

# Erforderliche Serveradressen für den ordnungsgemäßen Betrieb von Cisco Secure Endpoint und Malware Analytics

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Erforderliche Serveradressen für ordnungsgemäßen AMP-Betrieb](#)

[Serverstandorte](#)

[Nordamerika](#)

[Europa](#)

[Asien-Pazifik-Raum, Japan, China](#)

[Erforderliche Serveradressen für richtigen Cisco Secure Malware Analytics Cloud-Zugriff](#)

[North America Cloud \(NAM\)](#)

[Europäische Cloud \(EU\)](#)

[Erforderliche Serveradressen für eine ordnungsgemäße orbitale Verwendung](#)

[North America Cloud \(NAM\)](#)

[Europäische Cloud \(EU\)](#)

[Asien-Pazifik-Raum, Japan, China \(APJC\) Cloud](#)

[Statische IP-Adressen](#)

## Einleitung

In diesem Dokument werden die Server beschrieben, die erforderlich sind, damit das Produkt Cisco Secure Endpoint (AMP) und Malware Analytics (Threat Grid) Updates, Suchvorgänge und Berichte miteinander kommunizieren und abschließen können. Um den Vorgang erfolgreich abzuschließen, muss Ihre Firewall die Verbindung vom Connector/der Appliance zu den erforderlichen Servern zulassen.

**Vorsicht:** Alle Server verwenden ein Rundlauf-IP-Adressenschema für Lastenausgleich, Fehlertoleranz und Betriebszeit. Aus diesem Grund können sich die IP-Adressen ändern. Cisco empfiehlt, die Firewall mit *CNAME* anstelle einer IP-Adresse zu konfigurieren.

**Vorsicht:** Datenverkehr, der zu Cisco Servern gelangt, kann nicht der TLS-Entschlüsselung unterzogen werden.

## Voraussetzungen

### Anforderungen

Dieser Tech Zone-Artikel bezieht sich auf die folgenden Cisco Produkte, die in Cisco Secure Endpoint (AMP) und Malware Analytics (Threat Grid) integriert sind:

- Cisco AMP für Netzwerke (FirePOWER Management Center und Sensoren)
- Cisco Secure Endpoint Private Cloud
- Cisco Secure Endpoint Public Cloud
- Cisco Secure Email Appliance und Cisco Email Security (ESA und CES)
- Cisco Secure Web Appliance (WSA)
- Cisco Secure Malware Analytics Cloud und/oder Appliance (Threat Grid)
- SDWAN/IOS-XE

## Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

## Erforderliche Serveradressen für ordnungsgemäßen AMP-Betrieb

### Serverstandorte

Die AMP- und Threat Grid-Server befinden sich an drei verschiedenen Standorten:

- Nordamerika (AMP und Threat Grid)
- Europa (AMP und Threat Grid)
- Japan (nur AMP)

### Nordamerika

In dieser Tabelle sind die Serverstandorte für Nordamerika aufgeführt. Je nach Erstellungsdatum des Kontos können sich die Serveradressen unterscheiden:

Kategorie	Zweck	Server	Anschluss
Cisco Secure Endpoint: Public Cloud	Dispositionsserver	cloud-ec-asn.amp.cisco.com cloud-ec-est.amp.cisco.com enrolment.amp.cisco.com	TCP 443
	Konsole	console.amp.cisco.com	TCP 443
	Management-Server	mgmt.amp.cisco.com	TCP 443
	Ereignisserver	intake.amp.cisco.com	TCP 443
	Richtlinien	policy.amp.cisco.com	TCP 443
	Connector-Downloads und -Updates	upgrades.amp.cisco.com	TCP 80 und 443
	Fehlerberichterstattung	crash.amp.cisco.com	TCP 443
	Endgeräte-IOCs	ioc.amp.cisco.com	TCP 443
	TETRA-Aktualisierungsserver	tetra-defs.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80 und 443
	macOS und Linux Clam Definitionen	clam-defs.amp.cisco.com	TCP 80 und 443
	Erweiterte benutzerdefinierte Erkennungen	custom-signatures.amp.cisco.com	TCP 443
	Remote-Dateiabruf	rff.amp.cisco.com submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net	TCP 443

