Comprendre la DACL 802.1x, la liste de contrôle d'accès par utilisateur, l'ID de filtre et le comportement de suivi des périphériques

Table des matières

Introduction

Ce document décrit la fonctionnalité de suivi des périphériques IP, les déclencheurs d'ajout et de suppression d'un hôte et l'impact du suivi des périphériques sur la liste de contrôle d'accès 802.1x.

Théorie de suivi des périphériques

Ce document décrit le fonctionnement de la fonctionnalité du suivi des périphériques IP, y compris les déclencheurs pour ajouter et supprimer un hôte.

L'impact du suivi des périphériques sur la liste de contrôle d'accès téléchargeable (DACL) 802.1x est également expliqué.

Le comportement change entre les versions et les plates-formes.

La deuxième partie du document porte sur la liste de contrôle d'accès (ACL) renvoyée par le serveur AAA (Authentication, Authorization, and Accounting) et appliquée à la session 802.1x.

Une comparaison entre la liste de contrôle d’accès DACL, la liste de contrôle d’accès par utilisateur et la liste de contrôle d’accès Filter-ID est présentée.

En outre, certaines mises en garde relatives à la réécriture de la liste de contrôle d’accès et à la liste par défaut sont abordées.

Le suivi des périphériques ajoute une entrée lorsque :

- il apprend la nouvelle entrée via la surveillance DHCP.
- Il apprend la nouvelle entrée via une requête ARP (Address Resolution Protocol) (lit l'adresse MAC de l'expéditeur et l'adresse IP de l'expéditeur à partir du paquet ARP).

Cette fonctionnalité est parfois appelée inspection ARP, mais elle n'est pas la même que l'inspection ARP dynamique (DAI).

Cette fonctionnalité est activée par défaut et ne peut pas être désactivée. Il est également appelé surveillance ARP, mais les débogages ne l'affichent pas après l'activation de la fonction « debug arp snooping ».

La surveillance ARP est activée par défaut et ne peut pas être désactivée ou contrôlée.

L'analyse de périphérique supprime une entrée en l'absence de réponse pour une requête ARP (envoi d'une sonde pour chaque hôte dans la table d'analyse de périphérique, par défaut toutes les 30 secondes).

Configuration du suivi des périphériques

```
ip dhcp excluded-address 192.168.0.1 192.168.0.240
ip dhcp pool POOL
   network 192.168.0.0 255.255.255.0
!
ip dhcp snooping vlan 1
ip dhcp snooping
ip device tracking
!
interface Vlan1
  ip address 192.168.0.2 255.255.255.0
ip route 0.0.0.0 0.0.0.0 10.48.66.1
!
```

```
interface FastEthernet0/1
  description PC
```

Tests de suivi des périphériques

<#root>

```
BSNS-3560-1#
```

show ip dhcp binding

```
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.0.241    0100.5056.994e.a1       Mar 02 1993 02:31 AM    Automatic

BSNS-3560-1#
```

show ip device tracking all

```
IP Device Tracking = Enabled
------------------------------------------------------------
  IP Address     MAC Address       Interface          STATE
------------------------------------------------------------
192.168.0.241   0050.5699.4ea1 FastEthernet0/1        ACTIVE
```

Débogues de la version 12.2.33, suivi de périphérique IP mis à jour par la surveillance DHCP

La surveillance DHCP remplit la table de liaison :

<#root>

```
BSNS-3560-1#
```

show debugging

```
DHCP Snooping packet debugging is on
DHCP Snooping event debugging is on
DHCP server packet debugging is on.
DHCP server event debugging is on.
track:
  IP device-tracking redundancy events debugging is on
  IP device-tracking cache entry Creation debugging is on
  IP device-tracking cache entry Destroy debugging is on
  IP device-tracking cache events debugging is on

02:30:57: DHCP_SNOOPING: checking expired snoop binding entries
02:31:12: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Fa0/1 for pak.  Was Vl1
02:31:12: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Vl1 for pak.  Was Fa0/1
02:31:12: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Fa0/1 for pak.  Was Vl1
```

```
02:31:12:

 DHCP_SNOOPING: received new DHCP packet from input interface

 (FastEthernet0/1)
02:31:12:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPREQUEST, input
 interface: Fa0/1, MAC da: 001f.27e6.cfc0, MAC sa: 0050.5699.4ea1, IP da: 192.168.0.2,
 IP sa: 192.168.0.241, DHCP ciaddr:

 192.168.0.241, DHCP yiaddr: 0.0.0.0,
 DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 0050.5699.4ea1
02:31:12:

 DHCP_SNOOPING: add relay information option

.
02:31:12: DHCP_SNOOPING_SW: Encoding opt82 CID in vlan-mod-port format
02:31:12: DHCP_SNOOPING_SW: Encoding opt82 RID in MAC address format
02:31:12: DHCP_SNOOPING: binary dump of relay info option, length: 20 data&colon;
0x52 0x12 0x1 0x6 0x0 0x4 0x0 0x1 0x1 0x3 0x2 0x8 0x0 0x6 0x0 0x1F 0x27 0xE6 0xCF 0x80
02:31:12: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: 001F.27E6.CFC0,
 packet is flooded to ingress VLAN: (1)
02:31:12: DHCP_SNOOPING_SW: bridge packet send packet to cpu port: Vlan1.
02:31:12:

DHCPD: DHCPREQUEST received from client 0100.5056.994e.a1

.
02:31:12:

DHCPD: Sending DHCPACK to client 0100.5056.994e.a1 (192.168.0.241)

.
02:31:12: DHCPD: unicasting BOOTREPLY to client 0050.5699.4ea1 (192.168.0.241).
02:31:12: DHCP_SNOOPING: received new DHCP packet from input interface (Vlan1)
02:31:12:

DHCP_SNOOPING: process new DHCP packet, message type: DHCPACK

, input interface:
 Vl1, MAC da: 0050.5699.4ea1, MAC sa: 001f.27e6.cfc0, IP da: 192.168.0.241,
 IP sa: 192.168.0.2, DHCP ciaddr: 192.168.0.241, DHCP yiaddr: 192.168.0.241,
 DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0, DHCP chaddr: 0050.5699.4ea1
02:31:12:

DHCP_SNOOPING: add binding on port FastEthernet0/1

.
02:31:12: DHCP_SNOOPING: added entry to table (index 189)
02:31:12: DHCP_SNOOPING: dump binding entry: Mac=00:50:56:99:4E:A1 Ip=192.168.0.241
 Lease=86400     ld Type=dhcp-snooping Vlan=1 If=FastEthernet0/1
```

Une fois la liaison DHCP ajoutée à la base de données, elle déclenche la notification pour le suivi des périphériques :

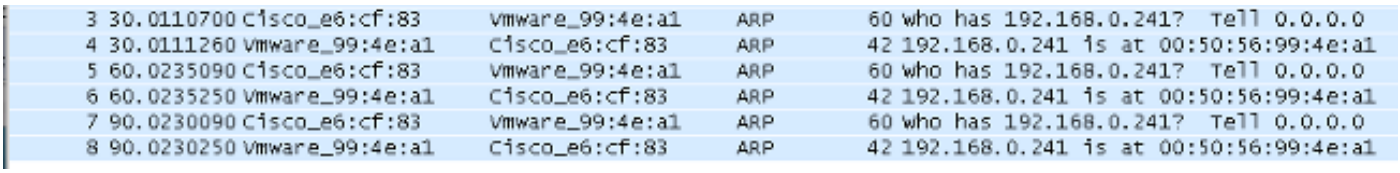
```
<#root>

02:31:12:

sw_host_track-ev:host_track_notification: Add event for host 0050.5699.4ea1,
```

```
 192.168.0.241 on interface FastEthernet0/1


02:31:12: sw_host_track-ev:Async Add event for host 0050.5699.4ea1, 192.168.0.241
 on interface FastEthernet0/1
02:31:12: sw_host_track-ev:MSG = 2
02:31:12: DHCP_SNOOPING_SW no entry found for 0050.5699.4ea1 0.0.0.1 FastEthernet0/1
02:31:12:

DHCP_SNOOPING_SW host tracking not found for update add dynamic
 (192.168.0.241, 0.0.0.0, 0050.5699.4ea1) vlan 1


02:31:12: DHCP_SNOOPING: direct forward dhcp reply to output port: FastEthernet0/1.
02:31:12:

sw_host_track-ev:Add event: 0050.5699.4ea1, 192.168.0.241, FastEthernet0/1


02:31:12: sw_host_track-obj_create:0050.5699.4ea1(192.168.0.241) Cache entry created
02:31:12:

sw_host_track-ev:Activating host 0050.5699.4ea1, 192.168.0.241 on
 interface FastEthernet0/1


02:31:12: sw_host_track-ev:0050.5699.4ea1 Starting cache timer: 30 seconds
```

