Ejemplo virtual clásico y Zona-basado del Firewall Cisco IOS del Firewall de la configuración de aplicación

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Antecedentes
Soporte de característica
Configuración de VRF
Descripción de las aplicaciones del campo común para el escudo de protección IOS que reconoce VRF
Configuración no admitida
Configurar
Firewall que reconoce VRF de la obra clásica del Cisco IOS
El Cisco IOS que reconoce VRF Zona-basó el escudo de protección IOS de la directiva
Conclusión
Verificación
Troubleshooting
Información Relacionada

Introducción

Este documento describe el trasfondo técnico de las características de firewall virtual que reconoce VRF, el procedimiento de configuración y casos de uso para diversos escenarios de aplicación.

La versión 12.3(14)T del Cisco IOS ® Software introdujo el Firewall (que reconoce VRF) virtual, extendiendo la familia virtual de la característica de la Encaminamiento-expedición (VRF) para ofrecer la inspección de paquetes stateful, el Firewall transparente, la Inspección de la aplicación, y el Filtrado de URL, además del VPN existente, del NAT, de QoS, y de otras características que reconoce VRF. La mayoría de los escenarios previsibles de la aplicación aplicarán el NAT con las otras funciones. Si el NAT no se requiere, el rutear puede ser aplicado entre los VRF proporcionar la Conectividad inter-VRF. Las capacidades que reconoce VRF de las ofertas del Cisco IOS Software en el Firewall del Cisco IOS y el Cisco IOS clásicos Zona-basaron el Firewall de la directiva, con los ejemplos de ambos modelos de la configuración proporcionados en este documento. Un mayor foco se pone en la configuración de escudo de protección de la directiva Zona-Basar.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

Convenciones

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

Antecedentes

Soporte de característica

El Firewall que reconoce VRF está disponible en la Seguridad avanzada, los Servicios IP avanzados, y las imágenes Enterprise avanzadas, así como las imágenes de la herencia-nomenclatura que llevan la designación *o3*, que indica la integración del conjunto de funciones del Cisco IOS Firewall. Capacidad que reconoce VRF del Firewall combinada en las versiones de la línea principales del Cisco IOS Software en 12.4. El Cisco IOS Software Release 12.4(6)T o Posterior se requiere para aplicar el Firewall Zona-basado que reconoce VRF de la directiva. El Firewall Zona-basado Cisco IOS de la directiva no trabaja con la falla de estado.

Configuración de VRF

El Cisco IOS Software mantiene las configuraciones para el VRF global y todo el soldado VRF en el archivo de misma configuración. Si la configuración del router se accede a través de la interfaz de la línea de comandos, el control de acceso papel-basado ofrecido en la característica de las opiniones CLI se puede utilizar para limitar la capacidad del router operativa y del personal a cargo de la administración. Las aplicaciones de administración tales como Cisco Security Manager (CS) también proporcionan el control de acceso papel-basado para asegurar que restringen a los personales operativos al nivel adecuado de capacidad.

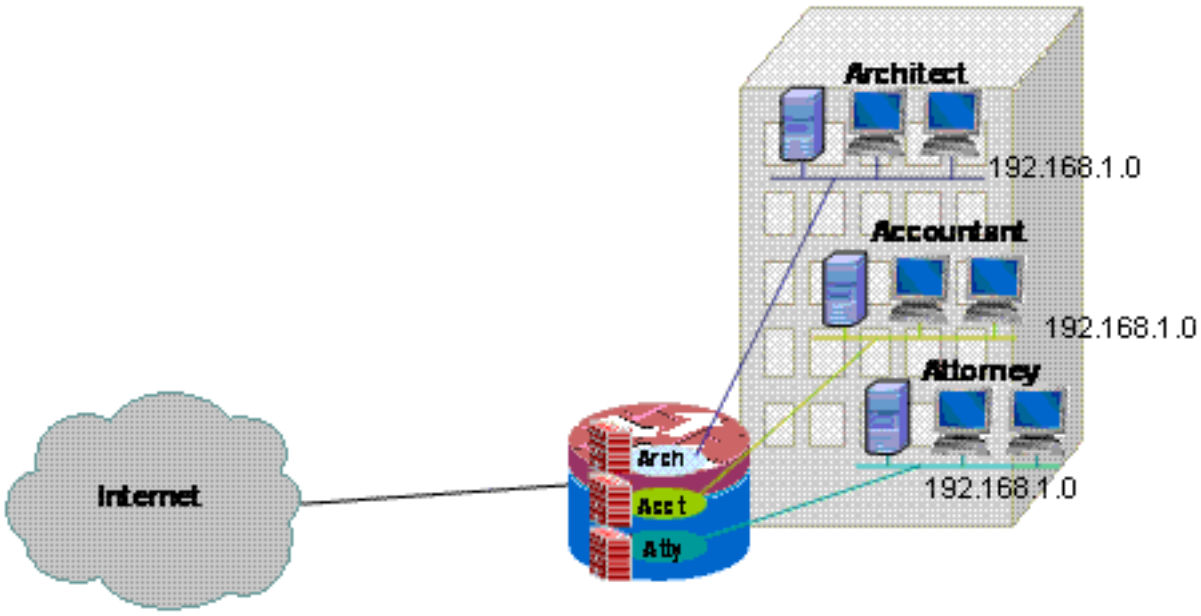
Descripción de las aplicaciones del campo común para el escudo de protección IOS que reconoce VRF

El Firewall que reconoce VRF agrega la inspección de paquetes stateful a la capacidad del ruteo virtual/de la expedición del Cisco IOS (VRF). La traducción de la dirección del /port del IPSec VPN, del Network Address Translation (NAT) (PALMADITA), el Sistema de prevención de intrusiones (IPS) y otros servicios de Seguridad de Cisco IOS se pueden combinar con el Firewall que reconoce VRF para proporcionar a un conjunto completo de Servicios de seguridad en los VRF. Los VRF proporcionan el soporte para los espacios múltiples de la ruta que emplean la

