación, un modelo de confianza basado en direcciones IP; el cual permite o deniega el acceso a un host basándose en la dirección IP del cliente.

Métodos de autenticación adicionales, tales como autenticación criptográfica o autenticación fuerte de dos factores usando contraseñas que sirven sólo una vez, ayudan notablemente a mitigar estos ataques.

Control de Acceso

La manera más efectiva de mitigar ataques IP *Spoofing* es configurar adecuadamente el control de acceso, por ejemplo, al denegar acceso a cualquier tráfico que se origine en una red externa que aduzca tener una dirección origen perteneciente a la red interna. Sin embargo, este método sólo es verdaderamente efectivo si las direcciones internas son las únicas confiables, siendo inefectivo si direcciones externas, aún un pequeño grupo de ellas, son consideradas confiables.

Filtrado RFC 2827

Como se discutió en la sección 7.5, en el RFC 2827 se recomienda el filtrado de tráfico en el borde de la red del ISP, donde las redes de los clientes se conectan, permitiendo, así, sólo el tráfico de aquellos prefijos asignados al cliente. Adicionalmente, los clientes del proveedor de servicios pueden implementar filtros de egreso para prevenir que su red se convierta en fuente de ataques DoS.

8.2.2. PROTEGIÉNDOSE DE *SNIFFERS* DE PAQUETES

Los *sniffers* de paquetes representan una amenaza considerable a la seguridad de la red, pues capturan el tráfico que circula por la red, poniendo en jaque la habilidad de mantener la confidencialidad e integridad de la información.

Infraestructura LAN basada en Switches

Una infraestructura LAN basada en switches representa un gran obstáculo para los sniffers de paquetes pues al separar dominios de colisión, se reduce la cantidad de tráfico que es vista por el dispositivo que realiza el *sniffing*. El atacante tendrá acceso sólo al tráfico destinado al puerto específico al que está conectado.

Sin embargo, esto no elimina del todo la amenaza, puesto que con ataques combinados como el de inundación de MACs se puede saturar la tabla de MACs del switch, con información inservible, y lograr que este se comporte como un hub. Para evitar esto, se puede configurar los switches para que sus puertos acepten un número limitado de direcciones MACs.

Herramientas Anti-*Sniffers*

Otro método para mitigar la acción de los *sniffers* de paquetes es usar software o hardware diseñado para detectar el uso de los mismos. Herramientas anti-*sniffers* están disponibles y pueden detectar cambios en los tiempos de respuesta de los hosts para determinar si estos están procesando más tráfico del propio. Otras herramientas en software pueden correr en los hosts y detectar si la interfaz de red ha entrado a modo promiscuo, lo cual es necesario para facilitar las actividades de *sniffing*.

Criptografía

Uno de los métodos más efectivos para protegerse de los *sniffers* de paquetes es usar criptografía. Un *sniffer* de paquetes que monitorea un canal cifrado captura información que aparenta ser cadenas aleatorias de bits. La criptografía involucra el uso de túneles VPN IPSec, el uso de SSH (*Secure Shell*) para conectarse a otro sistema, o el uso de SSL (*Secure Socket Layer*).

8.2.3. MITIGACIÓN DE ATAQUES DE CONTRASEÑAS

Estos ataques pueden ser fácilmente mitigados a través de la implementación de autenticación criptográfica o el uso de contraseñas que sirvan una sola vez. Sin embargo, no todos los dispositivos, aplicaciones o hosts soportan estos métodos de autenticación. Por lo tanto, se hace necesario implementar el bloqueo de cuentas de usuario tras un número determinado de intentos fallidos de autenticación. Esto ayuda a reducir las oportunidades que un atacante tiene para romper una contraseña a través de ataques de fuerza bruta. Dichos ataques implican que el atacante simplemente intentará acceder ingresando nombres de usuarios y contraseñas diferentes hasta finalmente obtener acceso a una cuenta en el sistema. Estos métodos pueden ser manuales o automatizados.

Autenticación

Uno de los métodos más efectivos para contrarrestar ataques de contraseñas es implementar contraseñas difíciles de descifrar para cuentas con privilegios de administrador y proporcionar a los usuarios la capacitación adecuada para que elijan contraseñas igualmente complejas para sus propias cuentas y accesos. Muchos sistemas operativos incluyen herramientas para poner a prueba las contraseñas, guiando a los usuarios en la elección de una contraseña compleja.

Otro método efectivo es usar autenticación fuerte, tal como contraseñas que sirven una sola vez, conocidas como OTPs (*One-time passwords*). Éste es un sistema de autenticación de dos factores que requiere que la persona tenga dos elementos para completar la autenticación. Típicamente, estos elementos son algo que la persona tiene y algo que ella conoce. Por ejemplo, muchos sistemas OTPs usan tarjetas *token*, que son dispositivos en hardware (también los hay en software) que generan una clave aleatoria única, ya sea a intervalos de tiempo definidos o cada vez que se usan. Este sistema requiere que un número de identificación personal (PIN) sea ingresado para generar la OTP apropiada. En algunos casos, las contraseñas generadas aleatoriamente son combinadas con el PIN para crear una contraseña completamente única para ese momento. Este método es muy similar al usado en los cajeros automáticos de los bancos, donde el usuario debe tener su tarjeta de crédito o débito, y debe conocer su PIN para poder acceder a su cuenta.

Pruebas de Contraseñas

Probar contraseñas implica que el administrador realice intentos periódicos de romper las contraseñas de las cuentas, con el objetivo de identificar y corregir contraseñas débiles o fáciles de descifrar. Típicamente, esto se realiza pasando el archivo de contraseñas del sistema por programas tales como L0phtCrack 4, Crack o John the Ripper. Estos programas pueden aplicar intercambios de minúsculas por mayúsculas y agregar caracteres alfanuméricos a una lista o diccionario de contraseñas conocidas.

Educar al Usuario

Los usuarios deben ser instruidos con respecto a la elección de sus contraseñas recordándoles que no deben elegir nombres de cosas que poseen, nombres de miembros de su familia o de alguna mascota. Las políticas de seguridad efectivas contienen políticas de contraseñas que orientan al usuario en cuanto a cómo crear contraseñas complejas. Las siguientes recomendaciones pueden ser usadas. Las contraseñas deben:

- Consistir de al menos ocho caracteres de longitud.
- Contener caracteres en mayúscula y minúscula.
- Contener caracteres tanto alfanuméricos como no alfanuméricos, tales como #, @, % y $.

Idealmente, las contraseñas deberían ser generadas aleatoriamente. Desafortunadamente, ese tipo de contraseñas son también las más difíciles de recordar, lo que lleva a los usuarios a escribirlas en papel, creando riesgos adicionales.

8.2.4. MITIGACIÓN DE ATAQUES DE HOMBRE EN EL MEDIO

Estos ataques pueden ser mitigados efectivamente sólo a través del empleo de criptografía. Si la comunicación es cifrada, el atacante podrá capturar solo el texto cifrado. Si, en cambio, el atacante puede determinar o capturar la llave de la sesión, un ataque de esta naturaleza es posible.

Un ataque de hombre en el medio contra una sesión cifrada puede tener éxito solo si el atacante es capaz de intervenir el proceso de intercambio de llaves. Antes que una sesión cifrada pueda establecerse, ambas partes deben coincidir en el empleo de una llave de sesión que será usada para cifrar el tráfico en ambas direcciones. Para este fin, ambas partes deberán realizar un intercambio de llaves Diffie-Helman, mediante el cual la llave de sesión es derivada de una combinación de llaves privadas y públicas, o de lo contrario es comunicada por algún otro medio (preferiblemente fuera de banda). Un atacante podría colocarse en el medio de las dos partes, de tal manera de negociar una llave distinta con

cada parte y reenviar la comunicación lo suficientemente rápido para mantener el ritmo de comunicación con ambas partes.

8.2.5. MITIGACIÓN DE ATAQUES DE REDIRECCIÓN DE PUERTOS

Para mitigar estos ataques se requiere el uso de modelos de confianza, que pueden ser implementados con restricciones de acceso apropiadas entre los hosts. Mientras haya una relación de confianza implícita entre hosts basada en direcciones IP, la posibilidad de sufrir un ataque de redirección de puertos existe. Un sistema de detección/prevención de intrusos situado en el host (HIDS/HIPS) puede ser usado para detectar e incluso evitar que un atacante intente instalar software de redirección de puertos, tal como *HTTP tunnel* o *NetCat*.

8.2.6. PROTEGIÉNDOSE DE VIRUS, GUSANOS, CABALLOS DE TROYA, ADWARE, SPYWARE Y DEMÁS

La manera más efectiva para mitigar ataques de virus o troyanos es el uso de software antivirus e IDS/IPSs. Estos métodos de mitigación pueden ser desplegados a nivel de host y a nivel de red. La clave es recordar que muchas veces estas aplicaciones o sistemas dependen de bases de datos de firmas de virus y troyanos, y por tanto deben ser mantenidas al día.

Se ha desarrollado software Anti-espía (*Anti-Spyware*), que complementa la acción de los antivirus e IDS/IPSs, permitiendo la detección, bloqueo y limpieza de programas espías o de archivos que almacenan y envían información sensible del usuario, impidiendo o revirtiendo cambios en programas o archivos del sistema.

CAPITULO IX

REDES PRIVADAS VIRTUALES

CAPITULO IX

REDES PRIVADAS VIRTUALES (VPN: *Virtual Private Networks*)

9.1. DEFINICIONES DE RED PRIVADA VIRTUAL

En su sentido más amplio una VPN (*Virtual Private Network*) o Red Privada Virtual es un conjunto de elementos de red en los que se han implementado protocolos para el intercambio de información de manera segura. Esta implementación puede ser hecha sobre una red pública como Internet, o sobre una red privada compartida usando cualquier plataforma: Frame-Relay, ATM, IP, IP/MPLS, etc. Bajo esta definición, podemos tener VPNs implementadas no sólo sobre Internet, sino también, sobre la red privada de algún proveedor de servicios, quien sería capaz de crear redes "virtuales" o lógicas para cada uno de sus clientes, siendo cada una de éstas privadas e invisibles entre sí.

La privacidad en la red virtual se puede lograr no sólo a través del cifrado como sería en el caso de una VPN sobre Internet, usando IPSec; sino también a través del uso de PVCs o circuitos virtuales permanentes para el caso de Frame-Relay o ATM; con políticas o

listas de control de acceso para el caso de una red IP; o mediante el empleo de LSPs (*Label-Switched Paths* o caminos conmutados a partir de etiquetas) para el caso de una red IP/MPLS.

Sin embargo, la definición de VPN o Red Privada Virtual más difundida y sobre la cual se enfoca este capítulo, es la siguiente: Una VPN es aquella red que permite a dos o más sitios o usuarios de una organización comunicarse mediante el uso de una combinación de tecnologías de cifrado, autenticación, y protocolos para encapsular la información en túneles, que proporcionan un transporte seguro de la información sobre la red pública Internet.

Una VPN sobre Internet es una opción mucho menos costosa que usar líneas dedicadas entre cada sitio, o usar una red privada de algún proveedor de servicios.

9.2. TIPOS DE VPN

9.2.1. VPN DE SITIO A SITIO

Consiste en dos o más puntos terminales (*endpoints*) configurados como pares (*peers*) VPN el uno del otro. El término "punto terminal" se refiere al punto donde la VPN, es decir la conexión cifrada, comienza o termina. El tráfico designado que viaja de un extremo a otro es cifrado cuando pasa por el primer

punto terminal y descifrado cuando pasa por el otro. El cifrado es configurado manualmente en ambos extremos o negociado por cada par VPN. Los puntos terminales en este tipo de VPNs son normalmente ruteadores, firewalls con funcionalidad VPN, o dispositivos VPN (en hardware) especializados.

Como se muestra en la figura 9.1 todo el tráfico entre el sitio A y el sitio B viaja por la Internet pero a través de un túnel VPN. Es posible configurar los puntos terminales para que cifren sólo tráfico específico. Cabe resaltar que el tráfico en las redes internas (LANs) ya no está cifrado. Se cifra cuando sale del ruteador hacia Internet y se descifra cuando entra al ruteador en el otro lado.

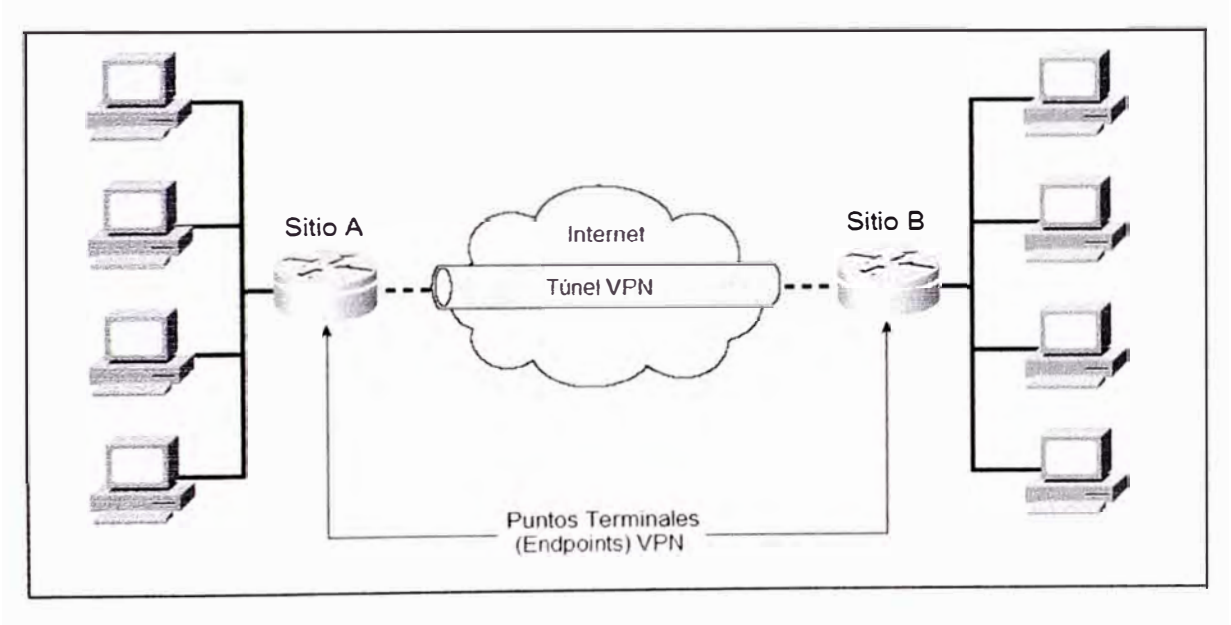

FIGURA 9.1 - Conexión VPN de Sitio a Sitio

Una extensión de este tipo de VPN es aquella donde los puntos de terminación VPN son los hosts mismos que van a intercambiar la información. Este esquema también se conoce como VPN de extremo a extremo.

Las VPNs sitio a sitio se dividen en dos categorías:

- **VPNs Intranet:** Usadas para interconectar de manera segura las distintas localidades de una organización. Las Intranet VPNs permiten a una organización, que puede estar distribuida en múltiples lugares alrededor del mundo, funcionar como una sola red segura.

- **VPNs Extranet:** Proporcionan un canal seguro para la comunicación de una organización con sus socios de negocios, que pueden ser por ejemplo: proveedores, clientes, distribuidores, entre otros.

Las VPNs sitio a sitio son una alternativa a una infraestructura de red WAN usada para conectar oficinas sucursales, oficinas en casa, o sitios de socios de negocio a toda o parte de la red de la organización.

9.2.2. VPN DE ACCESO

También conocidas como VPNs de Acceso Remoto, estas redes usualmente involucran un software cliente VPN instalado en la computadora del usuario

remoto. El usuario remoto se puede conectar a Internet vía acceso conmutado (*dial-up*), cable módem, xDSL, o incluso desde la LAN de otra organización, usando su salida a Internet.

Para acceder a la red de la organización a la que pertenece el usuario remoto, el cliente VPN crea una conexión cifrada desde la computadora del usuario hasta el punto de terminación VPN. Estos puntos de terminación, para el caso de las VPNs de acceso, pueden ser ruteadores, firewalls con funcionalidad VPN, o concentradores VPN.

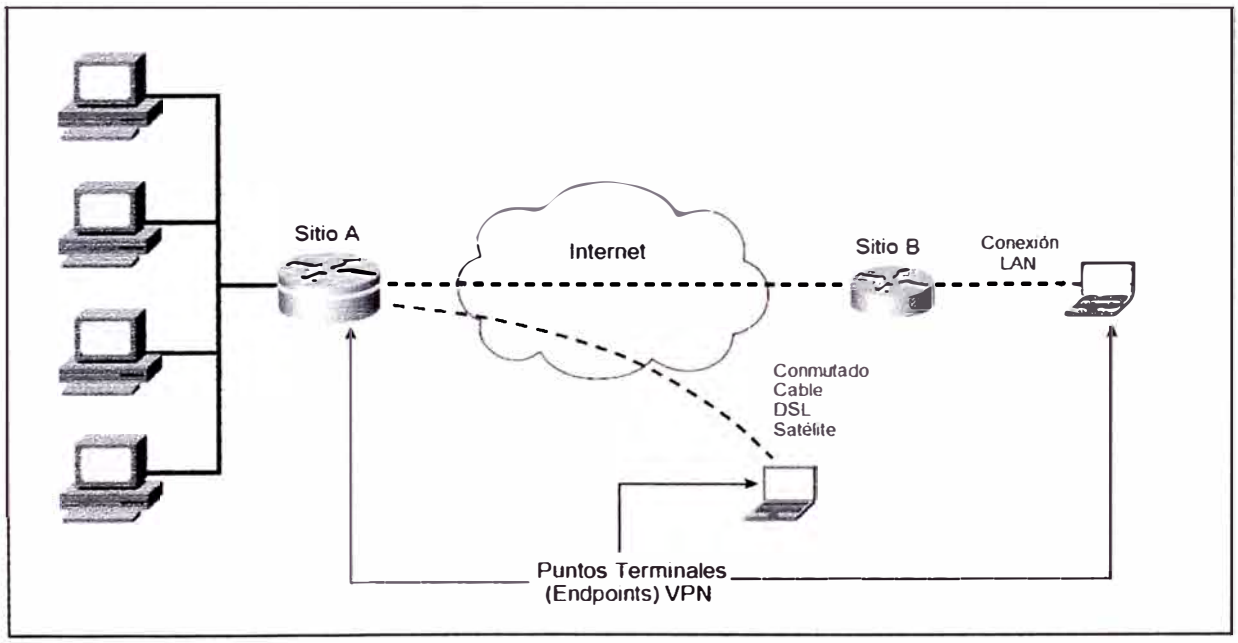

FIGURA 9.2 - Conexiones VPN de Acceso Remoto

En la figura 9.2 se muestran conexiones VPN de tipo acceso remoto contra el sitio A, en donde todo el tráfico de los usuarios remotos hacia A es cifrado, desde que sale de la computadora del usuario hasta que llega al ruteador en A. Este método funciona siempre y cuando el tráfico del cliente VPN no sea bloqueado por una lista de control de acceso o una regla en un firewall. El diseño estándar en redes empresariales grandes es el de implementar el punto de terminación VPN en el perímetro, donde se encuentra el ruteador y el firewall.

9.3. INFRAESTRUCTURA DE SISTEMAS ABIERTOS IPSEC (*Internet Protocol Security*)

IPSec no es un protocolo sino una infraestructura de protocolos abiertos que proveen autenticación de origen, integridad y confidencialidad de la información, y protección *anti-replay*, la cual es una característica de seguridad que detecta cuando un mensaje en la red ha sido recibido más de una vez. IPSec se implementa sobre IPv4 e IPv6. Fue definido en el RFC 2401 de 1997, y hecho estándar por el IETF en 1998.

9.4. IKE (*Internet Key Exchange* o Intercambio de Llaves sobre Internet)

El protocolo de intercambio de llaves sobre Internet IKE (*Internet Key Exchange*), descrito en el RFC 2409, es un protocolo de manejo de llaves estándar usado en conjunto con IPSec.

IKE es un protocolo híbrido basado principalmente en ISAKMP (*Internet Security Association and Key Management Protocol*), descrito en el RFC 2408. IKE también implementa algunas características de otros dos protocolos de manejo de llaves: Oakley, descrito en el RFC 2412; y SKEME. La política de protección dentro de las asociaciones de seguridad es negociada y establecida con la ayuda del protocolo ISAKMP, mientras que las llaves de sesión para el cifrado y la autenticación de paquetes son negociadas e intercambiadas con la ayuda de los protocolos Oakley y SKEME.

- **ISAKMP (*Internet Security Association and Key Management Protocol*)** o protocolo para administración de llaves y asociaciones de seguridad en Internet, define los formatos de la carga útil, los mecanismos para la implementación de un protocolo de intercambio de llaves y la negociación de asociaciones de seguridad.

- **Oakley:** Protocolo de intercambio de llaves que define cómo obtener material autenticado para llaves criptográficas. Para lograr esto utiliza por defecto el algoritmo Diffie-Hellman autenticado. Oakley describe una serie de intercambios de llaves, llamados "modos" y detalla los servicios provistos por cada uno, como por ejemplo, protección de la identidad, autenticación. Y PFS (*Perfect Forward Secrecy*) o perfecta confidencialidad hacia adelante.

- **SKEME:** Protocolo de intercambio de llaves que define cómo obtener material para llaves criptográficas autenticado. Provee anonimato, repudiación y un rápido refresco de llaves.

IKE le provee a IPSec un canal privado y autenticado para administración de llaves, a través del cual las partes pueden comunicarse y negociar llaves de sesión para los protocolos AH y ESP, y negociar también el cifrado, autenticación y los algoritmos de compresión para la sesión. IKE se emplea para realizar la autenticación de los pares VPN, y la negociación, modificación o borrado de Asociaciones de Seguridad (SA) de IKE y de IPSec.

9.5. ASOCIACIONES DE SEGURIDAD Y POLÍTICAS DE PROTECCIÓN O SEGURIDAD

Una Asociación de Seguridad o SA (*Security Association*) contiene toda la información requerida para la ejecución de varios servicios de seguridad de red: servicios a nivel de la capa de red IP, tales como autenticación de cabecera y aquellos para encapsular la carga útil; servicios a nivel de la capa de transporte y aplicación; o servicios de autoprotección del tráfico para las negociaciones.

Una Asociación de Seguridad (SA) es identificada unívocamente por tres parámetros:

- **SPI (*Security Parameters Index*) o Índice de Parámetros de Seguridad:** Es una cadena de bits asignada a la SA y que tiene significado local solamente. Es usado para seleccionar la SA bajo la cual se procesará un paquete recibido.

- **Dirección IP Destino:** Sólo puede ser una dirección *Unicast*, es decir, un destino específico.

- **Identificador de Protocolo de Seguridad:** Indica si la asociación es una SA del protocolo ESP o de AH. Cada asociación de seguridad (SA) usa ESP o AH; si se necesitan ambos, se crean dos SAs.

IPsec puede ser configurado sin IKE. Sin embargo, IKE enriquece a IPSec proporcionando características adicionales, flexibilidad, y facilidad en la configuración.

Las asociaciones de seguridad (SAs) de IPSec deben existir para que IPSec proteja el tráfico de red. IKE maneja dichas SAs a nombre de IPSec, y automáticamente negocia las políticas de protección entre los pares IPSec. Si no hay SAs IPSec presentes para cierto destino VPN, IPSec le pedirá a IKE que las negocie y cree a nombre suyo.

Para negociar y crear SAs IPSec, los procesos IKE en ambos pares VPN deben establecer primero una sesión de manejo de llaves IKE sobre la cual negociarán y crearán una instancia de la política de protección IPSec. Debido a que las negociaciones

IKE deben ser protegidas, cada negociación empieza cuando cada uno de los pares VPN se pone de acuerdo en una política de protección IKE común compartida. Esta política de protección IKE establece qué parámetros de seguridad serán usados para proteger las negociaciones IKE subsiguientes.

Luego de que los pares VPN se han puesto de acuerdo en una política de protección IKE, los parámetros de seguridad de la política son identificados por una asociación de seguridad (SA) IKE, establecida en cada uno de los pares, y que se aplicará al tráfico IKE subsiguiente durante la negociación.

En esta sesión protegida, las SAs IPSec son negociadas y establecidas. Con una política de protección de tráfico (SA IPSec) establecida y el material de llaves criptográficas intercambiado usando el método Diffie-Hellman, IPSec puede comenzar a proteger el tráfico de red. Cuando el tiempo de vida de las SAs IPSec expira, se invoca IKE nuevamente, creándose nuevas SAs IPSec.

Es importante diferenciar entre las dos clases de políticas de protección usadas por IKE/IPSec:

- La política de protección IKE que resulta en SAs IKE, define la protección de la sesión de manejo de llaves IKE solamente.
- La política de protección IPSec que resulta en SAs IPSec, define la protección del tráfico de red.

9.6. PARÁMETROS DE POLÍTICAS DE SEGURIDAD IKE (FASE 1)

La importancia de la Fase 1 de IKE radica en que proporciona la negociación necesaria para crear un canal seguro a través del cual la negociación de la Fase 2 podrá tomar lugar.

Es muy importante que los parámetros de las políticas IKE/ISAKMP en ambas partes coincidan. Si la configuración difiere, no podrán negociar la conexión VPN. Dependiendo de las características de los dispositivos VPN, será posible configurar múltiples políticas, para que los dispositivos busquen una que coincida. Esta característica proporciona flexibilidad ante escenarios diversos.

Se deben considerar los siguientes puntos para la definición de una política de seguridad IKE/ISAKMP.

9.6.1. IDENTIFICACIÓN DEL PAR VPN

El par VPN es el dispositivo en el otro extremo de la conexión VPN que funciona como punto de terminación, y con el que se negocia para crear el túnel VPN. Este par VPN puede ser identificado ya sea por su dirección IP o su nombre de host.

9.6.2. MÉTODO DE DISTRIBUCIÓN DE LLAVES

Esto normalmente se determina dependiendo del tamaño esperado de la red VPN. Para redes que sólo requieren algunos pares (*peers*) VPN, es posible distribuir manualmente las llaves, es decir, configurar cada *peer* manualmente. Esta tarea puede resultar complicada y engorrosa en redes grandes donde hay muchas sesiones VPN punto a punto cada una con una llave distinta. Para redes grandes, es recomendable usar un servidor CA (*Certificate Authority*) o Autoridad Certificadora. Este método permite un crecimiento significativo pues un CA confiable identifica a cada *peer* VPN a través del certificado digital que este posea. Si no se van a distribuir manualmente las llaves, se necesita implementar IKE para soportar el método de distribución de llaves elegido.

9.6.3. MÉTODO DE AUTENTICACIÓN

Existen varias maneras de configurar los equipos VPN para que se autentiquen entre sí durante la fase 1 de la negociación IKE y establezcan la SA. El tipo de autenticación a usar se determina usualmente por el número de túneles VPNs que se manejarán y cuan dinámico será el ambiente de red. A continuación tres de los métodos usados:

- **Llave Secreta Pre-compartida (*PSK: Pre-Shared Keys*)**

  Si la organización requiere conectividad VPN con algunos pocos sitios, se podría emplear configuración de autenticación estática en los equipos. A esta

configuración estática se le conoce como de llaves pre-compartidas puesto que las llaves criptográficas son configuradas manualmente en cada par VPN. Las llaves pre-compartidas son cadenas alfanuméricas (similares a las contraseñas) que deben coincidir exactamente en cada par VPN para que se pueda negociar la conexión.

