

Multiple Matrices op ISE 2.2 configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Meervoudige matringen](#)

[DefCon-overeenkomsten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[1. Basisswitchconfiguratie voor RADIUS/CTS](#)

[2. CTS-PAC](#)

[3. CTS-configuratie op een schakelaar.](#)

[4. Basisconfiguratie van CTS op ISE.](#)

[5. Meervoudige matrices en configuratie van DefCon op ISE.](#)

[6. SGT-classificatie](#)

[7. Downloaden van het CTS-beleid](#)

[Verifiëren](#)

[Meervoudige matringen](#)

[DefCon-implementatie](#)

[Problemen oplossen](#)

[PAC-bevoorrading](#)

[Downloaden van milieugegevens](#)

[CTS-beleid](#)

Inleiding

Dit document beschrijft het gebruik van meerdere TrustSec matrices en DefCon matrices in Cisco Identity Services Engine (ISE) 2.2. Dit is een nieuwe TrustSec optie die in ISE 2.2 voor een betere granulariteit in het netwerk wordt geïntroduceerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van Cisco TrustSec (CTS)-componenten
- Basiskennis van de CLI-configuratie van Catalyst-switches

- Ervaring met configuratie van Identity Services Engine (ISE)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Identity Services Engine 2.2
- Cisco Catalyst switch 3850 3.07.3.E
- Cisco Catalyst switch 3750X 15.2(4)E1
- Windows 7-machines

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

In ISE 2.0 is er een mogelijkheid om slechts één productie TrustSec matrix te gebruiken voor alle netwerkapparaten. ISE 2.1 toegevoegd kenmerk, dat halveringmatrix wordt genoemd, dat kan worden gebruikt voor test- en implementatiedoeleinden. Het in een haltebestendige matrix geschapen beleid wordt alleen toegepast op netwerkapparaten die voor tests worden gebruikt. De rest van de apparaten gebruikt nog steeds een productiematrix. Als eenmaal is bevestigd dat de matrixprinter goed werkt, kunnen alle andere apparaten naar deze matrixprinter worden verplaatst en wordt deze een nieuwe productiematrix.

ISE 2.2 biedt twee nieuwe TrustSec-functies:

1. Meervoudige matrices - mogelijkheid om verschillende matrixen aan netwerkapparaten toe te wijzen
2. DefCon-matrix - deze matrix wordt naar alle netwerkapparaten in een bepaalde situatie geduwd, geactiveerd door een beheerder

Het is mogelijk om één enkele matrixfunctie te gebruiken of een productie- en haltematrixfunctie in ISE 2.2.

Meervoudige matringen

Als u meerdere matrices wilt gebruiken, moet u deze optie inschakelen onder **Workcenters > TrustSec > Settings > Workprocesinstellingen**, zoals in de afbeelding:

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Under Administration, the path is TrustSec > BYOD > Profiler > Posture > Device Administration > Passiveld. The left sidebar shows a tree view with General TrustSec Settings, TrustSec Matrix Settings, Work Process Settings (selected), SXP Settings, and ACI Settings. The main content area is titled 'Work Process Settings' and contains four radio button options: 'Single Matrix', 'Multiple Matrices' (selected), 'Production and Staging Matrices with approval process', and 'Use DEFCONS' (unchecked). At the bottom right, there are 'Cancel' and 'Save' buttons.

Als deze optie is ingeschakeld, kunt u nieuwe matrieken maken en later netwerkapparaten aan de specifieke matrix toewijzen.

DefCon-overeenkomsten

DefCon matrices zijn speciale matrices die op elk moment klaar zijn om te worden gebruikt. Wanneer ingezet, worden alle netwerkapparaten automatisch aan deze matrix toegewezen. ISE herinnert zich nog de laatste productiematrix voor alle netwerkapparaten, zodat deze verandering op elk punt kan worden teruggedraaid wanneer DefCon wordt gedeactiveerd. U kunt maximaal vier verschillende DefCon-matrices definiëren:

