Trusted Internet Connections (TIC) 3.0

Cisco Overlay Guidance

April, 2021

Contents

Introduction

Trusted Internet Connections (TIC), originally established in 2007, is a federal cybersecurity initiative intended to enhance network and perimeter security across the Federal Government. The Office of Management and Budget (OMB), the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security agency (CISA), and the General Services Administration (GSA) oversee the TIC initiative, setting requirements and an execution framework for agencies to implement a baseline perimeter or multi-boundary security standard.

The initial versions of TIC consolidated federal networks and standardized perimeter security for the federal enterprise. As outlined in OMB Memorandum M-19-26: *Update to the Trusted Internet Connections (TIC) Initiative*, this modernized version of TIC expands upon the original program to drive security standards and leverage advances in technology as agencies adopt mobile and cloud environments. The goal of TIC 3.0 is to secure federal data, networks, and boundaries while providing visibility into agency traffic, including cloud communications.

Cisco's approach to TIC 3.0

Cisco's security approach for TIC 3.0 is not only designed to fulfill the requirements of distributed Policy Enforcement Points (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.

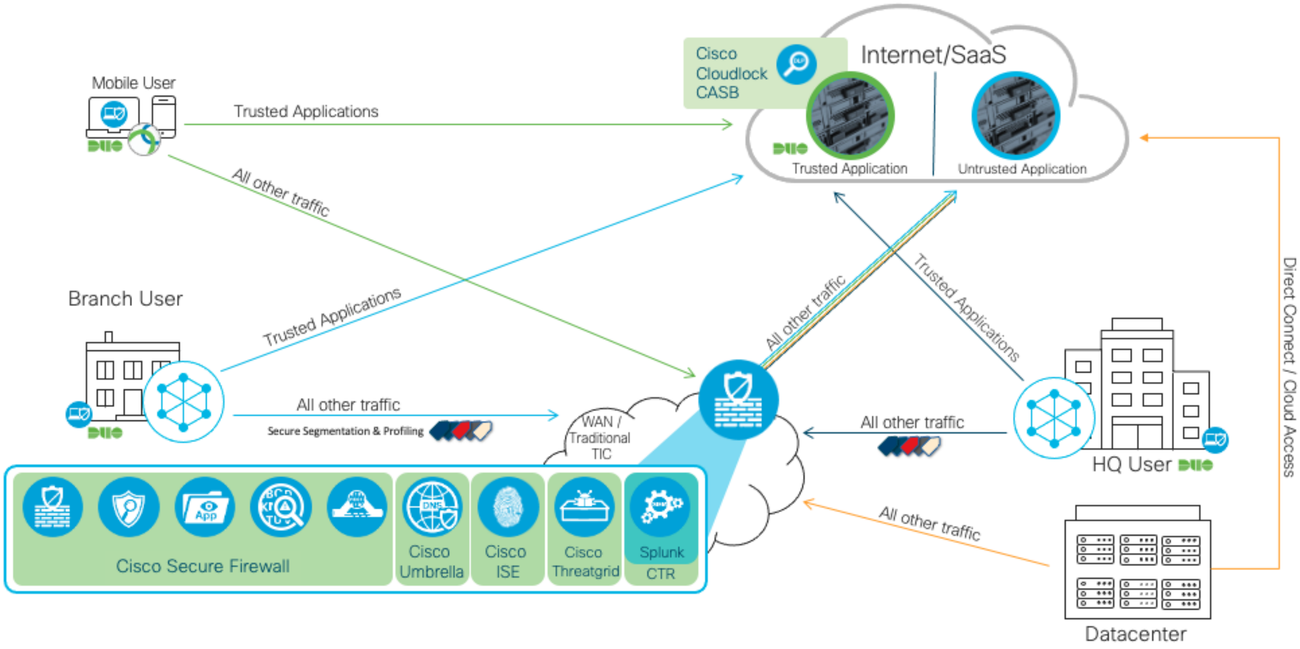

Figure 1.
Cisco TIC 3.0 Architecture

The purpose of this document is to provide an at-a-glance view of the Cisco portfolio against the required security capabilities for TIC 3.0. For further details on the architecture, go to Cisco TIC 3.0 Architecture Guide. Additional, for configuration guidance, go to Cisco TIC 3.0 Design Guide.