Los pares VPN se autentican el uno al otro, procesando y enviando el resultado de aplicar una función *hash* a datos que incluyen la llave pre-compartida. Si la contraparte VPN que lo recibe es capaz de crear independientemente el mismo resultado usando su llave pre-compartida, entonces sabrá que ambos comparten la misma clave secreta y autenticará a la otra parte.

La administración de múltiples conexiones VPN usando llaves pre-compartidas puede volverse engorrosa a medida que el número de conexiones crece.

- **Firmas y Certificados Digitales RSA**

  RSA es un sistema criptográfico de llave pública usado para autenticación en la fase 1 de IKE. RSA fue desarrollado en 1977 por Ron Rivest, Adi Shamir, y Leonard Adelman.

El método de firmas RSA emplea una configuración de firmas digitales en el que cada dispositivo firma digitalmente un conjunto de datos y los envía hacia la otra parte. Este método emplea una Autoridad Certificadora (CA) para que genere un certificado digital de identidad único que sea asignado a cada par VPN para la autenticación. El certificado digital de identidad funciona de manera similar a una llave pre-compartida pero proporciona un nivel mucho mayor de seguridad. Tanto el que inicia como el que responde a una sesión IKE usando firmas RSA, envía su propio identificador (IDi o IDr), su certificado digital de identidad, y una firma RSA que consiste en una variedad de valores IKE, todos cifrados por el método de cifrado (DES o 3DES) negociado por IKE.

- **"*Nonces*" cifrados por RSA**

  Este método requiere que cada parte genere un número pseudo aleatorio o *nonce*, y lo cifre con la llave pública RSA de la otra parte. La autenticación se inicia cuando cada parte descifra el *nonce* de la otra parte con una llave privada local (y otra información disponible pública y privada), y luego usa el *nonce* descifrado para generar un *hash* o compendio de mensaje cifrado.

  Este método es más seguro que el de llave pre-compartida puesto que un *nonce* diferente es generado con cada negociación. Además, permite que cada

parte pueda, en caso sea necesario, negar que formara parte de un intercambio. Sin embargo, su configuración es compleja.

9.6.4. ALGORITMO DE CIFRADO DE MENSAJES

- **DES (*Data Encryption Standard*):** DES es un algoritmo de cifrado simétrico de 56 bits. Utiliza un bloque de 64 bits de texto llano y lo convierte en texto cifrado del mismo tamaño, cifrándolo con una llave secreta. La longitud de la llave es de 64 bits también, pero como 8 bits son usados para la paridad, quedan 56 bits como longitud efectiva de la llave. Por ser simétrico, ambas partes deben conocer la llave secreta, la cual es usada tanto para cifrar como para descifrar.

  DES fue desarrollado en 1974 por IBM y convertido en estándar por el gobierno de los Estados Unidos en 1977. Fue re-certificado como estándar cada cinco años por el Instituto Nacional de Estándares y Tecnología (NIST), pero en 1997 un evento patrocinado por RSA y realizado con la participación de 14000 usuarios de computadoras, hizo posible descifrar un mensaje que había sido cifrado con DES, descubriendo la llave después de probar con solo 18 cuatrillones de las 72 cuatrillones de llaves posibles. NIST tuvo que escoger otro algoritmo para reemplazarlo, y el elegido fue el algoritmo Rijndael, que se convirtió en AES (*Advanced Encryption Standard*).

Por esta razón, DES no debe ser usado si la información es altamente sensible. Normalmente se usa para conexiones VPN a localidades fuera de los Estados Unidos que no pueden pagar niveles mayores de cifrado debido a las políticas de exportación de tecnología de los Estados Unidos.

- **3DES (*Triple-Data Encryption Standard*):** 3DES es un algoritmo de cifrado simétrico de 168 bits. 3DES aplica tres fases diferenciales de DES, triplicando efectivamente la longitud de la llave a 168 bits.

- **AES (*Advanced Encryption Standard*):** AES o Estándar de Cifrado Avanzado es un algoritmo de cifrado simétrico. Fue el resultado de una convocatoria mundial organizada por el Instituto Nacional de Estándares y Tecnología (NIST) en 1997 para adquirir un algoritmo de cifrado con miras a reemplazar a DES. El algoritmo elegido fue el Rijndael, desarrollado por dos belgas: Vincent Rijmen y Joan Daemen. AES proporciona fuerte cifrado para entornos variados: plataformas de software estándares y diversas implementaciones en hardware. AES está diseñado para ser más seguro que DES, pues trabaja con llaves de mayor longitud, a la vez que asegura que la única forma de descifrar un mensaje sea que el atacante intente cada llave posible. AES tiene una longitud de llave variable, pudiendo especificar llaves de 128 bits (por defecto), de 192 bits, o de 256 bits. También es más rápido que 3DES.

9.6.5. ALGORITMO DE INTEGRIDAD DE MENSAJES (*Hash*)

El algoritmo de *hash* es una fórmula matemática que convierte un mensaje de entrada de cualquier longitud en una cadena de dígitos única de longitud fija conocida como "*message digest*" o compendio de mensaje y que representa al mensaje original. Un hash es una función unilateral, es decir que es casi imposible revertir el proceso para determinar el mensaje original a partir de ésta. Además, una función hash no producirá el mismo "*message digest*" para dos entradas distintas. Debido a que el "*message digest*" es usualmente más pequeño que el mensaje original, es mucho más eficiente firmar el "*digest*" o compendio que el mensaje original. Los algoritmos de Hash más usados son;

- **MD5 (*Message Digest 5*):** La salida de MD5 es de 128 bits. Debido a que su "message digest" es de menor tamaño, su procesamiento es más rápido.

- **SHA-1 (*Secure Hash Algorithm 1*):** La salida de SHA-1 es de 160 bits, y debido a que es mayor que para el caso de MD5, SHA-1 se considera más seguro. Sin embargo, requiere más ciclos de CPU para su procesamiento.

HMAC (*Keyed-Hashing Message Authentication*) es una variante que proporciona un nivel de seguridad extra, realizando procesos criptográficos adicionales y usando una llave secreta para el cálculo y verificación de los

valores de autenticación del mensaje. HMAC es una variante que puede ser adicionada a los algoritmos de *hash* soportados.

9.6.6. INTERCAMBIO DE LLAVES USANDO DIFFIE-HELLMAN

El algoritmo Diffie-Hellman, también llamado acuerdo de llave exponencial, fue descubierto en 1976 por Whitfield Diffie y Martin Hellman. La seguridad que provee deriva de la dificultad que existe para calcular algoritmos discretos de números muy grandes. Diffie-Hellman es usado para deducir una llave secreta compartida, sobre canales no seguros y sin tener que transmitírsela el uno al otro. Se emplea mucho hoy en día en el manejo de llaves, proporcionando material de llaves criptográficas para otros algoritmos simétricos, tales como DES o MD5 con HMAC.

Existen siete "grupos" Diffie-Hellman con longitudes de llaves variables. Los más usados son el grupo 1 con 768 bits, y el grupo 2 con 1024 bits.

En la figura 9.3 y a continuación se muestra el funcionamiento de Diffie-Hellman:

1. A y B acuerdan usar un valor generador g y un módulo p. Generalmente, el generador g es un valor pequeño (e.g. 2, 3, ...) y p es un número primo grande.

2. A tiene o escoge un número entero grande X_A que se mantendrá secreto, y le envía a B el valor público Y_A, calculado de la siguiente manera:

$$Y_A = g^{X_A} \bmod p$$

3. B tiene o escoge un número entero grande X_B que se mantendrá secreto, y le envía a A el valor público Y_B, calculado de la siguiente manera:

$$Y_B = g^{X_B} \bmod p$$

4. A calcula el valor K_A a partir de Y_B: $K_A = Y_B^{X_A} \bmod p$

5. B calcula el valor K_B a partir de Y_A: $K_B = Y_A^{X_B} \bmod p$

6. Pero resulta que: $K_A = K_B = g^{X_A X_B} \bmod p$

De esta manera, A y B han compartido un valor secreto que no ha sido transmitido. Incluso si alguien escuchó el medio y capturó la información intercambiada, no hay manera que pueda hallar el valor secreto a partir de la información capturada. Esto debido a que calcular un logaritmo discreto de Y_A o Y_B no es factible hasta el momento.

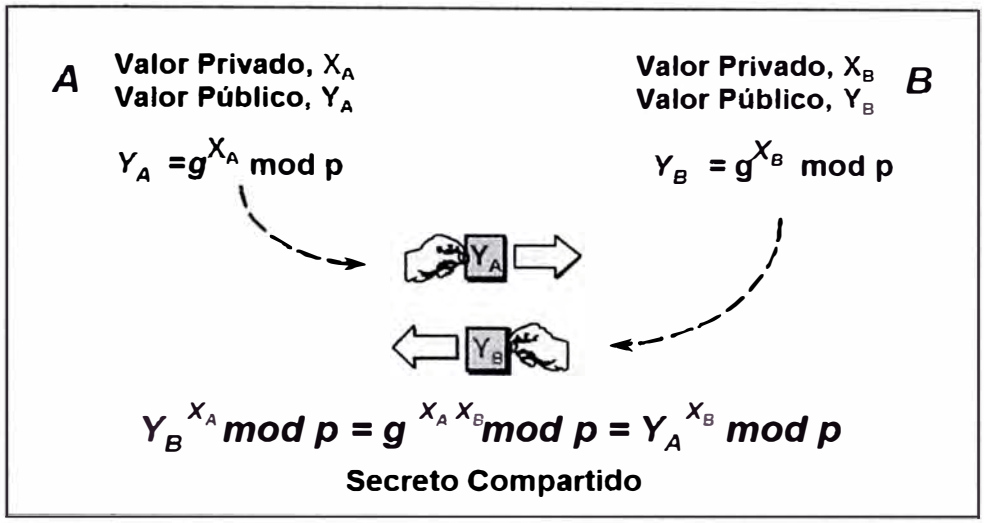

FIGURA 9.3 - Intercambio de Llaves usando Diffie-Hellman

Por el contrario, un atacante tratará de interceptar el intercambio para convertirse en un intermediario entre las partes, negociando un valor secreto con cada una y haciéndoles creer que están conversando entre ellas. Este tipo de ataque es conocido como de "Hombre en el Medio".

Debido a esto, se desarrolló una mejora: el protocolo Diffie-Hellman Autenticado, o STS (*Station-to Station*). La inmunidad contra ataques de Hombre en el Medio se obtiene al permitir que las dos partes se autentiquen entre ellas mediante el uso de firmas digitales o certificados de llave pública. Antes de la ejecución del protocolo, las dos partes (A y B) obtienen una par de llaves pública/privada y un certificado para la llave pública. Durante la ejecución, A firma ciertos mensajes incluyendo el valor público Y_A. B procede

de manera similar. Aunque un atacante C, capture los mensajes entre A y B, no podrá falsificar las firmas sin las llaves privadas de A y B.

9.6.7. TIEMPO DE VIDA DE LA ASOCIACIÓN DE SEGURIDAD IKE

El tiempo de vida de la SA IKE es el tiempo que cada sistema espera antes de iniciar otro intercambio de llaves. Esto permite a los sistemas renegociar constantemente la conexión, reduciendo enormemente la posibilidad de que un atacante que husmee el tráfico pueda descifrar la conexión.

9.7. PARÁMETROS DE POLÍTICAS DE SEGURIDAD IPSEC (FASE 2)

Las políticas IPSec son también llamadas políticas IKE de Fase 2 puesto que, si se emplea IKE para negociar las SAs IPSec, dichas políticas se utilizan durante la segunda fase de la negociación IKE. IKE Fase 1 establece un túnel bidireccional seguro o SA IKE, el cual es usado para completar la negociación de las SAs IPSec. Los dispositivos VPN deben negociar dos SAs IPSec unidireccionales separadas para facilitar el tráfico bidireccional entre los pares VPN.

9.7.1. MODOS DE VPN IPSEC

IPSec usa dos modos distintos para las VPNs, cada uno de los cuales tiene un propósito específico. Por tanto, es importante seleccionar el modo adecuado al configurar una VPN. Los modos VPN IPSec son los siguientes:

- **Modo Túnel:** Este modo es comúnmente usado tanto para VPNs de sitio a sitio como para VPNs de acceso remoto, en las que el destino final no es el punto de terminación VPN. Tanto la información de origen como la de destino (en el encabezado IP original) es cifrada cuando se usa el modo túnel y no es descifrada hasta que llega al punto de terminación VPN.

- **Modo Transporte:** Este modo es comúnmente usado cuando el destino final es el punto de terminación VPN. El encabezado IP original no es cifrado cuando se usa este modo.

9.7.2. PROTOCOLOS IPSEC

- **ESP (*Encapsulating Security Payload*):** ESP proporciona autenticación de origen de los datos, cifrado y servicios *anti-replay*. Es responsable de llevar la información de un origen a un destino de manera segura, verificando que la información no haya sido alterada, y asegurándose que la sesión no pueda ser interceptada.

ESP puede ser usado para validar al emisor, ya sea por sí mismo o en conjunto con AH (*Authentication Header*). ESP puede ser configurado para cifrar el paquete de datos entero o sólo la carga útil del paquete. La IANA (Autoridad en Asignación de Números en Internet) asignó a ESP el número 50, el cual va en el campo de Protocolo de IPv4, o en el campo de Siguiente Encabezado de IPv6. En la figura 9.4 se muestra un paquete IPv4 sin ser encapsulado, y cómo ESP encapsula dicho paquete IPv4 tanto en modo transporte como en modo túnel:

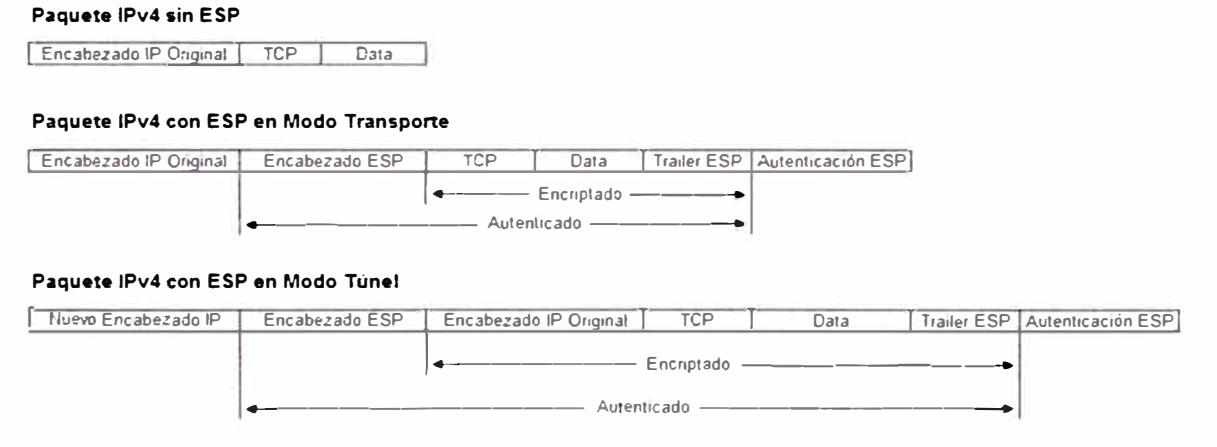

FIGURA 9.4 - Encapsulado de IPv4 con ESP en Modo Transporte y en Modo Túnel

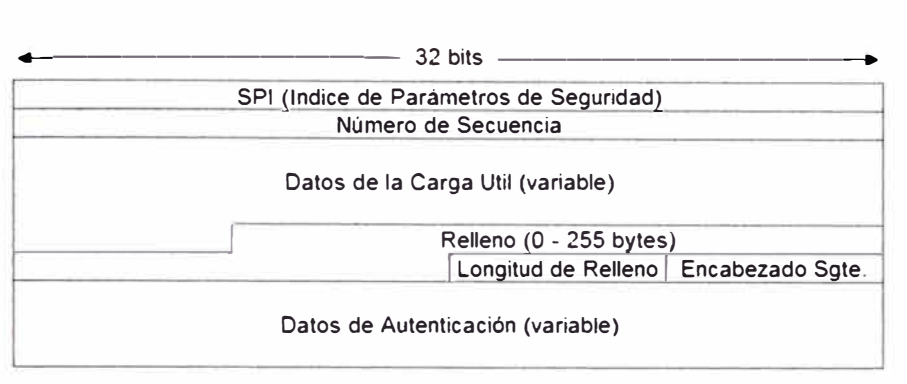

FIGURA 9.5 – Formato del Paquete ESP

Formato del Paquete ESP

En la figura 9.5 se muestra el formato que tiene el paquete ESP, y a continuación se describe cada uno de sus campos.

- **SPI (*Security Parameters Index*) o Índice de Parámetros de Seguridad:** El campo SPI es un valor arbitrario de 32 bits que, en combinación con la dirección IP y el protocolo de seguridad ESP, identifica unívocamente la Asociación de Seguridad para este datagrama. Este valor es normalmente seleccionado por el sistema destino durante el establecimiento de la SA. El conjunto de valores SPI en el rango del 1 al 255 están reservados por la IANA para uso futuro. El valor SPI cero (0) está reservado para uso local o una implementación específica y no debe ser enviado hacia fuera. Por ejemplo, una implementación de administración de llaves podría usar el

valor cero para indicar que no existe una SA todavía. Este campo es mandatorio.

Número de Secuencia: Este campo de 32 bits (sin signo) contiene el valor de un contador incremental. Es mandatorio y está presente aún así el receptor elija no habilitar el servicio *anti-replay* para una SA específica. Tanto los contadores del origen como del destino son inicializados a cero cuando la SA es establecida. Si el servicio *anti-replay* está habilitado (por defecto lo está), el número de secuencia nunca debe volver a cero. Por lo tanto, los contadores de las partes deben inicializarse estableciendo una nueva SA y por lo tanto una nueva llave, antes que se transmita el paquete 2^32 en una SA.

- **Datos de la Carga Util:** Es un campo mandatorio y variable que contiene información descrita por el campo de Encabezado Siguiente. Si el algoritmo usado para cifrar la carga útil requiere información de sincronización criptográfica, como un Vector de Inicialización (IV), entonces esta información puede ser llevada explícitamente en este campo.

Relleno (para Cifrado): Muchos factores requieren el uso del campo de relleno, por ejemplo, si el algoritmo de cifrado empleado requiere que la longitud del texto llano (datos de carga útil, encabezado siguiente, relleno y

longitud de relleno) sea un múltiplo de un número de bytes, e.g. el tamaño del bloque de un cifrador de bloque. El relleno también se necesita, independientemente de los requerimientos del algoritmo de cifrado, para asegurarse que los campos estén alineados con el límite de 32 bits, tal como se puede ver en la figura 9.5.

Longitud del Relleno: Indica el número de bytes del relleno que lo precede. El rango válido es de 0 a 255 bytes, donde un valor de cero indica que no hay bytes de relleno presentes. Este campo es mandatorio.

- **Encabezado Siguiente:** Es un campo de 8 bits que identifica el tipo de datos contenido en el campo de Datos de la Carga Útil, e.g. un encabezado de extensión en IPv6 o un identificador de protocolo de capa superior. El valor de este campo es elegido de un conjunto de números de protocolos IP definidos por la IANA. Este campo es mandatorio.

- **Información de Autenticación:** Es un campo de longitud variable que contiene un Valor de Chequeo de Integridad (ICV) calculado a partir del paquete ESP, sin incluir la Información de Autenticación. La longitud del campo es especificada por la función de autenticación elegida. Este campo es opcional, y sólo se incluye si el servicio de autenticación ha sido elegido para la SA en cuestión. La especificación del algoritmo de autenticación

debe indicar la longitud del ICV, las reglas de comparación y los pasos para la validación.

- **AH (*Authentication Header*) o Encabezado de Autenticación**

  AH provee autenticación de origen o verificación de que la información proviene realmente del emisor. Esta funcionalidad también previene la interceptación de sesiones. AH proporciona servicios *anti-replay* pero no cifrado de datos. Mientras que ESP sólo autentica la carga útil, AH autentica al encabezado IP. AH no es compatible con NAT (*Network Address Translation*) o PAT (*Port Address Translation*) puesto que estos cambian la dirección IP origen, haciéndola distinta de la dirección IP origen en el encabezado de autenticación. El tráfico sería entonces rechazado por la contraparte IPSec, pues la dirección IP origen en el encabezado IP y en el encabezado de autenticación no coincidirían. La IANA asignó el número de protocolo 51 para AH, el cual va en el campo de Protocolo del paquete IPv4, o en el campo de Encabezado Siguiente de IPv6. En la figura 9.6 se muestra un paquete IPv4 sin ser encapsulado, y cómo AH modifica dicho paquete IPv4 tanto en modo transporte como en modo túnel.

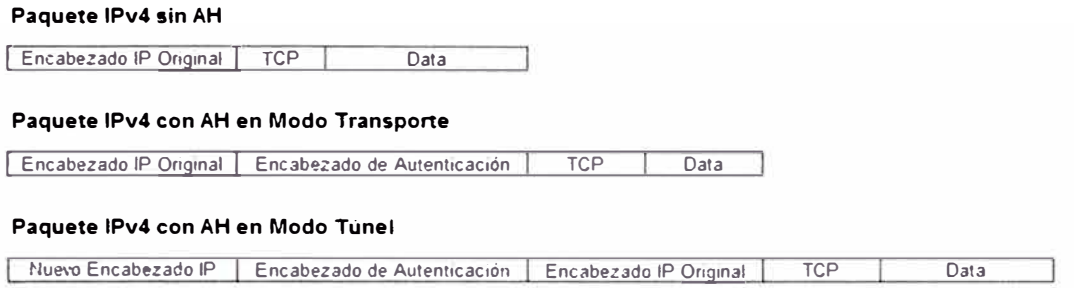

FIGURA 9.6 - AH modificando a un paquete IPv4 en Modo Transporte y en Modo Túnel

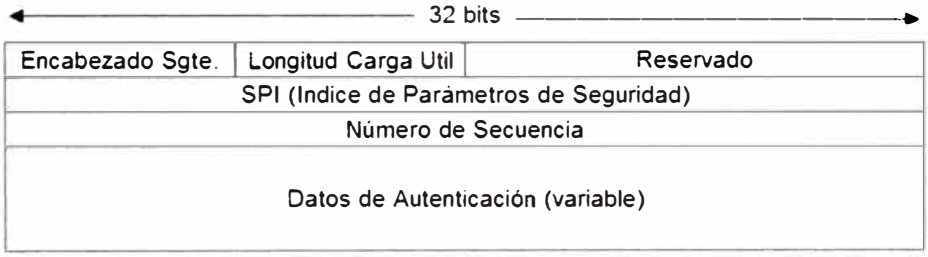

FIGURA 9.7 – Formato del Paquete AH

Formato de Paquete AH

En la figura 9.7 se muestra el formato que tiene el paquete AH. A continuación se describe cada uno de los campos.

- **Encabezado Siguiente:** Es un campo de 8 bits que identifica el tipo de carga útil que sigue al Encabezado de Autenticación. El valor de este campo es elegido de un conjunto de números de protocolo IP definidos por la IANA.

- **Longitud de la Carga Útil:** Este campo de 8 bits especifica la longitud del Encabezado de Autenticación en palabras de 32 bits.

- **Reservado:** Este campo de 16 bits está reservado para uso futuro. Debe ser puesto a cero.

SPI (*Security Parameters Index*) o Índice de Parámetros de Seguridad: El campo SPI es un valor arbitrario de 32 bits que, en combinación con la dirección IP y el protocolo de seguridad AH, identifica unívocamente la Asociación de Seguridad para este datagrama. Este valor es normalmente seleccionado por el sistema destino durante el establecimiento de la SA. El conjunto de valores SPI en el rango del 1 al 255 están reservados por la IANA para uso futuro. El valor SPI cero (0) está reservado para uso local o una implementación específica y no debe ser enviado hacia fuera. Por ejemplo, una implementación de administración de llaves podría usar el valor cero para indicar que no existe una SA todavía. Este campo es mandatorio.

- **Número de Secuencia:** Este campo de 32 bits (sin signo) contiene el valor de un contador incremental. Es mandatorio y está presente aún así el receptor elija no habilitar el servicio *anti-replay* para una SA específica. Tanto los contadores del origen como del destino son inicializados a cero

cuando la SA es establecida. Si el servicio *anti-replay* está habilitado (por defecto lo está), el número de secuencia nunca debe volver a cero. Por lo tanto, los contadores de las partes deben inicializarse estableciendo una nueva SA y por lo tanto una nueva llave, antes que se transmita el paquete 2^32 en una SA.

- **Datos de Autenticación:** Este es un campo variable que contiene el Valor de Chequeo de Integridad (ICV) para este paquete. El campo debe tener como longitud un múltiplo entero de 32 bits, por lo que puede existir un relleno explícito. El algoritmo de autenticación debe especificar la longitud del ICV y las reglas de comparación y pasos para la validación.

9.7.3. TRANSFORMADAS IPSEC

Las transformadas y grupos de transformadas son una combinación definida de protocolos IPSec, algoritmos de cifrado y de *hash*. La combinación que se elija puede enfocarse más en la autenticación, cifrado o combinarse para cubrir ambos. Los siguientes protocolos y algoritmos son combinados para crear las transformadas:

- Protocolos IPSec: AH y ESP
- Algoritmos de Cifrado: DES, 3DES, AES.
- Algoritmos de *Hash*: SHA-1 y MD5 (con o sin HMAC)

9.7.4. TIEMPO DE VIDA DE LA ASOCIACIÓN DE SEGURIDAD IPSEC

El tiempo de vida de una SA IPSec determina con qué intervalo los dispositivos VPN renegociarán la conexión. Una conexión que cambia constantemente es extremadamente difícil de descifrar, puesto que las muestras de información continúan cambiando, y no se deja información consistente para que un criptógrafo la descifre. Si el criptógrafo fuera capaz de descubrir las llaves para la conexión, sólo serían válidas durante el tiempo de vida de las SAs. El tiempo de vida de las SAs IPSec, se puede configurar ya sea en segundos (siendo 3600 segundos el valor por defecto) o por kilobytes, es decir, la cantidad de información que pasa a través del túnel.

9.7.5. PFS (*Perfect Forward Secrecy*) O PERFECTA CONFIDENCIALIDAD HACIA ADELANTE

Por cuestiones de eficiencia, se puede especificar que una misma Asociación de Seguridad o SA IKE Fase 1 (*Main Mode* o Modo Principal para IPSec) sea usada para negociar múltiples Asociaciones de Seguridad o SAs IKE Fase 2 (*Quick Mode* o Modo Rápido para IPSec).

Recíprocamente, se puede especificar que cada SA IKE Fase 1 sea usada para una SA IKE Fase 2. Es decir, el demonio IKE creará una nueva SA IKE por cada negociación de SA IPSec. Esto proporciona una característica de seguridad

conocida como PFS (*Perfect Forward Secrecy* o Perfecta Confidencialidad hacia adelante) con protección de llaves e identidades.

Con PFS, la exposición de una llave solo podría exponer la información protegida por dicha llave. Si un atacante fuera capaz de adivinar o capturar una llave para una sesión, eso no le serviría para descifrar mensajes de sesiones previas (que puedan haber usado el mismo par de llaves pública/privada para generar la llave de cifrado simétrica). Dicho de otra manera, con PFS no deberá ser posible determinar llaves de sesiones previas aún así se conozca una o las dos llaves privadas usadas para generarlas. De la misma manera, un atacante no podrá descifrar mensajes usando llaves derivadas de la captura de información de sesiones previas.

