ASA上的CWS流向内部服务器的流量被阻止

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[网络图](#)
[问题](#)
[解决方案](#)
[最终配置](#)
[相关信息](#)

简介

本文档介绍在思科自适应安全设备(ASA)9.0版及更高版本上配置思科云网络安全(CWS)（以前称为ScanSafe）时遇到的常见问题。

使用CWS时，ASA透明地将所选HTTP和HTTPS重定向到CWS代理服务器。管理员能够允许、阻止或警告最终用户，以便通过在CWS门户上适当配置安全策略来保护他们免受恶意软件攻击。

先决条件

要求

思科建议您了解以下配置：

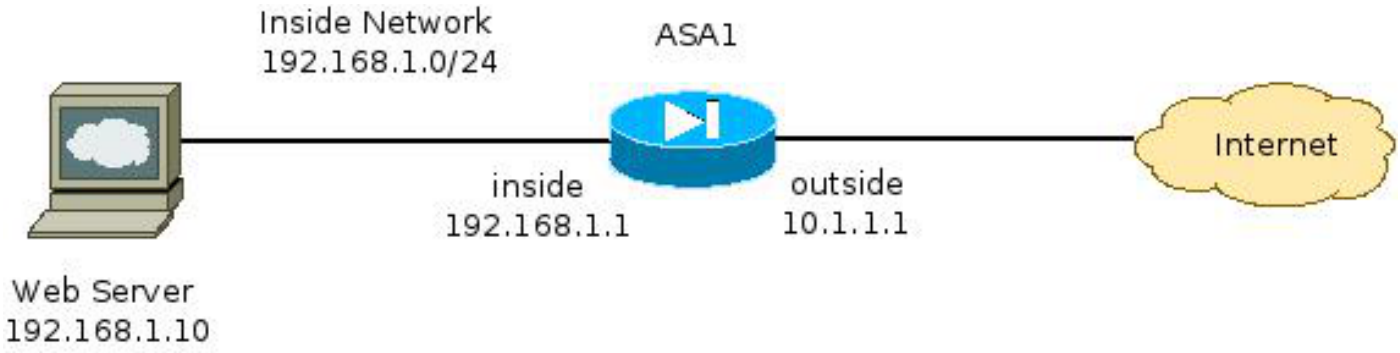
- 通过CLI和/或自适应安全设备管理器(ASDM)的Cisco ASA
- 思科ASA上的思科云Web安全

使用的组件

本文档中的信息基于Cisco ASA。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

网络图



问题

在ASA上配置Cisco CWS时遇到的常见问题是内部Web服务器无法通过ASA访问时。例如，以下是与上一节所示拓扑对应的示例配置：

```
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
```

使用此配置时，来自外部使用IP地址10.1.1.10的内**部Web服务器可能**无法访问。此问题可能由多种原因引起，例如：

- Web服务器上托管的内容类型。
- CWS代理服务器不信任Web服务器的安全套接字层(SSL)证书。

解决方案

任何内部服务器上托管的内容通常被视为可信。因此，无需使用CWS扫描流向这些服务器的流量。您可以使用以下配置将流量添加到此类内部服务器的允许列表：

```
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
```

使用此配置时，TCP端口80和**443**上发往位于**192.168.1.10的内**部Web服**务器**的流量不**再重定向到CWS代理服务器。**如果网络中有多台此类型的服务器，可以将它们添加到名为**ScanSafe-bypass**的对象组。

最终配置

以下是最终配置的示例：

```
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
```

相关信息

- Cisco ASA连接器快速配置指南
- Cisco ASA 9.0 CLI配置指南
- 技术支持和文档 - Cisco Systems