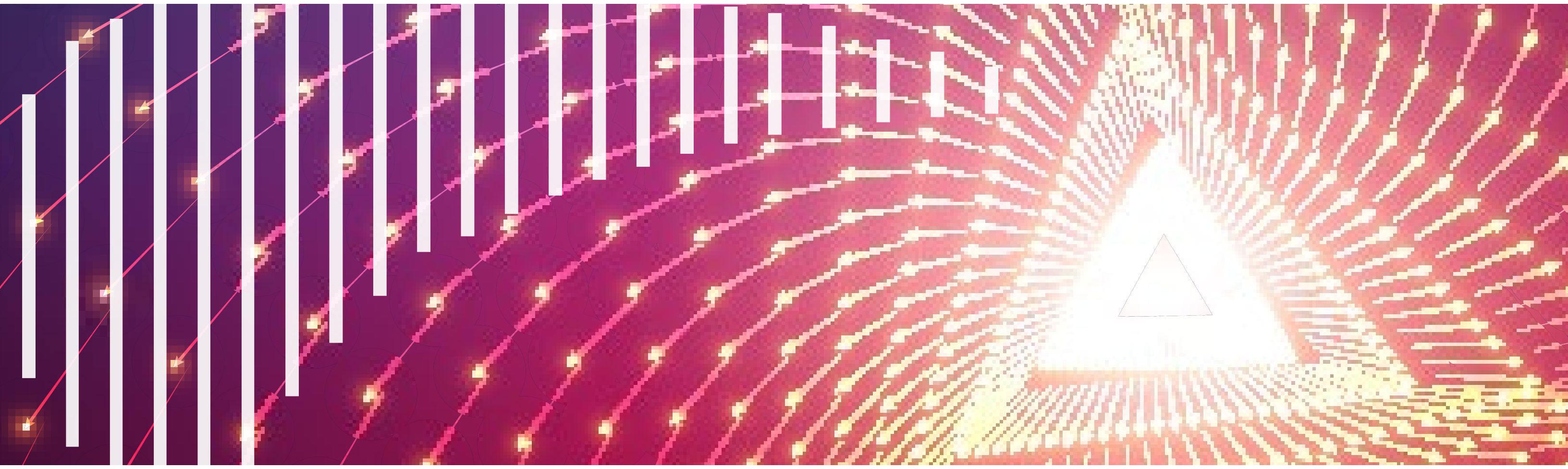
SONICWALL®



Today’s Firewall is More Important in a Multi-Perimeter World

Know what’s in the new cornerstone for enterprise security

Executive Summary

Cloud computing, virtualization, mobility – and now expansive work-from-home policies – have dramatically changed how organizations conduct business. As enterprises become more distributed and as more remote users access more cloud-based applications, the traditional perimeter that separates inside from outside, and trusted from untrusted, is increasingly disappearing.

Anywhere, anytime access fosters collaboration and enables gains in productivity, but also adds the security challenges of provisioning access based on user, device-type, application, access type – and even time of day – to the ongoing, previous security challenges that continue to exist. Equally important, attackers continue to strengthen their skills and refine their techniques. Creative threats are coming from a variety of vectors, including high-risk URLs and weaponized web applications.

In an age of anywhere, anytime, hyper-distributed business where legacy cybersecurity solutions fall short, what’s needed is stronger secure gateways to protect the perimeter no matter where it is located. To stay ahead of the threats, it’s time for security professionals to re-embrace Next-Generation Firewalls (NGFW).

The New Business Normal is No Longer New

The design, implementation, and deployment of modern network architectures, such as virtualization and cloud, continue to be a game-changing strategy for many organizations. Virtualizing the data center, migrating to the cloud, or a combination of both, demonstrates significant operational and economic advantages as public cloud services, always-on internet, and collaboration technologies empower teams to connect, communicate, and be productive from anywhere. However, vulnerabilities within virtual and cloud environments are well-documented and new vulnerabilities are discovered regularly that yield serious security implications and challenges.

