Trusted Internet Connections (TIC) 3.0

Architecture Guide

October 2021

Contents

Trusted Internet Connections (TIC) 3.0

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

Cybersecurity and Infrastructure Security Agency (CISA), in coordination with the General Services Administration (GSA) and Office of Management and Budget (OMB), outline seven strategic goals to guide the modernization of TIC.

- Boundary-Focused - the expansion into the cloud and mobile environments bring new capabilities to support diverse 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

While previous iterations 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, and 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.

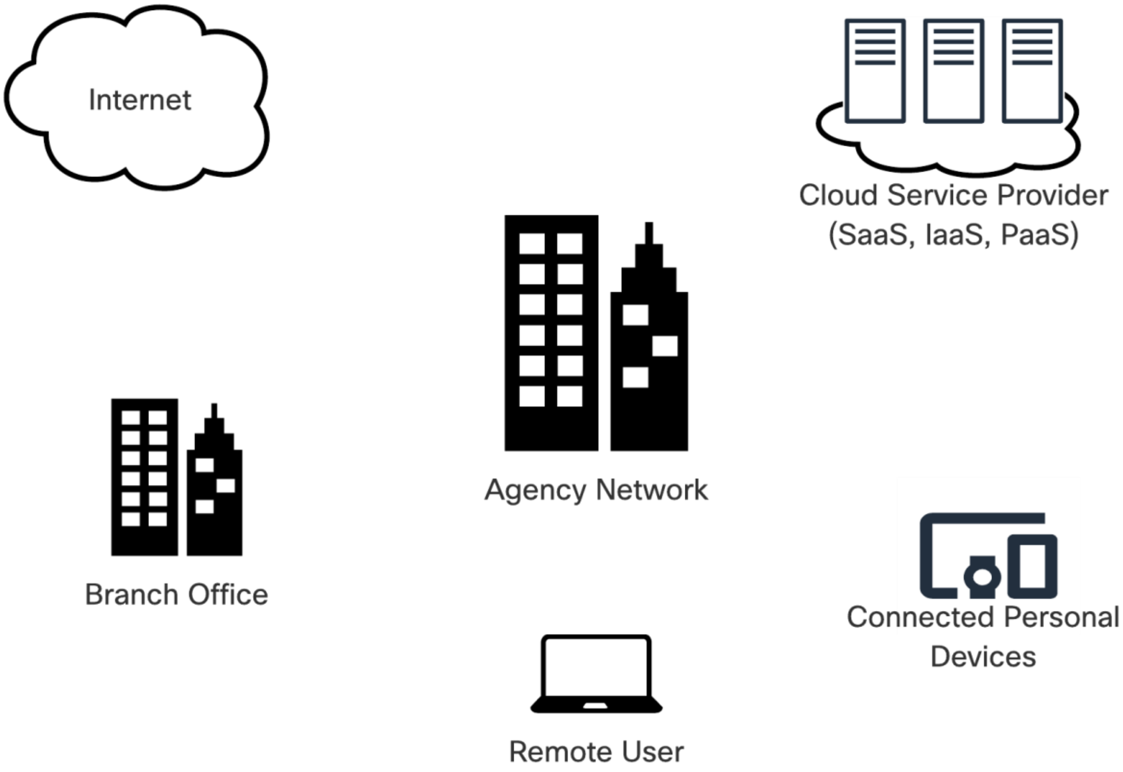

Internet
Cloud Service Provider (SaaS, IaaS, PaaS)
Agency Network
Branch Office
Connected Personal Devices
Remote User

Figure 1.
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 most effectively for their architecture.

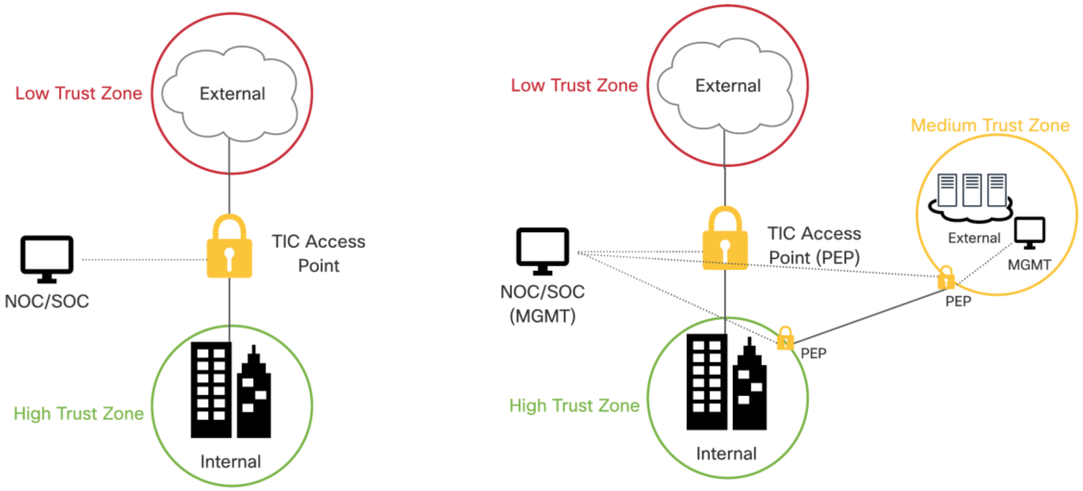


Figure 2.
TIC 2.0 vs. TIC 3.0 architecture changes

The update to TIC 3.0 introduces new concepts, capabilities, and approaches that established a foundation for network security. A fundamental change calls for TIC use cases to support multiple security approaches that focus on protecting agency data transmitted and stored beyond agency network boundaries. The use cases demonstrate scenarios that accommodate a distributed deployment of TIC capabilities across multiple PEPs, in addition to, or instead of, deployment of a single TIC PEP implementation for external connections. To meet this objective, CISA releases a security capabilities list comprising of universal security capabilities that outline the guiding principles for TIC use cases and then specific PEP capabilities that inform technical implementation for each part of the network.

Cisco SAFE

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 places in the network (PINs), simplifying complexity across the enterprise by implementing a model that focuses on the areas that a company must secure. Comparable to the TIC 3.0 security capability documentation, this model treats each area holistically, focusing on today’s threats and the capabilities needed to secure each PIN against those threats.

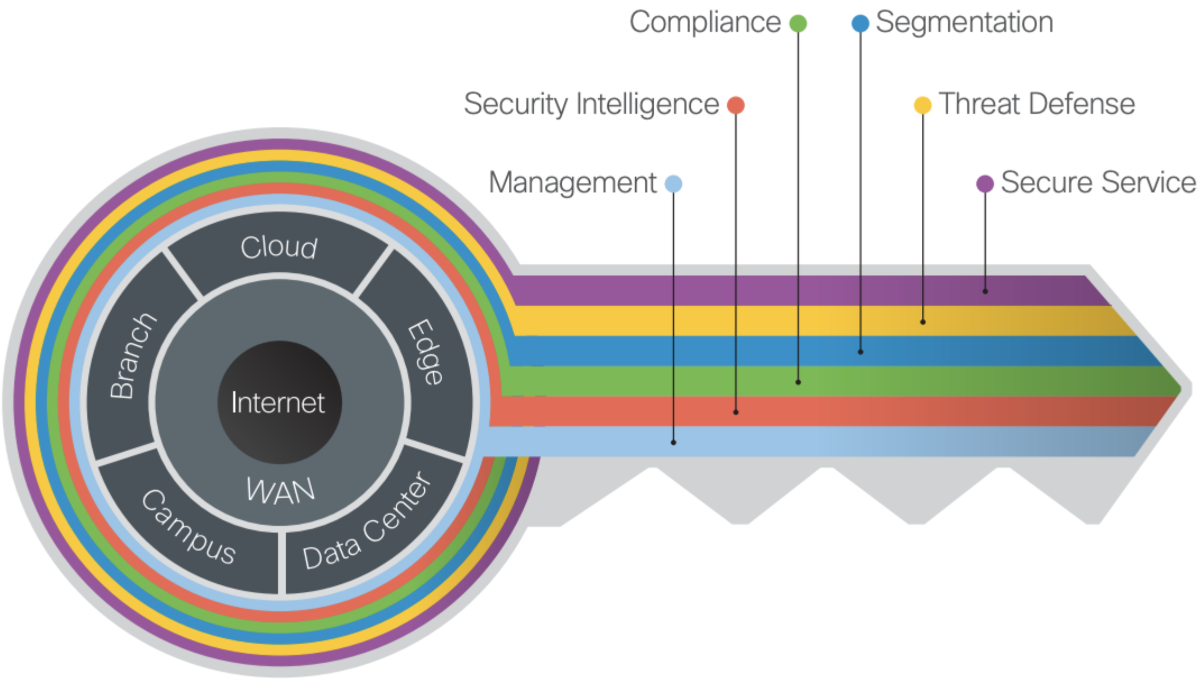


Figure 3.
The key to SAFE organizes the complexity of holistic security into PINs

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 today’s threats and 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.

