Modèle de liste verte Cisco ISE TrustSec (IP par défaut refusée) avec SDA

Contenu

Introduction

Ce document décrit comment activer le modèle allow-list (Default Deny IP) de TrustSec dans SDA (Software Defined Access). Ce document fait appel à plusieurs technologies et composants, notamment Identity Services Engine (ISE), Digital Network Architecture Center (DNAC) et Switches (Border and Edge).

Deux modèles Trustsec sont disponibles :

- Modèle de liste de refus (IP d'autorisation par défaut) : Dans ce modèle, l'action par défaut est Permit IP et toute restriction doit être explicitement configurée avec l'utilisation de listes d'accès de groupe de sécurité (SGACL). Ceci est généralement utilisé lorsque vous ne comprenez pas parfaitement les flux de trafic au sein de leur réseau. Ce modèle est assez facile à mettre en oeuvre.
- Modèle de liste verte (IP de refus par défaut) : Dans ce modèle, l'action par défaut est Deny IP et, par conséquent, le trafic requis doit être explicitement autorisé avec l'utilisation des SGACL. Ceci est généralement utilisé lorsque le client comprend bien le type de flux de trafic dans son réseau. Ce modèle nécessite une étude détaillée du trafic du plan de contrôle, ainsi qu'il peut bloquer TOUT le trafic, dès qu'il est activé.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Authentification Dot1x/MAB
- Cisco TrustSec (CTS)
- Protocole d'échange de sécurité (SXP)
- Proxy Web
- Concepts de pare-feu
- DNAC

Components Used

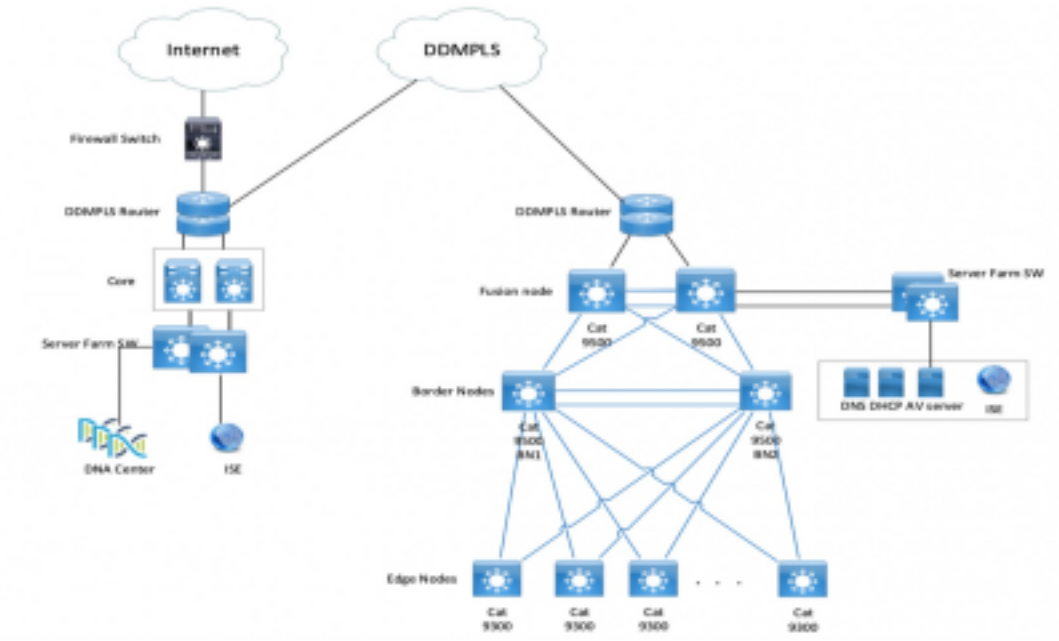
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Noeuds de périphérie 9300 et 9500 avec IOS 16.9.3
- DNAC 1.3.0.5
- ISE 2.6 patch 3 (deux noeuds - Déploiement redondant)
- DNAC et ISE sont intégrés
- Les noeuds de périphérie et de périphérie sont provisionnés par DNAC
- Le tunnel SXP est établi de ISE (haut-parleur) aux deux noeuds de périphérie (écouteur)
- Les pools d’adresses IP sont ajoutés à l’intégration de l’hôte

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.

Configuration

Diagramme du réseau



Configuration

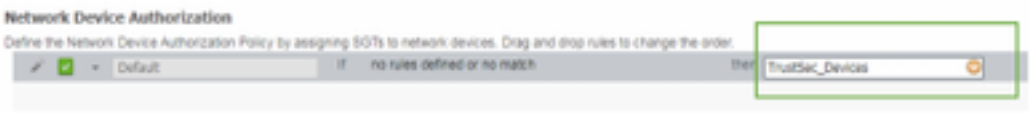
Voici les étapes à suivre pour activer le modèle Allow-List (IP par défaut refusée) :

1. Modifiez la SGT des commutateurs inconnus en périphériques TrustSec.
2. Désactivez l'application basée sur les rôles CTS.
3. Mappage IP-SGT sur les commutateurs en périphérie et en périphérie à l'aide du modèle DNAC.
4. Basculement SGACL à l'aide du modèle DNAC.
5. Enable Allow-List (Default Deny IP) dans la matrice trustsec.
6. Créer SGT pour les terminaux/utilisateurs.
7. Créer une SGACL pour les terminaux/utilisateurs (pour le trafic de superposition de production).

Étape 1. Modifiez la SGT des commutateurs inconnus en périphériques TrustSec.

Par défaut, le Security Group Tag (SGT) inconnu est configuré pour l'autorisation des périphériques réseau. Le passage à TrustSec Device SGT offre plus de visibilité et aide à créer des SGACL spécifiques au trafic initié par le commutateur.

