Exemplo de configuração do aplicativo de firewall virtual baseado em zona e Clássico do Cisco IOS Firewall

Contents

Introduction

Este documento descreve os aspectos técnicos dos recursos de firewall virtual preparado para VRF, o procedimento de configuração e casos de uso para vários cenários de aplicação.

O Cisco IOS® Software Release 12.3(14)T introduziu o Virtual (compatível com VRF) Firewall, estendendo a família de recursos Virtual Routing-Forwarding (VRF) para oferecer inspeção de pacote stateful, firewall transparente, inspeção de aplicativos e filtragem de URL, além de VPN, NAT, QoS e outros recursos compatíveis com VRF. Os cenários de aplicação mais previsíveis aplicarão o NAT com outros recursos. Se o NAT não for necessário, o roteamento pode ser aplicado entre VRFs para fornecer conectividade entre VRF. O Cisco IOS Software oferece recursos com reconhecimento de VRF no Cisco IOS Classic Firewall e no Cisco IOS Zone-Based Policy Firewall, com exemplos de ambos os modelos de configuração fornecidos neste documento. Um foco maior é a configuração do firewall de política baseada em zona.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Suporte de recurso

O firewall com reconhecimento de VRF está disponível em Advanced Security (Segurança avançada), Advanced IP Services (Serviços IP avançados) e em Advanced Enterprise images (Imagens corporativas avançadas), bem como imagens de nomenclatura antiga que transportam a designação *o3*, que indica a integração do conjunto de recursos do Cisco IOS Firewall. Recurso de firewall com reconhecimento de VRF mesclado nas versões principais do software Cisco IOS em 12.4. O Cisco IOS Software Release 12.4(6)T ou posterior é necessário para aplicar o VRF-Aware Zone-Based Policy Firewall. O Cisco IOS Zone-Based Policy Firewall não funciona com failover stateful.

Configuração de VRF

O Cisco IOS Software mantém configurações para o VRF global e para todos os VRFs privados no mesmo arquivo de configuração. Se a configuração do roteador for acessada através da Interface de Linha de Comando, o controle de acesso baseado em funções oferecido no recurso de Exibições de CLI pode ser usado para limitar a capacidade do pessoal operacional e de gerenciamento do roteador. Aplicativos de gerenciamento, como o Cisco Security Manager (CSM), também fornecem controle de acesso baseado em funções para garantir que a equipe operacional esteja restrita ao nível apropriado de capacidade.

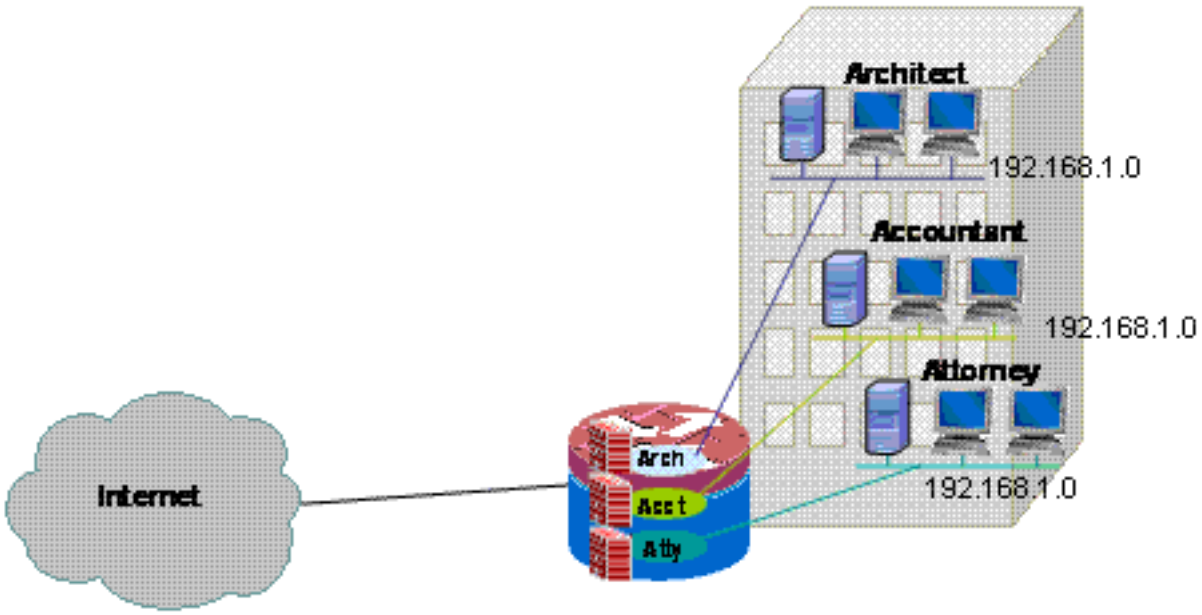
Visão geral de usos comuns para o firewall IOS com reconhecimento de VRF

