CISCO
SECURE

White Paper
Cisco Public

Cisco Secure – Meeting the DNI NITTF Maturity Framework

The bridge to possible

Table of Contents

Preface

U.S. Government Agencies that interact with or handle classified national security information on computer networks must ensure responsible sharing and safeguarding, including auditing, of the users and systems anywhere data is accessed or resides. Conducting a continuous audit of system logs to evaluate and monitor access, however, doesn't address all issues related to security incidents, including knowledge of how the attempt or successful compromise of systems and classified information occurred, or where that data went.

The National Insider Threat Policy strengthens the protection and safeguarding of classified information. While an accurate audit of cyber events is critical, investment in deterring, detecting, and mitigating insider threats is equally important.

In 2018, the National Insider Threat Task Force (NITTF), along with executive branch members, began looking at ways to strengthen the national effort of mitigating insider threats. The effort of this endeavor is the Insider Threat Program Maturity Framework. This framework is designed to help all executive branch departments and agencies progress toward optimizing their insider threat program capabilities.

Cisco realizes that insider threat is a dynamic problem set, and as the NITTF notes, Insider Threat requires resilient and adaptable programs to address the evolving threat landscape. Utilizing Cisco Secure solutions along with your Security Information and Event Management (SIEM) solution, agencies are able to safeguard classified information from exploitation, compromise, or other unauthorized disclosure.

Insider Threat References

Table 1

Insider Threat References documents and other reference sources containing information that may be useful to understanding topics in this document.

Doc Number	Title
ICS 500-27	Collection and Sharing of Audit Data for Intelligence Community (IC) Information Resources by IC Elements
Presidential Memorandum	National Insider Threat Policy and Minimum Standards
Publication	Insider Threat Mitigation for U.S Critical Infrastructure Entities: Guidelines from an Intelligence Perspective
Executive Order 13587	Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information
Maturity Framework	Insider Threat Program Maturity Framework
CNSS Instruction No. 1015	Enterprise Audit Management (EAM) for National Security Systems
CNSS Directive No. 504	Directive on Protecting National Security Systems from Insider Threat
DODI 8500.02	Information Assurance Implementation
DODI 8530.01	Cybersecurity Activities Support to DoD Information Network Operations

Understanding US Government-wide Insider Threat Programs

To ensure responsible sharing and safeguarding of classified national security information on computer networks, the President of the United States issued Executive Order 13587 in October 2011, defining requirements for agencies that interact with classified information; he also created the Senior Information Sharing and Safeguarding Steering Committee. Additionally, in November of 2012, the President of the United States issued the National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, requiring each Executive Branch department and agency (D/A) with access to classified material to establish an Insider Threat program. Insider Threat programs include the capability to monitor user activity on networks and manually/or electronically gather, integrate, review, assess, and respond to information derived from several sources.

Related to classified information, Intelligence Community Standard (ICS) 500-27 defines the User Activity Monitoring mandatory requirements. The National Insider Threat Policy strengthens the protection and safeguarding of classified information.

Enterprise Audit Management (EAM), User Activity Monitoring (UAM), and Continuous Monitoring, are related activities that seek to identify anomalous behavioral and network events indicative of a potential compromise. CNSS Directive No 504, Directive on Protecting National Security Systems from Insider Threat defines UAM. CNSS Instruction No. 1015, Enterprise Audit Management (EAM) Instruction for National Security Systems defines EAM.

Enterprise Audit Management

CNSS Instruction No. 1015, Enterprise Audit Management (EAM) Instruction for National Security Systems, defines EAM as "the identification, collection, correlation, analysis, storage, and reporting of audit information, and monitoring and maintenance of this capability.

An EAM solution should be deployed to collect, store, and provide access to audit data. For each type of audit (specific to system/mission/data) where auditable events are identified, auditing is conducted to properly capture and store that data, followed by analysis and reporting. Certain high-profile events trigger automated notification to designated individuals, such as system security officers or D/As incident response center/team."

User Activity Monitoring

CNSS Directive No. 504, Directive on Protecting National Security Systems from Insider Threat, defines User Activity Monitoring (UAM) as "the technical capability to observe and record the actions and activities of an individual, at any time, on any device accessing U.S. Government information in order to detect insider threats and to support authorized investigations.".

UAM data must be attributable to a specific user. The D/A should incorporate this data into an analysis system capable of identifying anomalous behavior…"

Continuous monitoring is the process used to maintain a current security status for one or more information systems or the entire suite of information systems on which the operational mission of the organization depends. Conducting a continuous audit of system logs to evaluate and monitor access was the first step, but does not provide real-time knowledge of an attempt to compromise, and a system wide view of how an attack was orchestrated. When data is compromised, log analysis alone will not provide certain understanding of everywhere the data moved.

What agencies need is both a robust system analysis and behavioral analysis tool that has the capability to collect both EAM and UAM data, as well as the ability to perform continuous monitoring. This solution works as part of a comprehensive system that requires all users and devices to be identified, and all network traffic to be viewed in order to identify anomalies. Working together, an accurate audit of Cyber events can be seen, while also deterring, detecting, and mitigating insider threats.

- **EAM is:** a structured, consistent and continuous collection and reporting process across the whole of an organization for identifying, assessing, deciding upon responses to, and reporting upon the efficiencies of, or upon threats that affect the operational continuance of functionality.
- **UAM is:** a structured, consistent and continuous collection and reporting process across the whole of an organization at the device level for identifying, assessing, deciding upon responses to, and acting upon specific analysis of employee threat behaviors. Unlike EAM, the purpose of UAM is to gather detailed and substantive content about behavioral activity, which may be indicative of an insider threat.[1]

The cyber attack continuum encompasses the events before, during, and after a breach or attempted breach. Log data may give clues as to what happened, but doesn't note anomalies that may occur or trigger immediate mitigation efforts. In addition, agencies must learn from attempted breaches, to implement measures that can limit future attacks.

[1] National Insider Threat Task Force (NITTF) Memorandum for: Senior Insider Threat Program Official All Executive Branch Departments and Agencies (NITTF-2014-008).

Insider Threat Program Maturity Framework

The NITTF has developed, in collaboration with executive branch departments and agencies, a maturity framework to enhance the Minimum Standards that Executive Order 13587 initiated.* The Insider Threat Program Maturity Framework enhances the Minimum Standards and enables executive branch departments and agencies to increase their effectiveness.

