Serveur proxy de messagerie

Les serveurs proxy de messagerie étendent la capacité de messagerie à distance aux utilisateurs de VPN SSL sans client. Lorsque les utilisateurs tentent d'établir une session par courriel par l'intermédiaire du serveur proxy de messagerie, le client de messagerie établit un tunnel à l'aide du protocole SSL.

Les protocoles du serveur proxy de messagerie sont les suivants :

POP3S

POP3S est l'un des serveurs proxy de messagerie pris en charge par le VPN SSL sans client. Par défaut, l'appareil de sécurité est à l'écoute du port 995, et les connexions sont automatiquement autorisées vers le port 995 ou vers le port configuré. Le serveur proxy POP3 autorise uniquement les connexions SSL sur ce port. Une fois le tunnel SSL établi, le protocole POP3 démarre, puis l'authentification a lieu. POP3S permet de recevoir des courriels.

IMAP4S

IMAP4S est l'un des serveurs proxy de messagerie pris en charge par le VPN SSL sans client. Par défaut, l'appareil de sécurité est à l'écoute du port 993, et les connexions sont automatiquement autorisées vers le port 993 ou vers le port configuré. Le serveur proxy IMAP4 autorise uniquement les connexions SSL sur ce port. Une fois le tunnel SSL établi, le protocole IMAP4 démarre, puis l'authentification a lieu. IMAP4S permet de recevoir des courriels.

SMTPS

SMTPS est l'un des serveurs proxy de messagerie pris en charge par le VPN SSL sans client. Par défaut, l'appareil de sécurité est à l'écoute du port 988, et les connexions sont automatiquement autorisées vers le port 988 ou le port configuré. Le serveur proxy SMTPS autorise uniquement les connexions SSL sur ce port. Après l'établissement du tunnel SSL, le protocole SMTPS démarre, puis l'authentification a lieu. SMTPS permet d'envoyer des courriels.

Configurer le serveur proxy de messagerie

Exigences du serveur proxy de messagerie

- Les utilisateurs qui accèdent au courriel à partir d'emplacements locaux et distants par l'intermédiaire du serveur proxy de messagerie ont besoin de comptes de messagerie distincts dans leur programme de messagerie pour l'accès local et à distance.
- Les sessions de proxy de messagerie nécessitent l'authentification de l'utilisateur.

Définir les groupes de serveurs AAA

Procédure

Étape 1 Accédez à **Configuration** > **Features (Fonctionnalités de configuration)** > **VPN** > **E-mail Proxy (Serveur proxy de messagerie VPN)** > **AAA**.

Étape 2 Choisissez l'onglet approprié (POP3S, IMAP4S ou SMTPS) pour associer les groupes de serveurs AAA et configurer la stratégie de groupe par défaut pour ces sessions.

- AAA Server Groups (Groupes de serveurs AAA) : cliquez pour accéder au panneau AAA Server Groups (Groupes de serveurs AAA) (Configuration > Features (Fonctionnalités) > Properties (Propriétés) > AAA Setup (Configuration AAA) > AAA Server Groups (Groupes de serveurs AAA)), où vous pouvez ajouter ou modifier des groupes de serveurs AAA.
- Group Policies (Stratégies de groupe) cliquez pour accéder au panneau Group Policy (Stratégie de groupe) (Configuration > Features (Fonctionnalités) > VPN (VPN) > General (Général) > Group Policy (Stratégie de groupe)), où vous pouvez ajouter ou modifier des stratégies de groupe.
- Authentication Server Group (Groupe de serveurs d'authentification) : sélectionnez le groupe de serveurs d'authentification pour l'authentification de l'utilisateur. La valeur par défaut est de n'avoir aucun serveur d'authentification configuré. Si AAA est défini comme méthode d'authentification (Configuration > Features (Fonctionnalités) > AAA (AAA) > VPN (VPN) > E-Mail Proxy (Serveur proxy de messagerie) > Authentication (Authentification)), vous devez configurer un serveur AAA et le choisir ici, sinon l'authentification échoue toujours.
- Authorization Server Group (Groupe de serveurs d'autorisation) : sélectionnez le groupe de serveurs d'autorisation pour l'autorisation de l'utilisateur. La valeur par défaut est de n'avoir aucun serveur d'autorisation configuré.
- Accounting Server Group (Groupe de serveurs de comptabilité) : sélectionnez le groupe de serveurs de comptabilité pour la comptabilité des utilisateurs. La valeur par défaut est de n'avoir aucun serveur de comptabilité configuré.
- Default Group Policy (Stratégie de groupe par défaut) : sélectionnez la stratégie de groupe à appliquer aux utilisateurs lorsque AAA ne renvoie pas d'attribut CLASSID. La longueur doit être comprise entre 4 et 15 caractères alphanumériques. Si vous ne spécifiez pas de stratégie de groupe par défaut et qu'il n'y a pas de CLASSID, l'ASA ne peut pas établir la session.

