Sécurité, accès Internet et ports de communication

Les rubriques suivantes présentent des informations sur la sécurité du système, l'accès Internet et les ports de communication :

Exigences de sécurité

Pour protéger le Cisco Secure Firewall Management Center, vous devez l'installer sur un réseau interne protégé. Bien que centre de gestion soit configuré pour ne disposer que des services et des ports nécessaires, vous devez vous assurer que les attaques ne peuvent pas l'atteindre.

Si le centre de gestion et ses périphériques gérés résident sur le même réseau, vous pouvez connecter les interfaces de gestion des périphériques au même réseau interne protégé que le centre de gestion. Cela vous permet de contrôler les périphériques en toute sécurité à partir de centre de gestion. Vous pouvez également configurer plusieurs interfaces de gestion pour permettre à centre de gestion de gérer et d'isoler le trafic des périphériques sur d'autres réseaux.

Quelle que soit la manière dont vous déployez vos périphériques, les communications inter-systèmes sont chiffrées. Vous devez toutefois prendre des mesures pour vous assurer que les communications entre les périphériques ne peuvent pas être interrompues, bloquées ou altérées, par exemple par un déni de service distribué (DDoS) ou une attaque de type "man-in-the-middle" (homme du milieu).

Cisco Clouds (Nuages Cisco)

Le centre de gestion communique avec les ressources dans le nuage Cisco pour les fonctionnalités suivantes :

- **protection améliorée contre les logiciels malveillants**

  Le nuage public est configuré par défaut; Pour apporter des modifications, consultez *Modifier les options AMP* dans le Guide de configuration Cisco Secure Firewall Management Center Device.

- **Filtrage d'URL**

Pour en savoir plus, consultez le chapitre sur le *filtrage d'URL* dans Guide de configuration Cisco Secure Firewall Management Center Device.

- **Connexion à Cisco Umbrella**

  Pour en savoir plus, consultez Politiques DNS de Cisco Umbrella.

Exigences d'accès Internet

Par défaut, le système est configuré pour se connecter à Internet sur les ports 443/tcp (HTTPS) et 80/tcp (HTTP). Si vous ne souhaitez pas que vos périphériques aient un accès direct à l'internet, vous pouvez configurer un serveur mandataire. Pour de nombreuses fonctionnalités, votre emplacement peut déterminer les ressources auxquelles le système accède.

Dans la plupart des cas, c'est centre de gestion qui accède à Internet. Les deux centre de gestion d'une paire à haute disponibilité doivent avoir un accès Internet. Selon la fonctionnalité, il arrive que les deux homologues accèdent à Internet et parfois seul l'homologue actif y accède.

Parfois, les périphériques gérés accèdent également à Internet. Par exemple, si la configuration de votre protection contre les programmes malveillants utilise l'analyse dynamique, les périphériques gérés envoient les fichiers directement dans le nuage Cisco Secure Malware Analytics. Vous pouvez également synchroniser un périphérique avec un serveur NTP externe.

De plus, à moins que vous ne désactiviez le suivi d'analyse Web, votre navigateur peut communiquer avec les serveurs d'analyse Web de Google (Google.com) ou d'Amplitude (amplitude.com) pour fournir à Cisco des données d'utilisation non nominatives.

Tableau 1 : Exigences d'accès Internet

Caractéristiques	Motif	Centre de gestion Haute disponibilité	Ressource
Défense contre les programmes malveillants	Recherche de programmes malveillants dans le nuage.	Les deux homologues effectuent des recherches.	Reportez-vous à Adresses de serveur requises pour le bon fonctionnement de Cisco Secure Endpoint et le fonctionnement de Malware Analytics.
	Téléchargez les mises à jour de signatures pour la préclassification des fichiers et l'analyse des programmes malveillants locaux.	Les homologues actifs téléchargent et se synchronisent en mode veille.	updates.vrt.sourcefire.com amp.updates.vrt.sourcefire.com
	Envoyer des fichiers pour analyse dynamique (périphériques gérés). Requête de résultats de l'analyse dynamique (centre de gestion).	Les deux homologues interrogent pour obtenir des rapports d'analyse dynamique.	fmc.api.threatgrid.com fmc.api.threatgrid.eu

Caractéristiques	Motif	Centre de gestion Haute disponibilité	Ressource
AMP pour les points terminaux	Recevez les événements de programmes malveillants détectés par AMP pour les points terminaux à partir du nuage AMP. Affichez les événements de programmes malveillants détectés par le système dans AMP pour les points terminaux. Utilisez les listes de blocage et d'autorisation de fichiers centralisées créées dans AMP pour les points terminaux afin de remplacer les dispositions du nuage AMP.	Les deux homologues reçoivent des événements. Vous devez également configurer la connexion au nuage sur les deux homologues (la configuration n'est pas synchronisée).	Reportez-vous à Adresses de serveur requises pour le bon fonctionnement de Cisco Secure Endpoint et le fonctionnement de Malware Analytics.
Renseignements de sécurité	Télécharger les flux de renseignements sur la sécurité	Les homologues actifs téléchargent et se synchronisent en mode veille.	intelligence.sourcefire.com
Filtrage d'URL	Télécharger des données de catégorie d'URL et de réputation. Interroger (rechercher) manuellement les données de catégorie d'URL et de réputation. Rechercher des URL non classées.	Les homologues actifs téléchargent et se synchronisent en mode veille.	URL : • regsvc.sco.cisco.com • est.sco.cisco.com • updates-talos.sco.cisco.com • updates.ironport.com Blocs IPv4 : • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 Blocs IPv6 : • 2a04:e4c7:ffff::/48 • 2a04:e4c7:fffe::/48
Licences intelligentes Cisco	Communiquer avec le Cisco Smart Software Manager.	L'homologue actif communique.	tools.cisco.com:443 www.cisco.com
Cisco Success Network (Réseau de succès Cisco)	Transmettez des informations et des statistiques d'utilisation.	L'homologue actif communique.	api-sse.cisco.com:8989 dex.sse.itd.cisco.com dex.eu.sse.itd.cisco.com

