Encrypted Traffic Analytics Non-Fabric

Prescriptive Deployment Guide

October, 2019

Table of Contents

Introduction

About The Solution

The rapid rise in encrypted traffic is changing the threat landscape. As more businesses become digital, a significant number of services and applications are using encryption as the primary method of securing information. Encrypted traffic has increased by more than 90 percent annually

Encryption technology has enabled much greater privacy and security for enterprises and individuals that use the Internet to communicate and transact business online. Mobile, cloud, and web applications rely on well implemented encryption mechanisms that use keys and certificates to ensure security and trust. However, businesses are not the only ones to benefit from encryption. Threat actors have leveraged these same benefits to evade detection and to secure their malicious activities.

Traditional flow monitoring, as implemented in the Cisco® Network as a Sensor (NaaS) solution and through the use of Flexible NetFlow (FNF), provides a high-level view of network communications by reporting the addresses, ports, and byte and packet counts of a flow. In addition, intraflow metadata, or information about events that occur inside of a flow, can be collected, stored, and analyzed within a flow monitoring framework. This data is especially valuable when traffic is encrypted, because deep-packet inspection is no longer viable. This intraflow metadata, called Encrypted Traffic Analytics (ETA), is derived by using new data elements or telemetry that is independent of protocol details, such as the lengths and arrival times of packets within a flow. These data elements have the property of applying equally well to both encrypted and unencrypted flows.

ETA focuses on identifying malware communications in encrypted traffic through passive monitoring, the extraction of relevant data elements, and supervised machine learning with cloud-based global visibility.

ETA extracts two main data elements: the Initial Data Packet (IDP) and the Sequence of Packet Length and Time (SPLT).

✍ For more information about Encrypted Traffic Analytics, see the complete ETA white paper.

What is Covered in This Document

This document provides guidance on deploying ETA and NaaS configuration to routers and switches without the assistance of Cisco DNA Center in a Non-Fabric environment.

What is Not Covered in This Document

This guide does not address the initial deployment of Cisco Stealthwatch. This guide also does not go in depth into the design of the solution, instead that will be in the new, consolidated ETA Design Guide.

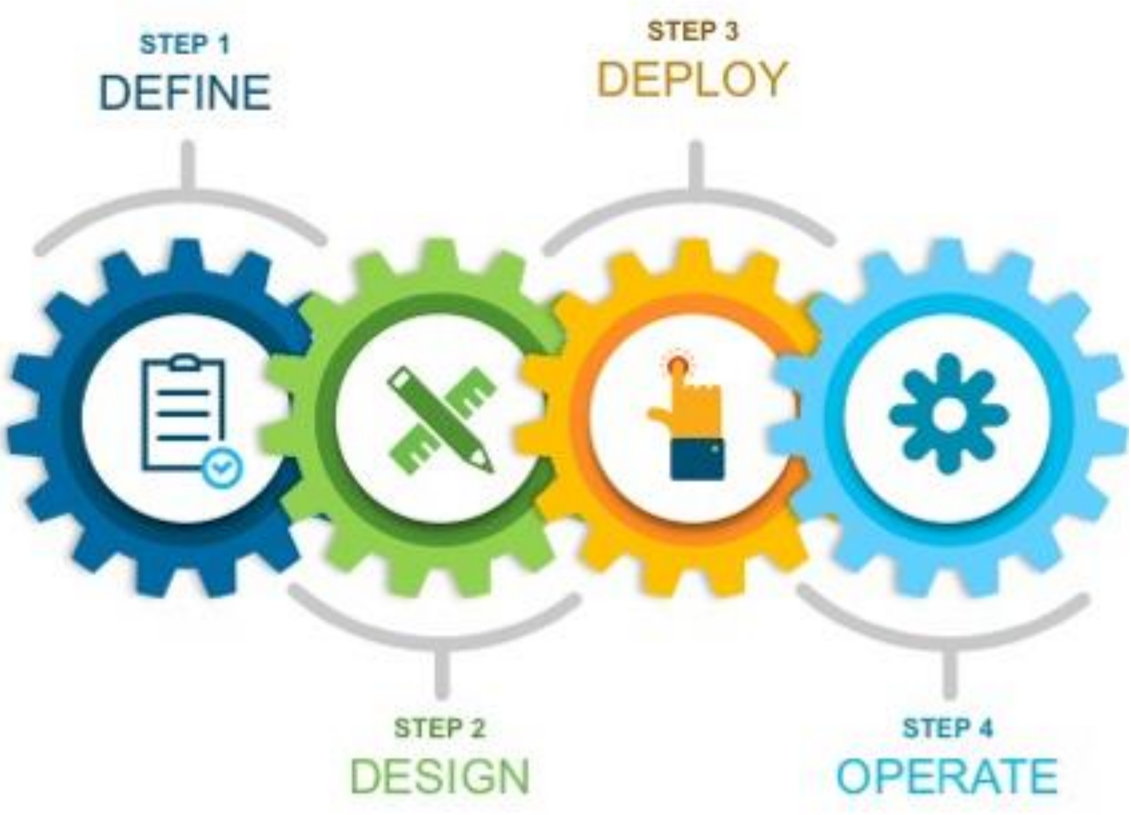


Figure 1 Implementation Flow

This document contains four major sections:

- The **Define** section defines problem areas and provides information about how to plan for deployment, and other considerations.
- The **Design** section provides you with high level guidance for deciding where to deploy both ETA and FNF.
- The **Deploy** section provides information about various configuration and best practices.
- The **Operate** section shows how to use and troubleshoot the solution.

Define

1. This section provides a high level overview of the ETA and Stealthwatch solution as well as its components.

ETA Deployment Components

NetFlow

NetFlow is a standard that defines data elements exported by network devices that describe the “conversations” on the network. NetFlow is unidirectional, and each device on the network can export different NetFlow data elements. When processed, NetFlow data can tell you the important details in network transactions involving data communication between endpoints, information about when the conversation occurred, how long it lasted, and what protocols were used. It is a Layer 3 (and possibly Layer 2, depending on where it’s enabled or match conditions) network protocol that you can easily enable on wired and wireless devices for visibility into the network flows, as well as enhanced network anomaly and malware detection.

For more information, see the Cisco IOS NetFlow web page

Cisco Stealthwatch

Cisco Stealthwatch harnesses the power of network telemetry—including but not limited to NetFlow, IPFIX, proxy logs, and deep packet inspection of raw packets—to provide advanced network visibility, security intelligence, and analytics. This visibility allows a Stealthwatch database record to be maintained for every communication that traverses a network device. This aggregated data can be analyzed to identify hosts with suspicious patterns of activity. Stealthwatch has different alarm categories using many different algorithms that watch behavior and identify suspicious activity. Stealthwatch leverages NetFlow data from network devices throughout all areas of the network—access, distribution, core, data center, and edge—providing a concise view of normal traffic patterns throughout and alerting when policies defining abnormal behavior are matched. For more information, see the Cisco Stealthwatch web page.

For more information, see the Cisco Stealthwatch web page.

Cisco Cognitive Intelligence

Cisco Cognitive Intelligence finds malicious activity that has bypassed security controls or entered through unmonitored channels (including removable media) and is operating inside an organization’s environment. Cognitive Intelligence is a cloud-based product that uses machine learning and statistical modeling of networks. It creates a baseline of the traffic in your network and identifies anomalies. It analyzes user and device behavior and web traffic, to discover command-and-control communications, data exfiltration, and potentially unwanted applications operating in your infrastructure.

For more information, see the Cisco Cognitive Intelligence web page.

Encrypted Traffic Analytics

Encrypted Traffic Analytics is a Cisco IOS-XE feature that uses advanced behavioral algorithms to identify malicious traffic patterns through analysis of intraflow metadata of encrypted traffic, detecting potential threats hiding in encrypted traffic.

For more information, see the Cisco Encrypted Traffic Analytics web page.

Supported Devices

The below devices support ETA with the minimum IOX-XE version of 16.6.4 however IOS XE 16.9.2 is recommended.

Cisco Catalyst 9300 Series Switches

The Cisco® Catalyst 9300 Series Switches are Cisco's lead stackable enterprise switching platform built for security, Internet of Things (IoT), mobility, and cloud. They are the next generation of the industry's most widely deployed switching platform. The 9300 Series forms the foundational building block for Software-Defined Access (SD-Access), Cisco's lead enterprise architecture.

At 480 Gbps, the 9300 Series is industry's highest-density stacking bandwidth solution with the most flexible uplink architecture. It is the first platform optimized for high-density 802.11ac Wave 2 and sets new maximums for network scale.

These switches are also ready for the future, with an x86 CPU architecture and more memory, enabling them to host containers and run third-party applications and scripts natively within the switch. The switches are based on the Cisco Unified Access™ Data Plane (UADP) 2.0 architecture, which not only protects your investment but also allows a larger scale and higher throughput as well as enabling Encrypted Traffic Analytics.

For more information, see the Cisco Catalyst 9300 Series Switches web page.

Catalyst 9500 and 9600 devices are not supported for ETA.

Cisco Catalyst 9400 Series Switches

The Cisco Catalyst 9400 Series Switches are Cisco's leading modular enterprise access switching platform, built for security, IoT, and cloud. The platform provides unparalleled investment protection with a chassis architecture that is capable of supporting up to 9 Tbps of system bandwidth and unmatched power delivery for high-density IEEE 802.3BT (60W Power over Ethernet [PoE])

The 9400 Series delivers state-of-the-art high availability with capabilities such as uplink resiliency and N+1/N+N redundancy for power supplies. The platform is enterprise-optimized with an innovative dual-serviceable fan tray design and side-to-side airflow and is closet-friendly with a depth of approximately 16 inches (41 cm).

A single system can scale up to 384 access ports with your choice of 1 Gigabit Ethernet copper Cisco UPOE® and PoE+ options. The platform also supports advanced routing and infrastructure services, SD-Access capabilities, and network system virtualization. These features enable optional placement of the platform in the core and aggregation layers of small to medium-sized campus environments.

For more information, see the Cisco Catalyst 9400 Series Switches web page.

Catalyst 9500 and 9600 devices are not supported for ETA.

Cisco Cloud Services Router 1000v

The Cisco Cloud Services Router (CSR) 1000v is a virtual-form-factor router that delivers comprehensive WAN gateway and network services functions into virtual and cloud environments. Using familiar, industry-leading Cisco IOS XE Software networking capabilities, the CSR 1000v enables enterprises to transparently extend their WANs into provider-hosted clouds. Similarly, cloud providers themselves can use it to offer enterprise-class networking services to their tenants or customers.

For more information see the Cisco Cloud Services Router web page.

Cisco Integrated Services Virtual Router

The Cisco® Integrated Services Virtual Router (ISRv) is a virtual form-factor Cisco IOS XE Software router that delivers comprehensive WAN gateway and network services functions into virtual environments. Using familiar, industry-leading Cisco IOS XE networking capabilities (the same features present on Cisco 4000 Series ISRs and ASR 1000 Series physical routers), the Cisco ISRv enables enterprises to deliver WAN services to their remote locations using the Cisco Enterprise

Network Functions Virtualization (Enterprise NFV) solution. Similarly, service providers can use it to offer enterprise-class networking services to their tenants or customers.

For more information see the Cisco Integrated Services Virtual Router web page.

Cisco 1000 Series Integrated Services Router

The Cisco 1000 Series Integrated Services Router (ISRs) with Cisco IOS XE Software combine Internet access, comprehensive security, and wireless services (LTE Advanced 3.0 wireless WAN and 802.11ac wireless LAN) in a single, high-performance device. The routers are easy to deploy and manage, with cutting-edge, scalable, multicore separate data and control plane capabilities.

The Cisco 1000 Series ISRs are well suited for deployment as customer premises equipment (CPE) in enterprise branch offices and in service provider managed environments, as well as in environments requiring a smaller form factor.

For more information see the Cisco 1100 Series web page.

Cisco 4000 Series Integrated Services Router

The Cisco 4000 Series ISRs have revolutionized WAN communications in the enterprise branch. With new levels of built-in intelligent network capabilities and convergence, the routers specifically address the growing need for application-aware networking in distributed enterprise sites. These locations tend to have lean IT resources. But they often also have a growing need for direct communication with both private data centers and public clouds across diverse links, including Multiprotocol Label Switching (MPLS) VPNs and the Internet.

The Cisco® 4000 Series contains six platforms: the 4451, 4431, 4351, 4331, 4321 and 4221 ISRs.

For more information see the Cisco 4000 Series web page.

Cisco ASR 1000 Series Aggregation Services Router

The Cisco ASR 1000 Series aggregates multiple WAN connections and network services, including encryption and traffic management, and forwards them across WAN connections at line speeds from 2.5 to 200 Gbps. The routers contain both hardware and software redundancy in an industry-leading high-availability design.

The ASR 1000 Series supports Cisco IOS XE Software, a modular operating system with modular packaging, feature velocity, and powerful resiliency. The ASR 1000 Series Embedded Services Processors (ESPs), which are based on Cisco Flow Processor technology, accelerate many advanced features such as crypto-based access security; Network Address Translation (NAT), threat defense with zone-based firewall, deep packet inspection, Cisco Unified Border Element, and a diverse set of data-center-interconnect features. These services are implemented in Cisco IOS XE without the need for additional hardware support.

For more information, see the Cisco ASR 1000 Series web page.

Requirements for enabling ETA

Cisco Catalyst 9000 switching products

Product	License if Applicable	Recommended version
Cisco Stealthwatch Flow Collector	L-ST-FC-VE-K9	7.0 7.1
Cisco Stealthwatch Flow Collector	L-ST-SMC-VE-K9	7.0

		7.1
Cisco Stealthwatch Flow Sensor v7.1	L-ST-FS-VE-K9	7.1

Cognitive Intelligence

Cognitive Intelligence is included by default in all Stealthwatch Enterprise licenses beginning with Stealthwatch v6.9.1. ETA is enabled in Stealthwatch v6.9.2.

No special software, hardware, or licensing is required other than Stealthwatch 6.9.4 or later. Cisco provides Cognitive Intelligence to any customer that owns term licensing via any buying method. Cisco fulfills requests for Cognitive Intelligence activation sent to the sw-cta-activation@cisco.com alias for customers with a valid Flow Rate license purchase. Requests for activation should include the customer's sales order information.

Cisco Catalyst 9000 switching products

Product	License if Applicable	Recommended version
Cisco Catalyst 9300 Series Switches	DNA Advantage	16.9.2 or later
Cisco Catalyst 9400 Series Switches		

Cisco IOS XE routers

Product	License if Applicable	Recommended version
Cisco 4000 ISR Series Routers	DNA Advantage	16.9.2 or later
Cisco Integrated Services Virtual Router (ISRv)*		
Cisco CSR 1000v Cloud Services Router*		
Cisco 1000 ISR Series Routers*		
Cisco ASR 1001-X System, Crypto, 6 built-in GE, Dual P/S		
Cisco ASR 1002-HX System, Crypto, 8 built-in GE and 8 built-in 10GE ports, Dual P/S		
Cisco CSR 1000v- Amazon Web Services Bring Your Own License*		
Cisco ASR 1004 chassis, dual P/S		
Cisco ASR 1006 chassis, dual P/S		
Cisco ASR 1000 Embedded Services Processor, 20 Gb	DNA Advantage	16.9.2 or later
Cisco ASR 1000 Embedded Services Processor, 40 Gb		
Cisco ASR 1000 Embedded Services Processor, 100 Gb		
Cisco ASR 1000 Embedded Services Processor, 200 Gb		

Design

Requirements

This section provides you with high level guidance for deciding where to deploy both ETA and FNF in your traditional, non-fabric, campus and routed WAN infrastructures. This Cisco design guide has also been updated to include IOS-XE 16.9.2 and Stealthwatch 6.10 or 7.0 as the recommended releases of software when implementing ETA and Flexible NetFlow in your environment.

> For in-depth design guidance for ETA, please refer to the ETA Design Guide for further information.

Campus Wired

In campus networks, prior to the introduction of ETA, NetFlow monitoring of wired traffic was typically configured on any combination of access ports, access switch uplinks to distribution, or distribution switches. Often, NetFlow would be configured at either the distribution layer of the network or at the uplink ports from the access layer switches, providing a distributed and scalable means of monitoring traffic entering or leaving the access switch.

Starting with Cisco IOS XE 16.6.2 on the Cisco Catalyst 9300 and 9400 Series Switches licensed for DNA Advantage, ETA was introduced and additional data elements such as the IDP and SPLT in encrypted communications began to be exported in ETA records, enabling analysis of these data elements for the purpose of performing a crypto audit and/or malware detection. Although ETA is supported in IOS-XE 16.6.2 and later, we only recommend the use of 16.9.2 or later due to scalability enhancements introduced in that release.

With the introduction of ETA support on the Catalyst 9300 and 9400 switches in the network, the strategy as to where to configure ETA and flexible NetFlow will change. Encrypted Traffic Analytics should be considered to be an access layer technology and be configured as close as possible to the wired endpoints. The primary reason for this is twofold, timestamps of traffic derived for use in the SPLT, and support of any intra-switch (East/West) traffic. With wired traffic, the recommendation therefore is to configure both ETA and flexible NetFlow on the access ports of the switch.

> Only the Catalyst 9300 and 9400 access switches support ETA. The Catalyst 9500 and 9600 switches do not support ETA regardless of where they are deployed in the network.

Campus Wireless

An in depth discussion of monitoring campus wireless traffic is beyond the scope of this document at this time. Monitoring of wireless traffic in a centralized (WLC local mode) deployment, as discussed earlier, is possible when deploying a Catalyst 9800 series wireless controller running IOS-XE 16.10.1 or greater. Additionally, the wireless traffic could be redirected to a Cisco Stealthwatch Flow Sensor running version 7.1 via SPAN or tap from/at the switch to which the controller is attached, and the flow sensor can then export both ETA and FNF data.

> AireOS based 2500, 5500 and 8500 series wireless controllers do not support ETA and hence a Stealthwatch v7.1 flow sensor would be required.

For FlexConnect deployments, if the wireless access points are connected to a Catalyst 9300 or 9400 switch, ETA can be configured on the respective trunk or access ports the FlexConnect APs are attached to. As all wireless data traffic egresses the AP into the wired network at the switch port, only that port needs to be configured for ETA and FNF monitoring.

