**CISCO ISE CISCO IDENTITY SERVICE ENGINE**

**MASTER I**

SECURITE DES SYSTEMES D’INFORMATION

2023-2024

**MEMBRE DU GOUPE :**

GO Stanislas

GOUMBRI Levi

SOULAMA Ezekiel

SOMMAIRE

[**INTRODUCTION** 3](#_Toc174203512)

[**1.** **Définition de CISCO ISE** 3](#_Toc174203513)

[**1.1** **Composants Clés** 3](#_Toc174203514)

[**1.1.1** **ISE Node ou Nœud ISE** 3](#_Toc174203515)

[**1.1.2** **Base de données** 5](#_Toc174203516)

[**1.2** **Composant Réseau** 5](#_Toc174203517)

[**1.2.1** **Network Access Devices (NAD)** 5](#_Toc174203518)

[**1.2.2** **Network Protocol** 6](#_Toc174203519)

[**1.3** **Intégration et Connectivité** 6](#_Toc174203520)

[**1.3.1** **Sources d’identité** 6](#_Toc174203521)

[**1.3.2** **API et Extensibilité** 6](#_Toc174203522)

[**1.4** **Déploiement** 7](#_Toc174203523)

[**1.4.1** **Sur Site (On-Premises)** 7](#_Toc174203524)

[**1.4.2** **Dans le cloud (on Cloud)** 7](#_Toc174203525)

[**1.4.3** **En Hybride** 7](#_Toc174203526)

[**1.5** **Sécurité et Résilience** 7](#_Toc174203527)

[**1.5.1** **Redondance et Haute Disponibilité** 7](#_Toc174203528)

[**1.5.2** **Data Encryption** 7](#_Toc174203529)

[**2.** **Fonctionnalités de Cisco ISE** 7](#_Toc174203530)

[**3.** **Comparaison Cisco ISE, NAC et ACS** 11](#_Toc174203531)

[**3.1** **Cisco NAC** 11](#_Toc174203532)

[**3.2** **Cisco ACS** 12](#_Toc174203533)

[**3.3** **Cisco NAC vs Cisco ACS vs Cisco ISE** 13](#_Toc174203534)

[**4.** **Gestion des utilisateurs via une connexion VPN** 14](#_Toc174203535)

[**4.1** **Configuration d'un RA-VPN basé sur le client sur Cisco ASA** 15](#_Toc174203536)

[**4.2** **Configurer ISE pour le VPN ASA** 32](#_Toc174203537)

[**4.3** **Tester la configuration** 34](#_Toc174203538)

[**5.** **Définition de la Posture** 40](#_Toc174203539)

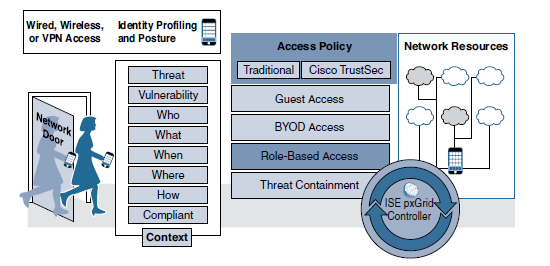
# **INTRODUCTION**

Cisco Identity Services Engine (ISE) est un système de contrôle d'accès réseau et d'application de politiques basé sur l'identité. Il fonctionne comme un moteur de politiques commun qui permet le contrôle d'accès aux points de terminaison et l'administration des périphériques réseau pour les entreprises. Vous pouvez exploiter Cisco ISE pour garantir la conformité, améliorer la sécurité de l'infrastructure et rationaliser les opérations de service. Un administrateur Cisco ISE peut collecter des données contextuelles en temps réel pour un réseau, notamment les utilisateurs et les groupes d'utilisateurs (qui ?), le type d'appareil (quoi ?), l'heure d'accès (quand ?), l'emplacement d'accès (où ?), le type d'accès (filaire, sans fil ou VPN) (comment ?) et les menaces et vulnérabilités du réseau.

Davantage la gouvernance et la sécurité des systèmes d’information devient de plus en plus critique, en vue d’atténuer et gérer cette problématique, nous verrons plus en détails comment l’outil Cisco ISE pourrait nous aider à atteindre ces objectifs.

# **Définition de CISCO ISE**

Cisco Identity Services Engine (ISE) est une solution de gestion de la politique d'accès réseau qui permet de contrôler et sécuriser l'accès aux ressources réseau en fonction de l'identité des utilisateurs, des périphériques et des politiques définies.



Voici un aperçu de son architecture :

## **Composants Clés**

### **ISE Node ou Nœud ISE**

Le nœud ISE est l'unité de base de la solution Cisco ISE. Chaque nœud peut jouer différents rôles dans l'architecture. Les nœuds ISE peuvent être regroupés en clusters pour assurer la haute disponibilité, la répartition de charge et la redondance. Ces nœuds gèrent des services comme :

**Les Cores Services** :

* **Authentication Services** : Gère l'authentification des utilisateurs et des périphériques via des protocoles tels que RADIUS, TACACS+, et EAP
* **Authorization Services** : Applique les politiques d'accès définies en fonction des règles spécifiées pour les utilisateurs et les périphériques.
* **Accounting Services** : Enregistre les données relatives aux sessions d'accès, y compris les connexions réussies et échouées, ainsi que les changements d'état des sessions.

**Les Policy Services Nodes (PSNs)** :

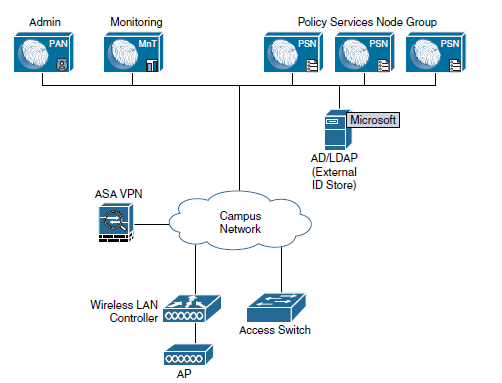
* **Policy Decision Points (PDP)** : Évaluent les demandes d'accès selon les politiques d'autorisation définies.
* **Policy Enforcement Points (PEP)** : Appliquent les décisions de politique à l'accès réseau et exécutent les actions appropriées (comme l'accès, la mise en quarantaine, etc.).
* **Policy Administration Points (PAP)** : Interface pour la configuration et la gestion des politiques d'accès.

**Les Managements Nodes (MN)** :

* **Policy Administration** : Permet la configuration et la gestion des politiques de sécurité.
* **System Administration** : Fournit des outils pour la gestion du système, la surveillance, et la génération de rapports.

**Le Monitoring & Reporting** :

* **Monitoring** : Surveille les activités du réseau, les événements d'authentification, et les sessions en cours.
* **Reporting** : Génère des rapports détaillés sur les événements, les tendances d'accès, et les statistiques de sécurité.



### **Base de données**

Cisco ISE dispose de deux options pour la configuration de sa base de données. L’option :

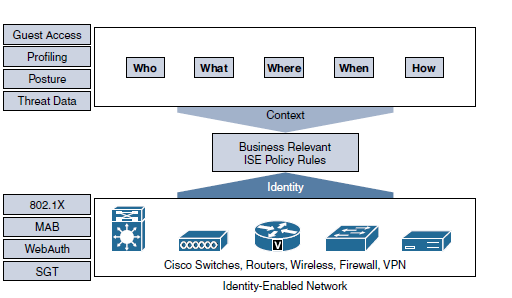
* **Internal Database :** Base de données intégrée utilisée pour stocker les informations de configuration, les politiques, et les données d'identité.
* **External Database :** Bases de données externes telles que LDAP, Microsoft Active Directory, ou bases de données SQL pour l'authentification et la gestion des identités.

## **Composant Réseau**

### **Network Access Devices (NAD)**

Pour la gestion du réseau informatique du système d’information, Cisco ISE s’appuie sur des périphériques comme :

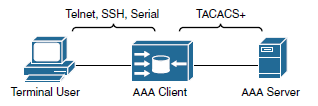
* **Les Switch** : Commutateurs réseau qui interagissent avec Cisco ISE pour l'authentification des utilisateurs et des périphériques connectés.
* **Wireless Access Points** : Points d'accès sans fil qui utilisent Cisco ISE pour appliquer des politiques d'accès sur les connexions Wi-Fi.
* **VPN Gateways** : Passerelles VPN qui utilisent Cisco ISE pour l'authentification et l'autorisation des utilisateurs distants.



### **Network Protocol**

Pour gérer l’authentification et les accès Cisco ISE dispose de protocoles comme :

* **RADIUS** : Les appareils ou services envoient des requêtes d'authentification et d'autorisation à Cisco ISE via le protocole RADIUS.
* **TACACS** : Les appareils ou services utilisent le protocole TACACS+ pour communiquer avec Cisco ISE pour les demandes d'authentification et d'autorisation.



## **Intégration et Connectivité**

### **Sources d’identité**

Pour la gestion des identités, Cisco ISE s’appuie sur les annuaires ou des sources externes tels que :

* **LDAP/AD** : L’intégration avec des annuaires LDAP ou Microsoft Active Directory pour la gestion des utilisateurs et des groupes.
* **External Identity Sources** : L’intégration avec d'autres sources d'identité comme des bases de données SQL ou des services d'annuaire tiers.

### **API et Extensibilité**

Cisco ISE offre une possibilité d’intégration d’API et d’extensibilité c’est-à-dire l’intégration d’un :

* **REST API** : Pour l'intégration avec des systèmes tiers, la gestion automatisée, et la personnalisation
* **Syslog** : Pour envoyer des journaux d'événements vers des systèmes de gestion des informations et des événements de sécurité (SIEM).

## **Déploiement**

Le déploiement de l’outils Cisco ISE peut être effectué de différente manière comme :

### **Sur Site (On-Premises)**

* **Physical Appliances** : Serveurs physiques installés sur site pour un contrôle direct de l'infrastructure.
* **Virtual Appliances** : Déploiement de Cisco ISE sur des machines virtuelles dans un environnement de virtualisation local.

### **Dans le cloud (on Cloud)**

* **Cloud Deployment** : Déploiement de Cisco ISE dans des environnements cloud tels qu'AWS, Azure, ou autres fournisseurs de services cloud.

### **En Hybride**

* **Hybrid Deployment** : Combinaison de déploiements sur site et dans le cloud pour une flexibilité accrue et une résilience améliorée.

