Prólogo

Este libro presenta los mecanismos de seguridad desplegados en las redes Ethernet, Wi-Fi (*Wireless-Fidelity*), IP (*Internet Protocol*) y MPLS (*Multi-Protocol Label Switching*). Estos mecanismos se clasifican en función de las cuatro funciones siguientes:

– protección de datos;

– control de acceso;

– partición de la red;

– monitorización de datos.

La protección de datos es proporcionada por los servicios de confidencialidad y control de la integridad de los datos:

– La confidencialidad consiste en garantizar que los datos sólo puedan ser interpretados por personas autorizadas; este servicio se obtiene a través del mecanismo de cifrado de los datos en cuestión;

– la verificación de la integridad consiste en detectar cambios en los datos transferidos; este servicio se obtiene a partir de una función *hash* o de un algoritmo de cifrado que genera un sello.

El control de acceso lo proporciona el servicio de autentificación de un tercero. Este servicio consiste en verificar la identidad de la persona que desea acceder a una red. Este servicio se obtiene normalmente a partir de una función *hash*, como la verificación de la integridad.

La partición de red es proporcionada por el servicio de *red privada virtual* (VPN, *Virtual Private Network*). Este servicio permite formar grupos de usuarios cerrados y

la comunicación sólo entre usuarios pertenecientes al mismo grupo. Cabe señalar que el control de acceso también permite la partición implícita de la red.

El monitoreo de datos consiste en la aplicación de reglas de datos que permiten su transferencia o la detección de ataques. El servicio se provee en base al análisis de los campos que los diferentes protocolos agregan a la estructura de datos transmitida.

La red

El rol de la red apunta al enrutamiento de datos entre dos *hosts*. La red consta de dos entidades (figura 1):

– *Red de Área Local* (LAN, *Local Area Network*) es la red a la que se conectan los *hosts;* por lo general, se trata de una red privada desplegada por empresas;

– *Red de Área Amplia* (WAN, *Wide Area Network*) es la red que interconecta las LANs; se trata generalmente de una red pública desplegada por operadores de acceso y tránsito a Internet.

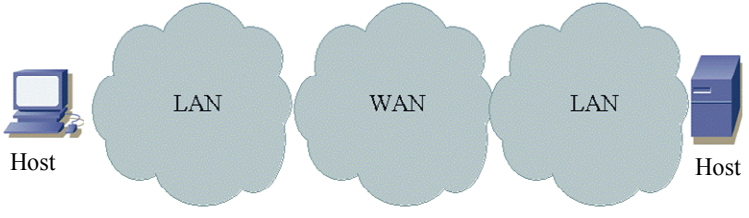

Figura 1. *La arquitectura de la red*

La LAN se construye a partir de dos tipos de bloques: el bloque de acceso y el bloque central (figura 2):

– el bloque de acceso conecta los *hosts* de red; los bloques de acceso pueden aplicarse a diferentes tipos de *host*:

- computadoras, teléfonos;
- servidores de aplicaciones;
- la red y el sistema operativo de seguridad;
- la WAN;
- el bloque central permite interconectar los bloques de acceso.

La WAN del proveedor de servicios de Internet está estructurada en tres entidades (figura 3):

– la red de acceso: corresponde a la conexión de la LAN al primer sitio técnico del operador;

– la red de agregación: recoge el tráfico de las redes de acceso; por lo general, tiene una cobertura regional;

– la red básica: conecta las diferentes redes de agregación; por lo general, tiene cobertura nacional; también proporciona la interfaz entre los operadores.

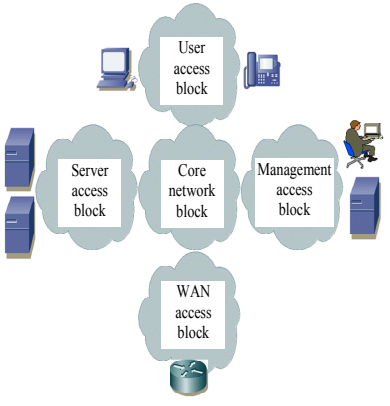

Figura 2. *Arquitectura de la LAN*

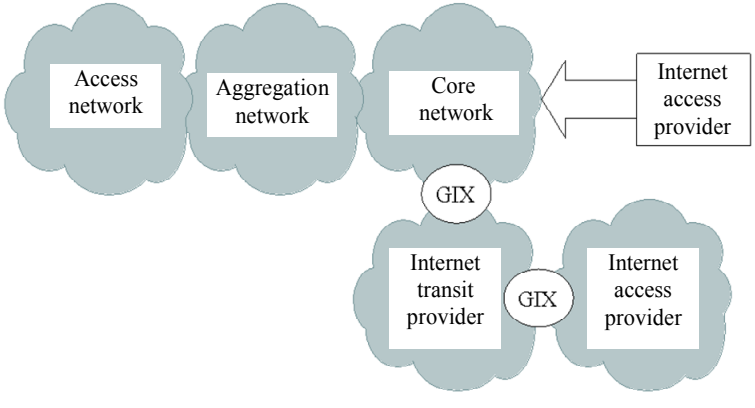

Figura 3. *Arquitectura de la WAN*

La interconexión de las WANs de los distintos proveedores de servicios de Internet se realiza al nivel de la red básica de dos maneras diferentes:

