Configurar a colocação de etiquetas Inline ASA 9.3.1 TrustSec

Índice

Introdução

Este original 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 é executada pelo ASA com o uso do grupo de segurança que o Access Control List (SGACL) definiu localmente e o interruptor do ® do Cisco IOS que usa o papel baseou o Access Control List (RBACL) transferido do Identity Services Engine (ISE).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

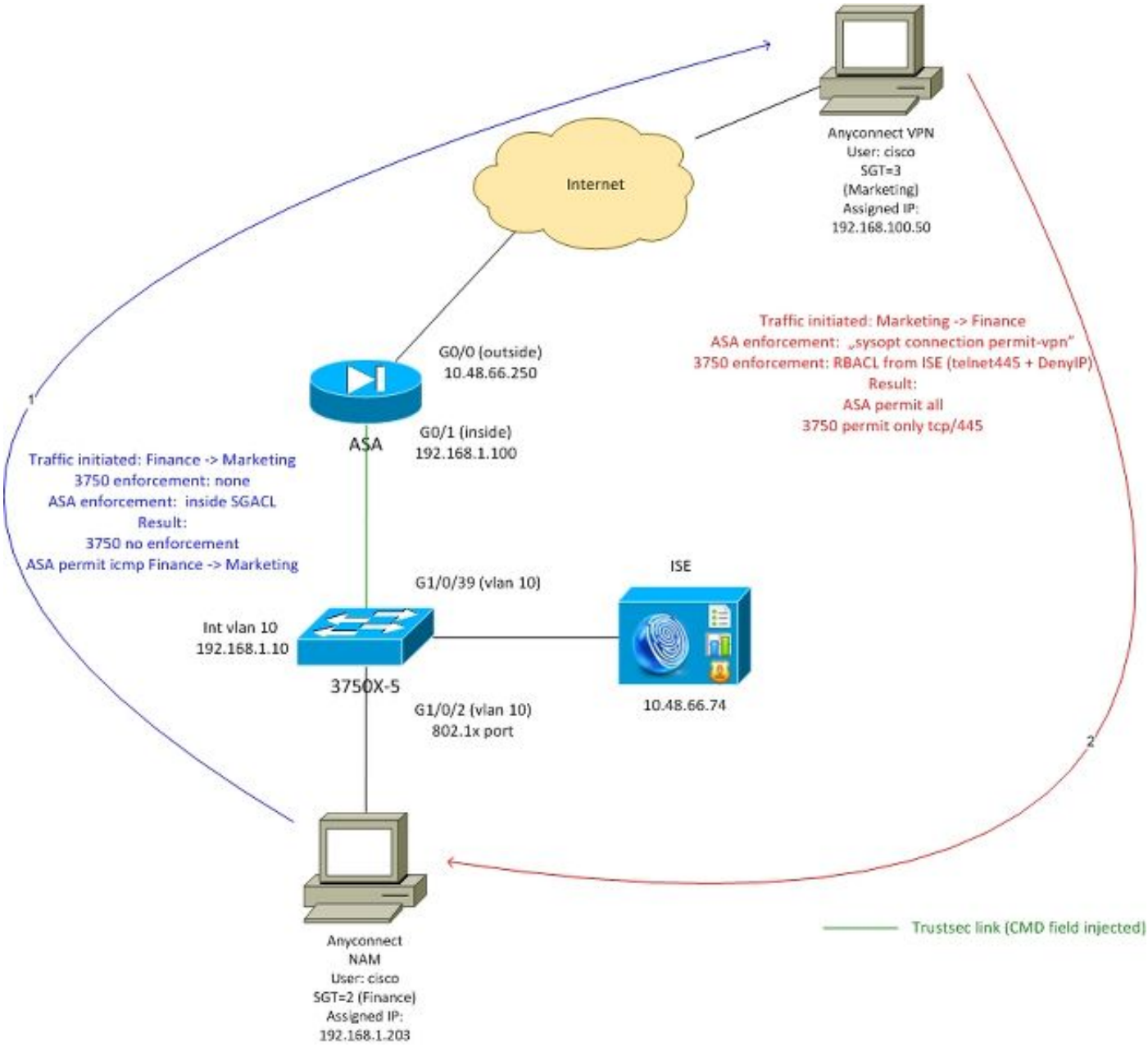
> **Note**: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

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 do grupo de segurança (SGT) que descreve a fonte do pacote.

