Konfigurationsbeispiel für die klassische und zonenbasierte virtuelle Firewall der Cisco IOS Firewall

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Hintergrundinformationen
Funktionsunterstützung
VRF-Konfiguration
Überblick über häufige Einsatzmöglichkeiten für VRF-sensitive IOS-Firewall
Nicht unterstützte Konfiguration
Konfigurieren
VRF-kompatible klassische Cisco IOS-Firewall
VRF-sensitive Cisco IOS zonenbasierte IOS-Firewall
Schlussfolgerung
Überprüfen
Fehlerbehebung
Zugehörige Informationen

Einführung

Dieses Dokument beschreibt den technischen Hintergrund zu VRF-fähigen virtuellen Firewall-Funktionen, das Konfigurationsverfahren und die Anwendungsfälle für verschiedene Anwendungsszenarien.

Mit der Cisco IOS® Softwareversion 12.3(14)T wurde eine virtuelle (VRF-kompatible) Firewall eingeführt, die die VRF-Funktionspalette (Virtual Routing-Forwarding) um Stateful Packet Inspection, transparente Firewall, Anwendungsinspektion und URL-Filterung ergänzt um bestehende VPN-, NAT-, QoS- und andere VRF-fähige Funktionen. In den meisten vorhersehbaren Anwendungsszenarien wird NAT mit anderen Funktionen angewendet. Wenn keine NAT erforderlich ist, kann das Routing zwischen VRFs angewendet werden, um VRF-übergreifende Verbindungen bereitzustellen. Die Cisco IOS-Software bietet VRF-fähige Funktionen sowohl in der klassischen Cisco IOS-Firewall als auch in der zonenbasierten Cisco IOS-Firewall. Beispiele für beide Konfigurationsmodelle finden Sie in diesem Dokument. Ein größerer Schwerpunkt liegt auf der zonenbasierten Firewall-Konfiguration.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Funktionsunterstützung

Die VRF-kompatible Firewall ist in Advanced Security-, Advanced IP Services- und Advanced Enterprise-Images sowie in älteren Nomenklatur-Images mit der *o3*-Kennzeichnung verfügbar, die die Integration des Funktionssatzes der Cisco IOS Firewall anzeigt. Die VRF-kompatible Firewall-Funktion wurde in Version 12.4 der Cisco IOS-Software-Mainline-Versionen zusammengefasst. Die Cisco IOS Softwareversion 12.4(6)T oder höher ist erforderlich, um eine VRF-sensitive zonenbasierte Firewall anzuwenden. Die zonenbasierte Cisco IOS-Firewall für Richtlinien funktioniert nicht mit Stateful Failover.

VRF-Konfiguration

Die Cisco IOS-Software verwaltet Konfigurationen für die globale VRF-Instanz und alle privaten VRF-Instanzen in derselben Konfigurationsdatei. Wenn auf die Router-Konfiguration über die Befehlszeilenschnittstelle zugegriffen wird, kann die in der CLI Views-Funktion angebotene rollenbasierte Zugriffskontrolle verwendet werden, um die Funktionalität von Router-Betriebs- und Verwaltungspersonal zu beschränken. Verwaltungsanwendungen wie Cisco Security Manager (CSM) bieten außerdem eine rollenbasierte Zugriffskontrolle, um sicherzustellen, dass das Betriebspersonal auf das entsprechende Leistungsniveau beschränkt ist.

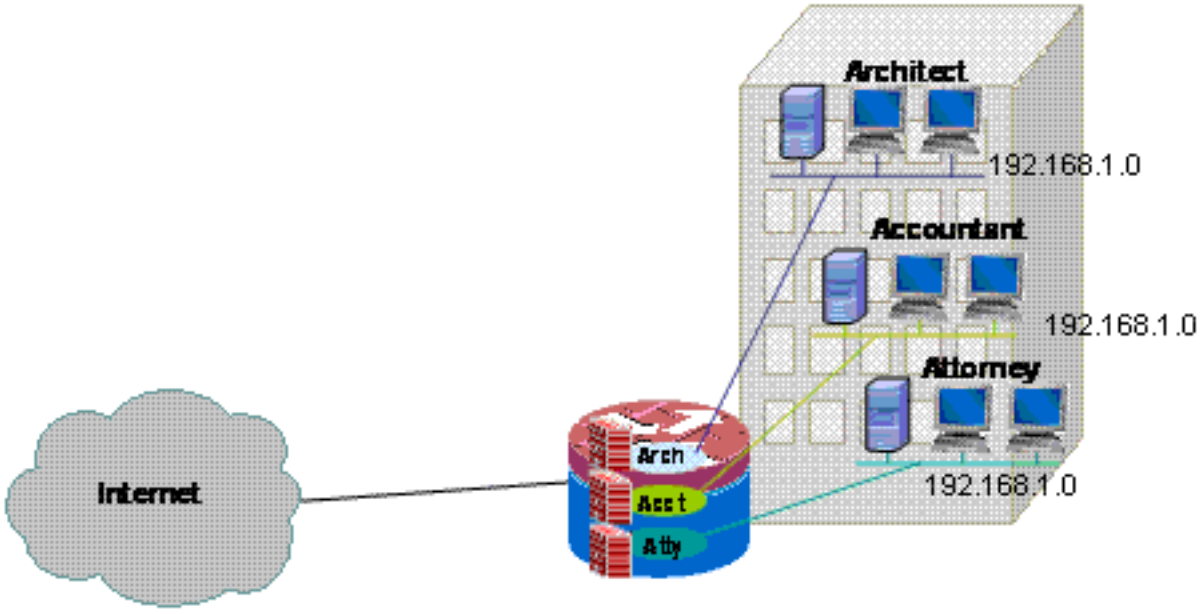
Überblick über häufige Einsatzmöglichkeiten für VRF-sensitive IOS-Firewall

