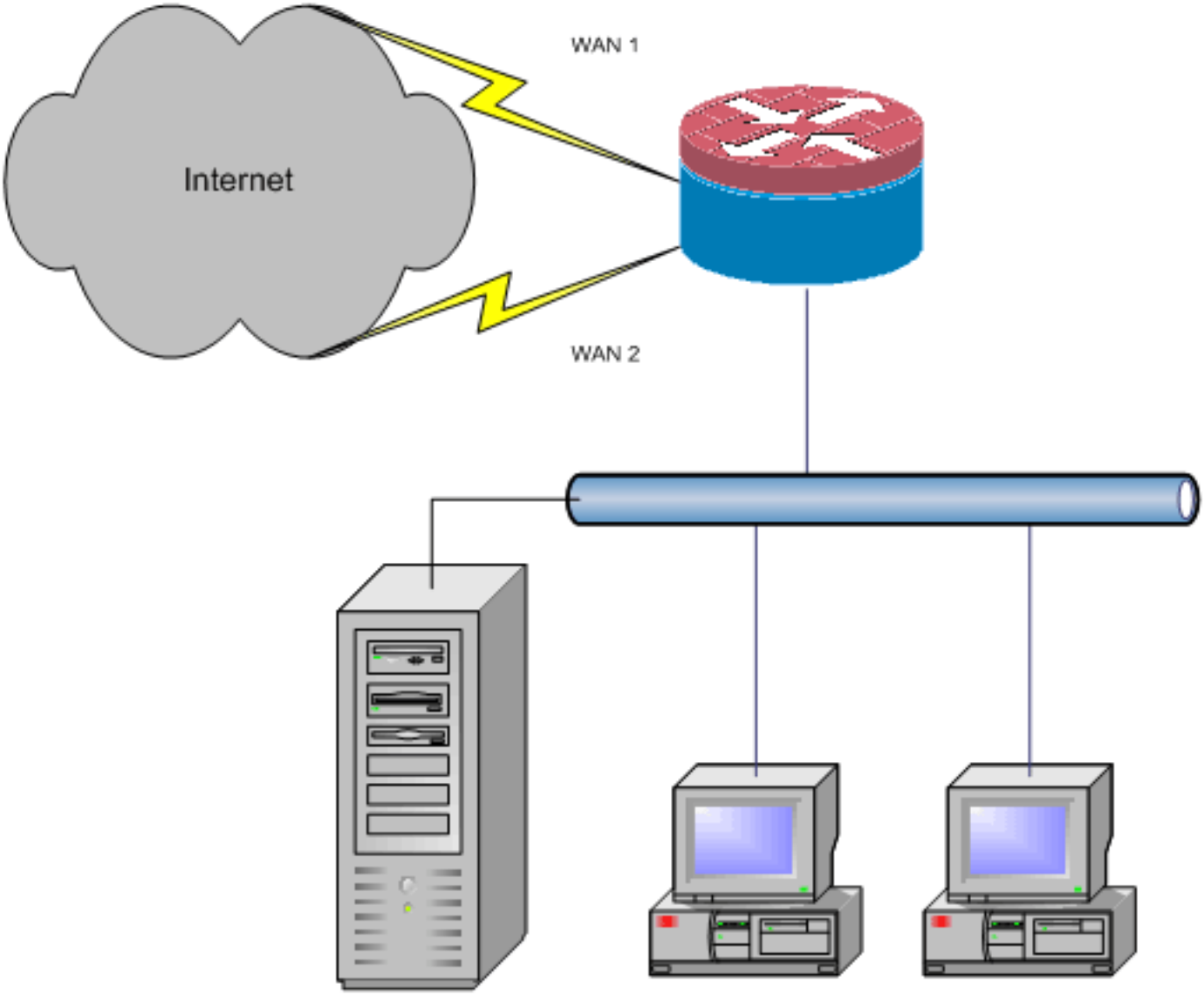
Распределение нагрузки и брандмауэр зональных политик NAT IOS с оптимизированной граничной маршрутизацией для двух подключений к Интернету

Содержание

Введение

Этот документ описывает конфигурацию для маршрутизатора Cisco IOS® для соединения сети с Интернетом с Технологией NAT через два подключения ISP. Если равноценные пути к заданному получателю доступны, ПРЕОБРАЗОВАНИЕ СЕТЕВЫХ АДРЕСОВ В CISCO IOS может распределить последующие соединения TCP и сеансы UDP несколько сетей соединения. Если одно из соединений становится неприменимым, отслеживание объектов, компонент Оптимизированной граничной маршрутизации (OER), может использоваться для деактивации маршрута, пока соединение не становится доступным снова, который гарантирует доступность сети inspite нестабильности или ненадежности Интернет-соединения.