	Verhaltensschutz	apde.amp.cisco.com	TCP 443
	Gerätesteuerung	endpoints.amp.cisco.com	TCP 443
Android-Anschluss	Dispositionsserver	cloud-android-asn.amp.cisco.com	TCP 443
CSC/iOS-Anschluss	Dispositionsserver	cloud-ios-asn.amp.cisco.com	TCP 443
		cloud-ios-est.amp.cisco.com	
Cisco Secure Endpoint: Private Cloud	Upstream-Dispositionsserver <v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Upstream-Dispositionsserver > v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Yum-Server	packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443
	Support-Sitzung	support-sessions.amp.cisco.com	TCP 2
	Dispositionsserver (von FMC)	6.0 - 6.2.x: cloud-sa.amp.sourcefire.com 6.3.x + : cloud-sa.amp.cisco.com	TCP 443
AMP für Netzwerke: Firepower	Ereignisse (von FMC)	5.x - 6.2.x: export.amp.sourcefire.com 6.3.x + : export.amp.cisco.com	TCP 443
	API (von FMC)	5.x - 6.2.x: api.amp.sourcefire.com 6.3.x + : api.amp.cisco.com UND api.amp.sourcefire.com	TCP 443
	Dynamische Analyse (vom Sensor)	5.x: intel.api.sourcefire.com 6.x: panacea.threatgrid.com UND fmc.api.threatgrid.com * Je nach Patch-Version 6.x kann eine der beiden URLs verwendet werden.	TCP 443
	Dateireputation (ESA/WSA)	>= 15.x: cloud-esa-asn.amp.cisco.com cloud-esa-est.amp.cisco.com < 15.x: cloud-sa.amp.cisco.com	TCP 443
	Dateianalyse (ESA/WSA/SMA)	panacea.threatgrid.com	TCP 443
	API (ESA)	>= 15.x: api.amp.cisco.com < 15.x: k. A.	TCP 443
ESA/WSA/SMA	Ereignisserver (ESA)	>= 15.x: intake.amp.cisco.com < 15.x: k. A.	TCP 443
	Management-Server (ESA)	>= 15.x: mgmt.amp.cisco.com < 15.x: k. A.	TCP 443
Meraki	Dispositionsserver	cloud-meraki-asn.amp.cisco.com cloud-meraki-est.amp.cisco.com	TCP 443
SD-WAN	Dispositionsserver	cloud-isr-asn.amp.cisco.com cloud-isr-est.amp.cisco.com	TCP 443

## Europa

In dieser Tabelle sind die Serverstandorte für Europa aufgeführt. Je nach Erstellungsdatum des Kontos können sich die Serveradressen unterscheiden:

Kategorie	Zweck	Server	Anschluss
Cisco Secure Endpoint: Public Cloud	Dispositionsserver	cloud-ec-asn.eu.amp.cisco.com cloud-ec-est.eu.amp.cisco.com enrolment.eu.amp.cisco.com	TCP 443
	Konsole	console.eu.amp.cisco.com	TCP 443

