為各種方案配置ASA訪問控制清單

目錄

簡介

本檔案介紹如何在調適型安全裝置(ASA)上為各種方案設定存取控制清單(ACL)。

必要條件

需求

思科建議您瞭解ASA。

採用元件

本文檔中的資訊基於ASA軟體版本8.3及更高版本。

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

ASA使用ACL來確定流量是被允許還是被拒絕。預設情況下，從**較低**安全層級介面傳輸到**較高**安全層級介面的流量會遭到拒絕，而從**較高**安全層級介面傳輸到**較低**安全層級介面的流量則允許通過。此行為也可以使用ACL覆蓋。

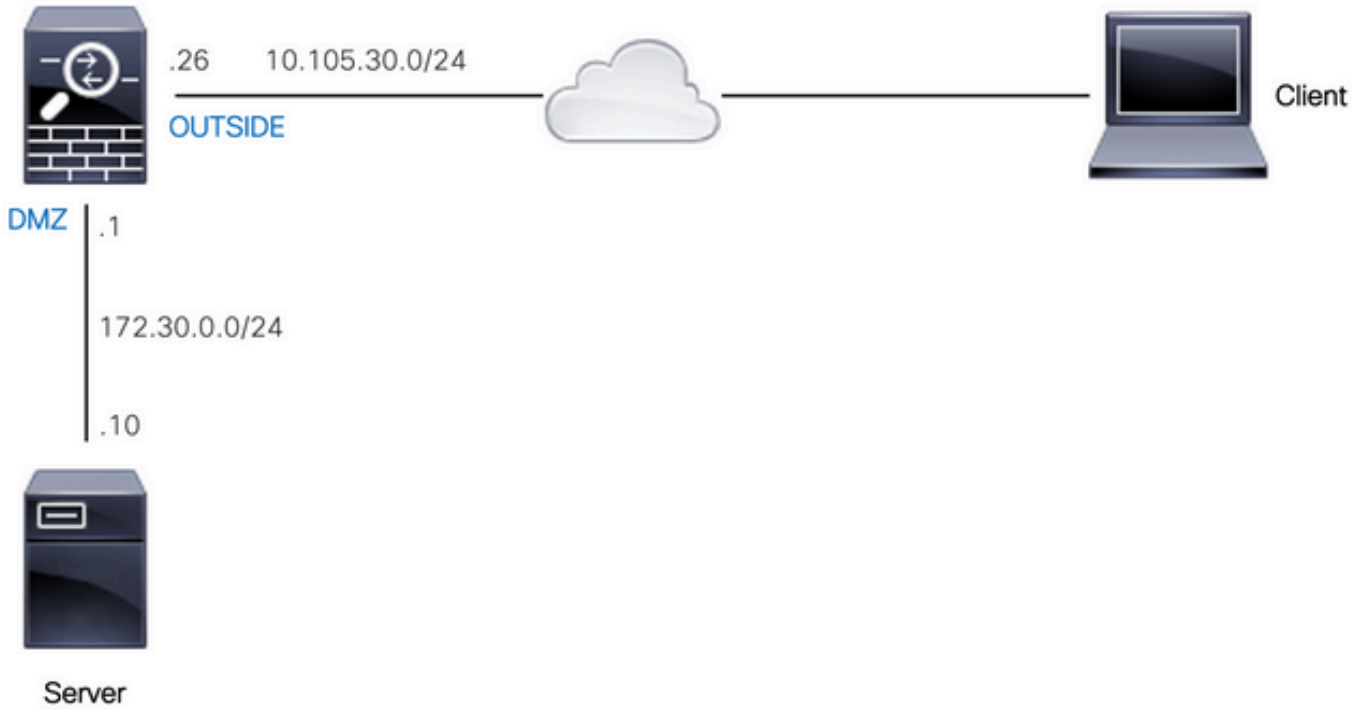
在存在NAT規則的情況下，在ASA的早期版本（8.2及更早版本）中，ASA會檢查ACL，然後根據匹配的NAT規則取消轉換資料包。在8.3及更高版本中，ASA在檢查ACL之前先解譯資料包。這意味著，對於ASA 8.3版及更高版本，根據主機的實際IP地址（而不是轉換後的IP地址）來允許或拒絕流量。ACL由一個或多個訪問控制條目(ACE)組成。

設定

案例 1.配置Ace以允許訪問位於DMZ後面的Web伺服器

位於外部介面後方的網際網路客戶端想要訪問在DMZ介面後託管的網路伺服器，該伺服器在TCP埠80和443上偵聽。

網路圖表



Web伺服器的實際IP地址為172.30.0.10。靜態一對一NAT規則配置為允許Internet使用者使用已轉換的IP地址10.105.130.27訪問Web伺服器。當使用與「outside」介面IP地址10.105.130.26位於同一子網的已轉換IP地址配置靜態NAT規則時，預設情況下，ASA在「outside」介面上對10.105.130.27執行proxy-arp:

```
object network web-server
```

