# Table of Contents

- **Introduction** .......................................................................................................................... 1
- **Design Overview** ..................................................................................................................... 2
- **Components at a glance** .......................................................................................................... 6
- **Use cases** ................................................................................................................................ 9
  - Crypto audit and malware detection in encrypted traffic .......................................................... 9
  - Deployment considerations ........................................................................................................... 18
    - Enabling ETA and FNF in campus networks ............................................................................. 18
    - Enabling ETA and Flexible NetFlow on routers at the edge and in WAN branch networks ... 21
- **Deployment details** .................................................................................................................. 33
- **Appendix A: ETA data elements** ............................................................................................. 57
- **Appendix B: Product list for ETA** ............................................................................................ 58
  - Stealthwatch .............................................................................................................................. 58
  - Cognitive Intelligence ............................................................................................................... 58
  - LAN access layer ....................................................................................................................... 58
  - Wide Area Network .................................................................................................................. 59
- **Appendix C: Requirements for enabling ETA** ......................................................................... 60
- **Appendix D: References** .......................................................................................................... 61
- **Glossary** .................................................................................................................................. 62
Introduction

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. More specifically, encrypted traffic has increased by more than 90 percent annually, with more than 40 percent of websites encrypting traffic in 2016 versus 21 percent in 2015.

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

Traditional flow monitoring, as implemented in the Cisco® Network as a Sensor (NaaS) solution and through the use of 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 are independent of protocol details, such as the lengths and arrival times of packets within a flow. These data elements have the property of applying equally well to both encrypted and unencrypted flows.

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

ETA extracts two main data elements: the initial data packet and the sequence of packet length and times.

**Reader tip**

Design Overview

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® version 6.9.4 or 6.10.2 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).

Cisco NaaS provides deeper visibility into the network by leveraging Flexible NetFlow on switches, routers and wireless LAN controllers (WLCs). When leveraging Cisco Identity Services Engine (ISE), pxGrid, Cisco TrustSec®, and Cisco Stealthwatch, NaaS can additionally quarantine attacks.

Since the release of Cisco IOS-XE 16.6.2 for Cisco Catalyst 9300 and 9400 Series Switches and the ASR 1000 Series, 1100 and 4000 Series ISRs, ISRv, and CSR 1000v routers, the NaaS solution deployed with Stealthwatch 6.9.2 and integrated with Cognitive Intelligence was extended, through the introduction of ETA, to include the ability to conduct cryptographic assessment or crypto audit as well as malware detection in TLS or SSL encrypted traffic.

This version of the Cisco Validated Design has been updated to include the use of IOS XE 16.6.4 and Stealthwatch 6.9.4 or 6.10.2 as the recommended releases, replacing earlier software releases.

Flexible NetFlow and ETA

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 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.

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

<table>
<thead>
<tr>
<th>Information element</th>
<th>Flow key?</th>
<th>NetFlow v9 length</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceIPv4Address (sourceIPv6Address)</td>
<td>Y</td>
<td>4 (16)</td>
</tr>
<tr>
<td>destinationIPv4Address (destinationIPv6Address)</td>
<td>Y</td>
<td>4 (16)</td>
</tr>
<tr>
<td>sourceTransportPort</td>
<td>Y</td>
<td>2</td>
</tr>
<tr>
<td>destinationTransportPort</td>
<td>Y</td>
<td>2</td>
</tr>
<tr>
<td>protocolIdentifier</td>
<td>Y</td>
<td>1</td>
</tr>
<tr>
<td>flowStartSysUpTime</td>
<td>N</td>
<td>4</td>
</tr>
</tbody>
</table>
Table 2. SPLT template

<table>
<thead>
<tr>
<th>Information element</th>
<th>Flow key?</th>
<th>NetFlow v9 length</th>
</tr>
</thead>
<tbody>
<tr>
<td>sourceIPv4Address (sourceIPv6Address)</td>
<td>Y</td>
<td>4 (16)</td>
</tr>
<tr>
<td>destinationIPv4Address (destinationIPv6Address)</td>
<td>Y</td>
<td>4 (16)</td>
</tr>
<tr>
<td>sourceTransportPort</td>
<td>Y</td>
<td>2</td>
</tr>
<tr>
<td>destinationTransportPort</td>
<td>Y</td>
<td>2</td>
</tr>
<tr>
<td>protocolIdentifier</td>
<td>Y</td>
<td>1</td>
</tr>
<tr>
<td>flowStartSysUpTime</td>
<td>N</td>
<td>4</td>
</tr>
<tr>
<td>flowEndSysUpTime</td>
<td>N</td>
<td>4</td>
</tr>
<tr>
<td>packetDeltaCount</td>
<td>N</td>
<td>8</td>
</tr>
<tr>
<td>octetDeltaCount</td>
<td>N</td>
<td>8</td>
</tr>
<tr>
<td>Sequence of Packet Lengths and Times (SPLT)</td>
<td>N</td>
<td>40</td>
</tr>
</tbody>
</table>

Crypto audit

Crypto audit is the capability of viewing/reporting and eventually alerting and alarming on the crypto fields in the 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 Stealthwatch flow collector. Once collected, these records can be queried by the Stealthwatch Management Console (SMC) for analysis.

These flow records can be collected by a 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.

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 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 Stealthwatch as well as for cryptographic assessment based on ETA data.