– conexión directa, cuando los proveedores de servicios de Internet operan en el mismo territorio;

– conexión realizada por un proveedor de tránsito de Internet, si no es el caso anterior; la red de tránsito de Internet tiene una arquitectura similar a la de la red central del proveedor de servicios de Internet.

Un *punto de intercambio* (GIX, *Global Internet eXchange*) permite a los distintos proveedores de acceso y tránsito a Internet intercambiar tráfico a través de acuerdos de *interconexión* mutua, generalmente basados en el equilibrio de volumen de datos transmitidos y recibidos (figura 3).

Introducción a la criptografía

El capítulo 1 presenta los conceptos básicos de la criptografía. La criptografía aborda los aspectos de seguridad de las comunicaciones, con el objetivo de proporcionar servicios de confidencialidad, control de integridad y autentificación de terceros.

El servicio de confidencialidad se implementa mediante mecanismos de cifrado. Existen dos familias principales de algoritmos criptográficos: los algoritmos simétricos de clave secreta y los asimétricos de clave pública y privada.

Los algoritmos simétricos son muy adecuados para el cifrado de datos, pero plantean el problema de establecer la clave secreta. Dos métodos de uso común son la generación a partir del algoritmo Diffie-Hellman y el transporte de la clave secreta usando algoritmos asimétricos. El cifrado se proporciona, por ejemplo, mediante el algoritmo *estándar de cifrado avanzado* (AES, *Advanced Encryption Standard*) o el algoritmo *estándar de cifrado triple de datos* (3DES, *Triple Data Encryption Standard*).

Los algoritmos asimétricos encuentran su campo de aplicación en el transporte de claves secretas y en la firma digital. En el primer caso, la clave secreta es cifrada por la clave pública y descifrada por la clave privada. En el segundo caso, ocurre lo contrario. El cifrado es proporcionado por algoritmos basados en la exponencialidad modular como el algoritmo RSA (nombrado por las iniciales de sus tres inventores Rivest, Shamir, Adleman) o el algoritmo de *cifrado de curvas elípticas* (ECC, *Elliptic Curve Cryptography*).

La función *hash* es otro tipo de función criptográfica. Convierte una cadena de cualquier longitud (los datos a proteger) en una cadena de menor tamaño y generalmente fijo (un compendio). La función *hash* puede ser ejecutada por los dos algoritmos siguientes:

– MD5 (*Message Digest 5*) que calcula un compendio de 128 bits;

– SHA (*Secure Hash Algorithm*) que calcula un compendio de 160 a 512 bits.

El sello se basa en la clave secreta y proporciona el servicio de control de la integridad de los datos. El sello puede calcularse de dos maneras diferentes:

– el algoritmo de cifrado simétrico se aplica a los datos, el sello es entonces el último bloque del criptograma;

– la función *hash* se aplica a un conjunto que comprende los datos y una clave secreta, cuya asociación se define, por ejemplo, mediante la función de cálculo HMAC (*Hashed Message Authentication Code*).

La firma se basa en el cifrado del compendio mediante una clave privada y el descifrado mediante una clave pública. Ésta proporciona el servicio de integridad y de no-repudio de la fuente de los datos recibidos por el destinatario.

La distribución de claves públicas está asociada a la presentación de un certificado. El certificado es una estructura de datos firmada por una autoridad de certificación que garantiza que el emisor de dicha clave pública es el titular.

El mecanismo 802.1x

El capítulo 2 presenta el mecanismo de control de acceso 802.1x desplegado en la LAN utilizando las tecnologías siguientes:

– Tecnología Ethernet en caso de acceso a un *switch*;

– Tecnología Wi-Fi en el caso de una conexión a un *punto de acceso* (AP, *Access Point*).

El mecanismo 802.1x define tres componentes (figura 4):

– el solicitante es el dispositivo (por ejemplo, un computador) que desea acceder a la red Ethernet o Wi-Fi;

– el autentificador es el dispositivo (*switch* Ethernet o punto de acceso Wi-Fi) que controla el acceso del solicitante a la LAN;

– el servidor de autentificación es el dispositivo que autentifica al solicitante y permite el acceso a la LAN.