	Management-Server	mgmt.eu.amp.cisco.com	TCP 443
	Ereignisserver	intake.eu.amp.cisco.com	TCP 443
	Richtlinien	policy.eu.amp.cisco.com	TCP 443
	Connector-Downloads und -Updates	upgrades.eu.amp.cisco.com	TCP 80 und 443
	Fehlerberichterstattung	crash.eu.amp.cisco.com	TCP 443
	Endgeräte-IOCs	ioc.eu.amp.cisco.com	TCP 443
	TETRA-Aktualisierungsserver	tetra-defs.eu.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80 und 443
	macOS und Linux Clam Definitionen	clam-defs.eu.amp.cisco.com	TCP 80 und 443
	Erweiterte benutzerdefinierte Erkennungen	custom-signatures.eu.amp.cisco.com	TCP 443
	Remote-Dateiabruf	rff.eu.amp.cisco.com submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net	TCP 443
	Verhaltensschutz	apde.eu.amp.cisco.com	TCP 443
	Gerätesteuerung	endpoints.eu.amp.cisco.com	TCP 443
Android-Anschluss	Dispositionsserver	cloud-android-asn.eu.amp.cisco.com	TCP 443
CSC/iOS-Anschluss	Dispositionsserver	cloud-ios-asn.eu.amp.cisco.com cloud-ios-est.eu.amp.cisco.com	TCP 443
	Upstream-Dispositionsserver <v2.4	cloud-pc-est.eu.amp.cisco.com cloud-pc-asn.eu.amp.cisco.com	TCP 443
Cisco Secure Endpoint: Private Cloud	Upstream Dispositionsserver > v2.4	cloud-pc-est.eu.amp.cisco.com cloud-pc-asn.eu.amp.cisco.com	TCP 443
	Yum-Server	packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443
	Support-Sitzung	support-sessions.amp.cisco.com	TCP 2
	Disposition Server (von FMC)	6.0 - 6.2.x: cloud-sa.eu.amp.sourcefire.com 6.3.x+: cloud-sa.eu.amp.cisco.com	TCP 443
AMP für Netzwerke: Firepower	Ereignisse (von FMC)	5.x - 6.2.x: export.eu.amp.sourcefire.com 6.3.x+: export.eu.amp.cisco.com	TCP 443
	API (von FMC)	5.x - 6.2.x: api.amp.sourcefire.com UND api.eu.amp.sourcefire.com 6.3.x+: api.amp.sourcefire.com UND api.eu.amp.cisco.com	TCP 443
	Dynamische Analyse (vom Sensor)	5.x: intel.api.sourcefire.com 6.x: panacea.bedrohgrid.eu UND fmc.api.bedrohgrid.eu Je nach Patch-Version 6.x kann eine der URLs verwendet werden.	TCP 443
	Dateireputation (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
ESA/WSA/SMA	Dateianalyse (ESA/WSA/SMA)	panacea.bedrohgrid.eu	TCP 443
	API (ESA)	>= 15.x: api.eu.amp.cisco.com < 15,x: k. A.	TCP 443
	Ereignisserver (ESA)	>= 15.x: intake.eu.amp.cisco.com < 15,x: k. A.	TCP 443
	Management-Server (ESA)	>= 15.x: mgmt.eu.amp.cisco.com < 15,x: k. A.	TCP 443
SD-WAN	Dispositionsserver	cloud-isr-asn.eu.amp.cisco.com cloud-isr-est.eu.amp.cisco.com	TCP 443

## Asien-Pazifik-Raum, Japan, China

In dieser Tabelle sind die Serverstandorte für den Asien-Pazifik-Raum, Japan und China aufgeführt:

Kategorie	Zweck	Server	Anschluss
Cisco Secure Endpoint: Public Cloud	Disposition-Server	cloud-ec-asn.apjc.amp.cisco.com cloud-ec-est.apjc.amp.cisco.com enrolment.apjc.amp.cisco.com	TCP 443
	Konsole	console.apjc.amp.cisco.com	TCP 443
	Management-Server	mgmt.apjc.amp.cisco.com	TCP 443
	Ereignisserver	intake.apjc.amp.cisco.com	TCP 443
	Richtlinien	policy.apjc.amp.cisco.com	TCP 443
	Connector-Downloads und -Updates	upgrades.apjc.amp.cisco.com	TCP 80 und 443
	Fehlerberichterstattung	crash.apjc.amp.cisco.com	TCP 443
	Endgeräte-IOCs	ioc.apjc.amp.cisco.com	TCP 443

