

Configurar IPs e regras de firewall seguros necessários para a análise de malware

Contents

[Introdução](#)

[Problema](#)

[Ambiente](#)

[Resolução](#)

[Dispositivo de análise de malware seguro](#)

[Interface do administrador](#)

[Limpar interface](#)

[Interface suja](#)

[Saída de interface suja](#)

[Entrada de interface suja](#)

[Nuvem de análise de malware segura](#)

[Nuvem nos Estados Unidos \(EUA\)](#)

[Nuvem na Europa \(UE\)](#)

[Nuvem no Canadá \(CA\)](#)

[Nuvem da Austrália \(AU\)](#)

[Nuvem da Índia \(IN\)](#)

[Conteúdo relacionado](#)

Introdução

Este documento descreve os nomes de host, endereços IP e portas necessários para o Cisco Secure Malware Analytics (nuvem e dispositivo).

Problema

O Cisco Secure Malware Analytics requer conectividade de saída e de entrada para nomes de host, endereços IP e portas específicos. Se esses fluxos forem bloqueados, recursos como acesso ao portal, atualizações, licenciamento, suporte remoto e integrações poderão falhar.

Ambiente



Note: Consulte primeiro este documento, que inclui portas e IPs adicionais para outros



serviços.

[IPs e portas necessários para o Threat Grid](#)

Este documento inclui IPs e portas adicionais para outros serviços com base na versão do dispositivo.

Consulte a documentação dos Guias de instalação e atualização: [Guias de instalação de dispositivos do Threat Grid](#)

Resolução

Regras de firewall para o upstream do firewall para o dispositivo:

*Os IPs estavam corretos no momento da publicação. Confirme localmente via nslookup que eles ainda estão corretos.

Dispositivo de análise de malware seguro

Interface do administrador

Fonte	Destino	Protocolo	Porta	Direção	Ação	Notas
QUALQUER UM	Interface do administrador	TCP	22	IN	Permissão	SSH
QUALQUER UM	Interface do administrador	TCP	80/443	IN	Permissão	Permita o acesso à interface GUI do administrador.
Interface do administrador	IP do Servidor NFS	TCP	2049	OUT	Permissão	*Deve estar aberto para usar o recurso de Backup NFS ou Clustering.

Limpar interface

Fonte	Destino	Protocolo	Porta	Direção	Ação	Notas
-------	---------	-----------	-------	---------	------	-------

QUALQUER UM	Limpar interface	TCP	80/443	IN	Permissão	Permita o acesso à interface de GUI limpa.
QUALQUER UM	Limpar interface	TCP	8443	IN	Permissão	*Deve estar aberto para usar o recurso Admin over Clean.
QUALQUER UM	Limpar interface	TCP	9443	IN	Permissão	*Deve estar aberto para usar o recurso Glovebox de exemplo.
Limpar interface	Email Relay Server configurado	TCP	25	OUT	Permitir	O equipamento usa a interface de limpeza para iniciar conexões SMTP com o servidor de e-mail configurado.
Limpar interface	Servidor DNS limpo configurado	TCP/UDP	53	OUT	Permissão	*Opcional, necessário apenas se Limpar DNS estiver configurado.
Limpar interface	Servidor Syslog configurado	TCP/UDP	514	OUT	Permissão	Permita a conectividade com o servidor designado para receber mensagens de Syslog e notificações do Threat Grid.
Limpar interface	Servidor LDAP	TCP/UDP	389/636	OUT	Permissão	*Opcional, necessário apenas se o LDAP estiver configurado.

Interface suja

Saída de interface suja

Fonte	Destino	Protocolo	Porta	Ação	Nota
-------	---------	-----------	-------	------	------

Interface suja	Internet	QUALQUER UM	QUALQUER UM	Permissão	Permitir o tráfego de saída de amostras, opcionalmente encaminhado por proxy através dos datacenters da Cisco. (Para obter resultados precisos, é necessário que o malware tenha permissão para entrar em contato com seu servidor de comando e controle usando qualquer porta e protocolo projetados para usar.)
-------------------	----------	----------------	----------------	-----------	---

Entrada de interface suja

Fonte	Destino	Protocolo	Porta	Ação	Nota
QUALQUER UM	Internet suja	QUALQUER UM	QUALQUER UM	Negar	Negar todas as conexões de entrada.

