802.1x DACL, por usuário ACL, ID de filtro, e comportamento de seguimento do dispositivo

Índice

Introdução

Este documento descreve como os recursos de tracking do dispositivo IP trabalham, que incluem o que os disparadores são adicionar e remover um host. Também, o impacto do dispositivo que segue no Access Control List carregável do 802.1x (DACL) é explicado. As mudanças do comportamento entre versões e Plataformas.

O segundo parte do documento focaliza no Access Control List (ACL) retornado pelo server do Authentication, Authorization, and Accounting (AAA) e aplicado ao 802.1x a sessão. Uma

comparação entre o DACL, por usuário ACL e ID de filtro ACL é apresentada. Também, algumas advertências com respeito à reescrita ACL e o ACL padrão são discutidos.

Teoria de seguimento do dispositivo

O seguimento do dispositivo adiciona uma entrada quando:

- aprende a entrada nova através da espião DHCP.
- aprende a entrada nova através de uma requisição de protocolo de resolução de endereço (ARP) (lê o MAC address do remetente e o endereço IP de Um ou Mais Servidores Cisco ICM NT do remetente do pacote ARP). Que a funcionalidade lhe está chamada às vezes inspeção ARP, mas não é o mesmo que a inspeção ARP dinâmica (DAI). Que a característica está permitida à revelia e não pode ser desabilitada. Está chamado igualmente espião ARP, mas debuga não a mostrará que depois que “debugar a espião arp” é permitida. A espião ARP é permitida à revelia e não pode ser desabilitada ou controlado.

O seguimento do dispositivo remove uma entrada quando não há nenhuma resposta para uma requisição ARP (que envia a ponta de prova para cada host no dispositivo que segue a tabela, à revelia os cada 30 segundos).

Configuração de seguimento do dispositivo

```
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
```

Dispositivo que segue testes

```
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
```

Debuga da versão 12.2.33, seguimento do dispositivo IP actualizado pela espião

DHCP

A espião DHCP povoa a tabela de ligação:

```
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
```

Depois que o emperramento DHCP é adicionado ao base de dados, provoca a notificação para o seguimento do dispositivo:

```
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
```

As pontas de prova ARP são enviadas à revelia cada 30 segundos:

```
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
```

Depois que a entrada é removida do dispositivo que segue a tabela, a entrada obrigatória correspondente DHCP é ainda lá:

```
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
```

Há a edição quando você tem uma reação ARP, mas o dispositivo que segue a entrada está removido de qualquer maneira. Que o erro parece estar na versão 12.2.33 e não apareceu no software da versão 12.2.55 ou 15.x.

Igualmente há algumas diferenças ao segurar com a porta L2 (porta de acesso) e o L3 move (nenhum switchport).

Ponta de prova e espião ARP

Dispositivo que segue com a característica da espião ARP:

```
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
```

Dispositivo IP que segue para a versão 12.2.55 - Comando oculto

Para a versão 12.2 pôde haver uma necessidade de usar um comando oculto a fim ativá-la:

```
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
```

Dispositivo IP que segue para a versão 12.2.55 - Exemplo do IP Estático

Neste exemplo, o PC foi configurado com um endereço IP estático. Debuga a mostra que depois que você obtém uma reação ARP (MSG=2), o dispositivo que segue a entrada é atualizada.

```
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
```

Tão cada requisição ARP do PC atualiza o dispositivo que segue a tabela (o MAC address do remetente e o endereço IP de Um ou Mais Servidores Cisco ICM NT do remetente do pacote ARP).

Dispositivo IP que segue para a versão 15.x

Éimportante recordar que algumas das características tais como DACL para o 802.1x não estão apoiadas na versão LAN Lite (ser cuidadoso - o Cisco Feature Navigator não mostra sempre a informação correta).

