ASA 9.3.1 TrustSec встроенная маркировка - пример конфигурации

Содержание

Введение

Этот документ описывает, как использовать функцию, внедренную в Выпуске 9.3.1 Устройства адаптивной защиты (ASA) - TrustSec Встроенная Маркировка. Та функция позволяет ASA принимать кадры TrustSec, а также передавать им. Таким образом, ASA может быть легко интегрирован в домене TrustSec без потребности использовать протокол обмена TrustSec SGT (SXP).

Данный пример представляет удаленного пользователя VPN, которые были назначенной меткой тега группы безопасности (SGT) = 3 (Маркетинг) и пользователь 802.1x, которые были назначенной меткой SGT = 2 (Финансы). Осуществление трафика будет выполнено и ASA с помощью Списка контроля доступа группы безопасности (SGACL), определенного локально и коммутатором IOS с помощью Роли базирующегося списка контроля доступа (RBACL), загруженной от платформы Identity Services Engine (ISE).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Базовые знания о конфигурации VPN Настройки интерфейса командной строки ASA и Протокола SSL
- Базовые знания о конфигурации VPN для удаленного доступа на ASA
- Базовые знания о платформе Identity Services Engine (ISE) и сервисах TrustSec

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения:

- Программное обеспечение Cisco ASA, Версия 9.3.1 и позже
- Аппаратные средства Cisco ASA 55x5 или ASAv.
- Windows 7 с защищенным мобильным клиентом Cisco AnyConnect Secure Mobility, выпуском 3.1
- Cisco Catalyst 3750X переключается с программным обеспечением 15.0.2 и позже
- Cisco ISE, Выпуск 1.2 и позже

Настройка

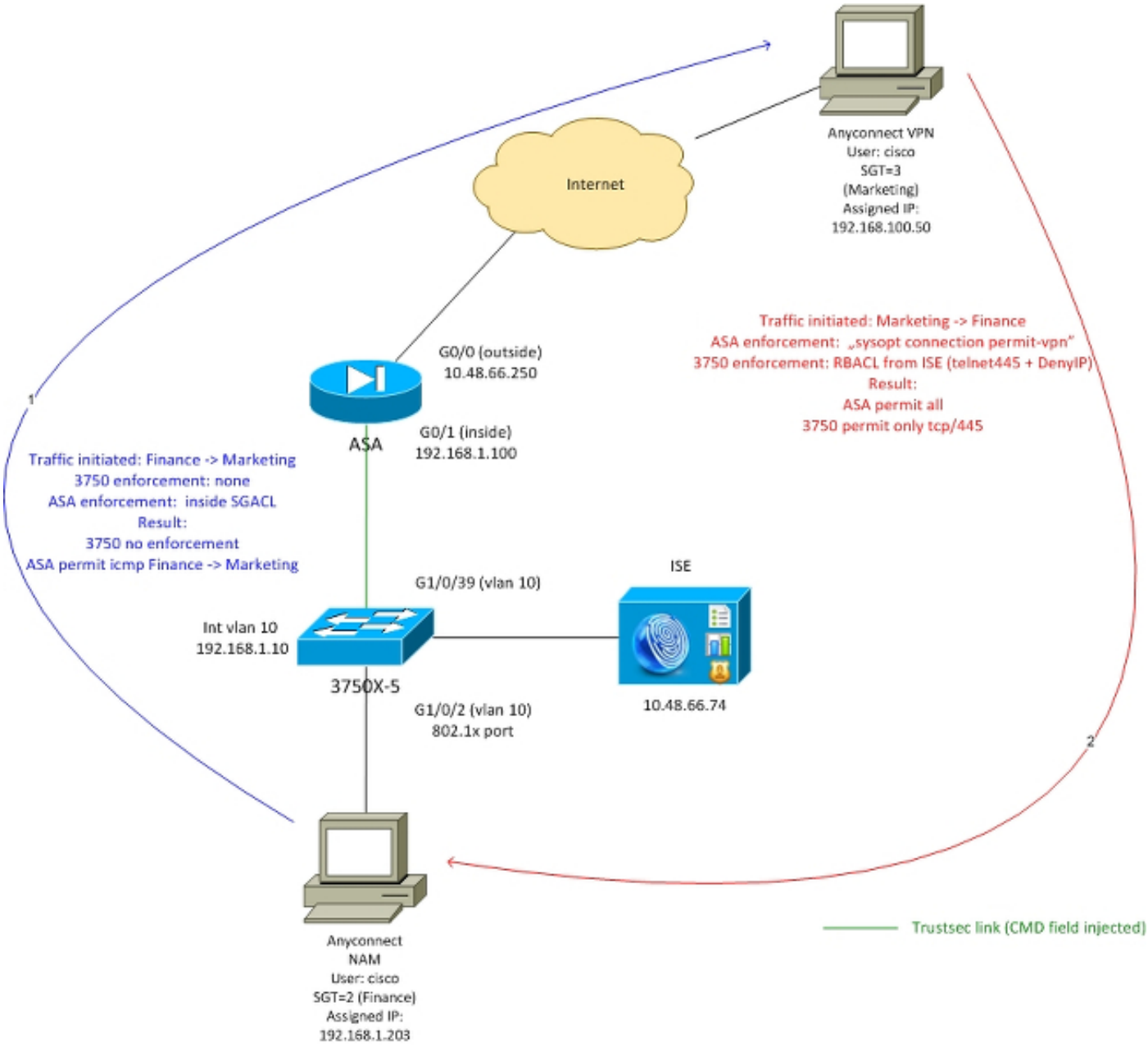
> **Примечание:** Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

