Cisco Secure Network Analytics Phased Approach to Tuning

Last Updated: Jun 25, 2021

Use this guide to learn the simple phased approach to tuning Cisco Secure Network Analytics (formerly Stealthwatch) v7.3. This guide is not intended to replace full Secure Network Analytics training, but allows for a framework to simplify operationalizing Secure Network Analytics with a tuning framework. Repeat these steps when you add a new collection of flow exporters to the deployment.

Reference for additional information on interpreting alarms:
https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/securit_events_alarm_categories/SW_7_3_Security_Events_and_Alarm_Categories_DV_3_0.pdf

Audience

This guide is for those with basic knowledge of Secure Network Analytics, host groups, and policy management. Refer to the Secure Network Analytics Desktop Client User Guide and online help for reference information on any terms.
https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/smc_users_guide/SW_7_3_Stealthwatch_Desktop_Client_User_Guide_DV_1_0.pdf

Training Offerings

List of available training offerings
https://www.cisco.com/c/en/us/products/security/stealthwatch/learning-services.html

Six Phased Approach to Tuning

Secure Network Analytics not only applies machine learning but also allows the flexibility to apply business logic and policy for threat detection. To do this, it enables you to apply granular classification, host groups, custom security events, and custom policies to meet business needs.

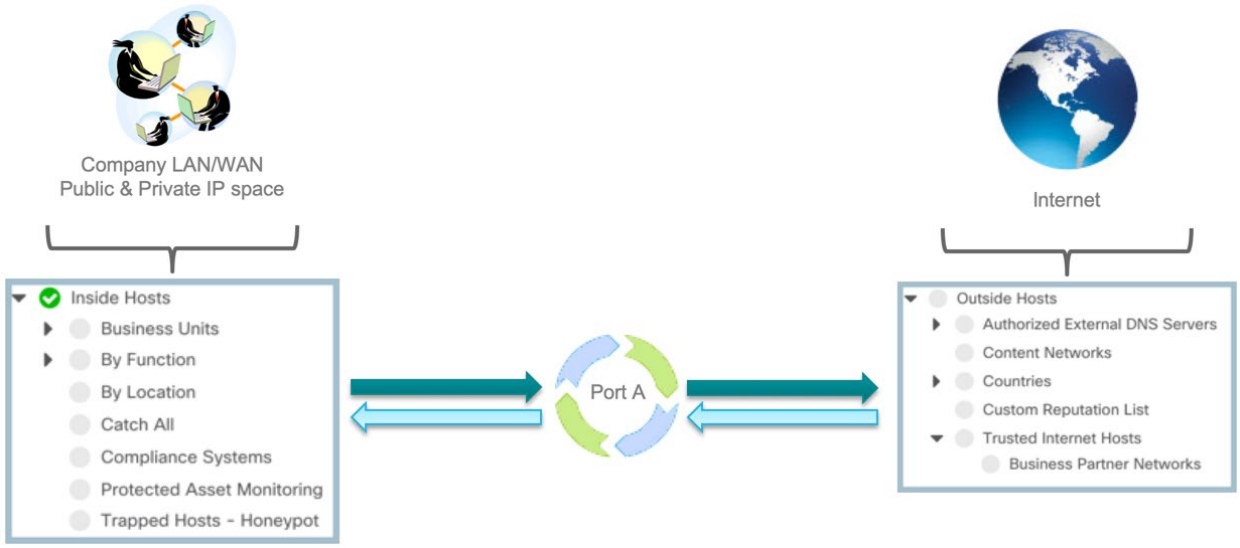
Phase 6: Classify Undefined Applications

Phase 1: Classify Inside

Bring RFC1918 and public IPs to Inside Inside

By default, all IP address space falls under the Outside Host Group until you define what makes up your LAN/WAN infrastructure or "Inside Hosts."

Separating the Internet (known as "Outside Hosts") from Inside Hosts allows for detecting suspicious traffic to/from the Internet.

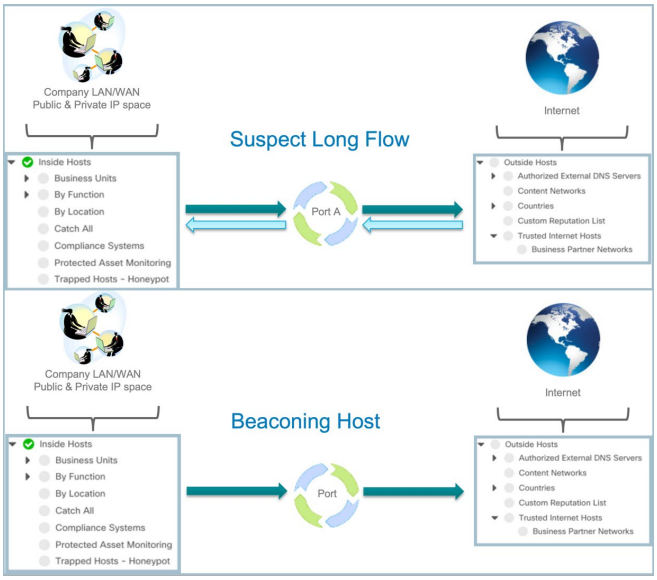


Why is it important to classify the Inside Host group?

There are several alarms that trigger that focus between inside and outside traffic. Capturing the organizations owned IP space will reduce false positives.

Some alarms affected include:

- Suspect Data Loss
- Exfiltration
- Suspect Quiet Long Flow
- Suspect Long Flow
- Beaconing Hosts
- High File Sharing Index

