# Configurer la liste de contrôle d'accès ASA pour divers scénarios

## Table des matières


- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - Scénario 1. Configuration d'un ACE pour autoriser l'accès à un serveur Web situé derrière la DMZ
    - Diagramme du réseau
    - Vérifier
  - Scénario 2. Configuration d'un ACE pour autoriser l'accès à un serveur Web avec un nom de domaine complet (FQDN)
    - Diagramme du réseau
    - Vérifier
  - Scénario 3. Configurer un ACE pour autoriser l'accès à un site Web uniquement pendant une durée spécifique dans une journée
    - Diagramme du réseau
    - Vérifier
  - Scénario 4. Configuration d'un ACE pour bloquer les unités BPDU (Bridge Protocol Data Unit) via un ASA en mode transparent
    - Diagramme du réseau
    - Vérifier
  - Scénario 5. Autoriser le trafic à passer entre les interfaces ayant le même niveau de sécurité
    - Diagramme du réseau
    - Vérifier
  - Scénario 6. Configuration d'un ACE pour contrôler le trafic prêt à l'emploi
    - Diagramme du réseau
    - Vérifier
- Journalisation
- Dépannage


## Introduction

Ce document décrit comment configurer une liste de contrôle d'accès (ACL) sur l'appareil de sécurité adaptatif (ASA) pour divers scénarios.

## Conditions préalables

### Exigences

Cisco recommande que vous ayez connaissance de l'ASA.

### Composants utilisés

Les informations de ce document sont basées sur un logiciel ASA version 8.3 et ultérieure.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

## Informations générales

Les listes de contrôle d'accès sont utilisées par l'ASA pour déterminer si le trafic est autorisé ou refusé. Par défaut, le trafic qui passe d'une interface de niveau de sécurité inférieur à une interface de niveau de sécurité supérieur est refusé, tandis que le trafic d'une interface de niveau de sécurité supérieur à une interface de niveau de sécurité inférieur est autorisé. Ce comportement peut également être outrepassé par une ACL.

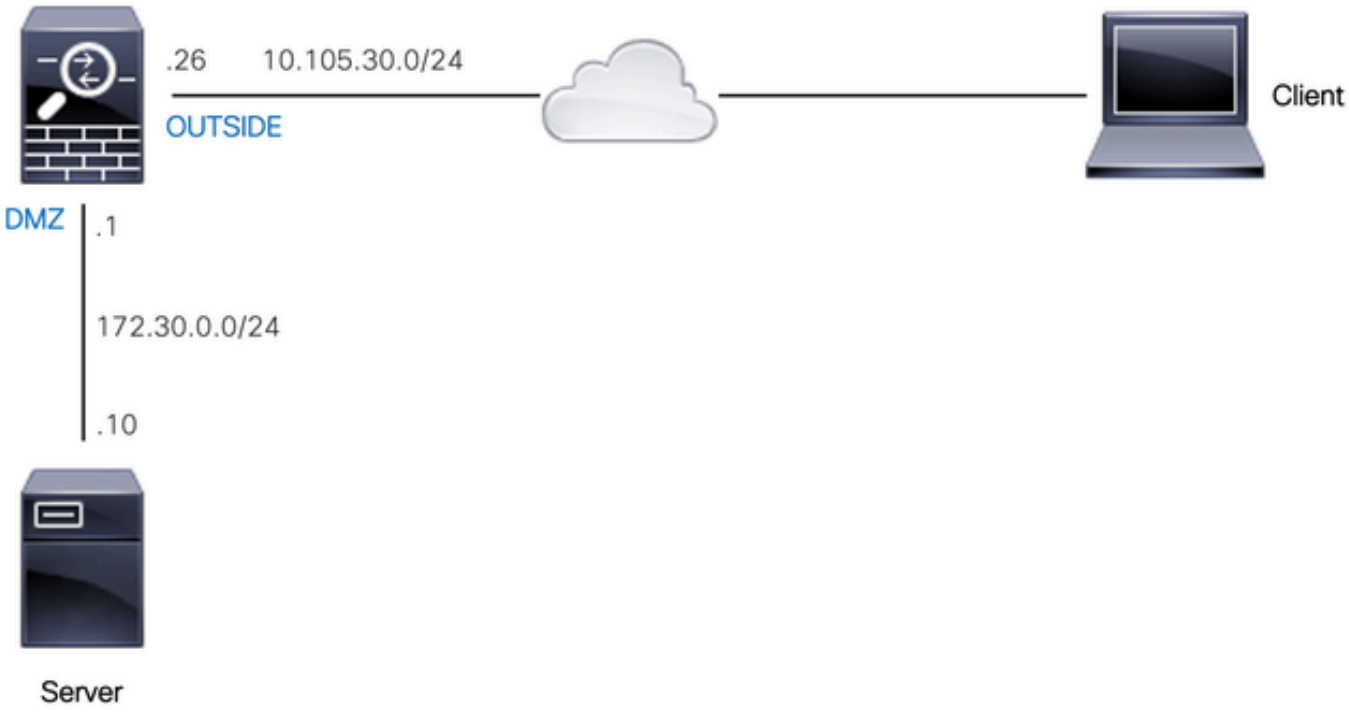
En présence de règles NAT, dans les versions antérieures de l'ASA (8.2 et antérieures), l'ASA vérifie la liste de contrôle d'accès avant d'annuler la traduction du paquet en fonction de la règle NAT qui a été mise en correspondance. Dans les versions 8.3 et ultérieures, l'ASA détraduit le paquet avant de vérifier les listes de contrôle d'accès. Cela signifie que pour un ASA version 8.3 et ultérieure, le trafic est autorisé ou refusé en fonction de l'adresse IP réelle de l'hôte au lieu de l'adresse IP traduite. Les listes de contrôle d’accès sont constituées d’une ou de plusieurs entrées de contrôle d’accès.

