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.

Le logiciel Cisco IOS® Version 12.3(14)T a introduit le pare-feu virtuel (VRF), étendant la gamme de fonctions VRF (Virtual Routing-Forwarding) pour offrir l'inspection dynamique des paquets, un pare-feu transparent, l'inspection des applications et le filtrage des URL, en plus des fonctionnalités VPN, NAT, QoS existantes et d'autres fonctionnalités VRF. La plupart des scénarios d'application prévisibles appliqueront NAT avec d'autres fonctionnalités. Si la NAT n'est pas requise, le routage peut être appliqué entre les VRF pour fournir une connectivité entre VRF. Le logiciel Cisco IOS offre des fonctionnalités compatibles VRF dans le pare-feu classique Cisco IOS et le pare-feu de stratégie basé sur une zone Cisco IOS, avec des exemples des deux modèles de configuration fournis dans ce document. Une plus grande attention est accordée à la configuration du pare-feu de stratégie basé sur les zones.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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-Aware est disponible dans les images Advanced Security, Advanced IP Services et Advanced Enterprise, ainsi que dans les images de nomenclature héritée qui portent la désignation *o3*, ce qui indique l'intégration du jeu de fonctions de pare-feu Cisco IOS. Fonctionnalité de pare-feu VRF-Aware fusionnée dans les versions principales du logiciel Cisco IOS dans la version 12.4. La version 12.4(6)T ou ultérieure du logiciel Cisco IOS est requise pour appliquer le pare-feu de stratégie basé sur des zones VRF. Le pare-feu de stratégie basé sur les zones Cisco IOS ne fonctionne pas avec le basculement dynamique.

Configuration VRF

Le logiciel Cisco IOS gère les configurations du VRF global et de tous les VRF privés dans le même fichier de configuration. Si vous accédez à la configuration du routeur via l'interface de ligne de commande, le contrôle d'accès basé sur les rôles proposé dans la fonction Vues de l'interface de ligne de commande peut être utilisé pour limiter les capacités du personnel d'exploitation et de gestion du routeur. Les applications de gestion telles que Cisco Security Manager (CSM) fournissent également un contrôle d'accès basé sur les rôles pour garantir que le personnel opérationnel est limité au niveau de capacité approprié.

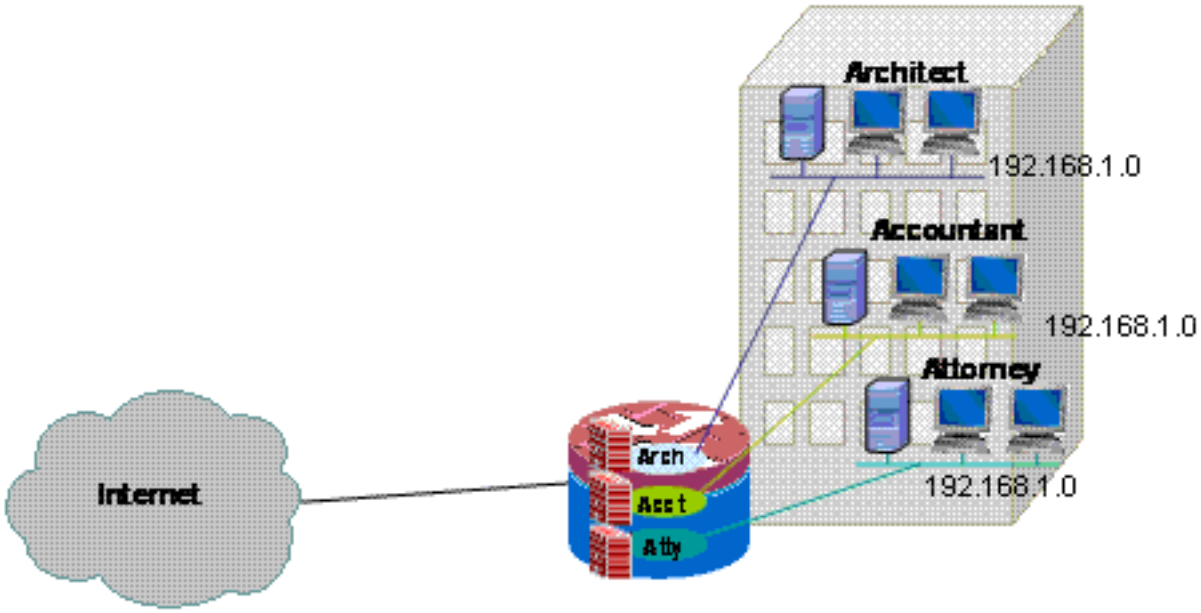
Présentation des utilisations courantes du pare-feu IOS compatible VRF