Caractéristiques	Motif	Centre de gestion Haute disponibilité	Ressource
Cisco Support Diagnostics (Diagnostics de l'assistance Cisco)	Accepte les demandes autorisées et transmet les renseignements et les statistiques d'utilisation.	L'homologue actif communique.	api-sse.cisco.com:8989
Mises à jour du système	Télécharger les mises à jour *directement* de Cisco sur centre de gestion : • Logiciel système • Règles d'intrusion • Base de données relative aux vulnérabilités (VDB) • Base de données de géolocalisation (GeoDB)	Mettez à jour les règles de prévention des intrusions, la VDB et la GeoDB sur l'homologue actif, qui se synchronise ensuite avec la base de données de secours. Mettre à niveau le logiciel système indépendamment sur chaque homologue.	cisco.com sourcefire.com
Intégration Réponse aux menaces SecureX	Consultez le guide d'intégration approprié.		
Synchronisation de l'heure	Synchronisez l'heure dans votre déploiement. Non pris en charge avec un serveur mandataire.	Tous les périphériques utilisant un serveur NTP externe doivent avoir un accès Internet.	0.sourcefire.pool.ntp.org 1.sourcefire.pool.ntp.org 2.sourcefire.pool.ntp.org 3.sourcefire.pool.ntp.org
Flux RSS	Affichez le blogue Cisco Threat Research sur le tableau de bord.	Tout appareil affichant des flux RSS doit avoir un accès Internet.	blog.talosintelligence.com
Whois	Demandez des informations whois pour un hôte externe. Non pris en charge avec un serveur mandataire.	Tout appareil demandant des informations whois doit avoir un accès Internet.	Le client whois tente de deviner quel est le bon serveur à interroger. S'il ne peut pas deviner, il utilise : • Manipulations du NIC : whois.networksolutions.com • Adresses IPv4 et noms de réseau : whois.arin.net

Exigences relatives aux ports de communication

Le centre de gestion communique avec les périphériques gérés à l'aide d'un canal chiffré de communication bidirectionnelle SSL sur le port 8305/tcp. Ce port *doit* rester ouvert pour la communication de base.

D'autres ports permettent une gestion sécurisée ainsi que l'accès aux ressources externes requises par des fonctionnalités spécifiques. En général, les ports liés à la fonctionnalité restent fermés jusqu'à ce que vous

activiez ou configuriez la fonctionnalité associée. Ne modifiez *pas* et ne fermez pas un port ouvert avant de comprendre en quoi cette action affectera votre déploiement.

Tableau 2 : Exigences relatives aux ports de communication

Port	Protocole/Fonctionnalité	Plateformes	Direction	Détails
53/tcp 53/udp	DNS		Sortant	DNS
67/udp 68/udp	DHCP (protocole de configuration dynamique des hôtes)		Sortant	DHCP (protocole de configuration dynamique des hôtes)
123/udp	NTP;		Sortant	Synchronisez l'heure.
162/udp	SNMP		Sortant	Envoyez des alertes SNMP à un serveur de déroutement distant.
389/tcp 636/tcp	LDAP		Sortant	Communiquez avec un serveur LDAP pour l'authentification externe. Obtenez les métadonnées pour les utilisateurs LDAP détectés (Centre de gestion uniquement). Configurable.
443/tcp	HTTPS	Centre de gestion	Entrant	Autorisez la connexion entrante sur le port 443 si vous intégrez le centre de gestion avec un connecteur de périphérique sécurisé sur site.
443/tcp	HTPS	Centre de gestion	Sortant	Autorisez le trafic sortant du port 443 si vous intégrez centre de gestion vers CDO à l'aide du connecteur infonuagique.
443/tcp	HTPS	Centre de gestion	Sortant	Autorisez la connexion sortante pour le port 443 si vous procédez à l'intégration de centre de gestion à l'aide de SecureX.
443/tcp	HTTPS		Sortant	Envoyez et recevez des données d'Internet
514/udp	Syslog (alertes)		Sortant	Envoyez des alertes à un serveur syslog distant.
1812/udp 1813/udp	RADIUS		Sortant	Communiquez avec un serveur RADIUS pour l'authentification externe et la gestion comptable. Configurable.

Port	Protocole/Fonctionnalité	Plateformes	Direction	Détails
8305/tcp	Communications concernant les périphériques		Les deux	Communiquez en toute sécurité entre les périphériques d'un déploiement Configurable. Si vous modifiez ce port, vous devez le modifier pour *tous* les périphériques du déploiement. Nous vous recommandons de conserver la valeur par défaut.

Sujets connexes

Ajouter un objet d'authentification externe LDAP pour CDO
Ajouter un objet d'authentification externe RADIUS pour CDO

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.