带SDA的思科ISE TrustSec允许列表模型（默认拒绝IP）

目录

简介

本文档介绍如何在软件定义访问(SDA)中启用TrustSec的允许列表（默认拒绝IP）模型。 本文档涉及多种技术和组件，包括身份服务引擎(ISE)、数字网络架构中心(DNAC)和交换机（边界和边缘）。

有两种可用的Trustsec模型：

- 拒绝列表模型（默认允许IP）：在此模型中，默认操作为Permit IP，应使用安全组访问列表

(SGACL)显式配置任何限制。 当您不完全了解其网络中的流量传输时，通常使用此方法。该模型实施起来相当简单。

- 允许列表模型（默认拒绝IP）：在此模型中，默认操作为Deny IP，因此使用SGACL应明确允许所需的流量。当客户对其网络中的流量类型有公平的了解时，通常使用此方法。此模型需要详细研究控制平面流量，并且它在启用时有可能阻止所有流量。

先决条件

要求

Cisco 建议您了解以下主题：

- Dot1x/MAB身份验证
- 思科TrustSec(CTS)
- 安全交换协议(SXP)
- Web代理
- 防火墙概念
- DNAC

使用的组件

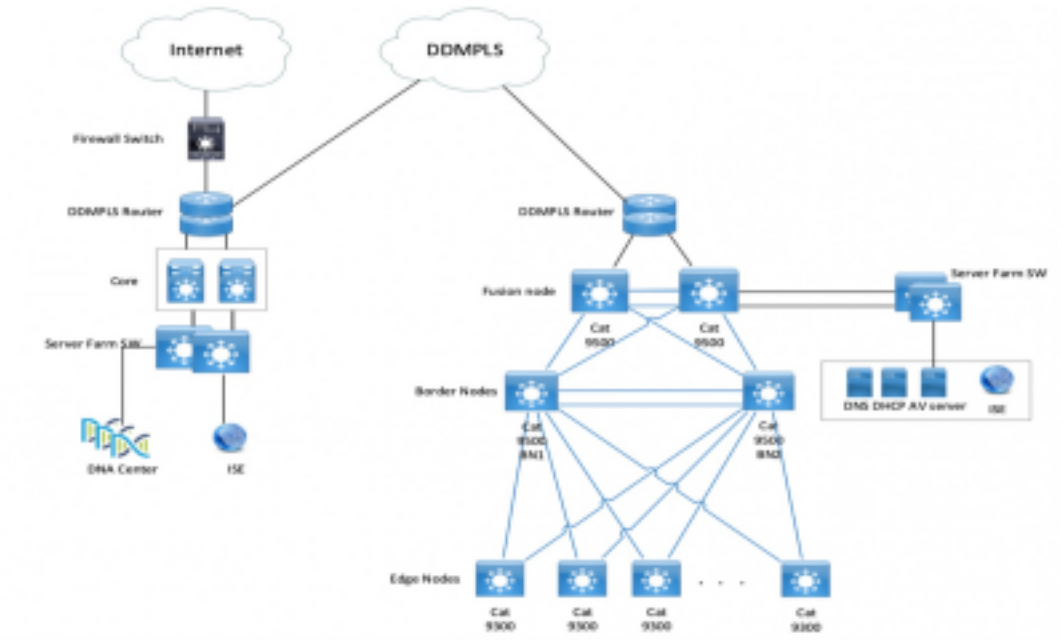
本文档中的信息基于以下软件和硬件版本：

- 9300边缘和9500边界节点（交换机），带IOS 16.9.3
- DNAC 1.3.0.5
- ISE 2.6补丁3（两个节点 — 冗余部署）
- DNAC和ISE集成
- 边界节点和边缘节点由DNAC调配
- SXP隧道从ISE（扬声器）建立到两个边界节点（侦听器）
- IP地址池已添加到主机自注册

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

网络图



配置

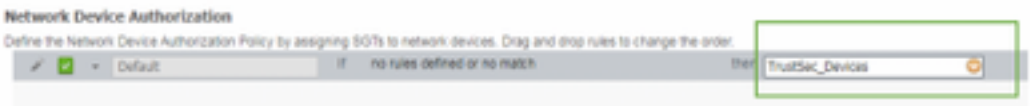
以下是启用允许列表模型（默认拒绝IP）的步骤：

1. 将交换机SGT从Unknown更改为TrustSec设备。
2. 禁用基于CTS角色的实施。
3. 使用DNAC模板的边界和边缘交换机上的IP-SGT映射。
4. 使用DNAC模板回退SGACL。
5. 在trustsec矩阵中启用允许列表（默认拒绝IP）。
6. 为终端/用户创建SGT。
7. 为终端/用户创建SGACL（用于生产重叠流量）。

步骤1.将交换机SGT从Unknown更改为TrustSec设备。

默认情况下，为网络设备授权配置未知安全组标记(SGT)。将其更改为TrustSec设备SGT可提供更高的可视性，并有助于为交换机发起的流量创建特定于SGACL。

导航至**工作中心> TrustSec > Trustsec策略>网络设备授权**，然后将其从未知更改为Trustsec_Devices



步骤2.禁用CTS基于角色的实施。

- 一旦允许列表模型（默认拒绝）就位，所有流量都会在交换矩阵中被阻止，包括底层组播和广播流量，如中间系统到中间系统(IS-IS)、双向转发检测(BFD)、安全外壳(SSH)流量。
- 连接到交换矩阵边缘以及边界的所有TenGig端口都应使用此处的命令进行配置。在此情况下，从此接口发起的流量和到此接口的流量不受实施限制。

```
Interface tengigabitethernet 1/0/1

no cts role-based enforcement
```

> **注意**：为简单起见，可以在DNAC中使用范围模板。否则，对于每台交换机，都需要在调配过程中手动完成。以下代码段显示如何通过DNAC模板执行此操作。

```
interface range $uplink1

no cts role-based enforcement
```

