Cisco IOS Firewall Classic 및 Zone-Based Virtual Firewall 애플리케이션 컨피그레이션 예

목차

소개

이 문서에서는 다양한 애플리케이션 시나리오에 대한 VRF 인식 가상 방화벽 기능, 컨피그레이션 절차 및 활용 사례에 대한 기술적 배경을 설명합니다.

Cisco IOS® Software Release 12.3(14)T는 기존 VPN, NAT, QoS 및 기타 VRF 인식 기능 외에 상태 저장 패킷 검사, 투명 방화벽, 애플리케이션 검사 및 URL 필터링을 제공하도록 가상(VRF 인식) 방화벽 기능을 확장함으로써 Virtual Routing-Forwarding(VRF) 방화벽을 도입했습니다. 가장 가까운 애플리케이션 시나리오는 NAT를 다른 기능과 함께 적용합니다. NAT가 필요하지 않은 경우 VRF 간에 라우팅을 적용하여 VRF 간 연결을 제공할 수 있습니다. Cisco IOS Software는 Cisco IOS Classic Firewall 및 Cisco IOS Zone-Based Policy Firewall에서 VRF 인식 기능을 제공하며, 이 문서에서는 두 구성 모델의 예를 제공합니다. Zone-Based Policy Firewall Configuration에 더 큰 관심이 집중됩니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

기능 지원

VRF 인식 방화벽은 고급 보안, 고급 IP 서비스, 고급 엔터프라이즈 이미지 및 *o3* 지정을 전달하는 레거시 명명법 이미지에서 사용할 수 있으며, 이는 Cisco IOS 방화벽 기능 세트의 통합을 나타냅니다. 12.4에서 Cisco IOS Software Mainline Release에 통합된 VRF 인식 방화벽 기능. VRF 인식 영역 기반 정책 방화벽을 적용하려면 Cisco IOS Software 릴리스 12.4(6)T 이상이 필요합니다. Cisco IOS Zone-Based Policy Firewall은 스테이트풀 장애 조치에서 작동하지 않습니다.

VRF 컨피그레이션

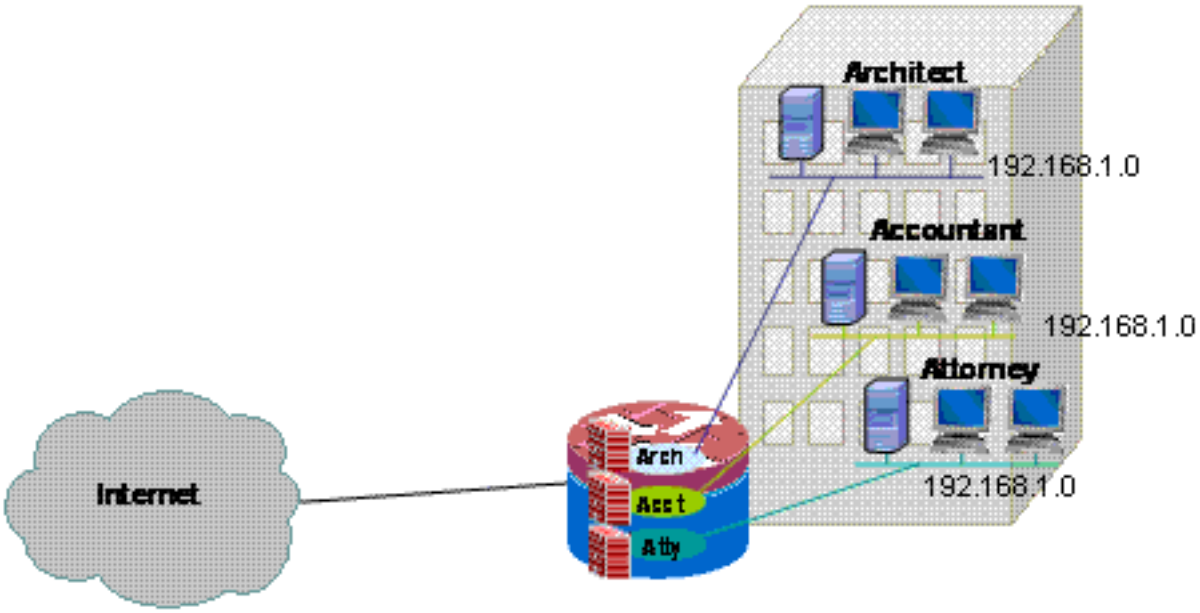
Cisco IOS Software는 동일한 컨피그레이션 파일에서 전역 VRF 및 모든 프라이빗 VRF에 대한 컨피그레이션을 유지 관리합니다. CLI(Command-Line Interface)를 통해 라우터 컨피그레이션에 액세스할 경우 CLI Views(CLI 보기) 기능에 제공되는 역할 기반 액세스 제어를 사용하여 라우터 운영 및 관리 인력의 기능을 제한할 수 있습니다. CSM(Cisco Security Manager)과 같은 관리 애플리케이션도 역할 기반 액세스 제어를 제공하여 운영 인력이 적절한 수준의 기능으로 제한되도록 합니다.

