安全网络分析外部连接指南

目录

简介

外部连接

Additional Information

- 思科安全服务交换(SSE)
  - 区域和主机
- 直接软件下载（试用版）
- MITER ATT&CK®框架
- 威胁源

联系支持人员

简介

使用此指南查看某些安全网络分析功能快速运行所需的外部连接。这些外部连接可以是域或终端。域是用来标识Internet资源（通常是网站或服务）的名称；和终端是指通过网络进行通信的实际设备或节点。由于本指南的重点是Web服务，因此这些服务显示为URL。下表按字母顺序列出外部连接URL。

外部连接

外部连接Url	目的
https://analytics.int.obsrvbl.com	安全网络分析使用安全云分析服务进行遥测数据交换。
https://api.apj.sse.itd.cisco.com	在亚太地区、日本和中国(APJC)地区，思科需要将数据传输到Amazon Web Services(AWS)。在将警报转发到Cisco XDR时使用，也用于客户服务指标。
https://api.eu.ss e.itd.cisco.com	在欧洲(EU)地区中传输到Amazon Web Services(AWS)的数据时需要思科的许可。在将警报转发到Cisco XDR时使用，也用于客户服务指标。

外部连接Url	目的
https://api-sse.cisco.com	思科为美国(US)地区的数据传输至Amazon Web Services(AWS)而要求。在将警报转发到Cisco XDR时使用，也用于客户服务/成功指标。
https://apix.cisco.com	由Secure Network Analytics用于直接软件下载功能。
https://dex.sse.itd.cisco.com	发送和收集客户成功指标所需
https://est.sco.cisco.com	发送和收集客户成功指标所需
https://eventing-ingest.sse.itd.cisco.com	发送和收集客户成功指标所需
https://feodotracker.abuse.ch/downloads/ipblocklist.txt	Threat Feed是必需的，当启用Analytics时，Threat Feed用于安全网络分析警报和观察。
https://id.cisco.com	由Secure Network Analytics用于直接软件下载功能。
https://intelligence.sourcefire.com/auto-update/auto-dl.cgi/00:00:00:00:00:00/Download/files/ip-filter.gz	Threat Feed是必需的，当启用Analytics时，Threat Feed用于安全网络分析警报和观察。
https://intelligence.sourcefire.com/auto-update/auto-dl.cgi/00:00:00:00:00:00/Download/files/url-filter.gz	Threat Feed是必需的，当启用Analytics时，Threat Feed用于安全网络分析警报和观察。
https://lancope.flexnetoperations.com/control/lncp/LancopeDownload	安全网络分析威胁情报源（用于安全网络分析警报和安全事件）需要。这需要Secure Network Analytics威胁情报源许可证。
https://mx*.sse.itd.cisco.com	发送和收集客户成功指标所需
https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json	启用分析功能后，允许访问警报的MITER信息。
https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobile-attack.json	启用分析功能后，允许访问警报的MITER信息。
https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json	启用Analytics时，允许访问警报的MITER信息。

外部连接Url	目的
https://brlcbwaicj.execute-api.us-east-1.amazonaws.com/test/get-doh-intel	当启用Analytics时，所需的威胁源用于安全网络分析警报和观察。
https://s3.amazonaws.com/onconfig/global-blacklist	当启用Analytics时，所需的威胁源用于安全网络分析警报和观察。
https://sensor.anz-prod.obsrvbl.com	在亚太地区、日本和中国(APJC)地区，思科需要将数据传输到Amazon Web Services(AWS)。在将警报转发到Cisco XDR时使用，也用于客户服务指标。
https://sensor.eu-prod.obsrvbl.com	在欧洲(EU)地区中传输到Amazon Web Services(AWS)的数据时需要思科的许可。在将警报转发到Cisco XDR时使用，也用于客户服务指标。
https://sensor.ext.obsrvbl.com	思科为美国(US)地区的数据传输至Amazon Web Services(AWS)而要求。在将警报转发到Cisco XDR时使用，也用于客户服务指标。
https://smartreceiver.cisco.com	用于访问思科智能软件许可。有关详细信息，请参阅智能许可指南。如有需要，可使用替代离线许可。有关详细信息，请参阅版本说明。
https://software.cisco.com	由Secure Network Analytics用于直接软件下载功能。
https://softwarecloud.cisco.com	由Secure Network Analytics用于直接软件下载功能。
https://www. 思科.com	思科域必需，用于智能许可、云代理和防火墙连接测试。

Additional Information

要进一步评估使用特定域和终端连接的方式和原因，请参阅：

- 思科安全服务交换(SSE)
- 直接软件下载（试用版）
- MITER ATT&CK®框架
- 威胁源

思科安全服务交换(SSE)

