SonicWall Next-Generation Firewall Buyer’s Guide

How to choose the right next-generation firewall to secure your network

SONICWALL®

Table of Contents

Executive Summary

Ransomware is up. IoT attacks are up. Encrypted threats are up. In a rapidly changing IT landscape — one characterized by companies rushing headlong into the cloud, network traffic percent increases in the double digits, and BYOD and remote work policies — cybercriminals are enjoying unprecedented opportunities. And protecting against these attacks is becoming increasingly challenging, as businesses need to protect multiple attack surfaces and implement the latest security controls just to keep up.

The enterprise perimeter now extends to anywhere work gets done. And regardless of whether your entry points are on-premises, in the cloud, in the data center or at the branch office, each one needs to be protected. The good news is that security defenses have evolved, too — particularly firewalls, the most important security defense to protect any enterprise perimeter, including those of distributed and diffuse enterprises.

The firewalls of today are more agile, more capable and more powerful than when the technology debuted 20 years ago. As enterprises consider these next-generation firewalls (NGFW), there are several criteria that should be considered, including features, platform capabilities, performance and management.

Evolution of the Firewall

Cybercrime looks nothing like it did two decades ago. Fortunately, neither do firewalls: Today's next-generation firewalls feature a host of new security controls, significantly higher performance and a great variety of form factors. How do these firewalls compare to their early ancestors? Let's take a look:

Access Control Lists (ACLs) or Stateless Firewall

Network ACLs have existed for a long time. They are used to filter network traffic. With ACLs, traffic can be allowed or denied in both inbound and outbound directions. Network ACLs are typically configured in routers, switches or servers using layer 2 to layer 4 rules based on IP address, MAC address and ports.

A typical ACL rule in a network device looks as follows:

```
<Rule Number> <ACL Name> <Source IP / Port> <Destination IP / Port> <Allow / Deny>
```

ACLs inspect individual packets but do not inspect flows or maintain state of the flow.

Stateful Firewall

Stateful firewall is different from ACLs or stateless firewall, mainly because they can inspect network connections all the way from layer 2 to layer 7. Stateful firewalls maintain the context of a given connection. This means packets are matched to connections they belong to, offering additional security to prevent hacking techniques like spoofing. Some stateful firewalls can also perform deep packet inspection and can be installed on dedicated hardware.

Zone-Based Firewall (ZBF)

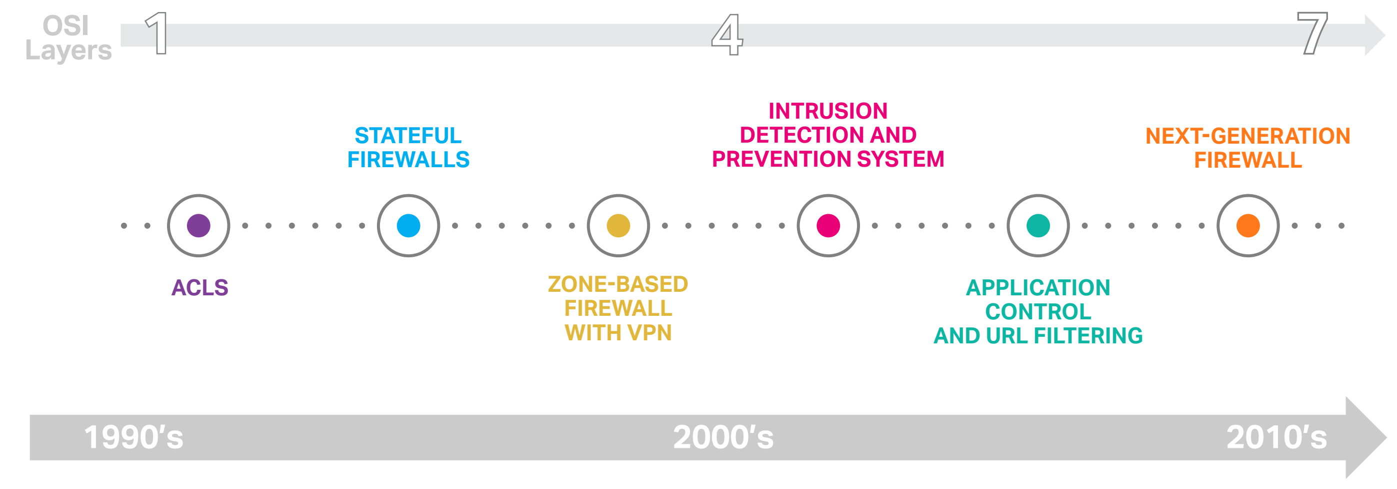
Zone-based firewall is like stateful firewall, except it is configured using more advanced networking concepts. Instead of assigning rules based on connection and interfaces, an administrator would create zones and assign multiple interfaces to those zones. Some of the common zones used are LAN (private or trusted), WAN (public or untrusted) and DMZ (demilitarized zone). Multiple zones can have rules to fully inspect, allow or deny connections.