Fonte	Destino	Protocolo	Porta	Ação	Nota
Interface suja	Internet	TCP	22	Permissão	Serviços de atualização, instantâneo de suporte e licenciamento.
Interface suja	Internet	TCP/UDP	53	Permissão	Permitir DNS de saída.
Interface suja	Internet	UDP	123	Permissão	Permitir NTP de saída.
Interface suja	Internet	TCP	19791	Permissão	Permita a conectividade para o suporte Secure Malware Analytics.
Interface suja	Guarda-chuva da Cisco	TCP	443	Permissão	Conecte-se com serviços de detecção e enriquecimento de terceiros.
Interface suja	Total deVírus	TCP	443	Permissão	Conecte-se com serviços de detecção e enriquecimento de terceiros.
Interface suja	Nuvem detitânio	TCP	443	Permissão	Conecte-se com serviços de detecção e enriquecimento de terceiros.



aviso: Os endereços IP listados permanecem ativos após 29 de maio de 2023.

Fonte	Destino	Protocolo	Porta	Direção	Hostname	Detalhes
Interface suja	63.97.201.96 63.162.55.96	TCP	19791	OUT	rash.threatgrid.com	Suporte remoto / Modo de suporte do dispositivo
Interface suja	63.97.201.97 63.162.55.97	TCP	22	OUT	appliance- updates.threatgrid.com	Usado para uploads de diagnóstico de suporte automático.  Note: Requer software versão 1.2+
Interface suja	63.97.201.98 63.162.55.98	TCP	22	OUT	support- snapshots.threatgrid.com	Usado para uploads de diagnóstico de suporte automático.  Note: Requer software versão 1.2+
Interface suja	63.97.201.99 63.162.55.99	TCP	22	OUT	appliance- licensing.threatgrid.com	Gerenciamento de licenças

Nuvem de análise de malware segura

Nuvem nos Estados Unidos (EUA)

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

Hostname	IP	Porta	Detalhes
panacea.threatgrid.com	IPv4: 63.97.201.67 63.162.55.67 IPv6: 2602:811:9007:6::61 2602:811:900b:6::6e	443	Para Secure Malware Analytics Portal e dispositivos integrados (ESA/WSA/FTD/ODNS/Meraki)
glovebox.chi.threatgrid.com	IPv4: 200.194.241.35 IPv6: 2602:811:900f:6::6e	443	Janela Interação de exemplo
glovebox.rcn.threatgrid.com	IPv4: 63.97.201.67 IPv6: 2602:811:9007:6::61	443	Janela Interação de exemplo
glovebox.scl.threatgrid.com	IPv4: 63.162.55.67 IPv6: 2602:811:900b:6::6e	443	Janela Interação de exemplo
fmc.api.threatgrid.com	IPv4: 63.97.201.67 63.162.55.67 IPv6: 2602:811:9007:6::61	443	FMC/FTD Serviço de análise de ficheiros

	2602:811:900b:6::6e		
--	---------------------	--	--

Nuvem na Europa (UE)

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

Hostname	IP	Porta	Detalhes
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	Para Secure Malware Analytics Portal e dispositivos integrados (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	Janela Interação de exemplo
glovebox.fam.threatgrid.eu	IPv4: 200.194.242.35 IPv6: 2602:811:9006:6::6e	443	Janela Interação de exemplo
fmc.api.threatGrid.eu	IPv4: 62.67.214.195 200.194.242.35	443	FMC/FTDServiço de análise de ficheiros

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

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

Nuvem no Canadá (CA)

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

Hostname	IP	Porta	Detalhes
panacea.threatGrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	443	Para Secure Malware Analytics Portal e dispositivos integrados (ESA/WSA/FTD/ODNS/Meraki)
glovebox.kam.threatGrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	443	Janela Interação de exemplo
fmc.api.threatGrid.ca	IPv4: 200.194.240.35 IPv6: 2602:811:900d:6::6e	443	FMC/FTD Serviço de análise de ficheiros

Nuvem da Austrália (AU)

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

Hostname	IP	Porta	Detalhes
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	Para Secure Malware Analytics Portal e dispositivos integrados (ESA/WSA/FTD/ODNS/Meraki)
glovebox.syd.threatgrid.com.au	IPv4: 200.194.246.35 200.194.247.35 IPv6: 2602:811:900e:6::6e 2602:811:9003:6::6e	443	Janela Interação de exemplo
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	FMC/FTD Serviço de análise de ficheiros

Nuvem da Índia (IN)

URL de acesso: <https://panacea.threatgrid.in>

Hostname	IP	Porta	Detalhes
panacea.threatgrid.in	IPv4:	443	Para Secure Malware Analytics Portal e

	200.194.244.35 IPv6: 2602:811:9001:6::6e		dispositivos integrados (ESA/WSA/FTD/ODNS/Meraki)
glovebox.bom.threat.grid.in	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6::6e	443	Janela Interação de exemplo
fmc.api.threatgrid.com.in	IPv4: 200.194.244.35 IPv6: 2602:811:9001:6::6e	443	FMC/FTD Serviço de análise de ficheiros

Para obter mais requisitos do Cisco Secure Malware Analytics, como dispositivos, consulte este artigo:

Conteúdo relacionado

Para obter os requisitos mais recentes, consulte .

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.