VPN host to LAN router usando OpenVPN

El propósito de este documento es describir cómo configurar una puerta de enlace OpenVPN para una red privada virtual host to LAN. Las secciones en las que se divide son los siguientes:

- **Porque usar OpenVPN como puerta de enlace VPN.**
- **Configuración por defecto para VPN host to LAN con OpenVPN.**
- **Autenticación con usuario y contraseña en OpenVPN.**
- **Autenticación con certificados digitales X.509 en OpenVPN.**
- **VPN en modo Router o Bridge.**
- **Estadísticas de VPN y mensajes de registro.**

Porque usar OpenVPN como puerta de enlace VPN.

Zeroshell, desde su primera version es capaz de actuar como puerta de enlace VPN en las conexiones de Host to Lan. Sin embargo, solo se admite VPN L2TP/IPSec. Esta combinación de túneles, el primero (IPSec) autenticado por el IKE con certificados X.509 y el segundo (L2TP) autenticado con nombre de usuario y la contraseña de Kerberos 5 KDC, ha mostrado sus límitaciones. Muchas de las dudas de L2TP/IPSec, que han sido resueltas mediante el uso de OpenVPN, se enumeran a continuación:

- **No es posible evitar el despliegue de un certificado X.509 y la clave privada relacionada con cualquier cliente de VPN. Este problema se puede resolver con la construcción de una PKI (Infraestructura de Clave Pública) para firmar y administrar certificados X.509. Zeroshell tiene el módulo de Autoridad de certificación X.509, pero en cualquier caso, su gestión podría tomar demasiado tiempo para algunas organizaciones.**

- **Después de la autenticación X.509, no es posible evitar la autenticación en segundo lugar con nombre de usuario y contraseña. Esta doble autenticación, en algunos casos, podría considerarse como una pérdida de tiempo, especialmente cuando el certificado se almacena en una tarjeta inteligente y para desbloquear la clave privada, se necesita introducir el codigo PIN.**

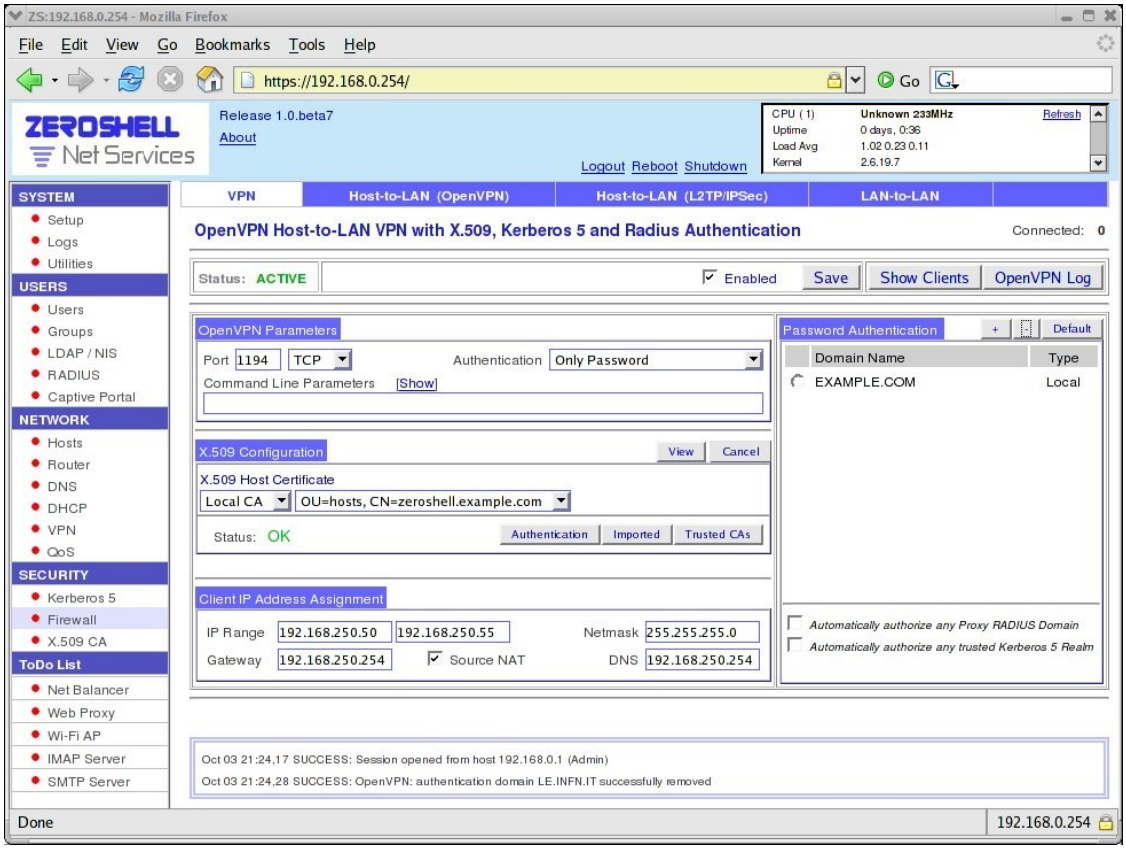
- **Los clientes VPN L2TP/IPSec son de difícil configuración aun en el caso de que el sistema operativo incluya soporte para este tipo de VPN.**

- **Los clientes deben llegar a Internet a través de un router NAT o el servidor VPN debe tener una dirección IP privada, el protocolo IPSec tiene algunos problemas de autenticación por el hecho de que, en la puerta de enlace NAT se modifican las cabeceras IP. La solución a este tipo de problemas consiste tanto en el uso de los routers NAT o el uso de técnicas no estandarizadas de VPN "pass-through" o en el NAT-T (NAT Transversal), que permiten encapsular los paquetes IPSec en el flujo UDP (puerto 4500). El NAT-T es un protocolo estandarizado, pero los clientes VPN necesitan negociar el uso de NAT-T con la VPN sólo cuando realmente hay un dispositivo NAT entre ellos.**

Para evitar los problemas relacionados con el uso de L2TP/IPSec, comenzad con la versión 1.0.beta7 de Zeroshell, en la cual es posible configurar el uso de OpenVPN para actuar como puerta de enlace VPN para las conexiones de la RoadWarrior's. Observe que, Zeroshell ya estaba utilizando OpenVPN para hacer posible la conexión VPN LAN a LAN, ya sea en modo de router o bridge y con la posibilidad de transportar el 802.1Q VLAN a través de Internet. La estabilidad y la flexibilidad demostrada en la VPN LAN-to-LAN ha sido un factor importante para utilizar este software también para el HOST a LAN.