The maturity framework consists of 19 Elements aligned with the Minimum Standards topic areas. Each maturity element (ME) identifies a capability or attribute of an advanced Insider Threat Program and provides the information needed to assist programs in strengthening their insider threat programs. The framework has the following 19 elements:

Senior Official / Insider Threat Program Leadership	
ME1	Exists as a dedicated effort, positioned in the department and/or agency to ensure access to leadership to build support, identify resources, and integrate insider threat objectives within the department and/or agency's mission and functions.
ME2	Employs metrics to determine progress in achieving program objectives and to identify areas requiring improvement.
ME3	Ensures insider threat program adapts to changes in law, policy, organizational structure, and information technology architecture.
ME4	Employs risk management principles tailored to address the evolving threat environment and mission needs.

Program Personnel	
ME5	Includes stakeholders from a broad range of functional areas and others with specialized disciplinary expertise to strengthen insider threat programs.
ME6	Provides continuing education and training in appropriate fields and disciplines to help professionalize the insider threat cadre.

Employee Training and Awareness	
ME7	Provides training and materials to all employees addressing the full range of insider threats to create a culture of insider threat awareness and prevention within the department and/or agency.

Access to Information	
ME8	Develops automated or scheduled processes for regular and timely receipt and integration of information from all relevant department and agency stakeholders.
ME9	Establishes procedures to receive notification with predictable frequency of information relevant to insider threat from the US Government and federal partner data holders.
ME10	Employs documented processes to validate information sources and identify and assess the use of new information sources.

*NITTF Maturity Framework

Monitoring User Activity	
ME11	Establishes a user activity monitoring capability on all US Government endpoints/devices and government-owned IT resources connected to US Government computer networks accessible by cleared department and/or agency personnel.
ME12	Ensures UAM requirements are incorporated into department and/or agency IT planning, design, and accreditation processes.
ME13	Establishes capabilities to monitor the activity and conduct independent audits of insider threat programs personnel with access to inside threat information and tools.

Information Integration, Analysis, and Response	
ME14	Employs data integration methodologies and advanced analytics to help detect anomalous activity and potential insider threats.
ME15	Employs behavioral science methodologies to help identify indicators of potential insider threats.
ME16	Employs risk scoring capability based on behavioral and workplace factors to assist with detection of anomalous activity and potential insider threats and in the application of tailored mitigation strategies.
ME17	Documents procedures and agreements with other US Government insider threat programs to request or refer information on insider threats of mutual concern.
ME18	Employs case management tools to ensure integrity and effectiveness of the insider threat inquiry and response processes.
ME19	Conducts routine exercises to improve integration, analysis and response procedures and processes.

Meeting the Maturity Framework with Cisco Secure Solutions

Insider threats are one of the fastest growing threats in the modern security network. The Cisco Secure Insider Threat Maturity Framework solution that meets the NITTF Maturity Framework Elements leverages the Cisco Cyber Threat Defense design bringing together NetFlow telemetry from network infrastructure, Cisco Identity Services Engine (ISE) for user and device identity (for UAM and EAM data), and the Cisco Secure Network Analytics (SNA) system to provide network behavior analysis and threat detection.

SNA utilizes the network itself as a sensor to detect threats based on network behavior and uses gathered network telemetry generated by devices, firewalls, endpoints, and physical sensors analyzing all traffic to expose suspicious or malicious activities caused by insider threats. SNA is constantly monitoring the network's behavior to detect threats everywhere. Over time, SNA sees all network traffic and establishes a baseline for normal behavior. This allows SNA to find various kinds of threats that would otherwise go undetected. Network traffic is a source of truth for any and all suspicious activity and thus enhances contextual awareness, allowing SNA to dive deep into the forensics. Cisco ISE allows for SNA to have the user mapped to each and every flow record. SNA will notify when an anomaly occurs. As an example, if a remote desktop user is doing something out of the ordinary, or attempting to access sensitive material at an unusual time, SNA will trigger an alert.

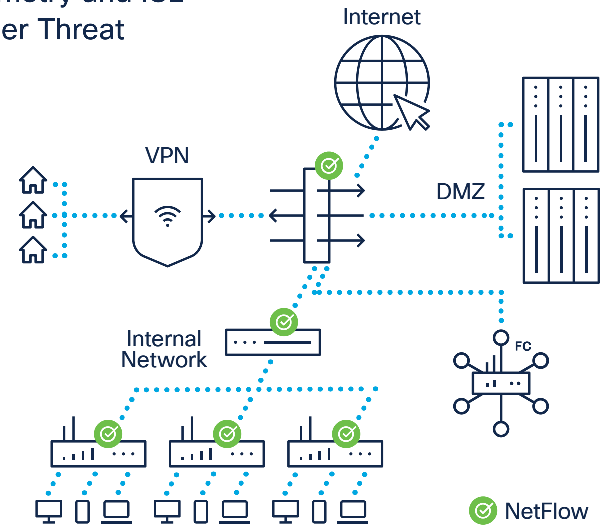
Because SNA looks for behavioral anomalies, it is especially great for monitoring lateral movement for insider threats. Most organizations focus on protecting their networks from targeted attacks from external sources and lose sight of threats that start within their networks.

The SNA dashboard provides much more than just alerts. It provides a view into all session traffic with information on top internal/external hosts or devices and how much communication is happening between these devices. It also has the ability to drill down into past events with a variety of search and filtering features for deeper forensic analysis even on a specific user. This is especially useful for both NetOps and SecOps teams looking to sift through east-west traffic with ease.

This section will map how the Cisco Secure Insider Threat Maturity Framework solution meets and exceeds the NITTF Maturity Framework Elements.

Using NetFlow Telemetry and ISE to Capture the Insider Threat

Figure 1



Both ISE and SNA meet UAM for insider threat directives and contribute to overall system security and insider threat detection. Additionally, the Cisco Secure Client (AnyConnect) (with APEX License) that is used for VPN connection can be utilized to capture and feed activity from endpoint workstations into the current security NetFlow records – see Figure 2: Cisco Secure Client (with APEX License) for additional NetFlow records.