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

配置此ACE以僅允許Internet上的任何源IP地址連線到TCP埠80和443上的Web伺服器。在入站方向將ACL分配給外部介面：

```
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
```

驗證

使用這些欄位運行Packet Tracer命令。 追蹤封包的輸入介面:outside

協定：TCP

源IP地址：網際網路上的任何IP地址

源IP埠：任何臨時埠

目標IP地址：Web伺服器的轉換IP地址(10.105.130.27)

目的地埠：80或443

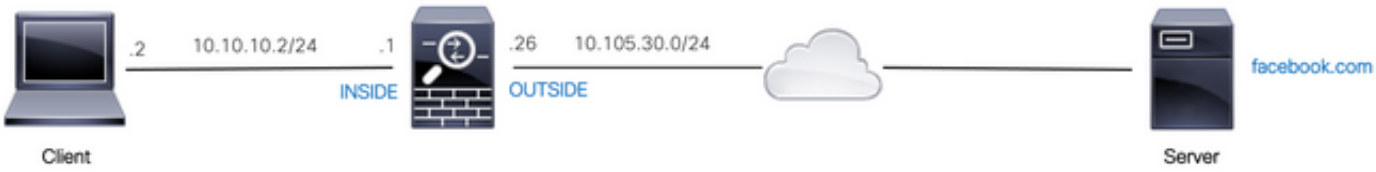
```
ciscoasa# packet-tracer input outside tcp 10.0.50.50 1234 10.105.130.27 443

!--- 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
```

案例 2.配置Ace以允許使用FQDN訪問Web伺服器

允許IP地址為10.10.10.2且位於區域網(LAN)中的客戶端訪問facebook.com。

網路圖表



確保在ASA上正確配置DNS伺服器：

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

將此網路對象、FQDN對象和ACE配置為允許IP地址為10.10.10.2的客戶端訪問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
```

驗證

show dns的輸出顯示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
```

訪問清單顯示解析的FQDN對象，還顯示解析的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
```

案例 3.配置Ace以允許僅在一天中的特定時間內訪問網站

LAN中的客戶端僅允許每天中午12:00至下午2:00訪問IP地址為10.0.20.20的網站。

網路圖表

確保在ASA上正確配置時區：

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

為所需的持續時間配置時間範圍對象：

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

配置這些網路對象和ACE，以允許LAN中的任何源IP地址僅在名為**BREAK_TIME的時間範圍對象中提及的時間段內訪問網站：**

```
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
```

驗證

當ASA上的時鐘指示時間範圍對象內的時間時，時間範圍對象處於活動狀態:

```
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
```

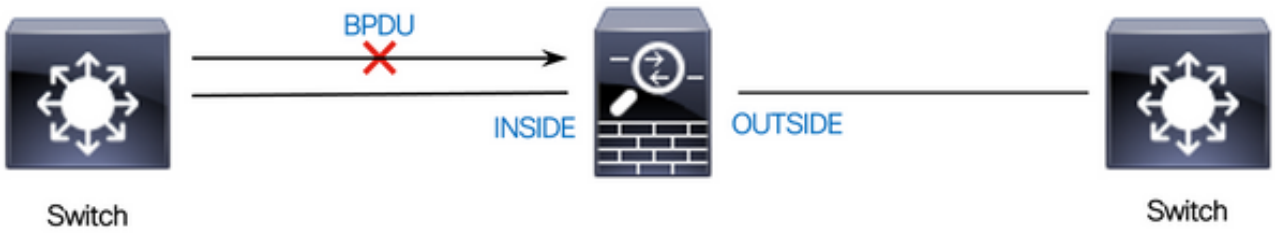
當ASA上的時鐘指示時間範圍對象之外的時間時，時間範圍對象和ACE都處於非活動狀態：

```
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
```

案例 4.配置Ace以阻止橋接協定資料單元(Bpdu)在透明模式下通過ASA

為了防止生成樹協定(STP)出現環路，預設情況下BPDU會以透明模式通過ASA。要阻止BPDU，您需要配置EtherType規則以拒絕它們。

網路圖表



配置EtherType ACL以阻止BPDU在入站方向通過ASA的「內部」介面，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
```

