

Configurar a marcação em linha do ASA 9.3.1 TrustSec

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[ISE - Etapas de configuração](#)

[1. SGT para finanças e marketing](#)

[2. ACL do grupo de segurança para o marketing de tráfego > Finanças](#)

[3. Vinculando ACL na matriz](#)

[4. Regra de autorização para acesso VPN Atribuindo SGT = 3 \(Marketing\)](#)

[5. Regra de autorização para acesso 802.1x Atribuição SGT = 2 \(Finanças\)](#)

[6. Adicionando dispositivo de rede, gerando PAC para ASA](#)

[7. Adicionar dispositivo de rede, Configurar segredo para provisionamento automático de PAC do switch](#)

[ASA - Etapas de configuração](#)

[1. Acesso VPN básico](#)

[2. Importar PAC e ativar cts](#)

[3. SGACL para finanças de tráfego > marketing](#)

[4. Ativar cts na interface interna](#)

[Switch - Etapas de Configuração](#)

[1. 802.1x básico](#)

[2. Configuração e provisionamento de CTS](#)

[3. Ativar cts na interface do ASA](#)

[Verificar](#)

[Troubleshoot](#)

[Atribuição SGT](#)

[Aplicação no ASA](#)

[Aplicação do switch](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como usar o recurso implementado no Adaptive Security Appliance (ASA) versão 9.3.1 - marcação em linha TrustSec. Esse recurso permite que o ASA receba quadros TrustSec e envie-os. Dessa forma, o ASA pode ser facilmente integrado no domínio TrustSec sem a necessidade de usar o TrustSec SGT Exchange Protocol (SXP).

Este exemplo apresenta o usuário remoto VPN que recebeu a tag Security Group Tag (SGT) = 3

(Marketing) e o usuário 802.1x que receberam a tag SGT = 2 (Finanças). A aplicação de tráfego é realizada pelo ASA com o uso da Security Group Access Control List (SGACL) definida localmente e pelo switch Cisco IOS® usando a RBACL (Role Based Access Control List) baixada do Identity Services Engine (ISE).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do ASA CLI e configuração do Secure Socket Layer (SSL) VPN
- Configuração de VPN de acesso remoto no ASA
- Serviços ISE e TrustSec

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Software Cisco ASA, versão 9.3.1 e posterior
- Hardware Cisco ASA 55 horas por dia, 5 dias por semana ou ASAv
- Windows 7 com Cisco AnyConnect Secure Mobility Client, versão 3.1
- Switch Cisco Catalyst 3750X com software 15.0.2 e posterior
- Cisco ISE, versão 1.2 e posterior

