

Redes Privadas Virtuales

Isaac Clerencia

Warp Networks S.L.

17 de junio de 2005

- 1 ¿Cómo funciona una VPN?
 - ¿Qué es una VPN?
 - Escenarios
- 2 Tecnologías VPN
 - IPSec
 - PPTP
 - L2TP
 - VPNs SSL
- 3 OpenVPN
 - Características principales
 - ¿Cómo funciona?
 - Seguridad en OpenVPN
 - VPNs y redes
 - Configuración
- 4 Finalizando

Índice

- 1 ¿Cómo funciona una VPN?
 - ¿Qué es una VPN?
 - Escenarios
- 2 Tecnologías VPN
 - IPSec
 - PPTP
 - L2TP
 - VPNs SSL
- 3 OpenVPN
 - Características principales
 - ¿Cómo funciona?
 - Seguridad en OpenVPN
 - VPNs y redes
 - Configuración
- 4 Finalizando

¿Qué es una VPN?

VPN

Red IP privada y segura que pasa a través de otra red IP no segura, normalmente Internet

WANs antes de las VPNs

- Las empresas contrataban costosos circuitos dedicados entre oficinas
- La popularidad de Internet proporcionó ancho de banda barato pero inseguro
- Tráfico a través de Internet:

Cabecera IP	Cabecera TCP/UDP	Datos Aplicación
----------------	---------------------	------------------

Seguridad de la VPN

Una VPN garantiza las siguientes condiciones:

- Confidencialidad
- Autenticidad
- Integridad

Tráfico a través de una VPN

Para cumplir las condiciones anteriores, los paquetes IP que se desean transmitir:

- Se cifran para garantizar la confidencialidad
- Se firman para garantizar la autenticidad e integridad

El paquete resultante se encapsula en un nuevo paquete IP y se envía a través de la red insegura al otro extremo de la VPN:



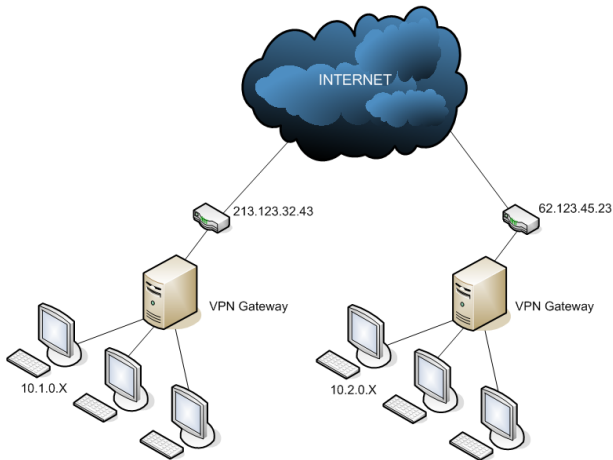
Escenarios típicos de VPNs

- Interconexión de redes privadas a través de Internet
- Road Warriors

Interconexión de redes privadas

- Ejemplo: conexión de dos oficinas de una empresa
- Se establece una VPN entre dos gateways, cada uno de una red privada
- Las máquinas de las redes utilizan esos gateways como routers
- Cuando un gateway recibe un paquete dirigido a la red privada del otro extremo lo envía a través de la VPN de modo seguro
- ¡Cuidado!, el tráfico sólo es protegido por la VPN en el recorrido entre los dos gateways

Interconexión de redes privadas: esquema



Road warriors

- Ejemplo: trabajadores remotos (Road Warriors)
- Cada persona con permiso puede conectar desde cualquier lugar
- El ordenador debe contar con un cliente VPN, que establece una conexión al concentrador de VPNs de la red corporativa
- A partir de ese momento todo el tráfico desde el ordenador a la red corporativa queda protegido por la VPN

Índice

- 1 ¿Cómo funciona una VPN?
 - ¿Qué es una VPN?
 - Escenarios
- 2 **Tecnologías VPN**
 - IPSec
 - PPTP
 - L2TP
 - VPNs SSL
- 3 OpenVPN
 - Características principales
 - ¿Cómo funciona?
 - Seguridad en OpenVPN
 - VPNs y redes
 - Configuración
- 4 Finalizando

Características de IPSec

- Estándar de Internet
- No funciona sobre TCP/UDP si no directamente sobre IP
- Validación de usuarios:
 - Certificados X509 (SSL)
 - Claves secretas compartidas por ambos extremos
 - Claves RSA
- Complejo de configurar
- Problemas con NAT, resueltos en nuevas versiones (NAT-T)
- La negociación de la conexión utiliza el protocolo ISAKMP
- Más información: <http://en.wikipedia.org/wiki/IPsec>

Características de PPTP

- Tecnología creada por Microsoft
- Sesión PPP sobre un tunel GRE
- Inseguro: <http://www.schneier.com/pptp-faq.html>

Características de L2TP (Layer 2 Tunneling Protocol)

- Protocolo para crear túneles de nivel 2 sobre UDP
- Encapsula protocolos como PPP o Ethernet
- Los clientes pueden recibir fácilmente una dirección IP interna
- No proporciona características de seguridad, por lo que se suele utilizar para crear VPNs sobre túneles IPSec

