Stealthwatch and Cognitive Threat Analytics Configuration Guide
(for Stealthwatch System v6.9.1)

Introduction
Cisco Cognitive Threat Analytics (CTA) quickly detects suspicious web traffic and/or NetFlow and responds to attempts to establish a presence in your environment and to attacks that are already under way. Stealthwatch sends NetFlow data to the CTA cloud for analysis once CTA is enabled on the Stealthwatch System. CTA provides better analysis and detection if you use both NetFlow and web traffic data. While no additional licenses are required to send NetFlow data to CTA, Stealthwatch ProxyWatch is required to send web traffic data from the Stealthwatch System to CTA. See “Related Resources” at the end of this document for links to more information about these products.

Note: The Stealthwatch Management Console and Flow Collector can be configured to connect to the Internet via a proxy server. The CTA system supports HTTP/HTTPS proxies with SSL inspection disabled. The Stealthwatch System does not support SOCKS proxy.

Data
Two categories of data are sent to the CTA Data Center in London over SCP and HTTPS: perimeter NetFlow and web logs. Web log data is only sent it you have Stealthwatch ProxyWatch.

The NetFlow data includes:
- 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 web log data includes:
- timestamp
- server IP address
- client TCP ports
- bytes transferred from Client to Server
- HTTP referer 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
Configure Stealthwatch Management Console

To configure the CTA component on the Stealthwatch Management Console, complete the following steps:

1. Configure your network firewall to allow communication from the Stealthwatch Management Console to the following IP address and port 443:
   a. cognitive.cisco.com - 108.171.128.81
      
      **Note:** If public DNS is not allowed, you will need to configure the resolution locally on the Stealthwatch Management Console.

2. Log in to Stealthwatch Management Console.

3. Go to Administer Appliance.

4. Click **Configuration > System Time and NTP**. Make sure the **Enable Network Time Protocol** check box is selected.

   **Note:** If the system does not have accurate NTP time, the appliance will not connect properly to CTA.

5. Click **Home**. Under Docker Services, click **Configure** for Cognitive Threat Analytics Dashboard Component.

6. Select the **Dashboard Component** check box to enable the CTA component on the Security Insight Dashboard and the Host Report.

7. (Optional) Select the **Automatic Updates** check box to enable CTA to send updates automatically from the cloud.

   **Note:** The automatic updates will mostly cover security fixes and small enhancements for the CTA cloud. These updates will also be available through the normal Stealthwatch release process. You can disable this option any time to stop the automatic updates from the cloud. If you enable automatic updates on the Stealthwatch Management Console, you need to enable it on the Flow Collector(s).

8. Click **Apply**.

   **Note:** It will take a minute for the Docker service to update and show the CTA component on the Security Insight Dashboard and the Host Report.

Configure Flow Collector

To configure the CTA component on the Flow Collector, complete the following steps:

**Note:** You will need to configure the CTA Data Uploader on each Flow Collector to get accurate results.

1. Configure your network firewall to allow communication from the Flow Collector(s) to the following IP addresses and port 443:
   a. etr.cloudsec.sco.cisco.com - 108.171.128.86
   b. cognitive.cisco.com - 108.171.128.81
      
      **Note:** If public DNS is not allowed, you will need to configure the resolution locally on the Flow Collector(s).

2. Log in to Flow Collector.

3. Click **Configuration > System Time and NTP**. Make sure the **Enable Network Time Protocol** check box is selected.

   **Note:** If the system does not have accurate NTP time, the appliance will not connect properly to CTA.

5. Select the Data Uploader check box to enable sending data from your Flow Collector to the CTA engine.

6. (Optional) Select the Automatic Updates check box to enable CTA to send updates automatically from the cloud.
   
   Note: The automatic updates will mostly cover security fixes and small enhancements for the CTA cloud. These updates will also be available through the normal Stealthwatch 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 Stealthwatch Management Console.

7. Click Apply.

Verification
To verify that the CTA Docker Services are configured properly, complete the following steps:

Note: To disable CTA, click Configure and un-select the check boxes. If you click Stop, the docker container stops but if the Flow Collector reboots, CTA will re-enable.

1. Check that Docker Services on the Stealthwatch Management Console and the Flow Collector(s) show Enabled.

2. Check that the CTA component has appeared on the Security Insight Dashboard and Host Report.

3. From the navigation menu, click Dashboard > Cognitive Threat Analytics. The CTA Dashboard page will open. Click Device Accounts from the menu in the upper-right corner of the page. Check if there are accounts for each Flow Collector configured and that they are uploading data.
   
   Note: After configuration, allow two days for the CTA engine to learn how your network behaves.

Related Resources

- For more information about CTA, go to their website at https://cognitive.cisco.com or their product documentation at
- For more information about Cloud Terms and Offer Descriptions for all Cisco cloud product:
- For more information about the Cisco Universal Cloud Agreement:
- For more information about the omnibus offer description:
- For more information about Stealthwatch ProxyWatch and web proxy, go to the Stealthwatch Customer Community at https://lancope.force.com/Customer, and click Product Documentation.

Note: You are asked to create an account on your first visit to the site.