Ejemplo de Configuración de Aplicación de Firewall Virtual Clásico y Basado en Zona de Cisco IOS Firewall

Contenido

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 software Cisco IOS® introdujo el firewall virtual (con reconocimiento de VRF), ampliando la familia de funciones de reenvío de routing virtual (VRF) para ofrecer inspección de paquetes con estado, firewall transparente, inspección de aplicaciones y filtrado de URL, además de las funciones existentes de VPN, NAT, QoS y otras que reconocen VRF. Los escenarios de aplicaciones más previsibles aplicarán NAT con otras funciones. Si no se requiere NAT, se puede aplicar el ruteo entre los VRF para proporcionar conectividad entre VRF. El software Cisco IOS ofrece capacidades de reconocimiento de VRF tanto en Cisco IOS Classic Firewall como en Cisco IOS Zone-Based Policy Firewall, con ejemplos de ambos modelos de configuración proporcionados en este documento. Se presta mayor atención a la configuración de firewall de políticas basada en zonas.

Prerequisites

Requirements

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 las imágenes Advanced Security, Advanced IP Services y Advanced Enterprise, así como en las imágenes de la nomenclatura antigua que llevan la designación *o3*, que indica la integración del conjunto de funciones de Cisco IOS Firewall. Función de firewall con detección de VRF que se fusiona en las versiones principales del software IOS de Cisco en 12.4. Se requiere la versión 12.4(6)T o posterior del software del IOS de Cisco para aplicar el firewall de políticas basado en zonas que reconoce VRF. El Cisco IOS Zone-Based Policy Firewall no funciona con stateful failover.

Configuración de VRF

Cisco IOS Software mantiene las configuraciones para el VRF global y todos los VRF privados en el mismo archivo de configuración. Si se accede a la configuración del router a través de la interfaz de línea de comandos, el control de acceso basado en roles ofrecido en la función de vistas de CLI se puede utilizar para limitar la capacidad del personal de administración y funcionamiento del router. Las aplicaciones de gestión, como Cisco Security Manager (CSM), también proporcionan control de acceso basado en funciones para garantizar que el personal operativo esté limitado al nivel adecuado de capacidad.

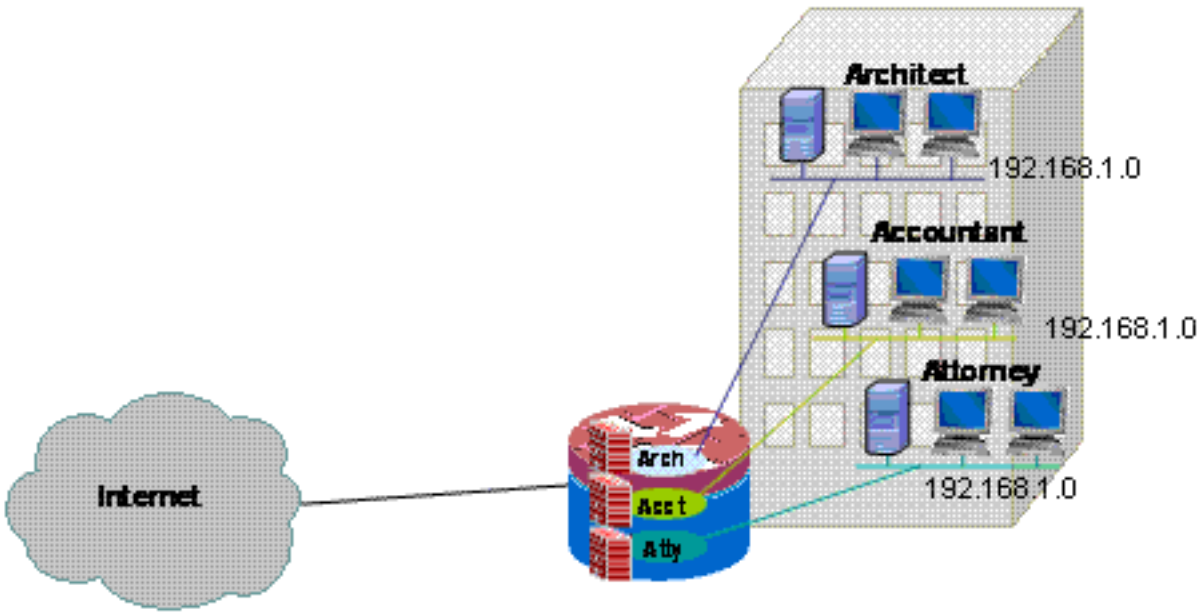
Descripción General de Usos Comunes para el Firewall de IOS con Reconocimiento de VRF