El mecanismo 802.1x se basa en una serie de protocolos (figura 4):

– el *protocolo de autentificación extensible sobre LAN* (EAPOL, *Extensible Authentication ProtocolOver LAN*) intercambiado entre el solicitante y el autentificador;

– el *protocolo de autentificación extensible* (EAP, *Extensible Authentication Protocol*) intercambiado entre el solicitante y el autentificador o servidor de autentificación; el EAP es compatible con el EAPOL sobre la interfaz entre el solicitante y el autentificador;

– el protocolo RADIUS (*Remote Authentication Dial-In User Service*) intercambiado entre el autentificador de identificación y el servidor de autentificación; el protocolo RADIUS soporta el EAP en la interfaz entre el autentificador y el servidor de autentificación;

– el EAP-Method intercambiado entre el solicitante y el servidor de la solicitud; el EAP-Method está soportado por el EAP.

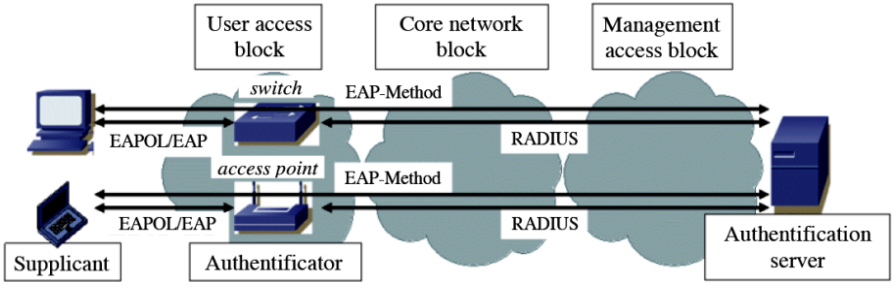

Figura 4. *El mecanismo 802.1x*

El EAP-Method ofrece varios tipos de autentificación:

– el método EAP-MD5: el cliente se identifica con una contraseña. Este método es similar al *protocolo CHAP* (*Challenge-Enlace Authentication Protocol*) basado en el *protocolo punto a punto* (PPP, *Point to Point Protocol*) utilizado para las conexiones punto a punto;

– el método EAP-TLS (*Transport Layer Security*): la autentificación es mutua entre el solicitante y el servidor de autentificación mediante certificados;

– el método EAP-TTLS (*Tunneled-TLS*): la autentificación es mutua entre el solicitante y el servidor de autentificación a través de un certificado de la parte del servidor de autentificación, el solicitante puede utilizar una contraseña.

Además de la autentificación, el EAPOL se utiliza para generar las claves de cifrado y control de integridad utilizadas por los mecanismos WPA1 (*Wi-Fi Protected Access*) y WPA2 descritos en el capítulo 3.

Mecanismos del WPA

El capítulo 3 presenta los mecanismos de seguridad WPA1 y WPA2 aplicados a la red Wi-Fi. La tecnología Wi-Fi es originalmente una tecnología para acceder a la LAN privada, utilizando la transmisión de radio. Su particularidad es la utilización de bandas de frecuencias libres. También se despliega en la WAN pública para crear *hotspots*.

Los mecanismos de seguridad WPA1 y WPA2 se utilizan únicamente en la red privada. La protección desplegada en el caso de los *hotspots* suele aplicar la protección del transporte descrita en el capítulo 5.

La seguridad de la interfaz de radio se inició con el mecanismo WEP (*Wired Equivalent Privacy*). Debido a sus debilidades, fue sustituido por el mecanismo WPA1 y luego por el mecanismo WPA2. Estos tres mecanismos implementan específicamente los servicios de control de acceso y protección de datos de terceros.

Para el mecanismo WEP, el control de acceso de terceros se basa en el algoritmo RC4 (*Rivest Cipher* 4). El control de acceso tiene lugar durante la fase de autentificación, que es un procedimiento asociado al protocolo de conexión de datos MAC (*Medium Access Control*).

Los mecanismos WPA1 y WPA2 utilizan el mecanismo 802.1x descrito en el capítulo 2 para el control de acceso. La fase de autentificación está precedida por el procedimiento para acordar la política de seguridad entre el punto de acceso y la estación.

Para los mecanismos WEP y WPA1, el cifrado se realiza mediante el algoritmo RC4. Para el mecanismo WEP, la *clave Maestra* (*Master Key*) se utiliza para cifrar cada trama Wi-Fi.

Para el mecanismo WPA1, el cifrado se obtiene a partir de una clave derivada de la clave Maestra, que se utiliza temporalmente. En asociación con el cifrado, se

añade un protocolo que contiene el vector de inicialización al protocolo de conexión de datos MAC (figura 5):

– el protocolo WEP en el caso del mecanismo WEP;

– el *protocolo de integridad de clave temporal* (*TKIP, Temporal Key Integrity Protocol*) en el caso del mecanismo WPA1.

