

Beveiligde malware-analyse configureren

Vereiste IP's en firewallregels

Inhoud

[Inleiding](#)

[uitgifte](#)

[milieu](#)

[resolutie](#)

[Secure Malware Analytics-apparaat](#)

[Admin-interface](#)

[Schone interface](#)

[vuile interface](#)

[Dirty Interface Outbound](#)

[Dirty Interface Inbound](#)

[Secure Malware Analytics Cloud](#)

[Verenigde Staten \(VS\) Cloud](#)

[Cloud in Europa \(EU\)](#)

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

[Cloud in Australië \(AU\)](#)

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

[Gerelateerde inhoud](#)

Inleiding

Dit document beschrijft de hostnamen, IP-adressen en poorten die nodig zijn voor Cisco Secure Malware Analytics (cloud en toestel).

uitgifte

Cisco Secure Malware Analytics vereist uitgaande en inkomende connectiviteit met specifieke hostnamen, IP-adressen en poorten. Als deze stromen worden geblokkeerd, kunnen functies zoals portaaltoegang, updates, licenties, externe ondersteuning en integraties mislukken.

milieu



Opmerking: raadpleeg eerst dit document, dat aanvullende IP's en poorten voor andere



services bevat.

[Vereiste IP's en poorten voor Threat Grid](#)

Dit document bevat extra IP's en poorten voor andere services op basis van de toestelversie.

Raadpleeg de documentatie Installatie- en upgradehulplijnen: [Installatiehulplijnen voor bedreigingsrasters](#)

resolutie

Firewallregels voor de firewall die stroomopwaarts naar het apparaat loopt:

*IPs waren correct op het moment van publicatie. Bevestig lokaal via nslookup dat deze nog steeds correct zijn.

Secure Malware Analytics-apparaat

Admin-interface

bron	Bestemming	Protocol	Port	richting	Actie	Opmerkingen
WILLEKEURIG	Admin-interface	TCP	22	IN	Allow (toestaan)	SSH
WILLEKEURIG	Admin-interface	TCP	80/443	IN	Allow (toestaan)	Toegang toestaan tot de GUI-interface van de beheerder.
Admin-interface	IP van NFS-server	TCP	2049	UIT	Allow (toestaan)	*Moet geopend zijn om de NFS-back-up- of clusterfunctie te kunnen gebruiken.

Schone interface

bron	Bestemming	Protocol	Port	richting	Actie	Opmerkingen
------	------------	----------	------	----------	-------	-------------

WILLEKEURIG	Schone interface	TCP	80/443	IN	Allow (toestaan)	Toegang verlenen tot de Clean GUI Interface.
WILLEKEURIG	Schone interface	TCP	8443	IN	Allow (toestaan)	*Moet open zijn om Admin over Clean Feature te gebruiken.
WILLEKEURIG	Schone interface	TCP	9443	IN	Allow (toestaan)	*Moet open zijn om de voorbeeldfunctie Glovebox te gebruiken.
Schone interface	Geconfigureerde e-mailrelayserver	TCP	25	UIT	toestaan	Het toestel gebruikt de clean interface om SMTP-verbindingen met de geconfigureerde mailserver te initiëren.
Schone interface	Geconfigureerde schone DNS-server	TCP/UDP	53	UIT	Allow (toestaan)	*Optioneel, alleen vereist als Clean DNS is geconfigureerd.
Schone interface	Geconfigureerde SYSLOG-server	TCP/UDP	514	UIT	Allow (toestaan)	Verbinding toestaan met de server die is aangewezen om Syslog-berichten en meldingen over het dreigingsraster te ontvangen.
Schone interface	LDAP-server	TCP/UDP	389/636	UIT	Allow (toestaan)	*Optioneel, alleen vereist als LDAP is geconfigureerd.

vuile interface

Dirty Interface Outbound

bron	Bestemming	Protocol	Port	Actie	Opmerking
------	------------	----------	------	-------	-----------

vuile interface	Internet	WILLEKEURIG	WILLEKEURIG	Allow (toestaan)	Sta uitgaand verkeer van monsters toe, optioneel geproxyd via Cisco-datacenters. (Om nauwkeurige resultaten te krijgen, is het vereist dat malware contact kan opnemen met zijn command and control server met behulp van welke poort en protocol het is ontworpen om te gebruiken.)
-----------------	----------	-------------	-------------	------------------	--

Dirty Interface Inbound

bron	Bestemming	Protocol	Port	Actie	Opmerking
WILLEKEURIG	vuil internet	WILLEKEURIG	WILLEKEURIG	ontkennen	Ontken alle inkomende verbindingen.

bron	Bestemming	Protocol	Port	Actie	Opmerking
vuile interface	Internet	TCP	22	Allow (toestaan)	Updaten, ondersteunen van momentopnamen en licentiediensten.
vuile interface	Internet	TCP/UDP	53	Allow (toestaan)	Uitgaande DNS toestaan.
vuile interface	Internet	UDP	123	Allow (toestaan)	Uitgaande NTP toestaan.
vuile interface	Internet	TCP	19791	Allow (toestaan)	Connectiviteit toestaan voor de ondersteuning van Secure Malware Analytics.
vuile interface	Cisco Umbrella	TCP	443	Allow (toestaan)	Maak verbinding met detectie- en verrijkingsservices van derden.
vuile interface	Virus totaal	TCP	443	Allow (toestaan)	Maak verbinding met detectie- en verrijkingsservices van derden.

vuile interface	titaniumwolk	TCP	443	Allow (toestaan)	Maak verbinding met detectie- en verrijkingsservices van derden.
-----------------	--------------	-----	-----	------------------	--