O comando oculto da versão 12.2 pode ser executado, mas não terá nenhum efeito. Na versão de software 15.x, o dispositivo IP que segue (IPDT) é permitido à revelia somente para as relações que têm o 802.1x permitido:

```
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
```

Após a remoção da configuração do 802.1x da porta, IPDT será removido igualmente dessa porta. O status de porta pôde ser “TRAGAR”, assim que é necessário ter do “o acesso de modo switchport” e do “o automóvel do porta-controle authenticaion” a fim ter o seguimento do dispositivo IP ativado nessa porta. O limite máximo do dispositivo de interface é ajustado ao 10:

```
bsns-3750-5(config-if)#ip device tracking maximum ?
 <1-10>  Maximum devices
```

Dispositivo IP que segue para o ® do Cisco IOS XE

Além disso, o comportamento no Cisco IOS XE 3.3 mudou quando comparado à versão do Cisco IOS 15.x. O comando oculto da versão 12.2 é Obsoleto, mas este erro será retornado agora:

```
3850-1#  no ip device tracking int g1/0/48
% Command accepted but obsolete, unreleased or unsupported; see documentation.
```

No Cisco IOS XE, o seguimento do dispositivo é ativado para todas as relações (mesmo essas que não têm o 802.1x configurado):

```
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)
```

Também, não há nenhum limite para entradas máximas pela porta (0 significam deficiente).

Dispositivo IP que segue com 802.1x e DACL para a versão 12.2.55

Se o 802.1x é configurado com DACL, o dispositivo que segue a entrada está usado a fim encher o endereço IP de Um ou Mais Servidores Cisco ICM NT do dispositivo. Este exemplo mostra o trabalho de seguimento do dispositivo para um IP estaticamente configurado:

```
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
```

Esta é uma sessão do 802.1x construída com da “o ICMP licença todo o qualquer” DACL:

```
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 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
```

Isto mostra um ACL aplicado:

```
 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)
```

Também, o ACL na relação do Fa0/1 é o mesmo:

```
BSNS-3560-1#show ip access-lists interface fa0/1
    permit icmp any any
```

Mesmo que o padrão seja o dot1x ACL:

```
BSNS-3560-1#show ip interface fa0/1
FastEthernet0/1 is up, line protocol is up
 Inbound  access list is Auth-Default-ACL
```

Pôde-se esperar para que o ACL use “alguns” como 192.168.0.244. Que os trabalhos como este para o proxy do AUTH, mas para o src “algum” do 802.1x DACL não estão mudados ao IP detectado do PC.

Para o proxy do AUTH, um ACL original do ACS é posto em esconderijo e mostrado com o comando show ip access-list e (por usuário com IP específico) um ACL específico é aplicado na relação com o comando do Fa0/1 da relação da lista de acesso da mostra IP. Contudo, o autêntico-proxy não usa o seguimento IP do dispositivo.

Que se o endereço IP de Um ou Mais Servidores Cisco ICM NT não é detectado corretamente? Após o seguimento do dispositivo é desabilitado:

```
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
```

Tão nenhum endereço IP de Um ou Mais Servidores Cisco ICM NT é anexado então, mas o DACL é aplicado ainda:

```
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
```

Nesta encenação, o dispositivo que segue para o 802.1x não é exigido. A única diferença é aquela que conhece o endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente adiantado pode ser usada para uma solicitação de acesso do RAIO. Após o atributo 8 é anexado:

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

Existirá na solicitação de acesso e no ACS será possível criar umas regras mais granuladas da autorização:

```
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
```

Mantenha na mente que TrustSec igualmente precisa o dispositivo IP que segue para o IP aos emperramentos SGT.

Dispositivo IP que segue com 802.1x e DACL para a versão 15.x

Que é a diferença entre a versão 15.x e a versão 12.2.55 em DACL? No software Version15.x, trabalha o mesmos que para o autêntico-proxy. O ACL genérico pode ser visto quando o **comando show ip access-list** está inscrito (resposta posta em esconderijo do AAA), mas depois que o comando do **Fa0/1 da relação da lista de acesso da mostra IP**, o src “algum” está substituído pelo endereço IP de origem do host (conhecido através do dispositivo IP que segue).

