Exemplo virtual clássico e Zona-baseado do Cisco IOS Firewall do Firewall da configuração do aplicativo

Índice

Introdução

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.

A liberação 12.3(14)T do Cisco IOS ® Software introduziu o Firewall (VRF-ciente) virtual, estendendo a família virtual da característica da Roteamento-transmissão (VRF) para oferecer a inspeção de pacote de informação do stateful, o Firewall transparente, a inspeção de aplicativo, e a Filtragem URL, além do que o VPN existente, o NAT, o QoS, e outras características VRF-cientes. A maioria de encenações previsíveis do aplicativo aplicarão o NAT com outros recursos. Se o NAT não é exigido, distribuir pode ser aplicada entre VRF fornecer a Conectividade inter-VRF. As capacidades VRF-cientes das ofertas do Cisco IOS Software no Firewall do Cisco IOS e no Cisco IOS clássicos Zona-basearam o Firewall da política, com exemplos de ambos os modelos da configuração fornecidos neste documento. Um foco maior é colocado na configuração de firewall da política Zona-Basear.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Convenções

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

Informações de Apoio

Suporte de recurso

O Firewall VRF-ciente está disponível na segurança avançada, Serviços IP avançados, e imagens de empreendimento avançadas, assim como imagens da legado-nomenclatura que levam a designação *o3*, que indica a integração do Cisco IOS Firewall Feature Set. Capacidade VRF-ciente do Firewall fundida em versões de linha principal do Cisco IOS Software em 12.4. O Cisco IOS Software Release 12.4(6)T ou Mais Recente é exigido para aplicar o Firewall Zona-baseado VRF-ciente da política. O Firewall Zona-baseado Cisco IOS da política não trabalha com comutação classificada.

Configuração de VRF

O Cisco IOS Software mantém configurações para VRF global e todos os VRF privados no arquivo de mesma configuração. Se a configuração de roteador é alcançada através da interface de linha de comando, o controle de acesso papel-baseado oferecido na característica das opiniões CLI pode ser usado para limitar a capacidade de roteador operacional e de equipes de gerenciamento. Os aplicativos de gerenciamento tais como o Cisco Security Manager (CS) igualmente fornecem o controle de acesso papel-baseado para assegurar que os pessoais operacionais estão restringidos ao nível apropriado da capacidade.

Vista geral dos usos comuns para o firewall de IOS VRF-ciente

O Firewall VRF-ciente adiciona a inspeção de pacote de informação do stateful à capacidade do roteamento virtual/transmissão do Cisco IOS (VRF). A tradução de endereços da /porta do IPSec VPN, do Network Address Translation (NAT) (PANCADINHA), o Intrusion Prevention System (IPS) e outros serviços de Cisco IOS Security podem ser combinados com o Firewall VRF-ciente para fornecer um conjunto completo de Serviços de segurança nos VRF. Os VRF fornecem o apoio para os espaços da rota múltipla que empregam a numeração de sobreposição do endereço IP de Um ou Mais Servidores Cisco ICM NT, assim que um roteador pode ser dividido em exemplos discretos múltiplos do roteamento para a separação do tráfego. O Firewall VRF-ciente inclui uma etiqueta VRF na informação de sessão para toda a atividade da inspeção que o roteador está seguindo, para manter a separação entre a informação de estado de conexão que pode ser idêntica em cada outro respeito. O Firewall VRF-ciente pode inspecionar inspeciona entre relações dentro de um VRF, assim como entre relações nos VRF que diferem, por exemplo

nos casos onde o tráfego cruza limites VRF, de modo que a flexibilidade máxima da inspeção do Firewall seja realizada para o tráfego intra-VRF e inter-VRF.

