ASA と Catalyst 3750X シリーズ スイッチ TrustSec の設定例とトラブルシューティング ガイド

内容

概要

この記事では、Cisco セキュア適応型セキュリティ アプライアンス（ASA）と Cisco Catalyst 3750X シリーズ スイッチ（3750X）上で Cisco TrustSec（CTS）を設定する方法について説明します。

セキュリティ グループ タグ（SGT）と IP アドレス間のマッピングを取得するため、ASA は SGT Exchange Protocol（SGT）を使用します。次に、SGT に基づくアクセス コントロール リストを使用して、トラフィックをフィルタリングします。3750X は、ロールベースのアクセス コントロール リスト（RBACL）を Cisco Identity Services Engine（ISE）からダウンロードし、それらに基づいてトラフィックをフィルタリングします。この記事では、通信の動作や予期されるデバッグについて説明するため、パケット レベルの詳細を示します。

前提条件

要件

次の項目に関する基本的な知識が推奨されます。

- CTS のコンポーネント
- ASA および Cisco IOS の CLI 設定

使用するコンポーネント

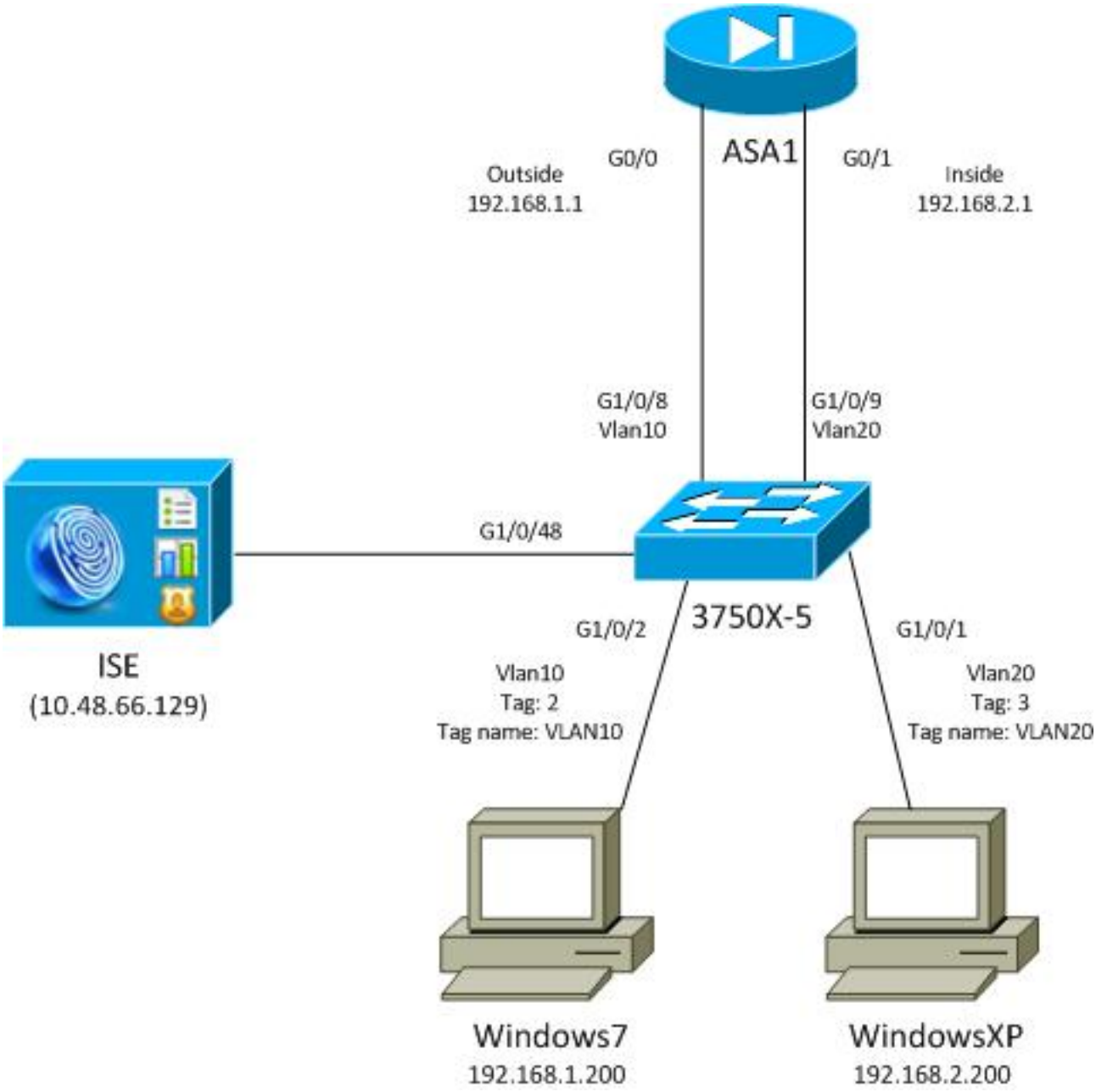
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ASA ソフトウェア バージョン 9.1 以降
- Microsoft（MS）Windows 7 および MS Windows XP
- Cisco 3750X ソフトウェア バージョン 15.0 以降
- Cisco ISE ソフトウェア バージョン 1.1.4 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

ネットワーク図



Traffic flow

次に、トラフィック フローを示します。

- ポート認証のため、3750X を **G1/0/1 および G1/0/2 で設定します。**
- ISE は認証、認可、およびアカウンティング（AAA）サーバとして使用されます。
- MAC アドレス バイパス（MAB）は MS Windows 7 の認証に使用されます。
- IEEE 802.1x は、使用する認証方式が問題とならないことを示すために、MS Windows XP に使用されます。

正常に認証されると、ISE は SGT を返し、3750X はそのタグを認証セッションにバインドします。また、両方のステーションの IP アドレスを **ip device tracking** コマンドを使用して学習します。次に、スイッチは SXP を使用して、SGT と IP アドレス間のマッピング テーブルを ASA に送信します。両方の MS Windows PC に ASA を示すデフォルトのルーティングがあります。

SGT にマッピングされた IP アドレスからのトラフィックを ASA が受信すると、SGT に基づいて ACL を使用できるようになります。また、3750X をルータ（両方の MS Windows ステーションのデフォルト ゲートウェイ）として使用している場合は、ISE からダウンロードされたポリシ

ーに基づいてトラフィックをフィルタリングできます。

次に、設定と検証のステップを示します。それぞれのステップについては、このドキュメントのそれぞれのセクションで詳しく説明します。

- ip device tracking コマンドを使用した 3750X でのポート認証
- 認証、SGT、およびセキュリティ グループ アクセス コントロール リスト（SGACL）のポリシーの認証用の ISE 設定
- ASA および 3750X での CTS 設定
- 3750X（自動）および ASA（手動）での Protected Access Credential（PAC）のプロビジョニング
- ASA および 3750X での環境の更新
- 3750X でのポート認証の検証および適用
- 3750X でのポリシーの更新
- SXP 交換（リスナーとしての ASA、スピーカーとしての 3750X）
- SGT ACL を使用した ASA でのトラフィック フィルタリング
- ISE からダウンロードしたポリシーを使用した 3750X でのトラフィック フィルタリング

設定

ip device tracking コマンドを使用した 3750X でのポート認証

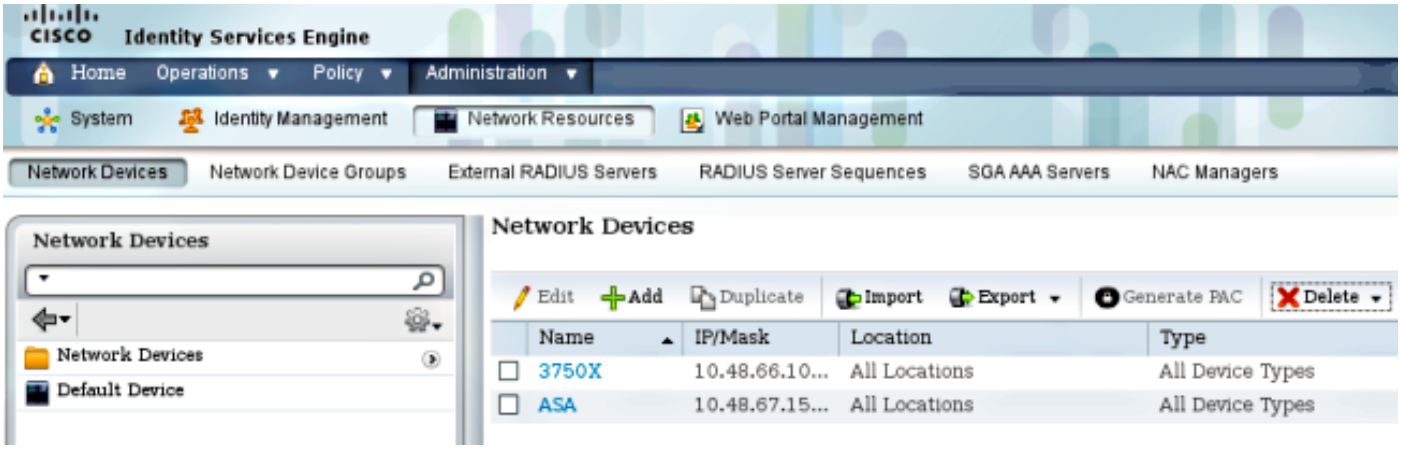
これは、802.1x または MAB の一般的な設定です。ISE からアクティブな通知を使用している場合にのみ、RADIUS の認可変更（CoA）が必要です。

```
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
```