O usuário remoto VPN termina a sessão de SSL no ASA e é atribuído 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 tem SGACL configurado na interface interna que permite o tráfego ICMP iniciado da finança ao mercado.

O ASA permite 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 o fluxo está criado uma vez, pacote de informação de retorno é aceitado automaticamente (baseado na inspeção).

O 3750 Switch usa RBACL a fim controlar o tráfego recebido do mercado para financiar.

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

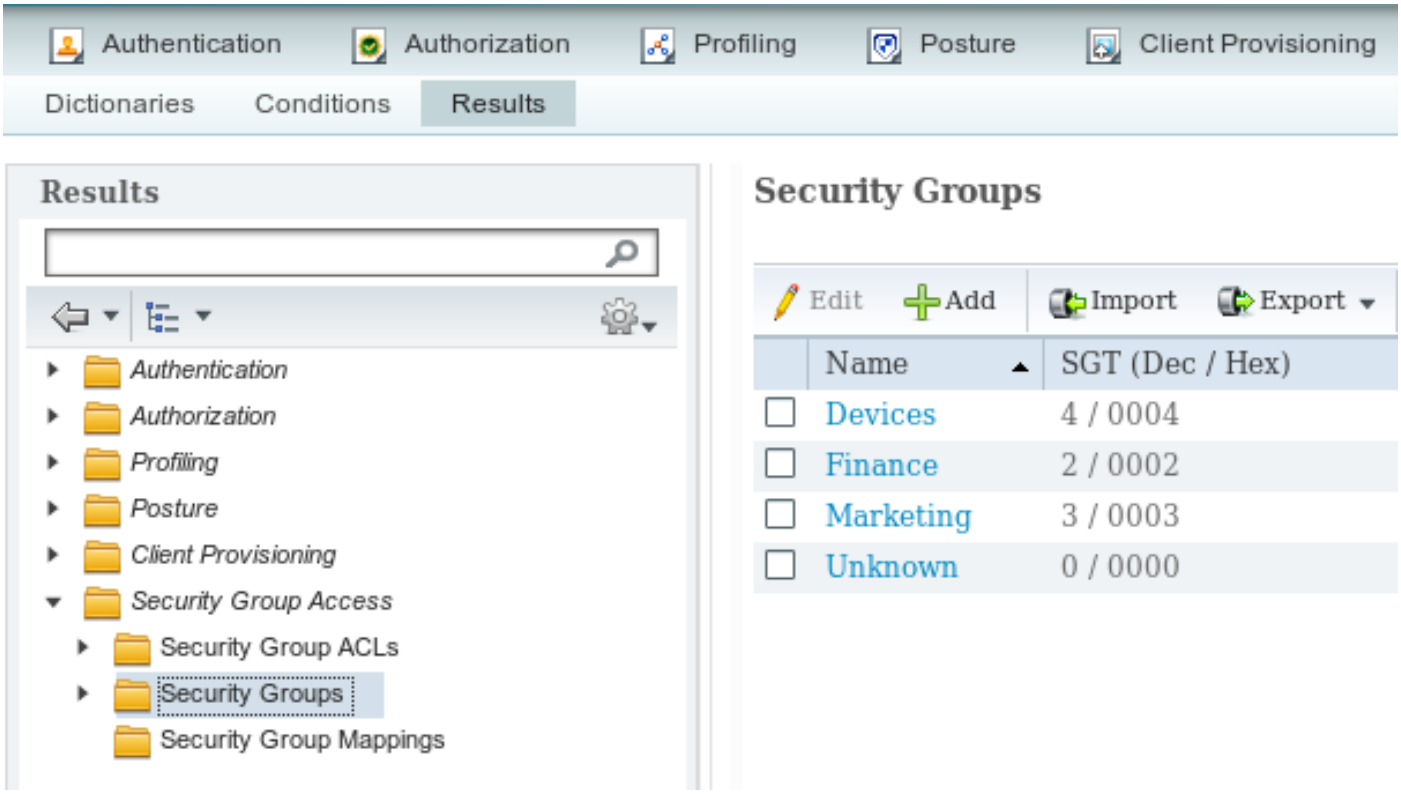
> **Note**: Para o firewall stateful ciente de Trustsec no Firewall baseado zona do ® do Cisco IOS pode ser usado, por exemplo, consulte:

Note: O ASA poderia ter o tráfego de controlo SGACL que vem do usuário remoto VPN. A fim simplificar a encenação, não foi apresentado neste artigo. Por exemplo consulte: [Classificação de SGT VPN ASA versão 9.2 e exemplo de configuração de aplicação]

ISE - Configuration Steps

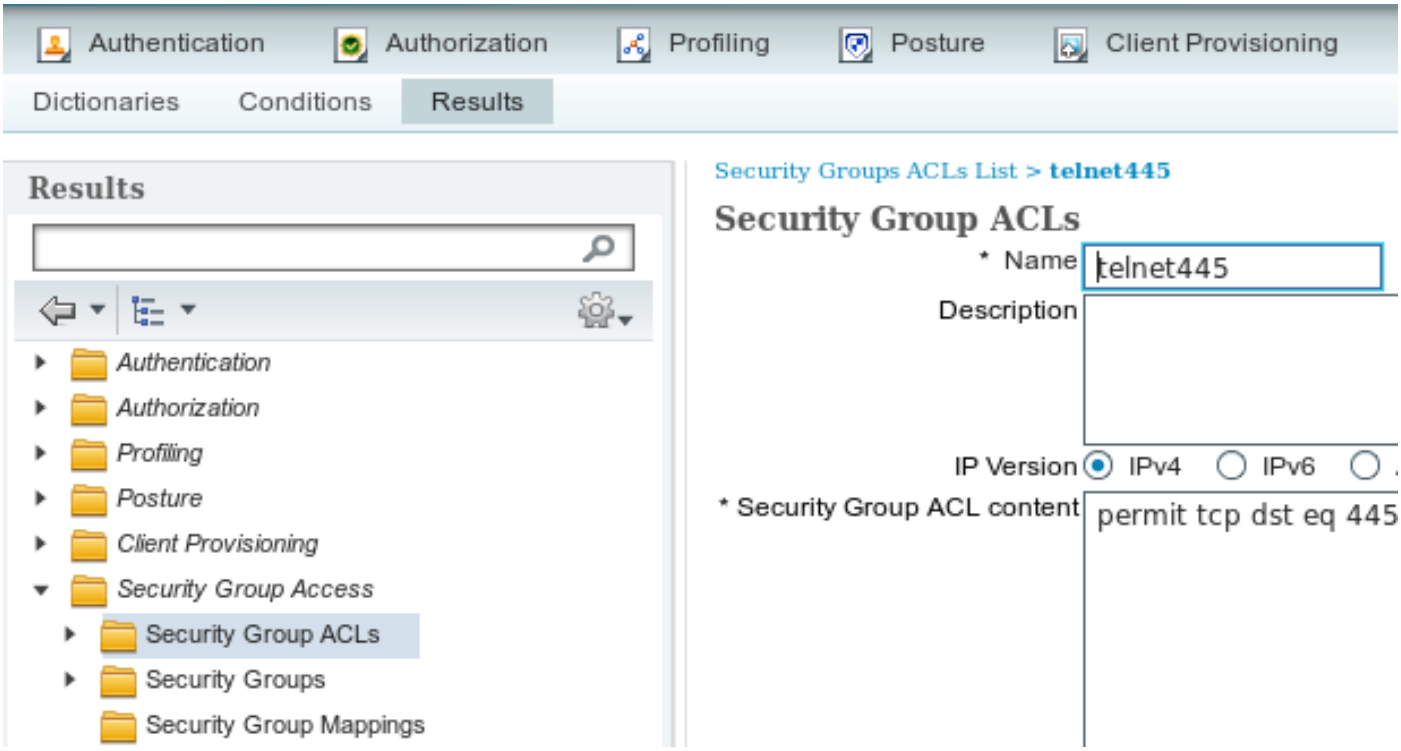
1. SGT para a finança e o mercado

Navegue **grupos do > segurança do acesso do grupo ao > segurança da política > dos resultados** e crie SGT para a finança e o mercado segundo as indicações desta imagem.