Cisco Secure Client (with APEX License)

Figure 2

- NetFlow Record (Source IP, Destination IP, etc)
- Unique Device ID (correlate records from same endpoint)
- Device Name* (bsmith-WIN7)
- Local DNS* (starbucks.com), Target DNS**
- Process Name (iexplore.exe)
- Process Identifier (iexplore.exe unique ID)
- Parent Process Name (process that launched iexplore.exe)
- Parent Process Identifier (launching process unique ID)

*Admin can choose not to collect this data

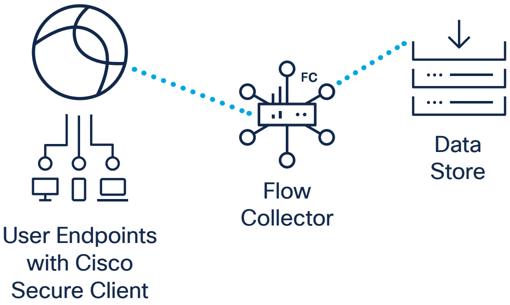
For seamless protection of branch networks, the SNA Learning Network (SLN) monitors, builds policies based on traffic patterns, and reports anomalies or suspicious activity. Together, this solution provides deep visibility across the entire department and/or agency and delivers fast threat detection with quick response (even automated mitigation), along with the ability to provide historical data related to any incident that may occur.

Utilizing this Cisco Secure Insider Threat Maturity Framework solutions along with Security Information and an Event Management (SIEM) solution, agencies are able to safeguard classified information from exploitation, compromise, or other unauthorized disclosure.

With Cisco Secure Client you can view endpoint enriched NetFlow by performing flow searches on devices providing Cisco Secure Client (AnyConnect) Network Visibility Module (NVM) data. You can retain all NVM telemetry records with the SNA Data Store meeting Insider Threat Mandates of holding UAM data (see Figure 3: Retaining all NVM telemetry records with the SNA Data Store).

Retaining all NVM Telemetry Records with the SNA Data Store

Figure 3



NVM Telemetry

Session

Start Time*
End Time*
Source IP*
Source Port*
Destination IP*
Bytes Sent*
Bytes Received*
Packet Count* (derived)
Protocol*

Interface

Interface Info UID
Interface Index
Interface Type
Interface Name
Interface Details List
Interface Mac Addr.

User and OS

UDID
User
User Account Type
Agent Version
Virtual Station Name
OS Name
OS Version
OS Edition
System Manufacturer
System Type

Process

Process Account
Process Account Type
Process ID
Process Name*
Process Hash*
Process Path
Process Args
Parent Process ID
Parent Process Account
Process Account
Parent Process Name*
Parent Process Hash*
Parent Process Path
Parent Process Args
Host Name
DNS Suffix
Module Name List
Module Hash List
Parent Process Name
Parent Process Hash

*NVM telemetry records available within non-Data Store deployment

Using the Cisco Secure Client monitors user activity and meets these maturity elements[2]:

ME8	The Cisco Insider Threat Maturity Framework solution develops automated or scheduled processes for regular and timely receipt and integration from various relevant agency stakeholders.
ME11	By establishing a user activity monitoring capability on US Government endponts and devices (Windows, Linux) connected to US Government computer networks accessible by cleared department and/or agency personnel.
ME12	The Cisco Maturity Framework Insider Threat solution has a management console and the utilization ensures UAM requirements are incorporated into accredited processes, many of which can be automated as well as put into procedure such as Insider Threat Hub playbooks.
ME13	The Cisco Insider Threat Maturity Framework solution establishes the capability to monitor the activity and conduct independent audits of Insider Threat Program personnel with access to insider threat information and tools. Monitoring access to all devices on the network not just desktops and servers.
ME14	The Cisco Insider Threat Maturity Framework solution employs data integration methodologies and advanced analytics to help detect anomalous activity and potential insider threats.
ME15	The Cisco Insider Threat Maturity Framework solution employs behavioral science methodologies to help identify indicators of potential insider threats.
ME16	The Cisco Insider Threat Maturity Framework solution employs risk scoring capability based on behavioral and workplace factors to assist with detection of anomalous activity and potential insider threats and in the application of tailored mitigation strategies.
ME17	The Cisco Insider Threat Maturity Framework solution can assist with the documentation of procedures (e.g., playbook information) that assist with the requesting and referring of information on insider threats of mutual concern.
ME18	The Cisco Insider Threat Maturity Framework solution along with the Cisco SecureX platform (integrated platform management available with any Cisco Secure subscription) employs case management tools and ensures integrity and effectiveness of the insider threat inquiry and response process.
ME19	The Cisco Insider Threat Maturity Framework solution allows for routine, automated, repeatable exercises to improve integration, analysis and response procedures and processes.

[2] Detailed information about each Maturity Element can be found here: https://www.dni.gov/files/NCSC/documents/nittf/20181024_NITTF_MaturityFramework_web.pdf

Specific Examples of SNA Alerts to Identify Insider Threats

SNA can generate over 100 different alert types out of the box for all kinds of different activity and thousands more can be created with customer security events. Some of these alerts focus specifically on insider threats. As an example, SNA has the ability to classify every device connected to the network into logical host groups by functions, locations, device types, etc. and it will trigger an alert if any unusual access or activity occurs. If a device in the marketing host group tries to access a server that hosts sensitive employee data (that would normally be only accessed by the HR host group) an alert will be triggered.

Organizations can also create their own custom policy violation alerts within SNA to trigger on things like traffic to blocked countries, connections to an external server, etc. So even if an attacker gains access to the network, or legitimate employees are trying to access sensitive data they don't shouldn't be, SNA will immediately detect this activity and provide an alert.

- **Data Hoarding** alerts could also be indicative of an insider threat. There are two types of this alert category that Cisco Secure Network Analytics will generate: suspect data hoarding and target data hoarding.
  - **Suspect data hoarding** identifies an inside host, acting as a client, that is downloading data from other hosts. If the client exceeds its set threshold or its expected behavioral norm, it is considered the suspect and will fire this alert.
  - **Target Data hoarding** is a similar alert that identifies an internal host, but this time the host is acting as a server, delivering data to a host or set of hosts. This device is likely a target of an attack being initiated by one of the other connected devices. Both alerts clearly indicate misuse and suspicious behavior to an extent. Should this activity continue, or more targets/suspects get identified, an additional alert for data exfiltration will fire off, indicating that obvious unwanted data transfer is occurring.
- **Internal Brute Force attacks** occur when an attacker uses automated tools or manually attempts numerous password combinations to break into a protected system. This attacker could either be the disgruntled employee or an external threat that has infiltrated and compromised your systems and been snooping around unnoticed. If compromised, systems can fall victim to unwanted configuration changes, data theft, or slowdowns that can seriously impact the business. Both of these users would be capable of navigating their way through east-west traffic and breaching a system using an automated tool.

SNA also sees an abnormally large volume of login attempts as evidence to support an alert. If a SOC operator gets an alert, a simple firewall rule or host isolation can stop the threat in its tracks, and a look through previous session traffic can identify other devices that this insider threat may have been poking around in.

