Modelo de lista de permissões do Cisco ISE TrustSec (IP de negação padrão) com SDA

Contents

Introduction

Este documento descreve como ativar o modelo de lista de permissões (Default Deny IP) do TrustSec no Software Defined Access (SDA). Este documento envolve várias tecnologias e componentes que incluem Identity Services Engine (ISE), Digital Network Architecture Center (DNAC) e Switches (Borda e Borda).

Há dois modelos Trustsec disponíveis:

- Modelo de lista de negação (IP de permissão padrão): Neste modelo, a ação padrão é Permit IP (Permitir IP) e todas as restrições devem ser configuradas explicitamente com o uso de Security Group Access Lists (SGACLs). Isso é geralmente usado quando você não tem uma compreensão completa dos fluxos de tráfego na rede. Esse modelo é bastante fácil de implementar.

- Modelo de Lista de Permissão (IP de Negação Padrão): Neste modelo, a ação padrão é Deny IP (Negar IP) e, portanto, o tráfego necessário deve ser explicitamente permitido com o uso de SGACLs. Geralmente, isso é usado quando o cliente tem uma compreensão justa do tipo de fluxo de tráfego em sua rede. Esse modelo exige um estudo detalhado do tráfego do plano de controle, bem como o potencial de bloquear TODO o tráfego, no momento em que ele é ativado.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Autenticação Dot1x/MAB
- Cisco TrustSec (CTS)
- Protocolo de intercâmbio de segurança (SXP)
- Web Proxy
- Conceitos de firewall
- DNAC

Componentes Utilizados

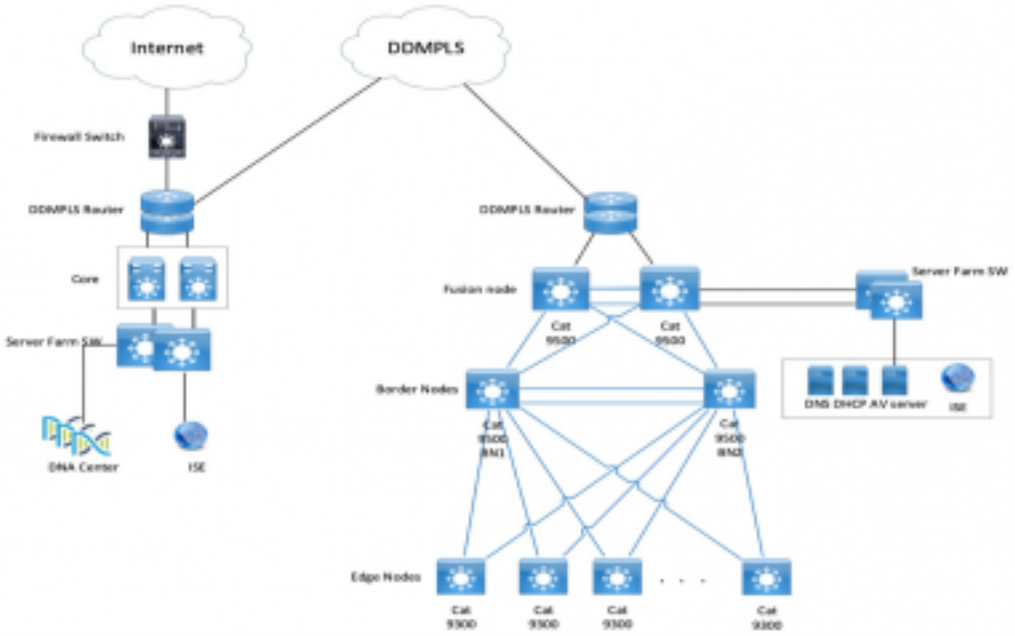
As informações neste documento são baseadas nestas versões de software e hardware:

- 9300 Edge e 9500 Border Nodes (Switches) com IOS 16.9.3
- DNAC 1.3.0.5
- Patch 3 do ISE 2.6 (dois nós - implantação redundante)
- O DNAC e o ISE estão integrados
- Os nós de borda e borda são provisionados pelo DNAC
- O túnel SXP é estabelecido do ISE (alto-falante) para ambos os nós de borda (ouvinte)
- Os pools de endereços IP são adicionados à integração do 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 Rede



Configuração

Estas são as etapas para ativar o modelo Allow-List (IP de negação padrão):

1. Altere o SGT dos switches desconhecidos para dispositivos TrustSec.
2. Desative a imposição baseada em funções CTS.
3. Mapeamento IP-SGT em switches de borda e borda usando o modelo DNAC.
4. Fallback SGACL usando Modelo de DNAC.
5. Habilitar Allow-List (IP de negação padrão) na Matriz Trustsec.
6. Crie SGT para endpoints/usuários.
7. Crie SGACL para endpoints/usuários (para tráfego de sobreposição de produção).

Etapa 1. Altere o SGT dos switches desconhecidos para dispositivos TrustSec.

Por padrão, a SGT (Security Group Tag) desconhecida é configurada para autorização de dispositivo de rede. A alteração para o TrustSec Device SGT oferece mais visibilidade e ajuda a criar SGACL específico para o tráfego iniciado pelo Switch.

Navegue até **Centros de trabalho > TrustSec > Política Trustsec > Autorização de dispositivo de rede** e altere-a para Trustsec_Devices de Desconhecido

Etapa 2. Desative a aplicação baseada em funções do CTS.

- Depois que o modelo Allow-List (Negação padrão) estiver estabelecido, todo o tráfego será bloqueado na estrutura, incluindo o tráfego de multicast subjacente e de broadcast, como Sistema intermediário para sistema intermediário (IS-IS), Bidirectional Forwarding Detection (BFD), Secure Shell (SSH).

