Network as a Sensor with Stealthwatch and Stealthwatch Learning Networks for Threat Visibility and Defense Deployment Guide

February 2017
# Table of Contents

## Introduction ..................................................................................................................................... 1

## Network as a Sensor ....................................................................................................................... 3

- Cisco Network as a Sensor ............................................................................................................. 3
- Components at a Glance .................................................................................................................. 3

## Retail Use Case ............................................................................................................................... 7

- Business Problem .......................................................................................................................... 7
- Solution ........................................................................................................................................... 8

## HealthCare Use Case ..................................................................................................................... 11

- Business Problem .......................................................................................................................... 11
- Solution ........................................................................................................................................... 12

## Finance Use Case .......................................................................................................................... 13

- Business Problem .......................................................................................................................... 13
- Solution ........................................................................................................................................... 14

## Design Overview ........................................................................................................................... 15

## Deployment Details ....................................................................................................................... 16

- Deploying Cisco ISE (pxGrid) ......................................................................................................... 18
- Deploying Cisco Stealthwatch ......................................................................................................... 28
- Integrating Cisco ISE with Cisco Stealthwatch ............................................................................... 33
- Enabling NetFlow on Network Devices ........................................................................................... 41
- Configuring Access Switch with Wired Support Only ..................................................................... 43
- Configuring NetFlow on the WLC .................................................................................................. 48
- Quarantining SGT ............................................................................................................................ 52
- Quarantining VLAN .......................................................................................................................... 55
- Verifying and Testing ....................................................................................................................... 56
# Table of Contents

## Enabling Stealthwatch Learning Network License in Remote Site Networks

- Introduction ................................................................................................................. 61
- Components at a Glance ............................................................................................ 61

## Unusual-Time-of-Day Anomaly Use Case

- Business Problem ........................................................................................................ 63
- Solution ......................................................................................................................... 64

## New Edge Anomaly Use Case

- Business Problem ........................................................................................................ 65
- Solution ......................................................................................................................... 66

## Unusual-Data-Transfer Anomaly Use Case

- Business Problem ........................................................................................................ 67
- Solution ......................................................................................................................... 68

## Design Overview

- ................................................................................................................................. 69

## Deployment Details

- Deploying Cisco Stealthwatch Centralized Agent Manager ......................................... 70
- Configuring Network Element (ISR) ............................................................................... 74
- Installing Agent Virtual Service Via Script .................................................................... 76

## Appendix A: Product List for StealthWatch

- Stealthwatch .................................................................................................................. 98
- Identity Management ..................................................................................................... 98
- LAN Access Layer ......................................................................................................... 99
- Wireless LAN Controllers ............................................................................................ 99

## Appendix B: Product List for StealthWatch Learning Network License

- ISR Platforms ............................................................................................................... 100
- Stealthwatch Learning Network License ........................................................................ 101

## Glossary

- ................................................................................................................................. 102
Introduction

The Cisco Stealthwatch product line provides visibility and security intelligence across the extended enterprise—to the data center, to the cloud, and now to the remote site—with Cisco Stealthwatch Learning Network License.

The Stealthwatch Learning Network License helps you enhance protection against remote site network threats and provides granular visibility at the remote site level and local detection with machine learning intelligence. It strengthens your existing network investments by embedding security into your routers. It then uses packet capture, machine learning, and device-level mitigation to improve remote site office visibility, protection, and incident response.

The solution turns Cisco Integrated Services Router (ISR) into a security sensor to monitor remote site traffic with NetFlow, Network-Based Application Recognition (NBAR), Deep Packet Inspection, machine learning, and packet capture. Enabling traffic monitoring to be done at the remote site, this solution provides faster detection and response for remote site network threats. You can use the Stealthwatch Learning Network License alongside Stealthwatch, ISE with pxGrid, and Talos to gain superior end-to-end protection.

Cisco Stealthwatch (campus) and Stealthwatch Learning Networks License (remote site) management tools can be deployed on the same server (separate instances) but work together to enable threat detection in use cases such as remote-site-to-remote-site and headquarters-to-remote-site.

Stealthwatch provides central detection with full historical data to perform sophisticated threat analysis and make policy changes for effective long-term, network-wide threat mitigation.

Figure 1  NaaS SLNL—physical topology
Figure 2  Better Together use case—logical topology

- Netflow and Behavior Analytics for Branch Level Security
- Integrated Threat Intelligence with Cisco Identity Services Engine (ISE)
- Complete Broad and Deep Branch Level Visibility
Network as a Sensor

This guide describes how to enable NaaS in campus (“east-to-west traffic,” also called behind the firewall traffic) for wired and wireless users and now also includes how to enable NaaS in a remote-site with SLNL.

Cisco NaaS provides deeper visibility in your network by leveraging NetFlow on switches, routers and wireless LAN controllers (WLCs), and it can quarantine attacks, leveraging Cisco ISE, pxGrid, and Cisco Stealthwatch.

For more information, see Cisco Cyber Threat Defense and Cisco Rapid Threat Containment.

CISCO NETWORK AS A SENSOR

A network’s attack surface is continually growing. Today’s technology trends such as mobility, cloud, and the Internet of Things (IOT) are multiplying the points of infiltration into your network, and attackers are getting more sophisticated. Often attackers are part of international cybercrime organizations or organizations such as WikiLeaks, and those individuals from both inside or outside of the trusted network may have various motivations for disclosing vital proprietary or personal information. The attackers may understand your network and defenses better than you do. Many times, they will use legitimate user credentials to accomplish their objectives. As a result, discovery and network remediation of the breaches are complex, time consuming, and extremely costly.

When addressing such a complex security problem, depending on a single hardware or software component is not the right approach. Rather than taking a Swiss army knife approach (a single tool for multipurpose), you need to take a toolbox approach instead, which can provide function-specific tools. The Cisco NaaS solution is a toolbox consisting of NetFlow, Cisco ISE, and Cisco Stealthwatch. These tools are tightly integrated to help you leverage the entire network in order to:

- Detect anomalous traffic flows such as malware.
- Identify user access policy violations.
- Obtain deep and broad visibility in all network traffic.

COMPONENTS AT A GLANCE

NetFlow

NetFlow is a small package of metadata describing the “conversations” on the network. It contains the important details in network transactions' endpoints of data communication, information about when the conversation occurred, how long it lasted, and what protocols were used. It is a Layer 3 (possibly Layer 2, based on where it’s enabled or match conditions) network protocol, which you can easily enable on wired and wireless devices for visibility into the network flows, as well as enhanced network anomaly and security detection.
Cisco Identity Service Engine

Cisco ISE is a single policy-control-point for identity, access control, and device security across wired, wireless, and VPN networks. You can leverage ISE to determine additional network context for exported NetFlow from network devices. It’s a threat-centric policy server that can exchange context via pxGrid and can mitigate threats in real-time and prevent their spread across the network.

For more information, see Cisco Identity Services Engine.

Cisco Platform Exchange Grid

Cisco pxGrid is part of Cisco ISE technology that allows sharing rich contextual data with other Cisco platforms, as well as integrated partner ecosystem solutions. This makes it easier than ever to add features to identify, mitigate, and remediate security threats across the network. Overall, secure access control is centralized and simplified to securely deliver vital business services, enhance infrastructure security, enforce compliance, and streamline service operations.

For more information, see Cisco Platform Exchange Grid.

Cisco TrustSec

Combined with ISE, Cisco TrustSec can segment your network and enforce role-based, topology-independent, and access-independent access control by using software-defined segmentation—also known as Security Group Tags (SGTs)—in order to simplify the provisioning and management. Simply stated, the data can be tagged in such a way that its classification can be used throughout the network in order to make various routing and data security decisions.

For more information, see Cisco TrustSec.
Cisco Stealthwatch

Cisco Stealthwatch harnesses the power of network telemetry—including but not limited to NetFlow, IPFIX, proxy logs, and deep packet inspection (DPI) on raw packets—in order to provide advanced network visibility, security intelligence, analytics, and protection across the entire attack continuum (before, during, and after). This visibility allows a metadata record to be maintained for every communication that traverses a network device. You can analyze this aggregated data in order to identify hosts with suspicious patterns of activity. Stealthwatch has a specific Reconnaissance alarm category with several different algorithms watching behavior and identifying suspicious activity. It is basically leveraging NetFlow data from network devices throughout all layers of the network—access, distribution, core, and edge.

Figure 4  Data flows with Stealthwatch

For more information, see Cisco Stealthwatch.

Network as a Sensor

You can transform your existing Cisco network infrastructure into a security sensor and monitoring system, giving you a powerful and scalable solution for gaining deep visibility (who, what, when, where, and how), control, and analytics of the network traffic by simply activating NetFlow.

For more information, see Network as a Sensor.
Figure 5  Typical NaaS topology in a remote site/campus scenario

Normal Behavior
Accessing production server during normal business hours

Anomalous Behavior
Accessing Production Server during non-business hours triggers alarm in Stealthwatch and admin has option to quarantine suspicious device.

User/Device context data from ISE

- Device Type: Mac
- User: John Doe
- Security Group: Developer
- Corporate Asset: Yes

TrustSec Egress Policy Matrix

<table>
<thead>
<tr>
<th>SRC/DST</th>
<th>Production_Server</th>
<th>Finance_Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee</td>
<td>Permit All</td>
<td>Deny All</td>
</tr>
</tbody>
</table>

Stealthwatch Security Policy
(Triggers alarm if below conditions are met)

- Rule/Event: Employee access to Production Servers
- Object
  - TrustSec ID: 4
  - TrustSec Name: Employee
  - Orientation: Yes (Bi-directional traffic, succes or failed attempt)
- Peer
  - TrustSec ID: 11
  - TrustSec Name: Production_Server

Connection Details
Time of day: 12AM - 6AM (Accessing during midnight is suspicious.)
Retail Use Case

Retail stores have a credit card processing network. Normal behavior, then, is for the point-of-sale systems to communicate with a credit card processor, via HTTPS, sending the credit card transactions. These networks are very sensitive. Attackers love to get their hands on the traffic because credit card data can be easily monetized. This solution uses Stealthwatch to whitelist the expected network traffic and look for any new behaviors.

BUSINESS PROBLEM

If one of the point-of-sale (POS) terminals were compromised (maybe by malware), the network communications would change—such as the POS Terminal sending data to an unauthorized Command and Control server or infecting other endpoints by malware propagation.

Example 1

The compromised local POS server starts sending (north-south) communications to an external malware Command and Control (C&C) server instead of the real payment server.
Example 2
The local POS server is compromised and starts propagating malware to other POS terminals in the network. This lateral movement across a network segment is often referred to as east-west.

SOLUTION
Stealthwatch would detect the change in network behavior and receives alerts on the dashboard about the anomalous behavior and identify the compromised systems, allowing the retail organization complete visibility into their network and to rapidly mitigate the compromise.
Example 1

When the compromised Local POS server starts sending (north–south) communications to an external malware C&C Server instead of the real payment server, enabling NetFlow on the switches or WLCs gives deeper visibility into the network with Stealthwatch, and it can flag that activity and alert the anomalous behavior. This will allow the admin to further investigate and quarantine a compromised user or device.
Example 2

As the compromised local POS server commands a POS terminal to start propagating malware to other POS terminals, in a NetFlow-enabled network, Stealthwatch can flag this activity and alert it as an anomalous behavior, because communication between the POS terminals is not normal behavior. This will allow the admin to further investigate and quarantine a compromised user or device.
HealthCare Use Case

Our healthcare records are just as valuable to attackers as our credit card numbers and online passwords. In the wake of recent cyberattacks, hospitals are required to have HIPAA-compliant wired and wireless networks that can provide complete and constant visibility in to their network traffic in order to protect sensitive medical devices (such as electronic medical records servers, vital monitors or nurse workstations) so that a malicious device cannot compromise the networks.

BUSINESS PROBLEM

A patient’s mobile device is compromised by malware, and the network communication changes, infecting other endpoints by malware propagation (east-west).
SOLUTION

When a patient’s mobile device starts communicating with any medical devices, it’s considered an abnormal behavior, whether the attempt is successful or not. Enabling NetFlow on the switches or WLCs gives deeper visibility into the network traffic behavior with Stealthwatch, and it can flag the unusual activity and alert as an anomalous behavior in SMC dashboard. This will allow the admin to further investigate and quarantine a compromised device with a single click.
Finance Use Case

In an increasingly open network environment, financial institutions must:

- Protect the confidentiality, integrity, and availability of networks, applications, and data per regulatory and industry requirements.
- Define strict standards for network availability and security best practices—and stiff penalties for failure to meet or prove compliance with those standards.
- Provide customers and employees with 24/7 availability to critical financial information, without tolerating security breaches or unexpected interruptions in service.

BUSINESS PROBLEM

An employee at a financial institution uses his personal mobile device to access application (north–south), but when the device is compromised by malware and the network communication behavior changes, the device starts to communicate with the finance server.

Figure 6  Remote site office network without NaaS solution
**SOLUTION**

When an employee uses his mobile device to start communicating with any Finance Server instead of application server, it’s considered an abnormal behavior in this scenario, whether the attempt is successful or not. Enabling NetFlow on the switches or WLCs gives deeper visibility into the network traffic behavior with Stealthwatch, and it can flag the unusual activity and alert as an anomalous behavior in SMC dashboard. This allows the admin to further investigate and quarantine a compromised device with a single click.

*Figure 7  Remote site office network with NaaS solution*
Design Overview

The NaaS solution provides comprehensive visibility into all network traffic through the use of Cisco NetFlow technology. Cisco NetFlow technology is supported across Cisco enterprise wireless LAN controllers, switches, and routers in order to enable complete non-performance-impacting telemetry to be implemented at all layers of the network. Coupling this enhanced visibility with identity and context information from the Cisco Stealthwatch, ISE and TrustSec solution enables security operators to better understand a network’s traffic.

This guide focuses only on enabling NetFlow on Catalyst 3850 Switch and 5520/8540 wireless LAN controllers campus network access devices.

Figure 8  Example network

Tech Tip

CA Server is recommended for pxGrid certificates. NTP is required because time sync is needed for this solution to work.