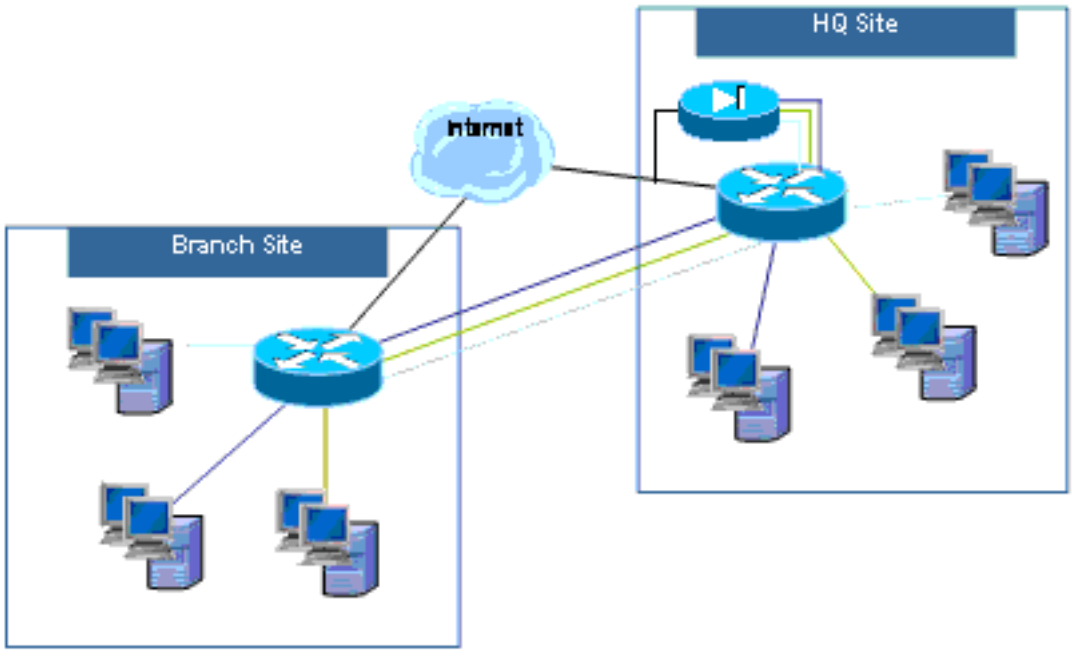
enumeración de la dirección IP que solapa, así que un router puede ser dividido en los casos discretos múltiples de la encaminamiento para la separación del tráfico. El Firewall que reconoce VRF incluye una escritura de la etiqueta VRF en la información de la sesión para toda la actividad del examen que el router esté siguiendo, para mantener la separación entre la información de estado de la conexión que puede ser idéntica en cada otro respecto. El Firewall que reconoce VRF puede examinar examina entre las interfaces dentro de un VRF, así como entre las interfaces en los VRF que diferencian, por ejemplo en caso de que el tráfico cruza los límites VRF, para observar la flexibilidad máxima del examen del Firewall para el tráfico intra-VRF e inter-VRF.

Las aplicaciones que reconoce VRF del Firewall Cisco IOS se pueden agrupar en dos categorías básicas:

- Multi-arrendatario, solo-sitio — Acceso a internet para los arrendatarios múltiples con los espacios de dirección superpuesta o los espacios segregados de la ruta en una sola premisa. El escudo de protección con estado se aplica a la conectividad a Internet cada VRF para reducir más lejos la probabilidad del compromiso a través de las conexiones NAT abiertas. la Puerto-expedición se puede aplicar para permitir la Conectividad a los servidores en los VRF.



Un ejemplo de una aplicación del solo-sitio del multi-arrendatario para el modelo clásico que reconoce VRF de la configuración de escudo de protección y el modelo Zona-basado que reconoce VRF de la configuración de escudo de protección se proporciona en este documento.
- Multi-arrendatario, multi-sitio — Arrendatarios múltiples que comparten el equipo en una Conectividad de la necesidad de la Red grande entre los sitios múltiples por la conexión de los VRF de los arrendatarios en diversos sitios con el VPN o las conexiones WAN. El acceso a internet se puede requerir para cada arrendatario en uno o más sitios. Para simplificar la Administración, varios departamentos pueden derrumbarse sus redes en un router de acceso para cada sitio, pero los diversos departamentos requieren la segregación del espacio de la



dirección. Los ejemplos de configuración para las aplicaciones del multi-sitio del multi-arrendatario para el modelo clásico que reconoce VRF de la configuración de escudo de protección y el modelo Zona-basado que reconoce VRF de la configuración de escudo de protección serán proporcionados en una actualización próxima a este documento.

Configuración no admitida

El Firewall que reconoce VRF está disponible en las imágenes del Cisco IOS que soportan Multi-VRF CE (VRF Lite) y MPLS VPN. La capacidad del Firewall se limita a las interfaces NON-MPLS. Es decir, si una interfaz participa en el tráfico MPLS-etiquetado, el examen del Firewall no se puede aplicar en esa interfaz.

Un router puede examinar solamente el tráfico inter-VRF si el tráfico debe ingresar o dejar un VRF a través de una interfaz para cruzar a un diverso VRF. Si el tráfico se rutea directamente a otro VRF, no hay interfaz física donde las políticas del firewall pueden examinar el tráfico, así que el router no puede aplicar el examen.

La configuración VRF Lite es interoperable con el NAT/PAT solamente si el `interior nacional del IP` o el `exterior nacional del IP` se configura en las interfaces donde el NAT/PAT se aplica para modificar las direcciones de origen o de destino o los números del puerto para la actividad de la red. La característica de la interfaz virtual NAT (NVI), identificada por la adición de una configuración `nacional del permiso del IP a las` interfaces que aplican el NAT o la PALMADITA, no se soporta para la aplicación inter-VRF NAT/PAT. Esta falta de Interoperabilidad entre VRF Lite y interfaz NAT-virtual es seguida por el pedido de mejora CSCek35625.

Configurar

En esta sección, se explican el Firewall del Cisco IOS que reconoce VRF y las configuraciones de escudo de protección Zona-basadas que reconoce VRF clásicos de la directiva.

Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Firewall que reconoce VRF de la obra clásica del Cisco IOS

En esta sección encontrará la información para configurar las funciones descritas en este documento.

El Firewall clásico que reconoce VRF del Cisco IOS (antes llamado CBAC), que es identificado por el uso del `IP examina`, ha estado disponible en Cisco IOS Software puesto que el Firewall clásico fue ampliado para soportar el examen que reconoce VRF en el Cisco IOS Software Release 12.3(14)T.

Firewall clásico que reconoce VRF del Cisco IOS de la configuración

El Firewall clásico que reconoce VRF utiliza el sintaxis de la misma configuración como Firewall NON-VRF para la configuración de la directiva del examen:

```
router(config)#ip inspect name name service
```

Los parámetros de inspección se pueden modificar para cada VRF con las opciones de configuración VRF-específicas:

```
router(config)#ip inspect [parameter value] vrf vrf-name
```

Las listas de la directiva del examen se configuran global, y una directiva del examen se puede aplicar a las interfaces en los VRF múltiples.

Cada VRF lleva su propio conjunto de los parámetros de inspección para los valores tales como protección del servicio negado (DOS), temporizadores de sesión TCP/UDP/ICMP, configuraciones del rastro de auditoría, etc. Si una directiva del examen se utiliza en los VRF múltiples, la Configuración de parámetros VRF-específica reemplaza cualquier configuración global que sea llevada por la directiva del examen. Refiera al Firewall del Cisco IOS y a la protección clásicos del servicio negado del sistema de prevención de intrusiones para más información sobre cómo ajustar los parámetros del protección DoS.

