

# Colocação de etiquetas inline ASA 9.3.1

## TrustSec - exemplo de configuração

### Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[ISE - Passos de configuração](#)

1. [SGT para a finança e o mercado](#)
2. [Grupo de segurança ACL para o mercado do tráfego - >Finance](#)
3. [ACL obrigatório na matriz](#)
4. [Regra da autorização para o acesso VPN que atribui SGT = 3 \(mercado\)](#)
5. [Regra da autorização para o acesso do 802.1x que atribui SGT = 2 \(finança\)](#)
6. [Adicionando o dispositivo de rede, gerando o PAC para o ASA](#)
7. [Adicionando o dispositivo de rede, configurando o segredo para o abastecimento automático do interruptor PAC](#)

[ASA - Passos de configuração](#)

1. [Acesso básico VPN](#)
2. [Importe o PAC e permita cts](#)
3. [SGACL para a finança do tráfego - > mercado](#)
4. [Permita cts na interface interna](#)

[Etapas da configuração de switch](#)

1. [802.1x básico](#)
2. [Configuração e abastecimento CTS](#)
3. [Permita cts na relação ao ASA](#)

[Troubleshooting](#)

[Atribuição SGT](#)

[Aplicação no ASA](#)

[Comute a aplicação](#)

[Referências](#)

[Cisco relacionado apoia discussões da comunidade](#)

### Introdução

Este documento descreve como usar a característica executada na liberação adaptável 9.3.1 da ferramenta de segurança (ASA) - colocação de etiquetas Inline de TrustSec. Que a característica permite que o ASA receba quadros de TrustSec assim como os envie. Esta maneira ASA pode facilmente ser integrada dentro do domínio de TrustSec sem a necessidade de usar o protocolo de intercâmbio de TrustSec SGT (SXP).

Este exemplo apresenta o usuário remoto VPN que foram atribuídos a etiqueta da etiqueta do grupo de segurança (SGT) = 3 (mercado) e o usuário do 802.1x que foram atribuídos a etiqueta SGT = 2 (finança). A aplicação do tráfego será executada pelo ASA usando o grupo de segurança que o Access Control List (SGACL) definiu localmente e os IO comutam usando o Access Control List baseado papel (RBACL) transferido do Identity Services Engine (ISE).

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Software de Cisco ASA, versão 9.3.1 e mais recente
- Hardware 55x5 ou ASAv de Cisco ASA.
- Windows 7 com Cliente de mobilidade Cisco AnyConnect Secure, liberação 3.1
- Cisco Catalyst 3750X Switch com software 15.0.2 e mais atrasado
- Cisco ISE, libera 1.2 e mais atrasado