Die VRF-kompatible Firewall ergänzt die Cisco IOS Virtual Routing/Forwarding (VRF)-Funktion um eine Stateful Packet Inspection. IPsec VPN, Network Address Translation (NAT)/Port Address Translation (PAT), Intrusion Prevention System (IPS) und andere Cisco IOS-Sicherheitsdienste können mit VRF-kompatibler Firewall kombiniert werden, um eine vollständige Reihe von Sicherheitsservices in VRFs bereitzustellen. VRFs unterstützen mehrere Routing-Bereiche, die eine überlappende IP-Adressennummerierung verwenden, sodass ein Router zur Trennung des Datenverkehrs in mehrere separate Routing-Instanzen aufgeteilt werden kann. Die VRF-

kompatible Firewall enthält in den Sitzungsinformationen ein VRF-Label für alle vom Router verfolgten Inspektionsaktivitäten, um eine Trennung zwischen Informationen zum Verbindungsstatus zu gewährleisten, die in jeder anderen Hinsicht identisch sein können. Die VRF-kompatible Firewall kann die Prüfung zwischen Schnittstellen innerhalb einer VRF-Instanz sowie zwischen Schnittstellen in VRF-Instanzen, die sich unterscheiden, z. B. bei Überschreitung von VRF-Grenzen durch den Datenverkehr, durchführen. So wird sowohl für den VRF-internen als auch für den VRF-internen Datenverkehr eine maximale Flexibilität bei der Firewall-Überprüfung erreicht.

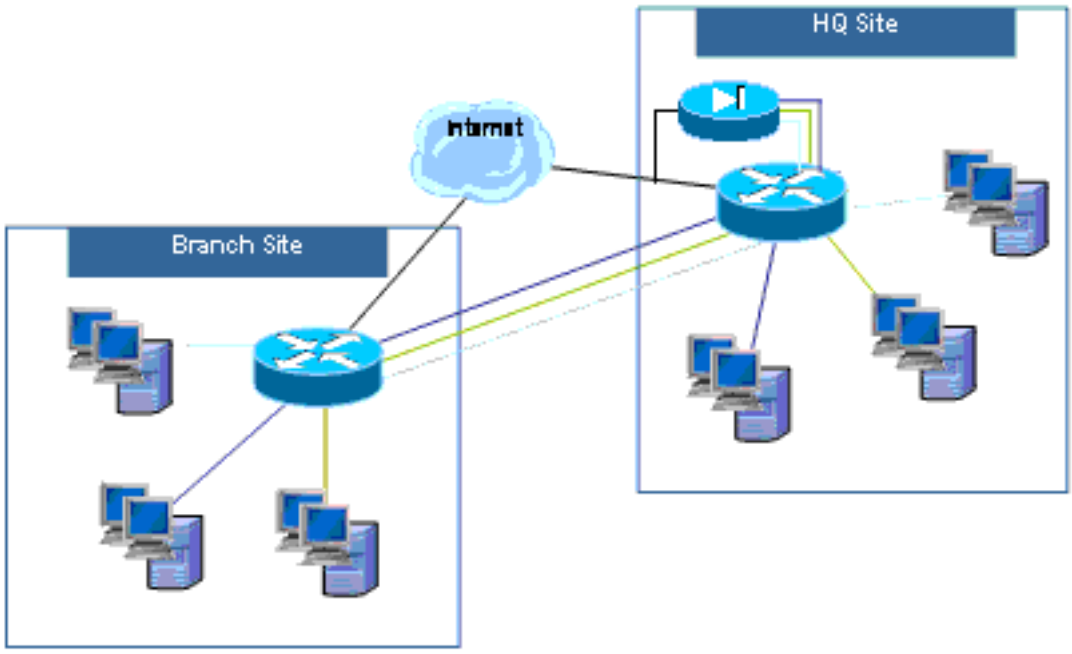
VRF-kompatible Cisco IOS Firewall-Anwendungen können in zwei grundlegende Kategorien eingeteilt werden:

- Multi-Tenant, ein Standort - Internetzugang für mehrere Tenants mit sich überschneidenden Adressräumen oder getrennten Routenräumen an einem Standort. Stateful-Firewall wird auf die Internetverbindungen jedes VRF angewendet, um die Wahrscheinlichkeit von Kompromittierungen durch offene NAT-Verbindungen weiter zu reduzieren. Port-Forwarding kann angewendet werden, um Verbindungen zu Servern in VRFs zu ermöglichen.



Ein Beispiel für eine Multi-Tenant-Anwendung an einem Standort für das VRF-sensitive Konfigurationsmodell für die klassische Firewall und das VRF-sensitive zonenbasierte Firewall-Konfigurationsmodell ist in diesem Dokument enthalten.

