Encrypted Traffic Analytics

Solutions Adoption Prescriptive Reference—Design 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. Gartner estimates that more than 80% of enterprises' web traffic is encrypted in 2019. In fact, as of May 2019, 94% of all Google web traffic is encrypted. And nearly 80% of web pages loaded by Firefox use HTTPS.

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 using NetFlow, 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.

Deploying ETA technology provides the ability to identify malware communications in encrypted traffic through passive monitoring, the extraction of relevant data elements, and supervised machine learning with cloud-based global visibility, while also allowing you to perform a cryptographic assessment, identifying the elements of the encryption used such as:

- TLS version
- Encryption key exchange
- Encryption algorithm and key length
- Encryption authentication algorithm
- Encryption MAC

ETA extracts two main data elements: the initial data packet (IDP) and the sequence of packet length and time (SPLT). These elements are then communicated using a dedicated NetFlow template to Cisco Stealthwatch Enterprise. When used in conjunction with Flexible NetFlow, a complete view of the life of the flow is possible providing the capability to not only identify malicious traffic but anomalous behavior and customizable policy violations in your network utilizing

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

What is new in this version of the ETA for Cisco SD-Access Design Guide

There have been no significant changes to the design guidance for deploying ETA in a traditional, non-SD-Access fabric. Only a new minimum version of Cisco IOS XE has been specified in this document.

In the previous version of the ETA for Cisco SD-Access Validated Design, templates were used within Cisco DNA Center to provision, both ETA and FNF on the Cisco Catalyst 9300 and 9400 Series Switches. In this guide, the new Cisco Stealthwatch Security Analytics (SSA) service within Cisco DNA Center v 1.3.1 is used.

In the previous CVD, only the Cisco Catalyst® 9300 and 9400 fabric edge switches were discussed as they were the only switching platforms to support ETA. In this version of the CVD, coverage has been expanded to include the provisioning of Flexible NetFlow in support of Network as a Sensor (NaaS) on the Cisco Catalyst® 3850 and 3650 switches as well as the Catalyst 9200.

Cisco Catalyst® 3850, 3650, and 9200 switches do not support ETA.

What is Covered in This Document

This document provides design guidance for the deployment of NaaS with ETA, providing cryptographic assessment of the cipher suites used for TLS-encrypted communications, as well as the ability to identify malicious traffic in the encrypted communications of endpoints. Design guidance is provided for both Cisco SD-Access fabrics and traditional networking environments inclusive of resources and endpoints in LAN, WAN, and the Amazon Web Services (AWS) Cloud.

The ETA solution components discussed in this document consists of

- Cisco Stealthwatch Enterprise
- Cognitive Intelligence
- Cisco ISR4000, ISR1000, Cloud Services Router (CSR), Integrated Services Virtual Router (ISRv), and ASR1000 routers
- Cisco Catalyst 9300 and 9400 series switches
- Cisco DNA Center Controller within Cisco SD-Access fabrics
- Cisco Stealthwatch Security Analytics service (SSA)

The Cisco SSA service, and the automation it provides, will only be discussed within design guidance for SD-Access fabrics with Cisco DNA Center. The Cisco SSA service only supports the provisioning of the ASR1000 and ISR4000 series of routers.

What is Not Covered in This Document

This document does not provide prescriptive deployment and configuration guidance for any of the ETA solution components. These Prescriptive Deployment Guides can be found on Cisco.com in Design Zone for Campus Wired and Wireless LAN

This document is limited to enabling ETA in your network and does not provide design guidance around the deployment and installation considerations for Cisco Stealthwatch Enterprise and assumes an operational deployment in your network.

This document does not discuss LAN, wireless or WAN technology design and deployment considerations in traditional networks outside of those considerations influenced when deploying ETA.

Finally, this document does not discuss design and deployment considerations for Cisco DNA Center and the Cisco SD-Access fabric architecture other than design requirements to implement ETA.

About This Guide

This new ETA design guide consolidates information for both Cisco SD-Access fabrics with the Cisco DNA Center Controller and traditional networking environments which had been previously contained in two distinct documents into a single design guide. Due to differences in how NetFlow and ETA are deployed respective to the architecture deployed, separate sections have been written to accommodate deployment specific guidance. Along with the consolidated design guidance,

actual deployment and configuration guidance has been removed from this document and can now be found in two new prescriptive deployment guides which can be found here Design Zone for Campus Wired and Wireless LAN.

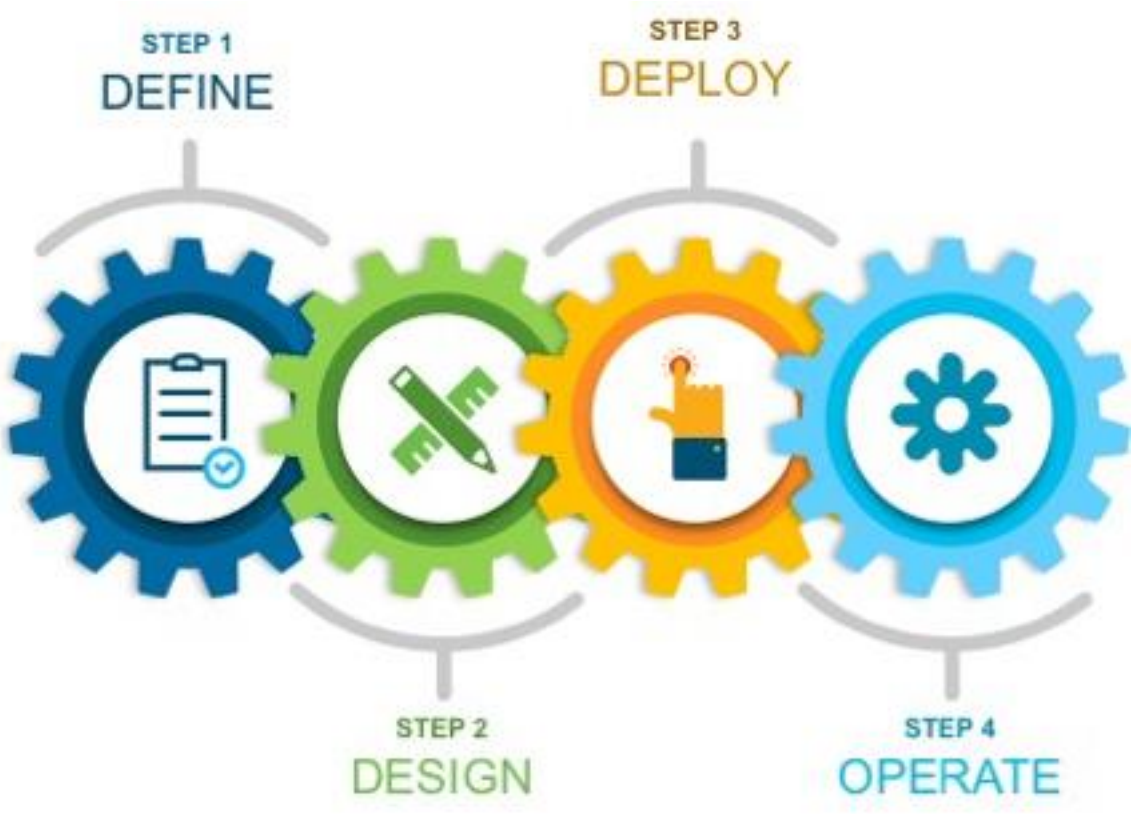


Figure 1 Implementation Flow

This document contains two major sections:

- The **Define** section defines problem areas and provides information about how to plan for deployment, and other considerations.
- The **Design** section shows how to design a secure, wired access network.

For guidance regarding deployment and operation, please refer to the ETA prescriptive deployment guide for either traditional or Cisco SD-Access network architectures which can be found in Design Zone for Campus Wired and Wireless LAN.

Define

Audience

This document is intended for use by network administrators and security administrators where applicable in implementing Flexible NetFlow and ETA within their networks adhering to best practices tested by Cisco.

Purpose of this document

This guide describes how to enable NaaS with ETA, providing both cryptographic assessment of the cipher suites used for Transport Layer Security (TLS)-encrypted communications as well as the ability to identify malicious traffic patterns with the encrypted traffic of users in both campus and branch networks. Also included is ability to monitor traffic to and from resources located in the Amazon Web Services (AWS) cloud. This Cisco Validated Design discusses the use of Cisco Stealthwatch® Enterprise when integrated with Cisco Cognitive Intelligence in passively monitoring encrypted endpoint and server traffic traversing Cisco Catalyst® 9300 and 9400 Series Switches or Cisco IOS® XE based routers, such as the Cisco ASR 1000 Series, 4000 Series Integrated Services Routers (ISRs), 1000 Series ISR, Integrated Services Virtual Router (ISRv), and Cloud Services Router (CSR) 1000v supporting ETA and Flexible NetFlow (FNF).

This ETA design guide will discuss the considerations necessary for you to decide where and how to deploy ETA and Flexible NetFlow to reap the full benefits of Cisco Stealthwatch's security analytics capabilities. It provides two simple use cases depicting the additional benefit that ETA provides in either Cisco SD-Access fabrics or traditional networking architectures over the original NaaS solution.

Solution design summary

The ETA solution makes use of NetFlow and ETA data collection at network devices throughout your network. Data that is collected from the Catalyst 9000 series switches and IOS-XE based ISR and ASR 1000 series routers is then exported via NetFlow v9 to Cisco Stealthwatch flow collectors in your network for processing of the flow data. By default, metadata from Internet bound traffic is sent to Cognitive Intelligence, a Cisco cloud-based service where it is processed via machine learning for identification of potential malware. The result of this processing in the event of suspicious traffic is then categorized and communicated back to your Cisco Stealthwatch Enterprise management console.

The two use cases for ETA that will be discussed in this document are cryptographic assessment or crypto audit and malware detection.

Flexible NetFlow and ETA

ETA makes use of specialized IDP and SPLT templates for collection of metadata used in the analysis of the encrypted data traffic. This data is then exported as dedicated NetFlow or IPFIX records to Cisco Stealthwatch flow collectors where initial analysis is performed. Upon enabling ETA globally on the network device using the `et-analytics` command, a dedicated NetFlow v9 or IPFIX, record, monitor, and exporter are automatically enabled and configured on the network device. The ETA record definition is not customizable and will be used in conjunction with a separate, user defined Flexible NetFlow configuration to be discussed.

IPFIX is supported today with Cisco Stealthwatch Enterprise as well as on supported IOS XE based routers running minimally 16.12.1. IPFIX on the Catalyst 9300 and 9400 is not supported at the time of publication of this document.

The following tables depicting the IDP and SPLT templates list those NetFlow key and non-key fields included in the exported record when ETA is enabled. As you can see, this is a small subset of the data elements that can be collected via FNF, which is why ETA and FNF are configured.

Table 1 IDP template

Information element	Flow key	NetFlow v9 length
sourceIPv4Address (sourceIPv6Address)	Y	4 (16)
destinationIPv4Address (destinationIPv6Address**)**	Y	4 (16)
sourceTransportPort	Y	2
destinationTransportPort	Y	2
protocolIdentifier	Y	1
flowStartSysUpTime	N	4
flowEndSysUpTime	N	4
**packetDeltaCount	N	8
**octetDeltaCount	N	8
initialDataPacket (v9), or ipHeaderPacketSection (IPFIX)	N	1300

Table 2 IDP template

Information element	Flow key	NetFlow v9 length
sourceIPv4Address (sourceIPv6Address)	Y	4 (16)
destinationIPv4Address (destinationIPv6Address**)**	Y	4 (16)
sourceTransportPort	Y	2
destinationTransportPort	Y	2
protocolIdentifier	Y	1
flowStartSysUpTime	N	4
flowEndSysUpTime	N	4
**packetDeltaCount	N	8
**octetDeltaCount	N	8
Sequence of Packet Lengths and Times (SPLT)	N	40

**The PACKETDELTACOUNT and OCTETDELTACOUNT information elements have been removed in IOS XE 17.1.1 for supported routers and the Catalyst 9300 and 9400 switches.

Although it is possible to configure just ETA, it is necessary to also configure FNF for analysis of encrypted traffic in the Cognitive Intelligence cloud for malware detection. This is because ETA sends only information about the IDP and SPLT collected and processed by the switch. For full NetFlow statistics containing connection and peer information such as number of bytes, packet rates, round trip times, and so on, you must also configure FNF. For the singular purpose of performing a crypto audit, however, it is only necessary to enable ETA on the switch.

Crypto audit

Crypto audit is the capability of viewing/reporting and eventually alerting and alarming on the crypto fields in the Cisco Stealthwatch database. The crypto audit functionality provides detailed information about the cipher suites used for HTTPS communications, including the encryption version, key exchange, key length, cipher suite, authentication algorithm, and hash used.

With the crypto audit functionality enabled by ETA, the unencrypted metadata in the client hello and clientKeyExchange messages provides information that is used to make inferences about the client's TLS library and the cipher suites used. The collection of this information begins with the initial data packet (IDP), or first packet of the flow, and continues through subsequent messages that make up the TLS handshake. This data is exported by the device via NetFlow to the Cisco Stealthwatch flow collector. Once collected, these records can be queried by the Cisco Stealthwatch Management Console (SMC) for analysis.

These flow records can be collected by a Cisco Stealthwatch flow collector over a period of time and subsequently filtered, searched through, and reported on by the SMC for auditing purposes helping ensure that the most secure cipher suites are used to secure confidential information, as well as providing evidence of regulatory compliance.

Malware detection

When implementing ETA, in addition to cryptographic assessment, the metadata collected can be used to detect malware within the encrypted traffic without the need to decrypt the traffic when Cisco Stealthwatch is integrated with Cognitive Intelligence. When Flexible NetFlow and DNS information is combined with the ETA metadata found in the IDP, other ETA data elements such as the sequence of packet length and times (SPLT) provide a unique and valuable means of identifying malware through the detection of suspicious traffic.

SPLT telemetry is composed of a set of two parameters describing each of the first few packets of a flow—the length of the application payload in that packet and the interarrival time from the previous packet. Only packets that carry some application payload are considered; the rest (such as SYN or SYN/ACK) are ignored. The SPLT provides visibility beyond the first packet of the encrypted flows. The analysis of the metadata contained in the IDP and SPLT greatly enhance the accuracy of malware detection in the Cognitive Intelligence cloud.

By default, only traffic, including DNS queries, crossing the enterprise network perimeter (i.e., Internet bound) and outside of the enterprise address space, which may also be referred to as the "trust boundary," is sent to the Cognitive Intelligence cloud for malware analysis. All traffic is monitored, and records are exported to the Cisco Stealthwatch flow collector. After processing, the flow collector sends only the metadata for this external traffic to the Cognitive Intelligence cloud in an encrypted TLS tunnel for further analysis, as shown below. All other internal traffic will be processed by the flow collector for conformance to policies established at Cisco Stealthwatch as well as for cryptographic assessment based on ETA data.

The enterprise address space or trust boundary is administered through the Host Groups definitions at the SMC. By default, a CATCH ALL host group is defined and consists of the RFC1918 address space. For more information on how to change the default behavior to include internal address space, see "Deployment Considerations" in the next section of this document.

The following two diagrams depict this data collection for both traditional networks and Cisco SD-Access fabric.

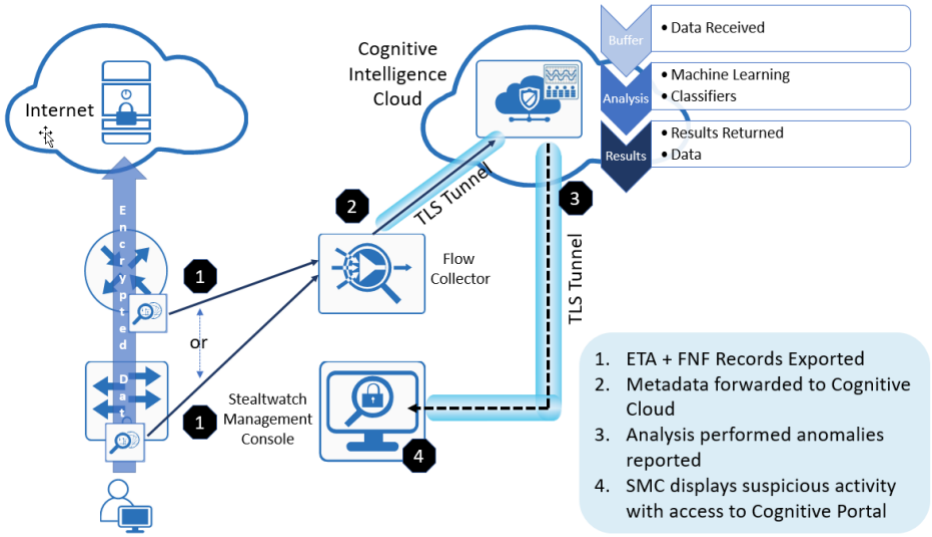


Figure 2 ETA malware detection traditional network

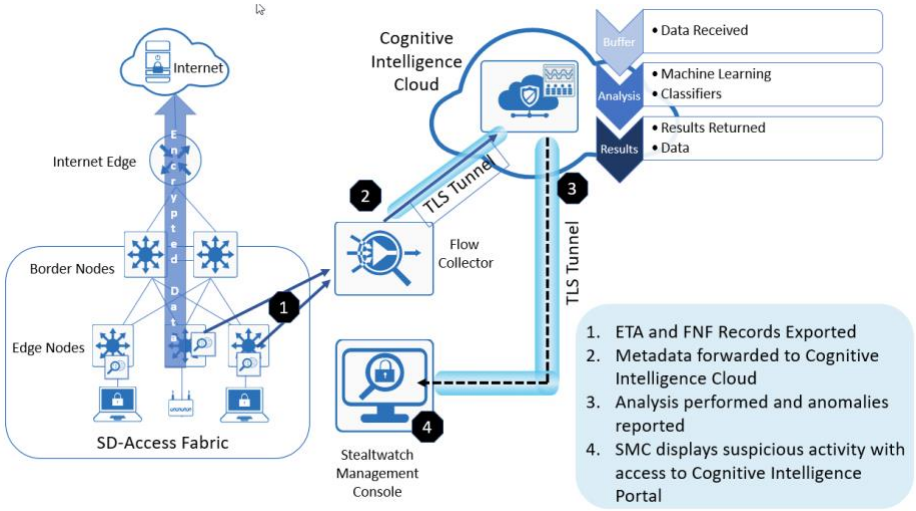


Figure 3 ETA malware detection in SD-Access fabric

Initially, after establishing connectivity between your Cisco Stealthwatch deployment and the Cognitive Intelligence cloud, there will be a brief "training" period in which analysis results will not be immediately displayed at the SMC. Rather than decrypting the traffic, Cisco Stealthwatch with Cognitive Intelligence uses machine-learning algorithms. The training period allows the system to learn the behavior of the customer network. The length of the training period depends entirely on the amount of traffic seen. Once this initial period is complete, Cognitive Intelligence analyzes the encrypted traffic data elements within the ETA records by applying machine learning and statistical modeling with existing classifiers. The global risk map and ETA data elements reinforce each other in the Cognitive Intelligence engine. Together, these algorithms and elements pinpoint malicious patterns such as data exfiltration in encrypted traffic to help identify threats and improve incident response times.