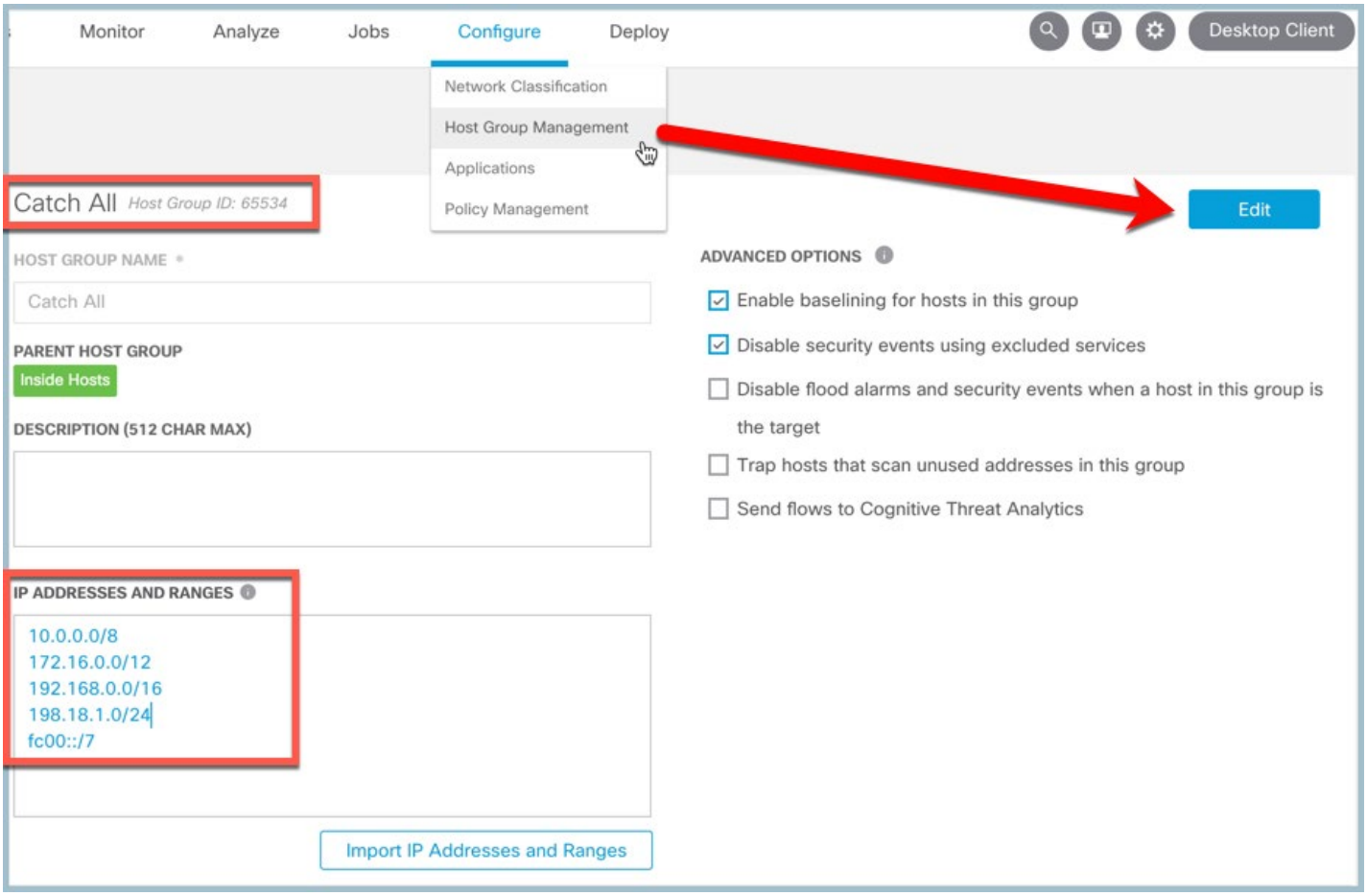


Phase 1: Tell Secure Network Analytics What IP Space Your Organization Owns

The "Catch All" host group within Inside Hosts is a special group to quickly bring in all IP space owned by the organization.

Catch All should contain:

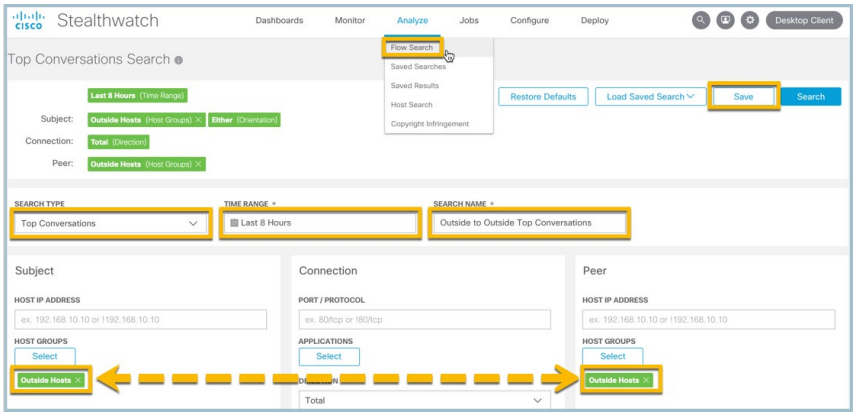
- All non-routable IP space (RFC1918 & RFC4193), which is defined by default.
- All registered public IP space owned by the organization, which needs to be identified.



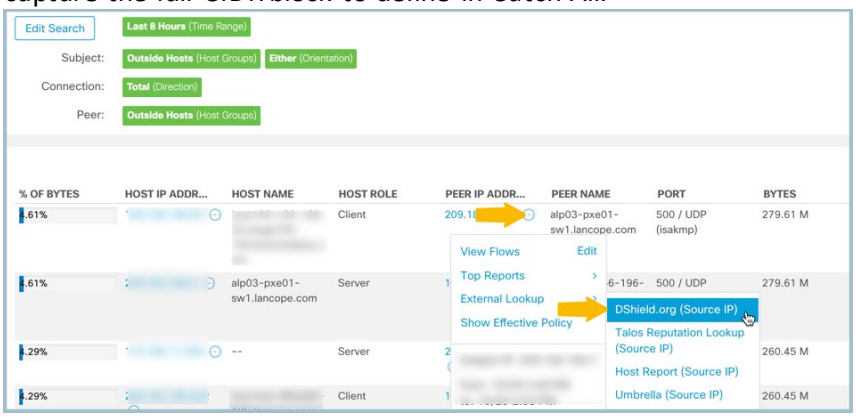
Phase 1: Tell Secure Network Analytics What IP Space Your Organization Owns

An easy way to classify what IP space is owned by the organization is to:

- Run a Top Conversations for the last 8 hours between Outside to Outside as illustrated below.
- Save the search with name "Outside to Outside Top Conversations" to make it easy to rerun.
- If you see outside-to-outside traffic, one of the IP ranges should be moved to the Inside Hosts.



- Look for IP addresses repeated within the Top Conversations and view the name resolution to help identify
- Perform a D-Shield.org Lookup or "who is" to determine which IP is registered by the organization and capture the full CIDR block to define in Catch All.



- Populate the "Catch All" host group with all of the registered public IP space
- Repeat above until you've captured all IP ranges owned by the organization

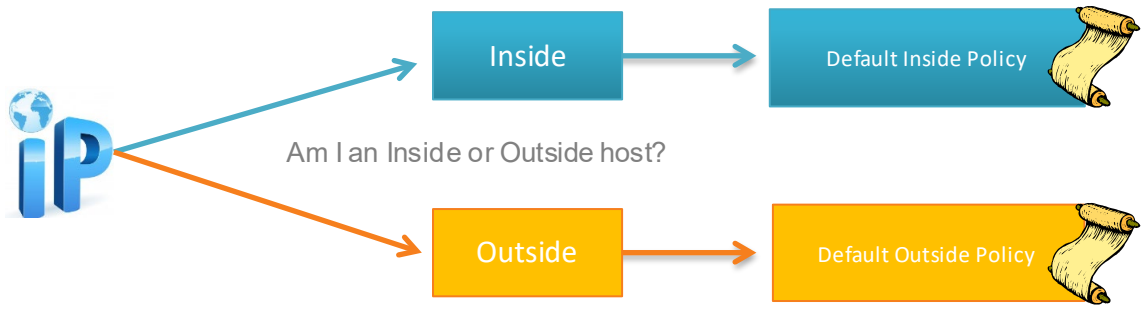
NOTE: You should see IP addresses used as NAT gateways and/or proxies while you're reviewing outside to outside IP addresses. You will need to also classify those individual IP addresses within the NAT Gateway and/or Proxy Servers host group for a proper policy to be applied.

