Exemplo de Configuração de Nuvem TrustSec com MACsec 802.1x no Switch Catalyst 3750X Series

Contents

Introduction

Este artigo descreve as etapas necessárias para configurar uma nuvem Cisco TrustSec (CTS) com criptografia de link entre dois switches Catalyst 3750X Series (3750X).

Este artigo explica o processo de criptografia Media Access Control Security (MACsec) de switch a switch que usa o Security Association Protocol (SAP). Esse processo usa o modo IEEE 802.1x em vez do modo manual.

Esta é uma lista das etapas envolvidas:

- Fornecimento de PAC (Protected Access Credential) para dispositivos semente e não semente
- Autenticação NDAC (Network Device Admission Control) e negociação MACsec com SAP para gerenciamento de chaves
- Atualização de ambiente e política

- Autenticação de porta para clientes
- Marcação de tráfego com o Security Group Tag (SGT)
- Aplicação de políticas com a ACL do grupo de segurança (SGACL)

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico dos componentes CTS
- Conhecimento básico da configuração CLI dos switches Catalyst
- Experiência com a configuração do Identity Services Engine (ISE)

Componentes Utilizados

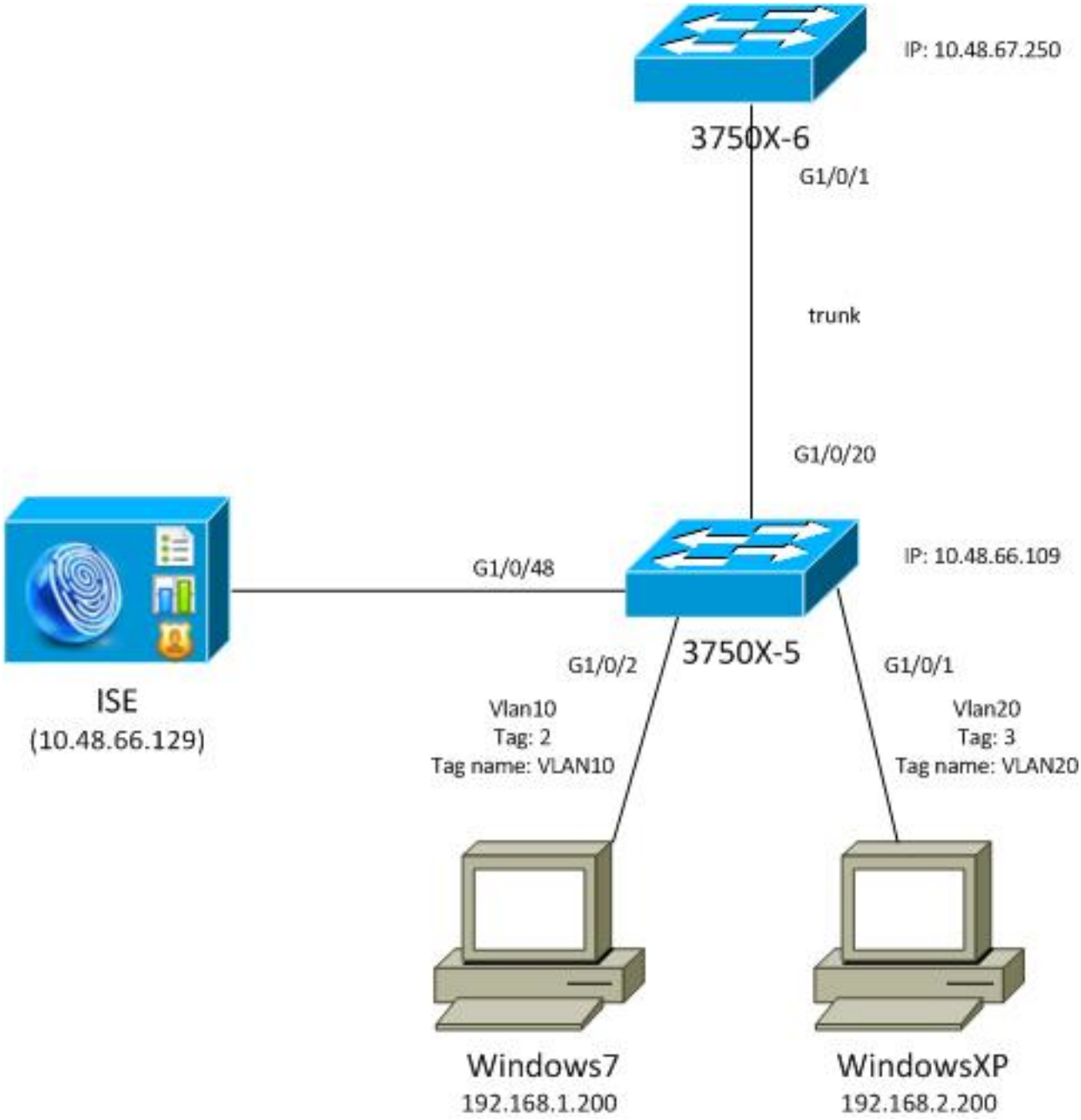
As informações neste documento são baseadas nestas versões de software e hardware:

- Microsoft (MS) Windows 7 e MS Windows XP
- Software 3750X, versões 15.0 e posteriores
- Software 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



Neste diagrama de topologia de rede, o switch 3750X-5 é o dispositivo semente que conhece o endereço IP do ISE e baixa automaticamente a PAC usada para autenticação subsequente na nuvem CTS. O dispositivo de seed atua como um autenticador 802.1x para dispositivos não-seed. O switch Cisco Catalyst 3750X-6 Series (3750X-6) é o dispositivo não semente. Ele atua como um suplicante 802.1x para o dispositivo de seed. Depois que o dispositivo não semente é autenticado no ISE por meio do dispositivo semente, é permitido o acesso à nuvem CTS. Após uma autenticação bem-sucedida, o status da porta 802.1x no switch 3750X-5 é alterado para **autenticado** e a criptografia MACsec é negociada. O tráfego entre os switches é marcado com SGT e criptografado.

Esta lista resume o fluxo de tráfego esperado:

- O seed 3750X-5 conecta-se ao ISE e faz o download da PAC, que é usada posteriormente para uma atualização de ambiente e política.
- O 3750X-6 não semente executa a autenticação 802.1x com a função de solicitante para autenticar/autorizar e baixar a PAC do ISE.
- O 3750X-6 executa uma segunda sessão 802.1x Extensible Authentication Protocol-Flexible

Authentication via Secure Protocol (EAP-FAST) para se autenticar no túnel protegido com base na PAC.
- O 3750X-5 faz o download de políticas SGA para si mesmo e em nome do 3750X-6.
- Uma sessão SAP ocorre entre o 3750X-5 e o 3750X-6, as cifras MACsec são negociadas e a política é trocada.
- O tráfego entre os switches é marcado e criptografado.

Configurar switches semente e não semente

O dispositivo semente (3750X-5) é configurado para usar o ISE como um servidor RADIUS para CTS:

```
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

cts authorization list ise

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
```

A aplicação de RBACL (Lista de Controle de Acesso Baseada em Função) e SGACL (Lista de Controle de Acesso Baseada em Grupo de Segurança) está habilitada (elas serão usadas posteriormente):

```
cts role-based enforcement
cts role-based enforcement vlan-list 1-1005,1007-4094
```

O dispositivo não semente (3750X-6) é configurado somente para Autenticação, Autorização e Tarifação (AAA) sem a necessidade de autorização RADIUS ou CTS:

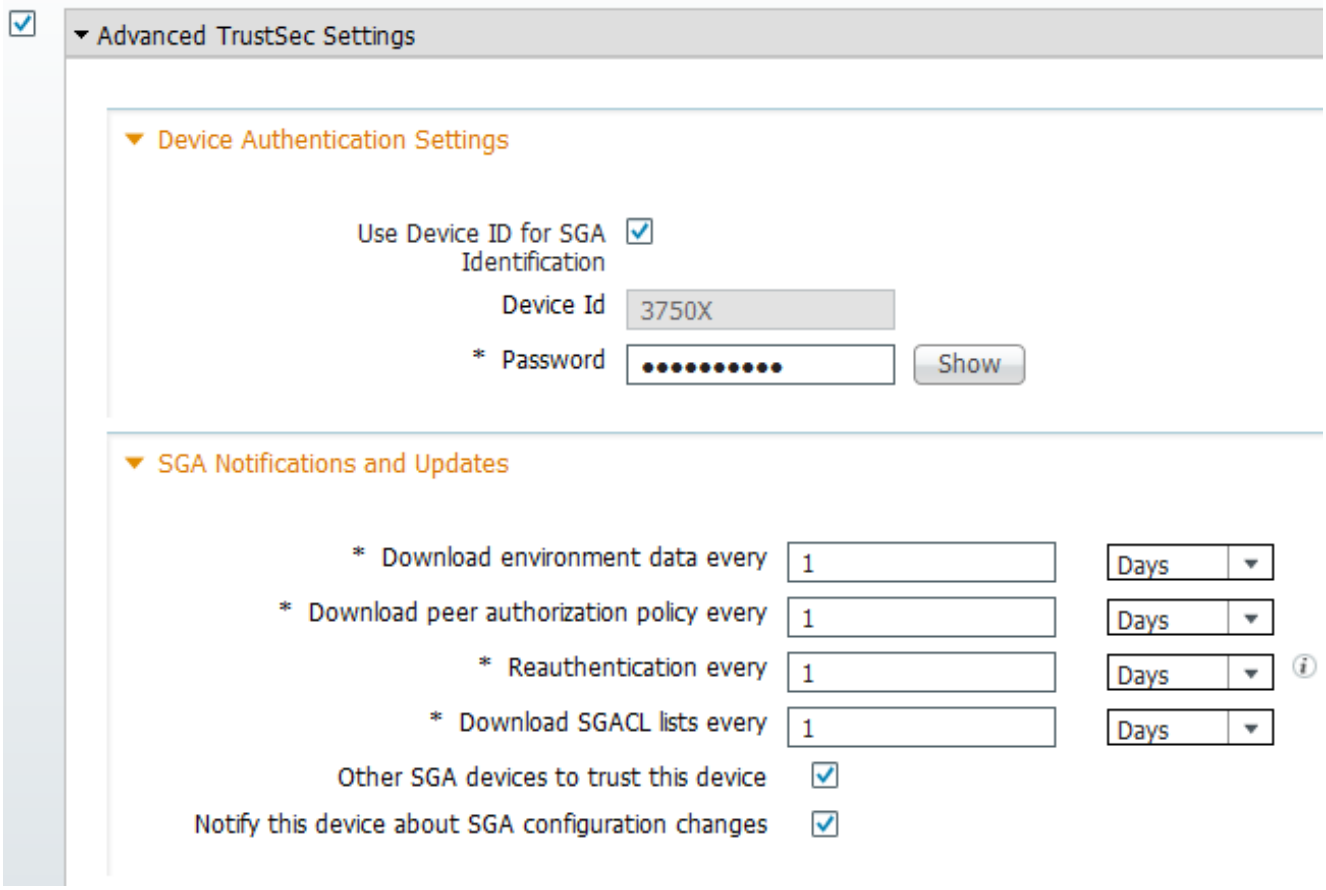
```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
```

Antes de habilitar 802.1x na interface, é necessário configurar o ISE.

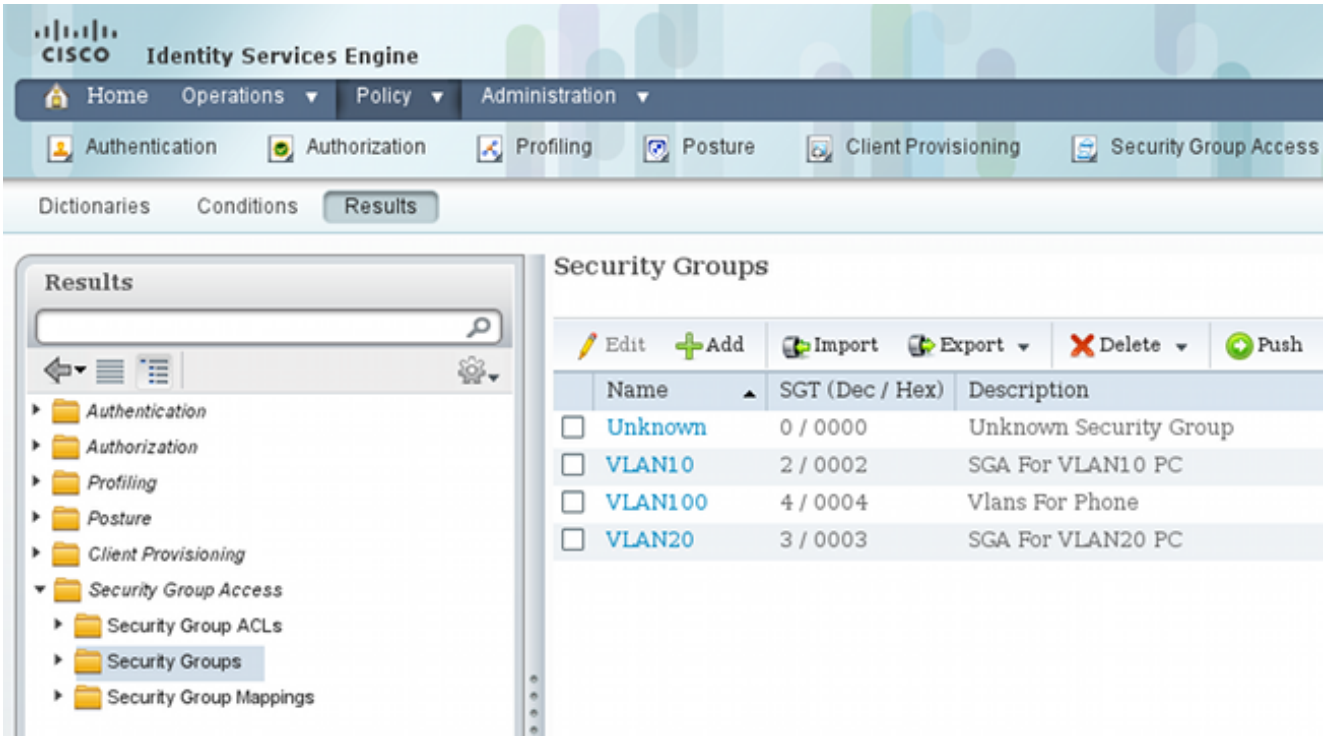
Configurar o ISE

Conclua estas etapas para configurar o ISE:

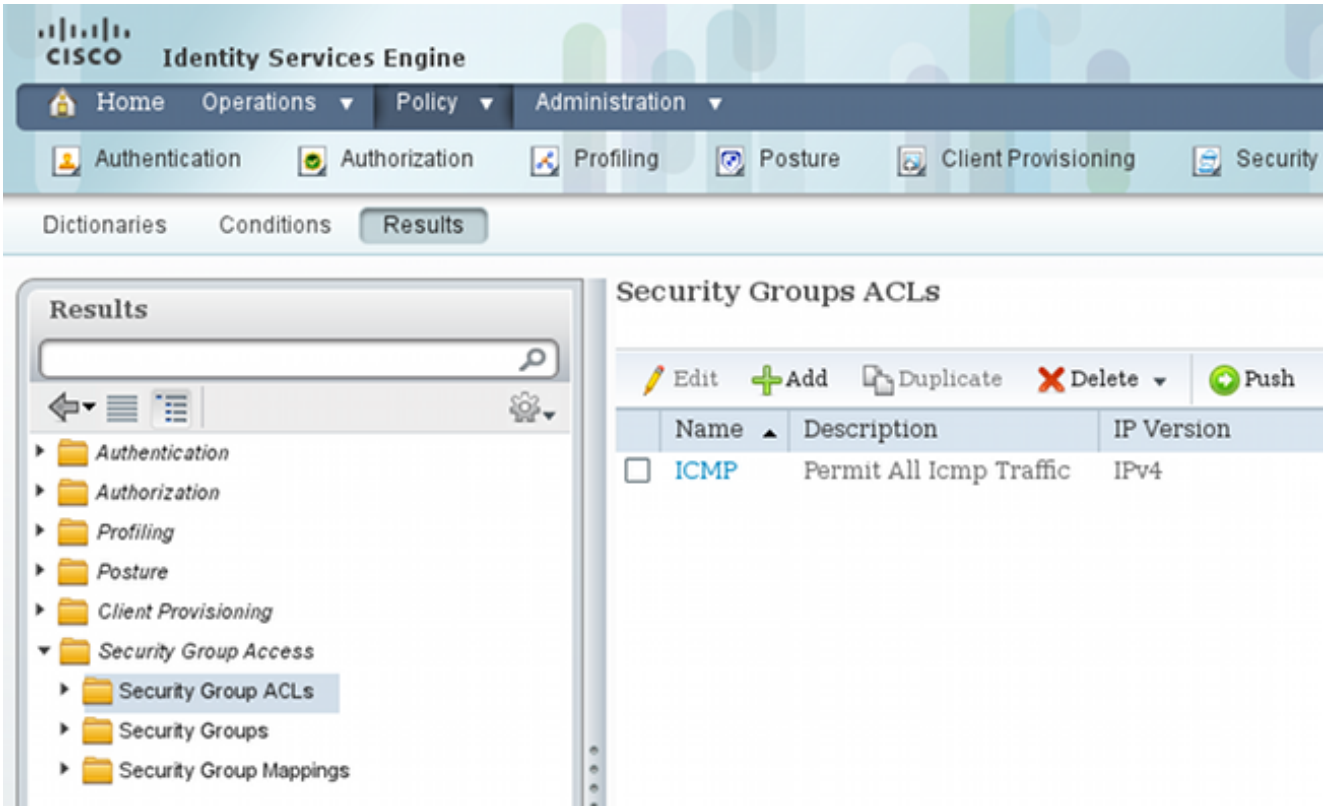
1. Navegue até **Administration > Network Resources > Network Devices** e adicione ambos os switches como Network Access Devices (NADs). Em **Advanced TrustSec Settings**, configure uma senha CTS para uso posterior na CLI do switch.