Si PFS es especificado en una política de seguridad IPSec, un nuevo intercambio Diffie-Hellman se produce con cada Modo Rápido (Quick Mode) IPSec, proporcionando material criptográfico para llaves con mayor entropía y, por lo tanto, mayor resistencia ante ataques criptográficos. Cada intercambio Diffie-Hellman requiere largas operaciones de exponenciación, lo que incrementa el uso del CPU y disminuye el desempeño.

Otros parámetros a considerar para las políticas de seguridad IPSec son:

- Definir la contraparte IPSec, es decir, el dispositivo VPN al otro extremo de la conexión, ya sea por dirección IP o nombre de host.
- Identificar a qué hosts o redes locales se les permitirá enviar tráfico a través del túnel VPN.
- Seleccionar el tipo de iniciación de Asociación de Seguridad, es decir, determinar si las SAs IPSec serán negociadas usando IKE, lo cual es recomendable, o usando IPSec manual. Cuando se configuran los parámetros IPSec manualmente, se deben ingresar todas las llaves necesarias para crear la conexión. Este tipo de configuración remueve la funcionalidad que permite a los pares VPN renegociar y constantemente cambiar los parámetros de conexión, y reduce enormemente la seguridad de la conexión.

En la figura 9.8 se puede apreciar los principales parámetros de las políticas de seguridad IKE e IPSec para una VPN de dos puntos.

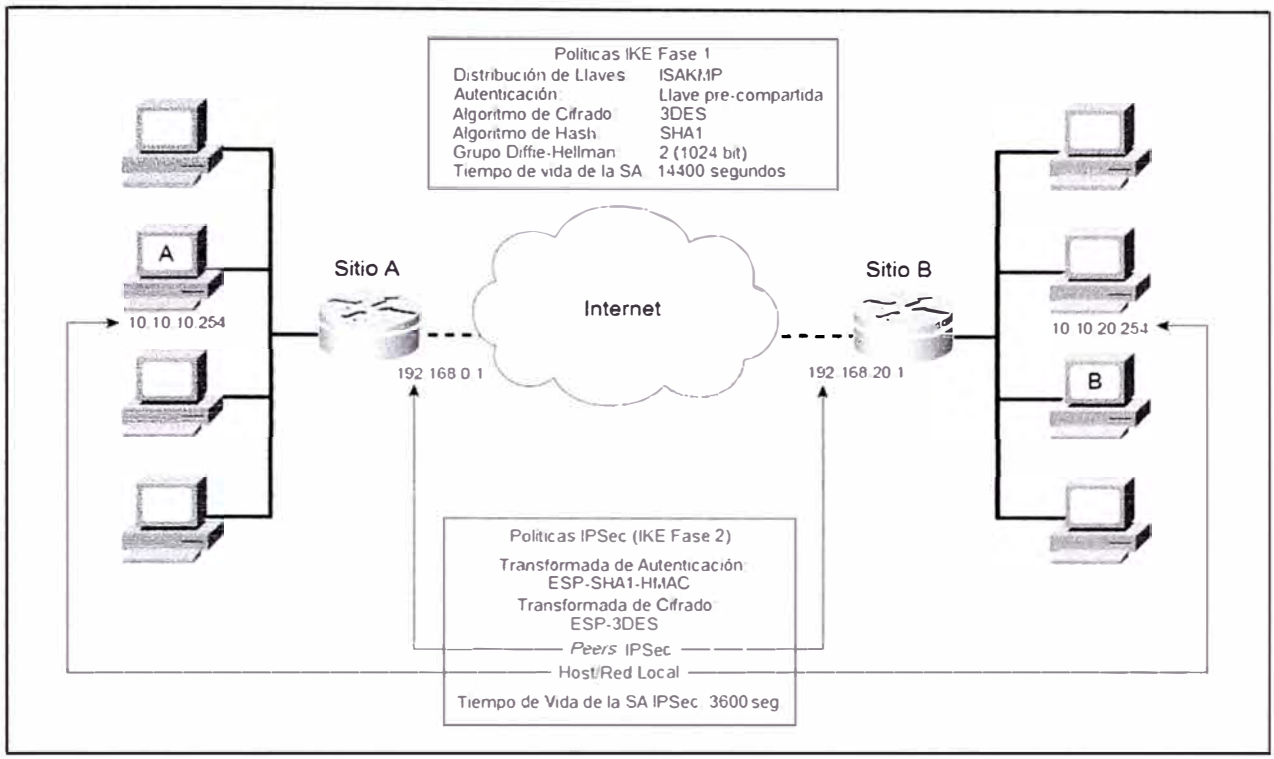

FIGURA 9.8 - Parámetros de Políticas de Seguridad IKE/ISAKMP e IPSec

Otros elementos empleados en el proceso IPSec son:

- **SPD (*Security Policy Database*) o Base de Datos de Políticas de Seguridad:** IPSec emplea la SPD para saber como manejar los mensajes. Así, para cada paquete IP, decide si proporciona sus servicios de seguridad, si deja pasar el paquete, o si lo descarta. Una SPD contiene entradas, cada una de las cuales define un grupo de tráfico IP (a través de valores en los campos de IP y protocolos de las capas superiores), y apunta a una SA para dicho tráfico.

- **SAD (*Security Association Database*) o Base de Datos de Asociaciones de Seguridad:** En toda implementación IPSec, existe una base de datos que define los parámetros asociados con cada Asociación de Seguridad (SA), tales como:
  - Información de AH: algoritmo de autenticación, llaves, tiempo de vida de las llaves, etc.
  - Información de ESP: algoritmo de cifrado y autenticación, llaves, Vectores de Inicialización (IVs), tiempos de vida de las llaves.
  - Contador de Número de Secuencia: usado para generar un número que va en el campo de Número de Secuencia de AH y ESP.
  - Ventana *Anti-replay*: usada para determinar si el paquete AH o ESP entrante es repetido.
  - Tiempo de Vida de la Asociación de Seguridad.
  - Bandera de sobreflujo de contador de secuencia: indica qué hacer cuando ocurre un sobreflujo del contador de secuencia.
  - Modo de Protocolo IPSec: Modo túnel o modo transporte.
  - MTU (Unidad de Transferencia Máxima) de la trayectoria: determina si existe alguna limitación con el MTU de la trayectoria. Esto está íntimamente ligado con la fragmentación. En la mayoría de casos, la fragmentación se da después de aplicar el proceso IPSec. El MTU en el dispositivo que realiza el cifrado, o en los dispositivos previos al cifrado, debe ser especificado de tal manera que considere que el proceso de encapsulado en túnel adicionará una nueva cabecera (*overhead*).

Es decir si el MTU por defecto es 1500 bytes deberá configurarse un MTU menor (e.g. 1400 bytes) considerando el *overhead* generado por IPSec.

9.8. FUNCIONAMIENTO DE IPSEC

Se requieren cinco pasos para crear y finalizar un túnel IPSec para una VPN. Los puntos de terminación VPN realizan diferentes funciones en cada paso para establecer la conexión cifrada.

PASO 1:

El tráfico "interesante" inicia el proceso IPSec. Se llama tráfico 'interesante" a aquel que va a ser cifrado. Qué tráfico es considerado "interesante" se determina durante la formulación de la política de seguridad. La política es luego implementada en una interfaz en particular para cada contraparte IPSec.

Por ejemplo, en el caso de una VPN sitio a sitio, el usuario en la computadora origen del sitio B inicia una conexión con el sistema destino en el lado A. Si el dispositivo VPN en B reconoce el tráfico como tráfico "interesante" inicia el proceso IKE con el dispositivo VPN en A.

Para el caso de una VPN de acceso remoto, el usuario en su computadora u otro dispositivo puede seleccionar qué conexiones serán aseguradas con IPSec, mediante un

Cliente VPN (en software) o definiendo políticas IPSec en el sistema operativo, Cuando se genera tráfico interesante, es decir, que está dentro de lo especificado en el Cliente VPN o la política IPSec del S.O., entonces el cliente VPN iniciará el proceso de negociación IKE Fase 1, como se indica en el siguiente paso.

PASO 2: IKE Fase 1

El propósito básico de IKE Fase 1 es autenticar a los pares IPSec y establecer un canal seguro entre ellos para habilitar los intercambios IKE. En resumen, IKE Fase 1 realiza las siguientes funciones:

- Autentica y protege la identidad de los pares IPSec.
- Negocia entre los pares una política IKE que coincida, para proteger el intercambio IKE.
- Realiza un intercambio Diffie-Hellman autenticado con la finalidad de tener llaves secretas compartidas.
- Establece un túnel seguro para negociar los parámetros IKE Fase 2.

La Fase 1 ocurre en dos modos:

- ***Main Mode* o Modo Principal:** El modo principal tiene tres intercambios de dos vías entre el emisor y el receptor.
  - Primer Intercambio: Se ponen de acuerdo en el algoritmo y "hashes" a ser usados para asegurar las comunicaciones IKE.

- Segundo Intercambio: Usa un intercambio Diffie-Hellman para generar las llaves secretas compartidas o pasar los "nonces" (números aleatorios enviados a la otra parte, que luego son firmados y devueltos para comprobar su identidad).

  Tercer intercambio: Verifica la identidad de la otra parte. El valor de identidad puede ser la dirección IP de la contraparte IPSec en formato cifrado. La contribución principal del Modo Principal es la de hacer coincidir las SAs IKE entre los pares, para proporcionar una tubería protegida para los intercambios IKE subsiguientes. La SA IKE especifica los siguientes parámetros para el intercambio IKE: método de autenticación a ser usado, algoritmos de cifrado y hash, el grupo Diffie-Hellman a ser usado, el tiempo de vida de la asociación de seguridad IKE en segundos o kilobytes, y los valores de la llave secreta compartida para los algoritmos de cifrado. La asociación de seguridad IKE es bidireccional.

- **Modo Agresivo:** En el Modo Agresivo, se realizan menos intercambios que en el Modo Principal. En el primer intercambio, casi todo es comprimido en los valores de SA IKE propuestos: la llave Diffie-Hellman pública, un "nonce" que es firmado por la parte que lo origina, y la identidad del paquete, que puede ser usada para verificar la identidad a través de un tercero. El receptor envía de regreso todo lo que se necesita para completar el intercambio. La única cosa que se deja para el emisor es confirmar el intercambio. La debilidad de usar el Modo Agresivo es que ambas partes intercambian información antes de que haya un canal seguro. Por lo tanto, es posible

husmear el medio y descubrir quién creó la nueva SA. Sin embargo, es más rápido que el modo principal.

PASO 3: IKE Fase 2

El propósito de IKE Fase 2 es negociar las SAs IPSec para establecer el túnel IPSec. IKE Fase 2 realiza las siguientes funciones:

- Negocia los parámetros de las SAs IPSec protegidos por una SA IKE existente.
- Establece una Asociación de Seguridad (SA) IPSec.
- Periódicamente renegocia las SAs IPSec para garantizar la seguridad.
- Opcionalmente, realiza un intercambio Diffie-Hellman adicional.

IKE Fase 2 tiene un solo modo, llamado *Quick Mode* o Modo Rápido. Éste ocurre una vez que IKE ha establecido el túnel seguro en la fase 1. Negocia una política IPSec compartida, obtiene el material criptográfico de llave secreta compartida usado por los algoritmos de seguridad IPSec, y establece SAs IPSec. El Modo Rápido intercambia "nonces" que proporcionan protección *anti-replay*. Los "nonces" son usados para generar nuevo material de llave secreta compartida y previene que ataques de *playback* generen SAs falsos. El Modo Rápido es también usado para renegociar una nueva SA IPSec cuando el tiempo de vida de la SA IPSec ha expirado.

Si PFS (*Perfect Forward Secrecy*) es especificado en una política de seguridad IPSec, un nuevo intercambio Diffie-Hellman se produce con cada Modo Rápido IPSec (*Quick*

Mode), proporcionando material criptográfico para llaves con mayor entropía y, por lo tanto, mayor resistencia ante ataques criptográficos. Cada intercambio Diffie-Hellman requiere largas operaciones de exponenciación, lo que incrementa el uso del CPU y disminuye el desempeño.

PASO 4: Túnel Cifrado IPSec

Una vez que la Fase 2 de IKE está completa y el Modo Rápido ha establecido las SAs IPSec, la información es intercambiada a través del túnel IPSec. Los paquetes son cifrados y descifrados usando el cifrado especificado en la SA IPSec. El túnel se establece y la información de asociaciones de seguridad IPsec es almacenada en la base de datos de SAs en ambos pares. Negociaciones posteriores toman lugar según los parámetros negociados durante la fase 2.

PASO 5: Finalización del Túnel

Las SAs IPSec terminan cuando son borradas o cuando se agota su tiempo de vida. El tiempo de vida de una SA llega a su fin cuando un número especificado de segundos transcurre o cuando un número especificado de bytes ha pasado a través del túnel. Cuando las SAs terminan, las llaves son también descartadas. Si las SAs IPSec son aún necesarias para el flujo de tráfico, IKE realizará una nueva negociación de fase 2 y, si fuera necesario, una nueva negociación de fase 1. Una negociación es exitosa cuando se crean nuevas SAs y nuevas llaves. También se puede especificar que se establezcan

nuevas SAs antes que las existentes expiren, de tal manera que el flujo de tráfico continúe de manera ininterrumpida.

9.9. CRIPTOGRAFÍA DE LLAVE SECRETA PRE-COMPARTIDA

Es un sistema en el que dos partes comparten el mismo valor secreto. Éste es usado tanto para cifrar como descifrar la información antes de enviarla o leerla. Cualquiera que sepa la llave secreta podrá cifrar y descifrar la información (Ver figura 9.9). El algoritmo de Llave Secreta Pre-Compartida es eficiente para grandes volúmenes de información. El problema con este sistema se presenta al momento de transferir el conocimiento de la llave secreta entre todas las partes involucradas, manteniéndola secreta al mismo tiempo. Este problema fue resuelto con el desarrollo de sistemas de pares de llaves asimétricas.

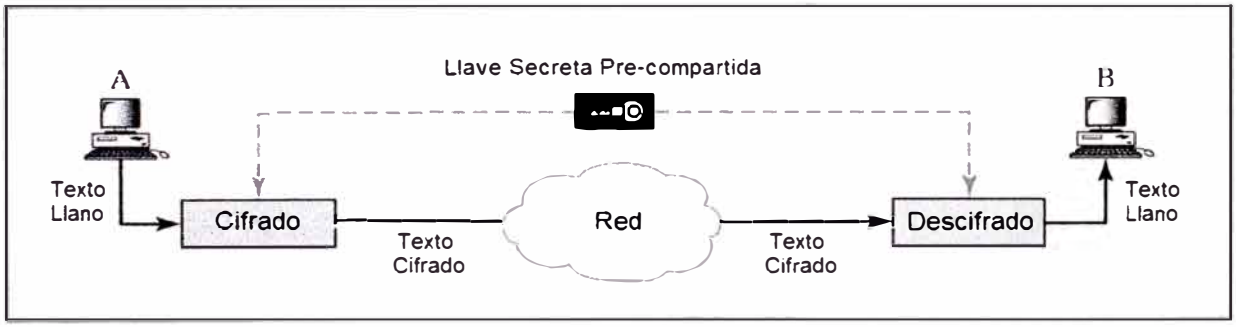

FIGURA 9.9 - Criptografía de Llave Secreta Pre-compartida

9.10. CRIPTOGRAFÍA DE LLAVE PÚBLICA (*PKI: Public Key Infrastructure*)

Este sistema, también llamado Infraestructura de Llave Pública o Criptografía de Llave Asimétrica, usa un par de llaves relacionadas entre sí pero distintas. Una de las llaves, la Llave Privada, está asociada con un sistema o entidad específica y es mantenida en secreto. La otra llave es la Llave Pública y puede ser distribuida libremente por canales de comunicación no seguros. Estas llaves están relacionadas matemáticamente, de tal manera que la información cifrada con la llave pública solo puede ser descifrada con la llave privada (Ver figura 9.10). Debe existir, sin embargo, la seguridad de que una llave pública en particular sea la llave pública real de la entidad con la cual uno se va a comunicar. Esto es hecho al distribuir llaves públicas en la forma de Certificados Digitales, también llamados de Certificados de Seguridad o de Llave Pública. El algoritmo de Llave Pública es más eficiente para pequeños volúmenes de información.

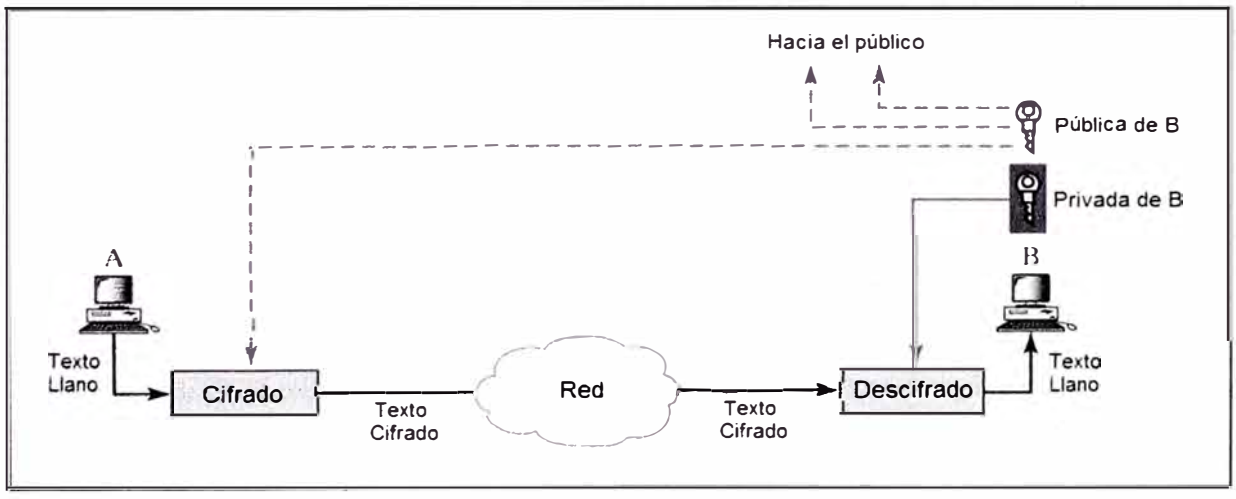

FIGURA 9.10 – Criptografía de Llave Pública (PKI)

9.11. CERTIFICADOS DIGITALES Y AUTORIDADES CERTIFICADORAS (CA)

Un certificado digital o de seguridad asocia una llave pública con una persona, dispositivo u otra entidad en particular. El certificado es expedido por una entidad, en la cual los usuarios han puesto su confianza, llamada Autoridad Certificadora (CA: *Certificate Authority*) quien garantiza la identidad del portador de la llave privada correspondiente. La CA firma digitalmente el certificado con su llave privada, de tal manera que puede ser verificado usando la llave pública de la CA.

El Certificado Digital es un paquete que contiene información acerca de la identidad del portador del certificado: su nombre o dirección IP, el número de serie del certificado, fecha de expiración del certificado y una copia de la llave pública del portador del certificado. El formato estándar del certificado digital está definido en la especificación X.509 versión 3 de la ISO (*International Organization for Standarization*) u Organización Internacional para la Estandarización.

La distribución de llaves o certificados en un medio no confiable y cuyo control es cuestionable (como Internet, por ejemplo), justifica la existencia de las Autoridades Certificadoras. Éstas son organizaciones confiables que proporcionan certificados digitales. Entre ellas tenemos a Verisign, Entrust y Netscape. Un cliente se registra con una autoridad certificadora; una vez que la CA verifica las credenciales del cliente, se emite un certificado.

Los certificados tienen un tiempo de vida específico, definido por una fecha y hora de inicio, y una fecha y hora de expiración. Sin embargo, pueden darse situaciones en las que la confidencialidad de una llave haya sido comprometida, y que necesiten la revocación del certificado. En este caso, la Autoridad Certificadora podrá revocar el certificado. Esto es llevado a cabo incluyendo el número de serie del certificado en una lista de revocación de certificados (CRL: *Certificate Revocation List*) actualizada y publicada regularmente por la CA y accesible a los usuarios de certificados.

En la figura 9.11 se muestra un ejemplo de VPN usando Certificados Digitales. En dicho ejemplo, el origen A genera tráfico destinado para B, el cual es pasado hacia el ruteador. El ruteador en A compara el tráfico contra sus políticas de seguridad y determina que el tráfico debe ser cifrado y enviado hacia el ruteador en B, que es el punto terminal VPN. El ruteador A chequea si existe una SA IPSec hacia el ruteador B. Si no la hay, inicia la negociación de una SA IKE. Como parte de la negociación, ambos ruteadores intercambian certificados digitales que han sido firmados por una Autoridad Certificadora (CA) en la que ambos confían. Cuando reciben el certificado de la otra parte, cada ruteador descarga una lista de revocación de certificados (CRL) ya sea del CA o de un punto de distribución de CRLs, y verifica que el certificado de la otra parte no haya sido revocado. Tras verificar los certificados, las partes completan la negociación de la SA IKE, seguida de la negociación de la SA IPSec. La información es transferida entre el origen A y el destino B tan pronto como el túnel VPN haya sido creado.

La ventaja de emplear una CA es que las partes o *peers* ya no tienen que intercambiar manualmente llaves pre-compartidas o "nonces". Cuando dos *peers* inician la negociación IKE, intercambian llaves públicas las cuales son luego autenticadas por la CA. Este proceso mejora enormemente la administración pues no hay la necesidad de mantener llaves para cada juego de *peers*. Por tanto, esta solución es fácilmente escalable.

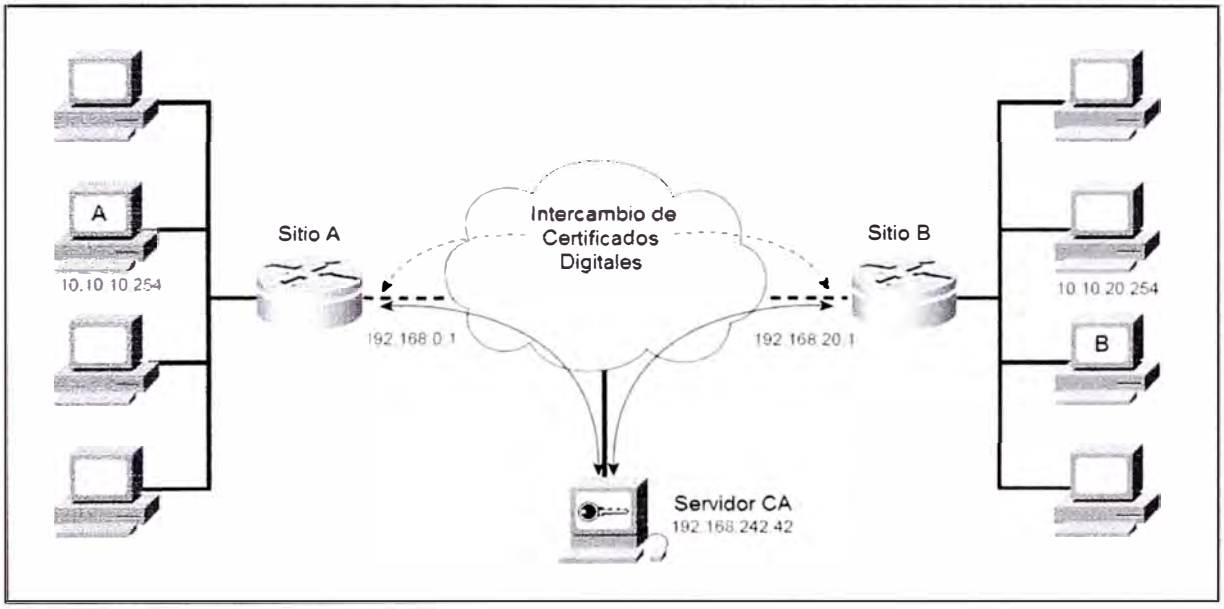

FIGURA 9.11 – VPN usando Certificados Digitales

9.12. FIRMAS DIGITALES

Una firma digital es una firma electrónica que puede ser usada para autenticar la identidad de un emisor o del firmante de un documento. También puede ser usada para asegurarse que el contenido original de un mensaje o documento que ha sido

transmitido esté intacto. En general, el emisor usa su llave privada para crear una firma digital, y la envía junto con la información. El receptor usa la llave pública del emisor y la información para verificar la firma digital.

Existen diferentes métodos para generar y verificar una firma digital. En uno de ellos el emisor genera, a partir de la información o mensaje, un valor de *hash* de un solo sentido (*message digest*). Luego lo cifra usando su llave privada y obtiene la firma digital. Seguidamente envía el mensaje junto con la firma digital. El destinatario usa la llave pública del emisor para descifrar la firma digital, obteniendo el valor de hash (*message digest*). A la vez, genera su propio valor de *hash* de un solo sentido, a partir del mensaje recibido. Finalmente compara ambos valores. Este proceso se puede apreciar en la figura 9.12.

En otro método, el emisor usa su llave privada y la información como entrada para un algoritmo de *hash* que genera la firma digital. El receptor usa la información, la llave pública del emisor, y la firma digital como entrada del algoritmo de verificación que chequea la firma digital.

Una diferencia entre una firma digital y un valor de *hash* de llave simétrica es que sólo el portador de la llave privada puede generar la firma digital, mientras que cualquiera de los portadores de una llave simétrica puede generar el valor de *hash* de llave simétrica.

Por lo tanto, una firma digital proporciona no repudiación haciendo difícil que el emisor niegue haber enviado un mensaje.