El firewall que reconoce VRF agrega inspección de paquetes stateful a la capacidad de routing/reenvío virtual (VRF) de Cisco IOS. IPsec VPN, traducción de direcciones de red (NAT)/traducción de direcciones de puerto (PAT), sistema de prevención de intrusiones (IPS) y otros servicios de seguridad de Cisco IOS se pueden combinar con firewall con detección de VRF para proporcionar un conjunto completo de servicios de seguridad en los VRF. Los VRF proporcionan soporte para varios espacios de ruta que emplean la numeración de direcciones IP

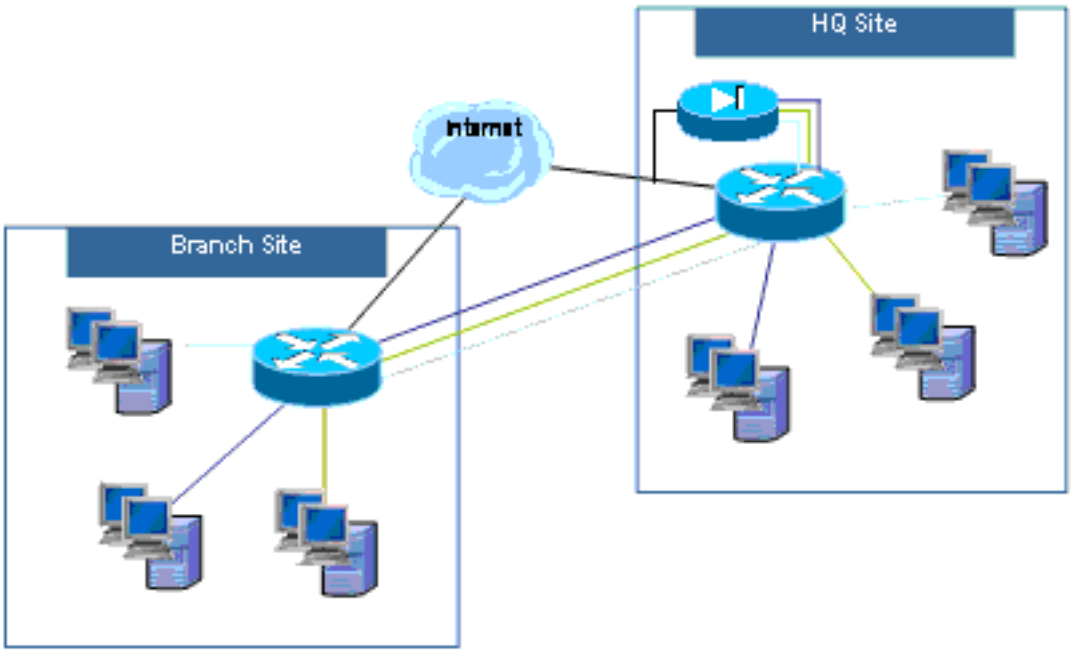
superpuestas, de modo que un router se pueda dividir en varias instancias de ruteo discretas para la separación del tráfico. El firewall que reconoce VRF incluye una etiqueta VRF en la información de sesión para todas las actividades de inspección que el router está realizando un seguimiento, a fin de mantener la separación entre la información de estado de conexión que puede ser idéntica en todos los aspectos. El firewall que reconoce VRF puede inspeccionar entre interfaces dentro de un VRF, así como entre interfaces en VRF que difieren, por ejemplo, en los casos en que el tráfico atraviesa los límites de VRF, de modo que se obtiene la máxima flexibilidad de inspección del firewall tanto para el tráfico intra-VRF como entre VRF.

Las aplicaciones de Cisco IOS Firewall que reconocen VRF se pueden agrupar en dos categorías básicas:

- Varios arrendatarios, un solo sitio: acceso a Internet para varios arrendatarios con espacios de direcciones superpuestos o espacios de ruta segregados en una única instalación. El firewall con inspección activa (stateful) se aplica a la conectividad a Internet de cada VRF para reducir aún más la probabilidad de que se produzcan riesgos a través de conexiones NAT abiertas. El reenvío de puertos se puede aplicar para permitir la conectividad a los servidores en los
  VRF.



