在Catalyst 3750X系列交換機上使用802.1x MACsec的TrustSec雲配置示例

目錄

簡介

本文介紹在兩台Catalyst 3750X系列交換機(3750X)之間使用鏈路加密配置Cisco TrustSec(CTS)雲所需的步驟。

本文說明了使用安全關聯協定(SAP)的交換機到交換機的媒體訪問控制安全(MACsec)加密過程。此過程使用IEEE 802.1x模式而不是手動模式。

以下是相關步驟的清單：

- 種子和非種子裝置的保護訪問憑證(PAC)調配
- 用於金鑰管理的網路裝置准入控制(NDAC)身份驗證和與SAP的MACsec協商
- 環境和策略更新
- 使用者端的連線埠驗證
- 具有安全組標籤(SGT)的流量標籤
- 使用安全組ACL(SGACL)實施策略

必要條件

需求

思科建議您瞭解以下主題：

- CTS元件的基礎知識
- Catalyst交換器CLI組態的基本知識
- 身分識別服務引擎(ISE)配置體驗

採用元件

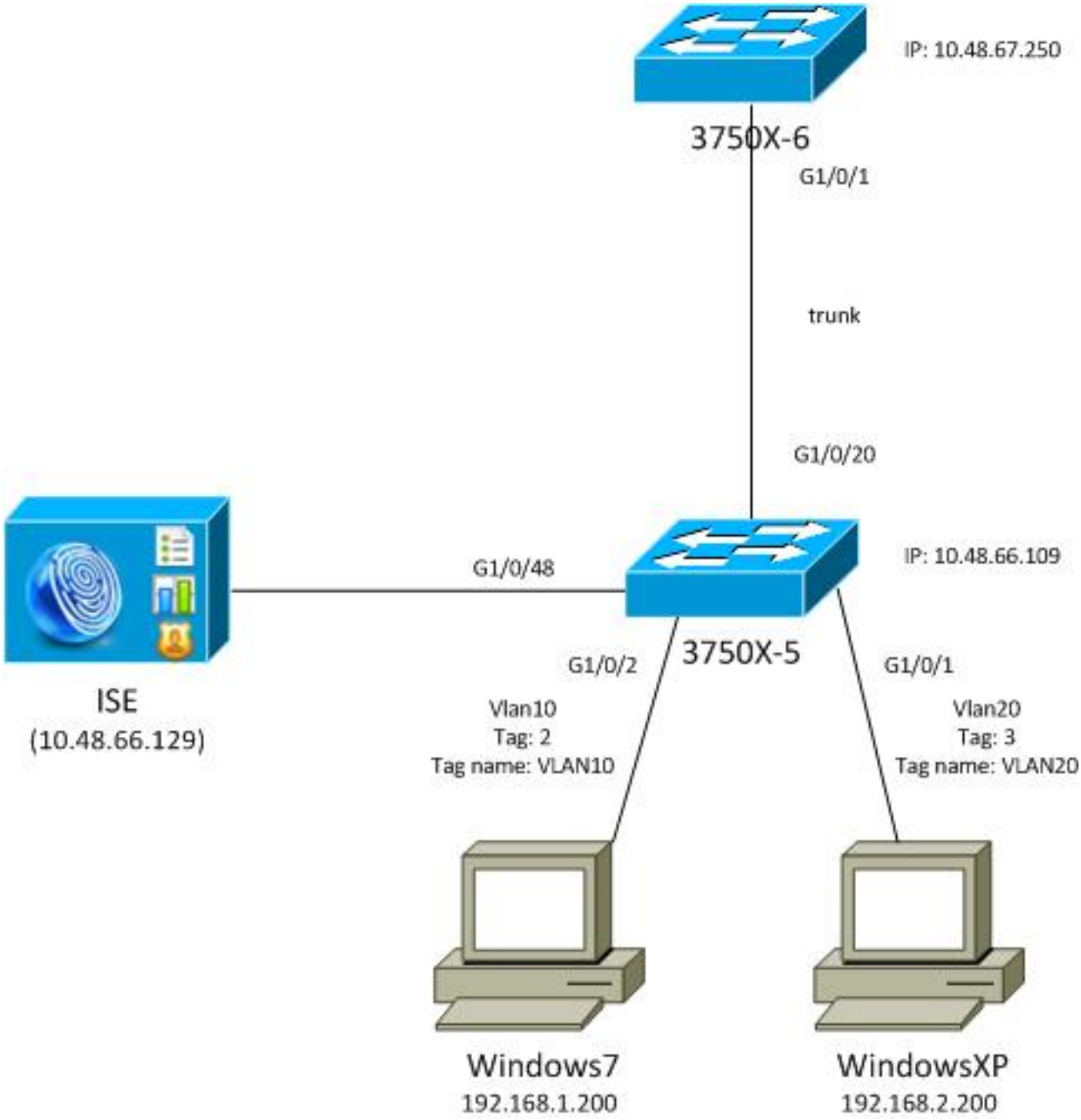
本文中的資訊係根據以下軟體和硬體版本：

- Microsoft(MS)Windows 7和MS Windows XP
- 3750X軟體15.0版及更新版本
- ISE軟體，版本1.1.4及更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

網路圖表



在此網路拓撲圖中，3750X-5交換機是知道ISE的IP地址的種子裝置，它自動下載PAC，用於在CTS雲中進行後續身份驗證。種子裝置充當非種子裝置的802.1x驗證器。Cisco Catalyst 3750X-6系列交換機(3750X-6)是非種子裝置。它充當種子裝置的802.1x請求方。非種子裝置通過種子裝置向ISE進行身份驗證後，允許訪問CTS雲。成功驗證後，3750X-5交換器上的802.1x連線埠狀態會變更為**authenticated**，且會交涉MACsec加密。交換器之間的流量接著會使用SGT標籤並加密。