Cisco's Cognitive Intelligence processes the ETA and NetFlow data in a dedicated data center. Deployment is aligned on the security and data governance principles applied in production and complies with Cisco cloud-operations standards regulating security and privacy attributes. Input data is typically processed within 2 to 4 hours and is erased after processing.

Solution 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 communications 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.

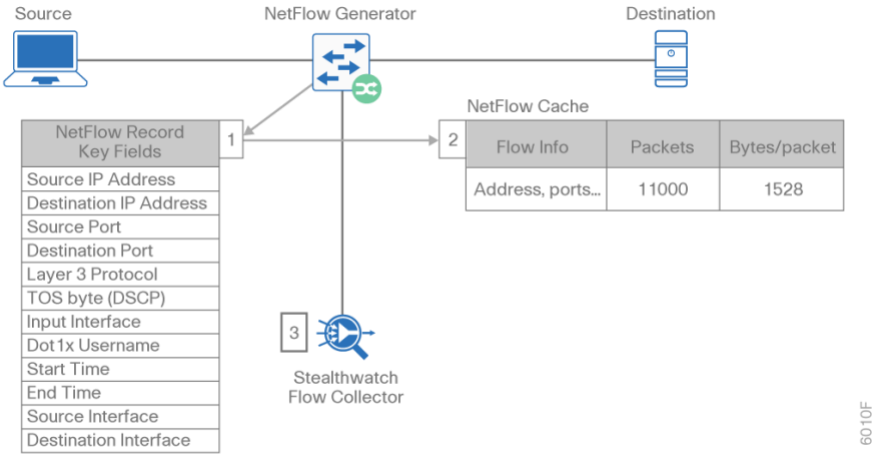


Figure 4 NetFlow operation on a network device

For more information, see the Cisco IOS NetFlow web page.

Cisco Stealthwatch Enterprise

Cisco Stealthwatch® Enterprise provides enterprise-wide network visibility and applies advanced security analytics to detect and respond to threats in real time. Using a combination of behavioral modeling, machine learning, and global threat intelligence, Cisco Stealthwatch Enterprise can quickly, and with high confidence, detect threats such as command-and-control (C&C) attacks, ransomware, distributed-denial-of-service (DDoS) attacks, illicit cryptomining, unknown malware, and insider threats. With a single, agentless solution, you get comprehensive threat monitoring across the entire network traffic, even if it's encrypted.

This visibility allows a Cisco 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. Cisco Stealthwatch has different alarm categories using many different algorithms that watch behavior and identify suspicious activity. Cisco 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 and alerting when policies defining abnormal behavior are matched.

For more information, see the Cisco Stealthwatch web page.

Cisco Stealthwatch v7.1 Flow Sensor

The Flow Sensor is an optional component of Cisco Stealthwatch Enterprise and produces telemetry for segments of the switching and routing infrastructure that can't generate NetFlow natively. It also provides visibility into the application layer data. In addition to all the telemetry collected by Cisco Stealthwatch, the Flow Sensor provides additional security context to enhance the Cisco Stealthwatch security analytics. And starting with Cisco Stealthwatch Software Release 7.1, Flow Sensor is also able to generate enhanced ETA telemetry to be able to analyze encrypted traffic. Advanced behavioral modeling and cloud-based, multilayered machine learning is applied to this dataset to detect advanced threats and perform faster investigations. The Flow Sensor is installed on a mirroring port or network tap and generates telemetry based on the observed traffic.

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. It is a cloud-based product that uses machine learning and statistical modeling of networks. Cognitive Intelligence 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 an 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.

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.

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 can support 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 Switch web page.

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.

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.

Cisco Software-Defined Access and Cisco DNA Center

Cisco Digital Network Architecture (Cisco DNA™) provides a roadmap to digitization and a path to realize immediate benefits of network automation, assurance, and security. Cisco's SD-Access architecture is the Cisco DNA evolution from traditional campus LAN designs. Cisco SD-Access uses Cisco DNA Center for designing, provisioning, applying policy, and providing campus wired and wireless network assurance for an intelligent network. Fabric technology, an integral part of SD-Access, introduces programmable overlays, enabling easy-to-deploy network virtualization across the wired and wireless campus. In addition to network virtualization, fabric technology provides software-defined segmentation and policy enforcement based on user identity and group membership. Software-defined segmentation is seamlessly integrated using Cisco group based policy technology, providing micro-segmentation through the use of scalable groups within a virtual network. Using Cisco DNA Center to automate the creation of virtual networks reduces operational expenses, as well as reducing risk, due to Cisco DNA Center's integrated security and improved network performance provided by the assurance and analytics capabilities.

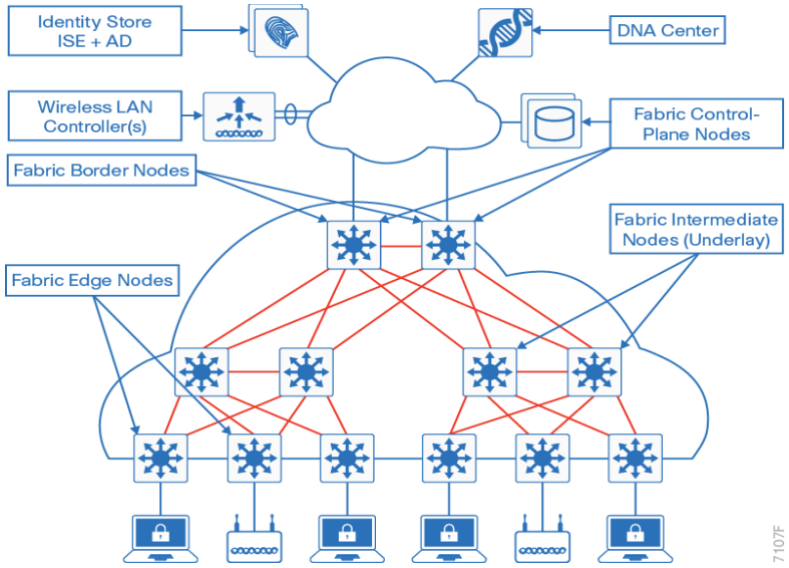


Figure 5 Cisco SD-Access architectural components

For more information see, Cisco Digital Network Architecture (Cisco DNA)

Customer Use Cases

Crypto Audit and Malware Detection in encrypted traffic

When implementing the NaaS with ETA solution, traffic encrypted using transport layer security (TLS) or even older libraries such as secure socket layer (SSL) may now be audited to ensure that the latest TLS libraries and cipher suites are being used to encrypt sensitive communications between clients and servers. The crypto audit capability inherent to ETA can inspect the data elements of the IDP and subsequent TLS handshake messages and, using NetFlow, export this information for auditing purposes.

Along with the crypto audit capability, traffic bound for the Internet can be further analyzed without the need to decrypt the traffic for possible signs of malware and data exfiltration through Cisco Stealthwatch integration with Cognitive Intelligence. As Cisco Stealthwatch analyzes the ETA and FNF exported data, metadata of traffic destined to addresses outside of the enterprise address space is forwarded to the Cognitive Intelligence Cloud services for processing.

As discussed earlier, the crypto audit capability, when combined with FNF, provides insightful information about encrypted traffic patterns between endpoints, servers, and IoT devices. This information is leveraged in detecting the use of flawed libraries, suboptimal cipher suites, and potentially suspicious communications when combined with Cisco Cognitive Intelligence.

The following use cases provide some examples of the benefits of the crypto audit functionality and ability to detect malware when you implement the Cisco NaaS 2.0 with ETA solution.

Healthcare use case, Cisco SD-Access fabric

With the ever-increasing growth in electronic health records (EHRs), healthcare organizations have begun to deploy EHR systems not only on-premises but in hybrid clouds and, in the case of smaller organizations, completely cloud-based implementations. Communications with these cloud-based services must be secured to protect patient health information subject to Health Insurance Portability and Accountability Act (HIPAA) compliance; thus, when accessing the EHR servers, endpoints use HTTPS for communications.

Business problem

Healthcare organizations must ensure that the most secure TLS libraries and cipher suites are used for communications between wired workstations throughout the medical facility and the EHR systems, regardless of where the workstations and EHR systems are deployed. As access to EHR services in the cloud continues to become more common and in some cases required, these communications need to be analyzed more closely for any signs of suspicious activity.

The following diagram depicts communication between a local medical server, a bedside monitor, and a nurse's workstation, as well as communications between these devices and a cloud-based EHR system in a Cisco SD-Access fabric.

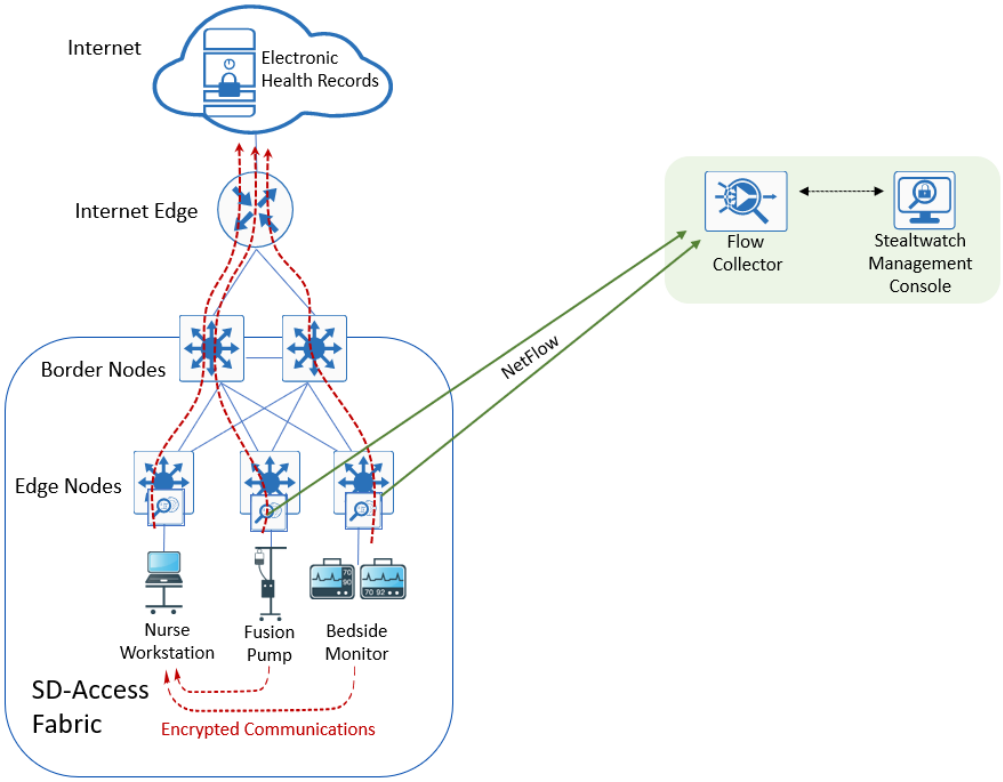


Figure 6 Encrypted medical communications in Cisco SD-Access fabric

The edge nodes to which these devices are attached support Flexible NetFlow; however, all communications are encrypted using HTTPS for transport. The information collected via NetFlow shows that the application is HTTPS and provides information relative to source and destination addressing as well as other characteristics of the flow, but nothing further. The only means to check that TLS and not SSL is used, and what version of either has been negotiated, is through a packet capture to collect the IDP and subsequent handshake messages at the switch, as well as additional confirmation of the settings at the endpoint itself.

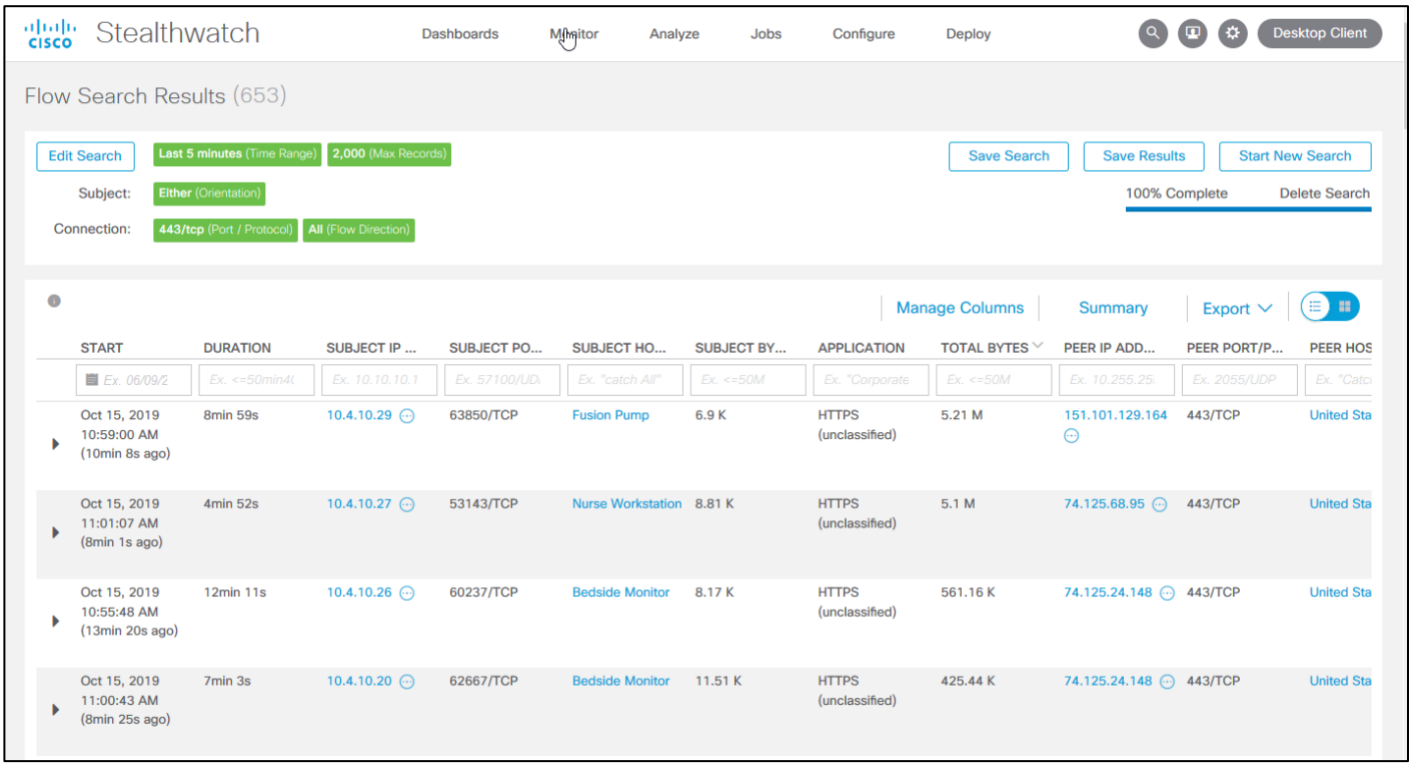


Figure 7 Cisco Stealthwatch display without ETA Healthcare Solution

Solution

With Cisco Catalyst 9000 access switches at the fabric edge running IOS-XE 16.6.4 or later and Cisco Stealthwatch Enterprise 6.9.4 or later, you can enable ETA and FNF on the edge nodes and passively monitor encrypted flows. During the initial conversation between the bedside monitor and the nursing station, the client's IDP initiating the TLS handshake and several subsequent unencrypted messages are collected. Once exported to the NetFlow collector, the unencrypted metadata can be used to collect information regarding the cipher suite, version, and client's public key length as reported by the cipher suite. Additionally, all traffic destined to cloud-based services will be analyzed by Cisco Stealthwatch enhanced with Cognitive Intelligence for any suspicious activity.

The client's actual public key length is not collected. Cisco Stealthwatch displays information about the key reported by the cipher suite.