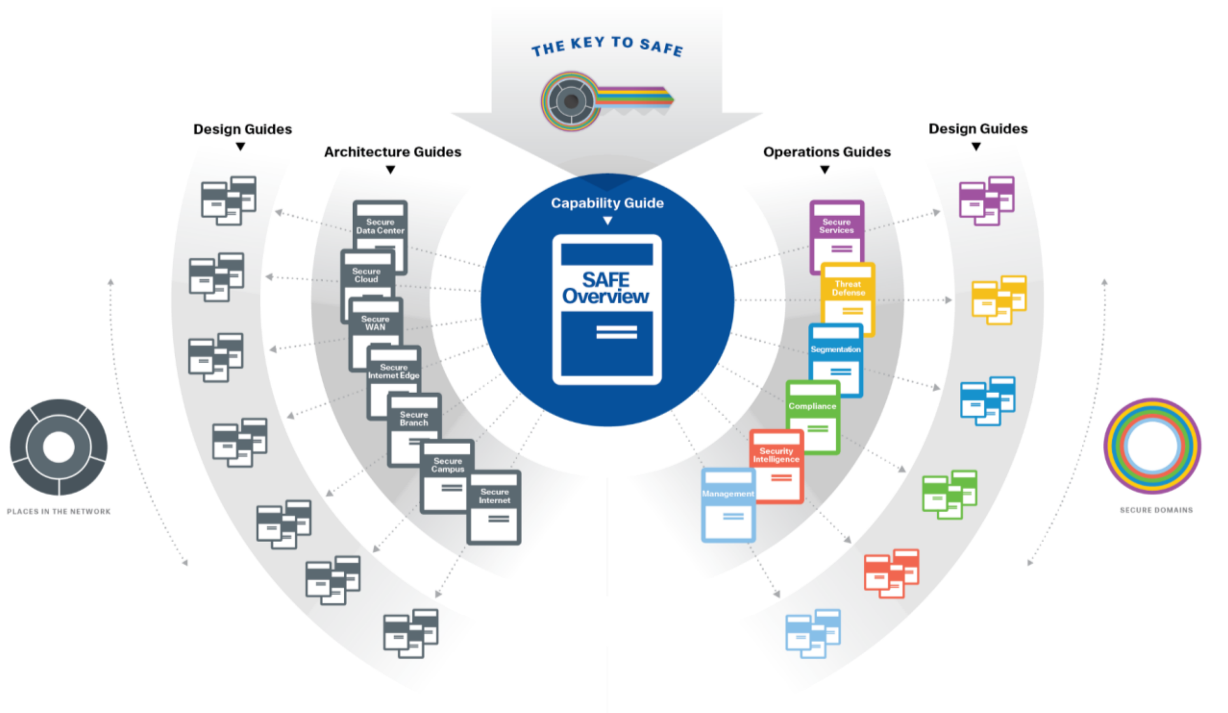


Figure 4.
SAFE Architecture and Design Guides

More information about how Cisco SAFE simplifies security, along with this and other Cisco Validated Designs (CVD), can be found here: https://www.cisco.com/go/safe.

TIC 3.0 Security Capability Requirements

In this section the capabilities outlined in volume 3 of the TIC 3.0 guidance will be mapped to a SAFE icon for further use in the document. Not all capabilities listed here will map specifically to a product in the architecture, with some features being guiding principles when designing a security architecture.

Universal Capabilities

SAFE Icon	Cisco Offered	Capability	Description
📥	✓	**Backup and Recovery**	Keep copy of configuration and data to allow for quick restoration of service in the event of malicious incidents, system failures, or corruption.
SIEM	✓	**Central Log Management with Analysis**	Collecting, storing, and analyzing telemetry to aid in discovery and response to malicious activity.
📋	✓	**Configuration Management**	Implementing a formal plan for documenting and managing changes to an environment.

SAFE Icon	Cisco Offered	Capability	Description
	✓	**Incident Response Plan and Incident Handling**	Documenting and implementing a set of instructions, procedures, or technical capabilities to sense and detect, respond to, limit consequences of malicious cyberattacks, and restore the integrity of the network and associated systems.
	✓	**Inventory**	Developing, documenting, and maintaining a current inventory of all systems, networks, and components so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.
	✓	**Least Privilege**	Designing the security architecture such that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.
	✓	**Secure Administration**	Performing administrative tasks in a secure manner, using secure protocols.
	✓	**Strong Authentication**	Verifying the identity of users, devices, or other entities through rigorous means (e.g. multi-factor authentication) before granting access.
	✓	**Time Synchronization**	Coordinating clocks on all systems (e.g. servers, workstations, network devices) to enable accurate comparison of timestamps between systems.
	✓	**Vulnerability Management**	Proactively working to discover vulnerabilities, including the use of both active and passive means of discovery, and taking action to mitigate discovered vulnerabilities.
	✓	**Patch Management**	Identifying, acquiring, installing, and verifying patches for products and systems.
	✓	**Auditing and Accounting**	Capturing business records, including logs and other telemetry, and making them available for auditing and accounting as required.
	✓	**Resilience**	Ensuring that systems, services, and protections maintain acceptable performance under adverse conditions.

SAFE Icon	Cisco Offered	Capability	Description
	✓	**Enterprise Threat Intelligence**	Obtaining threat intelligence from private and government sources and implementing mitigations for the identified risks.
	✓	**Situational Awareness**	Maintaining effective awareness, both current and historical, across all components.
	✓	**Dynamic Threat Discovery**	Using dynamic approaches to discover new malicious activity.
	✓	**Policy Enforcement Parity**	Consistently applying security protections and other policies, independent of the communication mechanism.
	✓	**Effective Use of Shared Services**	Employing shared services, where applicable, that can be individually tailored, measured to independently validate service conformance, and offer effective protections for tenants against malicious actors.
	✓	**Integrated Desktop, Mobile, and Remote Policies**	Defining policies such that they apply to a given agency entity no matter its locations.

PEP Security Capabilities

The published documentation, which can be found here, lists ten different policy enforcement points in the network. While Cisco do have solutions for solutions such as Email and Unified Communications and Collaboration (UCC), they will be out of scope for this documentation. This guide will focus its attention to the security capabilities in the PEPs below.

File PEP Security Capabilities

SAFE Icon	Cisco Offered	Capability	Description
	✓	**Anti-malware**	Anti-malware protections detect the presence of malicious code and facilitate its quarantine or removal.
	—	**Content Disarm & Reconstruction**	Content disarm and reconstruction technology detects the presence of unapproved active content and facilitates its removal.

SAFE Icon	Cisco Offered	Capability	Description
	✓	**Detonation Chamber**	Detonation chambers facilitate the detection of malicious code through the use of protected and isolated execution environments to analyze the files.
DLP	✓	**Data Loss Prevention**	Data loss prevention technologies detect instances of the exfiltration, either malicious or accidental, of agency data.

Web PEP Capabilities

SAFE Icon	Cisco Offered	Capability	Description
	✓	**Break and Inspect**	Terminate encrypted traffic, logging or performing policy enforcement against the plaintext, and re-encrypting the traffic, if applicable, before transmitting to the final destination.
	✓	**Active Content Mitigation**	Detect the presence of unapproved active content and facilitate its removal.
	✓	**Certificate Denylisting**	Prevent communication with entities that use a set of known bad certificates.
	✓	**Content Filtering**	Detect the presence of unapproved content and facilitate its removal or denial of access.
	✓	**Authenticated Proxy**	Require entities to authenticate with the proxy before making use of it, enabling user, group, and location aware security controls.
DLP	✓	**Data Loss Prevention**	Detect instances of the exfiltration, either malicious or accidental, of agency data.
DNS	✓	**DNS-over-HTTPS Filtering**	Prevents entities from using the DNS-over-HTTPS protocol, possibly evading DNS-based protections.
	✓	**RFC Compliance Enforcement**	Ensure that traffic complies with protocol definitions.
	✓	**Domain Category Filtering**	Allow for classes of domains (e.g. banking, medical) to receive a different set of security protections.

SAFE Icon	Cisco Offered	Capability	Description
	✓	**Domain Reputation Filter**	Form of domain Denylisting based on a domain's reputation, as defined by either the agency or an external entity.
	✓	**Bandwidth Control**	Limiting the amount of bandwidth used by different classes of domains.
	✓	**Malicious Content Filtering**	Detect the presence of malicious content and facilitate its removal.
	✓	**Access Control**	Allow an agency to define policies limiting what actions may be performed by connected users and entities.

Networking PEP Capabilities

SAFE Icon	Cisco Offered	Capability	Description
	✓	**Access Control**	Prevent the ingest, egress, or transiting of unauthorized network traffic.
	✓	**IP Denylisting**	Prevent the ingest or transiting of traffic received from or destined to a deny listed IP address.
	✓	**Host Containment**	Enable a network to revoke or quarantine a host's access to the network.
	✓	**Network Segmentation**	Separates a given network into subnetworks, facilitating security controls between the subnetworks, and decreasing the attack surface of the network.
	✓	**Microsegmentation**	Divides the network, either physically or virtually, according to the communication needs of application and data workflows, facilitating security controls to protect the data.

DNS PEP Capabilities

SAFE Icon	Cisco Offered	Capability	Description
DNS	✓	**DNS Sinkholing**	A form of Denylisting that protect clients from accessing malicious domains by responding to DNS queries for those domains.

SAFE Icon	Cisco Offered	Capability	Description
DNS	✓	**DNNSEC for Agency Clients**	Ensure that domain name lookups from agency clients, whether for internal or external domains, are validated.
DNS	✓	**DNNSEC for Agency Domains**	Ensure that all agency domain names are secured using DNSSEC, enabling external entities to validate their resolution the domain names.
DNS	✓	**NCPS E^3A DNS Protections**	Intrusion prevention capability, provided by DHS, that includes a DNS Sinkholing security service.

Intrusion Detection PEP Capabilities

SAFE Icon	Cisco Offered	Capability	Description
	✓	**Endpoint Detection and Response**	Combine endpoint and network event data to aid in the detection of malicious activity.
	✓	**Intrusion Protection Systems (IPS)**	Detect malicious activity, attempt to stop the activity, and report the activity.
	✓	**Adaptive Access Control**	Factor in additional context, like security risk, operational needs, and other heuristics, when evaluating access control decisions.
	−	**Deception Platforms**	Provide decoy environments, from individual machines to entire networks, that can be used to deflect attacks away from the operational systems supporting agency missions/business functions.
	✗	**Certificate Transparency Log Monitoring**	Allows agencies to discover when new certificates are issued for agency domains.

Enterprise PEP Capabilities

SAFE Icon	Cisco Offered	Capability	Description
SIEM	✗	**Security Orchestration Automation, and Response (SOAR)**	Define, prioritize, and automate the response to security incidents.
	✓	**Shadow IT Detection**	Detect the presence of unauthorized software and systems in use by an agency.

SAFE Icon	Cisco Offered	Capability	Description
	✓	**Virtual Private Network (VPN)**	Provide a secure communications mechanism between networks that may traverse across unprotected or public networks.

Data Protection PEP Capabilities

SAFE Icon	Cisco Offered	Capability	Description
	✓	**Access Control**	Allow an agency to define policies concerning the allowable activities of users and entities to data and resources.
	✓	**Protections for Data at Rest**	Secure data stored on any device or storage medium.
	✓	**Protections for Data in Transit**	Secure data that is actively moving from one location to another, such as across the internet or through a private enterprise network.
DLP	✓	**Data Loss Prevention**	Detect instances of the exfiltration, either malicious or accidental, of agency data.
	✓	**Data Access and Use Telemetry**	Identify agency sensitive data stored, processed, or transmitted, including those located at a service provider. Enforce detailed logging for access or changes to sensitive data.

