Modelo de lista de permitidos Cisco ISE TrustSec (denegación de IP predeterminada) con SDA

Contenido

Introducción

Este documento describe cómo habilitar el modelo allow-list (Default Deny IP) de TrustSec en el acceso definido por software (SDA). Este documento incluye varias tecnologías y componentes que incluyen Identity Services Engine (ISE), Digital Network Architecture Center (DNAC) y Switches (Borde y Borde).

Hay dos modelos Trustsec disponibles:

- Modelo de lista de denegación (IP de permiso predeterminado): En este modelo, la acción predeterminada es Permit IP (Permitir IP) y cualquier restricción debe configurarse explícitamente con el uso de Listas de Acceso de Grupos de Seguridad (SGACL). Esto se utiliza generalmente cuando no se conoce completamente el flujo de tráfico dentro de su red. Este modelo es bastante fácil de implementar.
- Modelo de lista de permitidos (Default Deny IP): En este modelo, la acción predeterminada es Deny IP y, por lo tanto, el tráfico requerido debe permitirse explícitamente con el uso de SGACL. Esto se utiliza generalmente cuando el cliente conoce bien el tipo de flujos de tráfico dentro de su red. Este modelo requiere un estudio detallado del tráfico del plano de control, además de tener el potencial de bloquear TODO el tráfico, en el momento en que está habilitado.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Autenticación Dot1x/MAB
- Cisco TrustSec (CTS)
- Protocolo de intercambio de seguridad (SXP)
- Proxy web
- Conceptos de firewall
- DNAC

Componentes Utilizados

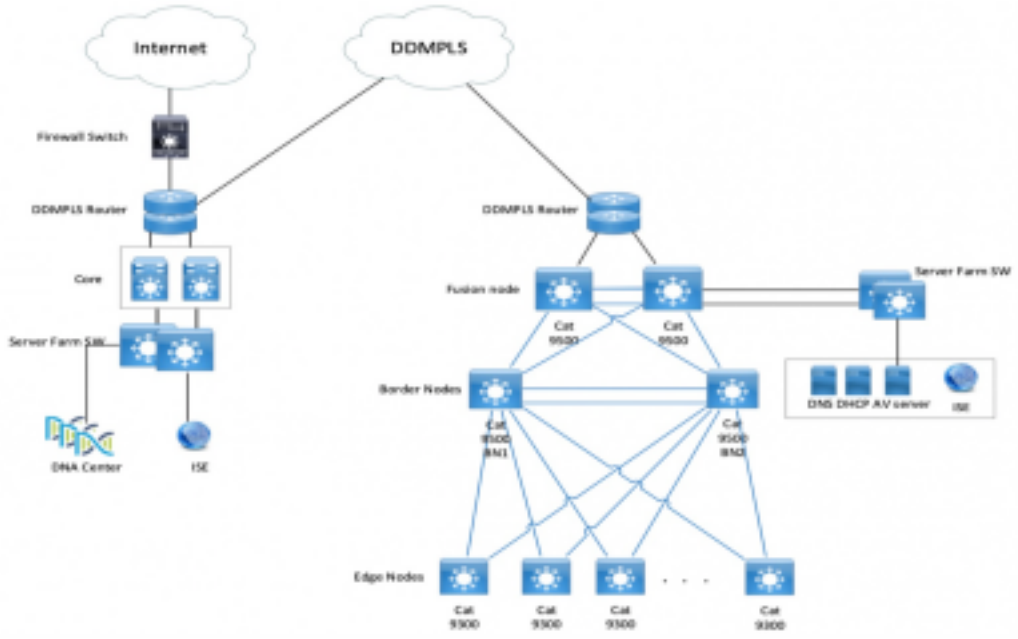
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Nodos de borde 9300 y 9500 (switches) con IOS 16.9.3
- DNAC 1.3.0.5
- ISE 2.6 parche 3 (dos nodos: implementación redundante)
- DNAC e ISE integrados
- El DNAC aprovisiona los nodos de borde y borde
- El túnel SXP se establece desde ISE (altavoz) a ambos nodos de borde (receptor)
- Los conjuntos de direcciones IP se agregan a la incorporación del host

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

Diagrama de la red



Configuración

Estos son los pasos para habilitar el modelo Allow-List (Default Deny IP):

1. Cambie los switches SGT de dispositivos desconocidos a dispositivos TrustSec.
2. Desactive la aplicación basada en roles de CTS.
3. Asignación de IP-SGT en switches de borde y borde mediante plantilla DNAC.
4. SGACL de reserva mediante plantilla DNAC.
5. Habilite Allow-List (Default Deny IP) en la matriz de trustsec.
6. Crear SGT para terminales/usuarios.
7. Cree SGACL para terminales/usuarios (para tráfico de superposición de producción).

Paso 1. Cambie los switches SGT de dispositivos desconocidos a dispositivos TrustSec.

De forma predeterminada, la Security Group Tag (SGT) desconocida se configura para la autorización de dispositivos de red. Cambiar a SGT de dispositivo TrustSec proporciona más visibilidad y ayuda a crear SGACL específica para el tráfico iniciado por el switch.

Vaya a **Centros de trabajo > TrustSec > Política Trustsec > Autorización de dispositivo de red** y cámbielo a Trustsec_Devices desde Desconocido

Paso 2. Desactive la aplicación basada en roles de CTS.

- Una vez que se ha implementado el modelo Allow-List (Default Deny), todo el tráfico se bloquea en el fabric, incluido el tráfico de multidifusión y difusión subyacente, como sistema intermedio a sistema intermedio (IS-IS), detección de reenvío bidireccional (BFD), Secure Shell (SSH).