有关DNAC模板的详细信息，请参阅本文档的此URL。

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

步骤3.使用DNAC模板的边界和边缘交换机上的IP-SGT映射。

其思想是，即使所有ISE都关闭，本地IP-SGT映射也可在交换机上使用。这可确保底层已打开，与关键资源的连接完好无损

第一步是将关键服务绑定到SGT（例如Basic_Network_Services/1000）。 其中一些服务包括：

- 底层/ISIS子网
- ISE/DNAC
- 监控工具
- AP的子网（如果是OTT）
- 终端服务器
- 关键服务 — 例如：IP电话

示例：

```
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
```

步骤4.使用DNAC模板回退SGACL。

SGT映射在使用SGT创建相关SGACL之前是无用的，因此，我们的下一步是创建SGACL，在ISE节点关闭时（当ISE服务关闭、SXP隧道关闭，因此SGACL和IP SGT映射不动态下载时）用作本地回退。

此配置将推送到所有边缘和边界节点。

回退基于角色的ACL/合同:

```
ip access-list role-based FALLBACK

permit ip
```

TrustSec设备到TrustSec设备：

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

上述SGACL确保交换矩阵交换机和底层IP之间的通信

TrustSec设备到SGT 1000:

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

上述SGACL确保交换机和接入点与ISE、DNAC、WLC和监控工具之间的通信

SGT 1000到TrustSec设备：

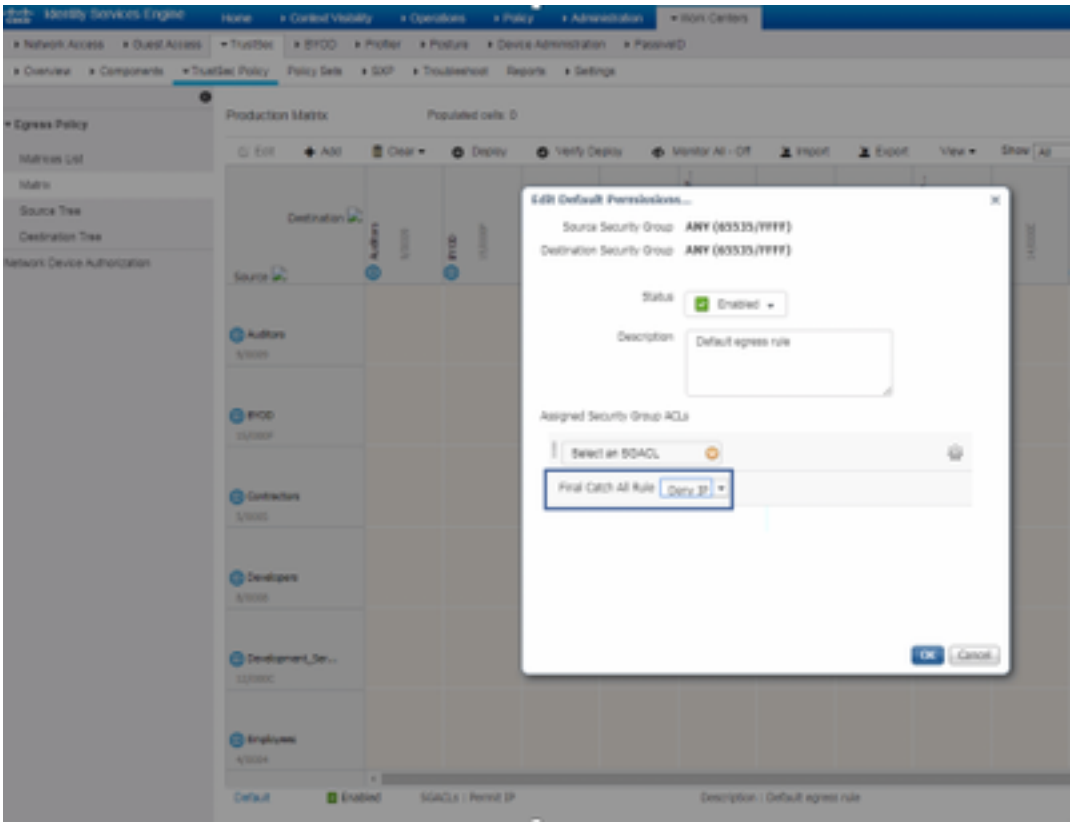
```
cts role-based permissions from 1000 to 2 FALLBACK
```