Naviguez jusqu'à **Centres de travail > TrustSec > Stratégie Trustsec > Autorisation de périphérique réseau**, puis changez-le en Trustsec_Devices from Unknown



Étape 2. Désactivez l'application basée sur les rôles CTS.

- Une fois le modèle Allow-List (Deny par défaut) en place, tout le trafic est bloqué dans le fabric, y compris le trafic de diffusion et de multidiffusion sous-jacent, tel que le trafic IS-IS (Intermediate System-to-Intermediate System), BFD (Bidirectional Forwarding Detection),

Secure Shell (SSH).

- Tous les ports TenGig se connectant à la périphérie du fabric ainsi qu'à la bordure doivent être configurés avec la commande ici. Une fois que ceci est en place, le trafic initié à partir de cette interface et qui vient à cette interface ne sont pas soumis à l'application.

```
Interface tengigabitethernet 1/0/1

no cts role-based enforcement
```

> **Note**: Cela peut être fait avec l'utilisation d'un modèle de plage dans DNAC pour plus de simplicité. Sinon, pour chaque commutateur, il est nécessaire de le faire manuellement lors du provisionnement. L'extrait ci-dessous montre comment le faire via un modèle DNAC.

```
interface range $uplink1

no cts role-based enforcement
```

Pour plus d'informations sur les modèles DNAC, *reportez-vous à* cette URL pour le 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

Étape 3. Mappage IP-SGT sur les commutateurs en périphérie et en périphérie avec modèle DNAC.

L'idée est que le mappage IP-SGT local soit disponible sur les commutateurs même si tout ISE tombe en panne. Cela garantit que la sous-couche est opérationnelle et que la connectivité aux ressources critiques est intacte

La première étape consiste à lier les services critiques à une SGT (ex - Basic_Network_Services/1000). Certains de ces services incluent :

- Sous-réseau/ISIS
- ISE/DNAC
- Outil de surveillance
- Sous-réseau du point d'accès en cas d'OTT
- Serveur Terminal Server
- Services critiques - Ex : Téléphone IP

Exemple :

```
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
```

Étape 4. Basculement SGACL avec modèle DNAC.

Un mappage SGT n'est d'aucune utilité tant qu'une SGACL appropriée n'est pas créée à l'aide de la SGT. Par conséquent, notre prochaine étape consisterait à créer une SGACL qui agit en tant que secours local en cas de panne des noeuds ISE (lorsque les services ISE sont hors service, que le tunnel SXP est hors service et donc que les SGACL et le mappage IP SGT ne sont pas téléchargés dynamiquement).

Cette configuration est transmise à tous les noeuds Edge et border.

Liste de contrôle d'accès/contrat basé sur les rôles de secours :

```
ip access-list role-based FALLBACK

permit ip
```

Périphériques TrustSec à Périphériques TrustSec :

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

Au-dessus de la SGACL Garantir la communication au sein des commutateurs de fabric et des adresses IP de sous-couche

Périphériques TrustSec à SGT 1000 :

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

Au-dessus de SGACL Assurez la communication des commutateurs et des points d'accès à ISE, DNAC, WLC et outils de surveillance

SGT 1000 vers périphériques TrustSec :

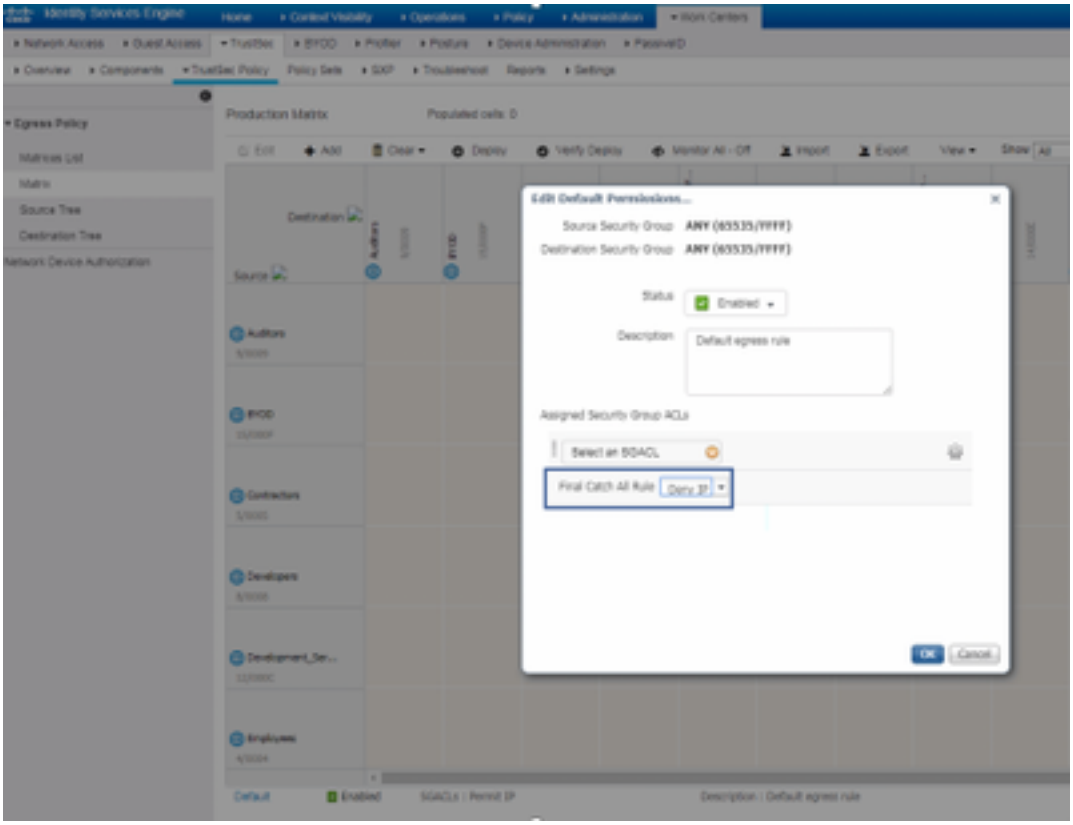
```
cts role-based permissions from 1000 to 2 FALLBACK
```

