Configurez les plusieurs matrices de TrustSec sur ISE 2.2

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Informations générales
Plusieurs matrices
Matrices de DefCon
Configurez
Diagramme du réseau
Configurations
1. Configuration de base du commutateur pour RADIUS/CTS
2. CTS PAC
3. Configuration CTS sur un commutateur.
4. Configuration de base CTS sur ISE.
5. Plusieurs matrices et configuration de DefCon sur ISE.
6. Classification SGT
7. Téléchargement de stratégie CTS
Vérifiez
Plusieurs matrices
Déploiement de DefCon
Dépannez
Ravitaillement PAC
Téléchargement de données d'environnement
Stratégies CTS

Introduction

Ce document décrit l'utilisation de plusieurs matrices de TrustSec et de matrices de DefCon dans le Logiciel Cisco Identity Services Engine (ISE) 2.2. C'est une nouvelle fonctionnalité introduite de TrustSec dans ISE 2.2 pour une meilleure finesse dans le réseau.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base des composants du Cisco TrustSec (CTS)

- Connaissance de base de configuration CLI des Commutateurs de Catalyst
- Expérience avec la configuration du Cisco Identity Services Engine (ISE)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Dans ISE 2.0 il y a une possibilité pour utiliser seulement une matrice de TrustSec de production pour tous les périphériques de réseau. La caractéristique ajoutée ISE 2.1 a appelé la matrice de mise en place qui peut être utilisée pour des buts de test et d'implémentation. Des stratégies créées dans la matrice de mise en place sont appliquées seulement aux périphériques de réseau utilisés pour des tests. Le reste des périphériques utilisent toujours la matrice de production. Une fois que la matrice de présentation est confirmée pour fonctionner bien, tous autres périphériques peuvent être déplacés à elle et ce devient nouvelle matrice de production.

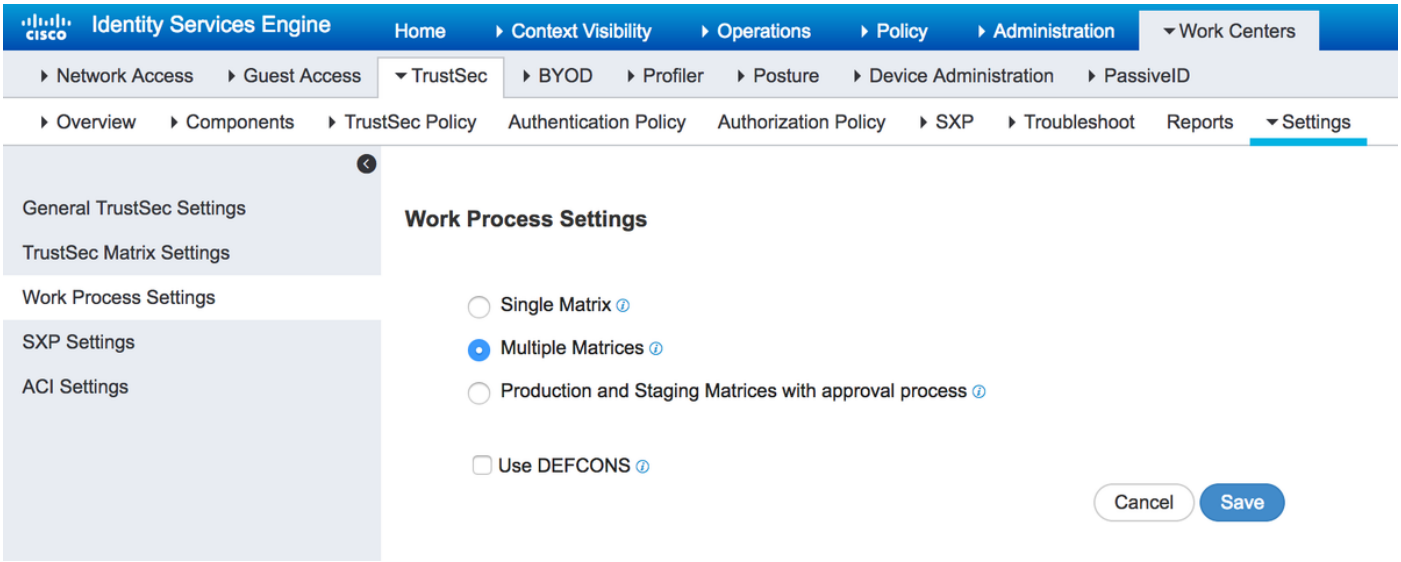
ISE 2.2 est livré avec deux nouvelles configurations de TrustSec :

1. Plusieurs matrices - capacité d'assigner différentes matrices aux périphériques de réseau
2. Matrice de DefCon - cette matrice est poussée à toute la situation de périphériques de réseau en particulier, déclenchée par l'administrateur

Il est possible d'utiliser la caractéristique simple de matrice ou la caractéristique de matrice de production et de mise en place dans ISE 2.2.

Plusieurs matrices

Afin d'utiliser de plusieurs matrices, vous devez activer cette option sous des **centres de travail > TrustSec > des configurations > des configurations de processus de travail**, suivant les indications de l'image :



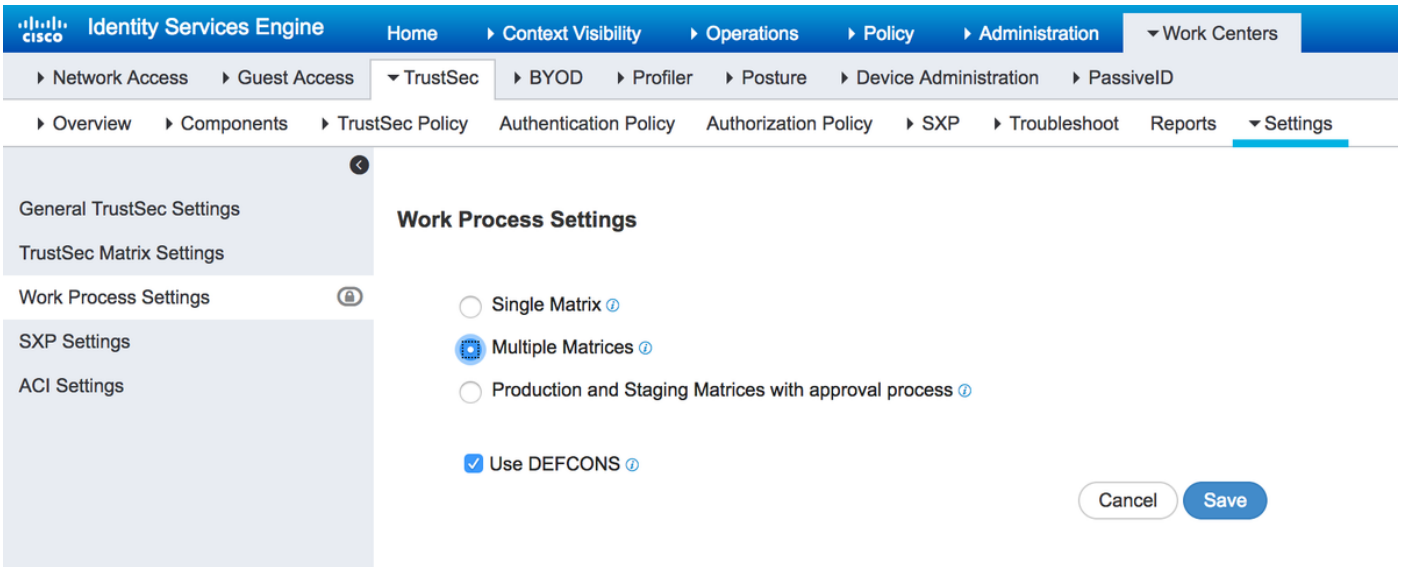
Une fois que ceci est activé, vous pouvez créer de nouvelles matrices et plus tard assigner des périphériques de réseau à la matrice spécifique.