Unified Threat Management (UTM)

UTM firewalls were originally designed to consolidate multiple stand-alone security controls into a single appliance. Security controls (such as firewall, intrusion prevention, URL filtering and antivirus) are combined into a single operating system and management console. This solution is ideal for small and medium-sized businesses that do not have a big security budget, or do not have high performance and scalability requirements.

Next-Generation Firewall (NGFW)

The concept of NGFW was first defined by Gartner, publisher of the Magic Quadrant for Network Firewalls. NGFWs have the option to add all the security controls that are available in UTMs, as well as advanced controls such as VPN, user control, application control and sandboxing. Apart from advanced security controls, NGFWs are designed to support the high performance and scalability needs of large enterprises. The rest of this document will focus on NGFWs and different factors that enterprises should consider in their buying decision.


OSI Layers
1
4
7
STATEFUL FIREWALLS
INTRUSION DETECTION AND PREVENTION SYSTEM
NEXT-GENERATION FIREWALL
ACLS
ZONE-BASED FIREWALL WITH VPN
APPLICATION CONTROL AND URL FILTERING
1990's
2000's
2010's

Essential NGFW Capabilities

Zone-Based Firewall (ZBF)

ZBFs offer stateful inspection with advanced network security features for large enterprise network infrastructure. A ZBF or stateful firewall is the foundation for any NGFW, and a basic requirement to support other features. Choose ZBFs over stateful firewalls for enterprises with large networks, as it is easier to configure and define policies with ZBFs.

Virtual Private Network (VPN)

Distributed enterprises typically have remote branch offices that need secure access to the corporate network. The recent expansion in Work-From-Home (WFH) policies has also resulted in many employees working remotely. VPNs provide robust, secure access to corporate networks and resources, so it is essential to consider VPN as part of your NGFW.

It is important to make sure the NGFW provides a comprehensive VPN solution with site-to-site and remote-access encryption. It should include advanced features such as route-based VPN and easy VPN with dynamic routing. A VPN is also important in case you are considering an SD-WAN solution.

VPN configuration should be simple. It needs to be managed from within the NGFW user interface, with configuration wizards that provide step-by-step guidance in setting up the VPN tunnels. Enterprises should consider a VPN concentrator at the edge to manage both IPsec and SSL VPN connections.

Intrusion Prevention System

Intrusion Detection and (or) Prevention System (IDS/IPS) was originally developed as a stand-alone solution, which later became part of the NGFW stack. IPS within the NGFW provides an additional layer of needed security by stopping attacks that exploit vulnerabilities. The intrusion detection is done using signatures for known exploits, and is based on anomaly detection.

IPS within the NGFW can be deployed in detection mode (alert only) or in prevention mode (alert and block). There is no performance penalty for detection mode compared to prevention mode. Initially configure IPS in detection mode before moving to prevention mode to understand exploits, explore false positives and perform incident responses. An important aspect to look for in an IPS is the threat intelligence feed that keeps the signature database up to date in the NGFW.

Application Control

NGFWs came into fruition with the addition of application control, IPS and URL filtering, forming a single enterprise-class platform. Application control allows enterprises to define firewall policies based on applications (e.g., Facebook, YouTube, Salesforce) and micro-applications (e.g., chat and IMs). Application Control gives granular control over network traffic based on user identity and email addresses while providing application-layer access control to regulate web browsing, file transfer, email exchange and email attachments.

Look at the type of applications that are included in a NGFW database to make sure all the applications that are in use within the enterprise are supported.

