Trusted Internet Connections (TIC) 3.0

Remote Worker Architecture Guide

July, 2020
Contents

Abstract .................................................................................................................................................. 3
TIC 3.0 Overview .................................................................................................................................. 4
Cisco SAFE Overview ................................................................................................................................. 6
Business Flows ......................................................................................................................................... 8
Attack Surface ........................................................................................................................................ 10
Security Capabilities .............................................................................................................................. 12
Architecture Overview ............................................................................................................................... 14
Solution Overview .................................................................................................................................... 17
Abstract
Since 2007, the TIC initiative has evolved from simply reducing external network connections to protecting agency enterprise perimeters, mobile, and cloud connections with a focus on increasing the use of boundary protection capabilities to protect agency assets from an evolving threat landscape. Over time, higher bandwidth demands, transport encryption, and perimeter services were placed on agency TICs beyond their ability to scale.

Cisco’s security approach for TIC 3.0 is not only designed to fulfill the requirements of distributed policy enforcement points (PEP) in the agency network but is also designed to fit with the relationships between TIC and other federal initiatives such as Continuous Diagnostics and Mitigations (CDM) and the National Institute of Standards and Technology (NIST) Zero trust Architecture.

Zero Trust is a security model that shifts the access conversation from traditional perimeter-based security and instead focuses on secure access to applications based on user identity, the trustworthiness of their device and the security policies you set, as opposed to the network from where access originates. Zero Trust models assume that an attacker is present on the network and that an enterprise-owned network infrastructure is no different. Zero Trust Architecture (ZTA) focuses on three key elements in the network, regardless of their location, securing the workforce, securing the workplace, and securing the workloads.

Figure 1.
Cisco Common Policy Model with SD-WAN & TIC
TIC 3.0 Overview

The purpose of the Trusted Internet Connection (TIC) initiative is to enhance network and perimeter security across the Federal Government. Previously this was done through consolidation of external connections; however, TIC 3.0 provides agencies with increased flexibility to use modern network architecture and frameworks as they adapt to modern architecture and frameworks for government information technology (IT) resource utilization.

Teleworkers require access to resources on the agency campus, agency-sanctioned cloud services, and on the public web. Each of these security patterns presents unique risks and corresponding security capabilities for appropriate use. In mid-March 2020, the Office of Management and Budget (OMB) issued guidance directing agencies to maximize telework across the country for federal workers and extend telework flexibilities to contract workers wherever feasible. The Cybersecurity and Infrastructure Security Agency (CISA) released an update to its TIC program that focuses on the recent surge in federal telework. While the exact numbers aren’t known, it’s clear that thousands of additional federal employees are working from home either full time or part-time.

For existing and new teleworkers, providing appropriate, secure technology and work-from-home policies are essential to enable the business of government at any time and in any place. For employees who are already teleworking, these provisions are already in place. New teleworkers in a crisis situation may not be equipped with government-furnished equipment (GFE) to accomplish remote work. One of the biggest challenges in the current environment is policy preventing the remote workforce from accessing enterprise computing resources using non-GFE. Understandably, agencies need to provide secure access to government networks and ensure employees use secure devices. They also need to tailor access to users’ jobs, so users can access only the resources they need to accomplish their work. Historically, the rule of thumb was that users needed GFE.

CISA, in coordination with the General Services Administration (GSA) and OMB, outlines seven strategic goals to guide the modernization of TIC.

- Boundary-Focused - the expansion into cloud and mobile environments adds new capabilities to support varied security services. TIC 3.0 divides agency architectures by trust zones, shifting emphasis from a strictly physical network perimeter to the boundaries of each zone. This shift is the most fundamental change from legacy TIC.
- Descriptive, Not Prescriptive - one-size-fits-all approach no longer works. The updated reference architecture, capabilities, and use cases will broaden the concepts of the program to accommodate these new environments.
- Risk-Based to Accommodate Varying Risk Tolerances - In cases where additional controls are necessary to manage residual risk, agencies are obligated to apply the control or explore compensating controls that achieve the same protections to manage risks.
- Environment-Agnostic - Every agency is unique, and TIC 3.0 provides the flexibility to manage that.
- Dynamic and Readily Adaptable - innovation moves at a rapid pace, and the TIC Program Management Office (PMO) has designed this initiative to keep up with that.
- Automated and Streamlined Verification - the goal is to define scalable, comprehensive, and continuous validation processes with an automated metric collection as applicable.
- Delineate the NCPS and TIC Initiatives - National Cybersecurity Protection System (NCPS) EINSTEIN and TIC initiatives will continue to support and complement each other.