Ver la actividad clásica que reconoce VRF del Firewall del Cisco IOS

Los comandos " show " que reconoce VRF del Firewall diferencian de los comandos NON-VRF-enterados, porque los comandos que reconoce VRF requieren que usted especifique el VRF en el comando " show ":

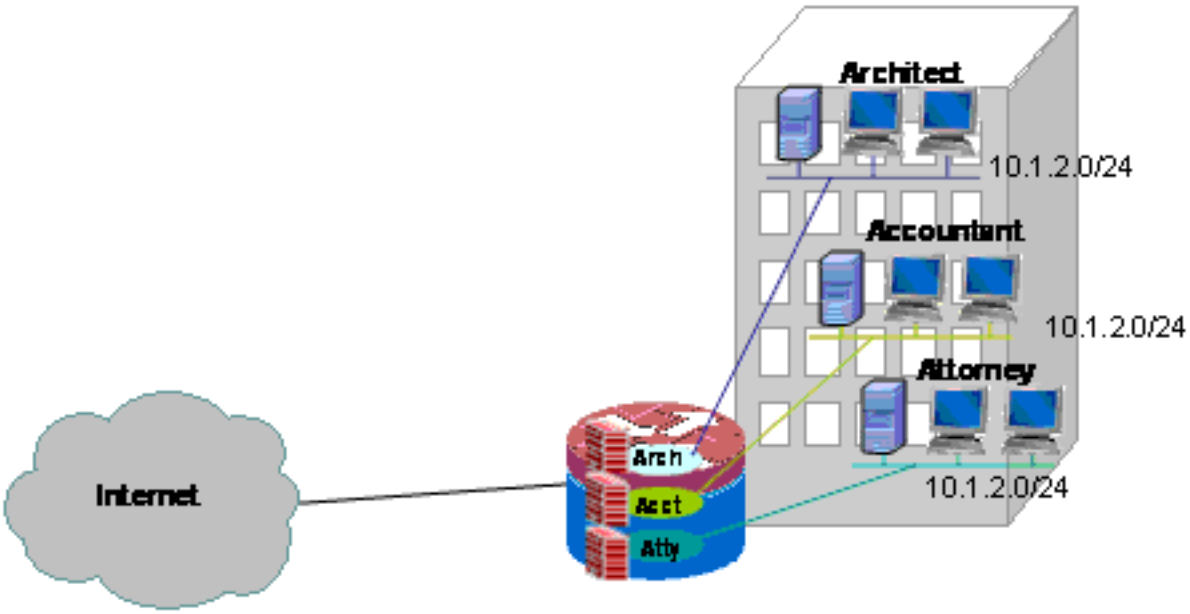
```
router#show ip inspect [ all | config | interfaces | name | sessions | statistics ] vrf vrf-name
```

Firewall de la obra clásica del Solo-sitio Multi-VRF

sitios del Multi-arrendatario que ofrecen el acceso a internet mientras que un servicio del arrendatario puede utilizar el Firewall que reconoce VRF para afectar un aparato el espacio de dirección superpuesta y las políticas del firewall de la plancha de caldera para todos los arrendatarios. Los requisitos para el espacio del routable, el NAT, y el acceso remoto y el servicio del VPN de sitio a sitio se pueden acomodar también a la oferta de los servicios personalizados para cada arrendatario, con la ventaja de disposición un VRF para cada cliente.

Esta aplicación utiliza el espacio de dirección superpuesta para simplificar la Administración de espacio de la dirección. Pero, esto puede causar los problemas que ofrecen la Conectividad entre los diversos VRF. Si la Conectividad no se requiere entre los VRF, el dentro-a-exterior tradicional NAT puede ser aplicado. La puerto-expedición NAT se utiliza para exponer los servidores en el

arquitecto (arco), el contable (acct), y el abogado VRF (atty). El Firewall ACL y las directivas deben acomodar la actividad NAT.



Firewall de la configuración y NAT clásicos para una red de la obra clásica del Solo-sitio Multi-VRF

sitios del Multi-arrendatario que ofrecen el acceso a internet mientras que un servicio del arrendatario puede utilizar el Firewall que reconoce VRF para afectar un aparato el espacio de dirección superpuesta y las políticas del firewall de la plancha de caldera para todos los arrendatarios. Los requisitos para el espacio del routable, el NAT, y el acceso remoto y el servicio del VPN de sitio a sitio se pueden acomodar también a la oferta de los servicios personalizados para cada arrendatario, con la ventaja de disposición un VRF para cada cliente.

Las políticas del firewall clásicas existen, que define el acceso a y desde el diversos LAN y conexiones WAN:

		Fuente de conexión			
		Internet	Arco	Acct	Atty
Destino de la conexión	Internet	N/A	HTTP, HTTPS FTP, DNS, S TP	HTTP, HTTPS FTP, DNS, S TP	HTTP, HTTPS FTP, DNS, S TP
	Arco	FTP	N/A	Niegue	Niegue
	Acct	SMTP	Niegue	N/A	Niegue
	Atty	HTTPS TP	Niegue	Niegue	N/A

Los host en cada uno de los tres VRF pueden acceder los servicios HTTP, HTTPS, FTP, y DNS en el Internet pública. Una lista de control de acceso (ACL 111) será utilizada para restringir el acceso para los tres VRF (puesto que cada VRF permite el acceso a los servicios idénticos en Internet), solamente diversas directivas del examen será aplicada, para proporcionar las estadísticas del examen por-VRF. Los ACL separados se pueden utilizar para proporcionar los contadores ACL por el VRF. Inverso, los host en Internet pueden conectar con los servicios según lo descrito en la tabla anterior de la directiva, según lo definido por ACL 121. El tráfico se debe examinar en las ambas direcciones para acomodar la vuelta con los ACL que protegen la Conectividad en la dirección opuesta. La configuración del NAT se comenta para describir el acceso puerto-remitido a los servicios en los VRF.

