配置ASA 9.3.1 TrustSec轴向标记

Contents

Introduction

本文在可适应的安全工具(ASA)版本9.3.1描述如何使用实现的功能- TrustSec轴向标记。功能允许ASA接收TrustSec帧以及发送他们。此方式ASA可以在TrustSec域内容易地集成，不用需要使用TrustSec SGT交换协议(SXP)。

此示例提交分配SGT标记= 2的远程VPN用户(SGT)标记=分配安全组标记的3 (营销)和802.1x用户(财务)。数据流实施由ASA进行与访问控制表的使用安全组(SGACL)定义得本地，并且Cisco IOS交换机使用角色根据从身份服务引擎(RBACL)下载的访问控制表(ISE)。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- ASA CLI配置和安全套接字层SSL VPN配置
- 在ASA的远程访问VPN配置
- ISE和TrustSec服务

Components Used

本文档中的信息基于以下软件版本：

- Cisco ASA软件，版本9.3.1和以上
- Cisco ASA硬件55x5或ASAv
- 与Cisco AnyConnect安全移动客户端的Windows 7，版本3.1
- Cisco有软件的15.0.2 Catalyst 3750X交换机及以后
- Cisco ISE，版本1.2及以后

Configure

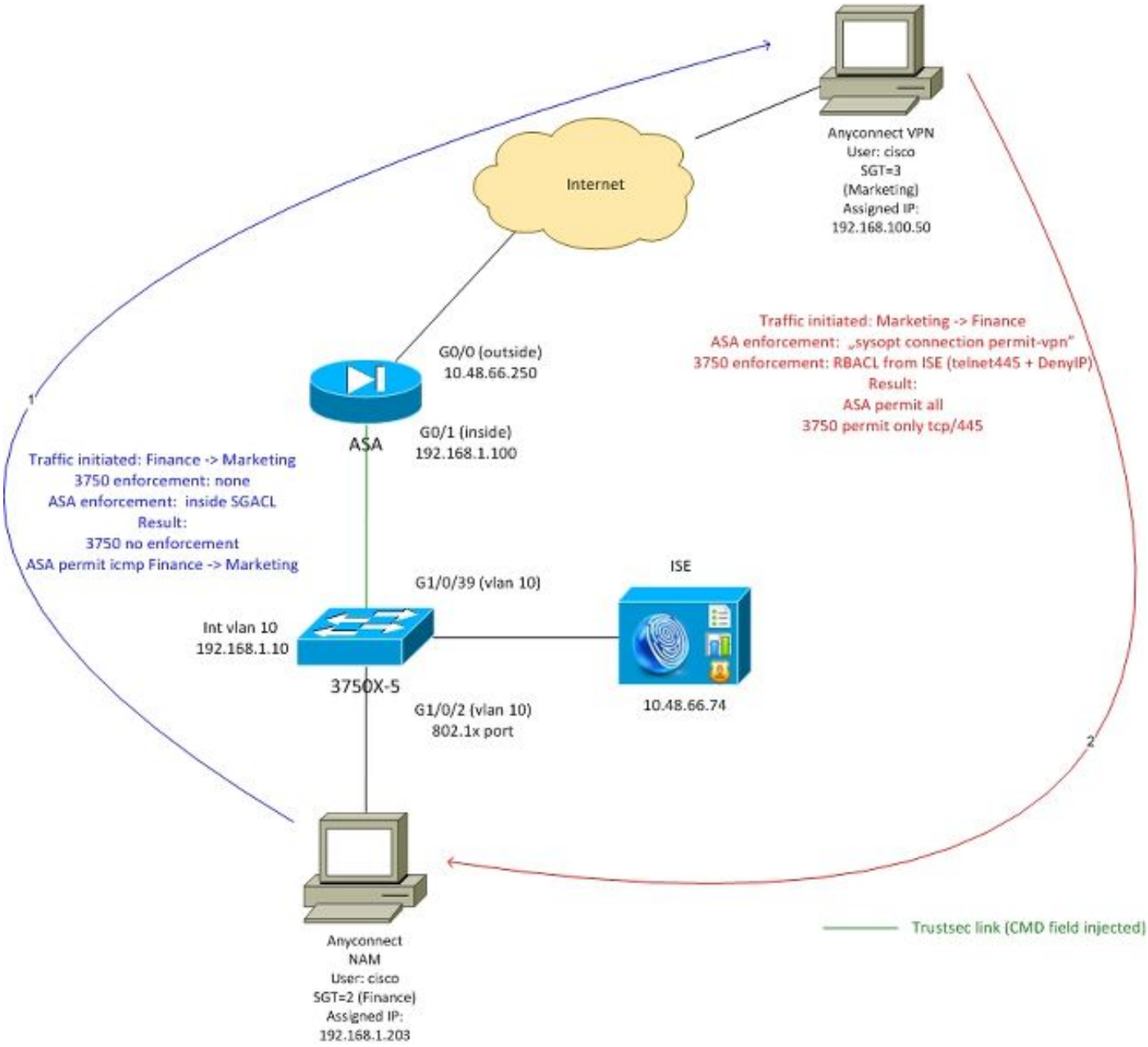
> **Note**:使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

