Cisco IOS-configuratievoorbeeld voor cloudfirewall en Zone-gebaseerde virtuele firewall

Inhoud

Inleiding

Dit document beschrijft de technische achtergrond van de VRF-bewuste virtuele firewallfuncties, configuratieprocedure en gebruikscases voor verschillende toepassingsscenario's.

Cisco IOS-softwarerelease 12.3(14)T geïntroduceerde virtuele (VRF-bewuste) firewall, die de Virtual Routing-Forwarding (VRF)-familie uitbreidt om stateful Packet inspection, Transparante firewall, Toepassingsinspectie en URL-filtering aan te bieden, naast bestaande VPN, NAT, QoS en andere VRF-bewuste functies. De meeste voorzienbare toepassingsscenario's zullen NAT met andere kenmerken toepassen. Als NAT niet vereist is, kan de routing tussen VRF's worden toegepast om interVRF-connectiviteit te bieden. Cisco IOS-software biedt mogelijkheden die zich bewust zijn van VRF in zowel Cisco IOS Classic Firewall als Cisco IOS Zone-Based Policy Firewall, met voorbeelden van beide configuratiemodellen in dit document. Er wordt meer nadruk gelegd op de configuratie van de Zone-Based Policy Firewall.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

Ondersteuning voor functies

VRF-bewuste firewall is beschikbaar in geavanceerde security, geavanceerde IP-services en geavanceerde ondernemingsafbeeldingen, evenals legacy-nomenclatuur-afbeeldingen die de *o3*-aanwijzing dragen, wat de integratie van de Cisco IOS-firewallfunctieset aangeeft. VRF-bewuste firewallmogelijkheden die in Cisco IOS-softwarereleases van de hoofdlijn worden samengevoegd in 12.4. Cisco IOS-softwarerelease 12.4(6)T of later moet worden toegepast VRF-Aware Zone-Based Policy Firewall. De Cisco IOS Zone-Based Policy Firewall werkt niet met stateful failover.

VRF-configuratie

Cisco IOS-software onderhoudt configuraties voor de wereldwijde VRF en alle particuliere VRF's in hetzelfde configuratiebestand. Als de routerconfiguratie door de Opdracht-Lijn interface wordt benaderd, kan de op rol gebaseerde toegangscontrole die in de CLI-weergave wordt aangeboden worden gebruikt om de capaciteit van router operationeel en beheerpersoneel te beperken. Beheertoepassingen zoals Cisco Security Manager (CSM) bieden ook rolgebaseerde toegangscontrole om te waarborgen dat het operationele personeel wordt beperkt tot het juiste niveau van capaciteit.

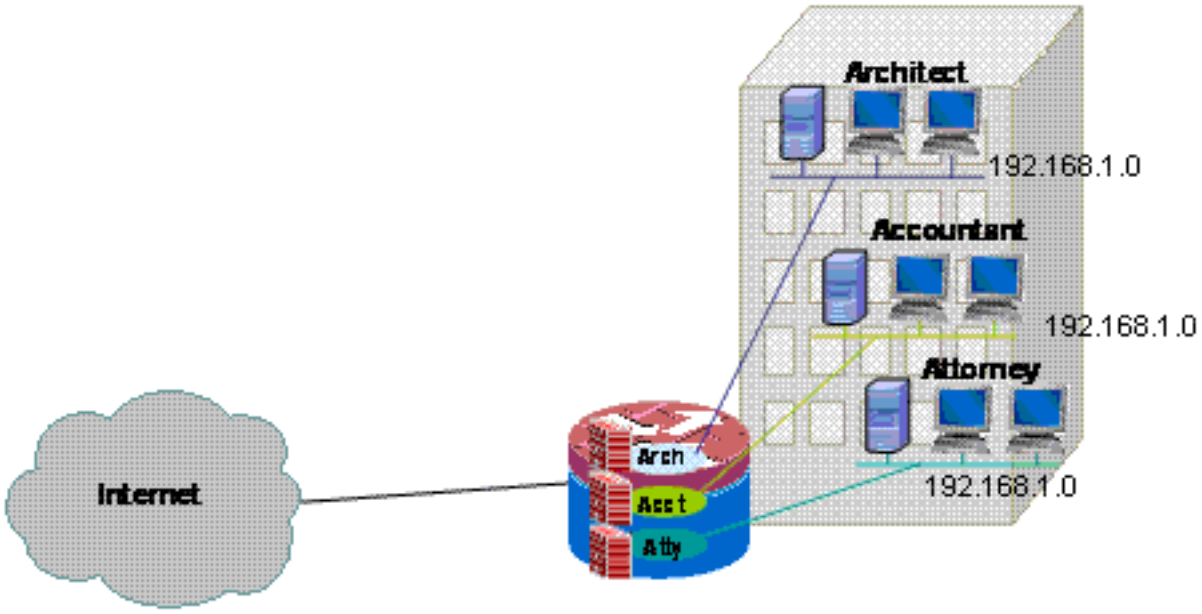
Overzicht van gemeenschappelijke toepassingen voor VRF-bewuste IOS-firewall