**Figure 1. ETA malware detection in Cognitive Intelligence cloud**

ETA and FNF records for TLS-encrypted endpoint traffic destined internally to other endpoints or servers within the organization’s internal address space are not sent to the Cognitive Intelligence cloud for further inspection. However, with the combined ETA and FNF records, cryptographic assessment can still be performed on these flows, whether destined internally or externally to the fabric.

**Tech tip**

The enterprise address space or trust boundary (as identified by internal IP addresses or **Inside Hosts** as defined in Stealthwatch) is administered through the Host Groups settings within the SMC. By default, a Catch All host group is defined and consists of the RFC1918 address space. For more information, see “Deployment,” later in this document.
Design Overview

After integration of Stealthwatch and Cognitive Intelligence, FNF and ETA metadata are immediately sent to the Cognitive Intelligence cloud for analysis. Initially, there will be a brief “training” period in which analysis results may not be displayed at the SMC. This is completely normal and depends entirely on the amount of traffic seen.

Once this initial period is complete, Cognitive Intelligence analyzes the new 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. Rather than decrypting the traffic, Stealthwatch with Cognitive Intelligence uses machine-learning algorithms to pinpoint malicious patterns such as data exfiltration in encrypted traffic to help identify threats and improve incident response times.

**Tech tip**

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.

**Assumptions**

This guide assumes that Stealthwatch components have been installed and configured. You should use this guide along with the Network as a Sensor with Stealthwatch and Stealthwatch Learning Networks for Threat Visibility and Defense Deployment Guide.

Additionally, and beyond the scope of this guide, the NaaS with Stealthwatch guide discusses Stealthwatch integration with ISE, which can be used to profile devices and provide identity based policy and networking services supporting software-defined segmentation through Cisco TrustSec and Cisco Rapid Threat Containment for quarantine of suspicious traffic.

**Reader tip**

For more information about related technologies, see the web pages for Cisco Cyber Threat Defense, Cisco Rapid Threat Containment, and Cisco TrustSec.
Components at a glance

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 2.** NetFlow operation on a network device

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

Cisco Stealthwatch

Cisco Stealthwatch harnesses the power of network telemetry—including NetFlow, IPFIX, proxy logs, and deep packet inspection of raw packets—to provide advanced network visibility, security intelligence, and analytics. This visibility allows a Stealthwatch database record to be maintained for every communication that traverses a network device. This aggregated data can be analyzed to identify hosts with suspicious patterns of activity. Stealthwatch has different alarm categories using many different algorithms that watch behavior and identify suspicious activity. Stealthwatch leverages NetFlow data from network devices throughout all areas of the network—access, distribution, core, data center, and edge—providing a concise view of normal traffic patterns and alerting when policies defining abnormal behavior are matched.

For more information, see the Cisco Stealthwatch web page.

Cisco Cognitive Intelligence

Cisco Cognitive Intelligence finds malicious activity that has bypassed security controls or entered through unmonitored channels (including removable media) and is operating inside an organization’s environment. 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 is capable of supporting up to 9 Tbps of system bandwidth and unmatched power delivery for high-density IEEE 802.3BT (60W Power over Ethernet [PoE])

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

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

For more information, see the Cisco Catalyst 9400 Series 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
introduced into provider-hosted clouds. Similarly, cloud providers themselves can use it to offer enterprise-class networking services to their tenants or customers.

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

Cisco Integrated Services Virtual Router
The Cisco® Integrated Services Virtual Router (ISRv) is a virtual form-factor Cisco IOS XE Software router that delivers comprehensive WAN gateway and network services functions into virtual environments. Using familiar, industry-leading Cisco IOS XE networking capabilities (the same features present on Cisco 4000 Series ISRs and ASR 1000 Series physical routers), the Cisco ISRv enables enterprises to deliver WAN services to their remote locations using the Cisco Enterprise Network Functions Virtualization (Enterprise NFV) solution. Similarly, service providers can use it to offer enterprise-class networking services to their tenants or customers.

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

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

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

For more information see the Cisco 1100 Series web page.

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

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

For more information see the Cisco 4000 Series web page.

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

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

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

Crypto audit and malware detection in encrypted traffic

When the NaaS with ETA solution is implemented, traffic encrypted using TLS or even older libraries such as SSL may now be audited to help 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 in 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 Stealthwatch integration with Cognitive Intelligence. As 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 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, sub-optimal 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

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.
The switch to which these devices are attached, and the router through which the traffic flows, both support Flexible NetFlow; however, all communications are encrypted using HTTPS for transport. The information collected via NetFlow shows that the application is HTTPS and provide 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.
Use cases

Figure 4. Stealthwatch display without ETA healthcare solution

Solution
With Cisco Catalyst 9000 access switches or 1000 and 4000 Series ISR, ASR 1000 Series, ISRv, or CSR 1000v routers running Cisco IOS XE 16.6.4 and Stealthwatch 6.9.4 or 6.10.2, you can enable ETA in addition to flexible NetFlow on switch or router interfaces and passively monitor encrypted flows. During the initial conversation between the medical endpoint and the EHR server, 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 Stealthwatch enhanced with Cognitive Intelligence for any suspicious activity.

Tech tip
The client’s actual public key length is not collected. Stealthwatch displays information about the key reported by the cipher suite.
Now the healthcare organization can audit the encryption used for HTTPS communications between various endpoints and servers while also monitoring that the endpoint or server has not been compromised in order to better ensure the privacy of confidential patient health information. The following figure shows the additional encryption information collected by enabling ETA.
With the integration of Cognitive Intelligence, it is also possible to be alerted to suspicious behavior on the Stealthwatch dashboard and investigate whether or not a device has been compromised within the Cognitive Intelligence portal as seen below.

