

Cisco IOS Firewall Classic and Zone–Based Virtual Firewall Application Configuration Example

Document ID: 100595

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Background Information

- Feature Support

- VRF Configuration

Overview of Common Uses for VRF–Aware IOS Firewall

Unsupported Configuration

Configure

- VRF–Aware Cisco IOS Classic Firewall

- VRF–Aware Cisco IOS Zone–Based Policy IOS Firewall

- Conclusion

Verify

Troubleshoot

Related Information

Introduction

Cisco IOS® Software Release 12.3(14)T introduced Virtual (VRF–aware) Firewall, extending the Virtual Routing–Forwarding (VRF) feature family to offer stateful packet inspection, transparent firewall, application inspection, and URL filtering, in addition to existing VPN, NAT, QoS, and other VRF–aware features. This document offers technical background on VRF–aware Virtual firewall features, configuration procedure, and use cases for various application scenarios. Most foreseeable application scenarios will apply NAT with other features. If NAT is not required, routing can be applied between VRFs to provide inter–VRF connectivity. Cisco IOS Software offers VRF–aware capabilities in both Cisco IOS Classic Firewall and Cisco IOS Zone–Based Policy Firewall, with examples of both configuration models provided in this document. A greater focus is placed on Zone–Based Policy Firewall Configuration.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

Feature Support

VRF-Aware Firewall is available in Advanced Security, Advanced IP Services, and Advanced Enterprise images, as well as legacy-nomenclature images that carry the *o3* designation, which indicates integration of the Cisco IOS Firewall Feature Set. VRF-Aware Firewall capability merged into Cisco IOS Software Mainline Releases in 12.4. Cisco IOS Software Release 12.4(6)T or later is required to apply VRF-Aware Zone-Based Policy Firewall.

VRF Configuration

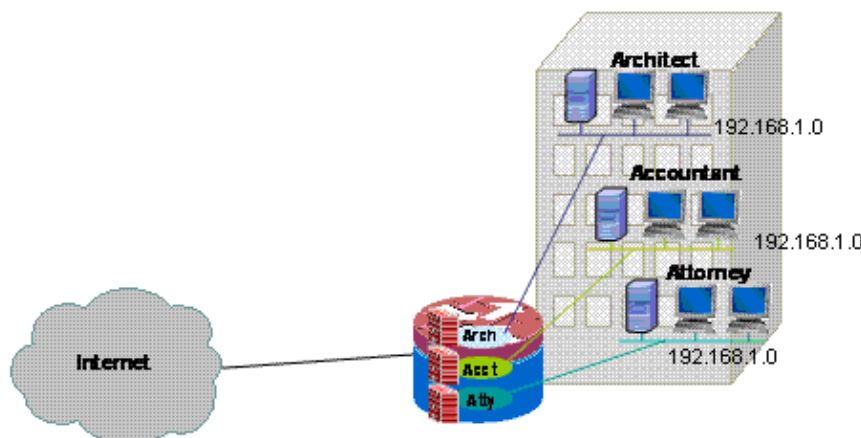
Cisco IOS Software maintains configurations for the global VRF and all private VRFs in the same configuration file. If the router configuration is accessed through the Command-Line Interface, role-based access control offered in the CLI Views feature can be used to limit the capability of router operational and management personnel. Management applications such as Cisco Security Manager (CSM) also provide role-based access control to assure that operational personnel are restricted to the appropriate level of capability.

Overview of Common Uses for VRF-Aware IOS Firewall

VRF-Aware Firewall adds stateful packet inspection to the Cisco IOS Virtual Routing/Forwarding (VRF) capability. IPsec VPN, Network Address Translation (NAT)/Port Address Translation (PAT), Intrusion Prevention System (IPS) and other Cisco IOS security services can be combined with VRF-Aware Firewall to provide a complete set of security services in VRFs. VRFs provide support for multiple route spaces that employ overlapping IP address numbering, so a router can be divided into multiple discrete routing instances for traffic separation. The VRF-Aware firewall includes a VRF label in session information for all inspection activity that the router is tracking, to maintain separation between connection state information that can be identical in every other respect. VRF-Aware firewall can inspect between interfaces within one VRF, as well as between interfaces in VRFs that differ, for example in cases where traffic crosses VRF boundaries, so that maximum firewall inspection flexibility is realized for both intra-VRF and inter-VRF traffic.