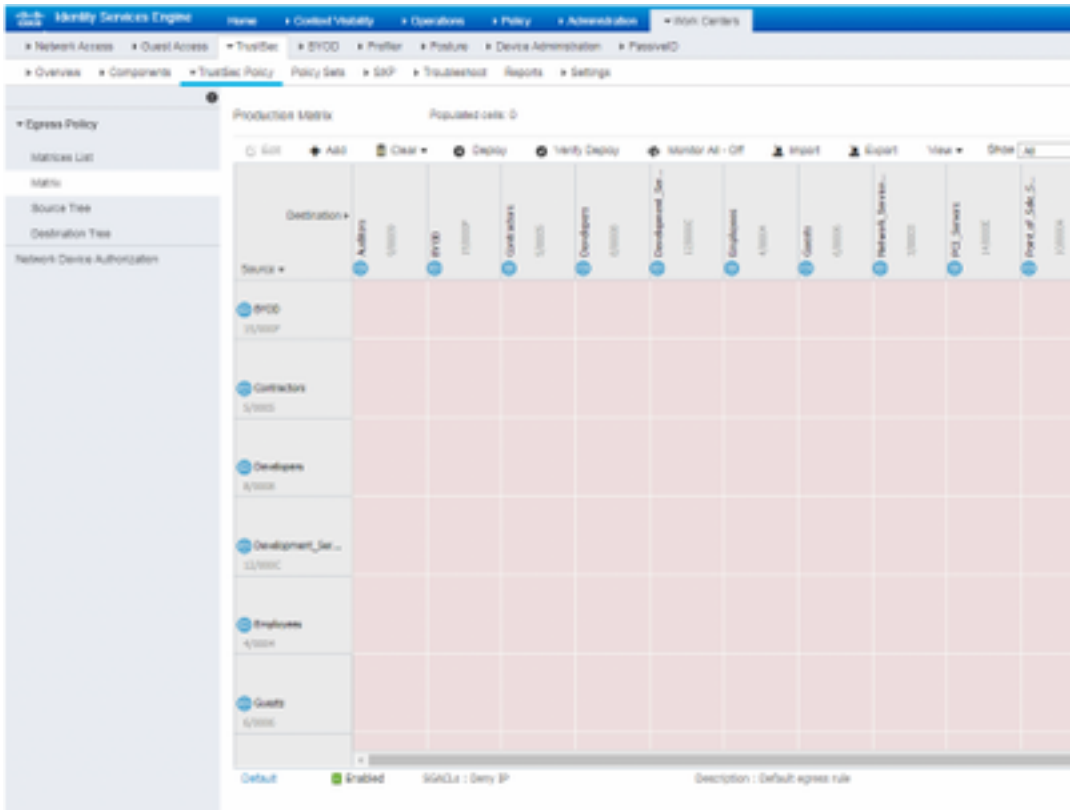
Au-dessus de SGACL Assurez la communication des points d'accès à ISE, DNAC, WLC et outils de surveillance aux commutateurs

Étape 5. Activer le modèle Allow-List (Refus par défaut) dans la matrice TrustSec.

La condition est de refuser la plupart du trafic sur le réseau et d'autoriser une moindre mesure. Ensuite, moins de stratégies sont nécessaires si vous utilisez le refus par défaut avec des règles d'autorisation explicites.

Accédez à **Centres de travail > Trustsec > Stratégie TrustSec > Matrice > Par défaut** et changez-le en **Refuser tout** dans la règle de capture finale.





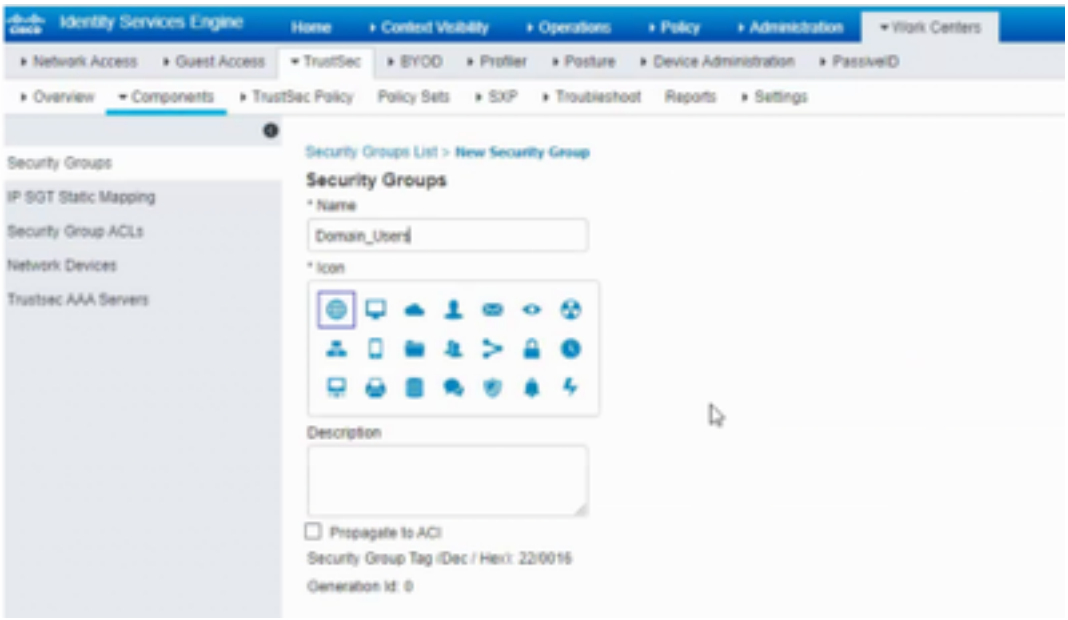
Note: Cette image représente (toutes les colonnes sont en rouge par défaut), le refus par défaut a été activé et seul le trafic sélectif peut être autorisé après la création de la SGACL.