Waarschuwing: de vermelde IP-adressen blijven actief na 29 mei 2023.

bron	Bestemming	Protocol	Port	richting	Hostnaam	Details
vuile interface	63.97.201.96 63.162.55.96	TCP	19791	UIT	rash.threatgrid.com	Ondersteuning op afstand / apparaatondersteuningsmodus
vuile interface	63.97.201.97 63.162.55.97	TCP	22	UIT	appliance-updates.threatgrid.com	Wordt gebruikt voor automatische ondersteuning van diagnostische uploads.  Opmerking: vereist softwareversie 1.2+
vuile interface	63.97.201.98 63.162.55.98	TCP	22	UIT	support-snapshots.threatgrid.com	Wordt gebruikt voor automatische ondersteuning van diagnostische uploads.  Opmerking: vereist softwareversie 1.2+
vuile interface	63.97.201.99 63.162.55.99	TCP	22	UIT	appliance-licensing.threatgrid.com	Licentiebeheer

Secure Malware Analytics Cloud

Verenigde Staten (VS) Cloud

URL voor toegang: <https://panacea.threatgrid.com>

Hostnaam	IP	Port	Details
panacea.threatgrid.com	IPv4: 63.97.201.67 63.162.55.67 IPv6: 2602:811:9007:6::61 2602:811:900b:6:6e	443	Voor Secure Malware Analytics Portal en geïntegreerde apparaten (ESA/WSA/FTD/ODNS/Meraki)
glovebox.chi.threatgrid.com	IPv4: 200 194 241 35 IPv6: 2602:811:900F:6:6E	443	Voorbeeldinteractievenster
glovebox.rcn.threatgrid.com	IPv4: 63.97.201.67 IPv6: 2602:811:9007:6::61	443	Voorbeeldinteractievenster
glovebox.scl.threatgrid.com	IPv4: 63.162.55.67 IPv6: 2602:811:900b:6:6e	443	Voorbeeldinteractievenster
fmc.api.threatgrid.com	IPv4: 63.97.201.67 63.162.55.67 IPv6:	443	Bestandsanalyseservice FMC/FTD

	2602:811:9007:6::61		
	2602:811:900b:6:6e		

Cloud in Europa (EU)

URL voor toegang: <https://panacea.threatgrid.eu>

Hostnaam	IP	Port	Details
panacea.threatGrid.eu	IPv4: 62.67.214.195 200.194.242.35 200.194.245.35 IPv6: 2602:811:9006:6:6e 2602:811:900c:6:6e	443	Voor Secure Malware Analytics Portal en geïntegreerde apparaten (ESA/WSA/FTD/ODNS/Meraki)
glovebox.muc.threatGrid.eu	IPv4: 62.67.214.195 200.194.245.35 IPv6: 2602:811:900c:6:6e	3	Voorbeeldinteractievenster
glovebox.fam.threatGrid.eu	IPv4: 200.194.242.35 IPv6: 2602:811:9006:6:6e	443	Voorbeeldinteractievenster
fmc.api.threatGrid.eu	IPv4: 62.67.214.195	443	FMC/FTDFile Analysis Service

	200.194.242.35		
	200.194.245.35		
	IPv6:		
	2602:811:9006:6:6e		
	2602:811:900c:6:6e		

Het oude IP 89.167.128.132 is met pensioen, werk uw firewallregels bij met deze IP's.

Canada (CA) Cloud

URL voor toegang: <https://panacea.threatgrid.ca>

Hostnaam	IP	Port	Details
Panacea.ThreatGrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6:6e	443	Voor Secure Malware Analytics Portal en geïntegreerde apparaten (ESA/WSA/FTD/ODNS/Meraki)
glovebox.kam.threatGrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6:6e	443	Voorbeeldinteractievenster
fmc.api.threatGrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6:6e	443	Bestandsanalyseservice FMC/FTD

Cloud in Australië (AU)

URL voor toegang: <https://panacea.threatgrid.com.au>

Hostnaam	IP	Port	Details
panacea.threatgrid.com.au	IPv4: 200.194.246.35 200.194.247.35 IPv6: 2602:811:900e:6:6e 2602:811:9003:6:6e	443	Voor Secure Malware Analytics Portal en geïntegreerde apparaten (ESA/WSA/FTD/ODNS/Meraki)
glovebox.sydney.threatgrid.com.au	IPv4: 200.194.246.35 200.194.247.35 IPv6: 2602:811:900e:6:6e 2602:811:9003:6:6e	443	Voorbeeldinteractievenster
fmc.api.threatgrid.com.au	IPv4: 200.194.246.35 200.194.247.35 IPv6: 2602:811:900e:6:6e 2602:811:9003:6:6e	443	Bestandsanalyseservice FMC/FTD

India (IN) Cloud

URL voor toegang: <https://panacea.threatgrid.in>

Hostnaam	IP	Port	Details
----------	----	------	---------

panacea.threatGrid.in	IPv4: 200.194.244.35 IPv6: 2602:8111:9001:6:6e	443	Voor Secure Malware Analytics Portal en geïntegreerde apparaten (ESA/WSA/FTD/ODNS/Meraki)
glovebox.bom.threatGrid.in	IPv4: 200.194.244.35 IPv6: 2602:8111:9001:6:6e	443	Voorbeeldinteractievenster
fmc.api.threatgrid.com.in	IPv4: 200.194.244.35 IPv6: 2602:8111:9001:6:6e	443	Bestandsanalyseservice FMC/FTD

Voor meer vereisten voor Cisco Secure Malware Analytics, zoals apparaten, raadpleegt u dit artikel:

Gerelateerde inhoud

Voor de laatste eisen, zie.

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.