Konfiguration von TrustSec Multiple Matrices auf ISE 2.2

Inhalt

Einführung

In diesem Dokument wird die Verwendung mehrerer TrustSec-Matrizen und DefCon-Matrizen in der Cisco Identity Services Engine (ISE) 2.2 beschrieben. Dies ist eine neue TrustSec-Funktion, die in der ISE 2.2 eingeführt wurde, um die Präzision im Netzwerk zu verbessern.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundkenntnisse der Komponenten von Cisco TrustSec (CTS)

- Grundkenntnisse der CLI-Konfiguration von Catalyst Switches
- Erfahrung mit der ISE-Konfiguration (Identity Services Engine)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

In der ISE 2.0 besteht die Möglichkeit, für alle Netzwerkgeräte nur eine TrustSec-Produktionsmatrix zu verwenden. ISE 2.1 bietet zusätzlich eine Funktion, die als Staging Matrix bezeichnet wird und für Test- und Implementierungszwecke verwendet werden kann. Richtlinien, die in der Bereitstellungsmatrix erstellt werden, werden nur auf Netzwerkgeräte angewendet, die für Tests verwendet werden. Die übrigen Geräte verwenden noch die Produktionsmatrix. Sobald bestätigt wird, dass die Staging-Matrix einwandfrei funktioniert, können alle anderen Geräte in diese Matrix verschoben werden, und es wird eine neue Produktionsmatrix.

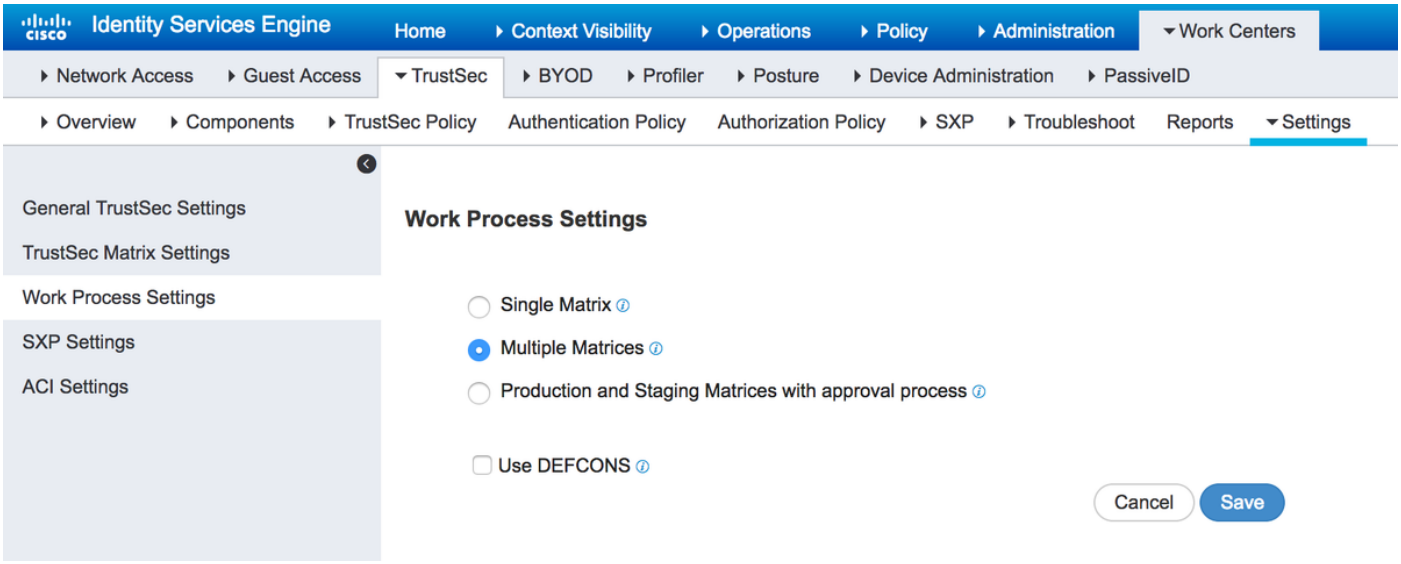
Die ISE 2.2 umfasst zwei neue TrustSec-Funktionen:

1. Mehrere Matrizen - Möglichkeit, Netzwerkgeräten unterschiedliche Matrizen zuzuweisen
2. DefCon-Matrix - Diese Matrix wird vom Administrator ausgelöst und an alle Netzwerkgeräte in einer bestimmten Situation weitergeleitet.

Die ISE 2.2 bietet die Möglichkeit, entweder eine einzelne Matrix-Funktion oder die Produktions- und Staging-Matrix-Funktion zu verwenden.

Mehrere Matrizen

Um mehrere Matrizen zu verwenden, müssen Sie diese Option unter **Work Centers > TrustSec > Settings > Work Process Settings** aktivieren, wie im Bild gezeigt:



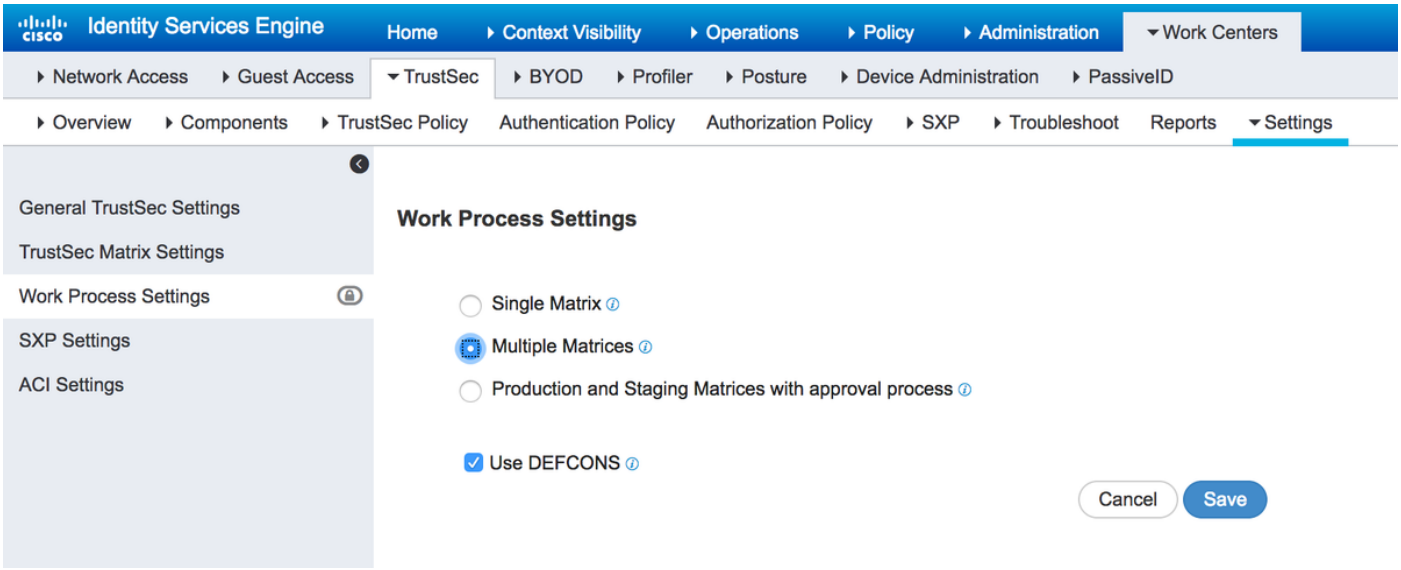
Nach der Aktivierung können Sie neue Matrizen erstellen und später Netzwerkgeräte der jeweiligen Matrix zuweisen.

DefCon-Matrizen

DefCon-Matrizen sind spezielle Matrizen, die jederzeit bereitgestellt werden können. Bei der Bereitstellung werden alle Netzwerkgeräte dieser Matrix automatisch zugewiesen. Die ISE speichert immer noch die letzte Produktionsmatrix für alle Netzwerkgeräte, sodass diese Änderung jederzeit rückgängig gemacht werden kann, wenn DefCon deaktiviert wird. Sie können bis zu vier verschiedene DefCon-Matrizen definieren:

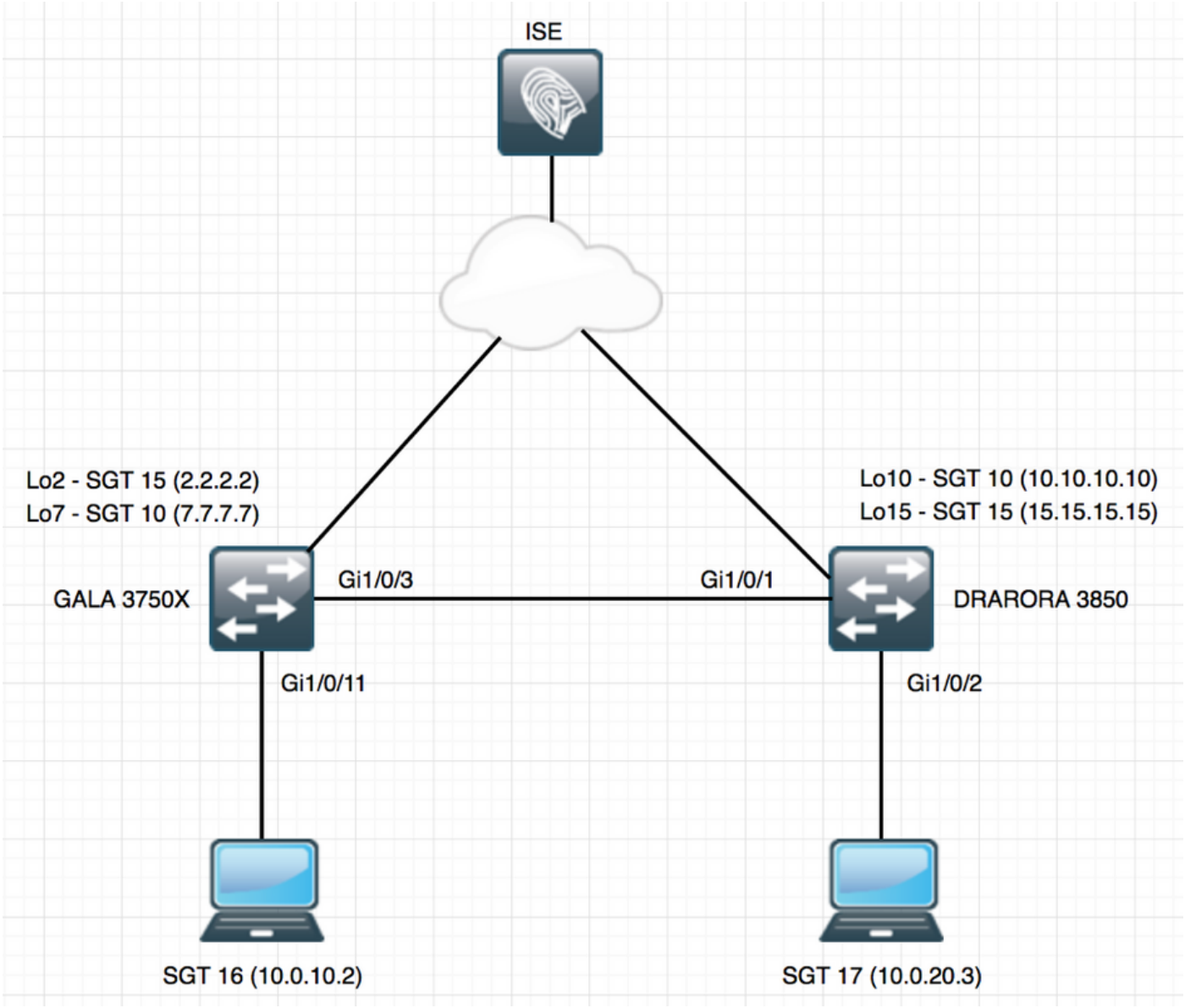
1. DefCon1 - Kritisch
2. DefCon2 - Schwer
3. DefCon3 - Deutlich
4. DefCon4 - Mittel

DefCon-Matrizen können in Kombination mit allen drei Arbeitsabläufen verwendet werden:



Konfigurieren

Netzwerkdiagramm



Konfigurationen

Um mehrere Matrizen zu verwenden, müssen Sie diese unter "Arbeitsprozess-Einstellungen" aktivieren. Aktivieren Sie in diesem Beispiel auch die DefCon-Matrix.

1. Grundlegende Switch-Konfiguration für 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
```

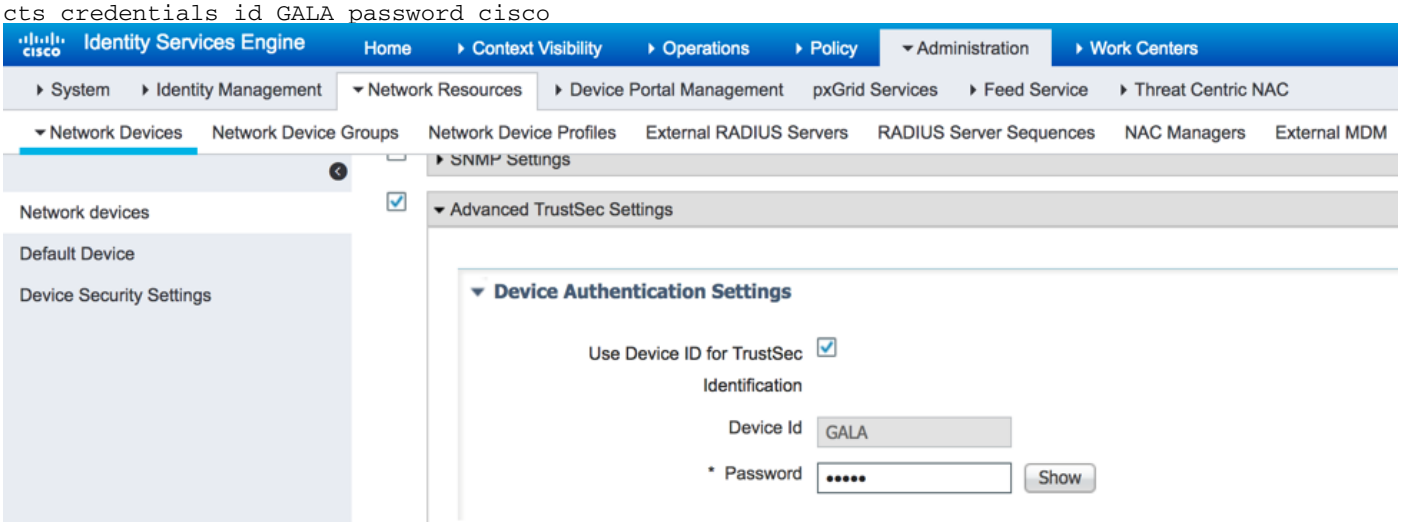
Um CTS-Informationen zu erhalten, müssen Sie eine CTS-Autorisierungsliste erstellen:

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

2. CTS PAC

Um CTS PAC (Protected Access Credentials) von der ISE zu erhalten, müssen Sie unter der Advanced TrustSec-Konfiguration für das Netzwerkgerät dieselben Anmeldeinformationen für den Switch und die ISE konfigurieren:

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



Nach der Konfiguration kann ein Switch CTS PAC herunterladen. Ein Teil davon (PAC-Opaque) wird in jeder RADIUS-Anfrage als AV-Paar an die ISE gesendet, sodass die ISE überprüfen kann, ob die PAC für dieses Netzwerkgerät noch gültig ist:

```
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:
000200B000030001000400010E6796CD7BBF2FA4111AD9FB4FEFB5A5000060094000300100012FABE10F3DCBCB152C54FA5
BFE124CB00000013586BB31500093A809E11A93189C7BE6EBDFB8FDD15B9B7252EB741ADCA3B2ACC5FD923AEB7BDFE48
A3A771338926A1F48141AF091469EE4AFC8C3E92A510BA214A407A33F469282A780E8F50F17A271E92D1FEE1A29ED427
B985F9A0E00D6CDC934087716F4DEAF84AC11AA05F7587E898CA908463BDA9EC7E65D827
  Refresh timer is set for 11y13w
```

3. CTS-Konfiguration auf einem Switch.

Nach dem Herunterladen von PAC kann der Switch zusätzliche CTS-Informationen anfordern (Umgebungsdaten und Richtlinien):

