Содержание

Cisco IOSÂ® Software Release 12.4 (6) T представила Zone-Based Policy межсетевой экран (ZBPFW), новую модель конфигурации для Набора функций межсетевого экрана Cisco IOS. Эта новая модель конфигурации обладает интуитивно понятными политиками для межсетевых экранов с несколькими интерфейсами, повышенной детализацией приложения политики межсетевого экрана и политикой запрета всего трафика между зонами безопасности межсетевого экрана, которая применяется ко всему желательному трафику вплоть до применения явной политики.

Zone-Based Policy межсетевой экран (также известный как Межсетевой экран Зональной Политики или ZFW) изменяет конфигурацию межсетевого экрана от более старой основанной на интерфейсе модели (CBAC) к более гибкому, большему количеству понятной зональной модели. Интерфейсы присваиваются зонам, а политика проверки — трафику, передаваемому между зонами. Межзонные политики отличаются значительной гибкостью и детализацией. Поэтому различные политики проверки можно применять к нескольким группам узлов, связанных с одним и тем же интерфейсом маршрутизатора.

Политика межсетевого экрана настроена с CiscoÂ® Policy Language (CPL), который использует иерархическую структуру для определения контроля для сетевых протоколов и групп хостов, к которым будет применен контроль.

Предварительные условия

Требования

Cisco рекомендует иметь основное понимание Cisco IOSÂ® CLI.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Series маршрутизаторы Cisco 2900
- Выпуск ПО IOS 15.2 (4) M2

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.

Поддержка WAAS с межсетевым экраном Cisco IOS

WAAS (Сервисы WAAS) поддержка с межсетевым экраном Cisco IOS был представлен в Cisco IOS Release 12.4 (15) T. Это предоставляет интегрированный межсетевой экран, который оптимизирует совместимые безопасностью глобальные сети (WAN) и решения для ускорения приложений со следующими преимуществами:

- Оптимизирует глобальную сеть (WAN) через полные возможности проверки трафика потоком.
- Упрощает соответствие Отрасли платежной карты (PCI).
- Защищает ускоренный трафик прозрачной глобальной сети (WAN).
- Интегрирует сети WAAS прозрачно.
- Поддерживает Оборудование управления сетью (NME) WAE (Глобальное Ядро приложения) модули или автономные развертывания устройства WAAS.

WAAS имеет механизм автоматического обнаружения, который использует параметры TCP во время начального трехэтапного установления связи, используемого для определения устройств WAE прозрачно. После автоматического обнаружения оптимизированные трафики (пути) испытывают изменение в порядковом номере TCP, чтобы позволить оконечным точкам различать оптимизированные и неоптимизированные трафики.

Поддержка WAAS межсетевого экрана IOS обеспечивает корректировку внутренних переменных состояния TCP, используемых для контроля уровня 4, на основе сдвига в упомянутом выше порядковом номере. Если межсетевой экран Cisco IOS замечает, что трафик успешно завершил автоматическое обнаружение WAAS, это разрешает сдвиг исходного порядкового номера для трафика и поддерживает состояние Уровня 4 на оптимизированном трафике.

Сценарии развертывания оптимизации трафика WAAS

Следующие разделы описывают два других сценария оптимизации трафика WAAS для развертываний в филиалах компании. Оптимизация трафика WAAS работает с характеристикой межсетевого экрана Cisco на Cisco ISR (ISR).

Рисунок ниже показов пример сквозной оптимизации трафика WAAS с межсетевым экраном Cisco. В этих определенных развертываниях Оборудование управления сетью (NME)-WAE устройство находится на том же устройстве как межсетевой экран Cisco. Протокол WCCP используется для перенаправления трафика для перехвата.

- **Развертывания ответвления WAAS с устройством вне пути**
- **Развертывания ответвления WAAS со встроенным устройством**

Развертывания ответвления WAAS с устройством вне пути

Глобальное Ядро приложения (WAE), устройство может быть или автономным устройством Механизма автоматизации глобальной сети (WAN) (WAE) Cisco или Cisco Сетевой модуль WAAS (NME-WAE) , который установлен на Маршрутизаторе ISR (ISR) как механизм интегрированного сервиса (как показано в Развертываниях Ответвления Сервиса WAAS [WAAS] рисунка).