Le pare-feu VRF-Aware ajoute l'inspection dynamique des paquets à la fonctionnalité VRF (Virtual Routing/Forwarding) de Cisco IOS. Les services VPN IPsec, NAT (Network Address Translation)/PAT (Port Address Translation), IPS (Intrusion Prevention System) et d'autres services de sécurité Cisco IOS peuvent être combinés avec le pare-feu VRF-Aware pour fournir un ensemble complet de services de sécurité dans les VRF. Les VRF prennent en charge plusieurs espaces de routage qui utilisent la numérotation des adresses IP qui se chevauchent, de sorte qu'un routeur peut être divisé en plusieurs instances de routage distinctes pour la séparation du trafic. Le pare-feu VRF-Aware inclut une étiquette VRF dans les informations de session pour toutes les activités d'inspection que le routeur suit, afin de maintenir une séparation entre les informations d'état de connexion qui peuvent être identiques à tous les autres égards. Le pare-feu

VRF-Aware peut inspecter les interfaces au sein d'un VRF, ainsi qu'entre les interfaces des VRF qui diffèrent, par exemple dans les cas où le trafic dépasse les limites de VRF, de sorte que la flexibilité d'inspection maximale du pare-feu soit assurée pour le trafic intra-VRF et inter-VRF.

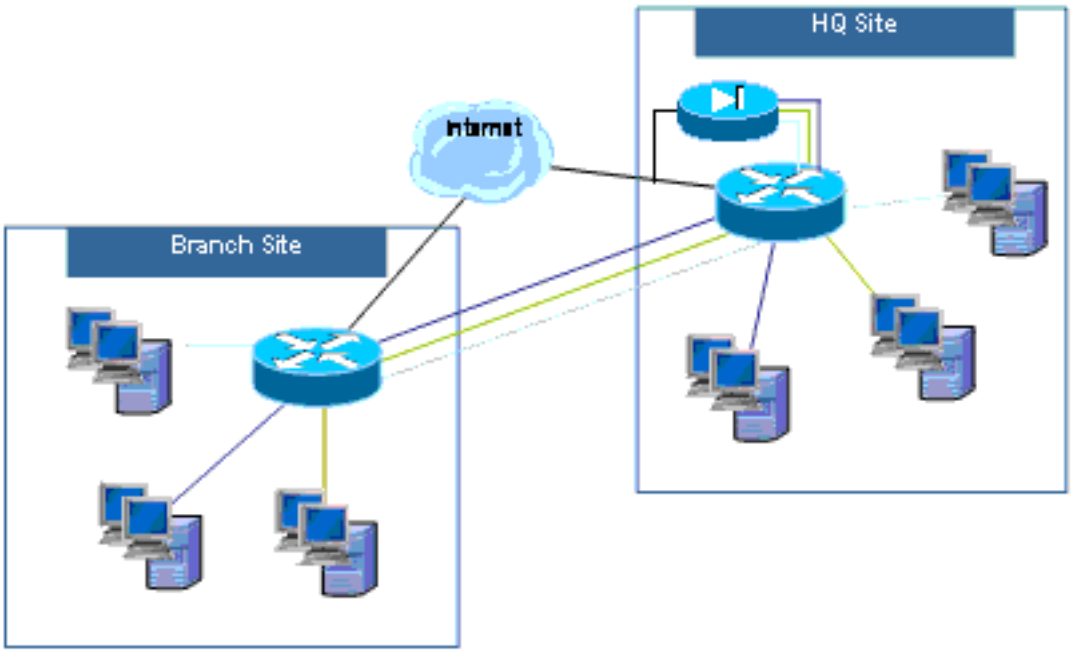
Les applications de pare-feu Cisco IOS compatibles VRF peuvent être regroupées en deux catégories de base :

- Multilocataire, site unique : accès Internet pour plusieurs locataires avec des espaces d'adresses qui se chevauchent ou des espaces de route séparés dans un seul site. Un pare-feu dynamique est appliqué à la connectivité Internet de chaque VRF afin de réduire davantage les risques de compromission par le biais de connexions NAT ouvertes. Le transfert de port peut être appliqué pour permettre la connectivité aux serveurs dans les VRF.