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. This is comparable to the fourth volume released by CISA, detailing use case architectures where these security capabilities apply. 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)).

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.

This document will focus on three 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

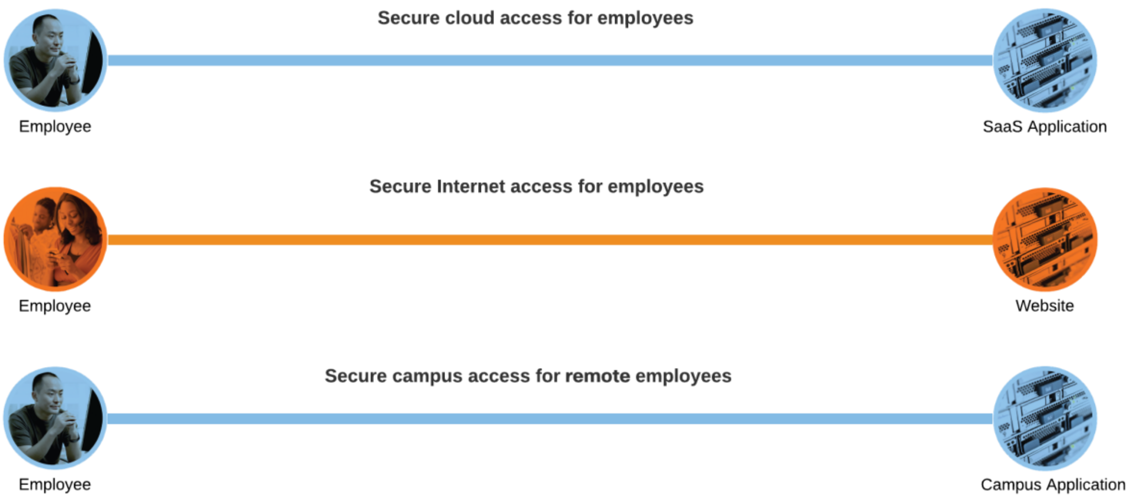

Secure cloud access for employees
Employee
SaaS Application
Secure Internet access for employees
Employee
Website
Secure campus access for remote employees
Employee
Campus Application

Figure 5.
TIC 3.0 Business flows

Securing employees accessing internet resources

TIC documentation refers to the Internet in two capacities:

- A mean of data and IT traffic transport
- An environment used for web browsing purposes, otherwise known as the “web”

This use case refers to the latter, where traffic originating from an agency location or device would like to access the web, and the application or service being accessed is not known or initially trusted by the agency.

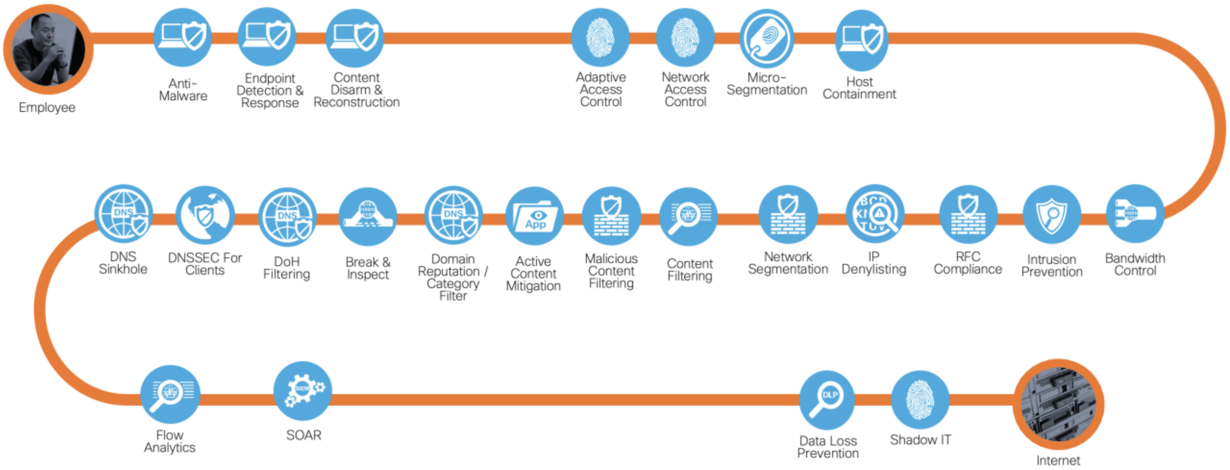


Figure 6.
Secure Internet Access business flow with required capabilities

In the secure internet access business flow, the most rigorous capabilities are required. Elements such as domain reputation filters are required to ensure that no users access domains with known malware, and break and inspect mechanisms are put in place to safeguard encrypted communications.

Securing employees accessing trusted applications

Trusted applications can be treated a little differently to typical web traffic. Using Office365 as an example:

- The domains are already known and therefore require no domain protections
- It is not recommended to break the encrypted connection to Office365 and therefore should bypass inspection
- Extra security controls such as MFA and DLP can be added to Office365 to reduce burden on a web gateway

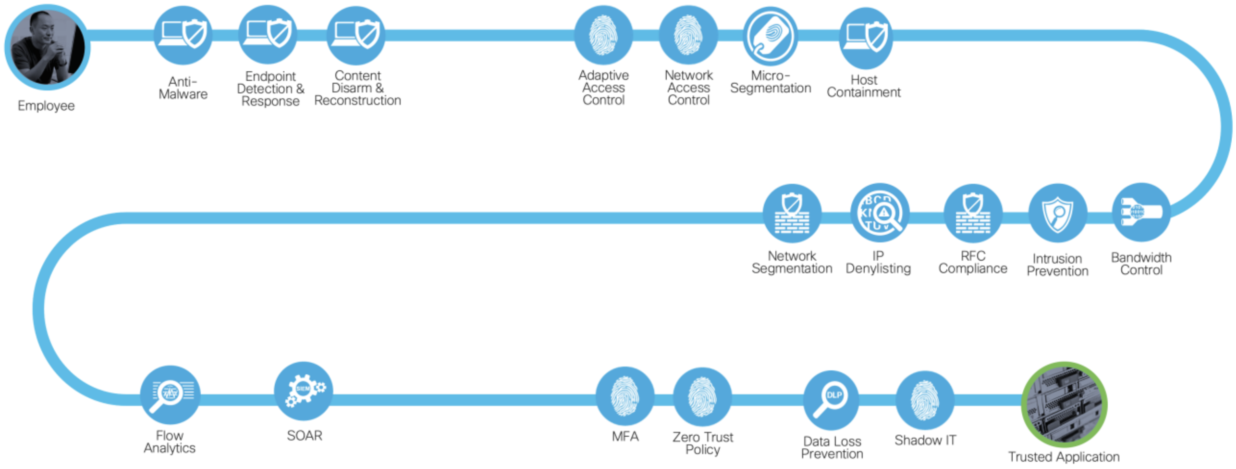


Figure 7.
Secure access to trusted applications with required capabilities

This results in a reduced capability set for protecting trusted applications. It is still important to look for malware within traffic and to have access control mechanisms on the applications, however, the need for DNS and SSL control is lost.

Securing employees accessing internal applications

Internal applications will be treated the same as trusted applications. There is a need for traffic to be encrypted while being transported back to the data center and the same security capabilities apply such as Multi-Factor Authentication (MFA), Data Loss Prevention (DLP) and access control.

Solution to capability mapping

The three potential origination points for users are the agency campus, branch offices, and remote users.

Traditional TIC

The TIC 3.0 Traditional TIC use case enumerates the TIC protections for agency campus. The guide will primarily focus on the branch and remote workers and internet edge capabilities will only be highlighted when needed. For a complete guide to securing the internet edge see Secure Internet Edge.

Agency branch

The Branch office use case defines how network and multi-boundary security should be applied when an agency has personnel in more than one physical location. This document is scoped to detail the security protections applied to the branch locations and not necessarily the network configurations when deploying them. This guide leverages Cisco SD-WAN, however, the security protections detailed here are not exclusive to running alongside the SD-WAN platform.

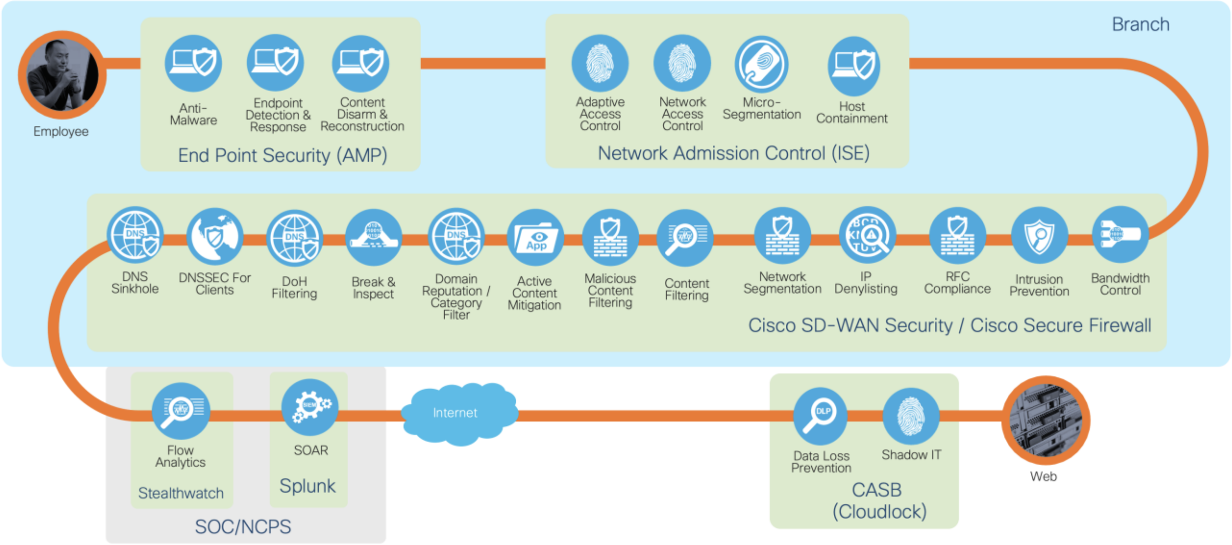


Figure 8.
Using on prem security capabilities for direct internet access

The first solution is to use the security capabilities that exist on the Cisco SD-WAN branch routers, or to pair a branch router with a small Cisco firewall such as a device from the Cisco Firepower 1000 series. Both the SD-WAN routers and Cisco Secure Firewalls provide application level firewall controls, malicious content filtering and intrusion prevention through Snort. Both platforms have their advantages. Cisco SD-WAN security policies are created in the same dashboard (Cisco vManage) used to control the SD-WAN routing policies, providing an integrated experience between network and security controls. Cisco Secure Firewall is a platform that may already exist on an agency campus and therefore it may be advantageous to unify security policies across locations.

