INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN

USERS

Argentina $ 22.- // México $ 49.-

Técnico en REDES &SEGURIDAD

22

VLAN, VPN Y TRABAJO REMÓTO

En esta clase conoceremos los diferentes tipos de redes virtuales existentes y entregaremos recomendaciones sobre seguridad. Además, veremos herramientas para trabajar sobre VPN.

- CLASIFICACIÓN Y PROTOCOLOS
- CONCEPTO DE TUNELIZACIÓN
- ACCESO REMOTO
- FUNCIONAMIENTO DE OPENVPN
- APLICACIONES RECOMENDADAS

USERS

Técnico en REDES & SEGURIDAD

Coordinador editorial
Paula Budris

Asesores técnicos
Federico Pacheco
Javier Richarte

Nuestros expertos
José Bustos
Gustavo Cardelle
Rodrigo Chávez
Santiago Crocioni
Alejandro Gómez
Gilberto González
Javier Medina
Gustavo Martín Moglie
Juan Ortiz
Pablo Pagani
Gerardo Pedraza
Marcelo Soria

Curso visual y práctico **Técnico en redes y seguridad** es una publicación de Fox Andina en coedición con Dálaga S.A. Esta publicación no puede ser reproducida ni en todo ni en parte, por ningún medio actual o futuro sin el permiso previo y por escrito de Fox Andina S.A. Distribuidores en Argentina: Capital: Vaccaro Sánchez y Cía. S.C., Moreno 794 piso 9 (1091), Ciudad de Buenos Aires, Tel. 5411-4342-4031/4032; Interior: Distribuidora Interplazas S.A. (DISA) Pte. Luis Sáenz Peña 1832 (C1135ABN), Buenos Aires, Tel. 5411-4305-0114. Bolivia: Agencia Moderna, General Acha E-0132, Casilla de correo 462, Cochabamba, Tel. 5914-422-1414. Chile: META S.A., Williams Rebolledo 1717 - Ñuñoa - Santiago, Tel. 562-620-1700. Colombia: Distribuidoras Unidas S.A., Carrera 71 Nro. 21 - 73, Bogotá D.C., Tel. 571-486-8000. Ecuador: Disandes (Distribuidora de los Andes) Calle 7° y Av. Agustín Freire, Guayaquil, Tel. 59342-271651. México: Distribuidora Intermex, S.A. de C.V., Lucio Blanco #435, Col. San Juan Tlihuaca, México D.F. (02400), Tel. 5255 52 30 95 43. Perú: Distribuidora Bolivariana S.A., Av. República de Panamá 3635 piso 2 San Isidro, Lima, Tel. 511 4412948 anexo 21. Uruguay: Espert S.R.L., Paraguay 1924, Montevideo, Tel. 5982-924-0766. Venezuela: Distribuidora Continental Bloque de Armas, Edificio Bloque de Armas Piso 9no., Av. San Martín, cruce con final Av. La Paz, Caracas, Tel. 58212-406-4250.

Impreso en Sevagraf S.A. Impreso en Argentina.

Copyright ® Fox Andina S.A. I, MMXIII.

Técnico en redes y seguridad / coordinado por Paula Budris. - 1a ed. - Buenos Aires: Fox Andina, 2013
576 p. ; 28 x 20 cm. (Users; 22)

ISBN 978-987-1857-78-4

1. Informática. 2. Redes. I. Budris, Paula, coord.
CDD 004.68

En esta clase veremos...

Redes privadas virtuales, sus características, funcionamiento y ventajas de su uso; también, revisaremos algunas opciones para realizar trabajo remoto.

En la clase anterior, revisamos alternativas de servidores, conocimos el funcionamiento de los servidores de backup y entregamos algunas recomendaciones de aplicaciones y consejos para administrarlos. Vimos el funcionamiento de los servidores de actualización y de los servidores de antivirus. Aprendimos a instalar y configurar un servidor proxy y los clientes correspondientes; por último, conocimos algunos protocolos de autenticación y analizamos la técnica Evilgrade.

En la presente clase, nos encargaremos de conocer las características y el funcionamiento de las redes privadas virtuales, analizaremos sus conceptos fundamentales y las ventajas que nos ofrecen. Conoceremos los protocolos asociados y los tipos de VPN, así como también sus modos de funcionamiento.

Revisaremos los mecanismos y protocolos de seguridad en redes privadas virtuales, conoceremos el funcionamiento de Hamachi y describiremos la plataforma libre OpenVPN.

22

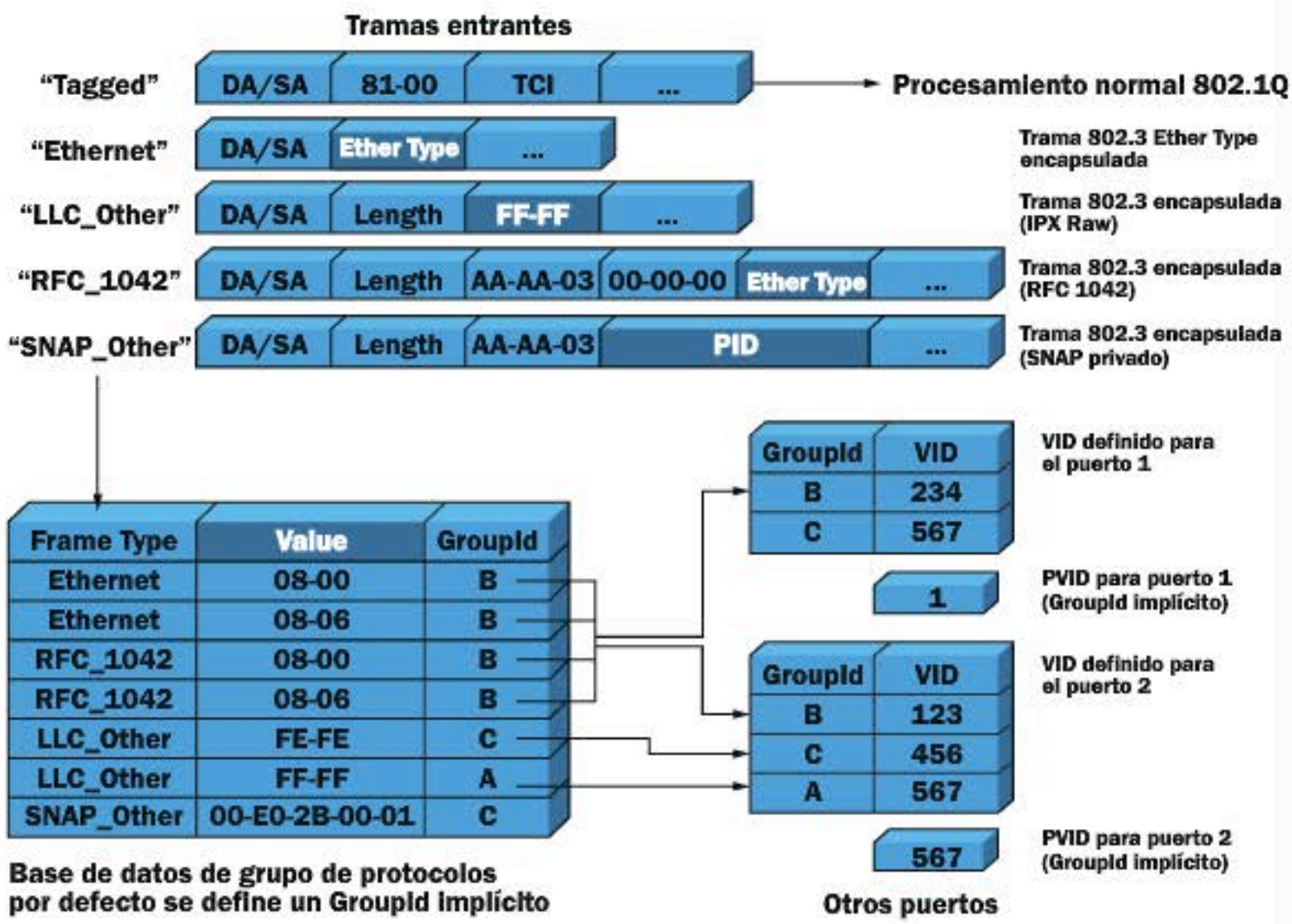
Qué son las VLAN o redes virtuales

Aquí revisaremos los procedimientos que siguen los switches que poseen soporte para redes virtuales; también, conoceremos las características del estándar IEEE 802.1Q aplicable a redes MAN y LAN.

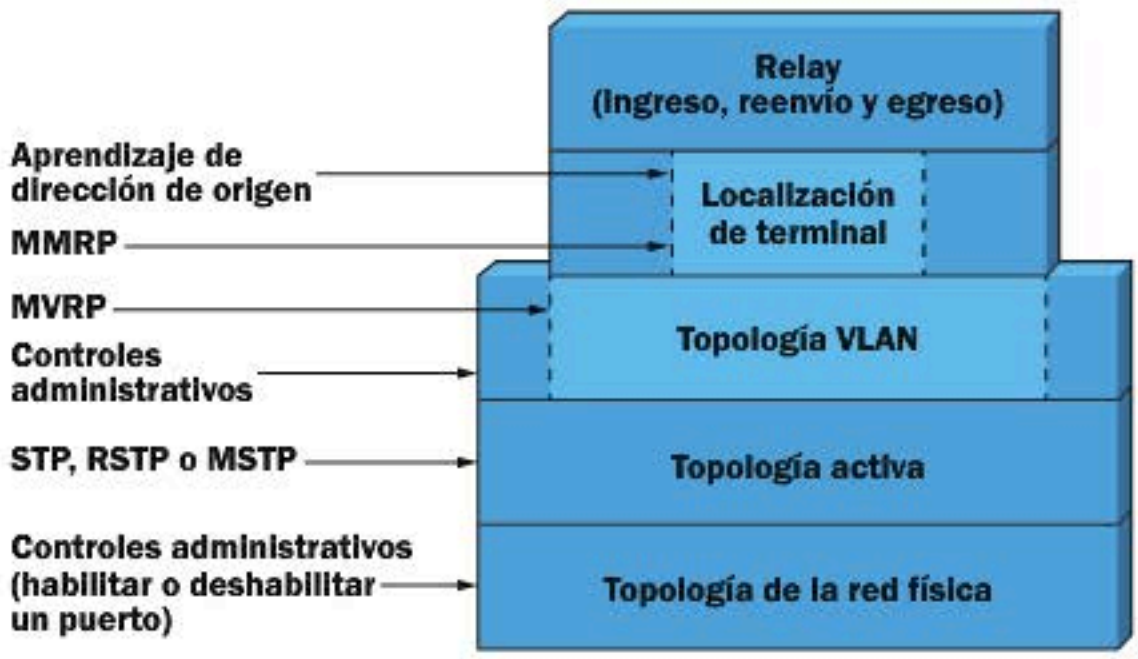
Las **redes virtuales** (**VLAN**, *Virtual Local Area Network*) permiten encapsular la información enviada de un punto a otro e identifican las tramas (Capa 2) con una etiqueta (llamada también tag) que aísla los paquetes del resto de la red. Las VLAN se representan con números, los **VID** *(VLAN Identifiers)*, y se utilizan, principalmente para segmentar un único dominio de broadcast a múltiples dominios. Muchos protocolos y aplicaciones requieren hacer uso de la función de broadcast, pero, sin la existencia de VLAN, una trama de broadcast puede viajar hasta segmentos de red distantes del lugar donde son requeridos. Esto consume recursos de los equipos y reduce el ancho de banda disponible.

Características

Las VLAN proveen, además, mayor seguridad en la red, ya que un usuario que se conecta a un puerto no podrá escanear



En este diagrama vemos ejemplos de operación de clasificación de VLAN sobre la base de puerto y protocolo.



Aquí vemos las capas que integran una solución Virtual LAN. Cada capa cumple una función bien definida.

toda la red en forma completa. Un administrador puede definir qué segmentos de la red son visibles para los usuarios. Es posible, por ejemplo, limitar la visibilidad a los dispositivos de un departamento que maneja información sensible. Algo importante de resaltar es que las VLAN no encriptan la información transmitida. Las VLAN y los VIDs proveen una referencia conveniente y consistente a los switches para:

- Realizar las tareas de identificación de reglas de clasificación de frames de usuario dentro de VLAN.
- Alargar efectivamente la MAC address de origen y destino tratando los frames y la información de direccionamiento para las distintas VLAN en forma independiente.
- Realizar la identificación y posterior selección de las distintas topologías activas en la red de datos.
- Identificar los parámetros de configuración que particionan o restringen el acceso desde una parte de la red a otra.

Reuniendo esta capacidad, es posible que los switches con soporte para VLAN emulen un número de LANs interconectadas y administradas de forma independiente. Se dice que una LAN forma parte, pertenece o es miembro de una VLAN, cuando fue seleccionada por los administradores de la red para recibir frames asignados a una VLAN. De igual manera, las terminales conectadas a esas LANs y que pueden recibir frames asignados a la VLAN se dice que están ligadas a esa VLAN.
El tag de una VLAN permite que los frames contengan información de prioridad aun cuando no hayan sido clasificados como pertenecientes a una VLAN en particular.

Topología

En cuanto a la topología, cada switch coopera con otros para manejar un protocolo tipo Spanning Tree para calcular una o más topologías, libres de loops y completamente conectadas. Este cálculo soporta la calidad de servicio y provee rápida recuperación ante fallas de los componentes, ya que utiliza conectividad física alternativa sin requerir intervención humana. Todos los frames de datos de usuario clasificados como pertenecientes a una VLAN determinada son restringidos por el proceso de reenvío de cada switch a una única topología activa. Por lo tanto, cada VLAN es asociada con un Spanning Tree, pero varias VLAN pueden compartir la misma asociación. En cualquier momento, la extensión de una VLAN puede reducirse al máximo para incluir solo las LANs que se encargan de proveer comunicación entre los dispositivos que se encuentran conectados. La asignación dinámica de las VLAN provee flexibilidad y conserva el ancho de banda, al costo de la complejidad de administración de la red.

Segmentar para mayor seguridad

La segmentación de las redes permite que un usuario o servicio solo pueda acceder a los dispositivos que el administrador determina. Es posible segmentar la red utilizando firewalls, lo cual resulta efectivo pero ineficiente, ya que es más difícil de mantener y más costoso para implementar. La solución correcta para segmentar usuarios y servicios es asignar un VID a cada grupo de usuarios y definir con qué otros grupos pueden interactuar.