Ce document fournit un exemple d'application multilocataire à site unique pour le modèle de configuration de pare-feu VRF-Aware Classic et le modèle de configuration de pare-feu VRF-Aware Zone-Based.

- Multilocataire et multisite : plusieurs locataires qui partagent des équipements sur un grand réseau ont besoin d'une connectivité entre plusieurs sites par la connexion de VRF de locataires sur différents sites via des connexions VPN ou WAN. Un accès à Internet peut être requis pour chaque locataire sur un ou plusieurs sites. Afin de simplifier la gestion, plusieurs services peuvent regrouper leurs réseaux en un seul routeur d'accès pour chaque site, mais plusieurs services nécessitent une séparation de l'espace



d'adressage.

Des exemples de configuration pour des applications multisites mutualisées pour le modèle de configuration de pare-feu VRF-Aware Classic et le modèle de configuration de pare-feu VRF-Aware Zone-Based seront fournis dans une prochaine mise à jour de ce document.

Configuration non prise en charge

VRF-Aware Firewall est disponible sur les images Cisco IOS qui prennent en charge Multi-VRF CE (VRF Lite) et MPLS VPN. La fonctionnalité de pare-feu est limitée aux interfaces non MPLS. Autrement dit, si une interface participe au trafic étiqueté MPLS, l'inspection de pare-feu ne peut pas être appliquée sur cette interface.

Un routeur ne peut inspecter le trafic inter-VRF que si le trafic doit entrer dans un VRF ou en sortir via une interface pour passer à un VRF différent. Si le trafic est acheminé directement vers un autre VRF, il n'existe aucune interface physique sur laquelle une politique de pare-feu peut inspecter le trafic, de sorte que le routeur ne peut pas appliquer l'inspection.

La configuration VRF Lite est interopérable avec NAT/PAT uniquement si `ip nat inside` ou `ip nat outside` est configurée sur des interfaces où NAT/PAT est appliqué pour modifier les adresses source ou de destination ou les numéros de port pour l'activité du réseau. La fonctionnalité NAT Virtual Interface (NVI), identifiée par l'ajout d'une configuration `ip nat enable` aux interfaces qui appliquent NAT ou PAT, n'est pas prise en charge pour l'application NAT/PAT inter-VRF. Cette absence d'interopérabilité entre VRF Lite et NAT-Virtual Interface est suivie par la demande d'amélioration CSCek35625.

Configuration

Dans cette section, nous expliquons les configurations des pare-feu Cisco IOS Classic Firewall et VRF Zone-Based Policy Firewall.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) afin d'obtenir plus d'informations sur les commandes utilisées dans cette section.

Pare-feu classique Cisco IOS compatible VRF

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

Le pare-feu classique Cisco IOS VRF-Aware (anciennement CBAC), identifié par l'utilisation d'`ip inspect`, est disponible dans le logiciel Cisco IOS depuis que le pare-feu classique a été étendu pour prendre en charge l'inspection VRF dans le logiciel Cisco IOS Version 12.3(14)T.

Configuration du pare-feu classique Cisco IOS compatible VRF

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

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

Les paramètres d'inspection peuvent être modifiés pour chaque VRF avec des options de configuration spécifiques à VRF :

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

Les listes de stratégies d'inspection sont configurées globalement et une stratégie d'inspection peut être appliquée aux interfaces de plusieurs VRF.

Chaque VRF comporte son propre ensemble de paramètres d'inspection pour des valeurs telles que la protection par déni de service (DoS), les temporisateurs de session TCP/UDP/ICMP, les paramètres de piste d'audit, etc. Si une politique d'inspection est utilisée dans plusieurs VRF, la configuration de paramètre spécifique à VRF remplace toute configuration globale transportée par la politique d'inspection. Référez-vous à Cisco IOS Classic Firewall and Intrusion Prevention System Denial-of-Service Protection pour plus d'informations sur la façon de régler les paramètres de protection DoS.

