内部サーバへの ASA トラフィックに対する CWS がブロックされる

内容

概要

このドキュメントでは、Cisco Adaptive Security Appliances（ASA）バージョン 9.0 以降で Cisco Cloud Web Security（CWS、旧名称 ScanSafe）を設定する場合の一般的な問題について説明します。

CWS では、ASA は選択された HTTP および HTTPS を CWS プロキシ サーバに透過的にリダイレクトします。管理者は、エンドユーザをマルウェアから保護するために CWS ポータルでセキュリティ ポリシーを適切に設定し、エンドユーザに対して許可、ブロック、または警告することができます。

前提条件

要件

次の設定に関する知識があることが推奨されます。

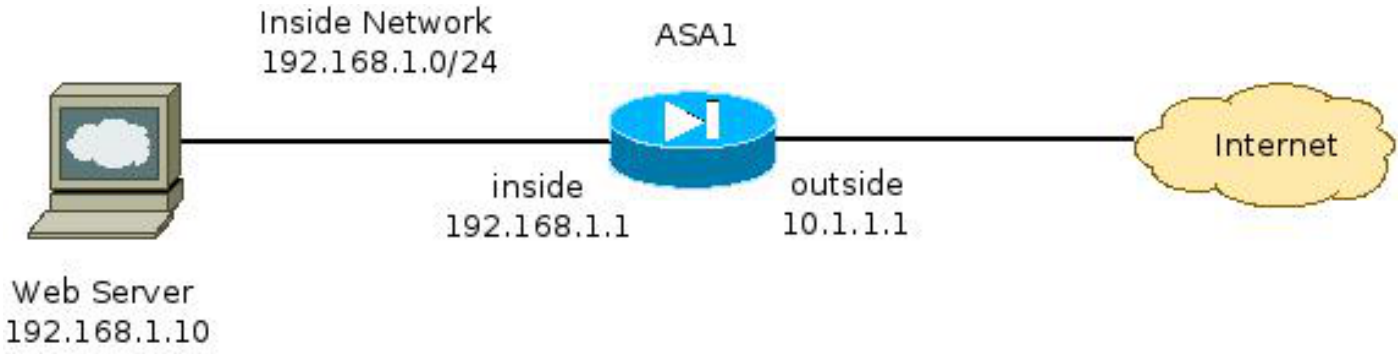
- CLI と Adaptive Security Device Manager（ASDM）の両方、またはいずれかを利用した Cisco ASA
- Cisco ASA での Cisco Cloud Web Security

使用するコンポーネント

このドキュメントの情報は、Cisco ASA に基づくものです。

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。

ネットワーク図



問題

ASA 上で Cisco CWS を設定する場合に一般的に発生する問題は、内部 Web サーバに ASA を介してアクセスできないときに発生します。たとえば、先のセクションで示したトポロジに対するサンプル設定は次のとおりです。

```
hostname ASA1
!
<snip>
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
!
<snip>
object network inside-network
subnet 192.168.1.0 255.255.255.0
object network web-server
host 192.168.1.10
!
<snip>
access-list outside_access_in permit tcp any host 192.168.1.10 eq www
access-list outside_access_in permit tcp any host 192.168.1.10 eq https
access-list http-traffic extended permit tcp any any eq www
access-list https-traffic extended permit tcp any any eq https
!
<snip>
scansafe general-options
server primary fqdn proxy193.scansafe.net port 8080
server backup fqdn proxy1363.scansafe.net port 8080
retry-count 5
license <license key>
!
<snip>
object network inside-network
nat (inside,outside) dynamic interface
object network web-server
nat (inside,outside) static 10.1.1.10
!
access-group outside_access_in in interface outside
```

```
!
<snip>
class-map http-class
match access-list http_traffic
class-map https-class
match access-list https_traffic
!
policy-map type inspect scansafe http-pmap
parameters
http
policy-map type inspect scansafe https-pmap
parameters
https
!
policy-map outside-policy
class http-class
inspect scansafe http-pmap fail-close
class https-class
inspect scansafe https-pmap fail-close
!
service-policy outside-policy interface inside
```

この設定では、外部の IP アドレス 10.1.1.10 から内部 Web サーバにアクセスできなくなる可能性があります。この問題には、次のようないくつかの原因があります。

- Web サーバでホストされるコンテンツのタイプ。
- Web サーバの Secure Socket Layer（SSL）証明書が CWS プロキシ サーバで信頼されていない。

解決方法

内部サーバでホストされるコンテンツは一般に信頼できると見なされます。したがって、CWS でこれらのサーバに対するトラフィックをスキャンする必要はありません。次の設定を使用して、このような内部サーバへのトラフィックを許可リストに追加できます。

```
ASA1(config)# object-group network ScanSafe-bypass
ASA1(config-network-object-group)# network-object host 192.168.1.10
ASA1(config-network-object-group)# exit
ASA1(config)# access-list http_traffic line 1 deny tcp
  any object-group ScanSafe-bypass eq www
ASA1(config)# access-list https_traffic line 1 deny tcp
  any object-group ScanSafe-bypass eq https
```

この設定では、TCP ポート **80 および 443 上の 192.168.1.10 の内部 Web サーバへのトラフィックは、CWS プロキシ サーバにリダイレクトされなくなります。**ネットワーク内にこのタイプのサーバが複数ある場合、**ScanSafe-bypass** という名前のオブジェクト グループに追加できます。

Final Configuration

次に、最終的な設定の例を示します。

```
hostname ASA1
!
interface GigabitEthernet0/0
  nameif outside
  security-level 0
```

```
  ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/1
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/2
  no nameif
  no security-level
  no ip address
!
interface GigabitEthernet0/3
  no nameif
  no security-level
  no ip address
!
interface Management0/0
  management-only
  no nameif
  no security-level
  no ip address
!
object network inside-network
  subnet 192.168.1.0 255.255.255.0
object network web-server
  host 192.168.1.10
object-group network ScanSafe-bypass
  network-object host 192.168.1.10
!
access-list outside_access_in permit tcp any host 192.168.1.10 eq www
access-list outside_access_in permit tcp any host 192.168.1.10 eq https
access-list http_traffic deny tcp any object-group ScanSafe-bypass eq www
access-list http-traffic extended permit tcp any any eq www
access-list https_traffic deny tcp any object-group ScanSafe-bypass eq https
access-list https-traffic extended permit tcp any any eq https
!
scansafe general-options
  server primary fqdn proxy193.scansafe.net port 8080
  server backup fqdn proxy1363.scansafe.net port 8080
  retry-count 5
  license
!
pager lines 24 mtu outside 1500
mtu inside 1500
no asdm history enable
arp timeout 14400
!
object network inside-network
  nat (inside,outside) dynamic interface
object network web-server
  nat (inside,outside) static 10.1.1.10
!
access-group outside_access_in in interface outside
!
route outside 0.0.0.0 0.0.0.0 10.1.1.254 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
```

```
!
class-map http-class
  match access-list http_traffic
class-map https-class
  match access-list https_traffic
!
policy-map type inspect scansafe
  http-pmap
  parameters
    http
policy-map type inspect scansafe https-pmap
  parameters
    https
!
policy-map inside-policy
class http-class
  inspect scansafe http-pmap fail-close
class https-class
  inspect scansafe https-pmap fail-close
!
service-policy inside-policy interface inside
```

関連情報

- Cisco ASA Connector クイックコンフィギュレーション ガイド
- Cisco ASA 9.0 CLI 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