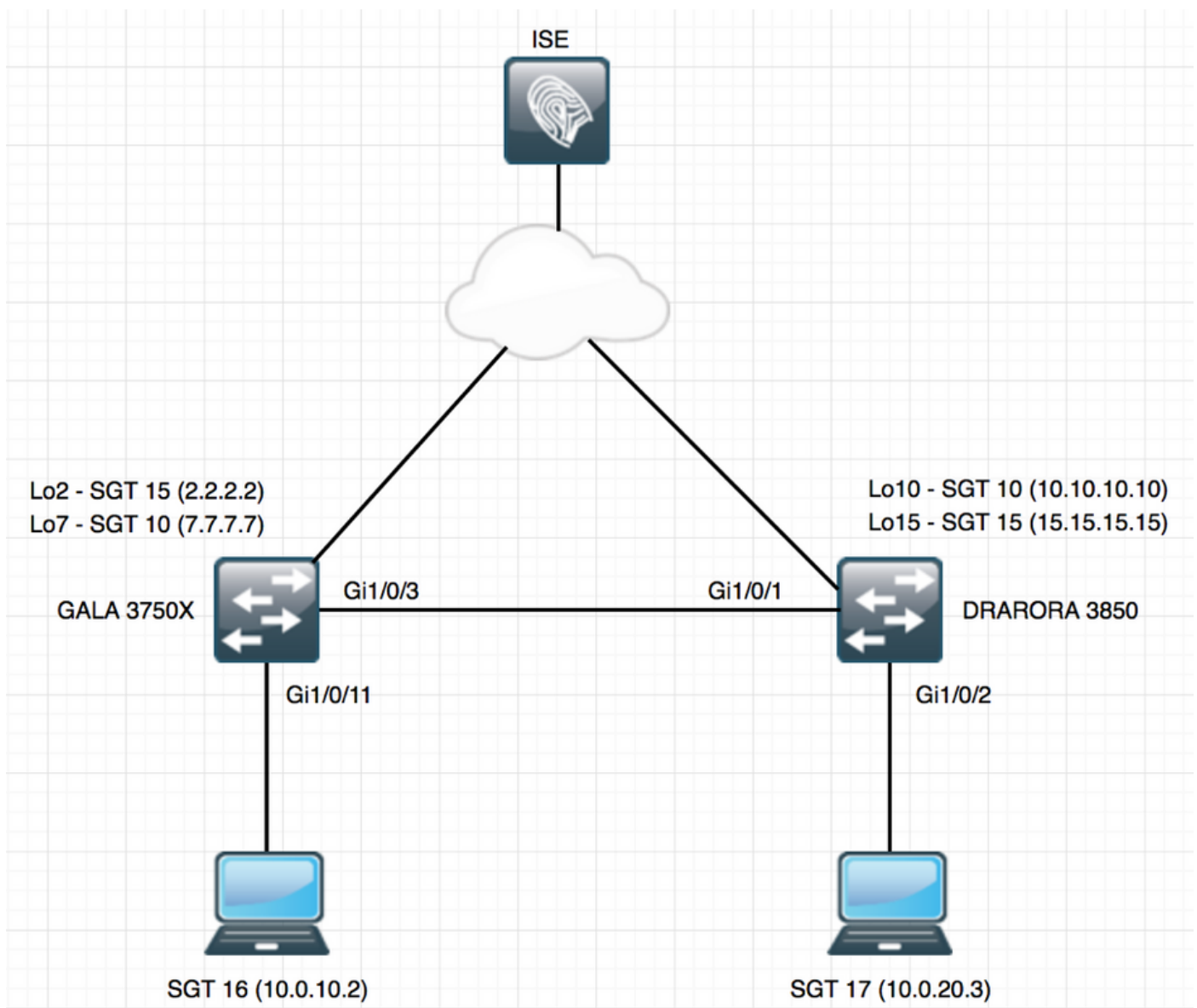
1. DefCon1 - Kritisch
2. DefCon2 - ernstig
3. DefCon3 - substantieel
4. DefCON4 - matig

DefCon matrices kan in combinatie met alle drie de werkprocesopties worden gebruikt:

This screenshot is identical to the one above, but the 'Use DEFCONS' checkbox is now checked, indicating that the configuration has been updated. The 'Multiple Matrices' radio button remains selected.

Configureren

Netwerkdigram



Configuraties

Als u meerdere matrixen wilt gebruiken, moet u dit uitschakelen onder Instellingen werkproces. In dit voorbeeld, schakelt u ook de DefCon matrix in.

1. Basisswitchconfiguratie voor 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
```

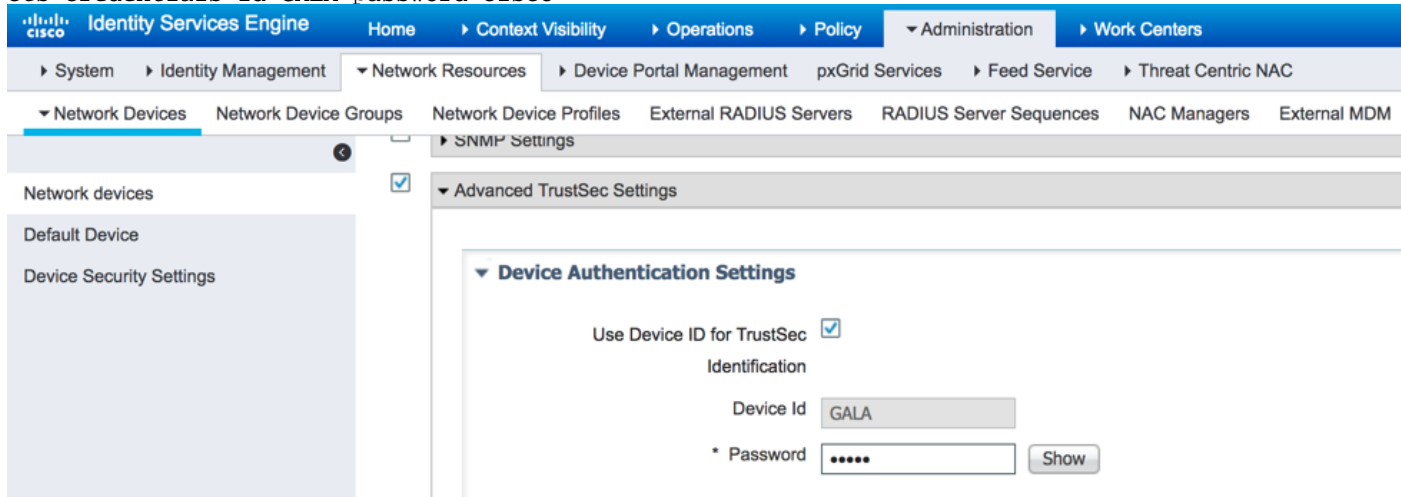
Om informatie over CTS te verkrijgen, moet u een lijst van CTS-vergunningen opstellen:

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

2. CTS-PAC

Om CTS PAC (Protected Access Credentials) van ISE te ontvangen, moet u dezelfde geloofsbrieven op schakelaar en ISE onder Geavanceerde TrustSec configuratie voor netwerkapparaat configureren:

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



Zodra dit is ingesteld kan een schakelaar CTS PAC downloaden. Eén deel ervan (PAC-gedekt) wordt als AV-paar in elk RADIUS-verzoek naar ISE verzonden, zodat ISE kan verifiëren of PAC voor dit netwerkapparaat nog steeds geldig is:

```
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. CTS-configuratie op een schakelaar.

