ASA with CX/FirePower Module and CWS Connector Configuration Example

Contents

Introduction

This document describes how to use the Cisco Adaptive Security Appliance (ASA) with the Context Aware (CX) module, also known as the Next Generation firewall, and Cisco Cloud Web Security (CWS) Connector.

Prerequisites

Requirements

Cisco recommends that you have:

- 3DES/AES License on ASA (Free license)
- Valid CWS service/license to use CWS for the required number of users

- Access to ScanCenter Portal to generate the Authentication Key

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

Scope

This document shows these areas of technology and products:

- Cisco ASA 5500-X Series Adaptive Security Appliances provides Internet edge firewall security and intrusion prevention.
- Cisco Cloud Web Security provides granular control over all web content that is accessed.

Use Case

The ASA CX/FirePower module has the capability to support both the Content Security and Intrusion Prevention requirement, dependent upon the license features enabled on the ASA CX/FirePower. Cloud Web Security is not supported with the ASA CX/FirePower module. If you configure both the ASA CX/FirePower action and Cloud Web Security inspection for the same traffic flow, the ASA only performs the ASA CX/FirePower action. In order to leverage the CWS features for Web Security, you need to ensure the traffic is bypassed in the match statement for ASA CX/FirePower. Typically, in such a scenario, customers will use CWS for Web Security and AVC (port 80 and 443) and CX/FirePower module for all other ports.

