Configurazione di più matrici TrustSec su ISE 2.2

Sommario

Introduzione

Questo documento descrive l'uso di più matrici TrustSec e matrici DefCon in Cisco Identity Services Engine (ISE) 2.2. Questa è una nuova funzione TrustSec introdotta in ISE 2.2 per migliorare la granularità nella rete.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base dei componenti Cisco TrustSec (CTS)
- Conoscenze base della configurazione CLI degli switch Catalyst

- Esperienza nella configurazione di Identity Services Engine (ISE)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Identity Services Engine 2.2
- Cisco Catalyst Switch 3850 03.07.03.E
- Cisco Catalyst Switch 3750X 15.2(4)E1
- computer Windows 7

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Ad ISE 2.0 è possibile usare solo una matrice di produzione TrustSec per tutti i dispositivi di rete. ISE 2.1 ha aggiunto una funzione chiamata staging matrix che può essere utilizzata a scopo di test e implementazione. I criteri creati nella matrice di gestione temporanea vengono applicati solo ai dispositivi di rete utilizzati per i test. Gli altri dispositivi utilizzano ancora la matrice di produzione. Una volta confermato che la matrice di gestione temporanea funziona correttamente, è possibile spostarvi tutti gli altri dispositivi e trasformarla in una nuova matrice di produzione.

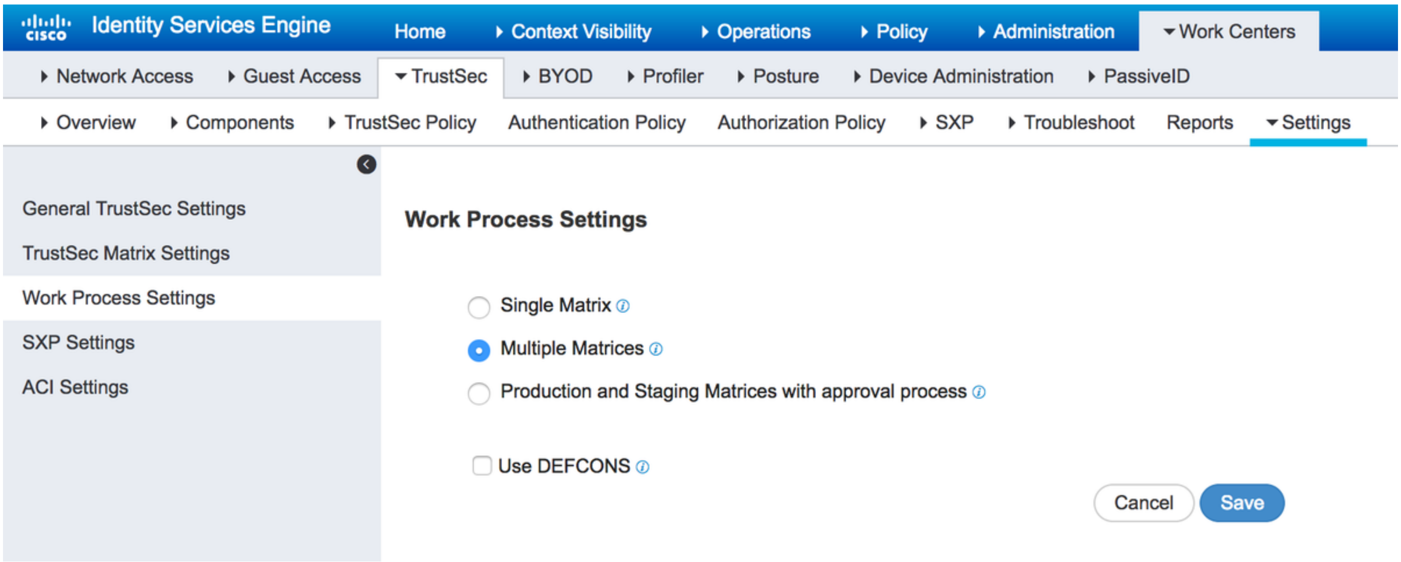
ISE 2.2 è dotato di due nuove funzioni TrustSec:

1. Matrici multiple: possibilità di assegnare matrici diverse ai dispositivi di rete
2. Matrice DefCon: questa matrice viene inviata a tutti i dispositivi di rete in una particolare situazione, attivata dall'amministratore

In ISE 2.2 è possibile utilizzare sia la funzione matrice singola che la funzione matrice produzione e allestimento.

Matrici multiple

Per utilizzare più matrici, è necessario attivare questa opzione in **Centri di lavoro > TrustSec > Impostazioni > Impostazioni processo di lavoro**, come mostrato nell'immagine:



Work Process Settings

○ Single Matrix

● Multiple Matrices

○ Production and Staging Matrices with approval process

□ Use DEFCONS

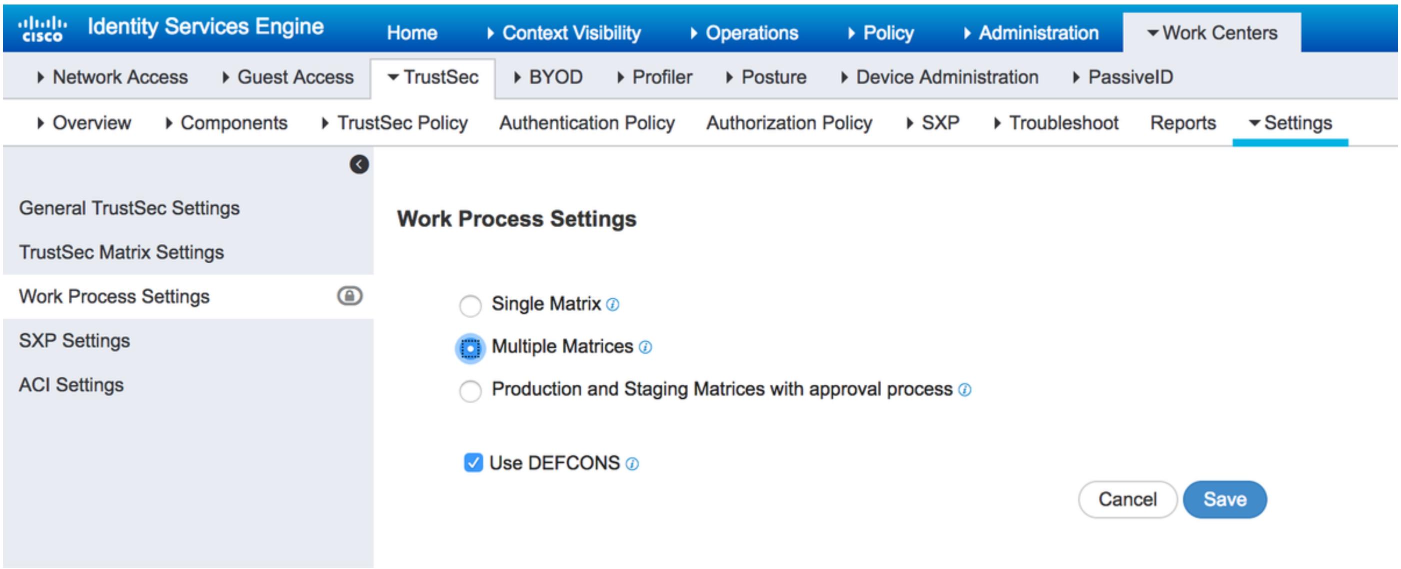
Una volta attivata questa opzione, è possibile creare nuove matrici e successivamente assegnare i dispositivi di rete alla matrice specifica.

Matrici DefCon

Le matrici DefCon sono matrici speciali, pronte per essere distribuite in qualsiasi momento. Al momento della distribuzione, tutti i dispositivi di rete vengono automaticamente assegnati a questa matrice. ISE ricorda ancora l'ultima matrice di produzione per tutti i dispositivi di rete, quindi questa modifica può essere ripristinata in qualsiasi momento quando DefCon viene disattivato. È possibile definire fino a quattro diverse matrici DefCon:

1. DefCon1 - Critica
2. DefCon2 - Grave
3. DefCon3 - Sostanziale
4. DefCon4 - Sufficiente

Le matrici DefCon possono essere utilizzate in combinazione con tutte e tre le opzioni di processo di lavoro:



Work Process Settings

○ Single Matrix

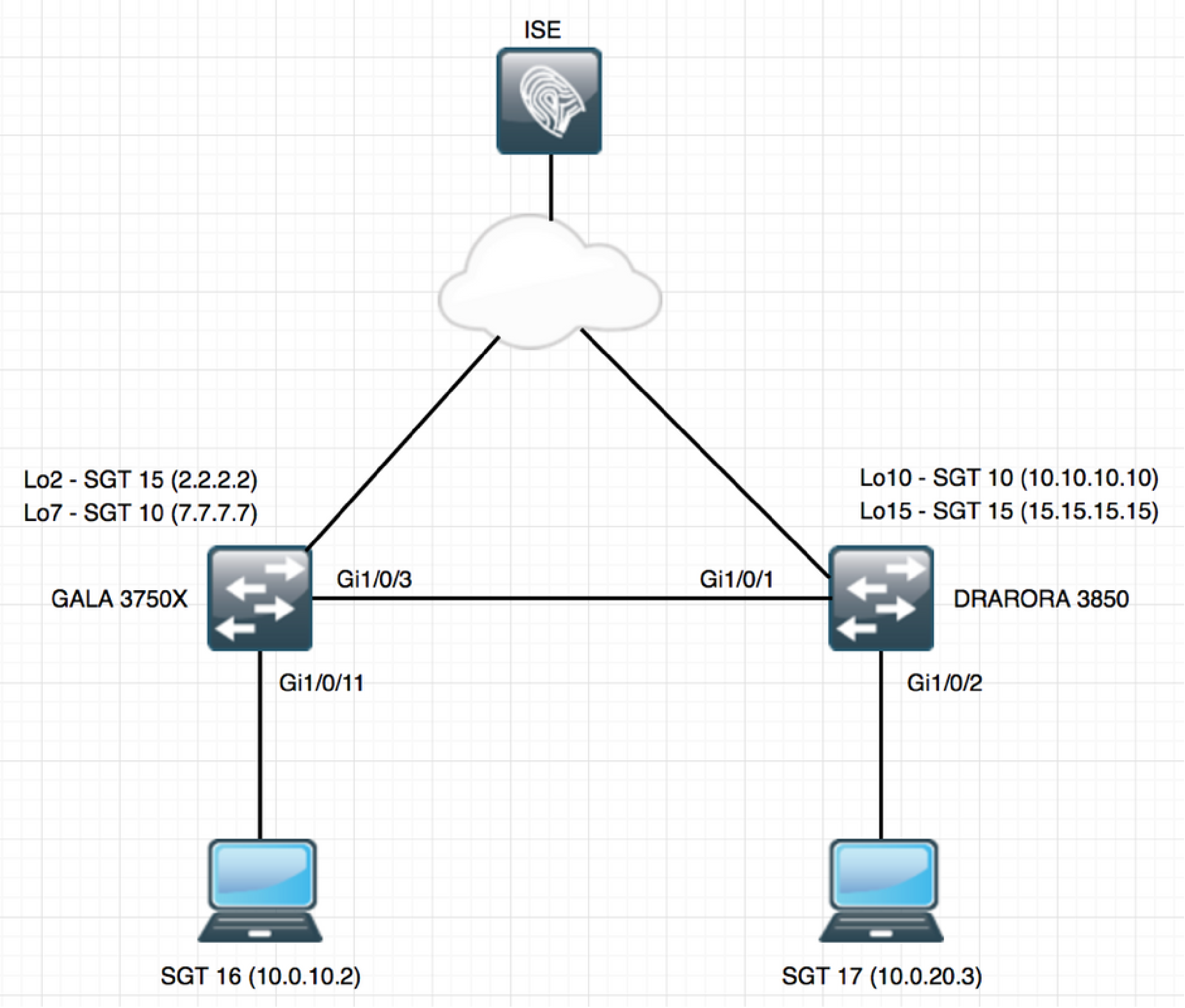
● Multiple Matrices

○ Production and Staging Matrices with approval process

☑ Use DEFCONS

Configurazione

Esempio di rete



Configurazioni

Per utilizzare più matrici, è necessario attivarle in Impostazioni processo di lavoro. In questo esempio, abilitare anche la matrice DefCon.

