Классический брандмауэр Cisco IOS и пример конфигурации приложения зонального виртуального брандмауэра

Содержание

Введение

В этом документе изложены общие технические сведения о функциях виртуального межсетевого экрана с поддержкой VRF, описана процедура настройки и показаны варианты использования для различных практических сценариев.

Релиз 12.3 Программного обеспечения Cisco IOS (14) T представил Действительный (осведомленный о VRF) Межсетевой экран, расширив семейство функции Передачи виртуальной маршрутизации (VRF) для предложения проверки пакетов с отслеживанием состояния, прозрачного межсетевого экрана, контроля приложения и фильтрации URL-адресов, в дополнение к существующей VPN, NAT, QoS и другим осведомленным о VRF функциям. Большинство обозримых сценариев приложения применит NAT с другими функциями. Если NAT не требуется, маршрутизация может быть применена между VRF для обеспечения подключения меж-VRF. Программное обеспечение Cisco IOS предлагает осведомленные о VRF возможности и в Межсетевом экране Классики Cisco IOS и в Zone-Based Policy межсетевом экране Cisco IOS с примерами обеих моделей конфигурации, предоставленных в этом документе. Больший фокус размещен в Конфигурацию Zone-Based Policy межсетевого экрана.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

Поддержка возможностей

Осведомленный о VRF Межсетевой экран доступен в Дополнительной безопасности, Усовершенствованных IP-сервисах, и Усовершенствованных Корпоративных образах, а также образах устаревшей номенклатуры, которые несут *o3* обозначение, которое указывает на интеграцию Набора функций межсетевого экрана Cisco IOS. Осведомленная о VRF возможность Межсетевого экрана объединилась в Основные релизы программного обеспечения Cisco IOS в 12.4. Программное обеспечение Cisco IOS версии 12.4(6)T или позже требуется, чтобы применять Осведомленный о VRF Zone-Based Policy межсетевой экран. Zone-Based Policy межсетевой экран Cisco IOS не работает с перехватом управления при отказе с синхронизацией состояния.

Конфигурация VRF

Программное обеспечение Cisco IOS поддерживает конфигурации для глобального VRF и всех частных VRF в файле одинаковой конфигурации. Если к конфигурации маршрутизатора обращаются через Интерфейс командной строки, основанное на роли управление доступом, предлагаемое в функции Представлений CLI, может использоваться для ограничения возможности в рабочем состоянии маршрутизатора и специалисты в области управления. Приложения управления сетью, такие как Cisco Security Manager (CSM) также предоставляют основанное на роли управление доступом, чтобы гарантировать, что в рабочем состоянии персонал ограничен соответствующим уровнем возможности.

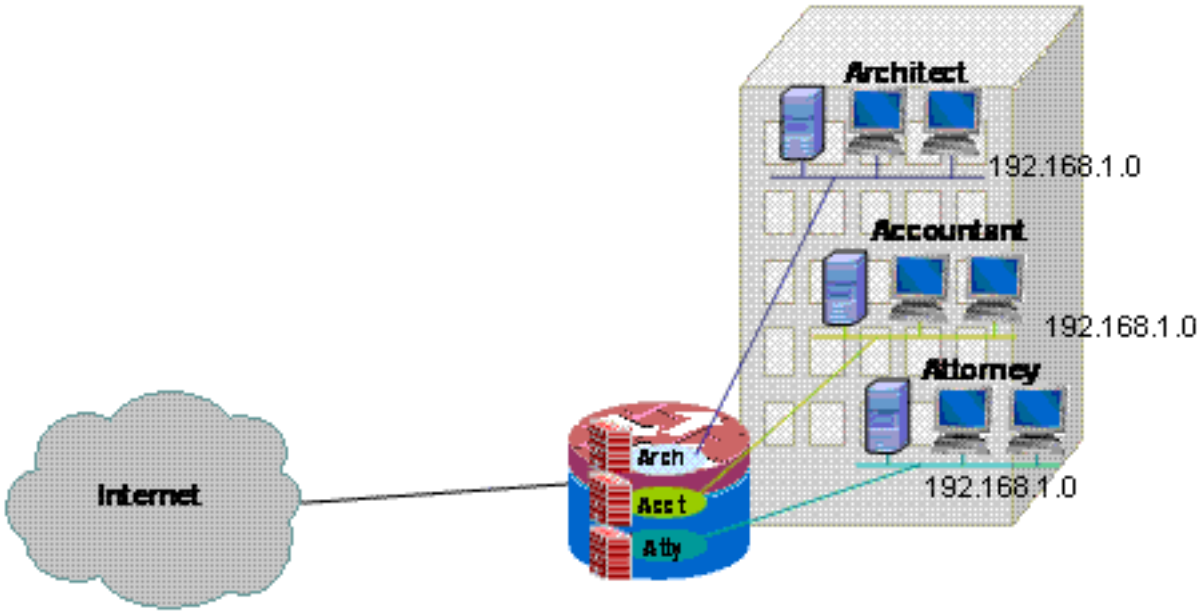
Обзор общего использования для осведомленного о VRF межсетевого экрана IOS

Осведомленный о VRF Межсетевой экран добавляет проверку пакетов с отслеживанием состояния к Виртуальной маршрутизации Cisco IOS / Передача (VRF) возможности. IPSec VPN, Переадресация/Port Технологии NAT (PAT), Система предотвращения вторжений (IPS)

и другие сервисы Безопасности Cisco IOS может быть объединен с Осведомленным о VRF Межсетевым экраном для обеспечения полного набора сервисов безопасности в VRF. VRF оказывают поддержку для пробелов несколька маршрутов, которые используют перекрывающуюся нумерацию IP-адреса, таким образом, маршрутизатор может быть разделен на множественные дискретные экземпляры маршрутизации для разделения трафика. Осведомленный о VRF межсетевой экран включает метку VRF в информацию о сеанса для всего инспекционного действия, которое маршрутизатор отслеживает, для поддержания разделения между информацией о состоянии соединения, которая может быть идентичной в любом уважении. Осведомленный о VRF межсетевой экран может осмотреть, осматривают между интерфейсами в одном VRF, а также между интерфейсами в VRF, которые отличаются, например в случаях, где трафик пересекает границы VRF, так, чтобы максимальная гибкость контроля межсетевого экрана была осознана и для внутри-VRF и для трафика меж-VRF.