Las ventajas en el uso de OpenVPN en RoadWarrior VPN son:

- **El servicio OpenVPN es muy y fácilmente configurable mediante la interfaz web (ver la imagen);**



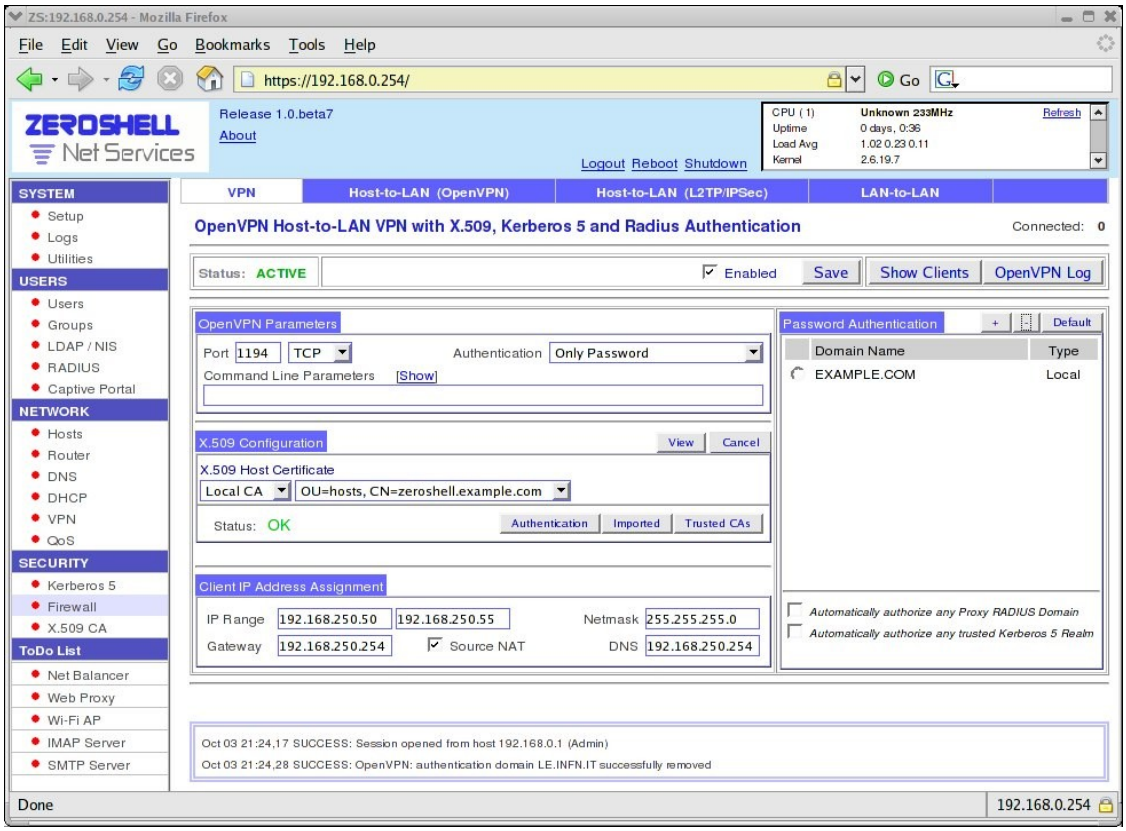
- **Además de la autenticación de cliente X.509 que exige que cualquier usuario tenga un certificado personal y la clave privada relacionada, mediante el uso de OpenVPN es posible autenticarse con nombre de usuario y contraseña, contra un servidor RADIUS externo o en contra de un externo y el local Kerberos 5 KDC (ver la nota al final del documento). Tambien es posible la autenticación de los usuarios de un dominio de Active Directory de Microsoft.**

- **Como puede verse en el documento de configuración del cliente OpenVPN para Windows, Linux, Mac OS X y Windows Mobile para Pocket PC, una interfaz gráfica de usuario OpenVPN es instalable en los sistemas operativos más utilizados. "OpenVPN client configuration for Windows, Linux, Mac OS X and Windows Mobile for Pocket PC,"**

- **Cuando OpenVPN está configurado para utilizar los dispositivos de TAP (software para tarjetas Ethernet), encapsula las tramas Ethernet en el túnel cifrado SSL.**

- **La ventaja en el uso de una VPN Ethernet es que, además de la modalidad router en el que actúa como un router gateway VPN de capa 3, es posible unir las tarjetas Ethernet con la VPN. De esta manera, no sólo el protocolo IP, se pueden enviar a través de la VPN, sino tambien los protocolos de capa 3 como SPX / IPX de NetWare, AppleTalk y NetBEUI. Debido a que en modo bridge, Los datos de ethernet son transmitidos a traves de la VPN, es posible utilizar para los clientes remotos VPN, el mismo servidor DHCP que se utiliza para la continuación de LAN.**