Additionally, SNA can detect reconnaissance activity, TOR traffic, C&C traffic, firewall policy violations (the list goes on) and more with the ability to create your own custom security event activity to look for specific policy violations.

Certification and Accreditation on Government Networks

The Cisco Secure solution (Cisco Secure Network Analytics and Cisco ISE) is an approved architecture and has gone through the Certification and Accreditation process on US Government networks, to ascertain the specific technical security requirements and assurances for confidentiality, integrity, and availability.

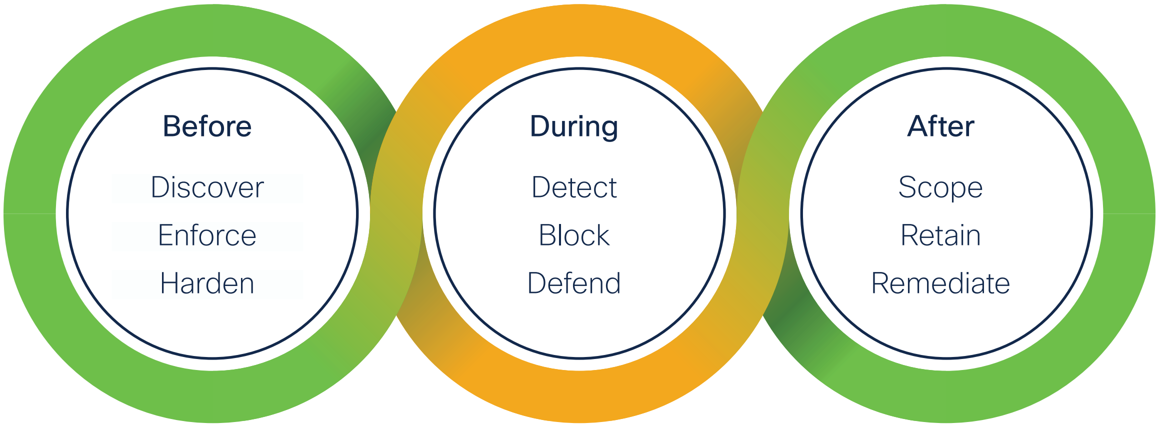
This makes it easy to deploy (the hard work has been done – certification, security approval, and customer approval).

Using Your Network as a Sensor

The Cisco Secure Insider Threat Maturity Framework solution works with your Security Information and Event Management (SIEM) solution to turn your entire network into a sensor to provide knowledge before, during, and after a cyber attack. Utilizing Cisco Identity Services Engine (ISE), along with Cisco SNAs, anomalies are quickly identified and appropriately handled.

When a device first attempts to access a network, checks can be performed prior to the device or user getting anywhere on the network; if the device does not comply, then it can be quarantined and isolated in order to remediate to an approved state for network access.

The Attack Continuum



Strategic Imperatives

Visible

Network-Integrated

Broad Sensor Base

Context Sharing and Automation

Focused

Continuous Advanced Threat Protection

Security Intelligence

Integrated

Leading Products Working Together as a System

Built for Scale, Consistent Control, Management

In addition, the type of device, user, and history of the two, can allow for very granular controls of what can be accessed. While the user is going about normal job duties, a behavior model is created for how the network and devices are normally accessed, which can be tuned for groups of similar workers, locations, or other agency specific criteria. If a user or device does something unusual, alerts can notify security analysts to look further, or for known bad behavior, can go as far as automatically removing them from the network or isolating them for remediation.

By accurately knowing who, what, when, where, and how the data is being accessed, and if the behavior is normal or not, you can be confident in your ability to secure the environment and go after any bad actors or malicious tactics both in real time and after the fact.

Easy Deployment that Leverages Existing Infrastucture

Installation and deployment is easy and intuitive, leveraging the existing infrastructure, the router, the switch and the firewall. Probes and taps do not need to be deployed everywhere; simply put in standard configuration on your existing routers, switches, and firewalls to export NetFlow. As devices are routing communications around the network, a log of every single conversation is acquired, which is a very powerful component in catching and deterring insider threats.

Installation and deployment can be done in a day on large agencies and organizations with complex networks and will support these core capabilities:

- **Flow analysis:** The ability to analyze flow records
- **Anomaly detection:** The ability to analyze traffic for deviations from baselines that may indicate anomalous behavior
- **Real-time reporting and alerting:** The ability to generate security alerts and network performance alerts on a real-time basis.
- **Insider threat hubs, security operations centers, network operations and security information assurance teams:** Can see who is using the network, what applications and services are in use, and how well they are performing.

Teams can rapidly detect and prioritize security threats, pinpoint network issues and misuse, find suboptimal performance issues, and manage event response across the organization.

Cisco Identity Services Engine

The network no longer sits within four secure walls. It extends to wherever employees and data travel. Employees today demand access to work resources from more devices and through more nonenterprise networks than ever before. Mobility, digitization, and the Internet of Things (IoT) are changing the way we live and work. As the modern network expands, so does the complexity of marshaling resources, managing disparate security solutions, and controlling risk. Agencies are challenged with supporting a proliferation of network-enabled devices even as a myriad of security threats and highly publicized data breaches demonstrate the importance of protecting access to the evolving network.

A different approach is required to both manage and secure the evolving enterprise network. This approach can be accomplished with the Cisco Identity Services Engine (ISE).Visibility and control help organizations get ahead of threats. That means having deep visibility into the users, devices, and applications accessing your network. It also means gaining the dynamic control to make sure that only the right people with trusted devices get the right level of access to agency services.

ISE simplifies the delivery of consistent, highly secure access control across wired and wireless multivendor networks and remote VPN connections. With far-reaching, intelligent sensor and profiling capabilities, ISE can reach deep into the network to deliver superior visibility into who and what are accessing resources. It can share vital contextual data with technology partner integrations, and it can implement Cisco TrustSec policy[3] for software-defined segmentation. Cisco ISE transforms the network from a simple conduit for data into a security enforcer that accelerates the time to detection and time to resolution of threats.

[3] More about Cisco TrustSec here: http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html

Cisco Secure Network Analytics

Today's networks are more complex and distributed than ever before. New security challenges arise weekly. The ever-evolving threat landscape, along with trends, such as cloud computing and the Internet of Things, further complicates the situation. Unfortunately, as more and more users and devices are added to the network, gaining visibility into what's going on is harder to achieve. And you can't protect what you can't see.

Seeing into all traffic flows, applications, users, and devices that are known and unknown is critical to determine whether there may be anomalous behavior occurring on your network. Using sophisticated behavioral analytics, secure network analytics (SNA) transforms data from existing infrastructure into actionable intelligence for improved network visibility and security and accelerated incident response.