Visibility into network traffic is provided through NetFlow export from Cisco WLC and switches, while identity services, including the user name and profile information, is provided through ISE. Stealthwatch Flow Collector provides NetFlow collection services and performs analysis in order to detect suspicious activity. SMC provides centralized management for all Stealthwatch appliances and provides real-time data correlation, visualization, and consolidated reporting of combined NetFlow and identity analysis.
Deployment Details

The deployment described is based on several design and deployment guides that comprise the reference network architecture:

- Cisco Cyber Threat Defense v2.0 Design Guide
- Configuring pxGrid in an ISE Distributed Environment Guide
- Deploying Cisco Stealthwatch 6.7.1 with Cisco pxGrid Guide
- User-to-Data-Center Access Control Using TrustSec Deployment Guide
- Campus LAN and Wireless LAN Design Summary

IP addresses used in this guide are examples; you should use addressing that is applicable to your architecture.

Cisco ISE has different personas, or nodes, for which it can be configured:

- Policy Administration Node (PAN)—A node that runs the Administration persona
- Monitoring and Troubleshooting Node (MnT)—A node that runs the Monitoring persona
- Policy Service Node (PSN)—A node that runs the Policy Service persona
- pxGrid—A node that enables ecosystem partners to obtain user and device contextual information from ISE

For a standalone configuration in which the appliance uses all personas, the maximum number of endpoints that can be supported is 10,000—dependent upon the installation hardware. To support a greater number of endpoints, to add additional resiliency, or to distribute policy services, you divide the personas across multiple physical or virtual appliances. In this example, there are five virtual nodes.

Two nodes are running both administration and monitoring personas: one is primary for these personas and one is secondary. Two additional nodes are running the Policy Service persona. One node is for the pxGrid service.

**Tech Tip**

Stealthwatch does not support pxGrid high availability.

This configuration offers resiliency and allows the deployment to scale to 10,000 endpoints for some hardware choices. To scale beyond 10,000 endpoints, you must deploy all personas on dedicated appliances. For more information about deployment size and scaling recommendations, see Cisco Identify Services Engine Hardware Installation Guide, Release 2.0.
Table 1  
Cisco ISE node IP addresses and hostnames

<table>
<thead>
<tr>
<th>Device Persona</th>
<th>Shorthand</th>
<th>IP address</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ISE primary Policy Administration Node and secondary</td>
<td>Primary PAN</td>
<td>10.4.48.41</td>
<td>ise-1.cisco.local</td>
</tr>
<tr>
<td>Monitoring and Troubleshooting node</td>
<td>Secondary MnT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco ISE secondary Policy Administration Node and secondary</td>
<td>Secondary PAN</td>
<td>10.4.48.42</td>
<td>ise-2.cisco.local</td>
</tr>
<tr>
<td>Monitoring and Troubleshooting node</td>
<td>Primary MnT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco ISE Policy Service Node</td>
<td>First PSN</td>
<td>10.4.48.43</td>
<td>ise-3.cisco.local</td>
</tr>
<tr>
<td>Cisco ISE additional Policy Service Node</td>
<td>Additional PSN</td>
<td>10.4.48.44</td>
<td>ise-4.cisco.local</td>
</tr>
<tr>
<td>Cisco ISE pxGrid Node</td>
<td>pxGrid</td>
<td>10.4.48.45</td>
<td>pxgrid.cisco.local</td>
</tr>
</tbody>
</table>

Similarly to ISE, Stealthwatch also consists of different components: UDP Director, Flow Sensor, Flow Collector, and SMC. Each has to be installed and configured separately. UDP Director and Flow Sensor are optional and are not covered in this guide.

The Flow Collector serves as a central collection point per location and analysis point for NetFlow data generated by all NetFlow generators. SMC acts as the single pane of glass to visualize this data, and this will be what a system admin will be interacting with most of the time.

Table 2  
Stealthwatch node IP addresses and hostnames

<table>
<thead>
<tr>
<th>Device Persona</th>
<th>Shorthand</th>
<th>IP address</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stealthwatch Flow Collector</td>
<td>FC</td>
<td>10.4.48.70</td>
<td>fc1.cisco.local</td>
</tr>
<tr>
<td>Stealthwatch Management Console</td>
<td>SMC</td>
<td>10.4.48.71</td>
<td>smc1.cisco.local</td>
</tr>
</tbody>
</table>
## How to Read Commands

This guide uses the following conventions for commands that you enter at the command-line interface (CLI).

- **Commands to enter at a CLI prompt:**
  
  ```
  configure terminal
  ```

- **Commands that specify a value for a variable:**
  
  ```
  ntp server 10.10.48.17
  ```

- **Commands with variables that you must define:**
  
  ```
  class-map [highest class name]
  ```

- **Commands at a CLI or script prompt:**
  
  ```
  Router# enable
  ```

- **Long commands that line wrap are underlined.**

  ```
  police rate 10000 pps burst 10000 packets conform-action
  ```

- **Noteworthy parts of system output (or of device configuration files) are highlighted:**

  ```
  interface Vlan64
  ip address 10.5.204.5 255.255.255.0
  ```

## Deploying Cisco ISE (pxGrid)

1. Install Cisco ISE (pxGrid) node
2. Create custom pxGrid certificate template (CA-signed)
3. Bind CA-signed pxGrid certificate on pxGrid node
4. Configure certificate trust list
5. Register and enable ISE pxGrid node operation

In this deployment, the Cisco ISE nodes are running as virtual machines. The installation process is detailed in the [Campus 802.1X Authentication Technology Design Guide](#), and you should use it as a reference for complete step-by-step instructions on how to deploy fully distributed (Four Nodes) ISE environment.

This solution assumes that an ISE 2.0 Distributed Environment with the latest patches (see Appendix A) is already deployed and focuses on pxGrid Node only.

For more information, see the [Cisco pxGrid design guides](#).

### Procedure 1: Install Cisco ISE (pxGrid) node

**Step 1:** Boot new Cisco ISE.

**Step 2:** At the initial prompt, enter `setup`. The installation begins.
Step 3: Enter the host name, IP address, subnet mask, and default gateway of Cisco ISE.

Enter hostname[ ]: pxgrid
Enter IP address[ ]: 10.4.48.45
Enter IP netmask[ ]: 255.255.255.0
Enter IP default gateway[ ]: 10.4.48.1

Step 4: Enter Domain Name System (DNS) information.

Enter default DNS domain[ ]: cisco.local
Enter primary nameserver[ ]: 10.4.48.10
Add secondary nameserver? Y/N : N

Step 5: Configure the time.

Enter NTP server[time.nist.gov]: ntp.cisco.local
Add another NTP server? Y/N [N]: N
Enter system timezone[UTC]: PST8PDT

Step 6: Configure an administrator account.

You must configure an administrator account in order to access the CLI console. This account is not the same as the one used to access the GUI.

Enable SSH Service? Y/N [N]: Y
Enter username[admin]: admin
Enter password: [password]
Enter password again: [password]

Cisco ISE completes the installation and reboots. This process takes from several minutes to over an hour, depending on available resources. Do not press CTRL+C during the installation, or the installation aborts.

The installation procedure is now complete for Primary pxGrid ISE node. You need a Plus License for the pxGrid feature. For more information, see the Cisco ISE Ordering Guide.

**Tech Tip**

After you have finished software installation, you should check the release notes to see if there are patches available to apply that are appropriate for the requirements of your organization. After you download any required patches, you can automatically distribute and apply them to all nodes by navigating to Administration > System > Maintenance, selecting Patch Management, and following the instructions. Minimum ISE 2.0 with Patch 2 is recommended for pxGrid and Stealthwatch 6.7.1 Integration. ISE Patch 2 upgrade will also enable EPS Unquarantine button under Operations > Adaptive Network Control > Endpoint Assignment.

For more information about Cisco ISE Design Considerations, refer to ISE configuration guides. For pxGrid, you may also refer to pxGrid design guides. For TrustSec design and deployment, see http://www.cisco.com/go/trustsec.
Procedure 2  Create custom pxGrid certificate template (CA-signed)

The pxGrid Custom-Template is required for pxGrid operation between the pxGrid Publisher (Cisco ISE) and pxGrid Subscriber/Client (Stealthwatch SMC) in a Certificate Authority (CA)–signed environment.

This solution assumes that an Enterprise CA Server was used as the CA Authority. The CA root certificate was imported into the trusted system certificates store of each of the ISE nodes. The certificate–signing request (CSR) node requests were serviced by the CA using the web server template and admin “usage” certificates defined in the ISE nodes, except for the pxGrid nodes, which will use the pxGrid Custom-Template created in this step.

Step 1: Login to Microsoft CA Server (example: MS Windows Server 2012).

Step 2: Navigate to Control Panel > System and Security > Administrative Tools > Certification Authority, and expand the Root CA Server (example: Root-CA).

Step 3: Right-click Certificate Templates, and then choose Manage. The Certificate Templates Console opens.

Step 4: In the Certificate Templates Console, right-click User Template, and then choose Duplicate Template.

Step 5: Click the General tab, and then rename the template pxGrid.
Step 6: Clear the Publish certificate in Active Directory checkbox.

Step 7: (Optional) Change the validity and renewal periods as required.

Step 8: Navigate to Extensions tab > Application Policies and click Edit.

Step 9: Click Add.

Step 10: Select Server Authentication and click OK.

Step 11: Remove Encryption File System and Secure Email. Click OK.

Step 12: Select Issuance Policies, and click Edit.

Step 13: Click Add and select All issuance policies. Click OK.

Step 14: Click OK to return to the template properties window.

Step 15: On the Subject Name tab, choose Supply in the request.

Step 16: Click Apply, and then click OK.

Step 17: In the Certification Authority window, right-click Certificate Template, and then select New > Certificate Template to issue.

Step 18: Select the newly created pxGrid certificate template, and click OK.

Step 19: Verify that the custom pxGrid certificate template (with the intended purpose “Server Authentication, Client Authentication”) is listed, along with Web Server and Client-Server Authentication certificates, as shown below:

For more detailed instructions, see Deploying Stealthwatch with Cisco pxGrid, which also includes instructions on Self-Signed Certificates.
Procedure 3  Bind CA-signed pxGrid certificate on pxGrid node

Step 1: In your browser, open the CA Server at https://ca.cisco.local/certsrv

Step 2: Select Download a CA certificate, certificate chain, or CRL.

**Tech Tip**
Even for hierarchical CA deployment, download the CA certificate and not the CA Certificate chain.

Step 3: Select Base 64, click Download CA certificate, and then save it (certnew.cer) to your local machine.

**Tech Tip**
This solution uses ISE version 2.0; configuration steps and navigation paths in ISE version 1.4 and earlier may vary.

Step 4: In your browser, connect and login to the ISE pxGrid node in standalone mode (example: https://pxgrid.cisco.local).

Step 5: Navigate to Administration > System > Certificates, and in the left navigation pane, expand Certificate Management and select Trusted Certificates.

Step 6: Click Import.

Step 7: Click Browse.

Step 8: Enter the above-downloaded certificate.

Step 9: Select Trust for authentication within ISE.
Step 10: Click Submit. The certificate is imported into the Trusted Certificates store.

Step 11: Navigate to Administration > System > Certificates, and in the left navigation pane, expand Certificate Management and select Certificate Signing Requests.

Step 12: Click Generate Certificate Signing Requests (CSR).

Step 13: In the Certificate(s) will be used for list, choose pxGrid.

Step 14: Check the pxGrid node under Node(s).

Step 15: Click Generate.

Step 16: Click Export and save the file on your local machine (example: pxGrid.pem).

Step 17: In your browser, open your CA Server (example: https://ca.cisco.local/certsrv).

Step 18: Select Request a certificate.

Step 19: Click Submit a certificate request by using a base-64-encoded.

*Tech Tip*

If you see the error “No Certificate Templates Could Be Found,” see this Microsoft knowledge base article.

Step 20: Open the pxGrid.pem that was saved on your local machine earlier.
Step 21: Copy all content from pxGrid.pem and paste it in Saved Request box.

Step 22: In the Certificate Template list, choose pxGrid, and then click Submit.

Step 23: Select Base-64 encoded format.

Step 24: Click Download certificate and save it to your local machine.

Step 25: Rename certnew.cer to pxGrid-cert-signed-by-ca.cer. This avoids any confusion with other generated certificates.

Step 26: In your browser, open the ISE pxGrid node (example: https://pxgrid.cisco.local).

Step 27: Navigate to Administration > System > Certificates, and in the left navigation pane, expand Certificate Management and select Certificate Signing Requests.

Step 28: From the CSR(s) listed on the right, select the pxGrid CSR, and then click Bind Certificate.
Step 29: Browse to the pxGrid-cert-signed-by-ca.cer file downloaded earlier.

Step 30: Under Usage, verify that pxGrid is selected, and then click Submit.

Step 31: In the dialog box requesting a restart, click YES. pxGrid node restarts.

**Procedure 4  Configure certificate trust list**

The nodes use public key infrastructure (PKI) to secure communications between them. So once the binding is completed in the previous step and pxGrid node restarts successfully, you can export the system certificate from pxGrid node and import it into Primary PAN and Primary MnT. In this deployment, you need to import the custom pxGrid template into both ISE-1 (Primary PAN) and ISE-2 (Primary MnT). If PAN and MnT are completely separate nodes you should separately import the certificates to individual PAN and MnT personas.

Step 1: In your browser, log in to the pxGrid node (example: https://pxgrid.cisco.local).

Step 2: If you receive certificate warnings, acknowledge them and continue.

Step 3: Navigate to Administration > System > Certificates, and in the left navigation pane, expand Certificate Management and choose System Certificates.

Step 4: Select pxGrid certificate, and then click Export.

Step 5: Select Export Certificate and Private Key, enter the private key (example: SecretKey), and then click Export. The file saves to the local machine.

Step 6: In your browser, log in to the Primary PAN (example: https://ise-1.cisco.local).

Step 7: Navigate to Administration > System > Certificates, and in the left navigation pane, expand Certificate Management, choose System Certificates, and then click Import.
Step 8: In the Select Node list, ensure that ise-1 (Primary PAN) is selected.