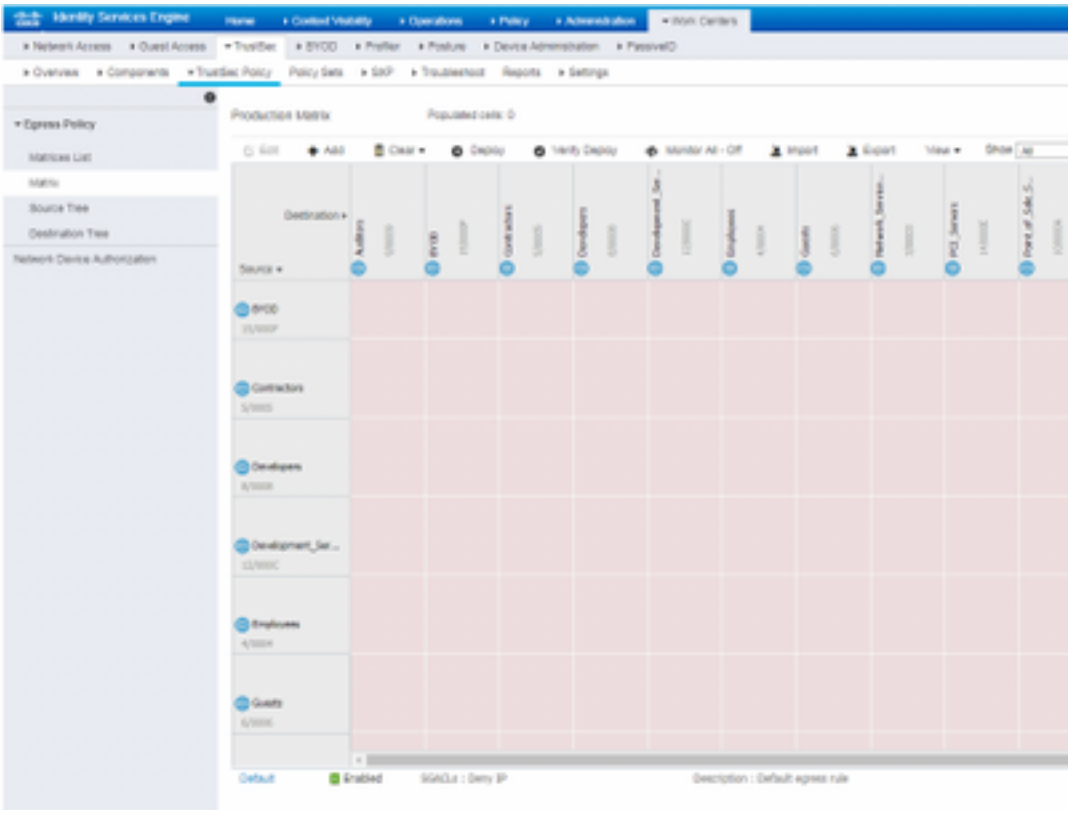
以上SGACL确保从接入点到ISE、DNAC、WLC和监控工具到交换机的通信

步骤5.在TrustSec矩阵中启用允许列表模型（默认拒绝）。

要求是拒绝网络上的大多数流量，并允许较小的范围。如果将默认拒绝与显式允许规则结合使用，则需要的策略更少。

导航至工**作中心(Work Centers)> Trustsec > TrustSec策略(TrustSec Policy)>矩阵(Matrix)>默认(Default)**，并将其更改**为在最终捕获**规则中拒绝全部(Deny All)。



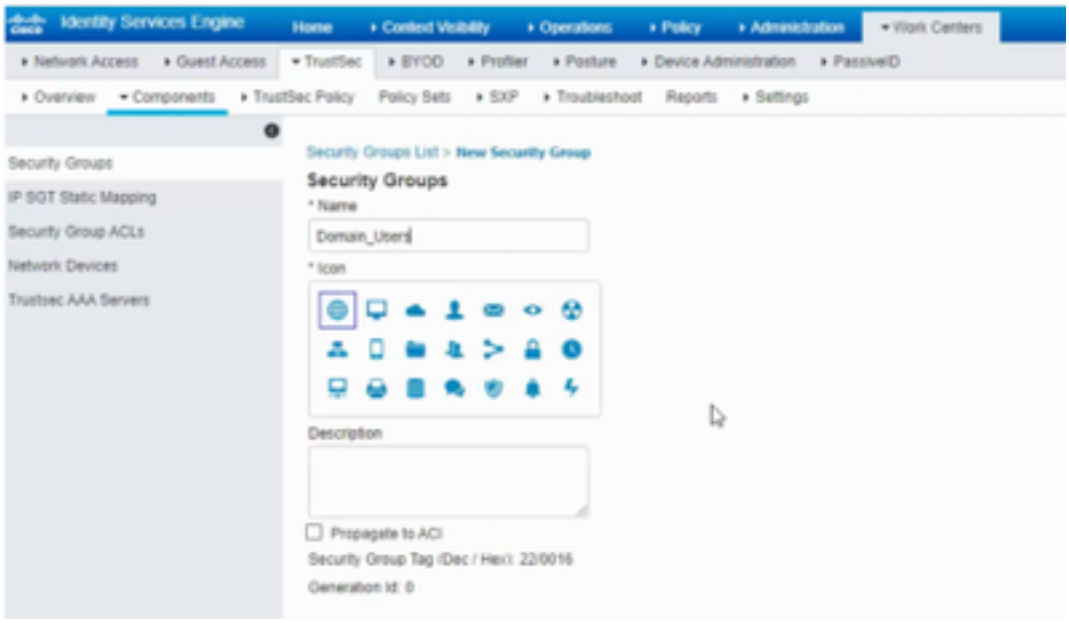


注意：此映像表示（默认情况下，所有列均为红色），已启用默认拒绝，并且在SGACL创建后只能允许选择性流量。

步骤6.为终端/用户创建SGT。

在SDA环境中，只应从DNAC GUI创建新SGT，因为ISE/DNAC中的SGT数据库不匹配导致大量数据库损坏。

要创建SGT，请登录到**DNAC > Policy > Group-Based Access Control > Scalable Groups > Add Groups**，页面将您重定向到**ISE Scalable Group**，单击**Add，输入SGT名称并保存它。**



