

CHAPITRE 4 :

DEPLOIEMENT DE LA PLATE-FORME CISCO ISE

Après avoir achevé les notions théoriques, nous passons à la mise en place de notre solution, laquelle représente notre tâche principale.

Le déploiement se fera en trois phases :

- La préparation des Switches d'accès qui consiste à configurer et activer tous les services et fonctionnalités nécessaires au déploiement de la solution ISE.
- La mise en place de la solution ISE qui consiste à configurer et activer les services d'authentification, d'autorisation, de profiling, de provisionning et de posture sur tous les serveurs ISE
- Le déploiement chez les clients qui consiste à activer sur les interfaces des Switches d'accès toutes les fonctionnalités pour la mise en production de la solution ISE

I. PRESENTATION DE LA SOLUTION ISE DEPLOYEE A MTN-CI

1. Les équipements networks

Pour l'implémentation de la solution ISE, les équipements principalement concernés :

- Un commutateur (Switch Catalyst 2960 pour la plupart)
- Un point d'accès Les machines virtuelles requises serviront à installer :
- Un contrôleur de domaine
- La plate-forme Cisco ISE
- Un contrôleur 4404 du réseau local sans fil (WLC)
- Les PC
- Les téléphones

2. Architecture du réseau

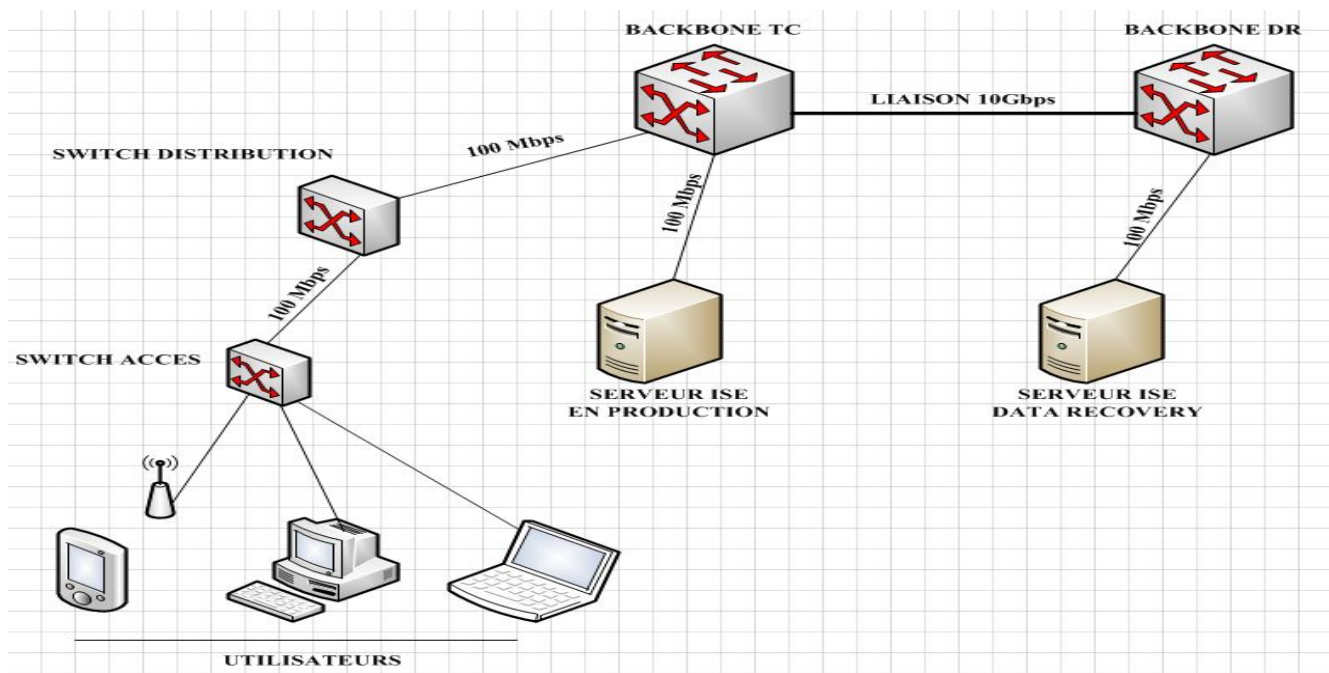


Figure 6 : Architecture du réseau

3. Installation de la plate-forme ISE

L'installation de la plate-forme c'est fait sur deux sites différents :

- Un serveur 3355 Admin/Monitor primaire et un serveur 3315 Policy sur le site de Technology-Center MTN. (nœud primaire)
- un serveur 3355 Admin/Monitor Secondaire et un serveur 3315 Policy sur le site de Data Recovery MTN. (nœud secondaire)

Le nœud peut assurer un ou plusieurs des services suivants :

- Administration : permet de manipuler les configurations systemes reliées aux fonctionnalités telles que l'authentification et l'autorisation

- Le monitoring : fourni les services de journalisation « log » et des outils de depannage « troubleshooting » avancés.
- Services de la politique « policy service » : fourni l'accès au reseau, la validation de posture, l'accès des visiteurs « guest », « client provisionning » et les services de profilage.