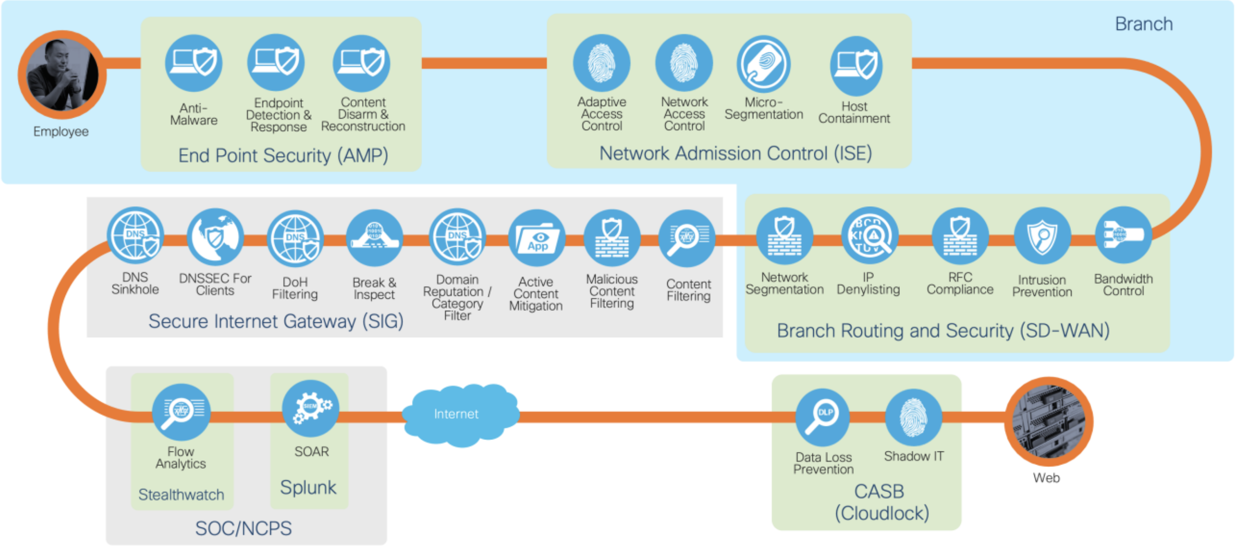


Figure 9.
Secure access to trusted applications with required capabilities

An alternate approach is to have all of the protection needed for secure internet traffic in another location, such as the Traditional TIC or in a cloud web security stack. For more details on how Cisco SD-WAN connects to secure internet gateways see Cisco Umbrella Integration.

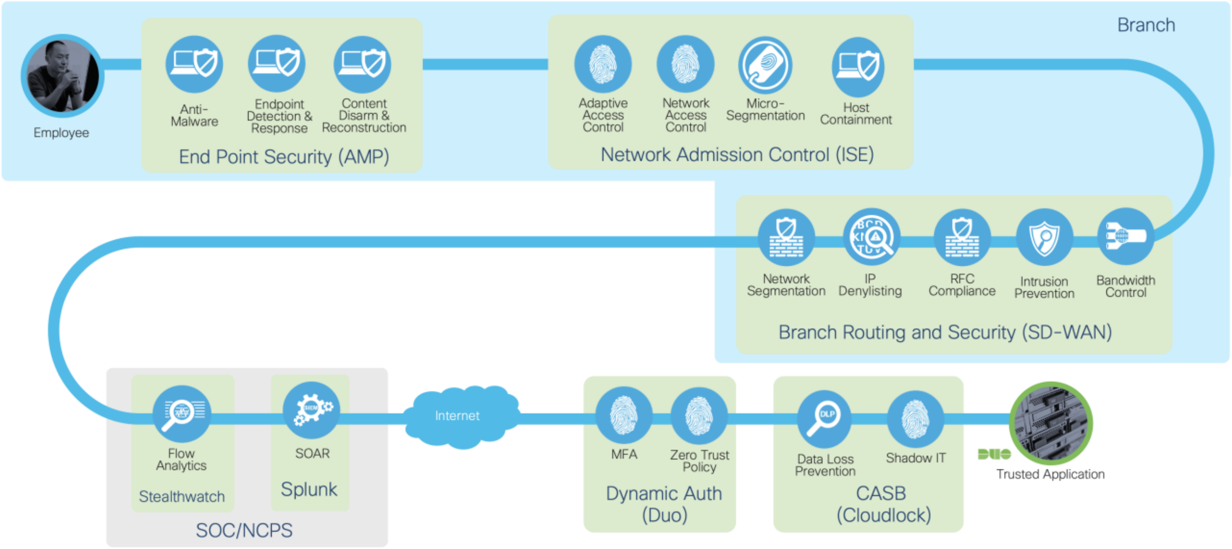


Figure 10.
Secure access to trusted applications with required capabilities

Removing the protections for secure internet leads us to an architecture known as Direct Cloud Access (DCA). The concept of DCA is to directly send traffic to trusted applications in the cloud, while back hauling the rest of the traffic through a Traditional TIC. This architecture provides performance enhancements for popular applications such as Office365 and WebEx with a minimum viable security set, while applying more strenuous security measures for internet traffic.

Roaming users

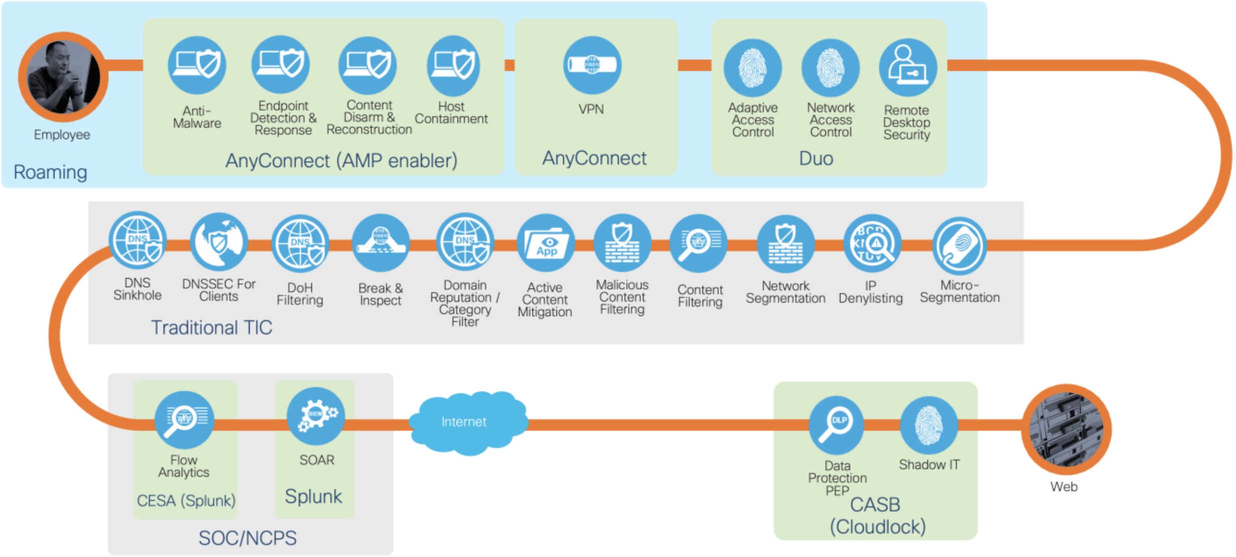


Figure 11.
Secure access to internet from roaming user

The same security practices can be applied regardless of the location. As federal civilian agencies respond to the COVID-19 pandemic, 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.

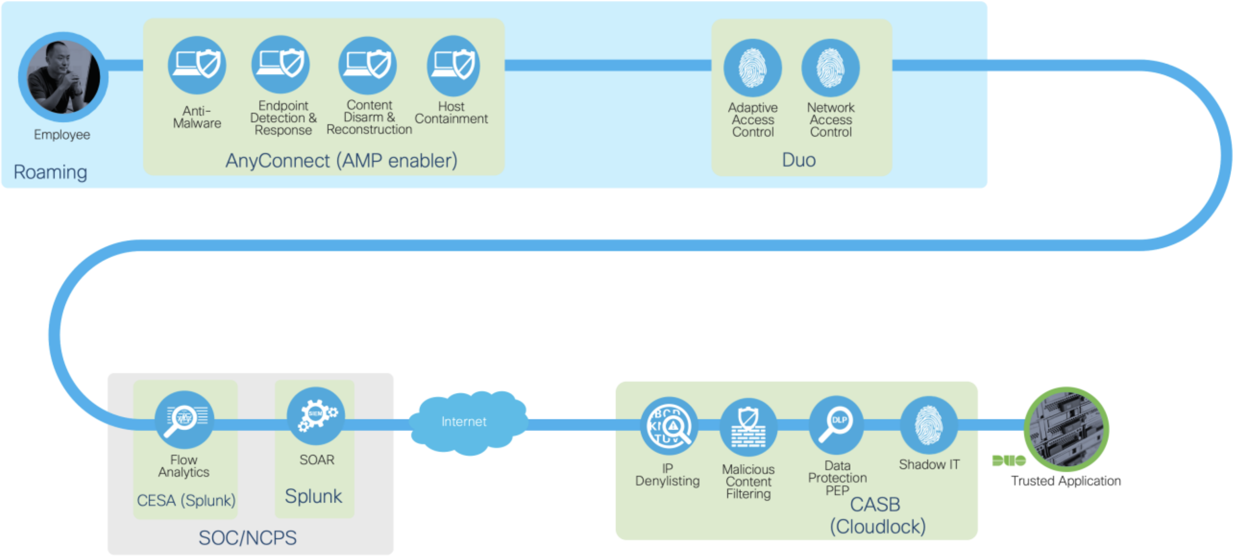


Figure 12.
Secure access to trusted applications from roaming user

With the use of VPN split tunneling, access to trusted applications can be split from the VPN tunnel for better performance. The use of a Cloud Access Security Broker (CASB) such as Cloudlock, enables access control and data protections at the application itself, removing the need for most web security capabilities outlined by TIC. For the remainder of internet traffic, all data is sent back through the Traditional TIC via a VPN tunnel, where existing TIC protections reside.

