Encrypted Traffic Analytics in Software-Defined Access Deployment Guide

July 2018
# Table of Contents

Introduction ........................................................................................................................... 1  
Design overview ..................................................................................................................... 2  
  - Software-Defined Access .................................................................................................. 2  
  - Flexible NetFlow and ETA ............................................................................................... 3  
  - Crypto audit ...................................................................................................................... 4  
  - Malware detection .......................................................................................................... 4  
Components at a glance ........................................................................................................... 7  
Use cases .................................................................................................................................. 10  
  - Crypto Audit and Malware detection in encrypted traffic .................................................. 10  
Deployment considerations ...................................................................................................... 18  
  - Enabling ETA and FNF in campus fabric ....................................................................... 19  
Deployment details ............................................................................................................... 24  
  - Integrating Cognitive Intelligence with Stealthwatch ....................................................... 24  
  - Creating DNA Center templates for provisioning ETA and FNF .................................... 29  
  - Performing a crypto audit and investigating malware ..................................................... 40  
Appendix A: ETA data elements for fabric edge switches ...................................................... 50  
Appendix B: Product list for ETA.......................................................................................... 51  
  - Stealthwatch .................................................................................................................. 51  
  - Cognitive Intelligence ...................................................................................................... 51  
  - SD-Access fabric edge .................................................................................................... 51  
  - Wireless controller and access point ............................................................................. 51  
  - DNA Center .................................................................................................................... 52  
  - Identity Services Engine ............................................................................................... 52  
Appendix C: Requirements for enabling ETA ........................................................................ 53  
Appendix D: References ......................................................................................................... 54  
Appendix E: Template for ETA and FNF removal ................................................................. 55  
Glossary ................................................................................................................................... 56
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 is independent of protocol details, such as the lengths and arrival times of packets within a flow. These data elements have the property of applying equally well to both encrypted and unencrypted flows.

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

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

**Reader tip**

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

This guide describes how to enable NaaS with ETA, providing cryptographic assessment of the cipher suites used for TLS-encrypted communications, as well as the ability to identify malicious traffic patterns in the encrypted traffic of users by using Cisco Software-Defined Access (SD-Access). This Cisco Validated Design discusses the use of Cisco Stealthwatch® version 6.9.4 or 6.10.2 when integrated with Cognitive Intelligence in passively monitoring encrypted wired or wireless endpoint traffic accessing the fabric, either through access ports of Cisco Catalyst® 9300 or 9400 Series edge nodes supporting Flexible NetFlow (FNF) or fabric-enabled wireless access points) connected to the fabric edge nodes.

Tech tip

Cognitive Threat Analytics will soon be renamed Cognitive Intelligence. This name change is reflected throughout this document. This change is not reflected in the actual products yet and you will see that screenshots of both the Stealthwatch Management Console and the Cognitive portal still reflect the older Cognitive Threat Analytics product name.

Cisco NaaS provides deeper visibility into the network by leveraging FNF on switches, access points, and routers. When used with Cisco DNA Center™, Cisco Identity Services Engine (ISE), pxGrid, Cisco TrustSec®, and Cisco Stealthwatch, NaaS can additionally quarantine attacks.

With the release of Cisco IOS® XE Software 16.6.4 for Cisco Catalyst 9300 and 9400 Series fabric edge switches, deployed with Stealthwatch 6.9.4 or 6.10.2 and integrated with Cognitive Intelligence, the NaaS solution is enhanced, through the use of ETA, to include the ability to conduct cryptographic assessment or crypto audit as well as malware detection of TLS- or Secure Sockets Layer (SSL)-encrypted traffic.

This guide focuses specifically on cryptographic assessment and malware detection for fabric-attached endpoints’ communications to Internet-based services. Although crypto audit is possible for all fabric endpoints attached to devices with ETA enabled, only flows destined to the Internet are monitored, with information sent to the Cognitive Intelligence Cloud for further analysis for malware.

Software-Defined Access

The SD-Access architecture is supported by fabric technology for the campus, which enables the use of virtual networks (overlay networks) running on a physical network (underlay network) in order to create alternative topologies to connect devices. Overlay networks are commonly used to provide Layer 2 and Layer 3 logical networks with virtual machine mobility in data center fabrics (examples include Cisco Application Centric Infrastructure [Cisco ACI™], Virtual Extensible LAN [VXLAN], and FabricPath). Overlay networks are also used in WANs to provide secure tunneling from remote sites (examples include Multiprotocol Label Switching [MPLS], Dynamic Multipoint VPN [DMVPN], and generic routing encapsulation [GRE]). This section provides information about the SD-Access architecture elements. SD-Access design recommendations are covered in the Design Considerations section.