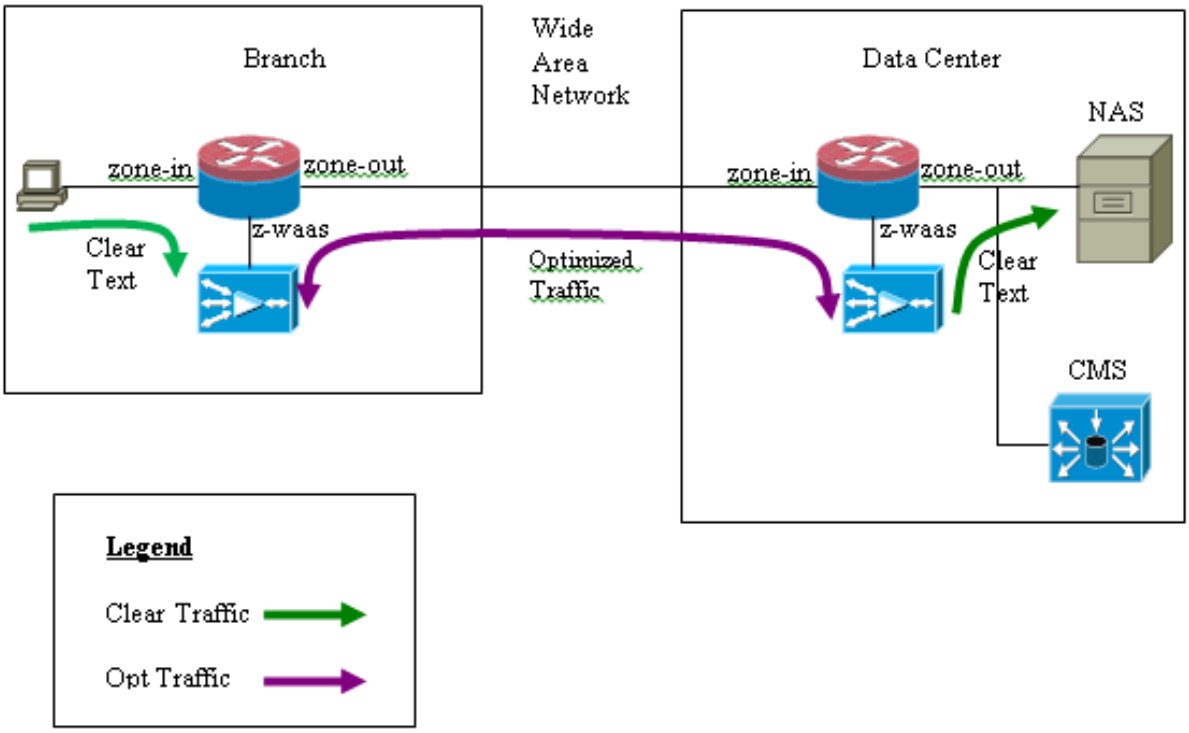
Рисунок ниже показов развертывания ответвления WAAS, которые используют протокол WCCP для перенаправления трафика к автономному устройству WAE вне пути для перехвата трафика. Конфигурация для этой опции совпадает с развертываниями ответвления WAAS с NME-WAE.

Пример схемы сети

Конфигурация и поток пакетов

Ниже приводится схема, изображающая настройку в качестве примера с оптимизацией WAAS, включенной для сквозного трафика и CMS

(Система централизованного управления) присутствующий в конце Сервера. waas подарок модулей в конце Ответвления и конце ЦОД должен зарегистрироваться в CMS для их операций. Замечено, что CMS использует HTTPS для него? s связь с модулями WAAS.



Сквозной трафик WAAS

Следующий пример предоставляет сквозную конфигурацию оптимизации трафика WAAS для межсетевого экрана Cisco IOS, который использует WCCP для перенаправления трафика к устройству WAE для перехвата трафика

Раздел 1: WCCP FW IOS отнесся Config

```
ip wccp 61ip wccp 62ip inspect waas enable
```

Раздел 2: Config политики FW IOS

```
class-map type inspect most-traffic match protocol icmp match protocol ftp match protocol tcp
match protocol udp!policy?map type inspect p1 class type inspect most?traffic  inspect class
class?default  drop
```