- Todos los puertos TenGig que se conectan al borde del fabric, así como al borde, deben configurarse con el comando aquí. Con esto en su lugar, el tráfico iniciado desde esta interfaz y que llega a esta interfaz no están sujetos a aplicación.

```
Interface tengigabitethernet 1/0/1

no cts role-based enforcement
```

> **Nota:** Esto se puede hacer con el uso de una plantilla de rango en DNAC para simplificar. De lo contrario, para cada switch, es necesario hacerlo manualmente durante el aprovisionamiento. El siguiente fragmento de código muestra cómo hacerlo a través de una plantilla DNAC.

```
interface range $uplink1

no cts role-based enforcement
```

Para obtener más información sobre las plantillas DNAC, *consulte* esta URL para el documento.

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

Paso 3. Asignación de IP-SGT en switches de borde y borde con plantilla DNAC.

La idea es que la asignación IP-SGT local esté disponible en los switches incluso si todo ISE deja de funcionar. Esto garantiza que Underlay esté activo y que la conectividad con los recursos críticos esté intacta

El primer paso es Enlazar servicios críticos a una SGT (ex - Basic_Network_Services/1000). Algunos de estos servicios incluyen:

- Subred subyacente/ISIS
- ISE/ DNAC
- Herramienta de supervisión
- Subred de AP en caso de OTT
- Terminal Server
- Servicios críticos: por ejemplo: Teléfono IP

Ejemplo:

```
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
```

Paso 4. SGACL de reserva con plantilla DNAC.

Una asignación SGT no es útil hasta que se crea una SGACL relevante usando la SGT y, por lo tanto, nuestro siguiente paso sería crear una SGACL que actúe como reserva local en caso de que los nodos ISE se desactiven (cuando los servicios ISE están inactivos, el túnel SXP se desactiva y, por lo tanto, las SGACL y la asignación IP SGT no se descargan dinámicamente).

Esta configuración se envía a todos los nodos Edge y de borde.

Contrato/ACL basada en roles de reserva:

```
ip access-list role-based FALLBACK

permit ip
```

Dispositivos TrustSec para dispositivos TrustSec:

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

Sobre SGACL Garantizar la comunicación dentro de los switches de fabric y las IP subyacentes

Dispositivos TrustSec a SGT 1000:

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

Sobre SGACL Garantizar la comunicación de los switches y puntos de acceso a ISE, DNAC, WLC y herramientas de monitoreo

SGT 1000 a dispositivos TrustSec:

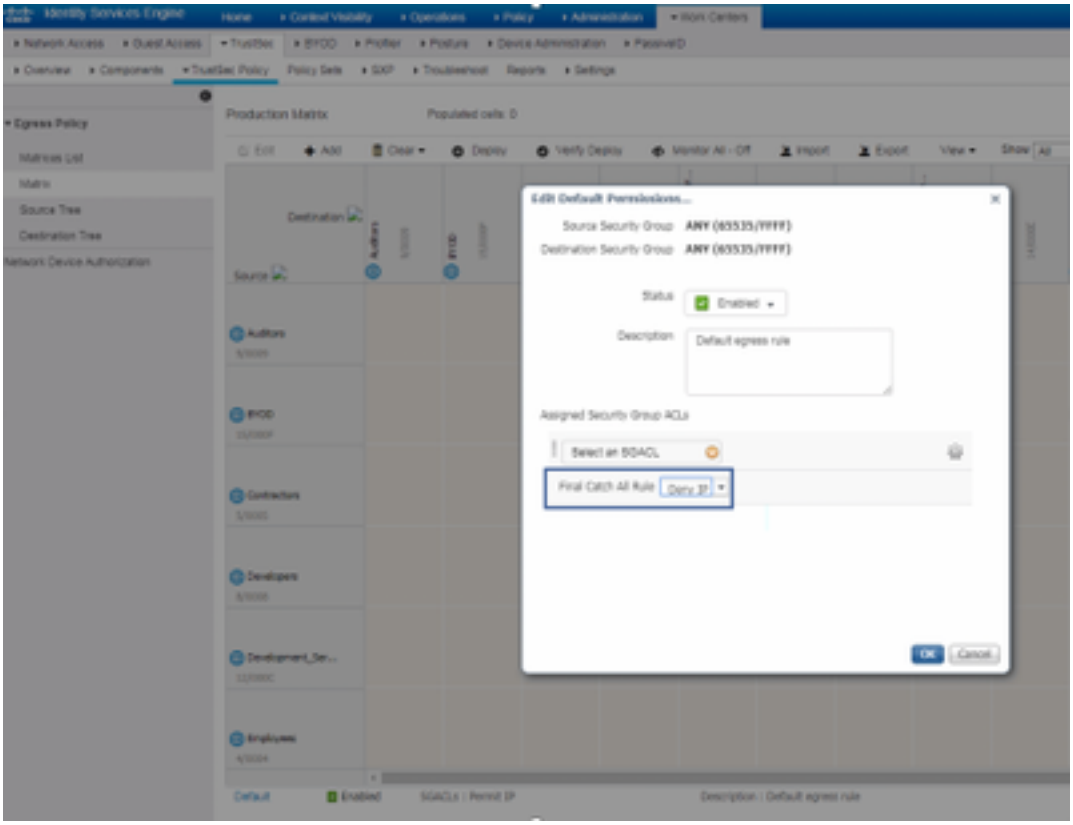
```
cts role-based permissions from 1000 to 2 FALLBACK
```

