Adresses de serveur requises pour une analyse sécurisée des terminaux et des programmes malveillants

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Adresses de serveur requises pour le terminal sécurisé
  - Emplacements des serveurs
    - Amérique du Nord
    - Europe
    - Asie-Pacifique, Japon, Chine
- Adresses de serveur requises pour l'écosystème AMP
    - Amérique du Nord
    - Europe
    - Asie-Pacifique, Japon, Chine
- Adresses de serveur requises pour le cloud Secure Malware Analytics
- Adresses de serveur requises pour Orbital
  - Adresses IP statiques pour Orbital 1.7+
    - Cloud d'Amérique du Nord (NAM)
    - Cloud européen (UE)
    - Cloud Asie-Pacifique, Japon, Chine (APJC)
- Adresses IP statiques

Introduction

Ce document décrit les serveurs requis pour activer les communications produit du connecteur Cisco Secure Endpoint.

Conditions préalables

Pour permettre aux produits Cisco Secure Endpoint (anciennement Cisco AMP) et Cisco Secure Malware Analytics (anciennement Threat Grid) de communiquer et d'effectuer des mises à jour, des recherches et des rapports, votre pare-feu doit permettre la connectivité entre le connecteur/l'appareil et les serveurs requis.

Exigences

Cet article de la zone technique s'applique à ces produits Cisco s'intégrant à Cisco Secure Endpoint (AMP).

- Terminaux sécurisés pour les réseaux (Firepower Management Center et capteurs)
- Cloud privé de terminal sécurisé
- Cloud public pour terminaux sécurisés
- Appliance de sécurisation de la messagerie et sécurité de la messagerie Cisco (ESA et CES)
- Appareil Web sécurisé (WSA)
- Catalyst SDWAN/IOS-XE

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

⚠ Mise en garde : Tous les serveurs utilisent un schéma d’adresses IP round-robin pour l’équilibrage de charge, la tolérance aux pannes et la disponibilité. Par conséquent, les adresses IP peuvent changer, et Cisco recommande que le pare-feu soit configuré avec des noms d'hôte au lieu d'une adresse IP. Si vous ne parvenez pas à pare-feu en fonction des noms d'hôte, assurez-vous que toutes les adresses IP répertoriées au bas de ce document sont des destinations autorisées.

⚠ Mise en garde : Tout trafic entrant vers les serveurs Cisco ne peut pas être soumis au déchiffrement TLS.

Adresses de serveur requises pour le terminal sécurisé

Emplacements des serveurs

Les serveurs Cisco Secure Endpoint se trouvent dans trois emplacements différents :

- Amérique du Nord
- Europe
- Japon

Amérique du Nord

Catégorie	Objectif	Serveur	Port
Cisco Secure Endpoint : Cloud public	Serveur de disposition	cloud-ec-asn.amp.cisco.com cloud-ec-est.amp.cisco.com enrolment.amp.cisco.com	TCP 443
	Console	console.amp.cisco.com	TCP 443
	Serveur de gestion	mgmt.amp.cisco.com	TCP 443
	Serveur d'événements	intake.amp.cisco.com	TCP 443
	Politiques	policy.amp.cisco.com	TCP 443
	Téléchargements et mises à jour du connecteur	upgrades.amp.cisco.com	TCP 80 et 443
	Signalement des erreurs	crash.amp.cisco.com	TCP 443
	IOC des terminaux	ioc.amp.cisco.com	TCP 443
	Serveur de mise à jour TETRA	tetra-defs.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80 et 443
	Définitions des revendications macOS et Linux	clam-defs.amp.cisco.com	TCP 80 et 443
	Détections personnalisées avancées	custom-signatures.amp.cisco.com	TCP 443
	Récupération de fichier à distance	rff.amp.cisco.com submit.amp.cisco.com	TCP 443
	TÉTRA	nimbus.bitdefender.net	TCP 443
	Protection des comportements	apde.amp.cisco.com	TCP 443

	Contrôle des périphériques	endpoints.amp.cisco.com	TCP 443
Connecteur Android	Serveur de disposition	cloud-android-asn.amp.cisco.com	TCP 443
Connecteur CSC/iOS	Serveur de disposition	cloud-ios-asn.amp.cisco.com cloud-ios-est.amp.cisco.com	TCP 443
Cisco Secure Endpoint : Cloud privé	Serveur de disposition en amont <v2.4>	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Serveur de destruction en amont >v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Serveur Yum	packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443
	Session de support	support-sessions.amp.cisco.com	TCP 22