1. Configurazione di base dello switch per RADIUS/CTS

```
radius server ISE
 address ipv4 10.48.17.161 auth-port 1812 acct-port 1813
 pac key cisco

aaa group server radius ISE
 server name ISE
 ip radius source-interface FastEthernet0

ip radius source-interface FastEthernet0

aaa server radius dynamic-author
 client 10.48.17.161 server-key cisco
```

```
aaa new-model aaa authentication dot1x default group ISE aaa accounting dot1x default start-stop
group ISE
```

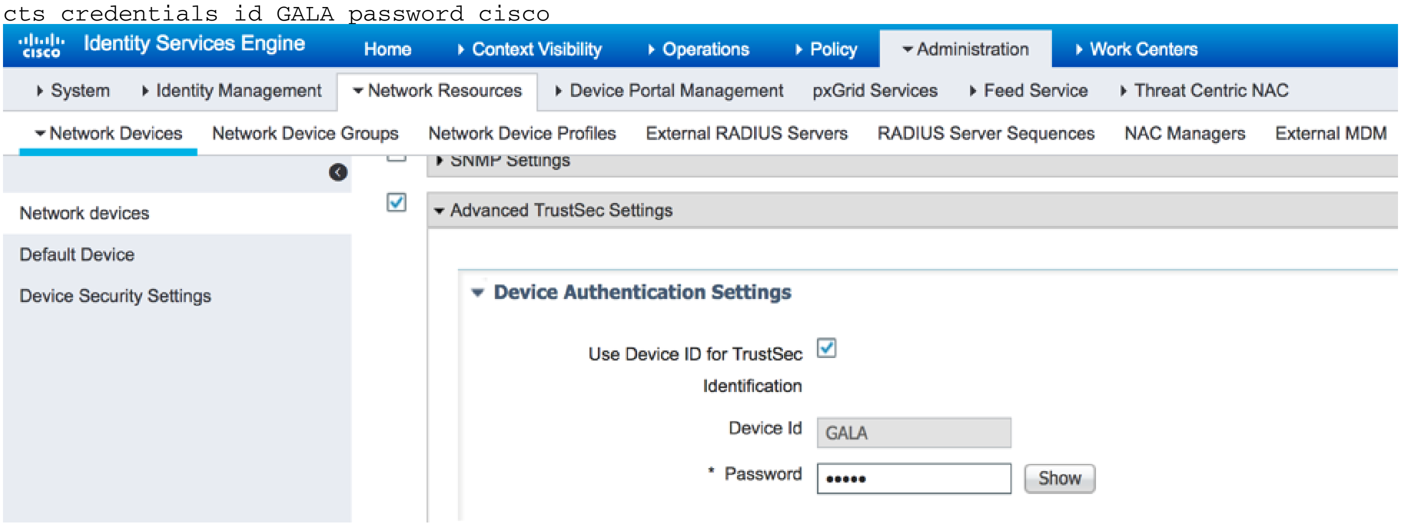
Per ottenere informazioni CTS, è necessario creare un elenco di autorizzazioni CTS:

```
cts authorization list LIST
aaa authorization network LIST group ISE
```

2. PAC CTS

Per ricevere la PAC CTS (Protected Access Credentials) da ISE, è necessario configurare le stesse credenziali sullo switch e ISE in Configurazione Advanced TrustSec per il dispositivo di rete:

```
cts credentials id GALA password cisco
```



☑ Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification ☑

Device Id GALA

* Password •••••

Una volta configurata questa opzione, uno switch può scaricare la PAC CTS. Una parte (PAC-Opaque) viene inviata come coppia AV in ogni richiesta RADIUS ad ISE, in modo che ISE possa verificare se la PAC per questo dispositivo di rete è ancora valida:

```
GALA#show cts pacs
  AID: E6796CD7BBF2FA4111AD9FB4FEFB5A50
  PAC-Info:
    PAC-type = Cisco Trustsec
    AID: E6796CD7BBF2FA4111AD9FB4FEFB5A50
    I-ID: GALA
    A-ID-Info: Identity Services Engine
    Credential Lifetime: 17:05:50 CEST Apr 5 2017
  PAC-Opaque:
000200B00003000100040010E6796CD7BBF2FA4111AD9FB4FEFB5A50000600940003010012FABE10F3DCBCB152C54FA5
BFE124CB00000013586BB31500093A809E11A93189C7BE6EBDFB8FDD15B9B7252EB741ADCA3B2ACC5FD923AEB7BDFE48
A3A771338926A1F48141AF091469EE4AFC8C3E92A510BA214A407A33F469282A780E8F50F17A271E92D1FEE1A29ED427
B985F9A0E00D6CDC934087716F4DEAF84AC11AA05F7587E898CA908463BDA9EC7E65D827
  Refresh timer is set for 11y13w
```

3. Configurazione CTS su uno switch.

Una volta scaricata la PAC, lo switch può richiedere ulteriori informazioni CTS (dati di ambiente e policy):

```
GALA#cts refresh environment-data

GALA#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 0-06:Unknown
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.48.17.161, port 1812, A-ID E6796CD7BBF2FA4111AD9FB4FEFB5A50
          Status = ALIVE
          auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
    0-ce:Unknown
    2-ce:TrustSec_Devices
    3-ce:Network_Services
    4-ce:Employees
    5-ce:Contractors
    6-ce:Guests
    7-ce:Production_Users
    8-ce:Developers
    9-ce:Auditors
    10-ce:Point_of_Sale_Systems
    11-ce:Production_Servers
    12-ce:Development_Servers
    13-ce:Test_Servers
    14-ce:PCI_Servers
    15-ce:BYOD
    255-ce:Quarantined_Systems
Environment Data Lifetime = 86400 secs
Last update time = 07:48:41 CET Mon Jan 2 2006
Env-data expires in   0:23:56:02 (dd:hr:mm:sec)
Env-data refreshes in 0:23:56:02 (dd:hr:mm:sec)
Cache data applied           = NONE
State Machine is running

GALA#cts refresh policy

GALA#show cts role-based permissions
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

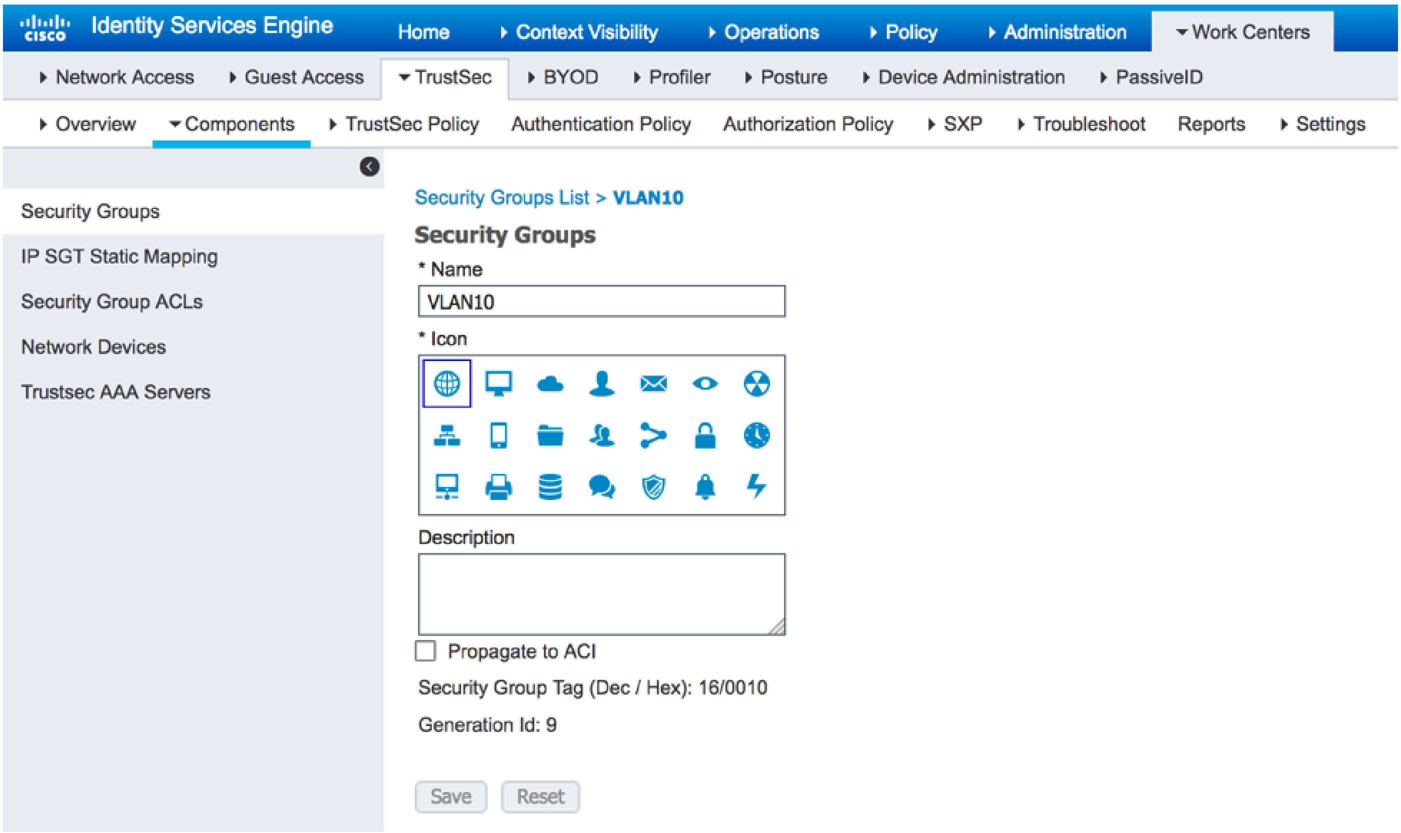
Èpossibile che non vi siano criteri scaricati da ISE, il motivo è che l'imposizione CTS non è abilitata sullo switch:

```
cts role-based enforcement
cts role-based enforcement vlan-list 1-4094

GALA#show cts role-based permissions
IPv4 Role-based permissions default:
Permit IP-00
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

In entrambi gli output, è possibile visualizzare i valori predefiniti - SGT creati per impostazione predefinita (0, 2-15, 255) e il criterio **Consenti IP** predefinito.

