Cisco Secure Network Analytics Customer Test Drive 7.3.0

About this lab

This guide for the preconfigured demonstration includes:

Requirements

About this solution

Lab 0. Validate Wkst1
Lab 1. Remote access breach using stolen credentials
Lab 2. Monitor trusted third-party and VPN access
Lab 3. Analyze historical traffic to identify threats from suspect countries
Lab 4. Data hoarding
Lab 5. Use data exfiltration to track inside and outside hosts
Lab 6. Detect internal Telnet traffic
Lab 7. Detect suspicious SMB traffic
Lab 8. Network segmentation violations
Lab 9. Detect traffic to rogue DNS servers
Lab 10. Use ETA for compliance and malware detection
Lab 11. Public cloud monitoring and threat protection

Appendix A. Integrate Splunk using the Secure Network Analytics App
Appendix B. About NetFlow & IPFIX

What’s next?
## Requirements

The table below outlines the requirements for this preconfigured demonstration.

<table>
<thead>
<tr>
<th>Required</th>
<th>Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop with network capabilities</td>
<td>Cisco AnyConnect®</td>
</tr>
<tr>
<td>A Cisco.com account. Register <a href="#">here</a> if you do not already have an account.</td>
<td>Second device for reading lab notes</td>
</tr>
</tbody>
</table>
About this solution

Welcome to the Cisco Secure Network Analytics Customer Test Drive 7.3.0 dCloud (Demo Cloud) Test Drive Labs! This lab will show in real-time traffic how Cisco Secure Network Analytics (formerly named Stealthwatch) is the leader in the Network Detection and Response (NDR) Gartner quadrant and can transform the network into a sensor to detect insider threats and identify anomalous behavior such as malware, distributed botnets, data exfiltration, and more. You get hands-on access to a fully configured environment with traffic that you generate to test first-hand live use cases including:

- Breach Detection
- Insider and Advanced Threat Detection
- High Risk Application Detection
- Policy Violations
- Encrypted Traffic Analytics
- Public Cloud Monitoring

In this lab, you play the role of an attacker generating traffic, and then you log in to Secure Network Analytics as a defender to learn how to respond to these attacks. Completing these labs will help provide experience and test plans to effectively use and operationalize Cisco Secure Analytics (Stealthwatch). Everything learned in these labs can be carried over into a production deployment.
Disclaimer

This lab should be running for at least 1 hour before performing exercises. For best results let the lab run for at least 24 hours before starting exercises.

dCloud is a powerful lab environment for education purposes. There are often thousands of different types of labs running simultaneously. To allow for more labs to run within the dCloud datacenters, resources are shared across labs which could cause slower than normal response times during heavy usage.

Secure Network Analytics requires reserved resources of RAM and CPU in production deployments. Within these labs we do not have the RAM and CPU reserved. Please note: any slowness in queries or detection could be caused because of this so allow extra time for results.

It may take:

- Flow records 1-2 minutes after generating traffic to appear in Secure Network Analytics
- Events will appear 5-30 minutes after traffic is generated.
About This Test Drive Lab

The Cisco Secure Network Analytics Test Drive has been built as a training platform to gain first-hand experience to understand and setup Secure Network Analytics. Students get to experience life-like cyber security attack situations in a virtualized enterprise lab environment, playing the role of an attacker and defender. Using an environment like many enterprise networks, students will learn and understand how their own environments get compromised, how security breaches get detected, and how to respond using Secure Network Analytics.

Topology

This lab includes preconfigured users and components to illustrate scripted scenarios and features of Cisco Secure Network Analytics. Most components are fully configurable with predefined administrative user accounts. You can see the IP address and user account credentials to access a component by clicking the component icon in the Topology menu of your active session and in the scenario steps that require their use.

You will use the same topology, accounts, and IP addresses so refer to those sections during later labs as needed.
Accounts and Passwords for this dCloud Lab

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
<th>Endpoint Devices</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>wkst1\Administrator</td>
<td>Cisco12345</td>
<td>Workstation1</td>
<td>198.19.30.36</td>
</tr>
<tr>
<td>admin</td>
<td>Cisco12345</td>
<td>Management Console</td>
<td>198.19.20.136</td>
</tr>
<tr>
<td>admin</td>
<td>Cisco12345</td>
<td>Flow Collector</td>
<td>198.19.20.137</td>
</tr>
<tr>
<td>admin</td>
<td>Cisco12345</td>
<td>Flow Sensor</td>
<td>198.19.20.138</td>
</tr>
<tr>
<td>admin</td>
<td>Cisco12345</td>
<td>UDP Director</td>
<td>198.19.20.139</td>
</tr>
<tr>
<td>admin</td>
<td>Cisco12345</td>
<td>Remote Workstation</td>
<td>198.18.1.36</td>
</tr>
<tr>
<td>admin</td>
<td>Cisco12345</td>
<td>Splunk</td>
<td>198.19.20.140</td>
</tr>
<tr>
<td>root</td>
<td>Cisco12345</td>
<td>CDS</td>
<td>198.19.20.134</td>
</tr>
<tr>
<td>admin</td>
<td>Cisco12345</td>
<td>CSR</td>
<td>198.19.10.2, 198.19.20.1, 198.19.30.1</td>
</tr>
<tr>
<td>admin</td>
<td>Cisco12345</td>
<td>ASAv</td>
<td>198.19.10.1, 198.18.133.100</td>
</tr>
<tr>
<td>dcloud\administrator</td>
<td>Cisco12345</td>
<td>AD1</td>
<td>198.19.20.10</td>
</tr>
<tr>
<td>root</td>
<td>Cisco12345</td>
<td>Attacker_desktop</td>
<td>198.19.20.6</td>
</tr>
<tr>
<td>admin</td>
<td>Cisco12345</td>
<td>WSA</td>
<td>198.19.20.51</td>
</tr>
<tr>
<td>admin</td>
<td>Cisco12345</td>
<td>ISE</td>
<td>198.19.20.141</td>
</tr>
<tr>
<td>admin</td>
<td>Cisco12345</td>
<td>Endpoint Concentrator</td>
<td>198.19.20.142</td>
</tr>
<tr>
<td>swcadmin</td>
<td>Cisco12345</td>
<td>SWC Sensor</td>
<td>198.19.20.143</td>
</tr>
<tr>
<td>admin</td>
<td>dCloud1231</td>
<td>Cisco Telemetry Broker (CTB)</td>
<td>198.19.20.53</td>
</tr>
<tr>
<td>admin</td>
<td>Cisco12345</td>
<td>Network Forensics Appliance (NFA)</td>
<td>198.19.20.135</td>
</tr>
</tbody>
</table>
Get started

This lab enables you to become familiar with dCloud. It walks through connecting, validating the machine you will be connecting to in the data center, and ensuring that Secure Network Analytics is up and available.

2. Select My Hub, as shown below.
3. Select View for Cisco Secure Network Analytics Customer Test Drive 7.3.0 session.

![My Hub Session](image)
Lab 0. Validate Wkst1

At the end of this section, you will have access to the lab environment, mapped to the resources you will need. Let’s begin.

1. Select Servers to view the servers running for this lab. The Servers tab displays all the systems running with the lab environment.
   Note: You can turn systems on or off, if needed, from this location.

2. To work in this lab, you will need to access Wkst1, which gives you access to all data center resources. Click the Remote Desktop link to launch a web Remote Desktop session built within dCloud.
Validate Wkst1 - ipconfig

Wkst1 will be the remote desktop session within the datacenter you use. Let’s validate the IP address of your Wkst1.

Refer to the figure below, as you follow these steps:

1. From the Wkst1, open cmd.exe from the desktop.
2. Type ipconfig, and then press Enter.
3. Validate the IP address of your Wkst1 is 198.19.30.36.
4. Make note of this IP address, because you will use it in most labs.
Validate Wkst1 – Install Tor Browser

To generate traffic and validate results, you will install the Tor browser. All network traffic generated by the Wkst1 will be accounted for by NetFlow records, stored as a network audit trail and used to detect threats east and west inside the network and north and south to the Internet. Refer to screenshot shown below.

1. Open Chrome from the desktop of the Wkst1, and then open https://www.torproject.org/download using the bookmark in Chrome.

2. Click the Windows Sig to Download Tor install file.

**Note:** We want to download Tor as part of the lab to capture NetFlow data. If the download is slow due to class volume you will find the downloaded .exe within the “Downloads\lab content” folder on Wkst1 so you can install from there.

3. Install torbrowser-install.exe using all default settings. As you install, make note of the file size of the .exe download which is ~54 MB; you will search for this in an upcoming lab.
4. From your desktop, click Start Tor Browser, click Connect when Tor launches, and then search for “what is flexible netflow,” as shown below.

   a. Review a few articles and perform other searches to generate traffic through the Tor network.
   b. Keep Tor Browser open for the next exercise.

   **Note:** Everything being searched through Tor is encrypted through the browser.
Validate Wkst1 - netstat

This lab will use the netstat (network statistics) command line tool to display incoming and outgoing network connections from Wkst1. It will also show that those connections will be accounted for through NetFlow. You are using netstat to see what connections exist to validate being able to search Secure Network Analytics for any active or historical network conversations.

Launch cmd.exe from the Desktop by right-clicking and Run as administrator, and type:

```
netstat -bn | findstr /v 127 | findstr /v exe
```

**Note**: netstat will not run unless you run cmd.exe as an administrator.

The ‘-n’ is needed so the system does not perform name resolution. This enables you to see the Foreign IP address to which you are connecting. The ‘-b’ will display process name. The findstr /v command will filter the results to display less information as shown below. Make note of the Foreign IP addresses being connected to. You will be able to search Secure Network Analytics for historical network conversations to and from the WKST1 IP address.

**Tip**: Leave the command prompt open for later use.
Validate Wkst1 – Flow Search

The Wkst1 IP address has been validated and the connections established. You will query Secure Network Analytics to become comfortable with how NetFlow is collected. A later lab will provide a deeper understanding of NetFlow.

1. If not open, launch Chrome from the desktop of your Wkst1.
2. Select the SMC (WebUI) bookmark from the Appliances folder of the bookmark toolbar.
3. Log in with username admin and password Cisco12345

4. Select Analyze > Flow Search from the menu bar, as shown below.

The top portion of the Flow Search window will show the filter criteria. Make sure to define the filter exactly as defined below.

1. Select Last 8 Hours for the Time Range.
2. Enter the Subject host IP Address using the WKST1 IP address of 198.19.30.36, and then press Enter.
3. Type 443/tcp in the Port/Protocol Connection, and then press Enter for the selection to take effect). Note: that we are limiting the flow query to encrypted https or 443/tcp connections.
4. Within the Peer section, click Select under Host Groups and select Outside Hosts then click Apply. Outside hosts represent any IP address on the Internet.
5. Click **Search** to begin running the flow query of any connection in the last 8 hours between WKST1 and the Internet using https or 443/tcp, as shown below.

Let’s find the flow associated to the previous lab where you downloaded the ~54 MB Tor.exe file. 

1. In the **Total Bytes** header row, type **>50M** to filter the results to only display flows that were greater than 50 MB of data exchanged, shown below. You may need to scroll to the right from the scroll bar at the bottom of the browser window or unzoom your browser to see the Total Bytes column.

2. Select the **toggle button**, shown below, to display a quick view of the flow records.
The flow table results should resemble the screenshot shown below.

1. Scroll through the flows. You should see a flow between your Wkst1, **198.19.30.36**, as the subject connected to an Internet facing peer.

2. In the search below, the ~54 MB download was with **82.195.75.101** out of Germany over https. **Note:** The peer IP address may be different from when you downloaded your Tor executable.

3. Notice the **MB size** coming down from the peer to your Wkst1.

4. Click the **black triangle** to expand context and details of the conversation.
1. Select the **toggle button** as shown below to show a table view of the flow records.
2. Click the **X** to remove the Total Bytes filter and show all flow results.

With the filters removed:

Select **Manage Columns > Subject > check mark Subject NAT > Set**
NAT stitching is a unique capability leveraging perimeter devices. The system works together with these perimeter devices, and can correlate internal and external IP address information as shown below:

1. **Scroll down** to the bottom of the flow table.
2. **Scroll right** and take notice of the list of Peer Hosts. These Peer hosts should match the Foreign Address your Workstation was connecting to in the above labs creating a complete network audit trail of network connectivity.
Filter the flow table by one of the Foreign IP addresses which begins with “:443” that you saw in the netstat lab.

1. In the **Peer IP Address** header row, enter an IP address you observed in your netstat lab above. The IP address may vary from what is listed in the figure below.

2. Select the **black triangle** on the left of one of the flows to view details, shown below. Make note of context written into a flow record.

3. Select the **toggle button** as shown below to show a quick view of flows.
Validate Wkst1 – SMC Host Group review

Let’s go through a brief review of asset grouping called Host Groups within Stealthwatch to give you a basic understanding on applying more granular threat detection and behavioral analytics.

1. Within the SMC, navigate to **Configure > Host Group Management**
2. You will see a tree structure listed. Highlight **Catch All** as shown below.
3. Select the **Edit button** as shown below.
4. Highlight **198.19.30.37-198.19.255.255** and hit Delete on your keyboard to remove this range from the group.
5. Select **Save** as show below.

Reference the tree structure as we describe the basics of Host Groups. Host Groups offer flexibility in the way you can organize hosts or assets within your organization. In general, hosts can belong to multiple groups allowing you to apply your own business logic. In addition, you can define policies per host group and/or per host. A host group is essentially a virtual container of multiple host IP addresses or IP address ranges that have similar attributes, such as location, function, or topology. By grouping hosts into host groups, you can control how the Stealthwatch Flow Collectors monitor and respond to the behavior of those hosts as a group, rather than individually.

In the steps above we had you remove a group of IP addresses from the “Catch All” group.