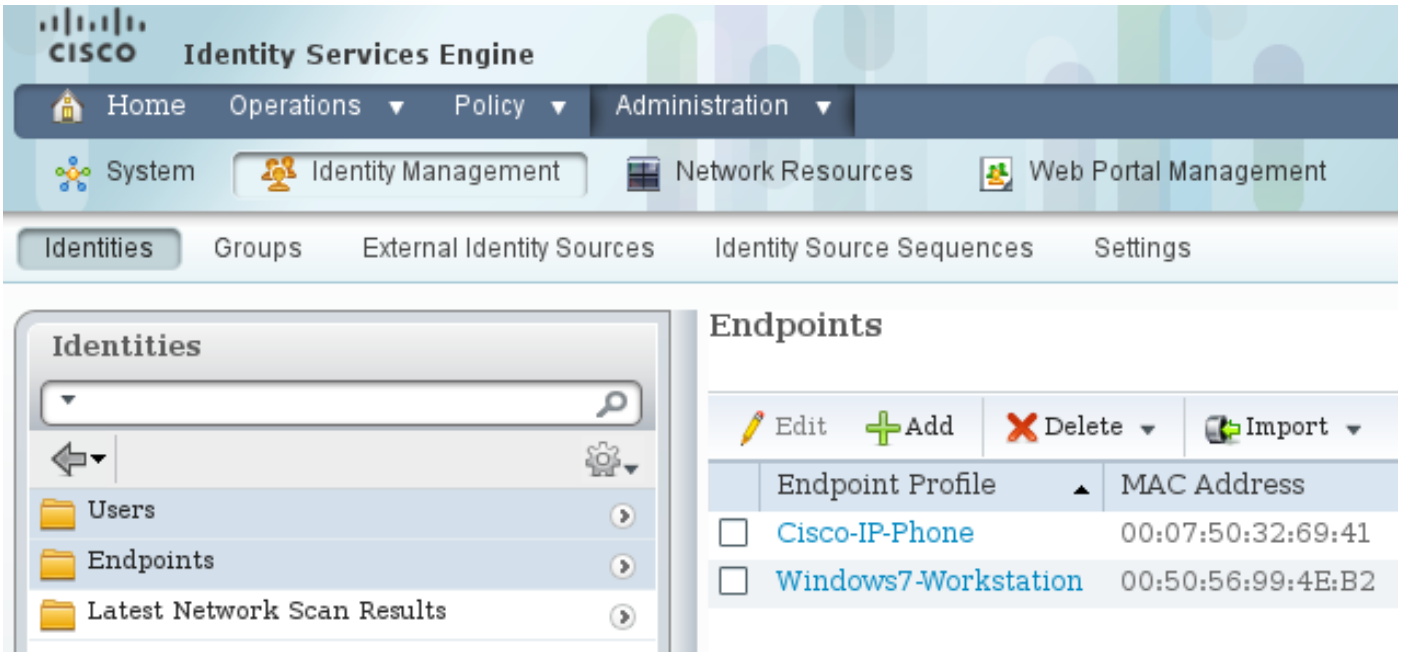
```
spanning-tree portfast

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
```

認証、SGT、および SGACL のポリシーの ISE 設定

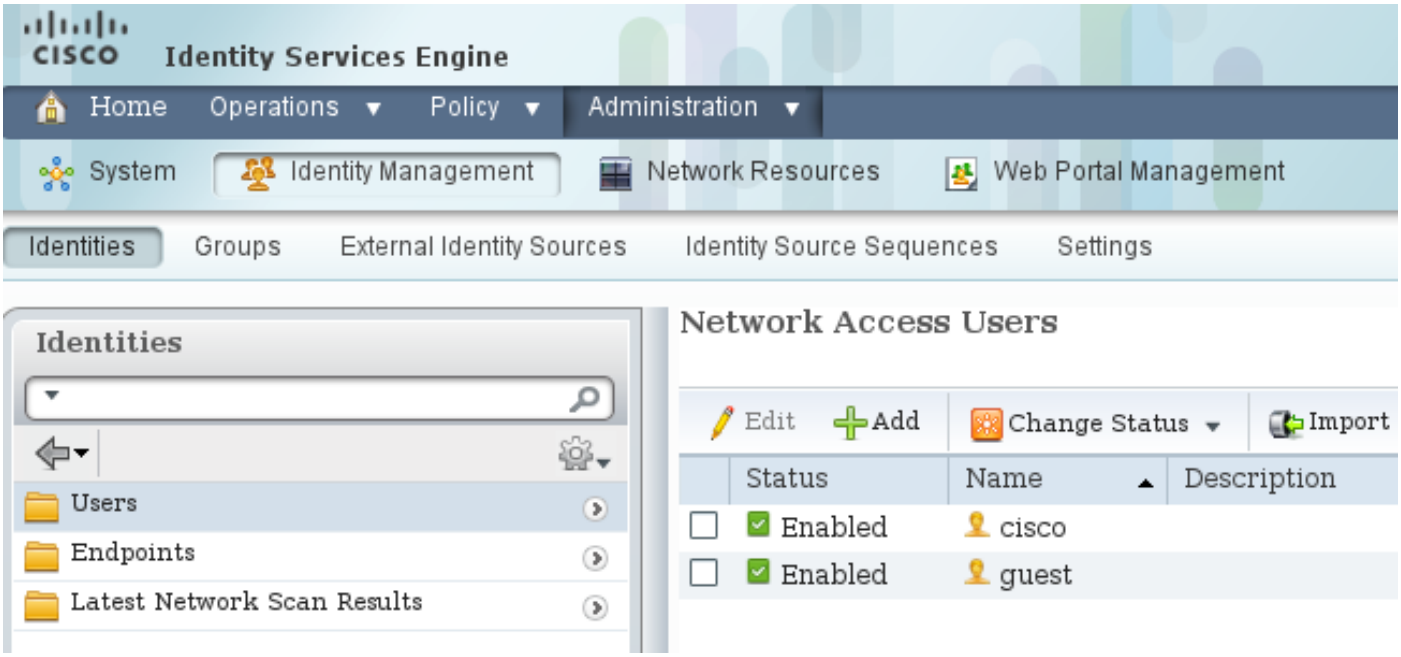
ISE には、[Administration] > [Network Devices] で設定したネットワーク デバイスが両方とも必要です。



MAB 認証を使用する MS Windows 7 の場合、[Administration] > [Identity Management] > [Identities] > [Endpoints] でエンドポイント ID（MAC アドレス）を作成する必要があります。

