SOLUTION BRIEF

# TIC 3.0: Components and Practical Applications for Securing Federal Agency Infrastructure

**The previous policies "required agency traffic to flow through a physical TIC access point, which has proven to be an obstacle to the adoption of cloud-based infrastructure", according to the policy memo.[1]**

## Executive Summary

The Trusted Internet Connection (TIC) initiative, designed in 2007, was meant to help U.S. federal government agencies migrate from numerous uncontrolled and unmonitored internet connections to fewer, more controlled access points. Its initial goal was to bring the civilian parts of the government in-line with the Department of Defense's earlier consolidation of its internet access to a small number of high-bandwidth gateways protected by a consistent set of intrusion detection and prevention capabilities. TIC has evolved considerably since it was conceived in an attempt to improve security, increase flexibility for agencies, and address newer technologies.

This solution brief will explain the evolution of TIC and the expanded use cases. Then, it will cover the robust security solutions Fortinet Federal offers to address the myriad requirements of TIC 3.0.

## Evolution of TIC: A Need for More Flexibility

*TIC 1.0* featured single and multi-agency TIC access providers (TICAPs), Managed Trusted Internet Protocol Services (MTIPS), and commercial TICs available through the Networx contract. However, implementation was uneven, resulting in continued vulnerability across the federal government due to continued use of legacy connections.

*TIC 2.0* introduced a reference architecture with an expanded set of capabilities and technical requirements, features such as virtual private network (VPN) connections, and a limited capability for federal users to access cloud environments.

*TIC 2.2*, Managed Trusted Internet Protocol Services (MTIPS), allowed government agencies to use consolidated models to host their presence with authorized providers, such as CenturyLink (now part of Lumen), Verizon, and AT&T. This enabled agencies to provision much of their security services from these providers, thereby removing the need to manage security on-premises.

The Federal Risk and Authorization Management Program (FedRAMP) had an overlay with TIC 2.0 that allowed service providers to deliver TIC-required controls in a virtualized cloud environment. Unfortunately, the only way a U.S. government user could connect to a FedRAMP-compliant cloud or to the internet was through an agency's network connection. This meant that traffic from mobile and field users had to be routed through an agency's permanent infrastructure. This added latency and required additional bandwidth for the extra routing, and it undercut key advantages of cloud-based architectures.

### TIC 3.0: Expanded use cases

*TIC 3.0*, released by the Office of Management and Budget in September 2019, introduces needed flexibility, and allows federal users to define additional use cases as their enterprise IT needs and functional requirements change. It marks a major step in the evolution of federal connectivity, bringing government IT closer to the capabilities available to the private sector. The use cases that have been most prominent in TIC 3.0 discussions are:

- **Cloud.** TIC 3.0 is a potential game-changing enabler for federal use of cloud technology. It moves the paradigm beyond simple virtualization of a physical TIC. The recently released temporary guidance[2] issued by the Cybersecurity and Infrastructure Security Agency (CISA) enables direct connection from the user to the cloud. A permanent TIC 3.0 cloud

use case is likely to cover connection and some of the most common cloud models—Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), Email-as-a-Service (EaaS), and Platform-as-a-Service (PaaS). It will allow users and providers to take better advantage of cloud technology. For instance, cloud providers will be enabled to patch applications seamlessly and transparently for TIC 3.0 users.

- **Agency branch office.** This use case assumes that a branch office currently utilizes the agency's headquarters for most of its IT services and web access. It enables agencies to directly connect approved traffic to the internet via software-defined wide-area networking (SD-WAN), and to push security out to the edge or branch office. As a result, users in the field environment have faster, more secure, more reliable, and less costly access to core agency IT functions and web services. This use case was finalized in April 2021.[3]

**Agencies are moving from virtual private networks (VPNs) to more robust identity management solutions as they implement Trusted Internet Connections 3.0 architectures.[4]**

- **Remote users.** This use case is an evolution of the original FedRAMP TIC overlay, providing greater flexibility in how a field user can connect to an agency's traditional network, a cloud, or the internet using government-furnished equipment.
- **Traditional TIC.** For federal connectivity not covered by these increasingly common use cases, the legacy model of TICAPs, MTIPs, and the Networx contract continue to apply.

TIC 3.0 begins to eliminate barriers to greater federal use of the cloud. It enables broader federal adoption of emerging technologies like SD-WAN, breaks down policy-driven bottlenecks in federal network access points, and enables more robust federal network security. It addresses the challenges of ever-greater numbers of federal employees working remotely or connecting to off-premises cloud environments—especially during the COVID-19 pandemic.

