为各种场景配置ASA访问控制列表

目录

简介

本文档介绍如何在自适应安全设备(ASA)上为各种场景配置访问控制列表(ACL)。

先决条件

要求

Cisco建议您了解ASA。

使用的组件

本文档中的信息基于ASA软件版本8.3及更高版本。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

ASA使用ACL来确定是允许还是拒绝流量。默认情况下，会拒绝从较低安全级别接口传递到**较高**安全级别接口的流量，而允许从较高安全级别接口**传递到较低**安全级别接口的流量。此行为也可以使用 ACL 改写。

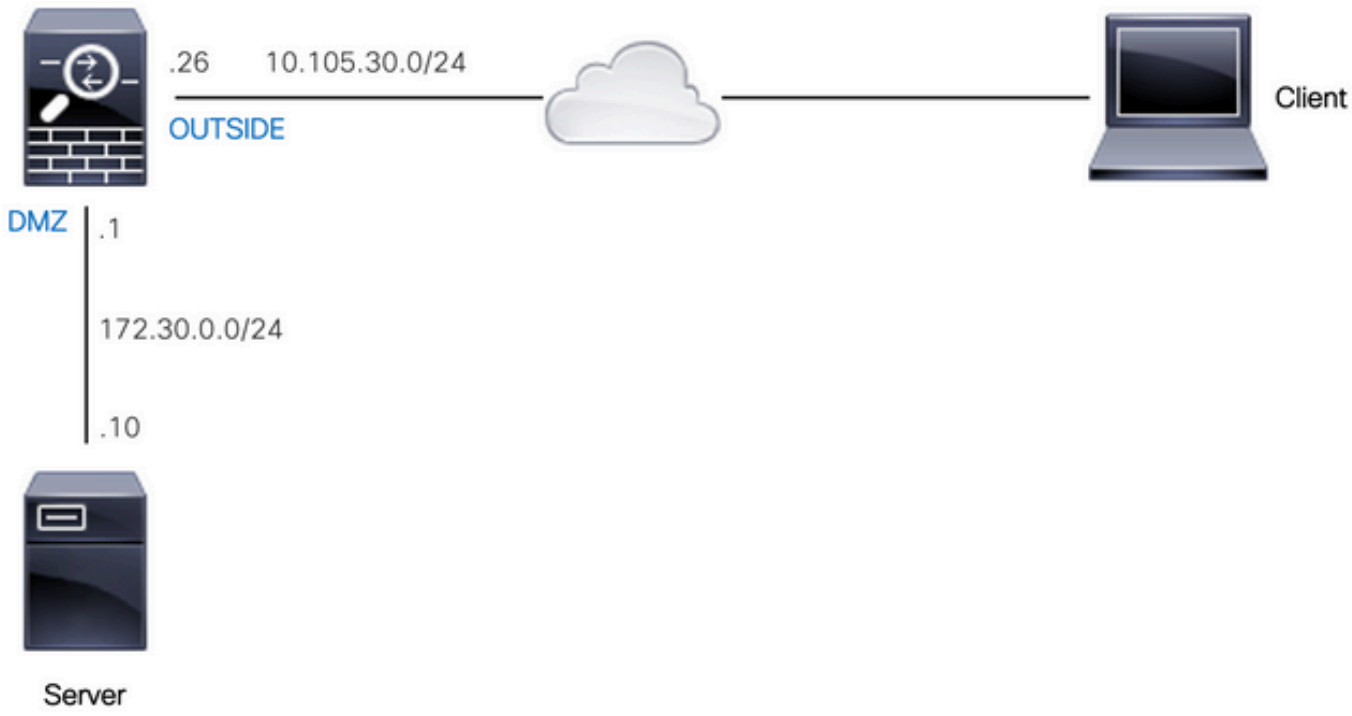
在NAT规则存在的情况下，在ASA的早期版本（8.2及更早版本）中，ASA会检查ACL，然后根据匹配的NAT规则取消转换数据包。在版本8.3及更高版本中，ASA会在检查ACL之前取消转换数据包。这意味着，对于ASA 8.3版及更高版本，根据主机的实际IP地址而不是转换后的IP地址来允许或拒绝流量。ACL由一个或多个访问控制条目(ACE)组成。