此清單彙總了預期的流量：

- 種子3750X-5連線到ISE並下載PAC，稍後用於環境和策略更新。
- 非種子3750X-6使用請求者角色執行802.1x身份驗證，以便從ISE驗證/授權和下載PAC。
- 3750X-6執行第二個802.1x可擴充驗證通訊協定 — 透過安全通訊協定(EAP-FAST)的彈性驗證，以便根據PAC使用受保護通道進行驗證。
- 3750X-5可自行下載並代表3750X-6下載SGA策略。
- 在3750X-5和3750X-6之間執行SAP會話，協商MACsec密碼，並交換策略。
- 交換器之間的流量會進行標籤和加密。

配置種子交換機和非種子交換機

種子裝置(3750X-5)配置為使用ISE作為CTS的RADIUS伺服器：

```
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
```

已啟用基於角色的訪問控制清單(RBACL)和基於安全組的訪問控制清單(SGACL)實施（稍後將使用）：

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

非種子裝置(3750X-6)僅設定為驗證、授權和記帳(AAA)，不需要RADIUS或CTS授權：

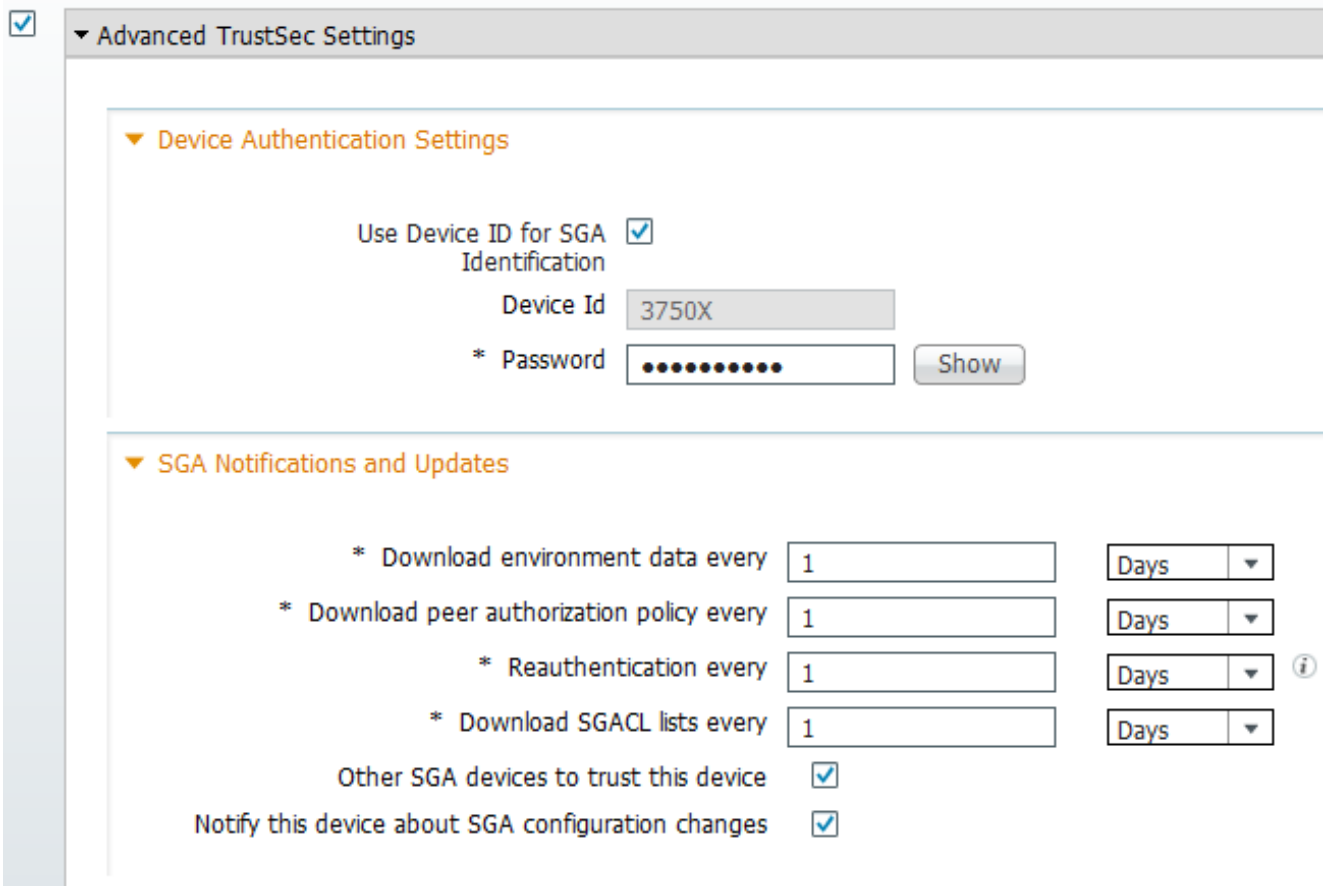
```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
```