Wide Area Networking

Much the same as campus networks, NetFlow has been deployed heavily in wide area networks as well as the Internet edge. Several considerations exist as to where NetFlow may be configured such as platform scalability relative to the Netflow cache size, processor and memory impact, and bandwidth required for NetFlow record export. These factors are all important when considering whether to implement NetFlow in a branch/remote location or at WAN aggregation routers.

With Cisco IOS XE version 16.6.2 or 16.7.1 and the SEC/K9 license, Encrypted Traffic Analytics was introduced for all models of the Cisco 4000 Series ISRs, all models of the Cisco ASR 1000 Series, as well as the ISRv, CSR 1000v, and Cisco 1000 Series routers. As with the switches, only Cisco IOS XE 16.9.2 or later is recommended for production ETA deployments.

When implementing ETA in the WAN or at the Internet edge, additional consideration is required as ETA scaling relative to the number of flows per second (FPS), is lower than regular Flexible NetFlow and the bandwidth required for ETA record transmission to the flow collector is in addition to, and greater than, NetFlow by itself.

ETA data collection is more processor intensive than regular flexible NetFlow collection and so the number of flows per second subject to ETA inspection is lower than for NetFlow. This may rule out ETA deployment at the Internet edge router or a WAN aggregation router and necessitating the ETA inspection closer to the endpoint. In branch deployments, this would mean enabling ETA at the branch. Alternatively, for Internet edge or other routed environments, if FPS scaling is of concern, it may be necessary to implement a Stealthwatch v7.1 flow sensor.

Please refer to the “Scale” section under “General Considerations” for router performance numbers.

In addition to the bandwidth consumed for flexible NetFlow export, additional bandwidth is required to support ETA and may amount to as much as 10% to 15% of the transmitted TCP WAN traffic. This obviously must be considered when deciding on your ETA deployment strategy and whether deployment of ETA in a branch is acceptable or whether collection at the WAN aggregation router may be necessary. Obviously, bandwidth will be less of a concern for an Internet edge or campus router where FPS scaling is more of a factor.

Logical topology

The following diagram depicts a typical logical topology that we will be discussing for our ETA deployment strategies in a traditional, no SD-Access fabric.

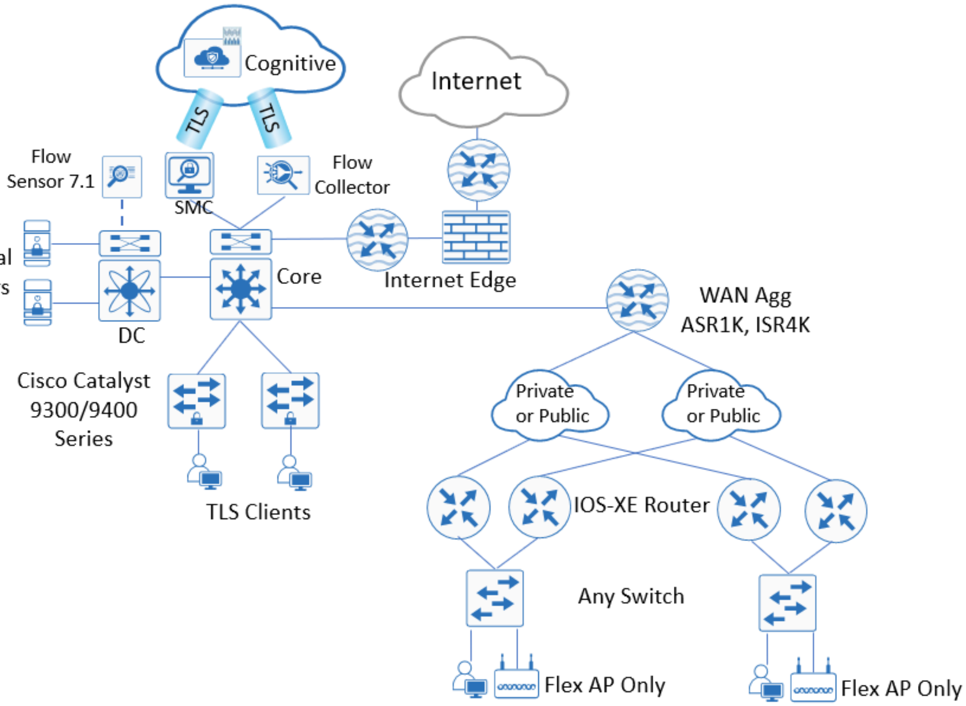
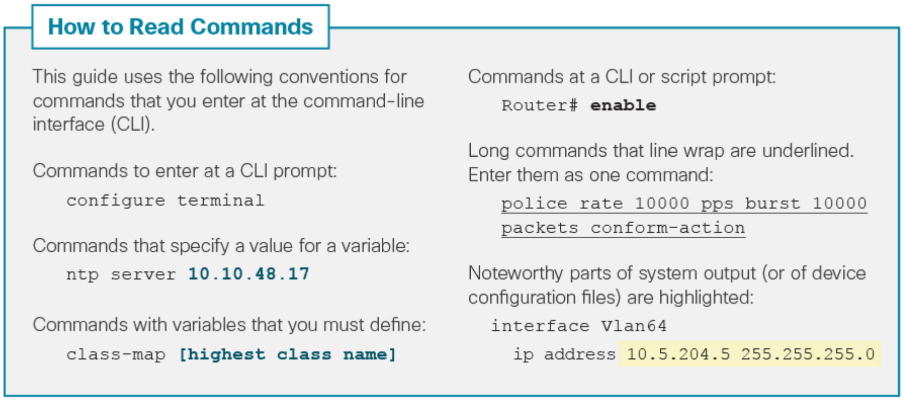


Figure 2 Traditional network logical topology

Deploy



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. Enter them as one command:

```
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
```

This section describes those procedures necessary to enable ETA and FNF on the Cisco Catalyst 9300 and 9400 Series Switches in the campus as well as the ISR and ASR routers for a branch WAN. It consists of four processes in which you perform Stealthwatch and ETA integration, enable ETA and FNF on Cisco Catalyst switches, enable ETA and FNF on Cisco routers, and use the Stealthwatch and the Cognitive Intelligence portal user interfaces for crypto audit and malware detection.

Process: Cognitive Intelligence integration and Crypto Audit App installation in Stealthwatch

This Process assume that either direct communication or communication via a proxy are permitted from the Stealthwatch Management Console and Flow Collectors to the Cognitive Intelligence Cloud. These communications are all via port 443, and their addresses are:

Service Description	Service URL	Service IP
CTA login page CTA public landing page CTA TAXII service CTA data ingest service	https://cta.eu.amp.cisco.com https://cognitive.cisco.com (alias) https://td.cloudsec.sco.cisco.com/CWSP (alias) https://taxii.cloudsec.sco.cisco.com (alias) https://etr.cta.eu.amp.cisco.com scp+ssh://etr.cta.eu.amp.cisco.com https://etr.cloudsec.sco.cisco.com (alias) scp+ssh://etr.cloudsec.sco.cisco.com (alias)	AWS EIPs: • 34.242.41.248 • 34.242.94.137 • 34.251.54.105 • 34.251.210.21 • 34.255.162.33 • 54.194.49.205 Cisco IPs: • 146.112.59.0/24 • 208.69.38.0/24

If you use the API offered by Cisco CTA to export your security data into your own SIEM solution, and you reference Cisco's API by IP address and not by URL, Cisco recommends that you change your setting in your SIEM solution to use the URL as high availability is implemented via Domain Name System (DNS).

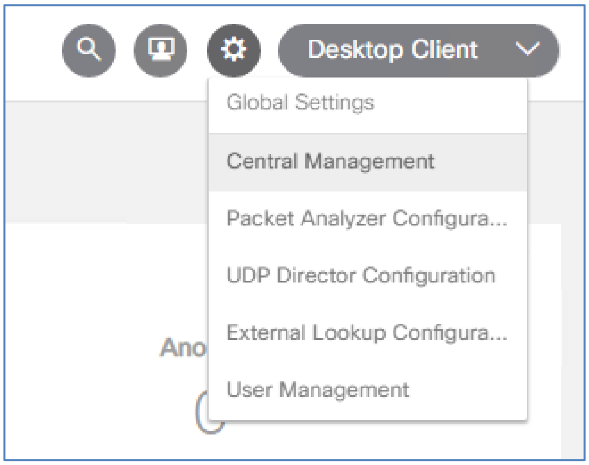
For additional information, please refer to Cisco Field Notice FN-7205.

Procedure 1: Configure Stealthwatch Management Console v7.0 for Cognitive Intelligence integration

This Procedure goes through how to connect Stealthwatch Management Console to Cognitive Intelligence for ETA enablement.

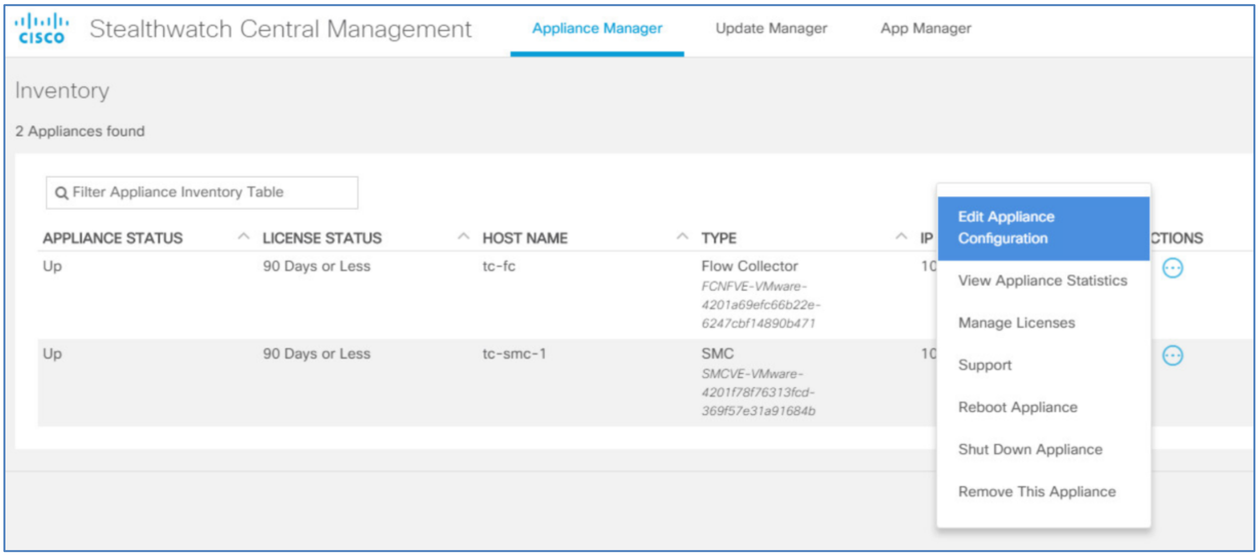
1. Log in to Stealthwatch Management Console.

2. Click on the **GLOBAL SETTINGS** icon, ⚙ and then click **CENTRAL MANAGEMENT.**

2. 

Desktop Client
Global Settings
Central Management
Packet Analyzer Configura...
UDP Director Configuration
External Lookup Configura...
User Management
Ano

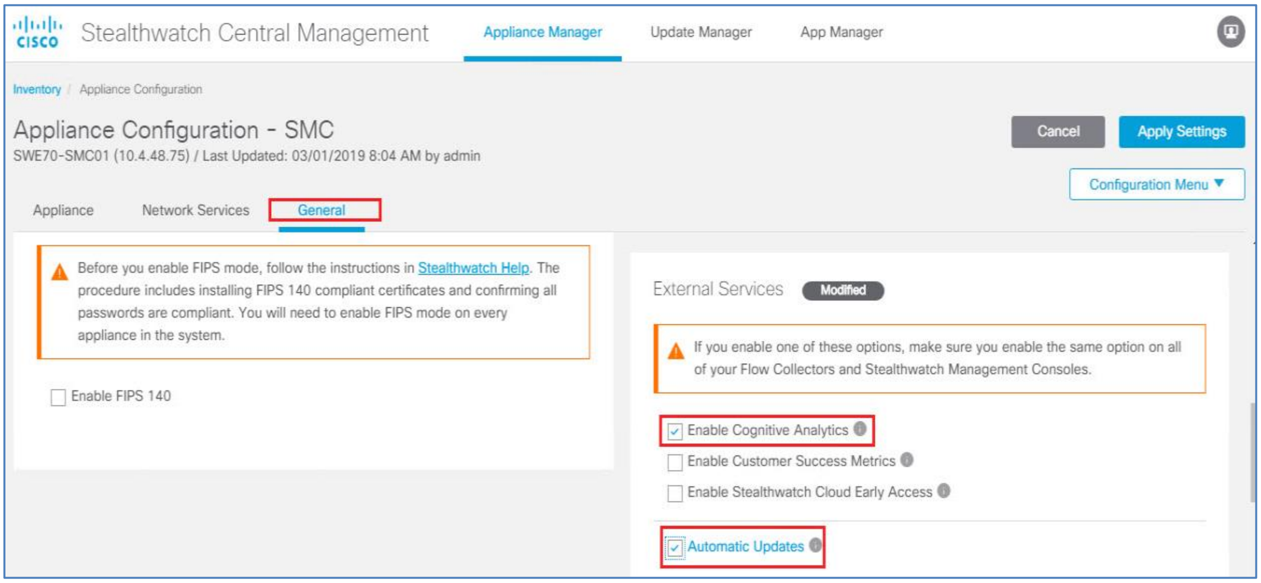
3. Click on the ellipsis ⋯ under the Actions column for your SMC. Click **EDIT APPLIANCE CONFIGURATION**.

3. 

APPLIANCE STATUS	LICENSE STATUS	HOST NAME	TYPE	IP	CTIONS
Up	90 Days or Less	tc-fc	Flow Collector FCNFVE-VMware-4201a69efc66b22e-6247cbf14890b471	10	⋯
Up	90 Days or Less	tc-smc-1	SMC SMCVE-VMware-4201f78f76313fcd-369f57e31a91684b	10	⋯

4.

4. Click **GENERAL** then under External Services, select the **ENABLE COGNITIVE ANALYTICS** check box to enable the Cognitive Analytics component on the Security Insight Dashboard and the Host Report. Optionally, select the Automatic Updates check box to enable Cognitive Analytics to send updates automatically from the cloud.


Stealthwatch Central Management | Appliance Manager | Update Manager | App Manager

Inventory / Appliance Configuration

Appliance Configuration - SMC

SWE70-SMC01 (10.4.48.75) / Last Updated: 03/01/2019 8:04 AM by admin

Cancel | Apply Settings | Configuration Menu ▼

Appliance | Network Services | General

Before you enable FIPS mode, follow the instructions in Stealthwatch Help. The procedure includes installing FIPS 140 compliant certificates and confirming all passwords are compliant. You will need to enable FIPS mode on every appliance in the system.

□ Enable FIPS 140

External Services Modified

If you enable one of these options, make sure you enable the same option on all of your Flow Collectors and Stealthwatch Management Consoles.

☑ Enable Cognitive Analytics

□ Enable Customer Success Metrics

□ Enable Stealthwatch Cloud Early Access

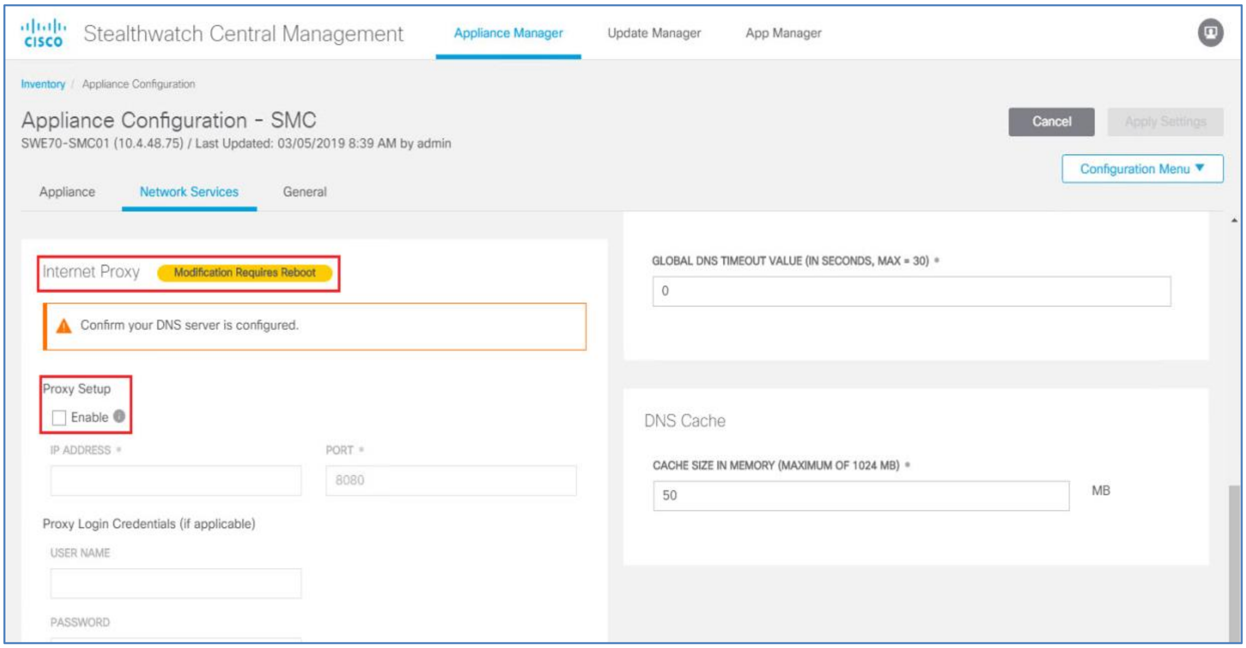
☑ Automatic Updates

The automatic updates will mostly cover security fixes and small enhancements for the Cognitive Analytics cloud. These updates will also be available through the normal Stealthwatch release process. You can disable this option any time to stop the automatic updates from the cloud. If you enable automatic updates on the Stealthwatch Management Console, you need to enable it on the Flow Collector(s).