The Catch All group in Stealthwatch performs a special function within the product. The contents of the Catch All group establish what IP addresses a company utilizes, owns, or otherwise controls. By default, this includes all private IPv4 and IPv6 address space. What should be added to the Catch All group is all the customer’s public IP address space. We had you remove a group of public IP space that is part of this lab, but we want to treat them as outside for the remainder of the exercise. In a later lab you will see how host group automation takes place.
By default, each SMC domain contains the following top-level host groups to which you can add sub host groups for easier reporting and more focused behavioral analytics:

1. **Inside Hosts** – Contains all host groups whose hosts have been specifically defined as being a part of your network. Make note of example groups such as Compliance Systems, Protected Asset Monitoring, and Trapped Hosts – Honeypot.

2. **Outside Hosts** – Contains all host groups whose hosts have not been specifically defined as being a part of your network. Make note of the sub groups such as Authorized External DNS Servers, Countries, Customer Reputation List, and Trusted Internet Hosts.

3. (optional) **Command & Control** and **Tor** – These are optional feeds you can subscribe to for automated updates of new command and control servers and Tor entry and exit nodes.

**Summary**

In this **Validate Wkst1 lab**, you:

- Became familiar with Wkst1 to which you connected in the datacenter.
- Learned that all network conversations are accounted for from this machine through NetFlow collection.
- Learned how to run a basic Flow Search in Secure Network Analytics to see all https flow between your Wkst1 and the Internet (Outside Hosts).
- Learned the basics of what a Host Group is and editing the Catch All group.
Lab 1. Remote access breach using stolen credentials

According to a Ponemon Institute Cost of Data Breach Study of 419 companies in 13 countries, $3.62 million is the average total cost of a data breach. To help combat this, it is critical to try to account for 100% of network conversations to detect threats that bypass traditional monitoring solutions.

Review the supporting lab video overview here > https://cs.co/SWTestDrive-Lab1

About breach detection

To help get into the mind of an attacker, take a minute to review the persona of “Harry the Hacktivist” and how he operates. Understanding the attacker can help you build solutions to defend your organization.

Using the image below, ensure you are collecting full NetFlow somewhere along the path between the attacker and victim IP.
Test Drive Objectives

In this test drive, you will see first-hand the importance of capturing flow data from as close to the endpoints as possible to be able to account for all active and historical network conversations.

Test Drive Requirements

- Stealthwatch Management Console (SMC) any version
- Stealthwatch Flow Collector any version
- Any version of NetFlow from within the network

Test Drive Outline

1. Task 1. Connect to a server running Remote Desktop within a datacenter
2. Task 2. Download an exploit-kit and perform reconnaissance
3. Task 3. Install exploit-kit
Task 1: Connect to a Remote Desktop server within a data center

Below is a list of realities of why you need to build stronger defenses beyond access control lists or firewalls:

- Firewalls are as good as the person implementing them, mistakes happen.
- If the access control policy is misconfigured and any rule is moved to the top, how would you detect this before?
- Detect threats when an authorized server is used with stolen credentials.
- Account for all traffic on the inside of the firewall so you can build a general ledger of both authorized and non-authorized traffic making it through the firewall and provide a second chance detection.

Scenario: You have been performing reconnaissance against an organization and have identified a remote desktop server that is exposed to the Internet. You have discovered the below credentials to the server and begin building a foothold inside the organization. In this lab, you will need to access Wkst1, which gives you access to all data center resources.

Note: If Remote Desktop is already up, move to Task 2.

Otherwise, click Remote Desktop link to launch a web Remote Desktop session built within dCloud shown below.

Note: Username = wkst = Administrator. Password = C1sco12345.

You are now inside the organizations data center by leveraging a server exposed to the Internet and using stolen credentials!
Task 2: Download an exploit-kit and perform reconnaissance

Now that you are inside the data center, let’s download some tools to make it easier to build a foothold and begin breaching the organization further. One of the first phases of any attack is reconnaissance. Various open source tools are available to attackers. In order to break the Cyber Kill Chain, detection tools must be able to identify when this type of attack is occurring.

We are going to find targets to connect to through scanning activity and attempt to identify vulnerabilities in the target network.

1. From Wkst1, open the Downloads folder within Windows Explorer and double-click the git-material.sh script.
2. Open the lab-exploit-kit folder double click on recon.bat which will search for common management ports (22 = ssh, 23 = telnet, and 3389 = Remote Desktop).
3. The recon.bat will pause so you can see the below nmap scan is what is running. Press any key to continue the scan.

   nmap -n -v -Pn -sS -p 22,23,3389 198.19.20.0/24 --disable-arp-ping

**Note:** The scan could take over 5 minutes to complete. When complete, you will see results like those shown in the screenshot below.
2. Make note of the number of hosts scanned and scroll through to see what hosts are listening on given ports. You will see the host 198.19.20.134 as one of the results listening on SSH 22/tcp. This will be the host in the next lab that is compromised.

What does the nmap commands mean?

- **-n**: Tells Nmap to *never* do reverse DNS resolution on the active IP addresses it finds. Since DNS can be slow even with Nmap's built-in parallel stub resolver, this option can slash scanning times.

- **-v**: verbose meaning shows the contents on the screen.

- **-Pn**: (no ping) This option skips the Nmap discovery stage altogether. Normally, Nmap uses this stage to determine active machines for heavier scanning. By default, Nmap only performs heavy probing such as port scans, version detection, or OS detection against hosts that are found to be up. Disabling host discovery with -Pn causes Nmap to attempt the requested scanning functions against every target IP address specified.

- **-sS**: This is the most popular scan type because it the fastest way to scan ports of the most popular protocol (TCP). It is stealthier than connect scan, and it works against all functional TCP stacks (unlike some special-purpose scans such as FIN scan).

- **-p**: Port scan on multiple ports. In this case ports 22, 23 and 3389

--**disable-arp-ping**: Nmap normally does ARP or IPv6 Neighbor Discovery (ND) discovery of locally connected Ethernet hosts, even if other host discovery options such as -Pn or -PE are used. To disable this implicit behavior, use the --disable-arp-ping option.

The default behavior is normally faster, but this option is useful on networks using proxy ARP, in which a router speculatively replies to all ARP requests, making every target appear to be up according to ARP scan.

**Task 3: Install exploit-kit**

Let’s SCP and install the exploit-kit on one of the servers identified during the network scan.

1. Open **WinSCP** from the Desktop as shown below. **Note:** If an update appears, ignore the update.
2. Select CDS (which is one of the servers identified in the previous scan) as shown below.

3. Select Login and if a password box appears insert Cisco12345 for the password.

5. Within the left panel of WinSCP, browse to c:\Users\Administrator.WKST1\Downloads\lab-exploit-kit on the left-hand navigation pane, as shown below.

6. Highlight install-exploit-kit.sh and install-exploit-kit.tar

7. Drag and drop install-exploit-kit.sh and install-exploit-kit.tar within root in the right pane, as shown below.

8. Close WinSCP when the transfer is complete.
9. From the Wkst1 desktop, open Putty and use the CDS session to SSH into 198.19.20.134 (which is the server we installed the exploit-kit on) with username root.

10. Enter the password Cisco12345 when prompted in the Putty session window.

11. Once logged in, enter pwd to make sure you are in the root directory. This is where you placed the exploit files.

12. Run the “./install-exploit-kit” command, as shown below to install the tools used to create a foothold within the organization.

13. Run ls -l and make note that the exploit kit has captured a customer database with the name encrypted-customer-DB. You can exit out of the SSH session.
Task 4: Investigate security events generated in Secure Network Analytics

Secure Network Analytics will have stored flow records for all north-south and east-west connections to the Remote Desktop server and detected the attack traffic that was initiated in the previous labs. While not covered in this document, you could have also received an alert via email or a syslog message to your SIEM as the attack was unfolding.

1. **Return to the SMC WebUI.** If you need to reopen the SMC, use Chrome from the WKST1 remote desktop session and select the SMC (WebUI) form the Appliances bookmark folder. Login with username admin and password Cisco12345.

2. **Type the IP address of WKST1 in the search window, by selecting the magnifying glass in the top right hand corner. Insert 198.19.30.36, and press enter as shown below.**

3. **Make note of the high percentages under the below categories.**
   a. The categories are like reputation scores that show the host is a Concern, for it is exceeding the normal level of Concern and Reconnaissance for this host.
   
   - CI = Concern Index
   - RC = Reconnaissance

4. **Click the IP address 198.19.30.36 to open the Host Report.**
Investigate the following sections within the Host Report for 198.19.30.36 as shown below.

1. The row across the top shows the alarm categories that have triggered: **Concern Index** and **Recon**.
2. **Host Summary** will display the status, hostname (if applicable), Host Groups, seen dates, allow you to apply Adaptive Network Control Policy to the host with the Identity Services Engine (ISE), and/or select Flows to investigate the host further.
3. **Traffic by Peer Host Groups** will provide a visual of flows east-west to other internal hosts (on the left) and north-south to hosts on the Internet (on the right.)
4. **Alarms by Type** will display alarms triggered in the past 7 days.
   a. Make note of the “**CSE: Possible Remote Access Breach**” and “**Addr_Scan/tcp**” alarms.
   b. The CSE is a custom security event setup to alarm any time an outside host successfully connects inside the network over a remote access protocol like RDP. CSEs can be setup to help audit and detect segmentation policy violations.
5. Scrolling down the page and observe that the **Top Security Events** section will illustrate any security event this host was engaged in as the Source or Target. Notice the Addr.Scan events with the targeted port and target hosts. These events generated from the reconnaissance scans in the previous lab, as shown below.

6. The **Users & Sessions** section will display user information gathered from ISE such as MAC address, device type, and logged in username.

7. The Application Traffic **Internal** will display the top application usage trends for this host within the network.

8. The Application Traffic **External** will display the top application usage trends for this host to the Internet.
9. Scroll back up on the host report and click the alarm type of .**CSE: Possible Remote Access Breach** as shown below.

**Note:** It is easier to “Deselect All” below the legend of the Alarms by Type and just select .**CSE: Possible Remote Access Breach** to make it easier to select the desired alarm.

This will pull back a list of alarms as shown below.

1. The **Source Host Groups** that connected. Hover over the name and you will see the host in coming from Outside Hosts > Countries > Other > Unknown.
2. The **Source** host that connected.
3. The **Target** host (the Remote Desktop Server you are connected to.)
4. Select the **Actions** circle.
5. Click **View Flows** and run a flow query to investigate further.
Explore more within the interface and select the context sensitive Secure Network Analytics Help on various screens shown below. The context sensitive help will assist in explaining the information displayed on various reports.

**Summary**

Within this test drive, you learned:

- How to generate traffic crossing a NetFlow exporter that will cause Secure Network Analytics alarms to trigger.
- How to investigate using Secure Network Analytics for reconnaissance alarms and other security events.
Lab 2. Monitor trusted third-party and VPN access

It is important to monitor third-party and employee VPN access to better protect your organizations intellectual property and customer data. When threats are detected, it is critical to be able to provide rapid threat containment.

Watch the supporting lab video overview here > https://cs.co/SWTTestDrive-Lab2

Test Drive Objectives

This lab will familiarize you with the Network Visibility Module and its integration with Secure Network Analytics along with rapid threat containment using ISE. AnyConnect is not just a VPN Client anymore and has not been for quite some time with its modular approach to providing security services. In this lab, we will focus on the Visibility provided by AnyConnect and ISE for threat containment.

Test Drive Requirements

- Stealthwatch Management Console (SMC)
- Stealthwatch Flow Collector
- Cisco Identity Services Engine (ISE)
- AnyConnect 4.2 or later
- Any version of NetFlow meeting the minimum supported fields mentioned in the NetFlow lab.

Test Drive Outline

Task 1. Gain visibility into user and endpoint behavior with the NVM Module
Task 2. Initiate attack traffic
Task 3. Block host with ISE ANC
Task 1: Gain visibility into user and endpoint behavior with NVM

AnyConnect Secure Mobility Client increases visibility and control across the extended network, preventing compromised endpoints from gaining access to critical resources. In this lab we will be observing:

- Visibility into user and endpoint behavior with the Network Visibility Module (NVM)

Cisco AnyConnect NVM leverages the Network Visibility Flow, or nvzFlow (pronounced: en-vizzy-flow) protocol to capture user and endpoint behavior both on and off-premise. The job of nvzFlow is to collect flows from endpoints, along with a small set of high-value data related to each flow originating from the endpoint in a lightweight manner in standard IPFIX records. This empowers flow collection solutions to leverage this rich data to create visibility into user and endpoint behavior and as well as long term trending and analytics.

The five key visibility categories conveyed by the protocol or Enhanced Context are:

- User
- Device
- Application
- Location
- Destination

1. From [https://dcloud.cisco.com](https://dcloud.cisco.com), My Hub, Sessions, click View for the Cisco Secure Network Analytics Customer Test Drive 7.3.0 lab and log into the Remote Workstation as shown below.

2. Once logged into the remote workstation an AnyConnect client should pop up as shown below:

3. Select Connect and login with username employee and password: C1sco12345.
4. You should see the below stating the connection has taken place

**Figure 1.** AnyConnect Successful Login

Open the **command prompt** from the Desktop of the remote workstation and perform an **ipconfig**.

1. Pay attention to the IP address for Ethernet 2 as shown below which should be **198.19.10.100**.

   ![Command Prompt](image)

2. This IP address was assigned by the VPN connection and will be investigated within the lab.

Employees and contractors regularly take their laptops home to work. While the laptop is protected on your organizations network, it is not protected on their home network. The employee not only does work on the laptop but browses the web as well.
Task 2: Initiate attack traffic

The attacker has installed malware on the remote PC to obtain valid user credentials. Next the attacker will use various tools to gain visibility into the network layout of the organization.