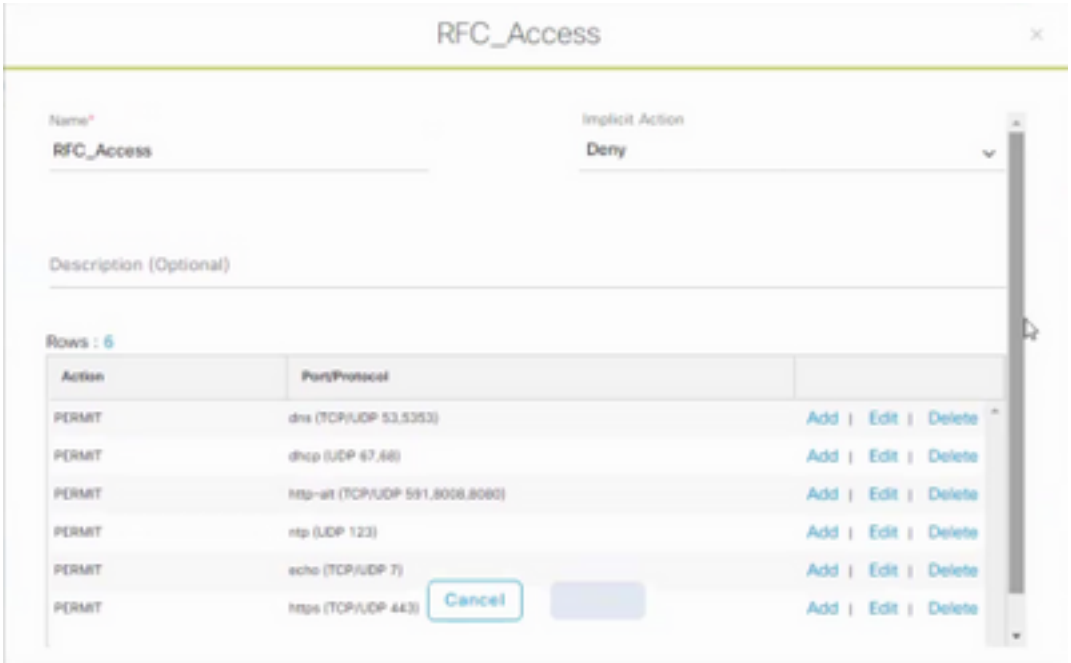
通过PxGrid集成，DNAC中会反映相同的SGT。这与将来创建所有SGT的步骤相同。

步骤7.为终端/用户创建SGACL（用于生产重叠流量）。

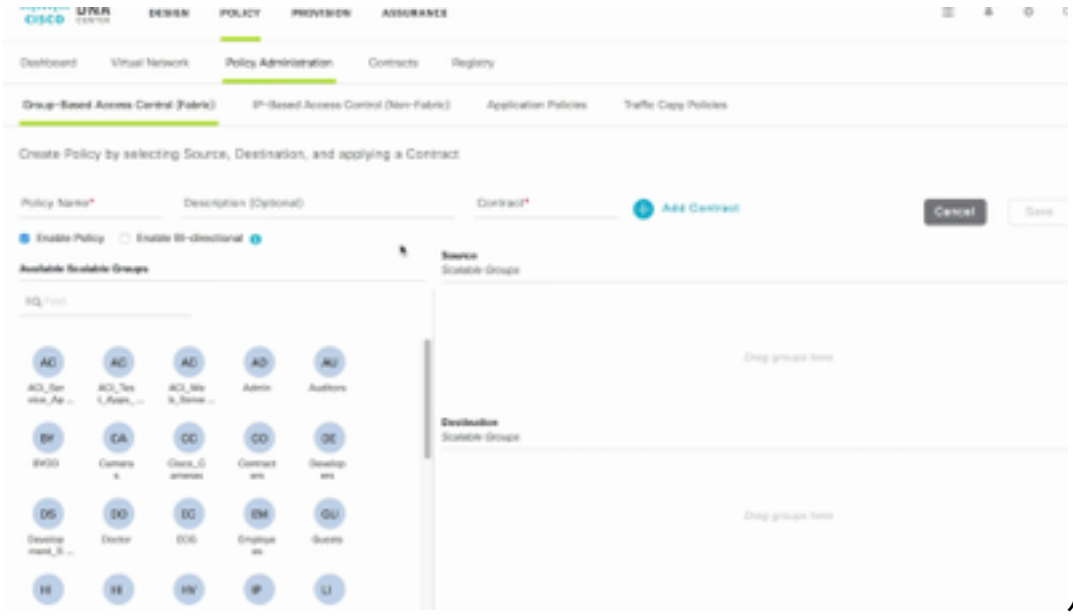
在SDA环境中，应仅从DNAC GUI创建新SGT。

```
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)
```

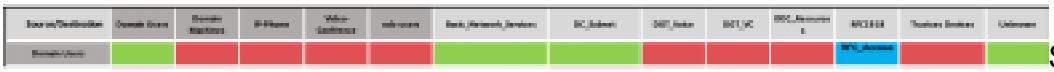
要创建合同，请登**录到DNAC**，然后导航至**策略>合同>添加合同>添加所需协议**，然后单击**保存。**



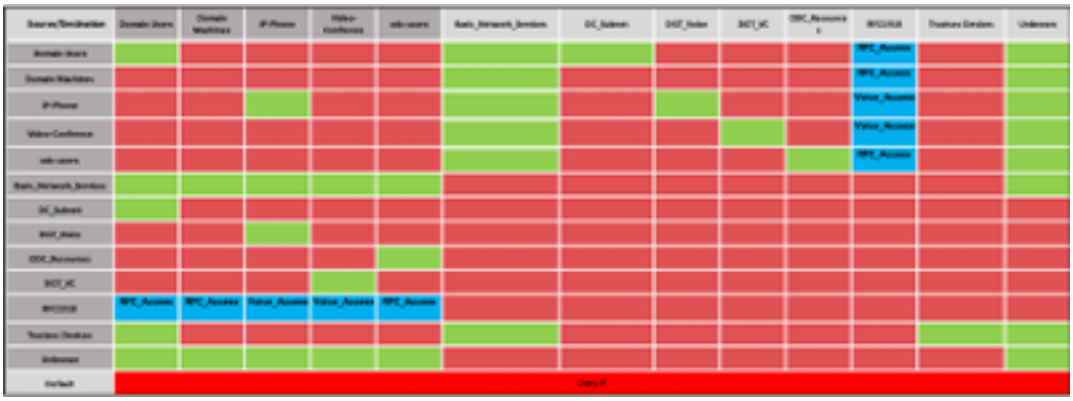
要创建合同，请登录DNAC并导航到**Policy > Group-Based Access Control > Group-Based-Access-Policies > Add Policies > Create policy（含给定信息），现在单击Save** ，然后单击Deploy。

