Vereiste IP’s en poorten voor Secure Malware Analytics

Inhoud

Inleiding

Dit document beschrijft de netwerkinformatie die aan uw firewall moet worden toegevoegd om Secure Malware Analytics goed te laten werken.

Bijgedragen door Cisco TAC-engineers.

Secure Malware Analytics-clouds

VS(Verenigde Staten) Cloud

Access URL: https://panacea.threatgrid.com)

Hostname	IP	Port	Gegevens
panacea.threatgrid.com	63.97.201.67 4.14.36.148 63.162.55.67	443	Voor Secure Malware Analytics-portal en geïntegreerde apparaten (ESA/WSA/FTD/ODNS/Meraki)
glovebox.chi.threatgrid.com	200.194.241.35	443	Voorbeeldvenster Interactie
glovebox.rcn.threatgrid.com	63.97.201.67	443	Voorbeeldvenster Interactie

glovebox.scl.threatgrid.com	63.162.55.67	443	Voorbeeldvenster Interactie
fmc.api.threatgrid.com	63.97.201.67 4.14.36.148	443	FMC/FTD-service voor bestandsanalyse

EU(Europe) Cloud

Access URL: https://panacea.threatgrid.eu

Hostname	IP	Port	Gegevens
panacea.bedreiggrid.eu	89.167.128.132	443	Voor Secure Malware Analytics-portal en geïntegreerde apparaten (ESA/WSA/FTD/ODNS/Meraki)
glovebox.bedreiggrid.eu	89.167.128.132	443	Voorbeeldvenster Interactie
fmc.api.bedreiggrid.eu	89.167.128.132	443	FMC/FTD-service voor bestandsanalyse

Vanaf 13 januari 2024 wordt het IP gewijzigd voor de EU Cloud. De oude IP's zouden met pensioen gaan. Dit kan worden gewijzigd. Als dit wordt uitgesteld, wordt het document dienovereenkomstig bijgewerkt.

Dit zijn de nieuwe IP's die naar buiten moeten kunnen worden verzonden om de Malware Analytics Cloud-functionaliteit goed te laten functioneren.

Hostname	IP	Port	Gegevens
panacea.bedreiggrid.eu	62.67.214.195 200.194.242.35	443	Voor Secure Malware Analytics-portal en geïntegreerde apparaten (ESA/WSA/FTD/ODNS/Meraki)
glovebox.muc.bedreiggrid.eu	62.67.214.195	443	Voorbeeldvenster Interactie
glovebox.fam.bedreiggrid.eu	200.194.242.35	443	Voorbeeldvenster Interactie
fmc.api.bedreiggrid.eu	62 67 214 195 200 194 242 35	443	FMC/FTD-service voor bestandsanalyse

CA(Canada) Cloud

Access URL: https://panacea.threatgrid.ca

Hostname	IP	Port	Gegevens

panacea.bedreiggrid.ca	200.194.240.35	443	Voor Secure Malware Analytics-portal en geïntegreerde apparaten (ESA/WSA/FTD/ODNS/Meraki)
glovebox.kam.bedreiggrid.ca	200.194.240.35	443	Voorbeeldvenster Interactie
fmc.api.bedreiggrid.ca	200.194.240.35	443	FMC/FTD-service voor bestandsanalyse

AU(Australië) Cloud

Access URL: https://panacea.threatgrid.au

Hostname	IP	Port	Gegevens
panacea.threatgrid.com.au	124.19.22.171	443	Voor Secure Malware Analytics-portal en geïntegreerde apparaten (ESA/WSA/FTD/ODNS/Meraki)
glovebox.syd.threatgrid.com.au	124.19.22.171	443	Voorbeeldvenster Interactie
fmc.api.threatgrid.com.au	124.19.22.171	443	FMC/FTD-service voor bestandsanalyse

Secure Malware Analytics-applicatie

Dit zijn de aanbevolen firewallregels per interface van de Secure Malware Analytics-applicatie.