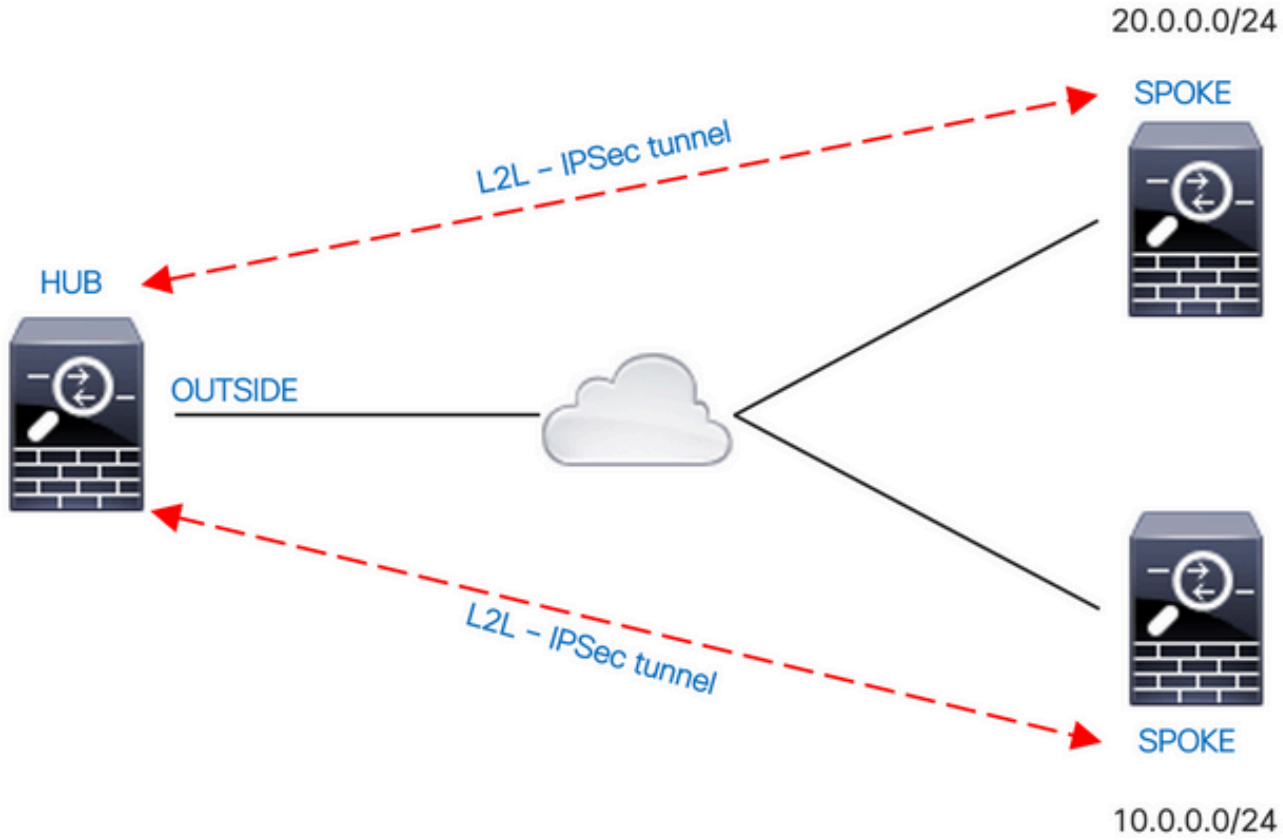
驗證

檢查訪問清單中的命中計數以驗證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)
```

案例 5.允許流量在同等安全級別的介面之間通過

網路圖表



預設情況下，在相同安全級別的介面之間通過的流量會被阻止。要允許具有相等安全級別的介面之間的通訊，或允許流量進入和退出同一介面（髮夾/迴轉），請在全域性配置模式下使用**same-security-traffic**命令。

此命令顯示如何允許具有相同安全級別的不同介面之間的通訊：

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

以下範例顯示如何允許同一介面中的和之外的通訊：

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

對於進入介面但隨後從同一介面路由出去的VPN流量，此功能非常有用。例如，如果您有一個中心輻射型VPN網路，其中此ASA是中心，遠端VPN網路是輻射型，為了使一個輻射型與另一個輻射型通訊，流量必須到達ASA，然後再次傳出到另一個輻射型。

驗證

如果不使用**same-security-traffic permit inter-interface**命令，Packet Tracer的輸出將表明，由於以下所示的隱式規**則，同一安全級別的不同介面之間通過的流量將被阻止：**

```
!--- 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的輸出會顯示，由於以下所示的隱式規**則，傳入和傳出同一介面的流量會被阻止：**

```
!--- 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
```

案例 6.配置Ace以控制到機箱的流量

control-plane關鍵字指定是否使用ACL控制流向裝置的流量。與使用control-plane選項應用的管理訪問規則相比，用於裝置間管理流量(由http、ssh或telnet等命令定義)的訪問控制規則的優先順序更高。因此，即使遭到轉儲ACL明確拒絕，也必須允許此類允許的管理流量進入。