Network Diagram

ASA和3750X之间的连接为手工的cts被配置。那意味着两个设备能发送和接收与Cisco元数据字段(CMD)的被修改的以太网帧。该字段包括描述信息包的来源的安全组标记(SGT)。

远程VPN用户终止在ASA的SSL会话和分配SGT标记3 (营销)。

本地公司802.1x用户，在成功的验证分配SGT标记2后(财务)。



ASA有在允许从财务初始化的ICMP数据流到营销的内部接口配置的SGACL。

ASA允许所有数据流初始化从去除VPN用户(由于“sysopt连接permit-vpn”配置)。

意味着在ASA的SGACL有状态的流一次被创建，返回信息包自动地被接受(基于检查)。

3750交换机用途RBACL为了控制从营销收到的数据流提供经费。

意味着的RBACL是无状态的每个信息包被检查，但是在3750X平台的TrustSec实施进行在目的地。此方式交换机对数据流的实施负责从营销的提供经费。

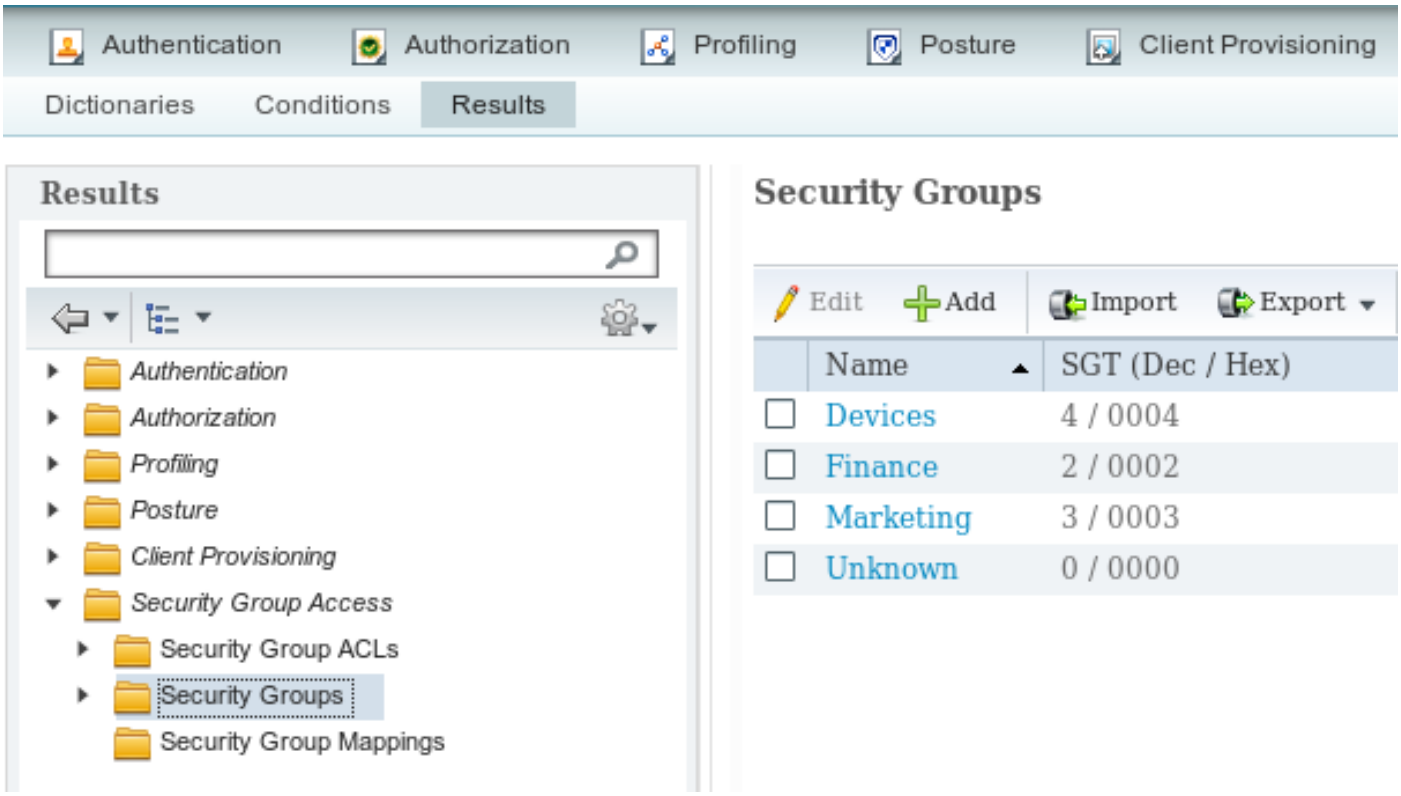
Note:对于在Cisco IOS区域基于防火墙的Trustsec意识状态防火墙能使用，例如，请参考：