配置

场景 1.配置Ace以允许访问位于DMZ后面的Web服务器

位于外部接口后面的互联网客户端想要访问托管在DMZ接口后面的Web服务器，该接口侦听TCP端口80和443。

网络图



Web服务器的实际IP地址是172.30.0.10。静态一对一NAT规则配置为允许Internet用户使用已转换的IP地址10.105.130.27访问Web服务器。默认情况下，当静态NAT规则配置有与“外部”接口IP地址10.105.130.26位于同一子网的已转换IP地址时，ASA在“外部”接口上对10.105.130.27执行proxy-arp:

```
object network web-server
```

```
nat (dmz,outside) static 10.105.130.27
```

配置此ACE以仅允许Internet上的任何源IP地址连接到TCP端口80和443上的Web服务器。将ACL分配到入站方向的外部接口：

```
access-list OUT-IN extended permit tcp any host 172.30.0.10 eq www
access-list OUT-IN extended permit tcp any host 172.30.0.10 eq https
access-group OUT-IN in interface outside
```

验证

使用这些字段运行packet-tracer命令。 跟踪数据包的入口接口：外部

协议：TCP

源IP地址：互联网上的任何IP地址

源IP端口：任何临时端口

目的IP地址：Web服务器的转换IP地址(10.105.130.27)

目标端口：80或443

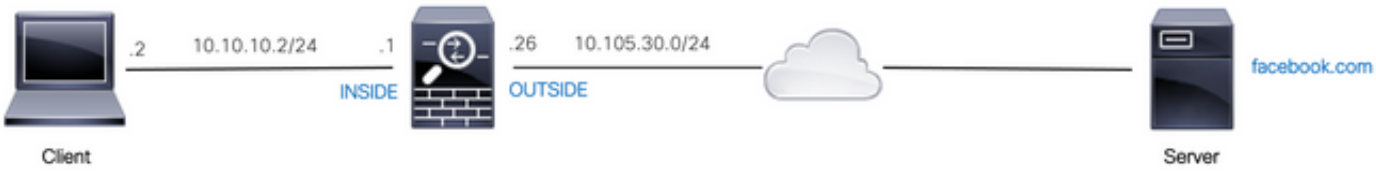
```
ciscoasa# packet-tracer input outside tcp 10.0.50.50 1234 10.105.130.27 443

!--- NAT untranslate from 10.105.130.27/443 to 172.30.0.10/443


Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network web-server
nat (dmz,outside) static 10.105.130.27
Additional Information:
NAT divert to egress interface dmz
Untranslate 10.105.130.27/443 to 172.30.0.10/443

!--- The configured ACL is permitting this packet to 172.30.0.10 on TCP port 443


Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group OUT-IN in interface outside
access-list OUT-IN extended permit tcp any host 172.30.0.10 eq https
Additional Information:

!--- Final result shows allow from the outside interface to the dmz interface

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: dmz
output-status: up
```

```
output-line-status: up
Action: allow
```

场景 2：配置Ace以允许使用FQDN访问Web服务器

允许IP地址为10.10.10.2且位于局域网(LAN)中的客户端访问facebook.com。

网络图



确保在ASA上正确配置了DNS服务器：

```
ciscoasa# show run dns
dns domain-lookup outside
dns server-group DefaultDNS
name-server 10.0.2.2
name-server 10.0.8.8
```

将此网络对象、FQDN对象和ACE配置为允许IP地址为10.10.10.2的客户端访问facebook.com。

```
object network obj-10.10.10.2
host 10.10.10.2

object network obj-facebook.com
fqdn facebook.com

access-list IN-OUT extended permit ip object obj-10.10.10.2 object obj-facebook.com
access-group IN-OUT in interface inside
```

验证

show dns的输出显示FQDN facebook.com的已解析IP地址：

```
ciscoasa# show dns

Host Flags Age Type Address(es)
facebook.com (temp, OK) 0 IP 10.0.228.35
```