**Retail PCI use case**

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 8. Auditing encrypted credit card transaction with FNF**

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 9.** Stealthwatch display without ETA retail

![Stealthwatch display without ETA retail](image)

**Solution**

With Cisco Catalyst 9000 access switches or 1000 and 4000 Series ISR, ASR 1000 Series, ISRv, or CSR 1000v routers running IOS XE 16.6.4 and Stealthwatch 6.9.4 or 6.10.2, you can enable ETA in addition to 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.

**Tech tip**

The client’s actual public key length is not collected. Stealthwatch displays information about the key reported by the cipher suite.
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 Stealthwatch and the Cognitive Intelligence cloud.

With 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.
In the event that 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 Stealthwatch 6.9.4 or 6.10.2, the inherent Cognitive Intelligence integration, and ETA found in Cisco IOS XE 16.6.4, 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 11.** Stealthwatch display with ETA

**Figure 12.** Malware in encrypted retail traffic
Deployment considerations

Many organizations have enabled NetFlow on their switches and routers. Deployment scenarios, and the locations in the network where Flexible NetFlow has 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.

In many campus networks, monitoring is 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. Prior to ETA and Stealthwatch version 6.9.2 with Cognitive Intelligence integration, encrypted traffic analysis was not available with traditional NetFlow. Starting with Cisco IOS XE 16.6.2 on the Cisco Catalyst 9300 and 9400 Series Switches, 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. With the introduction of ETA on the 9300 and 9400 Series switches, it is necessary to review the current NetFlow monitoring strategy to incorporate ETA into that strategy.

Flexible NetFlow has likewise been enabled in many WANs for the same reasons. Along with Cisco Catalyst 9300 and 9400 Series Switches and the release of Cisco IOS XE 16.6.2, ETA also became available for the Cisco IOS XE based routers such as the ASR 1000 Series, 4000 Series ISRs, 1100 ISR, ISRv, and CSR 1000v routers, providing the same metadata information as the Cisco Catalyst 9300 and 9400 Series without the need to decrypt the traffic.

This document provides you with the necessary guidance for deciding where to deploy both ETA and FNF in your campus and routed WAN infrastructures and the associated considerations when making those decisions. This Cisco Validated Design has also been updated to include IOS-XE 16.6.4 and Stealthwatch 6.9.4 or 6.10.2 as the recommended releases of software when implementing ETA and Flexible NetFlow in your environment.

Enabling ETA and FNF in campus networks

With Cisco IOS XE 16.6.4, ETA is supported on Cisco Catalyst 9300 and 9400 Series Switches when used as access layer switches in the network. ETA is supported on any 9300 or 9400 Series Layer 2 or Layer 3 physical interface. It is not supported on management, trunk, port-channel, switched virtual interface (SVI), or loopback interfaces. Further, you cannot apply ETA and Cisco Application Visibility and Control features on the same interface.

Although it is possible to simply configure 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 as 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.

When you are configuring ETA and FNF on 9300 and 9400 Series switches running Cisco IOS XE 16.6.4, we recommend that you configure both ETA and FNF on the switch’s access ports, as close to the endpoint as possible. With both ETA and FNF configured on the access ports, flow information for north–south communications as well as for east–west communications between switch ports, switch stack members, or modular line cards is also available. Although east–west communications will not be sent to Cognitive for further analysis, the benefits derived from Stealthwatch and its inherent ability to be configured to detect anomalous behavior can still be realized.

Tech tip

Prior to Cisco IOS XE 16.6.4, configuring both ETA and FNF on the same interface or VLAN was not recommended, as there were unresolved issues. The alternative was to configure ETA on the access port and FNF on the uplinks. This limitation was removed with the release of Cisco ISO XE 16.6.4.
Deployment considerations

**Tech tip**

In Cisco IOS XE 16.6.4, ETA and Cisco Application Visibility and Control (AVC) features cannot be applied on the same interface.

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 Stealthwatch. In doing so, however, you will lose the benefit of east–west inspection.

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 13. ETA and FNF configured on access ports**

North/South Traffic Inspection

![Network diagram showing traffic inspection](image)

**Caution**

In addition to ETA and FNF configuration on the access ports, in Cisco IOS XE 16.6.4 ETA is also now supported on a VLAN through the `vlan configuration [vlan id]` command. We do not recommend the configuration of ETA specifically on the VLAN, however, as this may result in lower processing performance of ETA flow records and may result in flow records being dropped.
Deployment considerations

When provisioning the access ports for both ETA and FNF, FNF must always be provisioned 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.