VRF-bewuste firewall voegt stateful pakketinspectie toe aan de Cisco IOS Virtual Routing/Forwarding (VRF)-mogelijkheid. IPsec VPN, Network Address Translation (NAT)/Port Address Translation (PAT), Inbraakpreventiesysteem (IPS) en andere Cisco IOS security services kunnen worden gecombineerd met VRF-bewuste firewall om een volledige reeks beveiligingsservices in VRF's te leveren. VRFs bieden ondersteuning voor meerdere routekaarten die overlappende IP-adresnummering gebruiken, zodat een router in meerdere afzonderlijke routinginstanties kan worden verdeeld voor verkeersscheiding. De VRF-bewuste firewall omvat een etiket VRF in sessieinformatie voor alle inspectieactiviteit die de router volgt, om scheiding tussen de informatie van de verbindingsstaat te handhaven die in elk ander respect identiek kan zijn. VRF-bewuste firewall kan inspecties tussen interfaces binnen één VRF, zowel tussen interfaces in VRFs die verschillen, bijvoorbeeld in gevallen waar het verkeer VRF grenzen overschrijdt, zodat de maximum flexibiliteit van de firewallinspectie voor zowel intra-VRF als

interVRF verkeer wordt gerealiseerd.

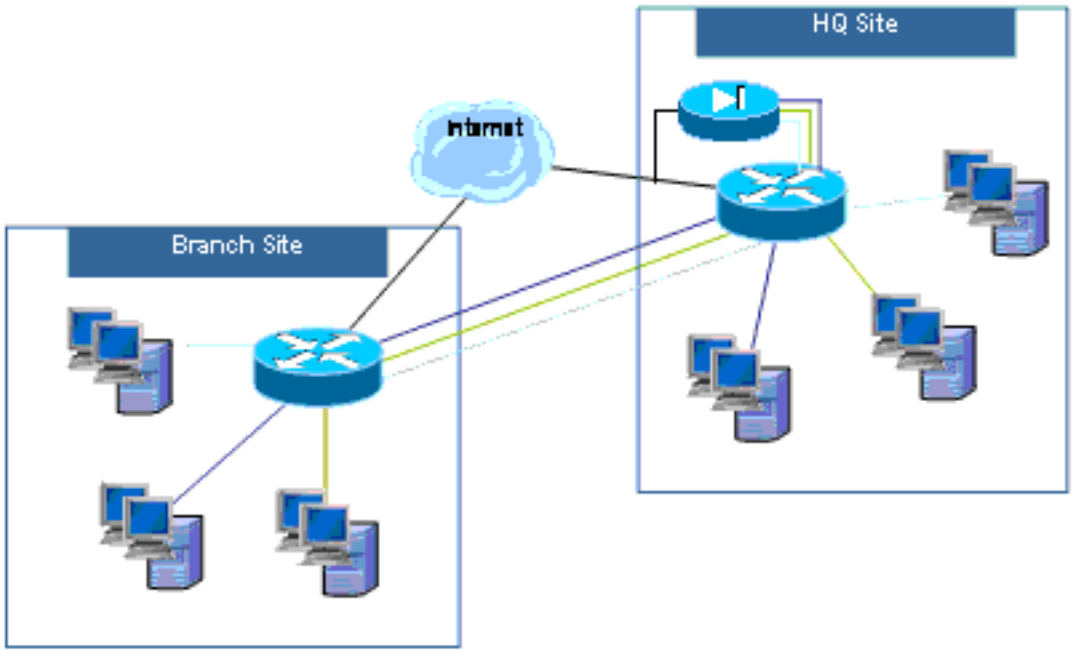
VRF-bewuste Cisco IOS-firewalltoepassingen kunnen in twee basiscategorieën worden ingedeeld:

- Meervoudige huurder, enig-plaats-internet toegang voor meerdere huurders met overlappende adresruimten of gesegregeerde routeruimten op één enkele plaats. Er wordt een stateful firewall toegepast op de internetconnectiviteit van elke VRF om de kans op een compromis door middel van open NAT-verbindingen verder te verminderen. Poortverzending kan worden toegepast om connectiviteit op servers in VRFs mogelijk te maken.



In dit document is een voorbeeld opgenomen van een toepassing met meerdere huurders voor zowel VRF-bewuste Classic Firewall als het VRF-Aware Zone-Based Firewall Configuration-model.