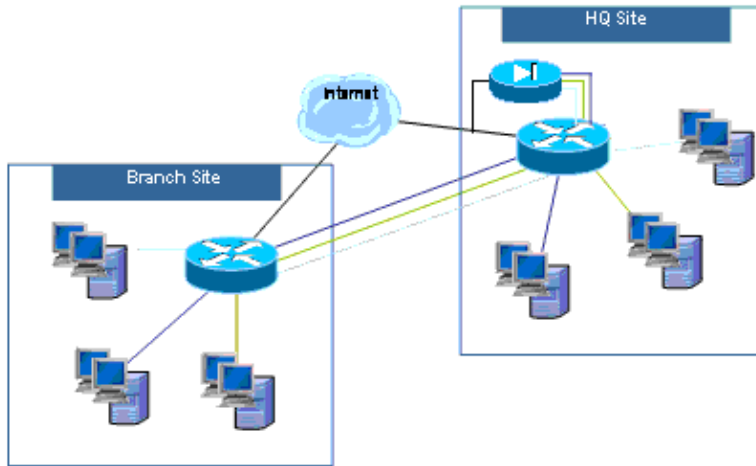
VRF-Aware Cisco IOS Firewall applications can be grouped into two basic categories:

- Multi-tenant, single-site Internet access for multiple tenants with overlapping address spaces or segregated route spaces at a single premise. Stateful firewall is applied to each VRF's internet connectivity to further reduce the likelihood of compromise through open NAT connections. Port-forwarding can be applied to allow connectivity to servers in VRFs.



An example of a multi-tenant single-site application for both VRF-Aware Classic Firewall configuration model and VRF-Aware Zone-Based Firewall configuration model is provided in this document.

- Multi-tenant, multi-site Multiple tenants that share equipment in a large network need connectivity between multiple sites by the connection of VRFs of tenants at different sites through VPN or WAN connections. Internet access can be required for each tenant at one or more sites. In order to simplify management, several departments can collapse their networks into one access router for each site, but various departments require address-space segregation.



Configuration examples for multi-tenant multi-site applications for both VRF-Aware Classic Firewall configuration model and VRF-Aware Zone-Based Firewall configuration model will be provided in a forthcoming update to this document.

Unsupported Configuration

VRF-Aware Firewall is available on Cisco IOS images that support Multi-VRF CE (VRF Lite) and MPLS VPN. Firewall capability is limited to non-MPLS interfaces. That is, if an interface will participate in MPLS-labeled traffic, firewall inspection cannot be applied on that interface.

A router can only inspect inter-VRF traffic if traffic must enter or leave a VRF through an interface to cross to a different VRF. If traffic is routed directly to another VRF, there is no physical interface where a firewall policy can inspect traffic, so the router is unable to apply inspection.

VRF Lite configuration is interoperable with NAT/PAT only if `ip nat inside` or `ip nat outside` is configured on interfaces where NAT/PAT is applied to modify source or destination addresses or port numbers for network activity. The NAT Virtual Interface (NVI) feature, identified by the addition of an `ip nat enable` configuration to interfaces that apply NAT or PAT, is not supported for inter-VRF NAT/PAT application. This lack of interoperability between VRF Lite and NAT-Virtual Interface is tracked by enhancement request CSCek35625.

Configure

In this section, the VRF-Aware Cisco IOS Classic Firewall and VRF-Aware Zone-Based Policy Firewall configurations are explained.

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

VRF-Aware Cisco IOS Classic Firewall

In this section, you are presented with the information to configure the features described in this document.

Cisco IOS VRF-Aware Classic Firewall (formerly called CBAC), which is identified by the use of `ip inspect`, has been available in Cisco IOS Software since the Classic Firewall was extended to support VRF-aware inspection in Cisco IOS Software Release 12.3(14)T.

Configure Cisco IOS VRF-Aware Classic Firewall

VRF-Aware Classic Firewall uses the same configuration syntax as non-VRF firewall for the configuration of the inspection policy:

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

Inspection parameters can be modified for each VRF with VRF-specific configuration options:

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

Inspection policy lists are configured globally, and an inspection policy can be applied to interfaces in multiple VRFs.

Each VRF carries its own set of inspection parameters for values such as denial-of-service (DoS) protection, TCP/UDP/ICMP session timers, audit-trail settings, etc. If one inspection policy is used in multiple VRFs, the VRF-specific parameter configuration supersedes any global configuration that is carried by the inspection policy. Refer to Cisco IOS Classic Firewall and Intrusion Prevention System Denial-of-Service Protection for more information on how to tune DoS protection parameters.