This document is intended to be used in conjunction with the SD-Access Design and Deployment Guides found at the following page:

https://www.cisco.com/go/designzone

This Cisco Validated Design was prepared in support of ETA and FNF when implemented in an SD-Access fabric based on DNA Center version 1.1.6 or 1.1.7. Version 1.1.X does not support the workflow automation necessary for provisioning ETA and FNF for wired and wireless scenarios. Instead, DNA Center templates will be used to provision the fabric edge nodes in this guide, as manual configuration of ETA and FNF on the Cisco Catalyst 9300 and 9400 Series Switches is not supported.
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 SPLIT 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 SPLIT templates list those NetFlow key and nonkey fields included in the exported record when ETA is enabled. As can be seen, this is a small subset of the data elements that can be collected via FNF, which is why both 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>
<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>initialDataPacket (v9), or ipHeaderPacketSection (IPFIX)</td>
<td>N</td>
<td>1300</td>
</tr>
</tbody>
</table>

Table 2. SPLIT 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 (SPLIT)</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 clientHello 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 (FC). Once collected, these records are queried by 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 also 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 Time (SPLT) provide a unique and valuable means for 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 enhances 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 collected, and after processing the metadata is sent by the Stealthwatch Flow Collector to the Cognitive Intelligence cloud in an encrypted TLS tunnel for further analysis, as shown in the figure below.
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 addresses or Inside Hosts as defined in Stealthwatch) are administered through the Host Groups settings within the SMC. By default, a Catch All host group is defined and consists of the RFC 1918 address space. For more information, see “Deployment,” later in this document.

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 typically lasts only a few hours.

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 Encrypted Traffic Analytics 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 the SD-Access fabric, along with its associated border nodes, has been deployed. For more information about SD-Access, see the SD-Access Design and Deployment Guides found at the following page:

https://www.cisco.com/go/designzone

This guide also 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.
Components at a glance

Software-Defined Access

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

Figure 2. SD-Access architectural components

NetFlow

NetFlow is a standard that defines data elements exported by network devices that describe the “conversations” on the network. NetFlow is unidirectional, and each device on the network can export different NetFlow data elements. When processed, NetFlow data can tell you the important details in network transactions involving data communication between endpoints, information about when the conversation occurred, how long it lasted, and what protocols were used. It is a Layer 3 (and possibly Layer 2, depending on where it’s enabled or match conditions) network protocol that you can easily enable on wired and wireless devices for visibility into the network flows, as well as enhanced network anomaly and malware detection.
Cisco Stealthwatch
Cisco Stealthwatch harnesses the power of network telemetry—including but not limited to NetFlow, IPFIX, proxy logs, and deep packet inspection of raw packets—to provide advanced network visibility, security intelligence, and analytics. This visibility allows a Stealthwatch database record to be maintained for every communication that traverses a network device. This aggregated data can be analyzed to identify hosts with suspicious patterns of activity. Stealthwatch has different alarm categories using many different algorithms that watch behavior and identify suspicious activity. Stealthwatch leverages NetFlow data from network devices throughout all areas of the network—access, distribution, core, data center, and edge—providing a concise view of normal traffic patterns throughout and alerting when policies defining abnormal behavior are matched.

For more information, see the Cisco Stealthwatch web page.

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

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

Tech tip
Cognitive Threat Analytics will soon be renamed Cognitive Intelligence. This name change is reflected throughout this document. This change is not reflected in the actual products yet and you will see that screenshots of both the Stealthwatch Management Console and the Cognitive portal still reflect the older Cognitive Threat Analytics product name.
Encrypted Traffic Analytics

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

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

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 Cisco Catalyst 9300 Series Switches form the foundational building block for SD-Access, Cisco’s lead enterprise architecture.

At 480 Gbps, the 9300 Series is the industry’s highest-density stacking bandwidth solution with the most flexible uplink architecture. The Cisco Catalyst 9300 Series is the first optimized platform for high-density 802.11ac Wave 2. It 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 Cisco Catalyst 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.
Use cases

Crypto Audit and Malware detection in encrypted traffic

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

Along with the crypto audit capability, traffic bound for the Internet can be further analyzed without the need to decrypt the traffic for possible signs of malware and data exfiltration through 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 Intelligence Cloud services for processing.

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

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

Healthcare use case

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 edge nodes to which these devices are attached support Flexible NetFlow; however, all communications are encrypted using HTTPS for transport. The information collected via NetFlow shows that the application is HTTPS and provides information relative to source and destination addressing as well as other characteristics of the flow, but nothing further. The only means to check that TLS and not SSL is used, and what version of either has been negotiated, is through a packet capture to collect the IDP and subsequent handshake messages at the switch, as well as additional confirmation of the settings at the endpoint itself.
Solution
With Cisco Catalyst 9000 access switches at the fabric edge running Cisco IOS-XE 16.6.4 and Stealthwatch 6.9.4 or 6.10.2, you can enable ETA in addition to FNF on the edge nodes 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.

Figure 6. Addition of ETA in healthcare
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.