4. Configurazione CTS di base su ISE.

Creare nuovi Security Group Tags (SGT) e alcune policy su ISE per poterli usare in seguito. Passare a **Centri di lavoro > TrustSec > Componenti > Gruppi di sicurezza**, fare clic su **Aggiungi** per creare un nuovo SGT:



Security Groups List > **VLAN10**

Security Groups

* Name: VLAN10

* Icon

Description

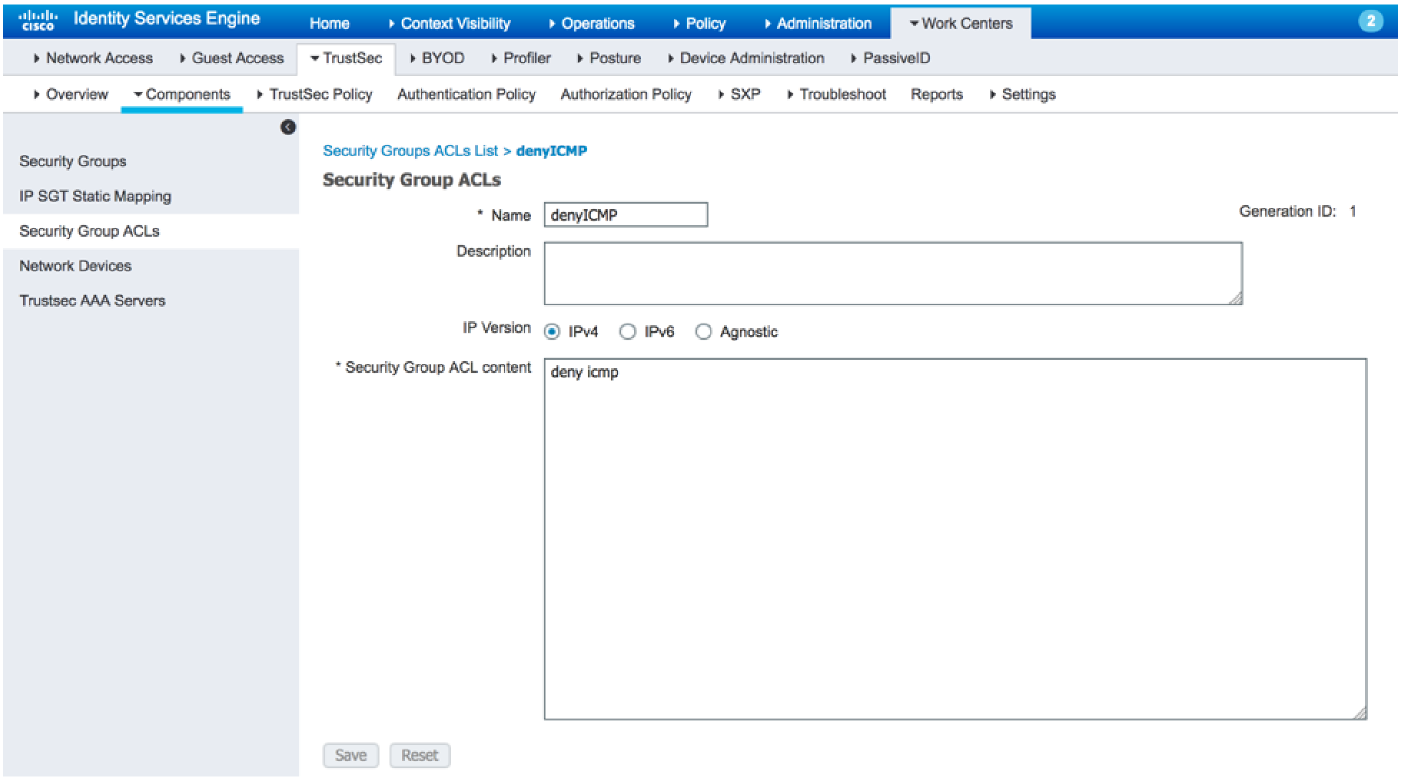
□ Propagate to ACI

Security Group Tag (Dec / Hex): 16/0010

Generation Id: 9

Save Reset

Per creare un elenco di controllo di accesso del gruppo di sicurezza (SGACL, Security Group Access Control List) per il filtro del traffico, scegliere **ACL del gruppo di sicurezza**, come mostrato nell'immagine:



Security Groups ACLs List > **denyICMP**

Security Group ACLs

* Name: denyICMP

Generation ID: 1

Description

IP Version: ● IPv4 ○ IPv6 ○ Agnostic

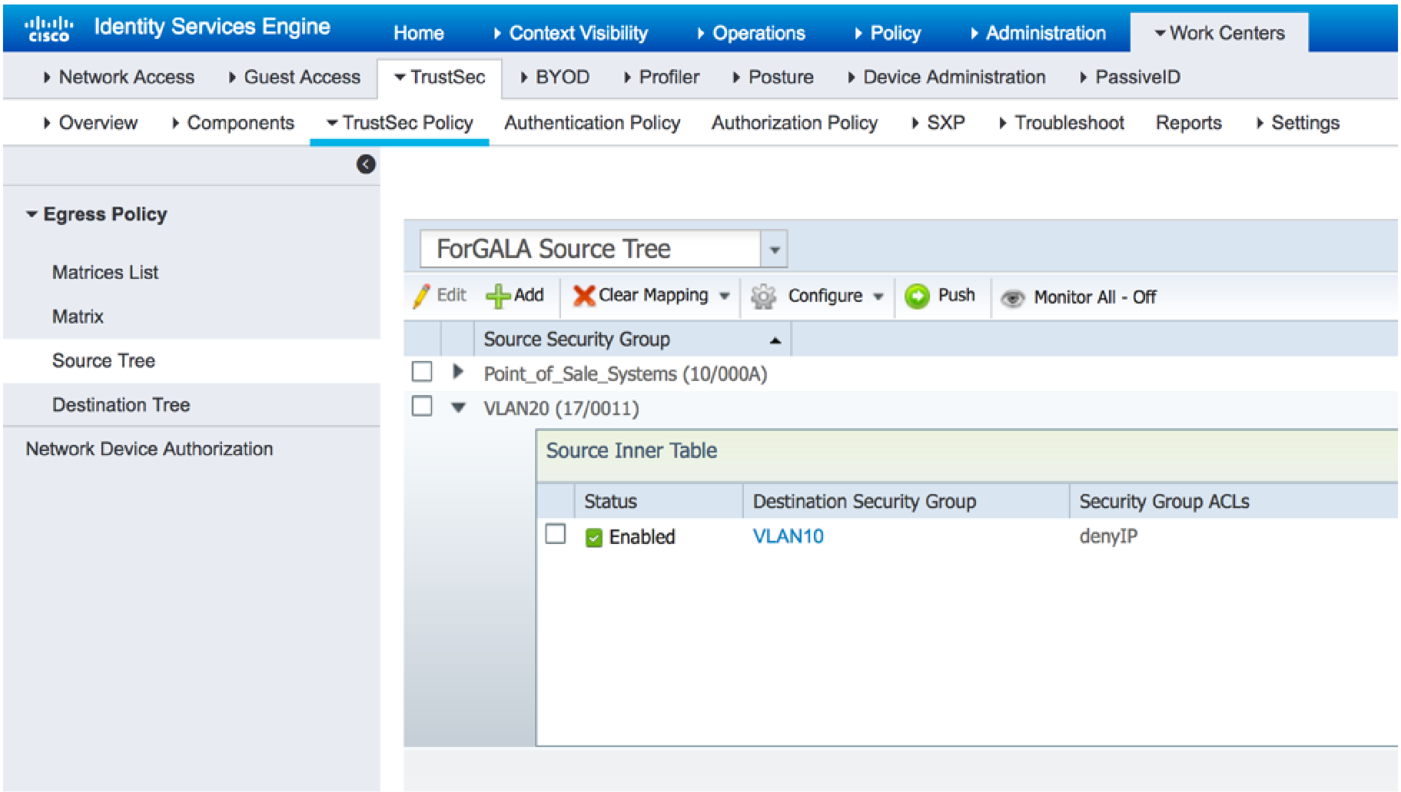
* Security Group ACL content:

```
deny icmp
```

Save Reset

Analogamente, è possibile creare altri SGT e SGACL. Una volta creati i SGT e i SGACL, è possibile collegarli nei criteri CTS, per fare ciò passare a **Centri di lavoro > TrustSec > TustSec**

Policy > Egress Policy > Source Tree, come mostrato nell'immagine:



ForGALA Source Tree

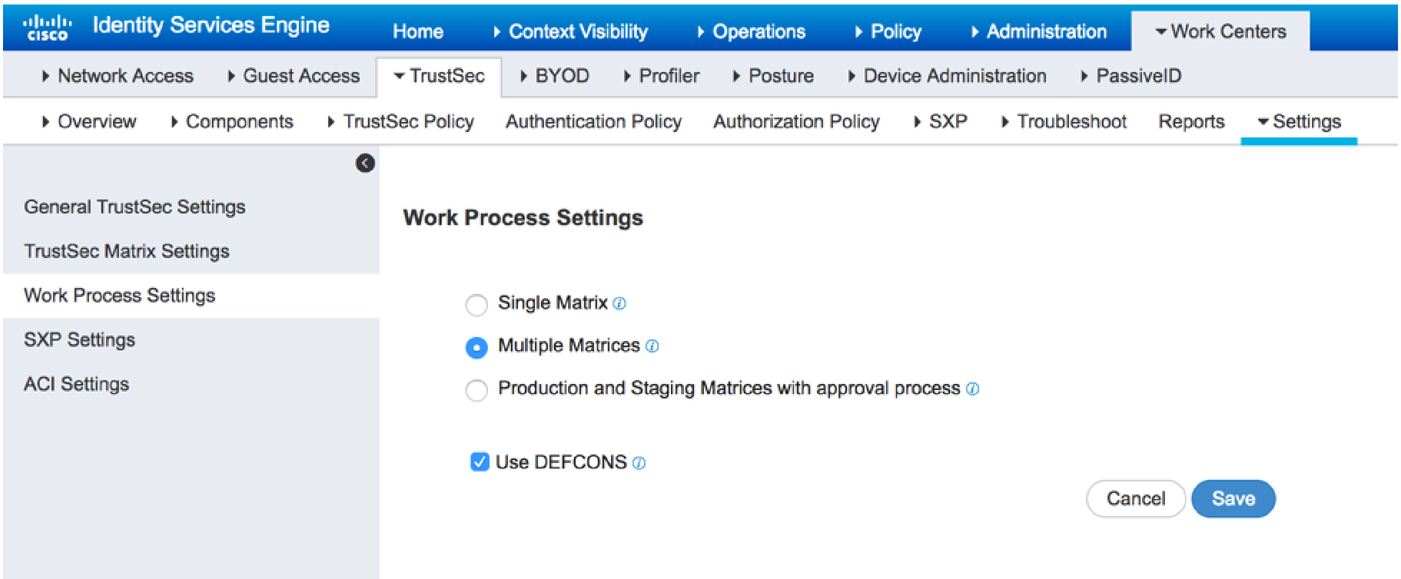
		Source Security Group
□	▸	Point_of_Sale_Systems (10/000A)
□	▾	VLAN20 (17/0011)

Source Inner Table

	Status	Destination Security Group	Security Group ACLs
□	✓ Enabled	VLAN10	denyIP

5. Matrici multiple e configurazione DefCon su ISE.

In questo esempio sono stati configurati i criteri per la matrice **ForGALA**. Per passare da una matrice all'altra, è possibile utilizzare il menu a discesa. Per abilitare più matrici, passare a **Centri di lavoro > TrustSec > Impostazioni > Impostazioni processo di lavoro** e abilitare Matrici multiple e matrici DefCon, come mostrato nell'immagine:



Work Process Settings

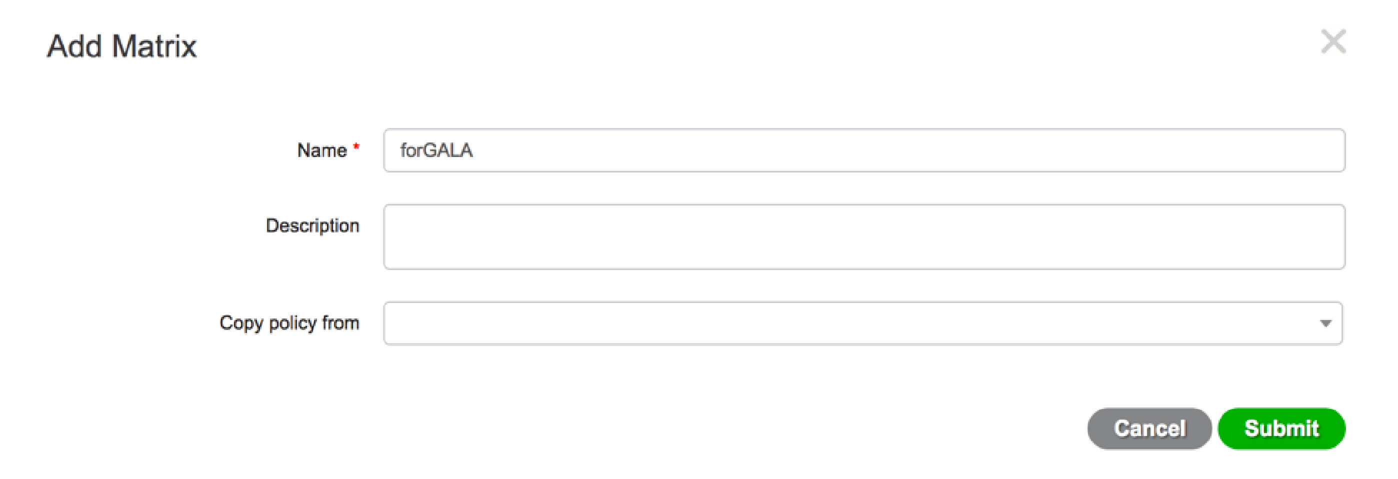
○ Single Matrix

● Multiple Matrices

○ Production and Staging Matrices with approval process

☑ Use DEFCONS

Quando questa opzione è attivata, è disponibile una matrice di produzione predefinita, sebbene sia possibile creare altre matrici. Passare a **Centri di lavoro > TrustSec > Criteri TrustSec > Criteri in uscita > Elenco matrici** e fare clic su **Aggiungi**:



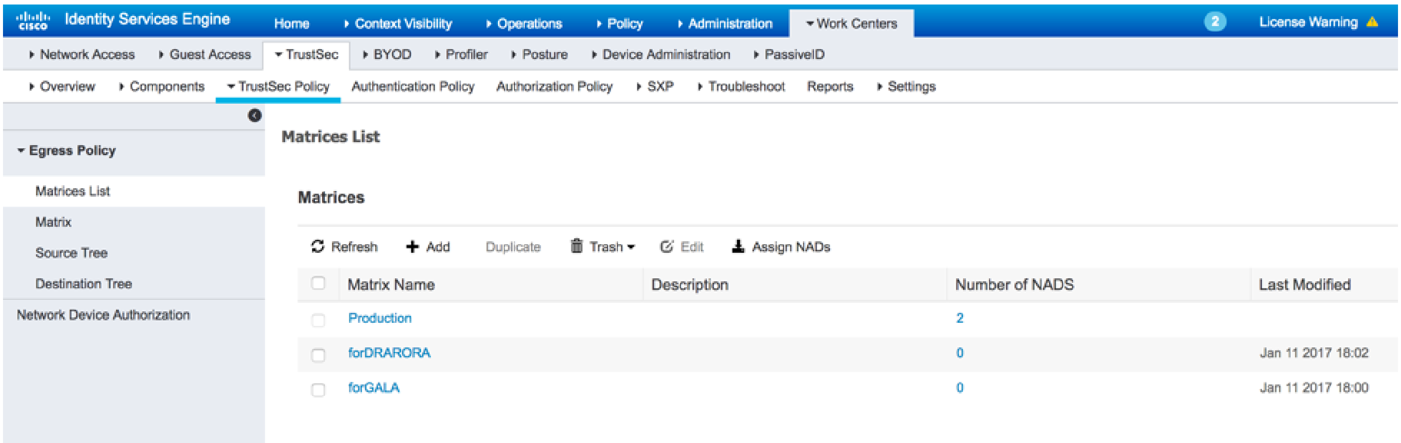
Add Matrix

Name * forGALA

Description

Copy policy from

Esiste un'opzione per copiare i criteri che dovrebbero diventare parte del nuovo criterio dalla matrice già esistente. Creare due matrici: una per lo switch 3750X e un'altra per lo switch 3850. Una volta create le matrici, è necessario assegnare i dispositivi di rete a tali matrici, poiché per impostazione predefinita tutti i dispositivi di accesso alla rete abilitati per TrustSec vengono assegnati alla matrice Produzione.

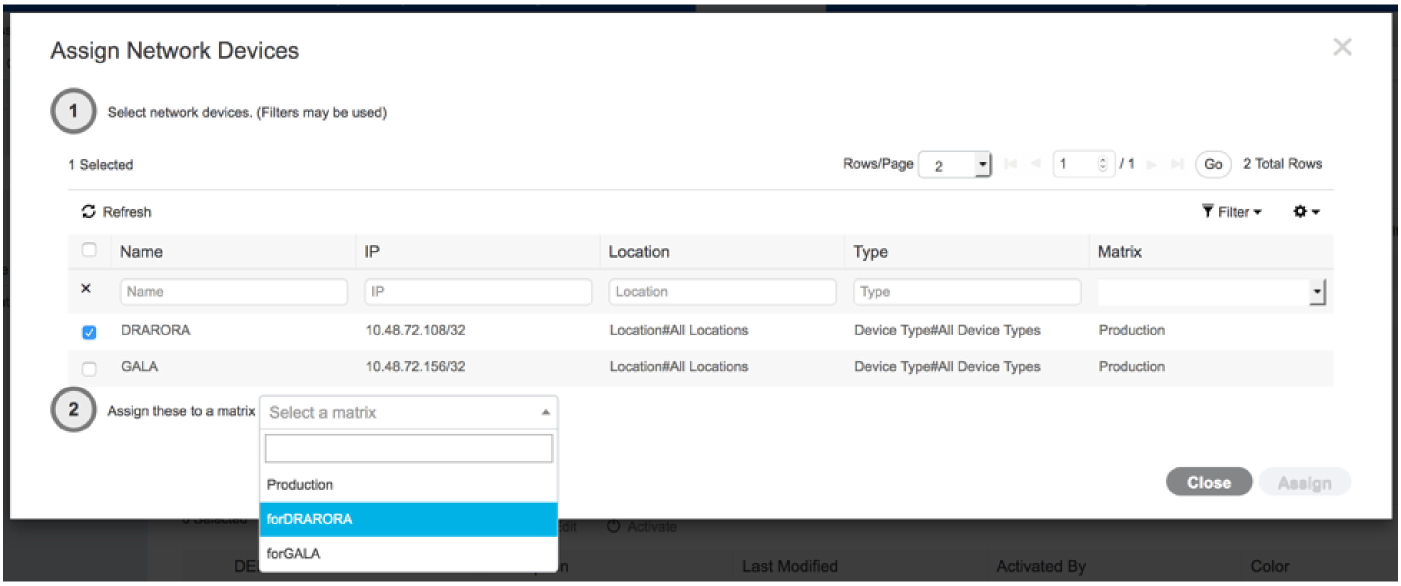


Matrices List

Matrices

□	Matrix Name	Description	Number of NADS	Last Modified
□	Production		2	
□	forDRARORA		0	Jan 11 2017 18:02
□	forGALA		0	Jan 11 2017 18:00

Per assegnare NAD, fare clic su **Assegna NADs** in Elenco matrici, selezionare la periferica alla quale si desidera assegnare la matrice e scegliere la matrice creata dal menu a discesa e fare clic su **Assegna**, come mostrato nell'immagine:



Assign Network Devices

1 Select network devices. (Filters may be used)

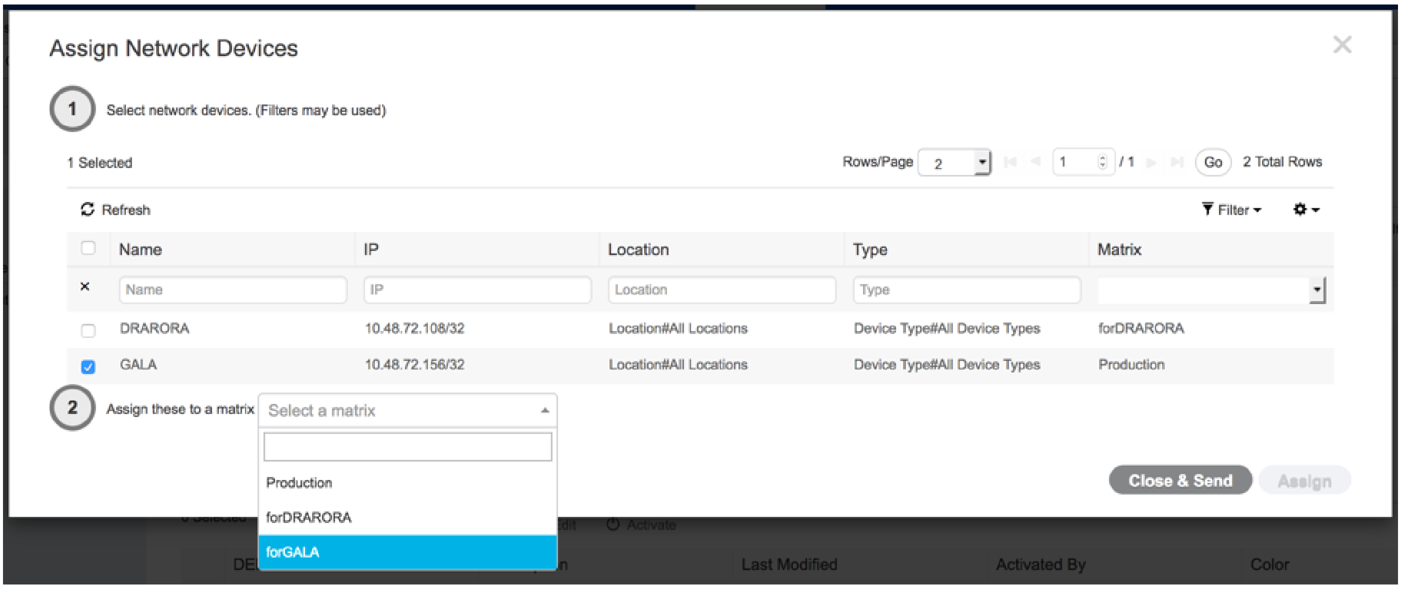
1 Selected

Rows/Page 2 | 1 /1 | Go | 2 Total Rows

□	Name	IP	Location	Type	Matrix
☑	DRARORA	10.48.72.108/32	Location#All Locations	Device Type#All Device Types	Production
□	GALA	10.48.72.156/32	Location#All Locations	Device Type#All Device Types	Production

2 Assign these to a matrix: Select a matrix

Lo stesso può essere fatto per altri dispositivi, quindi fare clic sul pulsante **Assegna**:



Assign Network Devices

1 Select network devices. (Filters may be used)

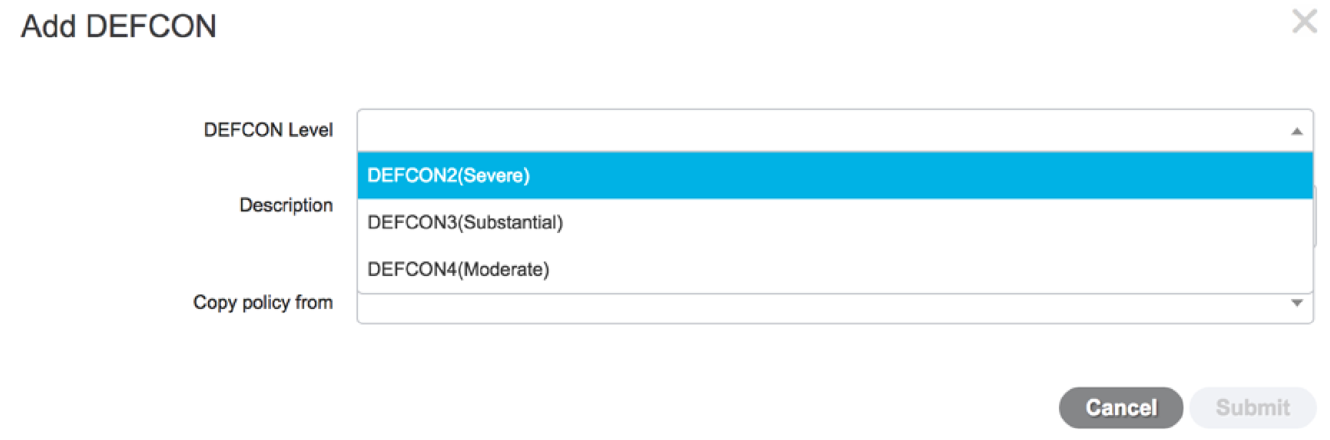
1 Selected — Rows/Page 2 — 1 / 1 — Go — 2 Total Rows

