Endereços de servidor necessários para operações de análise de malware adequadas do Cisco Secure Endpoint &

Contents

Introdução

Este documento descreve os servidores necessários para permitir que o produto Cisco Secure Endpoint (antigo Cisco AMP) e o produto Cisco Secure Malware Analytics (antigo Threat Grid) se comuniquem e completem atualizações, pesquisas e relatórios. Para concluir as operações com êxito, o firewall deve permitir a conectividade do conector/dispositivo com os servidores necessários.

⚠ Cuidado: todos os servidores usam um esquema de endereço IP de rodízio para balanceamento de carga, tolerância a falhas e tempo de atividade. Portanto, os endereços IP podem mudar e a Cisco recomenda que o firewall seja configurado com CNAME em vez de um endereço IP.

⚠ Cuidado: todo o tráfego que chega em direção aos servidores Cisco não pode estar sujeito à descriptografia TLS.

Pré-requisitos

Requisitos

Este artigo da Tech Zone aplica-se aos seguintes produtos da Cisco integrados ao produto Cisco Secure Endpoint (AMP) e à análise de malware (Threat Grid):

- Endpoints seguros da Cisco para redes (Firepower Management Center e sensores)
- Nuvem privada do Cisco Secure Endpoint
- Nuvem pública do Cisco Secure Endpoint
- Cisco Secure Email Appliance e Cisco Email Security (ESA e CES)
- Cisco Secure Web Appliance (WSA)
- Nuvem e/ou dispositivo do Cisco Secure Malware Analytics (Threat Grid)
- SDWAN/IOS-XE

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Endereços de servidor necessários para as operações adequadas do Cisco Secure Endpoint

Locais do servidor

Os servidores Cisco Secure Endpoint e Cisco Secure Malware Analytics estão localizados em três locais diferentes:

- América do Norte (Cisco Secure Endpoint e Cisco Secure Malware Analytics)
- Europa (Cisco Secure Endpoint e Cisco Secure Malware Analytics)
- Japão (somente Cisco Secure Endpoint)

América do Norte

Esta tabela lista os locais de servidor para a América do Norte. Com base na data de criação da conta, os endereços do servidor podem ser diferentes:

Categoria	Propósito	Servidor	Porta
Endpoint seguro da Cisco: nuvem pública	Servidor de disposição	cloud-ec-asn.amp.cisco.com cloud-ec-est.amp.cisco.com	TCP 443

		enrolment.amp.cisco.com	
	Console	console.amp.cisco.com	TCP 443
	Servidor de gerenciamento	mgmt.amp.cisco.com	TCP 443
	Servidor de eventos	intake.amp.cisco.com	TCP 443
	Políticas	policy.amp.cisco.com	TCP 443
	Downloads e atualizações do Connector	upgrades.amp.cisco.com	TCP 80 e 443
	Relatório de Erros	crash.amp.cisco.com	TCP 443
	IOCs de endpoint	ioc.amp.cisco.com	TCP 443
	Servidor de atualização TETRA	tetra-defs.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80 e 443
	Definições de Clam para macOS e Linux	clam-defs.amp.cisco.com	TCP 80 e 443
	Detecções personalizadas avançadas	custom-signatures.amp.cisco.com	TCP 443
	Busca Remota de Arquivo	rff.amp.cisco.com submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net	TCP 443
	Proteção de comportamento	apde.amp.cisco.com	TCP 443
	Controle de dispositivo	endpoints.amp.cisco.com	TCP 443
Conector Android	Servidor de disposição	cloud-android-asn.amp.cisco.com	TCP 443
Conector CSC/iOS	Servidor de disposição	cloud-ios-asn.amp.cisco.com cloud-ios-est.amp.cisco.com	TCP 443
Ponto de extremidade seguro da Cisco: nuvem	Servidor de descarte de upstream <v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443