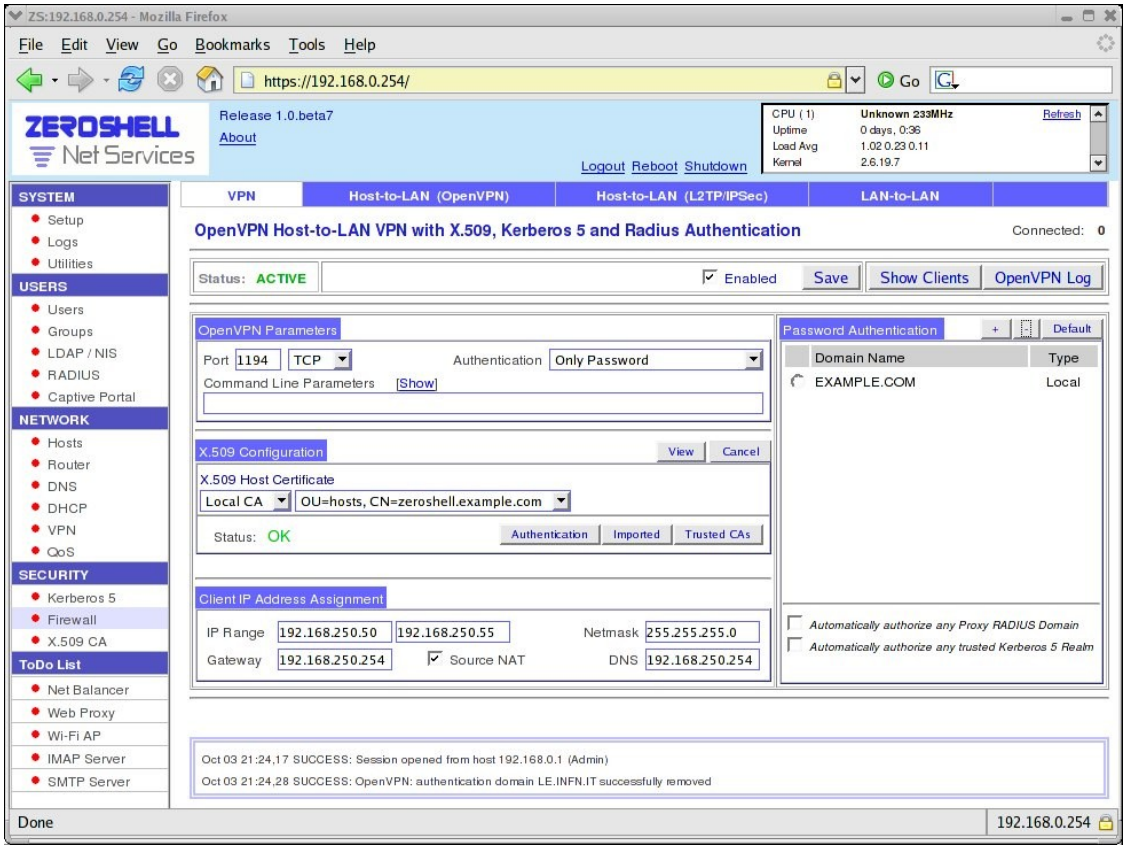
- **En último análisis, el enfoque de OpenVPN parece robusto, porque no sólo utiliza los algoritmos de cifrado más fuertes disponibles en las bibliotecas de OpenSSL, sino también porque los desarrolladores son cuidadosos acerca de la calidad del código. Esto hace de OpenVPN un software seguro y estable mediante la reducción de la presencia de agujeros de seguridad.**



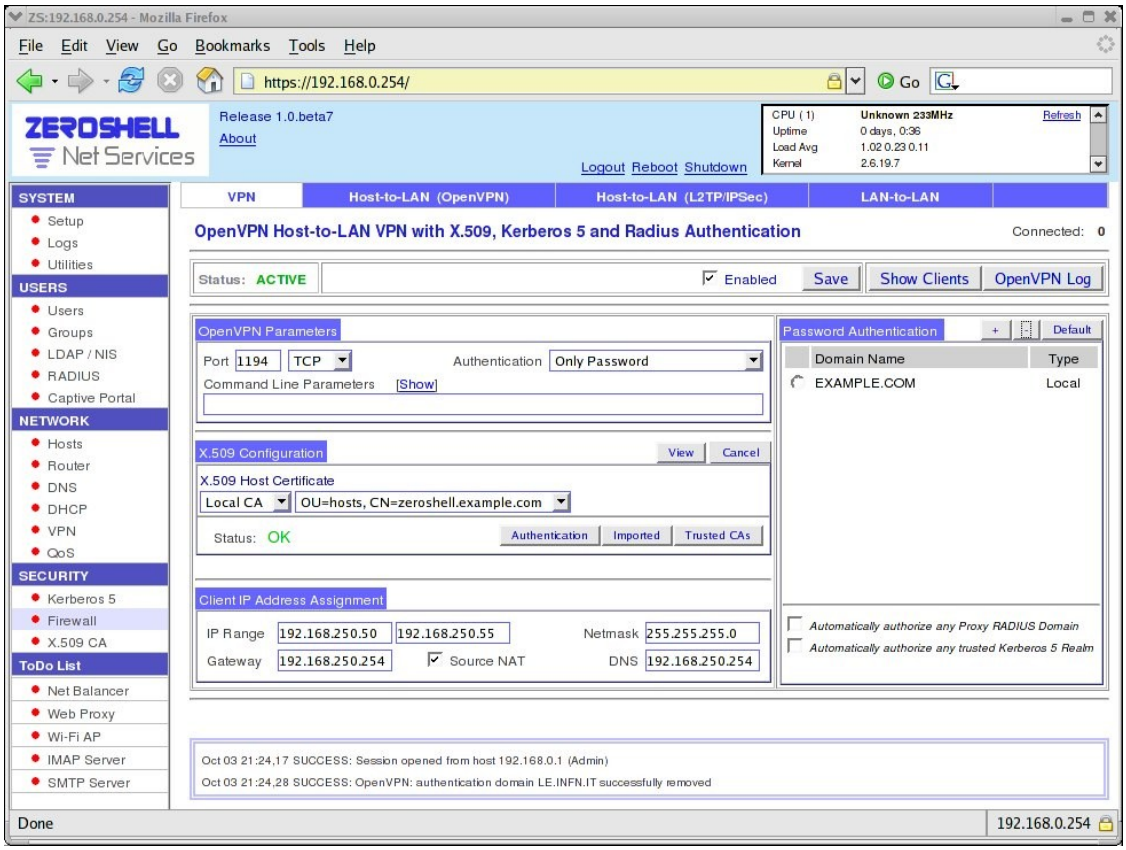
OpenVPN web interface

Configuración VPN por defecto de host a LAN con OpenVPN:

La configuración por defecto hace que sea muy facil empezar a usar la VPN. Para empezar a usar VPN en zeroshell e iniciar el proceso OpenVPN para escuhar las conexiones entrantes haga clic en [VPN] -> [host-a-LAN (OpenVPN)] (ver la imagen).