Les sondes ARP sont envoyées par défaut toutes les 30 secondes :

<#root>

```
02:41:12: sw_host_track-ev:0050.5699.4ea1 Stopping cache timer
02:41:12: sw_host_track-ev:0050.5699.4ea1:

Send Host probe (0)


02:41:12: sw_host_track-ev:0050.5699.4ea1 Starting cache timer: 30 seconds
02:41:42: sw_host_track-ev:0050.5699.4ea1 Stopping cache timer
02:41:42: sw_host_track-ev:0050.5699.4ea1:

Send Host probe (1)


02:41:42: sw_host_track-ev:0050.5699.4ea1 Starting cache timer: 30 seconds
02:42:12: sw_host_track-ev:0050.5699.4ea1 Stopping cache timer
02:42:12: sw_host_track-ev:0050.5699.4ea1:

Send Host probe (2)


02:42:12: sw_host_track-ev:0050.5699.4ea1 Starting cache timer: 30 seconds
02:42:42: sw_host_track-ev:0050.5699.4ea1 Stopping cache timer
02:42:42:

sw_host_track-obj_destroy:0050.5699.4ea1(192.168.0.241): Cache entry deleted


02:42:42: sw_host_track-ev:0050.5699.4ea1 Stopping cache timer
```



3	30.0110700	Cisco_e6:cf:83	Vmware_99:4e:a1	ARP	60 who has 192.168.0.241? Tell 0.0.0.0
4	30.0111260	Vmware_99:4e:a1	Cisco_e6:cf:83	ARP	42 192.168.0.241 is at 00:50:56:99:4e:a1
5	60.0235090	Cisco_e6:cf:83	Vmware_99:4e:a1	ARP	60 who has 192.168.0.241? Tell 0.0.0.0
6	60.0235250	Vmware_99:4e:a1	Cisco_e6:cf:83	ARP	42 192.168.0.241 is at 00:50:56:99:4e:a1
7	90.0230090	Cisco_e6:cf:83	Vmware_99:4e:a1	ARP	60 who has 192.168.0.241? Tell 0.0.0.0
8	90.0230250	Vmware_99:4e:a1	Cisco_e6:cf:83	ARP	42 192.168.0.241 is at 00:50:56:99:4e:a1

Une fois l'entrée supprimée de la table de suivi des périphériques, l'entrée de liaison DHCP correspondante est toujours présente :

```
<#root>

BSNS-3560-1#

show ip device tracking all


IP Device Tracking = Enabled
---------------------------------------------------------------
  IP Address     MAC Address       Interface          STATE
---------------------------------------------------------------

BSNS-3560-1#

show ip dhcp binding


IP address       Client-ID/              Lease expiration        Type
                 Hardware address
192.168.0.241    0100.5056.994e.a1       Mar 02 1993 03:06 AM    Automatic
```

Il y a un problème lorsque vous avez une réponse ARP, mais l'entrée de suivi de périphérique est supprimée quand même.

Ce bogue semble être dans la version 12.2.33 et n'est pas apparu dans la version 12.2.55 ou 15.x du logiciel.

Il existe également des différences lors de la gestion avec le port L2 (access-port) et le port L3 (no switchport).

Sonde et surveillance ARP

Suivi des périphériques avec la fonctionnalité de surveillance ARP :

```
<#root>

BSNS-3560-1#

show debugging


ARP:
  ARP packet debugging is on
Arp Snoop:
  Arp Snooping debugging is on
```

```
03:43:36: sw_host_track-ev:0050.5699.4ea1 Stopping cache timer
03:43:36: sw_host_track-ev:0050.5699.4ea1: Send Host probe (0)
03:43:36:
```

IP ARP: sent req src 0.0.0.0 001f.27e6.cf83,

dst 192.168.0.241 0050.5699.4ea1 FastEthernet0/1

```
03:43:36: sw_host_track-ev:0050.5699.4ea1 Starting cache timer: 30 seconds
03:43:36: IP ARP: rcvd rep src 192.168.0.241 0050.5699.4ea1, dst 0.0.0.0 Vlan1
```

Suivi des périphériques IP pour la version 12.2.55 - Commande masquée

Pour la version 12.2, utilisez une commande masquée afin de l'activer :

<#root>

```
BSNS-3560-1#
```

show ip device tracking all

```
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 2
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0
------------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface                STATE
------------------------------------------------------------------------
192.168.0.244   0050.5699.4ea1  55   FastEthernet0/1          ACTIVE

Total number interfaces enabled: 1
Enabled interfaces:
```

  Fa0/1

```
BSNS-3560-1#
```

ip device tracking interface fa0/48

```
BSNS-3560-1#
```

show ip device tracking all

```
IP Device Tracking = Enabled
IP Device Tracking Probe Count = 2
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0
------------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface                STATE
------------------------------------------------------------------------
10.48.67.87     000c.2978.825d  1006 FastEthernet0/48         ACTIVE
```

```
10.48.67.31     020a.dada.dada  1006 FastEthernet0/48         ACTIVE
10.48.66.245    acf2.c5ed.8171  1006 FastEthernet0/48         ACTIVE
192.168.0.244   0050.5699.4ea1  55   FastEthernet0/1          ACTIVE
10.48.66.193    000c.2997.4ca1  1006 FastEthernet0/48         ACTIVE
10.48.66.186    0050.5699.3431  1006 FastEthernet0/48         ACTIVE

Total number interfaces enabled: 2
Enabled interfaces:

  Fa0/1, Fa0/48
```

Suivi des périphériques IP pour la version 12.2.5 - Exemple d'IP statique

Dans cet exemple, le PC a été configuré avec une adresse IP statique. Les débogages montrent qu'après avoir reçu une réponse ARP (MSG=2), l'entrée de suivi du périphérique est mise à jour.

<#root>

```
01:03:16: sw_host_track-ev:0050.5699.4ea1 Stopping cache timer
01:03:16: sw_host_track-ev:0050.5699.4ea1: Send Host probe (0)
01:03:16: sw_host_track-ev:0050.5699.4ea1 Starting cache timer: 30 seconds
01:03:16: sw_host_track-ev:host_track_notification: Add event for host 0050.5699.4ea1,
 192.168.0.241 on interface FastEthernet0/1, vlan 1
01:03:16: sw_host_track-ev:Async Add event for host 0050.5699.4ea1, 192.168.0.241
 on interface FastEthernet0/1
01:03:16: sw_host_track-ev:

MSG = 2


01:03:16: sw_host_track-ev:Add event: 0050.5699.4ea1, 192.168.0.241, FastEthernet0/1
01:03:16: sw_host_track-ev:

0050.5699.4ea1: Cache entry refreshed


01:03:16: sw_host_track-ev:Activating host 0050.5699.4ea1, 192.168.0.241 on
 interface FastEthernet0/1
01:03:16: sw_host_track-ev:0050.5699.4ea1 Starting cache timer: 30 seconds
```

Ainsi, chaque requête ARP du PC met à jour la table de suivi des périphériques (l'adresse MAC de l'expéditeur et l'adresse IP de l'expéditeur du paquet ARP).