VRF 인식 IOS 방화벽의 일반적인 사용 개요

VRF 인식 방화벽은 상태 저장 패킷 검사를 Cisco IOS VRF(Virtual Routing/Forwarding) 기능에 추가합니다. IPsec VPN, NAT(Network Address Translation)/PAT(Port Address Translation), IPS(Intrusion Prevention System) 및 기타 Cisco IOS 보안 서비스를 VRF 인식 방화벽과 결합하여 VRF에 완벽한 보안 서비스를 제공할 수 있습니다. VRF는 겹치는 IP 주소 번호 지정을 사용하는 여러 경로 공간을 지원하므로 라우터를 여러 개별 라우팅 인스턴스로 분할하여 트래픽 분리를 수행할 수 있습니다. VRF 인식 방화벽은 모든 면에서 동일할 수 있는 연결 상태 정보 간의 분리를 유지하기 위해 라우터가 추적하는 모든 검사 활동에 대한 세션 정보에 VRF 레이블을 포함합니다. VRF 인식 방화벽은 한 VRF 내의 인터페이스 간 및 다른 VRF의 인터페이스 간(예: 트래픽이 VRF 경계를 교차하는 경우)를 검사할 수 있으므로 intra-VRF 및 inter-VRF 트래픽 모두에 대해 방화벽 검사 유연성이 극대화됩니다.

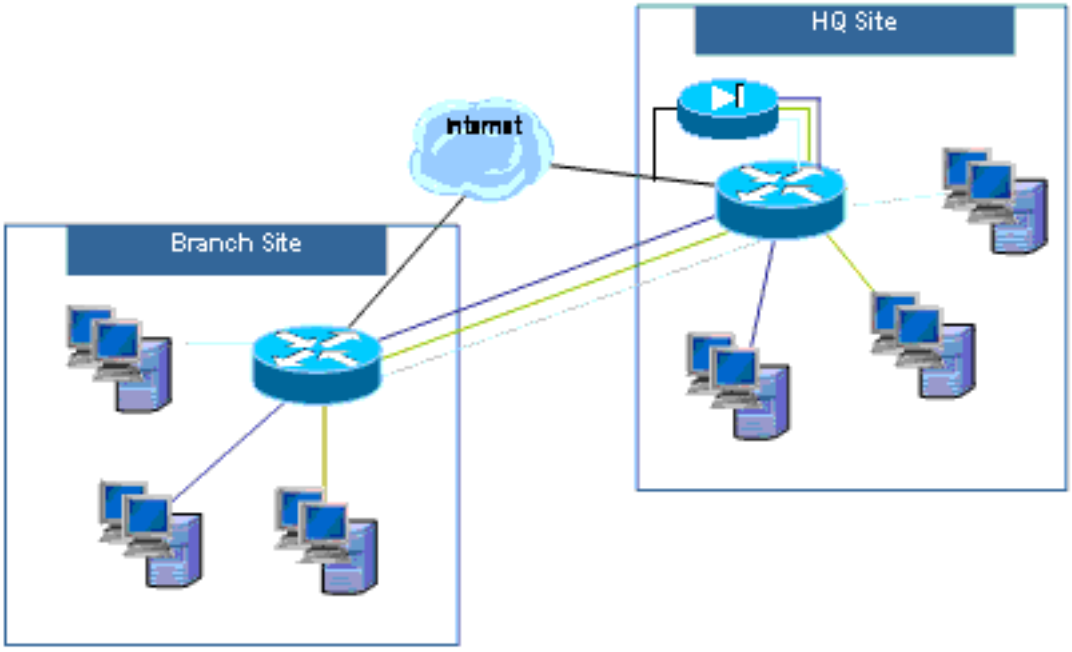
VRF 인식 Cisco IOS 방화벽 애플리케이션은 두 가지 기본 범주로 그룹화할 수 있습니다.

- 다중 테넌트, 단일 사이트 - 주소 공간 또는 분리된 경로 공간이 하나의 전관에서 겹치는 여러 테넌트를 위한 인터넷 액세스. 스테이트풀 방화벽은 각 VRF의 인터넷 연결에 적용되어 개방형 NAT 연결을 통해 보안 침해 가능성을 더욱 줄입니다. 포트 전달을 적용하여 VRF의 서버에 연결할 수 있습니다



. 이 문서에서는 VRF 인식 클래식 방화벽 컨피그레이션 모델과 VRF 인식 영역 기반 방화벽 컨피그레이션 모델 모두에 대한 멀티 테넌트 단일 사이트 애플리케이션의 예를 제공합니다.