O firewall com reconhecimento de VRF adiciona inspeção de pacote stateful ao recurso de roteamento/encaminhamento virtual (VRF) do Cisco IOS. A VPN IPsec, a Conversão de Endereço de Rede (NAT - Network Address Translation)/Conversão de Endereço de Porta (PAT - Port Address Translation), o Sistema de Prevenção de Invasão (IPS - Intrusion Prevention System) e outros serviços de segurança do Cisco IOS podem ser combinados com o Firewall com VRF para fornecer um conjunto completo de serviços de segurança em VRFs. Os VRFs oferecem suporte a vários espaços de rota que empregam numeração de endereços IP sobrepostos, de modo que um roteador possa ser dividido em várias instâncias de roteamento discretas para separação de tráfego. O firewall com VRF inclui um rótulo VRF nas informações da sessão para todas as

atividades de inspeção que o roteador está rastreando, para manter a separação entre as informações de estado da conexão que podem ser idênticas em todos os outros aspectos. O firewall com reconhecimento de VRF pode inspecionar entre interfaces dentro de um VRF, bem como entre interfaces em VRFs diferentes, por exemplo, em casos em que o tráfego atravessa os limites de VRF, de modo que a máxima flexibilidade de inspeção de firewall seja obtida para o tráfego intra-VRF e inter-VRF.

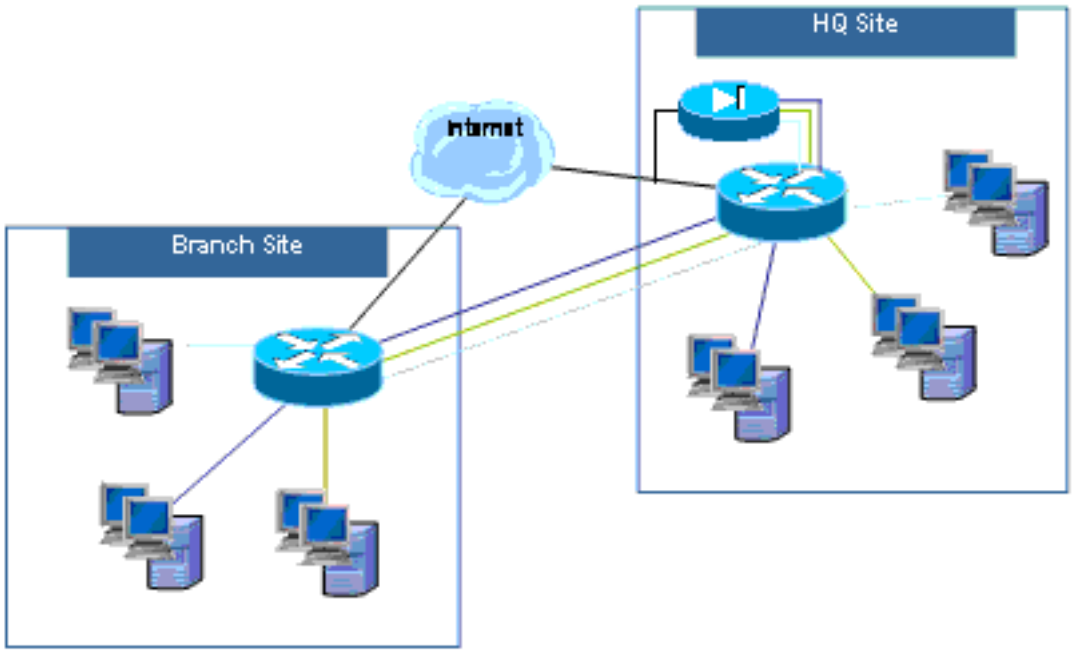
Os aplicativos com reconhecimento de VRF do Cisco IOS Firewall podem ser agrupados em duas categorias básicas:

- Multilocatário, único local: acesso à Internet para vários locatários com espaços de endereço sobrepostos ou espaços de rota segregados em um único local. O firewall stateful é aplicado à conectividade de Internet de cada VRF para reduzir ainda mais a probabilidade de comprometimento por meio de conexões NAT abertas. O encaminhamento de portas pode ser aplicado para permitir a conectividade com servidores em VRFs.