Matrices de DefCon

Les matrices de DefCon sont les matrices spéciales, prêtes à être déployé à tout moment. Une fois déployés, tous les périphériques de réseau sont automatiquement assignés à cette matrice. ISE se souvient toujours la dernière matrice de production pour tous les périphériques de réseau, ainsi cette modification peut être retournée de retour à un point quelconque quand DefCon est désactivé. Vous pouvez définir jusqu'à quatre matrices différentes de DefCon :

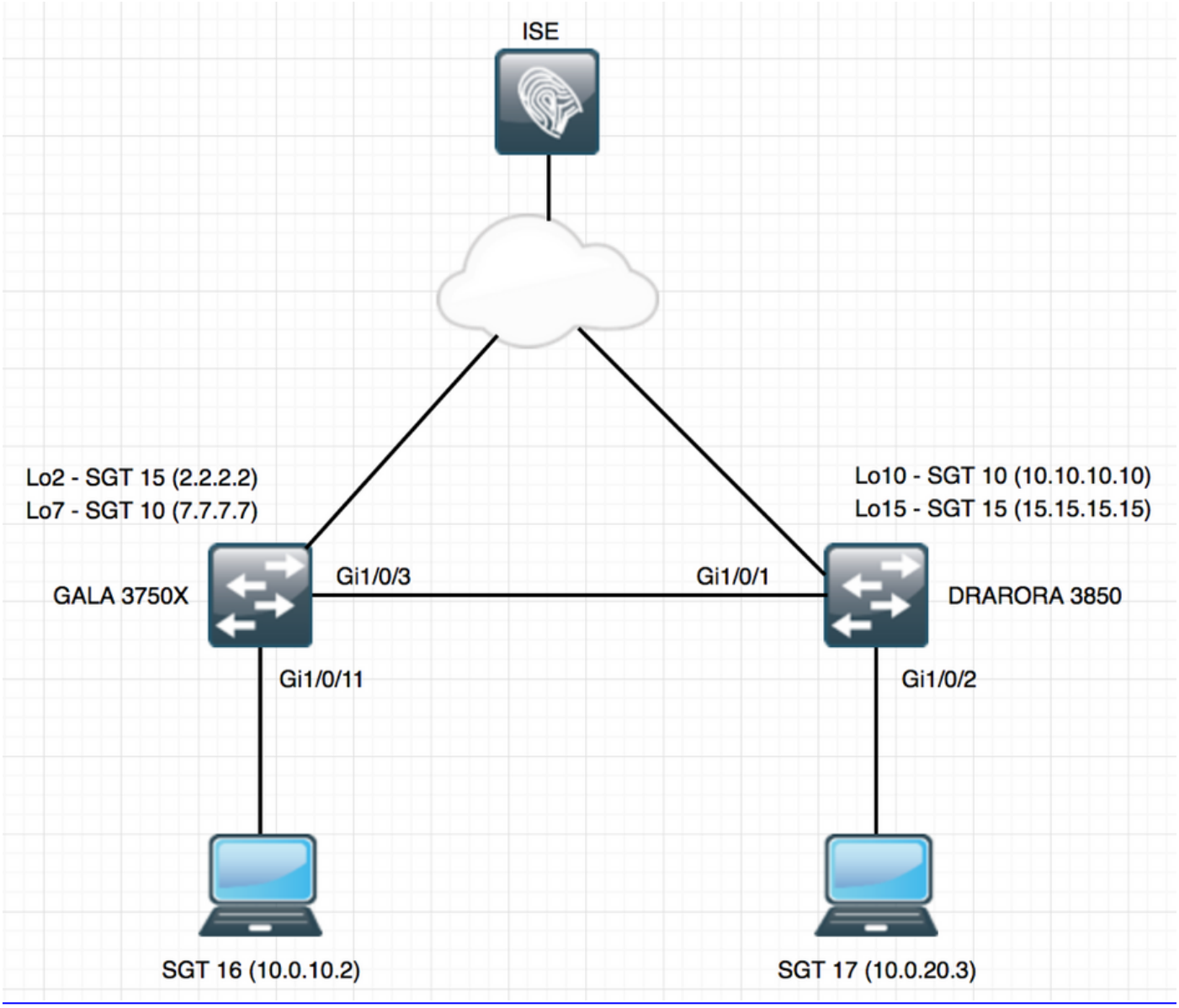
1. DefCon1 - Essentiel
2. DefCon2 - Grave
3. DefCon3 - Substantiel
4. DefCon4 - Modéré

Des matrices de DefCon peuvent être utilisées en combination avec chacune des trois options de processus de travail :



Configurez

Diagramme du réseau



Configurations

Afin d'utiliser de plusieurs matrices, vous devez l'activer sous des configurations de procédé de travail. Dans cet exemple, activez également la matrice de DefCon.

1. Configuration de base du commutateur pour 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
```

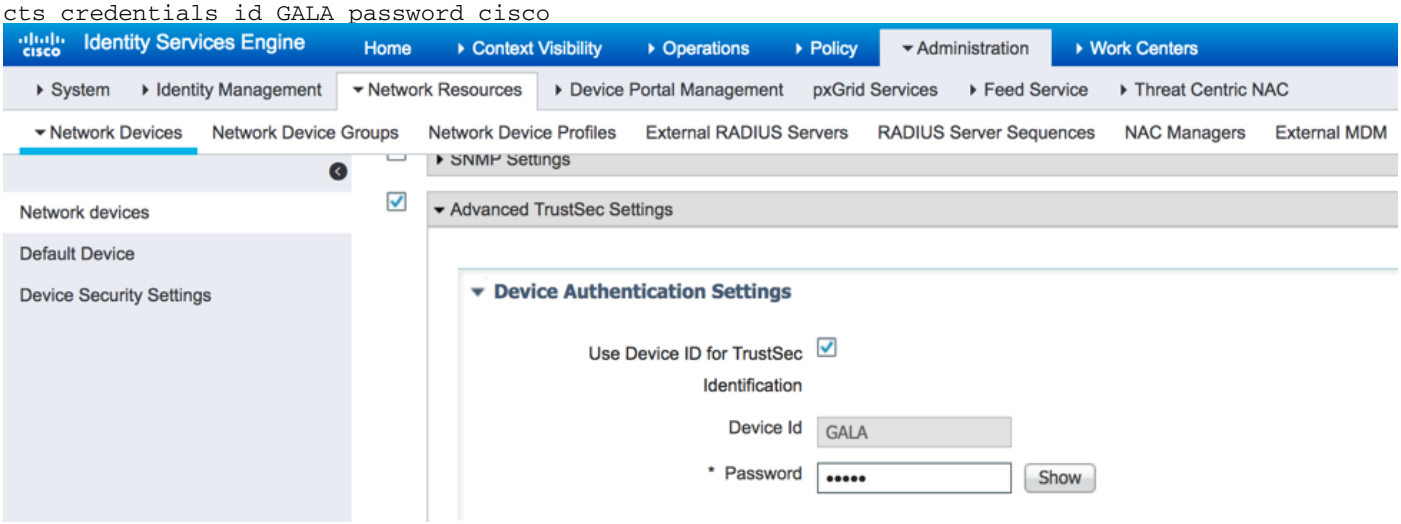
Afin d'obtenir les informations CTS, vous devez créer la liste d'autorisation CTS :

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

2. CTS PAC

Pour recevoir CTS PAC (qualifications de Protected Access) d'ISE, vous devez configurer les mêmes qualifications sur le commutateur et ISE sous la configuration avancée de TrustSec pour le périphérique de réseau :

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



Une fois que ceci est configuré, un commutateur peut télécharger CTS PAC. Une part de lui (PAC-opaque) est envoyée comme paire AV dans chaque demande RADIUS à ISE, ainsi comme ISE peut vérifier si le PAC pour ce périphérique de réseau est encore valide :

```
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:
000200B00003000100040010E6796CD7BBF2FA4111AD9FB4FEFB5A5000060094000301001 2FABE10F3DCBCB152C54FA5
BFE124CB00000013586BB31500093A809E11A93189C7BE6EBDFB8FDD15B9B7252EB741ADCA3B2ACC5FD923AEB7BDFE48
A3A771338926A1F48141AF091469EE4AFC8C3E92A510BA214A407A33F469282A780E8F50F17A271E92D1FEE1A29ED427
B985F9A0E00D6CDC934087716F4DEAF84AC11AA05F7587E898CA908463BDA9EC7E65D827 Refresh timer is set
for 11y13w
```

3. Configuration CTS sur un commutateur.

Une fois que le PAC est téléchargé, le commutateur peut demander les informations supplémentaires CTS (des environnement-données et des stratégies) :

