

Adresses de serveur requises pour le bon fonctionnement de Cisco Secure Endpoint & Malware Analytics

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Adresses de serveur requises pour le bon fonctionnement des terminaux sécurisés Cisco](#)

[Emplacements des serveurs](#)

[Amérique du Nord](#)

[Europe](#)

[Asie-Pacifique, Japon, Chine](#)

[Adresses de serveur requises pour un accès cloud Cisco Secure Malware Analytics approprié](#)

[Adresses de serveur requises pour une utilisation orbitale appropriée](#)

[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 permettre au produit Cisco Secure Endpoint (anciennement Cisco AMP) et au produit Cisco Secure Malware Analytics (anciennement Threat Grid) de communiquer et d'effectuer des mises à jour, des recherches et des rapports. Pour mener à bien les opérations, votre pare-feu doit autoriser la connectivité entre le connecteur/dispositif et les serveurs requis.

 Attention : 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 CNAME au lieu d'une adresse IP.

 Attention : tout trafic entrant vers les serveurs Cisco ne peut pas être soumis au déchiffrement TLS.

Conditions préalables

Exigences

Cet article de la Zone technique concerne les produits Cisco suivants, qui s'intègrent au produit Cisco Secure Endpoint (AMP) et à Malware Analytics (Threat Grid) :

- Terminaux sécurisés Cisco pour réseaux (Firepower Management Center et capteurs)
- Cloud privé Cisco Secure Endpoint
- Cloud public Cisco Secure Endpoint
- Appliance de sécurisation de la messagerie Cisco et sécurité de la messagerie Cisco (ESA et CES)
- Appareil Web sécurisé Cisco (WSA)
- Cisco Secure Malware Analytics Cloud et/ou appliance (Threat Grid)
- 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.

Adresses de serveur requises pour le bon fonctionnement des terminaux sécurisés Cisco

Emplacements des serveurs

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

- Amérique du Nord (Cisco Secure Endpoint et Cisco Secure Malware Analytics)
- Europe (Cisco Secure Endpoint et Cisco Secure Malware Analytics)
- Japon (Cisco Secure Endpoint uniquement)

Amérique du Nord

Ce tableau répertorie les emplacements des serveurs en Amérique du Nord. En fonction de la date de création du compte, les adresses du serveur peuvent être différentes :

Catégorie	Objectif	Serveur	Port
Terminaux sécurisés Cisco : cloud public	Serveur de disposition	cloud-ec-asn.amp.cisco.com cloud-ec-est.amp.cisco.com	TCP 443

		enrolment.amp.cisco.com	
	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
Terminaux sécurisés Cisco : 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	TCP 443
		pc-packages.amp.cisco.com	TCP 443
	Session de support	support-sessions.amp.cisco.com	TCP 22
Pare-feu sécurisé (AMP pour les réseaux)	Disposition Server (à partir du FMC ou du capteur si FDM est géré)	6.0 - 6.2 : cloud-sa.amp.sourcefire.com	TCP 443
		6.3 - 7.6 : cloud-sa.amp.cisco.com	
		7.7+ : cloud-ngfw-asn.amp.cisco.com AND cloud-ngfw-est.amp.cisco.com	
	Réception d'événements (depuis FMC)	7.7+ : intake.amp.cisco.com	TCP 443
	Enregistrement de console (depuis FMC)	7.7+ : mgmt.amp.cisco.com	TCP 443
Livraison d'événements (depuis FMC)	6.0 - 6.2 : export.amp.sourcefire.com	TCP 443	
	6.3+ : export.amp.cisco.com		
API (de FMC)	6.0 - 6.2 : api.amp.sourcefire.com	TCP 443	
	6.3+ : api.amp.cisco.com ET api.amp.sourcefire.com		
Passerelle de messagerie sécurisée (ESA) Appareil Web sécurisé (WSA)	Réputation des fichiers (ESAWSA)	>= 15.x : cloud-esa-asn.amp.cisco.com cloud-esa-est.amp.cisco.com	TCP 443
		< 15.x : cloud-sa.amp.cisco.com	
Gestionnaire de messagerie électronique et Web sécurisé (SMA)	API (ESA)	>= 15.x : api.amp.cisco.com	TCP 443
		< 15.x : S/O	
Serveur d'événements (ESA)		>= 15.x : intake.amp.cisco.com	TCP 443
		< 15.x : S/O	