Dans un deploiement assurant la haute disponibilité, le nœud administratif primaire est le seul nœud actif, et sur lequel s'effectuent tous les changements. Le nœud secondaire est en etat d'attente « standby » et recoit d'une manniere continu la configuraton du nœud principal.

Par conséquent, il possède toujours une copie complète de la configuration. Au cas où le nœud primaire est devenu hors service, le responsable doit se connecter à l'interface du nœud secondaire et le promouvoir pour pouvoir configurer les règles.

a. Caractéristiques des serveurs utilisés

➤ Le serveur 3355 Admin/Monitor

Les spécifications de ce serveur sont les suivants :

- Un processeur unique : Quad-core Intel Xeon (Nehalem)
- Une mémoire vive de 4Gbits
- 2*300Go HDD SAS, monté en RAID miroir
- Lecteur CD /DVD-ROM
- Quatre ports Ethernet (10, 100 et 1000 Mbps)
- Deux ports Gigabit Ethernet
- Un port serial
- Deux ports VGA
- IOS de version 1.4.0.253
- Patch information : 3,5,6

➤ Le serveur 3315 Policy

- Un processeur unique : Quad-core Intel Xeon (Core 2 Quad)
- Une mémoire vive de 4Gbits
- 2*250Go HDD SATA
- Lecteur CD /DVD-ROM
- Quatre ports Ethernet (10, 100 et 1000 Mbps)
- Deux ports Gigabit Ethernet
- Un port serial
- Un port VGA
- IOS de version 1.4.0.253
- Patch information : 3,5,6

b. L'application ISE

L'administration de l'application ISE se fait via une interface WEB auquel l'on accède grâce à une adresse IP. Logiquement, suite aux différentes configurations effectuées sur les équipements des utilisateurs, avant d'accéder au menu de l'application, il y a la phase d'authentification. La figure suivante montre l'interface d'authentification.

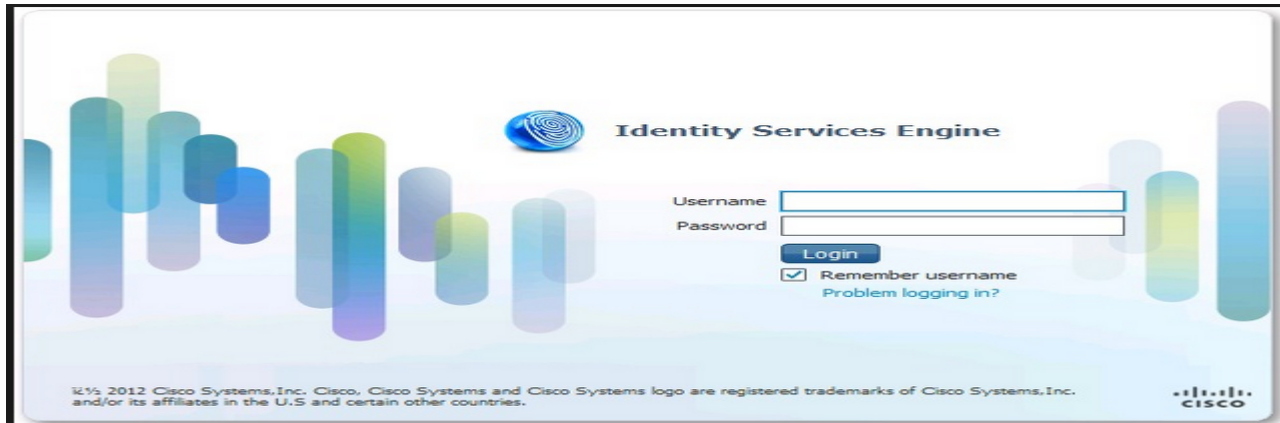


Figure 7 : Interface d'authentification de l'ISE

Après le login nous avons le menu que présente la solution ISE pour l'exploitation complète des ressources qu'elle offre.