- Todas as portas do TenGig que se conectam à borda da estrutura, bem como a borda, devem ser configuradas com o comando aqui. Com isso em vigor, o tráfego iniciado a partir dessa interface e que chega a essa interface não está sujeito à aplicação.

```
Interface tengigabitethernet 1/0/1

no cts role-based enforcement
```

> **Note**: Isso pode ser feito com o uso de um modelo de intervalo no DNAC para simplificar. Caso contrário, para cada switch, é necessário fazer manualmente durante o provisionamento. O trecho abaixo mostra como fazer isso através de um modelo de DNAC.

```
interface range $uplink1

no cts role-based enforcement
```

Para obter mais informações sobre modelos de DNAC, *consulte* este URL para o 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

Etapa 3. Mapeamento IP-SGT em switches de borda e borda com modelo DNAC.

A ideia é que o mapeamento IP-SGT local esteja disponível nos switches mesmo que todo ISE fique inoperante. Isso garante que a Subcamada esteja ativa e que a conectividade com os recursos críticos esteja intacta

A primeira etapa é vincular serviços críticos a um SGT (ex - Basic_Network_Services/1000). Alguns desses serviços incluem:

- Sub-rede de sub-rede/ISIS
- ISE/DNAC
- Ferramenta de monitoramento
- Sub-rede do AP em caso de OTT
- Servidor de terminal
- Serviços essenciais - Ex: Telefone IP

Exemplo:

```
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
```

Etapa 4. Fallback SGACL com Modelo de DNAC.

Um mapeamento SGT não tem utilidade até que um SGACL relevante seja criado usando o SGT e, portanto, nossa próxima etapa seria criar um SGACL que atue como um Fallback local no caso de os nós do ISE ficarem inativos (quando os serviços do ISE estão inativos, o túnel SXP fica inativo e, portanto, o SGACL e o mapeamento SGT IP não são baixados dinamicamente).

Essa configuração é enviada para todos os nós de borda e borda.

Contrato/ACL com base em função de retorno:

```
ip access-list role-based FALLBACK

permit ip
```

Dispositivos TrustSec para dispositivos TrustSec:

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

Acima da SGACL Garanta a comunicação com switches de malha e IPs subjacentes

Dispositivos TrustSec para SGT 1000:

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

Acima da SGACL Garanta a comunicação de switches e access points com ISE, DNAC, WLC e ferramentas de monitoramento

Dispositivos SGT 1000 para TrustSec:

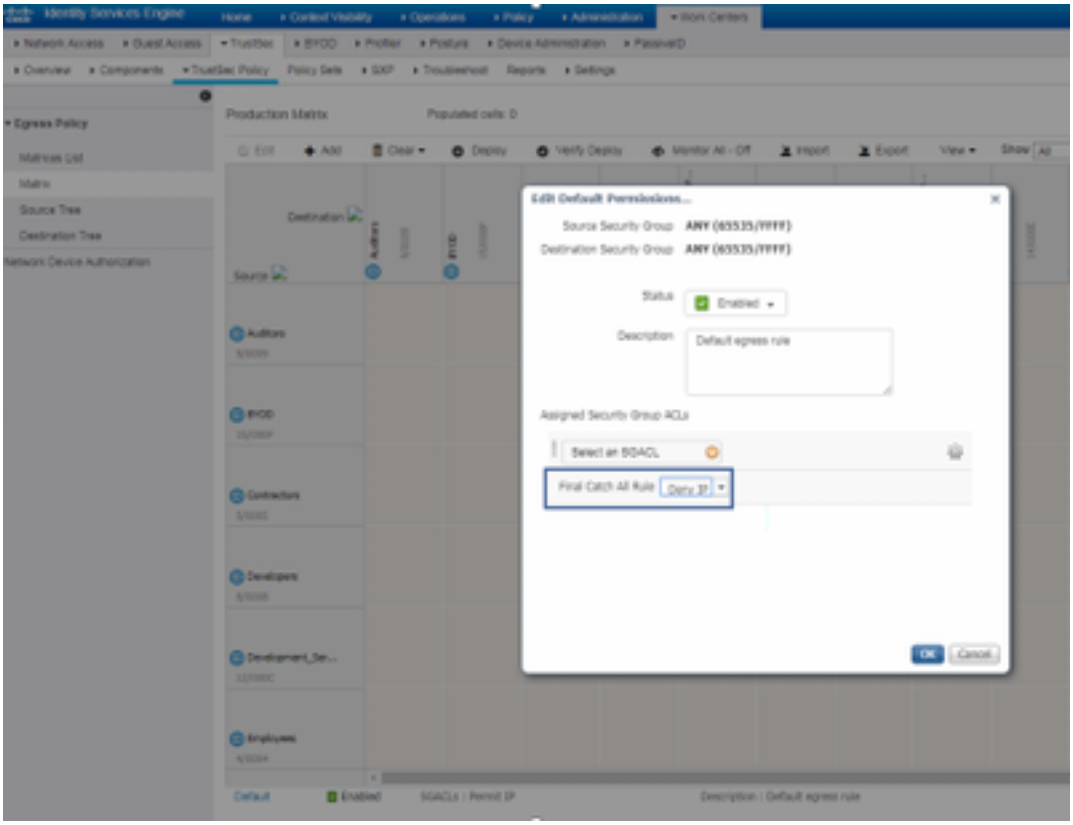
```
cts role-based permissions from 1000 to 2 FALLBACK
```