Этот документ описывает дополнительные настройки для применения Zone-Based Policy межсетевого экрана Cisco IOS для добавления возможности проверки трафика потоком увеличить защиту базовой основы сети, обеспеченную NAT.

Предварительные условия

Требования

Этот документ предполагает, что у вас уже есть LAN и подключения к глобальной сети (WAN), которые работают, и не предоставляет конфигурацию или устранение проблем общих сведений для установления начального подключения.

Этот документ не описывает способ дифференцироваться между маршрутами. Поэтому нет никакого способа предпочесть более выбираемое соединение по менее - выбираемое соединение.

Этот документ описывает, как настроить OER, чтобы включить или отключить любой интернет-маршрут - на основе достижимости серверов DNS интернет-провайдера. Необходимо определить определенные хосты, которые достижимы через только одно из подключений ISP и не могли бы быть доступными, если то подключение ISP не доступно.

Используемые компоненты

Эта конфигурация была разработана с маршрутизатором Cisco 1811, который выполняется 12.4 (15) программное обеспечение T2 Advanced IP Services. Если другая версия программного обеспечения используется, некоторые функции могут не быть доступными, или команды настройки могли бы отличаться от показанных в этом документе. Подобные конфигурации должны быть доступными на всех платформах маршрутизатора Cisco IOS, невзирая на то, что конфигурация интерфейса будет, вероятно, варьироваться между другими платформами.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

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

Настройка

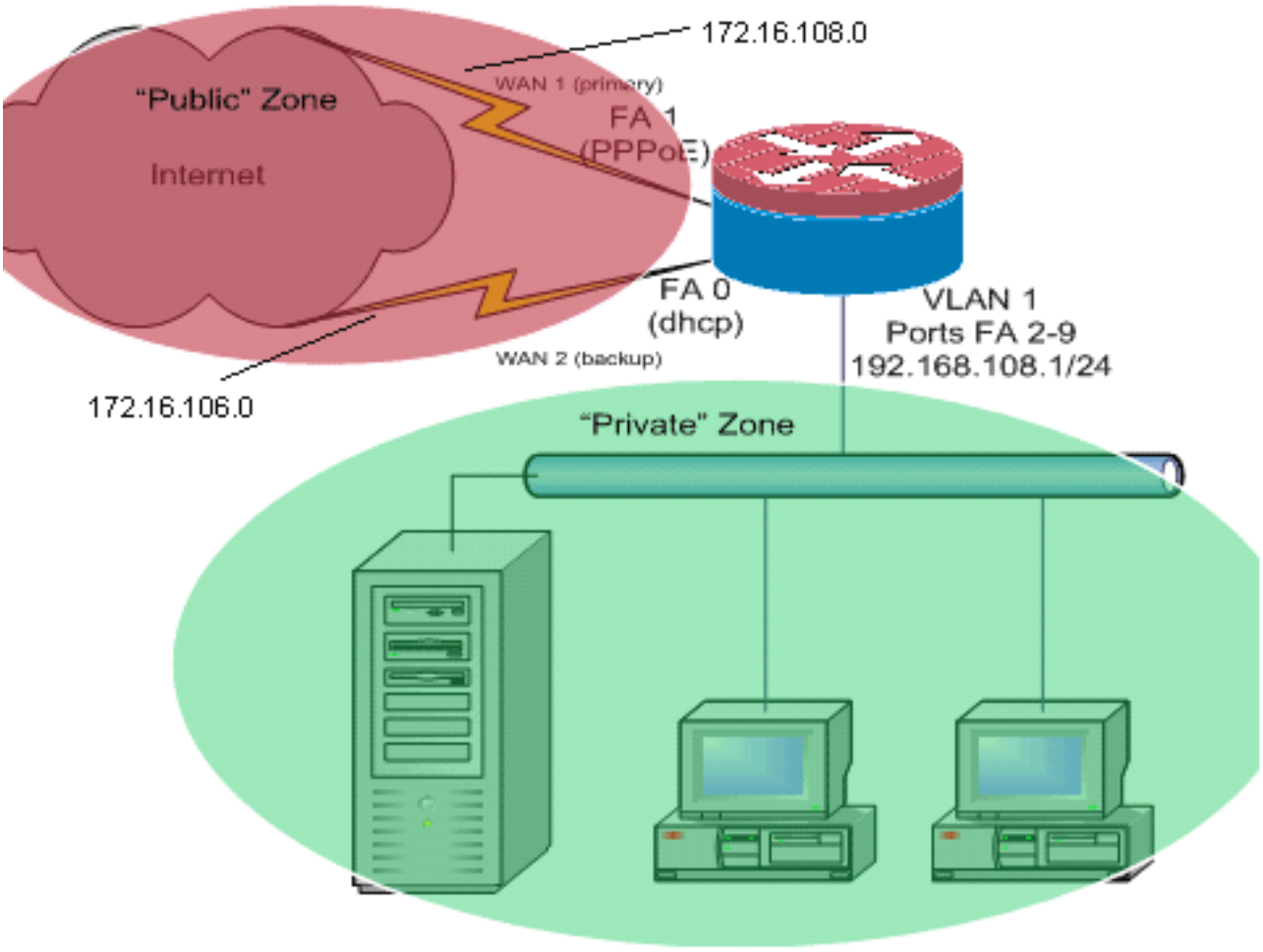
Вы, возможно, должны были бы добавить маршрутизацию на основе политик для определенного трафика, чтобы быть уверенными, что это всегда использует одно подключение ISP. Примеры трафика, который мог бы потребовать этого поведения, включают VPN-клиентов IPSec, телефоны VoIP и любой другой трафик, который должен всегда использовать только одну из опций подключения ISP для предпочтения того же IP-адреса, более высокой скорости или более низкой задержки на соединении.