## **Sécurité et Résilience**

Pour implémenter l’aspect sécurité et la résilience, Cisco ISE dispose de certains modules notamment le module Redondance et Haute disponibilité et le module Data Encryption.

### **Redondance et Haute Disponibilité**

* **Deployment with HA** : Déploiement de Cisco ISE avec une configuration de haute disponibilité (HA) pour garantir la continuité du service en cas de panne.
* **Load Balancing** : Utilisation de dispositifs de répartition de charge pour équilibrer le trafic entre plusieurs nœuds Cisco ISE.

### **Data Encryption**

* **In-Transit Encryption** : Chiffrement des données en transit entre les clients, les périphériques réseau, et Cisco ISE.
* **At-Rest Encryption** : Chiffrement des données stockées dans les bases de données internes et externes.

Ainsi voici présenter l’architecture de l’outils Cisco ISE, à la suite de cela nous verrons les fonctionnalités dont il dispose.

# **Fonctionnalités de Cisco ISE**

Cisco ISE est un système de contrôle d'accès basé sur des politiques consolidées qui intègre un sur-ensemble de fonctionnalités disponibles dans les plates-formes de politiques Cisco existantes. Cisco ISE exécute les fonctions suivantes :

• Combine l'authentification, l'autorisation, la comptabilité (AAA), la posture et le profileur dans un seul appareil

• Fournit une gestion complète de l'accès invité pour l'administrateur Cisco ISE, les administrateurs sponsors agréés ou les deux

• Assure la conformité des points de terminaison en fournissant des mesures complètes de provisionnement des clients et en évaluant la posture des périphériques pour tous les points de terminaison qui accèdent au réseau, y compris les environnements 802.1X

• Fournit une prise en charge de la découverte, du profilage, du placement basé sur des politiques et de la surveillance des périphériques de points de terminaison sur le réseau

• Permet une politique cohérente dans les déploiements centralisés et distribués qui permettent aux services d'être fournis là où ils sont nécessaires

• Utilise des fonctionnalités d'application avancées, notamment l'accès au groupe de sécurité (SGA) via l'utilisation de balises de groupe de sécurité (SGT) et de listes de contrôle d'accès au groupe de sécurité (SGACL)

• Prend en charge l'évolutivité pour prendre en charge un certain nombre de scénarios de déploiement, des petits bureaux aux environnements de grande entreprise

Les fonctions clés suivantes de Cisco ISE vous permettent de gérer l'intégralité de votre réseau d'accès.

**Fournir un accès réseau basé sur l'identité**

La solution Cisco ISE fournit une gestion des identités sensible au contexte dans les domaines suivants :

• Cisco ISE détermine si les utilisateurs accèdent au réseau sur un appareil autorisé et conforme aux politiques.

• Cisco ISE établit l'identité, l'emplacement et l'historique d'accès de l'utilisateur, qui peuvent être utilisés à des fins de conformité et de création de rapports.

• Cisco ISE attribue des services en fonction du rôle d'utilisateur attribué, du groupe et de la politique associée (rôle professionnel, emplacement, type d'appareil, etc.).

• Cisco ISE accorde aux utilisateurs authentifiés l'accès à des segments spécifiques du réseau, à des applications et services spécifiques, ou aux deux, en fonction des résultats d'authentification.

Les fonctions clés suivantes de Cisco ISE vous permettent de gérer différents scénarios de déploiement.

**Gérer différents scénarios de déploiement**

Vous pouvez déployer Cisco ISE sur l'ensemble d'une infrastructure d'entreprise, prenant en charge les réseaux câblés, sans fil et virtuels privés (VPN) 802.1X.

L'architecture Cisco ISE prend en charge les déploiements autonomes et distribués (également appelés « haute disponibilité » ou « redondants ») où une machine assume le rôle principal et une autre machine « de secours » assume le rôle secondaire. Cisco ISE propose des personnages, des services et des rôles configurables distincts, qui vous permettent de créer et d'appliquer des services Cisco ISE là où ils sont nécessaires sur le réseau. Le résultat est un déploiement Cisco ISE complet qui fonctionne comme un système entièrement fonctionnel et intégré.

Vous pouvez déployer des nœuds Cisco ISE avec un ou plusieurs personnages d'administration, de surveillance et de service de politique, chacun exécutant une partie vitale différente dans votre topologie globale de gestion des politiques réseau. L'installation de Cisco ISE avec un personnage d'administration vous permet de configurer et de gérer votre réseau à partir d'un portail centralisé pour promouvoir l'efficacité et la facilité d'utilisation.

Vous pouvez également choisir de déployer la plateforme Cisco ISE en tant que nœud de posture en ligne pour appliquer les politiques et exécuter les demandes de changement d'autorisation (CoA) lorsque les utilisateurs accèdent au réseau via des WLC et/ou des concentrateurs VPN qui ne prennent pas en charge les fonctionnalités nécessaires pour faciliter la gestion des politiques Cisco ISE.

Les fonctions clés suivantes de Cisco ISE vous permettent de gérer la fourniture d’une authentification et une autorisation utilisateur de base.

**Fournir une authentification et une autorisation utilisateur de base**

Les politiques d'authentification utilisateur dans Cisco ISE vous permettent de fournir une authentification pour un certain nombre de types de sessions de connexion utilisateur à l'aide de divers protocoles d'authentification standard, notamment, mais sans s'y limiter, le protocole d'authentification par mot de passe (PAP), le protocole d'authentification par poignée de main (CHAP), le protocole d'authentification extensible protégé (PEAP) et le protocole d'authentification extensible (EAP). Cisco ISE spécifie les protocoles autorisés disponibles pour les périphériques réseau sur lesquels l'utilisateur tente de s'authentifier et spécifie les sources d'identité à partir desquelles l'authentification utilisateur est validée.

Cisco ISE autorise une large gamme de variables dans les politiques d'autorisation pour garantir que seuls les utilisateurs autorisés peuvent accéder aux ressources appropriées lorsqu'ils accèdent au réseau. La version initiale de Cisco ISE prend uniquement en charge l'accès géré par RADIUS au réseau interne et à ses ressources.

Au niveau le plus fondamental, Cisco ISE prend en charge la norme 802.1X, le contournement de l'authentification MAC (MAB) et la connexion par authentification Web basée sur un navigateur pour l'authentification utilisateur de base et l'accès via les réseaux filaires et sans fil. Lors de la réception d'une demande d'authentification, la « partie externe » de la politique d'authentification est utilisée pour sélectionner l'ensemble des protocoles autorisés à être utilisés lors du traitement de la demande. Ensuite, la « partie interne » de la politique d'authentification est utilisée pour sélectionner la source d'identité utilisée pour authentifier la demande. La source d'identité peut être constituée d'un magasin d'identités spécifique ou d'une séquence de magasins d'identités qui répertorie un ensemble d'identités accessibles jusqu'à ce que l'utilisateur reçoive une réponse d'autorisation définitive.

Une fois l'authentification réussie, le flux de session passe à la politique d'autorisation. (Il existe également des options disponibles qui permettent à Cisco ISE de traiter la politique d'autorisation même lorsque l'authentification n'a pas réussi.) Cisco ISE vous permet de configurer le comportement pour les cas d’« échec d'authentification », d'« utilisateur non trouvé » et d'« échec du processus », et également de décider de rejeter la demande, de l'abandonner (aucune réponse n'est émise) ou de poursuivre la politique d'autorisation. Dans les cas où Cisco ISE continue d'exécuter l'autorisation, vous pouvez utiliser l'attribut « AuthenticationStaus » dans le dictionnaire « NetworkAccess » pour incorporer le résultat de l'authentification dans le cadre de la politique d'autorisation.

Le résultat de la politique d'autorisation est l'attribution par Cisco ISE d'un profil d'autorisation qui peut également impliquer une liste de contrôle d'accès téléchargeable spécifiant la gestion du trafic sur le périphérique d'application de la politique réseau. L'ACL téléchargeable spécifie les attributs RADIUS qui sont renvoyés lors de l'authentification et qui définissent les privilèges d'accès utilisateur accordés une fois authentifié par Cisco ISE.

Les fonctions clés suivantes de Cisco ISE vous permettent d’intégrer l’évaluation de la posture du client.

**Intégrer l'évaluation de la posture du client**

Pour garantir que les mesures de sécurité réseau imposées restent pertinentes et efficaces, Cisco ISE vous permet de valider et de maintenir les capacités de sécurité sur toute machine cliente qui accède au réseau protégé. En utilisant des politiques de posture conçues pour garantir que les paramètres ou applications de sécurité les plus récents sont disponibles sur les machines clientes, l'administrateur Cisco ISE peut s'assurer que toute machine cliente qui accède au réseau respecte et continue de respecter les normes de sécurité définies pour l'accès au réseau d'entreprise. Les rapports de conformité de posture fournissent à Cisco ISE un instantané du niveau de conformité de la machine cliente au moment de la connexion de l'utilisateur, ainsi qu'à chaque fois qu'une réévaluation périodique a lieu.

L'évaluation de la posture et la conformité s'effectuent à l'aide de l'un des types d'agent suivants disponibles dans Cisco

ISE :

• Cisco NAC Web Agent : un agent temporaire que l'utilisateur installe sur son système au moment de la connexion et qui n'est plus visible sur la machine cliente une fois la session de connexion terminée.

• Agent Cisco NAC : un agent persistant qui, une fois installé, reste sur une machine cliente Windows ou Mac OS X pour exécuter toutes les fonctions de connexion utilisateur et de conformité de sécurité pour les clients Windows XP, Windows Vista, Windows 7 ou Mac OS 10.5 et 10.6, respectivement.

Les fonctions clés suivantes de Cisco ISE vous permettent de définir des sponsors et des sessions d’invitées.

**Définition des sponsors et gestion des sessions d'invités**

Les administrateurs et employés Cisco ISE qui bénéficient d'un accès approprié au portail d'inscription des invités Cisco ISE en tant que sponsors invités peuvent créer des comptes de connexion d'invités temporaires et spécifier les ressources réseau disponibles pour permettre aux invités, visiteurs, sous-traitants, consultants et clients d'accéder au réseau. Les sessions d'accès invité sont associées à des temporisateurs d'expiration, ce qui permet de contrôler efficacement l'accès des invités à un jour, une période, etc.

Tous les aspects d'une session d'utilisateur invité (y compris la création et la résiliation de compte) sont suivis et enregistrés dans Cisco ISE afin que vous puissiez fournir des informations d'audit et résoudre les problèmes d'accès aux sessions, si nécessaire.