- Multi-Tenant, mehrere Standorte - Mehrere Tenants, die Geräte in einem großen Netzwerk gemeinsam nutzen, benötigen Verbindungen zwischen mehreren Standorten durch die Verbindung von VRFs von Tenants an verschiedenen Standorten über VPN- oder WAN-Verbindungen. Für jeden Tenant an mindestens einem Standort kann ein Internetzugang erforderlich sein. Um die Verwaltung zu vereinfachen, können mehrere Abteilungen ihre Netzwerke in einem Access Router für jeden Standort zusammenfassen. Verschiedene Abteilungen erfordern jedoch eine Trennung der Adressbereiche.



Konfiguration

sbeispiele für Multi-Tenant-Anwendungen mit mehreren Standorten für das Konfigurationsmodell "VRF-kompatible klassische Firewall" und das Konfigurationsmodell "VRF-kompatible zonenbasierte Firewall" werden in einer kommenden Aktualisierung dieses Dokuments bereitgestellt.

Nicht unterstützte Konfiguration

Die VRF-kompatible Firewall ist auf Cisco IOS-Images verfügbar, die Multi-VRF CE (VRF Lite) und MPLS VPN unterstützen. Firewall-Funktionen sind auf Nicht-MPLS-Schnittstellen beschränkt. Wenn also eine Schnittstelle an mit MPLS-Labels gekennzeichnetem Datenverkehr beteiligt ist, kann für diese Schnittstelle keine Firewall-Prüfung durchgeführt werden.

Ein Router kann nur dann VRF-internen Datenverkehr prüfen, wenn der Datenverkehr über eine Schnittstelle in eine VRF-Instanz gelangt oder diese verlässt, um eine Verbindung zu einer anderen VRF-Instanz herzustellen. Wenn der Datenverkehr direkt an eine andere VRF-Instanz weitergeleitet wird, gibt es keine physische Schnittstelle, über die eine Firewall-Richtlinie den Datenverkehr überprüfen kann. Der Router kann daher keine Überprüfung durchführen.

Die VRF Lite-Konfiguration ist nur dann mit NAT/PAT kompatibel, wenn `ip nat inside` oder `ip nat outside` auf Schnittstellen konfiguriert ist, auf denen NAT/PAT angewendet wird, um Quell- oder Zieladressen oder Portnummern für Netzwerkaktivitäten zu ändern. Die NAT Virtual Interface (NVI)-Funktion, die durch Hinzufügen einer `ip nat enable`-Konfiguration für Schnittstellen identifiziert wird, die NAT oder PAT anwenden, wird für VRF NAT/PAT-übergreifende Anwendungen nicht unterstützt. Dieser Mangel an Interoperabilität zwischen VRF Lite und NAT-Virtual Interface wird durch die Erweiterungsanfrage CSCek35625 nachverfolgt.

Konfigurieren

In diesem Abschnitt werden die VRF-kompatiblen Cisco IOS Classic Firewall- und VRF-kompatiblen zonenbasierten Firewall-Konfigurationen erläutert.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere

Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

VRF-kompatible klassische Cisco IOS-Firewall

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Die Cisco IOS VRF-kompatible klassische Firewall (ehemals CBAC), die durch die Verwendung von `ip inspect` identifiziert wird, ist in der Cisco IOS-Software verfügbar, seit die klassische Firewall um die VRF-kompatible Prüfung in Version 12.3(14)T der Cisco IOS-Software erweitert wurde.

Konfigurieren der Cisco IOS VRF-kompatiblen klassischen Firewall

Die VRF-kompatible klassische Firewall verwendet für die Konfiguration der Prüfrichtlinie dieselbe Konfigurationssyntax wie eine Nicht-VRF-Firewall:

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

Prüfparameter können für jede VRF-Instanz mit VRF-spezifischen Konfigurationsoptionen geändert werden:

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

Die Listen der Überprüfungsrichtlinien werden global konfiguriert, und eine Prüfrichtlinie kann auf Schnittstellen in mehreren VRFs angewendet werden.

Jede VRF-Instanz verfügt über eigene Prüfparameter für Werte wie DoS-Schutz (Denial-of-Service), TCP/UDP/ICMP-Sitzungs-Timer, Prüfpfadeinstellungen usw. Wenn eine Prüfrichtlinie in mehreren VRF-Instanzen verwendet wird, setzt die VRF-spezifische Parameterkonfiguration alle globalen Konfigurationen außer Kraft, die von der Prüfrichtlinie übernommen werden. Weitere Informationen zur Abstimmung von DoS-Schutzparametern finden Sie unter Cisco IOS Classic Firewall und Intrusion Prevention System Denial-of-Service Protection.

