Exemple de configuration d'une application de pare-feu virtuel basé sur la zone et de pare-feu Cisco IOS classique

Contenu

Introduction

Ce document décrit l'aspect technique des fonctionnalités de pare-feu virtuel, le processus de configuration et des cas d'utilisation pour divers scénarios d'application de VRF-Aware.

La version de logiciel 12.3(14)T de Cisco IOS® a introduit le Pare-feu (Vrf-averti) virtuel, étendant la famille virtuelle de caractéristique de Routage-expédition (VRF) pour offrir l'inspection de paquet d'avec état, le Pare-feu transparent, l'inspection d'application, et le Filtrage URL, en plus de VPN existant, NAT, de QoS, et d'autres caractéristiques Vrf-averties. La plupart des scénarios prévisibles d'application appliqueront NAT avec d'autres configurations. Si NAT n'est pas exigé, conduisant peut être appliqué entre les vrf pour fournir la Connectivité d'inter-VRF. Capacités Vrf-averties d'offres de logiciel de Cisco IOS dans le Pare-feu classique de Cisco IOS et le Pare-feu basé sur zone de stratégie de Cisco IOS, avec des exemples des deux modèles de configuration fournis dans ce document. Un plus grand foyer est placé sur la configuration basée sur zone de Pare-feu de stratégie.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Prise en charge de fonctionnalité

Le Pare-feu Vrf-averti est disponible dans la sécurité avancée, les Services IP avancés, et les images avancées d'entreprise, aussi bien que les images de legs-nomenclature qui portent la désignation *o3*, qui indique l'intégration de l'ensemble de fonctionnalités du pare-feu Cisco IOS. La fonctionnalité de pare-feu Vrf-avertie a fusionné dans des versions principales de logiciel de Cisco IOS en 12.4. Le Logiciel Cisco IOS version 12.4(6)T ou plus tard est exigé pour appliquer le Pare-feu basé sur zone Vrf-averti de stratégie. Le Pare-feu basé sur zone de stratégie de Cisco IOS ne fonctionne pas avec le basculement dynamique.

Configuration de VRF

Le logiciel de Cisco IOS met à jour des configurations pour le VRF global et tous les vrf privés dans le même fichier de configuration. Si la configuration de routeur est accédée à par l'interface de ligne de commande, le contrôle d'accès basé sur rôle offert dans la caractéristique de vues CLI peut être utilisé pour limiter la capacité du routeur opérationnelle et du personnel de Gestion. Les applications d'administration telles que le Cisco Security Manager (CSM) fournissent également le contrôle d'accès basé sur rôle pour s'assurer que le personnel opérationnel est limité au niveau approprié de la capacité.

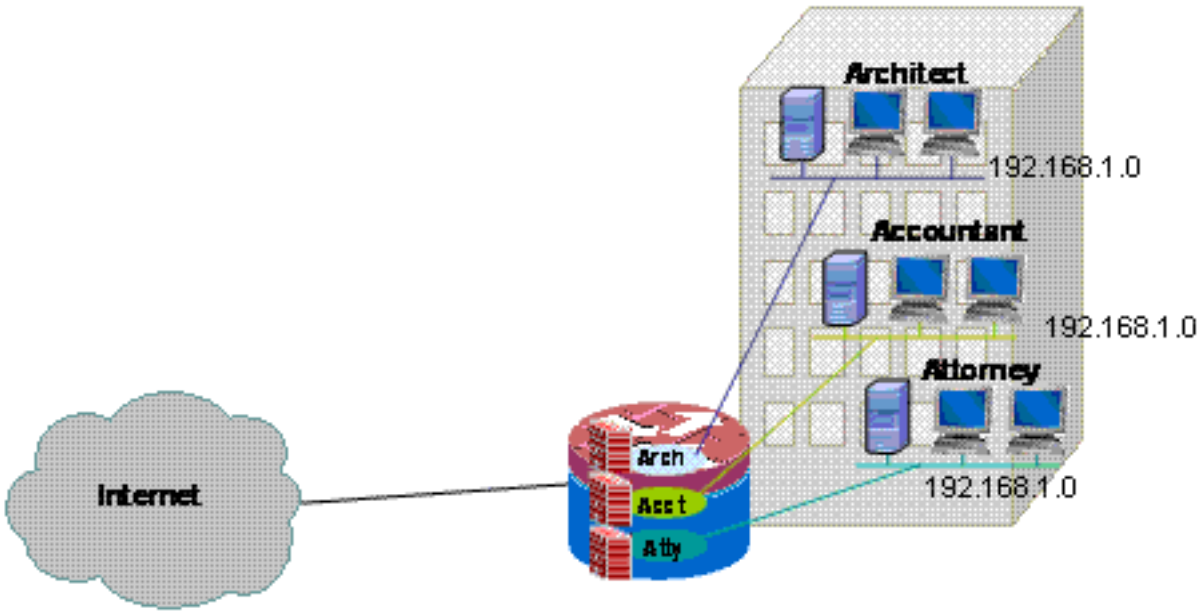
Aperçu des utilisations de terrain communal pour le pare-feu d'IOS Vrf-averti