Para la configuración rápida del cliente, utilice la configuración zeroshell.ovpn, disponible en la sección de descargas. Los parámetros especificados en este fichero reflejan la configuración por defecto de la VPN, y sólo la dirección IP y el nombre de host necesitan ser cambiados para conectarse. Para más información sobre la configuración del cliente de VPN, consulte el siguiente How-To.
Las características de la configuración por defecto, junto con las razones de esta elección, La siguiente imagen de la configuración de OpenVPN puede ser útil como un resumen.



- **OpenVPN le permite seleccionar el protocolo de transporte UDP o TCP en el tunel SSL cifrado. Zeroshell utiliza TCP por defecto, ya que rápidamente se volverá a negociar la conexión VPN si aparecen problemas de conectividad. Por el contrario con UDP, cuando el servicio ha caído, cliente y servidor sólo vuelven a intentar la conexión después de un cierto número de segundos establecido por el parámetro *--ping-restart n.* Un factor determinante en el uso de TCP fue por el hecho que los puertos TCP son a menudo menos bloqueados por los cortafuegos que los UDP.**

- **Además del protocolo, el puerto en el que se aceptan las conexiones de cliente también puede ser seleccionado. De forma predeterminada, Zeroshell utiliza el puerto 1194 ya que este es el oficial asignado por la IANA para OpenVPN.**

- **La autenticación se configura de manera que se autentican sólo los nombres de usuario y contraseñas de los usuarios locales de Zeroshell. Autenticación con certificados digitales X.509 o RADIUS remoto o servidor de Kerberos 5 no es lo suficientemente intuitiva para ser incluido en la configuración por defecto.**

- **Dado que la autenticación del cliente con X.509 está por defecto desactivada, el servidor OpenVPN requiere un certificado con el fin de establecer un canal cifrado con los clientes VPN. Por defecto, este certificado es el que genera automáticamente en el primer arranque de Zeroshell.**

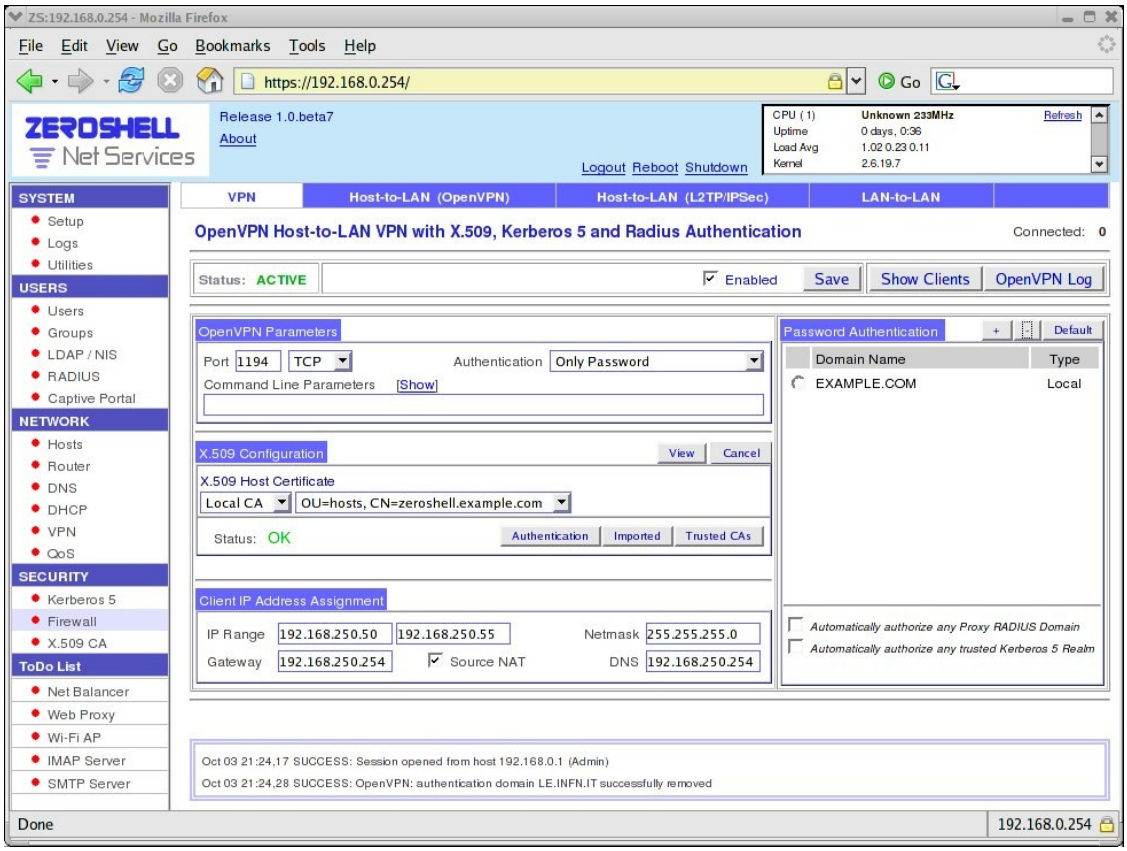
- **De forma predeterminada, se ejecuta Zeroshell OpenVPN en modo de enrutamiento en las direcciones IP de subred 192.168.250.0/255.255.255.0 y la puerta de enlace predeterminada y DNS 192.168.250.254. Además, el NAT está activado por defecto para evitar tener que configurar las rutas estáticas o tener que habilitar el protocolo RIP versión 2 en los routers para llegar a los clientes conectados en VPN.**