## Configurer

### Scénario 1. Configuration d'un ACE pour autoriser l'accès à un serveur Web situé derrière la DMZ

Le client sur Internet, situé derrière l'interface externe, veut accéder à un serveur Web hébergé derrière l'interface DMZ et écoutant sur les ports TCP 80 et 443.

Diagramme du réseau




L'adresse IP réelle du serveur Web est 172.30.0.10. Une règle NAT statique un-à-un est configurée pour permettre aux utilisateurs Internet d'accéder au serveur Web avec une adresse IP traduite 10.105.130.27. L'ASA effectue un proxy-arp pour 10.105.130.27 sur l'interface externe par défaut lorsqu'une règle NAT statique est configurée avec une adresse IP traduite qui tombe dans le même sous-réseau que l'adresse IP d'interface externe 10.105.130.26 :

```
object network web-server
 nat (dmz,outside) static 10.105.130.27
```

Configurez cette entrée de contrôle d’accès pour autoriser toute adresse IP source sur Internet à se connecter au serveur Web uniquement sur les ports TCP 80 et 443. Attribuez la liste de contrôle d’accès à l’interface externe dans la direction entrante :

```
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
```

Vérifier

Exécutez une commande packet-tracer avec ces champs. Interface d'entrée sur laquelle tracer le paquet : extérieur

Protocole : TCP

adresse IP source: Toute adresse IP sur Internet

Port IP source : Tout port éphémère

adresse IP de destination: Adresse IP traduite du serveur Web (10.105.130.27)

Port de destination : 80 ou 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:

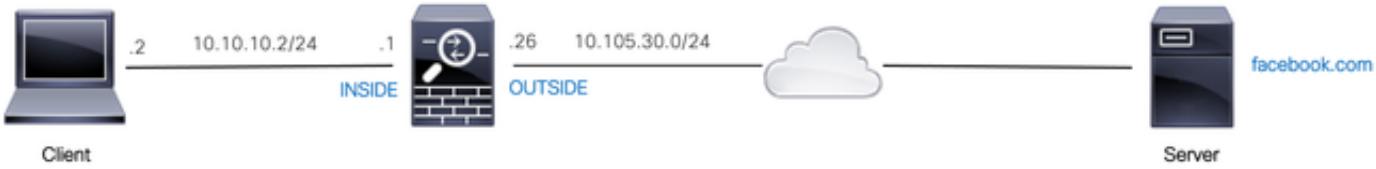
!--- Final result shows allow from the outside interface to the dmz interface

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

## Scénario 2. Configuration d’un ACE pour autoriser l’accès à un serveur Web avec un nom de domaine complet (FQDN)

Le client dont l'adresse IP est 10.10.10.2 et qui se trouve sur le réseau local (LAN) est autorisé à accéder à facebook.com.