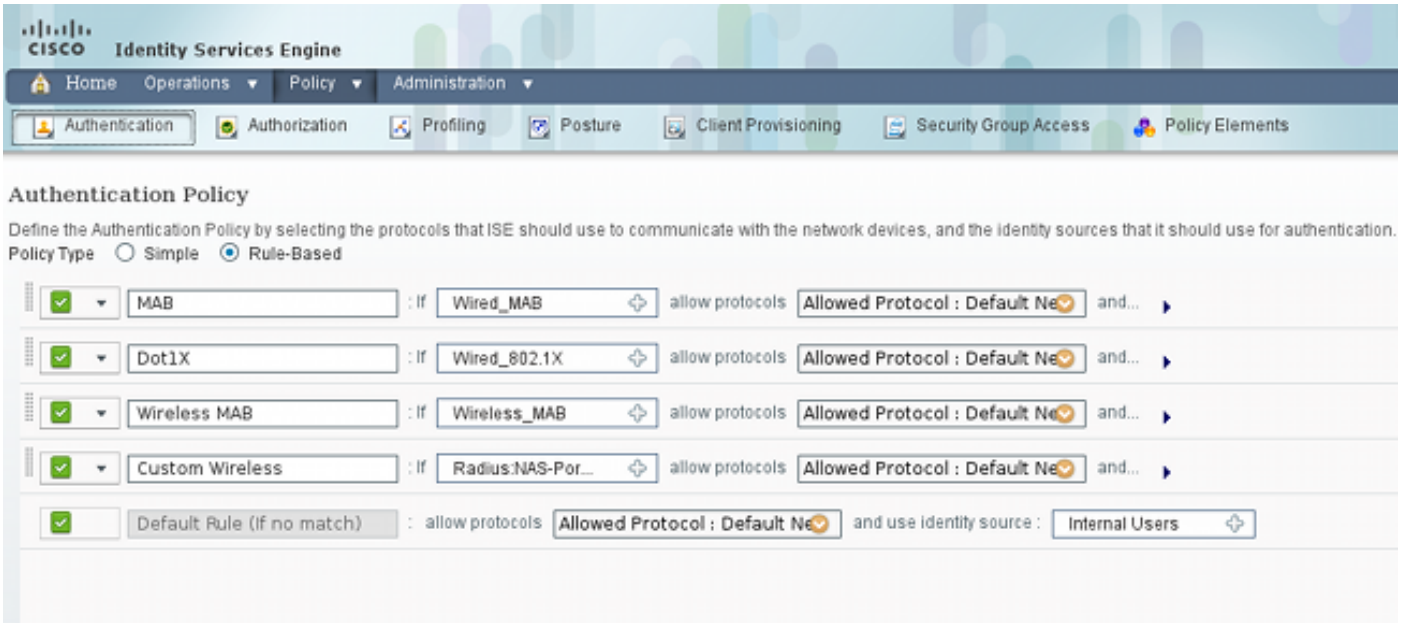


802.1x 認証を使用する MS Windows XP の場合、[Administration] > [Identity Management] > [Identities] > [Users] でユーザ ID（ユーザ名）を作成する必要があります。

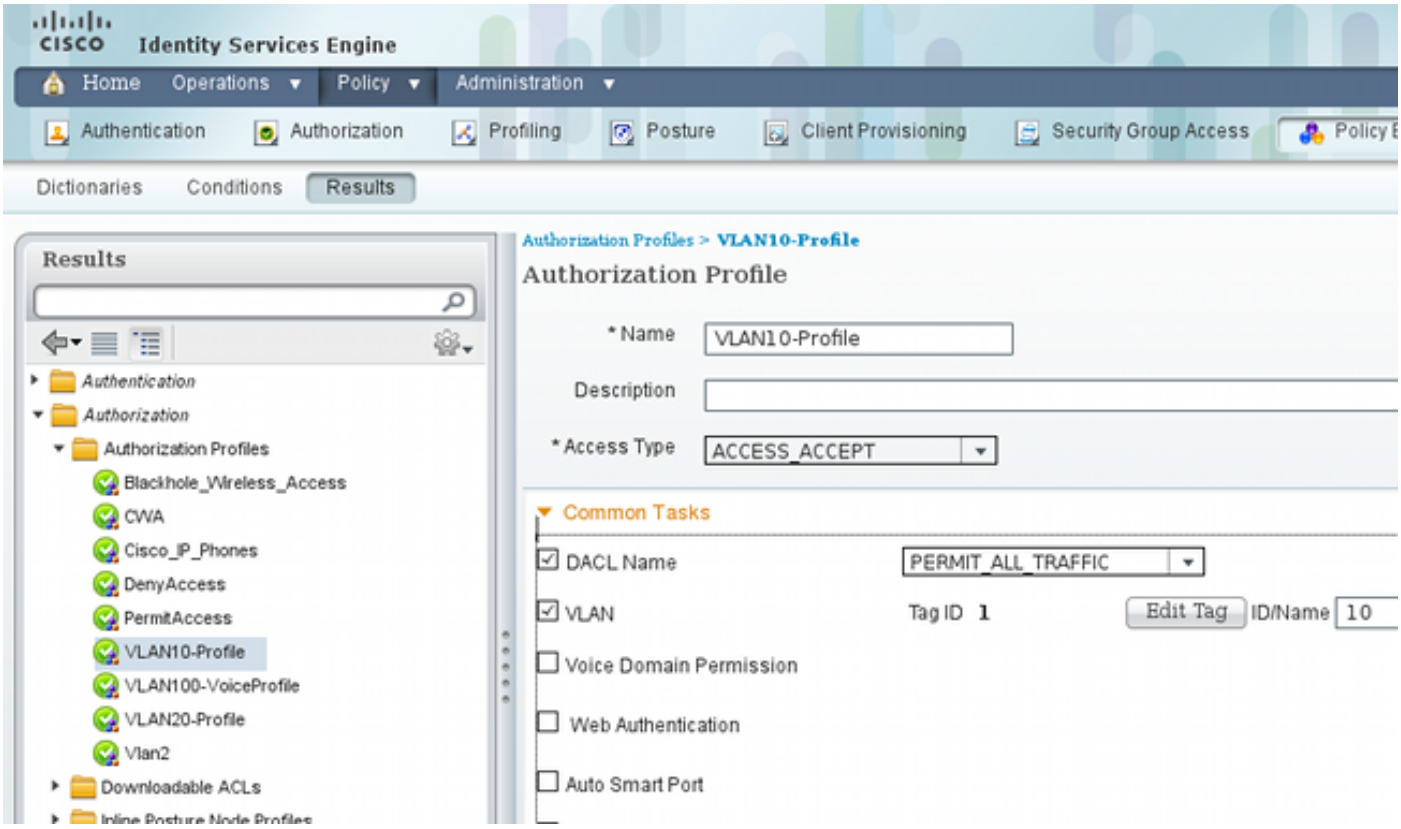


ユーザ名 **cisco** が使用されます。これらのクレデンシャルを使用して、MS Windows XP を Extensible Authentication Protocol-Protected EAP（EAP-PEAP）用に設定します。

ISE では、デフォルトの認証ポリシーが使用されます（これを変更しないでください）。最初に MAB 認証用のポリシー、2 番目に 802.1x 認証用が使用されます。



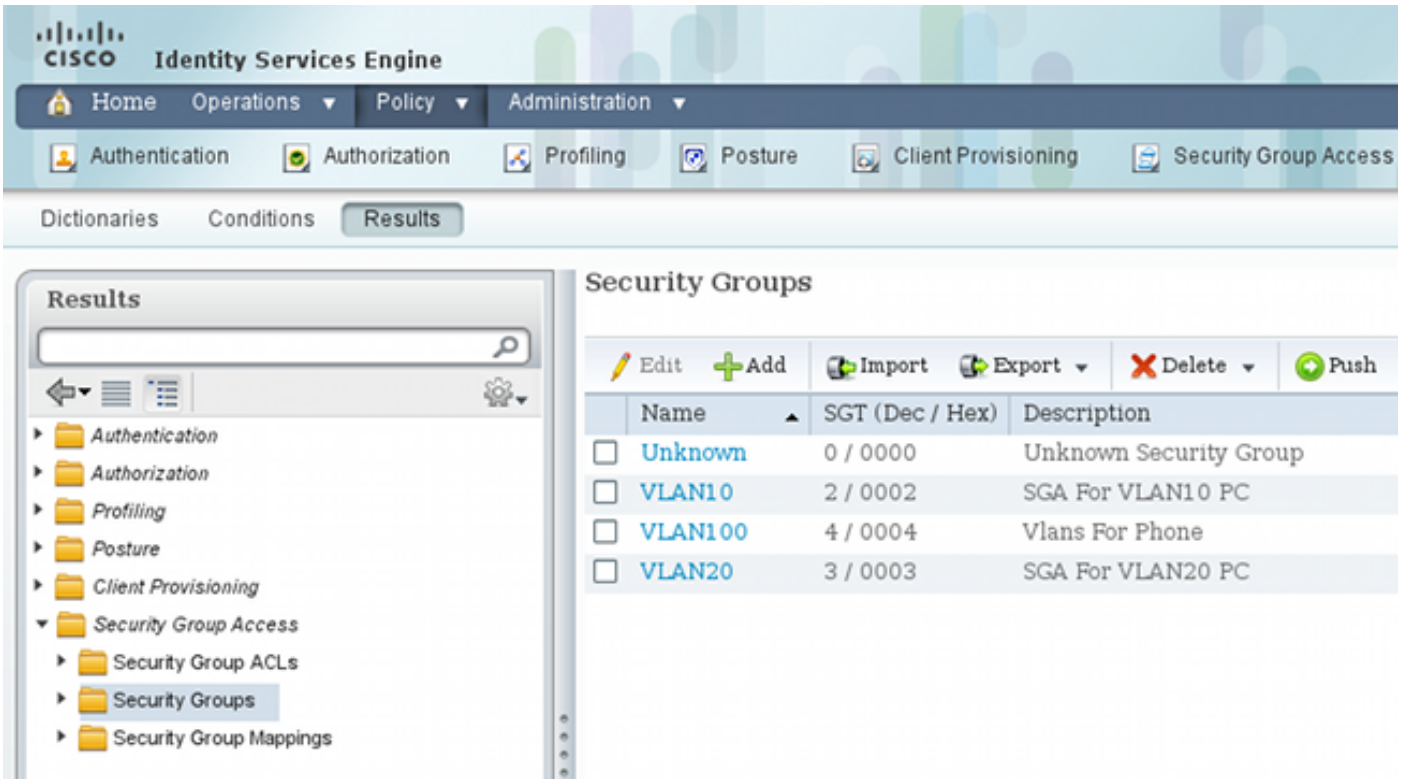
認可ポリシーを設定するには、[Policy] > [Results] > [Authorization] > [Authorization Profiles] で認可プロファイルを定義する必要があります。MS Windows 7 のプロファイルには、すべてのトラフィックを許可するダウンロード可能な ACL（DACL）を備えた VLAN10-Profile を使用します。