Firewall y configuración del NAT clásicos del Multi-arrendatario del Solo-sitio:

```
version 12.4
!
ip cef
!
ip vrf acct
!
ip vrf arch
!
ip vrf atty
!
ip inspect name acct-fw ftp
ip inspect name acct-fw tcp
ip inspect name acct-fw udp
ip inspect name acct-fw icmp
ip inspect name arch-fw ftp
ip inspect name arch-fw tcp
ip inspect name arch-fw udp
ip inspect name arch-fw icmp
ip inspect name atty-fw ftp
ip inspect name atty-fw tcp
ip inspect name atty-fw udp
ip inspect name atty-fw icmp
ip inspect name fw-global tcp
ip inspect name fw-global udp
ip inspect name fw-global icmp
!
!
interface FastEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-FE 0$
 ip address 172.16.100.10 255.255.255.0
 ip access-group 121 in
 ip nat outside
 ip inspect fw-global in
 ip virtual-reassembly
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 no cdp enable
!
interface FastEthernet0/1.171
 encapsulation dot1Q 171
 ip vrf forwarding acct
 ip address 10.1.2.1 255.255.255.0
 ip access-group 111 in
 ip nat inside
```

```
 ip inspect acct-fw in
 ip virtual-reassembly
 no cdp enable
!
interface FastEthernet0/1.172
 encapsulation dot1Q 172
 ip vrf forwarding arch
 ip address 10.1.2.1 255.255.255.0
 ip access-group 111 in
 ip nat inside
 ip inspect arch-fw in
 ip virtual-reassembly
 no cdp enable
!
interface FastEthernet0/1.173
 encapsulation dot1Q 173
 ip vrf forwarding atty
 ip address 10.1.2.1 255.255.255.0
 ip access-group 111 in
 ip nat inside
 ip inspect atty-fw in
 ip virtual-reassembly
 no cdp enable
!
ip route 0.0.0.0 0.0.0.0 172.16.100.1
ip route vrf acct 0.0.0.0 0.0.0.0 172.16.100.1 global
ip route vrf arch 0.0.0.0 0.0.0.0 172.16.100.1 global
ip route vrf atty 0.0.0.0 0.0.0.0 172.16.100.1 global
!
ip nat pool pool-1 172.16.100.100 172.16.100.199 netmask
255.255.255.0 add-route
ip nat inside source list 101 pool pool-1 vrf acct
overload
ip nat inside source list 101 pool pool-1 vrf arch
overload
ip nat inside source list 101 pool pool-1 vrf atty
overload
!
! The following static NAT translations allow access
from the internet to
! servers in each VRF.  Be sure the static translations
correlate to “permit”
! statements in ACL 121, the internet-facing list.
!
ip nat inside source static tcp 10.1.2.2 21
172.16.100.11 21 vrf arch extendable
ip nat inside source static tcp 10.1.2.3 25
172.16.100.12 25 vrf acct extendable
ip nat inside source static tcp 10.1.2.4 25
172.16.100.13 25 vrf atty extendable
ip nat inside source static tcp 10.1.2.5 80
172.16.100.13 80 vrf atty extendable
!
access-list 101 permit ip 10.1.2.0 0.0.0.255 any
access-list 111 permit tcp 10.1.2.0 0.0.0.255 any eq www
access-list 111 permit tcp 10.1.2.0 0.0.0.255 any eq 443
access-list 111 permit tcp 10.1.2.0 0.0.0.255 any eq
smtp
access-list 111 permit tcp 10.1.2.0 0.0.0.255 any eq ftp
access-list 111 permit tcp 10.1.2.0 0.0.0.255 any eq
domain
access-list 111 permit udp 10.1.2.0 0.0.0.255 any eq
domain
access-list 111 permit icmp 10.1.2.0 0.0.0.255 any
```

```
access-list 121 permit tcp any host 172.16.100.11 eq ftp
access-list 121 permit tcp any host 172.16.100.12 eq
smtp
access-list 121 permit tcp any host 172.16.100.13 eq
smtp
access-list 121 permit tcp any host 172.16.100.13 eq www
end
```

Verifique el Firewall y el NAT clásicos para una red de la obra clásica del Solo-sitio Multi-VRF

El examen de la traducción de dirección de red y del Firewall se verifica para cada VRF con estos comandos:

Examine las rutas en cada VRF con el comando del **[vrf-name] del vrf de la ruta de IP de la demostración**:

```
stg-2801-L#show ip route vrf acct Routing Table: acct Codes: C - connected, S - static, R - RIP,
M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF
NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF
external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS
inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded
static route Gateway of last resort is 172.16.100.1 to network 0.0.0.0 172.16.0.0/24 is
subnetted, 1 subnets S 172.16.100.0 [0/0] via 0.0.0.0, NVI0 10.0.0.0/24 is subnetted, 1 subnets
C 10.1.2.0 is directly connected, FastEthernet0/1.171 S* 0.0.0.0/0 [1/0] via 172.16.100.1 stg-
2801-L#
```

Marque la actividad NAT de cada VRF con el comando **nacional del [vrf-name] del vrf del tra del IP de la demostración**:

```
stg-2801-L#show ip nat tra vrf acct Pro Inside global Inside local Outside local Outside global
tcp 172.16.100.12:25 10.1.2.3:25 --- --- tcp 172.16.100.100:1078 10.1.2.3:1078 172.17.111.3:80
172.17.111.3:80
```

Monitoree las estadísticas del examen del Firewall de cada VRF con el **IP de la demostración examinan el** comando del **nombre VRF**:

```
stg-2801-L#show ip insp se vrf acct Established Sessions Session 66484034
(10.1.2.3:1078)=>(172.17.111.3:80) tcp SIS_OPEN
```

El Cisco IOS que reconoce VRF Zona-basó el escudo de protección IOS de la directiva

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Si usted agrega el Firewall Zona-basado Cisco IOS de la directiva a las configuraciones del router multi-VRF, esto lleva poca diferencia del Firewall de la zona en las aplicaciones NON-VRF. Es decir, la determinación de la directiva observa aun así las reglas que un Firewall Zona-basado NON-VRF de la directiva observa, salvo la adición de algunas estipulaciones multi-VRF-específicas:

- Una zona de Seguridad Zona-basada del Firewall de la directiva puede contener las interfaces de solamente una zona.
- Un VRF puede contener más de una zona de Seguridad.
- El Firewall Zona-basado de la directiva es dependiente en la encaminamiento o el NAT para permitir que el tráfico se mueva entre los VRF. Las políticas del firewall que examinan o los pasos trafican entre los Zona-pares inter-VRF no son adecuados permitir que el tráfico se mueva entre los VRF.

El Cisco IOS que reconoce VRF de la configuración Zona-basó el Firewall de la directiva

El Firewall Zona-basado que reconoce VRF de la directiva utiliza el sintaxis de la misma configuración como Firewall Zona-basado NON-VRF-enterado de la directiva, y asigna las interfaces a las zonas de Seguridad, define las políticas de seguridad para el tráfico que se mueve entre las zonas, y asigna la política de seguridad a las asociaciones apropiadas de los zona-pares.

la configuración VRF-específica es innecesaria. Los Parámetros de configuración global son aplicados, a menos que un parámetro-mapa más específico se agregue al examen en un directiva-mapa. Incluso en el caso donde un parámetro-mapa se utiliza para aplicar una configuración más específica, el parámetro-mapa no es VRF-específico.

