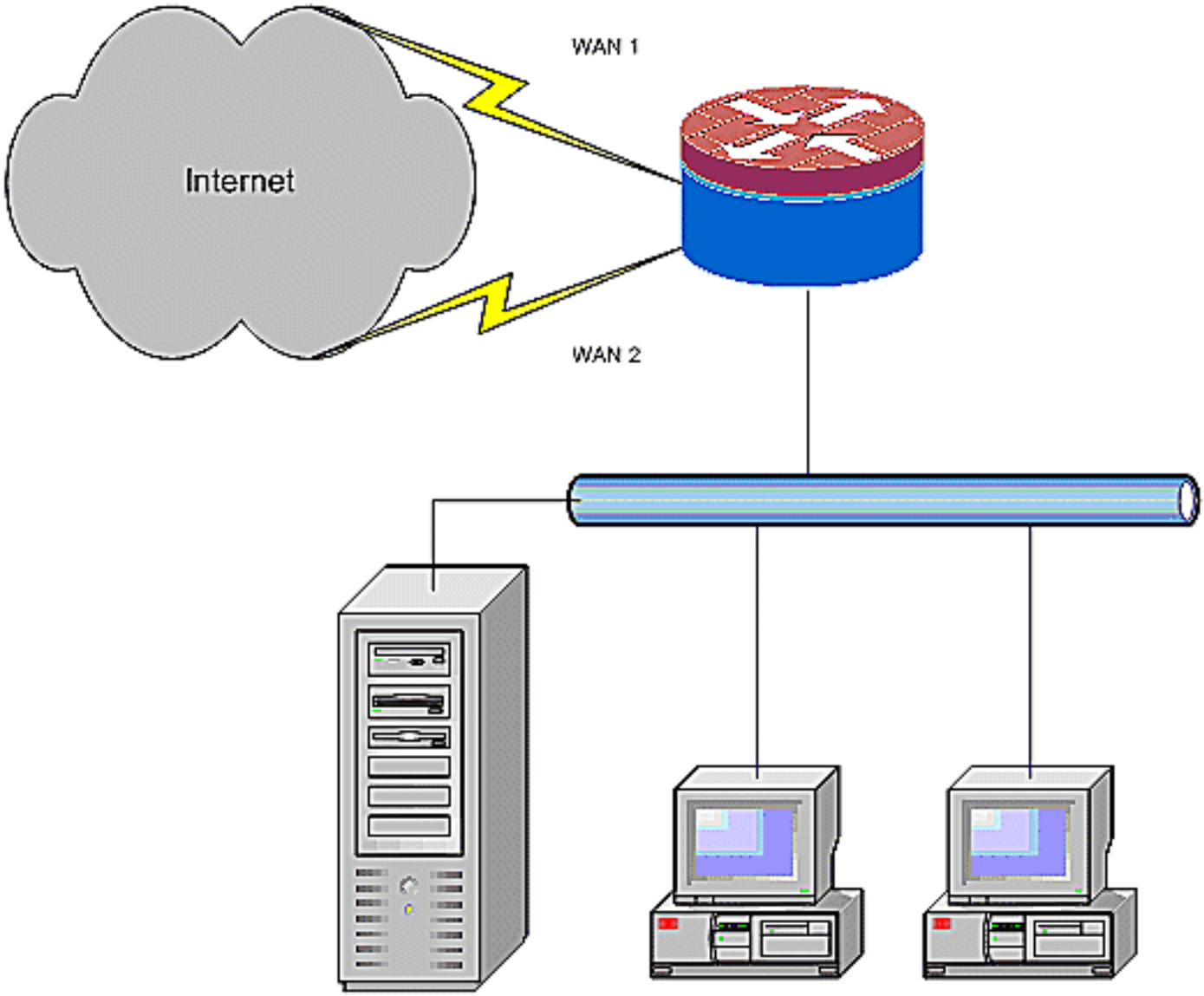
Распределение нагрузки NAT IOS с брандмауэром зональных политик для двух подключений ISP

Содержание

Введение

Этот документ предоставляет пример конфигурации для маршрутизатора Cisco IOS® для соединения сети с Интернетом с Технологией NAT посредством двух подключений ISP. Если равноценные пути к заданному получателю доступны, NAT программного обеспечения Cisco IOS может распределить последующие соединения TCP и сеансы UDP несколько сетей соединения.