Configurar

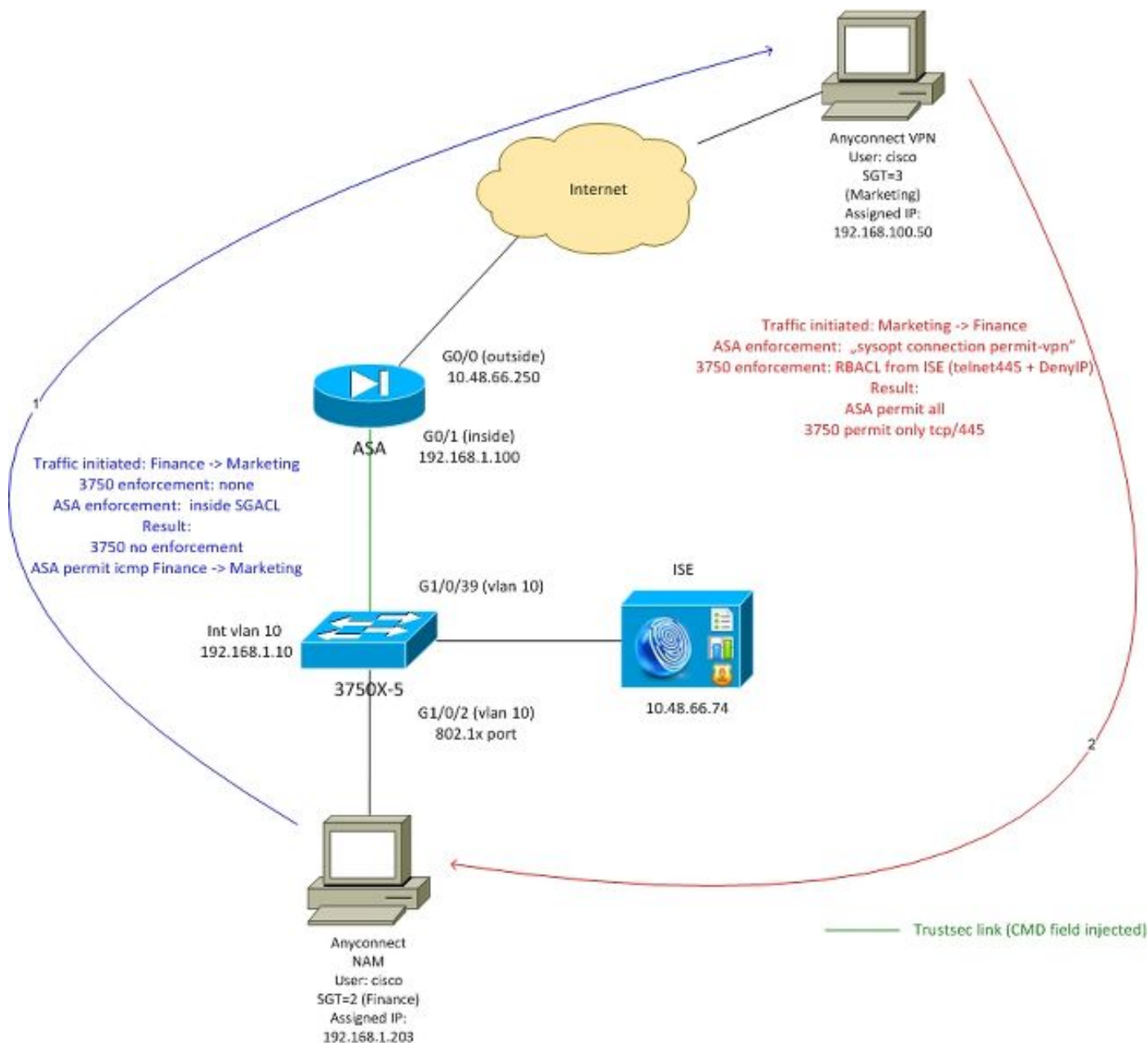
Note: Use a [Command Lookup Tool \(somente clientes registrados\)](#) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

A conexão entre ASA e 3750X é configurada para cts manuais. Isso significa que ambos os dispositivos podem enviar e receber quadros Ethernet modificados com o Cisco Metadata Field (CMD). Esse campo inclui Security Group Tag (SGT), que descreve a origem do pacote.

O usuário de VPN remoto encerra a sessão SSL no ASA e recebe a tag 3 SGT (Marketing).

Usuário 802.1x corporativo local depois que a autenticação bem-sucedida foi atribuída à tag SGT 2 (Finance).



O ASA tem SGACL configurado na interface interna que permite o tráfego ICMP iniciado do departamento financeiro ao departamento de marketing.

O ASA permite que todo o tráfego iniciado remova o usuário da VPN (devido à configuração "sysopt connection permit-vpn").

O SGACL no ASA é stateful, o que significa que, depois que o fluxo é criado, o pacote de retorno é aceito automaticamente (com base na inspeção).

O switch 3750 usa RBACL para controlar o tráfego recebido de Marketing para Finanças.

O RBACL é stateless, o que significa que cada pacote é verificado, mas a aplicação do TrustSec na plataforma 3750X é executada no destino. Dessa forma, o switch é responsável pela aplicação do tráfego de Marketing para Finanças.