- **Por último, se habilita la compresión LZO y el cifrado del tráfico. Sin embargo, estas dos características no pueden ser establecidas en la interfaz web y, por tanto, no se pueden desactivar.**

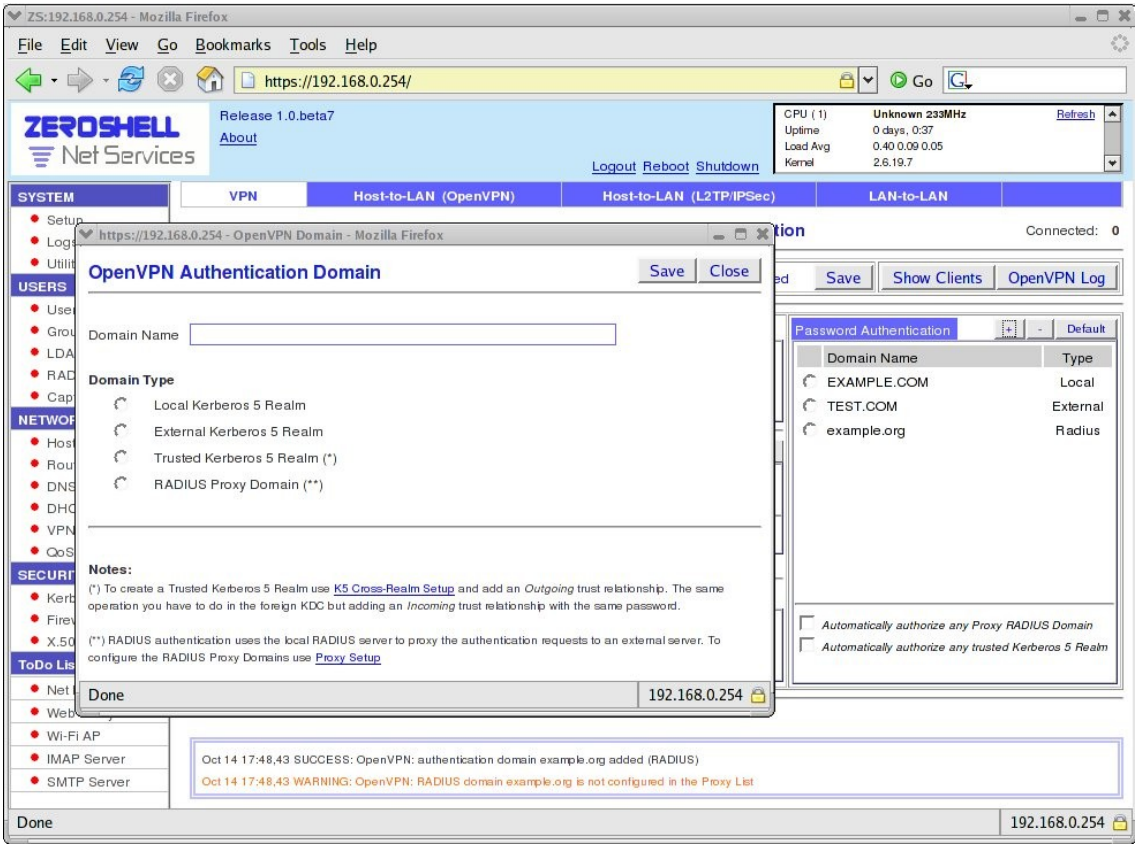
En este punto, después de haber echado un vistazo a la configuración inicial de VPN to LAN, veremos cómo ajustar Zeroshell a nuestras necesidades. Es obvio que el software OpenVPN tiene una configuración muy flexible gracias a sus numerosos ajustes, pero que la interfaz web de Zeroshell sólo permite un número limitado de ellos. En el intento de evitar el problema, la página de configuración incluye un campo de línea de comandos de configuración de parámetros, donde se pueden introducir directamente en el proceso de OpenVPN.

OpenVPN, autenticación con usuario y contraseña

Uso de la selección de autenticación (ver imagen).



El método de autenticación se puede seleccionar usando, nombre de usuario y contraseña única, certificado digital X.509 o ambos. Para la autenticación con nombre de usuario y contraseña, diferentes fuentes se pueden utilizar para verificar las credenciales. Zeroshell selecciona el proveedor de autenticación correcto basado en el dominio indicado en el nombre de usuario, que debe estar en formato de "nombre de usuario@dominio". Si el usuario no indica el dominio, Zeroshell utiliza el dominio predeterminado cuya configuración se describe más adelante y que en principio coinciden con la base de datos de usuarios locales. Las fuentes de autenticación pueden ser "Kerberos 5", "Kerberos realm in cross authentication" con KDC local o RADIUS server externo. La siguiente imagen muestra cómo configurar la autenticación de dominios.



sources de autenticación para OpenVPN

Haga clic en el botón [+] en el boton de autenticación de contraseña para abrir un formulario que se utiliza para configurar el dominio de autenticación.

Dominio Kerberos 5

Escriba el nombre en el campo de Nombre de Dominio y seleccione “External Kerberos 5 Realm” o “Trusted Kerberos 5 Realm”. En el primer caso, las credenciales son verificadas simplemente intentando adquirir un TGT (Ticket Granting Ticket). En el segundo caso, además de la adquisición de TGT, la adquisición de un billete válido de servicio busca la relación de confianza entre el Zeroshell REALM local y el externo. Es evidente que en este segundo caso se ofrece un mayor nivel de seguridad debido a la verificación de la autenticidad del servidor de Kerberos, pero requiere una configuración más compleja ya que la relación de confianza se tiene que establecer entre Zeroshell y el KDC externo.

