Indirizzi server richiesti per le corrette operazioni di analisi malware di Cisco Secure Endpoint &

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati

Indirizzi server richiesti per le corrette operazioni Cisco Secure Endpoint

- Posizioni server
  - Nord America
  - Europa
  - Asia-Pacifico, Giappone, Cina

Indirizzi server richiesti per l'accesso cloud Cisco Secure Malware Analytics appropriato

Indirizzi server necessari per un corretto utilizzo orbitale

- Cloud del Nord America (NAM)
- Cloud europeo (UE)
- Asia-Pacifico, Giappone, Cina (APJC) Cloud

Indirizzi IP statici

Introduzione

Questo documento descrive i server necessari per abilitare il prodotto Cisco Secure Endpoint (in precedenza Cisco AMP) e il prodotto Cisco Secure Malware Analytics (in precedenza Threat Grid) per comunicare e completare aggiornamenti, ricerche e report. Per completare correttamente le operazioni, il firewall deve consentire la connettività dal connettore/accessorio ai server necessari.

⚠ Attenzione: tutti i server utilizzano uno schema di indirizzi IP round robin per il bilanciamento del carico, la tolleranza di errore e i tempi di attività. Pertanto, gli indirizzi IP potrebbero cambiare e Cisco consiglia di configurare il firewall con CNAME anziché con un indirizzo IP.

⚠ Attenzione: il traffico diretto ai server Cisco non può essere soggetto alla decrittografia TLS.

Prerequisiti

Requisiti

Questo articolo di Tech Zone si applica ai seguenti prodotti Cisco che si integrano con i prodotti

Cisco Secure Endpoint (AMP) e Malware Analytics (Threat Grid):

- Cisco Secure Endpoints per reti (Firepower Management Center e sensori)
- Cisco Secure Endpoint Private Cloud
- Cisco Secure Endpoint Public Cloud
- Cisco Secure Email Appliance e Cisco Email Security (ESA e CES)
- Cisco Secure Web Appliance (WSA)
- Cisco Secure Malware Analytics Cloud e/o appliance (Threat Grid)
- SDWAN/IOS-XE

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Indirizzi server richiesti per le corrette operazioni Cisco Secure Endpoint

Posizioni server

I server Cisco Secure Endpoint e Cisco Secure Malware Analytics si trovano in tre posizioni diverse:

- Nord America (Cisco Secure Endpoint e Cisco Secure Malware Analytics)
- Europa (Cisco Secure Endpoint e Cisco Secure Malware Analytics)
- Giappone (solo Cisco Secure Endpoint)

Nord America

Questa tabella elenca le posizioni dei server per il Nord America. In base alla data di creazione dell'account, gli indirizzi del server potrebbero essere diversi:

Categoria	Scopo	Server	Port
Cisco Secure Endpoint: cloud pubblico	Server di disposizione	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
	Server di gestione	mgmt.amp.cisco.com	TCP 443
	Server eventi	intake.amp.cisco.com	TCP 443

	Politiche	policy.amp.cisco.com	TCP 443
	Download e aggiornamenti dei connettori	upgrades.amp.cisco.com	TCP 80 e 443
	Segnalazione errori	crash.amp.cisco.com	TCP 443
	IOC endpoint	ioc.amp.cisco.com	TCP 443
	Server di aggiornamento TETRA	tetra-defs.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80 e 443
	Definizioni delle richieste di rimborso per macOS e Linux	clam-defs.amp.cisco.com	TCP 80 e 443
	Rilevamenti personalizzati avanzati	custom-signatures.amp.cisco.com	TCP 443
	Recupero file remoto	rff.amp.cisco.com submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net	TCP 443
	Protezione del comportamento	apde.amp.cisco.com	TCP 443
	Controllo dispositivo	endpoints.amp.cisco.com	TCP 443
Android Connector	Server di disposizione	cloud-android-asn.amp.cisco.com	TCP 443
Connettore CSC/iOS	Server di disposizione	cloud-ios-asn.amp.cisco.com cloud-ios-est.amp.cisco.com	TCP 443
Cisco Secure Endpoint: cloud privato	Server di disposizione upstream <v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Server di disposizione upstream >v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Server Yum	packages-v2.amp.sourcefire.com	TCP 443