## Configurar

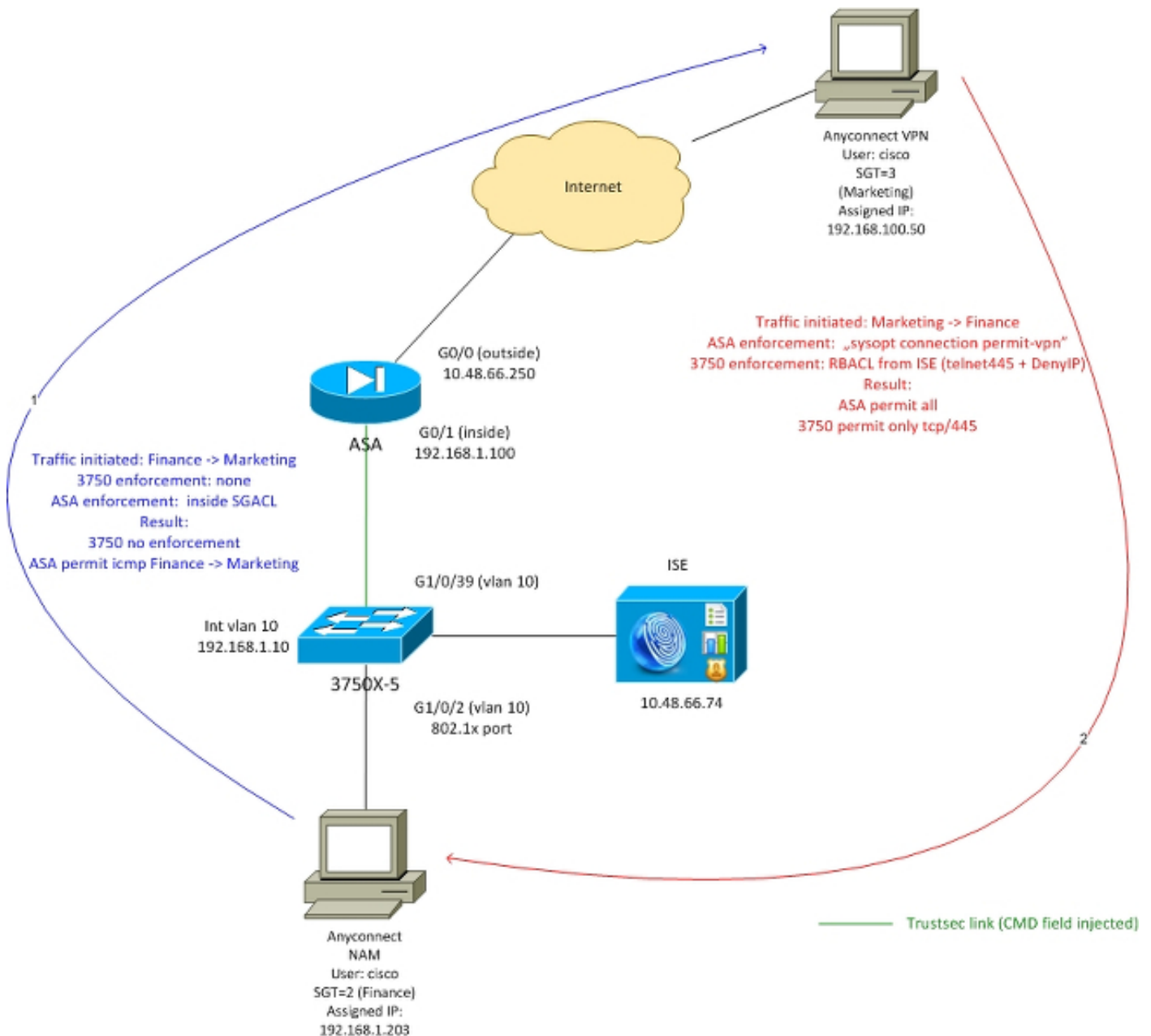
**Note:** Use a [Command Lookup Tool](#) ( [somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

### Diagrama de Rede

A conexão entre o ASA e o 3750X é configurada para cts manuais. Isso significa que ambos os dispositivos podem enviar e para receber frames da Ethernet alterados com Metadata de Cisco coloque (CMD). Esse campo inclui a etiqueta SGT que descreve a fonte do pacote.

O usuário remoto VPN está terminando a sessão de SSL no ASA e atribuída a etiqueta 3 SGT (mercado).

Usuário corporativo local do 802.1x depois que a autenticação bem sucedida foi atribuída a etiqueta 2 SGT (finança).



O ASA está tendo SGACL configurado na interface interna permitindo o tráfego ICMP iniciado da finança ao mercado.

O ASA permitirá todo o tráfego iniciado de remove o usuário VPN (devido “sysopt à configuração da conexão licença-VPN”).

SGACL no ASA é o stateful - que significa que uma vez o fluxo é pacote de informação de retorno criado está aceitado automaticamente (baseado no inspection).

O 3750 Switch está usando RBACL ao tráfego de controle recebido do mercado para financiar.

RBACL é apátrida - que significa que cada pacote está verificado - mas aplicação de TrustSec na plataforma 3750X é executado no destino. Este interruptor da maneira é responsável para a aplicação do tráfego do mercado financiar.

Nota:

Para o firewall stateful ciente de Trustsec em IO que Firewall de Basec da zona pode ser usada, por exemplo referem por favor o seguinte:

Nota:

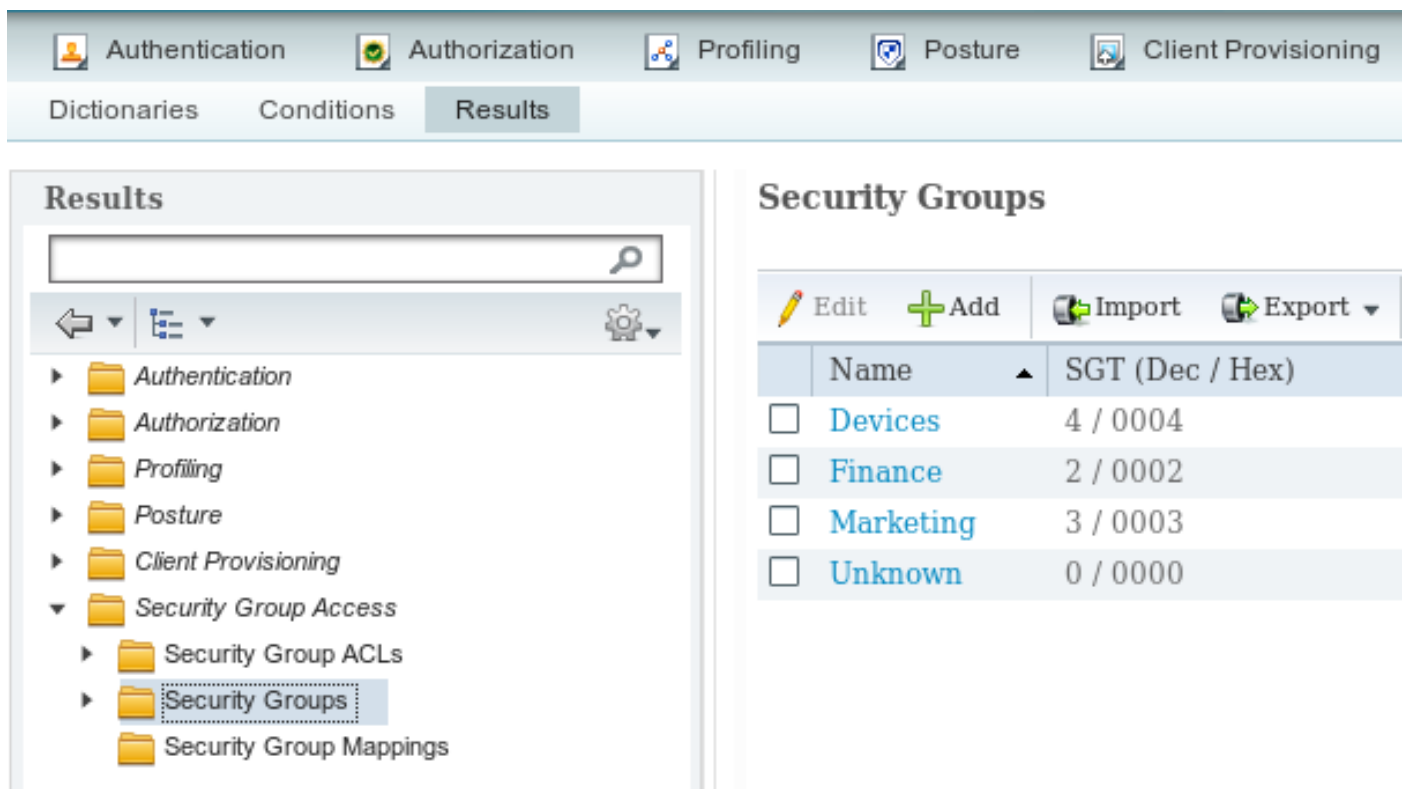
O ASA podia ter o tráfego de controlo SGACL que vem do usuário remoto VPN. Para simplificar a encenação não foi apresentado neste artigo. Por exemplo refira o seguinte:

[Exemplo de configuração da classificação e da aplicação da versão ASA 9.2 VPN SGT](#)

## ISE - Passos de configuração

### 1. SGT para a finança e o mercado

*Da política - > resultados - acesso do grupo do > segurança - os grupos do > segurança criam SGT para a finança e o mercado:*



The screenshot displays the ISE configuration interface. At the top, there are 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 search bar and navigation icons. On the left, a tree view shows the configuration hierarchy, with Security Groups selected. On the right, the Security Groups table is visible, listing groups and their corresponding SGT values.

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. Grupo de segurança ACL para o mercado do tráfego - >Finance

*Da política - > resultados - acesso do grupo do > segurança - o grupo ACL do > segurança cria o ACL que será usado ao tráfego de controle do mercado para financiar. Somente tcp/445 é permitido:*

The screenshot displays a network management interface with a top navigation bar containing icons and labels for Authentication, Authorization, Profiling, Posture, and Client Provisioning. Below this, a secondary bar shows 'Dictionaries', 'Conditions', and 'Results' tabs, with 'Results' being the active tab.

The main content area is divided into two sections. On the left, a 'Results' sidebar features a search bar and a tree view of configuration categories: Authentication, Authorization, Profiling, Posture, Client Provisioning, Security Group Access (expanded), Security Group ACLs (selected), Security Groups, and Security Group Mappings.

The right section, titled 'Security Groups ACLs List > telnet445', shows the configuration for a specific ACL. It includes a 'Name' field with the value 'telnet445', a 'Description' field, and an 'IP Version' section with radio buttons for IPv4 (selected), IPv6, and IPv4. Below this, the 'Security Group ACL content' field contains the text 'permit tcp dst eq 445'.

