Cisco ISE TrustSec Allow-List model (standaard Dense IP) met SDA

Inhoud

Inleiding

Dit document beschrijft hoe u het allow-list (Default Deny IP) model van TrustSec in Software Defined Access (SDA) kunt inschakelen. Dit document bevat meerdere technologie en onderdelen, waaronder Identity Services Engine (ISE), Digital Network Architecture Center (DNA) en switches (Border en Edge).

Er zijn twee modellen Trustsec beschikbaar:

- Model van toegangslijst (standaard IP-vergunning): In dit model is de standaardactie Toestaan IP en alle beperkingen moeten expliciet worden ingesteld met het gebruik van Security Group Access Lists (SGACL's). Dit wordt over het algemeen gebruikt wanneer u geen volledig begrip van verkeersstromen binnen hun netwerk hebt. Dit model is vrij gemakkelijk te implementeren.

- Model toestaan (standaard Deny IP): In dit model is de standaardactie Deny IP en daarom moet het gewenste verkeer expliciet worden toegestaan met het gebruik van SGACL's. Dit wordt in het algemeen gebruikt wanneer de klant een redelijk inzicht heeft in het soort verkeersstromen binnen hun netwerk. Dit model vereist een gedetailleerde studie van het verkeer van het controlevliegtuig evenals het potentieel om AL verkeer te blokkeren, wanneer het wordt geactiveerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Dot1x/MAB-verificatie
- Cisco TrustSec (CTS)
- Security exchange Protocol (SXP)
- Web proxy
- Firewallconcepten
- DNA

Gebruikte componenten

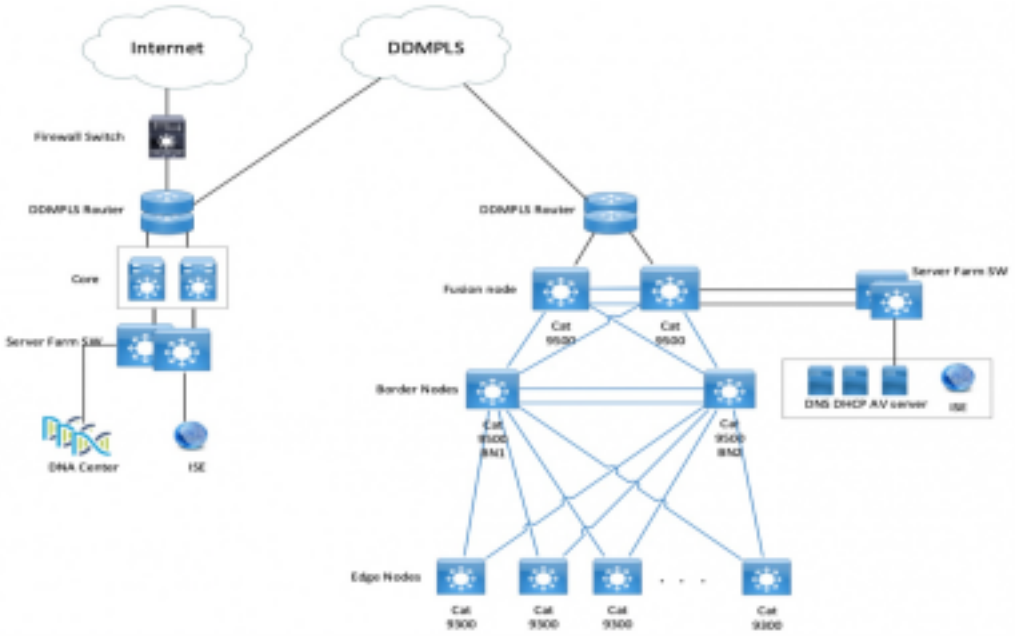
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Catalyst 9300 Edge en 9500 border-knooppunten (switches) met IOS 16.9.3
- DNA 1.3.0.5
- ISE 2.6-patch 3 (twee knooppunten - redundante implementaties)
- DNA en ISE zijn geïntegreerd
- Border en Edge-knooppunten worden bevoorraad door DNA
- SXP-tunnelbouw is ingesteld vanaf ISE (Luidspreker) naar beide grensknooppunten (Luistener)
- IP-adrespools worden toegevoegd aan host-instapsysteem

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.

Configureren

Netwerkdiagram



Configuratie

Dit zijn de stappen om het geoorloofde IP-model in te schakelen (standaard Deny IP):

1. Verandert switches SGT van Onbekend naar TrustSec-apparaten.
2. Uitschakelen van CTS Rol-gebaseerde handhaving.
3. IP-SGT Toewijzing op Rand- en Edge-switches met behulp van DNA-sjabloon.
4. Fallback SGACL met behulp van DNA-sjabloon.
5. Schakel de optie Sta-lijst in (standaard Deny IP) in de categorie Trustsec Matrix.
6. SGT voor endpoints/gebruikers maken
7. SGACL maken voor endpoints/gebruikers (voor productieverkeer)

Stap 1. Wijzig SGT van Onbekend naar TrustSec-apparaten.

Standaard is de onbekende Security Group Tag (SGT) ingesteld voor autorisatie van netwerkapparaten. Door het te wijzigen in TrustSec Apparaat SGT geeft meer zichtbaarheid en helpt u SGACL specifiek te maken voor Switch geïnitieerd verkeer.

Navigeren in op **Work Centers > TrustSec > Trustsec Policy > Network Devices Authorized** en veranderen het in Trustsec_Devices van Onbekend

Stap 2. Schakel CTS-Rol-gebaseerde rechtshandhaving uit.