Zodra PAC is gedownload, kan de switch om aanvullende CTS-informatie (milieu-gegevens en beleid) vragen:

```
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
```

U zou kunnen zien dat er geen beleid wordt gedownload van ISE, de reden is dat CTS handhaving niet op de schakelaar is geactiveerd:

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

GALA#show cts role-based permissions

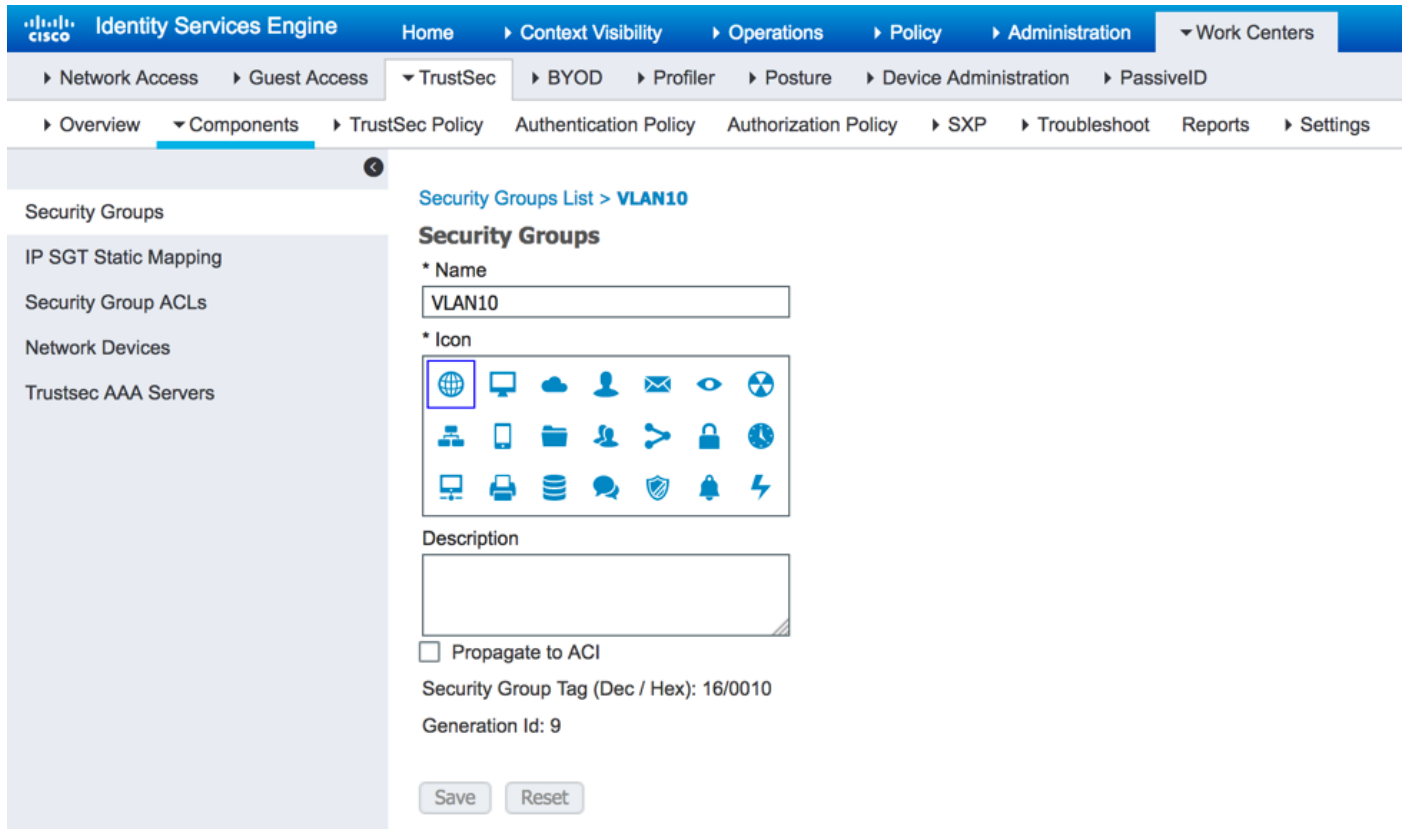
```
IPv4 Role-based permissions default:
Permit IP-00
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

In beide uitgangen zou u standaardwaarden kunnen zien - SGTs gecreëerd door standaard (0, 2-15, 255) en standaard **toestaan IP** beleid.

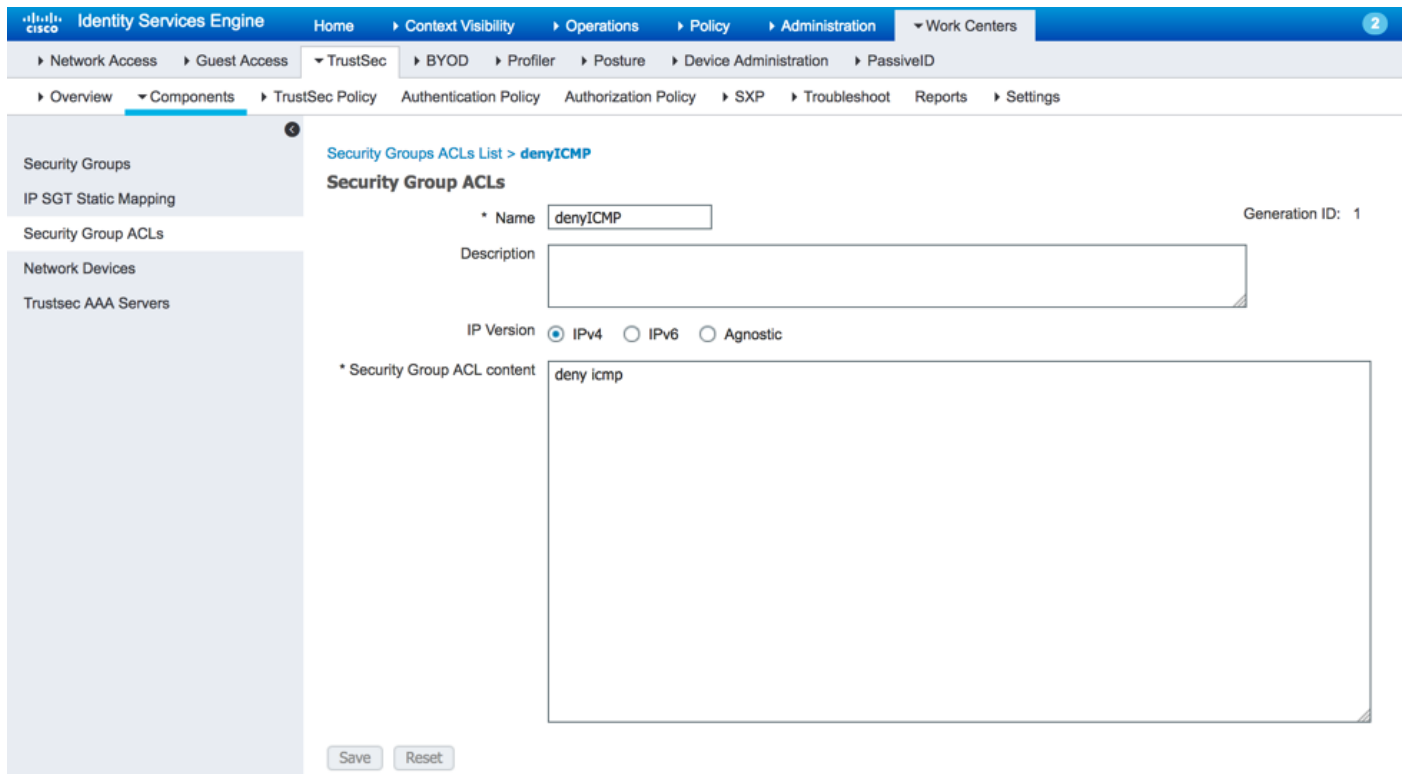
4. Basisconfiguratie van CTS op ISE.

Maak nieuwe veiligheidsgroeptags (SGT's) en weinig beleid op ISE om ze later te kunnen gebruiken. Navigeer naar **werkcentra > VertrouwenSec > Componenten > Beveiligingsgroepen**,

klik op **Toevoegen** om nieuwe SGT te creëren:



Om de Lijst van de Toegangscontrole van de Veiligheidsgroep (SGACL) voor verkeer het filtreren te maken, kies **de Groep van Beveiliging**, zoals in het beeld getoond:



Op dezelfde manier kun je andere SGT's en SGACL's maken. Nadat SGT's en SGACL's zijn gecreëerd, kunt u ze in het CTS-beleid aan elkaar koppelen om dit **te** doen door naar **Werkcentra > TrustSec > StustSec-beleid > Uitgangsbeleid > Bronboom**, zoals in de afbeelding getoond wordt:

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The navigation menu includes: Home, Context Visibility, Operations, Policy, Administration, Work Centers, Network Access, Guest Access, TrustSec, BYOD, Profiler, Posture, Device Administration, and PassiveID. The main content area is titled 'ForGALA Source Tree' and includes a table for 'Source Inner Table'.

Status	Destination Security Group	Security Group ACLs
<input checked="" type="checkbox"/> Enabled	VLAN10	denyIP

5. Meervoudige matrices en configuratie van DefCon op ISE.

In dit voorbeeld, hebt u beleid voor matrix **ForGALA** ingesteld. U kunt tussen de matrixen overschakelen door het uitrolmenu te gebruiken. U kunt meerdere matrixen activeren door naar **werkcentra > TrustSec > Instellingen > Werkprocesinstellingen** te navigeren en meerdere matrixen en defCon matrixen in te schakelen, zoals in de afbeelding wordt getoond:

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The navigation menu includes: Home, Context Visibility, Operations, Policy, Administration, Work Centers, Network Access, Guest Access, TrustSec, BYOD, Profiler, Posture, Device Administration, and PassiveID. The main content area is titled 'Work Process Settings' and includes a settings section with radio buttons for 'Single Matrix', 'Multiple Matrices', and 'Production and Staging Matrices with approval process', and a checked checkbox for 'Use DEFCONS'.

Als deze optie is ingeschakeld, is er een standaard productmatrix beschikbaar, hoewel u andere matrixen kunt maken. Navigeren in **naar werkcentra > TrustSec > TrustSec Policy > Egress Policy > Matrixlijst** en klik op **Add**:

Add Matrix



Name *

Description

Copy policy from

Er is een optie om beleid te kopiëren dat deel van de nieuwe uit de reeds bestaande matrix moet maken. Maak twee matrices - één voor 3750X-switch, een ander voor 3850-schakelaar. Zodra matrices gecreëerd zijn, moet u netwerkapparaten aan deze matrices toewijzen, omdat standaard alle TrustSec-enabled-netwerkttoegangsapparaten zijn toegewezen aan Producmatrix.

Matrix Name	Description	Number of NADs	Last Modified
<input type="checkbox"/> Production		2	
<input type="checkbox"/> forDRARORA		0	Jan 11 2017 18:02
<input type="checkbox"/> forGALA		0	Jan 11 2017 18:00

Als u NAD's wilt toewijzen, klikt u op **NAD's** toewijzen onder Matrixlijst, controleert u het apparaat dat u de matrix wilt toewijzen en kiest u de gemaakte matrix in het vervolgkeuzemenu en klikt u op **Toewijzen**, zoals in de afbeelding wordt weergegeven:

1 Selected

Rows/Page 2 / 1 / 1

Name	IP	Location	Type	Matrix
<input checked="" type="checkbox"/> DRARORA	10.48.72.108/32	Location#All Locations	Device Type#All Device Types	Production
<input type="checkbox"/> 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

U kunt dit ook voor andere apparaten doen, gevolgd door de klik op de knop **Toewijzen**:

Assign Network Devices

1 Select network devices. (Filters may be used)

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

Refresh Filter

Name	IP	Location	Type	Matrix
DRARORA	10.48.72.108/32	Location#All Locations	Device Type#All Device Types	forDRARORA
<input checked="" type="checkbox"/> 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**

Close & Send Assign

Nadat alle wijzigingen zijn uitgevoerd, klik op **Close&Send**, dat alle updates naar apparaten stuurt om CTS-beleid te verfrissen om nieuwe te downloaden. Creëer op dezelfde manier een Matrixprinter DefCon, die u uit bestaande matrixen kunt kopiëren:

Add DEFCON

DEFCON Level

Description

Copy policy from

DEFCON2(Severe)

DEFCON3(Substantial)

DEFCON4(Moderate)

Cancel Submit

Het uiteindelijke beleid ziet er uit als:

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

License Warning

TrustSec > BYOD > Profiler > Posture > Device Administration > PassivID

TrustSec Policy

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

DEFCON Matrix	Description	Last Modified	Activated By	Color
<input type="checkbox"/> DEFCON1_CRITICAL		Jan 4 2017 15:42		

6. SGT-classificatie

Er zijn twee opties voor tags aan clientopdrachten (maken van IP-SGT-afbeeldingen):

- *statisch* - met de **tag op basis van de rol-gebaseerde sgt-map voor IP_adres sgt**
- *dynamische* - via dot1x - authenticatie (tag wordt toegewezen als resultaat van succesvolle authenticatie)

Gebruik hier beide opties, twee ruiten machines verkrijgen SGT tag via dot1x verificatie en loopback interfaces met statische SGT tag. Om dynamische mapping in te zetten, voert u een autorisatiebeleid voor eindklanten in:

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

U kunt statische IP-SGT-mapping maken met behulp van opdrachten (bijvoorbeeld voor een GALA-switch):