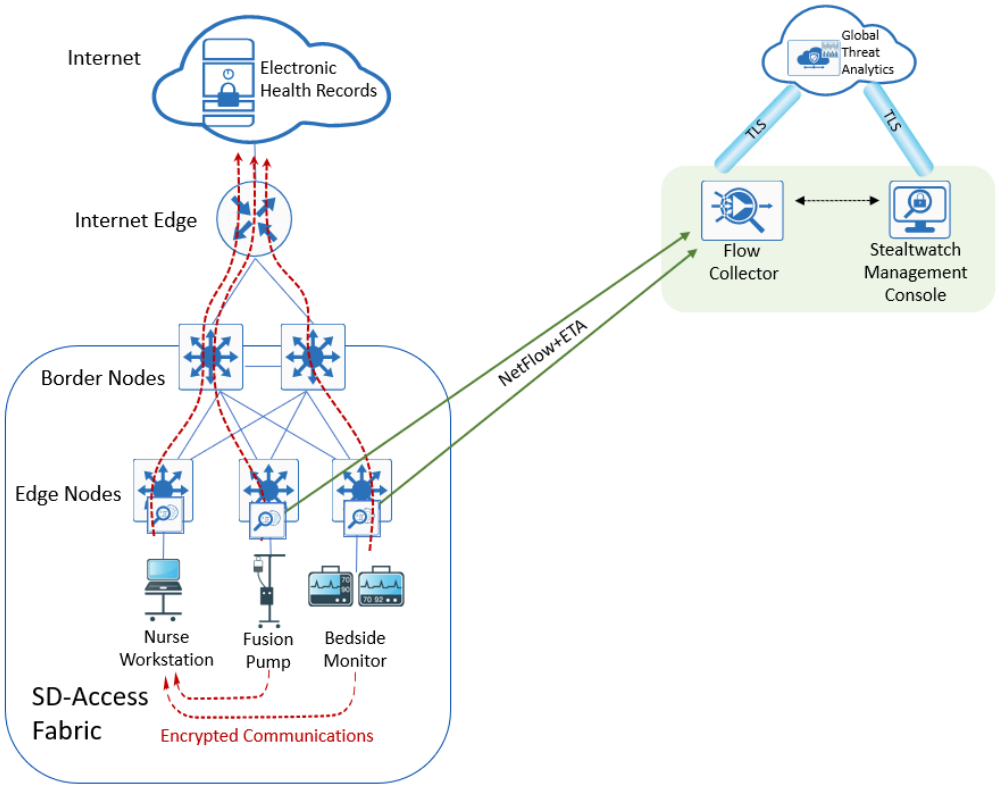


Figure 8 Addition of ETA in Healthcare Cisco SD-Access fabric

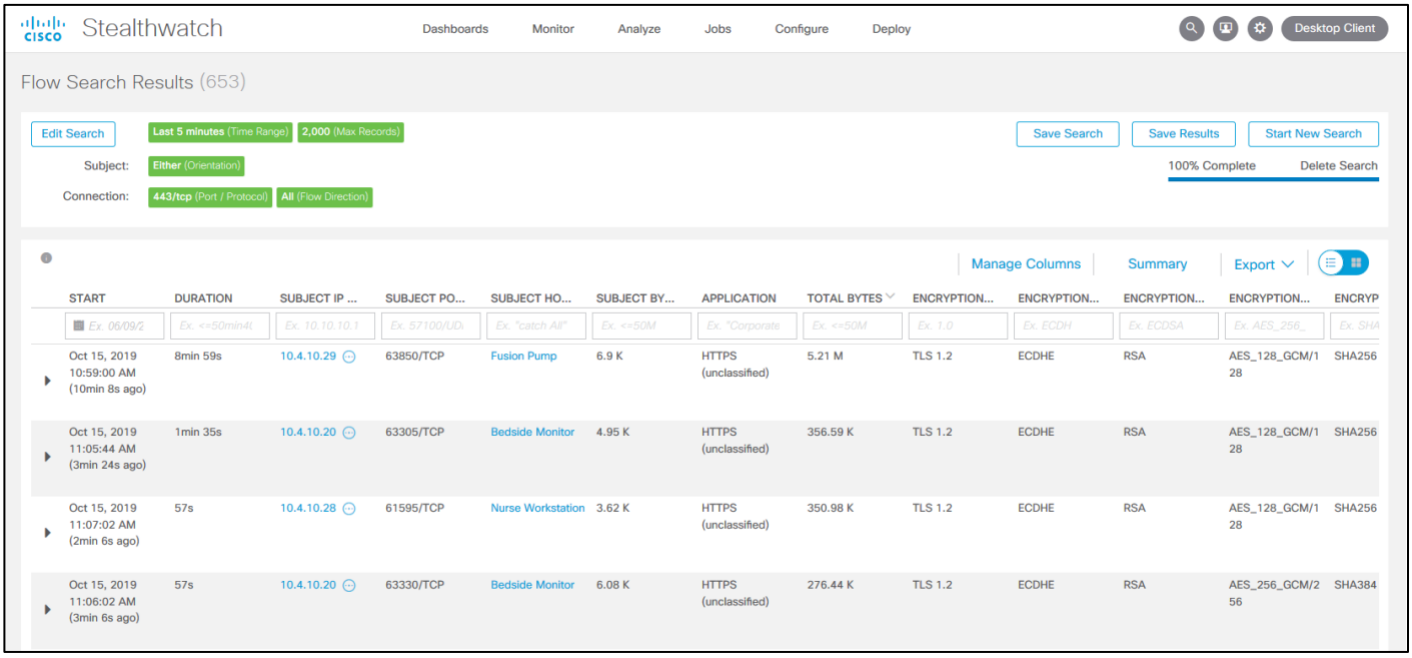


Figure 9 Cisco Stealthwatch display with ETA and FNF

With the integration of Cognitive Intelligence, it is also possible to be alerted to suspicious behavior on the Cisco Stealthwatch dashboard and investigate whether a device has been compromised within the Cognitive Intelligence portal, as seen below.

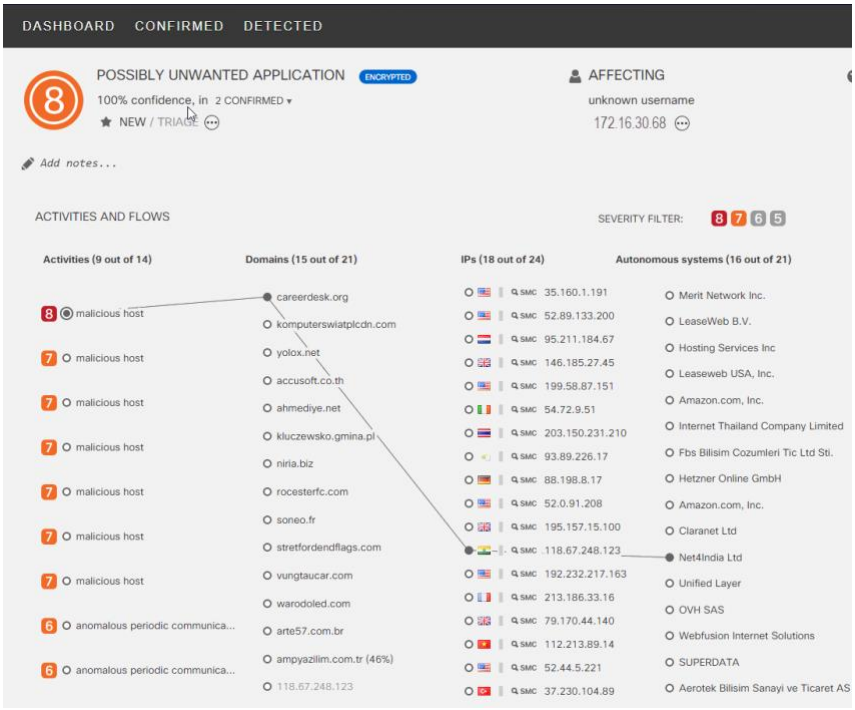


Figure 10 Malware in encrypted medical traffic

Retail PCI use case in traditional Campus LAN/WAN networks

Merchants conducting credit card transactions are all required to conform to the Payment Card Industry (PCI) Data Security Standard. Evidence of this conformance is completed through a PCI audit. During the PCI audit, the merchant's network security is audited for conformance to a set of requirements established and maintained by the PCI Security Standards Council.

Depending on the number of credit card transactions conducted in a year, the merchant might be subject to an annual audit while others may be required only to complete a Self-Assessment Questionnaire along with Attestation of Compliance, as well as documentation detailing validation results and compliance controls.

The scope of the PCI audit includes the collection, temporary storage, and transmission of credit card data encompassing the point-of-sale (POS) terminals; network infrastructure, including cryptography used to secure communications; servers and storage; and potentially onsite payment gateways communicating with the payment processor.

Business problem

In preparation for an upcoming PCI audit, part of which will revolve around wired POS terminals, a retailer operating numerous department stores needs to provide evidence of libraries of cipher suites used to encrypt credit card transactions. Auditing of encrypted communications between the POS terminal and an onsite payment gateway and the subsequent communications from the gateway to the payment processor will be in scope.

In addition to the audit of the cipher suites used, the auditor will request additional information regarding communications between payment gateways and cloud-based payment processors. Typical firewall and IPS logs will be presented, after having been inspected with additional correlation of any suspicious events found in the logs.

The following diagram depicts communication between POS terminals and the payment gateway in the enterprise, as well as communications between the payment gateway and a cloud-based payment processor system.

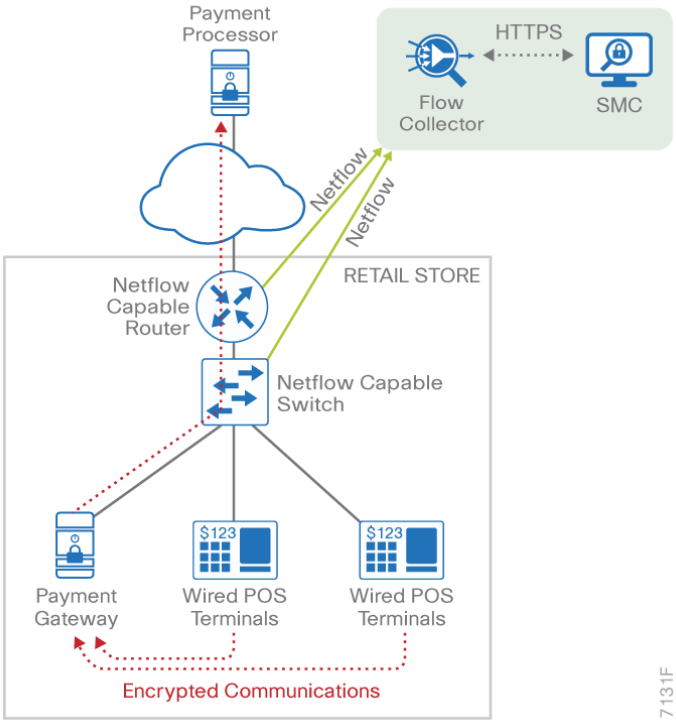


Figure 11 Auditing encrypted credit card transaction with FNF in a traditional network

The merchant has been upgrading many older POS terminals, which previously supported only TLS 1.0 with its known vulnerabilities, to now support TLS v1.2, in preparation for its annual audit and as a result of the PCI Council's deprecation of TLS 1.0. The merchant is looking for a means to provide a report showing TLS libraries and the cipher suites used to encrypt these credit card transactions, both to confirm the status of the upgrade process as well as to be used later as evidence of compliance with the auditors. Although FNF provides valuable information relative to communications between devices in scope for the audit, it does not provide detailed information regarding the encryption techniques used, as seen in the following figure.

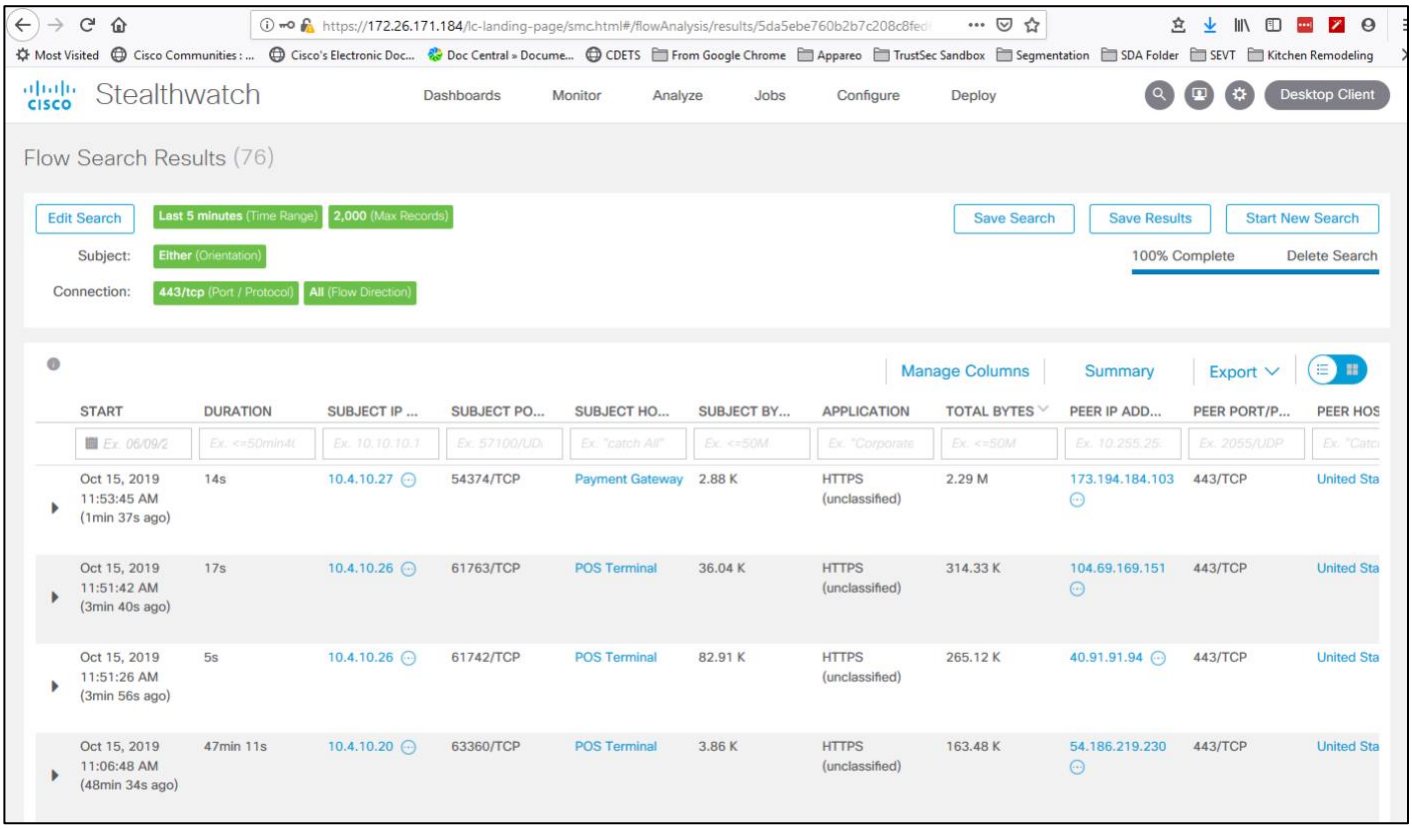


Figure 12 Cisco Stealthwatch display without ETA retail

Solution

With Cisco Catalyst 9300and 9400 access switches or ISR 1000 and 4000 Series, ASR 1000 Series, ISRv, or CSR 1000v routers running IOS XE 16.6.4 or later and Cisco Stealthwatch Enterprise running 6.9.4 or later, you can enable ETA and Flexible NetFlow on switch or router interfaces and passively monitor encrypted flows. During the initial conversation between the POS terminal and payment gateway or the payment gateway and the payment processor, the IDP initiating the TLS handshake and several subsequent unencrypted messages are collected. Once exported to the NetFlow collector, the unencrypted metadata can be used to collect information regarding the cipher suite, version, and client's public key length as reported by the cipher suite. Additionally, all traffic destined to cloud-based services will be analyzed in the Cognitive Intelligence cloud for any suspicious activity.

The client's actual public key length is not collected. Cisco Stealthwatch displays information about the key reported by the cipher suite.

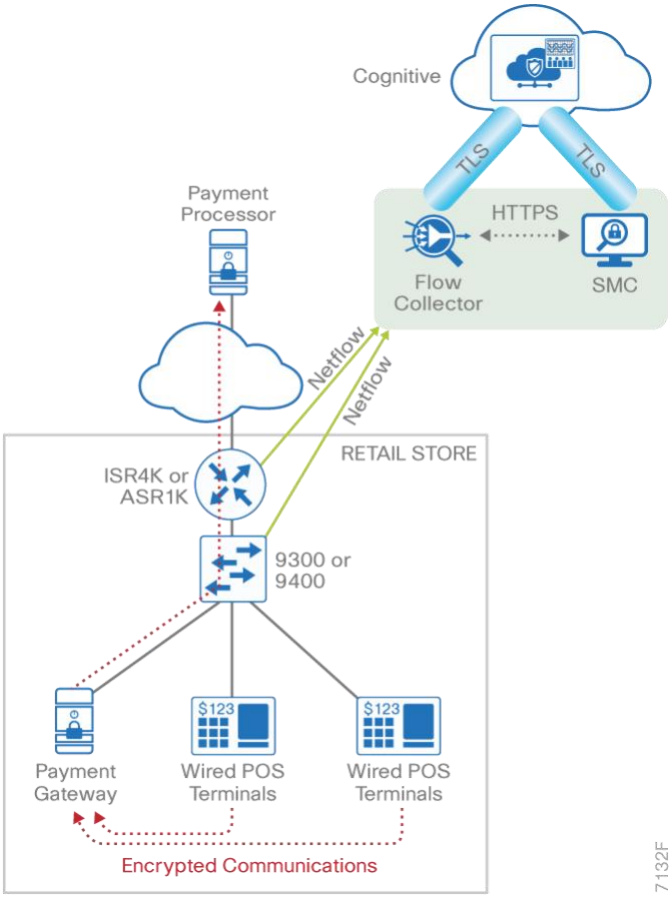


Figure 13 Addition of ETA in retail network

Now the merchant can audit encrypted communications between wired POS terminals distributed throughout the store and the payment gateway in order to ensure that all devices are compliant. Additionally, encrypted communications between the payment gateway and the processor can be verified and monitored for any suspicious activity, using both Cisco Stealthwatch and the Cognitive Intelligence cloud.

With Cisco Stealthwatch and ETA, the merchant can perform a crypto audit throughout the network to ensure that all devices have been upgraded while also using the results of the assessment to serve as validation of its compliance.

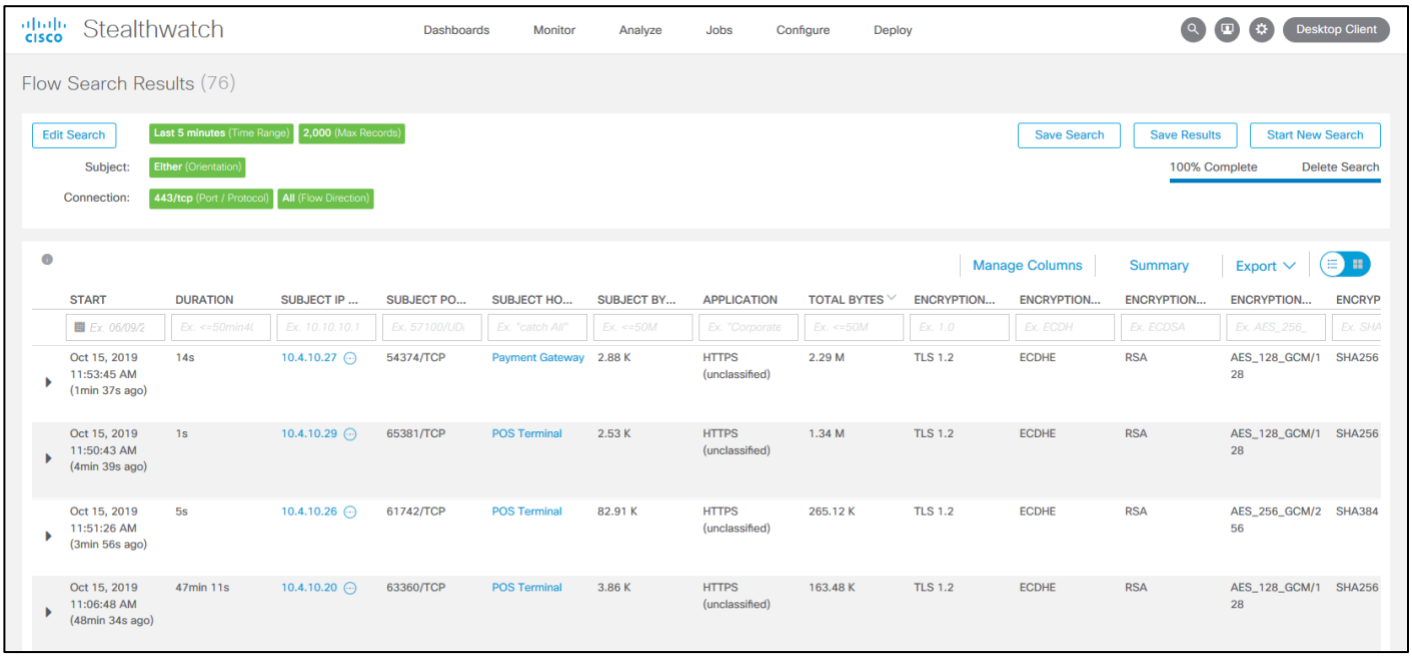


Figure 14 Cisco Stealthwatch display with ETA

If suspicious activity is detected during the pre-audit review of firewall and IPS logs, the collected data is augmented with Cognitive Intelligence analysis of this suspicious traffic. With Cisco Stealthwatch 6.9.4 or later, the inherent Cognitive Intelligence integration, and ETA found in Cisco IOS XE 16.6.4 or later, Cisco Stealthwatch and the Cognitive Intelligence portal may supplant log review as the first activity performed during daily operations and routine analysis of traffic among the PCI infrastructure.