Step 9: Next to Certificate File, click Browse.

Step 10: Enter the Certificate (.pem) and Private Key (.pvk) files exported from the pxGrid node earlier, and then click Submit.

Step 11: In the Select Node list, choose ise-2 (Primary MnT).

Step 12: Next to Certificate File, click Browse.

Step 13: Enter the Certificate (.pem) and Private Key (.pvk) files exported from the pxGrid node earlier, and then click Submit.

Procedure 5  Register and enable ISE pxGrid node operation

Step 1: In your browser, log in to the Primary PAN (example: https://ise-1.cisco.local).

Step 2: Navigate to Administration > System > Deployment, click Register, and then choose Register an ISE Node.

Step 3: Enter values for the FQDN, user name and password, and then click Next. The pxGrid registers and restarts.
Step 4: Navigate to Administration > System > Deployment, select pxGrid node, and then click Edit.

Step 5: In General Settings, clear all personas (Administrator, Monitoring and Policy Service), leaving only pxGrid selected.

Step 6: Click Save.

Step 7: Navigate to Administrator > pxGrid Services.

Step 8: In the Clients tab, verify that published client names (example: ise-admin-ise-1) appear.

In the ISE (pxGrid) console, verify that the pxGrid services are running by entering `show application status ise` command. This may take a while to appear.

Step 9: If Auto-Registration is disabled, click Enable Auto-Registration.

Step 10: Verify that you are connected to pxGrid.
Deploying Cisco Stealthwatch

1. Install Cisco Stealthwatch
2. Upload CA root certificate into Stealthwatch trusted store
3. Enable SSH on SMC via web client
4. Generate CSR request on SMC
5. Sign the pxGrid Client CSR request
6. Upload SMC identity certificate to SSL client identities

Procedure 1 Install Cisco Stealthwatch

This document assumes that Stealthwatch is already installed and licensed. If not, install and configure Stealthwatch Virtual-Appliances in the following order:
1. Flow Collector VE (Mandatory)
2. SMC VE (Mandatory)


Tech Tip
Make sure to configure the Network Time Protocol (NTP) and system time (the UTC time zone is highly recommended) settings on both Stealthwatch SMC and Flow Collector before proceeding.

Procedure 2 Upload CA root certificate into Stealthwatch trusted store

Step 1: In your browser, log in to the CA-Server (example: https://ca.cisco.local/certsrv).

Step 2: Click Download a CA certificate, certificate chain, or CRL.

Step 3: Select Base 64, and then click Download CA certificate.

Step 4: Save the Root-CA certificate (root-ca.crt) on your local machine.

Step 5: In your browser, log in to the SMC (example: https://smc1.cisco.local).
Step 6: Navigate to Admin User > Administer Appliance.

Step 7: From the side navigation, select Configuration > Certificate Authority Certificates.

Step 8: Click Browse and upload the root-ca.crt file.

Step 9: Enter Name, and then click Add Certificate.

**Tech Tip**
For Name, use underscores/hyphen and do not use spaces.

Step 10: Under Certificate Authority Certificates, verify that root-ca certificate is listed.

**Tech Tip**
If you have a Two Tier (Root & Subordinate) PKI CA (Certificate Authority) Hierarchy Deployment you may also upload the subordinate CA certificate (example: sub-ca.crt).

Procedure 3  Enable SSH on SMC via web client

Step 1: In your browser, log in to the SMC (example: https://smc1.cisco.local).

Step 2: Navigate to Admin User > Administer Appliance.

Step 3: From the side navigation, select Configuration > Services.

Step 4: Select Enable SSH, and then select Enable Root SSH Access.

Step 5: Click Apply.
**Procedure 4** Generate CSR request on SMC

In this procedure, you generate the SMC private key, the CSR to be signed by the CA authority. The CA template for pxGrid must contain an EKU of both client authentication and server authentication to be valid for pxGrid operation.

**Step 1:** Log in to SMC via the SSH client (example: Putty) and generate a private key.

```
openssl genrsa -out smc.key 4096
```

**Step 2:** Generate a SMC CSR request to be signed by the CA server.

```
openssl req -new -key smc.key -out smc.csr
```

**Step 3:** Copy the smc.csr and smc.key to your local machine from the SMC client. The certificate and key are used in the next procedure.

**Tech Tip**

Use an FTP Client (example: FileZilla) and connect to SMC client to download the certificate (smc.crt) and key (smc.key).

**Procedure 5** Sign the pxGrid Client CSR request

**Step 1:** In your browser, open your CA Server (example: https://ca.cisco.local/certsrv).

**Step 2:** Click Request a certificate.

**Step 3:** Click Submit a certificate request by using a base-64-encoded.

**Step 4:** In a text-editor, open smc.csr, which you downloaded from the SMC client in the previous procedure, and copy all content.

**Tech Tip**

Example of the content inside the smc.csr file:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIErzCCApcCAQAwajELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNBTElGT1JOSUEx
DDAKBgNVBAcMA1NKQzEOMAwGA1UECgwFQ0lTQ08xDTALBgNVBAMMEHNtYzEuY2lzY2
-----END CERTIFICATE REQUEST-----
```
Step 5: In Saved Request, paste the content that you copied from smc.csr.

Step 6: In the Certificate Template list, choose pxGrid, and then click Submit.

Step 7: Download the certificate in a base-64 encoded format (example: certnew.cer).

Step 8: Rename certnew.cer to smc-ca-signed.cer

Step 9: Change the extension of the certificate file from smc-ca-signed.cer to smc-ca-signed.crt. In next two procedures, only the .crt extension is accepted.

**Tech Tip**

Procedure 5 is a new step in Stealthwatch v6.7.1, and the certificate with the .crt extension is required for it. This certificate is used for pxGrid client authentication. If you are having trouble uploading the SSL client certificate, try using Google Chrome.

**Tech Tip**

For the initial connection between SMC and ISE (when setting up the attribution configuration), it is necessary that SMC trusts the ISE certificate. But ISE does not need to trust the SMC Identity Certificate. Hence uploading the SMC identity certificate to SSL Server Identity is not recommended.

**Procedure 6**  Upload SMC identity certificate to SSL client identities

Step 1: In your browser, log in to SMC (example: https://smc1.cisco.local).

Step 2: Navigate to Admin User > Administer Appliance.
Step 3: From the left sidebar, navigate to Configuration > SSL Certificate.

Step 4: Under SSL Client Identity, enter a friendly name (example: pxGrid-SSL-Client).

**Tech Tip**

For the friendly name, use underscores/hyphens instead of spaces.

The above Client SSL Certificate pxGrid-SSL-Client is selected later, when adding ISE nodes and enabling Cisco ISE Mitigation in SMC.

Step 5: Upload the SMC public certificate `smc-ca-signed.crt` file and private key pair.

![Certificate Upload](image)

Step 6: Click Upload Certificate, and then click OK.

**Tech Tip**

Use the same CA Server to issue both ISE Identity and pxGrid certificates.

The restart may take 30 minutes or more. If the message “SMBus Host Controller not enabled” appears in the console, ignore it.
Integrating Cisco ISE with Cisco Stealthwatch

1. Configure receipt of syslog events from Cisco ISE
2. Add ISE MNT and PSN nodes
3. Verify pxGrid services and switch to Endpoint Protection Services
4. Enable Active Directory configuration in SMC
5. Launch SMC desktop Java client for Windows
6. Enabling Java store to trust the CA certificate

Now that you have successfully installed and licensed Cisco ISE (pxGrid Publisher) and Stealthwatch (pxGrid Client), you can proceed with the integration.

Procedure 1  Configure receipt of syslog events from Cisco ISE

Step 1: In your browser, log in to the Primary PAN (example: https://ise-1.cisco.local).

Step 2: Navigate to Administrator > System > Logging > Remote Logging Targets.

Step 3: Click Add.

Step 4: For Logging Target, enter the details for the Stealthwatch SMC. (Do not enter the Flow Collector IP address, or else ISE Syslog details will not be received by Stealthwatch.)

- Name: Stealthwatch
- IP/Host Address: smc-ip-address (example: 10.4.48.71)
- Port: 3514 (Cisco’s Recommended Port)
**Tech Tip**

SMC defaults to listening on port 3514. If you choose to configure ISE with a different destination port, you need to change the configuration of the SMC, as well. Do not use port 514 or port 8514, because those are reserved for other services on SMC.

**Step 5:** Click Submit.

**Step 6:** From the left navigation pane, select Logging Categories.

**Step 7:** Enable syslog message for the following four categories Passed Authentications, Radius Accounting, Profiler, and Administrative and Operational Audit.

**Step 8:** In the Logging Categories list, choose Passed Authentications.

**Step 9:** Move the target named Stealthwatch from Available to Selected, as shown.

**Step 10:** Repeat the steps 8–9 for the three more logging categories: Radius Accounting, Profiler, and Administrative and Operational Audit.

**Step 11:** Filter the Targets column and make sure Stealthwatch has been added to all four categories, as shown.
Procedure 2  Add ISE MnT and PSN nodes

Now you configure the Cisco ISE MnT and PSN nodes so that you can receive syslog messages from the Cisco ISE device in order to provide identity data to Stealthwatch for hosts on your network.

Step 1: In your browser, log in to SMC (example: https://smc1.cisco.local).

Step 2: Navigate to Tools > Settings > Cisco ISE Configuration.

Step 3: Enter the ISE Cluster Name.

Step 4: Leave the SMC Local Port as 3514.

Step 5: Enter the ISE login User Name and Password. You must enter a super-admin user (example: admin) in order to authenticate ISE.
Step 6: Under Deployment Nodes, add the following:

- Primary Node Name: ise-2 (Primary MnT / Secondary PAN)
- Primary Node IP Address: 10.4.48.42
- Node Name (optional): ise-1 (Secondary MnT / Primary PAN)
- Node IP Address: 10.4.48.41

Because SMC primarily talks to MnT nodes in order to receive syslog data (and in this case, ise-2 is the Primary MnT), you must add ise-2 before ise-1. If the PAN Node is separate from MnT or PSN, you don’t need to add PAN node, because they do not transmit the relevant syslog messages. To add more ISE nodes, click the + icon next to the Node IP Address (optional) input field.

Additionally, in order to see the authenticated users listed under Network > Users in the SMC Web Client, you must add all PSNs.

Step 7: Click Save, and then check the sync-up status indicator between ISE and SMC. If the communication is successful, the Add Cisco ISE Mitigation button is visible. If the Add Cisco ISE Mitigation button is missing, go back to the Procedure 1 in this process and ensure that all four logging categories in ISE Syslog are properly configured.

Step 8: Click Add Cisco ISE Mitigation.
Deployment Details

Step 9: In the Certificate Selection list, choose the pxGrid-SSL-Client certificate that you created in Procedure 6, "Upload SMC Identity Certificate to SSL Client Identities."

Step 10: Under Migration Nodes, add Primary pxGrid Node.
- Primary PAN Node Name: pxgrid-primary
- Primary Node IP Address: 10.4.48.45

Tech Tip
If you run into any issues adding pxGrid node, try using Google Chrome.

Step 11: Click Save.

Step 12: Wait for the Success notification, and then click OK. The green sync-up indicator appears.

Procedure 3 Verify pxGrid services and switch to Endpoint Protection Services

Only after successfully adding pxGrid node in SMC (under Cisco ISE Mitigation) as shown above are you able to see smc listed in ISE under Clients (as shown in Step 2).

Step 1: In your browser, log in to the Primary PAN (example: https://ise-1.cisco.local).

Step 2: Navigate to Administration > pxGrid Services > Clients and verify that smc1 is registered as a pxGrid client.

Step 3: Select smc1, and then click Group.
Step 4: Delete the default Groups setting **Basic** (click the **X**), and then in the **Groups** list, choose **EPS**.

![Client Group](image)

Step 5: Click **Save**.

Step 6: Verify that the smc1 client group has changed to the EPS group.

---

**Procedure 4**  
**Enable Active Directory configuration in SMC**

Stealthwatch offers more visibility when you configure Active-Directory in SMC. After SMC starts querying Active-Directory, the User Info section will be populated, as shown.

![User Info](image)

**Step 1:** In your browser, log in to SMC (example: https://smc1.cisco.local).

**Step 2:** Navigate to Tools > Settings > Active Directory Configuration.

**Step 3:** Click **Add new configuration**.
**Step 4:** Enter the **Active Directory Lookup Configuration** details, for example:

- **Name:** ad.cisco.local
- **Host:** 10.4.48.10
- **Port:** 389
- **Base DN:** DC=cisco,DC=local
- **Bind DN:** CN=Administrator,CN=Users,DC=cisco,DC=local
- **Password:** C1sco123

**Step 5:** Click **Save**.

**Procedure 5**  
**Launch SMC desktop Java client for Windows**

Until now, you have used only the SMC Web Client. For additional control and visibility, you must enable the Java client.

**Step 1:** In your browser, log in to the SMC Web GUI (example: https://smc1.cisco.local).
Step 2: Click Launch SMC.

![Launch SMC](image)

*Figure 10  Swing (JAVA) client dashboard*

If you receive an error while launching the SMC client, the issue is most likely related to the SSL certificate. Proceed to Procedure 5.

**Procedure 6  Enabling Java store to trust the CA certificate**

*(Optional)*

Follow this procedure only if you received an error message when launching the SMC client. Otherwise, skip to “Enabling NetFlow on Network Device.”

Step 1: If you receive an error while launching the SMC client, the issue is most likely related to the SSL certificate. Proceed to step 4.

Step 2: On your Windows machine, which will run the SMC Java client, navigate to `C:\Program Files\Java\jre7\lib\security\` and locate the `cacerts` file.

*Tech Tip*

Based on the version of Java, you might have to change the path accordingly.

Step 3: Right-click the `cacerts` file and choose Properties.

Step 5: Enter a user name.

Step 6: Next to Full Control, select Allow.

Step 7: Click Apply, and then click OK twice.

Step 8: Locate the path of root-ca certificate (example: C:\root-ca.crt) that you downloaded on your local machine in Procedure 2, "Upload CA root certificate into Stealthwatch Trusted Store."

Step 9: At the Windows command prompt, change the directory.

   cd C:\Program Files\Java\jre7\bin\

Step 10: Insert the root certificate into the key store.

   keytool -keystore "C:\Program Files\Java\jre7\lib\security\cacerts" -importcert -alias root-cert -file "C:\root-ca.crt"

   **Tech Tip**

   If the above command fails, verify that all of the paths in the command above are correct.

   If keytool is not available, you may need to install the Java Development Kit. For more information, see Configuring pxGrid in an ISE Distributed-Environment Guide.

Step 11: Enter the password changeit, and then repeat the password.

Step 12: Opt to trust the certificate.

Step 13: Return to the SMC Web GUI (example: https://smc1.cisco.local) and click Launch SMC. The Java client starts.

   **Tech Tip**

   For debugging, you can enable the Java Console. Navigate to Control Panel > Java > Advanced tab, and under Java Console, select Show Console and click Apply and then OK.

ENABLING NETFLOW ON NETWORK DEVICES

This guide covers enabling NetFlow on only campus/remote site network access devices, the Catalyst 3850/2960X switch and 5520/8540 wireless LAN controllers. For information about enabling NetFlow on other devices, see the NetFlow Configuration Stealthwatch Wiki page.

   **Tech Tip**

   The 2960X switch is supported with release 15.2.5E1.
This solution assumes that the C3850/C2960 switch and WLC 5520/8540 are configured and added as network devices (in Cisco ISE under Administration > Network Resources > Network Devices). For more information about adding network devices, see the Campus 802.1X Authentication Technology Design Guide.

There are three components for Flexible NetFlow (FNF) configuration: Flow Record, Flow Exporter, and Flow Monitor. After you have configured all three components, you apply the Flow Monitor to a wired or wireless interface such as a L2/L3 port, VLAN, or WLAN (SSID). Lastly, you configure AVC for deeper visibility.

### Flow Record

A Flow Record defines the information that will be gathered by the NetFlow process, such as packets in the flow and the types of counters gathered per flow. Custom flow records specify a series of match and collect commands that tell the Cisco device which fields to include in the outgoing NetFlow record.

The match fields are the key fields, meaning that they are used to determine the uniqueness of the flow.

The collect fields are extra information that is included in the record in order to provide more detail to the collector for reporting and analysis.

When you configure Flow Record, you are telling the device to show all of the flow data traffic that enters (Ingress) or leaves (Egress) the device.

### Flow Exporter

The Flow Exporter defines where and how to send the NetFlow (Flow Records). In actuality a Flow Exporter defines a flow collector IP address and port as the destination, and in this case the Stealthwatch Flow Collector is the destination.

### Flow Monitor

A Flow Monitor describes the NetFlow cache or information stored in the cache. Additionally, the Flow Monitor links together the Flow Record and the Flow Exporter.

The Flow Monitor includes various cache characteristics such as the timers for exporting, the size of the cache, and, if required, the packet sampling rate.

As network traffic traverses the Cisco device, flows are continuously created and tracked. As the flows expire, they are exported from the NetFlow cache to the Stealthwatch Flow Collector.

A flow is ready for export when it is inactive for a certain time (for example, no new packets received for the flow); or if the flow is long lived (active) and lasts greater than the active timer (for example, long FTP download). There are timers to determine if a flow is inactive or if a flow is long lived.

---

**Table 3  NetFlow Validated Performance Data**

<table>
<thead>
<tr>
<th>Model</th>
<th>APs</th>
<th>Clients</th>
<th>Throughputs</th>
<th>Max Flows</th>
<th>Ingress</th>
<th>Egress</th>
</tr>
</thead>
<tbody>
<tr>
<td>8540</td>
<td>3000</td>
<td>32,000</td>
<td>17 Gbps</td>
<td>200,000</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>5520</td>
<td>750</td>
<td>10,000</td>
<td>7 Gbps</td>
<td>200,000</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>3850</td>
<td>—</td>
<td>1,000</td>
<td>2 Gbps</td>
<td>24,000</td>
<td>8,000</td>
<td>16,000</td>
</tr>
<tr>
<td>2960X</td>
<td>—</td>
<td>1,100</td>
<td>Up: 25M</td>
<td>16,000</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Down: 176M</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Application Visibility and Control

AVC classifies applications using deep packet inspection techniques with the Network-Based Application Recognition engine and provides application-level visibility and control into Wi-Fi networks. After the applications are recognized, the AVC feature enables you to either drop or mark the data traffic.

Using AVC, you can detect more than 1000 applications. AVC enables you to perform real-time analysis and create policies to reduce network congestion, costly network link use, and infrastructure upgrades.

**Tech Tip**

On Catalyst 3850 switch code 3.6.4, AVC is not supported on wired and wireless as part of NaaS Solution. AVC not supported on the 2960X switch, either.

Wired AVC (NBAR2) will be available in 16.3.1, but FNF support on wired AVC (NBAR2) will be available in 16.3.2. Therefore exporting flow record match application name to external collector such as Stealthwatch is not available until 16.3.2.

AVC is supported and functional as part of the NaaS solution test with WLCs (5520/8540).

---

**Configuring Access Switch with Wired Support Only**

1. Configure a flow record
2. Configure a flow exporter
3. Configure a flow monitor
4. Apply flow monitor to a support port type(s)

---

This procedure describes configuring the C3850 switch but applies to the C2960X switch with a few considerations, which will be discussed in this section.

Cisco Catalyst 3850 supports both ingress and egress FNF on all ports of the switch at line rate, whereas 2960X supports only ingress FNF.

Switch raw scalability is up to 24K-cached flows. Cisco Catalyst 3850 supports NetFlow Version 9, with IPv4, IPv6, Layer 2 flows, and sampled NetFlow. TCP flags are also exported as part of the flow information. When Cisco Catalyst 3850 switches are stacked together, each individual stack member exports its own flows to the collector, whereas 2960X switches scale up to 8K-cashed flows per switch or stack member.

Cisco Catalyst 3850 supports up to 16 flow monitors with eight different collectors simultaneously per flow monitor. Microflow policing is supported only for wireless clients.

The FNF feature on the Cisco Catalyst 3850 is enabled on the IP base version and earlier.
Procedure 1: Configure a flow record

Connect to the console of the switch and, in configuration mode, enter the appropriate commands in order to enable ingress and/or egress flow.

Option 1: Enable Ingress Flow