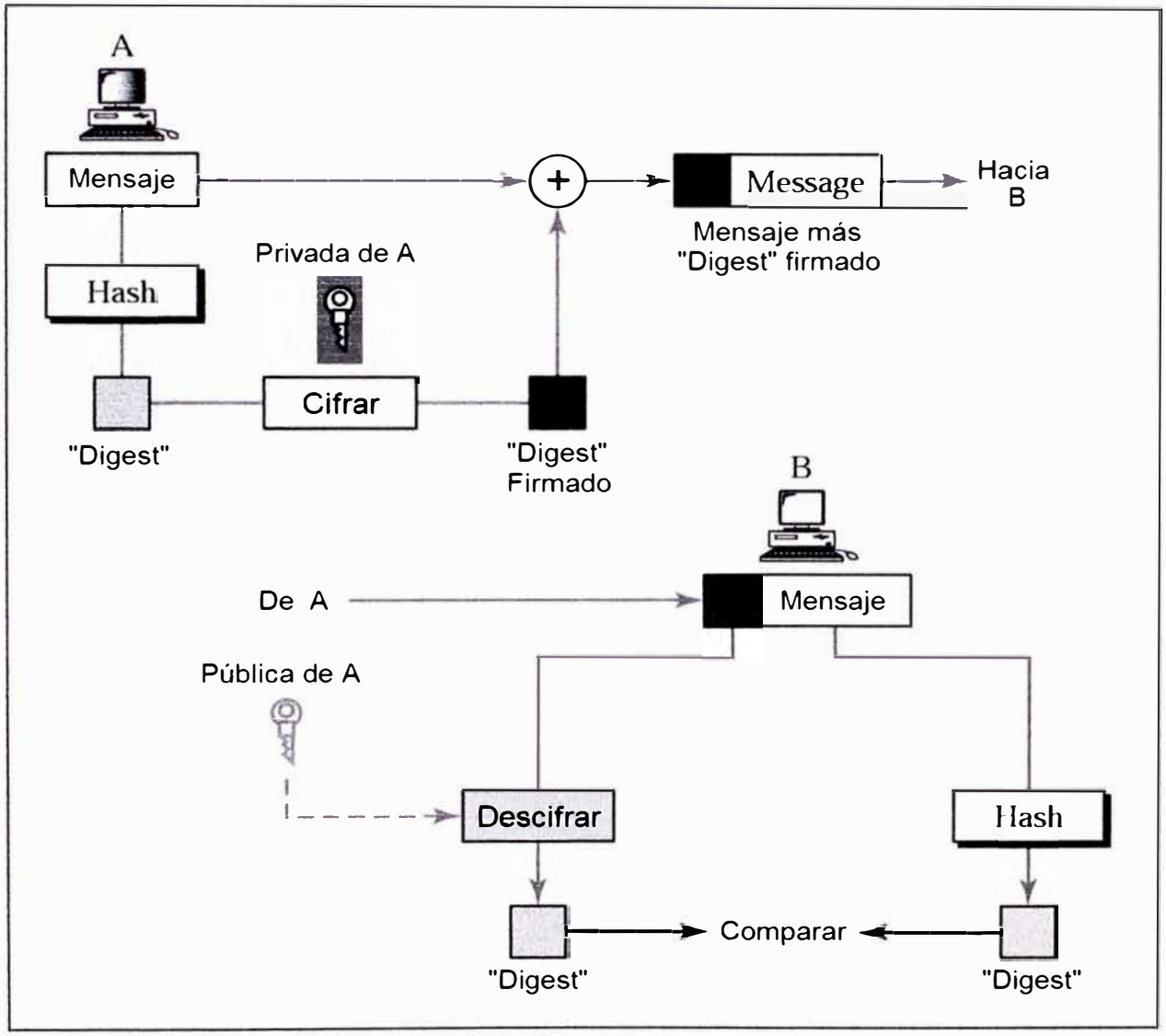

FIGURA 9.12 - Método para generar y verificar una Firma Digital

CAPÍTULO X

DISEÑOS DE SEGURIDAD EN REDES

CAPITULO X

DISEÑOS DE SEGURIDAD EN REDES

El propósito de este capítulo es el de proporcionar los lineamientos necesarios para el diseño e implementación de redes seguras. Entre los diseños de seguridad tratados, tenemos aquellos para redes pequeñas y medianas, tanto para datos como para telefonía IP, así como diseños de seguridad para soportar usuarios wireless y usuarios remotos.

La estrategia mostrada en cada uno de estos diseños ha sido desarrollada por Cisco Systems® y posee un enfoque modular que permite la creación de soluciones escalables y replicables a lo largo de toda una organización.

10.1. DISEÑO DE SEGURIDAD PARA REDES PEQUEÑAS

Las redes pequeñas comprenden los módulos de Internet Corporativo y de Campus. Los dispositivos y mecanismos de defensa usados en cada módulo, así como sus funciones y las amenazas que mitigan se detallan a continuación. En las figuras 10.1 y 10.2 se muestran diseños de seguridad para una red pequeña típica.

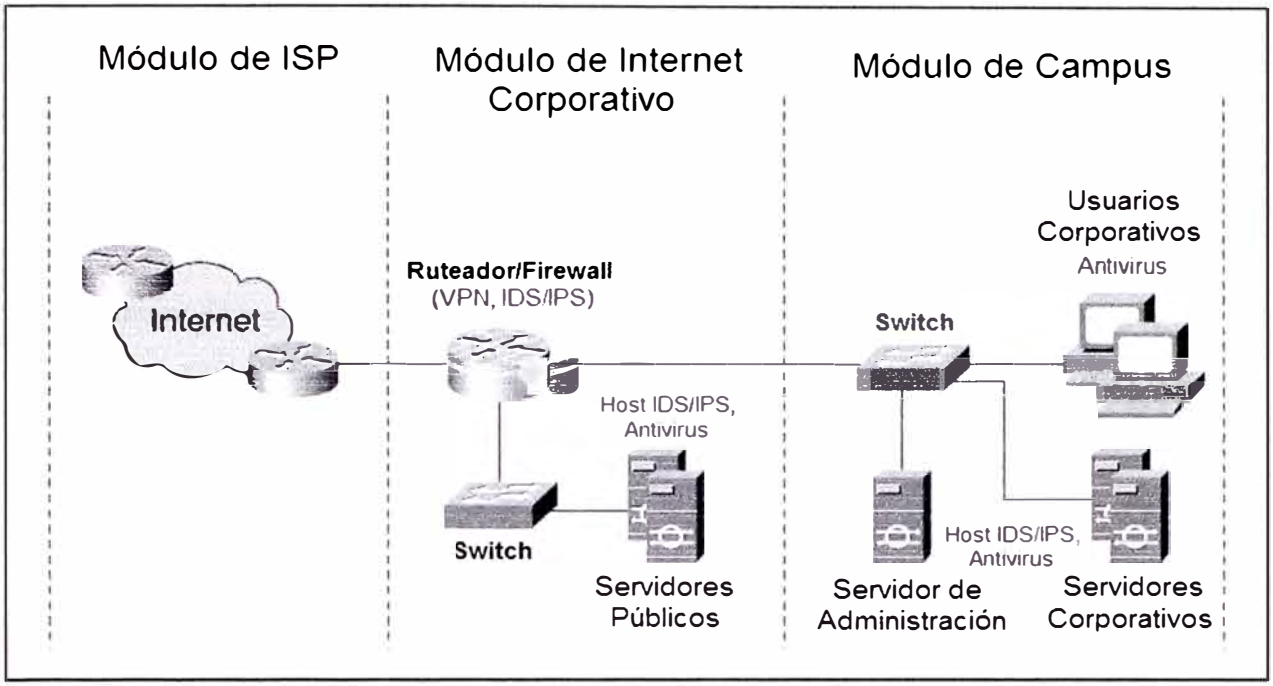

FIGURA 10.1 – Diseño de Seguridad para Redes Pequeñas – Ruteador/Firewall

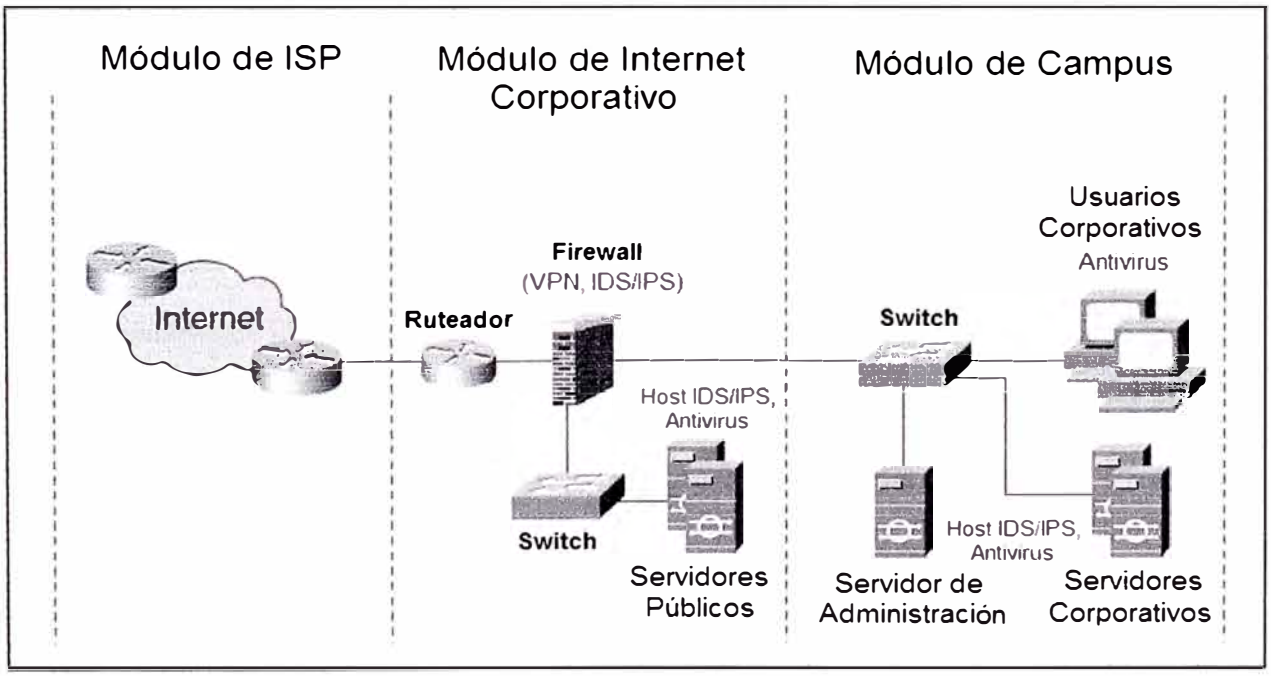

FIGURA 10.2 – Diseño de Seguridad para Redes Pequeñas – Firewall separado

MÓDULO DE INTERNET CORPORATIVO PARA REDES PEQUEÑAS

Proporciona a los usuarios internos conectividad hacia servicios de Internet y proporciona a usuarios de Internet acceso a información en los servidores públicos corporativos. Este módulo también proporciona acceso a ubicaciones remotas, teletrabajadores y usuarios viajeros a través del uso de conectividad VPN.

Distintos dispositivos conforman el módulo de Internet Corporativo, entre ellos:

- Servidor de Correo: Actúa como intermediario entre Internet y los servidores de correo de la Intranet, y escanea en busca de ataques basados en correos.
- Servidor DNS (*Domain Name System*): Sirve como servidor DNS autoritativo externo y transmite los requerimientos internos para resolución de nombres de dominio hacia Internet.
- Servidor Web/FTP: Proporciona información al público acerca de la organización
- Ruteador/Firewall: Proporcionan protección de recursos a nivel de red, filtrado de tráfico, inspección de estados, terminación de túneles VPN para sitios y/o usuarios remotos, e incluso cierto nivel de detección o prevención de intrusos (IDS/IPS).
- Switch Capa 2: Se asegura que la información de los dispositivos administrados conectados (servidores), llegue directamente al Firewall o Ruteador. Proporciona soporte de VLANs y VLANs privadas.

Mitigación de Amenazas en Módulo de Internet Corporativo para Redes Pequeñas

Los servidores públicos son los más propensos a sufrir ataques. Las siguientes son las amenazas esperadas:

- ☑ Acceso No Autorizado: Mitigado mediante el filtrado en el firewall y/o ruteador.
- ☑ Ataques en la Capa de Aplicación: Mitigados mediante Host IDS/IPSs en los servidores públicos.
- ☑ Ataques de Virus y Caballos de Troya: Mitigados mediante software antivirus a nivel de host.
- ☑ Ataques de Contraseñas: Existen limitados servicios vulnerables a ataques de contraseñas. Los Sistemas Operativos y Host IDS/IPSs pueden detectar la amenaza.
- ☑ Ataques de Denegación de Servicios: Mitigados al limitar la tasa de tráfico mediante CAR (*Committed Access Rate* o Tasa de Acceso Comprometida) en el ruteador de borde del ISP, e implementar control de los parámetros TCP en el firewall y/o ruteador (lado cliente) para limitar la exposición.
- ☑ IP *Spoofing* o Impostación de direcciones IP: Mitigado mediante filtrado según RFC 2827 y RFC 1918 en el ruteador de borde de lado del ISP y en el firewall y/o ruteador del lado cliente.
- ☑ *Sniffers* de paquetes: Implementar una infraestructura LAN basada en switches (pudiendo agregar VLANs), y usar Host IDS/IPSs para limitar la exposición.

- ☑ Reconocimiento de Red: Los Host IDS/IPSs pueden detectar la actividad de reconocimiento. Se recomienda hacer filtrado de protocolos y servicios para limitar su efectividad.
- ☑ Ataques de Explotación de Confianza: Aplicar un modelo de confianza restrictivo y VLANs privadas ayuda a mitigarlos.
- ☑ Redirección de Puertos: Se recomienda usar filtrado restrictivo y Host IDS/IPSs para limitar estos ataques.

MÓDULO DE CAMPUS PARA REDES PEQUEÑAS

El módulo de campus comprende las estaciones de trabajo de los usuarios, los servidores de la Intranet corporativos, los servidores de administración, y la infraestructura de Capa 2 asociada y requerida para la interconexión de los dispositivos. En el diseño de una red pequeña, esta funcionalidad de Capa 2 ha sido combinada en un solo switch.

A continuación los principales dispositivos que conforman este módulo:

- Switch de Capa 2 (con soporte para VLANs y VLANs privadas): Proporciona servicios de Capa 2 a los dispositivos de red cableados.
- Servidores Corporativos: Proporcionan servicios de correo electrónico (SMTP y POP3) a los usuarios internos, así como servicios de archivo, impresión y DNS a las estaciones de trabajo.

- Estaciones de Trabajo de Usuario: Proporcionan servicios de datos a usuarios autorizados en la red.
- Servidor de Administración: Facilita la administración de las configuraciones en general. Proporciona servicios Syslog para reportes, y servicios TACACS+ y/o RADIUS para autenticación, autorización y contabilidad.

Mitigación de Amenazas en el Módulo de Campus para Redes Pequeñas:

- ☑ Sniffers de Paquetes: Una estructura basada en switches limita su efectividad.
- ☑ Virus y Caballos de Troya: El empleo y actualización de Antivirus en los hosts, permite detectar y eliminar la mayoría de virus y caballos de Troya.
- ☑ Acceso No Autorizado: Este tipo de acceso es mitigado mediante el uso de Host IDS/IPSs y control de acceso para las aplicaciones.
- ☑ Ataques en la Capa de Aplicación: Los sistemas operativos, los dispositivos, y las aplicaciones deben ser mantenidos al día con los últimos parches o actualizaciones de seguridad. Los Host IDS/IPSs contribuyen a la protección.
- ☑ Ataques de Explotación de Confianza: Las VLANs privadas evitan que los hosts en la misma subred se comuniquen entre sí a menos que lo contrario haya sido especificado.
- ☑ Redirección de Puertos: Los Host IDS/IPSs evitan que se instalen programas agentes que realizan redirección de puertos.

Alternativas de Diseño para Redes Pequeñas

Cualquier desviación de este diseño estará enfocada principalmente en incrementar la capacidad de la red, y separar las funciones de seguridad en distintos dispositivos. Un ejemplo de esto es la figura 10.2 en la que se muestra un diseño de red con la función de firewall separada del ruteador, en un dispositivo aparte que a la vez tiene capacidad de IDS/IPS y concentrador VPN.

10.2. DISEÑO DE SEGURIDAD PARA REDES MEDIANAS

El diseño de seguridad para una Red Mediana comprende tres módulos: Internet Corporativo, Módulo Campus y Módulo WAN. La red mediana se construye sobre la base del diseño de red pequeña, aumentando su complejidad. Se han separado, y en algunos casos, ampliado las funciones provistas en cada módulo. La figura 10.3 muestra un diagrama de una red mediana típica.

MÓDULO DE INTERNET CORPORATIVO PARA REDES MEDIANAS

Proporciona a los usuarios internos conectividad hacia servicios de Internet, mientras que proporciona a usuarios de Internet acceso a información en los servidores públicos corporativos. Este módulo también proporciona acceso a ubicaciones remotas, teletrabajadores y usuarios viajeros a través del uso de conectividad VPN, y adicionalmente concentra tráfico de usuarios conmutados (*dial-up*) tradicionales.

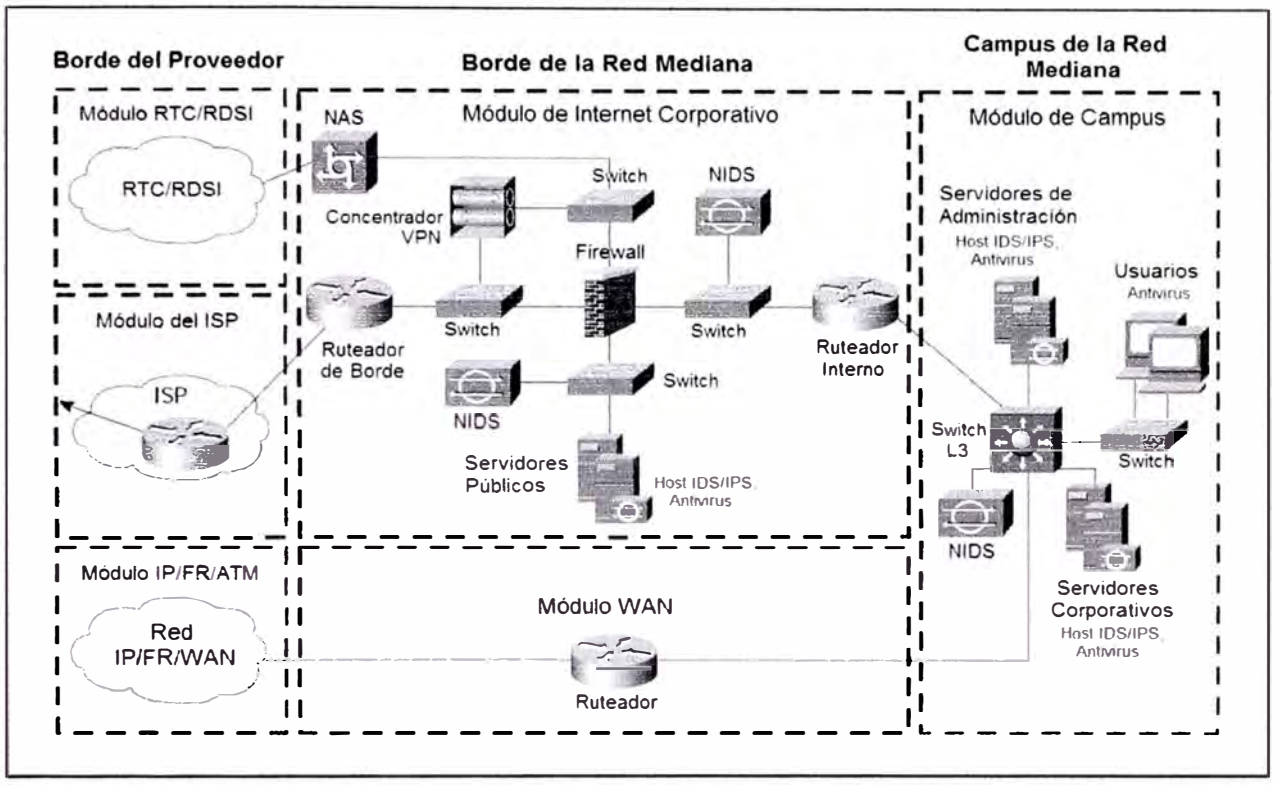

FIGURA 10.3 – Diseño de Seguridad para Redes Medianas

Tomando como base el módulo de Internet para una red pequeña, se han separado y agregado funciones mediante la adición de dispositivos VPN específicos para la terminación del acceso de usuarios remotos, la colocación de sensores NIDS en segmentos clave del módulo, y la facilidad para acceso de usuarios remotos a través de la Red Telefónica Conmutada (RTC) o la Red Digital de Servicios Integrados (RDSI).

A continuación una relación de dispositivos que se pueden encontrar en el módulo de Internet Corporativo de una red mediana:

- Servidor de Acceso Remoto (RAS: *Remote Access Server* o NAS: *Network Access Server*): Concentra las conexiones analógicas y puede autenticar individualmente a los usuarios remotos.
- Servidor DNS (*Domain Name System*): Sirve como servidor DNS autoritativo externo y transmite los requerimientos internos para resolución de nombres de dominio hacia Internet.
- Ruteador de Borde: Proporciona filtrado básico y conectividad en Capa 3 hacia Internet.
- Ruteador Interno: Proporciona separación a nivel de Capa 3 y encaminamiento o "ruteo" entre los módulos de Internet Corporativo y Campus.
- Servidor Web/FTP: Proporciona información al público acerca de la organización
- Firewall: Protege los recursos a nivel de la capa de red, proporciona filtrado de tráfico con inspección de estados, seguridad granular en el acceso de usuarios remotos, conectividad VPN para usuarios remotos, y autenticación de sitios remotos confiables.
- Switch Capa 2: Proporciona conectividad a nivel de Capa 2, con soporte para VLANs y VLANs privadas.
- Network IDS: Proporciona monitoreo de tráfico desde la Capa 4 hasta la Capa 7, en segmentos de red clave dentro del módulo.
- Servidor de Correo: Actúa como intermediario entre Internet y los servidores de correo de la Intranet, y escanea en busca de ataques basados en correos.

- Concentrador VPN: Autentica individualmente a usuarios remotos y finaliza los túneles IPSec.

Mitigación de Amenazas en Módulo de Internet Corporativo para Redes Medianas

El punto más probable de ataque dentro del módulo de Internet Corporativo está en el segmento de servicios públicos, es decir, donde se encuentran los servidores de acceso publico. Los servicios VPN también son vulnerables a ataques. A continuación una relación de las amenazas que se pueden presentar en este módulo:

- ☑ Ataques en la Capa de Aplicación: Mitigados usando Host IDS/IPSs y Network IDS/IPSs
- ☑ Ataques de Denegación de Servicios: Limitar la tasa de tráfico mediante CAR (*Committed Access Rate* o Tasa de Acceso Comprometida) en el ruteador de borde del ISP, e implementar control de los parámetros TCP en el firewal y/o ruteador (lado cliente) para limitar la exposición.
- ☑ IP *Spoofing* o Impostación de direcciones IP: Mitagado mediante filtrado según RFC 2827 y RFC 1918 en el ruteador de borde de lado del ISP y en el firewall y/o ruteador del lado cliente.
- ☑ Sniffers de paquetes: Implementar una infraestructura LAN basada en switches (pudiendo agregar VLANs), y usar Host IDS/IPSs para limitar la exposición.
- ☑ Reconocimiento de Red: Mitigado usando IDS/IPSs y haciendo filtrado de protocolos/servicios para limitar la efectividad.

- ☑ Ataques de Explotación de Confianza: Aplicar un modelo de confianza restrictivo y VLANs privadas para mitigarlos.
- ☑ Redirección de Puertos: Filtrado restrictivo y host IDS/IPSs para limitar los ataques.
- ☑ Ataques de Contraseñas: Mitigados usando contraseñas válidas sólo una vez (OTP: *One Time Passwords*).
- ☑ Acceso No Autorizado: Mitigado usando filtrado en el ISP, ruteador de borde y firewall corporativos, bloqueando el tráfico en puertos no autorizados.
- ☑ Ataques de Virus y Caballos de Troya: Mitigados usando Host IDS/IPSs, antivirus a nivel de host, filtrado de contenido a nivel de correos.
- ☑ Ataques de Hombre en el Medio: Mitigados mediante el cifrado del tráfico remoto.
- ☑ Descubrimiento de la Topología de Red: Mitigado mediante el uso de Listas de Control de Acceso en el ruteador de ingreso para limitar el acceso al concentrador VPN y al firewall.

Alternativas de Diseño en Módulo de Internet Corporativo para Redes Medianas

- El filtrado básico en el ruteador de borde puede ser reemplazado con la funcionalidad avanzada de un ruteador con características de firewall de inspección de estados. Esto refuerza la seguridad en el módulo.
- Un *Network* IDS podría ser colocado en la parte externa del firewall, para que monitoree y alerte ante ataques antes de que pasen a través del firewall. Los

parámetros de este NIDS deben ser configurados cuidadosamente por el alto número de alarmas que podrían generarse.

- El ruteador interno, colocado entre el firewall y el módulo de Campus, podría ser removido. La funcionalidad de capa 3 provista por este ruteador podría ser ofrecida por un Switch Capa 3 dentro del módulo de Campus.
- Se puede agregar alguna forma de filtrado de contenidos, tal como filtrado de URLs (*Uniform Resource Locator*) o de direcciones de páginas en Internet. Un ejemplo de esto es el empleo de dispositivos conocidos como *Proxy Caches*, que permiten almacenar las páginas recientemente accedidas para acelerar la navegación ante accesos posteriores. A estos dispositivos se les agrega, adicionalmente, funcionalidades de filtrado de URLs mediante el uso de Websense, un software que permite bloquear accesos a páginas web que pertenecen a alguna categoría pre-configurada que no está de acuerdo con las políticas de la organización. Dentro de estas categorías tenemos páginas de violencia, pornografía, *hacking*, páginas que contienen virus o espías, entre otros.

MÓDULO DE CAMPUS PARA REDES MEDIANAS

El módulo de campus en redes medianas comprende: las estaciones de trabajo de los usuarios, los servidores de la Intranet corporativos, los servidores de administración, y la infraestructura de Capa 2 y Capa 3 asociada y requerida para la interconexión de los dispositivos. El módulo de Campus para redes medianas se construye sobre la base del

diseño para redes pequeñas. Los nuevos dispositivos que aparecen en este módulo son Switches Capa 3, y Sensores NIDS.

A continuación la relación de dispositivos que conforman el módulo de Campus:

- Servidores de Autenticación: Proporcionan servicios de autenticación a los dispositivos de red que reciben las solicitudes, y autentican a los usuarios mediante, por ejemplo, esquemas de contraseñas válidas una sola vez.
- Servidores Corporativos: Proporcionan servicios de correo electrónico (SMTP y POP3) a los usuarios internos, así como servicios de archivo, impresión y DNS a las estaciones de trabajo.
- Switch Capa 2: Proporciona conectividad a nivel de Capa 2 y soporte de VLANs y VLANs privadas.
- Switch Capa 3: Encamina y conmuta el tráfico de producción y de administración dentro del módulo. Proporciona servicios de la capa de distribución a otros switches, y servicios avanzados tales como filtrado de tráfico, comunicaciones inter-VLAN, etc.
- Network IDS: Proporciona monitoreo de tráfico desde la Capa 4 hasta la Capa 7, en segmentos de red clave dentro del módulo.
- Host NIDS: Proporciona servicios de recolección de las alarmas de todos los NIDS en la red.

- Host de Administración SNMP: Proporciona administración SNMP para dispositivos.
- Servidor Syslog: Recolecta información de registros y eventos, proveniente de firewalls y Host NIDS.
- Servidor de Administración de Sistemas: Proporciona servicios de configuración, actualización de contenido y software para los dispositivos.
- Estaciones de Trabajo de Usuarios: Proporcionan servicios de datos a usuarios autorizados en la red.

Mitigación de Amenazas en el Módulo de Campus de Redes Medianas

☑ *Sniffers* de Paquetes: Una estructura basada en switches limita su efectividad.

☑ Virus y Caballos de Troya: El empleo y actualización de Antivirus en los hosts, permite detectar y eliminar la mayoría de virus y caballos de Troya.

☑ Acceso No Autorizado: Este tipo de acceso es mitigado mediante el uso de host IDS/IPSs y control de acceso para las aplicaciones.

☑ Ataques en la Capa de Aplicación: Los sistemas operativos, los dispositivos, y las aplicaciones deben ser mantenidos al día con los últimos parches o actualizaciones de seguridad. Los host IDS/IPSs contribuyen a la protección.

☑ Ataques de Explotación de Confianza: Las VLANs privadas evitan que los hosts en la misma subred se comuniquen entre sí, a menos que lo contrario haya sido especificado.

- ☑ Redirección de Puertos: Los host IDS/IPSs evitan que se instalen programas agentes que realizan redirección de puertos.
- ☑ IP *Spoofing* o Impostación de Direcciones IP: Mitigado usando filtrado según se especifica en el RFC 2827.
- ☑ Ataque de Contraseñas: Mitigado usando un servidor de autenticación que implemente autenticación de dos factores para aplicaciones clave.