Соединение между ASA и 3750X настроено для руководства cts. Это означает, что оба устройства могут передать и получить модифицируемые Фреймы Ethernet с Полем метаданных Cisco (cmd). То поле включает метку SGT, описывающую источник пакета.

Удаленный пользователь VPN завершает сеанс SSL на ASA, и назначил метку SGT 3 (Маркетинг).

Локальный корпоративный пользователь 802.1x после успешной аутентификации был назначен, SGT помечает 2 (Финансы).



ASA имеет SGACL, настроенный на внутреннем интерфейсе, обеспечивая трафик ICMP, инициируемый от Финансов до Маркетинга.

ASA разрешит, чтобы весь трафик инициировал от, удаляют пользователя VPN (из-за конфигурации "sysopt connection permit-vpn").

SGACL на ASA с отслеживанием состояния - что означает, что, как только поток является созданным возвращаемым пакетом, принят автоматически (на основе incpection).

3750 коммутаторов используют RBACL для контрольного трафика, полученного от Маркетинга для Финансирования.

RBACL является не сохраняющим состояние - что означает, что каждый пакет проверен - но осуществление TrustSec на 3750X платформа выполнено в назначении. Таким образом, коммутатор ответственен за осуществление трафика от Маркетинга для Финансирования.

Примечание:

Для осведомленного самонастраивающегося межсетевого экрана Trustsec на Зоне IOS

Межсетевой экран Basec может использоваться, Например см. придерживающееся:

Примечание:

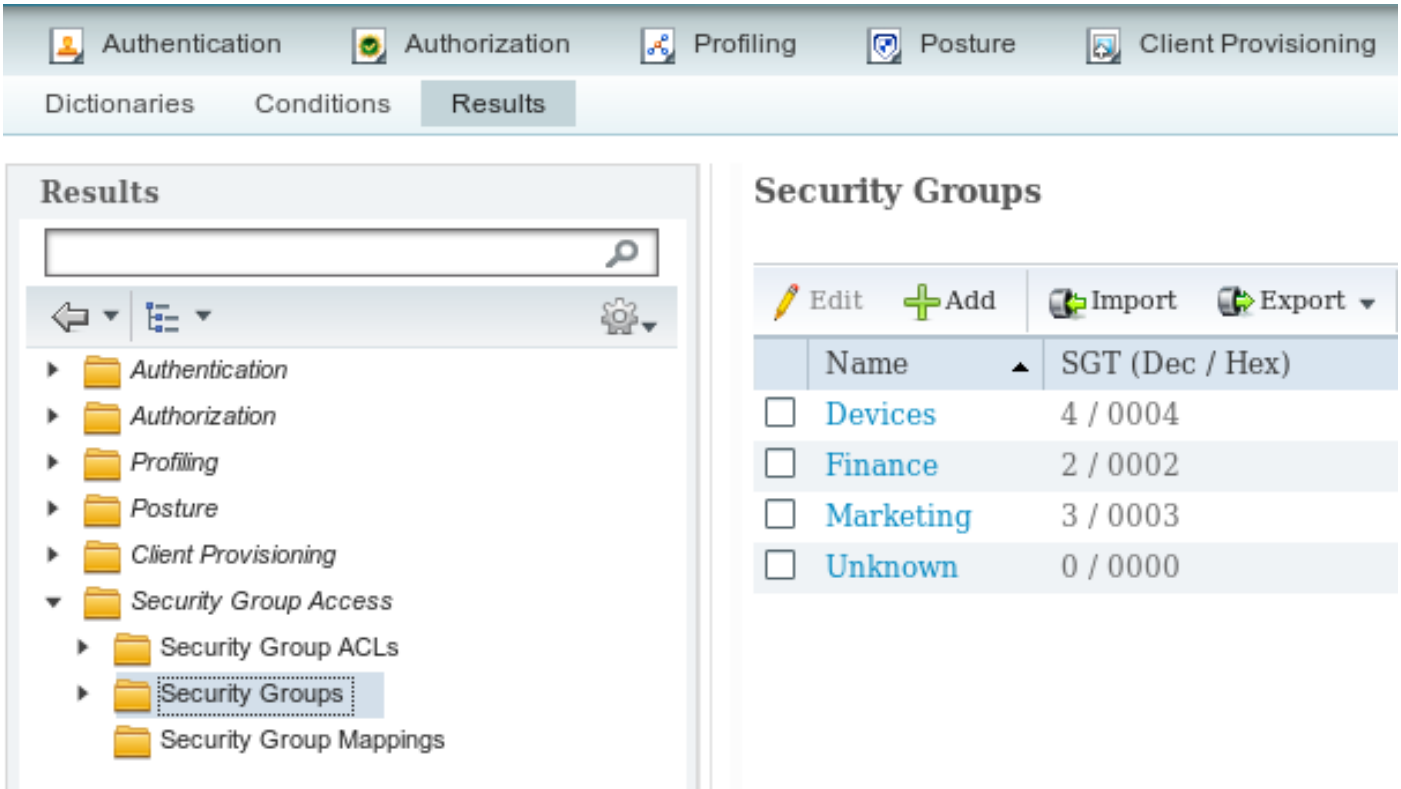
ASA мог иметь SGACL управление трафиком, прибывающим от удаленного пользователя VPN. Для упрощения сценария, это не было представлено в этой статье. Например, обратитесь к придерживающемуся:

[VPN версии ASA 9.2 классификация SGT и пример конфигурации осуществления]