Este é o exemplo para um telefone e um PC em uma porta (g1/0/1), a versão de software 15.0.2SE2 em 3750X:

```
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:  C0A80001000001012B680D23
     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
```

O telefone é autenticado através do desvio da autenticação de MAC (MAB), quando o PC usar o dot1x. O telefone e o PC usam o mesmo ACL:

```
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
```

Contudo, quando verificada no nível de interface a fonte foi substituída pelo endereço IP de Um ou Mais Servidores Cisco ICM NT do dispositivo. O dispositivo IP que seguem os disparadores que mudam e podem ocorrer a qualquer hora (muito mais tarde do que a sessão da autenticação e a transferência do ACL):

```
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
```

Ambos os endereços MAC devem ser marcados como a estática:

```
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
```

Entrada ACL específica

Quando a fonte “alguma” no DACL é substituída com o endereço IP de Um ou Mais Servidores Cisco ICM NT do host? Somente quando houver pelo menos duas sessões na mesma porta (dois suplicantes).

Não há nenhuma necessidade de substituir “” a fonte quando há somente uma sessão. Os problemas puderam aparecer quando há umas sessões múltiplas, e para não todo o seguimento do dispositivo IP conhece o endereço IP de Um ou Mais Servidores Cisco ICM NT do host. Nessa encenação ainda será “algum” para algumas entradas.

Esse comportamento é diferente em algumas Plataformas. Por exemplo, no 2960X com versão 15.0(2)EX o ACL será sempre específico mesmo quando há apenas uma sessão da autenticação pela porta. Contudo, para a versão 15.0(2)SE 3560X e 3750X, você precisa de ter pelo menos duas sessões para fazer esse específico ACL.

Controle-sentido

Àrevelia, o controle-sentido é tipo ambos:

```
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
```

Isso significa que antes que o suplicante esteja autenticado, o tráfego não pode ser enviado a ou da porta. Para “” no modo, o tráfego poderia ter sido enviado da porta ao suplicante, mas não do suplicante à porta (poderia ser útil para a VIGÍLIA na característica LAN).

Ainda, o interruptor aplica o ACL apenas no “” no sentido. Não importa que modo é usado.

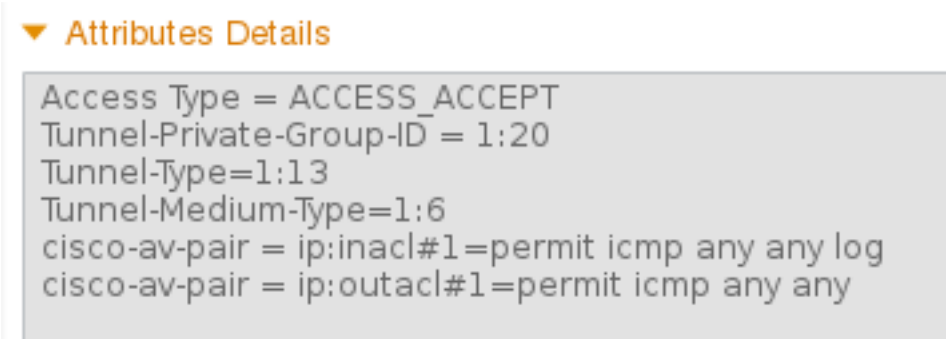
```
bsns-3750-5#sh ip access-lists interface g1/0/1 out
bsns-3750-5#sh ip access-lists interface g1/0/1 in
    permit ip host 192.168.2.200 any
    permit ip host 192.168.10.12 any
```

Isso significa basicamente que depois que a autenticação o ACL é aplicada para o tráfego à porta (no sentido) e todo o tráfego é permitido da porta (para fora sentido).

Dispositivo IP que segue com 802.1x e por usuário ACL para a versão 15.x

Éigualmente possível usar um usuário per. ACL que seja passado no Cisco-av-pair “IP: inacl” e “IP: outacl”.

Este exemplo de configuração é similar a uma configuração precedente, mas esta vez o telefone usa DACL e os usos por usuário ACL PC. O perfil ISE para o PC é:



O telefone ainda tem o DACL aplicado:

```
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:  C0A8000100000568431143D8
     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
```

Contudo, o PC na mesma porta usa o usuário per. ACL:

```
    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:  C0A800100000574311400B
     Acct Session ID:  0x000006D1
              Handle:  0x9D000568
```

A fim verificar como isso é fundido na porta gig1/0/1:

```
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
```

A primeira entrada foi tomada do usuário per. que ACL (observe a palavra-chave do log) e a segunda entrada é tomada do DACL. Ambos eles são reescritos pelo dispositivo IP que segue para o endereço IP de Um ou Mais Servidores Cisco ICM NT específico.