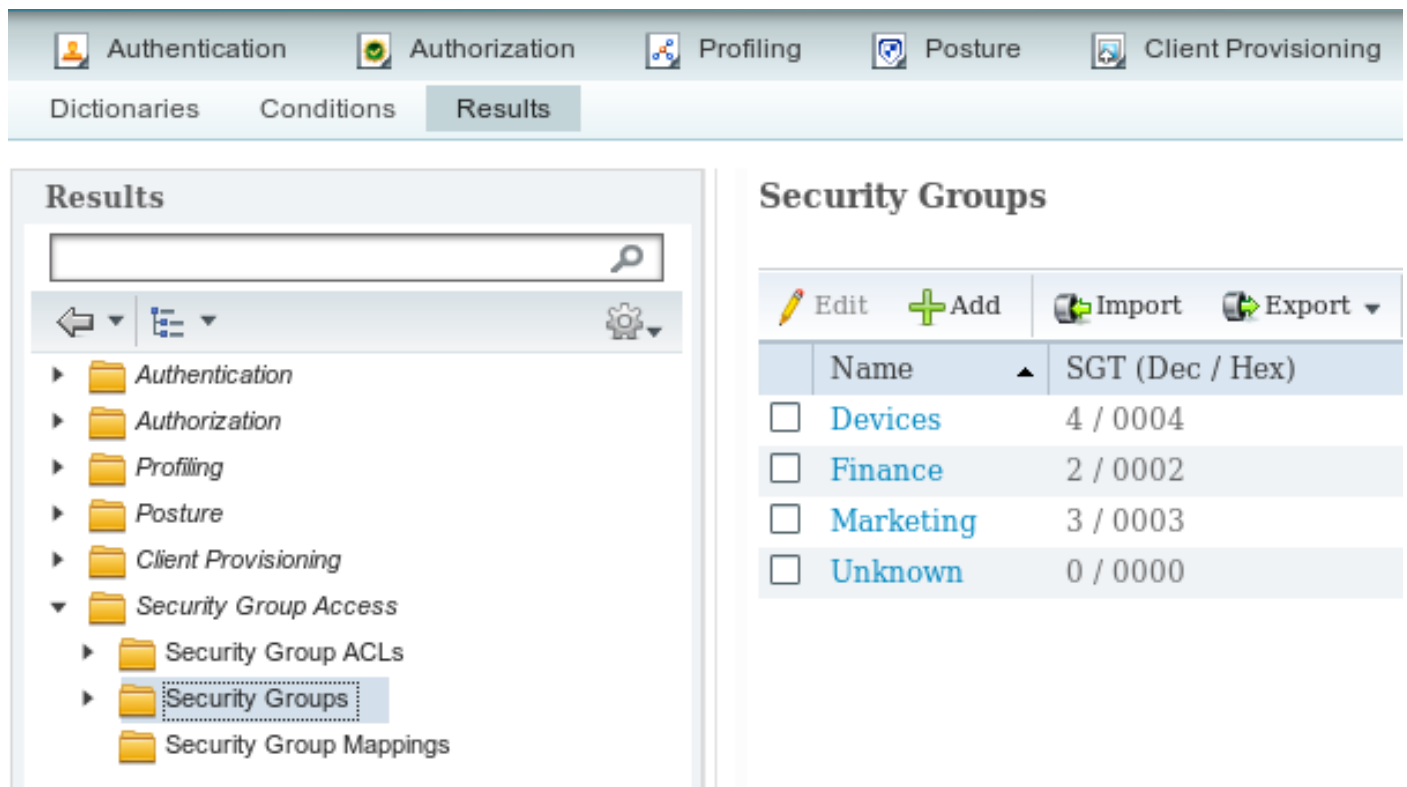
Note: Para o firewall stateful com reconhecimento de Trustsec no Cisco IOS ® Zone Based Firewall pode ser usado. Por exemplo, consulte:

Note: O ASA pode ter o SGACL controlando o tráfego que vem do usuário remoto de VPN. Para simplificar o cenário, ele não foi apresentado neste artigo. Por exemplo, consulte: [Exemplo de Configuração de Classificação e Imposição de VPN SGT do ASA versão 9.2](#)

ISE - Etapas de configuração

1. SGT para finanças e marketing

Navegue até **Policy > Results > Security Group Access > Security Groups** e crie SGT for Finance and Marketing como mostrado nesta imagem.