Осведомленные о VRF приложения межсетевого экрана Cisco IOS могут быть сгруппированы в две основных категории:

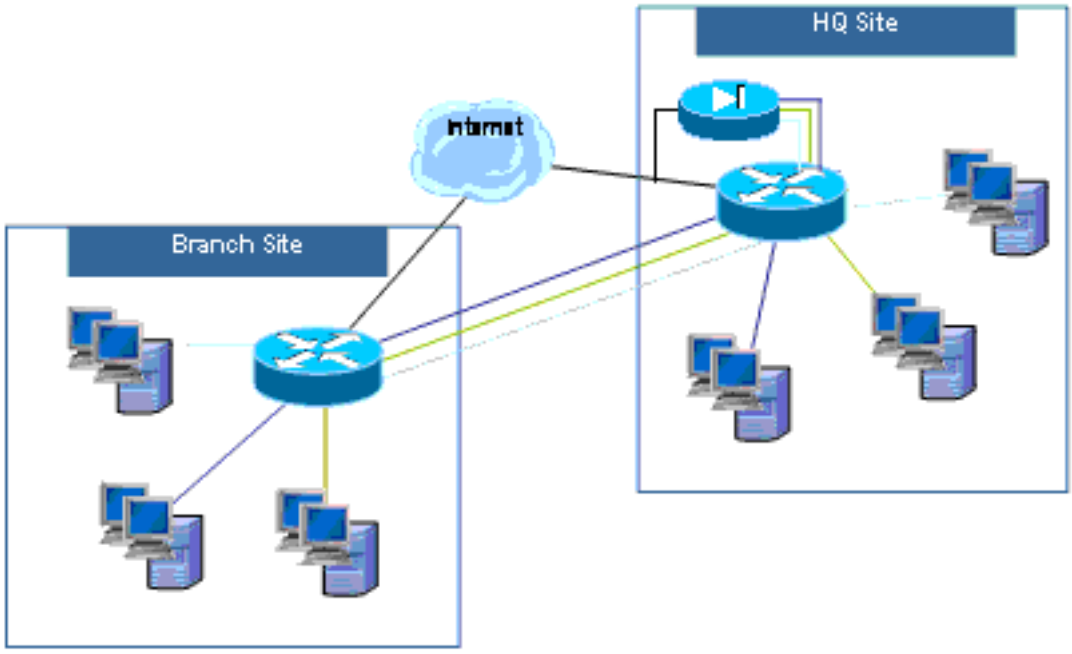
- С несколькими арендаторами, одиночный узел — доступ в Интернет для множественных арендаторов с адресными пространствами с перекрытием или отдельным маршрутом располагает с интервалами в одиночной предпосылке. Самонастраивающийся межсетевой экран применен к интернет-соединению каждого VRF для дальнейшего сокращения вероятности компромисса посредством открытых подключений NAT. Переадресация портов может быть применена для разрешения подключения серверам в
VRF.



Пример приложения одиночного узла с несколькими арендаторами и для Осведомленной о VRF Классической модели Конфигурации межсетевого экрана и для Осведомленной о VRF зональной модели Конфигурации межсетевого экрана предоставлен в этом документе.

- С несколькими арендаторами, для нескольких местоположений — Множественные арендаторы, которые совместно используют оборудование в подключении потребности большой сети между множественными узлами соединением VRF арендаторов на других узлах через VPN или подключения к глобальной сети (WAN). Доступ в Интернет может требоваться для каждого арендатора на одном или более узлах. Для упрощения

управления несколько отделов могут свернуть свои сети в один маршрутизатор доступа для каждого узла, но различные отделы требуют сегрегации адресного пространства.



Примеры конфигурации для приложений для нескольких местоположений с несколькими арендаторами и для Осведомленной о VRF Классической модели Конфигурации межсетевого экрана и для Осведомленной о VRF зональной модели Конфигурации межсетевого экрана будут предоставлены в предстоящем обновлении этого документа.

Неподдерживаемая конфигурация

Осведомленный о VRF Межсетевой экран доступен на Образах Cisco IOS, которые поддерживают CE мульти-VRF (Облегченный VRF) и MPLS VPN. Возможность межсетевого экрана ограничена интерфейсами не-MPLS. Т.е. если интерфейс будет участвовать в маркированном MPLS трафике, контроль межсетевого экрана не может быть применен на тот интерфейс.

Если трафик должен ввести или оставить VRF через интерфейс для пересечения к другому VRF, маршрутизатор может только осмотреть трафик меж-VRF. Если трафик маршрутизируется непосредственно к другому VRF, нет никакого физического интерфейса, где политика межсетевого экрана может осмотреть трафик, таким образом, маршрутизатор неспособен применить контроль.