Les fonctions clés suivantes de Cisco ISE vous permettent de gérer le trafic sans fil et VPN.

**Gérer le trafic sans fil et VPN avec des nœuds de posture en ligne**

Les nœuds de posture en ligne sont des nœuds de contrôle d'accès qui appliquent les politiques d'accès Cisco ISE et gèrent les demandes CoA.

Après l'authentification initiale (à l'aide d'EAP/802.1X et RADIUS), les machines clientes doivent encore passer par une évaluation de posture. Le processus d'évaluation de posture détermine si le client doit être restreint, refusé ou autorisé à accéder pleinement au réseau. Lorsqu'un client accède au réseau via un WLC ou un périphérique VPN, le nœud de posture en ligne est responsable de l'application des politiques et de la CoA que les autres périphériques réseau ne peuvent pas prendre en charge. C'est pour cette raison qu'un Cisco ISE peut être déployé en tant que nœud de posture en ligne derrière d'autres périphériques d'accès réseau sur votre réseau, tels que des WLC et des concentrateurs VPN.

Les fonctions clés suivantes de Cisco ISE vous permettent de gérer le profil des points de terminaison.

**Profil des points de terminaison sur le réseau**

Le service Profiler permet d'identifier, de localiser et de déterminer les capacités de tous les points de terminaison sur votre réseau (appelés identités dans Cisco ISE), quels que soient leurs types d'appareils respectifs, afin d'assurer et de maintenir un accès approprié à votre réseau d'entreprise. La fonction Cisco ISE Profiler utilise un certain nombre de sondes pour collecter les attributs de tous les points de terminaison de votre réseau et les transmettre à l'analyseur

Profiler où les points de terminaison connus sont classés en fonction de leurs politiques associées et des groupes d'identités.

# **Comparaison Cisco ISE, NAC et ACS**

## **Cisco NAC**

Cisco NAC (Network Access Control), Cisco ACS (Access Control Server), et Cisco ISE (Identity Services Engine) sont trois solutions développées par Cisco pour la gestion de l'accès réseau et la sécurité. Bien qu'elles partagent certains objectifs communs, elles diffèrent considérablement en termes de fonctionnalités et de capacités. Voici une comparaison détaillée de ces trois solutions :

**Objectif Principal**

* **Contrôle d'Accès au Réseau** : Cisco NAC est conçu pour contrôler l'accès au réseau en fonction de la conformité des dispositifs avec les politiques de sécurité.

**Fonctionnalités**

* **Évaluation de la Conformité** : Vérifie si les dispositifs respectent les politiques de sécurité avant de leur accorder l'accès au réseau.
* **Application des Politiques** : Met en quarantaine les dispositifs non conformes ou les restreint à un réseau d'invités.
* **Remédiation** : Aide à corriger les problèmes de conformité sur les dispositifs pour les rendre conformes aux politiques de sécurité.

**Cas d'Utilisation**

* **Environnements où la conformité des dispositifs est cruciale** : Par exemple, garantir que les dispositifs respectent les configurations de sécurité avant d'accéder au réseau.

**Déploiement**

* **Généralement utilisé dans des configurations moins complexes** : Où la principale préoccupation est la conformité des dispositifs.

## **Cisco ACS**

Cisco ACS (Access Control Server) est une solution de gestion des accès réseau utilisée pour l'authentification, l'autorisation et la comptabilisation des utilisateurs et des dispositifs. Bien qu'il soit maintenant remplacé par Cisco ISE, ACS reste une solution importante dans les déploiements existants. Voici une vue d'ensemble détaillée de Cisco ACS :

**Objectif Principal**

* **Gestion des Accès** : Cisco ACS est une solution d'authentification, d'autorisation et de comptabilisation (AAA) pour les utilisateurs et les dispositifs sur le réseau.

**Fonctionnalités**

* **Authentification et Autorisation** : Authentifie les utilisateurs et les dispositifs et les autorise à accéder à des ressources spécifiques.
* **Comptabilisation** : Suivi des activités des utilisateurs pour la facturation et l'audit.
* **Support des Protocoles** : Fonctionne avec RADIUS et TACACS+ pour gérer les politiques d'accès et de gestion.

**Cas d'Utilisation**

* **Gestion centralisée des politiques d'accès pour les dispositifs réseau** : Par exemple, contrôler l'accès à un routeur ou un switch.

***Déploiement***

* **Environnements où la gestion AAA est requise** : Cisco ACS est souvent déployé dans des environnements où une gestion de base des accès et des politiques est suffisante.

## **Cisco NAC vs Cisco ACS vs Cisco ISE**

|  |  |  |  |
| --- | --- | --- | --- |
| Caractéristique | Cisco NAC | Cisco ACS | Cisco ISE |
| **Objectif Principal** | Contrôle de la conformité des dispositifs | Authentification, autorisation et comptabilisation | Gestion centralisée des politiques d'accès |
| **Évaluation de la Conformité** | Oui | Non | Oui |
| **Authentification des Utilisateurs** | Non | Oui | Oui |
| **Autorisation Basée sur l'Identité** | Non | Oui | Oui |
| **Profilage des Dispositifs** | Limitée | Non | Oui |
| **Gestion des Invités** | Limitée | Non | Oui |
| **Reporting et Surveillance** | Basique | Basique | Avancé |
| **Intégration avec AD/LDAP** | Variable | Oui | Oui |
| **Remédiation** | Oui (limité) | Non | Oui (plus dynamique) |
| **Déploiement** | Moins complexe | Moyen | Complexe |

**Résumé**

* **Cisco NAC** : Ciblé principalement sur la conformité des dispositifs avant d'accorder l'accès au réseau. Il est idéal pour les environnements où la conformité des dispositifs est une préoccupation majeure.
* **Cisco ACS** : Une solution de gestion des accès et de comptabilisation plus ancienne, centrée sur les fonctionnalités de base d'authentification et d'autorisation, mais avec des capacités limitées en matière de gestion des politiques modernes.
* **Cisco ISE** : Offre une solution complète pour la gestion des politiques d'accès, l'authentification, l'autorisation, le profilage des dispositifs, et la gestion des invités. C'est une plateforme moderne et intégrée qui convient aux environnements complexes nécessitant une gestion détaillée et dynamique des accès réseau.

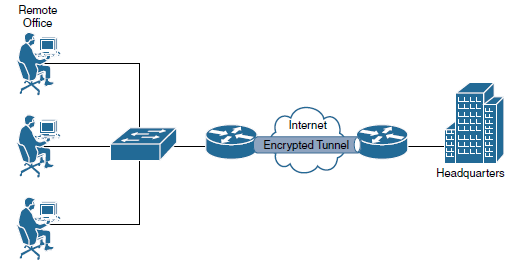
# **Gestion des utilisateurs via une connexion VPN**

Les VPN ou encore Virtual Private Network sont des réseaux virtuels basés sur internet qui permet l’interconnexion des locaux ou d’entreprise.

Il existe de nombreux types de réseaux privés virtuels (VPN). Les VPN :

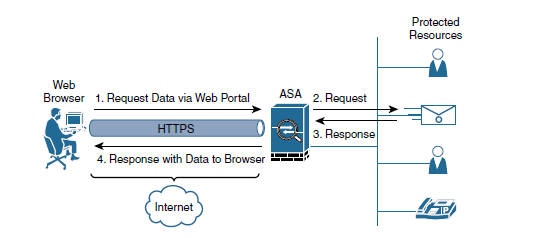
* **VPN site à site**

Un réseau privé virtuel (VPN) de site à site est un type de VPN qui connecte des réseaux entiers entre eux via Internet. Contrairement aux VPN de client à site, qui connectent des appareils individuels à un réseau, les VPN de site à site relient deux ou plusieurs réseaux, tels que des succursales ou des sites distants, permettant une communication transparente entre eux.



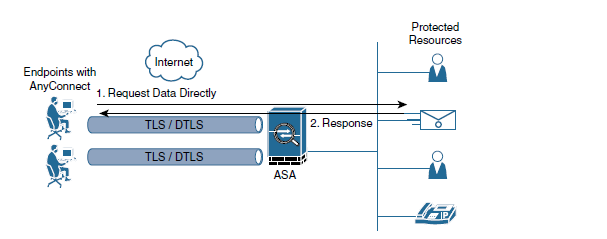
* **VPN d’accès à distance sans client**

Un VPN d'accès à distance sans client permet aux utilisateurs d'accéder à un réseau à distance sans avoir à installer de logiciel client VPN dédié sur leur appareil. Au lieu de cela, les utilisateurs se connectent via un navigateur Web standard.



* **VPN d’accès à distance basé sur le client**

Un VPN d'accès à distance basé sur le client (Virtual Private Network) est un type de VPN dans lequel les utilisateurs doivent installer et exécuter une application client VPN spécifique sur leur appareil pour établir une connexion sécurisée à un réseau distant. Cette configuration permet aux utilisateurs distants d'accéder aux ressources du réseau interne comme s'ils étaient physiquement présents au bureau.



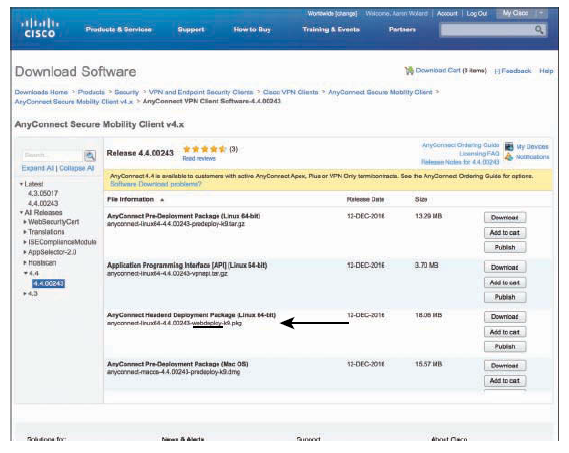
Le dernier type de VPN permettent de facilement gérer les utilisateurs à travers Cisco ASA (Adaptative Security Appliance) et Cisco AnyConnect Secure Mobility Client (AnyConnect) .

AnyConnect est avant tout un client VPN, mais c'est aussi bien plus que cela. Le client AnyConnect est modulaire, ce qui permet d'adapter d'autres modules de services de sécurité Cisco au client.

