Esempio di configurazione di un'applicazione Cisco IOS Firewall classica e Virtual Firewall basata su zona

Sommario

Introduzione

Questo documento descrive le conoscenze tecniche sulle funzionalità del firewall virtuale con supporto VRF, le procedure di configurazione e i casi di utilizzo per vari scenari applicativi.

Il software Cisco IOS® versione 12.3(14)T ha introdotto il firewall virtuale (compatibile con VRF), estendendo la famiglia di funzionalità VRF (Virtual Routing-Forwarding) per offrire ispezione dei pacchetti con informazioni stateful, firewall trasparente, ispezione delle applicazioni e filtro URL, oltre a VPN, NAT, QoS e altre funzionalità compatibili con VRF. Gli scenari applicativi più prevedibili applicheranno NAT con altre funzionalità. Se non è richiesto NAT, è possibile applicare il routing tra VRF per fornire connettività tra VRF. Il software Cisco IOS offre funzionalità compatibili con VRF sia in Cisco IOS Classic Firewall sia in Cisco IOS Zone-Based Policy Firewall, con esempi di entrambi i modelli di configurazione riportati in questo documento. Maggiore attenzione è dedicata alla configurazione del firewall dei criteri basati su zone.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

Supporto funzionalità

Il firewall compatibile con VRF è disponibile nelle immagini Advanced Security, Advanced IP Services e Advanced Enterprise, nonché nelle immagini della nomenclatura legacy con la designazione *o3* , che indica l'integrazione del set di funzionalità del firewall Cisco IOS. La funzionalità firewall compatibile con VRF viene unita alle versioni principali del software Cisco IOS nella versione 12.4. Per applicare il firewall delle policy basato su zone compatibili con VRF, è necessario il software Cisco IOS versione 12.4(6)T o successive. Cisco IOS Zone-Based Policy Firewall non funziona con failover stateful.

Configurazione VRF

Il software Cisco IOS mantiene le configurazioni per il VRF globale e per tutti i VRF privati nello stesso file di configurazione. Se si accede alla configurazione del router tramite l'interfaccia della riga di comando, il controllo degli accessi basato sui ruoli disponibile nelle visualizzazioni CLI può essere utilizzato per limitare le funzionalità del personale operativo e di gestione del router. Le applicazioni di gestione come Cisco Security Manager (CSM) offrono anche un controllo degli accessi basato sui ruoli per assicurare che il personale operativo sia limitato al livello di capacità appropriato.

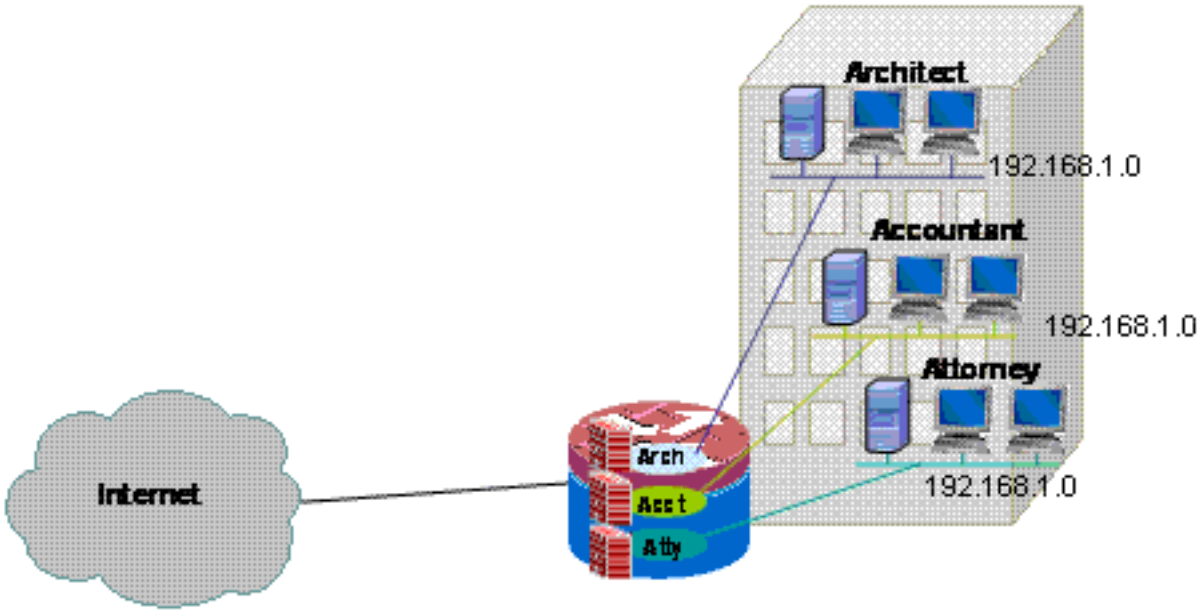
Panoramica degli utilizzi comuni per il firewall IOS compatibile con VRF