Affichage de l'activité de pare-feu classique Cisco IOS VRF

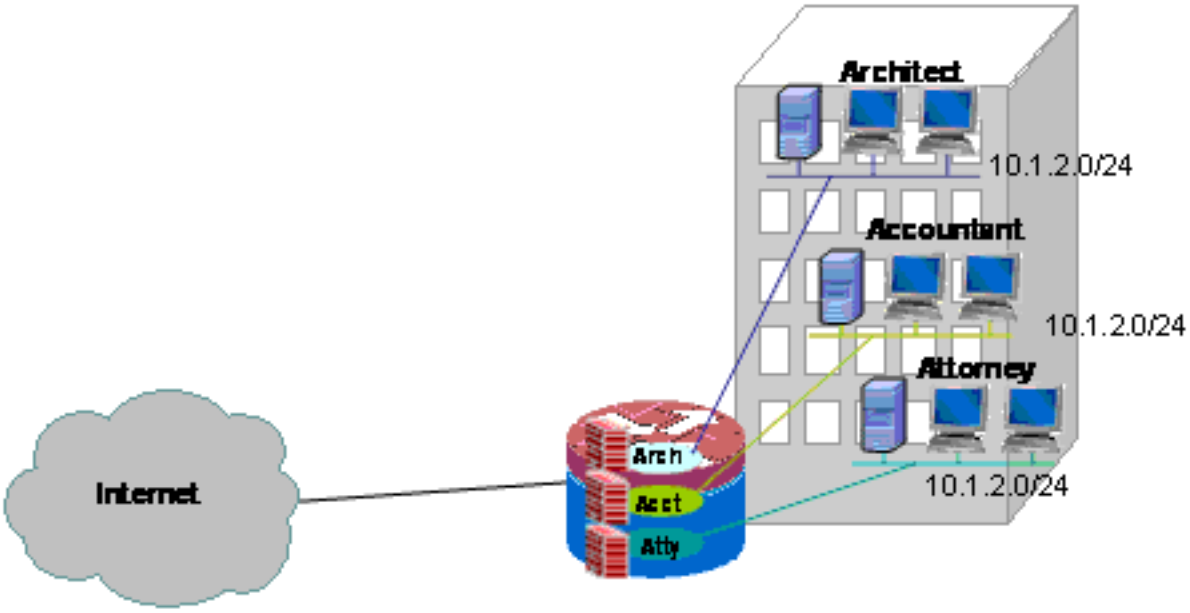
Le pare-feu VRF-Aware “ les commandes show ” diffèrent des commandes non VRF, car les commandes VRF-aware exigent que vous spécifiez le VRF dans la commande “ show ” :

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

Pare-feu classique multi-VRF à site unique

Les sites partagés qui offrent un accès Internet en tant que service partagé peuvent utiliser un pare-feu compatible VRF afin d'allouer un espace d'adressage qui se superpose et une politique de pare-feu standard pour tous les locataires. Les besoins en espace routable, en NAT, en accès à distance et en service VPN site à site peuvent être pris en charge, ainsi que l'offre de services personnalisés pour chaque locataire, avec l'avantage de fournir un VRF pour chaque client.

Cette application utilise un espace d'adressage qui se chevauche afin de simplifier la gestion de l'espace d'adressage. Mais cela peut causer des problèmes qui offrent une connectivité entre les différents VRF. Si la connectivité n'est pas requise entre les VRF, la NAT interne à externe traditionnelle peut être appliquée. Le transfert de port NAT est utilisé pour exposer les serveurs dans les VRF architecte (arch), comptable (acct) et avocat (atty). Les listes de contrôle d'accès et les politiques de pare-feu doivent prendre en charge l'activité NAT.



Configuration du pare-feu classique et de la fonction NAT pour un réseau classique multiVRF à site unique

Les sites partagés qui offrent un accès Internet en tant que service partagé peuvent utiliser un pare-feu compatible VRF pour allouer des espaces d'adressage qui se chevauchent et une politique de pare-feu standard pour tous les locataires. Les besoins en espace routable, en NAT, en accès à distance et en service VPN site à site peuvent être pris en charge, ainsi que l'offre de services personnalisés pour chaque locataire, avec l'avantage de fournir un VRF pour chaque client.

Une politique de pare-feu classique est en place, qui définit l'accès aux différentes connexions LAN et WAN et l'accès depuis ces connexions :