Suivi des périphériques IP pour la version 15.x

Il est important de se rappeler que certaines fonctionnalités telles que DACL pour 802.1x ne sont pas prises en charge dans la version LAN Lite (attention - Cisco Feature Navigator n'affiche pas toujours les informations correctes).

La commande masquée de la version 12.2 peut être exécutée, mais n'a aucun effet. Dans la version 15.x du logiciel, le suivi de périphérique IP (IPDT) par défaut est uniquement activé pour les interfaces pour lesquelles 802.1x est activé :

<#root>

bsns-3750-5#

show ip device tracking all

IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0

  IP Address   MAC Address   Vlan Interface   STATE

192.168.10.12   0007.5032.6941 100 GigabitEthernet1/0/1   ACTIVE
192.168.2.200   000c.29d7.0617 1   GigabitEthernet1/0/1   ACTIVE

Total number interfaces enabled: 2
Enabled interfaces:

Gi1/0/1, Gi1/0/2

bsns-3750-5#

show run int g1/0/3

Building configuration...

Current configuration : 38 bytes
!
interface GigabitEthernet1/0/3

bsns-3750-5(config)#

int g1/0/3

bsns-3750-5(config-if)#

switchport mode access

bsns-3750-5(config-if)#

authentication port-control auto

bsns-3750-5(config-if)#

do show ip device tracking all

IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0

  IP Address   MAC Address   Vlan Interface   STATE

192.168.10.12   0007.5032.6941 100 GigabitEthernet1/0/1   ACTIVE
192.168.2.200   000c.29d7.0617 1   GigabitEthernet1/0/1   ACTIVE

```
Total number interfaces enabled: 3
Enabled interfaces:
  Gi1/0/1, Gi1/0/2,
```

Gi1/0/3

Après la suppression de la configuration 802.1x du port, IPDT est également supprimé de ce port.

L'état du port est peut-être "DOWN", il est donc nécessaire d'avoir "switchport mode access" et "authentication port-control auto" afin d'avoir le suivi de périphérique IP activé sur ce port.

La limite maximale de périphériques d'interface est définie sur 10 :

<#root>

```
bsns-3750-5(config-if)#
```

ip device tracking maximum

```
 ?
  <1-10>  Maximum devices
```

Suivi des périphériques IP pour Cisco IOS-XE®

Là encore, le comportement de Cisco IOS-XE 3.3 a changé par rapport à Cisco IOS Version 15.x.

La commande masquée de la version 12.2 est obsolète, mais maintenant cette erreur est retournée :

<#root>

```
3850-1#
```

no ip device tracking int g1/0/48

```
% Command accepted but obsolete, unreleased or unsupported; see documentation.
```

Dans Cisco IOS-XE, le suivi des périphériques est activé pour toutes les interfaces (même celles pour lesquelles 802.1x n'est pas configuré) :

<#root>

```
3850-1#
```

show ip device tracking all

```
Global IP Device Tracking for clients = Enabled
```

```
Global IP Device Tracking Probe Count = 3
Global IP Device Tracking Probe Interval = 30
Global IP Device Tracking Probe Delay Interval = 0
-------------------------------------------------------------------------------------
  IP Address    MAC Address   Vlan  Interface           Probe-Timeout
   State    Source
-------------------------------------------------------------------------------------
10.48.39.29     000c.29bd.3cfa 1    GigabitEthernet1/0/48  30
   ACTIVE   ARP
10.48.39.28     0016.9dca.e4a7 1    GigabitEthernet1/0/48  30
   ACTIVE   ARP
10.48.76.117    0021.a0ff.5540 1    GigabitEthernet1/0/48  30
   ACTIVE   ARP
10.48.39.21     00c0.9f87.7471 1    GigabitEthernet1/0/48  30
   ACTIVE   ARP
10.48.39.16     0050.5699.1093 1    GigabitEthernet1/0/48  30
   ACTIVE   ARP
10.76.191.247   0024.9769.58cf 20   GigabitEthernet1/0/48  30
   ACTIVE   ARP
192.168.99.4    d48c.b52f.4a1e 99   GigabitEthernet1/0/12  30
   INACTIVE ARP
10.48.39.13     000c.296e.8dbc 1    GigabitEthernet1/0/48  30
   ACTIVE   ARP
10.48.39.15     0050.5699.128d 1    GigabitEthernet1/0/48  30
   ACTIVE   ARP
10.48.39.9      0012.da20.8c00 1    GigabitEthernet1/0/48  30
   ACTIVE   ARP
10.48.39.8      6c20.560e.1b64 1    GigabitEthernet1/0/48  30
   ACTIVE   ARP
10.48.39.11     000c.29e9.db25 1    GigabitEthernet1/0/48  30
   ACTIVE   ARP
10.48.39.5      0014.f15f.f7ca 1    GigabitEthernet1/0/48  30
   ACTIVE   ARP
10.48.39.4      000c.2972.57bc 1    GigabitEthernet1/0/48  30
   ACTIVE   ARP
10.48.39.7      5475.d029.74cf 1    GigabitEthernet1/0/48  30
   ACTIVE   ARP
10.48.76.108    001c.58de.9340 1    GigabitEthernet1/0/48  30
   ACTIVE   ARP
10.48.39.1      0006.f62a.c4a3 1    GigabitEthernet1/0/48  30
   ACTIVE   ARP
10.48.39.3      0050.5699.1bee 1    GigabitEthernet1/0/48  30
   ACTIVE   ARP
10.48.76.84     0015.58c5.e8b7 1    GigabitEthernet1/0/48  30
   ACTIVE   ARP
10.48.39.56     0015.fa13.9a40 1    GigabitEthernet1/0/48  30
   ACTIVE   ARP
10.48.39.59     0050.5699.1bf4 1    GigabitEthernet1/0/48  30
   ACTIVE   ARP
10.48.39.58     000c.2957.c7ad 1    GigabitEthernet1/0/48  30
   ACTIVE   ARP


Total number interfaces enabled: 57
Enabled interfaces:
  Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4, Gi1/0/5, Gi1/0/6, Gi1/0/7,
  Gi1/0/8, Gi1/0/9, Gi1/0/10, Gi1/0/11, Gi1/0/12, Gi1/0/13, Gi1/0/14,
  Gi1/0/15, Gi1/0/16, Gi1/0/17, Gi1/0/18, Gi1/0/19, Gi1/0/20, Gi1/0/21,
  Gi1/0/22, Gi1/0/23, Gi1/0/24, Gi1/0/25, Gi1/0/26, Gi1/0/27, Gi1/0/28,
  Gi1/0/29, Gi1/0/30, Gi1/0/31, Gi1/0/32, Gi1/0/33, Gi1/0/34, Gi1/0/35,
  Gi1/0/36, Gi1/0/37, Gi1/0/38, Gi1/0/39, Gi1/0/40, Gi1/0/41, Gi1/0/42,
  Gi1/0/43, Gi1/0/44, Gi1/0/45, Gi1/0/46, Gi1/0/47,
```

```
Gi1/0/48,

 Gi1/1/1,
  Gi1/1/2, Gi1/1/3, Gi1/1/4, Te1/1/1, Te1/1/2, Te1/1/3, Te1/1/4
3850-1#$

3850-1#sh run int

g1/0/48


Building configuration...

Current configuration : 39 bytes
!
interface GigabitEthernet1/0/48
end

3850-1(config-if)#

ip device tracking maximum

 ?
  <0-65535>  Maximum devices (0 means disabled)
```

En outre, il n'y a pas de limite pour le nombre maximal d'entrées par port (0 signifie désactivé).

Suivi des périphériques IP avec 802.1x et DACL pour la version 12.2.55

Si la norme 802.1x est configurée avec la liste de contrôle d'accès des périphériques, l'entrée de suivi du périphérique est utilisée afin de remplir l'adresse IP du périphérique.