- Multi-huurder, multi-site-Multisite huurders die apparatuur in een groot netwerk delen hebben behoefte aan connectiviteit tussen meerdere plaatsen door de verbinding van VRFs van huurders op verschillende plaatsen door VPN of WAN verbindingen. Internettoegang kan voor elke huurder op een of meer sites vereist zijn. Om beheer te vereenvoudigen, kunnen verscheidene afdelingen hun netwerken in één toegangsrouter voor elke site ineenstorten, maar verschillende afdelingen vereisen een gescheiden



adresruimte.

Configuratievoorbeelden voor multi-huurtoepassingen met meerdere sites voor zowel VRF-bewuste Classic Firewall-configuratiemodel als VRF-Aware Zone-Based Firewall-configuratiemodel worden in een volgende update van dit document gegeven.

Niet-ondersteunde configuratie

VRF-bewuste firewall is beschikbaar op Cisco IOS-afbeeldingen die multi-VRF CE (VRF Lite) en MPLS VPN ondersteunen. Firewallmogelijkheden zijn beperkt tot niet-MPLS interfaces. Dat wil zeggen, als een interface zal deelnemen aan verkeer met het MPLS-label, kan de inspectie van firewalls niet op die interface worden toegepast.

Een router kan alleen interVRF-verkeer inspecteren als het verkeer een VRF moet invoeren of verlaten door een interface om naar een andere VRF te kruisen. Als het verkeer direct naar een andere VRF wordt geleid, is er geen fysieke interface waar een firewallbeleid verkeer kan inspecteren, zodat de router geen inspectie kan toepassen.

VRF Lite-configuratie is alleen interoperabel met NAT/PAT als `ip-informatie binnen` of `ip-informatie buiten` op interfaces is ingesteld waar NAT/PAT wordt toegepast om bron- of doeladressen of poortnummers voor netwerkactiviteit aan te passen. De NAT Virtual Interface (NVI)-functie, geïdentificeerd door de toevoeging van een `IP-unit,` schakelt de configuratie in op interfaces die NAT of PAT toepassen, en wordt niet ondersteund voor inter-VRF NAT/PAT-toepassing. Dit gebrek aan interoperabiliteit tussen VRF Lite en NAT-virtuele interface wordt getraceerd door verbeteringsverzoek CSCek35625.

Configureren

In deze sectie, worden de VRF-bewuste Cisco IOS Clastic Firewall en de VRF-bewuste Zone-Based Policy Firewall configuraties uitgelegd.

Opmerking: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

VRF-bewust Cisco IOS mobiele firewall

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Cisco IOS VRF-Aware Clastic Firewall (voorheen CBAC), die door het gebruik van `IP-inspectie` wordt geïdentificeerd, is in Cisco IOS-software beschikbaar sinds de Classic Firewall werd uitgebreid tot ondersteuning VRF-bewuste inspectie in Cisco IOS-softwarerelease 12.3(14)T.

Cisco IOS VRF-bewuste klassieke firewall configureren

VRF-bewuste Classic Firewall gebruikt de zelfde configuratiesyntaxis als niet-VRF firewall voor de configuratie van het inspectiebeleid:

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

De parameters van de inspectie kunnen voor elke VRF met VRF-specifieke configuratieopties worden aangepast:

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

De lijsten van het inspectiebeleid worden mondiaal vormgegeven, en een inspectiebeleid kan worden toegepast op interfaces in meerdere VRF's.

Elke VRF heeft zijn eigen reeks inspectieparameters voor waarden zoals Denial-of-service (DoS)-bescherming, TCP/UDP/ICMP-sessietimers, audit-trailinstellingen, enz. Als één inspectiebeleid in meerdere VRFs wordt gebruikt, vervangt de VRF-specifieke parameterconfiguratie elke mondiale configuratie die door het inspectiebeleid wordt gedragen. Raadpleeg Cisco IOS Clastic Firewall and Inbraakpreventiesysteem Denial-of-Service Protection voor meer informatie over het instellen van DoS-beveiligingsparameters.

