Exemplo de configuração do TrustSec com ASA e o switch Catalyst 3750-X Series e Guia de solução de problemas

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Configurar](#)
[Diagrama de Rede](#)
[Fluxo de tráfico](#)
[Configurações](#)
[Autenticação de porta com o comando *ip device tracking* no 3750X](#)
[Configuração do ISE para políticas de autenticação, SGT e SGACL](#)
[Configuração CTS no ASA e no 3750X](#)
[Provisionamento de PAC no 3750X (Automático) e no ASA (Manual)](#)
[Atualização do ambiente no ASA e no 3750X](#)
[Verificação e aplicação de autenticação de porta no 3750X](#)
[Atualização de políticas no 3750X](#)
[SXP Exchange (o ASA como ouvinte e o 3750X como alto-falante)](#)
[Filtragem de tráfego no ASA com SGT ACL](#)
[Filtragem de tráfego no 3750X com políticas baixadas do ISE (RBACL)](#)
[Verificar](#)
[Troubleshoot](#)
[Provisionamento de PAC](#)
[Atualização de ambiente](#)
[Atualização de política](#)
[Exchange do SXP](#)
[SGACL no ASA](#)
[Informações Relacionadas](#)

Introduction

Este artigo descreve como configurar o Cisco TrustSec (CTS) no Cisco Secure Adaptive Security Appliance (ASA) e em um switch Cisco Catalyst 3750X Series (3750X).

Para aprender o mapeamento entre tags de grupos de segurança (SGTs) e endereços IP, o ASA usa o SGT Exchange Protocol (SXP). Em seguida, as Access Control Lists (ACLs) baseadas no

SGT são usadas para filtrar o tráfego. O 3750X baixa as políticas de RBACL (Role-Based Access Control List, lista de controle de acesso baseado em funções) do Cisco Identity Services Engine (ISE) e filtra o tráfego com base nelas. Este artigo detalha o nível do pacote para descrever como a comunicação opera e as depurações esperadas.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento básico destes tópicos:

- Componentes CTS
- Configuração CLI do ASA e do Cisco IOS®

Componentes Utilizados

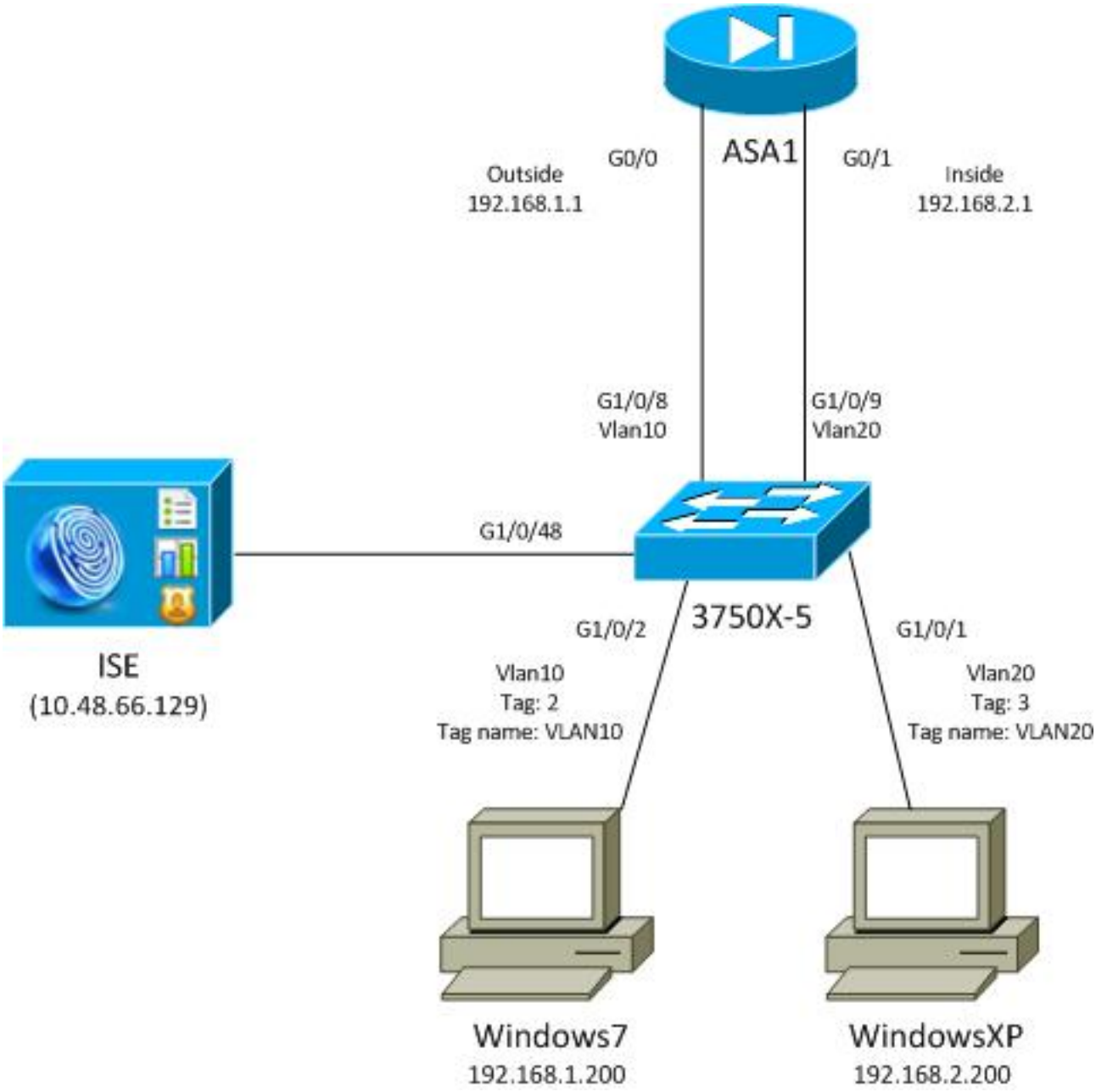
As informações neste documento são baseadas nestas versões de software e hardware:

- Software Cisco ASA, versões 9.1 e posteriores
- Microsoft (MS) Windows 7 e MS Windows XP
- Software Cisco 3750X, versões 15.0 e posteriores
- Software Cisco ISE, versões 1.1.4 e posteriores

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Diagrama de Rede



Fluxo de tráfico

Aqui está o fluxo de tráfego:

- O 3750X é configurado em **G1/0/1** e **G1/0/2** para autenticação de porta.
- O ISE é usado como o servidor AAA (Authentication, Authorization, and Accounting).
- O MAC Address Bypass (MAB) é usado para autenticação do MS Windows 7.
- O IEEE 802.1x é usado para o MS Windows XP para demonstrar que não importa qual método de autenticação é usado.

Após a autenticação bem-sucedida, o ISE retorna o SGT e o 3750X vincula essa tag à sessão de autenticação. O switch também aprende os endereços IP de ambas as estações com o comando **ip device tracking**. O switch usa o SXP para enviar a tabela de mapeamento entre o SGT e o endereço IP para o ASA. Ambos os computadores MS Windows têm um roteamento padrão que aponta para o ASA.

Depois que o ASA recebe o tráfego do endereço IP que é mapeado para o SGT, ele pode usar a ACL com base no SGT. Além disso, quando você usa o 3750X como um roteador (gateway

padrão para ambas as estações do MS Windows), ele pode filtrar o tráfego com base nas políticas baixadas do ISE.

Estas são as etapas de configuração e verificação, cada uma das quais é detalhada em sua própria seção mais adiante no documento:

- Autenticação de porta com o comando **ip device tracking** no 3750X
- Configuração do ISE para políticas de autenticação, SGT e SGACL (Security Group Access Control List, lista de controle de acesso do grupo de segurança)
- Configuração CTS no ASA e no 3750X
- Provisionamento de PAC (Protected Access Credential) no 3750X (automático) e no ASA (manual)
- Atualização do ambiente no ASA e no 3750X
- Verificação e aplicação da autenticação de porta no 3750X
- Atualização de políticas no 3750X
- Troca de SXP (o ASA como ouvinte e o 3750X como alto-falante)
- Filtragem de tráfego no ASA com SGT ACL
- Filtragem de tráfego no 3750X com políticas baixadas do ISE

Configurações

Autenticação de porta com o comando *ip device tracking* no 3750X

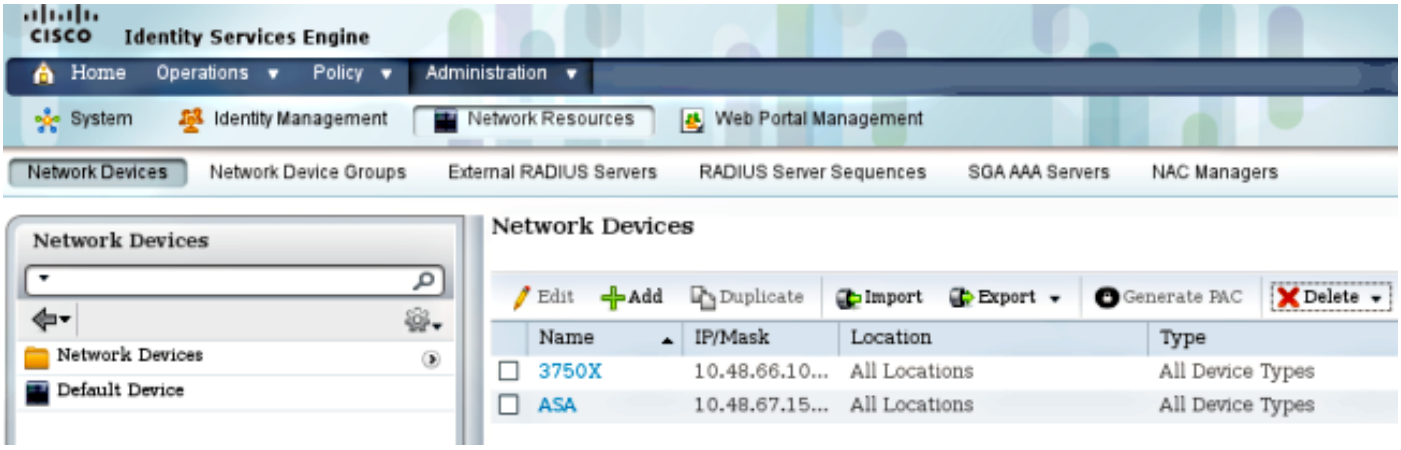
Esta é a configuração típica para 802.1x ou MAB. A alteração de autorização (CoA) do RADIUS é necessária somente quando você usa a notificação ativa do ISE.

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization network ise group radius
aaa accounting dot1x default start-stop group radius

!Radius COA
aaa server radius dynamic-author
 client 10.48.66.129 server-key cisco
 server-key cisco

ip device tracking

interface GigabitEthernet1/0/1
 description windowsxp
 switchport mode access
 authentication order mab dot1x
 authentication port-control auto
 mab
 dot1x pae authenticator
 spanning-tree portfast
!
interface GigabitEthernet1/0/2
 description windows7
 switchport mode access
 authentication order mab dot1x
 authentication port-control auto
```

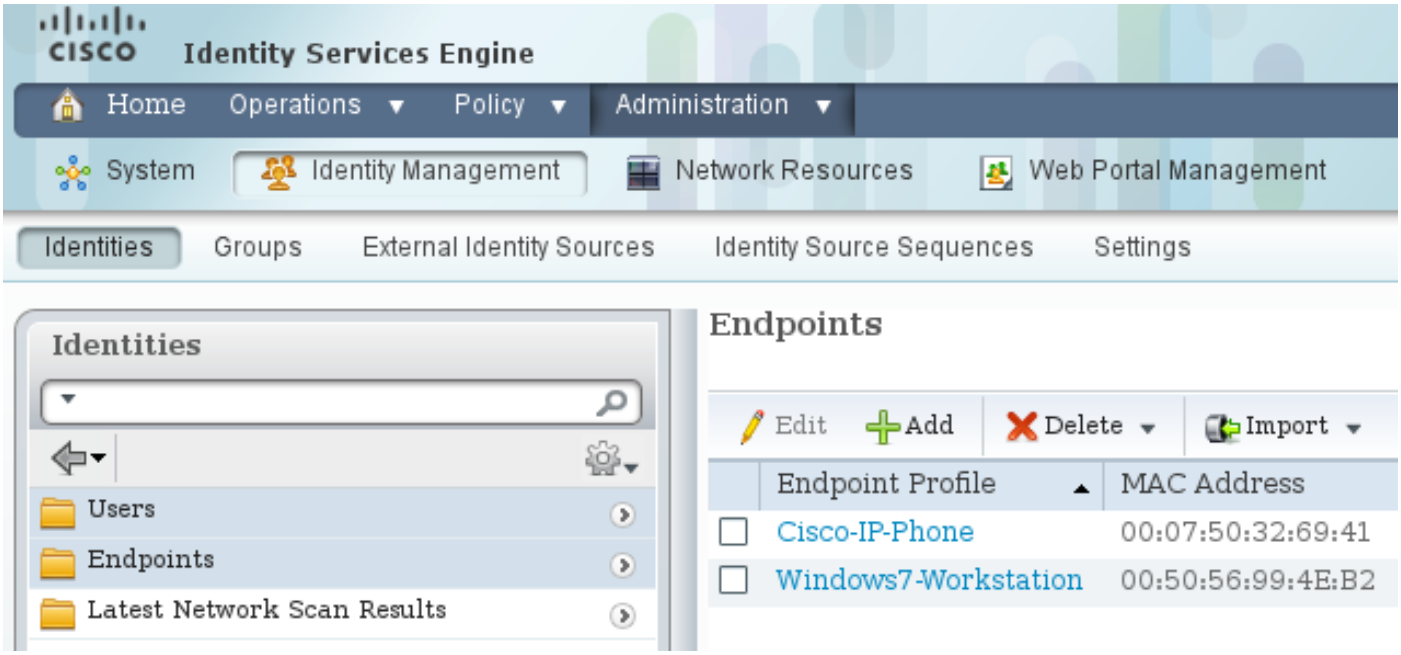
```
 mab
 dot1x pae authenticator
spanning-tree portfast

