在ASA流量的CWS对阻塞的内部服务器

目录

简介

本文描述遇到的常见问题，当您配置Cisco Cloud Web安全(以前叫作ScanSafe)时(的) CWS在Cisco可适应安全工具(ASA)版本9.0和以上。

使用CWS， ASA透明地重定向选定HTTP和HTTPS到CWS代理服务器。管理员有能力允许，阻塞或者警告最终用户为了从与安全策略相应的配置的恶意软件保护他们在CWS门户的。

先决条件

要求

思科建议您有这些配置知识：

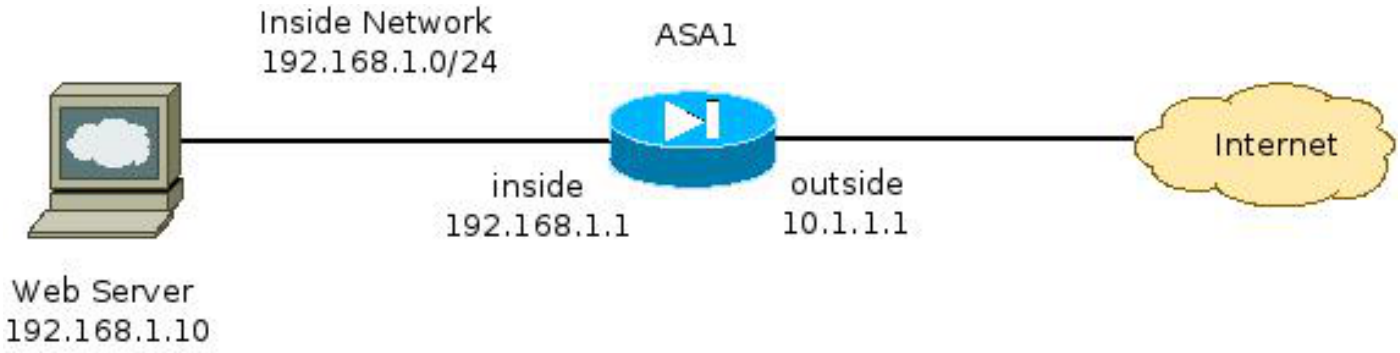
- 思科ASA通过CLI和可适应安全设备管理器(ASDM)
- 思科Cloud在思科ASA的Web安全

使用的组件

本文档中的信息根据思科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

遇到的常见问题，当您配置在ASA时的思科CWS发生，当内部网络服务器变得不可访问通过ASA。例如，这是对应于在前面部分说明的拓扑的配置示例：

```
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confguration，内部网络服务器从使用IP地址10.1.1.10威力的外面变得不可访问。此问题可以由多个原因导致，例如：

- 在Web服务器主机的内容种类。
- Web服务器的安全套接字层SSL证书没有由CWS代理服务器委托。

解决方案

在所有内部服务器主机的内容通常被认为值得信任。因此，扫描流量到有CWS的这些服务器是不必要的。您能怀特列表流量到有此配置的这样内部服务器：

```
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，对内部网络服务器的流量在TCP端口80和443的192.168.1.10不再重定向到CWS代理服务器。如果有多个服务器此输入网络，您能添加他们到对象组名为ScanSafe旁路。

最终配置

这是最终配置的示例：

```
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 <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
```

相关信息

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