Cisco ISE TrustSec-Zulassungslistenmodell (Standard Deny IP) mit SDA

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie das allow-list-Modell (Standard Deny IP) von TrustSec in Software Defined Access (SDA) aktiviert wird. Dieses Dokument enthält mehrere Technologien und Komponenten, darunter Identity Services Engine (ISE), Digital Network Architecture Center (DNAC) und Switches (Border and Edge).

Es stehen zwei TrustSec-Modelle zur Verfügung:

- Deny-List-Modell (IP mit Standardberechtigung): In diesem Modell lautet die Standardaktion "Permit IP" (IP zulassen), und alle Einschränkungen sollten explizit mit der Verwendung von Sicherheitsgruppen-Zugriffslisten (SGACLs) konfiguriert werden. Dies wird in der Regel dann verwendet, wenn Sie keinen vollständigen Überblick über die Datenverkehrsflüsse in ihrem Netzwerk haben. Dieses Modell ist ziemlich einfach zu implementieren.

- Zulassungslistenmodell (Standard-IP verweigern): In diesem Modell lautet die Standardaktion "IP verweigern". Daher sollte der erforderliche Datenverkehr explizit unter Verwendung von SGACLs zulässig sein. Dies wird in der Regel dann verwendet, wenn der Kunde die Art der Datenverkehrsflüsse innerhalb seines Netzwerks angemessen versteht. Dieses Modell erfordert eine detaillierte Untersuchung des Kontrollebenen-Datenverkehrs und hat das Potenzial, ALden Datenverkehr zu blockieren, sobald er aktiviert ist.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Dot1x/MAB-Authentifizierung
- Cisco TrustSec (CTS)
- Security Exchange Protocol (SXP)
- Webproxy
- Firewall-Konzepte
- DNAC

Verwendete Komponenten

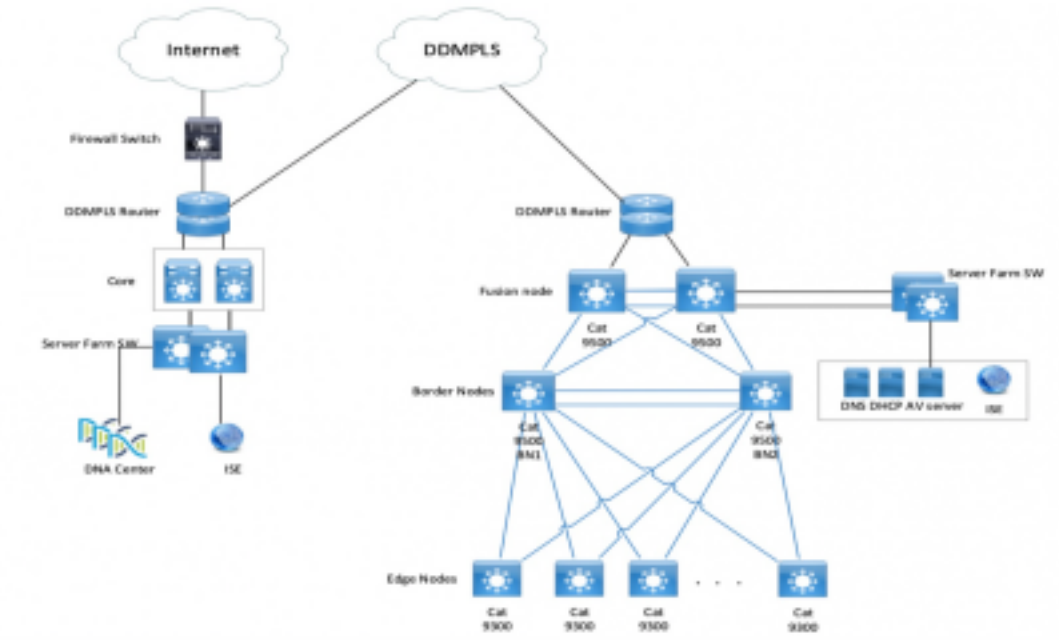
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- 9300 Edge- und 9500-Grenzknoten (Switches) mit IOS 16.9.3
- DNAC 1.3.0.5
- ISE 2.6 Patch 3 (zwei Knoten - redundante Bereitstellung)
- DNAC und ISE sind integriert
- Grenz- und Edge-Knoten werden von DNAC bereitgestellt
- Der SXP-Tunnel wird von der ISE (Lautsprecher) zu beiden Grenzknoten (Listener) eingerichtet.
- IP-Adresspools werden zum Hosting hinzugefügt

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.

Konfigurieren

Netzwerkdiagramm



Konfiguration

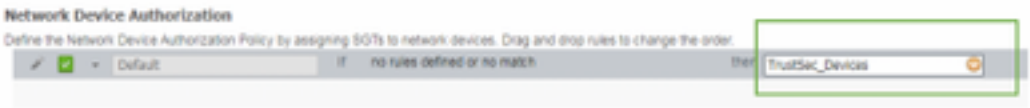
Dies sind die Schritte zum Aktivieren des Zulassungslistenmodells (Standard-IP-Adresse verweigern):

1. Ändern Sie das SGT von Unknown zu TrustSec Devices.
2. Deaktivieren Sie die rollenbasierte CTS-Durchsetzung.
3. IP-SGT-Zuordnung an Border- und Edge-Switches mithilfe der DNAC-Vorlage.
4. Fallback-SGACL mit DNAC-Vorlage.
5. Aktivieren der Zulassungsliste (Standard-IP verweigern) in der TrustSec-Matrix.
6. Erstellen Sie ein SGT für Endgeräte/Benutzer.
7. Erstellen Sie SGACL für Endgeräte/Benutzer (für Produktions-Overlay-Datenverkehr).

Schritt 1: Ändern Sie das SGT von Unknown zu TrustSec Devices.

Standardmäßig ist die unbekannte Security Group Tag (SGT) für die Autorisierung von Netzwerkgeräten konfiguriert. Die Änderung auf TrustSec-Geräte-SGT bietet mehr Transparenz und hilft bei der Erstellung von SGACLs speziell für Switch-initiierten Datenverkehr.

Navigieren Sie zu **Work Centers > TrustSec > TrustSec Policy > Network Device Authorization** (**Arbeitscenter > TrustSec > TrustSec-Richtlinie > Netzwerkgeräteautorisierung**), und ändern Sie sie dann in TrustSec_Devices (Vertrauenswürdige Geräte) von Unknown



Schritt 2: Deaktivieren Sie die rollenbasierte CTS-Durchsetzung.

