IPs e portas necessários para análise segura de malware

Contents

- Introdução
- Nuvens de análise de malware seguras
  - Nuvem nos EUA (Estados Unidos)
  - Nuvem da UE (Europa)
  - Nuvem da CA (Canadá)
  - Nuvem AU (Austrália)
- Dispositivo de análise de malware seguro
  - Interface suja
  - Saída de rede remota
  - Limpar interface
  - Interface do administrador

Introdução

Este documento descreve as configurações de rede essenciais que você precisa implementar em seu firewall para garantir a operação contínua do Secure Malware Analytics.

Contribuição dos engenheiros do Cisco TAC.

Nuvens de análise de malware seguras

Nuvem nos EUA (Estados Unidos)

URL de acesso: https://panacea.threatgrid.com

Hostname	IP	Porta	Detalhes
panacea.threatgrid.com	63.97.201.67 63.162.55.67	443	Para Secure Malware Analytics Portal e dispositivos integrados (ESA/WSA/FTD/ODNS/Meraki)
glovebox.chi.threatgrid.com	200.194.241.35	443	Janela Interação de exemplo
glovebox.rcn.threatgrid.com	63.97.201.67	443	Janela Interação de exemplo
glovebox.scl.threatgrid.com	63.162.55.67	443	Janela Interação de exemplo

fmc.api.threatgrid.com	63.97.201.67 63.162.55.67	443	FMC/FTD Serviço de análise de ficheiros

Nuvem da UE (Europa)

URL de acesso: https://panacea.threatgrid.eu

Hostname	IP	Porta	Detalhes
panacea.threatgrid.eu	62.67.214.195 200.194.242.35	443	Para Secure Malware Analytics Portal e dispositivos integrados (ESA/WSA/FTD/ODNS/Meraki)
glovebox.muc.threatgrid.eu	62.67.214.195	443	Janela Interação de exemplo
glovebox.fam.threatgrid.eu	200.194.242.35	443	Janela Interação de exemplo
fmc.api.threatGrid.eu	62.67.214.195 200.194.242.35	443	FMC/FTD Serviço de análise de ficheiros

O IP antigo 89.167.128.132 foi desativado. Atualize suas regras de firewall com os IPs acima.

Nuvem da CA (Canadá)

URL de acesso:https://panacea.threatgrid.ca

Hostname	IP	Porta	Detalhes
panaceia.threatGrid.ca	200.194.240.35	443	Para Secure Malware Analytics Portal e dispositivos integrados (ESA/WSA/FTD/ODNS/Meraki)
glovebox.kam.threatGrid.ca	200.194.240.35	443	Janela Interação de exemplo
fmc.api.threatGrid.ca	200.194.240.35	443	FMC/FTD Serviço de análise de ficheiros

Nuvem AU (Austrália)

URL de acesso:https://panacea.threatgrid.com.au

Hostname	IP	Porta	Detalhes
panacea.threatgrid.com.au	124.19.22.171	443	Para Secure Malware Analytics Portal e dispositivos integrados (ESA/WSA/FTD/ODNS/Meraki)
glovebox.syd.threatgrid.com.au	124.19.22.171	443	Janela Interação de exemplo

fmc.api.threatgrid.com.au	124.19.22.171	443	FMC/FTD Serviço de análise de ficheiros

Dispositivo de análise de malware seguro

A seguir estão as regras de firewall recomendadas por interface do Secure Malware Analytics Appliance.

Interface suja

Usado pelas VMs para se comunicar com a Internet para que as amostras possam resolver DNS e se comunicar com servidores de comando e controle (C&C)

Permissão:

Direção	Protocolo	Porta	Destino	Hostname	Detalhes
Saída	IP	QUALQUER UM	QUALQUER UM		Recomendado, exceto onde especificado na seção **Negar** aqui. Usado para permitir a conectividade para análise.
Saída	TCP	22	54.173.231.161 1 63.97.201.98 2 63.162.55.98 2	support-snapshots.threatgrid.com	Usado para uploads de diagnóstico de suporte automático Observação: requer software versão 1.2+
Saída	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	Atualizações do equipamento
Saída	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	Suporte remoto / Modo de suporte do dispositivo
Saída	TCP	22	54.173.124.172 1 63.97.201.99 2 63.162.55.99 2	appliance-licensing.threatgrid.com	Gerenciamento de licenças

[1]Esses IPs serão desabilitados em um futuro próximo.

[2]Esses são os IPs que substituiriam os do [1]. Sugerimos adicionar ambos os IPs até que a comunicação sobre as alterações de IP seja feita em um futuro próximo.

Saída de rede remota

Usado pelo dispositivo para encapsular o tráfego da VM para uma saída remota conhecida anteriormente como tg-

tunnel.

Direção	Protocolo	Porta	Destino
Saída	TCP	21413	173.198.252.53
Saída	TCP	21413	163.182.175.193 **
Saída	TCP	21417	69.55.5.250
Saída	TCP	21415	69.55.5.250
Saída	TCP	21413	76.8.60.91

Observação: a saída remota 4.14.36.142 foi removida e não está mais em produção. Verifique se todos os IPs mencionados foram adicionados à sua lista de exceções de firewall.

** A saída remota 163.182.175.193 será substituída por 173.198.252.53

Negar:

Direção	Protocolo	Porta(s)	Destino	Detalhes
Saída	SMTP	QUALQUER UM	QUALQUER UM	Para evitar que o malware envie spam.
Entrada	IP	QUALQUER UM	Secure Malware Analytics Appliance Dirty Interface	Recomendado, exceto quando especificado na seção **Permitir** acima. Usado para permitir comunicação para análise.

Limpar interface

Usado por vários serviços conectados para enviar amostras, bem como acesso de IU para analistas.

Permissão:

Direção	Protocolo	Porta(s)	Destino	Detalhes
Entrada	TCP	443 e 8443	Secure Malware Analytics Appliance Clean Interface	Acesso a WebUI e API
Entrada	TCP	9443	Secure Malware Analytics Appliance Clean Interface	Usado para Glovebox
Entrada	TCP	22	Secure Malware Analytics	Acesso TUI de administração sobre SSH

			Appliance Clean Interface	
Saída	TCP	19791	**Anfitrião:** rash.threatgrid.com 54.164.165.137 [1] ,34.199.44.202 [1] 63.97.201.96 [2] , 63.162.55.96 [2]	Modo de recuperação para suporte analítico seguro contra malware.

[1]Esses IPs serão desabilitados em um futuro próximo.

[2]Esses são os IPs que substituiriam os do [1]. Sugerimos adicionar ambos os IPs até que a comunicação sobre as alterações de IP seja feita em um futuro próximo.

Interface do administrador

Acesso à interface de usuário da administração.

Permissão:

Direção	Protocolo	Porta(s)	Destino	Detalhes
Entrada	TCP	443 e 8443	Interface de administração do Secure Malware Analytics Appliance	Usado para definir as configurações de hardware e licenciamento.
Entrada	TCP	22	Interface de administração do Secure Malware Analytics Appliance	Acesso TUI de administração sobre SSH

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.