ASA with CX/FirePower Module 및 CWS 커넥터 컨피그레이션 예

목차

소개

이 문서에서는 Cisco ASA(Adaptive Security Appliance)를 Next Generation Firewall이라고도 하는 CX(Context Aware) 모듈과 Cisco CWS(Cloud Web Security) 커넥터를 사용하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco는 다음과 같은 기능을 권장합니다.

- ASA의 3DES/AES 라이센스(무료 라이센스)

- 필요한 사용자 수에 대해 CWS를 사용하는 유효한 CWS 서비스/라이센스
- ScanCenter 포털에 액세스하여 인증 키 생성

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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

범위

이 문서에서는 다음과 같은 기술 및 제품 영역을 보여 줍니다.

- Cisco ASA 5500-X Series Adaptive Security Appliance는 인터넷 에지 방화벽 보안 및 침입 방지를 제공합니다.
- Cisco Cloud Web Security는 액세스하는 모든 웹 콘텐츠를 세부적으로 제어합니다.

활용 사례

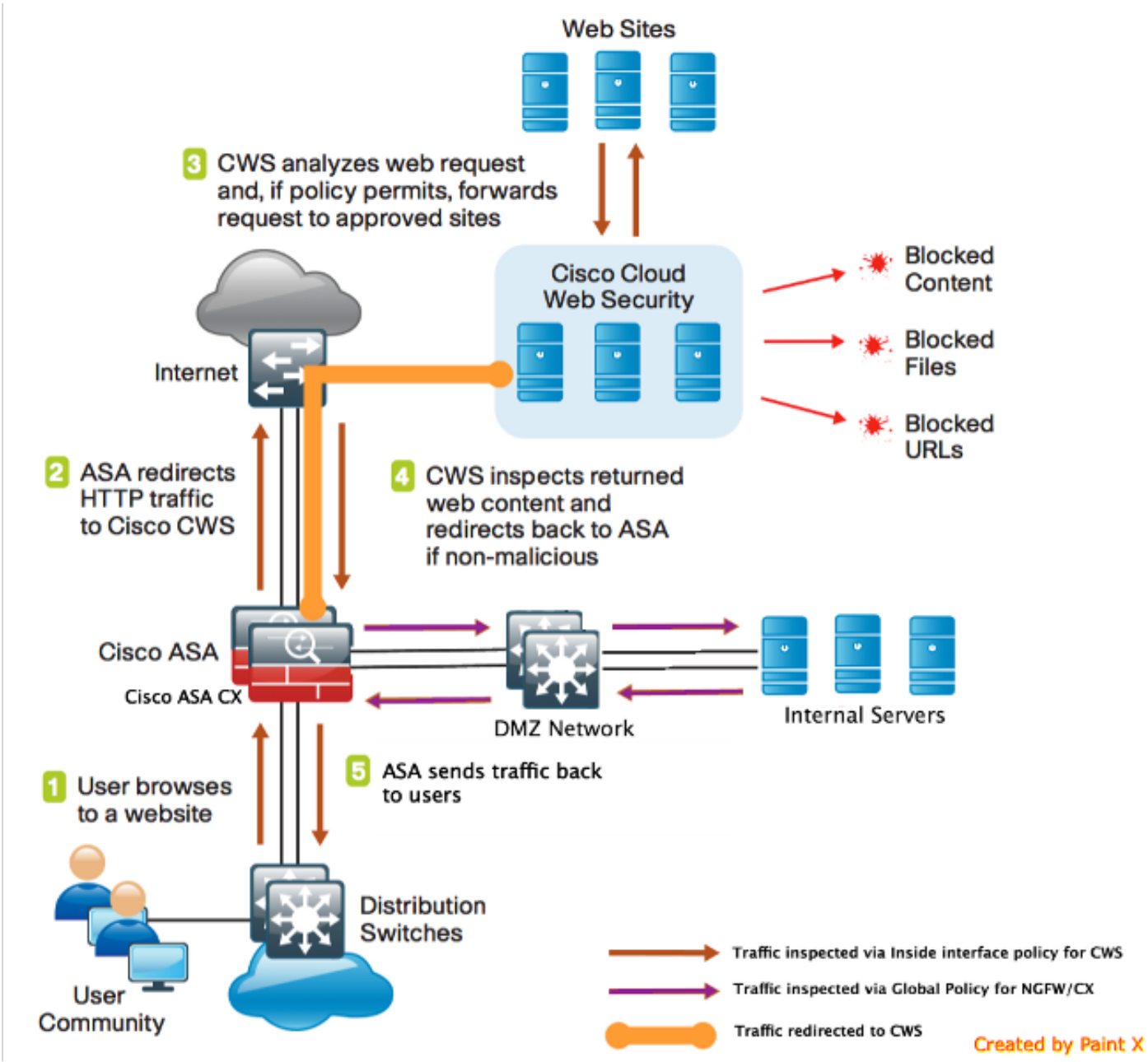
ASA CX/FirePower 모듈은 ASA CX/FirePower에서 활성화된 라이센스 기능에 따라 콘텐츠 보안 및 침입 방지 요구 사항을 모두 지원할 수 있습니다. Cloud Web Security는 ASA CX/FirePower 모듈에서 지원되지 않습니다. 동일한 트래픽 흐름에 대해 ASA CX/FirePower 작업과 Cloud Web Security 검사를 모두 구성한 경우 ASA는 ASA CX/FirePower 작업만 수행합니다. 웹 보안을 위한 CWS 기능을 활용하려면 ASA CX/FirePower에 대한 match 문에서 트래픽이 우회되는지 확인해야 합니다. 일반적으로 이러한 시나리오에서 고객은 다른 모든 포트에 대해 CWS for Web Security and AVC(포트 80 및 443) 및 CX/FirePower 모듈을 사용합니다.