Diagramme du réseau




Assurez-vous que le serveur DNS est correctement configuré sur l'ASA :

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

Configurez cet objet réseau, l'objet FQDN et l'ACE pour permettre au client dont l'adresse IP est 10.10.10.2 d'accéder à 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
```

Vérifier

Le résultat de la commande show dns affiche l'adresse IP résolue pour le nom de domaine complet facebook.com:

```
ciscoasa# show dns

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

La liste d'accès affiche l'objet FQDN comme résolu et indique également l'adresse IP résolue :

<#root>

```
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) 0
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
```

## Scénario 3. Configurer un ACE pour autoriser l'accès à un site Web uniquement pendant une durée spécifique dans une journée

Le client situé sur le réseau local est autorisé à accéder à un site Web dont l'adresse IP est 10.0.20.20, tous les jours, de 12 h à 14 h (heure locale uniquement).

Diagramme du réseau




Assurez-vous que le fuseau horaire est correctement configuré sur l'ASA :

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

Configurez un objet de plage de temps pour la durée requise :

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

Configurez ces objets réseau et l'ACE pour permettre à toute adresse IP source située sur le réseau local d'accéder au site Web uniquement pendant la période mentionnée dans l'objet de plage de temps nommé BREAK_TIME:

```
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
```

## Vérifier

L'objet de plage temporelle est actif lorsque l'horloge de l'ASA indique une heure comprise dans l'objet de plage temporelle :

```
<#root>

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) 0x
```

L'objet time-range et l'ACE sont inactifs lorsque l'horloge sur l'ASA indique une heure qui est en dehors de l'objet time-range :

```
<#root>

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
```

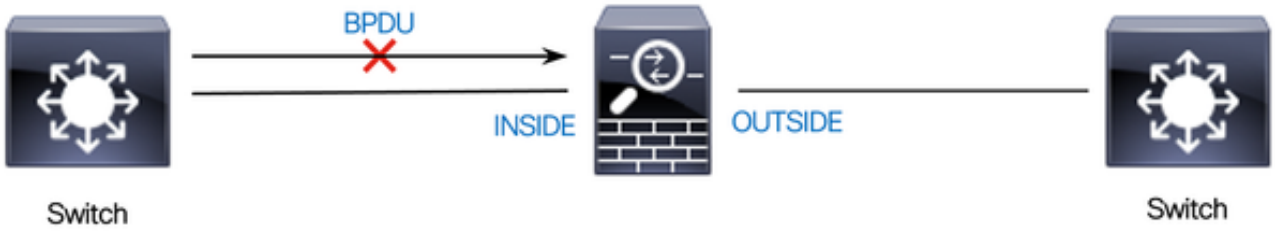
```
   used in: IP ACL entry


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) (inac
```

## Scénario 4. Configuration d'un ACE pour bloquer les unités BPDU (Bridge Protocol Data Unit) via un ASA en mode transparent

Pour empêcher les boucles avec le protocole STP (Spanning Tree Protocol), les unités BPDU sont transmises par défaut via l'ASA en mode transparent. Pour bloquer les BPDU, vous devez configurer une règle EtherType pour les refuser.

Diagramme du réseau




Configurez la liste de contrôle d'accès EtherType pour empêcher les BPDU de passer par l'interface interne de l'ASA dans la direction entrante, comme illustré ici :

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

Vérifier

Vérifiez le nombre d'occurrences dans la liste de contrôle d'accès pour vous assurer que les BPDU sont bloqués par l'ASA :

<#root>

```
ciscoasa# show access-list block-bpdu
access-list block-bpdu; 2 elements
access-list block-bpdu ethertype deny dsap bpdu
```