Para el mecanismo WPA2, el cifrado se basa en el algoritmo AES y la cabecera del protocolo de conexión de datos MAC se complementa con la cabecera de CCMP (*Counter-mode/Cipher block chaining* MAC *Protocol*) (figura 5).

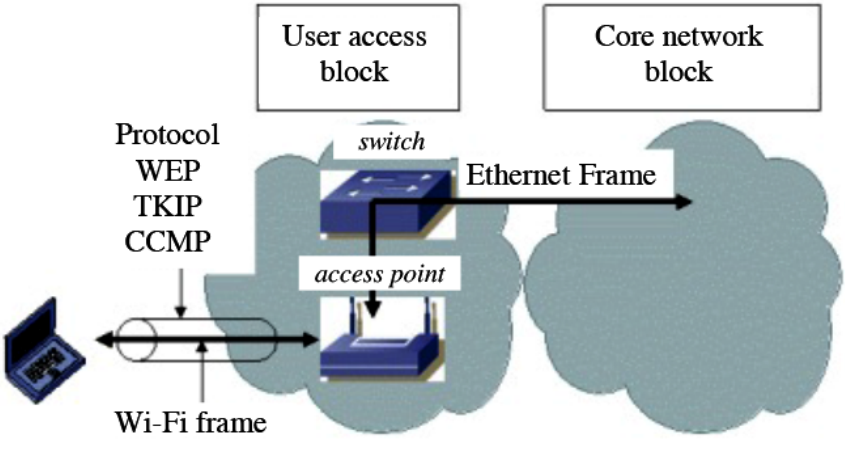

Figura 5. *Protocolos WEP, TKIP y CCMP*

El control de la integridad se realiza mediante una *comprobación de redundancia cíclica* (CRC, *Cyclic Redundancy Check*) para el mecanismo WEP. El mecanismo WPA1 utiliza el algoritmo MICHAEL. En el caso del mecanismo WPA2, la comprobación de integridad se obtiene a partir del algoritmo AES.

El mecanismo IPSec

El capítulo 4 presenta el mecanismo de seguridad IPSec (*Internet Protocol Security*) aplicado al paquete IP. Este mecanismo consta de dos partes (figura 6):

– el establecimiento de la asociación de seguridad entre dos pasarelas de seguridad, situados en los bloques de acceso de la LAN y la WAN;

– protección de datos entre estas dos pasarelas.

La asociación de seguridad se lleva a cabo en dos fases:

– la primera fase consiste en autentificar las pasarelas de seguridad que desean establecer la asociación de seguridad;

– la segunda fase establece los parámetros que deben utilizarse para la aplicación de la protección de datos (protocolo, algoritmo, clave).

Se han definido dos versiones de protocolos para el establecimiento de la asociación de seguridad. La primera versión se divide en tres partes:

– el *protocolo de asociación de seguridad en Internet y gestión de claves* (ISAKMP, *Internet Security Association and Key Management Protocol*) define el marco para establecer, modificar y eliminar la asociación de seguridad;

– el documento de *dominio de interpretación* (DOI, *Domain of Interpretation*) define los parámetros negociados para el uso del ISAKMP;

– el mecanismo IKEv1 (*Internet Key Exchange*) define los procedimientos de intercambio para el uso del ISAKMP.

El capítulo 4 describe solamente la segunda versión de IKEv2, que es más simple que la versión anterior. Esta versión combina las funcionalidades definidas en IKEv1 e ISAKMP, de las que elimina los procesos innecesarios. Elimina el carácter genérico de la versión anterior al integrar la función DOI que define los parámetros específicos de la asociación de seguridad.

La protección de datos introduce dos extensiones de la cabecera IPv4 o IPv6 (figura 6):

– la *cabecera de autentificación* (AH, *Authentication Header*) está diseñada para garantizar el control de la integridad, sin cifrado de datos (sin confidencialidad);

– la cabecera ESP (*Encapsulating Security Payload*) se utiliza para asegurar el control de la integridad y, opcionalmente, la confidencialidad de los paquetes IP.

La protección de datos entre las dos pasarelas de seguridad utiliza el modo túnel. Este modo se caracteriza por el hecho de que la cabecera AH o ESP encapsula el paquete IP original, y que el conjunto está a su vez encapsulado por una nueva cabecera IP.