Cet exemple montre le suivi des périphériques fonctionnant pour une adresse IP configurée de manière statique :

```
<#root>

BSNS-3560-1#

show ip device tracking all


IP Device Tracking = Enabled
IP Device Tracking Probe Count = 2
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0
---------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface                STATE
---------------------------------------------------------------------

192.168.0.244

  0050.5699.4ea1  2    FastEthernet0/1          ACTIVE

Total number interfaces enabled: 1
Enabled interfaces:
  Fa0/1
```

Il s'agit d'une session 802.1x créée avec la liste de contrôle d'accès DACL « permit icmp any any any » :

<#root>

```
BSNS-3560-1#

sh authentication sessions  interface fa0/1


           Interface:  FastEthernet0/1
         MAC Address:  0050.5699.4ea1


 IP Address:  192.168.0.244


           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  2


    ACS ACL:  xACSACLx-IP-DACL-516c2694


      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3042A900000008008900C5
      Acct Session ID:  0x0000000D
               Handle:  0x19000008

Runnable methods list:
       Method   State
       dot1x    Authc Success
```

<#root>

```
BSNS-3560-1#

show epm session summary


EPM Session Information
-----------------------
Total sessions seen so far : 1
Total active sessions      : 1

Interface               IP Address        MAC Address     Audit Session Id:
-----------------------------------------------------------------------------
FastEthernet0/1         192.168.0.244     0050.5699.4ea1   0A3042A900000008008900C5
```

Voici une liste de contrôle d’accès appliquée :

<#root>

```
 BSNS-3560-1#

show ip access-lists


Extended IP access list Auth-Default-ACL
    10 permit udp any range bootps 65347 any range bootpc 65348
    20 permit udp any any range bootps 65347
    30 deny ip any any (8 matches)

Extended IP access list xACSACLx-IP-DACL-516c2694 (per-user)


    10 permit icmp any any (6 matches)
```

En outre, la liste de contrôle d’accès sur l’interface fa0/1 est identique :

<#root>

```
BSNS-3560-1#

show ip access-lists interface fa0/1


     permit icmp any any
```

Même si la valeur par défaut est dot1x ACL :

<#root>

```
BSNS-3560-1#

show ip interface fa0/1


FastEthernet0/1 is up, line protocol is up
  Inbound  access list is Auth-Default-ACL
```

La liste de contrôle d’accès devrait utiliser « any » comme 192.168.0.244. Cela fonctionne comme ceci pour le proxy d'authentification, mais pour la DACL 802.1x src "any" n'est pas changé en l'IP détectée du PC.

Pour le proxy auth, une liste de contrôle d'accès d'origine de l'ACS est mise en cache et affichée avec la commande show ip access-list et une liste de contrôle d'accès spécifique (par utilisateur avec une adresse IP spécifique) est appliquée sur l'interface avec la commande show ip access-list interface fa0/1. Cependant, auth-proxy n'utilise pas le suivi IP du périphérique.

Que faire si l'adresse IP n'est pas détectée correctement ? Après la désactivation du suivi des périphériques :

<#root>

```
BSNS-3560-1#
show authentication sessions interface fa0/1


            Interface:  FastEthernet0/1
          MAC Address:  0050.5699.4ea1


 IP Address:  Unknown


            User-Name:  cisco
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  2


ACS ACL:  xACSACLx-IP-DACL-516c2694


      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3042A9000000000000C775
      Acct Session ID:  0x00000001
               Handle:  0xB0000000

Runnable methods list:
       Method   State
       dot1x    Authc Success
```

Aucune adresse IP n'est donc attachée, mais la liste de contrôle d'accès est toujours appliquée :

<#root>

```
BSNS-3560-1#
show ip access-lists


Extended IP access list Auth-Default-ACL
    10 permit udp any range bootps 65347 any range bootpc 65348
    20 permit udp any any range bootps 65347
    30 deny ip any any (4 matches)
Extended IP access list
 xACSACLx-IP-DACL-516c2694 (per-user)
```

```
    10 permit icmp any any
```

Dans ce scénario, le suivi des périphériques pour 802.1x n'est pas requis. La seule différence est que la connaissance préalable de l'adresse IP du client peut être utilisée pour une requête d'accès RADIUS. Une fois l'attribut 8 joint :

```
radius-server attribute 8 include-in-access-req
```

Il existe dans Access-Request et sur ACS il est possible de créer des règles d'autorisation plus granulaires :

```
00:17:44: RADIUS(00000001): Send Access-Request to 10.48.66.185:1645 id 1645/27, len 257
00:17:44: RADIUS:  authenticator F8 17 06 CE C1 85 E8 E8 - CB 5B 57 96 6C 07 CE CA
00:17:44: RADIUS:  User-Name           [1]   7   "cisco"
00:17:44: RADIUS:  Service-Type        [6]   6   Framed                    [2]
00:17:44: RADIUS:  Framed-IP-Address   [8]   6   192.168.0.244
```

N'oubliez pas que TrustSec a également besoin du suivi des périphériques IP pour les liaisons IP à SGT.

Suivi des périphériques IP avec 802.1x et DACL pour la version 15.x

Quelle est la différence entre la version 15.x et la version 12.2.55 dans la liste de contrôle d'accès DACL ? Dans le logiciel Version15.x, il fonctionne de la même manière que pour auth-proxy.

La liste de contrôle d'accès générique peut être vue quand la commande show ip access-list est entrée (réponse mise en cache depuis AAA), mais après la commande show ip access-list interface fa0/1, la commande src "any" est remplacée par l'adresse IP source de l'hôte (connue via le suivi de périphérique IP).

Voici l'exemple d'un téléphone et d'un PC sur un port (g1/0/1), version logicielle 15.0.2SE2 sur 3750X :

<#root>

```
bsns-3750-5#sh authentication sessions interface g1/0/1

            Interface:  GigabitEthernet1/0/1
          MAC Address:

 0007.5032.6941

           IP Address:
```

192.168.10.12

```
            User-Name:  00-07-50-32-69-41
               Status:  Authz Success
               Domain:
```

VOICE

```
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:
```

100

```
              ACS ACL:
```

xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2

```
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A800010000001012B680D23
      Acct Session ID:  0x0000017B
               Handle:  0x99000102

Runnable methods list:
       Method   State
       dot1x    Failed over
```

mab

Authc Success

```
----------------------------------------
            Interface:  GigabitEthernet1/0/1
          MAC Address:
```

0050.5699.4ea1

```
           IP Address:
```

192.168.2.200

```
            User-Name:
```

cisco

```
               Status:  Authz Success
               Domain:
```

DATA

```
      Security Policy:  Should Secure
      Security Status:  Unsecure
```

```
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:

 20


              ACS ACL:

xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2


      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A80001000001BD336EC4D6
      Acct Session ID:  0x000002F9
               Handle:  0xF80001BE


Runnable methods list:
       Method   State


  dot1x    Authc Success


       mab      Not run
```

Le téléphone est authentifié via MAC Authentication Bypass (MAB), tandis que le PC utilise dot1x. Le téléphone et le PC utilisent la même liste de contrôle d'accès :

```
<#root>

bsns-3750-5#

show ip access-lists xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2


Extended IP access list xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2 (

per-user

)
    10

permit ip any any
```

Cependant, lorsqu'elle est vérifiée au niveau de l'interface, la source a été remplacée par l'adresse IP du périphérique.

Le suivi des périphériques IP déclenche cette modification et peut se produire à tout moment (bien après la session d'authentification et le téléchargement de la liste de contrôle d'accès) :

```
<#root>
```

```
bsns-3750-5#
show ip access-lists interface g1/0/1

     permit ip
host 192.168.2.200
 any (5 matches)
     permit ip
host 192.168.10.12
 any
```

Les deux adresses MAC sont marquées comme statiques :

```
<#root>
bsns-3750-5#
sh mac address-table interface g1/0/1

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  20    0050.5699.4ea1
 STATIC
      Gi1/0/1
 100    0007.5032.6941
 STATIC
      Gi1/0/1
```

Entrée ACL spécifique

Quand la source « any » de la liste de contrôle d'accès est-elle remplacée par l'adresse IP de l'hôte ? Uniquement lorsqu'il y a au moins deux sessions sur le même port (deux demandeurs).