Étape 6. Créer SGT pour les terminaux/utilisateurs.

Dans l'environnement SDA, de nouvelles balises SGT ne doivent être créées qu'à partir de l'interface graphique DNAC, car il existe de nombreux cas de corruption de base de données en

raison d'une non-correspondance de la base de données SGT dans ISE/DNAC.

Afin de créer SGT, connectez-vous à **DNAC > Policy > Group-Based Access Control > Scalable Groups > Add Groups**, a Page Redirige vers **ISE Scalable Group**, cliquez sur **Add,** saisissez le nom SGT et enregistrez-le.



La même SGT se reflète dans DNAC via l'intégration PxGrid. Il s'agit de la même procédure pour toute création future de balises de groupe de sécurité.

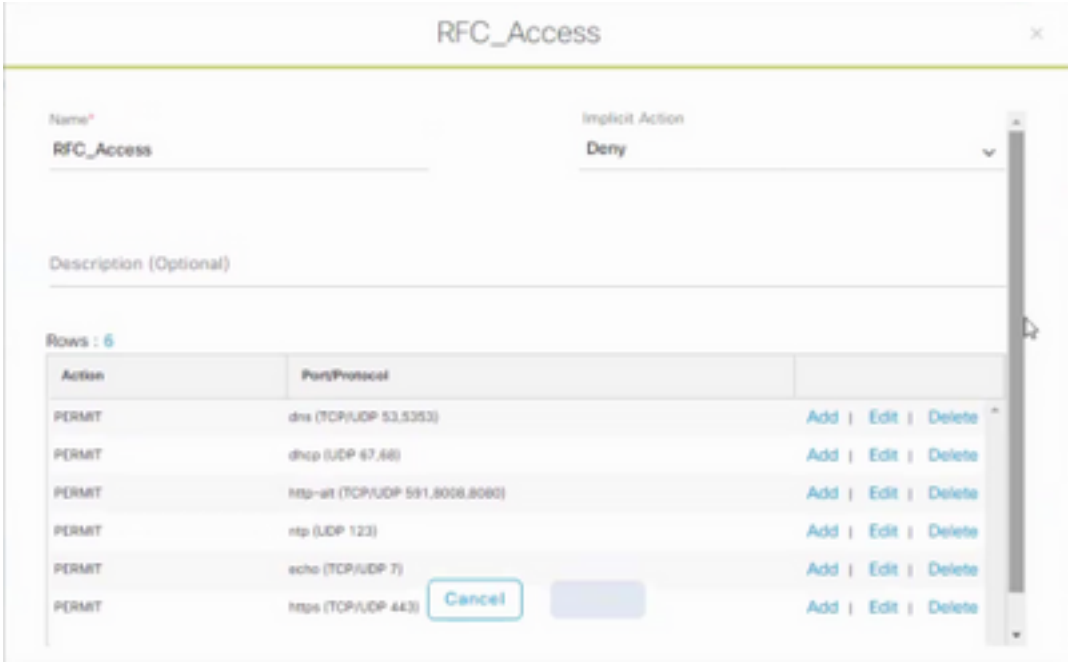
Étape 7. Créer une SGACL pour les terminaux/utilisateurs (pour le trafic de superposition de production).

Dans l'environnement SDA, la nouvelle SGT doit être créée uniquement à partir de l'interface utilisateur DNAC.

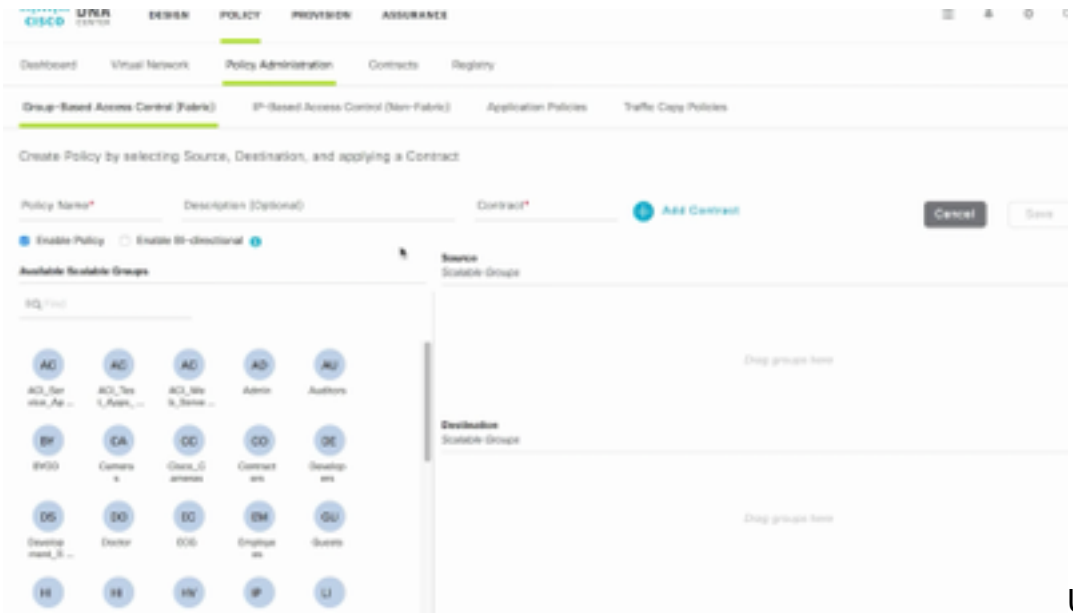
```
Policy Name: Domain_Users_Access

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)
```