```
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
```

Na succesvolle authenticatie bereikt de cliënt het autorisatiebeleid met een specifiek SGT-label als resultaat:

```
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
```

U kunt alle IP-SGT mappings controleren met de opdracht **cts op rol gebaseerde sgt-map alle tonen**, waar u de bron van elke mapping ziet (LOCAL - via dot1x authenticatie, CLI - statische toewijzing):

```
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. Downloaden van het CTS-beleid

Zodra de switch CTS PAC heeft en de omgevingsgegevens zijn gedownload, kan deze om CTS-beleid vragen. De switch downloaden niet alle beleidslijnen, maar alleen de beleidslijnen die nodig zijn - het beleid voor verkeer voorbestemd om de bekende SGT-tags te kunnen gebruiken - in het geval van een GALA-schakelaar, vraagt hij van ISE deze beleidslijnen:

- verkeersbeleid naar SGT 15
- verkeersbeleid naar SGT 10
- verkeersbeleid 16

Het resultaat van alle beleid voor GALA-switch:

```
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
```

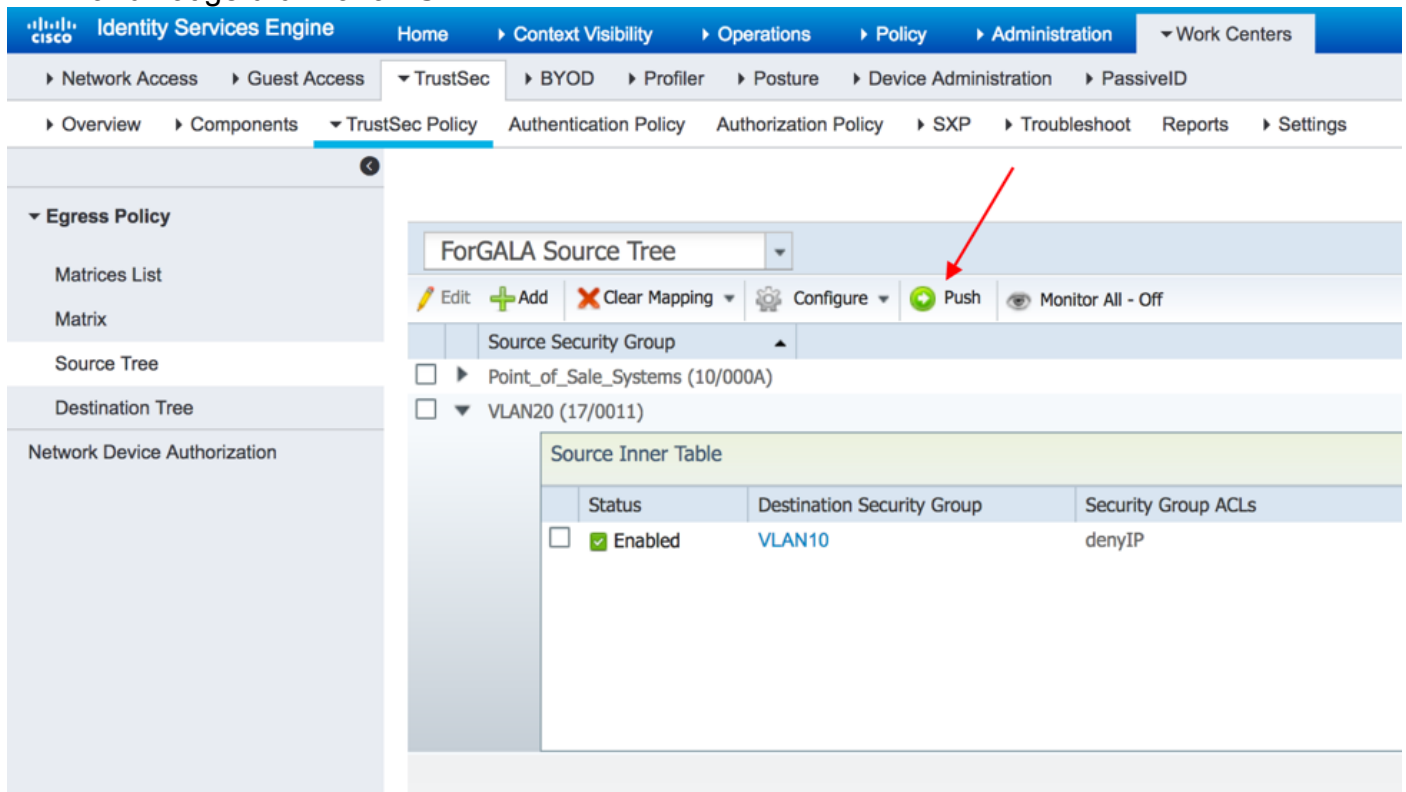
```
RBACL Monitor All for Configured Policies : FALSE
```

Switch verkrijgt beleid op twee manieren:

- CTS verfrist zich van de schakelaar zelf:

GALA#cts refresh policy

- Handmatige druk vanaf ISE:



Verifiëren

Meervoudige matringen

Het laatste SGT-IP-mappings- en CTS-beleid op beide switches voor dit voorbeeld:

GALA-schakelaar:

```
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
```

DRARORA-schakelaar:

```
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
```

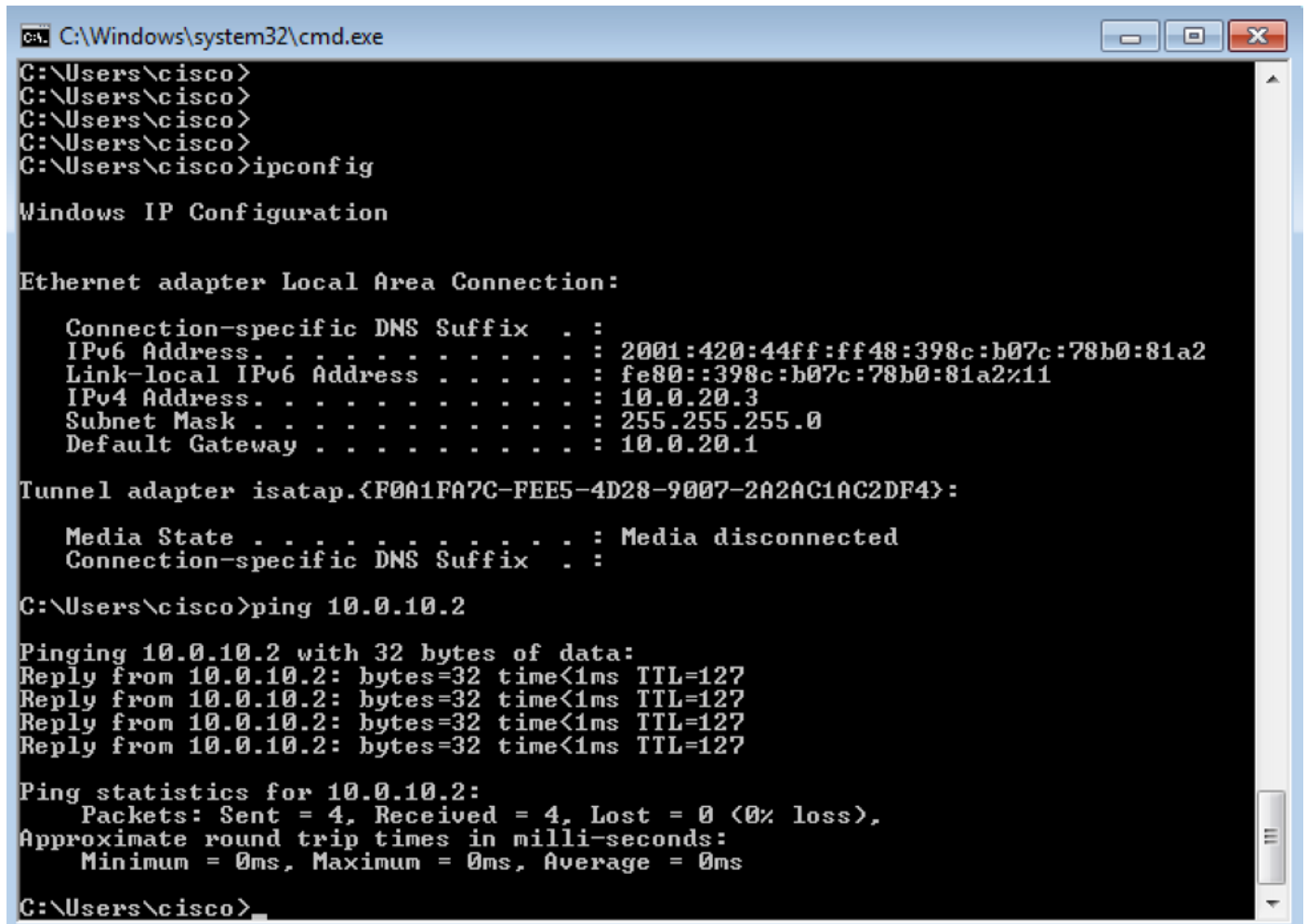
Let erop dat het beleid voor beide switches anders is (zelfs het zelfde beleid van 10 naar 15 is anders voor GALA en DRARORA). Dit betekent dat verkeer van 10 SGT naar 15 toegestaan is op DRARORA, maar geblokkeerd is op GALA:

```
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)

Op dezelfde manier kunt u vanuit het ene venster toegang krijgen tot een ander venster (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>
```