- Authorization Settings (Paramètres d'autorisation) : définissez les valeurs des noms d'utilisateur que l'ASA reconnaît pour l'autorisation. Cela s'applique aux utilisateurs qui s'authentifient à l'aide de certificats numériques et nécessitent une autorisation LDAP ou RADIUS.
  - Use the entire DN as the username (Utiliser le DN entier comme nom d'utilisateur) : sélectionnez cette option pour utiliser le nom distinctif pour l'autorisation.
  - Specify individual DN fields as the username (Préciser les champs DN individuels comme nom d'utilisateur) : sélectionnez cette option pour spécifier des champs DN particuliers pour l'autorisation de l'utilisateur.

    Vous pouvez choisir deux champs de nom distinctif, principal et secondaire. Par exemple, si vous choisissez EA, les utilisateurs s'authentifient en fonction de leur adresse courriel. Dans ce cas, un utilisateur portant le nom commun (CN) de John Doe et une adresse de courriel johndoe@cisco.com ne peut pas s'authentifier en tant que John Doe ou johndoe. Il doit s'authentifier en tant que johndoe@cisco.com. Si vous choisissez EA et O, M. Doe doit s'authentifier en tant que johndoe@cisco.com et Cisco Systems, Inc.
  - Primary DN Field (Champ DN principal) : sélectionnez le champ DN principal que vous souhaitez configurer pour l'autorisation. La valeur par défaut est CN. Les options disponibles sont les suivantes :

Champ DN	Définition
Pays (C)	L'abréviation du pays à deux lettres. Ces codes sont conformes aux abréviations de pays ISO 3166.
Nom usuel	Le nom d'une personne, d'un système ou d'une autre entité. Il s'agit du niveau le plus bas (le plus spécifique) dans la hiérarchie d'identification.
DNQ (Qualificatif du DN)	Un attribut de DN spécifique.
Adresses de courriel (EA)	L'adresse courriel de la personne, du système ou de l'entité qui possède le certificat.
GENQ (Qualificatif générationnel)	Un attribut générationnel tel que Jr., Sr. ou III.
Prénom (GN)	Le prénom du propriétaire du certificat.
Initiales (I)	Les premières lettres de chaque partie du nom du propriétaire du certificat.
Localité	La ville ou la localité où se trouve l'organisation.
Nom (N)	Le nom du propriétaire du certificat.
Organisation	Le nom de l'entreprise, de l'établissement, de l'agence, de l'association ou de toute autre entité.
Unité organisationnelle	Le sous-groupe dans l'organisation.
Numéro de série (SER)	Le numéro de série du certificat.
Nom de famille (SN)	Le nom de famille ou le nom de famille du propriétaire du certificat.
État/Province (S/P)	L'état ou la province où se trouve l'organisation.

Champ DN	Définition
Titre (T)	Le titre du propriétaire du certificat, par exemple, Dr.
Identifiant de l'utilisateur (UID)	Le numéro d'identification du propriétaire du certificat.

- Secondary DN Field (Champ DN secondaire) : (facultatif) sélectionnez le champ DN secondaire que vous souhaitez configurer pour l'autorisation. La valeur par défaut est (OU). Les options comprennent toutes celles du tableau précédent, avec l'ajout de **None** (Aucun), que vous choisissez si vous ne souhaitez pas inclure de champ secondaire.

Identifier les interfaces pour le serveur proxy de messagerie

L'écran Email Proxy Access (Accès au serveur proxy de messagerie) vous permet d'identifier les interfaces sur lesquelles configurer le serveur proxy de messagerie. Vous pouvez configurer et modifier des serveurs proxy de messagerie sur des interfaces individuelles, et vous pouvez configurer et modifier des serveurs proxy de messagerie pour une interface, puis appliquer vos paramètres à toutes les interfaces. Vous ne pouvez pas configurer de serveur proxy de messagerie pour les interfaces de gestion uniquement ou pour les sous-interfaces.