**Figure 7.** Stealthwatch display with ETA and FNF

**Figure 8.** Malware in encrypted medical traffic
Retail PCI use case

Merchants conducting credit card transactions are 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 around crypto suites used, the auditor will also 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 9. Auditing encrypted credit card transaction with FNF
The merchant has been upgrading many older POS terminals, which previously supported only TLSv1.0, with its known vulnerabilities, to now support TLS v1.2 in preparation for their annual audit and as a result of the PCI Council’s deprecation of TLS1.0. The merchant is now 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 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 10.** Stealthwatch display without ETA retail

![Stealthwatch display without ETA retail](image)

**Solution**

With Cisco Catalyst 9000 access switches at the fabric edge running Cisco IOS-XE 16.6.4 and Stealthwatch 6.9.4 or 6.10.2, you can enable ETA on switch 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 Cognitive Intelligence.

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 their 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 16.6.4s for the Cisco Catalyst 9300 and 9400 Series Switches, 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 13.** Malware in encrypted retail traffic
Deployment considerations

Many organizations have enabled NetFlow on their switches and routers. Deployment scenarios, and 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 before the availability of SD-Access, monitoring was typically performed at either the distribution layer of the network or at the uplink ports from the access layer switches, providing a distributed and scalable means of monitoring traffic entering or leaving the access layer.

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

With fabric technology in the campus, all IP traffic traversing the fabric is encapsulated with a VXLAN header appended to the frame. In Cisco IOS-XE release 16.6.4, which this Cisco Validated Design is based on, with the VXLAN header present, the original IP header of endpoint traffic is no longer visible for FNF inspection, and as a result only information about the outer VXLAN header is available.

With SD-Access and Cisco IOS-XE 16.6.4, what had previously been considered the distribution layer, and to an extent even the core, is now part of the underlay network and are considered to be intermediate nodes. As all traffic traversing the underlay is now encapsulated with a VXLAN header, provisioning the underlay network for FNF, whether at intermediate nodes or uplinks from edge nodes, is not an option, and it will be provisioned at the fabric edge nodes’ access ports or VLANs.

**Reader tip**

With Cisco IOS-XE 16.8.1, an enhancement known as Fabric Telemetry is introduced, providing information from both the VXLAN outer header and the information from the inner payload header as well. This enhancement is, however, applicable only to Flexible NetFlow, and not to ETA. Even though Cisco IOS-XE 16.8.1 is available now, the recommendations that are presented in this Cisco Validated Design for FNF and ETA provisioning on the access ports for wired endpoints and VLANs for wireless endpoints are unchanged.

Prior to the introduction of ETA and Stealthwatch version 6.9.2 with Cognitive Intelligence integration, encrypted traffic analysis was not available with traditional NetFlow. However, now with ETA enabled on Cisco Catalyst 9300 and 9400 Series Switches running Cisco IOS-XE 16.6.4, additional data elements such as the IDP and SPLT in encrypted communications are exported in ETA records, enabling analysis of these elements for the purpose of performing a crypto audit and/or malware detection. This document provides you with the necessary guidance to provision both ETA and FNF on fabric edge nodes in an SD-Access network.
Enabling ETA and FNF in campus fabric

With Cisco IOS-XE 16.6.4, configuration of both ETA and FNF are supported on the same Cisco Catalyst 9300 and 9400 Series access ports and VLANs when used as fabric edge nodes in an SD-Access network. For wired endpoints, ETA is provisioned by DNA Center on the fabric edge node’s access interfaces, and for wireless endpoints it is provisioned on the edge nodes’ VLAN(s) to which the wireless users belong.

Although it is possible to configure ETA and FNF through the Command-Line Interface (CLI) of the Cisco Catalyst 9300 and 9400 Series Switches, the use of DNA Center for provisioning the switches is the only method supported and is the one we will discuss in this Cisco Validated Design. Using a template within DNA Center, both ETA and FNF are provisioned on the Cisco Catalyst 9300 and 9400 Series Switches. A single template is used for provisioning ETA and FNF on the fabric edge nodes for both wired and wireless endpoints. Although it is possible to provision ETA by itself, FNF must also be provisioned for analysis of encrypted traffic by Cognitive Intelligence for malware detection, because ETA sends only information about the IDP and SPLT collected by the switch. For full NetFlow statistics containing connection and peer information, such as number of bytes, packet rates, round-trip times, and so on, you must also configure FNF.

Provisioning fabric edge nodes using templates in DNA Center

As previously discussed, DNA Center 1.1.X does not have the automated workflows necessary to provision ETA and FNF on fabric devices, and so templates will be used. The use of templates in provisioning these features should be considered a temporary measure until this automation is added in a future release of DNA Center.