Alternativas de Diseño en el Módulo de Campus para Redes Medianas

- Si la red es lo suficientemente pequeña, los switches de Acceso (Capa 2) pueden ser removidos. La funcionalidad de Capa 2 sería provista conectando los dispositivos directamente al switch de *Core*.
- El NIDS externo puede ser reemplazado por un módulo IDS, colocado en el Switch de *Core*, lo cual incrementa el desempeño al estar directamente conectado al *backplane* del switch.
- Si el desempeño no es un problema, se puede reemplazar el Switch Capa 3 con un Switch Capa 2 y hacer el Inter-VLAN y el filtrado en un ruteador que podría ser el "Ruteador Interno" del módulo de Internet Corporativo.

MÓDULO WAN PARA REDES MEDIANAS

La inclusión del módulo WAN (*Wide Area Network* o Red de Área Amplia) en el diseño de redes medianas es necesaria si existe un requerimiento de conexión hacia un sitio remoto a través de una red IP, Frame-Relay o ATM.

El diseño de este módulo incluye solo un dispositivo: un ruteador con capacidad de firewall (opcional pero recomendable), que proporcione encaminamiento, control de acceso, filtrado y mecanismos de QoS (Calidad de Servicio) para la comunicación con ubicaciones remotas.

Mitigación de Amenazas en el Módulo WAN

- ☑ IP *Spoofing* o Impostación de Direcciones IP: Mitigado usando filtrado a nivel de Capa 3 en el ruteador.
- ☑ Acceso No Autorizado: Mitigado al implementar control de acceso en el ruteador, reduciendo el número de protocolos a los que las oficinas remotas tienen acceso.

Alternativas de Diseño en el Módulo WAN

- Para proporcionar un nivel adicional de seguridad y privacidad de la información, se pueden usar VPNs con IPSec a través del enlace WAN.

- La capacidad de firewall con inspección de estados es opcional pero muy recomendable en un escenario donde no se pueda garantizar que se apliquen esquemas de seguridad satisfactorios en todos los sitios remotos. Por ejemplo, si una localidad remota contara con un acceso a Internet sin las medidas de seguridad adecuadas, un atacante podría acceder a dicha red. Ahora, si en los módulos WAN de las demás oficinas no existieran mecanismos de seguridad tales como ruteadores con firewalls, éstas podrían, también, ser víctimas de un ataque. Así el módulo WAN se convertiría en una puerta trasera para ataques.

Alternativas de Diseño y Consideraciones para Redes Medianas

- Si se emplea un túnel VPN IPSec para conectarse a la oficina central, se podría prescindir del módulo WAN, teniendo en cuenta que, debido a que Internet es una red de mejor esfuerzo, se perdería la capacidad de priorizar aplicaciones (QoS) y las garantías de tiempos de respuesta que un proveedor WAN podría ofrecer con una red privada.
- Se podría prescindir del módulo de Internet Corporativo en el caso que la oficina central tenga y permita acceso a Internet a las oficinas remotas, y siempre que la oficina local no requiera acceso a Internet local.
- Si la oficina central proporciona servicios de concentración VPN o de acceso remoto conmutado, estas características no serían necesarias en el módulo de Internet Corporativo.

- Los servidores de administración están normalmente situados en la oficina central, lo que significa que el tráfico de administración deberá atravesar ya sea el enlace WAN privado o una conexión VPN IPSec. En este último caso, debido a que algunos dispositivos están localizados en puntos anteriores al punto de terminación del túnel VPN, estos requerirán otro de tipo de administración, ya sea mediante el uso de túneles IPSec separados terminando en cada dispositivo o usando conexiones seguras tales como SSH (*Secure Shell*).

10.3. DISEÑO DE SEGURIDAD PARA REDES DE TELEFONÍA IP

TELEFONÍA IP EN REDES PEQUEÑAS

En este diseño se emplea como base el diseño para redes pequeñas. El módulo de Internet Corporativo se ha modificado para soportar servicios de voz hacia la RTC (Red Telefónica Conmutada) o RDSI (Red Digital de Servicios Integrados) para permitir realizar llamadas locales y para acceso WAN de contingencia. En el módulo de Campus se ha agregado la capacidad de separación de red en dos segmentos, uno de voz y otro de datos, conformando cada uno una VLAN distinta. El administrador de llamadas o central telefónica IP, el servidor *Proxy*, y los teléfonos IP residen en el segmento de voz. Todo el resto de dispositivos incluyendo estaciones de trabajo de los usuarios, servidores de administración y el sistema de correo de voz residen en el segmento de datos.

MÓDULO DE INTERNET PARA REDES PEQUEÑAS CON TELEFONÍA IP

El módulo de Internet Corporativo para telefonía IP en redes pequeñas concentra en un solo equipo una gran variedad de características tales como encaminamiento, servicios inter-VLAN, servicios de voz, NAT o traducción de direcciones, firewall de inspección de estados, e IDS/IPS, brindando protección de los recursos de red y filtrado avanzado. Este equipo es un ruteador con capacidad de firewall y habilitado para manejar voz.

El ruteador regula el acceso entre los segmentos de voz y datos a través de políticas de control de acceso e inspección de estados. Además la funcionalidad de IDS/IPS integrada permitirá alarmar y reaccionar ante actividad que coincida con firmas de ataques. Ver figura 10.4

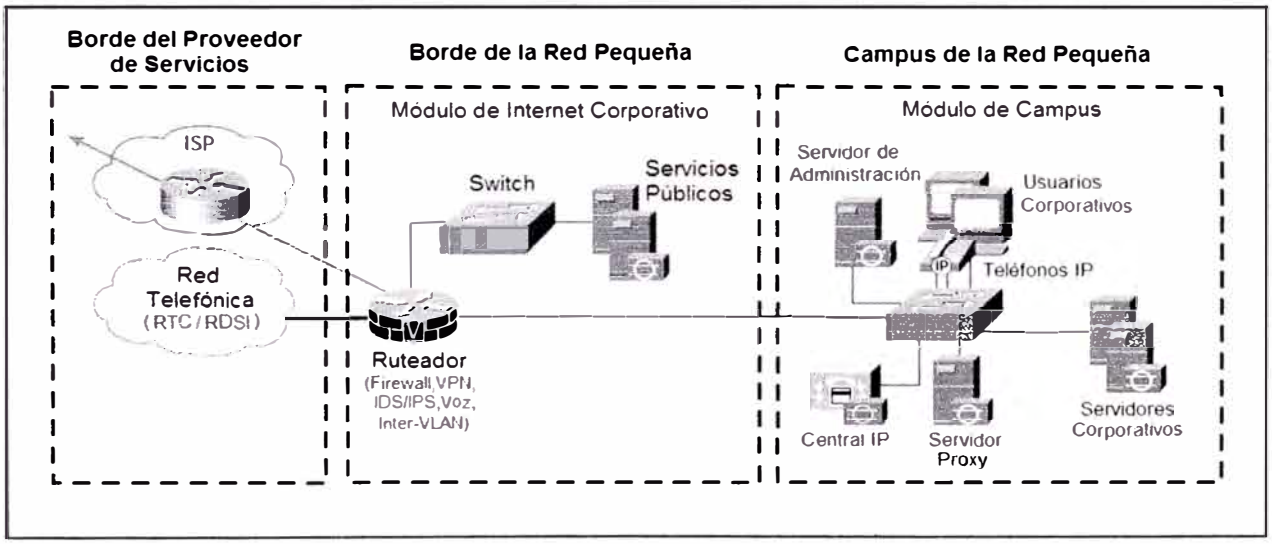

FIGURA 10.4 - Diseño de Seguridad para Telefonía IP en Redes Pequeñas

Mitigación de Amenazas para Voz en el Módulo de Internet Corporativo

- ☑ Acceso No Autorizado: Mitigado mediante filtrado en el firewall.
- ☑ Fraude Telefónico: Control de acceso para limitar que sólo se comuniquen entre sí dispositivos telefónicos conocidos.
- ☑ Ataques de Denegación de Servicios: Configuración de parámetros de control de TCP para limitar la exposición del administrador de llamadas o central telefónica IP. Estas acciones incluyen el limitar el número de sesiones permitidas y el número de sesiones semi-abiertas permitidas (estas últimas son aquellas que no han completado la negociación de tres vías).
- ☑ IP *Spoofing* o Impostación de direcciones IP: Tanto en el ruteador de borde del ISP como en el ruteador local se aplican filtros según las recomendaciones de los RFCs 1918 y 2827.

MODULO DE CAMPUS PARA REDES PEQUEÑAS CON TELEFONÍA IP

El módulo de Campus se ha adaptado para soportar Teléfonos IP basados en hardware y software, servicios *Proxy* y VLANs, todo esto combinado con las estaciones de trabajo de los usuarios, los servidores Intranet y de administración en una infraestructura basada en switches Capa 2.

A continuación la relación de dispositivos adicionados o modificados en el módulo de Campus:

- Switch Capa 2 (con soporte para VLANs): Proporciona servicios de Capa 2 a dispositivos de voz y datos.
- Servidor de Correo de Voz: Proporciona servicios de mensajería de voz a usuarios internos.
- Estaciones de Trabajo de Usuarios: Proporcionan a usuarios autorizados servicios de datos, y servicios de voz a través de teléfonos IP en software.
- Teléfonos IP en hardware: Proporcionan servicios de voz a usuarios de la red.
- Central Telefónica IP o Administrador de Llamadas: Proporciona servicios de voz a teléfonos IP.
- Servidor *Proxy*: Proporciona servicios de datos a teléfonos IP.

Mitigación de Amenazas para Voz en el Módulo de Campus

☑ *Sniffers* de Paquetes/Interceptación de Llamadas: Una infraestructura basada en switches limita su efectividad.

☑ Virus y Caballos de Troya: El empleo y actualización de Antivirus en los hosts, permite detectar y eliminar la mayoría de virus y caballos de Troya.

☑ Acceso No Autorizado: Este tipo de acceso es mitigado mediante el uso de host IDS/IPSs y control de acceso para las aplicaciones.

☑ Ataques en la Capa de Aplicación: Los sistemas operativos, los dispositivos, y las aplicaciones deben ser mantenidos al día con los últimos parches o actualizaciones de seguridad. Los host IDS/IPSs contribuyen a la protección.

- ☑ Ataques de Explotación de Confianza: Aplicar un modelo de relaciones de confianza restrictivas. Las VLANs privadas evitan que los hosts en la misma subred se comuniquen entre sí a menos que lo contrario haya sido especificado.
- ☑ Impostación de la Parte Llamante: Herramientas como *Arpwatch* permiten notificar sobre la existencia de dispositivos desconocidos.
- ☑ Fraude Telefónico: La central telefónica IP o administrador de llamadas no deberá permitir que dispositivos desconocidos reciban configuración.
- ☑ Ataques de Denegación de Servicios: La separación de los segmentos de voz y datos reduce significativamente la probabilidad de un ataque.
- ☑ Repudiación: Los usuarios son autenticados antes de acceder a las funciones del teléfono IP. De esta manera se reduce la probabilidad de que, posteriormente, un usuario pueda negar que una llamada ocurriera.

Alternativas de Diseño para Telefonía IP en Redes Pequeñas

- Se podría considerar pasar el servidor de correo de voz al segmento de voz, sin embargo, es usual que este tenga otros servicios corriendo, tales como correo electrónico y DNS, en cuyo caso debería quedarse en el segmento de datos.
- El ruteador podría hacer las veces de central telefónica IP o administrador de llamadas, siempre y cuando el sistema operativo del mismo, soporte esta funcionalidad adicional, y el número de teléfonos IP en la red esté dentro del rango soportado por el ruteador.

- Si esta red formara parte de una más grande, de tal manera que los servicios de voz estuvieran ubicados en una oficina remota, la configuración del ruteador con firewall sería más compleja para permitir los flujos de tráfico de voz y señalización de voz. Por otro lado, el ruteador necesitaría contar con la capacidad de servir temporalmente como central telefónica IP en caso fallara la comunicación con la central IP remota. Asimismo, habría que considerar el número de teléfonos IP que el ruteador podría soportar en caso se presentara dicha falla.

TELEFONÍA IP EN REDES MEDIANAS

Se emplea como base el diseño para redes medianas. El módulo de Internet Corporativo no sufre modificaciones. El módulo de Campus se ha adaptado para soportar teléfonos IP basados en hardware y software, servicios *Proxy*, VLANs para datos/voz, servicios de voz internos, y servicios de voz hacia la RTC (Red Telefónica Conmutada) o RDSI (Red Digital de Servicios Integrados) para permitir realizar llamadas locales y para acceso WAN de contingencia. Esto se observa en la figura 10.5.

A continuación la relación de dispositivos adicionados o modificados en el módulo de Campus:

- Switch Capa 3: Encamina y conmuta tráfico de datos, voz y administración dentro del módulo de Campus. Proporciona servicios de distribución para los switches de acceso, y soporta servicios avanzados tales como filtrado de tráfico.

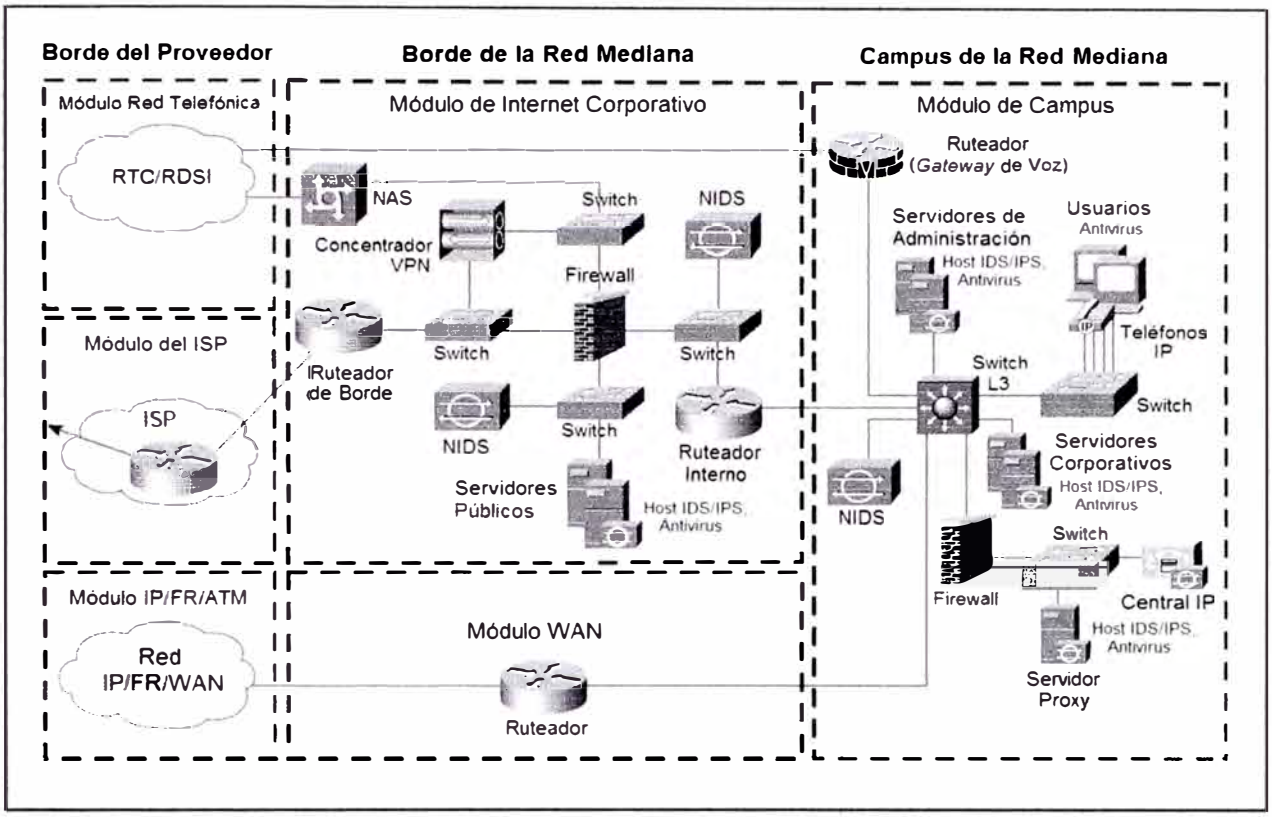

FIGURA 10.5 - Diseño de Seguridad para Telefonía IP en Redes Medianas

- Switch Capa 2 (con soporte para VLANs): Proporciona servicios de Capa 2 a dispositivos de voz y datos.
- Servidor de Correo de Voz: Proporciona servicios de mensajería de voz a usuarios internos.
- Estaciones de Trabajo de Usuarios: Proporcionan, a usuarios autorizados, servicios de datos, y servicios de voz a través de teléfonos IP en software.
- Teléfonos IP en hardware: Proporcionan servicios de voz a usuarios de la red.

- Central Telefónica IP o Administrador de Llamadas: Proporciona servicios de voz a teléfonos IP.
- Servidor *Proxy*: Proporciona servicios de datos a teléfonos IP.
- *Network* IDS: Proporciona monitoreo de tráfico desde la Capa 4 hasta la Capa 7, en segmentos de red clave dentro del módulo.
- Firewall de Inspección de Estados: Proporciona protección a nivel de red para la central telefónica IP o administrador de llamadas. Provee filtrado de tráfico con inspección de estados, mitigación de ataques DoS, y mitigación de impostación de direcciones IP.
- Ruteador para salida (*gateway*) de voz: Proporciona interconexión con las redes telefónicas (RTC/RDSI) para que los usuarios puedan hacer llamadas locales o en general para alcanzar destinos telefónicos fuera de la red (*offnet*).

Mitigación de Amenazas para Voz en Redes Medianas

- ☑ *Sniffers* de Paquetes/Interceptación de Llamadas: Una infraestructura basada en switches limita su efectividad.
- ☑ Virus y Caballos de Troya: El empleo y actualización de Antivirus en los hosts, permite detectar y eliminar la mayoría de virus y caballos de Troya.
- ☑ Acceso No Autorizado: Este tipo de acceso es mitigado mediante el uso de host IDS/IPSs y control de acceso para las aplicaciones.

- ☑ Ataques en la Capa de Aplicación: Los sistemas operativos, los dispositivos, y las aplicaciones deben ser mantenidos al día con los últimos parches o actualizaciones de seguridad. Los host IDS/IPSs contribuyen a la protección.
- ☑ Ataques de Explotación de Confianza: Aplicar un modelo de relaciones de confianza restrictivas. Las VLANs privadas evitan que los hosts en la misma subred se comuniquen entre sí a menos que lo contrario haya sido especificado.
- ☑ Impostación de la Parte Llamante: Herramientas como *Arpwatch* permiten notificar sobre la existencia de dispositivos desconocidos.
- ☑ Fraude Telefónico: La central telefónica IP o administrador de llamadas no deberá permitir que dispositivos desconocidos reciban configuración. Las políticas de control de acceso permitirán que sólo teléfonos IP conocidos se comuniquen entre sí.
- ☑ Ataques de Denegación de Servicios: La separación de los segmentos de voz y datos reduce significativamente la probabilidad de un ataque. La configuración de parámetros de control de TCP limita la exposición del Administrador de llamadas o central telefónica IP. Estas acciones incluyen el limitar el número de sesiones permitidas y el número de sesiones semi-abiertas permitidas (estas últimas son aquellas que no han completado la negociación de tres vías).
- ☑ Repudiación: Los usuarios son autenticados antes de acceder a las funciones del teléfono IP. De esta manera se reduce la probabilidad de que, posteriormente, un usuario pueda negar que una llamada ocurriera. Se registran los eventos de inicio y terminación de llamadas.

☑ IP *Spoofing* o Impostación de direcciones IP: Tanto en el ruteador de borde del ISP y en el firewall local se aplican filtros según las recomendaciones de los RFCs 1918 y 2827.

Alternativas de Diseño para Telefonía IP en Redes Medianas

- Una alternativa sería la implementación de alta disponibilidad para telefonía IP, considerando la adición de un par de firewalls en redundancia y una central telefónica IP o administrador de llamadas adicional.
- Otra opción sería colocar el sistema de correo de voz en un segmento DMZ adicional en el firewall. Esto permitiría proporcionar mitigación de ataques DoS hacia el sistema de correo de voz e inspección de estados entre éste y el servidor de correos en el segmento de datos.
- Si esta red formara parte de una más grande, de tal manera que los servicios de voz estuvieran ubicados en una oficina remota accesible vía el ruteador del Módulo WAN, la configuración en este ruteador y en el switch Capa 3 sería más compleja para permitir los flujos de tráfico de voz y señalización de voz. Por otro lado, ya sea el ruteador que sirve como puerta de enlace (*gateway*) hacia la RTC/RDSI, o en su defecto el ruteador WAN, tendrían que contar con la capacidad de servir temporalmente como central telefónica IP en caso fallara la comunicación con la central IP remota. Asimismo, habría que considerar el número de teléfonos IP que el ruteador mencionado podría soportar en caso se presentara dicha falla.

- Si se cuenta con un Switch Capa 3 modular, podría considerarse el adicionar un módulo de voz para telefonía tradicional (analógica/digital) como reemplazo del Ruteador de salida o *gateway* de voz.

10.4. DISEÑO DE SEGURIDAD PARA REDES WIRELESS

Al igual que en el mundo cableado, en el mundo wireless se puede implementar diferenciación de usuarios usando LANs virtuales inalámbricas (WLANs) asociadas a LANs virtuales cableadas. Se pueden tener escenarios donde cada VLAN soporte un esquema de seguridad específico, implementado usando mixturas de los estándares de seguridad 802.1X/EAP y VPNs IPSec. Cada WLAN es identificada usando un SSID único y es asociada a un identificador de VLAN cableada único. Más aún, los mecanismos de control de acceso a VLANs pueden ser implementados usando un servidor RADIUS. Por ejemplo, un Punto de Acceso (AP) podría asociar dinámicamente a un usuario con un identificador de VLAN devuelto por el servidor RADIUS, tras una autenticación exitosa usando 802.1X/EAP.

Si no se implementan VLANs wireless, se podrían implementar VPNs basadas en IPSec para imponer un esquema de privilegios por usuario o grupo de usuarios. Los usuarios requerirían usar un software cliente VPN en sus máquinas. La red wireless serviría solamente como medio de tránsito, dejando a un concentrador VPN la tarea de administrar los controles de seguridad.

DISEÑO DE SEGURIDAD DE RED WIRELESS CON EAP Y TKIP

Este diseño, mostrado en la figura 10.6, detalla un método genérico para usar EAP con TKIP como mecanismo de seguridad para acceder a la red corporativa.

Los dispositivos empleados en este diseño se detallan a continuación:

- Adaptador Wireless y Software Cliente: Proporcionan el hardware y software necesarios para establecer comunicaciones wireless hacia el Punto de Acceso (AP). Implementa un esquema de autenticación mutua con el AP, mediante algún tipo de autenticación mutua EAP.
- Punto de Acceso Wireless (*Wireless* AP): Vía EAP implementa autenticación mutua para clientes wireless. Puede soportar, en algunos casos, múltiples VLANs para diferenciación de usuarios.
- Switch de Capa 2 o 3 (L2/L3): Proporcionan conectividad Ethernet y filtrado a nivel de Capa 3 y 4 entre las Wireless LANs provenientes del AP y la red corporativa.
- Servidor RADIUS: Implementa autenticación basada en usuario, para clientes wireless a través del AP. Puede ser usado para especificar los parámetros de control de acceso de las VLANs a los usuarios y grupos de usuarios.
- Servidor DHCP: Entrega información de configuración IP a clientes wireless.
- Servidor OTP (Opcional): El servidor OTP (*One-Time Password*) o de contraseñas válidas sólo una vez, autoriza información OTP recibida del servidor RADIUS. Se aplica solo a clientes PEAP (*Protected* EAP).

- Servidor PKI (Opcional): El servidor PKI (*Public Key Infrastructure*) o de Infraestructura de Llave Pública proporciona certificados digitales X.509 v3 para identificación de usuarios y servidores.

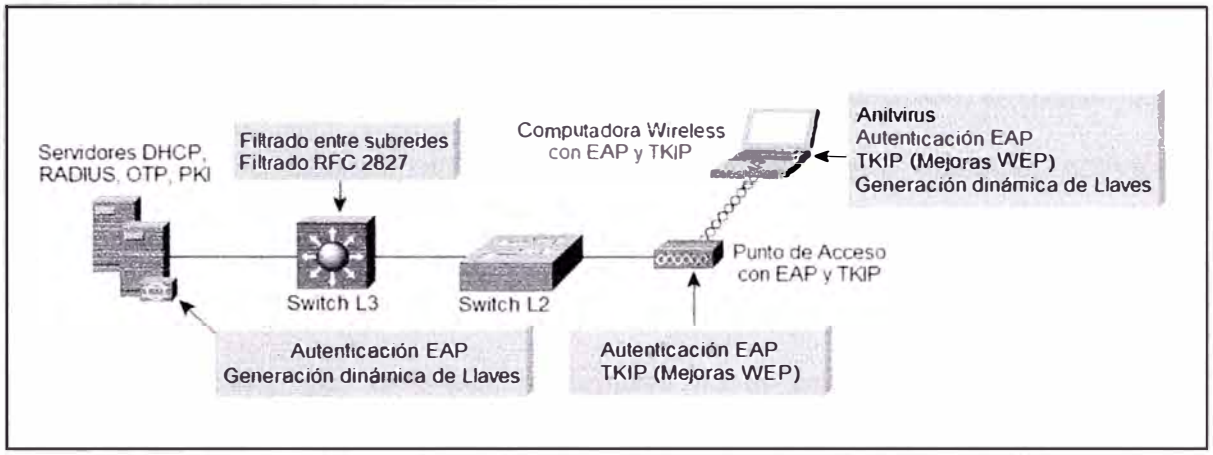

FIGURA 10.6 - Diseño de Seguridad para Redes Wireless con EAP y TKIP

Mitigación de Amenazas en Redes Wireless con EAP y TKIP

- ☑ *Sniffers* de Paquetes Wireless: Estos *sniffers* pueden emplear los mecanismos de ataque WEP conocidos para averiguar la llave de cifrado. Estas amenazas son mitigadas con las mejoras hechas a WEP, específicamente con la capacidad de cambiar las llaves con cada paquete; una característica que forma parte de TKIP.
- ☑ Acceso No Autorizado: Sólo los usuarios autenticados podrán acceder a la red wireless y cableada. Opcionalmente se puede configurar control de acceso en el switch de Capa 3 para limitar el acceso a la parte cableada de la red.

- ☑ Ataques de Hombre en el Medio: La naturaleza de la autenticación mutua de varios tipos de protocolos EAP combinada con el chequeo de integridad de mensaje (MIC) pueden minimizar los ataques bajo los cuales los atacantes buscan colocarse en medio de las comunicaciones wireless.
- ☑ IP *Spoofing* o Impostación de Direcciones IP: Un atacante no podrá realizar IP *spoofing* sin antes autenticarse en la WLAN. Aún autenticado, el filtrado según el RFC 2827 aplicado en el switch capa 3 restringirá cualquier actividad de impostación de direcciones en el segmento de subred local.
- ☑ Ataques ARP (*Address Resolution Protocol*) *Spoofing*: Un atacante no podrán realizar este tipo de ataque si primero no es capaz de autenticarse. Una vez autenticado, los ataques ARP *spoofing* pueden ser ejecutados al igual que se ejecutan en un medio cableado, con el fin de interceptar la información de los usuarios.
- ☑ Descubrimiento de la Topología de Red: Los atacantes no podrán realizar esto si primero no son capaces de autenticarse. Podrán ver que una WLAN existe al observar el SSID del AP, pero no podrán acceder a la red. Una vez autenticados vía EAP, el descubrimiento de topología estándar puede ocurrir de la misma manera que ocurre en una red cableada.