☐	Name	IP	Location	Type	Matrix
☐	DRARORA	10.48.72.108/32	Location#All Locations	Device Type#All Device Types	forDRARORA
☑	GALA	10.48.72.156/32	Location#All Locations	Device Type#All Device Types	Production

2 Assign these to a matrix: Select a matrix

- Production
- forDRARORA
- forGALA

Dopo aver eseguito tutte le modifiche, fare clic su **Close&Send** per inviare tutti gli aggiornamenti ai dispositivi e aggiornare le policy CTS in modo da scaricarne di nuove. Analogamente, creare una matrice DefCon, che è possibile copiare da matrici esistenti:



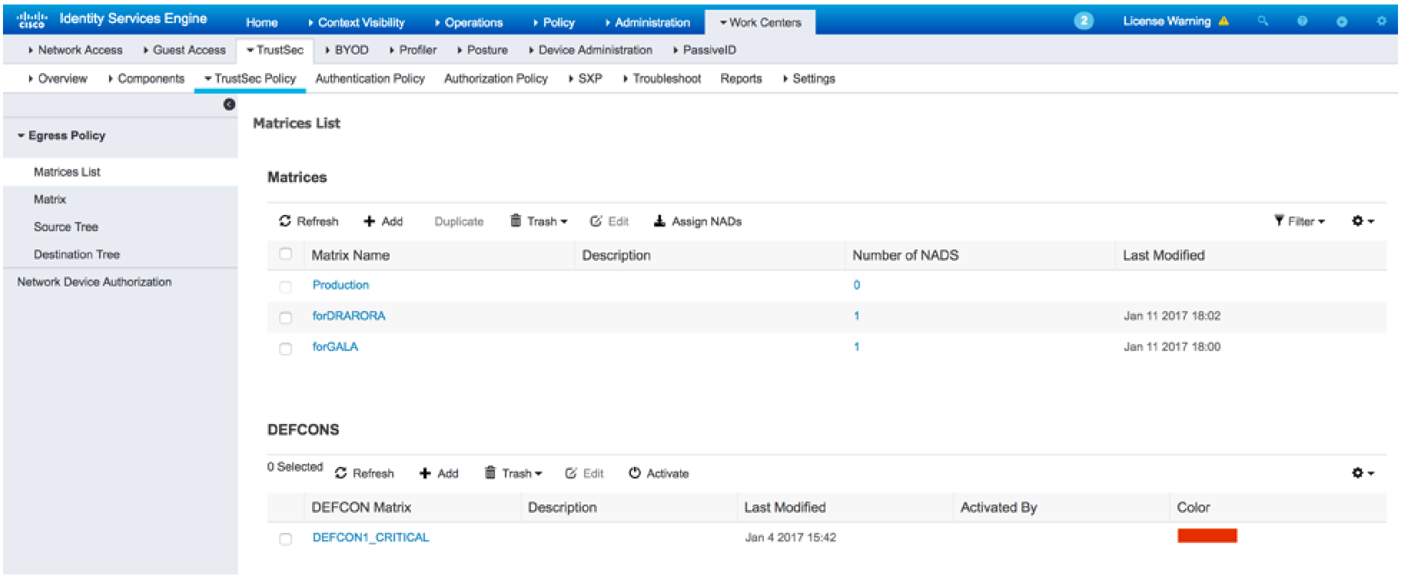
Add DEFCON

DEFCON Level:
- DEFCON2(Severe)
- DEFCON3(Substantial)
- DEFCON4(Moderate)

Description

Copy policy from

Le politiche finali sono:



Matrices List

Matrices

☐	Matrix Name	Description	Number of NADS	Last Modified
☐	Production		0	
☐	forDRARORA		1	Jan 11 2017 18:02
☐	forGALA		1	Jan 11 2017 18:00

DEFCONS

0 Selected

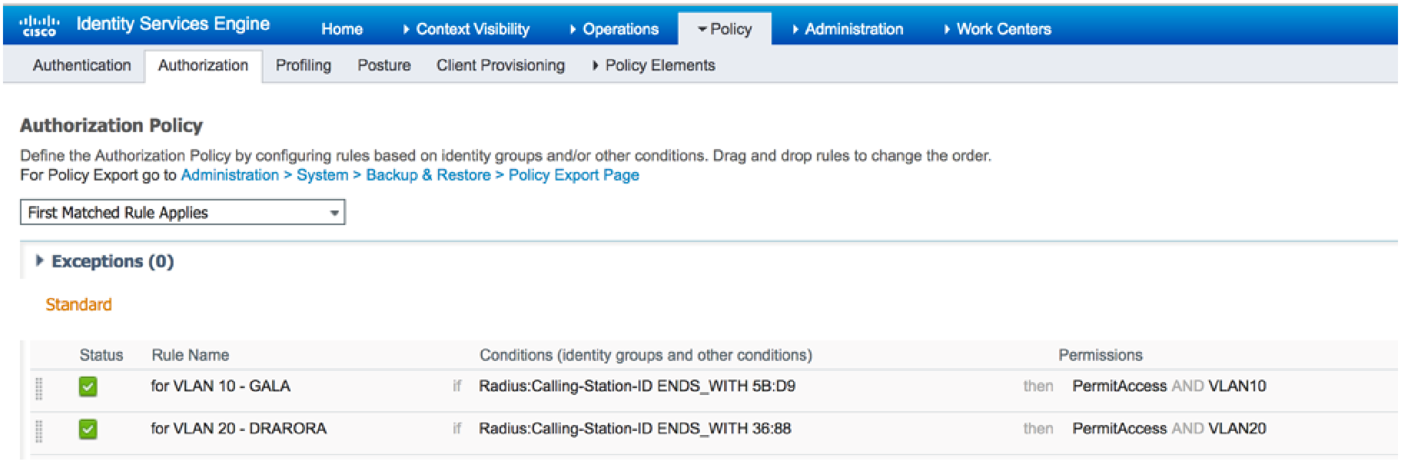
☐	DEFCON Matrix	Description	Last Modified	Activated By	Color
☐	DEFCON1_CRITICAL		Jan 4 2017 15:42		🟥

6. Classificazione SGT

Esistono due opzioni per le assegnazioni ai client (creazione di mapping IP-SGT):

- *static* - con ***tag sgt indirizzo_IP basato su ruolo cts***
- *dinamico* - tramite autenticazione dot1x (il tag viene assegnato in seguito all'autenticazione riuscita)

Utilizzare entrambe le opzioni: due computer Windows ottengono il tag SGT tramite l'autenticazione dot1x e le interfacce di loopback con il tag SGT statico. Per distribuire il mapping dinamico, creare i criteri di autorizzazione per i client finali:



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	for VLAN 10 - GALA	if	Radius:Calling-Station-ID ENDS_WITH 5B:D9	then	PermitAccess AND VLAN10
✓	for VLAN 20 - DRARORA	if	Radius:Calling-Station-ID ENDS_WITH 36:88	then	PermitAccess AND VLAN20

Per creare un mapping IP-SGT statico, utilizzare i comandi (ad esempio per lo switch GALA):

```
interface Loopback7
 ip address 7.7.7.7 255.255.255.0

interface Loopback2
 ip address 2.2.2.2 255.255.255.0

cts role-based sgt-map 2.2.2.2 sgt 15
cts role-based sgt-map 7.7.7.7 sgt 10
```

Dopo l'autenticazione, il client raggiunge i criteri di autorizzazione con un tag SGT specifico, ottenendo il risultato seguente:

```
GALA#show authentication sessions interface Gi1/0/11 details
            Interface:  GigabitEthernet1/0/11
          MAC Address:  0050.5699.5bd9
         IPv6 Address:  Unknown
         IPv4 Address:  10.0.10.2
            User-Name:  00-50-56-99-5B-D9
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  both
      Session timeout:  N/A
      Restart timeout:  N/A
    Common Session ID:  0A30489C000000120002330D
      Acct Session ID:  0x00000008
               Handle:  0xCE000001
       Current Policy:  POLICY_Gi1/0/11
```

```
Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
      Security Policy:  Should Secure
      Security Status:  Link Unsecure

Server Policies:
            SGT Value:  16

Method status list:
       Method           State

       mab              Authc Success
```

Èpossibile controllare tutti i mapping IP-SGT con il comando **show cts role-based sgt-map all**, in cui viene visualizzata l'origine di ogni mapping (LOCAL - tramite autenticazione dot1x, CLI - static assignment):

```
GALA#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
2.2.2.2                 15      CLI
7.7.7.7                 10      CLI
10.0.10.2               16      LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 2
Total number of LOCAL    bindings = 1
Total number of active   bindings = 3
```

7. Download criteri CTS

Una volta che lo switch ha la PAC CTS e i dati dell'ambiente sono stati scaricati, può richiedere i criteri CTS. Lo switch non scarica tutte le policy, ma solo quelle necessarie - policy per il traffico destinato a tag SGT noti - in caso di switch GALA, richiede da ISE tali policy:

- criteri per il traffico verso SGT 15
- criteri per il traffico verso SGT 10
- criteri per il traffico verso SGT 16

L'output di tutte le regole per lo switch GALA:

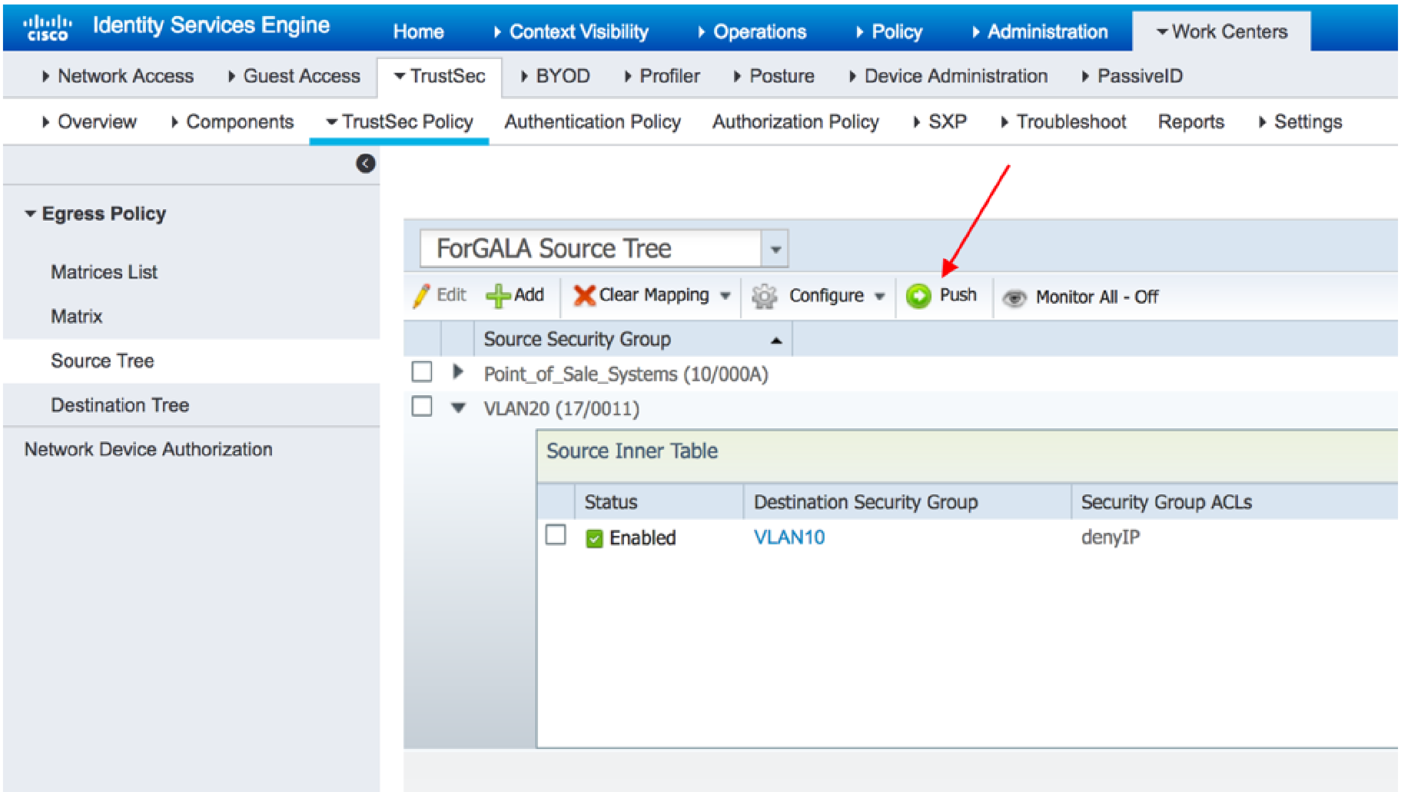
```
GALA#show cts role-based permissions
IPv4 Role-based permissions default:
Permit IP-00
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 15:BYOD:
denyIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 16:VLAN10:
denyIP-20
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

Switch ottiene le regole in due modi:

- Il CTS viene aggiornato dallo switch stesso:

```
GALA#cts refresh policy
```

- Pressione manuale da ISE:



	Source Security Group
□ ▶	Point_of_Sale_Systems (10/000A)
□ ▼	VLAN20 (17/0011)

Source Inner Table

	Status	Destination Security Group	Security Group ACLs
□	☑ Enabled	VLAN10	denyIP

Verifica

Matrici multiple

I mapping SGT-IP finali e le policy CTS su entrambi gli switch per questo esempio:

Interruttore GALA:

```
GALA#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
2.2.2.2                 15      CLI
7.7.7.7                 10      CLI
10.0.10.2               16      LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 2
Total number of LOCAL    bindings = 1
Total number of active   bindings = 3

GALA#show cts role-based permissions
IPv4 Role-based permissions default:
   Permit IP-00
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 15:BYOD:
   denyIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 15:BYOD:
   permitIP-20
```

```
IPv4 Role-based permissions from group 17:VLAN20 to group 16:VLAN10:
   permitIP-20
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

GALA#show cts rbacl | s permitIP
 name   = permitIP-20
   permit ip

GALA#show cts rbacl | s deny
 name   = denyIP-20
   deny ip
```

Switch DRARORA:

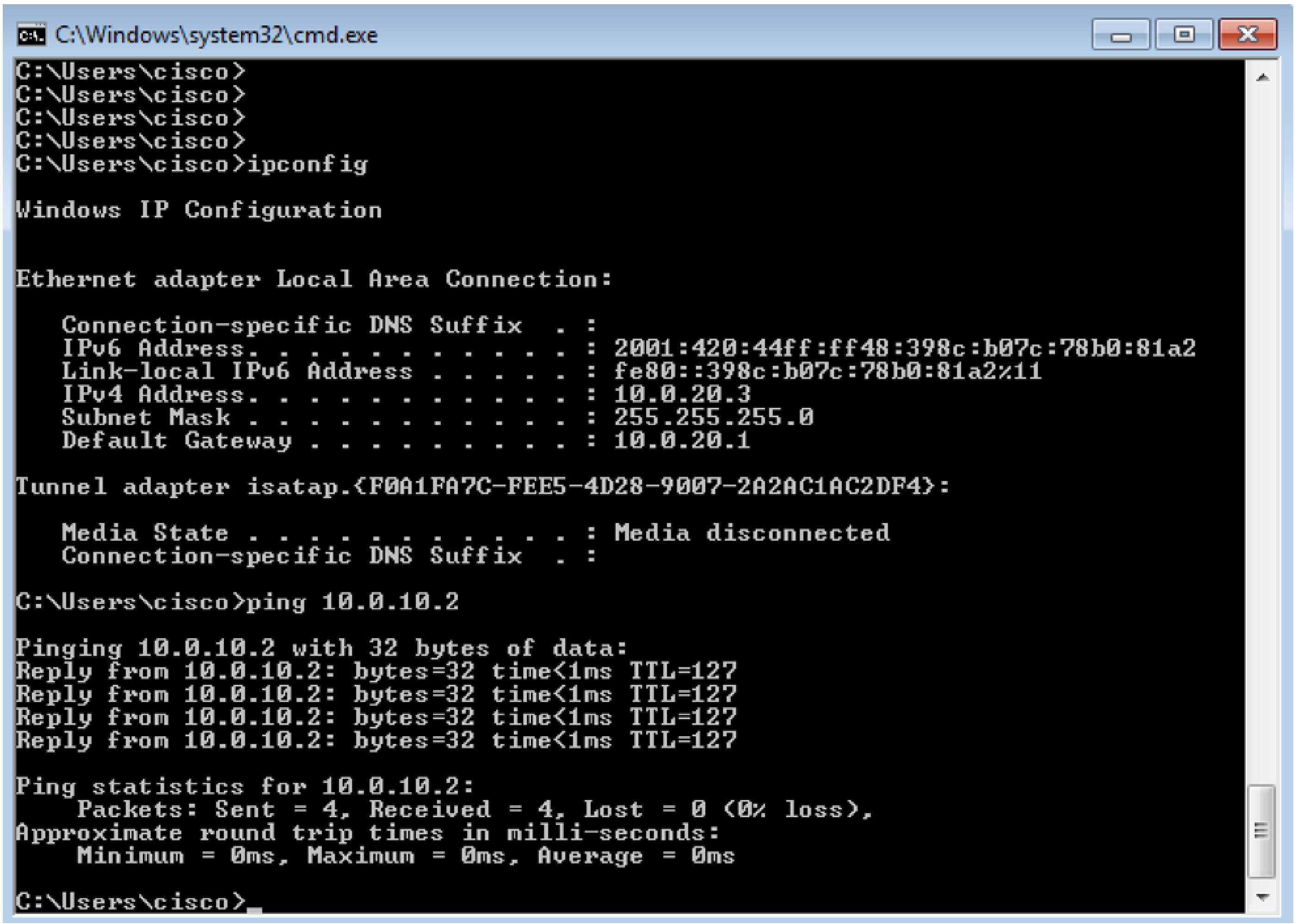
```
DRARORA#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
10.0.20.3               17      LOCAL
10.10.10.10             10      CLI
15.15.15.15             15      CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 2
Total number of LOCAL    bindings = 1
Total number of active   bindings = 3

DRARORA#show cts role-based permissions
IPv4 Role-based permissions default:
   Permit IP-00
IPv4 Role-based permissions from group 17:VLAN20 to group 10:Point_of_Sale_Systems:
   permitIP-20
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 15:BYOD:
   permitIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 15:BYOD:
   permitIP-20
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 17:VLAN20:
   denyIP-20
IPv4 Role-based permissions from group 16:VLAN10 to group 17:VLAN20:
   permitIP-20
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

Si noti che le policy per entrambi gli switch sono diverse (anche la stessa policy da 10 a 15 è diversa per gli switch GALA e DRARORA). Ciò significa che il traffico da SGT 10 a 15 è consentito su DRARORA, ma bloccato su GALA:

```
DRARORA#ping 15.15.15.15 source Loopback 10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 15.15.15.15, timeout is 2 seconds:
Packet sent with a source address of 10.10.10.10
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

GALA#ping 2.2.2.2 source Loopback 7
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
Packet sent with a source address of 7.7.7.7
```

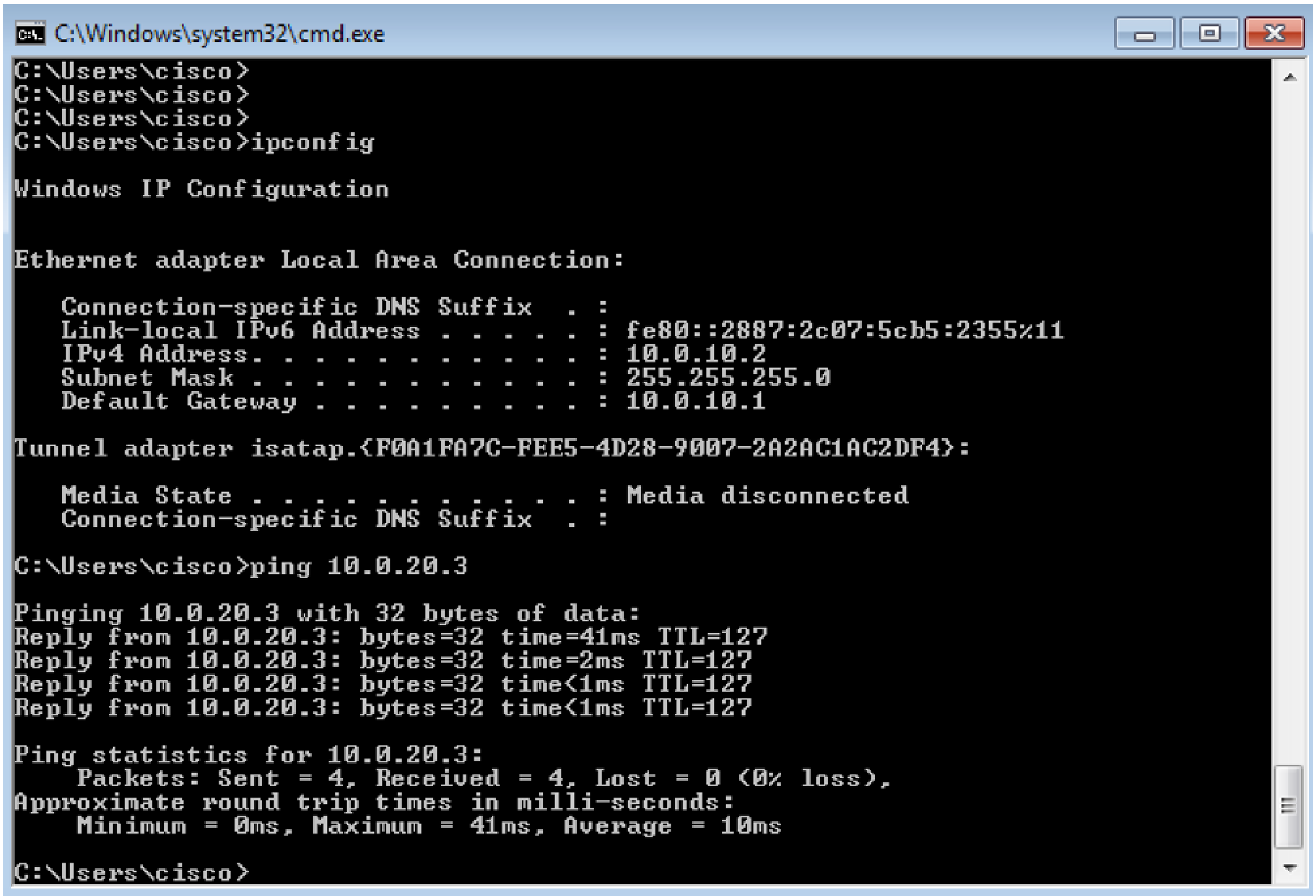
```
U.U.U
Success rate is 0 percent (0/5)
```

Analogamente, da una finestra è possibile accedere a un'altra (SGT 17 -> SGT 16):



```
C:\Users\cisco>
C:\Users\cisco>
C:\Users\cisco>
C:\Users\cisco>
C:\Users\cisco>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:420:44ff:ff48:398c:b07c:78b0:81a2
   Link-local IPv6 Address . . . . . : fe80::398c:b07c:78b0:81a2%11
   IPv4 Address. . . . . . . . . . . : 10.0.20.3
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.20.1

Tunnel adapter isatap.{F0A1FA7C-FEE5-4D28-9007-2A2AC1AC2DF4}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\cisco>ping 10.0.10.2

Pinging 10.0.10.2 with 32 bytes of data:
Reply from 10.0.10.2: bytes=32 time<1ms TTL=127
Reply from 10.0.10.2: bytes=32 time<1ms TTL=127
Reply from 10.0.10.2: bytes=32 time<1ms TTL=127
Reply from 10.0.10.2: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\cisco>_
```

