Cisco Secure Cloud Analytics

Internal Connection Watchlist Quick Start Guide

Table of Contents

Introduction to the Internal Connection Watchlist

Cisco Secure Cloud Analytics (formerly Stealthwatch Cloud) is a SaaS-based security service that detects and responds to threats in IT environments, both on-premises and in the cloud. This guide explains how to use Secure Cloud Analytics as a policy and segmentation auditing tool.

You can create allow and match rules from the Internal Connection Watchlist. If entities establish connections that trigger your match rules, and violate your firewall and segmentation policies, then the system generates an Internal Connection Watchlist Hit alert with the details of matching traffic. If you want to allow certain traffic that would otherwise trigger your match rule, then you can create a narrowly tailored allow rule for specific entities, as an exception.

Subnet Configuration

You can configure how the system generates alerts for entities within local, virtual cloud, and VPN subnets. You can also add a configured subnet to an entity group to facilitate adding a range of entities to that entity group at once. Based on the settings and subnet type, you can configure the subnet's sensitivity, which tunes the alerts that the system generates based on the subnet's settings. You can also configure whether the system generates an alert if it detects a new entity within the subnet range. See the following for more information:

Subnet Type	Configuration Options	Recommended Subnet Ranges
Local	• subnet range • relative threshold for alert generation • whether IP addresses are statically or dynamically assigned within the subnet • whether to alert on new entities detected within	• local entities in your on-premises network deployment • entities external to your on-premises network deployment that you control

	the subnet range	
Virtual Cloud (AWS and GCP)	• subnet range • relative threshold for alert generation • whether to alert on new entities detected within the subnet range	• cloud entities in your cloud-based network deployment
VPN	• subnet range	• entities within your VPN that may require network translation due to overlap that you do not want to track • entities external to your network deployment that are controlled by third parties

Configuring Local Subnet Alert Settings

You configure local subnets primarily for on-premises deployments. Specifically, you can configure local subnets for entities that are local to your on-premises network, or entities that are external to your on-premises network that you control. You can add one entry at a time, or upload multiple entries in a comma-separated value (CSV) file.

You can configure the following local subnet alert settings when you add a local subnet:

Parameter	**Description**
Prefix	The subnet prefix, in IPv4 format.
Length	The subnet length, in CIDR notation, from `1-32`. See https://tools.ietf.org/html/rfc4632 for more information.
Default Endpoint Sensitivity	The default subnet sensitivity, which influences the alerts that can be generated: • `high` - The system can generate `low`, `normal`, and `high` priority alerts. • `medium` - The system can generate `normal` and `high` priority alerts.

	• `low` - The system can generate `high` priority alerts.
Description	The local subnet description, displayed in the interface.

When adding a local subnet, you can configure the following alert generation settings:

Parameter	Description
Sensitivity	A subnet's sensitivity influences the alerts that can be generated: • `high` - The system can generate `low`, `normal`, and `high` priority alerts. • `medium` - The system can generate `normal` and `high` priority alerts. • `low` - The system can generate `high` priority alerts.
Static	Whether entities are statically assigned IP addresses in this subnet, or dynamically assigned IP addresses, such as through DHCP. If entities in this subnet receive statically assigned IP addresses, the system assumes that an IP address always correlates with the same entity.
New Device Alerts	Whether the system generates an alert for this subnet if a new device appears on this subnet. We recommend that you enable this parameter only if you also enable Static IP assignment for this subnet. Dynamically assigned IP addresses may cause the system to generate an excessive amount of new device alerts each time an existing device is dynamically assigned a different IP address.

Add an Entry to the Local Subnet Alert Settings

1. Select **Settings > Subnets > On-Premises**.
2. Click **Create On-Premises Subnet**.
3. Enter a CIDR block **Prefix** as an IPv4 address.
4. Enter a CIDR block **Length** from `1` to `32`.
5. Enter an entry **Description**.
6. You have the following options:

- Check **Static** to identify a subnet that statically assigns IP addresses.
- Uncheck **Static** to identify a subnet that dynamically assigns IP addresses.

7. You have the following options:
    - Select **New Device Alerts** to receive a new device alert if the system detects a new device on this subnet.
    - Uncheck **New Device Alerts** to suppress new device alerts if the system detects a new device on this subnet.
8. Click **Create**.
9. Select a **Sensitivity** from the drop-down list:
    - `low` - The system requires a high relative threshold to generate alerts.
    - `normal` - The system requires a moderate threshold to generate alerts.
    - `high` - The system requires a low threshold to generate alerts.