Funcionamiento

Funcionando como dispositivos distribuidos, los switches pueden, explícita o implícitamente, cooperar para localizar una LAN determinada donde reside la terminal que debe recibir los frames. De esta manera, los switches pueden reducir el tráfico enviando los frames a la LAN donde la transmisión es necesaria. De todas formas, debemos tener en cuenta que un switch, en forma individual, no puede determinar la localización precisa de una terminal, pero puede determinar por cuál puerto se debe enviar un frame para que llegue al destinatario. Para el funcionamiento de los switches, esto resulta suficiente para alcanzar a los destinatarios.

LAS VLAN PROVEEN MAYOR SEGURIDAD; UN USUARIO QUE SE CONECTA NO PODRÁ ESCANEAR LA RED.

El protocolo de registración de múltiples MAC (*Multiple MAC Registration Protocol*, o MMRP) permite que las terminales publiquen su presencia y su deseo de unirse o retirarse de un grupo multicast. También de registrar una MAC address en forma individual dentro del contexto de una VLAN. El protocolo comunica esta información a los switches, usando la VLAN y la topología activa.
Para incorporar las estaciones que no participan en MMRP, la gestión de los controles asociados con cada puerto le permiten al puerto identificar las LANs conectadas como estaciones conectadas que están destinadas a recibir direcciones de grupo específicas.
La operación continua de MMRP y la propagación de la información de localización a través de los switches utilizando la topología activa permite la reducción de tráfico multicast, y asegura una rápida restauración de la conectividad multicast sin la intervención humana.

Terminales

Cada terminal implícitamente publica su asociación a una LAN y su MAC address individual. Los switches aprenden de la dirección de origen cuando esta transmite un frame, y todos ellos, en la topología, "recuerdan" por qué puerto y VLAN se recibió una determinada MAC address de origen. Esta información que se adquiere se almacena en la base de datos de filtrado, para poder enviar los frames basados en la dirección de destino.
La arquitectura de la base de datos de filtrado en el estándar reconoce que:

- Para realizar algunas configuraciones, es necesario permitir que la información de direcciones aprendida en una VLAN sea compartida con las otras VLAN. A este procedimiento se lo conoce como **aprendizaje compartido de VLAN**.
- Aunque también debemos considerar que, para otras configuraciones, es deseable asegurar que la información de direcciones aprendidas en una VLAN no sea compartida con otras VLAN. Este es conocido como **aprendizaje independiente de VLAN**.
- Para otras configuraciones, es indiferente ya que la información aprendida es compartida por otras VLAN.

El aprendizaje compartido de VLAN se alcanza mediante la inclusión de la información aprendida por un número de VLAN en la misma base. El aprendizaje independiente de VLAN se alcanza incluyendo la información de cada VLAN en bases independientes.

Requisitos

En una red determinada, puede existir una combinación de requisitos de configuración por la cual switches independientes pueden ser contactados para compartir la información aprendida sobre VLAN particulares o sobre grupos de VLAN.
La estructura de la base de datos de filtrado habilita el aprendizaje compartido o independiente de VLAN. Por ejemplo, permite que la información aprendida sea compartida entre las VLAN en las que el aprendizaje compartido es necesario, mientras que también permite que la información sobre VLAN independientes no sea compartida. Analizando el grupo de restricciones sobre el aprendizaje y las definiciones fijas sobre VIDs que están actualmente activas, el switch puede determinar lo siguiente:

- Cuántas bases son requeridas para cumplir con las restricciones.

Captura de tráfico con la herramienta de sniffing Wireshark, donde se visualiza la información de la VLAN.

No.	Time	Source	Destination	Protocol	Length	Info
17	47.044000	ca:02:17:a4:00:1d	ca:02:17:a4:00:1d	LOOP	60	Reply
18	53.897000	10.200.200.1	224.0.0.9	RIPv2	130	Response
19	57.066000	ca:02:17:a4:00:1d	ca:02:17:a4:00:1d	LOOP	60	Reply
20	57.227000	ca:02:17:a4:00:1d	Broadcast	ARP	64	who has 10.100.100.10?
21	61.172000	ca:02:17:a4:00:1d	Broadcast	ARP	64	who has 10.100.100.10?
22	63.202000	ca:02:17:a4:00:1d	Broadcast	ARP	64	who has 10.100.100.10?
23	63.922000	10.2.2.1	224.0.0.9	RIPv2	126	Response
24	65.189000	ca:02:17:a4:00:1d	Broadcast	ARP	64	who has 10.100.100.10?
25	67.071000	ca:02:17:a4:00:1d	ca:02:17:a4:00:1d	LOOP	60	Reply
26	69.886000	10.100.100.1	224.0.0.9	RIPv2	130	Response
27	77.085000	ca:02:17:a4:00:1d	ca:02:17:a4:00:1d	LOOP	60	Reply
28	79.878000	10.200.200.1	224.0.0.9	RIPv2	130	Response
29	87.066000	ca:02:17:a4:00:1d	ca:02:17:a4:00:1d	LOOP	60	Reply
30	92.128000	10.2.2.1	224.0.0.9	RIPv2	126	Response

▶ Para cada VID, qué base va a publicar o, por otra parte, utilizar la información que ha sido aprendida.

La función de relay provista por cada switch controla:

▶ La clasificación de cada frame recibido como perteneciente a una y solo una VLAN, y el descarte o la aceptación del frame para procesamiento basado en la clasificación y el formato, que puede ser uno de los siguientes:
- ▶ **Untagged** (sin etiquetas), no se encarga de especificar la pertenencia a una VID particular.
- ▶ **Priority-tagged**, incluye información explícita sobre prioridad, pero no identifica una asociación con una VID.
- ▶ **VLAN-tagged**, se encarga de realizar la asociación del frame a una VID particular en forma explícita.

▶ La implementación de las decisiones por las cuales cada frame debe ser reenviado según la topología VLAN. Este aspecto del relay implementa las reglas de reenvío.

▶ Encolamiento de frames para transmisión a través de los puertos definidos, administración de los frames encolados, selección de los frames para transmisión y determinación del tipo de formato adecuado para la transmisión (tagged o untagged). Este aspecto del relay implementa las reglas de egreso.

La estructuración de la funcionalidad de relay para el ingreso, reenvío y egreso constituye un enfoque genérico de la provisión de la funcionalidad VLAN. Todos los switches con soporte para VLAN pueden reenviar correctamente los frames recibidos que están etiquetados con información de VLAN. Estos están clasificados como pertenecientes a un identificador VLAN por la cabecera VID. Todos los switches compatibles con VLAN pueden además clasificar los frames no etiquetados y los que tienen información sobre prioridad recibidos por algún puerto perteneciente a una VLAN. Además de la clasificación basada en el ingreso por defecto en un puerto, el estándar especifica una clasificación óptima basada en puerto y protocolo.

Frames

Los frames que contienen información de control para determinar la topología activa y la extensión de cada VLAN (por ejemplo Spanning Tree y MVRP) y frames de otro protocolo restringido (por ejemplo EAPOL y LLDP) no son reenviados. Las entradas estáticas configuradas de manera permanente en la base de datos aseguran que sean descartados por el proceso de reenvío. Las reglas de reenvío para los frames etiquetados facilitan la interoperabilidad de los switches con las terminales que soportan directamente la conexión del servicio MAC (*Medium Access Control*) a switches, transmitiendo frames etiquetados. Los frames transmitidos en una determinada LAN por un switch con capacidad VLAN para una determinada VLAN deben ser todos untagged o todos tagged con el mismo VID. A continuación, vemos algunos ejemplos de las funciones que mantienen la calidad del servicio:

VLAN Trunking Protocol

VTP es el encargado de mantener la consistencia de la configuración VLAN en la red. VTP gestiona la creación, borrado y renombrado de VLAN en una red sincronizando los dispositivos entre sí. De esta forma, evitamos tener que configurarlos individualmente. Los switches pueden configurarse en los modos: servidor, cliente o transparente. El servidor anuncia su configuración al resto de equipos. El cliente solo recibe la configuración que le envían los servidores. Un switch en modo transparente solo puede configurarse en forma local.

- ▶ Recepción de frames.
- ▶ Descarte de frames recibidos con error.
- ▶ Descarte de frames que no contienen datos de usuario.
- ▶ Descarte de tramas para suprimir loops en la topología de la red.
- ▶ Clasificación de las tramas recibidas de cada VLAN.
- ▶ Realización del descarte de aquellas tramas necesarias para soportar el control sobre cada topología que se encuentre activa.
- ▶ Descarte de tramas por aplicación de una política de filtrado.
- ▶ Medición de tramas, o descarte de tramas que exceden los límites.
- ▶ Reenvío de frames recibidos a otros puertos
- ▶ Mapeo de unidades de servicio y chequeo de secuencia de las tramas.
- ▶ Selección de la prioridad de salida.
- ▶ Transmisión de tramas.

Los procesos y las entidades que el modelo de operación incluye son:

- ▶ Un proceso del puerto del switch recibe y transmite.
- ▶ Clasifica las tramas recibidas en VLAN.
- ▶ Determina el formato etiquetado o sin etiquetar, o transmite las tramas.
- ▶ Entrega y acepta tramas desde la entidad MAC retransmisora.
- ▶ Las entidades LLC que soportan entidades de capa superior.
- ▶ Entidades de administración de fallas de conectividad.

En redes metropolitanas, se conoce como VLAN stacking o VLAN tunneling al procedimiento que permite encapsular un VID perteneciente a la red LAN del usuario. Es decir, el proveedor de servicio puede respetar dichas VLAN y reencapsular cada paquete que sale del usuario con otro número de VLAN solo válido dentro de la red metropolitana.
Es necesario considerar que el ancho de banda puede ser controlado con una granularidad que llega más allá del nivel de la VLAN. De esta forma, dentro de la VLAN, se puede llegar a controlar el ancho de banda por cada protocolo que esté pasando por ella (por ejemplo IP, TCP, UDP, SNA o también sobre aplicaciones como webmail, voz, video) logrando así garantizar que el tráfico de ciertas aplicaciones no se vea afectado por el tráfico realizado por otras. ■

VLAN: clasificación y protocolos

En estas páginas nos encargamos de analizar los distintos tipos de VLAN, así como también sus características y aplicaciones más importantes. Además, veremos las mejores prácticas aplicables en la industria.

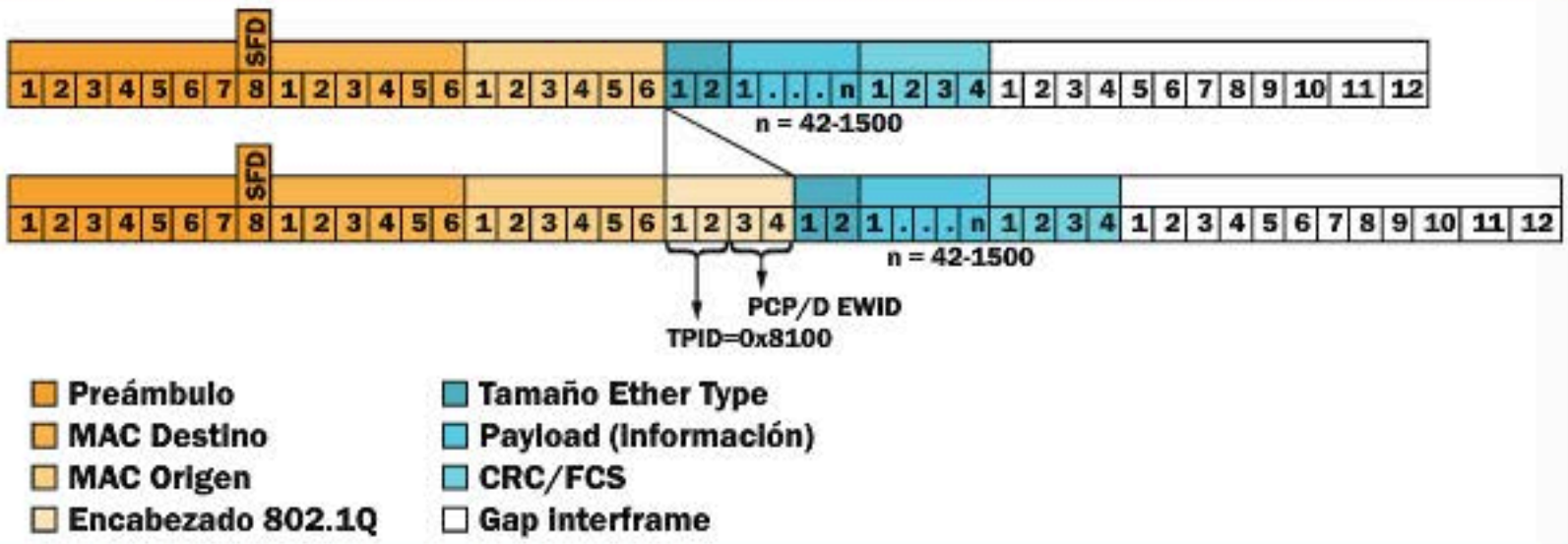
En forma predeterminada, todas las conexiones en un switch están en el mismo dominio de broadcast. Una **VLAN** (*Virtual Local Area Network*) puede ser utilizada para segmentar un único dominio de broadcasts en múltiples dominios en una red de capa 2. Muchos protocolos y aplicaciones requieren hacer uso de la función de broadcast. Las VLAN proveen además mayor seguridad en la red, ya que un usuario que se conecta a un puerto no podrá escanear o sniffear toda la red en forma completa.

IEEE 802.1Q ES EL ESTÁNDAR QUE DEFINE LAS VLAN SOBRE REDES ETHERNET.

Un administrador puede definir cuáles son los segmentos de red visibles para los usuarios. Es posible limitar la visibilidad a los dispositivos de un departamento que maneja información sensible. Utilizar VLAN resulta notoriamente más económico y fácil de administrar que utilizar routers para segmentar las redes.

Definición

Las VLAN pueden definirse de dos maneras básicas. Pueden ser de tipo estáticas o de tipo dinámicas. La VLAN estática separa los dominios usando puertos fijos previamente definidos del switch. La dinámica asigna VLAN sobre la base de datos del dispositivo, como por ejemplo la **MAC Addres** (Capa 2), el protocolo utilizado (Capa 3) o la dirección IP (Capa 3). Al conectarse un dispositivo, el switch consulta una base de datos para establecer la membresía a la VLAN definida. El uso de configuración estática puede ser apropiada en los puertos donde la configuración del dispositivo conectado es fija o cuando el administrador desea establecer una limitación administrativa. De esta manera, podemos definir, por ejemplo, que un usuario final tenga acceso a ciertos VIDs (*VLAN Identifiers*) definidos. El uso de la configuración dinámica puede ser apropiado en los puertos donde la configuración VLAN es inherentemente dinámica. Consideremos que un dispositivo determinado puede conectarse por distintos puertos de forma completamente aleatoria. Un ejemplo puede ser representado por usuarios sin un escritorio fijo, que se conectan desde distintos puestos.