Um exemplo de um aplicativo de local único para vários usuários para o modelo de configuração do VRF-Aware Classic Firewall e o modelo de configuração do VRF-Aware Zone-Based Firewall é fornecido neste documento.

- Multilocatário, vários locais—Vários locatários que compartilham equipamentos em uma rede grande precisam de conectividade entre vários locais pela conexão de VRFs de locatários em diferentes locais através de conexões VPN ou WAN. O acesso à Internet pode ser necessário para cada locatário em um ou mais locais. Para simplificar o gerenciamento, vários departamentos podem agrupar suas redes em um roteador de acesso para cada site, mas vários departamentos exigem segregação de espaço de



endereço. Ex
emplos de configuração para aplicativos multilocatário de vários locais para o modelo de configuração do VRF-Aware Classic Firewall e o modelo de configuração do VRF-Aware Zone-Based Firewall serão fornecidos em uma próxima atualização para este documento.

Configuração não suportada

O firewall com VRF está disponível em imagens do Cisco IOS que suportam VRF CE (VRF Lite) e VPN MPLS. O recurso de firewall é limitado a interfaces não MPLS. Ou seja, se uma interface participará de tráfego rotulado como MPLS, a inspeção de firewall não poderá ser aplicada nessa interface.

Um roteador só poderá inspecionar o tráfego entre VRF se o tráfego tiver que entrar ou sair de um VRF através de uma interface para cruzar com um VRF diferente. Se o tráfego for roteado diretamente para outro VRF, não haverá interface física onde uma política de firewall possa inspecionar o tráfego, de modo que o roteador não possa aplicar a inspeção.

A configuração do VRF Lite só é interoperável com NAT/PAT se `ip nat inside` ou `ip nat outside` estiver configurado em interfaces nas quais NAT/PAT é aplicado para modificar endereços de origem ou de destino ou números de porta para a atividade de rede. O recurso NAT Virtual Interface (NVI), identificado pela adição de uma configuração `ip nat enable` às interfaces que aplicam NAT ou PAT, não é suportado para o aplicativo NAT/PAT entre VRF. Essa falta de interoperabilidade entre VRF Lite e NAT-Virtual Interface é rastreada pela solicitação de aprimoramento CSCek35625.

Configurar

Nesta seção, são explicadas as configurações do Firewall Clássico do Cisco IOS com reconhecimento de VRF e do Firewall de Política Baseado em Zona com Reconhecimento de VRF.

Nota:Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Firewall Clássico com VRF

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

O Cisco IOS VRF-Aware Classic Firewall (anteriormente chamado de CBAC), identificado pelo uso de `inspeção de IP`, está disponível no Cisco IOS Software desde que o Classic Firewall foi estendido para suportar a inspeção com VRF no Cisco IOS Software Release 12.3(14)T.

Configurar o firewall clássico com reconhecimento de VRF do Cisco IOS

O firewall clássico com reconhecimento de VRF usa a mesma sintaxe de configuração do firewall não VRF para a configuração da política de inspeção:

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

Os parâmetros de inspeção podem ser modificados para cada VRF com opções de configuração específicas de VRF:

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

As listas de políticas de inspeção são configuradas globalmente e uma política de inspeção pode ser aplicada às interfaces em vários VRFs.

Cada VRF transporta seu próprio conjunto de parâmetros de inspeção para valores como proteção de negação de serviço (DoS), temporizadores de sessão TCP/UDP/ICMP, configurações de trilha de auditoria, etc. Se uma política de inspeção for usada em vários VRFs, a configuração de parâmetro específico de VRF substitui qualquer configuração global que seja transportada pela política de inspeção. Consulte Cisco IOS Classic Firewall and Intrusion Prevention System Denial-of-Service Protection para obter mais informações sobre como ajustar parâmetros de proteção DoS.