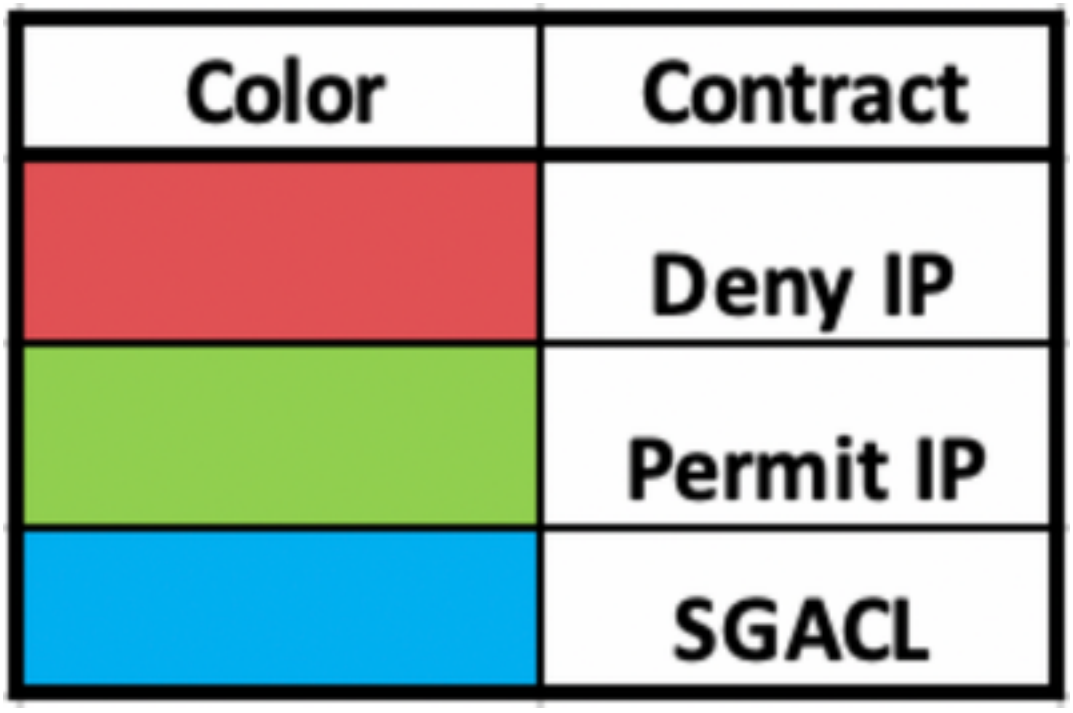


从DNAC配置SGACL/合同后，SGACL/合同会自动反映在ISE中。下面是SGT的单向矩阵视图示例。



SGACL矩阵（如下图所示）是允许列表（默认拒绝）模型的示例视图。

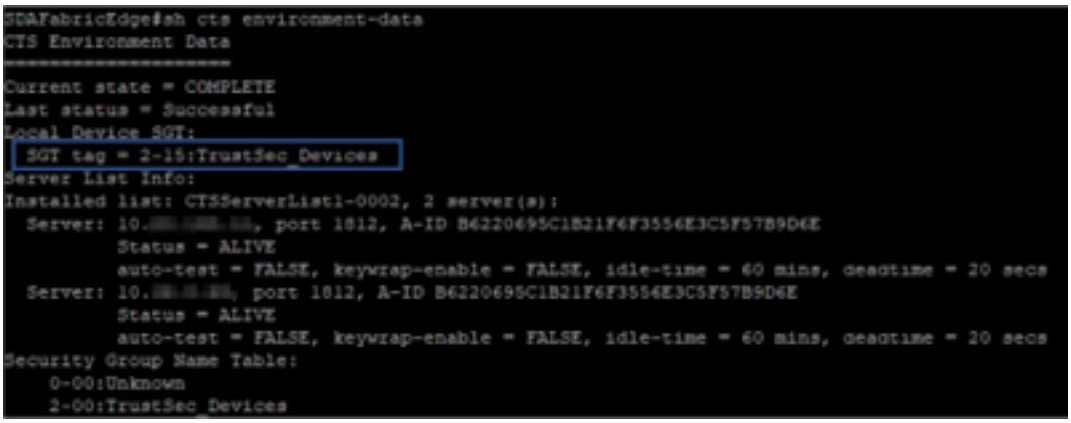




验证

网络设备SGT

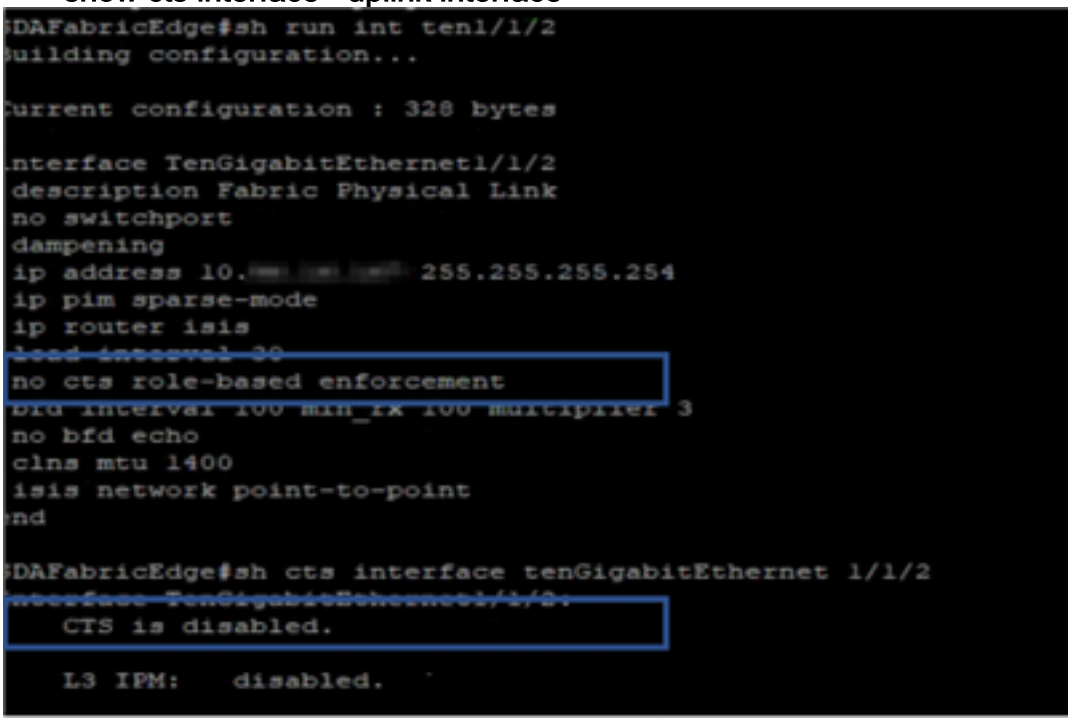
要验证ISE收到的交换机SGT，请运行以下命令：**show cts environmental-data**