En este diagrama, vemos una comparativa entre un frame Ethernet con soporte para el protocolo 802.1Q y sin él.

Otro ejemplo puede darse si la VLAN contiene caminos redundantes basados en un Spanning Tree. En este escenario, es deseable que los puertos de la red se configuren en forma dinámica para adaptarse a los cambios en el ruteo de las tramas. Claro que también es posible una combinación de ambas (estática y dinámica). El uso de la configuración estática y dinámica puede ser apropiado para puertos donde es preferible establecer restricciones en la configuración de algunos VIDs, pero manteniendo la flexibilidad de la registración dinámica para otros.

MVRP

El protocolo **MVRP** (*Multiple VLAN Registration Protocol*) define una aplicación que provee el servicio de registración de la VLAN. MVRP provee un mecanismo para el mantenimiento dinámico de los contenidos de los registros del proceso de registración dinámica y para propagar la información que contienen hacia otros bridges. Esta información permite a otros dispositivos compatibles con MVRP actualizar sus datos sobre los VIDs asociados con VLAN que actualmente poseen miembros activos, y a través de qué puertos esos miembros pueden ser alcanzados. Los puertos bridge pueden poseer una tabla de traducción de VIDs, que permite traducir un VID proveniente de otra red en un VID definido para la red que administra. El encargado de hacer la traducción es el servicio MVRP.

Tráfico

Por otro lado, también podemos clasificar las VLAN basándonos en el tráfico que transportan. La VLAN por default, normalmente la 1, es la que poseen todos los puertos al iniciar el switch. Esto permite, en el inicio del switch, que todos los dispositivos se encuentren en el mismo dominio de broadcast, y, por lo tanto, es posible que se comuniquen entre sí. En forma típica, la VLAN denominada default (1) no se puede eliminar.

La VLAN de datos o de usuario es la que generamos para transportar solo datos de usuario. De esta forma, es posible realizar configuraciones adecuadas para administrar este tipo de tráfico. La VLAN nativa es la que se asigna a un puerto trunk (troncal) que se comunica con otros switches o bridges. Un puerto 802.1Q troncal soporta tráfico proveniente de diversas VLAN así como también tráfico no etiquetado (no viene de una VLAN).

La VLAN de management se utiliza para administración del switch. De esta forma, cualquier puerto del switch puede llegar a hostear una VLAN de management.

La VLAN de voice transporta tráfico telefónico (de voz). Este tráfico típicamente posee prioridad ya que es muy sensible al delay.

IEEE

El estándar IEEE 802.1Q es el que define las VLAN sobre redes Ethernet. Determina los tags que deben llevar las tramas Ethernet y los procedimientos que deben utilizar los switches y bridges para manipularlos. El estándar provee además un esquema de priorización que brinda soporte para **QoS** (*Quality of Service*). Un frame con soporte para VLAN tendrá una cabecera de 4 bits con información sobre la VLAN donde se generó. Esta información será agregada y leída por los switches o bridges por donde transite.

El tráfico sin soporte para VLAN no contendrá tag con información de VLAN, pero, al ingresar a un segmento con soporte para VLAN, se etiquetará según las reglas definidas en la configuración. ■

Una configuración de VLAN en un proveedor de servicio para varios clientes. Así, es posible segmentar las redes.

Redes privadas virtuales

Analizaremos a fondo los tipos de VPN IPSec y SSL. Además, la criptografía y otras alternativas, y las recomendaciones sobre que implementar en cada caso.

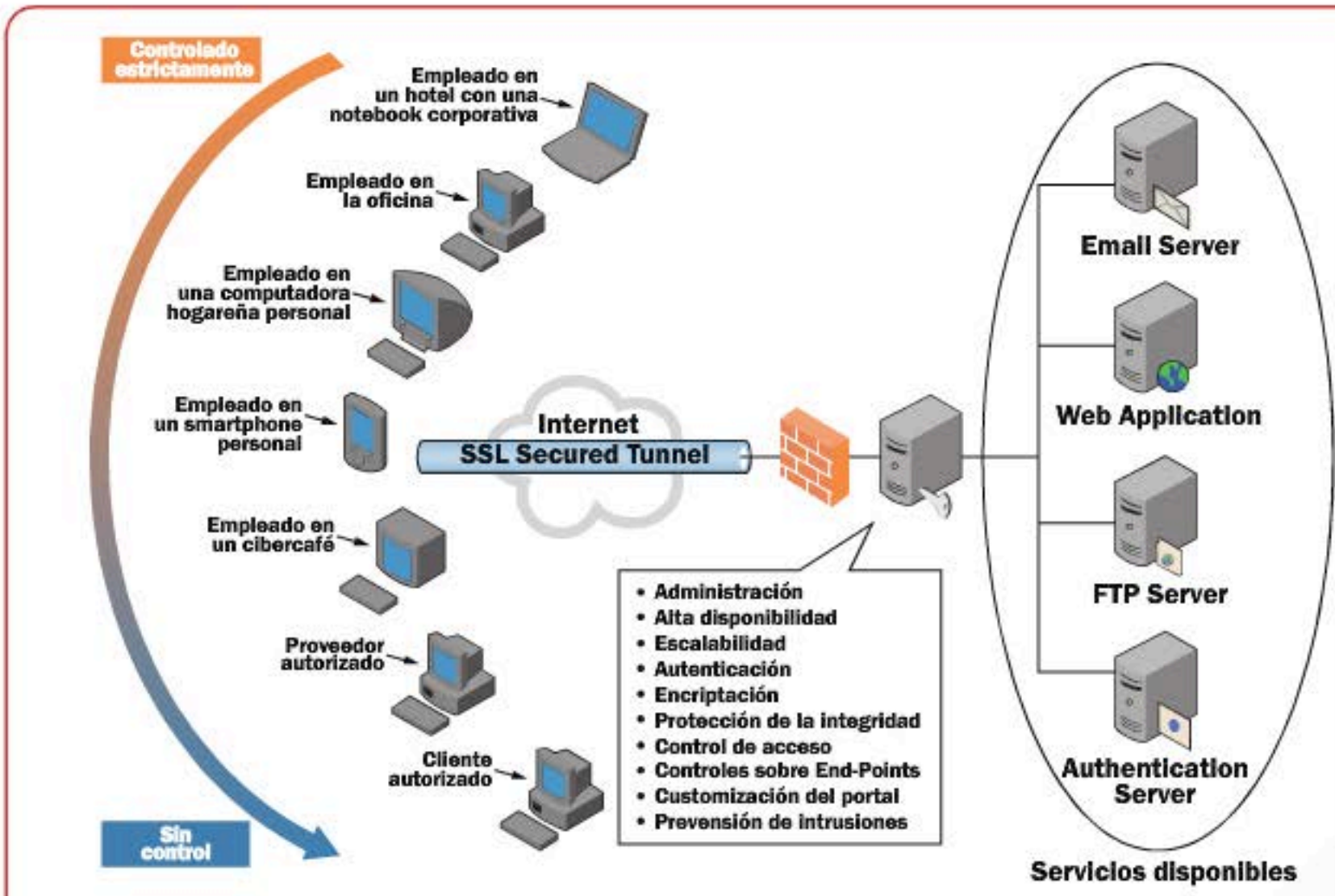
Una **VPN** (*Virtual Private Network*) permite generar conexiones seguras sobre medios inseguros, es decir, convierte una red pública o no confiable en una red privada sobre la cual nadie más podrá conocer su contenido. Una VPN brinda integridad, confidencialidad y autenticidad.

Es posible utilizar una VPN para conectar, de manera segura, oficinas y usuarios remotos por medio de un acceso a Internet económico, en lugar de a través de enlaces WAN dedicados.

Requisitos básicos

La implementación de una VPN requiere que se cumplan algunos requisitos básicos, por ejemplo identificación de usuarios y cifrado de los datos transmitidos. A continuación los analizamos en detalle:

- **Identificación de usuario**: una red privada virtual o VPN deben entregar los medios para que se realice la verificación de identidad de los usuarios que desean conectarse a ella, y restringir su acceso a



Una arquitectura de VPN SSL típica. Permite que cualquier dispositivo con soporte SSL inicie una conexión privada.

aquellos usuarios que no se encuentren debidamente autorizados.

- **Cifrado de datos**: los datos que se van a transmitir a través de Internet, antes deben ser cifrados, para que así no puedan ser leídos en el caso de que sean interceptados. Para realizar esta se utilizan algoritmos de cifrado como DES o 3DES, los cuales sólo pueden ser leídos por el emisor y el receptor de los datos.
- **Administración de claves**: las redes VPN deben asegurar los procesos de actualización de claves de cifrado para los usuarios que envían o reciben datos.
- Las redes privadas virtuales deben considerar el uso del algoritmo de seguridad SEAL.

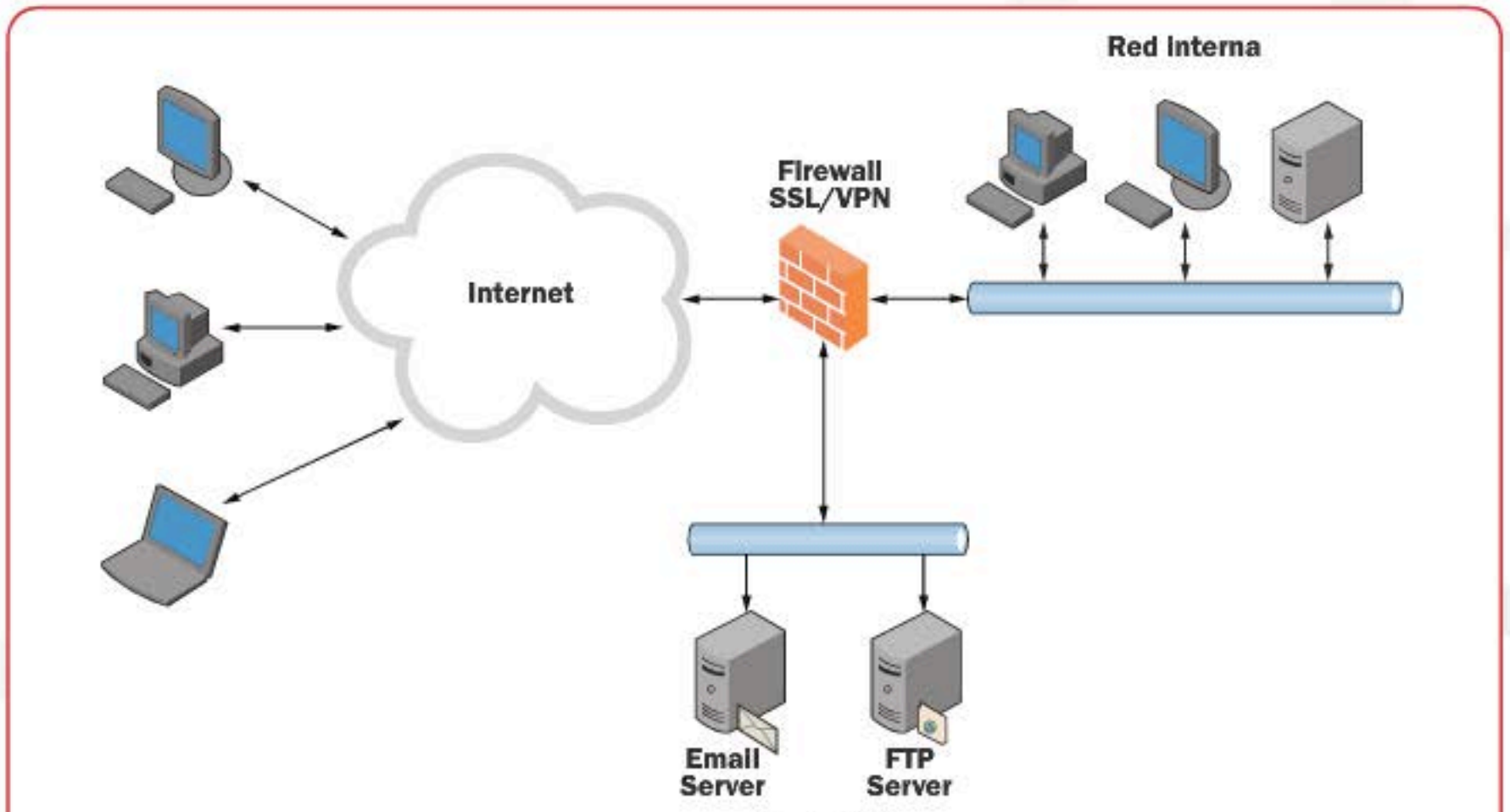
Un ejemplo típico de uso consiste en conectar dos o más sucursales de una empresa utilizando como vínculo Internet. Otro ejemplo consiste en permitir a los miembros del equipo técnico informático conectarse desde su casa al datacenter.

Tecnologías

Las tecnologías más comunes para establecer una VPN son **PPTP** (*Point to Point Tunneling*), **L2TP** (*Layer-2 Tunneling Protocol*) e **IPSEC** (*Internet Protocol Security*). PPTP fue desarrollado originalmente por un conjunto de empresas para proveer, a los usuarios, de acceso remoto a servidores en una red privada virtual. El estándar no describe mecanismos de encriptación ni autenticación. Sin embargo, sus implementaciones casi siempre lo hacen.

LAS VPN IPSEC Y SSL SON TECNOLOGÍAS COMPLEMENTARIAS QUE PROVEEN FUNCIONALIDADES DISTINTAS.