Por usuário o ACL podia ser verificado com o **comando all do epm debugar**:

```
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
```

E igualmente através do **comando show ip access-lists**:

```
bsns-3750-5#show ip access-lists
Extended IP access list GigabitEthernet1/0/1#IP#7844C6C (per-user)
   10 permit icmp any any log
```

Que sobre o IP: atributo do outacl? É omitido completamente na versão 15.x. O atributo foi recebido, mas o interruptor não faz aplicar-se/processo que atribui.

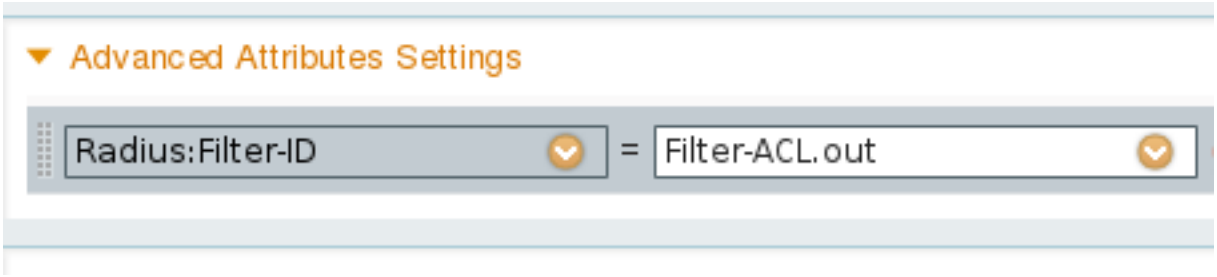
Diferença quando comparado ao DACL

Como referido na identificação de bug Cisco CSCut25702, o usuário per. ACL comporta-se diferentemente do que DACL. DACL com apenas uma entrada (“licença IP algum algum”) e um suplicante conectado a uma porta pode trabalhar corretamente sem seguimento do dispositivo IP permitido. “Nenhum” argumento não será substituído e todo o tráfego será permitido. Contudo, porque o usuário per. ACL é imperativo ter o seguimento do dispositivo IP permitido. Se é desabilitado e tem apenas a “licença IP qualquer qualquer” entrada e um suplicante, a seguir todo o tráfego estará obstruído.

Dispositivo IP que segue com 802.1x e ID de filtro ACL para a versão 15.x

Também, o ID de filtro [11] do atributo IETF pode ser usado. O servidor AAA retorna o nome ACL, que deve ser definido localmente no interruptor. O perfil ISE podia olhar como este:

Note que você precisa specifiy o sentido (em ou para fora). Para isso é necessário adicionar manualmente o atributo:



Então as mostras debugar:

```
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
```

Esse ACL será mostrado igualmente para a sessão autenticada:

```
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
```

E, como o ACL é o ativado à relação:

```
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
```

Note que este ACL pode ser fundido com outros tipos de ACL na mesma relação. Por exemplo, tendo na mesma porta de switch um outro suplicante que obtenha DACL do ISE: "licença IP algum algum" que você poderia ver:

```
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
```

Note que o seguimento do dispositivo IP reescreve o IP da fonte para cada fonte (suplicante).

Que sobre "para fora" a lista de filtro? Outra vez (como o usuário per. ACL), não será usada pelo interruptor.

Seguimento do dispositivo IP - Padrões e melhores prática

Para liberações mais cedo do que 15.2(1)E, antes que toda a característica possa usar IPDT ele precisa de ser permitido globalmente primeiramente com este comando CLI:

```
(config)#ip device tracking
```

Para as liberações 15.2(1)E e mais tarde, o comando de **seguimento do dispositivo IP** não é precisado mais. IPDT está permitido somente se uma característica que confie nele o permite. Se nenhuma característica permite IPDT, IPDT está desabilitado. "Nenhum comando de seguimento do dispositivo IP" não tem nenhum efeito. A característica específica tem permitir do controle/desabilitação IPDT.

