Classificação de SGT VPN ASA versão 9.2 e exemplo de configuração de aplicação

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Configurar](#)
[Diagrama de Rede](#)
[Configuração do ISE](#)
[Configuração do ASA](#)
[Verificar](#)
[Troubleshoot](#)
[Summary](#)
[Informações Relacionadas](#)

Introduction

Este documento descreve como usar um novo recurso na classificação Adaptive Security Appliance (ASA) Versão 9.2.1, TrustSec Security Group Tag (SGT) para usuários VPN. Este exemplo apresenta dois usuários de VPN que receberam um SGT e um Security Group Firewall (SGFW) diferentes, que filtram o tráfego entre os usuários de VPN.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da configuração CLI do ASA e da configuração VPN SSL
- Conhecimento básico da configuração da VPN de acesso remoto no ASA
- Conhecimento básico do Identity Services Engine (ISE) e dos serviços TrustSec

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

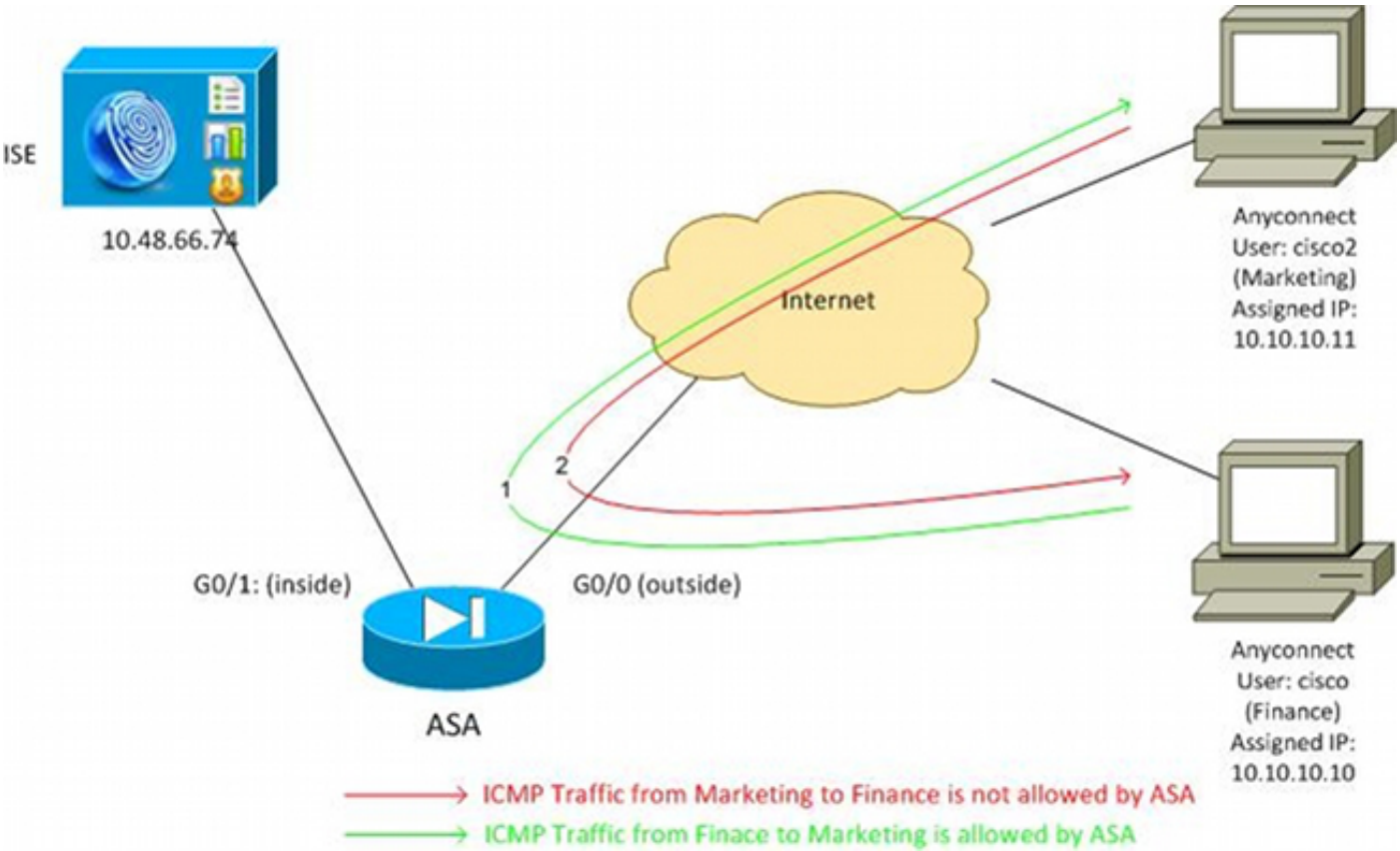
- Software Cisco ASA, versão 9.2 e posterior
- Windows 7 com Cisco AnyConnect Secure Mobility Client, versão 3.1
- Cisco ISE, versão 1.2 e posterior