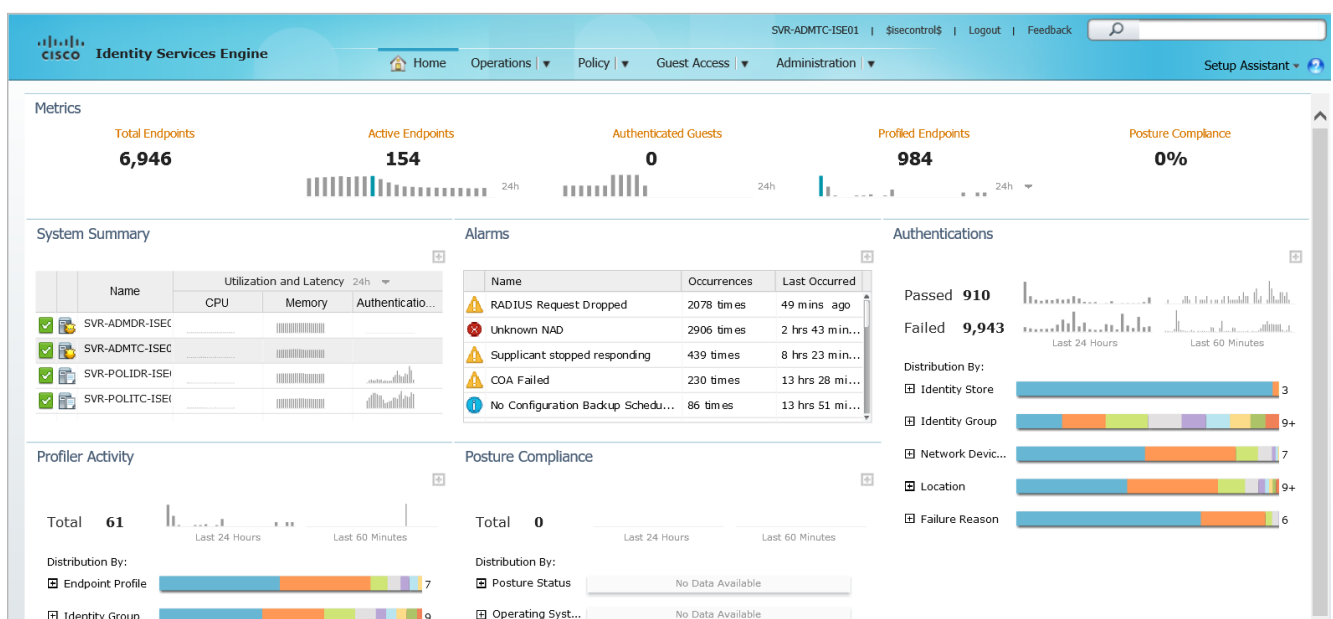


Figure 8 : ISE main page

II. LA CONFIGURATION DE L'ISE

Cette configuration consiste à configurer la redondance pour les serveurs Administrateur et Monitoring. Elle permet la définition des politiques d'authentification, d'autorisation, de provisionning et de profiling. Elle définit aussi les paramètres de création d'utilisateur Invités.

1. Authentification

Les politiques d'authentification à définir au niveau de l'ISE servent à identifier les différents utilisateurs ou machines demandant l'accès au réseau et ce en s'appuyant sur un ensemble de

protocoles tels que Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), Extensible Authentication Protocol (EAP) et Protected Extensible Authentication Protocol (PEAP). Lors de l'ajout de la règle, nous devons choisir les protocoles permis pour une telle méthode d'authentification et la source des identités (Identity Store).

Les sources qui peuvent être utilisées sont les suivantes :

- Utilisateurs internes
- Utilisateurs "Guest" (groupe d'utilisateurs défini sur la plate-forme)
- Terminaux internes
- Active Directory
- Bases de données LDAP
- RADIUS Token Server

Trois méthodes d'authentification sont supportées par l'ISE :

- 802.1X (abordé au cours du chapitre précédent)
- MAC Authentication Bypass (MAB) : certains périphériques tels que l'imprimante réseau et le téléphone IP, ne supportent pas l'authentification 802.1X. dans ce cas, elle pourra être effectuée en se référant à l'adresse MAC.
- L'authentification WEB via un portail captif

Les règles d'authentification qui ont été définies se limitaient aux deux premières méthodes. La première règle permet de vérifier l'existence des adresses MAC des périphériques dans la liste interne. Cette règle sera aussi utile pour la troisième méthode, laquelle est reportée à la phase d'autorisation. La seconde règle sert à authentifier les comptes utilisateurs, en premier lieu à partir du contrôleur Active Directory, puis à partir de la liste interne. En cas d'échec d'authentification pour un utilisateur de domaine, la seconde règle donne la possibilité de tester avec un utilisateur local. Ceci nous permettra de mieux localiser la défaillance ; il pourrait s'agir d'une erreur d'intégration avec Active directory ou d'une erreur au niveau de l'authentification en se référant au domaine.

<input checked="" type="checkbox"/>	MAB	: If	Wired_MAB OR Wireless_MAB	Allow Protocols :	Default Network Access
<input checked="" type="checkbox"/>	Default	: use	Internal Endpoints		
<input checked="" type="checkbox"/>	Dot1X	: If	Wired_802.1X OR Wireless_802.1X	Allow Protocols :	Default Network Access
<input checked="" type="checkbox"/>	Default	: use	Use_AD_then_local		
<input checked="" type="checkbox"/>	Default Rule (If no match)	: Allow Protocols :	Default Network Access	and use :	Use_AD_then_local

Figure 9 : Règle d'authentification

Afin d'autoriser plus qu'une source d'authentification pour une seule règle, il a fallu ajouter une séquence de source d'identité ou « Identity source Sequence » permettant de vérifier les identités en consultant les sources par ordre. La figure suivante montre la séquence définie :