radius-server host 10.48.66.129 pac key cisco
radius-server host 10.48.66.129 auth-port 1812
radius-server vsa send accounting
radius-server vsa send authentication
```

Configuração do ISE para políticas de autenticação, SGT e SGACL

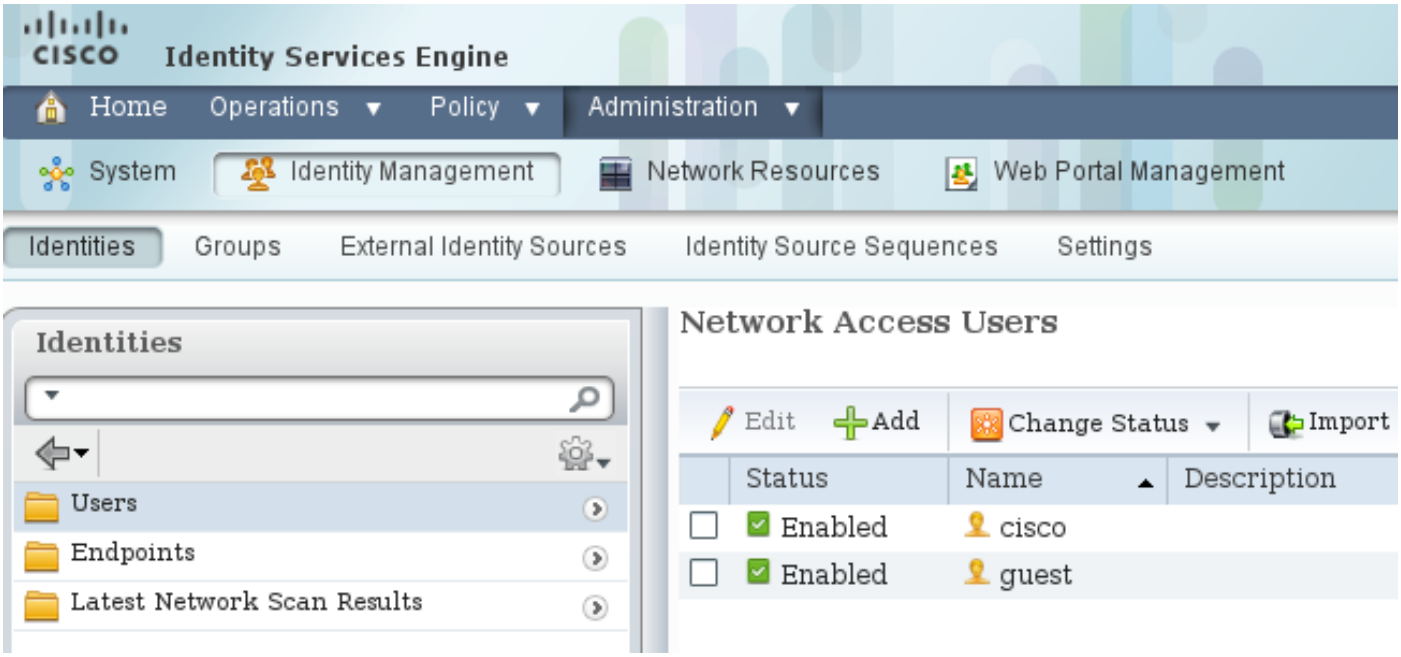
O ISE deve ter ambos os dispositivos de rede configurados em **Administração > Dispositivos de Rede**:



No MS Windows 7, que usa autenticação MAB, você deve criar Endpoint Identity (endereço MAC) em **Administration > Identity Management > Identities > Endpoints**:

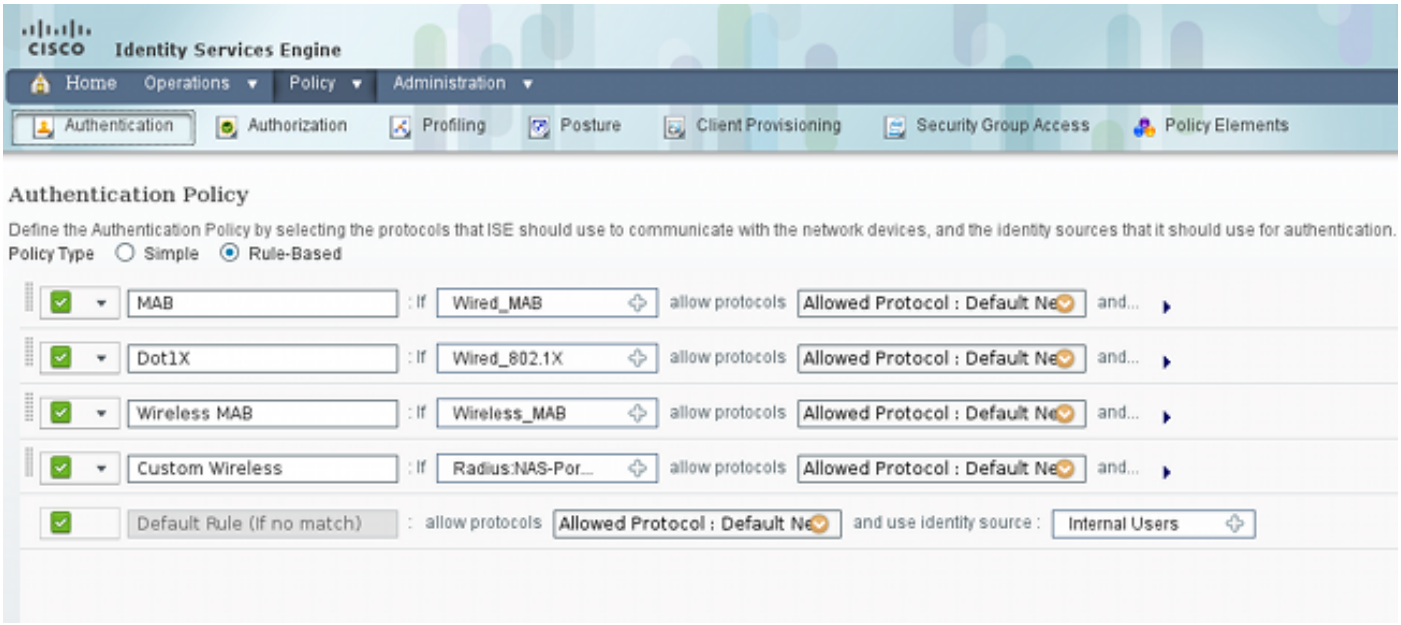


Para o MS Windows XP, que usa a autenticação 802.1x, você deve criar uma Identidade de usuário (nome de usuário) em **Administração > Gerenciamento de identidade > Identidades > Usuários**:

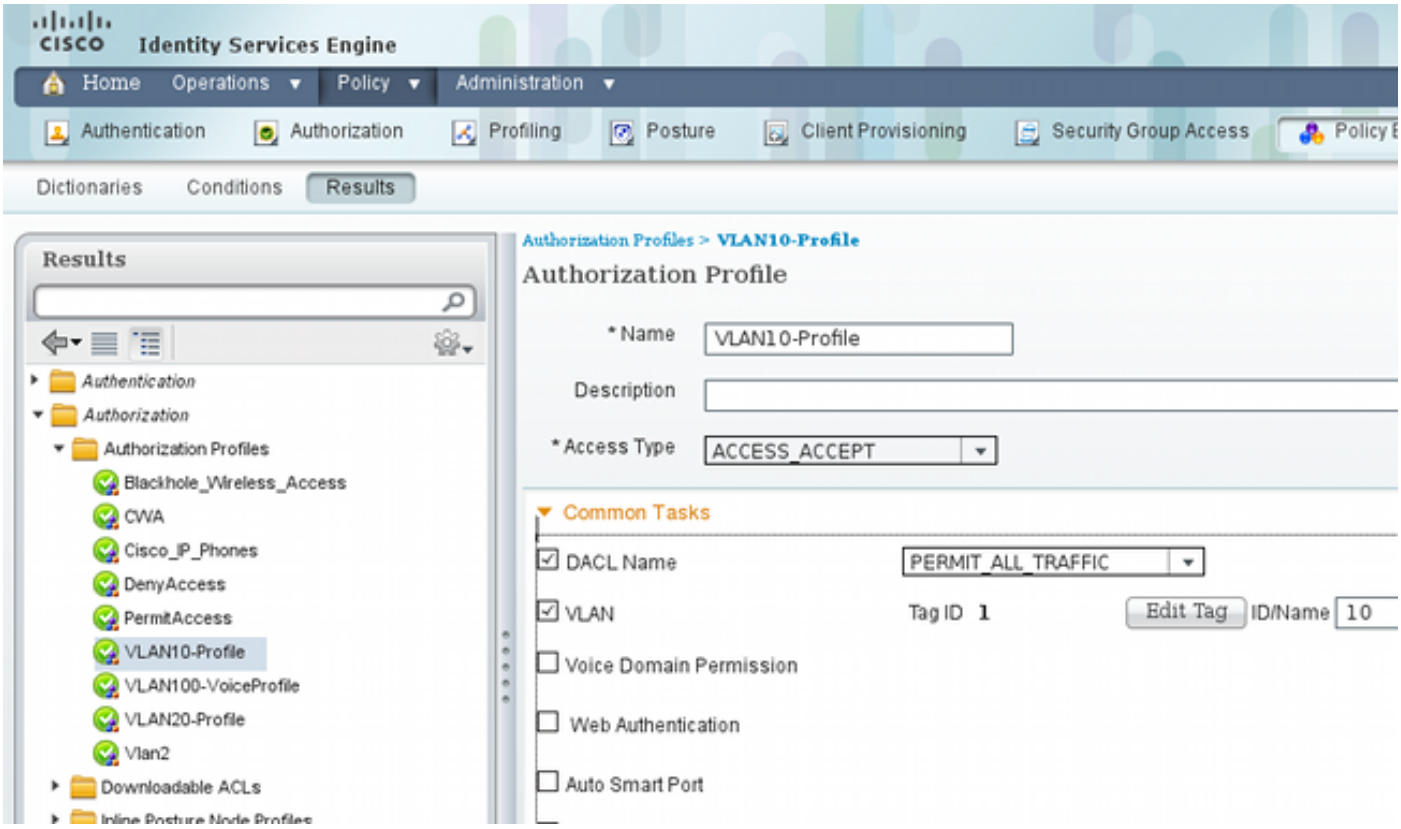


O nome de usuário **cisco** é usado. Configure o MS Windows XP para EAP protegido por protocolo de autenticação extensível (EAP-PEAP) com essas credenciais.

No ISE, as políticas de autenticação padrão são usadas (não altere isso). A primeira é a política para autenticação MAB e a segunda é 802.1x:



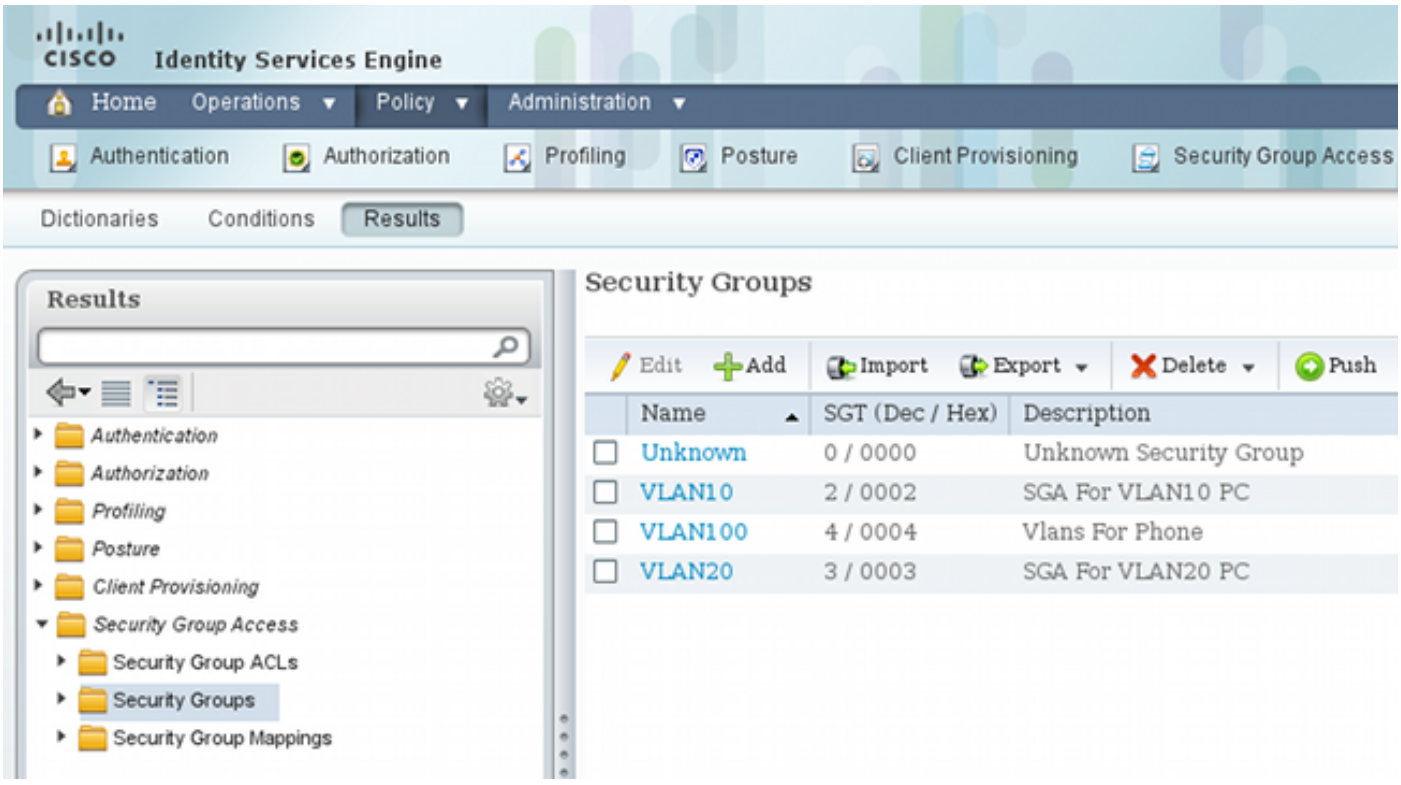
Para configurar políticas de autorização, você deve definir perfis de autorização em **Política > Resultados > Autorização > Perfis de autorização**. O perfil VLAN10 com ACL para download (DACL), que permite todo o tráfego, é usado para o perfil do MS Windows 7:



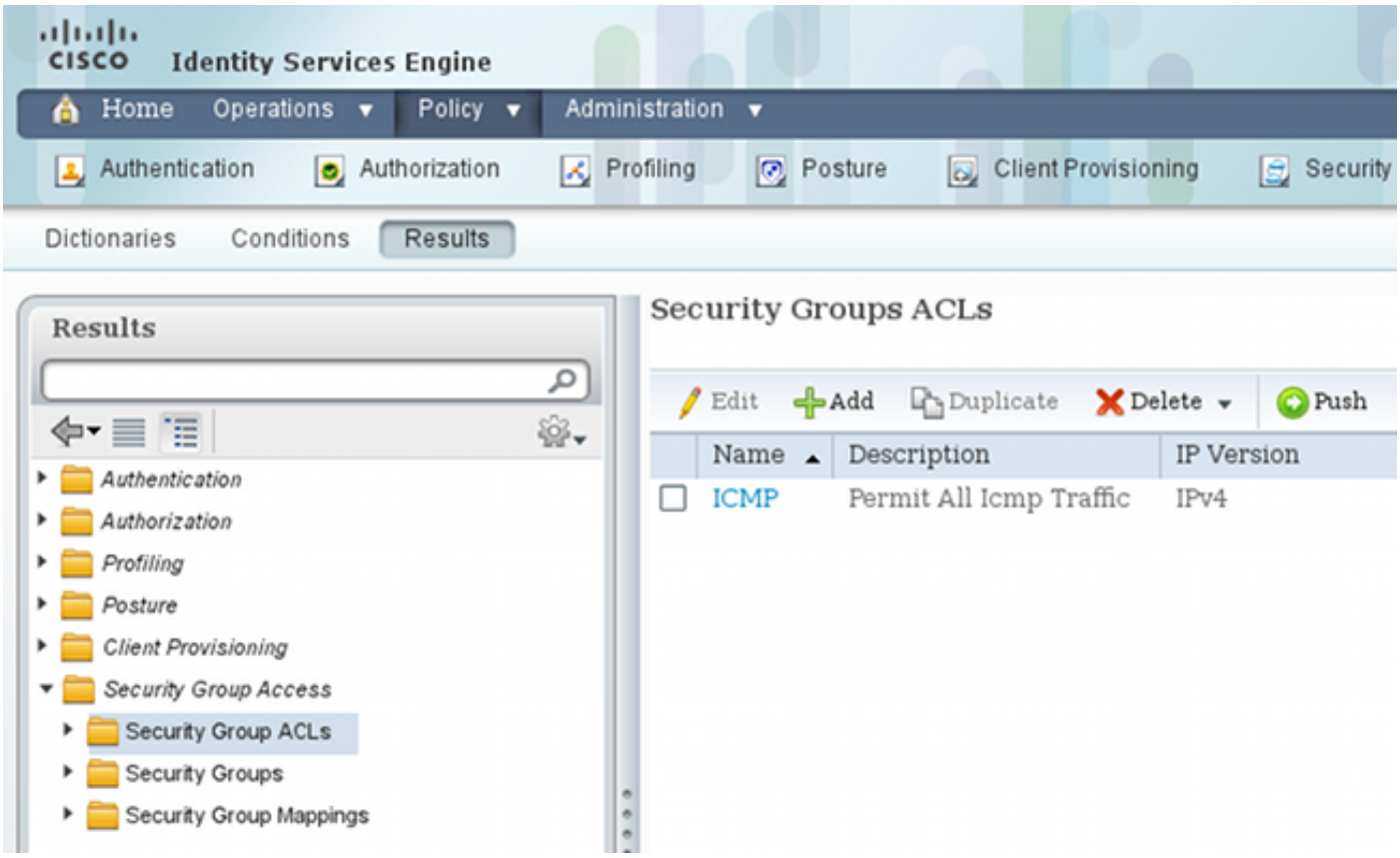