Облегченная конфигурация VRF совместима с NAT/PAT, только если `ip nat inside` или `ip nat outside` настроены на интерфейсах, где NAT/PAT применен для изменения адресов источника или назначения или номеров портов для активности сети. Функция виртуального интерфейса NAT (NVI), определенная добавлением конфигурации `ip nat enable` к интерфейсам, которые применяют NAT или PAT, не поддерживается для приложения NAT/PAT меж-VRF. Это отсутствие совместимости между Облегченным VRF и виртуальным интерфейсом NAT отслежено запросом на расширение CSCek35625.

Настройка

В этом разделе объяснены Осведомленный о VRF Межсетевой экран Классики Cisco IOS и Осведомленные о VRF конфигурации Zone-Based Policy межсетевого экрана.

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Осведомленный о VRF межсетевой экран классики Cisco IOS

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Cisco IOS Осведомленный о VRF Классический Межсетевой экран (раньше вызванный CBAC), который определен при помощи `ip inspect`, была доступна в программном обеспечении Cisco IOS, так как Классический Межсетевой экран был расширен для поддержки осведомленного о VRF контроля в программном обеспечении Cisco IOS версии 12.3(14)T.

Настройте Cisco IOS осведомленный о VRF классический межсетевой экран

Осведомленный о VRF Классический Межсетевой экран использует синтаксис одинаковой конфигурации в качестве межсетевого экрана не-VRF для конфигурации политики проверки:

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

Параметры проверки могут модифицироваться для каждого VRF со специфичными для VRF параметрами конфигурации:

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

Списки политики проверки настроены глобально, и политика проверки может быть применена к интерфейсам во множественных VRF.

Каждый VRF несет свой собственный набор параметров проверки для значений, таких как защита атаки Denial of Service (DoS), таймеры сеанса TCP/UDP/ICMP, параметры настройки контрольного журнала, и т.д. Если одна политика проверки используется во множественных VRF, специфичная для VRF настройка параметров заменяет любую глобальную конфигурацию, которую несет политика проверки. См. Защиту Атаки Denial of Service Межсетевого экрана и Системы предотвращения вторжений Классики Cisco IOS для получения дополнительной информации о том, как настроить параметры защиты от атак DoS.

Просмотр Cisco IOS осведомленное о VRF классическое действие межсетевого экрана

Осведомленный о VRF Межсетевой экран “показывает”, что команды отличаются от команд non-VRF-aware, потому что осведомленные о VRF команды требуют, чтобы вы задали VRF в команде “показа”:

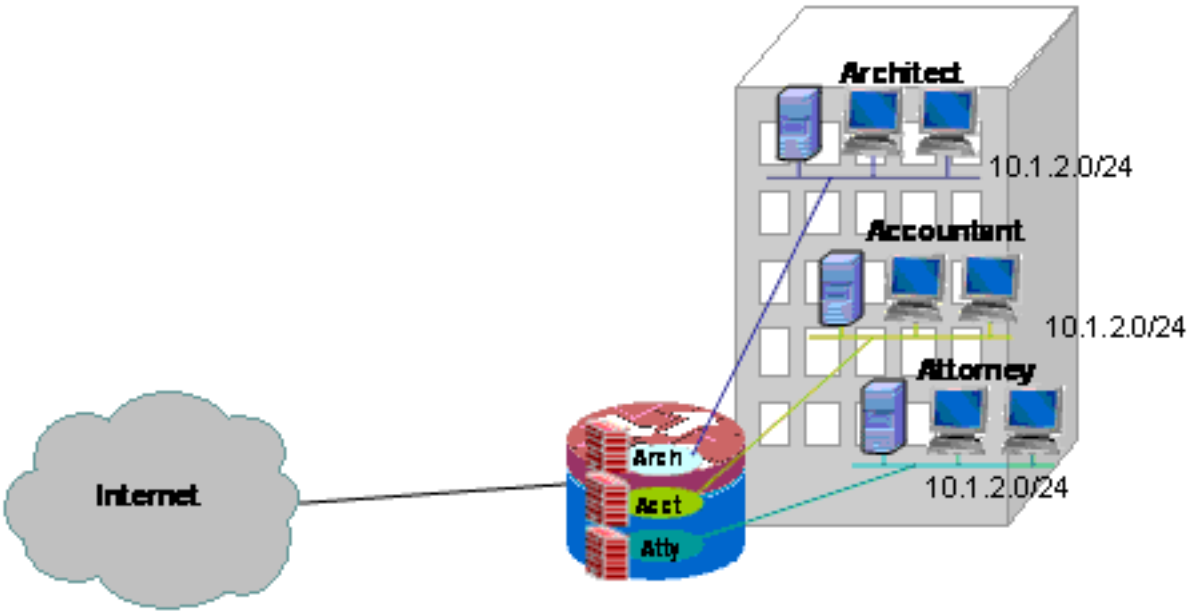
```
router#show ip inspect [ all | config | interfaces | name | sessions | statistics ] vrf vrf-name
```

Межсетевой экран классики Одиночного Узла мульти-VRF

Узлы с несколькими арендаторами, которые предлагают доступ в Интернет как сервис арендатора, могут использовать осведомленный о VRF межсетевой экран для выделения адресного пространства с перекрытием и шаблонной политики межсетевого экрана для всех арендаторов. Требования для маршрутизуемого пространства, NAT, и удаленного доступа и

сквозного VPN-соединение сервиса могут быть приняты также к предложению специализированных сервисов для каждого арендатора с преимуществом инициализации VRF для каждого клиента.

Это приложение использует адресное пространство с перекрытием для упрощения управления адресного пространства. Но, это может вызвать проблемы, которые предлагают подключение между различными VRF. Если подключение не требуется между VRF, традиционный NAT изнутри наружу может быть применен. Переадресация портов NAT используется для представления серверов в архитекторе (дуга), бухгалтер (acct) и поверенный (адвокат) VRF. ACL межсетевого экрана и политика должны принять активность NAT.