Phase 2: Build Policy Groups Framework (Use By Function)

Ensure Role Policies are tied to functional groups

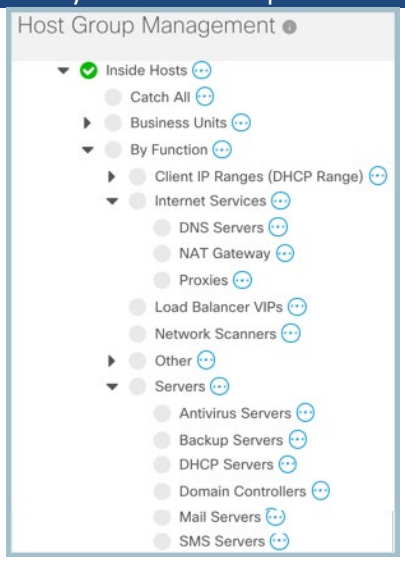
Start with the defaults.

- Every host belongs within the Inside or Outside host group structure and will be assigned a default policy until a more specific Role is defined.



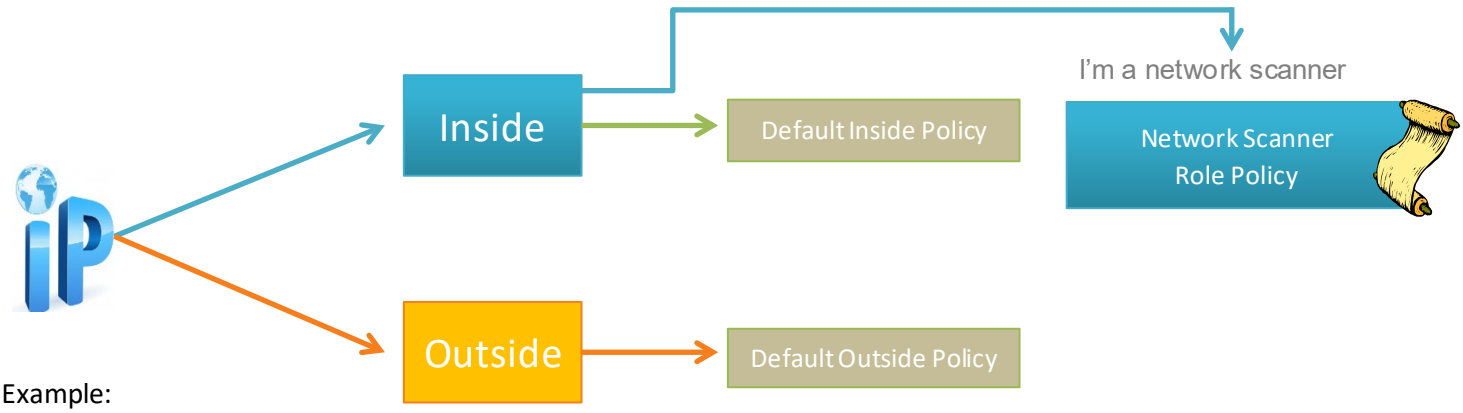
- Policies can be applied to Host Groups or individual IPs.
- **Best practice**: Build a collection of Host Groups that a Role policy is tied to based on the role/function of the system.

Below is a list of default By Function groups along with default Role Policies with an appropriate policy already mapped to the functional groups. Simply drop the IPs in their respective functional group for a more appropriate policy to take effect. The servers highlighted in yellow below should be classified as soon as possible to apply proper policy and help detect threats more effectively.

Default By Function Groups	Default Role Policies Mapped to By Function Groups
	• Antivirus & SMS Servers • Client IP Policy • DHCP Server • Firewalls, Proxies, & NAT Devices • Guest Wireless • Mail Server Policy • Network Management & Scanners • Policy for Testing Security Events • Suppress Bot Alarms • Trapped Hosts - Honeypot Policy • Trusted Internet Hosts • Trusted Users Policy • Untrusted Users Policy

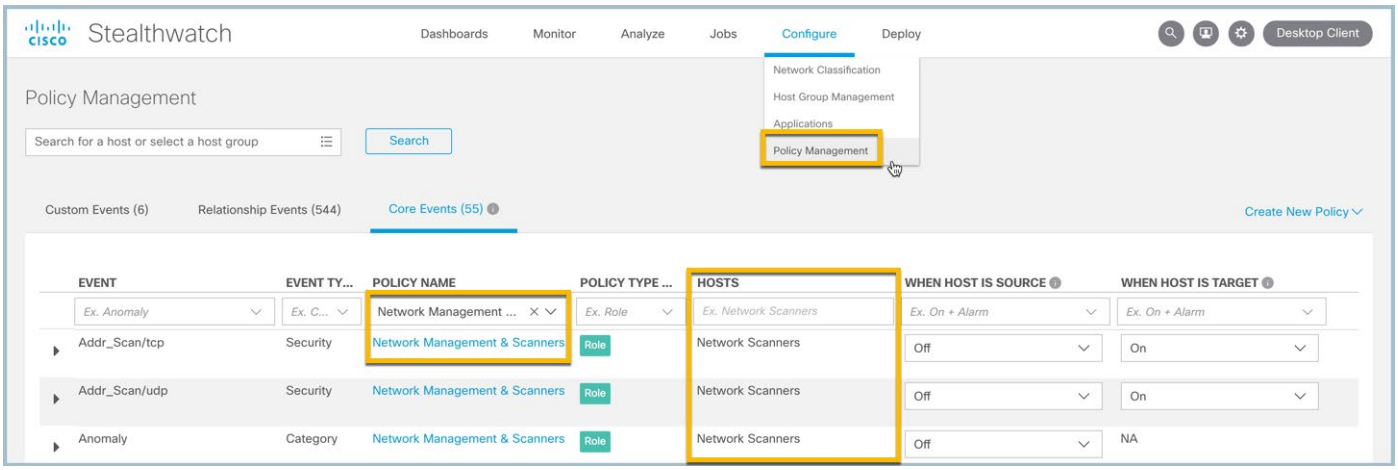
Phase 2: Build Policy Groups Framework

- The default inside and outside policy only takes effect if a host is NOT assigned a Role Policy.