### 3. ACL obrigatório na matriz

*Da política - > política de saída - > matriz ACL configurado ligamento para a fonte: Mercado e destino: Finança. O anexo igualmente nega o IP como o último ACL para deixar cair todo tráfego restante (sem essa política padrão será anexado, padrão é licença alguma).*

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 da autorização para o acesso VPN que atribui SGT = 3 (mercado)

Da política - > a autorização cria uma regra para o acesso remoto VPN. Todas as conexões de VPN estabelecidas através do cliente de AnyConnect 4.x obterão o acesso direto (PermitAccess) e serão atribuídas a etiqueta 3 SGT (mercado). A circunstância está usando a identidade Extentions de AnyConnect ([ACIDEX](#))

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

#### 5. Regra da autorização para o acesso do 802.1x que atribui SGT = 2 (finança)

Da política - > a autorização cria uma regra para o acesso do 802.1x. O suplicante que termina a sessão do 802.1x no 3750 Switch com username Cisco obterá o acesso direto (PermitAccess) e será atribuído a etiqueta 2 SGT (finança).

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 o dispositivo de rede, gerando o PAC para o ASA

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

Isso pode ser configurado da *administração* - > *dispositivos de rede*. Depois que o ASA é adicionado enrola para baixo ajustes de TrustSec e gerencia o PAC:

x

### 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

O Switches (3750X) apoia o abastecimento automático PAC - de modo que as etapas precisam de ser executadas somente para o ASA que apoia somente o abastecimento manual PAC.

## 7. Adicionando o dispositivo de rede, configurando o segredo para o abastecimento automático do interruptor PAC

Para o interruptor usar o segredo correto automático do abastecimento PAC apenas deve ser ajustada:

▼ Advanced TrustSec Settings

▼ Device Authentication Settings

Use Device ID for SGA Identification

Device Id

\* Password

Nota:

O PAC é usado para autenticar ao ISE e para transferir os dados do ambiente (por exemplo SGT) junto com a política (ACL). O ASA apoia somente dados do ambiente - as políticas precisam de ser configuradas manualmente no ASA. Suportes de IOS ambos - assim as políticas podem ser transferidas do ISE.

## ASA - Passos de configuração

### 1. Acesso básico VPN

Configurar o acesso básico SSL VPN para AnyConnect usando o ISE para a autenticação

```
Rule name: 802.1x
```

```
Condition: Radius:User-Name EQUALS cisco AND Radius:NAS-IP-Address EQUALS 192.168.1.10
```

```
Permissions: PermitAccess ANDFinance
```

### 2. Importe o PAC e permita cts

Importe o PAC gerado para o ASA (de Step6 da configuração ISE). Use 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  
25301ffffa98935ae5d219b9588bcb6656799917d2ade088c0a7e653ea1dca530e24274  
4366ed375488c4ccc3d64c78a7fc8c62c148ceb58fad0b07d7222a2c02549179dbf2a7  
4d4013e8fe
```

Permita 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
25301ffffa98935ae5d219b9588bcb6656799917d2ade088c0a7e653ea1dca530e24274
4366ed375488c4ccc3d64c78a7fc8c62c148ceb58fad0b07d7222a2c02549179dbf2a7
4d4013e8fe
```

Após ter permitido cts o ASA deve transferir 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 a finança do tráfego - > mercado

Configurar SGACL na interface interna. Esse ACL reservará iniciar somente o tráfego ICMP da finança ao mercado.

```
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 etiqueta para numerar:

```
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. Permita cts na interface interna

Após ter permitido 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 poderá enviar e receber os quadros de TrustSec (frames da Ethernet com campo do CMD). O ASA suporá que todos os quadros do ingresso sem uma etiqueta devem ser tratados como com a etiqueta 100. Todos os quadros do ingresso que já incluem a etiqueta serão confiados.

## Etapas da configuração de switch

### 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 depois que bem sucedido a autorização do 802.1x o usuário (autorizado através do ISE) deve ser atribuída a etiqueta 2 (finança).