En op een andere manier (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>

```

Om te bevestigen dat het juiste CTS-beleid werd toegepast, toont de controle **cts op rol gebaseerde** tellers output:

```

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 heeft 8 toegestane pakketten (4 van pingelen 17->16 en 4 van 16->17).

DefCon-implementatie

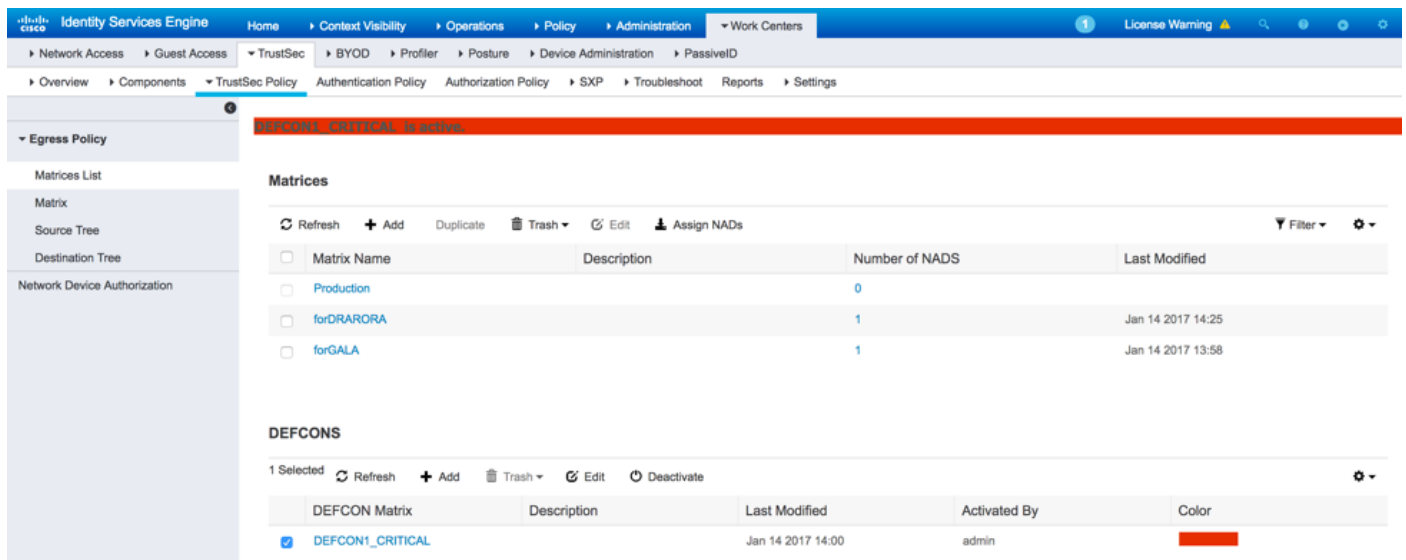
Indien nodig kunt u een DefCon-matrix inzetten onder **Workcenters > TrustSec > TrustSec Policy > Egress Policy > Matrixlijst**, controleer de DefCon-matrix die u wilt activeren en klik op **Activeren**:

DEFCONS

1 Selected Refresh Add Trash Edit Activate

DEFCON Matrix	Description	Last Modified	Activated By	Color
<input checked="" type="checkbox"/> DEFCON1_CRITICAL		Jan 14 2017 14:00		

Nadat DefCon is geactiveerd, ziet het menu op ISE er als volgt uit:



En beleid op wissels:

```
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
```

Verkeer van SGT 15 naar SGT 10 is niet toegestaan op beide switches:

```
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.
```