VRF-Aware Firewall aggiunge l'ispezione dei pacchetti con stato alla funzionalità Cisco IOS Virtual Routing/Forwarding (VRF). IPsec VPN, Network Address Translation (NAT)/Port Address Translation (PAT), Intrusion Prevention System (IPS) e altri servizi di sicurezza Cisco IOS possono essere combinati con il firewall compatibile con VRF per fornire una serie completa di servizi di sicurezza nei VRF. I VRF supportano più spazi di routing che utilizzano la numerazione degli indirizzi IP sovrapposta, consentendo di suddividere un router in più istanze di routing discrete per la separazione del traffico. Il firewall compatibile con VRF include un'etichetta VRF nelle informazioni sulla sessione per tutte le attività di ispezione tracciate dal router, in modo da mantenere una separazione tra le informazioni sullo stato della connessione che possono essere identiche sotto ogni altro aspetto. Il firewall compatibile con VRF è in grado di ispezionare le

interfacce all'interno di un VRF, nonché le interfacce in VRF che differiscono, ad esempio nei casi in cui il traffico oltrepassa i limiti del VRF, in modo da ottenere la massima flessibilità di ispezione del firewall sia per il traffico tra VRF che per il traffico tra VRF.

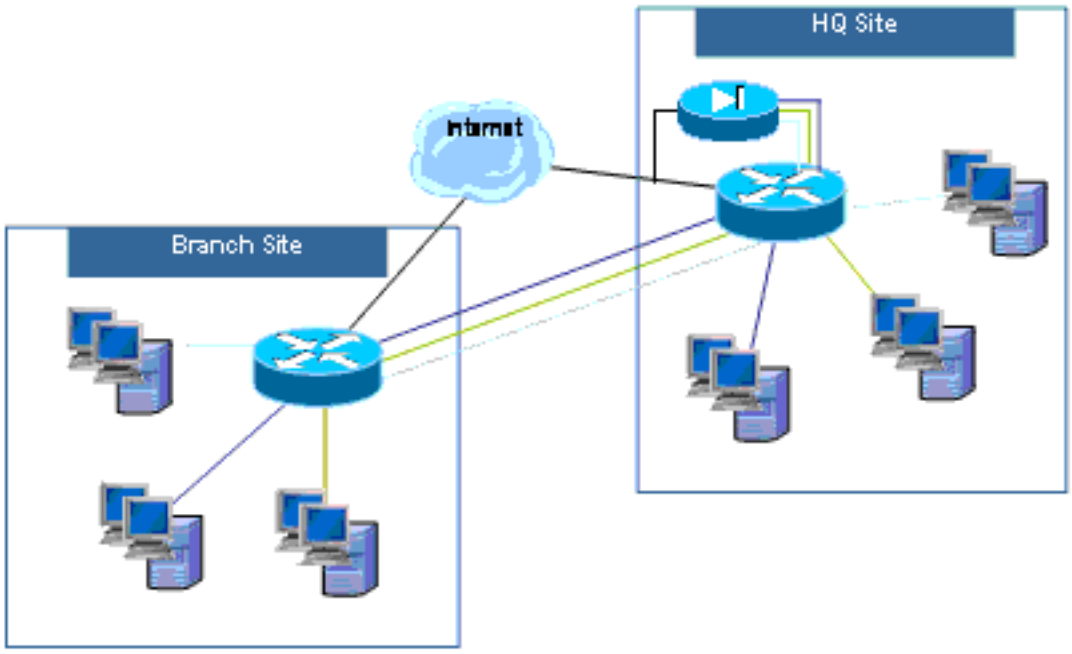
Le applicazioni Cisco IOS Firewall compatibili con VRF possono essere raggruppate in due categorie di base:

- Multi-tenant, sito singolo: accesso a Internet per più tenant con spazi di indirizzi sovrapposti o spazi di route separati in un'unica sede. Alla connettività Internet di ciascun VRF viene applicato un firewall stateful per ridurre ulteriormente la probabilità di compromissione tramite connessioni NAT aperte. È possibile applicare l'inoltro delle porte per consentire la connettività ai server nei
  VRF.



