IP e porte necessari per l'analisi sicura del malware

Sommario

Introduzione

Questo documento delinea le configurazioni di rete essenziali da implementare sul firewall per garantire il funzionamento senza problemi di Secure Malware Analytics.

Contributo dei tecnici Cisco TAC.

Cloud Secure Malware Analytics

US (Stati Uniti) Cloud

URL di accesso: https://panacea.threatgrid.com)

Nome host	IP	Port	Dettagli
panacea.threatgrid.com	63.97.201.67, 63.162.55.67	443	Per il portale di analisi sicura dei malware e i dispositivi integrati (ESA/WSA/FTD/ODNS/Meraki)
glovebox.chi.threatgrid.com	200.194.241.35	443	Finestra Interazione di esempio
glovebox.rcn.threatgrid.com	63.97.201.67	443	Finestra Interazione di esempio
glovebox.scl.threatgrid.com	63.162.55.67	443	Finestra Interazione di esempio

fmc.api.threatgrid.com	63.97.201.67, 63.162.55.67	443	Servizio analisi file FMC/FTD

Cloud UE (Europa)

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

Nome host	IP	Port	Dettagli
panacea.threat.eu	62.67.214.195, 200.194.242.35	443	Per il portale di analisi sicura dei malware e i dispositivi integrati (ESA/WSA/FTD/ODNS/Meraki)
glovebox.muc.threat.eu	62.67.214.195	443	Finestra Interazione di esempio
glovebox.fam.threat.eu	200.194.242.35	443	Finestra Interazione di esempio
fmc.api.threat.eu	62.67.214.195, 200.194.242.35	443	Servizio analisi file FMC/FTD

Il vecchio IP 89.167.128.132 è stato ritirato. Aggiornare le regole del firewall con gli IP sopra indicati.

CA (Canada) Cloud

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

Nome host	IP	Port	Dettagli
panacea.thregrid.ca	200.194.240.35	443	Per il portale di analisi sicura dei malware e i dispositivi integrati (ESA/WSA/FTD/ODNS/Meraki)
glovebox.kam.threat.ca	200.194.240.35	443	Finestra Interazione di esempio
fmc.api.threat.ca	200.194.240.35	443	Servizio analisi file FMC/FTD

AU (Australia) Cloud

URL di accesso:https://panacea.threatgrid.au

Nome host	IP	Port	Dettagli
panacea.threatgrid.com.au	124.19.22.171	443	Per il portale di analisi sicura dei malware e i dispositivi integrati (ESA/WSA/FTD/ODNS/Meraki)
glovebox.syd.threatgrid.com.au	124.19.22.171	443	Finestra Interazione di esempio

fmc.api.threatgrid.com.au	124.19.22.171	443	Servizio analisi file FMC/FTD

Appliance Secure Malware Analytics

Di seguito sono riportate le regole firewall consigliate per ciascuna interfaccia di Secure Malware Analytics Appliance.

Interfaccia dirty

Utilizzato dalle macchine virtuali per comunicare con Internet in modo che gli esempi possano risolvere il DNS e comunicare con i server di comando e controllo (C&C)

Consenti:

Direzione	Protocollo	Port	Destinazione	Nome host	Dettagli
In uscita	IP	QUALSIASI	QUALSIASI		Consigliato, ad eccezione dei casi specificati nella sezione **Nega**. Utilizzato per consentire la connettività per l'analisi.
In uscita	TCP	22	54.173.231.161 1 63.97.201.98 [2] 63.162.55.98 [2]	support-snapshots.threatgrid.com	Utilizzato per il caricamento automatico della diagnostica di supporto Nota: è richiesta la versione software 1.2+
In uscita	TCP	22	54.173.181.217 [1] , 54.173.182.46 [1] 63.162.55.97 [2] 63.97.201.97 [2]	appliance-updates.threatgrid.com	Aggiornamenti accessorio
In uscita	TCP	19791	54.164.165.137 [1], 34.199.44.202.[1] 63.97.201.96 [2], 63.162.55.96.[2]	rash.threatgrid.com	Supporto remoto/Modalità di supporto accessorio
In uscita	TCP	22	63.97.201.99 63.162.55.99	appliance-licensing.threatgrid.com	Gestione delle licenze

[1]Questi IP verranno disabilitati nel prossimo futuro.

[2]Questi sono i PI che sostituirebbero quelli indicati nel punto [1]. Si consiglia di aggiungere entrambi gli IP fino a quando la comunicazione sulle modifiche IP non verrà effettuata nel prossimo futuro.

Uscita dalla rete remota

Utilizzato dall'accessorio per il tunneling del traffico VM verso un'uscita remota precedentemente nota come tg-tunnel.

Direzione	Protocollo	Port	Destinazione
In uscita	TCP	21413	163.182.175.193

In uscita	TCP	21417	69.55.5.250
In uscita	TCP	21415	69.55.5.250
In uscita	TCP	21413	76.8.60.91

Nota: l'uscita remota 4.14.36.142 è stata rimossa e non è più in produzione. Accertarsi che tutti gli IP menzionati siano stati aggiunti all'elenco delle eccezioni del firewall.

Nega:

Direzione	Protocollo	Porta/e	Destinazione	Dettagli
In uscita	SMTP	QUALSIASI	QUALSIASI	Per evitare che il malware invii posta indesiderata.
In entrata	IP	QUALSIASI	Interfaccia dirty appliance di analisi malware sicura	Consigliato, ad eccezione dei casi specificati nella sezione **Consenti** sopra. Consente la comunicazione per l'analisi.

Interfaccia pulita

Utilizzato da diversi servizi connessi per inviare esempi e per consentire agli analisti l'accesso all'interfaccia utente.

Consenti:

Direzione	Protocollo	Porta/e	Destinazione	Dettagli
In entrata	TCP	443 e 8443	Interfaccia Clean di Secure Malware Analytics	Accesso a WebUI e API
In entrata	TCP	9443	Interfaccia Clean di Secure Malware Analytics	Utilizzato per Glovebox
In entrata	TCP	22	Interfaccia Clean di Secure Malware Analytics	Accesso all'interfaccia utente di amministrazione su SSH
In uscita	TCP	19791	**Host:** rash.threatgrid.com 54.164.165.137 [1] 34.199.44.202.[1] 63.97.201.96 [2] 63.162.55.96 [2]	Modalità di ripristino per il supporto di analisi malware sicuro.

[1]Questi IP verranno disabilitati nel prossimo futuro.

[2]Questi sono i PI che sostituirebbero quelli indicati nel punto [1]. Si consiglia di aggiungere entrambi gli IP fino a quando la comunicazione sulle modifiche IP non verrà effettuata nel prossimo futuro.

Interfaccia di amministrazione

Accesso all'interfaccia utente di amministrazione.

Consenti:

Direzione	Protocollo	Porta/e	Destinazione	Dettagli
In entrata	TCP	443 e 8443	Interfaccia di amministrazione di Secure Malware Analytics	Utilizzato per configurare le impostazioni per hardware e licenze.
In ingresso	TCP	22	Interfaccia di amministrazione di Secure Malware Analytics	Accesso all'interfaccia utente di amministrazione su SSH

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).