```
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
```

Sie sehen möglicherweise, dass keine Richtlinien von der ISE heruntergeladen werden. Der Grund dafür ist, dass die CTS-Durchsetzung auf dem Switch nicht aktiviert ist:

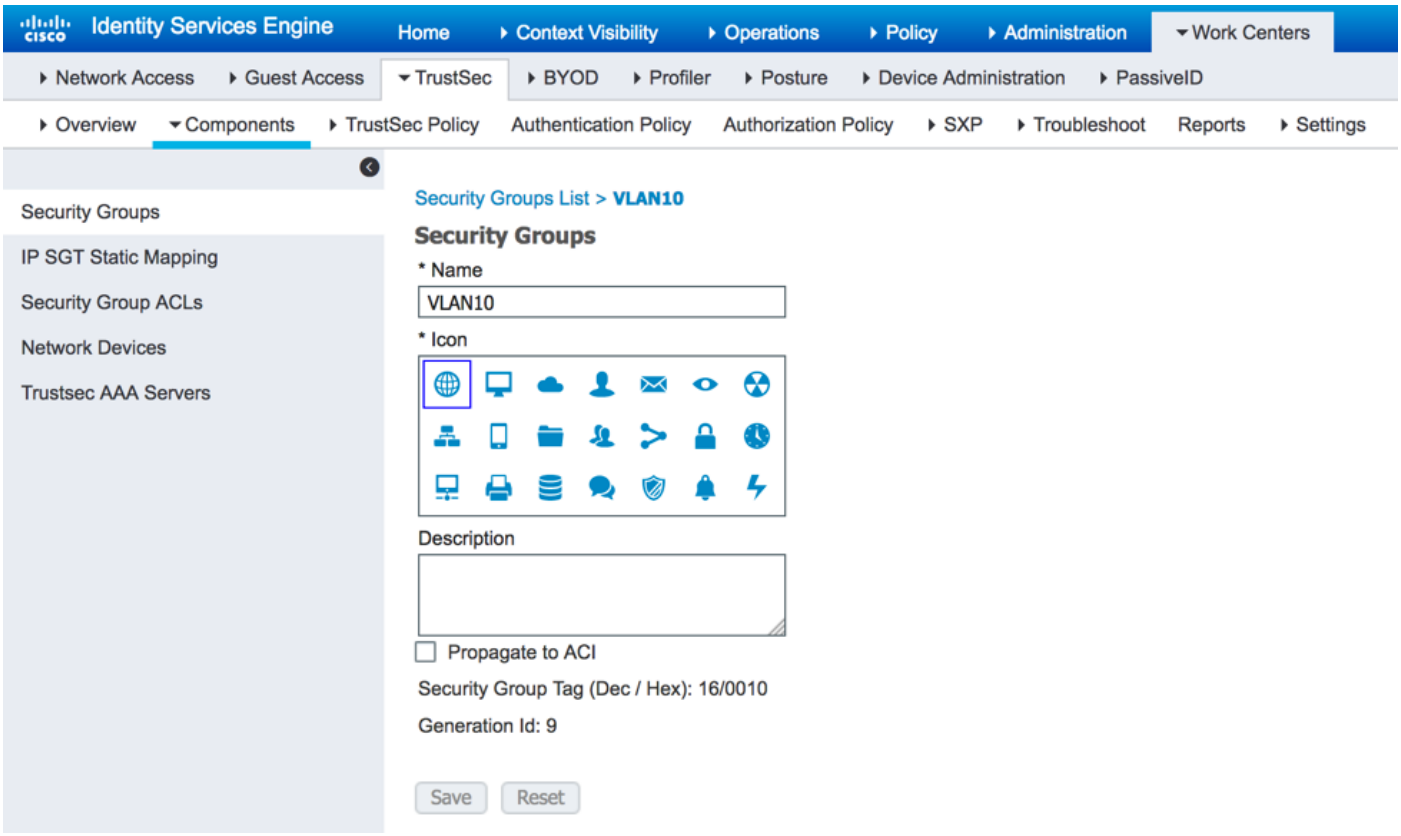
```
cts role-based enforcement
cts role-based enforcement vlan-list 1-4094

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 beiden Ausgängen werden Standardwerte angezeigt - standardmäßig erstellte SGTs (0, 2-15, 255) und die **IP-**Standardrichtlinie **für** die **Genehmigung**.

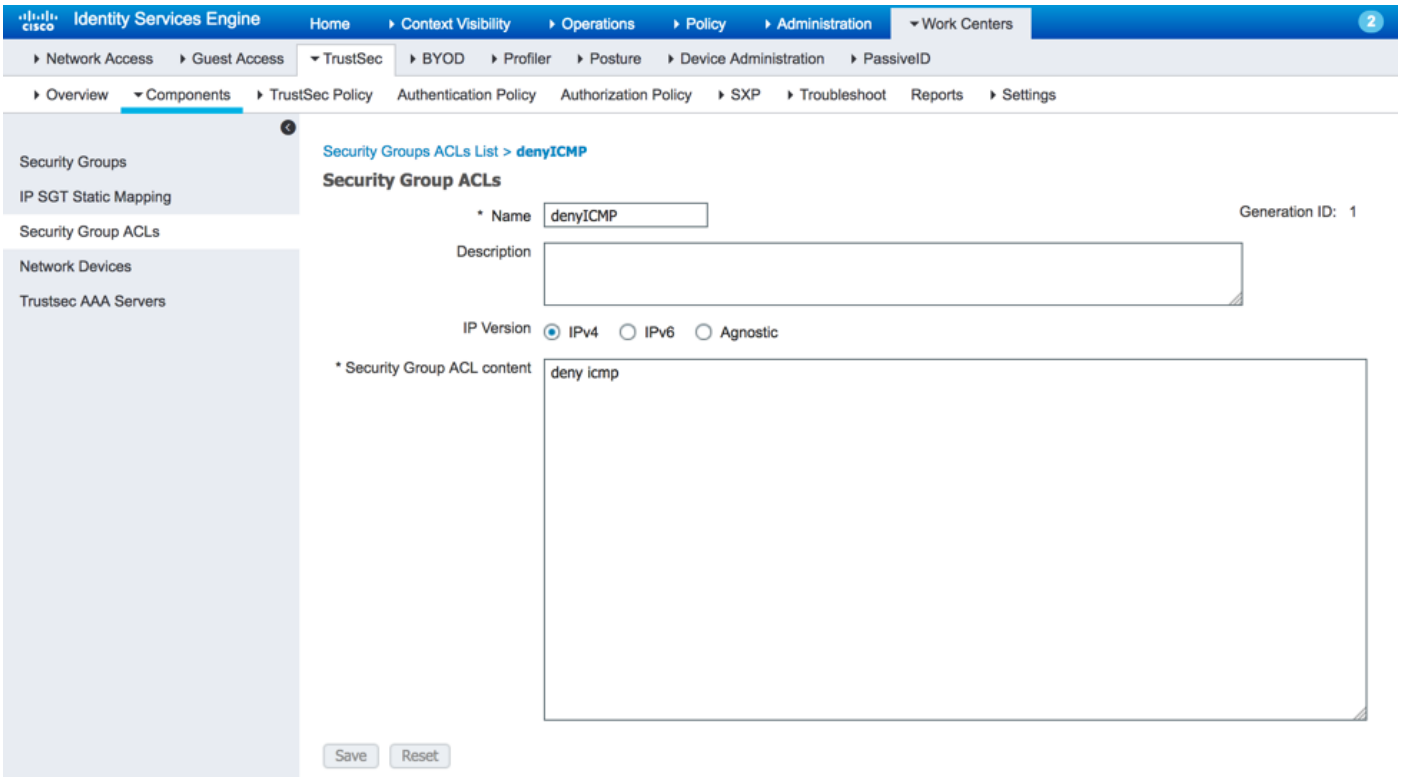
4. Grundlegende CTS-Konfiguration auf der ISE.

Erstellen Sie neue Security Group Tags (SGTs) und wenige Richtlinien für die ISE, um diese später zu verwenden. Navigieren Sie zu **Work Centers > TrustSec > Components > Security**

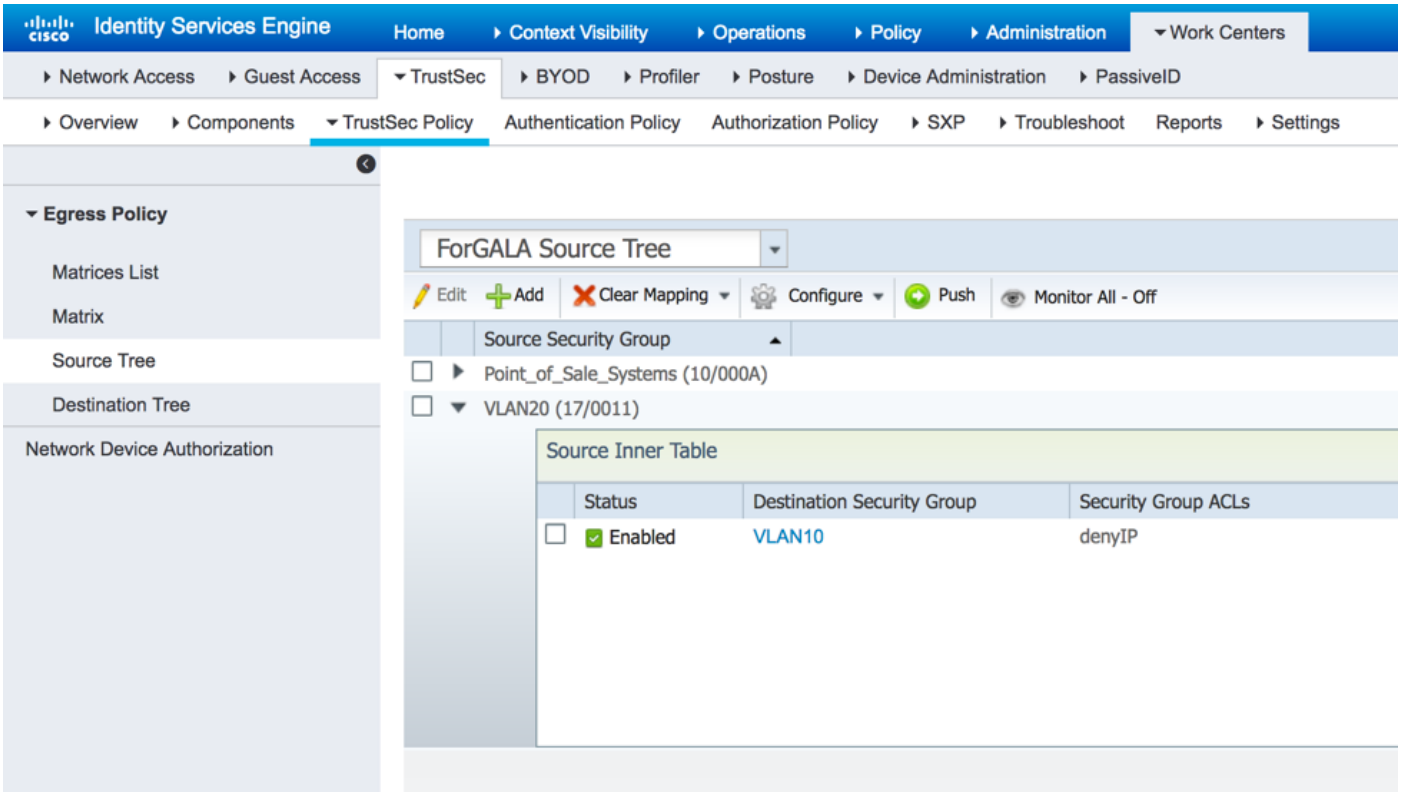
Groups, und klicken Sie auf **Add**, um ein neues SGT zu erstellen:



Um eine Security Group Access Control List (SGACL) für die Datenverkehrsfilterung zu erstellen, wählen Sie **Security Group ACLs (Sicherheitsgruppen-Zugriffskontrollliste) aus**, wie im Bild gezeigt:

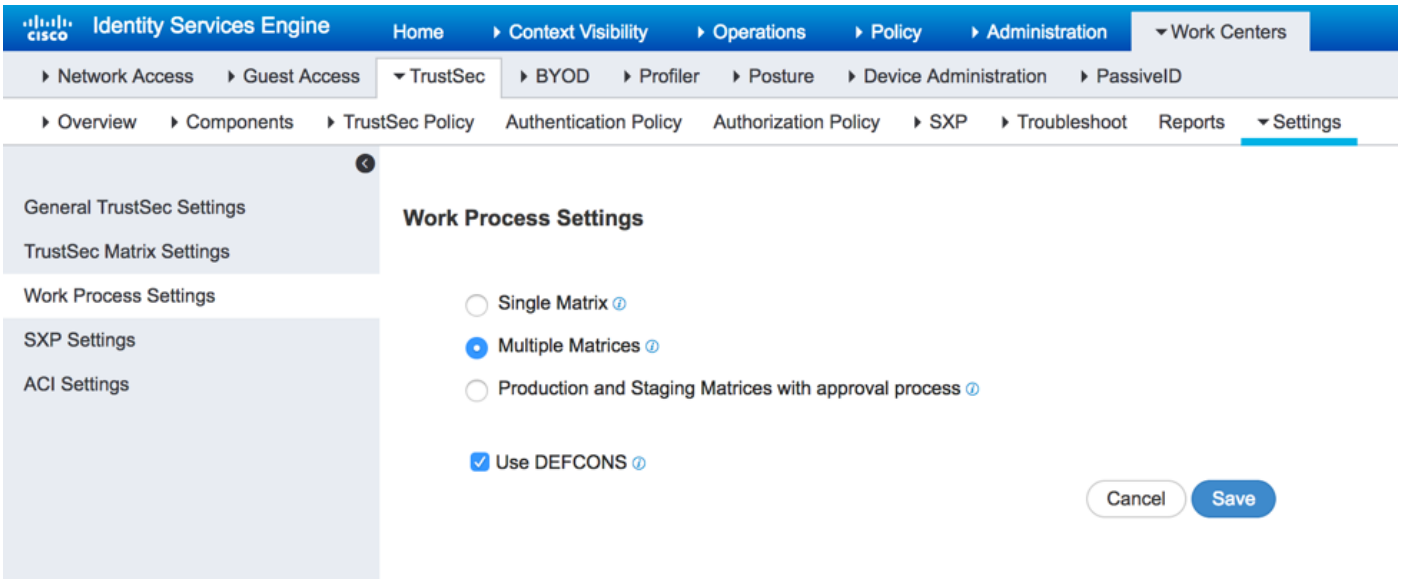


Ebenso können Sie andere SGTs und SGACLs erstellen. Nachdem Sie SGTs und SGACLs erstellt haben, können Sie sie in CTS-Richtlinien miteinander verknüpfen. Navigieren Sie dazu zu **Work Centers > TrustSec > TustSec Policy > Egress Policy > Source Tree**, wie im Bild gezeigt:



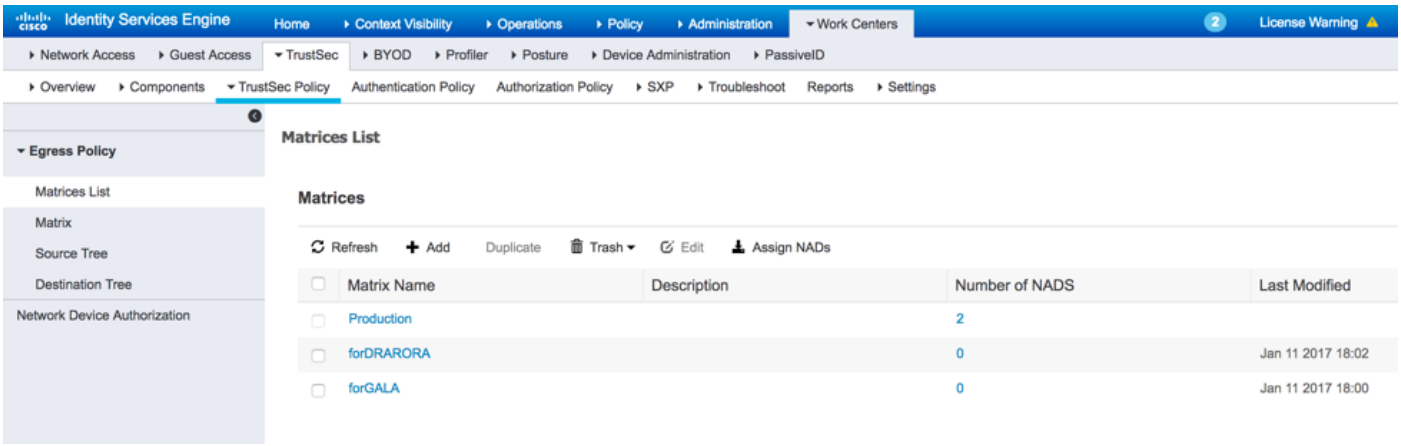
5. Mehrere Matrizen und DefCon-Konfiguration auf der ISE.

In diesem Beispiel haben Sie Richtlinien für die Matrix **ForGALA** konfiguriert. Um zwischen den Matrizen zu wechseln, können Sie das Dropdown-Menü verwenden. Um mehrere Matrices zu aktivieren, gehen Sie zu **Work Centers > TrustSec > Settings > Work Process Settings**, und aktivieren Sie Multiple Matrices and DefCon matrices (Mehrere Matrizen und DefCon-Matrizen), wie im Bild gezeigt:

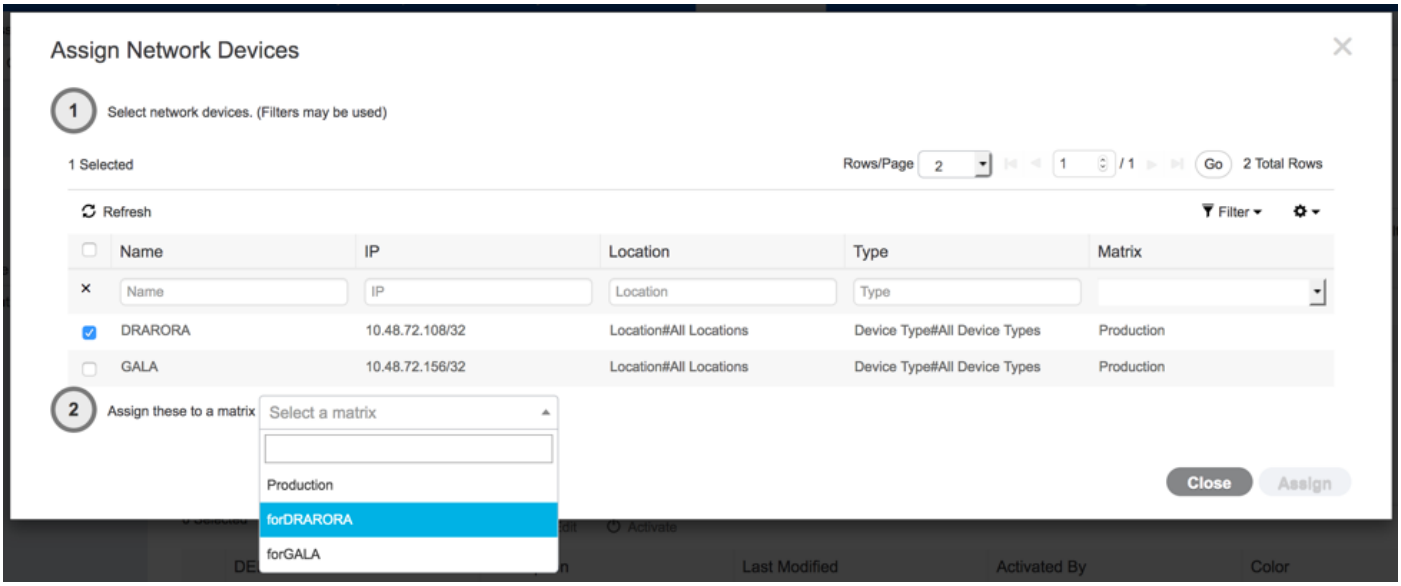


Wenn diese Option aktiviert ist, steht eine Standard-Produktionsmatrix zur Verfügung. Sie können jedoch auch andere Matrizen erstellen. Navigieren Sie zu **Work Centers > TrustSec > TrustSec Policy > Egress Policy > Matrices List**, und klicken Sie auf **Add**:

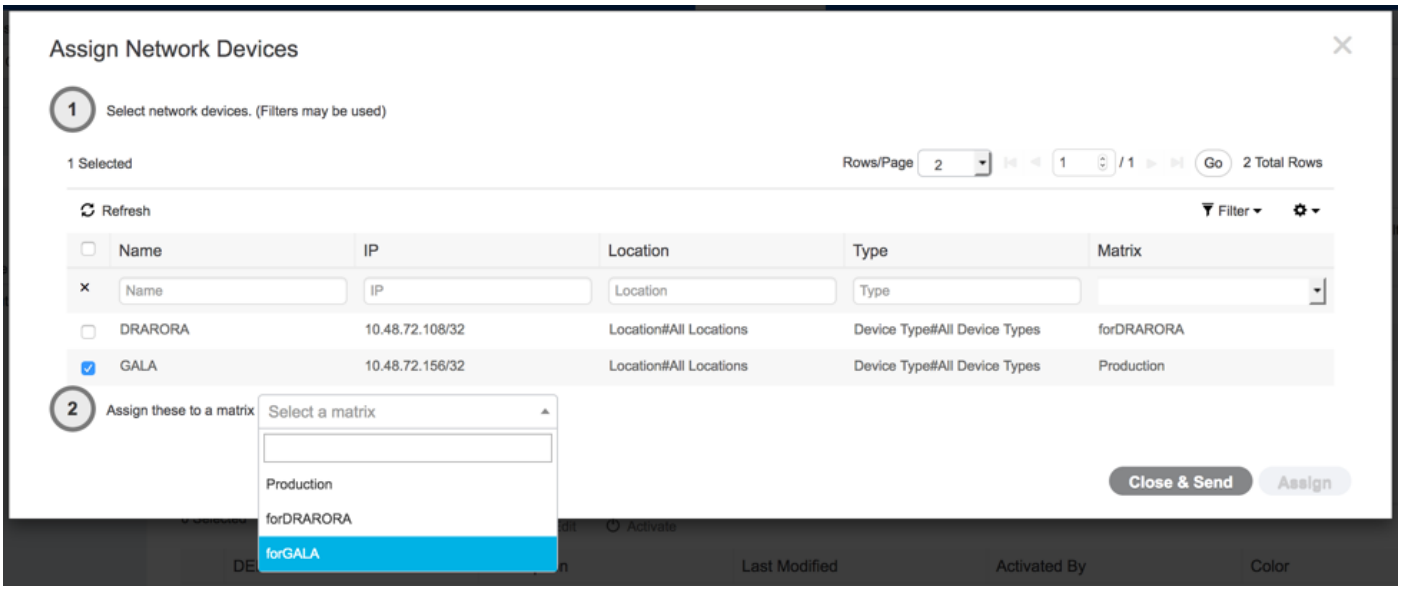
Es besteht die Möglichkeit, Richtlinien zu kopieren, die Teil der neuen Richtlinie aus der bereits vorhandenen Matrix werden sollten. Erstellen Sie zwei Matrizen - eine für den 3750X-Switch, eine weitere für den 3850-Switch. Nach dem Erstellen von Matrices müssen Sie diesen Matrizen Netzwerkgeräte zuweisen, da standardmäßig alle TrustSec-fähigen Netzwerkzugriffsgeräte der Produktionsmatrix zugewiesen sind.



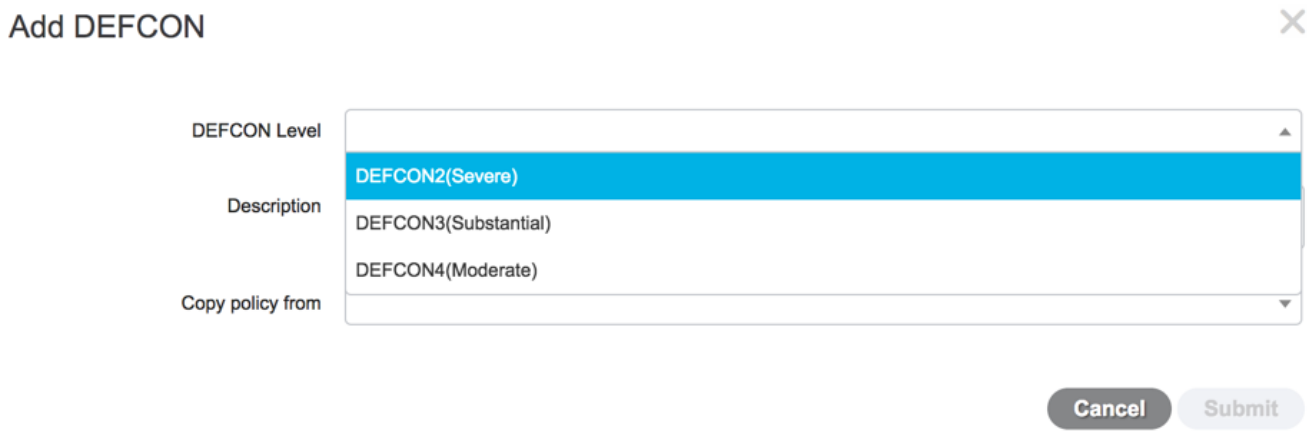
Um NADs zuzuweisen, klicken Sie unter Matrices List auf **Assign NADs (NADs zuweisen)**. Aktivieren Sie das Gerät, dem Sie die Matrix zuweisen möchten, und wählen Sie die erstellte Matrix aus dem Dropdown-Menü aus, und klicken Sie auf **Assign (Zuweisen)**, wie im Bild gezeigt:



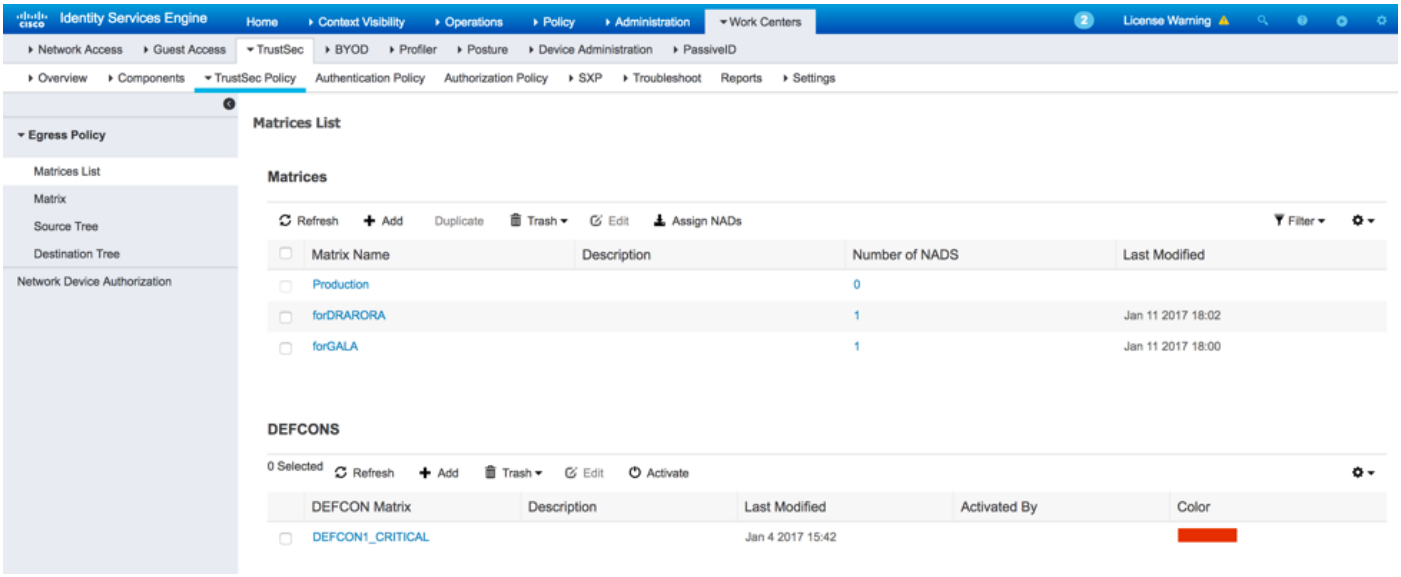
Sie können dies auch für andere Geräte tun, gefolgt von einem Klick auf die Schaltfläche **Zuweisen**:



Wenn alle Änderungen vorgenommen wurden, klicken Sie auf **Close&Send**, der alle Aktualisierungen an die Geräte sendet, um eine Aktualisierung der CTS-Richtlinien durchzuführen, um neue herunterzuladen. Erstellen Sie ebenfalls eine DefCon-Matrix, die Sie aus vorhandenen Matrizen kopieren können:



Die endgültigen Richtlinien sehen wie folgt aus:

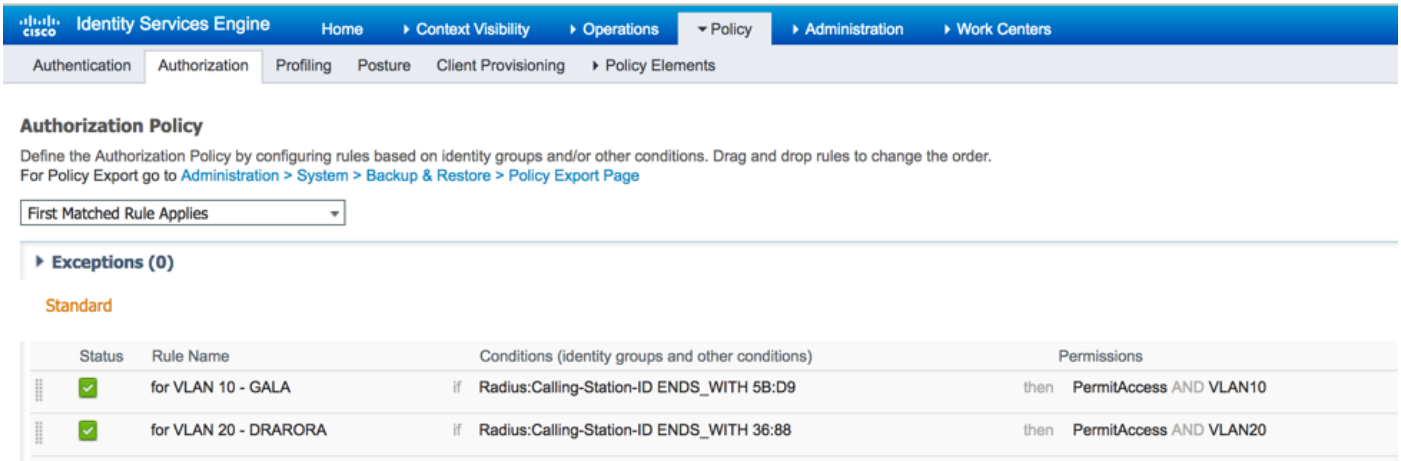


6. SGT-Klassifizierung

Es gibt zwei Optionen für Tags für Client-Zuweisungen (IP-SGT-Zuordnungen erstellen):

- *static* - mit **cts rollenbasiertem sgt-map** ***IP_address*** **sgt** ***tag***
- *dynamic* - via dot1x authentication (tag wird als Ergebnis der erfolgreichen Authentifizierung zugewiesen)

Verwenden Sie hier beide Optionen. Zwei Windows-Computer erhalten das SGT-Tag über die 802.1x-Authentifizierung und Loopback-Schnittstellen mit statischem SGT-Tag. Erstellen Sie zum Bereitstellen von dynamischer Zuordnung Autorisierungsrichtlinien für Endclients:



Um eine statische IP-SGT-Zuordnung zu erstellen, verwenden Sie Befehle (z. B. für 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
```

Nach erfolgreicher Authentifizierung trifft der Client auf die Autorisierungsrichtlinie mit einem spezifischen SGT-Tag, was zu folgenden Ergebnissen führt:

```
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
```

Sie können alle IP-SGT-Zuordnungen mit dem Befehl **show cts role-based sgt-map all** überprüfen, wobei Sie die Quelle jeder Zuordnung sehen (LOCAL - via dot1x-Authentifizierung, CLI - statische Zuweisung):

```
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. Herunterladen der CTS-Richtlinie

Sobald der Switch über CTS PAC verfügt und Umgebungsdaten heruntergeladen werden, kann er CTS-Richtlinien anfordern. Der Switch lädt nicht alle Richtlinien herunter, sondern nur diejenigen, die erforderlich sind - Richtlinien für Datenverkehr, der an bekannte SGT-Tags gerichtet ist - im Falle eines GALA-Switches fordert er von der ISE diese Richtlinien an:

- Richtlinie für Datenverkehr an SGT 15
- Richtlinie für Datenverkehr an SGT 10
- Richtlinie für Datenverkehr an SGT 16

Die Ausgabe aller Richtlinien für den GALA-Switch:

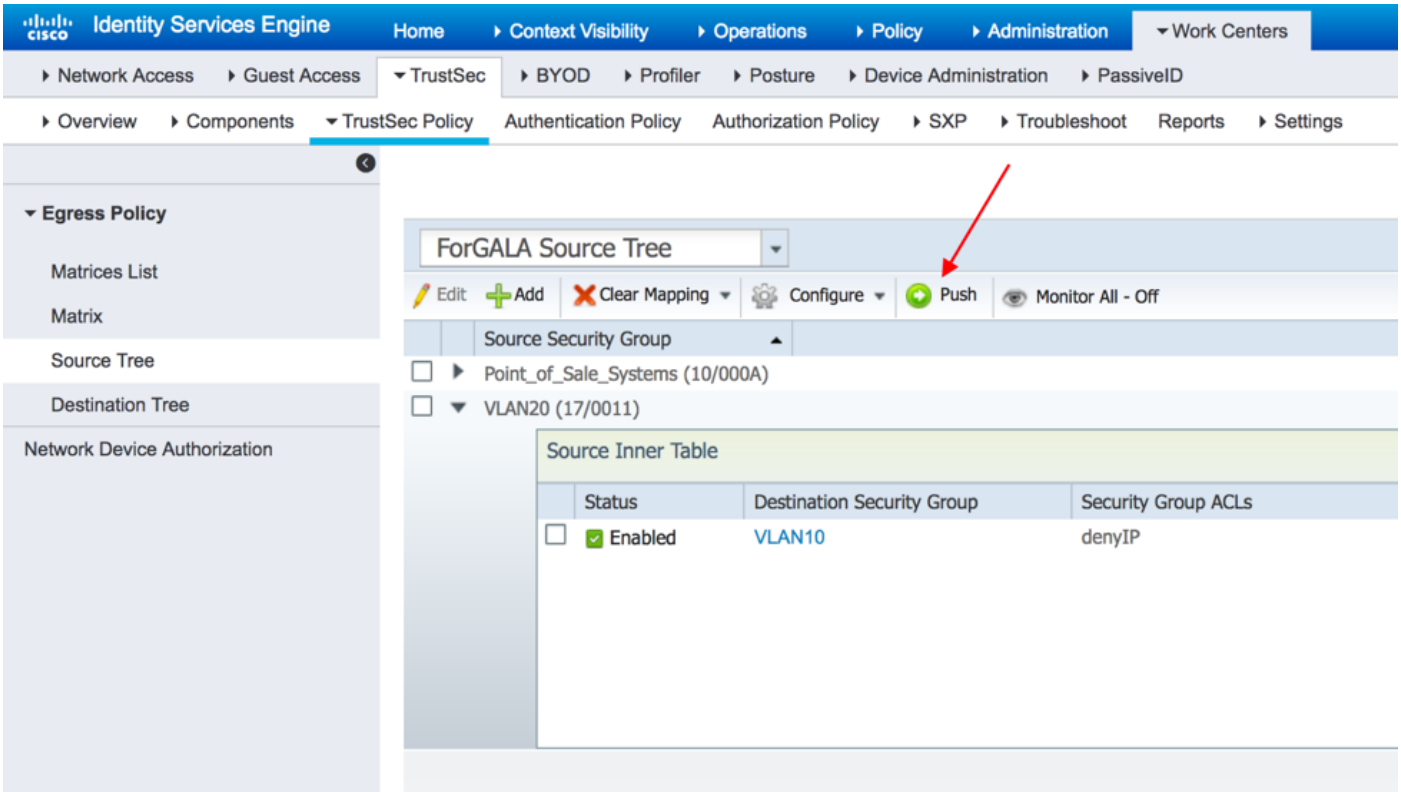
```
GALA#show cts role-based permissions
IPv4 Role-based permissions default:
Permit IP-00
IPv4 Role-based permissions from group 10:Point_of_Sale_Systems to group 15:BYOD:
denyIP-20
IPv4 Role-based permissions from group 17:VLAN20 to group 16:VLAN10:
denyIP-20
RBACL Monitor All for Dynamic Policies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

Der Switch erhält Richtlinien auf zwei Arten:

- CTS-Aktualisierung vom Switch selbst:

```
GALA#cts refresh policy
```

- Manueller Push von der ISE:



Überprüfen

Mehrere Matrizen

Die endgültigen SGT-IP-Zuordnungen und CTS-Richtlinien auf beiden Switches für dieses Beispiel:

GALA-Switch:

```
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-Switch:

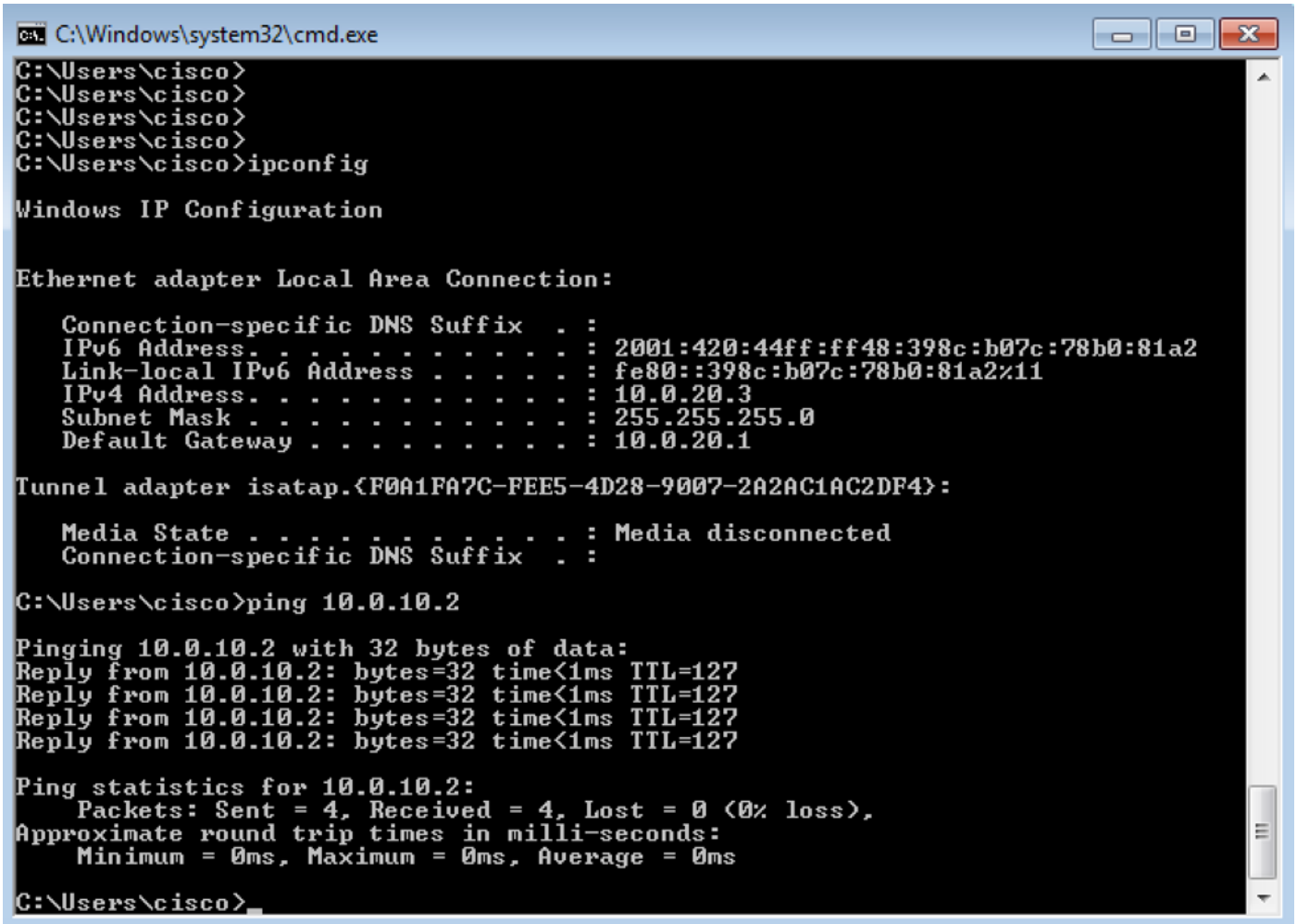
```
DRARORA#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

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
```

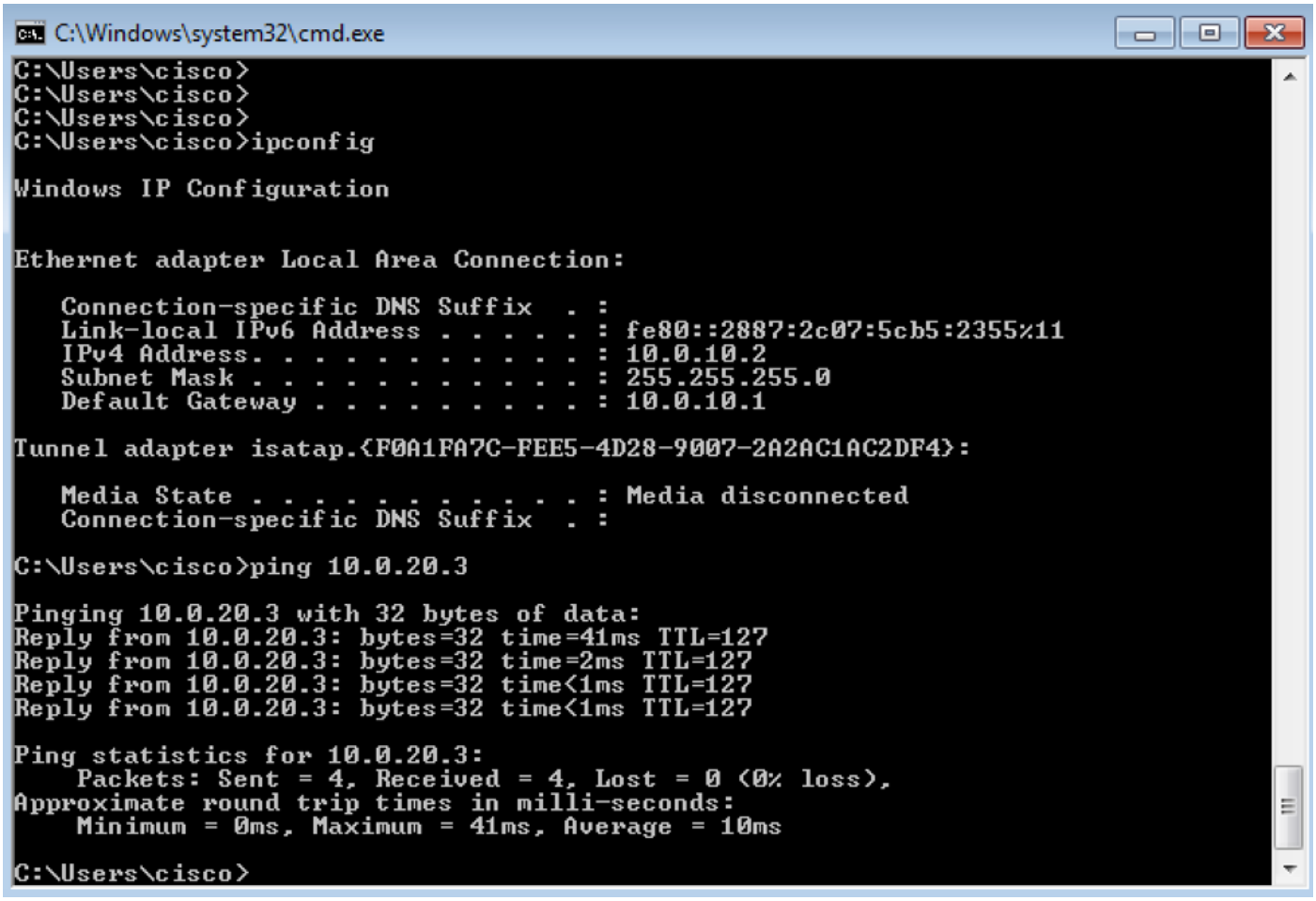
Beachten Sie, dass die Richtlinien für beide Switches unterschiedlich sind (für GALA- und DRARORA-Switches gelten sogar dieselben Richtlinien von 10 bis 15). Dies bedeutet, dass der Verkehr von SGT 10 bis 15 auf der DRARORA zugelassen, aber auf GALA blockiert ist:

```
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)
```

Ebenso können Sie von einem Fenster aus auf ein anderes zugreifen (SGT 17 -> SGT 16):



Eine andere Möglichkeit (SGT 16 -> SGT 17):