Uma configuração semelhante, VLAN20-Profile, é usada para o MS Windows XP com exceção do número da VLAN (20).

Para configurar os grupos SGT (tags) no ISE, navegue para **Política > Resultados > Acesso ao grupo de segurança > Grupos de segurança**.

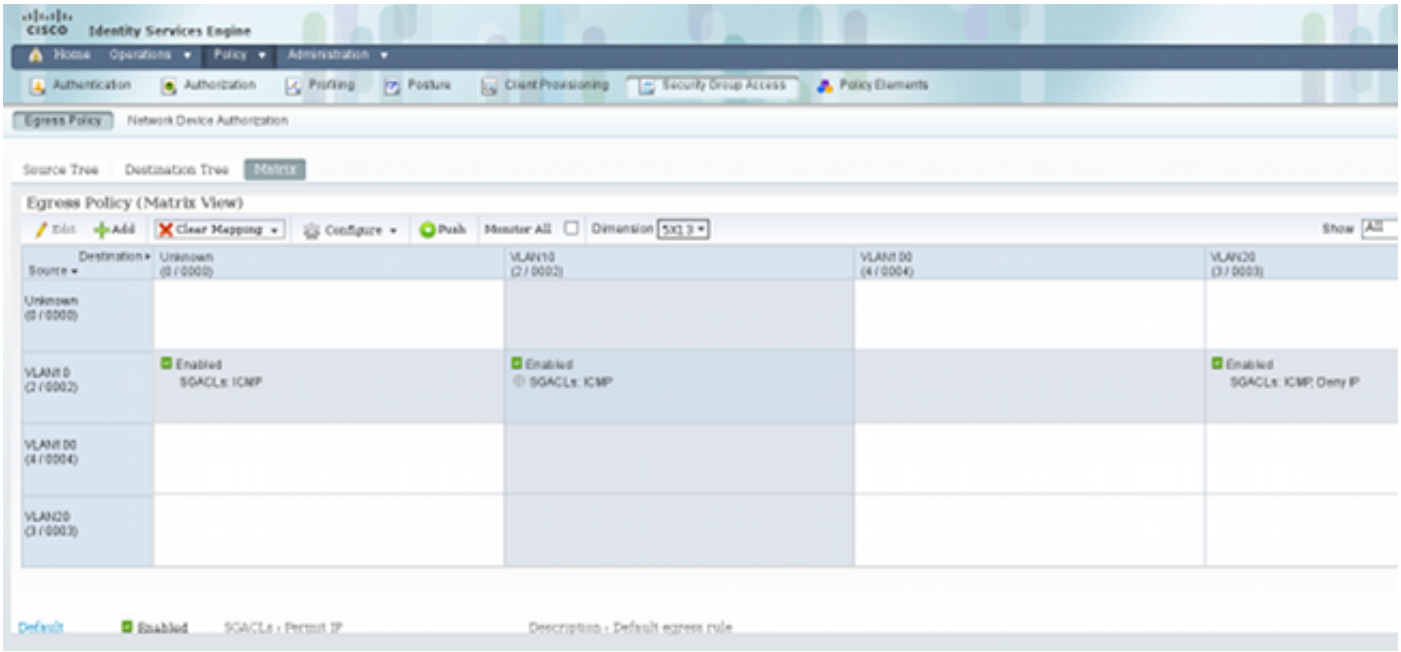
> **Observação**: não é possível escolher um número de etiqueta; ele é selecionado automaticamente pelo primeiro número livre, exceto 1. Você pode configurar apenas o nome SGT.



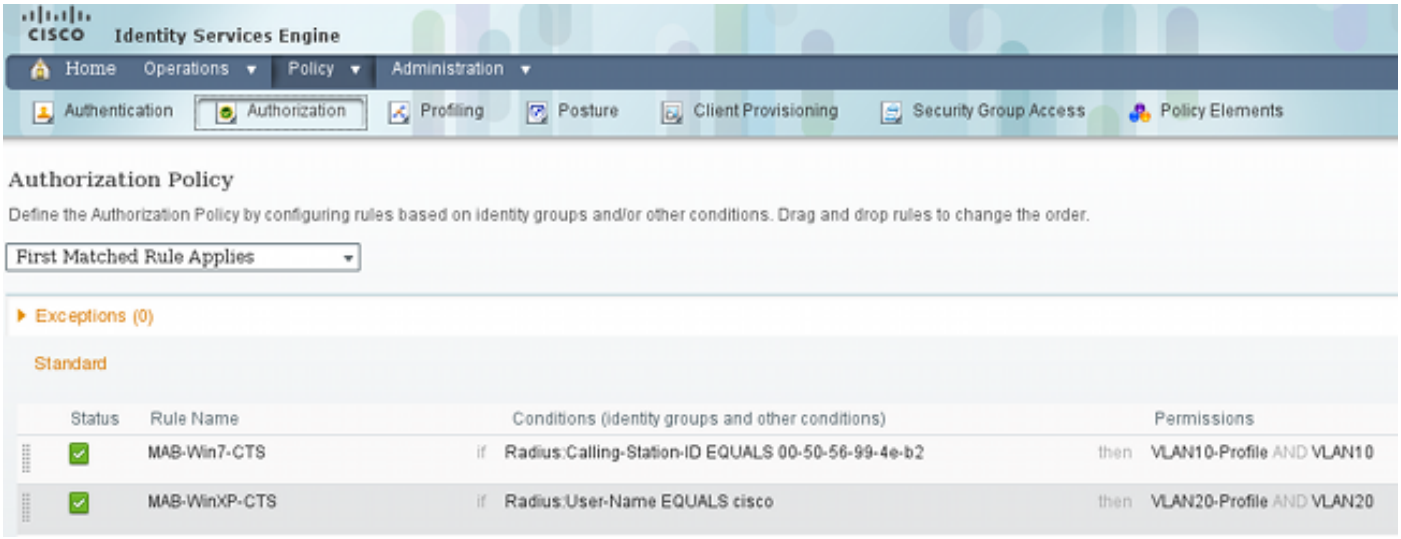
Para criar o SGACL para permitir o tráfego do Internet Control Message Protocol (ICMP), navegue para **Policy > Results > Security Group Access > Security Group ACLs**:



Para criar políticas, navegue para **Política > Acesso ao grupo de segurança > Política de saída**. Para o tráfego entre VLAN10 e a VLAN desconhecida ou VLAN10 ou VLAN20, a ACL ICMP é usada (**permit icmp**):



Para definir regras de autorização, navegue para **Política > Autorização**. Para o MS Windows 7 (endereço MAC específico), **VLAN10-Profile** é usado, retornando VLAN10 e DACL, e o perfil de segurança VLAN10 com o SGT nomeado **VLAN10**. Para o MS Windows XP (nome de usuário específico), **VLAN20-Profile** é usado, retornando a VLAN 20 e a DACL, e o perfil de segurança VLAN20 com o SGT nomeado **VLAN20**.



Conclua a configuração do switch e do ASA para que eles aceitem os atributos SGT RADIUS.

Configuração CTS no ASA e no 3750X

Você deve definir as configurações básicas de CTS. No 3750X, você deve indicar de quais políticas de servidor deve ser feito o download:

```
aaa authorization network ise group radius
cts authorization list ise
```

No ASA, somente o servidor AAA é necessário junto com o CTS que aponta para esse servidor:

```
aaa-server ISE protocol radius
aaa-server ISE (mgmt) host 10.48.66.129
 key *****
cts server-group ISE
```

> **Observação**: no 3750X, você deve apontar explicitamente para o servidor ISE com o comando **group radius**. Isso ocorre porque o 3750X usa o fornecimento automático de PAC.

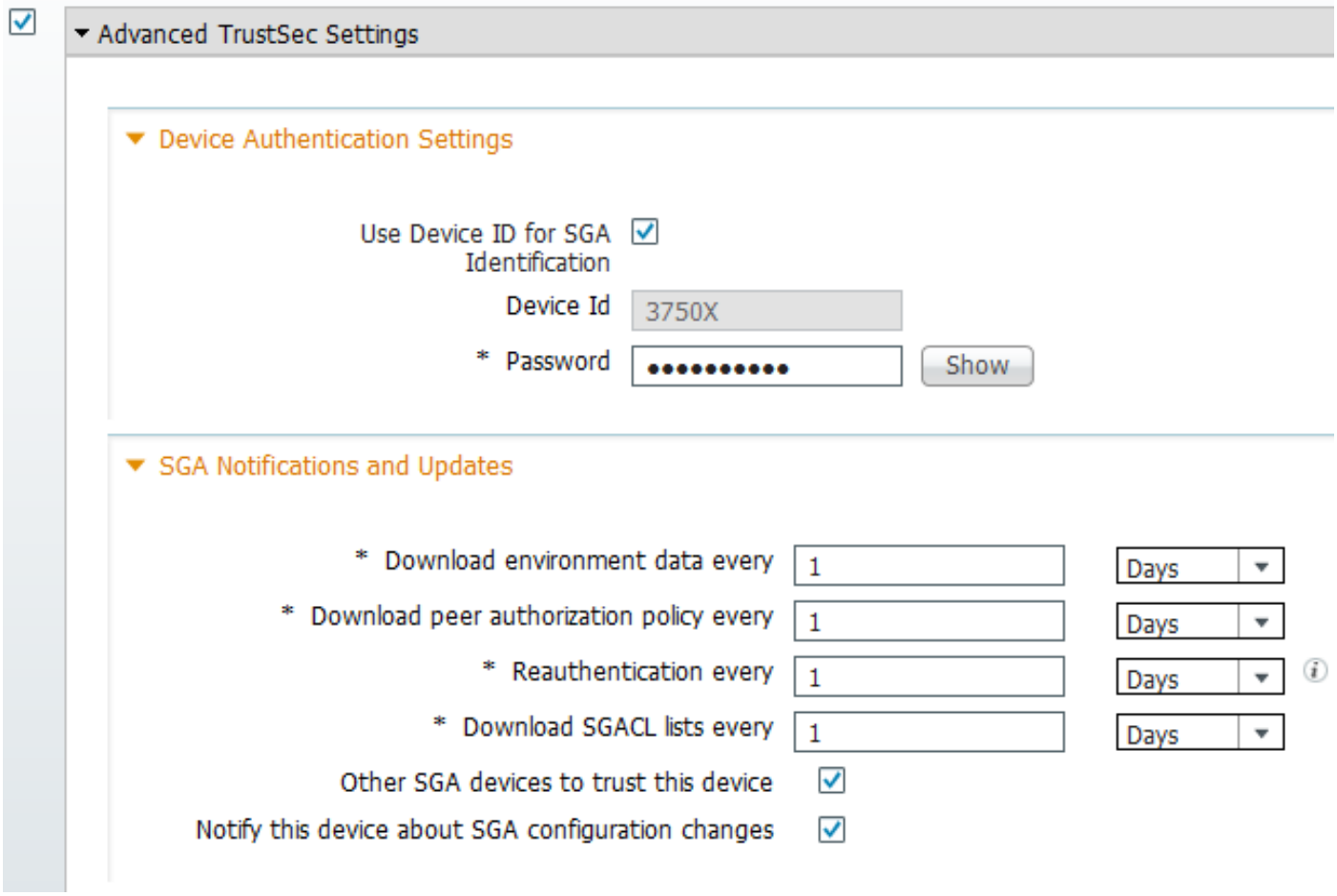
Provisionamento de PAC no 3750X (Automático) e no ASA (Manual)

Cada dispositivo na nuvem CTS deve se autenticar no servidor de autenticação (ISE) para ser confiável para outros dispositivos. Para isso, ele usa o método EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Protocol) (RFC 4851). Esse método exige que a PAC seja entregue fora da banda. Esse processo também é chamado de **phase0** e não é definido em nenhum RFC. A PAC para EAP-FAST tem uma função semelhante à do certificado para EAP-TLS (Extensible Authentication Protocol-Transport Layer Security). A PAC é usada para estabelecer um túnel seguro (fase 1), que é necessário para a autenticação na fase 2.

Provisionamento de PAC no 3750X

O 3750X oferece suporte ao provisionamento automático de PAC. Uma senha compartilhada é usada no switch e no ISE para baixar a PAC. Essa senha e ID devem ser configuradas no ISE em **Administration > Network Resources > Network Devices**. Selecione o switch e expanda a seção

Configurações avançadas do TrustSec para configurar:



Para que a PAC use essas credenciais, insira estes comandos:

```
bsns-3750-5#cts credentials id 3750X password ciscocisco
bsns-3750-5#show cts pacs
 AID: C40A15A339286CEAC28A50DBBAC59784
 PAC-Info:
   PAC-type = Cisco Trustsec
   AID: C40A15A339286CEAC28A50DBBAC59784
   I-ID: 3750X
   A-ID-Info: Identity Services Engine
   Credential Lifetime: 08:04:40 UTC Sep 25 2013
 PAC-Opaque: 000200B000030001000400010C40A15A339286CEAC28A50DBBAC59784000600940003
010094F559DAE0C837D7847F2454CAD7E80B0000001351C8235900093A803D7D427BFB5C6F0FBBDF
7EDF0818C58FECF97F8BDECF1B115FB0240260ADA8C96A46AA2A64C9EA2DB51E0E886768CA2D133D
2468D9D33339204BAA7E4CA2DE8E37FF1EB5BCB343408E9847998E301C26DDC6F91711F631A5B4C7
C2CB09EAB028630A3B22901FE3EF44F66FD019D09D2C46D92283
 Refresh timer is set for 2y24w
```

Provisionamento de PAC no ASA

O ASA oferece suporte apenas ao provisionamento manual de PAC. Isso significa que você deve gerá-lo manualmente no ISE (em dispositivos de rede/ASA):

Em seguida, o arquivo deve ser instalado (por exemplo, com FTP):

```
bsns-asa5510-17(config)# cts import-pac ftp://ftp:ftp@10.147.25.80/ASA.pac
password ciscocisco
!PAC Imported Successfully

bsns-asa5510-17(config)# show cts pac

 PAC-Info:
   Valid until: Jul 04 2014 13:33:02
   AID:         c40a15a339286ceac28a50dbbac59784
   I-ID:        ASA
   A-ID-Info:   Identity Services Engine
   PAC-type:    Cisco Trustsec
 PAC-Opaque:
   000200a80003000100040010c40a15a339286ceac28a50dbbac597840006008c000301
   0003d64668f2badc76e251683394b3d5690000001351d15dd900093a8044df74b2b71f
   e667d7b908db7aeea3229e61462bdb70f46580bef9425011126bbf6c2f4212ccdacf08
   c01ddbc7608c3a1ddeb996ba9bfbd1b207281e3edc9ff61b9e800f225dc3f82bd5f794
   7e0a86bee8a3d437af93f54e61858bac877c58d3fe0ec6be54b4c75fad23e1fd
```

Atualização do ambiente no ASA e no 3750X

Nesse estágio, ambos os dispositivos têm a PAC instalada corretamente e automaticamente começam a fazer o download dos dados do ambiente do ISE. Esses dados são basicamente números de etiqueta e seus nomes. Para disparar uma atualização de ambiente no ASA, digite este comando:

```
bsns-asa5510-17# cts refresh environment-data
```

Para verificá-lo no ASA (infelizmente, você não pode ver as tags/nomes SGT específicos, mas ele é verificado mais tarde), insira este comando:

```
bsns-asa5510-17(config)# show cts environment-data
CTS Environment Data
====================
Status:                    Active
Last download attempt:     Successful
Environment Data Lifetime: 86400 secs
Last update time:          05:05:16 UTC Apr 14 2007
Env-data expires in:       0:23:56:15 (dd:hr:mm:sec)
Env-data refreshes in:     0:23:46:15 (dd:hr:mm:sec)
```

Para verificá-lo no 3750X, acione uma atualização de ambiente com este comando:

```
bsns-3750-5#cts refresh environment-data
```

Para verificar os resultados, insira este comando:

```
bsns-3750-5#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
 SGT tag = 0-01:Unknown
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.48.66.129, port 1812, A-ID C40A15A339286CEAC28A50DBBAC59784
         Status = ALIVE    flag(0x11)
         auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs
Security Group Name Table:
 0001-60 :
    0-47:Unknown
    2-47:VLAN10
    3-47:VLAN20
    4-47:VLAN100
Transport type = CTS_TRANSPORT_IP_UDP
Environment Data Lifetime = 86400 secs
Last update time = 05:33:49 UTC Thu Apr 7 2011
Env-data expires in   0:16:46:50 (dd:hr:mm:sec)
Env-data refreshes in 0:16:46:50 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running
```

Isso mostra que todas as marcas e os nomes correspondentes foram baixados corretamente.

Verificação e aplicação de autenticação de porta no 3750X

Depois que o 3750X tiver os dados do ambiente, você deverá verificar se os SGTs estão aplicados às sessões autenticadas.

Para verificar se o MS Windows 7 está autenticado corretamente, insira este comando:

```
bsns-3750-5#show authentication sessions interface g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.4eb2
          IP Address:  192.168.1.200
           User-Name:  00-50-56-99-4E-B2
              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:  10
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
                 SGT:  0002-0
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A80001000001002B67334C
```

```
     Acct Session ID:  0x00000179
              Handle:  0x94000101

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

A saída mostra que a VLAN10 é usada junto com o SGT 0002 e a permissão de DACL para todo o tráfego.

Para verificar se o MS Windows XP está autenticado corretamente, insira este comando:

```
bsns-3750-5#sh 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
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
                 SGT:  0003-0
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A80001000000FE2B67334C
     Acct Session ID:  0x00000177
              Handle:  0x540000FF

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

A saída mostra que a VLAN 20 é usada junto com o SGT 0003 e a DACL que permite todo o tráfego

Os endereços IP são detectados com a funcionalidade ip device tracking. O switch DHCP deve ser configurado para rastreamento de dhcp. Em seguida, após a resposta de DHCP de rastreamento, ele aprende o endereço IP do cliente. Para um endereço IP configurado estaticamente (como neste exemplo), a funcionalidade arp snooping é usada, e um PC deve enviar qualquer pacote para que o switch possa detectar seu endereço IP.

Para rastreamento de dispositivo, um comando oculto pode ser necessário para ativá-lo nas portas:

```
bsns-3750-5#ip device tracking interface g1/0/1
bsns-3750-5#ip device tracking interface g1/0/2
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
```

```
-------------------------------------------------------------------------
192.168.1.200   0050.5699.4eb2  10   GigabitEthernet1/0/2     ACTIVE
192.168.2.200   0050.5699.4ea1  20   GigabitEthernet1/0/1     ACTIVE

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

Atualização de políticas no 3750X

O 3750X (ao contrário do ASA) pode fazer download de políticas do ISE. Antes de fazer o download e aplicar uma política, você deve ativá-la com estes comandos:

```
bsns-3750-5(config)#cts role-based enforcement
bsns-3750-5(config)#cts role-based enforcement vlan-list 1-1005,1007-4094
```

Se você não ativá-la, a política será baixada, mas não instalada e não usada para imposição.