5. Click **Apply Settings** and confirm.

6. (Optionally) To upload Stealthwatch data via internet proxy, from the Central Management page, click the ellipsis and then select **Edit Appliance Configuration.** Now select the **Network Services** tab. Scroll down to the Internet Proxy section and select the **Enable** checkbox. Fill out the form, then click **Apply Settings**.

Only transparent proxies are supported today for both the crypto audit and malware detection use cases.

5. 
Stealthwatch Central Management | Appliance Manager | Update Manager | App Manager

Inventory / Appliance Configuration

Appliance Configuration - SMC

SWE70-SMC01 (10.4.48.75) / Last Updated: 03/05/2019 8:39 AM by admin

Cancel | Apply Settings | Configuration Menu ▼

Appliance | Network Services | General

Internet Proxy Modification Requires Reboot

Confirm your DNS server is configured.

Proxy Setup

□ Enable

IP ADDRESS *

PORT * 8080

Proxy Login Credentials (if applicable)

USER NAME

PASSWORD

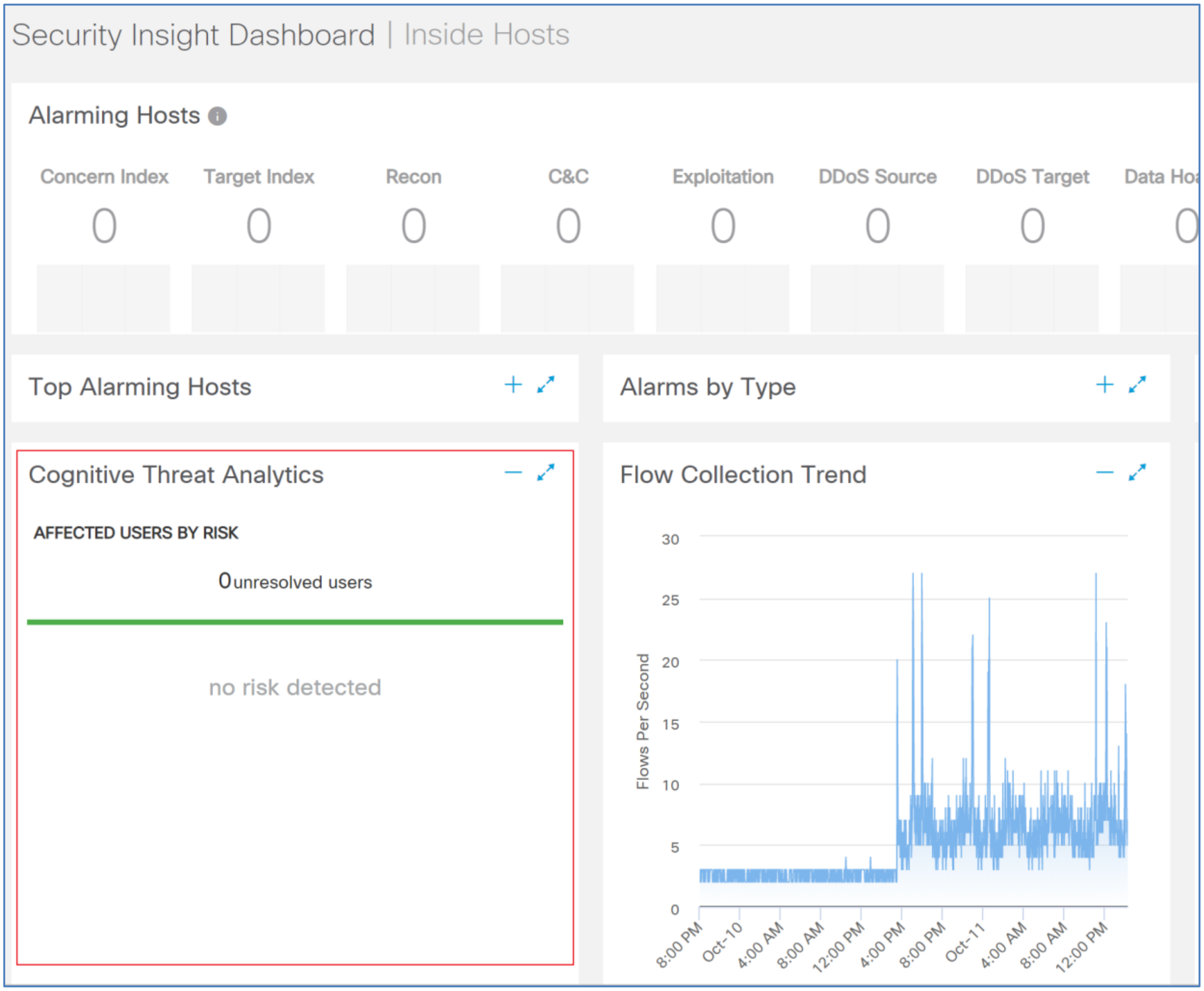
GLOBAL DNS TIMEOUT VALUE (IN SECONDS, MAX = 30) * 0

DNS Cache

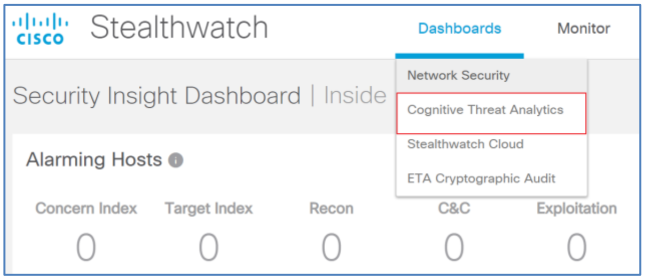
CACHE SIZE IN MEMORY (MAXIMUM OF 1024 MB) * 50 MB

Procedure 2: Verify integration between Stealthwatch and the Cognitive Intelligence cloud

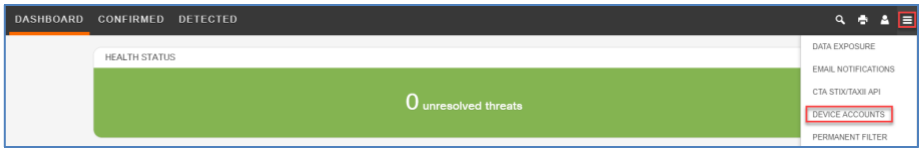
6. Check that the Cognitive Threat Analytics component has appeared on the Security Insight Dashboard and Host Report.



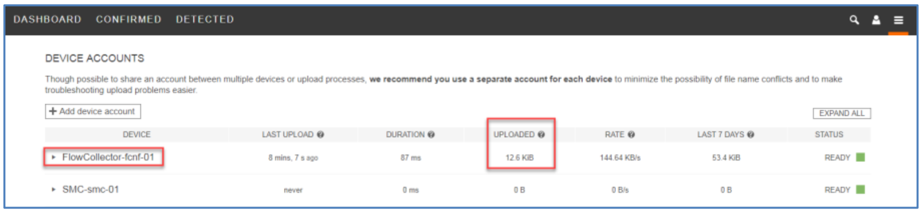
7. From the navigation menu, click **Dashboards > Cognitive Threat Analytics**. The Cognitive Intelligence Dashboard page opens.



8. Click the menu symbol in the upper-right corner of the page, and then click **Device Accounts** from the drop-down menu.



9. Check that accounts for each flow are collector configured and that they are uploading data.



DEVICE ACCOUNTS

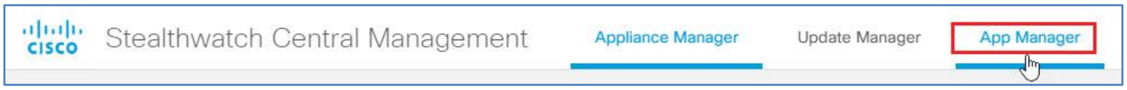
Though possible to share an account between multiple devices or upload processes, **we recommend you use a separate account for each device** to minimize the possibility of file name conflicts and to make troubleshooting upload problems easier.

DEVICE	LAST UPLOAD	DURATION	UPLOADED	RATE	LAST 7 DAYS	STATUS
▸ FlowCollector-fcnf-01	8 mins, 7 s ago	87 ms	12.6 KiB	144.64 KB/s	53.4 KiB	READY 🟩
▸ SMC-smc-01	never	0 ms	0 B	0 B/s	0 B	READY 🟩

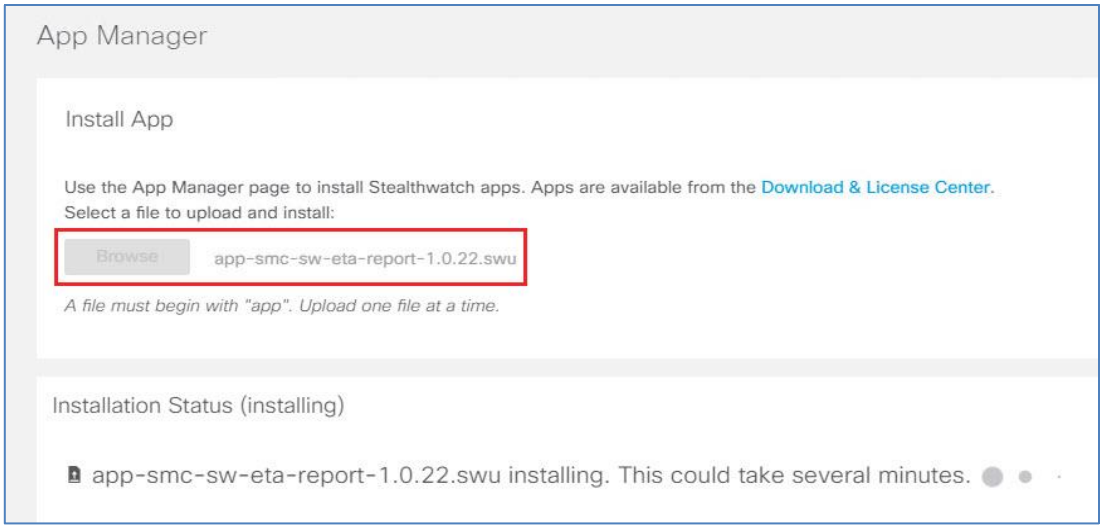
> If the Cognitive Intelligence widget does not display at the SMC, you will want to verify that both the flow collector and Stealthwatch Management Console have Network Time Protocol (NTP) configured correctly. If the flow collector or SMC time is offset from Cognitive Intelligence by more than a minute, the Cognitive Intelligence widget will not display.

Procedure 3: Installing the Stealthwatch Crypto Audit Application

1. From the Central Management user interface click App Manager.



2. Click Browse and select the file previously downloaded from Cisco.com. The upload and installation will begin immediately.



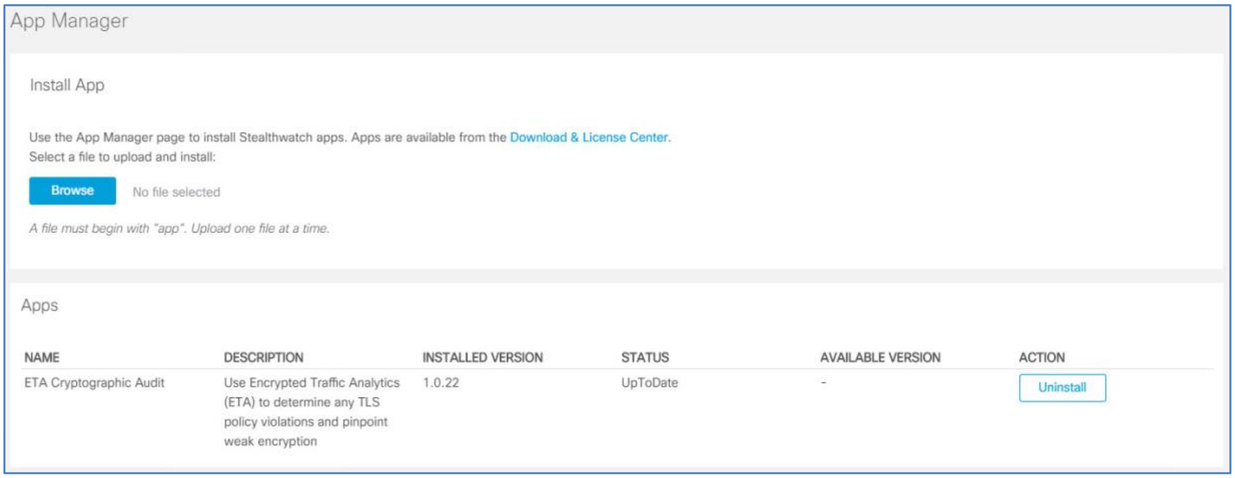
Use the App Manager page to install Stealthwatch apps. Apps are available from the Download & License Center.
Select a file to upload and install:

app-smc-sw-eta-report-1.0.22.swu

A file must begin with "app". Upload one file at a time.

app-smc-sw-eta-report-1.0.22.swu installing. This could take several minutes.

3. Once completed, the Crypto Audit application will be listed in App Manager.



App Manager

Install App

Use the App Manager page to install Stealthwatch apps. Apps are available from the Download & License Center.
Select a file to upload and install:

A file must begin with "app". Upload one file at a time.

Apps

NAME	DESCRIPTION	INSTALLED VERSION	STATUS	AVAILABLE VERSION	ACTION
ETA Cryptographic Audit	Use Encrypted Traffic Analytics (ETA) to determine any TLS policy violations and pinpoint weak encryption	1.0.22	UpToDate	-	Uninstall

Process: Configuring the Cisco Catalyst 9300 or 9400 Series

Procedure 1: Enable ETA on the Switch Globally and Define the Flow Export Destination

1. Either Telnet or connect to the console of the switch and enter configuration mode. Only one exporter IP address is supported for an ETA flow monitor. The configured inactive timer is applicable globally. You cannot configure different ports with different values.

```
AD5-9300# configure terminal
AD5-9300(config)# et-analytics
AD5-9300(config-et-analytics)# ip flow-export destination 10.4.48.70 2055
AD5-9300(config-et-analytics)# inactive-timeout 15
```

When configuring ETA globally on the switch, the command-line interface (CLI) permits the configuration of what is known as an ETA whitelist. Essentially this whitelist allows the creation of an access-list defining what traffic should be considered for ETA export. This whitelist is fully supported on the Cisco IOS XE routing platforms; however, it is not supported on the Cisco Catalyst switches and will result in the following error message: whitelist acl is not supported on Switch followed by %PARSE_RC-4-PRC_NON_COMPLIANCE: `whitelist acl eta-whitelist'.

Procedure 2: Configure Flexible NetFlow

When detailed NetFlow information is required over and above the encryption attributes contained in the IDP, Flexible NetFlow configuration is required on a switch interface over which the encrypted traffic will flow.

1. Configure the flow record.

```
AD5-9300#configure terminal
AD5-9300(config)#flow record FNF-REC
AD5-9300(config-flow-record)# match ipv4 protocol
AD5-9300(config-flow-record)# match ipv4 source address
AD5-9300(config-flow-record)# match ipv4 destination address
AD5-9300(config-flow-record)# match transport source-port
AD5-9300(config-flow-record)# match transport destination-port
```

```
AD5-9300(config-flow-record)# collect counter bytes long
AD5-9300(config-flow-record)# collect counter packets long
AD5-9300(config-flow-record)# collect timestamp absolute first
AD5-9300(config-flow-record)# collect timestamp absolute last
AD5-9300(config-flow-exporter)#exit
```

2. Configure the flow exporter.

```
AD5-9300(config)#flow exporter FNF-exp
AD5-9300(config-flow-exporter)# destination 10.4.48.70
AD5-9300(config-flow-exporter)# transport udp 2055
AD5-9300(config-flow-exporter)# template data timeout 30
AD5-9300(config-flow-exporter)# option interface-table
AD5-9300(config-flow-exporter)# option application-table timeout 10
AD5-9300(config-flow-exporter)#exit
```

3. Configure the flow monitor.

```
AD5-9300#configure terminal
AD5-9300(config)#flow monitor FNF-mon
AD5-9300(config-flow-monitor)# exporter FNF-exp
AD5-9300(config-flow-monitor)# cache timeout active 60
AD5-9300(config-flow-monitor)# record FNF-rec
AD5-9300(config-flow-monitor)#exit
```

4. Apply the monitor to the interface or range of interfaces.

```
AD5-9300#configure terminal
AD5-9300(config)#interface range GigabitEthernet 1/0/1-48
AD5-9300(config-if)# ip flow monitor FNF-mon input
AD5-9300(config-if)# ip flow monitor FNF-mon output
AD5-9300(config-if)#end
```

Procedure 3: Enable ETA on a switch interface or range of interfaces

```
AD5-9300#configure terminal
AD5-9300(config)#interface range GigabitEthernet 1/0/1-48
AD5-9300(config-if-range)#et-analytics enable
```

Procedure 4: Verify the ETA configuration

1. Verify that the ETA monitor "eta-mon" is a predefined name. Make sure the monitor is active by the status indicating "allocated..

```
AD5-9300#show flow monitor eta-mon
Flow Monitor eta-mon:
  Description:       User defined
  Flow Record:       eta-rec
  Flow Exporter:     eta-exp
  Cache:
  Type:                 normal (Platform cache)
  Status:               allocated
  Size:                 10000 entries
  Inactive Timeout:     15 secs
  Active Timeout:       1800 secs
```

2. If ETA is configured independently of FNF, verify the ETA monitor cache. When configuring both ETA and FNF on the same interface, you may disregard this step as when issuing the "*show flow monitor [monitor name] cache*" command, you will see that no cached entries are present. This is expected behavior due to how the ETA and FNF flow monitors are programmed on the interface. Instead use the "show flow monitor [monitor name] cache" command.

```
AD5-9300#show flow monitor eta-mon cache
  Cache type:                               Normal (Platform cache)
  Cache size:                                10000
  Current entries:                               7

  Flows added:                               52139
     —Active timeout    (  1800 secs)       8155
  Flows aged:                                52132
   —Inactive timeout    (    15 secs)      43977

IPV4 DESTINATION ADDRESS:  107.152.26.219
IPV4 SOURCE ADDRESS:       10.4.8.20
IP PROTOCOL:               6
TRNS SOURCE PORT:          52174
TRNS DESTINATION PORT:     443
counter bytes long:        9236
counter packets long:      56
timestamp abs first:       22:55:59.963
timestamp abs last:        23:18:23.963
interface input:           Null
interface output:          Null
```

3. Verify ETA flow exports.

```
AD5-9300#show flow exporter eta-exp statistics
Flow Exporter eta-exp:
Packet send statistics (last cleared 08:23:31 ago):
    Successfully sent:         4853
```

```
Client send statistics:
    Client: Flow Monitor eta-mon
      Records added:           7548
       —sent:                7548
      Bytes added:             6062810
       —sent:                6062810
```

4. Show platform software fed switch active fnf et-analytics-flow-dump to verify SPLT and IDP are exporting to the flow collector.

```
AD5-9300#show platform software fed active fnf et-analytics-flow-dump
 ET Analytics Flow dump


 =================
 Total packets received     :4606354
 Excess packets received    :1278
 Excess syn received        : 647831
 Total eta records added    : 635371
 Current eta records        : 0
 Total eta splt exported    : 616991
 Total eta IDP exported     : 616991


 (Index:0) 10.4.10.10, 10.4.48.75, protocol=6, source port=61793, dest port=443, flow
 done=u
 SPLT: len = 3, value = (1282,256)(35328,34304)(128,0)
 IDP: len = 557, value = 45:0:2:2d:13:a4:40:0:80:6
```

5. Check to see which interfaces et-analytics has been enabled on.

```
AD5-9300#show platform software et-analytics interfaces
ET-Analytics interfaces
 GigabitEthernet1/0/1
 GigabitEthernet1/0/2
 GigabitEthernet1/0/3
 GigabitEthernet1/0/19
 GigabitEthernet1/0/20
 GigabitEthernet1/0/21
 GigabitEthernet1/0/22
 GigabitEthernet1/0/46
 GigabitEthernet1/0/47
 GigabitEthernet1/0/48
```

```
ET-Analytics VLANs
 108-109
```

Process: Configuring Cisco IOS XE Based Routers

For a complete review of the use cases around where ETA and FNF should be deployed in the WAN, please refer to the new, consolidated, ETA Design Guide.