Le Pare-feu Vrf-averti ajoute l'inspection de paquet d'avec état à la capacité virtuelle de routage/expédition de Cisco IOS (VRF). IPsec VPN, traduction d'adresses du Traduction d'adresses de réseau (NAT) /Port (PAT), Système de prévention d'intrusion (IPS) et d'autres services de sécurité de Cisco IOS peuvent être combinés avec le Pare-feu Vrf-averti pour fournir un ensemble complet de Services de sécurité dans les vrf. Les vrf fournissent le support pour les plusieurs espaces d'artère qui utilisent la numérotation superposante d'adresse IP, ainsi un routeur peut être divisé en plusieurs exemples discrets de routage pour la séparation du trafic. Le Pare-feu Vrf-averti inclut une étiquette de VRF dans les informations de session pour toute l'activité d'inspection que le routeur dépiste, pour mettre à jour la séparation entre les informations d'état de connexion qui peuvent être identiques à chaque autre égard. Le Pare-feu Vrf-averti peut

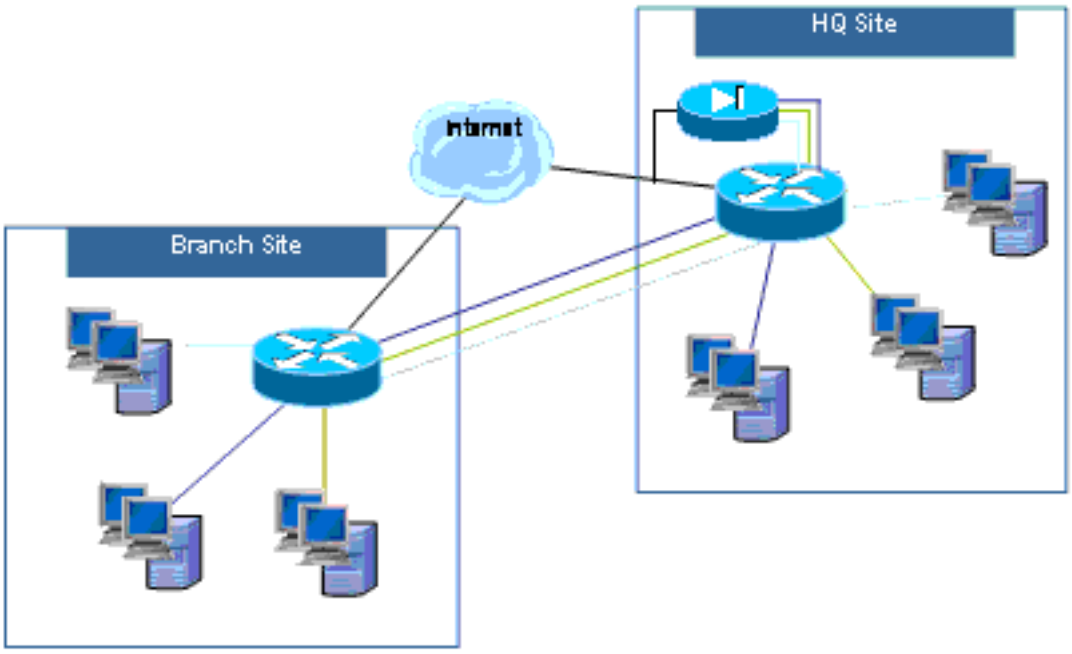
examiner examinent entre les interfaces à moins d'un VRF, aussi bien qu'entre les interfaces dans les vrf qui diffèrent, par exemple dans les cas où le trafic croise des bornes de VRF, de sorte que la flexibilité maximum d'inspection de Pare-feu soit réalisée pour le trafic d'intra-VRF et d'inter-VRF.

Des applications Vrf-averties de Pare-feu Cisco IOS peuvent être groupées dans deux catégories de base :

- Multi-locataire, site unique — Accès Internet pour de plusieurs locataires avec les espaces d'adressage superposants ou les espaces isolés d'artère à un site simple. Le pare-feu dynamique est appliqué à la connexion à internet de chaque vrf pour réduire plus loin la probabilité de la compromission par les connexions NAT ouvertes. La transmission du port peut être appliquée pour permettre la Connectivité aux serveurs dans les



vrf.
Un exemple d'une demande de site unique de multi-locataire de modèle classique Vrf-averti de configuration de Pare-feu et de modèle basé sur zone Vrf-averti de configuration de Pare-feu est fourni dans ce document.
- Multi-locataire, multisite — Plusieurs locataires qui partagent le matériel dans une Connectivité du besoin de grand réseau entre les plusieurs sites par la connexion des vrf des locataires à différents sites par le VPN ou les connexions WAN. L'accès Internet peut être exigé pour chaque locataire à un ou plusieurs sites. Afin de simplifier la Gestion, plusieurs services peuvent réduire leurs réseaux dans un routeur d'accès pour chaque site, mais les divers services exigent la ségrégation de l'espace



d'adressage.

