Configuring the Secure Cloud Analytics Connector

Configuring Cisco Connector for Secure Cloud Analytics

Cisco Secure Cloud Analytics (formerly Stealthwatch Cloud) provides the actionable security intelligence and visibility necessary to identify these kinds of malicious activities in real time. You can quickly respond before a security incident becomes a devastating breach. This guide will walk you through setting up the Cisco Cloud Connector in IOS-XE, on a Cisco Industrial Ethernet Switch.

Note For further information about **Cisco Secure Cloud Analytics (Stealthwatch Cloud)** or **Cisco Secure Network Analytics (Stealthwatch)** go to the following URL: https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html.

Limitations and Restrictions

- Only a predetermined set of fields can be collected - These include 9-tuple flow data of Src IP, Src Port, Dst IP, Dst Port and Protocol along with Flow Start, Flow End, Number of Packets and Bytes
- The mandatory fields are not enforced through CLI restrictions. In case a record does not have all the mandatory fields and we are unable to collect 9-tuple data, we shall discard that flow.
- The StealthWatch Connector for Secure Cloud Analytics will rely on the Switch’s routing functionality to send the packet to the Cloud Servers. No additional checks are done. Assumption is that appropriate routes exist.
- Monitor application restrictions inherent with Flexible Net Flow in terms of monitor application holds true with Secure Cloud Analytics as well. e.g no SVI, no VLAN, no egress monitor.
- The cloud exporter can’t be used with other exporters.
- The uploaded file naming convention includes a random string to uniquely identify every file and to prevent file overwrites. Example:

https://sensor.ext.obsrvbl.com/sign/ios-xe-17-2/2019/7/5/00:00:00/hostname-random_suffix.csv.gz We will aggregate and upload every 1 minute.

Before you begin

The Secure Cloud Analytics Connector is supported on **IE3300, IE3400, IE3400H Switches** only.

- **Network Advantage** and **dna-advantage license**

SUMMARY STEPS

1. stealthwatch-cloud-monitor service-key <you service key> hostname my_sensor
2. flow record SWCRec
3. flow exporter SWCExp
4. interface gi1/0/3

DETAILED STEPS

	Command or Action	Purpose

Step 1	stealthwatch-cloud-monitor service-key <you service key> hostname my_sensor
	Example:
	`stealthwatch-cloud-monitor`
	`    service-key <you service key>`
	`    hostname my_sensor`
	`    url https://sensor.ext.obsrvbl.com`
	`openssl s_client -showcerts -connect`
	`https://sensor.ext.obsrvbl.com:443`
	`openssl s_client -showcerts -connect`
	`s3.ap-southeast-2.amazonaws.com:443`
	Example:
	`openssl s_client -showcerts -connect`
	`https://sensor.ext.obsrvbl.com:443`
	`openssl s_client -showcerts -connect`
	`s3.ap-southeast-2.amazonaws.com:443`
		Please have valid root CAs installed based on your URL. Please use below CLI to figure out the ROOT CAs as per your URL
		Configuring the service-key and hostname, which is used for sensor registration. If no hostname is provided, the serial number of the box is used for registration.

Step 2	flow record SWCRec
	Example:
	`flow record SWCRec`
	`match ipv4 source address`
	`match ipv4 destination address`
	`match transport source-port`
	`match transport destination-port`
	`match ipv4 protocol`
	`collect counter bytes long`
	`collect counter packets long`
	`collect timestamp sys first`
	`collect timestamp sys last`
		Configure the fields in flow record for collecting data for Secure Cloud Analytics record.

Step 3	flow exporter SWCExp **Example:**	Configure a Secure Cloud Analytics exporter and attach it to a flow monitor to start exporting to Secure Cloud.

	Command or Action	Purpose

	`flow exporter SWCExp`
	`    destination stealthwatch-cloud`
	
	`flow monitor SWCMon`
	`    flow record SWCRec`
	`    flow exporter SWCExp`	

Step 4	interface gi1/0/3
	Example:
	`Interface gi1/0/3`
	`    ip flow monitor SWCMon input`
		Identify the interface on which you want to monitor the flows and attach the monitor having Secure Cloud Analytics exporter to that interface

What to do next

For further Secure Cloud Analytics configuration information, refer to the appropriate configuration guide here: https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-and-configuration-guides-list.html.

Troubleshooting

- debug logs can be enabled by using ‘debug Stealthwatch’ CLIs

```
switch#debug stealthwatch-cloud ?
  all          All debugs for SWC
  cert         Certificate Validation
  error        errors
  event        Events
  file-events  File notifications
```

- For Platform level debugs you may use “debug platform software swc” CLIs

```
switch#debug platform software swc ?
  all         all
  errors      Stealthwatch Cloud errors
  events      Stealthwatch Cloud events
  pkt-events  Stealthwatch Cloud data collection events
```

Show Commands

- **Switch-1# show stealthwatch-cloud detail**

```
========================================
Stealthwatch Cloud Parameters
========================================
   Service Key  : x8SS2q7e4twpcNWT35AsL6i6xHd24iXJvICo3N4sGx1U1pCqqs
   Sensor Name  : petra
   URL          : https://sensor.anz-prod.obsrvbl.com
========================================
Stealthwatch Cloud Sensor Info
========================================
   Sensor Status    : Registered
   Last heartbeat   : 2020-05-08T12:11:50
```

- **Switch-1# show platform software swc stats**

```
==========================
SWC Upload Statistics:
==========================
1 : Last file uploaded          :  202005081212_ufihi2
2 : Time of upload              :  202005081213 UTC
3 : Current file uploading      :
4 : Files queued for upload     :
5 : Number of files queued      :  0
6 : Last failed upload          :
7 : Files failed to upload      :  0
8 : Files successfully uploaded :  416
==========================
SWC File Creation Statistics:
==========================
9 : Last file created           :  202005081212_ufihi2
10: Time of creation            :  202005081212 UTC
==========================
SWC Flow Statistics:
==========================
11: Number of flows in prev file:  1
12: Number of flows in curr file:  0
13: Invalid dropped flows       :  0
==========================
SWC Flags:
==========================
14: Is Registered               :  Registered
15: File Delete         :  Enabled
16: Exporter            :  Enabled
```