Настройте классический межсетевой экран и NAT для сети классики Одиночного Узла мульти-VRF

Узлы с несколькими арендаторами, которые предлагают доступ в Интернет как сервис арендатора, могут использовать осведомленный о VRF межсетевой экран для выделения адресного пространства с перекрытием и шаблонной политики межсетевого экрана для всех арендаторов. Требования для маршрутизуемого пространства, NAT, и удаленного доступа и сквозного VPN-соединение сервиса могут быть приняты также к предложению специализированных сервисов для каждого арендатора с преимуществом инициализации VRF для каждого клиента.

Классическая Политика межсетевого экрана существует, который определяет доступ к и от различной LAN и подключений к глобальной сети (WAN):

		Источник подключения			
		Интернет	Дуга	Acct	Адвокат
Назначение соединения	Интернет	Н/Д	HTTP, FTP HTTPS, DNS, SMTP	HTTP, FTP HTTPS, DNS, SMTP	HTTP, FTP HTTPS, DNS,

					SMTP
	Дуга	Ftp	Н/Д	Deny	Deny
	Acct	SMTP	Deny	Н/Д	Deny
	Адвокат	SMTP HTTP	Deny	Deny	Н/Д

Хосты в каждом из этих трех VRF в состоянии обратиться к HTTP, HTTPS, FTP и сервисам DNS на общедоступном Интернете. Один Список управления доступом (ACL 111) будет использоваться для ограничения доступа для всех трех VRF (так как каждый VRF предоставляет доступ к идентичным сервисам в Интернете), но другая политика проверки будет применена, чтобы предоставить инспекционную статистику на VRF. Отдельные ACL могут использоваться для обеспечения счетчиков ACL на VRF. Обратно пропорционально хосты в Интернете могут соединиться с сервисами, как описано в предыдущей таблице политики, как определено ACL 121. Трафик должен быть осмотрен в обоих направлениях для размещения, возвращаются через ACL, которые защищают подключение в противоположном направлении. Конфигурация NAT прокомментирована для описания переданного порту доступа к сервисам в VRF.

Одиночный узел классический межсетевой экран с несколькими арендаторами и конфигурация NAT:

```
version 12.4
!
ip cef
!
ip vrf acct
!
ip vrf arch
!
ip vrf atty
!
ip inspect name acct-fw ftp
ip inspect name acct-fw tcp
ip inspect name acct-fw udp
ip inspect name acct-fw icmp
ip inspect name arch-fw ftp
ip inspect name arch-fw tcp
ip inspect name arch-fw udp
ip inspect name arch-fw icmp
ip inspect name atty-fw ftp
ip inspect name atty-fw tcp
ip inspect name atty-fw udp
ip inspect name atty-fw icmp
ip inspect name fw-global tcp
ip inspect name fw-global udp
ip inspect name fw-global icmp
!
!
interface FastEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-FE 0$
 ip address 172.16.100.10 255.255.255.0
 ip access-group 121 in
 ip nat outside
 ip inspect fw-global in
 ip virtual-reassembly
```

```
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 no cdp enable
!
interface FastEthernet0/1.171
 encapsulation dot1Q 171
 ip vrf forwarding acct
 ip address 10.1.2.1 255.255.255.0
 ip access-group 111 in
 ip nat inside
 ip inspect acct-fw in
 ip virtual-reassembly
 no cdp enable
!
interface FastEthernet0/1.172
 encapsulation dot1Q 172
 ip vrf forwarding arch
 ip address 10.1.2.1 255.255.255.0
 ip access-group 111 in
 ip nat inside
 ip inspect arch-fw in
 ip virtual-reassembly
 no cdp enable
!
interface FastEthernet0/1.173
 encapsulation dot1Q 173
 ip vrf forwarding atty
 ip address 10.1.2.1 255.255.255.0
 ip access-group 111 in
 ip nat inside
 ip inspect atty-fw in
 ip virtual-reassembly
 no cdp enable
!
ip route 0.0.0.0 0.0.0.0 172.16.100.1
ip route vrf acct 0.0.0.0 0.0.0.0 172.16.100.1 global
ip route vrf arch 0.0.0.0 0.0.0.0 172.16.100.1 global
ip route vrf atty 0.0.0.0 0.0.0.0 172.16.100.1 global
!
ip nat pool pool-1 172.16.100.100 172.16.100.199 netmask
255.255.255.0 add-route
ip nat inside source list 101 pool pool-1 vrf acct
overload
ip nat inside source list 101 pool pool-1 vrf arch
overload
ip nat inside source list 101 pool pool-1 vrf atty
overload
!
! The following static NAT translations allow access
from the internet to
! servers in each VRF.  Be sure the static translations
correlate to “permit”
! statements in ACL 121, the internet-facing list.
!
ip nat inside source static tcp 10.1.2.2 21
172.16.100.11 21 vrf arch extendable
ip nat inside source static tcp 10.1.2.3 25
172.16.100.12 25 vrf acct extendable
ip nat inside source static tcp 10.1.2.4 25
172.16.100.13 25 vrf atty extendable
```

```
ip nat inside source static tcp 10.1.2.5 80
172.16.100.13 80 vrf atty extendable
!
access-list 101 permit ip 10.1.2.0 0.0.0.255 any
access-list 111 permit tcp 10.1.2.0 0.0.0.255 any eq www
access-list 111 permit tcp 10.1.2.0 0.0.0.255 any eq 443
access-list 111 permit tcp 10.1.2.0 0.0.0.255 any eq
smtp
access-list 111 permit tcp 10.1.2.0 0.0.0.255 any eq ftp
access-list 111 permit tcp 10.1.2.0 0.0.0.255 any eq
domain
access-list 111 permit udp 10.1.2.0 0.0.0.255 any eq
domain
access-list 111 permit icmp 10.1.2.0 0.0.0.255 any
access-list 121 permit tcp any host 172.16.100.11 eq ftp
access-list 121 permit tcp any host 172.16.100.12 eq
smtp
access-list 121 permit tcp any host 172.16.100.13 eq
smtp
access-list 121 permit tcp any host 172.16.100.13 eq www
end
```