Web Control (URL Filtering)

Web control compares requested websites against a massive database containing millions of rated URLs, IP addresses and domains. It enables administrators to create and apply policies that allow or deny access to websites based on individual or group identity, or by time of day, using pre-defined categories. It also dynamically caches website ratings locally onto the NGFW for instantaneous response times. An NGFW should be able to do URL filtering based on business point of view (block based on category – business) as well as based on security (block based on reputation – security).

Consider NGFWs with threat intelligence feeds that is supported by world-class research team for IPS, application control and web control to make sure NGFW stops latest threats.

> “This year, we have also seen VPNs as one of the top security features being used by customers.”

2019 MAGIC QUADRANT FOR NETWORK FIREWALLS

Selecting Advanced NGFW Features

Network and Cloud Sandboxing

For effective zero-day threat protection, enterprises need NGFWs that include malware-analysis technologies and can detect evasive advanced threats. Sandboxing technology scans traffic and extracts suspicious code for analysis, but unlike other NGFW security controls, it also analyzes a broad range of file types and sizes. This enables enterprises to stop zero-day and evasive threats that can slip through other security controls within NGFW.

Enterprises need to consider solutions that offer both on-premises and cloud-delivered sandboxing based on their performance and privacy needs. This technology should be augmented with global threat intelligence infrastructure that rapidly deploys remediation signatures for newly identified threats to all NGFWs in the enterprise, thus preventing further infiltration.

Enterprises should consider sandboxing technology that examines every byte until the last byte before delivering a final verdict to allow or block. This avoids any false positives or negatives and ensures that highly elusive zero-day threats are blocked.

Multi-instance firewall

Multi-instance is a modern next-generation approach to legacy multi-tenancy that supports multiple firewalls with separate configuration on a single appliance. With this approach, each firewall instance is isolated with dedicated compute resources to avoid resource starvation. This allows enterprises to use containerized architecture. Enterprises can run multiple independent firewall instances, software versions and configurations on the same hardware without managing different physical appliances.

Look for dedicated threat intelligence when evaluating NGFWs.

Dedicated Threat Intelligence

As mentioned earlier, most of the security controls in an NGFW should be augmented by threat intelligence to keep them up-to-date on the latest threats and signatures, among other things. Threat intelligence feeds should be supported by a research team that gathers, analyzes and vets information round the clock and across the globe. Look for vendors with a dedicated team of cybersecurity professionals, advanced machine learning algorithms and security sensors that are spread around the globe to deliver up-to-date threat feeds that automatically block threats in nanoseconds. While looking into threat intelligence in NGFWs, it is important to consider DNS security that protects enterprises against malicious domains.

Networking Requirements

An enterprise-grade platform and operating system are at the core of any physical or virtual NGFW. There are many networking features within the operating system that make a big difference in evaluating and choosing your next NGFW. The following are a few that should be considered in enterprise deployments:

SD-WAN Security

SD-WAN technology allows organizations and enterprises with branch locations to build highly available and higher-performance WANs. By using low-cost internet access (broadband, 3G/4G/LTE, fiber), organizations can cost-effectively replace expensive WAN connection technologies such as MPLS with SD-WAN. SD-WAN Security enables distributed enterprises to build and protect high-performing networks across remote sites against cyberattacks.

High Availability/Clustering

NGFWs should support Active/Passive with state synchronization in high availability mode and Active/Active in clustering mode. It should also support the ability to offload the deep packet inspection load to passive appliance and to boost throughput.

Encrypted Traffic Inspection

This decrypts and inspects TLS/SSL encrypted traffic on the fly, without proxying. It also applies control policies to protect against threats hidden inside encrypted traffic. Enterprises should make sure that the NGFW supports the latest version of encryption protocols, such as TLS 1.3.

Top five capabilities needed in an NGFW platform:

- **Secure SD-WAN**
- **High Availability/Clustering**
- **Encrypted Traffic Inspection**
- **Multi-instance Firewall**
- **Dedicated Threat Intelligence**

Management

Enterprise-wide management of NGFWs is one of the most important considerations. This involves configuration of NGFWs and usability for day-to-day operations from a single-pane-of-glass console. This console needs to be able to manage most, if not all, security controls across multiple NGFWs deployed on-premises and in the cloud from a central location. Some of the important features that need to be considered are:

Unified Policy: This should provision layer 3 to layer 7 controls in a single rule base on every NGFW, providing admins with a centralized location for configuring policies.