Viewing Cisco IOS VRF-Aware Classic Firewall Activity

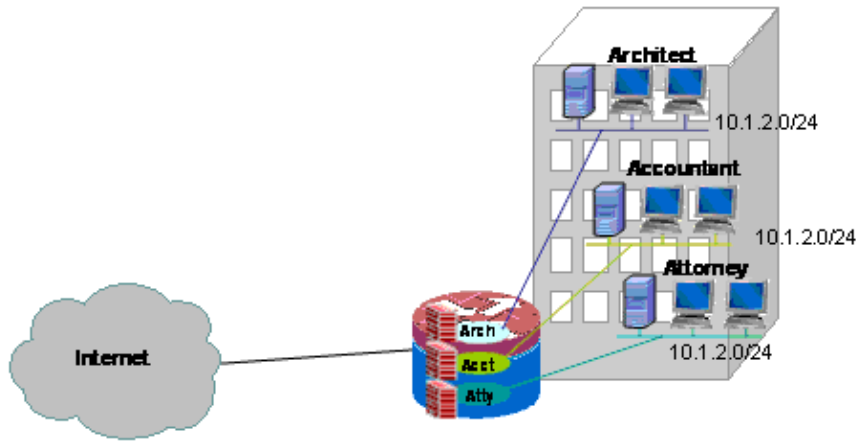
VRF-Aware Firewall `show` commands differ from non-VRF-aware commands, because VRF-aware commands require that you specify the VRF in the `show` command:

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

Multi-VRF Single-Site Classic Firewall

Multi-tenant sites that offer Internet access as a tenant service can use VRF-aware firewall in order to allocate overlapping address space and a boilerplate firewall policy for all tenants. Requirements for routable space, NAT, and remote-access and site-to-site VPN service can be accommodated as well to the offer of customized services for each tenant, with the benefit of provisioning a VRF for each customer.

This application uses overlapping address-space in order to simplify address space management. But, this can cause problems that offer connectivity between the various VRFs. If connectivity is not required between the VRFs, traditional inside-to-outside NAT can be applied. NAT port-forwarding is used to expose servers in the architect (arch), accountant (acct), and attorney (atty) VRFs. Firewall ACLs and policies must accommodate NAT activity.



Configure Classic Firewall and NAT for a Multi-VRF Single-Site Classic Network

Multi-tenant sites that offer Internet access as a tenant service can use VRF-aware firewall to allocate overlapping address space and a boilerplate firewall policy for all tenants. Requirements for routable space, NAT, and remote-access and site-to-site VPN service can be accommodated as well to the offer of customized services for each tenant, with the benefit of provisioning a VRF for each customer.

A Classic Firewall policy is in place, which defines access to and from the various LAN and WAN connections:

		Connection Source			
		Internet	Arch	Acct	Atty
Connection Destination	Internet	N/A	HTTP,HTTPS FTP, DNS, SMTP	HTTP,HTTPS FTP, DNS, SMTP	HTTP,HTTPS FTP, DNS, SMTP
	Arch	FTP	N/A	Deny	Deny
	Acct	SMTP	Deny	N/A	Deny
	Atty	HTTP SMTP	Deny	Deny	N/A

Hosts in each of the three VRFs are able to access HTTP, HTTPS, FTP, and DNS services on the public Internet. One Access-Control List (ACL 111) will be used to restrict access for all three VRFs (since each VRF allows access to identical services on the Internet), but different inspection policies will be applied, so as to provide per-VRF inspection statistics. Separate ACLs can be used to provide ACL counters per VRF. Inversely, hosts on the Internet can connect to services as described in the previous policy table, as defined by ACL 121. Traffic must be inspected in both directions to accommodate return through ACLs that protect connectivity in the opposite direction. NAT configuration is commented to describe port-forwarded access to services in VRFs.