En este documento se proporciona un ejemplo de una aplicación de sitio único de varios arrendatarios para el modelo de configuración de firewall clásico que reconoce VRF y el modelo de configuración de firewall basado en zonas que reconoce VRF.
- Varios arrendatarios y varios sitios: varios arrendatarios que comparten equipos en una red grande necesitan conectividad entre varios sitios mediante la conexión de VRF de arrendatarios en diferentes sitios a través de conexiones VPN o WAN. Se puede requerir acceso a Internet para cada arrendatario en uno o varios sitios. Para simplificar la gestión, varios departamentos pueden dividir sus redes en un único router de acceso para cada sitio, pero varios departamentos requieren segregación del espacio de



direcciones. En una próxima actualización de este documento se proporcionarán ejemplos de configuración para aplicaciones multisitio de varios arrendatarios tanto para el modelo de configuración de firewall clásico que reconoce VRF como para el modelo de configuración de firewall basado en zonas que reconoce VRF.

Configuración no admitida

El firewall que reconoce VRF está disponible en imágenes de Cisco IOS que admiten CE de VRF múltiple (VRF Lite) y VPN MPLS. La capacidad del firewall se limita a las interfaces que no son de MPLS. Es decir, si una interfaz participará en el tráfico etiquetado con MPLS, no se podrá aplicar la inspección de firewall en esa interfaz.

Un router sólo puede inspeccionar el tráfico entre VRF si el tráfico debe entrar o salir de un VRF a través de una interfaz para cruzar a un VRF diferente. Si el tráfico se rutea directamente a otro VRF, no hay una interfaz física donde una política de firewall pueda inspeccionar el tráfico, por lo que el router no puede aplicar la inspección.

La configuración de VRF Lite sólo puede interoperar con NAT/PAT si `ip nat inside` o `ip nat outside` está configurada en interfaces donde NAT/PAT se aplica para modificar direcciones de origen o destino o números de puerto para la actividad de red. La función NAT Virtual Interface (NVI), identificada mediante la adición de una configuración `ip nat enable` a las interfaces que aplican NAT o PAT, no es compatible con la aplicación NAT/PAT entre VRF. Esta falta de interoperabilidad entre VRF Lite y la interfaz virtual NAT se controla mediante la solicitud de mejora CSCek35625.

Configurar

En esta sección, se explican las configuraciones de firewall clásico de Cisco IOS que reconoce VRF y firewall de políticas basado en zonas que reconoce VRF.

Nota: Use el Command Lookup Tool (únicamente clientes registrados) para obtener más información sobre los comandos que se utilizan en esta sección.

Firewall clásico de Cisco IOS con detección de VRF

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

El Cisco IOS VRF-Aware Classic Firewall (anteriormente denominado CBAC), que se identifica mediante el uso de `ip inspect`, ha estado disponible en Cisco IOS Software desde que se amplió el firewall clásico para admitir la inspección con reconocimiento de VRF en la versión 12.3(14)T del software Cisco IOS.

Configuración del firewall clásico que reconoce VRF de Cisco IOS

El firewall clásico que reconoce VRF utiliza la misma sintaxis de configuración que el firewall que no es VRF para la configuración de la política de inspección:

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

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

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

Las listas de políticas de inspección se configuran globalmente y se puede aplicar una política de inspección a las interfaces en varios VRF.

Cada VRF lleva su propio conjunto de parámetros de inspección para valores como protección de denegación de servicio (DoS), temporizadores de sesión TCP/UDP/ICMP, configuración de pista de auditoría, etc. Si se utiliza una política de inspección en varios VRF, la configuración de parámetro específica de VRF reemplaza cualquier configuración global que se lleve a cabo mediante la política de inspección. Refiérase a Cisco IOS Classic Firewall and Intrusion Prevention System Denial-of-Service Protection para obtener más información sobre cómo ajustar los parámetros de protección DoS.