Example:

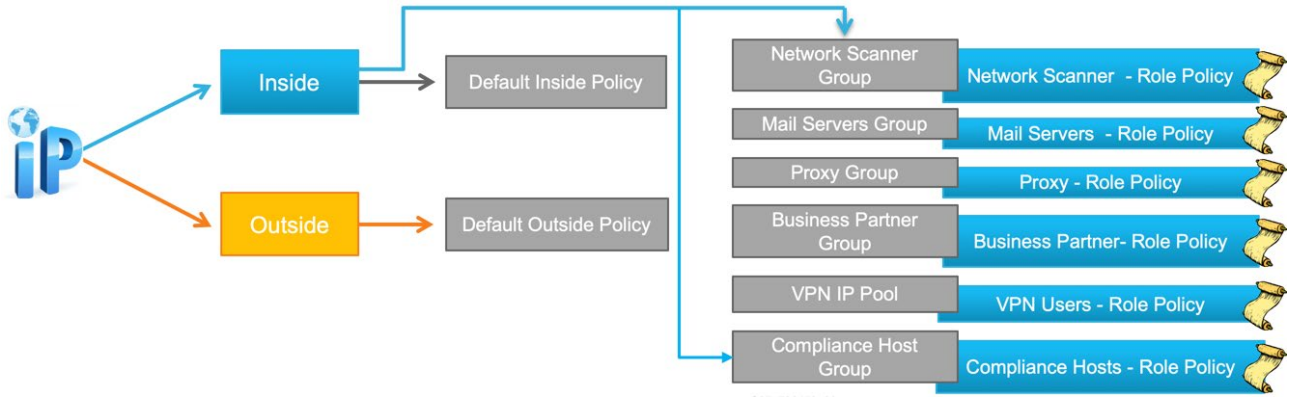
- Build a Host Group called Network Scanners (this group exists by default in version 7.1.)
- Build a Role Policy for Network Scanners and assign the Network Scanners group to this policy (this role policy already exists in version 7.1.)
- Add the Security Events a network scanner would trigger and adjust the policy:
  Add the Addr_Scan/tcp & Addr_Scan/udp and set the "When host is source" to Off as illustrated below.
- All flows seen by a network scanner are still recorded but an alarm will not generate for authorized scanning.



- By tuning the security event, it will by default tune the alarm category it contributes points to.
- To make tuning easy, it helps to build a Policy Groups framework to have policies tied to functions of systems.

Phase 2: Build Policy Groups Framework

- If you do not have the "By Function" defaults, that is not a problem. Follow this same simple framework.
- Once you have a framework of groups with role policies assigned to them, it is easy to move hosts to their respective function on the fly.
- **TIP:** You can select the Classify button on a host report and move the host to a pre-defined host group.



Best Practice: Do not over think policy. Although a host can be a member of multiple groups, each having its own Role Policy, try to only assign a single Role Policy for a given host to prevent confusion.

There are a number of security events built within Secure Network Analytics along with custom security events, so if one security event is tuned, chances are another event will detect a change in behavior.

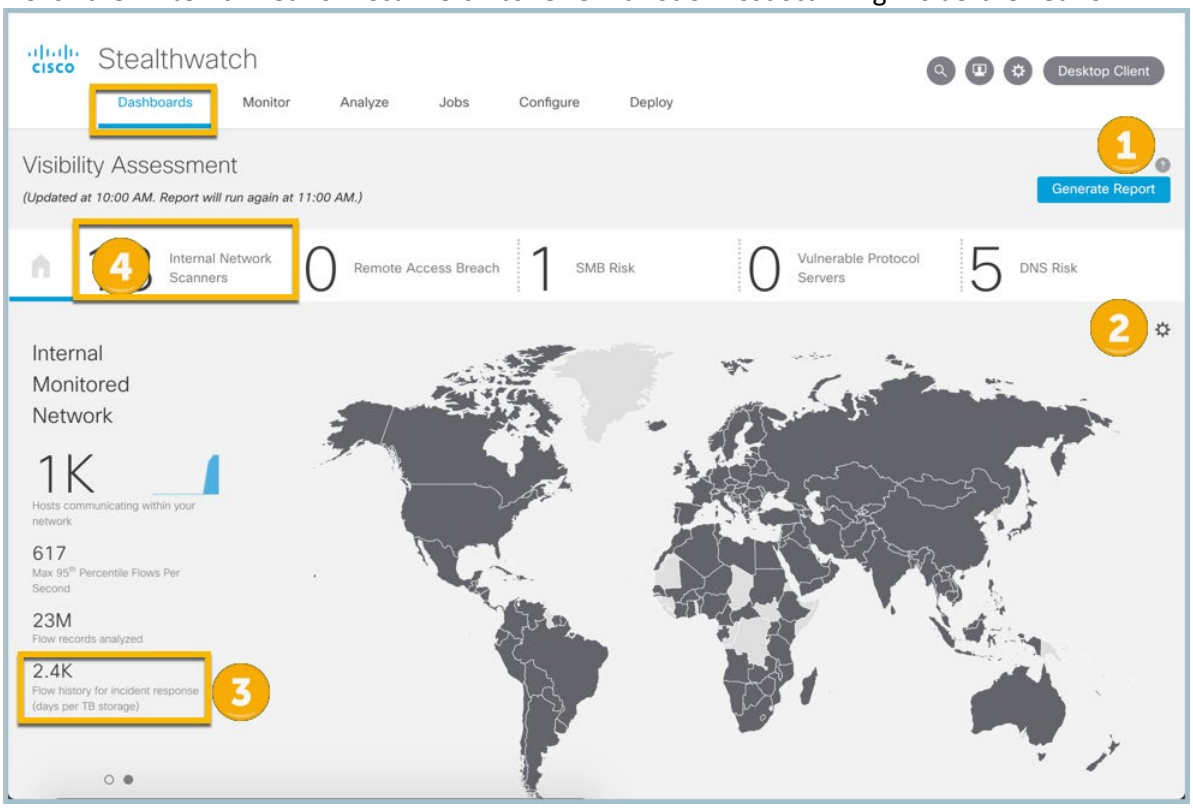
- If the same alarm type is part of two Role Polices and a host is part of both policies, that alarm could trigger twice, once for each policy. Avoid this by consolidating functional/role groups.
- Wait for alarms to trigger to know which alarm type should be added to a given Role Policy.
- The next section will illustrate how to quickly classify authorized scanners using the Visibility Assessment app that can be installed on the Secure Network Analytics version 7.1 and greater.

Phase 3: Classify Known Scanners

We will use the Visibility Assessment app to quickly classify known network scanners and also locate systems that may already be infected with malware.