주요 내용

- match **default-inspection-traffic** 명령은 Cloud Web Security 검사의 기본 포트를 포함하지 않습니다(80 및 443).
- 작업은 기능에 따라 양방향 또는 단방향으로 트래픽에 적용됩니다. 양방향으로 적용되는 기능의 경우 정책 맵을 적용하는 인터페이스로 들어오거나 나가는 모든 트래픽은 트래픽이 양방향으로 클래스 맵과 일치하면 영향을 받습니다. 전역 정책을 사용할 경우 모든 기능은 단방향입니다. 단일 인터페이스에 적용할 때 일반적으로 양방향인 기능은 전역적으로 적용되는 경우 각 인터페이스의 인그레스(ingress)에만 적용됩니다. 정책은 모든 인터페이스에 적용되므로 두 방향에서 모두 적용되므로 이 경우 양방향성이 이중화됩니다.
- TCP 및 UDP 트래픽(및 ICMP(Internet Control Message Protocol)에서 상태 기반 ICMP 검사를 활성화하면 서비스 정책은 개별 패킷만이 아니라 트래픽 플로우에서 작동합니다. 트래픽이 한 인터페이스의 정책에 있는 기능과 일치하는 기존 연결의 일부인 경우, 해당 트래픽 흐름은 다른 인터페이스의 정책에서 동일한 기능과 매칭할 수 없습니다. 첫 번째 정책만 사용됩니다.
- 인터페이스 서비스 정책은 지정된 기능에 대한 글로벌 서비스 정책보다 우선합니다.
- 최대 정책 맵 수는 64이지만 인터페이스당 정책 맵을 하나만 적용할 수 있습니다.

구성

네트워크 다이어그램



ASA 및 CWS의 트래픽 흐름

1. 사용자는 웹 브라우저를 통해 URL을 요청합니다.
2. 트래픽이 인터넷을 통해 ASA로 전송됩니다. ASA는 필수 NAT를 수행하고 프로토콜 HTTP/HTTPS를 기반으로 내부 인터페이스 정책과 일치하며 Cisco CWS로 리디렉션됩니다.
3. CWS는 ScanCenter 포털에서 수행한 컨피그레이션을 기반으로 요청을 분석하고 정책이 허용되는 경우 요청을 승인된 사이트로 전달합니다.
4. CWS는 반환된 트래픽을 검사하고 이를 ASA로 리디렉션합니다.
5. 유지 관리되는 세션 흐름에 따라 ASA는 트래픽을 다시 사용자에게 전송합니다.

ASA 및 CX/FirePower의 트래픽 흐름

1. HTTP 및 HTTPS를 제외한 모든 트래픽은 검사를 위해 ASA CX/FirePower와 일치하도록 구성되며 ASA 백플레인을 통해 CX/FirePower로 리디렉션됩니다.
2. ASA CX/FirePower는 구성된 정책에 따라 트래픽을 검사하고 필요한 허용/차단/경고 작업을 수행합니다.

