Cisco Secure Network Analytics

Global Threat Alerts Configuration Guide 7.4.2

Table of Contents

Introduction

Cisco global threat alerts (formerly Cognitive Intelligence) quickly detects suspicious web traffic and/or Cisco Secure Network Analytics (formerly Stealthwatch) flow records and responds to attempts to establish a presence in your environment and to attacks that are already under way. Secure Network Analytics sends flow records to the global threat alerts cloud for analysis once it is enabled in Secure Network Analytics. By default, global threat alerts processes Secure Network Analytics flow records for inside/outside host group traffic and DNS requests. You can specify additional host groups to monitor inside traffic. Global threat alerts also detects malicious patterns in encrypted traffic using Cisco encrypted traffic analytics.

Global threat alerts works with Secure Network Analytics to analyze flow records and Network Address Translations (NAT). While no additional licenses are required to send Secure Network Analytics flow records to global threat alerts, internet boundary NAT data is required to send web traffic data from Secure Network Analytics to global threat alerts. Refer to **Related Resources** at the end of this document for links to more information about these products.

- Global threat alerts has migrated to Amazon Web Services (AWS) Cloud, which results in new URLs and IP addresses. Refer to the following field notices for more information:
  Field Notice - May 2018
  Field Notice - October 2018

Support

> Global threat alerts is not supported when Smart Licensing Reservation is used.

- The Manager (formerly Stealthwatch Management Console) and Flow Collector can be configured to connect to the Internet via a proxy server. Refer to **Proxy Configuration** for more information.
- Global threat alerts analyzes each domain as long as the associated Flow Collector for that domain has been enabled. The list of generated alerts is an aggregate of data obtained from all domains; it is not split by domain.
- If a particular client IP address exists in more than one domain, global threat alerts identifies all the alerts for this IP address across all applicable domains and places these alerts into the same group in the results. You can, however, filter results by host group on the global threat alerts dashboard (from the main menu, choose

Monitor INTEGRATIONS > Global Threat Alerts), since host group data is collected separately for each Flow Collector.

- Global threat alerts is not supported on the Flow Collector (sFlow).
- Global threat alerts is not available when FIPS Encryption Libraries is enabled.

Encrypted Traffic Analytics Support

Global threat alerts can only detect encrypted traffic analytics information if you have an encrypted traffic analytics enabled switch and router. For more information about Secure Network Analytics and encrypted traffic analytics, refer to the Encrypted Traffic Analytics white paper and the Encrypted Traffic Analytics deployment guides.

Users and Data Roles

This user...	With this data role...	Allows access to...
Primary Admin	All Data (Read & Write)	• Global threat alerts dashboard • Global threat alerts Components
Power Analyst		
Configuration Manager	All Data (Read only) *	• Global threat alerts dashboard
Analyst		

* You can change the data role for Configuration Manager and Analyst to provide full access to global threat alerts. For more information, go to the *User Management Configuration* help topics.

Data

Two categories of data are sent to the AWS data center in Dublin:

- Secure Network Analytics flow records, if any of the following conditions are met:
  - Records for inside/outside host group traffic
  - Records for specific internal host group traffic (**See "Inside Hosts"**)
  - Records for DNS requests, if the server port is 53
  - Records for encrypted traffic analytics, if you have an encrypted traffic analytics enabled switch and router
- Web log data, if you have Secure Network Analytics Proxy Log

Secure Network Analytics Flow Records

Secure Network Analytics flow records include:

- IP address of host endpoint
- TCP or UDP port
- mac address
- protocol data*
- number of bytes and packets sourced per period
- FIN packet count
- flow identifier
- service ID
- Palo Alto application ID
- username
- MPLS label
- round trip time
- start time
- port range
- group IDs
- SYN packet count
- TrustSec security group tag id and name
- well-known service port
- application ID
- Flow Sensor application ID
- VLAN ID
- retransmit count
- list of exporters
- Flow Collector IP Address
- last active time
- autonomous system number
- VM ID
- RST packet count
- number of total bytes and packets since flow started
- protocol
- packet shaper application ID
- NBAR application ID
- connection count
- server response time
- flow sequence number
- SVRD metric

* The protocol data field contains miscellaneous data, such as URLS, SSL certificates, and special characters for header data.

Encrypted Traffic Analytics Flow Records

encrypted traffic analytics flow records are only sent if you have an encrypted traffic analytics enabled switch and router. For more information about Secure Network Analytics and encrypted traffic analytics, refer to the Encrypted Traffic Analytics white paper and the Encrypted Traffic Analytics deployment guides.