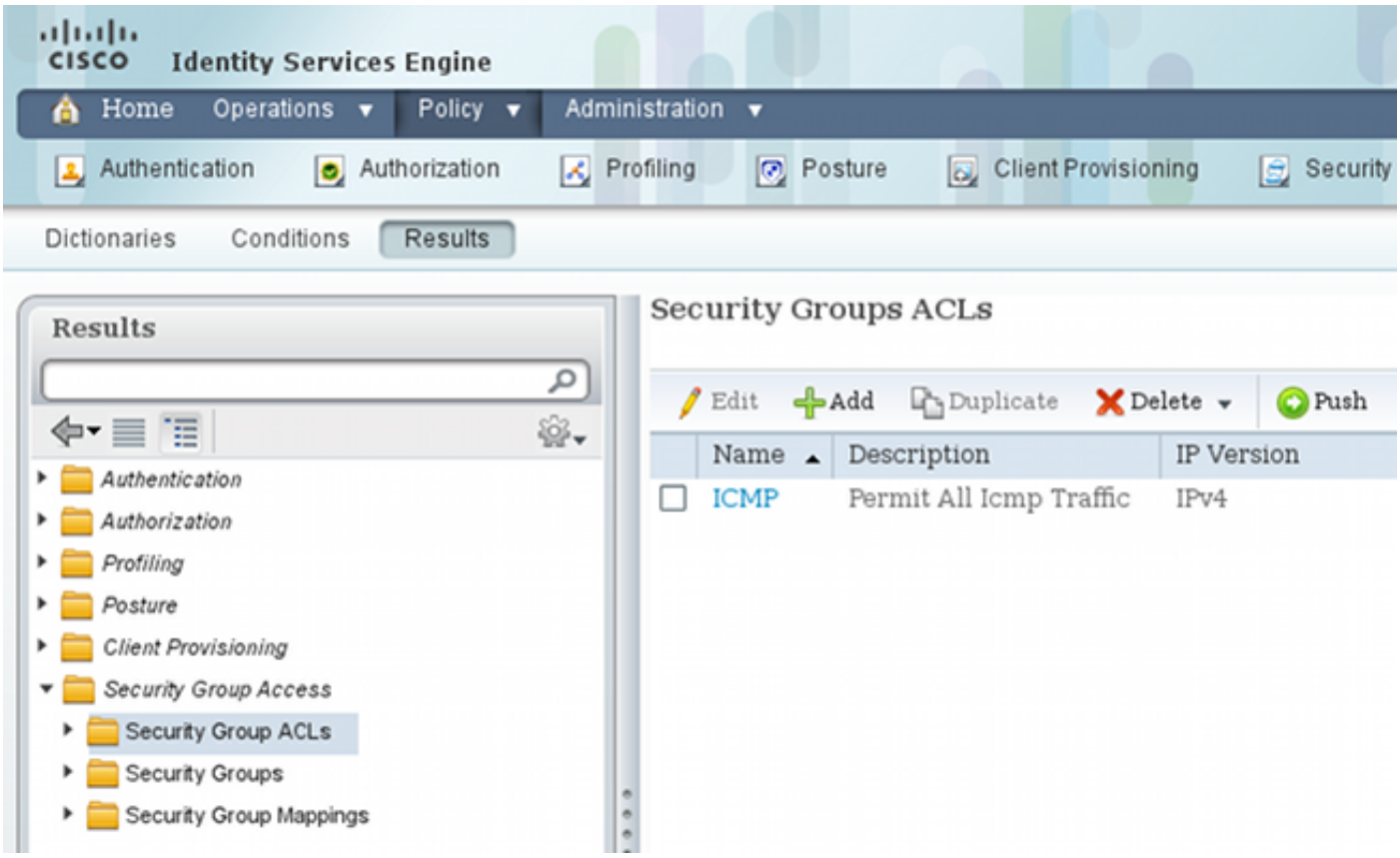
MS Windows XP には、VLAN 番号（20）以外は同様の設定である VLAN20-Profile を使用します。

ISE で SGT グループ（タグ）を設定するには、[Policy] > [Results] > [Security Group Access] > [Security Groups] に移動します。

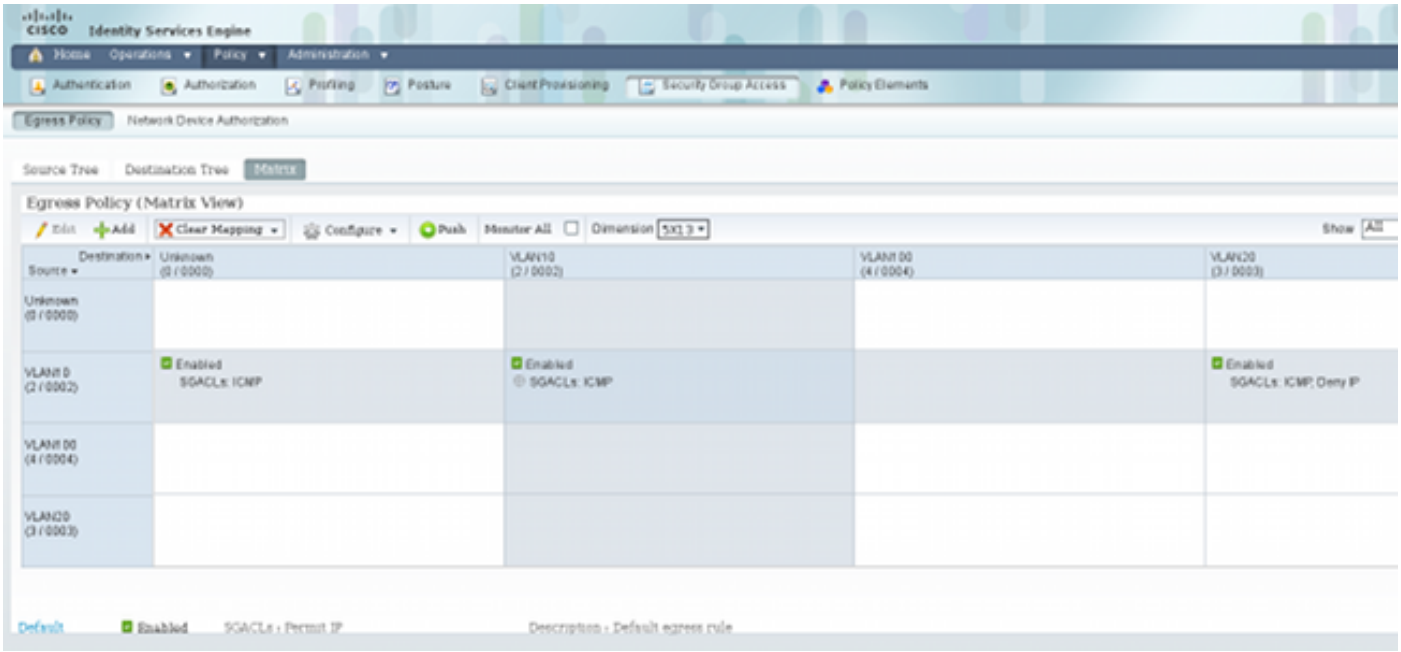
> **注**：タグ番号は選択できません。1を除く最初の空き番号によって自動的に選択されます。設定できるのは SGT 名のみです。