Para disparar uma atualização de política, insira este comando:

```
bsns-3750-5#cts refresh policy
Policy refresh in progress
```

Para verificar se a política é baixada do ISE, insira este comando:

```
bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 2:VLAN10:
       ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
       ICMP-20
       Deny IP-00
```

A saída mostra que somente a parte necessária da política é baixada.

Na nuvem CTS, o pacote contém o SGT do host de origem, e a **aplicação é feita no dispositivo de destino**. Isso significa que o pacote é encaminhado da origem para o último dispositivo, que é conectado diretamente ao host de destino. Esse dispositivo é o ponto de aplicação, pois conhece os SGTs de seus hosts conectados diretamente e sabe se o pacote de entrada com um SGT de origem deve ser permitido ou negado para o SGT de destino específico.

Essa decisão é baseada em políticas baixadas do ISE.

Neste cenário, todas as políticas são baixadas. No entanto, se você limpar a sessão de autenticação do MS Windows XP (SGT=VLAN20), não será necessário que o switch baixe qualquer política (linha) que corresponda à VLAN20, porque não há mais dispositivos desse SGT conectados ao switch.

A seção Avançado (Solução de problemas) explica como o 3750X decide quais políticas devem ser baixadas com um exame do nível do pacote.

SXP Exchange (o ASA como ouvinte e o 3750X como alto-falante)

O ASA não é compatível com SGT. Todos os quadros com SGT são descartados pelo ASA. É por isso que o 3750X não pode enviar quadros marcados com SGT para o ASA. Em vez disso, o SXP é usado. Esse protocolo permite que o ASA receba informações do switch sobre o mapeamento entre os endereços IP e o SGT. Com essas informações, o ASA pode mapear endereços IP para SGTs e tomar uma decisão com base no SGACL.

Para configurar o 3750X como um alto-falante, insira estes comandos:

```
cts sxp enable
cts sxp default source-ip 192.168.1.10
cts sxp default password cisco
cts sxp connection peer 192.168.1.1 password default mode local
```

Para configurar o ASA como um ouvinte, insira estes comandos:

```
cts sxp enable
cts sxp default password *****
cts sxp default source-ip 192.168.1.1
cts sxp connection peer 192.168.1.10 password default mode local listener
```

Para verificar se o ASA recebeu os mapeamentos, digite este comando:

```
bsns-asa5510-17# show cts sxp sgt-map ipv4 detail
Total number of IP-SGT mappings : 2
Total number of IP-SGT mappings shown: 2

SGT        : 2:VLAN10
IPv4       : 192.168.1.200
Peer IP    : 192.168.1.10
Ins Num    : 1
Status     : Active
Seq Num    : 49

SGT        : 3:VLAN20
IPv4       : 192.168.2.200
Peer IP    : 192.168.1.10
Ins Num    : 1
Status     : Active
Seq Num    : 39
```

Agora, quando o ASA recebe o pacote recebido com o endereço IP origem **192.168.1.200**, ele pode tratá-lo como se viesse de **SGT=2**. Para o endereço IP origem **192.168.200.2**, ele pode tratá-lo como se viesse de **SGT=3**. O mesmo se aplica ao endereço IP destino.

> **Observação**: o 3750X deve saber o endereço IP do host associado. Isso é feito por rastreamento de dispositivo IP. Para um endereço IP configurado estaticamente no host final, o switch deve receber qualquer pacote após a autenticação. Isso aciona o rastreamento de dispositivo IP para encontrar seu endereço IP, o que aciona uma atualização do SXP. Quando apenas o SGT é conhecido, ele não é enviado via SXP.

Filtragem de tráfego no ASA com SGT ACL

Esta é uma verificação da configuração do ASA:

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.2.1 255.255.255.0
```

Uma ACL é criada e aplicada à interface interna. Permite todo o tráfego ICMP de **SGT=3** a **SGT=2** (chamado de **VLAN10**):

```
access-list inside extended permit icmp security-group tag 3 any security-group
name VLAN10 any
access-group inside in interface inside
```

Observação: você pode usar o número ou o nome da tag.

Se você fizer ping do MS Windows XP com um endereço IP de origem de **192.168.2.200** (**SGT=3**) para o MS Windows 7 com um endereço IP de **192.168.1.200** (**SGT=2**), o ASA criará uma conexão:

```
%ASA-6-302020: Built outbound ICMP connection for faddr 192.168.1.200/0
(2:VLAN10) gaddr 192.168.2.200/512 laddr 192.168.2.200/512(3:VLAN20)
```

Quando você tentar o mesmo com Telnet, o tráfego será bloqueado:

```
Deny tcp src inside:192.168.2.200/2478(3:VLAN20) dst outside:192.168.1.200/23
(2:VLAN10) by access-group "inside"
```

Há mais opções de configuração no ASA. É possível usar uma marca de segurança e um endereço IP para a origem e o destino. Esta regra permite que o tráfego de eco ICMP da **tag SGT = 3** e o endereço IP **192.168.2.200** para a tag SGT chamada **VLAN10** e o endereço do host de destino **192.168.1.200**:

```
access-list inside extended permit icmp security-group tag 3 host 192.168.2.200
security-group name VLAN10 host 192.168.1.200 echo
```

Isso também pode ser obtido com grupos de objetos:

```
object-group security SGT-VLAN-10
 security-group name VLAN10
object-group security SGT-VLAN-20
 security-group tag 3
object-group network host1
 network-object host 192.168.1.200
object-group network host2
 network-object host 192.168.2.200
object-group service my-icmp-echo
 service-object icmp echo

access-list inside extended permit object-group my-icmp-echo
object-group-security SGT-VLAN-20 object-group host2 object-group-security
SGT-VLAN-10 object-group host1
```

Filtragem de tráfego no 3750X com políticas baixadas do ISE (RBACL)

Também é possível definir políticas locais no switch. No entanto, este exemplo apresenta políticas baixadas do ISE. As políticas definidas no ASA têm permissão para usar endereços IP e SGTs (e o nome de usuário do Ative Diretory) em uma regra. As políticas definidas no switch (local e do ISE) permitem apenas SGTs. Se você precisar usar endereços IP em suas regras, a filtragem no ASA é recomendada.

O tráfego ICMP entre o MS Windows XP e o MS Windows 7 é testado. Para isso, você deve alterar o gateway padrão do ASA para o 3750X no MS Windows. O 3750X tem interfaces de roteamento e é capaz de rotear os pacotes:

```
interface Vlan10
 ip address 192.168.1.10 255.255.255.0
!
interface Vlan20
 ip address 192.168.2.10 255.255.255.0
```

As políticas já foram baixadas do ISE. Para verificá-los, insira este comando:

```
 bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group Unknown:
       ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 2:VLAN10:
       ICMP-20
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
       ICMP-20
       Deny IP-00
```

O tráfego de VLAN10 (MS Windows 7) para VLAN20 (MS Windows XP) está sujeito à ACL ICMP-20, que é baixada do ISE:

```
bsns-3750-5#show ip access-lists ICMP-20
Role-based IP access list ICMP-20 (downloaded)
   10 permit icmp
```

Para verificar a ACL, insira este comando:

```
bsns-3750-5#show cts rbacl
CTS RBACL Policy
================
RBACL IP Version Supported: IPv4
 name   = Deny IP-00
 IP protocol version = IPV4
 refcnt = 2
 flag   = 0x41000000
 stale  = FALSE
 RBACL ACEs:
   deny ip

  name   = ICMP-20
 IP protocol version = IPV4
```

```
 refcnt = 6
 flag   = 0x41000000
 stale  = FALSE
 RBACL ACEs:
    permit icmp

 name   = Permit IP-00
 IP protocol version = IPV4
 refcnt = 2
 flag   = 0x41000000
 stale  = FALSE
 RBACL ACEs:
   permit ip
```

Para verificar o mapeamento de SGT e certificar-se de que o tráfego de ambos os hosts esteja marcado corretamente, insira este comando:

```
bsns-3750-5#show cts role-based sgt-map all
Active IP-SGT Bindings Information

IP Address              SGT     Source
============================================
192.168.1.200           2       LOCAL
192.168.2.200           3       LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 2
Total number of active   bindings = 2
```

O ICMP do MS Windows 7 (**SGT=2**) para o MS Windows XP (**SGT=3**) funciona bem com o ACL ICMP-20. Isso é verificado verificando-se os contadores para o tráfego de **2** a **3** (15 pacotes permitidos):

```
bsns-3750-5#show cts role-based counters
Role-based IPv4 counters
# '-' in hardware counters field indicates sharing among cells with identical
policies
From    To      SW-Denied       HW-Denied       SW-Permitted    HW-Permitted

2       0       0               0               1695            224
2       2       0               -               0               -

*       *       0               0               133258          132921

2       3       0               0               0               15
```

Depois de tentar usar o contador Telnet, os pacotes negados aumentam (não é permitido na ACL ICMP-20):

```
bsns-3750-5#show cts role-based counters
Role-based IPv4 counters
# '-' in hardware counters field indicates sharing among cells with identical
policies
From    To      SW-Denied       HW-Denied       SW-Permitted    HW-Permitted

2       0       0               0               1695            224
```

```
2       2       0               -               0               -

*       *       0               0               133281          132969

2       3       0               2               0               15
```

Observação: o caractere de estrela (*) mostrado na saída está relacionado a todo o tráfego que não está marcado (essa coluna e linha são chamadas de **desconhecidas** na Matriz no ISE e usam o número de marca **0**).

Quando você tem uma entrada de ACL com a palavra-chave log (definida no ISE), os detalhes do pacote correspondente e as ações tomadas são registrados como em qualquer ACL com a palavra-chave log.

Verificar

Consulte as seções de configuração individuais para ver os procedimentos de verificação.

Troubleshoot

Provisionamento de PAC

Problemas podem aparecer quando você usa o fornecimento automático de PAC. Lembre-se de usar a palavra-chave **pac** para o servidor RADIUS. O fornecimento automático de PAC no 3750X usa o método EAP-FAST com o Extensible Authentication Protocol com o método interno usando a autenticação Challenge Handshake Authentication Protocol (EAP-MSCHAPv2) da Microsoft. Ao depurar, você vê várias mensagens RADIUS que fazem parte da negociação EAP-FAST usada para criar o túnel seguro, que usa EAP-MSCHAPv2 com a ID e a senha configuradas para autenticação.

A primeira solicitação RADIUS usa AAA **service-type=cts-pac-provisioning** para notificar o ISE de que essa é uma solicitação PAC.

```
bsns-3750-5#debug cts provisioning events
bsns-3750-5#debug cts provisioning packets

*Mar  1 09:55:11.997: CTS-provisioning: New session socket: src=
10.48.66.109:57516 dst=10.48.66.129:1645
*Mar  1 09:55:11.997: CTS-provisioning: Sending EAP Response/Identity to
10.48.66.129
*Mar  1 09:55:11.997: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:11.997: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:11.997: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.006: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.006: CTS-provisioning: Sending EAPFAST response to
10.48.66.129
*Mar  1 09:55:12.006: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.106: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.115: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
```

```
*Mar  1 09:55:12.744: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.744: CTS-provisioning: Sending EAPFAST response to
10.48.66.129
*Mar  1 09:55:12.744: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.844: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.844: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.853: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.853: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.853: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.853: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.861: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.861: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.861: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.861: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.878: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.878: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.886: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.886: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.886: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.895: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.895: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.895: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.895: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.903: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.912: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.912: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.920: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.920: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.920: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.928: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.928: CTS-provisioning: Received RADIUS challenge from
10.48.66.129.
*Mar  1 09:55:12.970: CTS-pac-refresh: PAC C40A15A339286CEAC28A50DBBAC59784
refresh timer has been set for 20y30w
*Mar  1 09:55:12.970: CTS-provisioning: Ignoring key data.
*Mar  1 09:55:12.979: CTS-provisioning: Received TX_PKT from EAP method
*Mar  1 09:55:12.979: CTS-provisioning: Sending EAPFAST response to 10.48.66.129
*Mar  1 09:55:12.979: CTS-provisioning: OUTGOING RADIUS msg to 10.48.66.129:
*Mar  1 09:55:12.995: CTS-provisioning: INCOMING RADIUS msg from 10.48.66.129:
*Mar  1 09:55:12.995: CTS-provisioning: Received RADIUS reject from 10.48.66.129.
*Mar  1 09:55:12.995: CTS-provisioning: Successfully obtained PAC for A-ID
c40a15a339286ceac28a50dbbac59784
*Mar  1 09:55:12.995: CTS-provisioning: cts_provi_server_cleanup: 10.48.66.129
*Mar  1 09:55:12.995: CTS-provisioning: work complete, process terminating.
```

A **rejeição de RADIUS** no final da saída é esperada, já que você já recebeu PAC e não seguiu com um processo de autenticação adicional.

Lembre-se de que a PAC é necessária para todas as outras comunicações com o ISE. Mas, se você não o tiver, o switch ainda tentará uma atualização de ambiente ou política quando for configurado. Em seguida, ele não anexa **cts-opaqueue** (PAC) nas Solicitações RADIUS, o que causa as falhas.

Se a chave PAC estiver errada, esta mensagem de erro será exibida no ISE:

```
The Message-Authenticator RADIUS attribute is invalid
```

Você também verá esta saída de depurações (**debug cts provisioning + debug radius**) no switch se a chave PAC estiver errada:

```
Apr 20 10:07:11.768: CTS-provisioning: Sending EAP Response/Identity t
Apr 20 10:07:15.325: RADIUS(0000024B): Request timed out!
Apr 20 10:07:15.325: RADIUS: No response from (10.62.84.224:1645,1646) for
id 1645/37
```

Se você usar a convenção de **servidor radius** moderno, isso exibirá:

```
radius server KRK-ISE
 address ipv4 10.62.84.224 auth-port 1645 acct-port 1646
 pac key CISCO
```

> **Observação**: você deve usar no ISE a mesma senha usada nas **Configurações de autenticação do dispositivo**.

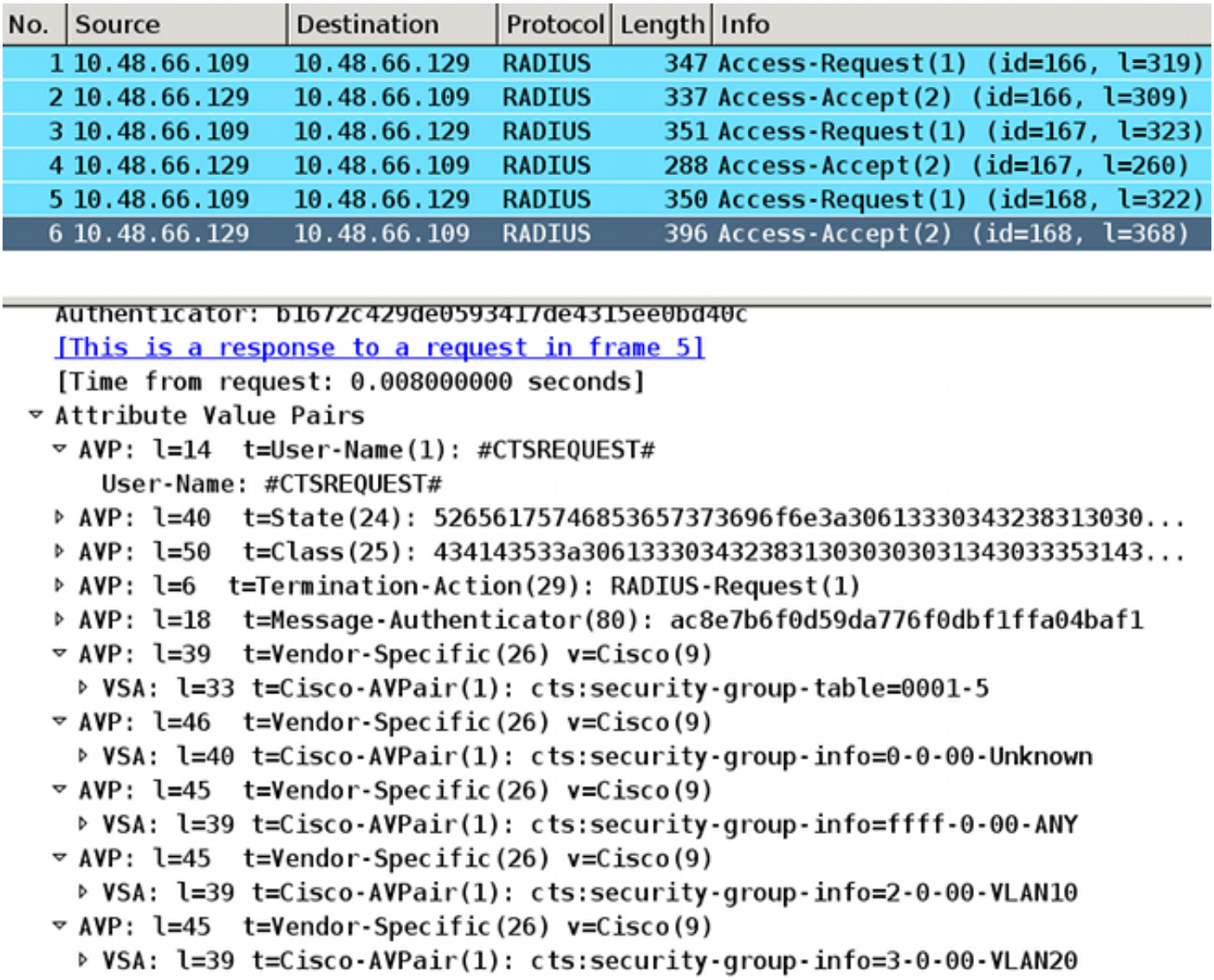
Após o fornecimento bem-sucedido de PAC, isso é exibido no ISE:

Authentication Summary	
Logged At:	June 26,2013 1:36:32.676 PM
RADIUS Status:	PAC provisioned
NAS Failure:	
Username:	3750
MAC/IP Address:	BC:16:65:25:A5:00
Network Device:	3750X : 10.48.66.109 :
Allowed Protocol:	NDAC_SGT_Service
Identity Store:	Internal CTS Devices
Authorization Profiles:	
SGA Security Group:	
Authentication Protocol :	EAP-FAST(EAP-MSCHAPv2)

Atualização de ambiente

A atualização do ambiente é usada para obter dados básicos do ISE, que inclui o número e o nome SGT. O nível do pacote mostra que são apenas três solicitações RADIUS e respostas com atributos.

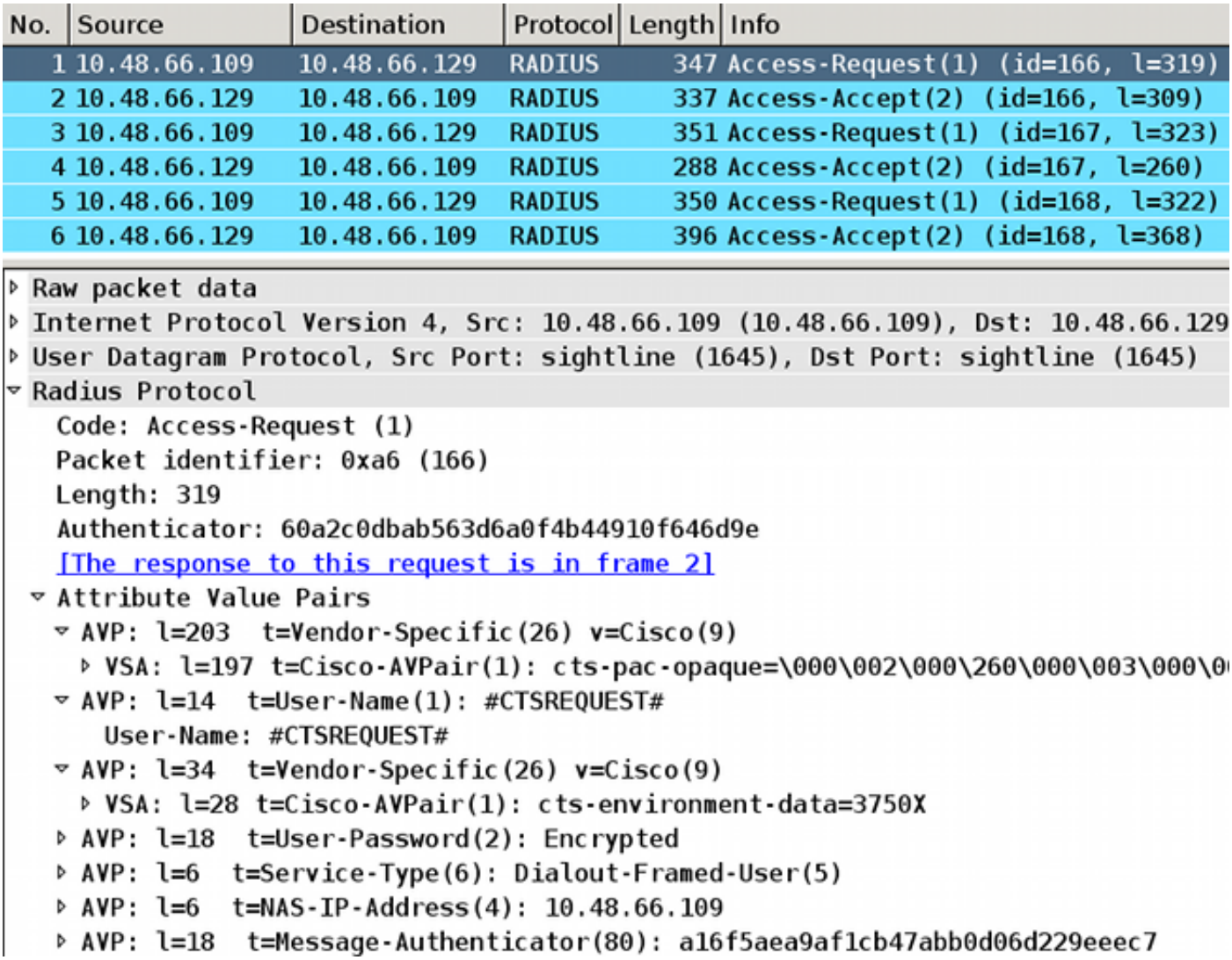
Para a primeira solicitação, o switch recebe o nome **CTSServerlist**. Para o segundo, ele recebe os detalhes dessa lista e, para o último, recebe todos os SGTs com marcas e nomes:



No.	Source	Destination	Protocol	Length	Info
1	10.48.66.109	10.48.66.129	RADIUS	347	Access-Request(1) (id=166, l=319)
2	10.48.66.129	10.48.66.109	RADIUS	337	Access-Accept(2) (id=166, l=309)
3	10.48.66.109	10.48.66.129	RADIUS	351	Access-Request(1) (id=167, l=323)
4	10.48.66.129	10.48.66.109	RADIUS	288	Access-Accept(2) (id=167, l=260)
5	10.48.66.109	10.48.66.129	RADIUS	350	Access-Request(1) (id=168, l=322)
6	10.48.66.129	10.48.66.109	RADIUS	396	Access-Accept(2) (id=168, l=368)

Aqui você vê o padrão **SGT 0**, **ffff**, e também dois definidos pelo cliente: a marca SGT 2 é chamada de **VLAN10** e a marca SGT 3 é chamada de **VLAN20**.

> **Observação**: todas as solicitações RADIUS incluem **cts-pac-opaque** como resultado do fornecimento de PAC.



No.	Source	Destination	Protocol	Length	Info
1	10.48.66.109	10.48.66.129	RADIUS	347	Access-Request(1) (id=166, l=319)
2	10.48.66.129	10.48.66.109	RADIUS	337	Access-Accept(2) (id=166, l=309)
3	10.48.66.109	10.48.66.129	RADIUS	351	Access-Request(1) (id=167, l=323)
4	10.48.66.129	10.48.66.109	RADIUS	288	Access-Accept(2) (id=167, l=260)
5	10.48.66.109	10.48.66.129	RADIUS	350	Access-Request(1) (id=168, l=322)
6	10.48.66.129	10.48.66.109	RADIUS	396	Access-Accept(2) (id=168, l=368)

No 3750X, você deve ver depurações para todas as três respostas RADIUS e as listas correspondentes, os detalhes da lista e a lista interna SGT específica:

```
bsns-3750-5#debug cts environment-data all

*Mar  1 10:05:07.454: CTS env-data&colon; cleanup mcast SGT table
*Mar  1 10:05:18.057: CTS env-data&colon; Force environment-data refresh
*Mar  1 10:05:18.057: CTS env-data&colon; download transport-type =
CTS_TRANSPORT_IP_UDP
*Mar  1 10:05:18.057:     cts_env_data START: during state env_data_complete,
got event 0(env_data_request)
*Mar  1 10:05:18.057: @@@ cts_env_data START: env_data_complete ->
env_data_waiting_rsp
*Mar  1 10:05:18.057: env_data_waiting_rsp_enter: state = WAITING_RESPONSE
*Mar  1 10:05:18.057: env_data_request_action: state = WAITING_RESPONSE
*Mar  1 10:05:18.057: cts_env_data_is_complete: FALSE, req(x0), rec(x0),
expect(x81), complete1(x85), complete2(xB5), complete3(x28B5)
*Mar  1 10:05:18.057: cts_aaa_req_setup: (CTS env-data)Private group appears DEAD,
attempt public group
*Mar  1 10:05:18.057: cts_aaa_req_setup: (CTS env-data)CTS_TRANSPORT_IP_UDP
*Mar  1 10:05:18.057: cts_aaa_req_setup: (CTS env-data)AAA req(x7C3DF10)
*Mar  1 10:05:18.057: cts_aaa_attr_add: AAA req(0x7C3DF10)
*Mar  1 10:05:18.057:   username = #CTSREQUEST#
*Mar  1 10:05:18.057:   cts-environment-data = 3750X
*Mar  1 10:05:18.057: cts_aaa_req_send: AAA req(0x7C3DF10) successfully sent to AAA.
*Mar  1 10:05:18.083: cts_aaa_callback: (CTS env-data)AAA req(0x7C3DF10)
response success
```

