Cisco VPN 3000 Concentrator FAQ

Contenido

Introducción

Este documento responde las preguntas más frecuentes (FAQ) sobre el Cisco VPN 3000 Series Concentrator.

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

General

Q. ¿Qué significa el mensaje de error "Lost Service"?

A. Si no se envia tráfico entre el VPN Concentrator y el VPN Client durante un período de tiempo, un paquete de Detección de Peer Inactivo (DPD) será enviado desde el VPN Concentrator al VPN Client para confirmar que su par aún esté allí. Si hay un problema de conectividad entre los dos peers y el Cliente VPN no responde al Concentrador VPN, el Concentrador VPN continúa enviando paquetes DPD durante un período de tiempo. Esto termina el túnel y genera un error si no recibe una respuesta durante ese intervalo de tiempo. Consulte el ID del bug de Cisco CSCdz45586 (clientes registrados solamente).

El error debe ser similar al siguiente:

```
SEV=4 AUTH/28 RPT=381 XXX.XXX.XXX.XX User [SomeUser] disconnected:
Duration: HH:MM:SS Bytes xmt: 19560 Bytes rcv: 17704 Reason:
Lost Service YYYY/MM/DD HH:MM:SS XXX.XXX.XXX.XXX
syslog notice
45549 MM/DD/YYYY HH:MM:SS SEV=4 IKE/123 RPT=XXX.XXX.XXX.XXX
Group [SomeDefault] User [SomeUser]
IKE lost contact with remote peer, deleting connection (keepalive type: DPD)
```

Causa: El peer remoto IKE no respondió a los keepalives dentro del tiempo previsto, por lo que la conexión al peer IKE fue eliminada. El mensaje incluye el mecanismo keep-alive utilizado. Este problema solamente puede reproducirse si la interfaz pública se desconecta durante una sesión de túnel activo. El cliente debe supervisar su conectividad de red ya que estos eventos se generan para identificar la causa raíz del problema de conectividad de la red potencial.

Inhabilite IKE keepalive en **%System Root%\Program Files\Cisco Systems\VPN Client\Profiles** en

la PC del Cliente que tiene el problema, y edite el **archivo PCF** (de ser posible) para la conexión.

Cambie **'ForceKeepAlives=0'** (valor predeterminado) a **'ForceKeepAlives=1'**.

Si el problema persiste, abra una Solicitud de Servicio con el Soporte Técnico de Cisco y proporcione el Cliente “Log Viewer” y los registros del VPN Concentrator cuando se produzca el problema.

Q. ¿Qué significa el mensaje de error "q-send failures detected for EMQ1 queue"?

A. Este mensaje de error aparece cuando hay demasiada información o eventos de debug en el buffer. No tiene ningún impacto negativo excepto la posible pérdida de algunos mensajes de eventos. Intente reducir los eventos al número mínimo necesario para evitar el mensaje.

Q. Mi grupo eliminado todavía puede verse en la configuración del VPN Concentrator. ¿Cómo puedo eliminar esto?

A. **Copie la configuración en el editor de texto (como el Bloc de Notas) y edite o elimine manualmente la información del grupo afectado designada en [ipaddrgrouppool #.0]**. Guarde la configuración y cárguela en el VPN Concentrator. Aquí se muestra un ejemplo.

```
!--- Change to 14.1 or any other number that is not in use !--- any number other than 0).
[ipaddrgrouppool 14.0] rowstatus=1 rangename= startaddr=172.18.124.1 endaddr=172.18.124.2
```

Q. ¿Es posible tener varios servidores primarios SDI?

A. Los VPN 3000 Concentrators pueden descargar solamente un archivo node secret por vez. En las Versiones de SDI previas a la 5.0, se pueden agregar varios servidores SDI, pero deben compartir el mismo archivo node secret (como servidores primarios y de respaldo). En la Versión de SDI 5.0, usted solamente puede ingresar un único servidor SDI primario (los servidores de respaldo se enumeran en el archivo node secret) y las réplicas de los servidores.