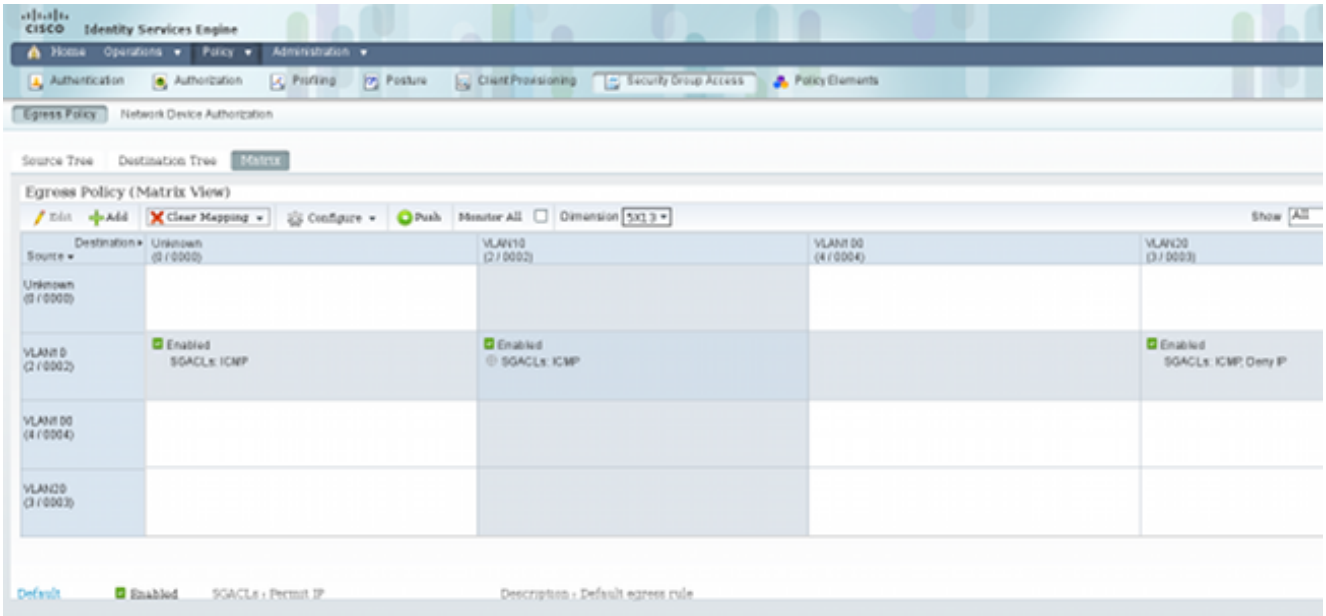
2. Navegue para **Política > Elementos de política > Resultados > Acesso ao grupo de segurança > Grupos de segurança** e adicione os SGTs apropriados. Essas marcas são baixadas quando os switches solicitam uma atualização de ambiente.



3. Navegue até **Policy > Policy Elements > Results > Security Group Access > Security Group ACLs** e configure um SGACL.



4. Navegue para **Política > Acesso ao grupo de segurança** e defina uma política com a matriz.



Observação: você deve configurar a política de autorização para o solicitante do MS Windows, para que ele receba a marca correta. Consulte Exemplo de Configuração e Troubleshooting do ASA e do Catalyst 3750X Series Switch TrustSec para obter uma configuração detalhada para isso.

Provisionamento de PAC para o 3750X-5

A PAC é necessária para a autenticação no domínio CTS (como a fase 1 para EAP-FAST) e também é usada para obter dados de ambiente e política do ISE. Sem a PAC correta, não é

possível obter esses dados do ISE.

Depois que você fornecer as credenciais corretas no 3750X-5, ele fará o download da PAC:

```
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: 08:31:32 UTC Oct 5 2013
 PAC-Opaque: 000200B000030001000400010C40A15A339286CEAC28A50DBBAC5978400060094
0003010076B969769CB5D45453FDCDEB92271C500000001351D15DD900093A8044DF74B2B71F
E667D7B908DB7AEEA32208B4E069FDB0A31161CE98ABD714C55CA0C4A83E4E16A6E8ACAC1D081
F235123600B91B09C9A909516D0A2B347E46D15178028ABFFD61244B3CD6F332435C867A968CE
A6B09BFA8C181E4399CE498A676543714A74B0C048A97C18684FF49BF0BB872405
 Refresh timer is set for 2y25w
```

A PAC é baixada via EAP-FAST com o Challenge Handshake Authentication Protocol (MSCHAPv2) da Microsoft, com as credenciais fornecidas na CLI e as mesmas credenciais configuradas no ISE.

A PAC é usada para a atualização do ambiente e da política. Para esses switches, use solicitações RADIUS com **cisco av-pair cts-pac-opaque**, que é derivado da chave PAC e pode ser descriptografado no ISE.

Provisionamento de PAC para o 3750X-6 e autenticação NDAC

Para que um novo dispositivo possa se conectar ao domínio CTS, é necessário habilitar 802.1x nas portas correspondentes.

O protocolo SAP é usado para o gerenciamento de chaves e a negociação do conjunto de cifras. O GMAC (Galois Message Authentication Code) é usado para autenticação e o GCM (Galois/Counter Mode) para criptografia.

No switch semente:

```
interface GigabitEthernet1/0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 cts dot1x
sap mode-list gcm-encrypt
```

No switch não semente:

```
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 cts dot1x
 sap mode-list gcm-encrypt
```

Isso é suportado apenas em portas de tronco (switch-switch MACsec). Para o MACsec do switch-

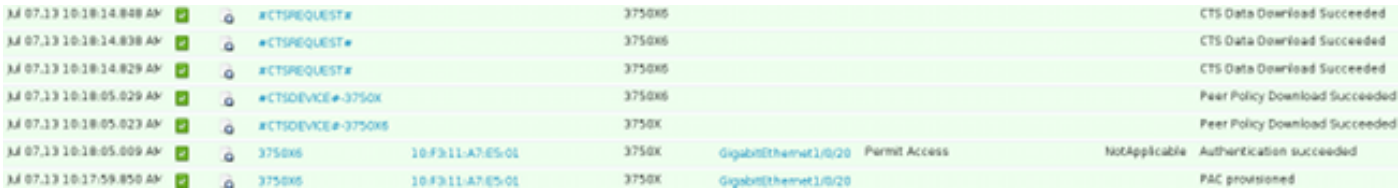
host, que usa o protocolo MACsec Key Agreement (MKA) em vez do SAP, consulte Configuração da Criptografia MACsec.

