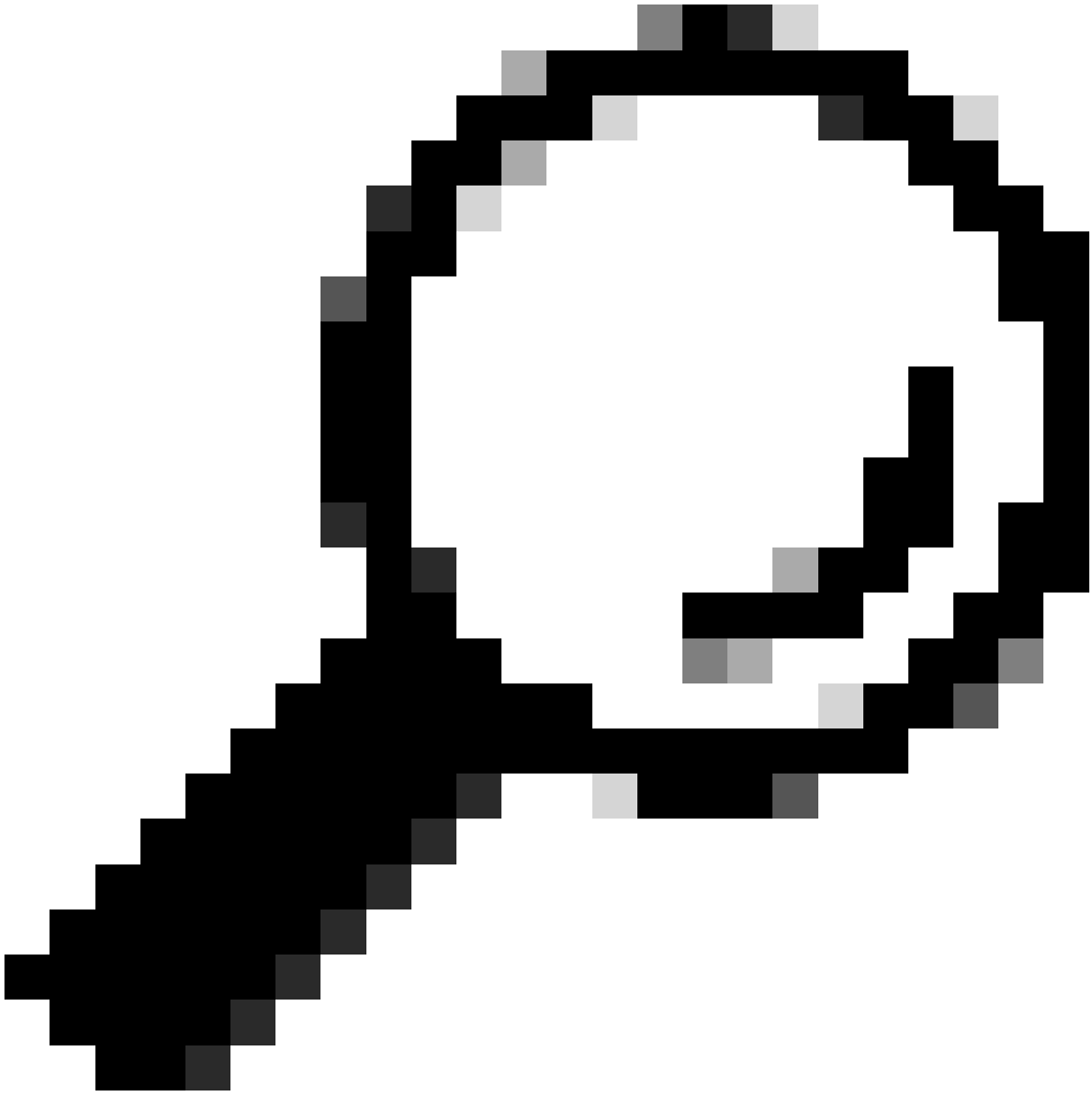
Secure Network Analytics Understanding External Connections Guide (Análise de rede segura entendendo as conexões externas)