The screenshot displays the Cisco ISE configuration interface. The top navigation bar includes tabs for Authentication, Authorization, Profiling, Posture, and Client Provisioning. Below this, there are sub-tabs for Dictionaries, Conditions, and Results. The main content area is split into two panes. The left pane, titled 'Results', shows a tree view of configuration objects. The 'Security Groups' folder is expanded and highlighted. The right pane, titled 'Security Groups', contains a table with the following data:

	Name	SGT (Dec / Hex)
<input type="checkbox"/>	Devices	4 / 0004
<input type="checkbox"/>	Finance	2 / 0002
<input type="checkbox"/>	Marketing	3 / 0003
<input type="checkbox"/>	Unknown	0 / 0000

2. ACL do grupo de segurança para o marketing de tráfego > Finanças

Navegue até **Policy > Results > Security Group Access > Security Group ACL (Política > Resultados > Acesso do grupo de segurança > ACL do grupo de segurança)** e crie uma ACL usada para controlar o tráfego de Marketing para Finanças. Somente tcp/445 é permitido conforme mostrado nesta imagem.

The screenshot displays the Cisco ISE configuration interface. At the top, there are navigation tabs for Authentication, Authorization, Profiling, Posture, and Client Provisioning. Below these are sub-tabs for Dictionaries, Conditions, and Results. The Results tab is active, showing a left-hand navigation pane with a tree structure. The tree includes folders for Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access, Security Group ACLs (selected), Security Groups, and Security Group Mappings. The main content area is titled 'Security Groups ACLs List > telnet445' and 'Security Group ACLs'. It contains a form with the following fields: 'Name' (telnet445), 'Description' (empty), 'IP Version' (IPv4 selected), and 'Security Group ACL content' (permit tcp dst eq 445).

3. Vinculando ACL na matriz

Navegue até **Política > Política de saída > Matriz** vincular a ACL configurada para a origem: **Marketing** e destino: **Finanças**. Também anexe **Deny IP** como a última ACL a descartar todo o tráfego restante como mostrado na imagem. (sem essa política padrão, o padrão é permit any)

Authentication Authorization Profiling Posture Client Provisioning Security Group Access

Egress Policy Network Device Authorization

Source Tree Destination Tree **Matrix**

Egress Policy (Matrix View)

Edit Add Clear Mapping Configure Push Monitor All Dimension 3X5

Destination Source	Devices (4 / 0004)	Finance (2 / 0002)
Devices (4 / 0004)		
Finance (2 / 0002)		
Marketing (3 / 0003)		<input checked="" type="checkbox"/> Enabled SGACLs: telnet445, Deny IP

4. Regra de autorização para acesso VPN Atribuindo SGT = 3 (Marketing)

Navegue até **Policy > Authorization** e crie uma regra para acesso remoto à VPN. Todas as conexões VPN estabelecidas através do cliente AnyConnect 4.x terão acesso total (PermitAccess) e receberão a tag SGT 3 (Marketing). A condição é usar o AnyConnect Identity Extentions ([ACIDEX](#)):

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

5. Regra de autorização para acesso 802.1x Atribuição SGT = 2 (Finanças)

Navegue até **Política > Autorização** e crie uma regra para acesso 802.1x. O requerente que encerra a sessão 802.1x no switch 3750 com o nome de usuário **cisco** obterá acesso total (PermitAccess) e receberá a tag SGT 2 (Finance).

```
Rule name: 802.1x
```

Condition: Radius:User-Name EQUALS cisco AND Radius:NAS-IP-Address EQUALS 192.168.1.10
Permissions: PermitAccess AND Finance

6. Adicionando dispositivo de rede, gerando PAC para ASA

Para adicionar o ASA ao domínio TrustSec, é necessário gerar o arquivo PAC manualmente. Esse arquivo é importado no ASA.

Isso pode ser configurado em **Administração > Dispositivos de Rede**. Depois que o ASA for adicionado, role para baixo até **as configurações do TrustSec** e **gere PAC** como mostrado nesta imagem.