privada	Servidor de descarte de upstream >v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Servidor Yum	packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443
	Sessão de suporte	support-sessions.amp.cisco.com	TCP 22
AMP para redes: Firepower	Servidor de disposição (do FMC)	6.0 - 6.2.x: cloud-sa.amp.sourcefire.com 6.3.x +: cloud-sa.amp.cisco.com	TCP 443
	Eventos (do FMC)	5.x - 6.2.x: export.amp.sourcefire.com 6.3.x +: export.amp.cisco.com	TCP 443
	API (do FMC)	5.x - 6.2.x: api.amp.sourcefire.com 6.3.x + : api.amp.cisco.com E api.amp.sourcefire.com	TCP 443
	Análise dinâmica (a partir do sensor)	5.x: intel.api.sourcefire.com 6.x: panacea.threatgrid.com E fmc.api.threatgrid.com *Dependendo da versão do patch 6.x, o URL pode ser usado	TCP 443
ESA/WSA/SMA	Reputação do arquivo (ESA/WSA)	>= 15.x: cloud-esa-asn.amp.cisco.com cloud-esa-est.amp.cisco.com < 15.x: cloud-sa.amp.cisco.com	TCP 443
	Análise de arquivo (ESA/WSA/SMA)	panacea.threatgrid.com	TCP 443
	API (ESA)	>= 15.x: api.amp.cisco.com < 15.x: N/D	TCP 443
	Servidor de eventos (ESA)	>= 15.x: intake.amp.cisco.com	TCP 443

		< 15.x: N/D	
	Servidor de gerenciamento (ESA)	>= 15.x: mgmt.amp.cisco.com < 15.x: N/D	TCP 443
Meraki	Servidor de disposição	cloud-meraki-asn.amp.cisco.com cloud-meraki-est.amp.cisco.com	TCP 443
SDWAN	Servidor de disposição	cloud-isr-asn.amp.cisco.com cloud-isr-est.amp.cisco.com	TCP 443

Europa

Esta tabela lista os locais de servidor para a Europa. Com base na data de criação da conta, os endereços do servidor podem ser diferentes:

Categoria	Propósito	Servidor	Porta
Endpoint seguro da Cisco: nuvem pública	Servidor de disposição	cloud-ec-asn.eu.amp.cisco.com cloud-ec-est.eu.amp.cisco.com enrolment.eu.amp.cisco.com	TCP 443
	Console	console.eu.amp.cisco.com	TCP 443
	Servidor de gerenciamento	mgmt.eu.amp.cisco.com	TCP 443
	Servidor de eventos	intake.eu.amp.cisco.com	TCP 443
	Políticas	policy.eu.amp.cisco.com	TCP 443
	Downloads e atualizações do Connector	upgrades.eu.amp.cisco.com	TCP 80 e 443
	Relatório de Erros	crash.eu.amp.cisco.com	TCP 443
	IOCs de endpoint	ioc.eu.amp.cisco.com	TCP 443
	Servidor de atualização TETRA	tetra-defs.eu.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80 e 443
	Definições de Clam para macOS e Linux	clam-defs.eu.amp.cisco.com	TCP 80 e 443

	Detecções personalizadas avançadas	custom-signatures.eu.amp.cisco.com	TCP 443
	Busca Remota de Arquivo	rff.eu.amp.cisco.com submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net	TCP 443
	Proteção de comportamento	apde.eu.amp.cisco.com	TCP 443
	Controle de dispositivo	endpoints.eu.amp.cisco.com	TCP 443
Conector Android	Servidor de disposição	cloud-android-asn.eu.amp.cisco.com	TCP 443
Conector CSC/iOS	Servidor de disposição	cloud-ios-asn.eu.amp.cisco.com cloud-ios-est.eu.amp.cisco.com	TCP 443
Ponto de extremidade seguro da Cisco: nuvem privada	Servidor de descarte de upstream <v2.4	cloud-pc-est.eu.amp.cisco.com cloud-pc-asn.eu.amp.cisco.com	TCP 443
	Upstream Servidor de descarte >v2.4	cloud-pc-est.eu.amp.cisco.com cloud-pc-asn.eu.amp.cisco.com	TCP 443
	Servidor Yum	packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443
	Sessão de suporte	support-sessions.amp.cisco.com	TCP 22
AMP para redes: Firepower	Servidor de disposição (do FMC)	6.0 - 6.2.x: cloud-sa.eu.amp.sourcefire.com 6.3.x+: cloud-sa.eu.amp.cisco.com	TCP 443
	Eventos (do FMC)	5.x - 6.2.x: export.eu.amp.sourcefire.com 6.3.x+: export.eu.amp.cisco.com	TCP 443
	API (do FMC)	5.x - 6.2.x: api.amp.sourcefire.com E api.eu.amp.sourcefire.com 6.3.x+: api.amp.sourcefire.com E api.eu.amp.cisco.com	TCP 443