Des exemples de configuration pour des demandes multisites de multi-locataire de modèle classique Vrf-averti de configuration de Pare-feu et de modèle basé sur zone Vrf-averti de configuration de Pare-feu seront fournis dans une prochaine mise à jour à ce document.

Configuration non vérifiée

Le Pare-feu Vrf-averti est disponible sur les images de Cisco IOS qui prennent en charge le CE de Multi-VRF (VRF Lite) et le MPLS VPN. La fonctionnalité de pare-feu est limitée aux interfaces non-MPLS. C'est-à-dire, si une interface participera au trafic MPLS-étiqueté, l'inspection de Pare-feu ne peut pas être appliquée sur cette interface.

Un routeur peut seulement examiner le trafic d'inter-VRF si le trafic doit entrer dans ou laisser un VRF par une interface pour croiser à un VRF différent. Si le trafic est conduit directement à un autre VRF, il n'y a aucune interface physique où une stratégie de Pare-feu peut examiner le trafic, ainsi le routeur ne peut pas appliquer l'inspection.

La configuration de Lite de VRF est interopérable avec NAT/PAT seulement si l'`ip nat intérieur` ou l'`ip nat outside` est configuré sur des interfaces où NAT/PAT est appliqué pour modifier la source ou les adresses de destination ou les numéros de port pour l'activité réseau. La caractéristique NAT de l'interface virtuelle (NVI), identifiée par l'ajout d'une configuration d'`ip nat enable aux` interfaces qui appliquent NAT ou PAT, n'est pas prise en charge pour l'application du l'inter-VRF NAT/PAT. Ce manque d'Interopérabilité entre le VRF Lite et l'interface Nat-virtuelle est dépisté par la demande d'amélioration CSCek35625.

Configurez

Dans cette section, le Pare-feu de Cisco IOS Vrf-averti et les configurations basées sur zone Vrf-averties classiques de Pare-feu de stratégie sont expliqués.

Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Pare-feu Vrf-averti de classique de Cisco IOS

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Le Pare-feu classique Vrf-averti de Cisco IOS (autrefois appelé le CBAC), qui est identifié en employant l'`ip inspect`, a été disponible dans le logiciel de Cisco IOS depuis que le Pare-feu classique a été étendu pour prendre en charge l'inspection Vrf-avertie dans le Logiciel Cisco IOS version 12.3(14)T.

Configurez le Pare-feu classique Vrf-averti de Cisco IOS

Le Pare-feu classique Vrf-averti utilise la même syntaxe de configuration que le Pare-feu de non-VRF pour la configuration de la stratégie d'inspection :

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

Des paramètres d'inspection peuvent être modifiés pour chaque VRF avec des options de configuration de Vrf-particularité :

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

Des listes de stratégie d'inspection sont configurées globalement, et une stratégie d'inspection peut être appliquée aux interfaces dans de plusieurs vrf.

Chaque VRF porte son propre ensemble de paramètres d'inspection pour des valeurs telles que des temporisateurs de protection du déni de service (DOS), de session TCP/UDP/ICMP, des configurations d'audit-trail, etc. Si une stratégie d'inspection est utilisée dans de plusieurs vrf, la configuration de paramètre de Vrf-particularité remplace n'importe quelle configuration globale qui est portée par la stratégie d'inspection. Référez-vous au Pare-feu de Cisco IOS et à la protection classiques de déni de service de système de prévention des intrusions pour plus d'informations sur la façon accorder des paramètres de protection DOS.

Visionnement de l'activité classique Vrf-avertie de Pare-feu de Cisco IOS

Les commandes Vrf-averties de « exposition » de Pare-feu diffèrent des commandes non-VRF-averties, parce que les commandes Vrf-averties exigent que vous spécifiez le VRF dans la commande de « exposition » :