- Zodra het model is toegestaan (standaard Deny), is al het verkeer geblokkeerd in de stof, inclusief underlay multicast en broadcast-verkeer zoals Intermediate System-to-Intermediate System (IS-IS), Bidirectional Forwarding Detection (BFD) en Secure Shell (SSH)-verkeer.

- Alle TienGig-poorten die zowel aan de wasrand als aan de rand zijn aangesloten, moeten hier

met de opdracht worden ingesteld. Als deze optie bestaat, is verkeer dat vanuit deze interface is geïnitieerd en dat naar deze interface komt, niet onderworpen aan handhaving.

```
Interface tengigabitethernet 1/0/1

no cts role-based enforcement
```

Opmerking: Dit kan worden gedaan met het gebruik van een gebiedsjabloon in DNA voor eenvoud. Anders moet elke schakelaar tijdens de voorziening handmatig worden uitgevoerd. Het onderstaande fragment toont hoe je het via een DNA-sjabloon moet doen.

```
interface range $uplink1

no cts role-based enforcement
```

Raadpleeg voor meer informatie over DNA-sjablonen deze URL voor het document.

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

Stap 3. IP-SGT Toewijzing op Rand- en Edge-switches met DNA-sjabloon.

Het idee is om IP-SGT-mapping op de switches beschikbaar te maken, zelfs als alle ISE-toetsen ingedrukt worden. Dit waarborgt dat Underlay boven is en dat de connectiviteit op de kritieke bronnen intact is

De eerste stap is om cruciale services te binden aan een SGT (ex - Basic_Network_Services/1000). Enkele van deze diensten zijn:

- Underlay/ISIS-subnet
- ISE/DNA
- Monitoringprogramma
- AP's Subnet in geval van OTT
- Terminalserver
- Kritische diensten - Ex: IP-telefoon

Voorbeeld:

```
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
```

Stap 4. Back-ups SGACL met DNA-sjabloon.

Een SGT-mapping is van geen gebruik totdat een relevante SGACL is gecreëerd met behulp van de SGT en daarom is onze volgende stap om een SGACL te maken die fungeert als een lokale Fallback voor het geval dat ISE-knooppunten omlaag gaan (wanneer ISE-services omlaag zijn, gaat de SXP-tunnel omlaag en worden SGACL's en IP SGT-mapping niet dynamisch gedownload).

Deze configuratie wordt naar alle Edge- en grensknooppunten geduwd.

Op back-up Rol gebaseerde ACL/contract:

```
ip access-list role-based FALLBACK

permit ip
```

TrustSec-apparaten om apparaten te vertrouwenSec:

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

Boven SGACL zorgen voor communicatie binnen fabricswitches en fungeren IP's

TrustSec-apparaten naar SGT 1000:

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

Boven SGACL zorgen voor communicatie van switches en access points naar ISE-, DNA-, WLC- en monitoringtools

SGT 1000 voor TrustSec-apparaten:

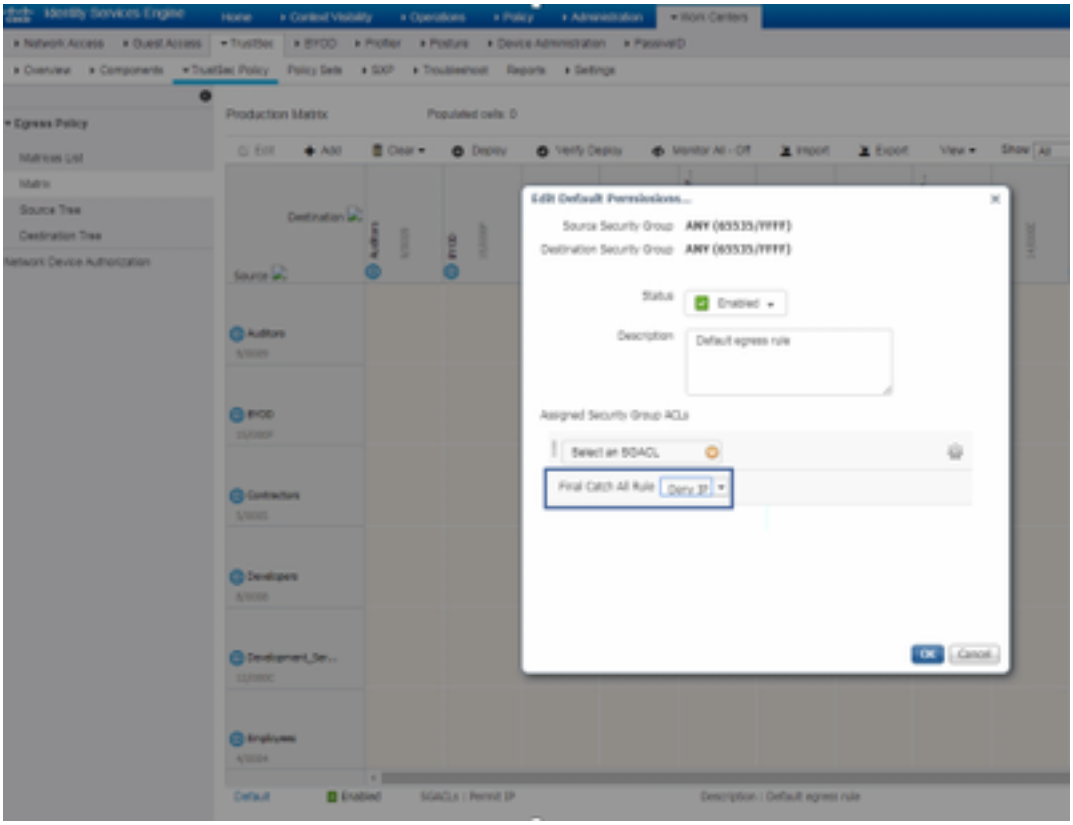
```
cts role-based permissions from 1000 to 2 FALLBACK
```