Exibição da atividade de firewall clássico com reconhecimento de VRF do Cisco IOS

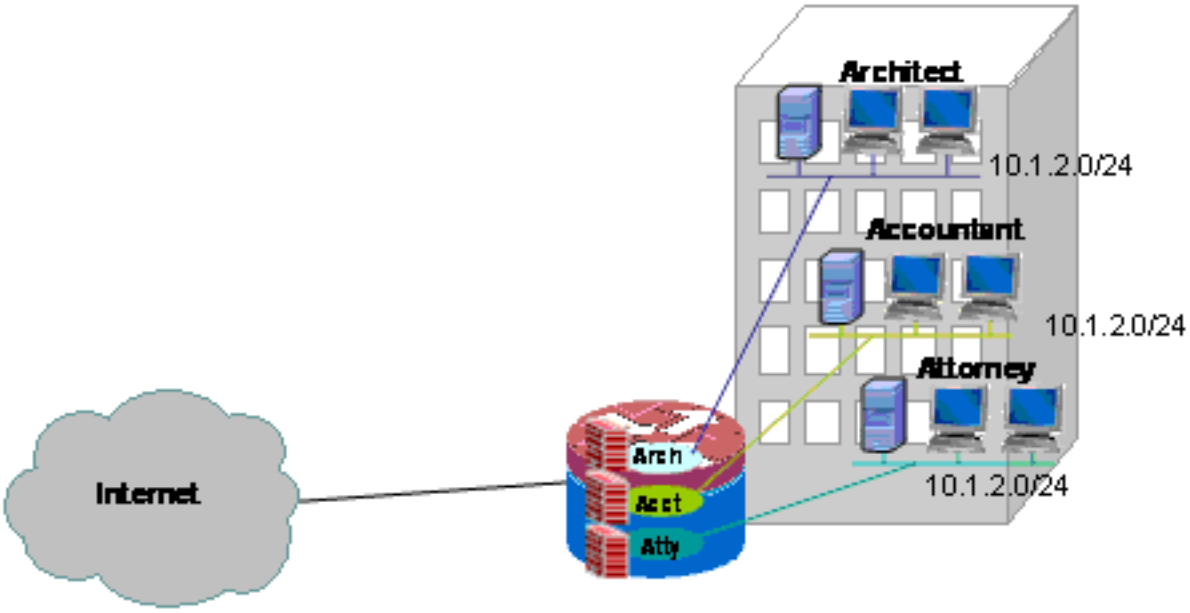
Os comandos "show" do firewall com reconhecimento de VRF diferem dos comandos que não reconhecem VRF, pois os comandos com reconhecimento de VRF exigem que você especifique o VRF no comando "show":

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

Firewall clássico de local único multi-VRF

Sites multilocatário que oferecem acesso à Internet como um serviço de locatário podem usar o firewall com reconhecimento de VRF para alocar espaço de endereço sobreposto e uma política de firewall padrão para todos os locatários. Os requisitos de espaço roteável, NAT, acesso remoto e serviço VPN site a site também podem ser acomodados à oferta de serviços personalizados para cada locatário, com o benefício de fornecer um VRF para cada cliente.

Esse aplicativo usa espaço de endereço sobreposto para simplificar o gerenciamento do espaço de endereço. Mas isso pode causar problemas que oferecem conectividade entre os vários VRFs. Se a conectividade não for necessária entre os VRFs, o NAT tradicional de dentro para fora pode ser aplicado. O encaminhamento de portas NAT é usado para expor servidores nos VRFs de arquiteto (arch), contador (acct) e advogado (atty). As ACLs e políticas de firewall devem acomodar a atividade de NAT.



Configurar o Firewall Clássico e o NAT para uma Rede Clássica de Local Único Multi-VRF

Sites multilocatário que oferecem acesso à Internet como um serviço de locatário podem usar o firewall com reconhecimento de VRF para alocar espaço de endereço sobreposto e uma política de firewall padrão para todos os locatários. Os requisitos de espaço roteável, NAT, acesso remoto e serviço VPN site a site também podem ser acomodados à oferta de serviços personalizados para cada locatário, com o benefício de fornecer um VRF para cada cliente.

