WAAS 구축을 통한 Cisco IOS Zone Based Firewall 상호 운용성 구성

목차

소개

이 문서에서는 Cisco IOS® Firewall 기능 집합의 새로운 구성 모델에 대해 설명합니다.이 새로운 컨피그레이션 모델은 다중 인터페이스 라우터에 대한 직관적인 정책, 향상된 방화벽 정책 애플리케이션 세분화, 올바른 트래픽을 허용하기 위해 명시적 정책이 적용될 때까지 방화벽 보안 영역 간의 트래픽을 금지하는 기본 거부-모두 정책을 제공합니다.

사전 요구 사항

요구 사항

Cisco에서는 Cisco IOS® CLI에 대한 지식을 보유하고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco 2900 Series 라우터
- Cisco IOS® 소프트웨어 릴리스 15.2(4) M2

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

영역 기반 정책 방화벽(Zone-Policy Firewall, ZFW 또는 ZBF라고도 함)은 방화벽 컨피그레이션을 이전 CBAC(Interface-Based Model)에서 보다 유연하고 이해하기 쉬운 영역 기반 모델로 변경합니다.인터페이스가 영역에 할당되고 검사 정책은 영역 간에 이동하는 트래픽에 적용됩니다.영역 간 정책은 상당한 유연성과 세분성을 제공하므로 동일한 라우터 인터페이스에 연결된 여러 호스트 그룹에 서로 다른 검사 정책을 적용할 수 있습니다.방화벽 정책은 Cisco® CPL(Policy Language)로 구성되며, 이는 네트워크 프로토콜에 대한 검사 및 검사가 적용되는 호스트 그룹을 정의하기 위해 계층 구조를 사용합니다.

Cisco IOS® 방화벽을 통한 WAAS 지원

Cisco IOS® 방화벽을 통한 WAAS(Wide Area Application Services) 지원은 Cisco IOS® Release 12.4(15)T에 도입되었습니다.보안 준수 WAN 및 애플리케이션 가속화 솔루션을 최적화하는 통합 방화벽을 제공합니다.

- 완벽한 스테이트풀 검사 기능을 통해 WAN 최적화
- PCI(Payment Card Industry) 규정 준수 간소화
- 투명한 WAN 가속화된 트래픽 보호
- WAAS 네트워크를 투명하게 통합
- NME(Network Management Equipment) WAE(Wide Area Application Engine) 모듈 또는 독립형 WAAS 장치 구축 지원

WAAS에는 WAE 장치를 투명하게 식별하기 위해 사용되는 초기 3방향 핸드셰이크 중에 TCP 옵션을 사용하는 자동 검색 메커니즘이 있습니다.자동 검색 후 최적화된 트래픽 흐름(경로)은 엔드포인트가 최적화되고 최적화되지 않은 트래픽 흐름을 구별할 수 있도록 TCP 시퀀스 번호가 변경됩니다.

IOS® 방화벽에 대한 WAAS 지원을 사용하면 앞서 언급한 시퀀스 번호의 변화를 기반으로 레이어 4 검사에 사용되는 내부 TCP 상태 변수를 조정할 수 있습니다.Cisco IOS® 방화벽이 트래픽 흐름이 WAAS 자동 검색을 성공적으로 완료했음을 알리면 트래픽 흐름에 대한 초기 시퀀스 번호 이동을 허용하고 최적화된 트래픽 흐름에서 레이어 4 상태를 유지합니다.

WAAS 트래픽 흐름 최적화 구축 시나리오

이 섹션에서는 지사 구축을 위한 두 가지 WAAS 트래픽 흐름 최적화 시나리오에 대해 설명합니다.WAAS 트래픽 흐름 최적화는 Cisco ISR(Integrated Services Router)의 Cisco 방화벽 기능과 함께 작동합니다.

이 그림은 Cisco 방화벽과 함께 엔드 투 엔드 WAAS 트래픽 흐름 최적화의 예를 보여줍니다.이 특정 구축에서는 NME-WAE 디바이스가 Cisco 방화벽과 동일한 디바이스에 있습니다.WCCP(Web Cache Communication Protocol)는 인터셉션을 위해 트래픽을 리디렉션하기 위해 사용됩니다.

