ASA 版本 9.2 VPN SGT 分类和实施配置示例

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[配置](#)
[网络图](#)
[ISE配置](#)
[ASA 配置](#)
[验证](#)
[故障排除](#)
[摘要](#)
[相关信息](#)

简介

本文在可适应安全工具(ASA)版本9.2.1描述如何使用新特性， TrustSec安全组标记(SGT)分类VPN用户。此示例提交分配一不同的SGT和安全组防火墙的两个VPN用户(SGFW)，过滤VPN用户之间的流量。

先决条件

要求

Cisco 建议您了解以下主题：

- ASA CLI配置和安全套接字层SSL VPN配置基础知识
- 远程访问VPN配置基础知识在ASA的
- 身份服务引擎(ISE)和TrustSec服务基础知识

使用的组件

本文档中的信息基于以下软件版本：

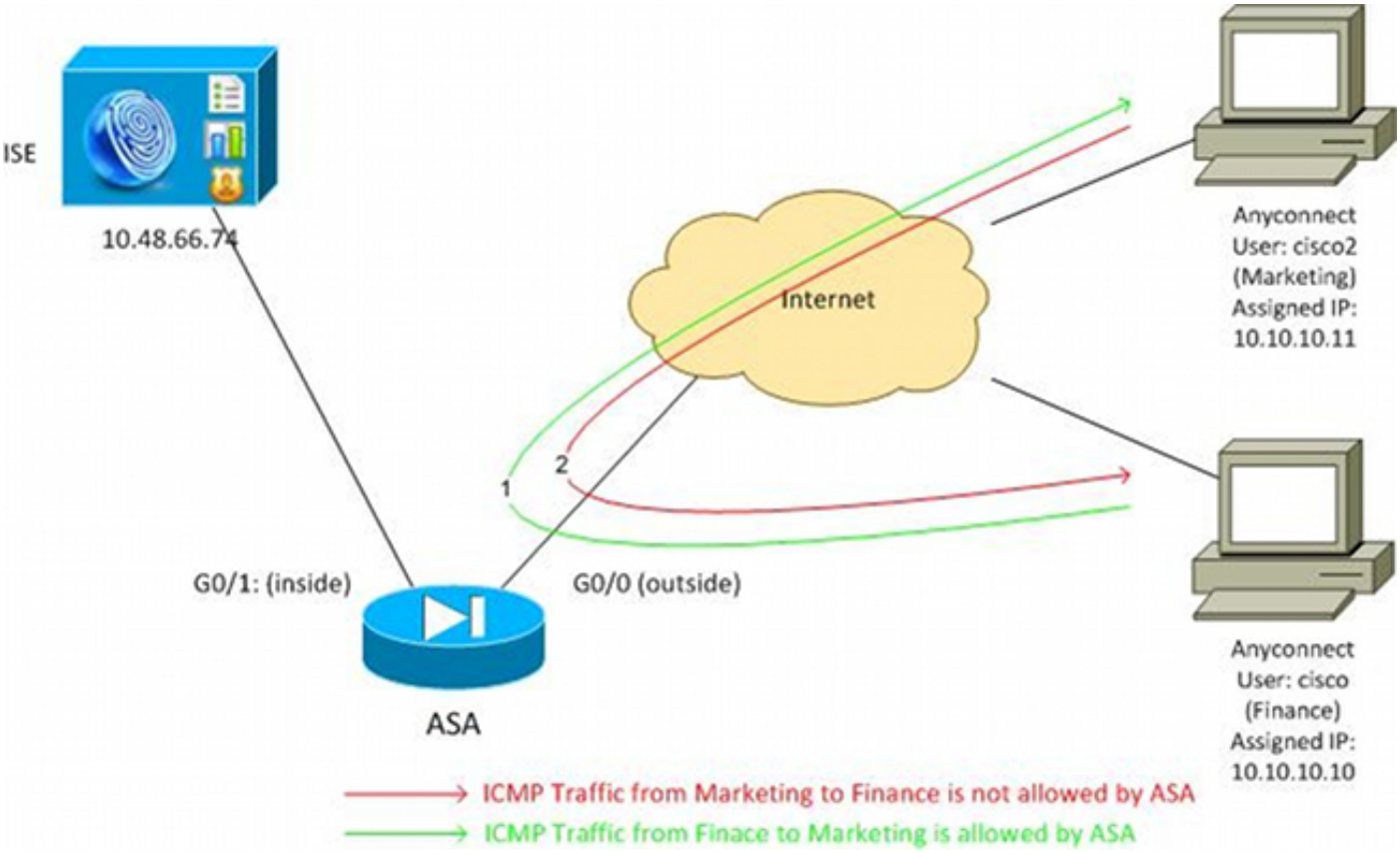
- Cisco ASA软件，版本9.2和以上
- 与Cisco AnyConnect安全移动客户端的Windows 7，版本3.1
- Cisco ISE，版本1.2及以后