구성

모든 인터넷 바인딩 웹(TCP/80) 트래픽과 매칭하고 모든 내부 트래픽을 제외하기 위한 액세스 목록

```
!ASA CWS HTTP Match
access-list cws-www extended deny ip any4 10.0.0.0 255.0.0.0
access-list cws-www extended deny ip any4 172.16.0.0 255.240.0.0
access-list cws-www extended deny ip any4 192.168.0.0 255.255.0.0
access-list cws-www extended permit tcp any4 any4 eq www
```

모든 인터넷 바인딩 HTTPS(TCP/443) 트래픽과 일치시키고 모든 내부 트래픽을 제외하기 위한 액세스 목록

```
!ASA CWS HTTPS Match
access-list cws-https extended deny ip any4 10.0.0.0 255.0.0.0
access-list cws-https extended deny ip any4 172.16.0.0 255.240.0.0
access-list cws-https extended deny ip any4 192.168.0.0 255.255.0.0
access-list cws-https extended permit tcp any4 any4 eq https
```

모든 내부 트래픽을 매칭하기 위한 액세스 목록, 모든 인터넷 바인딩 웹 및 HTTPS 트래픽 및 기타 모든 포트 제외

```
!ASA CX/FirePower Match
access-list asa-ngfw extended permit tcp any4 10.0.0.0 255.0.0.0 eq 80
access-list asa-ngfw extended permit tcp any4 172.16.0.0 255.240.0.0 eq 80
access-list asa-ngfw extended permit tcp any4 192.168.0.0 255.255.0.0 eq 80
access-list asa-ngfw extended deny tcp any4 any4 eq www
access-list asa-ngfw extended permit tcp any4 10.0.0.0 255.0.0.0 eq 443
access-list asa-ngfw extended permit tcp any4 172.16.0.0 255.240.0.0 eq 443
access-list asa-ngfw extended permit tcp any4 192.168.0.0 255.255.0.0 eq 443
access-list asa-ngfw extended deny tcp any4 any4 eq https
access-list asa-ngfw extended permit ip any4 any4
```

CWS 및 CX/FirePower의 트래픽과 일치시키기 위한 클래스 맵 컨피그레이션

```
! Match HTTPS traffic for CWS
class-map cmap-https
match access-list cws-https

! Match HTTP traffic for CWS
class-map cmap-http
match access-list cws-www

! Match traffic for ASA CX/FirePower
class-map cmap-ngfw
match access-list asa-ngfw
```

작업을 클래스 맵과 연결하는 정책 맵 컨피그레이션

```
!Inspection policy map to configure essential parameters for the rules and
optionally !identify the allowed list for HTTP traffic
policy-map type inspect scansafe http-pmap
parameters
default group cws_default
http

!Inspection policy map to configure essential parameters for the rules and
optionally !identify the allowed list for HTTPS traffic
policy-map type inspect scansafe https-pmap
parameters
default group cws_default
https

! Interface policy local to Inside Interface
policy-map cws_policy
class cmap-http
inspect scansafe http-pmap fail-open
class cmap-https
inspect scansafe https-pmap fail-open

! Global Policy with Inspection enabled using ASA CX
policy-map global_policy
class inspection_default
<SNIP>
class cmap-ngfw
cxsc fail-open
class class-default
user-statistics accounting
```

인터페이스에서 CX/FirePower 및 CWS에 대해 전역으로 정책 활성화

```
service-policy global_policy global
service-policy cws_policy inside
```

> **참고:** 이 예에서는 웹 트래픽이 보안 영역 내에서만 발생하는 것으로 가정합니다. 웹 트래픽을 예상하거나 전역 정책 내에서 동일한 클래스를 사용하는 모든 인터페이스에서 인터페이스 정책을 사용할 수 있습니다. 이는 CWS의 기능을 시연하고 MPF를 사용하여 요구 사항을 지원하기 위한 것입니다.

ASA에서 CWS 활성화(차이 없음)

```
scansafe general-options
server primary ip 203.0.113.1 port 8080
server backup ip 203.0.113.2 port 8080
retry-count 5
license xxxxxxxxxxxxxxxxxxxxxxxxxxxx
!
```

모든 연결에서 새 정책을 사용하도록 하려면 현재 연결을 끊어야 새 정책과 다시 연결할 수 있습니다. clear conn 또는 clear local-**host** 명령**을** 참조하십시오.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

서비스를 활성화하고 ASA가 트래픽을 리디렉션하는지 확인하려면 show scansafe **statistics** 명령

을 입력합니다. 이후 시도에서는 세션 수, 현재 세션 및 전송된 바이트의 증가분을 표시합니다.

```
csaxena-cws-asa# show scansafe statistics
Current HTTP sessions : 0
Current HTTPS sessions : 0
Total HTTP Sessions : 1091
Total HTTPS Sessions : 5893
Total Fail HTTP sessions : 0
Total Fail HTTPS sessions : 0
Total Bytes In : 473598 Bytes
Total Bytes Out : 1995470 Bytes
HTTP session Connect Latency in ms(min/max/avg) : 10/23/11
HTTPS session Connect Latency in ms(min/max/avg) : 10/190/11
```