```
*Mar  1 10:05:18.083:   AAA attr: Unknown type (447).
*Mar  1 10:05:18.083:   AAA attr: Unknown type (220).
*Mar  1 10:05:18.083:   AAA attr: Unknown type (275).
*Mar  1 10:05:18.083:   AAA attr: server-list = CTSServerList1-0001.
*Mar  1 10:05:18.083:   AAA attr: security-group-tag = 0000-00.
*Mar  1 10:05:18.083:   AAA attr: environment-data-expiry = 86400.
*Mar  1 10:05:18.083:   AAA attr: security-group-table = 0001-5.
*Mar  1 10:05:18.083: CTS env-data&colon; Receiving AAA attributes
 CTS_AAA_SLIST
    slist name(CTSServerList1) received in 1st Access-Accept
   slist name(CTSServerList1) created
 CTS_AAA_SECURITY_GROUP_TAG - SGT = unicast-unknown-00
 CTS_AAA_ENVIRONMENT_DATA_EXPIRY = 86400.
 CTS_AAA_SGT_NAME_LIST
   table(0001) received in 1st Access-Accept
   old name(), gen()
   new name(0001), gen(50)
 CTS_AAA_DATA_END
*Mar  1 10:05:18.083:     cts_env_data WAITING_RESPONSE: during state
env_data_waiting_rsp, got event 1(env_data_received)
*Mar  1 10:05:18.083: @@@ cts_env_data WAITING_RESPONSE: env_data_waiting_rsp ->
env_data_assessing
*Mar  1 10:05:18.083: env_data_assessing_enter: state = ASSESSING
*Mar  1 10:05:18.083: env_data_assessing_action: state = ASSESSING
*Mar  1 10:05:18.083: cts_env_data_is_complete: FALSE, req(x1089), rec(xC83),
expect(x28B5), complete1(x85), complete2(xB5), complete3(x28B5)
*Mar  1 10:05:18.083:     cts_env_data ASSESSING: during state env_data_assessing,
got event 3(env_data_incomplete)
*Mar  1 10:05:18.083: @@@ cts_env_data ASSESSING: env_data_assessing ->
env_data_waiting_rsp
*Mar  1 10:05:18.083: env_data_waiting_rsp_enter: state = WAITING_RESPONSE
*Mar  1 10:05:18.083: env_data_request_action: state = WAITING_RESPONSE
*Mar  1 10:05:18.083: cts_env_data_is_complete: FALSE, req(x1089), rec(xC83),
expect(x28B5), complete1(x85), complete2(xB5), complete3(x28B5)
*Mar  1 10:05:18.083: cts_aaa_req_setup: (CTS env-data)Private group appears DEAD,
attempt public group
*Mar  1 10:05:18.083: cts_aaa_req_setup: (CTS env-data)CTS_TRANSPORT_IP_UDP
*Mar  1 10:05:18.083: cts_aaa_req_setup: (CTS env-data)AAA req(x792FFD0)
*Mar  1 10:05:18.083: cts_aaa_attr_add: AAA req(0x792FFD0)
*Mar  1 10:05:18.091:   username = #CTSREQUEST#
*Mar  1 10:05:18.091:   cts-server-list = CTSServerList1
*Mar  1 10:05:18.091: cts_aaa_req_send: AAA req(0x792FFD0) successfully sent to AAA.
*Mar  1 10:05:18.099: cts_aaa_callback: (CTS env-data)AAA req(0x792FFD0)
response success
*Mar  1 10:05:18.099:   AAA attr: Unknown type (447).
*Mar  1 10:05:18.099:   AAA attr: Unknown type (220).
*Mar  1 10:05:18.099:   AAA attr: Unknown type (275).
*Mar  1 10:05:18.099:   AAA attr: server-list = CTSServerList1-0001.
*Mar  1 10:05:18.099:   AAA attr: server = c40a15a339286ceac28a50dbbac59784:
10.48.66.129:1812.
*Mar  1 10:05:18.099: CTS env-data&colon; Receiving AAA attributes
 CTS_AAA_SLIST
    2nd Access-Accept slist name(CTSServerList1), gen(0001)
 CTS_AAA_SERVERS
   server (c40a15a339286ceac28a50dbbac59784:10.48.66.129:1812) added
 CTS_AAA_DATA_END
*Mar  1 10:05:18.099:     cts_env_data WAITING_RESPONSE: during state
env_data_waiting_rsp, got event 1(env_data_received)
*Mar  1 10:05:18.099: @@@ cts_env_data WAITING_RESPONSE: env_data_waiting_rsp ->
env_data_assessing
*Mar  1 10:05:18.099: env_data_assessing_enter: state = ASSESSING
*Mar  1 10:05:18.099: env_data_assessing_action: state = ASSESSING
*Mar  1 10:05:18.099: cts_env_data_is_complete: FALSE, req(x108D), rec(xC87),
expect(x28B5), complete1(x85), complete2(xB5), complete3(x28B5)
```

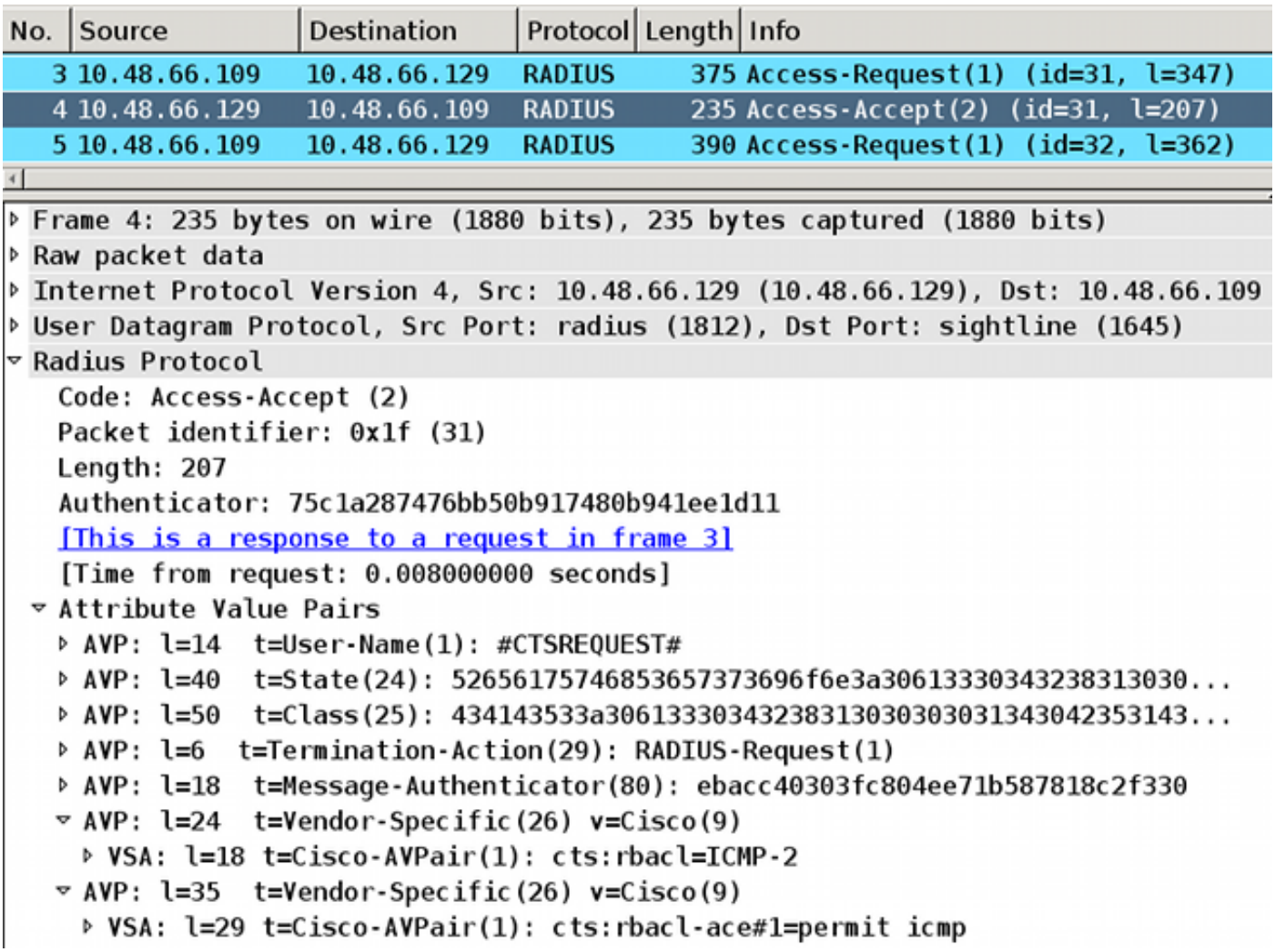
```
*Mar  1 10:05:18.099:     cts_env_data ASSESSING: during state env_data_assessing,
got event 3(env_data_incomplete)
*Mar  1 10:05:18.099: @@@ cts_env_data ASSESSING: env_data_assessing ->
env_data_waiting_rsp
*Mar  1 10:05:18.099: env_data_waiting_rsp_enter: state = WAITING_RESPONSE
*Mar  1 10:05:18.099: env_data_request_action: state = WAITING_RESPONSE
*Mar  1 10:05:18.099: cts_env_data_is_complete: FALSE, req(x108D), rec(xC87),
expect(x28B5), complete1(x85), complete2(xB5), complete3(x28B5)
*Mar  1 10:05:18.099: cts_aaa_req_setup: (CTS env-data)Using private server group
*Mar  1 10:05:18.099: cts_aaa_req_setup: (CTS env-data)CTS_TRANSPORT_IP_UDP
*Mar  1 10:05:18.099: cts_aaa_req_setup: (CTS env-data)AAA req(x7A6C4AC)
*Mar  1 10:05:18.099: cts_aaa_attr_add: AAA req(0x7A6C4AC)
*Mar  1 10:05:18.099:   username = #CTSREQUEST#
*Mar  1 10:05:18.099:   cts-security-group-table = 0001
*Mar  1 10:05:18.099: cts_aaa_req_send: AAA req(0x7A6C4AC) successfully sent to AAA.
*Mar  1 10:05:18.108: cts_aaa_callback: (CTS env-data)AAA req(0x7A6C4AC)
response success
*Mar  1 10:05:18.108:   AAA attr: Unknown type (447).
*Mar  1 10:05:18.108:   AAA attr: Unknown type (220).
*Mar  1 10:05:18.108:   AAA attr: Unknown type (275).
*Mar  1 10:05:18.108:   AAA attr: security-group-table = 0001-5.
*Mar  1 10:05:18.108:   AAA attr: security-group-info = 0-0-00-Unknown.
*Mar  1 10:05:18.108:   AAA attr: security-group-info = ffff-0-00-ANY.
*Mar  1 10:05:18.108:   AAA attr: security-group-info = 2-0-00-VLAN10.
*Mar  1 10:05:18.108:   AAA attr: security-group-info = 3-0-00-VLAN20.
*Mar  1 10:05:18.108:  CTS env-data&colon; Receiving AAA attributes
 CTS_AAA_SGT_NAME_LIST
   table(0001) received in 2nd Access-Accept
   old name(0001), gen(50)
   new name(0001), gen(50)
 CTS_AAA_SGT_NAME_INBOUND - SGT = unicast-unknown-00
   flag (128) server name (Unknown) added
  name (0001), request (1), receive (1)
  Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
 CTS_AAA_SGT_NAME_INBOUND - SGT = unicast-default-00
   flag (128) server name (ANY) added
  name (0001), request (1), receive (1)
  Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
 CTS_AAA_SGT_NAME_INBOUND - SGT = 2-00
   flag (128) server name (VLAN10) added
  name (0001), request (1), receive (1)
  Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
 CTS_AAA_SGT_NAME_INBOUND - SGT = 3-00
   flag (128) server name (VLAN20) added
  name (0001), request (1), receive (1)
  Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
 CTS_AAA_DATA_END
*Mar  1 10:05:18.108:     cts_env_data WAITING_RESPONSE: during state
env_data_waiting_rsp, got event 1(env_data_received)
*Mar  1 10:05:18.108: @@@ cts_env_data WAITING_RESPONSE: env_data_waiting_rsp ->
env_data_assessing
*Mar  1 10:05:18.108: env_data_assessing_enter: state = ASSESSING
*Mar  1 10:05:18.108: env_data_assessing_action: state = ASSESSING
*Mar  1 10:05:18.116: cts_env_data_is_complete: TRUE, req(x2085), rec(x2C87),
expect(x81), complete1(x85), complete2(xB5), complete3(x28B5)
*Mar  1 10:05:18.116:     cts_env_data ASSESSING: during state env_data_assessing,
got event 4(env_data_complete)
*Mar  1 10:05:18.116: @@@ cts_env_data ASSESSING: env_data_assessing ->
env_data_complete
*Mar  1 10:05:18.116: env_data_complete_enter: state = COMPLETE
*Mar  1 10:05:18.116: env_data_install_action: state = COMPLETE
```

Atualização de política

A atualização de política é suportada apenas no switch. É semelhante à atualização do ambiente. Essas são simplesmente Solicitações e Aceitações RADIUS.

O switch solicita todas as ACLs dentro da lista padrão. Em seguida, para cada ACL que não esteja atualizada (ou que não exista), ele envia outra solicitação para obter os detalhes.

Aqui está um exemplo de resposta quando você solicita uma ACL ICMP-20:



Lembre-se de que você deve ter a **imposição baseada em função cts** configurada para aplicar essa ACL.

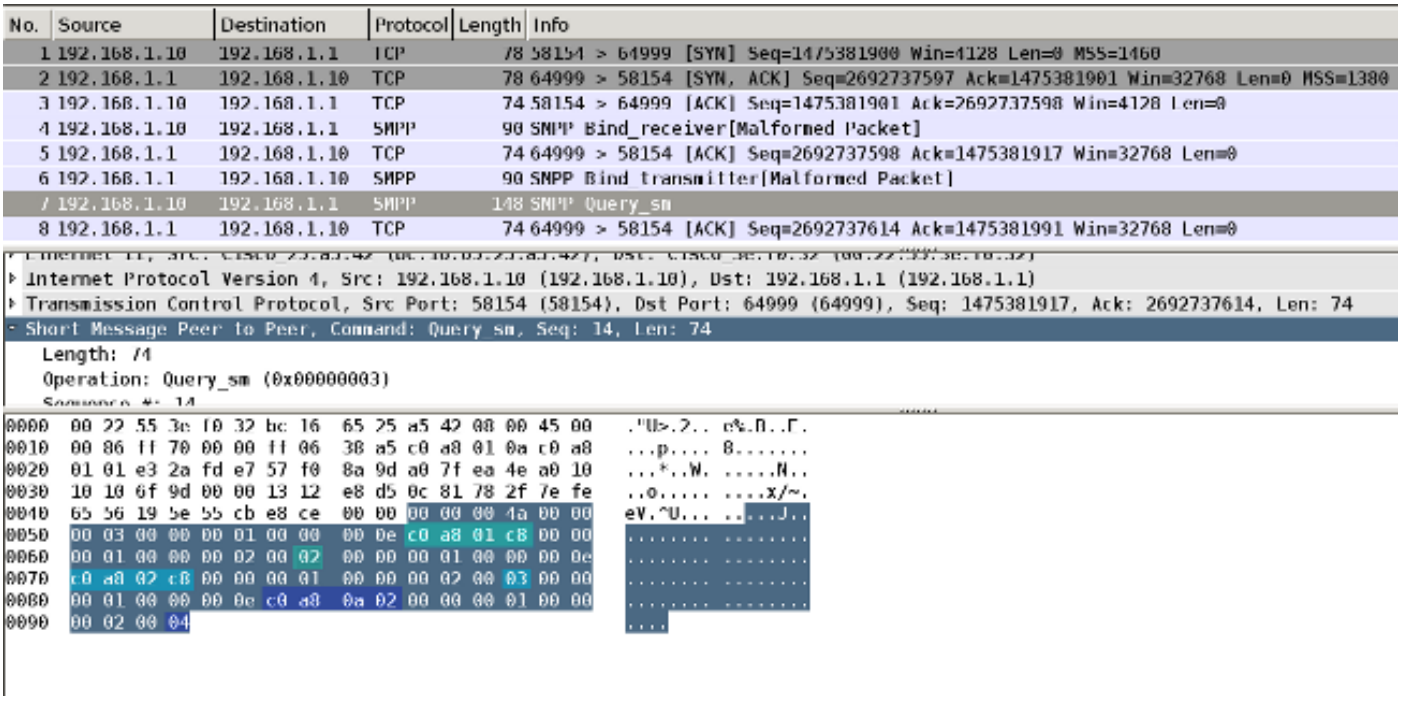
As depurações indicam se há alterações (com base no ID de geração). Nesse caso, você pode desinstalar a regra antiga, se necessário, e instalar uma nova. Isso inclui programação ASIC (suporte de hardware).