配置

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。

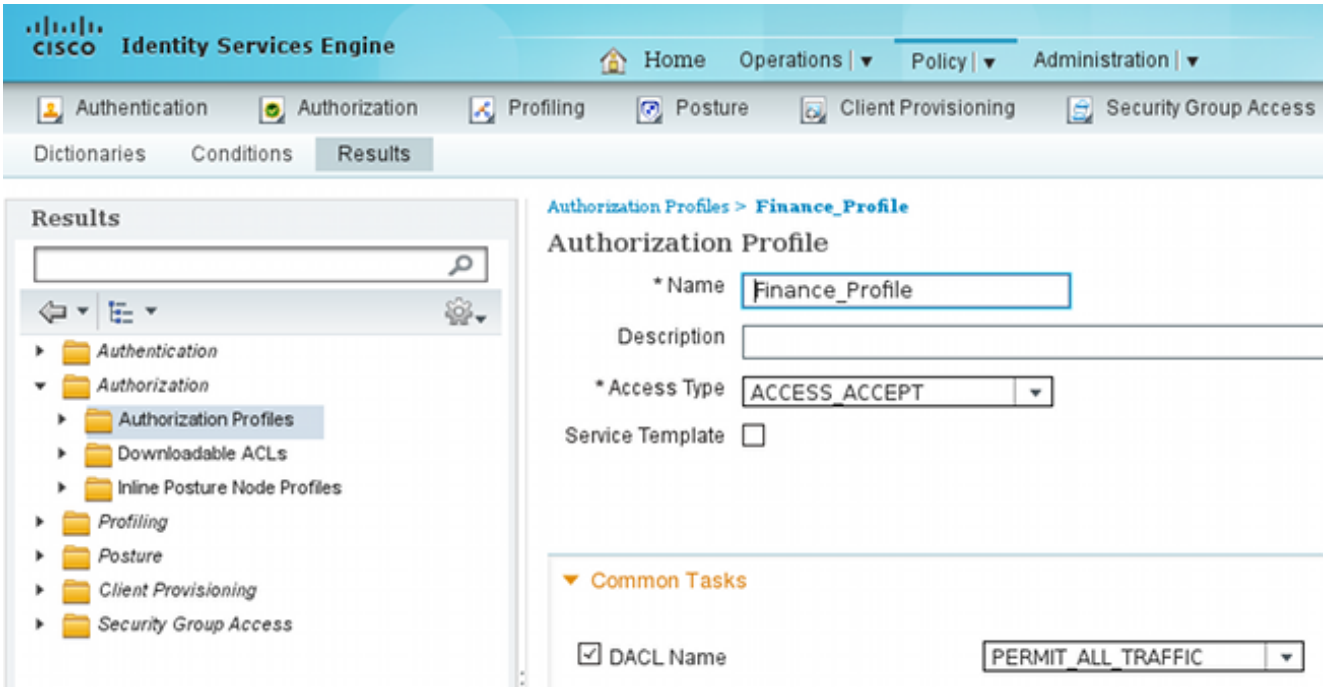
网络图

VPN用户‘cisco’分配到金融团队，允许首次对营销团队的互联网控制消息协议(ICMP)连接。 VPN用户'cisco2分配到营销团队，没有允许首次任何连接。



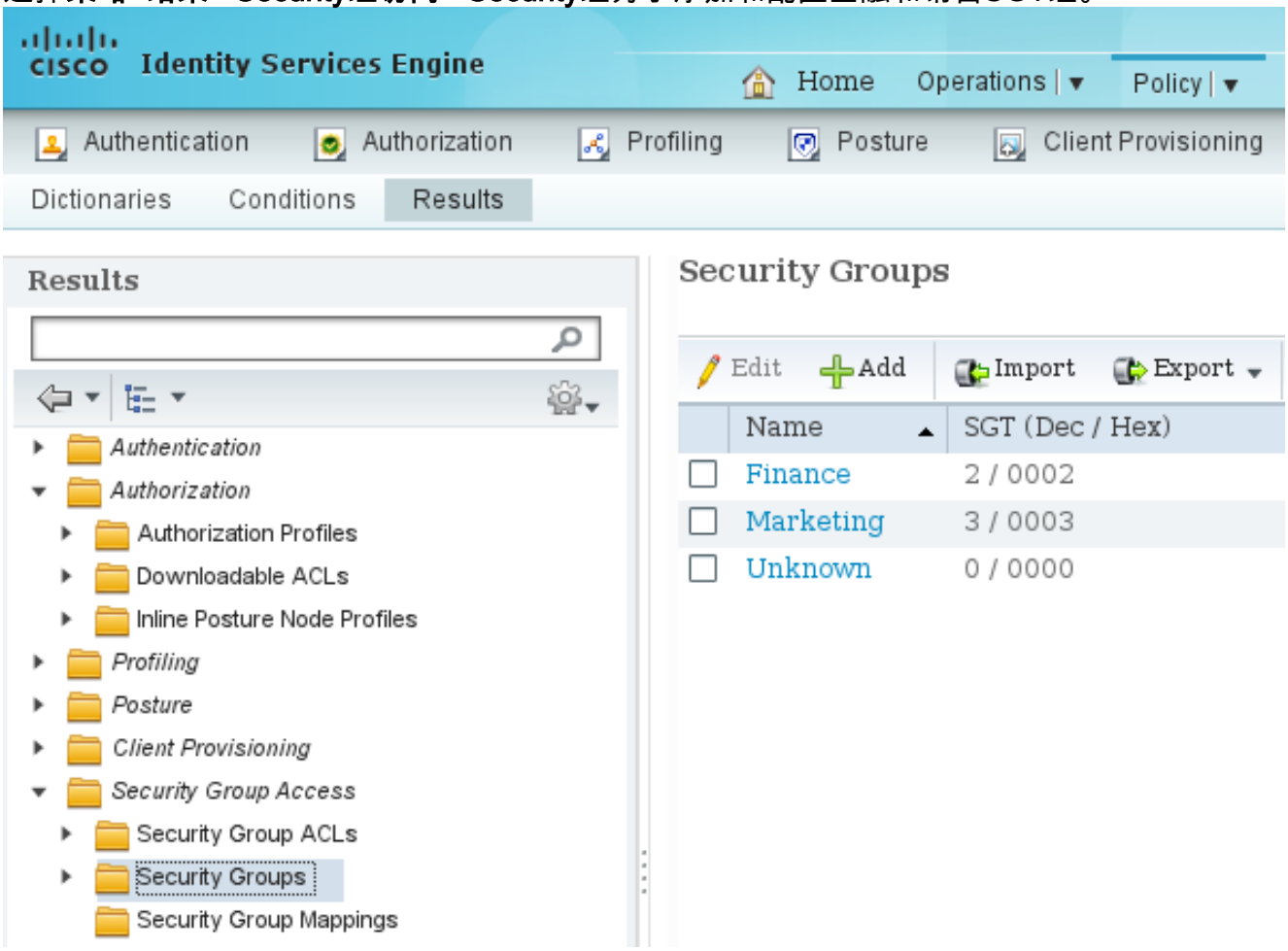
ISE配置

1. 选择**Administration >身份管理>标识**为了添加和配置用户‘cisco’ (从金融)和'cisco2 (从营销)。
2. 选择**Administration >网络资源>网络设备**为了添加和配置ASA作为网络设备。
3. 选择**策略>结果>授权>授权配置文件**为了添加和配置金融和市场授权配置文件。两配置文件包括一个属性，可下载的访问控制表(DACL)，允许所有流量。金融的一示例显示此处：