Please note that the following procedures are intended for traditional, routed, WANs and are not supported for SD-WAN. Cisco SD-WAN and Cisco vManage does not support ETA presently.

Procedure 1: Enable ETA on the Router Globally and Define the Flow Export Destination

1. Either Telnet or connect to the console of the router and enter configuration mode. Only one exporter IP address is required for an ETA flow monitor; however, up to four exporters are supported on the routers. The configured inactive timer is applicable globally.

```
RS11-4331#configure terminal
RS11-4331(config)# et-analytics
RS11-4331(config-et-analytics)# ip flow-export destination 10.4.48.70 2055
RS11-4331(config-et-analytics)# inactive-timeout 15
```

2. After configuring ETA globally and defining the flow-export destinations, you should verify that the service has initialized before moving to Procedure 2.

```
RS11-4331#show platform hardware qfp active feature et-analytics data runtime
```

Verify that "feature state" is "initialized."

```
ET-Analytics run-time information:


   Feature state          : initialized (0x00000004)
   Inactive timeout       : 15 secs (default 15 secs)
   Flow CFG information   :
       instance ID        : 0x0
       feature ID         : 0x0
       feature object ID  : 0x0
       chunk ID           : 0x4
```

3. If "initialized" is not displayed in step 2, wait before proceeding to Procedure 3 where you enable ETA on the interface.

Procedure 2: Configure optional whitelist

1. Configure extended IP access list to identify traffic to excluded from ETA inspection through the use of the permit statement. The **PERMIT** keyword is used to identify traffic to be excluded, or whitelisted from inspection. The following excludes all traffic between sources and destinations with an RFC1918 10.X.X.X address from ETA inspection.

```
RS11-4331#configure terminal
```

```
RS11-4331(config)#ip access-list extended eta-whitelist
RS11-4331(config-ext-nacl)#permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
RS11-4331(config-ext-nacl)#end
```

2. Under the global **ET-ANALYTICS** command, apply the access list to an et-analytics whitelist

```
RS11-4331#configure terminal
RS11-4331(config)#et-analytics
RS11-4331(config-et-analytics)#whitelist acl ETA-WHITELIST
RS11-4331(config-et-analytics)#end
RS11-4331#
```

Procedure 3: Enable ETA on a router interface

1. Enable ETA on the desired interface. Based on the WAN use case, this is either the DMVPN tunnel interface, the LAN interface, or in the case of DIA, the physical interface connected to the ISP. For the AWS use case it will be the LAN interfaces inside the VPC.

```
RS11-4331#configure terminal
RS11-4331(config)#interface TUNNEL10
RS11-4331(config-if)#et-analytics enable
RS11-4331(config-if)#end
```

Procedure 4: Configure Flexible NetFlow on the router

1. Configure the FNF record.

```
RS11-4331#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
RS11-4331(config)#flow record FNF-REC
RS11-4331(config-flow-record)# match ipv4 protocol
RS11-4331(config-flow-record)# match ipv4 source address
RS11-4331(config-flow-record)# match ipv4 destination address
RS11-4331(config-flow-record)# match transport source-port
RS11-4331(config-flow-record)# match transport destination-port
RS11-4331(config-flow-record)# match interface input
RS11-4331(config-flow-record)# match ipv4 tos
RS11-4331(config-flow-record)# collect interface output
RS11-4331(config-flow-record)# collect counter bytes long
RS11-4331(config-flow-record)# collect counter packets long
RS11-4331(config-flow-record)# collect timestamp absolute first
RS11-4331(config-flow-record)# collect timestamp absolute last
RS11-4331(config-flow-record)# collect ipv4 dscp
RS11-4331(config-flow-record)# collect ipv4 ttl minimum
RS11-4331(config-flow-record)# collect ipv4 ttl maximum
```

```
RS11-4331(config-flow-record)# collect transport tcp flags
RS11-4331(config-flow-record)# end
```

2. Configure the FNF exporter.

```
RS11-4331#configure terminal
RS11-4331(config)#flow exporter FNF-EXP
RS11-4331(config-flow-exporter)# destination 10.4.48.70
RS11-4331(config-flow-exporter)# source LOOPBACK0
RS11-4331(config-flow-exporter)# transport udp 2055
RS11-4331(config-flow-exporter)# template data timeout 30
RS11-4331(config-flow-exporter)# end
```

3. Configure the FNF monitor for traffic entering the interface.

```
RS11-4331#configure terminal
RS11-4331(config)#flow monitor FNF-MON
RS11-4331(config-flow-monitor)# exporter FNF-EXP
RS11-4331(config-flow-monitor)# cache timeout active 60
RS11-4331(config-flow-monitor)# record FNF-REC
RS11-4331(config-flow-monitor)# end
```

4. Apply the FNF input and output monitors to the desired interface. Based on the WAN use case, this is either the DMVPN tunnel interface, the LAN interface, or in the case of DIA, the physical interface connected to the ISP.

```
RS11-4331#configure terminal
RS11-4331(config)#interface tunnel10
RS11-4331(config-if)# ip flow monitor fnf-mon input
RS11-4331(config-if)# ip flow monitor fnf-mon output
RS11-4331(config-if)#end
```

Procedure 5: Validating ETA and Flexible NetFlow on the router.

1. Verify that ETA is enabled.

```
RS11-4331#show platform software et-analytics GLOBAL
ET-Analytics Global state
=========================
 All Interfaces   : Off
 IP Flow-record Destination: 10.4.48.70 : 2055
 Inactive timer: 15

 whitelist acl eta-whitelist

ET-Analytics interfaces
```

```
=========================
 Tunnel10


RS11-4331#show platform software et-analytics interface
ET-Analytics interfaces
=========================
 Tunnel10F
```

2. Verify the configured timeout.

```
RS11-4331# show platform hardware qfp active feature et-analytics data RUNTIME


ET-Analytics run-time information:


   Feature state          : initialized (0x00000004)
   Inactive timeout       : 15 secs (default 15 secs)
   Flow CFG information   :
       instance ID        : 0x0
       feature ID         : 0x0
       feature object ID : 0x0
       chunk ID           : 0x4
```

3. Verify the ETA flow statistics.

```
RS11-4331#show platform hardware  qfp active feature et-analytics data stats flow
ET-Analytics Stats:
    Flow statistics:
      feature object allocs : 19257
      feature object frees  : 19235
      flow create requests  : 787668
      flow create matching  : 768411
      flow create successful: 19257
      flow create failed, CFT handle: 0
      flow create failed, getting FO: 0
      flow create failed, malloc FO : 0
      flow create failed, attach FO : 0
      flow create failed, match flow: 0
      flow create failed, set aging : 150
      flow ageout requests          : 19218
      flow ageout failed, freeing FO: 0
      flow ipv4 ageout requests     : 0
      flow ipv6 ageout requests     : 0
      flow whitelist traffic match  : 0
```

4. Verify the ETA export statistics.

```
RS11-4331# show platform hardware qfp active feature et-analytics data STATS EXPORT
ET-Analytics 10.4.48.70:2055 Stats:
    Export statistics:
      Total records exported     : 88554
      Total packets exported     : 45553
      Total bytes exported       : 33287148
      Total dropped records      : 0
      Total dropped packets      : 0
      Total dropped bytes        : 0
      Total IDP records exported :
            initiator->responder : 77092
            responder->initiator : 11636
      Total SPLT records exported:
            initiator->responder : 77075
            responder->initiator : 11633
      Total SALT records exported:
            initiator->responder : 0
            responder->initiator : 0
      Total BD records exported  :
            initiator->responder : 0
            responder->initiator : 0
      Total TLS records exported :
            initiator->responder : 3835
            responder->initiator : 3815
```

Operate

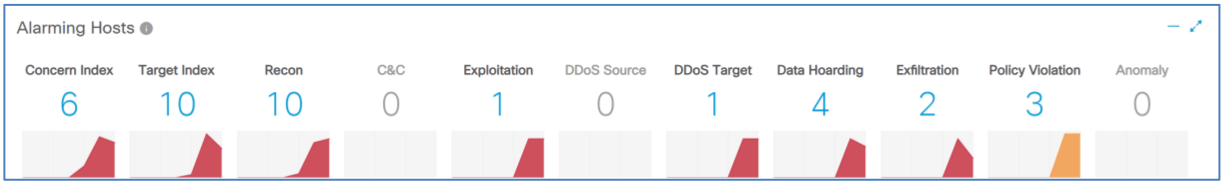
Navigating the Stealthwatch Security Insight Dashboard

The insight dashboard displays a variety of information regarding the status of the network. The following section gives a brief overview of the different parts of this dashboard.

The Security Insight Dashboard will be the first page shown once logged into the Stealthwatch Management Console.

Alarming Hosts

1. At the top of the page, the Alarming Hosts shows the number of hosts that are currently alarming within a certain category.



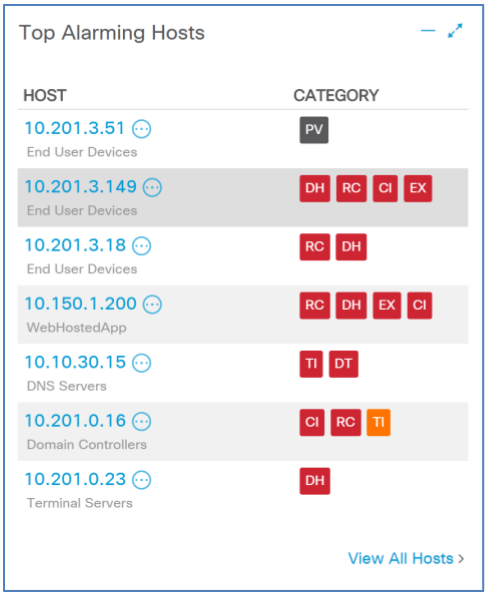
Alarming Hosts

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
6	10	10	0	1	0	1	4	2	3	0

2. The numbers are color-coded based on the overall severity of activity for the given alarm category. Beneath the number there is a trend graph that shows the total number of hosts that have generated alarms in the category, each day, for the past 7 days. Clicking on a number will pull up a list of all hosts currently generating alarms in the category.

Top Alarming Hosts

This section displays the top 7 alarming hosts in your environment. This is based on the overall amount of alarming behavior it has been a part of.



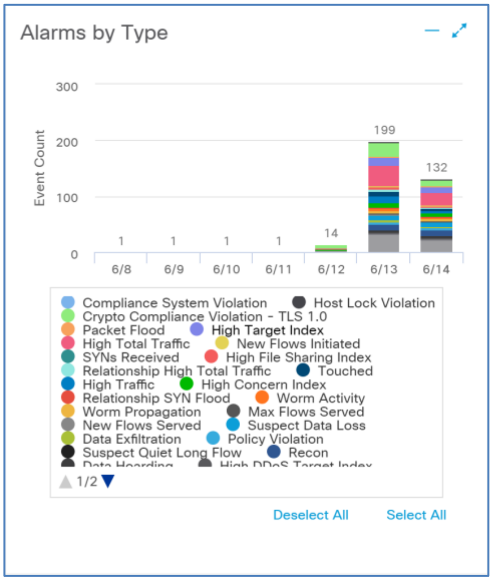
Top Alarming Hosts

HOST	CATEGORY
10.201.3.51 End User Devices	PV
10.201.3.149 End User Devices	DH RC CI EX
10.201.3.18 End User Devices	RC DH
10.150.1.200 WebHostedApp	RC DH EX CI
10.10.30.15 DNS Servers	TI DT
10.201.0.16 Domain Controllers	CI RC TI
10.201.0.23 Terminal Servers	DH

You can mouse over the listed categories on the right to show the percentage of alarms over a normal host. Additionally, you can click the ellipsis (…) to dig down deeper into that host’s activities.

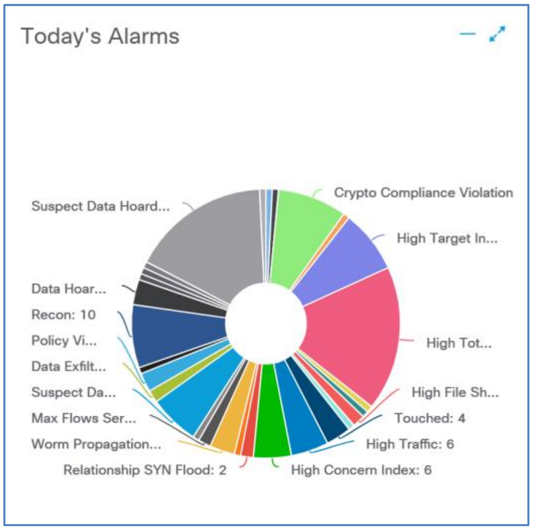
Alarms by Type

This is a graphical representation of the past weeks alarms broken down by day and alarm type.



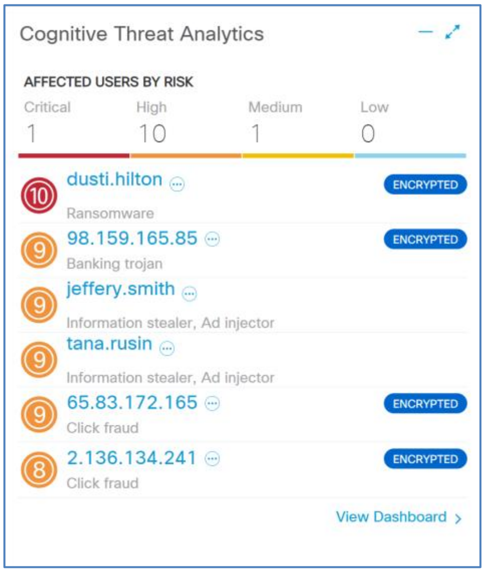
Todays Alarms

This pie chart provides an overview of all alarms that have occurred in the present day. You can click on any of the Alarm types in the chart to see the correlating alarm details for the day.



Cognitive Threat Analytics

Provides Stealthwatch with enchanced capabilitys allowing for Encrypted Traffic Analytics.



Cognitive Threat Analytics

AFFECTED USERS BY RISK

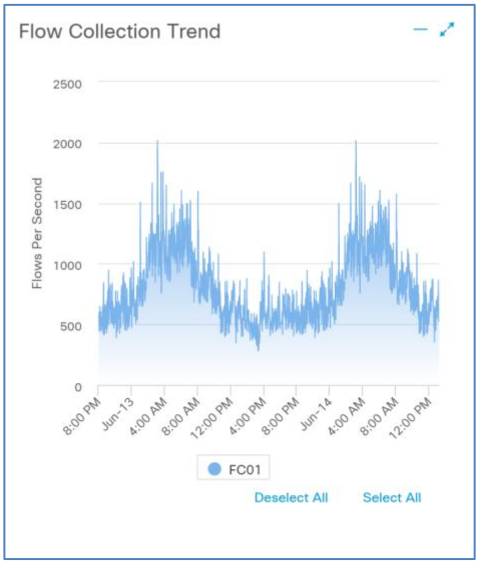
Critical	High	Medium	Low
1	10	1	0

Score	User / Host	Threat	Status
10	dusti.hilton	Ransomware	ENCRYPTED
9	98.159.165.85	Banking trojan	ENCRYPTED
9	jeffery.smith	Information stealer, Ad injector	
9	tana.rusin	Information stealer, Ad injector	
9	65.83.172.165	Click fraud	ENCRYPTED
8	2.136.134.241	Click fraud	ENCRYPTED

View Dashboard ›

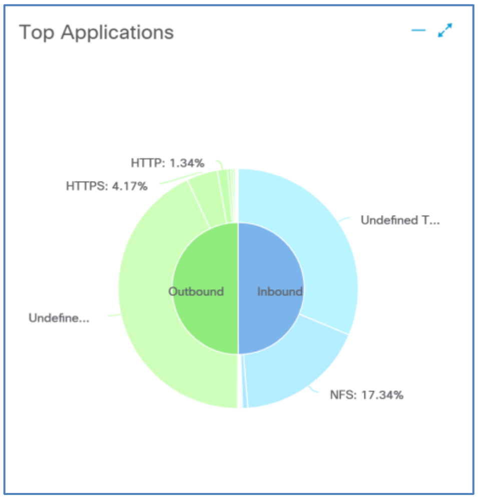
Flow Collection Tend

This chart shows the rate of NetFlow collection for all Flow Collectors over the past 48 hours. In deployments with multiple Collectors, you can select which appliance to see the collection trend for that particular collector.



