CWS op ASA traffic shaping op interne servers geblokkeerd

Inhoud

Inleiding

Dit document beschrijft een veelvoorkomend probleem dat u tegenkomt wanneer u Cisco Cloud Web Security (CWS) (voorheen bekend als ScanSafe) configureren op Cisco adaptieve security applicaties (ASA's) versies 9.0 en hoger.

Met CWS richt de ASA geselecteerde HTTP en HTTPS op een CWS proxy-server. Administrateurs hebben de mogelijkheid om eindgebruikers toe te staan, te blokkeren of te waarschuwen om hen tegen malware te beschermen met de juiste configuratie van veiligheidsbeleid op het CWS-portaal.

Voorwaarden

Vereisten

Cisco raadt aan dat u kennis hebt van deze configuraties:

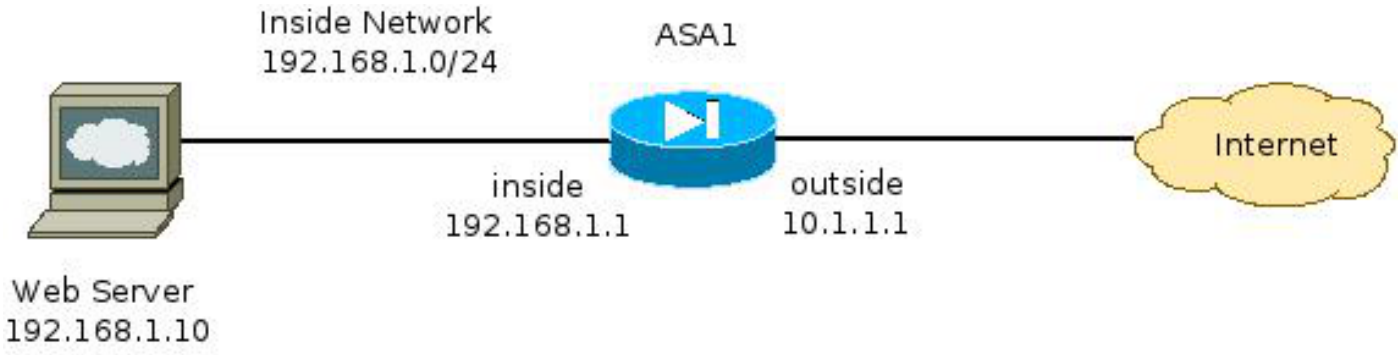
- Cisco ASA's via CLI en/of adaptieve security apparaatbeheer (ASDM)
- Cisco Cloud Web Security Appliance op Cisco ASA's

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco ASA's.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Netwerkdiagram



Probleem

Een algemeen probleem dat zich voordoet wanneer u Cisco CWS op de ASA-software configureren, treedt op wanneer de interne webservers ontoegankelijk worden door de ASA. Hier is bijvoorbeeld een voorbeeldconfiguratie die overeenkomt met de topologie die in de vorige sectie wordt geïllustreerd:

```
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
```

Met deze configuratie zou de interne webserver van buiten die het IP-adres **10.1.1.10** gebruikt, ontoegankelijk kunnen worden. Deze kwestie kan om meerdere redenen worden veroorzaakt, zoals:

- Het type inhoud dat op de webserver wordt gehost.
- Het Secure Socket Layer (SSL) certificaat van de webserver wordt niet vertrouwd door de CWS-proxyserver.

Oplossing

Inhoud die op een of meer interne servers wordt/worden opgeslagen, wordt over het algemeen als betrouwbaar beschouwd. Daarom is het niet nodig het verkeer naar deze servers met CWS te scannen. U kunt met deze configuratie verkeer aan dergelijke interne servers toevoegen aan de toegestane lijst:

```
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
```

Dankzij deze configuratie is het verkeer naar de interne webserver op **192.168.1.10** op TCP-poorten **80** en **443** niet langer opnieuw gericht op de CWS-proxy-servers. Als er meerdere servers van dit type in het netwerk zijn, kunt u deze toevoegen aan de doelgroep **ScanSafe-bypass**.

Eindconfiguratie

Hier is een voorbeeld van de laatste configuratie:

```
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
```

Gerelateerde informatie

- Cisco ASA Connector - handleiding voor snelle configuratie
- Cisco ASA 9900 CLI-configuratiegids
- Technische ondersteuning en documentatie – Cisco Systems