在介面上啟用802.1x之前，必須配置ISE。

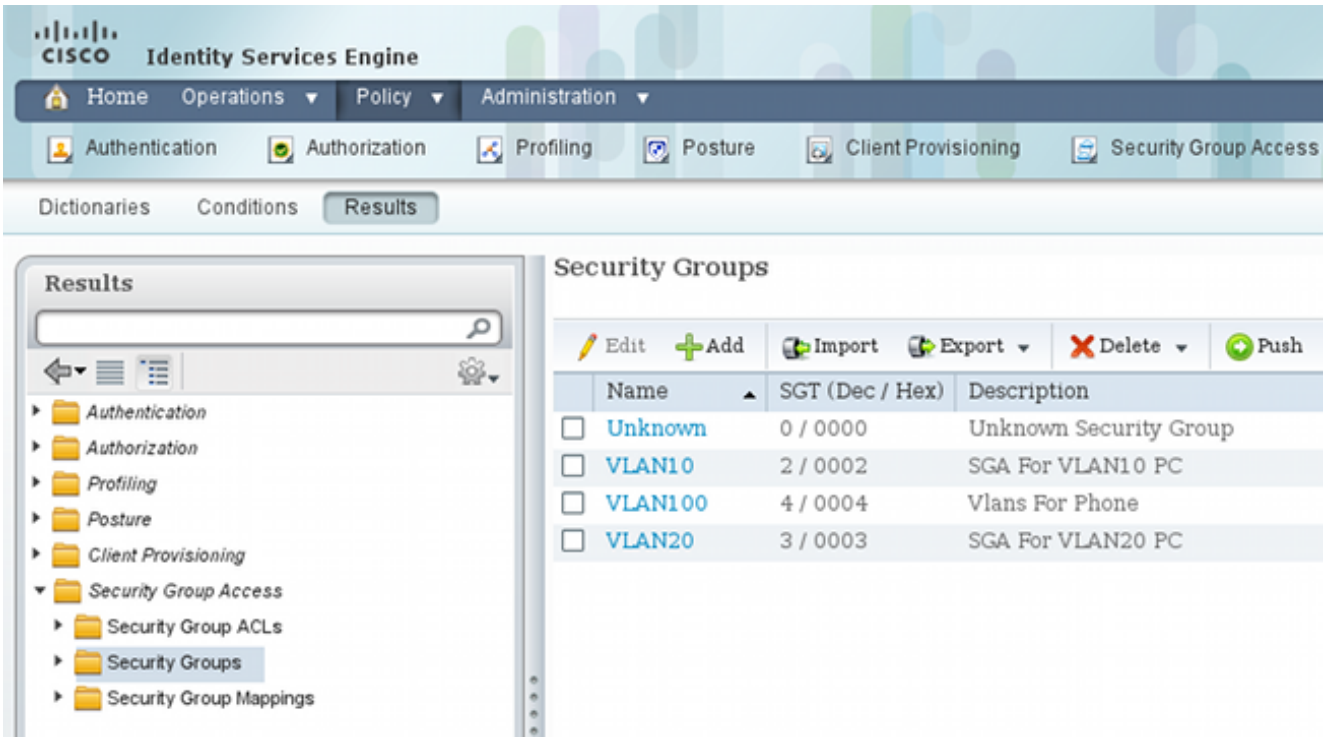
配置ISE

完成以下步驟以配置ISE:

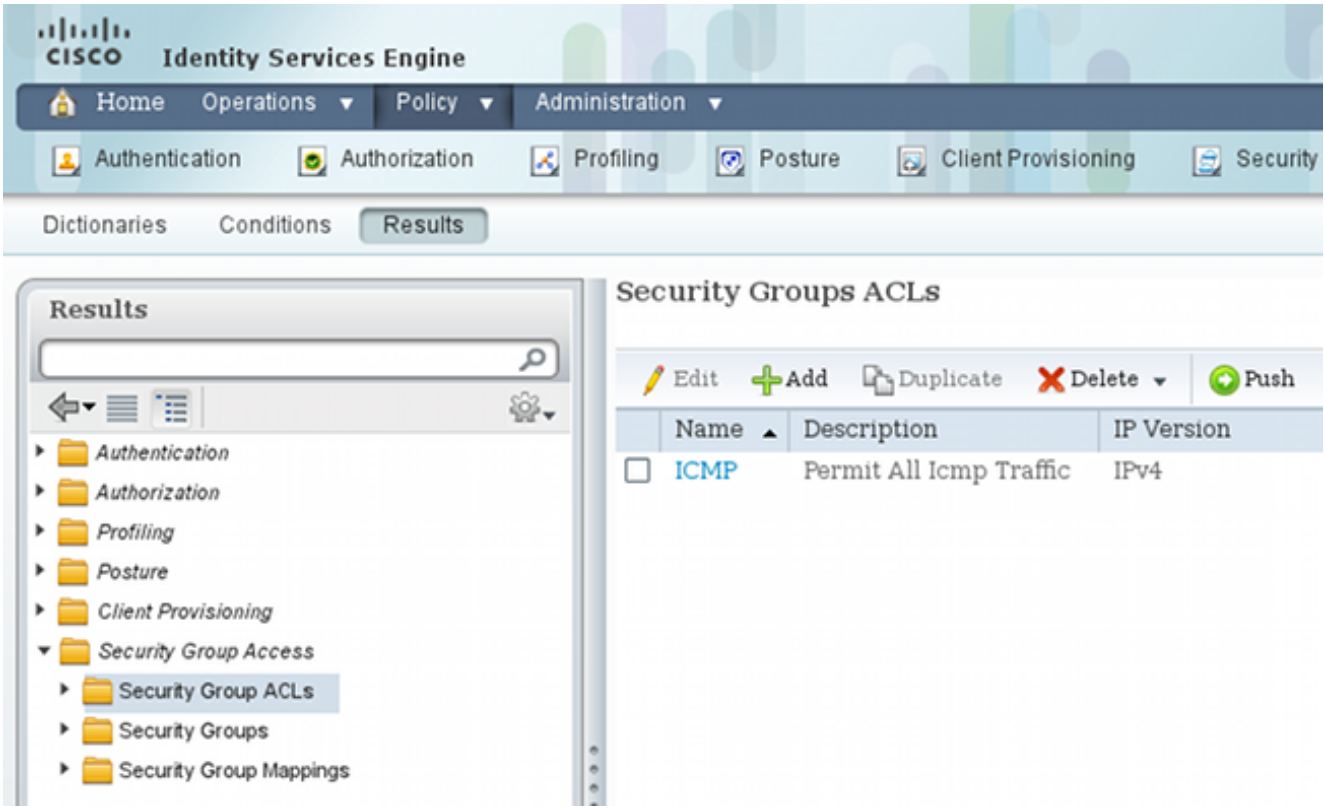
1. 導覽至**Administration > Network Resources > Network Devices**，然後將兩台交換器新增為網路存取裝置(NAD)。在**Advanced TrustSec Settings**下，配置一個CTS密碼，供以後在交換機CLI上使用。