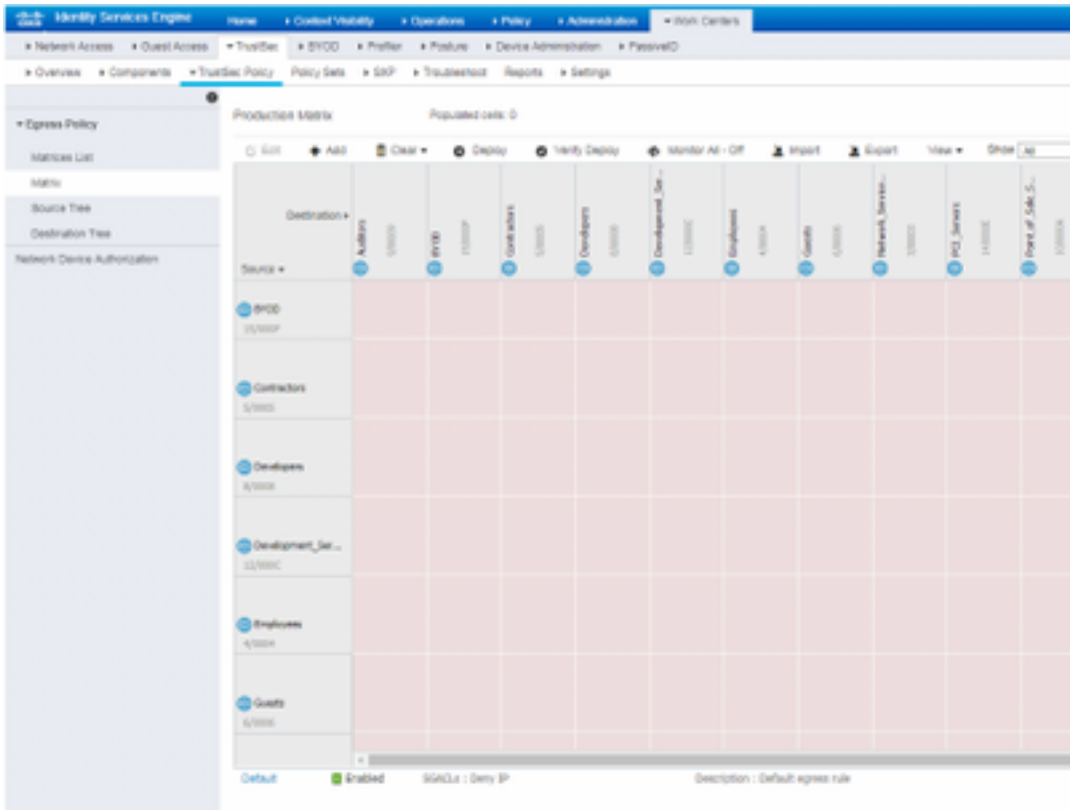
Acima da SGACL Garanta a comunicação de pontos de acesso com ISE, DNAC, WLC e ferramentas de monitoramento para switches

Etapa 5. Habilitar Modelo de Lista de Permissões (Negação Padrão) na Matriz TrustSec.

O requisito é negar a maioria do tráfego na rede e permitir uma menor extensão. Em seguida, serão necessárias menos políticas se você usar a negação padrão com regras de permissão explícitas.

Navegue até **Centros de trabalho > Trustsec > Política TrustSec > Matriz > Padrão** e altere-o para **Negar tudo** na regra de captura final.





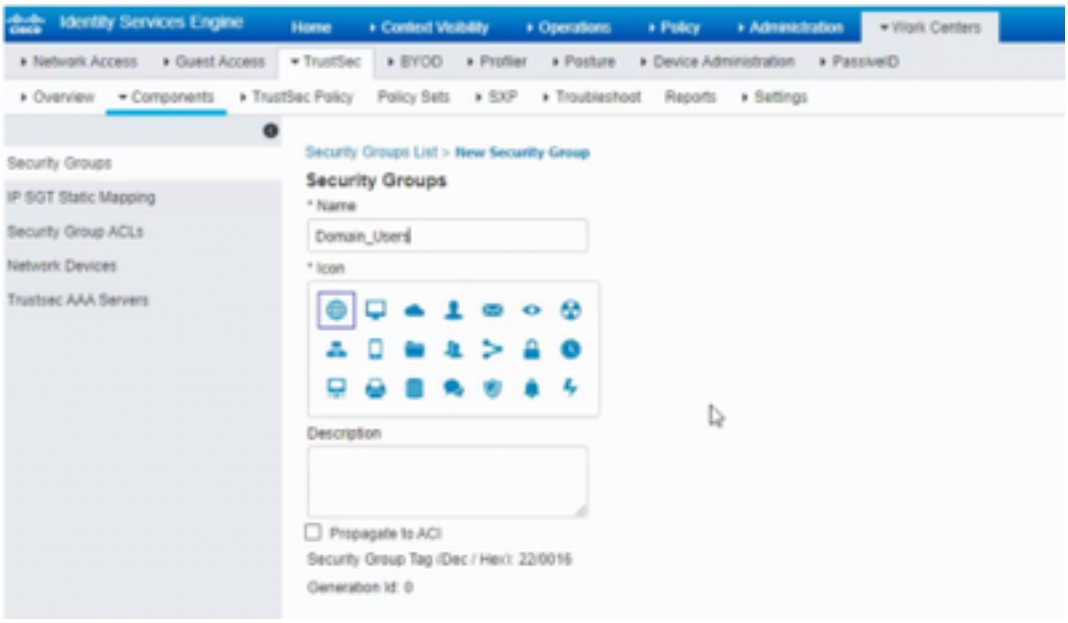
Note: Esta imagem representa (Todas as colunas estão em vermelho por padrão), a negação padrão foi ativada e somente o tráfego seletivo pode ser permitido após a criação da SGACL.

Etapa 6. Crie SGT para endpoints/usuários.

No ambiente SDA, o New SGT só deve ser criado a partir da GUI do DNAC, pois há vários casos

de corrupção do banco de dados devido à incompatibilidade do banco de dados SGT no ISE/DNAC.

Para criar SGT, faça login em **DNAC > Policy > Group-Based Access Control > Scalable Groups > Add Groups**, uma página o redireciona para **ISE Scalable Group**, clique em **Add,** insira o nome SGT e salve-o.



O mesmo SGT reflete no DNAC através da integração PxGrid. Este é o mesmo procedimento para toda a futura criação de SGT.

