Configurer l'ASA virtuel

Le déploiement ASA virtuel préconfigure l'accès ASDM. À partir de l'adresse IP client que vous avez spécifiée lors du déploiement, vous pouvez vous connecter à la gestion des adresses IP de l'ASA virtuel à l'aide d'un navigateur Web. Ce chapitre décrit également comment autoriser d'autres clients à accéder à ASDM et comment autoriser l'accès à l'interface de ligne de commande (SSH ou Telnet). D'autres tâches de configuration essentielles traitées dans ce chapitre comprennent l'installation de la licence et les tâches de configuration courantes fournies par les assistants dans ASDM.

Démarrer ASDM

Procédure

Étape 1 Sur le PC que vous avez spécifié comme client ASDM, saisissez l'URL suivante :

https://*asa_ip_address***/admin**

La fenêtre de lancement ASDM apparaît avec les boutons suivants :

- **Installer le lanceur ASDM et exécuter ASDM**
- **Exécuter ASDM**
- **Exécuter l'assistant de démarrage**

Étape 2 Pour télécharger le lanceur :

a) Cliquez sur **Install ASDM Launcher and Run ASDM** (Installer le lanceur ASDM et exécuter ASDM).

b) Laissez les champs du nom d'utilisateur et du mot de passe vides (pour une nouvelle installation), puis cliquez sur **OK**. En l'absence d'authentification HTTPS, vous pouvez accéder à ASDM sans nom d'utilisateur et mot de passe **d'activation**, qui est vide par défaut. Si vous avez activé l'authentification HTTPS, saisissez votre nom d'utilisateur et le mot de passe associé.

c) Enregistrez le programme d'installation sur votre PC, puis démarrez le programme d'installation. Le lanceur ASDM-IDM s'ouvre automatiquement une fois l'installation terminée.

d) Saisissez la gestion des adresses IP, laissez le nom d'utilisateur et le mot de passe vides (pour une nouvelle installation), puis cliquez sur **OK**. Si vous avez activé l'authentification HTTPS, saisissez votre nom d'utilisateur et le mot de passe associé.

Étape 3 Pour utiliser Java Web Start :

a) Cliquez **Run ASDM** (Exécuter ASDM) ou **Run Startup Wizard** (Exécuter l'assistant de démarrage).
b) Enregistrez le raccourci sur votre ordinateur lorsque vous y êtes invité(e). Vous pouvez également l'ouvrir au lieu de l'enregistrer.
c) Démarrez Java Web Start à partir du raccourci.
d) Acceptez tous les certificats en fonction des boîtes de dialogue qui s'affichent. Le lanceur Cisco ASDM-IDM apparaît.
e) Laissez le nom d'utilisateur et le mot de passe vides (pour une nouvelle installation), puis cliquez sur **OK**. Si vous avez activé l'authentification HTTPS, saisissez votre nom d'utilisateur et le mot de passe associé.

Effectuer la configuration initiale à l'aide d'ASDM

Vous pouvez effectuer la configuration initiale en utilisant les assistants et les procédures ASDM suivants.

- Exécuter l'assistant de démarrage
- (Facultatif) Autoriser l'accès aux serveurs publics derrière l'ASA virtuel
- (Facultatif) Exécuter les assistants de réseau privé virtuel (VPN)
- (Facultatif) Exécuter d'autres assistants dans ASDM

Pour la configuration de l'insterface de ligne de commande, consultez les guides de configuration de la CLI de la série Cisco Cisco Secure Firewall ASA .

Exécuter l'assistant de démarrage

Exécutez l'**assistant de démarrage** pour personnaliser la politique de sécurité en fonction de votre déploiement.

Procédure

Étape 1 Choisissez **Wizards (assistants)** > **Startup Wizard (assistant de démarrage)**.