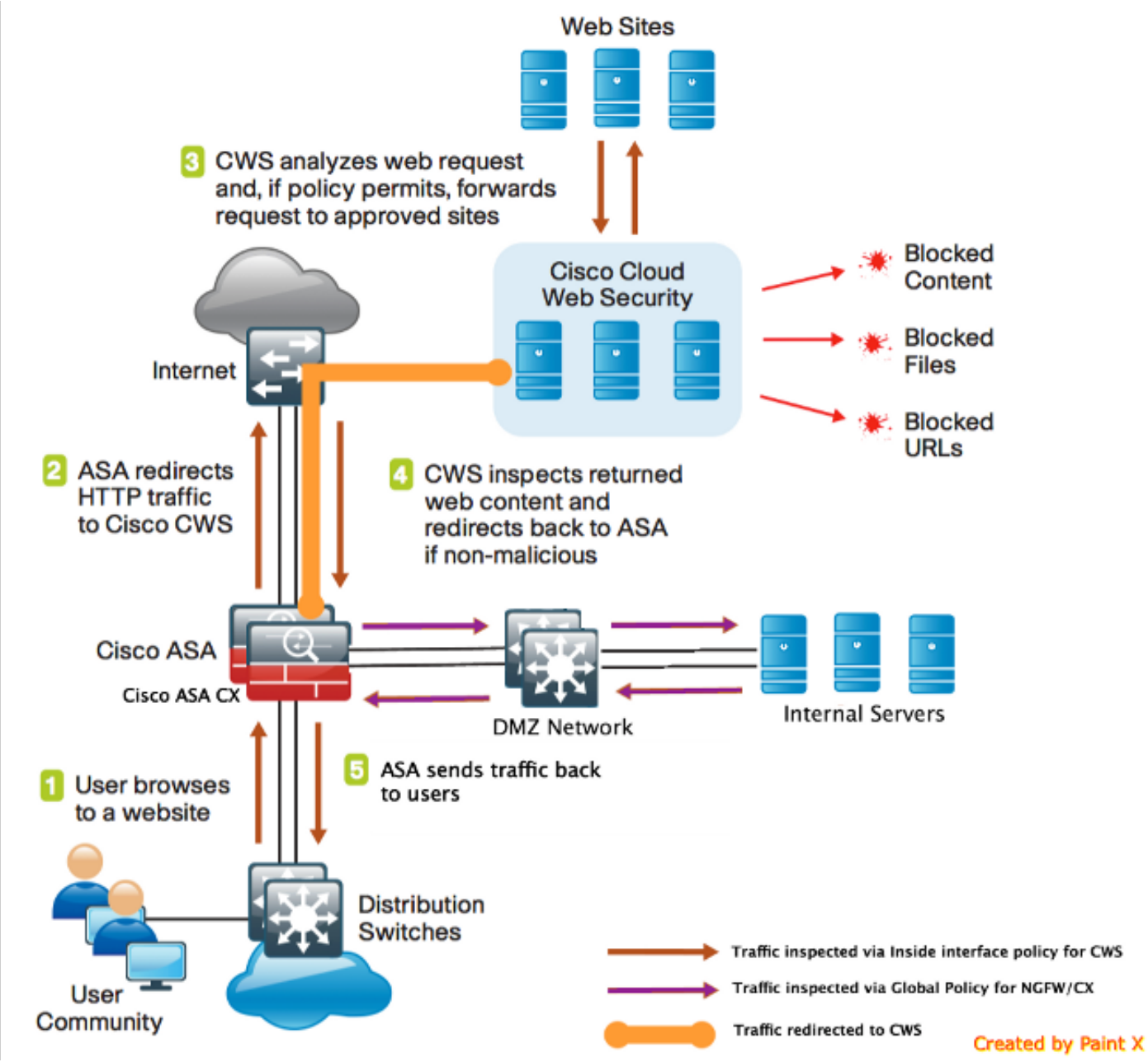
Key Points

- The **match default-inspection-traffic** command does not include the default ports for the Cloud Web Security inspection (80 and 443).
- Actions are applied to traffic bidirectionally or unidirectionally dependent upon the feature. For features that are applied bidirectionally, all traffic that enters or exits the interface to which you apply the policy map is affected if the traffic matches the class map for both directions. When you use a global policy all features are unidirectional; features that are normally bidirectional when applied to a single interface only apply to the ingress of each interface when applied globally. Because the policy is applied to all interfaces, the policy is applied in both directions so bidirectionality in this case is redundant.
- For TCP and UDP traffic (and Internet Control Message Protocol (ICMP) when you enable stateful ICMP inspection), service policies operate on traffic flows and not just individual packets**.** If traffic is part of an existing connection that matches a feature in a policy on one interface, that traffic flow cannot also match the same feature in a policy on another interface; only the first policy is used.
- Interface service policies take precedence over the global service policy for a given feature.

- The maximum number of policy maps is 64, but you can only apply one policy map per interface.

Configure

Network Diagram



Traffic Flow for the ASA and CWS

1. The user requests the URL via the web browser.
2. Traffic is sent to the ASA to go out the Internet. The ASA performs required NAT and based on the protocol HTTP/HTTPS, matches to the inside interface policy and gets redirected to Cisco CWS.
3. CWS analyzes the request based on the configuration done in the ScanCenter portal and if policy permits, forwards the request to approved sites.
4. CWS inspects the returned traffic and redirects the same to ASA.

5. Based on the session flow maintained, ASA sends traffic back to the user.

Traffic Flow for the ASA and CX/FirePower

1. All traffic other than HTTP and HTTPS is configured to match the ASA CX/FirePower for inspection and is redirected to CX/FirePower over the ASA backplane.
2. The ASA CX/FirePower inspects traffic based on the policies configured and takes the required allow/block/alert action.

Configurations

Access List to Match All Internet Bound Web (TCP/80) Traffic and Exclude All Internal Traffic

```
!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
```

Access List to Match All Internet Bound HTTPS (TCP/443) Traffic and Exclude All Internal Traffic

```
!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
```

Access List to Match All Internal Traffic, Exclude All Internet Bound Web and HTTPS Traffic and All Other Ports

```
!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
```

Class Map Configuration to Match Traffic for Both CWS and CX/FirePower

```
! 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
```

Policy Map Configuration to Associate Actions with Class Maps

```
!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
```

Activate Policy Globally for CX/FirePower and CWS on the Interface

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

> **Note**: In this example, it is assumed that web traffic originates only from inside the security zone. You can use interface policies on all interfaces where you expect web traffic or use the same classes within the global policy. This is just to demonstrate the functioning of CWS and use of MPF in order to support our requirement.

Enable CWS on the ASA (No Difference)

```
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
!
```

In order to ensure that all connections use the new policy, you need to disconnect the current connections so they can reconnect with the new policy. See the **clear conn** or **clear local-host** commands.

Verify

Use this section to confirm that your configuration works properly.

Enter the **show scansafe statistics** command in order to verify the service to be enabled and that the ASA redirects traffic. Subsequent tries show the increment in session counts, current sessions, and bytes transferred.

```
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
```

Enter the **show service-policy** command in order to see the increments in packets inspected

```
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
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

In order to troubleshoot any issues related to the above configuration and to understand the packet flow, enter this command:

```
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
```

Related Information

- [ASA 9.x Configuration Guide]
- [Technical Support & Documentation - Cisco Systems]