1. Once you have logged into AnyConnect, open up Zenmap from the desktop.
2. In the Target field of Zenmap insert the following command:
   ```
nmap -sS -v -n -Pn 198.19.20.0/24 --disable-arp-ping
   ```
3. While the scan executes read the following article:
4. Once the scan displays the ports for 198.19.20.10 cancel the scan as the attacker has the information, he/she needs to elevate privileges.
   a. The scan reveals an active directory server.
5. Open a command prompt and issue the following command: `ping -t 198.19.20.10`
6. Take note of the replies from the ping command.
Task 3: Block host with ISE ANC

1. Keep the remote_wkst tab open and select the dCloud architecture from the already open tabs within Chrome.
2. Remote Desktop into Wkst1 as shown below.

3. Open Chrome > select appliances from the Favorites menu and select SMC(WebUI).
4. The Security Insight Dashboard opens as shown below:
5. Observe the Top Alarming Hosts and the IP address of the Remote Workstation will appear as shown below:

```
<table>
<thead>
<tr>
<th>HOST</th>
<th>CATEGORY</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.101.24</td>
<td>PV CI SQ EP</td>
</tr>
<tr>
<td>10.10.101.46</td>
<td>PV</td>
</tr>
<tr>
<td>10.201.3.103</td>
<td>PV</td>
</tr>
<tr>
<td>198.19.10.100</td>
<td>CI NG</td>
</tr>
<tr>
<td>10.201.3.148</td>
<td>DH CI SQ</td>
</tr>
<tr>
<td>10.3.241.34</td>
<td>CI DH</td>
</tr>
<tr>
<td>10.241.0.18</td>
<td>CI NC</td>
</tr>
</tbody>
</table>
```

6. Select the IP address of **198.19.10.100** from the top alarming hosts to pivot into a host report as shown below:

```
Host Report | 198.19.10.100

Alarm Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Target Index</th>
<th>Recon</th>
<th>CAG</th>
<th>Expertation</th>
<th>DDoS Source</th>
<th>DDoS Target</th>
<th>Data Flowing</th>
<th>Calibration</th>
<th>Policy Violation</th>
<th>Anomaly</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Host Summary

User IP: 198.19.10.100

Traffic by Peer Host Group (last 12 hours)

```

7. At the top of the Host Snapshot Report we can see there are two alerts that are firing:
   a. The Concern Index and Recon
8. Scroll down to the security events and notice the Security Events (port scans) that attributed to this alert firing within Secure Network Analytics as shown below.

![Security Events Table]

At this point we have sufficient information to apply an Adaptive Network Control Policy through PxGrid and ISE.

9. From the Host Summary widget select the **Edit** from the ISE ANC Policy as shown below.

![Host Summary]

14. When the Applying ANC policy screen displays select **SW_Quarantine**.

![Applying ANC policy]

15. Select **Save**, and observe the policy applied to the host 198.19.10.100.
16. Access the remote_wkst tab in your browser and view the results of the ANC policy. The hosts VPN connection should have been disconnected and the ping packets are timing out.

Secure Network Analytics through PxGrid and ISE put this host in a remediation vlan until the security team has time to investigate the incident.

NOTE: In Secure Network Analytics 7.3.0 forward the ability to setup automatic ISE ANC response has been added.
Once there has been an investigation, the host can be put back on the network through Secure Network Analytics as shown below by editing the ANC policy to "No policy applied" and click save.

![Applying ANC policy](image)

10. Access the remote_wkst tab again and log into AnyConnect with the employee credentials of **Cisco12345**
11. Observe the pings have resumed as shown below.

```
% Command Prompt : ping 198.19.20.10
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
Reply from 198.19.20.10: bytes=32 time=1ms TTL=127
```

**Summary**

In this lab, you learned:

- The importance of accounting for all traffic from trusted 3rd party and VPN networks.
- How to detect threats hidden within trusted network connections.
- How to use the Top Alarming Hosts to find and threat and initiate an ISE ANC policy to block the hosts.
Lab 3. Analyze historical traffic to identify threats from suspect countries

Threats are hiding in legitimate network traffic through common web browsing or through ports and applications that are trusted within firewall rules and on the endpoint. One way to identify these threats is to account for all network traffic entering and leaving the organization to the Internet. Once this visibility is collected, retrospective analysis over this long-term history can be performed to identify what should not exist. Through this visibility and retrospection, detection of threats will be improved along with being able to improve enforcing network segmentation.

See the supporting lab video overview here > https://cs.co/SWTestDrive-Lab3.

Test Drive Objectives

Within this test drive, you will gain an understanding of the importance of accounting for all traffic entering and leaving your organization to the Internet to identify threats hidden within trusted connections. Most Secure Network Analytics deployments store 90+ days of network history and solutions can be architected to meet longer term needs such as a year plus. This history allows for detecting threats through retrospection along with building a long-term incident response platform.

Test Drive Requirements

- Stealthwatch Management Console (SMC) any version.
- Stealthwatch Flow Collector any version.
- Any version of NetFlow meeting the minimum supported fields mentioned in the NetFlow lab.
- NetFlow should be exported inside the firewall from any source with Internet access.
- Cisco Identity Services Engine (ISE) (this is optional for added context and quarantining.)

Test Drive Outline

Task 1. Generate traffic to random countries.
Task 2. Identify traffic to random countries.
Task 3. Identify possible command and control traffic over the past 7 days.
Task 4. Identify possible data loss over the past 7 days to suspect countries.
Task 1: Generate traffic to random countries

In this task, you will generate random traffic that is trusted from an installed application over common SSL web traffic.

1. Return to the Tor Browser, or re-open it from the desktop of Wkst1.

2. Search for “how does tor work” and reach through a few articles to generate traffic.

   Note: Browsing with TOR can be a very slow process.

3. Open and read the Wikipedia article shown below on how the Tor network works.
Task 2: Investigate traffic to random counties

Within this lab you will learn how to view all countries your Wkst1 has connected to.

1. Launch Chrome from the desktop of your Wkst1, as shown below.
2. Select the SMC (WebUI) bookmark from the Appliances folder of the bookmark toolbar.
3. Login with username admin and password Cisco12345

4. Enter the IP address of your Wkst1, **198.19.30.36**, into the Search filter and press Enter, as shown in the figure below.
5. Take note of the Alarms filter in the left-hand pane, and observe the alarm category scoring. This shows the overall behavioral reputation scoring of this host to indicate if any threats exist, as shown below.
6. Click the IP address **198.19.30.36** hyperlink to open a Host Report.
7. Focus on the **Traffic by Peer Host Group** report in the center. The right-hand side of this widget shows connections to Internet segments and should reflect connections to countries you initiated through the Tor browsing. Hover your mouse over the thicker lines to get a popup showing how much traffic is being exchanged with the given segment and your Wkst1, as shown below.

8. Now, let’s see what countries your host has peered with the most on the Internet. Click the **Flows** button within the Host Summary pane as shown below.

9. Within the query, select **Top Peers** for the **Search Type**, as shown below.

10. Select **Last 8 Hours** for the **Time Range**.

11. Define a name for the search by entering “**Top Countries Connected to by my Wkst1**” in the **Search Name** field.

12. Ensure the IP address **198.19.30.36** is displayed for the **Subject**.

13. Under **Peer Host Groups**, click **Select**.

14. Click **Include** and select **Countries**, under Outside Hosts, as shown below.

15. Click **Excludes** and select **Americas** and **Other**.
Note: We are excluding some groups to illustrate filtering and focus on less results.

16. Click **Apply**.
17. Make sure the filter matches exactly like what is displayed below and select **Search**.

18. You should see results like what is as shown below. Review the top peers your machine has connected to, how much traffic was transferred, and the ratio of traffic seen by your machine versus the peer host.

19. Select the **Stealthwatch Online Help**, as shown below, to get more details of how to interpret the results.
Task 3: Identify possible command and control traffic over the past 7 days

Now that you are comfortable generating traffic and interpreting results, let’s pick a broad collection of countries and see which internal hosts are being connected to the most. The Top Peers report will allow you to filter by flows over long periods of time to see if there are any persistent connections from suspect countries which could indicate command and control traffic. Often these connections remain unseen as they are connecting over trusted applications and bypassing any firewall rules.

1. Select **Analyze > Flow Search** from the menu bar, as shown below.

2. For the **Search Type**, select **Top Peers**, as shown below.

3. For the **Time Range**, select **Last 7 Days**.

4. For the **Search Name**, type “Top Internal Peers To Non Business Countries by flows.”

5. Within **Subject Host Groups**, select **Include**, and then check **Outside Hosts**

6. Select **Exclude**, check **Americas** and then click **Apply**.

7. Within **Peer Host IP Address**, type **10.201.3.0/24** (which represents one of the user segments within your organization).

8. Under **Advanced Options**, select **Flows** from the **Order By** drop down, shown below.
9. To begin the query, select **Search** in the top right corner. The query may take a few minutes.

10. You should see results like those in the screenshot below. Make note of the number of flows for the respective inside hosts.

11. In the top right corner, select **Save Search** so we can retrieve results later, as shown below. Keep the same name you defined above and click **Save**.

12. You should see a host listed with IP address of **10.201.3.15**. Click the number (765 in below example) in the **Flows** column to retrieve the flows for 10.201.3.15, as shown below. It may take a minute for all flows to be retrieved.
13. Within the flow results header row, type \texttt{80/tcp} in the \textit{Subject Port} filter, as illustrated below.

14. Type \texttt{>2K} in the \textit{Total Bytes} filter to reduce the displayed results. You may need to scroll to the right using the slider at the bottom of the browser window to see the Total Bytes column or unzoom the browser window.

15. Scroll through the flows, expand details, and make note of flows that include payload information as shown below. Many netflow exporters can include additional context.

16. After exploring a few flow details, click the Peer IP of \textbf{10.201.3.15} in one of the flow records to open a host report, as shown below.
17. Within the Host Report for 10.201.3.15, scroll down to the **Top Security Events** section, as shown below. Read the details of various security events and make note of the **Suspect Quiet Long Flow**. (if event is there, it may not be)

18. Take note of the added context associated with 10.201.3.15 within the **Users & Sessions** section, shown below. This section shows that the user “**gail**” was logged into this system along with MAC address and Device Type information. This information is received from Cisco Identity Services Engine (ISE).

19. The **Application Traffic Internal** tab will show what applications are being used inside the network and External will show the applications being used to the Internet.

20. Scroll up and select the **Stealthwatch Online Help** as shown below.

Task 4: Identify possible data loss over the past 7 days to suspect countries

The above Top Peer report was filtered on flow connections to identify persistent connections inside the network. Now let’s see if there was data movement over a long period of time. It is possible for bad actors to throttle data movement to try and stay hidden within normal traffic.

1. Let’s use the Saved Search and simply change the sort by variable. From the drop-down menu, select Analyze > Saved Searches for the “Top Internal Peers To Non Business Countries by flows” search.

   Note: If you forgot to save your previous search then look for it in Jobs > Job Management. Click it, and then click Save.

2. Select the Actions menu and click Edit, as shown below. You may need to scroll to the right using the slider bar at the bottom of the browser window.
3. Scroll down to the Advanced Options and change the Order by to Bytes.

4. Click the X to remove Americas from the search.

5. Click Search as shown below.

6. Observe that this will search all flows over the past 7 days and retrieve any large amounts of data moved. You should see results like below with a large number of bytes sent by 10.201.3.149. Click the hyperlink on the flows count (2,882 in the below example).
7. On one of the flow records, click the hyperlink for **10.201.3.149** to view the Host Report as shown below.

8. Explore the details within the host report to get an understanding of how Secure Network Analytics detected the behavior changes of the machine. With proper identification and accounting for all traffic you can increase the security posture for your organization.

![Host Report](https://lab.example.com/host-report.png)

### Summary

Within this lab, you learned:

- The importance of accounting for all traffic to and from the Internet.
- How to perform network retrospection to suspect countries.
- How to detect threats hidden within trusted network connections.
- How to filter on flow connections over long periods of time to help identity possible command and control traffic.
- How to filter on data movement over long periods of time to help identify possible data loss.
- Understanding how you can learn from having complete visibility and accounting to make better decisions in segmenting traffic to help prevent threats.
Lab 4. Data hoarding

One of the most valuable assets for an organization is its intellectual property, confidential information, and information stored in the company networks. Data breaches cost organizations millions of dollars. The global average cost of a data breach is $3.62 million and the average cost for each lost or stolen record containing sensitive and confidential information is $141. Insider threats, and disgruntled employees could take data and exfiltrate it for financial gain or just to cause harm.

The Secure Network Analytics Data Hoarding alarm indicates that a host within a network has downloaded an unusual amount of data from one or more servers. These events provide valuable insight into unauthorized data movement that might be taking place in the network.

Watch the supporting lab video overview here > https://cs.co/SWTestDrive-Lab4.

About Insider & Advanced Threat Detection

Refer to the image below to ensure you are collecting full netflow somewhere along the path between the attacker and victim IP.
Test Drive Objectives

Security events contribute index points to alarms. Alarms are grouped into Alarm categories.

Security Events Associated with the Data Hoarding Alarm Category include:

1. Suspect Data Hoarding
   a. Suspect Data Hoarding monitors how much TCP/UDP data an inside host, while acting as a client, downloads from internal servers. The event fires when the amount of data surpasses the threshold for a given host. This threshold is built automatically by baselining.
   b. This event is an indication of a particular host gathering data to prepare for exfiltration or other larger-than-normal downloads of internal data.

2. Target Data Hoarding
   a. Target Data Hoarding monitors how much TCP/UDP data an inside host, while acting as a server, serves to other inside clients. The event fires when the amount of data surpasses the threshold for a given host. This threshold is built automatically through baselining.
   b. This event is potentially an indication of one or many Inside Hosts gathering more data than normal from a particular Inside Host, potentially in preparation for exfiltration or misuse.
Test Drive Requirements

The Secure Network Analytics system configuration minimum requirements are:

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

Test Drive Outline

The “attacker” in this scenario will be downloading a large file. You choose the method of transfer (ftp, Windows file share, etc.), but the file needs to be over 300 MB.