Ver el Cisco IOS que reconoce VRF Zona-basó la actividad del Firewall de la directiva

Los comandos show Zona-basados que reconoce VRF del Firewall de la directiva son no diferentes de los comandos NON-VRF-enterados; El Firewall Zona-basado de la directiva aplica el tráfico que se mueve desde las interfaces en una zona de Seguridad a las interfaces en otra zona de Seguridad, sin importar las asignaciones VRF de las diversas interfaces. Así, el Firewall Zona-basado que reconoce VRF de la directiva emplea los mismos **comandos show** para ver la actividad del Firewall que son utilizados por el Firewall de la directiva Zona-Basar en las aplicaciones NON-VRF:

```
router#show policy-map type inspect zone-pair sessions
```

El Firewall Zona-basado Cisco IOS que reconoce VRF de la directiva utiliza los casos

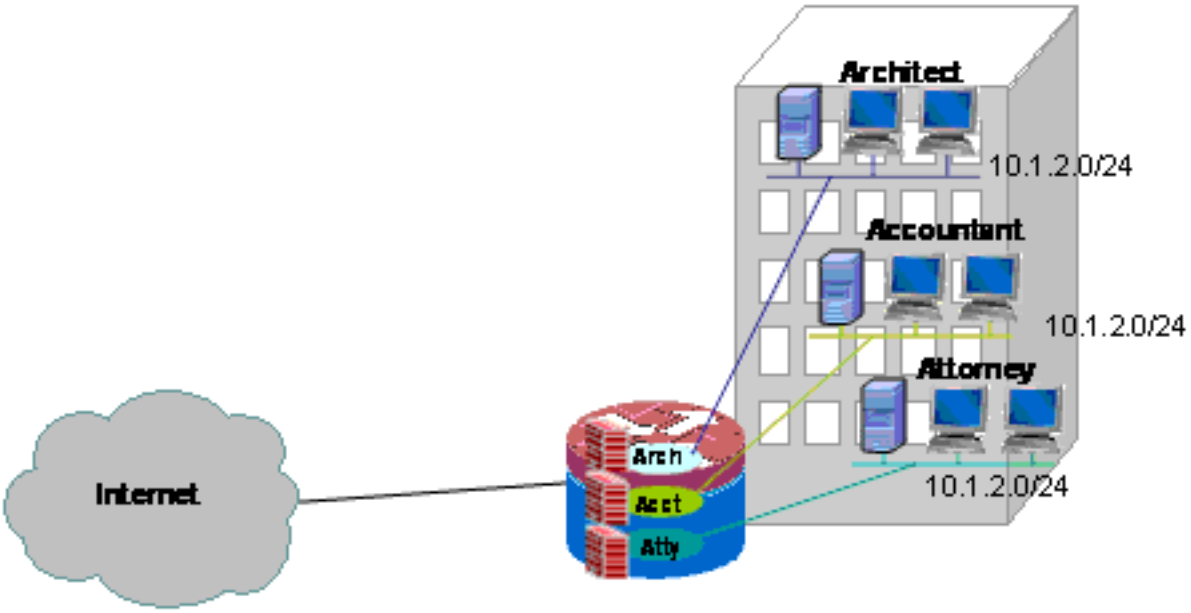
Los casos que reconoce VRF del uso del Firewall varían extensamente. Direccionamiento de estos ejemplos:

- Un despliegue que reconoce VRF del solo-sitio, usado típicamente para los recursos del multi-arrendatario o las redes al por menor
- Una sucursal/una aplicación al por menor/del telecommuter donde el tráfico de red privada se mantiene un VRF separado del tráfico de público-Internet. Aíslan a los usuarios del acceso a internet de los usuarios de la red comercial, y todo el tráfico de red comercial se dirige sobre una conexión VPN al sitio HQ para la aplicación de la política de Internet.

El Solo-sitio Multi-VRF Zona-basó el Firewall de la directiva

sitios del Multi-arrendatario que ofrecen el acceso a internet mientras que un servicio del arrendatario puede utilizar el Firewall que reconoce VRF para afectar un aparato el espacio de dirección superpuesta y las políticas del firewall de la plancha de caldera para todos los arrendatarios. Esta aplicación es típica para los LAN múltiples en un sitio dado que comparta a un router del Cisco IOS para el acceso a internet, o donde ofrecen un partner comercial tal como un photofinisher o cierto otro servicio una red de datos aislada con la Conectividad a Internet y a un poco de parte de específica la red del propietario de la premisa, sin el requisito del hardware de red adicional o de la conectividad a Internet. Los requisitos para el espacio del routable, el NAT, y el acceso remoto y el servicio del VPN de sitio a sitio se pueden acomodar también a la oferta de los servicios personalizados para cada arrendatario, con la ventaja de disposición un VRF para cada cliente.

Esta aplicación utiliza el espacio de dirección superpuesta para simplificar la Administración de espacio de la dirección. Pero, esto puede causar los problemas que ofrecen la Conectividad entre los diversos VRF. Si la Conectividad no se requiere entre los VRF, el dentro-a-exterior tradicional NAT puede ser aplicado. Además, la puerto-expedición NAT se utiliza para exponer los servidores en el arquitecto (arco), el contable (acct), y el abogado VRF (atty). El Firewall ACL y las directivas deben acomodar la actividad NAT.



El Solo-sitio de la configuración Multi-VRF Zona-basó el Firewall de la directiva y el NAT

el Multi-arrendatario localiza el acceso a internet de ofrecimiento mientras que un servicio del arrendatario puede utilizar el Firewall que reconoce VRF para afectar un aparato el espacio de dirección superpuesta y las políticas del firewall de la plancha de caldera para todos los arrendatarios. Los requisitos para el espacio del routable, el NAT, y el acceso remoto y el servicio del VPN de sitio a sitio se pueden acomodar también a la oferta de los servicios personalizados para cada arrendatario, con la ventaja de disposición un VRF para cada cliente.

Las políticas del firewall clásicas existen, que define el acceso a y desde el diversos LAN y conexiones WAN:

		Fuente de conexión			
		Internet	Arco	Acct	Atty
Destino de la conexión	Internet	N/A	HTTP, HTTPS FTP, DNS, S TP	HTTP, HTTPS FTP, DNS, S TP	HTTP, HTTPS FTP, DNS, S TP
	Arco	FTP	N/A	Niegue	Niegue
	Acct	SMTP	Niegue	N/A	Niegue
	Atty	HTTPS	Niegue	Niegue	N/A

		TP			

Los host en cada uno de los tres VRF pueden acceder los servicios HTTP, HTTPS, FTP, y DNS en el Internet pública. Un clase-mapa (soldado-público-cmap) se utiliza para restringir el acceso para los tres VRF, puesto que cada VRF permite el acceso a los servicios idénticos en Internet, solamente diversas polic-correspondencias es aplicado, para proporcionar las estadísticas del examen por-VRF. Inverso, los host en Internet pueden conectar con los servicios según lo descrito en la tabla anterior de la directiva, según lo definido por class-maps individual y las correspondencias de políticas para los zona-pares Internet-a-VRF. Un directiva-mapa separado se utiliza para prevenir el acceso a los servicios de administración del router en la uno mismo-zona de Internet público. La misma directiva se puede aplicar para prevenir el acceso del soldado VRF a la uno mismo-zona del router también.

La configuración del NAT se comenta para describir el acceso puerto-remitido a los servicios en los VRF.