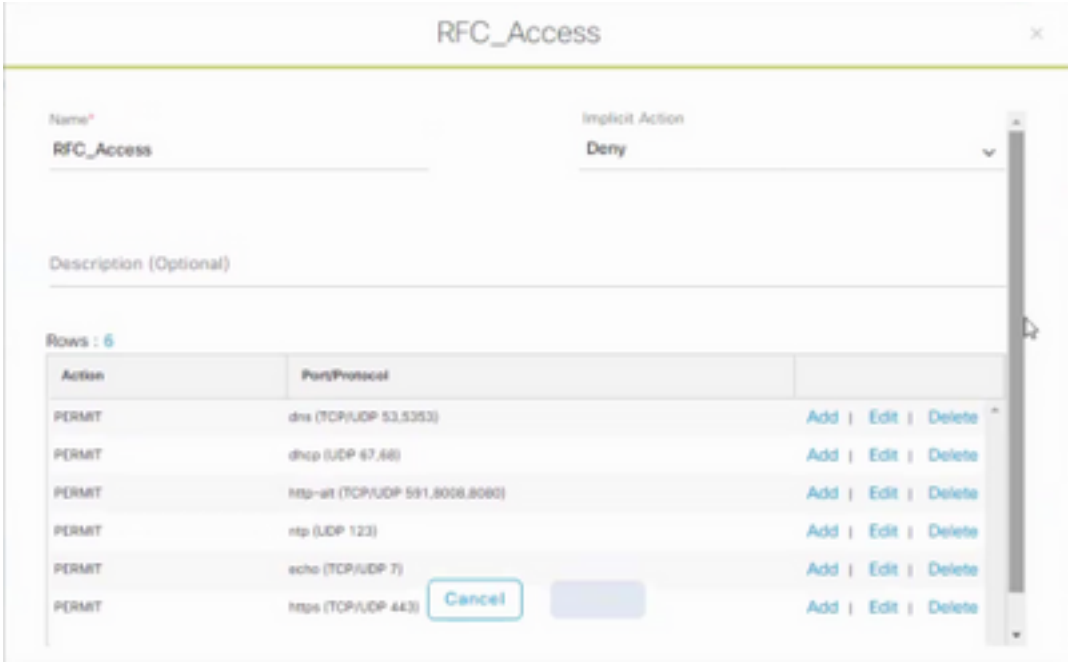
Passo 7. Crie SGACL para endpoints/usuários (para tráfego de sobreposição de produção).

No ambiente SDA, o New SGT deve ser criado somente a partir da GUI do DNAC.

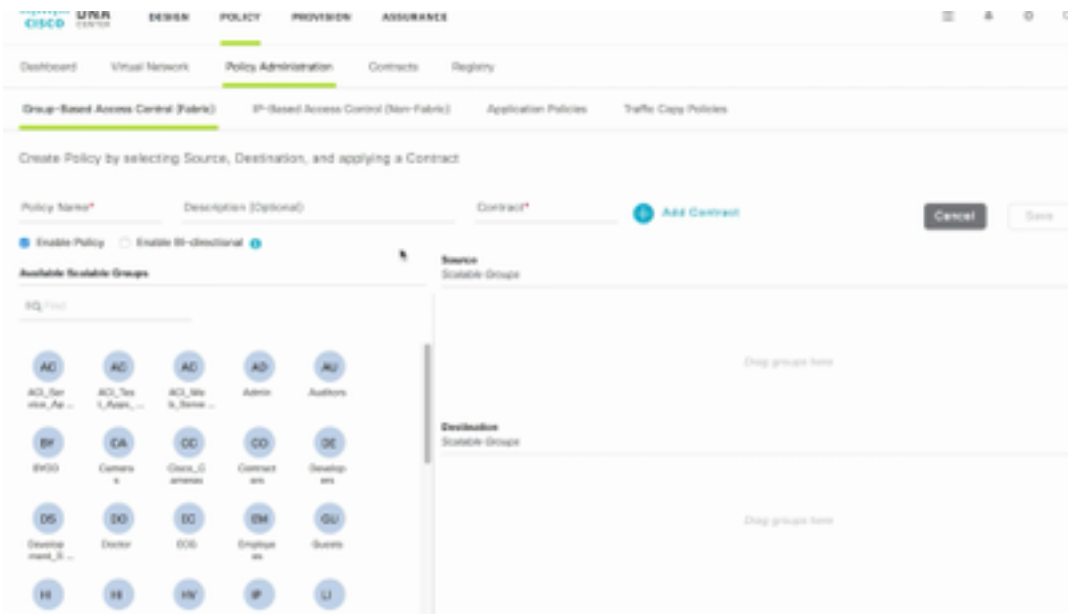
```
Policy Name: Domain_Users_Access

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)
```

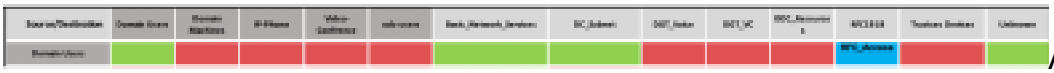
Para criar um **Contrato**, faça login no **DNAC** e navegue para **Política > Contratos > Adicionar contratos > Adicionar protocolos necessários** e clique em **Salvar**.



