

# Monitoring Remote Access Users (6.9)

## Use Case Abstract

### Customer situation

When it comes to security, the ability to monitor and control remote access often tops the list of concerns as the numbers of remote workers, third-party partners who need access, and cloud networks continue to rise.

### Solution

Using Cisco Stealthwatch® host groups, you can define, identify and monitor remote users. Create a host group that contains internal VPN IP addresses to keep track of the remote users who have network access, and a host group that contain the nodes that outside remote users will use to connect.

### Minimum requirements:

The Cisco Stealthwatch system configuration minimum requirements are:

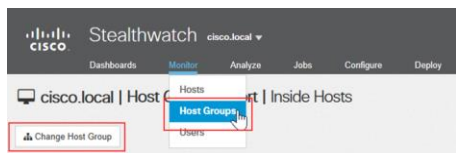
- Visibility of all host-to-host traffic from the core/distribution
- Stealthwatch Release 6.9 or greater

# Detecting Remote Network Access

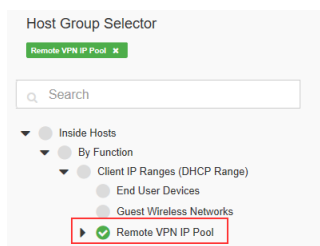
You need to monitor the following users:

- Those with remote access
- Those running internal services that reach out

To see remote users, run a Host Group report on the group that houses all the IP addresses for the VPN and remote users pool. From the Stealthwatch Management Console (SMC) Web User Interface (UI), click **Monitor** and choose **Host Groups**. Then, click **Change Host Group**.

