

Introduction aux services de pare-feu Secure Firewall ASA

Les services de pare-feu sont les fonctionnalités de l'ASA axées sur le contrôle de l'accès au réseau, y compris les services qui bloquent le trafic et les services qui permettent le flux du trafic entre les réseaux internes et externes. Ces services comprennent ceux qui protègent le réseau contre les menaces, telles que le déni de service (DoS) et d'autres attaques.

Les rubriques suivantes fournissent un aperçu des services de pare-feu.

- Comment mettre en œuvre les services de pare-feu, à la page 1
- Contrôle d'accès de base, à la page 2
- Filtrage URL, à la page 2
- Protection contre les menaces, à la page 2
- Services de pare-feu pour les environnements virtuels, à la page 3
- NAT (Network Address Translation; Translation d'adresses de réseau), à la page 4
- Inspection des applications, à la page 4
- Scénario d'utilisation : exposer un serveur au public, à la page 5

Comment mettre en œuvre les services de pare-feu

La procédure suivante fournit une séquence générale pour la mise en œuvre des services de pare-feu. Cependant, chaque étape est facultative et n'est nécessaire que si vous souhaitez fournir le service à votre réseau.

Avant de commencer

Configurez l'ASA conformément au guide de configuration sur les opérations générales, y compris au minimum les paramètres de base, la configuration de l'interface, le routage et l'accès de gestion.

Procédure

Étape 1 Implémentez le contrôle d'accès pour le réseau. Consultez Contrôle d'accès de base, à la page 2.

Étape 2 Implémentez le filtrage d'URL. Consultez Filtrage URL, à la page 2.

Étape 3 Implémentez la protection contre les menaces. Consultez Protection contre les menaces, à la page 2.

Étape 4 Implémentez des services de pare-feu adaptés aux environnements virtuels. Consultez Services de pare-feu pour les environnements virtuels, à la page 3.

Étape 5 Implémentez la traduction d'adresses réseau (NAT). Consultez NAT (Network Address Translation; Translation d'adresses de réseau), à la page 4.

Étape 6 Implémentez l'inspection d'application si les paramètres par défaut sont insuffisants pour votre réseau. Consultez Inspection des applications, à la page 4.

Contrôle d'accès de base

Les règles d'accès, appliquées par interface ou globalement, sont votre première ligne de défense. Vous pouvez abandonner, à l'entrée, des types de trafic spécifiques ou le trafic provenant d'hôtes ou de réseaux spécifiques, ou à destination de ceux-ci. Par défaut, l'ASA permet au trafic de circuler librement d'un réseau interne (niveau de sécurité supérieur) vers un réseau externe (niveau de sécurité inférieur).

Vous pouvez appliquer des critères d'accès pour limiter le trafic de l'intérieur vers l'extérieur ou autoriser le trafic de l'extérieur vers l'intérieur.

Les règles d'accès de base contrôlent le trafic à l'aide d'un « 5-tuple » de l'adresse source et du port, de l'adresse et du port de destination et du protocole. Consultez Règles d'accès et Listes de contrôle d'accès.

Vous pouvez enrichir vos règles en les rendant compatibles avec l'identité. Pour mettre en œuvre le contrôle d'identité, installez Cisco Identity Services Engine (ISE) sur un serveur distinct pour mettre en œuvre Cisco TrustSec. Vous pouvez ensuite ajouter des critères de groupe de sécurité à vos règles d'accès. Consultez ASA et Cisco TrustSec.

Filtrage URL

Le filtrage d'URL refuse ou autorise le trafic en fonction de l'URL du site de destination.

Pour mettre en œuvre le filtrage d'URL, abonnez-vous au service Cisco Umbrella, où vous configurez la politique de sécurité entreprise pour bloquer les sites malveillants en fonction du nom de domaine complet (FQDN). Vous pouvez autoriser ou bloquer les connexions en fonction du FQDN ou, pour les FQDN suspects, vous pouvez rediriger l'utilisateur vers le mandataire intelligent Cisco Umbrella, qui peut effectuer le filtrage d'URL. Le service Cisco Umbrella fonctionne par la gestion des demandes de recherche DNS des utilisateurs, en renvoyant l'adresse IP d'une page de blocage ou l'adresse IP du serveur proxy intelligent. Le service renvoie l'adresse IP réelle d'un nom de domaine complet (FQDN) pour les domaines autorisés. Consultez Cisco Umbrella.