- 다중 테넌트, 다중 사이트—대규모 네트워크에서 장비를 공유하는 여러 테넌트는 VPN 또는 WAN 연결을 통해 여러 사이트에 있는 테넌트의 VRF를 연결하여 여러 사이트 간에 연결해야 합니다. 하나 이상의 사이트에서 각 테넌트에 대해 인터넷 액세스가 필요할 수 있습니다. 관리를 간소화하기 위해 여러 부서에서는 각 사이트에 대해 하나의 액세스 라우터로 네트워크를 축소할 수 있지만, 여러 부서에서는 주소 공간 분리가 필요합니다



. VRF 인식 클래식 방화벽 구성 모델과 VRF 인식 영역 기반 방화벽 구성 모델 모두에 대한 멀티 테넌트 멀티 사이트 애플리케이션에 대한 컨피그레이션 예는 이 문서의 향후 업데이트에 제공될 예정입니다.

지원되지 않는 구성

VRF 인식 방화벽은 VRF Lite(Multi-VRF CE) 및 MPLS VPN을 지원하는 Cisco IOS 이미지에서 사용할 수 있습니다. 방화벽 기능은 비 MPLS 인터페이스로 제한됩니다. 즉, 인터페이스가 MPLS 레이블 트래픽에 참여하는 경우 해당 인터페이스에 방화벽 검사를 적용할 수 없습니다.

트래픽이 인터페이스를 통해 VRF를 들어오거나 나가는 경우에만 라우터가 VRF 간 트래픽만 검사할 수 있습니다. 트래픽이 다른 VRF로 직접 라우팅되는 경우 방화벽 정책이 트래픽을 검사할 수 있는 물리적 인터페이스가 없으므로 라우터가 검사를 적용할 수 없습니다.

VRF Lite 컨피그레이션은 NAT/PAT가 네트워크 활동에 대한 소스 또는 목적지 주소 또는 포트 번호를 수정하기 위해 적용되는 인터페이스에 NAT/IP `inside` 또는 `ip nat outside`가 구성된 경우에만 NAT/PAT와 상호운용됩니다. NAT 또는 PAT를 적용하는 인터페이스에 `ip nat`를 추가하여 식별되는 NVI(NAT Virtual Interface) 기능은 inter-VRF NAT/PAT 애플리케이션에서 지원되지 않습니다. VRF Lite와 NAT-Virtual 인터페이스 간의 상호운용성의 부재는 개선 요청 CSCek35625에 의해 추적됩니다.

구성

이 섹션에서는 VRF 인식 Cisco IOS Classic Firewall 및 VRF 인식 영역 기반 정책 방화벽 컨피그레이션에 대해 설명합니다.

참고: 이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 명령 조회 도구(등록된 고객만 해당)를 사용하십시오.

VRF 인식 Cisco IOS Classic Firewall

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

`ip` 를 사용하여 식별된 Cisco IOS VRF 인식 클래식 방화벽(이전 명칭: CBAC)은 Cisco IOS Software Release 12.3(14)T에서 VRF 인식 검사를 지원하도록 Classic Firewall이 확장되었으므로 Cisco IOS Software에서 사용할 수 있습니다.

Cisco IOS VRF 인식 클래식 방화벽 구성

VRF-Aware Classic Firewall은 검사 정책 컨피그레이션에 비 VRF 방화벽과 동일한 컨피그레이션 구문을 사용합니다.

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

VRF별 컨피그레이션 옵션을 사용하여 각 VRF에 대해 검사 매개변수를 수정할 수 있습니다.

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

검사 정책 목록은 전역으로 구성되며 검사 정책을 여러 VRF의 인터페이스에 적용할 수 있습니다.

각 VRF는 DoS(Denial-of-Service) 보호, TCP/UDP/ICMP 세션 타이머, 감사 추적 설정 등의 값에 대한 자체 검사 매개변수 집합을 전달합니다. 하나의 검사 정책이 여러 VRF에서 사용되는 경우 VRF 관련 매개변수 컨피그레이션이 검사 정책에 의해 전달되는 모든 전역 컨피그레이션을 대체합니다. DoS 보호 매개변수 조정 방법에 대한 자세한 내용은 Cisco IOS Classic Firewall and Intrusion Prevention System Denial-of-Service Protection을 참조하십시오.