## **Configuration d'un RA-VPN basé sur le client sur Cisco ASA**

Voici les differentes etapes à suiver pour configurer Cisco ASA et AnnyConnect :

**Étape 1. Téléchargez les derniers packages de tête de réseau AnyConnect.**



**Étape 2. Préparez la tête de réseau.**

Après vous être connecté à ASDM (Manager de Cisco ASA) , suivez ces étapes pour préparer la tête de réseau :

Étape 1. Accédez à Configuration > Accès distant VPN > Accès réseau (client) > Profils de connexion AnyConnect.

Étape 2. Cochez la case Activer l'accès client VPN Cisco AnyConnect sur les interfaces

Sélectionnées

Si vous n'avez pas chargé de packages AnyConnect, vous êtes invité à

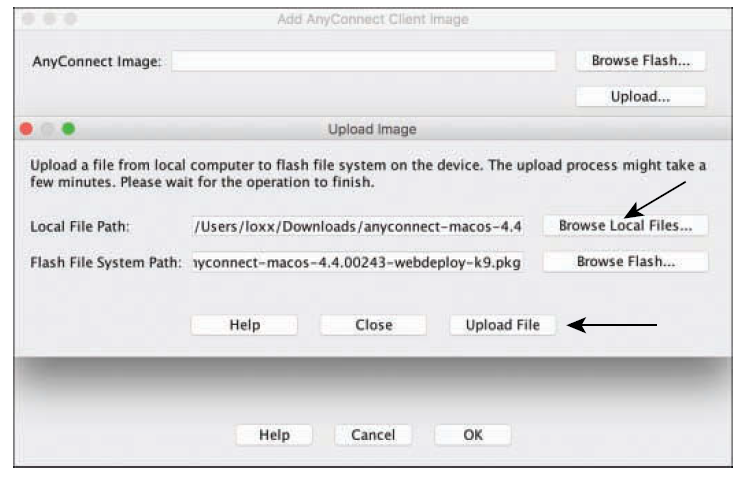
Indiquer « L'accès client AnyConnect ne peut pas être activé sans une

Image AnyConnect désignée. Souhaitez-vous désigner une image AnyConnect ?»

Si vous ne recevez pas ce message, cela signifie que vous avez déjà installé des packages AnyConnect sur l'ASA. Dans ce cas, accédez à

Configuration > Accès distant VPN > Accès réseau (client) > Logiciel client AnyConnect et cliquez sur Ajouter pour suivre la procédure.

Etape 3. Si vous recevez l’invite affichée, cliquez sur Oui pour ouvrir la boîte de dialogue Ajouter

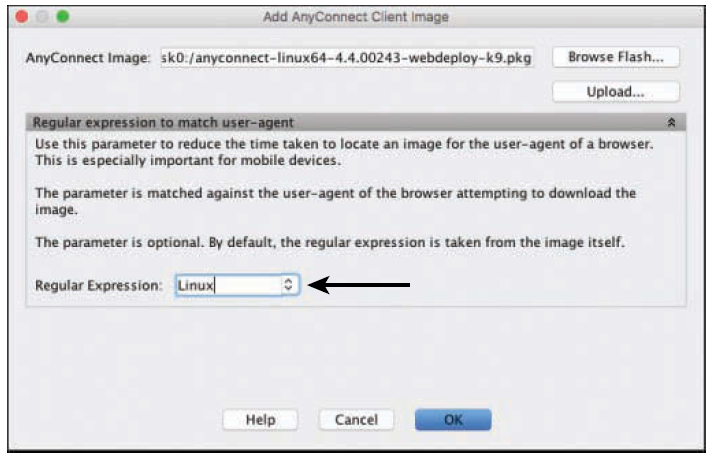


Étape 4. Cliquez sur Télécharger, cliquez sur Parcourir les fichiers locaux et sélectionnez l'un des packages que vous avez téléchargés, comme illustré dans la figure

Étape 5. Cliquez sur Télécharger le fichier.

Étape 6. Sélectionnez l'expression régulière du système d'exploitation pour qu'elle corresponde au type de système d'exploitation du package téléchargé, comme illustré dans la figure.

L'ASA s'attend à ce que le logiciel client Windows soit la valeur par défaut et, par conséquent, vous demande d'indiquer le système d'exploitation pour qu'il corresponde aux autres images pour Linux et Mac.



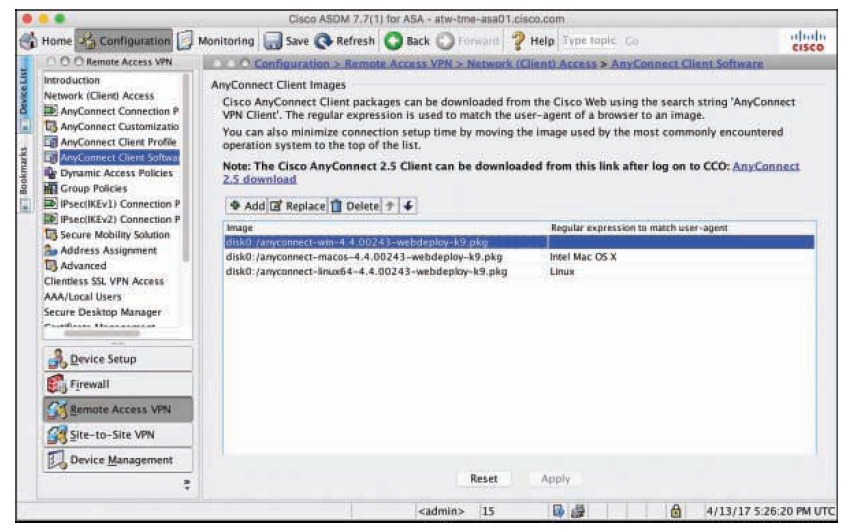
Étape 7. Cliquez sur OK pour terminer le téléchargement et le mappage.

Étape 8. Répétez les étapes 3 à 6 jusqu'à ce que Windows, Mac OS et Linux soient tous téléchargés.

Ignorez l'étape 5 pour Windows.

Étape 9. Cliquez sur Appliquer pour enregistrer les modifications de configuration dans la configuration en cours d'exécution.

Étape 10. Cliquez sur Enregistrer pour enregistrer la configuration dans la configuration de démarrage.



**Étape 3. Ajoutez un profil de connexion AnyConnect.**

Étape 1. Cochez la case Activer l'accès client VPN Cisco AnyConnect sur les interfaces Sélectionnées dans le tableau ci-dessous.

Étape 2. Dans le tableau des interfaces, choisissez l'interface que vous souhaitez utiliser pour

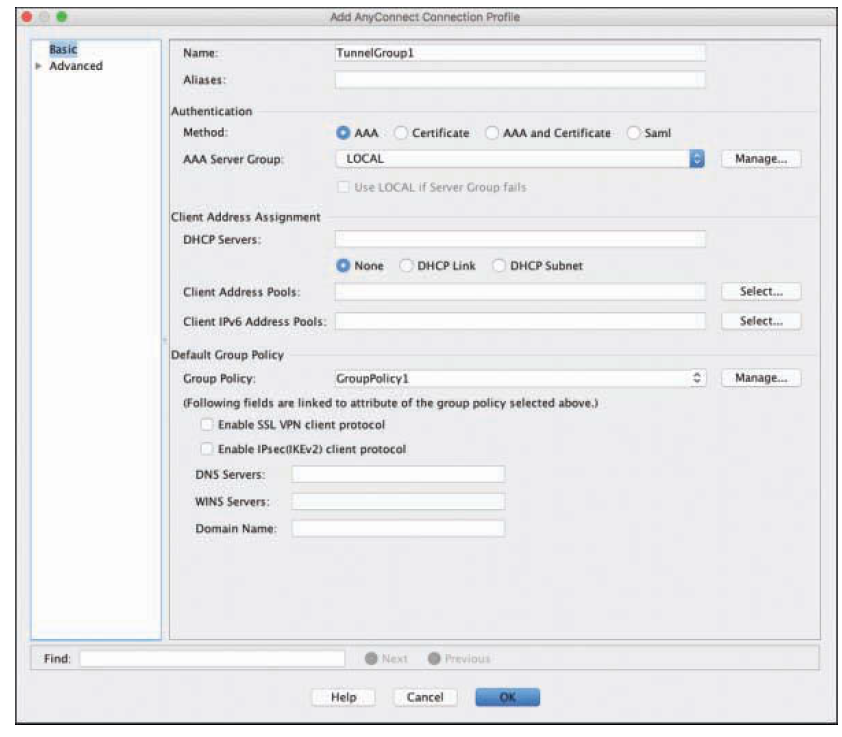
L’accès VPN. En général, l'interface externe est utilisée. Dans ce cas, cochez les cases Autoriser l'accès sous Accès SSL et IPsec (IKEv2) pour l'interface externe.

Étape 3. Cochez les cases Activer DTLS et Activer les services client.

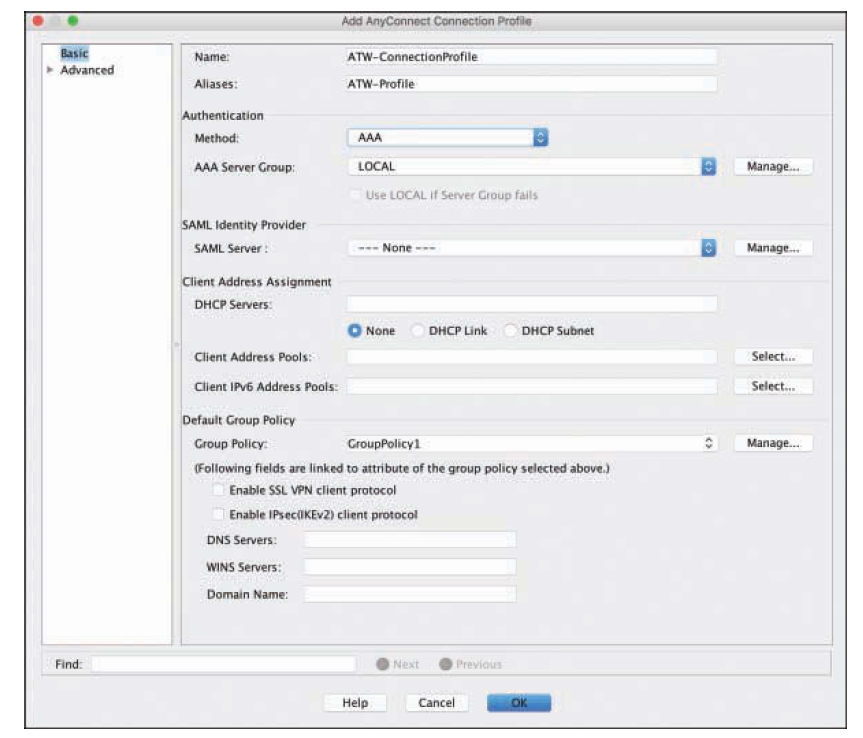
Étape 4. Sous le tableau, cochez la case Contourner les listes d'accès d'interface pour les sessions VPN entrantes, ce qui empêche l'ACL de devoir tenir compte du trafic autorisé des utilisateurs VPN vers le réseau interne. Cela est, bien entendu, spécifique à vos besoins dans le déploiement.