```
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
```

Vous pourriez voir qu'il n'y a aucune stratégie étant téléchargée d'ISE, la raison est que l'application CTS n'est pas activée sur le commutateur :

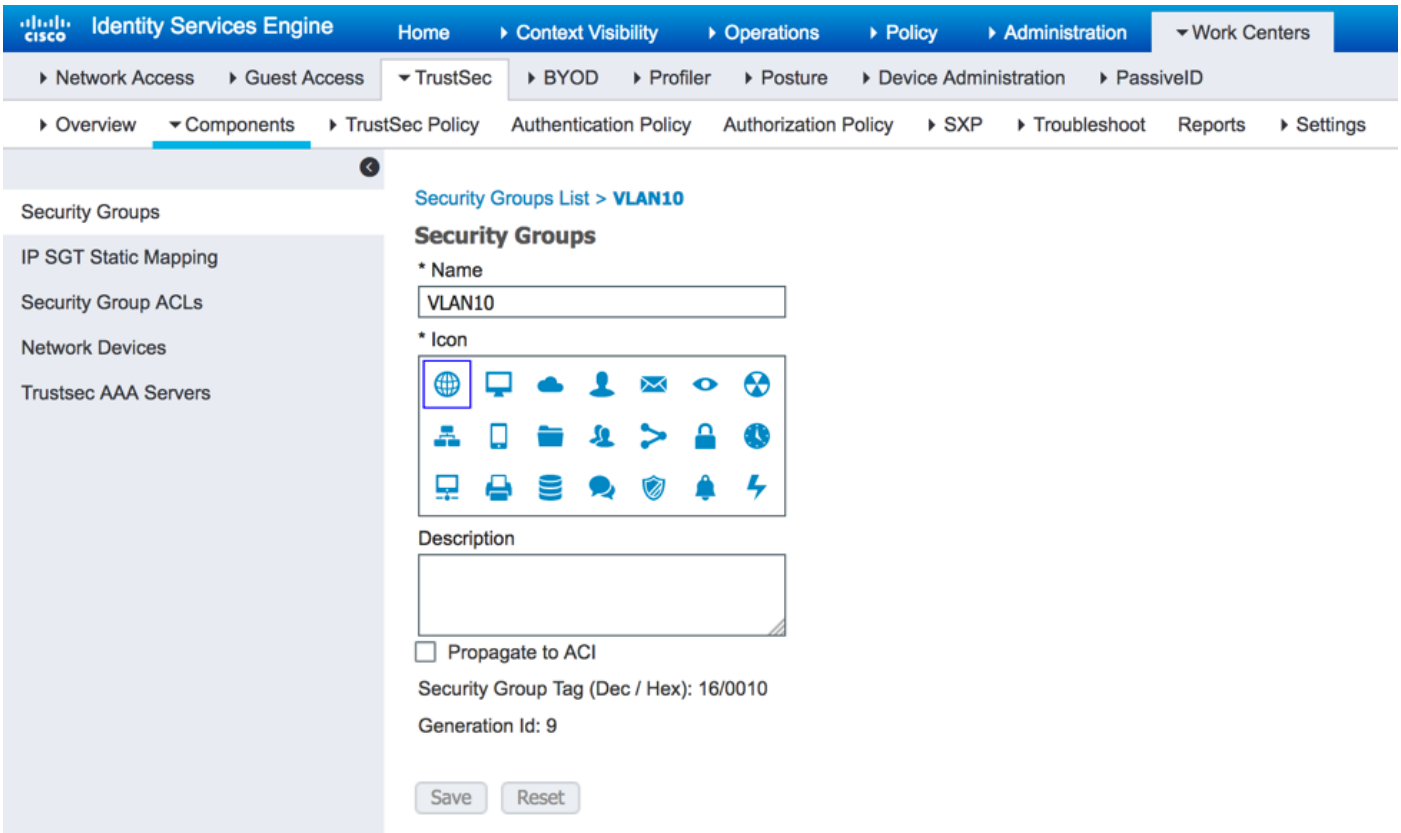
```
cts role-based enforcement
cts role-based enforcement vlan-list 1-4094