访问列表显示解析的FQDN对象，还显示解析的IP地址：

```
ciscoasa# show access-list IN-OUT
access-list IN-OUT; 2 elements; name hash: 0x1b5ff18e
access-list IN-OUT line 1 extended permit ip object obj-10.10.10.2 object obj-facebook.com
(hitcnt=1) 0x22075b2a
access-list IN-OUT line 1 extended permit ip host 10.10.10.2 fqdn facebook.com (resolved)
0xfea095d7
access-list IN-OUT line 1 extended permit ip host 10.10.10.2 host 10.0.228.35 (facebook.com)
(hitcnt=1) 0x22075b2a
```

场景 3：配置Ace仅在一天中的特定时间内允许访问网站

从12:00到12:00（仅IST），LAN中的客户端可以每天访问IP地址为10.0.20.20的网站。

网络图

确保在ASA上正确配置了时区：

```
ciscoasa# show run clock
clock timezone IST 5 30
```

为所需持续时间配置时间范围对象：

```
time-range BREAK_TIME
periodic daily 12:00 to 14:00
```

配置以下网络对象和ACE，以允许LAN中的任何源IP地址仅在名为**BREAK_TIME的时间范围对象中提及的时间段内访问网站：**

```
object network obj-website
host 10.0.20.20

access-list IN-OUT extended permit ip any object obj-website time-range BREAK_TIME
access-group IN-OUT in interface inside
```

验证

当ASA上的时钟指示时间范围对象内的时间时，时间范围对象处于活动状态:

```
ciscoasa# show clock
12:03:41.987 IST Mon Oct 4 2021

ciscoasa# show time-range BREAK_TIME

time-range entry: BREAK_TIME (active)
periodic daily 12:00 to 14:00
used in: IP ACL entry

ciscoasa# show access-list IN-OUT
access-list IN-OUT; 1 elements; name hash: 0x1b5ff18e
access-list IN-OUT line 1 extended permit ip any object obj-website time-range BREAK_TIME
(hitcnt=12) 0x5a66c8f9
access-list IN-OUT line 1 extended permit ip any host 10.0.20.20 time-range BREAK_TIME
(hitcnt=12) 0x5a66c8f9
```

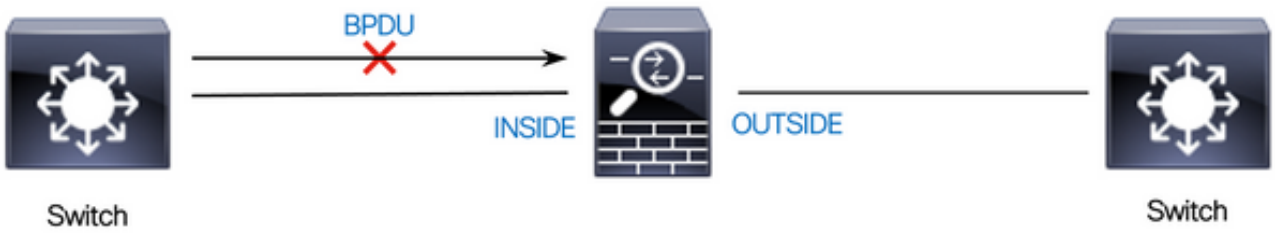
当ASA上的时钟指示时间范围对象之外的时间时，时间范围对象和ACE都处于非活动状态:

```
ciscoasa# show clock
14:15:44.409 IST Mon Oct 4 2021


ciscoasa# show time-range BREAK_TIME

time-range entry: BREAK_TIME (inactive)
periodic daily 12:00 to 14:00
used in: IP ACL entry


ciscoasa# show access-list IN-OUT
access-list IN-OUT; 1 elements; name hash: 0x1b5ff18e
access-list IN-OUT line 1 extended permit ip any object obj-website time-range BREAK_TIME
(hitcnt=0) (inactive) 0x5a66c8f9
access-list IN-OUT line 1 extended permit ip any host 10.0.20.20 time-range BREAK_TIME
(hitcnt=0) (inactive) 0x5a66c8f9
```