```
flow record FLOW-RECORD1-IN
  match datalink mac source address input
  match datalink mac destination address input
  match ipv4 tos
  match ipv4 ttl
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  match interface input
  match flow direction
  match flow cts source group-tag
  match flow cts destination group-tag
  collect counter bytes long
  collect counter packets long
  collect timestamp absolute first
  collect timestamp absolute last
```

Tech Tip

The `match interface output` and `collect interface input` cannot be configured in the ingress flow record. Also both `interface input` and `interface output` in the same flow record are not supported. Only configure one interface direction in one flow record (match or collect).

Tech Tip

On the 2960X, the flow record is slightly different. Not all fields are available. (Example: CTWS fields are not available).
flow record FLOW-RECORD1-IN
  match datalink mac source address input
  match datalink mac destination address input
  match ipv4 tos
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  collect interface input
  collect interface output
  collect counter bytes long
  collect counter packets long
  collect timestamp sys-uptime first
  collect timestamp sys-uptime last

Option 2: Enable Egress Flow

flow record FLOW-RECORD1-OUT
  match ipv4 tos
  match ipv4 ttl
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  match flow direction
  match flow cts source group-tag
  match flow cts destination group-tag
  collect counter bytes long
  collect counter packets long
  collect timestamp absolute first
  collect timestamp absolute last

Tech Tip

The match interface input and collect interface output cannot be configured in the egress flow record.
In the above flow records (Ingress and Egress), there are two statements involving TrustSec Security Groups Tags (SGTs).

match flow cts source group-tag
match flow cts destination group-tag

The statements ensure that any security group classification known to the switch or present on the wire is exported in the flow record. If you don’t plan to enable TrustSec to support NaaE, you can remove these two fields.

**Tech Tip**

The ability to monitor the security group in a NetFlow record first became available on the 3850/3650 in IOS XE version 3.6.4.

---

**Procedure 2** Configure a flow exporter

**Step 1:**

Connect to the console and, in configuration mode, enter the following commands.

The NetFlow standard is UDP port 2055.

```
flow exporter FLOW-COLLECTOR1
  destination 10.4.48.70
  transport udp 2055
```

**Tech Tip**

The C3850 switch can support up to eight different exporters (collectors) simultaneously per flow monitor.

---

**Procedure 3** Configure a flow monitor

Connect to the console and, in configuration mode, enter the following commands to enable ingress and/or egress flow.

**Option 1: Ingress Flow**