Cisco IOS VRF 인식 기존 방화벽 활동 보기

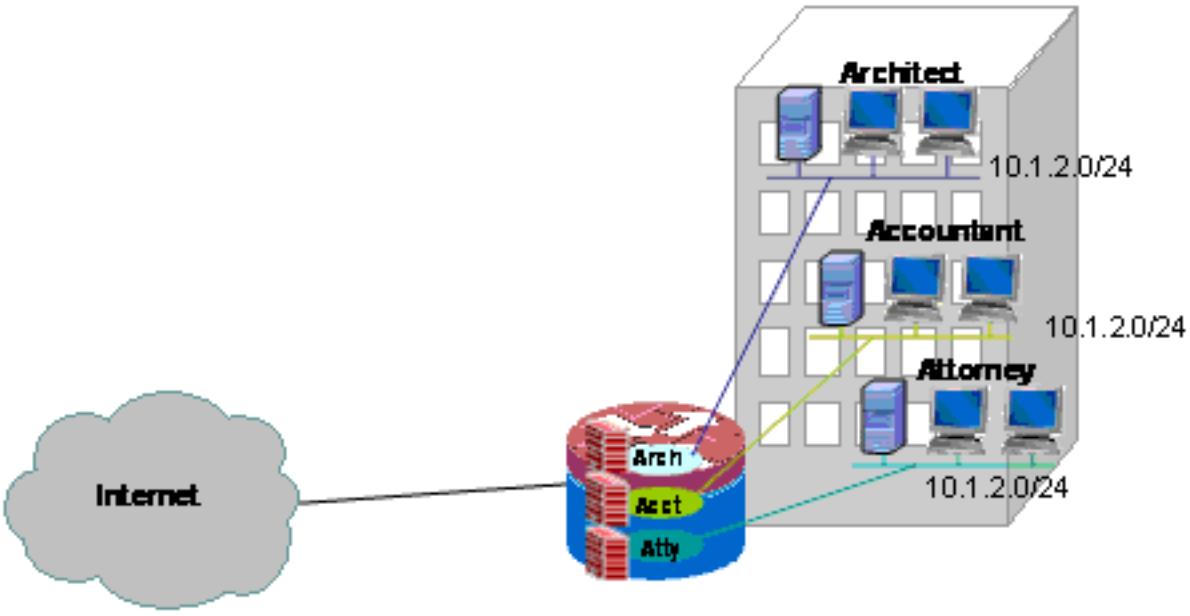
VRF 인식 방화벽 "show" 명령은 "show" 명령에서 VRF를 지정해야 하므로 VRF 인식 명령이 비 VRF 인식 명령과 다릅니다.

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

Multi-VRF Single-Site Classic Firewall

테넌트 서비스로 인터넷 액세스를 제공하는 다중 테넌트 사이트는 VRF 인식 방화벽을 사용하여 모든 테넌트에 대해 중복 주소 공간 및 공통 방화벽 정책을 할당할 수 있습니다. 라우팅 가능한 공간, NAT, 원격 액세스 및 Site-to-Site VPN 서비스에 대한 요구 사항은 물론 각 테넌트에 대한 맞춤형 서비스를 제공할 수 있으며, 각 고객에게 VRF를 프로비저닝할 수 있습니다.

이 애플리케이션은 주소 공간 관리를 간소화하기 위해 중복 주소 공간을 사용합니다. 그러나 이로 인해 다양한 VRF 간에 연결을 제공하는 문제가 발생할 수 있습니다. VRF 간에 연결이 필요하지 않은 경우 기존 내부-외부 NAT를 적용할 수 있습니다. NAT 포트 전달은 설계자(아키텍처), 회계사(acct) 및 변호사(atty) VRF의 서버를 노출하는 데 사용됩니다. 방화벽 ACL 및 정책은 NAT 활동을 수용해야 합니다.



Multi-VRF Single-Site Classic Network용 기본 방화벽 및 NAT 구성

테넌트 서비스로 인터넷 액세스를 제공하는 다중 테넌트 사이트는 VRF 인식 방화벽을 사용하여 모든 테넌트에 대해 중복 주소 공간과 공통 방화벽 정책을 할당할 수 있습니다. 라우팅 가능한 공간, NAT, 원격 액세스 및 Site-to-Site VPN 서비스에 대한 요구 사항은 물론 각 테넌트에 대한 맞춤형 서비스를 제공할 수 있으며, 각 고객에게 VRF를 프로비저닝할 수 있습니다.

다양한 LAN 및 WAN 연결에 대한 액세스를 정의하는 Classic Firewall 정책이 시행되었습니다.

		연결 소스			
		인터넷	아치	계정	아티
연결	인터넷	해당 없음	HTTP,HTTPS FTP, DNS,	HTTP,HTTPS FTP, DNS,	HTTP,HTTPS FTP,

			SMTP	SMTP	DNS, SMTP
대상	아치	FTP	해당 없음	거부	거부
	계정	SMTP	거부	해당 없음	거부
	아티	HTTP SMTP	거부	거부	해당 없음

3개의 VRF 각각에 있는 호스트는 공용 인터넷에서 HTTP, HTTPS, FTP 및 DNS 서비스에 액세스할 수 있습니다. 하나의 액세스 제어 목록(ACL 111)은 세 VRF 모두에 대한 액세스를 제한하는 데 사용됩니다(각 VRF는 인터넷에서 동일한 서비스에 대한 액세스를 허용하기 때문). 그러나 VRF당 검사 통계를 제공하기 위해 서로 다른 검사 정책이 적용됩니다. 별도의 ACL을 사용하여 VRF당 ACL 카운터를 제공할 수 있습니다. 반대로, 인터넷의 호스트는 ACL 121에 의해 정의된 대로 이전 정책 테이블에 설명된 서비스에 연결할 수 있습니다. 반대 방향으로 연결을 보호하는 ACL을 통해 돌아가도록 트래픽을 양방향으로 검사해야 합니다. NAT 컨피그레이션은 VRF의 서비스에 대한 포트 전달 액세스를 설명하기 위해 주석 처리됩니다.