Ensure you are collecting full NetFlow somewhere along the path between the attacker and victim IP.

In the following examples, the attacker IP address will be 198.19.30.36.

An employee has turned in their 2 weeks’ notice to work at another company. The employee is part of the account team that covers North America. She is leaving on good terms but is leaving for a competitor. There are various projects and trainings she was owner of within the company and is now downloading that sensitive data on her final day of employment. Secure Network Analytics will detect and alert you to this abnormality. Even though this user is allowed to access these servers, she is downloading an unusual amount of data.
Transfer a large amount of data on from your attacking system

The steps to conduct this attack will vary depending on the type of system that you are using both for your attack and for your file share. If you are using Windows and copying the file across a Windows file share, use Windows Explorer to connect from the attacker system. An FTP client would be used if you are connecting to a system serving files with an FTP server.

In this example, we will be transferring a 380 MB file via SCP from a database server to the Wkst1 within dCloud.

1. Launch WinSCP, from the desktop of WKST1.
   
   **Note:** If an update appears, ignore the update.

2. Select CDS, as shown below.
   
   **Note:** The IP address of **198.19.20.134**, the username is already cached for login.

3. Select Login and enter **C1sco12345** for the password if prompted.
   
   **Note:** If you see a prompt with a certificate warning in WinSCP, click **OK** and continue.
5. Locate the file **encrypted-customer-DB** and transfer it to your Downloads folder on the Wkst1.

   **Note:** if you do not see encrypted-customer-DB on the CDS server, you will need to SSH into CDS as root and run `./install-exploit-kit` which was completed in a different lab. This will surface the encrypted-customer-DB for this lab.

6. Initiate the transfer to the attacker system.

7. Close WinSCP.
Review Secure Network Analytics for Data Hoarding Alarms

Secure Network Analytics should have detected the data hoarding from your attacking system. The resulting data hoarding alarms for this attack can be observed in the Secure Network Analytics interface. While not covered in this document, you also could have received an alert via email or a syslog message to your SIEM.

1. Launch Chrome from the desktop of your Wkst1, as shown below.
2. Select the SMC (WebUI) bookmark from the Appliances folder of the bookmark toolbar.
3. Login with username admin and password C1sco12345.

![Image of Chrome and Secure Network Analytics login]

4. Look at the Data Hoarding section under Alarming Hosts. In this example, Secure Network Analytics has created six alarms for data hoarding traffic. Click the number below Data Hoarding to open up that alarm. In this example, you’d click 5.

![Image of Secure Network Analytics dashboard with Data Hoarding alarm]

5. Secure Network Analytics has determined that there is data hoarding activity above the acceptable threshold, which you can see in the DH column. Click the value in the DH section to further drill into the alarm.
6. We can see that the data hoarding alarm has far exceeded its threshold for 198.19.30.36. Click DH % value to get more details. In the below example, it would be 4,660%.

**Note:** This may take a minute or two to appear for this host.

7. Click the section that begins with “Observed” under Details to get additional information on this alarm.

8. In this example, the attacker system has connected to multiple hosts.

The host report provides informative widgets to investigate a host and includes:

1. **Cognitive Threat Analytics** – Detections from multilayered machine learning and global threat analytics to identify threats.

2. **Application Traffic** – The application traffic, amount of traffic, internally and externally.

3. Query the flows by using the Traffic by Peer Host Group, click the Protected Asset Monitoring host group and select View Flows as shown below. This will launch a flow query with our selected parameters.

**Figure 2.** Host Report

4. When the flow query is finished, displayed is subject IP address, subject port, subject host group, bytes, application, total bytes, peer address, peer port, peer host group and peer bytes.

   **Note:** The file we downloaded using SCP is presented in the flow data on this dashboard.
5. Select the down arrow on the left to get a general view of the flow data as shown below.

There is a lot of rich information in the above graphic and flow query we performed. We can see the start of the event, duration, the host group involved in the data transfer, the application used, total bytes, the peer IP address, peer port, peer host group and peer bytes.

This is a host that is allowed access to the peer system but has tripped the data hoarding alarm because amount of data being transferred is unusual compared to the normal baseline. The host group being accessed is in the Protected Assets. This host group could be defined with confidential servers, PII servers, or credit card processors. Segmenting assets allows for greater threat protection.

Also see this related article: [http://www.businessinsider.com/snowden-leaks-timeline-2016-9](http://www.businessinsider.com/snowden-leaks-timeline-2016-9) Explore more within the interface and select the context sensitive Stealthwatch Online Help on various screens as shown below. The context sensitive help will explain the information displayed on various reports.

**Summary**

Within this test plan, you learned:

- How to trigger alarms for data hoarding activity.
- How to review the data hoarding alarms within Secure Network Analytics.
Lab 5. Use data exfiltration to track inside and outside hosts

One of the most valuable assets for an organization is its intellectual property, confidential information, and information stored in the company networks. Data breaches cost organizations millions of dollars.

The Secure Network Analytics Exfiltration alarms tracks inside and outside hosts to which an abnormal amount of data has been transferred. If a host triggers events exceeding a configured threshold, it results in an Exfiltration alarm.

Watch the supporting lab video overview here > https://cs.co/SWTestDrive-Lab5.

Test Drive Objectives

Security events contribute index points to alarms. Alarms are grouped into Alarm categories.

The Suspect Data Loss security event is in the Exfiltration alarm category and based on observed flow rather than a number of default points assigned to the alarm category when the security event occurs.

When this event triggers, an inside host acting as a client has uploaded a cumulative amount of TCP or UDP payload data to an outside host, and the amount exceeds the threshold set in the policy applied to the inside host.

What does it mean when this alarms fires? A host is being used to upload more information to the Internet than is acceptable. This can be anything from someone using external backup services to maliciously exfiltrating corporate data.

Test Drive Requirements

- Stealthwatch Management Console (SMC) 6.9 or greater
- Stealthwatch Flow Collector any version 6.9 or greater
- Any version of NetFlow from within the network
- Visibility of all host-to-host traffic from the core/distribution

Test Drive Outline

The “attacker” in this scenario will be sending a large file from the system to a host on the Internet. In the example given in this document we will use ncat, but you could also transfer a file to a web file storage system like Google Drive or Dropbox.

Using the image below, ensure you are collecting full netflow somewhere along the path between the attacker and victim IP.

- In the following examples, the attacker IP address will be 198.19.30.36.

A disgruntled employee has downloaded customer information from a database server and is now sending critical sensitive data to a destination outside of your network. Secure Network Analytics will detect and alert you to this file transfer activity.
Transfer a large amount of data from your attacking system

The steps to conduct this attack will vary depending on the type of system that you are using both for your attack and for your external file share.

An FTP client would be used if you are connecting to a system serving files with an FTP server, or you could use a web browser to transfer the file to a service such as Google Drive or Dropbox. Transfer the 380 MB file to a remote host using ncat.

1. From Wkst1, open the Downloads folder within Windows Explorer and double-click the git-material.sh script.
2. Open the lab-exploit-kit folder and right-click exfil.bat selecting Run as administrator.
3. Click Yes to run the script as illustrated below.

3. The script will disable any host protections by restoring the ncat.exe tool which was part of the tools downloaded and will be used to transfer data. netcat is a computer networking utility for reading from and writing to network connections using TCP or UDP.
4. Following the prompts in the script you will see the command being used to transfer the encrypted-customer-DB over UDP port 53 (often open for DNS) to an outside host of 209.182.184.211.

Review Secure Network Analytics for Data Exfiltration alarms
Secure Network Analytics will have detected the data exfiltration from the dCloud attacking system. The data exfiltration alarms for this attack are seen in the Secure Network Analytics Security Insight Dashboard. While not covered in this document, you also could have received an alert via email or a syslog message to your SIEM.

1. To view the alarm, open a connection to your SMC and look at the Exfiltration section under Alarming Hosts as illustrated below. In this example, Secure Network Analytics has created an alarm for data exfiltration traffic. Click the number below Exfiltration to open up the alarms.

![Stealthwatch Security Insight Dashboard](image)

2. Secure Network Analytics has determined that there is data exfiltration activity above the acceptable threshold, which you can see in the EX column. Click the value in the EX cell (the IP used in the attack of 198.19.30.36) to further drill into the alarm.

![Stealthwatch Alarming Hosts](image)

3. Here we see that the data exfiltration alarm allows up to 1k points, and Secure Network Analytics has created an alarm because 198.19.30.36 has 252~K points of data exfiltration activity (this value may be different in your view). Click the section that begins with “Observed” under Details to get additional information on this alarm.

![Stealthwatch Exfiltration Details](image)
4. Click the Source Host IP address of **198.19.30.36** to open a Host Report.

5. From the Traffic by Peer Host Group (last 12 hours) widget, select the **United States** data stream, left click and view flows as seen below. This will query the Flow Collector with our parameters automatically selected.

6. After the query is finished, we can see that 198.19.30.36 (our attacker) is sending data using the port specified in the attack, 53/DNS, and sending that data out to the IP address specified in the exfiltration attack. (209.182.184.211)
7. Explore more within the interface and select the context sensitive Stealthwatch Online Help on various screens as shown below. The context sensitive help will explain the information displayed on various reports.

**Summary**

Within this test plan, you learned:

- How to trigger alarms for data exfiltration activity.
- How to review Secure Network Analytics data exfiltration alarms.
Lab 6. Detect internal Telnet traffic

About high risk application detection

Many organizations prohibit the use of Telnet on the network. It is an unsecure protocol because it transfers data in clear text, introducing the risk of exposing login credentials to an attacker. Telnet can open an organization up to data loss. Mainframes and financial systems that contain customer information often run Telnet, leaving them vulnerable to network monitoring attacks.

Secure Network Analytics Custom Security Events can be created to alarm on unauthorized Telnet communications or other unwanted applications against a group of hosts.

Watch the supporting lab video overview here > https://cs.co/SWTestDrive-Lab6.

Test Drive Objective

Security events contribute index points to alarms. Alarms are grouped into Alarm Categories.

The Policy Violations Alarm Category is a Custom Security event created to report on policy violations or unwanted communications in an organization.

Test Drive Requirements

The Secure Network Analytics system configuration minimum requirements are:

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

Test Drive Outline

Using the image below, ensure you are collecting full netflow somewhere along the path between the attacker and victim IP.

The “attacker” in this scenario will attempt to connect to a database using Telnet.

A system in the Inside Hosts group with a Telnet server is running on the network. This goes against security best practices, and in this test case we will create a Custom Security Event to monitor for this type of traffic.
Create a custom security event to detect internal Telnet traffic

Let’s set up a Custom Security Event to look for Telnet traffic internally, which uses port \texttt{23/tcp}.

1. Open the SMC web interface and navigate to \texttt{Configure > Policy Management}.

2. Select Custom Events.

Complete the following steps, being sure you exactly match the settings in the image below.

1. Enter Name: **CSE: Telnet Traffic**
   
   **a. Take note of the period in front of the CSE which will cause the name to sort first**

2. (optional) Enter description: **Telnet Traffic will violate Security Policy**

3. Status: **On**

4. Find + and select **Subject Host Group = Inside Hosts**

5. Find + and select **Subject Port/Protocols = 23/tcp** *(This is the default port used for Telnet.)*

6. Find + **Subject Packets = >3**

7. Find + **Subject Orientation = Server**

8. Find + **Peer Packets = >3** *(By defining a packet count on both the subject and peer it will cause the alarm to trigger only if the traffic is bidirectional.)*

9. In the upper right corner, click **Save**.
Enable the Telnet Server on Wkst1

In this task, we will show how easy it is for a user to install an application which could open a possible attack surface. A user has installed KTS Telnet server so they can access the machine while they are working remote.

Verify the Telnet service:

1. From Wkst1 select the **Start** button.
2. Expand **Programs**.
3. Expand **KTS** and open **Setup KpyM Telnet SSH Server**.
4. Review the setup options and hit the **ESC** key on your keyboard to exit the setup without any changes.
Connect to Server over Telnet from Remote VPN Workstation

In this task, we will use the Remote Workstation to connect to the Telnet server.


2. Select View for the current Cisco Secure Network Analytics Customer Test Drive 7.3.0.

3. Select the Remote Desktop hyperlink under Remote Workstation, as illustrated below.

   **Note:** If you have trouble connecting to the Remote Desktop, you may need to Re-boot the workstation from the Servers utility.

4. If you are prompted to log in, type admin for the username and C1sco12345 for the password.

5. **Launch** AnyConnect (if it does not automatically display; it is located in the services menu in the bottom right corner) and **Login** to Cisco AnyConnect Corporate VPN – Employees profile with username **employee** and password C1sco12345.
6. Launch Putty from the desktop and enter **198.19.30.36** in the host name field.

7. Select Telnet.

8. Press the Enter key to begin logging into the Telnet session use username **Administrator** with password **C1sco12345**.
9. Run a few commands to validate you have a successful Telnet session into 198.19.30.36. Start with `ipconfig` to verify the IP address. Next enter `cd Downloads` and `dir` to list the directory as illustrated below. Type `exit` to drop the Telnet session.

![Telnet Session](image)

Now, let’s take a look at the Policy Violation custom security event created for Internal Telnet Traffic
Review Secure Network Analytics for policy violations

Secure Network Analytics will have detected the traffic and created alarms for Internal Telnet traffic using the Custom Security Event created earlier in the lab.

1. On the Wkst1, if the Security Insight Dashboard is not already open, select **Chrome > appliances > SMC (WebUI)**
   a. If Chrome is already open with the Security Insight Dashboard displayed ignore step 1

2. On the dashboard you will see the Policy Violations alarm has been raised, a new Top Alarming Host violating policy, and Today’s Alarms would fire as shown below

3. Select **.CSE: Telnet Traffic** from the Today’s Alarms widget or Alarms by Type widget to bring up the details of the event

**Figure 3.** Policy Violations
This will bring up the host in question violating policy, as shown below.

4. In the details dialog box, select the hyperlink to View Details and investigate what policy was violated and get more information as to the security event that fired.