Single-Site Multi-Tenant Classic Firewall and NAT Configuration:
<pre> version 12.4 ! ip cef ! ip vrf acct ! ip vrf arch </pre>

```
!  
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

```

Verify Classic Firewall and NAT for a Multi-VRF Single-Site Classic Network

Network Address Translation and Firewall inspection is verified for each VRF with these commands:

Examine routes in each VRF with the **show ip route vrf [vrf-name]** command:

```

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, NV10
    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#

```

Check the NAT activity of each VRF with **show ip nat tra vrf [vrf-name]** command:

```

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

```

Monitor the firewall inspection statistics of each VRF with the **show ip inspect vrf name** command:

```
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-Aware Cisco IOS Zone-Based Policy IOS Firewall

In this section, you are presented with the information to configure the features described in this document.

If you add Cisco IOS Zone-Based Policy Firewall to multi-VRF router configurations, this bears little difference from Zone Firewall in non-VRF applications. That is, policy determination observes all the same rules that a non-VRF Zone-Based Policy Firewall observes, save for the addition of a few multi-VRF-specific stipulations:

- A Zone-Based Policy Firewall security zone can contain interfaces from only one zone.
- A VRF can contain more than one security zone.
- Zone-Based Policy Firewall is dependent on routing or NAT in order to allow traffic to move between VRFs. A firewall policy that inspects or passes traffic between inter-VRF Zone-Pairs is not adequate to permit traffic to move between VRFs.

Configure VRF-Aware Cisco IOS Zone-Based Policy Firewall

VRF-Aware Zone-Based Policy Firewall uses the same configuration syntax as non-VRF-Aware Zone-Based Policy Firewall, and assigns interfaces to security zones, defines security policies for traffic that moves between zones, and assigns the security policy to the appropriate zone-pair associations.

VRF-specific configuration is unnecessary. Global configuration parameters are applied, unless a more specific parameter-map is added to inspection on a policy-map. Even in the case where a parameter-map is used to apply more specific configuration, the parameter-map is not VRF-specific.

Viewing VRF-Aware Cisco IOS Zone-Based Policy Firewall Activity

VRF-Aware Zone-Based Policy Firewall **show** commands are no different from non-VRF-aware commands; Zone-Based Policy Firewall applies traffic that moves from interfaces in one security zone to interfaces in another security zone, regardless of the VRF assignments of various interfaces. Thus, VRF-Aware Zone-Based Policy Firewall employs the same **show** commands in order to view firewall activity as are used by Zone-Based Policy Firewall in non-VRF applications:

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

VRF-Aware Cisco IOS Zone-Based Policy Firewall Use Cases

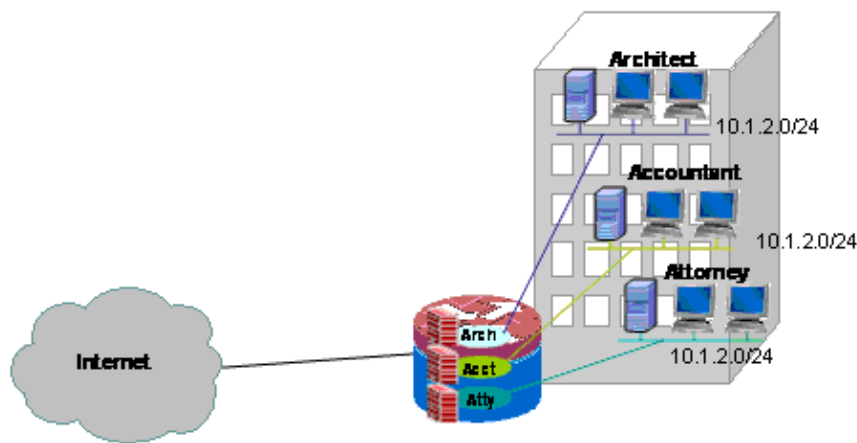
VRF-aware firewall use cases vary widely. These examples address:

- A single-site VRF-aware deployment, typically used for multi-tenant facilities or retail networks
- A branch office/retail/telecommuter application where private-network traffic is kept in a separate VRF from public-internet traffic. Internet-access users are isolated from business-network users, and all business-network traffic is directed over a VPN connection to the HQ site for Internet policy application.

Multi-VRF Single-Site Zone-Based Policy Firewall

Multi-tenant sites that offer Internet access as a tenant service can use VRF-aware firewall to allocate overlapping address space and a boilerplate firewall policy for all tenants. This application is typical for multiple LANs at a given site that shares one Cisco IOS router for Internet access, or where a business partner such as a photofinisher or some other service is offered an isolated data network with connectivity to the internet and some specific part of the network of the premise owner, without the requirement of additional network hardware or Internet connectivity. Requirements for routable space, NAT, and remote-access and site-to-site VPN service can be accommodated as well to the offer of customized services for each tenant, with the benefit of provisioning a VRF for each customer.

This application uses overlapping address-space in order to simplify address space management. But, this can cause problems offering connectivity between the various VRFs. If connectivity is not required between the VRFs, traditional inside-to-outside NAT can be applied. Additionally, NAT port-forwarding is used to expose servers in the architect (arch), accountant (acct), and attorney (atty) VRFs. Firewall ACLs and policies must accommodate NAT activity.



Configure Multi-VRF Single-Site Zone-Based Policy Firewall and NAT

Multi-tenant sites offering Internet access as a tenant service can use VRF-aware firewall to allocate overlapping address space and a boilerplate firewall policy for all tenants. Requirements for routable space, NAT, and remote-access and site-to-site VPN service can be accommodated as well to the offer of customized services for each tenant, with the benefit of provisioning a VRF for each customer.

A Classic Firewall policy is in place, which defines access to and from the various LAN and WAN connections:

		Connection Source			
		Internet	Arch	Acct	Atty
Connection Destination	Internet	N/A	HTTP,HTTPS FTP, DNS, SMTP	HTTP,HTTPS FTP, DNS, SMTP	HTTP,HTTPS FTP, DNS, SMTP
	Arch	FTP	N/A	Deny	Deny
	Acct	SMTP	Deny	N/A	Deny
	Atty	HTTP SMTP	Deny	Deny	N/A

Hosts in each of the three VRFs are able to access HTTP, HTTPS, FTP, and DNS services on the public Internet. One class-map (private-public-cmap) is used to restrict access for all three VRFs, since each VRF allows access to identical services on the Internet, but different polic-maps are applied, so as to provide per-VRF inspection statistics. Inversely, hosts on the Internet can connect to services as described in the previous policy table, as defined by individual class-maps and policy-maps for Internet-to-VRF zone-pairs. A separate policy-map is used to prevent access to the management services of the router in the self-zone from the public internet. The same policy can be applied to prevent access from the private VRFs to the self-zone of the router as well.

NAT configuration is commented to describe port-forwarded access to services in VRFs.

Single-Site Multi-Tenant Zone-Based Policy Firewall and NAT Configuration:

```
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

```

Verify Classic Firewall and NAT for a Multi-VRF Single-Site Classic Network

Network Address Translation and Firewall inspection is verified for each VRF with these commands:

Examine routes in each VRF with the **show ip route vrf [vrf-name]** command:

```
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, NV10
```

```
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#
```

Check each VRF s NAT activity with the show ip nat tra vrf [vrf-name] command:

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

Monitor firewall inspection statistics with the show policy-map type inspect zone-pair commands:

```
stg-2801-L#show policy-map type inspect zone-pair
Zone-pair: arch-pub

Service-policy inspect : arch-pub-pmap

Class-map: out-cmap (match-any)
  Match: protocol http
    1 packets, 28 bytes
    30 second rate 0 bps
  Match: protocol https
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol ftp
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: protocol smtp
    0 packets, 0 bytes
    30 second rate 0 bps
Inspect
  Packet inspection statistics [process switch:fast switch]
  tcp packets: [1:15]

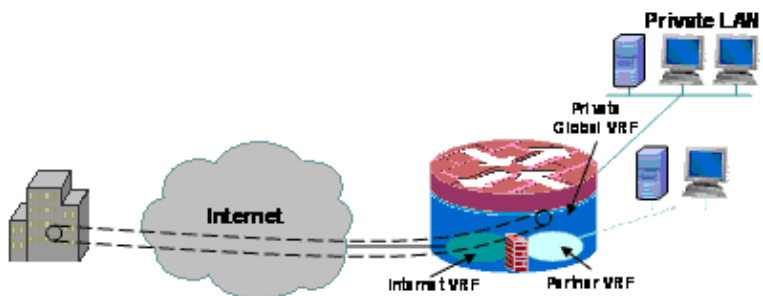
  Session creations since subsystem startup or last reset 1
  Current session counts (estab/half-open/terminating) [0:0:0]
  Maxever session counts (estab/half-open/terminating) [1:1:0]
  Last session created 00:09:50
  Last statistic reset never
  Last session creation rate 0
  Maxever session creation rate 1
  Last half-open session total 0