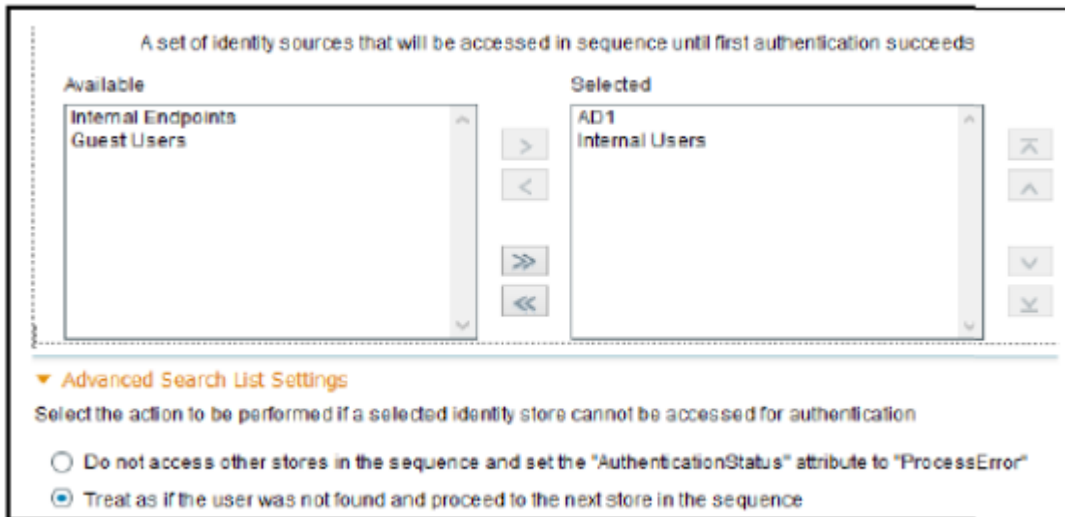


Figure 10 : Définition de la séquence « Use AD then local »

Il est possible de définir des règles avec des conditions simple ou composées. Une condition simple st basée sur un opérande, un opérateur tels que « equal to » et « no equal to » ainsi qu'une valeur. Ces conditions peuvent être définies au niveau de la librairie et appelées directement lors de la définition de la règle pour une meilleure organisation. Une condition composée rassemble deux conditions simples ou plus avec un opérateur OR ou AND. La figure suivante montre le rassemblement de deux conditions existante dans la librairie avec un opérateur OR pour la règle MAB.

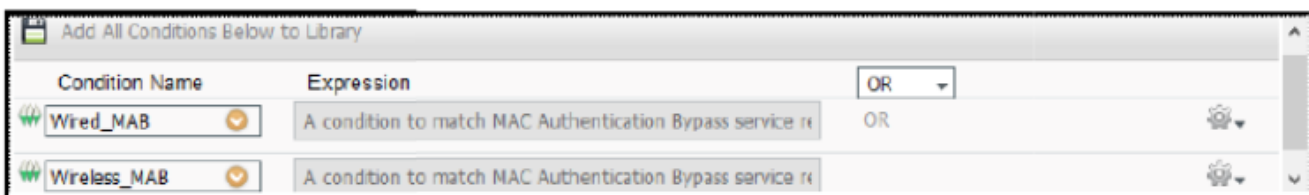


Figure 11 : Condition composée avec la règle MAB

Une fois l'authentification réussie, la session procède à la phase d'autorisation. Des options offertes par l'ISE permettent de vérifier la conformité avec des politiques d'autorisation même en cas d'échec d'authentification. Ces options sont indispensables pour faire fonctionner l'authentification WEB. L'authentification MAB sera considérée comme réussie même si l'adresse MAC de la machine est introuvable. Ceci est réalisable en changeant l'action à « continue » pour l'option « If user not found », comme indiqué sur la figure sui suit.

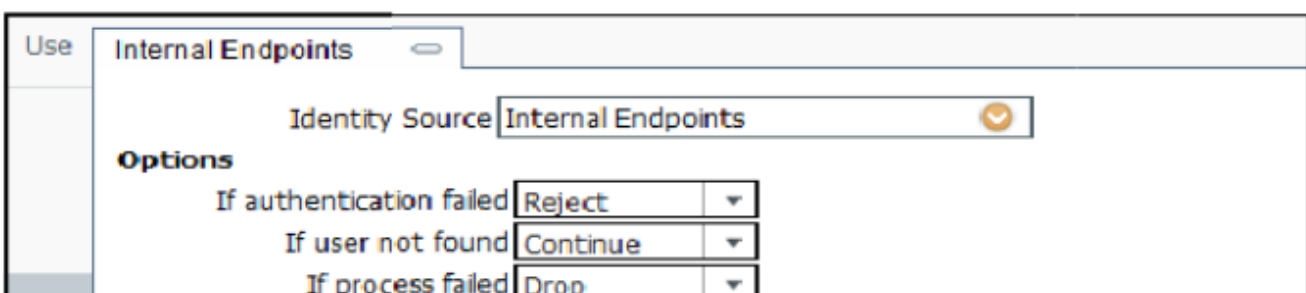
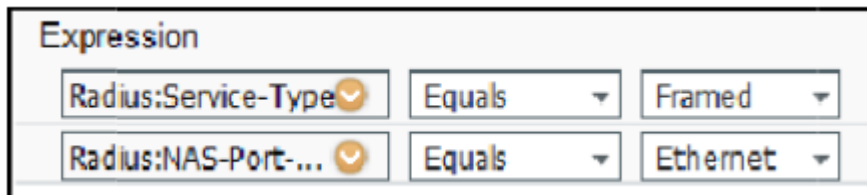


Figure 12 : Succès de l'authentification au cas où l'adresse MAC est introuvable

La définition des règles repose sur les attributs du protocole RADIUS. Les attributs constituent le principe le plus important du protocole RADIUS, aussi bien dans sa version initiale que pour ses extensions. Des champs attributs sont le fondement du protocole. Par conséquent, la bonne compréhension de leur signification et de leur rôle est indispensable pour tirer le meilleur parti de RADIUS. Chaque attribut possède un numéro approprié, auquel est associé un nom. Il existe un grand nombre d'attributs dans le protocole RADIUS, mais peu d'entre eux sont utiles dans le cas qui nous préoccupe ici :