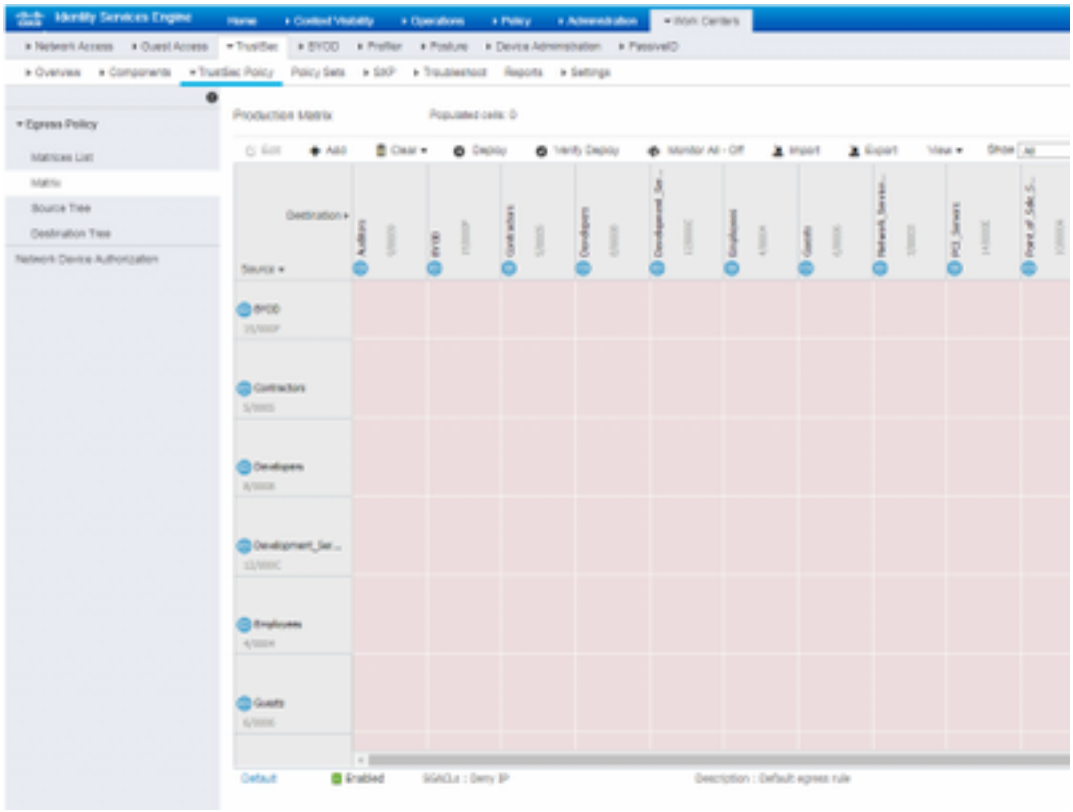
Boven SGACL zorgen voor communicatie van access points naar ISE, DNA, WLC en bewakingstools naar switches

Stap 5. Laat het model toestaan (standaard ontkenning) in TrustSec Matrix inschakelen.

De verplichting is om het grootste deel van het verkeer op het net te ontzeggen en in mindere mate toe te staan. Dan is er minder beleid nodig als je standaard ontkent met expliciete vergunningsregels.

Navigeer naar **werkcentra > Trustsec > TrustSec Policy > Matrix > Standaard** en verander deze naar **Deny All** in finale vangstregel.





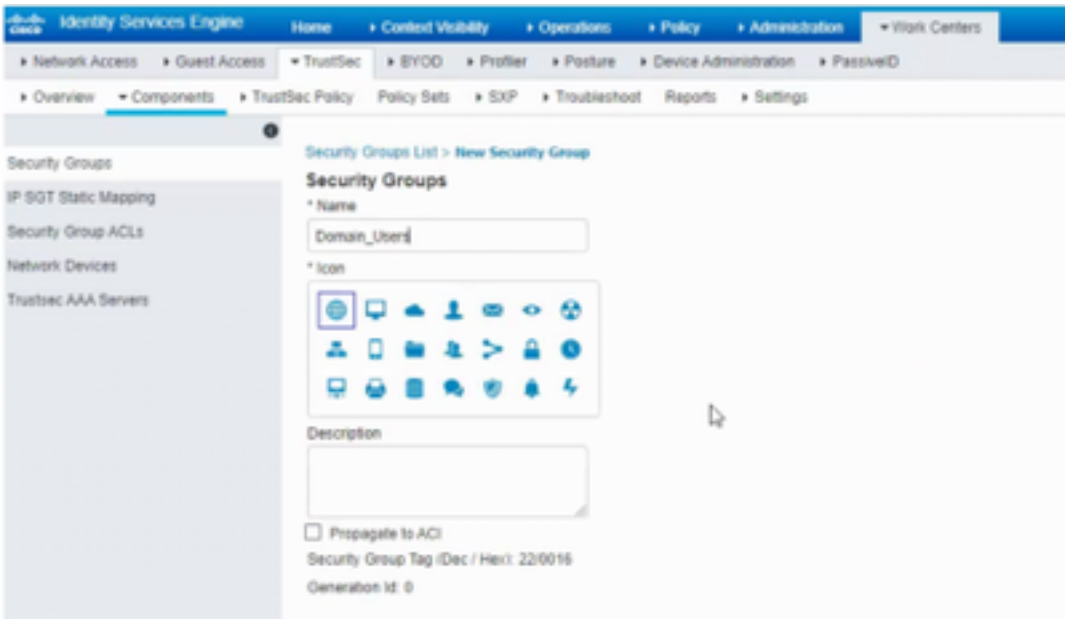
Opmerking: Dit beeld vertegenwoordigt (Alle Kolommen zijn standaard in Rood), standaard Deny is ingeschakeld en alleen selectief verkeer kan worden toegestaan na het maken van SGACL.