Étape 5. (Facultatif) Cochez la case Autoriser l'utilisateur à sélectionner un profil de connexion sur la page de connexion si cela convient à votre déploiement VPN de production. Maintenant que l'accès à distance avec AnyConnect est activé sur l'interface externe de l'ASA, l'étape logique suivante consiste à ajouter un nouveau profil de connexion.

Étape 6. Cliquez sur Ajouter pour ajouter un nouveau profil de connexion. L'écran Ajouter un profil de connexion AnyConnect s'affiche, comme illustré dans la Figure 19

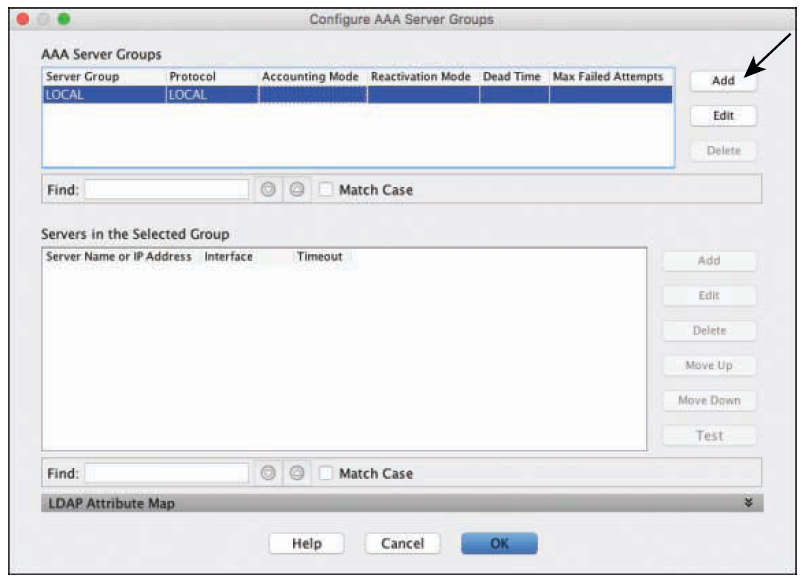


Étape 7. Renommez le profil de connexion de TunnelGroup1 en quelque chose qui a du sens pour vous et vos utilisateurs.



Étape 8. Dans la zone de texte Alias, indiquez un alias. Il peut parfois être utilisé par l'utilisateur final pour effectuer une sélection dans la liste déroulante lors de la connexion et peut être utilisé pour la correspondance d'URL. Pour cet exemple, utilisez ATW-Profile, comme indiqué dans la figure.

Étape 9. Dans la section Authentification, sélectionnez AAA dans le champ Méthode et cliquez sur Gérer. Le VPN nécessite un mécanisme pour authentifier les utilisateurs et les autoriser à se connecter. (Voir le chapitre 2, « Principes fondamentaux de AAA », pour un rappel sur l'authentification, l'autorisation et la comptabilité.) Par défaut, l'ASA utilise une base de données d'utilisateurs locale. Il s'agit évidemment d'une erreur de configuration que vous devez corriger immédiatement.



Étape 10. Cliquez sur Ajouter pour créer un nouveau groupe de serveurs AAA. Ce groupe sert d'espace réservé pour plusieurs serveurs RADIUS (PSN ISE).

Étape 11. Dans la boîte de dialogue Ajouter un groupe de serveurs AAA, illustrée dans la figure, indiquez un nom descriptif qui permet d'identifier les serveurs qui seront dans ce groupe. Dans l'exemple, le groupe est nommé ISE231-232 car il contiendra deux PSN ISE : atw-ise231 et atw-ise232. Rétrospectivement, un meilleur nom serait SJC-ISE, décrivant l'emplacement (San Jose) et les types de serveurs (ISE), qui prend en compte la possibilité d'ajouter davantage de PSN à l'avenir.

Étape 12. Dans la liste déroulante Protocole, choisissez RADIUS.

Étape 13. Laissez le paramètre Mode de comptabilité sur la valeur par défaut, Unique. Cela est important. Le mode unique envoie le paquet de comptabilité au serveur RADIUS actif uniquement, tandis que le mode simultané diffuse les paquets de comptabilité à tous les serveurs RADIUS du groupe. Ce n'est pas une bonne idée, en particulier avec les serveurs RADIUS qui suivent l'état de session, comme le fait ISE, et peut avoir des résultats indésirables.

Étape 14. Laissez le paramètre Mode de réactivation sur la valeur par défaut, Épuisement, le Temps mort sur la valeur par défaut de 10 minutes et le Nombre maximal de tentatives échouées sur la valeur par défaut de 3. Avec ces paramètres, un serveur RADIUS sera marqué comme non réactif (mort) après trois tentatives d'authentification sans réponse. La réactivation fait référence à la méthode par laquelle les serveurs RADIUS non réactifs (morts) sont remis en service sur l'ASA. Le mode d'épuisement ne ramènera pas un serveur mort tant que tous les serveurs du groupe n'auront pas été épuisés. Même ainsi, il attendra 10 minutes par défaut (Temps mort).

Étape 15. Cochez la case Activer la mise à jour de la comptabilité intermédiaire.

Étape 16. Cochez la case Intervalle de mise à jour et laissez la valeur par défaut de 24 heures. La comptabilité intermédiaire est importante pour ISE car elle permet de s'assurer qu'un utilisateur est toujours connecté et que la session réseau est toujours active.

Étape 17. Dans la section Application de la politique ISE, cochez la case Activer l'autorisation dynamique et laissez le paramètre Port d'autorisation dynamique à sa valeur par défaut de 1700. Comme vous le savez probablement en lisant les 18 premiers chapitres de ce livre, l'autorisation dynamique est le nom officiel de la modification de l'autorisation (CoA), que l'ASA effectue un peu différemment des périphériques réseau que vous avez configurés jusqu'à présent dans le livre. Pour la plupart des cas d'utilisation que vous avez vus dans ce livre, un CoA de réauthentification (CoA-ReAuth) est utilisé. À l'inverse, l'ASA utilise uniquement un type de CoA de poussée de politique (CoA-Push). Voici la différence :

■ CoA-ReAuth : lorsqu’un CoA est envoyé au périphérique d’accès au réseau (NAD), il envoie à son tour une demande au point de terminaison pour s’authentifier à nouveau, auquel cas un processus complet d’authentification et d’autorisation se produit à nouveau, avec un nouveau résultat d’autorisation envoyé au NAD.

■ CoA-Push : lorsqu’un CoA est envoyé à l’ASA, le paquet CoA contient déjà le nouveau résultat d’autorisation. Dans le cas de l’ASA, cela signifie qu’une nouvelle ACL est envoyée. Plus de détails sur cette méthode sont fournis plus loin dans le chapitre.

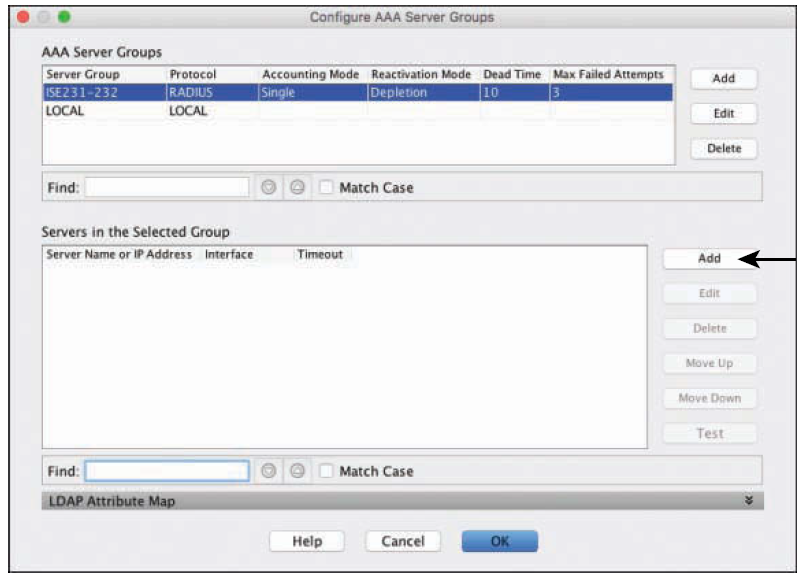


Étape 18. Cliquez sur OK. Laissez la fenêtre Configurer les groupes de serveurs AAA ouverte pour procéder à la configuration dans la section suivante.

**Étape 4. Ajoutez les PSN ISE au groupe de serveurs AAA.**

Avec le groupe de serveurs nouvellement créé (ISE231-232 dans l'exemple) sélectionné dans la fenêtre configurer les groupes de serveurs AAA, comme illustré dans la figure, suivez ces étapes :

Étape 1. À droite du volet Serveurs dans le groupe sélectionné, cliquez sur Ajouter pour créer un objet serveur RADIUS.



Étape 2. Dans la boîte de dialogue Ajouter un serveur AAA, illustrée à la figure, choisissez pour le nom de l'interface l'interface correcte la plus proche des PSN ISE. Dans l'exemple, il s'agit de l'interface interne.