- Open the Visibility Assessment from the Dashboards menu and complete the following steps for initial setup and classification:

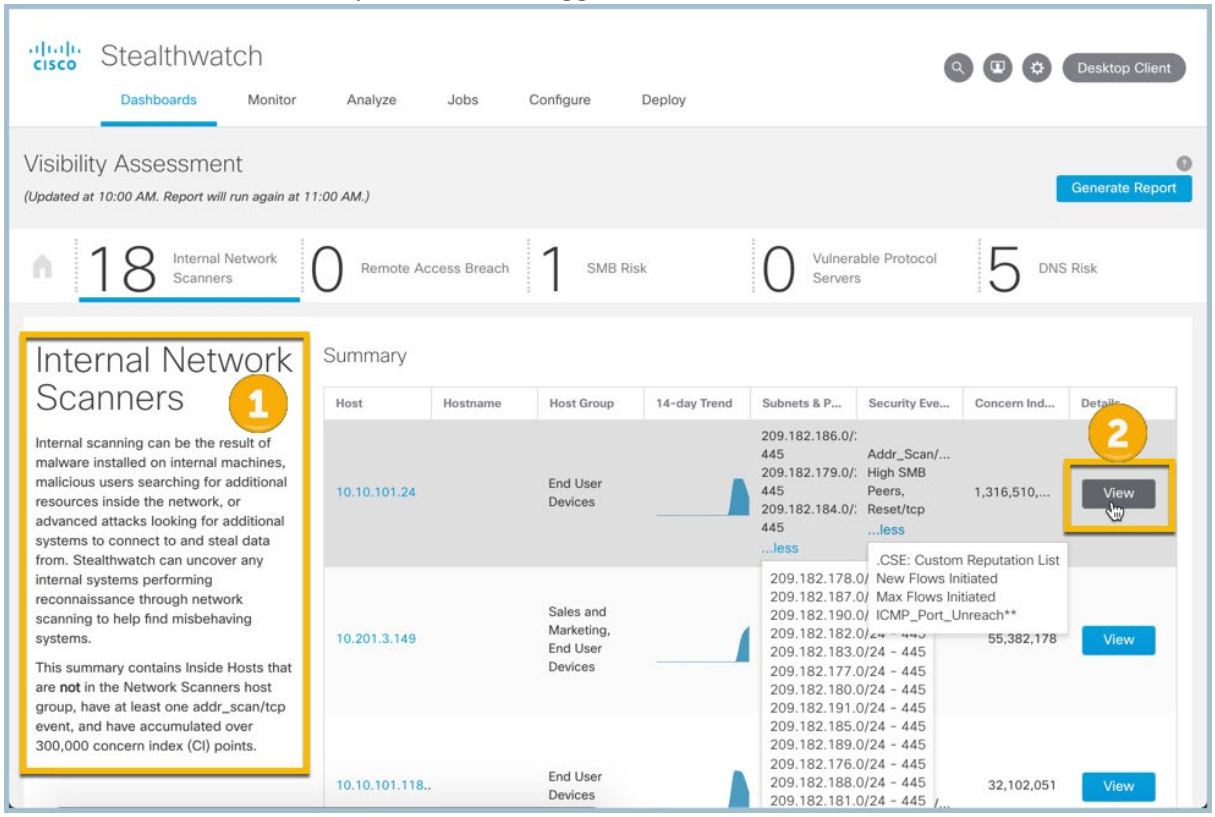
1. Select the online help by clicking the ? above the Generate Report button. Read the details of how this app may be used to detect internal scanners and other risk.
2. When first installing the app, you will need to select the gear icon above the map to define which countries your organization finds suspicious. This is useful in analyzing historical flow to find threats. You can select countries your organization does not do business in. After 14 days you will receive a report of suspect traffic to investigate.
3. Look at the amount of flow history that will be stored based on the current flow collection rate and amount of disk assigned.
4. Click the "Internal Network Scanners" to review a list of host scanning inside the network.



Phase 3: Classify Known Scanners

Within the Internal Network Scanners report:

1. Read the description of what is being detected through this report.
2. Investigate each IP by clicking View to understand which subnets and ports are being scanned, what security events have triggered, and when the behavior started.

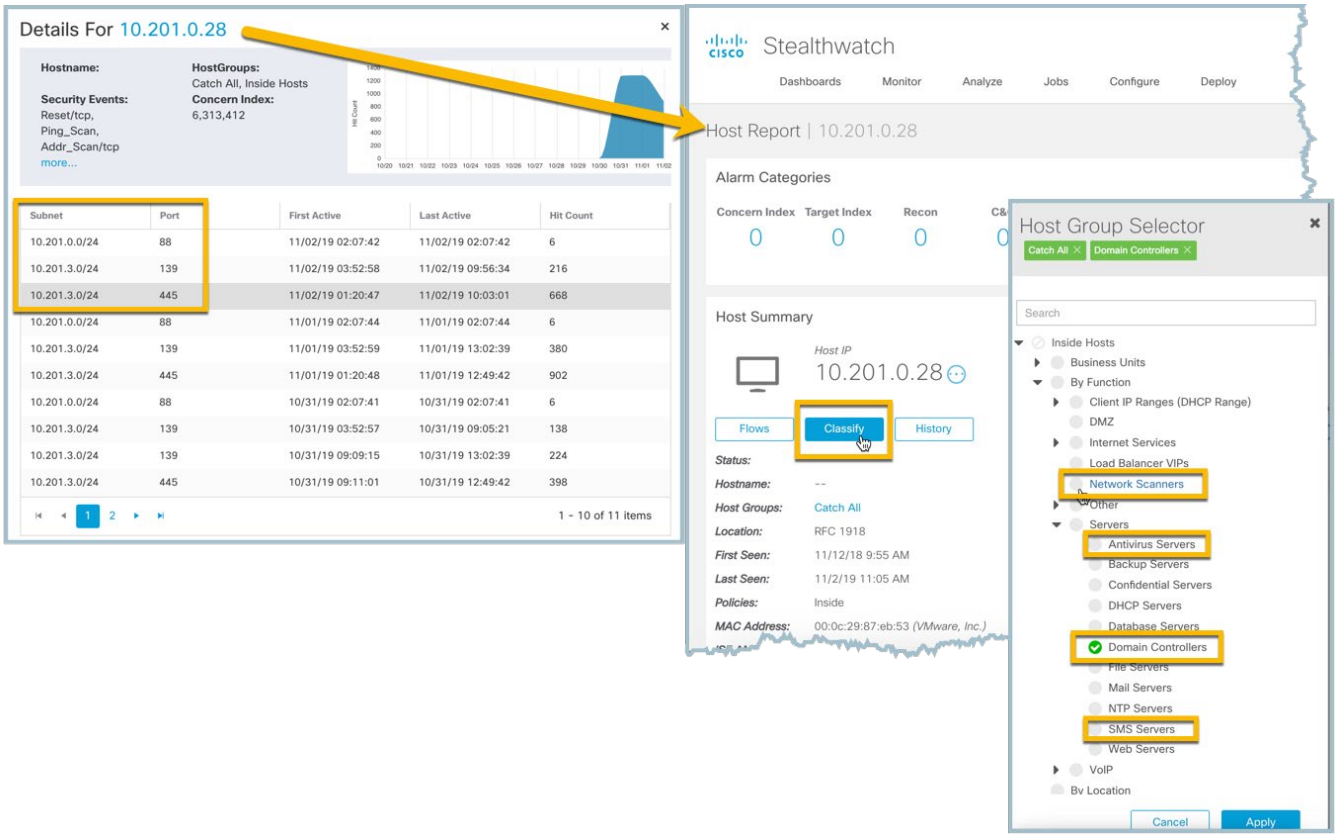


The following hosts will exhibit scan behavior based on communicating with many hosts on the network. Use host names to help determine the type of server. All of the below common server types already have an appropriate Role Policy defined. You simply need to classify the host in its respective By Function group:

- Vulnerability scanners
- Antivirus Servers
- SMS Servers
- DHCP Servers
- Domain Controllers

Phase 3: Classify Known Scanners

In the below example, 10.201.0.28 is communicating on Kerberos (port 88), NetBIOS (port 139) and SMB (port 445) as an authorized domain controller. Simply click the details for hyperlink, select the Classify button within the host report, and assign the host to its respective host group. In this example the host is a domain controller. The primary servers you will want to classify are authorized network scanners, management servers, SMS server, and antivirus servers. You may find host scanning that are already infected with malware and should be investigated.



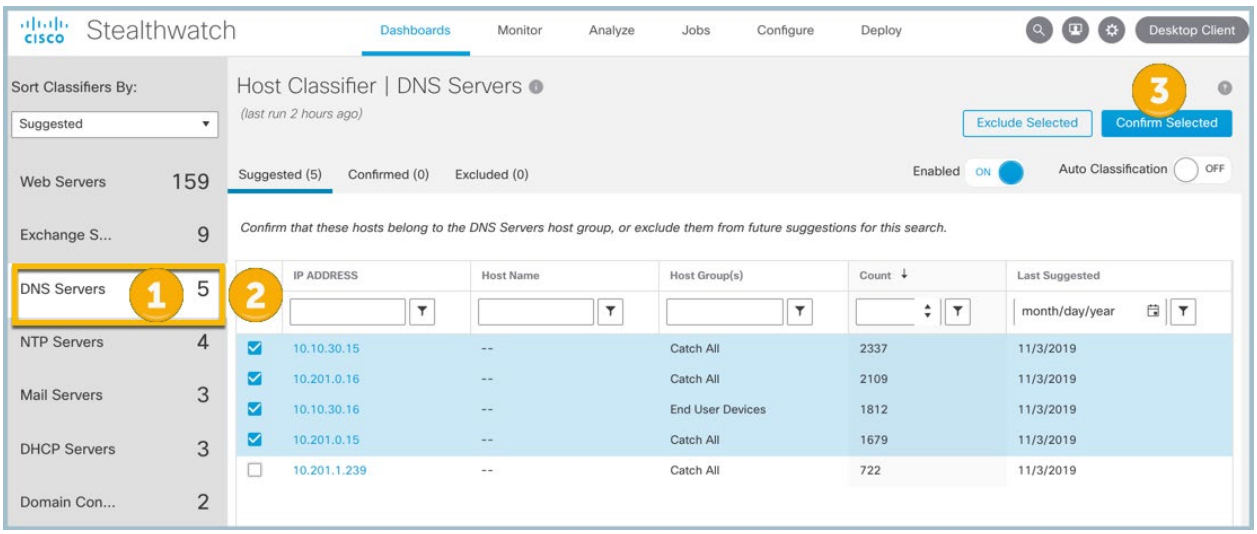
Note: The Visibility Assessment app will display results from the last 14 days each time you display the report. The host you may have classified will remain in the report until they age out after 14 days or you can uninstall and reinstall the app after initial tuning to quickly remove the host and start a fresh report.

Phase 4: Classify Known Common Server Types

Use the Host Classifier app to quickly classify known server types.

- Download the Host Classifier app through https://stealthwatch.flexnetoperations.com and install through Central Manager on your Manager (formerly known as the Stealthwatch Management Console).
- Once the app has been installed, launch Host Classifier from the Dashboards menu and open the online help by clicking the ? in the top right of the report. Read the details of how this app may be used to classify servers.
- The Web Servers and Exchange Servers are informative but primarily focus on classifying DNS, NTP, Mail, DHCP Servers, and Domain Controllers which can generate many alarms until properly classified.

1. Start with DNS Servers by selecting it from the list on the left.
2. Place a check next to each server that is an authorized DNS Server. Use host names to help determine the type of server.
3. Once you checked the authorized DNS Servers, select Confirm Selected, which will assign these hosts to the DNS Servers host group with a proper role policy assigned.



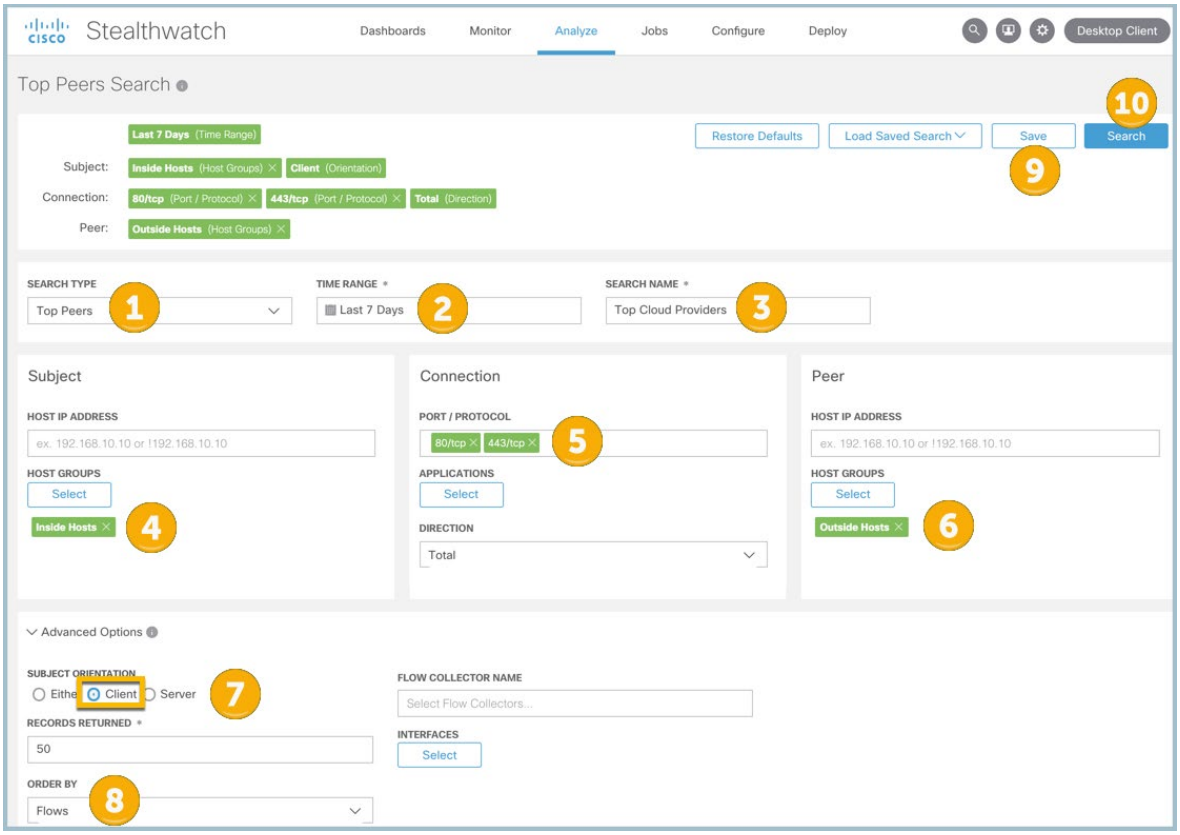
- Repeat the above classification for NTP Servers, Mail Servers, DHCP Servers, and Domain Controllers.
- You can use the Host Classifier app at any time a new collection of exporters are added to the deployment.