- Sobald das Allow-List-Modell (Default Deny) eingerichtet ist, wird der gesamte Datenverkehr in der Fabric blockiert, einschließlich des zugrunde liegenden Multicast- und Broadcast-Datenverkehrs wie Intermediate System-to-Intermediate System (IS-IS), Bidirectional

Forwarding Detection (BFD), Secure Shell (SSH).

- Alle 10Gig-Ports, die mit dem Fabric-Edge verbunden sind, sowie der Rahmen sollten mit dem folgenden Befehl konfiguriert werden. Wenn diese Schnittstelle aktiviert ist, wird der von dieser Schnittstelle initiierte Datenverkehr nicht durchgesetzt.

```
Interface tengigabitethernet 1/0/1

no cts role-based enforcement
```

> **Hinweis**: Dies kann durch Verwendung einer Bereichsvorlage in DNAC erfolgen, um die Komplexität zu erhöhen. Andernfalls muss der Switch bei der Bereitstellung manuell konfiguriert werden. Der folgende Ausschnitt zeigt, wie dies über eine DNAC-Vorlage geschieht.

```
interface range $uplink1

no cts role-based enforcement
```

Weitere Informationen zu DNAC-Vorlagen *finden Sie* in diesem Dokument.

https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2-1/user_guide/b_dnac_ug_1_2_1/b_dnac_ug_1_2_chapter_010000.html

Schritt 3: IP-SGT-Zuordnung auf Grenz- und Edge-Switches mit DNAC-Vorlage.

Es wird empfohlen, die lokale IP-SGT-Zuordnung auf den Switches bereitzustellen, selbst wenn die gesamte ISE ausfällt. So wird Underlay aktiviert und die Verbindung zu den kritischen Ressourcen bleibt erhalten.

Der erste Schritt besteht darin, kritische Services an ein SGT zu binden (ex - Basic_Network_Services/1000). Zu diesen Services gehören:

- Underlay/ISIS-Subnetz
- ISE/DNAC
- Überwachungs-Tool
- AP-Subnetz bei OTT
- Terminalserver
- Critical Services - Bsp.: IP-Telefon

Beispiel:

```
cts role-based sgt-map <ISE/DNAC Subnet> sgt 1000

cts role-based sgt-map  sgt 2

cts role-based sgt-map <Wireless OTT Infra> sgt 1000

cts role-based sgt-map <Underlay OTT AP Subnet> sgt 2

cts role-based sgt-map <Monitoring Tool IP> sgt 1000
```

```
cts role-based sgt-map vrf CORP_VN <Voice Gateway and CUCM Subnet> sgt 1000
```

Schritt 4: Fallback-SGACL mit DNAC-Vorlage.

Eine SGT-Zuordnung ist erst dann von Nutzen, wenn eine relevante SGACL mit dem SGT erstellt wurde. Im nächsten Schritt wird daher eine SGACL erstellt, die als lokaler Fallback fungiert, wenn ISE-Knoten ausfallen (wenn ISE-Dienste ausfallen, der SXP-Tunnel ausfällt und somit SGACLs und die IP-SGT-Zuordnung nicht dynamisch heruntergeladen wird).

Diese Konfiguration wird an alle Edge- und Randknoten übertragen.

Rollenbasierte Fallback-ACL/Vertrag:

```
ip access-list role-based FALLBACK

permit ip
```

TrustSec-Geräte für TrustSec-Geräte:

```
cts role-based permissions from 2 to 2 FALLBACK
```

Über SGACL Sicherstellen der Kommunikation innerhalb von Fabric-Switches und untergeordneten IPs

TrustSec-Geräte für SGT 1000:

```
cts role-based permissions from 2 to 1000 FALLBACK
```

Über SGACL Sicherstellen der Kommunikation von Switches und Access Points zur ISE, DNAC, WLC und Überwachungstools

SGT 1000 zu TrustSec-Geräten:

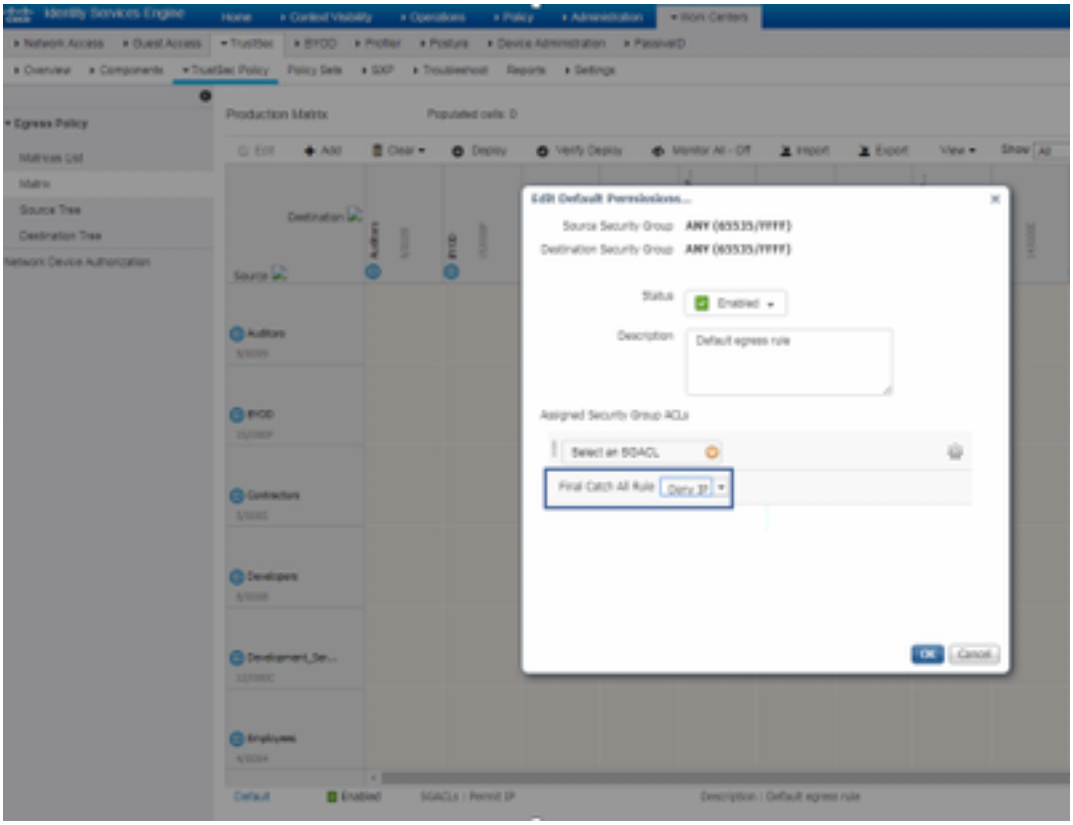
```
cts role-based permissions from 1000 to 2 FALLBACK
```