Provisioning ETA and FNF in an SD-Access fabric is a three-step process. The first step involves the creation of the wired and wireless template using the Template Editor within DNA Center. Once the templates have been created, we need to create a network profile under the Design Workflow in DNA Center and assign the appropriate sites to the profile. The final step is to provision those devices with this new network profile.

Tech tip

In DNA Center 1.1.X, there is a restriction that only one CLI template per device type per site is allowed. DNA Center 1.2 will introduce a feature known as composite templates that will remove that restriction. The use of composite templates and DNA Center 1.2 has not been validated.

SD-Access for wired users

When you configure ETA for wired users connecting to the fabric, it should be configured at the Cisco Catalyst 9300 or 9400 Series access ports. Although it is possible to configure ETA on the VLANs associated with the wired users, we recommend the use of the access port. Due to VXLAN encapsulation of all traffic leaving the access switch, as discussed earlier, it is not possible to configure ETA anywhere else within the fabric, such as the links connecting the fabric edge nodes to the fabric intermediate nodes.

Tech Tip

The configuration of ETA on the edge node’s fabric uplinks may have an adverse impact on network performance not to mention the unnecessary overhead placed on the switch exporting meaningless data that won’t be usable due to the original header being encapsulated within VXLAN.

For fabric edge nodes supporting ETA, FNF will be provisioned on the same physical interface as ETA, as discussed and seen in Figure 14. When provisioning the access ports for both ETA and FNF, FNF must always
Deployment considerations

be provisioned on the interface before ETA. Failure to do so may result in flexible NetFlow records not being exported. This provisioning order will be followed using the template provided later in the Deployment section.

Tech tip

In Cisco IOS-XE 16.8.1, FNF has been enhanced such that data for both the external VXLAN header as well as the encapsulated, internal header can now be collected. With this feature, FNF can now be configured on the uplinks from the edge nodes. ETA, however, is not supported by this enhancement, and thus we recommend configuring both ETA and FNF on the access ports of the edge node.

An additional consideration you need to be aware of is that when creating the flow record definition for FNF in the template, you are limited to the use of a five-tuple match definition per the following example.

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

This requirement is necessary due to the way in which both 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.

Figure 14. ETA and FNF configuration for monitoring wired user traffic
In Figure 14, ETA and FNF are provisioned on a subset of or on all access ports, as defined when provisioning the devices. ETA and FNF records are exported to the Stealthwatch Flow Collector. Once 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.

**SD-Access for wireless users**

When you configure ETA for wireless users connecting to the SD-Access fabric, you must configure ETA within the VLAN configuration associated with the wireless users at the Cisco Catalyst 9300 or 9400 Series fabric edge. For SD-Access wireless, a VXLAN tunnel is built between the access point and the fabric edge. Because traffic entering the fabric edge port to which the access point is attached is encapsulated, ETA monitoring is not possible on that port. Instead, ETA must be configured within the wireless VLAN configuration, allowing the traffic to be monitored prior to re-encapsulation in a new VXLAN tunnel between the edge node and the destination of the flow.

For SD-Access fabric edge nodes supporting ETA, FNF should be configured on the VLAN along with ETA, as depicted in Figure 15. As with the provisioning of the wired access ports, the same considerations involving the provisioning order of ETA and FNF and the five-tuple flow record definition apply to the VLAN provisioning.

**Figure 15.** ETA and FNF configuration for monitoring wireless user traffic
In Figure 15, ETA and FNF are provisioned on the appropriate VLAN(s) as defined when provisioning the devices. ETA and FNF records are exported to the Stealthwatch Flow Collector. Once 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 are 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 or trust boundary as defined in Stealthwatch will be sent to the Cognitive Intelligence Cloud.

**Fabric border node considerations**

In an earlier version of this Cisco Validated Design, we discussed the need to configure FNF on the border nodes’ external, non-fabric interfaces while configuring ETA separately on the edge nodes. This recommendation was due to issues seen when configuring both ETA and FNF on the same access interface or VLAN in earlier versions of IOS-XE 16.6. With Cisco IOS-XE 16.6.4 and later, these issues have been addressed and the appropriate scale testing completed, making the configuration of ETA and FNF on the edge node’s access interfaces the preferred and, now, the only supported method.

Two additional considerations for revising the previous guidance of FNF configuration at the border node and now recommending FNF provisioning at the edge nodes along with ETA, is the lack of automation for provisioning FNF at the border node as well as potential, albeit slim, FNF scalability concerns depending on the platform chosen as a border. Future DNA Center enhancements will provide automated provisioning of ETA and FNF on the same access interfaces and VLANs as this CVD now advocates thus providing future consistency between this CVD based on DNA Center 1.1.6 or 1.1.7 and templates and automated provisioning with later versions of DNA Center. Also, with configuration of ETA and FNF at the edge nodes, we are able to eliminate any concerns around platform scalability at the border.

An added benefit of access port or VLAN configuration is that we are also now able to monitor flow information for lateral communications within the fabric for Stealthwatch policy violations, all the way down to devices attached to the same edge node, and not just traffic leaving the fabric.