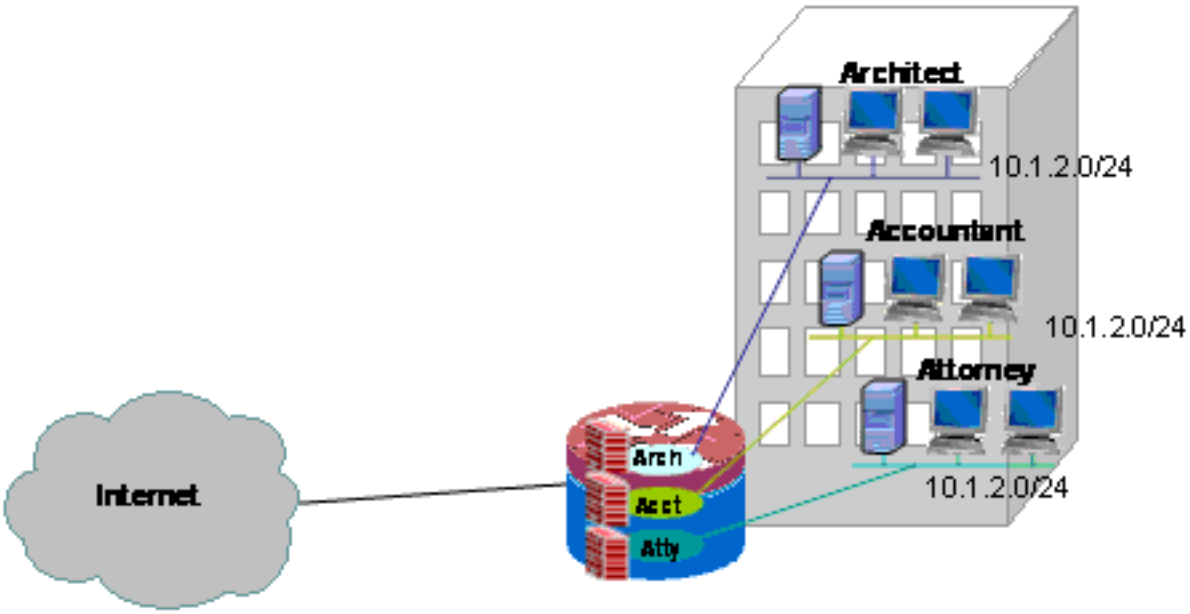
```
router#show ip inspect [ all | config | interfaces | name | sessions | statistics ] vrf vrf-name
```

Pare-feu de classique de site unique de Multi-VRF

sites de Multi-locataire qui offrent l'accès Internet pendant qu'un service de locataire peut employer le Pare-feu Vrf-averti afin d'allouer l'espace d'adressage superposant et une stratégie de Pare-feu de zones fixes pour tous les locataires. Des conditions requises pour l'espace routable, le service NAT, et de remote-access et de site à site VPN peuvent être aussi bien facilitées à l'offre des services personnalisés pour chaque locataire, avec l'avantage du ravitaillement un VRF pour chaque client.

Cette application emploie l'espace d'adressage superposant afin de simplifier la Gestion d'espace d'adressage. Mais, ceci peut poser les problèmes qui offrent la Connectivité entre les divers vrf. Si la Connectivité n'est pas exigée entre les vrf, l'à l'intérieur-à-extérieur traditionnel NAT peut être appliqué. La transmission du port NAT est utilisée pour exposer des serveurs dans l'architecte

(voûte), le comptable (acct), et les vrf (atty) de mandataire. Le Pare-feu ACLs et les stratégies doivent faciliter l'activité NAT.



Configurez le Pare-feu classique et NAT pour un réseau de classique de site unique de Multi-VRF

sites de Multi-locataire qui offrent l'accès Internet pendant qu'un service de locataire peut employer le Pare-feu Vrf-averti pour allouer l'espace d'adressage superposant et une stratégie de Pare-feu de zones fixes pour tous les locataires. Des conditions requises pour l'espace routable, le service NAT, et de remote-access et de site à site VPN peuvent être aussi bien facilitées à l'offre des services personnalisés pour chaque locataire, avec l'avantage du ravitaillement un VRF pour chaque client.

Une stratégie classique de Pare-feu est en place, qui définit l'accès à et des diverses connexions de LAN et WAN :

		Source de connexion			
		Internet	Voûte	Acct	Atty
Destination de connexion	Internet	S/O	HTTP, FTP HTTPS, DN, SMTP	HTTP, FTP HTTPS, DN, SMTP	HTTP, FTP HTTPS, DN, SMTP
	Voûte	FTP	S/O	Refusez	Refusez
	Acct	SMTP	Refusez	S/O	Refusez
	Atty	SMTP DE HTTP	Refusez	Refusez	S/O

Les hôtes dans chacun des trois vrf peuvent accéder au HTTP, le HTTPS, le FTP, et les services

DNS sur l'Internet public. Une liste de contrôle d'accès (ACL 111) sera utilisée pour limiter l'accès pour chacun des trois vrf (puisque chaque VRF permet l'accès aux services identiques sur l'Internet), mais les différentes stratégies d'inspection sera appliquée, afin de fournir des statistiques d'inspection de par-VRF. ACLs distinct peut être utilisé pour fournir des compteurs d'ACL par VRF. Inversement, les hôtes sur l'Internet peuvent se connecter aux services comme décrit dans la table précédente de stratégie, comme défini par l'ACL 121. Le trafic doit être examiné dans les deux directions pour faciliter le retour par ACLs qui protègent la Connectivité dans le sens inverse. La configuration NAT est commentée pour décrire l'accès port-expédié aux services dans les vrf.