Visualización de la Actividad del Firewall Clásico que Reconoce VRF de Cisco IOS

Los comandos "show" de firewall que reconocen VRF difieren de los comandos que no reconocen VRF, porque los comandos que reconocen VRF requieren que especifique el VRF en el comando "show":

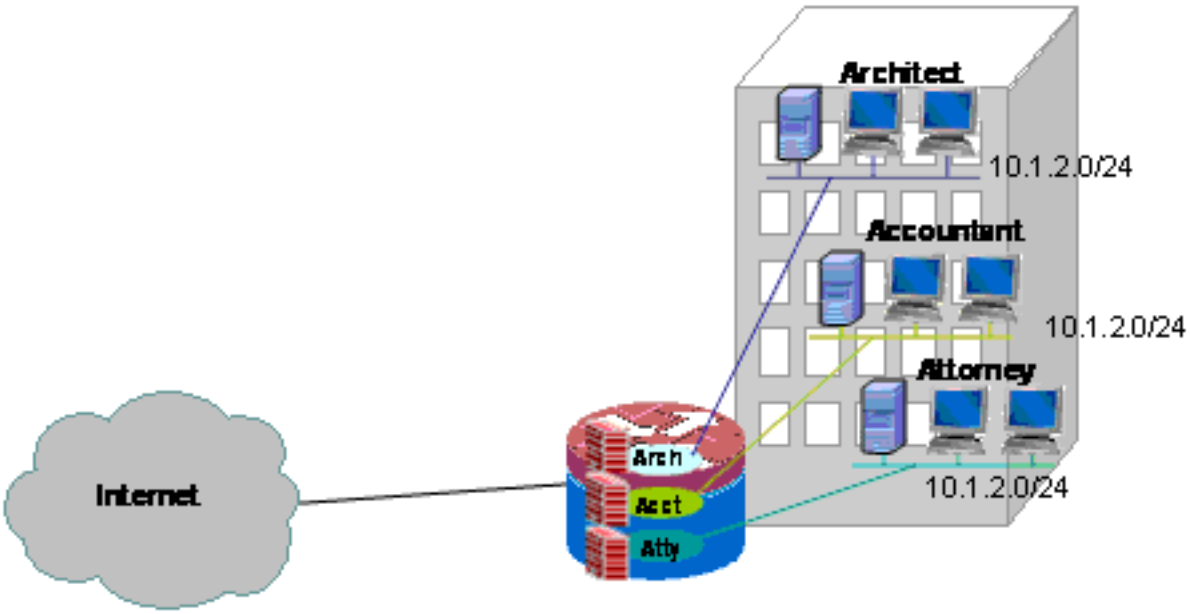
```
router#show ip inspect [ all | config | interfaces | name |
sessions | statistics ] vrf vrf-name
```

Firewall clásico de un solo sitio de VRF múltiple

Los sitios de varios arrendatarios que ofrecen acceso a Internet como servicio de arrendatario pueden utilizar un firewall con detección de VRF para asignar espacio de direcciones superpuestos y una política de firewall de placa de interconexiones para todos los arrendatarios. Los requisitos de espacio enrutable, NAT, acceso remoto y servicio VPN de sitio a sitio pueden

adaptarse a la oferta de servicios personalizados para cada arrendatario, con la ventaja de aprovisionar un VRF para cada cliente.

Esta aplicación utiliza el espacio de direcciones superpuesto para simplificar la administración del espacio de direcciones. Sin embargo, esto puede causar problemas que ofrecen conectividad entre los diversos VRF. Si no se requiere conectividad entre los VRF, se puede aplicar la NAT tradicional interna a externa. El reenvío de puertos NAT se utiliza para exponer servidores en los VRF de arquitecto (arch), contador (acct) y abogado (atty). Las ACL y políticas de firewall deben adaptarse a la actividad NAT.



Configure el firewall clásico y la NAT para una red clásica de un solo sitio de VRF múltiple

Los sitios de varios arrendatarios que ofrecen acceso a Internet como servicio de arrendatario pueden utilizar un firewall con detección de VRF para asignar espacio de direcciones superpuestos y una política de firewall de placa de incandescencia para todos los arrendatarios. Los requisitos de espacio enrutable, NAT, acceso remoto y servicio VPN de sitio a sitio pueden adaptarse a la oferta de servicios personalizados para cada arrendatario, con la ventaja de aprovisionar un VRF para cada cliente.