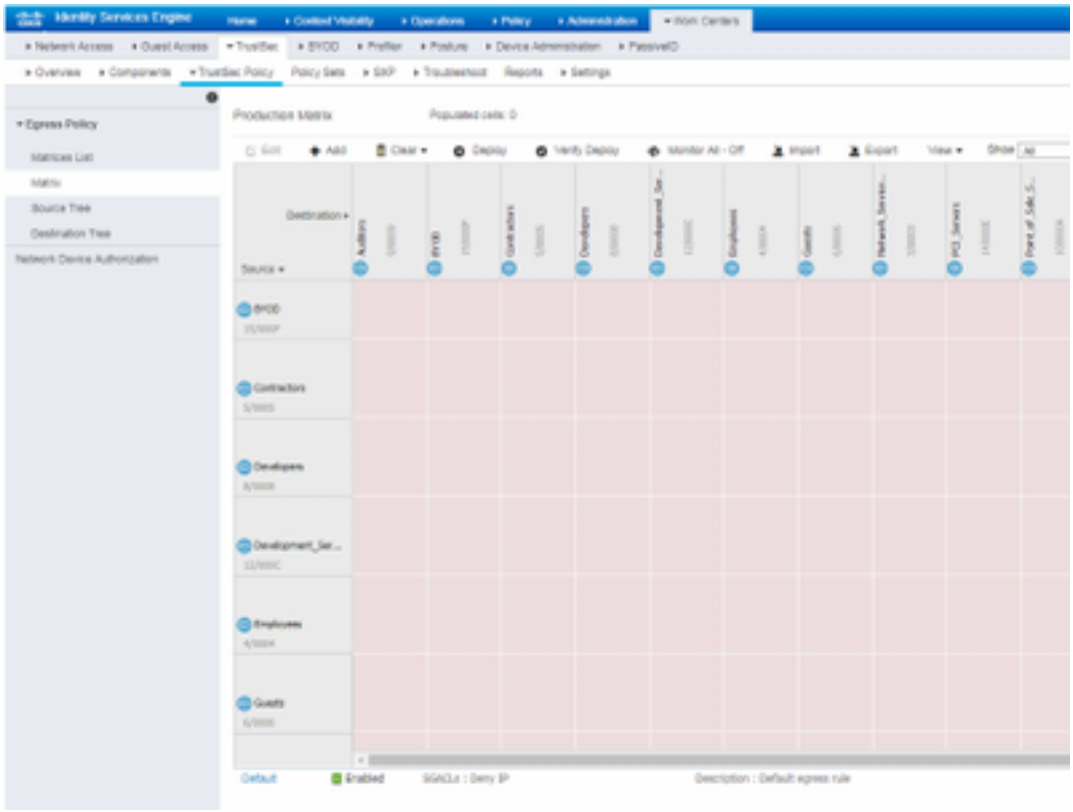
Por encima de SGACL Garantizar la comunicación de los puntos de acceso a ISE, DNAC, WLC y las herramientas de supervisión a los switches

Paso 5. Habilitar el modelo de lista de permitidos (Denegación predeterminada) en la matriz TrustSec.

El requisito es denegar la mayor parte del tráfico en la red y permitir en menor medida. A continuación, se necesitan menos políticas si utiliza la negación predeterminada con reglas de permiso explícitas.

Navegue hasta **Centros de Trabajo > Trustsec > Política TrustSec > Matriz > Predeterminado** y cámbielo a **Denegar todo** en la regla de captura final.





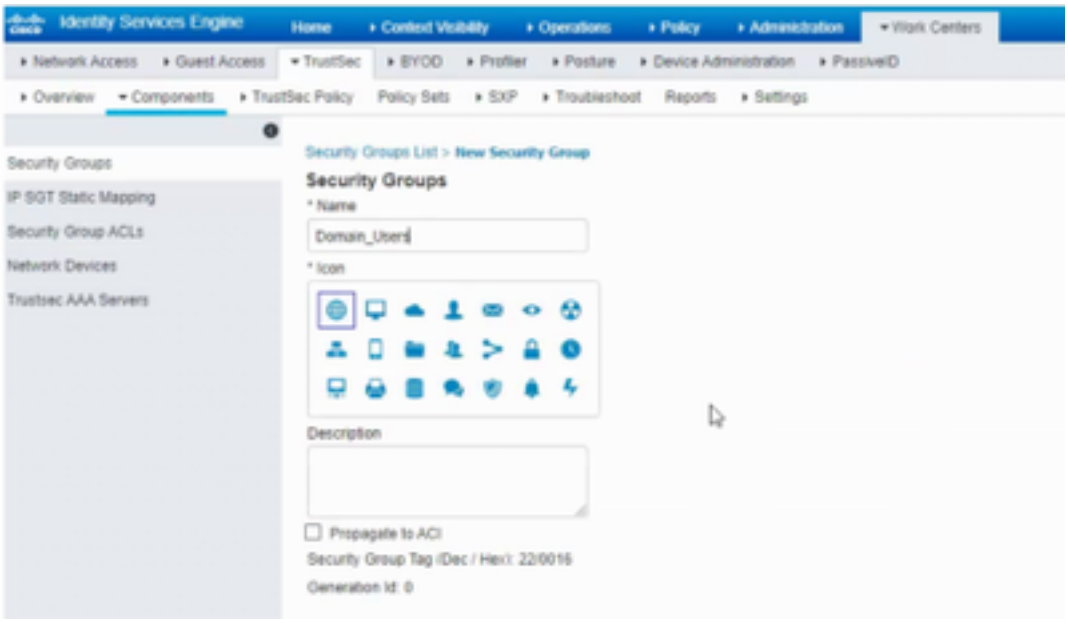
Nota: Esta imagen representa (todas las columnas están en rojo de forma predeterminada), se ha activado Denegar predeterminado y sólo se puede permitir el tráfico selectivo después de la creación de SGACL.

Paso 6. Crear SGT para terminales/usuarios.

En el entorno de SDA, la nueva SGT sólo se debe crear desde la GUI de DNAC, ya que hay

numerosos casos de corrupción en la base de datos debido a la discordancia de la base de datos de SGT en ISE/DNAC.

Para crear SGT, inicie sesión en **DNAC > Policy > Group-Based Access Control > Scalable Groups > Add Groups**, una página Redirige a **ISE Scalable Group**, haga clic en **Add,** introduzca el nombre SGT y guárdelo.



La misma SGT se refleja en DNAC a través de la integración PxGrid. Este es el mismo procedimiento para toda creación futura de SGT.