Procédure

Étape 1 Accédez à **Configuration** > **VPN** > **E-Mail Proxy** > **Access** (Configuration > VPN > Serveur proxy de messagerie > Accès) pour afficher ce qui est activé pour les interfaces.

- Interface : affiche les noms de toutes les interfaces configurées.
- POP3S Enabled (POP3S activé) : affiche si POP3S est activé pour l'interface.
- IMAP4S Enabled (IMAP4S activé) : affiche si IMAP4S est activé pour l'interface.
- SMTPS Enabled (SMTPS activé) : affiche si SMTPS est activé pour l'interface.

Étape 2 Cliquez sur **Edit** (Modifier) pour modifier les paramètres du serveur proxy de messagerie pour l'interface en surbrillance.

Configurer l'authentification pour le serveur proxy de messagerie

Configurez les méthodes d'authentification pour chacun des types de serveur proxy de messagerie.

Procédure

Étape 1 Accédez à **Configuration** > **Features** > **VPN** > **E-mail Proxy** > **Authentication** (Configuration > Fonctionnalités > VPN > Mandataire de messagerie > Authentification).

Étape 2 Choisissez parmi les multiples méthodes d'authentification :

- AAA —sélectionnez cette option pour exiger l'authentification AAA. Cette option nécessite un serveur AAA configuré. L'utilisateur présente un nom d'utilisateur, un serveur et un mot de passe. Les utilisateurs doivent présenter à la fois le nom d'utilisateur VPN et le nom d'utilisateur de courriel, séparés par le délimiteur de nom VPN, uniquement si les noms d'utilisateur sont différents l'un de l'autre.
- Certificate (Certificat) : sélectionnez cette option pour exiger l'authentification par certificat.

  Remarque
  L'authentification par certificat ne fonctionne pas pour les serveurs proxy de messagerie dans la version logicielle ASA actuelle.

  L'authentification par certificat exige que les utilisateurs disposent d'un certificat que l'ASA peut valider pendant la négociation SSL. Vous pouvez utiliser l'authentification par certificat comme seule méthode d'authentification pour le serveur proxy SMTPS. Les autres serveurs proxy de messagerie nécessitent deux méthodes d'authentification.

  L'authentification des certificats nécessite trois certificats, tous provenant de la même autorité de certification :

  - Un certificat d'autorité de certification sur l'ASA.

  - Un certificat d'autorité de certification sur le PC client.

  - Un certificat de navigateur Web sur le PC client, parfois appelé certificat personnel ou certificat de navigateur Web.
- Piggyback HTTPS (Authentification superposée HTTPS) : sélectionnez cette option pour exiger une authentification superposée.

  Ce schéma d'authentification exige qu'un utilisateur ait déjà établi une session VPN SSL sans client. L'utilisateur présente uniquement un nom d'utilisateur de courriel. Aucun mot de passe n'est requis. Les utilisateurs doivent présenter à la fois le nom d'utilisateur VPN et le nom d'utilisateur de courriel, séparés par le délimiteur de nom VPN, uniquement si les noms d'utilisateur sont différents l'un de l'autre.

  IMAP génère un nombre de sessions qui ne sont pas limitées par le nombre d'utilisateurs simultanés, mais qui sont prises en compte dans le nombre de connexions simultanées autorisées pour un nom d'utilisateur. Si le nombre de sessions IMAP dépasse ce maximum et que la connexion VPN SSL sans client expire, un utilisateur ne peut pas établir de nouvelle connexion par la suite. Il existe plusieurs solutions :

  Le courriel SMTPS utilise le plus souvent l'authentification superposée, car la plupart des serveurs SMTP ne permettent pas aux utilisateurs de se connecter.

  Remarque
  IMAP génère un nombre de sessions qui ne sont pas limitées par le nombre d'utilisateurs simultanés, mais qui sont prises en compte dans le nombre de connexions simultanées autorisées pour un nom d'utilisateur. Si le nombre de sessions IMAP dépasse ce maximum et que la connexion VPN SSL sans client expire, un utilisateur ne peut pas établir de nouvelle connexion par la suite. Il existe plusieurs solutions :

- L'utilisateur peut fermer l'application IMAP pour effacer les sessions avec l'ASA, puis établir une nouvelle connexion VPN SSL sans client.

  L'administrateur peut augmenter les connexions simultanées pour les utilisateurs IMAP (Configuration > Features > VPN > General > Group Policy > Edit Group Policy > General [Configuration > Fonctionnalités > VPN > Général > Stratégie de groupe > Modifier la stratégie de groupe > Général]).