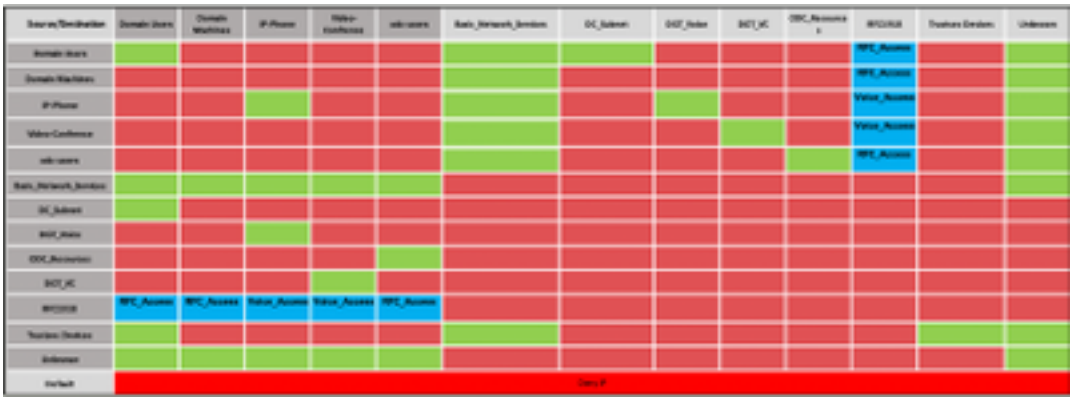
Para criar um Contrato, faça login no **DNAC** e navegue para **Política > Controle de acesso baseado em grupo > Políticas de acesso baseadas em grupo > Adicionar políticas > Criar política (com as informações fornecidas)** agora clique em **Salvar** e em **Implantar**.

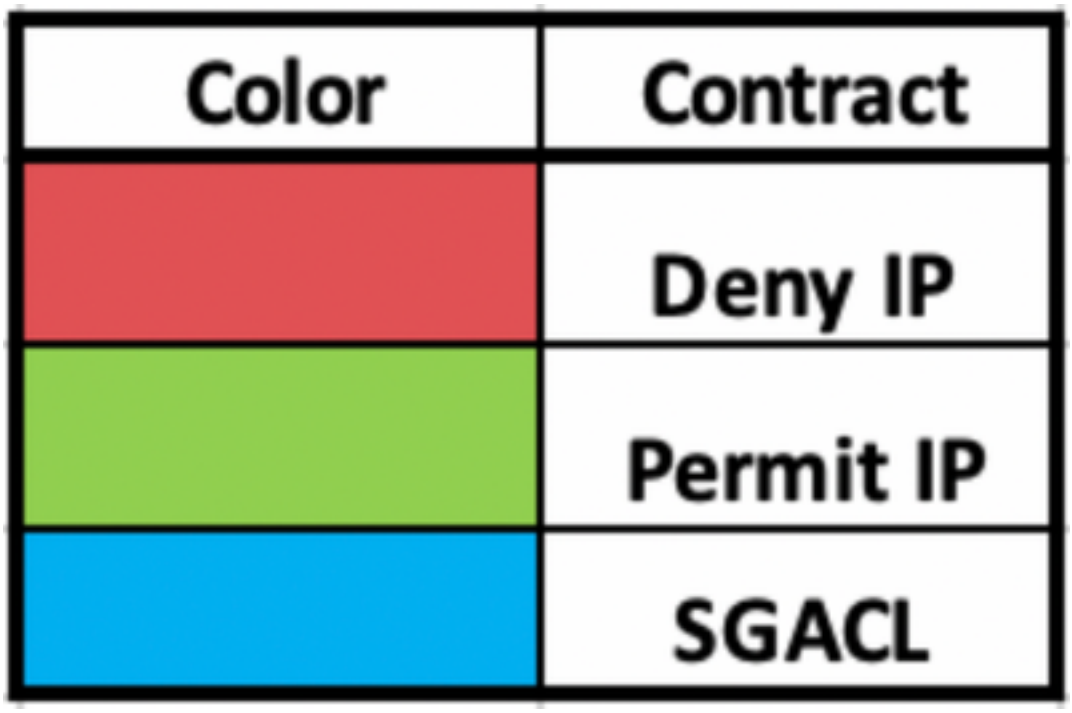


Depois que o SGACL/Contrato é configurado a partir do DNAC, ele reflete automaticamente no ISE. abaixo está um exemplo de exibição de matriz unidirecional para um sgt.



A GACL Matrix, como mostrado na imagem abaixo, é uma exibição de exemplo para o modelo Allow-list (Default Deny).





Verificar

Dispositivo de rede SGT

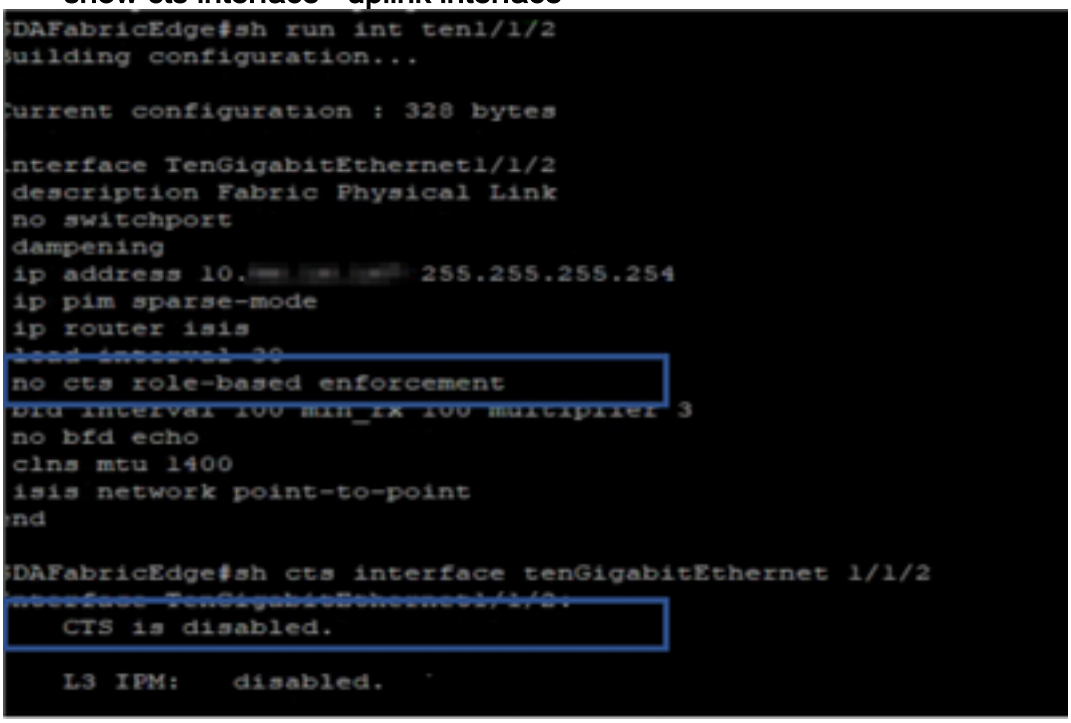
Para verificar os switches SGT recebidos pelo ISE, execute este comando: **show cts environment-data**

```
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
```