场景 4.配置Ace以阻止桥接协议数据单元(Bpdu)通过透明模式中的ASA

为防止生成树协议(STP)出现环路，默认情况下BPDU以透明模式通过ASA。要阻止BPDU，您需要配置EtherType规则以拒绝它们。

网络图



配置EtherType ACL以阻止BPDU在入站方向上通过ASA的“内部”接口，如下所示：

```
access-list block-bpdu ethertype deny dsap bpdu
access-list block-bpdu ethertype permit any
access-group block-bpdu in interface inside
```

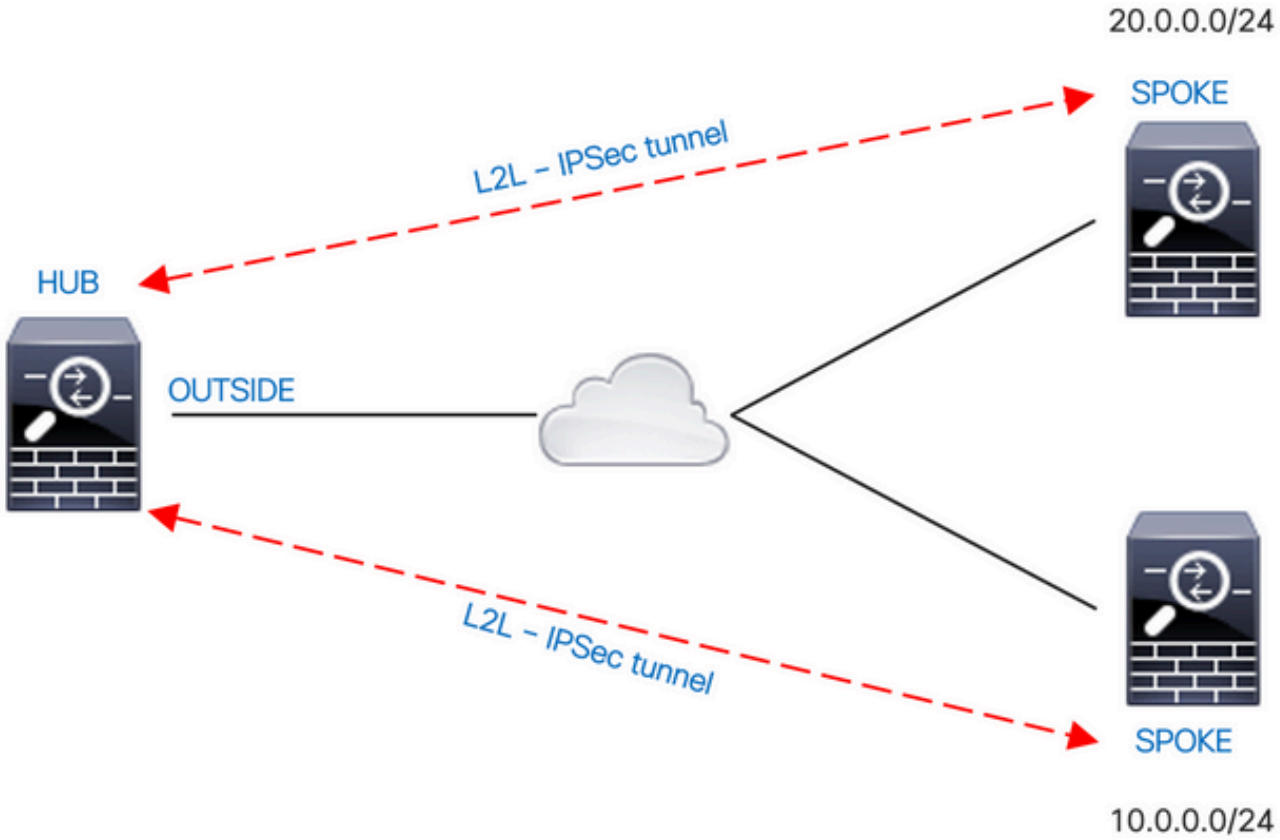
验证

检查访问列表中的命中计数以验证BPDU是否被ASA阻止：

```
ciscoasa# show access-list block-bpdu
access-list block-bpdu; 2 elements
access-list block-bpdu ethertype deny dsap bpdu(hitcount=14)
access-list block-bpdu ethertype permit any (hitcount=48)
```