Monitoring: Look for real-time monitoring, reporting and analytics to help troubleshoot, investigate risks, and guide smart security policy decisions and actions.

Cloud and on-prem: Configuration and management of NGFW should be available via the cloud or through an on-premises management system.

Scalability: It should scale to any size organization, managing networks with up to thousands of firewall devices deployed across many locations.

Console: Enterprises should look for a NGFW that uses a single pane of glass to manage all security functions, such as IPS, URL filtering and others, from a single location.

Technology Integration

It is important to consider the type of technology integrations that the NGFW supports. This allows enterprises to protect their existing investments. Some of the technology integrations to consider are:

SIEM: Integration with security incident and event management enables rigorous investigation of cybersecurity threats and examination of anomalous data.

IaaS: It should integrate with all major IaaS providers to support multi-cloud deployments across AWS, Azure or GCP.

Automation: It should enable business process automation through synchronized catalogs inventories, agreements and tickets.

Zero Trust Network Access (ZTNA): This augments the VPN to provide access to only sanctioned assets and networks while VPN provides layer 3 access.

NGFW Deployments

The three main deployments of NGFW are based on the environment: physical, virtual and cloud.

Physical: Enterprises should consider physical appliances for on-premises deployments that require high performance and connectivity. Physical appliances can offer more than 100 Gbps throughput and 100 GbE connectivity. Appliances come in various form factors and performance levels for different deployment needs from data centers to remote offices.

Virtual: NGFWs can be deployed in virtual environments. They can be managed using the same system that is used to manage physical appliance. There are a variety of virtual environments when choosing a virtual appliance. It is important to make sure that your environment is supported.

Cloud: Many companies are moving their data centers and applications to the cloud. NGFWs have evolved to support a variety of private and public clouds, including AWS, Azure, GCP and VMWare. Even if your organization has not yet embraced the cloud, it is important to select a vendor that supports all the major public clouds.

The three main deployments of NGFW are based on the environment: physical, virtual and cloud.

Price-Performance Ratio and Support

Price-Performance Ratio

Apart from security features, price and performance should also be considered. Every vendor has different models that vary widely in performance, and each one has different price points and pricing models. For example, physical appliances may have a one-time big purchase price with a few minor yearly subscriptions, while most cloud firewalls are priced based on yearly subscription.

Before getting into price/performance analysis, it is important to know the projected three-year or five-year total cost of ownership (TCO). Most vendors do not have an all-inclusive price; they will charge separately for appliance, licenses for different security controls and support. It is important to consider the cost of high availability pairs and clustering in calculating TCO.

After determining the total cost of ownership, you can perform price/performance analysis across different vendors. Let us say the three-year TCO came to $250,000 and the NGFW throughput is 100 Gbps. In that instance, the price/performance ration would be $250,000/100, or $2,500 per Gbps.

Support

Buying an NGFW is a significant and technically complex investment. Not only should you get support, but also choose a vendor that has excellent support ratings. Vendors provide many different support options, including simple phone support, on-site support and professional services. Enterprises can use professional services to help deploy, configure, tune and maintain their NGFWs to simplify operations. Support options also include availability by the number of days in a week and hours in a day, such as the examples shown below:

- Monday to Friday – 8 a.m. to 5 p.m. local time
- 24 hours and seven days a week (24/7)
- 24/7 with on-site support from a security professional
- 24/7 with continuous professional services support

Consider the cost of high availability pairs and clustering in calculating total cost of ownership.