Imediatamente após a ativação do 802.1x nas portas, o switch não semente atua como um solicitante para o switch semente, que é o autenticador.

Esse processo é chamado de NDAC e seu objetivo é conectar um novo dispositivo ao domínio CTS. A autenticação é bidirecional; o novo dispositivo tem credenciais que são verificadas no ISE do servidor de autenticação. Após o fornecimento de PAC, o dispositivo também se certifica de que se conecta ao domínio CTS.

> **Observação**: a PAC é usada para criar um túnel Transport Layer Security (TLS) para EAP-FAST. O 3750X-6 confia nas credenciais PAC fornecidas pelo servidor, de forma semelhante à maneira como um cliente confia no certificado fornecido pelo servidor para o túnel TLS para o método EAP-TLS.

Várias mensagens RADIUS são trocadas:



A primeira sessão do 3750X (comutador semente) é usada para fornecimento de PAC. EAP-FAST é usado sem PAC (um túnel anônimo para autenticação MSCHAPv2 é criado).

```
12131  EAP-FAST built anonymous tunnel for purpose of PAC provisioning
22037  Authentication Passed
11814  Inner EAP-MSCHAP authentication succeeded
12173  Successfully finished EAP-FAST CTS PAC provisioning/update
11003  Returned RADIUS Access-Reject
```

O nome de usuário e a senha MSCHAPv2 configurados através do comando **cts credentials** são usados. Além disso, um Access-Reject RADIUS é retornado no final, porque depois que a PAC já tiver fornecido, nenhuma autenticação adicional é necessária.

A segunda entrada no registro refere-se à autenticação 802.1x. O EAP-FAST é usado com a PAC fornecida anteriormente.

```
12168  Received CTS PAC
12132  EAP-FAST built PAC-based tunnel for purpose of authentication
11814  Inner EAP-MSCHAP authentication succeeded
15016  Selected Authorization Profile - Permit Access
11002  Returned RADIUS Access-Accept
```

Desta vez, o túnel não é anônimo, mas protegido pelo PAC. Novamente, as mesmas credenciais para a sessão MSCHAPv2 são usadas. Em seguida, ele é verificado em relação às regras de autenticação e autorização no ISE, e um RADIUS Access-Accept é retornado. Em seguida, o switch autenticador aplica os atributos retornados e a sessão 802.1x para essa porta passa para um estado autorizado.

Como é o processo para as duas primeiras sessões 802.1x a partir do switch de seed?

Aqui estão as depurações mais importantes da semente. A propagação detecta que a porta está ativa e tenta determinar qual função deve ser usada para 802.1x - o solicitante ou o autenticador:

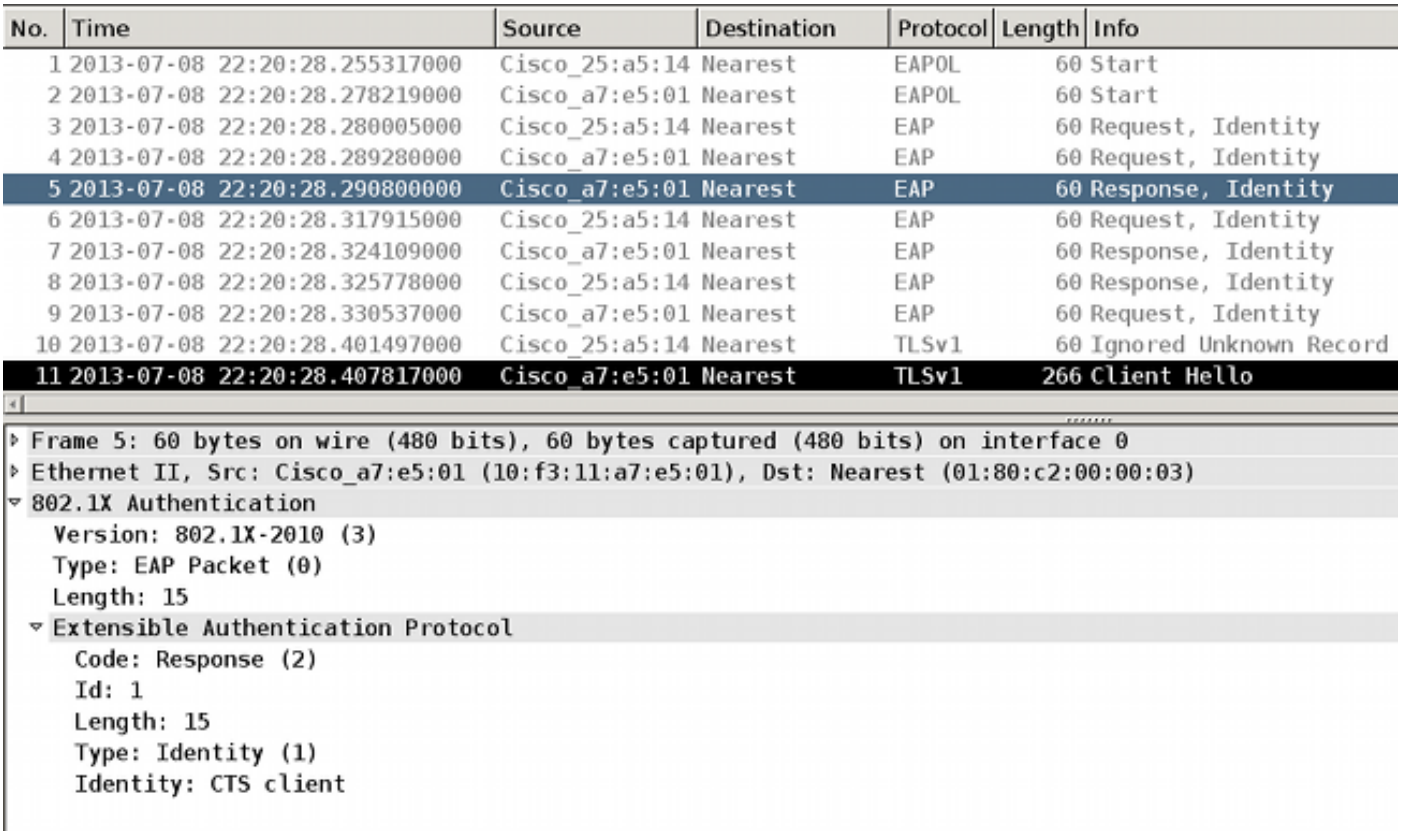
```
debug cts all
debug dot1x all
debug radius verbose
debug radius authentication

Apr 9 11:28:35.347: CTS-ifc-ev: CTS process: received msg_id CTS_IFC_MSG_LINK_UP
Apr 9 11:28:35.347: @@@ cts_ifc GigabitEthernet1/0/20, INIT: ifc_init ->
ifc_authenticating
Apr 9 11:28:35.356: CTS-ifc-ev: Request to start dot1x Both PAE(s) for
GigabitEthernet1/0/20
Apr 9 11:28:35.356: dot1x-ev(Gi1/0/20): Created authenticator subblock
Apr 9 11:28:35.356: dot1x-ev(Gi1/0/20): Created supplicant subblock

Apr 9 11:28:35.364: dot1x-ev:dot1x_supp_start: Not starting default supplicant
on GigabitEthernet1/0/20
Apr 9 11:28:35.381: dot1x-sm:Posting SUPP_ABORT on Client=7C24F2C

Apr 9 11:28:35.397: %AUTHMGR-5-START: Starting 'dot1x' for client (10f3.11a7.e501) on
Interface Gi1/0/20 AuditSessionID C0A800010000054135A5E32
```

Finalmente, a função de autenticador é usada, pois o switch tem acesso ao ISE. No 3750X-6, o papel do requerente é escolhido.

Detalhes sobre a seleção de função 802.1x

> **Observação**: depois que o switch solicitante obtém a PAC e é autenticado pelo 802.1x, ele baixa os dados do ambiente (descritos mais adiante) e aprende o endereço IP do servidor AAA. Neste exemplo, ambos os switches têm uma conexão dedicada (de backbone) para o ISE. Posteriormente, as funções podem ser diferentes; o primeiro switch que recebe uma resposta do servidor AAA torna-se o autenticador e o segundo torna-se o suplicante.

Isso é possível porque ambos os switches com o servidor AAA marcado como ALIVE enviam uma Identidade de Solicitação EAP (Extensible Authentication Protocol). Aquele que primeiro recebe a Resposta de identidade EAP se torna o autenticador e descarta as Solicitações de identidade subsequentes.