Os aplicativos VRF-cientes do Cisco IOS Firewall podem ser agrupados em duas categorias de básica:

- Multi-inquilino, único-local — Acesso ao Internet para inquilinos múltiplos com os espaços de endereço sobreposto ou espaços segregados da rota em uns únicos locais. O firewall stateful é aplicado à conectividade de Internet de cada VRF para reduzir mais a probabilidade do acordo através das conexões NAT abertas. a Porta-transmissão pode ser aplicada para permitir a Conectividade aos server nos VRF.Um exemplo de um pedido do único-local do multi-inquilino para o modelo clássico VRF-ciente da configuração de firewall e o modelo Zona-baseado VRF-ciente da configuração de firewall é fornecido neste documento.
- Multi-inquilino, multi-local — Inquilinos múltiplos que compartilham do equipamento em uma Conectividade da necessidade da rede grande entre sites múltiplo pela conexão dos VRF dos inquilinos em locais diferentes com o VPN ou conexões de WAN. O acesso ao Internet pode ser exigido para cada inquilino em uns ou vários locais. A fim simplificar o Gerenciamento, diversos departamentos podem desmoronar suas redes em um roteador de acesso para cada local, mas os vários departamentos exigem a segregação do espaço de endereços.Os exemplos de configuração para pedidos do multi-local do multi-inquilino para o modelo clássico VRF-ciente da configuração de firewall e o modelo Zona-baseado VRF-ciente da configuração de firewall serão fornecidos em uma atualização próxima a este documento.

Configuração não suportada

O Firewall VRF-ciente está disponível nas imagens IOS Cisco que apoiam Multi-VRF CE (VRF Lite) e MPLS VPN. A capacidade do Firewall é limitada às relações NON-MPLS. Isto é, se uma relação participará no tráfego MPLS-etiquetado, a inspeção do Firewall não pode ser aplicada nessa relação.

Um roteador pode somente inspecionar o tráfego inter-VRF se o tráfego deve incorporar ou deixar um VRF através de uma relação para se cruzar a um VRF diferente. Se o tráfego é distribuído diretamente a um outro VRF, não há nenhuma interface física onde uma política de firewall pode inspecionar o tráfego, assim que o roteador é incapaz de aplicar a inspeção.

A configuração VRF Lite é interoperáveis com NAT/PAT somente se o `interior nat IP` ou a `parte externa nat IP` são configurados nas relações onde o NAT/PAT está aplicado para alterar endereços de origem ou de destino ou números de porta para a atividade de rede. A característica da interface virtual NAT (NVI), identificada pela adição de um `IP nat permite a` configuração às relações que aplicam o NAT ou a PANCADINHA, não é apoiada para o aplicativo inter-VRF NAT/PAT. Esta falta da Interoperabilidade entre VRF Lite e relação NAT-virtual é seguida pela requisição de aprimoramento CSCek35625.

Configurar

Nesta seção, o Firewall do Cisco IOS VRF-ciente e as configurações de firewall Zona-baseadas VRF-cientes clássicos da política são explicados.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações

sobre os comandos usados nesta seção.

Firewall VRF-ciente do clássico do Cisco IOS

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

O Firewall clássico VRF-ciente do Cisco IOS (chamado anteriormente CBAC), que é identificado pelo uso do `IP inspeciona`, esteve disponível no Cisco IOS Software desde que o Firewall clássico foi estendido para apoiar a inspeção VRF-ciente no Cisco IOS Software Release 12.3(14)T.

Configurar o Firewall clássico VRF-ciente do Cisco IOS

O Firewall clássico VRF-ciente usa a sintaxe da mesma configuração como o Firewall NON-VRF para a configuração da política da inspeção:

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

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

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

As lista da política da inspeção são configuradas globalmente, e uma política da inspeção pode ser aplicada às relações em VRF múltiplos.

Cada VRF leva seu próprio grupo de parâmetros de inspeção para valores tais como a proteção da recusa de serviço (DoS), os temporizadores de sessão TCP/UDP/ICMP, os ajustes dos circuitos de auditoria, etc. Se uma política da inspeção é usada em VRF múltiplos, a configuração de parâmetro VRF-específica substitui toda a configuração global que for levada pela política da inspeção. Refira o Firewall do Cisco IOS e a proteção clássicos da recusa de serviço do sistema da prevenção de intrusão para obter mais informações sobre de como ajustar parâmetros da proteção de DOS.