The encrypted traffic analytics flow records include:

- initial data packet (IDP) *
- TLS session ID
- sequence of packet lengths and times (SPLT)
- selected cipher suite
- transport layer security (TLS) version

* The Initial Data Packet (IDP) contains mostly protocol related data and headers, such as Server Name Indication (SNI), protocol versions, offered and selected cypher suite and HTTP header fields (in case of unencrypted HTTP traffic). For protocols other than HTTPS/HTTP, it contains the protocol headers for the first 1500 bytes of the client/server communication (usually encrypted on the protocol level without the possibility of decryption without the rest of the data).

Web Log Data

One of the purposes of web log data is to provide a translation between an internal non-routable IP and external routable public IP via NAT.

> Refer to the Cisco Secure Network Analytics Proxy Log Configuration Guide for the proxy log configurations Secure Network Analytics supports.

The web log data includes:

- timestamp
- server IP address
- client TCP ports
- bytes transferred from Client to Server
- HTTP referrer header
- user-agent string
- elapsed time
- client username (optional)
- server TCP ports
- bytes transferred from server to client
- HTTP response status code
- response Mime Type or Content Type
- client IP address
- server name
- requested URL/URI
- HTTP request method
- HTTP location header
- action taken by the web security proxy

Configuring the Manager

Dashboard Component

To configure the global threat alerts component on the Manager, complete the following steps:

> All appliances must have a synchronized clock using an NTP server to connect to global threat alerts.

> On a pair of dual Managers, the secondary Manager will not connect to global threat alerts after configuration. This does not interfere with the Flow Collector receiving data and the primary Manager connects to global threat alerts and displays the widgets properly. If the primary Manager fails, the secondary Manager will connect to global threat alerts and display the widgets. When the original primary Manager comes up, both Managers will successfully connect to global threat alerts.

> At least one Manager needs internet access. If it also needs proxy configuration, refer to **Proxy Configuration** for more information.

1. Configure your network firewall to allow communication from the Manager to the following IP address and port 443:

Service	URL Alias	Service IPs
CTA public landing page	https://cta.eu.amp.cisco.com/ https://cognitive.cisco.com/ (alias)	AWS EIPs: *34.242.41.248 • 34.242.94.137 • 34.251.54.105
CTA login page	https://cta.eu.amp.cisco.com/ https://td.cloudsec.sco.cisco.com/CWSP/ (alias)	AWS EIPs: *34.242.41.248 • 34.242.94.137 • 34.251.54.105
CTA TAXII	https://cta.eu.amp.cisco.com/taxii	AWS EIPs:

Service	URL Alias	Service IPs
service	https://taxii.cloudsec.sco.cisco.com (alias)	*34.242.41.248 • 34.242.94.137 • 34.251.54.105

If public DNS is not allowed, you will need to configure the resolution locally on the Manager.

2. Log in to your Manager.
3. Select **Configure GLOBAL > Central Management**.
4. Click on the ••• (**Ellipsis**) icon under the Actions column for your Manager. Choose **Edit Appliance Configuration**.
5. Click the **General** tab.
6. Under External Services, check the **Enable Global Threat Alerts** check box to enable the global threat alerts component on the Security Insight dashboard and the Host Report.
7. (Optional) Check the **Automatic Updates** check box to enable global threat alerts to send updates automatically from the cloud.

   The automatic updates will mostly cover security fixes and small enhancements for the global threat alerts cloud. These updates will also be available through the normal Secure Network Analytics release process. You can disable this option any time to stop the automatic updates from the cloud. If you enable automatic updates on the Manager, you need to enable it on the Flow Collector(s).

8. Click **Apply Settings**.

   It will take a few minutes for the service to update and show the global threat alerts component on the Security Insight dashboard and the Host Report.

9. (Optional) To upload internet proxy, go to **Network Services**. Scroll down to the Internet Proxy section and check the **Enable** check box. Fill out the form, then click **Apply Settings**.

Inside Hosts

By default, global threat alerts processes Secure Network Analytics flow records for inside/outside host group traffic and DNS requests. By configuring an internal host group to send Secure Network Analytics flow records, the user adds additional data to be sent to the cloud for analysis. Adding specific host groups to global threat alerts monitoring is used for company internal servers (e.g. mail servers, file servers, web servers, authentication servers etc.) – adding traffic from the end users to those servers can improve the visibility of the exposure of data that can be potentially misused by malware running on the affected devices. Please don't check all the host groups for sending the data but only check the host groups representing internal servers.

To allow global threat alerts to monitor Inside Host traffic, complete the following steps:

1. Log in to your Manager.
2. Go to **Configure DETECTION > Host Group Management**.
3. Click on the applicable Inside Host Group and check the **Send Flow to Global Threat Alerts** check box.

> This feature enables monitoring traffic for all host groups under the selected parent host group. We recommend only enabling this option on child host groups to avoid potential performance issues.