Top Applications

This pie chart shows the top inbound and outbound application traffic types seen across the network.



Host Groups

Host Groups are containers of hosts or IP addresses that share attributes and policies. This allows you to better inform Stealthwatch about your network policy structure relative to user/server organizational groupings making it more efficient to establish acceptable communication patterns.

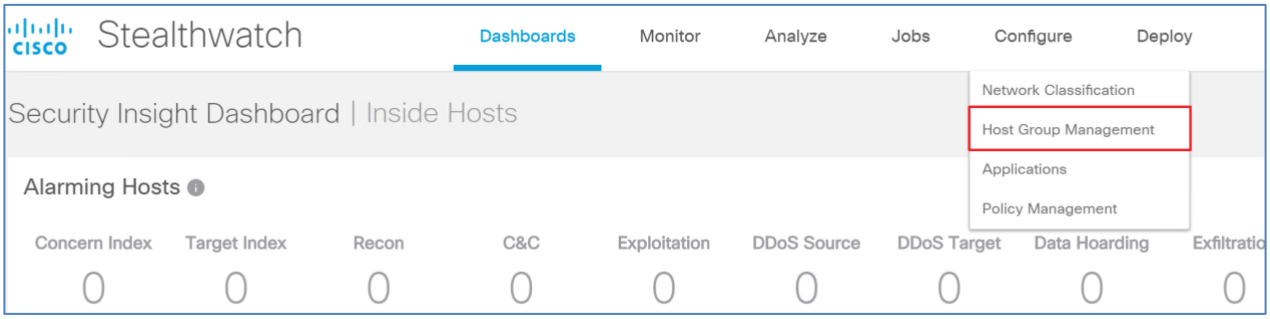
For example, if DHCP servers are configured within a host group, Stealthwatch knows they are legitiamate. If a rogue DHCP server appears with an address outside the hostgroup and starts handing out addresses, Stealthwatch will be able to quickly raise an alert.

Inside Hosts

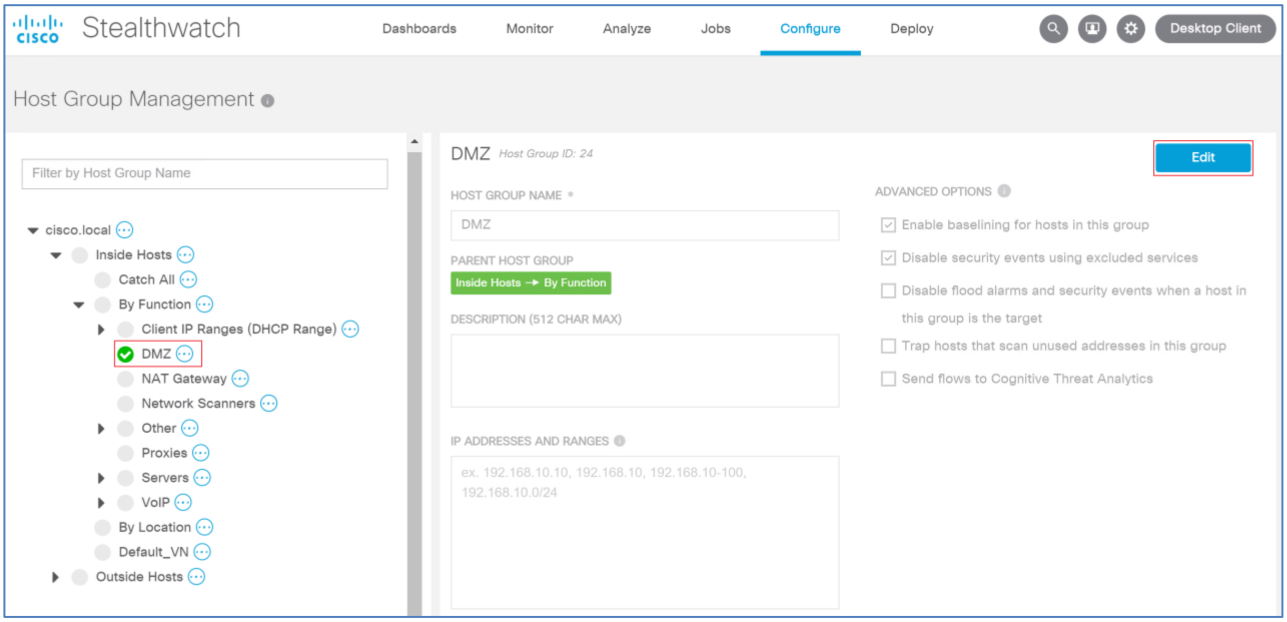
Inside Hosts are an integral part of Stealthwatch, they allow Stealthwatch to know what IP Addresses and Host Groups are considered internal to the network and which are not. By default, all RFC 1918 ranges are in the Inside Hosts/Catch All group. If using an IP range that is not covered by that spectrum for the internal network, it is important to add it to Inside Hosts so Stealthwatch does not report on inaccurate information.

Configuring a Host Group

1. Log into the Stealthwatch Management Console.
2. At the top hover over CONFIGURE and select HOST GROUP MANAGEMENT



3. Inside the HOST GROUP MANAGEMENT page you will see there are already some pre-defined Host Groups. If wanted, you can configure these by selecting a group and clicking EDIT.



DMZ *Host Group ID: 24*

HOST GROUP NAME *: DMZ

PARENT HOST GROUP: Inside Hosts → By Function

DESCRIPTION (512 CHAR MAX)

IP ADDRESSES AND RANGES: ex. 192.168.10.10, 192.168.10, 192.168.10-100, 192.168.10.0/24

ADVANCED OPTIONS

☑ Enable baselining for hosts in this group

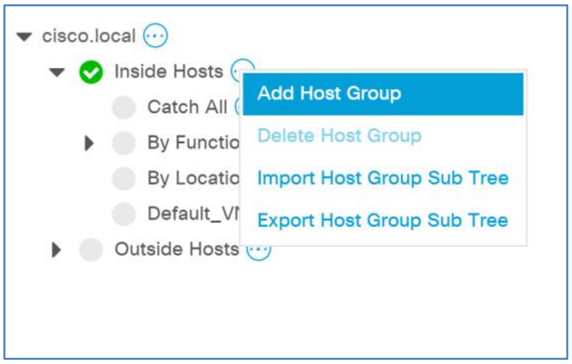
☑ Disable security events using excluded services

□ Disable flood alarms and security events when a host in this group is the target

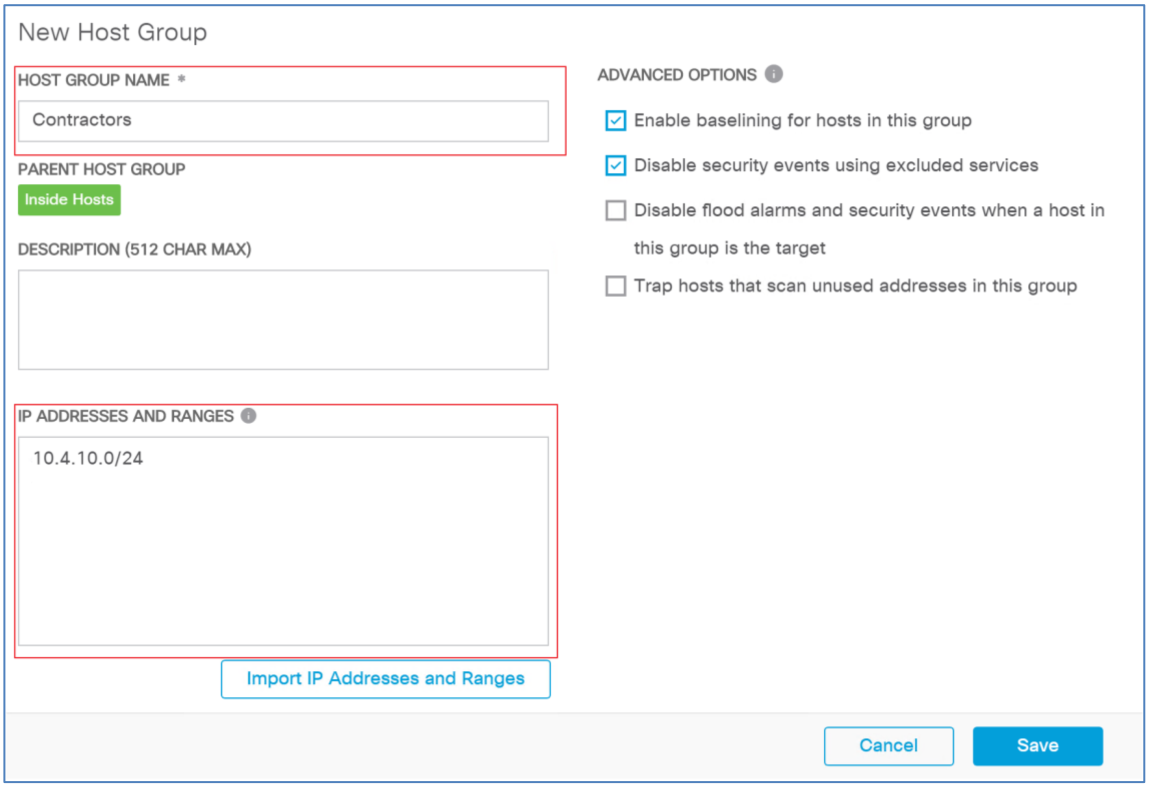
□ Trap hosts that scan unused addresses in this group

□ Send flows to Cognitive Threat Analytics

4. You can create a new group by clicking the ellipsis (…) next to the hierarchy you would like to add the group to and selecting **Add Host Group**.



In the resulting menu enter the group name under **Host Group Name** and then enter the IP range under the **IP Addresses and Ranges** section and click **Save**.



New Host Group

HOST GROUP NAME *

Contractors

PARENT HOST GROUP

Inside Hosts

DESCRIPTION (512 CHAR MAX)

IP ADDRESSES AND RANGES

10.4.10.0/24

ADVANCED OPTIONS

☑ Enable baselining for hosts in this group

☑ Disable security events using excluded services

□ Disable flood alarms and security events when a host in this group is the target

□ Trap hosts that scan unused addresses in this group

Crypto Audit

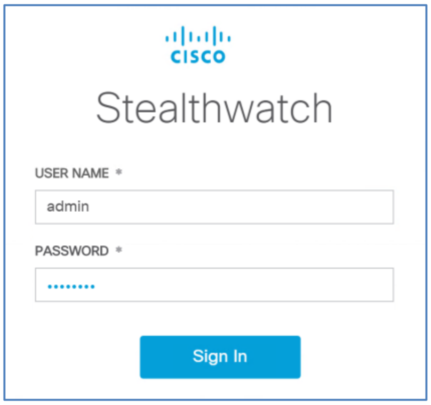
Crypto Audit is a useful tool to detect which cryptography version and cipher suite is being used within your network.

Preform a Crypto Audit Using the ETA Cryptographic Audit tool

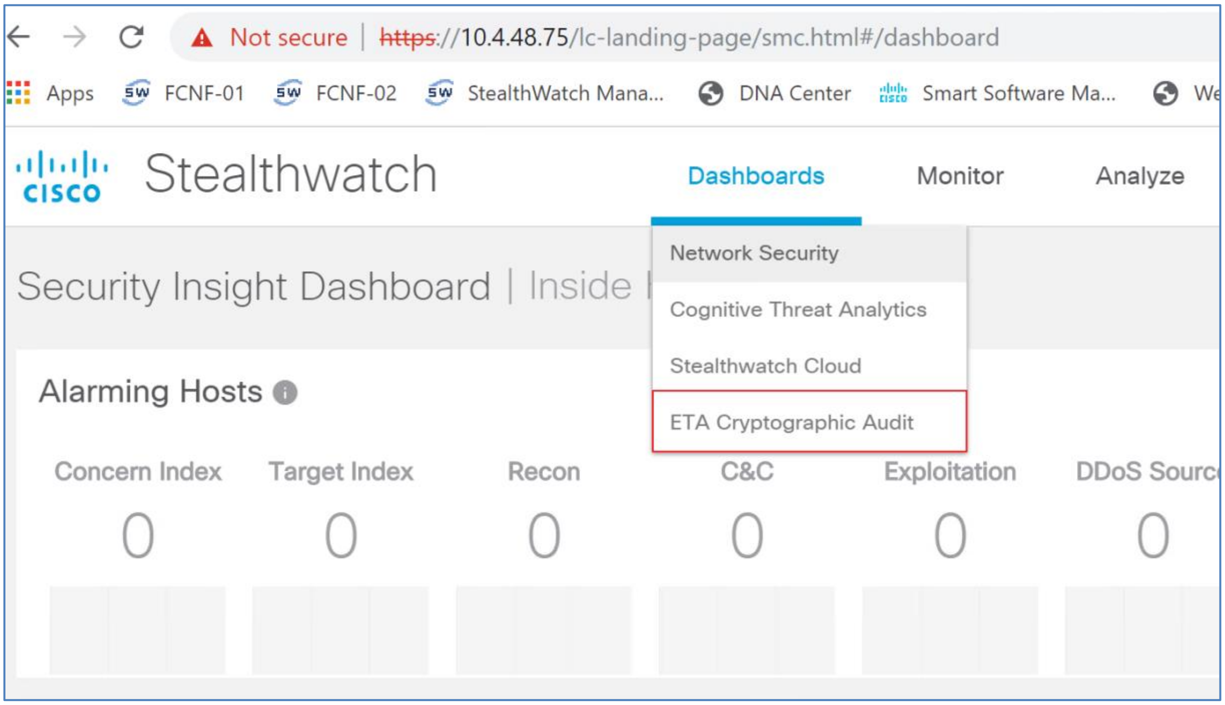
Currently the Crypto Audit tool runs against the server side flows in the selected host group. Therefor it is recommended to create or add internal servers into an inside host group to run the audit against.

If wanting to see both client-side and server-side orientation see Perform a Crypto Audit using Flow Search.

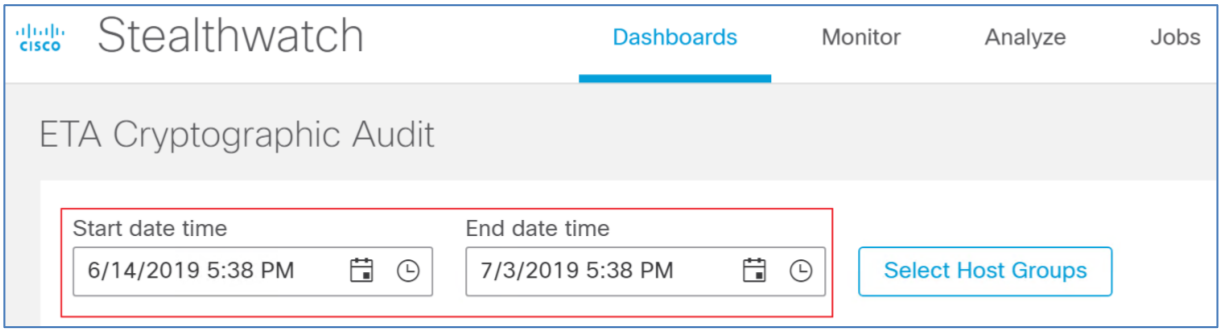
1. To start a crypto audit log into the **Stealthwatch Management Console**.



2. Hover over **Dashboards** and select **ETA Cryptographic Audit**.



3. In the Cryptographic Audit tool select the date and time you wish to run the audit.

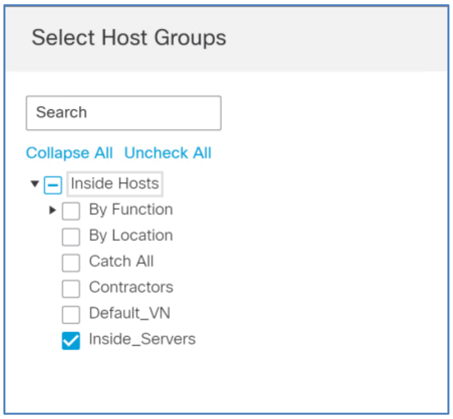


ETA Cryptographic Audit

Start date time: 6/14/2019 5:38 PM

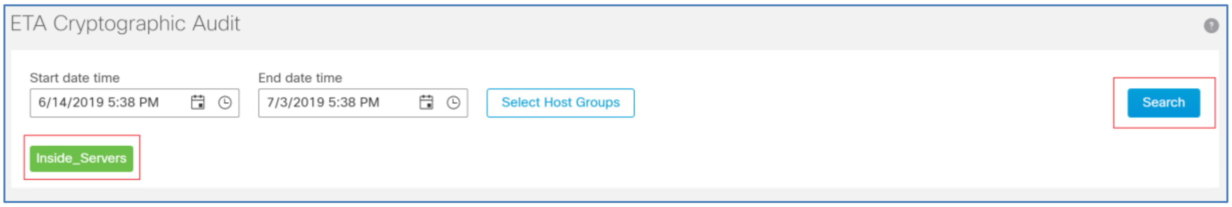
End date time: 7/3/2019 5:38 PM

4. Click **Select Host Group** and pick the group you wish to run the audit for and click **Apply.**



- ⊟ Inside Hosts
  - □ By Function
  - □ By Location
  - □ Catch All
  - □ Contractors
  - □ Default_VN
  - ☑ Inside_Servers