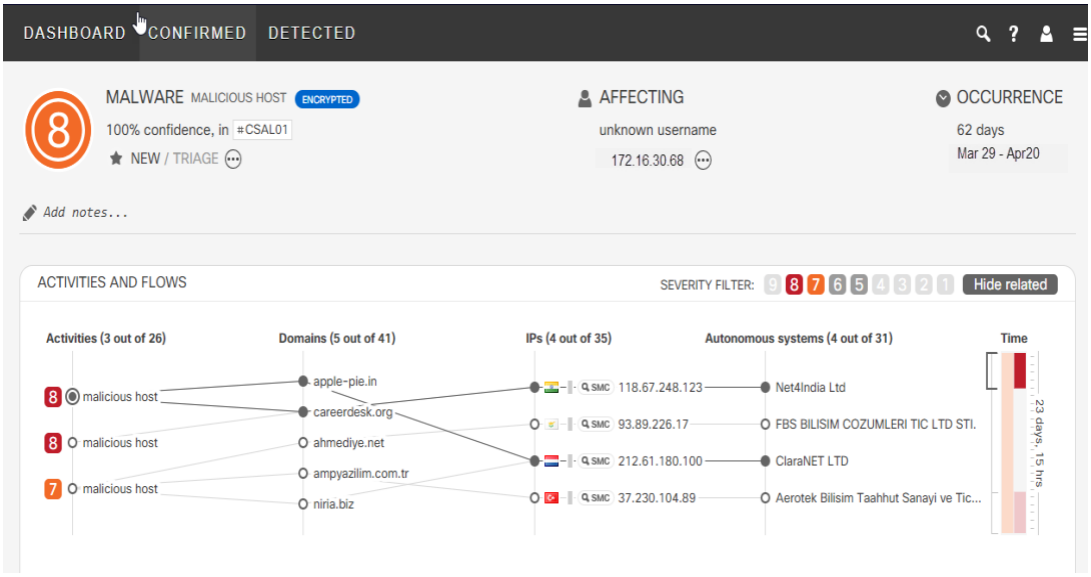


Figure 15 Malware in encrypted retail traffic

General Design Considerations

Wired Deployments

This design guide addresses ETA and the corresponding Flexible NetFlow (FNF) deployment considerations in both networks implementing Cisco SD-Access fabrics and traditional, non-fabric, networks. Prior to the introduction of ETA, many organizations had enabled NetFlow on their switches and routers. Deployment scenarios, and where Flexible NetFlow (FNF) had been enabled, vary from customer to customer and are dependent on the specific reasons for collecting the data, such as performance statistics, security events, monitoring for suspicious traffic, etc. When deploying ETA, it will be necessary to review any existing NetFlow monitoring strategies already in place to determine if changes are required.

Previously, in many campus networks, monitoring has typically performed 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. Now, with the introduction of ETA and network device support for it in hardware and software, optimal inspection occurs at the edge and as close to the endpoint as possible.

ETA is an access layer technology. Monitoring in distribution and core switches such as the 9500 and 9600 is not supported due to the amount of data flowing through these devices, and the computational requirements placed on the processor. If inspection is not possible in the access layer, the recommendation would be to implement the Cisco Stealthwatch v7.1 flow sensor utilizing either SPAN or electrical/optical TAPs (test access port).

Information regarding design and deployment considerations for the Cisco Stealthwatch v7.1 flow sensor, is beyond the scope of this design guide.

This design guide also addresses deployment considerations for ETA and FNF in Cisco SD-Access fabrics. Unlike uplinks in traditional networks, SD-Access fabrics are encapsulated with a VXLAN header. With the VXLAN encapsulation present, only information regarding the VXLAN header is available and not the original source header of the endpoint. Within SD-Access fabrics, there are strict guidelines discussed in the “Design” section that must be followed when deploying ETA and FNF.

Wireless Deployments

Relative to wireless networking, this design guide only addresses fabric enabled wireless in Cisco SD-Access fabrics and does not cover local mode or centralized (over the top/OTT) wireless deployments utilizing CAPWAP for both control and data plane traffic. The Cisco 5520, Cisco 8540, and Catalyst 9800 wireless controllers can all be used to implement fabric enabled wireless.

With fabric enabled wireless, ETA and FNF monitoring is configured on the fabric wireless VLAN on the Catalyst 9300 or 9400 switch regardless of the wireless controller used. When deploying fabric enabled wireless in an SD-Access network, a VXLAN tunnel is established between the access point and the Catalyst 9300 or 9400 access switch. Due to this VXLAN encapsulation, ETA and FNF monitoring are performed on the wireless VLAN rather than the access port itself.

With over the top wireless deployments used in traditional networks or in Cisco SD-Access fabrics, CAPWAP tunnels are established between the access point and the wireless controller and encapsulate the source IP header of the wireless endpoints. As with VXLAN encapsulation, only the CAPWAP header is collected by NetFlow and hence ETA and FNF monitoring of the wireless endpoint is not possible.

In over the top wireless deployments, Flexible NetFlow can be configured on the wireless controller itself, switches to which the controller is attached, or the Cisco Stealthwatch Flow Sensor v7.1 using SPAN or network taps. Although all wireless controllers support NetFlow, only the Cisco Catalyst 9800 series wireless controllers support ETA natively when deployed in local mode (OTT).

Although the Cisco Catalyst 9800 has supported ETA whether deployed as OTT or in the fabric since its introduction, only fabric enabled wireless used in a Cisco SD-Access fabric is discussed in this document.

When deploying the Cisco 5520 and 8500 series wireless controllers in local mode the Cisco Stealthwatch Enterprise v7.1 flow sensor supporting ETA can be used to generate ETA flow records when a SPAN or TAP is implemented on the switch to which those controller are attached.

Information regarding design and deployment considerations for the Cisco Stealthwatch v7.1 flow sensor, is beyond the scope of this design guide.

Summary of wired and wireless deployment models

The following table provides a brief summary of the technologies addressed within this design guide for deploying Encrypted Traffic Analytics and Flexible NetFlow.

Technology	Cisco SD-Access Fabrics	Traditional, Non-Fabric network
Wired	Fabric edge node wired endpoints	Campus access layer (wired only)
Wireless	Fabric enabled wireless (local mode/OTT not supported)	Cisco Stealthwatch v7.1 flow sensor (Catalyst 9800 not validated)
Routing	Cisco router as border node	Internet Edge or Cisco WAN (GETVPN, DMVPN, IWAN, AWS Cloud)

Table 1 Summary of design guidance for Cisco SD-Access fabrics and traditional networks

Cisco Stealthwatch host groups for crypto audit and malware detection

As discussed earlier, all traffic monitored by ETA is forwarded to the Cisco Stealthwatch flow collectors. Here the IDPs are analyzed and available for cryptographic assessment or Crypto Audit at the Cisco Stealthwatch Management Console regardless if the destination is internal or external, beyond the network perimeter; i.e. Internet. For malware detection, by default, only traffic that is destined externally will be analyzed and metadata sent to Cognitive for inspection.

Identification of what traffic is internal versus external is based on IP address and defined using **HOST GROUPS** defined at the SMC. By default, the only host group populated with IP addresses is the **INSIDE HOSTS – CATCH ALL** as seen below.

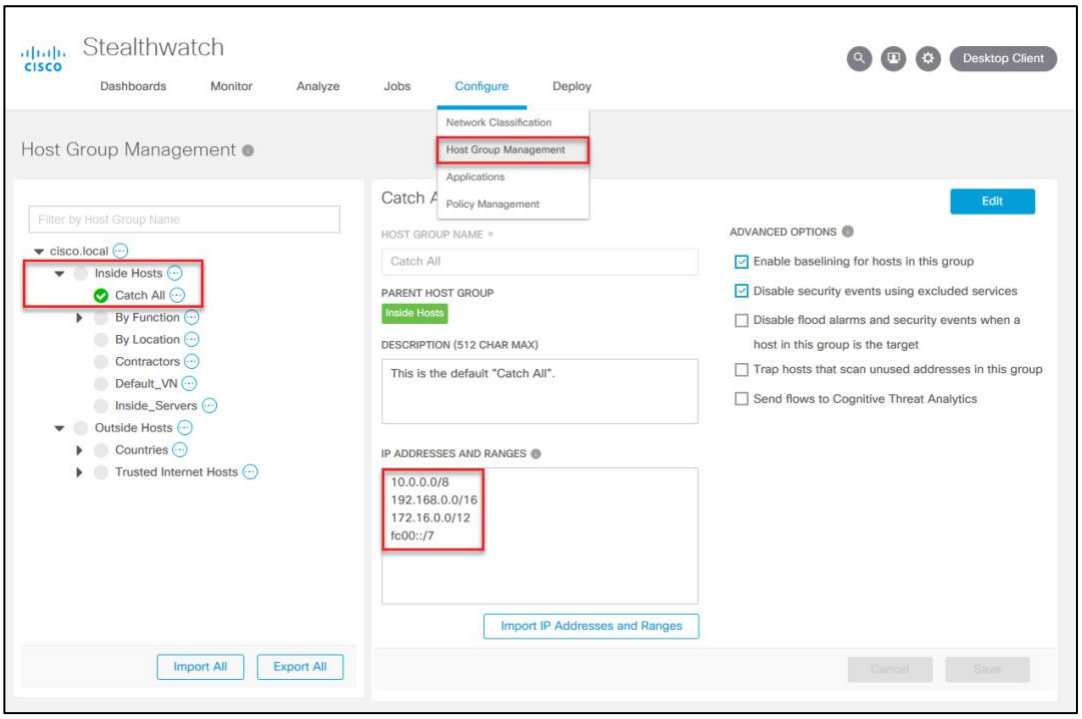


Figure 16 Inside Hosts - Catch All host group definition

In the CATCH ALL host group you can see that the RFC 1918 addresses are defined by default. As a result, any public IPv4 or IPv6 address falling outside of what is defined here will be considered to be outside of the network perimeter, and ETA and FNF metadata collected for traffic from those devices, both HTTP and HTTPS, is sent to the Cognitive Intelligence cloud for malware analysis. This CATCH ALL host group can be modified as in the case where you want to define your public addresses as internal traffic and not subject to further inspection other than crypto audit and typical Cisco Stealthwatch inspection and analysis.

Additionally, it is possible to define internal, private addresses in a custom host group you define and identify as traffic to be sent to the Cognitive cloud by selecting the SEND FLOWS TO COGNITIVE THREAT ANALYTICS check box as seen below. Note that this capability is only available in Cisco Stealthwatch v7.0 and later. If using an earlier version of Cisco Stealthwatch supporting ETA such as 6.9 or 6.10, you will need to customize the CATCH ALL host group.

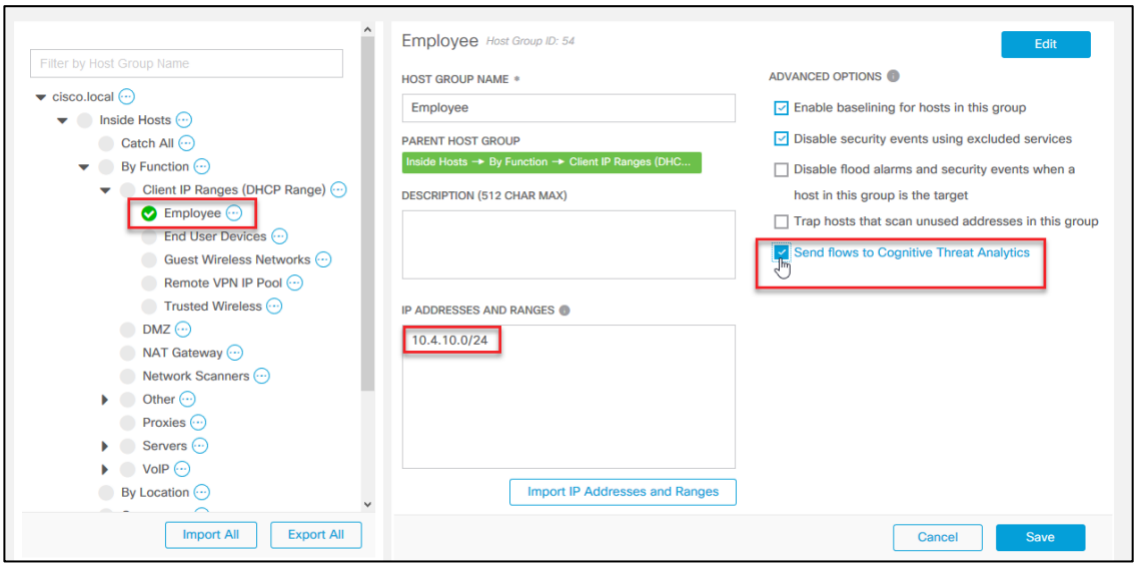


Figure 17 Host group definition configured to send flows to Cognitive

Specific design considerations for traditional Cisco networks

Requirements

This section provides you with the necessary guidance to assist you in deciding where to deploy both ETA and FNF in your traditional, non-fabric, campus and routed WAN infrastructures. This Cisco design guide has been updated to include IOS-XE 16.9.2 and Cisco Stealthwatch 6.10 or 7.0, as the minimum recommended releases of software when implementing ETA and Flexible NetFlow in your environment. For those customers requiring the Cisco Stealthwatch Flow Sensor supporting ETA record generation, Cisco Stealthwatch Enterprise version 7.1 will be required.

Coverage of the Cisco Stealthwatch Flow Sensor v7.1 is beyond the scope of this design guide. The use of the flow sensor will be discussed in the “Deployment Considerations” section however as it serves as an alternative solution for ETA data collection when Catalyst 9000 series switches aren’t present or the platform is unable to scale to the required ETA flows per second; i.e. campus distribution or core, WAN aggregation, or Internet Edge.

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 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 Cisco 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 Cisco 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.

In branch ETA deployments special consideration must also be given as to whether East/West monitoring within the branch is important, requiring Catalyst 9000 series switches. and the tradeoff of WAN bandwidth required to support a branch deployment model or whether monitoring should occur at the WAN aggregation routers along with attention to the scaling requirements required for a centralized deployment model.

This design guide explores six different scenarios in the “Deployment Considerations” section for ETA and NetFlow data collection on routers. The first five use cases focus on routers deployed at the Internet edge as well as for branch WAN scenarios, while the sixth highlights the use of ETA and FNF on a Cisco CSR 1000v installed in an AWS hybrid cloud environment.

Encrypted Traffic Analytics is currently not supported in Cisco SD-WAN deployments.

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.

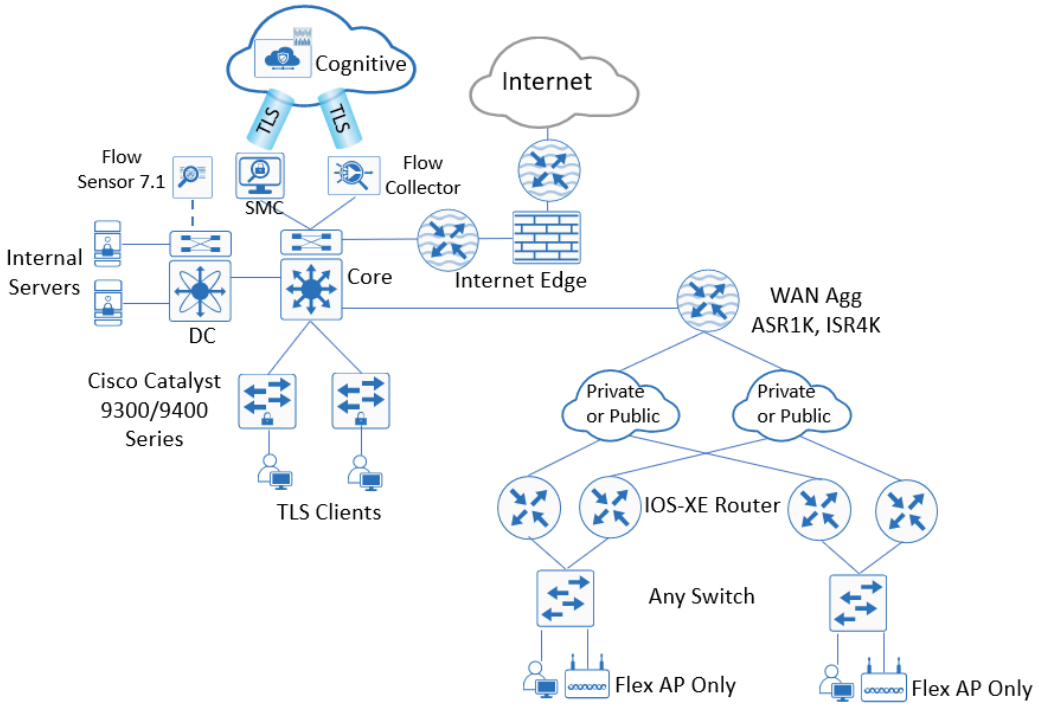


Figure 18 Traditional network logical topology

Deployment Considerations

Enabling ETA and FNF in traditional campus networks

When deploying ETA in a traditional switched network, the ideal location for monitoring is as close to the endpoint as possible on Catalyst 9300 and 9400 access switches. As the Catalyst 9500 and 9600 switches do not support ETA yet, ETA configuration on core or distribution switches is not possible. Although it is possible that a Catalyst 9300 or 9400 may be used as a distribution switch in a smaller network, the issue really becomes one of scale as the Catalyst 9300 and 9400 switches by default support a maximum of 2000 flows per second which may be easily exceeded depending on the number of endpoints connected to the access switches attached to the 9300 or 9400 serving as a distribution switch.

In IOS XE releases prior to 16.12.1, the CLI to configure ETA is present in the Catalyst 9500 and 9600. In IOS XE 16.12.1, this CLI was removed. ETA configuration on the Catalyst 9500 and 9600 is not supported today.

In those cases where monitoring must be performed at the distribution layer, the Cisco Stealthwatch 7.1 flow sensor can generate ETA records from traffic redirected to it via a test access port (TAP) or SPAN. Please refer to the Cisco Stealthwatch 7.1 Installation and Configuration Guide for more information.

ETA configuration is supported on any Catalyst 9300 or 9400 Series Layer 2 or Layer 3 physical interface. It is not supported on management, port-channel, switched virtual interface (SVI), or loopback interfaces. Although ETA is not supported on the logical port channel interface, it is supported on the member interfaces.

In 16.12.1, support was added for configuration of Flexible NetFlow on SVIs. This support does not include ETA which must be configured on the VLAN as described below.