4. Click **Save**.

Configuring the Flow Collector

To configure the global threat alerts component on the Flow Collector (NetFlow), complete the following steps:

> All appliances must have a synchronized clock using a NTP server to connect to global threat alerts.

> You will need to configure global threat alerts on each Flow Collector to get accurate results.

> After configuration, allow two days for the global threat alerts engine to learn how your network behaves.

1. Configure your network firewall to allow communication from the Flow Collector(s) to the following IP address and port 443:

Service	URL Alias	Service IPs
CTA public landing page	https://cta.eu.amp.cisco.com/ https://cognitive.cisco.com/ (alias)	AWS EIPs: *34.242.41.248 • 34.242.94.137 • 34.251.54.105
CTA login page	https://cta.eu.amp.cisco.com/ https://td.cloudsec.sco.cisco.com/CWSP/ (alias)	AWS EIPs: *34.242.41.248 • 34.242.94.137 • 34.251.54.105
CTA TAXII service	https://cta.eu.amp.cisco.com/taxii https://taxii.cloudsec.sco.cisco.com (alias)	AWS EIPs: *34.242.41.248 • 34.242.94.137 • 34.251.54.105
CTA data	https://etr.cta.eu.amp.cisco.com https://etr.cloudsec.sco.cisco.com (alias)	AWS EIPs: *34.251.210.21

Service	URL Alias	Service IPs
ingest service		• 34.255.162.33 • 54.194.49.205

If public DNS is not allowed, you will need to configure the resolution locally on the Flow Collector(s).

2. Log in to your Manager.
3. Select **Configure GLOBAL** > **Central Management**.
4. Click on the ••• (**Ellipsis**) icon under the Actions column for your Flow Collector (NetFlow). Choose **Edit Appliance Configuration**.
5. Click the **General** tab.
6. Under External Services, check the **Enable Global Threat Alerts** check box to enable sending data from your Flow Collector to the global threat alerts engine.
7. (Optional) Check the **Automatic Updates** check box to enable global threat alerts to send updates automatically from the cloud.

   The automatic updates will mostly cover security fixes and small enhancements for the global threat alerts cloud. These updates will also be available through the normal Secure Network Analytics release process. You can disable this option any time to stop the automatic updates from the cloud. If you enable automatic updates on the Flow Collectors, you need to enable it on the Manager.

8. Click **Apply Settings**.

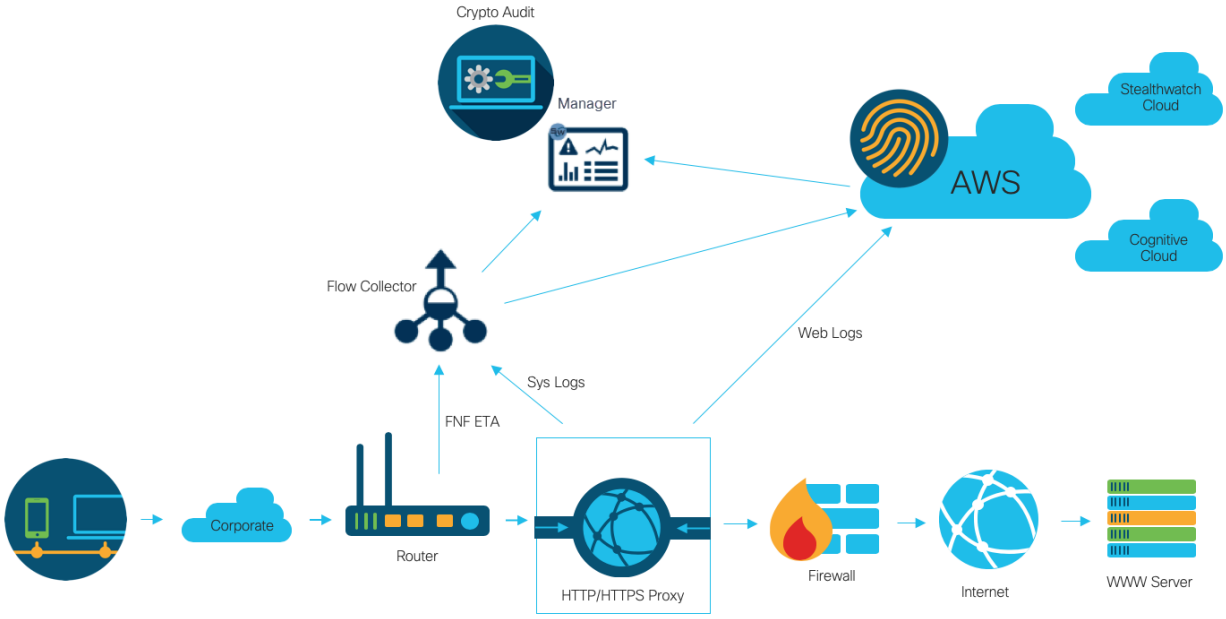
Proxy Configuration

To achieve this, configure the Manager and Flow Collector to connect to the Internet via a proxy server. Global threat alerts supports HTTP/HTTPS proxies with SSL inspection disabled. Secure Network Analytics does not support SOCKS proxy.