Permite conectarse a un servidor desde cualquier punto en Internet con la misma autenticación y los mismos accesos que si estuviésemos en la LAN. Este protocolo es utilizado, por ejemplo, en servidores Windows Server bajo el servicio RRAS (*Routing and Remote Access Service*). La implementación primitiva de Microsoft no ofrecía una protección robusta de los datos. Las nuevas versiones de Windows Server introducen mejoras en cuanto a la robustez de la encriptación, pero aun así no son recomendables. La principal debilidad radica en el primitivo protocolo 3DES de encriptación utilizado por MS-CHAP v2. L2TP facilita el manejo de paquetes PPP a través de una red, de manera tal que resulte transparente para los usuarios de ambos extremos del túnel y para las aplicaciones que estos corren. L2TP utiliza mensajes de control y mensajes de datos. Los mensajes de control se usan para establecer, mantener y borrar los túneles. Al utilizar PPP para el establecimiento del enlace, L2TP soporta los mecanismos de autenticación RADIUS, PPP, PAP y CHAP, lo que le brinda gran flexibilidad a la hora de implementación. L2TP no posee características criptográficas robustas, ya que no realiza la autenticación para cada uno de los paquetes que viajan por él. Esto permite la suplantación de identidad. Al no comprobar la integridad de cada paquete, es posible realizar un ataque de denegación de servicio (DoS) mediante mensajes falsos de control, que den por acabado el túnel o la conexión.



Una arquitectura de VPN SSL provista por un firewall, que permite realizar un acceso completo a la red de datos.

El protocolo L2TP no ofrece mecanismos para generación automática de claves o refresco automático de claves. Esto permite que alguien que descifre la clave pueda utilizarla por largos períodos sin ser advertido.

UNA VPN SSL PUEDE SER DEL TIPO PORTAL, PERMITE UNA ÚNICA CONEXIÓN A UN SITIO WEB O TÚNEL.

El estándar IPSec utiliza estos protocolos:

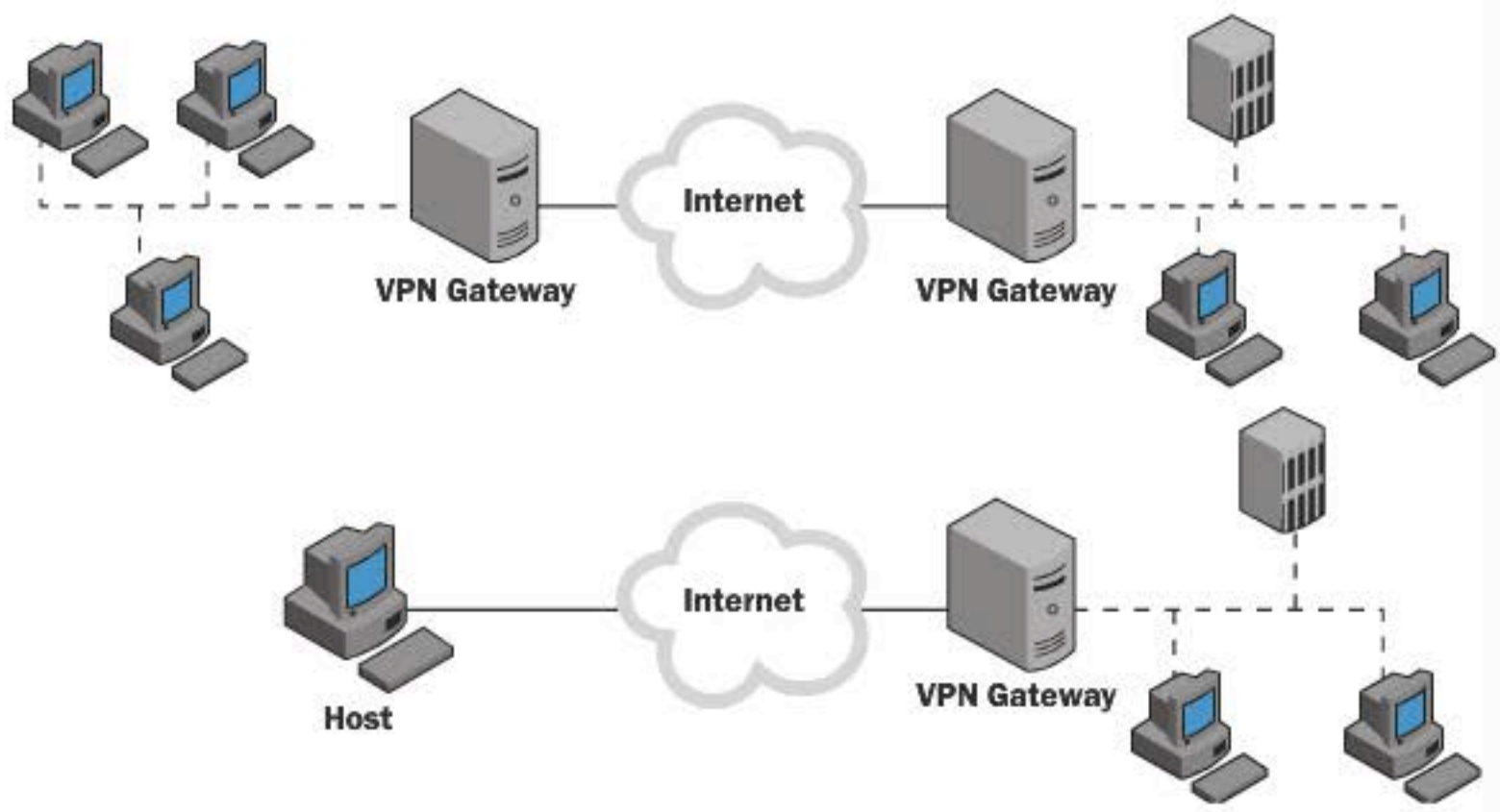
- **AH** (*Authentication Header*): provee autenticación del origen e integridad de los paquetes IP, pero no provee encriptación.
- **ESP** (*Encapsulating Security Payload*): provee confidencialidad, mediante encriptación de datos y autenticación de datos de origen e integridad.
- **IKE** (*Internet Key Exchange*): IPSec usa IKE para negociar las configuraciones de la conexión. Autentica los puntos terminales, y define los parámetros de seguridad de las conexiones, entre otras tareas.
- **IPComp** (*IP Payload Compression Protocol*): es un protocolo que permite comprimir los paquetes antes de realizar el proceso de encriptación.

Criptografía

Una VPN puede utilizar ambas formas de criptografía, simétrica y asimétrica. La criptografía simétrica utiliza la misma clave para el cifrado y descifrado, mientras que la criptografía asimétrica utiliza claves distintas para el cifrado y descifrado, o firmar digitalmente y verificar una firma. La criptografía simétrica es, por lo general, más eficiente y requiere menos potencia de procesamiento que la criptografía asimétrica, por lo que normalmente se utiliza para cifrar la mayor parte de los datos que están siendo enviados a través de una VPN. Un problema con la criptografía simétrica se presenta en el proceso de intercambio de claves; las claves deben ser intercambiadas fuera de línea para asegurar la confidencialidad. Algoritmos comunes que implementan la criptografía simétrica incluyen *Digital Encryption Standard* (DES), *Triple DES* (3DES) y *Advanced Encryption Standard* (AES), *Blowfish*, RC4, *International Data Encryption Algorithm* (IDEA), entre otros.

Seguridad

Es importante entender que las VPN no eliminan todo el riesgo de las redes. Si bien las VPN pueden reducir considerablemente el riesgo, en particular para las comunicaciones que se producen a través de redes públicas, no eliminan todo el riesgo para tales comunicaciones. Un problema potencial es la robustez de la implementación. Por ejemplo, fallas en un algoritmo de cifrado o el software que implementa el algoritmo podrían permitir a los atacantes descifrar el tráfico interceptado. Otra cuestión es la divulgación de la clave de cifrado. Un atacante que descubre una clave podría no solo descifrar el tráfico, sino también hacerse pasar por un usuario legítimo. Otra área de riesgo implica la disponibilidad. Un modelo común para la seguridad de la información se basa en los conceptos de confidencialidad, integridad y disponibilidad. Aunque las VPN están diseñadas para apoyar la confidencialidad y la integridad, por lo general no mejoran la disponibilidad, la capacidad de los usuarios autorizados para acceder a los sistemas según sea necesario. De hecho, muchas implementaciones de VPN, en realidad, tienden a reducir la disponibilidad de alguna manera, ya que añaden más componentes y servicios a la infraestructura de red existente. Esto depende en gran medida del modelo de arquitectura VPN elegida y los detalles de la implementación. ■



Arquitecturas para una VPN IPSec: arriba, un **site-to-site**; abajo, un cliente conectándose a una VPN a través de un **gateway**.

VPN: funcionamiento

Smartphone con cliente VPN
Las nuevas tecnologías también permiten que los teletrabajadores puedan acceder a datos alojados en la empresa desde su teléfono celular o tablet.

ÁMBITO HOGAREÑO

Notebook con cliente VPN
Los teleworkers pueden hacer su trabajo desde la comodidad de su hogar usando equipos portátiles o de escritorio, siempre y cuando tengan instalado un cliente VPN.

CONEXIONES MÓVILES

INTERNET

ÁMBITO CORPORATIVO

VPN Firewall
Dispositivo encargado de gestionar la comunicación entre los servidores internos de la empresa y los usuarios conectados remotamente.

File Server
Servidor de archivos corporativo accesible en forma segura no solo por usuarios locales mediante la red LAN, sino también por usuarios remotos.

Túnel seguro
Las conexiones VPN se llevan a cabo mediante un túnel virtual que garantiza la seguridad de las transacciones.

Tipos de VPN.
Ventajas y desventajas

Existen distintos tipos de VPN; aquí analizaremos sus ventajas, desventajas y características más importantes en forma detallada.

Una **VPN** o *Virtual Private Network* hace referencia a la posibilidad de establecer un vínculo con una computadora o servidor; de esta forma, podremos acceder a todos los servicios que la red brinda o por el que nos conectamos a la empresa. Como ya sabemos, la comunicación entre los dos extremos de la red privada a través de la red pública se hace creando túneles virtuales entre los dos puntos, mediante sistemas de encriptación y autenticación que aseguren la confidencialidad e integridad de los datos. Los tipos de VPN que existen son: Tunneling, VPN site-to-site, VPN de acceso remoto y VPN interna.

Página web de software libre con todas las características de VPN.

Tunneling

Esta técnica consiste en abrir conexiones entre dos máquinas por medio de un protocolo seguro, como puede ser **SSH** (*Secure Shell*), a través de las cuales realizaremos las transferencias inseguras, que pasarán de este modo a ser seguras. En una conexión segura, se envían los datos por un túnel; este tipo de técnica requiere de forma imprescindible tener una cuenta de acceso seguro en la máquina con la que queremos comunicar los datos, y la conexión puede ser LAN O WAN.

VPN site-to-site

Este esquema se utiliza para conectar oficinas remotas con la sede central de una organización, por ejemplo. El equipo central VPN, que posee un vínculo a Internet en forma permanente, acepta las conexiones vía Internet que provienen de los sitios y establece el túnel VPN. Debemos considerar que los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, por lo general, mediante conexiones de banda ancha.

VPN de acceso remoto

Esta implementación se trata de comunicaciones en las que los usuarios se conectan con la empresa desde sitios remotos (por ejemplo, desde oficinas comerciales, casas u hoteles, entre otras ubicaciones) utilizando Internet como medio de acceso. Una vez que han sido autenticados, tienen un nivel de acceso muy similar al que poseen desde la red local de la empresa, usando un nombre de usuario y contraseña adecuados.

Seguridad y privacidad

Si bien las VPN proveen un alto nivel de seguridad y también de confidencialidad, hay que tener cuidado en la forma en que las utilizamos y nos conectamos a ellas. En especial, porque muchas veces activamos la opción que permite recordar las contraseñas cuando nos conectamos, y, de esta forma, nuestro inicio de sesión quedará disponible para otros usuarios.

VPN interna

Consiste en establecer redes privadas virtuales dentro de una misma red local. El objetivo último es aislar partes de la red y sus servicios entre sí, aumentando la seguridad. Una aplicación muy típica de este modelo se utiliza para aumentar la seguridad en redes de acceso inalámbrico, separándolas así de la red física, para evitar posibles fugas de información o accesos no autorizados.

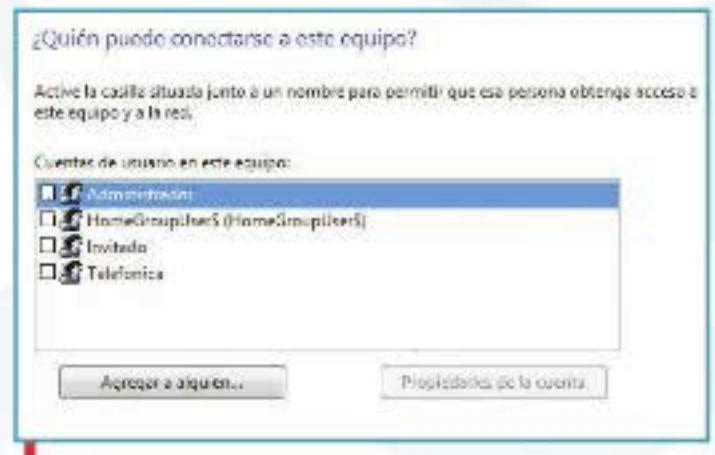
SEGURIDAD, CONFIABILIDAD Y ENCRIPTACIÓN: TRES PUNTOS CLAVE EN LA CONEXIÓN A VPN.

Características

Si bien estos son los tipos de VPN que se pueden crear de acuerdo con el lugar donde nos encontremos o el tipo de acceso que queramos, también es importante el protocolo que usan, para garantizar seguridad y fiabilidad a la conexión de confianza que establecemos. Estamos hablando en especial de tres protocolos: PPTP, IPSec y L2TP.

- **PPTP** (*Point to Point Tunneling Protocol*): hecho para proveer una red privada virtual entre usuarios de acceso remoto y servidores de red. PPTP fue diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en Internet y tener la misma autenticación, encriptación y los accesos de LAN como si discaran directamente al servidor. Es uno de los más usados por su facilidad de creación, la elección de protocolos de seguridad y su manipulación.