So as previous versions of TIC focused on a single boundary between an agency and the Internet, TIC 3.0 addresses agencies’ distributed networks to include branch offices, remote users, service providers, and must
continue to be flexible to accommodate additional entities in the future. The generalized architecture in the figure below emphasizes the distributed nature of the agency network.

![Generalized Agency Architecture](image)

**Figure 2.**
Generalized Agency Architecture

TIC 2.2 implemented security by backhauling all data through a single large border between agency network and external network, where all security capabilities such as firewalls, intrusion detection/prevention, web application firewalls, and data loss prevention systems resided. In version 3.0, the inclusion of medium trust zones and distributed PEPs gives agencies the autonomy to implement security capabilities in the most efficient manner for their architecture.

![TIC 2.0 vs. TIC 3.0 architecture changes](image)

**Figure 3.**
TIC 2.0 vs. TIC 3.0 architecture changes

An individual PEP may enforce all of the security capabilities associated with a given trust zone. Some PEPs may only meet a subset of the applicable security capabilities and can be combined with complimentary PEPs to meet all capabilities.
Cisco SAFE Overview

SAFE simplifies end-to-end security by using views of complexity depending on the audience’s needs. Ranging from business flows and their respective threats to the corresponding security capabilities, architectures, and designs, SAFE provides guidance that is holistic and understandable. The SAFE Model organizes the network into logical areas called placed in the network (PIN), simplifying complexity across the enterprise by implementing a model that focuses on the areas that a company must secure. This model treats each area holistically, focusing on today’s threats and the capabilities needed to secure each PIN against those threats. Cisco has deployed, tested, and validated critical designs. These solutions provide guidance and best practices that ensure efficient and secure remote access to the resources.

Figure 4.
The key to SAFE organizes the complexity of holistic security into Places in the Network (PINs) and Secure Domain

This document will use Cisco SAFE to help understand how your business flows through each of the PINs as we move towards adoptions of distributed PEPs in the federal network. Taking an example for one of the locations; the Internet edge is the highest-risk PIN because it is the primary ingress for public traffic and the primary egress point to the Internet. Simultaneously, it is a critical resource that businesses need in today’s Internet-based economy. SAFE matches up defensive capabilities against the categories of threats today simplifies security by starting with business flows and then addressing their respective threats with corresponding security capabilities, architectures, and designs. SAFE provides guidance that is holistic and understandable.
More information about how Cisco SAFE simplifies security, along with this and other Cisco Validated Designs (CVD), can be found here: www.cisco.com/go/safe.
Business Flows

SAFE uses the concept of business flows to simplify the identification of threats. Using business flows enables the selection of capabilities necessary to protect them. The PINs that have been highlighted by CISA include remote users, branch offices, traditional TIC (campus), and cloud (Software as a Service (SaaS) / Infrastructure as a Service (IaaS) / Platform as a Service (PaaS)). This document will focus on the remote worker use case. Although treated as separate entities, it is important the security capabilities in each of the use cases and PEPs are integrated as one holistic security platform for best performance and ease of management.

As federal civilian agencies respond to the COVID-19 situation, the number of federal agency employees working from remote locations has increased dramatically. To support agencies as they respond to this surge in teleworking, CISA has issued this interim TIC guidance to help agencies leverage existing resources to secure their networks. The solutions outlined in this document will be catered towards this interim guidance and updated accordingly when the full use case has been released.

The interim use case focuses on how security should be applied when communication occurs between a remote user and agency-sanctioned cloud services. Teleworker communications with agency hosted resources and web entities should continue to follow agency protections. TIC 3.0’s Traditional TIC use case enumerates the TIC protections for agency campus. For more information go to https://www.cisco.com/c/dam/en/us/solutions/collateral/design-zone/cisco-validated-profiles/secure-dc-design-guide-cvd.pdf

This document will focus on four key business flows;

- Securing employees accessing internet resources
- Securing employees accessing trusted external partner applications
- Securing employee accessing an application hosted on the agency campus
- Securing email communications. Email security is called out as a security capability required in the overall TIC architecture, and while the details of its deployment are out of scope for this document, more information on its application and deployment can be found at cisco.com/go/emailsecurity.