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

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети:



В данном примере конфигурации, как показано в схеме сети, описан доступ к маршрутизатору, который использует IP-подключение с поддержкой конфигурации DHCP к одному ISP (обозначен как FastEthernet 0) и подключение PPPoE через другое соединение с ISP. Типы соединения не оказывают определенного влияния на конфигурацию, пока отслеживание объектов и Оптимизированная граничная маршрутизация (OER) и/или маршрутизация на основе политик не должны использоваться с назначенным на DHCP Интернет-соединением. В этих случаях может быть очень трудно определить маршрутизатор следующего перехода для маршрутизации в соответствии с политикой или OER.

Обсуждение политики межсетевого экрана

Этот пример конфигурации описывает политику межсетевого экрана, которая позволяет простой TCP, UDP и соединения ICMP от “внутренней” зоны безопасности до “внешней” зоны безопасности и принимает исходящие FTP - соединения и трафик соответствующих данных и для активных передач и для передач пассивного FTP. Любой трафик сложного приложения (например, VoIP передача сигналов и среды), который не обрабатывается этой основной политикой, будет, вероятно, работать с уменьшенной возможностью или может отказать полностью. Эта политика межсетевого экрана блокирует все соединения от “общей” зоны безопасности до “частной” зоны, которая включает все соединения, которые приняты передачей Порта NAT. Необходимо создать дополнительные конфигурации политики межсетевого экрана для размещения дополнительного трафика, который не обрабатывается этой базовой конфигурацией.

При наличии вопросов на дизайне политики Zone-Based Policy межсетевого экрана и конфигурации, обратитесь к Руководству по дизайну Zone-Based Policy межсетевого экрана

и Руководству по приложениям.