Stap 6. Maak SGT voor endpoints/gebruikers.

In SDA Environment, dient er enkel een nieuw SGT te worden gecreëerd vanuit de DNA GUI,

aangezien er talrijke gevallen zijn van corruptie in gegevensbestanden door de mismatch van de SGT-databank in ISE/DNA.

Om SGT te maken, logt u in bij **DNA > Policy > Group-Based Access Control > Scalable Groepen > Add Group**, wijst een pagina u naar **ISE Scalable Group** terug, klikt u op **Add,** voert u de SGT-naam in en slaat u deze op.



Dezelfde SGT weerspiegelt in DNA door PxGrid-integratie. Dit is dezelfde procedure voor alle toekomstige SGT-creaties.

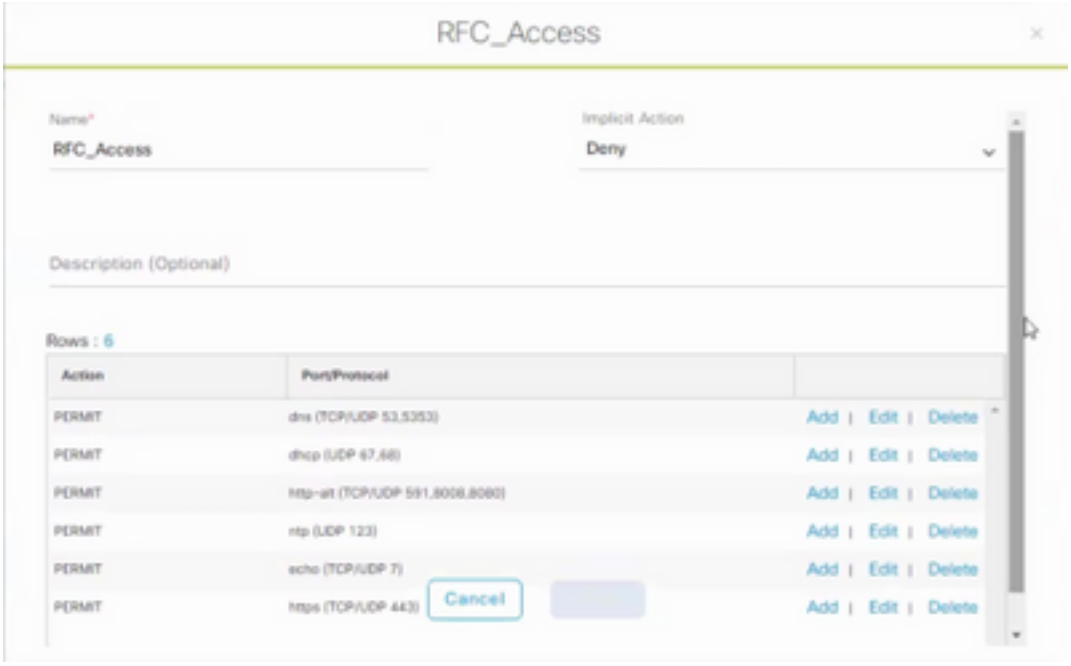
Stap 7. Maak SGACL voor endpoints/gebruikers (voor productieverkeer).

In SDA Environment, dient alleen een nieuwe SGT te worden gecreëerd vanuit de DNA GUI.

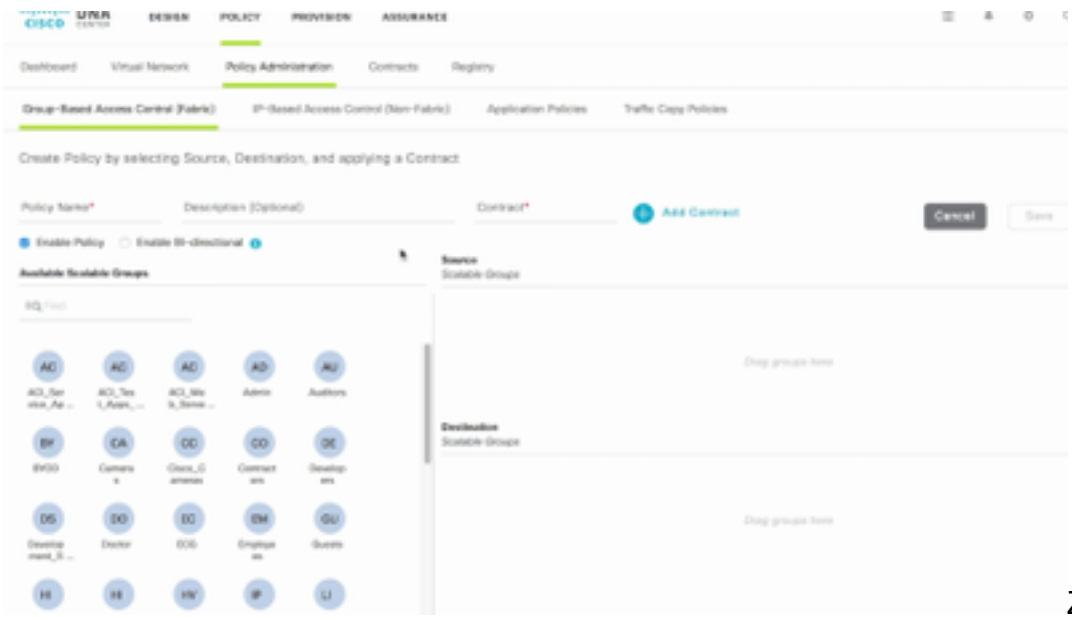
```
Policy Name: Domain_Users_Access

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)
```

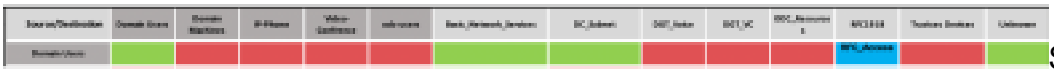
Als u een **contract** wilt maken, logt u in bij **DNA** en vervolgens klikt u op **Beleid > Contracten > Add Contracts > Add Files > Add added protocol** en vervolgens op **Save**.