Anzeigen der klassischen Firewall-Aktivität von Cisco IOS VRF

Die Befehle "show" der VRF-fähigen Firewall unterscheiden sich von nicht VRF-kompatiblen Befehlen, da für VRF-kompatible Befehle die Angabe der VRF-Instanz im Befehl "show" erforderlich ist:

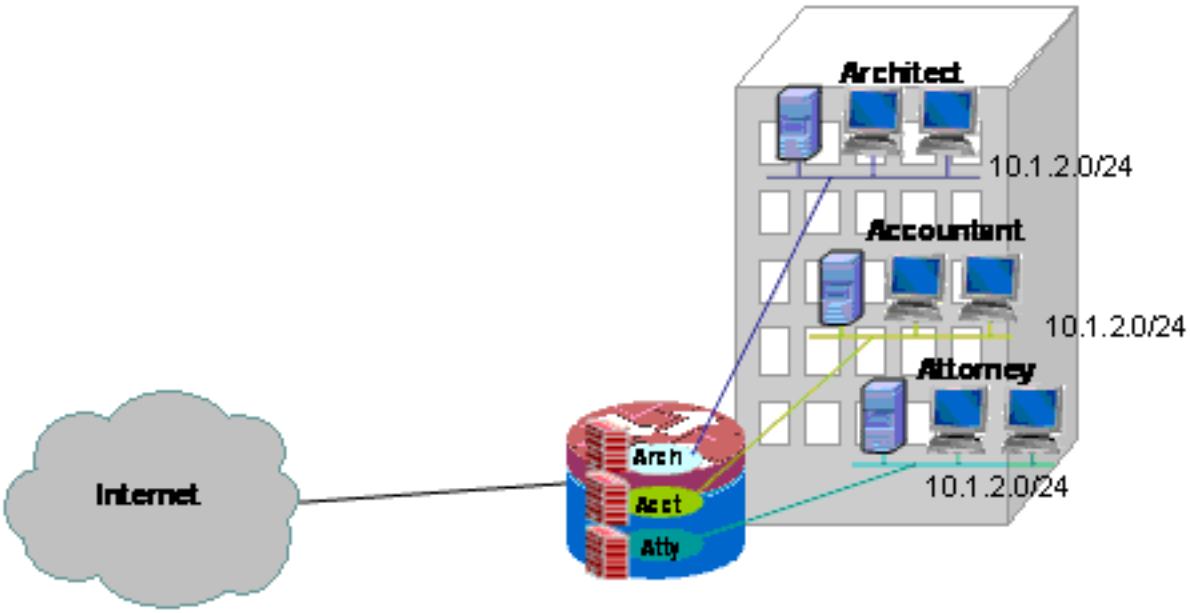
```
router#show ip inspect [ all | config | interfaces | name |
sessions | statistics ] vrf vrf-name
```

Klassische Firewall mit mehreren VRF-Instanzen

Multi-Tenant-Standorte, die als Tenant-Service Internetzugang bieten, können VRF-kompatible Firewall verwenden, um überlappenden Adressraum und eine Standardtext-Firewall-Richtlinie für alle Tenants zuzuweisen. Anforderungen an routingfähigen Speicherplatz, NAT, Remote-Zugriff

und Site-to-Site-VPN-Service können ebenso berücksichtigt werden wie das Angebot individueller Services für jeden Tenant, mit dem Vorteil, dass für jeden Kunden ein VRF bereitgestellt wird.

Diese Anwendung verwendet überlappende Adressbereiche, um das Adressraummanagement zu vereinfachen. Dies kann jedoch zu Problemen führen, die die Verbindung zwischen den verschiedenen VRFs ermöglichen. Wenn zwischen den VRFs keine Verbindung erforderlich ist, kann eine herkömmliche NAT für interne und externe Verbindungen angewendet werden. Die NAT-Port-Forwarding wird verwendet, um Server in den VRFs für Architekten (Architektur), Buchhalter (Akt) und Anwalt (Anwalt) verfügbar zu machen. Firewall-ACLs und -Richtlinien müssen NAT-Aktivitäten berücksichtigen.



Klassische Firewall und NAT für ein Classic Network mit mehreren VRF-Instanzen konfigurieren

Multi-Tenant-Standorte, die als Tenant-Service Internetzugang bieten, können mithilfe der VRF-kompatiblen Firewall überlappenden Adressbereich zuweisen und eine Standardtext-Firewall-Richtlinie für alle Tenants erstellen. Anforderungen an routingfähigen Speicherplatz, NAT, Remote-Zugriff und Site-to-Site-VPN-Service können ebenso berücksichtigt werden wie das Angebot individueller Services für jeden Tenant, mit dem Vorteil, dass für jeden Kunden ein VRF bereitgestellt wird.

Eine Klassische Firewall-Richtlinie definiert den Zugriff auf und von den verschiedenen LAN- und WAN-Verbindungen:

		Verbindungsquelle			
		Internet	Arsch	Konto	Atty
Verbindungsziel	Internet	K/A	HTTP, HTTPS FTP, DNS, SMTP	HTTP, HTTPS FTP, DNS, SMTP	HTTP, HTTPS FTP, DNS, SMTP

	Arsch	FTP	K/A	Ablehnen	Ablehnen
	Konto	SMTP	Ablehnen	K/A	Ablehnen
	Atty	HTTP SMTP	Ablehnen	Ablehnen	K/A

Hosts in den drei VRF-Instanzen können im öffentlichen Internet auf HTTP-, HTTPS-, FTP- und DNS-Dienste zugreifen. Es wird eine Zugriffskontrollliste (ACL 111) verwendet, um den Zugriff für alle drei VRFs einzuschränken (da jede VRF-Instanz den Zugriff auf identische Dienste im Internet ermöglicht). Es werden jedoch unterschiedliche Überprüfungsrichtlinien angewendet, um VRF-Inspektionsstatistiken bereitzustellen. Separate ACLs können verwendet werden, um ACL-Zähler pro VRF bereitzustellen. Hosts im Internet dagegen können eine Verbindung zu Services herstellen, wie in der vorherigen Richtlinientabelle beschrieben, wie in ACL 121 definiert. Der Datenverkehr muss in beide Richtungen inspiziert werden, um die Rückleitung durch ACLs zu ermöglichen, die die Konnektivität in die entgegengesetzte Richtung schützen. Die NAT-Konfiguration beschreibt den Port-Weiterleitungszugriff auf Services in VRFs.