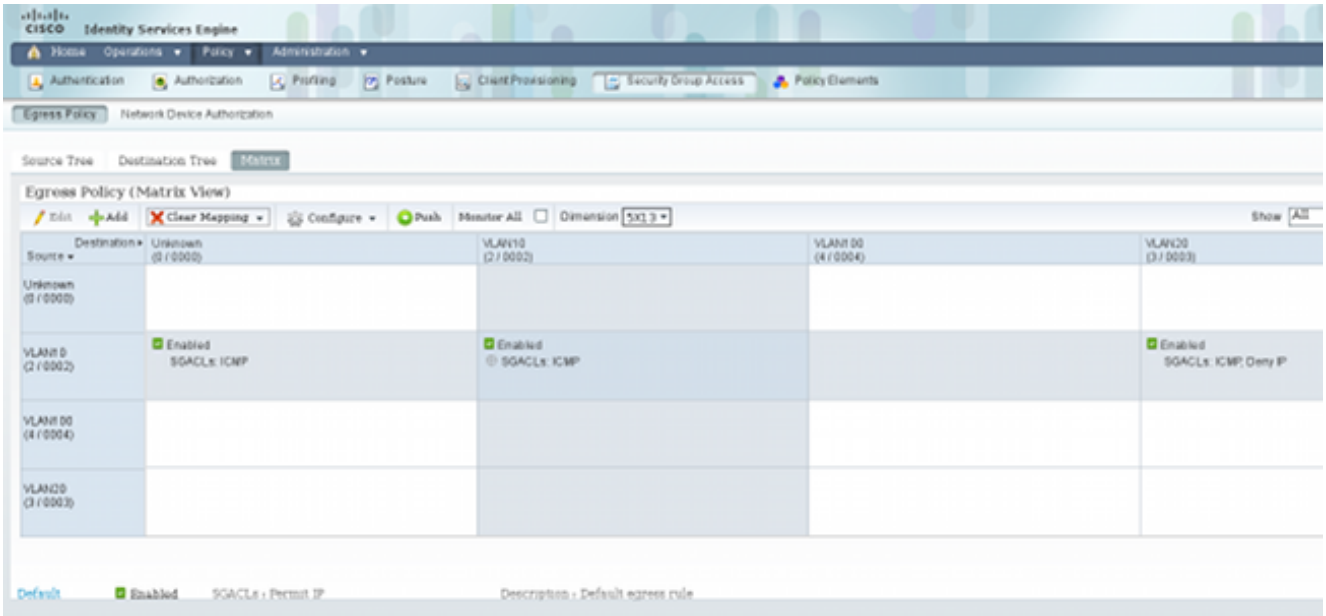
2. 導航到**Policy > Policy Elements > Results > Security Group Access > Security Groups**，然後新增適當的SGT。當交換機請求環境刷新時，會下載這些標籤。



3. 導航到**Policy > Policy Elements > Results > Security Group Access > Security Group ACLs**，然後配置SGACL。



4. 導航到**Policy > Security Group Access**，然後使用矩陣定義策略。



注意：必須為MS Windows請求方配置授權策略，以便它接收正確的標籤。有關此配置的詳細資訊，請參閱[ASA和Catalyst 3750X系列交換機TrustSec配置示例和故障排除指南]。

3750X-5的PAC布建

在CTS域中進行身份驗證時需要PAC（對於EAP-FAST為phase1），並且還用於從ISE獲取環境和策略資料。如果沒有正確的PAC，則無法從ISE獲取該資料。

在3750X-5上提供正確憑證後，它會下載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
```

PAC通過EAP-FAST下載，使用Microsoft的Challenge Handshake身份驗證協定(MSCHAPv2)、CLI中提供的憑證和ISE上配置的相同憑證。

PAC用於環境和策略刷新。對於這些交換器，請將RADIUS要求與**cisco av配對cts-pac-opaque**（從PAC金鑰派生，可在ISE上解密）搭配使用。

適用於3750X-6和NDAC驗證的PAC布建

為了讓新裝置能夠連線到CTS域，必須在相應埠上啟用802.1x。

SAP協定用於金鑰管理和密碼套件協商。Galois Message Authentication Code(GMAC)用於身份驗證，Galois/Counter Mode(GCM)用於加密。

在種子交換器上：

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

在非種子交換器上：

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

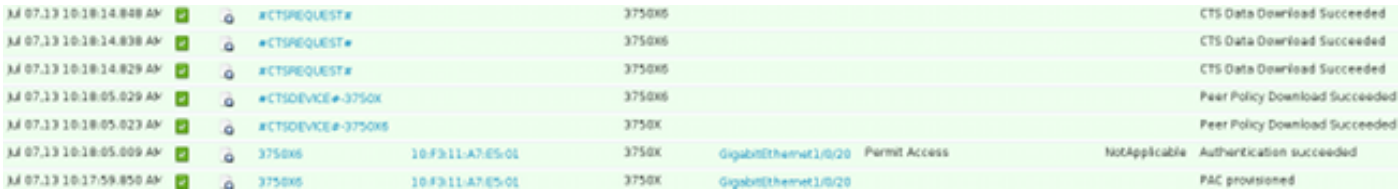
只有主干連線埠（交換器 — 交換器MACsec）支援此功能。有關使用MACsec金鑰協定(MKA)協定而非SAP的交換機主機MACsec，請參閱配置MACsec加密。

在連線埠上啟用802.1x後，非種子交換器會立即充當種子交換器（即驗證器）的請求者。

此過程稱為NDAC，其目的是將新裝置連線到CTS域。身份驗證是雙向的；新裝置具有在身份驗證伺服器ISE上驗證的憑證。在PAC調配後，裝置也確保連線到CTS域。

註:PAC用於為EAP-FAST構建傳輸層安全(TLS)隧道。3750X-6信任伺服器提供的PAC憑證，類似於客戶端信任伺服器為EAP-TLS方法的TLS隧道提供的證書的方式。

交換多個RADIUS訊息：



3750X（種子交換機）的第一個會話用於PAC調配。使用EAP-FAST時不使用PAC（為MSCHAPv2身份驗證構建了匿名隧道）。

