Configurer la stratégie d’autorisation en fonction de l’attribut vlan-id sur ISE

Table des matières

Introduction

Scénario

Étapes de configuration

- côté NAD
- côté ISE

Essai

- côté NAD
- côté ISE

Introduction

Cet article décrit les étapes à suivre pour configurer la politique d'autorisation ISE en fonction de l'attribut d'ID de VLAN envoyé par le NAD. Cette fonctionnalité est uniquement disponible avec IBNS 2.0.

Scénario

Les clients souhaitent renseigner l'ID de VLAN configuré sur l'interface d'accès et l'utiliser ultérieurement pour fournir l'accès sur ISE.

Étapes de configuration

côté NAD

1. Configurez le commutateur pour envoyer les attributs de rayon VLAN dans la demande d’accès.

```
Device# configure terminal
Device(config)# access-session attributes filter-list list TEST
Device(config-com-filter-list)# vlan-id
Device(config-com-filter-list)# exit
Device(config)# access-session accounting attributes filter-spec include list TEST
Device(config)# access-session authentication attributes filter-spec include list TEST
Device(config)# end
```

NOTE: Un avertissement peut s'afficher lorsque vous entrez la commande « access-session accounting attributes filter-spec include list TEST » pour accepter la migration vers IBNS 2.

```
Switch(config)#access-session accounting attributes filter-spec include list TEST
This operation will permanently convert all relevant authentication commands to their CPL control-policy
Do you wish to continue? [yes]:
```

Consultez le guide suivant pour plus de détails : [Vlan-id radius attributes config guide]

côté ISE

1. Créez une stratégie d'authentification en fonction de vos besoins (MAB/DOT1X).

2. La stratégie d'autorisation inclura le type de condition suivant, assurez-vous de correspondre à la syntaxe exacte

```
Radius·Tunnel-Private-Group-ID EQUALS (tag=1)
```

Exemple :

Pour un ID de VLAN = 77



Essai

côté NAD

```
Switch#sh run interface Tw1/0/3
Building configuration...

Current configuration : 336 bytes
!
interface TwoGigabitEthernet1/0/3
 switchport access vlan 77
 switchport mode access
```

```
 device-tracking attach-policy DT_POLICY
 access-session host-mode multi-host
 access-session closed
 access-session port-control auto
 mab
 dot1x pae authenticator
 spanning-tree portfast
 service-policy type control subscriber POLICY_Tw1/0/3
end

Switch#
```

```
Switch#sh auth sess inter Tw1/0/3 details
            Interface:  TwoGigabitEthernet1/0/3
               IIF-ID:  0x1FA6B281
          MAC Address:  c85b.768f.51b4
         IPv6 Address:  Unknown
         IPv4 Address:  10.4.18.167
            User-Name:  C8-5B-76-8F-51-B4
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-host
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  33781F0A00000AE958E57C9D
      Acct Session ID:  0x0000000e
               Handle:  0x43000019
       Current Policy:  POLICY_Tw1/0/3


Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
      Security Policy:  Should Secure

Server Policies:


Method status list:
       Method           State
          mab           Authc Success

Switch#
```

côté ISE

Overview

Event	5200 Authentication succeeded
Username	C8:5B:76:8F:51:B4
Endpoint Id	C8:5B:76:8F:51:B4
Endpoint Profile	Unknown
Authentication Policy	Default >> MAB
Authorization Policy	Default >> Vlan-id test
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2021-11-25 21:06:55.187
Received Timestamp	2021-11-25 21:06:55.187
Policy Server	ise30baaamex
Event	5200 Authentication succeeded
Username	C8:5B:76:8F:51:B4
User Type	Host

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11027	Detected Host Lookup UseCase (Service-Type = Call Check (10)) System Scan
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15041	Evaluating Identity Policy
15048	Queried PIP - Normalised Radius.RadiusFlowType
15013	Selected Identity Source - Internal Endpoints
24209	Looking up Endpoint in Internal Endpoints IDStore - C8:5B:76:8F:51:B4
24211	Found Endpoint in Internal Endpoints IDStore
22037	Authentication Passed
24715	ISE has not confirmed locally previous successful machine authentication for user in Active Directory
15036	Evaluating Authorization Policy
15048	Queried PIP - Radius.Tunnel-Private-Group-ID
15016	Selected Authorization Profile - PermitAccess
24209	Looking up Endpoint in Internal Endpoints IDStore - C8:5B:76:8F:51:B4
24211	Found Endpoint in Internal Endpoints IDStore
11002	Returned RADIUS Access-Accept

CiscoAVPair	cts-pac-opaque=****, service-type=Call Check, audit-session-id=33781F0A00000AEA58E88DB4, method=mab, client-iif-id=491113166, vlan-id=77

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.