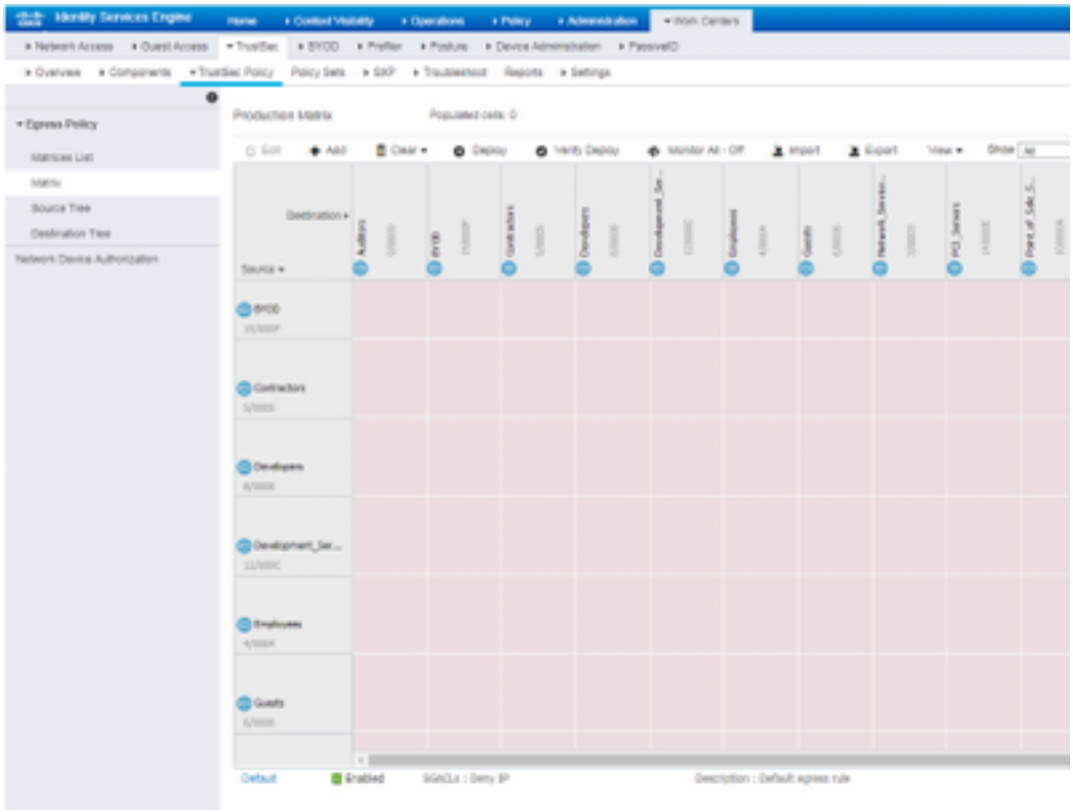
Über SGACL Sicherstellen der Kommunikation von Access Points zur ISE, DNAC, WLC und Überwachungstools zu Switches

Schritt 5: Aktivieren Sie in der TrustSec-Matrix das Allow-List-Modell (Standard Deny).

Die Anforderung besteht darin, den Großteil des Datenverkehrs im Netzwerk zu verweigern und einen geringeren Umfang zuzulassen. Wenn Sie die Standardeinstellung "Ablehnen" mit expliziten Genehmigungsregeln verwenden, sind weniger Richtlinien erforderlich.

Navigieren Sie zu **Work Center > TrustSec > TrustSec Policy > Matrix > Default** und ändern Sie sie in **Deny All** in final catch Rule (Alle **verweigern**).





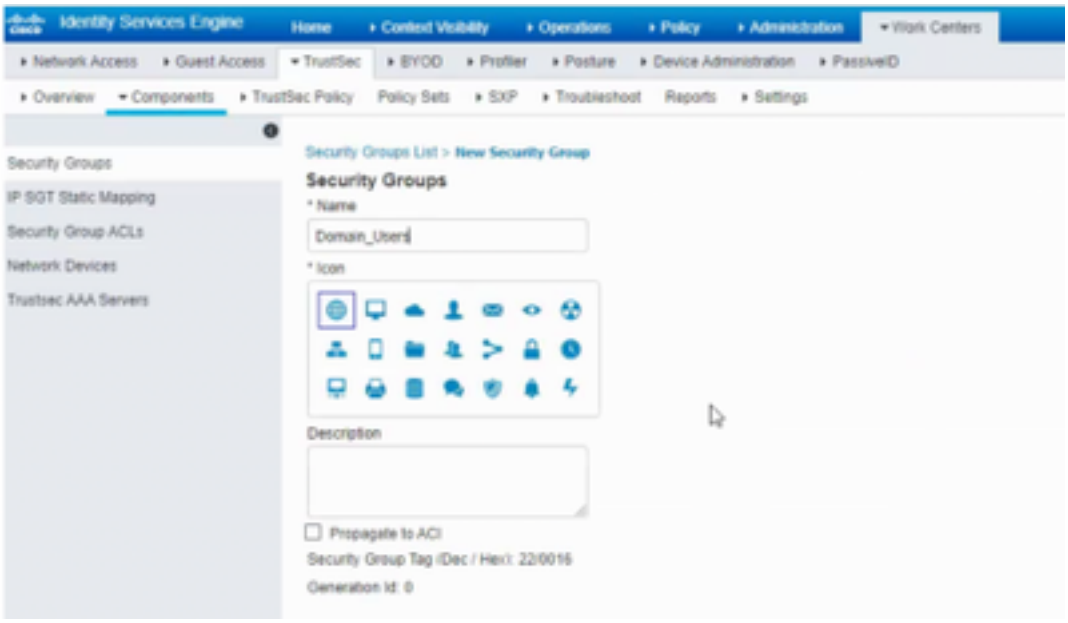
Hinweis: Dieses Bild stellt dar (Alle Spalten sind standardmäßig rot), die Standardeinstellung "Verweigern" wurde aktiviert und nur selektiver Datenverkehr kann nach der Erstellung der SGACL zugelassen werden.

