OpenVPN Server y la instalación de clientes y configuración en Debian 7

Por Michael David Under: Open Source On: 04 de abril 2014
Descargar tus eBooks gratuitos AHORA - 10 eBooks gratuitos de Linux para administradores

Este artículo detalla cómo obtener conectividad IPv6 en OpenVPN usando Debian Linux . El proceso ha sido probado en Debian 7 en un VPS KVM con IPv6 conectividad como el servidor, y un escritorio Debian 7. Los comandos se deben ejecutar como root.
Instalar OpenVPN en Linux

Instalar OpenVPN en Debian
¿Qué es OpenVPN?

OpenVPN es un programa que utiliza VPN SSL / TLS para crear conexiones VPN seguras y codificadas, para dirigir su tráfico de Internet, lo que impide fisgonear. Open VPN es muy capaz de atravesar de forma transparente a través de firewalls. De hecho, si la situación lo requiere, se puede ejecutar en el mismo puerto TCP como HTTPS (443), por lo que el tráfico indistinguibles y por lo tanto casi imposible de bloquear.

OpenVPN puede usar una variedad de métodos, tales como llaves pre-compartidas secretas, certificados, o nombres de usuario / contraseñas, para permitir que los clientes se autentican en el servidor. OpenVPN utiliza el protocolo OpenSSL e implementa muchas características de seguridad y de control, tales como la autenticación de desafío y respuesta, capacidad de inicio de sesión único, balanceo de carga y conmutación por error de características y soporte de múltiples daemon.
¿Por qué utilizar OpenVPN?

Piense en comunicaciones seguras - pensar OpenVPN. Si no quieres que nadie husmeando en su tráfico de Internet, utilizar OpenVPN para enrutar todo el tráfico a través de un altamente encriptados, túnel seguro.

Esto es especialmente importante cuando se conecta a redes WIFI pública en aeropuertos y otros lugares. Nunca se puede estar seguro de quién está husmeando en su tráfico. Puede canalizar el tráfico a través de su propio servidor OpenVPN para impedir la obtención.

Si se encuentra en cualquiera de los países que monitorean rutinariamente todos sus sitios web de tráfico y bloquear a voluntad, puede utilizar OpenVPN a través del puerto TCP 443 , para que sea indistinguible de tráfico HTTPS. Usted puede incluso combinar OpenVPN con otras estrategias de seguridad, como el tráfico de un túnel OpenVPN sobre un túnel SSL, para vencer a las técnicas de inspección profunda de paquetes que podrían ser capaces de identificar las firmas de OpenVPN.
Requisitos del sistema

OpenVPN requiere unos requisitos muy mínimos para funcionar. Un sistema con 64 MB de RAM y 1 GB de espacio en disco duro es suficiente para ejecutar OpenVPN. OpenVPN funciona en casi todos los principales sistemas operativos.
Instalación y configuración de OpenVPN en Debian 7
Instalar OpenVPN en servidor maestro

Ejecute el siguiente comando para instalar OpenVPN.

Apt-get install openvpn

De forma predeterminada, los scripts fáciles rsa se instalan bajo / usr / share / easy-rsa / 'directorio. Por lo tanto, tenemos que copiar estos scripts a la ubicación deseada, es decir / root / easy-rsa .

Mkdir / root / easy-rsa
cp-prv / usr/share/doc/openvpn/examples/easy-rsa/2.0 / root / easy-rsa

Generar certificado de CA y la clave de CA

Abrir el archivo ' vars 'y crea los siguientes cambios, pero antes de hacer los cambios que sugerimos para tomar copia de seguridad del archivo original.

Vars # cp {,. Orig}

Utilizando su editor de texto, configurar los valores predeterminados para fácil-rsa. Por ejemplo.

KEY_SIZE = 4,096
KEY_COUNTRY = "IN"
KEY_PROVINCE = "UP"
KEY_CITY = "Noida"
KEY_ORG = "Home"
KEY_EMAIL = "user@example.net"

Aquí, estoy usando la clave 4096 bits. Usted puede utilizar el 1024 , 2048 , 4096 o 8192 bits clave sería CUM.

Exportar los valores predeterminados mediante la ejecución del comando.

Source. / Vars

Limpiar los certificados generados con anterioridad.

. / Clean-all

A continuación, ejecute el comando siguiente para generar Certificado de CA y CA clave.

#. / Build-ca

Generar el certificado de servidor mediante la ejecución del comando. Sustituir el 'nombre de servidor' con su nombre-servidor.

Nombre-servidor #. / Build-key-server

Generar el Diffie Hellman PEM certificado.

#. / Build-dh

Generar el certificado de cliente. Sustituir el 'nombre del cliente con su cliente-name.

#. / Build-key nombre_cliente

Generar el código HMAC.

Openvpn - genkey - secreto / root / easy-rsa / keys / ta.key

Copie los certificados en los equipos cliente y servidor de la siguiente manera.

Asegúrese de que el ca.crt está presente tanto en el cliente y el servidor.
El ca.key clave debe ser en el cliente.
El servidor requiere server.crt , dh4096.pem , server.key y ta.key .
client.crt , client.key y ta.key deben estar en el cliente.