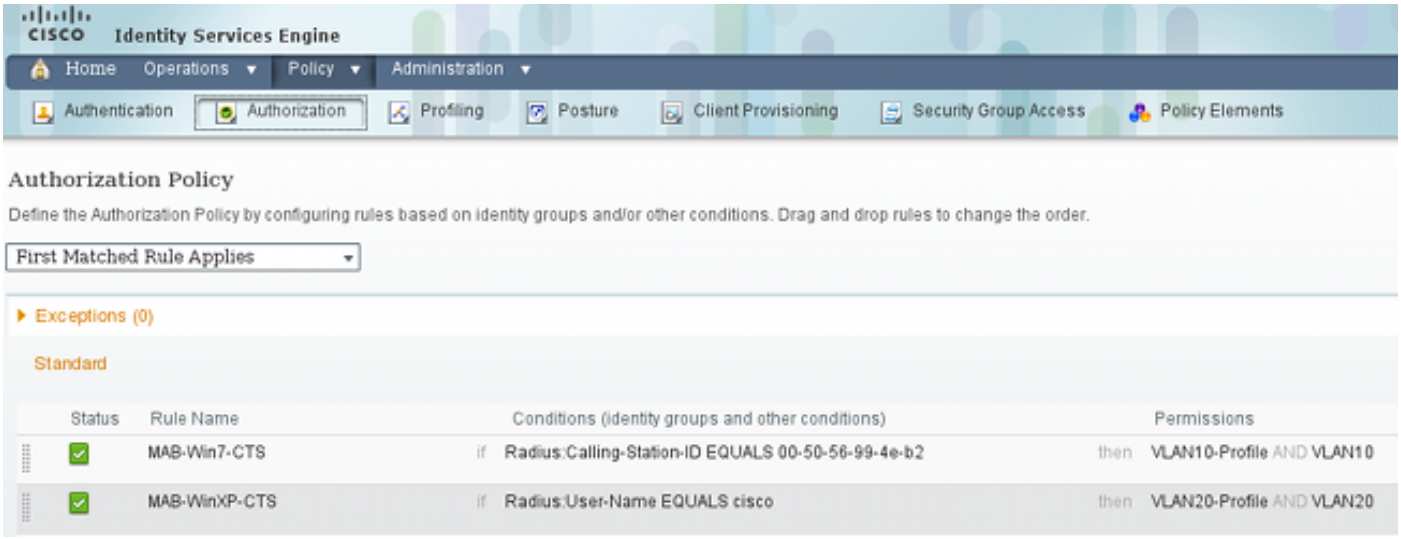
SGACL を作成して Internet Control Message Protocol（ICMP）トラフィックを許可するには、[Policy] > [Results] > [Security Group Access] > [Security Group ACLs] に移動します。



ポリシーを作成するには、[Policy] > [Security Group Access] > [Egress Policy] に移動します。VLAN10 と未知の VLAN か VLAN10、または VLAN20 間のトラフィックには、ICMP ACL を使用します（**permit icmp**）。



認可ルールを設定するには、[Policy] > [Authorization] に移動します。MS Windows 7（特定の MAC アドレス）の場合、**VLAN10-Profile を使用して VLAN10 および DACL と、VLAN10** という SGT を持つセキュリティ プロファイル VLAN10 を返します。MS Windows XP（特定のユーザ名）の場合、**VLAN20-Profile を使用して VLAN 20 および DACL と、VLAN20** という SGT を持つセキュリティ プロファイル VLAN20 を返します。



SGT RADIUS 属性を承認するためのスイッチと ASA 設定を終了します。

ASA および 3750X での CTS 設定

基本的な CTS 設定を行う必要があります。3750X では、ダウンロードするサーバ ポリシーを指定する必要があります。

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

ASA では、AAA サーバと、そのサーバを示す CTS のみが必要です。

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

> **注**:3750Xでは、**group radius**コマンドを使用してISEサーバを明示的に指定する必要があります。これは、3750X が自動 PAC プロビジョニングを使用するためです。

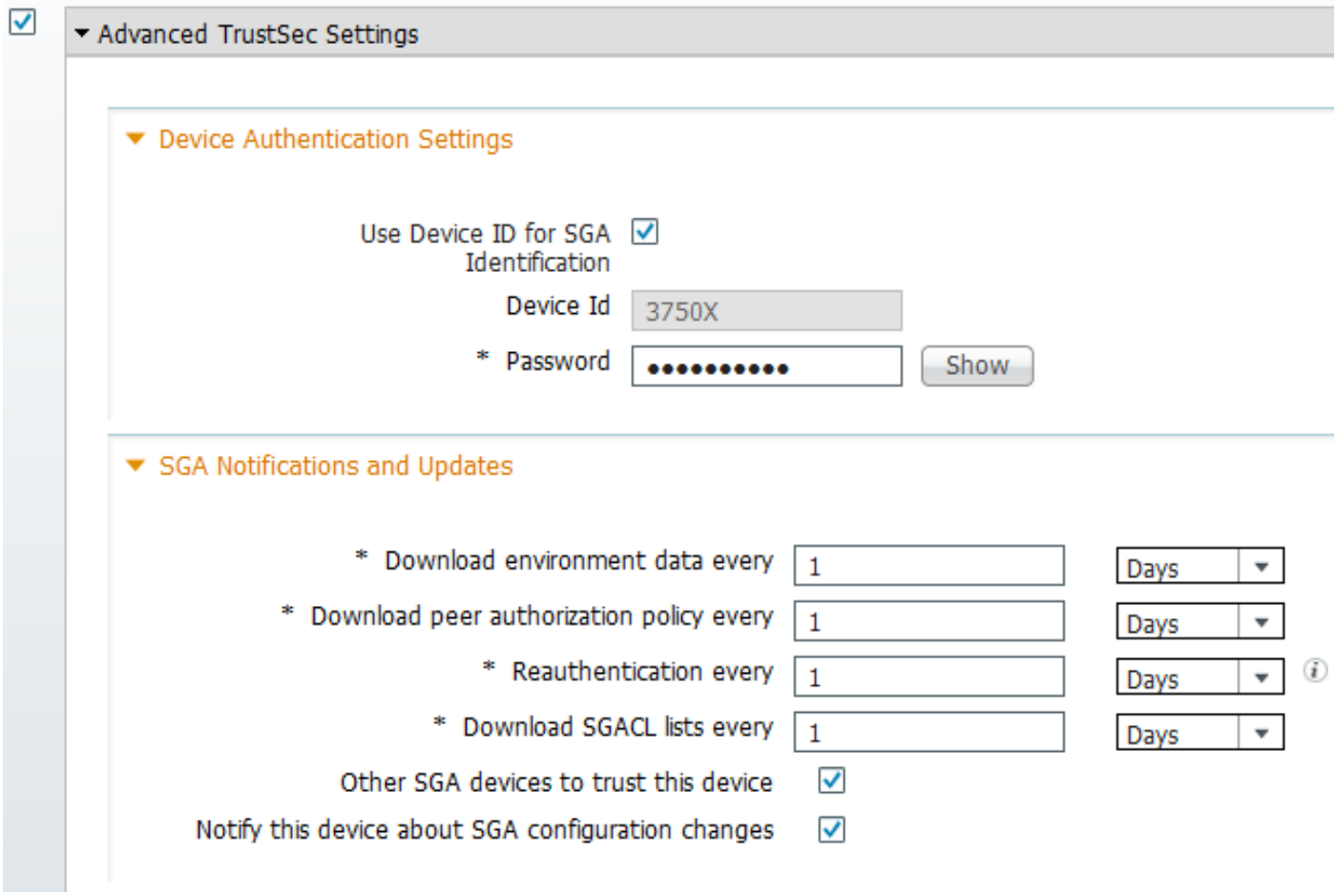
3750X（自動）および ASA（手動）での PAC プロビジョニング

CTS クラウド内の各デバイスは、他のデバイスによって信頼されるように、認証サーバ（ISE）の認証が必要です。これには、Extensible Authentication Protocol-Flexible Authentication via Secure Protocol（EAP-FAST）方式（RFC 4851）を使用します。この方式には、PAC が提供するアウトオブバンドが必要です。また、このプロセスは **phase0** とも呼ばれ、RFC では定義されていません。EAP-FAST 用の PAC には Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）の証明書と同じロールがあります。PAC を使用して phase2 の認証に必要なセキュア トンネル（phase1）を確立します。

3750X での PAC プロビジョニング

3750X は自動 PAC プロビジョニングをサポートします。スイッチと ISE で共有パスワードを使用して PAC をダウンロードします。このパスワードと ID は [Administration] > [Network Resources] > [Network Devices] で ISE に設定する必要があります。スイッチを選択し、

[Advanced TrustSec Settings] **セクションを展開して設定を行います。**



PAC にこれらのクレデンシャルを使用させるには、次のコマンドを入力します。

```
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
```