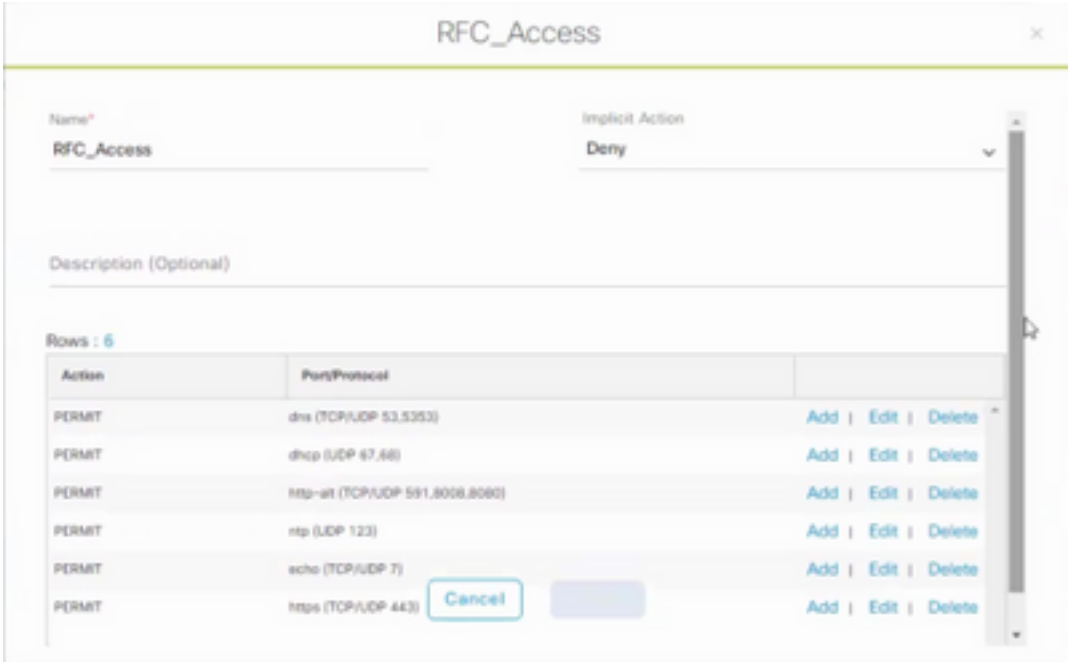
Paso 7. Cree SGACL para terminales/usuarios (para tráfico de superposición de producción).

En el entorno SDA, la nueva SGT sólo se debe crear a partir de la GUI de DNAC.

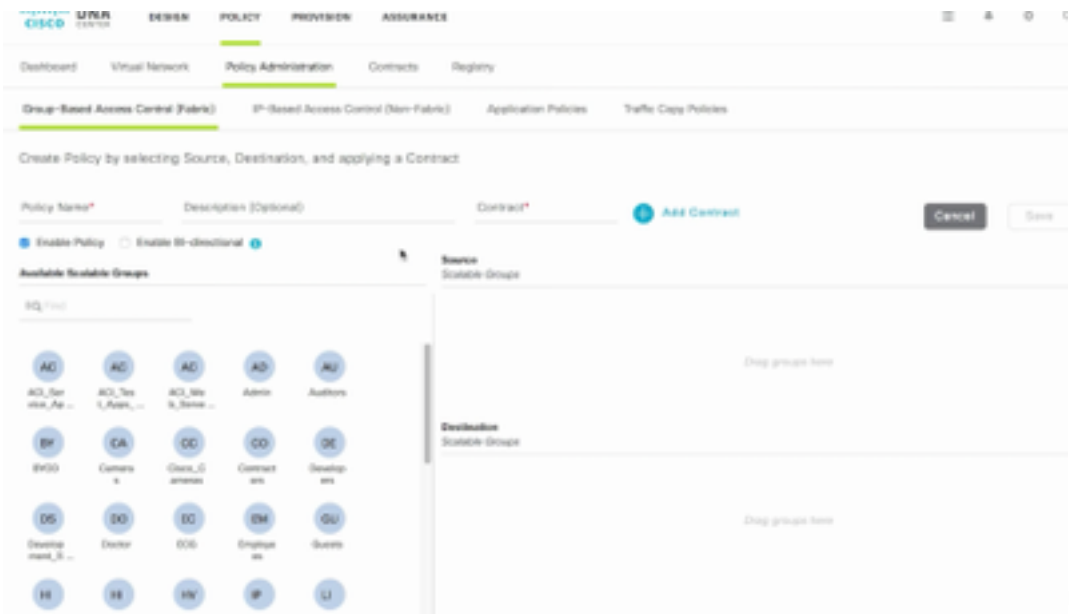
```
Policy Name: Domain_Users_Access

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)
```

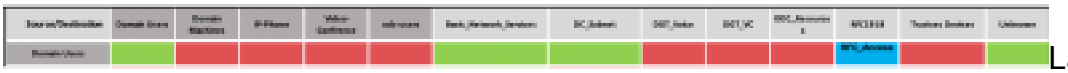
Para crear un **Contrato**, inicie sesión en **DNAC** y navegue hasta **Política > Contratos > Agregar Contratos > Agregar protocolo necesario** y luego haga clic en **Guardar**.