5. Here we can see the Custom Security Event we created has fired for Internal Telnet Traffic.

6. To see additional information, click the circle under Actions and select Associated Flows.

With AnyConnect 4.2 forward, it can be configured to export accounting telemetry into Secure Network Analytics to provide additional information about endpoints on the network. This additional information includes the process name and user associated with a network connection.

See this article for information on AnyConnect exporting flow information for visibility: https://blogs.cisco.com/security/an-introduction-to-the-new-cisco-network-visibility-flow-protocol-nvzflow
Let’s view the process information associated with the flow.

- Select **Manage Columns** with the flow search results as illustrated below.

**Figure 4.** Associated Flows

1. Check **Flow Action** in the **Connection** section, as illustrated below. This will show firewall action when flow is collected from an NGFW or ASA.
2. Check **Subject Process Name** and **Subject User** in the **Subject** section, as illustrated below. This will show process and user information exported from AnyConnect nvzflow.
3. Check **Peer Process Name** in the **Peer** section, as illustrated below.
4. Click **Set**.

**Figure 5.** Manage Columns

As you can see within the Column selector above, there is a great deal of context that can be written into a Secure Network Analytics flow record to build a general ledger of network conversations.
Let's investigate with this added context:

1. Type permitted in the **Flow Action filter** as illustrated below. This will show all flows that were permitted through a firewall.

2. Type .exe in the **Subject Process filter** as illustrated below. This will display any flows with .exe in the process name.

3. Make note of the putty.exe that was used in the previous lab to telnet into 198.19.30.36.

### Note:
You can connect back to the Remote VPN Workstation and use Nmap on the desktop to generate more traffic targeting the internal 198.19.20.0/24 subnet if you would like to explore more.

In this test case we created a custom security event to notify us if Secure Network Analytics ever sees internal Telnet traffic an alarm will fire as indicated above.

Telnet is an unsecure protocol with clear text traffic. It should never be used. This is just an example of how to create custom security events within Secure Network Analytics.

Explore more within the interface and select the context sensitive Secure Network Analytics Help on various screens as shown below. The context sensitive help will explain the information displayed on various reports.

### Summary

Within this test plan, you learned:

- How to create a Custom Security Event for Telnet communications.
- How to generate telnet traffic from the network.
- How to review the Network Security dashboard for Custom Security Alarms.
Lab 7. Detect suspicious SMB traffic

Threat actors frequently target organizations by exploiting the Server Message Block (SMB) protocol to gain control of hosts. SMB is commonly used in many organizations and attackers use it to mask their activities on the network. Targeted destructive malware, such as Conficker, exploits vulnerabilities in SMB to deploy proxy tools, backdoors, and destructive tools.

Watch the supporting lab video overview here > https://cs.co/SWTestDrive-Lab7.

On Friday, May 12, 2017, computer users around the world faced a new and very dangerous threat from malware discovered on the Internet dubbed WannaCry. This malware has been traced back to a cache of malware reported stolen from a government agency and disclosed by unknown attackers less than a year ago.

Captured in the wild and examined by members of Cisco’s industry - leading Talos threat intelligence team, the initial strain of WannaCry contains a malware payload that installs ransomware on an infected host computer. It scans heavily over TCP port 445 and can make use of a vulnerability present in certain unpatched Windows machines. WannaCry has the ability to spread throughout a network, similar to a worm, leading to widespread infections. WannaCry is wreaking havoc across the Internet, and we are likely to see variants for years to come.
Test Drive Objective

Security events contribute index points to alarms. Alarms are grouped into Alarm categories.

Secure Network Analytics monitors for hosts with many SMB sessions with hosts outside the network, which is consistent with worm propagation. The initial strain of WannaCry malware relies on the Server Message Block (SMB) protocol to infect and propagate computers running Microsoft Windows on the network. Secure Network Analytics has a number of alerts based on suspicious SMB activity. Specifically, high SMB traffic and SMB connections to numerous different hosts. This provides an easy indication of hosts compromised with WannaCry.

The initial strain of WannaCry malware will try to propagate inside the network laterally (from host to host) in an attempt to infect as many hosts as possible. This propagation action has been noted sometimes even before the malware triggers its ransomware payload. Secure Network Analytics is designed to detect lateral movements, especially between systems on the same subnet.

- Any reconnaissance and scanning activity, even between systems on the same subnet, is tracked by Stealthwatch.
- The Stealthwatch Worm Propagation detection report tracks and correlates scanning activity with successful connections to external command-and-control hosts, which is consistent with activity from WannaCry and other worms.

Secure Network Analytics will correlate different activities observed on a specific host computer and consider that IP as suspect based on numerical scores related to each observation. Secure Network Analytics then accumulates those scores under one index for each host IP address and raises an alarm called Concern Index. The higher this Concern Index numerical value rises, the more likely the host is engaging in malicious activity.

Test Drive Requirements

The Secure Network Analytics system configuration minimum requirements are:

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

Test Drive Outline

You will need to identity an IP address that will be the “attacker” along with an external IP or web address that you will transfer your simulated stolen data to during the following steps.

The “attacker” in this scenario will be sending packets targeting Windows file sharing SMB protocol 445/tcp.

Using the image below, ensure you are collecting full netflow somewhere along the path between the attacker and victim IP.

In this attack scenario, a Windows file share has been exposed to the public Internet and has become infected. This goes against security best practices.

Download the Exploit-Kit and Execute smb-malware.bat

To simulate SMB malware, you will pull the lab scripts using GitHub.
4. From Wkst1, open the Downloads folder within Windows Explorer and double-click the git-material.sh script.

5. Open the lab-exploit-kit folder double click on smb-malware.bat.

6. The smb-malware.bat file will scan the 209.182.176.0/20 address space as shown below.

Review Secure Network Analytics for the Alarms fired for High SMB Peers

Open Chrome and select Appliances SMC (WebUI) from the Favorites folder.

1. Log into Secure Network Analytics using the following: admin / Cisco12345

2. The Security Insight Dashboard will display when successfully logged in as shown.

3. Navigate to the Top Alarming Hosts widget and select the attacker (198.19.30.36) to view a Host Snapshot of the host.

4. When the Host Snapshot displays, scroll down to Top Security Events as shown below

5. Observe the security event High SMB Peers — 445. The nmap scan has tripped a security event which indicates that a host has many Server Message Block (SMB) sessions to the outside, which is consistent with the WannaCry malware.

This will run a flow query for the flows associated with this security event.

7. Scroll down to see the flows related to the nmap scan.

8. To get a condensed view of the flows select the Manage Columns > Connection tab from the flow query and de-select: (if applicable)
   a. Encryption TLS/SSL Version
   b. Encryption Key Exchange
   c. Encryption Authentication Algorithm
   d. Encryption Algorithm and Key Length
   e. Encryption MAC

9. Select Set.

10. Notice all the flows related to SMB Traffic to the address space scanned using nmap.
Explore more within the interface and select the context sensitive Stealthwatch Online Help on various screens shown below. The context sensitive help will assist in explaining the information displayed on various reports.

Summary

Within this test plan, you learned:

- How to simulate SMB traffic using nmap.
- How to review the Network Security dashboard for Top Alarming Hosts.
Lab 8. Network segmentation violations

Network administrators are faced with the challenge of creating policies that are effective and do not impede legitimate access. Administrators often do not know the roles of everyone within the company, nor what assets they need access to. They need to be able to see existing network traffic, and they need a way to model policies and assess their accuracy without enforcing them.

Watch the supporting lab video overview here > https://cs.co/SWTestDrive-Lab8.
Test Drive Objectives

Secure Network Analytics provides visibility into network traffic, which allows network administrators to do the following:

- Inventory network assets and classify them based on role or function
- Gain insight into user behavior and interactions on the network

With the information provided by Secure Network Analytics, an administrator can design segmentation based on network activity. Using host and host group policies, proposed segmentation policies can be tested without enforcing them. Alarms can be created to trigger on policies to see what affect they might have without disrupting critical business activities.

Test Drive Requirements

The Secure Network Analytics system configuration minimum requirements are:

- Visibility of all host-to-host traffic from the core/distribution
- Cisco Identity Service Engine for user information
- Stealthwatch Release 6.9 or greater

Test Drive Outline

Task 1: Verify the current host group tree
Task 2: Demonstrate how host group automation can work with an IPAM to help with segmentation
Task 3: Create a policy and test out network segmentation violations

Test Drive Scenario:

When we think of security at the network level, we immediately call to mind firewalls, access control lists, and other complex, static methods of security enforcement. Alternative techniques for separating traffic or secluding host communities often rely on even more complexity, such as VRF’s. Agility becomes a challenge with these static methods, costs increase as we add more devices into the network for security enforcement, or complexity increases in trying to maintain a consistent, network wide policy. While these challenges are in themselves barriers to success, perhaps an even bigger challenge is in validation and ongoing knowledge of whether these efforts are working or effective at achieving the intended goal.

Secure Network Analytics is uniquely suited to validating the results of your security investment by providing full disclosure of what is happening in the network before and after deploying security measures.

This scenario uses the comprehensive Flow Query tool to validate network segmentation between host device communities. What methods do you have to quickly discern the effectiveness of your security efforts?
Task 1: Verify the current host group tree

1. Log in to Secure Network Analytics: Open Chrome, and then select Favorites > Appliances > SMC (WebUI).
2. Log in to the SMC using the following username and password credentials: admin / C1sco12345.
3. Select Configure > Host Group Management.
4. Highlight By Location and make note that there are no sub groups under By Location. We will use the API to programmatically update this group structure.
Task 2: Demonstrate how host group automation can work with an IPAM to help with segmentation

We will be using GitHub to pull the lab scripts.

1. From the Wkst1 desktop, launch the Git Bash program as illustrated below.
2. Type `pwd` to verify you are in the /c/Users/Adminstrator.WKST1 directory.
3. Type `cd Downloads`, and then press Enter.
4. Type `git clone https://github.com/sw-dcloud-lab/lab-hga`, and then press Enter to download.

Note: If the lab-hga folder already exists, you can refresh content by changing directories `cd` into /Downloads/lab-hga and run `git pull https://github.com/sw-dcloud-lab/lab-hga`. 
5. Navigate to the Downloads > lab-hga folder on Wkst1.

6. Double-click the update_dCloudHostGroup.bat script, and then select Run as illustrated below.

Verify the host groups have been updated

1. Log in to Secure Network Analytics: Open Chrome and select Favorites > Appliances > SMC (WebUI). If you are already logged into the SMC, refresh the browser to update the information displayed.

2. Log in to the SMC using the following credentials:
   a. admin (username)
   b. C1sco12345 (password)
3. Select Configure > Host Group Management.

4. Highlight By Location and make note of the updated locations with IP ranges.

5. Highlight Protected Asset Monitoring and make note of the IP address **198.19.20.134**.
Task 3: Create a policy and test out network segmentation violations

In this task, we will create a custom security event and test out the new policy.

1. Open the SMC web interface and navigate to Configure > Policy Management.
2. Select Custom Events.

Complete the following steps:

1. Enter Name: .CSE: Unauthorized Connection to Protected Assets.
2. Take note of the period (.) in front of the CSE which will cause the name to sort first.
3. (Optional) Enter description: Unauthorized Connection will violate Security Policy.
5. Find + and select Subject Host Group = Protected Asset Monitoring.
6. Find + and select Peer Host Group = Client IP Ranges (DHCP Range).
7. Save as illustrated below.

In this task, we will use the Remote Workstation to connect to the Telnet server.

1. Open https://dcloud.cisco.com in a web browser, and then select My Hub.
2. Select View for the current Cisco Secure Network Analytics 7.1 & ETA Test Drive Lab.
3. Select the Remote Desktop hyperlink under Remote Workstation as illustrated below.

4. If you are prompted to log in, use admin for the username and Cisco12345 for the password.

5. Launch AnyConnect and log in to Cisco AnyConnect Corporate VPN – Employees profile with username employee and password Cisco12345.

Note: AnyConnect may already be running from a previous session.
Generate traffic to the Protected Assets host group

6. Launch Chrome from the desktop, and then enter https://198.19.20.134 in the host name field
   a. Note: Allow the security exception if requested

7. Close Chrome, and then launch WinSCP from the desktop as illustrated below.

8. For File Protocol, select SCP.

9. For the Host Name, Type 198.19.20.134.

10. Enter root for the username and Cisco12345 for the password.

11. Select Login.

   Note: If a security exception displays, select Yes.
12. **Drag and drop** the file *encrypted-customer-DB* from the /root folder on the right panel to the Documents folder in the left panel as illustrated below. Once the file finishes copying, close Winscp.

![Image of file transfer](image)

Verify segmentation violations

Now, let’s login into Secure Network Analytics to verify the segmentation violations.

1. Log in to Secure Network Analytics: Open Chrome and select Favorites > Appliances > SMC (WebUI). If you are already logged into the SMC, refresh the browser to update information displayed.

2. Log into the SMC using admin for the username and C1sco12345 for the password.

3. Select Monitor > Host Groups as illustrated below.

4. Select Change Host Group.

5. Check Protected Asset Monitoring.

6. Select Apply.
Explore the reporting within the Host Group Report for Protected Asset Monitoring

You may need to wait a few minutes and refresh this dashboard for all traffic and alarm reporting to show up. Notice the Policy Violation

1. Make note of the traffic Summary as illustrated below in how much traffic has entered and left this host group as illustrated below.

2. Make note of the IP address 198.19.20.134 in the Top Alarming Hosts

3. Make note of the Top Host Groups by Traffic which illustrates traffic to other internal host groups and traffic to the Internet. Click the Remote VPN IP Pool and select View Flows.
4. When flow results return, select **Manage Columns** as illustrated below.