Europe

Catégorie	Objectif	Serveur	Port
Cisco Secure Endpoint : Cloud public	Serveur de disposition	cloud-ec-asn.eu.amp.cisco.com cloud-ec-est.eu.amp.cisco.com enrolment.eu.amp.cisco.com	TCP 443
	Console	console.eu.amp.cisco.com	TCP 443
	Serveur de gestion	mgmt.eu.amp.cisco.com	TCP 443
	Serveur d'événements	intake.eu.amp.cisco.com	TCP 443
	Politiques	policy.eu.amp.cisco.com	TCP 443

	Téléchargements et mises à jour du connecteur	upgrades.eu.amp.cisco.com	TCP 80 et 443
	Signalement des erreurs	crash.eu.amp.cisco.com	TCP 443
	IOC des terminaux	ioc.eu.amp.cisco.com	TCP 443
	Serveur de mise à jour TETRA	tetra-defs.eu.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80 et 443
	Définitions des revendications macOS et Linux	clam-defs.eu.amp.cisco.com	TCP 80 et 443
	Détections personnalisées avancées	custom-signatures.eu.amp.cisco.com	TCP 443
	Récupération de fichier à distance	rff.eu.amp.cisco.com submit.amp.cisco.com	TCP 443
	TÉTRA	nimbus.bitdefender.net	TCP 443
	Protection des comportements	apde.eu.amp.cisco.com	TCP 443
	Contrôle des périphériques	endpoints.eu.amp.cisco.com	TCP 443
Connecteur Android	Serveur de disposition	cloud-android-asn.eu.amp.cisco.com	TCP 443
Connecteur CSC/iOS	Serveur de disposition	cloud-ios-asn.eu.amp.cisco.com cloud-ios-est.eu.amp.cisco.com	TCP 443
Cisco Secure Endpoint : Cloud privé	Serveur de disposition en amont <v2.4>	cloud-pc-est.eu.amp.cisco.com cloud-pc-asn.eu.amp.cisco.com	TCP 443
	Serveur de disposition en amont >v2.4	cloud-pc-est.eu.amp.cisco.com cloud-pc-asn.eu.amp.cisco.com	TCP 443
	Serveur Yum	packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443
	Session de support	support-sessions.amp.cisco.com	TCP 22

Asie-Pacifique, Japon, Chine

Catégorie	Objectif	Serveur	Port
Cisco Secure Endpoint : Cloud public	Serveur de destruction	cloud-ec-asn.apjc.amp.cisco.com cloud-ec-est.apjc.amp.cisco.com enrolment.apjc.amp.cisco.com	TCP 443
	Console	console.apjc.amp.cisco.com	TCP 443
	Serveur de gestion	mgmt.apjc.amp.cisco.com	TCP 443
	Serveur d'événements	intake.apjc.amp.cisco.com	TCP 443
	Politiques	policy.apjc.amp.cisco.com	TCP 443
	Téléchargements et mises à jour du connecteur	upgrades.apjc.amp.cisco.com	TCP 80 et 443
	Signalement des erreurs	crash.apjc.amp.cisco.com	TCP 443
	IOC des terminaux	ioc.apjc.amp.cisco.com	TCP 443
	Serveur de mise à jour TETRA	tetra-defs.apjc.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80 et 443
	Définitions des revendications macOS et Linux	clam-defs.apjc.amp.cisco.com	TCP 80 et 443
	Détections personnalisées avancées	custom-signatures.apjc.amp.cisco.com	TCP 443
	Récupération de fichier à distance	rff.apjc.amp.cisco.com submit.amp.cisco.com	TCP 443
	TÉTRA	nimbus.bitdefender.net	TCP 443
	Protection des comportements	apde.apjc.amp.cisco.com	TCP 443
	Contrôle des périphériques	endpoints.apjc.amp.cisco.com	TCP 443

Connecteur Android	Serveur de destruction	cloud-android-asn.apjc.amp.cisco.com	TCP 443
Connecteur CSC/iOS	Serveur de destruction	cloud-ios-asn.apjc.amp.cisco.com cloud-ios-est.apjc.amp.cisco.com	TCP 443
Cisco Secure Endpoint : Cloud privé	Serveur de disposition en amont < v2.4	cloud-pc-est.apjc.amp.cisco.com cloud-pc-asn.apjc.amp.cisco.com	TCP 443
	Serveur de disposition en amont > v2.4	cloud-pc-est.apjc.amp.cisco.com cloud-pc-asn.apjc.amp.cisco.com	TCP 443
	Serveur Yum	packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443 TCP 443
	Session de support	support-sessions.amp.cisco.com	TCP 22

Adresses de serveur requises pour l'écosystème AMP

Cette section traite des noms d'hôte requis pour les appliances intégrées AMP, tels que Cisco Secure Firewall, Secure Email Gateway, etc.