Раздел 3: FW IOS Зональный и Зонально-парный config

```
zone security zone-inzone security zone-outzone security z-waas zone?pair security in?out source
zone-in destination zone-outservice?policy type inspect p1zone?pair security out-in source zone-
out destination zone-inservice?policy type inspect p1
```

Раздел 4: Интерфейсный config

```
interface GigabitEthernet0/0 description Trusted interface ip address 172.16.11.1 255.255.255.0
ip wccp 61 redirect in zone?member security zone-in

!interface GigabitEthernet0/1 description Untrusted interface ip address 203.0.113.1
255.255.255.0 ip wccp 62 redirect in zone?member security zone-out
```

Обратите внимание на новую конфигурацию в Cisco IOS Release 12.4 (20) T и 12.4 (22), T размещает механизм интегрированного сервиса в свою собственную зону и не должен быть частью никого зонально-парного. Зональные пары настроены между зоной - в и зоной.

```
interface Integrated?Service?Enginel/0 ip address 192.168.10.1 255.255.255.0 ip wccp redirect
exclude in zone?member security z-waas
```

Без зоны, настроенной на Интегрированном? Сервис? Трафик Enginel/0 отброшен со следующим сообщением отбрасывания:

```
*Mar 9 11:52:30.647: %FW-6-DROP_PKT: Dropping tcp session 172.16.11.59:44191 172.16.10.10:80 due
to One of the interfaces not being cfged for zoning with ip ident 0
```

Трафик CMS (устройство WAAS, регистрирующееся в Центральном Менеджере)

Следующий пример предоставляет config для обоих упомянутые ниже сценарии:

- сквозная конфигурация оптимизации трафика WAAS для межсетевого экрана Cisco IOS, который использует WCCP для перенаправления трафика к устройству WAE для перехвата трафика
- Разрешение трафика CMS (трафик управления WAAS плавный CMS к/ота от/к устройства WAAS).

Раздел 1: WCCP FW IOS отнесся Config

```
ip wccp 61ip wccp 62ip inspect waas enable
```

Раздел 2: Config политики FW IOS

```
class-map type inspect most-traffic match protocol icmp match protocol ftp match protocol tcp
match protocol udppolicy?map type inspect p1 class type inspect most?traffic  inspect class
class?default  drop
```

Раздел 2. 1: политика FW IOS отнеслась к трафику CMS

Обратите внимание, что карта классов ниже необходима, чтобы позволить трафику CMS проходить.

```
class-map type inspect waas-special match access-group 123policy-map type inspect p-waas-man
class type inspect waas-special   pass class class-default  drop
```

Раздел 3: FW IOS Зональный и Зонально-парный config

```
zone security zone-inzone security zone-outzone security z-waas zone?pair security in?out source
zone-in destination zone-outservice?policy type inspect p1zone?pair security out?in source zone-
out destination zone-inservice?policy type inspect p1
```

Раздел 3. 1: CMS FW IOS отнесся Зональный и Зонально-парный config

Обратите внимание на зональных пар ***waas***, и-***waas*** требуются, чтобы применять политику, созданную выше для трафика CMS.

```
zone-pair security waas-out source z-waas destination zone-outservice-policy type inspect p-
waas-manzone-pair security out-waas source zone-out destination z-waasservice-policy type
inspect p-waas-man
```

Раздел 4: Интерфейсный config

```
interface GigabitEthernet0/0
description Trusted interface
ipaddress 172.16.11.1 255.255.255.0
ip wccp 61 redirect in
zone?member security zone-in
!
interface GigabitEthernet0/1
description Untrusted interface
ip address 203.0.113.1 255.255.255.0
ip wccp 62 redirect in
zone?member security zone-out! interface Integrated?Service?Enginel/0
ip address 192.168.10.1 255.255.255.0
```

```
ip wccp redirect exclude in
zone?member security z-waas
```

Раздел 5: Access-list для трафика CMS

Обратите внимание на Access-list, который используется для трафика CMS. Это позволяет Трафик HTTPS в обоих направления, поскольку трафик CMS является HTTPS.

```
access-list 123 permit tcp any eq 443 anyaccess-list 123 permit tcp any any eq 443
```