Klassische Firewall und NAT-Konfiguration für Multi-Tenant-Umgebungen mit einem Standort:

```
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
```

Klassische Firewall und NAT für ein Classic Network mit mehreren VRF-Instanzen überprüfen

Network Address Translation und Firewall Inspection für jedes VRF mit den folgenden Befehlen:

Untersuchen Sie Routen in jeder VRF-Instanz mit dem Befehl **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#
```

Überprüfen Sie die NAT-Aktivität der VRF-Instanzen mit dem Befehl **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
```

Überwachen Sie die Firewall-Überprüfungsstatistiken für jede VRF-Instanz mit dem Befehl **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
```

VRF-sensitive Cisco IOS zonenbasierte IOS-Firewall

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Wenn Sie Cisco IOS Zone-Based Policy Firewall zu Multi-VRF-Routerkonfigurationen hinzufügen, unterscheidet sich dies kaum von Zone Firewall in Nicht-VRF-Anwendungen. D. h. bei der Richtlinienbestimmung werden dieselben Regeln beachtet, die auch von einer zonenbasierten Firewall ohne VRF-Instanz beachtet werden, außer bei der Ergänzung um einige Multi-VRF-spezifische Vorgaben:

- Eine Zone-Based Policy Firewall-Sicherheitszone kann Schnittstellen aus nur einer Zone enthalten.
- Eine VRF-Instanz kann mehr als eine Sicherheitszone enthalten.
- Zonenbasierte Richtlinien-Firewall hängt vom Routing oder NAT ab, damit der Datenverkehr zwischen VRFs verschoben werden kann. Eine Firewall-Richtlinie, die den Datenverkehr zwischen VRF-Zonenpaaren prüft oder weiterleitet, reicht nicht aus, um den Datenverkehr zwischen VRF-Instanzen zu ermöglichen.

Konfigurieren einer VRF-kompatiblen zonenbasierten Cisco IOS-Firewall

Die VRF-basierte zonenbasierte Firewall verwendet dieselbe Konfigurationssyntax wie die nicht VRF-sensitive zonenbasierte Firewall und weist Sicherheitszonen Schnittstellen zu, definiert Sicherheitsrichtlinien für Datenverkehr, der zwischen Zonen fließt, und weist die Sicherheitsrichtlinie den entsprechenden Zonenpaarzuordnungen zu.

Eine VRF-spezifische Konfiguration ist nicht erforderlich. Globale Konfigurationsparameter werden angewendet, es sei denn, der Inspektion auf einer Richtlinienzuordnung wird eine spezifischere Parameterzuordnung hinzugefügt. Auch wenn eine Parameterzuordnung zur Anwendung einer spezifischeren Konfiguration verwendet wird, ist die Parameterzuordnung nicht VRF-spezifisch.

Anzeigen von VRF-sensiblen zonenbasierten Cisco IOS Firewall-Aktivitäten

VRF-sensitive zonenbasierte Firewall-**Anzeigebefehle** unterscheiden sich nicht von nicht VRF-kompatiblen Befehlen. Die zonenbasierte Firewall wendet Datenverkehr an, der von Schnittstellen in einer Sicherheitszone zu Schnittstellen in einer anderen Sicherheitszone wechselt, unabhängig von den VRF-Zuweisungen verschiedener Schnittstellen. Daher verwendet die VRF-sensitive zonenbasierte Firewall die gleichen **show-**Befehle, um Firewall-Aktivitäten anzuzeigen, die von zonenbasierten Richtlinien-Firewalls in Nicht-VRF-Anwendungen verwendet werden:

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

VRF-kompatible zonenbasierte Cisco IOS Firewall-Anwendungsfälle

VRF-kompatible Firewall-Anwendungsfälle unterscheiden sich erheblich. In diesen Beispielen werden folgende Themen behandelt:

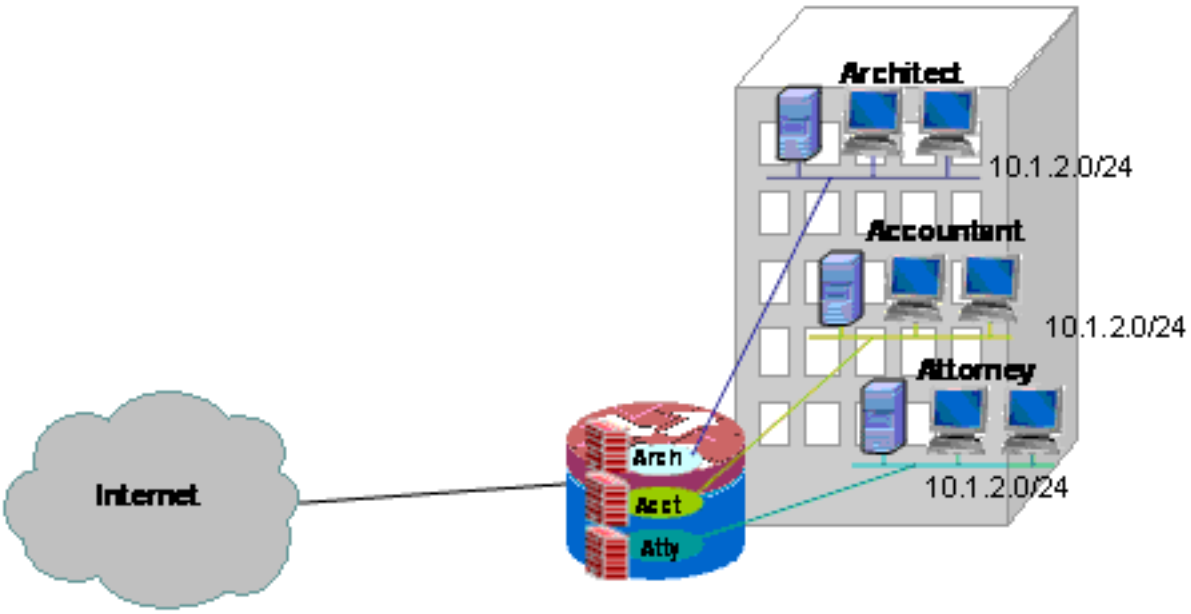
- Eine VRF-basierte Bereitstellung an einem Standort, die in der Regel für Multi-Tenant-

Anlagen oder Netzwerke im Einzelhandel verwendet wird
- Eine Anwendung für Zweigstellen/Einzelhandel/Telearbeiter, bei der der private Netzwerkverkehr in einer separaten VRF-Instanz vom öffentlichen Internetdatenverkehr getrennt gehalten wird. Internetzugriffsbenutzer sind von Geschäftsnetzwerkbenutzern isoliert, und der gesamte geschäftliche Netzwerkverkehr wird für die Anwendung von Internetrichtlinien über eine VPN-Verbindung mit dem Hauptsitz geleitet.

