Introduction à Secure Firewall ASA

Le Secure Firewall ASA offre des fonctionnalités avancées de pare-feu dynamique et de concentrateur VPN dans un seul appareil. L'ASA comprend de nombreuses fonctionnalités avancées, comme des contextes de sécurité multiples (semblables aux pare-feu virtualisés), la mise en grappe (combinaison de plusieurs pare-feu en un seul pare-feu), les pare-feu transparents (couche 2) ou routés (couche 3), les moteurs d'inspection avancés, IPsec Prise en charge de VPN, de VPN SSL et de VPN SSL sans client et de nombreuses autres fonctionnalités.

Compatibilité matérielle et logicielle

Pour obtenir la liste complète du matériel et des logiciels pris en charge, consultez la section Compatibilité Cisco ASA.

Compatibilité VPN

Consultez Plateformes VPN prises en charge, série Cisco ASA.

Nouvelles fonctionnalités

Cette section énumère les nouvelles fonctionnalités de chaque version.

Remarque Les messages syslog nouveaux, modifiés et obsolètes sont répertoriés dans le guide des messages syslog.

Nouvelles fonctionnalités dans l'ASA 9.19(1)

Publication : 29 novembre 2022

Fonctionnalités	Description
Caractéristiques de la plateforme	
Secure Firewall 3105	Nous avons présenté l'ASA pour le Secure Firewall 3105.
Solution virtuelle ASA Auto Scale avec équilibreur de charge de la passerelle Azure	Vous pouvez maintenant déployer la solution virtuelle ASA Auto Scale avec équilibreur de charge de la passerelle sur Microsoft Azure. Consultez les fonctionnalités Interfaces pour en savoir plus.
Caractéristiques du pare-feu	
Soutien aux groupes de service du réseau	Vous pouvez désormais définir un maximum de 1 024 groupes de services réseau.
Fonctionnalités de haute disponibilité et d'évolutivité	
Suppression des propos tendancieux	Les commandes, les sorties de commande et les messages syslog qui contenaient les termes « Master » (maître) et « Slave » (esclave) ont été remplacés par « Control » (contrôle) et « Data » (données). Commandes nouvelles/modifiées : **cluster control-node**, **enable as-data-node**, **prompt**, **show cluster history**, **show cluster info**
Regroupement virtuel d'ASA sur Amazon Web Services (AWS)	L'ASA virtuel prend en charge le regroupement d'interfaces individuelles pour un maximum de 16 nœuds sur AWS. Vous pouvez utiliser la mise en grappe avec ou sans équilibreur de charge de la passerelle AWS.
Fonctionnalités de routage	
Prise en charge du redémarrage progressif de BGP pour IPv6	Nous avons ajouté la prise en charge du redémarrage progressif de BGP pour la famille d'adresses IPv6. Commandes nouvelles/modifiées : Commande existante, étendue à la prise en charge de la famille IPv6 : **ha-mode graceful-restart**
Caractéristiques de l'interface	
Prise en charge virtuelle de l'IPv6 par l'ASA	ASAv pour prendre en charge le protocole réseau IPv6 sur les plateformes du nuage privé et public. Les utilisateurs peuvent désormais : • Activer et configurer une adresse de gestion IPv6 via la configuration day0. • Attribuer des adresses IPv6 à l'aide de méthodes DHCP et statiques.

