SOLUTION BRIEF

TIC 3.0: Secure SD-WAN Enables Connectivity Without Performance Degradation

The Trusted Internet Connection (TIC) initiative, designed to enhance network and perimeter security across the federal government, has evolved considerably since it was conceived a decade ago as an attempt to tame the "Wild West" of federal Internet access through thousands of disparate – and in many cases – undocumented connections with varying levels of security.

TIC 1.0 was modeled after the U.S. Defense Department's consolidation of its Internet access to a small number of high-bandwidth gateways protected by a consistent set of intrusion detection and prevention capabilities. It featured Trusted Internet Connections (TIC), single and multi-agency access providers (TICAPs), Managed Trusted Internet Protocol Service (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. While the FedRAMP TIC overlay allowed service providers to deliver TIC-required controls in a virtualized cloud environment, the only way a U.S. government user could connect to a FedRAMP-compliant cloud or to the Internet was from an agency's network connection, which meant mobile or 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 architecture such as the ability for ubiquitous access from any location with Internet connectivity.

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
- Agency branch office
- Remote users
- Traditional TIC

TIC 3.0 marks a major step in the evolution of federal connectivity, bringing government IT closer to the capabilities available to the private sector.

The TIC 3.0 agency branch office use case 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.

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[1] 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, by enabling cloud providers to seamlessly and transparently patch applications for TIC 3.0 users.

Agency branch office: This use case assumes the existence of a branch office that currently utilizes the agency's headquarters for the majority 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.

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.

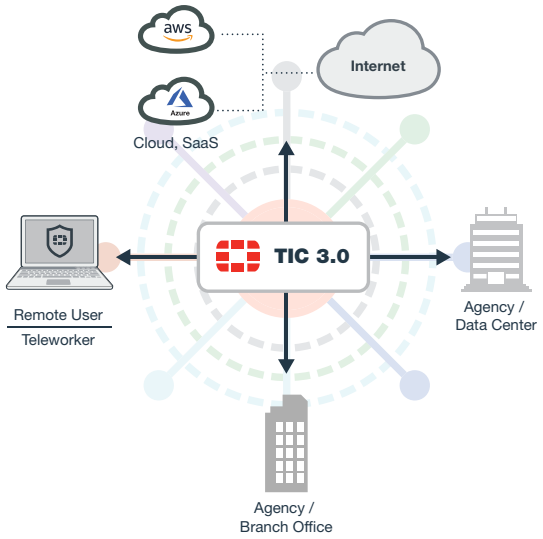
Traditional TIC: For federal connectivity not covered by these increasingly common use cases, the current model of "permanent" connections and TICAPs, MTIPS, and the Networx contract continues to apply.

The temporary guidance[2] issued by CISA in response to the surge in federal employee telework due to the COVID-19 pandemic was built off the use case for branch offices and addresses capabilities such as email, networking, intrusion detection, and data protection.

Access Models Evolve Under TIC 3.0

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.

Fortinet's FortiGate Next-Generation Firewall (NGFW) Appliance has been the technology of choice for service providers delivering TIC capability under MTIPS, through which service providers are authorized by the federal government to provide agencies with secure commercial Internet connections that meet the security requirements of TIC 2.2. FortiGate NGFW includes next-generation firewall security, advanced routing, and WAN optimization capabilities. Fortinet's 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 – not through point products bolted on.

SD-WAN Enables Better Performance and Built-in Security

Fortinet's Secure SD-WAN technology 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 SD-WAN provides a branch-centric approach to traffic management. It can determine the optimal path for traffic – Multiprotocol Label Switching (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.

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.

SD-WAN Supports the TIC 3.0 Branch Office Use Case

The Branch Office Use Case[2] 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 is able to 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 will reduce agency network costs by shifting from expensive 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.

Standalone SD-WAN solutions[3] generally provide some level of security, but many lack data center-grade protection, including intrusion prevention system technologies and the ability to inspect SSL-encrypted traffic. Such security gaps may inhibit an SD-WAN solution's ability to detect and counter threats. That's why it's essential to implement an SD-WAN solution that has strong security capabilities built in – such as Fortinet's Secure SD-WAN. By deploying Fortinet's Secure SD-WAN offering, full Layer 7/application security can be enabled at the edge, combining the highest level of protection with a segmented approach.

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.

Beyond security, agencies gain other operational benefits with 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 software-as-a-service (SaaS) solutions, which reduces agency IT expenses.

Many standalone SD-WAN solutions lack data-center grade protection, which may inhibit their ability to detect and counter threats. That's why it's essential to implement an SD-WAN solution that has strong security capabilities built in.

Because SD-WAN solutions improve the speed and latency users experience in accessing cloud-based software, they support broader implementation of software-as-a-service (SaaS) solutions, which reduces agency IT expenses.

Why Fortinet

Federal agencies have relied on Fortinet's proven performance in previous generations of TIC services, and this same world-class security underpins Fortinet's support for TIC 3.0 and SD-WAN. Fortinet's Secure SD-WAN[4] solution is the first to combine independently validated and fully integrated security with an SD-WAN networking solution that is capable of meeting the growing IT requirements of federal agencies. It is the only solution that provides a fully integrated SD-Branch solution where WAN, LAN, and security functionality can all be managed using a single management console. FortiGate 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. For more information, visit www.fortinetfederal.com.

[1] https://www.cisa.gov/sites/default/files/publications/CISA-TIC-TIC%203.0%20Interim%20Telework%20Guidance-2020.04.08.pdf

[2] https://www.cisa.gov/sites/default/files/publications/Draft%20TIC%203.0%20Branch%20Office%20Use%20Case.pdf

[3] https://www.fortinet.com/content/dam/fortinet/assets/ebook/eb-federal-agencies-sd-wan.pdf

[4] https://www.fortinet.com/resources-campaign/government/how-your-agency-can-modernize-using-securesd-wan-market-trends-report

FORTINET

www.fortinet.com

Copyright © 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

June 4, 2020 3:34 PM

674886-0-0-EN

C:\Users\cyan\Documents\Creative Services - Misc\Document Edits\TIC 3\sb-tic-3.0-secure-sdwan-enables-connectivity-5192020-638AM\sb-tic-3.0-secure-sdwan-enables-connectivity-5192020-638AM