Il n'est pas nécessaire de remplacer la source « any » lorsqu'il n'y a qu'une seule session.

Les problèmes apparaissent lorsqu'il y a plusieurs sessions et que tous les périphériques IP ne connaissent pas l'adresse IP de l'hôte. Dans ce scénario, il est toujours « any » pour certaines entrées.

Ce comportement est différent sur certaines plates-formes. Par exemple, sur le 2960X avec la version 15.0(2)EX, la liste de contrôle d'accès est toujours spécifique, même lorsqu'il n'y a qu'une seule session d'authentification par port.

Cependant, pour les versions 3560X et 3750X 15.0(2)SE, vous devez disposer d'au moins deux sessions pour rendre cette liste spécifique.

Direction De Contrôle

Par défaut, control-direction est de type both :

```
<#root>

bsns-3750-5(config)#

int g1/0/1


bsns-3750-5(config-if)#

authentication control-direction ?


  both  Control traffic in BOTH directions
  in    Control inbound traffic only

bsns-3750-5(config-if)#

authentication control-direction both
```

Cela signifie qu'avant l'authentification du demandeur, le trafic ne peut pas être envoyé vers ou depuis le port. En mode « in », le trafic aurait pu être envoyé d'un port à un demandeur, mais pas d'un demandeur au port (ce qui pourrait être utile pour la fonctionnalité WAKE sur LAN).

Cependant, le commutateur applique la liste de contrôle d'accès uniquement dans la direction « in ». Peu importe le mode utilisé.

```
<#root>

bsns-3750-5#

sh ip access-lists interface g1/0/1 out



bsns-3750-5#

sh ip access-lists interface g1/0/1 in


     permit ip host 192.168.2.200 any
     permit ip host 192.168.10.12 any
```

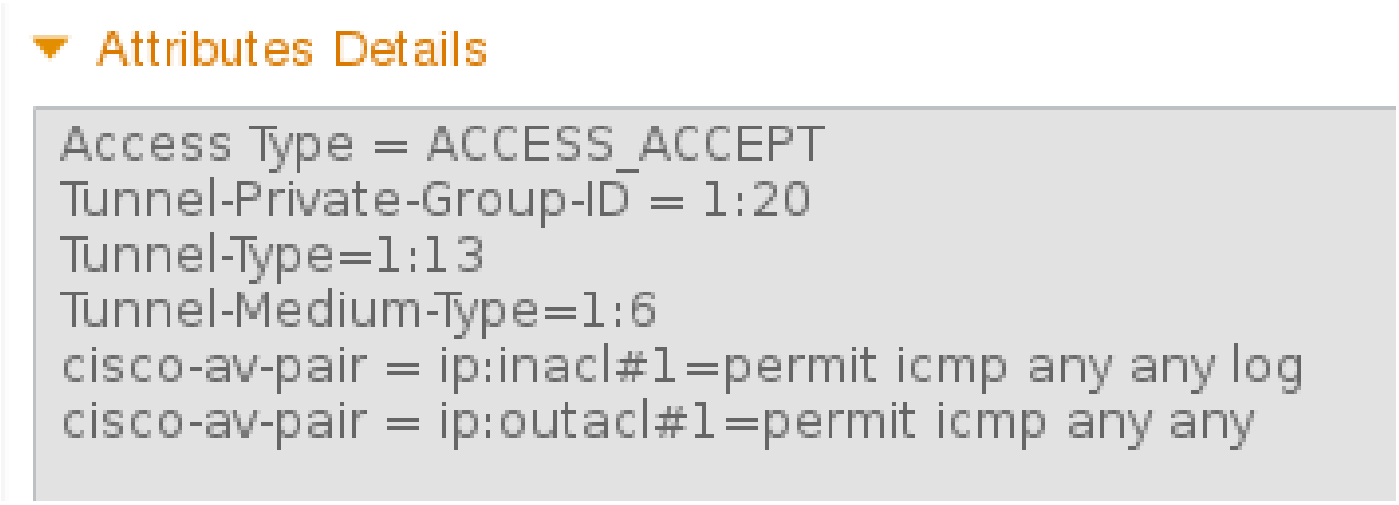
Cela signifie essentiellement qu'après l'authentification, la liste de contrôle d'accès est appliquée

pour le trafic vers le port (dans la direction) et tout le trafic est autorisé à partir du port (dans la direction).

Suivi des périphériques IP avec 802.1x et ACL par utilisateur pour la version 15.x

Il est également possible d'utiliser une liste de contrôle d'accès par utilisateur qui est passée dans cisco-av-pair « ip : inacl » et « ip : outacl ».

Cet exemple de configuration est similaire à une configuration précédente, mais cette fois, le téléphone utilise la liste de contrôle d'accès DACL et le PC utilise la liste de contrôle d'accès par utilisateur. Le profil ISE du PC est le suivant :



La DACL est toujours appliquée sur le téléphone :

<#root>

bsns-3750-5#

show authentication sessions interface g1/0/1

```
            Interface:  GigabitEthernet1/0/1
          MAC Address:  0007.5032.6941
           IP Address:
```

192.168.10.12

```
            User-Name:  00-07-50-32-69-41
               Status:  Authz Success
               Domain:
```

VOICE

```
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  100
             ACS ACL:
```

xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2

```
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A800100000568431143D8
      Acct Session ID:  0x000006D2
               Handle:  0x84000569

Runnable methods list:
       Method   State
       dot1x    Failed over
       mab      Authc Success

bsns-3750-5#
```

sh ip access-lists xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2

```
Extended IP access list xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2 (per-user)
    10
```

permit ip any any

Cependant, le PC sur le même port utilise la liste de contrôle d'accès par utilisateur :

<#root>

```
    Interface:  GigabitEthernet1/0/1
          MAC Address:  0050.5699.4ea1
           IP Address:
```

192.168.2.200

```
            User-Name:  cisco
               Status:  Authz Success
               Domain:
```

DATA

```
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  20
```

Per-User ACL: permit icmp any any log

```
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A80001000005674311400B
      Acct Session ID:  0x000006D1
               Handle:  0x9D000568
```

Afin de vérifier comment il est fusionné sur le port gig1/0/1 :

<#root>

```
bsns-3750-5#
```

show ip access-lists interface g1/0/1

```
     permit icmp host 192.168.2.200 any log
     permit ip host 192.168.10.12 any
```

La première entrée provient de la liste de contrôle d'accès par utilisateur (notez le mot clé log) et la seconde est tirée de la liste de contrôle d'accès.

Les deux sont réécrits par le suivi de périphérique IP pour l'adresse IP spécifique.

La liste de contrôle d'accès par utilisateur a pu être vérifiée avec la commande debug epm all :

<#root>

```
Apr 12 02:30:13.489: EPM_SESS_EVENT:
```

IP Per-User ACE: permit icmp any any log received

```
Apr 12 02:30:13.489: EPM_SESS_EVENT:Recieved string
```

GigabitEthernet1/0/1#IP#7844C6C

```
Apr 12 02:30:13.489: EPM_SESS_EVENT:Add ACE [permit icmp any any log] to ACL
 [GigabitEthernet1/0/1#IP#7844C6C]
Apr 12 02:30:13.497: EPM_SESS_EVENT:Executed [ip access-list extended
 GigabitEthernet1/0/1#IP#7844C6C] command through parse_cmd. Result= 0
Apr 12 02:30:13.497: EPM_SESS_EVENT:Executed [permit icmp any any log]
 command through parse_cmd. Result= 0
Apr 12 02:30:13.497: EPM_SESS_EVENT:Executed [end] command through
 parse_cmd. Result= 0
Apr 12 02:30:13.497: EPM_SESS_EVENT:
```

Notifying PD regarding Policy (NAMED ACL)
application on the interface GigabitEthernet1/0/1

Et aussi via la commande show ip access-lists :

<#root>

```
bsns-3750-5#
```

show ip access-lists

```
Extended IP access list GigabitEthernet1/0/1#IP#7844C6C (per-user)
```

```
10 permit icmp any any log
```

Qu'en est-il de l'attribut ip : outacl ? Il est complètement omis dans la version 15.x. L'attribut a été reçu, mais le commutateur n'applique/ne traite pas cet attribut.