SNA dramatically improves network visibility, security, and response times to questionable incidents across the entire network. It helps security operations staff gain real-time situational awareness of all users, devices, and traffic on the network, in the data center, and in the cloud. And it allows security teams to quickly and effectively respond to threats before, during, and after a security incident by providing real-time, continuous monitoring and pervasive views into all network traffic.

Applying context-aware security analysis to automatically detect anomalous behaviors, SNA can identify a wide range of attacks, including malware, zero-day attacks, distributed denial-of-service (DDoS) attempts, advanced persistent threats (APTs), and insider threats.

SNA is comprised of a number of components to provide a robust and comprehensive view of network activity. The two primary components to this system required for operation are the Flow Collector and SNA Management Console appliances. These can be deployed as physical appliances and as virtual machines. The flow collector aggregates all of the network telemetry data SNA uses to conduct its analysis. It performs stitching and deduping operations on the incoming data to create the conversational flow record, and handles most of the analytical heavy lifting for the system.

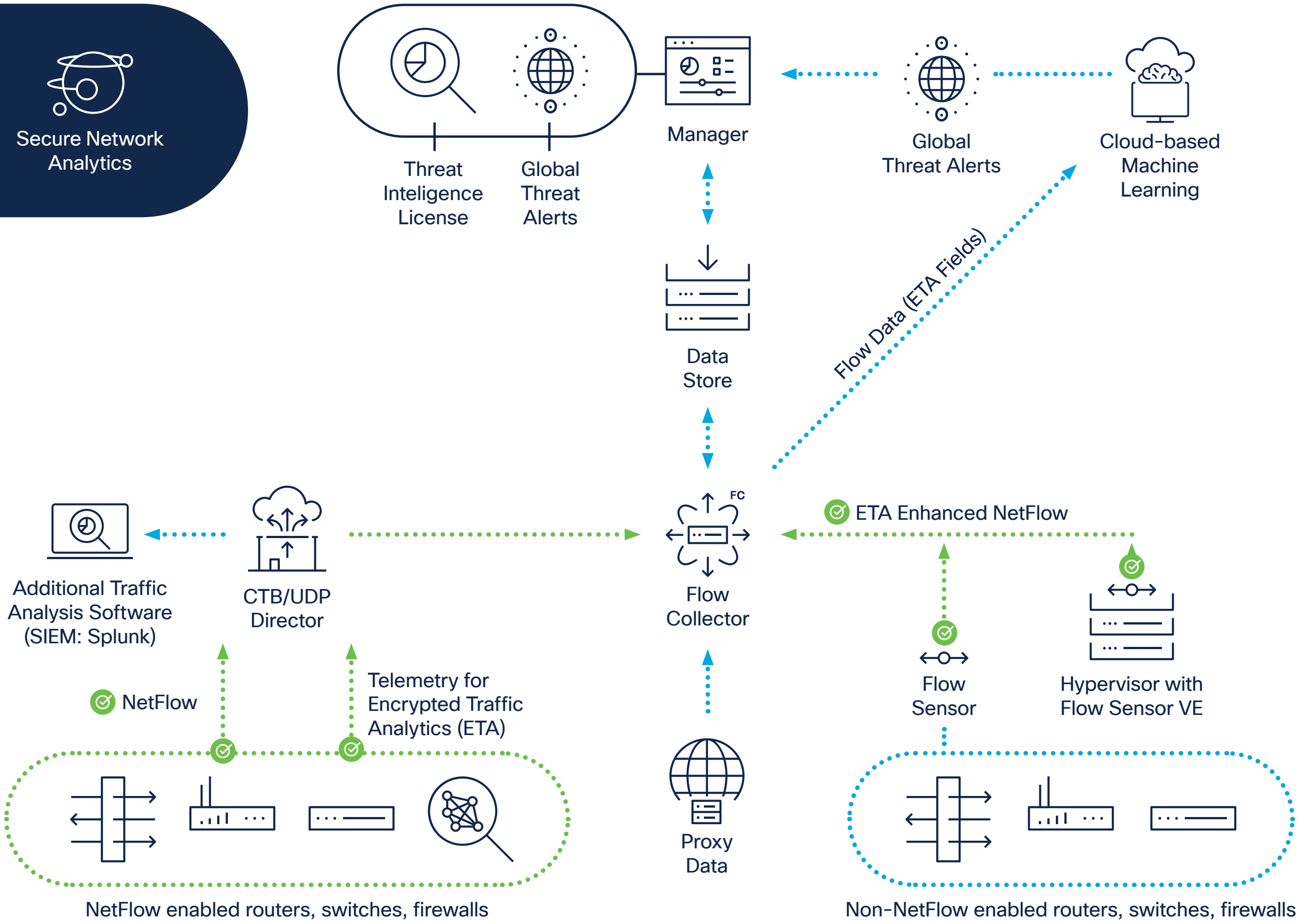
The SNA Management Console works as your microscope and your macroscope into this sea of data collected by the Cisco Secure Network Analytics system. In addition, it takes in additional telemetry from identity services, such as Active Directory and Cisco ISE, and threat intel to add context to the collected network traffic.

Flow Sensors are used to generate NetFlow in areas of the network that don't possess native exporting capabilities, by reading PCAP data from a SPAN or TAP port and converting that to NetFlow data (to include Layer 7). The Flow Sensor can also be deployed as a physical or virtual appliance.

Secure Network Analytics

The SNA System

Figure 4


Threat Inteligence License
Global Threat Alerts
Manager
Global Threat Alerts
Cloud-based Machine Learning
Data Store
Flow Data (ETA Fields)
Additional Traffic Analysis Software (SIEM: Splunk)
CTB/UDP Director
FC
Flow Collector
ETA Enhanced NetFlow
NetFlow
Telemetry for Encrypted Traffic Analytics (ETA)
Flow Sensor
Hypervisor with Flow Sensor VE
Proxy Data
NetFlow enabled routers, switches, firewalls
Non-NetFlow enabled routers, switches, firewalls

SNA Component Descriptions

The following provides a description of each of the SNA system components

Secure Network Analytics Manager: A physical or virtual appliance that aggregates, organizes, and presents the analysis from flow collectors, Cisco Identity Services Engine, and other sources.

Secure Network Analytics Flow Collector: A physical or virtual appliance that aggregates and normalizes network telemetry and application data collected from data exporters such as cisco routers, switches, and firewalls.