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
```

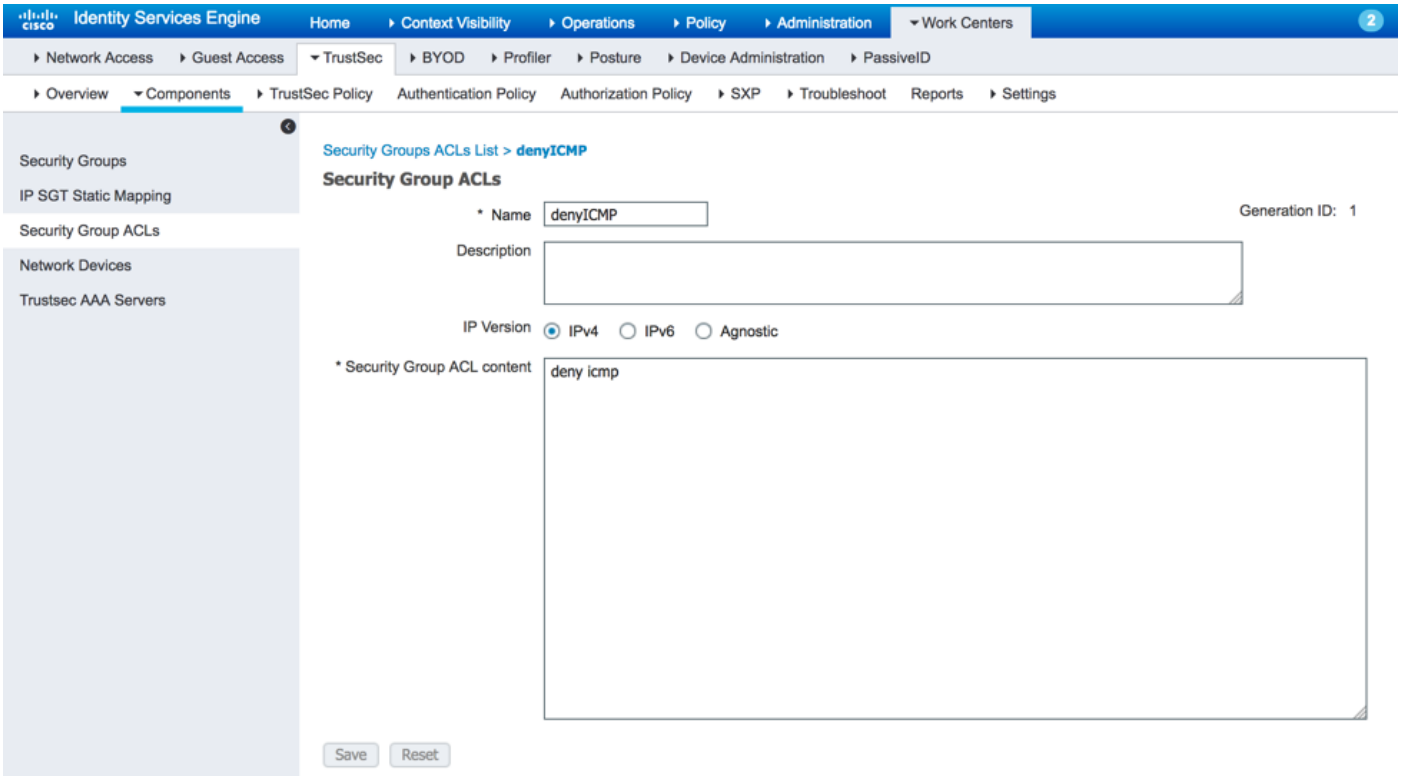
Dans les deux sorties, vous pourriez voir des valeurs par défaut - SGTs créé par le par défaut (0, 2-15, 255) et la stratégie **IP d'autorisation de** par défaut.

4. Configuration de base CTS sur ISE.

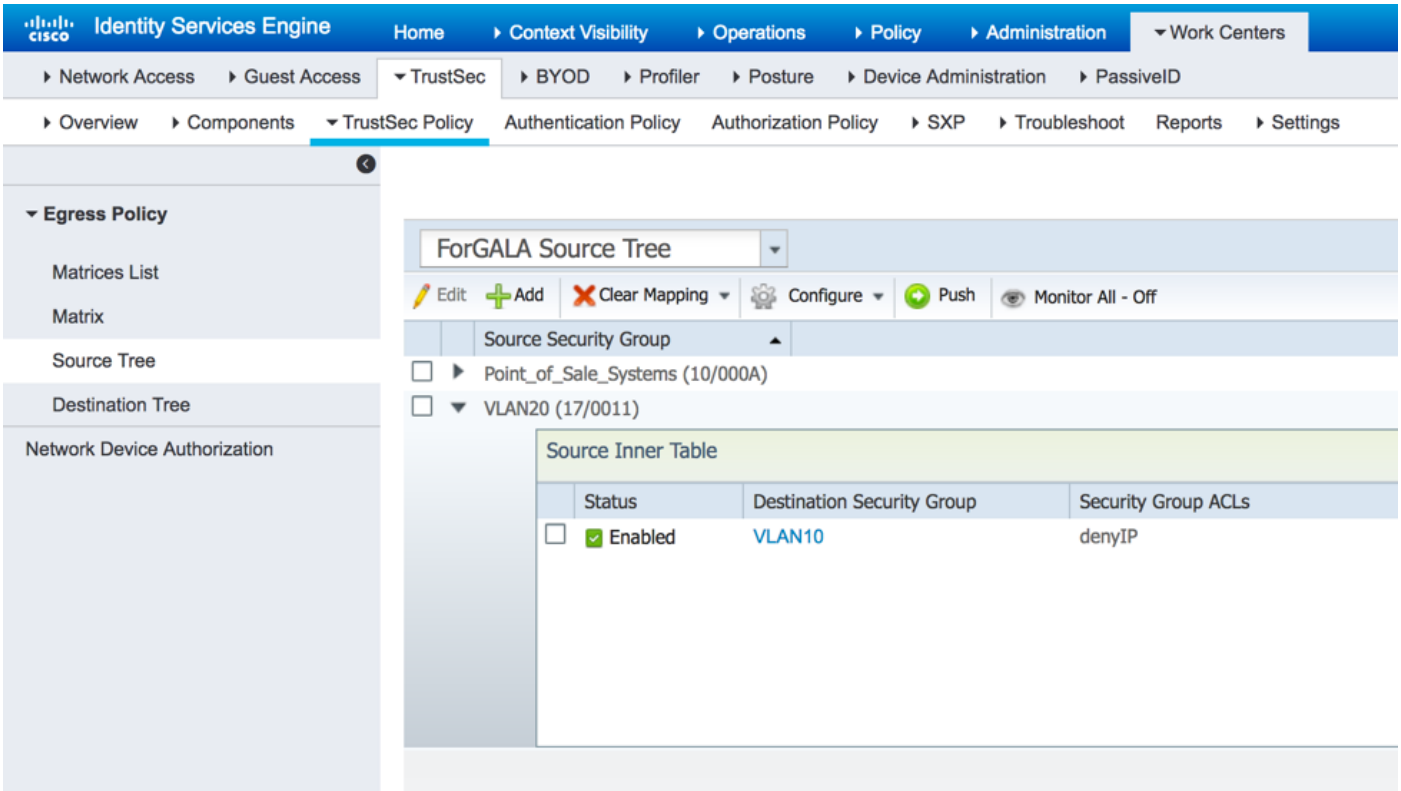
Créez les nouvelles balises de groupe de sécurité (SGTs) et peu de stratégies sur ISE afin de les utiliser plus tard. Naviguez vers des **centres de travail > TrustSec > des composants > des groupes de sécurité**, cliquez sur Add pour créer nouveau SGT :



Pour créer la liste de contrôle d'accès de groupe de sécurité (SGACL) pour le filtrage de trafic, choisissez le **groupe de sécurité ACLs**, suivant les indications de l'image :



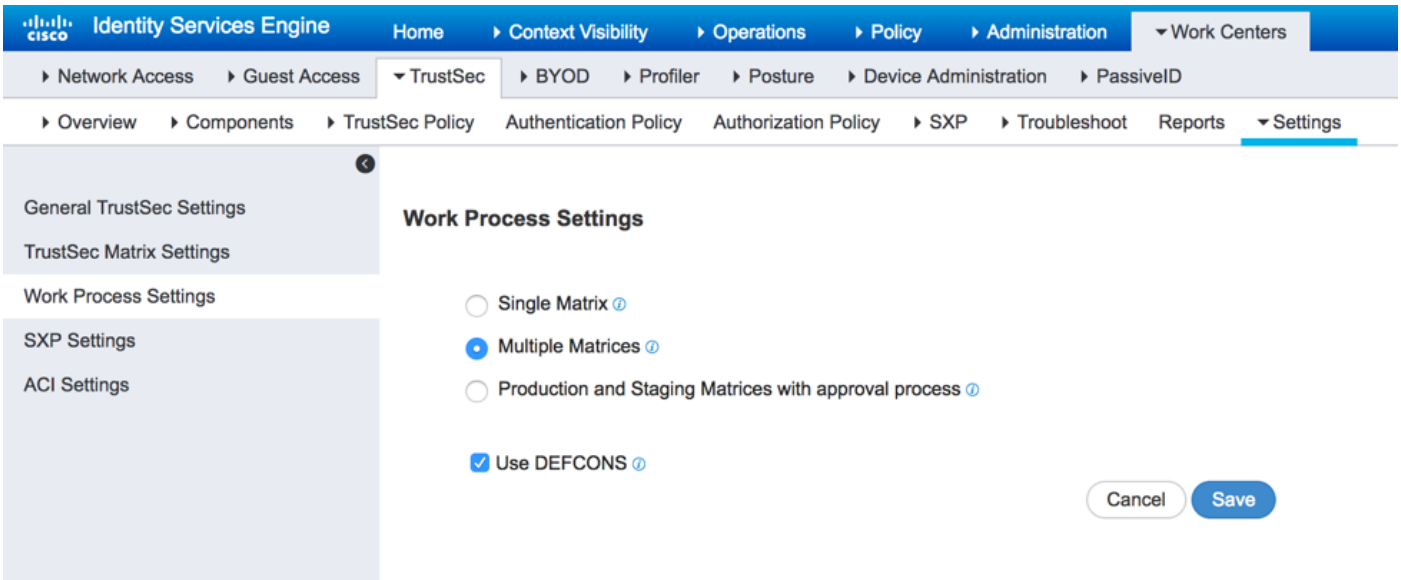
De même, vous pouvez créer l'autres SGTs et SGACLs. Une fois que SGTs et SGACLs sont créés, vous pouvez les attacher ensemble dans des stratégies CTS, pour faire naviguez ainsi **arborescence** vers des **centres de travail > la stratégie de TrustSec > de TustSec > de sortie stratégie > source**, suivant les indications de l'image :



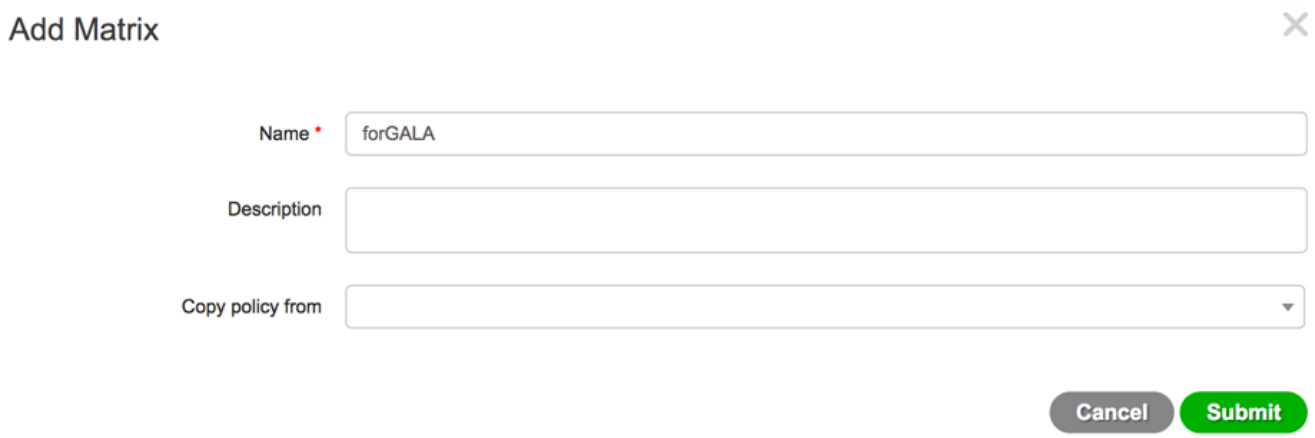
5. Plusieurs matrices et configuration de DefCon sur ISE.

Dans cet exemple, vous avez configuré des stratégies pour la matrice **ForGALA**. Afin de commuter entre les matrices, vous pouvez utiliser le menu déroulant. Afin d'activer de plusieurs matrices, naviguez vers des **centres de travail > TrustSec > des configurations > des**

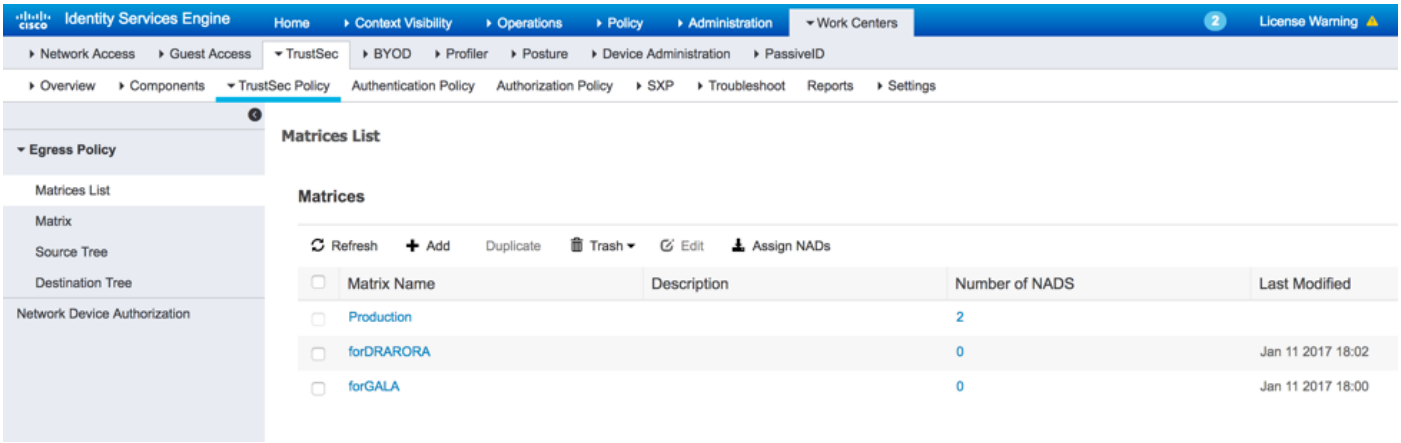
configurations de processus de travail et activez les plusieurs matrices de matrices et de DefCon, suivant les indications de l'image :



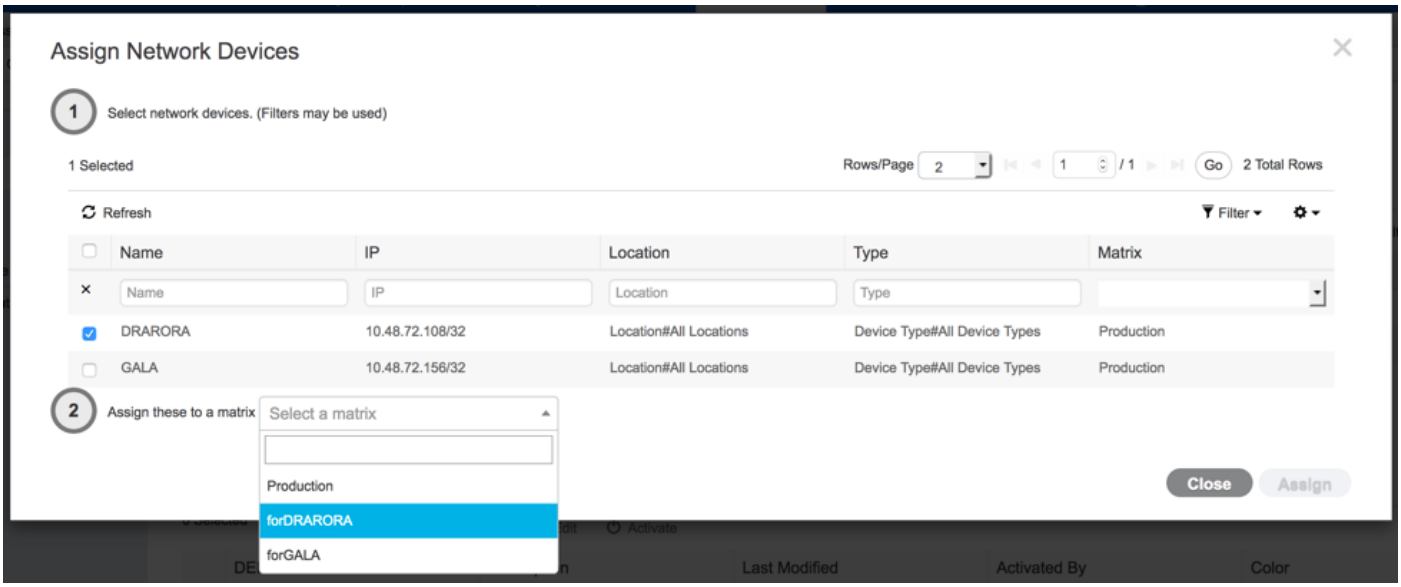
Quand cette option est activée, il y a matrice par défaut de production disponible, bien que vous puissiez créer d'autres matrices. Naviguez vers des **centres de travail > TrustSec > stratégie de TrustSec > stratégie > des matrices de sortie les répertorient** et cliquent sur Add :



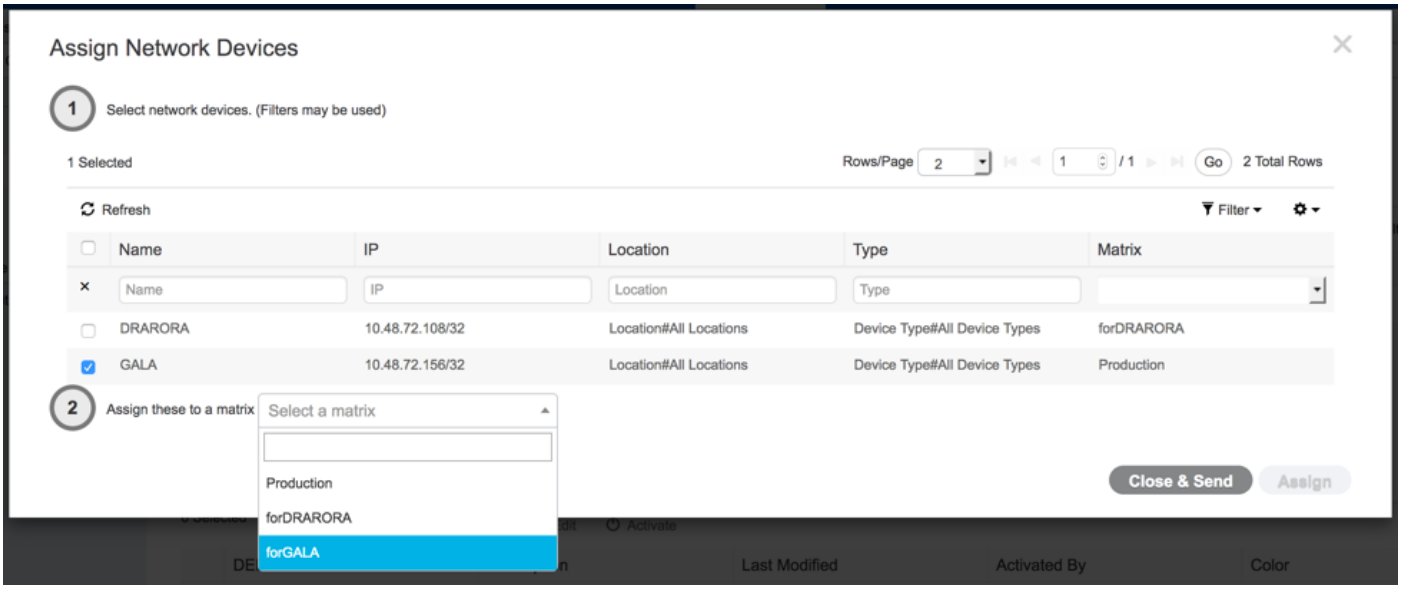