Q. Aparece un mensaje de error del Emisor "SSL certificate will expire in 28 days" . ¿Qué debo hacer?

A. El mensaje indica que su certificado de Secure Socket Layer (SSL) vencerá en 28 días. Este certificado se utiliza para navegar en la administración de la red a través del HTTPS. Usted puede mantener las configuraciones predeterminadas del certificado, o puede configurar diversas opciones antes de generar el certificado nuevo. Seleccione **Configuration > System > Management Protocols > SSL** para hacerlo. Seleccione **Administration > Certificate Management** y haga clic en **Generar** para renovar el certificado.

Si le preocupa la seguridad en su concentrador VPN y desea impedir el acceso no autorizado, desactive HTTP y/o HTTPS en la interfaz pública desde Configuration (Configuración) > Policy Management (Administración de políticas) > Traffic Management (Administración del tráfico) > Filtres (Filtros). Si necesita conectarse a su Concentrador VPN en Internet a través de HTTP o HTTPS, puede especificar el acceso basándose en la dirección de origen. Para hacerlo, vaya a Administration (Administración) > Access Rights (Derechos de acceso) > Access Control List (Lista de control de acceso). Para obtener más información, puede usar el menú de ayuda en la esquina superior derecha de la ventana.

Q. ¿Cómo puedo ver la información de usuario en la base de datos de usuario interna? No puede verse desde el archivo de configuración.

A. Seleccione **Administration > Access Rights > Access Settings**, elija **Config File Encryption=None**, y guarde la configuración para ver los usuarios y las contraseñas. Debe poder buscar el usuario específico.

Q. ¿Cuántos usuarios puede almacenar la base de datos interna?

A. El número de usuarios depende de la versión y está especificado en la sección **Configuration > User Management** de la Guía del Usuario para su versión de VPN 3000 Concentrator. Se permiten 100 usuarios o grupos (la suma de usuarios y grupos debe ser igual o menor que 100) en VPN 3000 Releases de 2.2 a 2.5.2. En VPN 3000 Releases 3.0 y posteriores, el número para los Concentradores 3005 y 3015 sigue siendo 100. Para los VPN 3030 y 3020 Concentrators, el número es 500, para los VPN 3060 o 3080 Concentrators, el número es 1000. Además, utilizando un servidor de autenticación externa mejora la escalabilidad y la facilidad de uso.

Q. ¿Cuál es la diferencia entre el gateway predeterminado del túnel y el gateway predeterminado?

A. El concentrador VPN 3000 utiliza el gateway predeterminada del túnel para rutear a los usuarios tunelizados dentro de la red privada (normalmente el router interno). El VPN Concentrator utiliza el gateway predeterminado para rutear paquetes a Internet (generalmente un router externo).

Q. Si coloco mi concentrador VPN 3000 detrás de un firewall o router que ejecute las listas de control de acceso, ¿qué puertos o protocolos necesito permitir que ingresen?

A. Este diagrama enumera los puertos y los protocolos.

Servicio	Número de Protocolo	Puerto de Origen	Puerto de Destino
Conexión de Control de PPTP	6 (TCP)	1023	1723
Encapsulación de Túnel PPTP	47 '(GRE)	N/A	N/A
Administración de Claves ISAKMP/IPSec	17 (UDP)	500	500
Encapsulación de Túnel IPsec	50 (ESP)	N/A	N/A
Transparencia IPSec NAT	17 (UDP)	10000 (default)	10000 (default)

Nota: El puerto de Transparencia de Traducción de Dirección de Red (NAT) se configura con cualquier valor en el rango 4001 a 49151. En las versiones 3.5 o posteriores, se puede configurar el IPSec en TCP a través de **Configuration > System > Tunneling Protocols > IPSec > al IPSec en TCP**. Puede ingresar hasta 10 puertos TCP (1 - 65535) separados por comas. Si esta opción está

configurada, asegúrese de que estos puertos estén habilitados en su firewall o en el router que ejecuta las listas de control de acceso.

