CX/FirePower モジュールと CWS コネクタを使った ASA の設定例

内容

概要

このドキュメントでは、Cisco 適応型セキュリティ アプライアンス (ASA) をコンテキスト認識型 (CX) モジュール (次世代ファイアウォールとも呼ばれる) および Cisco クラウド Web セキュリティ (CWS) コネクタと組み合わせて使用する方法について説明します。

前提条件

要件

Cisco では次の前提を満たす推奨しています。

- ASA の 3DES/AES ライセンス（無料ライセンス）
- 必要な数のユーザが CWS を使用するための有効な CWS サービス/ライセンス
- ScanCenter ポータルにアクセスして認証キーを生成できること

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

範囲

このドキュメントでは、次の分野のテクノロジーと製品について示します。

- Cisco ASA 5500-X シリーズ適応型セキュリティ アプライアンスは、インターネット エッジのファイアウォール セキュリティと侵入防御を提供します。
- Cisco クラウド Web セキュリティは、アクセスされるすべての Web コンテンツをきめ細かく制御できます。

使用例

ASA CX/FirePower モジュールは、ASA CX/FirePower で有効化されたライセンス機能に応じて、コンテンツ セキュリティと侵入防御の両方の要件をサポートできます。ASA CX/FirePower モジュールでは、クラウド Web セキュリティはサポートされません。同じトラフィック フローに対して ASA CX/FirePower のアクションとクラウド Web セキュリティ インスペクションの両方を設定すると、ASA は ASA CX/FirePower のアクションのみを実行します。Web セキュリティに関する CWS の機能を利用するには、ASA CX/FirePower の match ステートメントでトラフィックがバイパスされるようにする必要があります。通常、このようなシナリオでは、Web セキュリティと AVC（ポート 80 と 443）のために CWS を使用し、他のすべてのポートのために CX/FirePower モジュールを使用します。