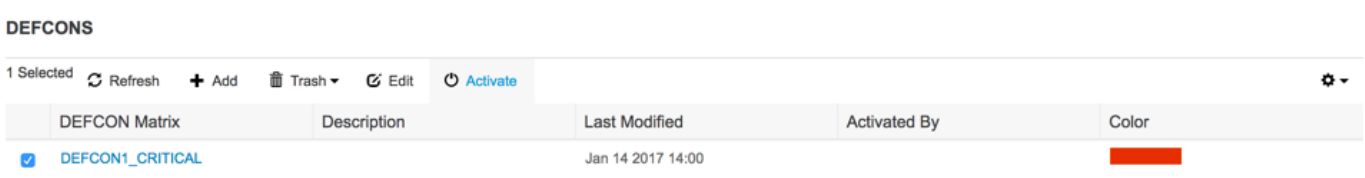
Um zu überprüfen, ob die richtige CTS-Richtlinie angewendet wurde, überprüfen Sie die Ausgabe der **rollenbasierten CTS-**Zähler:

```
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
```

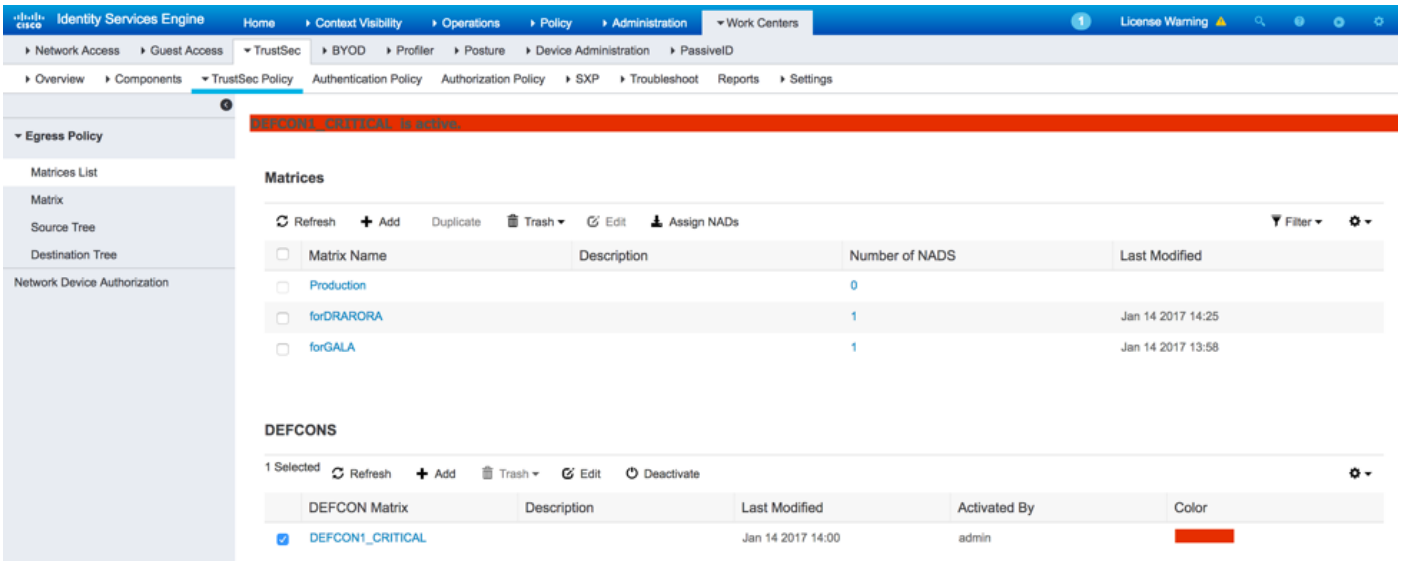
GALA verfügt über 8 zugelassene Pakete (4 von ping 17->16 und 4 von ping 16->17).

DefCon-Bereitstellung

Falls erforderlich, stellen Sie die DefCon-Matrix unter **Work Centers > TrustSec > TrustSec Policy > Egress Policy > Matrices List bereit**, aktivieren Sie die DefCon-Matrix, die Sie aktivieren möchten, und klicken Sie auf **Activate**:



Sobald DefCon aktiviert ist, sieht das Menü auf der ISE wie folgt aus:



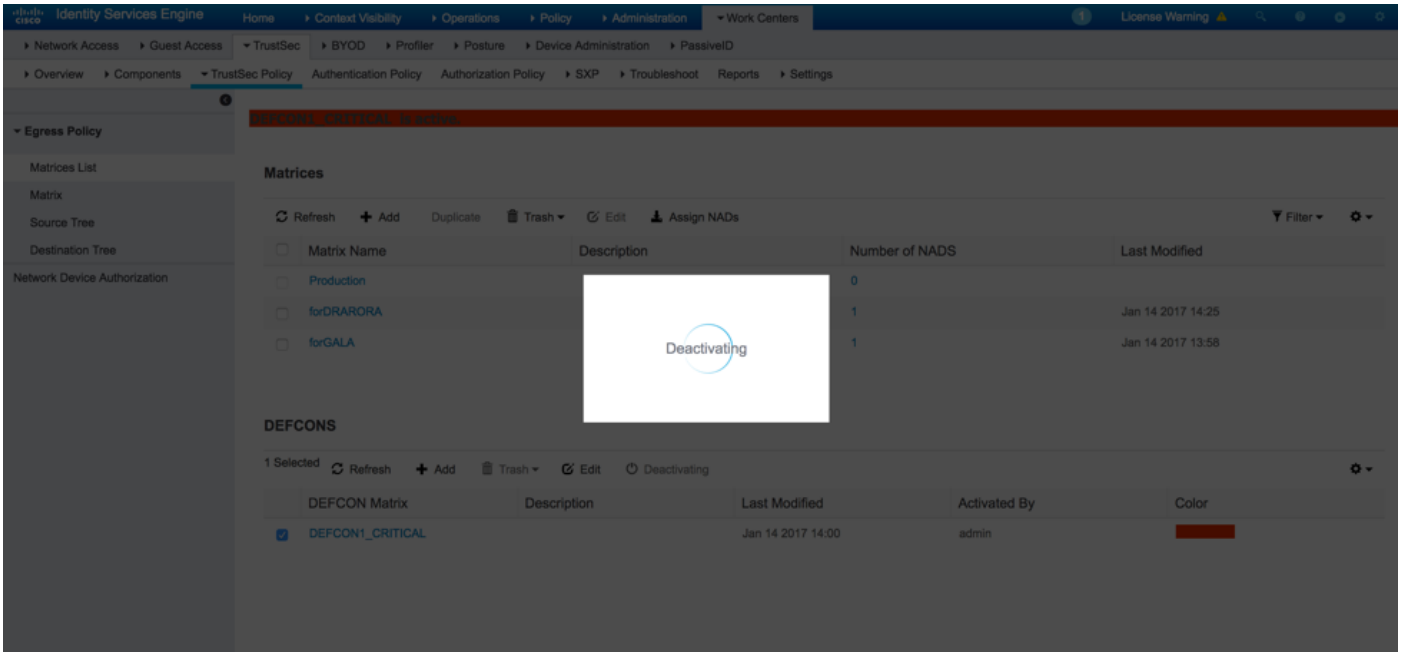
Richtlinien für Switches:

```
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
```

Der Datenverkehr zwischen SGT 15 und SGT 10 ist auf beiden Switches nicht zulässig:

```
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)
```

Sobald die Bereitstellung wieder stabil ist, können Sie DefCon deaktivieren und Switches fordern die alten Richtlinien an. Um DefCon zu deaktivieren, navigieren Sie zu **Work Centers > TrustSec > TrustSec Policy > Egress Policy > Matrices List**, aktivieren Sie die aktive DefCon-Matrix, und klicken Sie auf **Deaktivierung**:



Beide Switches fordern sofort alte Richtlinien an:

```
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
```

Fehlerbehebung

PAC-Bereitstellung

Dies ist Teil einer erfolgreichen PAC-Bereitstellung:

```
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
```

Die RADIUS-Ablehnung wird erwartet, da die PAC-Bereitstellung erfolgreich abgeschlossen wurde.

Download von Umgebungsdaten

Dies zeigt den erfolgreichen Download von Umgebungsdaten vom 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) 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
```

CTS-Richtlinien

CTS-Richtlinien werden als Teil von RADIUS-Meldungen durchgesetzt. Die **Laufzeitprotokollierungskomponente "Runtime-AAA"** wird auf "Debug on ISE" (**Administration > Logging > Debug Log Configuration**) und unter "Debug Log Configuration" (Debug-Protokollkonfiguration) auf dem Switch festgelegt, um alle Probleme im Zusammenhang mit CTS zu beheben:

```
debug cts coa
debug radius
```

Überprüfen Sie außerdem, welche Richtlinien auf dem Switch auf dem 3750X zugeordnet sind:

```
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               -
```

Aufgrund der CiscobugID CSCuu32958 können Sie denselben Befehl auf 3850 nicht verwenden.