ISE - действия настройки

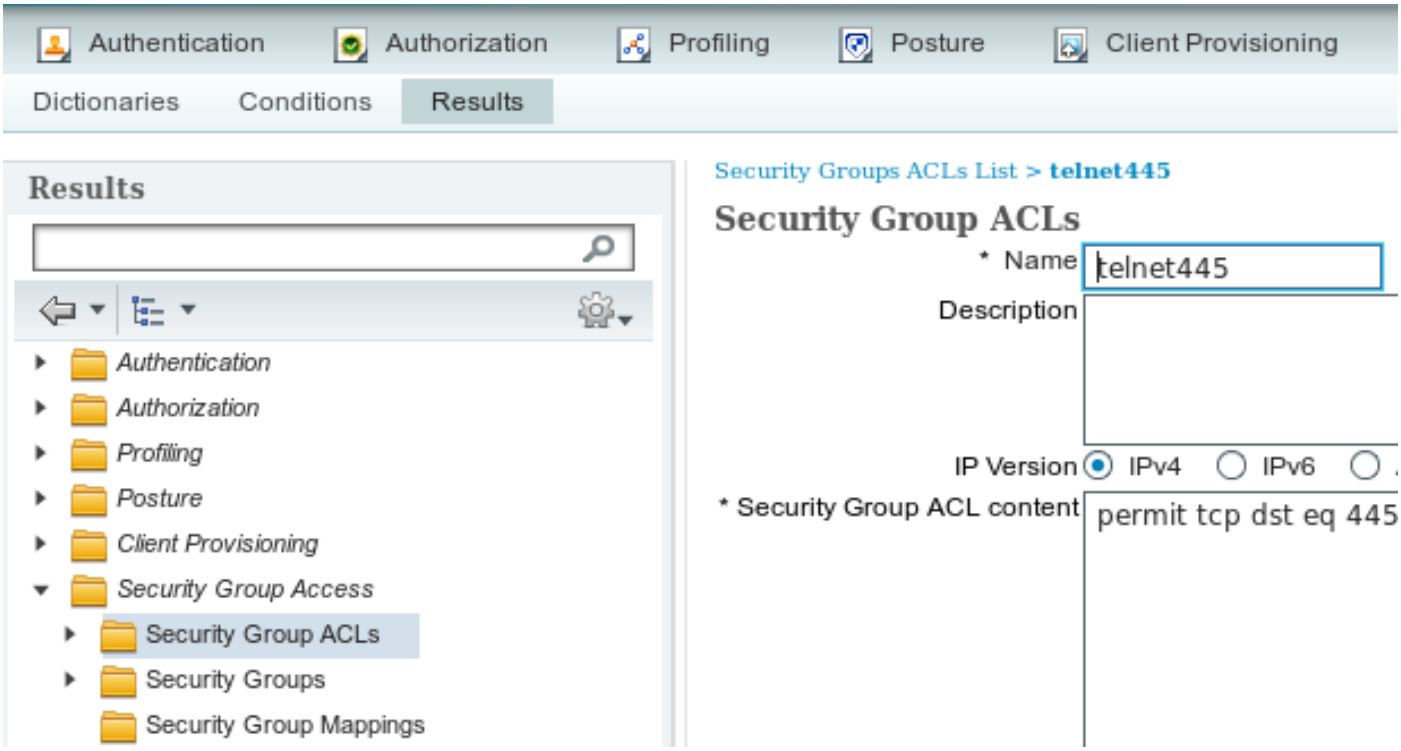
1. SGT для финансов и маркетинга

От *Политики-> Результаты-> Security Групповой доступ - Группы> Security* создают SGT для Финансов и Маркетинга:



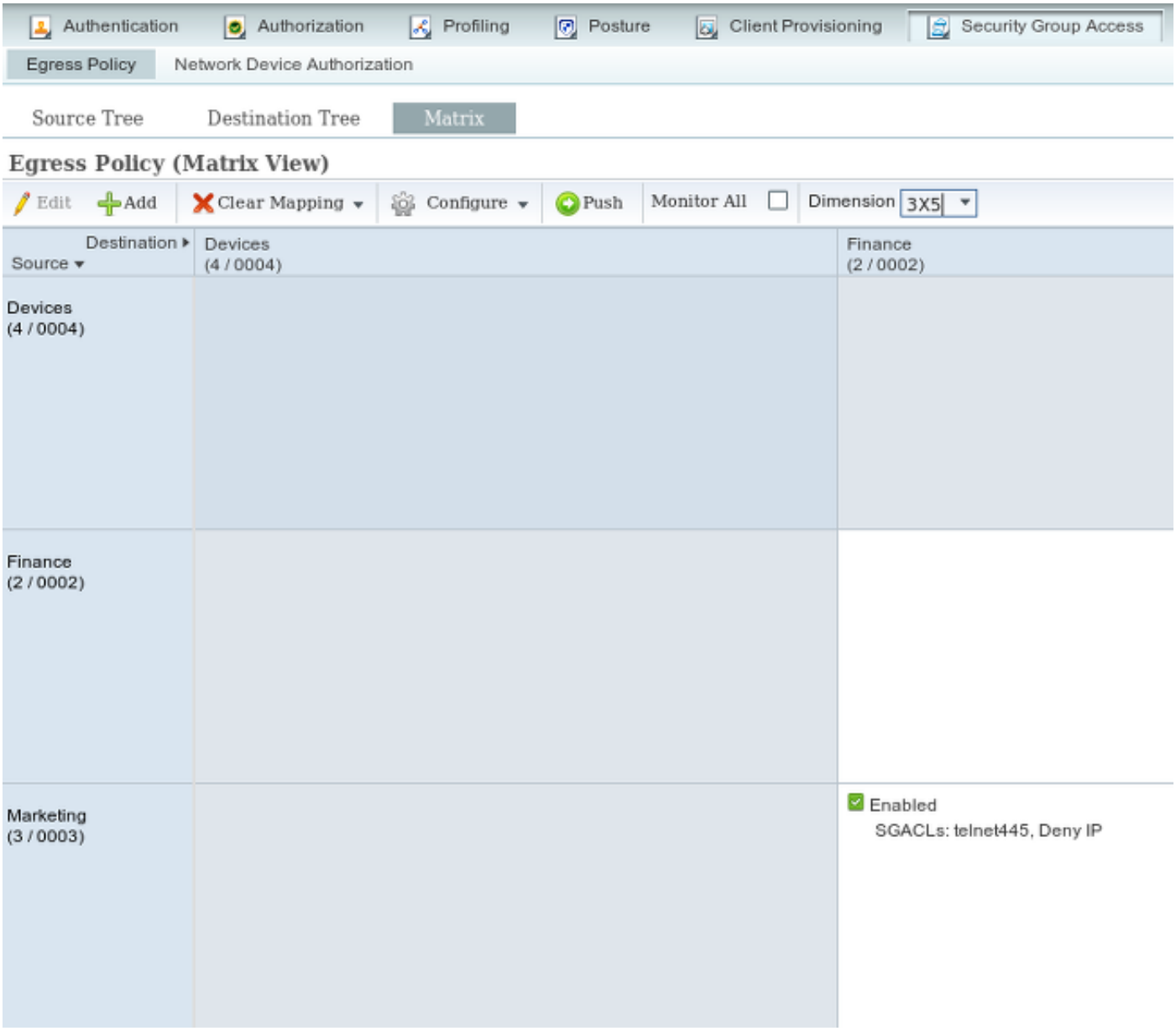
2. ACL группы безопасности для Маркетинга трафика-> Финансы