An additional consideration is that when creating the flow record definition for FNF in the template, you are limited to the use of a 5-tuple match definition, as shown in the following example.

```plaintext
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. If you add additional match statements to the FNF flow record definition, you will find that ETA records are exported but FNF records are not.

In Figure 13, 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 Stealthwatch flow collector. Once they are processed, a crypto audit can be conducted against all traffic originating from those ports, 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.

**Tech tip**

As discussed earlier in the malware detection section, only data for traffic destined to IP addresses outside of the enterprise address space as defined in Stealthwatch will be sent to the Cognitive Intelligence cloud.

**ETA and NetFlow timers**

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 Stealthwatch is able to 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 hard-coded timers and adjustable timers for ETA and FNF.

**Table 3.** Timers for ETA and FNF

<table>
<thead>
<tr>
<th>Timer</th>
<th>Seconds recommended/default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Catalyst 9000 ETA inactive timeout</td>
<td>15/disabled</td>
</tr>
<tr>
<td>Cisco Catalyst 9000 FNF cache active timeout</td>
<td>60/1800</td>
</tr>
<tr>
<td>Cisco Catalyst 9000 FNF cache inactive timeout</td>
<td>15/15</td>
</tr>
</tbody>
</table>
Deployment considerations

ETA and FNF support in Cisco Catalyst 9300 and 9400 Series Switches

The Cisco Catalyst 9300 Series Switches support analysis of up to 2000 new flows per second 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.

The Cisco Catalyst 9400 Series Switches support analysis of up to 3500 new flows per second for ETA. At 3500 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 3500 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.

In addition to the Cisco Catalyst 9300 and 9400 Series specifications, you need to carefully consider the number of 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 Stealthwatch flow collectors, please refer to https://www.cisco.com/c/en/us/support/security/stealthwatch/products-technical-reference-list.html.

Reader tip

For more information about design considerations for the Stealthwatch system, see the Cisco Cyber Threat Defense v2.0 Design Guide and the Cisco Stealthwatch data sheets.

Enabling ETA and Flexible NetFlow on routers at the edge and in WAN branch networks

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 4000 Series ISRs and most models of the ASR 1000 Series, as well as the ISRv, CSR 1000v, and Cisco 1000 Series routers. In this updated version of the Cisco Validated Design, we recommend and have validated the use of IOS XE 16.6.4 with all of the routers listed above.

Reader tip

Prior to Cisco IOS XE 16.6.3 ETA was not supported for ASR 1000 Series routers with the ESP100 or ESP200, as well as the ASR1002-HX (ESP100-based router). Support for these platforms came in Cisco IOS XE 16.6.4.

ETA is supported on integrated Ethernet ports, 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.

ETA is not supported on management interfaces, the VRF-Aware Software Infrastructure interface, and internal interfaces. At present there is also no support for ETA on interfaces configured for virtual routing and forwarding (VRF) or IPv6 traffic. Because Cisco IOS XE is supported only on the platforms listed above, 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
Deployment considerations

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 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.

When configuring ETA on the routing platforms, there is no restriction on configuring FNF on the same interface, as had been the case with the Cisco Catalyst 9300 and 9400 Series Switches prior to IOS-XE 16.6.4, but other considerations exist. 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.

**Tech tip**

FNF monitoring of generic routing encapsulation (GRE) tunnels encrypted with IPsec through the use of the `crypto` command on the tunnel interface, rather than through the use of `tunnel protection` command syntax, will be unable to collect unencrypted FNF information.

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, ETA and NetFlow records are exported to 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 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.

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.

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 absolutely 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.

**Tech tip**

Malware detection through analysis of ETA metadata with Cognitive Intelligence is applicable only to perimeter traffic, the destination IP addresses of which lie outside the enterprise address space as defined by *Inside Hosts* within Stealthwatch, and not to internal, inter-branch traffic.

**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.

**Table 4. Timers for ETA and FNF**

<table>
<thead>
<tr>
<th>Timer</th>
<th>Seconds recommended/default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE-based router ETA NetFlow inactive timer</td>
<td>15/15</td>
</tr>
<tr>
<td>Cisco IOS XE-based router Flexible NetFlow cache active timeout</td>
<td>60/1800</td>
</tr>
<tr>
<td>Cisco IOS XE-based router Flexible NetFlow cache inactive timeout</td>
<td>15/15</td>
</tr>
</tbody>
</table>
## Router ETA and FNF support

The following table provides NetFlow information for the ASR 1000 Series, 4000 Series ISRs, CSR 1000v, ISRv, and Cisco 1100 ISR.

### Table 5. Router ETA and FNF scalability

<table>
<thead>
<tr>
<th>Platform</th>
<th>Recommended flows per second*</th>
</tr>
</thead>
<tbody>
<tr>
<td>4451 ISR</td>
<td>40000</td>
</tr>
<tr>
<td>4431 ISR</td>
<td>23000</td>
</tr>
<tr>
<td>4351 ISR</td>
<td>10500</td>
</tr>
<tr>
<td>4331 ISR</td>
<td>6000</td>
</tr>
<tr>
<td>4321 ISR</td>
<td>2600</td>
</tr>
<tr>
<td>4221 ISR</td>
<td>1700</td>
</tr>
<tr>
<td>1100 ISR</td>
<td>7000</td>
</tr>
<tr>
<td>ISRv</td>
<td>30000**</td>
</tr>
<tr>
<td>CSR 1000v</td>
<td>48000***</td>
</tr>
<tr>
<td>ASR 1001-X</td>
<td>33000</td>
</tr>
<tr>
<td>ASR 1001-HX</td>
<td>38000</td>
</tr>
<tr>
<td>ASR 1002-X</td>
<td>32800</td>
</tr>
<tr>
<td>ASR 1002-HX</td>
<td>29000</td>
</tr>
<tr>
<td>RP2/ESP40</td>
<td>47400</td>
</tr>
<tr>
<td>RP2/ESP100</td>
<td>28400</td>
</tr>
<tr>
<td>RP2/ESP200</td>
<td>26200</td>
</tr>
</tbody>
</table>

* 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)
Branch use cases

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 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.

Reader tip

For configuration information for the six use cases, see “Deployment Details,” later in this 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 in Figure 14, 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 Stealthwatch flow collector and perimeter traffic is sent to the Cognitive Intelligence cloud for further analysis.

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 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 Figure 14 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.
**Figure 14.** Use Case 1: Branch crypto audit and malware detection at Internet edge

Internet edge configuration

**Process**

**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 in Figure 15, 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.

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 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 a number of 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...
Deployment considerations

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.

**Figure 15.** Use Case 2: Branch crypto audit and malware detection at WAN aggregation—GETVPN/DMVPN

![Diagram](image)

**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.

**Reader tip**

For additional configuration information, see the Design Zone for Branch, WAN, and Internet Edge (DMVPN) or Security in the WAN (GETVPN/IPsec) sites.