**Figure 7. Flow Table**

5. Ensure the columns highlighted below are checked, in addition to the standard columns as illustrated below:
   
   a. Connections: select all of the **Encryption columns** and **Flow Action**
   
   b. Subject: select **Subject NAT** and **Subject Process Name**
   
   c. Peer: select **Peer NAT** and **Peer Process Name**
6. Review the flow table results and you should see results similar to below:

   a. The Encryption columns should reflect the TLS version information used in the https sessions. This field is only populated by switches, routers, and exporters capable of exporting ETA flow records such as the Catalyst 9000 platform. Having access to this level of information throughout your network will allow for crypto auditing and ensuring the latest TLS encryption is being used.

   b. Peer Process Name will show the application used on the AnyConnect workstation to generate the network traffic. This field is only populated if AnyConnect 4.2 or later is running on the endpoint with the network visibility module configured to export flow telemetry into Secure Network Analytics.

   c. The Flow Action will show permit or deny if exporting flow from an ASA or NGFW into Secure Network Analytics.

![Flow Table Result Example]

Summary

Within this test plan, you learned:

- How host groups can automatically be updated. There is a Host Group Automation service that may be purchased to simplify synching your IPAM with the SMC host group tree.
- How to create a custom security event.
- How to generate traffic to a Custom Security Event.
- How to investigate through the Host Group Report.
- How to view added context within the Flow Table results.
Lab 9. Detect traffic to rogue DNS servers

Rogue DNS attacks are difficult to detect without tools because the network appears to be operating normally. Rogue DNS servers arise from either a Trojan or another form of attack. After the initial attack, hackers embed their own DNS server on a network to redirect traffic to external sites for malicious purposes.

Watch the supporting lab video overview > [https://cs.co/SWTestDrive-Lab9](https://cs.co/SWTestDrive-Lab9).

Test Drive Objectives

The Secure Network Analytics Management Console (SMC) Web User Interface (UI) Flow Search and Custom Events functions can detect DNS activity from illegitimate DNS servers. You can save custom events and schedule custom searches to periodically identify possible rogue DNS traffic. A custom flow search with the following criteria can detect rogue DNS traffic:

- Port/Protocol
- Included/excluded hosts
- Orientation of the object and peer
- Application signature

Test Drive Requirements

The Secure Network Analytics system configuration minimum requirements are:

- Visibility of host-to-host traffic from the core/distribution
- Secure Network Analytics Release 6.9 or greater

Attack Scenario

A user has inserted a USB key that they found on the street into their PC, and since then has been complaining that their PC is accessing strange internet sites when they use their web browser. Secure Network Analytics will detect and alert you to any device on your network that is accessing unauthorized DNS servers.

The reason you should be concerned about rogue DNS servers on your network is that they could redirect traffic from the intended hosts that a client is attempting to reach. For example, a user that is attempting to access Amazon.com could be redirected by a rogue DNS server to a phishing site that has been crafted to look like Amazon, thus potentially compromising their account. This is known as DNS Hijacking, and additional information on DNS Hijacking can be found at [https://en.wikipedia.org/wiki/DNS_hijacking](https://en.wikipedia.org/wiki/DNS_hijacking).
Task 1: Validate Custom Security Event for Traffic to Rogue DNS Servers

1. Log in to Secure Network Analytics: Open Chrome and select Favorites > Appliances > SMC (WebUI). If you are already logged into the SMC refresh the browser to update information displayed.

2. Log into the SMC using the following credentials, using admin for the username and Cisco12345 for the password.


4. Select Custom Events.

5. Scroll down and find CSE: Unauthorized DNS Traffic. Select Edit from the actions, as illustrated below.

   Note: This rule was pre-configured for this lab but can be replicated in any environment running Secure Network Analytics 6.9 or greater.

6. Switch the Status to ON.

7. Review the Find section. This section defines what flows to look for which would be any traffic over UDP or TCP port 53 (which is the default DNS port), and between Inside Hosts, excluding authorized Internet Services parent group and the Outside Hosts, excluding Authorized External DNS Servers such as Cisco Umbrella, and then click Save, as illustrated below.
Task 3: Monitor for Rogue DNS Server Access

In this section, we will generate traffic to an unauthorized DNS server to generate alerts.

1. Access the command line from the desktop on your Wkst1, (start > run > cmd)
2. Type the command nslookup as illustrated below.
3. Next type the command: server 8.8.8.8
4. Now type in a few addresses for the rogue server to resolve as illustrated below.
   a. www.amazon.com
   b. www.facebook.com
   c. www.cisco.com
   d. www.microsoft.com

Figure 8. nslookup sample dialog

You should start to see alerts from the custom security event showing up on the Security Insights Dashboard after a few minutes.
5. **Click** the section slice of pie that shows **CSE: Unauthorized DNS Traffic** to bring up a listing of the events generated by your alert.

6. To investigate further, click the **View Details** for the **198.19.30.36** as illustrated below.
7. To investigate the flow records, select **Associated Flows** from the **Actions** as illustrated below.

As you can see, the system 198.19.30.36 accessed a rogue DNS server at 8.8.8.8.

**Summary**

Within this test plan, you learned:

- How to create a custom security event to detect rogue DNS servers.
- How to trigger and then investigate a rogue DNS server event.
Lab 10.  Use ETA for compliance and malware detection

About encrypted traffic analytics (ETA)

The percentage of encrypted traffic has been increasing each year since the IP protocol began to support cryptography. The use of Internet Protocol (IP) Secure Sockets Layer (SSL) and Transport Layer Security (TLS) cryptography grew 90 percent from 2015 to 2016. Industry analysts from Gartner predict that more than 80 percent of all web traffic will be encrypted by 2019. Encrypted traffic hides possible threats to a network. Until recently, there was no way to analyze encrypted traffic without decrypting it; making it difficult to effectively monitor networks for threats.

Cisco Encrypted Traffic Analytics addresses this problem by producing new telemetry data specifically derived from SSL / TLS connections. This data is then exported to a Secure Network Analytics Flow Collector where it is processed and stitched with connection data to provide new insights into network communications.

Watch the supporting lab video overview here > https://cs.co/SWTestDrive-Lab10.

Test Drive Objectives

Using ETA technology, Secure Network Analytics detects malware in encrypted traffic without decryption by collecting network telemetry from Cisco IOS-XE devices including routers, switches, and Wireless LAN Controllers. ETA data is also produced by the version 7.1 or later Secure Network Analytics Flow Sensor. Secure Network Analytics uses this data along with advanced entity modeling and multilayer machine learning to improve the fidelity of malware detection in encrypted traffic. These new techniques also use the Talos global threat map to identify and correlate known global threats to the local environment.

Test Drive Requirements

Visit http://www.cisco.com/go/eta for an overview on ETA, how to enable it, and how to get started.

The Secure Network Analytics system configuration requirements are:

- Stealthwatch Management Console & Flow Collector release 6.9.2 or greater. It is suggested that to get maximum benefit out of ETA you deploy the latest version of Secure Network Analytics. Note that Secure Network Analytics apps are only supported in version 7 and later.
- To use the Secure Network Analytics Crypto Audit app you will need Secure Network Analytics v7.0 or later components.
- To use the Cognitive Threat Analytics (CTA) capabilities you will need to ensure that the SMC and Flow Collector can communicate over the Internet (either direct or through a non-SSL proxy).
- To use ETA for malware detection the CTA feature must be enabled. Note that Secure Network Analytics with CTA can detect some forms of malware without ETA data.
- To investigate the source of some Internet malware detections it is necessary to send Internet NAT or proxy data to the Flow Collector. This allows for public IP addresses to be stitched into the connection data at the Flow Collector.
Test Drive Outline

Task 1. Enable Encrypted Traffic Analytics
Task 2. Verify Encrypted Traffic Analytics
Task 3. Crypto audit to enforce authorized encryption standards
Task 4. Encrypted Malware Detection

Task 1: Enable encrypted traffic analytics

ETA-capable platforms include the following devices (routers, switches or wireless LAN controllers running Cisco IOS-XE version 16.6 or later with a security feature license):

- Cisco Catalyst 9300 series switch
- ASR 1000 Series Aggregation Services Routers
- 4000 Series Integrated Services Routers
- Cloud Services Router 1000V Series
- Stealthwatch Flow Sensor v7.1 or later

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose/Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode</td>
</tr>
<tr>
<td>Step 3</td>
<td>et-analytics</td>
<td>Enters encrypted traffic analytics configuration mode</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip flow-export destination ip-address port [vrf vrf-name]</td>
<td>Configures the destination IP address optional VRF name. The ETA records are exported to this destination.</td>
</tr>
<tr>
<td>Step 5</td>
<td>exit</td>
<td>Returns to global configuration mode</td>
</tr>
<tr>
<td>Step 6</td>
<td>interface interface-id</td>
<td>Specifies the interface and port number and enters interface configuration mode</td>
</tr>
<tr>
<td>Step 7</td>
<td>et-analytics enable</td>
<td>Enables encrypted traffic analytics on this interface</td>
</tr>
<tr>
<td>Step 8</td>
<td>end</td>
<td>Returns to privileged EXEC mode</td>
</tr>
</tbody>
</table>
Below is an example of a configuration on a CSR which is already enabled in this lab.

Device> enable
Device# configure terminal
Device(config)# et-analytics
Device(config-et-analytics)# ip flow-export destination 192.0.2.1 2055 vrf green
Device(config-et-analytics)# exit
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# et-analytics enable
Device(config-if)# end

Task 2: Verify Encrypted Traffic Analytics

ETA uses flow metadata to identify malware components, maintaining the integrity of the encrypted traffic without the need for decryption and without compromising data integrity.

ETA extracts the following main data elements from the network flow: the sequence of packet lengths and times (SPLT), TLS-specific features, and the initial data packet (IDP). Cisco’s Application-Specific Integrated Circuit (ASIC) architecture provides the ability to extract these data elements without slowing down the data network. Separate templates can be defined for each of the data elements.

The following show commands are used to view ETA configuration information on a network router.

1. From Wkst1, access putty from the desktop.
2. Select the CSR router as shown below

3. Insert the following password: C1sco12345
4. Issue the following commands:

   a. Device# `show platform hardware qfp active feature et-analytics datapath interface gigabitEthernet 2`

   ```
   CSR#e qfp active feature et-analytics datapath interface gigabitEthernet 2
   uidb handle: 0x3fe
   Interface Name: GigabitEthernet2
   ```

   b. Device# `show platform hardware qfp active feature et-analytics datapath memory`

   ```
   CSR#show platform hardware qfp active feature et-analytics datapath memory
   ET-Analytics memory information:
   Size of FO : 3200 bytes
   No. of FO allocs : 30825
   No. of FO frees : 30814
   ```

   c. Device# `show platform hardware qfp active feature et-analytics datapath runtime`

   ```
   CSR#show platform hardware qfp active feature et-analytics datapath runtime
   ET-Analytics run-time information:
   Feature state : initialized (0x00000004)
   Inactive timeout : 15 secs (default 15 secs)
   Flow CFG information :
     instance ID : 0x0
     feature ID : 0x0
     feature object ID : 0x0
     chunk ID : 0x4
   ```
d. Device# show platform hardware qfp active feature et-analytics datapath stats export

```
CSR#$rm hardware qfp active feature et-analytics datapath stats export
ET-Analytics 198.19.20.139:2055 Stats:
    Export statistics:
        Total records exported : 1871
        Total packets exported : 1303
        Total bytes exported   : 1254684
        Total dropped records  : 10723
        Total dropped packets  : 2155
        Total dropped bytes    : 600148
        Total IDP records exported:
            initiator->responder : 739
            responder->initiator : 126
        Total SPLIT records exported:
            initiator->responder : 729
            responder->initiator : 123
        Total SALT records exported:
            initiator->responder : 0
            responder->initiator : 0
        Total BD records exported:
            initiator->responder : 0
            responder->initiator : 0
        Total TLS records exported:
            initiator->responder : 16
            responder->initiator : 16
```

--More--
e. Device# show platform hardware qfp active feature et-analytics datapath stats flow

```
CSR#$rm hardware qfp active feature et-analytics datapath stats flow
ET-Analytics Stats:
    Flow statistics:
    feature object allocs : 785
    feature object frees  : 775
    flow create requests  : 27964
    flow create matching  : 27179
    flow create successful: 785
    flow create failed, CFT handle: 0
    flow create failed, getting FO: 0
    flow create failed, malloc FO : 0
    flow create failed, attach FO : 0
    flow create failed, match flow: 0
    flow create, aging already set: 2
    flow ageout requests   : 775
    flow ageout failed, freeing FO: 0
    flow ipv4 ageout requests: 0
    flow ipv6 ageout requests: 0
    flow whitelist traffic match : 0
```
Task 3: Crypto audit to enforce authorized encryption standards

Generate Traffic to a Protected Server running TLS 1.0


Secure Network Analytics can retain encryption related attributes of observed network connections and display it in the SMC, enabling Crypto auditing and assurance use cases.

1. Launch Chrome from the desktop of Wkst1.
2. From the Test Sites bookmark toolbar select Compliance-Server and fakesensitivedata.csv to download. See the image below. Using the infrastructure directly you can audit the cryptographic levels being used for any server hosting sensitive data.

![This is a confidential server hosting all customer data!!!](https://compliance-server/confidential.html)

[https://compliance-server/confidential.html](https://compliance-server/confidential.html)
[https://compliance-server/fakesensitivedata.csv](https://compliance-server/fakesensitivedata.csv)
Use the Cryptographic Audit app (Secure Network Analytics v7.0 or later)

A crypto audit dashboard has been added within Secure Network Analytics to help audit and report on traffic that does not meet your company encryption standards and compliances. This dashboard is available in Secure Network Analytics 7.0 as an importable App.