Q. ¿Cómo puedo hacer para que el concentrador VPN vuelva a los valores predeterminados de fábrica?

A. Desde la pantalla File Management (Administración de archivos), elimine el archivo "config" y reinicie. Si se borra este archivo por accidente, se conserva una copia de respaldo "config.bak".

Q. ¿Puedo utilizar TACACS+ para la autenticación Administrativa? ¿Qué debo tener en cuenta mientras lo hago?

A. Sí, a partir de Concentrador VPN 3000 Versión 3.0, puede usar un TACACS+ para la Autenticación administrativa. Después de configurar el TACACS+, asegúrese de probar la autenticación antes de cerrar la sesión. La configuración inadecuada del TACACS+ puede prohibirle el acceso. Esto requiere un inicio de sesión del puerto de la consola para invalidar el TACACS+ y solucionar el problema.

Q. ¿Qué debo hacer cuándo se olvida la contraseña administrativa?

A. En las versiones 2.5.1 y posteriores, conecte una PC con el puerto de la consola del VPN Concentrator usando un cable serial de conexión directa RS-232 y la PC configurada para:

- 9600 bits por segundo
- 8 bits de datos
- sin paridad
- 1 bit de parada
- control de flujo de hardware activado
- Emulación de VT100

Reinicie el VPN Concentrator. Después de completar la verificación de diagnóstico, una línea de tres puntos (...) aparece en la consola. Presione **CTRL-C** dentro de los tres segundos posteriores a la aparición de los puntos. Aparece un menú que le permite reajustar las contraseñas del sistema a sus valores predeterminados.

Q. ¿Cuál es el propósito del nombre de grupo y de la contraseña de grupo?

A. El nombre y la contraseña de grupo se usan para crear un hash que luego es empleado para generar una asociación de seguridad.

Q. ¿El VPN Concentrator representa el ARP en nombre de los usuarios tunelizados?

A. Sí.

Q. ¿Dónde coloco el concentrador VPN 3000 en relación con mi escudo de protección de red?

A. El Concentrador VPN 3000 puede colocarse en la zona desmilitarizada (DMZ) de un firewall,

enfrente o detrás de ella o en forma paralela a la misma. No se recomienda tener interfaces públicas y privadas en la misma LAN virtual (VLAN).

Q. ¿Hay manera de inhabilitar el proxy ARP en el Cisco VPN 3000 Concentrator?

A. **El** Proxy Address Resolution Protocol (ARP) no puede inhabilitarse en el Cisco VPN 3000 Concentrator.

Q. ¿Dónde puedo encontrar errores de programación informados para el Concentrador VPN 3000?

A. **Los** usuarios pueden utilizar el Bug Toolkit (clientes registrados solamente) para encontrar la información detallada sobre los bugs.

Q. ¿Dónde puedo encontrar ejemplos de configuración para el concentrador VPN 3000?

A. Además de la sección de documentación del VPN 3000 Concentrator, usted puede encontrar más ejemplos de configuración en la Página de Soporte de Cisco VPN 3000 Series Concentrator.

Q. ¿Cómo puedo aumentar el registro para mejorar los depuradores para eventos específicos?

A. Puede ir a **Configuration > System > Events > Classes** y configurar los eventos específicos (como IPsec o PPTP) para obtener mejores debugs. El debugging se debe activar solamente durante el troubleshooting porque puede causar la degradación del rendimiento. Para el debug de IPSec, active IKE, el IKEDBG, IPSEC, IPSECDBG, AUTH, y AUTHDBG. Si usa certificados, agregue la clase CERT a la lista.

Q. ¿Cómo puedo monitorear el tráfico hacia el VPN 3000 Concentrator?

A. La interfaz de HTML que viene con el VPN 3000 Concentrator le permite tener una funcionalidad básica de monitoreo si busca en **Monitoring > Sessions**. El VPN 3000 Concentrator también se puede monitorear con el Simple Network Management Protocol (SNMP) usando un administrador SNMP de su elección. Como opción alternativa, puede adquirir la solución Cisco VPN/ Security Management Solution (VMS). La solución Cisco VMS proporciona las funciones claves para implementar el VPN 3000 Concentrator Series y requiere un monitoreo detallado del acceso remoto y de las VPN de sitio a sitio, en función de los IPSec, L2TP, y PPTP. Consulte VPN Security Management Solution para obtener más información sobre VMS.