- User-name
- User- password
- NAS-Port
- Service-Type

A titre d'exemple, la condition prédéfinie « Wired_802.1X » affecte les valeurs suivantes aux attributs Service-Type et NAS-Port :



Expression		
Radius:Service-Type	=	Framed
Radius:NAS-Port...	=	Ethernet

Figure 13 : Attributs RADIUS de l'authentification DOT1X sur le réseau filaire

2. Posture et Client provisioning

Les services de posture fournis par CISCO ISE permettent de vérifier la disponibilité des dernières mises à jour au niveau de la machine du client ou l'existence de certaines applications tels que les anti-virus et les anti-spywares. Afin d'évaluer la machine, le client doit disposer de l'un de ces deux agents :

- CISCO NAC WEB AGENT : un agent temporaire que les clients installent lors du login et qui disparaît une fois le login terminé. Il est recommandé pour les utilisateurs ayant un accès pour une période bien déterminé.
- CISCO NAC AGENT : un agent persistant qui, une fois installé, subsiste sur une machine Windows ou Mac pour permettre l'évaluation lors des prochaines connexions. Il est généralement utilisé par les utilisateurs du domaine.

Par ailleurs, ces agents peuvent faciliter la remédiation des machines en affichant un message expliquant la procédure et en fournissant des fichiers à télécharger et installer. La plate-forme ISE donne la possibilité de rediriger les clients vers une page de téléchargement des agents pour ceux qui n'en disposent pas et ce grâce à une option à configurer au niveau du profil d'autorisation. Ce service est appelé "**Client Provisioning**". La figure qui suivra expose les règles de "Client Provisioning" définies : la première fournit l'agent temporaire "Web Agent" aux invités "Guests", alors que la deuxième fournit l'agent persistant aux autres utilisateurs qui sont principalement les membres du domaine. Il est à préciser que l'ordre des règles est primordial pour assurer une bonne affectation. Par exemple, en inversant l'ordre, tous les utilisateurs téléchargeront l'agent persistant et la deuxième règle ne sera jamais appliquée.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
Web Agent for Guests	If Guest	and Windows All	and Condition(s)	then WebAgent 4.9.0.1007
NAC Agent for others	If Any	and Windows All	and Condition(s)	then NACAgent 4.9.0.1009

Figure 14 : Règles du clients provisioning

La liste qui suit présente des versions multiples des deux types d'agents NAC, temporaires et persistants.

Download Remote Resources				
<input type="checkbox"/>	Name	Type	Version	Description
<input type="checkbox"/>	NACAgent 4.9.0.52	NACAgent	4.9.0.52	NAC Windows Agent (ISE 1.1.3 ...
<input type="checkbox"/>	NACAgent 4.9.0.55	NACAgent	4.9.0.55	NAC Windows Agent (ISE 1.1.3 ...
<input type="checkbox"/>	NACAgent 4.9.4.3	NACAgent	4.9.4.3	NAC Windows Agent - ISE 1.2, I...
<input type="checkbox"/>	NACAgent 4.9.5.4	NACAgent	4.9.5.4	NAC Windows Agent - ISE 1.2 a...
<input type="checkbox"/>	NACAgent 4.9.5.7	NACAgent	4.9.5.7	NAC Windows Agent - ISE 1.2 a...
<input type="checkbox"/>	WebAgent 4.9.0.1005	WebAgent	4.9.0.1005	NAC WebAgent (ISE 1.2 release)
<input type="checkbox"/>	WebAgent 4.9.0.1007	WebAgent	4.9.0.1007	NAC WebAgent (ISE 1.2 release...
<input type="checkbox"/>	WebAgent 4.9.0.24	WebAgent	4.9.0.24	NAC WebAgent (ISE 1.1.1 or later)

Figure 15 : Exemple de liste des agents NAC

Après avoir fourni les agents permettant l'évaluation de posture aux clients, nous devons procéder à la phase de définition des règles de posture.

- Une règle s'écrit : Si condition(s) alors exigence
- Aussi, une exigence peut être décomposée comme suit : Si condition(s) alors action de remédiation

Dans une règle d'exigence, une condition simple peut être :

- Un fichier : vérifier l'existence d'un fichier, la date du fichier ainsi que sa version
- Un registre : s'assurer de l'existence d'une clé de registre ou la valeur de la clé
- Une application : vérifier si une application est en train de fonctionner
- Un service : vérifier si un service est en exécution

Nous pouvons aussi former une condition composée à base de conditions simples ou composées. En outre, des conditions composées intégrées avec l'ISE existent : Antivirus et Antispyware. Lors de l'ajout d'une condition d'antivirus et après le choix du système d'exploitation, la liste des vendeurs s'affiche :