El Multi-arrendatario del Solo-sitio Zona-basó el Firewall y la configuración del NAT de la directiva:

```
version 12.4
!
ip cef
!
ip vrf acct
!
ip vrf arch
!
ip vrf atty
!
class-map type inspect match-any out-cmap
 match protocol http
 match protocol https
 match protocol ftp
 match protocol smtp
 match protocol ftp
!
class-map type inspect match-all pub-arch-cmap
 match access-group 121
 match protocol ftp
!
class-map type inspect match-all pub-acct-cmap
 match access-group 122
 match protocol http
!
class-map type inspect pub-atty-mail-cmap
match access-group 123
 match protocol smtp
!
class-map type inspect pub-atty-web-cmap
 match access-group 124
 match protocol http
!
policy-map type inspect arch-pub-pmap
 class type inspect out-cmap
  inspect
!
policy-map type inspect acct-pub-pmap
 class type inspect out-cmap
  inspect
!
```

```
policy-map type inspect atty-pub-pmap
 class type inspect out-cmap
  inspect
!
policy-map type inspect pub-arch-pmap
 class type inspect pub-arch-cmap
  inspect
!
policy-map type inspect pub-acct-pmap
 class type inspect pub-acct-cmap
  inspect
!
policy-map type inspect pub-atty-pmap
 class type inspect pub-atty-mail-cmap
  inspect
 class type inspect pub-atty-web-cmap
  inspect
!
policy-map type inspect pub-self-pmap
 class class-default
  drop log
!
zone security arch
zone security acct
zone security atty
zone security public
zone-pair security arch-pub source arch destination
public
 service-policy type inspect arch-pub-pmap
zone-pair security acct-pub source acct destination
public
 service-policy type inspect acct-pub-pmap
zone-pair security atty-pub source atty destination
public
 service-policy type inspect atty-pub-pmap
zone-pair security pub-arch source public destination
arch
 service-policy type inspect pub-arch-pmap
zone-pair security pub-acct source public destination
acct
 service-policy type inspect pub-acct-pmap
zone-pair security pub-atty source public destination
atty
 service-policy type inspect pub-atty-pmap
zone-pair security pub-self source public destination
self
 service-policy type inspect pub-self-pmap
!
!
interface FastEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-FE 0$
 ip address 172.16.100.10 255.255.255.0
 ip nat outside
 zone-member security public
 ip virtual-reassembly
 speed auto
 no cdp enable
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 no cdp enable
!
```

```
interface FastEthernet0/1.171
 encapsulation dot1Q 171
 ip vrf forwarding acct
 ip address 10.1.2.1 255.255.255.0
 ip nat inside
 zone-member security acct
 ip virtual-reassembly
 no cdp enable
!
interface FastEthernet0/1.172
 encapsulation dot1Q 172
 ip vrf forwarding arch
 ip address 10.1.2.1 255.255.255.0
 ip nat inside
 zone-member security arch
 ip virtual-reassembly
 no cdp enable
!
interface FastEthernet0/1.173
 encapsulation dot1Q 173
 ip vrf forwarding atty
 ip address 10.1.2.1 255.255.255.0
 ip nat inside
 zone-member security atty
 ip virtual-reassembly
 no cdp enable
!
ip route 0.0.0.0 0.0.0.0 172.16.100.1
ip route vrf acct 0.0.0.0 0.0.0.0 172.16.100.1 global
ip route vrf arch 0.0.0.0 0.0.0.0 172.16.100.1 global
ip route vrf atty 0.0.0.0 0.0.0.0 172.16.100.1 global
!
ip nat pool pool-1 172.16.100.100 172.16.100.199 netmask
255.255.255.0 add-route
ip nat inside source list 101 pool pool-1 vrf acct
overload
ip nat inside source list 101 pool pool-1 vrf arch
overload
ip nat inside source list 101 pool pool-1 vrf atty
overload
!
! The following static NAT translations allow access
from the internet to
! servers in each VRF.  Be sure the static translations
correlate to “inspect”
! statements in in the Zone Firewall configuration, the
internet-facing list.
! Note that the ACLs used in the firewall correspond to
the end-host address, not
! the NAT Outside address
!
ip nat inside source static tcp 10.1.2.2 21
172.16.100.11 21 vrf arch extendable
ip nat inside source static tcp 10.1.2.3 25
172.16.100.12 25 vrf acct extendable
ip nat inside source static tcp 10.1.2.4 25
172.16.100.13 25 vrf atty extendable
ip nat inside source static tcp 10.1.2.5 80
172.16.100.13 80 vrf atty extendable
!
access-list 101 permit ip 10.1.2.0 0.0.0.255 any
access-list 121 permit ip any host 10.1.2.2
access-list 122 permit ip any host 10.1.2.3
access-list 123 permit ip any host 10.1.2.4
```

```
access-list 124 permit ip any host 10.1.2.5
!
! Disable CDP
!
no cdp run
!
end
```

Verifique el Firewall y el NAT clásicos para una red de la obra clásica del Solo-sitio Multi-VRF

El examen de la traducción de dirección de red y del Firewall se verifica para cada VRF con estos comandos:

Examine las rutas en cada VRF con el comando del **[vrf-name] del vrf de la ruta de IP de la demostración**:

```
stg-2801-L#show ip route vrf acct Routing Table: acct Codes: C - connected, S - static, R - RIP,
M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF
NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF
external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS
inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded
static route Gateway of last resort is 172.16.100.1 to network 0.0.0.0 172.16.0.0/24 is
subnetted, 1 subnets S 172.16.100.0 [0/0] via 0.0.0.0, NVI0 10.0.0.0/24 is subnetted, 1 subnets
C 10.1.2.0 is directly connected, FastEthernet0/1.171 S* 0.0.0.0/0 [1/0] via 172.16.100.1 stg-
2801-L#
```

Marque la actividad NAT cada VRF con el comando nacional del [vrf-name] del vrf del tra del IP de la demostración:

```
stg-2801-L#show ip nat translations Pro Inside global Inside local Outside local Outside global
tcp 172.16.100.12:25 10.1.2.3:25 --- --- tcp 172.16.100.100:1033 10.1.2.3:1033 172.17.111.3:80
172.17.111.3:80 tcp 172.16.100.11:21 10.1.2.2:23 --- --- tcp 172.16.100.13:25 10.1.2.4:25 --- --
- tcp 172.16.100.13:80 10.1.2.5:80 --- ---
```