## Key Concepts of TIC 3.0

Under TIC 3.0, agencies are granted discretion to apply the objectives at a level that is commensurate with the type of resources being protected. They must adhere to the following key concepts:

- **Security capabilities** define the scope of agencies' responsibilities. They must be able to manage traffic, protecting its confidentiality and integrity. They must ensure that data is not altered in transit and that only authorized parties can see its contents, with sender and receiver identification and enforcement. They also must ensure service resiliency for continuity of operations and respond effectively and in a timely manner to threats.
- **Policy enforcement points (PEPs)** comprise eight network-level capabilities that inform technical implementation for relevant use cases.[5] These include files, the web, DNS, email, enterprise, intrusion detection, networking, and resiliency.
- **Trust zones** should be established based on the sensitivity of the data in each zone.[6] Agencies are responsible for implementing protections that are appropriate for the data in each zone. Enforcement can be distributed to different locations along the path, such as the network edge or cloud access gateway, as long as the level of protection is appropriate for the zone.
- **Management entities** oversee and control data protections for an agency. The entity can be an organization, network device, tool, function, or application.[7] The entity can control the collection, processing, analysis, and display of information collected from the policy enforcement points, and it allows IT professionals to control devices on the network. The expansion of potential management entities is a part of the flexibility that TIC 3.0 brings for federal organizations.

Fortinet solutions map extremely closely with the requirements of TIC 3.0 for all use cases. What follows is a summary of how Fortinet can provide coverage for the basic components of TIC 3.0, the network and security operations center (NOC and SOC) elements, trust zones, and PEPs. To close, we will take a closer look at how Fortinet Secure SD-WAN is a perfect fit for the agency branch office use case.

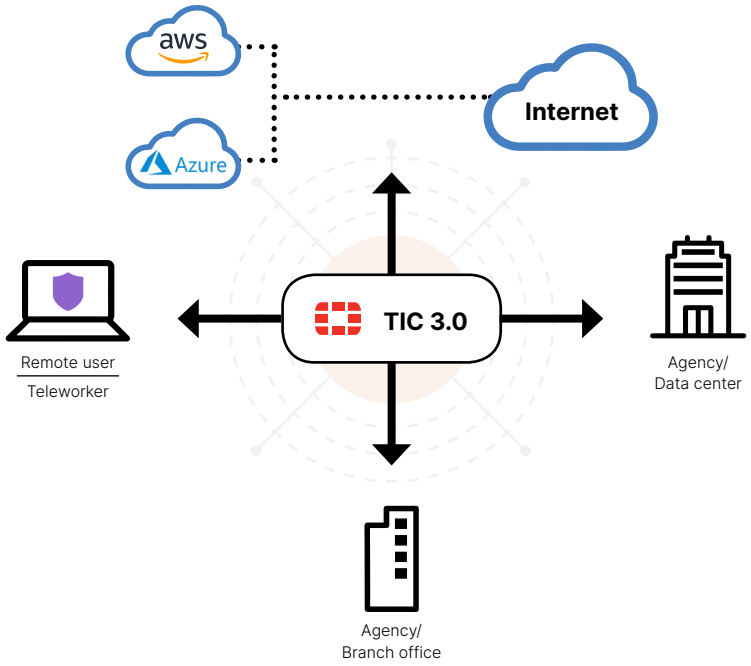



Figure 1: Fortinet and TIC 3.0 diagram.

## Primary TIC 3.0 Components: Fortinet Builds a Robust Foundation

The Fortinet **FortiGate Next-Generation Firewall** (NGFW) appliance has been the technology of choice for service providers delivering TIC capability going back to TIC 2.2. The FortiGate NGFW includes next-generation firewall security, advanced routing, and WAN optimization capabilities. The Fortinet Secure SD-WAN solution is an extended capability built into FortiGate NGFW. With a total systems approach, it leverages software and hardware to deliver routing, critical network functions and applications (such as voice, video, Wi-Fi, and internet), and comprehensive network security on a single platform with performance at scale.

Now agencies can use the same technology that powers MTIPS to meet and even exceed the security requirements of TIC 3.0, supporting the evolution of agency networks into distributed enterprises and providing field users with the same speed and capabilities available in agency headquarters. Agencies can be assured that Fortinet solutions scale to government-sized networks with thousands or even tens of thousands of sites. And Fortinet can meet the TIC use cases with platforms that provide tried-and-true security controls natively through the Fortinet Security Fabric—rather than through point products that are bolted on.