Quando você permite IPDT, você tem que recordar sobre a edição do "endereço de IP duplicado" sobre. Veja para pesquisar defeitos do "Mensagens de Erro de 0.0.0.0 endereço de IP duplicado" para mais informação.

Recomenda-se desabilitar IPDT em uma porta de tronco:

```
(config-if)# no ip device tracking
```

No Cisco IOS mais atrasado, é um comando diferente:

```
(config-if)#ip device tracking maximum 0
```

Recomenda-se permitir IPDT na porta de acesso e atrasar pontas de prova ARP a fim evitar a edição do "endereço de IP duplicado":

```
(config-if)#ip device tracking probe delay 10
```

Reescrita da relação ACL para a versão 15.x

Para a relação ACL, trabalha antes da autenticação:

```
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
```

Contudo, depois que a autenticação sucede é reescrita (ultrapassagem) pelo ACL retornado do servidor AAA (não importa se é DACL, IP: inacl, ou filterid).

Esse ACL (test1) pode obstruir o tráfego (que seria permitido normalmente no modo aberto), mas depois que a autenticação não importa anymore. Mesmo quando nenhum ACL é retornado do servidor AAA, a relação ACL overwritten e o acesso direto é fornecido. Aquele é um bit que engana-se desde que o Ternary Content Addressable Memory (TCAM) indica que o ACL é ainda ativado no nível de interface. Está aqui um exemplo da versão 15.2.2 em 3750X:

```
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
```

Essa informação é válida somente para o nível de interface, não para o nível da sessão. Um pouco mais de informação (apresenta um ACL combinado) pode ser deduzida de:

```
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 2.2.2.2 host 1.1.1.1
```

A primeira entrada é criada como a “licença IP que todo o qualquer” DACL é retornado para a autenticação bem sucedida (e é substituído “” por uma entrada do dispositivo que segue a tabela). A segunda entrada é o resultado da relação ACL e é aplicada para todas as autenticações novas (antes da autorização).

Infelizmente, (outra vez dependente da plataforma) ambos os ACL são concatenados. Isso acontece na versão 15.2.2 em 3750X. Isso significa aquele para a sessão autorizada, ambos eles é aplicado. Primeiramente o DACL e segundo a relação ACL. É por isso quando você adiciona o “deny ip any any explícito”, o DACL não tomará na consideração a relação ACL. Geralmente há não explícito nega no DACL e então a relação ACL é aplicada em seguida que.

O comportamento para a versão 15.0.2 em 3750X é o mesmo, mas o **comando interface sh da lista de acesso IP** não mostra a relação ACL anymore (mas ele será concatenado ainda com a relação ACL a menos que explícito negam no DACL existe).

ACL padrão usado para o 802.1x

Há dois tipos do padrão ACL:

- Autêntico-padrão-ACL-ABERTO - usado para o modo aberto
- Autêntico-padrão-ACL - usado para o acesso fechado

o autêntico-padrão-ACL e autêntico-padrão-ACL-ABERTOS são usados quando a porta está no estado desautorizado. À revelia, o acesso fechado é usado. Isso significa que antes que a autenticação todo o tráfego esteja deixada cair a não ser que esse permita pelo autêntico-padrão-ACL. Este tráfego da maneira DHCP é permitido antes da autorização bem sucedida. O endereço IP de Um ou Mais Servidores Cisco ICM NT é atribuído e o DACL transferido pode corretamente ser aplicado. Que o ACL está criado automaticamente e não pode ser encontrado na configuração.

```
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
```

Écriado dinamicamente para a primeira autenticação (entre a fase da authentication e autorização) e removido depois que a última sessão é removida.

O Autêntico-Padrão-ACL permite somente o tráfego DHCP. Depois que a autenticação sucede e o DACL novo está transferido, está aplicado a essa sessão. Quando o modo é mudado para abrir autêntico-padrão-ACL-ABERTO aparece e está usado e trabalha exatamente da mesma forma como o Autêntico-Padrão-ACL:

```
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
```

Ambos os ACL podem ser personalizados, mas serão vistos nunca na configuração.

```
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#
```

Abra o modo

A seção anterior descreveu o comportamento para ACL (que inclui esse usado à revelia para o modo aberto). O comportamento para o modo aberto é:

- permite todo o tráfego (conforme o padrão autêntico-padrão-ACL-ABERTO) quando a sessão está em um estado desautorizado.