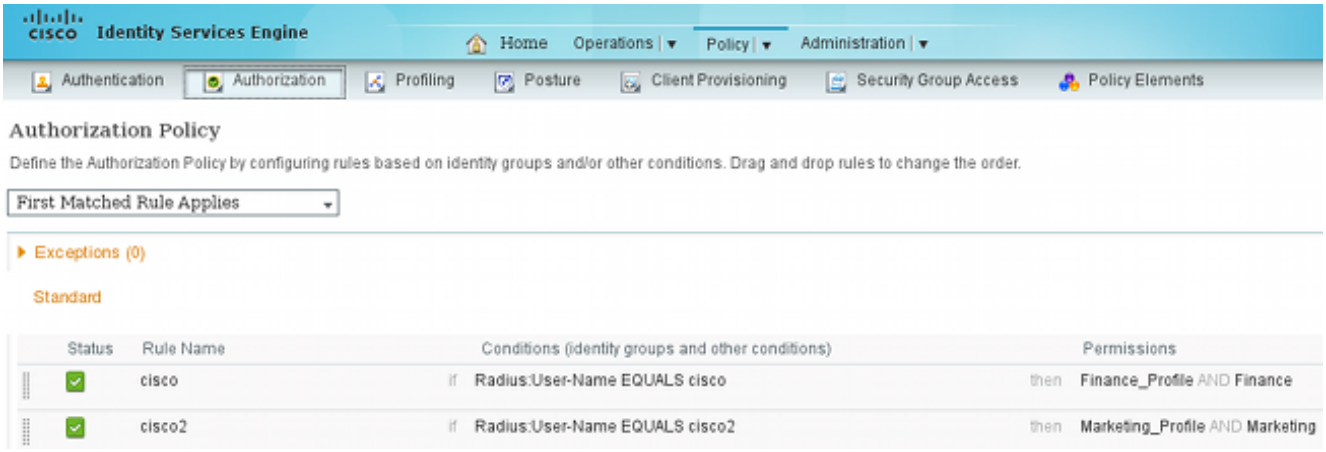


每配置文件可能有特定，限制式DACL，但是对于此方案所有流量允许。执行由SGFW没有执行，没有DACL分配到每VPN会话。过滤与SGFW的流量允许使用SGTs而不是DACL使用的IP地址。

4. 选择**策略>结果> Security组访问> Security组**为了添加和配置金融和销售SGT组。



5. 选择**策略>授权**为了配置两个授权规则。第一个规则与SGT组金融一起分配允许全部的流量)的Finance_profile (DACL到‘cisco’用户。 第二个规则与销售SGT的组一起分配允许全部的流量)的Marketing_profile (DACL到'cisco2用户。