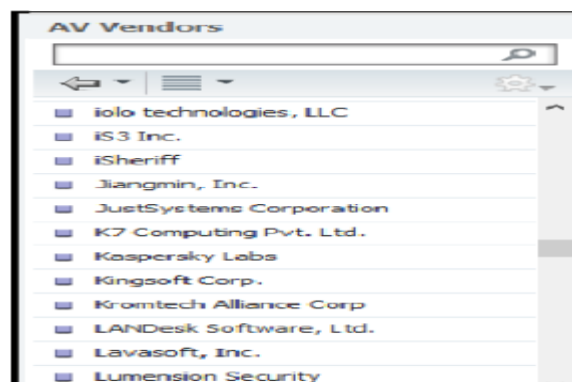
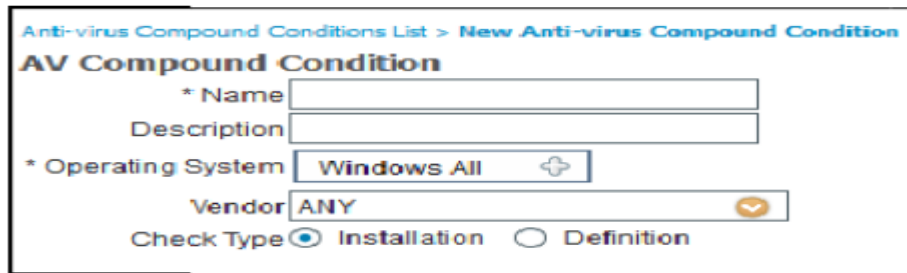


Figure 16 : Liste des vendeurs

Pour une telle condition, CISCO ISE donne la possibilité d'examiner la machine pour vérifier l'existence de l'antivirus ou même la disposition d'une version récente. Ceci est réalisable en analysant le fichier de définition de la version par les Agents NAC. En conséquence, les versions reconnues par l'ISE doivent être mise à jour continuellement.



Anti-virus Compound Conditions List > New Anti-virus Compound Condition

AV Compound Condition

* Name

Description

* Operating System +

Vendor ✓

Check Type ☒ Installation ☐ Definition

Figure 17 : Champs à remplir d'une condition d'antivirus

3. Autorisation

Les politiques d'autorisation à définir mettent en application les politiques d'authentification et de posture ; ces politiques sont déclarées comme étant des conditions. Sur la base de ces conditions, l'utilisateur aura l'autorisation appropriée. Pour résumer, une règle d'autorisation s'écrit :

Si conditions (attributs ou groupes d'utilisateurs) alors permissions (profil d'autorisation).

Dans notre cas, nous avons besoin des attributs d'authentification et de posture ainsi que des groupes d'utilisateurs. Afin de vérifier l'état de la machine par rapport à la règle de posture, nous avons recours à l'attribut "PostureStatus ». Cet attribut peut avoir trois valeurs :

- Unknown : aucune donnée n'a été obtenue pour évaluer la machine ; l'agent NAC n'est pas disponible
- Noncompliant : la machine n'est pas conforme avec une ou plusieurs règles
- Compliant : la machine est conforme avec les règles

Afin de vérifier l'identité de l'utilisateur du domaine, nous avons recours à l'attribut "ExternalGroups" et ce en prenant comme valeur le nom d'un groupe du domaine. Les utilisateurs inscrits sur le portail captif sont affectés directement à un groupe d'utilisateur nommé "Guest", lequel peut être exploité lors de l'ajout de la règle. Avant d'ajouter une règle, nous devons créer le profil d'autorisation associé. Dans un tel profil, nous avons le choix entre plusieurs options telles que l'affectation à un VLAN, la redirection vers un URL (portail d'authentification Web, portail de Client Provisioning, URL externe, etc.), à base d'une liste de contrôle d'accès, et même l'application d'un ACL sur le port du commutateur.

A titre d'exemple, nous avons créé le profil d'autorisation CWA permettant de rediriger les utilisateurs vers le portail captif en se référant à la liste d'accès définie au niveau des WLC et Switch et sur laquelle on s'attardera ultérieurement.

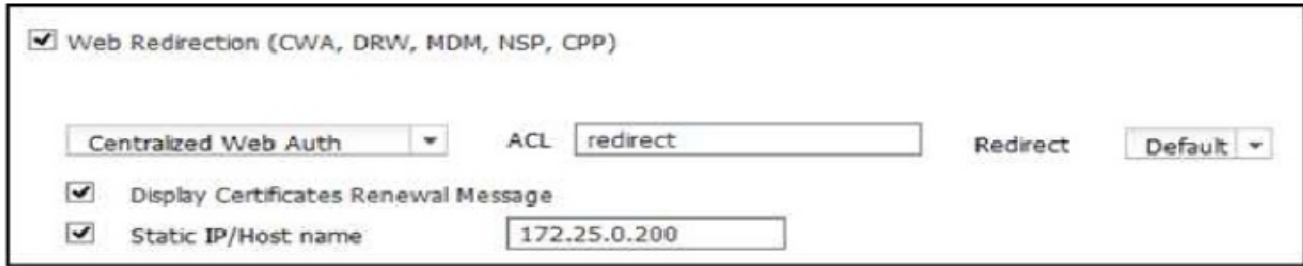


Figure 18 : Profil d'authentification CWA

Après avoir terminé la création des profils, nous pouvons définir les règles. Ces règles autorisent l'accès aux utilisateurs authentifiés au domaine ou via le portail web et ayant des machines conformes aux règles de posture. Un user de domaine ne disposant pas de l'agent NAC ou non conforme avec les politique de posture est redigé vers la page client Provisioning. Sinon, l'user est redigé vers le portail WEB incluant une phase de validation de posture.