When you are configuring ETA and FNF on Catalyst 9300 and 9400 Series switches, configuration of both ETA and FNF on the switch's access ports is recommended. With both ETA and FNF configured on the access ports, flow information for north-south communications out of the switch, as well as for east-west communications between switch ports, switch stack members, or modular line cards is also available. Although east-west communications by default will not be sent to Cognitive for further analysis unless host groups have been customized as described earlier, the benefits derived from Cisco Stealthwatch and its inherent ability to be configured to detect anomalous behavior can still be realized.

When configuring both ETA and FNF on the same interface, issuing the `show flow monitor eta-mon cache` command discussed in the ETA Deployment Guide, you will see that no cached entries are present for ETA. This is expected behavior due to how the ETA and FNF flow monitors are programmed on the interface. Instead use the `show flow monitor [FNF monitor name] cache` command.

Two ETA configuration scenarios should be avoided; configuration of ETA on the VLAN for wired users, and ETA configuration on both the access ports and uplinks from the access switch. By configuration on the VLAN we do not mean the SVI but configuration following the `vlan [id]` configuration command. If configured on the VLAN, two ETA records will be sent for every flow if a L2 uplink or trunk is used effectively reducing the platform scale by 50 percent. Likewise, when configuring on both access and trunk interfaces two records will be sent for every flow as well; one from the access port and one from the trunk.

Configuration of ETA on the VLAN for traditional, non-fabric switching environments although possible is NOT supported.

Although we recommend that FNF be configured on the access ports of the switch, the only real requirement is that FNF be located along the path of the traffic, and the flow information will be stitched by Cisco Stealthwatch. In doing so, however, you will lose the benefit of east-west inspection on the switch itself.

The main point to consider regardless of where Flexible NetFlow is enabled is that we must inspect the traffic bidirectionally; the source to destination flow and the return flow from the destination. In the ETA deployment guides, you will see that for Flexible NetFlow, an input FNF flow monitor and an output FNF flow monitor are applied to the interface. As discussed earlier, when ETA is enabled globally, the flow monitor for ETA is defined automatically and when ETA is enabled on the interface through the `et-analytics enable` command, the associated ETA flow monitor will be automatically enabled bidirectionally.

Prior to IOS XE 16.12.1 ETA and Application Visibility Control (AVC) could not be configured on the same Catalyst 9300 or 9400 switch. With the release of IOS XE 16.12.1, ETA and AVC can coexist on the same switch however not the same interface. In traditional non-fabric networks, the recommended workaround is to configure AVC on the access ports while configuring ETA on the uplink ports.

The following figure depicts a configuration in which north-south and east-west traffic inspection is performed on either internal or external client-to-server traffic with ETA and FNF on the access ports.

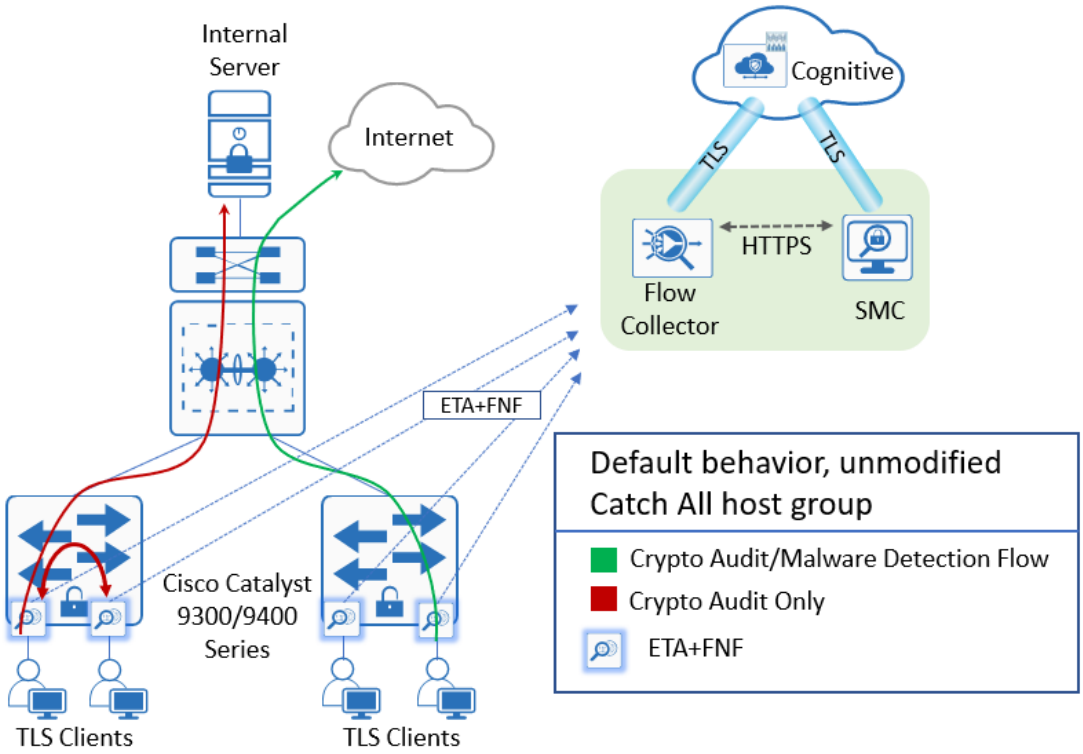


Figure 19 ETA and FNF configured on access ports

In the figure above, ETA and FNF are provisioned on a subset or all access ports as defined when configuring the devices. ETA and FNF records are exported to the Cisco Stealthwatch flow collector. Once they are processed, a crypto audit can be conducted at the SMC against all traffic originating from those ports as depicted by the red lines, while the metadata for DNS queries and traffic destined to the Internet is sent in an encrypted tunnel for analysis in the Cognitive Intelligence cloud for malware as depicted by the green line.

When provisioning the access ports for both ETA and FNF, FNF must always be configured on the interface before ETA. Failure to do so may result in FNF records not being exported. When removing ETA and FNF from an interface, the reverse order must be followed: ETA removed first and then FNF.

When configuring ETA and FNF on a switch interface, there are effectively two NetFlow templates being applied for metadata collection. As a result, when creating the flow record definition for FNF, you are limited to the use of a 5-tuple match definition, as shown in the following example. There are no restrictions as to collect fields that can be configured.

```
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
```

This requirement is necessary as a result of the means by which the ETA and FNF monitors operate when applied to the same interface. In IOS XE 17.1.1, If you add additional match statements to the FNF flow record definition, an error will occur when you attempt to configure ETA. Prior to IOS XE 17.1.1A you will be able to configure both however you will find that ETA records are exported but FNF records are not.

If ETA and FNF are applied to different interfaces, as in the case where ETA is applied to the access port and FNF is applied to the uplink, this 5-tuple limitation does not apply. As discussed earlier, although recommended that ETA and FNF are configured on the same interface, FNF monitors could be configured bidirectionally anywhere along the path between the source endpoint and the destination.

Note that the 5-tuple limitation when configuring ETA and FNF on the same switch interfaces does not apply to the supported routers.

In addition to interface configuration considerations, timer settings are an important part of NetFlow data export. Timers are critical for getting timely information about a flow to the collection and analysis engine. The Flexible NetFlow active timer should be set to 1 minute. This ensures that Cisco Stealthwatch can provide near real-time visibility and analysis on any long-lived flows. There are three timers that are recommended to be customized. The ETA timer is less important as the IDP record is exported immediately and the SPLT records are sent after the first few packets have been received. The following table summarizes both recommended and default timers for ETA and FNF.

Timer	Seconds - Recommended/Default
Cisco Catalyst 9000 ETA inactive timeout	15 /disabled
Cisco Catalyst 9000 FNF cache active timeout	60/1800
Cisco Catalyst 9000 FNF cache inactive timeout	15/15

Table 2 Timers for ETA and FNF on Catalyst 9000 series switches

Enabling ETA and FNF in traditional WAN and Internet edge

With the support for ETA in combination with FNF, encrypted endpoint traffic traversing Cisco routers can now be monitored for both cryptographic compliance and the presence of malware without the need to decrypt that traffic. As with the Cisco Catalyst 9300 and 9400 Series switches, ETA and NetFlow records are exported to Cisco Stealthwatch flow collectors for processing. The IDP information is used to provide detailed information about the cryptographic suite negotiated between the source and destination. For those flows with destinations outside of the enterprise address space or enterprise trust boundary as it is also referred to, the Cisco Stealthwatch flow collector sends the ETA metadata found in the IDP and SPLT, along with the NetFlow records to the Cognitive Intelligence cloud for further analysis for malware.

ETA is supported on integrated Ethernet ports and on all versions of the network interface modules (NIMs) for the 4000 Series ISRs, and on all Ethernet shared port adapter (SPA) and SPA interface processor (SIP) modules for the ASR 1000 Series. The SM-X modules available for the 4000 Series ISRs do not support ETA. In addition to the ISR4K and ASR1K routers, ETA is supported on the Cisco 1100 series routers as well as the CSR and ISRv routers.

ETA is not supported on management interfaces, the VRF-Aware Software Infrastructure interface, and internal interfaces. ETA is not supported on Cisco ISR Generation 2 routers.

As with the Cisco Catalyst 9300 and 9400 Series, although it is possible to configure just ETA, it is necessary to also configure FNF for analysis of encrypted traffic in the Cognitive Intelligence cloud for malware detection, because ETA sends information only about the IDP and SPLT collected and processed by the router. For full NetFlow statistics containing connection and peer information, such as number of bytes, packet rates, round trip times, and so on, you must also configure FNF.

When configuring ETA on the routing platforms, there are no restriction on configuring FNF on the same interface, such as with the 5-tuple flow record as is the case with the Cisco Catalyst 9300 and 9400 Series Switches.

Other unique considerations exist for ETA and FNF monitoring on the same interface for routers. The main consideration in configuring both on the same interface involves whether the interface is configured for IPsec. ETA monitoring occurs prior to encryption, whereas FNF occurs post-encryption, and hence only ESP data is visible. For deployments implementing direct

IPsec connections or Group Encrypted Transport VPN (GET VPN), we recommend that you configure ETA and FNF on the LAN interfaces, while with technologies such as Dynamic Multipoint VPN (DMVPN), either the LAN or the tunnel interfaces can be configured with both. With tunnel interfaces, both Flexible NetFlow and ETA data can be collected without any problem.

FNF monitoring of generic routing encapsulation (GRE) tunnels encrypted with IPsec using the crypto command on the tunnel interface, rather than using tunnel protection command syntax, will be unable to collect unencrypted FNF information. Please refer to the ETA deployment guide for detailed configuration information.

This Cisco Validated Design explores six different deployment scenarios for ETA and NetFlow data collection on routers. The first five use cases focus on routers deployed at the Internet edge as well as for branch WAN scenarios, while the sixth highlights the use of ETA and FNF on a Cisco CSR 1000v installed in an AWS hybrid cloud environment. Special consideration must be given to the location where ETA should be enabled and the requirements for that support. When monitoring traffic at the Internet edge, the routers on which ETA and FNF will be enabled must be capable of supporting the number of new flows per second for all Internet traffic traversing the edge. For branch WAN deployments, the decision as to where to enable ETA will depend on the information desired. Specifically, it depends on whether the purpose is malware detection and cryptographic assessment of Internet-bound traffic only or malware detection and cryptographic assessment of Internet-bound traffic as well as cryptographic assessment of all internal traffic, the latter having a greater impact on the bandwidth required. When considering an AWS deployment using a CSR 1000v with both VPN established to the enterprise network and NAT providing direct Internet access from AWS, monitoring must occur on the CSR's inside interfaces.

When deciding where to configure ETA and FNF, you must first consider the bandwidth required to support ETA and FNF exports. For ETA, each flow requires approximately 10 to 20 kilobits of data, including Layer 2 and 3 headers. For example, 100 new flows per second would require 1 to 2 Mbps depending on the amount of encrypted vs unencrypted traffic. Where this consideration comes into play is in deciding whether ETA should be enabled in the branch, as low-bandwidth sites may not have the necessary free bandwidth and, depending on quality-of-service (QoS) policy, may result in dropped ETA records as well as other scavenger or best-effort traffic being dropped.

In order to conserve bandwidth when deploying ETA on Cisco routers, it is possible to make use of IPFIX format as opposed to NetFlow v9 for exporting FNF ETA data. Although beyond the scope of this document, IPFIX requires less bandwidth than NetFlow v9 as the ETA IDP with IPFIX does not need to be padded to 1500B as is the case with NetFlow v9.

support for IPFIX on Cisco routers was introduced in IOS XE 16.11.1. The Cisco Catalyst switches currently do not support IPFIX. Also note the Cisco SSA service also does not currently support IPFIX when provisioning Cisco routers.

A second consideration in deciding where to configure ETA, is the number of flows per second the routing platform supports for ETA data collection as it does differ from regular Flexible NetFlow. ETA, as is the case with any other feature, consumes additional processor and memory resources in the router to collect the ETA data. When deciding where to configure ETA, you should consult Table 5 below to make sure that you will not exceed the platform's capabilities. If the platform's capabilities are exceeded, the resultant effect, while not adversely impacting overall router performance, will be missing ETA data, resulting in lower malware detection efficacy.

A feature known as "whitelisting" which is supported on the routing platforms, may be used to filter what traffic is subject to ETA data collection, thereby limiting the processing requirements of the platform and providing additional flexibility when configuring ETA. Cisco IOS XE based routers have the unique ability to create ETA "whitelist" Access Control List (ACL) that can be applied to the et-analytics configuration. With a whitelist ACL it is possible to define a subset of traffic that are considered trusted / safe and need not be subjected to ETA inspection, thereby reducing the number of ETA records collected & exported to just Internet-bound traffic, for example. This obviously conserves not only WAN bandwidth, but also lowers the overall number of flows per second that must be processed for ETA.

In addition to bandwidth consumption and platform scalability concerns, the location where ETA is configured may have an impact on the accuracy of the metadata collected. For the IDP, collection can occur on any supported device along the path

of the flow, as traffic characteristics such as jitter have no impact on the collected metadata. For SPLT, however, it is recommended, although not necessary, that you configure ETA as close to the source as possible to eliminate the impact of traffic characteristics such as jitter introduced in the WAN or even the impact of QoS mechanisms such as traffic shaping or policing. Given the tradeoff of the cost in consumed bandwidth as a result of the ETA overhead versus the effect on SPLT data accuracy, and as long as platform scalability is not a concern, configuring ETA at the WAN aggregation might make more sense, especially if jitter is not an issue and buffering due to traffic shaping is not excessive. If, however, cryptographic assessment or auditing of traffic between branches is required for GET VPN WANs, ETA must be configured in the branch. Examples are presented in the use cases later in this guide.

ETA and NetFlow timers

In addition to interface configuration considerations, timer settings are an important part of NetFlow and ETA data export. It is necessary to adjust only the FNF cache active timeout, as the other two settings' default values are fine. The following table summarizes both default timers and adjustable timers for ETA and FNF.

Timer	Seconds - Recommended/Default
Cisco IOS XE-based router ETA NetFlow inactive timer	15 /15
Cisco IOS XE-based router Flexible NetFlow cache active timeout	60/1800
Cisco IOS XE-based router Flexible NetFlow cache inactive timeout	15/15

Table 3 Timers for ETA and FNF on Routers

Branch Design Scenarios and Considerations

This section describes six use cases that illustrate different methods for collecting ETA and NetFlow data for a branch environment and a use case dedicated to configuration of ETA and FNF on a router in the Amazon Web Services cloud. These use cases have all been validated for functionality and stability. When considering any of the deployment models that these use cases depict, it is important to correctly size the Cisco Stealthwatch flow collector(s) to which the ETA and NetFlow records are exported, as well as to understand the scalability of the routers deployed for processing new flows per second.

For configuration information for the six use cases, see the "Encrypted Traffic Analytics in Cisco Non-Fabric Networks Deployment Guide". The only configuration steps that vary from use case to use case are the actual interfaces to which ETA and the FNF monitor commands are applied.

Use case 1: Branch crypto audit & malware detection—Internet edge only

In this deployment scenario, shown below, only endpoint traffic that is destined for the Internet is monitored. ETA and FNF are both configured on the Ethernet interface of a 4K Series ISR or, more likely, an ASR 1000 Series Internet edge router connected to a corporate firewall. Here, all traffic, both encrypted and unencrypted, is monitored, and the ETA and NetFlow data exported to the Cisco Stealthwatch flow collector and perimeter traffic is sent to the Cognitive Intelligence cloud for further analysis.

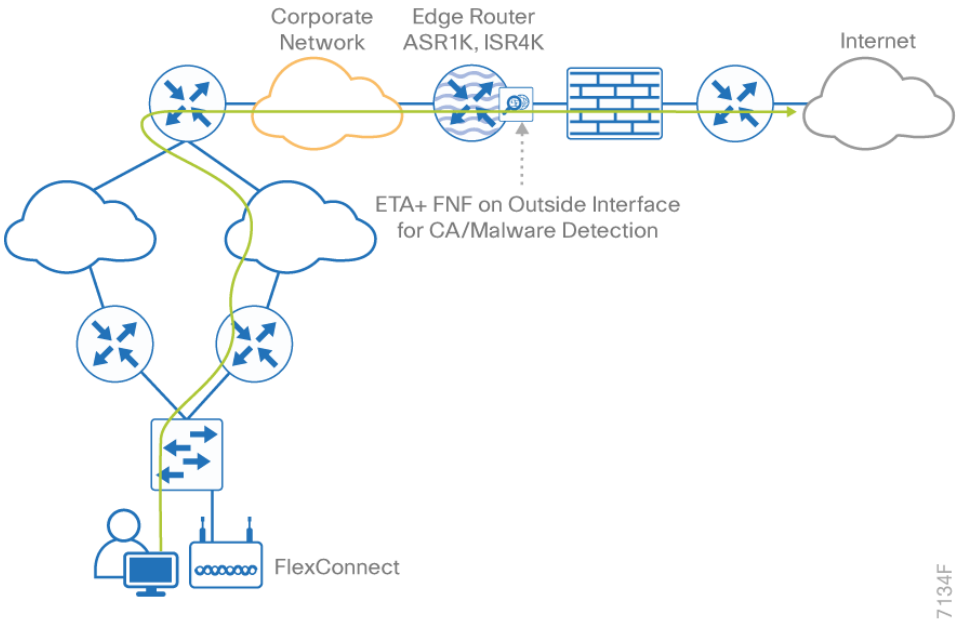


Figure 20 Use Case 1: Branch crypto audit and malware detection at Internet edge

This use case allows for all Internet bound traffic from the branch as well as from the campus and data center to be monitored. A cryptographic assessment for all encrypted traffic leaving the enterprise is possible, as well as analysis for malware in the Cognitive Intelligence cloud. Due to the placement of ETA and FNF, monitoring and cryptographic assessment of internal traffic between enterprise endpoints and servers is not possible, because monitoring is performed only at the edge.

When considering this deployment model, it will be important to correctly size the Cisco Stealthwatch flow collector to which the ETA and NetFlow records will be exported, as well as to ensure that the Internet edge router is correctly sized and capable of processing the required flows per second.

