CWS sur le trafic ASA vers les serveurs internes bloqué

Contenu

Introduction

Ce document décrit un problème courant rencontré lors de la configuration de Cisco Cloud Web Security (CWS) (précédemment appelé ScanSafe) sur les appliances de sécurité adaptatifs (ASA) Cisco versions 9.0 et ultérieures.

Avec CWS, l'ASA redirige de manière transparente les protocoles HTTP et HTTPS sélectionnés vers un serveur proxy CWS. Les administrateurs peuvent autoriser, bloquer ou avertir les utilisateurs finaux afin de les protéger des programmes malveillants grâce à la configuration appropriée des stratégies de sécurité sur le portail CWS.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître ces configurations :

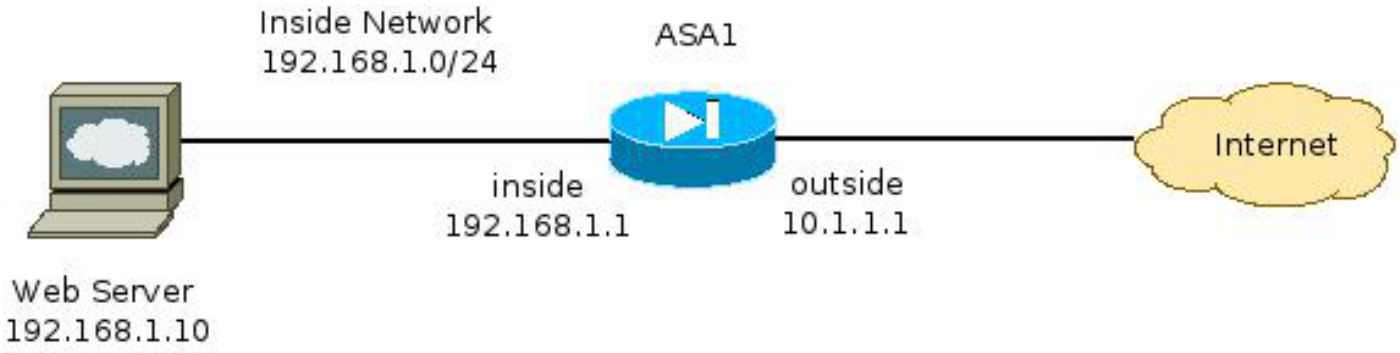
- Cisco ASA via CLI et/ou Adaptive Security Device Manager (ASDM)
- Cisco Cloud Web Security sur Cisco ASA

Components Used

Les informations de ce document sont basées sur les ASA Cisco.

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.

Diagramme du réseau



Problème

Un problème courant se produit lorsque vous configurez Cisco CWS sur l'ASA lorsque les serveurs Web internes deviennent inaccessibles via l'ASA. Par exemple, voici un exemple de configuration qui correspond à la topologie illustrée dans la section précédente :

```
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
```

Avec cette configuration, le serveur Web interne de l'extérieur qui utilise l'adresse IP **10.1.1.10** pourrait devenir inaccessible. Ce problème peut être causé par plusieurs raisons, telles que :

- Type de contenu hébergé sur le serveur Web.
- Le certificat SSL (Secure Socket Layer) du serveur Web n'est pas approuvé par le serveur proxy CWS.

Solution

Le contenu hébergé sur un ou plusieurs serveurs internes est généralement considéré comme fiable. Par conséquent, il n'est pas nécessaire d'analyser le trafic vers ces serveurs avec CWS. Vous pouvez ajouter du trafic à ces serveurs internes à la liste autorisée avec cette configuration :

```
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
```

Avec cette configuration, le trafic vers le serveur Web interne à **192.168.1.10** sur les ports TCP **80** et **443** ne sont plus redirigés vers les serveurs proxy CWS. S'il existe plusieurs serveurs de ce type dans le réseau, vous pouvez les ajouter au groupe d'objets nommé **ScanSafe-bypass**.

Configuration finale

Voici un exemple de configuration finale :

```
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
```

Informations connexes

- Guide de configuration rapide du connecteur Cisco ASA
- Guide de configuration de l'interface de ligne de commande Cisco ASA 9.0
- Support et documentation techniques - Cisco Systems