Fonctionnalités	Description
Proxy jumelé VXLAN pour l'ASA virtuel pour l'équilibreur de charges de la passerelle Azure.	Vous pouvez configurer une interface VXLAN en mode proxy apparié pour l'ASA virtuel dans Azure afin de l'utiliser avec l'équilibreur de charges de la passerelle Azure (GWLB). L'ASA virtuel définit une interface externe et une interface interne sur un seul NIC en utilisant des segments VXLAN dans un serveur mandataire jumelé. Commandes nouvelles/modifiées : **port externe, segment-id externe, port interne, segment-id interne, proxy paired**
La correction d'erreur par défaut (FEC) sur les ports fixes du Secure Firewall 3100 est passée de cl74-fc à cl108-rs pour les émetteurs-récepteurs SR, CSR et LR de 25 Go+.	Lorsque vous définissez le FEC sur Auto sur les ports fixes du Secure Firewall 3100, le type par défaut est désormais défini sur cl108-rs au lieu de cl74-fc pour les émetteurs-récepteurs SR, CSR et LR de 25 Go. Commandes nouvelles/modifiées : **fec**
Caractéristiques de la licence	
Prise en charge de la réservation de licences virtuelles permanentes pour l'ASAv5 sur KVM et VMware	Une nouvelle commande est disponible que vous pouvez exécuter pour remplacer la licence DPP par défaut et demander à Cisco Smart Software Manager (SSM) d'envoyer une licence DPP ASAv5 lorsque vous déployez ASAv avec 2GB RAM sur KVM et VMware. Vous pouvez modifier la même commande en ajoutant la forme <*no*> pour rétablir la licence de l'ASAv5 à la licence DPP par défaut en fonction de la configuration de la mémoire vive.
Fonctions d'administration, de surveillance et de dépannage	
Pile CiscoSSH maintenant par défaut	La pile Cisco SSH est maintenant utilisée par défaut. Commandes nouvelles ou modifiées : **ssh stack ciscossh**
Fonctionnalités du VPN	
Prise en charge de l'interface de bouclage VTI	Vous pouvez désormais définir une interface de bouclage comme interface source pour un VTI. La possibilité d'hériter de l'adresse IP d'une interface de bouclage au lieu d'une adresse IP configurée de manière statique a également été ajoutée. L'interface de boucle avec retour permet de résoudre les échecs de chemin. Si une interface tombe en panne, vous pouvez accéder à toutes les interfaces grâce à l'adresse IP attribuée à l'interface de boucle avec retour. Commandes nouvelles/modifiées : **tunnel source interface**, **ip unnumbered**, **ipv6 unnumbered**
Prise en charge de l'interface de tunnel virtuel dynamique (VTI dynamique)	L'ASA est améliorée grâce à l'ITV dynamique. Un seul VTI dynamique peut remplacer plusieurs configurations de VTI statique sur le concentrateur. Vous pouvez ajouter de nouveaux satellites à un concentrateur sans modifier la configuration du concentrateur. Dynamique VTI prend en charge les rayons dynamiques (DHCP). Commandes nouvelles/modifiées : **interface virtual-Template, ip unnumbered, ipv6 unnumbered, tunnel protection ipsec policy.**
Support VTI pour EIGRP et OSPF	Le routage EIGRP et OSPFv2/v3 est désormais pris en charge sur l'interface du tunnel virtuel. Vous pouvez maintenant utiliser ces protocoles de routage pour partager les informations de routage et pour acheminer le flux de trafic à travers le tunnel VPN basé sur VTI entre les pairs.

Fonctionnalités	Description
TLS 1.3 dans le VPN d'accès à distance	Vous pouvez désormais utiliser TLS 1.3 pour chiffrer les connexions VPN d'accès à distance. TLS 1.3 ajoute la prise en charge des chiffrements suivants : • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256 • TLS_AES_256_GCM_SHA384 Cette fonctionnalité nécessite Cisco Secure Client, version 5.0.01242 ou ultérieure. Commandes nouvelles/modifiées : **sslserver-version, sslclient-version**.
Prise en charge de la double pile pour les clients tiers IKEv2	Secure Firewall ASA prend désormais en charge les demandes d'IP à double pile provenant de clients VPN d'accès à distance tiers IKEv2. Si le client VPN d'accès à distance tiers demande des adresses IPv4 et IPv6, l'ASA peut désormais attribuer les deux versions d'adresses IP à l'aide de plusieurs sélecteurs de trafic. Cette fonction permet aux clients VPN d'accès à distance tiers d'envoyer des données IPv4 et IPv6 par le biais d'un seul tunnel IPsec. Commandes nouvelles/modifiées : **show crypto ikev2 sa, show crypto ipsec sa, show vpn-sessiondb ra-ikev2-ipsec**.
Sélecteur de trafic pour l'interface VTI statique	Vous pouvez maintenant attribuer un sélecteur de trafic à une interface VTI statique. Commandes nouvelles/modifiées : **tunnel protection ipsec policy**.
Spécifier la version maximum du protocole SSL/TLS	Vous pouvez désormais spécifier la version maximum du protocole SSL/TLS que l'ASA peut utiliser en tant que client ou serveur. Commandes nouvelles ou modifiées : **ssl client-max-version, ssl client-max-version**.