Secure Network Analytics Data Store: The Data Store is a new and improved database architecture design for SNA comprised of a three-node database cluster. Flow ingest by Flow Collectors is separated from data storage. The SNA Data Store scales telemetry consumption, provides data resiliency, and increases search performance for the most demanding enterprise-class environments. You can also store Cisco Secure Firewall Logs (both ASA and NGFW) on Premise with the Data Store enriching UAM data.

Note: Data Store and NVM data collection enables extended and continuous remote worker visibility to include working on-network (full tunnel), on and off network (split tunnel), and off network (without VPN).

Flow Sensor: A physical or virtual appliance that provides an overlay solution for generating enriched flow data. A flow sensor is generally needed for infrastructure that is not capable of producing unsampled NetFlow data at line rates, for third-party components that do not support unsampled NetFlow, and for other environments where additional security context is required (e.g. monitoring UAM data).

Threat Feed: A global threat feed that provides an additional layer of protection against known botnets and other sophisticated attacks. This feed correlates suspicious network activity with data on thousands of known command-and-control servers.

Secure Network Analytics Endpoint License: An add-on that allows Cisco Secure Client (AnyConnect) telemetry data to be captured from devices that connect to the network, such as desktop computers, laptops, and smartphones. This feature provides detailed NVM reports and customized security alarms.

Cisco Telemetry Broker: Telemetry Broker optimizes telemetry pipelines for the hybrid cloud. It vastly simplifies the consumption of telemetry data for customers' business-critical tools by brokering hybrid cloud data, filtering unneeded data, and transforming data into a usable format.

User Datagram Protocol (UDP) Director: A physical or virtual appliance that allows UDP traffic to be redirected to multiple collection points, such as network management solutions and Hadoop and similar frameworks that store and process large datasets.

Advantages of Using SNA and ISE Together for Monitoring User Activity

By utilizing SNA together with the ISE, you get critical network visibility better control access to data and resources, and an upper hand against attackers and insiders. This Cisco Insider Threat solution assesses for inclusion in UAM on all US Government endpoints and devices, networks, and Government resources to identify critical assets in a classified environment, controlled unclassified environments, and personally identifiable information which if degraded, stolen, or exploited would cause damage to personnel, facilities and infrastructure, mission, or national security.

This Cisco Secure solution can allow for risk assessment models to be created about the effectiveness of the technical and physical monitoring risk profile for insider threat. The capability also can help reinforce the integrity and effectiveness of the Insider Threat Program's mission ensuring there is no misuse or mishandling of information accessed, developed, or retained by the Insider Threat Program. Cisco Secure solutions can also conduct independent monitoring and auditing of Insider Threat personnel (Watch the Watcher) and acts as a check to ensure there is not mishandling or misuse of information. The integrated solution offers many additional benefits (see Table 2: SNA and ISE Integrated Solution Benefits).

SNA and ISE Integrated Solution Benefits

Table 2

Solution Benefit		Description
1	Better Network Visibility	The SNA system collects and analyzes NetFlow from your routers, switches, and firewalls. It then delivers comprehensive visibility at the network core, edge, data center, and cloud. Cisco ISE adds to this visibility with in-depth device and user data.
2	More Detailed Security Context	By integrating SNA and ISE, you can see a myriad of details about network traffic, users, and devices. Instead of just a device's IP address, Cisco ISE delivers other key details, including user name, device type, location, the services being used, and when and how the device accessed the network.
3	Faster Threat Detection	With the combination of network visibility and security context, you can detect threats faster and more comprehensively.
4	Effective Network Segmentation	Cisco ISE can help you create and enforce segmentation policies to keep unauthorized users and devices from accessing restricted areas of the network. SNAs expansive visibility can help you determine how to most effectively segment the network, and help monitor the efficacy of your policies when they are in place.
5	Unified Access Control	With SNA and ISE together, you can create, enforce, and monitor role-based access control policies throughout the entire network all from one place. ISE grants appropriate network access to users and devices based on advanced profiling capabilities. It then shares this data with SNA for more precise threat detection. SNA feeds user behavior back to ISE to immediately update access policies for suspicious or compromised users.

6	Dramatically Improved Incident Response and Forensics	SNA and ISE help you quickly identify the source of an incident. When SNA detects anomalous traffic, it can send an alert to Cisco ISE to automatically quarantine the user.
7	Actionable Security Intelligence	Use your entire network as a sensor and an enforcer by turning massive amounts of data from existing network infrastructure into actionable security intelligence.
8	Greater Operational Efficiency	The combined solution significantly reduces the manual actions needed to detect, investigate, and remediate threats. The device onboarding burden for your IT staff is eased with self-service onboarding through ISE.
9	Ability to Harness Security as an Enabler	With effective, scalable security across the entire network, you can more confidently expand and enhance your network through initiatives such as digitization, mobility, cloud, and the Internet of Things (IoT).
10	Enhanced Compliance	More easily pinpoint and remediate any violations of industry and government regulations.

Advantages of Using SNA and ISE Together for Information Integration, Analysis, and Response

With the Cisco Secure solution, departments and/or agencies with a large or geographically dispersed workforce can increase effectiveness of identifying insider threat occurrences through the use of data aggregation and normalization utilities and advanced analytics. SNA and ISE working together helps manage large data volumes as a first step in establishing a baseline from which to identify anomalous behavior. This allows insider threat analysts to contextualize the behavior in supporting decisions to conduct inquiries, refer matters to response elements in an organized manor, and assist with mitigation strategies.

With the human-centric nature of the insider threat, it's important to have behavior science capabilities. SNA delivers best of breed behavior science analytics. Cisco Secure assists behavior science expertise personnel by assisting with additional context and allows for the adjustment and fine tuning of insider threat indicators, triggers, and thresholds.

Cisco Secure makes it easy to run periodic exercises to improve effectiveness in conducting inquiry and response processes with Insider Threat operating procedures. This builds best practices, and allows for a multidisciplinary approach in analyzing behavioral anomalies. The Cisco Secure solutions can run these exercises to build and enhance best practices and improve in the analyzing of behavioral anomalies as well as testing the adequacy of insider threat indicators, triggers, and thresholds.

Key Benefits and Integrating into SIEM Tool

By implementing Cisco Secure solution and integrating with your SIEM tool of choice, your agency will comply with both the letter and spirit of the requirements outlined in ICS 500-27 and future proof you cyber security efforts all while leveraging the investment already made in your networks (see Table 3: ICS 500-27 Requirements Mapping to Cisco Secure and SIEM).