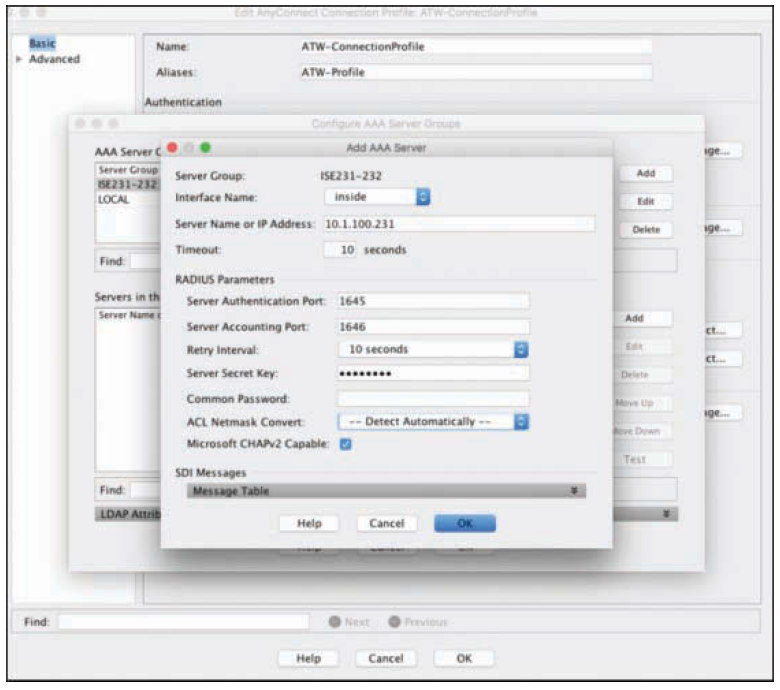
Étape 3. Dans le champ Nom du serveur ou adresse IP, saisissez le nom DNS ou l'adresse IP du premier PSN et laissez la valeur Délai d'expiration à la valeur par défaut de 10 secondes.

Étape 4. Laissez les champs Port d'authentification du serveur et Port de comptabilité du serveur à leurs valeurs par défaut de 1645 et 1646, respectivement.

Étape 5. Laissez l'intervalle de nouvelle tentative à la valeur par défaut de 10 secondes.

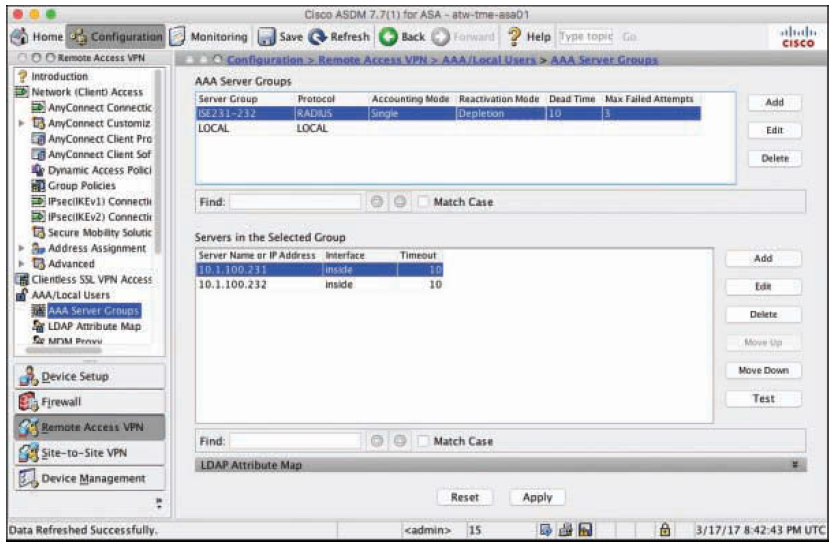
Étape 6. Dans le champ Clé secrète du serveur, indiquez le secret partagé RADIUS qui est utilisé entre l'ASA et l'ISE. Il doit être le même que celui configuré dans la définition d'objet NAD dans l'ISE.

Étape 7. Dans la liste déroulante Conversion du masque de réseau ACL, choisissez Détecter automatiquement. Il s'agit d'un paramètre intéressant. Tandis que les ACL des commutateurs Cisco Catalyst utilisent un masque générique dans l'ACL au lieu d'un masque de réseau standard, l'ASA utilise un masque de réseau standard pour sa configuration ACL. Étant donné que l'ASA peut accepter les ACL téléchargeables (dACL) envoyées depuis ISE, ces dACL peuvent être configurées pour la méthode du masque de réseau générique ou standard. La définition du serveur RADIUS dans l'ASA peut être configurée pour l'une ou l'autre, ou pour détecter automatiquement laquelle est envoyée.



Étape 8. Cliquez sur OK.

Étape 9. Répétez les étapes 1 à 8 pour chacun des PSN.



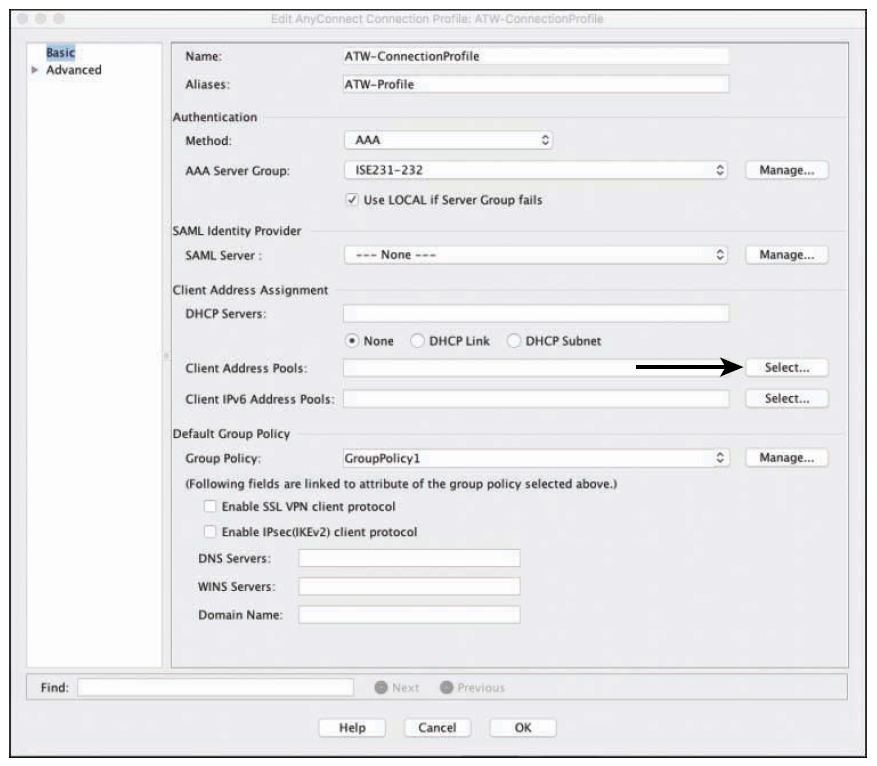
Étape 10. Cliquez sur Appliquer.

Étape 11. Cliquez sur Enregistrer.

L’étape suivante consiste à configurer l’attribution de l’adresse client.

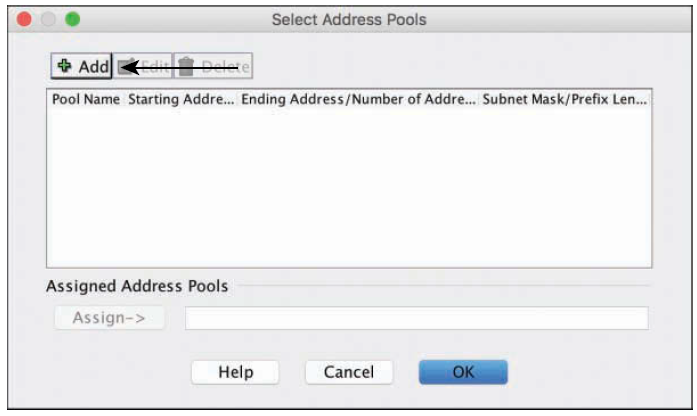
**Étape 5. Ajoutez un pool d'adresses client.**

La figure suivante montre le profil de connexion après la configuration du groupe de serveurs AAA. L’élément suivant dans la configuration est la section Fournisseur d’identité SAML. Cela ne s’applique pas à l’exemple de configuration ISE actuel, donc laissez le champ Serveur SAML défini sur Aucun.



Vous devez pouvoir attribuer une adresse IP aux clients lorsqu'ils se connectent au VPN. Comme indiqué dans la section Attribution d'adresses client de la figure, vous pouvez configurer le profil de connexion pour utiliser un serveur DHCP externe afin d'attribuer des adresses IP aux points de terminaison de connexion, ou vous pouvez utiliser un pool d'adresses configuré localement sur l'ASA. Cet exemple utilise ce dernier. Les étapes suivantes montrent comment utiliser un pool d'adresses :

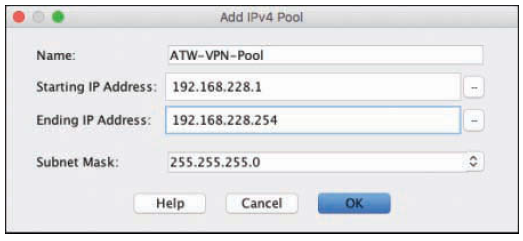
Étape 1. Cliquez sur Sélectionner à droite de Pools d'adresses client, comme indiqué dans la figure, pour ouvrir la boîte de dialogue Sélectionner les pools d'adresses, illustrée dans la figure.



Étape 2. Cliquez sur Ajouter pour ouvrir la boîte de dialogue Ajouter un pool IPv4, illustrée dans la figure.

Étape 3. Donnez un nom explicite au pool d'adresses. À titre d'exemple, utilisez ATW-VPN-Pool.

Étape 4. Saisissez les adresses IP de début et de fin, ainsi que le masque de sous-réseau.



Étape 5. Cliquez sur OK pour revenir à la boîte de dialogue Sélectionner les pools d'adresses.

Étape 6. Sélectionnez le pool d'adresses IPv4 nouvellement créé et cliquez sur Attribuer, comme indiqué dans la figure.



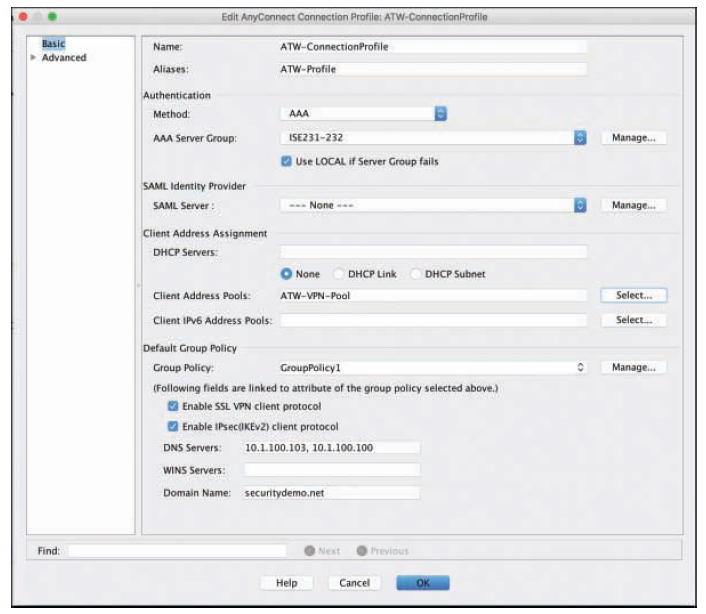
Étape 7. Cliquez sur OK. Vous revenez à l'écran Profil de connexion, avec le pool d'adresses attribué. L'étape logique suivante consiste à configurer une stratégie de groupe, mais cela n'est pas nécessaire pour les objectifs de ce chapitre. Laissez donc la valeur par défaut de GroupPolicy1, comme indiqué dans la figure

Étape 8. Cochez la case Activer le protocole client VPN SSL.