SSE终端用于数据传输到Amazon Web Services(AWS)，由思科用于您的服务指标，以及将警报转发到Cisco XDR时。它们因地区和主机而异。使用SSE连接器提供的服务发现机制动态发现终端。将检测发布到Cisco XDR时，安全网络分析尝试发现名为“xdr-data-platform”的服务及其API终端“Events”。

区域和主机

根据生产环境中的区域，以下是主机：

美国

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

欧盟

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

亚太地区

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

直接软件下载（试用版）

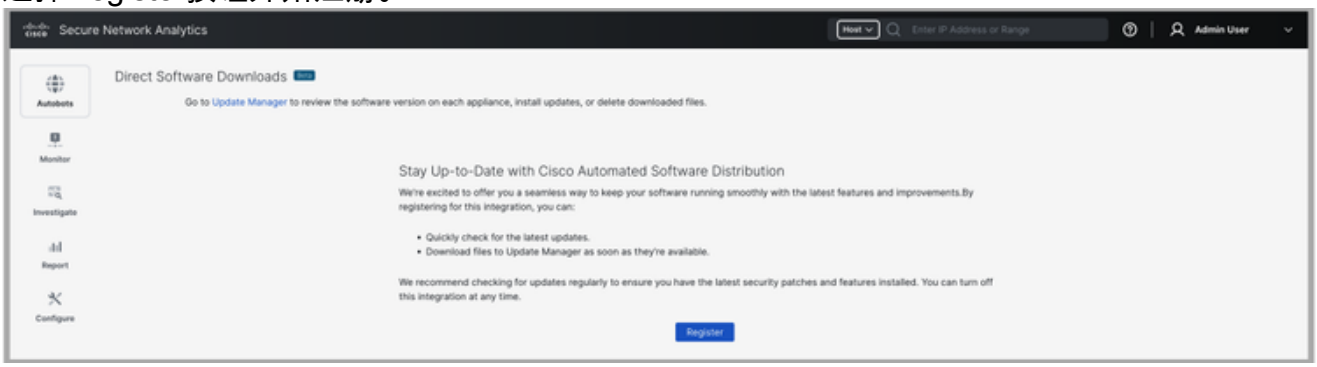
直接软件下载功能使用以下连接：

- https://apix.cisco.com

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

要使用此新功能将软件和补丁更新文件直接下载到您的更新管理器，请确保您已使用cisco.com用户ID(CCOID)注册。

1. 登录到Manager。
2. 从主菜单中选择Configure > Global > Central Management。
3. 选择Update Manager选项卡。
4. 选择Direct Software Downloads链接以打开注册页面。
5. 选择Register按钮开始注册。



6. 单击提供的链接。
7. 在Activate Your Device页面，选择Next。
8. 使用您的cisco.com用户ID(CCOID)登录。
9. 激活完成后，将显示“Device Activated”（设备激活）消息。
10. 返回Manager上的Direct Software Downloads页面，然后选择Continue。
11. 选择EULA和K9协议的链接以阅读并接受条款。接受条款后，选择Continue。

有关直接软件下载的详细信息，请联系思科支持。

MITER ATT&CK®框架

MITER ATT&CK®框架是一个基于真实世界观测的公开可用的敌方战术和技术的知识库。当您在安全网络分析中启用分析后，MITRE策略和技术可协助进行网络安全威胁情报、检测和响应。

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

以下连接允许Secure Network Analytics访问警报的MITER信息：

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

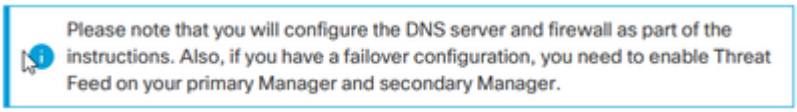
- https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json

威胁源

Cisco Secure Network Analytics Threat Feed（以前称为Stealthwatch Threat Intelligence Feed）提供来自全球威胁源的有关网络威胁的数据。源经常更新，包括IP地址、端口号、协议、主机名以及已知用于恶意活动的URL。源中包含以下主机组：命令和控制服务器、Bogons和Tors。

要在集中管理中启用威胁源，请按照“帮助”中的说明操作。

1.登录到您的主Manager。
2.选择Configure > Global > Central Management。
3.选择（帮助）图标，然后选择帮助。
4.选择Appliance Configuration > Threat Feed。



有关威胁源的详细信息，请参阅系统配置指南。

联系支持人员

对于技术支持：

- 联系您当地的思科合作伙伴
- 联系思科支持
- 在思科支持部门提交案例
- 致电1-800-553-2447（美国）
- 通过思科全球支持联系人查找全球支持编号

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。