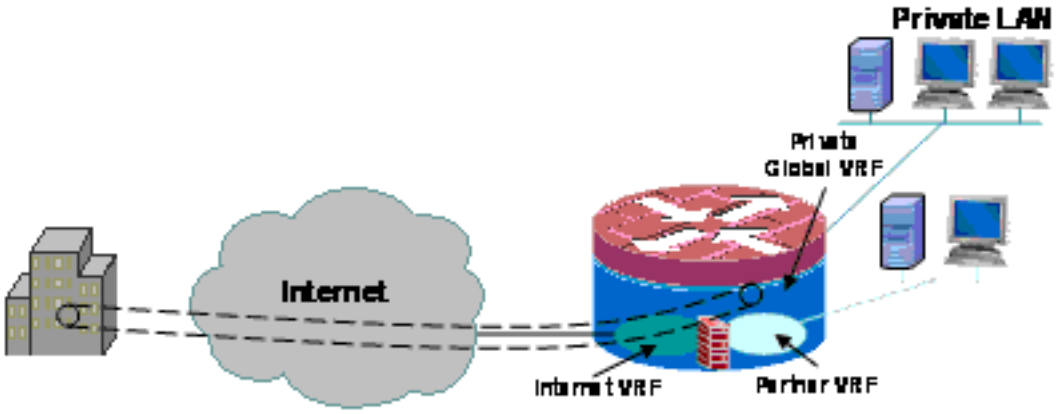
Las estadísticas del examen del Firewall del monitor con el **tipo del directiva-mapa de la demostración examinan los** comandos de los zona-**pares**:

```
stg-2801-L#show policy-map type inspect zone-pair Zone-pair: arch-pub Service-policy inspect :
arch-pub-pmap Class-map: out-cmap (match-any) Match: protocol http 1 packets, 28 bytes 30 second
rate 0 bps Match: protocol https 0 packets, 0 bytes 30 second rate 0 bps Match: protocol ftp 0
packets, 0 bytes 30 second rate 0 bps Match: protocol smtp 0 packets, 0 bytes 30 second rate 0
bps Inspect Packet inspection statistics [process switch:fast switch] tcp packets: [1:15]
Session creations since subsystem startup or last reset 1 Current session counts (estab/half-
open/terminating) [0:0:0] Maxever session counts (estab/half-open/terminating) [1:1:0] Last
session created 00:09:50 Last statistic reset never Last session creation rate 0 Maxever session
creation rate 1 Last half-open session total 0 Class-map: class-default (match-any) Match: any
Drop (default action) 8 packets, 224 bytes
```

El Firewall Zona-basado Solo-sitio de la directiva Multi-VRF, conexión de Internet con el respaldo en la zona de “Internet”, VRF global tiene conexión al HQ

Esta aplicación está bien adaptada a las implementaciones del telecommuter, a las pequeñas ubicaciones al por menor, y a cualquier otro despliegue de red de sitio remoto que requiera la segregación de los recursos de red privada del acceso de red pública. Aislando a los usuarios del hotspot de la conectividad a Internet y del hogar o del público a un *público* VRF, y aplicando una ruta predeterminado en el VRF global que rutea todo el tráfico de red privada a través de los túneles VPN, los recursos en el VRF privado, global y el *público Internet*-accesible VRF ningún accesibilidad el uno al otro, así han quitado totalmente la amenaza del compromiso del host de la soldado-red por la actividad de público-Internet. Además, un VRF adicional puede ser aprovisionado para proporcionar un espacio protegido de la ruta para otros consumidores que

necesitan un espacio de red aislado, tal como terminales de la lotería, máquinas atmósfera, placa de carga que procesa las terminales, u otras aplicaciones. El Wi-Fi múltiple SSID puede ser aprovisionado para ofrecer a acceso a ambos la red privada, así como un hotspot público.



Este ejemplo describe la configuración para dos conexiones a Internet de banda ancha, aplicando la PALMADITA (sobrecarga NAT) para los host en el *público* y el *partner* VRF para el acceso a Internet público, con la conectividad a Internet confiada por SLA monitoreando en las dos conexiones. La red privada (en el VRF global) utiliza una conexión del GRE sobre IPSec para mantener la Conectividad a HQ (configuración incluida para el router de centro distribuidor VPN) sobre los dos links de banda ancha. En caso que una o la otra de las conexiones de banda ancha falle, la Conectividad al centro distribuidor VPN se mantiene, que permite el acceso ininterrumpido a la red HQ, puesto que el punto final local del túnel no se ata específicamente a tampoco de las conexiones de Internet.

Un Firewall zona-basado de la directiva existe acceso y de los controles a y desde el VPN a la red privada, y entre el público y el partner LAN y Internet para permitir el acceso a internet saliente, pero ningunas conexiones adentro a las redes locales de Internet:

	Internet	Público	Partner	VPN	Privado
Internet	N/A	Niegue	Niegue	Niegue	Niegue
Público	HTTP, HTTPS, FTP, DNS	N/A	Niegue	Niegue	Niegue
Partner		Niegue	N/A		
VPN	Niegue	Niegue	Niegue	N/A	
Privado	Niegue	Niegue	Niegue		N/A

La aplicación NAT para el hotspot y el tráfico de la partner-red hace el compromiso de Internet público mucho menos probablemente, pero la posibilidad todavía existe que los usuarios malintencionados o el software pueden explotar a una sesión NAT activa. La aplicación de la inspección con estado minimiza las ocasiones que los host locales pueden ser comprometidos atacando a una sesión de NAT abierta. Este ejemplo emplea un 871W, pero la configuración se puede replicar fácilmente con otras Plataformas ISR.

Configure el Firewall Zona-basado Solo-sitio de la directiva Multi-VRF, conexión de Internet primaria con el respaldo, VRF global tiene VPN al escenario HQ