```
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
```

使用通過**cts credentials**命令配置的MSCHAPv2使用者名稱和密碼。此外，由於在PAC已布建後，不需要進行進一步的驗證，因此會在結尾返回RADIUS存取拒絕。

日誌中的第二個條目是指802.1x身份驗證。EAP-FAST用於之前調配的PAC。

```
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
```

這一次，隧道不是匿名的，而是受PAC保護。再次使用MSCHAPv2會話的相同憑據。然後，根據ISE上的身份驗證和授權規則進行驗證，並返回RADIUS Access-Accept。然後，身份驗證器交換機應用返回的屬性，該埠的802.1x會話將變為授權狀態。

種子交換機上前兩個802.1x會話的過程是什麼樣的？

下面是seed中最重要的調試。種子檢測到埠已啟動，並嘗試確定應該對802.1x（請求方或驗證方）使用哪個角色：

```
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
```

最後，使用身份驗證器角色，因為交換機可以訪問ISE。在3750X-6上，選擇請求者角色。

有關802.1x角色選擇的詳細資訊

> **注意**：請求方交換機獲得PAC並經過802.1x驗證後，將下載環境資料（稍後說明），並獲取AAA伺服器的IP地址。在本例中，兩台交換機都有專用的（主幹）ISE連線。之後，角色可以不同；從AAA伺服器收到響應的第一台交換機成為身份驗證器，第二台交換機成為請求方。

這是可能的，因為AAA伺服器標籤為ALIVE的兩台交換器都傳送了可擴充驗證通訊協定(EAP)要求身分。首先收到EAP身份響應的身份驗證器將成為身份驗證器，並丟棄後續的身份請求。

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

```
▸ Frame 5: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: Cisco_a7:e5:01 (10:f3:11:a7:e5:01), Dst: Nearest (01:80:c2:00:00:03)
▾ 802.1X Authentication
    Version: 802.1X-2010 (3)
    Type: EAP Packet (0)
    Length: 15
  ▾ Extensible Authentication Protocol
      Code: Response (2)
      Id: 1
      Length: 15
      Type: Identity (1)
      Identity: CTS client
```

選擇802.1x角色後（在此場景中，3750X-6是請求方，因為它尚未訪問AAA伺服器），下一個資料包涉及用於PAC調配的EAP-FAST交換。使用者名稱**CTS client**用於RADIUS請求使用者名稱並作為EAP身份：

```
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]
```

建立匿名EAP-FAST隧道後，對使用者名稱3750X6（cts憑據）**進行**MSCHAPv**2會**話。在交換機上看不到這一點，因為它是TLS隧道（已加密），但PAC調配的ISE上的詳細日誌證明了這一點。您可以檢視**CTS Client**以獲取RADIUS使用者名稱並作為EAP身份響應。但是內部方法(MSCHAP)使用**3750X6** 使用者名稱：

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

進行第二個EAP-FAST身份驗證。這一次，它使用之前調配的PAC。同樣地，**CTS client**用作RADIUS使用者名稱和外部身分，而**3750X6**則用作為內部身分(MSCHAP)。身份驗證成功：

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)

但是這一次，ISE在RADIUS接受資料包中返回多個屬性：

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
```

這裡，驗證器交換器會將連線埠變更為授權狀態：

```
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
```

