Cisco Stealthwatch

Stealthwatch and Cognitive Intelligence Configuration Guide 7.3

Table of Contents

Introduction

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

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

> Cognitive Intelligence 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

Stealthwatch Support

- The 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.
- Cognitive Intelligence is only available for the default domain or site within Stealthwatch; multiple domains or sites is not supported.
- Cognitive Intelligence is not supported on the Flow Collector sFlow.
- Cognitive Intelligence is not available when FIPS Encryption Libraries is enabled.

ETA Support

Cognitive Intelligence can only detect ETA information if you have an ETA enabled switch and router. For more information about Stealthwatch and ETA, 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)	• Cognitive Dashboard • Cognitive Components
Power Analyst		
Configuration Manager	All Data (Read only) *	• Cognitive Dashboard
Analyst		

* You can change the data role for Configuration Manager and Analyst to provide full access to Cognitive. 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:

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

Stealthwatch Flow Records

The Stealthwatch 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.

ETA Flow Records

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

The ETA 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 Stealthwatch Proxy Log Configuration Guide for the proxy log configurations Stealthwatch 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 Stealthwatch Management Console

Dashboard Component

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

> All appliances must have a synchronized clock using a NTP server to connect to Cognitive Intelligence.

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

> At least one SMC 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 Stealthwatch Management Console to the following IP address and port 443:

AWS Elastic IPs	• 34.242.41.248 • 34.242.94.137 • 34.251.54.105
Cisco Streamline IPs	• 146.112.59.0/24 • 208.69.38.0/24

> 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. Click on the ⚙ (**Global Settings**) icon. Choose **Central Management**.

4. Click on the ••• (**Ellipsis**) icon under the Actions column for your SMC. Choose **Edit Appliance Configuration**.
5. Click the **General** tab.
6. Under External Services, check the **Enable Cognitive Intelligence** check box to enable the Cognitive Intelligence component on the Security Insight Dashboard and the Host Report.
7. (Optional) Check the **Automatic Updates** check box to enable Cognitive Intelligence to send updates automatically from the cloud.

   The automatic updates will mostly cover security fixes and small enhancements for the Cognitive Intelligence 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 Settings**.

   It will take a few minutes for the service to update and show the Cognitive Intelligence 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, Cognitive Intelligence processes Stealthwatch flow records for inside/outside host group traffic and DNS requests. By configuring an internal host group to send Stealthwatch flow records, the user adds additional data to be sent to the cloud for analysis. Adding specific host groups to Cognitive Intelligence 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 Cognitive Intelligence to monitor Inside Host traffic, complete the following steps:

1. Log in to the SMC.
2. Go to **Configure > Host Group Management**.

3. Click on the applicable Inside Host Group and check the **Send Flow to Cognitive Intelligence** 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 Cognitive Intelligence component on the Flow Collector NetFlow, complete the following steps:

> All appliances must have a synchronized clock using a NTP server to connect to Cognitive Intelligence.

> You will need to configure the Cognitive Intelligence on each Flow Collector to get accurate results.

> After configuration, allow two days for the Cognitive Intelligence 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:

AWS Elastic IPs	• 34.242.41.248 • 34.242.94.137 • 34.251.54.105	• 34.251.210.21 • 34.255.162.33 • 54.194.49.205
Cisco Streamline IPs	• 146.112.59.0/24 • 208.69.38.0/24	

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

2. Log in to Stealthwatch Management Console.
3. Click on the ⚙ (**Global Settings**) icon. Choose **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 Cognitive Intelligence** check box to enable sending data from your Flow Collector to the Cognitive engine.

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

   The automatic updates will mostly cover security fixes and small enhancements for the Cognitive Intelligence 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.