ASA での PAC プロビジョニング

ASA は手動 PAC プロビジョニングのみをサポートします。つまり、（ネットワーク デバイス /ASA の）ISE で手動で生成する必要があります。

次に、そのファイルを（FTP などで）インストールします。

```
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:
   000200a800030001000400010c40a15a339286ceac28a50dbbac597840006008c000301
   0003d64668f2badc76e251683394b3d5690000001351d15dd900093a8044df74b2b71f
   e667d7b908db7aeea3229e61462bdb70f46580bef9425011126bbf6c2f4212ccdacf08
   c01ddbc7608c3a1ddeb996ba9bfbd1b207281e3edc9ff61b9e800f225dc3f82bd5f794
   7e0a86bee8a3d437af93f54e61858bac877c58d3fe0ec6be54b4c75fad23e1fd
```

ASA および 3750X での環境の更新

この段階で、どちらのデバイスにも PAC が正しくインストールされています。また、ISE 環境データのダウンロードが自動的に開始されます。このデータは基本的にタグ番号とそれらの名前です。ASA で環境の更新をトリガーするには、次のコマンドを入力します。

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

ASA 上で確認するには（特定の SGT タグ/名前を表示することはできませんが、後で検証されます）、次のコマンドを入力します。

```
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)
```

3750X 上でこれを確認するには、次のコマンドで環境の更新をトリガーします。

```
bsns-3750-5#cts refresh environment-data
```
その結果を検証するには、次のコマンドを入力します。

```
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
```
これには、すべてのタグと、それらに対応する名前が正しくダウンロードされていることが示されます。

3750X でのポート認証の検証および適用

3750X に環境データが備わったら、認証されたセッションに SGT が適用されていることを確認する必要があります。

MS Windows 7 が正しく認証されていることを確認するには、次のコマンドを入力します。

```
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:  C0A800010000001002B67334C
```

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

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

出力には、VLAN10 と SGT 0002 およびすべてのトラフィックを許可する DACL が使用されていることが示されます。

MS Windows XP が正しく認証されていることを確認するには、次のコマンドを入力します。

```
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
```

出力には、VLAN20 と SGT 0003 およびすべてのトラフィックを許可する DACL が使用されていることが示されます。

ip device tracking 機能によって IP アドレスが検出されます。DHCP スイッチを **DHCP スヌーピング**用に設定する必要があります。次に、DHCP スヌーピング応答の後、クライアントの IP アドレスが学習されます。静的に設定された IP アドレスの場合 (次の例を参照) 、**arp snooping** 機能が使用されます。また、PC はスイッチに対するすべてのパケットを IP アドレスが検出できるように送信する必要があります。

デバイス トラッキングの場合、ポート上でこれを有効するには隠しコマンドが必要な場合があります。

```
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
```

3750X でのポリシーの更新

3750X は（ASA とは異なり）ISE からポリシーをダウンロードできます。ポリシーをダウンロードして、適用する前に、次のコマンドで 3750X を有効にする必要があります。

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

有効にしないと、ポリシーをダウンロードしてもインストールされず、適用されません。

ポリシーの更新をトリガーするには、次のコマンドを入力します。

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

ISE からポリシーがダウンロードされていることを確認するには、次のコマンドを入力します。

```
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
```

出力には、ポリシーの必要な部分のみがダウンロードされていることが示されます。

CTS クラウドでは、パケットに送信元ホストの SGT が含まれており、**宛先デバイスで適用されます**。つまり、パケットは送信元から、宛先ホストに直接接続されている最後のデバイスに転送されます。そのデバイスは、直接接続されたそれ自体のホストの SGT を把握しており、送信元 SGT を持つ着信パケットを特定の宛先 SGT に許可または拒否する必要があることも認識しているため、適用ポイントとなります。

この決定は、ISE からダウンロードされたポリシーに基づきます。

このシナリオでは、すべてのポリシーがダウンロードされます。ただし、MS Windows XP の認証セッション（SGT=VLAN20）をクリアした場合は、VLAN20 に対応するポリシー（ロウ）をスイッチがダウンロードする必要はありません。これは、スイッチに接続されたその SGT からのデバイスがそれ以上ないためです。

[Advanced (Troubleshooting)] セクションには、3750X がダウンロードする必要があるポリシーを決定する方法と、パケット レベルの説明が示されます。

SXP 交換（リスナーとしての ASA、スピーカーとしての 3750X）

ASA では SGT がサポートされていません。SGT を持つすべてのフレームが ASA によってドロップされます。これが、3750X が SGT のタグ付きフレームを ASA に送信できない理由です。その代わりに、SXP が使用されます。このプロトコルでは、IP アドレスと SGT 間のマッピングに関するスイッチからの情報を受信することができます。その情報を使用して、ASA では、IP アドレスを SGT にマッピングし、SGACL に基づいて決定することができます。

スピーカーとして 3750X を設定するには、次のコマンドを入力します。

```
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
```

リスナーとして ASA を設定するには、次のコマンドを入力します。

```
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
```

ASA がマッピングを受信したことを確認するには、次のコマンドを入力します。

```
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
```

ここで、送信元 IP アドレス 192.168.1.200 の着信パケットを ASA が受信すると、そのパケットを SGT=2 から着信したかのように処理できます。送信元 IP アドレス が 192.168.200.2 の場合は、SGT=3 から着信したかのように処理できます。同様なことが、宛先 IP アドレスにも当てはまります。

> **注**:3750Xは、関連付けられたホストのIPアドレスを認識する必要があります。これは、IP デバイスのトラッキングにより行われます。エンド ホストの静的に設定された IP アドレスの場合、スイッチは認証後にすべてのパケットを受信する必要があります。これによって、IP デバイスのトラッキングがトリガーされ、IP アドレスが検出されて SXP 更新をトリガーされます。SGT のみが認識されている場合、SXP では送信されません。

SGT ACL を使用した ASA でのトラフィック フィルタリング

次に、ASA 設定チェックを示します。

```
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
```

ACL が作成され、内部インターフェイスに適用されます。**SGT=3 から SGT=2 (VLAN10 という**) へのすべての ICMP トラフィックが許可されます。

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

注：タグ番号またはタグ名を使用できます。

送信元 IP アドレス **192.168.2.200** (**SGT=3**) の MS Windows XP から IP アドレス **192.168.1.200** (**SGT=2**) の MS Windows 7 に ping すると、ASA は接続を構築します。

```
%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)
```

Telnet で同じことを試みると、トラフィックがブロックされます。

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

ASA にはより多くの設定オプションがあります。送信元と宛先の両方にセキュリティ タグと IP アドレスの両方を使用することができます。このルールでは、**SGT タグ = 3**、IP アドレス 192.168.2.200 から SGT タグが **VLAN10 という名前で宛先ホスト アドレスが 192.168.1.200** への ICMP エコー トラフィックを許可します。

```
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
```

これもオブジェクト グループで実行できます。

```
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
```

ISE (RBACL) からダウンロードしたポリシーを使用した 3750X でのトラフィック フィルタリ

ング

スイッチにローカル ポリシーを定義することも可能です。ただし、この例には ISE からダウンロードされたポリシーが存在しています。ASA で定義されているポリシーでは、1 つのルールに IP アドレスと SGT (および Active Directory からのユーザ名) の両方を使用することが許可されます。スイッチで定義されているポリシー (ローカルと ISE からの両方) では、SGT のみが許可されます。ルールに IP アドレスを使用することが必要な場合は、ASA でのフィルタリングを推奨します。

MS Windows XP と MS Windows 7 間の ICMP トラフィックがテストされます。このため、デフォルト ゲートウェイを ASA から MS Windows 上の 3750X に変更する必要があります。3750X にはルーティング インターフェイスがあり、パケットをルーティングできます。

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

ポリシーは ISE からすでにダウンロードされています。それらのポリシーを確認するには、次のコマンドを入力します。

```
 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
```

VLAN10 (MS Windows 7) から **VLAN20 (MS WindowsXP) へのトラフィックは、ISE からダウンロードされた ICMP-20 ACL の対象です。**

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

ACL 確認するには、次のコマンドを入力します。

```
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
```

SGT マッピングを確認して両方のホストからのトラフィックが正しくタグ付けされていることを確認するには、次のコマンドを入力します。

```
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
```

MS Windows 7（**SGT=2**）から MS Windows XP（**SGT=3**）への ICMP は ACL ICMP-20 で十分に機能します。**2 から 3 へのトラフィックのカウンタ（15 個の許可されたパケット）をチェックすることで、これを確認できます。**

```
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
```

Telnet カウンタの使用を試みると、拒否されたパケットが増加します（ICMP-20 ACL では許可されていません）。

```
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
```