단일 사이트 다중 테넌트 클래식 방화벽 및 NAT 컨피그레이션:

```
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
```

Multi-VRF Single-Site Classic Network용 기존 방화벽 및 NAT 확인

다음 명령을 사용하여 각 VRF에 대해 네트워크 주소 변환 및 방화벽 검사를 확인합니다.

show ip route vrf **[vrf-name]** 명령을 사용하여 각 VRF의 경로를 검토합니다.

```
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#
```

각 VRF의 NAT 활동(**show ip nat trvrf [vrf-name]** 명령)을 확인합니다.

```
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
```

show ip inspect vrf name 명령을 사용하여 각 VRF의 방화벽 검사 통계를 모니터링합니다.

```
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 인식 Cisco IOS Zone-Based Policy IOS Firewall]

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

다중 VRF 라우터 컨피그레이션에 Cisco IOS Zone-Based Policy Firewall을 추가하면 비 VRF 애플리케이션의 Zone Firewall과 거의 차이가 없습니다. 즉, 정책 결정은 비 VRF Zone-Based Policy Firewall이 관찰한 동일한 규칙을 준수하며, 몇 가지 다중 VRF 관련 조항을 추가할 경우 비용을 절약합니다.

- Zone-Based Policy Firewall 보안 영역은 하나의 영역에서만 인터페이스를 포함할 수 있습니다.
- VRF는 둘 이상의 보안 영역을 포함할 수 있습니다.
- Zone-Based Policy Firewall은 트래픽이 VRF 간에 이동할 수 있도록 라우팅 또는 NAT에 종속됩니다. VRF 간 영역-쌍 간에 트래픽을 검사하거나 전달하는 방화벽 정책은 VRF 간에 트래픽을 이동하는 것을 허용하지 않습니다.

VRF 인식 Cisco IOS Zone-Based Policy Firewall 구성

VRF 인식 영역 기반 정책 방화벽은 비 VRF 인식 영역 기반 정책 방화벽과 동일한 컨피그레이션 구문을 사용하며, 보안 영역에 인터페이스를 할당하고, 영역 간에 이동하는 트래픽에 대한 보안 정책을 정의하고, 적절한 영역 쌍 연결에 보안 정책을 할당합니다.

VRF별 컨피그레이션은 필요하지 않습니다. 정책 맵의 검사에 더 구체적인 매개변수 맵이 추가되지 않는 한 글로벌 컨피그레이션 매개변수가 적용됩니다. 매개변수 맵을 사용하여 더 구체적인 컨피그레이션을 적용하는 경우에도 매개변수 맵은 VRF에 특정하지 않습니다.

VRF 인식 Cisco IOS Zone-Based Policy Firewall 활동 보기

VRF 인식 영역 기반 정책 방화벽 **show** 명령은 VRF를 인식하지 않는 명령과 다르지 않습니다. Zone-Based Policy Firewall은 다양한 인터페이스의 VRF 할당에 관계없이 한 보안 영역의 인터페이스에서 다른 보안 영역의 인터페이스로 이동하는 트래픽을 적용합니다. 따라서 VRF 인식 영역 기반 정책 방화벽은 비 VRF 애플리케이션에서 영역 기반 정책 방화벽에서 사용하는 방화벽 활동을 보기 위해 동일한 **show** 명령을 사용합니다.

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

VRF 인식 Cisco IOS Zone-Based Policy Firewall 활용 사례

VRF 인식 방화벽 사용 사례는 광범위하게 다릅니다. 다음 예는 다음과 같습니다.