		pc-packages.amp.cisco.com	TCP 443
	Sessione di supporto	support-sessions.amp.cisco.com	TCP 22
AMP for Networks: Firepower	Server di eliminazione (da FMC)	6.0 - 6.2.x: cloud-sa.amp.sourcefire.com 6.3.x + : cloud-sa.amp.cisco.com	TCP 443
	Eventi (da FMC)	5.x - 6.2.x: export.amp.sourcefire.com 6.3.x +: export.amp.cisco.com	TCP 443
	API (da FMC)	5.x - 6.2.x: api.amp.sourcefire.com 6.3.x + : api.amp.cisco.com E api.amp.sourcefire.com	TCP 443
	Analisi dinamica (dal sensore)	5.x: intel.api.sourcefire.com 6.x: panacea.threatgrid.com E fmc.api.threatgrid.com *A seconda della versione della patch 6.x, è possibile utilizzare entrambi gli URL	TCP 443
ESA/WSA/SMA	Reputazione dei file (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
	Analisi dei file (ESA/WSA/SMA)	panacea.threatgrid.com	TCP 443
	API (ESA)	>= 15,x: api.amp.cisco.com < 15,x: N/D	TCP 443
	Event Server (ESA)	>= 15,x: intake.amp.cisco.com < 15,x: N/D	TCP 443
	Server di gestione (ESA)	>= 15,x: mgmt.amp.cisco.com < 15,x: N/D	TCP 443

Meraki	Server di disposizione	cloud-meraki-asn.amp.cisco.com cloud-meraki-est.amp.cisco.com	TCP 443
SD-WAN	Server di disposizione	cloud-isr-asn.amp.cisco.com cloud-isr-est.amp.cisco.com	TCP 443

Europa

In questa tabella sono elencate le posizioni dei server per l'Europa. In base alla data di creazione dell'account, gli indirizzi del server potrebbero essere diversi:

Categoria	Scopo	Server	Port
Cisco Secure Endpoint: cloud pubblico	Server di disposizione	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
	Server di gestione	mgmt.eu.amp.cisco.com	TCP 443
	Server eventi	intake.eu.amp.cisco.com	TCP 443
	Politiche	policy.eu.amp.cisco.com	TCP 443
	Download e aggiornamenti dei connettori	upgrades.eu.amp.cisco.com	TCP 80 e 443
	Segnalazione errori	crash.eu.amp.cisco.com	TCP 443
	IOC endpoint	ioc.eu.amp.cisco.com	TCP 443
	Server di aggiornamento TETRA	tetra-defs.eu.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80 e 443
	Definizioni delle richieste di rimborso per macOS e Linux	clam-defs.eu.amp.cisco.com	TCP 80 e 443
	Rilevamenti personalizzati avanzati	custom-signatures.eu.amp.cisco.com	TCP 443
	Recupero file remoto	rff.eu.amp.cisco.com submit.amp.cisco.com	TCP 443

	TETRA	nimbus.bitdefender.net	TCP 443
	Protezione del comportamento	apde.eu.amp.cisco.com	TCP 443
	Controllo dispositivo	endpoints.eu.amp.cisco.com	TCP 443
Android Connector	Server di disposizione	cloud-android-asn.eu.amp.cisco.com	TCP 443
Connettore CSC/iOS	Server di disposizione	cloud-ios-asn.eu.amp.cisco.com cloud-ios-est.eu.amp.cisco.com	TCP 443
Cisco Secure Endpoint: cloud privato	Server di disposizione upstream <v2.4	cloud-pc-est.eu.amp.cisco.com cloud-pc-asn.eu.amp.cisco.com	TCP 443
	Server di disposizione upstream >v2.4	cloud-pc-est.eu.amp.cisco.com cloud-pc-asn.eu.amp.cisco.com	TCP 443
	Server Yum	packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443
	Sessione di supporto	support-sessions.amp.cisco.com	TCP 22
AMP for Networks: Firepower	Server di eliminazione (da FMC)	6.0 - 6.2.x: cloud-sa.eu.amp.sourcefire.com 6.3.x+: cloud-sa.eu.amp.cisco.com	TCP 443
	Eventi (da FMC)	5.x - 6.2.x: export.eu.amp.sourcefire.com 6.3.x+: export.eu.amp.cisco.com	TCP 443
	API (da FMC)	5.x - 6.2.x: api.amp.sourcefire.com E api.eu.amp.sourcefire.com 6.3.x+: api.amp.sourcefire.com E api.eu.amp.cisco.com	TCP 443
	Analisi dinamica (dal sensore)	5.x: intel.api.sourcefire.com 6.x: panacea.threat grid.eu E fmc.api.threat.grid.eu A seconda della versione della patch 6.x, è possibile	TCP 443