Schritt 6: Erstellen Sie ein SGT für Endgeräte/Benutzer.

In der SDA-Umgebung sollte ein neues SGT nur über die DNAC-GUI erstellt werden, da es

aufgrund der Nichtübereinstimmung der SGT-Datenbank in ISE/DNAC zahlreiche Fälle von Datenbankbeschädigung gibt.

Um ein SGT zu erstellen, melden Sie sich bei **DNAC > Policy > Group-Based Access Control > Scalable Groups > Add Groups**, eine Seite leitet Sie zur **ISE Scalable Group** um, klicken Sie auf **Hinzufügen,** geben Sie den SGT-Namen ein und speichern Sie ihn.



Dasselbe SGT spiegelt sich in DNAC durch PxGrid-Integration wider. Dies ist das gleiche Verfahren für alle zukünftigen SGT-Erstellung.

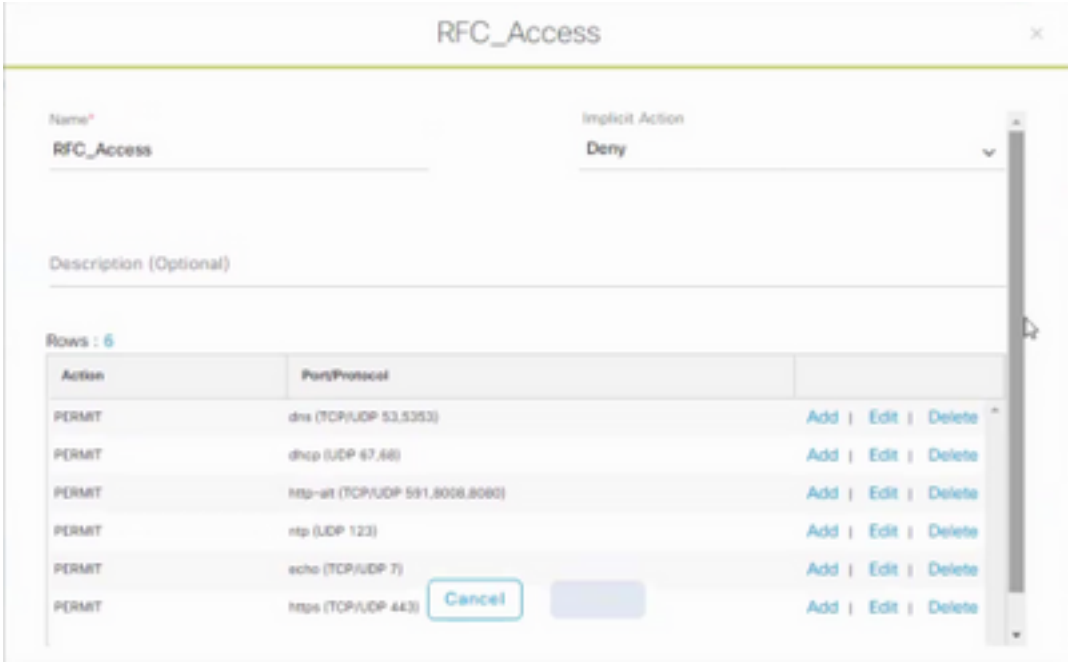
Schritt 7: Erstellen Sie SGACL für Endgeräte/Benutzer (für Produktions-Overlay-Datenverkehr).

In der SDA-Umgebung sollte ein neues SGT nur über die DNAC-GUI erstellt werden.

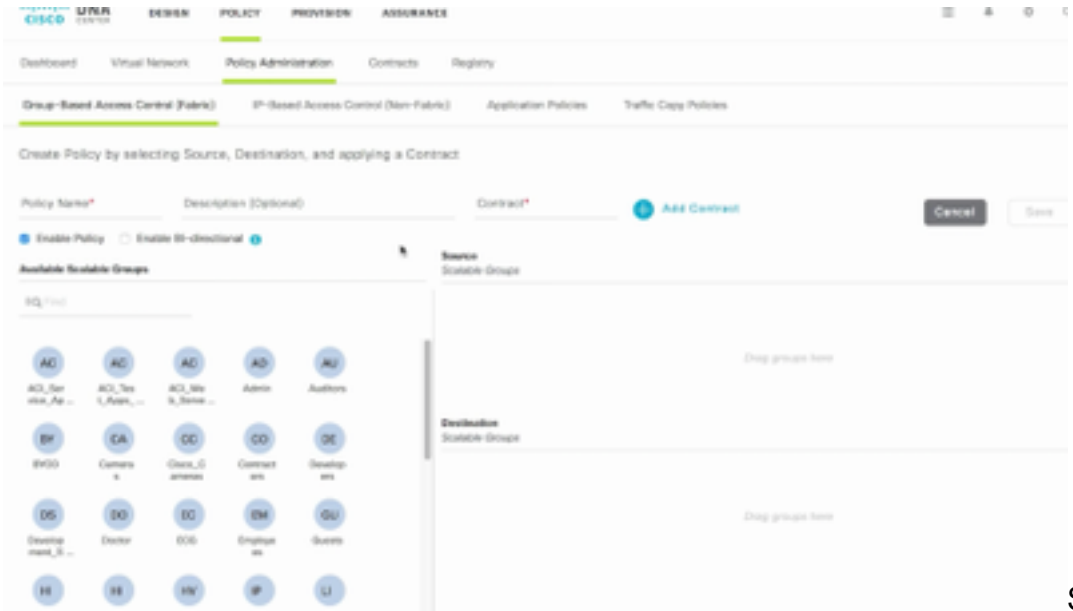
```
Policy Name: Domain_Users_Access

Contract : Permit

Enable Policy :

Enable Bi-Directional :

Source SGT : Domain Users (Drag from Available Security Group)

Destination SGT: Domain_Users, Basic_Network_Services, DC_Subnet, Unknown (Drag from Available
Security Group)


Policy Name: RFC_Access

Contract : RFC_Access (This Contract contains limited ports)

Enable Policy :

Enable Bi-Directional :

Source SGT : Domain Users (Drag from Available Security Group)
```

```
Destination SGT: RFC1918 (Drag from Available Security Group)
```

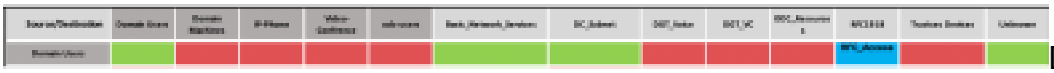
Um einen **Vertrag** zu erstellen, melden Sie sich bei **DNAC an** und navigieren Sie zu **Richtlinien > Verträge > Verträge hinzufügen > Erforderliches Protokoll hinzufügen** und klicken Sie dann auf **Speichern**.



