CWS sur le trafic ASA aux serveurs internes bloqués

Contenu

Introduction

Ce document décrit un problème courant produit quand vous configurez la sécurité Web de nuage de Cisco (CWS) (précédemment connu sous le nom de ScanSafe) sur des versions 9.0 et ultérieures des appliances de sécurité adaptable Cisco (ASA).

Avec CWS, l'ASA réoriente d'une manière transparente le HTTP et le HTTPS sélectionnés à un serveur proxy CWS. Les administrateurs ont la capacité de permettre, bloquer, ou avertir des utilisateurs afin de les protéger contre le malware avec la configuration appropriée des stratégies de sécurité sur le portail CWS.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de ces configurations :

- Cisco ASA par l'intermédiaire de CLI et/ou d'Adaptive Security Device Manager (ASDM)
- Cisco opacifient la sécurité Web sur Cisco ASA

Composants utilisés

Les informations dans ce document sont basées sur Cisco ASA.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un

environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Diagramme du réseau

Problème

Un problème courant produit quand vous configurez Cisco CWS sur l'ASA se pose quand les web server internes deviennent inaccessibles par l'ASA. Par exemple, voici une configuration d'échantillon 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 ce confguration, le web server interne de l'extérieur qui l'utilise l'adresse IP **10.1.1.10** pourrait devenir inaccessible. Cette question peut sont provoqué par par de plusieurs raisons, comme :

- Le type de contenu hébergé sur le web server.
- Le certificat de Protocole SSL (Secure Socket Layer) du web server n'est pas fait confiance par le serveur proxy CWS.

Solution

Le contenu hébergé sur n'importe quels serveurs internes est généralement considéré digne de confiance. Par conséquent, il n'est pas nécessaire de balayer le trafic à ces serveurs avec CWS. Vous pouvez le trafic de blanc-liste à de tels serveurs internes 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 au web server interne chez **192.168.1.10** sur les ports TCP **80** et **443** ne sont plus réorientés aux serveurs proxys CWS. S'il y a plusieurs les serveurs du ce saisissent le réseau, vous peuvent les ajouter au groupe d'objets nommé ScanSafe-**contournement**.

Configuration finale

Voici un exemple de la 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 <license key>
!
pager lines 24mtu 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 de connecteur de Cisco ASA
- Guide de configuration de Cisco ASA 9.0 CLI
- Support et documentation techniques - Cisco Systems