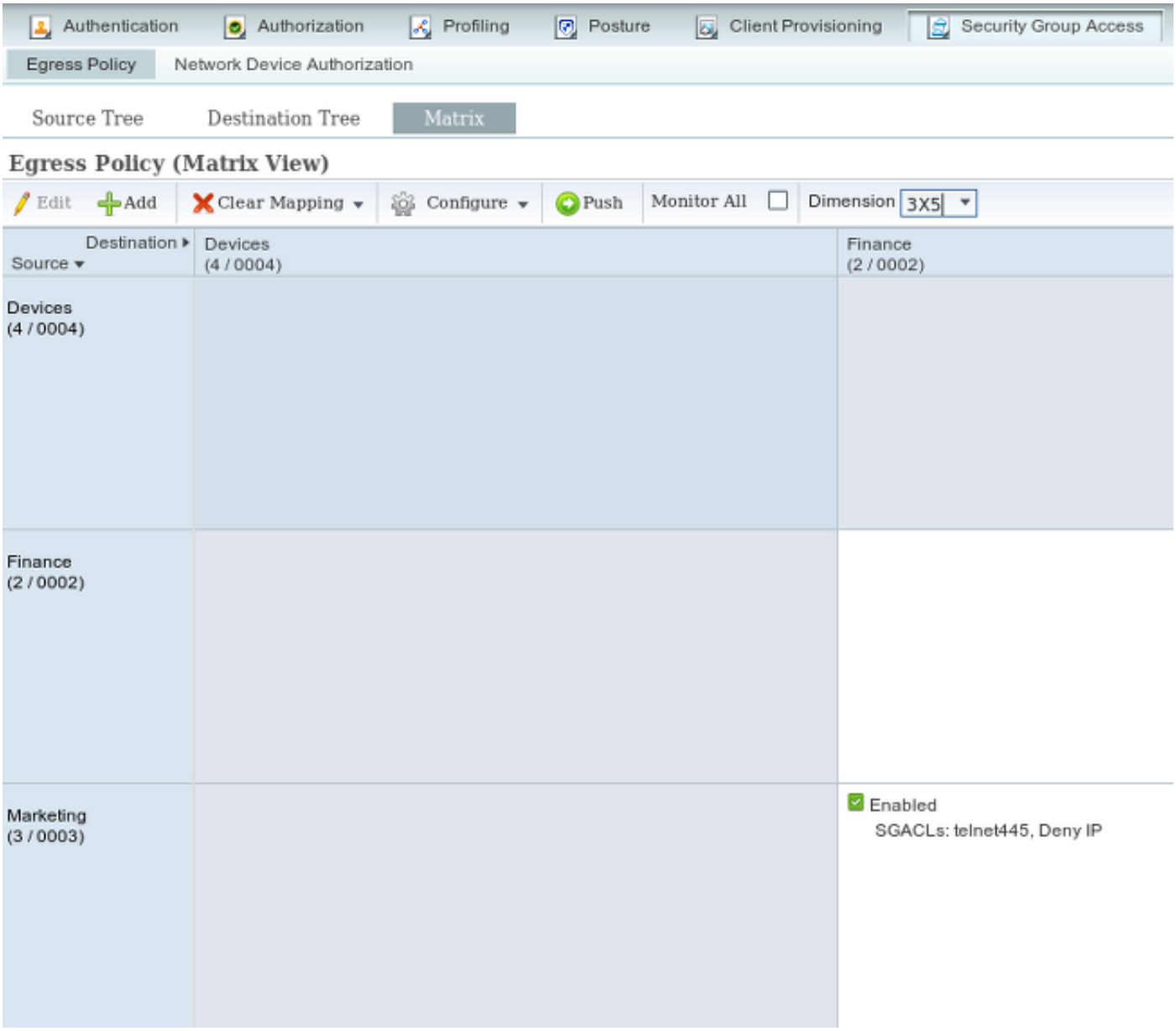
2. Grupo de segurança ACL para o mercado > a finança do tráfego

Navegue o **grupo ACL do > segurança do acesso do grupo ao > segurança da política > dos resultados** e crie o ACL que é usado ao tráfego de controle do mercado para financiar. Somente tcp/445 é permitido segundo as indicações desta imagem.



3. ACL obrigatório na matriz

Navegue à **política > à política de saída > à matriz** ACL configurado ligamento para a fonte: **Mercado** e destino: **Finança**. Igualmente o anexo **nega o IP** como o último ACL para deixar cair todo tráfego restante segundo as indicações da imagem. (sem essa política padrão será anexado, padrão é licença)



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

Navegue à **política > à autorização** e crie 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 é usar 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)

Navegue à **política > à autorização** e crie 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).