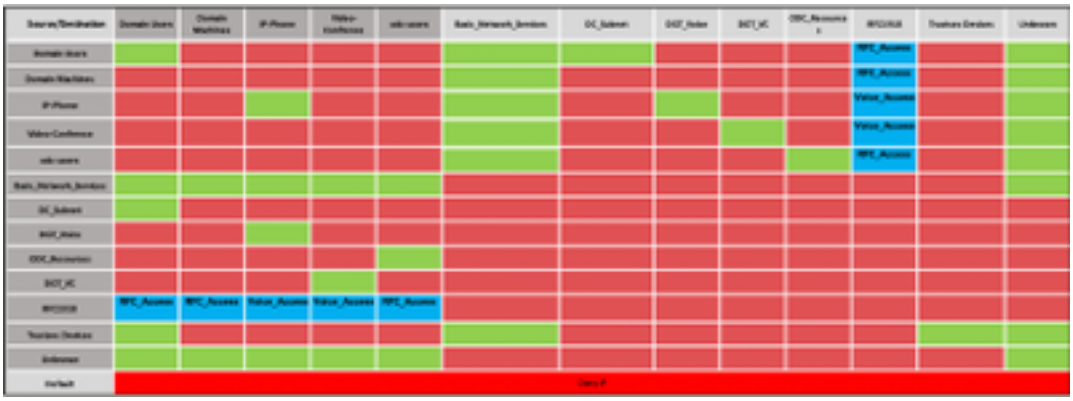
Um einen **Vertrag** zu erstellen, melden Sie sich bei **DNAC** an und navigieren Sie zu **Policy > Group-Based Access Control > Group-Based-Access-Policies > Add Policies > Create policy (Policy > Group-Based Access Control > Group-Based-Access-Policies > Add Policies > Create policy (mit den angegebenen Informationen)**. Klicken Sie jetzt auf **Save** und **Deploy.**

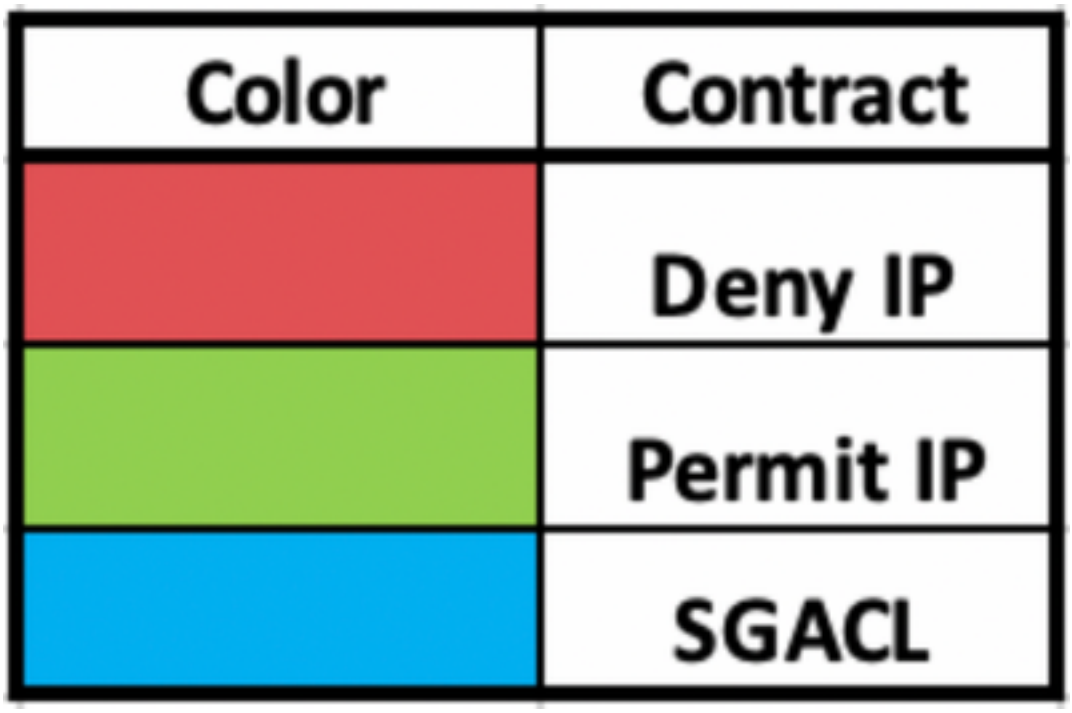


Sobald SGACL/Contract von DNAC konfiguriert wurde, wird es automatisch in ISE wiedergegeben. unten sehen Sie ein Beispiel für eine unidirektionale Matrx-Ansicht für einen Sgt.



Die SGACL-Matrix, wie in der Abbildung unten gezeigt, ist eine Beispielansicht für das Modell der Zulassungsliste (Standard-Verweigern).