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

In this deployment scenario, shown in Figure 16, 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).

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 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 a number of 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.

**Figure 16.** Use case 3: Branch or interbranch crypto audit and malware detection at WAN aggregation—DMVPN Phase 1

**Process**

**I Wan 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.

**Reader tip**

For additional configuration information, see the [Branch Iwan Cisco Validated Design](#).
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 17, 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.

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 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 Phase 2 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 of 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.
**Deployment considerations**

**Figure 17.** Use case 4: Branch or interbranch with crypto audit and malware detection in the branch—DMVPN Phase 2 or 3 or GETVPN

**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 could be configured on the access ports of the switch rather than the router.

**Reader tip**

For additional configuration information, see the Design Zone for Branch WAN, and Internet Edge (DMVPN) or Security in the WAN (GETVPN/IPsec) sites.

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

In the deployment scenario shown in Figure 18, 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.

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 Figure 18 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 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.

**Figure 18.** IWAN branch with direct internet access, crypto audit, and malware detection—DMVPN

**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.

**Reader tip**

For more information, see the [IWAN Direct Internet Access Design Guide](#).
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 19.

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.

Reader tip

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

Reader tip

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 cisco.com/c/en/us/td/docs/solutions/Hybrid_Cloud/Intercloud/CSR/AWS/CSRAWS.html

The AWS Internet Gateway (IGW) depicted in Figure 19 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 through the use of 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 19 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 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
Deployment considerations

It is possible to implement static NAT services in the case of SaaS for customer access to the hosted applications. In Figure 19 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 of the inherent benefit derived from Stealthwatch and FNF, is still possible for all traffic, whether internal or external.

**Tech tip**

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.

![Figure 19. Use case 6: ETA deployed on CSR in AWS cloud](image)

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

**Integrating Cognitive Intelligence with Stealthwatch**

These procedures assume that either direct communication or communication via a proxy is permitted from the Stealthwatch Management Console and flow collectors to the Cognitive Intelligence cloud. These communications are all via port 443, and their addresses are:
cognitive.cisco.com—108.171.128.81
etr.cloudsec.sco.cisco.com—108.171.128.86

**Procedure 1** Configure Stealthwatch Management Console for Cognitive Intelligence integration

**Step 1:** Log in to Stealthwatch Management Console.

**Step 2:** Click Administer Appliance
Step 3: Scroll down to Docker Services and click **Configure** next to the Cognitive Intelligence Dashboard service.

![Docker Services](image)

Step 4: Select the **Dashboard Component** check box.

Step 5: Optionally, click the **Automatic Updates** check box to enable Cognitive Intelligence to send updates automatically from the cloud.

The automatic updates mostly cover security fixes and small enhancements for the Cognitive Intelligence cloud. Once enabled, this feature must also be enabled on all flow collectors, as well. If not selected, these updates are delivered through the normal Stealthwatch release process.

Step 6: Click **Apply**.

![Procedure 2](image)

**Configure the flow collector**

Step 1: Log in to the flow collector.

Step 2: Scroll down to Docker Services and click **Configure** next to the Cognitive Intelligence Data Uploader service.
Step 3: Click the Log Upload check box. Sending data from your flow collector to the Cognitive Intelligence engine is enabled.

Step 4: Optionally, select the Automatic Updates check box to enable Cognitive Intelligence to send updates automatically from the cloud.

Step 5: Click Apply.

Step 6: Repeat this procedure to configure the Cognitive Intelligence Data Uploader on each flow collector in your deployment to get accurate results.

Procedure 3 Verify integration between Stealthwatch and the Cognitive Intelligence cloud

Step 1: Check that Docker Services on the Stealthwatch Management Console and the flow collector(s) have a status of Enabled.

Step 2: Check that the Cognitive Threat Analytics component has appeared on the Security Insight Dashboard and Host Report.
Step 3: From the navigation menu, click **Dashboards > Cognitive Threat Analytics**. The Cognitive Intelligence Dashboard page opens.

Step 4: Click the menu symbol in the upper-right corner of the page, and then click **Device Accounts** from the drop-down menu.

Step 5: Check that accounts for each flow are collector configured and that they are uploading data.

**Tech tip**

If the Cognitive Intelligence widget does not display at the SMC, you will want to verify that both the flow collector and Stealthwatch Management Console have Network Time Protocol (NTP) configured correctly. If the flow collector or SMC time is offset from Cognitive Intelligence by more than a minute, the Cognitive Intelligence widget will not display.
Procedure 4  Define the Inside Hosts address range in Stealthwatch

As discussed previously, only traffic that is destined to IP addresses outside of the enterprise address space or trust boundary, as well as all DNS requests regardless of domain, is sent to the Cognitive Intelligence cloud. The enterprise address space is configurable from within SMC using the Desktop Client.

Step 1:  At the SMC dashboard, click Desktop Client.


Step 3: The Host Group Editor window now opens. Expand the Inside Hosts and click Catch All. By default, the RFC 1918 addresses are defined in the Catch All category. These ranges can be modified and additional Host Groups added, as shown below, to provide additional flexibility in reporting, traffic management, and policy management based on role, location, or address space. For more information, see the Stealthwatch documentation.

![Host Group Editor](image)

Configuring the Cisco Catalyst 9300 or 9400 Series

**Procedure 1**  
Enable ETA on the switch globally and define the flow export destination

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

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

**Tech tip**

When configuring ETA globally on the switch, the command-line interface (CLI) permits the configuration of what is known as an ETA whitelist. Essentially this whitelist allows the creation of an access-list defining what traffic should be considered for ETA export. This whitelist is fully supported on the Cisco IOS XE routing platforms; however, it is not supported on the Cisco Catalyst switches and will result in the following error message: `whitelist acl is not supported on Switch followed by %PARSE_RC-4-PRC_NON_COMPLIANCE: ‘whitelist acl et-a whitelist’`
**Procedure 2** Configure Flexible NetFlow

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

**Step 1:** Configure the flow record.