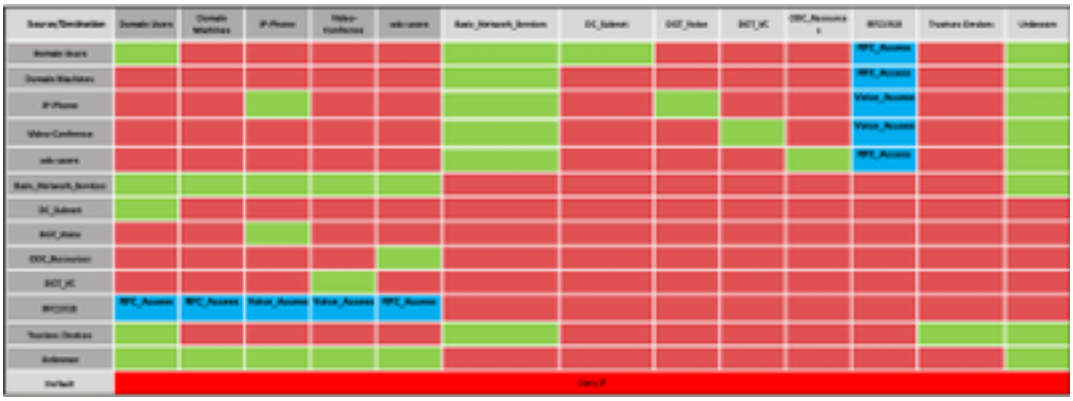
Para crear un contrato, inicie sesión en **DNAC** y navegue hasta **Policy > Group-Based Access Control > Group-Based-Access-Policies > Add Policies > Create policy (con la información dada)** ahora haga clic en Save y luego en Deploy.

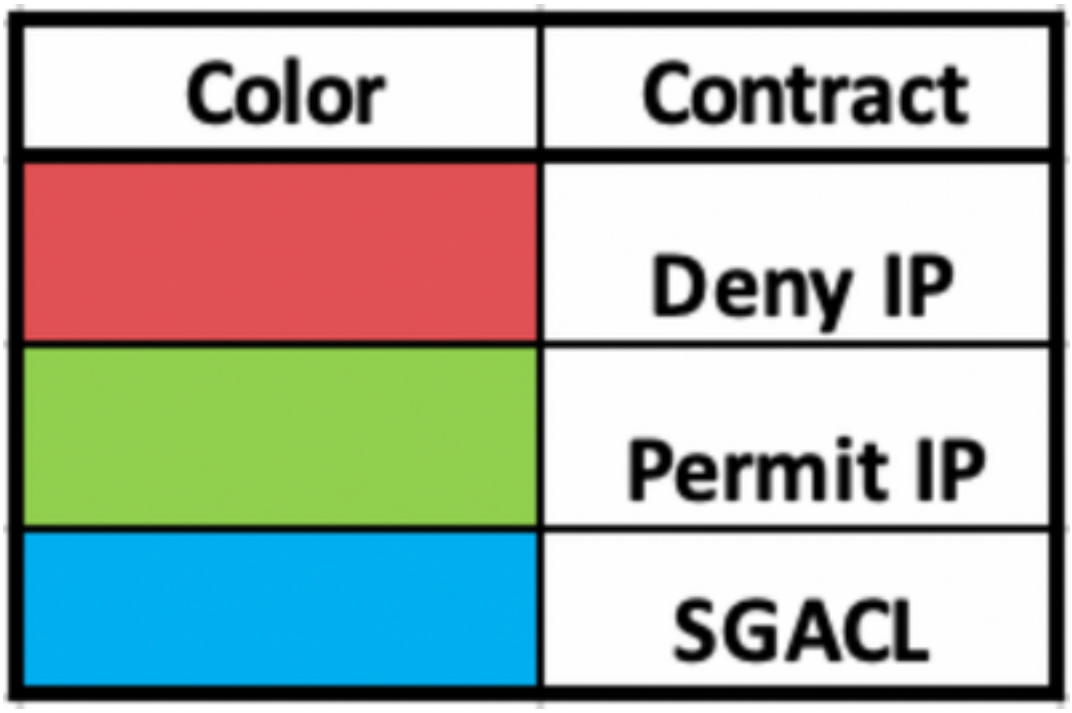


Una vez que SGACL/Contract se configura desde DNAC, se refleja automáticamente en ISE. a continuación se muestra un ejemplo de vista de matriz de una dirección para un sgt.



La matriz SGACL, como se muestra en la imagen siguiente, es una vista de ejemplo para el modelo Allow-list (Default Deny).





Verificación

SGT de dispositivos de red

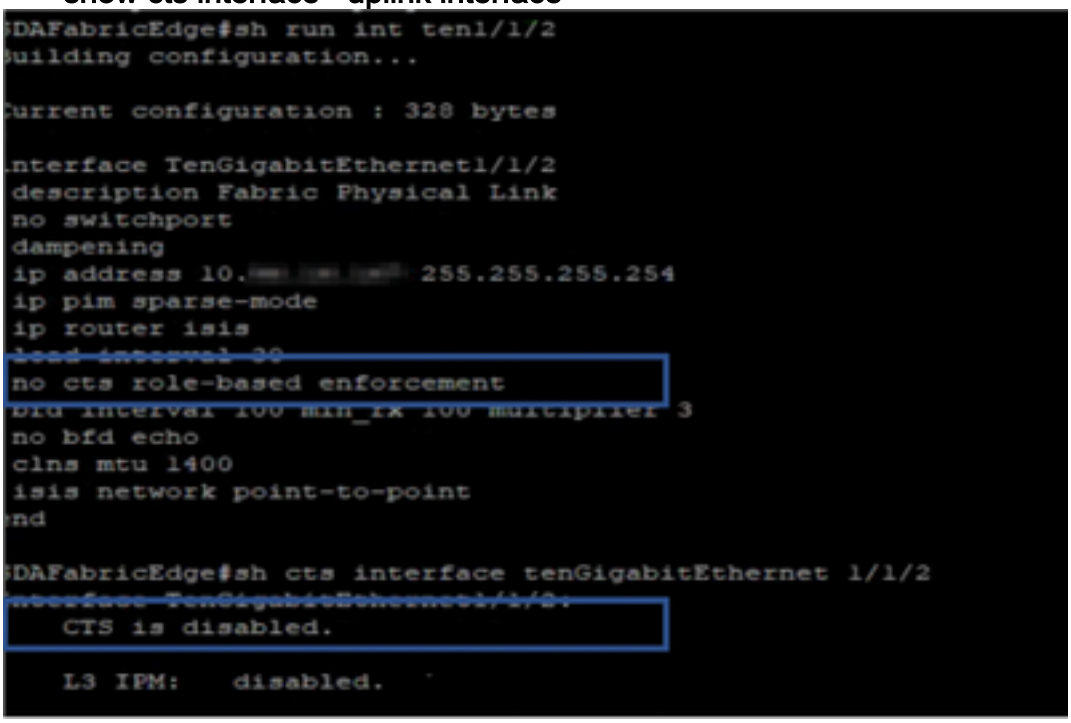
Para verificar los switches SGT recibidos por ISE, ejecute este comando: **show cts environment-data**

```
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
```