Additionally, ETA and FNF must be configured on an interface prior to the NAT of the source IP en route to the Internet. In the figure for example, it is assumed that the firewall depicted is performing the NAT function.

This deployment scenario obviously conserves branch WAN bandwidth, because no ETA exports are occurring at the branch. It also reduces the possible requirement for more flow collectors, depending on the number of branches, along with the licensing associated with monitoring all branch flows regardless of destination.

PROCESS: Internet edge configuration

Step 1 Configure ETA and FNF on the Internet edge router(s).

Step 2 Configure the ETA et-analytics command and FNF monitor commands on the "outside" LAN interface of the Internet edge router.

Use Case 2: Branch crypto audit & malware detection at WAN aggregation—GETVPN/DMVPN

In this deployment scenario, shown below, branch traffic that is destined for the corporate network or Internet is monitored. ETA and FNF are both configured on the Ethernet LAN interface of an ASR 1000 Series WAN aggregation

router providing connectivity to a campus or corporate network, and so this use case applies to WANs implementing point-to-point IPsec, DMVPN, or GETVPN.

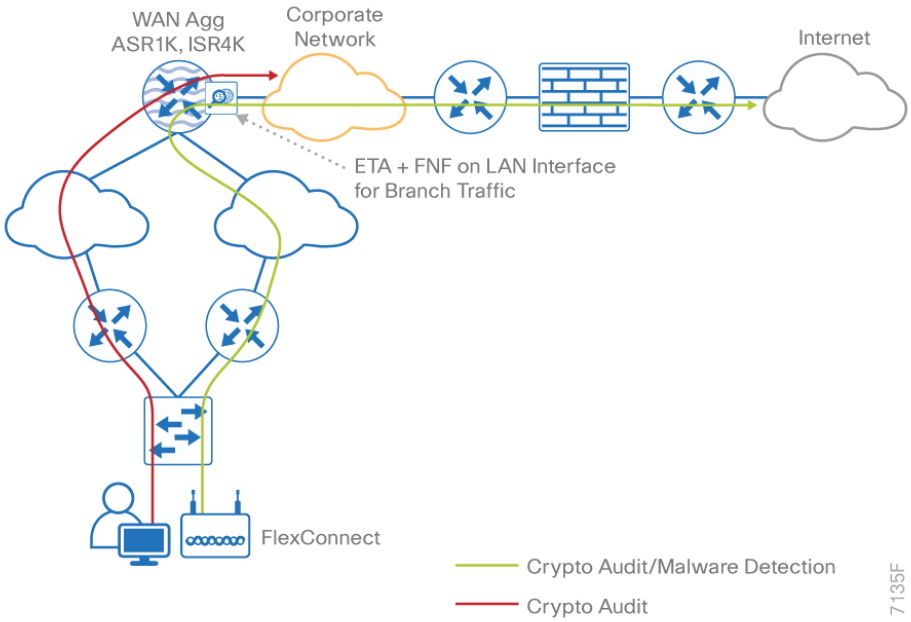


Figure 21 Use Case 2: Branch crypto audit and malware detection at WAN aggregation—GETVPN/DMVPN

This use case allows for the monitoring of all branch traffic destined for the campus, data center, or Internet without monitoring the traffic sourced in the campus and data center. This use case obviously does not support crypto audit on inter-branch communications, because that traffic would never be present on the aggregation router's LAN interface.

A cryptographic assessment of all encrypted branch traffic destined for the Internet is possible, however, as well as analysis for malware in the Cognitive Intelligence cloud. With the placement of the ETA and FNF monitoring at the WAN aggregation router, cryptographic assessment of branch endpoints communicating with campus endpoints and servers is also possible, and this is the major difference with Use Case 1.

When considering this deployment model, it is important to correctly size the Cisco Stealthwatch flow collector to which the ETA and NetFlow records will be exported, as well as to ensure that the WAN aggregation router is correctly sized and capable of processing the required flows per second. The flow collector chosen for this scenario depends on the number of branches, and on whether all traffic, internal or external, is monitored by ETA based on any ETA whitelists configured. It may also be desirable to deploy additional flow collectors if there are several WAN aggregation routers from which ETA and NetFlow records are exported.

In this use case, if crypto audit of internal traffic is not a requirement, it would be possible to configure an ETA whitelist restricting monitoring to traffic destined for the Internet. This reduces the overall number of ETA records exported but does not have any impact on the number of FNF flows being exported. The primary effect of implementing an ETA whitelist is a reduction in the number of flows per second that the flow collector needs to process.

This deployment scenario obviously conserves branch WAN bandwidth, because no ETA or FNF exports are occurring at the branch.

Process – WAN aggregation, LAN interface configuration

Step 1 Configure ETA and FNF on the WAN aggregation router(s).

Step 2 Configure the ETA et-analytics command and FNF monitor commands on the LAN interface of the WAN aggregation router.

Use Case 3: Branch or interbranch crypto audit and malware detection at WAN aggregation—DMVPN Phase 1

In this deployment scenario, shown below, branch traffic that is destined for another branch, the corporate network, or the Internet is monitored. ETA and FNF are both configured on the DMVPN tunnel interface of an ASR 1000 Series WAN aggregation router, providing connectivity to a campus or corporate network, and hence apply to WANs implementing Cisco Intelligent WAN (IWAN) DMVPN (Phase 1).

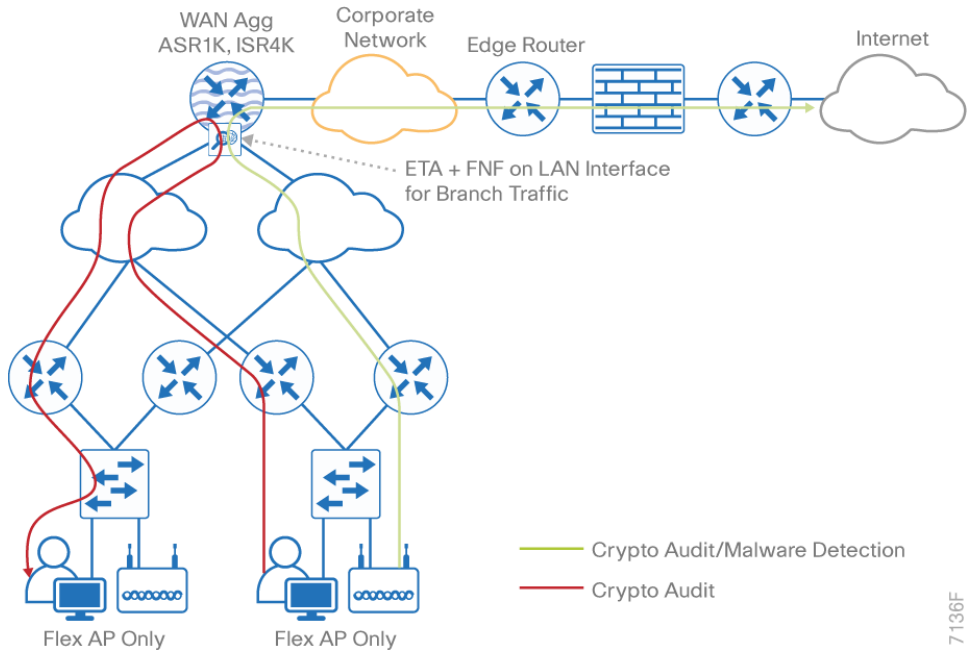


Figure 22 Use case 3: Branch or interbranch crypto audit and malware detection at WAN aggregation—DMVPN Phase 1

ETA and FNF are both able to monitor traffic when applied to the tunnel interface with the tunnel protection used to perform IPsec encryption over the WAN as both monitor traffic before IPsec encryption occurs. If the crypto command is used on the tunnel interface rather than tunnel protection, IPsec encryption occurs before FNF monitoring and all that is visible is ESP data. The crypto command should not be used.

A cryptographic assessment of all TLS-encrypted branch traffic destined for the Internet is possible, as well as analysis for malware in the Cognitive Intelligence cloud. With the placement of the ETA and FNF monitoring at the tunnel interface of the WAN aggregation router, cryptographic assessment of branch endpoints communicating with other endpoints and servers located in other branches, the campus network, or data center is also possible, and this is the major difference with Use Case 2. Crypto audit on inter-branch communications is possible as traffic flowing between branches must communicate (hairpin) through the WAN aggregation router via the tunnel interface.

When considering this deployment model, it is important to correctly size the Cisco Stealthwatch flow collector to which the ETA and NetFlow records are exported, as well as to ensure that the WAN aggregation router is correctly sized and capable of processing the required flows per second. The flow collector chosen for this scenario depends on the number of branches, and on whether all traffic, internal or external, leaving the branch is monitored by ETA if an ETA whitelist is used at the aggregation router. It may also be desirable to deploy additional flow collectors if there are several WAN aggregation routers from which ETA and NetFlow records are exported.

This deployment scenario obviously conserves branch WAN bandwidth, because no ETA or FNF exports are occurring at the branch while still allowing crypto audit of inter-branch traffic.

Process – IWAN aggregation, tunnel interface configuration

Step 1 Configure ETA and FNF on the WAN aggregation router(s).

Step 2 Configure the ETA et-analytics command and FNF monitor commands on the tunnel interface of the WAN aggregation router.

Use case 4: Branch or interbranch with crypto audit and malware detection in the branch—DMVPN Phase 2 or 3 or GETVPN

In this deployment scenario, shown in Figure 23, all ETA and FNF configuration is performed on the branch infrastructure. Branch traffic that is destined for another branch, the corporate network, or the Internet is monitored. ETA and FNF are both configured on the Ethernet LAN interface of a 4000 Series ISR or ASR 1000 Series branch router. If the LAN interface is a member of a port channel on the router, configuration for ETA and FNF must be performed on the port-channel member interfaces, because it is not supported on the port channel itself.

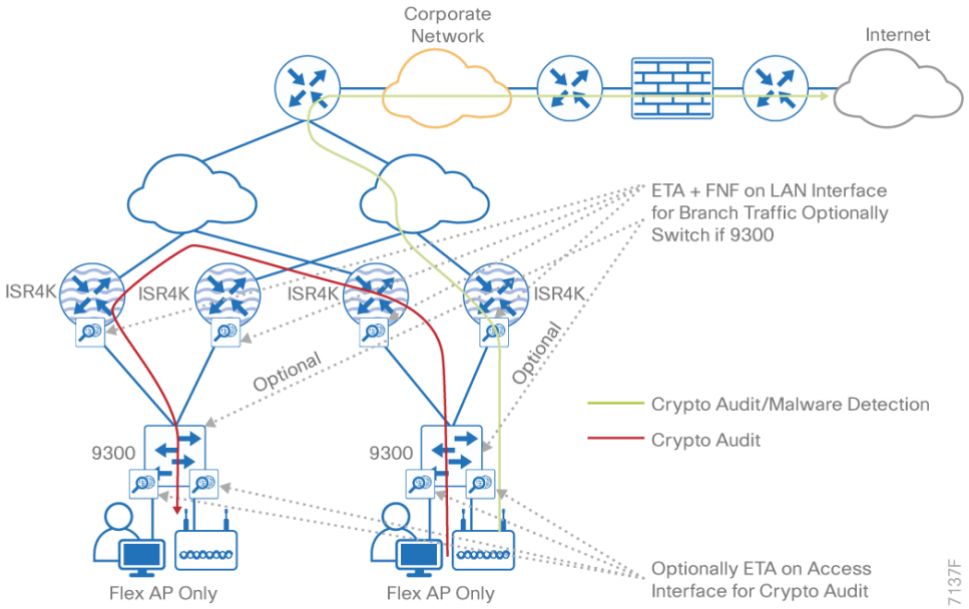


Figure 23 Use case 4: Branch or interbranch with crypto audit and malware detection in the branch—DMVPN Phase 2 or 3 or GETVPN

The purpose of this use case is to support a requirement for crypto audit for inter-branch traffic when the WAN is configured for GETVPN or DMVPN Phase 2 or 3 with support for dynamic tunneling between DMVPN spokes.

When a router is configured for GETVPN, IPsec encryption is configured directly on the WAN interface. The traffic is encrypted before FNF monitoring occurs, and hence only ESP information can be seen. For this reason, the LAN interface is used for ETA and FNF monitoring.

With DMVPN Phase 2 or 3, ETA and FNF must be configured in the branch to support dynamic tunneling between the spokes. Although ETA and FNF monitoring could be configured on the tunnel interface of the branch router as on the WAN aggregation router in Use Case 3, it has been arbitrarily configured on the LAN interface here for consistency with the GETVPN deployment; there is no added benefit in configuring on the LAN rather than the tunnel interface.

A cryptographic assessment of all TLS-encrypted branch traffic destined for the Internet is possible, as well as analysis for malware in the Cognitive Intelligence cloud. With the placement of the ETA and FNF monitoring at the LAN interface of the branch router, cryptographic assessment of branch endpoints communicating with other endpoints and servers located in other branches, the campus network, or data center is also possible.

When considering this deployment model, it is important to correctly size the Cisco Stealthwatch flow collector(s) to which the ETA and NetFlow records are exported. The flow collector chosen for this scenario depends on the number of branches monitored and whether it may be desirable to deploy additional flow collectors for receiving ETA and NetFlow records from groups of routers based on region or branch size.

This deployment scenario obviously consumes additional branch WAN bandwidth due to the overhead introduced by the export of ETA or FNF records. It is, however, the only deployment method capable of supporting GETVPN or dynamic inter-spoke tunneling with DMVPN Phase2 or 3 when crypto audit of the inter-branch traffic is required. This deployment scenario also allows for the greatest scalability as ETA data collection, and the number of flows per second that must be processed is distributed to all the branch routers rather than collected at the WAN aggregation router.

Should Cisco Catalyst 9300 Series or even 9400 Series access switches be deployed in the branch, it would also be entirely possible to configure ETA and FNF on the switch access ports.

Process – Branch deployment

Step 1 Configure ETA and FNF on the branch routers.

Step 2 Configure the ETA et-analytics command and FNF monitor commands on the LAN interface of the branch router.

Step 3 Optionally, if a Cisco Catalyst 9300 or 9400 Series Switch is present in the branch, ETA and FNF

Use case 5: IWAN branch with direct Internet access, crypto audit, and malware detection—DMVPN

In the deployment scenario shown below, branch traffic that is destined for another branch, the corporate network, or the Internet is monitored. Unlike any of the previous branch scenarios, direct internet access (DIA) is configured. This use case is based on the IWAN remote-site design with DIA.

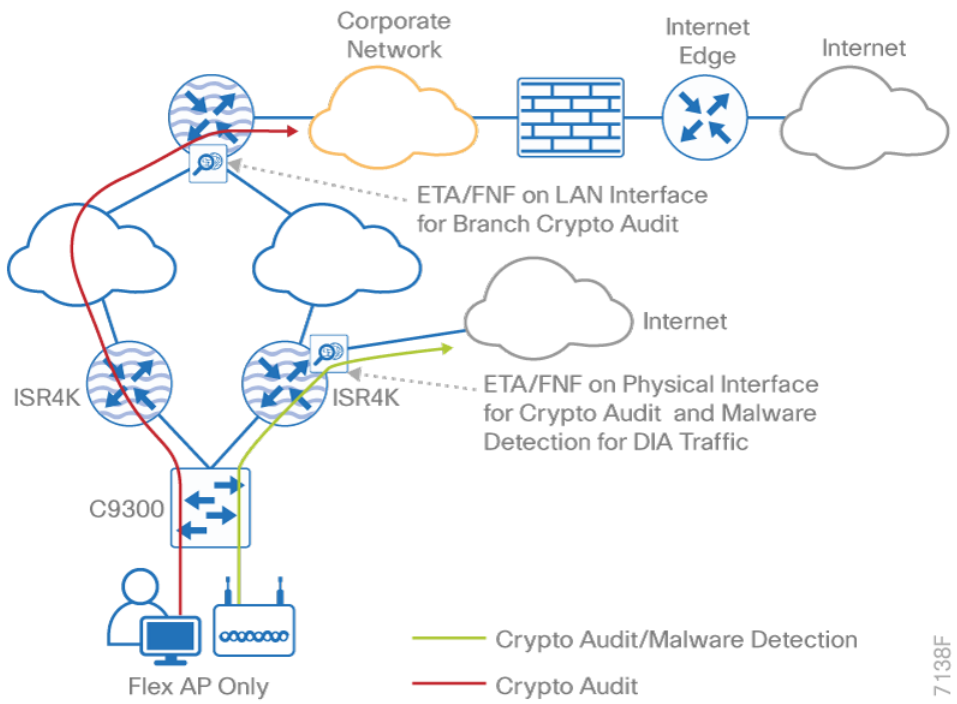


Figure 24 IWAN branch with direct internet access, crypto audit, and malware detection—DMVPN

The IWAN remote-site design provides the remote office with DIA solutions for web browsing and cloud services. This is commonly referred to as the local or direct Internet model, in which traffic accesses Internet services directly without traversing the WAN. With the direct Internet model, user web traffic and hosted cloud services traffic is permitted to use the local Internet link in a split-tunneling manner. In this model, a default route is generated locally, connecting each remote site directly to the Internet provider.

With DIA, ETA and FNF are both configured on the physical interface of a 4000 Series ISR or ASR 1000 Series branch router, providing connectivity to the ISP and the Internet. In the figure above, only one of the two branch routers has DIA configured. Should both routers provide DIA, ETA and FNF would be configured on the second router as well. Cryptographic assessment of all TLS-encrypted branch-traffic destined for the Internet is possible, as well as analysis for malware in the Cognitive Intelligence cloud.

In addition to the branch configuration monitoring Internet traffic, ETA and FNF can be configured on the DMVPN tunnel interface of the WAN aggregation routers. When traffic is being monitored at the tunnel interface of the WAN aggregation router, cryptographic assessment of branch endpoints communicating with other endpoints and servers located in other branches, the campus network, or the data center is also possible.

When considering this deployment model, it is important to correctly size the Cisco Stealthwatch flow collectors to which the ETA and NetFlow records are exported, as well as to ensure that the WAN aggregation router is correctly sized and capable of processing the required flows per second. The flow collectors chosen for this scenario depend on the number of branches and on whether separate flow collectors are used to collect only the branch exports while another is dedicated to monitoring the WAN aggregation routers. Additional flow collectors may also be desired for router assignment based on the geographical location of the branch.

This deployment scenario conserves some branch WAN bandwidth, as only the ETA and FNF exports for traffic destined to the Internet will be sent over the DMVPN tunnels. An ETA whitelist would not be required in the branch, as only Internet traffic will egress the physical interface connected to the ISP.

Process – IWAN with direct Internet access

Step 1 Configure ETA and FNF on the physical WAN interface of the branch routers for crypto audit and malware detection of traffic destined to the Internet.

Step 2 Configure ETA and FNF on the tunnel interface of the WAN aggregation router for crypto audit of inter-branch traffic and traffic destined for the campus or data center.