ASA 配置

1. 完成基本VPN配置。

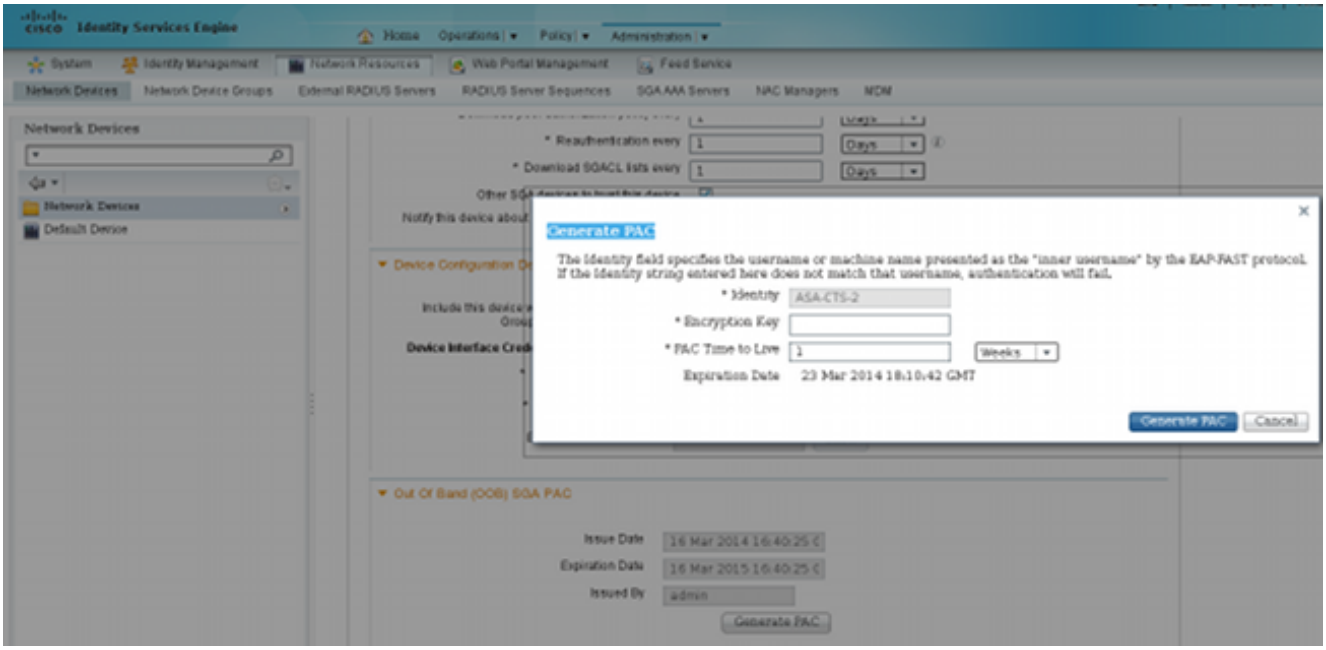
```
webvpn
 enable outside
 anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable

group-policy GP-SSL internal
group-policy GP-SSL attributes
 vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

tunnel-group RA type remote-access
tunnel-group RA general-attributes
 address-pool POOL
 authentication-server-group ISE
 accounting-server-group ISE
 default-group-policy GP-SSL
tunnel-group RA webvpn-attributes
 group-alias RA enable

ip local pool POOL 10.10.10.10-10.10.10.100 mask 255.255.255.0
```

2. 完成ASA AAA和TrustSec配置。

```
aaa-server ISE protocol radius
aaa-server ISE (outside) host 10.48.66.74
 key *****
cts server-group ISE
```

为了加入TrustSec网云， ASA需要验证与受保护的访问凭证(PAC)。ASA不支持设置自动的PAC，是该文件为什么在ISE需要手工生成和导入到ASA。

3. 选择**Administration >网络资源>网络设备> ASA >Advanced TrustSec设置**为了生成在ISE的PAC。选择**在**设置的**波段(OOB) PAC外面**为了生成文件。



4. 导入PAC对ASA。生成的文件在HTTP FTP服务器能放置。ASA用途导入文件。

```
ASA# cts import-pac http://192.168.111.1/ASA-CTS-2.pac password 12345678
!PAC Imported Successfully
ASA#
ASA# show cts pac

 PAC-Info:
   Valid until: Mar 16 2015 17:40:25
   AID:         ea48096688d96ef7b94c679a17bdad6f
   I-ID:        ASA-CTS-2
   A-ID-Info:   Identity Services Engine
   PAC-type:    Cisco Trustsec
 PAC-Opaque:
   000200b800030001000400010ea48096688d96ef7b94c679a17bdad6f0006009c000301
   0015e3473e728ae73cc905887bdc8d3cee00000013532150cc00093a8064f7ec374555
   e7b1fd5abccb17de31b9049066f1a791e87275b9dd10602a9cb4f841f2a7d98486b2cb
   2b5dc3449f67c17f64d12d481be6627e4076a2a63d642323b759234ab747735a03e01b
   99be241bb1f38a9a47a466ea64ea334bf51917bd9aa9ee3cf8d401dc39135919396223
   11d8378829cc007b91ced9117a
```