		utilizzare entrambi gli URL	
ESA/WSA/SMA	Reputazione dei file (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
	Analisi dei file (ESA/WSA/SMA)	panacea.threat.eu	TCP 443
	API (ESA)	>= 15,x: api.eu.amp.cisco.com < 15,x: N/D	TCP 443
	Event Server (ESA)	>= 15,x: intake.eu.amp.cisco.com < 15,x: N/D	TCP 443
	Server di gestione (ESA)	>= 15,x: mgmt.eu.amp.cisco.com < 15,x: N/D	TCP 443
SD-WAN	Server di disposizione	cloud-isr-asn.eu.amp.cisco.com cloud-isr-est.eu.amp.cisco.com	TCP 443

Asia-Pacifico, Giappone, Cina

Nella tabella seguente vengono elencate le posizioni dei server per l'Asia Pacifico, il Giappone e la Cina:

Categoria	Scopo	Server	Port
Cisco Secure Endpoint: cloud pubblico	Server di disposizione	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
	Server di gestione	mgmt.apjc.amp.cisco.com	TCP 443
	Server eventi	intake.apjc.amp.cisco.com	TCP 443
	Politiche	policy.apjc.amp.cisco.com	TCP 443

	Download e aggiornamenti dei connettori	upgrades.apjc.amp.cisco.com	TCP 80 e 443
	Segnalazione errori	crash.apjc.amp.cisco.com	TCP 443
	IOC endpoint	ioc.apjc.amp.cisco.com	TCP 443
	Server di aggiornamento TETRA	tetra-defs.apjc.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80 e 443
	Definizioni delle richieste di rimborso per macOS e Linux	clam-defs.apjc.amp.cisco.com	TCP 80 e 443
	Rilevamenti personalizzati avanzati	custom-signatures.apjc.amp.cisco.com	TCP 443
	Recupero file remoto	rff.apjc.amp.cisco.com submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net	TCP 443
	Protezione del comportamento	apde.apjc.amp.cisco.com	TCP 443
	Controllo dispositivo	endpoints.apjc.amp.cisco.com	TCP 443
Android Connector	Server di disposizione	cloud-android-asn.apjc.amp.cisco.com	TCP 443
Connettore CSC/iOS	Server di disposizione	cloud-ios-asn.apjc.amp.cisco.com cloud-ios-est.apjc.amp.cisco.com	TCP 443
Cisco Secure Endpoint: Cloud privato	Server di disposizione upstream < v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Server di disposizione upstream > v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Server Yum		

		packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443 TCP 443
	Sessione di supporto	support-sessions.amp.cisco.com	TCP 22
AMP for Networks: Firepower	Server di disposizione	6.0 - 6.2.x: cloud-sa.apjc.amp.sourcefire.com (IP statico) 6.3.x+: cloud-sa.apjc.amp.cisco.com	TCP 443
	Eventi	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 E api.amp.sourcefire.com 6.3.x+: api.amp.sourcefire.com E api.apjc.amp.cisco.com	TCP 443
	Analisi dinamica	Non sono attualmente presenti centri dati Threat Grid in APJC, quindi il È necessario utilizzare nomi host europei o nordamericani.	TCP 443
ESA/WSA/SMA	Reputazione dei file (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
	Analisi dei file (ESA/WSA/SMA)	Non sono attualmente presenti centri dati Threat Grid in APJC, quindi il È necessario utilizzare nomi host europei o nordamericani.	TCP 443
	API (ESA)	>= 15,x: api.apjc.amp.cisco.com < 15,x: N/D	TCP 443
	Event Server (ESA)		