Aplicación en puertos de enlace ascendente

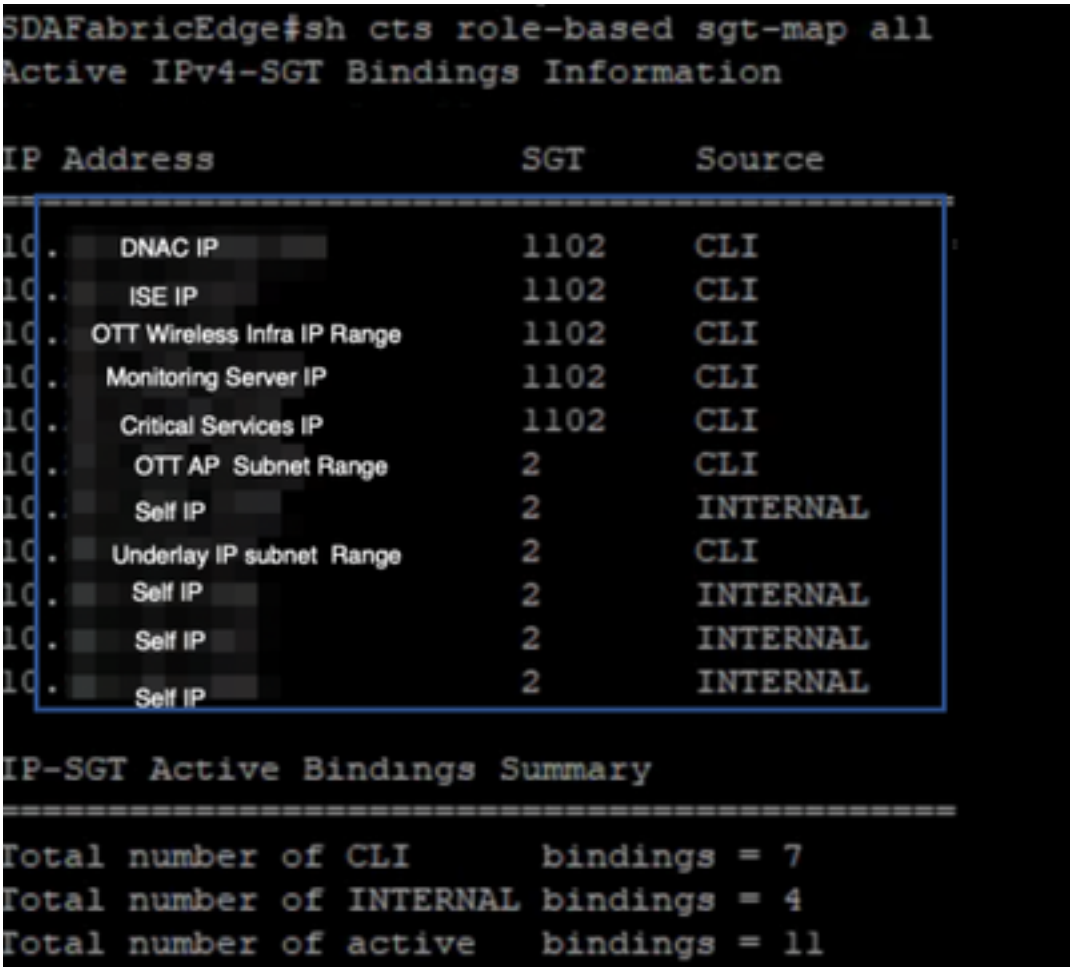
Para verificar la aplicación en la interfaz de link ascendente, ejecute estos comandos:

- **show run interface <uplink>**
- **show cts interface <uplink interface>**



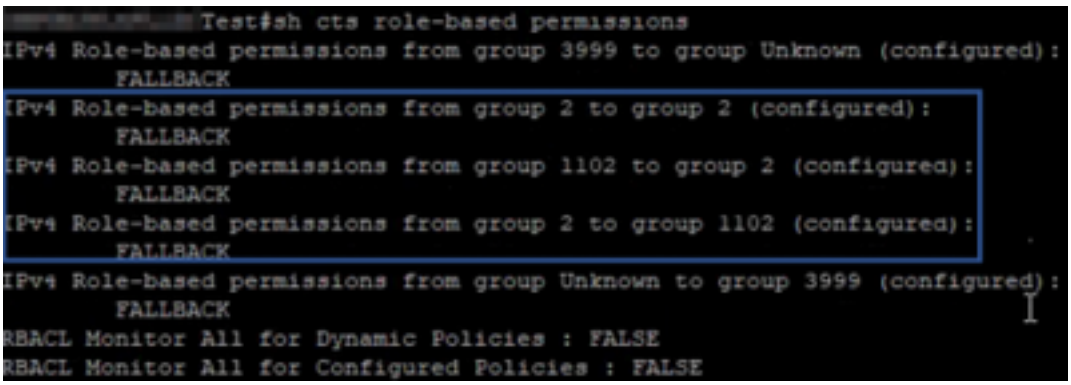
Asignación IP-SGT local

Para verificar mapeos IP-SGT configurados localmente, ejecute este comando: **sh cts role-based sgt-map all**



SGACL de FALLBACK local

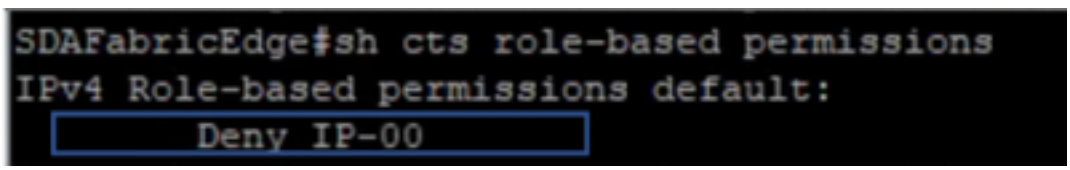
Para verificar FALLBACK SGACL, ejecute este comando: **sh cts role-based permit**



Nota: La SGACL impulsada por ISE tiene prioridad sobre la SGACL local.