Cisco IOS VRF-bewuste klassieke firewall-activiteit bekijken

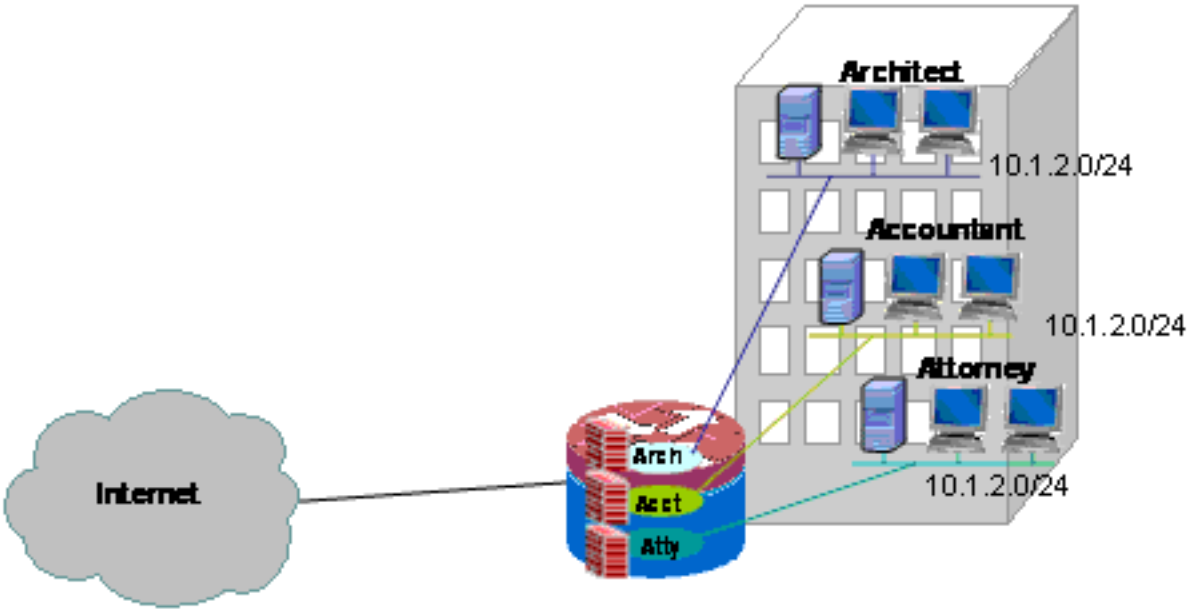
VRF-bewuste "show"-opdrachten van de firewall verschillen van niet-VRF-bewuste opdrachten, omdat voor de opdrachten die u van VRF-bewust zijn, u in de opdracht "show" het VRF-type specificeert:

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

MultiVRF-cloudfirewall voor één locatie

Meerhuurders die Internet toegang als huurdienst aanbieden kunnen VRF-bewuste firewall gebruiken om overlappende adresruimte en een boilerplate firewallbeleid voor alle huurders toe te wijzen. De vereisten voor routeerbare ruimte, NAT, en de verre toegang en de site-to-site VPN dienst kunnen evenals aan het aanbod van aangepaste services voor elke huurder worden aangepast, met het voordeel van het leveren van een VRF voor elke klant.

Deze toepassing gebruikt overlappende adres-ruimte om het beheer van de adresruimte te vereenvoudigen. Maar dit kan problemen veroorzaken die connectiviteit tussen de verschillende VRF's aanbieden. Als geen connectiviteit tussen de VRFs wordt vereist, kan de traditionele binnen-aan-buiten NAT worden toegepast. NAT port-through wordt gebruikt om servers in de architect (arch), accountant (act) en advocaat (atty) VRFs bloot te stellen. FirewallACL's en -beleid moeten NAT-activiteit bevatten.



Configureer de klassieke firewall en NAT voor een multiVRF-netwerk met één locatie

Meerhuurders die Internet toegang als huurdienst aanbieden kunnen VRF-bewuste firewall gebruiken om overlappende adresruimte en een boilerplate firewallbeleid voor alle huurders toe te wijzen. De vereisten voor routeerbare ruimte, NAT, en de verre toegang en de site-to-site VPN dienst kunnen evenals aan het aanbod van aangepaste services voor elke huurder worden aangepast, met het voordeel van het leveren van een VRF voor elke klant.

Er is een beleid dat is gebaseerd op de Klastische Firewall. Dit definieert de toegang tot en vanaf de verschillende LAN- en WAN-verbindingen:

		Connection-bron			
		Internet	Arch	toeschrijven	Atty
verbindingsbestemming	Internet	N.v.t.	HTTP, HTTPS, FTP, DNS, MTP	HTTP, HTTPS, FTP, DNS, MTP	HTTP, HTTPS, FTP, DNS, MTP
	Arch	FTP	N.v.t.	ontkennen	ontkennen
	toeschrijven	mtp	ontkennen	N.v.t.	ontkennen

	Atty	HTTP-HTTP	ontkennen	ontkennen	N.v.t.

De hosts in elk van de drie VRF's kunnen toegang krijgen tot HTTP, HTTPS, FTP en DNS-services op het openbare internet. Eén toegangscontrolelijst (ACL 111) zal worden gebruikt om de toegang voor alle drie de VRF's te beperken (aangezien elke VRF toegang tot identieke services op het internet toestaat), maar er zullen verschillende inspectiebeleidsmaatregelen worden toegepast om de inspectiestatistieken per VRF te verstrekken. Afzonderlijke ACL's kunnen worden gebruikt om ACL-tellers te leveren per VRF. Omgekeerd kunnen hosts op het internet worden aangesloten op diensten zoals beschreven in de vorige beleidstabel, zoals gedefinieerd door ACL 121. Het verkeer moet in beide richtingen worden geïnspecteerd om terugkeer door ACL's mogelijk te maken die connectiviteit in de tegenovergestelde richting beveiligen. De configuratie van NAT wordt becommentarieerd om de door poort gestuurde toegang tot de diensten in VRFs te beschrijven.