Supplementing the FortiGate NGFW in the Fortinet Security Fabric are the **FortiMail** secure email gateway, the **FortiWeb** web application firewall, and the artificial intelligence (AI)-powered automation of zero-day advanced malware detection and response with **FortiSandbox**.

## NOC/SOC Solutions: Building Integrated Security and Networking

In the NOC and SOC, **FortiManager**'s automation-driven, single-pane-of-glass management enables full visibility of the entire security architecture. It also helps teams maintain secure configuration management across the entire attack surface, including with cloud-based services. **FortiAnalyzer** enables analytics-driven security management with log collection and event correlation across the Security Fabric.

The **FortiSIEM** security information and event management tool automates security and performance monitoring across an agency, and **FortiAI** provides an AI-driven virtual security analyst so that cybersecurity staff can refocus from repetitive monitoring tasks toward more strategic contributions. And the **FortiSOAR** security orchestration, automation, and response solution provides innovative case management, automation, and orchestration, unifying operations and reducing alert fatigue.

## Trust Zone Solutions: Moving Beyond Legacy Authentication

Zero-trust network access is a critical component of TIC 3.0's trust zone concept. **FortiAuthenticator** enables identity management and multi-factor authentication (MFA) to verify users as they access different network resources. The **FortiNAC** network access control tool provides deep visibility and policy-based access control for all devices attempting to connect across an agency's infrastructure, including Internet-of-Things (IoT) devices at the network edge. And the **FortiInsight** user and entity behavior analytics tools use AI to watch for anomalous behavior that might be a sign of an unauthorized user with stolen credentials.

**The Fortinet Security Fabric is a broad, integrated, and automated platform with an open ecosystem that spans the extended digital attack surface and cycle, enabling self-healing security and networking to protect devices, data, and applications.**

## PEP Solutions: Enforcing Policies Across the Network

Fortinet Security Fabric solutions address 43 of the 46 required capabilities across all eight PEP functions, with the FortiGate NGFW meeting 33 on its own. Here is a summary of how the various PEPs can be architected using Fortinet tools:

- **Files PEP.** On the client, the **FortiClient** endpoint security solution and **FortiEDR** endpoint detection and response tool ensure file security. Across the infrastructure, **FortiMail** and **FortiSandbox** work in conjunction with **FortiGate NGFWs** to protect files in motion on an agency's infrastructure. The **FortiIsolator** browser isolation solution provides content disarm and reconstruction, where files from the web are accessed in a remote container and then risk-free content is rendered to users.
- **Email PEP. FortiClient** and **FortiInsight** work on the client, while **FortiMail**, **FortiWeb**, and **FortiSandbox** work with **FortiGate NGFWs** to fight spam, phishing, and data loss. The solution enables encryption for email messages in transit, malicious URL protections, URL click-through protections, and domain-based message authentication, reporting, and conformance (DMARC) for both incoming and outgoing mail.
- **Web PEP. FortiClient**, **FortiInsight**, **FortiMail**, and **FortiSandbox** work on the client and infrastructure, while **FortiSIEM** and **FortiAuthenticator** work at the management layer. This solution addresses requirements for break and inspect, active content mitigation, certificate blacklisting, content filtering, authenticated proxy, DNS-over-HTTPS filtering, and domain category and reputation filtering.
- **Networking PEP. FortiAP** wireless access points and **FortiSwitch** switches work in conjunction with the **FortiGate NGFW** to facilitate secure networking. **FortiGate** provides microsegmentation, IP blacklisting, and host containment, while **FortiAuthenticator** and **FortiNAC** ensure that only authorized users and devices are on the network. The solution provides IP blacklisting, host containment, and microsegmentation of the network.
- **Resiliency PEP.** The **FortiGate NGFW** works with **FortiDDoS** for protection against distributed denial-of-service (DDoS) attacks, and with the **FortiADC** application delivery controller to ensure security, high performance, and business continuity for an agency's applications.
- **DNS PEP. FortiClient** and **FortiGate** help prevent blackholing with the domain name system (DNS) and enables DNS Security Extensions (DNSSEC) for both clients and domains at an agency.
- **Intrusion Detection PEP. FortiClient** and **FortiEDR** cover the client, while **FortiGate NGFWs** work with **FortiSandbox** and the **FortiDeceptor** deception-based breach protector to secure the infrastructure. This solution provides endpoint detection and response, adaptive access control, deception platforms, and certificate transparency log monitoring.
- **Enterprise PEP. FortiClient**, **FortiEDR**, **FortiAnalyzer**, **FortiSIEM**, and **FortiSOAR** work with **FortiGate NGFWs** to provide VPN connectivity, detection of shadow IT activities, and security orchestration, automation, and response.

