# 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:

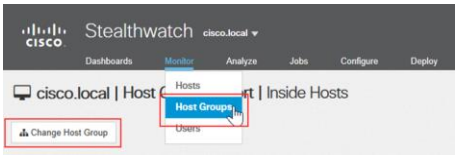
- Visibility of all host-to-host traffic from the core/distribution
- Stealthwatch Release 6.9 or greater

# Detecting Remote Network Access

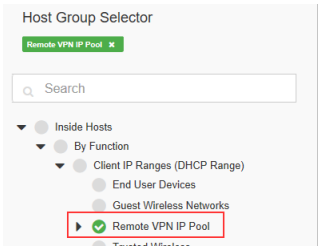
You need to monitor the following users:

- 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**.

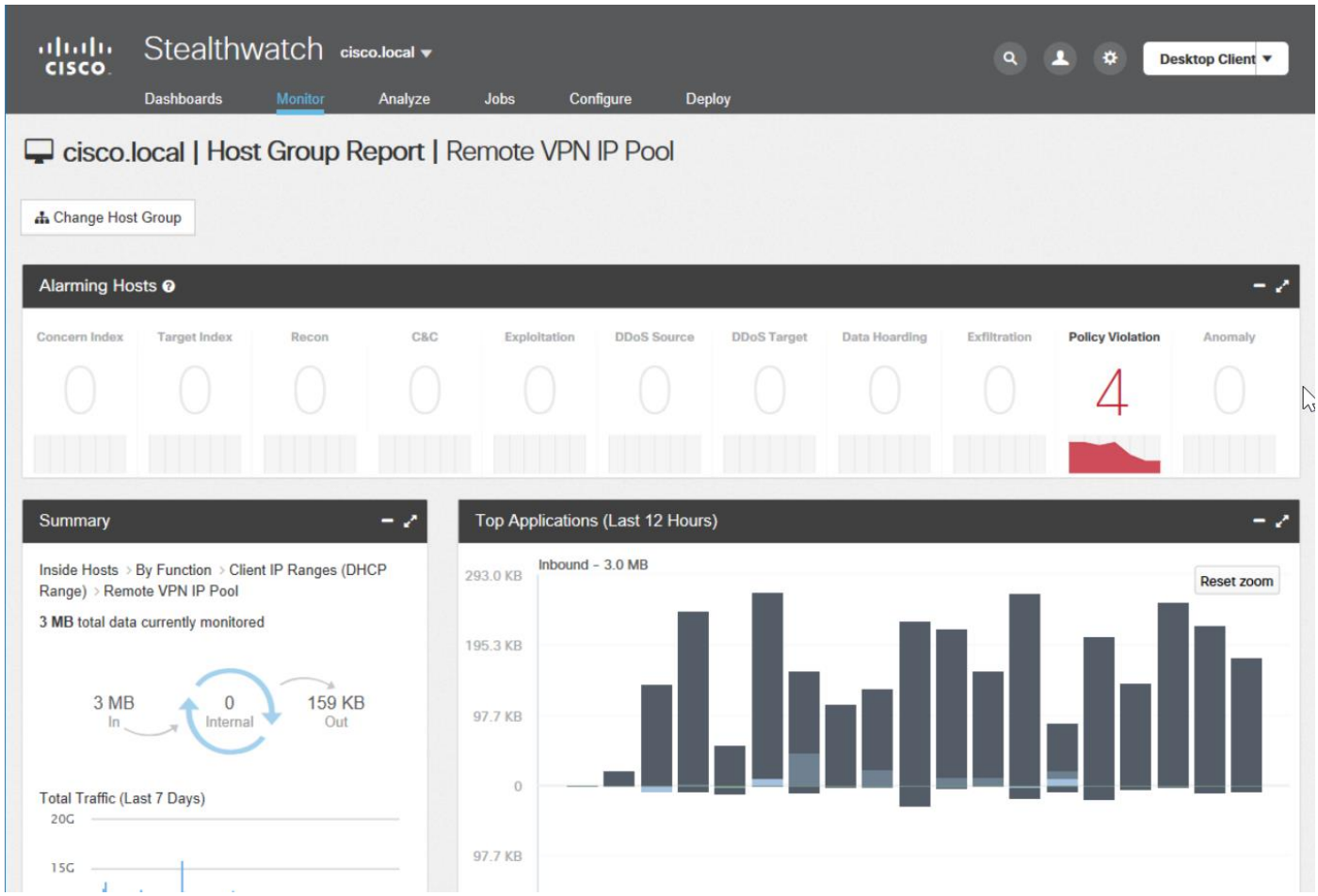



For our example, we use the Remote VPN IP Pool group.