Il y a une option de copier les stratégies qui devraient devenir une partie du neuf de la matrice déjà existante. Créez deux matrices - une pour le commutateur 3750X, un autre pour le commutateur 3850. Une fois que des matrices sont créées, vous devez assigner des périphériques de réseau à ces matrices, parce que par défaut tout le TrustSec activé des périphériques d'accès au réseau sont assignés à la matrice de production.



Pour assigner NADs, le clic **assignent l'**option de **NADs** sous la liste de matrices, vérifient le périphérique que vous voudriez assigner la matrice à et sélectionner la matrice créée du menu déroulant et du clic **assignez**, suivant les indications de l'image :

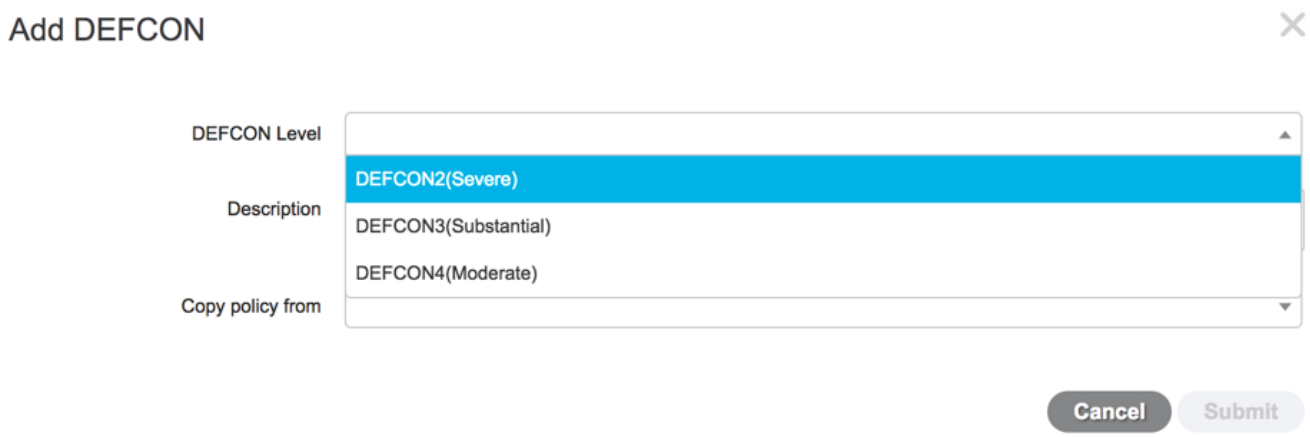


Vous pouvez faire la même chose pour d'autres périphériques, suivi du clic sur le bouton **Assign** :

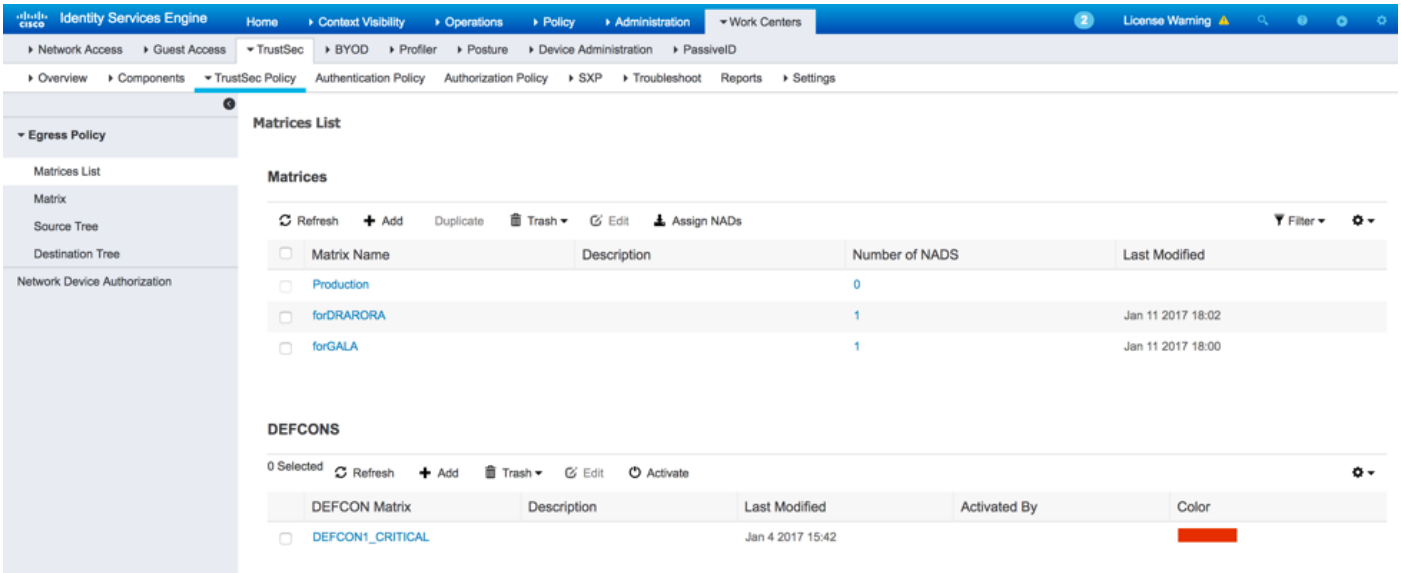


Une fois que toutes les modifications sont exécutées, cliquez sur en fonction **Close&Send**, qui envoie toutes les mises à jour aux périphériques pour exécuter une régénération des stratégies CTS afin de télécharger des neufs. De même, créez la matrice de DefCon, que vous pouvez

copier des matrices existantes :



Les stratégies finales ressemblent à :

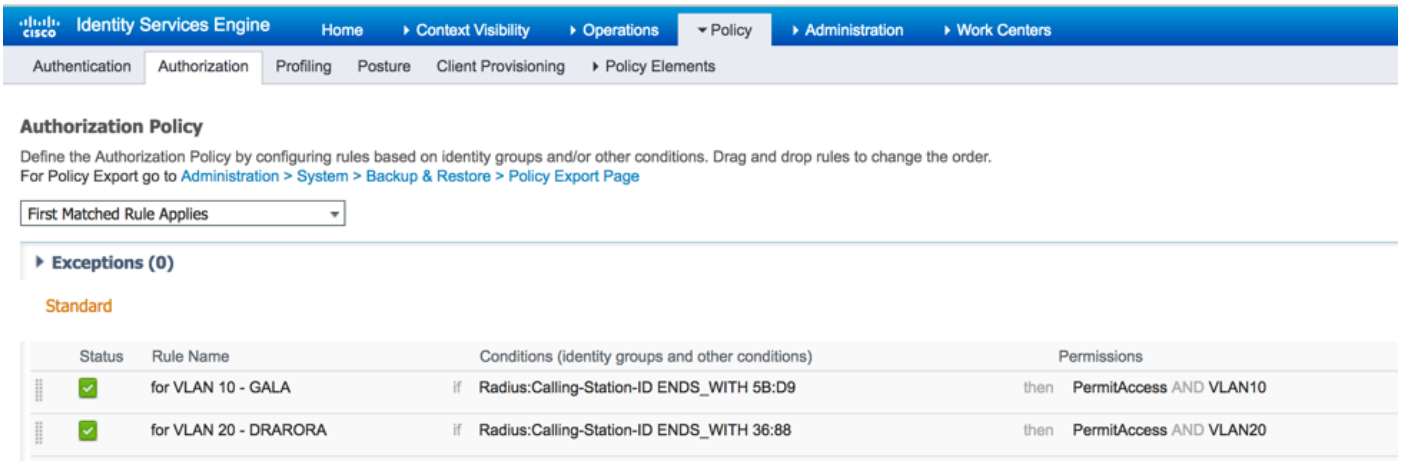


6. Classification SGT

Il y a deux options pour des balises aux affectations de clients (créez les mappages IP-SGT) :

- *statique* - avec la ***balise de*** **sgt d'*IP_address de* cts role-based sgt-map**
- *dynamique* - par l'intermédiaire de l'authentification de dot1x (la balise est assignée en raison de l'authentification réussie)

Utilisez les deux options ici, deux ordinateurs de fenêtres obtiennent la balise SGT par l'intermédiaire des interfaces d'authentification et de bouclage de dot1x avec la balise statique SGT. Pour déployer le mappage dynamique, créez les stratégies d'autorisation pour des clients d'extrémité :



Pour créer le mappage statique IP-SGT, l'utilisation commande (exemple pour le commutateur de 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
```