ICS 500-27 Requirements Mapping to Cisco Secure and SIEM Integrated Solution

Table 3

ICS 500-27 Requirements (U/FOUO)	Solution Provides
Authentication Events (Logon / Logoff)	✓
File & Object review (Create, Access, Delete, Modify, Permissions/Ownership Modifications)	✓
Writes / Downloads to external devices / media	✓
Uploads from external devices / media	✓
User and Group Management events User add, delete, modify, suspend, lock	✓
Group / Role add, delete, modify Use of Privileged / Special Rights events	✓
Security or audit policy changes	✓
Configuration changes	✓
Admin or root-level access	✓
Privilege / Role escalation	✓
Audit and log data accesses	✓
System Reboot, Restart & Shutdown	✓
Print to a device	✓
Print to a file	✓
Application initialization	✓
Export of information	✓
Import of information	✓

Why Cisco Secure

This Cisco Secure SNA and ISE solutions are the result of more than 20 years of network security experience and validated system architectures. They help you decrease risk by balancing flexibility and enablement with protection, transforming business procedures into automatic enforcement.

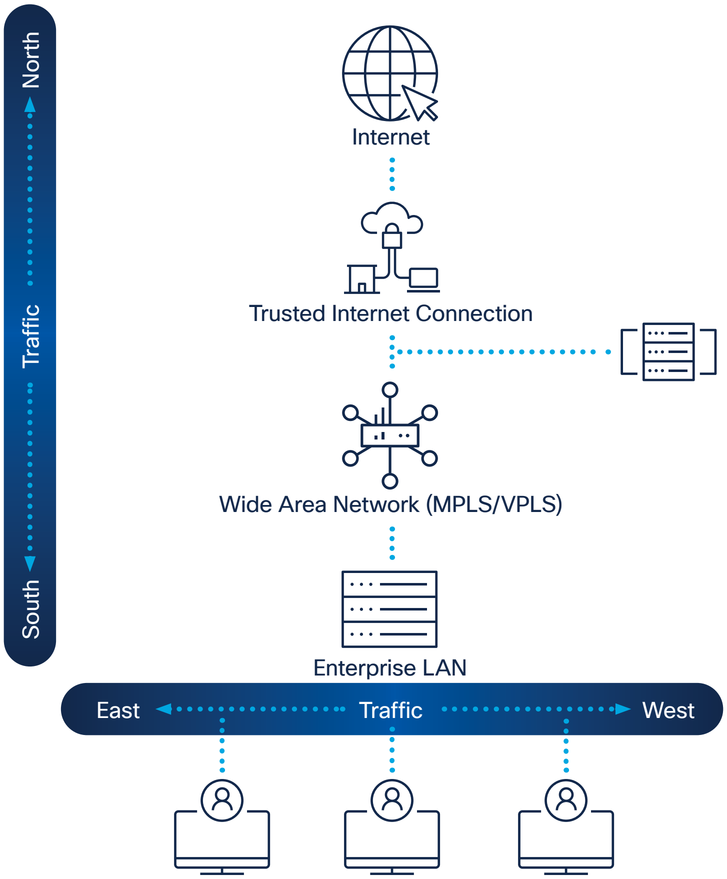
- **End-to-end security coverage for the entire infrastructure.** Traditional suppliers provide security through isolated endpoint devices on the network edge. With Cisco, security is embedded into every product in the network infrastructure, from routers and switches to the data center. This allows threats to be recognized within seconds or minutes, instead of days or hours.
- **Added value of network intelligence.** Each Cisco Secure product has built-in intelligence, and uses it to analyze current conditions and interoperate with other intelligent network devices. The result is an intelligent network security system, where all devices share threat information, and create rules to pass to the security center.
- **A global view of the security threat landscape.** Cisco Secure devices participate in Cisco Security Intelligence Operations (SIO), to provide an overview of security threats worldwide and locally. This allows them to dynamically and automatically adapt to changing threat environments in real time.
- **The very latest security products.** Cisco is constantly releasing innovative networking and support tools, and often leads the way in offering new security implementations. As your agency grows and develops, you can be confident that it will always have the most advanced level of security.
- **Award-winning, 24-hour technical support.** Cisco Secure solutions come from Cisco, a single, stable vendor who can meet your ongoing service and support needs. Outstanding quality and reliability are built into every Cisco Secure product, but if there is ever a problem, it can be replaced quickly.

A Security Model that Leverages Your Network

Because of the nature of determined attacker and insider threats, new tools and technologies are needed to develop a comprehensive response to the threats affecting government agencies. This must be done using a model that minimizes complexity and helps protect the business assets in a continuous fashion, while addressing the changes in business models, such as any-to-any. The security system should be integrated directly into the network fabric to maximize its efficiency and capability, while minimizing the risk normally associated with adding disparate, non-network-aware security controls. To design such a system, a new model is needed to ensure that this integration can properly take place, especially in the data center. where the margin of error is so small.

Network Traffic Flow

Figure 5



This model addresses the threat problem by looking at the actions you must take before, during, and after an attack, as well as across the broad range of attack vectors such as endpoints, mobile devices, data center assets, virtual machines, and even in the cloud. Where most security solutions tend to address the threat at a point in time, it is important to look at it as a continuous cycle.

Before an Attack

Context-aware security is required to defend against context-aware attackers. Organizations are fighting against attackers that have more information about their infrastructures than the defenders trying to protect them. To achieve information superiority over attackers and defend before an attack occurs, organizations need total visibility of their environment including, but not limited to, physical and virtual hosts, operating systems, applications, services, protocols, users, content, and network behavior. Defenders need to understand the risks to their infrastructure, based on target value, legitimacy of an attack, and history. If defenders do not understand what they are trying to protect, they will be unprepared to configure security technologies for defense. Visibility needs to span the entirety of the network, including endpoints, email and web gateways, virtual environments, mobile devices, and the data center. From this visibility, actionable alerts must be generated so that defenders can make informed decisions.

During an Attack

Modern threats are relentless and occur frequently. Traditional security technologies can evaluate an attack only at a point in time, based on a single data point of the attack itself. This approach is no match against advanced attacks.

Instead, government agencies need a security infrastructure based on the concept of awareness; one that can aggregate and correlate data from across the extended network with historical patterns and global attack intelligence to provide context and discriminate between active attacks, exfiltration, and reconnaissance versus simply background activity. This evolves security from an exercise at a point in time to one of continual analysis and decision-making. With this real-time insight security, professionals can employ intelligent automation to enforce security policies without manual intervention.

After an Attack

To address the full attack continuum, organizations need retrospective security. Retrospective security is a big data challenge, and a capability that few are able to deliver. With an infrastructure that can continuously gather and analyze data to create security intelligence, security teams can automatically identify IOCs, detect malware that is sophisticated enough to alter its behavior to avoid detection, and then remediate.