Search for a Local Subnet Alert Settings Entry

1. Select **Settings > Subnets > On-Premises**.
2. Enter a **Subnet Prefix** and click **Apply** to locate a local subnet alert settings entry.

Modify a Local Subnet Alert Settings Entry

1. Select **Settings > Subnets > On-Premises**.
2. For an existing entry, select a **Sensitivity** from the drop-down list.
3. You have the following options:
    - Select **Static** to identify a subnet that statically assigns IP addresses.
    - Uncheck **Static** to identify a subnet that dynamically assigns IP addresses.
4. You have the following options:
    - Select **New Device Alerts** to receive a new device alert if the system detects a new device on this subnet.
    - Uncheck **New Device Alerts** to suppress new device alerts if the system detects a new device on this subnet.

Uploading a Local Subnet Settings File

You can upload a comma-separated value file with multiple local subnet entries, one entry per line. Each line should be in the following format:

```
<cidr-prefix>,<cidr-length>,<description>,[sensitivity],[static-ip-assign],[new-device-alerts]
```

See the following for more information:

Parameter	Required	Allowed Values
`<cidr-prefix>`	yes	An IPv4 address.
`<cidr-length>`	yes	An integer from `1` to `32`.
`<description>`	yes	Any alphanumeric characters.
`[sensitivity]`	no	One of the following: • `low` - The system requires a high relative threshold to generate alerts. • `normal` - The system requires a moderate threshold to generate alerts. • `high` - The system requires a low threshold to generate alerts.
`[static-ip-assign]`	no	One of the following: • `true` - entities in the subnet receive statically assigned IP addresses • `false` - entities in the subnet receive dynamically assigned IP addresses
`[new-device-alerts]`	no	One of the following: • `true` - the system generates alerts for new devices detected in the subnet • `false` - the system suppresses alerts for new devices detected in the subnet We recommend that you set this parameter to `true` only if you also set `[static-ip-assign]` to true. Dynamically assigned IP addresses may cause the system to generate an excessive amount of new device alerts each time an existing device is dynamically assigned a different IP address.

Upload a Subnet Alert Settings File

1. Select **Settings > Subnets > On-Premises**.
2. Click **Upload CSV**.

3. Click **Upload File** to select your file for upload.

Modifying Virtual Cloud Subnet Settings

If you configure Cisco Secure Cloud Analytics public cloud monitoring (formerly Stealthwatch Cloud Public Cloud Monitoring) for a cloud-based environment using the default policy configuration provided, Secure Cloud Analytics retrieves cloud subnet information via the configured permissions.

You can configure the following alert generation settings for a virtual cloud subnet after the system detects an entry:

Parameter	Description
Sensitivity	A subnet's sensitivity influences the alerts that can be generated: • `high` - The system can generate `low`, `normal`, and `high` priority alerts. • `medium` - The system can generate `normal` and `high` priority alerts. • `low` - The system can generate `high` priority alerts.
Static	Whether entities are statically assigned IP addresses in this subnet, or dynamically assigned IP addresses, such as through DHCP. If entities in this subnet receive statically assigned IP addresses, the system assumes that an IP address always correlates with the same entity.
New Device Alerts	Whether the system generates an alert for this subnet if a new device appears on this subnet. Cisco recommends that you enable this parameter only if you also enable Static IP assignment for this subnet. Dynamically assigned IP addresses may cause the system to generate an excessive amount of new device alerts each time an existing device is dynamically assigned a different IP address.

After the system adds a virtual cloud subnet, you can search for the entry.

Search for a Virtual Cloud Subnet Alert Settings Entry

1. Select **Settings > Subnets**.
2. Select **Amazon Web Services**, **Google Cloud Platform**, or **Microsoft Azure**.

3. Enter a **Subnet Prefix** and click **Apply** to locate a virtual cloud subnet alert settings entry.

Modify a Virtual Cloud Subnet Alert Settings Entry

1. Select **Settings > Subnets**.
2. Select **Amazon Web Services**, **Google Cloud Platform**, or **Microsoft Azure**.
3. For an existing entry, select a **Sensitivity** from the drop-down list.
4. You have the following options:
    - Select **New Device Alerts** to receive a new device alert if the system detects a new device on this subnet.
    - Uncheck **New Device Alerts** to suppress new device alerts if the system detects a new device on this subnet.