	TETRA-Aktualisierungsserver	tetra-defs.apjc.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80 und 443
	macOS und Linux Clam Definitionen	clam-defs.apjc.amp.cisco.com	TCP 80 und 443
	Erweiterte benutzerdefinierte Erkennungen	custom-signatures.apjc.amp.cisco.com	TCP 443
	Remote-Dateiabruf	rff.apjc.amp.cisco.com submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net	TCP 443
	Verhaltensschutz	apde.apjc.amp.cisco.com	TCP 443
	Gerätesteuerung	endpoints.apjc.amp.cisco.com	TCP 443
Android-Anschluss	Disposition-Server	cloud-android-asn.apjc.amp.cisco.com	TCP 443
CSC/iOS-Anschluss	Disposition-Server	cloud-ios-asn.apjc.amp.cisco.com cloud-ios-est.apjc.amp.cisco.com	TCP 443
	Upstream Dispositionsserver < v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
Cisco Secure Endpoint: Private-Cloud	Upstream Dispositionsserver > v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Yum-Server	packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443 TCP 443
	Support-Sitzung	support-sessions.amp.cisco.com	TCP 2
	Disposition-Server	6.0 - 6.2.x: cloud-sa.apjc.amp.sourcefire.com (statische IP) 6.3.x+: cloud-sa.apjc.amp.cisco.com	TCP 443
AMP für Netzwerke: Firepower	Events	5.x - 6.2.x: export.apjc.amp.sourcefire.com 6.3.x+: export.apjc.amp.cisco.com	TCP 443
	API	5.2 - 6.2.x api.apjc.amp.sourcefire.com UND api.amp.sourcefire.com 6.3.x+: api.amp.sourcefire.com UND api.apjc.amp.cisco.com	TCP 443
	Dynamische Analyse	Derzeit gibt es in APJC keine Threat Grid-Rechenzentren, daher Es müssen europäische oder nordamerikanische Hostnamen verwendet werden.	TCP 443
	Dateireputation (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
	Dateianalyse (ESA/WSA/SMA)	Derzeit gibt es in APJC keine Threat Grid-Rechenzentren, daher Es müssen europäische oder nordamerikanische Hostnamen verwendet werden.	TCP 443
ESA/WSA/SMA	API (ESA)	>= 15.x: api.apjc.amp.cisco.com < 15,x: k. A.	TCP 443
	Ereignisserver (ESA)	>= 15.x: intake.apjc.amp.cisco.com < 15,x: k. A.	TCP 443
	Management-Server (ESA)	>= 15.x: mgmt.apjc.amp.cisco.com < 15,x: k. A.	TCP 443
SD-WAN	Dispositionsserver	cloud-isr-asn.apjc.amp.cisco.com cloud-isr-est.apjc.amp.cisco.com	TCP 443

## Erforderliche Serveradressen für richtigen Cisco Secure Malware Analytics Cloud-Zugriff

### North America Cloud (NAM)

#### Hostname

panacea.threatgrid.com

#### IP

63.97.201.67, 443

#### Anschluss Details

Für Threat Grid-Portal und integrierte Geräte (ESA/WSA/FTD/ODNS/Meraki)

	63.162.55.67		
glovebox.scl.threatgrid.com	63.162.55.67	443	Beispiel-Interaktionsfenster
glovebox.rcn.threatgrid.com	63.97.201.67	443	Beispiel-Interaktionsfenster
fmc.api.threatgrid.com	63.97.201.67, 63.162.55.67	443	FMC/FTD-Dateianalyse-Service

## Europäische Cloud (EU)

<u>Hostname</u>	<u>IP</u>	<u>Anschluss</u>	<u>Details</u>
panacea.bedrohgrid.eu	89.167.128.132	443	Für Threat Grid-Portal und integrierte Geräte (ESA/WSA/FTD/ODNS/Meraki)
glovebox.bedrohgrid.eu	89.167.128.132	443	Beispiel-Interaktionsfenster
fmc.api.bedrohgrid.eu	89.167.128.132	443	FMC/FTD-Dateianalyse-Service