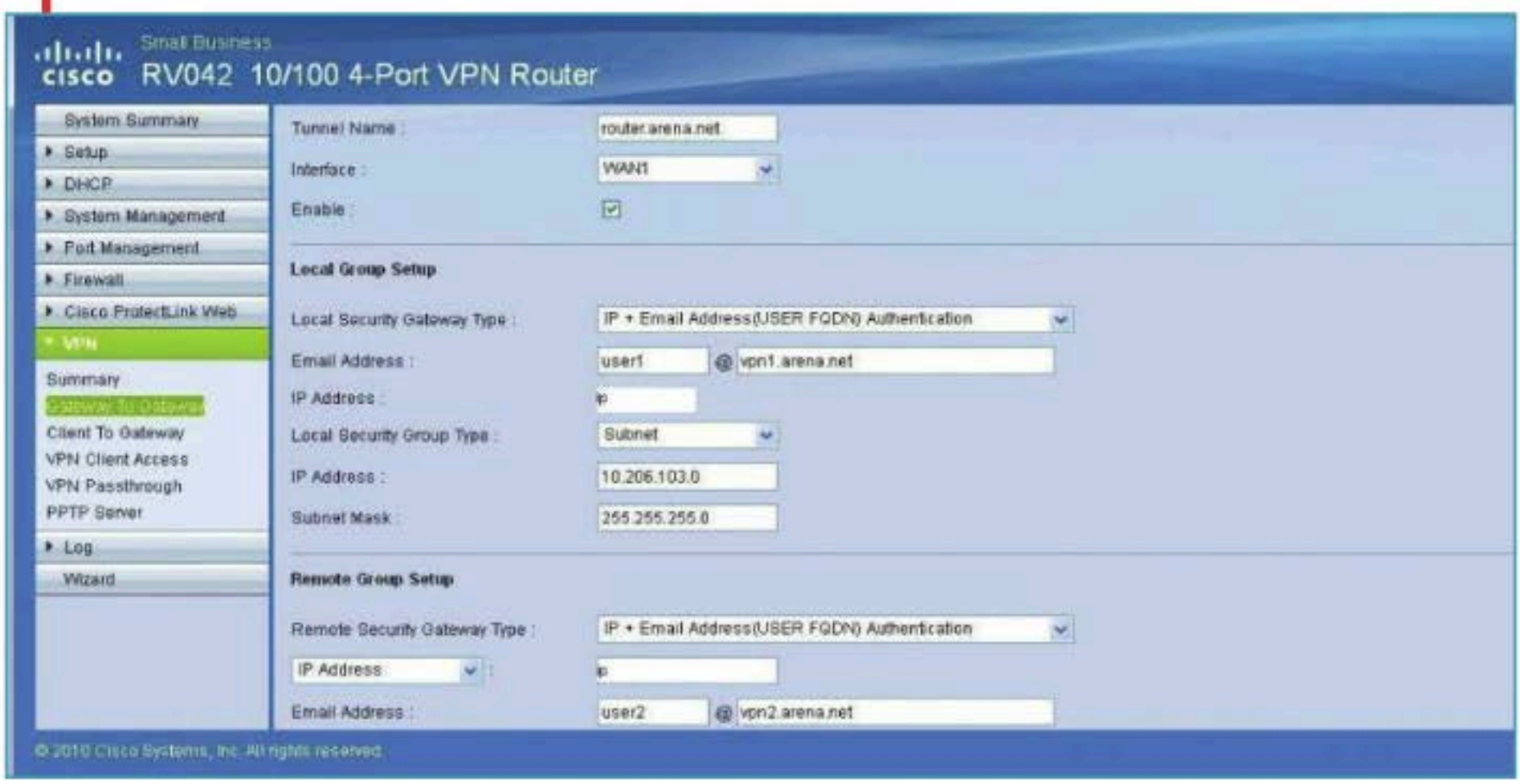
- **IPSec**: se encarga de remediar algunas falencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme. También provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son *Authentication Protocol* (AP) y *Encapsulated Security Payload* (ESP).



Para aceptar conexiones entrantes, pulsamos ALT, y elegimos Archivo/ Nueva conexión entrante.

- **L2TP** (*Layer-2 TunnelingProtocol*): facilita la realización de tunneling de paquetes PPP a través de una red de datos, de manera tal que sea lo más transparente posible a los usuarios de ambos extremos del túnel y para las aplicaciones que estos ejecuten en forma normal. Consideremos que L2TP utiliza dos tipos de mensajes: de control y de datos. Los mensajes de control son usados para el establecimiento, el mantenimiento y el borrado de los túneles y las llamadas. Utilizan un canal de control confiable en L2TP para garantizar el envío. Los mensajes de datos encapsulan los marcos PPP y se envían a través del túnel. ■

Aquí vemos un ejemplo de un cisco de una **VPN site-to-site** que debe saber los datos de destino, IP y subnet, entre otros.



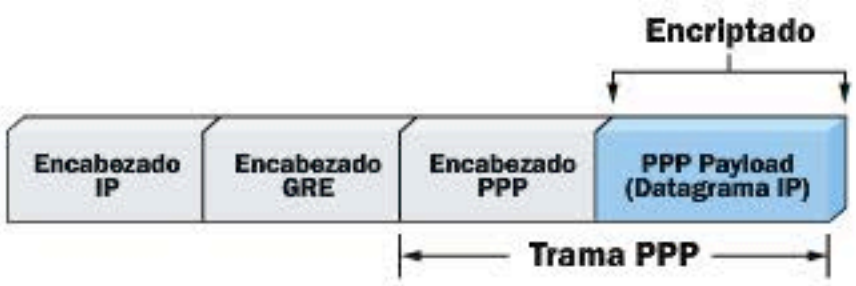
Tunelización en redes VPN

Veremos qué son y cómo se establecen los túneles generados por una VPN, las recomendaciones y, también, las limitaciones de implementación en un entorno corporativo.

Un túnel es un vínculo entre dos ubicaciones, que puede generarse sobre varios tipos de redes, ya sea sobre redes internas/privadas o redes públicas. El caso más habitual es sobre redes públicas, y se usa a fin de asegurar la confidencialidad e integridad de la información transmitida, aunque por definición no es necesario que un túnel esté encriptado.
Una de las principales motivaciones para utilizar un túnel generado por una VPN consiste en encriptar una comunicación TCP/IP de aplicaciones cliente/servidor. Con el auge de las conexiones y los dispositivos móviles, el uso de las VPN se ha popularizado para permitir que las aplicaciones cliente/servidor puedan funcionar de manera segura. Usar un túnel es una forma no solo de hacer más segura la conexión, sino también de que resulte más sencillo de establecer para el usuario final.

Uso

Todas las conexiones VPN utilizan túneles. Un túnel es un mecanismo para enviar información por medio de un protocolo que, de otra manera, no sería soportado por la red. El caso típico consiste en utilizar el protocolo IP para enviar otro protocolo en la sección de datos del datagrama IP.
Por ejemplo, utilizamos una VPN para ganar acceso a una aplicación o acceder a una base de datos porque, de otra manera, no podríamos hacerlo, ya que los puertos TCP están bloqueados y no pueden ser accedidos desde Internet, al no ser permitidos por los routers de borde. También los paquetes destinados a Active Directory (puerto 445) se envían encapsulados dentro de los paquetes de VPN. Cuando llegan al server de VPN, se desempaquetan y se reenvían a la red interna. De esta manera al desplazarse por un túnel, cuando la información viaja por Internet está encriptada, pero, al llegar a la red interna, se desempaqueta y desencripta. Debemos tener en cuenta que la encriptación no es end-to-end como puede ser, por ejemplo, en una aplicación web SSL.



Un paquete PPTP que contiene un datagrama IP encriptado. PPTP encripta los datos utilizando MS-CHAP v2 o EAP-TLS.

EL PROCESO DE TUNELIZACIÓN CONSISTE EN INTRODUCIR UN PAQUETE DENTRO DE OTRO.

Conceptualmente, lo que se genera son paquetes dentro de otros paquetes. Entonces, un paquete IP en su porción de datos contendrá otro paquete en forma completa. A esto se lo llama **IPIP tunnel** (*IP living in IP packets*). Ahora bien, al encapsular un paquete dentro de otro, debemos tener presente que el header se está duplicando y, de esta manera, se transporta menor carga útil, es decir, el MTU (*Max Transfer Unit*) disminuye. La cabecera IP usa 20 bytes, por lo que cada paquete consumirá un overhead de 20 bytes.

Componentes

A continuación, nos encargamos de enumerar los componentes que permiten generar una VPN y entregamos una caracterización de cada uno de ellos:

- **Servidor VPN:** un equipo que acepta conexiones VPN provenientes de clientes. Se encarga de empaquetar/encriptar y desempaquetar/desencriptar los paquetes.
- **Cliente VPN:** es un equipo que inicia la conexión hacia un servidor VPN. Puede ser una computadora o un router.
- **Túnel:** se trata de la porción de la conexión donde los datos se encuentran encapsulados.

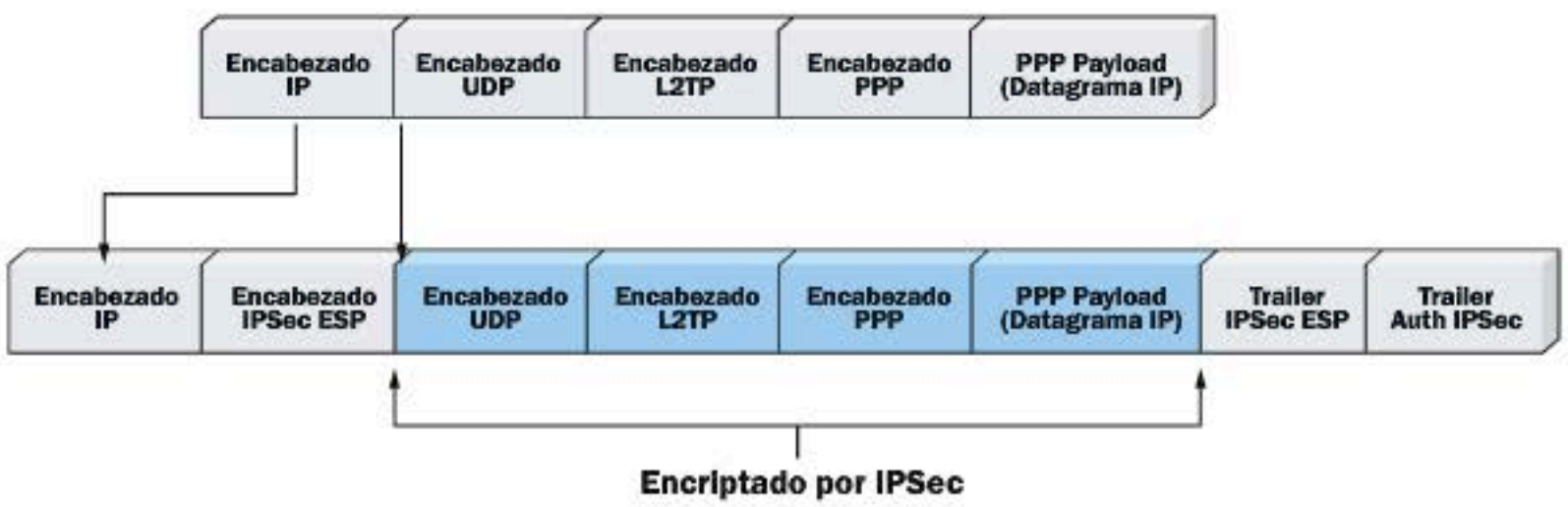
▶ **Conexión VPN**: es la porción de la conexión donde los datos están encriptados. En una VPN típica, los datos se encriptan y encapsulan en el mismo punto de la conexión.

Siempre debemos tener presente que es posible generar un túnel sin encriptar los datos; por ejemplo, una red MPLS tuneliza los datos sin encriptarlos. En ese caso, no se considera como una VPN, ya que no se encriptan los datos. Existen diversos protocolos para administrar túneles y encapsular datos. En el mundo Windows, se utilizan PPTP y L2TP como protocolos de tunelización, pero sin dudas el protocolo más difundido es IPSec.
NAT (*Network Address Translation*) y PAT (*Port Address Translation*) proveen una capa de seguridad adicional sobre la VPN y conservan las direcciones públicas, aunque presentan algunos desafíos.
ISAKMP (*Internet Key Management Protocol*) se basa en direcciones IP individuales para generar la encriptación, sin embargo, PAT trabaja generando múltiples llaves criptográficas para una sola dirección IP. La funcionalidad NAT-T (*IPSec NAT Traversal*) viaja a través de dispositivos NAT o PAT encapsulando el tráfico IPSec e ISAKMP en UDP (*User Datagram Protocol*). NAT-T fue introducido por el software Cisco IOS a partir de su versión 12.2 y es detectado en forma automática por los dispositivos VPN.
No es necesario realizar ninguna configuración, ya que se habilita por defecto como un comando global. NAT-T detecta un dispositivo PAT entre los extremos y negocia NAT-T si es soportado.

Aumento de túneles

Debemos tener en cuenta que, al aumentar la cantidad de túneles que se encuentran en funcionamiento, el ancho de banda tiende a decrecer. Cuando un router recibe un paquete desde un par del cual no ha desencriptado un paquete recientemente, se encargará de realizar una búsqueda, para ello se basa en los parámetros de seguridad que corresponden al paquete. Para este nuevo paquete, se negocia una llave de desencriptación, que se envía al motor de desencriptación por hardware para ser procesado. Tener tráfico que proviene de numerosos túneles tiende a afectar en forma negativa la performance.
Las plataformas con acelerador por hardware de encriptación IPSec son cada vez más comunes para reducir la sobrecarga de procesamiento, lo que redunda en un procesamiento lineal más predecible sin importar la cantidad de túneles. Por ejemplo, la línea de equipos Cisco 7600 tiene un procesamiento relativamente lineal sin importar la cantidad de carga, tanto si posee unos pocos túneles como miles de ellos.
El crecimiento de los túneles es una función que depende, por lo general, de la cantidad de sucursales que se conectan a la casa central. Por esta razón, la cantidad de túneles terminados debe considerarse al realizar el diseño y escoger los dispositivos por utilizar. Para esto, deben tenerse en cuenta tanto los túneles primarios como los túneles secundarios, que cada central debe generar en caso de falla. Recordemos que la cantidad de túneles por generar es un factor primordial a la hora de seleccionar la plataforma adecuada, pero los requerimientos de encriptación e interoperabilidad también son importantes y deben ser considerados. ■

Router Cisco 7600: se trata de una plataforma para grandes implementaciones que ofrece generación de túneles VPN entre otras características.



En este diagrama, vemos la estructura de un paquete PPP encapsulado por L2TP y encriptado por IPSec.