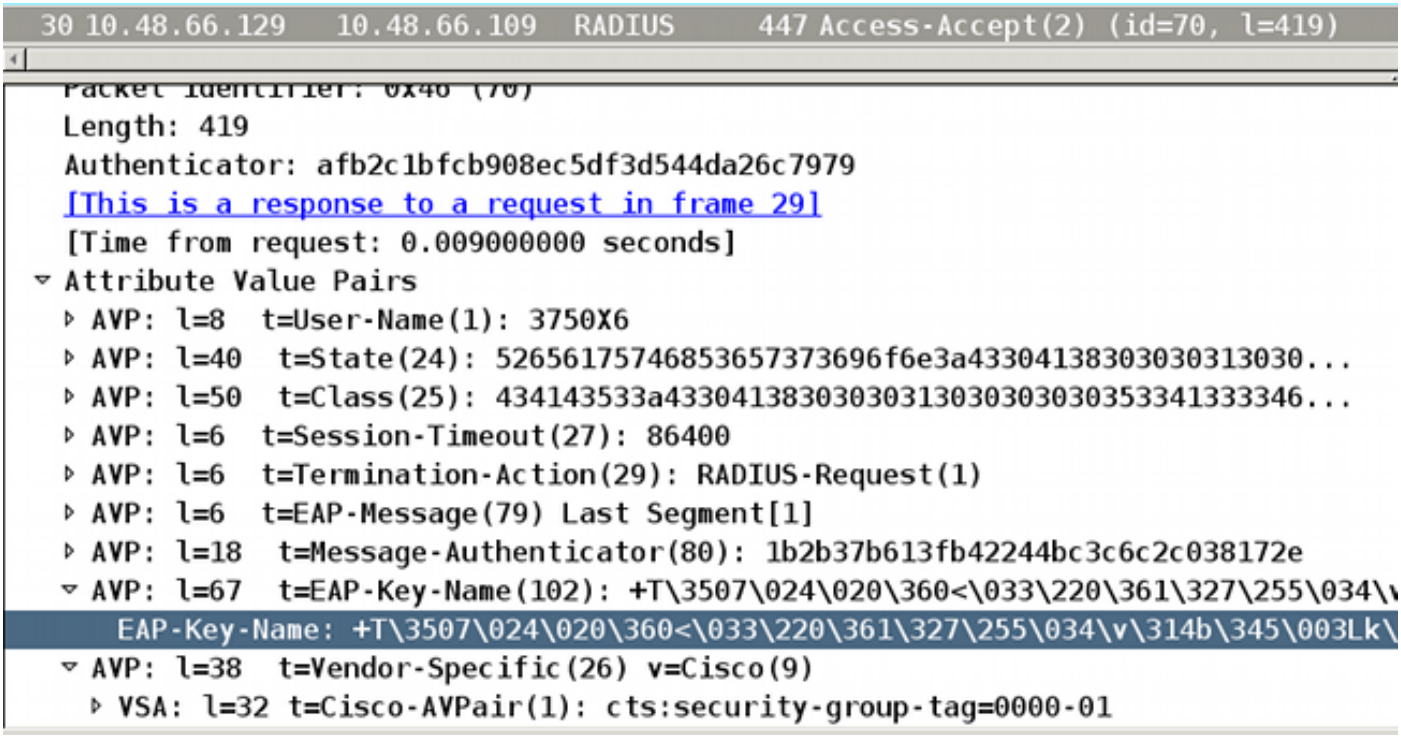
```
     Session timeout:  86400s (local), Remaining: 81311s
      Timeout action:  Reauthenticate
        Idle timeout:  N/A
   Common Session ID:  C0A800010000054135A5E321
     Acct Session ID:  0x0000068E
              Handle:  0x09000542

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

驗證器交換機如何得知使用者名稱是**3750X6**?對於RADIUS使用者名稱和外部EAP身份，使用**CTS client**，內部身份被加密且對驗證者不可見。使用者名稱由ISE獲取。最後一個RADIUS封包(Access-Accept)包含**username=3750X6**，而所有其他封包包含**username = Cts client**。這就是請求方交換器識別實際使用者名稱的原因。此行為與RFC相容。在RFC3579第3.0節中：

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

在802.1x身份驗證會話的最後一個資料包中，ISE返回帶有**EAP-Key-Name**的RADIUS Accept消息**cisco-av-pair**:

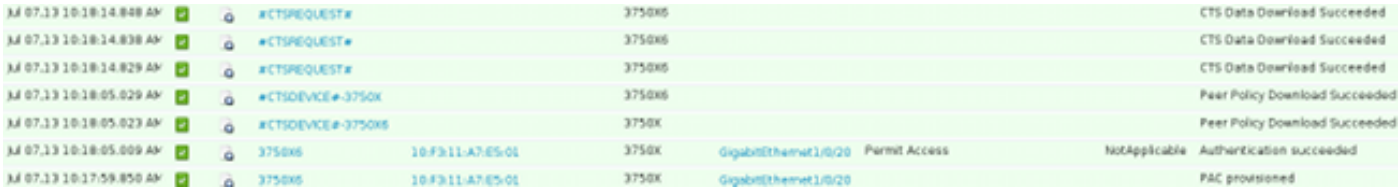


它用作SAP協商的金鑰材料。

此外，SGT會通過。這表示驗證器交換器使用預設值= 0標籤**來自請求方的流量**。您可以在ISE上配置特定值以返回任何其他值。這僅適用於無標籤流量；標籤流量不會重寫，因為預設情況下，身份驗證器交換機信任來自經過身份驗證的請求方的流量（但這也可以在ISE上更改）。

SGA策略下載

除了前兩個802.1x EAP-FAST會話（第一個用於PAC調配，第二個用於身份驗證）之外，還有其他RADIUS交換（無EAP）。以下是ISE日誌：



第三個日誌(**對等策略下載**)表示簡單的RADIUS交換：3760X6使用者的RADIUS請**求和RADIUS**接受。要為來自請求方的流量下載策略，需要執行此操作。最重要的兩個屬性是：