8. Click **Apply Settings**.

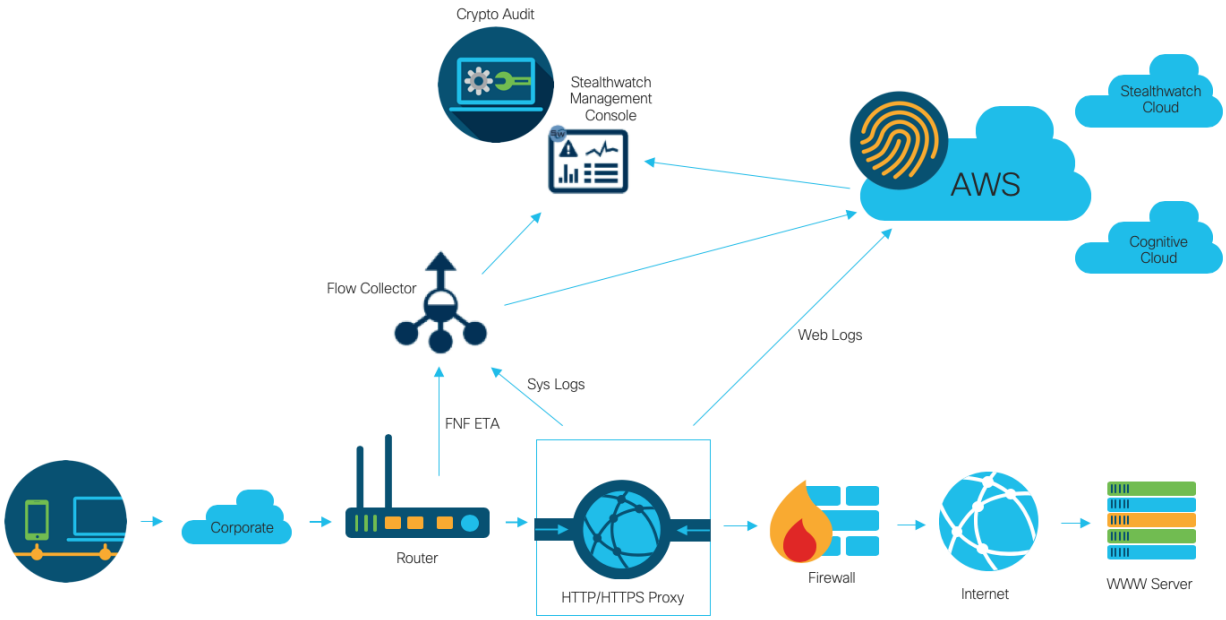
Proxy Configuration

To achieve this, configure the Stealthwatch Management Console and Flow Collector to connect to the Internet via a proxy server. Cognitive Intelligence supports HTTP/HTTPS proxies with SSL inspection disabled. Stealthwatch does not support SOCKS proxy.

For more information on how to set up web proxy, refer to the **Configuring the Stealthwatch Management Console** section of this document. For more information about configuring proxy logs, refer to the Stealthwatch 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 Cognitive System for more information.



You will get the best results from Cognitive 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 Stealthwatch Enterprise using a proxy when:

- Proxy logs are sent directly to the Flow Collector
- You enable ETA

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

Configure Blue Coat ProxySG to Upload Log Files to Cognitive System

Configure McAfee Web Gateway to Upload Log Files to Cognitive System

Configure WSA to Upload Log Files to Cognitive System

Verification

Docker Services

To verify that Cognitive Intelligence is configured properly, complete the following steps:

> To disable Cognitive Intelligence, go to **Central Manager > Edit Appliance Configuration > General** and un-select the **Enable Cognitive Intelligence** check box on each SMC and Flow Collector NetFlow.

1. Check that Cognitive Intelligence is enabled on your SMC and Flow Collector(s).
2. Check that the Cognitive Intelligence component has appeared on the Security Insight Dashboard and Host Report.
3. From the navigation menu, click **Dashboard > Cognitive Intelligence**. The Cognitive Intelligence 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.

ETA Integration

Cognitive Intelligence implements malware detection capability within the Encrypted Traffic Analytics (ETA) solution. To verify the ETA solution is set up correctly, Cognitive can generate ETA 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 ETA 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 Stealthwatch 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 the Cognitive Intelligence system.	None currently available.
SWD-13834	After performing a configuration restore, Cognitive Intelligence is disabled.	To overcome this, manually enable Cognitive after the backup restore process.
NA	If a user log ins to multiple Stealthwatch systems, they can't log in to the second system within Cognitive Intelligence.	To overcome this: • Wait 30 minutes for the first login to expire • Log out of Cognitive on the first system

Related Resources

- For more information about Cognitive Intelligence, 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 Stealthwatch 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 Stealthwatch 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: www.cisco.com/en/US/partner/support/tsd_cisco_worldwide_contacts.html

Copyright Information