Forcepoint

Issue Brief

Commercial Solutions for Classified Program

Leveraging CSfC to create secure, encrypted networks

Federal agencies understand how important protecting their networks and critical data is to mission continuity. However, there is a discrepancy between this and how agencies rate their cyber efforts. According to a recent study[1], 84% of Federal IT managers agree cybersecurity is a top or high priority within their agency, yet, just 51% rate the state of cybersecurity within their agency as "very effective." Two-thirds of those surveyed (66%) say the possibility of being the next headline-grabbing cybersecurity breach keeps them up at night. While ongoing budget constraints are always top of mind, some other challenges to formulating agency-wide cyber strategies according to respondents are:

- → Understanding evolving cybersecurity threats
- → The challenges of migrating to the cloud
- → Understanding technical vulnerabilities
- → Lack of collaboration between agency leaders and security leaders

Cyber criminals are opportunists that continuously evolve their methods of attack. And, as history has shown us, the government is often a primary target – with bad actors employing every tool in their arsenal to get around systems. In this environment, tactical agencies and their mission partners continue to grapple with the challenge of communicating securely and accessing mission critical information over distributed mission and partner networks, while enabling mobility.

In order to compete, agencies recognize a need to truly commercialize technology making it more scalable and usable to mission-focused environments. As the Department of Defense (DoD) becomes increasingly more global and mobile, programs and agencies are turning to Commercial Solutions for Classified (CSfC) solutions to address these challenges.

The National Security Agency (NSA) Information Assurance Directorate (IAD) introduced CSfC to strengthen the national cyber posture by allowing commercial solutions to be used to protect National Security Systems (NSS). CSfC outlines a list of components vetted against a common framework to meet NSA IAD's security requirements. CSfC is built on three pillars. First, the National Information Assurance Partnership (NIAP) evaluates and certifies components for inclusion in CSfC components. Next, each component must be layered to provide at least two independent capabilities. Finally, the components are tested for confidentiality and interoperability. The aim is to reduce time to certification from years to months or weeks. CSfC is how NSA executes its commercial cybersecurity strategy – architecting commercial products together in precise ways to protect classified information[2]. Stateful Traffic Filtering Firewall products used in CSfC solutions are validated by NIAP/CCEVS or CCA partnering schemes as complying with the current requirements of NIAP's collaborative Protection Profile for Network Devices (cPP ND) version 2.1 and PP-Module for Stateful Traffic Filtering Firewalls (MOD cPP FW) version 1.3. This validated compliance helps ensure that agencies adopting firewalls can adopt certified products that will enable both security and access to mission critical environments.

As agencies look to adopt CSfC approved firewall solutions, they must consider:

- → How to scale to support remote work and perform in a cloud connected world?
- → How to efficiently manage and scale physical, virtual, and cloud environments for fast and accurate deployment and maintenance of next generation firewalls (NGFWs)?
- → How to combat adversaries who are always evolving and using state-of-the-art intrusion techniques like evasions to take advantage of design flaws in many NGFWs?

Agencies now require elasticity for seamlessly scaling in physical, virtual, or cloud environments. Agencies must be able to rapidly increase or decrease connectivity and security at any point in the network and apply configurations throughout the network and dynamically adapt to changes in topology or

1 https://www.meritalk.com/study/federal-cybersecurity-in-a-changing-world/
2 https://www.nsa.gov/Portals/70/documents/resources/everyone/csfc/newsletter/bits-and-bytes-vol01-issue01.pdf

organization. Automating the provisioning and deployment of physical, virtual, and cloud to quickly enable new sites or workloads through centralized management across all environments becomes important in today's world. This enables administrators to efficiently deploy system policies to provide full visibility across the entire enterprise network and enables agencies to automate provisioning and orchestration to scale up cloud and virtual security.

Cyber criminals use sophisticated techniques to leverage trusted systems to obfuscate malicious data and penetrate agency network defenses undetected. An advanced evasion technique (AET) is a method of delivering an exploit or malicious content into a vulnerable target so that the traffic looks normal and security devices will pass it through. By combining attacks using several protocol layers, these advanced evasions bypass most existing security solutions because:

- → Many network security devices use packet-based inspection. This simplistic approach attempts to identify each and every evasion combination, determine whether or not it's dangerous, and then creates its own customized defense. Yet, each combination of evasions provides a new way to bypass traditional networking checks.
- → Patches for known exploits are ineffective against advanced evasions. Most organizations experience a delay before they are able to deploy patches for known vulnerabilities. Intrusion prevention, whether part of a NGFW or a standalone IPS, is intended to detect signs that an attacker is trying to exploit vulnerabilities that haven't been patched. However, evasions can hide these exploits from detection by traditional intrusion detection devices, allowing them to target endpoints, servers, databases, and other systems.
- → Many devices take shortcuts that sacrifice security for speed. Network security devices should defend against evasions at each layer in the networking stack, but many products take shortcuts, favoring speed over security. While this sometimes allows devices to operate faster, it leaves the network wide open to attack.
- → Lab testing may only be limited to previously identified exploits. Many security vendors tout performance against simulated and recorded evasions produced in predefined lab environments. When facing evasions, these systems typically go blind and allow exploits and malware into your systems and data.