Amenazas No Mitigadas en Redes Wireless con EAP y TKIP

- Ataque de Contraseñas: Varios tipos de EAP toman en cuenta que un atacante puede monitorear pasivamente los intercambios 802.1X/EAP entre el cliente wireless y el AP, y lo mitigan a través de distintos métodos. PEAP (Protected EAP), por ejemplo, establece un túnel TLS (*Transport Layer Security*) desde el cliente wireless hasta el servidor antes de pedir al usuario credenciales de autenticación. Aprovechando el hecho que EAP permite trabajar con otros métodos de autenticación, se podría implementar autenticación fuerte a través de OTP o contraseñas válidas solo una vez. EAP-TLS lo mitiga a través de criptografía de llave pública.

Nota: Tal como se mencionó en la sección 7.7.4, 802.1X tiene una debilidad en su diseño, pues considera al AP como elemento confiable. Esto lo hace, bajo ciertas condiciones, vulnerable a ataques de hombre en el medio y *hijacking* o interceptación.

DISEÑO DE SEGURIDAD DE RED WIRELESS VPN

Este diseño, mostrado en la figura 10.7, involucra un método general para usar VPNs IPSec como mecanismo de seguridad adicional para acceder a la red corporativa desde una Wireless LAN.

Los dispositivos usados en el diseño de red wireless VPN son:

- Adaptador Wireless y Software Cliente: Proporcionan el hardware y software necesarios para establecer comunicaciones wireless hacia el Punto de Acceso (AP).
- Cliente VPN para Acceso Remoto con software firewall personal: Un cliente en software que proporciona túneles cifrados de extremo a extremo entre PCs o laptops individuales y los dispositivos concentradores de VPNs de la red corporativa. El firewall personal proporciona protección al dispositivo.
- Punto de Acceso Wireless (*Wireless* AP): Proporciona filtrado IP entre la WLAN y la red corporativa.
- Switch de Capa 2 (L2): Proporciona conectividad Ethernet entre los APs y la red corporativa. Adicionalmente, algunos modelos recientes de switches de acceso tienen la capacidad de implementar control de acceso por VLANs, lo que puede proporcionar un nivel adicional de filtrado para IPSec.
- Switch de Capa 3 (L3): Encamina y conmuta datos de la red corporativa de un módulo a otro. Permite implementar políticas adicionales a través de filtrado a nivel de protocolo para el tráfico wireless.
- Servidor RADIUS: Autentica a los usuario wireless cuyos túneles terminan en el concentrador VPN. Opcionalmente se comunica con un servidor OTP.
- Servidor OTP (Opcional): El servidor OTP (*One-Time Password*) o de contraseñas válidas sólo una vez, autoriza información OTP recibida del servidor RADIUS.
- Servidor DHCP: Entrega información de configuración IP a clientes wireless VPN.

- Concentrador VPN: Autentica de manera individual a usuarios remotos y termina sus túneles IPSec. Puede proporcionar la funcionalidad de relevo de información DHCP para los clientes wireless.

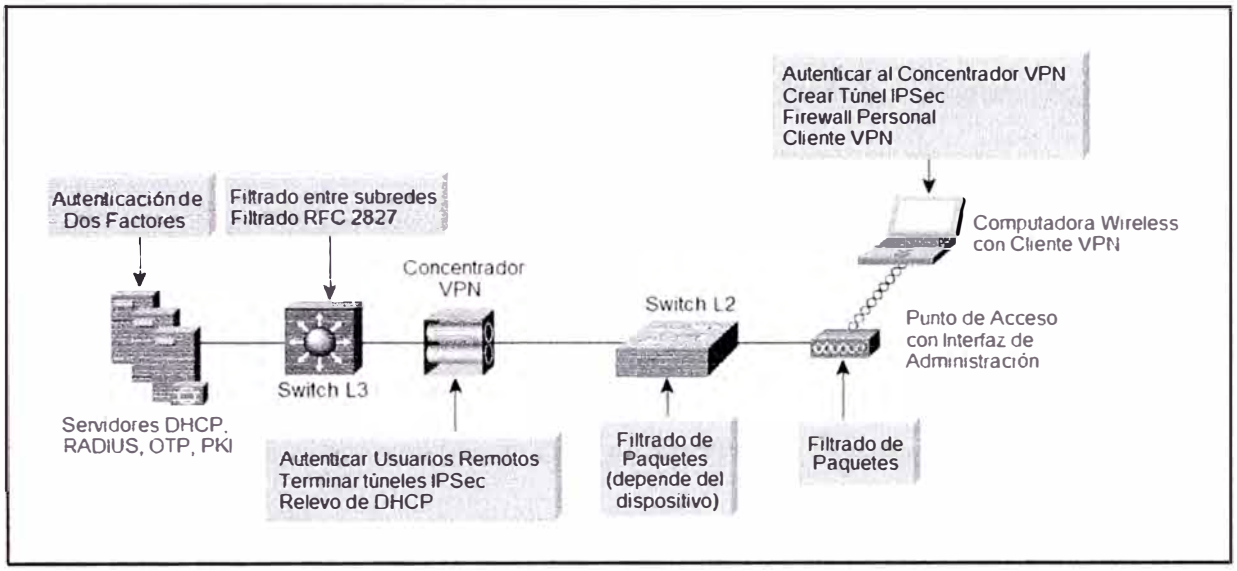

FIGURA 10.7 - Diseño de Seguridad para Redes Wireless VPN

Mitigación de Amenazas en Redes Wireless VPN

☑ *Sniffers* de Paquetes Wireless: Esta amenaza es mitigada mediante cifrado IPSec del tráfico del cliente wireless. Nuevas características en el software cliente VPN permiten especificar que el túnel VPN sea automáticamente establecido cuando la dirección IP WLAN correcta haya sido asignada al cliente. Esto elimina la interacción con el usuario para levantar el túnel y también protege al host de

difundir tráfico en el medio wireless que podría ser usado para ataques de inferencia.

- ☑ Ataques de Hombre en el Medio: Mitigados mediante el cifrado IPSec y la autenticación del tráfico del cliente.
- ☑ Acceso No Autorizado: Los únicos protocolos a los que se les permite pasar desde la WLAN hacia la red corporativa son: DHCP (para la configuración inicial IP) y los necesarios para el acceso VPN (DNS, IKE y ESP). El filtrado es realizado por el punto de acceso wireless y los switches de acceso. Opcionalmente, se puede implementar políticas de autorización en el concentrador VPN para grupos de usuarios individuales.
- ☑ IP *Spoofing* o Impostación de Direcciones IP: Los atacantes podrán impostar tráfico en la WLAN, pero solo paquetes IPSec válidos y autenticados llegarán a la red corporativa cableada.
- ☑ Ataques ARP (*Address Resolution Protocol*) *Spoofing*: Estos ataques podrán ser ejecutados, sin embargo, al estar cifrada la información hasta llegar al concentrador VPN, los atacantes no podrán interpretarla.
- ☑ Ataques de Contraseñas: Mitigados mediante políticas de contraseñas adecuadas, auditorías y opcionalmente, OTP (contraseñas válidas una sola vez).
- ☑ Descubrimiento de la Topología de Red: Solo se permite a los protocolos IKE, ESP, DNS y DHCP acceder desde el segmento wireless hacia la red corporativa. Se recomienda habilitar ICMP solo en la parte externa del concentrador VPN para propósitos de seguimiento de problemas.

Amenazas No Mitigadas en Redes Wireless VPN

- Impostación de MACs o IPs por parte de usuarios autenticados: Los ataques ARP *Spoofing* e IP *Spoofing* siguen siendo efectivos en la subred WLAN hasta que el cliente wireless use IPSec para asegurar la conexión.

Alternativas de Diseño en Redes Wireless

- El concentrador VPN podría usar Certificados Digitales o Llaves Pre-compartidas para la autenticación de los dispositivos wireless. Si se usan estas últimas, se recomienda emplear OTPs para autenticar a los usuarios. Sin OTP, los concentradores VPN estarían expuestos a ataques de fuerza bruta de inicio de sesión, por parte de atacantes que hubieran obtenido la llave compartida usada por el concentrador. El concentrador VPN emplearía los servicios RADIUS, los que a su vez contactarían al servidor OTP para autenticar a los usuarios.
- Se podría considerar el uso de servidores DHCP y DNS dedicados al segmento WLAN para contrarrestar ataques DoS que podrían afectar a los usuarios cableados, y contrarrestar ataques de reconocimiento, a través de consultas DNS.
- En lugar de usar servidores DNS dedicados, se podría considerar pre-configurar la IP del concentrador VPN en los clientes VPN. La desventaja de esto se vería cuando el concentrador tuviera que cambiar de IP. Entonces habría que modificar cada cliente VPN con el nuevo valor.

10.5. DISEÑO DE SEGURIDAD PARA REDES DE ACCESO REMOTO

Se considerarán las siguientes opciones para proporcionar conectividad a usuarios remotos, los cuales pueden ser tanto usuarios móviles, como teletrabajadores. El objetivo principal de estos diseños es proporcionar conectividad desde el sitio remoto hasta las oficinas principales de una organización, a través de un medio como Internet. A continuación las opciones:

- Acceso usando Software: Usuario remoto con software cliente VPN y firewall personal instalados en el host.
- Firewall en el lado remoto: El sitio remoto es protegido con un firewall en hardware que además proporciona conectividad VPN IPSec con las oficinas principales. La conectividad WAN es proporcionada por el ISP, típicamente, a través de un dispositivo para acceso de banda ancha. (e.g. módem DSL o Cable módem).
- Cliente VPN en hardware: El sitio remoto posee un cliente VPN en hardware que proporciona conectividad VPN IPSec hacia las oficinas principales. La conectividad WAN es proporcionada por el ISP, típicamente, a través de un dispositivo para acceso de banda ancha.
- Ruteador en el lado remoto: Un ruteador en el lado remoto proporciona funcionalidades de firewall y conectividad VPN IPSec hacia las oficinas principales. Este equipo podría proporcionar directamente el acceso de banda ancha, o podría conectarse con un dispositivo provisto por el ISP para este fin.

Las opciones de diseño mencionadas pueden apreciarse en la figura 10.8.

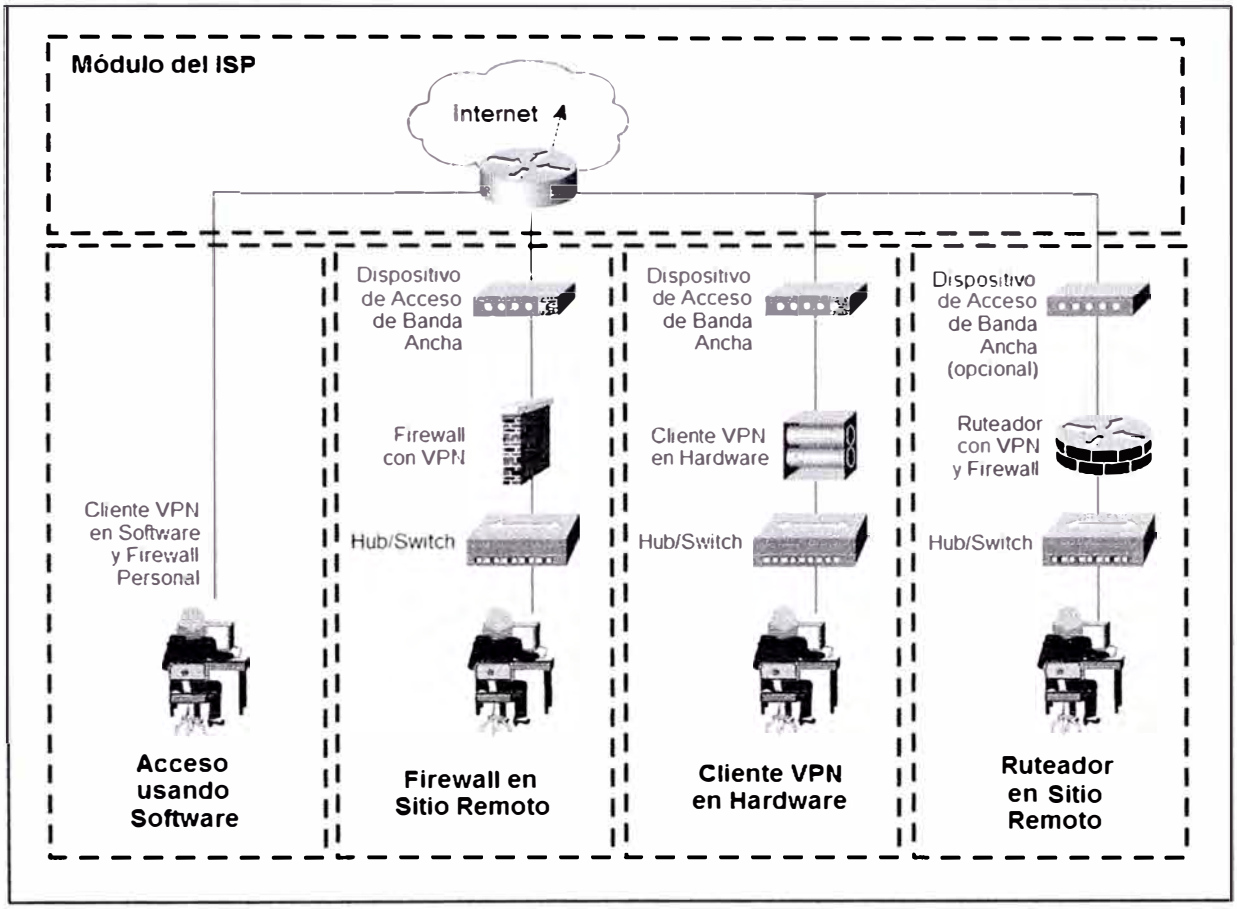

FIGURA 10.8 - Diseño de Red de Acceso Remoto con conectividad vía Internet

Los dispositivos empleados en una red de acceso remoto se detallan a continuación:

- Dispositivo de Acceso de Banda Ancha: proporciona acceso a la red de banda ancha. Usualmente es un cable módem o un ruteador/módem DSL.

- Cliente VPN en Software: Proporciona túneles cifrados de extremo a extremo entre PCs o laptops individuales y las oficinas principales.
- Cliente VPN en Hardware: Proporciona túneles cifrados de extremo a extremo entre el sitio remoto y las oficinas principales.
- Firewall con soporte VPN: Proporciona túneles cifrados de extremo a extremo entre el sitio remoto y las oficinas principales, además de protección a nivel de red de los recursos del sitio remoto, y filtrado de tráfico con inspección de estados.
- Ruteador con capacidad de firewall y VPN: Proporciona túneles cifrados de extremo a extremo entre el sitio remoto y las oficinas principales, además de protección a nivel de red de los recursos del sitio remoto, y filtrado de tráfico con inspección de estados. Adicionalmente, podría ofrecer servicios avanzados tales como voz, o QoS dentro del túnel VPN.
- Firewall Personal o en software: Proporciona protección a nivel de dispositivo para PCs o laptops individuales.
- Hub o Switch: Proporciona conectividad para dispositivos dentro del sitio remoto (puede ser integrado dentro del firewall o cliente VPN en hardware).

Amenazas Mitigadas en Redes de Acceso Remoto

☑ Acceso No Autorizado: Mitigado a través del filtrado y la inspección de estados de sesiones, en el firewall o en el ruteador del sitio remoto, o en su defecto, a través de control de acceso a nivel de aplicación con un firewall personal.

- ☑ Reconocimiento de Red: Se filtran protocolos en alguno de los dispositivos del sitio remoto para limitar su efectividad.
- ☑ Virus y Caballos de Troya: El empleo y actualización de Antivirus en los hosts, permite detectar y eliminar la mayoría de virus y caballos de Troya.
- ☑ IP *Spoofing* o Impostación de Direcciones IP: Mitigado a través de filtrado según los RFCs 2827 y 1918 en el ruteador de borde del ISP y en el dispositivo de borde del sitio remoto.
- ☑ Ataques de Hombre en el Medio: Mitigados mediante cifrado del tráfico remoto.

Alternativas de Diseño en Redes de Acceso Remoto

- Los diseños mostrados asumen que la conectividad es a través de Internet. Para el caso de accesos conmutados se requeriría en las oficinas principales un dispositivo para concentrar las llamadas analógicas o digitales, como por ejemplo un NAS (*Network Access Server*). Las llamadas digitales podrían hacerse directamente desde la PC o laptop remota con el hardware adecuado, o desde un dispositivo RDSI separado que deberá adaptarse al tipo de conexión proporcionada por el proveedor RDSI. Ya que una Red Digital de Servicios Digitales Integrados (RDSI) es considerada un medio de conectividad privado, se podría prescindir del cifrado de tráfico. Las llamadas analógicas, a través de la Red Telefónica Conmutada (RTC) típicamente se harían desde un módem conectado o integrado a la PC o laptop remota. El módem también podría estar integrado a un ruteador para que más de un

usuario pudiera acceder a la vez. Sin embargo esto no se acostumbra debido a las bajas velocidades (hasta 56 kbps) disponibles para llamadas analógicas.

- En algunos escenarios, el sitio remoto podría requerir soporte para telefonía IP. Para esto, se debe tener en consideración los anchos de banda mínimos requeridos por canal de voz (dependiendo del CODEC elegido), el número de canales de voz simultáneos, y algunas otras restricciones del fabricante del los teléfonos IP. En algunos casos es posible aplicar QoS, es decir, dar un tratamiento priorizado al tráfico de voz sobre el resto de tráfico, dentro del túnel.

CONCLUSIONES

1. La seguridad en una red es tan fuerte como el eslabón más débil. Todo elemento de red es un objetivo de ataque: ruteadores, switches, hosts, aplicaciones, redes componentes, los mismos dispositivos de seguridad y la información en sí.

2. La seguridad es un tema complejo que empieza por la definición de políticas o normas de seguridad, claras y flexibles, que deben ser respaldadas y aplicadas a lo largo de la organización. Éstas deben detallar las actividades permitidas y prohibidas, y los esfuerzos y responsabilidades relacionados con la seguridad. Debe ponerse especial énfasis en la concientización y capacitación de los usuarios de la red con relación a los riesgos de seguridad que sus acciones pueden crear. Es así como una buena estrategia de seguridad debe contemplar no solo aspectos de tecnología sino también aspectos de comportamiento humano.

3. Otro aspecto de seguridad importante, al que a veces no se le presta mucha atención, es la seguridad física. De nada serviría tener una implementación de seguridad que proteja de

ataques desde Internet, si los atacantes, externos o internos, pudieran ingresar a las oficinas de la organización y tener acceso físico a la información o a los dispositivos de red con poco o ningún control. Por tanto una buena implementación de seguridad debe contemplar aspectos de seguridad física perimetral, alarmas, dispositivos de vigilancia; control de acceso para ambientes clave a través de llaves, tarjetas de identidad o dispositivos biométricos, entre otros.

4. Los productos usados y la complejidad del diseño implementado para proporcionar seguridad diferirán de una red a otra, ya que cada diseño puede ser influenciado por distintos factores tales como: presupuesto, seguridad requerida, servicios ofrecidos, capacidad de acceso remoto, número de usuarios, efectividad en costo, administración, y conectividad requerida. Independientemente de qué productos sean usados dentro de un diseño determinado, debe proporcionarse siempre la funcionalidad requerida por la organización. Si el desempeño es una preocupación, debe usarse un dispositivo de seguridad especializado en vez de un dispositivo genérico, de múltiples propósitos.

5. La seguridad es un proceso continuo en perpetua evolución, no un esfuerzo de implementación en un momento determinado. Puesto que la única constante es el cambio, la postura de seguridad de una red debe ir a la par con las innovaciones tecnológicas, con los nuevos descubrimientos de amenazas y vulnerabilidades en los sistemas, y por supuesto, con los nuevos requerimientos y necesidades de la organización.

6. Antes se hablaba de implementaciones de seguridad con productos que resolvían temas puntuales de seguridad en determinada capa del modelo OSI o TCP/IP, y que no interactuaban entre sí. El problema es que si una capa es vulnerable, todo el sistema podría serlo. Debido a esto, la tendencia actual es pasar a sistemas de seguridad de varias capas integradas. Por tanto, debe existir integración y colaboración, es decir, trabajo conjunto coordinado entre los distintos elementos del sistema para poder frustrar los ataques.

7. Hoy en día, la rapidez con la que las amenazas aparecen y se propagan, es tal que un esquema de seguridad reactivo resulta insuficiente. Para que exista proactividad se requiere que los elementos de red sean más inteligentes, de tal forma que detecten amenazas y ataques antes que alcancen sus objetivos, y que puedan tomar acciones defensivas sin la necesidad de intervención humana. Esto a su vez requiere algoritmos avanzados de detección de amenazas e integración de dichos elementos con el resto de la red para la respectiva reconfiguración de dispositivos en caso de ataques. Además, se necesita un afinamiento adecuado de la sensibilidad de los dispositivos de seguridad para detectar ataques y no bloquear el tráfico válido. Por otro lado, es necesario verificar que todos los dispositivos que se conecten a la red, sobretodo los remotos, sobre los cuales el administrador tiene menor control, cumplan con requisitos mínimos para no poner en peligro al resto de la red. Dichos requisitos pueden incluir actualizaciones de seguridad del sistema operativo, actualizaciones del antivirus, la presencia y correcta configuración de sistemas de detección/prevención de intrusos basados en host, entre otros. Una implementación de seguridad de este tipo requerirá, por ejemplo, agentes instalados en los dispositivos de los usuarios que se comuniquen con un servidor que

maneje perfiles de seguridad, y evalúe si el dispositivo en cuestión cumple con los requisitos mínimos para permitirle el acceso a la red, o de lo contrario permitirle actualizarse antes de ingresar.

8. Ésta es la siguiente generación de seguridad en redes: una red capaz de adaptarse, previniendo y reaccionando automáticamente ante todo tipo de amenazas, conocidas o no; capaz de controlar e inspeccionar a profundidad el tráfico; de controlar y proteger de manera coordinada y dinámica los puntos terminales y toda la infraestructura de red, permitiendo conectividad segura y a la vez flexible, con métodos avanzados de autenticación y autorización de acceso a recursos específicos, y la capacidad de monitoreo y auditoría de las acciones realizadas.

GLOSARIO

3DES (Triple-DES): Algoritmo de cifrado basado en DES, que procesa cada bloque de información tres veces usando una llave distinta cada vez. 3DES es más difícil de "romper" que DES, pero a la vez es más lento.

802.11: Familia de especificaciones para redes LAN wireless, desarrollada por la IEEE. Define los protocolos tanto a nivel físico (PHY) como a nivel de control de acceso al medio (MAC). La especificación original usa la banda de 2.4 GHz y permite velocidades de hasta 1 o 2 Mbps. 802.11b mejora la velocidad hasta 11 Mbps. 802.11a utiliza la banda de 5 GHz y permite velocidades de hasta 54 Mbps. Finalmente, 802.11g trabaja a 2.4 GHz con velocidades de hasta 54 Mbps.

802.1q: Estándar de la IEEE que proporciona un mecanismo de identificación de LANs virtuales (VLANs) y la posibilidad de establecer niveles de Calidad de Servicio (QoS). Agrega 4 bytes al encabezado de las tramas Ethernet, de los cuales 3 bits son usados para el

campo de prioridad, permitiendo hasta ocho niveles de prioridad; mientras que 12 bits son usados para identificar hasta 4096 VLANs.

802.1X: Estándar diseñado para mejorar la seguridad de redes LAN cableadas o wireless, permitiendo a usuarios autenticarse contra una autoridad central. 802.1X emplea para el intercambio de mensajes durante el proceso de autenticación, al protocolo EAP (*Extensible Authentication Protocol*), que trabaja sobre redes LAN Ethernet, wireless o Token Ring. El algoritmo de autenticación propiamente usado se deja a elección. 802.1X define tres roles: El usuario o cliente que busca ser autenticado es llamado el Suplicante. El servidor que realiza la autenticación, típicamente un servidor RADIUS, es llamado el Servidor de Autenticación. El dispositivo en medio de los dos, que puede ser un punto de acceso wireless, es llamado el Autenticador.

AAA (*Authentication, Authorization and Accounting*): Autenticación, Autorización y Contabilidad—Enfoque de seguridad para acceso remoto que controla el acceso a una red al requerir identificación de usuarios, restringir el acceso a recursos específicos solamente, y mantener registros de uso para propósitos de facturación y auditoría de red.

AES (*Advanced Encryption Standard*): Estándar de Cifrado Avanzado--Algoritmo criptográfico de llave simétrica, previamente conocido como Rijndael, y que se espera sea el reemplazo de 3DES, como algoritmo de cifrado estandarizado por el gobierno de los Estados Unidos.

AH (*Authentication Header*): Encabezado de Autenticación—Protocolo IPSec y parte opcional del proceso IPSec que autentica el paquete entero. Proporciona protección *anti-replay* y verifica que el contenido de los paquetes no haya sido modificado en tránsito (integridad), y que provengan de la misma fuente (autenticidad del origen). Es un código matemático incrustado y transmitido en el paquete IP. Puede ser aplicado por si solo o en combinación con ESP.

***Anti-replay*:** Mecanismo o característica de seguridad mediante la cual el receptor de la información puede detectar y rechazar paquetes duplicados o recibidos anteriormente, puesto que podría tratarse de intentos de ataques de tipo *playback* o de repetición. IPSec proporciona este servicio mediante el uso de números de secuencia combinados con el uso de autenticación de datos. Este servicio no está disponible para asociaciones de seguridad establecidas manualmente, es decir, aquellas no establecidas con IKE.

AP (*Access Point*): Ver Punto de Acceso.

APNIC (*Asia Pacific Network Information Center*): Centro de Información de Red de Asia Pacífico—Organización sin fines de lucro responsable de la administración y registro de direcciones IP en Asia Pacífico, incluyendo Japón, Corea, China y Australia, entre otros.

***Applet*:** Módulo ejecutable pequeño que normalmente no tiene todas las características ni la interfaz de usuario de una aplicación normal. Java es el lenguaje de programación más

comúnmente asociado con los *applets*. Un *applet* corre dentro de una aplicación en una "caja de arena" o "máquina virtual", que es un conjunto de recursos de la computadora e instrucciones que componen el entorno necesario para la ejecución del *applet*.

ARA (*AppleTalk Remote Access*). Protocolo y producto que proporciona soporte a nivel de sistema para conexiones conmutadas (*dial-in*) hacia una red AppleTalk.

ARIN (American Registry of Internet Numbers): Registro Americano de Números de Internet—Organización sin fines de lucro establecida con el propósito de administrar y registrar direcciones IP en Norteamérica, Sudamérica, el Caribe y parte de África. Hasta 1997 estas tareas estaban asignadas a Network Solutions Inc. (InterNIC) por la IANA.

ARP (*Address Resolution Protocol*): Protocolo que traduce direcciones IP en direcciones MAC. Cuando un dispositivo A en una red LAN desea conectarse con otro dispositivo B, envía un mensaje *broadcast* ARP diciendo: "¿Quién tiene la dirección IP de B? Responder a A". Todos los dispositivos en la red reciben la solicitud. Si alguno de ellos tiene la IP solicitada o conoce la ruta hacia la IP solicitada, entonces responderá a A con un mensaje *unicast* especificando que la dirección IP B está en una determinada MAC. Para ser más eficiente y no repetir el proceso ARP para cada paquete, los dispositivos almacenan estas entradas en una tabla ARP, la cual es desechada después de un tiempo especificado por el sistema operativo.