Étape 2 Personnalisez la politique de sécurité en fonction de votre déploiement. Vous pouvez définir les éléments suivants :

- Nom d'hôte
- Nom de domaine
- Mot de passe administratif
- Interfaces
- Adresses IP
- du routage statique;

- Serveur DHCP
- Règles de traduction d'adresse réseau
- et plus encore…

(Facultatif) Autoriser l'accès aux serveurs publics derrière l'ASA virtuel

Le volet **Configuration** > **Firewall (Pare-feu)** > **Public Servers (Serveurs publics)** configure automatiquement la politique de sécurité pour rendre un serveur interne accessible à partir d'Internet. En tant que propriétaire d'entreprise, vous pouvez avoir des services de réseau interne, tels qu'un serveur web et FTP, qui doivent être disponibles pour un utilisateur externe. Vous pouvez placer ces services sur un réseau distinct derrière l'ASA virtuel, appelé zone démilitarisée (DMZ). En plaçant les serveurs publics sur DMZ, les attaques lancées contre les serveurs publics n'affectent pas vos réseaux internes.

(Facultatif) Exécuter les assistants de réseau privé virtuel (VPN)

Vous pouvez configurer le réseau privé virtuel (VPN) à l'aide des assistants suivants (**Wizards (assistants)** > **VPN Wizards (assistants VPN)**) :

- Site-to-Site VPN Wizard (assistant VPN de site à site) : crée un tunnel IPsec de site à site entre l'ASA virtuel et un autre périphérique compatible avec le réseau privé virtuel (VPN).
- AnyConnect VPN Wizard (assistant VPN AnyConnect) : configure l'accès à distance au réseau privé virtuel (VPN) SSL pour Cisco AnyConnect VPN client. Secure Client (services client sécurisés) fournit des connexions SSL sécurisées à l'ASA pour les utilisateurs distants avec une tunnellisation VPN complète aux ressources de l'entreprise. Vous pouvez configurer la politique ASA pour télécharger l'Secure Client (services client sécurisés) pour les utilisateurs distants lorsqu'ils se connectent pour la première fois par le biais d'un navigateur. Avec Secure Client (services client sécurisés) 3.0 et les versions ultérieures, le client peut exécuter le protocole VPN SSL ou IPsec IKEv2.
- Clientless SSL VPN Wizard (assistant VPN SSL sans client) : configure l'accès à distance au VPN SSL sans client pour un navigateur. Le VPN SSL sans client et par navigateur permet aux utilisateurs d'établir un tunnel VPN sécurisé d'accès à distance vers l'ASA à l'aide d'un navigateur Web. Après l'authentification, les utilisateurs accèdent à une page de portail et peuvent accéder à des ressources internes spécifiques prises en charge. L'administrateur réseau fournit un accès aux ressources par les utilisateurs par groupe. Les listes de contrôle d'accès peuvent être appliquées pour restreindre ou autoriser l'accès à des ressources d'entreprise spécifiques.
- IPsec (IKEv1 or IKEv2) Remote Access VPN Wizard (assistant VPN d'accès à distance IPsec (IKEv1 ou IKEv2) : configure l'accès à distance du VPN IPsec pour le client Cisco IPsec.

Pour plus d'informations sur la configuration d'une connexion ASA virtuel IPsec Virtual Tunnel Interface (VTI) à Azure, consultez Configurer la connexion ASA IPsec VTI à Azure.

(Facultatif) Exécuter d'autres assistants dans ASDM

Vous pouvez exécuter d'autres assistants dans ASDM pour configurer le basculement avec la haute disponibilité, l'équilibrage de charges des grappes VPN et la capture de paquets.

- Assistant de haute disponibilité et d'évolutivité : configurez le basculement ou l'équilibrage de charges VPN.
- Assistant de capture de paquets : configurez et exécutez la capture de paquets. L'assistant exécute une capture de paquets sur chacune des interfaces d'entrée et de sortie. Après avoir capturé des paquets, vous pouvez enregistrer les captures de paquets sur votre PC pour les examiner et les relire dans l'analyseur de paquets.

Configuration avancée

Pour poursuivre la configuration de votre ASA virtuel, consultez la documentation Naviguer dans la série Cisco Secure Firewall ASA.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.