在上行链路端口上实施

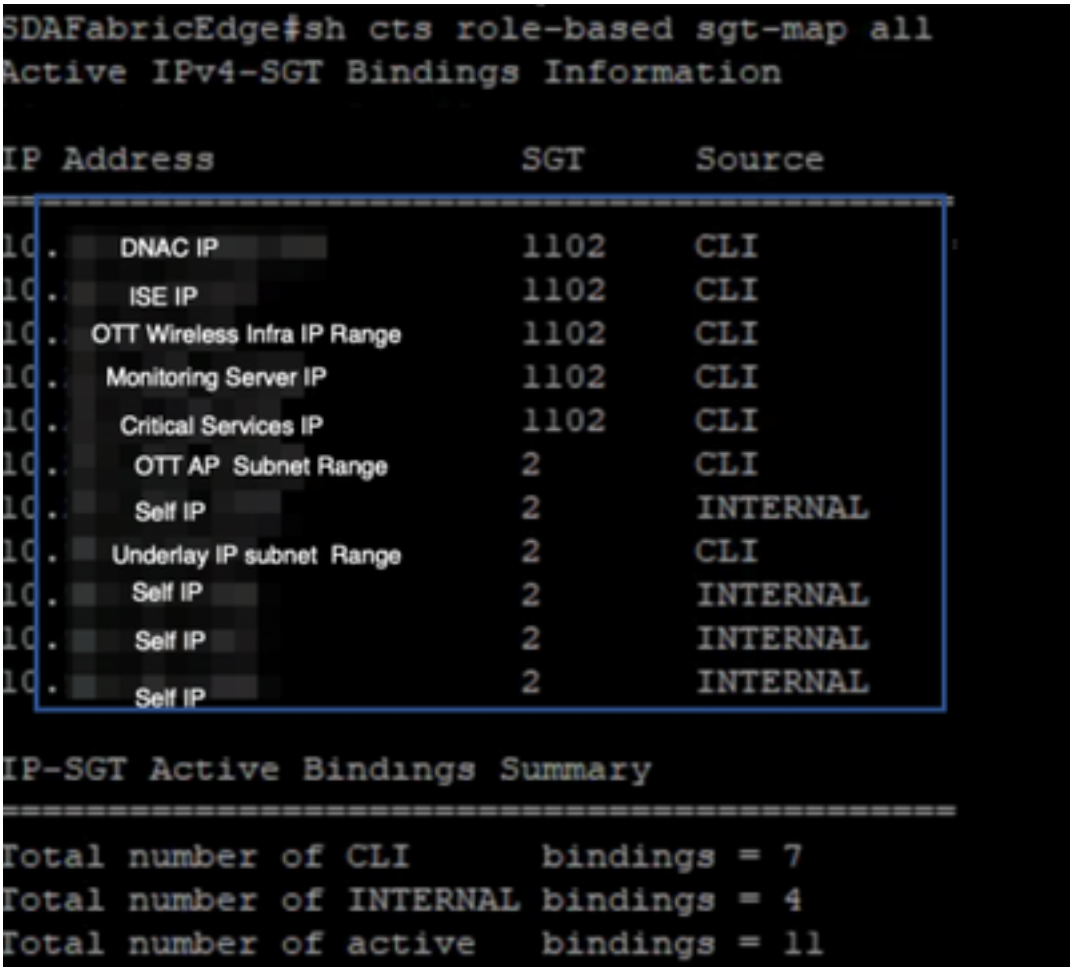
要验证上行链路接口上的实施，请运行以下命令：

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



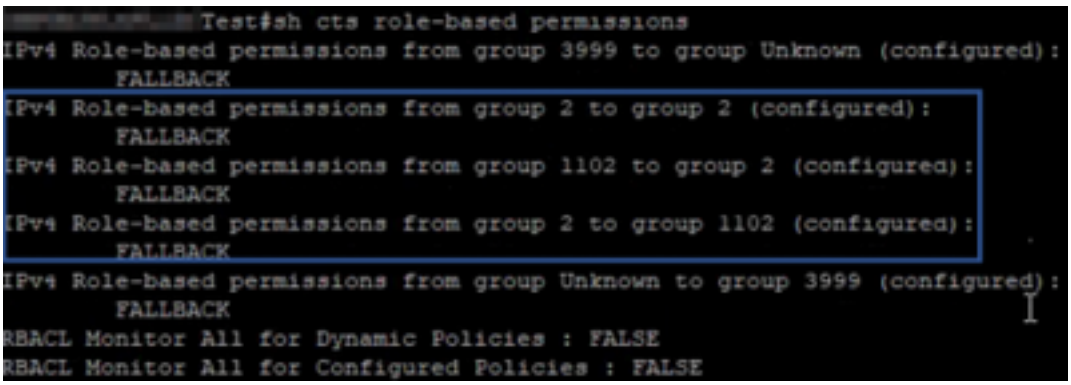
本地IP-SGT映射

要验证本地配置的IP-SGT映射，请运行以下命令：**sh cts role-based sgt-map all**



本地回退SGACL

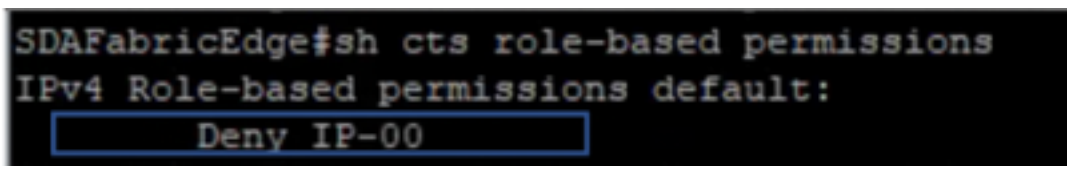
要验证FALLBACK SGACL，请运行以下命令：**sh cts role-based permission**