Serveur de gestion (ESA)

		>= 15.x : mgmt.amp.cisco.com < 15.x : S/O	TCP 443
Meraki MX	Serveur de disposition	cloud-meraki-asn.amp.cisco.com cloud-meraki-est.amp.cisco.com	TCP 443
SD-WAN	Serveur de disposition	cloud-isr-asn.amp.cisco.com cloud-isr-est.amp.cisco.com	TCP 443

Europe

Ce tableau répertorie les emplacements de serveur pour l'Europe. En fonction de la date de création du compte, les adresses du serveur peuvent être différentes :

Catégorie	Objectif	Serveur	Port
Terminaux sécurisés Cisco : 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
Terminaux sécurisés Cisco : 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
	Amont (liaisons montantes) Serveur de destruction >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	TCP 443
		pc-packages.amp.cisco.com	TCP 443
Session de support	support-sessions.amp.cisco.com	TCP 22	
Pare-feu sécurisé (AMP pour les réseaux)	Disposition Server (à partir du FMC ou du capteur si FDM est géré)	6.0 - 6.2 : cloud-sa.eu.amp.sourcefire.com	TCP 443
		6.3 - 7.6 : cloud-sa.eu.amp.cisco.com	
		7.7+ : cloud-ngfw-asn.eu.amp.cisco.com AND cloud-ngfw-est.eu.amp.cisco.com	
	Réception d'événements (depuis FMC)	7.7+ : intake.eu.amp.cisco.com	TCP 443
Enregistrement de console (depuis FMC)	7.7+ : mgmt.eu.amp.cisco.com	TCP 443	
Livraison d'événements (depuis FMC)	6.0 - 6.2 : export.eu.amp.sourcefire.com 6.3+ : export.eu.amp.cisco.com	TCP 443	

		6.0 - 6.2 : api.eu.amp.sourcefire.com 6.3+ : api.eu.amp.cisco.com ET api.eu.amp.sourcefire.com	
Passerelle de messagerie sécurisée (ESA) Appareil Web sécurisé (WSA) Gestionnaire de messagerie électronique et Web sécurisé (SMA)	Réputation des fichiers (ESA/WSA)	>= 15.x : cloud-esa-asn.eu.amp.cisco.com cloud-esa-est.eu.amp.cisco.com < 15.x : cloud-sa.eu.amp.cisco.com	TCP 443
	API (ESA)	>= 15.x : api.eu.amp.cisco.com < 15.x : S/O	TCP 443
	Serveur d'événements (ESA)	>= 15.x : intake.eu.amp.cisco.com < 15.x : S/O	TCP 443
	Serveur de gestion (ESA)	>= 15.x : mgmt.eu.amp.cisco.com < 15.x : S/O	TCP 443
SD-WAN	Serveur de disposition	cloud-isr-asn.eu.amp.cisco.com cloud-isr-est.eu.amp.cisco.com	TCP 443

Asie-Pacifique, Japon, Chine

Ce tableau répertorie les emplacements des serveurs pour l'Asie-Pacifique, le Japon et la Chine :

Catégorie	Objectif	Serveur	Port
Terminaux sécurisés Cisco : cloud public	Serveur de destruction	cloud-ec-asn.apjc.amp.cisco.com	TCP 443
		cloud-ec-est.apjc.amp.cisco.com	
		enrolment.apjc.amp.cisco.com	
	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	Amont (liaisons montantes) Serveur de disposition < v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Amont (liaisons montantes) Serveur de destruction > v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Serveur Yum	packages-v2.amp.sourcefire.com	TCP 443