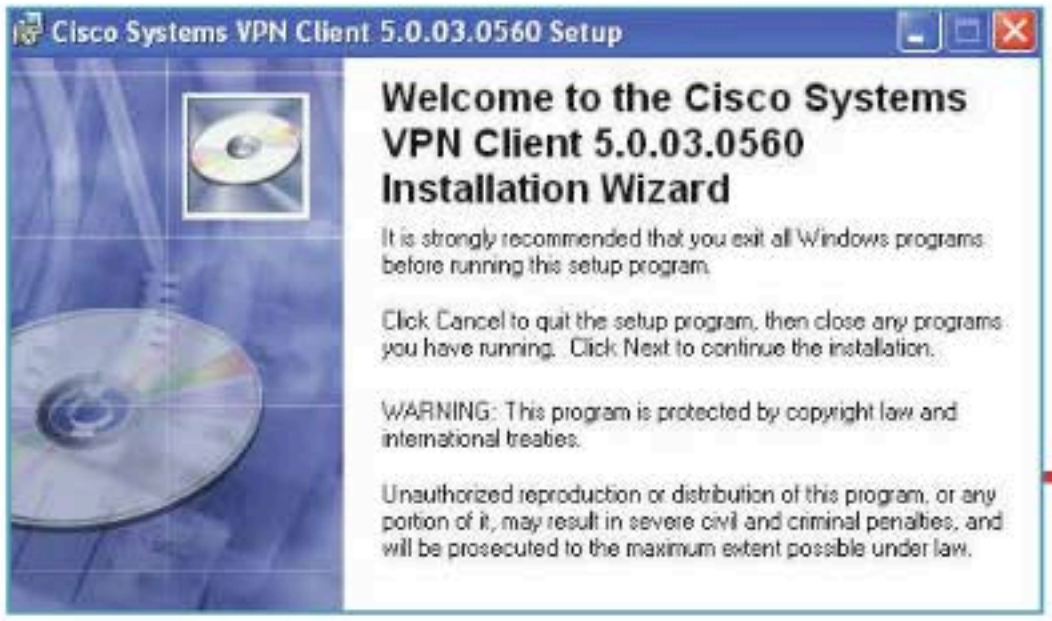
VPN en modo túnel y en modo transporte

En estas páginas, nos encargaremos de analizar las VPN en modo túnel y, también, en modo transporte. Además, veremos sus ventajas, desventajas, y los problemas más comunes.

Existen distintos tipos de VPN, pero, en nuestro caso, describiremos las más comunes, y que por esta razón se utilizan con mayor frecuencia: la VPN en modo túnel y la VPN en modo transporte.

Modo túnel

La VPN en modo túnel es aquella en la que todo el paquete IP es cifrado o autenticado. Para que este método funcione, obviamente el paquete resultante debe ser encapsulado en otro paquete IP (que puede ser IPv4 o IPv6) que contenga los datos del emisor y el receptor, y pueda ser enrutado. Este modo lo utilizamos en las VPN site-to-site, en las que dos redes distintas deben ser conectadas por un medio que brinde seguridad en la comunicación. Una de las principales ventajas de utilizar esta configuración es su altísima resistencia al repudio de las comunicaciones realizadas, así como también al descubrimiento de la información interna. Otro punto a favor es que puede utilizarse en casi cualquier ambiente, incluso en donde se encuentra configurada la funcionalidad de NAT. Su principal desventaja es lo complicado de utilizar una estructura de encriptación y desencriptado para protocolos que son de tiempo real, tal como la VoIP (Voz sobre IP). Esto se debe a los retardos que incrementan estas operaciones en los equipamientos de red dedicados y que degradan la calidad de las comunicaciones telefónicas.



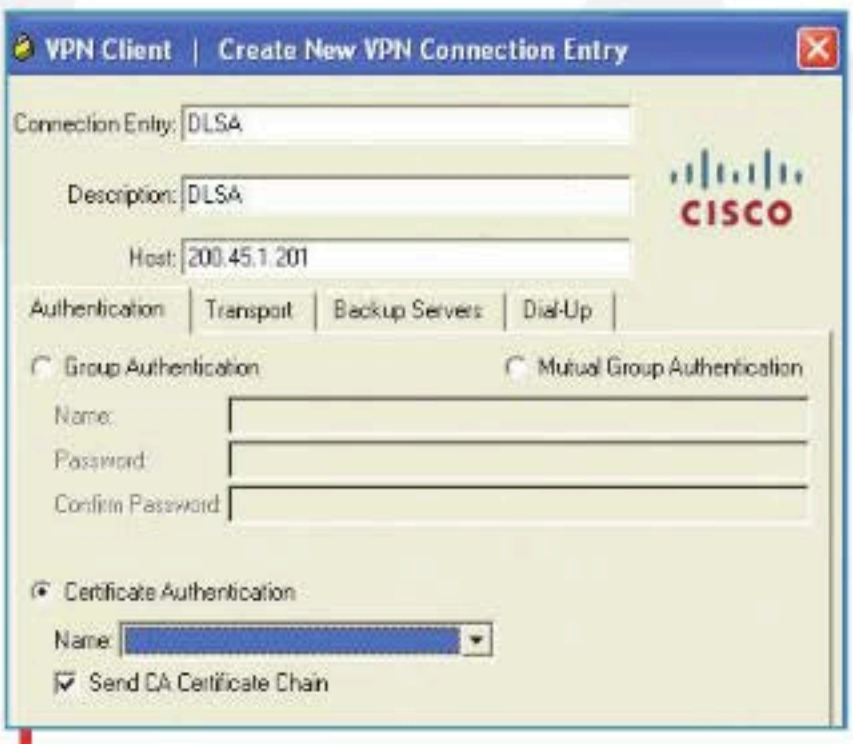
Instalación de uno de los clientes de VPN más populares. Este cliente por software permite a las PCs conectarse a una red corporativa privada.

Modo transporte

La VPN en modo transporte es aquella en la cual solo los datos del paquete IP son cifrados y, por lo tanto, las cabeceras del paquete original se mantienen intactas. Generalmente este tipo de VPN se da en las comunicaciones host-to-host dentro de una red; y son las más utilizadas para servicios que necesiten una alta tasa de seguridad sin comprometer calidad de tiempo de codificación.

Túnel IPsec

Aunque IPsec **es un protocolo de construcción de VPN, se vale de otros protocolos para su funcionamiento. Uno de estos protocolos es el denominado** ISAKMP (*Internet Security Association and Key Management Protocol*) **que, en conjunto con** IKE (*Internet Key Exchange*)**, permite el intercambio de claves de seguridad en Internet.**



Configuración del cliente para la fase de autenticación. En este caso, se realizará mediante un certificado enviado por el administrador de red.

En el caso de la VoIP o el VoRT, pueden utilizarse sin ningún inconveniente. Una de las principales desventajas de esta arquitectura de VPN es que resulta muy vulnerable a ataques de seguridad informática en la capa de transporte (ruteo), ya que cualquier actividad que modifique las tablas de rutas en los equipos intermedios permite que los paquetes puedan ser modificados o alterados o, incluso, solo vistos por un tercero. Esto no permite que las comunicaciones sean no repudiables.

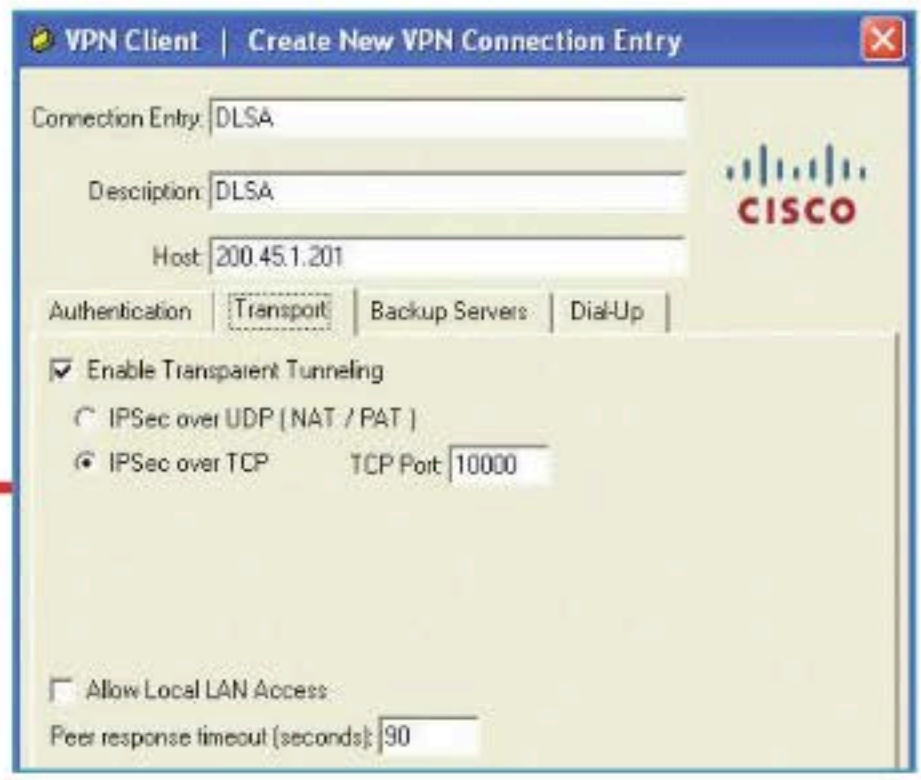
Seguridad

Ambas técnicas tienen en común que, desde el punto de vista de seguridad informática, su máxima debilidad es el compromiso del emisor o el receptor de las comunicaciones ya que, una vez conseguida la clave de encriptación o –en su defecto– una vez comprometido alguno de los extremos, resulta muy difícil de detectar en los cortafuegos y por los IDS. Para solventar este inconveniente, en algunos casos se utiliza una estructura más complicada de autenticación y encriptación que permite el no repudio de la comunicación y la encriptación del sistema.

Implementación

Para realizar ambos tipos de VPN, se utiliza el protocolo IPSec, que es un protocolo que se definió en 1995, pero que recién se estandarizó en el año 2005. Este protocolo realiza la encriptación y la autenticación del paquete IP original, sea este IPv4 o IPv6.

La inclusión de este protocolo es opcional en IPv4 y obligatoria en IPv6; además, provee de las funcionalidades de validación de integridad y no repetición. A su vez, este protocolo se compone de dos protocolos que proporcionan estas funcionalidades por separado: el **AH** (*Authentication Header*) y el **ESP** (*Encapsulating Security Payload*). La única diferencia entre los dos modos radica en que IPsec, para el modo túnel, le adiciona una cabecera de enrutamiento al protocolo original y encripta lo que está en su interior, modificando completamente el paquete, mientras que, en el modo transporte, solo encripta el payload interno.
Existen otros protocolos para VPN; entre los más conocidos, están **GRE** (*Generic Routing Encapsulation*), que solo se usa para túneles en Internet, y **L2TP** (*Layer 2 Tunneling Protocol*), que es utilizado de forma similar a GRE.
Los pasos para establecer un túnel VPN en ambos casos son similares, y los dispositivos para establecerlos solo difieren en si se trata de hosts particulares o si es una red completa la que se quiere conectar. En el caso de los hosts que se conectan a una puerta de entrada de VPN, la conexión se hace mediante software dedicado. Este software debe ser configurado para establecer los mismos parámetros y protocolos que el dispositivo destino (llamado en la jerga técnica, **terminador**).
Luego de indicar los parámetros (que pueden estar presentes en un archivo que pasa el administrador), debe suministrarse un usuario y una contraseña que sirven para la fase de autenticación. Por lo general, la VPN se arma en tres fases, una de preautenticación, una de encriptación y una de autenticación final. En el caso de la VPN de túnel, además existe una etapa de encapsulamiento dentro de un paquete IP, propio del dispositivo que genera la VPN. Una vez realizada la conexión, la seguridad y confiabilidad de la VPN dependen de la velocidad con la que cambian las claves de encriptación, la longitud de estas y la velocidad de procesamiento, entre otros factores clave.
En la actualidad, para la preautenticación se suelen usar funciones hash que permiten autenticar contra el terminador, el cual posee una base de datos. En la fase de encriptación, se usan los algoritmos MD5 y 3DES entre otros. ■



Configuración del cliente de VPN para PC en modo transporte. Puede verse que solo se especifica el protocolo de transporte por utilizar.

VPN de acceso remoto, site-to-site e internas

Analizaremos las características principales que requiere una VPN de acceso remoto, los tipos existentes y sus beneficios.

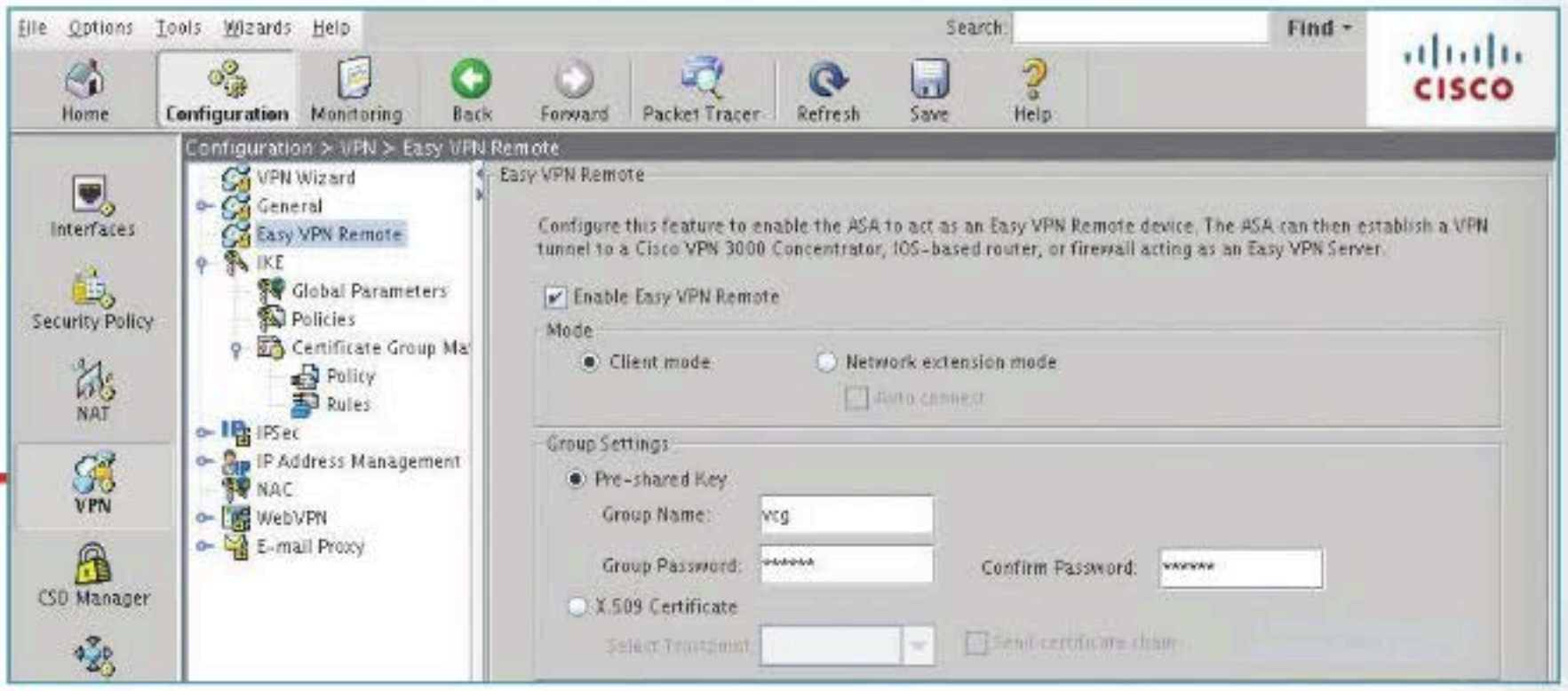
Las VPN site-to-site conectan redes enteras entre sí a través de otra u otras en común. En este tipo de VPN, las terminales no necesitan ejecutar un cliente de VPN, reciben y envían tráfico TCP/IP normal, y este pasa por un gateway de VPN. El gateway de VPN es el responsable de encapsular y encriptar el tráfico saliente, enviándolo a través de un túnel hacia otro gateway de VPN en el sitio de destino. Al recibir cada paquete, se remueve el encabezado, se desencripta el contenido y se reenvía hacia la terminal en la red privada de destino. Si la terminal dentro de la red privada devuelve una respuesta, el gateway de VPN realiza el proceso inverso, encriptando el contenido y enviándolo al otro VPN gateway a través de Internet.