注意：ISE推送的SGACL比本地SGACL具有优先级。

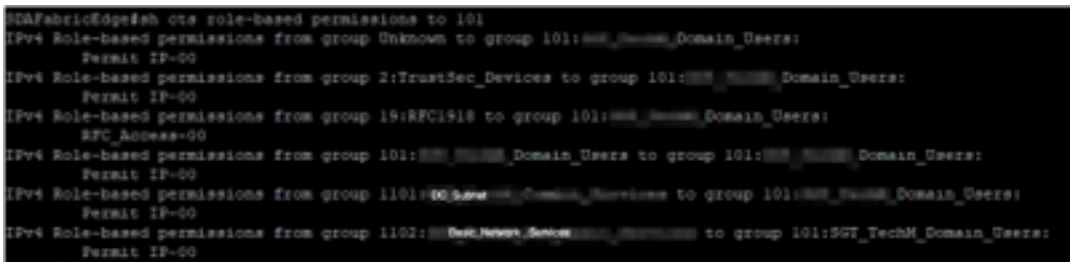
交换矩阵交换机上的允许列表（默认拒绝）启用

要验证允许列表（默认拒绝）模型，请运行以下命令：**sh cts role-based permission**



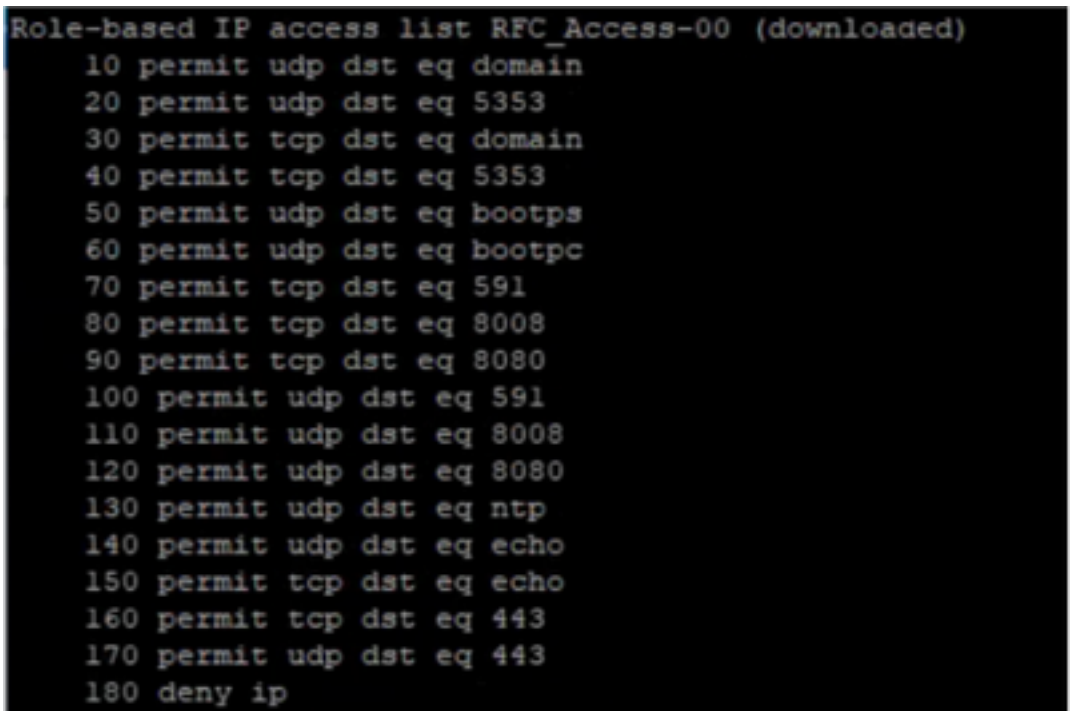
连接到交换矩阵的终端的SGACL

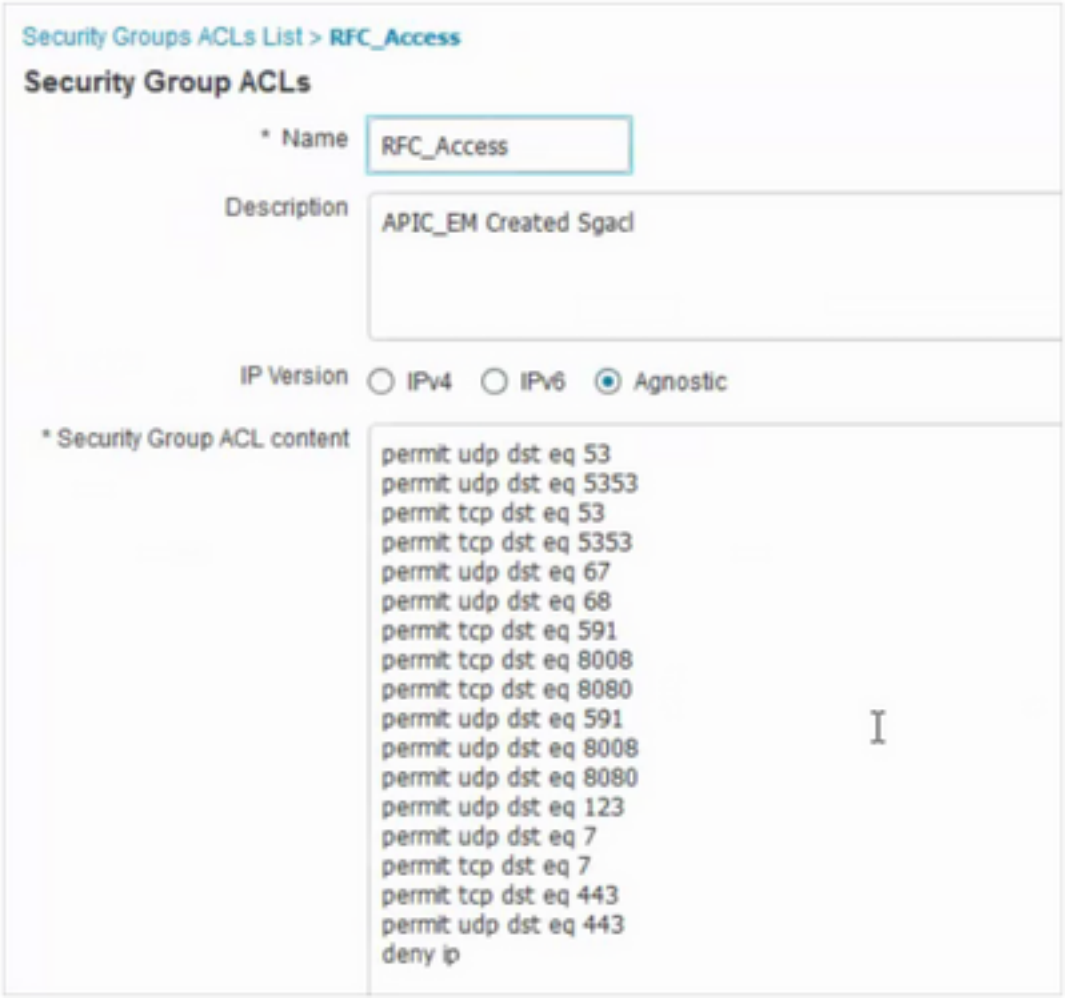
要验证从ISE下载的SGACL，请运行以下命令：**sh cts role-based permission**



验证DNAC创建的合同

要验证从ISE下载的SGACL，请运行以下命令：**show access-list <ACL/Contract Name>**





交换矩阵交换机上的底层SGACL计数器

要验证SGACL策略命中，请运行以下命令：**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
```

故障排除

问题1.在两个ISE节点都关闭的情况下。

如果两个ISE节点都关闭，ISE接收的IP到SGT映射将被删除，所有DGT都标记为未知，并且存在的所有用户会话在5-6分钟后停止。

> **注意：**仅当sgt(xxxx)->未知(0)SGACL访问限于DHCP、DNS和Web代理端口时，此问题才适用。

解决方案：

1. 创建SGT(例如RFC1918)。
2. 将RFC私有IP范围推送到两个边界。
3. 限制从sgt(xxxx)—> RFC1918访问DHCP、DNS和Web代理
4. 创建/修改sgacl sgt(xxxx)—>未知，带允许IP合同。

现在，如果两个ise节点都关闭，SGACL sgt—>未知命中，且存在的会话完好无损。

问题2. IP电话单向语音或无语音。

SIP上发生了IP转换扩展，IP到IP之间的RTP上发生了实际语音通信。CUCM和语音网关已添加到DGT_Voice。

解决方案：