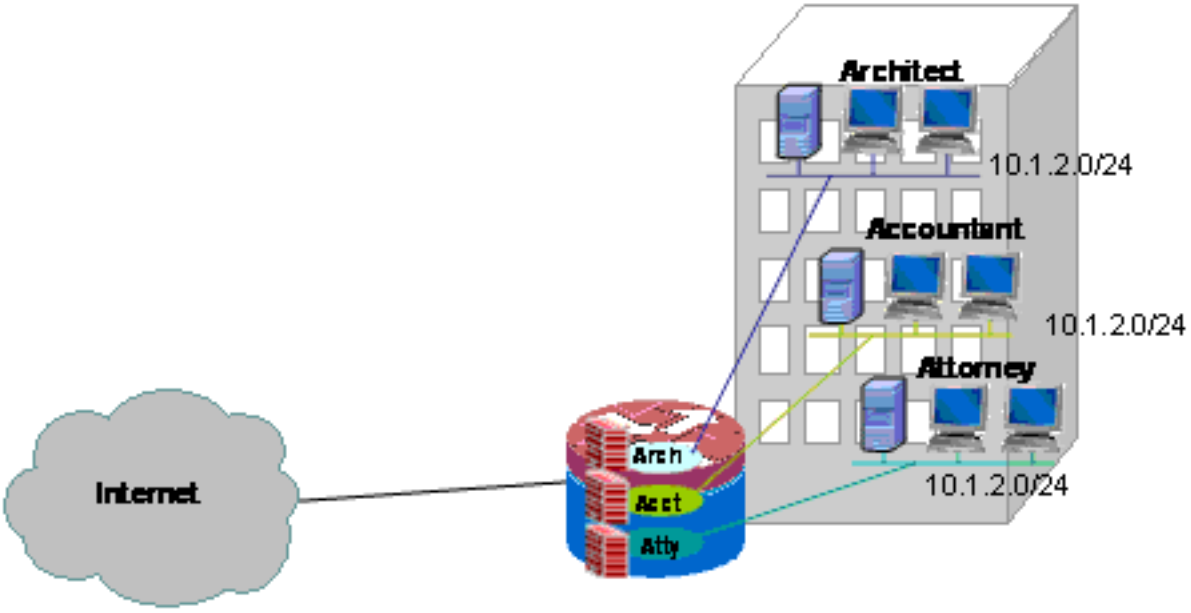
- 단일 사이트 VRF 인식 구축(일반적으로 다중 테넌트 시설 또는 소매 네트워크에 사용)
- 사설 네트워크 트래픽이 공용 인터넷 트래픽과 별도의 VRF에 유지되는 지사/소매/재택 근무 애플리케이션. 인터넷 액세스 사용자는 비즈니스 네트워크 사용자로부터 격리되며, 모든 비즈니스 네트워크 트래픽은 VPN 연결을 통해 인터넷 정책 애플리케이션을 위한 HQ 사이트에 전달됩니다.

다중 VRF 단일 사이트 영역 기반 정책 방화벽

테넌트 서비스로 인터넷 액세스를 제공하는 다중 테넌트 사이트는 VRF 인식 방화벽을 사용하여 모든 테넌트에 대해 중복 주소 공간과 공통 방화벽 정책을 할당할 수 있습니다. 이 애플리케이션은 특정 사이트의 여러 LAN에서 인터넷 액세스를 위해 하나의 Cisco IOS 라우터를 공유하거나, 포토퍼니셔나 일부 기타 서비스와 같은 비즈니스 파트너가 인터넷과 구내 소유자의 네트워크의 특정 부분

을 연결하는 격리된 데이터 네트워크를 추가 네트워크 하드웨어 또는 인터넷 연결 없이 제공하는 경우가 일반적입니다. 라우팅 가능한 공간, NAT, 원격 액세스 및 Site-to-Site VPN 서비스에 대한 요구 사항은 물론 각 테넌트에 대한 맞춤형 서비스를 제공할 수 있으며, 각 고객에게 VRF를 프로비저닝할 수 있습니다.

이 애플리케이션은 주소 공간 관리를 간소화하기 위해 중복 주소 공간을 사용합니다. 그러나 이로 인해 다양한 VRF 간에 연결을 제공하는 데 문제가 발생할 수 있습니다. VRF 간에 연결이 필요하지 않은 경우 기존 내부-외부 NAT를 적용할 수 있습니다. 또한 NAT 포트 전달은 설계자(아키텍처), 회계사(acct) 및 변호사(atty) VRF의 서버를 노출하는 데 사용됩니다. 방화벽 ACL 및 정책은 NAT 활동을 수용해야 합니다.



다중 VRF 단일 사이트 영역 기반 정책 방화벽 및 NAT 구성

테넌트 서비스로 인터넷 액세스를 제공하는 다중 테넌트 사이트는 VRF 인식 방화벽을 사용하여 모든 테넌트에 대해 중복 주소 공간과 공통 방화벽 정책을 할당할 수 있습니다. 라우팅 가능한 공간, NAT, 원격 액세스 및 Site-to-Site VPN 서비스에 대한 요구 사항은 물론 각 테넌트에 대한 맞춤형 서비스를 제공할 수 있으며, 각 고객에게 VRF를 프로비저닝할 수 있습니다.

다양한 LAN 및 WAN 연결에 대한 액세스를 정의하는 Classic Firewall 정책이 시행되었습니다.

		연결 소스			
		인터넷	아치	계정	아티
연결 대상	인터넷	해당 없음	HTTP,HTTPS FTP, DNS, SMTP	HTTP,HTTPS FTP, DNS, SMTP	HTTP,HTTPS FTP, DNS, SMTP
	아치	FTP	해당 없음	거부	거부
	계정	SMTP	거부	해당 없음	거부
	아티	HTTP SMTP	거부	거부	해당 없음

3개의 VRF 각각에 있는 호스트는 공용 인터넷에서 HTTP, HTTPS, FTP 및 DNS 서비스에 액세스할 수 있습니다. 각 VRF는 인터넷에서 동일한 서비스에 대한 액세스를 허용하지만 VRF당 검사 통계를 제공하기 위해 서로 다른 정책 맵이 적용되기 때문에 하나의 클래스 맵(private-public-map)을 사용하여 세 VRF에 대한 액세스를 제한합니다. 반대로, 인터넷의 호스트는 이전 정책 표에 설명된 대로 서비스에 연결할 수 있습니다. 개별 클래스 맵 및 Internet-to-VRF 영역 쌍용 정책 맵에 의해 정의됩니다. 별도의 정책 맵은 공용 인터넷에서 자체 영역에 있는 라우터의 관리 서비스에 액세스하지 못하도록 하는 데 사용됩니다. 프라이빗 VRF에서 라우터의 자체 영역에 대한 액세스를 방지하기 위해 동일한 정책을 적용할 수 있습니다.

NAT 컨피그레이션은 VRF의 서비스에 대한 포트 전달 액세스를 설명하기 위해 주석 처리됩니다.

단일 사이트 다중 테넌트 영역 기반 정책 방화벽 및 NAT 컨피그레이션:

```
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
```

Multi-VRF Single-Site Classic Network용 기존 방화벽 및 NAT 확인

다음 명령을 사용하여 각 VRF에 대해 네트워크 주소 변환 및 방화벽 검사를 확인합니다.

show ip route vrf **[vrf-name]** 명령을 사용하여 각 VRF의 경로를 검토합니다.

```
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#
```

show ip nat trvrf [vrf-name] 명령으로 각 VRF의 NAT 활동을 확인합니다.

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

show policy-map **type inspect zone-pair** 명령을 사용하여 방화벽 검사 통계 모니터링

```
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
```

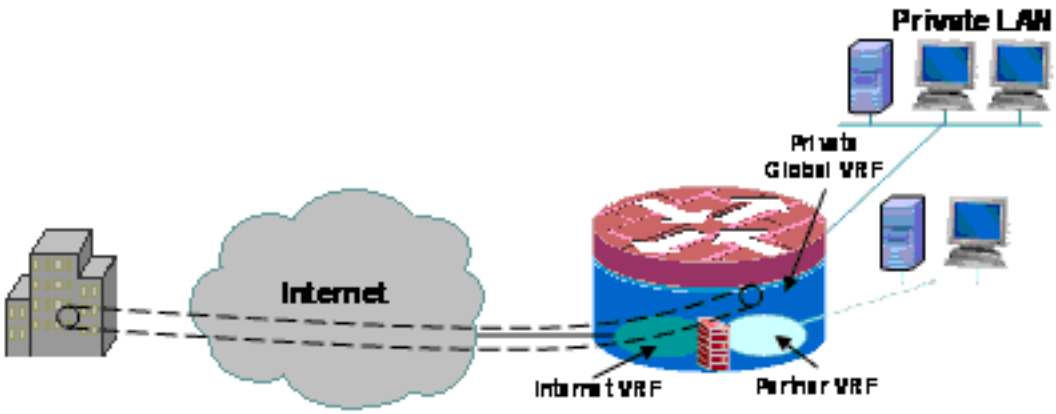
```
    Inspect
      Packet inspection statistics [process switch:fast switch]
      tcp packets: [1:15]

      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, "인터넷" 영역에서 백업을 통한 인터넷 연결, 글로벌 VRF가 HQ에 연결

이 애플리케이션은 재택 근무 구축, 소규모 소매점 위치 및 공용 네트워크 액세스와 사설 네트워크 리소스를 분리해야 하는 기타 원격 사이트 네트워크 구축에 적합합니다. 인터넷 연결 및 홈 또는 공용 핫스팟 사용자를 *공용* VRF로 격리하고 VPN 터널을 통해 모든 프라이빗 네트워크 트래픽을 라우팅하는 전역 VRF에 기본 경로를 적용함으로써 사설, 글로벌 VRF 및 인터넷 연결 *가능한 공용* VRF의 리소스는 서로 연결할 수 없으므로 공용 인터넷 활동으로 사설 네트워크 호스트 보안 침해의 위협을 완전히 제거합니다. 또한 추가 VRF를 프로비저닝하여 복권 터미널, ATM 시스템, 충전 카드 처리 터미널 또는 기타 애플리케이션과 같은 격리된 네트워크 공간을 필요로 하는 다른 소비자를 위해 안전한 경로 공간을 제공할 수 있습니다. 여러 Wi-Fi SSID를 프로비저닝하여 프라이빗 네트워크 및 공용 핫스팟에 대한 액세스를 제공할 수 있습니다.