Configuring VPN Subnet Alert Settings

VPN subnets identify external IP address spaces that are considered an extension of the managed network, such as trusted third party affiliates. You can configure these subnets for external entities controlled by third parties that you do not want to track.

You can configure the following VPN subnet alert settings when you add a VPN subnet:

Parameter	Description
Prefix	The subnet prefix, in IPv4 format.
Length	The subnet length, in CIDR notation, from `1-32`. See https://tools.ietf.org/html/rfc4632 for more information.
Description	The local subnet description, displayed in the interface.

After you add a VPN subnet, you can search for the entry.

In contrast with local subnet alert settings, you cannot modify the sensitivity, IP address assignment, or if an alert is generated when a new entity is detected for the VPN subnet. You can only modify the description displayed in the interface.

Add an Entry to the VPN Subnet Alert Settings

1. Select **Settings > Subnets > Virtual Private Networks**.
2. Click **Create VPN Subnet**.
3. Enter a CIDR block **Prefix** as an IPv4 address.

4. Enter a CIDR block **Length** from `1` to `32`.
5. Enter an entry **Description**.
6. Click **Create**.

Search for a VPN Subnet Alert Settings Entry

1. Select **Settings > Subnets > Virtual Private Networks**.
2. Enter a **Subnet Prefix** and click **Search** to locate a VPN subnet alert settings entry.

Modify a VPN Subnet Alert Settings Entry

1. Select **Settings > Subnets > Virtual Private Networks**.
2. Click the **Edit icon**.
3. Update the **Description**.
4. Click **Update**.

Entity Group Settings

You can configure entity groups for your Secure Cloud Analytics deployment, which group user-defined subnets and CIDR blocks. You can then use these groups for Internal Connection Watchlist entries, to monitor multiple entities, or possible entities from a given block of IP addresses, rather than create individual entries for each entity.

To add subnets, first configure them in the Subnets setting. For more information, see Subnet Configuration.

To add CIDR blocks, you can either define them individually, or upload a comma-separated value (CSV) file with multiple CIDR blocks. Each entry in the file must follow the format `prefix,length`, and only the first entry per line will be uploaded. If the system detects duplicate CIDR blocks, it will not add the duplicate blocks to the Entity Group.

Configuring Entity Groups

Create an Entity Group:

Procedure

1. Select **Settings > Entity Groups**.
2. Click **New Entity Group**.
3. Enter a **Name** and **Description** for your Entity Group.
4. Click **Next**.

The Subnets tab appears.

5. If you want to add subnets, you have the following options:
    - Select one or more subnets from the Add Subnets pane, then click **Add Selected to Group** to add them to the Entity Group.
    - Select one or more subnets from the Currently In Group pane, then click **Delete Selected** to remove them from the Entity Group.

    See Subnet Configuration for more information on creating subnets.
6. Select the CIDRs tab.
7. If you want to add CIDR blocks, you have the following options:
    - Enter a **CIDR Prefix** and **Length**, then click Add to add one CIDR block to the Entity Group. Enter a **Length** of `32` to only monitor the listed IP address, or a different value to monitor a larger CIDR block of values.
    - Click **Browse** and select a CSV file that contains CIDR blocks in the format `prefix,length` with one entry per line, then click **Upload** to add the first CIDR block in each line to the Entity Group.
8. Click **Create**.

Modify an Entity Group:

Procedure

1. Select **Settings > Entity Groups**.
2. Click edit for an existing Entity Group.
3. Enter a different **Name** and **Description** for your Entity Group.
4. Select the Subnets tab.
5. You have the following options:
    - Enter a **CIDR Prefix** and **Length**, then click Add to add one CIDR block to the Entity Group. Enter a **Length** of `32` to only monitor the listed IP address, or a different value to monitor a larger CIDR block of values.
    - Click **Browse** and select a CSV file that contains CIDR blocks in the format `prefix,length` with one entry per line, then click **Upload** to add the first CIDR block in each line to the Entity Group.
6. Select the CIDRs tab.
7. You have the following options:

- Select one or more subnets from the Add Subnets pane, then click **Add Selected to Group** to add them to the Entity Group.
- Select one or more subnets from the Currently In Group pane, then click **Delete Selected** to remove them from the Entity Group.

See Subnet Configuration for more information on creating subnets.

8. Click **Done** to save your changes.

Delete an Entity Group

Procedure

1. Select **Settings > Entity Groups**.
2. Click the delete icon for an existing Entity Group and confirm your selection.

Common Protocols and Programs for Alerting

See https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml for a comprehensive list of ports.