Конфигурация интерфейса командой строки CLI

Конфигурация ИНТЕРФЕЙСА КОМАНДНОЙ СТРОКИ (CLI) CISCO IOS

```
track timer interface 5
!
!
track 123 rtr 1 reachability
 delay down 15 up 10
!
track 345 rtr 2 reachability
 delay down 15 up 10
!
!---Configure timers on route tracking class-map type
inspect match-any priv-pub-traffic match protocol ftp
match protocol tcp match protocol udp match protocol
icmp ! policy-map type inspect priv-pub-policy class
type inspect priv-pub-traffic inspect class class-
default ! zone security public zone security private
zone-pair security priv-pub source private destination
public service-policy type inspect priv-pub-policy ! !
interface FastEthernet0 ip address dhcp ip dhcp client
route track 345 ip nat outside ip virtual-reassembly
zone security public ! !---Use “ip dhcp client route
track [number]” !--- to monitor route on DHCP interfaces
!--- Define ISP-facing interfaces with “ip nat outside”
interface FastEthernet1 no ip address pppoe enable no
cdp enable ! interface FastEthernet2 no cdp enable !
interface FastEthernet3 no cdp enable ! interface
FastEthernet4 no cdp enable ! interface FastEthernet5 no
cdp enable ! interface FastEthernet6 no cdp enable !
interface FastEthernet7 no cdp enable ! interface
FastEthernet8 no cdp enable ! interface FastEthernet9 no
cdp enable ! ! interface Vlan1 description LAN Interface
ip address 192.168.108.1 255.255.255.0 ip nat inside ip
virtual-reassembly ip tcp adjust-mss 1452 zone security
private !--- Define LAN-facing interfaces with “ip nat
inside” ! ! Interface Dialer 0 description PPPoX dialer
ip address negotiated ip nat outside ip virtual-
reassembly ip tcp adjust-mss zone security public !---
Define ISP-facing interfaces with “ip nat outside" ! ip
route 0.0.0.0 0.0.0.0 dialer 0 track 123 ! ! ip nat
inside source route-map fixed-nat interface Dialer0
overload ip nat inside source route-map dhcp-nat
interface FastEthernet0 overload !---Configure NAT
overload (PAT) to use route-maps ! ! ip sla 1 icmp-echo
172.16.108.1 source-interface Dialer0 timeout 1000
threshold 40 frequency 3 !---Configure an OER tracking
entry to monitor the !---first ISP connection ! ! ! ip
sla 2 icmp-echo 172.16.106.1 source-interface
FastEthernet0 timeout 1000 threshold 40 frequency 3 !---
Configure a second OER tracking entry to monitor !---the
second ISP connection ! ! ! ip sla schedule 1 life
forever start-time now ip sla schedule 2 life forever
start-time now !---Set the SLA schedule and duration ! !
! access-list 110 permit ip 192.168.108.0 0.0.0.255 any
!--- Define ACLs for traffic that will be !--- NATed to
the ISP connections ! ! ! route-map fixed-nat permit 10
match ip address 110 match interface Dialer0 ! route-map
dhcp-nat permit 10 match ip address 110 match interface
```

```
FastEthernet0 !--- Route-maps associate NAT ACLs with
NAT !--- outside on the ISP-facing interfaces
```

Используйте назначенное на dhcp отслеживание маршрута:

Конфигурация ИНТЕРФЕЙСА КОМАНДНОЙ СТРОКИ (CLI) CISCO IOS
interface FastEthernet0 description Internet Intf ip dhcp client route track 123 ip address dhcp ip nat outside ip virtual-reassembly speed 100 full-duplex no cdp enable

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

- **show ip nat translation — отображает активность NAT между внутренними и внешними хостами NAT.** Данная команда предоставляет подтверждение, что внутренние хосты переводятся на внешние адреса NAT.`Router#show ip nat tra Pro Inside global Inside local Outside local Outside global tcp 172.16.108.44:54486 192.168.108.3:54486 172.16.104.10:22 172.16.104.10:22 tcp 172.16.106.42:49620 192.168.108.3:49620 172.16.102.11:80 172.16.102.11:80 tcp 172.16.108.44:1623 192.168.108.4:1623 172.16.102.11:445 172.16.102.11:445 Router#`
- **show ip route – проверяет доступность нескольких маршрутов к Интернету.**`Router#show ip route 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 172.16.108.1 to network 0.0.0.0 C 192.168.108.0/24 is directly connected, Vlan1 172.16.0.0/24 is subnetted, 2 subnets C 172.16.108.0 is directly connected, FastEthernet4 C 172.16.106.0 is directly connected, Vlan106 S* 0.0.0.0/0 [1/0] via 172.16.108.1 [1/0] via 172.16.106.1`
- **сеансы show policy-map type inspect zone-pair** — Отображают действие контроля межсетевого экрана между узлами частной зоны и обще-зональными хостами. Эта команда предоставляет проверку, что трафик на внутренних хостах осмотрен, когда хосты связываются с сервисами в зоне внешней безопасности.

Устранение неполадок

Проверьте эти элементы, если соединения не работают после настройки маршрутизатора Cisco IOS с NAT:

- NAT применяется соответствующим образом на внешних и внутренних интерфейсах.

- Конфигурация NAT выполнена, а списки ACL отображают трафик, для которого необходимо преобразование сетевых адресов.
- Доступны несколько маршрутов к Интернету/WAN.
- При использовании отслеживания маршрута проверьте состояние отслеживания маршрута, чтобы гарантировать, что Интернет-соединения доступны.
- Политика межсетевого экрана точно отражает природу трафика, который вы хотите позволить через маршрутизатор.

Дополнительные сведения

- (межсетевой экран Cisco IOS)
- Справочник по командам сервисов IP-адресации Cisco IOS - команды NAT
- Дизайн и руководство по Zone-Based Policy межсетевому экрану
- Руководство по конфигурации оптимизированной граничной маршрутизации Cisco IOS, выпуск 12.4T
- Cisco Systems – техническая поддержка и документация