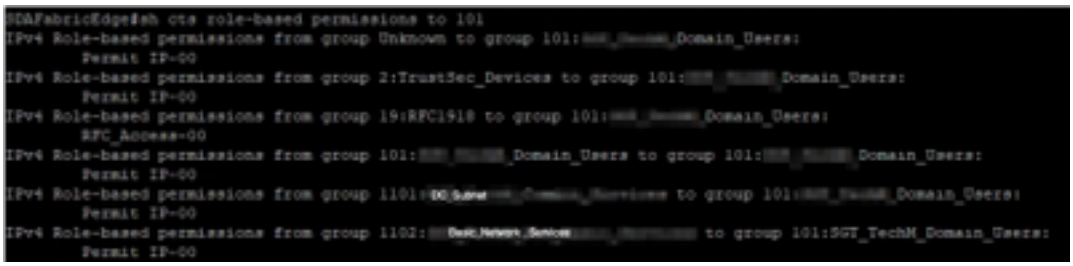
Habilitación Allow-List (Default Deny) en switches de fabric

Para verificar el modelo Allow-list (Default Deny), ejecute este comando: **sh cts role-based permit**



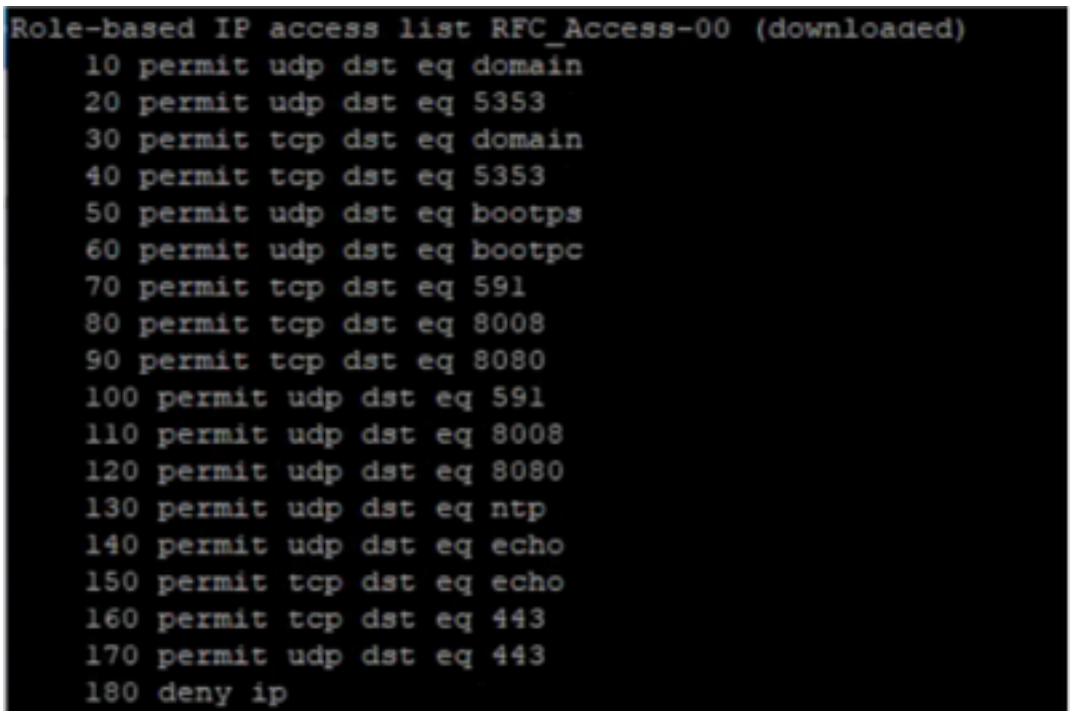
SGACL para terminales conectados al fabric