Class-map: class-default (match-any)
  Match: any
  Drop (default action)
    8 packets, 224 bytes
```

Multi-VRF Single-Site Zone-Based Policy Firewall, internet connection with backup in internet zone, global VRF has connection to HQ

This application is well suited to telecommuter deployments, small retail locations, and any other remote-site network deployment that requires segregation of private-network resources from public-network access. By isolating Internet connectivity and home or public hotspot users to a *public* VRF, and applying a default route in the global VRF that routes all private-network traffic through VPN tunnels, the resources in the private, global VRF and the Internet-reachable *public* VRF have no reachability to each other, thus completely removing the threat of private-net host compromise by public-internet activity. Furthermore, an additional VRF can be provisioned to provide a protected route space for other consumers needing an isolated network space, such as lottery terminals, ATM machines, charge-card processing terminals, or other applications.

Multiple Wi-Fi SSIDs can be provisioned to offer access to both the private network, as well as a public hotspot.



This example describes configuration for two broadband internet connections, applying PAT (NAT overload) for hosts in the *public* and *partner* VRFs for access to the public internet, with Internet connectivity assured by SLA monitoring on the two connections. The private network (in the global VRF) uses a GRE-over-IPsec connection to maintain connectivity to HQ (configuration included for the VPN head-end router) over the two broadband links. In the event that one or the other of the broadband connections fails, connectivity to the VPN head-end is maintained, which allows uninterrupted access to the HQ network, since the local endpoint of the tunnel is not tied specifically to either of the Internet connections.

A zone-based policy firewall is in place and controls access to and from the VPN to the private network, and between the public and partner LANs and the Internet in order to allow outbound internet access, but no connections in to the local networks from the Internet:

	Internet	Public	Partner	VPN	Private
Internet	N/A	Deny	Deny	Deny	Deny
Public	HTTP,HTTPS,FTP, DNS	N/A	Deny	Deny	Deny
Partner		Deny	N/A		
VPN	Deny	Deny	Deny	N/A	
Private	Deny	Deny	Deny		N/A

NAT application for hotspot and partner-net traffic makes compromise from the public internet much less likely, but the possibility still exists that malicious users or software can exploit an active NAT session. Application of stateful inspection minimizes chances that local hosts can be compromised by attacking an open NAT session. This example employs an 871W, but the configuration can be easily replicated with other ISR platforms.

Configure Multi-VRF Single-Site Zone-Based Policy Firewall, primary internet connection with backup, global VRF has VPN to HQ scenario

Multi-tenant sites that offer Internet access as a tenant service can use VRF-aware firewall to allocate overlapping address space and a boilerplate firewall policy for all tenants. Requirements for routable space, NAT, and remote-access and site-to-site VPN service can be accommodated as well to the offer of customized services for each tenant, with the benefit of provisioning a VRF for each customer.

```

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 BV11
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

```

This Hub Configuration provides an example of the VPN connectivity configuration:

```

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

```

Verify Multi-VRF Single-Site Zone-Based Policy Firewall, primary internet connection with backup, global VRF has VPN to HQ scenario

Network Address Translation and Firewall inspection is verified for each VRF with these commands:

Examine routes in each VRF with the **show ip route vrf [vrf-name]** command:

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

Check the NAT activity of each VRF with the **show ip nat tra vrf [vrf-name]** command:

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

Monitor firewall inspection statistics with the **show policy-map type inspect zone-pair** commands:

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

Conclusion

Cisco IOS VRF-Aware Classic and Zone-Based Policy Firewall offers reduced cost and administrative burden for providing network connectivity with integrated security for multiple networks with minimal hardware. Performance and scalability is maintained for multiple networks and provides an effective platform for network infrastructure and services without the increase of capital cost.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

Problem

Exchange server is not accessible from the outside interface of the Router.

Solution

Enable the SMTP Inspection in the router in order to fix this issue

Sample 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
```

Related Information

- [Zone-Based Policy Firewall Design Guide](#)
 - [Using Zone-Based Policy Firewall with VPN](#)
 - [VRF Aware Cisco IOS Firewall](#)
 - [Integrating NAT with MPLS VPNs](#)
 - [Designing MPLS Extensions For Customer Edge Routers](#)
 - [Verifying NAT Operation and Basic NAT Troubleshooting](#)
 - [PIX/ASA Multiple Context Configuration Example](#)
 - [Cisco IOS Firewall](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Feb 12, 2008

Document ID: 100595