Note:ASA可能有来自远程VPN用户的SGACL控制流量。为了简化方案，它在此条款上未被提交。例如请参考： [ASA 版本 9.2 VPN SGT 分类和实施配置示例]

ISE -Configuration Steps

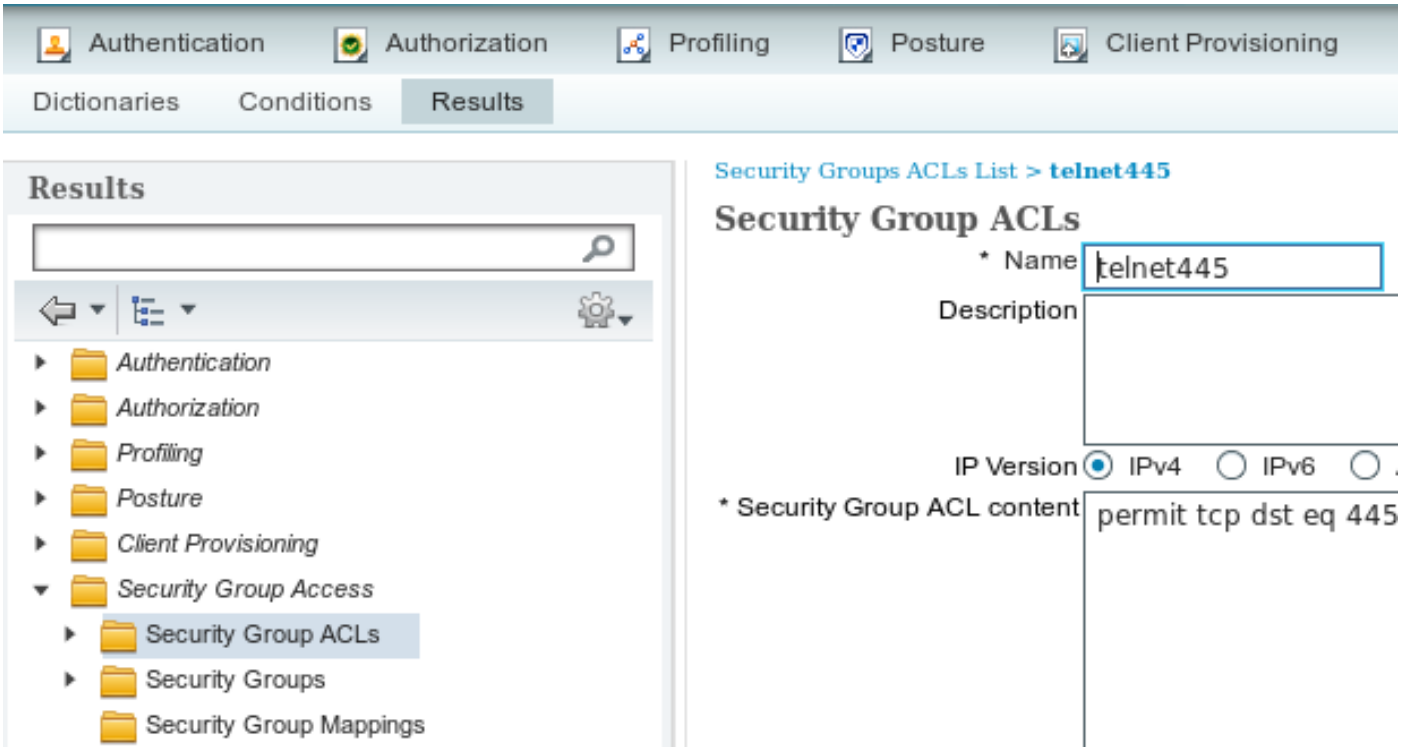
1. 财务和营销的SGT

如此镜像所显示，连接对**策略>结果> Security组访问> Security组**并且创建财务和营销的SGT。



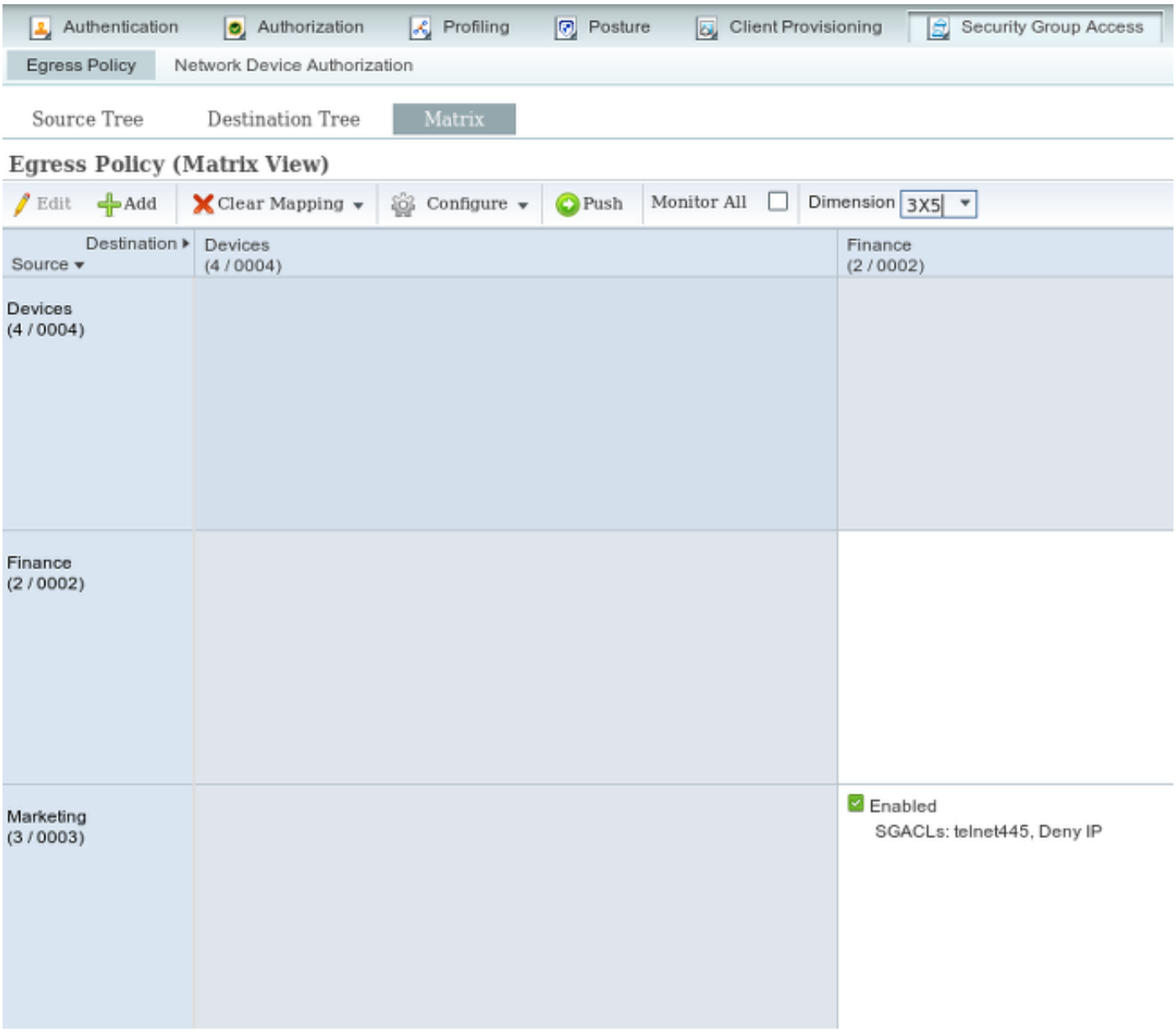
2. 数据流营销>财务的安全组ACL

连接对用于对从营销的控制数据流提供经费的**策略>结果> Security组访问> Security组ACL**并且创建ACL。如此镜像所显示，仅tcp/445允许。



3. 在矩阵的捆绑的ACL

连接对来源的**策略>出口策略>矩阵**捆绑被配置的ACL ：**营销**和目的地：**财务**。如镜像所显示，并且附上**拒绝IP**作为最后ACL降低其他数据流。(没有该默认策略将附有，默认值是许可证其中任一)



4. 分配VPN的访问的授权规则SGT = 3 (营销)

连接对**策略>授权**并且创建远程VPN访问的一个规则。通过AnyConnect 4.x客户端被建立的所有VPN连接将获得全部存取(PermitAccess)，并且分配SGT标记3 (营销)。情况是使用AnyConnect身份Extentions (ACIDEX) ：

```
Rule name: VPN
Condition: Cisco:cisco-av-pair CONTAINS mdm-tlv=ac-user-agent=AnyConnect Windows 4
Permissions: PermitAccess AND Marketing
```

5. 分配802.1x的访问的授权规则SGT = 2 (财务)