Recuerde que en esta fase, sólo el nombre de dominio está especificado, pero no la autoridad de los servidores de Kerberos.
La forma en que zeroshell verifica la autenticidad de los usuarios remotos se establece en [Kerberos 5]->[Realms]. Aquí, puede ser añadida la lista de los correspondientes servidores Kerberos o activar la detección automática de DNS que supone el uso de los registros SRV específicos para Kerberos. Si desea permitir que los usuarios del dominio de Microsoft Active Directory puedan ser autenticados en OpenVPN, simplemente recordar que un servidor Kerberos se ejecuta en cada controlador de dominio Windows 2000/2003 capaz de autenticar a los usuarios. Por lo tanto, se limitan a afirmar el dominio de Active Directory como Kerberos 5 externo y añadir el realm la lista de controladores de dominio en [Kerberos 5]->[Realms]. Desde el Directorio Activo DNS se pueden gestionar los registros SRV para Kerberos, el descubrimiento automático puede ser activado en lugar de decir los controladores de dominio.
Por último, en casilla de la autenticación de contraseña, tenga en cuenta que automáticamente se autoriza la confianza en Kerberos 5. Si se habilita, todos los usuarios que tienen una relación cruzada de autenticación pueden ser autenticados en VPN sin tener que agregar cada uno de estos dominios como se describe anteriormente.

RADIUS

Si los usuarios deben ser autenticados por un servidor RADIUS externo, el nombre de dominio debe ser introducido y RADIUS Proxy dominio seleccionado. Desde OpenVPN SE utiliza el mecanismo de proxy para consultar A FreeRADIUS local que ordena a las solicitudes autenticar la autoridad RADIUS. Primero compruebe que se está ejecutando y agrege el servidor RADIUS externo a la lista de servidores proxy que se encuentra en [RADIUS] -> [proxy]. La clave secreta del servidor RADIUS externo se debe especificar en esta lista.
Recuerde que cuando se solicite la autenticación el @dominio del nombre de usuario puede tener que ser eliminado de acuerdo con la configuración del servidor RADIUS externo. En este caso, al añadir el servidor RADIUS en [RADIUS] -> [Proxy], deshabilite el *No Strip* flag.
Si desea delegar a un servidor RADIUS para satisfacer directamente o delegar en otro servidor para cualquier solicitud de autenticación RADIUS que no está bajo los dominios de forma explícita, Añadir un "Default RADIUS" seleccionando "Realm Type box".

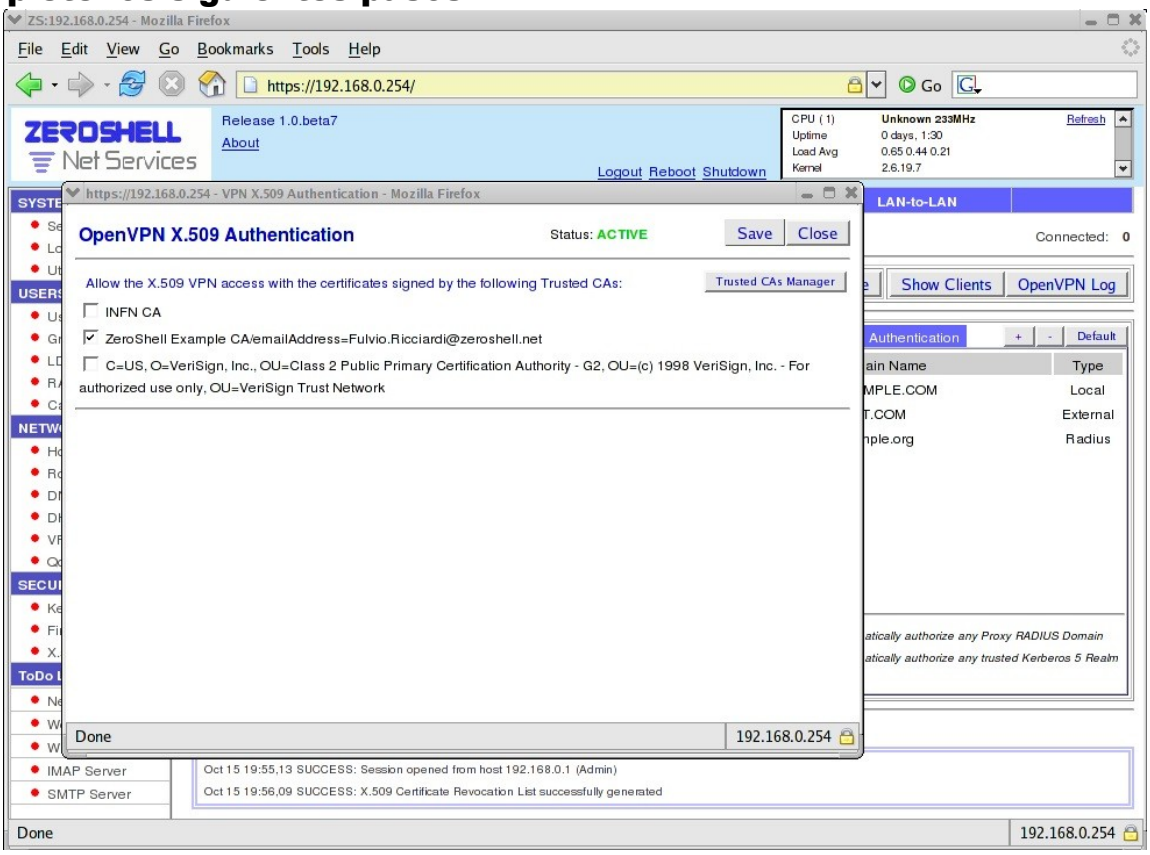
Por último, al igual que con la autenticación Kerberos 5, el frame de autenticación del password incluye una casilla que de estar marcada autoriza a cualquier dominio de Proxy Radius. Cuando se habilita esta casilla, se intenta la autenticación del proxy, incluso si el dominio no está explícitamente autorizado.
Después de haber visto la configuración del lado del servidor para la autenticación con nombre de usuario y contraseña, Cabe señalar que la opción "auth-user-pass" debe estar definida en el archivo de instalación del cliente VPN o en la línea de comandos openvpn a fin de solicitar las credenciales del cliente VPN.