When the COVID-19 pandemic struck, work went home — and cybercriminals followed

In the era of remote work, cloud computing, mobile devices, and IoT, the enterprise perimeter extends to anywhere that work gets done and is constantly changing. Remote-first and boundless workforces is the new business normal and the hyper-distributed business is here to stay. The distributed IT reality is creating an unprecedented explosion of exposure points across organizations and government agencies. As exposure points continue to multiply, cyber and business risk continues to escalate. Regardless of whether entry

WHITE PAPER

points are on-premises, in the cloud, in the data center, at a branch office, in a home office, or 'on the go,' each one needs to be protected.

Cyberattacks Are on the Rise

Cybercriminals are enjoying unprecedented opportunities. When the COVID-19 pandemic struck, work went home — and cybercriminals followed , propelling IoT malware attacks to new heights. Unchecked IoT devices can provide cybercriminals an open door into what may otherwise be a well-secured organization. IoT malware attacks have been rising over the last three years and in 2020 they skyrocketed. In 2019, SonicWall recorded 34.3 million IoT malware attacks. In 2020, that number rose to 56.9 million, a 66 percent increase.[1]

Beyond targeting remote workers, ransomware is up – as are encrypted threats.

Λ62%

Increase in ransomware in 2020

Λ66%

Increase in IoT malware attacks in 2020

Ransomware continues to be the most concerning threat to corporations and the preferred tool for cybercriminals. As reported in the 2021 SonicWall Cyber Threat Report, the effects of a global pandemic, combined with record highs in the price of cryptocurrency, drove ransomware to a staggering 62 percent increase over 2019.[2] When asked how effective their legacy firewalls were in preventing a ransomware attack, only 36 percent of security professionals reported that their organizations' firewalls are highly effective.[3]

In addition to taking advantage of low-hanging fruit, cybercriminals continue to use encryption to circumvent traditional network defenses and gain access to sensitive data. While TLS provides legitimate security benefits for web sessions and internet communications, cybercriminals are increasingly using this encryption protocol to hide malware, ransomware, zero-day attacks, and more. Traditional security controls, such as legacy firewalls, lack the capability or processing power to detect, inspect, and mitigate cyberattacks sent via HTTPS/TLS traffic, making this a highly successful avenue for hackers.

57% of security professionals revealed it takes three weeks to a month to configure legacy firewall rules

Enterprises Are Facing Daunting Challenges

With increasing numbers of devices and remote workers, enterprises are facing even more daunting challenges in protecting the business. Many enterprises, educational institutions, and government agencies have deployed a number of stand-alone appliances and disjointed defenses, which include traditional firewalls, Intrusion Prevention Systems (IPS), Virtual Private Networks (VPN), and sandboxing, to segment and secure different departments, data centers, and users.

Even though this type of deployment offers needed security, it has several drawbacks:

- **Management Complexity.** Stemming from a need to manage multiple networks, customers, and clouds, enterprises are using many different firewalls. However, the use of multiple vendors and stand-alone security products to secure networks and cloud infrastructure increases operational complexity and adds costs.
- **Policy Proliferation and Limited Visibility.** Operating across several segmented networks, clouds, or service definitions often results in the proliferation of different policies (many of which may be obsolete, duplicated, or shadowed). Beyond the limited visibility into the network security posture, with so many different firewall deployments in place, it can be difficult to manage them all to achieve consistent policies. In a recent industry study, 57 percent of security professionals revealed it takes three weeks (32%) to a month (25%) to configure legacy firewall rules to accommodate an update or a new application.[4]

- **Performance Bottlenecks.** Increases in enterprise and encrypted traffic traversing large-chassis firewalls impact network performance, creating a need to use expensive, hard-to-maintain load balancers to keep up with increasing network traffic. Further, organizations are often faced with challenges in upgrading legacy-based network firewalls that already exist within the infrastructure. Such legacy systems frequently create a bottleneck in terms of performance and ability to provide the enhanced security services required to secure applications and domains.
- **Constrained Resources.** IT management and security teams are understaffed, stretched too thin, and often operate in crisis mode. Constrained resources impact the ability to manage the security posture and provide consistent assurance of security.