Überprüfen

SGT für Netzwerkgeräte

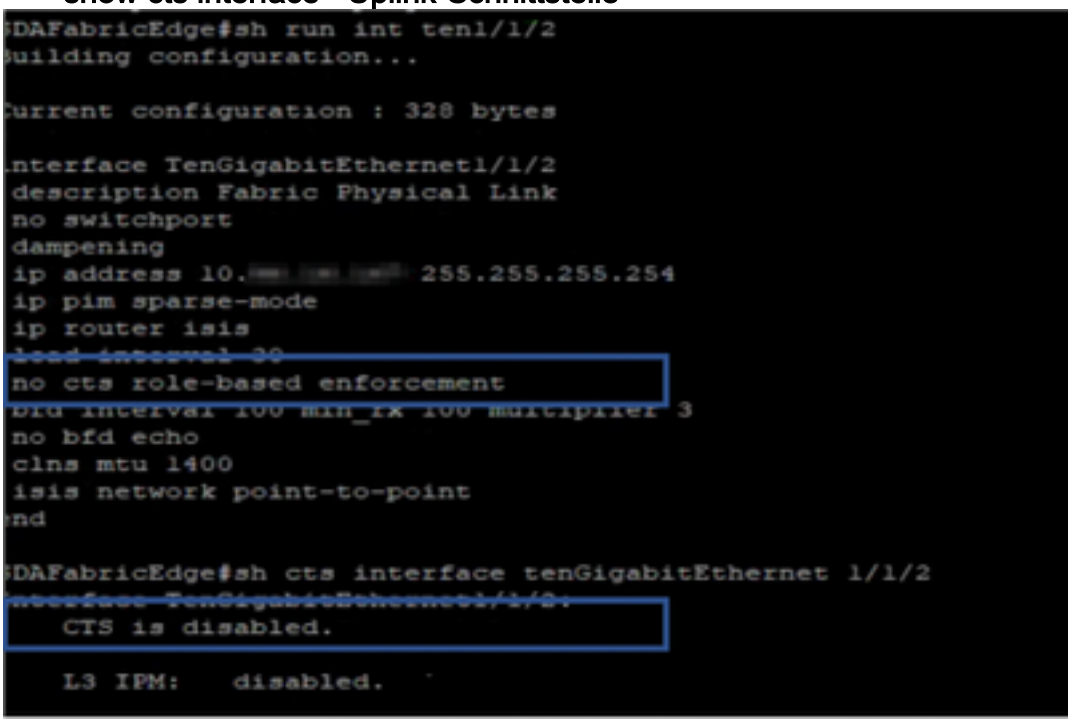
Führen Sie den folgenden Befehl aus, um die von der ISE empfangenen Switches SGT zu überprüfen: **Umgebungsdaten anzeigen**

```
SDAFabricEdge#sh cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 2-15:TrustSec_Devices
Server List Info:
Installed list: CTSServerList1-0002, 2 server(s):
  Server: 10.[redacted], port 1812, A-ID B6220695C1B21F6F3556E3C5F57B9D6E
          Status = ALIVE
          auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
  Server: 10.[redacted], port 1812, A-ID B6220695C1B21F6F3556E3C5F57B9D6E
          Status = ALIVE
          auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Security Group Name Table:
    0-00:Unknown
    2-00:TrustSec_Devices
```

Durchsetzung an Uplink-Ports

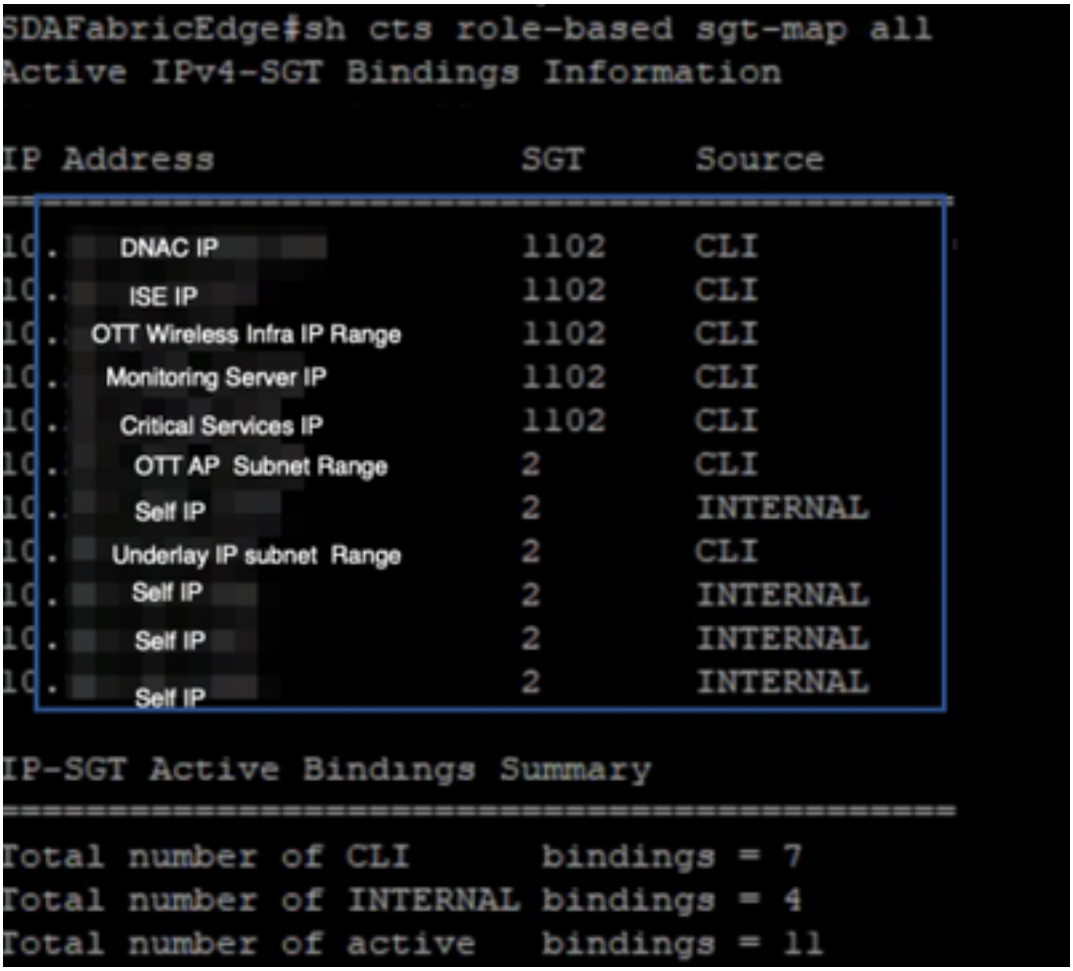
Führen Sie folgende Befehle aus, um die Durchsetzung auf der Uplink-Schnittstelle zu überprüfen:

- show run interface <Uplink>
- show cts interface <Uplink-Schnittstelle>



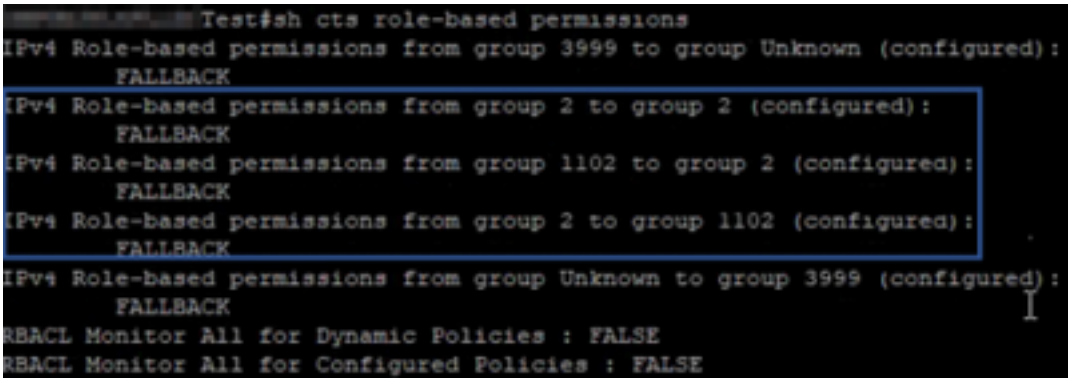
Lokale IP-SGT-Zuordnung

Um lokal konfigurierte IP-SGT-Zuordnungen zu überprüfen, führen Sie den folgenden Befehl aus:
sh cts role-based sgt-map all



Lokales FALLBACK-SGACL

Führen Sie zum Überprüfen von FALLBACK SGACL den folgenden Befehl aus: **sh cts role-based permit**



Hinweis: Die von der ISE bereitgestellte SGACL hat eine Priorität vor der lokalen SGACL.