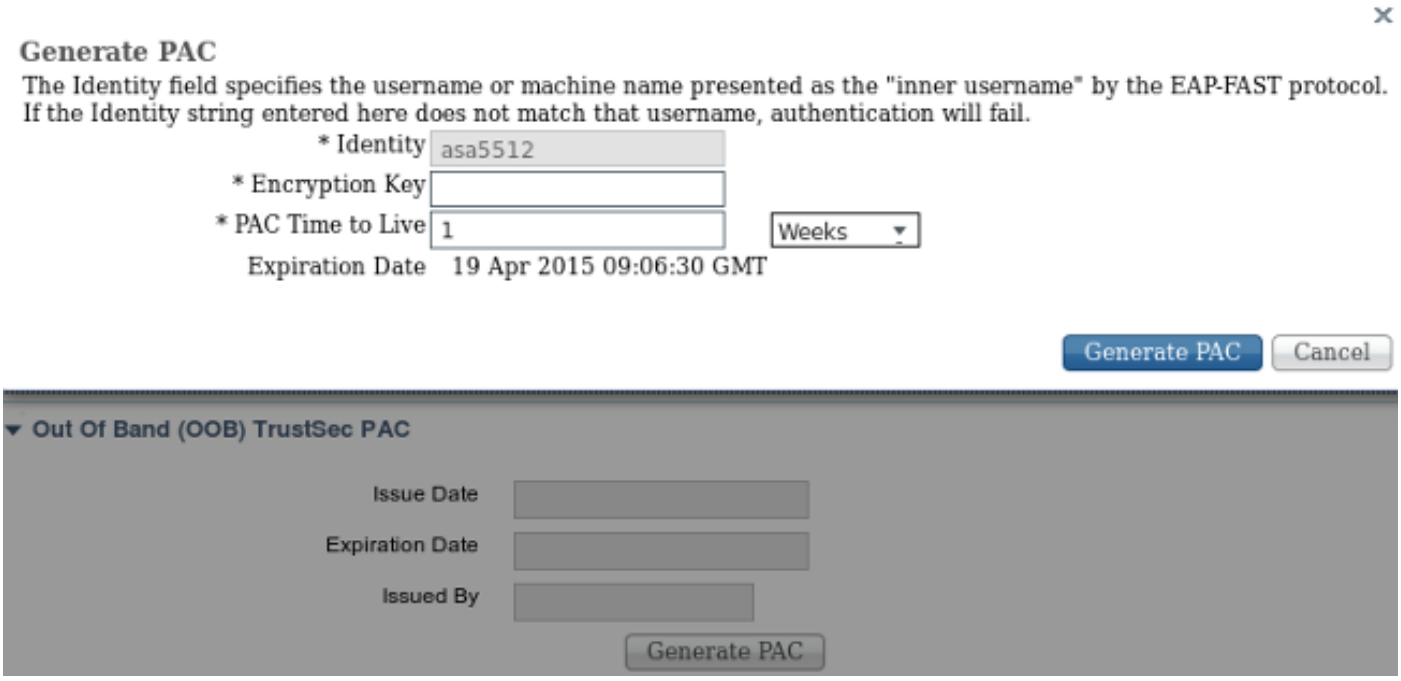
```
Rule name: 802.1x
```

```
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

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

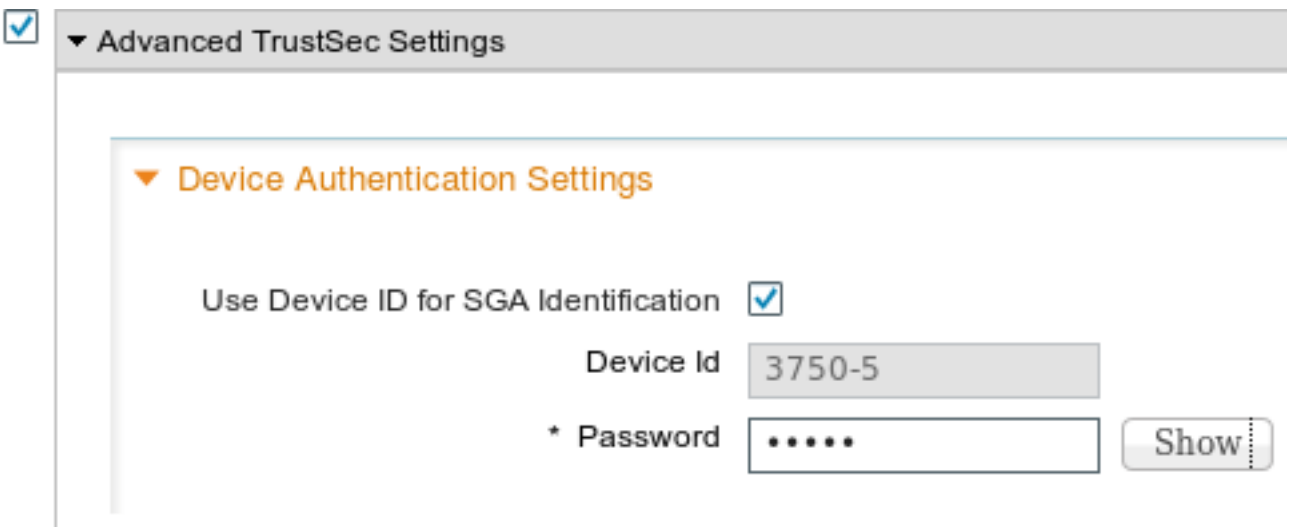
Isso pode ser configurado em **Administração > Dispositivos de Rede**. Depois que o ASA é adicionado, enrole para baixo **ajustes de TrustSec** e **gerencia o PAC** segundo as indicações desta imagem.



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

7. Adicionar o dispositivo de rede, configurar o segredo para o abastecimento automático do interruptor PAC

Para o interruptor que usa o abastecimento automático PAC, um segredo correto deve ser ajustado, segundo as indicações desta imagem.



Note: O PAC é usado para autenticar o ISE e transferir os dados do ambiente (por exemplo SGT) junto com a política (ACL). O ASA apoia somente dados do ambiente, políticas precisa de ser configurado manualmente no ASA. O ® do Cisco IOS apoia ambos, assim que as políticas podem ser transferidas do ISE.

ASA - Configuration Steps

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 AND Finance
```