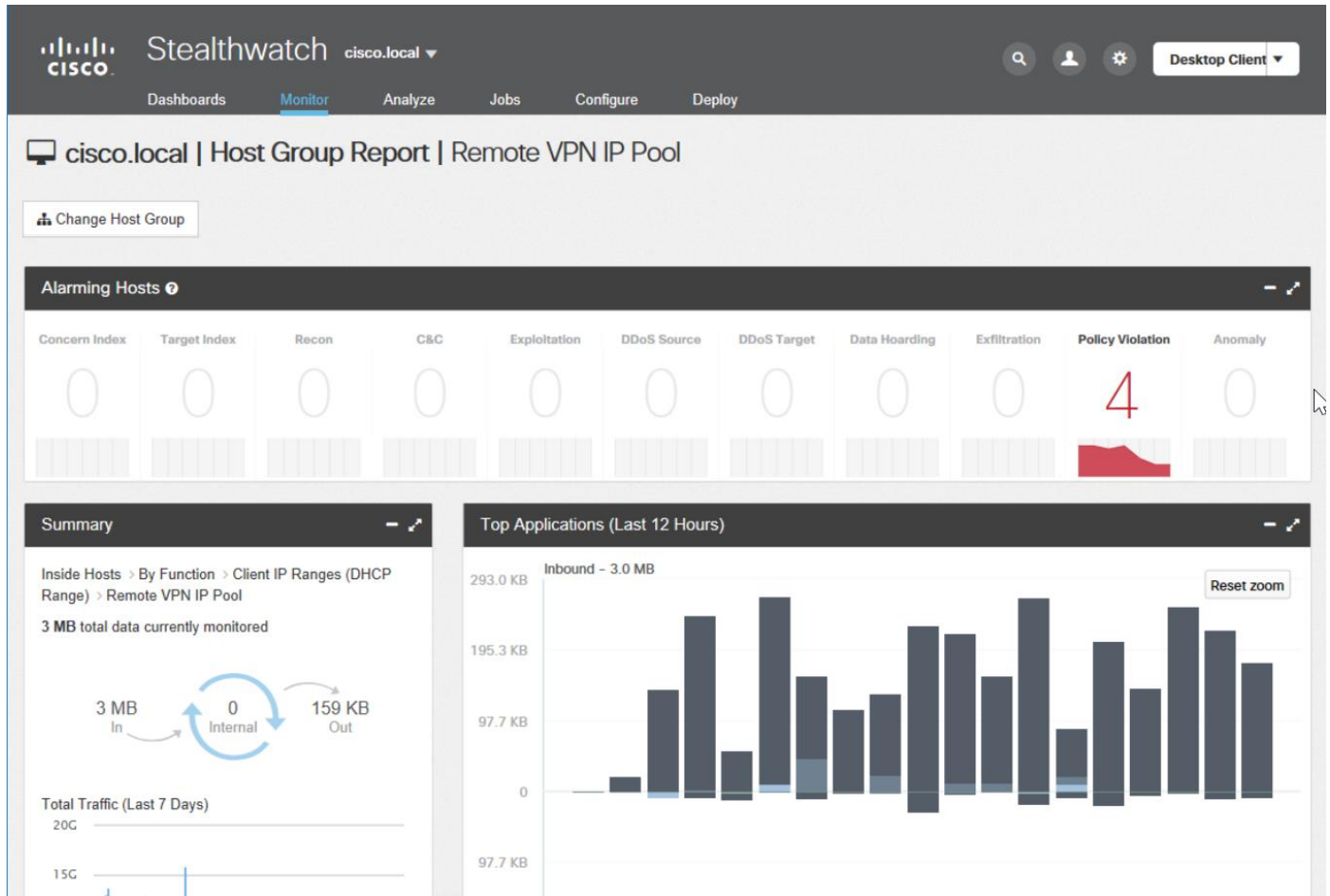


For our example, we use the Remote VPN IP Pool group.

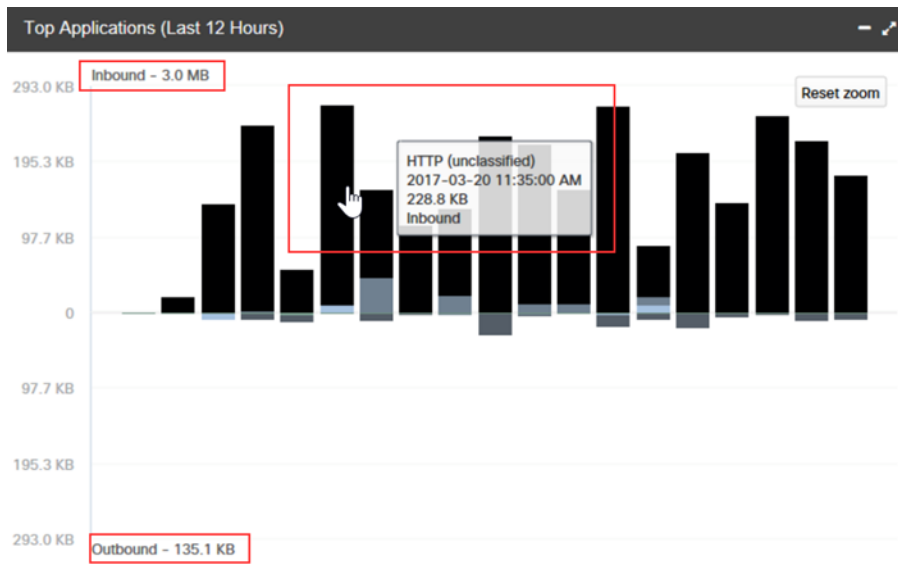


The figure shows an example of the Host Group Report.

## Monitoring Remote Access Users (6.9)

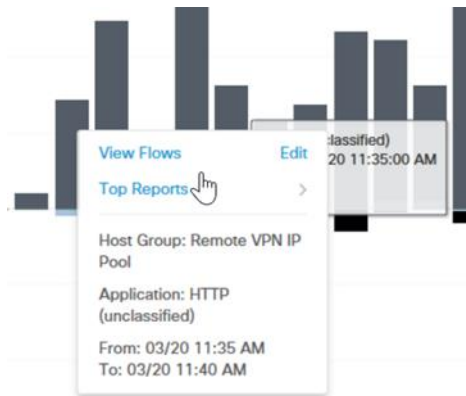


For a closer look at the activity, use the Top Applications widget that shows inbound and outbound traffic. To identify the application used, mouse over the bar graph.