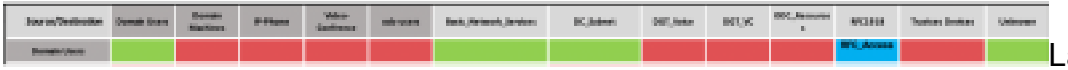
Afin de créer un **contrat**, connectez-vous à **DNAC** et naviguez jusqu'à **Policy > Contracts > Add Contracts > Add Required protocol** et cliquez sur **Save**.



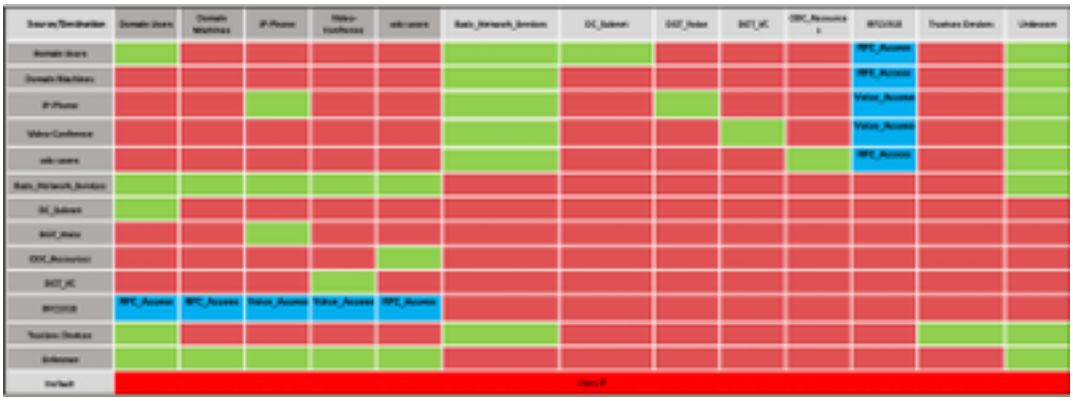
Afin de créer un contrat, connectez-vous à **DNAC** et naviguez jusqu'à **Policy > Group-Based Access Control > Group-Based Access-Policies > Add Policies > Create policy (avec les informations fournies)** maintenant cliquez sur **Save** et ensuite sur **Deploy**.

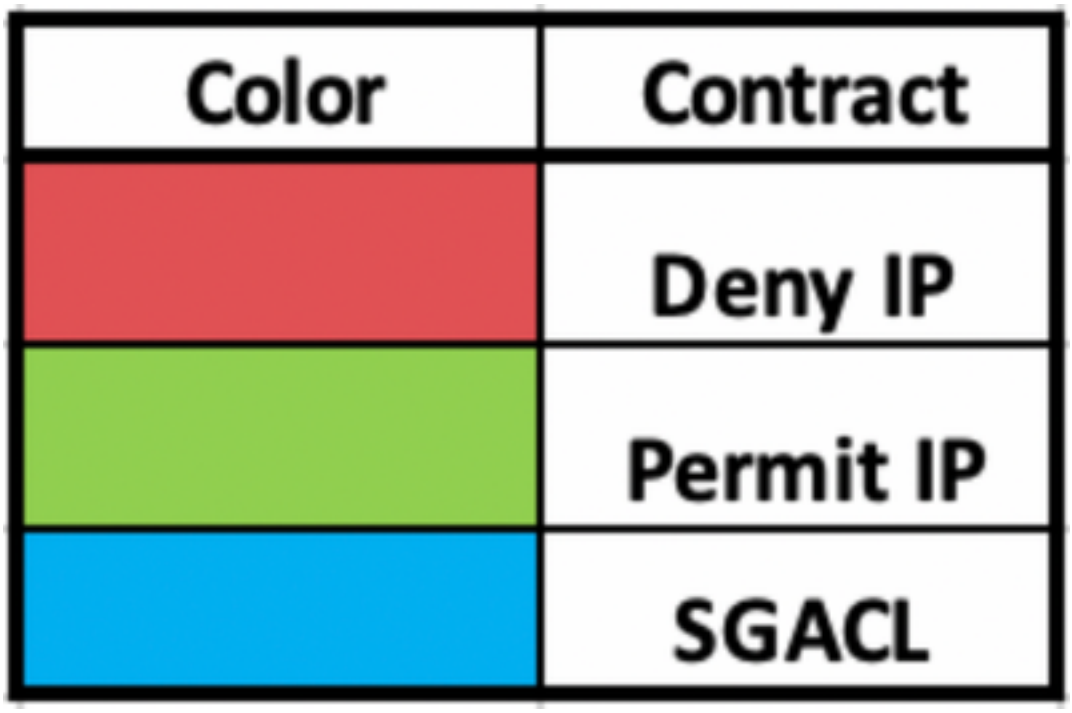


Une fois que SGACL/Contract est configuré à partir de DNAC, il se reflète automatiquement dans ISE. voici un exemple de vue matrx unidirectionnelle pour un sgt.



La matrice SGACL, comme l'illustre l'image ci-dessous, est un exemple de vue pour le modèle Allow-list (Default Deny).