Configuratie met één locatie voor multi-mode klassieke firewall en 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
```

Controleer de klassieke firewall en NAT voor een multi-VRF-netwerk met één locatie

Netwerkadresomzetting en -firewallinspectie worden voor elke VRF met deze opdrachten geverifieerd:

Onderzoek routes in elke VRF met de opdracht **tonen 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#
```

Controleer de NAT-activiteit van elke VRF met de opdracht **ip nat tra vrf [vrf-naam]**:

```
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
```

Controleer de statistieken van de firewallinspectie van elke VRF met de opdracht **ip inspect vrf-naam**:

```
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
```

VRF-bewuste Cisco IOS Zone-Based Policy IOS-firewall

Deze sectie bevat informatie over het configureren van de functies die in dit document worden

beschreven.

Als u Cisco IOS Zone-Based Policy Firewall aan multi-VRF routerconfiguraties toevoegt, heeft dit weinig verschil van Zone Firewall in niet-VRF-toepassingen. Dat wil zeggen, bij de bepaling van het beleid wordt aan alle dezelfde regels voldaan die een niet-VRF Zone-Based Policy Firewall vaststelt, behalve bij de toevoeging van een paar multiVRF-specifieke bepalingen:

- Een zone-Based Policy Firewall kan interfaces bevatten van slechts één zone.
- Een VRF kan meer dan één veiligheidsgebied bevatten.
- Zone-Based Policy Firewall is afhankelijk van routing of NAT om verkeer tussen VRF's toe te staan. Een firewallbeleid dat verkeer tussen VRF Zone-Parks inspecteert of doorgeeft is niet geschikt om verkeer tussen VRF's toe te staan.

VRF-bewuste Cisco IOS Zone-gebaseerde beleidsfirewall configureren

VRF-Aware Zone-Based Policy Firewall gebruikt de zelfde configuratiesyntaxis als niet-VRF-bewuste Zone-Based Policy Firewall, en wijst interfaces toe aan beveiligingsgebieden, definieert beveiligingsbeleid voor verkeer dat tussen zones beweegt en wijst het beveiligingsbeleid toe aan de juiste zone-paar associaties.

VRF-specifieke configuratie is onnodig. Mondiale configuratieparameters worden toegepast, tenzij er een specifiekere parameter-map wordt toegevoegd aan inspectie op een beleidskaart. Zelfs in het geval wanneer een parameter-map gebruikt wordt om specifiekere configuratie toe te passen is de parameter-map niet VRF-specifiek.

Bezig met VRF te bekijken Cisco IOS Zone-Based Policy Firewall

Opdrachten die niet anders zijn dan de opdrachten die niet vallen onder de VRF-bewuste Zone-Based Policy Firewall; Zone-Based Policy Firewall past verkeer toe dat zich van interfaces in één veiligheidszone naar interfaces in een andere beveiligingszone beweegt, ongeacht de VRF-opdrachten van verschillende interfaces. Zodoende gebruikt VRF-Aware Zone-Based Policy Firewall dezelfde **show**-opdrachten om firewallactiviteit te bekijken als die van Zone-Based Policy Firewall in niet-VRF-toepassingen:

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

VRF-bewuste Cisco IOS Zone-Based Policy Firewall-cases

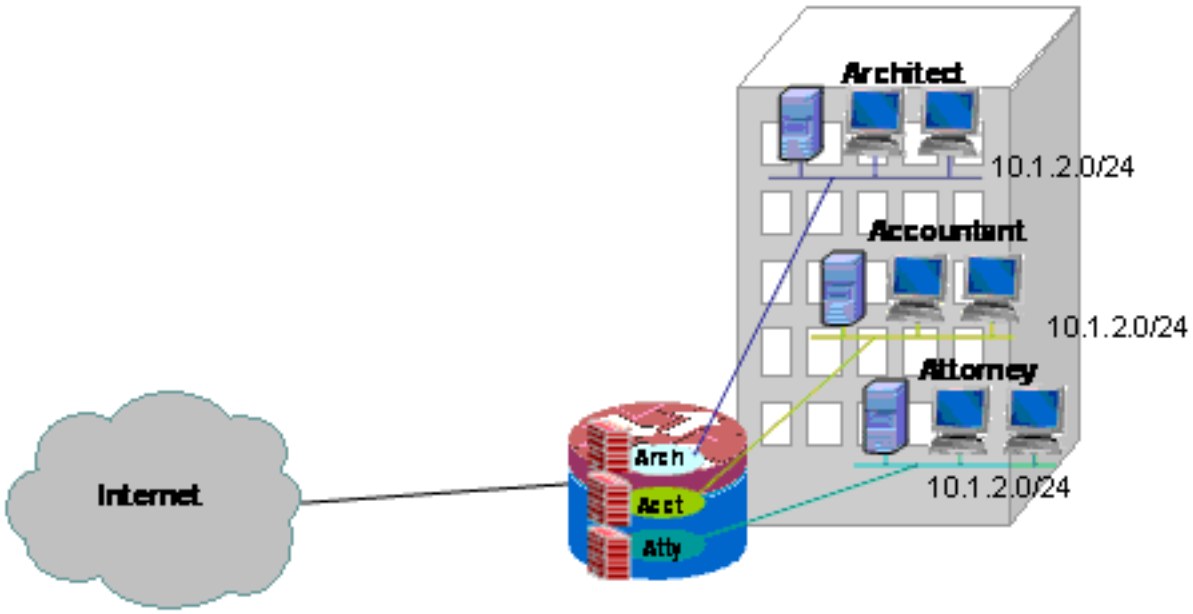
VRF-bewuste gevallen van firewallgebruik variëren sterk. Deze voorbeelden hebben betrekking op:

- Een op één locatie gebaseerde VRF-bewuste implementatie, die doorgaans wordt gebruikt voor meerdere huurfaciliteiten of retailnetwerken
- Een bijkantoor-/detailhandels-/telecomtoepassing waarbij het privé-netwerkverkeer gescheiden wordt gehouden van het openbaar internetverkeer. De gebruikers van de toegang van het internet zijn geïsoleerd van zaken-netwerk gebruikers, en al het zaken-netwerk verkeer wordt over een verbinding van VPN naar de plaats van het Hoofdkantoor voor de toepassing van het Internet beleid geleid.

MultiVRF-firewall met één locatie

Meerhuurders die Internet toegang als huurdienst aanbieden kunnen VRF-bewuste firewall gebruiken om overlappende adresruimte en een boilerplate firewallbeleid voor alle huurders toe te wijzen. Deze toepassing is typisch voor meerdere LAN's op een bepaalde website die één Cisco IOS-router voor internettoegang deelt, of waar een zakelijke partner zoals een fotofiniser of een andere service een geïsoleerd gegevensnetwerk met connectiviteit op het internet en een gedeelte van het netwerk van de predicaire eigenaar wordt aangeboden zonder de vereiste van extra netwerkhardware of internetconnectiviteit. De vereisten voor routeerbare ruimte, NAT, en de verre toegang en de site-to-site VPN dienst kunnen evenals aan het aanbod van aangepaste services voor elke huurder worden aangepast, met het voordeel van het leveren van een VRF voor elke klant.

Deze toepassing gebruikt overlappende adres-ruimte om het beheer van de adresruimte te vereenvoudigen. Maar dit kan problemen veroorzaken die connectiviteit tussen de verschillende VRF's aanbieden. Als geen connectiviteit tussen de VRFs wordt vereist, kan de traditionele binnen-aan-buiten NAT worden toegepast. Daarnaast wordt NAT port-expediteur gebruikt om servers in de architect (arch), accountant (act) en advocaat (atty) VRFs bloot te stellen. FirewallACL's en -beleid moeten NAT-activiteit bevatten.



Configuratie van multi-VRF single-site Zone-gebaseerde beleidsfirewall en NAT

Meerhuurdersites die internettoegang als huurservice aanbieden, kunnen gebruik maken van VRF-bewuste firewall om overlappende adresruimte en een boilerplate-firewallbeleid voor alle huurders toe te wijzen. De vereisten voor routeerbare ruimte, NAT, en de verre toegang en de site-to-site VPN dienst kunnen evenals aan het aanbod van aangepaste services voor elke huurder worden aangepast, met het voordeel van het leveren van een VRF voor elke klant.

Er is een beleid dat is gebaseerd op de Klastische Firewall. Dit definieert de toegang tot en vanaf de verschillende LAN- en WAN-verbindingen:

	Connection-bron			
	Internet	Arch	toeschrijve	Atty

				n	
verbindingsbestemming	Internet	N.v.t.	HTTP, HTTPS, FTP, DNS, MTP	HTTP, HTTPS, FTP, DNS, MTP	HTTP, HTTPS, FTP, DNS, MTP
	Arch	FTP	N.v.t.	ontkennen	ontkennen
	toeschrijven	mtp	ontkennen	N.v.t.	ontkennen
	Atty	HTTP-HTTP	ontkennen	ontkennen	N.v.t.