```
bsns-3750-5#debug cts all

Mar 30 02:39:37.151:  CTS authz entry: peer(Unknown-2) Receiving AAA attributes
   rcv rbacl list: flags: req(81)rcv(0)wait(80)prev(0)install(880)
    - SGT = 2-01:VLAN10
    - SGT = 2-01:VLAN10
   current arg_cnt=8, expected_num_args=11
   3rd Access-Accept rbacl received name(ICMP), gen(20)
   received_policyp->sgt(2-01:VLAN10)
   existing sgt_policy(73FFDB4) sgt(2-01:VLAN10)
   RBACL name(ICMP-20)flag(40000000) already exists
```

```
  acl_listp(740266C) old_acl_infop(0),exist_rbacl_type(0)
 CTS_AAA_AUTHORIZATION_EXPIRY = 86400.
 CTS_AAA_DATA_END

Mar 30 02:39:37.176: cts_authz_entry_complete_action: Policy download complete -
peer(Unknown-2) SGT(2-01:VLAN10) status(RBACL-POLICY SUCCEEDED)
Mar 30 02:39:37.176: cts_authz_rbacl_uninstall_cb:
Mar 30 02:39:37.176: uninstall cb_ctx:
Mar 30 02:39:37.176:   session_hdl = F1000003
Mar 30 02:39:37.176:   sgt_policyp = 73FFDB4, sgt=(2-01:VLAN10), magic(BABECABB)
Mar 30 02:39:37.176:   ip_version  = IPV6
Mar 30 02:39:37.176:   src-or-dst  = BOTH
Mar 30 02:39:37.176:   wait_rbm_install_ip_ver(0)
Mar 30 02:39:37.176:   wait_rbm_uninstall_ip_ver(C0000000)
Mar 30 02:39:37.176: cts_authz_rbacl_uninstall_cb:
Mar 30 02:39:37.176: uninstall cb_ctx:
Mar 30 02:39:37.176:   session_hdl = F1000003
Mar 30 02:39:37.176:   sgt_policyp = 73FFDB4, sgt=(2-01:VLAN10), magic(BABECABB)
Mar 30 02:39:37.176:   ip_version  = IPV4
Mar 30 02:39:37.176:   src-or-dst  = BOTH
Mar 30 02:39:37.176:   wait_rbm_install_ip_ver(0)
Mar 30 02:39:37.176:   wait_rbm_uninstall_ip_ver(40000000)

Mar 30 02:39:37.210: install cb_ctx:
Mar 30 02:39:37.210:   session_hdl = F1000003
Mar 30 02:39:37.210:   sgt_policyp = 73FFDB4, sgt=(2-01:VLAN10), magic(BABECABB)
Mar 30 02:39:37.210:   ip_version  = IPV6
Mar 30 02:39:37.210:   src-or-dst  = SRC
Mar 30 02:39:37.210:   wait_rbm_install_ip_ver(C0000000)
Mar 30 02:39:37.210:   wait_rbm_uninstall_ip_ver(0)
Mar 30 02:39:37.210: cts_authz_rbacl_install_cb: Waiting for more RBM callback
for remaining IP version(40000000) RBACL policy(73FFDB4) for SGT(2-01:VLAN10)
flag(41400001)
Mar 30 02:39:37.210: cts_authz_rbacl_install_cb:
Mar 30 02:39:37.210: install cb_ctx:
Mar 30 02:39:37.210:   session_hdl = F1000003
Mar 30 02:39:37.210:   sgt_policyp = 73FFDB4, sgt=(2-01:VLAN10), magic(BABECABB)
Mar 30 02:39:37.210:   ip_version  = IPV4
Mar 30 02:39:37.210:   src-or-dst  = SRC
Mar 30 02:39:37.210:   wait_rbm_install_ip_ver(40000000)
Mar 30 02:39:37.210:   wait_rbm_uninstall_ip_ver(0)
Mar 30 02:39:37.210: cts_authz_rbacl_install_cb: Program RBACL policy(73FFDB4)
for SGT(2-01:VLAN10) flag(41400001) success
```

Exchange do SXP

A atualização do SXP é acionada pelo código de rastreamento de dispositivo IP que encontra o endereço IP do dispositivo. Em seguida, o protocolo SMPP (Short Message Peer-to-Peer) é usado para enviar atualizações. Ele usa a **opção TCP 19** para autenticação, que é a mesma que o Border Gateway Protocol (BGP). O payload SMPP não está criptografado. O Wireshark não tem um decodificador adequado para o payload SMPP, mas é fácil encontrar dados dentro dele:



- O primeiro, **c0 a8 01 c8**, é **192.168.1.200** e tem **tag 2**.
- O segundo, **c0 a8 02 c8**, é **192.168.2.200** e tem **tag 3**.
- O terceiro, **c0 a8 0a 02,** é **192.168.10.2** e tem **tag 4** (este foi usado para testar o telefone **SGT=4**)

Aqui estão algumas depurações no 3750X depois que o rastreamento do dispositivo IP encontra o endereço IP do MS Windows 7:

```
bsns-3750-5#debug cts sxp message
bsns-3750-5#debug cts sxp internal
bsns-3750-5#debug cts sxp conn
bsns-3750-5#debug cts sxp mdb
bsns-3750-5#debug cts sxp error

Apr  7 00:39:06.874: CTS-SXP-CONN:sxp_process_message_event = CTS_SXPMSG_REQUEST
Apr  7 00:39:06.874: CTS-SXP-CONN:sxp_process_request  CTS_SXPMSG_REQ_CONN_NVGEN
Apr  7 00:39:06.874: CTS-SXP-CONN:cts_get_next_sxpconn_cli
Apr  7 00:39:06.874: CTS-SXP-CONN:cts_get_next_sxpconn_cli
Apr  7 00:39:06.874: CTS-SXP-INTNL:sxp_process_request boolean set
Apr  7 00:39:06.874: CTS-SXP-INTNL:sxp_send_request set boolean after
Apr  7 00:40:05.418: CTS-SXP-CONN:is_cts_sxp_rf_active
Apr  7 00:40:05.418: CTS-SXP-MDB:sxp_export_ipsgt_change 192.168.1.200/32 add 1
```

Aqui estão as depurações correspondentes no ASA:

```
bsns-asa5510-17# debug cts sxp all

%ASA-7-776018: CTS SXP: Binding 192.168.1.200->2:VLAN10 from peer 192.168.1.10
(instance 1) added in SXP database.
%ASA-7-776019: CTS SXP: Binding 192.168.1.200->2:VLAN10 added. Update binding
manager.
%ASA-6-776251: CTS SGT-MAP: Binding 192.168.1.200->2:VLAN10 from SXP added to
binding manager.
%ASA-7-776014: CTS SXP: SXP received binding forwarding request (add) binding
192.168.1.200->2:VLAN10.
```

Para ver mais depurações no ASA, você pode habilitar o nível de verbosidade da depuração:

```
bsns-asa5510-17# debug cts condition level detail
debug cts condition level detail is enable
```

SGACL no ASA

Depois que o ASA instalar corretamente os mapeamentos SGT recebidos pelo SXP, a ACL de grupos de segurança funcionará bem. Quando você encontrar problemas com o mapeamento, insira:

```
bsns-asa5510-17# debug cts sgt-map
```

A ACL com o grupo de segurança funciona exatamente da mesma forma que para o endereço IP ou a identidade do usuário. Os registros revelam problemas e a entrada exata da ACL que foi atingida.

Este é um ping do MS Windows XP para o MS Windows 7 que mostra que o packet tracer funciona corretamente:

```
bsns-asa5510-17# packet-tracer input inside icmp 192.168.2.200 8 0 192.168.1.200
detailed
<output ommitted>

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group inside in interface inside
access-list inside extended permit icmp security-group tag 3 any security-group
name VLAN10 any
Additional Information:
 Forward Flow based lookup yields rule:
 in  id=0xaaf2ae80, priority=13, domain=permit, deny=false
       hits=185, user_data=0xaa2f5040, cs_id=0x0, use_real_addr, flags=0x0,
protocol=1
       src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0, tag=3:VLAN20
       dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, tag=2:VLAN10, dscp=0x0
       input_ifc=inside, output_ifc=any

<output ommitted>
```

Informações Relacionadas

- Guia de configuração do Cisco TrustSec para 3750
- Guia de configuração do Cisco TrustSec para ASA 9.1
- Implantação e roadmap do Cisco TrustSec
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.