Configurar

Nota:Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

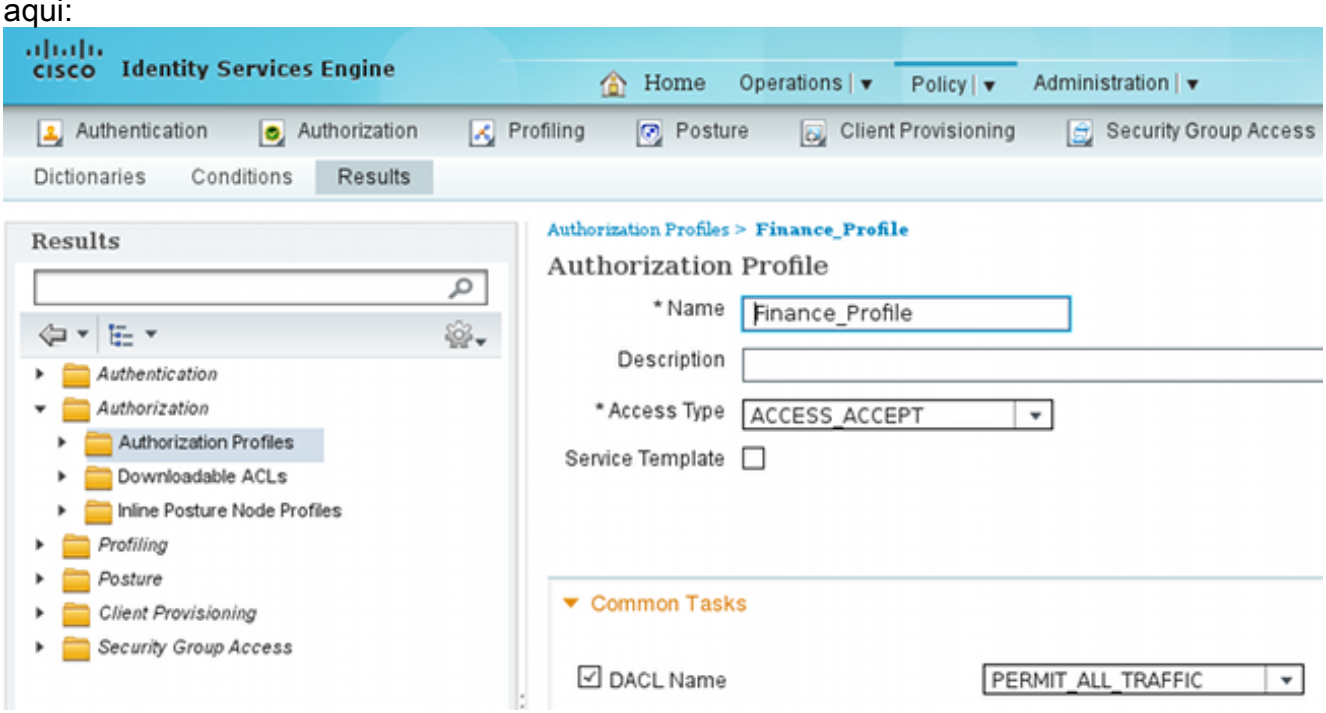
O usuário da VPN 'cisco' é atribuído à equipe financeira, que tem permissão para iniciar uma conexão do Internet Control Message Protocol (ICMP) com a equipe de marketing. O usuário da VPN 'cisco2' é atribuído à equipe de Marketing, que não tem permissão para iniciar nenhuma conexão.