**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 FNF active timer should be set to 1 minute. This ensures that Stealthwatch will be 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 several packets have been received. The following table summarizes both hard-coded timers and adjustable 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>
ETA 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 traffic exceeds 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, it is recommended that ETA be configured only when the Cisco Catalyst 9400 Series is used as an access switch, and not in distribution or the core of the network. As with the Cisco Catalyst 9300 Series, ETA on the 9400 Series when traffic exceeds 3500 flows per second may miss exporting ETA records for some flows, causing incomplete ETA fields in the flow analysis.

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 Cisco Catalyst 9300 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.
Deployment details

This section describes those procedures necessary to enable ETA and FNF on edge nodes within an SD-Access fabric. It consists of the processes for performing Stealthwatch and Global Threat Analytics integration and for enabling ETA and FNF on Cisco Catalyst 9300 and 9400 Series fabric edge switches for wired or wireless users, after which you can use the Stealthwatch and Cognitive Intelligence user interfaces for crypto audit and malware detection.

With DNA Center version 1.1.6 or 1.1.7, automatic provisioning through the DNA Center user interface is not supported. In order to configure ETA and FNF, it is necessary to make use of templates to provision the fabric edge nodes to enable both ETA and FNF.

Integrating Cognitive Intelligence with Stealthwatch

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

cognitive.cisco.com—108.171.128.81
etr.cloudsec.sco.cisco.com—108.171.128.86

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

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

**Step 2:** Click **Administer Appliance**.
Step 3: Scroll down to Docker Services and click **Configure** next to the Cognitive Threat Analytics 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** 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 Threat Analytics Data Uploader service.

![Docker Services](image)

Step 3: Click the **Log Upload** check box. Sending data from your Flow Collector to the Cognitive Intelligence engine is now 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 Cognitive Intelligence Cloud**

**Step 1:** Check that Docker Services on the Stealthwatch Management Console and Flow Collector(s) are set to Enabled.

![Docker Services](image1)

**Step 2:** Check that the Cognitive Threat Analytics component has appeared on the Security Insight Dashboard and Host Report.

![Stealthwatch Dashboard](image2)
**Deployment details**

**Step 3:** From the navigation menu, click **Dashboard > Cognitive Threat Analytics**. The Cognitive Intelligence Dashboard page opens.

![Dashboard > Cognitive Threat Analytics](image)

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

![Device Accounts](image)

**Step 5:** Check that there are accounts for each Flow Collector configured and that they are uploading data.

![Device Accounts](image)

**Tech tip**

If the Cognitive Intelligence widget does not display at the Stealthwatch Management Console, you will want to verify that both the Flow Collector and SMC 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, 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 2: The Stealthwatch desktop client launches. Expand the domain and select **Host Groups**. Now click **Configuration > Edit Host Groups**.

![Image of the Stealthwatch Management Console](image)

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 seen 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**.

![Image of the Host Group Editor for cisco.local](image)
Creating DNA Center templates for provisioning ETA and FNF

This Cisco Validated Design is based on DNA Center 1.1.6 or 1.1.7, which does not have workflow automation for ETA and FNF provisioning at the edge nodes. In future releases of DNA Center, this automation will be available. DNA Center 1.2 will introduce automation support for wired access, while DNA Center 1.3 will introduce support for fabric-enable wireless access.

Until automation is available to provision these features, you will need to use templates to configure ETA and FNF on the switches. This Cisco Validated Design provides one template that has been solution tested and will support provisioning ETA and FNF for both wired and wireless access. Naturally, this template can be modified to suit your particular needs, but it is suitable for most deployments as is.

**Tech tip**

You can assign only one template per device type per site within DNA Center 1.1.X. If one already exists, the commands necessary for ETA and FNF provisioning may be added to the existing template. This limitation will be removed in future DNA Center releases by a feature known as Composite Templates, which will allow more than one template to be assigned per device type.

**Procedure 1** Create templates for wired and wireless provisioning

**Step 1:** Access DNA Center and scroll down to the **Tools** section and select **Template Editor**.

**Step 2:** Click the + sign > **Create Project**. The project provides a logical grouping of templates.
Step 3: The Add New Project dialog box opens for you to complete. At the bottom, click Add.

![Add New Project](image)

Step 4: Repeat Step 2, but select Add Template.

Step 5: The Add New Template dialog box opens for you to complete. Add a Name for the new template. A single template will be created to address both wired and wireless provisioning. If more than one project exists, a drop-down is available to select the correct Project Name; otherwise the project created earlier is auto-filled.

![Add New Template](image)

Step 6: Click the arrow to select the correct Device Type. Scroll down and click the arrow next to Switches and Hubs. Scroll down and select either Cisco Catalyst 9300 Series Switches or Cisco Catalyst 9400 Series Switches.