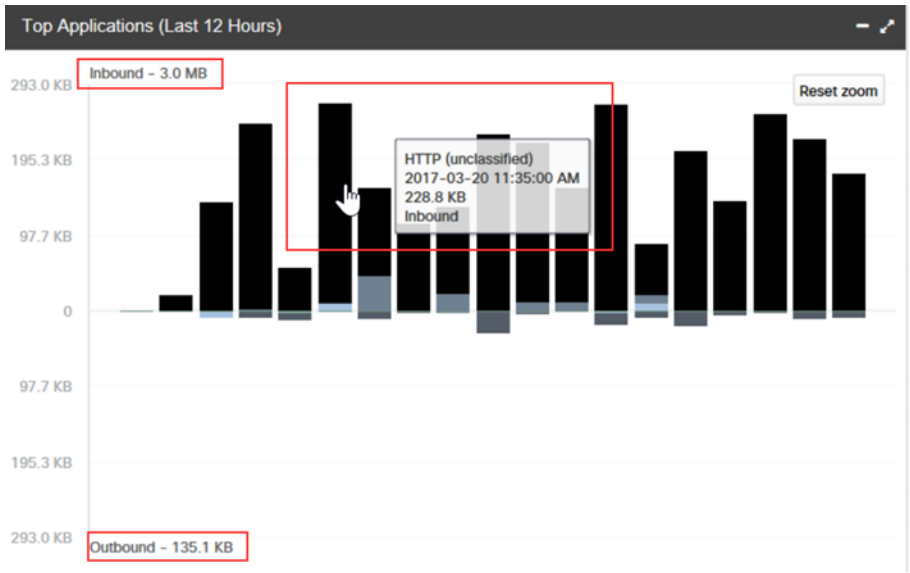



The figure shows an example of the Host Group Report.

## Monitoring Remote Access Users (6.9)

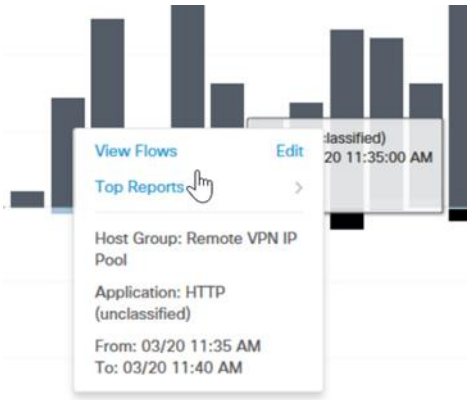



For a closer look at the activity, use the Top Applications widget that shows inbound and outbound traffic. To identify the application used, mouse over the bar graph.