2. Importe o PAC e permita cts

Importe o PAC gerado para o ASA (da etapa 6 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
```

A fim 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
```

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
   25301fffa98935ae5d219b9588bcb6656799917d2ade088c0a7e653ea1dca530e24274
   4366ed375488c4ccc3d64c78a7fc8c62c148ceb58fad0b07d7222a2c02549179dbf2a7
   4d4013e8fe
```

Depois que você permite 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 > o mercado do tráfego

Configurar SGACL na interface interna. O ACL reserva 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

Depois que você permite 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 os quadros de TrustSec (frames da Ethernet com campo do CMD). O ASA supõe 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 ao ASA, os cts são configurados 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
```

Também, a aplicação é permitida 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
```

A fim provision automaticamente o PAC:

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

Além disso, a senha deve combinar com a configuração correspondente em ISE (**dispositivo de rede > switch> TrustSec**). Agora, o ® do Cisco IOS inicia a sessão EAP-FAST com ISE a fim obter o PAC. Mais detalhe nesse processo pode ser encontrado aqui:

Exemplo de configuração do TrustSec com ASA e o switch Catalyst 3750-X Series e Guia de solução de problemas

A fim 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:
000200B000030001000400010EA48096688D96EF7B94C679A17BDAD6F000600940003010036 5AB3133998C86C1BA1B418
968C6069000001355261CCC00093A808F8A81F3F8C99A7CB83A8C3BFC4D573212C61CDCEB37ED279D683EE0DA60D86D
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.

Verificar

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

A verificação é coberta em seções individuais deste original.

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 a autorização ordena no ISE, todos os usuários AnyConnect4 foi atribuído à etiqueta do mercado.

O mesmos com sessão do 802.1x no interruptor. Depois que os revestimentos do módulo Network Analysis Modules de AnyConnect (NAM), interruptor da autenticação aplicarão a etiqueta 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
```

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

Aplicação no ASA

Quando você tentar enviar um tráfego da finança (192.168.1.203) ao mercado (192.168.100.50), bate a interface interna do ASA. Para a requisição de eco ICMP, 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 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. Note 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, 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, 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 financiar 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 é iniciada do mercado?

O ASA concede que (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 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
```

E, o ® do Cisco IOS aceita-a desde que combina telnet445 RBACL. Os aumentos corretos dos contadores:

```
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.

Este exemplo é apresentado de propósito a fim mostrar a diferença na configuração das políticas de TrustSec e a aplicação no ® ASA e de Cisco IOS. Esteja ciente das diferenças das políticas do ® do Cisco IOS transferidas de ISE (RBACL apátrida) e do Firewall baseado do stateful de TrustSec zona ciente.

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