		>= 15,x: intake.apjc.amp.cisco.com < 15,x: N/D	TCP 443
	Server di gestione (ESA)	>= 15,x: mgmt.apjc.amp.cisco.com < 15,x: N/D	TCP 443
SD-WAN	Server di disposizione	cloud-isr-asn.apjc.amp.cisco.com cloud-isr-est.apjc.amp.cisco.com	TCP 443

Indirizzi server richiesti per l'accesso cloud Cisco Secure Malware Analytics appropriato

Per i dettagli su Secure Malware Analytic Cloud e Appliance, fare riferimento a questo articolo: IP e porte richiesti per Secure Malware Analytics

Indirizzi server necessari per un corretto utilizzo orbitale

IP statici per Orbital 1.7+

Cloud del Nord America (NAM)

Nome host	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
IP NAT per archivio dati remoto		

	34.223.219.240 35.160.108.105 52.11.13.222	Numero di porta casuale alto

Per ulteriori informazioni, consultare la guida orbitale: https://orbital.amp.cisco.com/help/

Cloud europeo (UE)

Nome host	**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
IP NAT per archivio dati remoto		
	52.29.47.197 52.57.222.67 52.58.172.218	Numero di porta casuale alto

Per ulteriori informazioni, consultare la guida orbitale: https://orbital.eu.amp.cisco.com/help/

Asia-Pacifico, Giappone, Cina (APJC) Cloud

Nome host	**IP**	**Port**
orbital.apjc.amp.cisco.com	3.114.186.175 52.198.6.9	443

	18.177.242.101	
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
IP NAT per archivio dati remoto		
	52.194.143.206 52.69.138.67 54.95.9.136	Numero di porta casuale alto

Per ulteriori informazioni, consultare la guida orbitale: https://orbital.apjc.amp.cisco.com/help/

Indirizzi IP statici

Se il firewall blocca le connessioni TCP in uscita sulla porta 443 (in genere non è così), è necessario modificare le impostazioni del firewall prima di aggiornare i criteri. Se il tuo account è stato creato dopo febbraio 2016, disponi già di indirizzi IP statici scritti nei criteri standard. Se l'account è stato creato prima di febbraio 2016, è possibile contattare il Cisco Technical Assistance Center (TAC) per richiedere una migrazione dei criteri agli indirizzi IP statici.

Nota: per garantire la continuità delle operazioni e per assicurare che le disposizioni di malware rilevate per i file siano le stesse in entrambi i Firepower Management Center, sia il centro di gestione principale che quello secondario devono avere accesso ai server elencati in questo documento.

Nota: Cisco Secure Endpoint Console non utilizza IP statici e deve essere accessibile tramite DNS.

Indirizzi IP statici in Nord America	Indirizzi IP statici in Europa	Indirizzi IP statici in APJC
23.23.197.169 23.23.198.191	46.51.181.139 46.51.182.195	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
	54.217.232.226	52.196.115.166
	54.217.232.234	52.196.31.86

52.70.63.25
54.83.45.221
54.88.208.235

54.204.8.61
54.221.210.7
54.221.255.190
54.225.226.117
54.225.227.9
54.225.227.30
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

54.217.232.241
54.217.232.244
54.217.232.249
54.228.250.255
54.246.88.192
54.247.189.117

54.74.229.75

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

104.18.4.5
104.18.5.5

52.3.48.165
52.6.245.67

34.120.67.236
34.98.122.109

52.197.121.237
52.198.147.230
52.198.195.125
52.198.202.24
52.198.221.53
52.198.223.169
52.198.225.221
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

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

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		

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).