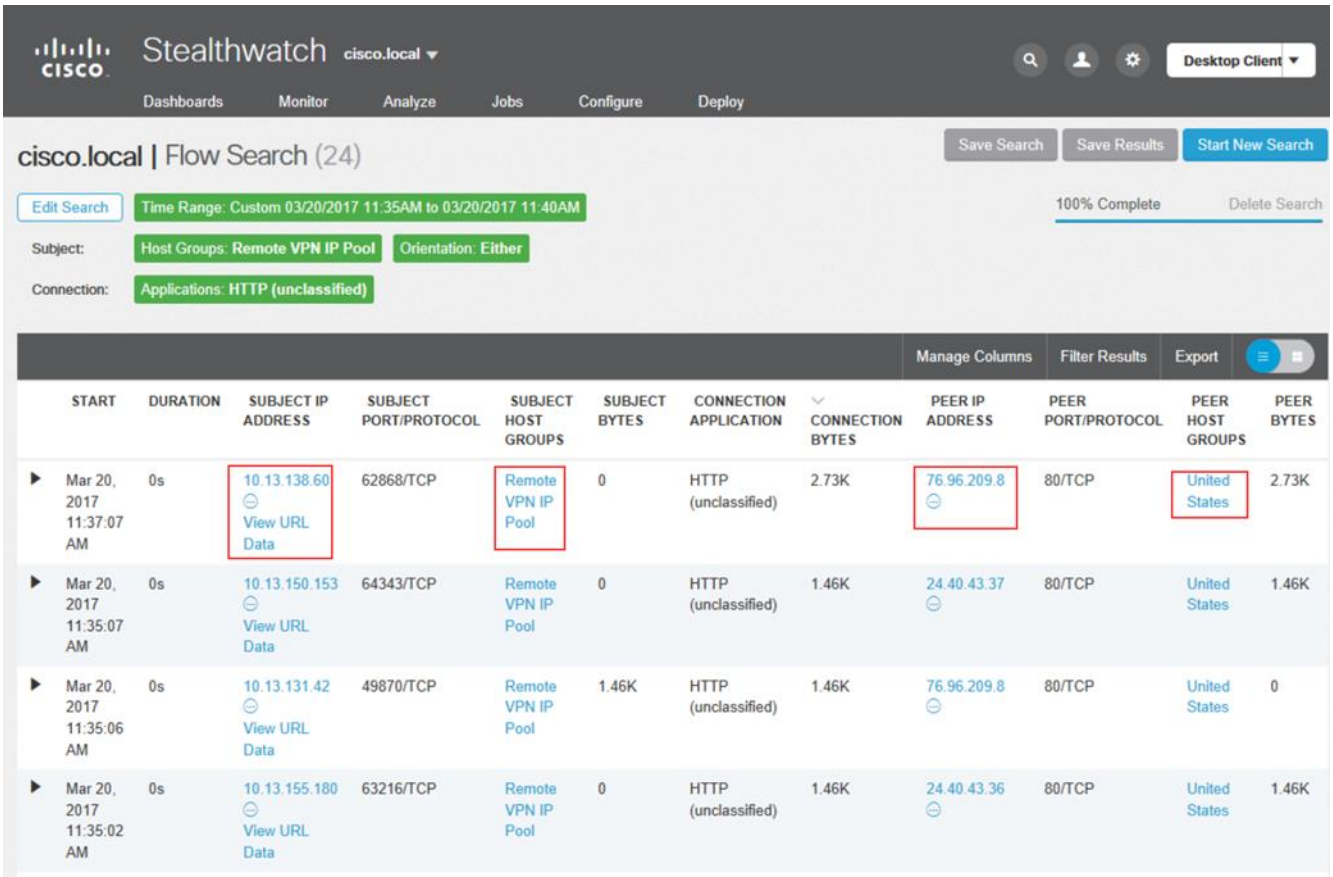



For more information such as Top Reports or the associated flows for this communication, click **a bar**.

## Monitoring Remote Access Users (6.9)



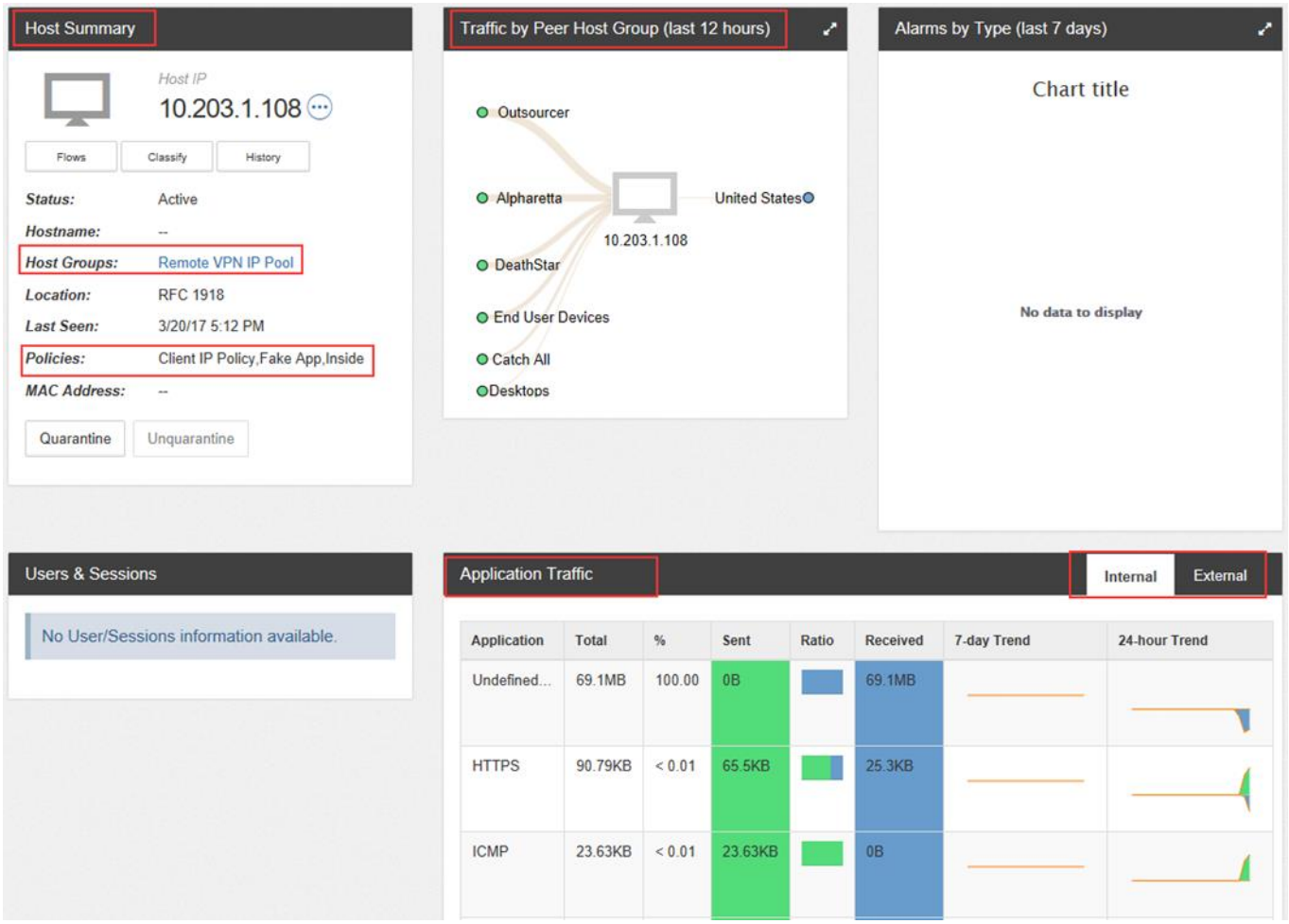

For our example, we perform a Flow Search to see what hosts are communicating through remote connections. The flow search shows the host IP, host group, peer IP, and peer host group, application, ports, protocol, and much more. For more information, click the **IP address**.




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)




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)