![Device Type Selection](image)
**Step 7:** Next click the arrow to select the correct **Software Type**. Scroll down and select **IOS-XE**. Once you are finished, click **Add**.

![Software Type Selection](image1)

**Step 8:** To view and confirm your template properties, from the Template Editor, click the gear next to the template you just defined, and select **Properties**.

![Template Editor](image2)

---

**Procedure 2**  Configure the template

In this procedure we will configure the actual commands used in the template to provision ETA and FNF on the Cisco Catalyst 9300 and 9400 Series Switches. The sample template provided below can be copied and pasted directly into the DNA Center Template Editor window.

```plaintext
et-analytics
ip flow-export destination $fc $fc_port
flow record fnf-rec
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
```
match transport destination-port
collect counter bytes long
collect counter packets long
collect timestamp absolute first
collect timestamp absolute last
flow exporter fnf-exp
destination $fc
transport udp $fc_port
template data timeout 30
option interface-table
option application-table timeout 10
flow monitor fnf-mon
exporter fnf-exp
cache timeout active 60
record fnf-rec
interface $wired_interface
ip flow monitor fnf-mon input
ip flow monitor fnf-mon output
et-analytics enable
vlan configuration $wireless_vlan
ip flow monitor fnf-mon input
ip flow monitor fnf-mon output
et-analytics enable
vlan configuration $wireless_guest_vlan
ip flow monitor fnf-mon input
ip flow monitor fnf-mon output
et-analytics enable

The dollar sign signifies that a user entry is required, and the text following the dollar sign will populate the user entry area when provisioning the device, as we discuss below. For further information regarding the Template Editor, please go to [https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-1/user_guide/b_dnac_ug_1_1/b_dnac_ug_1_1_chapter_01111.html](https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-1/user_guide/b_dnac_ug_1_1/b_dnac_ug_1_1_chapter_01111.html).

When you provision the switches using the template example above, you will need to provide the information in the following table.
Table 4. Values needed for template example

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>$fc</td>
<td>Flow Collector IP address</td>
</tr>
<tr>
<td>$fc_port</td>
<td>Flow Collector UDP port</td>
</tr>
<tr>
<td>$wired_interface</td>
<td>Interface(s) to be configured. If configuring a range, include the keyword range and use normal range syntax. Example: range Gi1/0/1-24,Gi2/0/1</td>
</tr>
<tr>
<td>$wireless_vlan</td>
<td>Wireless VLAN(s) to be configured. Use normal VLAN range syntax Example: 1028-1030,1032</td>
</tr>
<tr>
<td>$wireless_guest_vlan</td>
<td>Wireless guest VLAN to be configured</td>
</tr>
</tbody>
</table>

Step 1: Based on the example provided above, either create your customized template in a text editor or simply copy the example above.

Step 2: From the Template Editor, click the template you just created > click Edit > select Paste to paste in the commands from the template example above. This results in the text being populated as seen below.
Step 3: By default, any of the text strings following the $ sign that you will input information for are considered to be mandatory fields. You can change them to be optional by clicking the Form Editor icon in the top right corner of the Template Editor window. Select the field you wish to change, and de-select the Required box. The red asterisk as seen in the Form Editor indicates that the field is mandatory. There is also a box labeled Tooltip Text where you can add any optional tips for that field. Repeat these steps for any additional field you want to make optional.

Tech tip

We recommend that the fields for wired interfaces and wireless VLAN be configured as optional.

Step 4: Once you have made the changes necessary, be sure to click Actions > Save before selecting the CLI Editor icon to return to the template editing screen; otherwise your changes will be lost.
Step 5: When you are satisfied that your template is correct, click Action and select Check for errors. If any errors are found, correct them and repeat the check. Once the check completes successfully, click Save and, once confirmed, click Commit. The Commit dialog box will open where you can add any descriptive notes. Click Commit.

Procedure 3  Create a network profile

Now that the template has been defined, the next step is to create a network profile in DNA Center and assign the template to the profile. Network profiles are assigned to sites that have been previously created in DNA Center under Design > Network Hierarchy.

Step 1: In DNA Center, navigate to Design > Network Profiles and click the Add Profile button. In the pop up select Switching.

Step 2: In the Add a Network Profile workflow, enter a profile name and, in the Attach Templates box, click the Add button.
**Deployment details**

**Step 3:** Click the arrow under Device Type and select the Cisco Catalyst 9300 Series Switches. Then click the drop-down arrow under Template and select the ETA+FNF provisioning template you just created. Click the Add button again and now select the Cisco Catalyst 9400 Series Switches and the ETA+FNF template. Click **Save**.

![Add a Network Profile](image)

**Step 4:** Once the new network profile has been successfully saved, you will assign the sites to which this profile is applicable. Click **Assign Site** and then click the arrow for **Choose a site**. Select the sites for the network profile and click **Save**. Once completed you will see that the ETA+FNF Provisioning profile displays the number of sites you selected.