OpenVPN, autenticación con certificados digitales X.509

Autenticación con certificados digitales X.509, cada usuario que quiere conectarse en VPN necesita un certificado digital y la clave privada correspondiente, puede ser solicitada con o sin autenticación con nombre de usuario y contraseña según se trate de certificados X.509 + contraseña o certificado X.509 Sólo está seleccionado en la casilla de verificación de autenticación.
En el primer caso, si la autenticación X.509 es exitosa, una segunda autenticación se ejecuta con Kerberos 5 o RADIUS como se describió anteriormente. En general, cuando se utiliza este tipo de doble autenticación, el certificado digital X.509 no es el usuario, sino un certificado de host asignados a la máquina. Esta identificación de usuario (ya que varios usuarios pueden conectarse desde el mismo sistema) y por lo tanto el nombre de usuario y la contraseña solicitada.
En el segundo caso, los certificados personales asignados al usuario se utilizan cuando el usuario se identifica por el nombre común del certificado (CN field). Esto hace superfluas las solicitudes de credenciales adicionales.
Para obtener un certificado de cliente que seareconocido como válido por la puerta de entrada OpenVPN (ya sea personal asignado al usuario o host asignado a la máquina), se deben cumplir dos condiciones:

1. **la primera es que la Autoridad de Certificación ((CA for short) que firmó el certificado se encuentra en el archivo CAs de confianza en Zeroshell.**
2. **segunda es que esta entidad emisora está autorizada a verificar el acceso de VPN.**

Para cumplir estas dos condiciones, consulte la siguiente imagen y complete los siguientes pasos.



configuración de autenticación con certificados digitales

- **Haga clic en el botón [autenticación] de la configuración X.509. Como puede ver, se cargan los tres certificados de Autoridad de Certificación. Dado que todos los certificados digitales firmados por CA se consideran auténticos, sólo los correspondientes a la Autoridad de Certificación están autorizados para la conexión VPN. En nuestro caso, estos son los certificados expedidos por el ejemplo Zeroshell CA.**

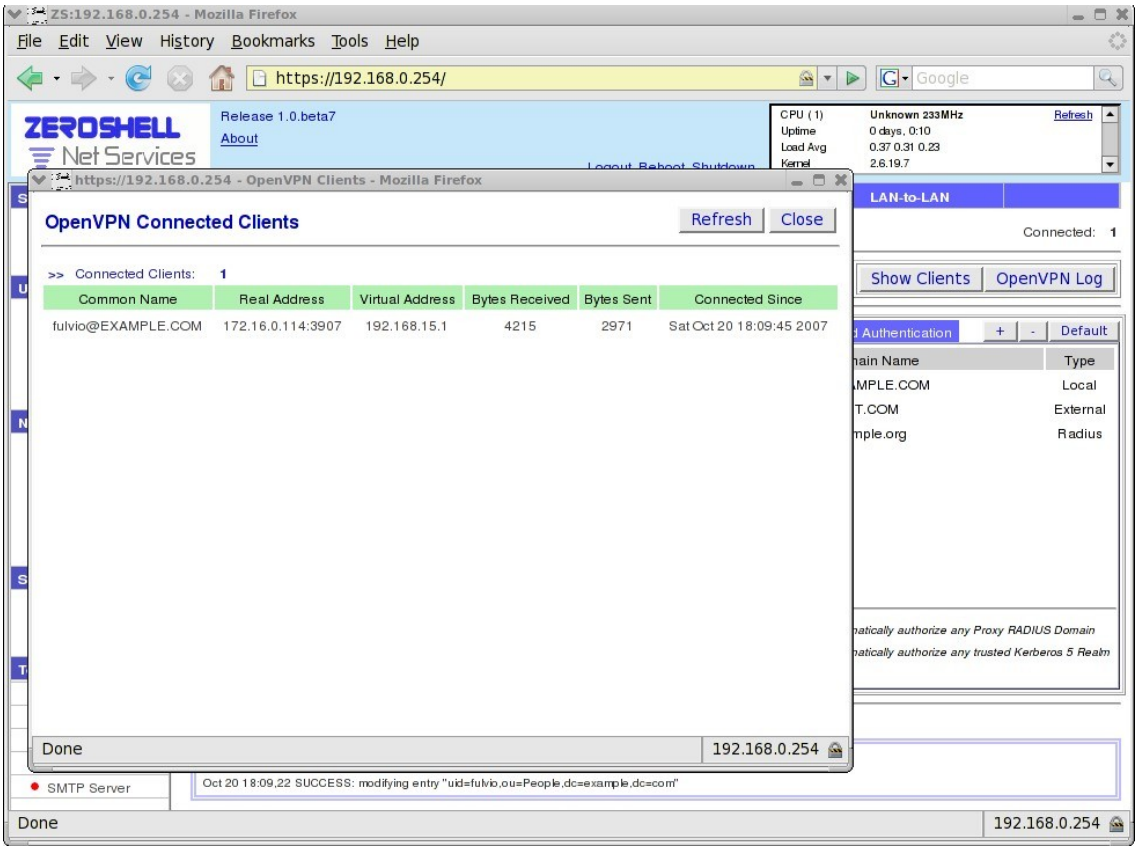
- **Haga clic en [Trusted CAs Manager] e importa (en formato PEM) el certificado de la Autoridad de Certificación que desee autorizar (Base-64 encryption) Si usted tiene una lista de certificados revocados (CRL) para la publicación de certificados revocados, puede cargarlos con el mismo procedimiento de importación CA. Gracias a la CRL,los certificados revocados no tendrán acceso a la puerta de enlace VPN.**

- **Volviendo al formulario “OpenVPN X.509 Authentication” puede verse que los CA recién importados se consideran una fuente fiable de certificación. Para autorizar las conexiones VPN a los clientes que tienen un certificado expedido por esta Autoridad de Certificación, simplemente marque la casilla de control y haga clic en [Save] para guardar.**