Características de VPNs SSL

- No existe un estándar para VPNs SSL, sino varias implementaciones distintas
- Sencillez de configuración e implantación
- OpenVPN es una de las implementaciones más extendidas y su sencillez de utilización la hace idonea para este curso

Índice

- 1 ¿Cómo funciona una VPN?
 - ¿Qué es una VPN?
 - Escenarios
- 2 Tecnologías VPN
 - IPSec
 - PPTP
 - L2TP
 - VPNs SSL
- 3 OpenVPN**
 - Características principales
 - ¿Cómo funciona?
 - Seguridad en OpenVPN
 - VPNs y redes
 - Configuración
- 4 Finalizando

Características principales

- Solución VPN SSL flexible
- Software libre bajo licencia GPL
- Espacio de usuario, alta portabilidad
- Multiplataforma: GNU/Linux, *BSD, Mac OS X, Windows

Funcionalidad

- Establecer túneles de nivel 2 o 3 sobre un puerto UDP o TCP
- Permite establecer balanceo de carga entre varios servidores
- Confidencialidad, autenticidad e integridad usando OpenSSL
- Interfaz gráfica de configuración en Windows y Mac OS X

Interfaz tun

- Un interfaz `tun` es un adaptador de red virtual
- El sistema operativo lo ve como una conexión punto a punto
- Un programa de espacio de usuario puede abrir el interfaz `tun` y leer y escribir paquetes IP en la interfaz
- Un interfaz `tap` es similar pero a nivel Ethernet

¿Cómo usar un interfaz tun para construir una VPN?

- Contamos con interfaces tun en dos máquinas
- Escribimos una aplicación de red simple que:
 - Establece una conexión entre ambas máquinas
 - Copia lo que lee del dispositivo tun al socket
 - Copia lo que lee del socket al dispositivo tun
- Esta aplicación proporciona una VPN sencilla sin seguridad

UDP o TCP

- Puede funcionar tanto sobre UDP como sobre TCP
- Es preferible utilizar UDP
- El puerto utilizado (asignado por la IANA) es el 1194

Algunos conceptos de seguridad

- Criptografía de clave simétrica
- Criptografía de clave pública
- Autoridades de certificación

Bridging vs. routing

- Bridging (nivel 2): crea una LAN virtual en una única subred
- Routing (nivel 3): crea una nueva subred virtual y establece rutas entre las subredes

Ventajas del bridging

- Los broadcast pasan a través de la VPN, permitiendo que funcione software que depende de ellos
- No es necesario configurar rutas
- Puede utilizarse con cualquier protocolo que funcione sobre Ethernet: IPv4, IPv6, IPX, ...

Ventajas del routing

- Eficiencia
- Escalabilidad
- Sencillez de configuración (desde el punto de vista de OpenVPN)

Claves estáticas

Configuración de OpenVPN con claves estáticas

La configuración con claves estáticas ofrece la configuración más sencilla y son ideales para VPNs punto a punto y pruebas de concepto

Ventajas y desventajas del uso de claves estáticas

Ventajas

- Configuración sencilla
- No es necesario mantener una PKI X509

Desventajas

- Poca escalabilidad, un cliente, un servidor
- Un compromiso de la clave afecta a sesiones anteriores
- La clave debe estar en texto plano en cliente y servidor
- La clave debe ser intercambiada utilizando un canal seguro existente

Configuración con clave estática (I)

Generación de la clave estática

```
openvpn --genkey --secret static.key
```

Configuración del servidor

```
dev tun  
ifconfig 10.8.0.1 10.8.0.2  
secret static.key
```

Configuración del cliente

```
remote remoteip  
dev tun  
ifconfig 10.8.0.2 10.8.0.1  
secret static.key
```

Configuración con clave estática (II)

Comprimir los datos transmitidos por la VPN

Simplemente es necesario añadir la siguiente línea en ambos ficheros de configuración:

```
comp-lzo
```

Permitir al cliente acceder a la subred del servidor

Añadir en el cliente:

```
route 192.168.4.0 255.255.255.0
```

y activar el reenvío de paquetes IP en la máquina

Configuración con PKI

Infraestructura necesaria

- Una clave pública y una privada para cada servidor y para cliente
- Una clave pública y una privada para la CA, utilizada para firmar los certificados de los servidores y clientes

Easy RSA

Easy RSA es un conjunto de utilidades proporcionadas junto a OpenVPN para facilitar la creación de la infraestructura de clave pública

Índice

- 1 ¿Cómo funciona una VPN?
 - ¿Qué es una VPN?
 - Escenarios
- 2 Tecnologías VPN
 - IPSec
 - PPTP
 - L2TP
 - VPNs SSL
- 3 OpenVPN
 - Características principales
 - ¿Cómo funciona?
 - Seguridad en OpenVPN
 - VPNs y redes
 - Configuración
- 4 Finalizando

Resumen

- Las VPNs unen conceptos de redes y criptografía
- Las VPNs en espacio de usuario son una solución sencilla y elegante
- Las VPNs son un bloque básico para construir desde pequeñas soluciones de telecomunicación seguras a grandes WAN

Más información

- Página web de OpenVPN: <http://openvpn.net/>
- OpenVPN HOWTO: <http://openvpn.net/howto.html>
- Presentación sobre VPNs y OpenVPN:
<http://openvpn.net/papers/BLUG-talk/>