Aplicação em portas de uplink

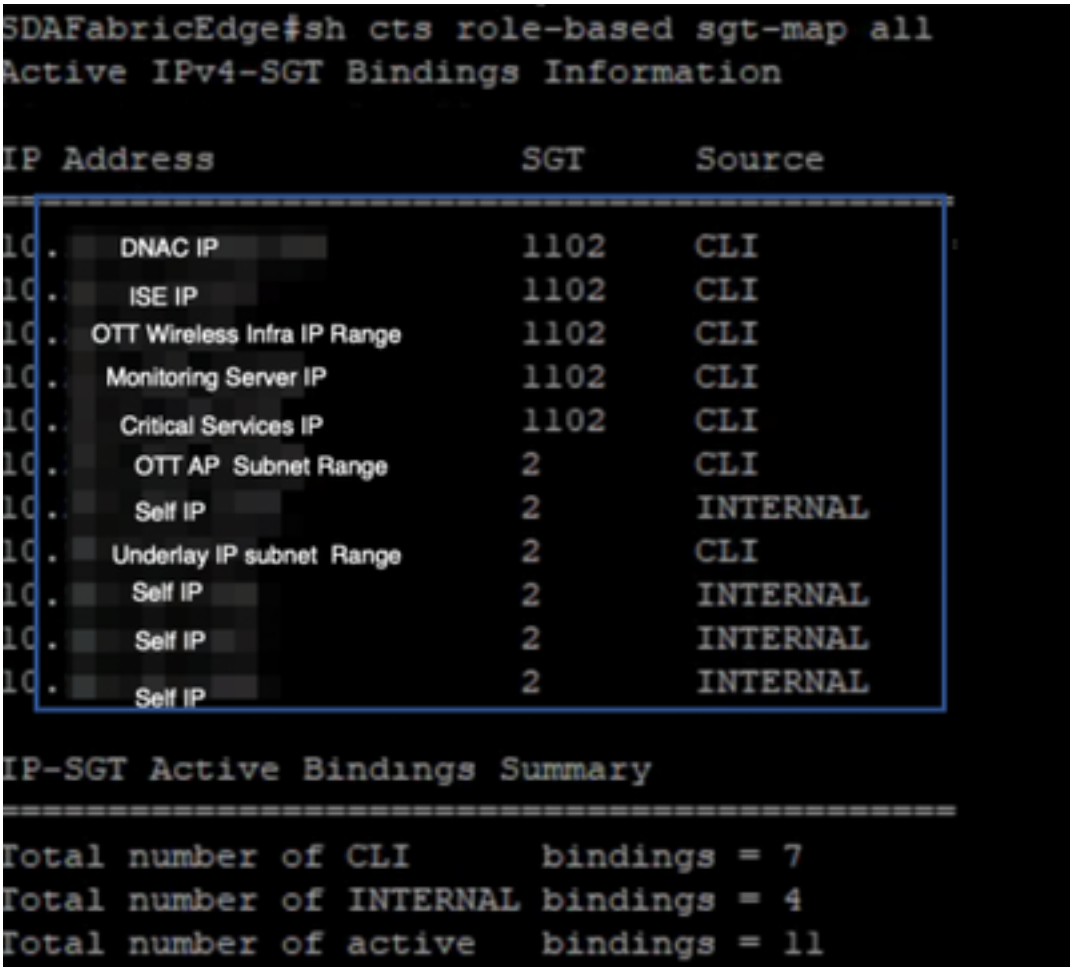
Para verificar a aplicação na interface de uplink, execute estes comandos:

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



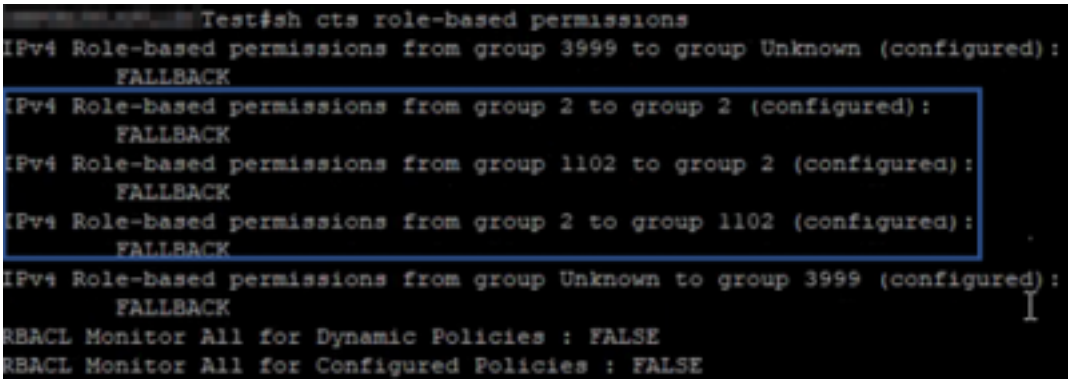
Mapeamento IP-SGT local

Para verificar os mapeamentos IP-SGT configurados localmente, execute este comando: **sh cts role-based sgt-map all**



SGACL de FALLBACK local

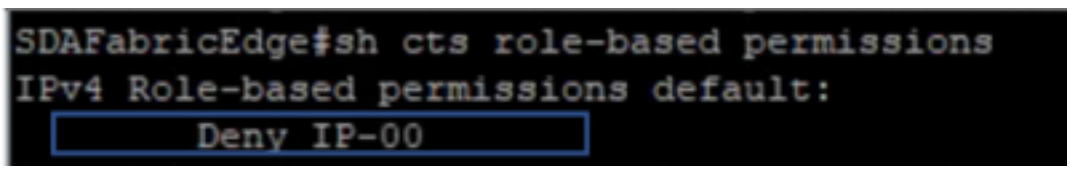
Para verificar FALLBACK SGACL, execute este comando: **sh cts role-based permit**



Note: A SGACL enviada pelo ISE tem uma prioridade sobre a SGACL local.