		Source de la connexion			
		Internet	Arche	Accéder	Tante
Destination de la connexion	Internet	S/O	HTTP,HTTPS FTP, DNS, SMTP	HTTP,HTTPS FTP, DNS, SMTP	HTTP,HTTPS FTP, DNS, SMTP
	Arche	FTP	S/O	Refuser	Refuser
	Accéder	SMTP	Refuser	S/O	Refuser
	Tant	HT	Refuser	Refuser	S/O

	e	TP SM TP			

Les hôtes de chacun des trois VRF peuvent accéder aux services HTTP, HTTPS, FTP et DNS sur l'Internet public. Une liste de contrôle d'accès (ACL 111) sera utilisée pour restreindre l'accès aux trois VRF (puisque chaque VRF autorise l'accès à des services identiques sur Internet), mais des politiques d'inspection différentes seront appliquées, afin de fournir des statistiques d'inspection par VRF. Des listes de contrôle d'accès distinctes peuvent être utilisées pour fournir des compteurs de liste de contrôle d'accès par VRF. Inversement, les hôtes sur Internet peuvent se connecter aux services comme décrit dans la table de stratégies précédente, comme défini par la liste de contrôle d'accès 121. Le trafic doit être inspecté dans les deux directions pour permettre le retour via des listes de contrôle d'accès qui protègent la connectivité dans la direction opposée. La configuration NAT est commentée pour décrire l'accès aux services transmis par port dans les VRF.

Configuration NAT et pare-feu classique multilocataire à site unique :

```
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
```

Vérification du pare-feu classique et de la fonction NAT pour un réseau classique à site unique multiVRF

La traduction d'adresses réseau et l'inspection du pare-feu sont vérifiées pour chaque VRF à l'aide des commandes suivantes :

Examinez les routes dans chaque VRF avec la commande **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 **show ip nat tra vrf [vrf-name]** :