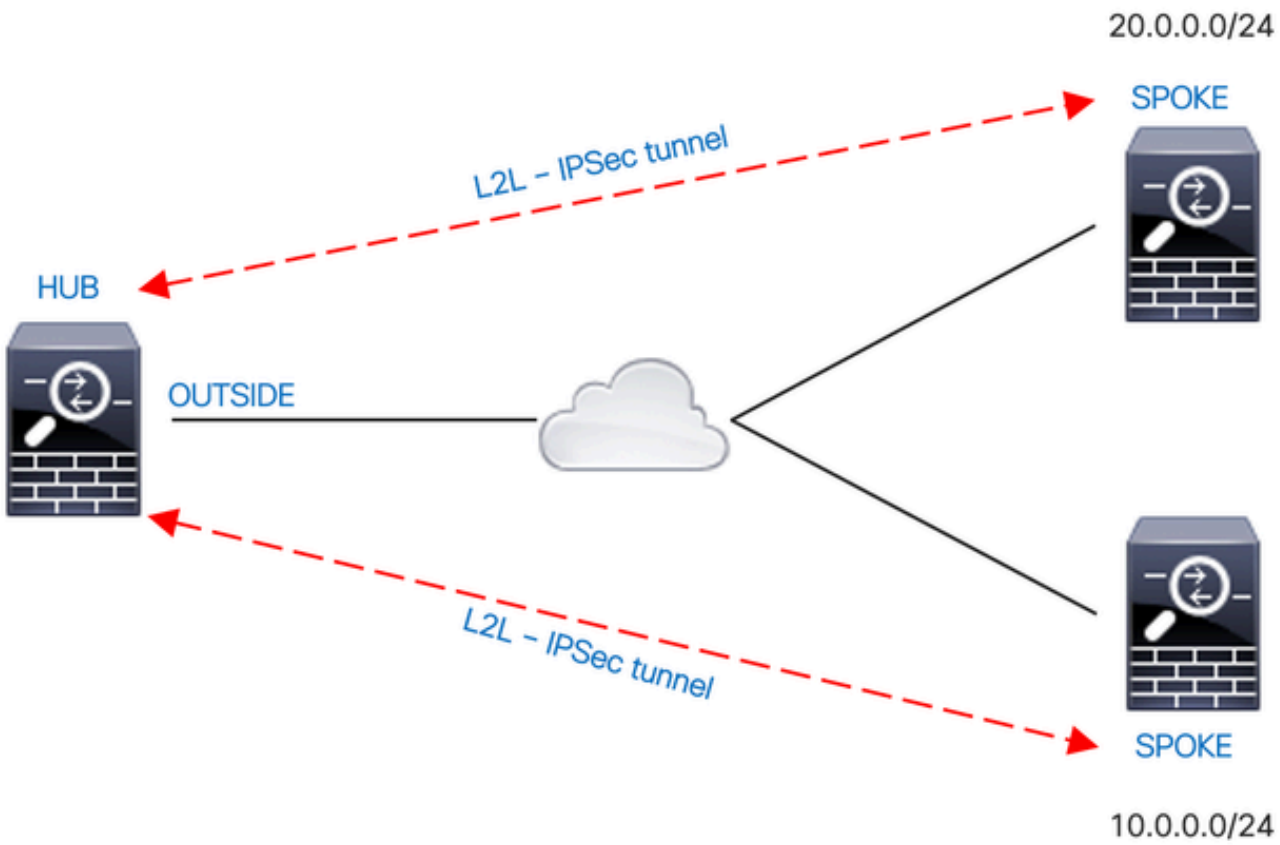
```
(hitcount=14)

access-list block-bpdu ethertype permit any (hitcount=48)
```

## Scénario 5. Autoriser le trafic à passer entre les interfaces ayant le même niveau de sécurité

Diagramme du réseau




Par défaut, le trafic qui passe entre les interfaces du même niveau de sécurité est bloqué. Pour permettre la communication entre des interfaces avec des niveaux de sécurité égaux, ou pour permettre au trafic d'entrer et de sortir de la même interface (hairpin/u-turn), utilisez la commande same-security-traffic en mode de configuration globale.

Cette commande montre comment autoriser la communication entre différentes interfaces qui ont le même niveau de sécurité :

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

Cet exemple montre comment autoriser la communication en entrée et en sortie de la même interface :

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

Cette fonctionnalité est utile pour le trafic VPN qui entre dans interface, mais qui est ensuite routé hors de cette même interface. Par exemple, si vous avez un réseau VPN Hub and Spoke où cet ASA est le concentrateur et les réseaux VPN distants sont des rayons, afin qu'un rayon puisse communiquer avec un autre rayon, le trafic doit aller à l'ASA, puis de nouveau à l'autre rayon.