검사된 패킷의 증분을 보려면 **show service-policy** 명령을 입력합니다.

```
asa# show service-policy
Global policy:
Service-policy: global_policy
Class-map: inspection_default
<SNIP>
<SNIP>
Class-map: cmap-ngfw
CXSC: card status Up, mode fail-open, auth-proxy disabled
packet input 275786624, packet output 272207060, drop 0,reset-drop 36,proxied 0
Class-map: class-default
Default Queueing Packet recieved 150146, sent 156937, attack 2031

Interface inside:
Service-policy: cws_policy
Class-map: cmap-http
Inspect: scansafe http-pmap fail-open, packet 176, lock fail 0, drop 0,
reset-drop 0, v6-fail-close 0
Class-map: cmap-https
Inspect: scansafe https-pmap fail-open, packet 78, lock fail 0, drop 13,
reset-drop 0, v6-fail-close 0
```

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

위의 컨피그레이션과 관련된 문제를 해결하고 패킷 흐름을 이해하려면 다음 명령을 입력합니다.

```
asa(config)# packet-tracer input inside tcp 10.0.0.1 80 192.0.2.105 80 det

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
<SNIP>
<This phase will show up if you are capturing same traffic as well>

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
```

```
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in <SNIP>

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
in 0.0.0.0 0.0.0.0 via 198.51.100.1, outside
<Confirms egress interface selected. We need to ensure we have CWS
connectivity via the same interface>

Phase: 4
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
in 10.0.0.0 255.255.254.0 via 10.0.0.0.1, inside

Phase: 5
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group inside_in in interface inside
access-list inside_in extended permit ip any any
Additional Information:
<SNIP>

Phase: 6
Type: NAT
Subtype:
Result: ALLOW
Config:
object network obj-inside_to_outside
nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 10.0.0.1/80 to 198.51.100.1/80
Forward Flow based lookup yields rule:
in <SNIP>

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in <SNIP>

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in <SNIP>

Phase: 9
```

Type: **INSPECT**
Subtype: **np-inspect**
Result: **ALLOW**
Config:
class-map cmap-http
match access-list cws-www
policy-map inside_policy
class cmap-http
inspect scansafe http-pmap fail-open
service-policy inside_policy interface inside
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7fff2cd3fce0, priority=72, **domain=inspect-scansafe**, **deny=false**
hits=8, user_data=0x7fff2bb86ab0, cs_id=0x0, use_real_addr,flags=0x0,protocol=6
src ip/id=10.0.0.11, mask=255.255.255.255, port=0, tag=0
dst ip/id=0.0.0.0, mask=0.0.0.0, **port=80**, tag=0, dscp=0x0
input_ifc=inside, output_ifc=any
<Verify the configuration, port, domain, deny fields>

Phase: 10
Type: **CXSC**
Subtype:
Result: **ALLOW**
Config:
class-map ngfw-cx
match access-list asa-cx
policy-map global_policy
class ngfw
cxsc fail-open
service-policy global_policy global
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7fff2c530970, priority=71, **domain=cxsc**, **deny=true**
hits=5868,user_data=0x7fff2c931380,cs_id=0x0,use_real_addr,flags=0x0,protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=0
dst ip/id=0.0.0.0, mask=0.0.0.0, port=80, tag=0, dscp=0x0
input_ifc=inside, output_ifc=any

Phase: 11
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
out <SNIP>

Phase: 12
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
out <SNIP>

Phase: 13
Type: USER-STATISTICS
Subtype: user-statistics
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
out <SNIP>

<In this example, IDFW is not configured>

Phase: 14
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in <SNIP>

Phase: 15
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in <SNIP>

Phase: 16
Type: USER-STATISTICS
Subtype: user-statistics
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
out <SNIP>

Phase: 17
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 3855350, packet dispatched to next module
Module information for forward flow ...
snp_fp_tracer_drop
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_inline_tcp_mod
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Module information for reverse flow ...
snp_fp_tracer_drop
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_inline_tcp_mod
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Result:
input-interface: **inside**
input-status: up
input-line-status: up
output-interface: **outside**
output-status: up

```
output-line-status: up
Action: allow
```

관련 정보

- ASA 9.x 컨피그레이션 가이드
- 기술 지원 및 문서 – Cisco Systems