	Análise dinâmica (a partir do sensor)	5.x: intel.api.sourcefire.com 6.x: panacea.threatgrid.eu E fmc.api.threatgrid.eu Dependendo da versão do patch 6.x, qualquer URL pode ser usado	TCP 443
ESA/WSA/SMA	Reputação do arquivo (ESA/WSA)	>= 15.x: cloud-esa-asn.eu.amp.cisco.com cloud-esa-est.eu.amp.cisco.com < 15.x: cloud-sa.eu.amp.cisco.com	TCP 443
	Análise de arquivo (ESA/WSA/SMA)	panacea.threatgrid.eu	TCP 443
	API (ESA)	>= 15.x: api.eu.amp.cisco.com < 15.x: N/D	TCP 443
	Servidor de eventos (ESA)	>= 15.x: intake.eu.amp.cisco.com < 15.x: N/D	TCP 443
	Servidor de gerenciamento (ESA)	>= 15.x: mgmt.eu.amp.cisco.com < 15.x: N/D	TCP 443
SDWAN	Servidor de disposição	cloud-isr-asn.eu.amp.cisco.com cloud-isr-est.eu.amp.cisco.com	TCP 443

Ásia-Pacífico, Japão, China

Esta tabela lista os locais de servidor para o Pacífico Asiático, Japão e China:

Categoria	Propósito	Servidor	Porta
Endpoint seguro da Cisco: nuvem pública	Servidor de disposição	cloud-ec-asn.apjc.amp.cisco.com cloud-ec-est.apjc.amp.cisco.com enrolment.apjc.amp.cisco.com	TCP 443
	Console	console.apjc.amp.cisco.com	TCP 443
	Servidor de gerenciamento	mgmt.apjc.amp.cisco.com	TCP 443
	Servidor de eventos	intake.apjc.amp.cisco.com	TCP 443

	Políticas	policy.apjc.amp.cisco.com	TCP 443
	Downloads e atualizações do Connector	upgrades.apjc.amp.cisco.com	TCP 80 e 443
	Relatório de Erros	crash.apjc.amp.cisco.com	TCP 443
	IOCs de endpoint	ioc.apjc.amp.cisco.com	TCP 443
	Servidor de atualização TETRA	tetra-defs.apjc.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80 e 443
	Definições de Clam para macOS e Linux	clam-defs.apjc.amp.cisco.com	TCP 80 e 443
	Detecções personalizadas avançadas	custom-signatures.apjc.amp.cisco.com	TCP 443
	Busca Remota de Arquivo	rff.apjc.amp.cisco.com submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net	TCP 443
	Proteção de comportamento	apde.apjc.amp.cisco.com	TCP 443
	Controle de dispositivo	endpoints.apjc.amp.cisco.com	TCP 443
Conector Android	Servidor de disposição	cloud-android-asn.apjc.amp.cisco.com	TCP 443
Conector CSC/iOS	Servidor de disposição	cloud-ios-asn.apjc.amp.cisco.com cloud-ios-est.apjc.amp.cisco.com	TCP 443
Ponto de extremidade seguro da Cisco:	Upstream Servidor de descarte < v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
Nuvem privada	Upstream Servidor de descarte > v2.4	cloud-pc-est.amp.cisco.com	TCP 443

		cloud-pc-asn.amp.cisco.com	
	Servidor Yum	packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443 TCP 443
	Sessão de suporte	support-sessions.amp.cisco.com	TCP 22
AMP para redes: Firepower	Servidor de disposição	6.0 - 6.2.x: cloud-sa.apjc.amp.sourcefire.com (IP estático) 6.3.x+: cloud-sa.apjc.amp.cisco.com	TCP 443
	Events	5.x - 6.2.x:export.apjc.amp.sourcefire.com 6.3.x+: export.apjc.amp.cisco.com	TCP 443
	API	5.2 - 6.2.x api.apjc.amp.sourcefire.com E api.amp.sourcefire.com 6.3.x+: api.amp.sourcefire.com E api.apjc.amp.cisco.com	TCP 443
	Análise dinâmica	No momento, não há data centers do Threat Grid na APJC, portanto, o Os nomes de host europeus ou norte-americanos devem ser usados.	TCP 443
ESA/WSA/SMA	Reputação do arquivo (ESA/WSA)	>= 15.x: cloud-esa-asn.apjc.amp.cisco.com cloud-esa-est.apjc.amp.cisco.com < 15.x: cloud-sa.apjc.amp.cisco.com	TCP 443
	Análise de arquivo (ESA/WSA/SMA)	No momento, não há data centers do Threat Grid na APJC, portanto, o Os nomes de host europeus ou norte-americanos devem ser usados.	TCP 443
	API (ESA)	>= 15.x: api.apjc.amp.cisco.com	TCP 443