## 2. Configuração e abastecimento CTS

Similarmente quanto para aos cts ASA é configurado e ponto ao ISE:

```
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
```

A aplicação é permitida igualmente para Layer3 e Layer2 (todos os vlans):

```
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
```

Para provision automaticamente o PAC:

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

Outra vez a senha deve combinar a configuração correspondente em ISE (dispositivo de rede - > interruptor - > TrustSec). Agora os IO iniciarão a sessão EAP-FAST com ISE para obter o PAC. Mais detalhe nesse processo pode ser encontrado aqui:

[O ASA e o exemplo de configuração de TrustSec do Catalyst 3750X Series Switch e pesquisam defeitos o guia](#)

Para verificar se o PAC é instalado:

```
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  
089E5B7CBB22A0D4BCEEF80F826A180B5227EAACBD07709DBDCD3CB42AA9F996829AE46F
```

```
Refresh timer is set for 4y14w
```

### 3. Permita cts na relação ao ASA

```
interface GigabitEthernet1/0/39
```

```
switchport access vlan 10
```

```
switchport mode access
```

```
cts manual
```

```
policy static sgt 101 trusted
```

A partir de agora o interruptor deve estar pronto para processar e enviar quadros de TrustSec e para reforçar as políticas transferidas do ISE.

## Troubleshooting

### Atribuição SGT

Depois que a sessão de VPN ao ASA é estabelecida a atribuição correta SGT 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
```

Conforme regras da autorização no ISE todos os usuários AnyConnect4 foram atribuídos à etiqueta do mercado.

O mesmos com sessão do 802.1x no interruptor. Depois que o interruptor da autenticação dos revestimentos de AnyConnect NAM aplicará a etiqueta correta retornada do ISE:

```
bsns-3750-5#show authentication sessions interface gi1/0/2 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
<b>dot1x</b>	<b>Authc Success</b>
mab	Stopped

Conforme a autorização ordena no ISE que todos os usuários conectados a esse interruptor deve ser atribuído a SGT = 2 (finança).

## Aplicação no ASA

Quando tentar enviar um tráfego da finança (192.168.1.203) a introduzi-lo no mercado (192.168.100.50) baterá a interface interna do ASA. Para a requisição de eco ICMP criará 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 aumente os contadores 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 pode igualmente ser confirmado olhando capturas de pacote de informação. Observe por favor que as etiquetas corretas estão indicadas:

```
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 requisição de eco ICMP entrante etiquetada com SGT = 2 (finança) e então uma resposta do usuário VPN que é etiquetado pelo ASA com SGT = 3 (mercado). Uma outra ferramenta de Troubleshooting - o pacote-projétil luminoso é igualmente TrustSec pronto.

Infelizmente o 802.1x PC não vê essa resposta porque obstruiu por RBACL apátrida no interruptor (explicação na próxima seção).

Uma outra ferramenta de Troubleshooting - o pacote-projétil luminoso é igualmente TrustSec pronto. Deixe-nos confirmar se o pacote ICMP entrante da finança será aceitado:

```
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**

Deixe-nos igualmente tentar iniciar toda a conexão de TCP da finança ao mercado, isso deve ser obstruído 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]
```

## Comute a aplicação

Deixe-nos verificar se o interruptor transferiu políticas do ISE corretamente:

```
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 do mercado para financiar é instalada corretamente. Somente tcp/445 é permitido conforme 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
```

Aquela é a razão pela qual a resposta do eco ICMP que vem do mercado financeiro foi deixada cair. Isso pode ser confirmado verificando os contadores para ver se há o tráfego de SGT 3 a 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 deixados cair pelo hardware (o contador atual é 65 e aumento de cada 1 segundo).

Que se a conexão tcp/445 será iniciada do mercado?

O ASA permitirá aquele (aceita todo o tráfego VPN devido do “à conexão licença-VPN sysopt”):

```
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 será 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
```

E os IO aceitarão desde que combina telnet445 RBACL. Os contadores corretos serão aumentados:

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

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

Esse exemplo foi apresentado para que a finalidade mostre a diferença na configuração das políticas de TrustSec e a aplicação no ASA e nos IO. Por favor igualmente esteja ciente das diferenças das políticas IO transferidas de ISE (RBACL apátrida) e do Firewall baseado do stateful de TrustSec zona ciente.

## Referências

- [Postura da versão ASA 9.2.1 VPN com exemplo de configuração ISE](#)
- [O ASA e o exemplo de configuração de TrustSec do Catalyst 3750X Series Switch e](#)

pesquisam defeitos o guia

- [Guia de configuração de switch de Cisco TrustSec: Compreendendo Cisco TrustSec](#)
- [Configurando um servidor interno para a autorização de usuário da ferramenta de segurança](#)
- [Guia de configuração de CLI da série VPN de Cisco ASA, 9.1](#)
- [Guia do Usuário do Cisco Identity Services Engine, liberação 1.2](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)