Configuração do ISE

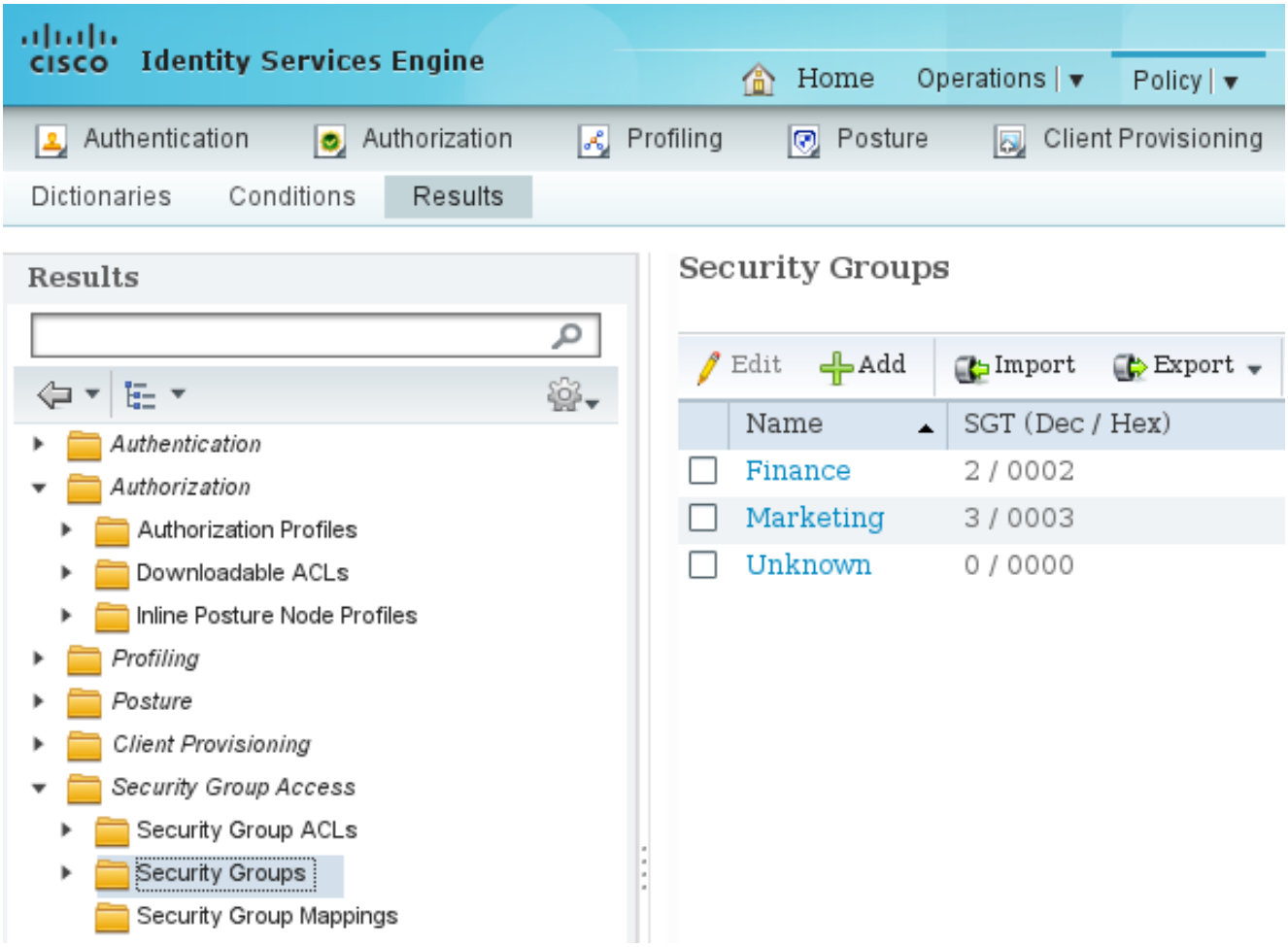
1. Escolha **Administration > Identity Management > Identities** para adicionar e configurar o usuário 'cisco' (do Departamento Financeiro) e 'cisco2' (do Departamento de Marketing).
2. Escolha **Administration > Network Resources > Network Devices** para adicionar e configurar o ASA como um dispositivo de rede.
3. Escolha **Policy > Results > Authorization > Authorization Profiles** para adicionar e configurar os perfis de autorização Finance e Marketing.Ambos os perfis incluem apenas um atributo,

lista de controle de acesso para download (DACL), que permite todo o tráfego. Um exemplo para Finanças é mostrado
aqui:

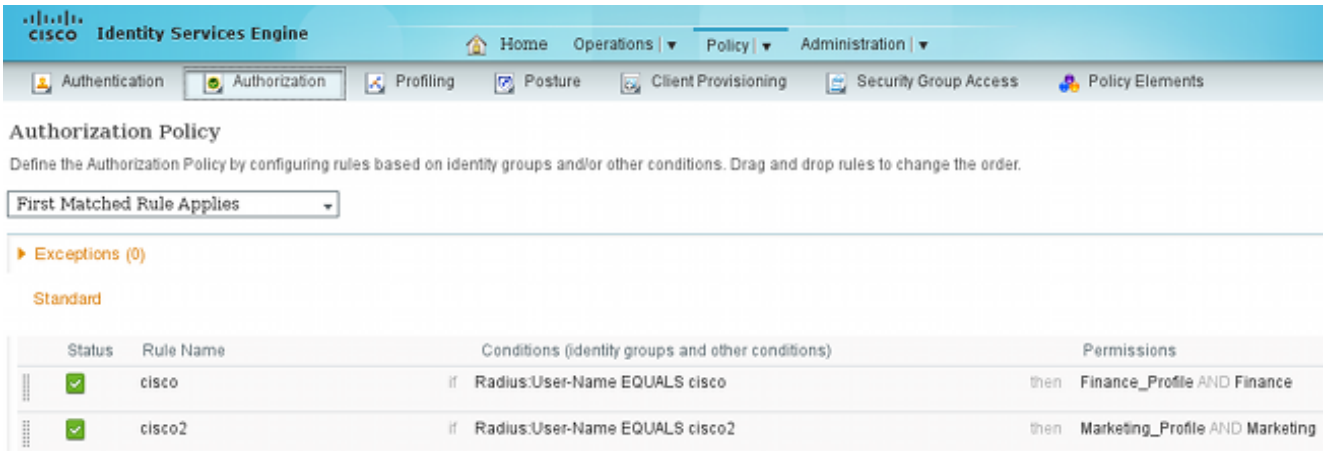


Cada perfil pode ter uma DACL específica e restritiva, mas para esse cenário todo o tráfego é permitido. A aplicação é realizada pelo SGFW, não pelo DACL atribuído a cada sessão VPN. O tráfego filtrado com um SGFW permite o uso apenas de SGTs em vez de endereços IP usados pelo DACL.

4. Escolha **Policy > Results > Security Group Access > Security Groups** para adicionar e configurar os grupos de SGT de Finanças e
Marketing.



5. Escolha **Policy > Authorization** para configurar as duas regras de autorização. A primeira regra atribui o Finance_profile (DACL que permite tráfego inteiro) junto com o grupo SGT Finance ao usuário 'cisco'. A segunda regra atribui o Marketing_profile (DACL que permite o tráfego inteiro) junto com o Marketing do grupo SGT ao usuário 'cisco2'.