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

Surveillez les statistiques d'inspection de pare-feu de chaque VRF à l'aide de la commande **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
```

Pare-feu IOS de politique basée sur la zone Cisco IOS compatible VRF

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

Si vous ajoutez Cisco IOS Zone-Based Policy Firewall aux configurations de routeurs à plusieurs VRF, cela n'a que peu de différence avec Zone Firewall dans les applications non VRF. En d'autres termes, la détermination des politiques respecte toutes les mêmes règles qu'observe un pare-feu de politiques basé sur des zones non VRF, sauf pour l'ajout de quelques stipulations spécifiques à plusieurs VRF :

- Une zone de sécurité Zone-Based Policy Firewall peut contenir des interfaces d'une seule zone.
- Un VRF peut contenir plusieurs zones de sécurité.
- Le pare-feu de stratégie basé sur les zones dépend du routage ou de la NAT afin de permettre au trafic de se déplacer entre les VRF. Une politique de pare-feu qui inspecte ou transmet le trafic entre les paires de zones VRF ne permet pas au trafic de se déplacer entre les VRF.

Configurer le pare-feu de stratégie basé sur les zones Cisco IOS compatible VRF

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

La configuration spécifique au VRF n'est pas nécessaire. Les paramètres de configuration globale sont appliqués, à moins qu'une carte-paramètre plus spécifique ne soit ajoutée à l'inspection sur une carte-politique. Même dans le cas où un paramètre-map est utilisé pour appliquer une configuration plus spécifique, le paramètre-map n'est pas spécifique à VRF.

Affichage de l'activité de pare-feu de stratégie basé sur la zone Cisco IOS sensible aux VRF

Les commandes **show** du pare-feu de stratégie basé sur une zone VRF ne diffèrent pas des commandes non compatibles VRF ; Le pare-feu de stratégie basé sur les zones applique le trafic qui passe des interfaces d'une zone de sécurité aux interfaces d'une autre zone de sécurité, indépendamment des affectations VRF de différentes interfaces. Ainsi, le pare-feu de stratégie basé sur une zone VRF utilise les mêmes commandes **show** afin d'afficher l'activité du pare-feu que le pare-feu de stratégie basé sur une zone dans les applications non VRF :

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

Exemples d'utilisation du pare-feu de stratégie basé sur la zone Cisco IOS compatible VRF

Les cas d'utilisation des pare-feu compatibles VRF varient considérablement. Ces exemples portent sur :

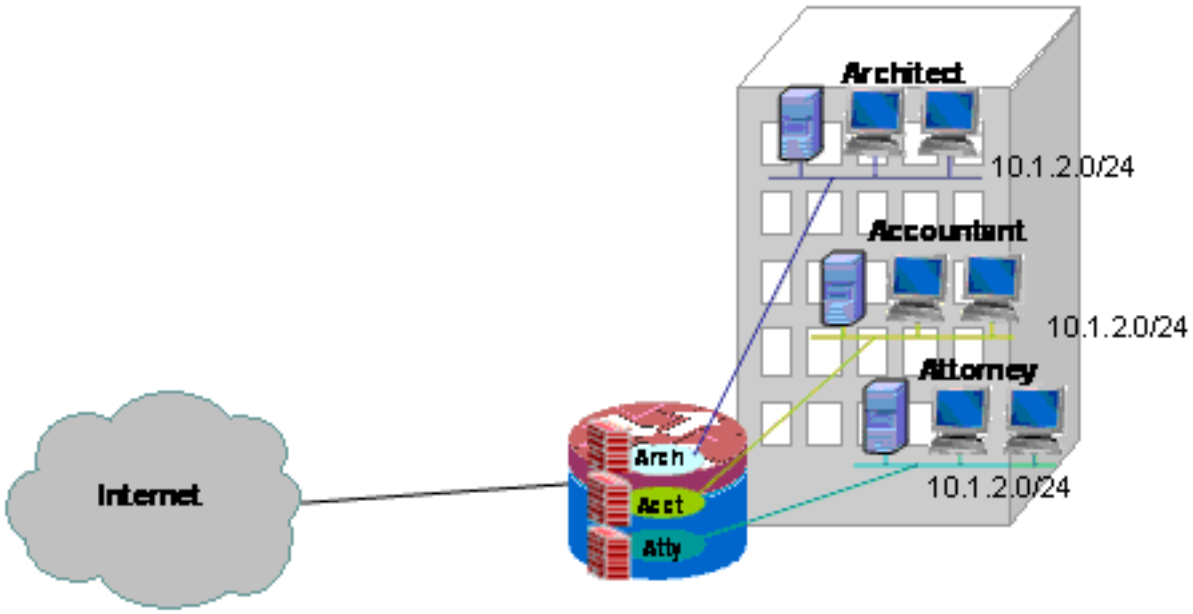
- Déploiement VRF sur un seul site, généralement utilisé pour les installations multilocataires ou les réseaux de vente au détail
- Application de filiale/de vente au détail/de télétravail dans laquelle le trafic de réseau privé est conservé dans un VRF distinct du trafic Internet public. Les utilisateurs d'accès à Internet sont

isolés des utilisateurs du réseau de l'entreprise et tout le trafic du réseau de l'entreprise est dirigé sur une connexion VPN au site HQ pour l'application de stratégie Internet.

Pare-feu de politique basé sur une zone de plusieurs VRF

Les sites partagés qui offrent un accès Internet en tant que service partagé peuvent utiliser un pare-feu compatible VRF pour allouer des espaces d'adressage qui se chevauchent et une politique de pare-feu standard pour tous les locataires. Cette application est typique de plusieurs réseaux locaux sur un site donné qui partage un routeur Cisco IOS pour l'accès à Internet, ou lorsqu'un partenaire commercial tel qu'un photofinisseur ou un autre service se voit proposer un réseau de données isolé avec une connectivité à Internet et une partie spécifique du réseau du propriétaire du site, sans nécessiter de matériel réseau supplémentaire ou de connectivité Internet. Les besoins en espace routable, en NAT, en accès à distance et en service VPN site à site peuvent être pris en charge, ainsi que l'offre de services personnalisés pour chaque locataire, avec l'avantage de fournir un VRF pour chaque client.

Cette application utilise un espace d'adressage qui se chevauche afin de simplifier la gestion de l'espace d'adressage. Mais cela peut causer des problèmes d'offre de connectivité entre les différents VRF. Si la connectivité n'est pas requise entre les VRF, la NAT interne à externe traditionnelle peut être appliquée. En outre, le transfert de port NAT est utilisé pour exposer les serveurs dans les VRF architecte (arch), comptable (acct) et avocat (atty). Les listes de contrôle d'accès et les politiques de pare-feu doivent prendre en charge l'activité NAT.



Configurer le pare-feu de stratégie de zone à site unique et NAT à plusieurs VRF

Les sites partagés offrant un accès Internet en tant que service partagé peuvent utiliser un pare-feu compatible VRF pour allouer des espaces d'adressage qui se chevauchent et une politique de pare-feu standard pour tous les locataires. Les besoins en espace routable, en NAT, en accès à distance et en service VPN site à site peuvent être pris en charge, ainsi que l'offre de services personnalisés pour chaque locataire, avec l'avantage de fournir un VRF pour chaque client.

Une politique de pare-feu classique est en place, qui définit l'accès aux différentes connexions LAN et WAN et l'accès depuis ces connexions :

		Source de la connexion			
		Internet	Arche	Accéder	Tante
Destination de la connexion	Internet	S/O	HTTP,HTTPS FTP, DNS, SMTP	HTTP,HTTPS FTP, DNS, SMTP	HTTP,HTTPS FTP, DNS, SMTP
	Arche	FTP	S/O	Refuser	Refuser
	Accéder	SMTP	Refuser	S/O	Refuser
	Tante	HTTP SMTP	Refuser	Refuser	S/O

Les hôtes de chacun des trois VRF peuvent accéder aux services HTTP, HTTPS, FTP et DNS sur l'Internet public. Une carte-classe (private-public-cmap) est utilisée pour restreindre l'accès aux trois VRF, puisque chaque VRF permet l'accès à des services identiques sur Internet, mais des cartes-politiques différentes sont appliquées, afin de fournir des statistiques d'inspection par VRF. Inversement, les hôtes sur Internet peuvent se connecter aux services comme décrit dans le tableau de stratégies précédent, tel que défini par les cartes-classes et les cartes-politiques individuelles pour les paires de zones Internet-VRF. Une carte-politique distincte est utilisée pour empêcher l'accès aux services de gestion du routeur dans la zone autonome à partir de l'Internet public. La même stratégie peut être appliquée pour empêcher l'accès des VRF privés à la zone autonome du routeur.

La configuration NAT est commentée pour décrire l'accès aux services transmis par port dans les VRF.

Configuration NAT et pare-feu de stratégie multilocataire à site unique :