ARP *Spoofing* (Impostación de ARP): Método de ataque efectivo para interceptar conexiones y realizar denegación de servicios. Estos ataques aprovechan una vulnerabilidad en el protocolo ARP, la cual consiste en que para mejorar la eficiencia, muchos sistemas actualizan sus tablas cada vez que reciben un mensaje ARP incluso si no lo solicitaron. Esto significa que un atacante podrá enviar un mensaje ARP a un host diciendo que un determinado destino está en su MAC. De esta manera, los paquetes que el host envíe al destino serán reencaminados hacia la máquina del atacante. *ARP Spoofing* solo funciona dentro de una VLAN o dominio de *broadcast*.

Asociación de Seguridad: En IPSec, conjunto de parámetros que describe cómo dos o más entidades usarán los servicios de seguridad de un protocolo de seguridad en particular (AH o ESP), para comunicar de manera segura un flujo de tráfico en particular. Las asociaciones de seguridad son unidireccionales y únicas para cada protocolo de seguridad.

ATM (*Asynchronous Transfer Mode*): Modo de Transferencia Asincrónica—Estándar internacional para la transmisión de múltiples tipos de servicios, tales como datos, voz y video, los cuales son transportados en celdas de longitud fija (53 bytes). El uso de celdas de longitud fija permite que su procesamiento ocurra en hardware, reduciendo así los retardos. ATM es una tecnología de conmutación diseñada para tomar ventaja de medios de transmisión de alta velocidad, a partir de 2 Mbps. El término "asincrónico" se refiere a que una celda es procesada de manera asincrónica con respecto a otras celdas relacionadas, y es puesta en cola antes de ser multiplexada sobre el medio de transmisión.

Autenticación de Dos Factores (*Two-factor authentication*): Sistema que confirma la identidad de los usuarios usando dos factores o elementos distintivos: algo que ellos poseen y algo que ellos conocen. Al requerir dos formas distintas de identificación electrónica se mejora la protección y confidencialidad de la información.

Autoridad Certificadora: Entidad en la cual dos partes han puesto su confianza, que autentica, emite, renueva y revoca certificados digitales. Además de establecer confianza en la asociación de la llave pública de un usuario con otra información en un certificado, relacionada con la seguridad, la Autoridad Certificadora o CA firma digitalmente la información del certificado usando su llave privada. De esta manera, dicho certificado puede ser verificado usando la llave pública de la CA.

***Backplane*:** (1) Tarjeta de circuitos electrónicos impresos que posee ranuras en las cuales se insertan otras tarjetas electrónicas. Es un bus de comunicaciones de alta velocidad al que se conectan componentes individuales: tarjetas o procesadores de interfaz, buses de distribución de datos y de energía. La capacidad del *backplane* determina la capacidad del dispositivo en su conjunto. (2) En computadoras, generalmente es sinónimo o parte de una tarjeta madre (*motherboard*).

***Backbone*:** (1) La parte principal de una red usada como el camino principal para transportar el tráfico entre segmentos de red. (2) Línea o serie de conexiones de alta velocidad que

forman un camino principal dentro de una red. El término alta velocidad es relativo al tamaño de la red.

BGP (*Border Gateway Protocol*): Protocolo de encaminamiento o "ruteo" estándar usado principalmente para redes grandes y heterogéneas con múltiples puertas de enlace. BGP permite a los ruteadores intercambiar solo información específica con ruteadores específicos en otros dominios. Los pares BGP intercambian rutas usando el puerto 179 de TCP. BGP fue inicialmente definido en el RFC 1163. Su actual versión, BGP-4, fue definida en el RFC 1771 y es actualmente usada en Internet.

BIND (*Berkeley Internet Name Daemon*): Implementación de un servidor DNS desarrollada y distribuida por la Universidad de California en Berkeley

***Broadcast* (Difusión):** Paquete (trama o datagrama) enviado a todos los nodos de una red o subred.

***Buffer*:** Un lugar temporal de almacenamiento de información, diseñado para compensar diferencias en la tasa de transmisión de un dispositivo a otro, o para retener la información cuando hay una diferencia en la ocurrencia de eventos. Las ráfagas de datos, por ejemplo, pueden ser almacenadas en *buffers*, hasta que puedan ser manejadas por el dispositivo de menor capacidad o velocidad de procesamiento. Un *buffer* puede ser un programa en software, o un dispositivo en hardware, tal como una memoria.

***Bus*:** (1) Término usado para describir cualquier clase de dispositivo electrónico en el que un número de elementos están cableados entre sí con un único cable, de tal manera que todos los elementos pueden usar el mismo cable para transmitir información al resto de elementos. Por ejemplo, los *buses* se usan internamente en computadoras para interconectarlas con sus dispositivos periféricos. (2) En una LAN, *bus* es un término usado para describir una topología LAN en la que el mismo cable está conectado a un número de dispositivos que comparten dicho cable para transmitir información entre sí. En esta topología cuando un dispositivo transmite, todos los demás dispositivos reciben la información, así no sea dirigida para ellos.

CA (*Certificate Authority*): Ver Autoridad Certificadora.

Certificado de Seguridad: Ver Certificado Digital

Certificado Digital: Documento electrónico que contiene información acerca de la identidad del portador del certificado: su nombre o dirección IP, el número de serie del certificado, fecha de expiración del certificado y una copia de la llave pública del portador del certificado. Un certificado digital o de seguridad asocia una llave pública con una persona, dispositivo u otra entidad en particular. El certificado es expedido por una entidad, en la cual los usuarios han puesto su confianza, llamada Autoridad Certificadora (CA: Certificate Authority) quien garantiza la identidad del portador de la llave privada correspondiente. La CA firma digitalmente el certificado con su llave privada, de tal manera que puede ser verificado usando

la llave pública de la CA. El formato estándar del certificado digital está definido en la especificación X.509 versión 3 de la ISO (*International Organization for Standarization*) u Organización Internacional para la Estandarización.

CHAP (*Challenge Handshake Authentication Protocol*): Protocolo de seguridad para autenticación usado en conexiones punto a punto PPP, el cual no envía la contraseña por el enlace, y realiza un saludo de tres vías, tal como se explica seguidamente: Una vez que se establece la conexión, el autenticador envía un *challenge* o mensaje desafío al solicitante. Éste responde enviando un valor calculado a partir de la contraseña secreta, usando una función de *hash* unilateral. El autenticador verifica la respuesta contra su propio cálculo del valor de *hash* esperado. Si coinciden, se valida exitosamente al solicitante, sino la conexión debe ser finalizada. Este proceso se da no solo al inicio de la conexión sino también durante la misma en intervalos de tiempo aleatorios. A pesar que la autenticación se realiza en un solo sentido, al negociar CHAP en ambas direcciones, la misma contraseña o secreto se puede usar para realizar autenticación mutua.

***Checksum* (Suma de chequeo):** Cálculo matemático aplicado al contenido de un paquete o archivo antes y después de ser transmitido. Los *checksums* son transmitidos (o almacenados) junto con la información, para detectar si ésta ha sido alterada durante la transmisión (o al ser almacenada y recuperada). Para esto, el receptor recalcula el *checksum* a partir de la información recibida.

Cifrado (*Encryption*): Transformación de la información en un formato no legible por alguien que no tenga la llave secreta para revertir el proceso (descifrado). Su propósito es asegurar la privacidad de la información.

CGI (*Common Gateway Interface*): Estándar para correr programas externos desde un servidor Web HTTP. CGI especifica cómo pasar argumentos al programa en ejecución como parte de una solicitud HTTP. También define un conjunto de variables ambientales. Comúnmente el programa generará un código HTML que será devuelto al navegador, pero también puede solicitar una redirección URL. Un programa CGI puede, por ejemplo, acceder a una base de datos y dar formato HTML a los resultados. Un programa CGI puede ser cualquier programa que acepte argumentos en la línea de comandos. PERL es una elección común para escribir *scripts* CGI.

CODEC (*COmpressor/DECompressor*): Tecnología para comprimir y descomprimir información. Los CODECs pueden ser implementados en software, hardware o una combinación de ambos. Los CODECs se emplean también para transformar señales de voz analógicas a señales digitales (*coder*), y señales digitales a señales analógicas (*decoder*).

Core: (1) Parte central de un sistema. (2) En una red jerárquica de switches, la capa de *Core* es el *backbone* (o punto medular) de conmutación de alta velocidad, diseñado para conmutar paquetes tan rápido como sea posible entre dispositivos de la capa de distribución.

CPU (*Central Processing Unit*): Unidad Central de Procesamiento—Es el "cerebro" de una computadora; el chip o microcircuito integrado principal que ejecuta y supervisa las operaciones, cálculos, e instrucciones.

Criptografía Simétrica: Estudio y aplicación de cifradores, o algoritmos de cifrado, que usan la misma llave secreta tanto para operaciones de cifrado como de descifrado.

Criptografía de Llave Secreta Pre-compartida: Ver Criptografía Simétrica.

CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*): Método de acceso al medio en una red, en el cual todos los dispositivos compiten equitativamente por el derecho a transmitir. Los dispositivos que están listos para transmitir chequean primero el medio en busca de una señal portadora. Si no se detecta portadora, un dispositivo puede transmitir. Si dos dispositivos transmiten a la vez, ocurre una colisión y cada uno se inhibe, esperando un tiempo aleatorio antes de intentar retransmitir. Este es el método de acceso al medio usado por Ethernet.

***Daemon* (*Disk And Execution MONitor*):** Ver demonio.

Datagrama: Un paquete de información usado en servicios no orientados a la conexión (como IP) que es encaminado hacia su destino, usando la dirección incluida en su cabecera.

Demonio: Proceso que corre en segundo plano, sin intervención del usuario, y que realiza alguna tarea administrativa o ejecuta comandos.

DES (*Data Encryption Standard*): El algoritmo de cifrado simétrico más usado alrededor del mundo. Desarrollado en 1977, emplea el método de cifrado en bloques, aplicando una llave de 56 bits a cada bloque de datos de 64 bits.

Diffie-Hellman: El intercambio de llaves Diffie-Hellman es una técnica criptográfica que permite a dos partes intercambiar números aleatorios, realizar cálculos e intercambiar los resultados para producir un nuevo y aparente número aleatorio que puede ser usado como "Llave Secreta". Incluso un espía que capture todos los intercambios involucrados, no podrá calcular el mismo valor secreto.

Dirección Ethernet: Ver Dirección MAC.

Dirección Física: Ver Dirección MAC.

Dirección IP: Identificador para dispositivos en una red TCP/IP usado para facilitar el transporte de información entre redes. Una dirección IP está compuesta de un número de red, un número de subred y un número de host. El formato de una dirección IP versión 4 es un número de 32 bits escrito como cuatro números entre 0 y 255 separados por puntos. La

asignación de direcciones IP públicas, aquellas visibles y encaminadas por Internet, está regulada por organizaciones como ARIN, RIPE o APNIC.

Dirección Lógica: Ver Dirección IP.

Dirección MAC: Identificador de hardware o dirección de la Capa de Enlace de Datos que debe identificar unívocamente a cada dispositivo dentro de una red LAN. Los dispositivos usan estas direcciones para distinguirse y localizarse entre sí, creando y actualizando tablas internas. Una dirección MAC tiene 6 bytes (48 bits) de longitud que son controlados por la IEEE. Originalmente las direcciones MAC que venían grabadas en las tarjetas de red Ethernet, no podían ser cambiadas. Actualmente esto es posible.

DMZ (*Demilitarized Zone*): Zona Desmilitarizada—Término usado en la milicia para referirse a una zona de seguridad entre líneas de batalla. Una DMZ es una zona en una red que no forma parte de la red interna, pero tampoco está totalmente abierta a Internet. Un firewall o ruteador usualmente protege esta zona con funcionalidades de filtrado de tráfico.

DNS (*Domain Name System or Service*): Servicio o Servidor en Internet que traduce los nombres de dominios a direcciones IP y viceversa. Esto permite a los usuarios especificar destinos remotos por nombre en lugar de por direcciones IP.

Dominio de *Broadcast*: Conjunto de dispositivos en una red que pueden recibir las tramas *broadcast* de cada uno de ellos. Un segmento o grupo de segmentos de red conectados con un *hub*, repetidor, *bridge* o *switch* están incluidos en un dominio de *broadcast*. Los límites de un dominio de *broadcast* están definidos por ruteadores y firewalls.

Dominio de Colisión: Red o segmento CSMA/CD separado de una red mayor por medio de un *bridge*, *switch*, ruteador, firewall o puerta de enlace. Un dominio de colisión es un grupo de dispositivos en una red cuyos paquetes pueden colisionar entre sí.

DSA (*Digital Signature Algorithm*): DSA es un algoritmo de llave pública, basado en el problema de logaritmos discretos, que es usado para generar firmas digitales para la autenticación de documentos electrónicos. A diferencia de RSA, DSA no puede ser usado para el cifrado de información, sólo para generar y verificar firmas digitales. DSA fue desarrollado por la Agencia de Seguridad Nacional de los Estados Unidos.

DSSS (*Direct-Sequence Spread Spectrum*): Tecnología de transmisión usada en redes LAN Wireless, en la que la señal de datos en la estación emisora es combinada con una secuencia de bits de una mayor tasa de datos (*chipping code*), que divide los datos del usuario de acuerdo a un índice de propagación. El *chipping code* es un patrón de bits redundante para cada bit transmitido, lo cual incrementa la resistencia de la señal ante interferencia, proporcionando integridad de los datos. Es uno de los esquemas de modulación prescrito por

el estándar 802.11 de la IEEE para comunicaciones wireless, y es el método de transmisión empleado por el estándar 802.11b de la IEEE.

EAP (*Extensible Authentication Protocol*): Es un protocolo general para autenticación que soporta múltiples métodos de autenticación, tales como tarjetas *token*, contraseñas válidas una sola vez, autenticación de llave pública, etc. El estándar 802.1X especifica cómo EAP debe ser encapsulado en tramas dentro de la LAN. En comunicaciones wireless que usan EAP, el usuario solicita conexión a la LAN wireless a través de un punto de acceso o AP, el cual solicita la identidad del usuario, para luego transmitirla a un servidor de autenticación como RADIUS. El servidor solicita al AP una prueba de identidad, la cual el AP obtiene del usuario y entrega al servidor para que éste complete el proceso de autenticación, validando o no al usuario solicitante. EAP es una extensión de PPP y está definido en el RFC 2284.

***Ethernet*:** Protocolo de red de área local en banda base desarrollado en 1976 por Xerox, en cooperación con DEC e Intel. *Ethernet* usa una topología de *bus* o de estrella y soporta tasas de transferencia de 10 Mbps. La especificación *Ethernet* sirvió de base al estándar 802.3 de la IEEE, el cual especifica la capa física y la capa de bajo nivel de software. *Ethernet* emplea CSMA/CD como método de acceso para manejar demandas simultáneas, y es uno de los estándares LAN más difundidos. Una versión mejorada, llamada *Fast Ethernet*, soporta tasas de transferencia de 100 Mbps. Una nueva versión, conocida como *Gibabit Ethernet* soporta tasas de transferencia de 1000 Mbps (1 Gibabit por segundo).

***Extranet*:** Red de colaboración que, a través de las tecnologías de telecomunicaciones disponibles, permite conectar a las empresas con sus proveedores, clientes u otras empresas que comparten objetivos en común. Una *Extranet* puede ser vista como una parte de la *Intranet* de la organización que se hace accesible a otras organizaciones, típicamente socios de negocios.

FHSS (*Frequency Hopping Spread Spectrum*): Tecnología de transmisión en la que la señal de datos es modulada con una señal portadora de banda angosta que "salta" de frecuencia en frecuencia en una secuencia pseudo-aleatoria pero conocida, la cual está en función del tiempo y se aplica sobre un amplio rango de frecuencias. La señal de energía está extendida en el dominio del tiempo en vez de que cada bit sea cortado en pequeños pedazos en el dominio de la frecuencia. Esta técnica reduce la interferencia ya que una señal de un sistema de banda angosta solo afectará a la señal de espectro extendido si ambas son transmitidas a la misma frecuencia al mismo tiempo. Si se sincroniza apropiadamente, un único canal lógico es mantenido. FHSS es uno de los esquemas de modulación prescritos para el estándar 802.11 de la IEEE. FHSS divide la banda de 2.4 Ghz, que tiene 83 MHz de ancho, en 79 saltos cada uno de 1 MHz de ancho, y ofrece velocidades de hasta 2 Mbps.

***Firewall*:** Software y/o hardware que protege los recursos de una red privada y refuerza los límites entre dos o más redes. Un firewall filtra paquetes determinando si debe reenviarlos o bloquearlos, de acuerdo a las reglas o políticas de seguridad configuradas. Existen tres tipos

de arquitecturas de firewalls: Filtrado (estático) de Paquetes, Basados en *Proxy*, y de Inspección de Estados.

***Firmware*:** Programa o instrucciones almacenados en una memoria de solo lectura (ROM) o similar.

***Frame Relay*:** Servicio de comunicaciones de datos de conmutación de paquetes, apropiado para entornos con demandas de tráfico en ráfagas. *Frame Relay* es un protocolo WAN de capa 2 del modelo de referencia OSI para transferencia de tramas o paquetes de longitud variable, a velocidades de hasta 2 Mbps. Está diseñado para trabajar sobre líneas digitales libres de ruido, y por lo tanto omite las facilidades de corrección de errores. *Frame Relay* sí puede detectar errores en las tramas pero no las corrige ni pide retransmisión, solo las descarta, pues dichas funciones deben descansar en protocolos de capas superiores. Esto lo hace más eficiente en el uso del ancho de banda. *Frame Relay* ofrece servicios de circuitos virtuales permanentes o PVCs y de circuitos virtuales conmutados o SVCs.

FTP (*File Transfer Protocol*): Protocolo de la familia TCP/IP empleado para copiar o transferir archivos de una computadora a otra. Es un protocolo cliente/servidor que permite al cliente FTP registrarse en un servidor o computadora remota, navegar por el sistema de archivos, y depositar o descargar archivos en dicho servidor.

***Gateway* (Puerta de Enlace):** (1) Hardware o software que realiza una traducción entre dos protocolos o medios disímiles. Un *gateway* puede funcionar en cualquiera o varias de las capas del modelo de referencia OSI. Por ejemplo, un *gateway* puede ser usado como traductor entre sistemas de correos. A diferencia de un *proxy*, un *gateway* recibe los mensajes como si fuera el receptor final. (2) Elemento en una red que actúa como punto de entrada a otra red. En la terminología de Internet se suele usar el término *gateway* en lugar de ruteador. (3) Cualquier mecanismo que proporciona acceso a otro sistema.

H.323: Estándar de la ITU-T para transferencia en tiempo real de datos, audio y videoconferencia sobre redes de conmutación de paquetes, tales como TCP/IP. H.323 es una extensión del estándar H.320 para videoconferencia sobre redes de conmutación de paquetes. H.323 es un estándar "sombrilla" que describe la arquitectura de sistemas y aplicaciones multimedia, y hace referencia a un conjunto de otros estándares (H.245, H.225.0 y Q.931) para describir los protocolos en sí.

***Hardware*:** Los componentes físicos mecánicos y/o eléctrico/electrónicos de un sistema de computadoras.

***Hash*:** Fórmula matemática que convierte un mensaje de cualquier longitud en una cadena de dígitos única de longitud fija conocida como "*message digest*" o compendio de mensaje y que representa al mensaje original. Un *hash* es una función unilateral, es decir que es casi

imposible revertir el proceso para determinar el mensaje original a partir de ésta. Además, una función *hash* no producirá el mismo "*message digest*" para dos entradas distintas.

Hipertexto: (1) Una manera de representar información, en la que texto, sonidos, imágenes y acciones son enlazadas entre sí de tal manera que pueden ser accedidos en cualquier orden de manera flexible. (2) Texto que contiene *links* o enlaces a otros documentos.

HMAC (*Hash function-based MAC*): Código de autenticación de mensajes basado en una función de *hash*. HMAC usa una o más llaves en conjunto con una función de *hash* para producir un *checksum* que se anexa al mensaje.

Host: (1) Computadora que permite a los usuarios comunicarse con otras computadoras en una red. (2) Computadora que proporciona servicios a otras computadoras en una red. Los servicios pueden incluir dispositivos periféricos como impresoras, almacenamiento de datos, correo electrónico, o acceso Web. Un host es también llamado Servidor.

HTML (*HyperText Markup Language*): Lenguaje simbólico utilizado para crear los documentos con hipertexto que se usan en la web. *Markup* se refiere a la secuencia de caracteres u otros símbolos que se insertan en determinados lugares del código para indicar cómo debe verse el documento, o para describir la estructura lógica del mismo.

HTTP (*HyperText Transfer Protocol*): El protocolo para mover archivos de hipertexto a través de Internet. Requiere un programa cliente HTTP en un lado, y un programa servidor HTTP en el otro. Es el protocolo de la capa de aplicación de la suite TCP/IP más usado en la *World Wide Web* (WWW).

***Hub*:** Concentrador que interconecta múltiples dispositivos con el resto de la LAN por medio de un solo enlace. Posee varios puertos a los cuales se conectan los clientes, y uno o más puertos que pueden ser usados para conectar el *hub* al *backbone* o a otra red. Un *hub* opera en la capa física del modelo de referencia OSI, y funciona como un repetidor multi-puertos: las señales recibidas en un puerto son inmediatamente retransmitidas a todos los demás puertos.

IANA (*Internet Assigned Numbers Authority*): Autoridad originalmente responsable de la supervisión de la asignación de direcciones IP, la coordinación en la asignación de parámetros de los protocolos previstos en los estándares técnicos de Internet, y la administración de los DNS, incluyendo la delegación de dominios de alto nivel y la supervisión del sistema de servidores de nombres raíz. Debido a que las direcciones en Internet deben ser únicas y a que el espacio de direcciones en Internet es limitado, existe la necesidad de que una organización controle y asigne bloques de direcciones. En 1997 la IANA le dio a ARIN esta responsabilidad para la región de América y parte de África. Así, junto con RIPE en Europa y APNIC en Asia-Pacífico, estas organizaciones manejan la asignación de direcciones IP en todo el mundo. Bajo la ICANN, la IANA continúa distribuyendo direcciones a los Registros

de Internet Regionales, coordina con el IETF y otros organismos para asignar parámetros de protocolos, y supervisar la operación de los DNS.

ICANN (*Internet Corporation for Assigned Names and Numbers*): Organización sin fines de lucro formada para asumir la responsabilidad de la asignación del espacio de direcciones IP, la asignación de parámetros de protocolo, administración del sistema de nombres de dominio, y las funciones de administración del sistema servidor raíz, antes realizadas bajo contrato con el gobierno de los Estados Unidos, por la IANA y otras entidades.

ICMP (*Internet Control Message Protocol*): Protocolo estándar de mensajes de control y error para sistemas IP. Fue definido en el RFC 792 y opera en la capa de red (IP). Los mensajes ICMP más conocidos son el *Echo Request* (Solicitud de Eco) y el *Echo Reply* (Respuesta de Eco) usados por PING.

IDEA (*International Data Encryption Algorithm*): Algoritmo de Cifrado de Datos Internacional—Desarrollado en Europa como una alternativa a los cifradores Estadounidenses, tales como DES. IDEA es un cifrador de bloque que usa bloques de 64 bits y llaves de 128 bits.

IEEE (*Institute of Electrical and Electronics Engineers*): Instituto de Ingenieros Eléctricos y Electrónicos–Organización de profesionales en ingeniería eléctrica y electrónica cuyas

actividades incluyen el desarrollo de estándares de comunicaciones y de redes. Los estándares de la IEEE para LANs son los más usados hoy en día.

IETF (*Internet Engineering Task Force*): Comunidad abierta formada por diseñadores de red, operadores, fabricantes e investigadores cuyo propósito es coordinar la operación, administración y evolución de Internet, y resolver asuntos relacionados con protocolos y arquitecturas de red, de corto y mediano alcance. Es una fuente de propuestas de estándares de protocolos que son enviados a la IAB (*Internet Architecture Board*) para su aprobación final. El IETF se reúne tres veces al año.

IKE (*Internet Key Exchange*): (1) Servicio de negociación de seguridad automática y administración de llaves criptográficas, usado con los protocolos IPSec. (2) Protocolo de intercambio de llaves, anteriormente conocido como ISAKMP/Oakley, empleado para intercambiar llaves criptográficas y establecer automáticamente asociaciones de seguridad.

***Intranet*:** Red privada dentro de una empresa u organización.

Internet: Red de redes de diseño descentralizado que interconecta millones de computadoras entre sí usando los protocolos TCP/IP. *Internet* evolucionó de la red ARPANET desarrollada en los 60's por el Departamento de Defensa de los Estados Unidos. Posteriormente creció para incluir instituciones educativas y de investigación.

IP (*Internet Protocol*): Protocolo de la capa de red que se encarga de fragmentar y encapsular en paquetes o datagramas la información proveniente de las capas superiores, y encaminarla desde su origen hacia su destino. Para esto se vale de la información contenida en la cabecera de los paquetes, la cual incluye dirección origen, destino, tiempo de vida, posición relativa del fragmento, tipo de servicio o prioridad, entre otros campos de control. La versión 4 de este protocolo es actualmente usada en Internet.

IPSec (*IP Security*): Infraestructura o conjunto de protocolos de seguridad de la IETF que buscan proteger las comunicaciones de red (típicamente sobre Internet) mediante cifrado, autenticación, protección *anti-replay* y protección contra análisis de flujos de tráfico, manteniendo la confidencialidad e integridad de la información.

ISDN (*Integrated Services Digital Network*): Estándar de Comunicaciones Internacional que posibilita la transmisión de señales digitales, en vez de analógicas, a través de líneas telefónicas tradicionales, permitiendo el envío y recepción de datos, voz y video a velocidades mayores que las proporcionadas por módems tradicionales. Hay dos tipos básicos de servicios ISDN: BRI (*Basic Rate Interface*) o interfaz de tasa básica que proporciona hasta 2 canales de datos de 64 kbps, y PRI (*Primary Rate Interface*) o interfaz de tasa primaria, que apunta a usuarios con requerimientos de capacidad mayores, proporcionando en el estándar europeo hasta 30 canales de 64 kbps.

ISO (*International Standards Organization*): Organización que crea estándares internacionales, incluyendo estándares de criptografía.

ISP (*Internet Service Provider*): Proveedor de Servicios de Internet.

***Kernel*:** Núcleo de un sistema operativo. El *Kernel* administra los recursos de la máquina, incluyendo el procesador, la memoria, los discos y dispositivos periféricos, los procesos, etc; y controla la manera como otro software componente puede acceder a estos recursos. El *Kernel* corre con un nivel de privilegios superior al de otros programas. La potencia y robustez del *Kernel* de un sistema operativo define en gran medida el desempeño general del sistema y su confiabilidad.

LAN (*Local Area Network*): Red de Área Local—Red de computadoras y otros dispositivos, que cubre un área geográfica limitada, típicamente una oficina, un edificio o un campus.

***Laptop*:** Computadora portátil.

MAC: (1) (*Media Access Control*) Control de Acceso al Medio—Subcapa inferior de las dos existentes en la capa de Enlace de Datos, definida por la IEEE. La subcapa MAC maneja el acceso al medio compartido, especificando si se va a usar un esquema de contención o de estafeta circulante. **(2) (*Message Authentication Code*)** Código de Autenticación de Mensaje—Etiqueta de autenticación, también llamada *checksum*, obtenida como resultado de

la aplicación de un esquema de autenticación y de una llave secreta sobre un mensaje. Las MACs son calculadas y verificadas con la misma llave de tal manera que solo puedan ser verificadas por el receptor.