```
flow monitor FLOW-MONITOR1-IN
  exporter FLOW-COLLECTOR1
  cache timeout active 60
  record FLOW-RECORD1-IN
```
Option 2: Egress Flow

flow monitor FLOW-MONITOR1-OUT
exporter FLOW-COLLECTOR1
cache timeout active 60
record FLOW-RECORD1-OUT

Procedure 4  Apply flow monitor to a support port type(s)

Connect to the console and, in configuration mode, enter the appropriate commands.

If you plan to quarantine end clients from Stealthwatch, make sure to enable Change of Authorization (CoA) on the Catalyst 3850 switch, which forces the client to re-authenticate and assign appropriate policy. CoA being disabled on the switch may cause an error as a result of ISE returning a RADIUS_FAIL message to Stealthwatch because it was unsuccessful in completing CoA. For information about configuring CoA on a 3850 switch, see Configuring CoA on the Switch.

Tech Tip

CoA on the Catalyst 2960X switch is not supported.

Option 1: Wired Interface

interface GigabitEthernet1/0/1
description Wired Client in Vlan
switchport access vlan 10
switchport mode access
ip flow monitor FLOW-MONITOR1-IN input
ip flow monitor FLOW-MONITOR1-OUT output
load-interval 30
no shutdown

Option 2: VLAN Interface

vlan configuration 100
ip flow monitor FLOW-MONITOR1-IN input
ip flow monitor FLOW-MONITOR1-OUT output

Tech Tip

VLAN 100 is the client VLAN and not the AP Management VLAN. You don’t need to configure flow-monitor on the AP Management VLAN.
NetFlow is now installed on the Catalyst 3850 switch.

### Configuring NetFlow on the WLC

3. Configure a flow exporter
4. Configure a flow monitor
5. Applying a flow monitor to a WLAN

For the WLC, you need to configure only two components:

- **NetFlow Exporter**—Network entity that exports the template with the IP traffic information. The WLC acts as an exporter.
- **NetFlow Collector**—Entity that collects all the IP traffic information from various NetFlow exporters.

**Tech Tip**

Cisco Wireless Controller does not support IPv6 address as Exporter for NetFlow. For more information, see [Cisco Wireless Controller Configuration Guide, Release 8.2](#).

---

**Procedure 1** Configure a flow exporter

Step 1: Browse and login to the 5520 or 8540 WLC (example: wlc.cisco.local).

Step 2: In the top right corner, click **Advanced**.

Step 3: On the Wireless tab, in the left navigation pane, expand NetFlow, and then click **Exporter**.

Step 4: Click **New**.

Step 5: Enter the following. Even though it’s asking you to enter the Exporter IP and port number, you must enter the Flow Collector IP and port.

- Exporter name: **Netflow-Collector**
- Exporter IP: **10.4.48.70** (Enter your SW Flow Collector IP Addr.)
- Port number: **2055** (by default, this is UDP 2055)
Step 6: Click Apply.

Step 7: Click Save Configuration.

**Procedure 2  Configure a flow monitor**

Step 1: Back on the Wireless tab, in the left navigation pane, expand Netflow, and then and click Monitor.

Step 2: Click New.

Step 3: Enter the monitor name (example: NetFlow-Monitor).

Step 4: Click Apply.

Step 5: On the Monitor List page, click the newly created Monitor (example: NetFlow-Monitor).

Step 6: In the Exporter name list, select Netflow–Collector.

**Tech Tip**

For WLC you don’t have a separate step to configure Flow Record. The configuration of Flow Record is part of Flow Monitor in the above steps.

Step 7: In the Record Name list, select Client Source and Destination Record.

**Tech Tip**

The Client Source and Destination Record (Higher Visibility) record name was added starting with WLC 8.2. You must use this record name with Stealthwatch in order to leverage the enhanced features of NetFlow v9.
Step 8: Click Apply. The Monitor List page reflects the following details.

![Monitor List Page](image)

Step 9: Click Save Configuration.

![Save Configuration Button](image)

**Procedure 3**  
**Applying a flow monitor to a WLAN**

Associate a NetFlow Monitor to a WLAN.

**Step 1:** Navigate to WLANs, and then click the WLAN ID to open the WLAN where you will configure NetFlow.

![WLAN Configuration](image)

**Step 2:** On the QoS tab, in the Netflow Monitor list, select Netflow-Monitor, which you created in “Configure a flow monitor.”

![QoS Tab](image)

**Step 3:** Click Apply.

*Tech Tip*

AVC is enabled by default when NetFlow is enabled on WLC 5520 or 8540.

**Step 4:** On WLC, make sure CoA is enabled. It is important when quarantining or unquarantining a device from Stealthwatch. Login to WLC, navigate to Security > Radius > Authentication, select the ISE Node to verify and from the Support for CoA list, select Enabled. Click Apply.
Step 5: Enable Interim Updates by navigating to WLANs tab. Select the WLAN ID and navigate to Security > AAA Servers, and in the RADIUS Server Accounting section, check the box next to Interim Update and change the internal to 180. Click Apply.

Step 6: Click Save Configuration.

Now you have completed required tasks to enable NetFlow on 5520/8540 Switch.

**Tech Tip**

Stealthwatch 6.7.1 doesn’t support WLAN as a flow interface (unable to consume SSID/AP MAC addresses). Instead it reports the physical interface of the switch, which causes the interface to report invalid utilization. In terms of flows, Stealthwatch won’t represent wireless flows differently. It appears similar to wired flows. This is expected to be resolved in a future release.

Enabling Quarantine

In Procedure 3, “Verify pxGrid services and switch to Endpoint Protection Services,” you subscribed the SMC (Stealthwatch) to the EPS Group in ISE. Until you create an authorization policy in ISE, clicking the Quarantine or Unquarantine button from the SMC dashboard (under Networks > Host > Host-IP) will have no effect.

**Tech Tip**

Due to an open bug in Stealthwatch 6.7.1, flows status is reported as Inactive, even though it’s Active, under the Host Summary. This has been fixed in 6.6.3 and 6.7.3.

Next, you configure an Authorization Policy that takes advantage of the quarantine attribute in order to assign a suspicious host to the Quarantine_System SGT and also define segmentation policy for the Quarantine_System SGT.
**Tech Tip**

Based on the specific use-case, you can quarantine traffic to a specific server in the data center. This example assumes that TrustSec has been enabled on the network device in ISE. For example, a Finance_Server SGT is configured. For step-by-step instructions about configuring TrustSec in the User-to-DC use case, see [User-to-Data-Center Access Control Using TrustSec Deployment Guide](#).

### Quarantining SGT

1. Configure Quarantine SGT
2. Configure authorization policy for Quarantine SGT

---

**Procedure 1**  Configure Quarantine SGT

**Step 1:** In your browser, log in to the Primary PAN (example: https://ise-1.cisco.local).

**Step 2:** Navigate to Work Centers > TrustSec > Components.

**Step 3:** Under Security Groups, verify the following SGTs have been created (tag number may vary).

- Employee (4/0004)
- Quarantined_Systems (255/00FF) SGT
- Finance_Server (1000/03E8)
- HR_Server (2000/07D0)

**Step 4:** Under Security Group ACLs, verify for a Deny_All ACL that includes “deny ip log” has been created.

**Step 5:** Navigate to Work Centers > TrustSec > Policy, expand Egress Policy, and then click Matrix.
Step 6: From the Matrix setting, double-click the box intersecting the source Quarantine_System and the destination Finance_Servers.

Step 7: Select the Deny_All ACL and make sure Status is Enabled.

Step 8: Click Save.

Step 9: Ensure the policy Matrix reflects the new policy, Deny_All.

**Tech Tip**

The top right of the menu bar will now show one notification, indicating the new TrustSec policy changes are not yet pushed to the switch.

Step 10: Click Push. The new policy change applies on the enforcer switch (example: Nexus 7000 in Datacenter).
Procedure 2  Configure authorization policy for Quarantine SGT

Step 1: In your browser, log in to the Primary PAN (example: https://ise-1.cisco.local).

Step 2: Navigate to Policy > Authorization Policy.

Step 3: In the Authorization Policy section, expand Exceptions.

Step 4: Click Create a New Rule.

Tech Tip
The ANC (Adaptive Network Control—Earlier, Endpoint Protection Service–EPS) is enabled by default in Cisco ISE 2.0.

Step 5: Configure the authorization policy with following settings:
- **Rule Name**: ANC_Quarantine_SGT
- **Conditions**: Create New Condition (Advanced Option) > Session > EPSStatus > (Equals) ‘Quarantine’
- **Permissions**: Security Group > Quarantine_Systems

Step 6: Click Done, and then click Save. Under the Exceptions condition, the configured authorization policies look like the following.

Step 7: You may also verify the Standard condition (for example, 802.1X policy with Employee SGT) that will be the initial tag assigned to the corporate user upon login.
Quarantining VLAN

1. Create an authorization profile
2. Configure an authorization policy

Procedure 1  Create an authorization profile

Step 1: Navigate to Policy > Policy Elements > Results.


Step 3: Expand Common Tasks, and then select VLAN.

Step 4: Enter the Quarantine VLAN ID (for example 666). Leave the default Tag ID set to 1.

Step 5: Click Add, and then click Save.

Procedure 2  Configure an authorization policy

Step 1: In your browser, log in to the Primary PAN (example: https://ise-1.cisco.local).

Step 2: Navigate to Policy > Authorization Policy.

Step 3: In the Authorization Policy section, expand Exception.

Step 4: Click Create a New Rule.

Step 5: If you have already created the ANC_Quarantine_SGT in the previous steps, then you will have to duplicate the policy and edit. To do so, click the triangle and select Duplicate Above or Duplicate Below.
Step 6: Edit and configure the authorization policy with following settings:

Rule Name: **ANC_Quarantine_VLAN**

Conditions: Create New Condition (Advanced Option) > Session > EPSStatus > (Equals) ‘Quarantine’

Permissions: Standard > Quarantine_VLAN

Step 7: Click Done, and then click Save. Under the Exceptions condition, the configured authorization policies look like the following.

<table>
<thead>
<tr>
<th>Status</th>
<th>Rule Name</th>
<th>Conditions (identity groups and other conditions)</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ANC_Quarantine_VLAN</td>
<td>Session EPSStatus EQUALS Quarantine</td>
<td>Quarantine_VLAN</td>
</tr>
</tbody>
</table>

**Verifying and Testing**

1. Perform Stealthwatch communication check with network devices
2. Test network visibility

In this process, you verify the NaaS deployment. If Quarantine is enabled, also test the containment (Quarantine) feature from the Stealthwatch Web GUI.

**Procedure 1** Perform Stealthwatch communication check with network devices

Step 1: Launch the Stealthwatch Java client and log in.

Step 2: From left pane, navigate to **Domain Name** (example: cisco.local) > Host Groups > Network Devices, and make sure all the NetFlow-enabled Network Access Devices are listed.

**Tech Tip**

Under **Network Devices**, a device will only be listed if NetFlow is configured properly. You cannot manually add a network device from the Stealthwatch client.
Step 3: From the left pane, expand **FlowCollectors** and make sure all the NetFlow enabled Network Access Devices are listed.

![Image of FlowCollectors interface]

**Tech Tip**

Under **FlowCollectors > fc1 > Exporters**, if a device is not listed, manually add all the NetFlow enabled devices as an Exporter within the Stealthwatch client. Right-click **Exporters**, select **Configuration > Add Exporters**, enter the IP address and name of the device, and then click **OK**.

Step 4: To verify NetFlow data collection, expand **FlowCollectors**, right-click your Flow Collector (example: fc1), and navigate to **Status > NetFlow Collection Status**. Under **Current NetFlow Traffic (bps)**, check the counters increment.

Step 5: Right-click the **Flow Collection Status** table header, and then check **Longest Duration Export** to enable the column to correlate the time duration for the flows.

**Tech Tip**

Here are a few **show** and **clear** commands to keep handy for troubleshooting or viewing your NetFlow data from the switch. The below validation commands are for ingress (IN) flows. You may repeat the commands for egress (OUT) traffic.

Commands to display NetFlow data:

- `show flow record FLOW-RECORD1-IN`
- `show flow monitor FLOW-MONITOR1-IN statistics`
- `show flow monitor FLOW-MONITOR1-IN cache`
- `show flow exporter FLOW-COLLECTOR1-IN statistics`

Commands to reset NetFlow data:

- `clear flow record FLOW-RECORD1-IN`
- `clear flow monitor FLOW-MONITOR1-IN statistics`
- `clear flow monitor FLOW-MONITOR1-IN cache`
- `clear flow exporter FLOW-COLLECTOR1-IN statistics`
Procedure 2  Test network visibility

Step 1: Connect a wired or wireless client (example: iPad, PC or VM) to the NetFlow-enabled Network Device (example: 3850 switch, 8540 or 5520 WLC) Interface (example: Physical, or WLAN).

Step 2: Log in to ISE (example: ise.cisco.local).

Step 3: Navigate to Operations > Radius Livelog, and based on the Authentication method (example: 802.1X), make sure the user connects successfully and assigned appropriate SGT (example: Employee).

Step 4: Log in to the Stealthwatch web-client (example: smc.cisco.local).

Figure 11  Typical Stealthwatch dashboard

Tech Tip

In Stealthwatch 6.7.1, SMC Web GUI Dashboard, the Top Applications chart doesn’t show application names and it cannot be customized to show NBAR granularity at the moment.

The above figure represents a typical Stealthwatch dashboard based on an active flow collection for a longer duration. A newly installed setup will not be able to populate all the widgets as shown above. Refer to Stealthwatch documentation on creating Custom Events, which are security policies to trigger Alarms.
Step 5: Navigate to Network > Users and verify the authenticated username is shown.

![Image of Users page]

Step 6: Click a user name with suspicious activity to reveal more details, as shown below.

![Image of User info page]

**Tech Tip**

User information populates based on information provided by Active Directory, and the Devices and Sessions table lists all of the recent devices used, including active clients. Select a device IP address to further investigate.
Step 7: Under Host Summary, click the Quarantine button in order to mitigate a suspicious device.

**Tech Tip**

The Quarantine or Unquarantine button functions only if the MAC Address field is populated under Host Summary.

When you click Quarantine or Unquarantine from Stealthwatch, you may see a success or failure message. The result could actually be the opposite of what the message indicates, due to the response delay from ISE to Stealthwatch.

The failure message can also occur if you mandate that the client re-authenticate (ISE will timeout and send a fail message over the API), but in fact the quarantine was successful (that is, the EPS status was set to true and when the user logs in again, the device is quarantined).

Step 8: After the device can safely connect to the network, click Unquarantine.

Step 9: Under Host Summary, click View Flows and optionally edit the parameters. Click Review Query, and then click Run to start Flow Query and show the result.

Step 10: Click Launch SMC. The Java client opens.

**Tech Tip**

In Stealthwatch 6.7.1, visibility into applications is limited. Many TCP/UDP applications are tagged as "Undefined TCP/Undefined UDP," causing finer granularity to be lost within Apps/Services category. This is in spite of NBAR classification being active. This is expected to be fixed for the 6.8 release.

Step 11: To test application visibility, from the left pane, expand FlowCollectors > fc1 > Exporters, right-click a network device (example: WLC 5520/8540), and navigate to Flows > Flow Table. If AVC is enabled, adding the Application (NBAR) column displays the application/website (example: YouTube) being browsed.

You have now successfully deployed and tested the NaaS solution.

For more information about using Stealthwatch, refer to the Stealthwatch Management Console User’s Guide from the Stealthwatch download center.
Enabling Stealthwatch Learning Network License in Remote Site Networks

INTRODUCTION

Stealthwatch Learning Network License

The Stealthwatch Learning Network License system is a hyper-distributed analytics architecture that inspects your remote site network traffic and applies machine-learning algorithms to perform a behavioral analysis. As a result, the system can identify anomalous behaviors, such as malware, distributed botnets, data exfiltration, and more.

The SLNL is a tool with the ability to spot zero-day attacks and is not based on predefined signatures.

SLNL requires the deployment of a router based agent. You can deploy multiple agents to your network edge to inspect traffic. These agents report the anomalies in real-time to the controller for additional system and user analysis. Based on the anomalies, you can provide relevance feedback, which the system incorporates into internal traffic models. This allows the system to better tune how it identifies and reports anomalies of interest.

You can also configure mitigations based on anomaly properties, such as hosts involved and application traffic transferred. These mitigations reduce or eliminate the impact of detected anomalies. The combination of behavioral analysis, user feedback, and traffic mitigation customizes the system to address the threats specific to your network and better protect your users. In addition, the agents can provide PCAPs of raw packets involved in anomalies.

Tech Tip

SLNL agent in the container is not supported along with Snort IPS, WAAS, or any other app running in the container. Cisco is currently testing the capability to support SNORT and SLN in same container. For the latest information, see your Cisco account team.

COMPONENTS AT A GLANCE

Figure 12  SLNL Enable Remote Site Example
Controller: Stealthwatch Centralized Agent Manager

**Reader Tip**

SLNL Controller has also been referenced as *SCA* (Stealthwatch Centralized Agent Manager) in few places (example: code, log files, scripts). But the official name for SCA is *Controller*.

The Stealthwatch controller acts as the management center of the Learning Network License system. It collates anomalies sent by all managed agents and performs a real-time analysis based on severity rating and internal relevance to determine which are of most interest to the user. It then reports these for further user review and relevance feedback and displays various graphs and data (including raw packet captures) to assist user analysis of anomalies. In response, the user can configure mitigations that match an anomaly’s characteristics, including IP address or application, and take an action. The controller forwards these mitigation policies and actions to distributed agents in your remote site.

**Tech Tip**

Only anomalies and graph data are sent over the network to the controllers. All NetFlow data remains local to the router in order to save bandwidth over the WAN. Compressed raw packet captures for anomalies are sent over the WAN only if the customer requests via Controller GUI to import them.

You must deploy at least one controller on your network. A router based agent can be associated with one controller.

For more information about hardware requirements and installation, see Cisco Stealthwatch Learning Network License Install and Upgrade Guides.

Agent: Stealthwatch Distributed Learning Agent

**Reader Tip**

SLNL Agent has also been referenced as *DLA* (Stealthwatch Distributed Learning Agent) in few places (example: code, log files, scripts). But the official name for DLA is *Agent*.

Each agent, deployed either in a software container (LXC, Linux Container), in the memory of a Cisco ISR in your remote site network, or on a UCS E-Series Blade of an ISR, monitors the flow of data traversing your network. The agent inspects NetFlow data to identify hosts and uses NBAR to identify the applications over which the hosts transfer traffic. Based on this data, as well as Deep Packet Inspection of raw packets traversing the router, the agent develops a baseline traffic model and is then able to identify anomalous traffic.

Agents report the anomalies of most interest to the controller for further system analysis and user relevance feedback. Agents also receive user-initiated mitigations from the controller and install quality of service (QoS) policies (class maps, policy maps, and access lists) to drop traffic you have identified as anomalous. If the ISR detects traffic that matches the mitigation characteristics, it takes action on matching traffic to prevent future anomalies.

You may deploy at most one agent per ISR and up to 1000 agents in your Learning Network License network.

**NetFlow**

SLN agents use NetFlow along with deep packet inspection of raw packets to monitor traffic traversing remote site routers. NetFlow is enabled on remote site-facing interfaces (those leading to the remote site hosts); whereas raw packets are typically captured from core-facing interfaces (those leading to the Core, other remote sites, or the Internet).
Unusual-Time-of-Day Anomaly Use Case

This use case describes how an unusual-time-of-day anomaly is detected simply based on the fact that it is an unusual event. The security admin may (or may not) choose to take mitigation action to drop the anomalous traffic. Furthermore, the administrator may choose to click the thumbs up button to reinforce the fact that this was a useful detection, and this action encourages the system to focus even more on similar detection like this in the future.

BUSINESS PROBLEM

After the agent has learned the network patterns, clusters and traffic graphs are created. The agent detected that normal operation for an internal user is to send HTTP traffic to a known server in remote site 1 at 12pm each day. Agent 1 detects http traffic to known server during night hours and reports it as unusual time of day anomaly to the controller.

Figure 13  Malicious unusual-time-of-day anomaly
SOLUTION

A security administrator logs into the controller, reviews the anomaly, determines this is malicious activity by a botnet, and clicks the thumbs up icon to assign relevant feedback to the anomaly.

The controller sends the mitigation to agent 1, and agent 1 updates the host ISR’s configuration. As that traffic enters the ISR, it detects and drops the traffic.

Figure 14  Malicious unusual-time-of-day anomaly mitigation
New Edge Anomaly Use Case

This use case describes how an unexpected edge anomaly is detected simply based on the fact that it is an unusual event. The security admin may (or may not) choose to take mitigation action to drop the anomalous traffic. Furthermore, the administrator may choose to click the thumbs up button to reinforce the fact that this was a useful detection and this action encourages the system to focus even more on similar detection like this in the future.

**Tech Tip**

An unexpected edge means that traffic of this type was never seen before on the customer’s network.

**BUSINESS PROBLEM**

A host outside the remote site sends HTTP traffic to an FTP server in Remote Site 2, within the internet cluster. A host external to the remote site does not usually send HTTP traffic to the FTP server in the remote site. This triggers an unexpected edge anomaly (edge refers to traffic belonging to a specific application between 2 clusters of hosts).

*Figure 15  Malicious unexpected created-edge anomaly*
**SOLUTION**

A security administrator logs into the controller, reviews the anomaly from the inbox, and examines the internal host’s identity information (collected from ISE), as well as threat intelligence from Talos regarding the external host. The administrator determines this is malicious activity by someone attempting multiple failed login attempts. The administrator clicks the thumbs up icon to assign relevant feedback to the anomaly. The system incorporates this feedback into the DRL algorithms. The administrator then configures a mitigation to drop traffic from this malicious host to the FTP server.

*Figure 16  Malicious unexpected created-edge anomaly mitigation*
Unusual-Data-Transfer Anomaly Use Case

This use case describes how suspicious activity of a transfer with an unusual number of packets (small or large) generates an anomaly. Anomaly detection is based on learning what is normal, and then observing abnormal activity. Mitigation is an independent action a customer may take to ensure anomalous packets are dropped (not forwarded by the router). Lastly, the customer may provide feedback to the system, such as thumbs-up, to encourage the system to increase its focus on anomalies of this type.

BUSINESS PROBLEM

A known malicious host external to the remote site establishes an HTTP connection to HTTP servers in remote site 1, in the cluster, and closes the connection soon after establishing it. Agent 1 detects the traffic, a very small or large number of packets, and reports this anomaly to the controller.

Figure 17  Malicious unusually-small-number-of-packets anomaly
**SOLUTION**

A security administrator logs into the controller, reviews the anomaly from the inbox, and examines the internal host’s identity collected from ISE, as well as threat intelligence from Talos regarding the external hosts. The administrator determines this is malicious activity, an attempt to run the unauthorized script on the HTTP server, and clicks the thumbs up icon to assign relevant feedback to the anomaly. The system incorporates this feedback into the DRL algorithms. The administrator then configures a mitigation to drop traffic from the malicious host.

You may choose to export anomaly events to a centralized SIEM system (example: Splunk). If you do so, you don’t need to log into the controller to notice this event. Once you notice something on your centralized SIEM system, then log into the controller to get details and to mitigate.

*Figure 18  Malicious unusually-small-number-of-packets anomaly mitigation*

For more use-case scenarios, see the [Example Use Cases](#).
Design Overview

The Cisco Stealthwatch Learning Network License embeds security into the network infrastructure to improve visibility and threat detection for remote site offices. The solution turns the Cisco ISR Series (see Table 4) into a security sensor to monitor remote site traffic with NetFlow, NBAR, machine learning, and packet capture. Enabling traffic monitoring to be done at the remote site, this solution provides faster detection and response for remote site network threats. The Stealthwatch Learning Network License can be used alongside Stealthwatch to gain superior protection from network core to edge, and edge to edge.

Figure 19  Example network

The Stealthwatch Learning Network License is specifically designed to take advantage of the Cisco Integrated Services Routers and their Cisco IOS XE module architecture. It allows the agent to be installed as a software agent in Cisco IOS XE containers.

The agent can also be installed on a Cisco UCS E-Series blade. For more information, see SLNL UCS E-Series Server Installation Guide.

For the list of supported platforms, see Appendix B. For more information refer to the SLNL Data Sheet.

Tech Tip

You may optionally install a solid state drive (SSD) carrier and SSD network interface module (NIM-SSD, which is also supported) for the agent.
Deployment Details

This section describes a deployment based on the following design and deployment guides, which comprise the reference network architecture:

- Cisco Stealthwatch Learning Network License Configuration Guide
- Cisco Stealthwatch Learning Network License Virtual Service Installation Guide.

**Reader Tip**

For installation prerequisites and system configuration prerequisites for controller (manager) and agent, see Controller Installation Prerequisites.

### Deploying Cisco Stealthwatch Centralized Agent Manager

1. Install the controller
2. Configure controller and agent communications

Now that you have successfully integrated Cisco ISE and Stealthwatch SMC, you can proceed with deploying Stealthwatch controller VM, which can be on the same ESXi Host in the Datacenter as the Stealthwatch SMC, if desired.

#### Procedure 1 Install the controller

**Step 1:** Download and import the controller image (example: sln-sca-k9-1.1.ova).

**Step 2:** Start the VM and log in (username: sln and password: cisco).

**Step 3:** Change the password, enter current password (`cisco`), and enter the new password.

**Step 4:** When prompted, initiate setup.