De hosts in elk van de drie VRF's kunnen toegang krijgen tot HTTP, HTTPS, FTP en DNS-services op het openbare internet. Eén class-map (particulier-publiek-kaart) wordt gebruikt om de toegang voor alle drie VRF's te beperken, aangezien elke VRF toegang tot identieke services op het internet toestaat, maar er worden verschillende polic-kaarten gebruikt om inspectiestatistieken per VRF te verstrekken. Omgekeerd kunnen hosts op het internet verbinding maken met diensten zoals beschreven in de vorige beleidstabel, zoals gedefinieerd door individuele klassenkaarten en beleidskaarten voor de zoneparen van Internet-to-VRF. Er wordt een aparte beleidskaart gebruikt om toegang tot de beheerservices van de router in de zelfzone te voorkomen vanaf het openbare internet. Het zelfde beleid kan ook worden toegepast om toegang van de privé VRFs tot de zelfzone van de router te verhinderen.

De configuratie van NAT wordt becommentarieerd om de door poort gestuurde toegang tot de diensten in VRFs te beschrijven.

Single-Site Multi-Tenant Zone-Based Policy Firewall en NAT configuratie:

```
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
```

Controleer de klassieke firewall en NAT voor een multi-VRF-netwerk met één locatie

Netwerkadresomzetting en -firewallinspectie worden voor elke VRF met deze opdrachten geverifieerd:

Onderzoek routes in elke VRF met de opdracht **tonen 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#
```

Controleer de NAT-activiteit van elke VRF met de opdracht 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        ---                ---
```

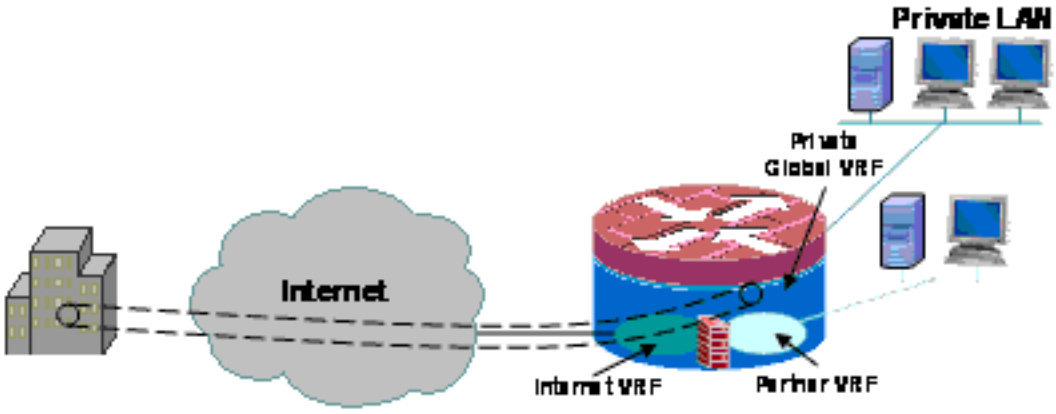
```
tcp 172.16.100.13:25   10.1.2.4:25        ---                ---
tcp 172.16.100.13:80   10.1.2.5:80        ---                ---
```

Controleer de statistiek van de firewallinspectie met de opdrachten van het **showbeleid-plattegrond**:

```
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
```

MultiVRF Single Site Zone Based Policy Firewall, internetverbinding met back-up in "internet"-zone, wereldwijde VRF heeft verbinding met het hoofdkwartier

Deze toepassing is goed geschikt voor telecommunicatie implementaties, kleine detailhandelslocaties en elke andere externe netwerkimplementatie die segregatie van private-netwerk bronnen van de toegang tot het openbare netwerk vereist. Door de internetconnectiviteit en de privé of openbare hotspot gebruikers aan een *openbaar* VRF te isoleren, en een standaardroute in het mondiale VRF toe te passen die al het particuliere netwerkverkeer door VPN-tunnels routeert, hebben de middelen in de particuliere, mondiale VRF en het internet-bereikbare *openbare* VRF geen bereikbaarheid voor elkaar, waardoor de dreiging van een privé-nethost-activiteit volledig wordt weggenomen. Bovendien kan een extra VRF voorzien worden om een beschermde routeruimte te bieden aan andere consumenten die een geïsoleerde netwerkruimte nodig hebben, zoals loterterminals, ATM-machines, betaalkaartverwerkingsterminals, of andere toepassingen. Meervoudige Wi-Fi SSID's kunnen worden aangeboden om toegang te bieden tot zowel het particuliere netwerk als een openbare hotspot.