方案 5.允许流量在具有相同安全级别的接口之间通过

网络图



默认情况下，阻止相同安全级别的接口之间通过的流量。要允许具有相同安全级别的接口之间的通信，或允许流量进入和退出同一接口（发夹/U转），请在全局配置模式下使用**same-security-traffic**命令。

此命令显示如何允许具有相同安全级别的不同接口之间的通信：

```
same-security-traffic permit inter-interface
```

此示例说明如何允许进出同一接口的通信：

```
same-security-traffic permit intra-interface
```

对于进入某接口然后又从同一接口路由出去的 VPN 流量，此功能非常有用。例如，如果您有一个中心辐射型VPN网络，其中此ASA是中心，而远程VPN网络是辐射点，为了使一个辐射点与另一个辐射点通信，流量必须转到ASA，然后再次传出到另一个辐射点。

验证

如果不使用**same-security-traffic permit inter-interface**命令，packet-tracer的输出表明，由于以下所示的隐式规**则，同一安全级别的不同接口之间通过的流量将被阻止：**

```
!--- The interfaces named 'test' and 'outside' have the same security level of 0

ciscoasa# show nameif
Interface Name Security
GigabitEthernet0/0 inside 100
GigabitEthernet0/1 dmz 50
GigabitEthernet0/2 test 0
GigabitEthernet0/5 outside 0
Management0/0 mgmt 0

!--- Traffic between different interfaces of same security level is blocked by an implicit rule

ciscoasa# packet-tracer input test tcp 172.16.20.10 1234 10.0.8.8 443 detailed


Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7f9960a2ff90, priority=110, domain=permit, deny=true
hits=0, user_data=0x0, cs_id=0x0, flags=0x3000, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none
input_ifc=test, output_ifc=any

Result:
input-interface: test
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame
0x00005638dfd7da57 flow (NA)/NA


!--- After running the command 'same-security-traffic permit inter-interface'

ciscoasa# show running-config same-security-traffic
same-security-traffic permit inter-interface

!--- Traffic between different interfaces of same security level is allowed

ciscoasa# packet-tracer input test tcp 172.16.20.10 1234 10.0.8.8 443 detailed

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7f9960a352d0, priority=2, domain=permit, deny=false
hits=2, user_data=0x0, cs_id=0x0, flags=0x3000, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none
```

```
input_ifc=test, output_ifc=any

Result:
input-interface: test
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

如果不使用**same-security-traffic permit intra-interface**命令，packet-tracer的输出会显示，由于以下所示的隐式规**则，传入和传出同一接口的流量会被阻止：**

```
!--- Traffic in and out of the same interface is blocked by an implicit rule

ciscoasa# packet-tracer input outside tcp 10.0.0.10 1234 10.1.0.10 443 detailed

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7f9960a32f30, priority=111, domain=permit, deny=true
hits=0, user_data=0x0, cs_id=0x0, flags=0x4000, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none
input_ifc=outside, output_ifc=outside

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame
0x00005638dfd7da57 flow (NA)/NA

!--- After running the command 'same-security-traffic permit intra-interface'

ciscoasa# show running-config same-security-traffic
same-security-traffic permit intra-interface


!--- Traffic in and out of the same interface is allowed

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7f99609291c0, priority=3, domain=permit, deny=false
hits=1, user_data=0x0, cs_id=0x0, flags=0x4000, protocol=0
```

```
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none
input_ifc=outside, output_ifc=outside


Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

方案 6.配置Ace以控制流向设备的流量

control-plane关键字指定是否使用ACL控制流向设备的流量。流向设备的管理流量(由http、ssh或telnet等命令定义)的访问控制规则比使用control-plane选项应用的管理访问规则具有更高的优先级。因此，即使被转储ACL明确拒绝，也必须允许此类允许的管理流量进入。

与常规访问规则不同，接口的一组管理规则末尾没有隐式拒绝。相反，任何与管理访问规则不匹配的连接都将由常规访问控制规则进行评估。或者，您可以使用ICMP规则控制到设备的ICMP流量。

网络图

使用control-plane关键字配置ACL，以阻止源自IP地址10.65.63.155且目的地为ASA的“外部”接口IP地址的流向设备的流量。

```
access-list control-plane-test extended deny ip host 10.65.63.155 any
access-group control-plane-test in interface outside control-plane
```

验证

检查访问列表中的命中计数以验证ACL是否阻止了流量：

```
ciscoasa# show access-list control-plane-test
access-list control-plane-test; 1 elements; name hash: 0x6ff5e700
access-list control-plane-test line 1 extended deny ip host 10.65.63.155 any (hitcnt=4)
0xedad4c6f
```

系统日志消息指示流量在“identity”接口上被丢弃：

```
Dec 27 2021 13:19:44: %ASA-4-106023: Deny tcp src outside:10.65.63.155/54108 dst
identity:10.105.130.26/8000 by access-group "control-plane-test" [0xedad4c6f, 0x0]
Dec 27 2021 13:19:45: %ASA-4-106023: Deny tcp src outside:10.65.63.155/54108 dst
```

```
identity:10.105.130.26/8000 by access-group "control-plane-test" [0xedad4c6f, 0x0]
Dec 27 2021 13:19:46: %ASA-4-106023: Deny tcp src outside:10.65.63.155/54108 dst
identity:10.105.130.26/8000 by access-group "control-plane-test" [0xedad4c6f, 0x0]
Dec 27 2021 13:19:47: %ASA-4-106023: Deny tcp src outside:10.65.63.155/54108 dst
identity:10.105.130.26/8000 by access-group "control-plane-test" [0xedad4c6f, 0x0]
```

日志记录

log关键字在ACE匹配用于网络访问的数据包(使用access-group命令应用的ACL)时设置日志记录选项。如果输入不带任何参数的log关键字，则可以在默认级别(6)和默认间隔（300秒）启用系统日志消息106100。如果不输入log关键字，则系统会为拒绝的数据包生成默认系统日志消息106023。日志选项包括：

- level — 介于0和7之间的严重性级别。默认值为6（信息性）。如果更改活动ACE的此级别，新级别将应用于新连接；现有连接将继续以上一级别记录。
- interval secs — 系统日志消息之间的时间间隔（以秒为单位），从1到600。默认值为 300。此值也用作从用于收集丢弃统计信息的缓存中删除非活动流的超时值。
- disable — 禁用所有ACE日志记录。
- default — 启用日志记录到消息106023。此设置与不包含log选项相同。

系统日志消息 106023:

```
Message:
%ASA-4-106023: Deny protocol src [interface_name :source_address /source_port ] [([idfw_user
|FQDN_string ], sg_info )] dst interface_name :dest_address /dest_port [([idfw_user |FQDN_string
], sg_info )] [type {string }, code {code }] by access_group acl_ID [0x8ed66b60, 0xf8852875]
```

说明：

实际IP数据包被ACL拒绝。即使没有为ACL启用日志选项，也会显示此消息。IP地址是实际IP地址，而不是通过NAT显示的值。如果找到匹配的IP地址，则会提供用户身份信息和FQDN信息。安全防火墙ASA记录身份信息（域\用户）或FQDN（如果用户名不可用）。如果身份信息或FQDN可用，则安全防火墙ASA会同时为源和目标记录此信息。