Contents

Introdução

Use este guia para revisar as conexões externas necessárias para que determinados recursos do Secure Network Analytics funcionem rapidamente. Essas conexões externas podem ser domínios ou endpoints. Domínios são nomes usados para identificar recursos na Internet, geralmente sites ou serviços; e terminais são dispositivos ou nós reais que se comunicam através de uma rede. Como o foco deste guia são os serviços da Web, eles serão mostrados como URLs. A tabela lista os URLs de conexões externas em ordem alfabética.



Tip: A tabela lista os URLs de conexões externas em ordem alfabética.

Conexões externas

URL da Conexão Externa	Propósito
https://analytics.int.obsrvbl.com	Usado pelo Secure Network Analytics para troca de dados de telemetria com serviços Secure Cloud Analytics.

https://api.apj.sse.itd.cisco.com	Exigido pela Cisco para trânsito de dados para a Amazon Web Services (AWS) para a região Ásia-Pacífico, Japão e China (APJC). Usado para encaminhar alertas ao Cisco XDR e também para métricas de atendimento ao cliente.
https://api.eu.sse.itd.cisco.com	Exigido pela Cisco para trânsito de dados para a Amazon Web Services (AWS) para a região da Europa (EU). Usado para encaminhar alertas ao Cisco XDR e também para métricas de atendimento ao cliente.
https://api-sse.cisco.com	Exigido pela Cisco para trânsito de dados para a Amazon Web Services (AWS) para a região dos Estados Unidos (EUA). Usado para encaminhar alertas ao

	Cisco XDR e também para métricas de atendimento ao cliente/sucesso.
https://apix.cisco.com	Usado pelo Secure Network Analytics para o recurso Direct Software Downloads.
https://dex.sse.itd.cisco.com	Necessário para o envio e a coleta de métricas de sucesso do cliente
https://est.sco.cisco.com	Necessário para o envio e a coleta de métricas de sucesso do cliente
https://eventing-ingest.sse.itd.cisco.com	Necessário para o envio e a coleta de métricas de sucesso do cliente
https://feodotracker.abuse.ch/downloads/ipblocklist.txt	Exigido pelo Threat Feed, que é usado para alertas e observações do Secure Network Analytics, quando o Analytics está habilitado.
https://id.cisco.com	Usado pelo Secure Network Analytics para o recurso Direct Software Downloads.
https://intelligence.sourcefire.com/auto-update/auto-	Exigido pelo

dl.cgi/00:00:00:00:00:00/Download/files/ip-filter.gz	Threat Feed, que é usado para alertas e observações do Secure Network Analytics, quando o Analytics está habilitado.
https://intelligence.sourcefire.com/auto-update/auto-dl.cgi/00:00:00:00:00:00/Download/files/url-filter.gz	Exigido pelo Threat Feed, que é usado para alertas e observações do Secure Network Analytics, quando o Analytics está habilitado.
https://lancope.flexnetoperations.com/control/lncp/LancopeDownload	Exigido pelo Secure Network Analytics Threat Intelligence Feed, usado para alarmes e eventos de segurança do Secure Network Analytics. Isso exige a licença do feed de inteligência de ameaças do Secure Network Analytics.
https://mx*.sse.itd.cisco.com	Necessário para o envio e a coleta de métricas de sucesso do cliente
https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json	Permite acessar informações de MITRE para alertas quando

	o Analytics está habilitado.
https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobile-attack.json	Permite acessar informações de MITRE para alertas quando o Analytics está habilitado.
https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json	Permite acessar informações de MITRE para alertas quando o Analytics está habilitado.
https://s3.amazonaws.com/onconfig/global-blacklist	Feed de ameaças obrigatório, que é usado para alertas e observações do Secure Network Analytics quando o Analytics está habilitado.
https://sensor.anz-prod.obsrvbl.com	Exigido pela Cisco para trânsito de dados para a Amazon Web Services (AWS) para a região Ásia-Pacífico, Japão e China (APJC). Usado para encaminhar alertas ao Cisco XDR e também para métricas de atendimento ao cliente.
https://sensor.eu-prod.obsrvbl.com	Exigido pela Cisco para