От *Политики-> Результаты-> Security Групповой доступ - ACL Группы> Security* создает ACL, который будет использоваться к контрольному трафику от Маркетинга для Финансирования. Только tcp/445 позволен:



3. Обязательный ACL в матрице

От *Политики-> Выходная политика-> Матрица* связывают настроенный ACL для Источника: Маркетинг и Назначение: Финансы. Присоединение также Запрещает, что IP как последний ACL понижается, весь другой трафик (без той политики по умолчанию будет подключен, по умолчанию является разрешением любой).



4. Правило авторизации для доступа VPN, назначающего SGT = 3 (Маркетинг)

От *Политики-> Авторизация* создают правило для удаленного доступа VPN. Все VPN-подключения установили через AnyConnect 4.x, клиент получит полный доступ (PermitAccess) и будет назначен, SGT помечает 3 (Маркетинг). Условие использует Идентификационные Расширения AnyConnect (ACIDEX)

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

5. Правило авторизации для доступа 802.1x, назначающего SGT = 2 (Финансы)

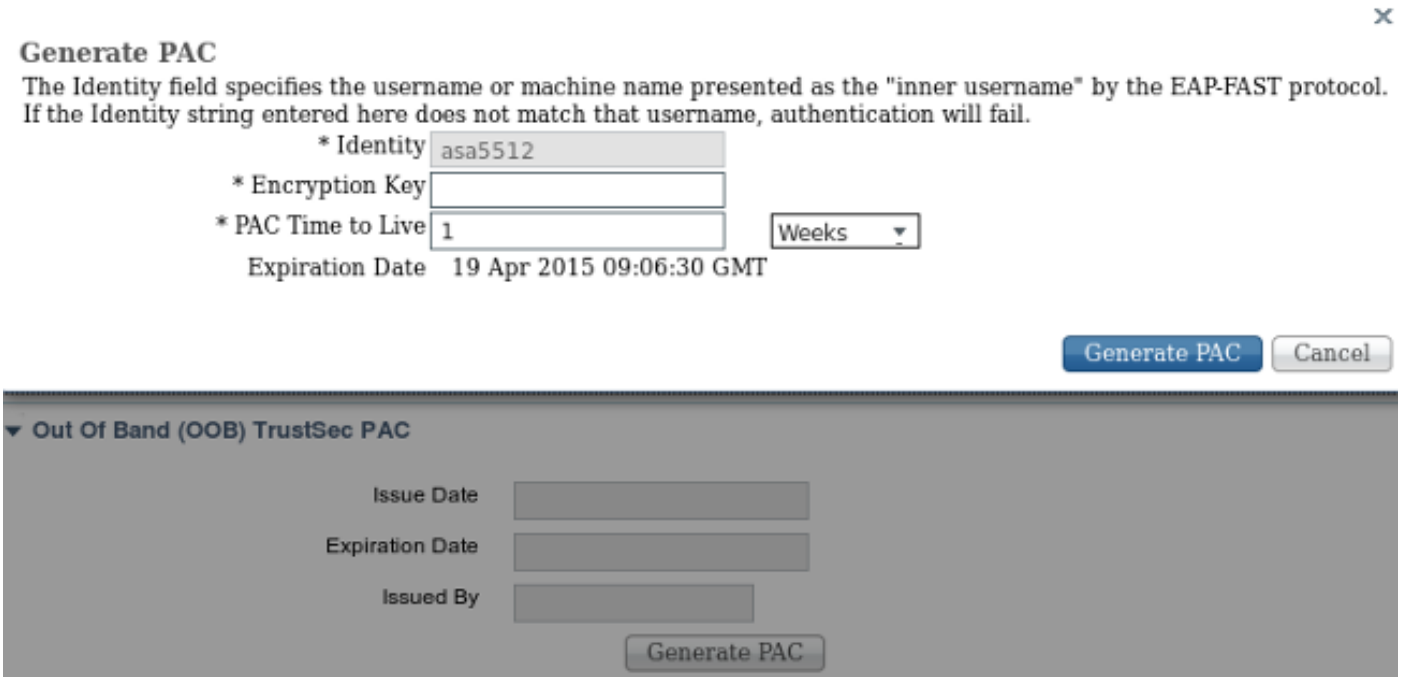
От *Политики-> Авторизация* создают правило для доступа 802.1x. Соискатель, завершающий сеанс 802.1x на 3750 коммутаторах с именем пользователя cisco, получит полный доступ (PermitAccess) и будет назначен, SGT помечает 2 (Финансы).