Weitere Threat Grid-Anforderungen, z. B. Appliances, finden Sie in diesem Artikel: [Erforderliche IP und Ports für Threat Grid](#)

## Erforderliche Serveradressen für eine ordnungsgemäße orbitale Verwendung

Statische IPs für Orbital 1.7+

### North America Cloud (NAM)

<u>Hostname</u>	<u>IP</u>	<u>Anschluss</u>
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	

NAT-IPs für Remote-Datenspeicher

34.223.219.240	Hohe zufällige Portnummer
35.160.108.105	
52.11.13.222	

Weitere Informationen finden Sie in der Online-Hilfe unter: <https://orbital.amp.cisco.com/help/>

## Europäische Cloud (EU)

<u>Hostname</u>	<u>IP</u>	<u>Anschluss</u>
orbital.eu.amp.cisco.com	3.120.91.16	443
	18.196.194.92	
	3.121.5.209	
ncp.orbital.eu.amp.cisco.com	18.194.154.159	443
	18.185.217.177	
	18.184.249.36	
update.orbital.eu.amp.cisco.com	3.123.83.189	443
	18.184.240.159	
	35.158.29.104	

NAT-IPs für Remote-Datenspeicher

52.29.47.197	Hohe
52.57.222.67	zufällige
52.58.172.218	Portnum
	mer

Weitere Informationen finden Sie in der Online-Hilfe unter: <https://orbital.eu.amp.cisco.com/help/>

## Asien-Pazifik-Raum, Japan, China (APJC) Cloud

<u>Hostname</u>	<u>IP</u>	<u>Ansch luss</u>
orbital.apjc.amp.cisco.com	3.114.186.175	443
	52.198.6.9	
	18.177.242.101	
ncp.orbital.apjc.amp.cisco.com	18.177.250.245	443
	13.230.62.75	
	18.176.196.172	
update.orbital.apjc.amp.cisco.com	54.248.22.154	443
	18.178.184.79	
	54.95.125.218	

NAT-IPs für Remote-Datenspeicher

52.194.143.206	Hohe
52.69.138.67	zufällige
54.95.9.136	Portnum
	mer

Weitere Informationen finden Sie in der Online-Hilfe unter: <https://orbital.apjc.amp.cisco.com/help/>

## Statische IP-Adressen

Wenn Ihre Firewall ausgehende TCP-Verbindungen auf Port 443 blockiert (was in der Regel nicht der Fall ist), müssen Sie Ihre Firewall-Einstellungen ändern, bevor Sie Richtlinien aktualisieren. Wenn Ihr Konto nach Februar 2016 eingerichtet wurde, verfügen Sie bereits über statische IP-Adressen, die in die Standardrichtlinien geschrieben wurden. Wenn Ihr Konto vor Februar 2016 eingerichtet wurde, können Sie sich an das Cisco Technical Assistance Center (TAC) wenden, um eine Migration der Richtlinien zu den statischen IP-Adressen zu beantragen.

**Hinweis:** Um die Kontinuität des Betriebs sicherzustellen und sicherzustellen, dass die erkannte Datei-Malware in beiden FirePOWER Management Centern gleich bleibt, müssen sowohl das primäre als auch das sekundäre Management Center Zugriff auf die in diesem Dokument aufgeführten Server haben.