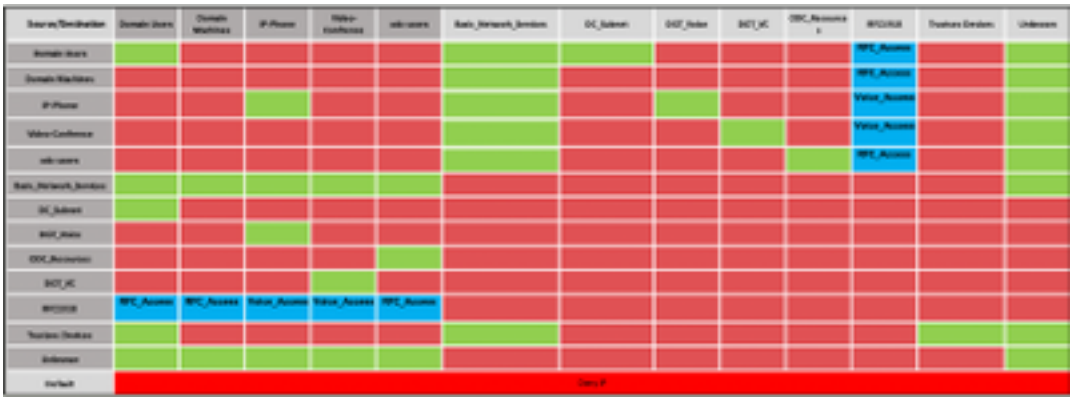
Om een **contract** te maken, logt u in bij de **DNA** en navigeer naar **beleid > Groepsgebaseerde toegangscontrole > Groepsgebaseerd toegangsbeleid > Toevoegen beleid > Beleid toevoegen (met de gegeven informatie)** nu op **Opslaan** en dan **implementeren.**

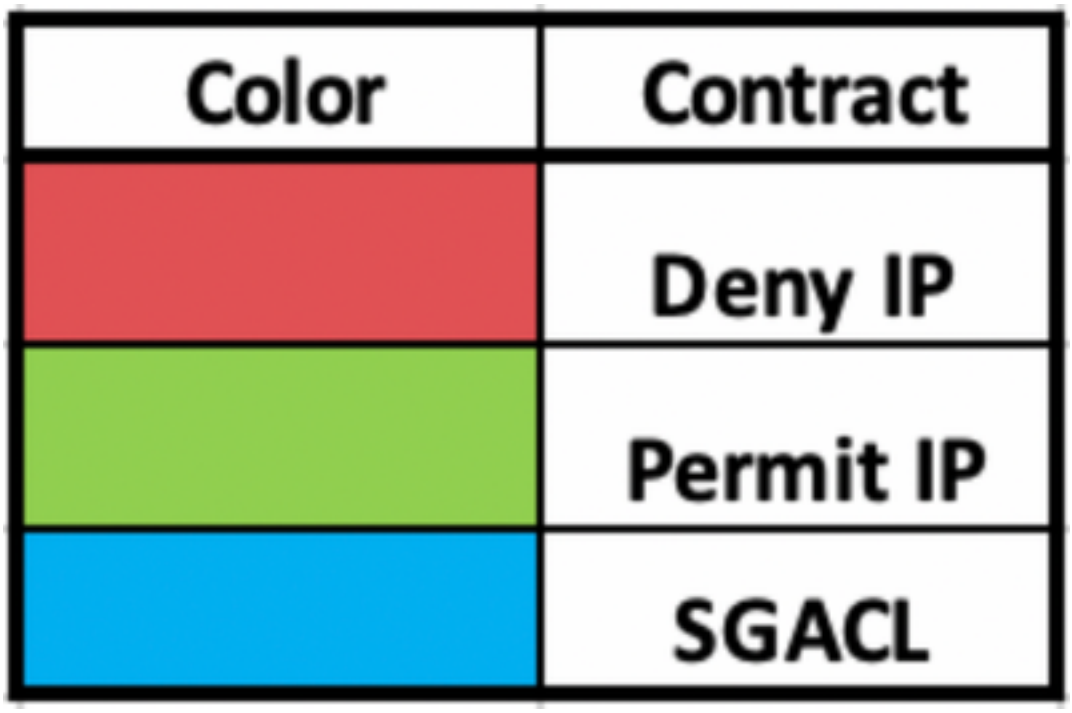


Zodra SGACL/contract uit DNA is geconfigureerd reflecteert het automatisch in ISE. hieronder is een voorbeeld van een matrx-weergave voor een sgt.



SGACL Matrix, zoals weergegeven in de afbeelding hieronder, is een voorbeeldweergave voor een staat-lijst (standaard Deny) model.