	trânsito de dados para a Amazon Web Services (AWS) para a região da Europa (EU). Usado para encaminhar alertas ao Cisco XDR e também para métricas de atendimento ao cliente.
https://sensor.ext.obsrvbl.com	Exigido pela Cisco para trânsito de dados para a Amazon Web Services (AWS) para a região dos Estados Unidos (EUA). Usado para encaminhar alertas ao Cisco XDR e também para métricas de atendimento ao cliente.
smartreceiver.cisco.com	Usado para acessar o Cisco Smart Software Licensing. Consulte o Smart Licensing Guide para obter detalhes. O licenciamento off-line alternativo está disponível, se preferir.

	Consulte as Notas de versão para obter detalhes.
https://software.cisco.com	Usado pelo Secure Network Analytics para o recurso Direct Software Downloads.
https://www.cisco.com	Necessário para o domínio Cisco, que é usado para Smart Licensing, proxy de nuvem e testes de conexão de firewall.

Informações adicionais

Para avaliar melhor como e por que as conexões específicas de domínio e endpoint são usadas, consulte os seguintes tópicos:

- Cisco Secure Service Exchange (SSE)
- Downloads de Software Diretos (Beta)
- MITRE ATT&CK® Framework
- Feed de ameaças

Cisco Secure Service Exchange (SSE)

Os endpoints SSE são usados para o trânsito de dados para o Amazon Web Services (AWS), pela Cisco para métricas de atendimento ao cliente e também são usados ao encaminhar alertas para o Cisco XDR. Elas variam
com base em Região e Hosts. Esses pontos de extremidade são descobertos dinamicamente usando um mecanismo de Descoberta de Serviços fornecido pelo Conector SSE. Ao publicar detecções no Cisco XDR, o Secure Network Analytics tenta descobrir um serviço intitulado "xdr-data-platform" e seus "Eventos" de endpoint de API.

Região e hosts

Dependendo da região nos ambientes de produção, os hosts são os seguintes:

US:

- https://api-sse.cisco.com
- https://sensor.ext.obsrvbl.com

UE:

- https://api.eu.sse.itd.cisco.com
- https://sensor.eu-prod.obsrvbl.com

APJC:

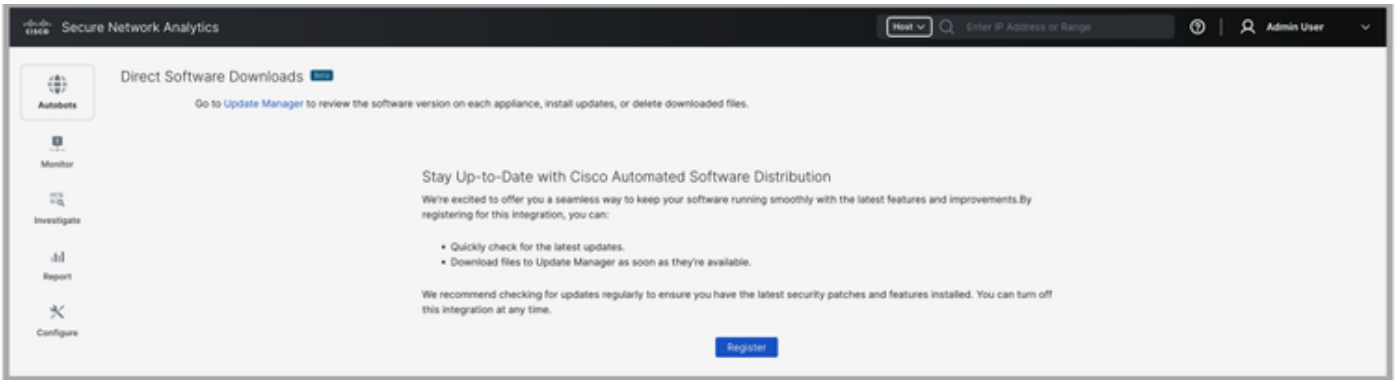
- https://api.apj.sse.itd.cisco.com
- https://sensor.anz-prod.obsrvbl.com