5. You should now see the host groups selected under the Start Date Time. Click Search to start the Crypto Audit.



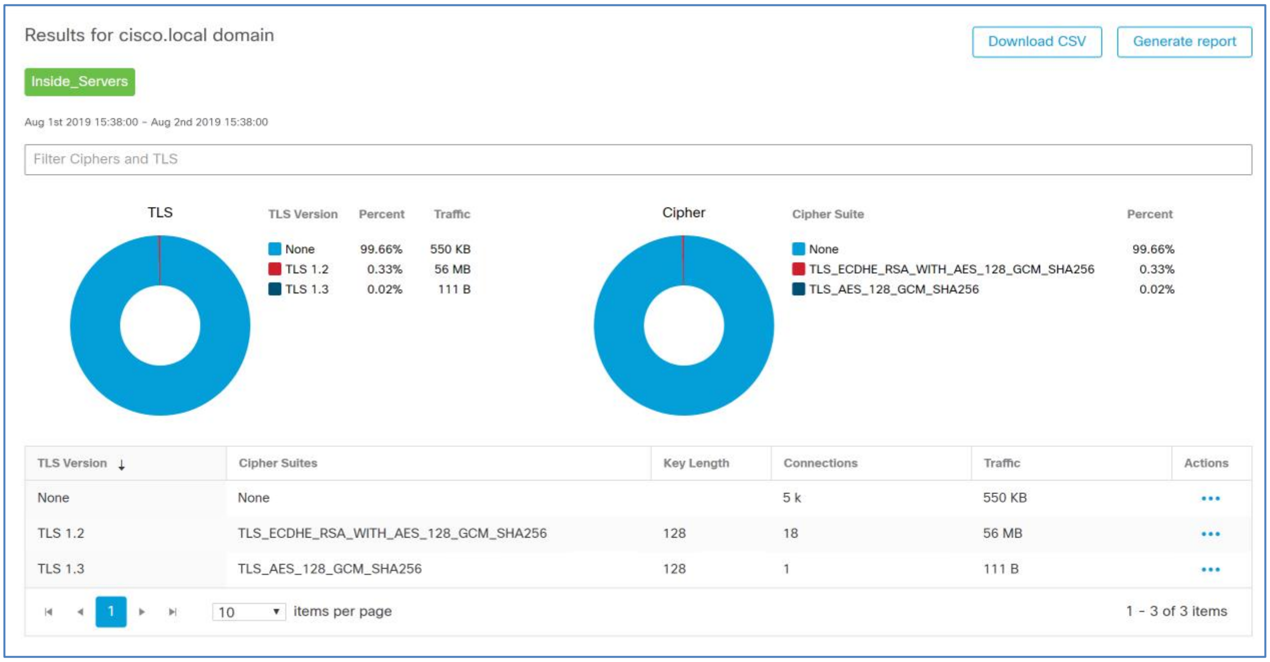
ETA Cryptographic Audit

Start date time: 6/14/2019 5:38 PM

End date time: 7/3/2019 5:38 PM

Inside_Servers

6. You will now see the results of the Crypto Audit showing the TLS version as well as the Cipher Suites being used.



Results for cisco.local domain

Inside_Servers

Aug 1st 2019 15:38:00 - Aug 2nd 2019 15:38:00

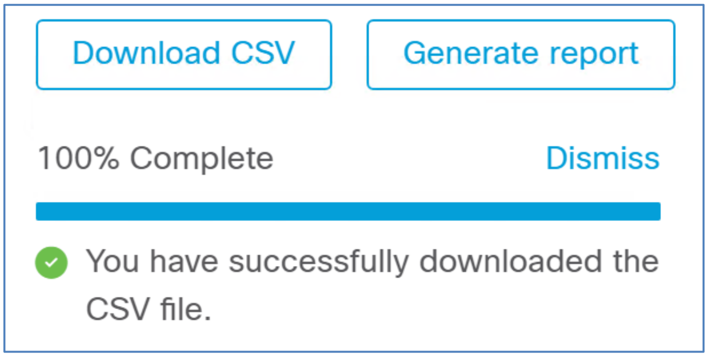
TLS Version	Percent	Traffic
🟦 None	99.66%	550 KB
🟥 TLS 1.2	0.33%	56 MB
■ TLS 1.3	0.02%	111 B

Cipher Suite	Percent
🟦 None	99.66%
🟥 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	0.33%
■ TLS_AES_128_GCM_SHA256	0.02%

TLS Version ↓	Cipher Suites	Key Length	Connections	Traffic	Actions
None	None		5 k	550 KB	•••
TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	128	18	56 MB	•••
TLS 1.3	TLS_AES_128_GCM_SHA256	128	1	111 B	•••

7. To export the report click the download CSV file, this report produces a one page report per server.

In the current version of the crypto audit application, the support is limited to 100 servers.



100% Complete

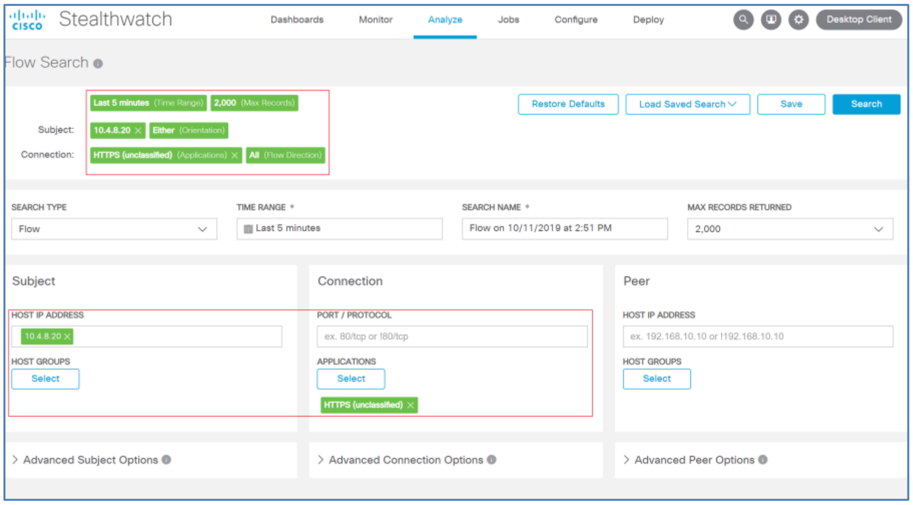
✓ You have successfully downloaded the CSV file.

Perform a Crypto Audit using Flow Search

1. In your browser, access SMC.

2. On the Dashboard, navigate to **ANALYZE > FLOW SEARCH.**

3. On the Flow Search page, create any filters against which you want to search.



Flow Search

Last 5 minutes (Time Range) 2,000 (Max Records)

Subject: 10.4.8.20 × Either (Orientation)

Connection: HTTPS (unclassified) (Applications) × All (Flow Direction)

SEARCH TYPE: Flow

TIME RANGE *: Last 5 minutes

SEARCH NAME *: Flow on 10/11/2019 at 2:51 PM

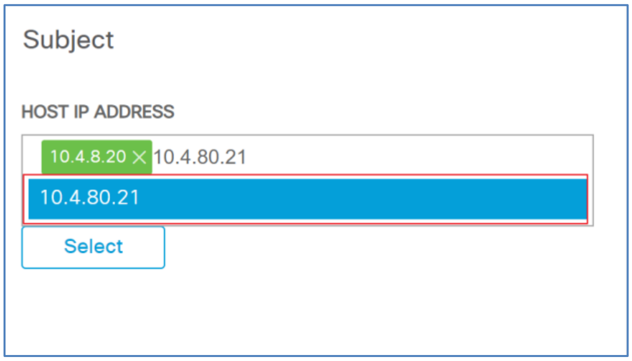
MAX RECORDS RETURNED: 2,000

Subject — HOST IP ADDRESS: 10.4.8.20 ×

Connection — PORT / PROTOCOL: ex. 80/tcp or !80/tcp; APPLICATIONS: HTTPS (unclassified) ×

Peer — HOST IP ADDRESS: ex. 192.168.10.10 or !192.168.10.10

When you type information such as the IP address, select the box that appears (with the entered text highlighted blue).

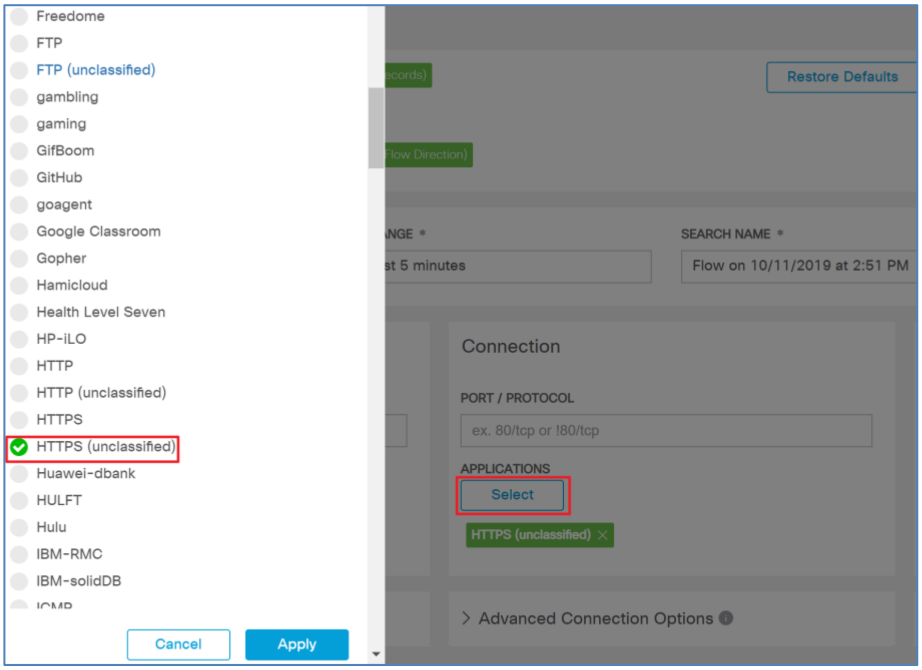


Subject

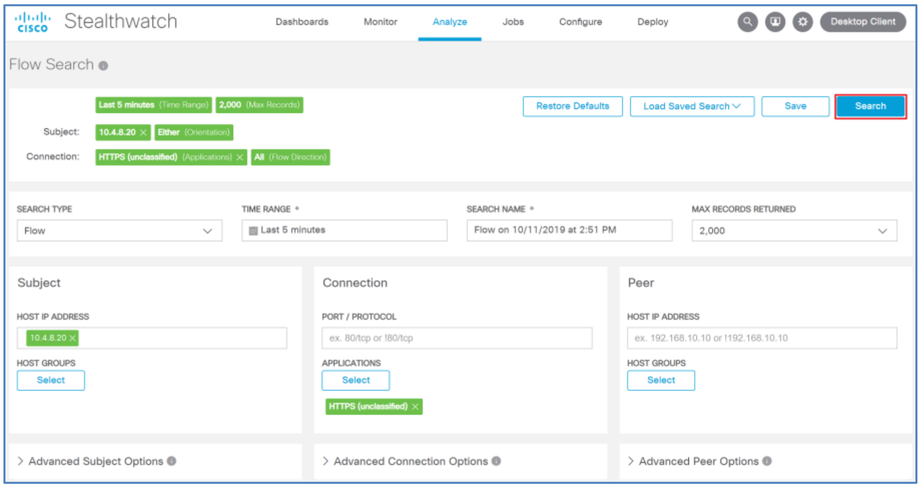
HOST IP ADDRESS: 10.4.8.20 × 10.4.80.21

10.4.80.21

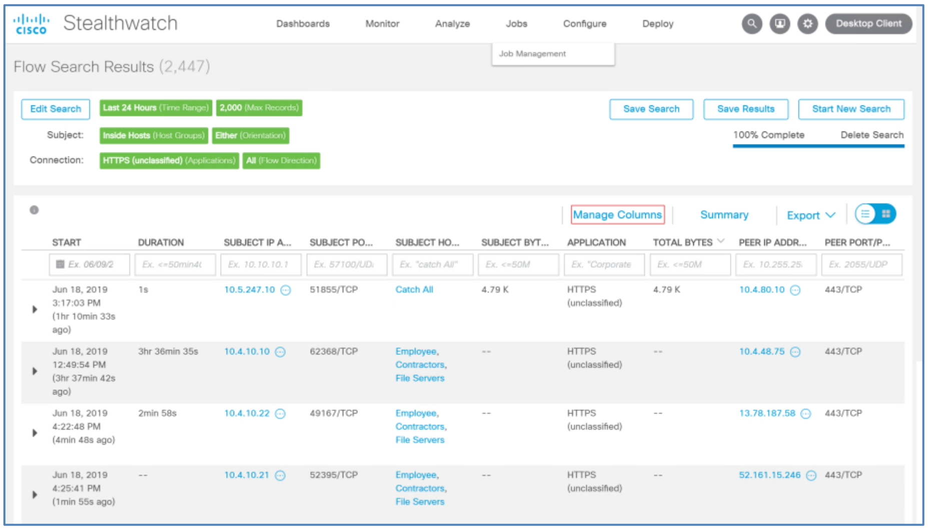
4. To select a specific application, click the **SELECT** button. From the pop-up, select the application to filter on (in this case HTTPS has been selected), and then click **DONE.**



5. With search criteria defined, click **SEARCH**. The search begins.



6. After the search has completed, the following screen appears, showing HTTPS flows and information derived from the IDP and TLS handshake. Notice that the ETA-specific data elements are not present. To enable the display of that information, click **MANAGE COLUMNS**.



Flow Search Results (2,447)

Edit Search | Last 24 Hours (Time Range) | 2,000 (Max Records)

Subject: Inside Hosts (Host Groups) | Either (Orientation)

Connection: HTTPS (unclassified) (Applications) | All (Flow Direction)

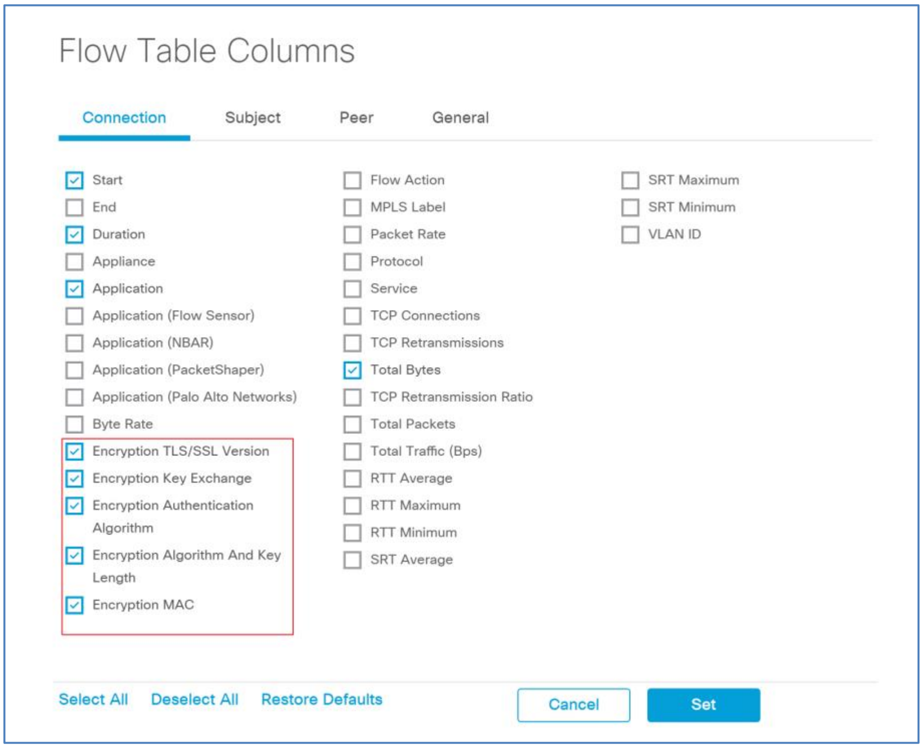
Save Search | Save Results | Start New Search

100% Complete | Delete Search

Manage Columns | Summary | Export

START	DURATION	SUBJECT IP A...	SUBJECT PO...	SUBJECT HO...	SUBJECT BYT...	APPLICATION	TOTAL BYTES	PEER IP ADDR...	PEER PORT/P...
Ex. 06/09/2	Ex. <=50min4(	Ex. 10.10.10.1	Ex. 57100/UD	Ex. "catch All"	Ex. <=50M	Ex. "Corporate	Ex. <=50M	Ex. 10.255.25	Ex. 2055/UDP
Jun 18, 2019 3:17:03 PM (1hr 10min 33s ago)	1s	10.5.247.10	51855/TCP	Catch All	4.79 K	HTTPS (unclassified)	4.79 K	10.4.80.10	443/TCP
Jun 18, 2019 12:49:54 PM (3hr 37min 42s ago)	3hr 36min 35s	10.4.10.10	62368/TCP	Employee, Contractors, File Servers	--	HTTPS (unclassified)	--	10.4.48.75	443/TCP
Jun 18, 2019 4:22:48 PM (4min 48s ago)	2min 58s	10.4.10.22	49167/TCP	Employee, Contractors, File Servers	--	HTTPS (unclassified)	--	13.78.187.58	443/TCP
Jun 18, 2019 4:25:41 PM (1min 55s ago)	--	10.4.10.21	52395/TCP	Employee, Contractors, File Servers	--	HTTPS (unclassified)	--	52.161.15.246	443/TCP

7. A pop-up appears. Scroll down and select the encryption fields to be added to the columns displayed. After selecting all encryption fields, scroll down and click **SET.**

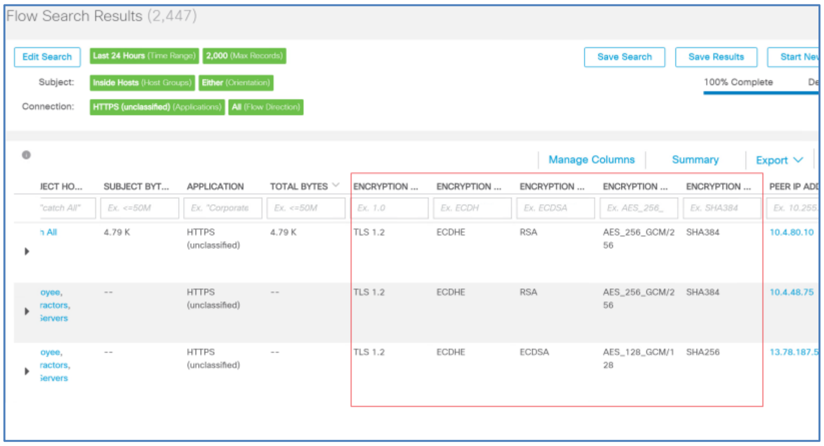


Flow Table Columns

Connection | Subject | Peer | General

☑ Start
☐ End
☑ Duration
☐ Appliance
☑ Application
☐ Application (Flow Sensor)
☐ Application (NBAR)
☐ Application (PacketShaper)
☐ Application (Palo Alto Networks)
☐ Byte Rate
☑ Encryption TLS/SSL Version
☑ Encryption Key Exchange
☑ Encryption Authentication Algorithm
☑ Encryption Algorithm And Key Length
☑ Encryption MAC
☐ Flow Action
☐ MPLS Label
☐ Packet Rate
☐ Protocol
☐ Service
☐ TCP Connections
☐ TCP Retransmissions
☑ Total Bytes
☐ TCP Retransmission Ratio
☐ Total Packets
☐ Total Traffic (Bps)
☐ RTT Average
☐ RTT Maximum
☐ RTT Minimum
☐ SRT Average
☐ SRT Maximum
☐ SRT Minimum
☐ VLAN ID