```
sudo ./setup-system
```

**Step 5:** Start network setup.

```
Do you want to setup networking now? : y
```
Step 6: Select the interface.

Choose an interface to configure (example: eth0)

Enter a number : 1

Step 7: Configure the IP address, subnet mask, and default gateway.

Choose one of the following actions:

Enter an action : Ipv4
Enter new IPv4 address [] : 10.4.48.72
Enter new IPv4 netmask [] : 255.255.255.0
Enter new IPv4 gateway [] : 10.4.48.1
Is this correct? : y

Step 8: Configure the Hostname.

Choose one of the following actions:

Enter an action : hostname
Enter new hostname []: controller1.cisco.local
Is this correct? : y

Step 9: Configure the DNS.

Choose one of the following actions:

Enter an action : dns
Enter new DNS Servers []: 10.4.48.10
Is this correct? : y

Step 10: Exit interface Setup.

Choose one of the following actions:

Enter a number (To exit) : 4

Step 11: Enable SSH.

Do you want to enable SSH service now? : y

Step 12: Enable NTP.

Do you want to configure NTP servers now? : y
FQDNs or IP addresses: 10.4.48.17
Do you want to proceed with this change? : y

Step 13: Generate a Self-Signed Controller TLS Certificate.

Do you want to make a self-signed certificate for the SCA? : y
Step 14: Generate a SLN Data Visualization (VIZ) TLS Certificate.

Do you want to generate a different VIZ certificate? : y
Do you want to interactively specify the cert subject DN? : y
Country Name [] : US
State or Province Name [] : CA
Locality Name [] : SJC
Organizational Name [] : CISCO
Organizational Unit Name [] : CSG
Common Name [] : controller1.cisco.local
Email Address [] : local

sudo reboot

Step 15: Re-check everything (example: NTP, DNS) after reboot (Preferably access via SSH).

ntpq -p
nslookup controller1.cisco.local

**Tech Tip**

Make sure the controller1 record has been added to the DNS.

Step 16: In your browser, log in to the controller (example: https://controller1.cisco.local). Use admin and cisco, and follow the instructions to reset password.

**Tech Tip**

If you get a warning saying “Your username or pass phrase is invalid. Please try again. (Password expired),” follow the instructions on [Resetting the Administrator Password](#).
Procedure 2  Configure controller and agent communications

Step 1: In the editor, open the controller configuration file `sca.conf`.

```
sudo vi /opt/cisco/sln/sca/sca.conf
```

Step 2: Modify the configuration by removing # symbol from the following lines.

```
allowSelfSignedCert = true
trustCertOnFirstUse = true
```

Step 3: Save your changes and exit the editor.

```
Press Esc
Enter : wq!
Press Enter.
```

Step 4: Restart controller processes.

```
sudo service ciscosln-sca restart
```
Configuring Network Element (ISR)

1. Configure NTP
2. Install NBAR2

Before you run the agent easy install script, NTP must be configured on the router, which in this case is the network element.

Configure NTP server addresses on the ISR to synchronize time between the controller, agent, and ISR. When you deploy agents to your network using the install script, the install script also configures Flexible NetFlow.

**Tech Tip**

NTP synchronization between the controller, agents, and network elements is critical to the operation of SLN. In addition, DNS entries must be configured for controller, agents and network element.

**Procedure 1** Configure NTP

**Step 1:** Configure the NTP source interface.

```
ntp source Loopback0
```

**Tech Tip**

Based on your setup you may choose to use GigabitEthernet0/0/0 or management interface.

**Step 2:** Connect to an NTP server.

```
ntp server 10.4.48.17
```

**Tech Tip**

You may define multiple addresses to specify backup NTP servers.

**Step 3:** Check NTP status and make sure the clock is synchronized.

```
show ntp status
```
Procedure 2  Install NBAR2

Step 1: Verify protocol pack status and note the version number.

show ip nbar protocol-pack active

Active Protocol Pack:
Name: Advanced Protocol Pack
Version: 17.0
Publisher: Cisco Systems Inc.
NBAR Engine Version: 23
Creation time: Mon Feb 15 07:27:20 UTC 2016
State: Active

Step 2: If the version is 17 or higher, skip to step 3. Otherwise, install the protocol-pack from CCO.

configure terminal

Step 3: Verify NBAR version.

show ip nbar version

NBAR software version: 23
NBAR minimum backward compatible version: 21

Loaded Protocol Pack(s):

Name: Advanced Protocol Pack
Version: 17.0
Publisher: Cisco Systems Inc.
NBAR Engine Version: 23
Creation time: Mon Feb 15 07:27:20 UTC 2016
State: Active
**Tech Tip**

If the protocol pack state is shown In-Active, check the engine version. It must be version 23, or the correct IOS license is missing.

### Installing Agent Virtual Service Via Script

1. Download OVA file to controller
2. Update Agent Properties File settings
3. Run the install script
4. Verify resulting NE configuration added via script
5. Configure agent container via controller WebGUI
6. Enable mitigation interface
7. Implement post-learning phase
8. Manually create a mitigation policy
9. Review network element CLI

Before you deploy your agents as virtual services, ensure that your ISRs have enough RAM and that the proper hardware installed, as described in [ISR 4000 Series Platform Requirements](#).

When you run the install script successfully, it should automatically take care of the following:

- Upload the OVA (example: sln-dla.ova) file to the ISR (network element)
- Configure Flexible NetFlow.
- Configure a virtual service (container) named `sln` and deploy the agent.
- Configure ISR and agent network settings.
- Add the new agent to the controller.

**Procedure 1**  
**Download OVA file to controller**

**Step 1:** On the [SLNL software download](#) page, download the agent OVA file (example: sln-dla-isr4k-cont-250Ms-3Gr-k9-1.1.ova).

**Step 2:** Upload to the controller.
**Tech Tip**

Upload the OVA to the controller using an SFTP client (example: FileZilla). The agent deployed in the test lab is a virtual service on an ISR’s bootflash (example: sln-dla-isr4k-cont-250Ms-3Gr-k9-1.1.ova), but you may also deploy it as a virtual service on a NIM-SSD (example: sln-dla-isr4k-cont-150Ms-3Gr-k9-1.1.ova).

**Procedure 2** Update Agent Properties File settings

**Tech Tip**

The Agent Properties File install.yaml is already on the controller, at following path:

```
/opt/cisco/sln/install_upgrade/container
```

The controller includes an agent install and upgrade properties file (install.yaml), and the agent install script (installation_auto.py). Running the agent install script requires configuring the agent install and upgrade properties file with agent, ISR, and network settings. You can configure the file to deploy multiple agents at one time. This file contains global settings, which apply to all deployed agents, and remote site-specific settings, which apply only to one ISR and agent.

**Tech Tip**

Details of each parameter can be found on the top section of the install.yaml file. You can find additional parameters in the comments that may be useful in your deployment, which is not mentioned below.

Step 1: Navigate to the /container directory.

```
cd /opt/cisco/sln/install_upgrade/container
```

Step 2: Copy the install.yaml.example file to install.yaml.

```
cp install.yaml.example install.yaml
```

**Tech Tip**

Make sure you copy (cp) and not rename (mv), because you might need to do it again in case you are unable to run and get the following message:

```
ERROR: Yaml parsing error:
ERROR: while parsing a block mapping
```

Step 3: Open the install.yaml install and upgrade properties file in the vi text editor.