```
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. Добавление сетевого устройства, генерируя PAC для ASA

Для добавления ASA к домену TrustSec, необходимо генерировать файл PAC вручную. Тот файл будет импортирован на ASA.

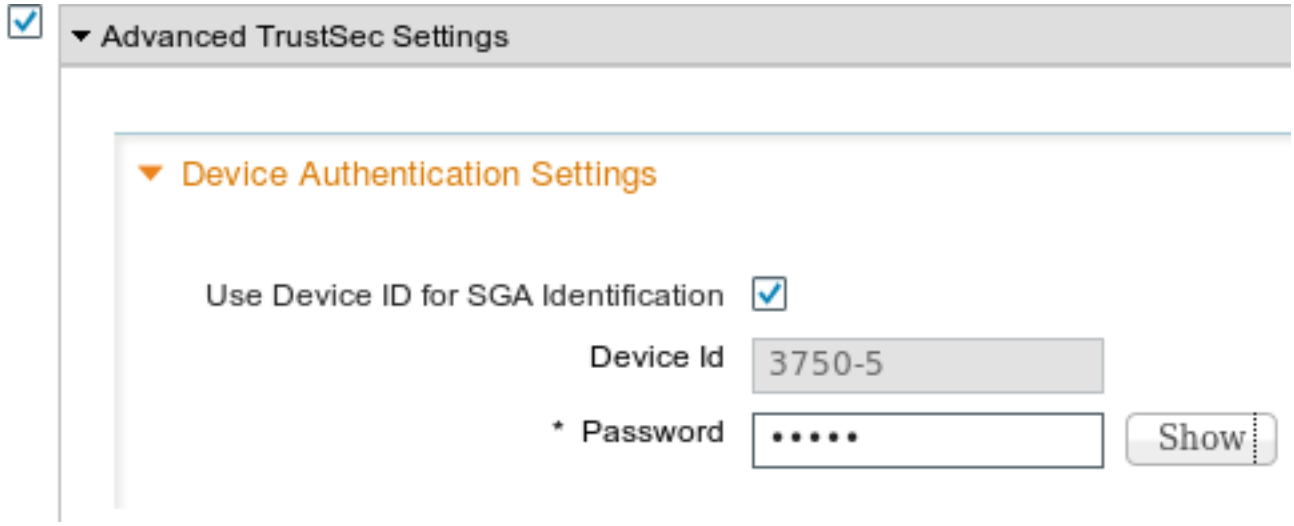
Это может быть настроено от *администрирования-> Сетевые устройства.* После того, как ASA добавлен, прокручивают вниз к параметрам настройки TrustSec и генерируют PAC:



Коммутаторы (3750X) поддерживают автоматическую инициализацию PAC - так, чтобы шаги были выполнены только для ASA, который поддерживает только ручную инициализацию PAC.

7. Добавление сетевого устройства, настраивая тайну для коммутатора автоматическая инициализация PAC

Для коммутатора с помощью автоматического PAC, настраивающего просто корректную тайну, должен быть установлен:



Примечание:

PAC используется для аутентификации на ISE и данных среды загрузки (например, SGT) наряду с политикой (ACL). ASA поддерживает только данные среды - политика должна быть вручную настроена на ASA. Поддержки IOS оба - так политика могут быть загружены от ISE.

ASA - действия настройки

1. Основной доступ VPN

Настройте основной доступ VPN SSL для AnyConnect с помощью ISE для аутентификации

