Copyrights and Trademarks

© 2019 Cisco Systems, Inc. All rights reserved.

NOTICE

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>iii</td>
</tr>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Data</td>
<td>2</td>
</tr>
<tr>
<td>Stealthwatch Flow Records</td>
<td>2</td>
</tr>
<tr>
<td>Web Log Data</td>
<td>2</td>
</tr>
<tr>
<td>Configuring the Stealthwatch Management Console</td>
<td>4</td>
</tr>
<tr>
<td>Dashboard Component</td>
<td>4</td>
</tr>
<tr>
<td>Inside Hosts</td>
<td>5</td>
</tr>
<tr>
<td>Configuring the Flow Collector</td>
<td>6</td>
</tr>
<tr>
<td>Verification</td>
<td>7</td>
</tr>
<tr>
<td>Docker Services</td>
<td>7</td>
</tr>
<tr>
<td>ETA Integration</td>
<td>7</td>
</tr>
<tr>
<td>Related Resources</td>
<td>9</td>
</tr>
<tr>
<td>Contacting Support</td>
<td>9</td>
</tr>
</tbody>
</table>
Introduction

Cisco Cognitive Analytics 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 Analytics cloud for analysis once it is enabled on the Stealthwatch System. By default, Cognitive Analytics processes Stealthwatch flow records for inside/outside host group traffic and DNS requests. You can also specify additional host groups to monitor inside traffic.

Cognitive Analytics provides better analysis and detection if you use both Stealthwatch flow records and web traffic data. While no additional licenses are required to send Stealthwatch flow records to Cognitive Analytics, Stealthwatch Proxy Log is required to send web traffic data from the Stealthwatch System to Cognitive Analytics. See “Related Resources” at the end of this document for links to more information about these products.

Notes:
- Cognitive Analytics 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
- The Stealthwatch Management Console and Flow Collector can be configured to connect to the Internet via a proxy server. Cognitive Analytics 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 Configuring the Stealthwatch Management Console.
- Cognitive Analytics does not work with Stealthwatch trial licenses. For more information on Stealthwatch licenses, refer to Downloading and Licensing Stealthwatch Products.
- Cognitive Analytics is only available for the default domain or site within Stealthwatch; multiple domains or sites is not supported.
- Cognitive Analytics is not supported on the Flow Collector sFlow.
Data

Two categories of data are sent to the Cognitive Analytics data center in London over SCP and HTTPS and 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 (See "Inside Hosts")
  - Records for DNS requests if the server port is 53
- 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
- payload*
- 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

*If the advanced settings on the Flow Sensor are enabled, this field will contain the configured amount of application payload data. Alternatively, this field could contain a URL provided by a Cisco IOS device with NBAR enabled.

Web Log Data

The web log data includes:

- timestamp
- server IP address
- elapsed time
- client username (optional)
- client IP address
- server name
- client TCP ports
- bytes transferred from Client to Server
- HTTP referrer header
- user-agent string
- server TCP ports
- bytes transferred from server to client
- HTTP response status code
- response Mime Type or Content Type
- 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 Analytics 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:
   - 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

   **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**. Click the **Enable Network Time Protocol** check box to set up a NTP server.

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

5. Click **Home**. Under Docker Services, click **Configure** for Cognitive Threat Analytics Dashboard Component.
7. (Optional) Select the **Automatic Updates** check box to enable Cognitive Analytics to send updates automatically from the cloud.

   **Note:** The automatic updates will mostly cover security fixes and small enhancements for the Cognitive Analytics 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 few minutes for the Docker service to update and show the Cognitive Analytics component on the Security Insight Dashboard and the Host Report.

9. (Optional) To upload internet proxy, go to **Configuration > Services**. Scroll down to the Internet Proxy section and enter your proxy IP and Ports, then click **Apply**.

**Inside Hosts**

By default, Cognitive Analytics 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 Analytics 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 Analytics to monitor Inside Host traffic, complete the following steps:

1. Log in to the SMC client interface.
2. Right click on the applicable Inside Host Group and click **Configuration > Host Group Properties**.

**Note:** 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.

3. Select the **Send Flow to Cognitive Threat Analytics (CTA)** check box.
4. Click **OK**.
Configuring the Flow Collector

To configure the Cognitive Analytics component on the Flow Collector NetFlow, complete the following steps:

**Note:** You will need to configure the Cognitive Analytics Data Uploader on each Flow Collector NetFlow 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:
   - AWS Elastic IPs:
     - 34.242.41.248
     - 34.242.94.137
     - 34.251.54.105
   - 34.251.210.21
   - 34.255.162.33
   - 34.255.162.33
   - 34.251.54.105
   - 54.194.49.205
   - Cisco Streamline IPs:
     - 146.112.59.0/24
     - 208.69.38.0/24

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


3. Click **Configuration > System Time and NTP**. Click the **Enable Network Time Protocol** check box to set up a NTP server.

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

4. Click **Home**. Under Docker Services, click **Configure** for Cognitive Threat Analytics Data Uploader.

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

6. (Optional) Select the **Automatic Updates** check box to enable Cognitive Analytics to send updates automatically from the cloud.

   **Note:** The automatic updates will mostly cover security fixes and small enhancements for the Cognitive Analytics 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

Docker Services

To verify that the Cognitive Analytics Docker Services are configured properly, complete the following steps:

**Note:** To disable Cognitive Analytics, go to the docker container in Administer Appliance, click **Configure** and un-select the check boxes. If you click **Stop**, the docker container will stop sending data, but it will re-enable if the Flow Collector reboots.

1. Check that Docker Services on the Stealthwatch Management Console and the Flow Collector(s) show Enabled.
2. Check that the Cognitive Analytics component has appeared on the Security Insight Dashboard and Host Report.
3. From the navigation menu, click **Dashboard > Cognitive Threat Analytics**. The Cognitive Analytics 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.

**Note:** After configuration, allow two days for the Cognitive Analytics engine to learn how your network behaves.

ETA Integration

Cognitive Analytics implements malware detection capability within the Encrypted Traffic Analytics (ETA) solution. To verify the ETA solution is set up correctly, CTA 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](https://examplemalwaredomain.com)
- **Botnet:** [https://examplebotnetdomain.com](https://examplebotnetdomain.com)
- **Phishing:** [https://internetbadguys.com](https://internetbadguys.com)

**Note:** 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 from [https://www.torproject.org/projects/torbrowser.html.en](https://www.torproject.org/projects/torbrowser.html.en). Launch the browser and go to a few websites.

**Note:** The TOR detection will display as "TOR relay" or "Possibly Unwanted Application" with a risk rating of 4.
Related Resources

- For more information about Cognitive Analytics, 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

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 email: tac@cisco.com
  - For phone support: 1-800-553-2447 (U.S.)