Para configurar las claves y certificados en el servidor, ejecute los comandos.

Mkdir-p / etc / openvpn / certs
Cp-pv / root / easy-rsa / keys / {ca. {Crt, clave}, nombre-servidor. {Crt, clave}, ta.key, dh4096.pem} / etc / openvpn / certs /

Configuración del servidor OpenVPN

Ahora tiene que configurar el servidor OpenVPN. Abrir el archivo ' / etc / openvpn / server.conf '. Por favor haga los cambios como se describe a continuación.

seguridad script del sistema 3
puerto 1194
udp proto
grifo dev

ca / etc / openvpn / certs / ca.crt
cert / etc / openvpn / certs / server-name.crt
clave / etc / openvpn / certs / server-name.key
dh / etc/openvpn/certs/dh4096.pem
tls-auth / etc / openvpn / certs / ta.key 0

servidor 192.168.88.0 255.255.255.0
ifconfig-pool-persistir ipp.txt
empujar "redirigir-gateway def1 bypass dhcp"
push "dhcp-option 8.8.8.8 DNS"
push "dhcp-option 8.8.4.4 DNS"

Keep Alive 1800 4000

cifrado DES-CBC-EDE3 # Triple-DES
comp-lzo

max-clientes 10

usuario nobody
nogroup grupo

persistir-key
tun-persistir

Conectarse openvpn.log
Estado status.log OpenVPN
verbo 5
mute 20

Habilitar el reenvío IP en el servidor.

Echo 1> / proc/sys/net/ipv4/ip_forward

Ejecute el comando siguiente para configurar OpenVPN para iniciar en el arranque.

Update-rc.d-f impagos openvpn

Iniciar servicio OpenVPN.

Service openvpn restart

Instalar OpenVPN en el Cliente

Ejecute el siguiente comando para instalar OpenVPN en la máquina cliente.

Apt-get install openvpn

Con un editor de texto, configurar la configuración del cliente OpenVPN en ' / etc / openvpn / client.conf ', en el cliente. Un ejemplo de configuración es la siguiente:

seguridad script del sistema 3
cliente
vpn_server_ip remoto
ca / etc / openvpn / certs / ca.crt
cert / etc / openvpn / certs / client.crt
clave / etc / openvpn / certs / client.key
cifrado DES-CBC-EDE3
comp-lzo sí
grifo dev
udp proto
tls-auth / etc / openvpn / certs / ta.key 1
nobind
auth-nocache
persistir-key
tun-persistir
usuario nobody

nogroup grupo

Ejecute el comando siguiente para configurar OpenVPN para iniciar en el arranque.

Update-rc.d-f impagos openvpn

Iniciar servicio OpenVPN en el cliente.

Service openvpn restart

Una vez que esté satisfecho de que OpenVPN está funcionando bien en IPv4 , aquí es cómo llegar a IPv6 de trabajo sobre OpenVPN.
Cómo trabajar con IPv6 en el servidor OpenVPN

Añada las siguientes líneas al final de la configuración del servidor ' / etc / openvpn / server.conf archivo '.

cliente a conectar / etc / openvpn / connect.sh cliente
desconexión de un cliente / etc / openvpn / disconnect.sh cliente

Estos dos scripts construir / destruir el túnel IPv6 cada vez que un cliente se conecta / desconecta.

Este es el contenido del cliente-connect.sh.

#! / Bin / bash
BASERANGE = "2a00: dd80: 003d: 000C"
ifconfig $ dev hasta
ifconfig $ dev agregar $ {} BASERANGE: 1001 :: 1/64
ip -6 añadir relincho de proxy 2a00: dd80: 003d: 000C: 1001 :: 2 dev eth0
exit 0

Mi anfitrión me asigna direcciones IPv6 del 2a00: dd80: 003d: 000C :: / 64 bloque. Por lo tanto, uso 2a00: dd80: 003d: 000C como BASERANGE. Modificar este valor de acuerdo con lo que su anfitrión le ha asignado.

Cada vez que un cliente se conecta a OpenVPN, este script asigna la dirección 2a00: dd80: 003d: 000C: 1001 :: 1 como la dirección IPv6 de la tap0 interfaz del servidor.

La última línea establece Vecino Descubrimiento de nuestro túnel. He añadido la dirección IPv6 del lado del cliente tap0 conexión como la dirección del proxy.

Este es el contenido del cliente-disconnect.sh .

#! / Bin / bash
BASERANGE = "2a00: dd80: 003d: 000C"
/ Sbin / ip -6 addr del $ {GAMA BASE} :: 1/64 $ dev dev
exit 0

Esto sólo elimina el IPv6 dirección túnel del servidor, cuando el cliente se desconecta. Modificar el

valor de BASERANGE según corresponda.

Hacer el ejecutable scripts.