1. From the SMC web interface launch Dashboards > ETA Cryptographic Audit
2. Select the date and time for the current day. For the end time it is easiest to select Today and Now.
3. Select the Subject Host Groups filter for the Protected Asset Monitoring.
4. Select the Peer Host Groups filter for the Inside Hosts.
5. Select Search.
6. Locate the TLS 1.0 connection and select View Flows as illustrated below.

If it is not already displayed in the flow results, select Manage Columns and select Encryption TLS/SSL Version and the other Encryption columns as illustrated below.
You should see results similar to below showing the connection you made to a compliance server running a weak TLS version.

![Screen shot of Flow Search watch dashboard showing results with an encryption warning]

**Alarming on Unauthorized Encryption**

Alarms may be setup to detect unauthorized traffic such as host running weaker versions of encryption. Let’s create a rule to alarm on servers run out of compliance encryptions. This can be replicated on any SMC running v7.0 or greater and is collecting ETA enriched NetFlow.
1. Navigate to Configure > Policy Management within the SMC.
2. Select Create New Policy > Custom Security Event as illustrated below

3. Create a rule to match exactly as illustrated in the image below and make sure the status is set to On. The rule is looking for any traffic where an internal server is running https running TLS 1.0 and there are at least 3 packets seen on both sides of the communication. The packet counts allow for looking for bidirectional flows only. After reviewing the rule select the Save button.

To show how the rule will detect unauthorized encryption, let’s look at the server that was connected to https://compliance-server in the above lab.
4. Type **198.19.20.134** in the search dialogue (magnifying glass) in the top right of the SMC web interface which is what compliance-server resolves to in the lab.

5. Click the hyperlink of 198.19.20.134 as illustrated below to open the host report.

6. Scroll down in the host report to the Top Security Events section and select the Target option as illustrated below. This should reflect the event that generated when you browsed to **https://compliance-server** in the previous task. These rules may be setup to meet your organization compliance needs for quick detection of unauthorized traffic.
Task 4: Encrypted Malware Detection

For this section, you will log in to a separate lab environment that has been running for a period of time long enough to allow for full machine learning for effective threat detection.


Navigate to: Instant Demo: Secure Network Analytics and follow the directions to view the instant demo.

Secure Network Analytics can be extended by enabling the cloud based Cognitive Threat Analytics (CTA). CTA uses Secure Network Analytics connection data that could include ETA metadata to identify encrypted threats. When first enabled, Secure Network Analytics users should be able to access CTA findings within 24-48 hours to allow for a good baseline and machine learning to take effect. To access Cognitive Threat Analytics, open the Secure Network Analytics Management Console (SMC) Web User Interface (UI) and locate the Cognitive Threat Analytics widget in the Security Insight Dashboard.

Note: If you have a Cisco AMP account that is also using Cognitive Threat Analytics you can request that your account be merged so that detections can be examined using data from either AMP or Secure Network Analytics. This allows for investigations from connection data all the way to files on a specific host.
For threat information, click an alarming host.

The Host Report displays with the following widgets:

- Host Summary
- Traffic by Peer Host Group

If the network includes integration with Cisco Identity Service Engine (ISE), you will see the following widgets along with Cognitive Intelligence Analytics:

- Users and Sessions
- Application Traffic
To see this threat in the Global Threat Analytics Dashboard, click the ellipses then click Open in Cognitive Intelligence.

The Global Threat Analytics Dashboard displays the threat details, including the complete story of how it went from “detected” to “confirmed.”

Select Asset Detail for added details of affected systems.
Take a few minutes to explore through the pages to learn about the threat detections.

Summary

In this, lab you learned:

- How to enable Encrypted Traffic Analytics
- How to verify Encrypted Traffic Analytics
- How to use the Crypto Audit Report to detect policy violations
- How to detect malware within encrypted traffic
Lab 11. Public cloud monitoring and threat protection

Many organizations are hosting part of their application infrastructure within public clouds. Gartner says infrastructure as a service (IaaS) has grown 31.3% in 2018. As businesses continue to move to the cloud, they must protect customer data and intellectual property for compliance and threat detection.

Watch the supporting lab video overview here > https://cs.co/SWTestDrive-Lab11.

Test Drive Objectives

Secure Cloud Analytics (formerly called Stealthwatch Cloud) is a SaaS visibility and threat detection service that can monitor public cloud infrastructure hosted in AWS, Azure, and Google Cloud for compliance and threat detection. Secure Cloud is integrated with Secure Network Analytics Enterprise via an API.

In this lab, we are going to examine an AWS account via Secure Cloud Analytics. In addition to network telemetry, referred to as VPC flow logs, Secure Cloud Analytics can retrieve additional context and behavior information for the Amazon Web Services from sources like CloudTrail and IAM (Identity and Access Management) as well as their available API. The diagram below highlights the Secure Cloud Analytics integrations.

Test Drive Requirements

- A Secure Cloud Analytics portal monitoring AWS or other cloud hosted infrastructure

Test Drive Outline

Task 1: AWS Account Review
Task 2: AWS Breach Lab
Task 3: Using the Secure Cloud Analytics user interface
Task 1: AWS

Amazon Web Services Architecture

For reference, the AWS account has multiple VPCs. We will be looking at the VPC named Cisco Test Drive.

1. Launch Chrome from the desktop of your Wkst1, as shown below.

2. Select the SWC dCloud Portal bookmark from the SWC folder of the bookmark toolbar as illustrated below.

3. Select Login via cisco-dcloud and enter username test drive and password C1sco12345!

4. When in the cloud UI, we will look more closely at the AWS network. Briefly scroll through and review the components within the default Dashboard:
o Alerts Overview – List of open alerts that can be investigated.
o Daily Traffic – Visualization of session traffic flow.
o Devices – Could of daily internal and external endpoints observed.
o Encrypted Traffic – Visual of the volume of encrypted traffic inbound and outbound.

5. Start by selecting **Investigate** and **Active Roles** from the drop down menu. Select the plus (+) sign next to **Web Server**. You should see a list like below.
4. Secure Cloud Analytics uses both APIs, as well as network telemetry to determine the types of endpoints, we call these “Roles”. Roles are automatically learned such as “AWS RDS Instances” and “Database Servers”. An endpoint can have multiple roles such as a Web Server that is also serving SSH sessions. Hovering over the will provide more context about the endpoint.

5. Next, we will look more closely at some other data that AWS provides and how Secure Cloud Analytics makes use of it. Select Report and AWS Visualizations as illustrated in the figure below. Expand us-east-2, Cisco Test Drive, and then 172.31.20.0/24, 172.31.10.0/24, and 172.31.200.0/24 like the image below.
6. If you hover over the instance ID, you will see the name given to it. The solid lines (you will need to zoom in) indicate that we have traffic between the devices/networks.

7. Next, select the **Security Groups** tab. AWS creates a default security group in each region. We will focus on **us-east-2**. A security group is like a firewall rule, permitting defined traffic and denying everything else. By default, the outbound rule is **allow all**. In the screenshot, we can see a WebServers security group allowing port 80 from everywhere and another one labeled **Overly-Permissive** that is allowing any port on any IP.

8. Scroll down to see all the security groups defined for this account, what they are allowing, and how much traffic has been observed. This can be used to verify or audit security groups.
**Traffic**

Bytes transferred via security group routes over the selected time range.

**Note:** Traffic and connection data depend on this service being configured to collect data relevant to each security group. Zeros in either column may not reflect the true usage of the security group if the traffic associated with it is not monitored.

<table>
<thead>
<tr>
<th>Account ID</th>
<th>Name</th>
<th>Identifier</th>
<th>CIDR</th>
<th>Ports</th>
<th>Connections</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>22018450040</td>
<td>Bastion Host</td>
<td>sg-0992648390c8e09042</td>
<td>0.0.0.0/0</td>
<td>0.0.0.32</td>
<td>0</td>
<td>22,3389</td>
</tr>
<tr>
<td>22018450040</td>
<td>Bastion Host</td>
<td>sg-0992648390c8e09042</td>
<td>10.0.0.0/32</td>
<td>3389</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>22018450040</td>
<td>Bastion Host</td>
<td>sg-0992648390c8e09042</td>
<td>40.71.103.46/32</td>
<td>3389</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>22018450040</td>
<td>CentOS 7 - x86_64 - with Updates HVM-1901_01-AutogenByAWSMSP-</td>
<td>sg-066b401cc28ee409c</td>
<td>0.0.0.0/0</td>
<td>0</td>
<td>0</td>
<td>22</td>
</tr>
<tr>
<td>22018450040</td>
<td>CentOS 7 - x86_64 - with Updates HVM-1901_01-AutogenByAWSMSP-1</td>
<td>sg-066b401cc28ee409c</td>
<td>0.0.0.0/0</td>
<td>0</td>
<td>0</td>
<td>22</td>
</tr>
<tr>
<td>22018450040</td>
<td>Database_Servers</td>
<td>sg-066b401cc28ee409c</td>
<td>24.126.243.153/32</td>
<td>3306</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>22018450040</td>
<td>Jumbox-Security-Group</td>
<td>sg-066b401cc28ee409c</td>
<td>0.0.0.0/0</td>
<td>3389</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>22018450040</td>
<td>Overy-Permissive-Wide-Open</td>
<td>sg-0331907c240c48292</td>
<td>0.0.0.0/0</td>
<td>0-65535</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>22018450040</td>
<td>SDtor_cisco-dcloud_alert_test</td>
<td>sg-0331907c240c48292</td>
<td>0.0.0.0/0</td>
<td>0-65535</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>22018450040</td>
<td>WebServer-Security-Group</td>
<td>sg-0331907c240c48292</td>
<td>0.0.0.0/0</td>
<td>80.443</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
9. Select IAM to see more about the users and roles associated to this account. Click the user “Admin” to see what permissions it has. You will notice it is a member of the Administrator Access policy which has “*” access, meaning this user has access to everything. Select other use accounts to contrast the permissions.

10. Select the CloudTrail tab to see recent changes to the AWS account. CloudTrail is a logging service that AWS provides, and that Secure Cloud Analytics can read. It is a great audit trail of user and machine activity that can be used to see who or what made a change. Later, we will show an alert based on a watchlist we built for CloudTrail. In the example below, we can see a user was recently created, followed by some login failures and then a success.
Secure Cloud Analytics can provide this data via a special role that is created in the customer account that gives this portal Read Only permissions to the data. To see more about how the integration works, click the Settings menu, and select Integrations. AWS is the first listed integration, while you will also see Azure, GCP, Kubernetes, Meraki, and Umbrella. The JSON document lists the various permissions used. In the next lab we will examine an AWS breach.
Task 2: AWS Breach Lab

Secure Cloud Analytics collects VPC flow logs (i.e. NetFlow) from AWS. In the AWS console you select which VPCs (Virtual Private Clouds) you want flow logs enabled on, when enabled for a VPC, any traffic between machines in the VPC and to the internet is recorded.

In this lab we will look at some of the active alerts for the demo portal. Below is how the AWS network has been setup.

1. Bastion Host – Remote Desktop Server w/public IP
2. ELB – Web load balancers (AWS Hosted Service)
3. RDS – Database Servers (AWS Hosted Service)
4. NatGW – Path for external traffic out of the VPC (AWS Hosted Service)
5. Web Servers – Standard EC2 instances running Apache

If you are not already logged into the Secure Cloud Analytics portal, do the following to access it:

1. Launch Chrome from the desktop of your Wkst1, as shown below.
2. Select the **SWC dCloud Portal** bookmark from the **SWC** folder of the bookmark toolbar as illustrated below.

3. Select **Login via cisco-dcloud** and enter username **test drive** and password **C1sco12345!**
4. Select the **Alerts** option from the **Monitor** menu as illustrated below. You should see a mix of alerts like below.
5. We will start with alert 433 (https://cisco-dcloud.obsrvbl.com/#/alerts/433). Search for 433 if you do not see it and click the hyperlink to get full details. This alert uses the IAM (Identity and Access Management) data from AWS to check for fraudulent activity. Scroll down to the supporting observations and you will see that user Patron tried unsuccessfully to login several times.
6. Click the black triangle next to the source IP address, and then click **Talos Intelligence** to pivot and see more detail about the source IP Address and its reputation. Notice the Network Owner is “Cisco Systems.” As a first step, Operations should reach out to the user and understand why they are not able to log in.

7. Go back to the main alerts page (https://cisco-dcloud.obsrvbl.com/#/alerts) and search for Alert 430 (https://cisco-dcloud.obsrvbl.com/#/alerts/430). You will see that after the failed login attempts, we have a Geographic Unusual API Usage trigger because a user logged in from an unusual country, in this case it was Japan. Secure Cloud Analytics monitors what countries normally access the API and can detect unusual behavior. This specific alert has a 14 day baseline period. In this case, it is the same user as the console logins alert.

8. Users can also select what countries are typically not associated with their account by selecting high risk countries from **Settings > Alerts > Alerts/Watchlists > Country Watchlist**.
9. Go back to the main alerts page Monitor > Alerts (https://cisco-dcloud.obsrvbl.com/#/alerts) and search for Alert 431 (https://cisco-dcloud.obsrvbl.com/alerts/431), this alert also uses data from AWS CloudTrail, it looks for security groups (e.g. firewall rules) that are overly permissive. If this was a real account, this would be very suspicious. We can easily pivot out from the alert Observation to see what else this user has been doing in the AWS account.

10. Click the black triangle next to the user and select Activity, then Observations. Scroll through the list of observations.
11. Similar to how Secure Cloud Analytics monitors the API for AWS, it monitors remote access protocols and what IPs are used to access the local network. In the previous example, the user enabled some very permissive policies for the instance, permitting any to any.

12. Go back to the Monitor > Alerts page and search for alert 435 (https://cisco-dcloud.obsrvbl.com/#/alerts/435) to see how an alert was triggered for what appears to be a Geographically Unusual Remote Access, the remote IP is the same one used in the Geographically Unusual API access.