- 경로 외 장치를 사용하는 WAAS 브랜치 구축

- 인라인 장치를 사용하는 WAAS 브랜치 구축

경로 외 장치를 사용하는 WAAS 브랜치 구축

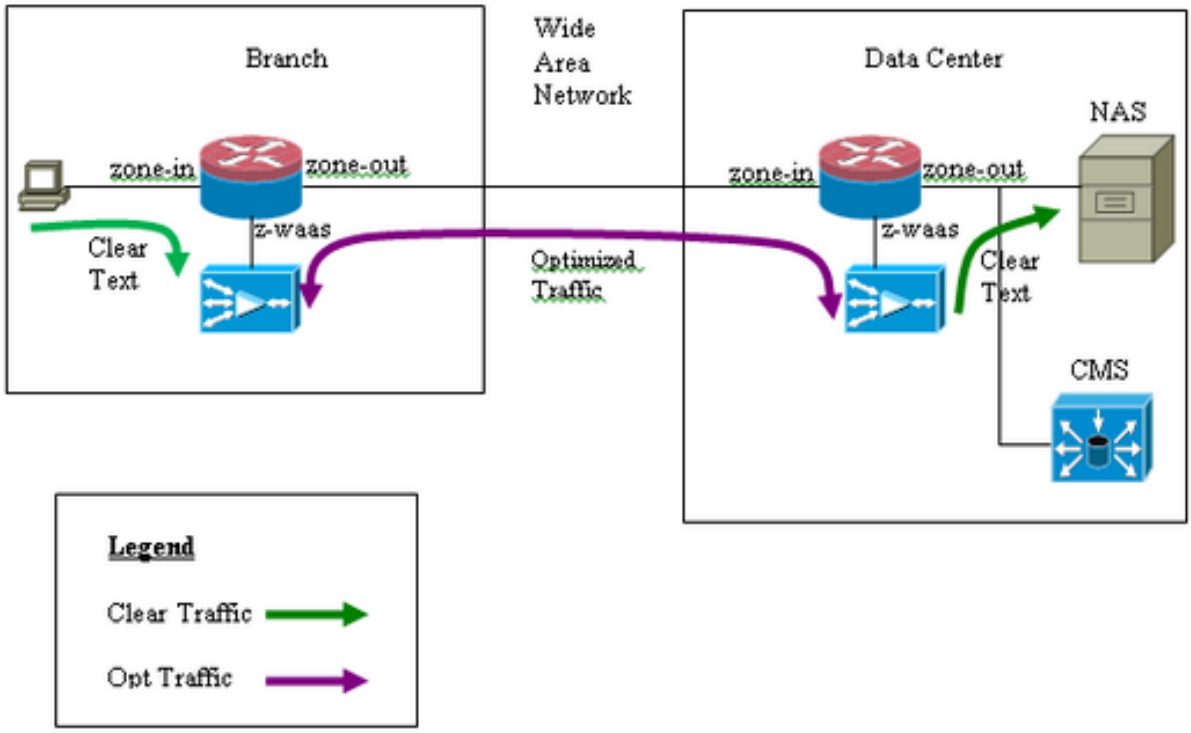
WAE 장치는 독립형 Cisco WAE(WAN Automation Engine) 장치 또는 ISR에 통합 서비스 엔진으로 설치되는 Cisco WAAS Network Module(NME-WAE)일 수 있습니다.

이 그림은 트래픽을 트래픽 가로채기를 위해 비경로 독립형 WAE 디바이스로 리디렉션하기 위해 WCCP를 사용하는 WAAS 브랜치 구축을 보여줍니다.이 옵션에 대한 컨피그레이션은 NME-WAE를 사용하는 WAAS 브랜치 구축과 동일합니다.

네트워크 다이어그램

컨피그레이션 및 패킷 흐름

이 다이어그램은 엔드 투 엔드 트래픽에 대해 WAAS 최적화가 켜져 있고 서버 끝에 있는 중앙 집중식 관리 시스템(CMS)이 켜진 경우의 설정 예를 보여줍니다.지사 엔드 및 데이터 센터(DC) 끝에 있는 WAAS 모듈은 운영을 위해 CMS에 등록해야 합니다.CMS는 WAAS 모듈과의 통신에 HTTPS를 사용하는 것으로 관찰되었습니다.



엔드 투 엔드 WAAS 트래픽 흐름

이 예에서는 트래픽을 트래픽 가로채기를 위해 WAE 디바이스로 리디렉션하기 위해 WCCP를 사용하는 Cisco IOS® 방화벽에 대한 엔드 투 엔드 WAAS 트래픽 흐름 최적화 컨피그레이션을 제공합니다.