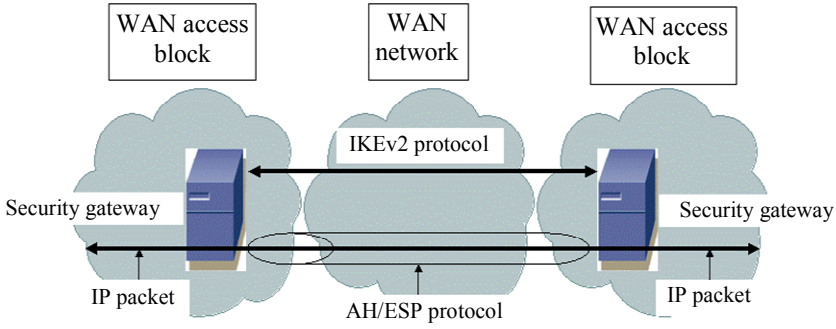

Figura 6. *El mecanismo IPSec*

Protocolos SSL / TLS / DTLS

El capítulo 5 presenta los protocolos de seguridad para la *capa de sockets seguros* (SSL, *Secure Sockets Layer*) y de *seguridad de capa de transporte* (TLS, *Transport Layer Security*) para el transporte de datos aplicados a los segmentos del *protocolo de control de transmisión* (TCP, *Transmission Control Protocol*). El protocolo de *datagram* TLS (DTLS) es una adaptación para el *protocolo de datagram de usuario* (UDP, *User Datagram Protocol*), el *protocolo de control de congestión de datagram* (DCCP, *Datagram Congestion Control Protocol*), el *protocolo de transmisión de control de stream* (SCTP, *Stream Control Transmission Protocol*) y el *protocolo de transporte en tiempo real seguro* (SRTP, *Secure Real-time Transport Protocol*).

El protocolo TLS está estandarizado por la IETF (*Internet Engineering Task Force*). Sigue el protocolo SSL, desarrollado por Netscape, cuyo objetivo original era establecer la seguridad de los intercambios entre un navegador y un servidor *web*.

Posteriormente se definieron varias versiones del protocolo TLS: TLS 1.0, TLS 1.1, TLS 1.2. La versión de TLS 1.0 corresponde a la versión 3.1 de SSL, que es la última versión del protocolo SSL. Las diferencias entre SSL 3.0, presente en los navegadores, y TLS 1.0 son mínimas, pero suficientes para que estos protocolos sean incompatibles.

TLS 1.0 se ha utilizado para corregir un fallo criptográfico en SSL 3.0 y para proporcionar algoritmos criptográficos para el intercambio de claves y la autentificación. TLS 1.1 es una revisión para proteger contra los ataques destacados sobre el uso del cifrado en modo *cadena de bloques cifrados* (CBC, *Cipher Block*

Chaining). TLS 1.2 integra elementos dispersos dentro del estándar y describe las extensiones TLS como parte integral del estándar.

La seguridad del transporte de datos se implementa entre un cliente que inicia la sesión y una *pasarela de seguridad* (*security gateway*) que actúa como servidor, ubicado en la LAN, en el bloque de acceso a la WAN.

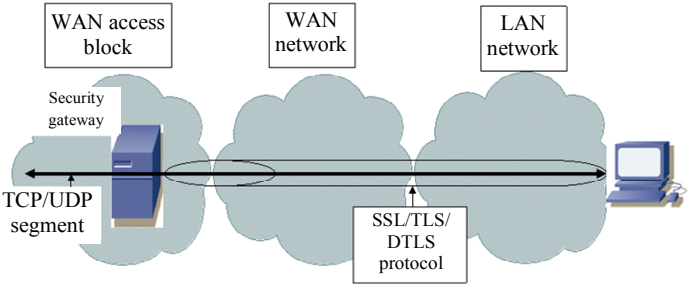

Figura 7. *Protocolos SSL, TLS y DTLS*

Gestión de la red

El capítulo 6 presenta los mecanismos de seguridad relacionados con los protocolos de gestión de red.

El *protocolo de gestión de red simple* (SNMP, *Simple Network Management Protocol*) permite realizar funciones de gestión de equipos (un *switch*, un *router*) que se dividen en tres áreas (figura 8):

– supervisión o gestión de alarmas;

– gestión de configuración;

– gestión del desempeño.

El SNMPv1 es la primera versión del protocolo. La seguridad se basa en una cadena llamada *comunidad* que proporciona derechos de lectura-escritura o de sólo-lectura. Esta versión tiene la desventaja de transportar esta contraseña en texto claro en el mensaje SNMP.

El SNMPv2 es la segunda versión del protocolo. Completa la estructura de la *base de información gestionada* (MIB, *Management Information Base*) que describe el equipo en forma de objetos. El protocolo también se mejora con nuevos mensajes. Sin embargo, no se realizan cambios en la seguridad de los intercambios.