Architecture Overview

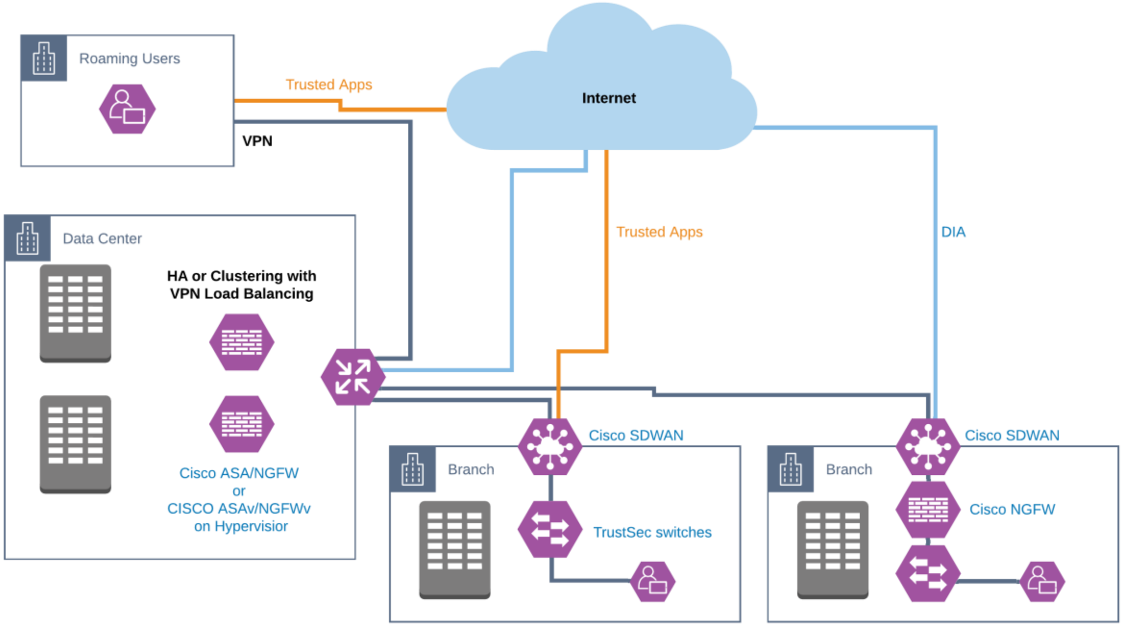


Figure 13.
TIC 3.0 architecture

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, 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 elements in the network, regardless of their location, securing the workforce, securing the workplace, and securing the workloads.

The guiding principles of ZTA resonate with the Universal capabilities outlined by TIC. For example:

- Developing, documenting, and maintaining a current inventory of all systems, networks, and components so that only authorized devices are given access
- Least privilege for each entity on the network
- Verifying the identity of users. Devices, or other entities through rigorous means such as MFA before granting access
- Constantly monitoring the network for vulnerabilities and staying up to date with the latest and greatest Threat Intelligence

TIC 3.0 offers agencies the freedom to implement a more flexible TIC model. It is common for agencies to utilize cloud services and accommodate remote workers' need access to all agency resources. These changes also impact the attack surface of the Federal Government. Instead of a singular location for policy enforcement, TIC 3.0 allows for distributing enforcement to different locations along the path if the deployed protections maintain a commensurate level of protection based on the agency's risk tolerance. This document will detail how remote users and branch offices can be permitted to directly interact with the cloud without routing back through the protections on the main agency campus.

Remote Users

Cisco Remote Access VPN

Traditionally, when teleworkers require access to agency-sanctioned cloud services, they first establish a trusted connection to agency campus resources (e.g., VPN). Aggregating all teleworker traffic through a single location facilitates security policy enforcement and protection parity at a central location. This security pattern also enables teleworkers and agency campus users to leverage the same connectivity to Cloud Solution Provider (CSP) resources (both conveyance and PEP). However, teleworker connections to agency campus concentrators at scale requires additional resources, incurs greater costs, and decreases performance. TIC 3.0 promotes connection methods that permit teleworkers to access agency sanctioned CSP resources while preserving policy enforcement parity and accommodating various risk tolerances.

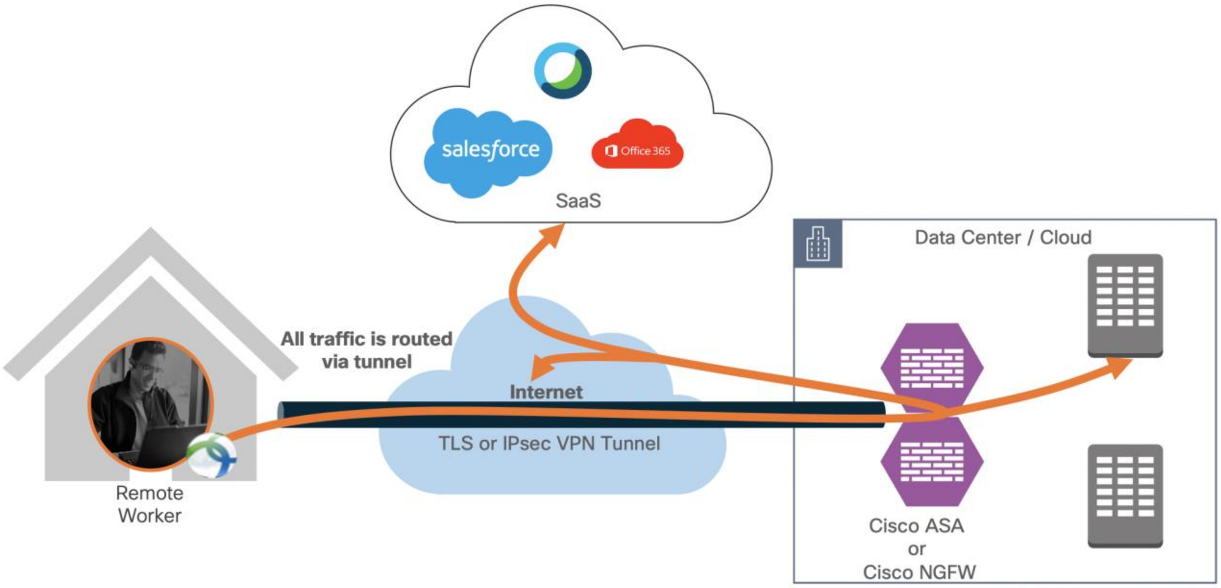


Figure 14.
Remote employee accessing resources hosted in the data center (tunnel-all)

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 are of two types: static and dynamic.

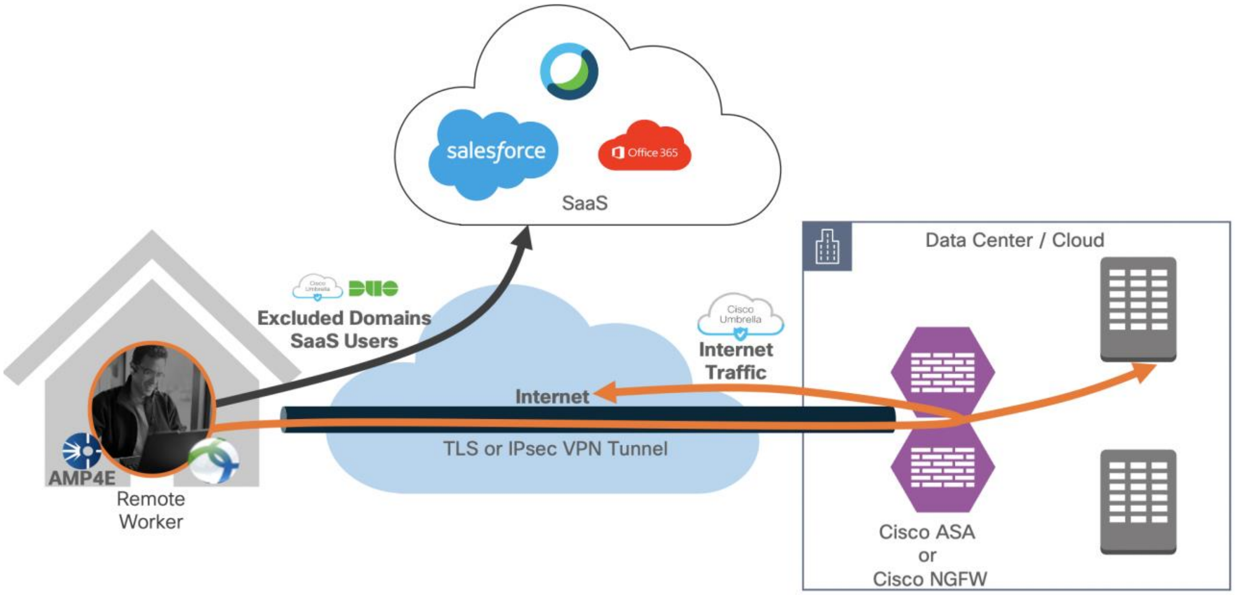


Figure 15.
Dynamic split tunnel applied (exclude traffic destined to exclude domains)

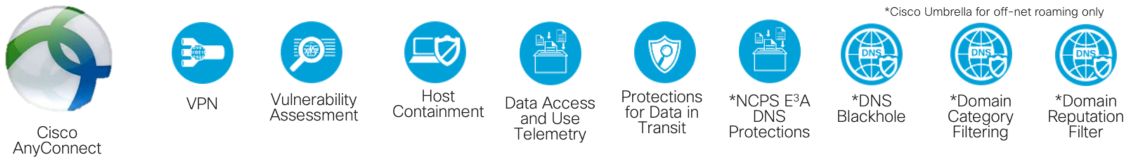
Static split tunneling involves defining the IP addresses of hosts and networks that should be included in or excluded from the remote access VPN tunnel. The limitation of the static split tunnel is that it is based on IP addresses defined in the split tunnel access control list. You can enhance split tunneling by defining dynamic split tunneling.