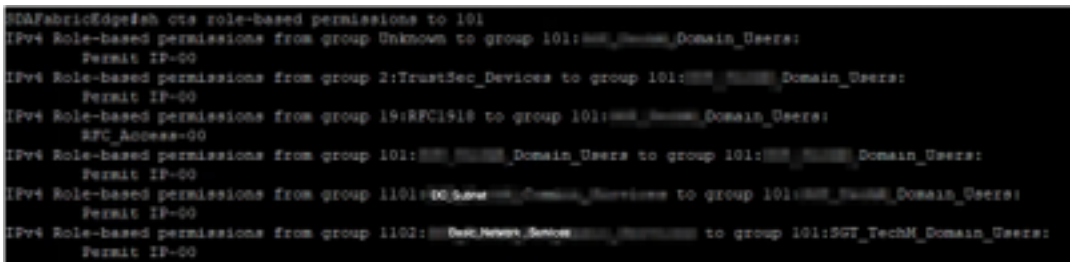
Listenzulassung (Standard-Verweigern) auf Fabric-Switches

Führen Sie den folgenden Befehl aus, um das Allow-list-Modell (Default Deny) zu überprüfen: **sh cts role-based permit**

```
SDAFabricEdge#sh cts role-based permissions
IPv4 Role-based permissions default:
        Deny IP-00
```

Mit Fabric verbundenes SGACL für Endgeräte

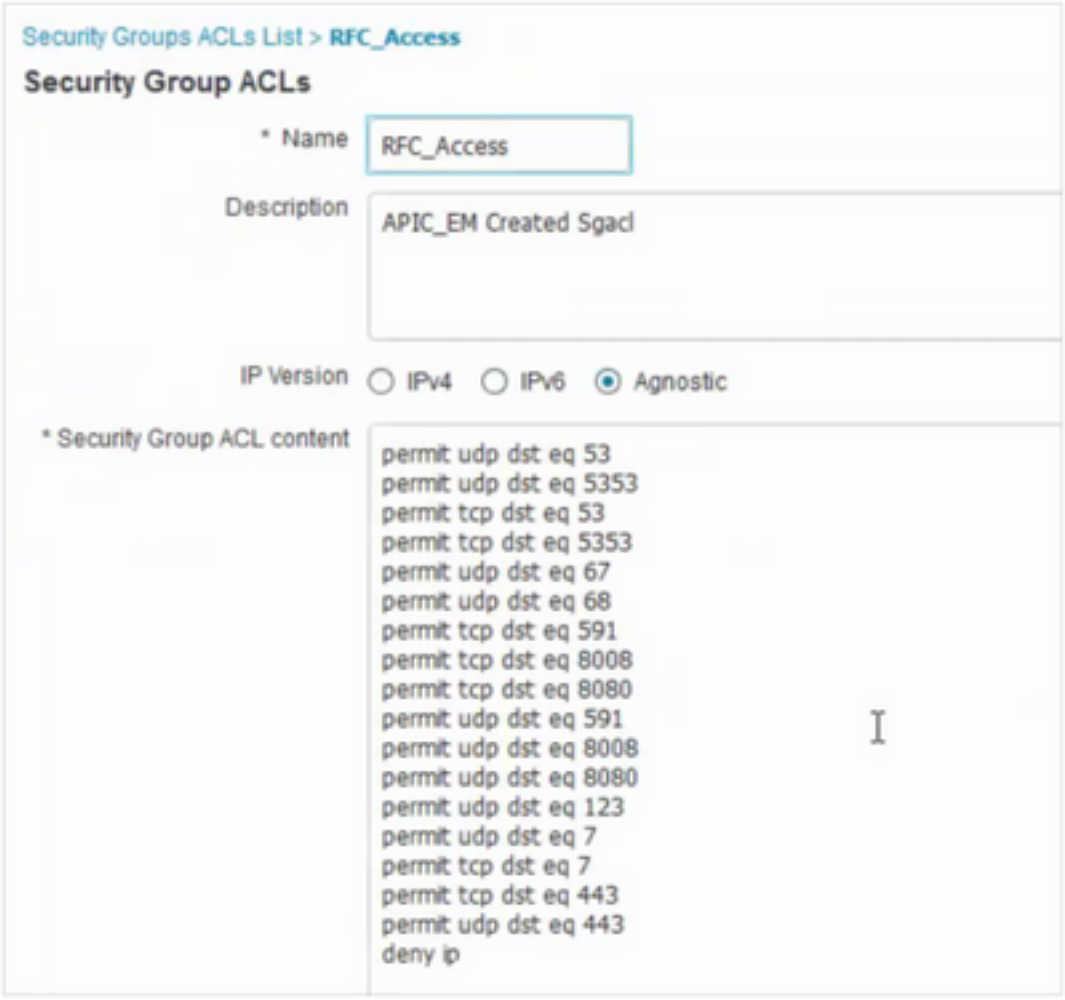
Führen Sie zum Überprüfen der von der ISE heruntergeladenen SGACL den folgenden Befehl aus: **sh cts role-based permit**



Von DNAC erstellter Vertrag überprüfen

Führen Sie zum Überprüfen der von der ISE heruntergeladenen SGACL den folgenden Befehl aus: **show access-list <ACL/Vertragsname>**

```
Role-based IP access list RFC_Access-00 (downloaded)
    10 permit udp dst eq domain
    20 permit udp dst eq 5353
    30 permit tcp dst eq domain
    40 permit tcp dst eq 5353
    50 permit udp dst eq bootps
    60 permit udp dst eq bootpc
    70 permit tcp dst eq 591
    80 permit tcp dst eq 8008
    90 permit tcp dst eq 8080
    100 permit udp dst eq 591
    110 permit udp dst eq 8008
    120 permit udp dst eq 8080
    130 permit udp dst eq ntp
    140 permit udp dst eq echo
    150 permit tcp dst eq echo
    160 permit tcp dst eq 443
    170 permit udp dst eq 443
    180 deny ip
```