```
vi install.yaml
```
Step 4: Update the OVA download location.

dla_ova_copy:
    src_host: 10.4.48.72
    src_username: [username]
    src_password: [password]
    src_ova_path: "[path]"
    dst_store: bootflash

Tech Tip
The recommended location is on the controller (Example: /home/sln/sln-dla-isr4k-cont-250Ms-3Gr-k9-1.1.ova) but can also be pointed to an FTP server. The location must be reachable by NE (example: ISR). Double-check the OVA path and file name, because it will change based on the code version.

Step 5: Update the VirtualPortGroup interfaces configuration.

Figure 21  Zoomed-in view of agent virtual interfaces on NE

vir_portgroup_1:
    ip_unnum: Loopback0

Tech Tip
For vir_portgroup_1 (Vi1), this design tested ip_unnum (internal) interface as Loopback0 and assigned a Loopback IP address. Based on your setup, you may decide to use GigabitEthernet0/0/0 or any other interface with an available address from its subnet and assign an internal routable ip-address instead. More information provided in Step 10.

vir_portgroup_2:
    ne_ip: 192.0.2.1
    ne_mask: 255.255.255.0
dla_dat_ip: 192.0.2.2
dla_dat_mask: 255.255.255.0
**Tech Tip**

Vir_portgroup_2 can have private addresses. It is internal and not advertised anywhere else except for agent & router (NE), so you can leave the default settings, as well.

**Step 6:** Enter credentials for ISR (NE).

    ne_username: admin
    ne_password: [password]

**Step 7:** Enter credentials for the agent to communicate with NE (ISR). In most cases, this should be the same as the credentials used in Step 6.

    dla_ne_login:
      username: admin
      password: [password]

**Step 8:** Enter credentials for the controller WebUI.

    sca_webui_login:
      username: admin
      password: [password]

**Step 9:** Enter credentials for the agent.

    dla_password: [password]
    dla_ssh_enable: yes

**Step 10:** Configure one or more remote site specific property settings.

    # Branch 1:
      - dla_hostname: agent1.cisco.local
        ne_ctl_ip: 10.255.242.9
        dla_ctl_ip: 10.255.242.10
        dla_ctl_mask: 255.255.255.252
        dla_ctl_gw: 10.255.242.9
        ne_netflow_interfaces:
          ifnames: ['Gi0/0/0.10','Gi0/0/0.11','Gi0/0/0.12']
**Tech Tip**

For dla_hostname, make sure the correct name is added to the DNS and also updated in the install.yaml script.

If you decide on using Loopback interface for unnumbered interface, in most cases you need to change the subnet from /32 to /30 so that you can have two addresses derived, one for net_ctl_ip and another for dla_ctl_ip.

Whether you decide to use Loopback0 or GigabitEthernet0/0/0 (assign internal routable ip-address), check if it’s pingable.

```
ping 10.4.48.72 source loopback0
```

where 10.4.48.72 is the controller, and loopback0 is the interface. In your case, it might be GigabitEthernet0/0/0.

For ne_ctl_ip, use the same IP address used for the interface Loopback0 on the NE.

For dla_ctl_ip, use the IP address used for the interface Loopback0 on the NE.

Flexible NetFlow is enabled on internal interfaces. This happens automatically when using a container-based agent, and you should not configure FNF manually. The FNF configuration must match exactly what the agent is expecting; hence it is auto-configured by the installer. It is auto-configured on all interfaces that you identify (in .yaml file) as remote site facing interfaces.

**Step 11:** For ifnames (Internal Interface), use GigabitEthernet sub-interface or Port-channel sub-interfaces (Port-channel1.10), based on your setup. Currently Port-channel only supports monitoring. Port-channels and most Tunnels don’t support mitigation.

Upon successful execution of the script, NetFlow will be configured on the specified (recommended internal) interfaces.

---

**Procedure 3 Run the install script**

**Step 1:** Navigate to the /container directory

```
cd /opt/cisco/sln/install_upgrade/container
```

**Step 2:** Run the installation_auto.py install script.

```
Sudo ./installation_auto.py -c install.yaml
```

**Step 3:** Provide passwords when prompted.

After successful execution of the script, similar result should display with the Succeeded count changed from 0 to 1, as shown in the figure below.

```
cd /opt/cisco/sln/install_upgrade/container
sudo ./installation_auto.py -c install.yaml
```
Tech Tip

If the script fails, you will see Failed:1 instead of Succeeded:1, and then you must check the logs under /opt/cisco/sln/install_upgrade/container/LOGS

For more information, see Install and Upgrade Guides.

Procedure 4  Verify resulting NE configuration added via script

Step 1: Check the VirtualPortGroup1 interfaces configuration.

    show running-config interface VirtualPortGroup1

Example

    interface VirtualPortGroup1
    ip unnumbered Loopback0
    no mop enabled
    no mop sysid
end

Step 2: Check the VirtualPortGroup2 interfaces configuration.

    show running-config interface VirtualPortGroup2
**Example**

```plaintext
interface VirtualPortGroup2
  ip address 192.0.2.1 255.255.255.0
  no mop enabled
  no mop sysid
end
```

**Step 3:** Show the IP route VirtualPortGroup1 interfaces configuration.

```plaintext
show running-config | inc ip route
```

**Example**

```plaintext
ip route 10.255.242.10 255.255.255.255 VirtualPortGroup1
```

**Step 4:** Check the Virtual-Service list.

```plaintext
show virtual-service list
```

**Example**

```plaintext
Virtual Service List:
Name     Status        Package Name
-----------------------------------------------------------
sln      Activated     sln-dla-isr4k-...
```

**Step 5:** Verify NetFlow Configuration: Flow Record.

```plaintext
show running-config flow record
```

**Example**

```plaintext
flow record SLN-NF-RECORD
  match ipv4 protocol
  match ipv4 source address
  match ipv4 destination address
  match transport source-port
  match transport destination-port
  collect datalink mac source address input
  collect datalink mac destination address output
  collect transport tcp flags
  collect interface input
  collect interface output
  collect flow direction
  collect counter bytes
```
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
collect application name
collect routing forwarding-status


show running-config flow exporter

Example
flow exporter SLN-NF-EXPORTER
destination 10.255.242.10
transport udp 2500
template data timeout 30


show running-config flow monitor

Example
flow monitor SLN-NF-MONITOR
exporter SLN-NF-EXPORTER
cache timeout active 60
cache entries 500000
record SLN-NF-RECORD


show running-config interface Gi0/0/0.10

Example
interface Gi0/0/0.10
encapsulation dot1Q 99
ip address 10.7.0.9 255.255.255.252
ip pim sparse-mode
ip flow monitor SLN-NF-MONITOR input
ip flow monitor SLN-NF-MONITOR output
delay 25000
end
**Tech Tip**

After you run the install script, you can register Smart Licensing on your controller and then enable the managed agents. For more information, see [Agent Management](#).

---

**Procedure 5**  Configure agent container via controller WebGUI

FNF is enabled on internal interfaces, while mitigation is enabled on all supported interfaces and packet buffer capture (PBC) is enabled on external interfaces, as shown in the below figure.

**Figure 23**  Network element interfaces

---

**Option 1: Select interface direction**

**Step 1:** In your browser, open the controller at https://controller1.cisco.local

**Step 2:** On the AGENTS tab, activate the agent listed by clicking **Enable**.

**Step 3:** Click **Continue**, and then confirm license usage.

**Step 4:** Click **Configure**, and then select the appropriate interfaces **Direction** from the drop-down.

- **Internal:** Select if the interface faces the remote site (NetFlow enabled interface).
- **External:** Select if the interface faces the Core (Traversing traffic interface).
- **Unconfigured:** Select if the interface is unused or faces neither.

**Option 2: Enable DPI/DNS/PBS on the interface**

Raw packet capture should be enabled on all external interfaces (unless unsupported). If it is not supported on all external interfaces, then it should be enabled on all internal interfaces. This is a manual operation—raw packet capture is disabled by default. You must enable it and then select the interfaces on which raw packets should be captured.

**Tech Tip**

When PBC is enabled on all interfaces, duplicate packet capture may occur.
If you want the ability to see raw packets captured for anomalies, enable the PBC feature. To enable the agent to perform DPI on raw packets traversing the router, and to provide enhanced anomaly detection, enable the DNS/DPI feature. Both of these features rely on the agent receiving a copy of raw packets traversing the router.

Step 1: Scroll-down and select Enable DPI/DNS (Global option) to enable raw packet capture.

**Tech Tip**

Monitoring interfaces will perform raw packet capture for the traffic.

Step 2: Select Enable PBC.

Step 3: In the Raw Packet Tx Interface (on NE) list, select VirtualPortGroup2 interface, on which the network element passes raw packets to the agent.

Step 4: In the Raw Packet Rx Interface (on Agent) list, select eth1 interface, on which the agent receives raw packets from the network element.

![Configuration Options](image)

**Tech Tip**

The configuration shown here is for container-based agents. The agent can also be installed on a Cisco UCS E-Series blade. For more information, see SLNL UCS E-Series Server Installation Guide.

Step 5: Scroll-up and in the Use for Raw Packet Capture column, select Enable PBC/DPI, next to an External interface (Example: Gi0/0/1, see figure 22).

Step 6: Click Submit. The status should change to Learning and it will take minimum of 7 days before the status changes to Ready. During this time, the SLNL is learning the traffic patterns and the network itself.
Procedure 6 Enable mitigation interface

Mitigation must be enabled on all supported interfaces of the network element, and the unsupported interfaces are grayed out in the controller WebGUI. This allows the agent to install an input-drop policy on all of these interfaces in the case you want to mitigate an anomaly.

**Step 1:** In your browser, open the controller at https://controller1.cisco.local

**Step 2:** On the AGENTS tab, next to the agent, click **Configuration**

**Step 3:** In the Use for Mitigation column, select **Enable mitigation**, next to all supported interface (example: Interface Gi0/0/1 and Gi0/0/0)

```
<table>
<thead>
<tr>
<th>Network Element Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>GigabitEthernet0/0/1</td>
</tr>
<tr>
<td>GigabitEthernet0/0/0</td>
</tr>
</tbody>
</table>
```

**Tech Tip**

SLN currently does not support mitigation on DMVPN tunnel interfaces. This will be resolved in a future software release.

**Step 4:** Click **Save**.

Procedure 7 Implement post-learning phase

Each agent learns independently. After the status (per agent) changes to **Ready** after running for 7 days (traffic-dependent), the SLNL has completed learning the traffic patterns and built a baseline traffic model. The model includes dynamically-generated clusters of hosts and what types of application traffic are transmitted between clusters at what times of day.

The system is smart and tries not to trigger false-positives. Deviations from the normal baseline model result in anomalies, whereas deviations that are considered within normal ranges do not trigger anomalies.

The system identifies anomalies by comparing observed traffic to the baseline model and noting deviations. After system deployment, each agent inspects traffic traversing its remote site router.

**Step 1:** In your browser, open the controller at https://controller1.cisco.local
Step 2: Click INBOX, and then check the anomalies reported.

Step 3: (Optional) Review the reported anomalies carefully and give feedback by selecting thumbs-up (accept) or thumbs-down (reject) to customize machine learning per your network.

Step 4: To drill down further, click the link in Description column.

Step 5: In the top-right corner, click Get PCAP files to send a request to the agent and request any PCAP files created during the anomaly detection.

Step 6: Click Download to save the file file_name.pcap.gz, which contains raw traffic details, including information related to the anomaly.

Step 7: (Optional) Open the PCAP file in Wireshark to further analyze the traffic related to reported anomaly.
**Tech Tip**

PCAP file is compressed (.gz), and it should not add extra load on WAN traffic. The largest PCAP file size (prior to compression) is 10MB.

Figure 24  Example of PCAP file opened in Wireshark

Step 8: If you identify suspicious activity, to review and modify the forward and reverse mitigation policy, scroll down and under Mitigate, click Mitigate this anomaly.
Step 9: To save, click Create mitigation policies.

Tech Tip

By default, mitigation from anomaly is bidirectional.

Step 10: Click the MITIGATION tab. You can see that policies are being applied.

Step 11: Click Partial to see the policy application is in process. After the process completes, you can see the policy is installed, and you can delete the policy here if necessary, as well.
**Tech Tip**

When you remove individual mitigations, only the ACL is removed from the network element and the rest stay inside the CLI.

**Procedure 8** Manually create a mitigation policy

(Optional)

Step 1: On the MITIGATION tab, click **Create mitigation**.

Step 2: Enter the agent name. (Example: agent1.cisco.local)

**Tech Tip**

You can apply mitigation to multiple agents at the same time.

Step 3: Select IP Protocol. (Example: TCP)

Step 4: Enter a source ip or subnet, or leave it as default (Any) to match on all source IP addresses.

**Tech Tip**

You can only define a subnet mask if you defined an IP address.

Step 5: Enter a source port or range, or leave it as default (Any) to match on all source ports.

**Tech Tip**

You must define a source IP address to define a source port.

Step 6: If you want to match a destination IP address or subnet, enter a destination IP or subnet, or enter Any to match on all source IP addresses. You can only define a subnet mask if you defined an IP address.

Step 7: If you want to match on a destination port, enter a destination port, or enter Any to match on all source ports. You must define a source IP address to define a source port.

Step 8: On the list, choose an IP protocol.

Step 9: Define duration for the mitigation.

Step 10: Click **Create mitigation**.
Step 11: (Optional) If you want to completely remove SLN mitigation configuration, click Delete all mitigations.

Procedure 9  Review network element CLI

The mitigation policy adds any existing service policy to the new policy created for mitigation.

NE (Router) Policy Example—Before Mitigation Applied