当您有正确PAC时，ASA自动地执行环境刷新。这下载从ISE的信息关于当前SGT组。

```
ASA# show cts environment-data sg-table

Security Group Table:
Valid until: 17:48:12 CET Mar 17 2014
Showing 4 of 4 entries

SG Name                          SG Tag     Type
-------                          ------     -------------
ANY                               65535     unicast
Unknown                               0     unicast
Finance                               2     unicast
Marketing                             3     unicast
```

5. 配置SGFW。最后一步是配置在允许从金融的ICMP流量到销售的外部接口的ACL。

```
access-list outside extended permit icmp security-group tag 2 any security-group
tag 3 any
access-group outside in interface outside
```

并且，安全组组名能使用而不是标记。

```
access-list outside extended permit icmp security-group name Finance any
security-group name Marketing any
```

为了保证接口ACL处理VPN流量，禁用默认情况下允许VPN流量，不用验证通过接口ACL的选项是必要的。

```
no sysopt connection permit-vpn
```

现在ASA应该准备分类VPN用户和进行根据SGTs的实施。

验证

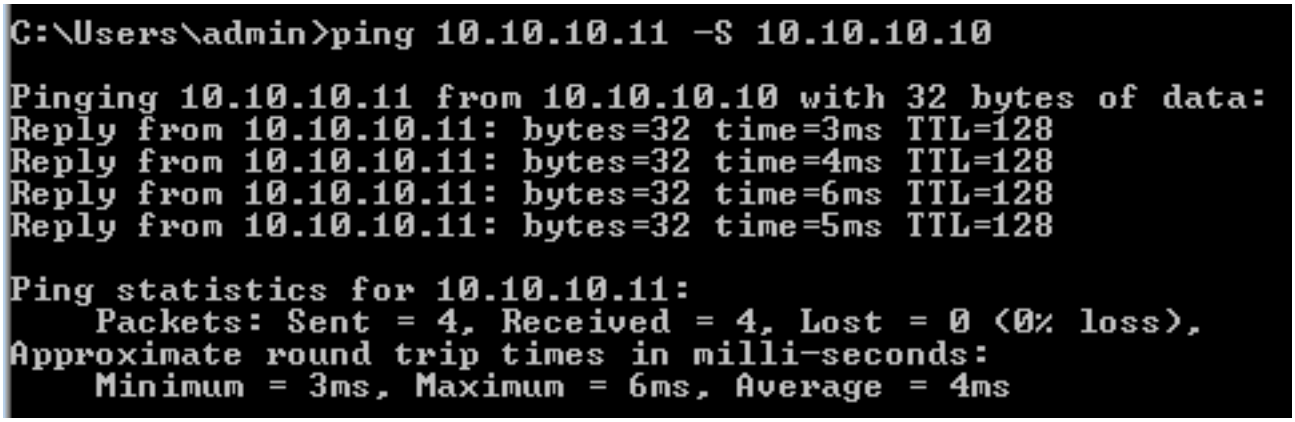
使用本部分可确认配置能否正常运行。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令。使用输出解释器工具来查看 show 命令输出的分析。

在VPN设立后，ASA提交应用的SGT给每会话。

```
ASA(config)# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : cisco                  Index        : 1
Assigned IP  : 10.10.10.10            Public IP    : 192.168.10.68
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 35934                  Bytes Rx     : 79714
Group Policy : GP-SSL                 Tunnel Group : RA
Login Time   : 17:49:15 CET Sun Mar 16 2014
Duration     : 0h:22m:57s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a8700a000010005325d60b
Security Grp : 2:Finance

Username     : cisco2                 Index        : 2
Assigned IP  : 10.10.10.11            Public IP    : 192.168.10.80
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Essentials
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 86171                  Bytes Rx     : 122480
Group Policy : GP-SSL                 Tunnel Group : RA
Login Time   : 17:52:27 CET Sun Mar 16 2014
Duration     : 0h:19m:45s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : c0a8700a000020005325d6cb
Security Grp : 3:Marketing
```