```
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
```

因此，身份驗證器交換機信任由請求方進行SGT標籤的流量(**cts:trusted-device=true**)，並且還使用**tag=0標籤未標籤的流量**。

第四個日誌指示相同的RADIUS交換。但是這次是為**3750X5使用者(驗證器**)準備的。這是因為兩個對等體必須擁有彼此的策略。值得注意的是，請求方仍不知道AAA伺服器的IP地址。這就是驗證器交換機代表請求方下載策略的原因。此資訊隨後在SAP協商中傳遞給請求方（以及ISE IP地址）。

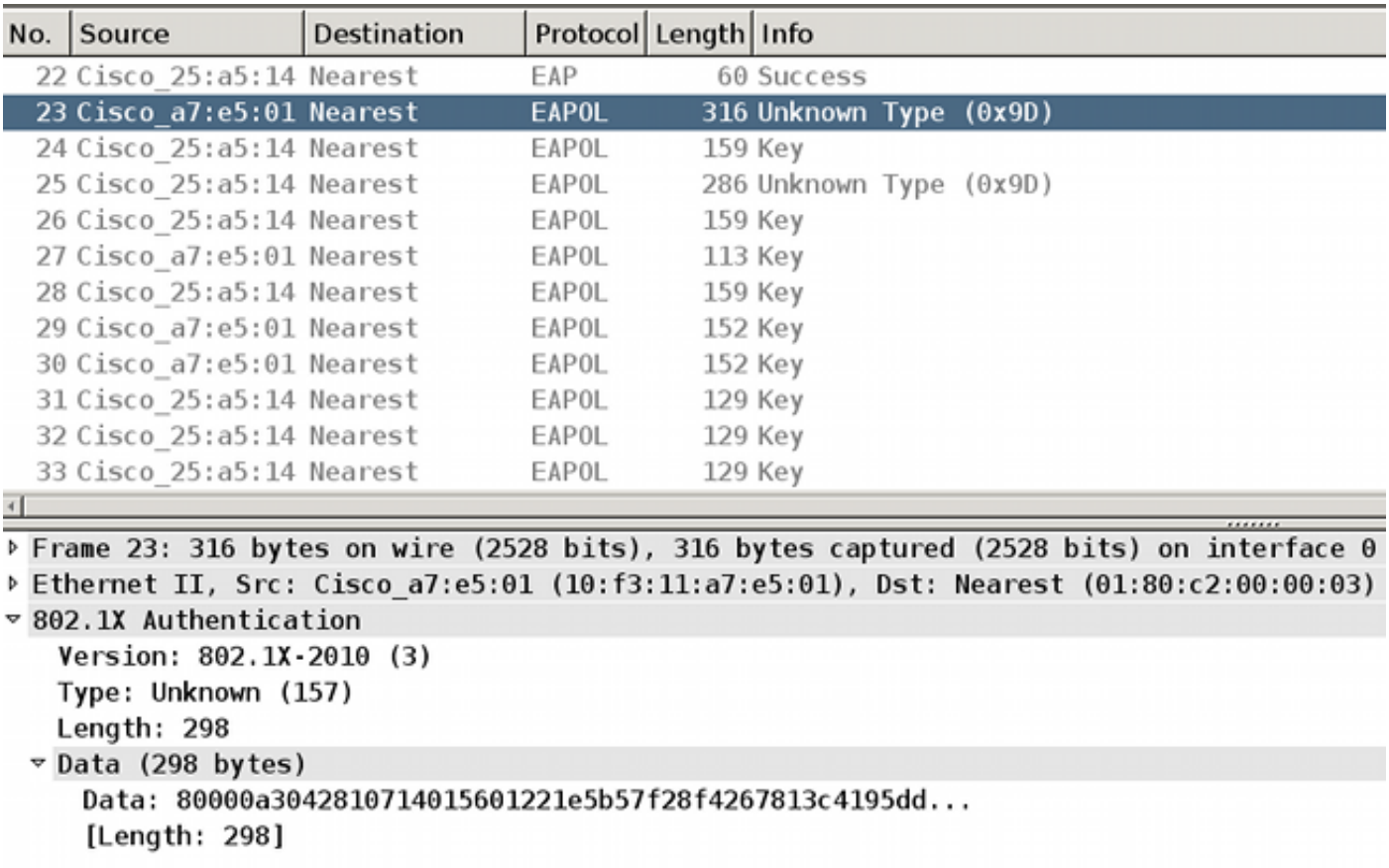
SAP協商

802.1x身份驗證會話完成後，將立即進行SAP協商。此協商是必需的，以便：

- 協商加密級別(使用**sap mode-list gcm-encrypt**命令)和密碼套件
- 為資料流量派生會話金鑰
- 執行重新生成金鑰的過程
- 執行其他安全檢查並確保前面步驟的安全

SAP是由Cisco Systems基於802.11i/D6.0的草案版本設計的協定。有關詳細資訊，請請求訪問[Cisco TrustSec安全關聯協定 — 支援Cisco Nexus 7000頁面的Cisco Trusted Security的協](#)議。

SAP Exchange符合802.1AE標準。LAN上的可擴充驗證通訊協定(EAPOL)金鑰交換會在請求者和驗證者之間進行，以便協商密碼套件、交換安全引數和管理金鑰。很遺憾，Wireshark沒有所有必需的EAP型別的解碼器：



這些任務的成功完成導致安全關聯(SA)的建立。

在supplicant客戶端交換機上：

```
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
```

在驗證器上：

```
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
```

這裡，連線埠使用**gcm-encrypt**模式，這表示流量經過驗證和加密，以及已正確進行SGT標籤。兩台裝置都沒有在ISE上使用任何特定的網路裝置授權策略，這意味著從裝置發起的所有流量都使用預設標籤**0**。此外，兩台交換器都信任從對等點收到的SGT（因為對等點原則下載階段的RADIUS屬性）。

環境和策略更新

將兩台裝置連線到CTS雲後，將啟動環境和策略更新。需要刷新環境才能獲得SGT和名稱，並且需要刷新策略才能下載在ISE上定義的SGACL。

在這個階段，請求方已經知道AAA伺服器的IP地址，因此它可以自己執行該操作。

有關環境和策略更新的詳細資訊，請參閱ASA和Catalyst 3750X系列交換機TrustSec配置示例和故障排除指南。

即使在未配置RADIUS伺服器時和CTS鏈路斷開時（指向身份驗證器交換機），請求方交換機仍會記住RADIUS伺服器IP地址。但是，可能會強制交換器將其遺忘：

```
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
```

若要驗證請求方交換機上的環境和策略，請輸入以下命令：

```
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
```

為什麼沒有顯示策略？不會顯示任何策略，因為必須啟用cts enforcement才能應用這些策略：

```
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
```

為什麼請求方只有一個**組Unknown**策略，而驗證方有更多？

```
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
```

使用者端的連線埠驗證

MS Windows客戶端已連線到3750-5交換機的**g1/0/1**埠並經過身份驗證：