8. Once the settings have been saved, the following screen appears, with all of the encryption fields selected.



Flow Search Results (2,447)

Edit Search | Last 24 Hours (Time Range) | 2,000 (Max Records) | Save Search | Save Results | Start Nev

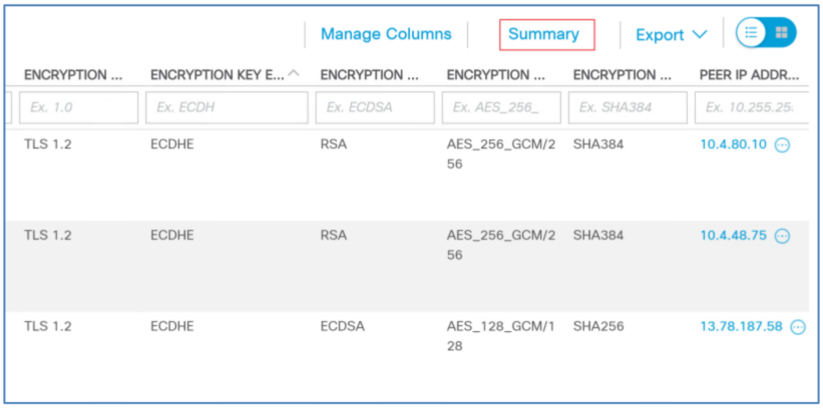
Subject: Inside Hosts (Host Groups) | Either (Orientation) — 100% Complete

Connection: HTTPS (unclassified) (Applications) | All (Flow Direction)

Manage Columns | Summary | Export

IECT HO...	SUBJECT BYT...	APPLICATION	TOTAL BYTES	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...	PEER IP ADI
"catch All"	Ex. <=50M	Ex. "Corporate	Ex. <=50M	Ex. 1.0	Ex. ECDH	Ex. ECDSA	Ex. AES_256_	Ex. SHA384	Ex. 10.255
ı All	4.79 K	HTTPS (unclassified)	4.79 K	TLS 1.2	ECDHE	RSA	AES_256_GCM/256	SHA384	10.4.80.10
oyee, ractors, iervers	--	HTTPS (unclassified)	--	TLS 1.2	ECDHE	RSA	AES_256_GCM/256	SHA384	10.4.48.75
oyee, ractors, iervers	--	HTTPS (unclassified)	--	TLS 1.2	ECDHE	ECDSA	AES_128_GCM/128	SHA256	13.78.187.5

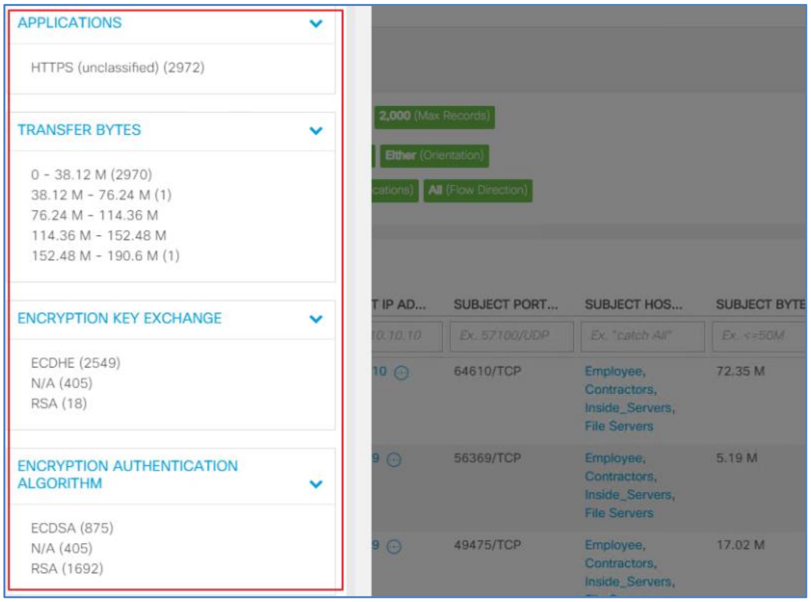
9. To produce a overview of the encryption information from the cipher suite used, click **SUMMARY.**



Manage Columns | Summary | Export

ENCRYPTION ...	ENCRYPTION KEY E...	ENCRYPTION ...	ENCRYPTION ...	ENCRYPTION ...	PEER IP ADDR...
Ex. 1.0	Ex. ECDH	Ex. ECDSA	Ex. AES_256_	Ex. SHA384	Ex. 10.255.25
TLS 1.2	ECDHE	RSA	AES_256_GCM/256	SHA384	10.4.80.10
TLS 1.2	ECDHE	RSA	AES_256_GCM/256	SHA384	10.4.48.75
TLS 1.2	ECDHE	ECDSA	AES_128_GCM/128	SHA256	13.78.187.58

10. This will bring up a panel on the side of your screen showcasing the information of the flow search in an organized view.



APPLICATIONS

HTTPS (unclassified) (2972)

TRANSFER BYTES

0 - 38.12 M (2970)
38.12 M - 76.24 M (1)
76.24 M - 114.36 M
114.36 M - 152.48 M
152.48 M - 190.6 M (1)

ENCRYPTION KEY EXCHANGE

ECDHE (2549)
N/A (405)
RSA (18)

ENCRYPTION AUTHENTICATION ALGORITHM

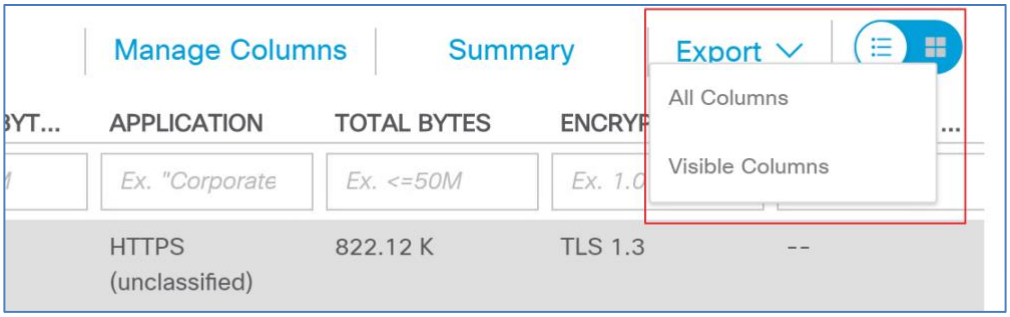
ECDSA (875)
N/A (405)
RSA (1692)

2,000 (Max Records) | Either (Orientation) | All (Flow Direction)

T IP AD...	SUBJECT PORT...	SUBJECT HOS...	SUBJECT BYTE
0.10.10	Ex. 57100/UDP	Ex. "catch All"	Ex. <=50M
10	64610/TCP	Employee, Contractors, Inside_Servers, File Servers	72.35 M
9	56369/TCP	Employee, Contractors, Inside_Servers, File Servers	5.19 M
9	49475/TCP	Employee, Contractors, Inside_Servers,	17.02 M

In the current version of Stealthwatch there is a known bug that is causing the **Encryption TLS/SSL Version** field from showing up in the summary view.

11. Once finished, you can click **Export** and choose either **all columns** or **visible columns** and it will be exported in CSV format to an Excel spreadsheet.

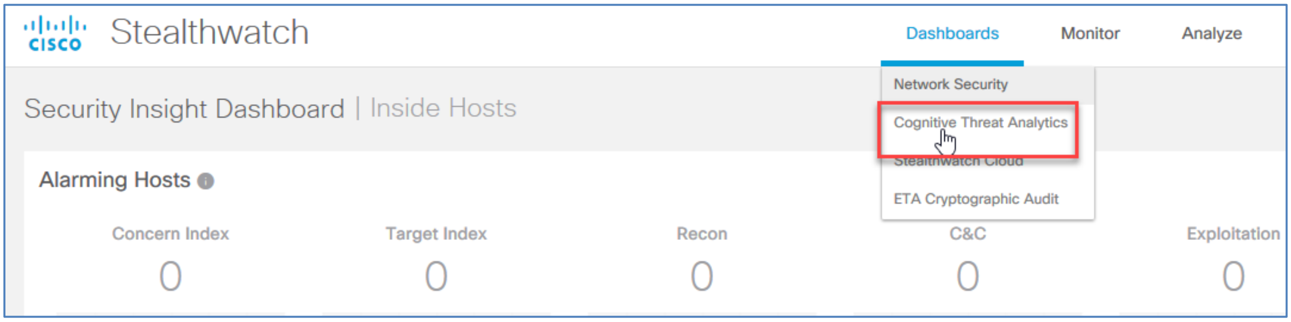


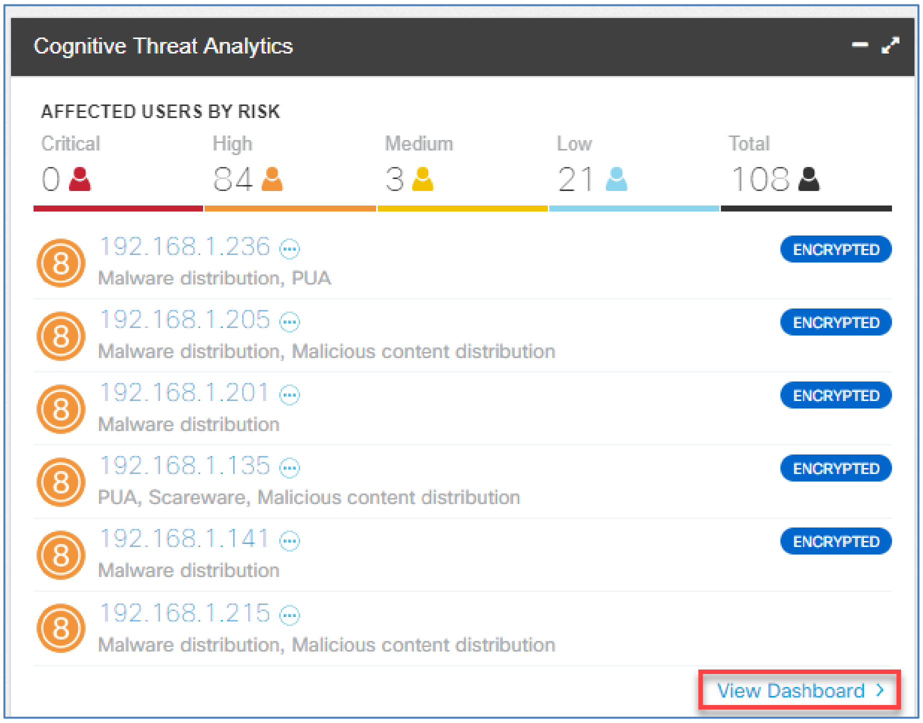
Investigate suspicious activity for malware through Cognitive Intelligence

The following information is meant to serve as a brief example of navigating the Cognitive Intelligence user interface to investigate infected hosts and suspicious activity. For complete information regarding portal administration and information regarding the fields displayed, refer to the Cisco ScanCenter Administrator Guide.

1. Access to the Cognitive Intelligence portal is integrated within the Stealthwatch Security Insight Dashboard. Within the SMC Dashboard, under **Dashboards**, access to the portal is available by selecting **Cognitive Treat Analytics** or by scrolling down to the Cognitive Intelligence widget as shown below and clicking **View Dashboard**.

   In looking at the Cognitive Intelligence widget in SMC, a summary of "Affected Users by Risk" can be seen. The blue "Encrypted" bubble next to each IP address below signifies that they had been classified as a result of ETA data elements within the Cognitive Intelligence cloud.





Cognitive Threat Analytics

AFFECTED USERS BY RISK

Critical	High	Medium	Low	Total
0	84	3	21	108

192.168.1.236 — ENCRYPTED
Malware distribution, PUA

192.168.1.205 — ENCRYPTED
Malware distribution, Malicious content distribution

192.168.1.201 — ENCRYPTED
Malware distribution

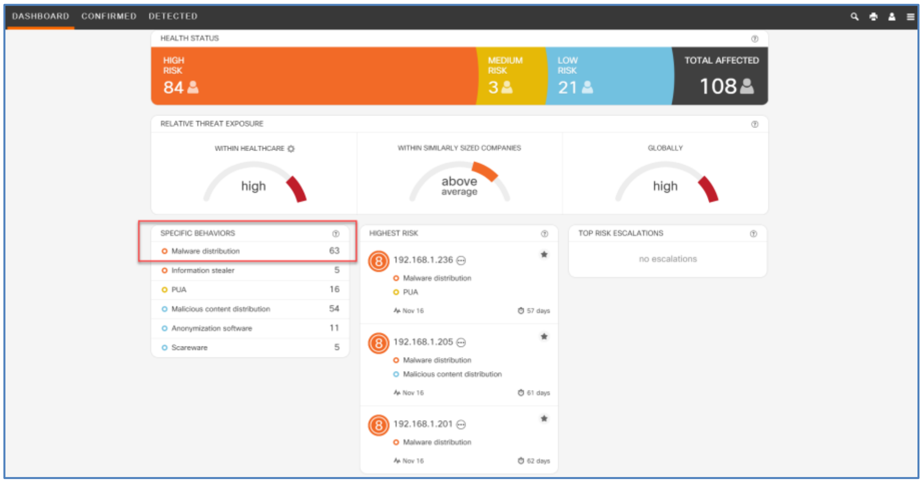
192.168.1.135 — ENCRYPTED
PUA, Scareware, Malicious content distribution

192.168.1.141 — ENCRYPTED
Malware distribution

192.168.1.215
Malware distribution, Malicious content distribution

View Dashboard >

2. Within the Cognitive Intelligence portal, the first view accessed is the Dashboard view. From this view, you are able to quickly view the overall health status of your network. Clicking any of the specific behaviors, such as **Malware Distribution**, displays a summary of compromised or suspicious endpoints.



HEALTH STATUS

HIGH RISK	MEDIUM RISK	LOW RISK	TOTAL AFFECTED
84	3	21	108

RELATIVE THREAT EXPOSURE

WITHIN HEALTHCARE	WITHIN SIMILARLY SIZED COMPANIES	GLOBALLY
high	above average	high

SPECIFIC BEHAVIORS

Malware distribution	63
Information stealer	5
PUA	16
Malicious content distribution	54
Anonymization software	11
Scareware	5

HIGHEST RISK

192.168.1.236
Malware distribution
PUA
Nov 16 — 57 days

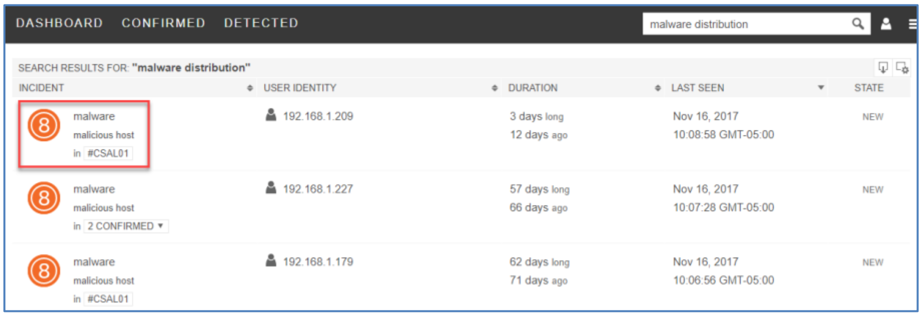
192.168.1.205
Malware distribution
Malicious content distribution
Nov 16 — 61 days

192.168.1.201
Malware distribution
Nov 16 — 62 days

TOP RISK ESCALATIONS

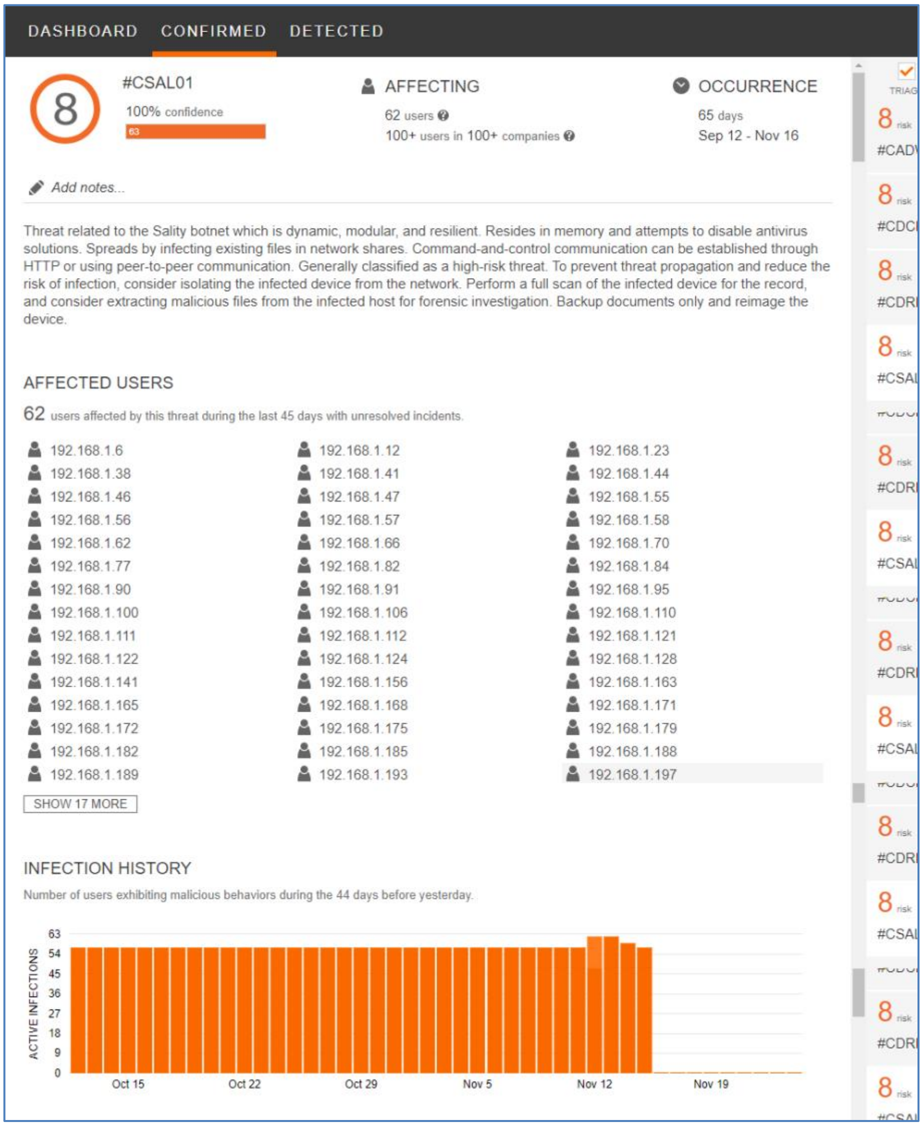
no escalations

3. With the summary information displayed, selecting the malware detected provides a description of the malware, as well as a summary of infected devices in your network.