Verifiëren

Netwerkapparaat SGT

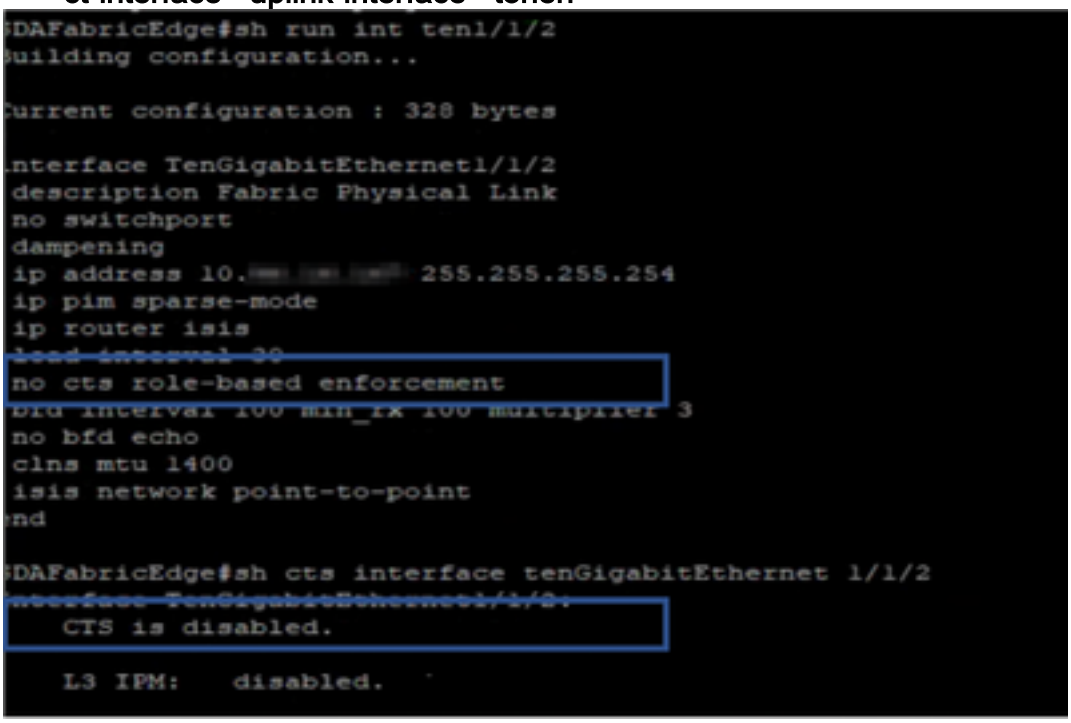
Om de door ISE ontvangen switches SGT te controleren, voert u deze opdracht uit: **toon cts omgevingsdata**

```
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
```

Handhaving op uplinks poorten

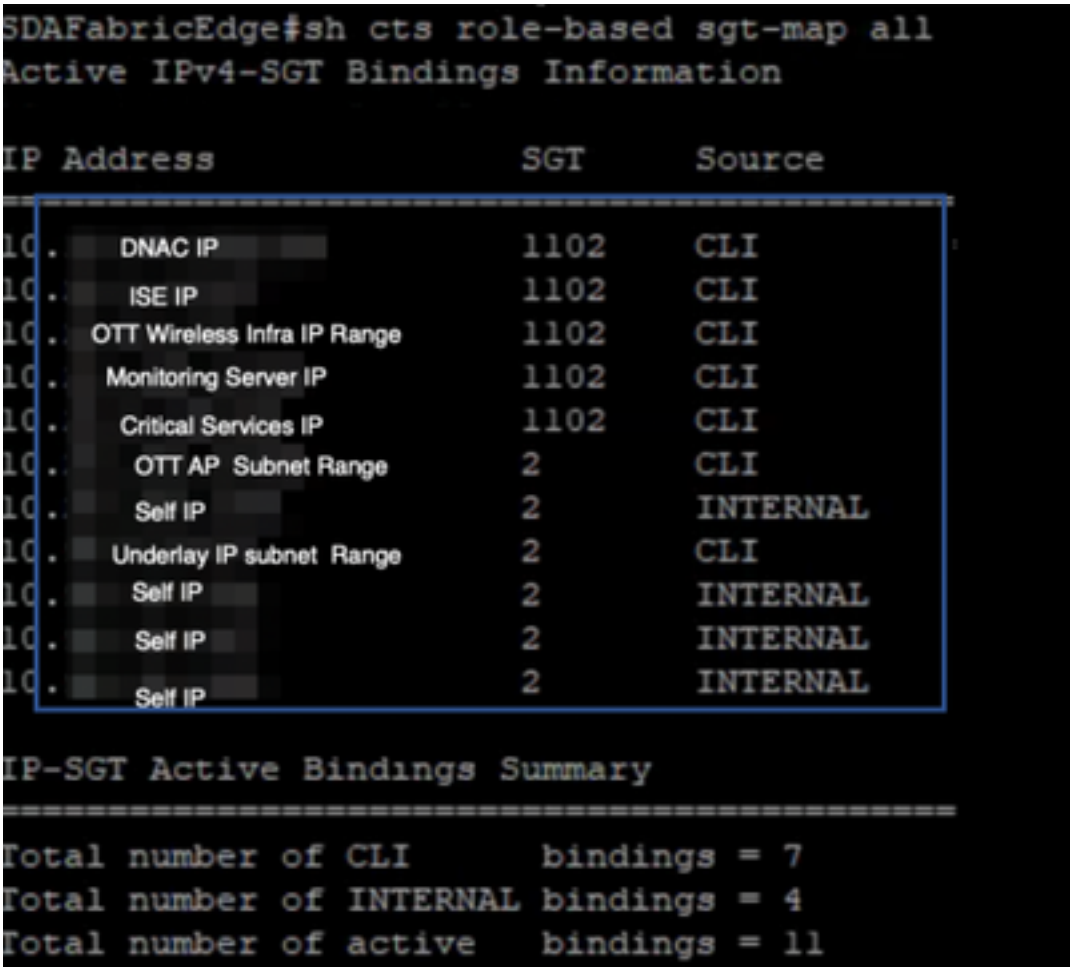
Om handhaving op de uplink-interface te controleren, voert u deze opdrachten uit:

- loopinterface <uplink> tonen
- ct-interface <uplink-interface> tonen



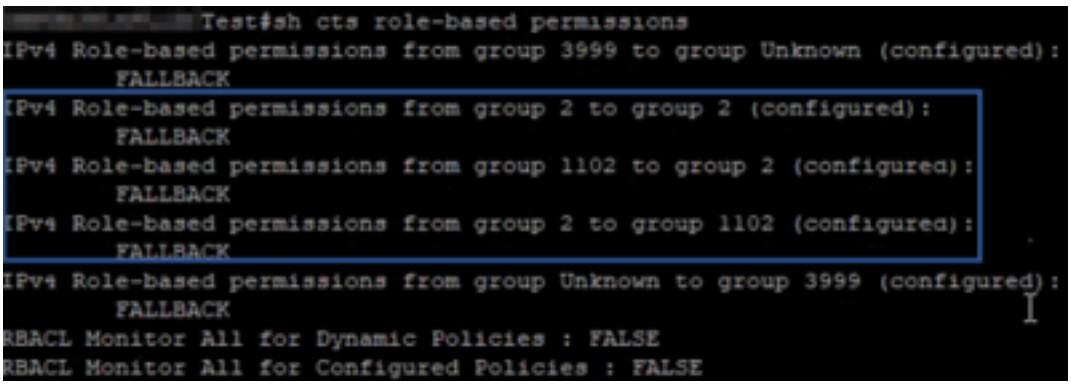
Toewijzing van lokale IP-SGT

Om lokaal geconfigureerde IP-SGT-mappings te controleren, voert u deze opdracht uit: **sh cts rollbased sgt-map all**



Lokale FALLBACK-SGACL

Om FALLBACK SGACL te controleren, voert u deze opdracht uit: **sh cts role-Based Toestemming**



Opmerking: SGACL die door ISE wordt geduwd heeft een prioriteit boven lokale SGACL.

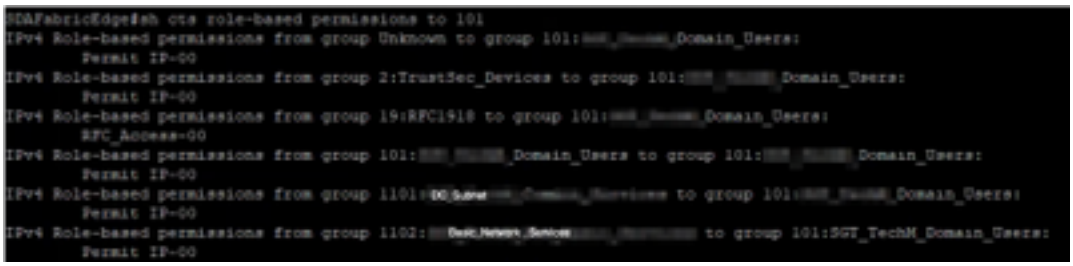
Sta-lijst (standaard naam) in werking op fabricswitches

Om het model van de Sta-lijst (standaard ontkenner) te controleren, voert u deze opdracht uit: **sh op rol gebaseerde toestemming**

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

SGACL voor endpoint verbonden met fabric

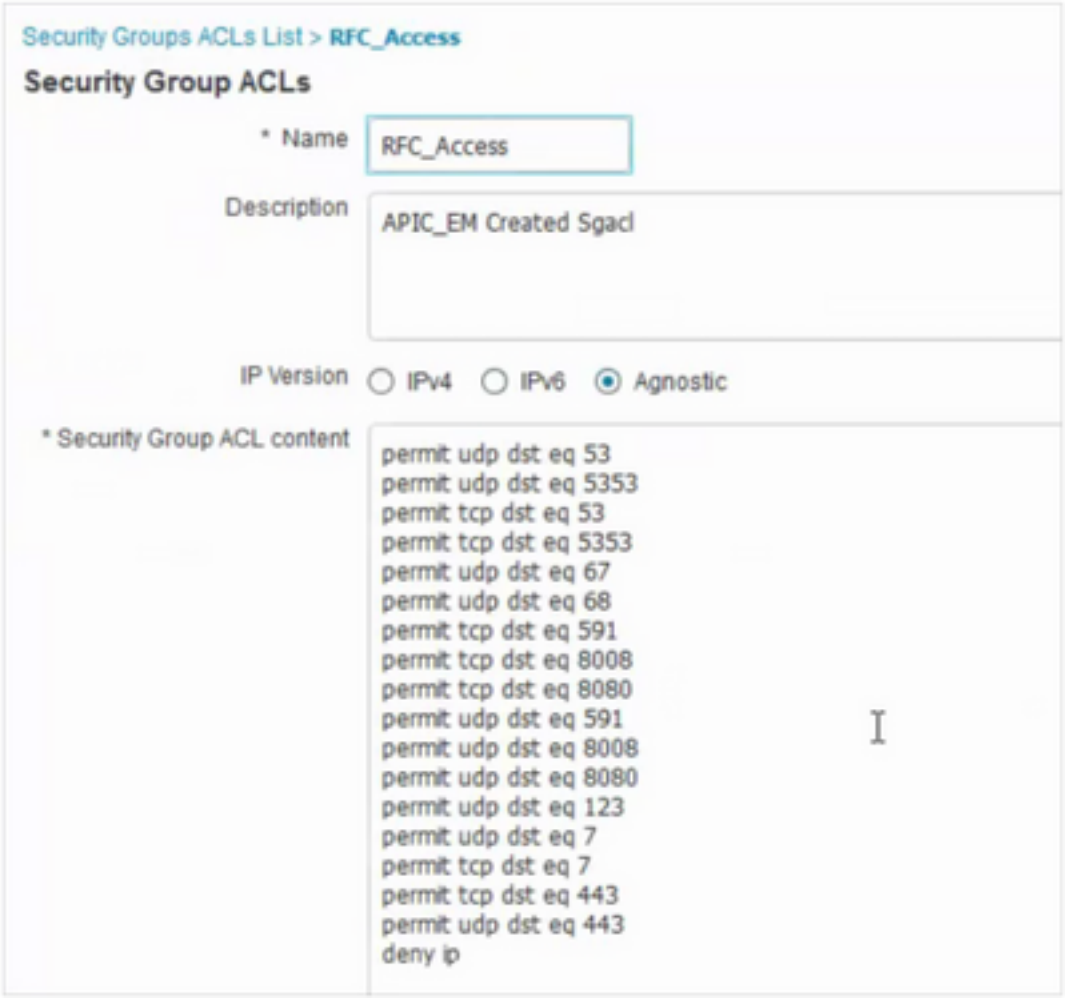
Om gedownload SGACL van ISE te verifiëren, voer deze opdracht uit: **sh op rol gebaseerde toestemming**