Forcepoint NGFWs are designed to connect and protect people and the data they use throughout the enterprise network – all with the greatest efficiency, availability, and security. Trusted by thousands of customers around the world, Forcepoint network security solutions enable businesses, government agencies, and other organizations to address critical issues efficiently and economically. Forcepoint's NGFW Series are eligible to be used as a traffic filtering firewall component in a CSfC solution[3].

Forcepoint's NGFW solution combines:

- → **Enterprise Connectivity** – Direct-to-cloud application routing combined with site-to-site VPNs, made scalable and resilient with advanced, mixed-device clustering.
- → **Extensible Security** – Market-leading intrusion prevention and access control that's integrated with cloud-based Forcepoint Web Security and Cloud Application Security Broker (CASB).

3 https://www.nsa.gov/resources/everyone/csfc/

→ **Management at Scale** – Real-world experience handling more than 1,800 sites from a single pane of glass with zero-touch deployment and rapid, interactive incident response.

Forcepoint NGFW combines fast, flexible networking (SD-WAN and LAN) with industry-leading security to connect and protect people and the data they use throughout diverse, evolving enterprise networks. Forcepoint NGFW provides consistent security, performance, and operations across physical, virtual, and cloud systems. It's designed from the ground up for high availability and scalability, as well as centralized management with full 360° visibility.

For agencies with site-to-site connectivity, or a distributed remote workforce, connecting all of the sites and users together is called a mesh and at scale it can be expensive, time consuming, and difficult to administer. With Forcepoint, customers can take full advantage of our VPN Client, which can be deployed easily without any additional costs to the consumer.

Forcepoint's government customers are able to improve how their VPNs are set up and ensure their architectures can scale for increased remote connectivity. The connectivity among the sites is designed so they can dynamically determine how to connect to each other. With on-demand VPNs, agencies can:

→ Configure VPNs centrally and update dynamically

→ Connect sites directly without creating bottlenecks due to backhauling

→ Scale to thousands of sites

→ Use public and private links seamlessly

This is important because it allows neighboring organizations to communicate more effectively. Instead of manually configuring every location, connectivity becomes dynamic. This allows a smaller equipment footprint at each site, with less complexity. Overall, this reduces cost as well as risk of network outages.

Forcepoint network security solutions are also seamlessly and centrally managed, whether physical, virtual, or in the cloud. Administrators can deploy, monitor, and update thousands of firewalls, VPNs, and IPSs in minutes, all from a single console – cutting network operating expenses by as much as 50%. Advanced clustering for firewalls and networks eliminates downtime, and administrators can rapidly map business processes into strong, accurate controls to block advanced attacks, prevent data theft, and properly manage encrypted traffic – all without compromising performance.

When it comes to security, for many years Forcepoint Sidewinder proxy firewalls have secured some of the most sensitive mission-critical environments. Now, the best of Sidewinder's application proxy technology is incorporated into the Forcepoint NGFW, providing even greater protection. In fact, Forcepoint's NGFW has been ranked at the top in both of NSS Labs' key tests of network security, including NGFW and NGIPS. Forcepoint also offers the industry's leading technology for detecting advanced malware.

Forcepoint NGFW pioneered evasion defenses. Forcepoint NGFW incorporates a variety of threat-discovery techniques that examine network traffic across its different layers. Forcepoint's approach not only identifies applications and users at a granular level, but also ensures that tricks such as out-of-order packet transmission or adulterated TCP acknowledgements can't be used to get malicious content through. The Forcepoint firewall provides unrivaled effectiveness in defeating evasions and is constantly updated to detect the newest, most advanced threats.

Forcepoint NGFW enables agencies to leverage next generation capabilities without sacrificing evasion protection or the application level security relied upon to protect mission critical data. Forcepoint NGFW offers a more effective and efficient approach, performing deep, full-stream inspection that:

- → Works uniformly across physical, virtual, and cloud deployment
- → Can be used as a standalone IPS or a full-function NGFW
- → Is unsurpassed in detecting malicious traffic
- → Is the pioneer in defeating evasion techniques
- → Provides interactive visibility across the entire enterprise network
- → Makes it easy to block offending sessions permanently

Forcepoint is committed to enabling organizations to empower employees with unobstructed access to confidential data while protecting intellectual property and simplifying compliance. As part of this commitment, Forcepoint maintains numerous global industry certifications and compliance for our products to ensure we meet and exceed deployment, documentation, security functionality, and security posture standards across the industry. All Forcepoint NGFW Appliances are powered by a unified core and offer consistent capabilities and management across all platforms. They are rigorously tested and have received many certifications required by government[4].

Immediate benefits from implementing Forcepoint NGFW include cost savings, increased capacity, higher availability, faster speeds, quicker deployment, and greater agility[5]. Specifically, IDC research[6] found that by switching to Forcepoint, customers saw 70% less maintenance downtime, 53% savings in IT staff time, and 86% fewer cyberattacks. These numbers would make a significant difference to any Federal agency.

Forcepoint NGFW offers a single source of protection across endless endpoints and is backed by Forcepoint's leading cybersecurity capabilities. Accessible anywhere, and scalable to fit your agency's needs.

Learn more about how Forcepoint NGFWs can enable your modernization in this latest ebook: The Network's Role in Modernization.

4 https://www.forcepoint.com/certifications/ngfw-certifications
5 https://www.forcepoint.com/form/thank-you-your-interest-ebook?form_id=1363&file=29831&resource=25181&category=ebooks
6 https://www.forcepoint.com/product/ngfw-next-generation-firewall

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.