Vendo a atividade clássica VRF-ciente do Firewall do Cisco IOS

Os comandos " show " VRF-cientes do Firewall diferem dos comandos NON-VRF-cientes, porque os comandos VRF-cientes exigem que você especifica o VRF no comando " show ":

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

Firewall do clássico do Único-local Multi-VRF

locais do Multi-inquilino que oferecem o acesso ao Internet enquanto um serviço do inquilino pode usar o Firewall VRF-ciente a fim atribuir o espaço de endereço sobreposto e uma política de firewall do texto constante para todos os inquilinos. As exigências para o espaço do roteável, o NAT, e o acesso remoto e o serviço do VPN de Site-para-Site podem ser acomodadas também à oferta de serviços personalizados para cada inquilino, com o benefício do abastecimento um VRF para cada cliente.

Este aplicativo usa o espaço de endereço sobreposto a fim simplificar o Gerenciamento de espaço de endereços. Mas, isto pode causar os problemas que oferecem a Conectividade entre os vários VRF. Se a Conectividade não é exigida entre os VRF, a dentro-à-parte externa tradicional NAT pode ser aplicada. A porta-transmissão NAT é usada para expor server no

arquiteto (arco), no contador (acct), e no advogado VRF (atty). O Firewall ACL e as políticas devem acomodar a atividade NAT.

Configurar o Firewall e o NAT clássicos para uma rede do clássico do Único-local Multi-VRF

locais do Multi-inquilino que oferecem o acesso ao Internet enquanto um serviço do inquilino pode usar o Firewall VRF-ciente para atribuir o espaço de endereço sobreposto e uma política de firewall do texto constante para todos os inquilinos. As exigências para o espaço do roteável, o NAT, e o acesso remoto e o serviço do VPN de Site-para-Site podem ser acomodadas também à oferta de serviços personalizados para cada inquilino, com o benefício do abastecimento um VRF para cada cliente.

Uma política de firewall clássica é no lugar, que defina o acesso a e do vários LAN e conexões de WAN:

		Origem da conexão			
		Internet	Arco	Acct	Atty
Destino da conexão	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	Negue	Negue
	Acct	SMTP	Negue	N/A	Negue
	Atty	HTTP S TP	Negue	Negue	N/A

Os anfitriões em cada um dos três VRF podem alcançar serviços HTTP, HTTPS, FTP, e DNS nos Internet públicas. Uma lista de controle de acesso (ACL 111) será usada para restringir o acesso para todos os três VRF (desde que cada VRF permite o acesso aos serviços idênticos no Internet), mas políticas diferentes da inspeção será aplicada, para fornecer estatísticas da inspeção por-VRF. Os ACL separados podem ser usados para fornecer contadores ACL pelo VRF. Inversamente, os anfitriões no Internet podem conectar aos serviços como descrito na tabela precedente da política, como definido por ACL 121. O tráfego deve ser inspecionado nos ambos sentidos para acomodar o retorno com os ACL que protegem a Conectividade na direção oposta. A configuração de NAT é comentada para descrever o acesso porta-enviado aos serviços nos VRF.

Firewall e configuração de NAT clássicos do Multi-inquilino do Único-local:

```
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 e o NAT clássicos para uma rede do clássico do Único-local Multi-VRF

A inspeção da tradução de endereço de rede e do Firewall é verificada para cada VRF com estes comandos:

Examine rotas em cada VRF com o comando do **[vrf-name] do vrf da rota da mostra IP**:

```
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 **nat do [vrf-name] do vrf do tra da mostra IP**:

```
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 da inspeção do Firewall de cada VRF com a **mostra IP inspecionam o** comando do **nome 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
```

O Cisco IOS VRF-ciente Zona-baseou o firewall de IOS da política

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

Se você adiciona o Firewall Zona-baseado Cisco IOS da política às configurações de roteador multi-VRF, este carrega pouca diferença do Firewall da zona nos aplicativos NON-VRF. Isto é, a determinação da política observa todas as mesmas regras que um Firewall Zona-baseado NON-VRF da política observa, salvo a adição de algumas estipulações multi-VRF-específicas:

- Uma zona de Segurança Zona-baseada do Firewall da política pode conter relações de somente uma zona.
- Um VRF pode conter mais de uma zona de Segurança.
- O Firewall Zona-baseado da política é dependente do roteamento ou do NAT a fim permitir que o tráfego mova-se entre VRF. Uma política de firewall que inspecione ou as passagens traficam entre os Zona-pares inter-VRF não são adequada permitir o tráfego mover-se entre VRF.

Configurar Cisco IOS VRF-ciente o Firewall Zona-baseado da política

O Firewall Zona-baseado VRF-ciente da política usa a sintaxe da mesma configuração como o Firewall Zona-baseado NON-VRF-ciente da política, e atribui relações às zonas de Segurança, define políticas de segurança para o tráfego que se move entre zonas, e atribui a política de segurança às associações apropriadas dos zona-pares.

a configuração VRF-específica é desnecessária. Os parâmetros de configuração globais são aplicados, a menos que um parâmetro-mapa mais específico for adicionado à inspeção em um mapa de política. Mesmo no caso onde um parâmetro-mapa é usado para aplicar uma configuração mais específica, o parâmetro-mapa não é VRF-específico.

Ver o Cisco IOS VRF-ciente Zona-baseou a atividade do Firewall da política

Os comandos show Zona-baseados VRF-cientes do Firewall da política são não diferentes dos comandos NON-VRF-cientes; O Firewall Zona-baseado da política aplica o tráfego que se move das relações em uma zona de Segurança para relações em uma outra zona de Segurança, apesar das atribuições VRF de várias relações. Assim, o Firewall Zona-baseado VRF-ciente da política emprega os mesmos **comandos show** a fim ver a atividade do Firewall que são usados pelo Firewall da política Zona-Basear nos aplicativos NON-VRF:

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

Cisco IOS VRF-ciente o Firewall Zona-baseado da política usa casos

os casos VRF-cientes do uso do Firewall variam extensamente. Endereço destes exemplos:

- Um desenvolvimento VRF-ciente do único-local, usado tipicamente para facilidades do multi-inquilino ou redes varejos
- Um aplicativo do escritório filial/retalho/telecommuter onde o tráfego de rede privada seja mantido em um VRF separado do tráfego do público-Internet. Os usuários do acesso ao Internet são isolados dos usuários da rede de negócio, e todo o tráfego de rede de negócio é dirigido sobre uma conexão de VPN ao local QG para o aplicativo da política de internet.

O Único-local Multi-VRF Zona-baseou o Firewall da política

locais do Multi-inquilino que oferecem o acesso ao Internet enquanto um serviço do inquilino pode usar o Firewall VRF-ciente para atribuir o espaço de endereço sobreposto e uma política de firewall do texto constante para todos os inquilinos. Este aplicativo é típico para as LAN múltiplas em um local dado que compartilhe de um roteador do Cisco IOS para o acesso ao Internet, ou em onde um parceiro de negócios tal como um photofinisher ou algum outro serviço é oferecido uma rede de dados isolada com Conectividade ao Internet e a algum específico parte da rede do proprietário dos locais, sem a exigência do hardware de rede adicional ou da conectividade de Internet. As exigências para o espaço do roteável, o NAT, e o acesso remoto e o serviço do VPN de Site-para-Site podem ser acomodadas também à oferta de serviços personalizados para cada inquilino, com o benefício do abastecimento um VRF para cada cliente.

Este aplicativo usa o espaço de endereço sobreposto a fim simplificar o Gerenciamento de espaço de endereços. Mas, isto pode causar os problemas que oferecem a Conectividade entre os vários VRF. Se a Conectividade não é exigida entre os VRF, a dentro-à-parte externa tradicional NAT pode ser aplicada. Adicionalmente, a porta-transmissão NAT é usada para expor server no arquiteto (arco), no contador (acct), e no advogado VRF (atty). O Firewall ACL e as políticas devem acomodar a atividade NAT.