Amérique du Nord

Pare-feu sécurisé (AMP pour les réseaux)	File Reputation (depuis FMC ou depuis NGFW si FDM est géré)	cloud-sa.amp.cisco.com cloud-ngfw-asn.amp.cisco.com cloud-ngfw-est.amp.cisco.com	TCP 443
	Réception d'événements (depuis FMC)	intake.amp.cisco.com	TCP 443
	Enregistrement de console (depuis FMC)	mgmt.amp.cisco.com	TCP 443
	Livraison d'événements (depuis FMC)	export.amp.cisco.com	TCP 443

	API (de FMC)	api.amp.cisco.com	TCP 443
Passerelle de messagerie sécurisée (ESA)	Réputation des fichiers	cloud-esa-asn.amp.cisco.com cloud-esa-est.amp.cisco.com cloud-sa.amp.cisco.com	TCP 443
	API	api.amp.cisco.com	TCP 443
	Serveur d'événements	intake.amp.cisco.com	TCP 443
	Serveur de gestion	mgmt.amp.cisco.com	TCP 443
Appareil Web sécurisé (WSA)	Réputation des fichiers	cloud-sa.amp.cisco.com	TCP 443
	API	api.amp.cisco.com	TCP 443
Meraki MX	Réputation des fichiers	cloud-meraki-asn.amp.cisco.com cloud-meraki-est.amp.cisco.com	TCP 443
Catalyst SDWAN	Réputation des fichiers	cloud-isr-asn.amp.cisco.com cloud-isr-est.amp.cisco.com	TCP 443

Europe

Pare-feu sécurisé (AMP pour les réseaux)	Réputation des fichiers (à partir de FMC ou du pare-feu de nouvelle génération si FDM est géré)	cloud-sa.eu.amp.cisco.com cloud-ngfw-asn.eu.amp.cisco.com cloud-ngfw-est.eu.amp.cisco.com	TCP 443
	Réception d'événements (depuis FMC)	intake.eu.amp.cisco.com	TCP 443
	Enregistrement de console (depuis FMC)	mgmt.eu.amp.cisco.com	TCP 443

	Livraison d'événements (depuis FMC)	export.eu.amp.cisco.com	TCP 443
	API (de FMC)	api.eu.amp.cisco.com	TCP 443
Passerelle de messagerie sécurisée (ESA)	Réputation des fichiers	cloud-esa-asn.eu.amp.cisco.com cloud-esa-est.eu.amp.cisco.com cloud-sa.eu.amp.cisco.com	TCP 443
	API	api.eu.amp.cisco.com	TCP 443
	Serveur d'événements	intake.eu.amp.cisco.com	TCP 443
	Serveur de gestion	mgmt.eu.amp.cisco.com	TCP 443
Appareil Web sécurisé (WSA)	Réputation des fichiers	cloud-sa.eu.amp.cisco.com	TCP 443
	API	api.eu.amp.cisco.com	TCP 443
Catalyst SDWAN	Réputation des fichiers	cloud-isr-asn.eu.amp.cisco.com cloud-isr-est.eu.amp.cisco.com	TCP 443

Asie-Pacifique, Japon, Chine

Pare-feu sécurisé (AMP pour les réseaux)	File Reputation (depuis FMC ou depuis NGFW si FDM est géré)	cloud-sa.apjc.amp.cisco.com cloud-ngfw-asn.apjc.amp.cisco.com cloud-ngfw-est.apjc.amp.cisco.com	TCP 443
	Réception d'événements (depuis FMC)	intake.apjc.amp.cisco.com	TCP 443
	Enregistrement de console (depuis FMC)	mgmt.apjc.amp.cisco.com	TCP 443
	Livraison d'événements (depuis FMC)	export.apjc.amp.cisco.com	TCP 443