Pare-feu classique de Multi-locataire de site unique et configuration 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
```

Vérifiez le Pare-feu classique et NAT pour un réseau de classique de site unique de Multi-VRF

L'inspection de traduction d'adresses réseau et de Pare-feu est vérifiée pour assurer chaque VRF avec ces commandes :

Examinez les artères dans chaque VRF avec la commande de **show ip route vrf [vrf-name]** :

```
stg-2801-L#show ip route vrf acct Routing Table: acct Codes: C - connected, S - static, R - RIP,
M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF
NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF
external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS
inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded
static route Gateway of last resort is 172.16.100.1 to network 0.0.0.0 172.16.0.0/24 is
subnetted, 1 subnets S 172.16.100.0 [0/0] via 0.0.0.0, NVI0 10.0.0.0/24 is subnetted, 1 subnets
C 10.1.2.0 is directly connected, FastEthernet0/1.171 S* 0.0.0.0/0 [1/0] via 172.16.100.1 stg-
2801-L#
```

Vérifiez l'activité NAT de chaque VRF avec la commande **nat de vrf de tra de show ip [vrf-name]** :

```
stg-2801-L#show ip nat tra vrf acct Pro Inside global Inside local Outside local Outside global
tcp 172.16.100.12:25 10.1.2.3:25 --- --- tcp 172.16.100.100:1078 10.1.2.3:1078 172.17.111.3:80
172.17.111.3:80
```

Surveillez les statistiques d'inspection de Pare-feu de chaque VRF avec la commande de **nom de vrf de show ip inspect** :