Après l'authentification réussie, le client frappe la stratégie d'autorisation avec la balise de la particularité SGT dans un résultat :

```
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
```

Vous pouvez vérifier tous les mappages avec le **show cts role-based sgt-map tous** IP-SGT de commande, où vous voyez la source de chaque mappage (GENS DU PAYS - par l'intermédiaire de l'authentification de dot1x, CLI - affectation statique) :

```
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. Téléchargement de stratégie CTS

Une fois que le commutateur a CTS PAC et données d'environnement est téléchargé, il peut demander des stratégies CTS. Le commutateur ne télécharge pas toutes les stratégies, mais seulement ceux qui sont exigées - des stratégies pour le trafic destiné aux balises connues SGT - en cas de commutateur de GALA, il demande à ISE ces stratégies :

- stratégie pour le trafic à SGT 15
- stratégie pour le trafic à SGT 10
- stratégie pour le trafic à SGT 16

La sortie de toutes les stratégies pour le commutateur de GALA :

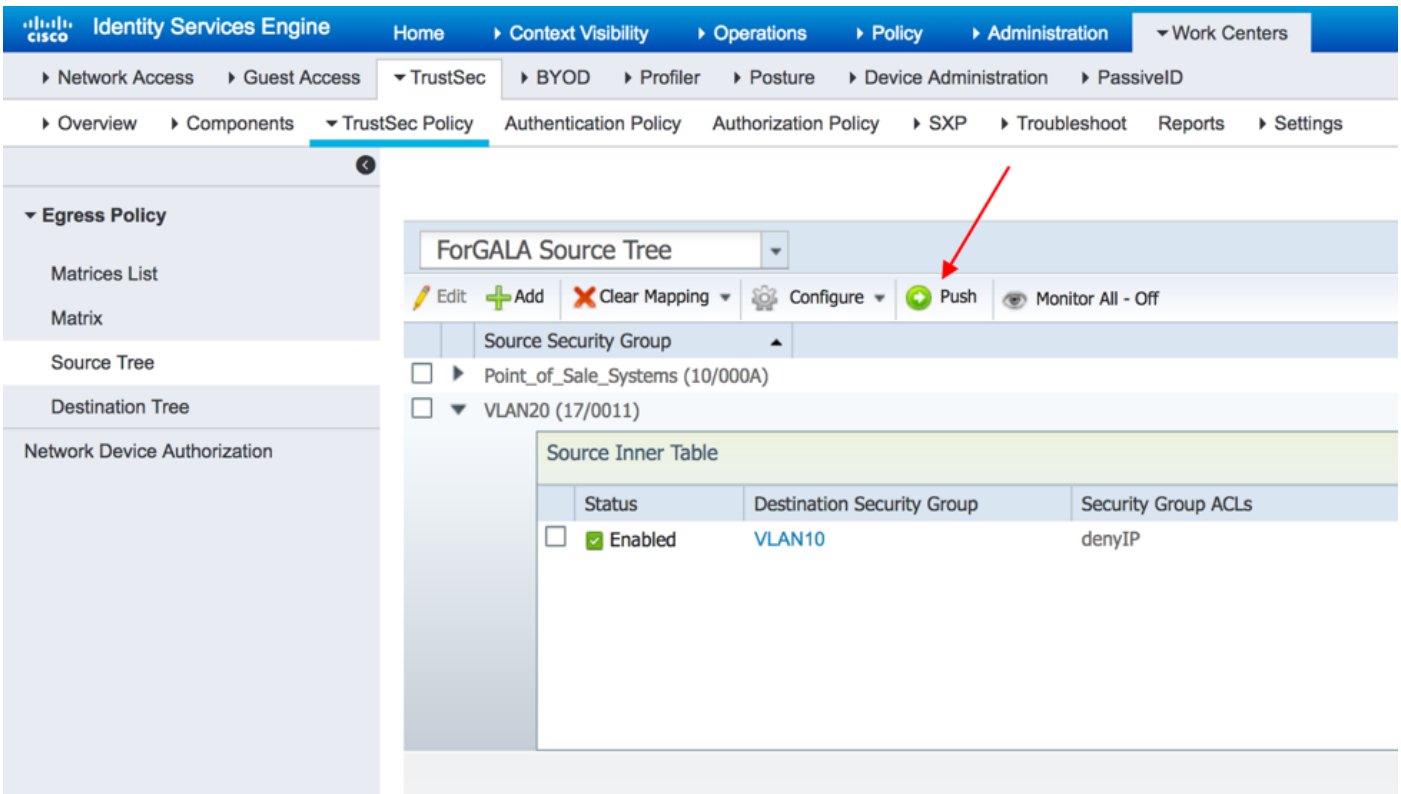
```
GALA#show cts role-based permissions IPv4 Role-based permissions default: Permit IP-00 IPv4
Role-based permissions from group 10:Point_of_Sale_Systems to group 15:BYOD: denyIP-20 IPv4
Role-based permissions from group 17:VLAN20 to group 16:VLAN10: denyIP-20 RBACL Monitor All for
Dynamic Policies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