Проверьте классический межсетевой экран и NAT для сети классики Одиночного Узла мульти-VRF

Контроль Трансляции сетевых адресов и Межсетевого экрана проверен для каждого VRF с этими командами:

Исследуйте маршруты в каждом VRF с **командой 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#
```

Проверьте активность NAT каждого VRF с **командой 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
```

Контролируйте статистику контроля межсетевого экрана каждого VRF с **командой 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
```

Осведомленная о VRF Cisco IOS зональный межсетевой экран IOS политики

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Если вы добавляете Zone-Based Policy межсетевой экран Cisco IOS к конфигурациям маршрутизатора мульти-VRF, это переносит мало различия от Зонального Межсетевого экрана в приложениях не-VRF. Т.е. определение политики наблюдает весь одинаковый правила, что Zone-Based Policy межсетевой экран не-VRF наблюдает, сохраните на добавление нескольких соглашений multi-VRF-specific:

- Зона безопасности Zone-Based Policy межсетевого экрана может содержать интерфейсы только от одной зоны.
- VRF может содержать несколько зон безопасности.
- Zone-Based Policy межсетевой экран зависит от маршрутизации или NAT, чтобы позволить трафику перемещаться между VRF. Политика межсетевого экрана, которая осматривает или передает трафик между Зональными Парами меж-VRF, не соответствует, чтобы разрешить трафику перемещаться между VRF.

Настройте осведомленный о VRF Zone-Based Policy межсетевой экран Cisco IOS

Осведомленный о VRF Zone-Based Policy межсетевой экран использует синтаксис одинаковой конфигурации в качестве Zone-Based Policy межсетевого экрана non-VRF-Aware, и назначает интерфейсы на зоны безопасности, определяет политику безопасности для трафика, который перемещается между зонами и назначает политику безопасности на соответствующие зонально-парные ассоциации.

Специфичная для VRF конфигурация является ненужной. Параметры глобальной конфигурации применены, пока более определенная карта параметра не добавлена к контролю на policy-map. Даже в случае, где карта параметра используется для применения более определенной конфигурации, карта параметра не специфична для VRF.

Просмотр осведомленного о VRF действия Zone-Based Policy межсетевого экрана Cisco IOS

Осведомленные о VRF **команды показа** Zone-Based Policy межсетевого экрана не отличаются от команд non-VRF-aware; Zone-Based Policy межсетевой экран применяет трафик, который перемещается от интерфейсов в одну зону безопасности к интерфейсам в другой зоне безопасности, независимо от присвоений VRF различных интерфейсов. Таким образом Осведомленный о VRF Zone-Based Policy межсетевой экран использует те же **команды показа** для просмотра действия межсетевого экрана, как используются Zone-Based Policy межсетевым экраном в приложениях не-VRF:

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

Осведомленные о VRF варианты использования Zone-Based Policy межсетевого экрана Cisco IOS

Осведомленные о VRF варианты использования межсетевого экрана значительно различаются. Эти примеры адрес:

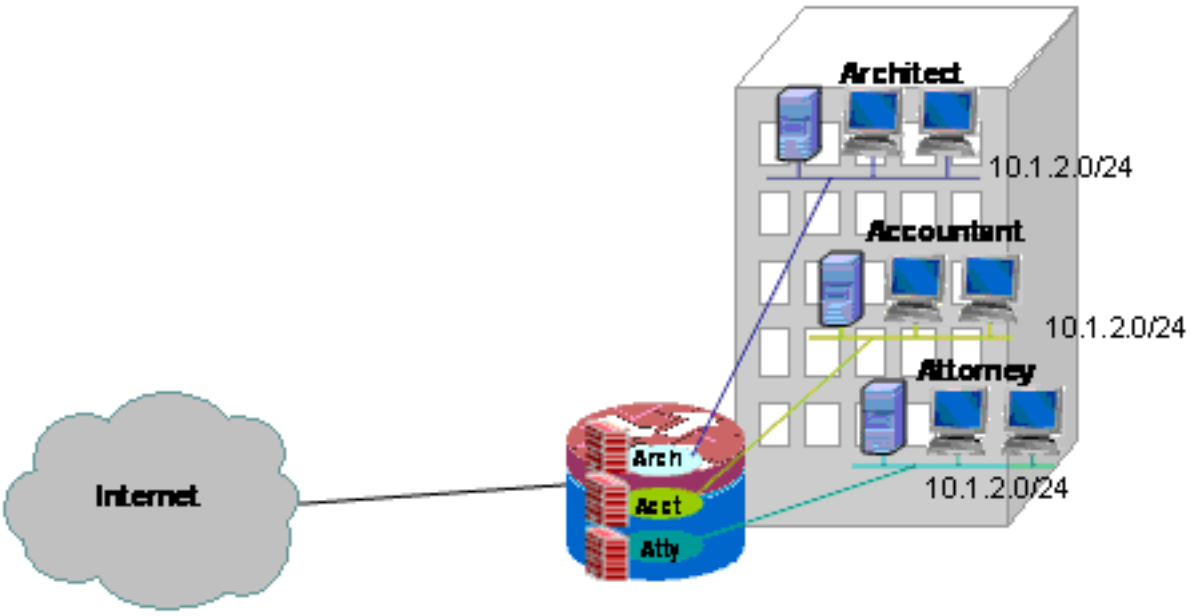
- Одиночный узел осведомленные о VRF развертывания, как правило, используемые для средств с несколькими арендаторами или розничных сетей
- Филиал компании/retail/telecommuter приложение, где трафик частной сети сохранен в отдельном VRF от трафика общего Интернета. Пользователи доступа в Интернет изолированы от пользователей коммерческой сети, и весь трафик коммерческой сети направлен по VPN-подключению к узлу HQ для интернет-приложения политики.

Межсетевой экран зональной политики с несколькими таблицами виртуальной маршрутизации и переадресации для одного объекта

Узлы с несколькими арендаторами, которые предлагают доступ в Интернет как сервис

арендатора, могут использовать осведомленный о VRF межсетевой экран для выделения адресного пространства с перекрытием и шаблонной политики межсетевого экрана для всех арендаторов. Это приложение типично для нескольких сегментов LAN на данном узле, который совместно использует один маршрутизатор Cisco IOS для доступа в Интернет, или где деловому партнеру, такому как фотофинишировавший или некоторый другой сервис предлагают отдельную сеть передачи данных с подключением к Интернету и некоторой определенной части сети владельца предпосылки без требования дополнительного сетевого оборудования или интернет-соединения. Требования для маршрутизуемого пространства, NAT, и удаленного доступа и сквозного VPN-соединение сервиса могут быть приняты также к предложению специализированных сервисов для каждого арендатора с преимуществом инициализации VRF для каждого клиента.

Это приложение использует адресное пространство с перекрытием для упрощения управления адресного пространства. Но, это может вызвать проблемы, предлагающие подключение между различными VRF. Если подключение не требуется между VRF, традиционный NAT изнутри наружу может быть применен. Кроме того, переадресация портов NAT используется для представления серверов в архитекторе (дуга), бухгалтер (acct) и поверенный (адвокат) VRF. ACL межсетевого экрана и политика должны принять активность NAT.



Настройте межсетевой экран зональной политики с несколькими таблицами виртуальной маршрутизации и переадресации для одного объекта и NAT

Узлы с несколькими арендаторами, предлагающие доступ в Интернет как сервис арендатора, могут использовать осведомленный о VRF межсетевой экран для выделения адресного пространства с перекрытием и шаблонной политики межсетевого экрана для всех арендаторов. Требования для маршрутизуемого пространства, NAT, и удаленного доступа и сквозного VPN-соединение сервиса могут быть приняты также к предложению специализированных сервисов для каждого арендатора с преимуществом инициализации VRF для каждого клиента.

Классическая Политика межсетевого экрана существует, который определяет доступ к и от различной LAN и подключений к глобальной сети (WAN):

	Источник подключения

		Интернет	Дуга	Acct	Адвокат
Назначение соединения	Интернет	Н/Д	HTTP, FTP HTTPS, DNS, SMTP	HTTP, FTP HTTPS, DNS, SMTP	HTTP, FTP HTTPS, DNS, SMTP
	Дуга	Ftp	Н/Д	Deny	Deny
	Acct	SMTP	Deny	Н/Д	Deny
	Адвокат	SMTP HTTP	Deny	Deny	Н/Д

Хосты в каждом из этих трех VRF в состоянии обратиться к HTTP, HTTPS, FTP и сервисам DNS на общедоступном Интернете. Один class-map (private-public-cmap) используется для ограничения доступа для всех трех VRF, так как каждый VRF предоставляет доступ к идентичным сервисам в Интернете, но другие polic-карты применены, чтобы предоставить инспекционную статистику на VRF. Обратно пропорционально хосты в Интернете могут соединиться с сервисами, как описано в предыдущей таблице политики, как определено отдельными командами class-map и policy-map для зональных пар Интернета к VRF. Отдельный policy-map используется для предотвращения доступа к сервисам управления маршрутизатора в самозоне из общего Интернета. Та же политика может быть применена для предотвращения доступа от частных VRF до самозоны маршрутизатора также.

Конфигурация NAT прокомментирована для описания переданного порту доступа к сервисам в VRF.

Одиночный узел Zone-Based Policy межсетевой экран с несколькими арендаторами и конфигурация NAT:

```
version 12.4
!
ip cef
!
ip vrf acct
!
ip vrf arch
!
ip vrf atty
!
class-map type inspect match-any out-cmap
 match protocol http
 match protocol https
 match protocol ftp
 match protocol smtp
 match protocol ftp
!
class-map type inspect match-all pub-arch-cmap
 match access-group 121
 match protocol ftp
!
class-map type inspect match-all pub-acct-cmap
 match access-group 122
```

```
 match protocol http
!
class-map type inspect pub-atty-mail-cmap
match access-group 123
 match protocol smtp
!
class-map type inspect pub-atty-web-cmap
 match access-group 124
 match protocol http
!
policy-map type inspect arch-pub-pmap
 class type inspect out-cmap
  inspect
!
policy-map type inspect acct-pub-pmap
 class type inspect out-cmap
  inspect
!
policy-map type inspect atty-pub-pmap
 class type inspect out-cmap
  inspect
!
policy-map type inspect pub-arch-pmap
 class type inspect pub-arch-cmap
  inspect
!
policy-map type inspect pub-acct-pmap
 class type inspect pub-acct-cmap
  inspect
!
policy-map type inspect pub-atty-pmap
 class type inspect pub-atty-mail-cmap
  inspect
 class type inspect pub-atty-web-cmap
  inspect
!
policy-map type inspect pub-self-pmap
 class class-default
  drop log
!
zone security arch
zone security acct
zone security atty
zone security public
zone-pair security arch-pub source arch destination
public
 service-policy type inspect arch-pub-pmap
zone-pair security acct-pub source acct destination
public
 service-policy type inspect acct-pub-pmap
zone-pair security atty-pub source atty destination
public
 service-policy type inspect atty-pub-pmap
zone-pair security pub-arch source public destination
arch
 service-policy type inspect pub-arch-pmap
zone-pair security pub-acct source public destination
acct
 service-policy type inspect pub-acct-pmap
zone-pair security pub-atty source public destination
atty
 service-policy type inspect pub-atty-pmap
zone-pair security pub-self source public destination
self
```