Q. ¿Cisco VPN 3000 Concentrator Series tiene un firewall integrado? ? Si es así, ¿qué características se admiten?

A. Mientras que la serie tienen un puerto integrado sin estado/ capacidades de filtración y NAT, Cisco sugiere que utilice un dispositivo como el Cisco Secure PIX Firewall para el firewall corporativo.

Q. ¿Qué opciones y protocolos VPN son soportados por el Cisco VPN 3000 Concentrator Series?

A. La serie soporta estas opciones de routing:

- Routing Information Protocol (RIP)
- RIP2
- Open Shortest Path First (OSPF)
- rutas estáticas
- Virtual Router Redundancy Protocol (VRRP)

Los protocolos VPN soportados incluyen el Point-to-Point Tunneling Protocol (PPTP), L2TP, L2TP/ IPSec, y el IPSec con o sin un dispositivo NAT entre el VPN3000 y el cliente final. IPSec a través de NAT se conoce como Transparencia NAT.

Q. ¿Qué mecanismos o sistemas de autenticación admite el Cisco VPN 3000 Concentrator Series para la PC del cliente?

A. Dominio NT, RADIUS o RADIUS proxy, RSA Security SecurID (SDI), Certificados Digitales, y autenticación interna son soportados.

Q. ¿Puedo hacer Traducción de Dirección de Red Estática (NAT) para los usuarios que salen a través del VPN 3000 Concentrator?

A. Sólo puede realizar traducción de dirección de puerto (PAT) para los usuarios que salen. No puede hacer una NAT estática en el VPN 3000 Concentrator.

Q. ¿Cómo puedo asignar una dirección IP estática a un Point-to-Point Tunneling Protocol (PPTP) específico o al usuario IPsec a través del VPN 3000 Concentrator?

A. Esta lista explica cómo asignar las direcciones IP estáticas:

- **Usuarios PPTP**En la sección de Administración de Direcciones IP, además de elegir su pool u opciones de Dynamic Host Configuration Protocol (DHCP), verifique la opción **Use Client Address**. Luego, defina el usuario y la dirección IP en el concentrador VPN 3000. Este usuario siempre obtiene la dirección IP configurada en el VPN Concentrator al conectarse.
- **Usuarios IPsec**En la sección Administración de Direcciones IP, además de elegir su pool o las opciones DHCP, verifique la opción **Use Address from Authentication Server**. Luego, defina el usuario y la dirección IP en el concentrador VPN 3000. Este usuario siempre obtiene la dirección IP configurada en el VPN Concentrator al conectarse. Todos los otros que pertenecen al mismo grupo o a otros grupos obtienen una Dirección IP del pool global o de DHCP.Con el software Cisco VPN 3000 Concentrator versión 3.0 o superior, tiene la opción de configurar un conjunto de direcciones por grupo. Esta característica puede ayudarlo a asignar una dirección de IP estática a un usuario determinado. Si configura un pool para un grupo, el usuario con IP estática obtiene la dirección IP asignada, y otros miembros del mismo grupo obtienen las direcciones IP del pool del grupo Esto se aplica solamente cuando utiliza el VPN Concentrator como servidor de autenticación.

Nota: Si utiliza un servidor de autenticación externo, necesita utilizar el servidor externo para asignar las direcciones correctamente.

Q. ¿Cuáles son los problemas de compatibilidad ya conocidos de los productos PPTP de Microsoft y del concentrador VPN 3000?

A. Esta información está basada en el VPN 3000 Series Concentrator del Software Release 3.5 y posteriores; VPN 3000 Series Concentrators, modelos 3005, 3015, 3020, 3030, 3060, 3080; y sistemas operativos Microsoft Windows 95 y posteriores.