In addition, the use of Unified Communications and Collaboration (UCC) tools will be reviewed, and Cisco’s solution for secure collaboration will be presented.
Figure 6.
Remote User Business flows
Attack Surface

The TIC 3.0 solution protects systems by applying security controls to the attack surface found across the distributed PINs. The attack surface spans the business flows used by humans, devices, networks, and the cloud. Agency networks typically have many employees, partners and guest users who use email, browse the web, and collaborate, regardless of location. The remote user use case focuses on six primary threats;

- **Phishing** – social engineering to trick people into clicking on a malicious link or opening an infected attachment of an email. Messages will look as if they are from a legitimate organization, usually a financial institution, but contains a link to a fake website that replicates the real one.

- **Unauthorized network access** – act of gaining access to a network, system, application or other resource without permission. The attacker could cause damage in many ways, perhaps by accessing sensitive files from a host, by planting a virus, or by hindering network performance by flooding your network with illegitimate packets.

- **Malware propagation** – devices present in the network are a significant source of contamination. Devices of employees, partners, or customers can be infected from multiple sources such as web use, email use, or lateral infection from other devices on the network. Devices accepting credit cards and the Internet of Things (IoT) are common attack points.

- **Web-based exploits** – malvertizing and compromised sites hosting exploit kits to take over employee devices using browser vulnerabilities.

- **Bring Your Own Device (BYOD)** – non-managed devices can roam enterprise network which increases chances of compromise and the spread of infection. The large variety of mobile devices makes security policies and posture checking almost impossible when no device standardization exists. Limited on-device security capabilities (e.g., firewall, anti-malware, browser sandboxing).

- **Botnet infestation** – networks made up of remote-controlled computers, or bots. These computers have been infected with an advanced form of malware which allows the devices to be remotely controlled. The controller of a botnet is able to direct the activities of these compromised computers to perform other attacks, steal data, or send spam.
Figure 7.
Attack Surface
Security Capabilities

The TIC 3.0 reference architecture breaks out capabilities into two parts. The first covers the foundational enterprise-level capabilities that outline the guiding principles for TIC use cases. Agencies have the discretion to determine the level of rigor necessary for applying universal capabilities based on federal guidelines and risk tolerance.

**Figure 8.**
TIC 3.0 Universal Capabilities

The second part is the individual PEP capabilities. These are network-level capabilities that inform technical implementation for relevant use cases.

**Figure 9.**
PEP Capabilities

Volume 4 of the TIC documentation released by CISA is a use case handbook that outlines which security controls, such as endpoint and user-based protection, should be put in place for use cases that have been successfully piloted or otherwise vetted by CISA. The interim teleworker guidance is composed of four trust
zones – agency teleworker, agency campus, web, and external partner. The figure below depicts the security capabilities that CISA deems essential for securing the use case appropriately.

**Figure 10.**
PEP Capabilities for Remote User use case

The interim teleworker guide has added in two additional PEPs that have not yet been called out in TIC; Unified Communications and Collaboration along side Data protection. COVID-19 restrictions require more and more people to telework, which in turn creates an influx of virtual meetings. Participants need to exercise caution and awareness of the content they are sharing to ensure that only authorized content is shared. Furthermore, the surge in telework requires agencies to have processes and tools in place to protect agency data, prevent data exfiltration, and ensure the privacy and integrity of data, considering that data may be accessed from devices beyond the protections and perhaps administration of agencies. Data protection capabilities must be considered and may be adapted for data stored and accessed at sanctioned agency cloud services on agency-owned devices, as well as on remote devices that are not owned by an agency.
Architecture Overview

Beginning with the first three flows for the remote worker, focusing on how they can securely connect to the applications in a trusted cloud, web, or agency campus. The first option is a direct connection from the user to a sanctioned cloud service or web site. Strict identity verification and security policy adherence will be implemented for every person and device trying to access resources. If the traffic is destined for a CSP, additional cloud protections in the form of a cloud access security broker (CASB) will ensure only authorized services and information is being exchanged.