```
 service-policy type inspect pub-self-pmap
!
!
interface FastEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-FE 0$
 ip address 172.16.100.10 255.255.255.0
 ip nat outside
 zone-member security public
 ip virtual-reassembly
 speed auto
 no cdp enable
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 no cdp enable
!
interface FastEthernet0/1.171
 encapsulation dot1Q 171
 ip vrf forwarding acct
 ip address 10.1.2.1 255.255.255.0
 ip nat inside
 zone-member security acct
 ip virtual-reassembly
 no cdp enable
!
interface FastEthernet0/1.172
 encapsulation dot1Q 172
 ip vrf forwarding arch
 ip address 10.1.2.1 255.255.255.0
 ip nat inside
 zone-member security arch
 ip virtual-reassembly
 no cdp enable
!
interface FastEthernet0/1.173
 encapsulation dot1Q 173
 ip vrf forwarding atty
 ip address 10.1.2.1 255.255.255.0
 ip nat inside
 zone-member security atty
 ip virtual-reassembly
 no cdp enable
!
ip route 0.0.0.0 0.0.0.0 172.16.100.1
ip route vrf acct 0.0.0.0 0.0.0.0 172.16.100.1 global
ip route vrf arch 0.0.0.0 0.0.0.0 172.16.100.1 global
ip route vrf atty 0.0.0.0 0.0.0.0 172.16.100.1 global
!
ip nat pool pool-1 172.16.100.100 172.16.100.199 netmask
255.255.255.0 add-route
ip nat inside source list 101 pool pool-1 vrf acct
overload
ip nat inside source list 101 pool pool-1 vrf arch
overload
ip nat inside source list 101 pool pool-1 vrf atty
overload
!
! The following static NAT translations allow access
from the internet to
! servers in each VRF.  Be sure the static translations
correlate to “inspect”
! statements in in the Zone Firewall configuration, the
```

```
internet-facing list.
! Note that the ACLs used in the firewall correspond to
the end-host address, not
! the NAT Outside address
!
ip nat inside source static tcp 10.1.2.2 21
172.16.100.11 21 vrf arch extendable
ip nat inside source static tcp 10.1.2.3 25
172.16.100.12 25 vrf acct extendable
ip nat inside source static tcp 10.1.2.4 25
172.16.100.13 25 vrf atty extendable
ip nat inside source static tcp 10.1.2.5 80
172.16.100.13 80 vrf atty extendable
!
access-list 101 permit ip 10.1.2.0 0.0.0.255 any
access-list 121 permit ip any host 10.1.2.2
access-list 122 permit ip any host 10.1.2.3
access-list 123 permit ip any host 10.1.2.4
access-list 124 permit ip any host 10.1.2.5
!
! Disable CDP
!
no cdp run
!
end
```

Проверьте классический межсетевой экран и NAT для сети классики Одиночного Узла мульти-VRF

Контроль Трансляции сетевых адресов и Межсетевого экрана проверен для каждого VRF с этими командами:

Исследуйте маршруты в каждом VRF с **командой 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#
```

Проверьте активность каждого VRF NAT с командой 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 --- ---
```

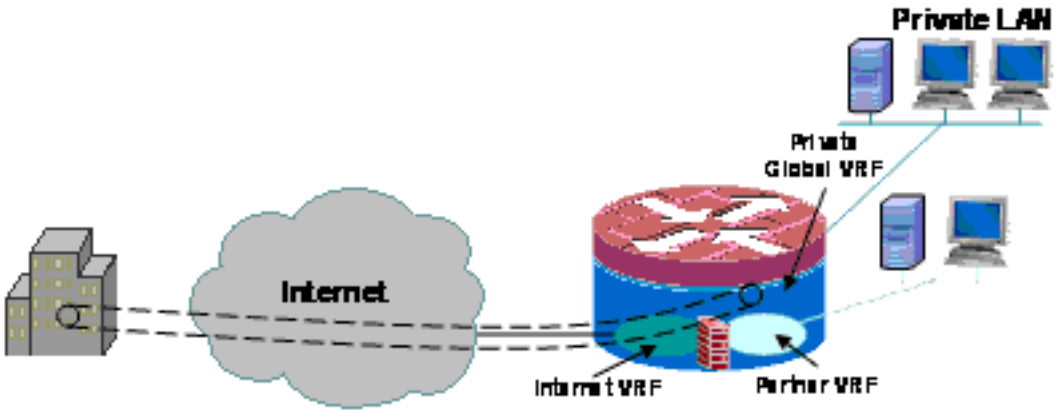
Статистика контроля межсетевого экрана монитора с **командами show policy-map type inspect zone-pair**:

```
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
```

Межсетевой экран зональной политики с несколькими таблицами виртуальной маршрутизации и переадресации для одного объекта, интернет-соединение с резервной копией в “интернет-” зоне, глобальный VRF имеет соединение с HQ

Это приложение хорошо подходит для развертываний дистанционного пользователя компьютера, небольших розничных местоположений и любого другого развертывания сети удаленного узла, которое требует сегрегации ресурсов частной сети от доступа к сети общего пользования. Путем изоляции интернет-соединения и домой или общие пользователи хот-спота к *общему* VRF и применения маршрута по умолчанию в глобальном VRF, который направляет весь трафик частной сети через VPN-туннели, ресурсы в частном, глобальном VRF и достижимом Интернетом *общем* VRF не имеют никакой достижимости друг другу, таким образом полностью удаляя угрозу частно-сетевого компромисса хоста действием общего Интернета. Кроме того, дополнительный VRF может быть настроен для обеспечения защищенного пространства маршрута для других потребителей, нуждающихся в отдельном сетевом пространстве, таких как лотерейные терминалы, банкоматы, терминалы обработки платежной карты или другие приложения. Множественный Wi-Fi SSIDs может быть настроен, чтобы предложить доступ обоим частная сеть, а также общий хот-спот.



Данный пример описывает конфигурацию для двух широкополосных интернет-соединений, применяя PAT (перегрузка NAT) для хостов в *общих* и *партнерских* VRF для доступа к общему Интернету, с интернет-соединением, которое гарантирует SLA, контролирующий на этих двух соединениях. Частная сеть (в глобальном VRF) использует GRE ПО IP-БЕЗОПАСНОМУ СОЕДИНЕНИЮ для поддержания подключения к HQ (конфигурация, включенная для маршрутизатора головного узла VPN) по этим двум широкополосным линиям связи. Если один или другие из сбоев широкополосных соединений, подключение к головному узлу VPN поддержано, который предоставляет непрерывный доступ к сети HQ, так как локальная оконечная точка туннеля не связана в частности ни к одному из Интернет-соединений.

Зональный межсетевой экран политики существует и управляет доступом к и от VPN до частной сети, и между общими и партнерскими LAN и Интернетом для разрешения исходящего доступа в Интернет, но никаких соединений в к локальным сетям из Интернета:

	Интернет	Public	Партнер	VPN	Частный
Интернет	Н/Д	Deny	Deny	Deny	Deny
Public	HTTP,	Н/Д	Deny	Deny	Deny

	HTTPS, FTP, DNS				
Партнер		Deny	Н/Д		
VPN	Deny	Deny	Deny	Н/Д	
Частный	Deny	Deny	Deny		Н/Д

Приложение NAT для хот-спота и партнерско-сетевого трафика идет на компромисс из общего гораздо менее вероятного Интернета, но возможность все еще существует, что злонамеренные пользователи или программное обеспечение могут использовать активную сессию NAT. Приложение проверки трафика потоком сводит к минимуму вероятность, что локальные хосты могут поставиться под угрозу путем нападения на открытый сеанс NAT. Данный пример использует 871 Вт, но конфигурация может быть легко реплицирована с другими платформами ISR.

Настройте Межсетевой экран зональной политики с несколькими таблицами виртуальной маршрутизации и переадресации для одного объекта, основное интернет-соединение с резервной копией, глобальный VRF имеет VPN к сценарию HQ

Узлы с несколькими арендаторами, которые предлагают доступ в Интернет как сервис арендатора, могут использовать осведомленный о VRF межсетевой экран для выделения адресного пространства с перекрытием и шаблонной политики межсетевого экрана для всех арендаторов. Требования для маршрутизуемого пространства, NAT, и удаленного доступа и сквозного VPN-соединение сервиса могут быть приняты также к предложению специализированных сервисов для каждого арендатора с преимуществом инициализации VRF для каждого клиента.

```
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
```

Эта Конфигурация концентратора предоставляет пример конфигурации возможности VPN - подключения:

```
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
```

Проверьте Межсетевой экран зональной политики с несколькими таблицами виртуальной маршрутизации и переадресации для одного объекта, основное интернет-соединение с резервной копией, глобальный VRF имеет VPN к сценарию HQ

Контроль Трансляции сетевых адресов и Межсетевого экрана проверен для каждого VRF с этими командами:

Исследуйте маршруты в каждом VRF с **командой show ip route vrf [vrf-name]**:

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

Проверьте активность NAT каждого VRF с **командой show ip nat tra vrf [vrf-name]**:

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

Статистика контроля межсетевого экрана монитора с **командами show policy-map type inspect zone-pair**:

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

Заключение

Cisco IOS Осведомленная о VRF Классика и предложения Zone-Based Policy межсетевого экрана уменьшила стоимость и административные накладные расходы для того, чтобы предоставить сетевому подключению интегрированные средства безопасности для множественных сетей с минимальными аппаратными средствами. Производительность и масштабируемость поддержаны для множественных сетей и предоставляют эффективную платформу для инфраструктуры сети и сервисов без увеличения капитальных затрат.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Проблема

Сервер Exchange не доступен от внешнего интерфейса маршрутизатора.

Решение

Включите Проверку SMTP в маршрутизаторе для устранения этой проблемы

Пример конфигурации

```
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
```

Дополнительные сведения

- Руководство по дизайну Zone-Based Policy межсетевого экрана

- Использование Zone-Based Policy межсетевого экрана с VPN
- Межсетевой экран Cisco IOS, следящий за маршрутизацией и пересылкой
- Интеграция NAT с MPLS VPN
- Разработка расширений MPLS для граничных маршрутизаторов клиента
- Проверка работы и устранение основных неисправностей NAT
- Пример конфигурации Составного контекста PIX/ASA
- (межсетевой экран Cisco IOS)
- Cisco Systems – техническая поддержка и документация