Phase 5: Classify Cloud Providers

Classifying common Internet providers within the Business Partners or Trusted Internet Hosts Outside Hosts groups will allow you to reduce unnecessary alarms caused by repeated traffic that is not a threat. As an example, it is very common to see Facebook as one of the top cloud providers with many employees spending a lot of time on Facebook. This exercise will often uncover suspect traffic as well that should be investigated.

Use the Top Peers report to find a list of common cloud providers for the organization. Navigate to Analyze, Flow Search and define the filter listed below:

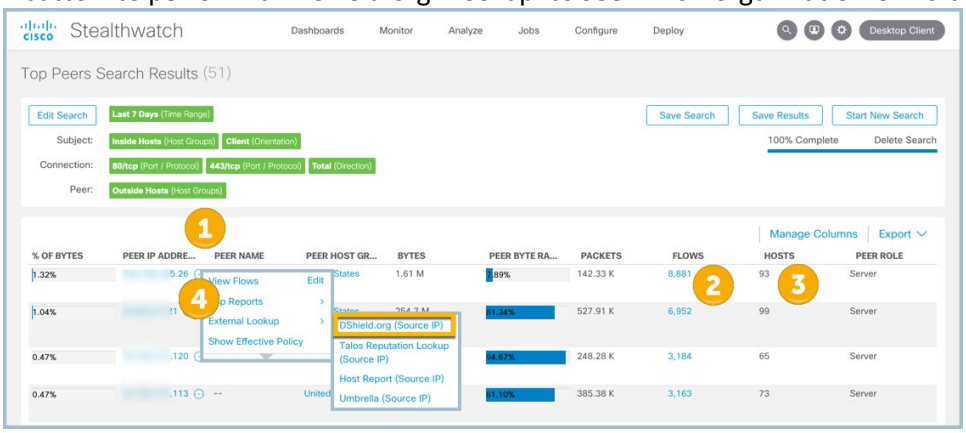
1. Select Top Peers for the Search Type.
2. Select Last 7 Days for Time Range.
3. Type "Top Cloud Providers" for the Search Name.
4. Select Inside Hosts as the Subject.
5. To focus on web traffic initially, type 80/tip for the Port/Protocol and press Enter. Type 443/tcp and press Enter.
6. Select Outside Hosts as the Peer.
7. Select Client for the Subject Orientation.
8. Select Flows for Order By.
9. Select Save to be able to use this report at a later time.
10. Select Search.



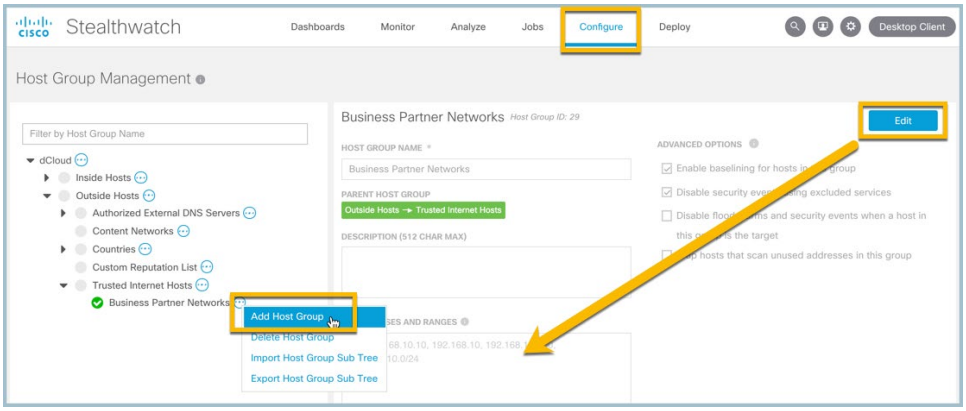
Phase 5: Classify Cloud Providers

The following alarms could trigger between Inside and Outside hosts: Suspect Data Loss, Suspect Long Flow and Beaconing Hosts. Using the output of this report, begin reviewing and classifying common networks for which you do not want to see these alarms.

1. Investigate the peer IP and host names to determine if this will be common traffic.
2. Identify the number of flows to these peers.
3. Identify the number of inside clients connecting to these peers.
4. Use the action button to perform a "DShield.org" lookup to see which organization owns this IP space.



- If you determine the traffic is authorized, capture the full CIDR network range owned by the outside peer from a "who is" lookup.
- Open Configure, Host Group Management and Add Host Group under Business Partner Network, or directly under Trusted Internet Hosts. Select Edit and paste in the full network ranges of the common peer network and save changes. This will inherit an appropriate policy to reduce false positives. Repeat this exercise after traffic has been collected for a couple weeks and any time a new group of exporters has been added to the deployment.