## Agency Branch Office Use Case: Enhanced Performance and Built-in Security With Fortinet Secure SD-WAN

The branch office use case in TIC 3.0 is composed of four trust zones: agency campus, agency branch office, cloud service provider (CSP), and web. Under TIC 3.0, a branch office user can interact directly with CSP resources without having to connect through the agency campus. SD-WAN boosts the performance of agency networks for non-headquarters workers and reduces agency network costs by shifting from expensive multiprotocol label switching (MPLS) infrastructure to more cost-effective direct internet access. However, security becomes even more important with the use of SD-WAN, because branch offices connecting directly to the internet inherently expand the agency's attack surface.

**The TIC 3.0 agency branch office use case enables agencies to directly connect approved traffic to the internet via SD-WAN and to push security out to the edge or branch office.**

Standalone SD-WAN solutions generally provide some level of security, but many lack data center-grade protection, including intrusion prevention system (IPS) technologies and the ability to inspect secure sockets layer (SSL)-encrypted traffic. Such security gaps may inhibit an SD-WAN solution's ability to detect and counter threats.

### Built-in security

That is why it is essential to deploy an SD-WAN solution with strong security capabilities built in. **Fortinet Secure SD-WAN** enables agencies to evolve their networking from a hub-and-spoke architecture—in which most local traffic is sent to a central location for security inspection before delivery to its final destination—to a software-defined networking architecture that is application aware and allows for real-time customization based on changing mission and user requirements.

Using a decentralized control mechanism, Fortinet Secure SD-WAN provides a branch-centric approach to traffic management. It can determine the optimal path for traffic—MPLS, 3G/4G/5G, or broadband—at any moment in time based on the specific application and desired user performance requirements. Benefits include reduced latency associated with forwarding decisions and a more scalable architecture.

### Security benefits

With Secure SD-WAN, which is FIPS 140-2 certified and IPv4 and IPv6 ready, users enjoy faster connections and better application performance than with a hub-and-spoke architecture. This speed and performance enables new TIC use cases, such as the agency branch office, and provides agencies with data confidentiality, integrity, and availability at any location. With strong built-in security, agencies gain multiple benefits:

- More robust security, because the Secure SD-WAN solution integrates tightly with advanced threat protection solutions such as sandboxing
- Less time spent on the management of networking and threat response because the agency has a single-pane-of-glass view into the operation of both functions
- Reduced costs, because consolidation of security and networking means that the agency has fewer devices to buy and maintain