		pc-packages.amp.cisco.com	TCP 443
			TCP 443
	Session de support	support-sessions.amp.cisco.com	TCP 22
Pare-feu sécurisé (AMP pour les réseaux)	Disposition Server (à partir du FMC ou du capteur si FDM est géré)	6.0 - 6.2 : cloud-sa.apjc.amp.sourcefire.com 6.3 - 7.6 : cloud-sa.apjc.amp.cisco.com 7.7+ : cloud-ngfw-asn.apjc.amp.cisco.com AND cloud-ngfw-est.apjc.amp.cisco.com	TCP 443
	Livraison d'événements (depuis FMC)	6.0 - 6.2 : export.eu.amp.sourcefire.com 6.3+ : export.eu.amp.cisco.com	TCP 443
	Réception d'événements (depuis FMC)	7.7+ : intake.apjc.amp.cisco.com	TCP 443
	Enregistrement de console (depuis FMC)	7.7+ : mgmt.apjc.amp.cisco.com	TCP 443
	API (de FMC)	6.0 - 6.2 : api.eu.amp.sourcefire.com 6.3+ : api.eu.amp.cisco.com ET api.eu.amp.sourcefire.com	TCP 443
Passerelle de messagerie sécurisée (ESA) Appareil Web sécurisé (WSA) Gestionnaire de messagerie électronique et Web sécurisé (SMA)	Réputation des fichiers (ESA/WSA)	>= 15.x : cloud-esa-asn.apjc.amp.cisco.com cloud-esa-est.apjc.amp.cisco.com < 15.x : cloud-sa.apjc.amp.cisco.com	TCP 443
	API (ESA)	>= 15.x : api.apjc.amp.cisco.com < 15.x : S/O	TCP 443
	Serveur d'événements (ESA)	>= 15.x : intake.apjc.amp.cisco.com < 15.x : S/O	TCP 443
	Serveur de gestion (ESA)	>= 15.x : mgmt.apjc.amp.cisco.com < 15.x : S/O	TCP 443
SD-WAN	Serveur de disposition	cloud-isr-asn.apjc.amp.cisco.com	TCP 443

		cloud-isr-est.apjc.amp.cisco.com	
--	--	----------------------------------	--

Adresses de serveur requises pour un accès cloud Cisco Secure Malware Analytics approprié

Pour plus d'informations sur Secure Malware Analytic Cloud and Appliance, reportez-vous à cet article : [Adresses IP et ports requis pour Secure Malware Analytics](#)

Adresses de serveur requises pour une utilisation orbitale appropriée

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

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 18.184.240.159 35.158.29.104	443
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	443


	18.178.184.79	
	54.95.125.218	
Adresses IP NAT pour le magasin de données distant		
	52.194.143.206	Numéro de port aléatoire élevé
	52.69.138.67	
	54.95.9.136	


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 modifier les paramètres de votre pare-feu avant de mettre à jour les stratégies. Si votre compte a été créé après février 2016, vous disposez déjà d'adresses IP statiques écrites dans les stratégies standard. Si votre compte a été créé avant février 2016, vous pouvez contacter le centre d'assistance technique Cisco (TAC) pour demander une migration des politiques vers les adresses IP statiques.

 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.

 Remarque : Cisco Secure Endpoint Console n'utilise pas d'adresses IP statiques et doit être accessible via DNS.

Adresses IP statiques en Amérique du Nord	Adresses IP statiques en Europe	Adresses IP statiques dans APJC
23.23.197.169	46.51.181.139	54.250.127.0
23.23.198.191	46.51.182.195	52.197.2.58
23.23.224.83	46.51.182.202	52.197.22.41
	46.137.99.242	52.69.16.172
50.16.242.171	52.16.63.115	13.112.137.80
50.16.244.193	52.16.95.58	52.198.208.254
	52.16.105.95	13.112.162.167
50.16.250.236	52.16.166.193	54.249.244.218
52.0.55.209		