Protection contre les menaces

Vous pouvez mettre en œuvre un certain nombre de mesures pour vous protéger contre l'analyse, le déni de service (DoS) et d'autres attaques. Un certain nombre de fonctionnalités ASA aident à protéger contre les attaques en appliquant des limites de connexion et en abandonnant des paquets TCP anormaux. Certaines fonctionnalités sont automatiques, d'autres sont configurables, mais ont des valeurs par défaut appropriées dans la plupart des cas, tandis que d'autres sont entièrement facultatives et vous devez les configurer si vous le souhaitez.

Voici les services de protection contre les menaces disponibles avec l'ASA.

- Protection contre la fragmentation des paquets IP : l'ASA effectue le réassemblage complet de tous les messages d'erreur ICMP et le réassemblage virtuel des fragments IP restants qui sont acheminés par l'ASA, et rejette les fragments qui échouent au contrôle de sécurité. Aucune configuration n'est nécessaire.
- Limites de connexion, normalisation TCP et autres fonctionnalités liées à la connexion : configurez les services liés à la connexion tels que les limites et les délais d'expiration de connexion TCP et UDP, l'aléatoireisation du numéro de séquence TCP, la normalisation TCP et le contournement de l'état TCP. La normalisation TCP est conçue pour abandonner les paquets qui ne semblent pas normaux. Consultez Paramètres de connexion.

  Par exemple, vous pouvez limiter les connexions TCP et UDP et les connexions amorces (une demande de connexion qui n'a pas terminé l'établissement de liaison entre la source et la destination). La limitation du nombre de connexions et de connexions amorces vous protège contre les attaques DoS. L'ASA utilise la limite amorce pour déclencher l'interception TCP, qui protège les systèmes internes contre une attaque DoS perpétrée en inondant une interface de paquets SYN de TCP.
- Détection des menaces : mettez en œuvre la détection des menaces sur l'ASA pour recueillir des statistiques afin d'identifier les attaques. La détection de base des menaces est activée par défaut, mais vous pouvez mettre en œuvre des statistiques avancées et une détection des menaces d'analyse. Vous pouvez bloquer les hôtes identifiés comme une menace d'analyse. Consultez Détection des menaces.

Services de pare-feu pour les environnements virtuels

Les environnements virtuels déploient des serveurs en tant que machines virtuelles, par exemple, dans VMware ESXi. Les pare-feu dans un environnement virtuel peuvent être des périphériques matériels classiques ou des pare-feu de machines virtuelles, comme ASA virtuel.

Les services de pare-feu traditionnel et de nouvelle génération s'appliquent aux environnements virtuels de la même manière qu'ils s'appliquent aux environnements qui n'utilisent pas de serveurs de machines virtuelles. Cependant, les environnements virtuels peuvent présenter des défis supplémentaires, car il est facile de créer et de démonter des serveurs.

En outre, le trafic entre les serveurs au sein du centre de données peut nécessiter autant de protection que le trafic entre le centre de données et les utilisateurs externes. Par exemple, si un agresseur prend le contrôle d'un serveur dans le centre de données, cela pourrait ouvrir des attaques sur d'autres serveurs du centre de données.

Les services de pare-feu pour les environnements virtuels ajoutent des fonctionnalités pour appliquer une protection de pare-feu spécifiquement aux machines virtuelles. Voici les services de pare-feu disponibles pour les environnements virtuels :

- Contrôle d'accès basé sur les attributs : vous pouvez configurer des objets réseau pour qu'ils correspondent au trafic en fonction des attributs et utiliser ces objets dans les règles de contrôle d'accès. Cela vous permet de dissocier les règles de pare-feu de la topologie du réseau. Par exemple, vous pouvez autoriser tous les hôtes avec l'attribut Engineering à accéder aux hôtes avec l'attribut Lab Server. Vous pourriez ensuite ajouter ou supprimer des hôtes avec ces attributs et la politique de pare-feu serait appliquée automatiquement sans qu'il soit nécessaire de mettre à jour les règles d'accès. Pour en savoir plus, consultez Contrôle d'accès basé sur les attributs.

NAT (Network Address Translation; Translation d'adresses de réseau)

L'une des fonctions principales de la traduction d'adresses réseau (NAT) est de permettre aux réseaux IP privés de se connecter à Internet. La NAT remplace une adresse IP privée par une adresse IP publique, en transformant les adresses privées du réseau privé interne en adresses légales et routables qui peuvent être utilisées sur l'Internet public. De cette façon, la NAT conserve les adresses publiques, car elle peut être configurée pour annoncer au moins une adresse publique pour l'ensemble du réseau vers le monde extérieur.