### Operational benefits

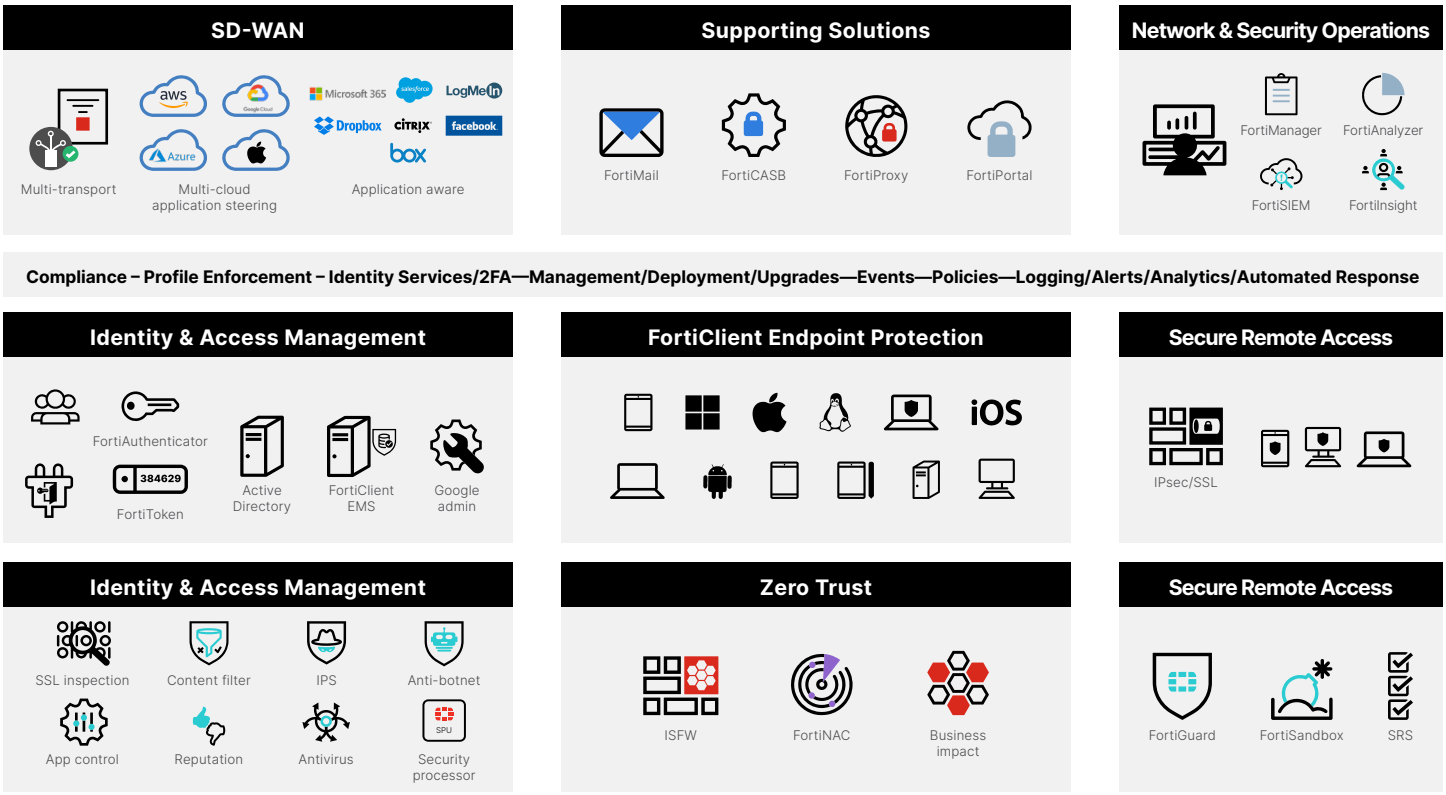
Beyond security, agencies gain other operational benefits with Fortinet Secure SD-WAN. Zero-touch deployment and centralized configuration management enable staff to roll out and configure new solutions without having to travel to each location, minimizing total cost of ownership. Furthermore, because SD-WAN solutions improve the speed and latency users experience in accessing cloud-based software, they support broader implementation of SaaS solutions, which reduces agency IT expenses.

Fortinet Secure SD-WAN is the first solution to combine independently validated and fully integrated security with an SD-WAN networking capability that can meet the growing IT requirements of federal agencies. It is the only solution that provides a fully integrated software-defined branch solution in which WAN, LAN, and security functionality can all be managed using a single management console. Fortinet Secure SD-WAN replaces separate WAN routers, WAN optimization, and security devices with a single solution that is application aware. In addition, Fortinet gives agencies flexibility in how they deploy SD-WAN, offering hardware appliances, virtual machines, and public cloud service providers.

## Why Fortinet?

Federal agencies have relied on Fortinet's proven performance for previous generations of TIC services, and this same world-class security underpins Fortinet's support for TIC 3.0. Fortinet's broad portfolio of integrated solutions reduces management overhead and closes security gaps. Further, purpose-built security processors prevent security from ever becoming a bottleneck—even at the scale of the largest federal agencies. For more information, visit www.fortinetfederal.com.

## Fortinet TIC 3.0 Security Architecture Components




[1] Aaron Boyd, "OMB Finalizes Long-Awaited Update to Internet Connection Policy," Nextgov, September 12, 2019.

[2] "Trusted Internet Connections 3.0 Interim Telework Guidance," CISA, accessed May 24, 2021.

[3] Dave Nyczepir, "First TIC 3.0 use cases finalized," FedScoop, April 7, 2021.

[4] Dave Nyczepir, "Agencies moving away from VPNs as they implement TIC 3.0," FedScoop, April 30, 2021.

[5] "Trusted Internet Connections 3.0, Vol. 3, Security Capabilities Handbook," CISA, December 2019.

[6] Aaron Boyd, "TIC 3 Commenters Put Faith in Zero Trust over CISA's Trust Zones," Nextgov, February 18, 2020.

[7] "Trusted Internet Connections 3.0, Vol. 3, Security Capabilities Handbook," CISA, December 2019.

FORTINET

www.fortinet.com



September 15, 2021 10:20 AM
9553314-0-0-EN