NGFW Feature Comparison of Top Five Vendors

	SonicWall	Cisco	Palo Alto	Fortinet	Check Point
Standard Security					
Zone-based FW	Yes	Yes	Yes	Optional	Optional
IPSec VPN	Yes	Yes	Yes	Yes	Yes
Route-based VPN	Yes	Yes	Yes	Yes	Yes
IPS	Yes	Yes	Yes	Yes	Yes
App Control	Yes	Yes	Yes	Yes	Yes
URL Filter	Yes	Yes	Yes	Yes	Yes
Advanced Security					
Sandboxing	Yes	Yes	Yes	Yes	Yes
True Multi-tenancy	Yes, Multi-instance	Yes, Multi-instance	No, Virtual Systems	No, Virtual Domains	No, Virtual Systems
Inspect Encrypted	Yes	Yes	Yes	Yes	Yes
Threat Intel	Yes	Yes	Yes	Yes	Yes
Remote Access					
VPN Client	IPSec & SSL VPN	SSL-VPN only	IPSec & SSL VPN	IPSec & SSL VPN	IPSec & SSL VPN
Mobile Client	Yes	Yes	Yes	Yes	Yes
ZTNA	Separate	Separate	Separate	Separate	No
Cloud and E-Mail					
Cloud App Security	Yes	Yes	Yes	Yes	Yes
E-Mail Protection	Yes	Yes	On Firewall	Yes	On Firewall
Networking					
HA/Clustering	Yes	Yes	Yes	Yes	Yes
SD-WAN	Yes	Not on NGFW	Yes	Yes	Separate
Switch management	Yes	Separate	No	Yes	No
Wireless	Yes	Separate	No	Yes	No
Management					
Unified Policy	Yes	Yes	Yes	Yes	Yes
Central Manager	Cloud & on-prem	Cloud & on-prem	On-prem only	Cloud & on-prem	On-prem only
Single pane of glass	Yes	No	No	Partial	No

Conclusion and Next Steps

To recap, there are many factors to consider and options to choose from before selecting your next-generation firewall. Some of those factors and choices include:

- **Security Controls:** IPS, Application Control, URL Filtering and others
- **Advanced Security:** Sandboxing, Zero Trust Network Access and others
- **Network Size:** This determines the number of NGFWs needed
- **Virtual or Cloud:** Enterprises with virtual and cloud environment need Virtual and Cloud NGFWs
- **Performance:** Choose a NGFW with enough capacity so it will not be a bottleneck in the network
- **Support options:** There are many options: online, on-site and professional service. Choose the option that's right for your team based on your team's expertise and workload.

When it comes to solving business challenges, enterprises are generally eager to adopt new technologies, such as cloud computing, workforce mobility and automation. But now, many enterprises are finding their digital transformation journey laden with new challenges, including a surge in the number of connected devices, millions of encrypted connections, increased bandwidth needs, continually evolving evasive attacks and increased operational costs.

The SonicWall Network Security appliance (NS*a*) and Network Security services platform (NS*sp*) is a next-generation firewall with multiple 100/40/10 GbE interfaces that can process millions of connections. Their high-speed connectivity and large port density — coupled with superior IPS and TLS1.3 inspection support — make these firewalls an ideal threat protection platform for enterprise Internet edge and data center deployments. And the newly introduced multi-instance capability (modern multi-tenancy) allows MSSPs and enterprises to provide guaranteed performance, reliability and availability while adhering to service level agreements.

Learn More

- Next-Generation Firewall for Data Center
- Next-Generation Firewall for Internet Edge
- Next-Generation Firewall for Public Clouds

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era in a work reality where everyone is remote, mobile and unsecure. SonicWall safeguards organizations mobilizing for their new business normal with seamless protection that stops the most evasive cyberattacks across boundless exposure points and increasingly remote, mobile and cloud-enabled workforces. 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 or follow us on Twitter, LinkedIn, Facebook and Instagram.

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

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. Except as set forth in the terms and conditions as specified in the license agreement for this product, SonicWall and/or its affiliates assume no liability whatsoever and disclaims any express, implied or statutory warranty relating to its products including, but not limited to, the implied warranty of merchantability, fitness for a particular purpose, or non- infringement. In no event shall SonicWall and/or its affiliates be liable for any direct, indirect, consequential, punitive, special or incidental damages (including, without limitation, damages for loss of profit, business interruption or loss of information) arising out of the use or inability to use this document, even if SonicWall and/or its affiliates have been advised of the possibility of such damages. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

As a best practice, SonicWall routinely optimizes its methodologies for data collection, analysis and reporting. This includes improvements to data cleansing, changes in data sources and consolidation of threat feeds. Figures published in previous reports may have been adjusted across different time periods, regions or industries. The materials and information contained in this document, including, but not limited to, the text, graphics, photographs, artwork, icons, images, logos, downloads, data and compilations, belong to SonicWall or the original creator and is protected by applicable law, including, but not limited to, United States and international copyright law and regulations.