Les autres fonctions de la NAT comprennent :

- Sécurité : le fait de garder les adresses IP internes masquées détourne les attaques directes.
- Solutions de routage IP : les adresses IP qui se chevauchent ne sont pas un problème lorsque vous utilisez la NAT.
- Souplesse : vous pouvez modifier les schémas d'adressages IP internes sans affecter les adresses publiques disponibles en externe. par exemple, pour un serveur accessible à Internet, vous pouvez conserver une adresse IP fixe pour l'utilisation d'Internet, mais à l'interne, vous pouvez modifier l'adresse du serveur.
- Traduction entre IPv4 et IPv6 (mode routé uniquement) : si vous souhaitez connecter un réseau IPv6 à un réseau IPv4, la NAT vous permet de traduire entre les deux types d'adresses.

La NAT n'est pas requise. Si vous ne configurez pas la NAT pour un ensemble donné de trafic, ce trafic ne sera pas traduit, mais toutes les politiques de sécurité seront appliquées normalement.

Voir :

- Traduction d'adresses réseau (NAT)
- Exemples et références de NAT

Inspection des applications

Des plateformes d'inspection sont nécessaires pour les services qui intègrent des renseignements d'adressage IP dans le paquet de données des utilisateurs ou qui ouvrent des canaux secondaires sur des ports attribués de manière dynamique. Ces protocoles obligent l'ASA à effectuer une inspection approfondie des paquets, à ouvrir les passages requis et à appliquer la traduction d'adresses réseau (NAT).

La politique d'ASA par défaut applique déjà l'inspection globalement pour de nombreux protocoles courants, tels que DNS, FTP, SIP, ESMTP, TFTP, etc. Les inspections par défaut peuvent être tout ce dont vous avez besoin pour votre réseau.

Cependant, vous devrez peut-être activer l'inspection pour d'autres protocoles ou affiner une inspection. De nombreuses inspections comprennent des options détaillées qui vous permettent de contrôler les paquets en fonction de leur contenu. Si vous connaissez bien un protocole, vous pouvez appliquer un contrôle fin à ce trafic.

Vous utilisez des politiques de service pour configurer l'inspection des applications. Vous pouvez configurer une politique de service globale ou appliquer une politique de service à chaque interface, ou les deux.

Voir :

- Politique de service
- Premiers pas avec l'inspection du protocole de la couche application
- Inspection des protocoles Internet de base
- Inspection des protocoles vocaux et vidéo
- Inspection des réseaux mobiles.

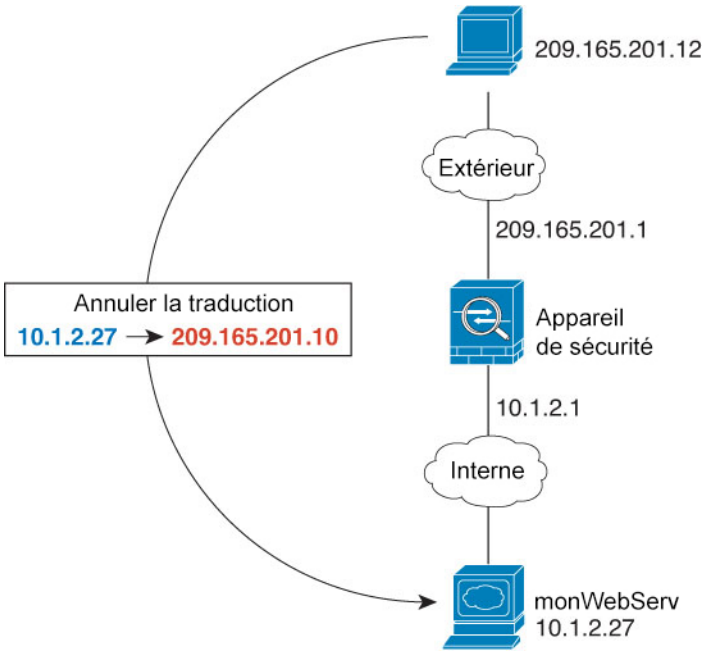
Scénario d'utilisation : exposer un serveur au public

Vous pouvez mettre certains services d'applications sur un serveur à la disposition du public. Par exemple, vous pourriez exposer un serveur Web, afin que les utilisateurs puissent se connecter aux pages Web, mais ne puissent effectuer aucune autre connexion au serveur.

Pour exposer un serveur au public, vous devez généralement créer des règles d'accès qui autorisent la connexion et des règles NAT qui assurent la traduction entre l'adresse IP interne du serveur et une adresse externe que le public peut utiliser. En outre, vous pouvez utiliser la traduction d'adresses de port (PAT) pour mapper un port interne à un port externe, si vous ne souhaitez pas que le service exposé à l'extérieur utilise le même port que le serveur interne. Par exemple, si le serveur Web interne ne fonctionne pas sur TCP/80, vous pouvez le mapper à TCP/80 pour faciliter les connexions pour les utilisateurs externes.

