

Configurare gli IP e le regole firewall richiesti da Analisi malware protetta

Sommario

[Introduzione](#)

[Problema](#)

[Ambiente](#)

[Risoluzione](#)

[Appliance Secure Malware Analytics](#)

[Interfaccia di amministrazione](#)

[Interfaccia pulita](#)

[Interfaccia dirty](#)

[Dirty Interface In Uscita](#)

[Interfaccia dirty in entrata](#)

[Secure Malware Analytics Cloud](#)

[Cloud statunitense](#)

[Cloud Europa \(UE\)](#)

[Cloud Canada \(CA\)](#)

[Australia \(AU\) Cloud](#)

[India \(IN\) Cloud](#)

[Contenuto correlato](#)

Introduzione

In questo documento vengono descritti i nomi host, gli indirizzi IP e le porte richiesti per Cisco Secure Malware Analytics (cloud e appliance).

Problema

Cisco Secure Malware Analytics richiede connettività in entrata e in uscita a nomi host, indirizzi IP e porte specifici. Se questi flussi vengono bloccati, è possibile che si verifichino errori in alcune funzionalità, ad esempio l'accesso al portale, gli aggiornamenti, le licenze, il supporto remoto e le integrazioni.

Ambiente

 Nota: Fare riferimento a questo documento, che include ulteriori IP e porte per altri servizi. [IP e porte necessari per Threat Grid](#)

Nel documento sono inclusi altri indirizzi IP e porte per altri servizi basati sulla versione dell'accessorio.

Consultare la documentazione delle Guide all'installazione e all'aggiornamento: [Guide all'installazione di appliance Threat Grid](#)

Risoluzione

Regole firewall per il firewall a monte del dispositivo:

*Gli IP erano corretti al momento della pubblicazione. Verificare localmente tramite nslookup che siano ancora corretti.

Appliance Secure Malware Analytics

Interfaccia di amministrazione

Origine	Destinazione	Protocollo	Port	Direzione	Azione	Note
QUALSIASI	Interfaccia di amministrazione	TCP	22	DENTRO	Allow (Autorizza)	SSH
QUALSIASI	Interfaccia di amministrazione	TCP	80/443	DENTRO	Allow (Autorizza)	Consente l'accesso all'interfaccia GUI di amministrazione.
Interfaccia di amministrazione	IP server NFS	TCP	2049	USCITA	Allow (Autorizza)	*Deve essere aperto per utilizzare la funzione di backup o clustering NFS.

Interfaccia pulita

Origine	Destinazione	Protocollo	Port	Direzione	Azione	Note
QUALSIASI	Interfaccia pulita	TCP	80/443	DENTRO	Allow (Autorizza)	Consente l'accesso all'interfaccia GUI pulita.
QUALSIASI	Interfaccia pulita	TCP	8443	DENTRO	Allow (Autorizza)	*Deve essere aperto per utilizzare la funzione Admin over Clean.
QUALSIASI	Interfaccia pulita	TCP	9443	DENTRO	Allow (Autorizza)	*Deve essere aperto per utilizzare la funzione Glovebox di esempio.
Interfaccia pulita	Server Relay Di Posta Elettronica Configurato	TCP	25	USCITA	Consenti	L'accessorio utilizza un'interfaccia pulita per avviare le connessioni SMTP al server di posta configurato.
Interfaccia pulita	Server DNS pulito configurato	TCP/UDP	53	USCITA	Allow (Autorizza)	*Facoltativo, richiesto solo se è configurato Clean DNS (Pulitura DNS).
Interfaccia pulita	Server syslog configurato	TCP/UDP	514	USCITA	Allow (Autorizza)	Consente la connettività al server designato per la ricezione dei messaggi Syslog e delle notifiche alla griglia delle minacce.
Interfaccia pulita	Server LDAP	TCP/UDP	389/636	USCITA	Allow (Autorizza)	*Facoltativo, richiesto solo se LDAP è configurato.

Interfaccia dirty

Dirty Interface In Uscita

Origine	Destinazione	Protocollo	Port	Azione	Nota
Interfaccia dirty	Internet	QUALSIASI	QUALSIASI	Allow (Autorizza)	Consente il traffico in uscita da esempi, facoltativamente inoltrati tramite centri dati Cisco. (Per ottenere risultati accurati, è necessario che il malware sia autorizzato a contattare il proprio server di comando e controllo utilizzando qualsiasi porta e protocollo che è progettato per utilizzare.)

Interfaccia dirty in entrata

Origine	Destinazione	Protocollo	Port	Azione	Nota
QUALSIASI	Internet sporco	QUALSIASI	QUALSIASI	Nega	Nega tutte le connessioni in ingresso.

Origine	Destinazione	Protocollo	Port	Azione	Nota
Interfaccia dirty	Internet	TCP	22	Allow (Autorizza)	Aggiornare, supportare i servizi di snapshot e gestione licenze.
Interfaccia dirty	Internet	TCP/UDP	53	Allow (Autorizza)	Consenti DNS in uscita.
Interfaccia dirty	Internet	UDP	123	Allow (Autorizza)	Consenti NTP in uscita.
Interfaccia dirty	Internet	TCP	19791	Allow (Autorizza)	Consente la connettività al supporto di analisi malware protetto.
Interfaccia dirty	Cisco Umbrella	TCP	443	Allow (Autorizza)	Connessione con servizi di rilevamento e arricchimento di terze parti.
Interfaccia	TotaleVirus	TCP	443	Allow	Connessione con servizi di

dirty				(Autorizza)	rilevamento e arricchimento di terze parti.
Interfaccia dirty	TitaniumCloud	TCP	443	Allow (Autorizza)	Connessione con servizi di rilevamento e arricchimento di terze parti.