```
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
```

這裡，交換器3750-5知道來自該主機的流量在傳送到CTS雲時應使用**SGT=3**進行標籤。

使用SGT進行流量標籤

如何嗅探和驗證流量？

這很難做到，因為：

- 只有IP流量支援嵌入式資料包捕獲（這是帶SGT和MACsec負載的修改後的乙太網幀）。
- 使用**replication**關鍵字的交換連線埠分析器(SPAN)連線埠 — 這可能會起作用，但問題在於，任

何Wireshark連線到監控作業階段的目的地連線埠的PC都會因為缺乏支援的802.1ae（可能發生在硬體層級）而捨棄訊框。
- 不帶**replication**關鍵字的SPAN連線埠會移除**cts**標頭，然後再將其置於目的地連線埠。

使用SGACL實施策略

CTS雲中的策略實施始終在目的地埠完成。這是因為只有最後一個裝置知道直接連線到該交換機的終端裝置的目標SGT。資料包僅攜帶源SGT。需要源和目標SGT才能做出決定。

這就是裝置不需要從ISE下載所有策略的原因。相反，它們只需要策略中與裝置直接連線裝置的SGT相關的部分。

這是3750-6，即請求方交換器：

```
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
```

這裡有兩個策略。第一個是未標籤流量（來往/來）的預設值。第二個是從**SGT=2**到未標籤的SGT，即**0**。存在此策略是因為裝置本身使用來自ISE的SGA策略，並且屬於**SGT=0**。此外，**SGT=0**是預設標籤。因此，您必須下載所有具有流量傳入/傳出**SGT=0規則的策略**。如果檢視該矩陣，您只會看到一個這樣的策略：**從2到0**。

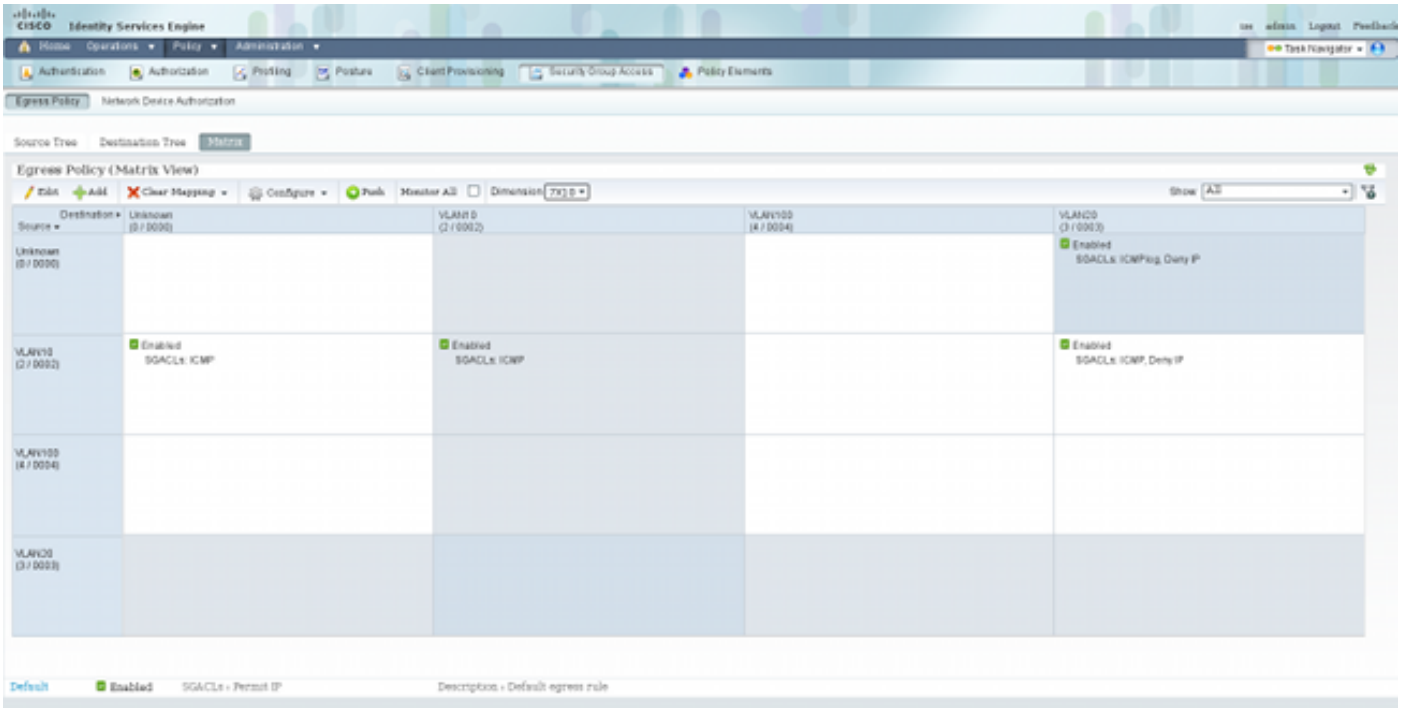
以下是3750-5，即驗證器交換器：

```
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
```

這裡還有一個策略：**從2到3**。這是因為802.1x客戶端(MS Windows)連線到**g1/0/1並**使用**SGT=3標籤**。這就是您必須將所有策略下**載到SGT=3的原因**。

嘗試從3750X-6(**SGT=0**)ping MS Windows XP(**SGT=3**)。3750X-5是執行裝置。

在此之前，必須在ISE上為從**SGT=0到SGT=3的流量配置策略**。此範例建立一個SGACL網際網路控制訊息通訊協定(ICMP)記錄檔，其中僅包含**permit icmp log**行，並將其用於從**SGT=0到SGT=3的流量的矩陣中**:



以下是執行交換器上的原則更新，以及新原則的驗證：

```
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
```

若要確認存取控制清單(ACL)是否從ISE下載，請輸入以下命令：

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

若要驗證是否已應用ACL（硬體支援），請輸入以下命令：

```
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
```

以下是ICMP之前的計數器：

```
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
```

以下是從SGT=0(3750-6交換器)對MS Windows XP(SGT=3)和計數器執行的ping:

```
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
```

以下是ACL計數器：

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

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- Cisco TrustSec 3750配置指南
- 適用於ASA 9.1的Cisco TrustSec配置指南
- Cisco TrustSec部署和路線圖
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。