- **Windows 95 Dial-Up Networking (DUN) 1.2**Microsoft Point-to-Point Encryption (MPPE) no es soportado por DUN 1.2. Para conectarse utilizando MPPE, instale el Acceso telefónico a redes 1.3 de Windows 95. Puede descargar la actualización DUN 1.3 de Microsoft del sitio Web de Microsoft.
- **Windows NT 4.0**El Windows NT es soportado completamente para las conexiones de Point-to-Point Tunneling Protocol (PPTP) al VPN Concentrator. Se requiere Service Pack 3 (SP3) o superior. Si ejecuta SP3, debe instalar los parches de Rendimiento y Seguridad de PPTP. Consulte el sitio Web de Microsoft para obtener información sobre el Rendimiento PPTP de Microsoft y la Actualización Seguridad para WinNT 4.0 .Observe que el Service Pack 5 de 128 bits no maneja las claves MPPE correctamente, y el PPTP quizá no transfiera los datos. Cuando ocurre esto, el registro de eventos muestra este mensaje:`103 12/09/1999 09:08:01.550 SEV=6 PPP/4 RPT=3 80.50.0.4 User [ testuser ] disconnected. Experiencing excessive packet decrypt failure.`Para solucionar este problema, descargue la actualización para que cómo obtenga el último Windows NT Service Pack 6a y el Service Pack 6a del Windows NT 4.0 disponible. Consulte el artículo de Microsoft Claves de MPPE que no se manejaron correctamente para una Solicitud MS-CHAP de 128 bits para obtener más información.

Q. ¿Cuál es la cantidad máxima de filtros permitidos en un concentrador VPN 3000?

A. La cantidad máxima de filtros que puede agregar en una unidad VPN 30xx (incluso 3030 o 3060) está establecida en 100. Los usuarios pueden encontrar información adicional sobre este problema en Cisco bug ID CSCdw86558 (sólo clientes registrados) .

Q. ¿Cuál es el número máximo de rutas en la línea 30xx de los concentradores VPN?

A. El número máximo de rutas es:

- El VPN 3005 Concentrator antes contaba con un máximo de 200 rutas. Este número ahora ha aumentado a 350 rutas. Consulte Cisco bug ID CSCeb35779 (sólo clientes registrados) para obtener más información.
- Se probó el Concentrador VPN 3030 hasta con 10.000 rutas.
- El límite de la tabla de ruteo en los Concentradores VPN 3030, 3060 y 3080 es proporcional a los recursos / memoria disponibles en cada dispositivo.
- El VPN 3015 Concentrator no tiene un límite máximo predefinido. Esto es válido para los Routing Information Protocol (RIP) y Open Shortest Path First (OSPF).
- El VPN 3020 Concentrator - Debido a una restricción de Microsoft, Windows XP PC no puede recibir una gran cantidad de Rutas Estáticas sin Clase (CSR). El VPN 3000 Concentrator limita el número de CSR que se insertan en un mensaje de respuesta DHCP INFORM cuando están configurado para ello. El VPN 3000 Concentrator limita el número de rutas a 28-42, según la clase.

Q. ¿Cómo borro totalmente las estadísticas de la interfaz en el VPN 3000 Concentrator?

A. Seleccione **Monitoring > Statistics > MIB-II > Ethernet** y reajuste las estadísticas para borrarlas para la sesión actual. Recuerde que esto no borra totalmente las estadísticas. Debe reiniciar para reajustar realmente las estadísticas (versus reajuste para monitorear).

Q. ¿Qué puertos debo permitir en el VPN Concentrator para la comunicación del Network Time Protocol (NTP)?

A. Permita el puerto 123 TCP y UDP.

Q. ¿Cuáles son las funciones de los puertos UDP 625xx?

A. Los puertos se utilizan para la comunicación de VPN Client entre el compensador real/el Deterministic NDIS Extender (DNE) y la pila de TCP/IP de la PC, y sólo se permiten para uso de desarrollo interno Por ejemplo, el puerto 62515 es utilizado por VPN Client para enviar la información al registro VPN Client. Otras funciones del puerto se muestran aquí.