注：出力に表示されるアスタリスク(*)文字は、タグ付けされていないすべてのトラフィックに関連しています(ISEのMatrixでは、この列と行は**unknown**と呼ばれ、タグ番号**0**を使用します)。

ログ キーワード（ISE で定義）を持つ ACL エントリがある場合、対応するパケットの詳細と実行されたアクションは、ACL としてログ キーワードを使用して記録されます。

確認

検証手順については、個々の設定セクションを参照してください。

トラブルシュート

PAC プロビジョニング

自動 PAC プロビジョニングを使用すると問題があるように思える場合があります。RADIUS サーバには **pac キーワードを使用することを覚えておいてください。**3750X での自動 PAC プロビジョニングでは、EAP-FAST 方式と、Microsoft の Challenge Handshake Authentication Protocol を使用する内部方式の Extensible Authentication Protocol （EAP-MSCHAPv2）認証を使用します。デバッグの際に、複数の RADIUS メッセージが表示されます。これらは、認証用に設定した ID とパスワードで EAP-MSCHAPv2 を使用する、セキュア トンネルを構築するために使用した EAP-FAST ネゴシエーションの一部です。

最初の RADIUS 要求では、これが PAC 要求であることを ISE に通知するために AAA **service-type=cts-pac-provisioning を使用します。**

```
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.
```

出力の最後の RADIUS reject は、すでに PAC を受信しており、それ以上の認証プロセスを継続しなかったので、予期されています。

ISE とのその他すべての通信に PAC が必要であることを覚えておいてください。ただし、PAC がない場合でも、スイッチは設定された時点で環境またはポリシーの更新を試行します。その後、RADIUS 要求に **cts-opaqueue**（PAC）を追加しないため、障害が発生します。

PAC キーが間違っている場合、次のエラー メッセージが ISE に表示されます。

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

また、PAC キーが間違っている場合、スイッチでのデバッグ（**debug cts provisioning + debug radius**）により次の出力が表示されます。

```
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
```

最近の **radius server 表記法を使用している場合、次のように表示されます。**

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

> **注**:ISEでは、[Device Authentication Settings] で使用したものと同じパスワードを使用する必要があります。

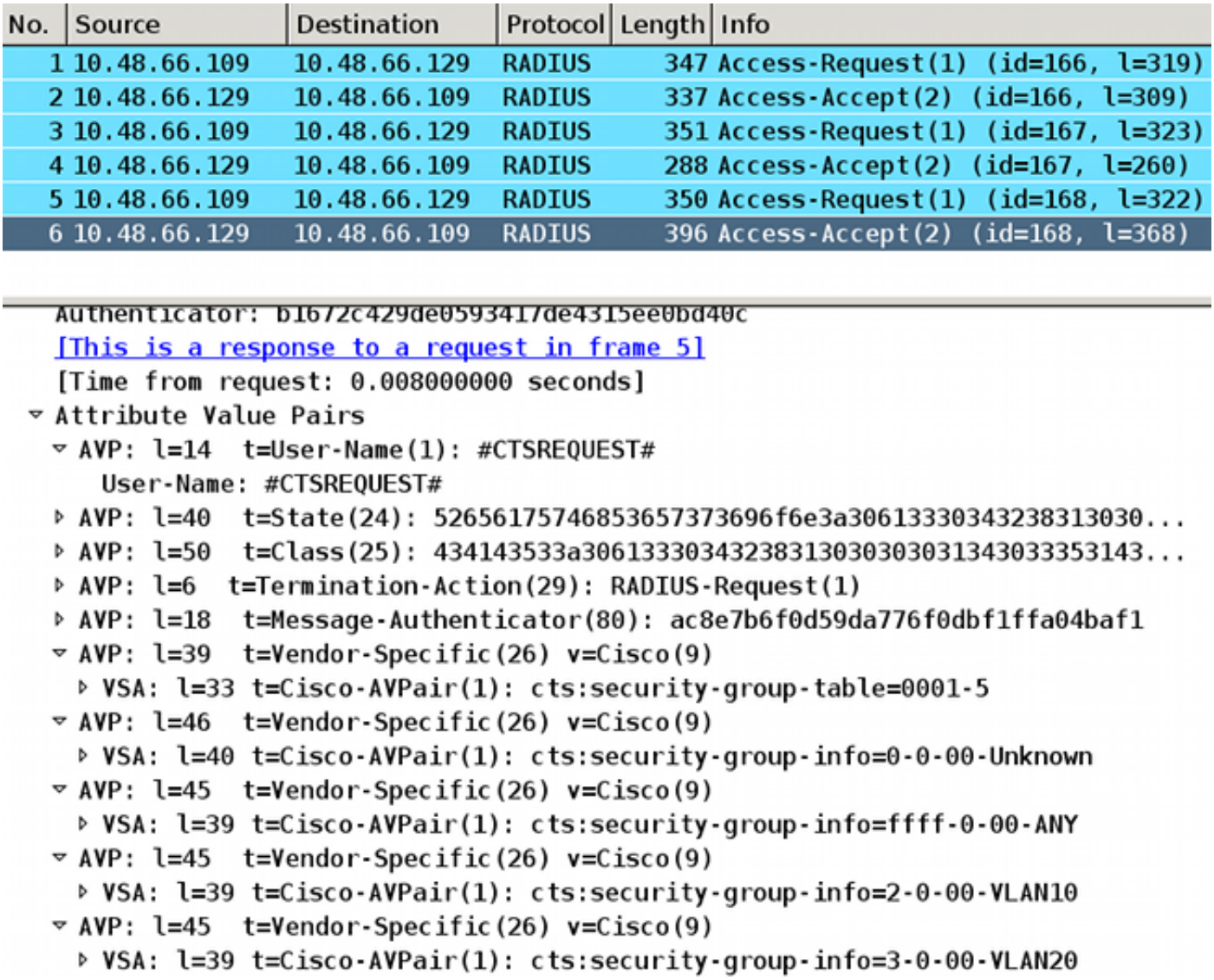
PAC プロビジョニングが正常に実行されると、ISE に次のように表示されます。

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)

環境の更新

環境の更新を使用して、SGT 番号と名前が含まれている基本的なデータを ISE から取得します。パケット レベルには、3 つの RADIUS 要求のみであることが表示され、属性で応答します。

最初の要求で、スイッチは **CTSServerlist** の名前を受け取ります。2 番目の要求で、スイッチはそのリストの詳細を受け取り、最後の要求ではタグと名前の付いたすべての SGT を受け取ります。



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)

デフォルトのSGT 0、ffff、および2つのカスタム定義が表示されます。SGTタグ2の名前はVLAN10で、SGTタグ3の名前はVLAN20です。

注：すべてのRADIUS**要求には、PACプロビジョニングの結果として**cts-pac-opaque**が含まれます。**

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)

SGT 3750X では、3 つのすべての RADIUS 応答とそれに対応するリスト、リストの詳細、および特定の SGT 内部リストについてデバッグが表示されます。

```
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)
```