MD5 (*Message Digest 5*): Algoritmo matemático que produce un *hash* seguro o compendio de mensaje. Si se cambiara algún carácter en el mensaje, el *digest* o compendio sería completamente diferente. Esta característica forma parte de una etapa vital al momento de producir una firma digital.

MIB (*Managemente Information Base*): Es una descripción formal de un conjunto de objetos de red que pueden ser administrados usando el protocolo SNMP (*Simple Network Management Protocol*). El formato de la MIB es definido como parte de SNMP. Todo el resto de MIBs son extensiones de esta MIB básica. Los desarrolladores de productos pueden crear y registrar nuevas extensiones MIB.

Módem (Modulador-Demodulador): Dispositivo en hardware que convierte señales digitales de computadoras en señales analógicas que pueden ser transmitidas sobre líneas telefónicas. Los módems tradicionales pueden transportar datos a velocidades de hasta 56 kbps.

Modo Promiscuo: Dícese de un dispositivo de red que captura todos los paquetes del medio al que está conectado sin importar a quién estén dirigidos.

Módulo: En matemáticas, un número mediante el cual se puede multiplicar logaritmos de un sistema para obtener los logaritmos de otro sistema.

***Multicast*:** Paquete enviado desde un nodo a múltiples nodos (no a todos los nodos existentes) de una red o subred. Es una comunicación punto-multipunto, usualmente usada para transmitir grandes volúmenes de información, como en el caso de vídeo, desde un host origen a múltiples host destino de manera simultánea. De esta forma, se optimiza el ancho de banda, pues la información viaja en un solo flujo hasta el punto más cercano a los destinos o hasta un punto de redistribución estratégicamente elegido.

NAS (*Network Access Server*): Servidor de Acceso a Red--Ver Servidor de Acceso.

NAT (*Network Address Translation*): Mecanismo de traducción de direcciones IP, usadas en una red, a direcciones IP distintas, conocidas dentro de otra red. Una red es denominada como interna y la otra como externa. Típicamente una organización asocia o "mapea" sus direcciones IP internas locales a una o más direcciones IP globales externas, y hace lo opuesto para paquetes entrantes. NAT permite mejorar la seguridad ya que cada comunicación saliente o entrante debe pasar por un proceso de traducción que también ofrece la oportunidad de distinguir o autenticar la solicitud, o ver si coincide con una solicitud previa. NAT también ayuda a conservar el número de direcciones IP globales que una organización necesita, e incluso permite que la organización emplee una sola dirección IP pública para sus

comunicaciones en Internet. NAT se implementa en servidores, ruteadores, firewalls, y en general en puertas de enlace a otras redes.

Nonce: Número aleatorio que varía con el tiempo y que es usado en protocolos de autenticación.

OFDM (*Orthogonal Frequency Division Multiplexing*): Método de modulación digital en el que la señal es separada en varios canales de banda angosta en diferentes frecuencias. OFDM es similar a la multiplexación por división de frecuencia tradicional (FDM). La diferencia radica en la manera en la que la señal es modulada y demodulada. Se le da prioridad a minimizar la interferencia (*crosstalk*) entre los canales que componen el flujo de datos. Se le pone menor énfasis en mejorar canales individuales.

OSI (*Open Systems Interconnection*): Modelo o arquitectura de siete capas desarrollado por la ISO para la interconexión de sistemas de comunicación de datos. Cada capa usa y se construye sobre los servicios provistos por aquellas debajo suyo. Es un programa de estandarización internacional para facilitar la comunicación entre sistemas de computadoras de diferentes fabricantes. Las siete capas son: 1) Física, 2) Enlace de datos, 3) Red, 4) Transporte, 5) Sesión, 6) Presentación, y 7) Aplicación.

PAP (*Password Authentication Protocol*): Protocolo de seguridad para autenticación usado en conexiones punto a punto PPP. El dispositivo que intenta conectarse debe enviar primero

su nombre de usuario y contraseña para poder ser validado. Esta información de autenticación es enviada en texto llano.

PAT (*Port Address Translation*): Función provista por dispositivos de red como ruteadores y firewalls, que permite a los hosts en una red comunicarse con otra red (e.g. Internet) sin revelar su dirección IP interna. A todos los paquetes salientes se les traduce su dirección IP origen por la dirección IP externa del dispositivo, y su puerto (TCP o UDP) origen por un puerto (TCP o UDP) disponible en la parte externa, a manera de poder distinguir los flujos para que los paquetes de regreso lleguen a su origen.

PDU (*Protocol Data Unit*): Mensaje de un protocolo dado que comprende la carga útil e información de control específica del protocolo, típicamente contenida en un encabezado. Los PDUs pasan por las interfases que existen entre las capas de protocolos (según el modelo OSI).

PEAP (*Protected Extensible Authentication Protocol*): Protocolo de Autenticación Extensible Protegido—Protocolo desarrollado conjuntamente por Microsoft, RSA Security y Cisco para transmitir información de autenticación, incluyendo contraseñas, a través de redes wireless. PEAP autentica a clientes LAN wireless usando certificados digitales solamente en el lado del servidor, creando túneles cifrados SSL/TLS entre el cliente y el servidor de autenticación. El túnel luego protege el intercambio subsiguiente de autenticación del usuario.

PEAP proporciona seguridad fuerte, extensibilidad de la base de datos de usuarios, soporte para autenticación con OTPs y caducidad de contraseñas.

***Peer*:** (1) Par o entidad al mismo nivel o capa. (2) Relación entre dispositivos de red que tienen mutuo acceso a recursos.

PKI (*Public Key Infrastructure*): Infraestructura de Llave Pública—Sistema que permite la creación, certificación y administración del tiempo de vida de certificados digitales para usuarios u otros sistemas. Los certificados digitales resultantes pueden ser usados para procesos de autenticación y cifrado dentro de IPSec, SSL, correo electrónico seguro y otras aplicaciones criptográficas. Incluye el uso de certificados digitales y autoridades certificadoras, así como el hardware y software empleado para administrar el proceso.

***Playback*:** Ver *Replay*.

POP3 (*Post Office Protocol 3*): La más reciente versión del protocolo estándar para la recepción de correo electrónico. POP3 es un protocolo cliente/servidor mediante el cual el cliente de correo se comunica con el servidor de correo para descargar los mensajes.

PPP (*Point-to-Point Protocol*): Es un protocolo de capa dos del modelo OSI, que proporciona un método estándar para transportar datagramas de múltiples protocolos sobre enlaces punto a punto. PPP está conformado por tres elementos principales: 1) Un método

para encapsular datagramas multi-protocolo. 2) Un protocolo de control de enlace (LCP: *Link Control Protocol*) para establecer, configurar y probar la conexión de enlace de datos, y 3) Una familia de protocolos de control de red (NCP: *Network Control Protocol*) para establecer y configurar diferentes protocolos de la capa de red.

Proxy: Programa o software intermediario que actúa como servidor único ante los clientes internos de una red local, y como cliente delegado ante los servidores de Internet. Es decir, atiende las consultas de los clientes (destinadas a servidores en Internet), actuando en su representación y ocultándolos. De esta manera, centraliza el tráfico entre Internet y una red privada, evitando que cada una de las máquinas de la red interna tenga que disponer necesariamente de direcciones IP públicas o conexiones directas a Internet. Un *proxy* puede disponer, adicionalmente, de caché o almacenamiento local de páginas o destinos más frecuentados para acelerar la navegación. Puede, asimismo, disponer de mecanismos de seguridad (firewall) los cuales impiden accesos no autorizados desde el exterior hacia la red privada.

PSTN (*Public Switched Telephone Network*): Servicio de comunicación de voz y datos de baja velocidad para el público en general que usa un sistema de líneas conmutadas. Es el servicio telefónico tradicional brindado a la mayoría de hogares en el mundo.

Puerta de enlace: Ver *Gateway*.

Punto de Acceso: Un punto de acceso wireless es un concentrador que interconecta a dispositivos wireless clientes con una LAN u otra red cableada. Un punto de acceso puede ser un dispositivo en hardware independiente o una computadora con una tarjeta de red wireless y el software adecuado.

QoS (*Quality of Service*): Calidad de Servicio—Capacidades de un dispositivo de red para proporcionar un nivel garantizado de desempeño tal como prioridad en la entrega de tráfico, ancho de banda o velocidad, latencia o retardos, y variación en los retardos. Proporcionar audio o video de buena calidad en una red, usualmente requiere de capacidades QoS.

RADIUS (*Remote Authentication Dial-In User Service*): Protocolo cliente/servidor y software que permiten a servidores de acceso remoto comunicarse con un servidor central, para autenticar a usuarios que intentan acceder a una red, y autorizar su acceso al sistema o servicio solicitado.

RAS (*Remote Access Server*): Servidor de Acceso Remoto. Ver Servidor de Acceso.

***Replay*:** Ataque que busca engañar a un sistema retransmitiendo un mensaje legítimo. Algunos protocolos incluyen mecanismos *anti-replay* para detectar y rechazar tales ataques.

Repudiación: La repudiación es la noción de negar que se haya producido una acción. Un ejemplo de repudiación sería negar que se haya recibido un elemento cuando en realidad sí se

ha recibido y esperar a que el proveedor proporcione otro. Por otro lado, deben registrarse las acciones que se no se desean que sean realizadas por un usuario no autorizado. Dicha no repudiación también puede obtenerse mediante el uso de firmas digitales y marcas de tiempo.

RDSI (Red Digital de Servicios Integrados): Ver ISDN.

RealAudio: Software comercial que toca archivos de audio en demanda, sin esperar a que terminen las largas transferencias de dichos archivos.

RFC (*Request for Comments*): Nombre del resultado y el proceso para crear un estándar en Internet. Los nuevos estándares son propuestos y publicados en Internet como RFCs. Las propuestas son revisadas por la IETF, una organización que busca el consenso y facilita la discusión; y eventualmente se establece un nuevo estándar. Sin embargo, el nombre o número de referencia del estándar retiene el acrónimo RFC. Los RFCs son documentos técnicos y administrativos acerca de Internet, que empezaron en 1969, y que abarcan diversos aspectos de las redes de computadoras, incluyendo protocolos, procedimientos, programas, recomendaciones, entre otros.

RIPE (*Réseaux IP Européens*): Forum de colaboración abierto a todas las partes interesadas en redes de área amplia (WAN) IP en Europa y más allá. El objetivo de RIPE es asegurar la coordinación administrativa y técnica necesaria para permitir la operación de una red pan-europea.

Router: Ver Ruteador.

RPC (*Remote Procedure Call*): Interfaz de programación que permite a un programa usar los servicios de otro programa en una máquina remota. El programa solicitante envía un mensaje e indicaciones al programa remoto, el cual las ejecuta y envía los resultados al programa solicitante. RPC es un modelo popular para implementar entornos cliente/servidor distribuidos.

RSA (Rivest, Shamir, Adleman): Algoritmo criptográfico de llave pública usado para cifrar mensajes y crear firmas digitales. RSA permite al usuario generar dos llaves criptográficas distintas pero relacionadas entre sí, siendo imposible calcular el valor de una llave a partir de la otra. Una de las llaves puede ser hecha pública, mientras que la otra debe ser privada, es decir, conocida solo por el usuario. Un mensaje cifrado con la llave pública sólo puede ser descifrado con la correspondiente llave privada. Este algoritmo fue desarrollado en 1977 por Ron Rivest, Adi Shamir, y Leonard Adleman. La empresa RSA Data Security Inc. toma el nombre de este algoritmo y adquiere los derechos sobre las patentes. Actualmente, RSA es el algoritmo de cifrado y autenticación más usado, y forma parte de navegadores de Internet como Netscape y Microsoft, entre otros muchos productos.

RTC (Red Telefónica Conmutada): Ver PSTN.

Ruteador: Dispositivo (o software) de propósito específico que maneja la conexión entre dos o más redes de conmutación por paquetes. Su principal función es la de examinar la dirección origen y destino de los paquetes que pasan a través de él, y decidir, bajo determinados criterios, por qué ruta enviarlos. Típicamente opera en la capa de red del modelo de referencia OSI, pero actualmente su funcionalidad se extiende a otras capas.

SA (*Security Association*): Ver Asociación de Seguridad.

Script: En programación de computadoras, un *script* es un programa o secuencia de instrucciones que son interpretadas o llevadas a cabo por otro programa y no directamente por el procesador de instrucciones de la computadora (como lo son los programas compilados). Algunos lenguajes *script* comunes son Perl, JavaScript y Visual Basic Script.

Servidor de Acceso: Dispositivo que conecta, a una red, distintos tipos de dispositivos de comunicaciones (usualmente remotos) y líneas de telecomunicaciones, proporcionando encaminamiento dentro de la red, y mecanismos de validación, entre otros.

SHA-1 (*Secure Hash Algorithm* 1ra revisión): Algoritmo de *hash* de un solo sentido, que produce una representación condensada de 160 bits, de un mensaje o información de cualquier longitud. El mensaje condensado o *message digest* puede ser ingresado al algoritmo de firmas digitales DSA (*Digital Signature Algorithm*) para generar o verificar la firma del mensaje. SHA fue desarrollado por la Agencia de Seguridad Nacional de los Estados Unidos

(NSA), y es una variante mejorada del algoritmo MD4. Ya que SHA genera un *hash* de 168 bits, es más resistente a ataques que MD5 (128 bits de *hash*), pero a la vez más lento.

***Shell*:** Intérprete de comandos o interfaz en software entre el usuario y el sistema operativo, que acepta comandos e invoca a los programas correspondientes.

Sistema de Información (IS): Es el conjunto de recursos humanos y técnicos que proveen almacenamiento, poder computacional, distribución y comunicación de la información requerida por toda o alguna parte de una organización.

Sistema Operativo: Software que controla la ejecución de programas. Un conjunto ordenado de rutinas y procedimientos para operar una computadora o sistema.

SLIP (*Serial Line Internet Protocol*): (1) Protocolo de paquetes serial usado para conectar un computadora remota a Internet usando módems o líneas seriales directas. SLIP requiere un proveedor de Internet con cuentas SLIP especiales o un emulador de cuentas SLIP. (2) Protocolo antecesor de PPP, empleado en conexiones seriales punto a punto usando TCP/IP.

SMTP (*Simple Mail Tranfer Protocol*): Protocolo de la familia TCP/IP usado para transferir correos electrónicos entre servidores. SMTP fue especificado en el RFC 821.

***Sniffer*:** Programa y/o dispositivo que monitorea y captura la información que viaja en una red. Los *sniffers* pueden ser usados para funciones de administración de red legítimas como auditorías o diagnósticos de anomalías de red, pero también pueden ser usados para robar información de una red.

***Sniffing*:** Término usado para describir el uso de un programa *sniffer* en una red, para monitorear y capturar tráfico de datos, con la finalidad de obtener acceso a la información. Es la interceptación pasiva de transmisiones de datos en una red.

SNMP (*Simple Network Management Protocol*): Protocolo de administración de redes TCP/IP que permite el monitoreo y control de dispositivos de red, administra las configuraciones, la recolección de estadísticas, el desempeño y la seguridad. SNMP usa MIBs (*Management Information Bases*) o bases de administración de la información, las que definen qué información está disponible desde cualquier dispositivo de red administrable.

S.O.: Sistema Operativo

***Software*:** Programa o conjunto de instrucciones. Se divide en dos categorías: Software del Sistema, que controla el comportamiento y funcionamiento del sistema (e.g. Sistema Operativo y programas afines), y Software de Aplicaciones, que realiza tareas específicas de procesamiento de información (e.g. Procesadores de palabras, hojas de cálculo, bases de datos)

SQL (*Structured Query Language*): Lenguaje de Consultas Estructurado—Lenguaje usado por bases de datos relacionales para hacer consultas, actualizaciones o administrar información.

SSID (*Service Set Identifier*): Identificador de una red LAN wireless que los dispositivos wireless deben usar para poder comunicarse con el concentrador o punto de acceso wireless respectivo. El SSID es una cadena alfanumérica de hasta 32 caracteres.

SSL (*Secure Socket Layer*): Protocolo que cifra las comunicaciones entre servidores Web y navegadores Web cliente, creando túneles sobre Internet. Proporciona cifrado de información, autenticación de servidores e integridad de mensajes.

SSH (*Secure Shell*): SSH es un programa de interfaz de usuario seguro, que puede usarse para acceder a un dispositivo remoto y ejecutar comandos. Fue desarrollado por SSH Communication Security Inc., y proporciona autenticación fuerte y comunicación segura sobre enlaces no seguros.

SYN (*Synchronize*): Bit de control en la cabecera TCP, usado al inicio de la conexión para indicar a la otra parte el número de secuencia con el que se va a empezar.

***Switch*:** En una LAN, un *switch* es un dispositivo que permite interconectar múltiples dispositivos de red entre sí. Cuando un *switch* recibe tramas o paquetes de datos por un

puerto, consulta su tabla interna y envía dichos paquetes sólo al puerto al que está conectado el destinatario. Sólo si no existe un registro en su tabla para dicho destinatario, envía el paquete a todos los puertos (*broadcast* o difusión), esperando que el destinatario sea alcanzable por alguno de sus puertos. Cuando el destinatario responde al *broadcast*, el *switch* aprende y crea un registro en su tabla, asociando al destinatario con el puerto por el cual vino la respuesta. Un *switch* permite mejorar el desempeño de la red al separar dominios de colisión, es decir, reduce la competencia por el acceso al medio y por el ancho de banda. Tradicionalmente un *switch* opera en la Capa 2 del modelo de referencia OSI, trabajando en base a direcciones físicas MAC (*Media Access Control*) de los dispositivos de red. Sin embargo, actualmente los *switches* poseen cada vez mayor inteligencia, incluyendo funcionalidades de capas superiores.

TACACS (*Terminal Access Controller Access Control System*): Sistema de Control de Acceso, Controlador de Acceso Terminal—Protocolo para autenticar a usuarios que buscan obtener acceso a dispositivos de red como ruteadores y servidores de acceso remoto.

TCP (*Transmission Control Protocol*): Protocolo de Control de la Transmisión—Protocolo orientado a la conexión de la capa de transporte del modelo de referencia OSI, que forma parte del conjunto de protocolos o "suite" TCP/IP. Dentro de las tareas de TCP se encuentran la segmentación de la información en paquetes, el reensamblado de los paquetes en el lado destino, el control de flujo de extremo a extremo, y la solicitud de retransmisión de paquetes perdidos o dañados. Un segmento o paquete TCP incluye campos para especificar el puerto

origen y el puerto destino, permitiendo distinguir entre diferentes aplicaciones en la máquina origen y destino.

***Telnet*:** Protocolo de emulación de terminal, comúnmente usado en redes basadas en TCP/IP. *Telnet* permite acceso remoto en texto llano a dispositivos administrados, proporcionando así, un método poco seguro de administración remota. La iniciación de una sesión *telnet* requiere que el usuario acceda al dispositivo ingresando credenciales de autenticación válidas, las que normalmente consisten en un nombre de usuario y contraseña.

TKIP (*Temporal Key Integrity Protocol*): Protocolo de Integridad de Llave Temporal—Parte del estándar 802.11i de la IEEE para cifrado en redes wireless. TKIP proporciona mezclado de llaves por paquete, chequeo de integridad de mensajes y un mecanismo de reciclado de llaves, solucionando las debilidades de WEP.

TLS (*Transport Layer Security*): Seguridad en Capa de Transporte—Protocolo estándar del IETF cuya intención es asegurar y autenticar las comunicaciones a través de redes públicas usando cifrado de datos. TLS proporciona privacidad e integridad de la información. TLS ha sido diseñado para ser el sucesor de SSL, y emplea los mismos métodos criptográficos pero soporta más algoritmos criptográficos.

***Trailer*:** Información de control de protocolo localizada al final del PDU

***Trap*:** Mecanismo de interrupción de programa que automáticamente actualiza a un host de administración de red SNMP sobre el estado de algún parámetro en el dispositivo administrado.

UDP (*User Datagram Protocol*): Protocolo de Datagrama de Usuario—Protocolo no orientado a la conexión que opera en la capa de transporte del modelo de referencia OSI, y forma parte de la "suite" TCP/IP. UDP proporciona intercambio de datagramas sin acuse de recibo ni garantías en la entrega. Un datagrama UDP incluye campos para especificar el puerto origen y el puerto destino, permitiendo distinguir entre diferentes aplicaciones en la máquina origen y destino.

***Unicast*:** (1) Paquete destinado a una sola dirección en una red. (2) Una dirección que solo un host reconocerá.

***Upgrade*:** Actualización de un producto en software o hardware, que provee mejoras con respecto a la versión anterior.

VLAN (*Virtual Local Area Network*): Una VLAN o Red de Área Local Virtual es un grupo lógico de dispositivos que aparentan estar en la misma LAN, independientemente de su ubicación física. Las VLANs permiten a los administradores de red dividir sus redes físicas en grupos más pequeños de redes lógicas. Al igual que las LANs, las VLANs consisten de un único dominio de *broadcast* o de difusión que se encuentra aislado de otras VLANs. El

funcionamiento de las VLANs se basa en el empleo de etiquetas para marcar los paquetes recibidos en puertos predefinidos, como pertenecientes a una VLAN determinada, y restringiendo su transmisión a otros puertos que no pertenezcan a dicha VLAN. Para intercambio de paquetes entre puertos conectados a otros switches, se usan puertos troncales configurados con mecanismos de etiquetado tales como 802.1q de la IEEE.

VLAN Privada: Funcionalidad adicional de Capa 2 del modelo de referencia OSI, presente en algunas marcas de switches que permite, dentro de una VLAN determinada, configurar a ciertos puertos como protegidos o aislados, los que no podrán enviar tráfico directamente a otros puertos configurados de la misma manera. Para que este envío se realice, todo el tráfico de dichos puertos deberá pasar antes por un dispositivo de Capa 3. El envío de tráfico entre estos puertos especialmente configurados y otros no configurados de esta manera, llamados no protegidos o promiscuos, deberá proceder de manera normal. Los puertos no protegidos o promiscuos podrán comunicarse con cualquier puerto de la VLAN privada. Adicionalmente, se da la posibilidad de crear comunidades, formadas por puertos aislados que podrán comunicarse entre sí y con puertos promiscuos, mas no con puertos aislados pertenecientes a otras comunidades.

WAN (*Wide Area Network*): Red de Área Amplia—Red física o lógica que proporciona la capacidad para que múltiples dispositivos se comuniquen entre sí, a través de una topología de transmisión interconectada común, en áreas geográficas mucho más amplias que aquellas

cubiertas por las redes de área local (LANs), tales como estados, países y el mundo. El mejor ejemplo de WAN pública es la Internet.

WEP (*Wired Equivalent Privacy*): Privacidad Equivalente a aquella de una Red Cableada—Método de cifrado de datos definido por el estándar 802.11, diseñado para prevenir el acceso de intrusos a una red wireless y la captura del tráfico LAN wireless a través de la interceptación. Con WEP, la información que viaja entre el punto de acceso wireless y el dispositivo wireless es cifrada usando llaves de 64, 128 o 256 bits. WEP ha probado ser inseguro.

WLAN (*Wireless Local Area Network*): Red de área local inalámbrica, es decir que usa como medio de transmisión el aire y transmite, típicamente, en una banda de frecuencia no licenciada como la banda de 2.4GHz. Una LAN wireless no requiere que los dispositivos wireless estén alineados de tal manera que haya línea de vista entre sí. Los puntos de acceso (AP) wireless o estaciones base, que también tienen conexión con la red cableada Ethernet, transmiten a una frecuencia de radio con un alcance de algunos cientos de metros, y pueden penetrar paredes y otras barreras no metálicas. Los clientes wireless son *laptops*, estaciones de trabajo o dispositivos electrónicos portátiles conocidos como PDAs (*Personal Digital Assistants*) que tienen tarjetas de red wireless. Los estándares de la IEEE para redes LAN wireless son el 802.11 y sus variantes 802.11a, b y g.

BIBLIOGRAFÍA

LIBROS

[1] Greg Bastien, Christian Abera Degu, "CCSP SECUR Exam Certification Guide" Cisco Press, – E.E.U.U, 2004.

[2] Ido Dubrawsky, Paul Grey, "CCSP Self-Study CCSP CSI Exam Certification Guide", Cisco Press – E.E.U.U, 2004.

DOCUMENTACIÓN ELECTRÓNICA: RFCs (*Request for Comments*)

[3] Information Sciences Institute University of Southern California, "RFC 791 - Internet Protocol (IP)", Network Working Group – setiembre, 1981.

[4] J. Postel, "RFC 792 - Internet Control Message Protocol (ICMP)", Network Working Group – setiembre, 1981.

[5] Information Sciences Institute University of Southern California, "RFC 793 - Transmission Control Protocol (TCP)", Network Working Group – setiembre, 1981.

[6] K. Lougheed, Y. Rekhter, "RFC 1163 - Border Gateway Protocol (BGP)", Network Working Group – junio, 1990.

[7] B. Lloyd, W. Simpson, "RFC 1334 - PPP Authentication Protocols", Network Working Group – octubre, 1992.

[8] W. Simpson, "RFC 1661 - The Point-to-Point Protocol (PPP)", Network Working Group – julio, 1994.

[9] Y. Rekhter, T. Li, "RFC 1771 - A Border Gateway Protocol 4 (BGP-4)", Network Working Group – marzo, 1995.

[10] Y. Rekhter, B. Moskowitz, D. Karrenberg, G.J. de Groot, E. Lear, "RFC 1918 - Address Allocation for Private Internets", Network Working Group – febrero, 1996.

[11] W. Simpson, "RFC 1994 - PPP Challenge Handshake Authentication Protocol (CHAP)", Network Working Group – agosto, 1996.

[12] B. Fraser, "RFC 2196 - Site Security Handbook", Network Working Group – setiembre, 1997.

[13] S. Kent, R. Atkinson, "RFC 2401 - Security Architecture for the Internet Protocol", Network Working Group – noviembre, 1998.

[14] S. Kent, R. Atkinson, "RFC 2402 - IP Authentication Header", Network Working Group – noviembre, 1998.

[15] S. Kent, R. Atkinson, "RFC 2406 - IP Encapsulating Security Payload (ESP)", Network Working Group – noviembre, 1998.

[16] D. Maughan, M. Schertler, M. Schneider, J. Turner, "RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP)", Network Working Group – noviembre, 1998.

[17] D. Harkins, D. Carrel, "RFC 2409 - The Internet Key Exchange (IKE)", Network Working Group – noviembre, 1998.

[18] H. Orman, "RFC 2412 - The OAKLEY Key Determination Protocol", Network Working Group – noviembre, 1998.

[19] G. Zorn, S. Cobb, "RFC 2433 - Microsoft PPP CHAP Extensions", Network Working Group – octubre, 1998.

[20] E. Rescorla, "RFC 2631 - Diffie-Hellman Key Agreement Method", Network Working Group – junio, 1999.

[21] B. Ferguson, D. Senie, "RFC 2827 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", Network Working Group – mayo, 2000.

[22] S. Farrell, J. Vollbrecht, P. Calhoun, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence, "RFC 2906 - AAA Authorization Requirements", Network Working Group – agosto, 2000.

ENLACES EN INTERNET

[23] www.cisco.com/go/safe

[24] www.faqs.org/rfc

[25] www.nsa.gov