SEARCH RESULTS FOR: **"malware distribution"**

INCIDENT	USER IDENTITY	DURATION	LAST SEEN	STATE
8 malware malicious host in #CSAL01	192.168.1.209	3 days long 12 days ago	Nov 16, 2017 10:08:58 GMT-05:00	NEW
8 malware malicious host in 2 CONFIRMED ▾	192.168.1.227	57 days long 66 days ago	Nov 16, 2017 10:07:28 GMT-05:00	NEW
8 malware malicious host in #CSAL01	192.168.1.179	62 days long 71 days ago	Nov 16, 2017 10:06:56 GMT-05:00	NEW



8 #CSAL01

100% confidence

63

AFFECTING

62 users

100+ users in 100+ companies

OCCURRENCE

65 days

Sep 12 - Nov 16

Add notes...

Threat related to the Sality botnet which is dynamic, modular, and resilient. Resides in memory and attempts to disable antivirus solutions. Spreads by infecting existing files in network shares. Command-and-control communication can be established through HTTP or using peer-to-peer communication. Generally classified as a high-risk threat. To prevent threat propagation and reduce the risk of infection, consider isolating the infected device from the network. Perform a full scan of the infected device for the record, and consider extracting malicious files from the infected host for forensic investigation. Backup documents only and reimage the device.

AFFECTED USERS

62 users affected by this threat during the last 45 days with unresolved incidents.

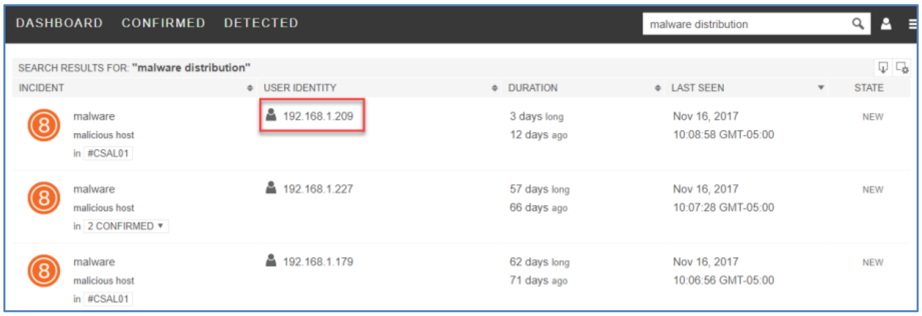
192.168.1.6	192.168.1.12	192.168.1.23
192.168.1.38	192.168.1.41	192.168.1.44
192.168.1.46	192.168.1.47	192.168.1.55
192.168.1.56	192.168.1.57	192.168.1.58
192.168.1.62	192.168.1.66	192.168.1.70
192.168.1.77	192.168.1.82	192.168.1.84
192.168.1.90	192.168.1.91	192.168.1.95
192.168.1.100	192.168.1.106	192.168.1.110
192.168.1.111	192.168.1.112	192.168.1.121
192.168.1.122	192.168.1.124	192.168.1.128
192.168.1.141	192.168.1.156	192.168.1.163
192.168.1.165	192.168.1.168	192.168.1.171
192.168.1.172	192.168.1.175	192.168.1.179
192.168.1.182	192.168.1.185	192.168.1.188
192.168.1.189	192.168.1.193	192.168.1.197

SHOW 17 MORE

INFECTION HISTORY

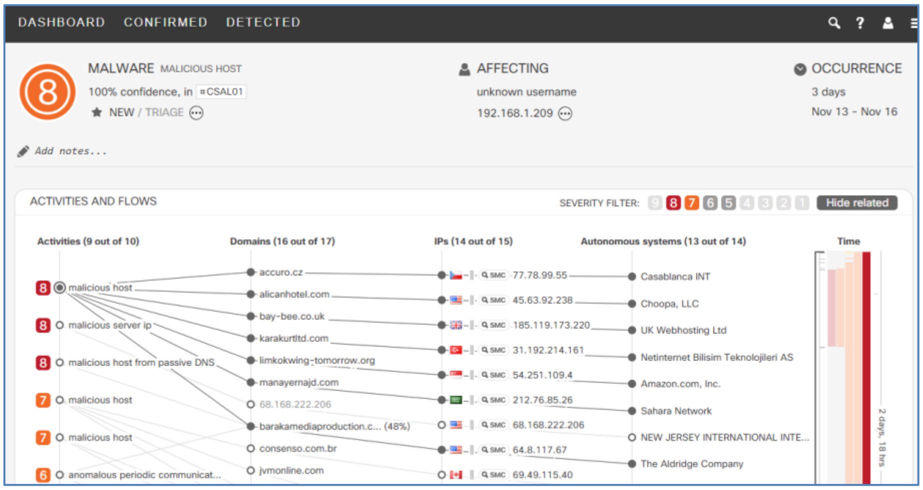
Number of users exhibiting malicious behaviors during the 44 days before yesterday.

4. From the summary information it is also possible for you to click an endpoint to view a histogram of activity leading up to the current security risk level (8 in this case).



SEARCH RESULTS FOR: **"malware distribution"**

INCIDENT	USER IDENTITY	DURATION	LAST SEEN	STATE
8 malware malicious host in #CSAL01	192.168.1.209	3 days long 12 days ago	Nov 16, 2017 10:08:58 GMT-05:00	NEW
8 malware malicious host in 2 CONFIRMED ▾	192.168.1.227	57 days long 66 days ago	Nov 16, 2017 10:07:28 GMT-05:00	NEW
8 malware malicious host in #CSAL01	192.168.1.179	62 days long 71 days ago	Nov 16, 2017 10:06:56 GMT-05:00	NEW



8 MALWARE MALICIOUS HOST
100% confidence, in #CSAL01
★ NEW / TRIAGE

AFFECTING
unknown username
192.168.1.209

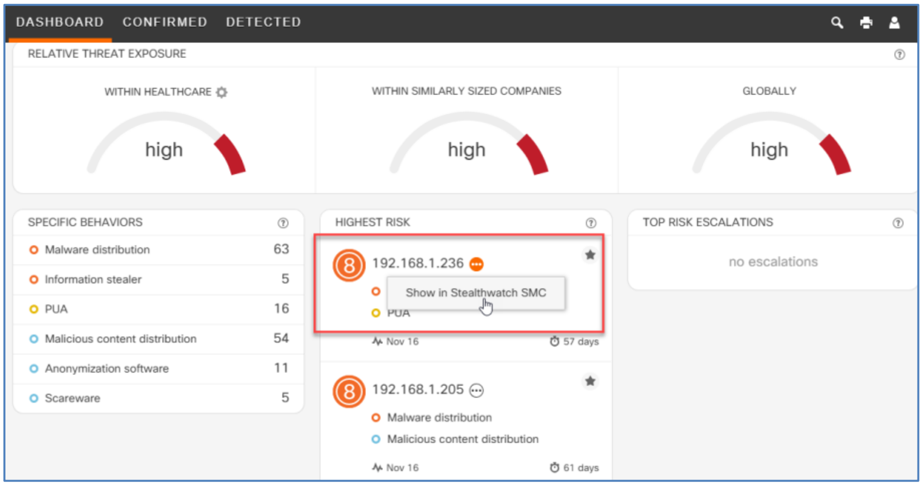
OCCURRENCE
3 days
Nov 13 - Nov 16

Add notes...

ACTIVITIES AND FLOWS

SEVERITY FILTER: 9 8 7 6 5 4 3 2 1 Hide related

5. At the Cognitive Intelligence dashboard, it is also possible to for you to view information that Stealthwatch has collected regarding an infected endpoint. To view that information, click on the **Show in Stealthwatch SMC** pop-up box that appears when you hover over the endpoint.



RELATIVE THREAT EXPOSURE

WITHIN HEALTHCARE	WITHIN SIMILARLY SIZED COMPANIES	GLOBALLY
high	high	high

SPECIFIC BEHAVIORS

Malware distribution	63
Information stealer	5
PUA	16
Malicious content distribution	54
Anonymization software	11
Scareware	5

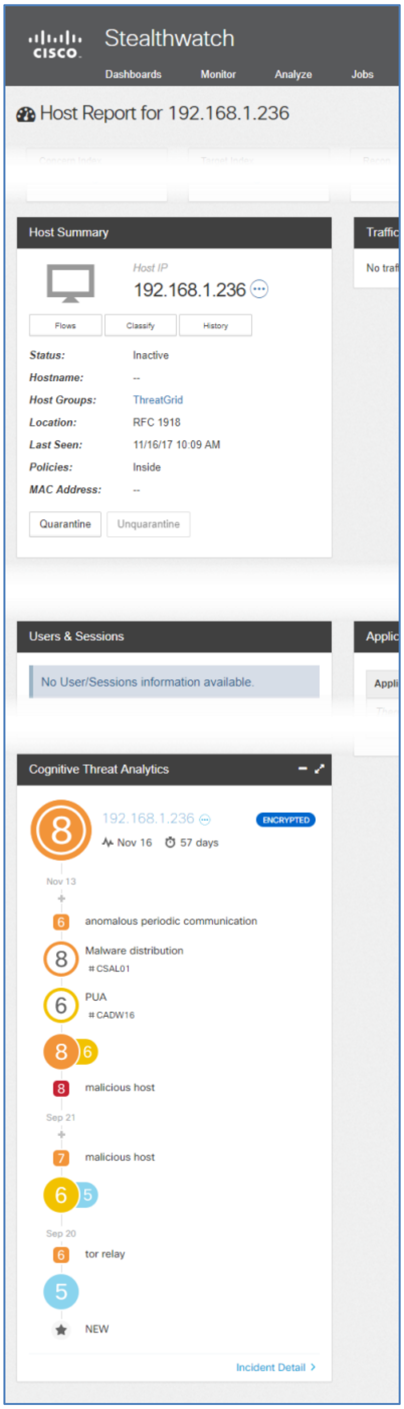
HIGHEST RISK

8 192.168.1.236
Show in Stealthwatch SMC
PUA
Nov 16 57 days

8 192.168.1.205
Malware distribution
Malicious content distribution
Nov 16 61 days

TOP RISK ESCALATIONS

no escalations



Host Report for 192.168.1.236

Host Summary

Host IP
192.168.1.236

Status:	Inactive
Hostname:	--
Host Groups:	ThreatGrid
Location:	RFC 1918
Last Seen:	11/16/17 10:09 AM
Policies:	Inside
MAC Address:	--

Users & Sessions

No User/Sessions information available.

Cognitive Threat Analytics

8 192.168.1.236 ENCRYPTED
Nov 16 57 days

Nov 13
6 anomalous periodic communication
8 Malware distribution
#CSAL01
6 PUA
#CADW16
8 6
8 malicious host
Sep 21
7 malicious host
6 5
Sep 20
6 tor relay
5
NEW

For further information regarding navigation of the Cognitive Intelligence user interface, refer to the "Threats Tab" section of the Cisco ScanCenter Administrator Guide.

About this guide

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unified Computing System (Cisco UCS), Cisco UCS B-Series Blade Servers, Cisco UCS C-Series Rack Servers, Cisco UCS S-Series Storage Servers, Cisco UCS Manager, Cisco UCS Management Software, Cisco Unified Fabric, Cisco Application Centric Infrastructure, Cisco Nexus 9000 Series, Cisco Nexus 7000 Series. Cisco Prime Data Center Network Manager, Cisco NX-OS Software, Cisco MDS Series, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

© 2019 Cisco Systems, Inc. All rights reserved.

Feedback & Discussion

For comments and suggestions about our guides, please join the discussion on Cisco Community.

Appendix A—New in this guide

This guide is new and is slightly updated from the previous version.

Appendix B—Hardware and software used for validation

This guide was validated using the following hardware and software.

Stealthwatch Enterprise and Cisco DNA Center

Product	License if Applicable	Recommended version
Cisco Stealthwatch Flow Collector	L-ST-FC-VE-K9	7.0 7.1
Cisco Stealthwatch Flow Collector	L-ST-SMC-VE-K9	7.0 7.1

ETA requires visibility of the connection between source and destination. A connection is equivalent to two flows; source IP to destination IP and destination IP to source IP. When planning the correct flow rate license to purchase, one must take this into account.

Cognitive Intelligence

Cognitive Intelligence is included by default in all Stealthwatch Enterprise licenses beginning with Stealthwatch v6.9.1. ETA is enabled in Stealthwatch v6.9.2.

No special software, hardware, or licensing is required other than Stealthwatch 6.9.4 or later. Cisco provides Cognitive Intelligence to any customer that owns term licensing via any buying method. Cisco fulfills requests for Cognitive Intelligence activation sent to the sw-cta-activation@cisco.com alias for customers with a valid Flow Rate license purchase. Requests for activation should include the customer's sales order information.

Catalyst Switches

Product	License if Applicable	Recommended version
Cisco Catalyst 9300 Series Switches	DNA Advantage	16.9.2 or later
Cisco Catalyst 9400 Series Switches		

Cisco Routers

Product	License if Applicable	Recommended version
Cisco 4000 ISR Series Routers	DNA Advantage	16.9.2 or later
Cisco Integrated Services Virtual Router (ISRv)*		
Cisco CSR 1000v Cloud Services Router*		
Cisco 1000 ISR Series Routers		
Cisco ASR 1001-X System, Crypto, 6 built-in GE, Dual P/S		
Cisco ASR 1002-HX System, Crypto, 8 built-in GE and 8 built-in 10GE ports, Dual P/S		
Cisco CSR 1000v- Amazon Web Services Bring Your Own License*		
Cisco ASR 1004 chassis, dual P/S		
Cisco ASR 1006 chassis, dual P/S		

Product	License if Applicable	Recommended version
Cisco ASR 1000 Embedded Services Processor, 20 Gb	DNA Advantage	16.9.2 or later
Cisco ASR 1000 Embedded Services Processor, 40 Gb		
Cisco ASR 1000 Embedded Services Processor, 100 Gb		
Cisco ASR 1000 Embedded Services Processor, 200 Gb		

Appendix C—Glossary

AAA authentication, authorization, and accounting

ACL access control list

AD Active Directory

AP Access Point

ASR Aggregation services router

AWS Amazon Web Services

AWS IGW Amazon Web Services internet gateway

BYOL Bring your own license

C&C server command and control server

CA certificate authority

CoA change of authorization

CSR certificate-signing request

CI Cisco Cognitive Intelligence

CVD Cisco Validated Design

DIA direct Internet access

DMVPN Dynamic Multipoint Virtual Private Network

DNS domain name system

DPI deep packet inspection

EC2 Elastic Computing 2

EHR electronic health record

ETA Encrypted Traffic Analytics

FC flow collector

FNF Flexible NetFlow

FPS flows per second

Gbps gigabits per second

GDOI Group Domain of Interest

GETVPN Group Encrypted Transport Virtual Private Network

GRE generic routing encapsulation

HIPAA Health Insurance Portability and Accountability Act

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol secure

IDP initial data packet

IoT Internet of things

IP Internet Protocol

IPS intrusion prevention system

ISE Cisco Identity Service Engine

ISR Integrated Services Router

IWAN Intelligent Wide Area Network

LAN local area network

Mbps megabits per second

mGIG multi gigabit

mGRE Multipoint Generic Routing Encapsulation

MnT monitoring and troubleshooting node

NaaS Network as a Sensor

NBAR Network-Based Application Recognition

NTP Network Time Protocol

PAN policy administration node

PSN policy service node

PCI payment card industry

PKI public key infrastructure

PoE Power over Ethernet

POS point of sale

PSN policy service node

pxGrid Platform Exchange Grid

RTC Rapid Threat Containment

SaaS software as a service

SPLT sequence of packet length and time

SSL Secure Sockets Layer

SVI switched virtual interface

TCP Transmission Control Protocol

TLS Transport Layer Security

UDP User Datagram Protocol

UPOE Cisco Universal Power over Ethernet

VASI virtual routing and forwarding aware software infrastructure

VLAN virtual local area network

VPC virtual private cloud

VPN virtual private network

VRF virtual routing and forwarding

VXLAN virtual extensible LAN

WAN wide area network

WLC wireless LAN controller

ZBFW zone-based firewall

Appendix D References

Cisco Catalyst 9300 Series Switches web page

Cisco Catalyst 9400 Series Switches

Cisco Cognitive Threat Analytics

Cisco CSR 1000v-BYOL version for AWS

Cisco Cyber Threat Defense Design Guide

Cisco DNA Center

Cisco Identity Services Engine web page

Cisco Platform Exchange Grid (pxGrid) web page

Cisco Rapid Threat Containment web page

Cisco Security web page

Cisco ScanCenter Administrator Guide

Cisco Stealthwatch Enterprise web page

Cisco TrustSec web page

Deploying the Cisco Cloud Services Router 1000V Series in Amazon Web Services, Design and Implementation Guide

Encrypted Traffic Analytics Router Configuration Guide

Encrypted Traffic Analytics White Paper

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

Stealthwatch Management Console User Guide