SONICWALL®

EXECUTIVE BRIEF

What's the Best NGFW for State and Local Governments?

Mobility, cloud apps and emerging threats demand more from today's next-gen firewall

Abstract

State and local governments are increasingly dependent on cloud-based apps and mobile connectivity. Meanwhile, cyberthreats are on the rise, and compliance and security requirements are more stringent than ever. Government agencies must embrace a boundless network security approach. This brief examines critical network security needs for today's agencies and explores best practices for selecting an effective next-generation firewall platform.

Introduction

Teleworking and cloud-based collaboration have opened state and local government networks to more cloud-based apps and connected mobile devices. IT departments are under increasing pressure to secure their data from continually evolving, evasive network attacks at faster speeds. The exponential rise in the number of connected endpoints, including IoT devices, has created more threat vectors for cybercriminals to launch advanced attacks such as zero-days and ransomware, many of which execute within memory.

In addition, government networks require continuity to ensure the flow of information and the services they provide across their network. To meet today's demands, IT directors need a highly reliable next-generation firewall that not only can scale to support a massive number of devices and encrypted connections simultaneously, but can also scan them for threats without compromising performance.

While risk escalates, more demand is placed upon constrained resources. Utilizing a cost-effective and easily manageable next-generation firewall that can handle the available bandwidth and support multiple networks and clouds has proven elusive. Cost becomes prohibitive, and the shortage of trained personnel becomes more acute.

State and local governments need to shift from conventional security models to a boundless network security approach that embraces mobility and the cloud. Network security today needs to be always on, always learning, and always ahead of emerging threats.

Network complexity

Government networks support diverse user groups. Each might require access to unique subnetworks or cloud environments. Security must operate across several segmented networks, clouds or service definitions, each of them with unique templates and device groups, often with different policies.

Moreover, such network diversity can include an inherent legacy of multi-vendor network security solutions. IT administrators do not want to manage separate firewalls for each of these networks or service definitions. Furthermore, they often need to service multiple user groups who each require unique configurations and, in some cases, must supply a clean pipe to them.

With numerous security devices covering various networks, managing access and security policies can become complicated and burdensome. Complexity can often create difficulties with security monitoring, access control, regulatory compliance and rapid mitigation. Inefficient management creates security bottlenecks and decreases business agility. This also contributes to greater operational overhead costs.

Best practices suggest that an effective firewall must integrate security services that can protect SaaS resources and cloud-based resources, as well as secure mobile and IoT endpoints.

A unified policy interface is necessary to enable primary schools to simply and intuitively create access and security policies globally across a diverse distributed network. Features designed to simplify deployment and setup while easing management can further help state and local governments to lower their total cost of ownership and realize a higher return on their security investment.

The need for speed

As government networks evolve and grow, they increase encrypted connections, endpoint devices, networks, cloud workloads, users and internet speeds. A firewall that cannot support any one of these becomes a bottleneck in the IT landscape. A firewall is meant to be a high-performing security check, not a point of weakness. With 70% of all sessions being encrypted, having a firewall that can process and examine this traffic without impacting the end-user experience is critical to productivity and information security.

An effective firewall should deliver scalability, reliability and deep security for simultaneous connections at multi-gigabit speeds. A best-practice multi-instance firewall will ensure high quality-of-service levels, with uninterrupted network availability and connectivity over 100 Gbps infrastructures.

Growing risks

The threat landscape continues to evolve as threats become increasingly evasive. SonicWall encounters and catalogs over 140,000 new and updated forms of malware every business day. These variants are updated frequently to bypass static filters in a variety of devices and services. Furthermore, many attackers outsource components, such as evasion tactics, boot lockers or runners, in order to make their malware more difficult to detect.

State and local governments are also increasingly at risk from attacks via IoT devices. Gartner estimates that there are over 20 billion IoT devices active today. By 2025, IDC expects that there will be over 41 billion IoT devices generating close to 80 zettabytes of data, much of it behind firewalls. Worse, many of these IoT devices will be unmanaged. Without controlled access to unmanaged devices, their common vulnerabilities can be exploited and can't be patched or managed by IT.

Unmanaged SaaS applications pose another risk. Government agencies use multiple software applications to enhance productivity and increase collaboration. Some of these applications are purchased with a license by the organization, such as Office 365, Teams or Jira. These are licensed, managed and sanctioned applications.

However, agency staff members increasingly use unlicensed and unmanaged applications that their IT departments either do not know about or do not approve of. This is known as shadow IT, and examples can include Dropbox or Google Drive. Seldom do state and local governments have knowledge about the compliance concerns, or threats involved in using these unsanctioned applications. Consequently, as they can have vulnerabilities that IT doesn't know about and are not sufficiently monitored or controlled by IT, these apps constitute an avenue for data leakage and breaches through stolen credentials and malware.

To address these risks, an effective next-generation firewall must ensure that every byte of every packet is inspected, while maintaining the high performance and low latency that busy networks require. Optimally, it should provide simultaneous, multi-threat and application scanning, as well as analysis of any size file, without packet reassembly. It should also be able to deliver fast response and continuous protection against zero-day threats from real-time intelligence updates that gather, analyze and vet cross-vector threat information from a multitude of global sources.

Conclusion

State and local governments need boundless security without compromise. This requires advanced threat protection and fast speeds at a minimal total cost of ownership. Best practices include multi-instance architectures and unified policy creation to make defending networks simpler and more effective.

SonicWall can help. The SonicWall Network Security services platform (NS*sp*) 15700 is a next-generation firewall with high multi-gig port density and throughput over 100 Gbps, which can process several million connections while inspecting for zero-day and advanced threats. It eliminates attacks in real time without slowing performance and is purpose-built to be highly reliable and deliver uninterrupted services.

Learn more. Visit www.sonicwall.com/products/firewalls/high-end

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

ExBrief-WhatsBestNGFWStateLocalGov-VG-3142