```
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
```

Le pare-feu d'IOS basé sur zone de stratégie de Cisco IOS Vrf-averti

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Si vous ajoutez le Pare-feu basé sur zone de stratégie de Cisco IOS aux configurations de routeur de multi-VRF, ceci soutient peu de différence de Pare-feu de zone dans des applications de non-VRF. C'est-à-dire, la détermination de stratégie observe toutes les mêmes règles qu'un Pare-feu basé sur zone de stratégie de non-VRF observe, sauf l'ajout de quelques conditions de multi-VRF-particularité :

- Une zone de sécurité du pare-feu basée sur zone de stratégie peut contenir des interfaces de seulement une zone.
- UN VRF peut contenir plus d'une zone de Sécurité.
- Le Pare-feu basé sur zone de stratégie est dépendant du routage ou NAT afin de permettre au trafic pour se déplacer entre les vrf. Une stratégie de Pare-feu qui examine ou les passages trafiquent entre les zone-paire d'inter-VRF n'est pas adéquat pour permettre au trafic pour se déplacer entre les vrf.

Configurez le Pare-feu basé sur zone de stratégie de Cisco IOS Vrf-averti

Le Pare-feu basé sur zone Vrf-averti de stratégie utilise la même syntaxe de configuration que le Pare-feu basé sur zone non-VRF-averti de stratégie, et assigne des interfaces aux zones de Sécurité, définit des stratégies de sécurité pour le trafic qui se déplace entre les zones, et assigne la stratégie de sécurité aux associations appropriées de zone-paire.

la configuration de Vrf-particularité est inutile. Les paramètres de configuration globale sont appliqués, à moins qu'un parameter-map plus spécifique soit ajouté à l'inspection sur un policy-map. Même dans le cas où un parameter-map est utilisé pour appliquer une configuration plus spécifique, le parameter-map n'est pas Vrf-particularité.

Visionnement de l'activité basée sur zone de Pare-feu de stratégie de Cisco IOS Vrf-averti

Les commandes show basées sur zone Vrf-averties de Pare-feu de stratégie ne sont pas différentes des commandes non-VRF-averties ; Le Pare-feu basé sur zone de stratégie applique le trafic qui se déplace des interfaces dans une zone de Sécurité aux interfaces dans une autre zone de Sécurité, indépendamment des attributions de VRF de diverses interfaces. Ainsi, le Pare-feu basé sur zone Vrf-averti de stratégie utilise les mêmes **commandes show** afin de visualiser l'activité de Pare-feu que sont utilisés par Pare-feu basé sur zone de stratégie dans des applications de non-VRF :

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

Cas d'utilisation basés sur zone de Pare-feu de stratégie de Cisco IOS Vrf-averti

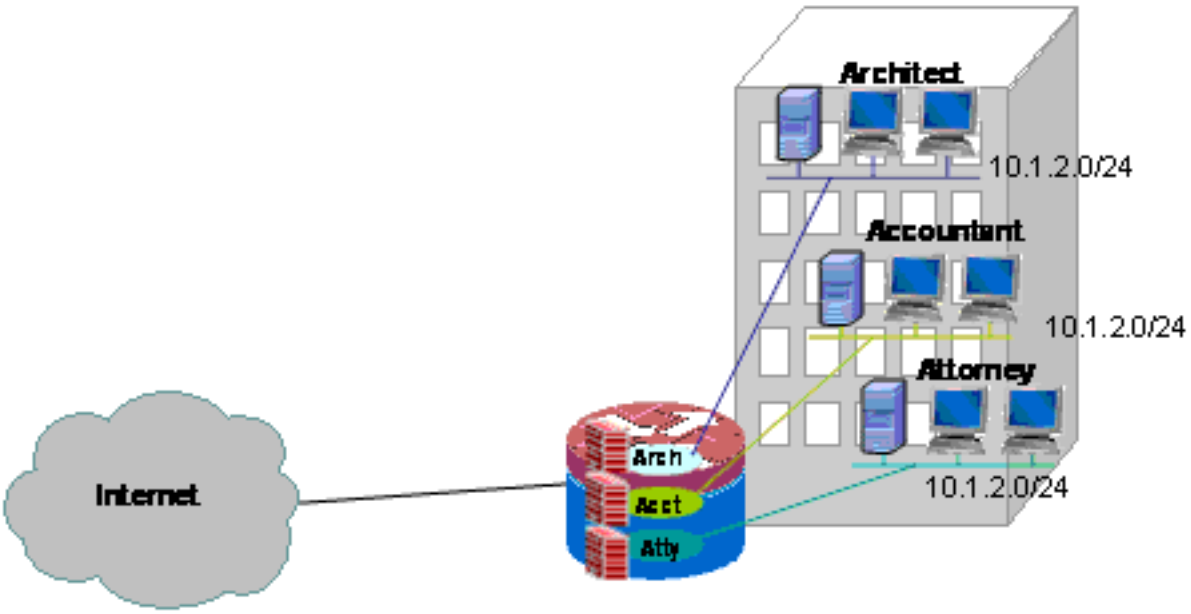
les cas d'utilisation Vrf-avertis de Pare-feu varient considérablement. Adresse de ces exemples :

- Un déploiement Vrf-averti de site unique, typiquement utilisé pour des équipements de multi-locataire ou des réseaux au détail
- Une application de succursale/détail/télétravailleur où le trafic de privé-réseau est maintenu dans un VRF distinct du trafic de public-Internet. Des utilisateurs d'accès Internet sont isolés dans des utilisateurs d'entreprise-réseau, et tout le trafic d'entreprise-réseau est dirigé au-dessus d'une connexion VPN au site QG pour l'application de stratégie d'Internet.

Pare-feu basé sur zone de stratégie de site unique de Multi-VRF

sites de Multi-locataire qui offrent l'accès Internet pendant qu'un service de locataire peut employer le Pare-feu Vrf-averti pour allouer l'espace d'adressage superposant et une stratégie de Pare-feu de zones fixes pour tous les locataires. Cette application est typique pour de plusieurs réseaux locaux à un site donné qui partage un routeur Cisco IOS pour l'accès Internet, ou à où un partenaire commercial tel qu'un photofinisher ou un autre service est offert un réseau de données d'isolement avec la Connectivité à l'Internet et à une certaine partie spécifique du réseau du propriétaire de site, sans condition requise de matériel réseau supplémentaire ou de connexion Internet. Des conditions requises pour l'espace routable, le service NAT, et de remote-access et de site à site VPN peuvent être aussi bien facilitées à l'offre des services personnalisés pour chaque locataire, avec l'avantage du ravitaillement un VRF pour chaque client.

Cette application emploie l'espace d'adressage superposant afin de simplifier la Gestion d'espace d'adressage. Mais, ceci peut poser des problèmes offrant la Connectivité entre les divers vrf. Si la Connectivité n'est pas exigée entre les vrf, l'à l'intérieur-à-extérieur traditionnel NAT peut être appliqué. Supplémentaire, la transmission du port NAT est utilisée pour exposer des serveurs dans l'architecte (voûte), le comptable (acct), et les vrf (atty) de mandataire. Le Pare-feu ACLs et les stratégies doivent faciliter l'activité NAT.



Configurez le Pare-feu basé sur zone de stratégie de site unique de Multi-VRF et NAT

le Multi-locataire situe l'accès Internet de offre pendant qu'un service de locataire peut employer le Pare-feu Vrf-averti pour allouer l'espace d'adressage superposant et une stratégie de Pare-feu de zones fixes pour tous les locataires. Des conditions requises pour l'espace routable, le service NAT, et de remote-access et de site à site VPN peuvent être aussi bien facilitées à l'offre des services personnalisés pour chaque locataire, avec l'avantage du ravitaillement un VRF pour chaque client.

Une stratégie classique de Pare-feu est en place, qui définit l'accès à et des diverses connexions de LAN et WAN :

		Source de connexion			
		Internet	Voûte	Acct	Atty
Destination de connexion	Internet	S/O	HTTP, FTP HTTPS, DN, SMTP	HTTP, FTP HTTPS, DN, SMTP	HTTP, FTP HTTPS, DN, SMTP
	Voûte	FTP	S/O	Refusez	Refusez
	Acct	SMTP	Refusez	S/O	Refusez
	Atty	SMTP DE HTTP	Refusez	Refusez	S/O

Les hôtes dans chacun des trois vrf peuvent accéder au HTTP, le HTTPS, le FTP, et les services DNS sur l'Internet public. Un class-map (privé-public-cmap) est utilisé pour limiter l'accès pour chacun des trois vrf, puisque chaque VRF permet l'accès aux services identiques sur l'Internet, mais pour différentes polic-MAPS sont appliqué, afin de fournir des statistiques d'inspection de

par-VRF. Inversement, les hôtes sur l'Internet peuvent se connecter aux services comme décrit dans la table précédente de stratégie, comme défini par différents class-map et policy-map pour des zone-paire d'Internet-à-VRF. Un policy-map distinct est utilisé pour empêcher l'accès aux services de supervision du routeur dans l'auto-zone de l'Internet public. La même stratégie peut être appliquée pour empêcher l'accès des vrf privés à l'auto-zone du routeur aussi bien.

La configuration NAT est commentée pour décrire l'accès port-expédié aux services dans les vrf.

Pare-feu basé sur zone de stratégie de Multi-locataire de site unique et configuration 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
```