In dit voorbeeld wordt de configuratie voor twee breedbandinternetverbindingen beschreven, waarbij PAT (NAT-overload) wordt toegepast op hosts in het *publiek* en *partner* VRF's voor toegang tot het openbare internet, waarbij de internetverbinding wordt gewaarborgd door SLA-toezicht op de twee verbindingen. Het privénetwerk (in het mondiale VRF) gebruikt een GRE-over-IPsec verbinding om connectiviteit op het hoofdkwartier (configuratie inbegrepen voor de VPN head-end router) te handhaven via de twee breedbandverbindingen. In het geval dat de een of de andere breedbandverbindingen mislukken, wordt de connectiviteit met het hoofd-eind van VPN behouden, wat ononderbroken toegang tot het hoofdnetwerk van het hoofdkwartier toestaat, aangezien het lokale eindpunt van de tunnel niet specifiek aan één van de internetverbindingen is verbonden.

Een op zone gebaseerde beleidsfirewall is aanwezig en controleert de toegang tot en van VPN naar het privénetwerk, en tussen het openbare en partnerLAN en het internet om uitgaande internettoegang mogelijk te maken, maar geen aansluitingen van internet op de lokale netwerken:

	Internet	Publiek	Partnerpartner	VPN	Private
Internet	N.v.t.	ontkennen	ontkennen	ontkennen	ontkennen
Publiek	HTTP, HTTPS, FTP, DNS	N.v.t.	ontkennen	ontkennen	ontkennen
Partnerpartner		ontkennen	N.v.t.		
VPN	ontkennen	ontkennen	ontkennen	N.v.t.	
Private	ontkennen	ontkennen	ontkennen		N.v.t.

NAT-toepassing voor hotspot en partner-net-verkeer maakt een compromis van het openbare internet veel minder waarschijnlijk, maar de mogelijkheid bestaat nog steeds dat kwaadaardige gebruikers of software een actieve NAT-sessie kunnen exploiteren. De toepassing van stateful inspection minimaliseert de kans dat lokale gastheren gecompromitteerd kunnen worden door een open NAT zitting aan te vallen. Dit voorbeeld gebruikt een 871W, maar de configuratie kan makkelijk gerepliceerd worden met andere ISR-platforms.

Configuratie van multi-VRF Single-Site Zone-Based Policy Firewall, primaire internetverbinding met back-up, wereldwijde VRF heeft VPN aan hoofdscenario

Meerhuurders die Internet toegang als huurdienst aanbieden kunnen VRF-bewuste firewall gebruiken om overlappende adresruimte en een boilerplate firewallbeleid voor alle huurders toe te wijzen. De vereisten voor routeerbare ruimte, NAT, en de verre toegang en de site-to-site VPN dienst kunnen evenals aan het aanbod van aangepaste services voor elke huurder worden aangepast, met het voordeel van het leveren van een VRF voor elke klant.

```
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
```

Deze hubconfiguratie biedt een voorbeeld van de VPN-connectiviteit-configuratie:

```
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
```

Controleer de Multiservice VRF-firewall op basis van één site van de VRF, de primaire internetverbinding met back-up, de mondiale VRF heeft VPN aan het hoofdscenario

Netwerkadresomzetting en -firewallinspectie worden voor elke VRF met deze opdrachten geverifieerd:

Onderzoek routes in elke VRF met de opdracht **tonen IP route vrf [vrf-name]**:

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

Controleer de NAT-activiteit van elke VRF met de opdracht **ip nat tra vrf [vrf-name]:**

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

Controleer de statistiek van de firewallinspectie met de opdrachten van het **showbeleid-plattegrond**:

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

Conclusie

Cisco IOS VRF-bewuste Classic en Zone-Based Policy Firewall biedt lagere kosten en administratieve lasten voor het bieden van netwerkconnectiviteit met geïntegreerde beveiliging voor meerdere netwerken met minimale hardware. Prestaties en schaalbaarheid worden gehandhaafd voor meerdere netwerken en bieden een effectief platform voor netwerkinfrastructuur en -diensten zonder de verhoging van kapitaalkosten.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Probleem

De uitwisselingsserver is niet toegankelijk van de buiteninterface van de router.

Oplossing

Schakel de TCP-inspectie in de router in om dit probleem op te lossen

Monsterconfiguratie

```
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
```

Gerelateerde informatie

- Ontwerpgids voor Zone-gebaseerde beleidsfirewall
- Gebruik van Zone-Based Policy Firewall met VPN
- VRF-bewuste Cisco IOS-firewall
- NAT integreren met MPLS VPN's
- MPLS-uitbreidingen ontwerpen voor klanten-randrouters
- NAT-handeling en fundamentele NAT-probleemoplossing controleren
- Configuratievoorbeeld van PIX/ASA meervoudige context
- Cisco IOS Firewall
- Technische ondersteuning en documentatie – Cisco Systems