	API (de FMC)	api.apjc.amp.cisco.com	TCP 443
Passerelle de messagerie sécurisée (ESA)	Réputation des fichiers	cloud-esa-asn.apjc.amp.cisco.com cloud-esa-est.apjc.amp.cisco.com cloud-sa.apjc.amp.cisco.com	TCP 443
	API	api.apjc.amp.cisco.com	TCP 443
	Serveur d'événements	intake.apjc.amp.cisco.com	TCP 443
	Serveur de gestion	mgmt.apjc.amp.cisco.com	TCP 443
Appareil Web sécurisé (WSA)	Réputation des fichiers	cloud-sa.apjc.amp.cisco.com	TCP 443
	API	api.apjc.amp.cisco.com	TCP 443
Catalyst SDWAN	Réputation des fichiers	cloud-isr-asn.amp.cisco.com cloud-isr-est.amp.cisco.com	TCP 443

Adresses de serveur requises pour le cloud Secure Malware Analytics

Pour plus d'informations sur Cisco Secure Malware Analytic Cloud and Appliance, reportez-vous à cet article : IP et ports requis pour Secure Malware Analytics

Adresses de serveur requises pour Orbital

Adresses IP statiques pour Orbital 1.7+

Cloud d'Amérique du Nord (NAM)

Nom de l'hôte	IP	Port
orbital.amp.cisco.com	54.71.115.87 54.68.234.245 54.200.174.54	443
ncp.orbital.amp.cisco.com	52.88.16.211 52.43.91.219 54.200.152.114	443
update.orbital.amp.cisco.com	54.71.197.112 54.188.114.190 54.188.131.5	443
Adresses IP NAT pour le magasin de données distant		
	34.223.219.240 35.160.108.105 52.11.13.222	Numéro de port aléatoire élevé

Pour plus d'informations, consultez le guide d'aide orbitale : https://orbital.amp.cisco.com/help/

Cloud européen (UE)

Nom de l'hôte	**IP**	**Port**
orbital.eu.amp.cisco.com	3.120.91.16 18.196.194.92 3.121.5.209	443
ncp.orbital.eu.amp.cisco.com	18.194.154.159 18.185.217.177 18.184.249.36	443
update.orbital.eu.amp.cisco.com	3.123.83.189	443

	18.184.240.159 35.158.29.104	
Adresses IP NAT pour le magasin de données distant		
	52.29.47.197 52.57.222.67 52.58.172.218	Numéro de port aléatoire élevé

Pour plus d'informations, consultez le guide d'aide orbitale : https://orbital.eu.amp.cisco.com/help/

Cloud Asie-Pacifique, Japon, Chine (APJC)

Nom de l'hôte	**IP**	**Port**
orbital.apjc.amp.cisco.com	3.114.186.175 52.198.6.9 18.177.242.101	443
ncp.orbital.apjc.amp.cisco.com	18.177.250.245 13.230.62.75 18.176.196.172	443
update.orbital.apjc.amp.cisco.com	54.248.22.154 18.178.184.79 54.95.125.218	443
Adresses IP NAT pour le magasin de données distant		
	52.194.143.206 52.69.138.67	Numéro de port

	54.95.9.136	aléatoire élevé

Pour plus d'informations, consultez le guide d'aide orbitale : https://orbital.apjc.amp.cisco.com/help/

Adresses IP statiques

Si votre pare-feu bloque les connexions TCP sortantes sur le port 443 (ce qui n'est généralement pas le cas), vous devez vous assurer que toutes les adresses IP répertoriées ici sont des destinations autorisées.

Remarque : Afin d'assurer la continuité des opérations et de s'assurer que les dispositions des fichiers malveillants détectés sont les mêmes sur les deux Firepower Management Center, les deux principaux et secondaires Management Center doivent avoir accès aux serveurs répertoriés dans ce document.

Adresses IP statiques en Amérique du Nord	Adresses IP statiques en Europe	Adresses IP statiques dans APJC
23.23.197.169 23.23.198.191 23.23.224.83 50.16.242.171 50.16.244.193 50.16.250.236 52.0.55.209 52.2.63.194 52.2.128.246 52.3.149.24 52.3.178.163 52.3.190.47 52.4.98.101 52.4.151.41 52.4.245.162 52.4.246.178 52.5.92.125 52.6.103.57 52.6.197.200 52.20.14.163 52.20.123.238	46.51.181.139 46.51.182.195 46.51.182.202 46.137.99.242 52.16.63.115 52.16.95.58 52.16.105.95 52.16.166.193 52.16.177.94 52.16.193.225 52.16.220.180 52.17.93.43 52.17.102.100 52.17.106.35 52.17.179.163 52.17.211.190 52.17.233.49 52.18.9.153 52.18.28.229 52.18.79.226 52.18.109.209 52.18.187.129 52.18.187.166	54.250.127.0 52.197.2.58 52.197.22.41 52.69.16.172 13.112.137.80 52.198.208.254 13.112.162.167 54.249.244.218 54.249.246.210 54.249.243.85 54.249.240.219 54.248.98.94 176.34.47.0 52.192.82.189 52.68.180.106 52.196.247.47 52.196.185.158 52.197.74.4 52.69.39.127 54.248.113.224 54.238.55.12 54.249.248.16 52.197.50.93

