ARMING DEFENSE AND INTELLIGENCE COMMUNITY ORGANIZATIONS WITH SECURITY RESILIENCE

How next-generation firewalls improve security controls for dynamic environments and reduce security complexity for global operations.

> A Scoop News Group Report

Network boundaries are drastically changing, opening new attack vectors for threat actors to target across IT infrastructure, operational technology, application supply chain and user accesses. The challenge this presents for defense and intelligence agencies is finding the balance between modernization initiatives while ensuring the security of classified information across their global operations.

One approach to securing the network is to add security tools and capabilities as the environment changes. But while that served certain purposes in the past, this has also added a great deal of complexity to the security environment making it difficult to manage in terms of both resources and a skilled workforce.

To improve security resilience and remain operational during disruptions, agency leaders need to consider next-generation firewall (NGFW) solutions that improve interconnectivity between their existing security tools in order to quickly adapt to changes across their networks.

WHAT IS DRIVING CHANGE?

The United States Air Force has often been lauded as a forward-thinking organization in terms of its IT investment strategies. In **a recent FedScoop interview**, James "Aaron" Bishop, CISO for the Department of the Air Force spoke about the challenges of defining the network perimeter and how they are securing their substantial IT environment.

Bishop referred to the Air Force as operating "150 little cities around the world," that encompasses a vast IT infrastructure with technology running on different lifecycles that needs to be upgraded, maintained, patched and replace.

"But as a warfighting mission," he explained, "I also have to extend that capability beyond that base. So now my networks have to go into expeditionary communications and extended aerial networks, etc. Now I need to understand where is that perimeter, where do I protect it [and] where do I pass it on to the next environment that may or may not be there today or tomorrow?"

"I challenge all my authorizing officials to look at where is the boundary I'm trying to protect and where is the data that I'm protecting within it. If I need to move that data, I need to understand where that protections go with that data. And so therein lies the change in the evolution of firewalls and perimeter defense," said Bishop.

"For federal agencies who deal with different classification levels, NGFWs are a necessary architecture upgrade that can better support the mission."

- Chris Crider
Security Systems Engineering Leader
Cisco

REDEFINING PERIMETER SECURITY

What Bishop, and many leaders across both the government and private sector are leaning into is a more modern approach to firewalls that relies on dynamic packet filtering rather than stateful packet inspection of network traffic.

"Firewalls and packet inspection is a key aspect to layers in defense, but it is no longer the bastion protection of a perimeter," shared Bishop in his interview, published in FedScoop on March 31, 2023. "'Where is a boundary?' is now the question of the hour. Is it the network I control, the cloud instance I control, the application I control? The reality is that it is all of these, plus where the data is."

NGFW can protect a wide array of network infrastructures, connected devices and operating systems from advanced threats. They can be embedded into the network, on a host, included in cloud environments, or with clustered appliances that scale to large traffic requirements, as software that runs on personal devices, on SD-WAN routers and secure Internet gateways.

Modern firewalls function as micro-perimeters that sit closer to the information or applications that need to be protected. It logs activity across disparate firewall devices, regardless of their location, and analyzes it against threat intelligence to create more uniform threat visibility and a stronger security posture.

"For federal agencies who deal with different classification levels, NGFWs are a necessary architecture upgrade that can better support the mission," explained Chris Crider, security systems engineering leader at Cisco. "While in the past firewalls were viewed as an enforcement and an inspection point for perimeter defenses, NGFWs help connect enforcement and inspection to the broader system that meets the criteria for initiatives like zero trust or secure service edge (SASE)."

NGFWs can see and block risky applications, block advanced malware and address evolving security threats to keep pace with the changing threat landscape. Application awareness makes security policy controls more dynamic. For example, a policy can follow a workload across a multi-cloud environment.

> **"[With Next Generation Firewalls] DOD and IC organizations can build and implement policies and additionally utilize security group tags to specify the privileges of a traffic source within a trusted network."**
>
> - Norman St. Laurent
> Cyber Security Specialist
> Cisco

"That means that DOD and IC organizations can build and implement policies and additionally utilize security group tags to specify the privileges of a traffic source within a trusted network. Then migrate into any cloud to provide services globally and take the analytics and logging to monitor traffic with a single pane of glass," added Norman St. Laurent, cyber security specialist at Cisco. "With NGFW organizations can always monitor what is happening on the network, have a holistic view of activity and full contextual awareness to see threat activity across users, hosts, networks and devices."