Multi-VRF, zonenbasierte Firewall mit einem Standort

Multi-Tenant-Standorte, die als Tenant-Service Internetzugang bieten, können mithilfe der VRF-kompatiblen Firewall überlappenden Adressbereich zuweisen und eine Standardtext-Firewall-Richtlinie für alle Tenants erstellen. Diese Anwendung ist typisch für mehrere LANs an einem Standort, die einen Cisco IOS-Router für den Internetzugriff gemeinsam nutzen, oder wenn einem Geschäftspartner wie einem Fotofinisher oder einem anderen Service ein isoliertes Datennetzwerk mit Internetverbindung und einem bestimmten Teil des Netzwerks des Eigentümers des Standorts angeboten wird, ohne dass zusätzliche Netzwerkhardware oder Internetverbindung erforderlich sind. Anforderungen an routingfähigen Speicherplatz, NAT, Remote-Zugriff und Site-to-Site-VPN-Service können ebenso berücksichtigt werden wie das Angebot individueller Services für jeden Tenant, mit dem Vorteil, dass für jeden Kunden ein VRF bereitgestellt wird.

Diese Anwendung verwendet überlappende Adressbereiche, um das Adressraummanagement zu vereinfachen. Dies kann jedoch zu Problemen bei der Anbindung zwischen den verschiedenen VRFs führen. Wenn zwischen den VRFs keine Verbindung erforderlich ist, kann eine herkömmliche NAT für interne und externe Verbindungen angewendet werden. Darüber hinaus wird die NAT-Port-Forwarding verwendet, um Server in den VRFs von Architect (arch), Accountant (acct) und Anwalt (attty) verfügbar zu machen. Firewall-ACLs und -Richtlinien müssen NAT-Aktivitäten berücksichtigen.



Konfiguration einer zonenbasierten Multi-VRF-Firewall und NAT für einen Standort

Multi-Tenant-Standorte, die als Tenant-Service Internetzugang bieten, können mithilfe der VRF-kompatiblen Firewall überlappenden Adressbereich zuweisen und eine Firewall-Standardrichtlinie für alle Tenants erstellen. Anforderungen an routingfähigen Speicherplatz, NAT, Remote-Zugriff und Site-to-Site-VPN-Service können ebenso berücksichtigt werden wie das Angebot individueller

Services für jeden Tenant, mit dem Vorteil, dass für jeden Kunden ein VRF bereitgestellt wird.

Eine Klassische Firewall-Richtlinie definiert den Zugriff auf und von den verschiedenen LAN- und WAN-Verbindungen:

		Verbindungsquelle			
		Internet	Arsch	Konto	Atty
Verbindungsziel	Internet	K/A	HTTP, HTTPS FTP, DNS, SMTP	HTTP, HTTPS FTP, DNS, SMTP	HTTP, HTTPS FTP, DNS, SMTP
	Arsch	FTP	K/A	Ablehnen	Ablehnen
	Konto	SMTP	Ablehnen	K/A	Ablehnen
	Atty	HTTP SMTP	Ablehnen	Ablehnen	K/A

Hosts in den drei VRF-Instanzen können im öffentlichen Internet auf HTTP-, HTTPS-, FTP- und DNS-Dienste zugreifen. Eine Klassenzuordnung (private-public-cmap) wird verwendet, um den Zugriff für alle drei VRFs zu beschränken, da jede VRF-Instanz den Zugriff auf identische Dienste im Internet ermöglicht. Es werden jedoch verschiedene Richtlinienzuweisungen angewendet, um VRF-Inspektionsstatistiken bereitzustellen. Hosts im Internet können hingegen eine Verbindung zu Services herstellen, wie in der vorherigen Richtlinientabelle beschrieben. Diese Funktion wird durch individuelle Klassenzuordnungen und Richtlinienzuordnungen für Internet-to-VRF-Zonenpaare definiert. Mithilfe einer separaten Richtlinienzuweisung wird der Zugriff auf die Verwaltungsdienste des Routers in der Selbstzone aus dem öffentlichen Internet verhindert. Dieselbe Richtlinie kann angewendet werden, um auch den Zugriff von privaten VRFs auf die Selbstzone des Routers zu verhindern.

Die NAT-Konfiguration beschreibt den Port-Weiterleitungszugriff auf Services in VRFs.

Multi-Tenant Zone-basierte Firewall und NAT-Konfiguration für einen Standort:

```
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
```

Klassische Firewall und NAT für ein Classic Network mit mehreren VRF-Instanzen überprüfen

Network Address Translation und Firewall Inspection für jedes VRF mit den folgenden Befehlen:

Untersuchen Sie Routen in jeder VRF-Instanz mit dem Befehl **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#
```

Überprüfen Sie die NAT-Aktivität der einzelnen VRF-Instanzen mit dem Befehl 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        ---                ---
```

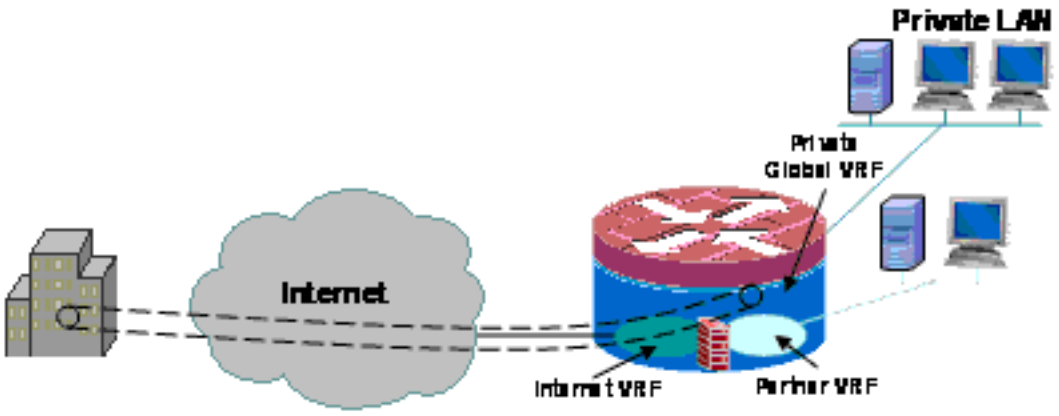
Überwachen Sie Firewall-Inspektionsstatistiken mit den Befehlen **show policy-map type inspect zone-pair**:

```
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 Zone Zone-Based Policy Firewall an einem Standort, Internetverbindung mit Backup in der "Internet"-Zone, globale VRF hat Verbindung zum Hauptsitz

Diese Anwendung eignet sich hervorragend für die Bereitstellung von Telearbeitern, kleinen Einzelhandelsstandorten und anderen Remote-Standorten, für die private Netzwerkressourcen vom öffentlichen Netzwerkzugriff getrennt werden müssen. Durch die Isolierung der Internetverbindung und der privaten oder öffentlichen Hotspot-Benutzer in eine *öffentliche* VRF-

Instanz und die Anwendung einer Standardroute in der globalen VRF-Instanz, die den gesamten privaten Netzwerkverkehr über VPN-Tunnel weiterleitet, sind die Ressourcen in der privaten, globalen VRF-Instanz und der *öffentlichen* VRF-Instanz *mit Internetzugang* nicht erreichbar, sodass die Gefahr durch private Hosts durch Aktivitäten vollständig beseitigt wird. Darüber hinaus kann eine zusätzliche VRF-Instanz bereitgestellt werden, um anderen Kunden, die einen isolierten Netzwerkbereich benötigen, einen geschützten Routenbereich bereitzustellen, z. B. Lotterieterminals, Geldautomaten, Terminals für die Kartenverarbeitung oder andere Anwendungen. Es können mehrere Wi-Fi-SSIDs bereitgestellt werden, um sowohl den Zugriff auf das private Netzwerk als auch auf einen öffentlichen Hotspot zu ermöglichen.