Security Capabilities of TIC 3.0

As described in the TIC Security Capabilities Catalog, the capabilities list is composed of two parts:

- **Universal Security Capabilities**: Enterprise-level capabilities that outline guiding principles for TIC Use Cases.
- **Policy Enforcement Point Security Capabilities**: Network-level capabilities that inform technical implementation for relevant use cases.

Universal Security Capabilities

The Universal capabilities are guiding principles as opposed to product capabilities. With some exceptions, such as strong authentication which is covered by Cisco Duo, the universal capabilities do not have a 1:1 mapping with a product or service in the Cisco portfolio, but rather each product offered by Cisco to meet the needs of TIC 3.0 follow the guiding principles outlined by CISA. For more information on how universal capabilities are met see the TIC 3.0 architecture guide.

Policy Enforcement Point (PEP) Capabilities

Files PEP Security Capabilities

TIC Security Capability	Service Name		Service Description
	Primary Service(s)	Complementary Service(s)	
Anti-malware	Cisco Anti-Malware Protection (AMP)	Cisco Secure Firewall, Cisco Secure Email, Cisco SD-WAN, Cisco Web Security Appliance (WSA), Threat Grid	AMP has two deployment scenarios; AMP for networks detects files as they traverse the network and can be found as a feature on many of the Cisco products (as seen from the Complementary services cell). AMP for endpoints (also known as Cisco Secure Endpoint) sits on endpoints and not only looks for malicious files (as determined by our threat intelligence feed or a custom policy) but also checks if any bad processes are running on the endpoints.
Content Disarm & Reconstruction	AMP	Threat Grid	AMP has the ability to disarm content, however, has no ability to reconstruct a message such as an email and send without the harmful portion of the message.
Detonation Chamber	Threat Grid		Threat Grid is a tool that is used when a file has an unknown disposition to AMP. Threat Grid opens the file in a sandbox and analyzes its behavior before deeming it malicious or not.
Data Loss Prevention (DLP)	Cisco Cloudlock		Cisco Cloudlock is a Cloud Access Security Broker (CASB) which performs DLP for files stored in Software as a Service (SaaS) applications such as Box.

Email PEP Security Capabilities

TIC Security Capability	Service Name		Service Description
	Primary Service(s)	Complementary Service(s)	
Anti-phishing Protections	Cisco Secure Email		Cisco Secure Email stops identity deception-based attacks such as social engineering and imposters by combining Cisco Talos threat intelligence with local email intelligence and advanced machine learning techniques to model trusted email behavior.
Anti-SPAM Protections	Cisco Secure Email		Cisco Secure Email blocks unwanted emails using a multilayered scanning architecture delivering the highest spam catch rate of greater than 99 percent, with a false-positive rate of less than one in one million.
Authenticated Received Chain	*Cisco Secure Email		Cisco Secure Email authenticated received chain is an email authentication system designed to allow an intermediate mail server like a mailing list or forwarding service to sign an email's original authentication results. *Roadmap
Data Loss Prevention	Cisco Secure Email		Cisco Secure Email protect outbound messages with DLP. Choose from an extensive policy library of more than 100 expert policies covering government, private sector, and company-specific regulations.
DMARC for Incoming Email	Cisco Secure Email		Cisco Secure Email define profiles to override (accept, quarantine, or reject) domain owners' policies. Send feedback reports to domain owners, which helps to strengthen their authentication deployments. Send delivery error reports to the domain owners if the DMARC aggregate report size exceeds 10 MB or the size specified in the RUA tag of the DMARC record.
DMARC for Outgoing Email	Cisco Secure Email		Cisco Secure Email automates the process of implementing the email authentication standard DMARC to better protect from phishing attacks using a customer domain(s).
Encryption for Email Transmission	Cisco Secure Email		Cisco Secure Email meets encryption requirements for regulations such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), or the Sarbanes-Oxley Act (SOX)—as well as state privacy regulations and European directives—without burdening the senders, recipients, or email administrators.
Malicious URL Protections	Cisco Secure Email		Cisco Secure Email protects users against malicious URLs with URL filtering, scanning of URLs in attachments, and managed (shortened) URLs. Appropriate policies are applied to the messages based on the reputation or category of the URLs.

