ASA上流向內部伺服器的CWS流量被阻止

目錄

簡介

本檔案介紹在思科調適型安全裝置(ASA)9.0及更新版本上設定思科雲端網路安全(CWS)（先前稱為ScanSafe）時遇到的常見問題。

藉助CWS，ASA透明地將選定的HTTP和HTTPS重定向到CWS代理伺服器。管理員能夠在CWS門戶上使用適當的安全策略配置允許、阻止或警告終端使用者，以保護他們免受惡意軟體的攻擊。

必要條件

需求

思科建議您瞭解以下設定：

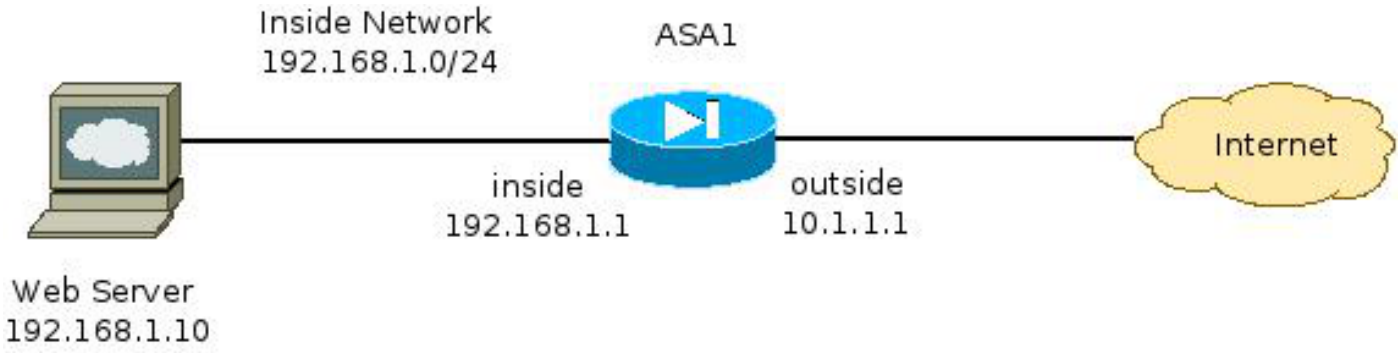
- 通過CLI和/或自適應安全裝置管理器(ASDM)的Cisco ASA
- Cisco ASA上的Cisco Cloud Web Security

採用元件

本文檔中的資訊基於Cisco ASA。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

網路圖表



問題

在ASA上配置Cisco CWS時遇到的常見問題是當通過ASA無法訪問內部Web伺服器時發生的。例如，以下是與上一節中所示的拓撲相對應的示例配置：

```
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
```

透過此設定，來自外部且使用IP位址10.1.1.10的內部Web伺服器可能會無法存取。導致此問題的原因有多種，例如：

- Web伺服器上承載的內容型別。
- CWS代理伺服器不信任Web伺服器的安全套接字層(SSL)證書。

解決方案

任何內部伺服器上託管的內容通常被認為值得信任。因此，沒有必要使用CWS掃描流向這些伺服器的流量。您可以使用以下配置將此類內部伺服器的流量新增到允許清單：

```
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
```

透過此設定，前往TCP連線埠80和443上192.168.1.10的內部Web伺服器的流量不會再重新導向到CWS代理伺服器。如果網路中有多個這種型別的伺服器，則可以將它們新增到名為ScanSafe-bypass的對象組中。

最終配置

以下是最終組態的範例：

```
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
```

相關資訊

- Cisco ASA聯結器快速配置指南
- Cisco ASA 9.0 CLI配置指南
- 技術支援與文件 - Cisco Systems