✕

Generate PAC

The Identity field specifies the username or machine name presented as the "inner username" by the EAP-FAST protocol. If the Identity string entered here does not match that username, authentication will fail.

* Identity

* Encryption Key

* PAC Time to Live

Expiration Date 19 Apr 2015 09:06:30 GMT

▼ Out Of Band (OOB) TrustSec PAC

Issue Date

Expiration Date

Issued By

Os switches (3750X) suportam provisionamento automático de PAC, de modo que as etapas só precisem ser executadas para o ASA, que suporta apenas o provisionamento manual de PAC.

7. Adicionar dispositivo de rede, Configurar segredo para provisionamento automático de PAC do switch

Para um switch que usa provisionamento automático de PAC, um segredo correto deve ser definido, como mostrado nesta imagem.

▼ Advanced TrustSec Settings

▼ Device Authentication Settings

Use Device ID for SGA Identification

Device Id

* Password

Note: A PAC é usada para autenticar o ISE e baixar dados do ambiente (por exemplo, SGT) junto com a política (ACL). O ASA oferece suporte apenas a dados de ambiente, as políticas precisam ser configuradas manualmente no ASA. O Cisco IOS® suporta ambos, para que as políticas possam ser baixadas do ISE.

ASA - Etapas de configuração

1. Acesso VPN básico

Configure o acesso VPN SSL básico para AnyConnect usando ISE para autenticação.

```
aaa-server ISE protocol radius
aaa-server ISE (inside) host 10.62.145.41
  key cisco

webvpn
  enable outside
  anyconnect-essentials
  anyconnect image disk0:/anyconnect-win-4.0.00051-k9.pkg 1
  anyconnect enable
  tunnel-group-list enable
  error-recovery disable

tunnel-group TAC type remote-access
tunnel-group TAC general-attributes
  address-pool (outside) POOL
  authentication-server-group ISE
  default-group-policy TAC
tunnel-group TAC webvpn-attributes
  group-alias TAC enable

ip local pool POOL 192.168.100.50-192.168.100.60 mask 255.255.255.0
```

2. Importar PAC e ativar cts

Importar PAC gerado para ASA (da Etapa 6 da configuração do ISE). Usar a mesma chave de criptografia:

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

Para verificar:

```
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
```

Ativar cts:

```
cts server-group ISE
```

Depois de habilitar o cts, o ASA deve baixar os dados do ambiente do ISE:

```
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. SGACL para finanças de tráfego > marketing

Configure o SGACL na interface interna. A ACL permite iniciar somente o tráfego ICMP do departamento financeiro para o departamento de marketing.

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

O ASA deve expandir o nome da marca para o número:

```
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. Ativar cts na interface interna

Depois de habilitar os cts na interface interna do ASA:

```
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
```

O ASA pode enviar e receber quadros TrustSec (quadros Ethernet com campo CMD). O ASA supõe que todos os quadros de entrada sem uma marca devem ser tratados como com a marca 100. Todos os quadros de entrada que já incluem a marca serão confiáveis.

Switch - Etapas de Configuração

1. 802.1x básico

```
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
```

Com essa configuração, após uma autorização 802.1x bem-sucedida, o usuário (autorizado via ISE) deve receber a tag 2 (Finanças).

2. Configuração e provisionamento de CTS

Da mesma forma, quanto ao ASA, o cts é configurado e aponta para o ISE:

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

Além disso, a aplicação está habilitada para Camada 3 e Camada 2 (todas as vlans):

```
cts role-based enforcement
cts role-based enforcement vlan-list 1-1005,1008-4094
```

Para provisionar a PAC automaticamente:

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

Novamente, a senha deve corresponder à configuração correspondente no ISE (**Network Device > Switch > TrustSec**). No momento, o Cisco IOS® inicia a sessão EAP-FAST com o ISE para obter a PAC. Mais detalhes sobre esse processo podem ser encontrados aqui:

[Exemplo de configuração do TrustSec com ASA e o switch Catalyst 3750-X Series e Guia de solução de problemas](#)

