目次

概要

この資料にコンテキストわかっている（ CX ）モジュール、別名次世代 ファイアウォールおよび Cisco クラウド Web セキュリティ（ CWS ）コネクタによって Cisco 適応性があるセキュリティ アプライアンス モデル（ ASA ）を使用する方法を記述されています。

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（自由なライセンス）の 3DES/AES ライセンス
- 有効なユーザの必須の数のために CWS を使用する CWS サービス/ライセンス
- 認証鍵を生成する ScanCenter ポータルへのアクセス

使用するコンポーネント

このドキュメントは、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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

範囲

この資料はテクノロジーおよび製品のこれらの工リアを示したものです:

- Cisco ASA 5500-X シリーズ適応性があるセキュリティ アプライアンス モデルはインターネット エッジ ファイアウォールセキュリティおよび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 コンテンツの粒状制御を提供します。

使用例

ASA CX/FirePower モジュールは ASA CX/FirePower で有効に なる ライセンス 機能に両方をコンテンツ セキュリティおよび侵入防御 要件、依存サポートする機能があります。 Cloud Web セキュリティは ASA CX/FirePower モジュールでサポートされません。 同じトラフィックフローのための ASA CX/FirePower 操作および Cloud Web セキュリティ インスペクションを両方設定する場合、ASA は ASA CX/FirePower 操作だけを行います。 Web セキュリティ用の CWS 機能を利用するために、ASA CX/FirePower のためのマッチ ステートメントでバイパスされますトラフィックを確認する必要があります。 通常、そのような場合には、顧客は Web セキュリティおよび AVC（ポート 80 および他のすべてのポートのために CWS をのための 443）および CX/FirePower モジュール使用します。

キー ポイント

- **一致デフォルト インスペクション トラフィック** コマンドは Cloud 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が含まれていません（80 および 443）。
- 操作はトラフィックに機能に依存双方向にまたは unidirectionally 適用されます。 双方向に加

えられる機能に関してはトラフィックが両方向のためのクラスマップと一致する場合、すべてのトラフィックは出入りしたりポリシーマップを加えるインターフェイス影響を受けています。 グローバル な ポリシーを使用するときすべての機能は単方向です; 普通双方向である機能は各インターフェイスの入力に単一 のインターフェイスに適用されたときグローバルに加えられたときだけ適用されます。 ポリシーがすべてのインターフェイスに適用されるので、ポリシーは両方向で適用されます従って bidirectionality はこの場合冗長です。

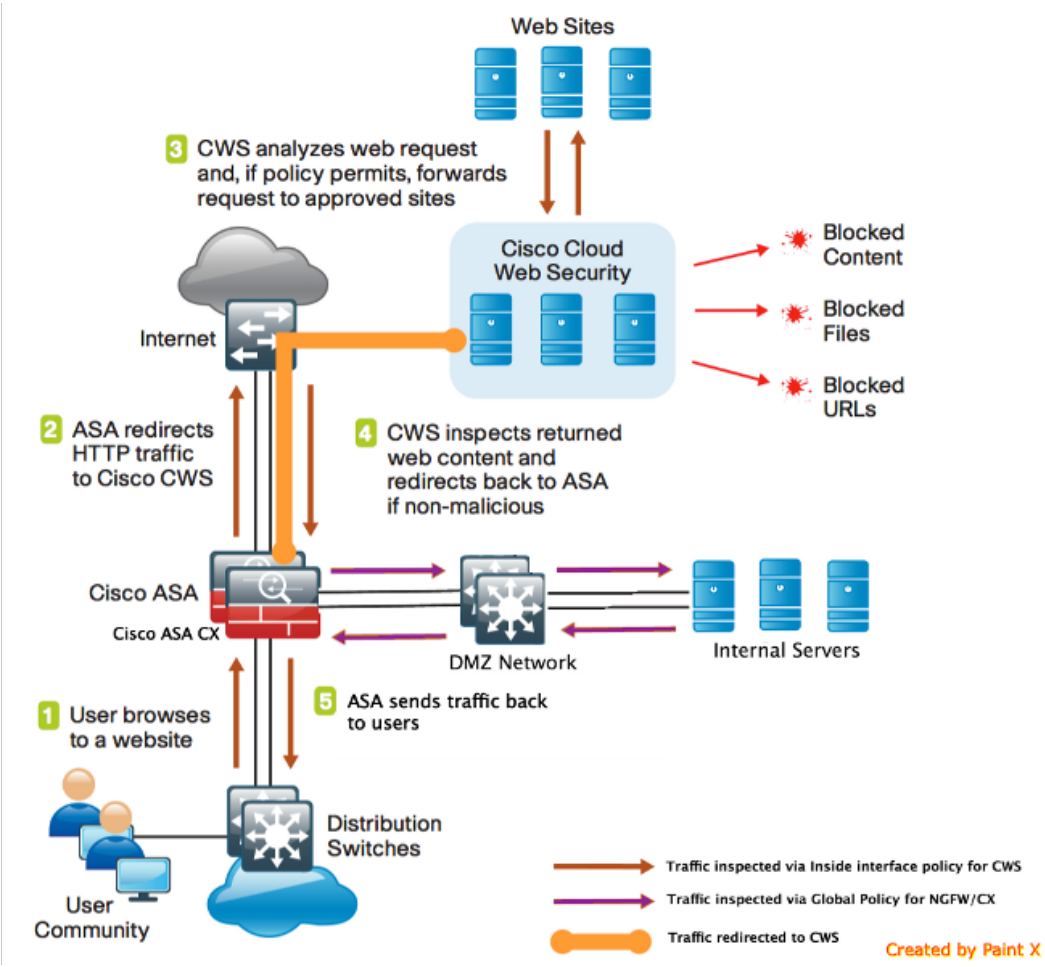
- TCP および UDP トラフィック (およびインターネット制御メッセージ プロトコル (ICMP) に関してはステートフル ICMP インスペクションを有効に するとき)、サービス ポリシーはトラフィックフローおよびちょうど個々のパケットを操作します。 トラフィックが 1 つのインターフェイスのポリシーの機能と一致する現在の接続の一部なら、そのトラフィックフローはまた別のインターフェイスのポリシーの同じ機能を一致することができません; 最初のポリシーだけ使用されます。