Downloads de Software Diretos (Beta)

As seguintes conexões são usadas pelo recurso Direct Software Downloads:

- https://apix.cisco.com
- https://software.cisco.com
- https://id.cisco.com

Para usar esse novo recurso para fazer download de software e corrigir arquivos de atualização diretamente para o Update Manager, certifique-se de que você se registrou usando sua ID de usuário cisco.com (CCOID).
1. Efetue login no Gerenciador.
2. No menu principal, escolha Configure > Global > Central Management.
3. Clique na guia Update Manager.
4. Clique no link Direct Software Downloads para abrir a página de registro.
5. Clique no botão Registrar para iniciar o processo de registro.



6. Clique no link fornecido.
7. Você será direcionado para a página Ativar seu dispositivo. Clique em Avançar para continuar.
8. Faça login com sua ID de usuário cisco.com (CCOID).

9. Você receberá uma mensagem "Device Ativated" (Dispositivo ativado) quando a ativação for concluída.
10. Volte para a página Direct Software Downloads no seu gerente e clique em Continue.
11. Clique nos links dos contratos EULA e K9 para ler e aceitar os termos. Quando os termos forem aceitos, clique em Continuar.

Para obter mais informações sobre os downloads diretos de software, entre em contato com o Suporte da Cisco

MITRE ATT&CK® Framework

O MITER ATT&CK® Framework é uma base de conhecimento publicamente disponível de táticas e técnicas de adversário baseadas em observações do mundo real. Quando você habilita a análise no Secure Network Analytics, as táticas e técnicas de MITER ajudam na inteligência, detecção e resposta a ameaças de segurança cibernética.

> To make sure Analytics is enabled, choose **Configure** > **Detection** > **Analytics** from the main menu, then click *Analytics On* Analytics On .

As conexões a seguir permitem que o Secure Network Analytics acesse informações do MITER Para as indicações:

- https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json
- https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobileattack.json
- https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterpriseattack.json

Feed de ameaças

O feed de ameaças do Cisco Secure Network Analytics (antigo feed de inteligência de ameaças do Stealthwatch) fornece dados do feed de ameaças global sobre ameaças à sua rede. O feed é atualizado com frequência e inclui endereços IP, números de porta, protocolos, nomes de host e URLs conhecidos por serem usados para atividades mal-intencionadas. Os seguintes grupos de hosts estão incluídos no feed: servidores de comando e controle, bogons e Tors.

Para ativar o Threat Feed no Gerenciamento central, siga as instruções na Ajuda.

1. Inicie a sessão no seu gerente principal.
2. Selecione Configure > Global > Central Management.
3. Clique no ícone (Ajuda). Selecione Help.
4. Selecione Configuração do dispositivo > Feed de ameaças.

> Please note that you will configure the DNS server and firewall as part of the instructions. Also, if you have a failover configuration, you need to enable Threat Feed on your primary Manager and secondary Manager.

Para obter mais informações sobre o Threat Feed, consulte o Guia de configuração do sistema.

Entrando em contato com o suporte

Se precisar de suporte técnico, siga um destes procedimentos:

- Entre em contato com seu parceiro Cisco local
- Entre em contato com o suporte da Cisco
- Para abrir um caso pela Web: http://www.cisco.com/c/en/us/support/index.html
- Para suporte por telefone: 1-800-553-2447 (EUA)
- Para números de suporte em todo o mundo: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

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.