**Hinweis:** Die AMP-Konsole verwendet keine statischen IPs und muss über DNS aufgerufen werden.

### Statische IP-Adressen in Nordamerika

23.23.197.169  
23.23.198.191

### Statische IP-Adressen in Europa

46.51.181.139  
46.51.182.195

### Statische IP-Adressen in APJC

54.250.127.0  
52.197.2.58

23.23.224.83	46.51.182.202	52.197.22.41
50.16.242.171	46.137.99.242	52.69.16.172
50.16.244.193	52.16.63.115	13.112.137.80
50.16.250.236	52.16.95.58	52.198.208.254
52.0.55.209	52.16.105.95	13.112.162.167
52.2.63.194	52.16.166.193	54.249.244.218
52.2.128.246	52.16.177.94	54.249.246.210
52.3.149.24	52.16.193.225	54.249.243.85
52.3.178.163	52.16.220.180	54.249.240.219
52.3.190.47	52.17.93.43	54.248.98.94
52.4.98.101	52.17.102.100	176.34.47.0
52.4.151.41	52.17.106.35	52.192.82.189
52.4.245.162	52.17.179.163	52.68.180.106
52.4.246.178	52.17.211.190	52.196.247.47
52.5.92.125	52.17.233.49	52.196.185.158
52.6.103.57	52.18.9.153	52.197.74.4
52.6.197.200	52.18.28.229	52.69.39.127
52.20.14.163	52.18.79.226	54.248.113.224
52.20.123.238	52.18.109.209	54.238.55.12
52.20.141.147	52.18.187.129	54.249.248.16
52.21.52.149	52.18.187.166	52.197.50.93
52.21.117.50	52.18.223.41	52.193.124.132
52.21.134.210	52.19.84.244	52.69.108.228
52.22.64.192	52.19.167.56	52.197.72.147
52.22.156.183	52.30.25.70	52.197.22.165
52.23.13.34	52.30.74.163	52.68.82.200
52.23.16.199	52.30.124.82	52.197.35.73
52.23.73.146	52.30.160.113	52.197.39.251
52.23.87.4	52.30.175.205	52.68.251.104
52.23.107.89	52.30.179.236	54.249.253.42
52.23.134.105	52.30.196.206	54.249.253.65
52.23.140.222	52.30.208.114	176.34.60.211
52.70.11.137	52.30.217.4	52.192.198.119
52.70.13.27	52.30.217.226	52.196.96.41
52.70.35.37	52.30.255.133	54.248.116.199
52.70.47.45	52.31.30.249	52.196.117.29
52.70.56.136	52.31.66.59	52.196.134.7
52.70.58.10	52.31.83.94	176.34.60.30
52.70.59.59	52.31.119.97	52.192.145.214
52.70.59.121	52.31.122.77	52.192.221.107
52.70.60.74	52.31.127.190	52.193.182.191
52.70.61.174	52.31.137.201	52.193.201.169
52.70.61.181	54.195.248.52	52.193.223.43
52.70.61.193	54.195.249.18	52.193.233.17
52.70.63.25	54.217.232.226	52.196.115.166
54.83.45.221	54.217.232.234	52.196.31.86
54.88.208.235	54.217.232.241	52.197.121.237
54.204.8.61	54.217.232.244	52.198.147.230
54.221.210.7	54.217.232.249	52.198.195.125
54.221.255.190	54.228.250.255	52.198.202.24
54.225.226.117	54.246.88.192	52.198.221.53
54.225.227.9	54.247.189.117	52.198.223.169
54.225.227.30	54.74.229.75	52.198.225.221



54.225.227.45  
54.225.227.105  
54.225.228.145  
54.225.228.166  
54.225.228.244  
54.227.247.102  
107.20.158.55  
107.20.203.8  
107.20.229.191  
107.20.234.220  
107.21.212.157  
107.21.217.202  
107.21.218.60  
128.177.8.0/24  
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

107.21.250.31  
107.21.236.143  
52.2.128.246  
52.18.202.103  
52.18.119.87  
192.111.5.0/24  
34.249.48.182  
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

52.198.226.104  
52.198.26.36  
52.198.94.104  
52.199.124.11  
52.199.127.80  
52.199.92.142  
52.68.1.146  
54.248.107.84  
54.248.109.124  
54.248.126.98  
54.248.236.127  
54.248.236.141  
54.248.236.144  
54.248.236.151  
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

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.