![Assign Site](image)

**Tech tip**

Please see Appendix E for the template to remove the ETA and FNF configurations from the edge nodes if ever necessary. As with the template used for provisioning, user input will be required to specify the interfaces or VLANs from which the configurations should be removed.

**Procedure 4** Provision ETA and FNF on the SD-Access edge nodes

With the template defined and assigned to a network profile, you are now ready to provision the SD-Access edge nodes.
Step 1: From the DNA Center home screen, select **Provision** and select the devices you want to provision by checking the box next to each device or selecting all. Click the **Actions** drop-down arrow and select **Provision**.

![Device Inventory](https://example.com/device_inventory.png)

Step 2: The next window, **Step 1 Assign Site**, opens. The selected devices will appear as well as the corresponding site that they are located in. If the device has not been assigned to a site yet, you will now select the site by clicking the drop-down arrow and choosing the site. Click **Next**.

![Provision Devices](https://example.com/provision_devices.png)
Step 3: The next window, **Step 2 Configuration**, opens. When deploying the template for ETA and FNF, nothing needs to be changed here and you can just click **Next**.

Step 4: The next window **Step 3 Advanced Configuration**, opens. In the Devices column on the left, you will see the template you just created. Select the box next to the template name or the device(s) listed below it. Provide the required information for the Flow Collector IP address, the UDP port number, and optionally the wired interfaces and appropriate VLANs to be configured. Click **Next**.

Step 5: The **Step 4 Summary** window opens. After verifying the details and the selection of the correct template, click **Deploy** and then either **Apply** now or schedule for later.
Step 6: A status message indicating that the provisioning has successfully started will pop-up, and after a few seconds another pop-up indicating that the provisioning successfully completed should appear. If the provisioning does not complete successfully, you will need to review your template for accuracy and rerun the provisioning.

Tech tip
Two of the most common reasons for a template not to be provisioned successfully are that one of the values specified, such as interface or VLAN, doesn’t exist or that a conflicting configuration already exists on the interface or VLAN; an example of the latter might be another previously defined flow monitor having been configured.

Step 7: Once successfully provisioned, the device inventory Provision Status column should reflect Success.

Step 8: You can then use the Command Runner tool, which can be found in the Tools section of the DNA Center homepage, to verify that the device has been configured correctly.
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 of investigating potential malware through the Stealthwatch integration with 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.
**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**.

![Screen showing Flow Search Results with HTTPS flows](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**.

![Pop-up showing encryption fields](image)
Step 7: Once the settings have been saved, the following screen appears with all of the encryption fields selected.

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: Clicking any attribute (such as TLS 1.0 under the Encryption TLS/SSL Version section) presents those flows.

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

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 in investigating infected hosts and suspicious activity. For complete information regarding portal administration and 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 Intelligence or by scrolling down to the Cognitive Intelligence widget as shown below and clicking View Dashboard.

In 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 signifies that this 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 can 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.
**Deployment details**

**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 (level 8 in this case).

**Step 5:** At the Cognitive Intelligence dashboard, it is also possible to view information that Stealthwatch has collected regarding an infected endpoint. To do so, click the **Show in Stealthwatch SMC** pop-up box that appears when placing your mouse 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 for fabric edge switches

<table>
<thead>
<tr>
<th>Data element name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequence of Packet Lengths and Times</td>
<td>An array of LENGTH values followed by an array of INTERARRIVAL TIME values describing the first N packets of a flow that carry 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</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 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></td>
<td></td>
<td></td>
<td>6.10.2 patch 3</td>
</tr>
<tr>
<td>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.

There is no special software other than Stealthwatch 6.9.4 or 6.10.2, validated within this CVD. Cisco provides CTA to any customer that owns term licensing via any buying method. Cisco fulfills requests for CTA 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.

## SD-Access fabric edge

<table>
<thead>
<tr>
<th>Functional area</th>
<th>Product</th>
<th>Software version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stackable access layer switch</td>
<td>Cisco Catalyst 9300 Series Switches</td>
<td>IOS-XE 16.6.4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DNA Advantage</td>
</tr>
<tr>
<td>Modular access layer switches</td>
<td>Cisco Catalyst 9400 Series Switches</td>
<td></td>
</tr>
</tbody>
</table>

## Wireless controller and access point

<table>
<thead>
<tr>
<th>Functional area</th>
<th>Product</th>
<th>Part number</th>
<th>DNA Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric wireless node</td>
<td>5520 wireless LAN controller</td>
<td>AIR-CT5520-K9</td>
<td>8.5.124.65</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DNA Advantage</td>
</tr>
<tr>
<td></td>
<td>2800 Series access points</td>
<td>AIR-AP2802X-x-K9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wireless DNA Advantage term license, per AP</td>
<td>AIR-DNA-A</td>
<td></td>
</tr>
</tbody>
</table>
## DNA Center