Информация о сеанса ZBF

Пользователь в 172.16.11.10 позади маршрутизатора R1 обращается к файловому серверу, размещенному позади удаленного конца с IP-адресом 172.16.10.10, сеанс ZBF создан из зонально-парного изменяемого, и после того маршрутизатор перенаправляет пакет к механизму WAAS для оптимизации.

```
R1#sh policy-map type inspect zone-pair in-out sesspolicy exists on zp in-out  Zone-pair: in-out
Service-policy inspect : p1    Class-map: most-traffic (match-any)      Match: protocol icmp
0 packets, 0 bytes        30 second rate 0 bps      Match: protocol ftp        0 packets, 0
bytes        30 second rate 0 bps      Match: protocol tcp        2 packets, 64 bytes        30
second rate 0 bps      Match: protocol udp        0 packets, 0 bytes        30 second rate 0 bps
Inspect      Number of Established Sessions = 1      Established Sessions        Session
3D4A32A0 (172.16.11.10:49300)=>(172.16.10.10:445) tcp SIS_OPEN/TCP_ESTAB          Created
00:00:40, Last heard 00:00:10          Bytes sent (initiator:responder) [0:0]
```

Сеанс, созданный в R1-WAAS и R2-WAAS из хоста удаленного сервера.

R1-WAAS

```
R1-WAAS#show statistics connectionCurrent Active Optimized Flows:                       1
Current Active Optimized TCP Plus Flows:          1   Current Active Optimized TCP Only Flows:
0   Current Active Optimized Single Sided Flows:      0   Current Active Optimized TCP
Preposition Flows:   0Current Active Auto-Discovery Flows:                 1Current Reserved
Flows:                              10Current Active Pass-Through Flows:
0Historical Flows:                                    13D:DRE,L:LZ,T:TCP Optimization RR:Total
Reduction RatioA:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,I:ICA,M:MAPI,N:NFS,S:SSL,W:WAN
SECURE,V:VIDEO, X: SMB Signed ConnectionConnID        Source IP:Port          Dest IP:Port
PeerID Accel RR    14    172.16.11.10:49185   172.16.10.10:445 c8:9c:1d:6a:10:61 TCDL  00.0%
```

R2-WAAS

```
R2-WAAS#show statistics connectionCurrent Active Optimized Flows:                       1
Current Active Optimized TCP Plus Flows:          1   Current Active Optimized TCP Only Flows:
0   Current Active Optimized TCP Preposition Flows:   0Current Active Auto-Discovery Flows:
0Current Reserved Flows:                              10Current Active Pass-Through Flows:
0Historical Flows:                                    9D:DRE,L:LZ,T:TCP Optimization RR:Total
Reduction RatioA:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEOConnID
Source IP:Port          Dest IP:Port            PeerID Accel RR    10    172.16.11.10:49185
172.16.10.10:445 c8:9c:1d:6a:10:81 TCDL  00.0%
```

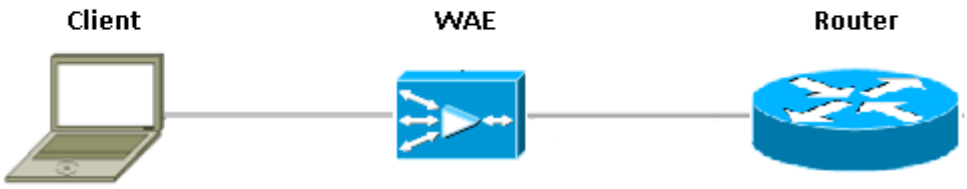
Действующая конфигурация маршрутизатора (R1) клиентской стороны с WAAS и ZBF включена.

```
R1#sh runBuilding configuration...Current configuration : 3373 bytes!hostname R1!boot-start-
markerboot bootstrap tftp c2900-universalk9-mz.SPA.153-3.M4.bin 255.255.255.255boot system flash
c2900-universalk9-mz.SPA.153-3.M4.binboot-end-marker!ip wccp 61ip wccp 62no ipv6 cef!parameter-
map type inspect global WAAS enable log dropped-packets enable max-incomplete low 18000 max-
incomplete high 20000multilink bundle-name authenticated!license udi pid CISCO2911/K9 sn
FGL171410K8license boot module c2900 technology-package securityk9license boot module c2900
technology-package uck9license boot module c2900 technology-package datak9hw-module pvdm 0/1!hw-
module sm 1!class-map type inspect match-any most-traffic match protocol icmp match protocol ftp
match protocol tcp match protocol udp!policy-map type inspect p1 class type inspect most-traffic
```

```
inspect class class-default  drop!zone security in-zonezone security out-zonezone security waas-
zonezone-pair security in-out source in-zone destination out-zone service-policy type inspect
p1zone-pair security out-in source out-zone destination in-zone service-policy type inspect
p1!interface GigabitEthernet0/0 description Connection to IPMAN FNN N6006654R bandwidth 6000 ip
address 203.0.113.1 255.255.255.0 ip wccp 62 redirect in ip flow ingress ip flow egress zone-
member security out-zone duplex auto speed auto!interface GigabitEthernet0/1 ip address
172.16.11.1 255.255.255.0 no ip redirects no ip proxy-arp ip wccp 61 redirect in zone-member
security in-zone duplex auto speed auto!interface SM1/0 description WAAS Network Module Device
Name dciacbra01c07 ip address 192.168.10.1 255.255.255.0 ip wccp redirect exclude in service-
module ip address 192.168.183.46 255.255.255.252 !Application: Restarted at Sat Jan  5 04:47:14
2008 service-module ip default-gateway 192.168.183.45 hold-queue 60 out!end
```