- a sessão está em um estado desautorizado durante a autenticação/autorização (boas para encenações da bota do modelo E do dispositivo da criptografia (PXE)) ou em seguida esse processo falha (bom para as encenações chamadas “baixo modo do impacto”).
- quando a sessão se move para o estado autorizado para plataformas múltiplas, os ACL estão concatenados e o primeiro DACL é usado, então a relação ACL.
- para o multi-AUTH ou o multi-domínio pôde haver umas sessões múltiplas ao mesmo tempo em estados diferentes (então o tipo diferente ACL se aplicará para cada sessão).

Quando a relação ACL for imperativa

Para o múltiplo 6500/4500 de Plataformas, a relação ACL é imperativa a fim aplicar corretamente o DACL.

Está aqui um exemplo com 4500 sup2 12.2.53SG6, nenhuma relação ACL:

```
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
```

Então depois que o host é autenticado, o DACL é transferido. Não será aplicado e a autorização falha.

```
*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
```

Após a relação o ACL é adicionado:

```
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
```

A authentication e autorização sucederá e o DACL será aplicado corretamente:

```
brisk#show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Gi2/3      0007.5032.6941  mab      VOICE    Authz Success  0A3043450000008001A2CE4
```

O comportamento não é dependente da “autenticação aberta”. A fim aceitar o DACL, você precisa a relação ACL para ambos abre/fechou o modo.

DACL em 4500/6500

No 4500/6500, o DACL é aplicado com acl_snoop DACLs. Um exemplo com 4500 sup2 12.2.53SG6 (telefone + PC) é mostrado aqui. Há um ACL separado para a Voz (10) e os dados (100) VLAN:

```
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
```

Os ACL são específicos porque IPDT tem as entradas corretas:

```
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
```

As sessões autenticadas confirmam os endereços:

```
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
```

Nesta fase o PC e o telefone respondem ao eco ICMP, mas aos presentes da relação ACL somente:

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

```
    permit ip host 192.168.10.12 any
```

Por quê? Porque o DACL foi incrementado somente o telefone (192.168.10.12). Para o PC, a relação ACL com modo aberto é usada:

```
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)
```

Em resumo, o acl_snoop será criado para o PC e o telefone, mas o DACL é retornado apenas para o telefone. Esse ACL é visto é por isso como o ativado à relação.

Estado do MAC address para o 802.1x

Quando a autenticação do 802.1x começa, o MAC address está considerado ainda como DINÂMICO mas a ação para esse pacote é GOTA:

```
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
```

Depois que a autenticação bem sucedida o MAC address se torna a estática e o número de porta estão fornecidos:

```
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
```

Isso é verdadeiro para toda a sessão mab/dot1x para ambos os domínios (VOICE/DATA).

Troubleshooting

Recorde ler o manual de configuração do 802.1x para suas versão de software e plataforma específicas.

Se você abre um caso de TAC, forneça a saída destes comandos:

- show tech
- mostre o detalhe do <xx> da relação da sessão da autenticação
- mostre o <xx> da relação da tabela de endereços MAC

Éigualmente bom recolher uma captura de pacote de informação da porta span e estes debugam:

- debugar o raio verboso
- debugar o epm todo
- debug authentication todo
- debugar o dot1x todo
- <yy> todo da característica do debug authentication
- debug aaa authentication
- **debug aaa authorization**

Informações Relacionadas

- manual de configuração dos serviços de autenticação do 802.1X, liberação 3SE do Cisco IOS XE (Catalyst 3850 Switch)
- Catalizador 3750-X e manual de configuração do software do Catalyst 3560-X Switch, Cisco IOS Release 15.2(1)E
- Manual de configuração do software 3750-X e 3560-X do catalizador, liberação 15.0(1)SE
- Manual de configuração do software do catalizador 3560, liberação 12.2(52)SE
- Suporte Técnico e Documentação - Cisco Systems