與常規訪問規則不同，介面的一組管理規則末尾沒有隱含的deny。相反，任何與管理訪問規則不匹配的連線都將由常規訪問控制規則進行評估。或者，您可以使用ICMP規則控制到裝置的ICMP流量。

網路圖表

使用control-plane關鍵字配置ACL以阻止源自IP地址10.65.63.155且目的地為ASA的「外部」介面IP地址的入站流量。

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

驗證

檢查存取清單中的命中的數量，確認ACL已封鎖流量：

```
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
```

系統日誌消息指示流量在「identity」介面上被丟棄：

```
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]
```

日誌記錄

log關鍵字可在ACE與用於網路訪問的資料包(使用access-group命令應用的ACL)匹配時設定日誌記錄選項。如果輸入不帶任何引數的log關鍵字，則在預設級別(6)和預設間隔（300秒）內啟用系統日誌消息106100。如果不輸入log關鍵字，則系統會為拒絕的資料包生成預設系統日誌消息106023。日誌選項包括：

- level — 介於0和7之間的嚴重性級別。預設值為6（資訊性）。如果更改活動ACE的此級別，則新級別將應用於新連線；現有連線將繼續記錄在上一級別。
- interval secs — 系統日誌消息之間的時間間隔（以秒為單位），從1到600。預設值為300。此值也用作從用於收集丟棄統計資訊的快取中刪除非活動流的超時值。
- disable — 禁用所有ACE日誌記錄。
- default — 啟用消息日誌記106023。此設定與不包含log選項相同。

Syslog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]
```

說明:

實際IP資料包被ACL拒絕。即使未為ACL啟用日誌選項，也會顯示以下訊息。IP地址是實際IP地址，而不是通過NAT顯示的值。如果找到匹配的IP地址，則會同時提供使用者身份資訊和FQDN資訊。安全防火牆ASA記錄身份資訊（域\使用者）或FQDN（如果使用者名稱不可用）。如果身份資訊或FQDN可用，則安全防火牆ASA會記錄源和目標的此資訊。

範例：

```
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]
```

Syslog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
```

說明:

列出初始發生次數或間隔內發生的總次數。此消息提供的資訊比消息106023多，消息僅記錄拒絕的

資料包，不包括命中計數或可配置級別。

當訪問清單行具有*log*引數時，由於非同步資料包到達安全防火牆ASA並由訪問清單評估，因此預期可以觸發此消息ID。例如，如果在安全防火牆ASA上收到一個ACK資料包（該資料包的連線表中不存在TCP連線），安全防火牆ASA可以生成消息106100，指示該資料包被允許；但是，由於無匹配連線，該資料包隨後將被正確丟棄。

該清單描述了消息值：

- 允許 |已拒絕 | est-allowed — 這些值指定ACL是允許還是拒絕資料包。如果該值為允許設定，則該資料包被ACL拒絕，但允許用於已建立的會話（例如，允許內部使用者訪問Internet，並且接受通常被ACL拒絕的響應資料包）。
- protocol - TCP、UDP、ICMP或IP協定號。
- interface_name — 已記錄流的源或目標的介面名稱。支援VLAN介面。
- source_address — 已記錄流的源IP地址。IP地址是實際IP地址，而不是通過NAT顯示的值。
- dest_address — 記錄流的目標IP地址。IP地址是實際IP地址，而不是通過NAT顯示的值。
- source_port — 記錄流的源埠（TCP或UDP）。對於ICMP，來源連線埠之後的編號為訊息型別。
- idfw_user — 使用者身份使用者名稱，以及當Secure Firewall ASA可以找到IP地址的使用者名稱時新增到現有系統日誌的域名。
- sg_info — 安全防火牆ASA可以找到IP地址的安全組標籤時新增到系統日誌的安全組標籤。安全組名稱將隨安全組標籤一起顯示（如果可用）。
- dest_port — 已記錄流的目標埠（TCP或UDP）。對於ICMP，目的地連線埠之後的編號為ICMP訊息代碼，此代碼適用於某些訊息型別。對於型別8，始終為0。有關ICMP消息型別的清單，請參閱URL:http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml。
- hit-cnt number — 此ACL條目在配置的時間間隔內允許或拒絕此流量的次數。當安全防火牆ASA為此流生成第一個消息時，值為1。
- first hit — 為此流生成的第一個消息。
- number - second interval — 累計命中計數的間隔。使用**access-list**命令和**interval**選項設定此時間間隔。
- 雜湊代碼 — 始終為對象組ACE和組成規則ACE列印兩個雜湊代碼。確定資料包所命中的ACE的值。要顯示這些雜湊代碼，請輸入**show-access list**命令。

範例：

```
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]
```

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。