Vérifier

Sans la commande same-security-traffic permit inter-interface, le résultat de packet-tracer indique que le trafic passant entre différentes interfaces du même niveau de sécurité est bloqué en raison d'une règle implicite comme montré ici :

<#root>

```
!--- 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**

**!--- 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
```

Sans la commande same-security-traffic permit intra-interface, le résultat de packet-tracer indique que le trafic entrant et sortant de la même interface est bloqué en raison d'une règle implicite comme montré ici :

```
<#root>


!--- 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**

**!--- 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**

## Scénario 6. Configuration d’un ACE pour contrôler le trafic prêt à l’emploi

Le mot clé control-plane spécifie si la liste de contrôle d’accès est utilisée pour contrôler le trafic prêt à l’emploi. Les règles de contrôle d'accès pour le trafic de gestion prêt à l'emploi (définies par des commandes telles que http, ssh, ou telnet) ont une priorité plus élevée qu'une règle d'accès de gestion appliquée avec l'option de plan de contrôle. Par conséquent, un tel trafic de gestion autorisé doit être autorisé à entrer même s'il est explicitement refusé par la liste de contrôle d'accès prête à l'emploi.

Contrairement aux règles d’accès standard, il n’y a pas de refus implicite à la fin d’un ensemble de règles de gestion pour une interface. Au lieu de cela, toute connexion qui ne correspond pas à une règle d'accès de gestion est ensuite évaluée par des règles de contrôle d'accès standard. Vous pouvez également utiliser les règles ICMP (Internet Control Message Protocol) pour contrôler le trafic ICMP vers le périphérique.

Diagramme du réseau




Une liste de contrôle d'accès est configurée avec le mot clé control-plane pour bloquer le trafic prêt à l'emploi provenant de l'adresse IP 10.65.63.155 et destiné à l'adresse IP de l'interface externe de l'ASA.

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

Vérifier

Vérifiez le nombre d’occurrences dans la liste de contrôle d’accès pour vous assurer que le trafic est bloqué par la liste de contrôle d’accès :

<#root>

```
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
```

Les messages Syslog indiquent que le trafic est abandonné sur l'interface d'identité :

<#root>

```
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
Dec 27 2021 13:19:46: %ASA-4-106023: Deny tcp src outside:10.65.63.155/54108 dst identity:10.105.130.26
Dec 27 2021 13:19:47: %ASA-4-106023: Deny tcp src outside:10.65.63.155/54108 dst identity:10.105.130.26
```

# Journalisation

Le mot clé log définit les options de journalisation lorsqu'une entrée de contrôle d'accès correspond à un paquet pour l'accès réseau (une liste de contrôle d'accès appliquée avec la commande access-group). Si vous entrez le mot-clé log sans argument, vous activez le message de journal système 106100 au niveau par défaut (6) et pendant l'intervalle par défaut (300 secondes). Si vous n'entrez pas le mot-clé log, le message de journal système par défaut 106023 est généré pour les paquets refusés. Les options de journal sont :

- level : niveau de gravité compris entre 0 et 7. La valeur par défaut est 6 (informatif). Si vous modifiez ce niveau pour une ACE active, le nouveau niveau s'applique aux nouvelles connexions ; les connexions existantes continuent d'être enregistrées au niveau précédent.
- interval secs : intervalle de temps en secondes entre les messages syslog, compris entre 1 et 600. La valeur par défaut est 300. Cette valeur est également utilisée comme valeur de délai d'attente pour la suppression d'un flux inactif du cache utilisé pour collecter les statistiques de suppression.
- disable : désactive toute la journalisation ACE.
- default : active la consignation dans le message 106023. Ce paramètre revient à ne pas inclure l'option de consignation.

Message Syslog 106023 :

```
Message:
%ASA-4-106023: Deny protocol src [interface_name :source_address /source_port ] [([idfw_user |FQDN_stri
```

Explication:

Un paquet IP réel a été refusé par la liste de contrôle d’accès. Ce message apparaît même si l'option de journal n'est pas activée pour une liste de contrôle d'accès. L'adresse IP est l'adresse IP réelle au lieu des valeurs affichées par la fonction NAT. Les informations d'identité utilisateur et les informations de nom de domaine complet sont fournies pour les adresses IP si une correspondance est trouvée. L'ASA de pare-feu sécurisé consigne les informations d'identité (domaine\utilisateur) ou le nom de domaine complet (si le nom d'utilisateur n'est pas disponible). Si les informations d'identité ou le nom de domaine complet sont disponibles, l'ASA de pare-feu sécurisé consigne ces informations pour la source et la destination.

Exemple :