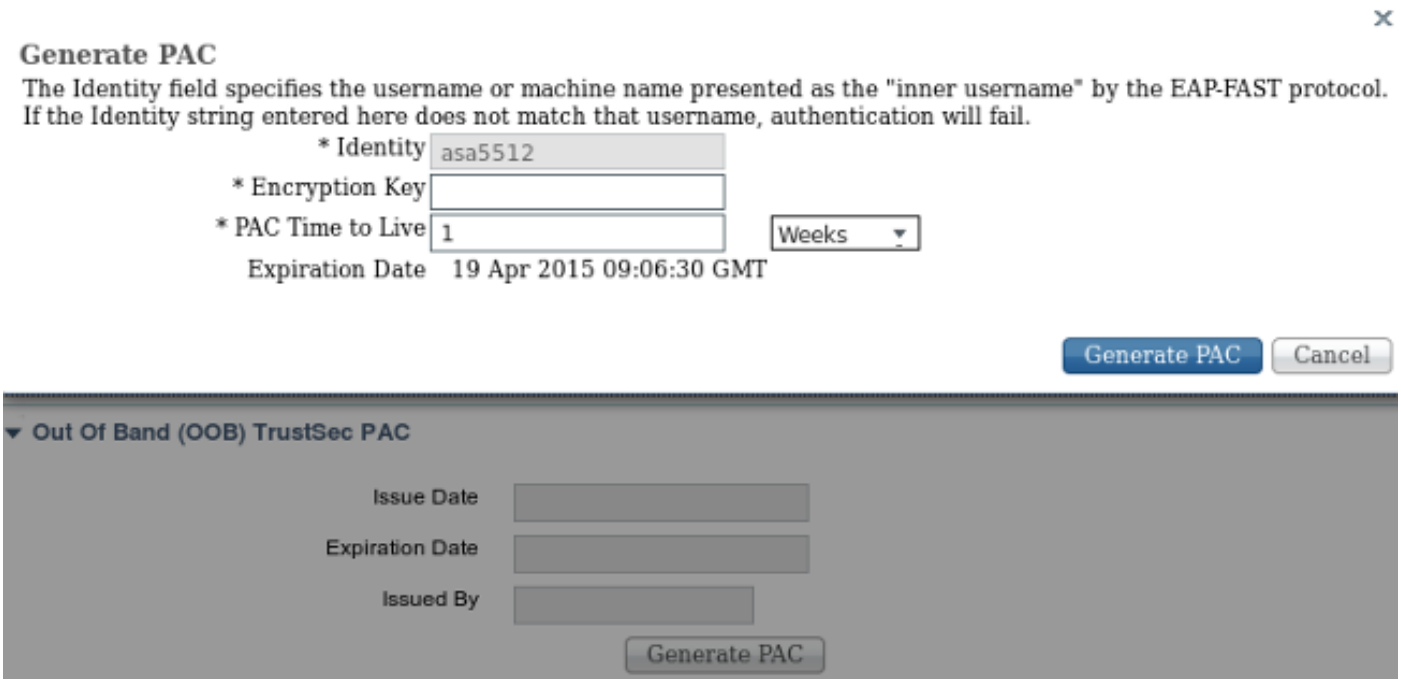
连接对**策略>授权**并且创建802.1x访问的一个规则。终止在交换机与用户名**cisco将**获得全部存取的3750的请求方802.1x会话(PermitAccess)，并且分配SGT标记2 (财务)。

```
Rule name: 802.1x
Condition: Radius:User-Name EQUALS cisco AND Radius:NAS-IP-Address EQUALS 192.168.1.10
Permissions: PermitAccess ANDFinance
```

6. 添加网络设备，生成ASA的PAC

为了添加ASA到TrustSec域，手工生成PAC文件是必要的。该文件在ASA被导入。

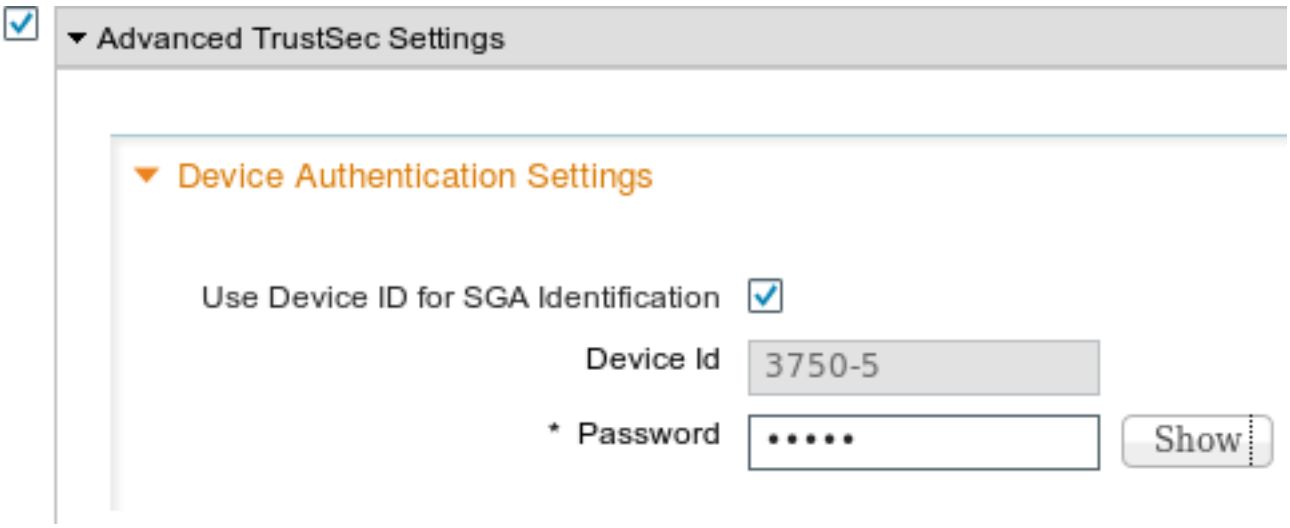
此操作可在**管理 > 网络设备** *下配置*。在ASA被添加后，如此镜像所显示，请移下来到**TrustSec设置**并且**生成PAC**。