Configurar o Firewall da política Multi-VRF e o NAT Zona-baseados Único-local

o Multi-inquilino situa o acesso ao Internet de oferecimento enquanto um serviço do inquilino pode usar o Firewall VRF-ciente para atribuir o espaço de endereço sobreposto e uma política de firewall do texto constante para todos os inquilinos. As exigências para o espaço do roteável, o NAT, e o acesso remoto e o serviço do VPN de Site-para-Site podem ser acomodadas também à oferta de serviços personalizados para cada inquilino, com o benefício do abastecimento um VRF para cada cliente.

Uma política de firewall clássica é no lugar, que defina o acesso a e do vários LAN e conexões de WAN:

		Origem da conexão			
		Internet	Arco	Acct	Atty
Destino da conexão	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	Negue	Negue
	Acct	SMTP	Negue	N/A	Negue
	Atty	HTTPS TP	Negue	Negue	N/A

Os anfitriões em cada um dos três VRF podem alcançar serviços HTTP, HTTPS, FTP, e DNS nos Internet públicas. Um mapa de classe (privado-público-cmap) é usado para restringir o acesso para todos os três VRF, desde que cada VRF permite o acesso aos serviços idênticos no Internet, mas polic-mapas diferentes é aplicado, para fornecer estatísticas da inspeção por-VRF. Inversamente, os anfitriões no Internet podem conectar aos serviços como descrito na tabela precedente da política, como definido por mapas de classe e por política-mapas individuais para os zona-pares Internet-à-VRF. Um mapa de política separado é usado para impedir o acesso aos serviços da gerência do roteador na auto-zona do Internet público. A mesma política pode ser aplicada para impedir também o acesso dos VRF privados à auto-zona do roteador.

A configuração de NAT é comentada para descrever o acesso porta-enviado aos serviços nos VRF.

O Multi-inquilino do Único-local Zona-baseou o Firewall e a configuração de NAT da política:

```
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 e o NAT clássicos para uma rede do clássico do Único-local Multi-VRF

A inspeção da tradução de endereço de rede e do Firewall é verificada para cada VRF com estes comandos:

Examine rotas em cada VRF com o comando do **[vrf-name] do vrf da rota da mostra IP**:

```
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 nat do [vrf-name] do vrf do tra da mostra IP:

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

As estatísticas da inspeção do Firewall do monitor com o **tipo do mapa de política da mostra inspecionam** comandos dos 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
```

O Firewall Zona-baseado Único-local da política Multi-VRF, conexão com o Internet com backup na zona do “Internet”, VRF global tem a conexão ao QG

Este aplicativo é poço - serido às disposições do telecommuter, aos lugar varejos pequenos, e ao todo o outro desenvolvimento de rede de site remoto que exigir a segregação de recursos de rede privada do acesso de rede pública. Isolando usuários do ponto quente da conectividade de

Internet e da HOME ou do público a um *público* VRF, e aplicando uma rota padrão no VRF global que distribui todo o tráfego de rede privada através dos túneis VPN, os recursos no VRF privado, global e no *público Internet*-alcançável VRF nenhuma alcançabilidade entre si, assim removeram completamente a ameaça do acordo do host da privado-rede pela atividade do público-Internet. Além disso, um VRF adicional pode ser fornecida fornecer um espaço protegido da rota para outros consumidores que precisam um espaço de rede isolado, tal como terminais da loteria, máquinas ATM, cartão de carga que processam terminais, ou outros aplicativos. O Wi-fi múltiplo SSID pode ser fornecida oferecer a acesso a ambos a rede privada, assim como a um ponto quente público.

Este exemplo descreve a configuração para duas conexões de Internet de banda larga, aplicando a PANCADINHA (sobrecarga NAT) para anfitriões no *público* e no *sócio* VRF para o acesso ao Internet público, com a conectividade de Internet assegurada pela monitoração SLA nas duas conexões. A rede privada (no VRF global) usa uma conexão do GRE-sobre-IPsec para manter a Conectividade a QG (configuração incluída para o roteador de extremidade principal VPN) sobre os dois links de faixa larga. Caso uma ou a outro das conexões de faixa larga falhar, a Conectividade à extremidade principal VPN está mantida, que permite o acesso ininterrupto à rede QG, desde que o ponto final local do túnel não é amarrado especificamente a tampouco das conexões com o Internet.

Um Firewall zona-baseado da política é no lugar e controla o acesso a e do VPN à rede privada, e entre o público e o sócio LAN e o Internet a fim não permitir dentro o acesso à internet de partida, mas a nenhuma conexão às redes local do Internet:

	Internet	Público	Sócio	VPN	Privado
Internet	N/A	Negue	Negue	Negue	Negue
Público	HTTP, HTTPS, FTP, DNS	N/A	Negue	Negue	Negue
Sócio		Negue	N/A		
VPN	Negue	Negue	Negue	N/A	
Privado	Negue	Negue	Negue		N/A

O pedido NAT para o tráfego do ponto quente e da sócio-rede faz o acordo do Internet público muito menos provavelmente, mas a possibilidade ainda existe que os usuários ou o software malicioso podem explorar uma sessão NAT ativa. O aplicativo da inspeção stateful minimiza possibilidades que os host locais podem ser comprometidos atacando uma sessão NAT aberta. Este exemplo emprega um 871W, mas a configuração pode facilmente ser replicated com outras plataformas ISR.

Configurar o Firewall Zona-baseado Único-local da política Multi-VRF, conexão com o Internet preliminar com backup, VRF global tem o VPN à encenação QG

locais do Multi-inquilino que oferecem o acesso ao Internet enquanto um serviço do inquilino pode usar o Firewall VRF-ciente para atribuir o espaço de endereço sobreposto e uma política de firewall do texto constante para todos os inquilinos. As exigências para o espaço do roteável, o NAT, e o acesso remoto e o serviço do VPN de Site-para-Site podem ser acomodadas também à oferta de serviços personalizados para cada inquilino, com o benefício do abastecimento 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 do hub fornece um exemplo da configuração da conectividade de 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 o Firewall Zona-baseado Único-local da política Multi-VRF, conexão com o Internet preliminar com backup, VRF global tem o VPN à encenação QG

A inspeção da tradução de endereço de rede e do Firewall é verificada para cada VRF com estes comandos:

Examine rotas em cada VRF com o comando do **[vrf-name] do vrf da rota da mostra IP**:

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

Verifique a atividade NAT de cada VRF com o comando **nat do [vrf-name] do vrf do tra da mostra IP**:

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

As estatísticas da inspeção do Firewall do monitor com o **tipo do mapa de política da mostra inspecionam** comandos dos zona-**pares**:

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

Conclusão

Custo VRF-ciente e sobrecarga administrativa reduzidos ofertas clássicos do Cisco IOS e Zona-baseados do Firewall da política para fornecer a conectividade de rede a segurança integrada para redes múltiplas com hardware mínimo. O desempenho e a escalabilidade são mantidos para redes múltiplas e proporcionam uma plataforma eficaz para a infraestrutura de rede e serviços sem o aumento do custo principal.

Verificar

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

Troubleshooting

Problema

O server de câmbio não é acessível da interface externa do roteador.

Solução

Permita a inspeção de SMTP no roteador a fim fixar esta edição

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 Zona-baseado do Firewall da política
- Usando o Firewall Zona-baseado da política com VPN
- Cisco IOS Firewall ciente VRF
- NAT de integração com MPLS VPNs
- Projetando Ramais MPLS para roteadores de ponta do cliente
- Verificando a Operação de NAT e Troubleshooting Básico de NAT
- Exemplo de configuração do contexto múltiplo PIX/ASA
- Cisco IOS Firewall
- Suporte Técnico e Documentação - Cisco Systems