Editorial Brief

Ten Must-Have Features for Your Next Generation Firewall

Find the right fit to protect your enterprise.

The need for extreme protection may be the driving force behind your decision to invest in a next-generation firewall (NGFW), but your enterprise also has other factors to consider. You want an NGFW that ensures business resiliency, a reasonable total cost of ownership (TCO), continuous uptime, scalability, and flexibility to handle change. It must fit your budget and your network's specific needs. Find an NGFW that meets the following criteria, and you will find an NGFW that meets those demands.

1. Central, Powerful Management

Logging into multiple firewalls and other components to make changes or view activity can burden your scarce resources. Look for a centralized management system that aggregates data across your security defenses and gives your security team the ability to respond quickly. A centralized system should let you deploy, view, and control all firewall activity through a single pane of glass. Central management should also give you the ability to automate routine tasks, reuse elements, and employ shortcuts and drill-downs to produce maximum efficiency with minimal effort.

2. User and Application Control

User and application control has become a must-have feature for NGFWs as the Internet continues to offer myriad places to lure employees away from productive activities. Application controls have advanced significantly beyond just visibility of ports and protocols. Now you should have the power to create detailed policies that can be based on characteristics such as user identity, user role, and specific aspects of a web application. Also look for more advanced user and application controls, such as the ability to expand user groups, domain names, and transport layer security (TLS) matches, as well as detailed user and application usage information in reports, logs, and statistics.

3. High Availability

Most consider downtime unacceptable on corporate networks even for routine maintenance. One key feature to achieving high availability and resiliency is the use of active-active clustering of your NGFW. Active-active clustering gives you uninterrupted operations during system updates and maintenance, allowing increased flexibility when process-intensive applications require more performance. Clusters should be able to be upgraded node by node without service breaks, operating with different software versions or hardware variants during maintenance.

intel Security

4. Plug-and-Play Deployment

If your enterprise encompasses many distributed locations, you need to find an NGFW that features plug-and-play capability. Using the cloud for installation and configuration, your NGFW should be easily installed by anyone at the remote location by plugging in power and physical network connectivity. The rest should be handled remotely. The savings in time and travel costs can be significant, often reducing implementations from weeks to minutes. Updates and upgrades to remote sites can be automated and performed just as seamlessly, with the ability to view and manage remote operations through the central management system.

5. Deep Packet Inspection

Deep packet inspection (DPI) is another must for your NGFW. This capability ensures that the various pieces of each packet are thoroughly examined to identify malformed packets, errors, known attacks, and any other anomalies. DPI can rapidly identify and then block Trojans, viruses, spam, intrusion attempts, and any other violations of normal protocol communications. Packet data analysis is typically done through various methods, including data stream-based inspection, vulnerability signatures, policy configurations, protocol identification and data normalization, and both clear-text HTTP and encrypted HTTPS connections. NGFWs equipped with DPI capabilities should also provide dynamic updates that can be automated, regularly updating recommended policy configurations and vulnerability-based protection fingerprints.

6. Protection Against Advanced Evasion Techniques

Advanced evasion techniques (AET) are notorious for their ability to combine attacks, change dynamically during attacks, and use several protocol layers, all with the intent of delivering malicious content or an exploit through a traffic stream that appears normal to less advanced security solutions. AET protection technologies remove obfuscations so traffic can be thoroughly inspected across multiple protocols and layers, providing full-stack, multilayer traffic normalization that deconstructs and decodes packets. When AET protection is built right into the core of the NGFW, even the most thorough data analysis and normalization does not impact network performance.

7. Multitenancy

Large enterprises and managed service providers have an essential need for an NGFW with multitenancy capabilities. This feature ensures distinction between domains to properly secure end users without sacrificing efficiency. Multitenancy capabilities provide separate but interoperable domain management abilities, which can also apply to separate business units, geographical locations, or external customer organizations. While multitenancy allows entities to remain separate, all enjoy the same situational awareness, administrative tools, automated functionality, constantly optimized connections, and other features available through your NGFW.

8. Adaptable, Convertible Architecture

The architecture of your next NGFW needs to be adaptable and convertible so you can most effectively deploy security as you need it. Look for an NGFW that is available as software or a physical or virtual appliance for the highest range of budgetary and architectural flexibility. Insist on a solution that can also change its roles as needed, serving as an NGFW, intrusion prevention system (IPS), layer 2 firewall, or firewall/VPN without the need for new licensing.

9. Enterprise-Level VPN

For resilient and flexible site-to-site connectivity, powerful virtual private network (VPN) technologies must be part of your NGFW. Many NGFWs feature IPsec VPN, which consists of a set of security protocols inserted at the packet processing layer of communication. IPsec comes with several advantages, one of which is the ability to handle security arrangements without the need to implement changes on individual computers. Look for NGFWs that can add even more power to your VPN by combining IPsec VPN with other advanced technologies, such as those that may combine links or tunnels to produce a cost-effective and highly available VPN connection. Make sure your NGFW has sufficiently powerful management tools to deploy, configure, and operate your VPNs.

10. Virtualization

With virtual appliances, you can easily and independently deploy a comprehensive security infrastructure using virtual machines. Each virtual appliance can serve an independent role, and even run its own software version and operating system. Virtual contexts offer a way to logically divide security gateway configurations into separately manageable instances on a single physical NGFW appliance. This approach is ideal for managed security service providers, who offer and manage security services for multiple customers using the same physical elements.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com