For more information such as Top Reports or the associated flows for this communication, click a **bar**.

## Monitoring Remote Access Users (6.9)



For our example, we perform a Flow Search to see what hosts are communicating through remote connections. The flow search shows the host IP, host group, peer IP, and peer host group, application, ports, protocol, and much more. For more information, click the **IP address**.

START	DURATION	SUBJECT IP ADDRESS	SUBJECT PORT/PROTOCOL	SUBJECT HOST GROUPS	SUBJECT BYTES	CONNECTION APPLICATION	CONNECTION BYTES	PEER IP ADDRESS	PEER PORT/PROTOCOL	PEER HOST GROUPS	PEER BYTES
Mar 20, 2017 11:37:07 AM	0s	10.13.138.60	62868/TCP	Remote VPN IP Pool	0	HTTP (unclassified)	2.73K	76.96.209.8	80/TCP	United States	2.73K
Mar 20, 2017 11:35:07 AM	0s	10.13.150.153	64343/TCP	Remote VPN IP Pool	0	HTTP (unclassified)	1.46K	24.40.43.37	80/TCP	United States	1.46K
Mar 20, 2017 11:35:06 AM	0s	10.13.131.42	49870/TCP	Remote VPN IP Pool	1.46K	HTTP (unclassified)	1.46K	76.96.209.8	80/TCP	United States	0
Mar 20, 2017 11:35:02 AM	0s	10.13.155.180	63216/TCP	Remote VPN IP Pool	0	HTTP (unclassified)	1.46K	24.40.43.36	80/TCP	United States	1.46K

The Host Summary displays, showing traffic by Peer Host Group, and internal and external Application Traffic. With this information, you can determine:

- The host group that the host belongs to
- The policies that are applied
- The hosts and groups that this host has been communicating with
- The applications that this host has been transmitting with

## Monitoring Remote Access Users (6.9)

The screenshot displays the SMC Web UI interface for monitoring remote access users. It is divided into several sections:

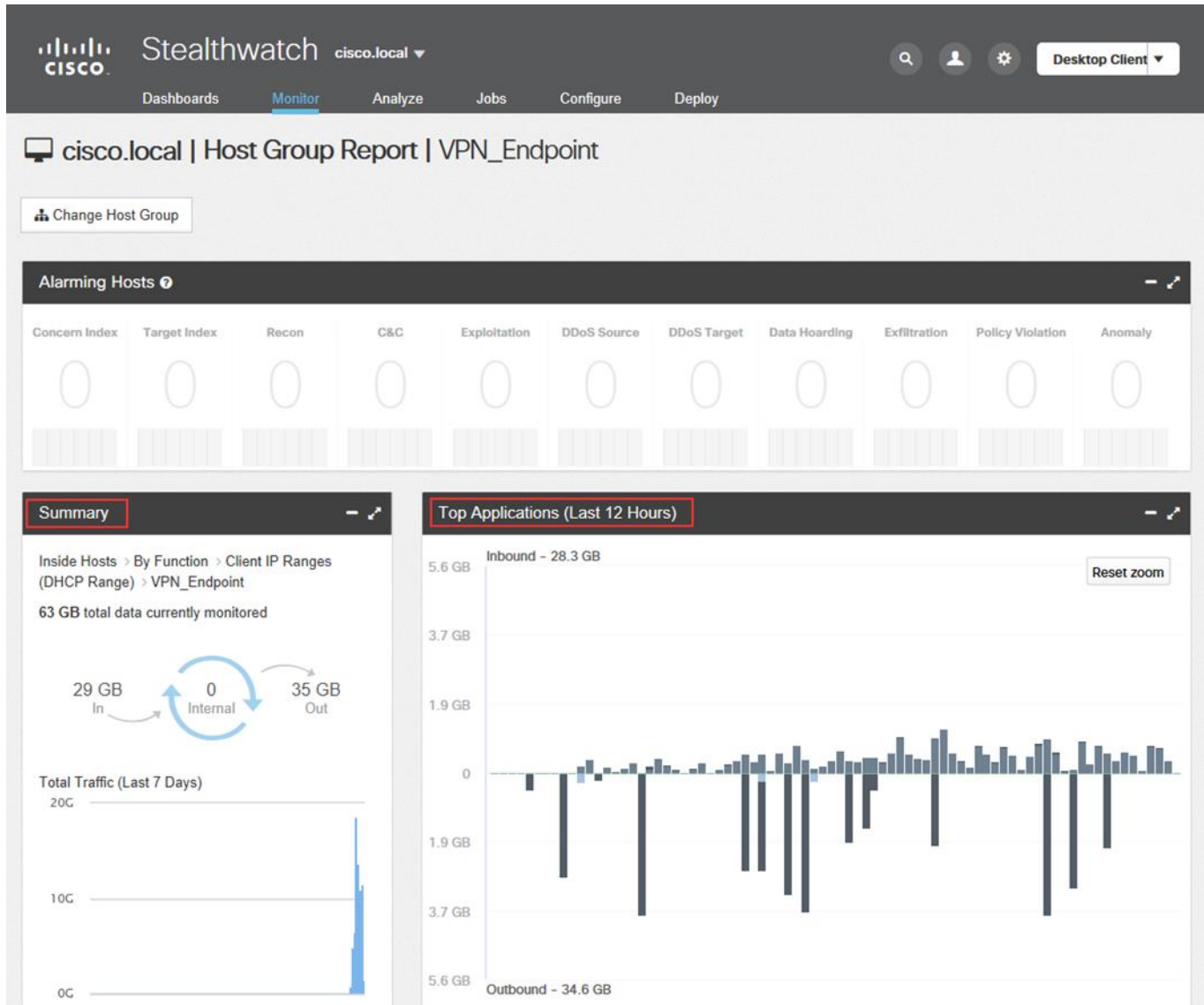
- Host Summary:** Shows details for Host IP 10.203.1.108. Key information includes:
  - Status: Active
  - Host Groups: Remote VPN IP Pool
  - Location: RFC 1918
  - Last Seen: 3/20/17 5:12 PM
  - Policies: Client IP Policy, Fake App, Inside
- Traffic by Peer Host Group (last 12 hours):** A Sankey diagram showing traffic flow from various peer host groups to the host 10.203.1.108. The groups listed are Outsourcer, Alpharetta, DeathStar, End User Devices, Catch All, and Desktops. The United States is also indicated as a source.
- Alarms by Type (last 7 days):** A chart area that currently displays "No data to display".
- Users & Sessions:** A section that currently displays "No User/Sessions information available."
- Application Traffic:** A table showing traffic details for Internal and External connections. The table includes columns for Application, Total, %, Sent, Ratio, Received, 7-day Trend, and 24-hour Trend.

Application	Total	%	Sent	Ratio	Received	7-day Trend	24-hour Trend
Undefined...	69.1MB	100.00	0B		69.1MB		
HTTPS	90.79KB	< 0.01	65.5KB		25.3KB		
ICMP	23.63KB	< 0.01	23.63KB		0B		

You can also look at the remote user connections by monitoring the Host Group that contains the IP addresses of the nodes used to connect to the internal network. For our example, we use the host group VPN\_Endpoint. This group contains all the IP addresses of the nodes used for VPN connection from the outside trusted users. Using the SMC Web UI, you can generate a host group report for the VPN\_Endpoint host group.

The host group report also shows inbound and outbound top applications and summary. For more information about inbound and outbound traffic, click **the bar graph**.

## Monitoring Remote Access Users (6.9)



DISCLAIMER WARRANTY: THIS CONTENT IS BEING PROVIDED "AS IS" AND AS SUCH MAY INCLUDE TYPOGRAPHICAL, GRAPHICS, OR FORMATTING ERRORS. CISCO MAKES AND YOU RECEIVE NO WARRANTIES IN CONNECTION WITH THE CONTENT PROVIDED HEREUNDER, EXPRESSED, IMPLIED, STATUTORY OR IN ANY OTHER PROVISION OF THIS CONTENT OR COMMUNICATION BETWEEN CISCO AND YOU. CISCO SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.