In questo documento viene fornito un esempio di applicazione multi-tenant a sito singolo per il modello di configurazione del firewall classico compatibile con VRF e il modello di configurazione del firewall basato su zona compatibile con VRF.

- Multi-tenant, multi-sito: più tenant che condividono apparecchiature in una rete di grandi dimensioni necessitano di connettività tra più siti tramite la connessione di VRF di tenant in siti diversi tramite connessioni VPN o WAN. L'accesso a Internet può essere richiesto per ogni tenant in uno o più siti. Per semplificare la gestione, diversi reparti possono comprimere le proprie reti in un router di accesso per ogni sito, ma diversi reparti richiedono la separazione dello spazio di



indirizzi. Gli esempi di configurazione per applicazioni multi-site multi-tenant per il modello di configurazione del firewall classico compatibile con VRF e il modello di configurazione del firewall basato su zona compatibile con VRF verranno forniti in un prossimo aggiornamento di questo documento.

Configurazione non supportata

Il firewall compatibile con VRF è disponibile sulle immagini Cisco IOS che supportano Multi-VRF CE (VRF Lite) e MPLS VPN. La funzionalità del firewall è limitata alle interfacce non MPLS. In altre parole, se un'interfaccia parteciperà al traffico con etichetta MPLS, non sarà possibile eseguire l'ispezione del firewall su tale interfaccia.

Un router può ispezionare il traffico tra VRF solo se il traffico deve entrare o uscire da un VRF tramite un'interfaccia per passare a un VRF diverso. Se il traffico viene instradato direttamente a un altro VRF, non vi è alcuna interfaccia fisica in cui i criteri del firewall possano ispezionare il traffico, quindi il router non è in grado di eseguire l'ispezione.

La configurazione di VRF Lite è interoperabile con NAT/PAT solo se `ip nat inside` o `ip nat outside` è configurato su interfacce in cui NAT/PAT viene applicato per modificare indirizzi di origine o di destinazione o numeri di porta per l'attività di rete. La funzionalità NAT Virtual Interface (NVI), identificata dall'aggiunta di una configurazione `ip nat enable` alle interfacce che applicano NAT o PAT, non è supportata per l'applicazione inter-VRF NAT/PAT. Questa mancanza di interoperabilità tra VRF Lite e l'interfaccia virtuale NAT è rilevata dalla richiesta di miglioramento CSCek35625.

Configurazione

In questa sezione vengono illustrate le configurazioni di Cisco IOS Classic Firewall con supporto VRF e VRF Zone-Aware Zone-Based Policy Firewall.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Cisco IOS Classic Firewall compatibile con VRF

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Il Cisco IOS VRF-Aware Classic Firewall (in precedenza denominato CBAC), identificato dall'uso di `ip inspect`, è disponibile nel software Cisco IOS da quando il firewall classico è stato esteso per supportare l'ispezione con riconoscimento VRF nel software Cisco IOS versione 12.3(14)T.

Configurazione di Cisco IOS VRF Classic Firewall

Il firewall classico compatibile con VRF utilizza la stessa sintassi di configurazione del firewall non VRF per la configurazione dei criteri di ispezione:

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

I parametri di ispezione possono essere modificati per ogni VRF con opzioni di configurazione specifiche del VRF:

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

Gli elenchi dei criteri di ispezione vengono configurati a livello globale ed è possibile applicare un criterio di ispezione alle interfacce in più VRF.

Ogni VRF dispone di una serie di parametri di ispezione per valori quali la protezione DoS (Denial-of-Service), i timer di sessione TCP/UDP/ICMP, le impostazioni di audit-trail e così via. Se in più VRF viene utilizzato un criterio di ispezione, la configurazione dei parametri specifica del VRF sostituisce qualsiasi configurazione globale eseguita dal criterio di ispezione. Per ulteriori informazioni su come regolare i parametri della protezione DoS, fare riferimento a Cisco IOS Classic Firewall and Intrusion Prevention System Denial-of-Service.