No.	Time	Source	Destination	Protocol	Length	Info
1	2013-07-08 22:20:28.255317000	Cisco_25:a5:14	Nearest	EAPOL	60	Start
2	2013-07-08 22:20:28.278219000	Cisco_a7:e5:01	Nearest	EAPOL	60	Start
3	2013-07-08 22:20:28.280005000	Cisco_25:a5:14	Nearest	EAP	60	Request, Identity
4	2013-07-08 22:20:28.289280000	Cisco_a7:e5:01	Nearest	EAP	60	Request, Identity
5	2013-07-08 22:20:28.290800000	Cisco_a7:e5:01	Nearest	EAP	60	Response, Identity
6	2013-07-08 22:20:28.317915000	Cisco_25:a5:14	Nearest	EAP	60	Request, Identity
7	2013-07-08 22:20:28.324109000	Cisco_a7:e5:01	Nearest	EAP	60	Response, Identity
8	2013-07-08 22:20:28.325778000	Cisco_25:a5:14	Nearest	EAP	60	Response, Identity
9	2013-07-08 22:20:28.330537000	Cisco_a7:e5:01	Nearest	EAP	60	Request, Identity
10	2013-07-08 22:20:28.401497000	Cisco_25:a5:14	Nearest	TLSv1	60	Ignored Unknown Record
11	2013-07-08 22:20:28.407817000	Cisco_a7:e5:01	Nearest	TLSv1	266	Client Hello

Depois que a função 802.1x é selecionada (neste cenário, o 3750X-6 é o requerente, porque ainda não tem acesso ao servidor AAA), os próximos pacotes envolvem a troca EAP-FAST para fornecimento de PAC. O nome de usuário **CTS client** é usado para o nome de usuário de solicitação RADIUS e como a identidade EAP:

```
Apr  9 11:28:36.647: RADIUS:  User-Name           [1]   12  "CTS client"
Apr  9 11:28:35.481: RADIUS:  EAP-Message         [79]  17
Apr  9 11:28:35.481: RADIUS:   02 01 00 0F 01 43 54 53 20 63 6C 69 65 6E 74        [ CTS client]
```

Depois que o túnel EAP-FAST anônimo é criado, uma sessão MSCHAPv2 ocorre para o nome de usuário **3750X6** (**credenciais cts**). Não é possível ver isso no switch, pois é um túnel TLS (criptografado), mas logs detalhados no ISE para fornecimento de PAC o comprovam. Você pode ver **CTS Client** para o nome de usuário RADIUS e como a resposta de identidade EAP. No entanto, para o método interno (MSCHAP), o nome de usuário **3750X6** é usado:

EAP Authentication Method :	EAP-MSCHAPv2
EAP Tunnel Method :	EAP-FAST
Username:	3750X6
RADIUS Username :	CTS client
Calling Station ID:	10:F3:11:A7:E5:01

A segunda autenticação EAP-FAST ocorre. Desta vez, ele usa a PAC fornecida anteriormente. Novamente, o **cliente CTS** é usado como o nome de usuário RADIUS e a identidade externa, mas **3750X6** é usado para a identidade interna (MSCHAP). Autenticação bem-sucedida:

RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	3750X6
MAC/IP Address:	10:F3:11:A7:E5:01
Network Device:	3750X : 10.48.66.109 : GigabitEthernet1/0/20
Allowed Protocol:	NDAC_SGT_Service
Identity Store:	Internal CTS Devices
Authorization Profiles:	Permit Access
SGA Security Group:	Unknown
Authentication Protocol :	EAP-FAST(EAP-MSCHAPv2)

No entanto, desta vez, o ISE retorna vários atributos no pacote RADIUS Accept:

Authentication Result

```
User-Name=3750X6
State=ReauthSession:C0A800010000053A33FD79AF
Class=CACS:C0A800010000053A33FD79AF:ise/162314118/3616
Session-Timeout=86400
Termination-Action=RADIUS-Request
EAP-Key-Name=2b:54:e8:37:14:10:f0:3c:1b:90:f1:d7:ad:1c:0b:cc:62:e5:03:4c:6b
cisco-av-pair=cts:security-group-tag=0000-01
cisco-av-pair=cts:supplicant-cts-capabilities=sap
MS-MPPE-Send-Key=ce:d6:28:6f:b4:c0:2a:96:69:93:fe:41:0d:1e:80:9d:31:e2:b8:c
MS-MPPE-Recv-Key=d4:8c:13:cd:d7:18:c7:1f:57:21:0d:de:39:fa:cd:68:aa:ca:1b:4f
```

Aqui, o switch autenticador altera a porta para o estado autorizado:

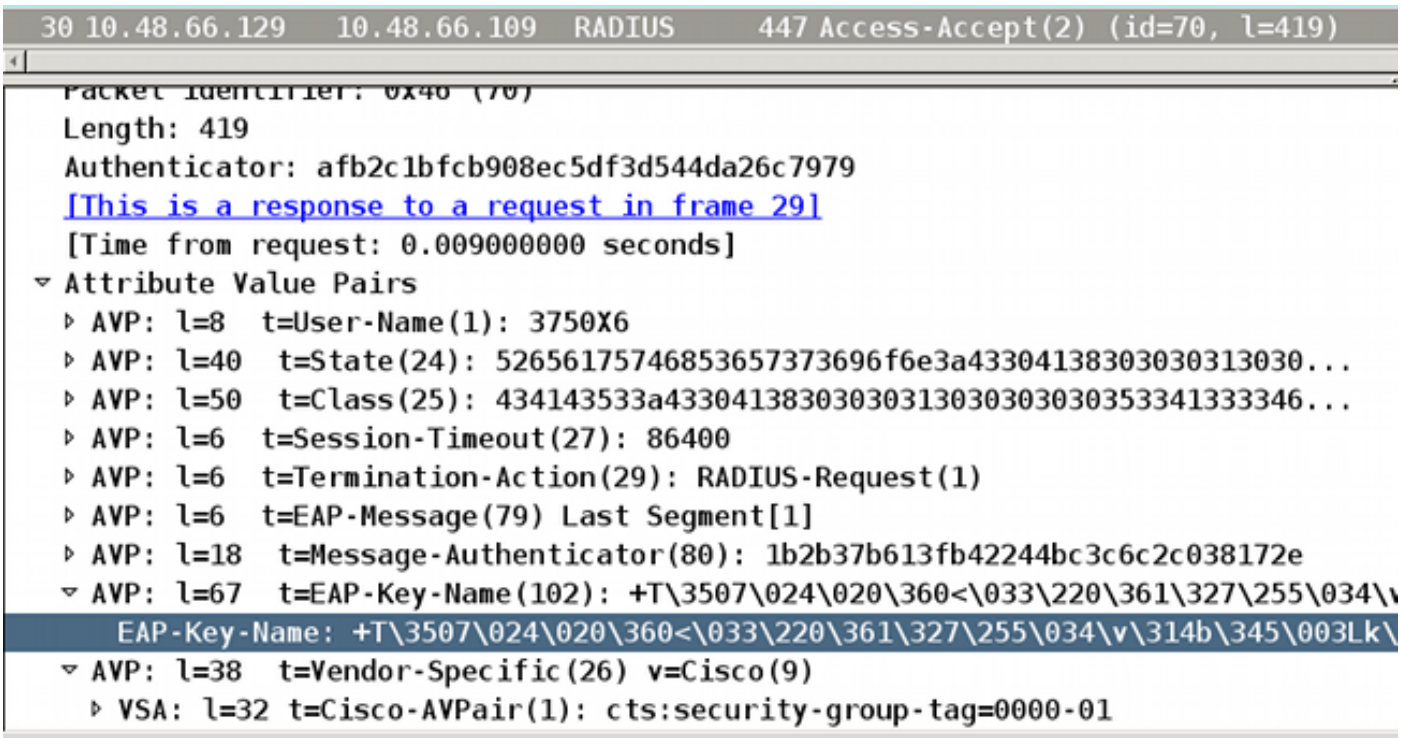
```
bsns-3750-5#show authentication sessions int g1/0/20
            Interface:  GigabitEthernet1/0/20
          MAC Address:  10f3.11a7.e501
           IP Address:  Unknown
             User-Name:  3750X6
                Status:  Authz Success
               Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
     Session timeout:  86400s (local), Remaining: 81311s
      Timeout action:  Reauthenticate
        Idle timeout:  N/A
   Common Session ID:  C0A800010000054135A5E321
     Acct Session ID:  0x0000068E
              Handle:  0x09000542

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

Como o switch autenticador aprende que o Nome de usuário é **3750X6**? Para o nome de usuário RADIUS e a identidade EAP externa, o **cliente CTS** é usado, e a identidade interna é

criptografada e não é visível para o autenticador. O nome de usuário é aprendido pelo ISE. O último pacote RADIUS (Access-Accept) contém **username=3750X6**, enquanto todos os outros continham **username = Cts client**. É por isso que o interruptor suplicante reconhece o nome de usuário real. Esse comportamento é compatível com RFC. Do RFC3579 seção 3.0:

```
The User-Name attribute within the Access- Accept packet need not be the same
as the User-Name attribute in the Access-Request.
```

No último pacote da sessão de autenticação 802.1x, o ISE retorna uma mensagem RADIUS Accept **cisco-av-pair** com o **EAP-Key-Name**:

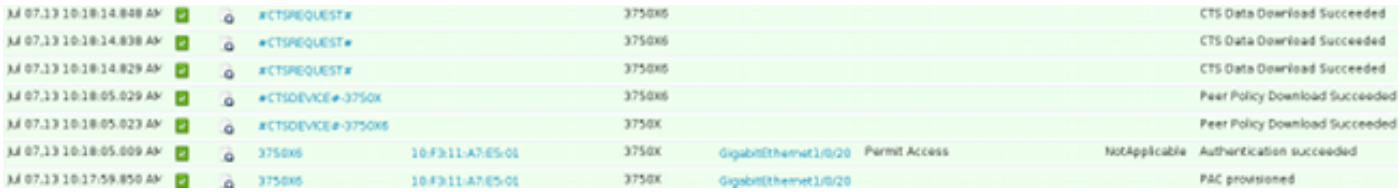


Isso é usado como material de chaveamento para a negociação SAP.

Além disso, o SGT é aprovado. Isso significa que o switch autenticador marca o tráfego do solicitante com um **valor padrão = 0**. Você pode configurar um valor específico no ISE para retornar qualquer outro valor. Isso se aplica somente ao tráfego não marcado; o tráfego marcado não é regravado porque, por padrão, o switch autenticador confia no tráfego do suplicante autenticado (mas isso também pode ser alterado no ISE).

Download de Política da SGA

Há trocas RADIUS adicionais (sem EAP) além das duas primeiras sessões 802.1x EAP-FAST (a primeira para fornecimento de PAC e a segunda para autenticação). Aqui estão os logs do ISE novamente:



O terceiro log (**Download de política de peer**) indica uma troca RADIUS simples: Solicitação

RADIUS e Aceitação RADIUS para o usuário **3760X6**. Isso é necessário para fazer o download de políticas para o tráfego do solicitante. Os dois atributos mais importantes são:

```
▾ AVP: l=31  t=Vendor-Specific(26) v=Cisco(9)
  ▸ VSA: l=25 t=Cisco-AVPair(1): cts:trusted-device=true
▾ AVP: l=38  t=Vendor-Specific(26) v=Cisco(9)
  ▸ VSA: l=32 t=Cisco-AVPair(1): cts:security-group-tag=0000-01
▾ AVP: l=38  t=Vendor-Specific(26) v=Cisco(9)
  ▸ VSA: l=32 t=Cisco-AVPair(1): cts:authorization-expiry=86400
```

Por causa disso, o switch autenticador confia no tráfego que é marcado como SGT pelo suplicante (**cts:trusted-device=true**) e também marca o tráfego não marcado com **tag=0**.

O quarto registro indica a mesma troca de RADIUS. No entanto, desta vez, é para o usuário **3750X5** (autenticador). Isso porque ambos os peers devem ter uma política um para o outro. É interessante observar que o solicitante ainda não sabe o endereço IP do servidor AAA. É por isso que o switch autenticador baixa a política em nome do suplicante. Essas informações são transmitidas posteriormente ao solicitante (juntamente com o endereço IP do ISE) na negociação SAP.

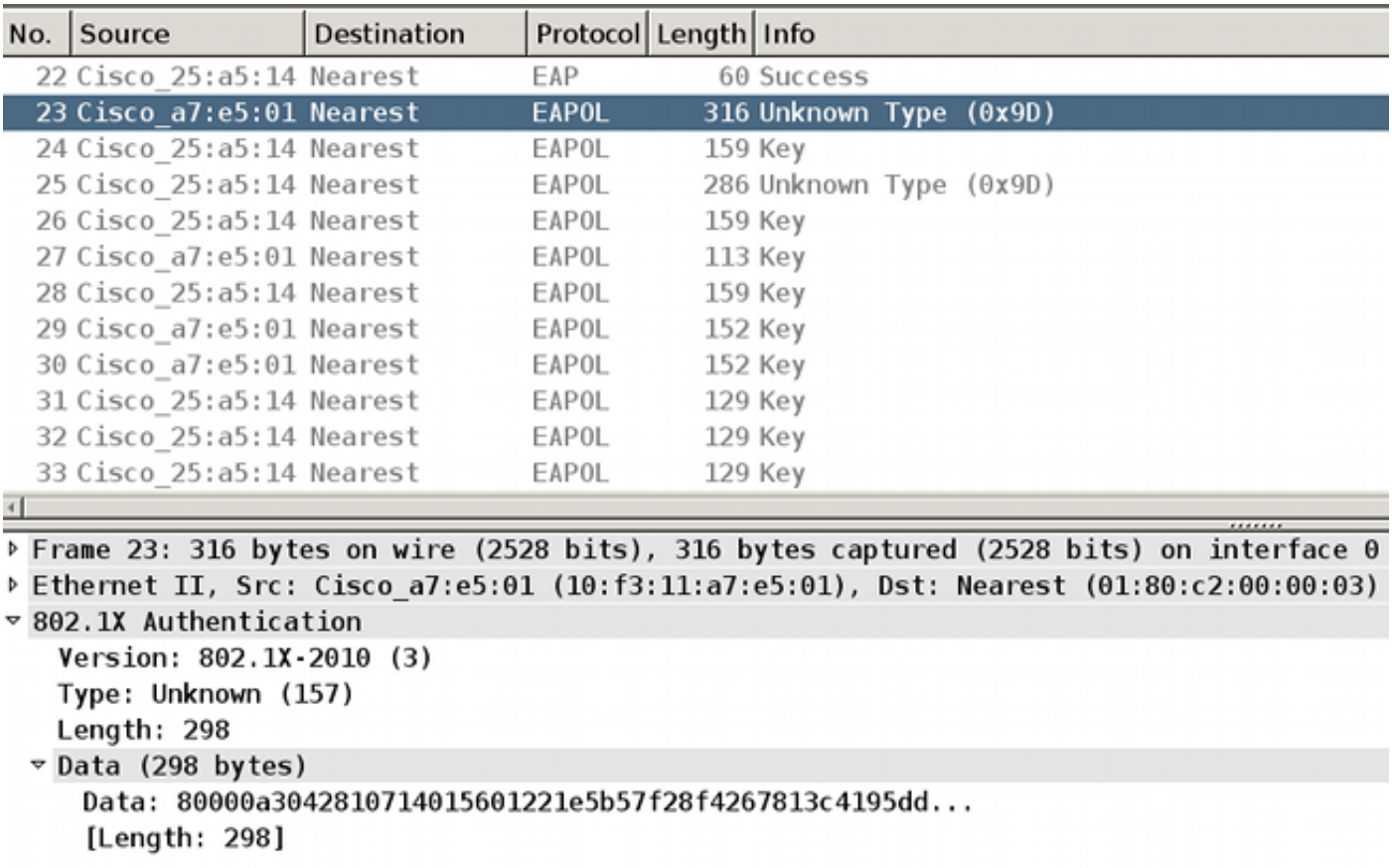
Negociação SAP

Imediatamente após a conclusão da sessão de autenticação 802.1x, ocorre a negociação SAP. Essa negociação é necessária para:

- Negocie os níveis de criptografia (com o comando **sap mode-list gcm-encrypt**) e conjuntos de cifras
- Derivar chaves de sessão para tráfego de dados
- Passar pelo processo de rechaveamento
- Execute verificações de segurança adicionais e verifique se as etapas anteriores estão protegidas

O SAP é um protocolo projetado pela Cisco Systems com base em uma versão preliminar do 802.11i/D6.0. Para obter detalhes, solicite acesso à página Cisco TrustSec Security Association Protocol - protocol supported Cisco Trusted Security for the Cisco Nexus 7000.

O Exchange SAP é compatível com 802.1AE. Uma troca de chave EAPOL (Extensible Authentication Protocol over LAN) ocorre entre o solicitante e o autenticador para negociar um conjunto de cifras, trocar parâmetros de segurança e gerenciar chaves. Infelizmente, o Wireshark não tem decodificador para todos os tipos de EAP necessários:



No.	Source	Destination	Protocol	Length	Info
22	Cisco_25:a5:14	Nearest	EAP	60	Success
23	Cisco_a7:e5:01	Nearest	EAPOL	316	Unknown Type (0x9D)
24	Cisco_25:a5:14	Nearest	EAPOL	159	Key
25	Cisco_25:a5:14	Nearest	EAPOL	286	Unknown Type (0x9D)
26	Cisco_25:a5:14	Nearest	EAPOL	159	Key
27	Cisco_a7:e5:01	Nearest	EAPOL	113	Key
28	Cisco_25:a5:14	Nearest	EAPOL	159	Key
29	Cisco_a7:e5:01	Nearest	EAPOL	152	Key
30	Cisco_a7:e5:01	Nearest	EAPOL	152	Key
31	Cisco_25:a5:14	Nearest	EAPOL	129	Key
32	Cisco_25:a5:14	Nearest	EAPOL	129	Key
33	Cisco_25:a5:14	Nearest	EAPOL	129	Key

A conclusão bem-sucedida dessas tarefas resulta no estabelecimento de uma associação de segurança (SA).

No comutador suplicante:

```
bsns-3750-6#show cts interface g1/0/1
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/1:
    CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
    Authentication Status:   SUCCEEDED
       Peer identity:       "3750X"
       Peer's advertised capabilities: "sap"
       802.1X role:         Supplicant
       Reauth period applied to link:  Not applicable to Supplicant role
   Authorization Status:    SUCCEEDED
       Peer SGT:            0:Unknown
       Peer SGT assignment: Trusted
   SAP Status:              SUCCEEDED
       Version:             2
        Configured pairwise ciphers:
            gcm-encrypt

       Replay protection:      enabled
       Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

   Propagate SGT:           Enabled
   Cache Info:
       Cache applied to link : NONE

   Statistics:
```

```
       authc success:              12
       authc reject:               1556
       authc failure:              0
       authc no response:          0
       authc logoff:               0
       sap success:                12
       sap fail:                   0
       authz success:              12
       authz fail:                 0
       port auth fail:             0

   L3 IPM:   disabled.

Dot1x Info for GigabitEthernet1/0/1
-----------------------------------
PAE                     = SUPPLICANT
StartPeriod             = 30
AuthPeriod              = 30
HeldPeriod              = 60
MaxStart                = 3
Credentials profile     = CTS-ID-profile
EAP profile             = CTS-EAP-profile
```

No autenticador:

```
bsns-3750-5#show cts interface g1/0/20
Global Dot1x feature is Enabled
Interface GigabitEthernet1/0/20:
    CTS is enabled, mode:    DOT1X
   IFC state:               OPEN
   Interface Active for 00:29:22.069
   Authentication Status:   SUCCEEDED
        Peer identity:       "3750X6"
       Peer's advertised capabilities: "sap"
        802.1X role:         Authenticator
       Reauth period configured:       86400 (default)
       Reauth period per policy:       86400 (server configured)
       Reauth period applied to link:  86400 (server configured)
       Reauth starts in approx. 0:23:30:37 (dd:hr:mm:sec)
       Peer MAC address is 10f3.11a7.e501
       Dot1X is initialized
   Authorization Status:    ALL-POLICY SUCCEEDED
        Peer SGT:            0:Unknown
       Peer SGT assignment: Trusted
    SAP Status:              SUCCEEDED
       Version:             2
       Configured pairwise ciphers:
            gcm-encrypt
           {3, 0, 0, 0} checksum 2

       Replay protection:      enabled
       Replay protection mode: STRICT

        Selected cipher:        gcm-encrypt

   Propagate SGT:           Enabled
   Cache Info:
       Cache applied to link : NONE
       Data loaded from NVRAM: F
       NV restoration pending: F
       Cache file name       : GigabitEthernet1_0_20_d
       Cache valid           : F
       Cache is dirty        : T
```

```
        Peer ID               : unknown
        Peer mac              : 0000.0000.0000
        Dot1X role            : unknown
        PMK                   :
             00000000 00000000 00000000 00000000
             00000000 00000000 00000000 00000000

    Statistics:
        authc success:              12
        authc reject:               1542
        authc failure:              0
        authc no response:          0
        authc logoff:               2
        sap success:                12
        sap fail:                   0
        authz success:              13
        authz fail:                 0
        port auth fail:             0

    L3 IPM:   disabled.

Dot1x Info for GigabitEthernet1/0/20
-----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

Aqui, as portas usam o modo **gcm-encrypt**, o que significa que o tráfego é autenticado e criptografado, bem como marcado corretamente pelo SGT. Nenhum dispositivo usa qualquer política de autorização de dispositivo de rede específica no ISE, o que significa que todo o tráfego iniciado do dispositivo usa a marca padrão de **0**. Além disso, ambos os switches confiam nos SGTs recebidos do peer (devido aos atributos RADIUS da fase de download da política de peer).

Atualização de ambiente e política

Depois que os dois dispositivos são conectados à nuvem CTS, uma atualização de ambiente e política é iniciada. A atualização do ambiente é necessária para obter os SGTs e nomes, e uma atualização de política é necessária para baixar o SGACL definido no ISE.

Nesse estágio, o suplicante já sabe o endereço IP do servidor AAA, então pode fazê-lo por si mesmo.

Consulte Exemplo de Configuração e Troubleshooting do ASA e do Catalyst 3750X Series Switch TrustSec para obter detalhes sobre o ambiente e a atualização da política.

O switch solicitante lembra o endereço IP do servidor RADIUS, mesmo quando não há um servidor RADIUS configurado e quando o link CTS é desativado (em direção ao switch autenticador). No entanto, é possível forçar o switch a esquecê-lo:

```
bsns-3750-6#show run | i radius
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-server vsa send authentication

bsns-3750-6#show cts server-list
CTS Server Radius Load Balance = DISABLED
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)

Preferred list, 1 server(s):
 *Server: 10.48.66.129, port 1812, A-ID C40A15A339286CEAC28A50DBBAC59784
        Status = ALIVE
        auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.48.66.129, port 1812, A-ID C40A15A339286CEAC28A50DBBAC59784
        Status = ALIVE
        auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs

bsns-3750-6#show radius server-group all
Server group radius
   Sharecount = 1  sg_unconfigured = FALSE
   Type = standard  Memlocks = 1
Server group  private_sg-0
    Server(10.48.66.129:1812,1646) Successful Transactions:
   Authen: 8   Author: 16      Acct: 0
   Server_auto_test_enabled: TRUE
   Keywrap enabled: FALSE

bsns-3750-6#clear cts server 10.48.66.129

bsns-3750-6#show radius server-group all
Server group radius
   Sharecount = 1  sg_unconfigured = FALSE
   Type = standard  Memlocks = 1
Server group  private_sg-0
```

Para verificar o ambiente e a política no switch solicitante, insira estes comandos:

```
bsns-3750-6#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
 SGT tag = 0-01:Unknown
Server List Info:
Security Group Name Table:
    0-00:Unknown
    2-00:VLAN10
    3-00:VLAN20
    4-00:VLAN100
Environment Data Lifetime = 86400 secs
Last update time = 03:23:51 UTC Thu Mar 31 2011
Env-data expires in   0:13:09:52 (dd:hr:mm:sec)
Env-data refreshes in 0:13:09:52 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running

bsns-3750-6#show cts role-based permissions
```

Por que nenhuma política é exibida? Nenhuma política é exibida, pois você deve habilitar a

aplicação de cts para aplicá-las:

```
bsns-3750-6(config)#cts role-based enforcement
bsns-3750-6(config)#cts role-based enforcement vlan-list all
bsns-3750-6#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
```