Étape 9. Cochez la case Activer le protocole client IPsec (IKEv2).

Étape 10. Dans le champ Serveurs DNS, indiquez les serveurs DNS à utiliser pour les clients connectés.

Étape 11. Dans le champ Nom de domaine, indiquez le nom de domaine DNS à attribuer aux clients.



Étape 12. Cliquez sur OK.

Étape 13. Cliquez sur Appliquer.

Étape 14. Cliquez sur Enregistrer.

Le profil de connexion AnyConnect est désormais entièrement configuré, avec un pool d'adresses à partir duquel attribuer des adresses IP client, prêtes à répondre aux requêtes SSL (TLS, en fait) et

IPsec (IKEv2). Cependant, vous n'êtes pas encore prêt à ce que vos clients rejoignent le VPN.

**Étape 6. Effectuez des tâches d'accessibilité au réseau.**

Les autres hôtes du réseau doivent savoir comment renvoyer le trafic aux adresses provenant du pool VPN. Il existe plusieurs façons d'accomplir cette tâche, dont le choix dépend de la préférence de votre équipe réseau et de l'exécution ou non de protocoles de routage dynamique sur votre ASA :

Si vous exécutez un protocole de routage dynamique, tel que OSPF ou EIGRP, vous pouvez redistribuer l'itinéraire du pool d'adresses dans ce protocole de routage.

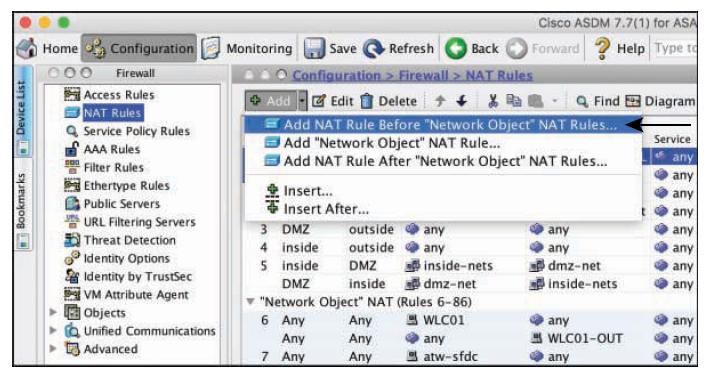
Vous pouvez ajouter une route statique dans le réseau qui envoie tout le trafic du pool VPN vers l'ASA.

Utilisez l'ASA comme passerelle par défaut. Cette option est courante dans les déploiements de plus petite taille, comme les succursales. Dans ce scénario, le trafic de retour est déjà envoyé à l'ASA.

L’option ASA dans cet exemple est la passerelle par défaut pour cet environnement, et par conséquent la troisième option est utilisée. Une fois le routage réglé, l'étape suivante consiste à s'assurer que le trafic vers et depuis le VPN est exempté de la traduction d'adresses réseau (NAT). Pour accomplir cette tâche, suivez ces étapes :

Étape 1. Accédez à Configuration > Pare-feu > Règles NAT.

Étape 2. Cliquez sur la flèche déroulante à côté d’Ajouter et choisissez Ajouter une règle NAT avant les règles NAT « Objet réseau », comme illustré dans la figure. Cela garantit que la règle est traitée correctement.



Étape 3. Dans la section Critères de correspondance : Paquet d'origine en haut de la boîte de dialogue Ajouter une règle NAT, choisissez l'interface interne de la liste déroulante Interface source, comme illustré dans la figure.

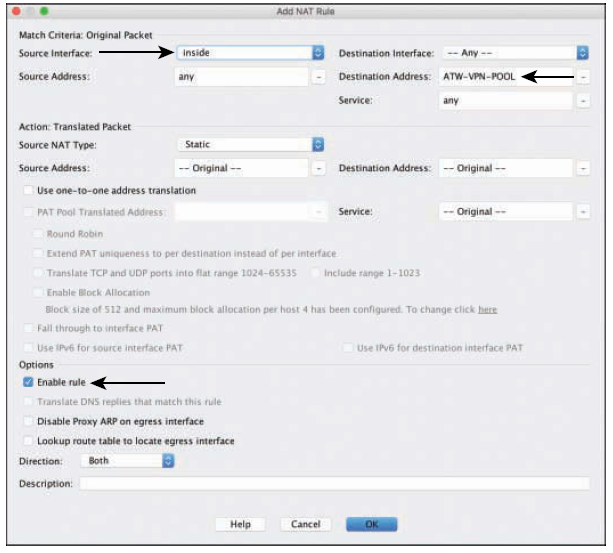
Étape 4. Laissez le champ Interface de destination défini sur N'importe laquelle.

Étape 5. Modifiez l'adresse de destination pour qu'elle corresponde aux adresses de votre pool d'adresses client. Vous pouvez utiliser le réseau ou créer un objet réseau.

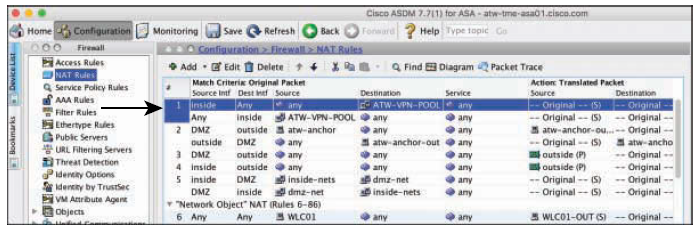
Étape 6. Dans la section Action : Paquet traduit, laissez le champ Type NAT source défini sur Statique et le champ Adresse source défini sur Original.

Étape 7. Dans la section Options, cochez la case Activer la règle.

Étape 8. Définissez le champ Direction sur Les deux, ce qui garantit que la règle NAT est créée pour également le trafic de retour.



Étape 9. Cliquez sur OK.

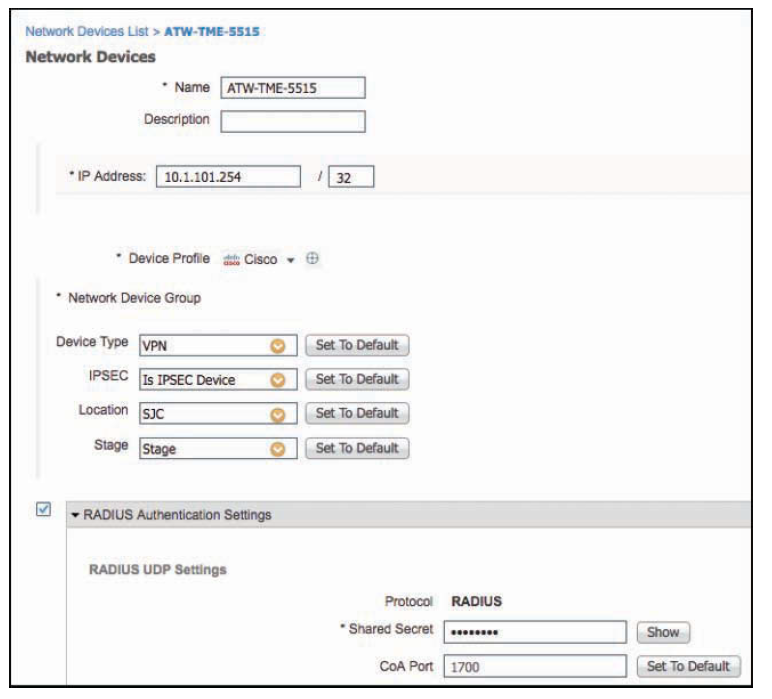


Étape 10. Cliquez sur Appliquer.

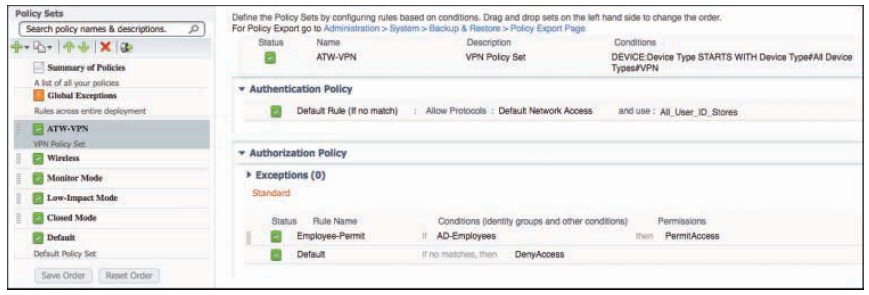
Étape 11. Cliquez sur Enregistrer.

## **Configurer ISE pour le VPN ASA**

À ce stade, toute la configuration requise dans l'ASA est terminée et il est temps de passer aux configurations requises dans ISE. L'ASA est un périphérique de couche d'accès lorsqu'il agit comme une tête de réseau VPN. Au lieu qu'un utilisateur final se connecte à un port de commutateur Catalyst ou s'associe au SSID Wi-Fi du WLC, l'utilisateur établit un tunnel vers l'ASA. Exactement comme les commutateurs et les WLC, l'ASA est le client RADIUS et ISE est le serveur RADIUS. En tant que tel, vous devez vous assurer qu'ISE dispose d'un objet NAD configuré pour l'ASA sous Centres de travail > Accès réseau > Ressources réseau >Périphériques réseau, et vous devez vous assurer que le secret partagé RADIUS correspond à ce qui a été configuré dans l'objet serveur AAA dans la configuration ASA. La figure suivante montre l'objet NAD configuré dans ISE.