Figure 11.
Direct connection to sanctioned cloud service or the web

The second option is to use the agency campus as an intermediary traffic forwarding step. A virtual private network (VPN) extends a corporate network through encrypted connections made over the Internet. Since the traffic is encrypted between the device and the network, traffic remains private as it travels. An employee can work outside the office and still securely connect to the corporate network. Advances in VPN technology have allowed security checks to be conducted on endpoints to make sure they meet a certain posture before connecting, ensuring that devices are up to date and contain no malicious files before being granted access to the corporate network.

As cloud environments play a larger role in agency operations, they offer value, including flexibility, agility and reduced costs. At the same time, agencies have many data center assets that they can’t move to the cloud. Some applications can’t be easily migrated, and other data may be subject to regulatory requirements that prevent that data from residing in public clouds. As a result, companies often pursue a hybrid cloud architecture, where some data and applications reside in agencies’ own data centers and some data and apps reside in public clouds. VPN’s play a key role in protecting both the user and the on prem assets, but there are cases where it becomes inefficient to backhaul traffic that is destined for trusted cloud applications. This behavior can be achieved using split-tunneling.

As the work-from-home trend grows due to the COVID-19 pandemic, the increased traffic puts more stress on enterprise VPN infrastructure, but one of the most effective ways to ease that stress is split tunneling. The
default behavior of a VPN client is to tunnel all traffic. The client sends everything through the tunnel unless a split tunnel is defined. Split tunnels can be implemented in two ways.

- Static split tunneling involves defining the IP addresses of hosts and networks that should be included in or excluded from the remote access VPN tunnel.

- Dynamic split tunneling is based on DNS domain names. Since the IP addresses associated with fully-qualified domain names (FQDN) can change or simply differ based on region, defining split tunneling based on DNS names provides a more dynamic definition of which traffic should, or should not, be included in the remote access VPN tunnel.

Split tunneling is useful when using trusted applications such as Cisco WebEx, salesforce, and office365 on the public Internet, freeing bandwidth in your VPN tunnel, and giving remote workers better performance using their everyday applications. Unknown or untrusted destinations can then continue to use the VPN tunnel, undergoing the extensive security checks that have been deployed at the agency, while reducing the load.

Figure 12.
Connect via Agency Campus to sanctioned cloud service or web

The final option CISA have proposed is to have an intermediary step in the cloud. Similar to backhauling data to an agency campus, traffic will be forwarded to a Secure Internet Gateway (SIG), where a security stack similar to that found on the campus would reside.
Figure 13.
Connect via Secure Internet Gateway (SIG) to sanctioned cloud service or web
Solution Overview

Cisco’s security approach for TIC 3.0 is not only designed to fulfill the requirements of distributed PEPs in the agency network but is also designed to fit with the relationships between TIC and other federal initiatives such as Continuous Diagnostics and Mitigations (CDM) and the National Institute of Standards and Technology (NIST) Zero trust Architecture. Zero Trust is a security model that shifts the access conversation from traditional perimeter-based security and instead focuses on secure access to applications based on user identity, the trustworthiness of their device, and the security policies you set, regardless of the network the user resides. Zero Trust models assume that an attacker is present on the network and that an enterprise-owned network infrastructure is no different. Zero Trust Architecture (ZTA) focuses on three key elements in the network, regardless of their location; securing the workforce, securing the workplace, and securing the workloads.

Securing the Workforce

In the past, enabling secure bring your own device (BYOD) programs required the installation of an agent or a client like mobile device management (MDM). That provided agency visibility into activity on BYOD devices, but at the cost of personal privacy. Employees were reluctant to sign up for BYOD with MDM. Now, low-cost, software-agnostic alternatives are available that do not compromise personal privacy and do not require rip and replacement of legacy systems. Duo Security offers solutions that enable secure BYOD with a Zero-Trust model, which establishes trust for every access request, regardless of device or location. Duo’s two FedRAMP-Authorized editions deliver strong cloud-based authentication and device visibility to ensure only trusted users and devices can access protected applications. For critical agency applications, it can require that the device is part of the Government-Furnished Equipment (GFE) fleet of equipment. Duo Federal MFA offers agencies easy-to-use, federal-grade two-factor authentication that protects and verifies user identities before allowing access to agency applications. Duo Federal Access adds unified endpoint visibility, which includes stronger role-based and location-based access policies, as well as biometric authentication enforcement – allowing or denying access based on device hygiene and notifying users to self-remediate out-of-date devices. These solutions align with FedRAMP/NIST 800-53 security controls, the NIST Digital Identity Guidelines (SP 800-63-3), and Federal Information Processing Standard (FIPS) 140-2 compliance requirements for federal organizations.