A single network perimeter has evolved into multiple micro-perimeters

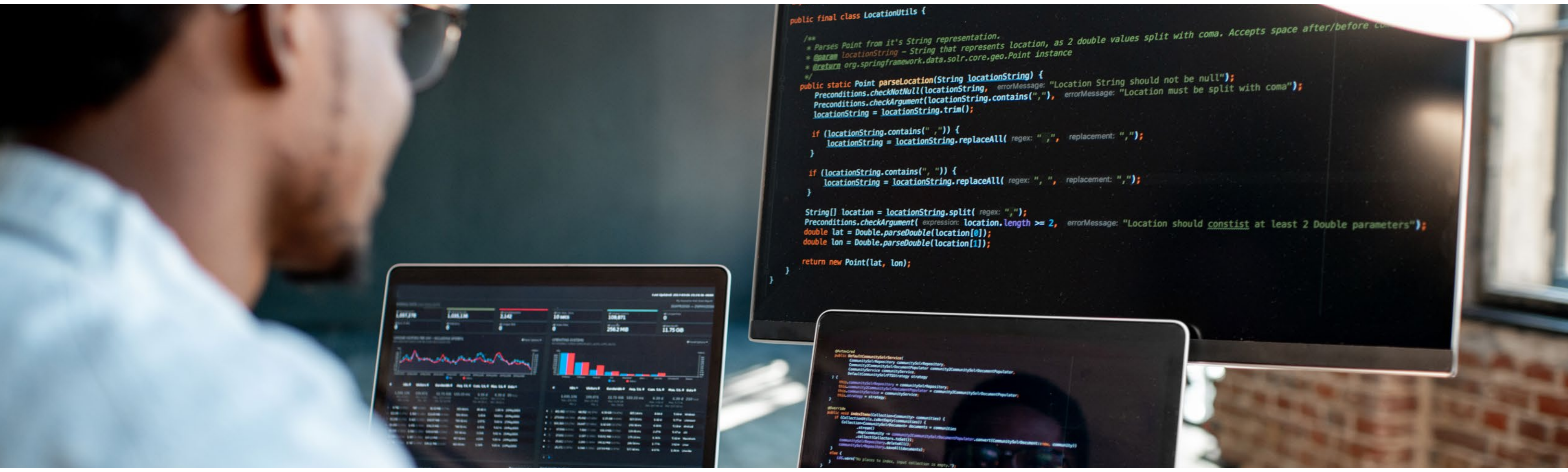
Legacy Firewalls for Network Defense: Past Their Prime

From the early beginnings of hardware appliances that provided protection in the form of access control lists, firewalls evolved from stateful firewalls to Zone-Based Firewalls (ZBF) with VPN functionality. The addition of Intrusion Detection and Prevention (IDS/IPS) further increased functionality to detect and prevent vulnerability exploits. As increasingly complex IT environments continued to allow attackers to evade defenses, Unified Threat Management (UTM) emerged to alleviate the pain and risk of deploying and maintaining multiple stand-alone security tools. The all-in-one UTM appliance combines security controls (firewall, intrusion detection/prevention, URL filtering, and antivirus) into a single operating system and management console.

As the first line of defense to protect everything inside the perimeter against intrusion and the last line of defense against data loss, firewalls have been without a doubt an indispensable component of the cyber defenders' arsenal against threat actors. However, the new business normal begs the question of why IT management and security teams are still relying on legacy firewalls when today's massively expanding distributed IT reality is fueled by:

- The pervasive cloud
- The race to digitize
- The proliferation of apps and devices
- Componentized and virtualized capabilities
- Borderless organizations
- Sensors everywhere

These converging forces are driving the demand for microsegmentation and zero trust network access. Enterprise data and myriad applications reside in any number of places, with users accessing them from an infinite number of locations. What was once a single network perimeter has evolved into multiple micro-perimeters , each of which needs to be secured. What was once the need to deploy a firewall to protect the internal network has become the need to embrace firewalling as a strategy, where consistent security controls are deployed via a combination of physical, virtual, and cloud-based firewalls everywhere you need them.



```
public final class LocationUtils {

    /**
     * Parses Point from it's String representation.
     * @param locationString - String that represents location, as 2 double values split with coma. Accepts space after/before
     * @return org.springframework.data.solr.core.geo.Point instance
     */
    public static Point parseLocation(String locationString) {
        Preconditions.checkNotNull(locationString,  errorMessage: "Location String should not be null");
        Preconditions.checkArgument(locationString.contains(","),  errorMessage: "Location must be split with coma");
        locationString = locationString.trim();

        if (locationString.contains(" ,")) {
            locationString = locationString.replaceAll( regex: " ,",  replacement: ",");
        }

        if (locationString.contains(", ")) {
            locationString = locationString.replaceAll( regex: ", ",  replacement: ",");
        }

        String[] location = locationString.split( regex: ",");
        Preconditions.checkArgument( expression: location.length >= 2,  errorMessage: "Location should constist at least 2 Double parameters");
        double lat = Double.parseDouble(location[0]);
        double lon = Double.parseDouble(location[1]);

        return new Point(lat, lon);
    }
}
```