Vérifiez le Pare-feu classique et NAT pour un réseau de classique de site unique de Multi-VRF

L'inspection de traduction d'adresses réseau et de Pare-feu est vérifiée pour assurer chaque VRF avec ces commandes :

Examinez les artères dans chaque VRF avec la commande de **show ip route vrf [vrf-name]** :

```
stg-2801-L#show ip route vrf acct Routing Table: acct Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route Gateway of last resort is 172.16.100.1 to network 0.0.0.0 172.16.0.0/24 is subnetted, 1 subnets S 172.16.100.0 [0/0] via 0.0.0.0, NVI0 10.0.0.0/24 is subnetted, 1 subnets C 10.1.2.0 is directly connected, FastEthernet0/1.171 S* 0.0.0.0/0 [1/0] via 172.16.100.1 stg-2801-L#
```

Vérifiez l'activité NAT de chaque vrf avec la commande nat de vrf de tra de show ip [vrf-name] :

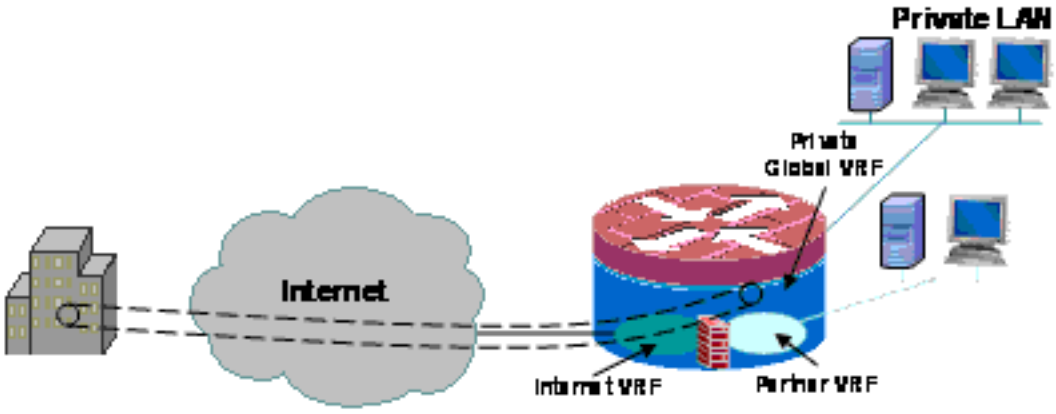
```
stg-2801-L#show ip nat translations Pro Inside global Inside local Outside local Outside global tcp 172.16.100.12:25 10.1.2.3:25 --- --- tcp 172.16.100.100:1033 10.1.2.3:1033 172.17.111.3:80 172.17.111.3:80 tcp 172.16.100.11:21 10.1.2.2:23 --- --- tcp 172.16.100.13:25 10.1.2.4:25 --- --- tcp 172.16.100.13:80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

Surveillez les statistiques d'inspection de Pare-feu avec les commandes de **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
```

Le Pare-feu basé sur zone de stratégie de site unique de Multi-VRF, connexion internet avec la sauvegarde dans la zone de « Internet », VRF global a la connexion au QG

Cette application est bien adaptée aux déploiements de télétravailleur, aux petits sites du détaillant, et à n'importe quel autre déploiement de réseau du site distant qui exige la ségrégation des ressources en privé-réseau de l'accès de public-réseau. En isolant des utilisateurs de connexion Internet et de maison ou de hotspot public à un VRF *public*, et en appliquant un default route dans le VRF global qui conduit tout le trafic de privé-réseau par des tunnels VPN, les ressources dans le VRF privé et global et le VRF *public Internet*-accessible aucune accessibilité entre eux, de ce fait complètement ont retiré la menace de la compromission d'hôte de privé-net par activité de public-Internet. En outre, un VRF supplémentaire peut provisioned pour fournir un espace protégé d'artère pour d'autres consommateurs ayant besoin d'un espace réseau d'isolement, tel que des terminaux de loterie, des ordinateurs atmosphère, la charge-carte traitant des terminaux, ou d'autres applications. Le plusieurs WiFi SSID peut provisioned pour offrir à accès à chacun des deux le réseau privé, aussi bien qu'à un hotspot public.