이 예에서는 두 개의 광대역 인터넷 연결에 대한 컨피그레이션을 설명합니다. 이 컨피그레이션은 *공용* 및 *파트너* VRF에 공용 인터넷 액세스를 위해 PAT(NAT 오버로드)를 적용하고, 두 연결의 SLA 모니터링을 통해 인터넷 연결을 보장합니다. 프라이빗 네트워크(글로벌 VRF의 경우)는 GRE-over-IPsec 연결을 사용하여 2개의 광대역 링크를 통해 HQ에 대한 연결(VPN 헤드엔드 라우터에 대한 컨피그레이션 포함)을 유지합니다. 하나 또는 다른 광대역 연결에 장애가 발생하는 경우 VPN 헤드엔드에 대한 연결이 유지되므로 터널의 로컬 엔드포인트가 인터넷 연결 중 하나에 특별히 연결되어 있지 않으므로 HQ 네트워크에 대한 무중단 액세스가 가능합니다.

영역 기반 정책 방화벽이 구축되어 있으며, 아웃바운드 인터넷 액세스를 허용하기 위해 VPN에서 사설 네트워크로, 그리고 퍼블릭 및 파트너 LAN과 인터넷 간에 액세스를 제어하고 인터넷을 통해 로컬 네트워크에 연결되지 않습니다.

	인터넷	공용	파트너	VPN	프라이빗
인터넷	해당 없음	거부	거부	거부	거부
공용	HTTP,HTTPS,FTP, DNS	해당 없음	거부	거부	거부
파트너		거부	해당 없음		
VPN	거부	거부	거부	해당 없음	
프라이빗	거부	거부	거부		해당 없음

핫스팟 및 파트너 네트워크 트래픽용 NAT 애플리케이션으로 인해 공용 인터넷에서의 보안 침해 가능성이 훨씬 적지만, 악의적인 사용자 또는 소프트웨어가 활성 NAT 세션을 악용할 수 있는 가능성은 여전히 존재합니다. 스테이트풀 검사를 적용하면 오픈 NAT 세션을 공격하여 로컬 호스트가 손상될 가능성이 최소화됩니다. 이 예에서는 871W를 사용하지만, 다른 ISR 플랫폼과 함께 구성을 쉽게 복제할 수 있습니다.

다중 VRF 단일 사이트 영역 기반 정책 방화벽 구성, 백업을 통한 기본 인터넷 연결, 글로벌 VRF는 VPN을 사용하여 HQ 시나리오

테넌트 서비스로 인터넷 액세스를 제공하는 다중 테넌트 사이트는 VRF 인식 방화벽을 사용하여 모든 테넌트에 대해 중복 주소 공간과 공통 방화벽 정책을 할당할 수 있습니다. 라우팅 가능한 공간, NAT, 원격 액세스 및 Site-to-Site VPN 서비스에 대한 요구 사항은 물론 각 테넌트에 대한 맞춤형 서비스를 제공할 수 있으며, 각 고객에게 VRF를 프로비저닝할 수 있습니다.

```
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
```

이 허브 컨피그레이션은 VPN 연결 컨피그레이션의 예를 제공합니다.

```
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
```

다중 VRF 단일 사이트 영역 기반 정책 방화벽, 백업을 통한 기본 인터넷 연결, 글로벌 VRF에 VPN-HQ 시나리오 확인

다음 명령을 사용하여 각 VRF에 대해 네트워크 주소 변환 및 방화벽 검사를 확인합니다.

show ip route vrf **[vrf-name]** 명령을 사용하여 각 VRF의 경로를 검토합니다.

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

show ip nat trvrf **[vrf-name]** 명령을 사용하여 각 VRF의 NAT 활동을 확인합니다.

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

show policy-map **type inspect zone-pair** 명령을 사용하여 방화벽 검사 통계 모니터링

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

결론

Cisco IOS VRF-Aware Classic 및 Zone-Based Policy Firewall은 최소한의 하드웨어로 여러 네트워크에 통합 보안을 제공하는 데 드는 비용 및 관리 부담을 줄여줍니다. 성능과 확장성은 여러 네트워크에 대해 유지되며 자본 비용 증가 없이 네트워크 인프라 및 서비스에 대한 효과적인 플랫폼을 제공합니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

문제

Exchange 서버는 라우터의 외부 인터페이스에서 액세스할 수 없습니다.

솔루션

이 문제를 해결하려면 라우터에서 SMTP 검사를 활성화합니다.

샘플 컨피그레이션

```
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
```

관련 정보

- 영역 기반 정책 방화벽 설계 가이드
- VPN과 함께 영역 기반 정책 방화벽 사용
- VRF 인식 Cisco IOS 방화벽
- NAT와 MPLS VPN 통합
- 고객 에지 라우터를 위한 MPLS 확장 설계
- NAT 작업 확인 및 기본 NAT 트러블슈팅
- PIX/ASA 다중 컨텍스트 컨피그레이션 예
- Cisco IOS Firewall
- 기술 지원 및 문서 – Cisco Systems