Différence par rapport à la DACL

Comme indiqué dans l'ID de bogue Cisco CSCut25702, la liste de contrôle d'accès par utilisateur se comporte différemment de la liste DACL.

Une liste de contrôle d'accès numérique avec une seule entrée (« permit ip any any any ») et un demandeur connecté à un port peut fonctionner correctement sans que le suivi de périphérique IP soit activé.

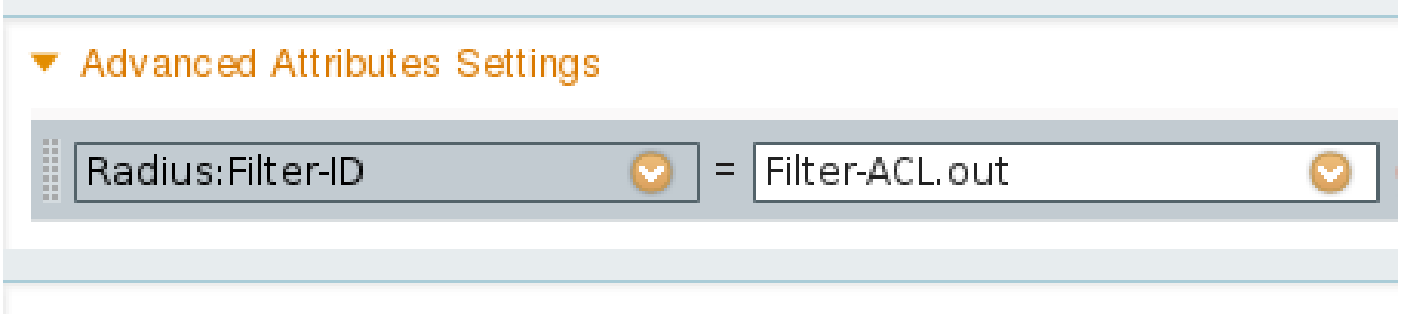
L'argument « any » n'est pas remplacé et tout le trafic est autorisé. Toutefois, pour la liste de contrôle d'accès par utilisateur, le suivi des périphériques IP doit obligatoirement être activé.

Si elle est désactivée et qu'elle comporte uniquement l'entrée « permit ip any any » et un demandeur, tout le trafic est bloqué.

Suivi des périphériques IP avec 802.1x et ACL Filter-ID pour la version 15.x

L'attribut IETF id_filtre [11] peut également être utilisé. Le serveur AAA renvoie le nom de la liste de contrôle d'accès, qui est définie localement sur le commutateur. Le profil ISE peut ressembler à ceci :

Notez que vous devez spécifier la direction (entrée ou sortie). Pour cela, il est nécessaire d'ajouter l'attribut manuellement :



Ensuite, le débogage montre :

<#root>

debug epm all

```
Apr 12 23:41:05.170: EPM_SESS_EVENT:Filter-Id :
```

Filter-ACL received

```
Apr 12 23:41:05.170: EPM_SESS_EVENT:Notifying PD regarding Policy (NAMED ACL)
 application on the interface GigabitEthernet1/0/1
```

Cette liste de contrôle d'accès est également affichée pour la session authentifiée :

<#root>

```
bsns-3750-5#
```

show authentication sessions interface g1/0/1

```
            Interface:  GigabitEthernet1/0/1
          MAC Address:  0050.5699.4ea1
           IP Address:  192.168.2.200
            User-Name:  cisco
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  20

 Filter-Id:  Filter-ACL

      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  C0A800010000059E47B77481
      Acct Session ID:  0x00000733
```

```
               Handle:  0x5E00059F


Runnable methods list:
       Method   State
       dot1x
```

Authc Success

```
       mab      Not run
```

Et, lorsque la liste de contrôle d’accès est liée à l’interface :

<#root>

```
bsns-3750-5#
```

show ip access-lists interface g1/0/1

```
     permit icmp host 192.168.2.200 any log
     permit tcp host 192.168.2.200 any log
```

Notez que cette liste de contrôle d’accès peut être fusionnée avec d’autres types de listes de contrôle d’accès sur la même interface. Par exemple, si vous avez sur le même port de commutateur un autre demandeur qui obtient la DACL d'ISE : « permit ip any any », vous pouvez voir :

<#root>

```
bsns-3750-5#
```

show ip access-lists interface g1/0/1

```
     permit icmp host 192.168.2.200 any log
     permit tcp host 192.168.2.200 any log
     permit ip host 192.168.10.12 any
```

Notez que le suivi du périphérique IP réécrit l'adresse IP source pour chaque source (demandeur).

Qu'en est-il de la liste de filtres « out » ? Encore une fois (en tant que liste de contrôle d’accès par utilisateur), elle n’est pas utilisée par le commutateur.

Suivi des périphériques IP - Valeurs par défaut et bonnes pratiques

Pour les versions antérieures à 15.2(1)E, avant qu'une fonctionnalité puisse utiliser IPDT, elle doit d'abord être activée globalement avec cette commande CLI :

<#root>

```
(config)#
```

ip device tracking

Pour les versions 15.2(1)E et ultérieures, la commande ip device tracking n'est plus nécessaire. IPDT n'est activé que si une fonctionnalité qui en dépend l'active.

Si aucune fonction n'active IPDT, IPDT est désactivé. La commande « no ip device tracking » n'a aucun effet. La fonctionnalité spécifique a le contrôle d'activer/désactiver IPDT.

Lorsque vous activez IPDT, vous devez vous souvenir du problème de « adresse IP dupliquée » sur . Consultez Dépannage des messages d'erreur « Duplicate IP Address 0.0.0.0 » pour plus d'informations.

Il est recommandé de désactiver IPDT sur un port agrégé :

<#root>

```
(config-if)#
```

no ip device tracking

Sur la version ultérieure de Cisco IOS, il s'agit d'une commande différente :

<#root>

```
(config-if)#
```

ip device tracking maximum 0

Il est recommandé d'activer IPDT sur le port d'accès et de retarder les sondes ARP afin d'éviter le problème « adresse IP dupliquée » :

<#root>

```
(config-if)#
```

ip device tracking probe delay 10

Interface ACL Rewrite pour la version 15.x

Pour l'ACL d'interface, elle fonctionne avant l'authentification :

```
<#root>

interface GigabitEthernet1/0/2
 description windows7
 switchport mode access

 ip access-group test1 in


 authentication order mab dot1x
 authentication port-control auto
 mab
 dot1x pae authenticator
end

bsns-3750-5#

show ip access-lists test1


Extended IP access list test1
    10 permit tcp any any log-input
```

Cependant, une fois l'authentification réussie, la liste de contrôle d'accès retournée par le serveur AAA la réécrit (en remplacement) (peu importe s'il s'agit de DACL, ip : inacl ou filterid).

Cette liste de contrôle d'accès (test1) peut bloquer le trafic (qui serait normalement autorisé en mode ouvert), mais après l'authentification, n'a plus d'importance.

Même si aucune liste de contrôle d'accès n'est renvoyée par le serveur AAA, la liste de contrôle d'accès de l'interface est écrasée et un accès complet est fourni.

Cela est un peu trompeur puisque la TCAM (Ternary Content Addressable Memory) indique que la liste de contrôle d'accès est toujours liée au niveau de l'interface.

Voici un exemple de la version 15.2.2 sur 3750X :

```
<#root>

bsns-3750-6#

show platform acl portlabels interface g1/0/2


Port based ACL: (asic 1)
---------------------------
  Input Label:  5    Op Select Index: 255
    Interface(s): Gi1/0/2
    Access Group:

test1

, 4 VMRs
    Ip Portal: 0 VMRs
    IP Source Guard: 0 VMRs
    LPIP: 0 VMRs
    AUTH: 0 VMRs
```

```
    C3PLACL: 0 VMRs
    MAC Access Group: (none), 0 VMRs
```

Ces informations ne sont valides que pour le niveau interface et non pour le niveau session. D'autres informations (présente une liste de contrôle d'accès composée) peuvent être déduites de :

<#root>

bsns-3750-6#

show ip access-lists interface g1/0/2

permit ip host 192.168.1.203 any

Extended IP access list

test1

10 permit icmp host x.x.x.x host n.n.n.n

La première entrée est créée en tant que DACL « permit ip any any » renvoyée pour une authentification réussie (et « any » est remplacé par une entrée de la table de suivi des périphériques).