E in un altro modo (SGT 16 -> SGT 17):



```
C:\Users\cisco>
C:\Users\cisco>
C:\Users\cisco>
C:\Users\cisco>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::2887:2c07:5cb5:2355%11
   IPv4 Address. . . . . . . . . . . : 10.0.10.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.10.1

Tunnel adapter isatap.{F0A1FA7C-FEE5-4D28-9007-2A2AC1AC2DF4}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\cisco>ping 10.0.20.3

Pinging 10.0.20.3 with 32 bytes of data:
Reply from 10.0.20.3: bytes=32 time=41ms TTL=127
Reply from 10.0.20.3: bytes=32 time=2ms TTL=127
Reply from 10.0.20.3: bytes=32 time<1ms TTL=127
Reply from 10.0.20.3: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.20.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 41ms, Average = 10ms

C:\Users\cisco>
```

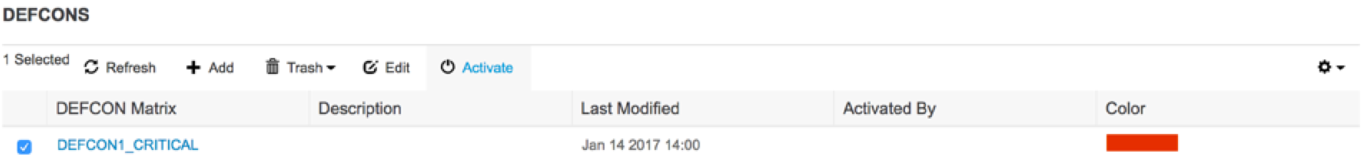
Per verificare che sia stato applicato il criterio CTS corretto, selezionare **show cts basato sul ruolo** dei contatori:

```
GALA#sh 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

17        16        0                 0                 0                 8
17        15        0                 -                 0                 -

10        15        4                 0                 0                 0

*         *         0                 0                 127               26
```

GALA ha 8 pacchetti autorizzati (4 da ping 17->16 e 4 da ping 16->17).

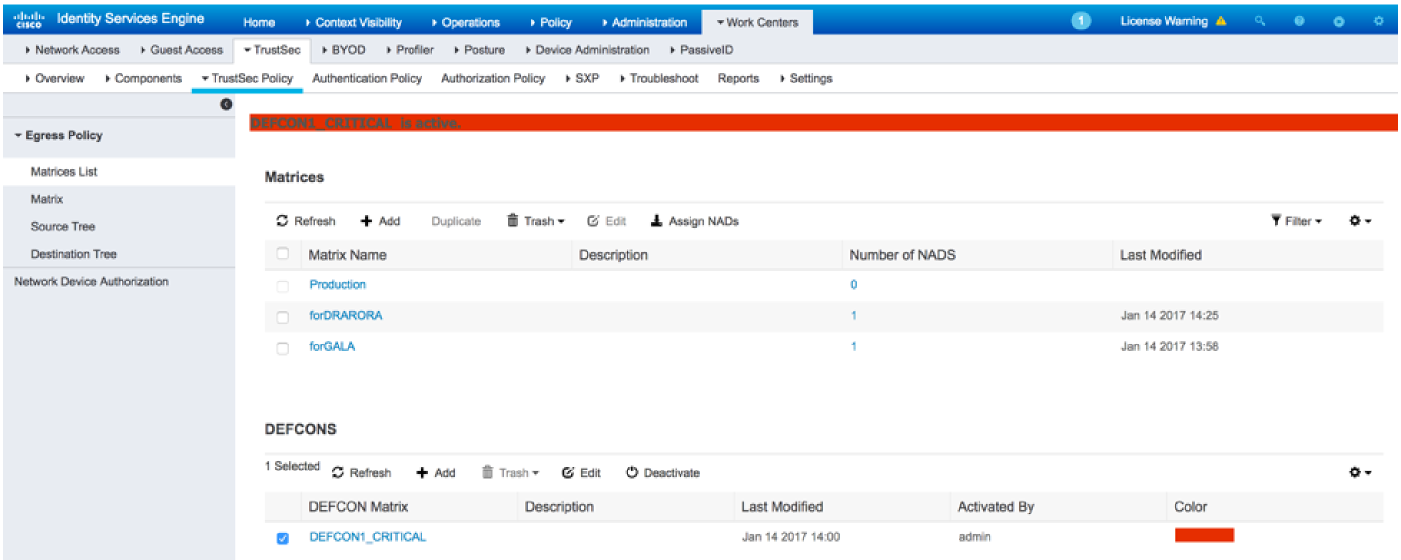
Distribuzione DefCon

Se necessario, distribuire la matrice DefCon in **Centri di lavoro > TrustSec > Criteri TrustSec > Criteri di uscita > Elenco matrici**, selezionare la matrice DefCon da attivare e fare clic su **Attiva**:



	DEFCON Matrix	Description	Last Modified	Activated By	Color
☑	DEFCON1_CRITICAL		Jan 14 2017 14:00		🟥

Una volta attivata la funzione DefCon, il menu di ISE avrà il seguente aspetto:



DEFCON1_CRITICAL is active.

Matrices

□	Matrix Name	Description	Number of NADS	Last Modified
□	Production		0	
□	forDRARORA		1	Jan 14 2017 14:25
□	forGALA		1	Jan 14 2017 13:58

DEFCONS

	DEFCON Matrix	Description	Last Modified	Activated By	Color
☑	DEFCON1_CRITICAL		Jan 14 2017 14:00	admin	🟥

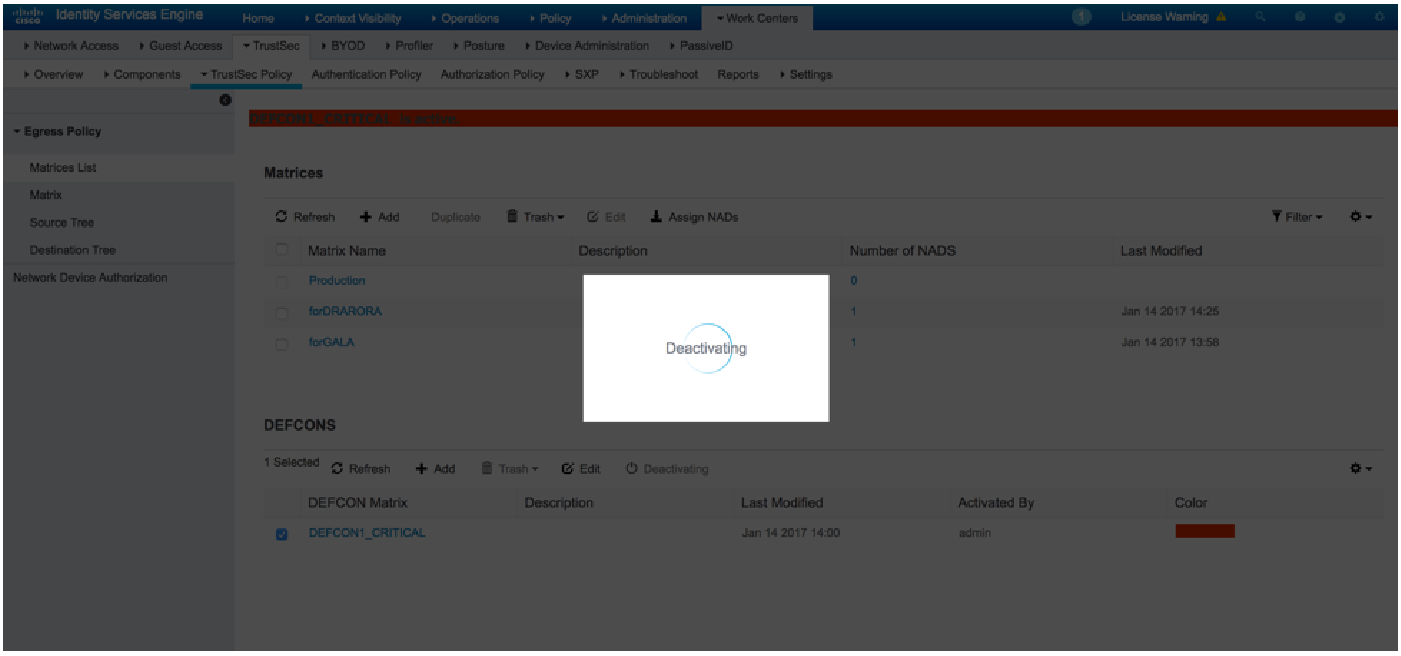
E i criteri sugli switch:

```
GALA#show cts role-based permissions
IPv4 Role-based permissions default:
Permit IP-00
IPv4 Role-based permissions from group 15:BYOD to group 10:Point_of_Sale_Systems:
denyIP-20
IPv4 Role-based permissions from group 15:BYOD to group 16:VLAN10:
denyIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 16:VLAN10:
denyIP-20
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

DRARORA#show cts role-based permissions
IPv4 Role-based permissions default:
Permit IP-00
IPv4 Role-based permissions from group 15:BYOD to group 10:Point_of_Sale_Systems:
denyIP-20
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 17:VLAN20:
permitIP-20
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

Il traffico tra la SGT 15 e la SGT 10 non è consentito su entrambi gli switch:

```
DRARORA#ping 10.10.10.10 source Loopback 15
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
Packet sent with a source address of 15.15.15.15
U.U.U
Success rate is 0 percent (0/5)

GALA#ping 7.7.7.7 source Loopback 2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 7.7.7.7, timeout is 2 seconds:
Packet sent with a source address of 2.2.2.2
U.U.U
Success rate is 0 percent (0/5)
```

Una volta che la distribuzione è nuovamente stabile, è possibile disattivare DefCon e gli switch richiedono le vecchie policy. Per disattivare DefCon, passare a **Centri di lavoro > TrustSec > Criteri TrustSec > Criteri di uscita > Elenco matrici**, controllare la matrice DefCon attiva e fare clic su **Disattiva**:



DEFCON1_CRITICAL is active.

Matrices

	Matrix Name	Description	Number of NADS	Last Modified
□	Production		0	
□	forDRARORA		1	Jan 14 2017 14:25
□	forGALA		1	Jan 14 2017 13:58

Deactivating

DEFCONS

	DEFCON Matrix	Description	Last Modified	Activated By	Color
☑	DEFCON1_CRITICAL		Jan 14 2017 14:00	admin	🟥

Entrambi gli switch richiedono immediatamente le vecchie policy:

```
DRARORA#show cts role-based permissions
IPv4 Role-based permissions default:
Permit IP-00
IPv4 Role-based permissions from group 17:VLAN20 to group 10:Point_of_Sale_Systems:
permitIP-20
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 15:BYOD:
permitIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 15:BYOD:
permitIP-20
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 17:VLAN20:
denyIP-20
IPv4 Role-based permissions from group 16:VLAN10 to group 17:VLAN20:
permitIP-20
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

GALA#show cts role-based permissions
IPv4 Role-based permissions default:
Permit IP-00
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 15:BYOD:
denyIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 15:BYOD:
permitIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 16:VLAN10:
permitIP-20
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