Cet exemple décrit la configuration pour deux connexions internet haut débit, appliquant PAT (surcharge NAT) pour des hôtes dans les vrf de *public* et de *partenaire* pour l'accès à l'Internet public, avec la connexion Internet assurée par la surveillance SLA sur les deux connexions. Le réseau privé (dans le VRF global) emploie a GRE-au-dessus-IPsec de la connexion pour mettre à jour la Connectivité au QG (configuration incluse pour le routeur de tête de réseau VPN) au-dessus des deux liens larges bandes. Au cas où une ou l'autre des connexions haut débit échouerait, la Connectivité à la tête de réseau VPN est mise à jour, qui permet l'accès ininterrompu au réseau QG, puisque le point final local du tunnel n'est pas attaché spécifiquement à non plus des connexions Internet.

Un Pare-feu basé sur zone de stratégie est accès en place et de contrôles à et du VPN au réseau privé, et entre les réseaux locaux de public et de partenaire et l'Internet afin de ne permettre l'accès d'Internet sortant, mais aucune connexion dedans aux réseaux locaux de l'Internet :

	Internet	Public	Partenaire	VPN	Privé
Internet	S/O	Refusez	Refusez	Refusez	Refusez
Public	HTTP, HTTPS, FTP, DN	S/O	Refusez	Refusez	Refusez
Partenaire		Refusez	S/O		
VPN	Refusez	Refusez	Refusez	S/O	
Privé	Refusez	Refusez	Refusez		S/O

La demande NAT de trafic de point névralgique et de partenaire-net fait la compromission à partir de l'Internet public beaucoup moins vraisemblablement, mais la possibilité existe toujours que les utilisateurs ou le logiciel malveillants peuvent exploiter une session NAT active. L'application de l'inspection avec état réduit des occasions que des hôtes locaux peuvent être compromis en attaquant une session NAT publique. Cet exemple utilise un 871W, mais la configuration peut être facilement répliquée avec d'autres Plateformes ISR.

Configurez le Pare-feu basé sur zone de stratégie de site unique de Multi-VRF, connexion internet

primaire avec la sauvegarde, VRF global a le VPN au scénario QG

sites de Multi-locataire qui offrent l'accès Internet pendant qu'un service de locataire peut employer le Pare-feu Vrf-averti pour allouer l'espace d'adressage superposant et une stratégie de Pare-feu de zones fixes pour tous les locataires. Des conditions requises pour l'espace routable, le service NAT, et de remote-access et de site à site VPN peuvent être aussi bien facilitées à l'offre des services personnalisés pour chaque locataire, avec l'avantage du ravitaillement un VRF pour chaque client.

```
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
```

Cette configuration de hub fournit un exemple de la configuration de connectivité 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
```

Vérifiez le Pare-feu basé sur zone de stratégie de site unique de Multi-VRF, connexion internet primaire avec la sauvegarde, VRF global a le VPN au scénario QG

L'inspection de traduction d'adresses réseau et de Pare-feu est vérifiée pour assurer chaque VRF avec ces commandes :

Examinez les artères dans chaque VRF avec la commande de **show ip route vrf [vrf-name]** :

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

Vérifiez l'activité NAT de chaque VRF avec la commande **nat de vrf de tra de show ip [vrf-name]** :

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

Surveillez les statistiques d'inspection de Pare-feu avec les commandes de **show policy-map type inspect zone-pair** :

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

Conclusion

Le Pare-feu classique de Cisco IOS et basé sur zone Vrf-averti de stratégie offre le coût et la charge administrative réduits pour fournir à la connexion réseau la Sécurité intégrée pour de plusieurs réseaux avec le matériel minimal. La performance et évolutivité est mise à jour pour de plusieurs réseaux et fournit une plate-forme efficace pour l'infrastructure réseau et des services sans augmentation des frais financiers.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Problème

Le serveur exchange n'est pas accessible de l'interface extérieure du routeur.

Solution

Permettez à l'inspection de SMTP dans le routeur afin de réparer cette question

Exemple de configuration

```
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
```

Informations connexes

- Guide basé sur zone de conception de Pare-feu de stratégie
- Utilisant le Pare-feu basé sur zone de stratégie avec le VPN
- Pare-feu Cisco IOS averti de VRF
- Intégrer NAT avec MPLS VPN
- Concevoir des extensions MPLS pour des Routeurs de Customer Edge
- Vérification de l'opération NAT et dépannage NAT de base
- Plusieurs exemple de configuration de contexte PIX/ASA
- Cisco IOS Firewall
- Support et documentation techniques - Cisco Systems