TIC Security Capability	Service Name		Service Description
	Primary Service(s)	Complementary Service(s)	
URL Click-Through Protection	Cisco Secure Email		Cisco Secure Email web interaction tracking is a fully integrated solution that allows IT administrators to track the end users who click on URLs that have been rewritten by Cisco Secure Email. Reports show top users who clicked on malicious URLs and the top malicious URLs clicked by end users.
NCPS E3A Protections	Cisco Secure Email		

Web PEP Security Capabilities

In the following tables, there are instances where a capability is shown to be covered by both a Cisco Firewall and natively in SD-WAN routers. These services are not intended to be deployed together, but rather as an either-or scenario. SD-WAN references a Next-Gen Firewall (NGFW) solution that resides within an IOS XE device and can be managed by the Cisco SD-WAN platform directly. Cisco Secure Firewall refers to Cisco's Firepower family of products and would be managed by the Cisco Firepower Management Center (FMC). This may be a desired option if already using Cisco Firepower products in the network and would like to unify security policies regardless of location from a single management platform.

*The Cisco Web Security Appliance (WSA) is a dedicated hardware appliance for web security. This appliance will not be the main focus for this guide, however, for more information on a dedicated on prem secure web gateway see Cisco WSA.

TIC Security Capability	Service Name		Service Description
	Primary Service(s)	Complementary Service(s)	
Break and Inspect	Cisco SD-WAN, Cisco Secure Firewall	*Cisco WSA	Both platforms have the ability to decrypt traffic based with a known certificate or by acting as a man in the middle.
Active Content Mitigation	Cisco SD-WAN, Cisco Secure Firewall	*Cisco WSA	Both platforms have the option to use application filters to mitigate active content or to use IPS rules to see potential exploits taking place within active content.
Certificate Denylisting	Cisco SD-WAN, Cisco Secure Firewall	*Cisco WSA	Cisco SD-WAN makes use of online certificate status protocol (OCSP) to confirm that the server's certificate is valid before establishing a connection. In addition to OCSP, Cisco Firepower devices have the ability to use certificate revocation lists (CRLs).
Content Filtering	Cisco SD-WAN, Cisco Secure Firewall	*Cisco WSA	Both platforms have the ability to block access to web pages or applications – for example blocking access to social media. Cisco Firepower devices also have the capabilities to establish file policies that will block all files of a particular type, regardless whether it is malicious.

TIC Security Capability	Service Name		Service Description
	Primary Service(s)	Complementary Service(s)	
Authenticated Proxy	*Cisco WSA		Cisco WSA supports LDAP and NTLM for authenticating to the proxy.
Data Loss Prevention	Cisco Cloudlock	*Cisco WSA	Cloudlock's DLP technology continuously monitors cloud environments to detect and secure sensitive information. It provides countless out-of-the-box policies such as detection of credit card numbers as well as highly tunable custom policies.
DNS-over-HTTPS Filtering	Cisco Secure Firewall	*Cisco WSA	Cisco Firepower devices have the ability to detect DNS-over-HTTPS as an application. A rule can be created to block its use.
RFC Compliance Enforcement	Cisco SD-WAN, Cisco Secure Firewall	*Cisco WSA	Not only do the platforms have the ability to force RFC compliance, rules can be enforced to block RFC compliant protocols. For example, a firewall rule could be created to block TLS 1.0 and force traffic to use TLS 1.2.
Domain Category Filtering	Cisco SD-WAN, Cisco Secure Firewall	*Cisco WSA	Both platforms have the ability to block traffic based on category.
Domain Reputation Filter	Cisco SD-WAN, Cisco Secure Firewall	*Cisco WSA	Cisco SD-WAN uses the BrightCloud intelligence feed. Cisco Firepower devices get the reputation score from Talos.
Bandwidth Control	Cisco SD-WAN, Cisco Secure Firewall	*Cisco WSA	Bandwidth control supported on all platforms.
Malicious Content Filtering	Cisco SD-WAN, Cisco Secure Firewall	AMP, *Cisco WSA	Although AMP is listed as a complementary service, both SD-WAN security policies and Cisco Secure Firewall use AMP to determine if a file is malicious or not. When a file is passing through the firewall, its hash is sent to AMP for a disposition. If the file contains known malicious content, the file can be blocked, and the host can be quarantined. Additionally, both platforms use the same Snort engine for their Intrusion Prevention System (IPS). Snort rules are available to detect malicious patterns in the network traffic. The advantage Cisco Firepower has in this scenario is the ability to load custom snort rules into the devices, whereas SD-WAN has only pre-built rules available.
Access Control	Cisco SD-WAN, Cisco Secure Firewall	*Cisco WSA	Cisco Firepower family has capabilities to provide user-based access control and has integrations into an identity service such as Active Directory. SD-WAN security policies are applied on a per VPN basis. A separate VPN can be configured for each set of user groups, such as guests and employees, and then access control can be applied differently to each.