```
ip access-list extended DNS
   permit tcp any eq domain any
   permit tcp any any eq domain
ip access-list extended EMAIL
   permit tcp any any eq smtp
   permit tcp any eq smtp any
   permit tcp any any eq 143
   permit tcp any eq 143 any
ip access-list extended SIP
   permit tcp any any eq 5060
   permit tcp any eq 5060 any
   permit udp any any eq 5060
   permit udp any eq 5060 any
ip access-list extended TELNET
   permit tcp any any eq telnet
   permit tcp any eq telnet any
ip access-list extended VIDEO
   permit udp any any eq 554
   permit udp any eq 554 any
ip access-list extended WEB
   permit tcp any any eq www
   permit tcp any eq www any
   permit tcp any any eq 443
   permit tcp any eq 443 any
   class-map match-all TELNET
```
match access-group name TELNET
class-map match-all SIP
  match access-group name SIP
class-map match-all EMAIL
  match access-group name EMAIL
class-map match-all WEB
  match access-group name WEB
class-map match-all VIDEO
  match access-group name VIDEO
class-map match-all DNS
  match access-group name DNS
policy-map MARKING
  class SIP
    set dscp ef
class VIDEO
  set dscp af41
class TELNET
  set dscp af32
class EMAIL
  set dscp af33
class WEB
  set dscp cs1
interface GigabitEthernet0/0/1
  ip address 10.200.2.5 255.255.255.252
  media-type rj45
  speed 1000
  no negotiation auto
  service-policy input MARKING
end

NE (Router) Policy Example—After Mitigation Applied
ip access-list extended DNS
  permit tcp any eq domain any
  permit tcp any any eq domain
ip access-list extended EMAIL
  permit tcp any any eq smtp
permit tcp any eq smtp any
permit tcp any any eq 143
permit tcp any eq 143 any
ip access-list extended SIP
permit tcp any any eq 5060
permit tcp any eq 5060 any
permit udp any any eq 5060
permit udp any eq 5060 any

ip access-list extended SLN DR in GigabitEthernet0/0/1
permit tcp host [source-ip] host [destination-ip]
pemit tcp host 10.200.20.10 host 10.250.10.30

ip access-list extended TELNET
permit tcp any any eq telnet
permit tcp any eq telnet any
ip access-list extended VIDEO
permit udp any any eq 554
permit udp any eq 554 any
ip access-list extended WEB
permit tcp any any eq www
permit tcp any eq www any
permit tcp any any eq 443
permit tcp any eq 443 any
class-map match-all TELNET
    match access-group name TELNET

class-map match-any SLN DR in GigabitEthernet0/0/1
    match access-group name SLN DR in GigabitEthernet0/0/1

class-map match-all SIP
    match access-group name SIP
class-map match-all EMAIL
    match access-group name EMAIL
class-map match-all WEB
    match access-group name WEB
class-map match-all VIDEO
 match access-group name VIDEO
class-map match-all DNS
 match access-group name DNS
policy-map MARKING
 class SIP
   set dscp ef
 class VIDEO
   set dscp af41
 class TELNET
   set dscp af32
 class EMAIL
   set dscp af33
 class WEB
   set dscp cs1

policy-map SLN_in_GigabitEthernet0/0/1
 description MARKING
 class SLN_DR_in_GigabitEthernet0/0/1
 police rate percent 100
  conform-action drop
  exceed-action drop
  violate-action drop

class SIP
   set dscp ef
 class VIDEO
   set dscp af41
 class TELNET
   set dscp af32
 class EMAIL
   set dscp af33
 class WEB
   set dscp cs1

interface GigabitEthernet0/0/1
Deployment Details

```
ip address 10.200.2.5 255.255.255.252
media-type rj45
speed 1000
no negotiation auto
service-policy input SLN_in_GigabitEthernet0/0/1
end
```

**Tech Tip**

For each interface that is enabled for mitigation, the same service policy is applied as in G0/0/1.

After the mitigation expires or it is manually removed, only the ACL is removed from CLI.

```
ip access-list extended DNS
 permit tcp any eq domain any
 permit tcp any any eq domain
ip access-list extended EMAIL
 permit tcp any any eq smtp
 permit tcp any eq smtp any
 permit tcp any any eq 143
 permit tcp any eq 143 any
ip access-list extended SIP
 permit tcp any any eq 5060
 permit tcp any eq 5060 any
 permit udp any any eq 5060
 permit udp any eq 5060 any
ip access-list extended SLN_DR_in_GigabitEthernet0/0/1
```

**Tech Tip**

Notice the empty ACL.

```
ip access-list extended TELNET
 permit tcp any any eq telnet
 permit tcp any eq telnet any
ip access-list extended VIDEO
 permit udp any any eq 554
 permit udp any eq 554 any
ip access-list extended WEB
```
permit tcp any any eq www
permit tcp any eq www any
permit tcp any any eq 443
permit tcp any eq 443 any

class-map match-all TELNET
  match access-group name TELNET

class-map match-any SLN_DR_in_GigabitEthernet0/0/1
  match access-group name SLN_DR_in_GigabitEthernet0/0/1

class-map match-all SIP
  match access-group name SIP

class-map match-all EMAIL
  match access-group name EMAIL

class-map match-all WEB
  match access-group name WEB

class-map match-all VIDEO
  match access-group name VIDEO

class-map match-all DNS
  match access-group name DNS

aU27-4451-2#sh run | sec policy

policy-map MARKING
  class SIP
    set dscp ef
  class VIDEO
    set dscp af41
  class TELNET
    set dscp af32
  class EMAIL
    set dscp af33
  class WEB
    set dscp cs1
**Tech Tip**

After the first mitigation is created on an agent’s router, SLN creates QoS policies (example: access-lists, class-maps, policy-maps) with the prefix SLN_DR_in_<interface-name>. These refer to SLN Drop Input configuration for each interface on which mitigation is enabled. This allows the agent to re-use this configuration if future mitigations are created or removed (by just modifying the access-lists). If all mitigations are removed, the commands related to QoS policies are removed.

```cpp
policy-map SLN_in_GigabitEthernet0/0/0
description MARKING
class SLN_DR_in_GigabitEthernet0/0/0
   police rate percent 100
   conform-action drop
   exceed-action drop
   violate-action drop

class SIP
   set dscp ef
class VIDEO
   set dscp af41
class TELNET
   set dscp af32
class EMAIL
   set dscp af33
class WEB
   set dscp cs1

interface GigabitEthernet0/0/1
   ip address 10.200.2.5 255.255.255.252
   media-type rj45
   speed 1000
   no negotiation auto
   service-policy input SLN_in_GigabitEthernet0/0/0
end
```
## Appendix A: Product List for StealthWatch

The following products and software versions have been validated for Stealthwatch in this CVD.

### STEALTHWATCH

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product</th>
<th>License Entitlement</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco SMC Server</td>
<td>Stealthwatch Management Console Virtual Edition</td>
<td>L-LC-SMC-VE-K9</td>
<td></td>
</tr>
</tbody>
</table>

### IDENTITY MANAGEMENT

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product</th>
<th>Part Numbers</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ISE Server</td>
<td>Cisco Identity Services Engine Virtual Appliance</td>
<td>ISE-VM-K9=</td>
<td>2.0.0.306 Cumulative Patch 2</td>
</tr>
<tr>
<td></td>
<td>Cisco Identity Services Engine 10000 EndPoint Base License</td>
<td>L-ISE-BSE-10K=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Identity Services Engine 5000 EndPoint Base License</td>
<td>L-ISE-BSE-5K=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Identity Services Engine 3500 EndPoint Base License</td>
<td>L-ISE-BSE-3500=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Identity Services Engine 2500 EndPoint Base License</td>
<td>L-ISE-BSE-2500=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Identity Services Engine 1500 EndPoint Base License</td>
<td>L-ISE-BSE-1500=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Identity Services Engine 1000 EndPoint Base License</td>
<td>L-ISE-BSE-1K=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Identity Services Engine 500 EndPoint Base License</td>
<td>L-ISE-BSE-500=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Identity Services Engine 250 EndPoint Base License</td>
<td>L-ISE-BSE-250=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco Identity Services Engine 100 EndPoint Base License</td>
<td>L-ISE-BSE-100=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ISE 10K Endpoint Plus Subscription License</td>
<td>L-ISE-PLS-S-10K=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ISE 5K Endpoint Plus Subscription License</td>
<td>L-ISE-PLS-S-5K=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ISE 3500 Endpoint Plus Subscription License</td>
<td>L-ISE-PLS-S-3500=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ISE 2500 Endpoint Plus Subscription License</td>
<td>L-ISE-PLS-S-2500=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ISE 1500 Endpoint Plus Subscription License</td>
<td>L-ISE-PLS-S-1500=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ISE 1K Endpoint Plus Subscription License</td>
<td>L-ISE-PLS-S-1K=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ISE 500 Endpoint Plus Subscription License</td>
<td>L-ISE-PLS-S-500=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ISE 250 Endpoint Plus Subscription License</td>
<td>L-ISE-PLS-S-250=</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ISE 100 Endpoint Plus Subscription License</td>
<td>L-ISE-PLS-S-100=</td>
<td></td>
</tr>
</tbody>
</table>
### LAN ACCESS LAYER

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product</th>
<th>Part Numbers</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stackable Access Layer Switch</td>
<td>Cisco Catalyst 3850 Series Stackable 48 Ethernet 10/100/1000 PoE+ ports</td>
<td>WS-C3850-48F</td>
<td>3.6.4.E(15.2.2E4) IP Base license</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 3850 Series Stackable 24 Ethernet 10/100/1000 PoE+ Ports</td>
<td>WS-C3850-24P</td>
<td>3.6.4.E(15.2.2E4) IP Base license</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 3850 Series 2 x 10GE Network Module</td>
<td>C3850-NM-2-10G</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 3850 Series 4 x 1GE Network Module</td>
<td>C3850-NM-4-1G</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 2960-X Series 24 Ethernet 10/100/1000 PoE+ Ports (2 SFP+)</td>
<td>WS-C2960X-24PD-L</td>
<td>15.2.5E1</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 2960-X Series 24 Ethernet 10/100/1000 PoE+ Ports (4 SFP)</td>
<td>WS-C2960X-24PS-L</td>
<td>15.2.5E1</td>
</tr>
</tbody>
</table>

### WIRELESS LAN CONTROLLERS

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product</th>
<th>Part Numbers</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>On Site Controller</td>
<td>Cisco 5520 Series Wireless Controller for up to 50 Cisco access points</td>
<td>AIR-CT5520-50-K9</td>
<td>8.2.100.0</td>
</tr>
<tr>
<td></td>
<td>Cisco 5520 Wireless Controller 100 AP License</td>
<td>LIC-CTS5520-100A</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Cisco 5520 Wireless Controller 50 AP License</td>
<td>LIC-CTS5520-50A</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Cisco 5520 Wireless Controller 1 AP Adder License</td>
<td>LIC-CT5520-1A</td>
<td>–</td>
</tr>
<tr>
<td>On Site Controller</td>
<td>Cisco 8540 Wireless Controller supporting 1000 access points</td>
<td>AIR-CT8540-1K-K9</td>
<td>8.2.100.0</td>
</tr>
<tr>
<td></td>
<td>Cisco 8540 Wireless Controller</td>
<td>AIR-CT8540-K9</td>
<td>–</td>
</tr>
<tr>
<td></td>
<td>Cisco 8540 Wireless Controller 1 AP Adder License</td>
<td>LIC-CT8540-1A</td>
<td>–</td>
</tr>
</tbody>
</table>
Appendix B: Product List for StealthWatch Learning Network License

The following products and software versions have been validated for Stealthwatch Learning Network License in this CVD.

### ISR PLATFORMS

<table>
<thead>
<tr>
<th>Product Family</th>
<th>Platforms Supported</th>
<th>License</th>
<th>Cisco IOS Images</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISR 4000 Series</td>
<td>Cisco 4331</td>
<td>SL-4330-IPB-K9, SL-4330-APP-K9</td>
<td>3.16.3S (15.5.3.S3)</td>
</tr>
<tr>
<td>Cisco 4351</td>
<td>SL-4350-IPB-K9, SL-4350-APP-K9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco 4431, 4451</td>
<td>SL-44-IPB-K9, and SL-44-DATA-K9 or SL-44-APP-K9</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISR 2900 Series</td>
<td>Cisco 2921, 2951 with UCS E-Series blade (UCS-E140S-M2/K9)</td>
<td>SL-29-IPB-K9, SL-29-DATA-K9</td>
<td></td>
</tr>
</tbody>
</table>

NBAR2 Protocol Pack Version 17.0.0 or greater
## STEALTHWATCH LEARNING NETWORK LICENSE

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Product</th>
<th>License Entitlement</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller</td>
<td>Stealthwatch Learning Network License Manager</td>
<td>L-SW-SCA-K9</td>
<td>1.1</td>
</tr>
<tr>
<td>Agent</td>
<td>Agent deployed as a virtual service on an ISR 43XX (1 year term)</td>
<td>L-SW-LN-43-1Y-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Agent deployed as a virtual service on an ISR 43XX (3 year term)</td>
<td>L-SW-LN-43-3Y-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Agent deployed as a virtual service on an ISR 44XX (1 year term)</td>
<td>L-SW-LN-44-1Y-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Agent deployed as a virtual service on an ISR 44XX (3 year term)</td>
<td>L-SW-LN-44-3Y-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Agent installed on a UCS E-Series blade server</td>
<td>L-SW-LN-UCS-1Y-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(1 year term)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Agent installed on a UCS E-Series blade server</td>
<td>L-SW-LN-UCS-3Y-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(3 year term)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Glossary

Agent  Stealthwatch Distributed Learning Agent (or DLA)
C&C server  command and control server
CA  certificate authority
CoA  Change of Authorization
CSR  certificate-signing request
Cisco ISE  Cisco Identity Service Engine
Cisco ISR  Cisco Integrated Services Router
Cisco NaaS  Cisco Network as a Sensor
Cisco pxGrid  Cisco Platform Exchange Grid
Controller  Stealthwatch Centralized Agent Manager (or SCA)
DNS  Domain Name System
DPI  deep packet inspection
DRL  distributed relevance learning
DLA  Stealthwatch Distributed Learning Agent (or Agent)
FC  Flow Collector
FNF  Flexible NetFlow
IOT  Internet of Things
ISE  Cisco Identity Service Engine
ISR  Cisco Integrated Services Router
MnT  Monitoring and Troubleshooting Node
NaaS  Cisco Network as a Sensor
NBAR  Network-Based Application Recognition
NTP  network time protocol
PAN  Policy Administration Node
PBC  Packet Buffer Capture
PKI  public key infrastructure
POS  point of sale
PSN  Policy Service Node
pxGrid  Cisco Platform Exchange Grid
QoS  quality of service
SCA  Stealthwatch Centralized Agent Manager (or Controller)
SGTs  Security Group Tags
SLNL  Stealthwatch Learning Network License
SMC  Stealthwatch Management Console
SSD  solid state drive
WLC  wireless LAN controller
You can use the feedback form to send comments and suggestions about this guide.