Avviso: Gli indirizzi IP elencati rimangono attivi dopo il 29 maggio 2023.

Origine	Destinazione	Protocollo	Port	Direzione	Nome host	Dettagli
Interfaccia dirty	63.97.201.96 63.162.55.96	TCP	19791	USCITA	rash.threatgrid.com	Supporto remoto/Modalità di supporto accessorio
Interfaccia dirty	63.97.201.97 63.162.55.97	TCP	22	USCITA	appliance-updates.threatgrid.com	Utilizzato per il caricamento automatico della diagnostica di supporto.  Nota: Richiede la versione software 1.2+
Interfaccia dirty	63.97.201.98 63.162.55.98	TCP	22	USCITA	support-snapshots.threatgrid.com	Utilizzato per il caricamento automatico della diagnostica di supporto.  Nota: Richiede la versione

						software 1.2+
Interfaccia dirty	63.97.201.99 63.162.55.99	TCP	22	USCITA	appliance- licensing.threatgrid.com	Gestione delle licenze

Secure Malware Analytics Cloud

Cloud statunitense

URL di accesso: <https://panacea.threatgrid.com>

Nome host	IP	Port	Dettagli
panacea.threatgrid.com	IPv4: 63.97.201.67 63.162.55.67 IPv6: 2602:811:9007:6::61 2602:811:900b:6:10:6e	443	Per il portale di analisi sicura dei malware e i dispositivi integrati (ESA/WSA/FTD/ODNS/Meraki)
glovebox.chi.threatgrid.com	IPv4: 200.194.241.35 IPv6: 2602:811:900f:06:06:6e	443	Finestra Interazione di esempio
glovebox.rcn.threatgrid.com	IPv4: 63.97.201.67 IPv6:	443	Finestra Interazione di esempio

	2602:811:9007:6::61		
glovebox.scl.threatgrid.com	IPv4: 63.162.55.67 IPv6: 2602:811:900b:6:10:6e	443	Finestra Interazione di esempio
fmc.api.threatgrid.com	IPv4: 63.97.201.67 63.162.55.67 IPv6: 2602:811:9007:6::61 2602:811:900b:6:10:6e	443	Servizio analisi file FMC/FTD

Cloud Europa (UE)

URL di accesso: <https://panacea.threatgrid.eu>

Nome host	IP	Port	Dettagli
panacea.threat.eu	IPv4: 62.67.214.195 200.194.242.35 200.194.245.35 IPv6: 2602:811:9006:6:6:6 2602:811:900c:06:06:6e	443	Per il portale di analisi sicura dei malware e i dispositivi integrati (ESA/WSA/FTD/ODNS/Meraki)
glovebox.muc.threat.eu	IPv4: 62.67.214.195	3	Finestra Interazione di esempio

	200.194.245.35 IPv6: 2602:811:900c:06:06:6e		
glovebox.fam.threat.eu	IPv4: 200.194.242.35 IPv6: 2602:811:9006:6:6:6	443	Finestra Interazione di esempio
fmc.api.threat.eu	IPv4: 62.67.214.195 200.194.242.35 200.194.245.35 IPv6: 2602:811:9006:6:6:6 2602:811:900c:06:06:6e	443	Servizio di analisi FMC/FTDFile

Il vecchio IP 89.167.128.132 è stato ritirato. Aggiornare le regole del firewall con questi IP.

Cloud Canada (CA)

URL di accesso: <https://panacea.threatgrid.ca>

Nome host	IP	Port	Dettagli
panacea.threatgrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6:06:06e	443	Per il portale di analisi sicura dei malware e i dispositivi integrati (ESA/WSA/FTD/ODNS/Meraki)

glovebox.kam.threat.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6:06:06e	443	Finestra Interazione di esempio
fmc.api.threat.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6:06:06e	443	Servizio analisi file FMC/FTD

Australia (AU) Cloud

URL di accesso: <https://panacea.threatgrid.com.au>

Nome host	IP	Port	Dettagli
panacea.threatgrid.com.au	IPv4: 200.194.246.35 200.194.247.35 IPv6: 2602:811:900e:6:10:6e 2602:811:9003:6:6:6	443	Per il portale di analisi sicura dei malware e i dispositivi integrati (ESA/WSA/FTD/ODNS/Meraki)
glovebox.syd.threatgrid.com.au	IPv4: 200.194.246.35 200.194.247.35 IPv6: 2602:811:900e:6:10:6e 2602:811:9003:6:6:6	443	Finestra Interazione di esempio

fmc.api.threatgrid.com.au	IPv4: 200.194.246.35 200.194.247.35 IPv6: 2602:811:900e:6:10:6e 2602:811:9003:6:6:6	443	Servizio analisi file FMC/FTD
---	--	-----	-------------------------------

India (IN) Cloud

URL di accesso: <https://panacea.threatgrid.in>

Nome host	IP	Port	Dettagli
panacea.minaccia.grigliasi	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6:6e	443	Per il portale di analisi sicura dei malware e i dispositivi integrati (ESA/WSA/FTD/ODNS/Meraki)
glovebox.bom.thregrid.in	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6:6e	443	Finestra Interazione di esempio
fmc.api.threatgrid.com.in	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6:6e	443	Servizio analisi file FMC/FTD

Per ulteriori requisiti di Cisco Secure Malware Analytics, ad esempio gli accessori, vedere questo articolo:

Contenuto correlato

Per i requisiti più recenti, vedere .

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).