L'exemple suivant rend un serveur Web du réseau privé interne accessible au public.

Illustration 1 : NAT statique pour un serveur Web interne



ASDM comprend un raccourci pour configurer les règles d'accès et de NAT requises, afin de simplifier le processus d'exposition d'un service sur un serveur interne au public.

Procédure

Étape 1 Choisissez **Configuration** > **Firewall (Pare-feu)** > **Public Servers (Serveurs publics)**.

Étape 2 Cliquez sur **Add** (ajouter).

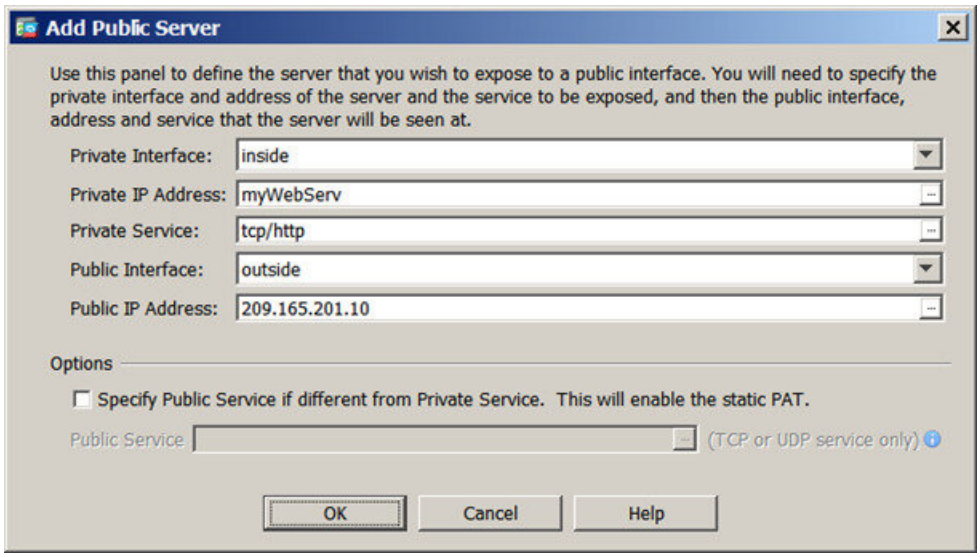
Étape 3 Définissez les caractéristiques privées et publiques du service que vous exposez.

- **Interface privée** : l'interface à laquelle le serveur réel est connecté. Dans cet exemple, « inside » (interne).
- **Adresse IP privée** : objet du réseau de l'hôte qui définit l'adresse IPv4 réelle du serveur. Vous ne pouvez pas préciser une adresse IPv6. Si vous n'avez pas encore d'objet contenant l'adresse, créez-en un en cliquant sur le bouton « ... », puis en cliquant sur **Add** (Ajouter). Dans cet exemple, le nom de l'objet serait MyWebServ et contiendrait l'adresse d'hôte 10.1.2.27.
- **Service privé** : le service réel qui est en cours d'exécution sur le serveur réel. Vous pouvez utiliser un service ou un objet de service prédéfini. Vous pouvez également utiliser un groupe d'objets de service, sauf si vous spécifiez également un service public auquel vous mappez le service privé.

  Vous pouvez exposer plusieurs services; toutefois, si vous spécifiez un service public, tous les ports sont mappés au même port public.

  Dans cet exemple, le port est **tcp/http**.
- **Interface publique** : l'interface par laquelle les utilisateurs externes peuvent accéder au serveur réel. Dans cet exemple, « outside » (externe).
- **Adresse publique** : l'adresse IPv4 vue par les utilisateurs externes. Vous pouvez spécifier l'adresse directement ou utiliser un objet réseau hôte. Dans cet exemple, l'adresse externe est 209.165.201.10.
- **Précisez le service public s'il est différent du service privé**, **le service public** : le service qui est en cours d'exécution sur l'adresse traduite. Précisez le service public uniquement s'il diffère du service privé. Par exemple, si le serveur Web privé fonctionne sur TCP/80 et que vous souhaitez utiliser le même port pour les utilisateurs externes, il n'est pas nécessaire de préciser le service public. Vous devez utiliser un service TCP ou UDP prédéfini si vous spécifiez un service public. Cet exemple n'utilise pas la traduction de port, alors ne sélectionnez pas cette option.

La boîte de dialogue doit ressembler à ce qui suit :



Étape 4 Cliquez sur **OK**, puis sur **Apply** (Appliquer).

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.