Configuração do ASA

1. Conclua a configuração básica de VPN.

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

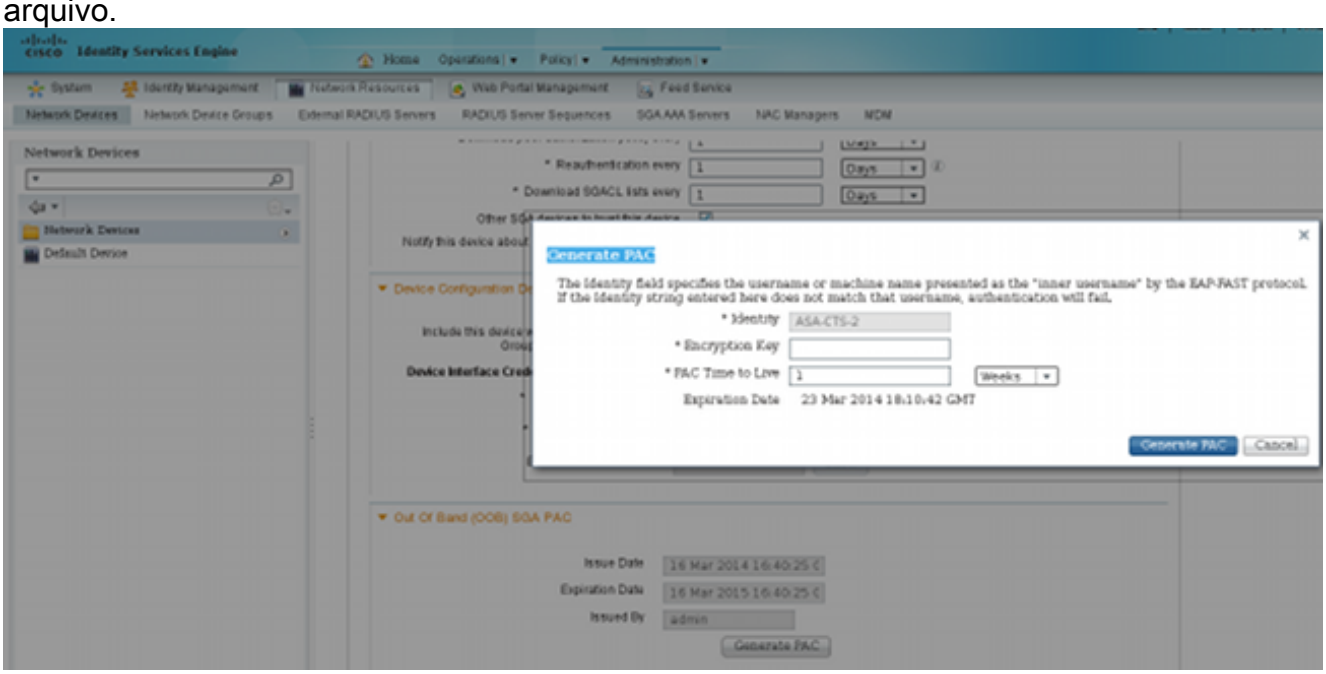
```
group-policy GP-SSL internal
group-policy GP-SSL attributes
 vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

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. Conclua a configuração ASA AAA e TrustSec.

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

Para participar da nuvem TrustSec, o ASA precisa se autenticar com a PAC (Protected Access Credential). O ASA não oferece suporte ao provisionamento automático de PAC, razão pela qual esse arquivo precisa ser gerado manualmente no ISE e importado para o ASA.

3. Escolha **Administration > Network Resources > Network Devices > ASA > Advanced TrustSec Settings** para gerar uma PAC no ISE. Escolha **fornecimento de PAC fora de banda (OOB)** para gerar o arquivo.



4. Importe a PAC para o ASA.O arquivo gerado pode ser colocado em um servidor HTTP/FTP. O ASA usa isso para importar o arquivo.

```
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:
  000200b80003000100040010ea48096688d96ef7b94c679a17bdad6f0006009c000301
  0015e3473e728ae73cc905887bdc8d3cee00000013532150cc00093a8064f7ec374555
  e7b1fd5abccb17de31b9049066f1a791e87275b9dd10602a9cb4f841f2a7d98486b2cb
  2b5dc3449f67c17f64d12d481be6627e4076a2a63d642323b759234ab747735a03e01b
  99be241bb1f38a9a47a466ea64ea334bf51917bd9aa9ee3cf8d401dc39135919396223
  11d8378829cc007b91ced9117a
```

Quando você tiver a PAC correta, o ASA executará automaticamente uma atualização de ambiente. Isso baixa informações do ISE sobre grupos SGT atuais.

```
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. Configure o SGFW. A última etapa é configurar a ACL na interface externa que permite o tráfego ICMP de Finanças para Marketing.

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

Além disso, o nome do Grupo de segurança pode ser usado em vez da marca.

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

Para garantir que a ACL de interface processe o tráfego de VPN, é necessário desativar a opção que, por padrão, permite o tráfego de VPN sem validação através da ACL de interface.

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

Agora, o ASA deve estar pronto para classificar usuários de VPN e executar a aplicação com base em SGTs .