Por que o suplicante tem apenas uma política para agrupar Desconhecido enquanto o autenticador tem mais?

```
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 3:VLAN20:
        ICMP-20
        Deny IP-00
```

Autenticação de porta para clientes

O cliente MS Windows está conectado e autenticado na porta g1/0/1 do switch 3750-5:

```
bsns-3750-5#show authentication sessions int 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:  C0A80001000001BD336EC4D6
     Acct Session ID:  0x000002F9
              Handle:  0xF80001BE


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

Aqui, o switch 3750-5 sabe que o tráfego desse host deve ser marcado com SGT=3 quando enviado para a nuvem CTS.

Marcação de tráfego com o SGT

Como você fareja e verifica o tráfego?

Isso é difícil porque:

- O Embedded Packet Capture é suportado apenas para tráfego IP (e este é um quadro Ethernet modificado com SGTs e payload MACsec).
- Porta Switched Port Analyzer (SPAN) com a palavra-chave **replication** - isso pode funcionar, mas o problema é que qualquer PC com Wireshark conectado à porta de destino de uma sessão de monitoramento descarta os quadros devido à falta de suporte de 802.1ae, o que pode acontecer no nível de hardware.
- A porta de SPAN sem a palavra-chave **replication** remove o cabeçalho **cts** antes que ele coloque uma porta de destino.

Aplicação de políticas com o SGACL

A aplicação de políticas na nuvem CTS é sempre feita na porta de destino. Isso ocorre porque somente o último dispositivo conhece o SGT de destino do dispositivo de ponto final que está conectado diretamente a esse switch. O pacote transporta apenas o SGT de origem. Tanto o SGT de origem quanto o de destino são necessários para tomar uma decisão.

Épor isso que os dispositivos não precisam fazer o download de todas as políticas do ISE. Em vez disso, eles precisam apenas da parte da política relacionada ao SGT para o qual o dispositivo tem dispositivos conectados diretamente.

Aqui está o 3750-6, que é o switch solicitante:

```
bsns-3750-6#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
```

Há duas políticas aqui. O primeiro é o padrão para tráfego não marcado (de/para). O segundo é de **SGT=2** para o SGT não marcado, que é **0**. Essa política existe porque o próprio dispositivo usa a política SGA do ISE e pertence a **SGT=0**. Além disso, **SGT=0** é uma marca padrão. Portanto, você deve fazer o download de todas as políticas que têm as regras de tráfego **de/para SGT=0**. Se você observar a matriz, verá apenas uma dessas políticas: **de 2 a 0**.

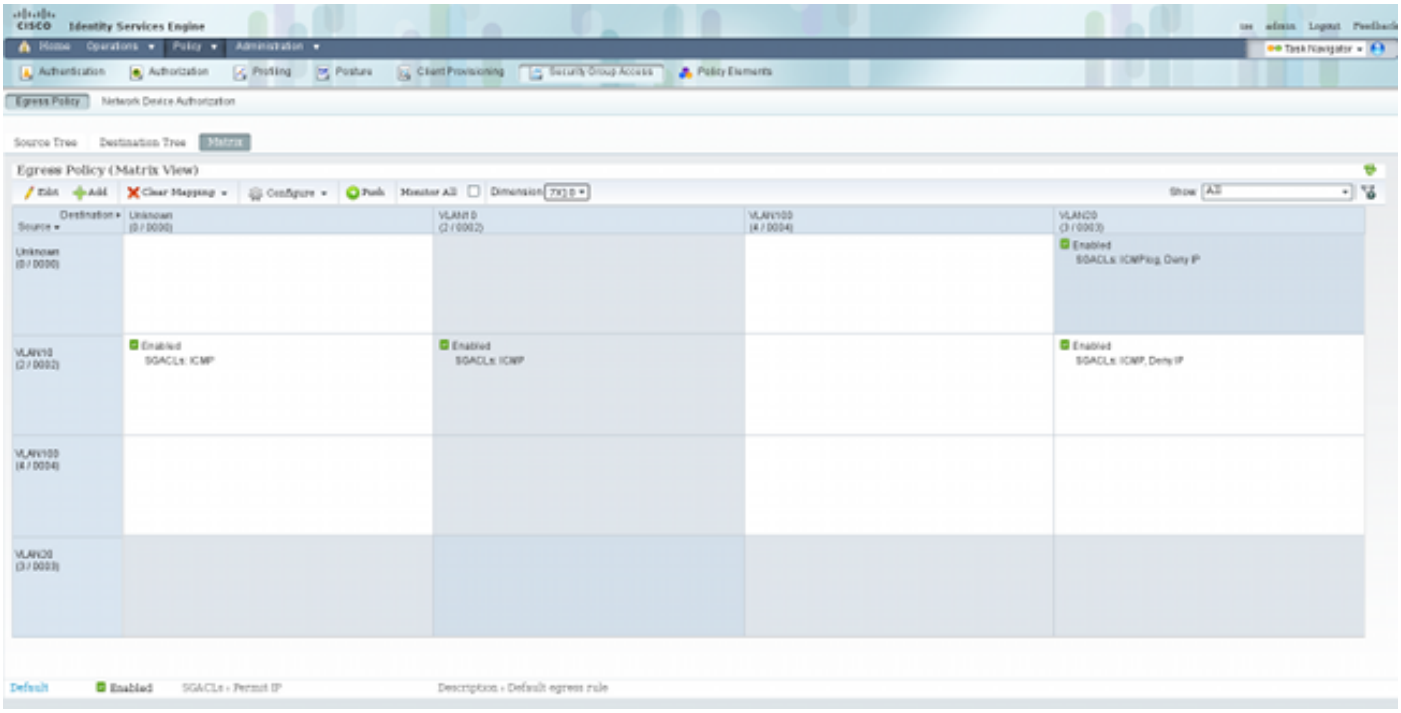
Aqui está o 3750-5, que é o switch autenticador:

```
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 3:VLAN20:
       ICMP-20
       Deny IP-00
```

Há aqui mais uma política: **de 2 para 3**. Isso ocorre porque o cliente 802.1x (MS Windows) está conectado a **g1/0/1** e marcado com **SGT=3**. É por isso que você deve fazer o download de todas as políticas **para SGT=3**.

Tente fazer ping de 3750X-6 (**SGT=0**) para o MS Windows XP (**SGT=3**). O 3750X-5 é o dispositivo de imposição.

Antes disso, você deve configurar uma política no ISE para o tráfego de **SGT=0 a SGT=3**. Este exemplo criou um log SGACL Internet Control Message Protocol (ICMP) somente com a linha, **permit icmp log**, e o usou na matriz para o tráfego de **SGT=0 a SGT=3**:



Aqui está uma atualização da política no switch de imposição e uma verificação da nova política:

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

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 Unknown to group 3:VLAN20:
        ICMPlog-10
        Deny IP-00
IPv4 Role-based permissions from group 2:VLAN10 to group 3:VLAN20:
       ICMP-20
       Deny IP-00
```

Para verificar se a ACL (Access Control List, Lista de controle de acesso) foi baixada do ISE, digite este comando:

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

Para verificar se a ACL está aplicada (suporte de hardware), insira este comando:

```
bsns-3750-5#show cts rbacl | b ICMPlog-10
 name    = ICMPlog-10
 IP protocol version = IPV4
```

```
 refcnt = 2
 flag   = 0x41000000
   POLICY_PROGRAM_SUCCESS
   POLICY_RBACL_IPV4
 stale  = FALSE
 ref_q:
   acl_infop(74009FC), name(ICMPlog-10)
 sessions installed:
   session hld(460000F8)
 RBACL ACEs:
 Num ACEs: 1
    permit icmp log
```

Aqui estão os contadores antes do ICMP:

```
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               4099            224

*       *       0               0               321810          340989

0       3       0               0               0               0

2       3       0               0               0               0
```

Aqui está um ping de **SGT=0** (switch 3750-6) para o MS Windows XP (**SGT=3**) e os contadores:

```
bsns-3750-6#ping 192.168.2.200
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.200, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

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               4099            224

*       *       0               0               322074          341126

0       3       0               0               0               5

2       3       0               0               0               0
```

Estes são os contadores da ACL:

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

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

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.