Para verificar se a PAC está instalada:

```
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:
```

```
000200B00003000100040010EA48096688D96EF7B94C679A17BDAD6F0006009400030100365AB3133998C86C1BA1B418
968C60690000001355261CCC00093A808F8A81F3F8C99A7CB83A8C3BFC4D573212C61CDCEB37ED279D683EE0DA60D86D
5904C41701ACF07BE98B3B73C4275C98C19A1DD7E1D65E679F3E9D40662B409E58A9F139BAA3BA3818553152F28AE04B
089E5B7CBB22A0D4BCEEFF80F826A180B5227EAACBD07709DBDCD3CB42AA9F996829AE46F
```

Refresh timer is set for 4y14w

3. Ativar cts na interface do ASA

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

A partir de agora, o switch deve estar pronto para processar e enviar quadros TrustSec e aplicar as políticas baixadas do ISE.

Verificar

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

A verificação é abordada em seções individuais deste documento.

Troubleshoot

Atribuição SGT

Depois que a sessão VPN para o ASA é estabelecida, a atribuição SGT correta deve ser confirmada:

```
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
```

De acordo com as regras de autorização do ISE, todos os usuários do AnyConnect4 foram atribuídos à marca de marketing.

O mesmo com a sessão 802.1x no switch. Depois que o AnyConnect Network Analysis Module (NAM) for concluído, o switch de autenticação aplicará a marca correta retornada do ISE:

```
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

De acordo com as regras de autorização do ISE, todos os usuários conectados a esse switch devem ser atribuídos a SGT = 2 (Finanças).

Aplicação no ASA

Quando você tenta enviar um tráfego do Finance (192.168.1.203) para o Marketing (192.168.100.50), ele atinge a interface interna do ASA. Para solicitação de eco ICMP, ela cria a sessão:

```
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)
```

e aumenta os contadores da ACL:

```
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)
```

Isso também pode ser confirmado ao observar capturas de pacotes. Observe que as marcas corretas são exibidas:

```
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
```

Há uma solicitação de eco ICMP de entrada marcada com SGT = 2 (Finance) e, em seguida, uma resposta do usuário VPN marcada pelo ASA com SGT = 3 (Marketing). Outra ferramenta de solução de problemas, o packet-tracer também está pronto para o TrustSec.

Infelizmente, o PC 802.1x não vê essa resposta porque está bloqueado pelo RBACL stateless no switch (explicação na próxima seção).

Outra ferramenta de solução de problemas, o packet-tracer também está pronto para o TrustSec. Vamos confirmar se o pacote ICMP recebido da Finance será aceito:

```
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

Vamos também tentar iniciar qualquer conexão TCP de Finance para Marketing, que deve ser bloqueada pelo ASA:

```
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]
```

Aplicação do switch

Vamos verificar se o switch baixou corretamente as políticas do ISE:

```
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
```

A política que controla o tráfego de Marketing para Finanças está instalada corretamente. Somente tcp/445 é permitido como por RBACL:

```
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
```

Essa é a razão pela qual a resposta de eco ICMP que vem de Marketing para Finanças foi descartada. Isso pode ser confirmado verificando-se os contadores de tráfego do SGT 3 para o 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
```

Os pacotes foram descartados pelo hardware (o contador atual é 65 e aumenta a cada 1 segundo).

E se a conexão tcp/445 for iniciada no Marketing?

O ASA permite isso (aceita todo o tráfego VPN devido ao "sysopt connection 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)
```

A sessão correta é criada:

```
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
```

Além disso, o Cisco IOS® aceita-o, já que ele corresponde ao telnet445 RBACL. Os contadores corretos aumentam:

```
bsns-3750-5#show cts role-based counters from 3 to 2
3      2      0      65      0      3
```

(a última coluna é o tráfego permitido pelo hardware). A sessão é permitida.

Este exemplo é apresentado de propósito para mostrar a diferença na configuração e aplicação das políticas TrustSec no ASA e no Cisco IOS®. Esteja ciente das diferenças das políticas do Cisco IOS® baixadas do ISE (RBACL stateless) e do firewall baseado em zona stateful com reconhecimento de TrustSec.

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 de switches com 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](#)