Visualizzazione dell'attività classica del firewall con Cisco IOS VRF

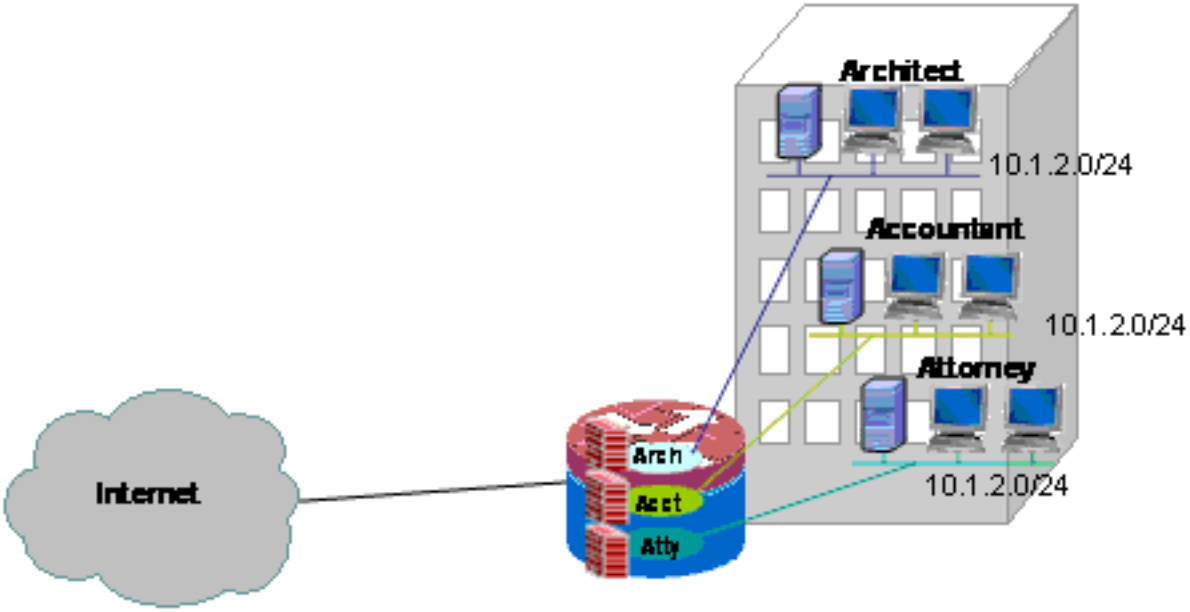
I comandi "show" del firewall compatibili con VRF sono diversi dai comandi non compatibili con VRF, in quanto i comandi compatibili con VRF richiedono di specificare il VRF nel comando "show":

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

Multi-VRF Single-Site Classic Firewall

I siti multi-tenant che offrono l'accesso a Internet come servizio tenant possono utilizzare un firewall compatibile con VRF per allocare lo spazio degli indirizzi sovrapposto e un criterio firewall standard per tutti i tenant. I requisiti per lo spazio instradabile, NAT, accesso remoto e servizio VPN da sito a sito possono essere soddisfatti, così come l'offerta di servizi personalizzati per ogni tenant, con il vantaggio di fornire un VRF per ogni cliente.

Questa applicazione utilizza uno spazio degli indirizzi sovrapposto per semplificare la gestione dello spazio degli indirizzi. Tuttavia, ciò può causare problemi di connettività tra i vari VRF. Se non è richiesta la connettività tra i VRF, è possibile utilizzare il tradizionale NAT interno-esterno. Il port forwarding NAT viene utilizzato per esporre i server nei VRF architect (arch), accountant (acct) e attorney (atty). Gli ACL e i criteri del firewall devono supportare l'attività NAT.



Configurazione di Classic Firewall e NAT per una rete classica multisito VRF su singolo sito

I siti multi-tenant che offrono l'accesso a Internet come servizio tenant possono utilizzare il firewall compatibile con VRF per allocare lo spazio degli indirizzi sovrapposto e un criterio firewall standard per tutti i tenant. I requisiti per lo spazio instradabile, NAT, accesso remoto e servizio VPN da sito a sito possono essere soddisfatti, così come l'offerta di servizi personalizzati per ogni tenant, con il vantaggio di fornire un VRF per ogni cliente.

Esiste una policy firewall classica che definisce l'accesso da e verso le varie connessioni LAN e WAN:

		Origine connessione			
		Internet	Arco	Account	Atty
Destinazione connessione	Internet	N/D	HTTP,HTTPS FTP, DNS, SMTP	HTTP,HTTPS FTP, DNS, SMTP	HTTP,HTTPS FTP, DNS, SMTP
	Arco	FTP	N/D	Nega	Nega
	Account	SMTP	Nega	N/D	Nega
	Atty	SMTP HTTP	Nega	Nega	N/D