Présentation fonctionnelle du pare-feu

Les pare-feu protègent les réseaux internes contre les accès non autorisés par des utilisateurs d'un réseau externe. Un pare-feu peut également protéger les réseaux internes les uns des autres, par exemple en séparant le réseau des ressources humaines du réseau des utilisateurs. Si vous avez des ressources réseau qui doivent être disponibles pour un utilisateur externe, comme un serveur Web ou FTP, vous pouvez placer ces ressources sur un réseau distinct derrière le pare-feu, appelé *zone démilitarisée* (DMZ). Le pare-feu permet un accès limité à la DMZ, mais comme celle-ci ne comprend que les serveurs publics, une attaque à cet endroit n'affecte que les serveurs et n'affecte pas les autres réseaux internes. Vous pouvez également contrôler quand les utilisateurs internes accèdent aux réseaux externes (par exemple, l'accès à Internet), en n'autorisant que certaines adresses, en exigeant une authentification ou une autorisation, ou en effectuant une coordination avec un serveur de filtrage d'URL externe.

Lorsqu'il est question de réseaux connectés à un pare-feu, le réseau *externe* se trouve devant le pare-feu, le réseau *interne* est protégé et se trouve derrière le pare-feu, et une *DMZ*, bien que située derrière le pare-feu, permet un accès limité aux utilisateurs externes. Étant donné que l'ASA vous permet de configurer de nombreuses interfaces avec des politiques de sécurité variées, y compris de nombreuses interfaces internes, de nombreuses DMZ et même de nombreuses interfaces externes si vous le souhaitez, ces termes sont utilisés dans un sens général uniquement.

Présentation de la politique de sécurité

Une politique de sécurité détermine quel trafic est autorisé à traverser le pare-feu pour accéder à un autre réseau. 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 actions au trafic pour personnaliser la politique de sécurité.

Autorisation ou refus de trafic avec critères d'accès

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. Pour les interfaces de groupe de ponts, vous pouvez également appliquer un critère d'accès EtherType pour autoriser le trafic non IP.

Application de la NAT

Voici quelques avantages de la NAT :

- Vous pouvez utiliser des adresses privées sur vos réseaux internes. Les adresses privées ne sont pas routables sur Internet.
- La NAT masque les adresses locales des autres réseaux afin que les agresseurs ne puissent pas découvrir l'adresse réelle d'un hôte.
- La NAT peut résoudre les problèmes de routage IP en prenant en charge le chevauchement des adresses IP.

Protection contre les fragments IP

L'ASA fournit une protection contre les fragments d'adresse IP. Cette fonctionnalité 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. Les fragments qui échouent à la vérification de sécurité sont abandonnés et enregistrés. Le réassemblage virtuel ne peut pas être désactivé.

Application du filtrage HTTP, HTTPS ou FTP

Bien que vous puissiez utiliser des listes d'accès pour empêcher l'accès sortant à des sites Web ou à des serveurs FTP spécifiques, la configuration et la gestion de l'utilisation du Web de cette manière ne sont pas pratiques en raison de la taille et de la nature dynamique d'Internet.

Vous pouvez configurer les fonctionnalités de sécurisation du web sur l'ASA. Vous pouvez également utiliser l'ASA en conjonction avec un produit externe tel que l'appliance Cisco pour la sécurité du web (WSA).