```
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. PAC импорта и включает cts

PAC импорта, генерируемый для ASA (от Step6 конфигурации ISE). Используйте тот же ключ шифрования:

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

'Для проверки:':

```
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:
   000200b000030000100040010c2dcb10f6e5474529815aed11ed981bc00060094000301
   007915dcb81032f2fdf04bfe938547fad2000000135523ecb300093a8089ee0193bb2c
   8bc5cfabf8bc7b9543161e6886ac27e5ba1208ce445018a6b07cc17688baf379d2f1f3
   25301fffa98935ae5d219b9588bcb6656799917d2ade088c0a7e653ea1dca530e24274
   4366ed375488c4ccc3d64c78a7fc8c62c148ceb58fad0b07d7222a2c02549179dbf2a7
   4d4013e8fe
```

Включите 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:
   000200b000030001000400 10c2dcb10f6e5474529815aed11ed981bc00060094000301
   007915dcb81032f2fdf04bfe938547fad2000000135523ecb300093a8089ee0193bb2c
   8bc5cfabf8bc7b9543161e6886ac27e5ba1208ce445018a6b07cc17688baf379d2f1f3
   25301fffa98935ae5d219b9588bcb6656799917d2ade088c0a7e653ea1dca530e24274
   4366ed375488c4ccc3d64c78a7fc8c62c148ceb58fad0b07d7222a2c02549179dbf2a7
   4d4013e8fe
```

После включения cts ASA должен загрузить данные среды от 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 для Финансов трафика-> Маркетинг

Настройте SGACL на внутреннем интерфейсе. Тот ACL позволит инициировать только трафик ICMP от Финансов до Маркетинга.

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

ASA должен развернуть название метки к номеру:

```
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. Включите cts на внутреннем интерфейсе

После включения cts на внутреннем интерфейсе 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
```

ASA будет в состоянии передать и принять кадры TrustSec (фреймы Ethernet с полем CMD). ASA предположит, что все входные кадры без метки должны рассматриваться как с меткой 100. Всем входным кадрам, которые уже включают метку, будут доверять.

Коммутатор - действия настройки

1. Основной 802.1x

```
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
```

С той конфигурацией после того, как успешная авторизация 802.1x, пользователю (авторизовавший через ISE) нужно назначить, помечает 2 (Финансы).

2. Конфигурация CTS и инициализация

Так же что касается ASA cts настроен и точка к 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
```

Также осуществление включено и для Layer3 и для Layer2 (весь 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
```

К PAC условия автоматически:

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

Снова пароль должен совпасть с соответствующей конфигурацией на ISE (Сетевое устройство-> Коммутатор-> TrustSec). Прямо сейчас IOS будет инициировать сеанс EAP-FAST с ISE для получения PAC. Больше подробности о том процессе может быть найдено здесь:

ASA и коммутатор Catalyst серии 3750X — пример конфигурации TrustSec и руководство по устранению неполадок

Проверить, установлен ли PAC:

```
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
968C6069000000135526 1CCC00093A808F8A81F3F8C99A7CB83A8C3BFC4D573212C61CDCEB37ED279D683EE0DA60D86D
5904C41701ACF07BE98B3B73C4275C98C19A1DD7E1D65E679F3E9D40662B409E58A9F139BAA3BA3818553152F28AE04B
089E5B7CBB22A0D4BCEEF80F826A180B5227EAACBD07709DBDCD3CB42AA9F996829AE46F
 Refresh timer is set for 4y14w
```

3. Включите cts на интерфейсе к ASA

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

С этого времени коммутатор должен быть готов обработать и передать кадры TrustSec и принудить политику, загруженную от ISE.

Устранение неполадок

Присвоение SGT

После того, как сеанс VPN к ASA установлен, корректное присвоение SGT должно быть подтверждено:

```
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
```

Согласно правилам авторизации на ISE все пользователи AnyConnect4 был назначен на Торгующую метку.

То же с 802.1x открывает сеанс на коммутаторе. После того, как NAM AnyConnect заканчивается, опознавательный коммутатор применится, корректная метка возвратилась из 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
```

Согласно правилам авторизации на ISE всех пользователей, связанных с тем коммутатором, нужно назначить на SGT = 2 (Финансы).

Осуществление на ASA

При попытке передать трафик от Финансов (192.168.1.203) к Маркетингу (192.168.100.50) это поразит внутренний интерфейс ASA. Для эхо-запроса протокола ICMP это создаст сеанс:

```
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)
```

и увеличьте счетчики 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)
```

Это может быть также подтверждено, смотря на захваты пакета. Заметьте, что отображены корректные метки:

```
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
```

Там поступает эхо-запрос протокола ICMP, помеченный с SGT = 2 (Финансы) и затем ответ от пользователя VPN, который помечен ASA с SGT = 3 (Маркетинг). Другое средство устранения проблем - пакетным трассировщиком является также готовый TrustSec.

К сожалению , ПК 802.1x не видит, что ответ, потому что это заблокировано RBACL не сохраняющим состояние на коммутаторе (пояснение в следующем разделе).

Другое средство устранения проблем - пакетным трассировщиком является также готовый TrustSec. Давайте подтвердим, будет ли принят входящий пакет ICMP от Финансов:

```
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
```

Давайте также попытаемся инициировать любой TCP - подключение от Финансов до Маркетинга, который должен быть заблокирован 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]
```

Осуществление коммутатора

Давайте проверим, загрузил ли коммутатор политику от ISE правильно:

```
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
```

Политика, управляющая трафиком от Маркетинга для Финансирования, установлена правильно. Только tcp/445 позволен согласно 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
```

Это - причина, почему был отброшен ответ эхо - запрос ICMP, прибывающий из Маркетинга для Финансирования. Это может быть подтверждено путем проверки счетчиков для трафика от SGT 3 до 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
```

Пакеты были отброшены аппаратными средствами (текущий счетчик равняется 65 и увеличению каждой 1 секунды).

Что, если соединение tcp/445 будет инициироваться от Маркетинга?

ASA обеспечит это (принимает весь трафик VPN из-за "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)
```

Корректный сеанс будет создан:

```
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
```

И IOS примет, так как он совпадает с telnet445 RBACL. Корректные счетчики будут увеличены:

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

(последний столбец является трафиком, разрешенным аппаратными средствами). Сеанс разрешен.

Тот пример был представлен для цели показать различие в конфигурации политики TrustSec и осуществлении на ASA и IOS. Также знайте о различиях политики IOS, загруженной от ISE (RBACL не сохраняющий состояние) и TrustSec осведомленный Зональный Базирующийся Межсетевой экран с отслеживанием состояния.

Ссылки

- Положение VPN версии ASA 9.2.1 с примером конфигурации ISE
- ASA и коммутатор Catalyst серии 3750X — пример конфигурации TrustSec и руководство по устранению неполадок
- Руководство конфигурации коммутатора Cisco TrustSec: понимание Cisco TrustSec
- Настройка внешний сервер для авторизации пользователя на устройстве безопасности
- Руководство конфигурации интерфейса командой строки VPN серии Cisco ASA, 9.1
- Руководство пользователя платформы Cisco Identity Services Engine, выпуск 1.2
- Cisco Systems – техническая поддержка и документация