Networking PEP Security Capabilities

TIC Security Capability	Service Name		Service Description
	Primary Service(s)	Complementary Service(s)	
Access Control	ISE	Cisco SD-WAN, Cisco Secure Firewall	Cisco's Secure Firewall provide access control policies up to layer 7 (application). ISE is Cisco's workplace security solution in a zero-trust architecture and is used to provide more granular access control across the full network infrastructure, not just when crossing boundaries.
IP Denylisting	ISE	Cisco SD-WAN, Cisco Secure Firewall	All access control products in the Cisco portfolio support blocking based on IP address.
Host Containment	AMP, ISE		AMP for endpoints can be used to contain compromised hosts from the endpoints itself. If AMP detects malicious activity on an endpoint, a policy can be sent down to stop all network activity from occurring until further notice. ISE is the network enforcer for host containment. ISE maintains host profiles for all devices in the network has the ability to assign access control policies to switches to contain traffic from any compromised hosts.
Network Segmentation	Cisco Secure Firewall, ISE, Cisco SD-WAN		Although typically used at network borders, smaller form factor firewalls can be used to divide larger networks into smaller sub networks. ISE is the backbone of Cisco's software defined access solution. ISE configures the network infrastructure and can divide the network using Security Group Tags (SGTs).
Microsegmentation	ISE	Cisco SD-WAN, Cisco Secure Firewall	Microsegmentation refers to the prevention of lateral movement of threats in the network using granular access control. ISE can be used to define and manage SGTs on the network to enforce access policies for users, applications, and devices.

Resiliency PEP Security Capabilities

TIC Security Capability	Service Name		Service Description
	Primary Service(s)	Complementary Service(s)	
DDoS Protections	Radware		Radware's Attack Mitigation Solution combines all the necessary DDoS attack prevention services to make organizations resilient to cyberattacks with a single-vendor, hybrid DDoS security solution.
Elastic Expansion	ASAv, FTDv, CSR1000v		
Regional Delivery	All		

DNS PEP Security Capabilities

TIC Security Capability	Service Name		Service Description
	Primary Service(s)	Complementary Service(s)	
DNS Sinkholing	Umbrella DNS, Cisco Secure Firewall, Cisco SD-WAN		Cisco Umbrella DNS is the primary solution for DNS protection offered by Cisco. Cisco Secure Firewalls, and Cisco SD-WAN also have the ability to block traffic based on DNS, both by category definition and user generated lists.
DNSSEC for Agency Clients	Umbrella DNS		Cisco Umbrella resolvers act as fully RFC compliant security aware resolvers by performing DNSSEC validation on queries to authoritative nameserver for signed zones. The full scope of Umbrella's support for DNSSEC can be found here.
DNSSEC for Agency Domains	Umbrella DNS		Cisco Umbrella resolvers act as fully RFC compliant security aware resolvers by performing DNSSEC validation on queries to authoritative nameserver for signed zones. The full scope of Umbrella's support for DNSSEC can be found here.
NCPS E3A DNS Protections	Umbrella DNS	Cisco Secure Firewall	Umbrella DNS, while being a security tool on its own, also has capability to forward DNS to another entity such as NCPS. Cisco Secure Firewall access policies can ensure that only the NCPS DNS resolver is in use.

Intrusion Detection PEP Security Capabilities

TIC Security Capability	Service Name		Service Description
	Primary Service(s)	Complementary Service(s)	
Endpoint Detection and Response	AMP	Duo	Cisco AMP for endpoints delivers next generation antivirus that stops today's complex attacks. Powered by Cisco Talos, we block more threats than any other security provider. See a threat once and block it everywhere. Duo also helps you control access to your applications through the policy system by restricting access when devices to not meet particular security requirements.
Intrusion Protection Systems (IPS)	Cisco SD-WAN, Cisco Secure Firewall		Both Cisco Secure Firewall and SD-WAN platforms use Snort IPS engine.
Adaptive Access Control	Cisco Secure Firewall	ISE	Cisco Secure Firewall take in additional context when making access decisions such as if a host has been compromised and detected by AMP for endpoints. Cisco ISE can also take advantage of some of these heuristics to quarantine devices from the network.