BUILDING SECURITY RESILIENCE

Over time organizations have acquired tools for their stateful firewalls, intrusion detection system, intrusion protection system, workload security, endpoint security, threat intelligence and encrypted traffic analysis. So, reducing complexity is one of the biggest pushes for organizations to adopt NGFWs because they wrap-up many security capabilities into one service.

A recent study, produced by Scoop News Group, asked 165 prequalified government leaders about the state and strength of their current security posture and explored trends around security complexity in federal government.

More than half (55%) of respondents reported that their security tools function moderately to completely independently from their suite of solutions. And 33% said their organization uses between 11 to 40 different vendors across their security technologies, while 11% use more than 50 security vendors.

"I remind people that there are over 3,100 U.S.-based security vendors — tens of thousands across the world — and while I will never argue against the necessity of a security tool, I do stress that at some point these innovations need to either work with something else or be bought by somebody," explained Crider. "At some point, leaders have to make choices on how to best implement security in their environment."

Second to reducing complexity is building resilience against modern threats. Malicious actors continue to develop advanced capabilities and organizations need to distinguish "friendly" traffic from "malicious" traffic.

While encryption ensures the confidentiality of data in motion, it is also a technique used by attackers to hide malicious payloads.

"Encryption is a huge challenge for everyone, and obviously, with an organization at my scale it's a massive problem as well," shared Bishop. "Encrypting traffic is key for confidentiality and being able to say I've got the data protected while in transit, as well as encryption at rest. But the issue then becomes, as I'm moving that data around, does the encryption go with it? Do I encrypt between the two and is that sufficient — aka, a tunnel VPN or something along those lines. Or is it something I need to worry about?"

NGFWs with embedded encryption visibility gives organizations the ability to not only check the efficacy and type of encryption on a payload, but with integrated threat intelligence the firewall can match analytics to known threats and determine if the traffic is malicious, stopping a threat before it even enters the network.

The **Cisco Security Analytics and Logging (SAL)** solution supports sources of traffic, including event logs from Cisco's firewalls, which can be combined with flow logs from internal network elements and cloud infrastructure for enhanced end-to-end visibility. This functionality therefore provides aggregated analysis by correlating logs generated at the perimeter, private network and public cloud infrastructures.

IN A SURVEY OF FEDERAL GOVERNMENT IT DECISION MAKERS:

55% said security tools function moderately to completely independently from their suite of solutions

33% said their agency uses between 11 to 40 different vendors

11% said their agency uses more than 50 different vendors

Source:
Scoop News Group study (January 2023)

> “I remind people that there are over 3,100 U.S.-based security vendors — tens of thousands across the world — and while I will never argue against the necessity of a security tool, I do stress that at some point these innovations need to either work with something else or be bought by somebody”
>
> - Chris Crider
> Security Systems Engineering Leader
> Cisco

PARTNER WITH PROVEN LEADERS

Finding the right partner to begin integrating security solutions is an important step. **According to Gartner**, organizations should look for some of the following key capabilities when implementing an NGFW:

- Standard firewall capabilities like stateful inspection.
- Integrated intrusion prevention.
- Application awareness and control to see and block risky applications.
- Threat intelligent sources.
- Upgrade paths to include future information feeds.
- Techniques to address evolving security threats.

Keeping up with all the IT demands and security needs can be overwhelming, but according to Crider, incremental innovations to solve security problems is better than spending valuable resources and budget dollars to overhaul the system.

“Cisco has ATOs today with everything in place, so we encourage our partner community in the federal government to evaluate what they are looking for today and see how we can help,” Crider explained.

Cisco firewalls have the Common Criteria (NDcPP, FW MOD, VPNGW MOD, IPS MOD) Certification as well as FIPS 140-3 Level 2 (all crypto, including management and VPN) on hardware appliances and Level 1 on virtual firewall appliances as well as USGv6 (NDP/HOST) Certification.

Learn more about integrating a firewall solution that will adapt with your organization’s evolving network needs.

This report was produced by Scoop News Group, for FedScoop, and underwritten by Cisco.

FEDSCOOP

CISCO