Ejemplo

Un ejemplo clásico para una VPN site-to-site son las sucursales de una misma empresa. Típicamente se conecta cada sucursal a casa central; de esta forma, los usuarios en las sucursales pueden acceder a los recursos disponibles de casa central como si estuvieran trabajando en ella. El protocolo más utilizado para estos casos es IPSec. La mayoría de los routers y firewalls actuales soportan IPSec, por lo que permite interoperabilidad, es decir, que es posible utilizar distintas marcas/modelos de routers para establecer un túnel. De todas maneras, lo recomendable es utilizar productos de la misma marca para evitar comportamientos inesperados.

Protocolos

Otro protocolo para generación de VPN site-to-site es el *Multiprotocol Label Switching* (**MPLS**), pero debemos tener en cuenta que no provee encriptación de datos en forma nativa. Solamente tuneliza y canaliza los paquetes por la red del proveedor del servicio. Este servicio es más costoso que una típica conexión a Internet, pero provee mayores prestaciones. **PPTP** (*Point to Point Tunneling Protocol*) y **L2TP** (*Layer 2 Tunneling Protocol*) sobre IPSec fueron incluidos en distintas versiones de Windows. Sin embargo, ninguno de estos permite



En esta imagen, podemos ver la interfaz de configuración de una Easy VPN en un firewall Cisco ASA5505.

realizar conexiones site-to-site, ya que requieren de un cliente. Además, debemos tener en cuenta que tanto PPTP como L2TP tienen numerosos problemas de seguridad y no deberían utilizarse. Por otro lado, es muy común encontrar VPN SSL, que son llamadas *client-less* (no requieren un cliente), pero de hecho utilizan un web browser como cliente. Por este motivo no son apropiadas para establecer VPN site-to-site. Dada su simplicidad de implementación y actualización, este tipo de VPN es utilizado para acceder a aplicaciones internas.

Consideremos que, en empresas grandes, es común encontrar que se destinan estas VPN como medidas de seguridad adicional por sobre las aplicaciones críticas. De esta manera, se asegura que el tráfico por dentro de la empresa viaje encriptado, y se establece un método doble de autenticación para acceder a las aplicaciones sensibles. Su funcionamiento es bastante simple, ya que suelen descargar y ejecutar algún software liviano, como por ejemplo, Java applets, controles ActiveX, o programas Win32 temporales que se eliminan una vez finalizada la sesión.

Soluciones

Las soluciones VPN pueden transportar tráfico de misión crítica, voz o datos de aplicaciones cliente/servidor sin comprometer la calidad de la comunicación. Las funciones de red integradas en los routers, como QoS, ruteo, soporte multicast, permiten conservar la calidad y confiabilidad del tráfico dentro de la VPN. Los productos Cisco ofrecen una variedad de VPN según sea el dispositivo por utilizar. A continuación, ofrecemos un detalle de las características y los beneficios principales de cada una de ellas:

- **IPsec VPN**: es la opción más común para establecer VPN site-to-site. Provee encriptación avanzada para asegurar la información en tránsito y soporta QoS. Debemos tener en cuenta que es recomendable utilizarla cuando se requiera interoperabilidad entre productos de distintos proveedores.

- **Easy VPN**: esta es una solución económica, ideal para pequeñas sucursales, con un soporte de IT limitado. Resulta perfecta para grandes implementaciones, en las que no es posible realizar configuraciones en cada uno de los dispositivos remotos. Su principal beneficio radica en la posibilidad de implementar configuraciones de políticas que se aplican de manera dinámica en los equipos. También soporta QoS. Su uso es recomendado para simplificar la configuración y administración de numerosos dispositivos, pero las características y flexibilidad que ofrece son limitadas. Se aconseja su uso solamente en los casos en los que se utilice un mix de productos Cisco y se requiera un rápido deploy. Esta tecnología está disponible únicamente en firewalls y VPN concentrators Cisco.

- **Dynamic Multipoint VPN**: este tipo de VPN es aconsejable cuando las distintas sucursales requieran comunicarse entre ellas a través de un enlace WAN público, o Internet. En estos casos, DM VPN es la solución indicada. Los beneficios que ofrece son configuración y administración simplificada para túneles GRE (*Generic Routing Encapsulation*) punto a punto. GRE es un protocolo desarrollado por Cisco, que ofrece encapsulamiento de varios protocolos sobre un vínculo punto a punto. Permite generar túneles spoke-to-spoke, que permiten rutear datos entre distintos túneles. Soporta QoS, multicast y ruteo. Es recomendable utilizarlo cuando se requiera ruteo entre distintos túneles.
Este tipo de VPN solo está disponible en routers Cisco.

La serie de routers Cisco 1900 provee aceleración de encriptación de VPN, Dynamic Multipoint VPN y Enhanced Easy VPN, entre otras funciones.

- **Group Encrypted Transport (GET) VPN**: se trata de una solución conocida como tunnel-less, que es útil en redes con redes WAN privadas, y también en sitios remotos que necesitan establecer una comunicación con los otros directamente. GET VPN provee eficiencia en el uso del ancho de banda sin que se vea afectada la encriptación de los datos. Además, simplifica la integración de la encriptación sobre redes MPLS (*Multiprotocol Label Switching*), que no proveen esta funcionalidad. Solo está disponible sobre routers Cisco. ■

Configuración de OpenVPN site-to-site

Para implementar OpenVPN **como gateway de VPN, debemos configurar OpenVPN en dos equipos y establecer el túnel. Una vez hecho esto, necesitamos configurarlos como gateways para que reciban y reenvíen todo el tráfico hacia las otras redes. Hay que tener en cuenta que cada equipo de la red que utiliza la VPN debe tener rutas hacia este equipo a fin de direccionar el tráfico que va hacia un equipo detrás de la VPN. Para evitar esta complejidad adicional, se recomienda que el host OpenVPN sea también el gateway de Internet; de esta forma, se utilizaría este como default gateway.**

Seguridad en redes VPN

Las VPN son un recurso de gran valor en los escenarios donde necesitamos vincular nuestros sitios o equipos a través de redes no seguras.

Las redes privadas virtuales (VPN) nos permiten establecer conexiones seguras a través de redes no seguras, como Internet. Las VPN protegen la información que transferimos a través de ellas mediante un conjunto de protocolos y nos permiten realizar diversas configuraciones, como por ejemplo, conectar de forma segura dos redes a través de Internet como si estuviesen conectadas en un mismo sitio en forma directa.
El hecho de realizar conexiones seguras a través de redes inseguras nos brinda grandes beneficios; quizás los más significativos son la flexibilidad y el costo.

Cuadro de diálogo donde se agrega una conexión VPN de tipo PPTP en Ubuntu Desktop 12.10.

Mediante VPN, los usuarios de nuestra red pueden seguir conectados a través de conexiones seguras por medio de Internet, aunque no se encuentren físicamente en su lugar habitual, logrando de este modo la independencia de su ubicación geográfica y aumentando así la flexibilidad de nuestra infraestructura.
Al realizar conexiones seguras a través de Internet, evitamos los altos costos relacionados con los vínculos privados, siempre que el ancho de banda contratado sea el adecuado.

LAS VPN INDEPENDIZAN AL USUARIO DE SU UBICACIÓN, FLEXIBILIZANDO LA RED.

IPSec

Los tipos de VPN son básicamente tres: VPN IPSec, VPN SSL y VPN PPTP. Nos centraremos en las VPN del tipo IPSec, ya que son el estándar para redes privadas virtuales y, por consiguiente, están incluidas en todos los sistemas operativos y dispositivos dedicados que implementan conexiones VPN.
Una VPN implementada con IPSec nos asegura tres conceptos fundamentales para proteger la información que transferimos a través de ella. A continuación, los describimos:

- **Autenticación**: IPSec realiza la verificación de las identidades de ambos extremos de las VPN mediante métodos de autenticación. Existe un gran número de modalidades de autenticación con las que contamos a la hora de configurar nuestras redes privadas virtuales; las más utilizadas son las claves precompartidas, las claves RSA y los certificados digitales.
- **Integridad**: las conexiones VPN aplican mecanismos especializados en la preservación de la integridad de los datos a fin de proteger la información de modificaciones por parte de intrusos durante la transferencia. La protección de la integridad se realiza mediante algoritmos denominados HASH, cuya aplicación se explica a continuación. A cada paquete de datos que se va a enviar desde un extremo a otro de la red privada virtual, se le agrega información de verificación (HASH) generada a partir de su contenido. Una vez recibidos los datos en el extremo destino,

se recalcula el HASH a partir de la información recibida y se compara el resultado con el HASH calculado en el extremo origen. En caso de detectar diferencias, se informa una anomalía de la integridad de los datos al extremo que envió la información. Los algoritmos de HASH que podemos utilizar son el Digesto de Mensaje (MD5) y el Algoritmo de Hash Seguro (SHA); MD5 es el protocolo más antiguo de los dos y se encuentra en proceso de reemplazo por SHA.

- **Confidencialidad**: uno de los requisitos más importantes para una VPN es la protección de la información ante el acceso por parte de usuarios no autorizados; este es un requisito vital ya que la información viaja a través de redes no seguras, como Internet. Algunos de los algoritmos que se utilizan para la encriptación de los datos a fin de protegerlos de usuarios no autorizados son el Estándar de Encriptación de Datos (DES) y su versión triple (Triple DES), como también el Estándar de Encriptación Avanzada (AES).

Modos de funcionamiento de IPSec

Es posible realizar la configuración de las redes privadas virtuales o VPN con tecnología IPSec, de esta forma nos aseguramos que funcionen en dos modalidades según nuestras necesidades: modo túnel y modo transporte. Si deseamos utilizar el **modo túnel** para nuestra VPN, se establece en los equipos que se ubican en los extremos de las redes que estamos vinculando mediante IPSec. Por ejemplo podemos aplicar este tipo de red privada virtual cuando necesitamos conectar dos redes LAN que se ubican en sitios distintos. Por otra parte, si lo que buscamos es proteger la conexión desde su origen hasta su fin es necesario utilizar el **modo transporte**, en éste caso la VPN IPSec se establece de extremo a extremo desde el cliente hacia el servidor donde se requiere acceder de forma segura.

Establecimiento de la conexión

El establecimiento de la conexión es un punto clave en la tecnología IPSec, ya que deben intercambiarse datos de configuración a través de redes no confiables, como Internet. El establecimiento de una VPN IPSec se realiza mediante el protocolo IKE (intercambio de claves de Internet), el cual efectúa la negociación de la conexión privada virtual en dos fases.

- **Fase 1 – Canal de administración**

En la primera fase, se utilizan algoritmos especiales para realizar el intercambio de datos entre los extremos de la VPN a fin de realizar su autenticación y lograr establecer una asociación de seguridad (SA) en la que se gestionarán los canales de datos mediante los cuales se enviará la información entre los extremos de la VPN.

Propiedades de una conexión VPN IPSec configurada en un equipo con sistema operativo Windows 7.

- **Fase 2 – Canales de comunicación**

Una vez establecido el canal de administración entre los extremos de la VPN, este se utiliza para gestionar las asociaciones de seguridad (SA) que tienen como finalidad la transferencia segura de datos entre los extremos de la red privada virtual.

Consideraciones de configuración

Debemos tener en cuenta que, para que una VPN IPSec se establezca correctamente, es necesario configurar los métodos de autenticación, y los algoritmos de integridad y encriptación de ambas fases del protocolo IKE de manera coherente en ambos extremos de la VPN; en caso contrario, la negociación de la red privada virtual no será posible.

IPSec es el estándar de Internet para la implementación de redes privadas virtuales, por lo que tiene que ser la primera opción para considerarse en el caso de que necesitemos implementar VPN en nuestra red. ■

Sitios de interés

Si bien en el momento de implementar una red privada virtual tendremos que recurrir a la documentación propia del equipo donde estemos realizando la configuración, un sitio por visitar para ampliar nuestra mirada sobre la teoría de las VPN de tecnología IPSec es la página web **www.ipsec-howto.com/spanish**. En cuanto a las VPN de tipo SSL, un exponente del software libre es el paquete OpenVPN, que está disponible para prácticamente todos los sistemas operativos. El sitio oficial es **www.openvpn.net**.

Software recomendado: Hamachi

Se trata de una aplicación cliente VPN muy fácil de usar que se encarga de establecer una conexión segura entre varias computadoras mediante P2P, a través de Internet.

Hamachi es una pequeña aplicación gratuita (hasta 5 clientes) que fue concebida por un desarrollador independiente y, luego, adquirida por LogMeIn, orientada al ámbito gamer, aunque muy pronto logró desembarcar en otros ambientes, como el uso de redes VPN caseras, en PyMEs e, incluso, en entornos corporativos.