TIC Security Capability	Service Name		Service Description
	Primary Service(s)	Complementary Service(s)	
Deception Platforms	–	Talos	Cisco do not provide deception platforms or Honeypots. However, Cisco Talos uses Honeypots as a tool to enrich the threat intelligence on all Cisco security products. If Talos catch an attack in their deception platforms, they develop the rules used to protect against that same attack in the event it happens to your network.
Certificate Transparency Log Monitoring	–		

Enterprise PEP Security Capabilities

TIC Security Capability	Service Name		Service Description
	Primary Service(s)	Complementary Service(s)	
Security Orchestration, Automation, and Response (SOAR)	–	*SecureX	SecureX connects the breadth of Cisco's integrated security portfolio and the customer's infrastructure for a consistent experience that unifies visibility, enables automation, and strengthens your security across network, endpoints, cloud, and applications. By connecting technology in an integrated platform, SecureX delivers measurable insights, desirable outcomes, and unparalleled cross-team collaboration. *SecureX is a cloud-based platform that at time of writing is not FEDRAMP ready. For updates on when this is available speak with your Cisco representative.
Shadow IT Detection	Cloudlock	Cisco Secure Firewall, Cisco SD-WAN, Cisco AnyConnect with CESA	Cisco Cloudlock is an API based CASB that provides visibility and control of cloud applications. Cisco Secure Firewall & Cisco SD-WAN provides application visibility and control for on-premise networks.
VPN	Cisco Secure Firewall, Cisco ASA, Cisco SD-WAN	Cisco AnyConnect	Cisco has two firewall platforms for VPN; Cisco ASA and Cisco Firepower. Cisco AnyConnect is a mobility client used to connect to these VPN devices. Cisco ASA does however support clientless VPN.

Unified Communications and Collaboration (UCC) PEP Security Capabilities

TIC Security Capability	Service Name		Service Description
	Primary Service(s)	Complementary Service(s)	
UCC Identity Verification	Cisco Hosted Collaboration Solution for Government (HCS-G)	Duo	Single Sign-on (SSO) across all the components in the Cisco HCS-G suite in conjunction with MFA using Duo.
UCC Encrypted Communication	Cisco HCS-G		FIPS 140-2 validated cryptography
UCC Connection Termination	Cisco HCS-G		Mechanisms exist that ensure the meeting host can positively control participation.
UCC Data Loss Prevention	Cisco HCS-G		Mechanisms exist for controlling the sharing of information between UCC participants, intentional or incidental.

Data Protection PEP Security Capabilities

TIC Security Capability	Service Name		Service Description
	Primary Service(s)	Complementary Service(s)	
Access Control	Cisco Cloudlock	Duo, ISE	Cisco Cloudlock is an API based CASB that provides visibility and control of cloud applications. Duo Access Gateway 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.
Protections for Data at Rest	Cisco Cloudlock		As an API based CASB solution, Cisco Cloudlock has the capability to monitor data in real time and at rest.
Protections for Data in Transit	Cisco SD-WAN, Cisco Secure Firewall	Cisco AnyConnect, Secure Network Analytics	Cisco's firewall infrastructure can send all data through encrypted tunnels while a combination of file policies and the firewall's IPS rule engine can ensure that only intended traffic flows through the network.
Data Loss Prevention	Cisco Cloudlock	Cisco AnyConnect, Secure Network Analytics	Cisco Cloudlock is a CASB which performs DLP for files and objects stored in SaaS applications such as Box or Webex Teams. For example, Cloudlock can detect Social Security Numbers being shared on a Webex chat.
Data Access and Use Telemetry	Cisco Cloudlock	Cisco AnyConnect, Secure Network Analytics	Cisco Cloudlock continuously monitors user behavior to detect anomalous activities, such as suspicious logins or downloads, and enables the prevention of malicious actors from stealing sensitive information.

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**.