Ensuite, vous devez configurer la politique d'accès à distance (accédez à Centres de travail> Accès réseau > Ensembles de politiques). La meilleure pratique habituelle consiste à dédier un ensemble de politiques aux politiques d'accès à distance, au lieu de les mélanger avec un ensemble de politiques filaire ou sans fil. Cela facilite le dépannage et évite toute confusion lors de la conception des politiques. La figure suivante montre un exemple d'ensemble de politiques pour les périphériques VPN, avec une règle d'autorisation générique qui envoie une acceptation d'accès RADIUS si l'utilisateur est membre du groupe Employés dans Active Directory.



Cette politique très simple est tout ce dont vous avez besoin pour que l'authentification et l'autorisation VPN fonctionnent. Bien entendu, la politique peut être ajustée et rendue beaucoup plus spécifique aux besoins de votre organisation. Par exemple, vous pouvez ajouter une évaluation de la posture à la politique.

## **Tester la configuration**

Pour tester votre configuration, le premier test que vous devez effectuer est un test AAA de base de l'ASA vers ISE, pour vous assurer que tout est correctement configuré pour l'authentification et l'autorisation. Ensuite, vous vous connecterez au portail sur l'ASA pour télécharger et installer AnyConnect. Enfin, vous vous connecterez au VPN et vérifierez que vous disposez d'une connectivité complète.

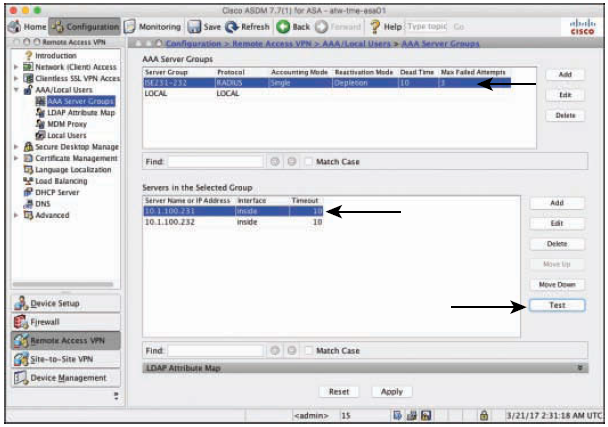
Effectuer un test AAA de base

Le premier test consiste à effectuer un test AAA de base. Depuis l'interface graphique ASDM :

Étape 1. Accédez à Configuration > VPN d'accès à distance > Utilisateurs AAA/locaux >Groupes de serveurs AAA.

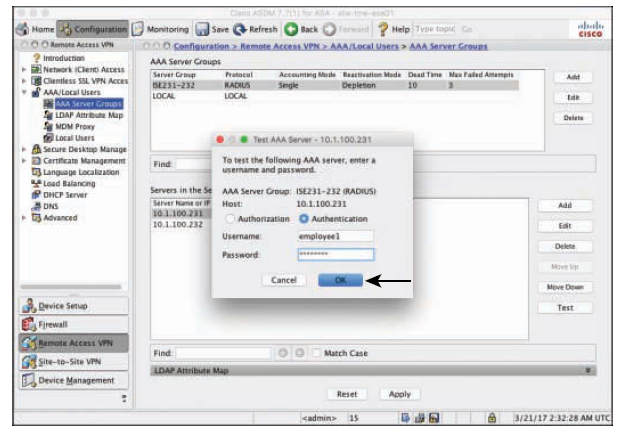
Étape 2. Sélectionnez le groupe de serveurs que vous avez configuré plus tôt dans AnyConnect.

Étape 3. Sélectionnez l’un des PSN que vous avez ajoutés au groupe de serveurs AAA, comme indiqué dans la figure suivante.



Étape 4. Cliquez sur Tester.

Étape 5. Dans la boîte de dialogue Tester le serveur AAA, illustrée dans la figure, choisissez Authentification, qui teste en fait à la fois l'authentification et l'autorisation car RADIUS effectue les deux dans une seule transaction.



Étape 6. Dans le champ Nom d'utilisateur, saisissez le nom d'utilisateur d'Active Directory de l'utilisateur qui doit recevoir un Access-Accept.

Étape 7. Saisissez le mot de passe de l'utilisateur.

Étape 8. Cliquez sur OK pour effectuer le test.

Étape 9. Si tout est correctement configuré, vous voyez un message de réussite tel que celui indiqué dans la figure suivante.

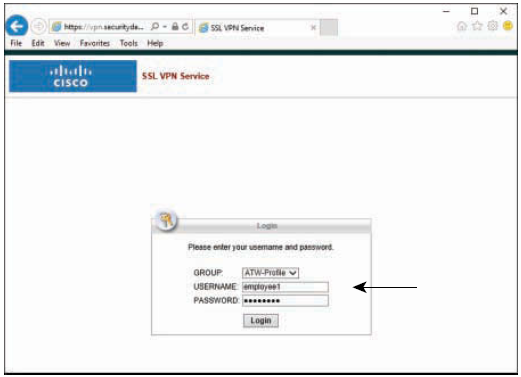


Connectez-vous au portail Web ASA

Après avoir confirmé que la configuration AAA dans l'ASA et dans ISE est correcte, le test suivant consiste à vous connecter au portail Web, où vous pouvez télécharger et installer AnyConnect. À partir d'un point de terminaison pouvant accéder à l'extérieur de votre ASA :

Étape 1. Ouvrez un navigateur Web et accédez à l'adresse IP externe de votre ASA à l'aide de HTTPS. Par exemple : <https://vpn.securitydemo.net/>. L'URL change automatiquement en /+CSCOE+/logon.html#.

Étape 2. Dans le portail, connectez-vous avec un nom d'utilisateur et un mot de passe, comme indiqué dans la figure. Le nom d'utilisateur et le mot de passe sont envoyés à ISE via une demande d'accès RADIUS.

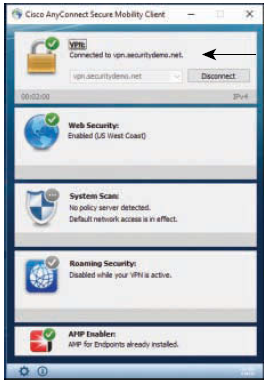


Étape 3. La connexion au portail lance automatiquement une applet ActiveX (Windows) ou une applet Java (non Windows) qui installe AnyConnect.

■ Si l'applet ne se lance pas, vous pouvez télécharger le programme d'installation manuel directement depuis le portail.

■ Si AnyConnect est déjà installé sur le point de terminaison, l'applet se connecte au VPN à l'aide des informations d'identification saisies dans le portail.

Étape 4. Une fois AnyConnect installé ou lancé, vous êtes connecté au VPN avec le tunnel établi, comme illustré dans la figure.



Connectez-vous au VPN via AnyConnect

Le troisième et dernier test consiste à vous connecter au VPN directement depuis AnyConnect. À partir du point de terminaison qui peut accéder à l'extérieur de votre ASA, sur lequel AnyConnect est désormais installé :

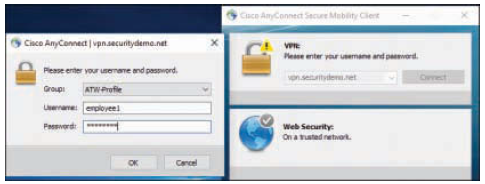
Étape 1. Lancez le client de mobilité sécurisée AnyConnect.

Étape 2. Saisissez le nom de domaine complet de l'interface externe de l'ASA ou l'adresse IP elle-même dans le champ de connexion VPN, comme indiqué dans la figure.



Étape 3. Cliquez sur Connecter.

Étape 4. Saisissez votre nom d'utilisateur et votre mot de passe dans la fenêtre contextuelle, comme indiqué dans la figure.



Étape 5. Cliquez sur OK.

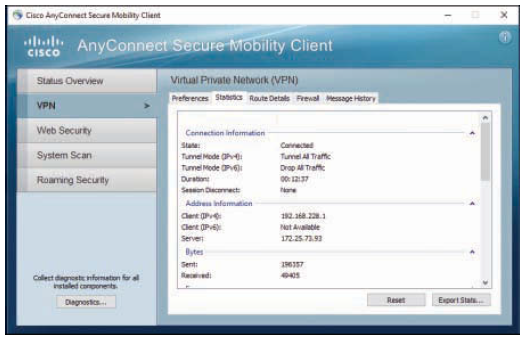
Le VPN s'établit et AnyConnect se réduit par défaut.

Étape 6. Cliquez sur l'icône AnyConnect dans la barre d'état système pour faire réapparaître l'interface utilisateur du client.

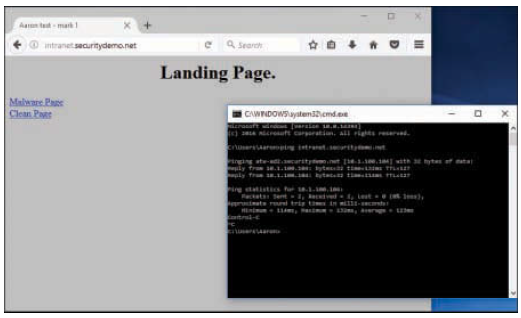
Étape 7. Cliquez sur l’icône d’engrenage dans le coin inférieur gauche du client AnyConnect pour afficher la fenêtre d’état, comme indiqué dans la figure.



Étape 8. Choisissez VPN > Statistiques pour voir plus d’informations de connexion sur le VPN, comme indiqué dans la figure.



Étape 9. À l’aide du navigateur Web, connectez-vous à un serveur, comme indiqué dans la figure.



Comme vous pouvez le constater par le Ping réussi et la navigation Web réussie vers un serveur interne, la connexion VPN est réussie et le trafic de retour revient également vers le client. Donc les administrateurs pourront gérer les clients VPN en fonction des règles et des politiques qui seront définis.

# **Définition de la Posture**

La posture dans Cisco ISE (Identity Services Engine) se réfère au processus d'évaluation de la conformité de sécurité des dispositifs qui tentent de se connecter à un réseau. Cette évaluation vérifie si les dispositifs respectent les politiques de sécurité et de conformité définies par l'organisation avant de leur accorder ou non l'accès au réseau. Cisco ISE utilise cette fonctionnalité pour garantir que les dispositifs ne présentent pas de vulnérabilités ou de configurations non sécurisées qui pourraient compromettre la sécurité du réseau. Autrement ditla posture, dans le contexte de Cisco Identity Services Engine (ISE), désigne l'état de sécurité d'un appareil au moment où il tente de se connecter à un réseau ; c'est un processus qui permet d'évaluer si un appareil (ordinateur, smartphone, IoT) est suffisamment sécurisé pour accéder à vos ressources réseau.