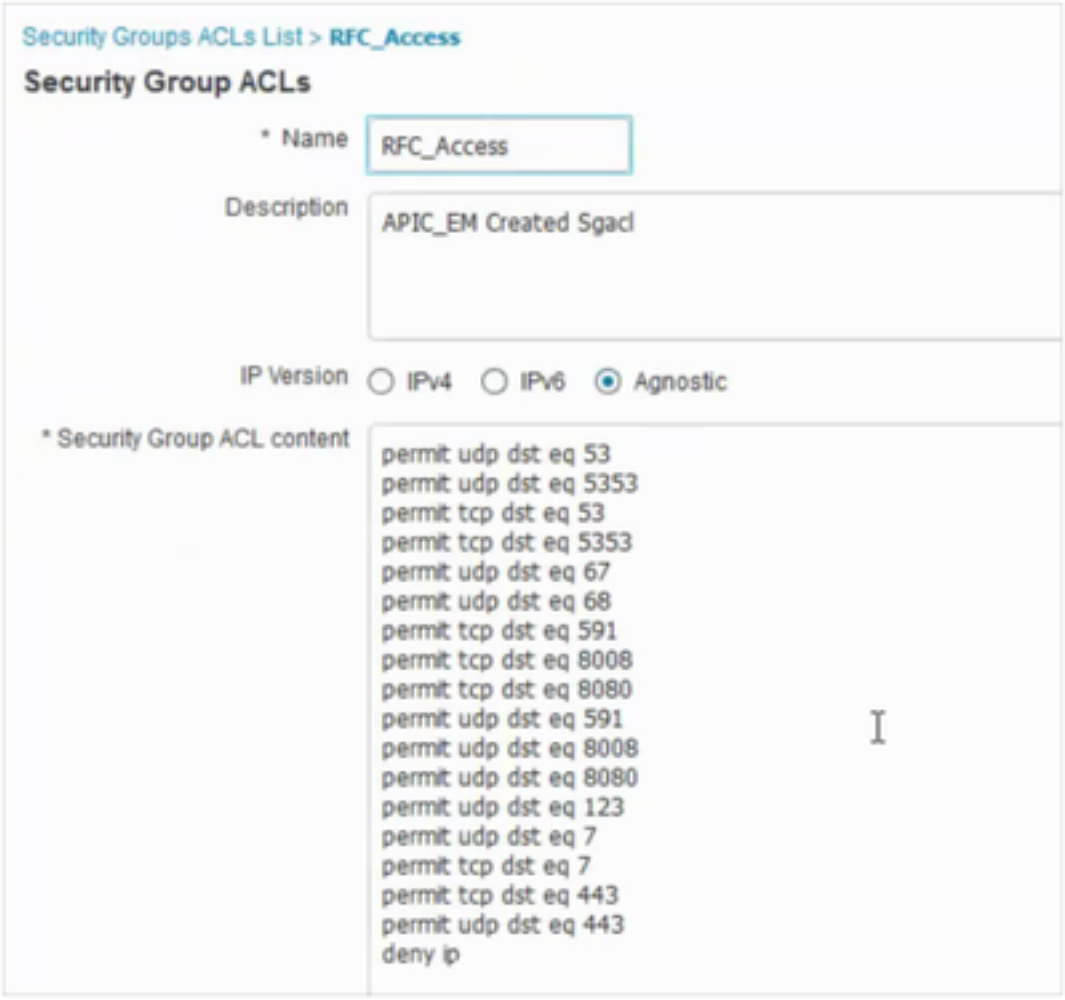
Para verificar la SGACL descargada de ISE, ejecute este comando: **sh cts role-based permit**



Verificar contrato creado por DNAC

Para verificar la SGACL descargada de ISE, ejecute este comando: **show access-list <ACL/Contract Name>**





Contador SGACL subyacente en switches de fabric

Para verificar los resultados de la política SGACL, ejecute este comando: **Show cts role-based counter**

```
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
```

Troubleshoot

Problema 1. En caso de que ambos nodos ISE estén inactivos.

En caso de que ambos nodos ISE estén inactivos, se elimina la asignación de IP a SGT recibida por ISE y todas las DGT se etiquetan como desconocidas, y todas las sesiones de usuario que existen se detienen después de 5-6 minutos.

> **Nota:** Este problema sólo se aplica cuando el acceso SGACL (sgt (xxxx) -> desconocido (0) se limita a DHCP, DNS y puerto de proxy web.

Solución:

1. Creó una SGT (p. ej. RFC1918).
2. Presione el rango de IP privada RFC a ambos extremos.
3. Limite el acceso a DHCP, DNS y proxy web desde sgt (xxxx) —> RFC1918
4. Crear/modificar sgacl sgt (xxxx) —> desconocido con contrato Permit IP.

Ahora, si ambos nodos ise se desactivan, SGACL indica—>resultados desconocidos y la sesión existente está intacta.

Problema 2. Voz unidireccional de teléfono IP o sin voz.

La conversión de la extensión a IP ocurrió en el SIP y la comunicación de voz real ocurre a través de RTP entre IP y IP. CUCM y Gateway de voz se agregaron a **DGT_Voice**.

Solución:

1. Se puede habilitar la misma ubicación o la comunicación de voz horizontal permitiendo el tráfico desde IP_Phone —> IP_Phone.
2. El rango de protocolo RTP Permitente en DGT RFC1918 puede permitir el resto de la ubicación. Se puede permitir el mismo rango para IP_Phone —> Unknown.

Problema 3. El punto final de VLAN crítico no tiene acceso a la red.

DNAC aprovisiona el switch con VLAN crítica para datos y, según la configuración, todas las nuevas conexiones durante la interrupción de ISE obtienen VLAN crítica y SGT 3999. La política Denegación predeterminada en trustsec restringe la nueva conexión para acceder a cualquier recurso de red.

Solución:

Empuje SGACL para SGT crítico en todos los switches de borde y extremo mediante la plantilla DNAC

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

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

Estos comandos se agregan a la sección de configuración.

> **Nota:** Todos los comandos se pueden combinar en una única plantilla y se pueden enviar durante el aprovisionamiento.

Problema 4. VLAN Crítica de Descarte de Paquetes.

Una vez que la máquina se encuentra en una VLAN crítica debido a la caída de los nodos ISE, hay una caída de paquetes cada 3-4 minutos (se observan 10 caídas como máximo) para todos los terminales en la VLAN crítica.

Observaciones: Los contadores de autenticación aumentan cuando los servidores están MUERTOS. Los clientes intentan autenticarse con PSN cuando los servidores se marcaron

DEAD.

Solución:

Lo ideal es que no haya ninguna solicitud de autenticación de un terminal si los nodos PSN ISE están inactivos.

Presione este comando en el servidor RADIUS con DNAC:

nombre de usuario de la prueba automática auto-test-on

Con este comando en el switch, envía mensajes de autenticación de prueba periódicos al servidor RADIUS. Busca una respuesta RADIUS del servidor. No es necesario un mensaje de éxito: basta con una autenticación fallida porque muestra que el servidor está vivo.

Additional Information

Plantilla final de DNAC:

```
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
```

Nota: Todas las interfaces de link ascendente en los nodos de borde se configuran sin aplicación y se supone que el link ascendente se conecta solamente con el nodo de borde. En los nodos de borde, las interfaces de enlace ascendente hacia los nodos de borde necesitan configurarse sin aplicación y eso debe hacerse manualmente.