Uma política de Firewall Clássico está em vigor, que define o acesso de e para as várias conexões LAN e WAN:

		Origem da conexão			
		Internet	Arco	Conta	Atty
Destino da conexão	Internet	N/A	HTTP,FTP HTTPS, DNS, SMTP	HTTP,FTP HTTPS, DNS, SMTP	HTTP,FTP HTTPS, DNS, SMTP
	Arco	FTP	N/A	Negar	Negar
	Conta	SMTP	Negar	N/A	Negar
	Atty	HTTP SMTP	Negar	Negar	N/A

Os hosts em cada um dos três VRFs podem acessar serviços HTTP, HTTPS, FTP e DNS na Internet pública. Uma lista de controle de acesso (ACL 111) será usada para restringir o acesso para todos os três VRFs (já que cada VRF permite acesso a serviços idênticos na Internet), mas serão aplicadas políticas de inspeção diferentes, de modo a fornecer estatísticas de inspeção por VRF. ACLs separadas podem ser usadas para fornecer contadores de ACL por VRF. Inversamente, os hosts na Internet podem se conectar a serviços conforme descrito na tabela de política anterior, conforme definido pela ACL 121. O tráfego deve ser inspecionado em ambas as direções para acomodar o retorno através das ACLs que protegem a conectividade na direção oposta. A configuração de NAT é comentada para descrever o acesso encaminhado de porta aos serviços em VRFs.

Firewall Clássico Multilocatário de Site Único e Configuração de NAT:

```
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 o firewall clássico e o NAT para uma rede clássica de local único multi-VRF

A Tradução de Endereço de Rede e a inspeção de Firewall são verificadas para cada VRF com estes comandos:

Examine rotas em cada VRF com o 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 a atividade NAT de cada VRF com o 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
```

Monitore as estatísticas de inspeção de firewall de cada VRF com o 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 IOS de política baseada em zona com reconhecimento de VRF do Cisco IOS

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Se você adicionar o Cisco IOS Zone-Based Policy Firewall a configurações de vários roteadores

VRF, isso não terá muita diferença do Zone Firewall em aplicativos não VRF. Ou seja, a determinação da política observa todas as mesmas regras que um firewall de política baseada em zona não-VRF observa, exceto para a adição de algumas condições específicas de vários VRF:

- Uma zona de segurança do firewall de política baseada em zona pode conter interfaces de apenas uma zona.
- Um VRF pode conter mais de uma zona de segurança.
- O firewall de política baseado em zona depende do roteamento ou NAT para permitir que o tráfego se mova entre VRFs. Uma política de firewall que inspeciona ou transmite tráfego entre os pares de zona entre VRF não é adequada para permitir que o tráfego se mova entre VRFs.

Configurar o firewall de política baseado em zona com reconhecimento de VRF do Cisco IOS

O firewall de política baseada em zona com reconhecimento de VRF usa a mesma sintaxe de configuração que o firewall de política baseada em zona sem reconhecimento de VRF e atribui interfaces a zonas de segurança, define políticas de segurança para o tráfego que se move entre zonas e atribui a política de segurança às associações de pares de zonas apropriadas.

A configuração específica de VRF é desnecessária. Os parâmetros de configuração global são aplicados, a menos que um mapa de parâmetros mais específico seja adicionado à inspeção em um mapa de políticas. Mesmo quando um mapa de parâmetros é usado para aplicar uma configuração mais específica, o mapa de parâmetros não é específico do VRF.

Exibição da atividade de firewall de política baseada em zona com reconhecimento de VRF do Cisco IOS

Os comandos **show** do firewall de política baseado em zona com reconhecimento de VRF não são diferentes dos comandos não compatíveis com VRF; O firewall de política baseado em zona aplica o tráfego que se move de interfaces em uma zona de segurança para interfaces em outra zona de segurança, independentemente das atribuições de VRF de várias interfaces. Assim, o firewall de política baseada em zona com reconhecimento de VRF emprega os mesmos comandos **show** para visualizar a atividade do firewall que são usados pelo firewall de política baseada em zona em aplicativos não VRF:

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

Casos de uso do firewall de política baseado em zona com reconhecimento de VRF do Cisco IOS