With dynamic split tunneling, you can fine-tune split tunneling based on DNS domain names. Because the IP addresses associated with full-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. If any addresses returned for excluded domain names are within the address pool included in the VPN, those addresses will then be excluded. Excluded domains are not blocked. Instead, traffic to those domains is kept outside the VPN tunnel.

Example: you could send traffic to Cisco WebEx, salesforce and Office365 on the public Internet, thus freeing bandwidth in your VPN tunnel for traffic that is targeted to servers within your protected network.

Cisco ASA natively supports the dynamic split-tunnel feature. On the Cisco Next-Generation firewall, the dynamic split tunnel feature is configured using Flex-Config.

Cisco AnyConnect


*Cisco Umbrella for off-net roaming only
Cisco AnyConnect
VPN
Vulnerability Assessment
Host Containment
Data Access and Use Telemetry
Protections for Data in Transit
*NCPS E^{3}A DNS Protections
*DNS Blackhole
*Domain Category Filtering
*Domain Reputation Filter

The Cisco 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 such as

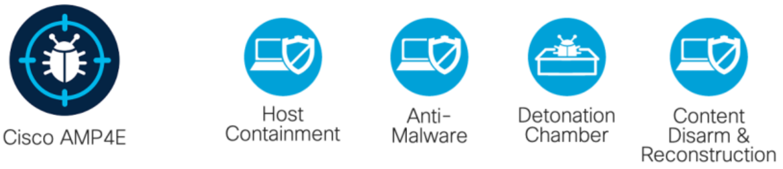
- Network Visibility Module (NVM)
- AMP Enabler
- Umbrella Roaming Security
- Cisco Common Cryptographic Module (C3M) which includes FIPS 140-2 compliant cryptography and National Security Agency (NSA) Suite B cryptography

Cisco Endpoint Security Analytics (CESA)

Historically, a flow collector provided the ability to collect IP network traffic as it enters or exits an interface of a switch or a router. It could determine the source of congestion in the network, the path of flow, but not much else. With NVM on the endpoint, the flow is augmented by rich endpoint context such as type of device, the user, the application, etc. This makes the flow records more actionable depending on the capabilities of the collection platform. The exported data provided with NVM which is sent via IPFIX is compatible with Cisco NetFlow collectors as well as other 3rd party flow collection platforms such as Splunk.

AnyConnect and Splunk are the infrastructures for CESA, which provides the monitoring and security analytics to address the lack of visibility in a split tunnel deployment. NVM provides a rich set of endpoint data, but it needs to be analyzed by an equally powerful technology. Using Splunk Enterprise, the agency security team can collect and analyze IPFIX flows generated by NVM, pulling out context such as user, device, application, location, and destination for each flow.

Cisco Secure Endpoint



AnyConnect AMP Enabler is used as a medium for deploying Cisco Secure endpoint. It pushes the endpoint software to a subset of endpoints from a server hosted locally within the enterprise and installs Secure Endpoint services to its existing user base. Cisco Secure Endpoint offers cloud-delivered Endpoint Protection and advanced Endpoint Detection and Response. It stops breaches and blocks malware, then rapidly detects, contains, and remediates advanced threats that evade front-line defenses.

- **Prevent** - Block known malware automatically leveraging the best global threat intelligence and enforce Zero Trust by blocking risky endpoints from gaining access to applications.
- **Detect** - Run complex queries and advanced investigations across all endpoints, and continuously monitor all file activity to detect stealthy malware.
- **Respond** - Rapidly contain the attack by isolating an infected endpoint and remediating malware across PCs, Macs, Linux, servers, and mobile devices (Android and iOS).

Cisco Secure Access by Duo

Cisco DUO
Strong Authentication
Integrated Desktop, Mobile, and Remote Policies
Vulnerability Assessment
Least Privilege
Dynamic Threat Discovery

Cisco Duo integrates with Cisco ASA or Cisco FTD VPN to add two-factor authentication for AnyConnect logins as well as a Zero Trust policy for VPN access.

Duo supports two-factor authentication in a variety of ways:

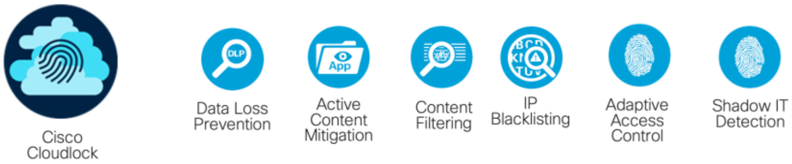
- ASA-SSL VPN using SAML
- ASA SSL VPN using RADIUS
- ASA SSL VPN using LDAPS
- FTD VPN using RADIUS

Additionally, Duo Federal Access adds unified endpoint visibility, which includes stronger role-based and location-based access policies, as well as biometric authentication enforcement. Ultimately 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, NIST's Digital Identity Guidelines (SP 800-63-3), and FIPS 140-2 compliance requirements for federal organizations.

For non-VPN users, Duo offers solutions to access both on-premise applications as well as SaaS based services. Duo Network Gateway (DNG) allows users to securely access internal web applications from any device, using any browser, without having to install or configure remote access software on their device. Users first authenticate to the DNG and approve a two-factor authentication request before they may access your different protected services. Duo checks the user, device, and network against an applications policy before allowing access to the application. For more information see Duo Network Gateway.

Cisco Duo Access Gateway (DAG) adds two-factor authentication, complete with inline self-service enrollment and Duo prompt, to popular cloud services like Salesforce and Google G Suite using SAML 2.0 federation. SAML delegates authentication from a service provider to an identity provider and is used for single sign-on solutions. Protected cloud applications redirect your users to the DAG server on your network. DAG acts as a SAML identity provider, authenticating your users using your existing primary authentication source for credential verification, and then prompting for two-factor authentication before permitting access to the SAML application. For more information see Duo Access Gateway.

Cisco Cloudlock



The downside of a split tunnel configuration is that all of the security benefits of the VPN are lost, and all of the PEP capabilities deployed at this aggregation point is bypassed. Cisco Cloudlock is a CASB solution that provides key protections such as DLP and geographic blocklists to the cloud. This enables users to not only get performance benefits from splitting trusted applications from the tunnel, but to maintain insight and access control to these applications. Key benefits of Cisco Cloudlock include:

- Identify and protect sensitive information within cloud environments and enforce automated, cross-platform response workflows
- Defend against account compromise with cross platform User and Entity Behavior Analytics for SaaS, IaaS, PaaS, and IDaaS environments
- Discover and control malicious and risky cloud apps connected to sanctioned cloud applications and infrastructure
- Increase the value of existing security investments by aggregating data streams and enforcing automated, cross-platform response workflows

Branch Network

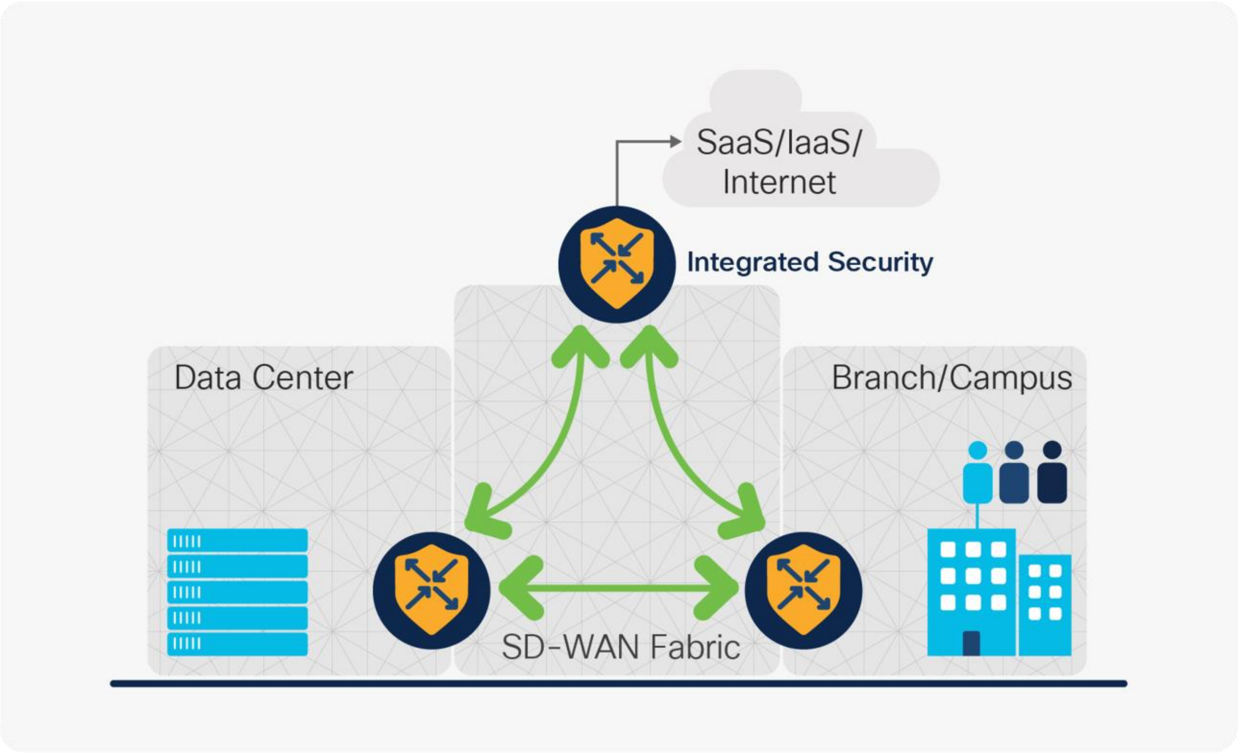


Figure 16.
Cisco SD-WAN fabric

As per TIC guidance, three security patterns capture the data flows for the agency branch office.

- **Back-haul data through campus** – the agency branch uses the agency campus as an intermediary traffic forwarding step. This is the Traditional TIC model, and while providing a high level of security, degrades performance for some applications.