El SNMPv3 es la tercera versión del protocolo. Su principal contribución es la introducción de mecanismos de seguridad más robustos:

– la comprobación de la integridad se basa en el algoritmo MD5 o SHA-1;

– La confidencialidad está garantizada por el algoritmo de cifrado DES.

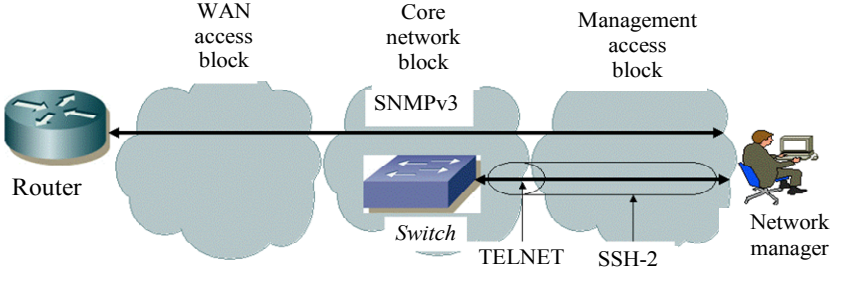

Figura 8. *Administración de la red*

TELNET es un protocolo que permite la conexión de un cliente, ubicado en el lado de la plataforma del administrador, con un intérprete de comandos en el lado del servidor, ubicado en el equipo a administrar. La sesión de TELNET se abre sobre la base de una contraseña que circula en texto claro entre el cliente y el servidor.

El protocolo de *shell seguro* (SSH, *Secure Shell*) proporciona servicios de autentificación, control de integridad y confidencialidad para los mensajes TELNET intercambiados (figura 8). SSH-2 es la versión estándar del protocolo. Se divide en tres partes:

– *Protocolo de capa de transporte* (*Transport Layer Protocol)* SSH (SSH-TRANS) es el protocolo que proporciona la base para el control de integridad y confidencialidad y la autentificación del servidor;

– *Protocolo de autentificación* SSH (SSH-USERAUTH) es el protocolo que permite autentificar al cliente;

– *Protocolo de conexión* SSH (SSH-CONNNECT) es el protocolo para mantener múltiples sesiones en una conexión SSH.

Tecnología MPLS

El capítulo 7 presenta los mecanismos para crear una partición de paquetes IP en la WAN.

Las redes de acceso y agregación WAN son en realidad redes Ethernet, cuya partición se describe en el capítulo 8 (figura 9).

La red central de la WAN es una red MPLS que integra la función VPN IP (figura 9).

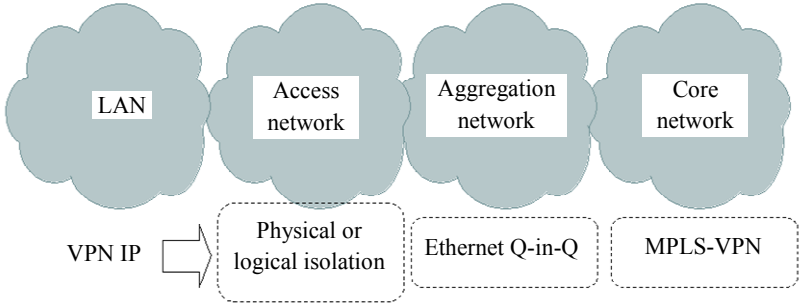

Figura 9. *La VPN IP*

La función MPLS consiste en etiquetar un paquete IP y utilizar esta etiqueta para conmutar en lugar de enrutar IP. Esta etiqueta LSP (*Label Switching Path*) es transportada por una cabecera MPLS que se inserta entre la capa 3 (IP) y la capa 2 (normalmente Ethernet).

La *tabla de conmutación de las etiquetas* (LFIB, *Label Forwarding Information Base*) se configura mediante dos protocolos:

– el *protocolo de distribución de etiquetas* (LDP, *Label Distribution Protocol*), que asocia una etiqueta con una dirección IP de red;este protocolo alimenta la tabla de la *base de información de etiquetas* (LIB, *Label Information Base*);

– el protocolo de enrutamiento *primero el camino más corto* (OSPF *Open Shortest Path First*) o protocolo de enrutamiento *sistema intermedio a sistema intermedio* (IS-IS, *Intermediate System to Intermediate System*), que determina un puerto de salida para una dirección de red IP; este protocolo completa la tabla de enrutamiento de la *base de información de enrutamiento* (*RIB, Routing Information Base*).

La función VPN es realizada por el equipo *proveedor de borde* (PE, *Provider Edge*) en el borde de la red central. Consiste en introducir los siguientes mecanismos:

– la partición de la tabla de enrutamiento, con el fin de propagar las rutas sólo en las instancias de enrutamiento específicas de un grupo cerrado de usuarios;

– el marcado de los paquetes IP con una etiqueta particular; esta etiqueta VPN es transportada por una cabecera MPLS adicional.