示例：

```
Dec 27 2021 14:58:25: %ASA-4-106023: Deny tcp src outside:10.65.63.155/56166 dst
inside:10.5.0.30/8000 by access-group "OUT-IN" [0x902a8ee8, 0x0]
Dec 27 2021 14:58:26: %ASA-4-106023: Deny tcp src outside:10.65.63.155/56166 dst
inside:10.5.0.30/8000 by access-group "OUT-IN" [0x902a8ee8, 0x0]
Dec 27 2021 14:58:27: %ASA-4-106023: Deny tcp src outside:10.65.63.155/56166 dst
inside:10.5.0.30/8000 by access-group "OUT-IN" [0x902a8ee8, 0x0]
```

系统日志消息 106100:

```
Message:

%ASA-6-106100: access-list acl_ID {permitted | denied | est-allowed} protocol interface_name
/source_address (source_port ) (idfw_user , sg_info ) interface_name /dest_address (dest_port )
(idfw_user , sg_info ) hit-cnt number ({first hit | number -second interval}) hash codes
```

说明：

将列出初始事件或时间间隔内的事件总数。此消息提供的信息比消息106023多，消息仅记录拒绝的数据包，不包括命中计数或可配置级别。

当访问列表行具有*log*参数时，由于非同步数据包到达安全防火墙ASA并由访问列表评估，因此预期可以触发此消息ID。例如，如果在安全防火墙ASA上收到ACK数据包（连接表中不存在TCP连接），安全防火墙ASA可以生成消息106100，指示允许该数据包；但是，由于不匹配连接，数据包稍后被正确丢弃。

该列表描述了消息值：

- 允许 |已拒绝 | est-allowed — 这些值指定ACL是允许还是拒绝数据包。如果值为允许值，则数据包被ACL拒绝，但被允许用于已建立的会话（例如，允许内部用户访问Internet，并且接受通常被ACL拒绝的响应数据包）。
- protocol - TCP、UDP、ICMP或IP协议号。
- interface_name — 已记录流量的源或目标的接口名称。支持VLAN接口。
- source_address — 已记录流的源IP地址。IP地址是实际IP地址，而不是通过NAT显示的值。
- dest_address — 已记录流量的目标IP地址。IP地址是实际IP地址，而不是通过NAT显示的值。
- source_port — 已记录流量的源端口（TCP或UDP）。对于ICMP，源端口后的编号是消息类型。
- idfw_user — 用户身份用户名，以及安全防火墙ASA可以找到IP地址的用户名时添加到现有系统日志的域名。
- sg_info — 安全防火墙ASA可以查找IP地址的安全组标记时添加到系统日志的安全组标记。安全组名称将随安全组标记一起显示（如果可用）。
- dest_port — 已记录流量的目标端口（TCP或UDP）。对于ICMP，目标端口后的编号为ICMP消息代码，对于某些消息类型可用。对于类型8，始终为0。有关ICMP消息类型的列表，请参阅URL:http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml。
- hit-cnt number — 此ACL条目在配置的时间间隔内允许或拒绝此流量的次数。当安全防火墙ASA为此流生成第一个消息时，值为1。
- first hit — 为此流生成的第一个消息。
- number — 第二个时间间隔 — 累计命中计数的时间间隔。使用带有**interval**选项的**access-list**命令设置此间隔。
- 散列代码 — 始终为对象组ACE和组成正则ACE打印两个散列代码。确定数据包在哪个ACE上命中。要显示这些散列代码，请输入**show-access list**命令。

示例：

```
Dec 27 2021 15:09:58: %ASA-6-106100: access-list OUT-IN permitted tcp
outside/10.65.63.155(56261) -> inside/10.5.0.30(8000) hit-cnt 1 first hit [0xa26b11fb,
0x00000000]
Dec 27 2021 15:10:15: %ASA-6-106100: access-list OUT-IN permitted tcp
outside/10.65.63.155(56266) -> inside/10.5.0.30(8000) hit-cnt 1 first hit [0xa26b11fb,
0x00000000]
Dec 27 2021 15:10:55: %ASA-6-106100: access-list OUT-IN permitted tcp
outside/10.65.63.155(56270) -> inside/10.5.0.30(8000) hit-cnt 1 first hit [0xa26b11fb,
0x00000000]
```

故障排除

目前没有针对此配置的故障排除信息。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。