- 62514 - Servicio del Cisco Systems, Inc. VPN al driver de IPSec de Cisco Systems
- 62515 - Driver de IPSec de Cisco Systems al servicio del Cisco Systems, Inc. VPN
- 62516 - Servicio VPN de Cisco Systems Inc. a XAUTH
- 62517 - Servicio VPN de XAUTH a Cisco Systems Inc.
- 62518 - Servicio VPN de Cisco Systems, Inc. a CLI
- 62519 - CLI to Cisco Systems, Inc VPN Service
- 62520 - Cisco Systems, Inc. Servicio VPN a UI
- 62521 - UI a Cisco Systems, Inc. VPN Service
- 62522: Mensajes del registro
- 62523 - Connection Manager to Cisco Systems, Inc. VPN Service
- 62524 - Servicio VPN de PPPTool a Cisco Systems Inc.

Q. ¿Puedo quitar la barra flotante WebVPN?

A. No puede quitar la barra de herramienta flotante ni cargar la barra de herramientas flotante mientras que establece la sesión WebVPN. Esto es porque cuando cierras esta ventana la sesión finaliza inmediatamente y cuando intenta acceder otra vez la ventana se carga otra vez. Ésta es la manera en que diseñaron las sesiones WebVPN originalmente. Usted puede cerrar la ventana principal pero no es posible cerrar la ventana flotante.

Software

Q. P.¿WebVPN soporta Outlook Web Access (OWA) 2003?

A. El soporte OWA 2003 para WebVPN en el VPN 3000 Concentrator ahora está disponible con las descargas de la versión 4.1.7 (clientes registrados solamente) .

Q. ¿Dónde puedo conseguir las revisiones de software más recientes para el Concentrador VPN 3000?

A. Todos los Cisco VPN 3000 Concentrators se envían con el código más actual, pero los usuarios pueden controlar las descargas (clientes registrados solamente) para verificar la disponibilidad de software más actualizado.

Consulte documentación sobre el Cisco VPN 3000 Series Concentrator para la última documentación sobre el VPN 3000 Concentrator.

Q. ¿Necesito un servidor TFTP para actualizar el VPN 3000 Concentrator? ¿Hay una manera alternativa de actualizar el cuadro?

A. Además de usar el TFTP, puede actualizar el VPN Concentrator descargando el último software en su disco duro. Entonces, desde un buscador en el sistema donde se localiza el software, diríjase a **Administration > Software Update** y busque el software descargado en su unidad de disco duro (apenas como la apertura de un archivo). Cuando lo encuentre, seleccione la pestaña Upload.

Q. ¿Qué significa el "k9" en el últimos nombres de códigos (tales como en "vpn3000-3.0.4 Rel-k9.bin")?

A. La designación “k9” para el nombre de la imagen ha reemplazado la designación 3DES originalmente utilizada (por ejemplo, vpn3000-2.5.2.F-3des.bin). Por lo tanto, "k9" ahora significa que esto es una imagen 3DES.

Q. ¿Debo utilizar la opción de la Compresión de datos bajo grupo IPSec para todos mis usuarios?

A. La compresión de datos aumenta el requisito de memoria y la utilización de la CPU para cada sesión de usuario y, por lo tanto, disminuye el rendimiento general del VPN Concentrator. Por esta razón, Cisco recomienda que habilite la compresión de datos solamente si todos los miembros del grupo son usuarios remotos que se conectan con un módem. Si cualquier miembro del grupo se conecta a través de la banda ancha, no habilite la compresión de datos para el grupo. En cambio, divide al grupo en dos, uno para los usuarios de módem y el otro para los usuarios de banda ancha. Active la compresión de datos sólo en el grupo de usuarios de módem.

Otras Características Avanzadas

Q. ¿El balanceo de carga funciona con las conexiones LAN a LAN?

A. El balanceo de carga es efectivo sólo en sesiones remotas iniciadas con Cisco VPN Software Client (Release 3.0 y posteriores). El resto de los clientes (PPTP, L2TP) y las conexiones de LAN a LAN pueden conectarse con un VPN Concentrator en el cual se habilita el balanceo de carga, pero no pueden participar en el equilibrio de cargas.