Vuile interface

Gebruikt door VM's om te communiceren met het internet, zodat monsters DNS kunnen oplossen en kunnen communiceren met commando en controle (C&C) servers
Toestaan:

Richting	Protocol	Port	Bestemming	Hostname	Gegevens
Uitgaand	IP	ALLE	ALLE		Aanbevolen behalve waar hier opgegeven in het gedeelte Deny. Gebruikt om connectiviteit voor analyse toe te staan.
Uitgaand	TCP	22	54.173.231.161 1 63.97.201.98 2 63.162.55.98 2	support-snapshots.threatgrid.com	Gebruikt voor automatische ondersteuning van diagnostische uploads Opmerking: vereist softwareversie 1.2+
Uitgaand	TCP	22	54.173.181.217 1 54.173.182.46 1	appliance-updates.threatgrid.com	Applicatie updates

			63.162.55.97 2 63.97.201.97 2		
Uitgaand	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	Remote-ondersteuning/modus voor applicatie-ondersteuning
Uitgaand	TCP	22	63.97.201.99 63.162.55.99	appliance-licensing.threatgrid.com	Licentiebeheer

[1]Deze IP's worden in de nabije toekomst uitgeschakeld.

[2]Dit zijn de IP's die de in [1] genoemde vervangen. Wij stellen voor om beide IP's toe te voegen totdat de communicatie over de IP-wijzigingen in de nabije toekomst is gemaakt.

Exit van extern netwerk

Gebruikt door het apparaat om VM-verkeer te tunnelen naar een externe uitgang voorheen bekend als tg-tunnel.

Richting	Protocol	Port	Bestemming
Uitgaand	TCP	21413	163.182.175.193
Uitgaand	TCP	21417	69.55.5.250
Uitgaand	TCP	21415	69.55.5.250
Uitgaand	TCP	21413	76.8.60.91

Opmerking: Remote Exit 4.14.36.142 is verwijderd en is niet langer in productie. Zorg ervoor dat alle genoemde IP's worden toegevoegd aan de lijst met uitzonderingen voor firewalls.

Ontkennen:

Richting	Protocol	Poorten	Bestemming	Gegevens
Uitgaand	SMTP	ALLE	ALLE	Om te voorkomen dat malware spam verstuurt.
Inkomend	IP	ALLE	Secure Malware Analytics-applicatie met vuile interface	Aanbevolen, behalve waar dit in het bovenstaande gedeelte Toestaan is gespecificeerd. Gebruikt om communicatie voor analyse toe te staan.

Clean-interface

Gebruikt door verschillende verbonden diensten om monsters in te dienen en UI-toegang voor analisten.
Toestaan:

Richting	Protocol	Poorten	Bestemming	Gegevens
Inkomend	TCP	443 8443	Secure Malware Analytics-applicatie met schone interface	WebUI- en API-toegang
Inkomend	TCP	9443	Secure Malware Analytics-applicatie met schone interface	Gebruikt voor Glovebox
Uitgaand	TCP	19791	Host: rash.threatgrid.com IP: 54 164 165 137 [1] IP: 34.199.44.2002 [1] IP: 63.97.201.96[2] IP: 63.162.55.96 [2]	Herstelmodus voor ondersteuning van Secure Malware Analytics.

[1]Deze IP's worden in de nabije toekomst uitgeschakeld.

[2]Dit zijn de IP's die de in [1] genoemde vervangen. Wij stellen voor om beide IP's toe te voegen totdat de communicatie over de IP-wijzigingen in de nabije toekomst is gemaakt.

Admin-interface

Toegang tot de administratie-gebruikersinterface.
Toestaan:

Richting	Protocol	Poorten	Bestemming	Gegevens
Inkomend	TCP	443 8443	Secure Malware Analytics-applicatie - Admin-interface	Hiermee configureert u instellingen voor hardware en licenties.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.