La deuxième entrée est le résultat de la liste de contrôle d'accès de l'interface et est appliquée à toutes les nouvelles authentifications (avant l'autorisation).

Malheureusement, les deux listes de contrôle d'accès sont concaténées (elles dépendent de la plate-forme). Cela se produit sur la version 15.2.2 sur 3750X.

Cela signifie que pour les sessions autorisées, les deux sont appliquées. Tout d'abord la DACL et ensuite l'ACL d'interface.

C'est pourquoi lorsque vous ajoutez « deny ip any any any » explicite, la liste de contrôle d'accès ne prend pas en compte la liste de contrôle d'accès de l'interface.

En général, il n'y a pas de refus explicite dans la DACL, puis la liste de contrôle d'accès de l'interface est appliquée.

Le comportement pour la version 15.0.2 sur 3750X est le même, mais la commande sh ip access-list interface n'affiche plus la liste de contrôle d'accès d'interface (mais elle est toujours concaténée avec la liste de contrôle d'accès d'interface sauf si un refus explicite existe dans la liste de contrôle d'accès d'interface).

ACL par défaut utilisée pour 802.1x

Il existe deux types de listes de contrôle d’accès par défaut :

- auth-default-ACL-OPEN - utilisé pour le mode ouvert
- auth-default-ACL : utilisée pour l'accès fermé

Les listes de contrôle d'accès auth-default-ACL et auth-default-ACL-OPEN sont toutes deux utilisées lorsque le port est à l'état non autorisé. Par défaut, l'accès fermé est utilisé.

Cela signifie qu'avant l'authentification, tout le trafic est abandonné, sauf celui autorisé par la liste de contrôle d'accès auth-default-ACL.

De cette manière, le trafic DHCP est autorisé avant l'autorisation.

L’adresse IP est attribuée et la liste de contrôle d’accès numérique téléchargée peut être correctement appliquée.

Cette liste de contrôle d’accès est créée automatiquement et est introuvable dans la configuration.

<#root>

```
bsns-3750-5#
sh run | i Auth-Default


bsns-3750-5#
sh ip access-lists Auth-Default-ACL

Extended IP access list
Auth-Default-ACL
    10 permit udp any range bootps 65347 any range bootpc 65348 (22 matches)
    20 permit udp any any range bootps 65347 (12 matches)
    30 deny ip any any
```

Il est créé dynamiquement pour la première authentification (entre la phase d'authentification et la phase d'autorisation) et supprimé après la dernière session.

Auth-Default-ACL autorise uniquement le trafic DHCP. Une fois l'authentification réussie et la nouvelle DACL téléchargée, elle est appliquée à cette session.

Lorsque le mode est modifié pour ouvrir auth-default-ACL-OPEN apparaît et qu'il est utilisé et fonctionne exactement de la même manière que Auth-Default-ACL :

<#root>

```
bsns-3750-5(config)#int g1/0/2
bsns-3750-5(config-if)#authentication open

bsns-3750-5#
```

show ip access-lists

```
Extended IP access list
```

Auth-Default-ACL-OPEN

```
    10 permit ip any any
```

Les deux listes de contrôle d'accès peuvent être personnalisées, mais elles ne sont jamais visibles dans la configuration.

<#root>

```
bsns-3750-5(config)#
```

ip access-list extended Auth-Default-ACL

```
bsns-3750-5(config-ext-nacl)#permit udp any any

bsns-3750-5#
```

sh ip access-lists

```
Extended IP access list Auth-Default-ACL
    10 permit udp any range bootps 65347 any range bootpc 65348 (22 matches)
    20 permit udp any any range bootps 65347 (16 matches)
    30 deny ip any any
    40 permit udp any any

bsns-3750-5#
```

sh run | i Auth-Def

```
bsns-3750-5#
```

Mode ouvert

La section précédente décrivait le comportement des listes de contrôle d'accès (y compris celle utilisée par défaut pour le mode ouvert). Le comportement du mode ouvert est le suivant :

- elle autorise tout le trafic (selon la commande auth-default-ACL-OPEN par défaut) lorsque la session est dans un état non autorisé.
- la session est dans un état non autorisé pendant l'authentification/l'autorisation (valable pour

les scénarios d'amorçage PXE (Encryption Appliance Model E)) ou après l'échec de ce processus (valable pour les scénarios appelés « mode à faible impact »).
- lorsque la session passe à l’état autorisé pour plusieurs plates-formes, les listes de contrôle d’accès sont concaténées et la première liste de contrôle d’accès est utilisée, puis la liste de contrôle d’accès d’interface.
- dans le cas d’une authentification ou d’un domaine multiples, il est possible que plusieurs sessions se déroulent simultanément dans des états différents (le type de liste de contrôle d’accès différent s’applique alors à chaque session).

Lorsque la liste de contrôle d’accès interface est obligatoire

Pour plusieurs plates-formes 6500/4500, la liste de contrôle d’accès d’interface est obligatoire afin d’appliquer correctement la liste de contrôle d’accès.

Voici un exemple avec 4500 sup2 12.2.53SG6, sans ACL d’interface :

<#root>

```
brisk#
```

show run int g2/3

```
!
interface GigabitEthernet2/3
 switchport mode access
 switchport voice vlan 10
 authentication host-mode multi-auth
 authentication open
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 mab
```

Une fois l’hôte authentifié, la liste de contrôle d’accès est téléchargée. Elle n'est pas appliquée et l'autorisation échoue.

<#root>

```
*Apr 25 04:38:05.239: RADIUS: Received from id 1645/19 10.48.66.74:1645,
```

Access-Accept,

```
 len 209
*Apr 25 04:38:05.239: RADIUS:  authenticator 35 8E 59 E4 D5 CF 8F 9A -
 EE 1C FC 5A 9F 67 99 B2
*Apr 25 04:38:05.239: RADIUS:  User-Name           [1]   41
  "
```

#ACSACL#-IP-PERMIT_ALL_TRAFFIC-51ef7db1

```
"
```

```
*Apr 25 04:38:05.239: RADIUS:  State               [24]  40
*Apr 25 04:38:05.239: RADIUS:   52 65 61 75 74 68 53 65 73 73 69 6F 6E 3A 30 61
  [ReauthSession:0a]
*Apr 25 04:38:05.239: RADIUS:   33 30 34 32 34 61 30 30 30 45 46 35 30 46 35 33
  [30424a000EF50F53]
*Apr 25 04:38:05.239: RADIUS:   35 41 36 36 39 33            [ 5A6693]
*Apr 25 04:38:05.239: RADIUS:  Class               [25]  54
*Apr 25 04:38:05.239: RADIUS:   43 41 43 53 3A 30 61 33 30 34 32 34 61 30 30 30
  [CACS:0a30424a000]
*Apr 25 04:38:05.239: RADIUS:   45 46 35 30 46 35 33 35 41 36 36 39 33 3A 69 73
  [EF50F535A6693:is]
*Apr 25 04:38:05.239: RADIUS:   65 32 2F 31 38 30 32 36 39 35 33 38 2F 31 32 38
  [e2/180269538/128]
*Apr 25 04:38:05.239: RADIUS:   36 35 35 33              [ 6553]
*Apr 25 04:38:05.239: RADIUS:  Message-Authenticato[80]  18
*Apr 25 04:38:05.239: RADIUS:   AF 47 E2 20 65 2F 59 39 72 9A 61 5C C5 8B ED F5
         [ G e/Y9ra\]
*Apr 25 04:38:05.239: RADIUS:  Vendor, Cisco       [26]  36
*Apr 25 04:38:05.239: RADIUS:   Cisco AVpair       [1]   30
  "
```

ip:inacl#1=permit ip any any

```
"
*Apr 25 04:38:05.239: RADIUS(00000000): Received from id 1645/19
*Apr 25 04:38:05.247:
```