1. 允许来自IP_Phone —> IP_Phone的流量，可以启用相同位置或东西语音通信。
2. DGT RFC1918中的允许RTP协议范围允许该位置的其余部分。IP_Phone —> Unknown允许相同的范围。

问题3.关键VLAN终端无网络访问。

DNAC为交换机调配关键VLAN以用于数据，根据配置，在ISE中断期间的所有新连接都将获得关键VLAN和SGT 3999。Default Deny in trustsec策略限制新连接访问任何网络资源。

解决方案：

使用DNAC模板在所有边缘和边界交换机上推送关键SGT的SGACL

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

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

这些命令将添加到配置部分。

注意：所有命令都可组合到一个模板中，并可在调配期间推送。

问题4.数据包丢入关键VLAN。

由于ISE节点关闭，计算机进入关键VLAN后，每3-4分钟（观察到最多10个丢包）就会出现数据包丢包，用于关键VLAN中的所有终端。

观察结果:当服务器为DEAD时，身份验证计数器增加。当服务器标记为DEAD时，客户端尝试使用PSN进行身份验证。

解决方案/解决方法：

理想情况下，如果ISE PSN节点关闭，则不应从终端发出任何身份验证请求。

在RADIUS服务器下使用DNAC推送此命令：

automate-tester username auto-test probe-on

在交换机中使用此命令，它会定期向RADIUS服务器发送测试身份验证消息。它从服务器查找RADIUS响应。无需成功消息 — 身份验证失败就足以了，因为它表明服务器处于活动状态。

其他信息

DNAC最终模板：

```
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
```

注意：边缘节点中的所有上行链路接口都配置为不实施，并且假设上行链路仅连接到边界节点。在边界节点上，需要配置通往边缘节点的上行链路接口，而无需实施，这必须手动完成。