For more information on how to set up web proxy, refer to the **Configuring the Manager** section of this document. For more information about configuring proxy logs, refer to the Cisco Secure Network Analytics Proxy Log Configuration Guide.

Refer to the diagram below for setup configuration:

This configuration requires the proxy to be in transparent mode for WSA. Refer to Configure WSA to Upload Log Files to Global Threat Alerts System for more information.



You will get the best results from global threat alerts using a proxy when:

- A Flow Collector collects flows before the proxy
- Proxy logs are sent directly to the cloud

You will get the best results from Secure Network Analytics using a proxy when:

- Proxy logs are sent directly to the Flow Collector
- You enable encrypted traffic analytics

For more information on connecting the proxy directly to the cloud, refer to:

Configure Blue Coat ProxySG to Upload Log Files to Global Threat Alerts System

Configure McAfee Web Gateway to Upload Log Files to Global Threat Alerts System

Configure WSA to Upload Log Files to Global Threat Alerts System

Verification

Docker Services

To verify that global threat alerts is configured properly, complete the following steps:

> To disable global threat alerts, go to **Central Manager > Edit Appliance Configuration > General** and un-select the **Enable Global Threat Alerts** check box on each Manager and Flow Collector (NetFlow).

1. Check that global threat alerts is enabled on your Manager and Flow Collector(s).
2. Check that the global threat alerts component has appeared on the Security Insight dashboard and Host Report.
3. From the navigation menu, click **Monitor INTEGRATIONS > Global Threat Alerts**. The global threat alerts dashboard page will open. Click **Device Accounts** from the menu in the upper-right corner of the page. Check that the account for each configured Flow Collector is uploading data and has a ready status.

Encrypted Traffic Analytics Integration

Global threat alerts implements malware detection capability within the encrypted traffic analytics solution. To verify the encrypted traffic analytics solution is set up correctly, global threat alerts can generate encrypted traffic analytics test incidents using specific test site domains. To generate these test incidents, browse to one of the following test sites using a host where the HTTPS session is passing through an encrypted traffic analytics enabled switch and router:

- Malware: https://examplemalwaredomain.com
- Botnet: https://examplebotnetdomain.com
- Phishing: https://internetbadguys.com

> The detection may initially show up as a risk rating of 5. The risk rating can increase with additional bad or repetitive behavior, such as going to multiple of the above URLs or repeatedly visiting the same URL.

- TOR detection: Download and install the TOR browser: https://www.torproject.org/projects/torbrowser.html.en and visit a few websites.
- The TOR detection will display as "TOR relay" or "Possibly Unwanted Application" with a risk rating of 4.

Known Issues

This section summarizes issues (bugs) that are known to exist in this release. Where possible, workarounds are included. The defect number is provided for reference.

Defect Number	Description	Workaround
CHOPIN-25314	If a Secure Network Analytics user has their privileges lifted or demoted (ex. Read Only to Read/Write or vice versa), it will take up to 30 minutes to propagate the change to global threat alerts.	None currently available.
SWD-13834	After performing a configuration restore, global threat alerts is disabled.	To overcome this, manually enable global threat alerts after the backup restore process.
NA	If a user logs in to multiple Secure Network Analytics systems, they can't log in to the second system within global threat alerts.	To overcome this: • Wait 30 minutes for the first login to expire • Log out of global threat alerts on the first system

Related Resources

- For more information about global threat alerts, go to their website at https://cognitive.cisco.com or their product documentation at http://www.cisco.com/c/en/us/td/docs/security/web_security/scancenter/administrator/guide/b_ScanCenter_Administrator_Guide/b_ScanCenter_Administrator_Guide_chapter_011110.html
- For more information about Cloud Terms and Offer Descriptions for all Cisco cloud products: http://www.cisco.com/c/en/us/about/legal/cloud-and-software/cloud-terms.html
- For more information about the Cisco Universal Cloud Agreement: http://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/universal-cloud-agreement.pdf
- For more information about the omnibus offer description: http://www.cisco.com/c/dam/en_us/about/doing_business/legal/docs/omnibus-cloud-security.pdf
- For more information about Secure Network Analytics Proxy Log and web proxy: https://www.cisco.com/c/en/us/support/security/stealthwatch/products-installation-and-configuration-guides-list.html

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Copyright Information