섹션 1. IOS-FW WCCP 관련 컨피그레이션:

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

섹션 2. IOS-FW 정책 구성:

```
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
```

섹션 3. IOS-FW 영역 및 영역 쌍 구성:

```
zone security zone-in
zone security zone-out
zone security z-waas
```

```
zone—pair security in—out source zone-in destination zone-out
service—policy type inspect p1

zone—pair security out-in source zone-out destination zone-in
service—policy type inspect p1
```

섹션 4. 인터페이스 구성:

```
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
```

> **참고:**Cisco IOS® Release 12.4(20)T 및 12.4(22)T의 새로운 컨피그레이션은 통합 서비스 엔진을 자체 영역에 배치하며 어떤 zone-pair에도 속하지 않아도 됩니다.영역 쌍은 zone-in 및 zone-out 간에 구성됩니다.

```
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
```

Integrated—Service—Engineel/0에 구성된 영역이 없는 경우, 이 삭제 메시지와 함께 트래픽이 삭제됩니다.

```
*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
```

CMS 트래픽 흐름(WAAS 장치가 중앙 관리자에 등록)

이 예에서는 나열된 두 시나리오에 대한 컨피그레이션을 제공합니다.

- 트래픽 가로채기를 위해 WAE 장치로 트래픽을 리디렉션하기 위해 WCCP를 사용하는 Cisco IOS® 방화벽에 대한 엔드 투 엔드 WAAS 트래픽 흐름 최적화 구성
- CMS 트래픽 허용(WAAS 장치에서 CMS로/WAAS 장치로 이동하는 WAAS 관리 트래픽)

섹션 1. IOS-FW WCCP 관련 컨피그레이션:

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

섹션 2. IOS-FW 정책 구성:

```
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
```

섹션 2.1. CMS 트래픽과 관련된 IOS-FW 정책:

참고:CMS 트래픽을 통과하려면 여기에서 클래스 맵이 필요합니다.

```
class-map type inspect waas-special
 match access-group 123

policy-map type inspect p-waas-man
 class type inspect waas-special
  pass
 class class-default
  drop
```

섹션 3. IOS-FW 영역 및 영역 쌍 구성:

```
zone security zone-in
zone security zone-out
zone security z-waas

zone–pair security in–out source zone-in destination zone-out
service–policy type inspect p1

zone–pair security out–in source zone-out destination zone-in
service–policy type inspect p1
```

섹션 3.1. IOS-FW CMS 관련 영역 및 영역 쌍 구성:

참고:영역 쌍**은 CMS** 트래픽**에** 앞서 생성한 정책을 적용하려면 waas-out 및 out-waas가 필요합니다.

```
zone-pair security waas-out source z-waas destination zone-out
service-policy type inspect p-waas-man

zone-pair security out-waas source zone-out destination z-waas
service-policy type inspect p-waas-man
```

섹션 4. 인터페이스 구성:

```
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
```
섹션 5. CMS 트래픽에 대한 액세스 목록

> **참고:**CMS 트래픽에 사용되는 액세스 목록입니다.CMS 트래픽은 HTTPS이므로 양방향으로 HTTPS 트래픽을 허용합니다.

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

ZBF 세션 정보

Router R1 뒤에 172.16.11.10의 사용자는 IP 주소가 172.16.10.10인 원격 엔드 뒤에 호스팅되는 파일 서버에 액세스하고, ZBF 세션은 out-out zone-pair에서 구축되며, 이후 라우터는 최적화를 위해 패킷을 WAAS 엔진으로 리디렉션합니다.

```
R1#sh policy-map type inspect zone-pair in-out sess

policy 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]
```

내부 호스트에서 원격 서버로 R1-WAAS 및 R2-WAAS에 내장된 세션

R1-WAAS:

```
R1-WAAS#show statistics connection

Current 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: 0
Current Active Auto-Discovery Flows:               1
```

```
Current Reserved Flows:                                10
Current Active Pass-Through Flows:                     0
Historical Flows:                                      13


D:DRE,L:LZ,T:TCP Optimization RR:Total Reduction Ratio
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,I:ICA,M:MAPI,N:NFS,S:SSL,W:WAN SECURE,V:VID
EO, X: SMB Signed Connection

ConnID        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 connection

Current Active Optimized Flows:                        1
   Current Active Optimized TCP Plus Flows:            1
   Current Active Optimized TCP Only Flows:            0
   Current Active Optimized TCP Preposition Flows:     0
Current Active Auto-Discovery Flows:                   0
Current Reserved Flows:                                10
Current Active Pass-Through Flows:                     0
Historical Flows:                                      9


D:DRE,L:LZ,T:TCP Optimization RR:Total Reduction Ratio
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEO

ConnID        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%
```