Q. ¿Cómo descifrar las contraseñas del archivo de configuración?

A. Diríjase a **Configuration > System > Management Protocols > XML** y luego a **administración | administración de archivo seleccione formato XML** . Utiliza el mismo nombre, o uno diferente, y abra el archivo para ver las contraseñas.

Q. ¿Puedo usar al mismo tiempo el Protocolo de redundancia del router virtual (VRRP) y el balance de carga?

A. No puede usar equilibrio de cargas con VRRP. En una configuración VRRP, el dispositivo de respaldo sigue inactivo a menos que el VPN Concentrator activo falle. En la configuración de equilibrio de carga, no hay dispositivos ociosos.

Q. ¿Todo el tráfico del cliente VPN de acceso remoto tiene que pasar a través de un túnel cifrado al VPN Concentrator en la empresa o el proveedor de servicio? ? Por ejemplo, ¿es posible que el acceso web salga a otros sitios directamente a través de la conexión de Internet ISP?

A. Sí. Este concepto se conoce como “tunelización dividida.” La tunelización dividida permite el acceso seguro a los recursos corporativos a través de un túnel cifrado mientras que permite el acceso a Internet directamente a través de los recursos ISP (éste elimina la red corporativa de la trayectoria para acceso web). El concentrador VPN serie 3000 de Cisco admite una tunelización dividida hacia el VPN Cliente de Cisco y el cliente de hardware VPN 3002 Para la seguridad complementaria, esta característica es controlable por el administrador del VPN Concentrator y no del usuario.

Q. ¿Es seguro utilizar tunelización dividida?

A. La tunelización dividida permite que tenga la conveniencia de buscar en Internet mientras que está conectada a través del túnel VPN. Sin embargo, nos presenta un cierto riesgo si el usuario de VPN conectado con la red corporativa es vulnerable a los ataques. Se recomienda que los usuarios utilicen un firewall personal en este caso. Las notas de versión para cualquier versión dada del cliente de VPN describen la interoperabilidad con los firewalls personales.

Q. ¿Cómo funciona el balanceo de carga en el Concentrator Cisco VPN 3000?

A. La carga se calcula como un porcentaje derivado de las conexiones activas divididas por las conexiones configuradas máximas. El master siempre intenta tener la menor carga posible porque soporta la carga adicional (inherente) de mantener a todas las sesiones de LAN a LAN administrativas, calculando el resto de la carga de miembro de agrupamiento, y es responsable de todas las redirecciones del cliente:

Para un agrupamiento funcional recién configurado, el master tiene aproximadamente 1 por ciento antes de que se haya establecido cualquier conexión. Por lo tanto, el master redirecciona las conexiones al concentrador de respaldo hasta que el porcentaje de carga en el respaldo sea más alto que el porcentaje de carga del master. Por ejemplo, dado que dos Concentradores de VPN 3030 en los estados “inactivos”, el master tiene 1 por ciento de carga. El secundario recibe 30 conexiones (carga del 2 por ciento) antes de que el master valide las conexiones.

Para verificar que el master valide las conexiones, diríjase a **Configuration > System > General> Sessions** y disminuye la cantidad máxima de conexiones a un número artificialmente bajo para aumentar rápidamente la carga puesta en el VPN Concentrator de respaldo.

Q. ¿Cuántos dispositivos de cabecera puede rastrear el Monitor de VPN?

A. El monitor VPN puede rastrear 20 dispositivos de cabecera. En un escenario radial, las

conexiones de los sitios remotos se monitorean en la cabecera. No hay necesidad de monitorear todos los sitios remotos y usuarios puesto que esa información se puede localizar en el router del hub. Estos dispositivos de cabecera pueden soportar hasta 20,000 usuarios remotos o 2,500 sitios remotos. Un dispositivo VPN de doble reposición que se sale de los sitios radiales se considera dos de los 20 dispositivos máximos que pueden ser monitoreados.

Información Relacionada

- Página de Soporte del Cisco VPN 3000 Concentrator
- Página de soporte del VPN 3000 Client de Cisco
- Soporte Técnico y Documentación - Cisco Systems