SGFW允许从金融(SGT=2)的ICMP流量对销售(SGT=3)。所以用户‘cisco’能ping用户'cisco2。



计数器增加：

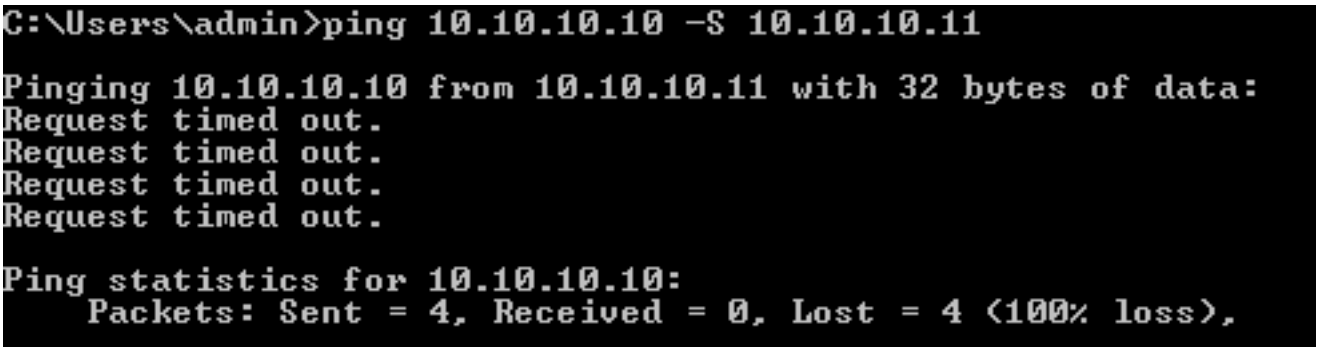
```
ASA(config)# show access-list outside
access-list outside; 1 elements; name hash: 0x1a47dec4
access-list outside line 1 extended permit icmp security-group
tag 2(name="Finance") any security-group tag 3(name="Marketing")
any (hitcnt=4) 0x071f07fc
```

连接创建：

```
Mar 16 2014 18:24:26: %ASA-6-302020: Built inbound ICMP connection for
faddr 10.10.10.10/1(LOCAL\cisco, 2:Finance) gaddr 10.10.10.11/0
laddr 10.10.10.11/0(LOCAL\cisco2, 3:Marketing) (cisco)
```

因为ICMP检查启用，回程数据流自动地接受。

当您设法从营销(SGT=3) ping提供经费(SGT=2) ：



ASA报告：

```
Mar 16 2014 18:06:36: %ASA-4-106023: Deny icmp src outside:10.10.10.11(LOCAL\cisco2,
3:Marketing) dst outside:10.10.10.10(LOCAL\cisco, 2:Finance) (type 8, code 0) by
access-group "outside" [0x0, 0x0]
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

请参阅这些文档：

- 与802.1x MACsec的TrustSec Cloud在Catalyst 3750X系列交换机配置示例

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

摘要

此条款展示关于怎样的一个简单的示例分类VPN用户和进行基本实施。VPN用户和其余的也SGFW过滤流量网络之间。SXP (TrustSec SGT交换协议)在ASA可以用于得到在IP和SGTs之间的映射信息。那允许ASA进行适当地分类会话的所有类型的实施(VPN或LAN)。

在ASA软件方面，版本9.2和以上， ASA也支持RADIUS更改授权(CoA) (RFC 5176)。从ISE发送的RADIUS CoA数据包，在一成功的VPN状态能包括cisco-av-pair与分配一个兼容用户到一不同的SGT后(更加安全的)组。关于更多示例，请参阅在相关信息部分的条款。

相关信息

- 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
- 技术支持和文档 - Cisco Systems