- インターフェイス サービス ポリシーはある特定の機能のためのグローバル サービス ポリシーに優先します。

- ポリシーマップの最大数は 64 です、しかしインターフェイス毎に 1 つのポリシーマップしか加えないことができます。

設定

ネットワーク図



ASA および CWS のためのトラフィックフロー

1. ユーザー要求 Webブラウザによる URL。

2. トラフィックは ASA に出かけるためにインターネット 送信 されます。 ASA は必須 NAT を行い、内部インターフェイス ポリシーにプロトコル HTTP/HTTPS に、一致 Cisco CWS にリダイレクトされます基づく。

3. CWS はポリシー割り当てが公認サイトに、要求を転送する場合門脈 ScanCenter でされる設定に基づいて要求を分析し。

4. CWS は戻されたトラフィックを検査し、ASA に同じをリダイレクトします。

5. 維持されるセッション フローに基づいて ASA はユーザにトラフィックを送り返します。

ASA および CX/FirePower のためのトラフィックフロー

1. HTTP および HTTPS 以外のすべてのトラフィックはインスペクション用の ASA CX/FirePower を一致するために設定され、ASA バックプレーン上の CX/FirePower にリダイレクトされます。

2. ASA CX/FirePower は設定されるポリシーに基づいてトラフィックを検査し、必須割り当て/ブロック/アラート処置をとります。

設定

すべてのインターネット バインドされた Web （ TCP/80 ）トラフィックを一致する、すべての内部 トラフィックを除くアクセス 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 バインドされた HTTPS （ TCP/443 ）トラフィックを一致する、すべての内部 トラフィックを除くアクセス 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 トラフィックを一致する アクセス リストはすべてのインターネット バインドされた Web および HTTPS トラフィックおよび他のすべてのポート除きます

```
!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 および CX/FirePower 両方のためのトラフィックを一致する クラスマップ 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
```

クラスマップと操作を関連付けるポリシーマップ設定

```
!Inspection policy map to configure essential parameters for the rules and
optionally !identify the whitelist 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 whitelist 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
```

インターフェイスの CX/FirePower および CWS のためのグローバルにアクティブ化ポリシー

```
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 ゾーンの中からだけ発信することが仮定されます。 Webトラフィックを期待するか、またはグローバル な ポリシー内の同じクラスを使用するすべてのインターフェイスのインターフェイス ポリシーを使用できます。 これはちょうど要件をサポートするために CWS の機能および MPF の使用を示すことです。

ASA（違い無し）のイネーブル CWS

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

すべての接続が新しいポリシーを使用するようにするために、現在の接続を切る必要があります 従って新しいポリシーと再接続できます。 **オフ conn を**参照するか、または**ローカル ホスト** コマンドを**クリアして下さい**。

確認

ここでは、設定が正常に動作していることを確認します。

ASA がトラフィックをリダイレクトすること有効に なるべきサービスを確認するために**提示 scansafe statistics コマンドを**入力すれば。 それに続く試みはセッションカウント、現在の転送されるセッションおよびバイトで増分を示します。

```
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
```

検査されるパケットの増分を見るために **show service policy コマンドを**入力して下さい:

```
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
```

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

関する問題を上の設定に解決し、パケットフローを理解するために、このコマンドを入力して下さい:

```
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 コンフィギュレーション ガイド
- テクニカルサポートとドキュメント - Cisco Systems