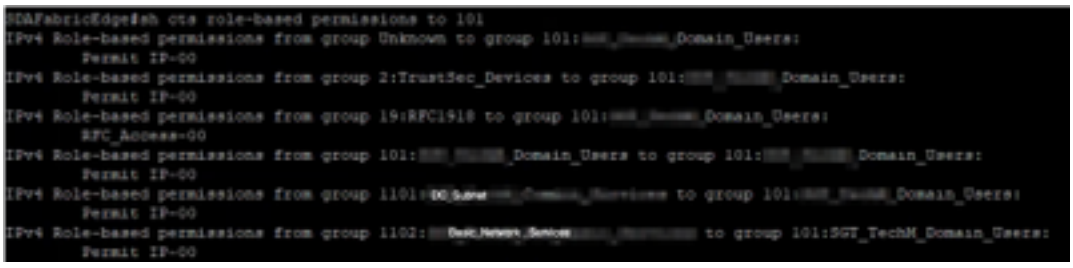
Ativação de Permitir Lista (Negação Padrão) em Switches de Estrutura

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



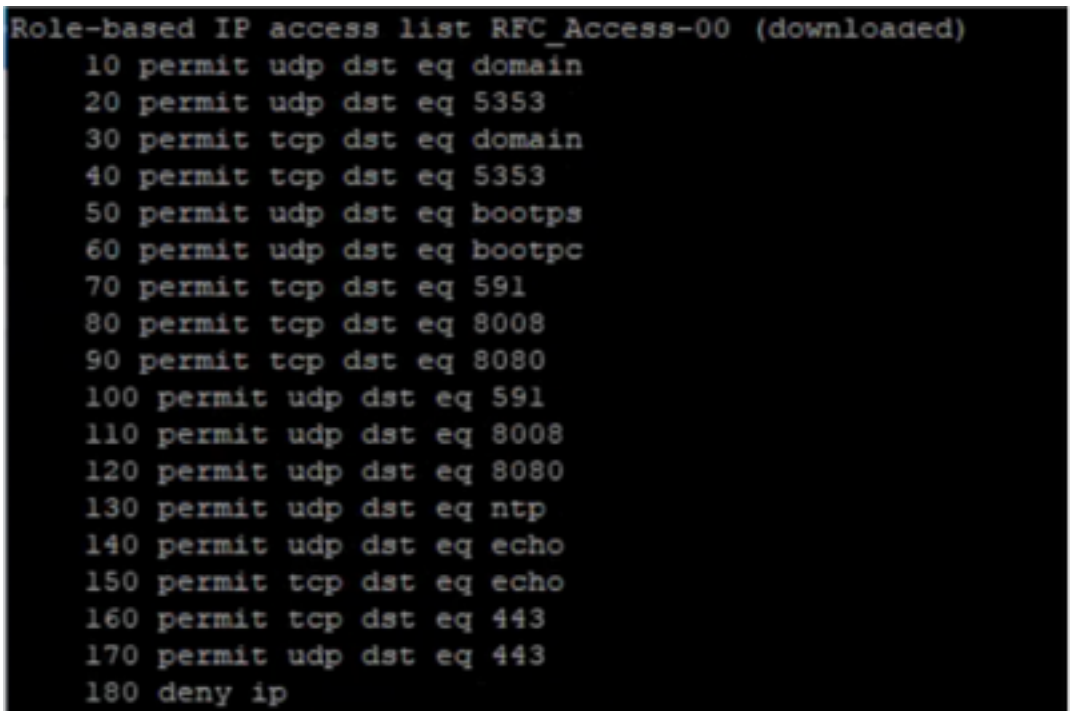
SGACL para Endpoint Conectado à Estrutura