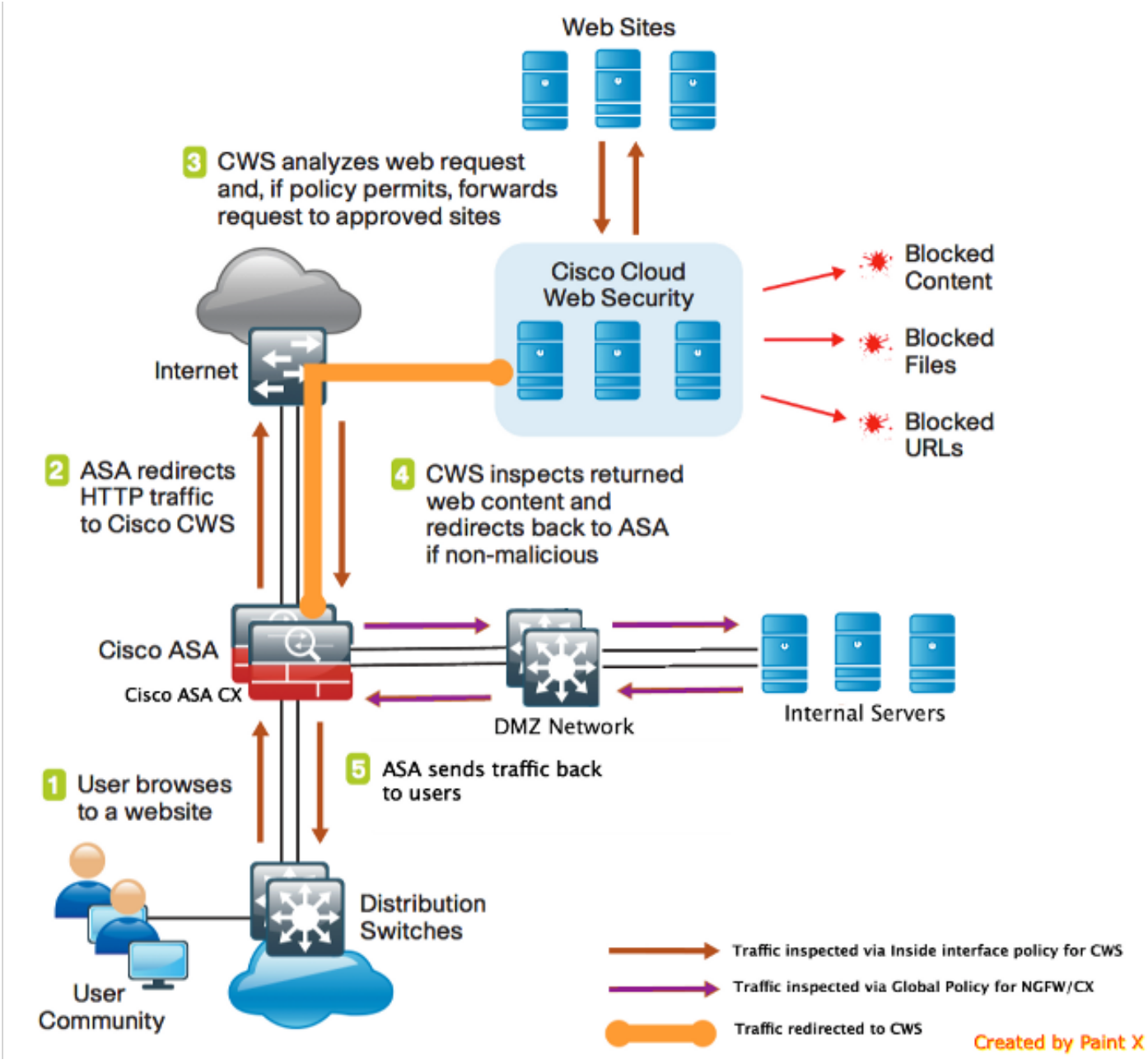
要点

- match default-inspection-traffic コマンドには、クラウド Web セキュリティ インスペクション用のデフォルト ポート（80 および 443）は含まれません。
- 機能に応じて、双方向または単方向のトラフィックにアクションが適用されます。双方向に適用される機能の場合、トラフィックが両方の方向のクラス マップと一致した場合に、ポリシー マップを適用するインターフェイスを出入りするすべてのトラフィックが影響を受けます。グローバル ポリシーを使用するときは、すべての機能が単方向です。単一のインターフェイスに適用したときに通常双方向である機能は、グローバルに適用すると、各インターフェイスの入力にのみ適用されます。ポリシーはすべてのインターフェイスに適用されるため、ポリシーは両方の方向に適用され、この場合の双方向は冗長になります。

- TCP および UDP トラフィック（および Internet Control Message Protocol（ICMP）（ステートフル ICMP インスペクションがイネーブルの場合））の場合、サービス ポリシーはトラフィック フローに対して作用し、個々のパケットに限定されません。トラフィックが、1 つのインターフェイスのポリシーの機能に一致する既存の接続の一部である場合、そのトラフィック フローを別のインターフェイスのポリシーにある同じ機能と照合することはできません。最初のポリシーのみが使用されます。
- 特定の機能については、インターフェイス サービス ポリシーはグローバル サービス ポリシーより優先されます。
- ポリシー マップの最大数は 64 ですが、各インターフェイスにはポリシー マップを 1 つだけ適用できます。

設定

ネットワーク図



ASA と CWS のトラフィック フロー

1. ユーザが Web ブラウザを介して URL を要求します。
2. インターネットに出て行くトラフィックが ASA に送信されます。ASA は必要な NAT を実行し、HTTP/HTTPS プロトコルに基づいて内部インターフェイス ポリシーと照合し、Cisco CWS にリダイレクトします。
3. CWS は ScanCenter ポータルで行なった設定に基づいて要求を分析し、ポリシーによって許可される場合は、要求を承認されたサイトに転送します。
4. CWS は返されたトラフィックを検査し、同じものを ASA にリダイレクトします。
5. ASA は、維持されているセッション フローに基づいてトラフィックをユーザに返送します。

ASA と CX/FirePower のトラフィック フロー

1. HTTP と HTTPS 以外のすべてのトラフィックは、検査のために ASA CX/FirePower と照合するように設定され、ASA のバックプレーン経由で CX/FirePower にリダイレクトされます。
2. ASA CX/FirePower は設定されたポリシーに基づいてトラフィックを検査し、必要な許可/ブロック/アラート アクションを実行します。

設定

すべてのインターネット経由の Web (TCP/80) トラフィックに一致し、すべての内部トラフィックを除外するアクセス リスト

```
!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
```

すべてのインターネット経由の HTTPS (TCP/443) トラフィックに一致し、すべての内部トラフィックを除外するアクセス リスト

```
!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
```

すべての内部トラフィックに一致し、すべてのインターネット経由の Web および HTTPS トラフィックとその他すべてのポートを除外するアクセス リスト

```
!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 と CX/FirePower の両方のトラフィックに一致するクラス マップの設定

```
! 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
```

クラス マップにアクションを関連付けるポリシー マップの設定

```
!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
```

インターフェイスでの CX/FirePower および CWS 用ポリシーのグローバルなアクティブ化

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

> **注**：この例では、Web トラフィックがセキュリティ ゾーンの内部からのみ発信されることを前提としています。Web トラフィックを想定するすべてのインターフェイスでインターフェイス ポリシーを使用するか、グローバル ポリシー内で同じクラスを使用できます。これは、ここでの要件をサポートする CWS の機能と MPF の使用方法を示すためのものです。

ASA での CWS の有効化（相違点なし）

```
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
!
```

すべての接続で新しいポリシーが使用されるようにするには、現在の接続を解除し、新しいポリシーを使用して再接続できるようにする必要があります。clear conn または clear local-host コマンドを参照してください。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

有効にするサービスと ASA によるトラフィックのリダイレクトを検証するには、**show scansafe statistics コマンドを入力します。**続けて試行すると、セッションの合計数、現在のセッション数、転送されたバイト数の増分が示されます。

```
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
```

show service-policyコマンドを入力し、検査されたパケット数の増加を確認します

```
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
```

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

上記の設定に関する問題をトラブルシューティングしたり、パケット フローを確認したりするには、次のコマンドを入力します。

```
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
```

関連情報

- ASA 9.x 構成ガイド
- テクニカル サポートとドキュメント – Cisco Systems