Vérification

SGT de périphérique réseau

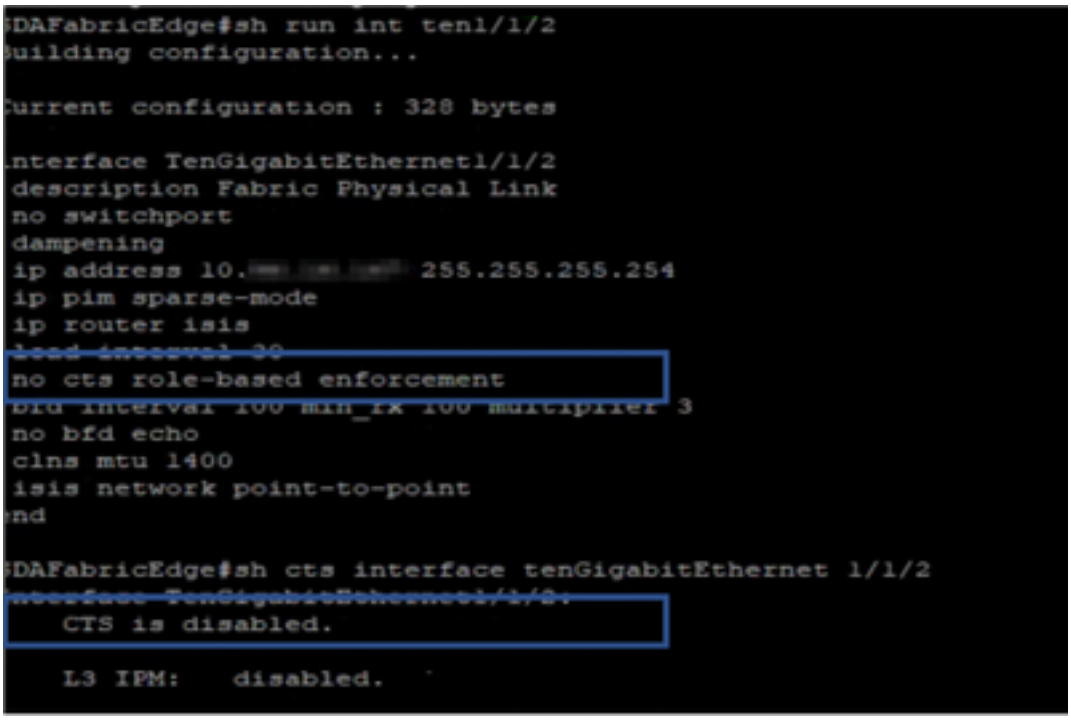
Afin de vérifier les commutateurs SGT reçus par ISE, exécutez cette commande : **show cts environment-data**

```
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
```

Application sur les ports de liaison ascendante

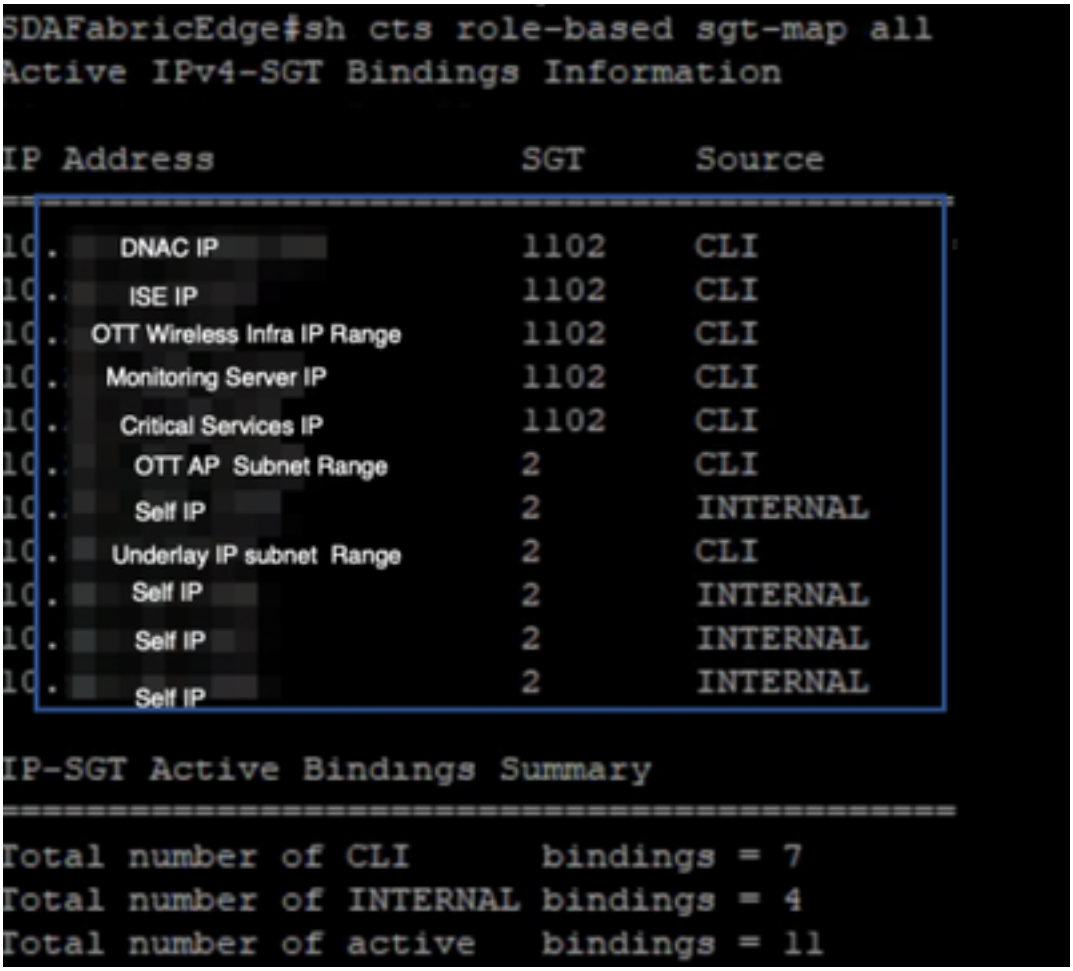
Afin de vérifier l'application sur l'interface de liaison ascendante, exécutez les commandes suivantes :