sitios del Multi-arrendatario que ofrecen el acceso a internet mientras que un servicio del arrendatario puede utilizar el Firewall que reconoce VRF para afectar un aparato el espacio de dirección superpuesta y las políticas del firewall de la plancha de caldera para todos los arrendatarios. Los requisitos para el espacio del routable, el NAT, y el acceso remoto y el servicio del VPN de sitio a sitio se pueden acomodar también a la oferta de los servicios personalizados para cada arrendatario, con la ventaja de disposición un VRF para cada cliente.

```
version 12.4
!
hostname stg-871
!
aaa new-model
!
aaa authentication login default local
aaa authorization console
aaa authorization exec default local
!
aaa session-id common
ip cef
!
no ip dhcp use vrf connected
!
ip dhcp pool priv-108-net
   import all
   network 192.168.108.0 255.255.255.0
   default-router 192.168.108.1
!
ip vrf partner
 description Partner VRF
 rd 100:101
!
ip vrf public
 description Internet VRF
 rd 100:100
!
no ip domain lookup
ip domain name yourdomain.com
!
track timer interface 5
!
track 123 rtr 1 reachability
 delay down 15 up 10
!
class-map type inspect match-any hotspot-cmap
 match protocol dns
 match protocol http
 match protocol https
 match protocol ftp
class-map type inspect match-any partner-cmap
 match protocol dns
 match protocol http
 match protocol https
 match protocol ftp
!
policy-map type inspect hotspot-pmap
 class type inspect hotspot-cmap
  inspect
 class class-default
!
zone security internet
zone security hotspot
zone security partner
```

```
zone security hq
zone security office
zone-pair security priv-pub source private destination public
 service-policy type inspect priv-pub-pmap
!
crypto keyring hub-ring vrf public
  pre-shared-key address 172.16.111.5 key cisco123
!
crypto isakmp policy 1
 authentication pre-share
 group 2
!
crypto ipsec transform-set md5-des-ts esp-des esp-md5-hmac
!
crypto ipsec profile md5-des-prof
 set transform-set md5-des-ts
!
bridge irb
!
interface Tunnel0
 ip unnumbered Vlan1
 zone-member security public
 tunnel source BVI1
 tunnel destination 172.16.111.5
 tunnel mode ipsec ipv4
 tunnel vrf public
 tunnel protection ipsec profile md5-des-prof
!
interface FastEthernet0
 no cdp enable
!
interface FastEthernet1
 no cdp enable
!
interface FastEthernet2
 switchport access vlan 111
 no cdp enable
!
interface FastEthernet3
 switchport access vlan 104
 no cdp enable
!
interface FastEthernet4
 description Internet Intf
 ip dhcp client route track 123
 ip vrf forwarding public
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
 speed 100
 full-duplex
 no cdp enable
!
interface Dot11Radio0
 no ip address
 !
 ssid test
    vlan 11
    authentication open
    guest-mode
 !
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 station-role root
 no cdp enable
```

```
!
interface Dot11Radio0.1
 encapsulation dot1Q 11 native
 no cdp enable
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Vlan1
 description LAN Interface
 ip address 192.168.108.1 255.255.255.0
 ip virtual-reassembly
 ip tcp adjust-mss 1452
!
interface Vlan104
 ip vrf forwarding public
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
!
interface Vlan11
 no ip address
 ip nat inside
 ip virtual-reassembly
 bridge-group 1
!
interface BVI1
 ip vrf forwarding public
 ip address 192.168.108.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
router eigrp 1
 network 192.168.108.0
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 Tunnel0
ip route vrf public 0.0.0.0 0.0.0.0 Vlan104 dhcp 10
ip route vrf public 0.0.0.0 0.0.0.0 FastEthernet4 dhcp
!
ip nat inside source route-map dhcp-nat interface Vlan104 vrf public overload
ip nat inside source route-map fixed-nat interface FastEthernet4 vrf public overload
!
ip sla 1
 icmp-echo 172.16.108.1 source-interface FastEthernet4
 timeout 1000
 threshold 40
 vrf public
 frequency 3
ip sla schedule 1 life forever start-time now
access-list 110 permit ip 192.168.108.0 0.0.0.255 any
access-list 111 permit ip 192.168.108.0 0.0.0.255 any
no cdp run
!
route-map fixed-nat permit 10
 match ip address 110
 match interface FastEthernet4
!
route-map dhcp-nat permit 10
 match ip address 111
 match interface Vlan104
!
```

```
bridge 1 protocol ieee
bridge 1 route ip
!
end
```

Esta Configuración del hub proporciona un ejemplo de la configuración de la conectividad VPN:

```
version 12.4
!
hostname 3845-bottom
!
ip cef
!
crypto keyring any-peer
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
!
crypto isakmp policy 1
 authentication pre-share
 group 2
crypto isakmp profile profile-name
   keyring any-peer
   match identity address 0.0.0.0
   virtual-template 1
!
crypto ipsec transform-set md5-des-ts esp-des esp-md5-hmac
!
crypto ipsec profile md5-des-prof
 set transform-set md5-des-ts
!
interface Loopback111
 ip address 192.168.111.1 255.255.255.0
 ip nat enable
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 media-type rj45
 no keepalive
!
interface GigabitEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 172.16.1.103 255.255.255.0
 shutdown
!
interface GigabitEthernet0/0.111
 encapsulation dot1Q 111
 ip address 172.16.111.5 255.255.255.0
 ip nat enable
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback111
 ip nat enable
 tunnel source GigabitEthernet0/0.111
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile md5-des-prof
!
router eigrp 1
 network 192.168.111.0
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 172.16.111.1
!
ip nat source list 111 interface GigabitEthernet0/0.111
!
```

```
access-list 1 permit any
access-list 111 deny   ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
access-list 111 permit ip 192.168.0.0 0.0.255.255 any
!
!
End
```

Verifique el Firewall Zona-basado Solo-sitio de la directiva Multi-VRF, conexión de Internet primaria con el respaldo, VRF global tiene VPN al escenario HQ

El examen de la traducción de dirección de red y del Firewall se verifica para cada VRF con estos comandos:

Examine las rutas en cada VRF con el comando del **[vrf-name] del vrf de la ruta de IP de la demostración**:

```
stg-2801-L#show ip route vrf acct
```

Marque la actividad NAT de cada VRF con el comando **nacional del [vrf-name] del vrf del tra del IP de la demostración**:

```
stg-2801-L#show ip nat translations
```

Las estadísticas del examen del Firewall del monitor con el **tipo del directiva-mapa de la demostración examinan los** comandos de los zona-**pares**:

```
stg-2801-L#show policy-map type inspect zone-pair
```

Conclusión

Coste que reconoce VRF y carga administrativa reducidos ofertas clásicos del Cisco IOS y Zona-basados del Firewall de la directiva para proveer de la conectividad de red la seguridad integrada para las Redes múltiples con el hardware mínimo. El funcionamiento y el scalability se mantiene para las Redes múltiples y proporciona una plataforma eficaz para la infraestructura de red y los servicios sin el aumento del coste de capital.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Problema

El servidor Exchange no es accesible de la interfaz exterior del router.

Solución

Permita a la inspección SMTP en el router para reparar este problema

Configuración de muestra:

```
ip nat inside source static tcp 192.168.1.10 25 10.15.22.2 25 extendable
ip nat inside source static tcp 192.168.1.10 80 10.15.22.2 80 extendable
ip nat inside source static tcp 192.168.1.10 443 10.15.22.2 443 extendable
```

```
access-list 101 permit ip any host 192.168.1.10
access-list 103 permit ip any host 192.168.1.10
access-list 105 permit ip any host 192.168.1.10

class-map type inspect match-all sdm-nat-http-1
 match access-group 101
 match protocol http

class-map type inspect match-all sdm-nat-http-2
 match access-group 103
 match protocol http

class-map type inspect match-all sdm-nat-http-3 **
 match access-group 105
 match protocol http

policy-map type inspect sdm-pol-NATOutsideToInside-1
 class type inspect sdm-nat-http-1
  inspect
 class type inspect sdm-nat-user-protocol--1-1
  inspect
 class type inspect sdm-nat-http-2
  inspect
 class class-default
policy-map type inspect sdm-pol-NATOutsideToInside-2 **
 class type inspect sdm-nat-user-protocol--1-2
  inspect
 class type inspect sdm-nat-http-3
  inspect
 class class-default

zone-pair security sdm-zp-NATOutsideToInside-1 source out-zone destination in-zone
 service-policy type inspect sdm-pol-NATOutsideToInside-2
```

Información Relacionada

- Guía de diseño Zona-basada del Firewall de la directiva
- Usando el Firewall Zona-basado de la directiva con el VPN
- Firewall Cisco IOS enterado VRF
- NAT de integración con el MPLS VPNs
- Diseño de las Extensiones MPLS para el Routers de la frontera del cliente
- Verificación del funcionamiento de NAT y resolución de problemas básicos de NAT
- Ejemplo de configuración del contexto múltiple del PIX/ASA
- Cisco IOS Firewall
- Soporte Técnico y Documentación - Cisco Systems