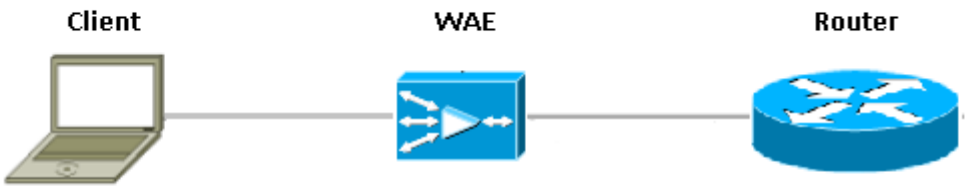
WAAS 및 ZBF가 활성화된 클라이언트측 라우터(R1)의 작업 컨피그레이션

```
R1#sh run
Building configuration...
Current configuration : 3373 bytes
!
hostname R1
!
boot-start-marker
boot bootstrap tftp c2900-universalk9-mz.SPA.153-3.M4.bin 255.255.255.255
boot system flash c2900-universalk9-mz.SPA.153-3.M4.bin
boot-end-marker
!
ip wccp 61
ip wccp 62
no ipv6 cef
!
parameter-map type inspect global
 WAAS enable
 log dropped-packets enable
 max-incomplete low 18000
 max-incomplete high 20000
multilink bundle-name authenticated
!
license udi pid CISCO2911/K9 sn FGL171410K8
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
```

```
license boot module c2900 technology-package datak9
hw-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-zone
zone security out-zone
zone security waas-zone
zone-pair security in-out source in-zone destination out-zone
 service-policy type inspect p1
zone-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
```

인라인 장치를 통한 WAAS 지사 구축

이 그림은 ISR 앞에 물리적으로 인라인 WAE 장치가 있는 WAAS 지사 구축을 보여줍니다.WAE 디바이스가 디바이스 앞에 있으므로 Cisco 방화벽은 WAAS 최적화 패킷을 수신하며, 따라서 클라이언트 측의 레이어 7 검사는 지원되지 않습니다.



WAAS 장치 간에 Cisco IOS® 방화벽을 실행하는 라우터에는 최적화된 트래픽만 표시됩니다.ZBF 기능은 초기 3방향 핸드셰이크(TCP 옵션 33 및 시퀀스 번호 이동)를 감시하며 예상 TCP 시퀀스 창을 자동으로 조정합니다(패킷 자체의 시퀀스 번호는 변경하지 않음). WAAS 최적화 세션에 전체 L4 상태 저장 방화벽 기능을 적용합니다.WAAS 투명 솔루션은 방화벽이 세션당 상태 기반 방화벽 및 QoS 정책을 시행하도록 지원합니다.

세부 정보

- 방화벽은 0x21 옵션이 있는 일반 TCP SYN 패킷을 확인하고 그에 대한 세션을 생성합니다 .WCCP는 포함되지 않으므로 입력 또는 출력 인터페이스에 문제가 없습니다.반환 SYN-ACK는 리디렉션된 패킷이 아니며 방화벽에서 이를 기록합니다.
- 방화벽은 SYN-ACK에서 0x21 옵션을 확인하고 필요한 경우 시퀀스 번호 점프를 수행합니다.또한 연결이 최적화된 경우 L7 검사를 끕니다.
- Router-1 시나리오와 이를 구별하는 유일한 측면은 반환 트래픽이 리디렉션되지 않는다는 것입니다.이 상자에는 2개의 반만 연결되어 있지 않습니다.

구성

WAAS 트래픽에 대한 특정 영역이 없는 표준 ZBF 컨피그레이션입니다.레이어 7 검사만 지원되지 않습니다.

WAAS와의 ZBF 상호운용성에 대한 제한 사항

- WCCP Layer 2 리디렉션 방법은 Cisco IOS® 방화벽에서 지원되지 않으며 GRE(Generic Routing Encapsulation) 리디렉션만 지원합니다.
- Cisco IOS® 방화벽은 WCCP 리디렉션만 지원합니다.WAAS가 패킷을 리디렉션하기 위해 PBR(Policy Based Routing)을 사용하는 경우 이 솔루션은 상호운용성을 보장하지 않으므로 지원되지 않습니다.
- Cisco IOS® 방화벽은 WAAS 최적화 TCP 세션에서 L7 검사를 수행하지 않습니다.
- Cisco IOS® 방화벽에는 WCCP 리디렉션을 위해 **ip inspect waas enable** 및 **ip wccp notify** CLI 명령이 필요합니다.
- NAT 및 WAAS-NM 상호 운용성을 갖춘 Cisco IOS® 방화벽은 현재 지원되지 않습니다.
- Cisco IOS® 방화벽 WAAS 리디렉션은 TCP 패킷에만 적용됩니다.
- Cisco IOS® 방화벽은 활성/활성 토폴로지를 지원하지 않습니다.
- 세션에 속하는 모든 패킷은 Cisco IOS® 방화벽 상자를 통과해야 합니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- 보안 구성 가이드:Zone-Based Policy Firewall, Cisco IOS Release 15M&T
- Zone-Based Policy Firewall 설계 및 애플리케이션 가이드
- 기술 지원 및 문서 – Cisco Systems