In diesem Beispiel wird die Konfiguration für zwei Breitband-Internetverbindungen beschrieben, wobei für Hosts in der *öffentlichen* und *Partner*-VRFs PAT (NAT-Overload) für den Zugriff auf das öffentliche Internet angewendet wird, wobei die Internetverbindung durch SLA-Überwachung auf den beiden Verbindungen gewährleistet wird. Das private Netzwerk (in der globalen VRF-Instanz) verwendet eine GRE-over-IPsec-Verbindung, um die Verbindung zum Hauptsitz (Konfiguration für den VPN-Headend-Router) über die beiden Breitbandverbindungen aufrechtzuerhalten. Falls eine der Breitbandverbindungen ausfällt, wird die Verbindung zum VPN-Headend aufrechterhalten, was einen unterbrechungsfreien Zugriff auf das HQ-Netzwerk ermöglicht, da der lokale Endpunkt des Tunnels nicht speziell an eine der Internetverbindungen gebunden ist.

Es ist eine zonenbasierte Richtlinien-Firewall vorhanden, die den Zugriff auf das und vom VPN zum privaten Netzwerk sowie zwischen den öffentlichen und Partner-LANs und dem Internet steuert, um einen ausgehenden Internetzugang zu ermöglichen, jedoch keine Verbindungen zu den lokalen Netzwerken aus dem Internet:

	Internet	Öffentlich	Partner	VPN	Privat
Internet	K/A	Ablehnen	Ablehnen	Ablehnen	Ablehnen
Öffentlich	HTTP, HTTPS, FTP, DNS	K/A	Ablehnen	Ablehnen	Ablehnen
Partner		Ablehnen	K/A		
VPN	Ablehnen	Ablehnen	Ablehnen	K/A	

Privat	Ablehnen	Ablehnen	Ablehnen		K/A

NAT-Anwendung für Hotspot- und Partner-Net-Datenverkehr beeinträchtigt die Wahrscheinlichkeit von Kompromittierungen aus dem öffentlichen Internet sehr viel weniger, aber es besteht weiterhin die Möglichkeit, dass böswillige Benutzer oder Software eine aktive NAT-Sitzung ausnutzen können. Die Anwendung einer Stateful Inspection minimiert die Wahrscheinlichkeit, dass lokale Hosts durch Angriffe auf eine offene NAT-Sitzung kompromittiert werden. In diesem Beispiel wird ein 871W-Wert verwendet, die Konfiguration kann jedoch problemlos mit anderen ISR-Plattformen repliziert werden.

Konfiguration einer zonenbasierten Multi-VRF-Firewall für einen Standort, einer primären Internetverbindung mit Backup; für die globale VRF-Instanz gilt das Szenario "VPN-zu-HQ".

Multi-Tenant-Standorte, die als Tenant-Service Internetzugang bieten, können mithilfe der VRF-kompatiblen Firewall überlappenden Adressbereich zuweisen und eine Standardtext-Firewall-Richtlinie für alle Tenants erstellen. Anforderungen an routingfähigen Speicherplatz, NAT, Remote-Zugriff und Site-to-Site-VPN-Service können ebenso berücksichtigt werden wie das Angebot individueller Services für jeden Tenant, mit dem Vorteil, dass für jeden Kunden ein VRF bereitgestellt wird.

```
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
```

Diese Hub-Konfiguration bietet ein Beispiel für die VPN-Verbindungskonfiguration:

```
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
```

Verifizierung der Multi-VRF-Firewall für eine Zone-Based-Policy-Firewall an einem Standort, primäre Internetverbindung mit Backup, globale VRF-Instanz verfügt über VPN-zu-HQ-Szenario

Network Address Translation und Firewall Inspection für jedes VRF mit den folgenden Befehlen:

Untersuchen Sie Routen in jeder VRF-Instanz mit dem Befehl **show ip route vrf [vrf-name]**:

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

Überprüfen Sie die NAT-Aktivität der einzelnen VRF-Instanzen mit dem Befehl **show ip nat tra vrf [vrf-name]:**

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

Überwachen Sie Firewall-Inspektionsstatistiken mit den Befehlen **show policy-map type inspect zone-pair**:

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

Schlussfolgerung

Die Cisco IOS VRF-kompatible klassische und zonenbasierte Firewall bietet einen geringeren Kosten- und Verwaltungsaufwand für die Bereitstellung von Netzwerkverbindungen mit integrierter Sicherheit für mehrere Netzwerke bei minimaler Hardware. Leistung und Skalierbarkeit werden für mehrere Netzwerke aufrechterhalten und bieten eine effektive Plattform für Netzwerkinfrastruktur und -services ohne Erhöhung der Kapitalkosten.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Problem

Der Zugriff auf den Exchange-Server ist von der externen Schnittstelle des Routers aus nicht möglich.

Lösung

Aktivieren Sie die SMTP-Inspektion im Router, um dieses Problem zu beheben.

Beispielkonfiguration

```
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
```

Zugehörige Informationen

- Designleitfaden für zonenbasierte Firewall-Richtlinien
- Verwendung einer zonenbasierten Firewall mit VPN

- VRF-kompatible Cisco IOS-Firewall
- Integration von NAT in MPLS-VPNs
- Entwerfen von MPLS-Erweiterungen für Edge-Router von Kunden
- Überprüfung des NAT-Betriebs und der grundlegenden NAT-Fehlerbehebung
- Konfigurationsbeispiel für PIX/ASA mit mehreren Kontexten
- Cisco IOS-Firewall
- Technischer Support und Dokumentation - Cisco Systems