Existe una política de firewall clásica que define el acceso a las diversas conexiones LAN y WAN y desde ellas:

		Origen de la conexión			
		Internet	Arch	Acct	Atty
Destino de la conexión	Internet	N/A	HTTP, HTTPS FTP, DNS, SMTP	HTTP, HTTPS FTP, DNS, SMTP	HTTP, HTTPS FTP, DNS, SMTP
	Arch	FTP	N/A	Denegar	Denegar
	Acct	SM	Denegar	N/A	Denegar

		TP			
	Atty	HTTP SMTP	Denegar	Denegar	N/A

Los hosts de cada uno de los tres VRF pueden acceder a los servicios HTTP, HTTPS, FTP y DNS en la Internet pública. Se utilizará una lista de control de acceso (ACL 111) para restringir el acceso a los tres VRF (ya que cada VRF permite el acceso a servicios idénticos en Internet), pero se aplicarán diferentes políticas de inspección para proporcionar estadísticas de inspección por VRF. Se pueden utilizar ACL independientes para proporcionar contadores ACL por VRF. Inversamente, los hosts en Internet pueden conectarse a los servicios como se describe en la tabla de políticas anterior, como se define en la ACL 121. El tráfico debe inspeccionarse en ambas direcciones para acomodar el retorno a través de ACL que protegen la conectividad en la dirección opuesta. La configuración NAT se comenta para describir el acceso de reenvío de puertos a los servicios en los VRF.

Firewall clásico de varios arrendatarios y configuración NAT de un 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 clásico y la NAT para una red clásica de un solo sitio de VRF múltiple

La traducción de direcciones de red y la inspección del firewall se verifican para cada VRF con estos comandos:

Examine las rutas en cada VRF con el comando **show ip route vrf [vrf-name]**:

```
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#
```

Verifique la actividad NAT de cada VRF con el comando **show ip nat tra vrf [vrf-name]**:

```
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 de inspección de firewall de cada VRF con el comando **show ip inspect vrf name**:

```
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
```

Firewall de IOS de políticas basadas en zonas de Cisco IOS que reconoce VRF

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

Si agrega Cisco IOS Zone-Based Policy Firewall a configuraciones de routers VRF múltiples, esto tiene poca diferencia con Zone Firewall en aplicaciones que no son VRF. Es decir, la determinación de políticas observa las mismas reglas que observa un firewall de políticas basado en zonas no VRF, excepto por la adición de algunas estipulaciones específicas de VRF múltiples:

- Una zona de seguridad de firewall de políticas basada en zonas puede contener interfaces de una sola zona.
- Un VRF puede contener más de una zona de seguridad.
- El firewall de políticas basado en zona depende del ruteo o la NAT para permitir que el tráfico se mueva entre los VRF. Una política de firewall que inspecciona o pasa el tráfico entre pares de zonas entre VRF no es adecuada para permitir que el tráfico se mueva entre los VRF.

Configuración del Firewall de Políticas Basado en Zonas de Cisco IOS que Reconoce VRF

El firewall de políticas basado en zonas que reconoce VRF utiliza la misma sintaxis de configuración que el firewall de políticas basado en zonas que no reconoce VRF, y asigna interfaces a zonas de seguridad, define políticas de seguridad para el tráfico que se mueve entre zonas y asigna la política de seguridad a las asociaciones de pares de zonas apropiadas.

La configuración específica de VRF no es necesaria. Se aplican los parámetros de configuración globales, a menos que se agregue un mapa de parámetro más específico a la inspección en un mapa de políticas. Incluso en el caso en que se utiliza un mapa de parámetro para aplicar una configuración más específica, el mapa de parámetro no es específico de VRF.

Visualización de la Actividad de Firewall de Política Basada en Zona de Cisco IOS que Reconoce VRF

Los comandos show **show-show-show** de firewall basado en zona que reconoce VRF no son diferentes de los comandos que no reconocen VRF; El firewall de políticas basado en zonas aplica el tráfico que se mueve de las interfaces de una zona de seguridad a las interfaces de otra zona de seguridad, independientemente de las asignaciones VRF de varias interfaces. Por lo tanto, el firewall de políticas basado en zonas que reconoce VRF emplea los mismos comandos **show** para ver la actividad del firewall que utiliza el firewall de políticas basado en zonas en aplicaciones que no son VRF:

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

Casos prácticos de firewall de políticas basado en zonas de Cisco IOS con identificación de VRF

Los casos prácticos de firewall con detección de VRF varían mucho. Estos ejemplos abordan:

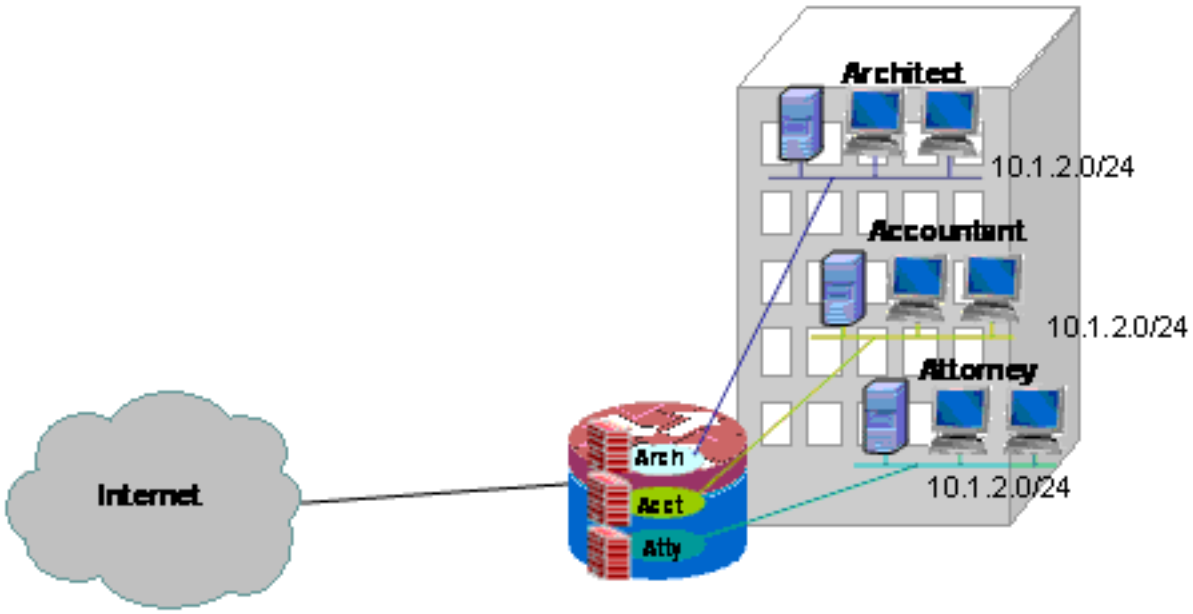
- Una implementación con detección de VRF en un solo sitio, que normalmente se utiliza para instalaciones de varios arrendatarios o redes minoristas
- Una aplicación de sucursal/minorista/teletrabajador donde el tráfico de red privada se mantiene en un VRF separado del tráfico de Internet público. Los usuarios de acceso a Internet están aislados de los usuarios de redes empresariales, y todo el tráfico de red

empresarial se dirige a través de una conexión VPN al sitio HQ para la aplicación de políticas de Internet.

Firewall de políticas basado en zonas de un solo sitio de VRF múltiple

Los sitios de varios arrendatarios que ofrecen acceso a Internet como servicio de arrendatario pueden utilizar un firewall con detección de VRF para asignar espacio de direcciones superpuestos y una política de firewall de placa de incandescencia para todos los arrendatarios. Esta aplicación es típica para varias LAN en un sitio determinado que comparte un router Cisco IOS para el acceso a Internet, o donde a un partner empresarial como un fotoacabado o algún otro servicio se le ofrece una red de datos aislada con conectividad a Internet y una parte específica de la red del propietario de la instalación, sin necesidad de hardware de red adicional o conectividad a Internet. Los requisitos de espacio enrutable, NAT, acceso remoto y servicio VPN de sitio a sitio pueden adaptarse a la oferta de servicios personalizados para cada arrendatario, con la ventaja de aprovisionar un VRF para cada cliente.

Esta aplicación utiliza el espacio de direcciones superpuesto para simplificar la administración del espacio de direcciones. Sin embargo, esto puede causar problemas al ofrecer conectividad entre los diversos VRF. Si no se requiere conectividad entre los VRF, se puede aplicar la NAT tradicional interna a externa. Además, el reenvío de puertos NAT se utiliza para exponer los servidores en los VRF de arquitecto (arch), contador (acct) y abogado (atty). Las ACL y políticas de firewall deben adaptarse a la actividad NAT.



Configuración de NAT y firewall de políticas basado en zonas de un solo sitio de VRF múltiple

Los sitios de varios arrendatarios que ofrecen acceso a Internet como servicio de arrendatario pueden utilizar un firewall con detección de VRF para asignar espacio de direcciones superpuesto y una política de firewall de placa de incandescencia para todos los arrendatarios. Los requisitos de espacio enrutable, NAT, acceso remoto y servicio VPN de sitio a sitio pueden adaptarse a la oferta de servicios personalizados para cada arrendatario, con la ventaja de aprovisionar un VRF para cada cliente.

Existe una política de firewall clásica que define el acceso a las diversas conexiones LAN y WAN y desde ellas:

		Origen de la conexión			
		Internet	Arch	Acct	Atty
Destino de la conexión	Internet	N/A	HTTP, HTTPS FTP, DNS, SMTP	HTTP, HTTPS FTP, DNS, SMTP	HTTP, HTTPS FTP, DNS, SMTP
	Arch	FTP	N/A	Denegar	Denegar
	Acct	SMTP	Denegar	N/A	Denegar
	Atty	HTTP SMTP	Denegar	Denegar	N/A

Los hosts de cada uno de los tres VRF pueden acceder a los servicios HTTP, HTTPS, FTP y DNS en la Internet pública. Se utiliza un mapa de clase (private-public-map) para restringir el acceso a los tres VRF, ya que cada VRF permite el acceso a servicios idénticos en Internet, pero se aplican diferentes mapas de políticas, de modo que se proporcionan estadísticas de inspección por VRF. Por el contrario, los hosts en Internet pueden conectarse a los servicios como se describe en la tabla de políticas anterior, como se define en los mapas de clase individuales y los mapas de políticas para los pares de zonas de Internet a VRF. Se utiliza un policy-map separado para evitar el acceso a los servicios de administración del router en la zona autónoma desde la Internet pública. Se puede aplicar la misma política para evitar el acceso de los VRF privados a la zona automática del router también.

La configuración NAT se comenta para describir el acceso de reenvío de puertos a los servicios en los VRF.

Firewall de políticas basado en zona de varios arrendatarios de un solo sitio y configuración NAT:

```
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 clásico y la NAT para una red clásica de un solo sitio de VRF múltiple

La traducción de direcciones de red y la inspección del firewall se verifican para cada VRF con estos comandos:

Examine las rutas en cada VRF con el comando **show ip route vrf [vrf-name]**:

```
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#
```

Verifique la actividad NAT de cada VRF con el comando show ip nat tra vrf [vrf-name]:

```
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        ---                ---
```

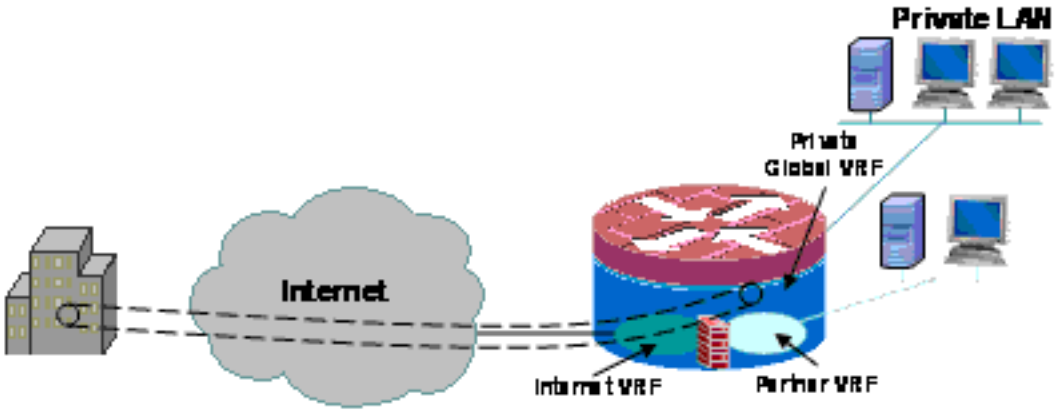
```
tcp 172.16.100.100:1033 10.1.2.3:1033     172.17.111.3:80    172.17.111.3:80
tcp 172.16.100.11:21    10.1.2.2:23       ---                ---
tcp 172.16.100.13:25    10.1.2.4:25       ---                ---
tcp 172.16.100.13:80    10.1.2.5:80       ---                ---
```

Monitoree las estadísticas de inspección del firewall con los comandos **show policy-map type inspect zone-pair**:

```
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
```

Firewall de políticas basado en zonas de un solo sitio de VRF múltiple, conexión a Internet con copia de seguridad en la zona de "Internet", VRF global tiene conexión a HQ

Esta aplicación es adecuada para implementaciones de teletrabajadores, pequeñas ubicaciones minoristas y cualquier otra implementación de red de sitio remoto que requiera la separación de los recursos de red privada del acceso a la red pública. Al aislar la conectividad a Internet y los usuarios de hotspot públicos o domésticos a un VRF *público*, y aplicar una ruta predeterminada en el VRF global que enruta todo el tráfico de red privada a través de túneles VPN, los recursos en el VRF privado, global y el *VRF público* accesible a *Internet* no tienen disponibilidad mutua, por lo que se elimina completamente la amenaza de compromiso de host de red privada por actividad de Internet pública. Además, se puede aprovisionar un VRF adicional para proporcionar un espacio de ruta protegido a otros consumidores que necesiten un espacio de red aislado, como terminales de lotería, cajeros automáticos, terminales de procesamiento de tarjetas de carga u otras aplicaciones. Se pueden aprovisionar varios SSID Wi-Fi para ofrecer acceso tanto a la red privada como a una zona Wi-Fi pública.