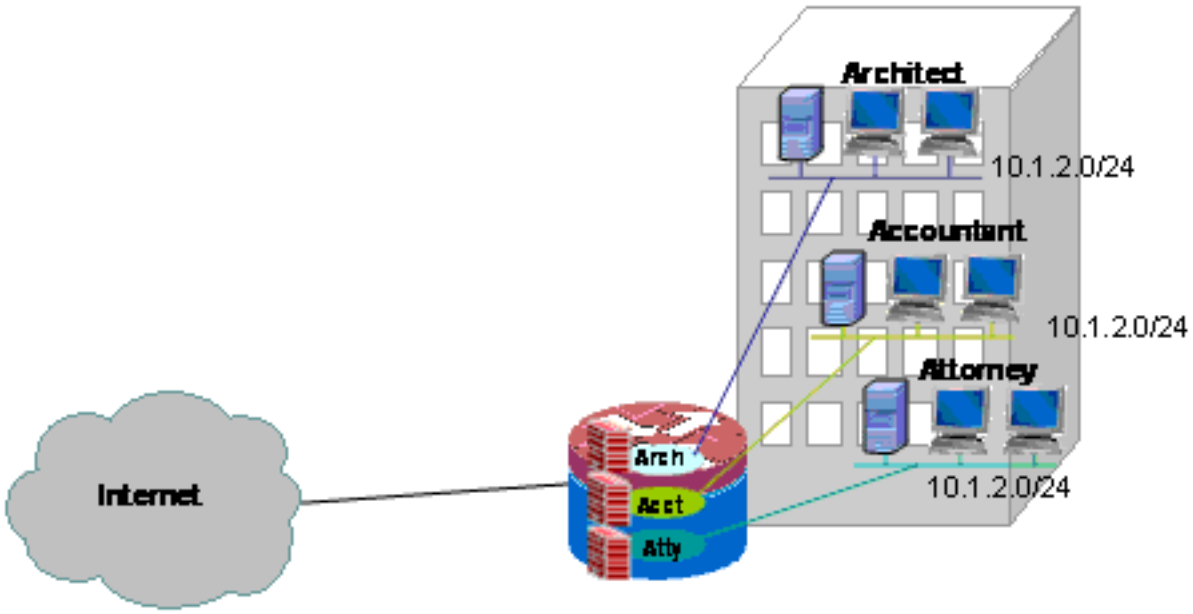
Os casos de uso de firewall com reconhecimento de VRF variam muito. Estes exemplos abordam:

- Implantação com reconhecimento de VRF de um único local, normalmente usada para instalações de vários usuários ou redes de varejo
- Um aplicativo de filial/varejo/telecomutador em que o tráfego de rede privada é mantido em um VRF separado do tráfego de Internet pública. Os usuários de acesso à Internet são isolados de usuários de rede de negócios e todo o tráfego de rede de negócios é direcionado através de uma conexão VPN ao site HQ para aplicação de política de Internet.

Firewall de política com base em zona de local único multi-VRF

Sites multilocatário que oferecem acesso à Internet como um serviço de locatário podem usar o firewall com reconhecimento de VRF para alocar espaço de endereço sobreposto e uma política de firewall padrão para todos os locatários. Esse aplicativo é típico para várias LANs em um determinado site que compartilha um roteador Cisco IOS para acesso à Internet, ou onde um parceiro de negócios, como um fotógrafo ou algum outro serviço, recebe a oferta de uma rede de dados isolada com conectividade com a Internet e alguma parte específica da rede do proprietário do local, sem a necessidade de hardware de rede adicional ou conectividade com a Internet. Os requisitos de espaço roteável, NAT, acesso remoto e serviço VPN site a site também podem ser acomodados à oferta de serviços personalizados para cada locatário, com o benefício de fornecer um VRF para cada cliente.

Esse aplicativo usa espaço de endereço sobreposto para simplificar o gerenciamento do espaço de endereço. Mas isso pode causar problemas ao oferecer conectividade entre os vários VRFs. Se a conectividade não for necessária entre os VRFs, o NAT tradicional de dentro para fora pode ser aplicado. Além disso, o encaminhamento de portas NAT é usado para expor servidores nos VRFs de arquiteto (arch), contador (acct) e advogado (atty). As ACLs e políticas de firewall devem acomodar a atividade de NAT.



Configurar o firewall de política com base em zona de local único e o NAT de vários VRF

Sites multilocatário que oferecem acesso à Internet como um serviço de locatário podem usar o firewall com reconhecimento de VRF para alocar espaço de endereço sobreposto e uma política de firewall padrão para todos os locatários. Os requisitos de espaço roteável, NAT, acesso remoto e serviço VPN site a site também podem ser acomodados à oferta de serviços personalizados para cada locatário, com o benefício de fornecer um VRF para cada cliente.