```
AD5-9300# configure terminal
AD5-9300(config)# flow record FNF-rec
AD5-9300(config-flow-record)# match ipv4 protocol
AD5-9300(config-flow-record)# match ipv4 source address
AD5-9300(config-flow-record)# match ipv4 destination address
AD5-9300(config-flow-record)# match transport source-port
AD5-9300(config-flow-record)# match transport destination-port
AD5-9300(config-flow-record)# collect counter bytes long
AD5-9300(config-flow-record)# collect counter packets long
AD5-9300(config-flow-record)# collect timestamp absolute first
AD5-9300(config-flow-record)# collect timestamp absolute last
AD5-9300(config-flow-exporter)# exit
```

**Step 2:** Configure the flow exporter.

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

**Step 3:** Configure the flow monitor.

```
AD5-9300# configure terminal
AD5-9300(config)# flow monitor FNF-mon
AD5-9300(config-flow-monitor)# exporter FNF-exp
AD5-9300(config-flow-monitor)# cache timeout active 60
AD5-9300(config-flow-monitor)# record FNF-rec
AD5-9300(config-flow-monitor)# exit
```
**Step 4:** Apply the monitor to the interface or range of interfaces.

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

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

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

**Procedure 4**  
Verify the ETA configuration

**Step 1:** Verify that the ETA monitor "eta-mon" is a predefined name. Make sure the monitor is active.

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

**Step 2:** Verify the ETA monitor cache.

```
AD5-9300#show flow monitor eta-mon cache
  Cache type: Normal (Platform cache)
  Cache size: 10000
  Current entries: 7
  Flows added: 52139
    - Active timeout ( 1800 secs) 8155
  Flows aged: 52132
```
-Inactive timeout (15 secs)  43977

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

Step 3: Verify ETA flow exports.

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

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

Step 4: Check to see which interfaces et-analytics has been enabled on.

AD5-9300#show platform software et-analytics interfaces
ET-Analytics interfaces
   GigabitEthernet1/0/1
   GigabitEthernet1/0/2
   GigabitEthernet1/0/3
   GigabitEthernet1/0/19
   GigabitEthernet1/0/20
Configuring Cisco IOS XE based routers

**Procedure 1**   Enable ETA on the router globally and define the flow export destination

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

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

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

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

Verify that “feature state” is “initialized.”

**ET-Analytics run-time information:**

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

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

**Procedure 2  Configure optional whitelist**

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

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

**Step 2:** Under the global et-analytics command, apply the access list to an et-analytics whitelist

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

**Procedure 3  Enable ETA on a router interface**

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

```
RS11-4331#configure terminal
RS11-4331(config)#interface Tunnel10
RS11-4331(config-if)#et-analytics enable
RS11-4331(config-if)#end
```

**Procedure 4  Configure Flexible NetFlow on the router**

**Step 1:** Configure the FNF record.

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

Step 2: Configure the FNF exporter.
RS11-4331#configure terminal
RS11-4331(config)#flow exporter fnf-exp
RS11-4331(config-flow-exporter)# destination 10.4.48.70
RS11-4331(config-flow-exporter)# source Loopback0
RS11-4331(config-flow-exporter)# transport udp 2055
RS11-4331(config-flow-exporter)# template data timeout 30
RS11-4331(config-flow-exporter)# end

Step 3: Configure the FNF monitor for traffic entering the interface.
RS11-4331#configure terminal
RS11-4331(config)#flow monitor fnf-mon
RS11-4331(config-flow-monitor)# exporter fnf-exp
RS11-4331(config-flow-monitor)# cache timeout active 60
RS11-4331(config-flow-monitor)# record fnf-rec
RS11-4331(config-flow-monitor)# end

Step 4: Apply the FNF input and output monitors to the desired interface. Based on the WAN use case, this is either the DMVPN tunnel interface, the LAN interface, or in the case of DIA, the physical interface connected to the ISP.
RS11-4331#configure terminal
RS11-4331(config)#interface tunnel10
RS11-4331(config-if)# ip flow monitor fnf-mon input
Procedure 5  Validating ETA and Flexible NetFlow on the router.

Step 1: Verify that ETA is enabled.

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

whitelist acl eta-whitelist
```

Step 2: Verify the configured timeout.