La red MPLS-VPN introduce direcciones de red públicas VPN-IPv4, construidas a partir de direcciones de red IPv4 públicas o privadas, lo que permite construir una red privada sobre una infraestructura pública.

La distribución de etiquetas VPN y direcciones VPN-IPv4 está asegurada por el protocolo de enrutamiento MP-BGP-4 (*Multi-Protocol Border Gateway Protocol*) intercambiado entre los equipos PE.

La red MPLS-VPN también permite la construcción de arquitecturas VPN complejas basadas en reglas de importación y exportación de rutas IPv4.

VPN Ethernet

El capítulo 8 presenta los mecanismos para dividir las tramas Ethernet en LANs y WANs.

La partición de tramas Ethernet en una LAN se realiza mediante la función VLAN (*Virtual LAN*) o Q-VLAN. Se basa en el marcado de tramas Ethernet, cada marca corresponde a un grupo cerrado de usuarios.

La partición de tramas Ethernet en una WAN puede realizarse utilizando las tres tecnologías siguientes:

– *Proveedor de puentes de transporte* (PBT, *Provider Bridge Transport*);

– *Servicio de LAN privada virtual* (VPLS, *Virtual Private LAN Service*);

– *Protocolo de túnel de capa 2* (L2TPv3, Layer 2 Tunnelling Protocol).

La tecnología PBT puede considerarse como una extensión de la función Q-VLAN realizada en la LAN. Generalmente se despliega en la red de agregación mediante la configuración de la doble marcación (*Q-in-Q*) de las tramas Ethernet.

La tecnología PBT también ha definido la partición de tramas Ethernet en la red central mediante la implementación de una cabecera Ethernet dual (*MAC- in-MAC*). Esta función no está desplegada y, por lo tanto, no se describe en el capítulo 8.

La tecnología VPLS es una extensión de la tecnología MPLS. Se despliega en la red central y tiene la ventaja de compartir el equipo P (*proveedor*) con la red MPLS-VPN.

La tecnología VPLS puede extenderse a la red de agregación con la función *H-VPLS* (*H-VPLS jerárquica*).

La tecnología L2TPv3 es una característica implementada para la transferencia de tramas Ethernet, sólo punto a punto, a través de una red de *routers* IP.

En resumen, la implementación de Ethernet VPN en la WAN se realiza de diferentes maneras (figura 10):

– a nivel de la red de acceso, la partición es física o lógica, dependiendo del tipo de tecnología utilizada; la conexión de dos usuarios en la red de acceso está generalmente prohibida; el tráfico de los usuarios debe transmitirse a la red de agregación;

– a nivel de red de agregación, el particionamiento se realiza utilizando la función H-VPLS o la marcación Ethernet dual (*Q-in-Q*);

– a nivel de red central, la partición se realiza mediante la función VPLS o MAC-in-MAC o L2TPv3.

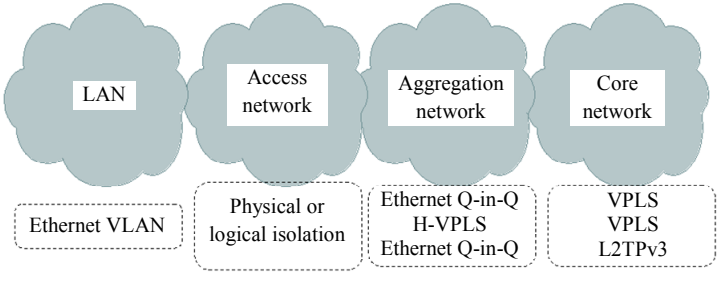

Figura 10. *VPN Ethernet*

Los servidores de seguridad (*firewalls*)

El capítulo 9 presenta las funcionalidades de los servidores de seguridad (*firewalls*). Monitorizan el paso de datos entre LANs y WANs controlando los campos de los diferentes protocolos de acuerdo con las reglas establecidas.

Hay varios tipos de servidores de seguridad que se caracterizan por las siguientes funciones:

– el *filtro de* paquetes sin estado: este control se aplica a los campos de las cabeceras de IP, TCP, UDP y el *protocolo de mensajes de control en Internet* (ICMP, *Internet Control Message Protocol*);

– el filtro de paquetes con estado: realiza el control de la máquina de estado de TCP; el control se lleva a cabo en las secuencias de segmentos TCP;

– el filtro de mensajes de aplicación: esta función la realizan las *pasarelas de la capa de aplicación* (ALG, *Application-Layer Gateway*) que inspeccionan el contenido del mensaje.