Esta práctica herramienta tiene la particularidad de no ser afectada por posibles obstáculos típicos, como routers o firewalls; y está disponible tanto para Windows como para Mac OS X, y una reciente versión Beta para entornos Linux.

Podremos conectar la PC de casa con la de la oficina, o la de otro familiar o amigo (o incluso todas ellas juntas), como si estuviesen en la misma red local. Los usos que podemos darle son variados: compartir archivos, impresoras o aplicaciones (sistemas contables, de stock o de control) entre la casa y la oficina, o entre dos o más sucursales de la oficina, jugar en red con juegos que no tienen la posibilidad de ser jugados vía Internet, pero sí mediante la red local.

Todas las comunicaciones que Hamachi realiza están codificadas por algoritmos de encriptación, por lo tanto, son totalmente seguras. La interfaz del programa es una pequeña ventana muy fácil de utilizar.

Se puede descargar la última versión disponible de Hamachi desde su sitio oficial: **https://secure.logmein.com/products/hamachi/download.aspx**.

Al instalarse, Hamachi crea un adaptador de red virtual. Windows detecta una nueva red, que debemos señalar como pública.

Instalación

La instalación es simple. Solo debemos ir confirmando los distintos pasos del asistente con el botón **Siguiente**, hasta **Terminar** el proceso. Hamachi instalará un adaptador virtual de red, es decir, en el administrador de dispositivos aparecerá una placa de red extra, la cual simula Hamachi, para llevar a cabo las conexiones con su nodo principal y con las PCs que deseemos conectarnos.

Luego, aparecerá en nuestra pantalla un pequeño panel, en el cual figura (arriba, en números grandes) la dirección IP virtual que nos han asignado.

Puesta en marcha

Del lado izquierdo, en la parte superior del panel principal se ubica el botón que permite encender los servicios de Hamachi, los cuales al arrancar no se activan en forma automática; tendremos que hacer clic sobre él para ponerlo en marcha. Más arriba, aparece el menú **Red**, debemos ingresar en él para **Crear una nueva red** o **Unirnos a una red existente**.

Al crear una nueva red, ingresamos un nombre cualquiera dentro del recuadro **ID de Red** y tecleamos una contraseña de acceso en el campo de abajo.

Varias redes pueden ser creadas, y todas ellas aparecerán en la ventana del Hamachi. Estas pueden ser eliminadas cuando ya no las necesitemos, haciendo un clic derecho sobre la red deseada y **Eliminar**.
Podremos unirnos a una red existente solo si conocemos su nombre y su contraseña, teniendo muy en cuenta escribir de manera correcta el nombre de la red (mayúsculas, minúsculas y espacios son tenidos en cuenta).
En el panel principal, aparecerán las redes a las cuales nos hemos conectado, junto con los usuarios que pertenecen a ellas –estén actualmente conectados o no– y su correspondiente IP virtual.
Dichos usuarios aparecerán en verde si están actualmente conectados a esa red y, en gris claro, si están desconectados de ella. Ante cualquier problema de conexión o para verificar que la creación de la red y la comunicación con los demás equipos se realizó correctamente, podemos hacer clic derecho sobre cada uno de los demás clientes y elegir la opción **Hacer ping**. Ante nosotros, se abrirá una ventana de consola en la que se dispara un comando ping a esa IP en forma reiterada, para comprobar si la conexión es satisfactoria.
Para ingresar en los recursos compartidos de otro cliente de nuestra red, debemos hacer clic derecho en el equipo deseado y, luego, ingresar en **Examinar...**
Al instante, aparecerá una ventana del Explorador de Windows que muestra las unidades e impresoras que están siendo compartidas con esta red en el otro extremo. Además, Hamachi permite enviar mensajes instantáneos a los usuarios de las redes a las cuales nos hemos conectado, desde el menú contextual de cada usuario y **Chat**.

El panel de configuración de Hamachi es muy simple e intuitivo.

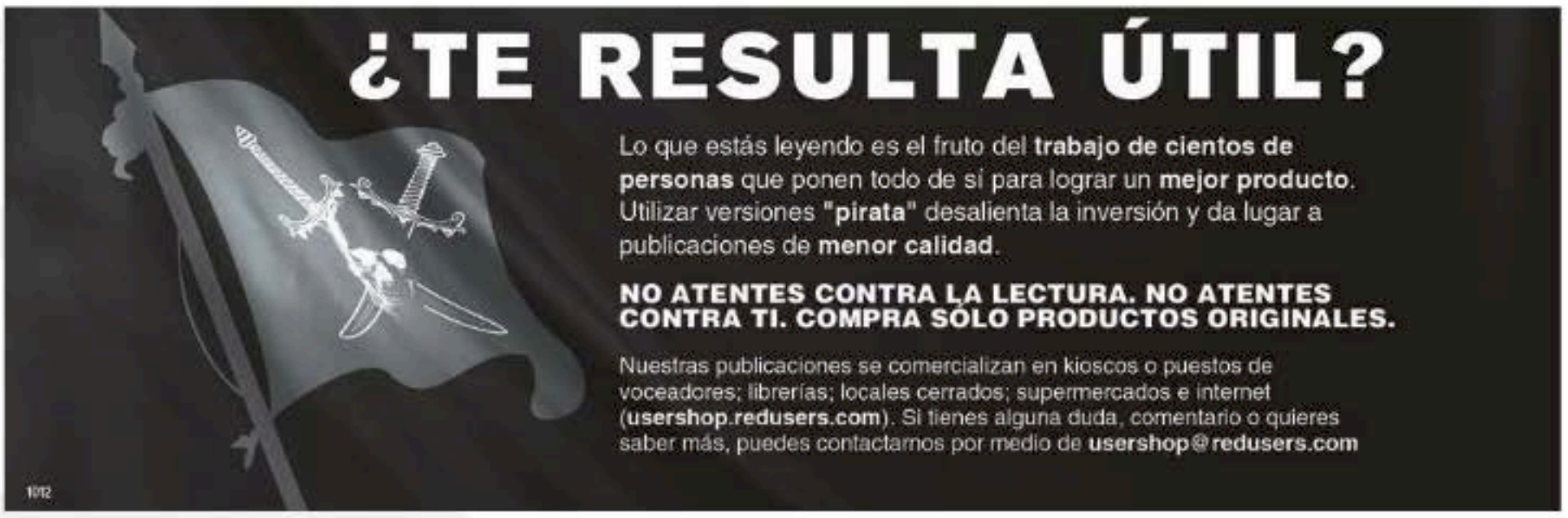
Configuración

Desde el menú **Sistema** es posible ingresar en el panel **Preferencias**, desde donde podremos activar o desactivar las tres funciones principales del programa:

- **Compresión**: disminuye la cantidad de datos por transferir entre los nodos de la misma red, pero requiere mayor cantidad de recursos (en especial procesador) para comprimir la información al enviarla y recibirla.
- **Cifrado**: requiere también mayor consumo de recursos del sistema, pero es altamente recomendable que esté activada para que los datos transferidos entre los nodos de nuestra red no puedan ser interpretados si se logra interceptarlos.
- **Actualizaciones automáticas**: se recomienda dejar activada esta opción, ya que Hamachi se actualiza en forma constante, mejorando su funcionamiento.

Ventajas

A diferencia de otros clientes para redes privadas virtuales, con Hamachi no es necesario abrir puertos en el router, ni configurar o desactivar firewalls. Además, no altera la configuración del adaptador de red principal: si deseamos desconectarnos de esa red, simplemente basta con cerrar el programa. ■



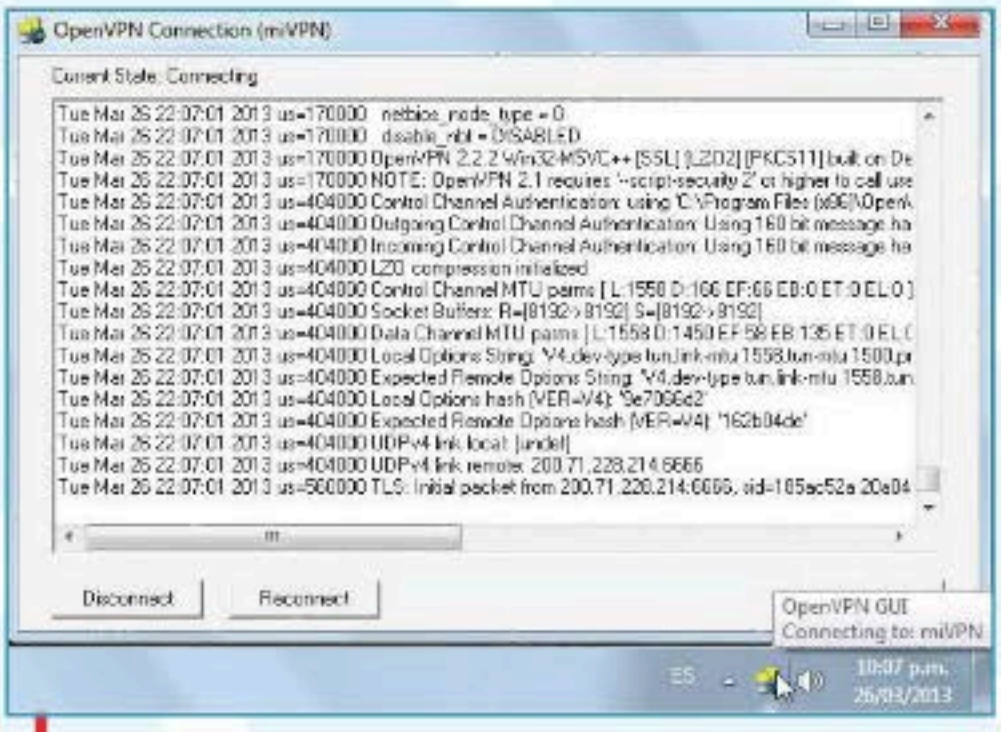
OpenVPN

Una solución robusta que nos permite establecer conexiones VPN SSL multiplataforma y sin preocuparnos por los costos de licenciamiento.

Si lo que necesitamos es una herramienta que nos permita implementar redes privadas virtuales (VPN) de forma flexible y sin costos de licenciamiento, una opción que no podemos dejar de tener en cuenta es **OpenVPN**. Se trata de una solución con capacidades para desplegar **VPN SSL**; se basa en la utilización de la misma tecnología que protege los accesos a los sitios web seguros en Internet. La solución es desarrollada por una comunidad internacional de programadores y está disponible para una amplia gama de sistemas operativos, entre los que podemos nombrar a GNU/Linux, Solaris, FreeBSD, NetBSD, Mac OS X y Microsoft Windows desde la versión 2000 en adelante.

Funcionamiento

En el momento de la instalación, OpenVPN crea en el equipo una interfaz virtual, mediante la cual se enviarán y recibirán los datos encriptados con el otro extremo de la VPN. Con el fin de adaptarse a nuestras necesidades, OpenVPN puede funcionar en dos modos: el **modo router** (**Tun**) y el **modo bridge** (**Tap**).
El primer modo es el más utilizado y establece una conexión punto a punto virtual a nivel IP, es decir, los paquetes ingresan por la interfaz virtual en uno de los extremos de la VPN, y son encriptados y ruteados hacia el otro extremo, donde son desencriptados y ruteados hasta el destino. El modo bridge establece una conexión segura entre las interfaces virtuales de ambos extremos de la VPN a nivel Ethernet. Este tipo de conexiones se utiliza para conectar dos sitios remotos a nivel de capa de enlace, como si estuviesen enlazados a un mismo switch.



Un cliente con Windows, iniciando una conexión con un servidor VPN mediante la herramienta **OpenVPN GUI**.

Métodos de autenticación

OpenVPN nos permite utilizar dos métodos para la autenticación de los extremos de la VPN: mediante una clave precompartida o utilizando certificados digitales emitidos por una autoridad certificante (CA). La primera opción es la más sencilla de configurar, simplemente se comparte una clave entre el extremo que tiene el rol de cliente y el que tiene el rol de servidor; presenta como desventaja la necesidad de escribir en texto plano la clave precompartida en los archivos de configuración, y la poca escalabilidad, ya que necesitamos crear una nueva conexión entre el servidor y cada cliente.
El método de autenticación mediante certificados digitales es la solución más robusta y escalable en escenarios con múltiples clientes ya que delega la emisión de credenciales de acceso en una autoridad certificante (CA). Si bien esta última alternativa nos exige un esfuerzo adicional, es la mejor opción para los escenarios donde la cantidad de clientes VPN es importante.

Configuración

Si bien existen interfaces gráficas para iniciar o detener las conexiones VPN, debemos realizar la configuración de la herramienta al estilo Linux mediante archivos de texto.

Administración

OpenVPN nos permite la gestión centralizada de las conexiones en nuestros servidores VPN mediante una interfaz de consola telnet o a través de interfaces gráficas como **OpenVPNControl**. Las ventajas de esta interfaz son las siguientes:

- No tiene costos de licenciamiento.
- Multiplataforma.
- Las conexiones VPN no presentan inconvenientes cuando atraviesan por un firewall ni cuando nos encargamos de aplicar traducción de direcciones (NAT) .

Como OpenVPN todavía no es un estándar, como sí lo es IPSec, aún no está soportado en la mayoría de los dispositivos de seguridad dedicados, como los firewalls empresariales. ■

PRÓXIMA ENTREGA

23

TELEFONÍA IP

En este fascículo veremos los alcances de la tecnología VoIP y las ventajas que ofrece sobre la telefonía convencional. También conoceremos las plataformas más utilizadas y los peligros que existen, como el sniffing.

Técnico en REDES &SEGURIDAD

PROFESORES EN LÍNEA
profesor@redusers.com

SERVICIOS PARA LECTORES
usershop@redusers.com

SOBRE LA COLECCIÓN

CURSO VISUAL Y PRÁCTICO QUE APORTA LOS SABERES NECESARIOS PARA FORMAR TÉCNICOS EXPERTOS EN REDES Y SEGURIDAD. INCLUYE UNA GRAN CANTIDAD DE RECURSOS DIDÁCTICOS COMO INFOGRAFÍAS, GUÍAS VISUALES Y PROCEDIMIENTOS REALIZADOS PASO A PASO.

Con la mejor metodología para llevar adelante el montaje y mantenimiento de las redes informáticas y con los aspectos clave para brindarles la protección necesaria, esta obra es ideal para aquellos aficionados que deseen profundizar sus conocimientos y para quienes quieran profesionalizar su actividad.

REDES &SEGURIDAD 00022
9 789871 857784

CONTENIDO DE LA OBRA