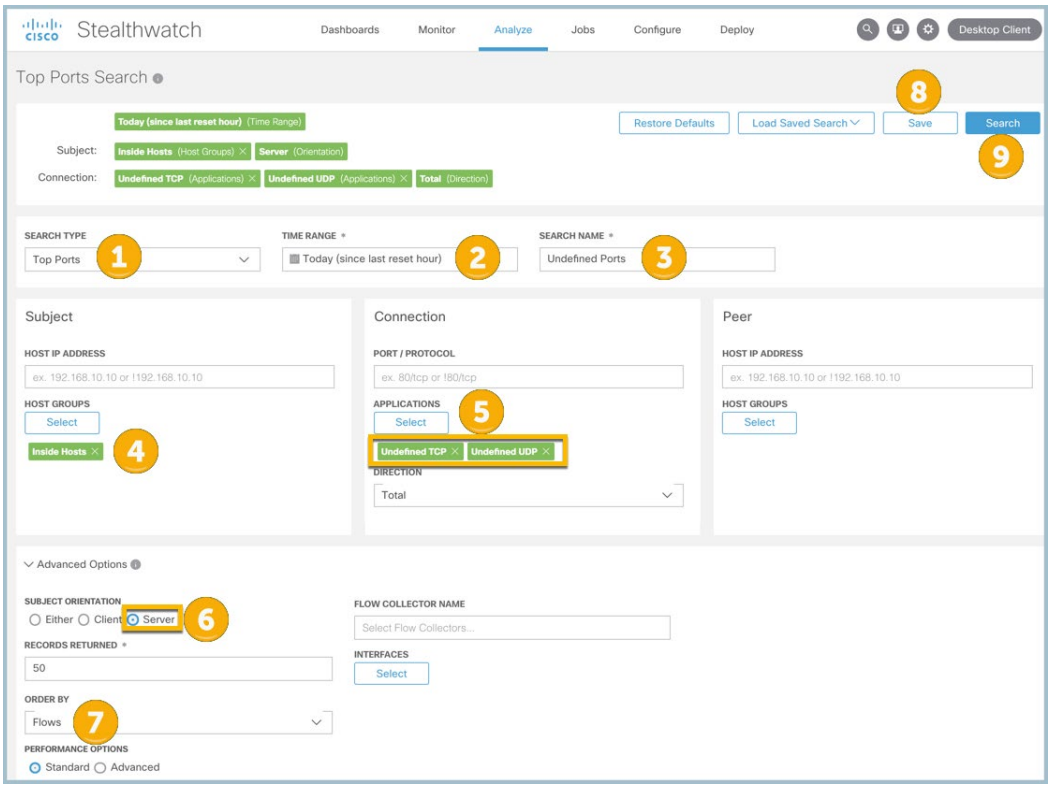


Phase 6: Classify Undefined Applications

There are hundreds of default applications already defined within Secure Network Analytics. However, every organization has custom services and applications running within their network. Classifying known applications for the organization helps the system become more intelligent around client/service determination which helps improve alarms.

Use the Analyze, Flow Search report with the below filters to identify top ports that are undefined:

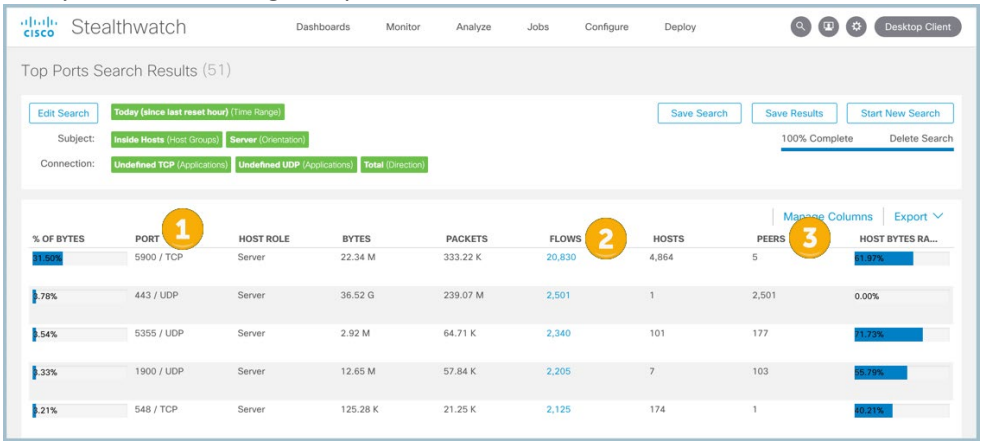
1. Select Top Ports for the Search Type.
2. Select Today for Time Range.
3. Type "Undefined Ports" for the Search Name.
4. Select Inside Hosts as the Subject.
5. Select Undefined TCP and Undefined UDP from the Applications list.
6. Select Server for the Subject Orientation.
7. Select Flows for Order By.
8. Select Save to be able to use this report at a later time.
9. Select Search.



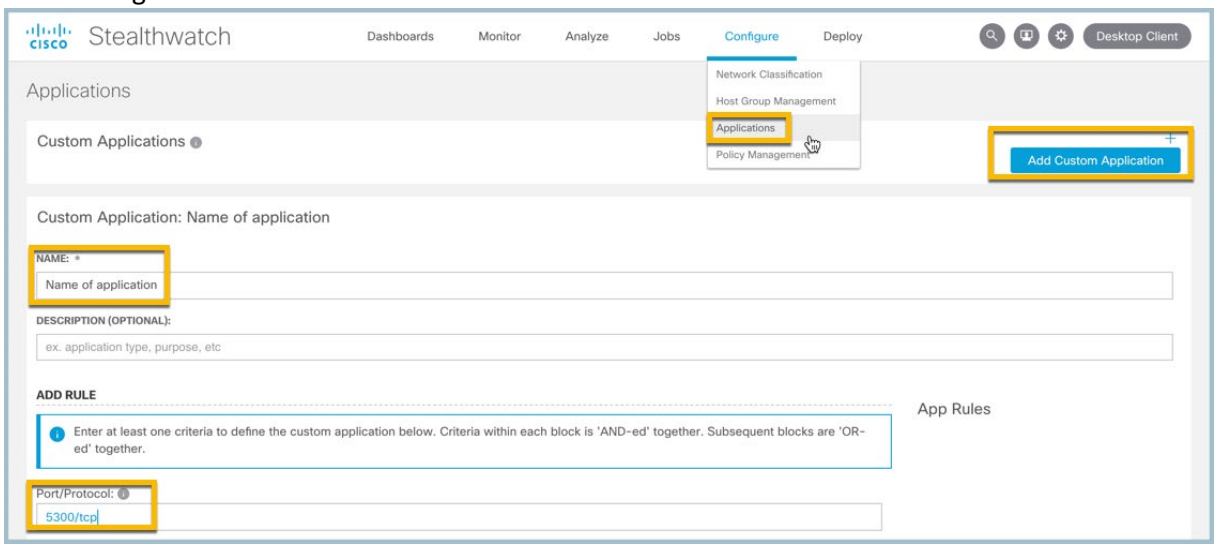
Phase 6: Classify Undefined Applications

Review the list of undefined applications to learn:

1. Which port is being used.
2. How many flows were observed.
3. How many clients are using this port.



- For each port that should be labeled, navigate to Configure > Applications.
- Select Add Custom Application.
- Provide a name and description for the application.
- Define the port associated with the application.
- Save changes.



- Repeat the above process to classify Undefined Applications.
- You do not need to perform this for every undefined port; you need only classify the common ports used within your network.