<table>
<thead>
<tr>
<th>Functional area</th>
<th>Product</th>
<th>Part number</th>
<th>Software version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric Controller</td>
<td>Cisco DNA Controller for fabric automation and assurance.</td>
<td>DN1-HW-APL</td>
<td>1.1.6 or 1.1.7</td>
</tr>
</tbody>
</table>

## Identity Services Engine

<table>
<thead>
<tr>
<th>Functional area</th>
<th>Product</th>
<th>Part number</th>
<th>Software version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity services and policy control</td>
<td>Cisco ISE 1-yr 100-session Plus license</td>
<td>L-ISE-PLS-S-100=</td>
<td>2.3</td>
</tr>
</tbody>
</table>
Appendix C: Requirements for enabling ETA

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 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.
Appendix D: References

Cisco Catalyst 9300 Series Switches
Cisco Catalyst 9400 Series Switches
Cisco Cognitive Threat Analytics
Cisco Cyber Threat Defense CVD
Cisco DNA Center Template Editor
Cisco DNA Center User Guide, Release 1.1
Cisco Identity Services Engine web page
Cisco Platform Exchange Grid web page
Cisco Rapid Threat Containment web page
Cisco Security web page
Cisco ScanCenter Administrator Guide
Cisco Stealthwatch Enterprise web page
Cisco Stealthwatch technical reference and specifications
Cisco TrustSec
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’s Guide
Software-Defined Access Design Guide
Appendix E: Template for ETA and FNF removal

The following example may be used to create a template to remove the configurations applied with the provisioning template outlined earlier in the document. The same steps will be required as when first creating the provisioning template and assigning it to a network profile however, you will want to create a unique template under the existing project and a new network profile dedicated to the removal of ETA and FNF configuration commands.

```
vlan configuration $wireless_guest_vlan
  no et-analytics enable
  no ip flow monitor fnf-mon input
  no ip flow monitor fnf-mon output

vlan configuration $wireless_vlan
  no et-analytics enable
  no ip flow monitor fnf-mon input
  no ip flow monitor fnf-mon output

Interface range $wired_interface
  no et-analytics enable
  no ip flow monitor fnf-mon input
  no ip flow monitor fnf-mon output
  exit

no flow monitor fnf-mon
no flow record fnf-rec
no flow exporter fnf-exp
no et-analytics
```

**Tech Tip**

When provisioning the 9300 and 9400 Series Switches by site, the network profile associated with that site will be used in the provisioning process. During network profile definition, site information is associated with the profile as we discussed in Procedure 3, step 4 in the section entitled “Creating DNA Center templates for provisioning ETA and FNF.” Because only one profile of a type, for example “switching,” can be associated with a site, you will need to either modify the original network profile used for provisioning ETA and FNF by removing the sites and then adding them to the new profile or, simply confirming a message that will appear when assigning the sites to the new profile, indicating that the sites will be removed from the old provisioning profile and associated with the new profile for removal of ETA and FNF.
Glossary

AP access point
ASR Aggregation Services Router
C&C Server command and control server
CA certificate authority
CoA change of authorization
CSR certificate-signing request
CI Cognitive Intelligence
CVD Cisco Validated Design
DIA Direct Internet Access
DMVPN Dynamic Multipoint Virtual Private Network
DNA-C Digital Network Architecture Center
DNS Domain Name System
DPI deep packet inspection
EHR electronic health records
ETA Encrypted Traffic Analytics
FC flow collector
FNF Flexible NetFlow
Gbps gigabits per second
GDOI Group Domain of Interest
GETVPN Group Encrypted Transport Virtual Private Network
GRE Generic Routing Encapsulation
HIPAA Health Insurance Portability and Accountability Act
HTTP hypertext transfer protocol
HTTPS hypertext transfer protocol secure
IDP initial data packet
IOT Internet of things
IP Internet Protocol
IPS intrusion prevention system
ISE Identity Service Engine
ISR Integrated Services Router
IWAN Intelligent Wide Area Network
LAN local area network
Mbps megabits per second
mGIG multi gigabit
mGRE Multipoint Generic Routing Encapsulation
MnT monitoring and troubleshooting node
NaaS Network as a Sensor
NBAR network-based application recognition
NTP network time protocol
PAN policy administration node
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
SPLIT sequence of packet length and times
SSL secure sockets layer
SVI switched virtual interface
TCP transmission control protocol
TLS transport layer security
UDP user datagram protocol
UPOE universal power over ethernet
VASI virtual routing and forwarding aware software infrastructure
VLAN virtual local area network
VPN virtual private network
VRF virtual routing and forwarding
VXLAN virtual extensible LIN
WAN wide area network
WLC wireless local area network controller
Please use the feedback form to send comments and suggestions about this guide.