Use case 6: CSR 1000v located in Amazon Web Services

As companies deploy hybrid clouds for hosting their applications, providing services and applications to branches or remote locations, or even hosting applications for software as a service (SaaS) offerings, visibility into server communications through NetFlow monitoring with ETA provides an invaluable tool for detecting suspicious behavior sourced from or destined to these resources. In Use Case 6, we highlight the use of a CSR 1000v as the router for a virtual private cloud (VPC) within Amazon Web Services (AWS), with ETA and FNF enabled as depicted in Figure 25.

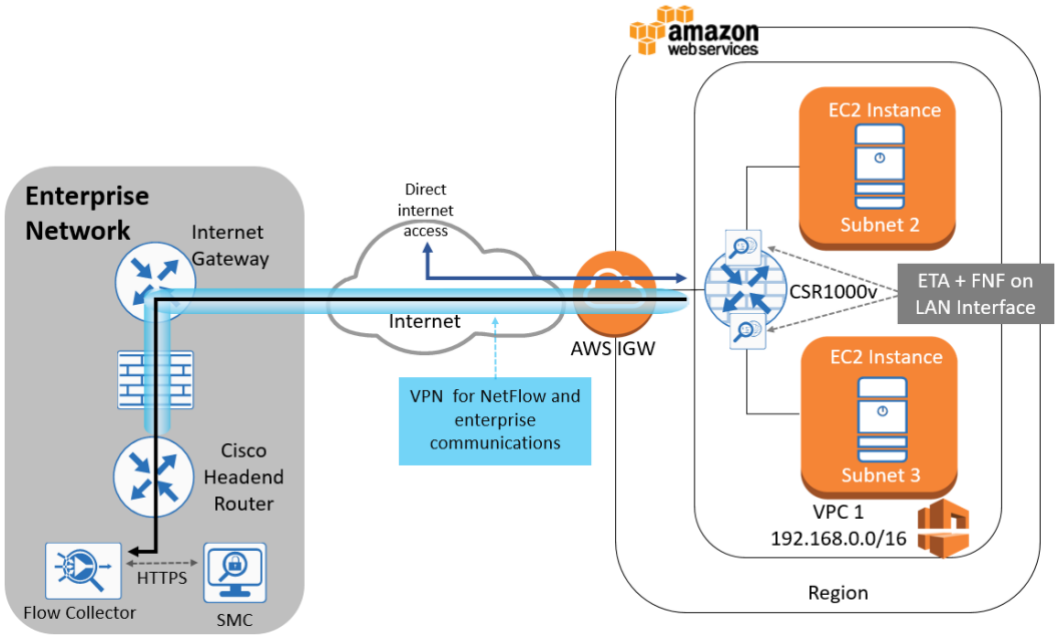


Figure 25 Use case 6: ETA deployed on CSR in AWS cloud

The CSR 1000v is deployed as an AWS Elastic Computing 2 (EC2) instance within a VPC. The CSR 1000v used in this example is the Bring Your Own License (BYOL) version available within the AWS Marketplace. When deploying the CSR 1000v, only one version of Cisco IOS XE is available from the AWS Marketplace; however, once you have established communications with the CSR 1000v, you can install whichever version of Cisco IOS XE you desire; Cisco IOS XE 16.6.4 was validated in this Cisco Validated Design.

For more information regarding the CSR 1000v-BYOL router for AWS, please visit https://aws.amazon.com/marketplace/pp/B00NF48FI2?qid=1529419855048&sr=0-3&ref_=brs_res_product_title

This use case assumes that you have already deployed a CSR 1000v within the AWS cloud. For further information regarding design and deployment guidance for a Cisco CSR 1000v in AWS, please refer to https://www.cisco.com/c/en/us/td/docs/solutions/Hybrid_Cloud/Intercloud/CSR/AWS/CSRAWS.html

The AWS Internet Gateway (IGW) depicted in Figure 25 is a mandatory AWS service and provides Internet access to the VPC. All traffic to and from the VPC will pass through the IGW freely, as access controls within AWS are using security groups which serve as a virtual firewall controlling communications to instances such as the CSR 1000v within the VPC.

Along with the CSR 1000v, there are two EC2 server instances hosting the applications, each in a dedicated subnet or network in the VPC. These servers require Internet access, and so all communications to and from these servers will be monitored by ETA and FNF.

In this example we are using the CSR 1000v to provide all routing within the VPC. The CSR's external interface is on the same subnet as the AWS IGW while two internal interfaces provide connectivity to the subnets in which the servers reside. It is on these two inside interfaces that ETA and FNF have been configured in order to monitor traffic to and from the servers.

In addition to routing, the CSR 1000v in this use case provides site-to-site VPN connectivity with the enterprise network, has a Cisco zone-based firewall (ZBFW) implemented, and provides NAT for server communications to the Internet.

In Figure 25 you can see that an IPsec connection using a virtual tunnel interface (VTI) has been established between the enterprise network and the CSR 1000v. This connection provides not only connectivity between the enterprise network and the servers in the AWS cloud but also connectivity back to the Cisco Stealthwatch flow collector in the enterprise's data center for ETA and FNF record exports.

Access to the servers in the VPC is controlled by the Cisco ZBFW running on the CSR 1000v. Although AWS security groups can be used to control access to the EC2 server instances, the Cisco ZBFW provides stateful inspection of all communications. Additionally, the Cisco ZBFW allows us to implement a policy for communications between servers in the different subnets such as might be required for a tiered application requiring segmentation between the web server and application or database.

NAT is enabled on the CSR 1000v for server communications to the Internet. In our example, we have implemented NAT overload or port address translation for outbound communications only. It would also be possible to implement static NAT services in the case of SaaS for customer access to the hosted applications.

In Figure 25 you can see that ETA and FNF have both been configured on the inside interfaces connecting the subnets where the servers reside. All traffic, whether bound for the enterprise network or the Internet, can be monitored. Placing ETA and FNF on the outside interface or on the VTI used for IPsec is not an option. If placed on the VTI, traffic to the Internet couldn't be monitored, as all traffic traversing the VTI is destined for the enterprise network and if placed on the physical interface, we would see only the NAT translated IP address or port and not the server's actual IP address.

As described, this use case provides monitoring of server communications in a typical hybrid cloud implementation for enterprise access. Although beyond the scope of this Cisco Validated Design, the IPsec VPN using a VTI could be replaced with DMVPN, with the AWS CSR 1000v serving as the spoke connecting to branches or remote sites for access to applications resident in the AWS cloud replacing the need to route traffic back to the enterprise. Regardless of the enterprise connectivity chosen, only the ETA and FNF metadata of the traffic destined to the Internet, or outside of the enterprise "trust boundary," will be forwarded to Cognitive Intelligence for further analysis. Cryptographic assessment, as well as all the inherent benefit derived from Cisco Stealthwatch and FNF, is still possible for all traffic, whether internal or external.

By default, EC2 instances will use Amazon's DNS servers. Access to these servers will not be through the CSR 1000v, even though it serves as the default gateway, but instead through a "reserved" AWS gateway for that AWS network/subnet. As a result, DNS requests will not be monitored, and the records won't be exported. As DNS metadata is used by Cognitive Intelligence in malware detection, the efficacy of malware detection will be greatly reduced. You must change the EC2 instance to make use of a DNS server reachable only through the CSR such that all DNS requests are monitored.

Process – CSR 1000v in AWS

Step 1 Configure ETA and FNF on the LAN (inside) interfaces of the CSR 1000v router for crypto audit and malware detection of traffic destined to the Internet.

Performance

Catalyst 9300 and 9400 switches

The Cisco Catalyst 9300 Series Switches support analysis of up to 2000 new flows per second (fps) for ETA. Flows are still created in the FNF hardware cache, but when exceeding 2000 flows per second, ETA may miss exporting ETA records for some flows, causing incomplete ETA fields in the flow analysis.

Platform	Recommended FPS
Cisco Catalyst 9300	2000
Cisco Catalyst 9400	2000

The Cisco Catalyst 9400 Series Switches by default, support analysis of up to 2000 new flows per second for ETA. At 2000 flows per second for ETA, it is recommended that it be configured only when the 9400 Series is used as an access switch and not in distribution or core of the network. As with the 9300 Series, ETA on the 9400 Series when exceeding 2000 flows per second may miss exporting ETA records for some flows, causing incomplete ETA fields in the flow analysis.

Configuration of ETA on 9300 and 9400 Series VLANs may affect the scale numbers listed here. ETA configuration on the VLAN is therefore not recommended, and ETA should be configured on the access ports to support the number of new flows per second listed above.

The Catalyst 9000 series switches use control plane policing (COPP) to limit ETA processing and the number of packets per second sent for ETA processing. If 2000 flows per second is exceeded at the switch, COPP protects system resources by dropping ETA records. When this occurs, collected ETA data quality suffers and may become unusable for flows where records have been dropped.

Changing the default values established for ETA in COPP is NOT recommended and a Cisco TAC service request should be opened to evaluate the issue as changing these values may have an adverse effect on platform operation and stability.

In order to check the COPP statistics, issue the command:

```
show platform hardware fed active qos queue stats internal cpu policer
```

In the output look for any drops in the High Rate App Queue as seen here:

```
                        CPU Queue Statistics
============================================================================================
                                                (default) (set)       Queue          Queue
QId  PlcIdx  Queue Name                 Enabled    Rate     Rate      Drop(Bytes)    Drop(Frames)
--------------------------------------------------------------------------------------------
23   18      High Rate App                Yes      13000    13000     0              0
```

In addition to the Cisco Catalyst 9300 and 9400 Series specifications, you need to carefully consider the number of Cisco Stealthwatch flow collectors required to support the 9300 and 9400 Series with ETA configured and the flows per second reaching the flow collectors. For the technical specifications for the various models of Cisco Stealthwatch flow collectors, please refer to the Flow Collector Specifications.

Cisco Routers

The following table provides information for the number of ETA flows per second with Flexible NetFlow enabled for the ASR 1000 Series, 4000 Series ISRs, CSR 1000v, ISRv, and Cisco 1100 ISR.

Platform	Recommended FPS*
4451 ISR	40000
4431 ISR	23000
4351 ISR	10500
4331 ISR	6000
4321 ISR	2600
4221 ISR	1700
1100 ISR	7000
ISRv	30000**
CSR 1000v	48000***
ASR 1001-X	33000
ASR 1001-HX	38000
ASR 1002-X	32800
ASR 1002-HX	29000
RP2/ESP40	47400
RP2/ESP100	28400
RP2/ESP200	26200

Table 5 Router ETA and FNF scalability

* HTTP/HTTPS/DNS unidirectional new flows per second

** (UCS-C240-M-4S CPU E5-2643 v4 3.4GHZ) 1 vCPU, 4096 MB Memory 8GB Disk

*** (ENCS5412/K9 CPU D-1557 1.50GHz 12 cores) ISRv-medium (4 CPU, 4GB Memory, 8GB Disk)

Specific design considerations for Cisco SD-Access fabrics

Requirements

In many campus networks before the availability of SD-Access, NetFlow monitoring was typically performed 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 layer.

SD-Access uses fabric technology to significantly change the campus architecture, driving the need to reconsider how FNF is deployed. Fabric technology in the campus enables the use of virtual networks (overlay networks) running on top of a physical network (underlay network) to create alternative topologies to connect devices. The underlay network is defined by the physical switches and routers that are part of the SD-Access network. An overlay network is created on top of the underlay to create a virtualized network. The data plane traffic and control plane signaling are contained within each virtualized network, maintaining isolation among the networks in addition to isolation from the underlay network. The SD-Access fabric implements virtualization by encapsulating user traffic over IP packets that are sourced and terminated at the boundaries of the fabric. The encapsulation technology used is Virtual Extensible LAN (VXLAN).

With the Cisco SD-Access fabric technology in the campus, all IP traffic traversing the fabric is encapsulated with a VXLAN header appended to the frame. With the VXLAN header present, the original IP header of endpoint traffic is no longer visible for FNF inspection and only information about the outer VXLAN header is available and as a result, the means by which the fabric is monitored needs to be changed.

With SD-Access and the use of VXLAN encapsulation, what had previously been considered the distribution layer, and to an extent even the core, is now part of the underlay network and considered to be intermediate nodes in the underlay network. As all traffic traversing the underlay is now encapsulated with a VXLAN header, provisioning the underlay network for FNF, whether at intermediate nodes or uplinks from edge nodes, is not an option, and it will be provisioned at the fabric edge nodes' access ports for wired endpoints or VLANs for wireless endpoints. Additionally, it is possible to monitor communications leaving the fabric at the external border towards the Internet if an ASR1000 or ISR 4000 router is present.

Prior to the introduction of ETA and Cisco Stealthwatch version 6.9.2 with Cognitive Intelligence integration, encrypted traffic analysis was not available with traditional NetFlow. However, now, with ETA enabled on Cisco Catalyst 9300 and 9400 Series Switches and Cisco routers running minimally Cisco IOS-XE 16.6.4, additional data elements such as the IDP and SPLT in encrypted communications are exported in ETA records in addition to Flexible NetFlow records. These ETA data elements provide information about encrypted communications using HTTPS for the purpose of cryptographic assessment or “crypto audit” and malware detection without the need to decrypt the traffic.

Although ETA will produce NetFlow data by itself, FNF must also be provisioned for analysis of encrypted traffic by Cognitive Intelligence for malware detection, because ETA sends only information about the IDP and SPLT collected by the switch. For full NetFlow statistics containing connection and peer information, such as number of bytes, packet rates, round-trip times, and so on, you must also configure FNF.

Logical topology

The following diagram provides a visual representation of a Cisco SD-Access fabric with ETA and FNF provisioned on the edge nodes’ access ports for wired users and at the external border’s non-fabric interface. By configuring ETA at the external border, we now provide ETA support, specifically for malware, to platforms that do not otherwise support it, such as Catalyst 3850s, 3650s and 9200s.

In the drawing, the red line reflects traffic destined to internal resources and upon which a crypto audit can be performed while the green line reflects traffic destined to the Internet which will not only be subject to crypto audit but assessed for malware as well. This relates to the earlier discussion regarding the Cisco Stealthwatch export of metadata to Cognitive for

DNS queries and all HTTP and HTTPS traffic destined to a public IP address, or a pre-defined IP address(es) or prefix you have manually selected for export in Cisco Stealthwatch HOST GROUPS at the Cisco Stealthwatch Management Console.

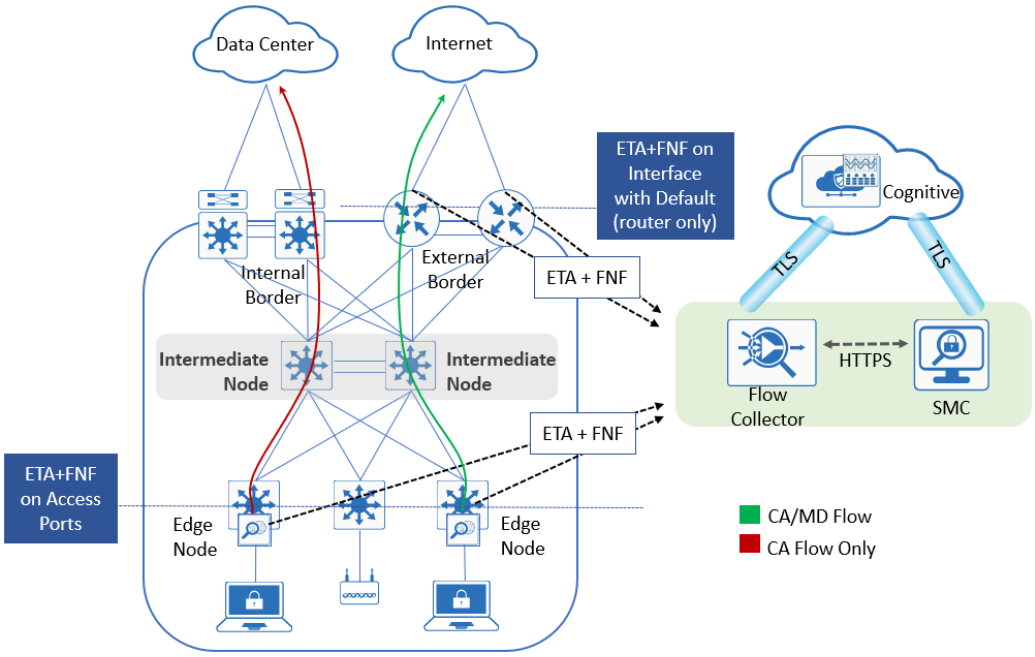


Figure 26 ETA/FNF for monitoring Cisco SD-Access wired traffic

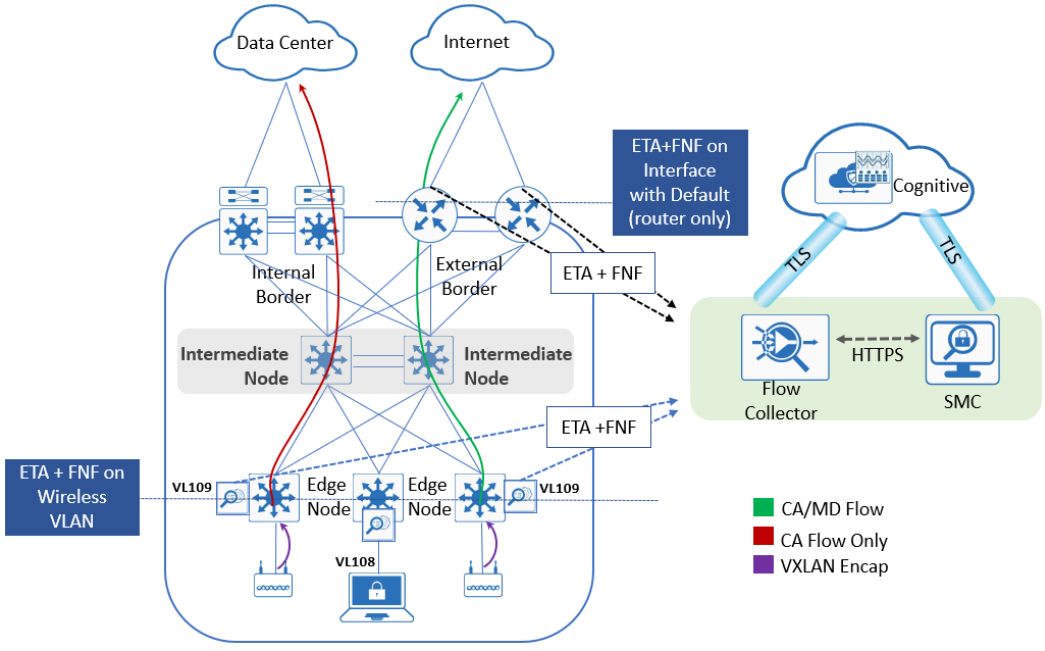


Figure 27 ETA-FNF configuration for monitoring Cisco SD-Access wireless traffic

Considerations

Enabling ETA and FNF in a Cisco SD-Access fabric

Prior to DNA Center 1.3.1, templates were used within Cisco DNA Center to provision, both ETA and FNF on the Cisco Catalyst 9300 and 9400 Series Switches. In this guide, the new Cisco Stealthwatch Security Analytics (SSA) service, available for use within Cisco DNA Center v 1.3.1, is used exclusively for provisioning ETA and FNF. The SSA service can also be used to remove ETA and FNF configuration from a previously provisioned device.