Controleer het contract dat door de DNA-computer is gemaakt

Om gedownload SGACL van ISE te verifiëren, voer deze opdracht uit: **toon access-list <ACL/contract Name>**

```
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
```



Underlay SGACL Counter op fabricswitches

Om SGACL-beleidshits te controleren, voert u deze opdracht uit: **Toon cts op rol gebaseerde teller**

```
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
```

Problemen oplossen

Vraag 1. Indien beide ISE-knooppunten zijn neergezet.

Heeft zowel de ISE-knooppunten als de ISE-knooppunten ingedrukt, dan wordt IP-naar-SGT-omzetting die door ISE is ontvangen, verwijderd en worden alle DGT's getagd als onbekend, en alle gebruikerssessies die na 5-6 minuten bestaan gestopt.

> Opmerking: Deze kwestie is alleen van toepassing wanneer sgt (xxxx) -> onbekende (0) SGACL-toegang is beperkt tot DHCP, DNS en web proxy poort.

Oplossing:

1. Er werd een SGT gecreëerd (bijvoorbeeld. RFC1918).
2. Druk op RFC privé IP-bereik aan beide randen.
3. Beperk de toegang tot DHCP-, DNS- en webproxy van sgt (xxxx) —> RFC1918
4. aanmaken/wijzigen sgom sgt (xxxx) —> onbekend met IP-contract toestaan.

Als beide knooppunten naar beneden gaan, SGACL sgt —>onbekende hits, en de sessie die er bestaat, is intact.

Vraag 2. Eenvoudige IP-telefoon of geen spraak.

De uitbreiding tot IP conversie vond plaats op SIP en de eigenlijke spraakcommunicatie gebeurt via RTP tussen IP en IP. CUCM en spraakgateway werden toegevoegd aan **DGT_Voice**.

Oplossing:

1. Dezelfde locatie of Oost-West spraakcommunicatie kan worden ingeschakeld door verkeer vanaf IP_Phone —> IP_Phone toe te staan.
2. De rest van de locatie kan worden toegestaan door het RTP-protocolbereik voor toegangsrechten in DGT RFC1918. Hetzelfde bereik kan worden toegestaan voor IP_telefoon —> Onbekend.

Kwestie 3. Kritisch VLAN-endpoint heeft geen netwerktoegang.

DNA-bepalingen schakelen voor Data en volgens de configuratie alle nieuwe verbindingen tijdens ISE-uitval naar Critisch VLAN en SGT 3999 over. De standaardontkenning in het beleid van de trustsec beperkt de nieuwe verbinding tot toegang tot om het even welke netwerkmiddelen.

Oplossing:

Druk op SGACL voor kritieke SGT op alle Edge- en grensswitches met behulp van DNA-sjabloon

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

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

Deze opdrachten worden toegevoegd aan het configuratiescherm.

> Opmerking: Alle opdrachten kunnen in één sjabloon worden gecombineerd en kunnen tijdens de provisioning worden geduwd.

Kwestie 4. Packet Drop-in Kritisch VLAN.

Zodra de machine in cruciaal VLAN is door ISE-knooppunten beneden, is er een pakketdaling in elke 3-4 minuten (Max. 10 druppels waargenomen) voor alle eindpunten in kritiek VLAN.

Opmerkingen: Verificatietellers nemen toe als servers DOOD zijn. Clients proberen te certificeren met PSN wanneer servers zijn gemarkeerd met DEAD.

Oplossing/werkruimte:

Idealiter zou er geen auth request uit een eindpunt moeten zijn als ISE PSN knooppunten omlaag zijn.

Duw deze opdracht onder de Straalserver met DNA:

Gebruikersnaam voor automatische test-test

Met deze opdracht in de schakelaar, stuurt het periodieke test authenticatieberichten naar de RADIUS server. Het zoekt een RADIUS-respons van de server. Een succesbericht is niet nodig - een mislukte authenticatie volstaat omdat het aantoont dat de server nog leeft.

Aanvullende informatie

DNA-eindmodel:

```
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
```

> Opmerking: Alle uplink-interfaces in randknooppunten worden geconfigureerd zonder handhaving en de veronderstelling is dat uplink alleen aan grensknooppunten verbindt. Op grensknooppunten moeten uplink interfaces naar randknooppunten worden geconfigureren zonder afdwinging en dat moet handmatig gebeuren.