Le commutateur obtient des stratégies de deux manières :

- CTS régénèrent du commutateur lui-même :

```
GALA#cts refresh policy
```

- Pousser manuel d'ISE :



Vérifiez

Plusieurs matrices

Les mappages de la finale SGT-IP et stratégies CTS sur les deux Commutateurs pour cet exemple :

Commutateur de 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
```

Commutateur 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
```

Observez que les stratégies pour les deux Commutateurs sont différentes (même la même stratégie de 10 à 15 est différente pour le commutateur de GALA et DRARORA). Ceci signifie qu'on permet le trafic de SGT 10 15 sur DRARORA, mais bloqué sur le 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)
```

De même, d'une fenêtre, vous pouvez accéder à un autre (SGT 17 - > SGT 16) :

```
C:\Windows\system32\cmd.exe
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>_
```

Et une autre manière (SGT 16 - > SGT 17) :

```
C:\Windows\system32\cmd.exe
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>
```

Pour confirmer que la stratégie correcte CTS était appliquée, vérifiez les **compteurs basés sur rôle de show cts** sortis :

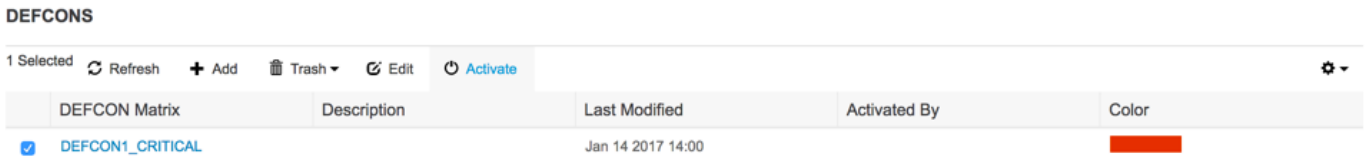
```
GALA#sh cts role-based counters
Role-based IPv4 counters
# '-' in hardware counters field indicates sharing among cells with identical policies
From    To      SW-Denied       HW-Denied       SW-Permitted    HW-Permitted