Gli host in ognuno dei tre VRF possono accedere ai servizi HTTP, HTTPS, FTP e DNS nella rete Internet pubblica. Verrà utilizzato un elenco di controllo di accesso (ACL 111) per limitare l'accesso per tutti e tre i VRF (poiché ogni VRF consente l'accesso a servizi identici su Internet), ma verranno applicati criteri di ispezione diversi, in modo da fornire statistiche di ispezione per VRF. È possibile utilizzare ACL separati per fornire contatori ACL per VRF. Inversamente, gli host su Internet possono connettersi ai servizi come descritto nella tabella dei criteri precedente, come definito da ACL 121. Il traffico deve essere ispezionato in entrambe le direzioni per consentire la restituzione del traffico tramite ACL che proteggono la connettività nella direzione opposta. La configurazione NAT viene commentata per descrivere l'accesso ai servizi inoltrato tramite porta nelle VRF.

Configurazione NAT e firewall classico multi-tenant per sito singolo:

```
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
```

Verifica del firewall classico e di NAT per una rete classica multisito VRF singola

Network Address Translation e l'ispezione dei firewall vengono verificati per ciascun VRF con questi comandi:

Esaminare le route in ogni VRF con il comando **show ip route vrf [nome-vrf]**:

```
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#
```

Controllare l'attività NAT di ciascun VRF con il comando **show ip nat tra vrf [nome-vrf]**:

```
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
```

Monitorare le statistiche di ispezione del firewall di ciascun VRF con il 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 criteri basati su zona Cisco IOS con riconoscimento VRF

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Se si aggiunge Cisco IOS Zone-Based Policy Firewall a configurazioni di router multi VRF, la differenza rispetto a Zone Firewall sarà minima nelle applicazioni non VRF. In altre parole, la

determinazione delle policy osserva tutte le stesse regole osservate da un firewall delle policy basato su zona non VRF, ad eccezione di alcune clausole specifiche di più VRF:

- Un'area di protezione del firewall dei criteri basata su aree può contenere interfacce di una sola area.
- Un VRF può contenere più aree di protezione.
- Il firewall dei criteri basato su zone dipende dal routing o dal NAT per consentire lo spostamento del traffico tra i VRF. Un criterio firewall che controlla o passa il traffico tra coppie di zone tra VRF non è adeguato per consentire lo spostamento del traffico tra VRF.

Configurazione di Cisco IOS Zone-Based Policy Firewall con riconoscimento VRF

Il firewall dei criteri basati sulle zone compatibili con VRF utilizza la stessa sintassi di configurazione del firewall dei criteri basati sulle zone non compatibili con VRF e assegna le interfacce alle aree di sicurezza, definisce i criteri di sicurezza per il traffico che si sposta tra le zone e assegna i criteri di sicurezza alle associazioni di coppia di zone appropriate.

Non è necessaria una configurazione specifica di VRF. Vengono applicati i parametri di configurazione globali, a meno che non venga aggiunta una mappa dei parametri più specifica per l'ispezione in una mappa dei criteri. Anche nel caso in cui una mappa dei parametri viene utilizzata per applicare una configurazione più specifica, la mappa dei parametri non è specifica per VRF.

Visualizzazione dell'attività del firewall per le policy basate su zone Cisco IOS compatibili con VRF

I comandi **show di** VRF-Aware Zone-Based Policy Firewall non sono diversi dai comandi senza VRF. Il firewall dei criteri basato su zone applica il traffico che si sposta dalle interfacce di un'area di sicurezza alle interfacce di un'altra area, indipendentemente dalle assegnazioni VRF di diverse interfacce. Pertanto, per visualizzare l'attività del firewall, il firewall dei criteri basati su zona compatibile con VRF utilizza gli stessi comandi **show** utilizzati dal firewall dei criteri basati su zona nelle applicazioni non VRF:

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

Casi di utilizzo del firewall per le policy basate su zone Cisco IOS compatibili con VRF

I casi di utilizzo del firewall compatibili con VRF variano notevolmente. Questi esempi riguardano:

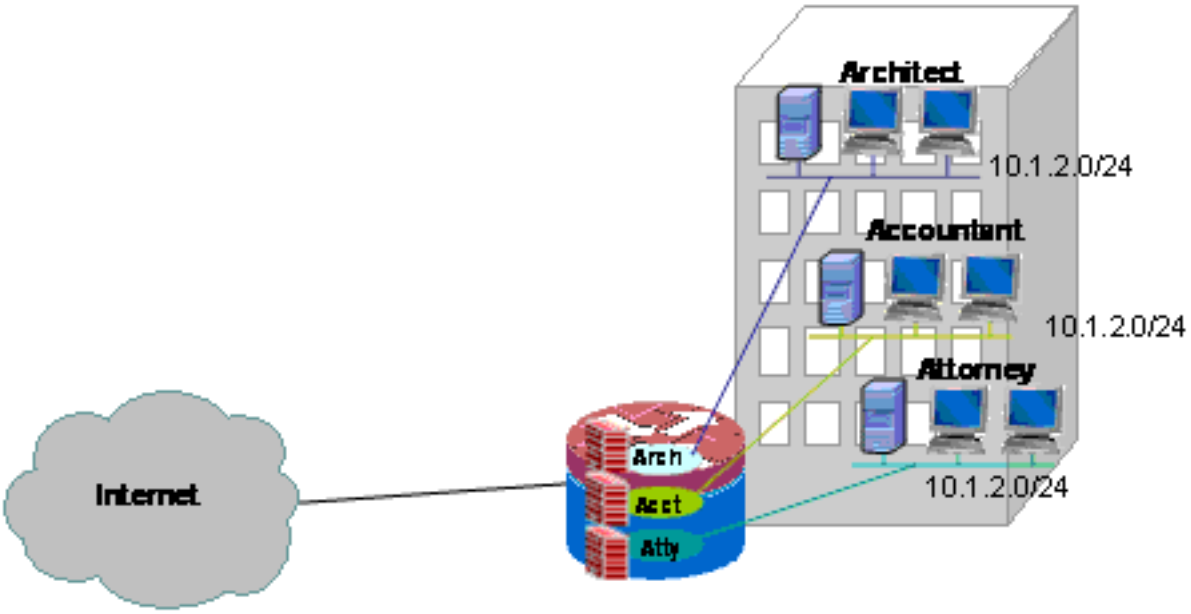
- Implementazione con riconoscimento VRF su un singolo sito, generalmente utilizzata per strutture multi-tenant o reti retail
- Applicazione per filiali, punti vendita, telelavoratori, in cui il traffico di rete privata viene mantenuto in un VRF separato dal traffico Internet pubblico. Gli utenti con accesso a Internet sono isolati dagli utenti della rete aziendale e tutto il traffico della rete aziendale viene indirizzato al sito della sede centrale per l'applicazione di criteri Internet tramite una connessione VPN.

Firewall criteri basato su area multisito VRF su singolo sito

I siti multi-tenant che offrono l'accesso a Internet come servizio tenant possono utilizzare il firewall

compatibile con VRF per allocare lo spazio degli indirizzi sovrapposto e un criterio firewall standard per tutti i tenant. Questa applicazione è in genere utilizzata per più LAN in un determinato sito che condivide un router Cisco IOS per l'accesso a Internet o in cui a un partner commerciale, ad esempio un photofinisher o un altro servizio, viene offerta una rete di dati isolata con connettività a Internet e a una parte specifica della rete del proprietario della sede, senza richiedere hardware di rete aggiuntivo o connettività Internet. I requisiti per lo spazio instradabile, NAT, accesso remoto e servizio VPN da sito a sito possono essere soddisfatti, così come l'offerta di servizi personalizzati per ogni tenant, con il vantaggio di fornire un VRF per ogni cliente.

Questa applicazione utilizza uno spazio degli indirizzi sovrapposto per semplificare la gestione dello spazio degli indirizzi. Tuttavia, ciò può causare problemi di connettività tra i vari VRF. Se non è richiesta la connettività tra i VRF, è possibile utilizzare il tradizionale NAT interno-esterno. Inoltre, il port forwarding NAT viene utilizzato per esporre i server nei VRF architect (arch), accountant (acct) e attorney (atty). Gli ACL e i criteri del firewall devono supportare l'attività NAT.



Configurazione di Multi-VRF Single-Site Zone-Based Policy Firewall e NAT

I siti multi-tenant che offrono l'accesso a Internet come servizio tenant possono utilizzare un firewall compatibile con VRF per allocare lo spazio degli indirizzi sovrapposto e un criterio firewall standard per tutti i tenant. I requisiti per lo spazio instradabile, NAT, accesso remoto e servizio VPN da sito a sito possono essere soddisfatti, così come l'offerta di servizi personalizzati per ogni tenant, con il vantaggio di fornire un VRF per ogni cliente.