EPM_SESS_ERR:Failed to apply ACL to interface

```
*Apr 25 04:38:05.247: EPM_API:In function epm_send_message_to_client
*Apr 25 04:38:05.247: EPM_SESS_EVENT:Sending response message to process
 AUTH POLICY Framework
*Apr 25 04:38:05.247: EPM_SESS_EVENT:Returning feature config
*Apr 25 04:38:05.247: EPM_API:In function epm_acl_feature_free
*Apr 25 04:38:05.247: EPM_API:In function epm_policy_aaa_response
*Apr 25 04:38:05.247: EPM_FSM_EVENT:Event epm_ip_wait_event state changed from
 policy-apply to ip-wait
*Apr 25 04:38:05.247: EPM_API:In function epm_session_action_ip_wait
*Apr 25 04:38:05.247: EPM_API:In function epm_send_ipwait_message_to_client
*Apr 25 04:38:05.247: EPM_SESS_ERR:NULL feature list for client ctx 1B2694B0
 for type DOT1X
*Apr 25 04:38:05.247:
```

%AUTHMGR-5-FAIL: Authorization failed for client
(0007.5032.6941) on Interface Gi2/3
AuditSessionID 0A304345000000060012C050

```
brisk#
```

show authentication sessions

```
Interface  MAC Address     Method   Domain   Status         Session ID
Gi2/3      0007.5032.6941  mab      VOICE
```

Authz Failed

```
   0A304345000000060012C050
```

Une fois la liste de contrôle d'accès interface ajoutée :

```
<#root>

brisk#

show ip access-lists all


Extended IP access list all
    10 permit ip any any (63 matches)

brisk#sh run int g2/3
!
interface GigabitEthernet2/3
 switchport mode access
 switchport voice vlan 10

 ip access-group all in


 authentication host-mode multi-auth
 authentication open
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 mab
```

L'authentification et l'autorisation réussissent et la liste de contrôle d'accès est appliquée correctement :

```
<#root>

brisk#

show authentication sessions



Interface  MAC Address     Method   Domain   Status         Session ID
Gi2/3      0007.5032.6941  mab      VOICE

 Authz Success

  0A30434500000008001A2CE4
```

Le comportement ne dépend pas de « authentication open ». Afin d'accepter la DACL, vous avez besoin de l'ACL d'interface pour le mode ouvert/fermé.

DACL sur 4500/6500

Sur les modèles 4500/6500, la liste de contrôle d'accès est appliquée avec les listes de contrôle d'accès acl_snoop. Un exemple avec 4500 sup2 12.2.53SG6 (téléphone + PC) est montré ici. Il

existe une liste de contrôle d’accès distincte pour les VLAN voix (10) et données (100) :

```
<#root>

brisk#

show ip access-lists


Extended IP access list

acl_snoop_Gi2/3_10


    10 permit ip host

 192.168.2.200

 any
    20 deny ip any any
Extended IP access list

acl_snoop_Gi2/3_100


    10 permit ip host

192.168.10.12

 any
    20 deny ip any any
```

Les listes de contrôle d'accès sont spécifiques car IPDT possède les entrées correctes :

```
<#root>

brisk#

show ip device tracking all


IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
IP Device Tracking Probe Delay Interval = 0
-----------------------------------------------------------------------
  IP Address     MAC Address   Vlan  Interface              STATE
-----------------------------------------------------------------------

192.168.10.12

  0007.5032.6941

100

  GigabitEthernet2/3     ACTIVE

192.168.2.200

  000c.29d7.0617
```

```
10

   GigabitEthernet2/3     ACTIVE
```

Les sessions authentifiées confirment les adresses :

```
<#root>

brisk#

show authentication sessions int g2/3


            Interface:  GigabitEthernet2/3
          MAC Address:  000c.29d7.0617
           IP Address:

192.168.2.200


            User-Name:  00-0C-29-D7-06-17
               Status:  Authz Success
               Domain:  VOICE
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3043450000003003258E0C
      Acct Session ID:  0x00000034
               Handle:  0x54000030

Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run

----------------------------------------
            Interface:  GigabitEthernet2/3
          MAC Address:  0007.5032.6941
           IP Address:

192.168.10.12


            User-Name:  00-07-50-32-69-41
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3043450000002E031D1DB8
      Acct Session ID:  0x00000032
               Handle:  0x4A00002E

Runnable methods list:
```

```
       Method   State
       mab      Authc Success
       dot1x    Not run
```

À ce stade, le PC et le téléphone répondent à l'écho ICMP, mais la liste de contrôle d'accès de l'interface présente uniquement :

<#root>

```
brisk#show ip access-lists interface g2/3
     permit ip host
```

192.168.10.12

```
 any
```

Pourquoi ? Parce que la DACL a été diffusée uniquement pour le téléphone (192.168.10.12). Pour le PC, la liste de contrôle d'accès d'interface avec le mode ouvert est utilisée :

<#root>

```
interface GigabitEthernet2/3
 ip access-group all in
 authentication open

brisk#
```

show ip access-lists all

```
Extended IP access list all
    10 permit ip any any (73 matches)
```

En résumé, acl_snoop est créé pour le PC et le téléphone, mais la DACL est renvoyée uniquement pour le téléphone. C'est pourquoi cette liste de contrôle d'accès est considérée comme liée à l'interface.

État de l'adresse MAC pour 802.1x

Lorsque l'authentification 802.1x démarre, l'adresse MAC est toujours considérée comme DYNAMIQUE, mais l'action pour ce paquet est DROP :

<#root>

```
bsns-3750-5#
```

show authentication sessions

```
Interface  MAC Address     Method   Domain   Status         Session ID
Gi1/0/1
```

0007.5032.6941

```
  dot1x    UNKNOWN
```

Running

```
     C0A8000100000596479F4DCE

bsns-3750-5#
```

show mac address-table interface g1/0/1

```
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 100
```

0007.5032.6941   DYNAMIC   Drop

```
Total Mac Addresses for this criterion: 1
```

Une fois l'authentification réussie, l'adresse MAC devient statique et le numéro de port est fourni :

<#root>

```
bsns-3750-5#
```

show authentication sessions

```
Interface  MAC Address     Method   Domain   Status         Session ID
Gi1/0/1
```

0007.5032.6941

```
  mab      VOICE
```

Authz Success

```
  C0A8000100000596479F4DCE

bsns-3750-5#
```

show mac address-table interface g1/0/1

```
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 100
```

0007.5032.6941   STATIC   Gi1/0/1

Cela est vrai pour toutes les sessions mab/dot1x pour les deux domaines (VOIX/DONNÉES).

Dépannage

N'oubliez pas de lire le guide de configuration 802.1x correspondant à la version et à la plate-forme de votre logiciel.

Si vous ouvrez un dossier TAC, fournissez le résultat de ces commandes :

- show tech
- show authentication session interface <xx> detail
- show mac address-table interface <xx>

Il est également utile de collecter une capture de paquets de port SPAN et les débogages suivants :

- debug radius verbose
- debug epm all
- debug authentication all
- debug dot1x all
- debug authentication feature <yy> all
- debug aaa authentication
- debug aaa authorization

Informations connexes

- Guide de configuration des services d'authentification 802.1X, Cisco IOS XE version 3SE (commutateurs Catalyst 3850)
- Guide de configuration du logiciel des commutateurs Catalyst 3750-X et Catalyst 3560-X, Cisco IOS version 15.2(1)E
- Guide de configuration du logiciel Catalyst 3750-X et 3560-X, version 15.0(1)SE
- Guide de configuration du logiciel Catalyst 3560, version 12.2(52)SE
- Assistance et documentation techniques - Cisco Systems

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.