17 16 0 0 0 8 17 15 0 - 0 - 10 15 4 0 0 0 * * 0 0 127 26
```

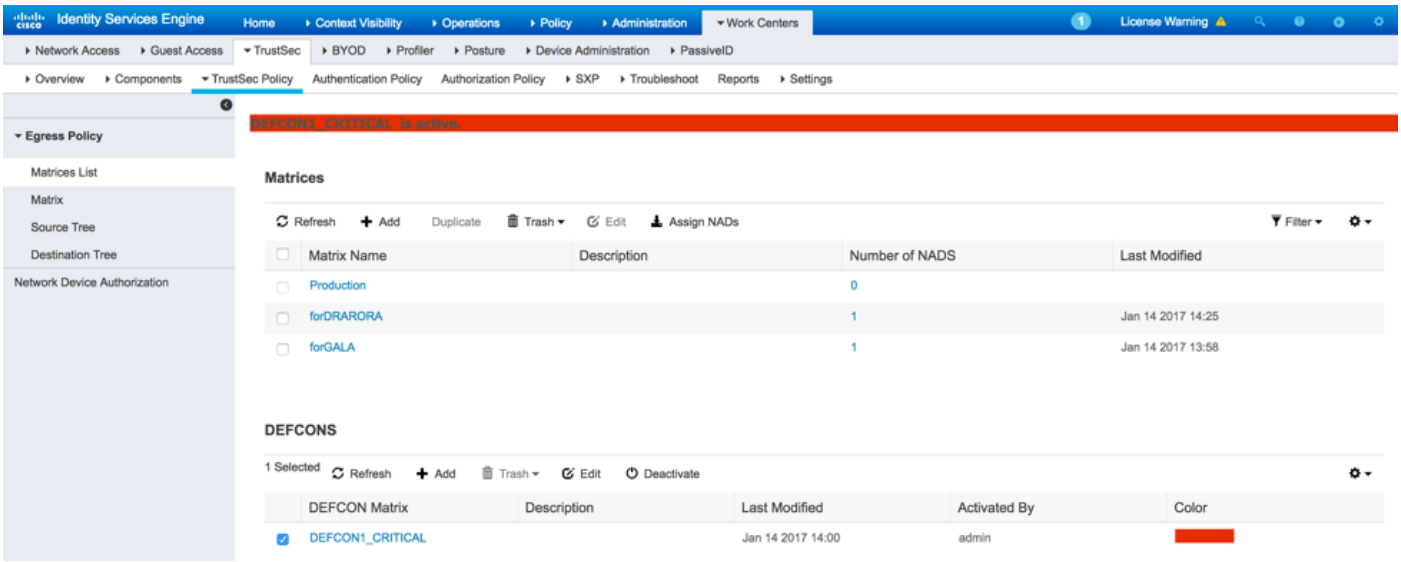
Le GALA a 8 paquets permis (4 de ping 17->16 et 4 de ping 16->17).

Déploiement de DefCon

En cas de besoin, déployez la matrice de DefCon sous des **centres de travail > TrustSec > stratégie de TrustSec > stratégie > des matrices de sortie les répertorient**, matrice de DefCon de contrôle que vous voudriez lancer et cliquer sur en fonction **Activate** :



Une fois que DefCon est lancé, le menu sur ISE ressemble à ceci :



Et maintient l'ordre sur des Commutateurs :

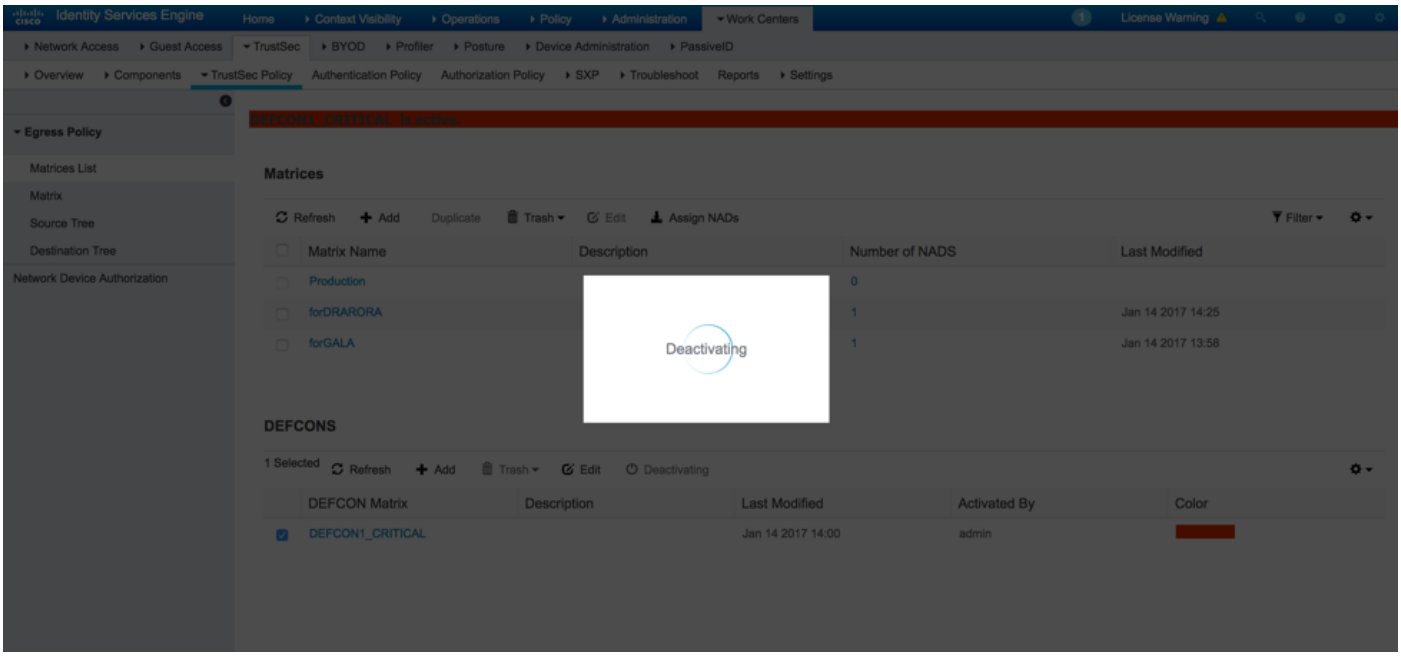
```
GALA#show cts role-based permissions IPv4 Role-based permissions default: Permit IP-00 IPv4
Role-based permissions from group 15:BYOD to group 10:Point_of_Sale_Systems: denyIP-20 IPv4
Role-based permissions from group 15:BYOD to group 16:VLAN10: denyIP-20 IPv4 Role-based
permissions from group 17:VLAN20 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
```

On ne permet pas le trafic de SGT 15 à SGT 10 sur les deux Commutateurs :

```
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)
```

Une fois que le déploiement est stable de nouveau, vous pouvez désactiver DefCon et les Commutateurs demandent les vieilles stratégies. Pour désactiver DefCon, naviguez vers des **centres de travail > TrustSec > stratégie de TrustSec > stratégie > des matrices de sortie les répertorient**, vérifient la matrice active de DefCon et cliquent sur en fonction **Deactivate** :



Les deux stratégies de demande de Commutateurs vieilles immédiatement :

```
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
```

Dépannez

Ravitaillement PAC

Ce fait partie de ravitaillement réussi 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**

L'anomalie de RAYON est prévue puisque le ravitaillement PAC est terminé avec succès.

Téléchargement de données d'environnement

Ceci affiche le téléchargement réussi de données d'environnement du commutateur :

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
```

Stratégies CTS

Des stratégies CTS sont poussées en tant qu'élément des messages de RAYON, ainsi du délai d'exécution-AAA se connectant le positionnement de composant pour mettre au point sur ISE (**gestion > se connectant > configuration de log de debug**) et mettent au point ci-dessous sur le commutateur devraient être suffisantes pour dépanner n'importe quel problème lié à CTS :

```
debug cts coa
debug radius
```

Additionaly, contrôle quelles stratégies sont appariées sur le 3750X d'allumage :

```
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 -
```

Vous ne pouvez pas utiliser la même commande sur 3850, en raison de CiscobugID CSCuu32958.