Think Beyond One Control Point

As organizations grapple with the changing state of growing and complex networks, they need solutions that address the entire enterprise. IT security, however, struggles to keep up with the pace of change, mainly due to a reliance on legacy-based network firewalls that already exist within the infrastructure.

The challenge is that in today's dynamic networks, the network has become an amorphous concept. To achieve agility, organizations need to be able to secure their workforce at the individual level and their digital assets at the granular, application-access level. However, legacy perimeter firewall technology was never intended for the more precise demands of granular microsegmentation and zero trust access policies. Legacy firewalls are too complex, inflexible, and ineffective in today's dynamic, hybrid-cloud environment. Research bears this out, as 62 percent of security professionals report that access control policies are not granular enough and 48 percent say it takes too long to implement controls.[5]

62%

of security professionals report that access control policies are not granular enough

Legacy firewalls are not only ill-suited for segmentation, but stand in the way of growth. Reliance on legacy systems limits business agility, impedes policy creation and enforcement, and hampers the ability to scale. Further legacy big chassis firewalls are more expensive than IT management teams may realize. Beyond the upfront cost of firewalls and hardware are the downstream costs of project management, IT resources, maintenance, and the risk of prolonged asset exposure due to lengthy implementation times. More than half of security professionals (60%) report that their organizations would consider reducing their legacy firewall footprint because of high labor and other costs.[6]

To succeed in today's digital world, it's vital to think beyond one control point and embrace "firewalling"— a policy-driven method for strategically coordinating advanced security.

Modern Firewalls for the Modern Enterprise

The firewalls of today are more agile, more capable, and more powerful than when the technology debuted 20 years ago. Today's Next-Generation Firewalls build on the strengths of past firewalls and include modern networking capabilities and all of the security controls found in UTM as well as SSL/TLS decryption, user control, application-level filtering, and sandboxing. The integration of Data Loss Prevention (DLP) within NGFW blocks the extraction of sensitive data, especially regulated data such as personally identifiable information (PII) and compliance-related data.

Criteria to consider in evaluating NGFWs include:

- Networking capabilities
- Security features
- Manageability
- Programmability

Networking Capabilities

An enterprise-grade platform and operating system are at the core of any physical or virtual NGFW. Capabilities that are vital in enterprise deployments include SD-WAN security, encrypted traffic inspection, High Availability/Clustering, and Zero Trust.

SD-WAN Security

Enterprises with remote locations and branch offices have historically relied on a traditional MPLS environment for connectivity. The drawback is that MLPS solutions hairpin internet traffic back to the data center, offer limited visibility, and are expensive to build and maintain. Now, with remote workforce policies here to stay, networks grow more distributed. Software-defined Wide Area Networks (SD-WAN) combine network and security functions with WAN capabilities to support dynamic, secure internet access. The beauty of SD-WAN is that the network is easily managed from a central controller, allowing network administrators to build policies and seamlessly push them to every device at once.

Encrypted Traffic Inspection

Data encryption plays an essential role in data security and privacy today, largely driven by the need to protect personally identifiable information. According to industry

research, for the first time, 50 percent of organizations have an overall encryption strategy applied consistently across their organization with 37 percent having a limited encryption strategy.[7]

The trouble is that organizations aren't the only ones using encryption. Threat actors use encryption protocols like Secure Sockets Layer and Transport Layer Security (TLS) to carry out phishing schemes, disguise malware, and hide communication between compromised systems and command-and-control servers. The threat is pervasive. With some 6.6 billion threats hidden inside of encrypted traffic , encrypted attacks spiked 260 percent in the first nine months of 2020 compared to the same period the previous year.[8]

6.6 billion

threats are hidden inside of encrypted traffic

^260%

Spike in encrypted attacks in the first nine months of 2020

NGFWs have the ability to decrypt and inspect traffic in real time while supporting a high number of simultaneous connections. Because SSL inspection can degrade performance, it's important that NGFW solutions have the ability to efficiently decrypt and inspect all encryption protocols (including TLS 1.3), scale to support increasing amounts of traffic, and re-encrypt traffic after inspection to ensure compliance with PCI, HIPAA, and other privacy regulations.