52.20.141.147	52.18.223.41	52.193.124.132
52.21.52.149	52.19.84.244	52.69.108.228
52.21.117.50	52.19.167.56	52.197.72.147
52.21.134.210	52.30.25.70	52.197.22.165
52.22.64.192	52.30.74.163	52.68.82.200
52.22.156.183	52.30.124.82	52.197.35.73
52.23.13.34	52.30.160.113	52.197.39.251
52.23.16.199	52.30.175.205	52.68.251.104
52.23.73.146	52.30.179.236	54.249.253.42
52.23.87.4	52.30.196.206	54.249.253.65
52.23.107.89	52.30.208.114	176.34.60.211
52.23.134.105	52.30.217.4	52.192.198.119
52.23.140.222	52.30.217.226	52.196.96.41
52.70.11.137	52.30.255.133	54.248.116.199
52.70.13.27	52.31.30.249	52.196.117.29
52.70.35.37	52.31.66.59	52.196.134.7
52.70.47.45	52.31.83.94	176.34.60.30
52.70.56.136	52.31.119.97	52.192.145.214
52.70.58.10	52.31.122.77	52.192.221.107
52.70.59.59	52.31.127.190	52.193.182.191
52.70.59.121	52.31.137.201	52.193.201.169
52.70.60.74	54.195.248.52	52.193.223.43
52.70.61.174	54.195.249.18	52.193.233.17
52.70.61.181	54.217.232.226	52.196.115.166
52.70.61.193	54.217.232.234	52.196.31.86
52.70.63.25	54.217.232.241	52.197.121.237
54.83.45.221	54.217.232.244	52.198.147.230
54.88.208.235	54.217.232.249	52.198.195.125
54.204.8.61	54.228.250.255	52.198.202.24
54.221.210.7	54.246.88.192	52.198.221.53
54.221.255.190	54.247.189.117	52.198.223.169
54.225.226.117	54.74.229.75	52.198.225.221
54.225.227.9	107.21.250.31	52.198.226.104
54.225.227.30	107.21.236.143	52.198.26.36
54.225.227.45	52.2.128.246	52.198.94.104
54.225.227.105	52.18.202.103	52.199.124.11
54.225.228.145	52.18.119.87	52.199.127.80
54.225.228.166	192.111.5.0/24	52.199.92.142
54.225.228.244	34.249.48.182	52.68.1.146
54.227.247.102		54.248.107.84
107.20.158.55		54.248.109.124
107.20.203.8		54.248.126.98
107.20.229.191		54.248.236.127
107.20.234.220		54.248.236.141
107.21.212.157		54.248.236.144
		54.248.236.151

107.21.217.202 107.21.218.60 174.129.203.65 54.161.128.60 54.234.131.176 52.206.206.244 34.225.208.192 52.22.120.193 34.199.250.32 34.199.238.4 34.194.224.132 34.198.112.150 34.224.236.198 52.20.233.31 192.111.4.0/24 192.111.7.0/24 54.71.197.112 54.188.114.190 54.188.131.5 192.35.177.23 104.18.39.201 172.64.148.55 104.18.4.5 104.18.5.5 52.3.48.165 52.6.245.67 34.120.67.236 34.98.122.109 2600:1f18:4016:be00::/64 2600:1f18:4016:be01::/64 2600:1f18:4016:be02::/64	34.248.52.55 99.81.233.22 3.123.83.189 18.184.240.159 35.158.29.104 192.35.177.23 104.18.39.201 172.64.148.55 104.18.4.5 104.18.5.5 52.3.48.165 52.6.245.67 34.120.67.236 34.98.122.109	54.248.237.93 54.249.246.7 54.250.127.131 192.111.6.0/24 54.248.22.154 18.178.184.79 54.95.125.218 192.35.177.23 104.18.39.201 172.64.148.55 18.180.25.43 54.95.253.127 54.249.195.77 104.18.4.5 104.18.5.5 52.3.48.165 52.6.245.67 34.120.67.236 34.98.122.109

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.