- **show run interface <liaison montante>**
- **show cts interface <interface de liaison ascendante>**



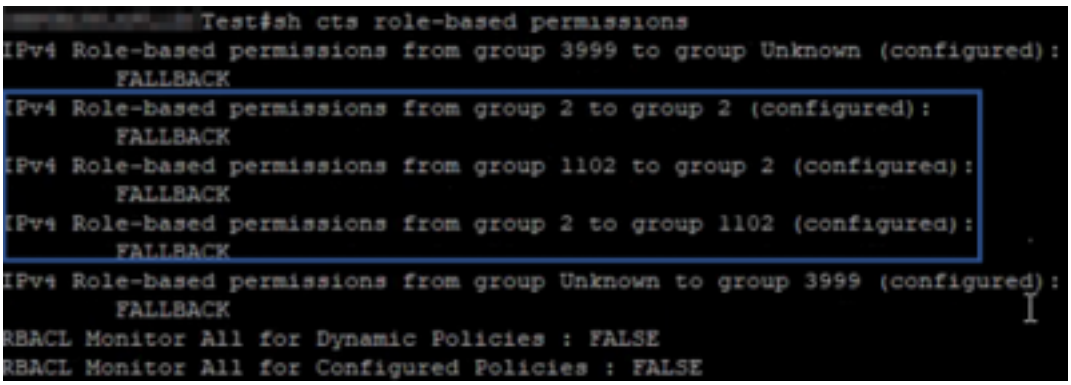
Mappage IP-SGT local

Afin de vérifier les mappages IP-SGT configurés localement, exécutez cette commande : **sh cts role-based sgt-map all**



SGACL FALLBACK local

Afin de vérifier FALLBACK SGACL, exécutez cette commande : **sh cts role-based permission**



Note: La SGACL poussée par ISE a une priorité sur la SGACL locale.

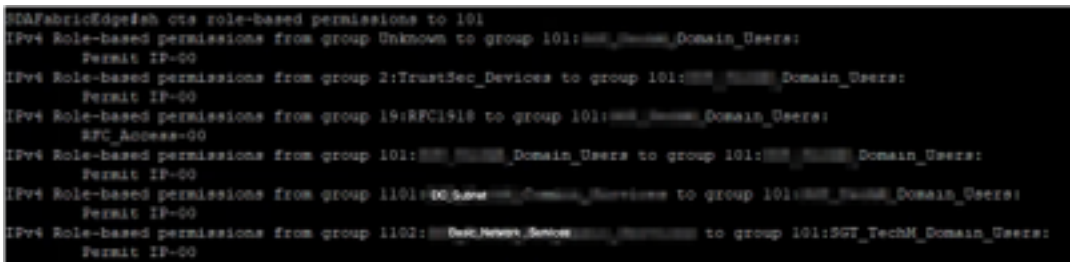
Activation Allow-List (Deny par défaut) sur les commutateurs de fabric

Afin de vérifier le modèle Allow-list (Default Deny), exécutez cette commande : **sh cts role-based permission**

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

SGACL pour les terminaux connectés au fabric

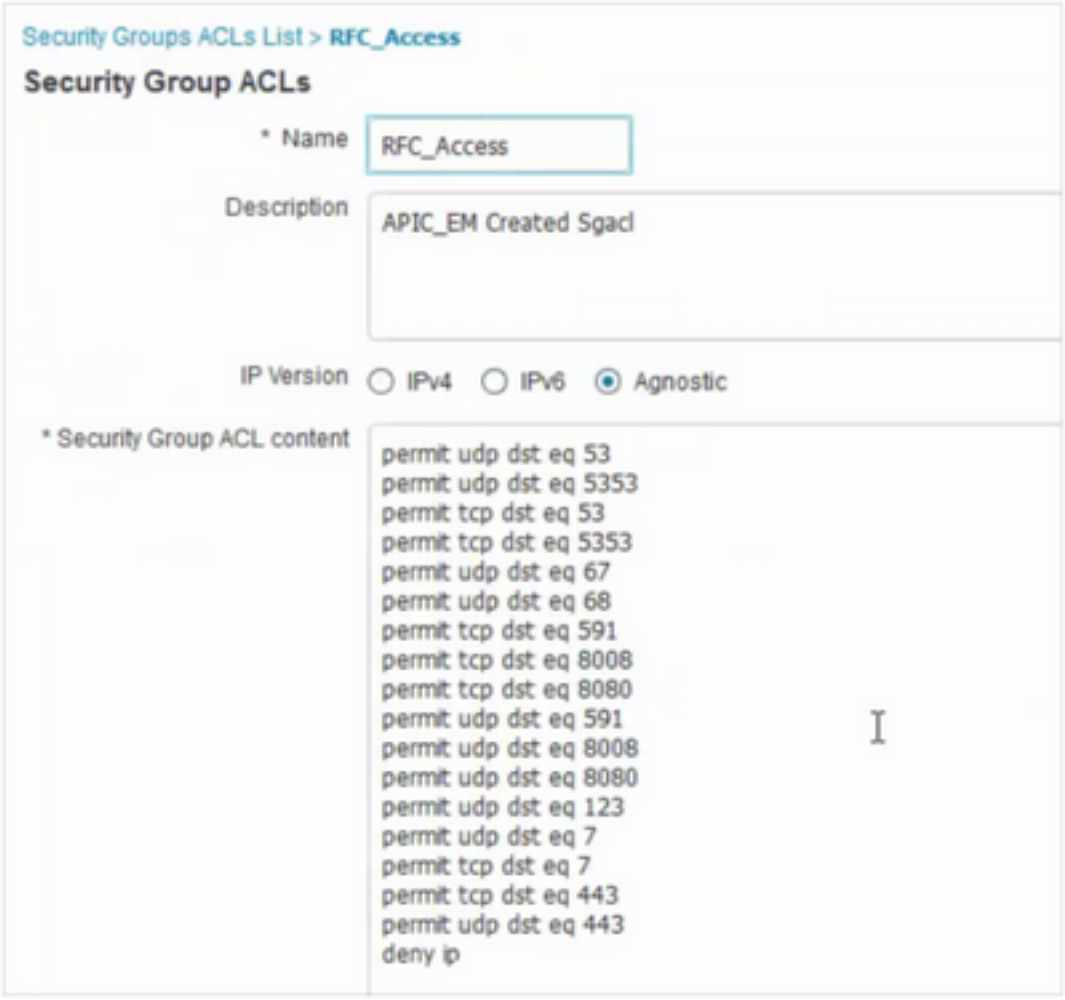
Afin de vérifier la SGACL téléchargée depuis ISE, exécutez cette commande : **sh cts role-based permission**