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

ET-Analytics run-time information:

   Feature state    : initialized (0x00000004)
   Inactive timeout: 15 secs (default 15 secs)
   Flow CFG information :
     instance ID    : 0x0
     feature ID     : 0x0
     feature object ID : 0x0
     chunk ID       : 0x4
```
Step 3: Verify the ETA flow statistics.

RS11-4331# show platform hardware qfp active feature et-analytics data stats flow

ET-Analytics Stats:

Flow statistics:

- feature object allocs : 19257
- feature object frees  : 19235
- flow create requests  : 787668
- flow create matching  : 768411
- flow create successful: 19257
- flow create failed, CFT handle: 0
- flow create failed, getting FO: 0
- flow create failed, malloc FO : 0
- flow create failed, attach FO : 0
- flow create failed, match flow: 0
- flow create failed, set aging : 150
- flow ageout requests   : 19218
- flow ageout failed, freeing FO: 0
- flow ipv4 ageout requests : 0
- flow ipv6 ageout requests : 0
- flow whitelist traffic match : 0

Step 4: Verify the ETA export statistics.

RS11-4331# show platform hardware qfp active feature et-analytics data stats export

ET-Analytics 10.4.48.70:2055 Stats:

Export statistics:

- Total records exported : 88554
- Total packets exported : 45553
- Total bytes exported   : 33287148
- Total dropped records : 0
- Total dropped packets : 0
- Total dropped bytes   : 0
- Total IDP records exported:
  - initiator->responder : 77092
Deployment details

responder->initiator : 11636
Total SPLIT records exported:
  initiator->responder : 77075
  responder->initiator : 11633
Total SALT records exported:
  initiator->responder : 0
  responder->initiator : 0
Total BD records exported:
  initiator->responder : 0
  responder->initiator : 0
Total TLS records exported:
  initiator->responder : 3835
  responder->initiator : 3815

Performing a crypto audit and investigating malware
The following procedures provide examples of performing a crypto audit at the Stealthwatch Management Console as well as investigating potential malware through the Stealthwatch integration to the Cognitive Intelligence portal.

Procedure 1  Perform a crypto audit from the SMC

Step 1:  In your browser, access SMC.

Step 2:  On the Dashboard, navigate to Analyze > Flow Search.

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

When you type information such as the IP address, select the box that appears (with the entered text underlined).
To select a specific application, click the **Select** button. From the pop-up, select the application to filter on (in this case HTTPS has been selected), and then click **Done**.

**Step 4:** With search criteria defined, click **Search**. The search begins.
**Deployment details**

**Step 5:** After the search has completed, the following screen appears, showing HTTPS flows and information derived from the IDP and TLS handshake. Notice that the ETA-specific data elements are not present. To enable the display of that information, click **Manage Columns**.

![Flow Search Results](image)

**Step 6:** A pop-up appears. Scroll down and select the encryption fields to be added to the columns displayed. After selecting all encryption fields, scroll down and click **Set**.

![Flow Search Results](image)
Step 7: Once the settings have been saved, the following screen appears, with all of the encryption fields selected.

![Flow Search Results](image)

Step 8: To produce a summary view of the encryption information from the cipher suite used, click Filter Results.
**Step 9:** A pop-up summarizing key flow attributes appears. As shown, information regarding the TLS library used and the encryption attributes are summarized and the number of relevant flows provided.
Step 10: Click any attribute (such as TLS 1.0 under the Encryption TLS/SSL Version section) to present those flows.

![Screenshot of Cisco Validated Design Deployment details](image)

Step 11: Once finished, you can click Export and the filtered information is exported in CSV format to an Excel spreadsheet.

![Screenshot of Export button](image)

**Procedure 2** Investigate suspicious activity for malware through Cognitive Intelligence

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

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

In looking at the Cognitive Intelligence widget in SMC, a summary of “Affected Users by Risk” can be seen. The blue “Encrypted” bubble next to each IP address below signifies that they had been classified as a result of ETA data elements within the Cognitive Intelligence cloud.
Step 2: Within the Cognitive Intelligence portal, the first view accessed is the Dashboard view. From this view, you are able to quickly view the overall health status of your network. Clicking any of the specific behaviors, such as Malware Distribution, displays a summary of compromised or suspicious endpoints.
**Step 3:** With the summary information displayed, selecting the malware detected provides a description of the malware, as well as a summary of infected devices in your network.
Step 4: From the summary information it is also possible for you to click an endpoint to view a histogram of activity leading up to the current security risk level (8 in this case).

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

For further information regarding navigation of the Cognitive Intelligence user interface, refer to the “Threats Tab” section of the Cisco ScanCenter Administrator Guide.
## Appendix A: ETA data elements

<table>
<thead>
<tr>
<th>Data element name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequence of packet lengths and times (SPLT)</td>
<td>An array of LENGTH values followed by an array of INTERARRIVAL TIME values describing the first N packets of a flow that carries application payload. Each LENGTH is encoded as a 16-bit integer to form a 20-byte array. Immediately following this, each INTERARRIVAL TIME is encoded as a 16-bit integer to form another 20-byte array.</td>