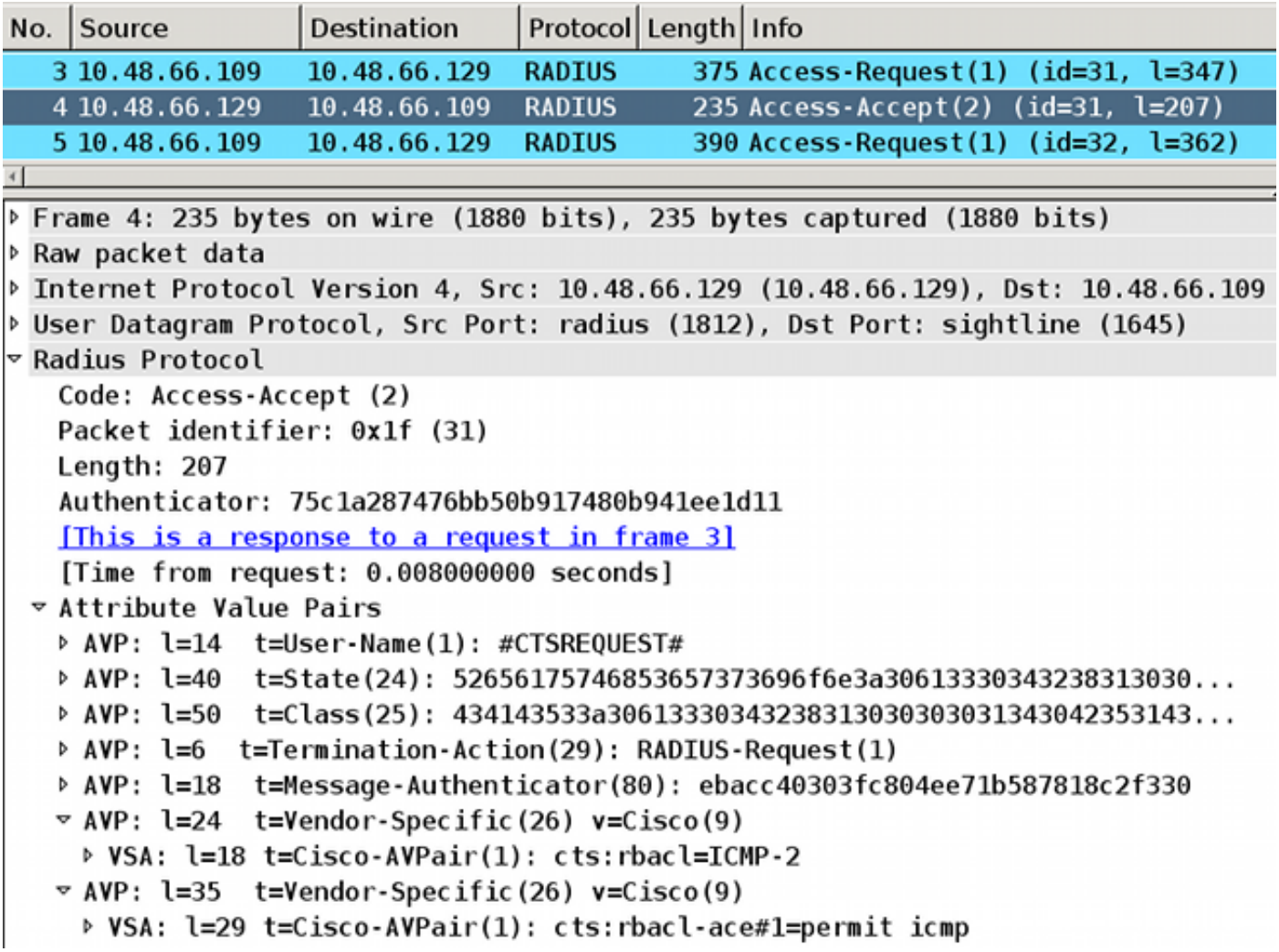
```
*Mar  1 10:05:18.099:     cts_env_data ASSESSING: during state env_data_assessing,
got event 3(env_data_incomplete)
*Mar  1 10:05:18.099: @@@ cts_env_data ASSESSING: env_data_assessing ->
env_data_waiting_rsp
*Mar  1 10:05:18.099: env_data_waiting_rsp_enter: state = WAITING_RESPONSE
*Mar  1 10:05:18.099: 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
```

ポリシーの更新

ポリシーの更新は、スイッチ上でのみサポートされます。これは、環境の更新と似ています。RADIUS の要求と応答にすぎません。

スイッチはデフォルト リスト内のすべての ACL を要求します。次に、最新ではない（または存在していない）各 ACL に、別の要求を送信して詳細を取得します。

次に、ICMP-20 ACL を要求する応答例を示します。



その ACL を適用するには、**cts role-based enforcement を設定しておく必要があることを覚えておいてください。**

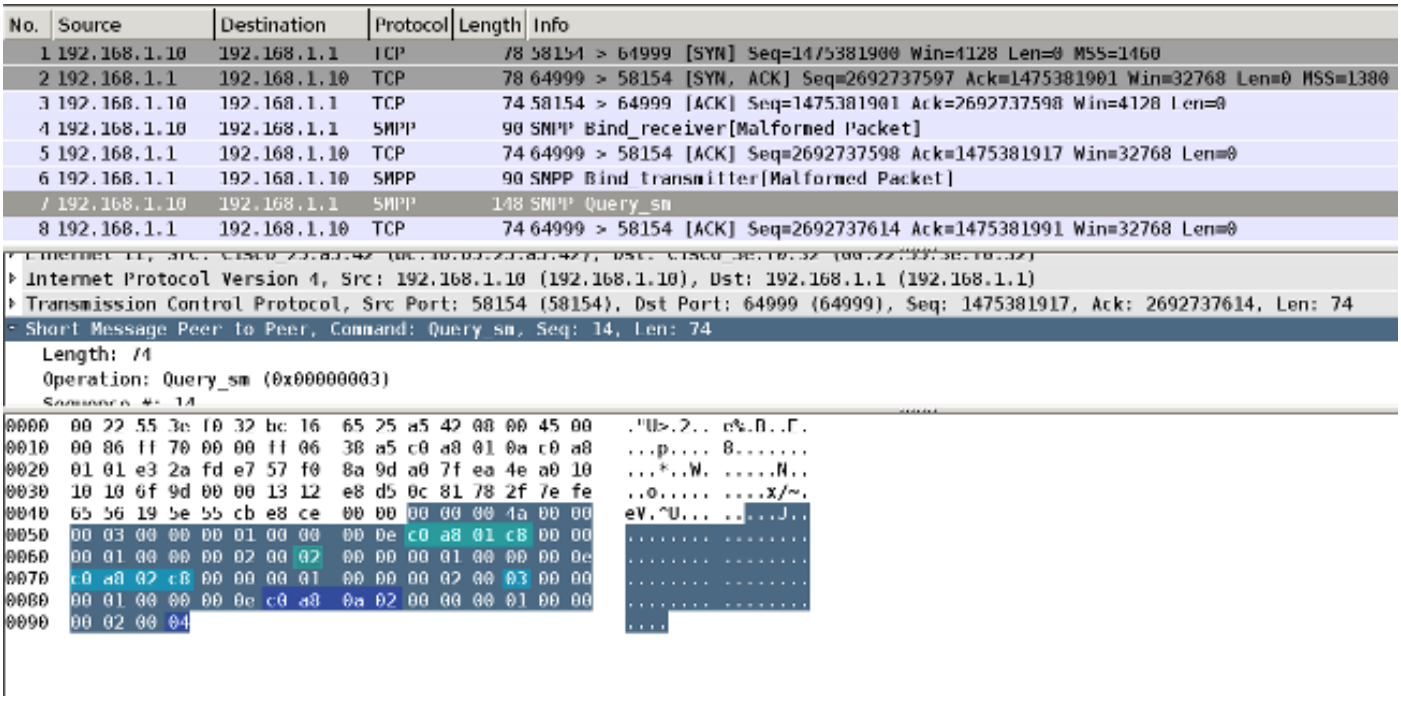
デバッグでは、変更があるかどうかが（gen ID に基づいて）特定されます。変更がある場合は、必要に応じて古いポリシーをアンインストールし、新しいポリシーをインストールすることができます。これには、ASIC のプログラミング（ハードウェア サポート）が含まれます。

```
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
```

SXP 交換

デバイスの IP アドレスを検索する IP デバイス トラッキング コードによって、SXP の更新がトリガーされます。次に、Short Message Peer-to-Peer（SMPP）プロトコルを使用して更新が送信されます。このプロトコルは、Border Gateway Protocol（BGP）と同様に、**TCP オプション 19 を認証に使用します。**SMPP ペイロードは暗号化されません。Wireshark には SMPP ペイロードに対する適切なデコーダがありませんが、内部のデータの検索は簡単です。



- 最初のデータ、c0 a8 01 c8 は 192.168.1.200 で、tag 2 があります。
- 2 番目のデータ、c0 a8 02 c8 は 192.168.2.200 で、tag 3 があります。
- 3 番目のデータ、c0 a8 0a 02 は 192.168.10.2 で、tag 4 があります (これは、電話機 SGT=4 のテストに使用されました) 。

次に、IP デバイス トラッキングで MS Windows 7 の IP アドレスを検索した後の 3750X でのデバッグを示します。

```
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
```

次に、ASA での対応するデバッグを示します。

```
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.
```

ASA でより多くのデバッグを表示するには、デバッグ詳細レベルを有効にします。

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

ASA での SGACL

ASA が SXP で受信した SGT マッピングを正しくインストールすると、セキュリティ グループ ACL がうまく機能します。マッピングに問題が発生した場合は、次のコマンドを入力します。

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

セキュリティ グループを持つ ACL は、IP アドレスやユーザ ID に対するのとまったく同じように機能します。ログによって問題が明確になり、正確に一致した ACL のエントリが明らかになります。

次に、MS Windows XP から MS Windows 7 への ping を示します。これには、パケット トレーサが正確に機能していることが示されています。

```
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>
```

関連情報

- 3750 用 Cisco TrustSec 設定ガイド
- ASA 9.1 用 Cisco TrustSec 設定ガイド
- Cisco TrustSec の展開およびロードマップ
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。