Rule Name	Conditions (identity groups and other conditions)	Permissions
Compliant and Domain User	\bar{f} (AD1:ExternalGroups EQUALS NSIT.local/Users/Utilisateurs du domaine AND Session:PostureStatus EQUALS Compliant)	then PermitAccess
Not compliant and Domain User	\bar{f} (AD1:ExternalGroups EQUALS NSIT.local/Users/Utilisateurs du domaine AND Session:PostureStatus NOT_EQUALS Compliant)	then CPP
Guest and Compliant	\bar{f} Guest AND Session:PostureStatus EQUALS Compliant	then PermitAccess
Guest and Not Compliant	\bar{f} Guest AND Session:PostureStatus NOT_EQUALS Compliant	then CWA
Guest Redirection	\bar{f} Network Access:AuthenticationStatus EQUALS UnknownUser	then CWA

Figure 19 : Règle d'authentification de posture

4. Configuration des Switches d'accès et des PC

Le déploiement de la solution chez les clients consiste en l'activation des services pour l'interaction avec le Cisco ISE sur les ports des Switches d'accès configurés ci-dessus. Elle consiste aussi à activer la fonctionnalité DOT1X sur les PC des utilisateurs finaux.

La configuration des interfaces se présente de la façon suivante :

```
Switch-Lab (config) # interface fastethernet 0/1
Switch-Lab (config-if) # authentication host-mode multi-auth
Switch-Lab (config-if) # authentication order mab dot1x
Switch-Lab (config-if) # authentication priority dot1x mab
Switch-Lab (config-if) # mab
Switch-Lab (config-if) # ip access-group ACL-DEFAULT in
Switch-Lab (config-if) # spanning-tree portfast
```

Commandes	Description
Ip access-group ACL-DEFAULT in	Applique l'access-list au port du switch dans la direction inbound
Authentication host-mode multi-auth	Permet plusieurs authentifications sur le même port du switch simultanément
Authentication order mab dot1x	Permet à l'administrateur de sélectionner l'ordre dans lequel les méthodes d'authentification sont exécutées
Authenticaton priority dot1x mab	Détermine la priorité des méthodes d'authentification
mab	Active le MAB sur l'interface
Spanning-tree portfast	Permet au port du switch de directement transiter de l'état Blocking à l'état forwarding du spanning-tree

Configurer une interface du Switch d'accès avec le 802.1X

```
Switch-Lab (config) # interface fastethernet 0/1
Switch-Lab (config-if) # authentication open
Switch-Lab (config-if) # authentication port-control auto
Switch-Lab (config-if) # dot1x pae authenticator
```

Commandes	Description
authentication open	Permet le passage d'un trafic avant que le port soit authentifié
authentication port-control auto	Permet une authentification basée sur le port et indique au port de démarrer dans un état unauthorized, permettant seulement les frames EAPOL d'envoyer et de recevoir à travers ce port
Dot1x pae authenticator	Définit le port comme celui d'un authentificateur

Configurer l'interface 802.1X avec des commandes optionnelles

```
Switch-Lab (config) # interface fastethernet 0/1
Switch-Lab (config-if) # authentication periodic
Switch-Lab (config-if) # authentication timer reauthenticate
```

Commandes	Description
authentication periodic	Permet au Switch de demander au client de se réauthentifier de façon périodique
authentication timer reauthenticate	Configure l'intervalle de temps de réauthentification

III. CONFIGURATION DES SWITCH

La configuration de ces Switches sert à intégrer les serveurs ISE dans le réseau de MTN. Elle permet donc la communication entre les serveurs et tous les autres équipements intervenant dans le fonctionnement de la solution ISE. Ce sont les équipements des utilisateurs finaux (PC, Téléphones, autres), les Switches d'accès, les contrôleurs Wifi, les point d'accès wifi, etc.

1. Configuration des Switches d'interconnexion des Serveurs ISE

Pour configurer les interfaces des switch sur lesquels sont connectés les serveurs du site principal Techno-Center :

Interfaces XXX
Switchport mode access
Switch access vlan XX
Spanningtreeportfast

Pour configurer les interfaces des switch sur lesquels sont connectés les serveurs du site secondaire :

Interfaces XXX
Switchport mode access
Switch access vlan XX
Spanningtreeportfast

2. Configuration des switch d'accès

Pour s'assurer que le Cisco ISE est en mesure d'interagir avec les Switches d'accès et que ses fonctions s'exécutent avec succès à travers les segments réseaux, nous avons besoin de configurer les Switches d'accès avec les fonctions nécessaires : la synchronisation de l'heure avec le serveur NTP, le RADIUS/AAA (Authentification, Autorisation et Accounting), le 802.1X, le MAB et autres pour la communication avec les serveurs Cisco ISE.