Chmod 700 / etc / openvpn / cliente-connect.sh
Chmod 700 / etc / openvpn / cliente-disconnect.sh

Agregue las siguientes entradas al / etc / rc.local '(También puede modificar los sysctls apropiados en / etc / sysctl.conf).

echo 1> / proc/sys/net/ipv6/conf/all/proxy_ndp
echo 1> / proc/sys/net/ipv4/ip_forward
echo 1> / proc/sys/net/ipv6/conf/all/forwarding
/ Etc / init.d / firewall stop && / etc / init.d / firewall inicio

Estas entradas se activan Neighbor Discovery and Forwarding. También he añadido un servidor de seguridad.

Crear ' / etc / init.d / firewall 'y poner en el siguiente contenido.

#! / Bin / sh
# Descripción: Firewall
IPT = / sbin / iptables
IPT6 = / sbin/ip6tables
case "$ 1"
iniciar)
$ IPT-F ENTRADA
$ IPT-A estado ENTRADA-i eth0-m - ESTABLECIDO estado,-j ACCEPT RELACIONADOS
$ IPT-A INPUT-i eth0-p tcp - dport 22-j ACCEPT
$ IPT-A INPUT-i eth0-p icmp-j ACCEPT
$ IPT-A INPUT-i eth0-p udp - dport 1194-j ACCEPT
$ IPT-A INPUT-i pulse +-j ACCEPT
$ IPT-A FORWARD-i tap +-j ACCEPT
$ IPT-A FORWARD estado-m - ESTABLECIDO estado,-j ACCEPT RELACIONADOS
$ IPT-t nat-F POSTROUTING
$ IPT-t nat-A POSTROUTING-s 10.8.0.0/24-o eth0-j MASQUERADE
$ IPT-A INPUT-i eth0-j DROP
$ IPT6-F ENTRADA
$ IPT6-A-i eth0-ENTRADA m Estado - ESTABLECIDO estado,-j ACCEPT RELACIONADOS
$ IPT6-A INPUT-i eth0-p tcp - dport 22-j ACCEPT
$ IPT6-A INPUT-i eth0-p ICMPv6-j ACCEPT
$ IPT6-A FORWARD-s 2a00: dd80: 003d: 000C :: / 64 i tap0-o eth0-j ACCEPT
$ IPT6-A INPUT-i eth0-j DROP
exit 0
;;
Deténgase)
$ IPT-F
$ IPT6-F
exit 0

```
;;
*)
echo "Uso: / etc / init.d / firewall {start | stop}"
salida 1
;;
esac
```

Ejecutar '/ etc / rc.local 'e iniciar el servidor de seguridad.

```
# Sh / etc / rc.local
```

Esto completa las modificaciones del lado del servidor.
Introducción IPv6 trabajar con OpenVPN en el Cliente

Agregue la siguiente como las últimas líneas de su archivo de configuración del cliente ' / etc / openvpn / client.conf '.

```
# Crea el túnel ipv6
/ etc / openvpn / up.sh
abajo / etc / openvpn / down.sh
# Necesitará esta manera cuando el cliente se desconecta le dice al servidor
explícita-exit-notify
```

Los de arriba y abajo guiones construir / destruir los puntos extremos de cliente IPV6 de la conexión tap0 cliente cada vez que un cliente se conecta / desconecta hacia o desde el servidor OpenVPN.

Aquí está el contenido de up.sh.

```
#! / Bin / bash
IPV6BASE = "2a00: dd80: 3d: c"
ifconfig $ dev hasta
ifconfig $ dev IPV6BASE agregar $ {}: 1001 :: 2/64
ip -6 ruta por defecto a través de add $ {} IPV6BASE: 1001 :: 1
exit 0
```

El script asigna la dirección IPV6 2a00: dd80: 3d: c: 1001 :: 2 como la dirección IPV6 cliente y establece la ruta por defecto IPv6 a través del servidor.

Modificar IPV6BASE a ser el mismo que BASERANGE en la configuración del servidor.

Aquí está el contenido de down.sh.

```
#! / Bin / bash
IPV6BASE = "2a00: dd80: 3d: c"
/ Sbin / ip -6 addr del $ {} IPV6BASE :: 2/64 $ dev dev
/ Sbin / ip link set dev $ dev abajo
/ Sbin / ip route del :: / 0 a través de $ {} IPV6BASE :: 1
exit 0
```

Esto sólo elimina la dirección IPv6 del cliente y derriba la ruta IPV6 cuando el cliente se desconecta del servidor.

Modificar IPV6BASE a ser el mismo que BASERANGE en la configuración del servidor y crea script ejecutable.

Chmod 700 / etc / openvpn / up.sh
Chmod 700 / etc / openvpn / down.sh

Opcionalmente, modifique / etc / resolv.conf 'y añadir servidores IPV6 de Google para la resolución DNS.

nameserver 2001:4860:4860 :: 8888
nameserver 2001:4860:4860 :: 8844

Reinicie openvpn en el servidor y luego conectarse a él desde el cliente. Usted debe estar conectado. Visita test-ipv6.com ver que su conectividad IPv6 a través de OpenVPN está funcionando.
Enlaces de referencia

OpenVPN Página de Inicio