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

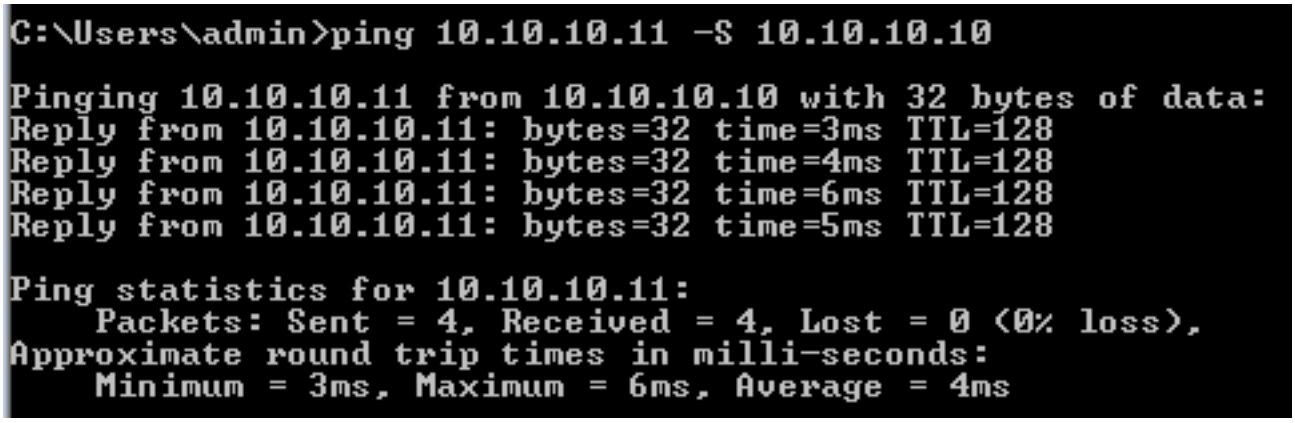
O Ferramenta Output Interpreter (registrado somente clientes) oferece suporte a determinados **show** comandos. Use a Output Interpreter Tool para exibir uma análise de **show** Saída do comando.

Depois que a VPN é estabelecida, o ASA apresenta um SGT aplicado a cada sessão.

```
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
```

O SGFW permite o tráfego ICMP do departamento financeiro (SGT=2) ao de marketing (SGT=3). É por isso que o usuário 'cisco' pode fazer ping no usuário 'cisco2'.



Os contadores aumentam:

```
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
```

A conexão foi criada:

```
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)
```

O tráfego de retorno é aceito automaticamente, pois a inspeção ICMP está habilitada.

Ao tentar fazer ping de Marketing (SGT=3) para Finanças (SGT=2):

```
C:\Users\admin>ping 10.10.10.10 -S 10.10.10.11

Pinging 10.10.10.10 from 10.10.10.11 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Relatórios ASA:

```
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]
```

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Consulte estes documentos:

- Exemplo de Configuração de Nuvem TrustSec com MACsec 802.1x no Switch Catalyst 3750X Series
- Exemplo de configuração do TrustSec com ASA e o switch Catalyst 3750-X Series e Guia de solução de problemas

Summary

Este artigo apresenta um exemplo simples de como classificar usuários de VPN e executar a aplicação básica. O SGFW também filtra o tráfego entre os usuários da VPN e o restante da rede. O SXP (TrustSec SGT Exchange Protocol) pode ser usado em um ASA para obter as informações de mapeamento entre IP e SGTs. Isso permite que um ASA execute a aplicação para todos os tipos de sessões que foram devidamente classificadas (VPN ou LAN).

No software ASA, Versão 9.2 e posterior, o ASA também oferece suporte à Alteração de Autorização (CoA) RADIUS (RFC 5176). Um pacote RADIUS CoA enviado do ISE após uma postura de VPN bem-sucedida pode incluir cisco-av-pair com um SGT que atribui um usuário compatível a um grupo diferente (mais seguro). Para obter mais exemplos, consulte os artigos na seção Informações Relacionadas.

Informações Relacionadas

- Exemplo de postura de VPN na ASA versão 9.2.1 com configuração do ISE
- Exemplo de configuração do TrustSec com ASA e o switch Catalyst 3750-X Series e Guia de solução de problemas
- Guia de configuração do switch Cisco TrustSec: noções básicas sobre o Cisco TrustSec

- Como configurar um servidor externo para autorização de usuário de dispositivo de segurança
- Guia de configuração de CLI para VPN da Cisco ASA Series, 9.1
- Manual do usuário do Cisco Identity Services Engine, versão 1.2
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.