  – Désactivez l'authentification HTTPS/empilage pour le serveur proxy de messagerie.

- Mailhost (hôte de messagerie) : (SMTPS uniquement) sélectionnez cette option pour exiger l'authentification de l'hôte de messagerie. Cette option s'affiche uniquement pour SMTPS, car POP3S et IMAP4S effectuent toujours l'authentification de l'hôte de messagerie. Il nécessite le nom d'utilisateur de courriel, le serveur et le mot de passe de l'utilisateur.

Identifier les serveurs proxy

Ce panneau Default Server (Serveur par défaut) vous permet d'identifier les serveurs proxy auprès de l'ASA et de configurer un serveur par défaut, un port et une limite de session non authentifiée pour les serveurs proxy de messagerie.

Procédure

Étape 1 Accédez à **Configuration** > **Features** > **(Fonctionnalités de configuration)** > **VPN** > **E-mail Proxy (Proxy de messagerie)** > **Default Servers (Serveurs par défaut).**

Étape 2 Configurez les champs suivants :

- Name or IP Address (Nom ou adresse IP) : saisissez le nom DNS ou l'adresse IP du serveur proxy de messagerie par défaut.
- Port : saisissez le numéro de port sur lequel l'ASA écoute le trafic du serveur proxy de messagerie. Les connexions sont automatiquement autorisées sur le port configuré. Le serveur proxy de messagerie autorise uniquement les connexions SSL sur ce port. Une fois le tunnel SSL établi, le serveur proxy de messagerie démarre, puis l'authentification a lieu.

  Les valeurs par défaut sont les suivantes :

  - 995 (pour POP3S)
  - 993 (pour IMAP4S)
  - 988 (pour SMTPS)

- Enable non-authenticated session limit (Activer la limite de session non authentifiée) : sélectionnez cette option pour restreindre le nombre de sessions de serveur proxy de messagerie non authentifiées. Vous permet de définir une limite pour les sessions en cours d'authentification, empêchant ainsi les attaques DOS. Lorsqu'une nouvelle session dépasse la limite définie, l'ASA met fin à la connexion non authentifiée la plus ancienne. S'il n'existe aucune connexion non authentifiée, la connexion en cours d'authentification la plus ancienne est terminée sans mettre fin aux sessions authentifiées.

Les connexions du serveur proxy de messagerie ont trois états :

- Unauthenticated (Non authentifié) : état des nouvelles connexions par courriel.
- Authenticating (Authentification) : état lorsque la connexion présente un nom d'utilisateur.
- Authenticated (Authentifié) : état lorsque l'ASA authentifie la connexion.

Configurer les délimiteurs

Ce panneau configure les délimiteurs de nom d'utilisateur/mot de passe et les délimiteurs de serveur pour l'authentification du serveur proxy de messagerie.

Procédure

Étape 1 Accédez à **Configuration** > **Features** > **(Fonctionnalités de configuration)** > **VPN** > **E-mail Proxy (Serveur proxy de messagerie VPN)** > **Delimiters (Délimiteurs).**

Étape 2 Configurez les champs suivants :

- Délimiteur de nom d'utilisateur/mot de passe : sélectionnez un délimiteur pour séparer le nom d'utilisateur du VPN du nom d'utilisateur du courriel. Les utilisateurs ont besoin des deux noms d'utilisateur lors de l'utilisation de l'authentification AAA pour le serveur proxy de messagerie, et le nom d'utilisateur du VPN et le nom d'utilisateur du courriel sont différents. Lorsqu'ils se connectent à une session de serveur proxy de messagerie, les utilisateurs saisissent les deux noms d'utilisateur, séparés par le délimiteur que vous configurez ici, ainsi que le nom du serveur de messagerie.

  Remarque
  Les mots de passe des utilisateurs du serveur proxy de messagerie VPN SSL sans client ne peuvent pas contenir de caractères utilisés comme délimiteur.

- Délimiteur de serveur : sélectionnez un délimiteur pour séparer le nom d'utilisateur du nom du serveur de messagerie. Il doit être différent du délimiteur de nom VPN. Les utilisateurs saisissent leur nom d'utilisateur et leur serveur dans le champ de nom d'utilisateur lorsqu'ils se connectent à une session de serveur proxy de messagerie.

  Par exemple, en utilisant : comme limiteur de nom VPN et @ comme limiteur de serveur, lors de la connexion à un programme de messagerie par courriel proxy, les utilisateurs saisiraient leur nom d'utilisateur au format suivant : vpn_username:e-mail_username@server.

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.