Application de l'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 exigent que l'ASA effectue une inspection approfondie des paquets.

Application des politiques de QoS

Certains trafics réseau, comme les messages vocaux et le streaming vidéo, ne peuvent pas tolérer de longs temps de latence. La QoS est une fonctionnalité réseau qui vous permet de donner la priorité à ces types de trafic. La QoS renvoie à la capacité d'un réseau à fournir un meilleur service au trafic réseau sélectionné.

Application des limites de connexion et de la normalisation TCP

Vous pouvez limiter les connexions TCP et UDP ainsi que les connexions amorces. 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. Une connexion amorce est une demande de connexion qui n'a pas terminé l'établissement de liaison entre la source et la destination.

La normalisation TCP est une fonctionnalité composée de paramètres de connexion TCP avancés conçus pour abandonner les paquets qui n'apparaissent pas normaux.

Activation de la détection des menaces

Vous pouvez configurer la détection des menaces par analyse et la détection des menaces de base, ainsi que l'utilisation des statistiques pour analyser les menaces.

La détection des menaces de base détecte les activités qui peuvent être liées à une attaque, comme les attaques DoS, et envoie automatiquement un message de journal système.

Une attaque par analyse typique se compose d'un hôte qui teste l'accessibilité de chaque adresse IP d'un sous-réseau (en analysant de nombreux hôtes dans le sous-réseau ou en balayage de nombreux ports dans un hôte ou un sous-réseau). La fonction de détection des menaces par analyse détermine quand un hôte effectue une analyse. Contrairement à la détection d'analyse IPS qui est basée sur les signatures de trafic, la fonction de détection des menaces par analyse ASA gère une base de données étendue qui contient des statistiques d'hôte pouvant être analysées pour l'activité d'analyse.

La base de données d'hôtes suit les activités suspectes telles que les connexions sans activité de retour, l'accès à des ports de service fermés, les comportements TCP vulnérables tels que les IPID non aléatoires, etc.

Vous pouvez configurer l'ASA pour envoyer des messages de journal système sur un agresseur ou vous pouvez banir automatiquement l'hôte.

Présentation du mode pare-feu

L'ASA fonctionne dans deux modes de pare-feu différents :

- Acheminé
- Transparent

En mode routage, l'ASA est considéré comme un saut de routeur dans le réseau.

En mode transparent, l'ASA agit comme une « présence sur le réseau câblé » ou un « pare-feu furtif », et n'est pas considéré comme un saut de routeur. L'ASA se connecte au même réseau sur ses interfaces interne et externe dans un « groupe de ponts ».

Vous pouvez utiliser un pare-feu transparent pour simplifier la configuration de votre réseau. Le mode transparent est également utile si vous souhaitez que le pare-feu soit visible par les agresseurs. Vous pouvez également utiliser un pare-feu transparent pour le trafic qui serait autrement bloqué en mode routé. Par exemple, un pare-feu transparent peut autoriser les flux de multidiffusion à l'aide d'une liste d'accès EtherType.

Le mode routé prend en charge le routage et le ponts intégrés. Vous pouvez donc également configurer des groupes de ponts en mode routé et acheminer le routage entre les groupes de ponts et les interfaces normales. En mode routé, vous pouvez répliquer la fonctionnalité en mode transparent; si vous n'avez pas besoin du mode de contexte multiple ou de la mise en grappe, vous pouvez envisager d'utiliser le mode routé.

Présentation de l'inspection dynamique

Tout le trafic qui passe par l'ASA est inspecté à l'aide de l'algorithme de sécurité adaptatif et est autorisé ou abandonné. Un filtre de paquet simple peut vérifier l'adresse source, l'adresse de destination et les ports appropriés, mais il ne vérifie pas si la séquence ou les indicateurs des paquets sont corrects. Un filtre vérifie également *chaque* paquet par rapport au filtre, ce qui peut être un processus lent.

Remarque La fonction de contournement d'état TCP vous permet de personnaliser le flux de paquet.