		< 15.x: N/D	
	Servidor de eventos (ESA)	>= 15.x: intake.apjc.amp.cisco.com < 15.x: N/D	TCP 443
	Servidor de gerenciamento (ESA)	>= 15.x: mgmt.apjc.amp.cisco.com < 15.x: N/D	TCP 443
SDWAN	Servidor de disposição	cloud-isr-asn.apjc.amp.cisco.com cloud-isr-est.apjc.amp.cisco.com	TCP 443

Endereços de servidor necessários para o acesso apropriado à nuvem do Cisco Secure Malware Analytics

Para obter detalhes sobre Secure Malware Analytic Cloud and Appliance, consulte este artigo: IPs e portas necessários para Secure Malware Analytics

Endereços de servidor necessários para uso orbital adequado

IPs estáticos para Orbital 1.7+

Nuvem da América do Norte (NAM)

Hostname	IP	Porta
orbital.amp.cisco.com	54.71.115.87 54.68.234.245 54.200.174.54	443
ncp.orbital.amp.cisco.com	52.88.16.211 52.43.91.219 54.200.152.114	443
update.orbital.amp.cisco.com	54.71.197.112 54.188.114.190 54.188.131.5	443

IPs NAT para Armazenamento de Dados Remoto		
	34.223.219.240 35.160.108.105 52.11.13.222	Número de porta aleatório alto

Para obter mais informações, consulte o guia de ajuda orbital: https://orbital.amp.cisco.com/help/

Nuvem europeia (UE)

Hostname	**IP**	**Porta**
orbital.eu.amp.cisco.com	3.120.91.16 18.196.194.92 3.121.5.209	443
ncp.orbital.eu.amp.cisco.com	18.194.154.159 18.185.217.177 18.184.249.36	443
update.orbital.eu.amp.cisco.com	3.123.83.189 18.184.240.159 35.158.29.104	443
IPs NAT para Armazenamento de Dados Remoto		
	52.29.47.197 52.57.222.67 52.58.172.218	Número de porta aleatório alto

Para obter mais informações, consulte o guia de ajuda orbital: https://orbital.eu.amp.cisco.com/help/

Ásia-Pacífico, Japão, China (APJC) Nuvem

Hostname	**IP**	**Porta**

orbital.apjc.amp.cisco.com	3.114.186.175 52.198.6.9 18.177.242.101	443
ncp.orbital.apjc.amp.cisco.com	18.177.250.245 13.230.62.75 18.176.196.172	443
update.orbital.apjc.amp.cisco.com	54.248.22.154 18.178.184.79 54.95.125.218	443
IPs NAT para Armazenamento de Dados Remoto		
	52.194.143.206 52.69.138.67 54.95.9.136	Número de porta aleatório alto

Para obter mais informações, consulte o guia de ajuda orbital: https://orbital.apjc.amp.cisco.com/help/

Endereços IP estáticos

Se o seu firewall bloquear conexões TCP de saída na porta 443 (o que geralmente não é o caso), você deverá alterar as configurações do firewall antes de atualizar quaisquer diretivas. Se sua conta foi estabelecida após fevereiro de 2016, você já tem endereços IP estáticos gravados nas políticas padrão. Se sua conta foi estabelecida antes de fevereiro de 2016, você pode entrar em contato com o Cisco Technical Assistance Center (TAC) para solicitar uma migração das políticas para os endereços IP estáticos.

Observação: para garantir a continuidade das operações e garantir que as disposições de malware de arquivo detectado sejam as mesmas em ambos os Firepower Management Centers, os Centros de gerenciamento primário e secundário devem ter acesso aos servidores listados neste documento.

Observação: o Cisco Secure Endpoint Console não usa IPs estáticos e deve ser acessado através do DNS.