交换机(3750X)支持设置自动的PAC，因此步骤需要为支持手工PAC只设置的ASA仅完成。

7. 添加网络设备，配置交换机自动PAC设置的秘密

如此镜像所显示，对于使用设置自动的PAC的交换机，必须设置一个正确的秘密。



Note:PAC用于验证ISE和与策略(ACL)一起下载环境数据(即SGT)。ASA在ASA支持仅环境数据，策略需要手工被配置。Cisco IOS支持两个，因此策略可以从ISE下载。

ASA -Configuration Steps

1. 基本的VPN访问

使用认证的， ISE配置AnyConnect的基本的SSL VPN访问。

```
Rule name: 802.1x
Condition: Radius:User-Name EQUALS cisco AND Radius:NAS-IP-Address EQUALS 192.168.1.10
Permissions: PermitAccess AND Finance
```

2. 导入PAC和Enable (event) cts

导入为ASA生成的PAC (从第6步ISE配置)。请使用同一加密密钥：

```
BSNS-ASA5512-4# cts import-pac http://10.229.20.86/asa5512.pac password ciscocisco
PAC Imported Successfully
```

为了验证：

```
BSNS-ASA5512-4# show cts pac

 PAC-Info:
   Valid until: Apr 11 2016 10:16:41
   AID:         c2dcb10f6e5474529815aed11ed981bc
   I-ID:        asa5512
   A-ID-Info:   Identity Services Engine
   PAC-type:    Cisco Trustsec
 PAC-Opaque:
   000200b00003000100040010c2dcb10f6e5474529815aed11ed981bc00060094000301
   007915dcb81032f2fdf04bfe938547fad2000000135523ecb300093a8089ee0193bb2c
   8bc5cfabf8bc7b9543161e6886ac27e5ba1208ce445018a6b07cc17688baf379d2f1f3
   25301fffa98935ae5d219b9588bcb6656799917d2ade088c0a7e653ea1dca530e24274
   4366ed375488c4ccc3d64c78a7fc8c62c148ceb58fad0b07d7222a2c02549179dbf2a7
   4d4013e8fe
```

Enable (event) cts ：

```
BSNS-ASA5512-4# show cts pac

 PAC-Info:
   Valid until: Apr 11 2016 10:16:41
   AID:         c2dcb10f6e5474529815aed11ed981bc
   I-ID:        asa5512
   A-ID-Info:   Identity Services Engine
   PAC-type:    Cisco Trustsec
 PAC-Opaque:
   000200b00003000100040010c2dcb10f6e5474529815aed11ed981bc00060094000301
   007915dcb81032f2fdf04bfe938547fad2000000135523ecb300093a8089ee0193bb2c
   8bc5cfabf8bc7b9543161e6886ac27e5ba1208ce445018a6b07cc17688baf379d2f1f3
   25301fffa98935ae5d219b9588bcb6656799917d2ade088c0a7e653ea1dca530e24274
   4366ed375488c4ccc3d64c78a7fc8c62c148ceb58fad0b07d7222a2c02549179dbf2a7
   4d4013e8fe
```

在您enable (event) cts， ASA必须从ISE后下载环境数据：

```
BSNS-ASA5512-4# show cts environment-data
```

```
CTS Environment Data
====================
Status:                     Active
Last download attempt:      Successful
Environment Data Lifetime: 86400 secs
Last update time:           10:21:41 UTC Apr 11 2015
Env-data expires in:        0:00:37:31 (dd:hr:mm:sec)
Env-data refreshes in:      0:00:27:31 (dd:hr:mm:sec)
```

3. 数据流财务>营销的SGACL

配置在内部接口的SGACL。ACL准许初始化仅ICMP数据流从财务到营销。

```
access-list inside extended permit icmp security-group name Finance any security-group name
Marketing any
access-group inside in interface inside
```

ASA必须扩展标记的名字编号：

```
BSNS-ASA5512-4(config)# show access-list inside
access-list inside line 1 extended permit icmp security-group name Finance(tag=2) any security-
group name Marketing(tag=3) any (hitcnt=47) 0x5633b153
```

4. 在内部接口的Enable (event) cts

在您在ASA后内部接口的enable (event) cts ：

```
interface GigabitEthernet0/1
 nameif inside
cts manual
  policy static sgt 100 trusted
 security-level 100
 ip address 192.168.1.100 255.255.255.0
```

ASA能发送和接收TrustSec帧(与CMD字段的以太网帧)。ASA假设，没有标记的所有入口帧必须对待与标记100。已经包括标记的所有入口帧将委托。

交换机配置步骤

1. 基本的802.1x

```
aaa new-model

aaa authentication dot1x default group radius
aaa authorization network default group radius

dot1x system-auth-control

interface GigabitEthernet1/0/2
 description windows7
 switchport access vlan 10
 switchport mode access
 authentication host-mode multi-domain
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast
```

```
radius-server host 10.48.66.74 pac key cisco
```