Этот документ описывает дополнительную настройку для применения Zone-Based Policy межсетевого экрана Cisco IOS (ZFW) для добавления возможности проверки трафика потоком увеличить защиту базовой основы сети, обеспеченную NAT.

Предварительные условия

Требования

Этот документ предполагает, что вы работаете с LAN и подключениями к глобальной сети (WAN), и не предоставляет конфигурацию или устранение проблем общих сведений для установления начального подключения. В данном документе не описано, как различать маршруты, поэтому здесь не предлагается способ предпочесть более желательное соединение менее желательному.

Используемые компоненты

Сведения в этом документе основываются на маршрутизаторе Cisco серии 1811 года с 12.4

(15) программное обеспечение T3 Advanced IP Services. Если другая версия программного обеспечения используется, некоторые функции не доступны, или команды настройки могут отличаться от показанных в этом документе. Подобная конфигурация доступна на всех платформах маршрутизатора Cisco IOS, невзирая на то, что конфигурация интерфейса, вероятно, варьируется 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

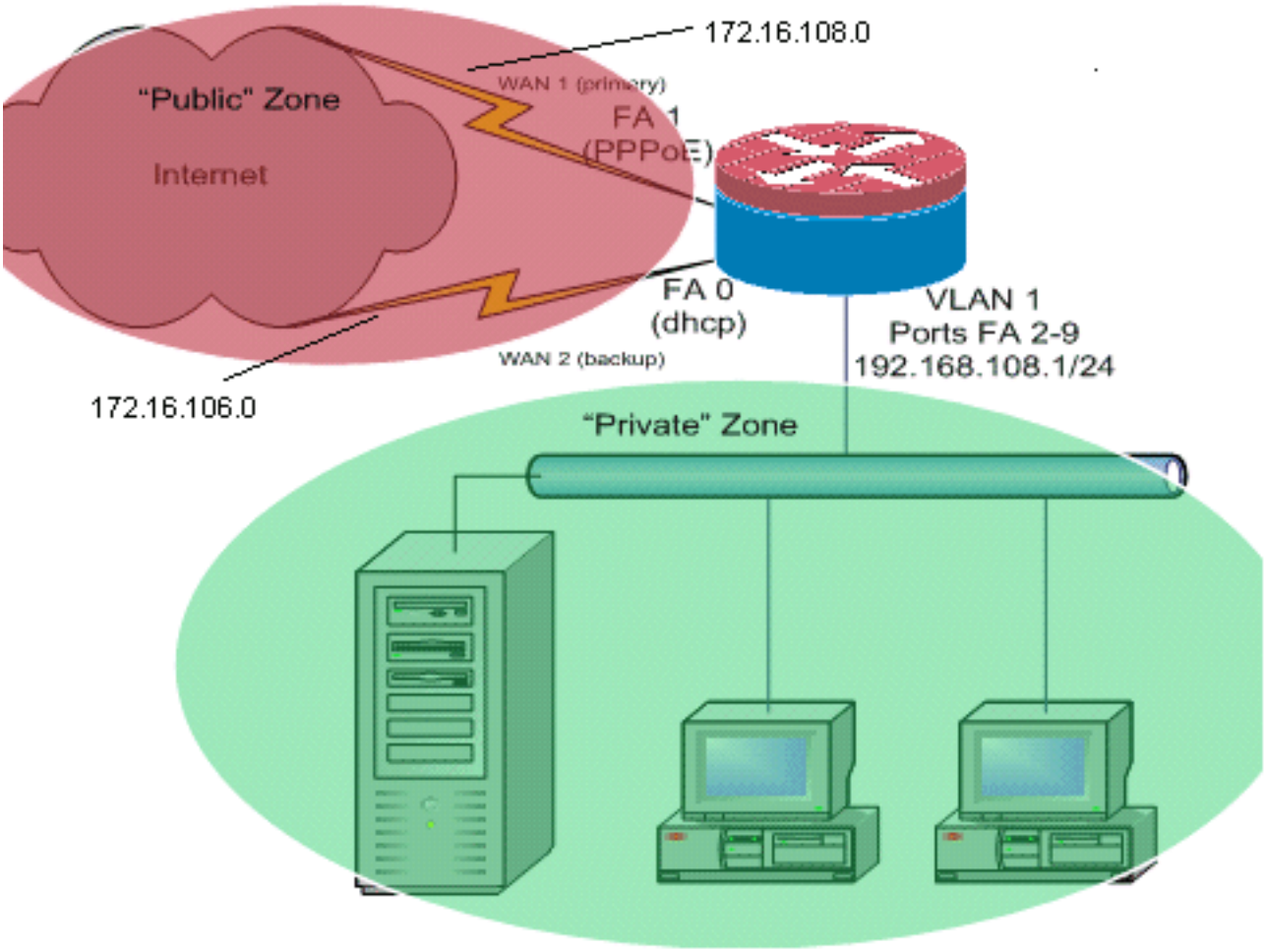
В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