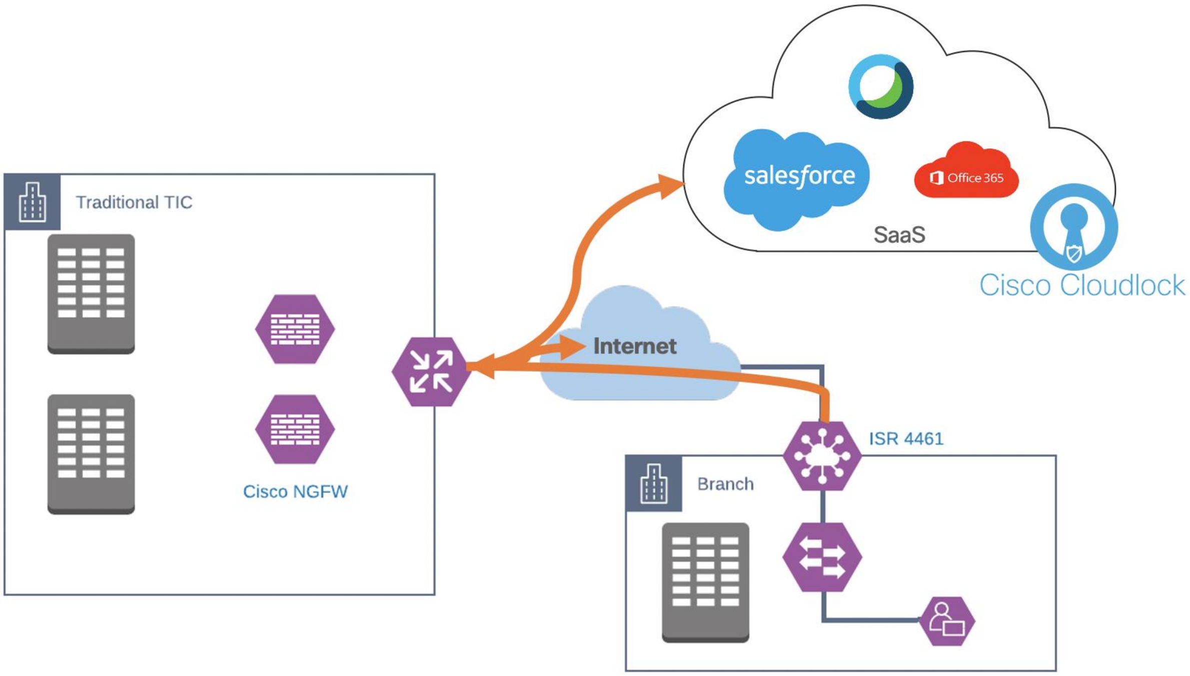


Figure 17.
Cisco SD-WAN backhaul all traffic

- **Direct Cloud Access (DCA)** – a DCA architecture optimizes the forwarding path of trusted applications while other traffic still back-hauls to the agency campus over VPN. DCA monitors the candidate path (DCA path vs. back-haul to campus) performance and chooses the optimized path in policy to get the best SaaS application performance.

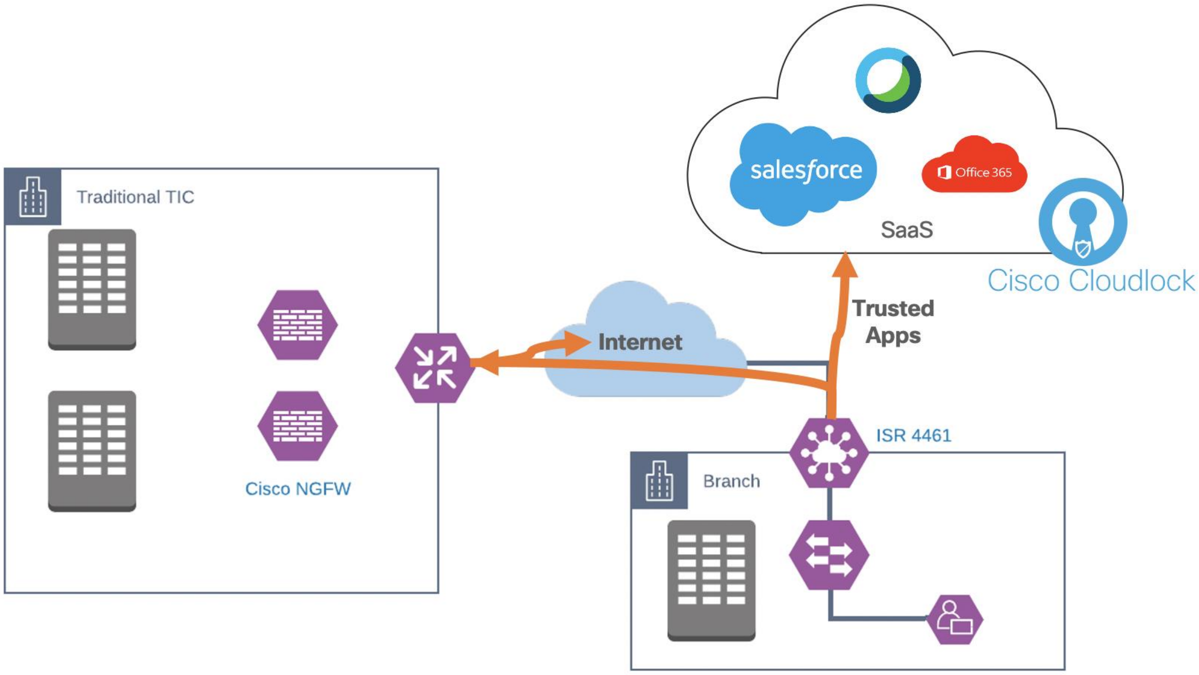


Figure 18.
Cisco SD-WAN Direct Cloud Access

- **Direct Internet Access (DIA)** – a DIA architecture sends all traffic through a local breakout unless destined for the agency campus (internal resources). In this scenario, branch office performance is optimized, however all of the security applied at the campus PEP need to be transferred to the branch.

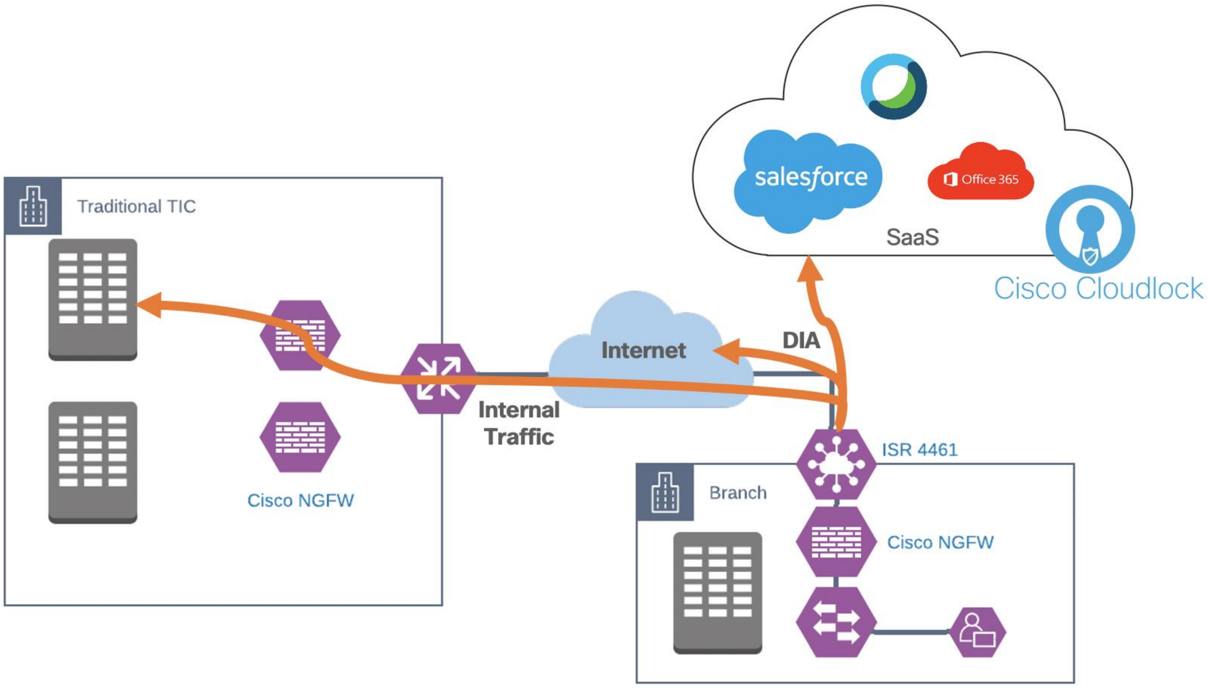
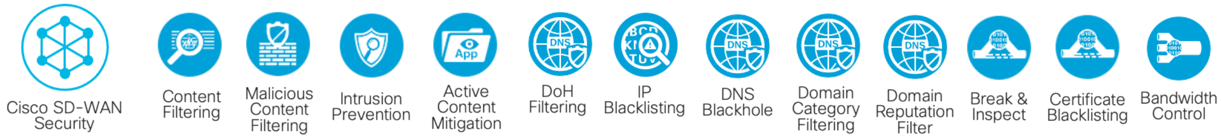


Figure 19.
Cisco SD-WAN Direct Internet Access with Cisco NGFW

Regardless of the traffic patterns deployed at the agency, Cisco SD-WAN optimizes the network in a single overlay that extends to data center, cloud and branch locations. With a single WAN fabric, all policies and configuration can be centrally managed, even across multicloud environments.

Cisco SD-WAN Security



To enable DCA at the branch sites, security embedded in SD-WAN routers provide onsite capabilities that include:

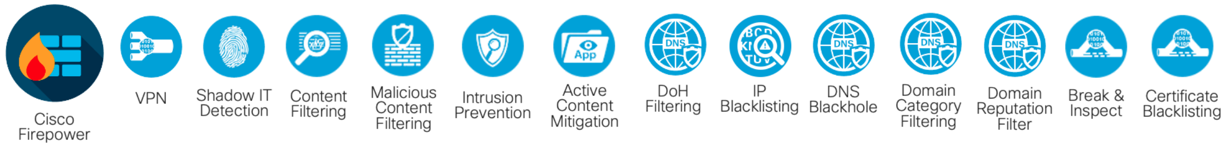
- Enterprise Firewall with Application Awareness restricts access to specific Internet destinations based on IP address/ port/ application family and more
- Intrusion Prevention System (IPS) with deep-packet inspection mitigates network attacks by providing your network with the intelligence to accurately identify, classify, and stop or block malicious traffic in real-time
- URL Filtering enforces acceptable user control to block or allow web traffic based on 82+ different categories and web reputation scores, with the added option to block/allow web traffic
- AMP for networks leverages global threat intelligence, advanced sandboxing, and real-time malware blocking to prevent breaches by continuously analyzing the file activity across the extended network to detect, contain, and remove malware immediately

Identical to the remote user scenario, where trusted applications are split from the VPN tunnel, Cisco Cloudlock will provide the CASB protections to SaaS applications split out in a DCA architecture.