使用该配置，在成功后必须分配802.1x授权用户(被认证通过ISE)标记2 (财务)。

2. CTS配置和设置

同样地，至于对于ASA，配置cts和对ISE的点：

```
aaa new-model

aaa authentication dot1x default group radius
aaa authorization network default group radius

dot1x system-auth-control

interface GigabitEthernet1/0/2
 description windows7
 switchport access vlan 10
 switchport mode access
 authentication host-mode multi-domain
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast

radius-server host 10.48.66.74 pac key cisco
```

并且，实施为Layer3和Layer2 (所有VLAN)被启用：

```
aaa new-model

aaa authentication dot1x default group radius
aaa authorization network default group radius

dot1x system-auth-control

interface GigabitEthernet1/0/2
 description windows7
 switchport access vlan 10
 switchport mode access
 authentication host-mode multi-domain
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast

radius-server host 10.48.66.74 pac key cisco
```

为了自动地设置PAC ：

```
bsns-3750-5#cts credentials id 3750-5 password ciscocisco
```

再次，密码必须与在ISE (**网络设备> Switch> TrustSec**)的对应的配置匹配。现在， Cisco IOS起动与ISE的EAP-FAST会话为了获得PAC。可以找到在该进程的更多详细资料这里：

[ASA 和 Catalyst 3750X 系列交换机 TrustSec 配置示例和故障排除指南]

为了验证是否安装PAC ：

```
bsns-3750-5#show cts pacs
```

```
 AID: EA48096688D96EF7B94C679A17BDAD6F
 PAC-Info:
   PAC-type = Cisco Trustsec
   AID: EA48096688D96EF7B94C679A17BDAD6F
   I-ID: 3750-5
   A-ID-Info: Identity Services Engine
   Credential Lifetime: 14:41:24 CEST Jul 10 2015
 PAC-Opaque:
000200B000030001000400010EA48096688D96EF7B94C679A17BDAD6F000600940003010036 5AB3133998C86C1BA1B418
968C6069000000135526 1CCC00093A808F8A81F3F8C99A7CB83A8C3BFC4D573212C61CDCEB37ED279D683EE0DA60D86D
5904C41701ACF07BE98B3B73C4275C98C19A1DD7E1D65E679F3E9D40662B409E58A9F139BAA3BA3818553152F28AE04B
089E5B7CBB22A0D4BCEEF80F826A180B5227EAACBD07709DBDCD3CB42AA9F996829AE46F
 Refresh timer is set for 4y14w
```

3. 在接口的Enable (event) cts对ASA

```
interface GigabitEthernet1/0/39
 switchport access vlan 10
 switchport mode access
 cts manual
  policy static sgt 101 trusted
```

从现在起，交换机一定准备处理和发送TrustSec帧和强制执行从ISE下载的策略。

Verify

使用本部分可确认配置能否正常运行。

验证在本文的各自的部分报道。

Troubleshoot

SGT分配

在对ASA的VPN会话建立后，必须确认正确的SGT分配：

```
BSNS-ASA5512-4# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : cisco                  Index        : 13
Assigned IP  : 192.168.100.50         Public IP    : 10.229.20.86
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA256  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 10308                  Bytes Rx     : 10772
Group Policy : TAC                    Tunnel Group : TAC
Login Time   : 15:00:13 UTC Mon Apr 13 2015
Duration     : 0h:00m:25s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a801640000d000552bd9fd
Security Grp : 3:Marketing
```

根据授权在ISE规定，所有AnyConnect4用户分配到营销标记。

同样与在交换机的802.1x会话。在AnyConnect网络分析模块(NAM)完成后，认证交换机将应用从ISE返回的正确的标记：

```
bsns-3750-5#show authentication sessions interface g1/0/2 details
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.36ce
        IPv6 Address:  Unknown
        IPv4 Address:  192.168.1.203
           User-Name:  cisco
              Status:  Authorized
              Domain:  DATA
      Oper host mode:  multi-domain
    Oper control dir:  both
     Session timeout:  N/A
   Common Session ID:  0A30426D000000130001B278
     Acct Session ID:  Unknown
              Handle:  0x53000002
      Current Policy:  POLICY_Gi1/0/2

Local Policies:
       Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
     Security Policy:  Should Secure
     Security Status:  Link Unsecure

Server Policies:
           SGT Value:  2

Method status list:
      Method           State
      dot1x            Authc Success
      mab              Stopped
```

根据授权在ISE规定，所有用户被联络到该交换机必须分配对SGT = 2 (财务)。

在ASA的实施

当您设法从财务(192.168.1.203)发送数据流到销售(192.168.100.50)，击中ASA内部接口。对于ICMP响应请求，它创建会话：

```
Built outbound ICMP connection for faddr 192.168.100.50/0(LOCAL\cisco, 3:Marketing) gaddr
192.168.1.203/1 laddr 192.168.1.203/1(2)
```

并且增加ACL计数器：

```
BSNS-ASA5512-4(config)# sh access-list

access-list inside line 1 extended permit icmp security-group name Finance(tag=2) any security-
group name Marketing(tag=3) any (hitcnt=138)
```