> If you want to allow traffic over a certain protocol for trusted hosts, create a narrowly tailored allow rule in conjunction with a broad match rule.

Protocol or Program	Associated Ports
Domain Name Service (DNS)	53/TCP, 53/UDP
Server Message Block (SMB)/Samba	445/TCP
SMB/Samba via NetBIOS	137/TCP, 137/UDP, 138/UDP, 139/TCP
SSH	22/TCP
TeamViewer	5938/TCP, 5938/UDP
telnet	23/TCP, 23/UDP
Virtual Network Computing (VNC)	5800/TCP, 5900/TCP by default
Windows Remote Desktop	3389/TCP, 3389/UDP

Creating a Policy Violation Rule

Note the following as you create policy violation rules:

- Because Secure Cloud Analytics does not influence your traffic flow, allow and match rules do not function as firewall rules. Even if traffic matches these rules and the system generates an alert, this does not directly allow or block the traffic. It does allow you to research the entities involved with the alert and traffic.
- By default, rules that you add to the Internal Connection Watchlist are match rules. Enable **Connections are Allowed** to create an allow rule. Generally, use this in conjunction with a broader match rule to allow legitimate traffic for trusted hosts, while triggering the match rule for all other traffic of that type.
- Specify a CIDR **Block Size** of `32` if you want to alert on a single source or destination entity. See https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing#IPv4_CIDR_blocks for more information on CIDR block boundaries and the IP addresses within the CIDR block you specify.
- If you want to alert on a source entity using a specific protocol or program, enter a **Destination IP** of `0.0.0.0`, **Destination Block Size** of `0`, and the **Destination Ports** associated with the protocol or program.

Create a policy violation rule:

Before You Begin

- Log into the web portal UI.

Procedure

1. Select **Settings > Alerts > Internal Connections Watchlist**.
2. Click **New Watchlist Item**.
3. Enter a watchlist entry **Rule Name** and **Description**.
4. Select a **Connection Rule Type** of `Allowed` if you want connections that match this entry to not generate observations or alerts. Select `NOT Allowed` if you want connections that match this entry to generate observations or alerts.

   You must add at least one `NOT Allowed` rule to the Internal Connection Watchlist before adding any `Allowed` rules.
5. Select a **Protocol** from the drop-down list..
6. Select **Source** to expand the field.
7. You have the following options:

   Select **CIDR**, then enter an **IP** address and **Bytes/Length** to define the source CIDR block. Enter a **Bytes/Length** of `32` to only monitor the listed IP address, or a different value to monitor a larger CIDR block of values.

Select **Entity Groups**, click **Add Entity Group(s)**, select one or more Entity groups, and click **Add to Source**.

8. If you want to limit the source to certain ports, enter individual Source **Ports**, or port ranges.
9. Select **Destination** to expand the field.
10. You have the following options:

    Select **CIDR**, then enter an **IP** address and **Bytes/Length** to define the destination CIDR block. Enter a **Bytes/Length** of `32` to only monitor the listed IP address, or a different value to monitor a larger CIDR block of values.

    Select **Entity Groups**, click **Add Entity Group(s)**, select one or more Entity groups, and click **Add to Destination**.
11. If you want to limit the destination to certain ports, enter individual Destination **Ports**, or port ranges.
12. Click **Save**.

Viewing Policy Violation Alerts

If traffic triggers one of the match rules, then the system generates an Internal Connection Watchlist Observation. The system also generates an Internal Watchlist Connection Hit alert. Unlike other alerts, which may result from multiple observations, the system can generate an Internal Connection Watchlist Hit alert with only 1 observation, if the traffic related to the observations triggers one of your match rules. However, if multiple observations trigger one of the match rules, the system generates the alert, and lists all of the supporting observations within the alert.

You can filter the alerts list to view only these alerts.

View Policy Violation Alerts

Before You Begin

- Log into the web portal UI.

Procedure

1. Select **Monitor > Alerts**.
2. Enter `internal connection watchlist hit` in the filter field, then click the **(Magnifying Glass)** icon to sort the alerts list.

Additional Resources

For more information about Secure Cloud Analytics, refer to the following:

- https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html for a general overview
- https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html to sign up for a 60-day Free Trial
- https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html for documentation resources
- https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html for installation and configuration guides, including the Secure Cloud Analytics Initial Deployment Guide

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
- For Secure Cloud Analytics Free Trial customers, open a case by email: swatchc-support@cisco.com

Copyright Information