SGACL-Zähler auf Fabric-Switches ausführen

Führen Sie zum Überprüfen von SGACL-Richtlinienzugriffen den folgenden Befehl aus:
Rollenbasierter Zähler anzeigen

```
Role-based IPv4 counters
From    To      SW-Denied  HW-Denied  SW-Permitt HW-Permitt SW-Monitor HW-Monitor
*       *       0          0          0          0          0          0
2       2       0          0          1644843    0          0          0
1101    2       0          0          0          0          0          0
1102    2       0          0          0          0          0          0
101     101     0          0          0          0          0          0
1101    101     0          0          0          57647      0          0
1102    101     0          0          0          12541      0          0
1103    101     0          0          0          25         0          0
```

Fehlerbehebung

Ausgabe 1 Wenn beide ISE-Knoten ausgefallen sind.

Wenn beide ISE-Knoten ausgefallen sind, wird die von der ISE empfangene IP-zu-SGT-Zuordnung entfernt, alle DGTs werden als unbekannt gekennzeichnet, und alle vorhandenen Benutzersitzungen werden nach 5-6 Minuten beendet.

> **Hinweis**: Dieses Problem tritt nur auf, wenn der Zugriff auf sgt (xxxx) -> unbekannte (0) SGACL auf DHCP-, DNS- und Webproxy-Port beschränkt ist.

Lösung:

1. SGT erstellt (z. B. RFC 1918).
2. Push RFC Private IP Range (privater RFC-IP-Bereich) an beiden Rändern.
3. Einschränken des Zugriffs auf DHCP, DNS und Webproxy von sgt (xxxx) —> RFC1918
4. Erstellen/Ändern von sgacl sgt (xxxx) —> unbekannt mit dem Permit IP-Vertrag.

Wenn nun beide ise-Knoten ausfallen, werden SGACL sgt—>unbekannte Treffer und die existierende Sitzung intakt.

Ausgabe 2: IP-Telefon: unidirektionale Sprachübertragung oder ohne Sprachübertragung.

Die Umwandlung von Erweiterung auf IP erfolgte auf SIP, und die eigentliche Sprachkommunikation erfolgt über RTP zwischen IP und IP. CUCM und Voice Gateway wurden **DGT_Voice** hinzugefügt.

Lösung:

1. Derselbe Standort oder Ost-West-Sprachkommunikation kann aktiviert werden, indem Datenverkehr vom IP_Phone —> IP_Phone zugelassen wird.
2. Der restliche Standort kann durch den RTP-Protokollbereich für das Zulassen in DGT RFC 1918 zugelassen werden. Der gleiche Bereich kann für IP_Phone —> Unknown (IP_Telefon —> Unbekannt) zugelassen werden.

Ausgabe 3 Kritischer VLAN-Endpunkt hat keinen Netzwerkzugriff.

DNAC stellt einen Switch mit einem kritischen VLAN für Daten bereit. Gemäß der Konfiguration erhalten alle neuen Verbindungen bei ISE-Ausfall ein kritisches VLAN und ein SGT 3999. Die Standardrichtlinie 'Verweigern in TrustSec' schränkt die neue Verbindung für den Zugriff auf Netzwerkressourcen ein.

Lösung:

Push SGACL for Critical SGT on All Edge and Border Switches using DNAC Template

```
cts role-based permissions from 0 to 3999 FALLBACK

cts role-based permissions from 3999 to 0 FALLBACK
```

Diese Befehle werden dem Konfigurationsabschnitt hinzugefügt.

> **Hinweis**: Alle Befehle können in einer einzelnen Vorlage zusammengefasst und bei der Bereitstellung gedrückt werden.

Ausgabe 4: Paket-Drop-in-kritisches VLAN

Wenn sich der Computer aufgrund von ISE-Knoten im kritischen VLAN befindet, wird alle 3 bis 4 Minuten ein Paketverlust (maximal 10 Verwerfungen) für alle Endpunkte im kritischen VLAN festgestellt.

Beobachtungen: Die Anzahl der Authentifizierungszähler erhöht sich, wenn Server DEAD sind. Clients versuchen, sich mit PSN zu authentifizieren, wenn die Server als DEAD markiert wurden.

Lösung/Problemumgehung:

Im Idealfall sollte es keine Authentifizierungsanfrage von einem Endpunkt geben, wenn ISE-PSN-Knoten ausgefallen sind.

Drücken Sie diesen Befehl unter Radius-Server mit DNAC:

automatische Testerkennung für Benutzernamen

Mit diesem Befehl im Switch werden regelmäßig Testauthentifizierungsmeldungen an den RADIUS-Server gesendet. Er sucht vom Server nach einer RADIUS-Antwort. Eine Erfolgsmeldung ist nicht erforderlich - eine fehlgeschlagene Authentifizierung reicht aus, weil sie zeigt, dass der Server aktiv ist.

Zusätzliche Informationen

DNAC-abschließende Vorlage:

```
interface range $uplink1

no cts role-based enforcement

! .

cts role-based sgt-map <ISE Primary IP> sgt 1102

cts role-based sgt-map <Underlay Subnet> sgt 2

cts role-based sgt-map <Wireless OTT Subnet>sgt 1102

cts role-based sgt-map <DNAC IP> sgt 1102

cts role-based sgt-map <SXP Subnet> sgt 2

cts role-based sgt-map <Network Monitoring Tool IP> sgt 1102

cts role-based sgt-map vrf CORP_VN <Voice Gateway Subnet> sgt 1102

!

ip access-list role-based FALLBACK

permit ip

!

cts role-based permissions from 2 to 1102 FALLBACK

cts role-based permissions from 1102 to 2 FALLBACK

cts role-based permissions from 2 to 2 FALLBACK

cts role-based permissions from 0 to 3999 FALLBACK
```

```
cts role-based permissions from 3999 to 0 FALLBACK
```

Hinweis: Alle Uplink-Schnittstellen in Edge-Knoten werden ohne Durchsetzung konfiguriert. Es wird davon ausgegangen, dass der Uplink nur mit dem Grenzknoten verbunden ist. Bei Grenzknoten müssen Uplink-Schnittstellen zu Edge-Knoten ohne Durchsetzung konfiguriert werden. Dies muss manuell erfolgen.