Traditional TIC

The Traditional TIC use case defines how network security should be applied when an agency has one physical location and seeks to connect to the web for both general web services as well as to a trusted external partner. For the DCA and remote user use case, where will split traffic between trusted internet services and general web use, it was assumed that the agency would be using a Traditional TIC when backhauling untrusted traffic. When doing DIA at the branch, the Traditional TIC capabilities need to be brought to the branch network.

Cisco Secure Firewall



To enable DIA at the branch site, it is recommended to secure the network with a dedicated Cisco Secure Firewall device. The Cisco Firepower 1000 series family of NGFW is a smaller form factor device designed to extend the firewall footprint outside of the “traditional” perimeter and provide the same level of security at the edge. The Cisco Firepower 1000 series includes the same Cisco Next-Generation Intrusion Prevention System (NGIPS), Application Visibility and Control, Advanced Malware Protection (AMP) for Networks, and reputation-based URL filtering that can be found in higher range devices, only with lower bandwidth support.

The Cisco Firepower Management Center (FMC) is the administrative nerve center used to unify policy across all Cisco Secure Firewall devices regardless of location. If Cisco Secure Firewall is already deployed at the agency campus, those same policies and intrusion rules used to protect the back-hauled traffic can be applied to the local breakout traffic at the branch, increasing the branch performance while suffering no degradation to security.

Cisco TrustSec

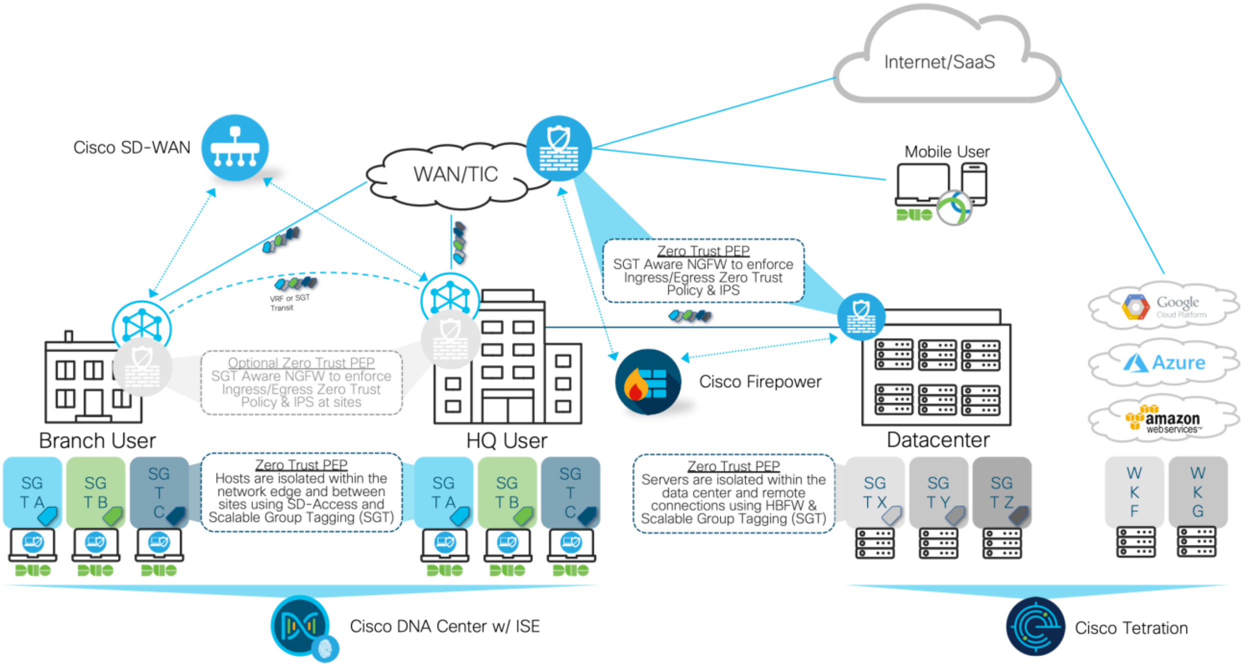

Internet/SaaS
Cisco SD-WAN
WAN/TIC
Mobile User
Zero Trust PEP
SGT Aware NGFW to enforce Ingress/Egress Zero Trust Policy & IPS
VRF or SGT Transit
Optional Zero Trust PEP
SGT Aware NGFW to enforce Ingress/Egress Zero Trust Policy & IPS at sites
Cisco Firepower
Google Cloud Platform
Azure
amazon web services
Branch User
HQ User
Datacenter
SG T A
SG T B
SG T C
Zero Trust PEP
Hosts are isolated within the network edge and between sites using SD-Access and Scalable Group Tagging (SGT)
SG T A
SG T B
SG T C
Zero Trust PEP
Servers are isolated within the data center and remote connections using HBFW & Scalable Group Tagging (SGT)
SG T X
SG T Y
SG T Z
W K F
W K G
DUO
Cisco DNA Center w/ ISE
Cisco Tetration

Figure 20.
Distributed SGT enforcement with Cisco SD-WAN

Revisiting Zero Trust, it was defined above as **"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."**

Cisco's TrustSec solution focuses on group-based segmentation **after** authenticating network connections. TrustSec software-defined segmentation dynamically organizes endpoints into logical groups, called security groups. These groups are irrespective of IP addressing or physical location. In fact, in most complex enterprises, these roles include multiple subnets and multiple buildings. This concept is the foundation to **securing the workplace**, one of the ZTA pillars. Cisco TrustSec allows policies to be defined and enforced, regardless of network location, giving agencies the ability to take policies that may have been created for the campus and extend them out to branches.

Cisco Identity Services Engine (ISE)

Cisco ISE
Inventory
Network Access Control
Adaptive Access Control
Network Segmentation
Micro-Segmentation
Host Containment
IP Blacklisting
Policy Enforcement Parity

TrustSec policies are centrally managed by the Cisco Identity Services Engine (ISE), a secure network access platform enabling increased management awareness, control, and consistency for users and devices accessing an organization's network. ISE is an integral part of software-defined access for policy implementation, enabling the dynamic mapping of users and devices to scalable groups and simplifying end-to-end security policy enforcement.

Appendix A: Additional Security Products

Cisco Secure Email

Today, spam and malware are part of a complex Email security picture that includes inbound threats and outbound risks. The all-in-one Cisco Secure Email offers simple, fast deployment, with few maintenance requirements, low latency, and low-operating costs. The set-and-forget technology frees your staff after the automated policy settings go live. The solution then automatically forwards security updates to Cisco's cloud-based threat intelligence solution. Threat intelligence data is refreshed in the Email appliance every 3 to 5 minutes, providing you with an up-to-date threat defense response hours or days before other vendors. Flexible deployment options and smooth integration with your existing infrastructure make this appliance an excellent fit for your Email security needs.

Cisco Hosted Collaboration Solution for Government (HCS-G)

Cisco HCS-G lets your agency benefit from secure and reliable cloud-based collaboration that can be scaled as your agency's needs change. It empowers you with:

- **Voice and Video** - Industry-leading call and session management, based on Cisco Unified Communications Manager (UCM), that enables a full set of telephony services, including voicemail and integrated messaging for IP phones, mobile phones, or desktop clients.
- **Mobility** - Simplify with one number to dial, redirect, and move calls between Cisco desktop and mobile phones. Empower employees to be productive anywhere, anytime with Cisco Jabber unified communications client, letting them access all Cisco collaboration workloads, instant messaging, presence, voice, video, voice messaging, desktop sharing, and conferencing.
- **Instant Messaging and Presence** - With Cisco Jabber, you can get the information you faster and more efficiently and make your availability known to other team members. Plus open an instant-messaging session, make a phone/video call, or start a Cisco WebEx meeting from your mobile device with just one click.
- **Conferencing** - Use real-time video to present, share, or collaborate anywhere, anytime on any authorized device. WebEx Web Conferencing, a FedRAMP Authorized Service, lets your team talk face-to-face across great distances, empowering everyone with the same information at the same time for better outcomes. Plus, reduce travel and make meetings more engaging with high-definition (HD) video, audio, and content sharing.

Cisco Secure Network Analytics

Cisco Secure Network Analytics, formerly 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. Cisco Secure Network Analytics 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.

Cisco Encrypted Traffic Analysis

Traditional flow monitoring provides a high-level view of network communications by reporting the addresses, ports and byte, and packet counts of a flow. In addition, intraflow metadata or information about events that occur inside of a flow can be collected, stored, and analyzed within a flow-monitoring framework. This data is especially valuable when traffic is encrypted, because deep-packet inspection is no longer viable. This intraflow metadata, called Encrypted Traffic Analytics (ETA), is derived by using new types of data elements or telemetry that are independent of protocol details, such as the lengths and arrival times of messages within a flow. Cisco Encrypted Traffic Analytics focuses on identifying malware communications in encrypted traffic through passive monitoring the extraction of relevant data elements and supervised machine learning with cloud-based global visibility.

Cisco Web Security Appliance (WSA)

The Cisco Web Security Appliance (WSA) simplifies security with a high-performance, dedicated appliance, and the Cisco Web Security Virtual Appliance (WSAV) allows businesses to deploy web security quickly and easily, wherever and whenever it is needed. The Cisco WSA was one of the first secure web gateways to combine leading protections to help organizations address the growing challenges of securing and controlling web traffic. It enables simpler, faster deployment with fewer maintenance requirements, reduced latency, and lower operating costs. “Set and forget” technology frees staff after initial automated policy settings go live, and automatic security updates are pushed to network devices every 3 to 5 minutes. Flexible deployment options and integration with your existing security infrastructure help you meet quickly evolving security requirements.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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