Compromises that would have gone undetected for weeks or months can be rapidly identified, scoped, contained, and remediated. This threat-centric security model lets organizations address the full attack continuum across all attack vectors and respond at any time, all the time, and in real time.

NetFlow

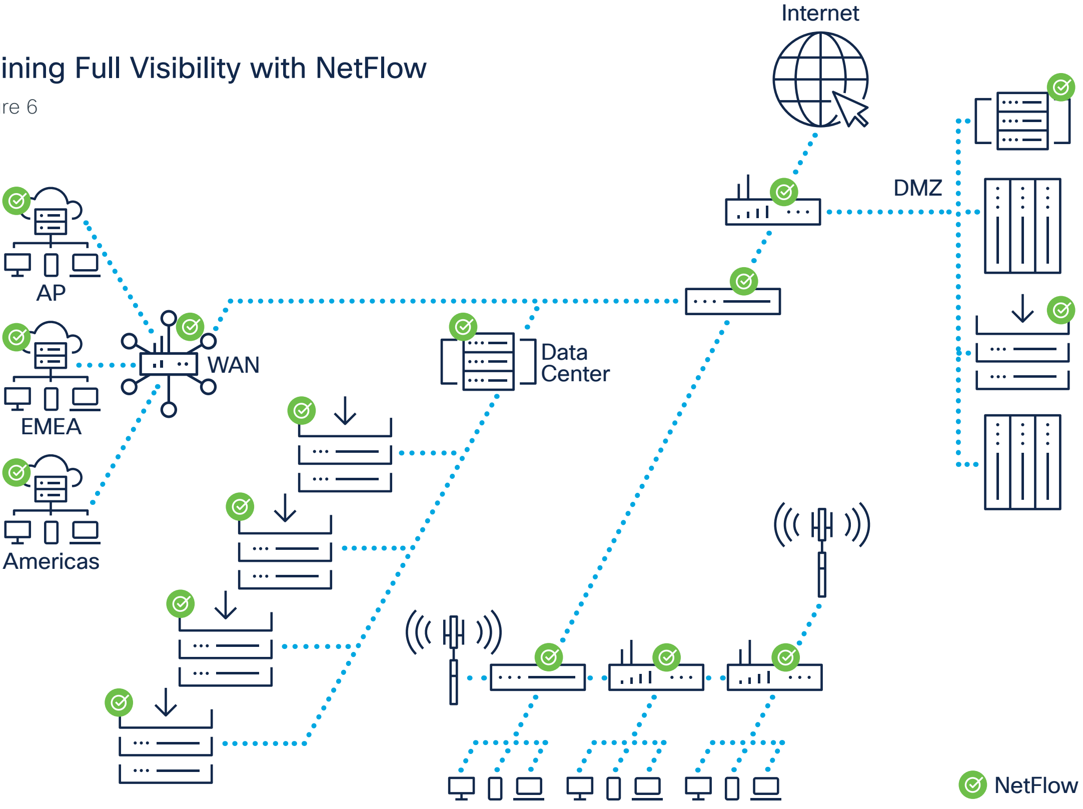
NetFlow is embedded in Cisco networking equipment, which characterizes network operations by examining connection data. Standardized through the RFC process, variants of NetFlow are available in network equipment from such vendors as Arista, Citrix, Juniper, Palo Alto, a variety of Linux operating systems distributions and Cisco Secure Network Analytics can get NetFlow from Cloud environments as well as virtual machines.

NetFlow measures IP network traffic attributes of a traffic flow. A flow is identified as a unidirectional stream of packets between a given source and destination as it traverses the network. NetFlow was initially created to measure network traffic characteristics such as bandwidth, application performance, and utilization. NetFlow has traditionally been used for billing and accounting, network capacity planning, and availability monitoring.

NetFlow is a reporting technology. As a NetFlow-enabled network device processes traffic, the device gathers data about the traffic flow and reports (or exports) the data to a defined collector. Older versions of NetFlow exported data only after the connection closed. Newer NetFlow implementations added the capability of defining one or more expiry timers (active or inactive) or conditions (connection complete or cache full). The nature of NetFlow reporting has tremendous security applications including the ability to provide non-repudiation, anomaly detection, and investigative capabilities.

Gaining Full Visibility with NetFlow

Figure 6



Cisco takes advantage of NetFlow. Using this approach, the solution has defined NetFlow records for each solution device to maximize the security monitoring potential of each device by collecting packet fields such as TCP flags, time-to-live (TTL) values, protocol, and application name using Next Generation Network-Based Application Recognition (NBAR2) and Cisco AVC.

The latest iteration of NetFlow extends the capabilities to help customer determine how to optimize resource usage, plan network capacity, and identify the optimal application layer for quality of service (QoS). NetFlow plays a vital role in network security by detecting denial-of-service (DoS) attacks and network-propagated worms.

SNA is a purpose-built, high-performance network visibility and security intelligence solution. Through the collection, aggregation, and analysis of NetFlow data, along with other contextual data sources such as identity data from Cisco ISE, system-specific data such as syslog and Simple Network Management Protocol (SNMP), and application data via NBAR2 and Cisco AVC. SNA helps insider threat, network operations and security operations staff gain real-time situational awareness of all users, devices, and traffic on the network. SNA also allows security operations staff to quickly and effectively respond to threats before, during, and after a security incident by providing real-time continuous forensics and a view into all network traffic.

Conclusion

This document discusses some of the challenges in defending networks against modern, advanced threats and provides design guidance for using solutions from Cisco Secure.

The solution focuses on meeting the NITTF Maturity Framework, as well as improving situational awareness and reducing the time required to detect and respond to threats acting inside the network, not just at the traditional network perimeter. The solution enables the network infrastructure to provide increased visibility and control, and incorporates Cisco's leading security technologies in an integrated design. The end result is a real improvement in the detection of insider threats and the defender's ability to detect, block, and remediate threats in advanced ways.

Utilizing solutions from Cisco Secure along with your Security Information and Event Management (SIEM) solution, agencies are able to safeguard classified information from exploitation, compromise, or other unauthorized disclosure, in alignment with the intent of ICS 500-27.

Learn more about the National Insider Threat Task Force and their mission

Visit dni.gov/index.php/ncsc-how-we-work/ncsc-nittf

Learn more about Cisco Cybersecurity for the United States Federal Government

Visit cisco.com/c/en/us/products/security/cisco-cybersecurity-for-government.html#~resources