Note that although the Cisco SSA application is the preferred method for provisioning ETA and FNF in Cisco DNA Center1.3.1 and later, it is still possible to use templates as documented in the previous version of this CVD and contained in the appendix of the new ETA for Cisco SD-Access Deployment Guide. However, when using templates, there is no support for provisioning border routers in the Cisco SD-Access fabric. Manual configuration of ETA and FNF via CLI is not supported.

The SSA service is not installed by default in Cisco DNA Center 1.3.1 and must installed manually after upgrade to version 1.3.1 or installation of a new appliance. As part of the installation procedure, it is also necessary to complete the configuration steps to integrate Cisco DNA Center with your Cisco Stealthwatch Enterprise deployment. Even though the SSA service is an optional package, it is linked to a specific version of Cisco DNA Center and hence SSA package upgrades will only be available at the time of release of a new version of DNAC.

The Cisco SSA service, dynamically provisions both ETA and FNF for wired and fabric enabled wireless endpoint monitoring on Catalyst 9300, 9400, 9200, 3850, and 3650 edge nodes. As the Catalyst 9200, 3850, and 3650 switches do not support ETA, only FNF will be configured on these devices. SSA configures both ETA and FNF globally as well as applying the et-analytics configuration and applicable flow monitor (both directions) on the access interface for wired endpoints or VLAN for wireless endpoints.

Although possible to manually configure ETA and FNF on wired VLANs, however not supported by SSA, it is not recommended nor supported by Cisco as the overall scale for ETA processing will effectively be cut in half as ETA records would be processed twice. This caveat applies *only* to wired VLANs.

In addition to the support for Cisco Catalyst switches, the Cisco SSA application includes ETA provisioning support to ASR1000 and ISR 4000 series routers when configured as anywhere, or external borders in a Cisco SD-Access fabric. ETA support for border nodes only applies to routers and does not include the Catalyst 9500 or 9600 when used as a border as ETA is not supported on these platforms.

Relative to IOS XE licensing requirements, the Cisco DNA Advantage license has always been required to enable ETA but Flexible NetFlow, when used by itself, only requires Cisco DNA Essentials. In order to use the SSA service to configure Catalyst switches and routers, a DNA Advantage license must be present on the device. As a result, in order to configure Flexible NetFlow on a Catalyst 3650 or 3850 switch, a DNA Advantage license must be present on the device or else it will be considered not ready.

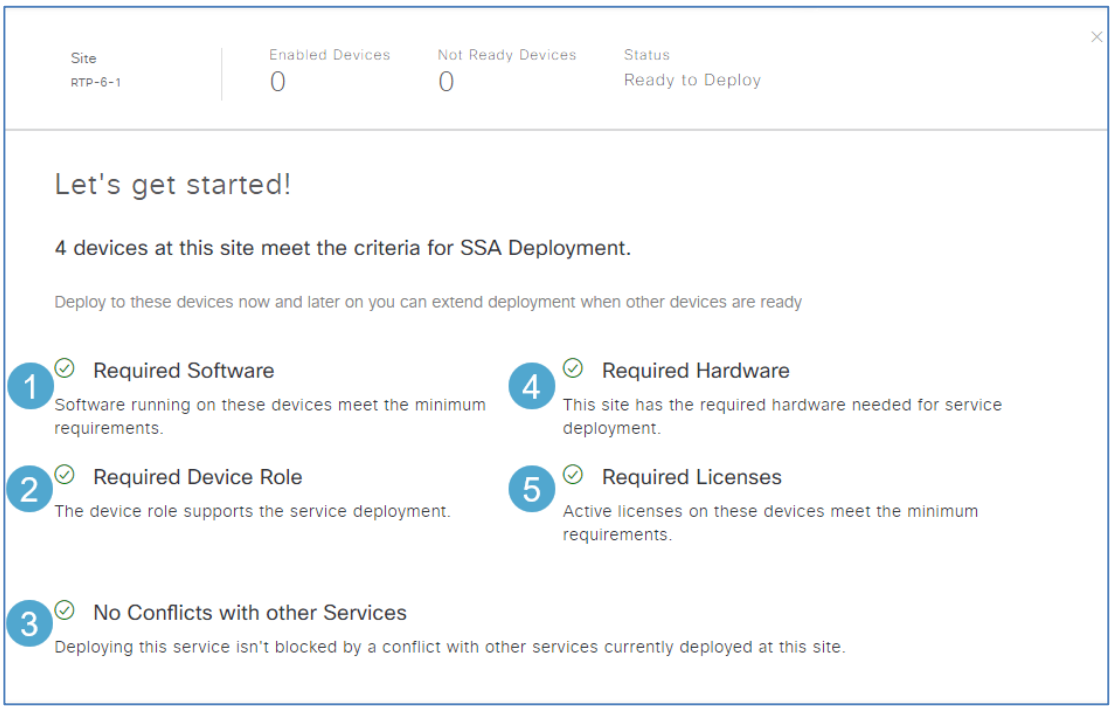
Cisco Stealthwatch Security Analytics service on Cisco DNA Center

The Cisco SSA service was introduced with the release of Cisco DNA Center v1.3.1 to automate the provisioning of ETA and FNF. The SSA service will eliminate the need for the use of templates in provisioning ETA and FNF on network devices that support encrypted traffic analytics, and FNF for Network as a Sensor (NaaS) on those devices lacking ETA support. Although the Cisco SSA service running on Cisco DNA Center is supported in both traditional networks as well as SD-Access fabrics, the discussion in this guide will be limited to Cisco SD-Access. With this release of the Cisco SSA service, provisioning occurs on only Cisco SD-Access edge nodes and at ASR or ISR border routers with a default route.

The SSA service performs the following tasks:

- Assess those devices within the fabric to determine deployment readiness
- Enable Cisco Stealthwatch Security Analytics through provisioning of ETA and FNF
- Monitor deployment status

Upon launching the SSA service and selecting the site to be provisioned, the following screen displays the steps that are completed as part of the readiness assessment.



1. REQUIRED SOFTWARE – A minimum version of IOS-XE must be installed on the device. Please refer to the Appendix for more information.

2. REQUIRED DEVICE ROLE – The device role within the Cisco DNA Center inventory must support the deployment model for provisioning that device; for example, supported switches must have a DEVICE ROLE set to ACCESS whereas a router must have a DEVICE ROLE set to BORDER ROUTER.

3. NO CONFLICTS WITH OTHER SERVICES – A compatibility check is run against other services already configured on the device. The device must not be configured for AVC or other NetFlow configuration.

4. REQUIRED HARDWARE – The device must support either ETA or FNF as deployed for NaaS. Please refer to the Appendix for more information.

5. REQUIRED LICENSE – The device must be licensed for DNA Advantage.

If all the criteria are met, the device will be considered ready for provisioning.

The Cisco SSA service assesses the devices by checking the global inventory to determine those devices ready to be provisioned for ETA and FNF or just FNF alone and then can hierarchically provision devices starting at the ALL SITES or ALL FABRICS level. Whether sites or fabrics are selected, it is possible to drill down hierarchically, the most granular selection being at the floor level. All devices at the selected level of the hierarchy can then be provisioned accordingly. It is not

possible to individually select devices for provisioning. The Cisco SSA service is also used for disabling devices previously provisioned through the same hierarchical process. If a new linecard is added to a modular chassis or new switch to an existing stack, a **RESYNC** of the device in the Cisco DNA Center inventory will result in all applicable ports or VLANs of that new device to be configured appropriately.

The SSA service provisions ETA and FNF on the Cisco Catalyst® 9300 and 9400 series switches, ASR1000/ISR4000 routers, and only FNF on the Cisco Catalyst® 9200, 3850, and 3650 switches. If a device already has an existing NetFlow configuration such as for Cisco Application Visibility Control (AVC), the device will be considered to have a conflicting service and will be listed as **NOT READY**. With this release of Cisco DNA Center and the SSA service, AVC, reliant upon application based NetFlow and NBAR, and ETA are mutually exclusive and only one or the other may be configured on the device.

For Flexible NetFlow support on the Catalyst 3850, 3650, and 9200 switches, only DNA Essentials licensing is required. However, in order to use the Cisco SSA service to automatically provision Flexible NetFlow on these devices, it is necessary to license these platforms with DNA Advantage

SSA provisions the Catalyst® 9300 and 9400 switches with the Flexible NetFlow record, exporter, and monitor along with the et-analytics (ETA) global configurations. The flow monitor and ETA are then applied to the access interfaces for wired users. The fabric interfaces are always excluded from this configuration as well as the Gigabit 0/0 management Interface and any interface that an access point is attached to.

For fabric-enabled wireless, ETA and FNF will also be configured on the wireless VLANs for monitoring of wireless endpoints. The SSA service only supports ETA and FNF provisioning for fabric enabled wireless and not CUWN “over the top” deployments where a CAPWAP tunnel is established between a Cisco access point (AP) and Cisco wireless controller (WLC) running in local mode. Fabric enabled wireless monitoring is accomplished through SSA provisioning both ETA and FNF on the wireless VLAN of the Catalyst 9300/9400 edge node. The VLAN must be used for wireless monitoring due to the VXLAN tunnel extending between the Cisco AP and terminating at the access port the AP is physically connected to. The same holds true for the Catalyst 9200, 3850, and 3650 where although no ETA will be configured, the FNF flow monitors are provisioned on the wireless VLAN.

SSA provisions the Catalyst® 9200, 3850, and 3650 switches with only the Flexible NetFlow record, exporter, and monitor due to lack of ETA support. As with the Catalyst® 9300 and 9400 series switches, the flow monitor is then applied to the access interfaces for wired users and the wireless VLANs for wireless endpoints while the fabric interface as well as any interface where an access point is attached are always excluded from configuration.

In addition to support for Cisco switches, the SSA service will also provision the Cisco ASR1000 and ISR4000 series of routers when configured as an external or anywhere border router. The SSA service will provision the Flexible NetFlow record, exporter, and monitor along with the et-analytics (ETA) global configuration on the router and then apply the flow monitor and ETA on sub-interfaces (for virtual networks) where a default route has been learned or toward a subnet with a public IP not defined as an IP pool in Cisco DNA Center.

Regardless of platform, SSA determines the source interface that will be used for ETA and FNF record exports by looking for the next hop for the flow collector’s IP address specified in Cisco DNA Center. The interface used to source the exports will reside in the underlay and have a route to the flow collector in the global routing table for the underlay. The integrated management interface of a switch or router is never used as the source interface. ETA and FNF record exports will be sent to UDP port 2055 for both ETA and FNF.

SSA service Flexible NetFlow configuration for Catalyst 9000 series and 3X50 series of switches

The following is provided for informational reference only. Manual modification of these configurations, although possible, is not supported.

The FNF record deployed by the SSA service is defined as follows:

```
flow record SSA-FNF-REC

   match ipv4 protocol
```

```
   match ipv4 source address
   match ipv4 destination address
   match transport source-port
   match transport destination-port
   collect timestamp absolute first
   collect timestamp absolute last
   collect counter bytes long
   collect counter packets long
```

Note that when the SSA service configures ETA and FNF on a Catalyst 9000 series switch interface, there are effectively two NetFlow templates being applied for metadata collection. As a result, when creating the flow record definition for FNF, the flow record definition is limited to the use of a 5-tuple match definition, as shown above. Although the Catalyst 3650 and 3850 series switches do not support ETA and only an FNF template will be used on an interface, the same 5-tuple record will still be used as above.

The flow monitor that will be configured for use on the access ports in both the input and output direction by the SSA service is defined as follows:

```
flow monitor SSA-FNF-MON
   exporter SSA-FNF-EXP
   cache timeout active 60
   record SSA-FNF-REC
```

The flow exporter that will be configured is defined as follows:

```
flow exporter SSA-FNF-EXP
   destination [ip address]
   transport udp 2055
   template data timeout 30
   option interface-table
   option application-table timeout 10
```

Applicable interfaces will be configured with:

```
ip flow monitor SSA-FNF-MON input
ip flow monitor SSA-FNF-MON output
```

SSA service Flexible NetFlow configuration for Cisco ASR1000 and ISR4000 border routers

The following is provided for informational reference only. Manual modification of these configurations, although possible, are not be supported.

The FNF record deployed by the SSA service is defined as follows:

```
flow record SSA-FNF-REC
   match ipv4 protocol
   match ipv4 source address
   match ipv4 destination address
   match transport source-port
   match transport destination-port
   match interface input
   match ipv4 tos
   collect timestamp absolute first
   collect timestamp absolute last
   collect counter bytes long
   collect counter packets long
   collect interface output
   collect ipv4 dscp
   collect ipv4 ttl minimum
   collect ipv4 ttl maximum
   collect transport tcp flags
```

Note that the 5-tuple limitation when configuring ETA and FNF on the same switch interfaces does not apply to the supported routers hence additional NetFlow key fields will be defined as seen above.

The flow monitor that will be configured for use on the access ports in both the input and output direction by the SSA service is defined as follows:

```
flow monitor SSA-FNF-MON
   exporter SSA-FNF-EXP
   cache timeout active 60
   record SSA-FNF-REC
```

The flow exporter that will be configured is defined as follows:

```
flow exporter SSA-FNF-EXP
   destination [ip address]
   transport udp 2055
   template data timeout 30
```

Applicable interfaces will be configured with:

```
ip flow monitor SSA-FNF-MON input
ip flow monitor SSA-FNF-MON output
```

SSA service Encrypted Traffic Analytic configuration for Cisco Catalyst 9300 and 9400 switches and Cisco ASR1000 and ISR4000 routers

Globally the following commands will be added:

```
et-analytics
 ip flow-export destination [ip address] 2055
 inactive-timeout 15
```

Applicable interfaces will be configured with:

```
 et-analytics enable
```

Performance

Catalyst 9300 and 9400 switches

The Cisco Catalyst 9300 Series Switches support analysis of up to 2000 new flows per second (fps) for ETA. Flows are still created in the FNF hardware cache, but when exceeding 2000 flows per second, ETA may miss exporting ETA records for some flows, causing incomplete ETA fields in the flow analysis.

Platform	Recommended FPS
Cisco Catalyst 9300	2000
Cisco Catalyst 9400	2000

The Cisco Catalyst 9400 Series Switches by default, support analysis of up to 2000 new flows per second for ETA. At 2000 flows per second for ETA, it is recommended that it be configured only when the 9400 Series is used as an access switch and not in distribution or core of the network. As with the 9300 Series, ETA on the 9400 Series when exceeding 2000 flows per second may miss exporting ETA records for some flows, causing incomplete ETA fields in the flow analysis.

Configuration of ETA on 9300 and 9400 Series VLANs may affect the scale numbers listed here. ETA configuration on the VLAN is therefore not recommended, and ETA should be configured on the access ports to support the number of new flows per second listed above.

The Catalyst 9000 series switches use control plane policing (COPP) to limit ETA processing and the number of packets per second sent for ETA processing. If 2000 flows per second is exceeded at the switch, COPP protects system resources by dropping ETA records. When this occurs, collected ETA data quality suffers and may become unusable for flows where records have been dropped. Although possible to change the default settings used by COPP, it is recommended that a Cisco service request be opened to evaluate the issue as changing these values may have an adverse effect on platform operation and stability.

In order to check the COPP statistics, issue the command:

```
show platform hardware fed active qos queue stats internal cpu policer
```

In the output look for any drops in the High Rate App Queue as seen here:

```
                        CPU Queue Statistics
============================================================================================
                                                 (default) (set)       Queue         Queue
QId PlcIdx  Queue Name                  Enabled    Rate     Rate       Drop(Bytes)   Drop(Frames)
--------------------------------------------------------------------------------------------
23   18     High Rate App                 Yes      13000    13000      0             0
```

In addition to the Cisco Catalyst 9300 and 9400 Series specifications, you need to carefully consider the number of Cisco Stealthwatch flow collectors required to support the 9300 and 9400 Series with ETA configured and the flows per second reaching the flow collectors. For the technical specifications for the various models of Cisco Stealthwatch flow collectors, please refer to the Flow Collector Specifications.

Cisco Routers

The following table provides information for the number of ETA flows per second with Flexible NetFlow enabled for the ASR 1000 Series and the ISR 4000 Series.

Platform	Recommended FPS*
4451 ISR	40000
4431 ISR	23000
4351 ISR	10500
4331 ISR	6000
4321 ISR	2600
4221 ISR	1700
ASR 1001-X	33000
ASR 1001-HX	38000
ASR 1002-X	32800
ASR 1002-HX	29000
RP2/ESP40	47400
RP2/ESP100	28400
RP2/ESP200	26200

Table 5 Router ETA and FNF scalability

* HTTP/HTTPS/DNS unidirectional new flows per second

Appendix A—New in this guide

There have been no significant changes to the design guidance for deploying ETA in a traditional, non-SD-Access fabric. Only a new minimum version of Cisco IOS XE has been specified in this document.

In the previous version of the ETA for Cisco SD-Access Validated Design, templates were used within Cisco DNA Center to provision, both ETA and FNF on the Cisco Catalyst 9300 and 9400 Series Switches. In this guide, the new Cisco Stealthwatch Security Analytics (SSA) service within Cisco DNA Center v 1.3.1 is used.

In the previous CVD, only the Cisco Catalyst® 9300 and 9400 switches were discussed as they were the only switching platforms to support ETA. In this version of the CVD, coverage has been expanded to include the provisioning of Flexible NetFlow in support of Network as a Sensor (NaaS) on the Cisco Catalyst® 3850 and 3650 switches.

Cisco Catalyst® 3850 and 3650 switches do not support ETA.

Appendix B—Hardware and software discussed in design guide

This guide was developed using the following hardware and software.

Cisco 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
Cisco Stealthwatch Flow Sensor v7.1	L-ST-FS-VE-K9	7.1
Cisco DNA Center with Cisco Stealthwatch Security Analytics (SSA) Service	NA	1.3.1

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 Cisco Stealthwatch v6.9.2.

No special software, hardware, or licensing is required other than Cisco 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 3850 Series Switches*	DNA Advantage	16.9.2 or later
Cisco Catalyst 3850 Series Switches*		
Cisco Catalyst 9300 Series Switches		
Cisco Catalyst 9400 Series Switches		

*Catalyst 3650 and 3850 switches have only been included in ETA design guidance for SD-Access.

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		

*Only applicable to ETA for traditional networks and not supported by SSA Service in Cisco DNA Center 1.3.1.

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

Cisco Stealthwatch Management Console User Guide

About this guide

Feedback & discussion

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

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.