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

Необходимо добавить маршрутизацию на основе политики для особого трафика, чтобы обеспечить использование им только одного соединения с ISP. Примеры трафика, который может потребовать этого поведения, включают VPN-клиентов IPSec, трафик телефонии VoIP и любой другой трафик, который использует только одну из опций подключения ISP для предпочтения того же IP-адреса, более высокой скорости или более низкой задержки на соединении.

Схема сети

В настоящем документе используется следующая схема сети:



Этот пример конфигурации описывает маршрутизатор доступа, который использует настроенный через DHCP IP - подключение для одного интернет-провайдера (как показано FastEthernet 0), и соединение PPPoE по другому подключению ISP. Типы соединения не оказывают определенного влияния на конфигурацию, но некоторые типы соединений могут препятствовать удобству пользования этой конфигурации в определенных сценариях отказов. Это происходит особенно в случаях, где возможность подключения с помощью IP-адреса по связанному с Ethernet сервису глобальной сети (WAN) используется, например, кабельный модем или услуги DSL, где дополнительное устройство завершает возможность подключения к глобальной сети (WAN) и предоставляет переключение Ethernet маршрутизатору Cisco IOS. В случаях, где статическая ip адресация применена, в противоположность назначенным на DHCP адресам или PPPoE, и Сбой WAN происходит, такой, что Порт Ethernet все еще поддерживает Соединение Ethernet к устройству возможности подключения к глобальной сети (WAN), маршрутизатор продолжает пытаться распределить нагрузку подключение и через хорошие и через плохие подключения к глобальной сети (WAN). Если ваши развертывания требуют, чтобы неактивные маршруты были удалены из распределения нагрузки, обратитесь к конфигурации, предоставленной в Распределении нагрузки ПРЕОБРАЗОВАНИЯ СЕТЕВЫХ АДРЕСОВ В CISCO IOS и Zone-Based Policy межсетевом экране с Оптимизированной граничной маршрутизацией Для Двух Интернет-соединений, которая описывает добавление Оптимизированной граничной маршрутизации для мониторинга законности маршрута.

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 эквивалентных

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, вероятно, работает 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 переадресацией портов NAT. Если необходимо, необходимо отрегулировать политику проверки межсетевого экрана для отражения профиля приложения и политики безопасности.

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.

Конфигурации

Эти конфигурации используются в данном документе:

!--- конфигурацию

```
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 nat outside ip virtual-
reassembly zone security public ! interface
FastEthernet1 no ip address pppoe enable no cdp enable !
interface FastEthernet2 no cdp enable !--- Output
Suppressed 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 ! 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 ! 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
```

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 translation** 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 “частным” - зональными хостами и “общественностью” - зональные хосты. Эта команда предоставляет проверку, что трафик внутренних хостов осмотрен, когда хосты связываются с сервисами во “внешней” зоне безопасности.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Если соединения не работают после настройки маршрутизатора Cisco IOS с помощью NAT, убедитесь, что:

- 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.
- Политика межсетевого экрана точно отражает природу трафика, который вы хотите позволить через маршрутизатор.

Дополнительные сведения

- Поддержка голосовых технологий
- Поддержка продуктов Голосовой и Унифицированной связи
- Устранение неполадок в системах IP-телефонии Cisco
- Дизайн и руководство по Zone-Based Policy межсетевому экрану
- Cisco Systems – техническая поддержка и документация