```
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
```

Vérification du pare-feu classique et de la fonction NAT pour un réseau classique à site unique multiVRF

La traduction d’adresses réseau et l’inspection du pare-feu sont vérifiées pour chaque VRF à l’aide des commandes suivantes :

Examinez les routes dans chaque VRF avec la commande **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 à l'aide de la commande show ip nat tra vrf [vrf-name] :

```
stg-2801-L#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
```

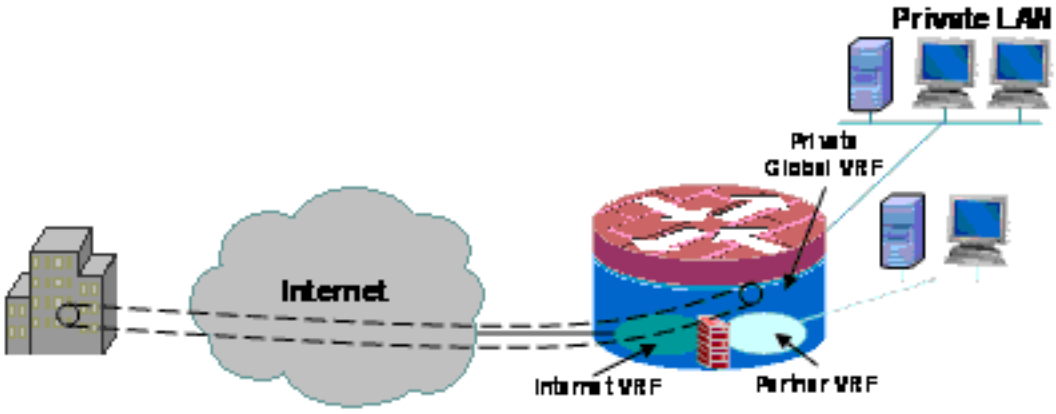
```
tcp 172.16.100.12:25   10.1.2.3:25        ---                ---
tcp 172.16.100.100:1033 10.1.2.3:1033     172.17.111.3:80    172.17.111.3:80
tcp 172.16.100.11:21   10.1.2.2:23        ---                ---
tcp 172.16.100.13:25   10.1.2.4:25        ---                ---
tcp 172.16.100.13:80   10.1.2.5:80        ---                ---
```

Surveillez les statistiques d'inspection du pare-feu avec les commandes **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
```

Pare-feu de stratégie à site unique VRF, connexion Internet avec sauvegarde dans “ zone ” Internet, VRF global a une connexion à HQ

Cette application est parfaitement adaptée aux déploiements de télétravailleurs, aux petits commerces et à tout autre déploiement de réseau de sites distants nécessitant une séparation des ressources de réseau privé et de l'accès au réseau public. En isolant la connectivité Internet et les utilisateurs de points d'accès publics ou privés à un VRF *public*, et en appliquant une route par défaut dans le VRF global qui achemine tout le trafic de réseau privé via des tunnels VPN, les ressources du VRF privé, global et du *VRF public* accessible à Internet n'ont aucune accessibilité l'une à l'autre, éliminant ainsi complètement la menace de compromission de l'hôte de réseau privé par l'activité Internet public. En outre, un VRF supplémentaire peut être provisionné pour fournir un espace de routage protégé aux autres consommateurs qui ont besoin d'un espace réseau isolé, tel que des terminaux de loterie, des distributeurs automatiques, des terminaux de traitement de cartes de débit ou d'autres applications. Plusieurs SSID Wi-Fi peuvent être configurés pour offrir un accès au réseau privé et à un point d'accès public.