Cependant, un pare-feu dynamique comme l'ASA prend en compte l'état d'un paquet :

- S'agit-il d'une nouvelle connexion?

  S'il s'agit d'une nouvelle connexion, l'ASA doit vérifier le paquet par rapport aux listes d'accès et effectuer d'autres tâches pour déterminer si le paquet est autorisé ou refusé. Pour effectuer cette vérification, le premier paquet de la session passe par le « chemin de gestion de session » et, selon le type de trafic, il peut également passer par le « chemin de plan de commande ».

  Le chemin de gestion de session est responsable des tâches suivantes :

  - Effectuer les vérifications de la liste d'accès
  - Effectuer des recherches de route
  - Attribuer des traductions NAT (xlates)
  - Établir des sessions dans le « chemin rapide »

  L'ASA crée des flux de transfert et d'inversion dans le chemin rapide pour le trafic TCP; l'ASA crée également des renseignements sur l'état de connexion pour les protocoles sans connexion comme UDP et ICMP (lorsque vous activez l'inspection ICMP), afin qu'ils puissent également utiliser le chemin rapide.

Remarque Pour les autres protocoles IP, comme SCTP, l'ASA ne crée pas de flux de chemin inverse. Par conséquent, les paquets d'erreur ICMP qui font référence à ces connexions sont abandonnés.

  Certains paquets nécessitant une inspection de couche 7 (la charge utile des paquets doit être inspectée ou modifiée) sont transmis au chemin du plan de commande. Des moteurs d'inspection de couche 7 sont nécessaires pour les protocoles qui ont au moins deux canaux : un canal de données, qui utilise des numéros de port connus, et un canal de contrôle, qui utilise des numéros de port différents pour chaque session. Ces protocoles comprennent FTP, H.323 et SNMP.

- S'agit-il d'une connexion établie?

  Si la connexion est déjà établie, l'ASA n'a pas besoin de revérifier les paquets; la plupart des paquets correspondants peuvent passer par le chemin « rapide » dans les deux sens. Le chemin rapide est responsable des tâches suivantes :

  - Vérification de la somme de contrôle IP
  - Recherche de session

- Vérification du numéros de séquence TCP
- Traductions NAT en fonction des sessions existantes
- Ajustements des en-têtes de couche 3 et 4

Les paquets de données pour les protocoles qui nécessitent une inspection de couche 7 peuvent également passer par le chemin rapide.

Certains paquets de session établis doivent continuer à emprunter le chemin de gestion de session ou le chemin du plan de commande. Les paquets qui empruntent le chemin de gestion de session comprennent les paquets HTTP qui nécessitent une inspection ou un filtrage de contenu. Les paquets qui empruntent le chemin du plan de commande comprennent les paquets de contrôle pour les protocoles qui nécessitent une inspection de couche 7.

Présentation fonctionnelle VPN

Un VPN est une connexion sécurisée sur un réseau TCP/IP (tel qu'Internet) qui s'affiche comme une connexion privée. Cette connexion sécurisée s'appelle un tunnel. L'ASA utilise des protocoles de tunnellisation pour négocier les paramètres de sécurité, créer et gérer des tunnels, encapsuler des paquets, transmettre ou recevoir des paquets par le tunnel et les désencapsuler. L'ASA fonctionne comme un point terminal de tunnel bidirectionnel : il peut recevoir des paquets simples, les encapsuler et les envoyer à l'autre extrémité du tunnel où ils sont désencapsulés et envoyés à leur destination finale. Il peut également recevoir des paquets encapsulés, les désencapsuler et les envoyer à leur destination finale. L'ASA invoque divers protocoles standard pour remplir ces fonctions.

L'ASA remplit les fonctions suivantes :

- Établit des tunnels
- Négocie les paramètres du tunnel
- Authentifie les utilisateurs
- Attribue des adresses d'utilisateur
- Chiffre et déchiffre les données
- Gère les clés de sécurité
- Gère le transfert de données dans le tunnel
- Gère le transfert de données entrant et sortant en tant que point terminal de tunnel ou routeur

L'ASA invoque divers protocoles standard pour remplir ces fonctions.