52.2.63.194	52.16.177.94	54.249.246.210
52.2.128.246	52.16.193.225	54.249.243.85
52.3.149.24	52.16.220.180	54.249.240.219
52.3.178.163	52.17.93.43	54.248.98.94
52.3.190.47	52.17.102.100	176.34.47.0
52.4.98.101	52.17.106.35	52.192.82.189
52.4.151.41	52.17.179.163	52.68.180.106
52.4.245.162	52.17.211.190	52.196.247.47
52.4.246.178	52.17.233.49	52.196.185.158
52.5.92.125	52.18.9.153	52.197.74.4
52.6.103.57	52.18.28.229	52.69.39.127
52.6.197.200	52.18.79.226	54.248.113.224
52.20.14.163	52.18.109.209	54.238.55.12
52.20.123.238	52.18.187.129	54.249.248.16
52.20.141.147	52.18.187.166	52.197.50.93
52.21.52.149	52.18.223.41	52.193.124.132
52.21.117.50	52.19.84.244	52.69.108.228
52.21.134.210	52.19.167.56	52.197.72.147
52.22.64.192	52.30.25.70	52.197.22.165
52.22.156.183	52.30.74.163	52.68.82.200
52.23.13.34	52.30.124.82	52.197.35.73
52.23.16.199	52.30.160.113	52.197.39.251
52.23.73.146	52.30.175.205	52.68.251.104
52.23.87.4	52.30.179.236	54.249.253.42
52.23.107.89	52.30.196.206	54.249.253.65
52.23.134.105	52.30.208.114	176.34.60.211
52.23.140.222	52.30.217.4	52.192.198.119
52.70.11.137	52.30.217.226	52.196.96.41
52.70.13.27	52.30.255.133	54.248.116.199
52.70.35.37	52.31.30.249	52.196.117.29
52.70.47.45	52.31.66.59	52.196.134.7
52.70.56.136	52.31.83.94	176.34.60.30
52.70.58.10	52.31.119.97	52.192.145.214
52.70.59.59	52.31.122.77	52.192.221.107
52.70.59.121	52.31.127.190	52.193.182.191
52.70.60.74	52.31.137.201	52.193.201.169
52.70.61.174	54.195.248.52	52.193.223.43
52.70.61.181	54.195.249.18	52.193.233.17
52.70.61.193	54.217.232.226	52.196.115.166
52.70.63.25	54.217.232.234	52.196.31.86
54.83.45.221	54.217.232.241	52.197.121.237
54.88.208.235	54.217.232.244	52.198.147.230
	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	107.21.236.143	52.198.94.104
54.225.227.105	52.2.128.246	52.199.124.11
54.225.228.145	52.18.202.103	52.199.127.80
54.225.228.166	52.18.119.87	52.199.92.142
54.225.228.244	192.111.5.0/24	52.68.1.146
54.227.247.102	34.249.48.182	54.248.107.84
107.20.158.55	34.248.52.55	54.248.109.124
107.20.203.8	99.81.233.22	54.248.126.98
107.20.229.191	3.123.83.189	54.248.236.127
107.20.234.220	18.184.240.159	54.248.236.141
107.21.212.157	35.158.29.104	54.248.236.144
107.21.217.202	192.35.177.23	54.248.236.151
107.21.218.60	104.18.39.201	54.248.237.93
128.177.8.0/24	172.64.148.55	54.249.246.7
174.129.203.65	104.18.4.5	54.250.127.131
54.161.128.60	104.18.5.5	192.111.6.0/24
54.234.131.176	52.3.48.165	54.248.22.154
52.206.206.244	52.6.245.67	18.178.184.79
34.225.208.192	34.120.67.236	54.95.125.218
52.22.120.193	34.98.122.109	192.35.177.23
34.199.250.32		104.18.39.201
34.199.238.4		172.64.148.55
34.194.224.132		18.180.25.43
34.198.112.150		54.95.253.127
34.224.236.198		54.249.195.77
52.20.233.31		104.18.4.5
192.111.4.0/24		104.18.5.5
192.111.7.0/24		52.3.48.165
54.71.197.112		52.6.245.67
54.188.114.190		34.120.67.236
54.188.131.5		34.98.122.109
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		

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.