</tr>
<tr>
<td>Initial data packet (IDP)</td>
<td>The content of the first packet of this flow that contains actual payload data, starting at the beginning of the IP header.</td>
</tr>
</tbody>
</table>
Appendix B: Product list for ETA

The following products and software versions have been validated for Stealthwatch in this Cisco Validated Design.

Stealthwatch

<table>
<thead>
<tr>
<th>Functional area</th>
<th>Product</th>
<th>License entitlement</th>
<th>Software version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco flow collector</td>
<td>Cisco Stealthwatch flow collector for NetFlow Virtual Edition</td>
<td>L-ST-FC-VE-K9</td>
<td>6.9.4 patch 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6.10.2 patch 3</td>
</tr>
<tr>
<td>Cisco SMC Server</td>
<td>Cisco Stealthwatch Management Console Virtual Edition</td>
<td>L-ST-SMC-VE-K9</td>
<td>6.9.4 patch 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6.10.2 patch 3</td>
</tr>
</tbody>
</table>

Cognitive Intelligence

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

No special software, hardware, or licensing is required other than Stealthwatch 6.9.4 or 6.10.2, validated within this Cisco Validated Design. 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.

LAN access layer

<table>
<thead>
<tr>
<th>Functional area</th>
<th>Product</th>
<th>Software version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stackable and modular access layer switches</td>
<td>Cisco Catalyst 9300 Series Switches</td>
<td>Cisco IOS XE 16.6.4</td>
</tr>
<tr>
<td></td>
<td>Cisco Catalyst 9400 Series Switches</td>
<td>DNA Advantage</td>
</tr>
</tbody>
</table>
## Wide Area Network

<table>
<thead>
<tr>
<th>Functional area</th>
<th>Product</th>
<th>Software version</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WAN branch routers or Cloud</strong></td>
<td>Cisco 4000 ISR Series Routers</td>
<td>Cisco IOSXE 16.6.4</td>
</tr>
<tr>
<td></td>
<td>Cisco Integrated Services Virtual Router (ISRv)</td>
<td>SEC/K9</td>
</tr>
<tr>
<td></td>
<td>Cisco CSR 1000v Cloud Services Router</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco 1000 ISR Series Routers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ASR 1001-X System, Crypto, 6 built-in GE, Dual P/S</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ASR 1002-HX System, Crypto, 8 built-in GE and 8 built-in 10GE ports, Dual P/S</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco CSR 1000v- Amazon Web Services Bring Your Own License</td>
<td></td>
</tr>
<tr>
<td><strong>WAN aggregation routers</strong></td>
<td>Cisco ASR 1004 chassis, dual P/S</td>
<td>Cisco IOSXE 16.6.4</td>
</tr>
<tr>
<td></td>
<td>Cisco ASR 1006 chassis, dual P/S</td>
<td>SEC/K9</td>
</tr>
<tr>
<td></td>
<td>Cisco ASR 1000 Embedded Services Processor, 20 Gb</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ASR 1000 Embedded Services Processor, 40 Gb</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ASR 1000 Embedded Services Processor, 100 Gb</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ASR 1000 Embedded Services Processor, 200 Gb</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco ASR 1000 Route Processor 2</td>
<td></td>
</tr>
</tbody>
</table>
Appendix C: Requirements for enabling ETA

Cisco Catalyst 9000 switching products
To deploy ETA, you can either order a Cisco ONE Advantage subscription (3, 5, or 7 years) with the Cisco Catalyst 9300 Series Switch as detailed below or purchase a la carte.

Steps for ordering the Cisco ONE Advantage subscription:
1. Purchase Cisco Catalyst 9000 switching hardware.
2. Attach the Cisco ONE Advantage subscription, which provides:
   • ISE Plus licensing for 25 endpoints. You can purchase more separately.
   • Stealthwatch, which includes:
     - Licensing for 25 flows per second per switch
     - SMC and flow collector software but does not include any server hardware
   • Cognitive Intelligence license for connection to the Cisco security cloud.
   • ETA-enabled Stealthwatch software, 6.9.4 or 6.10.2, now shipping.
   • Software support.

For more information, see Cisco ONE Subscription for Switching.

Cisco IOS XE routers
Cisco routers require the Security/K9 license to support ETA.
Appendix D: References

Cisco Catalyst 9300 Series Switches web page
Cisco CSR 1000v-BYOL version for AWS
Cisco Cyber Threat Defense Design Guide
Cisco Identify Services Engine web page
Cisco Platform Exchange Grid (pxGrid) web page
Cisco Rapid Threat Containment web page
Cisco Security web page
Cisco ScanCenter Administrator Guide
Cisco Stealthwatch Enterprise web page
Cisco TrustSec web page
Deploying the Cisco Cloud Services Router 1000V Series in Amazon Web Services, Design and Implementation Guide
Encrypted Traffic Analytics Router Configuration Guide
Encrypted Traffic Analytics White Paper
Network as a Sensor with Stealthwatch and Stealthwatch Learning Networks for Threat Visibility and Defense, Deployment Guide
Stealthwatch Management Console User Guide
Glossary

ASR  Aggregation services router
AWS  Amazon Web Services
BYOL  Bring your own license
C&C server  command and control server
CA  certificate authority
CoA  change of authorization
CSR  certificate-signing request
Cognitive Intelligence  Cisco Cognitive Intelligence
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
FNF  Flexible NetFlow
Gbps  gigabits per second
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
AWS IGW  Amazon Web Services internet gateway
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
NaaS  Network as a Sensor
NBAR  Network-Based Application Recognition
NTP  Network Time Protocol
PAN  policy administration 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
SPLIT  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
VLAN  virtual local area network
VPC  virtual private cloud
VPN  virtual private network
VRF  virtual routing and forwarding
WAN  wide area network
WLC  wireless LAN controller
ZBFW  zone-based firewall