那可以也被确认查看信息包获取。注意正确的标记显示：

```
BSNS-ASA5512-4(config)# capture CAP interface inside
BSNS-ASA5512-4(config)# show capture CAP

  1: 15:13:05.736793       INLINE-TAG 2 192.168.1.203 > 192.168.100.50: icmp: echo request
  2: 15:13:05.772237       INLINE-TAG 3 192.168.100.50 > 192.168.1.203: icmp: echo reply
  3: 15:13:10.737236       INLINE-TAG 2 192.168.1.203 > 192.168.100.50: icmp: echo request
  4: 15:13:10.772726       INLINE-TAG 3 192.168.100.50 > 192.168.1.203: icmp: echo reply
```

有流入的ICMP ECHO请求标记用SGT = 2 (财务)然后自由ASA标记SGT = 3的VPN用户的一种回应(营销)。另一个故障检修工具，信息包跟踪程序也是准备好的TrustSec。

不幸地， 802.1x PC看不到该答案，因为由在交换机(在下个部分的解释的无状态的RBACL阻拦了)。

另一个故障检修工具，信息包跟踪程序也是准备好的TrustSec。请确认自财务的流入的ICMP信息包是否将接受：

```
BSNS-ASA5512-4# packet-tracer input inside icmp inline-tag 2 192.168.1.203 8 0 192.168.100.50
Mapping security-group 3:Marketing to IP address 192.168.100.50

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.48.66.1 using egress ifc  outside

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group inside in interface inside
access-list inside extended permit icmp security-group name Finance any security-group name
Marketing any
Additional Information:

<some output omitted for clarity>

Phase: 13
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 4830, packet dispatched to next module

Result:
input-interface: inside
input-status: up
input-line-status: up
```

```
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: allow
```

请也设法首次从财务的所有TCP连接与销售，那必须由ASA阻拦：

```
Deny tcp src inside:192.168.1.203/49236 dst outside:192.168.100.50/445(LOCAL\cisco, 3:Marketing)
by access-group "inside" [0x0, 0x0]
```

交换实施

请验证交换机是否从ISE正确地下载了策略：

```
bsns-3750-5#show cts role-based permissions
IPv4 Role-based permissions default:
       Permit IP-00
IPv4 Role-based permissions from group 2:Finance to group Unknown:
       test_deny-30
IPv4 Role-based permissions from group 8 to group Unknown:
       permit_icmp-10
IPv4 Role-based permissions from group Unknown to group 2:Finance:
       test_deny-30
       Permit IP-00
IPv4 Role-based permissions from group 3:Marketing to group 2:Finance:
        telnet445-60
        Deny IP-00
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

控制从营销的数据流提供经费正确地安装的策略。仅tcp/445根据RBACL允许：

```
bsns-3750-5#show cts rbacl telnet445
CTS RBACL Policy
================
RBACL IP Version Supported: IPv4
 name   = telnet445-60
 IP protocol version = IPV4
 refcnt = 2
 flag   = 0x41000000
 stale  = FALSE
 RBACL ACEs:
   permit tcp dst eq 445
```

那是原因为什么来自营销提供经费的ICMP回音回应下降了。那可以通过检查计数器确认从SGT 3的数据流对SGT 2 ：

```
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

*       *       0               0               223613          3645233

0       2       0               0               0               122

3       2       0               65              0               0

2       0       0               0               179             0
```

```
8       0       0               0               0               0
```
信息包由硬件丢弃了(当前计数器是65和增加每1秒)。

tcp/445连接若从营销被起动？

ASA承认(接受所有VPN流量由于“sysopt连接permit-vpn”) ：

```
Built inbound TCP connection 4773 for outside:192.168.100.50/49181
(192.168.100.50/49181)(LOCAL\cisco, 3:Marketing) to inside:192.168.1.203/445 (192.168.1.203/445)
(cisco)
```
正确的会话被创建：

```
BSNS-ASA5512-4(config)#  show conn all | i 192.168.100.50
TCP outside  192.168.100.50:49181 inside  192.168.1.203:445, idle 0:00:51, bytes 0, flags UB
```
因为匹配telnet445 RBACL，并且， Cisco IOS接受它。正确的计数器增量：

```
bsns-3750-5#show cts role-based counters from 3 to 2
3       2       0               65              0               3
```
(最后一栏是硬件允许的数据流)。会话允许。

在TrustSec策略配置和实施故意地展示此示例为了显示出区别在ASA和Cisco IOS。 注意Cisco IOS策略区别从ISE (无状态的RBACL)和TrustSec意识有状态的区域基于防火墙下载的。

Related Information

- ASA 版本 9.2.1 基于 ISE 的 VPN 安全评估配置示例
- ASA 和 Catalyst 3750X 系列交换机 TrustSec 配置示例和故障排除指南
- 思科 TrustSec 交换机配置指南：了解思科 TrustSec
- 为安全设备用户授权配置外部服务器
- 思科 ASA 系列 VPN CLI 配置指南，版本 9.1
- 思科身份服务引擎用户指南，版本 1.2
- Technical Support & Documentation - Cisco Systems