Endereços IP estáticos na América	Endereços IP estáticos na	Endereços IP estáticos na

do Norte	Europa	APJC
23.23.197.169 23.23.198.191 23.23.224.83 50.16.242.171 50.16.244.193 50.16.250.236 52.0.55.209 52.2.63.194 52.2.128.246 52.3.149.24 52.3.178.163 52.3.190.47 52.4.98.101 52.4.151.41 52.4.245.162 52.4.246.178 52.5.92.125 52.6.103.57 52.6.197.200 52.20.14.163 52.20.123.238 52.20.141.147 52.21.52.149 52.21.117.50 52.21.134.210 52.22.64.192 52.22.156.183 52.23.13.34 52.23.16.199 52.23.73.146 52.23.87.4 52.23.107.89 52.23.134.105 52.23.140.222 52.70.11.137 52.70.13.27 52.70.35.37 52.70.47.45 52.70.56.136 52.70.58.10 52.70.59.59 52.70.59.121 52.70.60.74	46.51.181.139 46.51.182.195 46.51.182.202 46.137.99.242 52.16.63.115 52.16.95.58 52.16.105.95 52.16.166.193 52.16.177.94 52.16.193.225 52.16.220.180 52.17.93.43 52.17.102.100 52.17.106.35 52.17.179.163 52.17.211.190 52.17.233.49 52.18.9.153 52.18.28.229 52.18.79.226 52.18.109.209 52.18.187.129 52.18.187.166 52.18.223.41 52.19.84.244 52.19.167.56 52.30.25.70 52.30.74.163 52.30.124.82 52.30.160.113 52.30.175.205 52.30.179.236 52.30.196.206 52.30.208.114 52.30.217.4 52.30.217.226 52.30.255.133 52.31.30.249 52.31.66.59 52.31.83.94 52.31.119.97 52.31.122.77 52.31.127.190 52.31.137.201 54.195.248.52	54.250.127.0 52.197.2.58 52.197.22.41 52.69.16.172 13.112.137.80 52.198.208.254 13.112.162.167 54.249.244.218 54.249.246.210 54.249.243.85 54.249.240.219 54.248.98.94 176.34.47.0 52.192.82.189 52.68.180.106 52.196.247.47 52.196.185.158 52.197.74.4 52.69.39.127 54.248.113.224 54.238.55.12 54.249.248.16 52.197.50.93 52.193.124.132 52.69.108.228 52.197.72.147 52.197.22.165 52.68.82.200 52.197.35.73 52.197.39.251 52.68.251.104 54.249.253.42 54.249.253.65 176.34.60.211 52.192.198.119 52.196.96.41 54.248.116.199 52.196.117.29 52.196.134.7 176.34.60.30 52.192.145.214 52.192.221.107 52.193.182.191 52.193.201.169 52.193.223.43

52.70.61.174
52.70.61.181
52.70.61.193
52.70.63.25
54.83.45.221
54.88.208.235

54.204.8.61
54.221.210.7
54.221.255.190
54.225.226.117
54.225.227.9
54.225.227.30
54.225.227.45
54.225.227.105
54.225.228.145
54.225.228.166
54.225.228.244
54.227.247.102
107.20.158.55
107.20.203.8
107.20.229.191
107.20.234.220
107.21.212.157
107.21.217.202
107.21.218.60
128.177.8.0/24
174.129.203.65

54.161.128.60
54.234.131.176
52.206.206.244
34.225.208.192
52.22.120.193
34.199.250.32
34.199.238.4
34.194.224.132
34.198.112.150
34.224.236.198
52.20.233.31

192.111.4.0/24

192.111.7.0/24

54.71.197.112

54.195.249.18
54.217.232.226
54.217.232.234
54.217.232.241
54.217.232.244
54.217.232.249
54.228.250.255
54.246.88.192
54.247.189.117

54.74.229.75

107.21.250.31

107.21.236.143

52.2.128.246

52.18.202.103

52.18.119.87

192.111.5.0/24

34.249.48.182

34.248.52.55

99.81.233.22

3.123.83.189

18.184.240.159

35.158.29.104

192.35.177.23
104.18.39.201
172.64.148.55

52.193.233.17
52.196.115.166
52.196.31.86
52.197.121.237
52.198.147.230
52.198.195.125
52.198.202.24
52.198.221.53
52.198.223.169
52.198.225.221
52.198.226.104
52.198.26.36
52.198.94.104
52.199.124.11
52.199.127.80
52.199.92.142
52.68.1.146
54.248.107.84
54.248.109.124
54.248.126.98
54.248.236.127
54.248.236.141
54.248.236.144
54.248.236.151
54.248.237.93
54.249.246.7
54.250.127.131

192.111.6.0/24

54.248.22.154

18.178.184.79

54.95.125.218

192.35.177.23
104.18.39.201
172.64.148.55

54.188.114.190 54.188.131.5 192.35.177.23 104.18.39.201 172.64.148.55		

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.