Esiste una policy firewall classica che definisce l'accesso da e verso le varie connessioni LAN e WAN:

		Origine connessione			
		Internet	Arco	Account	Atty
Destinazione connessione	Internet	N/D	HTTP,HTTPS FTP, DNS, SMTP	HTTP,HTTPS FTP, DNS, SMTP	HTTP,HTTPS FTP, DNS, SMTP

	Arco	FTP	N/D	Nega	Nega
	Account	SMTP	Nega	N/D	Nega
	Atty	SMTP HTTP	Nega	Nega	N/D

Gli host in ognuno dei tre VRF possono accedere ai servizi HTTP, HTTPS, FTP e DNS nella rete Internet pubblica. Una class-map (private-public-cmap) viene utilizzata per limitare l'accesso a tutti e tre i VRF, poiché ogni VRF consente l'accesso a servizi identici su Internet, ma vengono applicate mappe politiche diverse, in modo da fornire statistiche di ispezione per VRF. Al contrario, gli host su Internet possono connettersi ai servizi come descritto nella tabella dei criteri precedente, come definito dalle singole mappe delle classi e dalle mappe dei criteri per le coppie di zone Internet-VRF. Per impedire l'accesso dalla rete pubblica a Internet ai servizi di gestione del router nell'area autonoma, viene utilizzata una mappa dei criteri distinta. È possibile applicare la stessa policy per impedire l'accesso dei VRF privati anche alla zona autonoma del router.

La configurazione NAT viene commentata per descrivere l'accesso ai servizi inoltrato tramite porta nelle VRF.

Firewall dei criteri basato su aree multi-tenant per sito singolo e configurazione 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
```

Verifica del firewall classico e di NAT per una rete classica multisito VRF singola

Network Address Translation e l'ispezione dei firewall vengono verificati per ciascun VRF con questi comandi:

Esaminare le route in ogni VRF con il comando **show ip route vrf [nome-vrf]**:

```
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#
```

Controllare l'attività NAT di ciascun VRF con il comando show ip nat tra vrf [nome-vrf]:

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

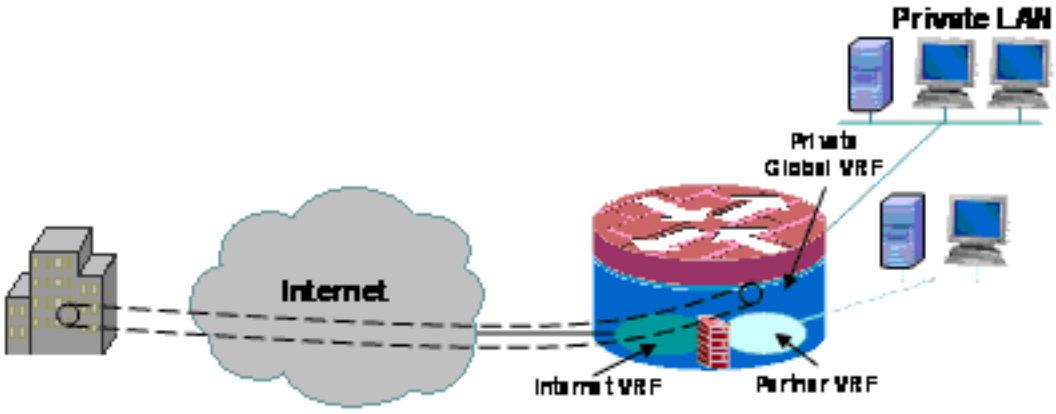
Monitorare le statistiche di ispezione del firewall con i comandi **show policy-map type inspect zone-pair**:

```
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
```

Multi-VRF Single-Site Zone-Based Policy Firewall, connessione Internet con backup in zona "Internet", Global VRF ha connessione alla sede centrale

Questa applicazione è particolarmente adatta per installazioni di telelavoratori, piccole postazioni di vendita al dettaglio e qualsiasi altra installazione di rete di siti remoti che richiede la separazione delle risorse di rete private dall'accesso alla rete pubblica. Isolando la connettività Internet e gli utenti degli hotspot pubblici o privati a un VRF *pubblico* e applicando un percorso predefinito nel VRF globale che instrada tutto il traffico della rete privata attraverso i tunnel VPN, le risorse del VRF privato globale e del VRF *pubblico* raggiungibile da Internet non hanno alcuna raggiungibilità reciproca, rimuovendo così completamente la minaccia di compromissione dell'host della rete privata da parte dell'attività Internet pubblica. Inoltre, è possibile fornire un ulteriore VRF per fornire uno spazio di passaggio protetto ad altri consumatori che necessitano di uno spazio di rete isolato, come terminali per lotterie, sportelli bancomat, terminali per il trattamento di carte di addebito o altre applicazioni. È possibile effettuare il provisioning di più SSID Wi-Fi per offrire accesso sia alla rete privata che a un hotspot pubblico.



Nell'esempio viene descritta la configurazione di due connessioni Internet a banda larga, applicando PAT (NAT overload) per gli host delle VRF *pubbliche* e dei *partner* per l'accesso all'Internet pubblica, con la connettività Internet garantita dal monitoraggio degli SLA sulle due connessioni. La rete privata (nel VRF globale) utilizza una connessione GRE-over-IPsec per mantenere la connettività alla sede centrale (configurazione inclusa per il router headend VPN) sui due collegamenti a banda larga. In caso di guasto di una delle due connessioni a banda larga, viene mantenuta la connettività all'headend VPN, che consente un accesso ininterrotto alla rete HQ, poiché l'endpoint locale del tunnel non è legato specificamente a nessuna delle connessioni Internet.

Èpresente un firewall dei criteri basato su zone che controlla l'accesso dalla VPN alla rete privata e l'accesso dalla VPN alla rete privata e tra le LAN pubbliche e partner e Internet per consentire l'accesso a Internet in uscita, ma non le connessioni alle reti locali da Internet:

	Internet	Public	Partner	VPN	Private
Internet	N/D	Nega	Nega	Nega	Nega
Public	HTTP,HTTPS,FTP, DNS	N/D	Nega	Nega	Nega
Partner		Nega	N/D		
VPN	Nega	Nega	Nega	N/D	
Private	Nega	Nega	Nega		N/D

L'applicazione NAT per il traffico degli hotspot e delle reti dei partner riduce le probabilità di compromissione da Internet pubblica, ma esiste ancora la possibilità che utenti o software dannosi possano sfruttare una sessione NAT attiva. L'applicazione dell'ispezione con conservazione dello stato riduce al minimo le probabilità che gli host locali possano essere compromessi attaccando una sessione NAT aperta. Questo esempio utilizza uno switch 871W, ma la configurazione può essere facilmente replicata con altre piattaforme ISR.

Configurazione di Multi-VRF Single-Site Zone-Based Policy Firewall, connessione Internet principale con backup, globale VRF ha lo scenario da VPN a HQ

I siti multi-tenant che offrono l'accesso a Internet come servizio tenant possono utilizzare il firewall compatibile con VRF per allocare lo spazio degli indirizzi sovrapposto e un criterio firewall

standard per tutti i tenant. I requisiti per lo spazio instradabile, NAT, accesso remoto e servizio VPN da sito a sito possono essere soddisfatti, così come l'offerta di servizi personalizzati per ogni tenant, con il vantaggio di fornire un VRF per ogni 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
```

Questa configurazione hub fornisce un esempio della configurazione della connettività 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
```

Verifica del firewall dei criteri basato su una singola zona su più VRF, connessione Internet principale con backup, scenario globale VRF da VPN a HQ

Network Address Translation e l'ispezione dei firewall vengono verificati per ciascun VRF con questi comandi:

Esaminare le route in ogni VRF con il comando **show ip route vrf [nome-vrf]**:

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

Controllare l'attività NAT di ciascun VRF con il comando **show ip nat tra vrf [nome-vrf]**:

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

Monitorare le statistiche di ispezione del firewall con i comandi **show policy-map type inspect zone-pair**:

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

Conclusioni

Cisco IOS VRF-Aware Classic e Zone-Based Policy Firewall offrono costi e oneri amministrativi ridotti per fornire connettività di rete con sicurezza integrata per più reti con hardware minimo. Prestazioni e scalabilità vengono mantenute per reti multiple e forniscono una piattaforma efficace per l'infrastruttura e i servizi di rete senza l'aumento dei costi di capitale.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Problema

Il server Exchange non è accessibile dall'interfaccia esterna del router.

Soluzione

Per risolvere il problema, abilitare l'ispezione SMTP nel router

Esempio di configurazione

```
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
```

Informazioni correlate

- Guida alla progettazione del firewall per i criteri basati sulle zone
- Utilizzo del firewall dei criteri basato su zone con VPN
- Cisco IOS Firewall compatibile con VRF
- Integrazione di NAT con VPN MPLS
- Progettazione delle estensioni MPLS per i router perimetrali dei clienti
- Verifica del funzionamento e risoluzione dei problemi base del protocollo NAT
- Esempio di configurazione a contesto multiplo per PIX/ASA
- Cisco IOS Firewall
- Documentazione e supporto tecnico – Cisco Systems