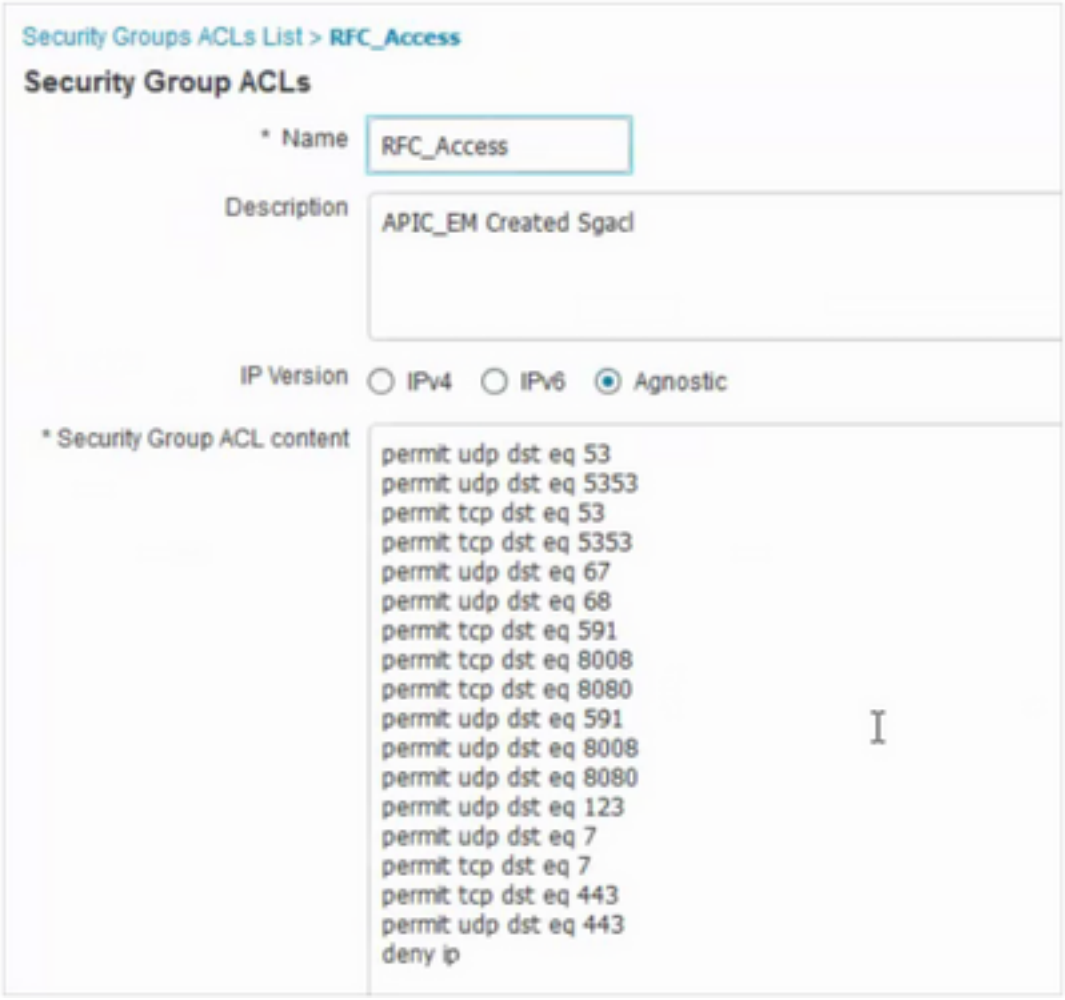
Para verificar o SGACL baixado do ISE, execute este comando: **sh cts role-based permit**



Verificar o contrato criado pela DNAC

Para verificar o SGACL baixado do ISE, execute este comando: **show access-list <ACL/Contract Name>**





Submeter o contador SGACL em switches de estrutura

Para verificar os acertos da política SGACL, execute 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. Caso os dois nós do ISE estejam inativos.

Caso ambos os nós do ISE estejam inoperantes, o mapeamento de IP para SGT recebido pelo ISE é removido e todos os DGTs são marcados como desconhecidos, e todas as sessões de usuário existentes são interrompidas após 5 a 6 minutos.

> **Note**: Esse problema é aplicável somente quando sgt (xxxx) -> desconhecido (0) O acesso SGACL é limitado a DHCP, DNS e porta proxy da Web.

Solução:

1. Criado um SGT (ex. RFC1918).
2. Empurre o intervalo de IP privado de RFC para ambas as bordas.
3. Limite o acesso ao DHCP, DNS e proxy da Web do sgt (xxxx) —> RFC1918
4. Criar/modificar sgacl sgt (xxxx) —> desconhecido com contrato de licença IP.

Agora, se ambos os nós do ise ficarem inativos, sgt SGACL—>ocorrências desconhecidas e a sessão existente estiver intacta.

Problema 2. Telefone IP unidirecional ou sem voz.

A extensão para conversão de IP aconteceu no SIP e a comunicação de voz real ocorre sobre o RTP entre IP e IP. CUCM e Gateway de Voz foram adicionados ao **DGT_Voice**.

Solução:

1. A mesma localização ou comunicação de voz leste-oeste pode ser ativada permitindo o tráfego de IP_Phone —> IP_Phone.
2. O restante do local pode ser permitido pelo intervalo do protocolo RTP de permissão no DGT RFC1918. O mesmo intervalo pode ser permitido para IP_Phone —> Desconhecido.

Problema 3. O ponto final crítico da VLAN não tem acesso à rede.

O DNAC provisiona o switch com VLAN crítica para dados e, conforme a configuração, todas as novas conexões durante a interrupção do ISE obtêm VLAN crítica e SGT 3999. A política Default Deny in trustsec restringe a nova conexão para acessar qualquer recurso de rede.

Solução:

Empurre SGACL para SGT crítico em todos os switches de borda e borda usando o modelo DNAC

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

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

Esses comandos são adicionados à seção de configuração.

> **Note**: Todos os comandos podem ser combinados em um único modelo e podem ser enviados durante o provisionamento.

Problema 4. Pacote com VLAN Crítica.

Quando a máquina está em uma VLAN crítica devido aos nós do ISE desativados, há uma queda de pacote a cada 3 a 4 minutos (máximo de 10 descartes observados) para todos os endpoints em uma VLAN crítica.

Observações: Os contadores de autenticação aumentam quando os servidores estão INATIVOS. Os clientes tentam autenticar com PSN quando os servidores foram marcados como DEAD.

Solução/Solução alternativa:

Idealmente, não deve haver nenhuma solicitação de autenticação de um endpoint se os nós PSN do ISE estiverem inativos.

Empurre este comando no servidor radius com DNAC:

teste automático-testador-automático-nome de usuário-teste automático

Com esse comando no switch, ele envia mensagens periódicas de autenticação de teste ao servidor RADIUS. Ele procura uma resposta RADIUS do servidor. Uma mensagem de êxito não é necessária - uma autenticação com falha é suficiente porque mostra que o servidor está ativo.

Additional Information

Modelo final do 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
```

> **Note**: Todas as interfaces de uplink em nós de borda são configuradas sem aplicação e presume-se que o uplink se conecta somente ao nó de borda. Nos nós de borda, as

interfaces de uplink em direção aos nós de borda precisam ser configuradas sem imposição e isso precisa ser feito manualmente.