Cet exemple décrit la configuration de deux connexions Internet haut débit, en appliquant la PAT (surcharge NAT) pour les hôtes des VRF *publics* et *partenaires* pour l'accès à l'Internet public, avec une connectivité Internet assurée par la surveillance SLA sur les deux connexions. Le réseau privé (dans le VRF global) utilise une connexion GRE sur IPsec pour maintenir la connectivité à HQ (configuration incluse pour le routeur de tête de réseau VPN) sur les deux liaisons haut débit. En cas d'échec d'une ou de l'autre des connexions haut débit, la connectivité à la tête de réseau VPN est maintenue, ce qui permet un accès ininterrompu au réseau HQ, puisque le point de terminaison local du tunnel n'est pas spécifiquement lié à aucune des connexions Internet.

Un pare-feu de stratégie basé sur une zone est en place et contrôle l'accès au réseau privé privé depuis et vers le réseau privé, et entre les réseaux locaux publics et partenaires et Internet afin de permettre l'accès Internet sortant, mais aucune connexion aux réseaux locaux à partir d'Internet :

	Internet	Public	Partenaire	VPN	Privé
Internet	S/O	Refuser	Refuser	Refuser	Refuser
Public	HTTP,HTTPS, FTP, DNS	S/O	Refuser	Refuser	Refuser
Partenaire		Refuser	S/O		
VPN	Refuser	Refuser	Refuser	S/O	
Privé	Refuser	Refuser	Refuser		S/O

L'application NAT pour le trafic de points d'accès et de réseaux partenaires rend les compromis provenant de l'Internet public beaucoup moins probables, mais il existe toujours la possibilité que des utilisateurs ou des logiciels malveillants puissent exploiter une session NAT active. L'application d'une inspection dynamique réduit les risques de compromission des hôtes locaux en attaquant une session NAT ouverte. Cet exemple utilise un 871W, mais la configuration peut être facilement répliquée avec d'autres plates-formes ISR.

Configuration du pare-feu de stratégie multi-VRF basé sur une zone unique, connexion Internet principale avec sauvegarde, VRF global a VPN vers HQ scénario

Les sites partagés qui offrent un accès Internet en tant que service partagé peuvent utiliser un pare-feu compatible VRF pour allouer des espaces d'adressage qui se chevauchent et une politique de pare-feu standard pour tous les locataires. Les besoins en espace routable, en NAT, en accès à distance et en service VPN site à site peuvent être pris en charge, ainsi que l'offre de services personnalisés pour chaque locataire, avec l'avantage de fournir 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 concentrateur fournit un exemple de 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
```

Vérifier le pare-feu de stratégie multi-VRF basé sur une zone unique, la connexion Internet principale avec la sauvegarde, le VRF global a VPN vers HQ scénario

La traduction d'adresses réseau et l'inspection du pare-feu sont vérifiées pour chaque VRF à l'aide des commandes suivantes :

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

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

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

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

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

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

Conclusion

Cisco IOS VRF-Aware Classic and Zone-Based Policy Firewall offre une réduction des coûts et de la charge administrative pour fournir une connectivité réseau avec une sécurité intégrée pour plusieurs réseaux avec un matériel minimal. Les performances et l'évolutivité sont maintenues pour plusieurs réseaux et fournissent une plate-forme efficace pour l'infrastructure et les services réseau sans augmentation des coûts d'investissement.

Vérification

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

Dépannage

Problème

Le serveur Exchange n'est pas accessible depuis l'interface externe du routeur.

Solution

Activez l'inspection SMTP dans le routeur afin de résoudre ce problème

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 de conception du pare-feu de stratégie basé sur les zones
- Utilisation du pare-feu de stratégie basé sur les zones avec VPN
- Pare-feu Cisco IOS compatible VRF
- Intégration de la NAT aux VPN MPLS
- Conception des extensions MPLS pour les routeurs de périphérie client
- Vérification de l'opération NAT et dépannage NAT de base
- Exemple de configuration de contexte multiple PIX/ASA
- Cisco IOS Firewall
- Support et documentation techniques - Cisco Systems