Securing the workforce is not only limited to identifying the users, but also ensuring that their devices have not been compromised - a weak point for malware to enter the network. Cisco Advanced Malware Protection (AMP) for Endpoints integrates prevention, detection, and response capabilities in a single solution, leveraging the power of cloud-based analytics. In the rapidly evolving world of malware, threats are becoming harder and harder to detect. The most advanced 1% of these threats, those that will eventually enter and wreak havoc in your network, could potentially go undetected. However, AMP for Endpoints provides comprehensive protection against that 1%. AMP is underpinned by the advanced threat intelligence from Talos, an industry-leading threat intelligence team, comprised of world-class researchers, analysts, and engineers. Industry-leading visibility, actionable intelligence, and vulnerability research drive rapid detection and protection for Cisco customers.

Securing the Workplace

Network access control (NAC), forms the foundation of a Zero-Trust implementation. In a Zero-Trust network, any exploitable device has to be shielded or segmented to reduce the likelihood of a criminal finding and exploiting the device. Moreover, the remaining devices have to be protected from other compromised and exploited devices. Effective security requires a known inventory of the entities using the network, and visibility into the security posture of the devices. The access control decision occurs when equipment attempts to connect to the network. Traditionally, network engineers accomplished this with fixed attributes such as a combination of network switch location or IP address. IP and location based policies will inherently trust the equipment without knowing whether the equipment is vulnerable or exploited. The traditional trust is also based on easily spoofable attributes. When moving to Zero Trust, the decision must be made on a number of factors, including identity and behavior, and it must be verified regularly based on device behavior and any changing factors. In particular, the organization must be able to respond to newly discovered threats and vulnerabilities by limiting the original network access or cutting it off altogether. On-prem network protections are out of scope for this remote user document.

Securing the workplace typically means keeping your network safe while users traverse it. In the case of the teleworker, you are no longer trying to secure the workplace, but ensure the user is secure as they traverse this, now public, workspace. The industry-leading AnyConnect Secure Mobility Client is a modular endpoint software product. It not only provides VPN access through Secure Sockets Layer (SSL) and IPsec IKEv2 but also offers enhanced security through various built-in modules. These modules provide services such as compliance through the VPN with ASA, network visibility into endpoint flows within Stealthwatch or off-network roaming protection with Cisco Umbrella. AnyConnect clients are available across a broad set of platforms, including Windows, macOS, Linux, iOS, Android, Windows Phone/Mobile, BlackBerry, and ChromeOS.

Cisco AnyConnect incorporates the Cisco Common Cryptographic Module (C3M). This Cisco SSL implementation includes FIPS 140-2 compliant cryptography modules and National Security Agency (NSA) Suite B cryptography as part of its Next Generation Encryption (NGE) algorithms. NGE introduces new encryption, authentication, digital signatures, and key exchange algorithms for escalating security and performance requirements. RFC 6379 defines the Suite B cryptography algorithms conform to meet U.S. FIPS 140-2 standards.

Cisco AnyConnect’s Always-On operation prevents access to Internet resources when the computer is not on a trusted network unless a VPN session is active. Enforcing the VPN to always be on in this situation protects the user from security threats posed by public internet. When Always-On is enabled, it establishes a VPN session automatically after the user logs in and upon the detection of an untrusted network. Nonetheless, this will not interfere with split tunneling; any traffic destined to a trusted destination will be forwarded directly to its destination. The VPN session remains open until the user logs out of the computer, or the session timer or idle session timer (specified in the ASA group policy) expires. AnyConnect continually attempts to re-establish the connection to reactivate the session if it is still open; otherwise, it continuously attempts to establish a new VPN
session. When Always-On is enabled in the VPN Profile, AnyConnect protects the endpoint by deleting all the other downloaded AnyConnect profiles and ignores any public proxies configured to connect to the ASA.

The Cisco Umbrella Roaming Security module for Cisco AnyConnect Mobility Client enforces security at the DNS layer to block malware, phishing, and command and control callbacks over any port. Umbrella provides real-time visibility into all internet activity per hostname (and optionally AD username) both on and off your network or VPN. The client may optionally be disabled on the network to defer to on network settings. The roaming module allows for full update control, and an option to disable automatically behind a full tunnel VPN connection. For off-net roaming, Umbrella will provide real-time visibility into all of the internet activity originating from the teleworker.