Risoluzione dei problemi

preparazione PAC

Questa operazione fa parte della procedura di preparazione PAC:

```
GALA#debug cts provisioning packets
GALA#debug cts provisioning events

*Jan  2 04:39:05.707: %SYS-5-CONFIG_I: Configured from console by console
*Jan  2 04:39:05.707: CTS-provisioning: Starting new control block for server 10.48.17.161:
*Jan  2 04:39:05.707: CTS-provisioning: cts_provi_init_socket: Checking for any vrf associated
with 10.48.17.161
*Jan  2 04:39:05.707: CTS-provisioning: New session socket: src=10.48.72.156:65242
dst=10.48.17.161:1812
*Jan  2 04:39:05.716: CTS-provisioning: cts_provi_init_socket: Checking for any vrf associated
with 10.48.17.161
*Jan  2 04:39:05.716: CTS-provisioning: cts_provi_init_socket: Adding vrf-tableid: 0 to socket
*Jan  2 04:39:05.716: CTS-provisioning: New session socket: src=10.48.72.156:65242
dst=10.48.17.161:1812
*Jan  2 04:39:05.716: CTS-provisioning: Sending EAP Response/Identity to 10.48.17.161
*Jan  2 04:39:05.716: CTS-provisioning: OUTGOING RADIUS msg to 10.48.17.161:
1E010EE0:          01010090 64BCBC01 7BEF347B
1E010EF0: 1E32C02E 8402A83D 010C4354 5320636C
1E010F00: 69656E74 04060A30 489C3D06 00000000
1E010F10: 06060000 00021F0E 30303037 37643862
1E010F20: 64663830 1A2D0000 00090127 4141413A
1E010F30: 73657276 6963652D 74797065 3D637473
1E010F40: 2D706163 2D70726F 76697369 6F6E696E
1E010F50: 674F1102 00000F01 43545320 636C6965
1E010F60: 6E745012 73EBE7F5 CDA0CF73 BFE4AFB6
1E010F70: 40D723B6 00
*Jan  2 04:39:06.035: CTS-provisioning: INCOMING RADIUS msg from 10.48.17.161:
1EC68460:          0B0100B5 E4C3C3C1 ED472766
1EC68470: 183F41A9 026453ED 18733634 43504D53
1EC68480: 65737369 6F6E4944 3D306133 30313161
1EC68490: 314C3767 78484956 62414976 37316D59
1EC684A0: 525F4D56 34517741 4C362F69 73517A72
1EC684B0: 7A586132 51566852 79635638 3B343353
1EC684C0: 65737369 6F6E4944 3D766368 72656E65
1EC684D0: 6B2D6973 6532322D 3432332F 32373238
1EC684E0: 32373637 362F3137 37343B4F 1C017400
1EC684F0: 1A2B2100 040010E6 796CD7BB F2FA4111
1EC68500: AD9FB4FE FB5A5050 124B76A2 E7D34684
1EC68510: DD8A1583 175C2627 9F00
*Jan  2 04:39:06.035: CTS-provisioning: Received RADIUS challenge from 10.48.17.161.
*Jan  2 04:39:06.035: CTS-provisioning: A-ID for server 10.48.17.161 is
"e6796cd7bbf2fa4111ad9fb4fefb5a50"
*Jan  2 04:39:06.043: CTS-provisioning: Received TX_PKT from EAP method
*Jan  2 04:39:06.043: CTS-provisioning: Sending EAPFAST response to 10.48.17.161
*Jan  2 04:39:06.043: CTS-provisioning: OUTGOING RADIUS msg to 10.48.17.161:
<...>
*Jan  2 04:39:09.549: CTS-provisioning: INCOMING RADIUS msg from 10.48.17.161:
1EC66C50:          0309002C 1A370BBB 58B828C3
1EC66C60: 3F0D490A 4469E8BB 4F06047B 00045012
1EC66C70: 7ECF8177 E3F4B9CB 8B0280BD 78A14CAA
1EC66C80: 4D
*Jan  2 04:39:09.549: CTS-provisioning: Received RADIUS reject from 10.48.17.161.
*Jan  2 04:39:09.549: CTS-provisioning: Successfully obtained PAC for A-ID
e6796cd7bbf2fa4111ad9fb4fefb5a50
```

Rifiuto RADIUS previsto. Provisioning PAC completato.

Download dati ambiente

Ciò indica che il download dei dati di ambiente dallo switch è riuscito:

```
GALA#debug cts environment-data

GALA#
*Jan  2 04:33:24.702: CTS env-data: Force environment-data refresh
*Jan  2 04:33:24.702: CTS env-data: download transport-type = CTS_TRANSPORT_IP_UDP
*Jan  2 04:33:24.702:     cts_env_data START: during state env_data_complete, got event
0(env_data_request)

*Jan  2 04:33:24.702: cts_aaa_attr_add: AAA req(0x5F417F8)
*Jan  2 04:33:24.702:   username = #CTSREQUEST#
*Jan  2 04:33:24.702: cts_aaa_context_add_attr: (CTS env-data SM)attr(GALA)
*Jan  2 04:33:24.702:   cts-environment-data = GALA
*Jan  2 04:33:24.702: cts_aaa_attr_add: AAA req(0x5F417F8)
*Jan  2 04:33:24.702: cts_aaa_context_add_attr: (CTS env-data SM)attr(env-data-fragment)
*Jan  2 04:33:24.702:   cts-device-capability = env-data-fragment
*Jan  2 04:33:24.702: cts_aaa_req_send: AAA req(0x5F417F8) successfully sent to AAA.
*Jan  2 04:33:25.474: cts_aaa_callback: (CTS env-data SM)AAA req(0x5F417F8) response success
*Jan  2 04:33:25.474: cts_aaa_context_fragment_cleanup: (CTS env-data SM)attr(GALA)
*Jan  2 04:33:25.474: cts_aaa_context_fragment_cleanup: (CTS env-data SM)attr(env-data-fragment)

*Jan  2 04:33:25.474:   AAA attr: Unknown type (450).
*Jan  2 04:33:25.474:   AAA attr: Unknown type (274).
*Jan  2 04:33:25.474:   AAA attr: server-list = CTSServerList1-0001.
*Jan  2 04:33:25.482:   AAA attr: security-group-tag = 0000-10.
*Jan  2 04:33:25.482:   AAA attr: environment-data-expiry = 86400.
*Jan  2 04:33:25.482:   AAA attr: security-group-table = 0001-19.
*Jan  2 04:33:25.482: CTS env-data: Receiving AAA attributes
  CTS_AAA_SLIST
    slist name(CTSServerList1) received in 1st Access-Accept
    slist name(CTSServerList1) created
  CTS_AAA_SECURITY_GROUP_TAG - SGT = 0-10:unicast-unknown
  CTS_AAA_ENVIRONMENT_DATA_EXPIRY = 86400.
  CTS_AAA_SGT_NAME_LIST
    table(0001) received in 1st Access-Accept
    need a 2nd request for the SGT to SG NAME entries
    new name(0001), gen(19)
  CTS_AAA_DATA_END

*Jan  2 04:33:25.784: cts_aaa_callback: (CTS env-data SM)AAA req(0x8853E60) response success
*Jan  2 04:33:25.784: cts_aaa_context_fragment_cleanup: (CTS env-data SM)attr(0001)
*Jan  2 04:33:25.784:   AAA attr: Unknown type (450).
*Jan  2 04:33:25.784:   AAA attr: Unknown type (274).
*Jan  2 04:33:25.784:   AAA attr: security-group-table = 0001-19.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = 0-10-00-Unknown.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = ffff-13-00-ANY.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = 9-10-00-Auditors.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = f-32-00-BYOD.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = 5-10-00-Contractors.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = 8-10-00-Developers.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = c-10-00-Development_Servers.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = 4-10-00-Employees.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = 6-10-00-Guests.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = 3-10-00-Network_Services.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = e-10-00-PCI_Servers.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = a-23-00-Point_of_Sale_Systems.
*Jan  2 04:33:25.784:   AAA attr: security-group-info = b-10-00-Production_Servers.
*Jan  2 04:33:25.793:   AAA attr: security-group-info = 7-10-00-Production_Users.
```

```
*Jan  2 04:33:25.793:   AAA attr: security-group-info = ff-10-00-Quarantined_Systems.
*Jan  2 04:33:25.793:   AAA attr: security-group-info = d-10-00-Test_Servers.
*Jan  2 04:33:25.793:   AAA attr: security-group-info = 2-10-00-TrustSec_Devices.
*Jan  2 04:33:25.793:   AAA attr: security-group-info = 10-24-00-VLAN10.
*Jan  2 04:33:25.793:   AAA attr: security-group-info = 11-22-00-VLAN20.
*Jan  2 04:33:25.793:  CTS env-data: Receiving AAA attributes
  CTS_AAA_SGT_NAME_LIST
    table(0001) received in 2nd Access-Accept
    old name(0001), gen(19)
    new name(0001), gen(19)
  CTS_AAA_SGT_NAME_INBOUND - SGT = 0-68:unicast-unknown
   flag (128) sgname (Unknown) added
   name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sgname, name = 0001, req = 1, rcv = 1
   Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
  CTS_AAA_SGT_NAME_INBOUND - SGT = 65535-68:unicast-default
   flag (128) sgname (ANY) added
   name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sgname, name = 0001, req = 1, rcv = 1
   Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
  CTS_AAA_SGT_NAME_INBOUND - SGT = 9-68
   flag (128) sgname (Auditors) added
   name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sgname, name = 0001, req = 1, rcv = 1
   Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
  CTS_AAA_SGT_NAME_INBOUND - SGT = 15-68
   flag (128) sgname (BYOD) added
   name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sgname, name = 0001, req = 1, rcv = 1
   Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
  CTS_AAA_SGT_NAME_INBOUND - SGT = 5-68
   flag (128) sgname (Contractors) added
   name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sgname, name = 0001, req = 1, rcv = 1
   Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
  CTS_AAA_SGT_NAME_INBOUND - SGT = 8-68
   flag (128) sgname (Developers) added
   name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sgname, name = 0001, req = 1, rcv = 1
   Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
  CTS_AAA_SGT_NAME_INBOUND - SGT = 12-68
   flag (128) sgname (Development_Servers) added
   name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sgname, name = 0001, req = 1, rcv = 1
   Setting SG Name receving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
  CTS_AAA_SGT_NAME_INBOUND - SGT = 4-68
   flag (128) sgname (Employees) added
   name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sgname, na
*Jan  2 04:33:25.793:     cts_env_data WAITING_RESPONSE: during state env_data_waiting_rsp, got
event 1(env_data_received)
*Jan  2 04:33:25.793: @@@ cts_env_data WAITING_RESPONSE: env_data_waiting_rsp ->
env_data_assessing
*Jan  2 04:33:25.793: env_data_assessing_enter: state = ASSESSING
*Jan  2 04:33:25.793: cts_aaa_is_fragmented: (CTS env-data SM)NOT-FRAG attr_q(0)
*Jan  2 04:33:25.793: env_data_assessing_action: state = ASSESSING
*Jan  2 04:33:25.793: cts_env_data_is_complete: FALSE, req(x1085), rec(x1487)
*Jan  2 04:33:25.793: cts_env_data_is_complete: TRUE, req(x1085), rec(x1487), expect(x81),
complete1(x85), complete2(xB5), complete3(x1485)
*Jan  2 04:33:25.793:     cts_env_data ASSESSING: during state env_data_assessing, got event
4(env_data_complete)
*Jan  2 04:33:25.793: @@@ cts_env_data ASSESSING: env_data_assessing -> env_data_complete
*Jan  2 04:33:25.793: env_data_complete_enter: state = COMPLETE
*Jan  2 04:33:25.793: env_data_install_action: state = COMPLETE
```

criteri CTS

Poiché i criteri CTS vengono inseriti come parte dei messaggi RADIUS, il componente di registrazione **runtime-AAA** impostato su debug su ISE (**Amministrazione > Registrazione > Configurazione registro di debug**) e i debug di livello inferiore sullo switch devono essere sufficienti per risolvere i problemi relativi a CTS:

```
debug cts coa
debug radius
```

Verificare inoltre le policy corrispondenti sullo switch - su switch 3750X:

```
GALA#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

10      15      5               0               0               0

*       *       0               0               815             31

17      15      0               0               0               0
17      16      0               -               0               -
```

Non è possibile usare lo stesso comando su 3850 a causa di CiscobugID CSCuu32958.