Este ejemplo describe la configuración para dos conexiones de Internet de banda ancha, aplicando PAT (sobrecarga NAT) para hosts en VRF *públicos* y *partners* para el acceso a Internet pública, con conectividad a Internet asegurada por la supervisión SLA en las dos conexiones. La red privada (en el VRF global) utiliza una conexión GRE sobre IPsec para mantener la conectividad con HQ (configuración incluida para el router de cabecera VPN) a través de los dos enlaces de banda ancha. En el caso de que una u otra de las conexiones de banda ancha falle, se mantiene la conectividad con la cabecera VPN, lo que permite un acceso ininterrumpido a la red HQ, ya que el extremo local del túnel no está vinculado específicamente a ninguna de las conexiones de Internet.

Existe un firewall de políticas basado en zonas y controla el acceso a y desde la VPN a la red privada, y entre las LAN públicas y de los partners e Internet para permitir el acceso a Internet saliente, pero no hay conexiones a las redes locales desde Internet:

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

La aplicación NAT para el tráfico de zonas Wi-Fi y de redes de partners hace que sea mucho menos probable que se produzcan riesgos desde la Internet pública, pero todavía existe la posibilidad de que usuarios o software malintencionados puedan explotar una sesión NAT activa. La aplicación de la inspección activa (stateful) minimiza las posibilidades de que los hosts locales se vean comprometidos atacando una sesión NAT abierta. Este ejemplo utiliza un 871W, pero la configuración se puede replicar fácilmente con otras plataformas ISR.

Configuración de Multi-VRF Single-Site Zone-Based Policy Firewall, conexión principal a Internet con copia de seguridad, VRF global tiene un escenario de VPN a HQ

Los sitios de varios arrendatarios que ofrecen acceso a Internet como servicio de arrendatario pueden utilizar un firewall con detección de VRF para asignar espacio de direcciones superpuestos y una política de firewall de placa de incandescencia para todos los arrendatarios.

Los requisitos de espacio enrutable, NAT, acceso remoto y servicio VPN de sitio a sitio pueden adaptarse a la oferta de servicios personalizados para cada arrendatario, con la ventaja de aprovisionar 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 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 de políticas basado en zonas de VRF múltiple, la conexión principal a Internet con copia de seguridad, el VRF global tiene un escenario de VPN a HQ

La traducción de direcciones de red y la inspección del firewall se verifican para cada VRF con estos comandos:

Examine las rutas en cada VRF con el comando **show ip route vrf [vrf-name]**:

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

Verifique la actividad NAT de cada VRF con el comando **show ip nat tra vrf [vrf-name]**:

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

Monitoree las estadísticas de inspección del firewall con los comandos **show policy-map type inspect zone-pair**:

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

Conclusión

Cisco IOS VRF-Aware Classic and Zone-Based Policy Firewall ofrece un coste reducido y una carga administrativa para proporcionar conectividad de red con seguridad integrada para varias redes con hardware mínimo. El rendimiento y la escalabilidad se mantienen para varias redes y proporcionan una plataforma eficaz para la infraestructura y los servicios de red sin el aumento de los costes de capital.

Verificación

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

Troubleshoot

Problema

No se puede acceder al servidor Exchange desde la interfaz exterior del router.

Solución

Habilite la Inspección SMTP en el router para solucionar 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 de firewall de políticas basado en zonas
- Uso del firewall de políticas basado en zonas con VPN
- Firewall Cisco IOS con identificación de VRF
- Integración de NAT con MPLS VPN
- Diseño De Extensiones MPLS Para Routers De Borde Del Cliente
- Verificación del funcionamiento de NAT y resolución de problemas básicos de NAT
- Ejemplo de Configuración de Contexto Múltiple PIX/ASA
- Cisco IOS Firewall
- Soporte Técnico y Documentación - Cisco Systems