**Secure the Workloads**

At its core, zero trust is about access to applications. All applications. Establishing user identity and device trust set the table for seamless and secure access to applications – on-premises or in the cloud – with no discernible difference. Zero Trust for Workloads addresses several important risks for the enterprise:

- An attacker exploiting application vulnerabilities can move laterally to compromise critical systems.
- An attacker obtaining sensitive data and exfiltrating the data out of the network.
- Disparate controls between internal applications and external cloud-based applications creating blind spots for defenders.

For bootstrapping existing environments into Zero-Trust models, the network must evaluate trust and make access control decisions at the point of network communication. This is no simple feat considering our application services often spread across cloud service providers, data centers, and other heterogeneous virtualized environments. An application ecosystem is defined to contain only the application’s dependencies: services, processes, and network communications. Access control can then be applied using an allowlist or default-deny, such that only what the application requires is permitted regardless of the network or environment. Trust should be defined by the application requirements, rather than the network location.

The Cisco Tetration platform enables holistic workload protection for multi-cloud data centers by using:

- AllowList-based segmentation, allowing operators to control network communication within the data center, enabling a Zero-Trust model
- Behavior baselining, analysis, and identification of deviations for processes running on servers
- Detection of common vulnerabilities and exposures associated with the software packages installed on servers
- The ability to act proactively, such as quarantining server(s) when vulnerabilities are detected and blocking communication when policy violations are detected.

validated-profiles/secure-dc-design-guide-cvd.pdf where Tetration is used to protect the agency campus, and any connections, including remote users, that reach out to use its services.

Cisco protects SaaS based applications in the form of a Cloud Access Security Broker (CASB). Cisco Cloudlock is a cloud-native CASB that secures your cloud identities, data, and apps that enables compliance and improved productivity. Cisco Cloudlock is a simple, open, and automated solution that combats cloud account compromises, data breaches, and cloud app ecosystem risks, by providing actionable cybersecurity intelligence. Key benefits include:

- **Defend against cyber threats** – provides protection against account compromise with cross-platform User and Entity Behavior Analytics (UEBA). Cloudlock also detects activities outside of whitelisted countries and actions performed across distances in an impossible amount of time.
- **Manage compliance in the cloud** – enforce compliance through out-of-the-box policies designed for PCI-DSS, SOX, and other compliance-specific information & tailor policies to proprietary concerns, such as intellectual property through our highly configurable policy engine.
- **Enrich existing security investments** – complement Cisco Cloudlock’s UEBA with automated response actions such as requiring MFA (such as Cisco’s DUO), restricting application access, and reducing maximum session length. Also, aggregate on-premises logs with Cisco Cloudlock app risk insight for superior Shadow IT visibility.
- **Protect sensitive information** – pinpoint excessively exposed sensitive information within cloud environments based on defined content or exposure criteria & users can enforce automated, contextual policy-driven response actions.

**Complete network visibility**

Up to this point, we have mostly spoken about inline protections and the security practices we can employ to establish trust in the network. However, out of band monitoring can be a useful tool in detecting deviations in the network norm and comparing active flows against known malware signatures to detect malicious activity such as data hoarding or denial-of-service. NIST has identified that a strong CDM program implementation is key to the success of ZTA. The third phase of CDM – *Network Security Management "what is happening on the network?"* – requires the management of network and perimeter components, host and device components, data at rest and in transit, and user behavior and activities. This includes management of events (MNGEVT); operate, monitor, and improve (OMI); design and build-in security (DBS); boundary protection (BOUND); supply chain risk management (SCRM); and ongoing authorization.

Visibility across the network and connected devices is achieved via several methods. Within the enterprise, each capability provides an increasing breadth of visibility and context. They provide visibility and security intelligence across an entire organization before, during, and after an attack. Cisco Stealthwatch™ provides continuous real-time monitoring of, and pervasive views into, all network traffic. It dramatically improves visibility across the extended network and accelerates response times for suspicious incidents. It creates a baseline of normal web and network activity for a network host and applies context-aware analysis to automatically detect anomalous
behaviors. Stealthwatch™ 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.