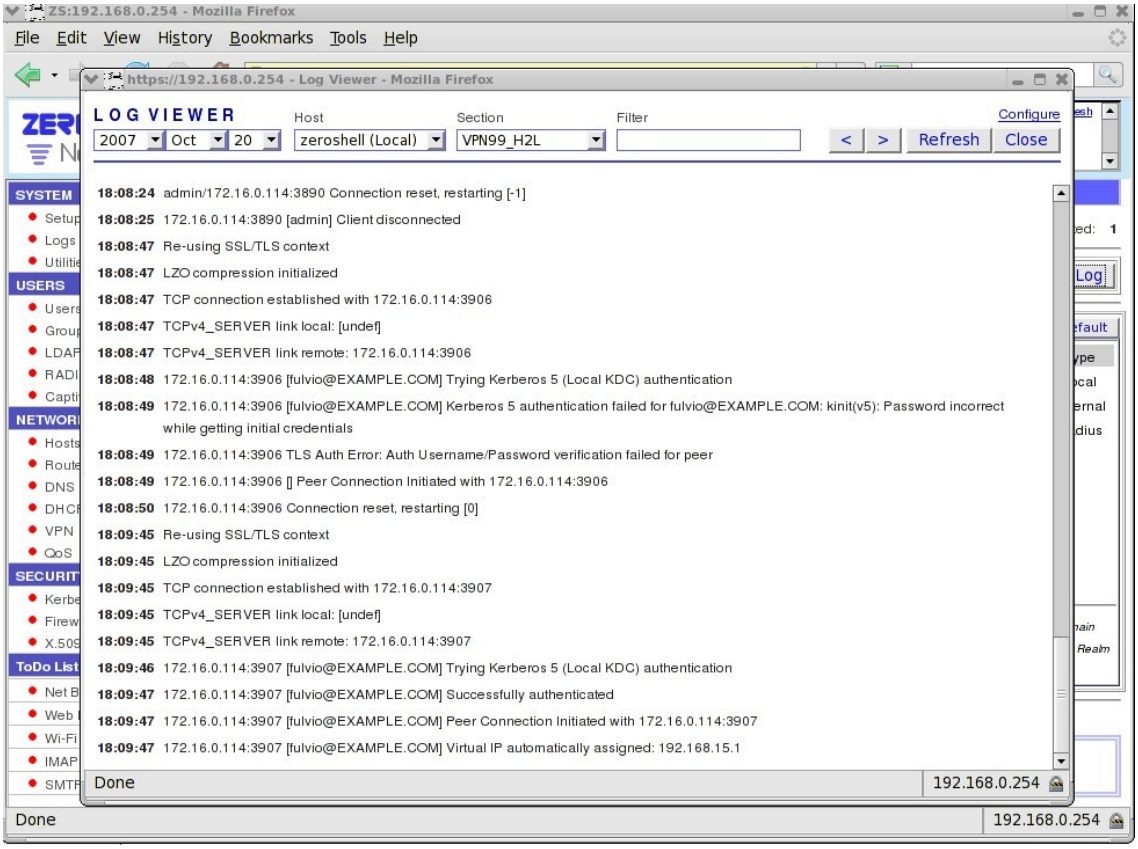
VPN en modo Routed o Bridge

Comenzando con Zeroshell 1.0.beta7, se puede ver que la interfaz de VPN99 virtual se crea automáticamente y se configura durante el inicio. Este es un dispositivo TAP es decir, un software de interfaz Ethernet con el que OpenVPN se conecta con el túnel SSL cifrado y permite la gestión del núcleo como si fuera cualquier otro tipo de tarjeta de red Ethernet. Esto significa que a esta interfaz se le puede asignar una dirección IP y configurarla o hacerla parte de un puente, junto con otras interfaces de Ethernet. En función de si se opta por la primera posibilidad o la segunda (donde VPN99 es un miembro de un puente) Las conexiones VPN serán en modo router o en bridge.
Es evidente que si se selecciona el modo router, la dirección IP asignada a la interfaz de VPN99 debe coincidir con la puerta de enlace predeterminada asignadas a clientes VPN. Esto no debe hacerse manualmente desde Zeroshell la dirección IP a VPN99 se asigna automáticamente cuando el servicio de red privada virtual se configura. Por último, es importante señalar que de la forma que se configura OpenVPN en Zeroshell, los clientes conectados simultáneamente en VPN están aislados unos de otros y por lo tanto no se pueden comunicar a no ser por la puerta de enlace. Esta elección fue forzada por los criterios de seguridad con la que, por ejemplo, queremos evitar que un cliente VPN pueda rastrear el tráfico no dirigido a él. Sin embargo, si usted quiere que los clientes VPN puedan comunicarse unos con otros, simplemente agregar client-to-client en la linea de comandos de la interfaz web. Esta configuración permitirá la visibilidad en la capa 2 por el proceso de OpenVPN y no en el núcleo que permite a los clientes verse unos a otros. Dado que el núcleo no controla esta comunicación, no hay esperanzas de configurar el Firewall (Netfilter) para evitar cualquier tipo de tráfico entre los clientes de la red privada virtual.

Estadísticas de VPN y mensajes de registro



Estadísticas VPN



Mensajes de registro VPN

Notas:

La manera en que los usuarios se autentican dependen de la configuración del servidor OpenVPN. Zeroshell apoya un sistema multi-autenticación de dominio en el que usted tiene que configurar la fuente de autenticación que puede ser un KDC de Kerberos 5 (local, externo y de confianza) o un servidor RADIUS externo.
Uno de estos dominios de autenticación se establece que el dominio predeterminado. Los usuarios del dominio por defecto no necesitan especificar el nombre de usuario en forma usuario@dominio (por ejemplo, fulvio@example.com). Observe que el nombre de dominio no es sensible, porque si el dominio está configurado para ser un realm Kerberos V, se convierte automáticamente a mayúsculas.