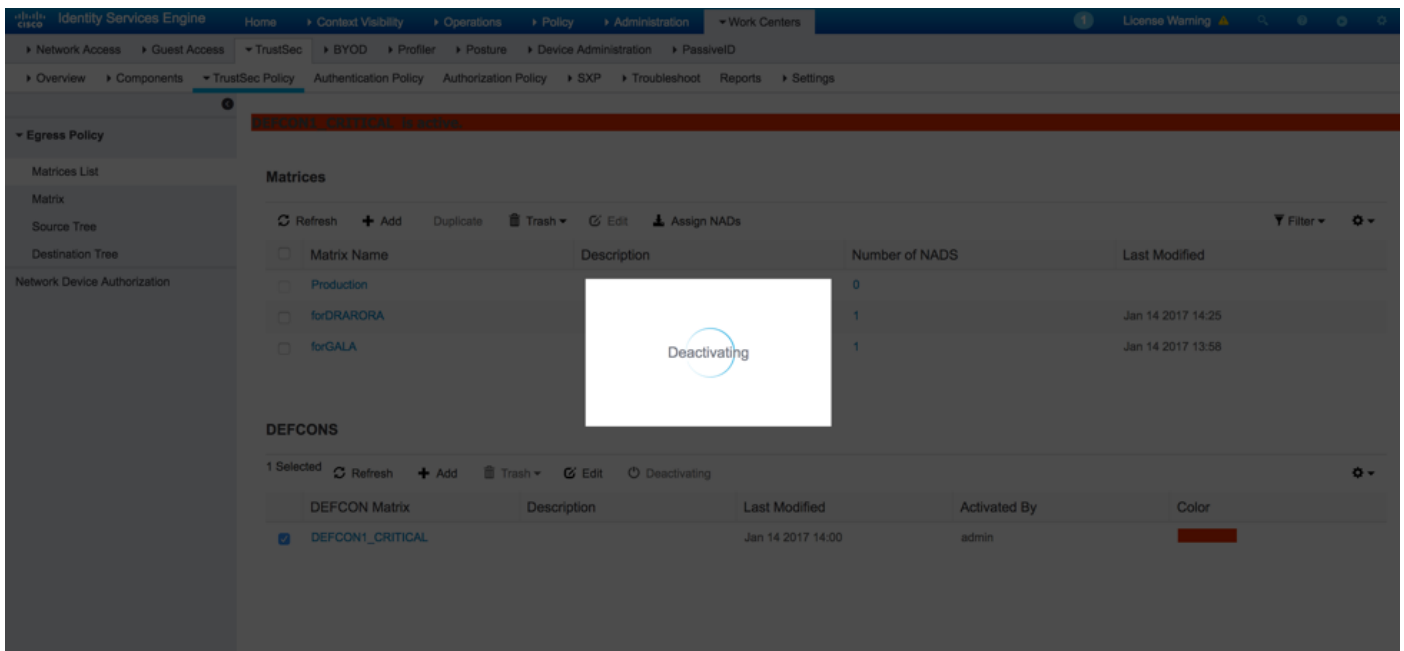
```
Sending 5, 100-byte ICMP Echos to 7.7.7.7, timeout is 2 seconds:
```

```
Packet sent with a source address of 2.2.2.2
```

```
U.U.U
```

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

Als de implementatie weer stabiel is, kunt u DefCon deactiveren en de schakelaars om het oude beleid vragen. Om DefCon te deactiveren, navigeer naar **Werkcentra > VertrouwenSec > Beleid > Uitgangsbeleid > Matrixlijst**, controleer de actieve matrix van DefCon en klik op **Deactiveren**:



Beide switches vragen direct om oud beleid:

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

Problemen oplossen

PAC-bevoorrading

Dit maakt deel uit van succesvolle PAC-voorzieningen:

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
```

RADIUS wordt afgekeurd omdat PAC-provisioning is voltooid.

Downloaden van milieugegevens

Dit toont de succesvolle download van omgevingsgegevens van de switch:

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) sname (Unknown) added
    name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sname, name = 0001, req = 1, rcv = 1
    Setting SG Name receiving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
CTS_AAA_SGT_NAME_INBOUND - SGT = 65535-68:unicast-default
    flag (128) sname (ANY) added
    name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sname, name = 0001, req = 1, rcv = 1
    Setting SG Name receiving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
CTS_AAA_SGT_NAME_INBOUND - SGT = 9-68
    flag (128) sname (Auditors) added
    name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sname, name = 0001, req = 1, rcv = 1
    Setting SG Name receiving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
CTS_AAA_SGT_NAME_INBOUND - SGT = 15-68
    flag (128) sname (BYOD) added
    name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sname, name = 0001, req = 1, rcv = 1
    Setting SG Name receiving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
CTS_AAA_SGT_NAME_INBOUND - SGT = 5-68
    flag (128) sname (Contractors) added
    name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sname, name = 0001, req = 1, rcv = 1
    Setting SG Name receiving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
CTS_AAA_SGT_NAME_INBOUND - SGT = 8-68
    flag (128) sname (Developers) added
    name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sname, name = 0001, req = 1, rcv = 1
    Setting SG Name receiving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
CTS_AAA_SGT_NAME_INBOUND - SGT = 12-68
    flag (128) sname (Development_Servers) added
    name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sname, name = 0001, req = 1, rcv = 1
    Setting SG Name receiving bit CTS_ENV_DATA_SGT_NAME_ENTRY on
CTS_AAA_SGT_NAME_INBOUND - SGT = 4-68
    flag (128) sname (Employees) added
    name (0001), request (1), receive (1)
cts_env_data_aaa_sgt_sname, 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

```

CTS-beleid

Het CTS-beleid wordt geduwd als onderdeel van RADIUS-berichten, zodat **een** logbestand **dat** uit **een** programma **bestaat** dat is ingesteld om op ISE te debug (**Administratie > Vastlegging > Loggen > Debug Log Configuration**) en onder de debugs in schakelaar voldoende mate is om problemen met CTS op te lossen:

```
debug cts coa
debug radius
```

Controleer daarnaast welk beleid er op de schakelaar past: op 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	-

U kunt dezelfde opdracht niet gebruiken op 3850 vanwege Cisco bugID [CSCu32958](#).