Stealthwatch™ dramatically improves:

- Real-time threat detection
- Incident response and forensics
- Network segmentation
- Network performance and capacity planning
- Ability to satisfy regulatory requirements

For more information on Stealthwatch, refer to https://cisco.com/go/stealthwatch.

Figure 14.
Anyconnect with Network Visibility Module

Many networks would benefit from offloading remote worker traffic from their VPN infrastructure. Improving VPN throughput, and the network performance users. Offloading specific types of traffic (like Office365, WebEx and other SaaS applications) to a VPN split-tunnel that manages traffic directly to its destination split tunneling disadvantage include a lack of visibility into the traffic being split off. Networks may need to offload more traffic than the obvious SaaS services to maintain acceptable end-user performance. However, deciding what is safe to move to a split-tunnel is a challenge without detailed visibility into what types of traffic the VPN endpoints are generating. The Network Visibility Module was introduced with the release of AnyConnect 4.2 and is intended to help solve this issue. As users gain the ability to do their work anywhere outside of the office, administrators find it harder and harder to plan for capacity and service and to provide auditing, and ensure compliance. This new model of work can cause blind spots for the administrator as security implementations become more complex and difficult. AnyConnect with NVM is the solution to overcome these blind spots and provides even more visibility, including application visibility. NVM is essentially NetFlow for the endpoint, and under the hood is the Cisco nvzFlow protocol, an add-on to the IPFIX protocol, which itself is based on Cisco NetFlow version 9. Cisco nvzFlow allows NVM to give the administrator information based on the following 5 key visibility categories;

- User
- Device
- Application
- Destination
For more information about AnyConnect and the NVM module, please visit: https://www.cisco.com/go/anyconnect

Got Splunk?
AnyConnect and Splunk are the infrastructures for Cisco Endpoint Security Analytics (CESA), which provides the monitoring and security analytics to address the lack of visibility in a split tunnel deployment. With many IT orgs resistant to deploying any new infrastructure, CESA allows IT to use what they already have deployed to gain the VPN, Zero-Trust, and remote work endpoint visibility they seek. CESA also uses the highly detailed traffic telemetry from AnyConnect VPN clients. The outcome of this visibility? IT orgs can now identify what traffic is safe to put into a split VPN tunnel to optimize VPN throughput capacity. Furthermore, we mentioned AnyConnect’s ability to enable dynamic split tunneling, which makes it easy to direct split-tunnel traffic by domain name (e.g., put all “*webex*.cisco.com” into the split tunnel). Dynamic Split Tunneling analytics is also supported in CESA, addressing endpoint security use cases such as;

- Data loss detection
- Day-zero malware and threat hunting
- Zero-Trust monitoring
- Unapproved applications and SaaS visibility
- Security evasion and user attribution
- Asset inventory

Cisco Unified Communications Manager (UCM) Cloud for Government

![Cisco UCM Cloud for Government](image)

Figure 15. Cisco UCM Cloud for Government

Telework often requires virtual meetings, and the interim guidance for remote workers requires UCC services that offer protections appropriate to the content to be shared. Cisco UCM Cloud for Government unites Cisco’s industry-leading collaboration services (voice, video, instant messaging, presence, mobility, and conferencing) from the Cisco cloud, with built-in U.S. government-level security to give agencies the power to collaborate
securely with anyone, anywhere. Cisco UCM gives each user the right tools for their job; from administrators and thought leaders, to production and field personnel, and beyond.

With Cisco UCM Cloud for Government, your team benefits from a one service, one experience for everyone solution that is Federal Risk and Authorization Management Program (FedRAMP) authorized to better protect your agency’s data and privacy.

- **Dedicated deployments**: sensitive data is securely contained in U.S. data centers, which are accessible by U.S. citizens only. Separate deployments for each customer for added separation of agency data.

- **End-to-end encryption**: FIPS 140-2 validated cryptography for secure communications.

- **Constantly monitored**: Continuous scanning against a database of current global security vulnerabilities.

- **Application-based policy enforcement and management**: Configurations and user roles are set on the per-application level. Policies follow users as they roam networks. Customize, manage, and enforce usage features.

- **Government-defined architecture and SLAs**: The architecture based on FedRAMP security requirements. U.S. government-defined Service-Level Agreements (SLAs) are used to resolve security events.

- **Third-party reviews and audits upon FedRAMP authorization**: Regularly audited by an independent FedRAMP third-party assessment organization. Monthly reviews of security stature with sponsoring agency.