Activer les fonctions AAA (Authentication, Authorization and Accounting) et 802.1X de façon globale

Sw-prestige-xx >enable
Sw-prestige-xx #configure terminal
Sw-prestige-xx (config) #aaa new-model
Sw-prestige-xx (config) #dot1x system-auth-control

Permettre l'authentification locale pour la console et le VTY

Sw-prestige-xx #aaa authentication login NO_RADIUS local
Sw-prestige-xx (config) #line con 0
Sw-prestige-xx (config-line) #login authentication NO_RADIUS
Sw-prestige-xx (config) #line vty 0 15

Commandes	Description
Aaa new-model	Active globalement le modèle d'accès AAA sur le switch
Dot1x system-auth-control	Active globalement l'authentification 802.1X sur le switch
Aaa authentication login NO_RADIUS local	Crée une méthode login AAA avec le nom NO_RADIUS qui utilise le nom d'utilisateur et le mot de passe de la base de données locale
Line con 0	Entre en mode configuration console
Line VTY 0 15	Entre en mode configuration VTY pour les 16 premières lignes VTY
Login authentication NO_RADIUS	Spécifie la liste de méthode pour l'authentification, et est demandé soit en mode de configuration console ou VTY

Activer les différentes fonctions AAA entre le Switch et le Cisco ISE incluant les fonctions d'authentification DOT1X et MAB

Sw-prestige-xx #aaa authentication dot1x default group radius
Sw-prestige-xx (config) #aaa authorization network default group radius
Sw-prestige-xx (config) #aaa accounting dot1x default start-stop group radius

Définir sur le Switch, le Cisco ISE comme serveur RADIUS

```
Sw-prestige-xx # radius-server host IP auth-port ID acct-port ID key cisco ID
Sw-prestige-xx (config) # radius-server host IP auth-port ID acct-port ID key cisco ID
```

Configurer le Switch pour interagir avec le Cisco ISE agissant comme le serveur RADIUS

```
Sw-prestige-xx (config) # radius-server vsa send authentication
Sw-prestige-xx (config) # radius-server vsa send authorization
```

Définir quels attributs RADIUS inclure avec les requêtes d'authentification

```
Sw-prestige-xx (config) # radius-server attribute 6 on-for-login-auth
Sw-prestige-xx (config) # radius-server attribute 8 include-in-access-req
Sw-prestige-xx (config) # radius-server attribute 25 access-request include
```

Spécifier ici les paramètres pour s'assurer que le Switch est en mesure de manipuler de façon appropriée le comportement de changement d'autorisation RADIUS supportant la fonction de posture venant de Cisco ISE.

```
aaa server radius dynamic-author
client IP server-key ID cisco ID
client IP server-key ID cisco ID
```

Activer « deviceTracking » pour la substitution de l'IP dans le contrôle d'accès dynamiques sur les ports du Switch.

```
ip device tracking
```

S'assurer que le Cisco ISE est en mesure de compiler les messages logs du Switch

```
logging monitor informational
logging origin-id ip
logging source-interface <interface_id>
logging host IP transport udp port ID
logging host IP transport udp port ID
```

Mettre en place les fonctions de logging standard sur le Switch pour supporter les possibles Troubleshooting/Recording pour les fonctions Cisco ISE.

```
Epm login
```

Normalement, un message Syslog contient l'adresse IP de l'interface qu'il utilise pour quitter le Switch. La commande spécifie que les paquets syslog contiennent l'adresse IP d'une interface particulière, indifféremment de quelle interface le packet utilise pour sortir du Switch. Le service Monitoring de Cisco ISE requiert que la commande utilise l'adresse IP utilisée pour ajouter le Switch comme client AAA dans le Cisco ISE.

```
logging source-interface <type number>
```

Créer un access-list pour définir le trafic permis avant que le port soit authentifié

```
Sw-prestige-xx (config) # ip access-list extended ACL-DEFAULT
Sw-prestige-xx (config) # remark NTP
Sw-prestige-xx (config) # permitudp any anyeqntp
```

```
Sw-prestige-xx (config) # remark DHCP
Sw-prestige-xx (config) # permit udp any eqbootpc any eqbootps
Sw-prestige-xx (config) # remark DNS
Sw-prestige-xx (config) # permitudp any anyeq domain
Sw-prestige-xx (config) # remark Ping
Sw-prestige-xx (config) # permiticmp any any
Sw-prestige-xx (config) # remark PXE / TFTP
Sw-prestige-xx (config) #permitudp any anyeqtftp
Sw-prestige-xx (config) # permittcp any host IP eq PORT
Sw-prestige-xx (config) # permittcp any host IP eq PORT
Sw-prestige-xx (config) # remark Drop all the rest
Sw-prestige-xx (config) # deny ip any anylog
```

IV. SAUVEGARDE

Dans toute configuration informatique, la sauvegarde est nécessaire afin de parer à toute éventualité d'incident. Cette configuration de la sauvegarde consiste à :

- Créer un répertoire sur n'importe quel support à partir du Cisco ISE. Pour faire la sauvegarde, des serveurs FTP, TFTP ou autres peuvent être utilisés.
- Lancer la sauvegarde de l'administrateur et du monitoring à partir du Cisco ISE.

Tout au long de ce quatrième chapitre, nous avons essayé d'aborder les configurations nécessaires des différents éléments constituant notre solution et ce, en alternant entre la citation des principes de fonctionnement et celle des configurations appliquées, tout en illustrant avec les figures explicatives.

Bien que la solution soit configurée et mise en place, une phase de test est indispensable afin de valider le comportement des différents composants vis-à-vis des machines tentant d'accéder au réseau.