```
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 
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 
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 
```

Message Syslog 106100 :

```
Message:

%ASA-6-106100: access-list acl_ID {permitted | denied | est-allowed} protocol interface_name /source_ad
```

Explication:

L'occurrence initiale ou le nombre total d'occurrences pendant un intervalle sont répertoriés. Ce message fournit plus d'informations que le message 106023, qui consigne uniquement les paquets refusés et n'inclut pas le nombre d'occurrences ou un niveau configurable.

Lorsqu'une ligne de liste d'accès comporte l'argument log, cet ID de message doit pouvoir être déclenché en raison d'un paquet non synchronisé qui arrive à l'ASA Secure Firewall et qui est évalué par la liste d'accès. Par exemple, si un paquet ACK est reçu sur le pare-feu ASA sécurisé (pour lequel aucune connexion TCP n'existe dans la table de connexion), le pare-feu ASA sécurisé peut générer le message 106100, indiquant que le paquet a été autorisé ; cependant, le paquet est ensuite abandonné correctement en raison de l'absence de connexion correspondante.

La liste décrit les valeurs du message :

- autorisé | refusé | est-allowed : ces valeurs indiquent si le paquet a été autorisé ou refusé par la liste de contrôle d'accès. Si la valeur est définie, le paquet a été refusé par la liste de contrôle d’accès, mais a été autorisé pour une session déjà établie (par exemple, un utilisateur interne est autorisé à accéder à Internet et les paquets de réponse qui seraient

normalement refusés par la liste de contrôle d'accès sont acceptés).

- protocol : TCP, UDP, ICMP ou un numéro de protocole IP.
- interface_name : nom d'interface de la source ou de la destination du flux consigné. Les interfaces VLAN sont prises en charge.
- source_address : adresse IP source du flux consigné. L'adresse IP est l'adresse IP réelle au lieu des valeurs affichées par la fonction NAT.
- dest_address : adresse IP de destination du flux consigné. L'adresse IP est l'adresse IP réelle au lieu des valeurs affichées par la fonction NAT.
- source_port : port source du flux consigné (TCP ou UDP). Pour ICMP, le numéro situé après le port source est le type de message.
- idfw_user : nom d'utilisateur de l'identité de l'utilisateur, avec le nom de domaine qui est ajouté au syslog existant lorsque l'ASA du pare-feu sécurisé peut trouver le nom d'utilisateur pour l'adresse IP.
- sg_info : balise de groupe de sécurité ajoutée au syslog lorsque l'ASA du pare-feu sécurisé peut trouver une balise de groupe de sécurité pour l'adresse IP. Le nom du groupe de sécurité s'affiche avec la balise du groupe de sécurité, si disponible.
- dest_port : port de destination du flux consigné (TCP ou UDP). Pour ICMP, le numéro situé après le port de destination est le code de message ICMP, qui est disponible pour certains types de messages. Pour le type 8, il est toujours 0. Pour obtenir la liste des types de messages ICMP, consultez l'URL suivante : Paramètres du protocole ICMP (Internet Control Message Protocol).
- hit-cnt number : nombre de fois que ce flux a été autorisé ou refusé par cette entrée de liste de contrôle d'accès dans l'intervalle de temps configuré. La valeur est 1 lorsque l'ASA de pare-feu sécurisé génère le premier message pour ce flux.
- first hit — Premier message généré pour ce flux.
- number - second interval : intervalle au cours duquel le nombre d'occurrences est cumulé. Définissez cet intervalle avec la commande access-list avec l'option interval.
- Codes de hachage : deux codes sont toujours imprimés pour l'ACE du groupe d'objets et l'ACE régulière constitutive. Les valeurs sont déterminées sur l'ACE sur lequel le paquet a atteint. Pour afficher ces codes de hachage, entrez la commande show-access list.

Exemple :

```
Dec 27 2021 15:09:58: %ASA-6-106100: access-list OUT-IN permitted tcp outside/10.65.63.155(56261) -> in
Dec 27 2021 15:10:15: %ASA-6-106100: access-list OUT-IN permitted tcp outside/10.65.63.155(56266) -> in
Dec 27 2021 15:10:55: %ASA-6-106100: access-list OUT-IN permitted tcp outside/10.65.63.155(56270) -> in
```

# Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.