Vérifier le contrat créé par DNAC

Afin de vérifier la SGACL téléchargée depuis ISE, exécutez cette commande : **show 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
```



Compteur SGACL sous-jacent sur les commutateurs de fabric

Afin de vérifier les accès aux stratégies SGACL, exécutez cette commande : **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
```

Dépannage

Problème 1. Si les deux noeuds ISE sont hors service.

Si les deux noeuds ISE sont désactivés, le mappage IP/SGT reçu par ISE est supprimé et tous les DGT sont marqués comme inconnus, et toutes les sessions utilisateur qui existent s'arrêtent après 5 à 6 minutes.

> **Note**: Ce problème ne s'applique que si sgt (xxxx) -> inconnu (0) l'accès SGACL est limité au port DHCP, DNS et proxy Web.

Solution :

1. Création d'une SGT (ex. RFC1918).
2. Poussez la plage d'adresses IP privées RFC sur les deux bords.
3. Limiter l'accès au serveur DHCP, DNS et proxy Web à partir de sgt (xxxx) —> RFC1918
4. Créer/modifier sgacl sgt (xxxx) —> inconnu avec le contrat Permit IP.

Maintenant, si les deux noeuds ise tombent en panne, sgt—>accès inconnu SGACL et la session qui existe sont intacts.

Problème 2. Voix unidirectionnelle sur téléphone IP ou pas de voix.

L'extension à la conversion IP s'est produite sur SIP et la communication vocale réelle s'est produite sur RTP entre IP et IP. CUCM et la passerelle vocale ont été ajoutés à **DGT_Voice**.

Solution :

1. Le même emplacement ou la communication vocale est-ouest peut être activé en autorisant le trafic à partir d'IP_Phone —> IP_Phone.
2. Le reste de l'emplacement peut être autorisé par la plage de protocoles Permitting RTP dans DGT RFC1918. La même plage peut être autorisée pour IP_Phone —> Inconnu.

Problème 3. Le point de terminaison VLAN critique n'a pas d'accès au réseau.

DNAC provisionne le commutateur avec le VLAN critique pour les données et, selon la configuration, toutes les nouvelles connexions pendant la panne ISE obtiennent le VLAN critique et SGT 3999. La stratégie Refuser par défaut dans trustsec limite la nouvelle connexion à accéder à toutes les ressources réseau.

Solution :

Push SGACL for Critical SGT sur tous les commutateurs Edge et Border à l'aide du modèle DNAC

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

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

Ces commandes sont ajoutées à la section de configuration.

> **Note**: Toutes les commandes peuvent être combinées en un seul modèle et peuvent être poussées pendant le provisionnement.

Problème 4. VLAN critique de la liste déroulante de paquets.

Une fois que la machine est dans le VLAN critique en raison de noeuds ISE en panne, il y a une perte de paquet toutes les 3 à 4 minutes (10 pertes max. observées) pour tous les points d'extrémité du VLAN critique.

Observations : Compteurs d'authentification en augmentation lorsque les serveurs sont DEAD. Les clients tentent de s'authentifier auprès de PSN lorsque les serveurs sont marqués comme DEAD.

Solution/Solution :

Idéalement, il ne devrait pas y avoir de demande d'authentification d'un point de terminaison si les noeuds PSN ISE sont hors service.

Poussez cette commande dans radius server avec DNAC :

automate-testeur username auto-test probe-on

Avec cette commande dans le commutateur, il envoie des messages d'authentification de test périodiques au serveur RADIUS. Il recherche une réponse RADIUS à partir du serveur. Un message de réussite n'est pas nécessaire : une authentification échouée suffit car elle indique que le serveur est actif.

Additional Information

Modèle final 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: Toutes les interfaces de liaison ascendante dans les noeuds de périphérie sont

configurées sans application et on suppose que la liaison ascendante se connecte uniquement au noeud de périphérie. Sur les noeuds de périphérie, les interfaces de liaison ascendante vers les noeuds de périphérie doivent être configurées sans application et cela doit être fait manuellement.