13. Another example behavior change Secure Cloud Analytics looks for is when a machine that hasn’t been accessed remotely is accessed for the 1st time (after the baseline period). Go back to the Monitor > Alerts page and search for alert 434 (https://cisco-dcloud.obsrvbl.com/#/alerts/434), the supporting observations for this is “Remote Access Observation”. This has been used to detect out of compliance access, for example a user changing a rule so they login from home vs using the VPN or by a machine being compromised and made a terminal server.
In our examples, so far, we have detected:

- Failed logins.
- Followed by an unusual login.
- A security group change on an instance.
- Followed by new and unusual remote accesses.

At this point, we have a good case to 1) disable the user Patron and 2) lock down or terminate the instance. Ideally, we would want to know what else this instance has been doing to see what the attacker may have done while accessing the machine. Go back to the Monitor > Alerts page and search for alert 463.

Because this alert looks for unusual traffic leaving the network, supporting observations will typically have the current and new peak values. In this example, we have a new peak of 3GB of external traffic, old peak of 195MB and record profile outlier for Dropbox of 2.96GB with and old value of 0. The example uses Dropbox, but a variety of profiles would have been matched for the new peak.
14. Click the black triangle next to the host and select Device as illustrated below. This will show more details about the host traffic. We can see the spike in traffic over the past 30 days.

15. Scroll through the rest of the page and other tables to see more traffic details about the host. We will cover more details on using the portal in the next lab.
Task 3: Using the Secure Cloud Analytics User Interface

In this lab, we will look at some current alerts and how to use the UI to troubleshoot the network and endpoints.

1. Go back to the Monitor > Alerts page and search for alert 562 (https://cisco-dcloud.obsrvbl.com/-/alerts/562) and open it. This device is a Remote Desktop server used to administer the public cloud workloads. This alert looks for excessive login attempts, this is typical of a host with a public IP address and an open remote access policy. This first step to remediate would be to change the security group policy for this host.
2. To see more about the traffic for one of the external IPs, select the down arrow next to the IP address and then Find IP on Multiple Days. In the example screenshot below we can see the external IP has increased the amount of attack traffic.
3. Go back to the alert and select a time stamp, as illustrated below (you can pick any time) to see the raw flow data collected that produced the alert. In this example, we see multiple small byte/packet counts that indicate the likelihood of what appears to be a dictionary login attack.

### Supporting Observations

**Multiple Access Failures Observation**

Device had multiple failed application (e.g., FTP, SSH, RDP) access attempts.

![Time Table](image)

<table>
<thead>
<tr>
<th>Time</th>
<th>Device</th>
<th>Port</th>
<th>Profile</th>
<th>Connected Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/7/20 3:00 PM</td>
<td>bastion1</td>
<td>3389 (terminal)</td>
<td>RDP</td>
<td>185.193.88.77</td>
</tr>
</tbody>
</table>

### Session Traffic

![Session Table](image)

<table>
<thead>
<tr>
<th>Time</th>
<th>IP</th>
<th>Connected IP</th>
<th>Port</th>
<th>Connected Port</th>
<th>Protocol</th>
<th>Bytes</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/7/20 7:17 PM</td>
<td>10.0.1.2</td>
<td>185.193.88.77</td>
<td>3389 (terminal)</td>
<td>33556</td>
<td>TCP</td>
<td>1,036</td>
<td>2,558</td>
</tr>
<tr>
<td>12/7/20 7:14 PM</td>
<td>10.0.1.2</td>
<td>185.193.88.77</td>
<td>3389 (terminal)</td>
<td>44802</td>
<td>TCP</td>
<td>2,596</td>
<td>0</td>
</tr>
<tr>
<td>12/7/20 7:14 PM</td>
<td>10.0.1.2</td>
<td>185.193.88.77</td>
<td>3389 (terminal)</td>
<td>52904</td>
<td>TCP</td>
<td>1,116</td>
<td>0</td>
</tr>
<tr>
<td>12/7/20 7:14 PM</td>
<td>10.0.1.2</td>
<td>185.193.88.77</td>
<td>3389 (terminal)</td>
<td>39976</td>
<td>TCP</td>
<td>0</td>
<td>3,180</td>
</tr>
</tbody>
</table>
4. Navigate to Monitor > Observations to see more Observations for the portal.
5. Select types to see the list of all potential Observations.

6. Select By Devices to show which devices have the most Observations as illustrated below.
7. Navigate to **Reports > Traffic Summary** to show traffic summarization data. From here, you can query specific time periods to determine top IPs, ports, etc. The view below shows the traffic spike from the exfiltration to Dropbox.
8. Navigate to **Investigate > Session Traffic** to show how to build queries of all the stored flow data. You can filter by IPs, Ports, Protocol, Byte Counts, Packet Counts and time period. You can also use put a hyphen (-) in front of a field to remove it from the query. In the example below, we are running a query for all traffic, except 443.

Secure Cloud Analytics is charged by the volume of flows that are analyzed. In every portal, you can see the volume of flows by navigating to **Report > Monthly Flows Report**. We call each million flows an EMF (estimated mega flow), the monthly quantity is what is used.
Free Trial


**Note:** A typical free trial period is 60 days. These lab exercises are using the AWS public cloud, but Secure Cloud Analytics also supports Microsoft Azure, Google Cloud Platform, and Premises Networks.

Summary

You have learned how to monitor and protect cloud hosted infrastructure using Secure Cloud Analytics.
Appendix A. Integrate Splunk using the Secure Network Analytics App

Many enterprises want to use the Splunk console to aggregate actionable intelligence and integrate Cisco Secure Network Analytics® behavioral analytics into a common view.

This use case describes how to configure a recommended syslog format for Splunk along with how to configure sending alarms out of the Secure Network Analytics Management Console (SMC). There are three main steps:

- Configure response management rules (Send syslog messages from the SMC)
- Configure response management actions
- Configure syslog message format

View alarms in Splunk

1. Open Chrome, select Splunk from the Favorites menu, and then choose Top Alarming Hosts.

2. Splunk Enterprise will open. From the top of the menu, select Cisco Secure Network Analytics App.

3. Observe that the data will populate after a minute and you can see the Daily Alarm Summary, Weekly Alarm Summary and Alarms.

Within the Cisco Secure Network Analytics Splunk App there are various reports you can pull from Splunk, based on three
main categories as shown below:

a. Alarm  
b. Monitor  
c. Analyze

4. Each main category has sub-categories to display data Secure Network Analytics has sent to Splunk.
Appendix B. About NetFlow & IPFIX

What is NetFlow?
NetFlow is a feature that was originally introduced on Cisco routers that provides the ability to collect IP network traffic as it enters or exits an interface. By analyzing the data provided by NetFlow, a network administrator can determine things such as the source and destination of traffic, class of service, and the causes of congestion.

What are the various kinds of NetFlow?
Most enterprise class networking devices today support some variant of NetFlow. These can go by different names, so you may run across one or more of these in client environments:

- FNF (Flexible NetFlow)
- NSEL (NetFlow Security Event Logging)
- IPFIX (IP Flow Information Export)
- TNF (Traditional NetFlow)
- FlowCache
- NetFlow-lite Phase 1
- NetFlow-lite Phase 2
- AVC (Application Visibility and Control)
- NBAR2 (Network-Based Application Recognition)
- sFlow (Sampled Flow)

These all differ in various ways, and some Cisco devices can export NBAR2 as part of AVC which can provide extra application information to assist in investigations with Secure Network Analytics.

What NetFlow information is Secure Network Analytics expecting to see?
Secure Network Analytics expects specific NetFlow fields to be passed for it to properly analyze network traffic. Together, these fields comprise the NetFlow template.

The most common issue experienced when setting up Secure Network Analytics is invalid template errors. On most devices, you will be able to modify the NetFlow fields sent to Secure Network Analytics to receive the proper template information. For those devices that cannot send the proper template information, you will need to either rely on the NetFlow generated by other devices or install a device like a Secure Network Analytics Flow Sensor to generate NetFlow that Secure Network Analytics can interpret for you.
The **Required** and **Optional** NetFlow fields that Secure Network Analytics ingests are:

<table>
<thead>
<tr>
<th>Description</th>
<th><strong>Required or Optional?</strong></th>
<th><strong>Notes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>match ipv4 protocol</td>
<td><strong>Required</strong></td>
<td>Key field</td>
</tr>
<tr>
<td>match ipv4 source address</td>
<td><strong>Required</strong></td>
<td>Key field</td>
</tr>
<tr>
<td>match ipv4 destination address</td>
<td><strong>Required</strong></td>
<td>Key field</td>
</tr>
<tr>
<td>match transport source-port</td>
<td><strong>Required</strong></td>
<td>Key field</td>
</tr>
<tr>
<td>match transport destination-port</td>
<td><strong>Required</strong></td>
<td>Key field</td>
</tr>
<tr>
<td>match interface input</td>
<td><strong>Required</strong></td>
<td>Key field</td>
</tr>
<tr>
<td>match ipv4 tos</td>
<td><strong>Required</strong></td>
<td>Key field</td>
</tr>
<tr>
<td>collect interface output</td>
<td><strong>Required</strong></td>
<td>Key field</td>
</tr>
<tr>
<td>collect counter bytes</td>
<td><strong>Required</strong></td>
<td>Key field</td>
</tr>
<tr>
<td>collect counter packets</td>
<td><strong>Required</strong></td>
<td>Key field</td>
</tr>
<tr>
<td>collect timestamp sys-uptime first</td>
<td><strong>Required</strong></td>
<td>For calculating duration</td>
</tr>
<tr>
<td>collect timestamp sys-uptime last</td>
<td><strong>Required</strong></td>
<td>For calculating duration</td>
</tr>
<tr>
<td>collect routing next-hop address ipv4</td>
<td>Optional</td>
<td>Used for closest interface determination</td>
</tr>
<tr>
<td>collect ipv4 dscp</td>
<td>Optional</td>
<td>Used for closest QoS monitoring</td>
</tr>
<tr>
<td>collect ipv4 ttl minimum</td>
<td>Optional</td>
<td>Used for to understand the path of flow</td>
</tr>
<tr>
<td>collect ipv4 ttl maximum</td>
<td>Optional</td>
<td>Used for to understand the path of flow</td>
</tr>
<tr>
<td>collect transport tcp flags</td>
<td>Optional</td>
<td>Used for reporting on TCP flags</td>
</tr>
<tr>
<td>collect routing destination AS</td>
<td>Optional</td>
<td>Used for AS reporting</td>
</tr>
<tr>
<td>collect application name</td>
<td>Optional</td>
<td>Used to capture layer 7 application name when NBAR2 is being used</td>
</tr>
<tr>
<td>collect application http host</td>
<td>Optional</td>
<td>Used to capture URL information when AVC is being used</td>
</tr>
</tbody>
</table>
Enable flow: Steps

1. Create a Flow Record
2. Configure the Exporter
3. Configure the Monitor
4. Configure the Interface(s)

View flow configurations from the CSR Router

1. Open Putty, load the CSR configuration, and then open the session as shown below:

2. When the session loads with the username admin, insert Cisco12345 for the password.
3. Use the following command to view the interfaces flow is being exported from: show flow interface.
4. Observe the output which should look like this:

```
CSR#show flow interface
Interface GigabitEthernet1
  FNF: monitor: IPV4_NETFLOW
direction: Input
traffic(ip): on
Interface GigabitEthernet2
  FNF: monitor: IPV4_NETFLOW
direction: Input
traffic(ip): on
```

Note: The direction of the flow: Input. When enabling flow, it is best practice to enable flow on the interface in the ingress direction.
5. View the flow exporter with the following command: `show run flow exporter`.
6. The output should be the same as below for `show run flow exporter`:

   ![Flow Exporter Configuration](image)

   **Note:** The cache timeout on Cisco devices be default is **30 minutes**. Secure Network Analytics needs the cache active timeout to be 1 minute or 60 seconds.

7. Issue the following command: `show run flow monitor`.
8. Observe the output which should be the same as the `show run flow monitor` shown below:

   ![Flow Monitor Configuration](image)

9. Issue the command: `show run flow record`.

10. Take note of the output shown in the **Show flow record**: 
Note: The highlighted match and collect statements above are required fields in Secure Network Analytics. The other fields are optional to collect additional data.

Review this tool that was built by a Cisco engineering on sample NetFlow configurations on a per devices bases: https://configurenetflow.info/. This is a good resourced when having NetFlow enabled within your environment.
Review a NetFlow packet capture

1. From Wkst1, open the Downloads > lab content from Windows Explorer.

2. Open the Netflow sample folder.

3. Open the netflow-example.pcap file
   a. Note: If a Wireshark update window appears, select skip this version.
4. Select the first packet from the capture.

Wireshark packet listing of netflow-example.pcap

5. In the middle section of Wireshark, click the plus sign (+) next to Cisco NetFlow/IPFIX.

Packet details of netflow-example.pcap

6. Click to expand one of the PDU’s, as shown above. PDU is short for Protocol Data Unit—the term used to describe data as it moves from one layer of the OSI model to another. In this reference, PDU is often used synonymously with packet.

7. Compare the fields in the PDU to the figure below.
Expanded PDU

You may need to do a similar analysis of a packet if Secure Network Analytics is giving invalid template errors for a device, and the configuration looks accurate.

If any NetFlow fields are missing, like the source IP, time stamps, or byte counters that Secure Network Analytics requires, you will need to have the NetFlow record on the source exporters adjusted to contain the minimum required fields.

Summary

Within this lab, you learned:

- That Secure Network Analytics uses NetFlow as its primary data source.
- The different types of NetFlow.
- Which NetFlow fields are required and which fields are optional.
- How to decode a NetFlow packet with Wireshark.
- How to decode an IPFIX packet with Wireshark.
What’s next?

Talk about it on the dCloud Community!