Présentation du contexte de sécurité

Vous pouvez partitionner un ASA unique en plusieurs périphériques virtuels, appelés contextes de sécurité. Chaque contexte de sécurité est un périphérique indépendant, avec sa politique de sécurité, ses interfaces et ses administrateurs. Les contextes multiples sont similaires au fait d'avoir plusieurs périphériques autonomes. De nombreuses fonctionnalités sont prises en charge en mode de contexte multiple, notamment les tables de

routage, les fonctionnalités de pare-feu, IPS et la gestion; cependant, certaines fonctionnalités ne sont pas prises en charge. Consultez les chapitres consacrés aux fonctionnalités pour en savoir plus.

En mode de contexte multiple, l'ASA comprend une configuration pour chaque contexte qui identifie la politique de sécurité, les interfaces et presque toutes les options que vous pouvez configurer sur un périphérique autonome. L'administrateur système ajoute et gère les contextes en les configurant dans la configuration système, qui, à l'instar d'une configuration monomode, est la configuration de démarrage. La configuration système identifie les paramètres de base de l'ASA. La configuration système n'inclut aucune interface réseau ni aucun paramètre réseau pour elle-même; au contraire, lorsque le système doit accéder à des ressources réseau (comme le téléchargement des contextes à partir du serveur), il utilise l'un des contextes désigné comme contexte d'administration.

Le contexte d'administration est comme un contexte de sécurité, sauf que lorsqu'un utilisateur se connecte au contexte d'administration, cet utilisateur dispose de droits d'administrateur système et peut accéder au système et à tous les autres contextes.

Présentation de la mise en grappe d'ASA

La mise en grappe d'ASA vous permet de regrouper plusieurs ASA en un seul périphérique logique. Une grappe offre toute la commodité d'un seul appareil (gestion, intégration dans un réseau), tout en offrant le débit accru et la redondance de plusieurs périphériques.

Vous effectuez toute la configuration (à l'exception de la configuration de démarrage) sur l'unité de contrôle uniquement; la configuration est ensuite répliquée sur les unités membres.

Services spéciaux et existants

Pour certains services, la documentation se trouve en dehors des guides de configuration principaux et de l'aide en ligne.

Guides de services spéciaux

Des services spéciaux permettent à l'ASA d'interagir avec d'autres produits Cisco; par exemple, en fournissant un mandataire de sécurité pour les services téléphoniques (Unified Communications), en fournissant le filtrage du trafic réseau de zombies en conjonction avec la base de données dynamique du serveur de mise à jour de Cisco, ou en fournissant des services WCCP pour l'appliance Cisco pour la sécurité du web. Certains de ces services spéciaux sont couverts par des guides distincts :

- Guide de filtrage du trafic du réseau de zombies Cisco ASA
- Guide de mise en œuvre de Cisco ASA NetFlow
- Guide de Cisco ASA Unified Communications
- Guide de redirection du trafic WCCP Cisco ASA
- Guide de mise en œuvre des outils SNMP version 3

Guide des services existants

Les services existants sont toujours pris en charge sur l'ASA, mais il peut y avoir de meilleurs services de remplacement que vous pouvez utiliser à la place. Les services existants sont couverts dans un guide distinct :

Guide des fonctionnalités existantes de Cisco ASA

Ce guide comprend les chapitres suivants :

- Configuration de RIP
- Règles AAA pour l'accès au réseau
- À l'aide des outils de protection, qui comprennent la prévention de l'usurpation d'adresse IP (**ip verify reverse-path**), la configuration de la taille des fragments (**fragment**), le blocage des connexions indésirables (**shun**), la configuration des options TCP (pour ASDM) et la configuration de l'audit IP pour la prise en charge IPS de base (**ip audit**).
- Configuration des services de filtrage

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.