Uma política de Firewall Clássico está em vigor, que define o acesso de e para as várias conexões LAN e WAN:

		Origem da conexão			
		Internet	Arco	Conta	Atty
Destino da	Internet	N/A	HTTP,FTP HTTPS,	HTTP,FTP HTTPS,	HTTP,FTP

conexão			DNS, SMTP	DNS, SMTP	HTTPS, DNS, SMTP
	Arco	FTP	N/A	Negar	Negar
	Conta	SMTP	Negar	N/A	Negar
	Atty	HTTP SMTP	Negar	Negar	N/A

Os hosts em cada um dos três VRFs podem acessar serviços HTTP, HTTPS, FTP e DNS na Internet pública. Um mapa de classe (private-public-cmap) é usado para restringir o acesso para todos os três VRFs, já que cada VRF permite acesso a serviços idênticos na Internet, mas mapas de políticas diferentes são aplicados, de modo a fornecer estatísticas de inspeção por VRF. Inversamente, os hosts na Internet podem se conectar a serviços conforme descrito na tabela de política anterior, conforme definido por mapas de classe individuais e mapas de política para pares de zonas de Internet para VRF. Um mapa de política separado é usado para impedir o acesso aos serviços de gerenciamento do roteador na zona autônoma da Internet pública. A mesma política pode ser aplicada para impedir o acesso dos VRFs privados à zona automática do roteador também.

A configuração de NAT é comentada para descrever o acesso encaminhado de porta aos serviços em VRFs.

Firewall de política com base em zona para vários usuários de um único local e configuração de 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 o firewall clássico e o NAT para uma rede clássica de local único multi-VRF

A Tradução de Endereço de Rede e a inspeção de Firewall são verificadas para cada VRF com estes comandos:

Examine rotas em cada VRF com o 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 a atividade NAT de cada VRF com o comando show ip nat tra vrf [vrf-name]:

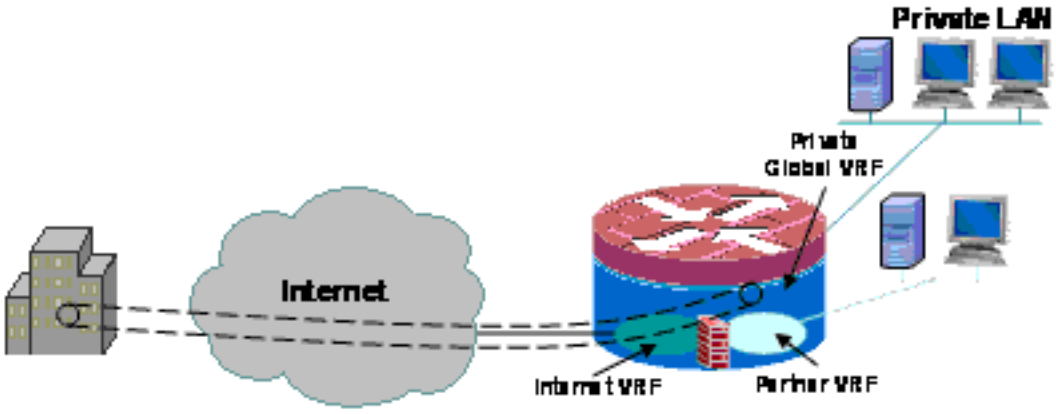
```
stg-2801-L#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 172.16.100.12:25   10.1.2.3:25        ---                ---
tcp 172.16.100.100:1033 10.1.2.3:1033     172.17.111.3:80    172.17.111.3:80
tcp 172.16.100.11:21   10.1.2.2:23        ---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

Monitore estatísticas de inspeção de firewall com os 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 política com base em zona de local único multi-VRF, conexão com a Internet com backup na zona "internet", VRF global tem conexão com o HQ

Esse aplicativo é adequado para implantações de telecomutador, pequenos locais de varejo e qualquer outra implantação de rede de local remoto que exija segregação de recursos de rede privada do acesso à rede pública. Isolando a conectividade com a Internet e os usuários de hotspots domésticos ou públicos em um VRF *público*, e aplicando uma rota padrão no VRF global que roteia todo o tráfego de rede privada através de túneis VPN, os recursos no VRF privado, global e no *VRF* público acessível pela Internet não têm acessibilidade entre si, eliminando assim completamente a ameaça de comprometimento de host de rede privada por atividade da Internet pública. Além disso, um VRF adicional pode ser fornecido para fornecer um espaço de rota protegido para outros consumidores que precisam de um espaço de rede isolado, como terminais de loteria, máquinas ATM, terminais de processamento de cartões de débito ou outros aplicativos. Vários SSIDs Wi-Fi podem ser provisionados para oferecer acesso à rede privada, bem como a um hotspot público.



Este exemplo descreve a configuração para duas conexões de Internet de banda larga, aplicando PAT (sobrecarga de NAT) para hosts em VRFs *públicas* e *parceiras* para acesso à Internet pública, com conectividade de Internet garantida pelo monitoramento de SLA nas duas conexões. A rede privada (no VRF global) usa uma conexão GRE-sobre-IPsec para manter a conectividade com HQ (configuração incluída para o VPN head-end router) sobre os dois links de banda larga. Caso uma ou outra das conexões de banda larga falhe, a conectividade com o head-end da VPN é mantida, o que permite acesso ininterrupto à rede HQ, já que o endpoint local do túnel não está vinculado especificamente a nenhuma das conexões de Internet.

Um firewall de política baseado em zona está instalado e controla o acesso à VPN para a rede privada, e entre as LANs públicas e de parceiros e a Internet para permitir o acesso de saída à Internet, mas nenhuma conexão com as redes locais da Internet:

	Internet	Público	Parceiro	VPN	Privado
Internet	N/A	Negar	Negar	Negar	Negar
Público	HTTP,HTTPS,FTP, DNS	N/A	Negar	Negar	Negar
Parceiro		Negar	N/A		
VPN	Negar	Negar	Negar	N/A	
Privado	Negar	Negar	Negar		N/A

O aplicativo NAT para hotspot e tráfego de rede de parceiros torna muito menos provável o comprometimento da Internet pública, mas ainda existe a possibilidade de que usuários mal-intencionados ou software possam explorar uma sessão NAT ativa. A aplicação de inspeção stateful minimiza as chances de que os hosts locais possam ser comprometidos ao atacar uma sessão NAT aberta. Este exemplo emprega 871W, mas a configuração pode ser facilmente replicada com outras plataformas ISR.

Configurar o firewall de política de local único multi-VRF, conexão de Internet primária com backup, VRF global tem VPN para cenário HQ

Sites multilocatário que oferecem acesso à Internet como um serviço de locatário podem usar o firewall com reconhecimento de VRF para alocar espaço de endereço sobreposto e uma política

de firewall padrão para todos os locatários. Os requisitos de espaço roteável, NAT, acesso remoto e serviço VPN site a site também podem ser acomodados à oferta de serviços personalizados para cada locatário, com o benefício de fornecer um 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 configuração de hub fornece um exemplo da configuração de conectividade 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
```

Verificar o firewall de política de local único multi-VRF, a conexão de Internet principal com backup, o VRF global tem VPN para o cenário HQ

A Tradução de Endereço de Rede e a inspeção de Firewall são verificadas para cada VRF com estes comandos:

Examine rotas em cada VRF com o comando **show ip route vrf [vrf-name]**:

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

Verifique a atividade NAT de cada VRF com o comando **show ip nat tra vrf [vrf-name]:**

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

Monitore estatísticas de inspeção de firewall com os comandos **show policy-map type inspect zone-pair**:

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

Conclusão

O Cisco IOS VRF-Aware Classic e Zone-Based Policy Firewall oferece custo reduzido e carga administrativa para fornecer conectividade de rede com segurança integrada para várias redes com hardware mínimo. O desempenho e a escalabilidade são mantidos para várias redes e fornecem uma plataforma eficaz para infraestrutura e serviços de rede sem o aumento do custo de capital.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Problema

O servidor Exchange não está acessível da interface externa do Roteador.

Solução

Ative a inspeção SMTP no roteador para corrigir esse problema

Configuração de exemplo

```
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
```

Informações Relacionadas

- Guia de design do firewall de política baseado em zona
- Usando o firewall de política baseado em zona com VPN
- Firewall IOS Cisco com reconhecimento de VRF
- Integração de NAT com VPNs MPLS
- Projetando Extensões MPLS Para Roteadores De Borda Do Cliente
- Verificando a Operação de NAT e Troubleshooting Básico de NAT
- Exemplo de configuração de contexto múltiplo PIX/ASA
- Cisco IOS Firewall
- Suporte Técnico e Documentação - Cisco Systems