Развертывания ответвления WAAS со встроенным устройством

Рисунок ниже показов развертывания ответвления Сервиса WAAS (WAAS), которые имеют встроенное Глобальное Ядро приложения (WAE) устройство, которое является физически перед Маршрутизатором ISR (ISR). Поскольку устройство WAE перед устройством, межсетевой экран Cisco получает оптимизированные пакеты WAAS, и в результате контроль Уровня 7 на клиентской стороне не поддерживается.



Маршрутизатор, выполняющий Межсетевой экран IOS между устройствами WAAS, видит только оптимизированный трафик. Функция ZBF наблюдает за начальным трехэтапным квитированием (параметр TCP 33 и сдвиг порядкового номера), и это автоматически отрегулировало ожидаемое окно последовательности TCP (doesn? t изменяют порядковый номер в самом пакете). Это применяется, полные функции самонастраивающегося межсетевого экрана L4 WAAS оптимизировали сеансы. WAAS прозрачное решение упрощает Межсетевой экран, принуждают на самонастраивающийся межсетевой экран сеанса и политики QoS.

Подробные данные

- Межсетевой экран видит обычный Пакет TCP SYN с 0x21 опцией и создает сеанс для нее. Нет никаких проблем с интерфейсами ввода или вывода, так как не включен WCCP. SYN-ACK return не является перенаправленным пакетом, и межсетевой экран принимает во внимание его.
- Межсетевой экран проверяет для 0x21 опции в SYN-ACK и выполняет переход порядкового номера при необходимости. Если соединение оптимизировано, это также выключает контроль L7.
- Нужно заметить, что единственный аспект, который отличает это от сценария Router1, - то, что не перенаправлен ответный трафик. Существует № 2? половина? соединения на этой коробке.

!--- конфигурацию

Стандартная конфигурация ZBF без любой определенной зоны для трафика WAAS. Только контроль Уровня 7 не будет поддерживаться.

Ограничения для совместимости ZBF с WAAS

- Метод перенаправления WCCP уровня 2 не поддерживается на межсетевом экране

IOS, это только поддерживает перенаправление универсальной инкапсуляции маршрутизации (GRE).
- Межсетевой экран IOS только поддерживает перенаправление WCCP. Если WAAS будет использовать маршрутизацию на основе политик (PBR) для перенаправления пакетов, то это решение НЕ гарантирует совместимость и следовательно неподдерживаемый.
- Межсетевой экран IOS не выполнит, контроль L7 на WAAS оптимизировал сеансы TCP.
- Межсетевой экран IOS требует**? ip inspect waas включает? и? ip wccp уведомляет?** Команды CLI для перенаправления WCCP**.**
- Межсетевой экран IOS с NAT и совместимостью WAAS-NM не поддерживается в настоящее время.
- Межсетевой экран IOS перенаправление WAAS только применен для пакетов TCP.
- Межсетевой экран IOS не поддерживает активный / активные топологии. Все пакеты, принадлежащие сеансу MUST, текут через коробку Межсетевого экрана IOS.

Дополнительные сведения

Руководство по конфигурации системы безопасности: Zone-Based Policy межсетевой экран, Cisco IOS Release 15M&T

Дизайн и руководство по Zone-Based Policy межсетевому экрану