Los servidores de seguridad se despliegan en la LAN, en el bloque de acceso a la WAN. Están integrados en la *zona desmilitarizada* (DMZ, *Demilitarized Zone*).

Dos filtros de paquetes enmarcan la DMZ:

– uno para los filtros de paquetes del *front-end* (*front-end firewall*), que inspecciona los paquetes intercambiados entre la WAN y la zona desmilitarizada;

– el otro para filtro de paquetes del *back-end* (*backend firewall*) inspecciona los paquetes intercambiados entre la LAN y la zona desmilitarizada.

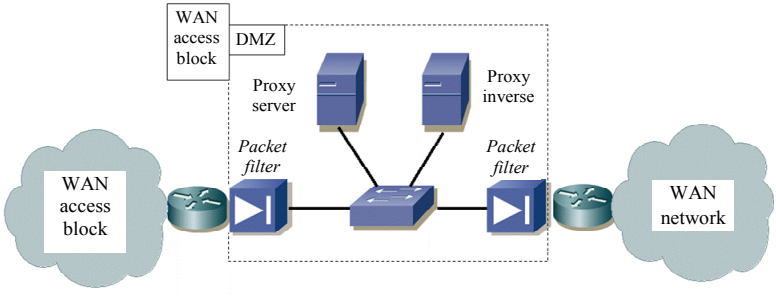

Figura 11. *La zona desmilitarizada*

La zona desmilitarizada alberga dos tipos de servidores de seguridad de aplicaciones: el servidor *proxy* y el servidor *proxy inverso*. El servidor *proxy* (o *proxy inverso*) comprueba el flujo del cliente (o servidor) conectado a la LAN.

La *traducción de dirección de red (*NAT, *Network Address Translation*), o *traducción de dirección y puerto de red* (NAPT, *Network Address and Port Translation*), es un tipo particular de *servidor de seguridad* (*firewall*). Esta función sólo permite el tráfico iniciado por *hosts* LAN y bloquea cualquier intento de conexión desde la WAN.

Varias configuraciones NAPT definen un filtrado más o menos selectivo: el cono abierto, el cono restringido a direcciones, el cono restringido a puertos, el cono simétrico.

El sistema NAT/NAPT presenta dificultades para ciertos flujos que deben pasar por él y para los que se definen mecanismos específicos:

– aplicaciones con identificación específica como ICMP;

– protocolos que protegen la carga del paquete IP, tales como el ESP del mecanismo de seguridad IPSec (*IP Security*);

– aplicaciones que llevan direcciones IP, como el *protocolo de información de sesión* (SIP, *Session Information Protocol*) y el *protocolo de descripción de sesión* (SDP, *Session Description Protocol*);

– flujos establecidos dinámicamente, como el *protocolo de transferencia de archivos* (FTP, *File Transfer Protocol*) o el *protocolo de transporte en tiempo real* (RTP, *Real-time Transport Protocol*);

– paquetes IP fragmentados.

Detección de intrusión

El capítulo 10 presenta las funcionalidades de los *sistemas de detección de intrusión* (IDS, *Intrusion Detection System*) y de los *sistemas de prevensión de intrusión* (IPS, *Intrusion Prevention System*). Estos dos tipos de sistemas se agrupan bajo el nombre de *sistemas de prevensión y detección de intrusión* (IDPS, *Intrusion Detection Prevention System*).

Estos dispositivos monitorean los datos que pasan entre la LAN y la WAN, o dentro de la LAN, basándose en el análisis de datos para detectar ataques.

Los métodos de detección de intrusos se implementan utilizando las siguientes técnicas:

– detección basada en firmas de ataques conocidos en datos que circulan en la LAN;

– la detección de anomalías basadas en el análisis de actividades sospechosas en el comportamiento de un *host*;

– análisis de los protocolos para verificar su conformidad con las normas.

En la red se despliegan diferentes tipos de dispositivos IDPS dependiendo de la ubicación o función que se realice:

– *Red basada en* IDPS (N-IDPS, *Network-based* IDPS): este dispositivo permite la monitorización de datos en los diferentes segmentos de la LAN;este dispositivo se aplica generalmente en interfaces Ethernet;

– *Red no cableada* IDPS (W-IDPS, *Wireless* IDPS): este dispositivo permite monitorizar los datos a través de la interfaz de radio Wi-Fi; es un caso especial del sistema N-IDPS;

– *Host basado en* IDPS (H-IDPS, *Home-based* IDPS): este dispositivo tiene una funcionalidad similar a la de los dispositivos anteriores; permite la monitorización de datos sólo a nivel de *host* de red;

– *Análisis de comportamiento de red* (NBA, *Network Behavior Analysis*): este dispositivo le permite realizar un análisis de tráfico específico para detectar actividades inusuales.