High Availability/Clustering

Most consider downtime unacceptable on corporate networks – even for routine maintenance. High Availability (HA) is a deployment in which two firewalls are placed in a group and their configuration is synchronized to prevent a single point of failure on the network. A heartbeat connection between the firewall peers ensures seamless failover in the event that a peer goes down. Setting up two firewalls in an HA pair provides redundancy and helps to ensure business continuity.

Firewalls can be set up for HA in one of two modes:

- **Active/Passive.** Both firewalls share the same configuration settings. One actively manages traffic until a path, link, system, or network failure occurs. When the active firewall fails, the passive firewall transitions to the active state, takes over seamlessly, and enforces the same policies to maintain network security.
- **Active/Active.** Both firewalls actively process traffic and work synchronously to handle session setup and session ownership. Both firewalls individually maintain session tables and routing tables and synchronize to each other.

Zero Trust

As more workloads move to the cloud and teleworking becomes the new normal, the old paradigm of security controls at the perimeter or on user devices is no longer adequate. A more effective approach to take is Zero Trust, where everything is untrusted until proven otherwise, and access is controlled to the one entity that remains constant – the data.

Rooted in the principle of "never trust, always verify," Zero Trust advocates rejecting all previous implicit assumptions about trust in the network and not trusting users, packets, interfaces, or the network. In a Zero Trust network, users can only access what is needed to do their job and nothing more. Stringent verification is based on user credentials, access time, and device compliance.

Next-generation firewalls serve as a cornerstone in delivering a zero-trust environment

Microsegmentation is the preferred method for getting to a Zero Trust network. By using microsegmentation to define internal trust boundaries down to a single machine or application, and granularly controlling traffic flow, organizations can reduce the attack surface and prevent threats from spreading laterally.

Next-generation firewalls serve as a cornerstone in delivering a zero-trust environment . By enabling the identification, inspection, and granular control of all users and applications in the enterprise, they allow security professionals the flexibility to place protections at multiple levels and effectively defend against the rapidly changing threats to prevent loss of sensitive data.

Security Features

A NGFW is within the third generation of firewall technology, designed to address advanced security threats at the application level through intelligent, context-aware security features. Security controls found within next-generation firewalls extend zero trust security to any perimeter and include:

- Virtual Private Network
- Zone-Based Firewall
- Intrusion Detection and/or Prevention
- Application Control
- Web Control (URL Filtering)
- DNS Security (DNS Filtering)
- Multi-Instance Firewall
- Network and Cloud Sandboxing
- Dedicated Threat Intelligence

Virtual Private Network

Virtual Private Networks have long helped enterprise organizations to securely connect distributed offices to each other over the internet by providing encrypted connections. Now, with increasingly mobile workforces and the expansion in work-from-home policies driving the need for secure, anytime remote access, the demand for VPNs has been steadily increasing.

For flexible and resilient connectivity, site-to-site and client-to-site VPN technologies are critical components of any NGFW. Site-to-site VPNs are ideal for large-scale enterprises where the multi-department and/or multi-site exchange of information needs to be carried out continuously and securely. Client-based VPNs allow users to be connected to a remote network by establishing an encrypted link between the device and the remote network.

Zone-Based Firewall

A drawback of traditional firewalls is that they require a large number of configuration commands to apply access control lists to the interfaces. In contrast, zone-based firewalls provide a more flexible, easy way to configure and manage network access. With a zone-based firewall, zones are created for each part of the network that requires different access and traffic control policies. Multiple interfaces are assigned to a zone, with security policies assigned to traffic between the zones. Beyond the ease of management, zone-based firewalls allow for a higher level of conceptualization and control of the network. Establishing zones, for example, allows for the creation of separate areas where specific network ports, subnets, or VLANs can exist with their own firewall rules while still being managed through a single interface.

Intrusion Detection and/or Prevention

Intrusion Detection and Intrusion Prevention Systems operate simultaneously to monitor and analyze network traffic to detect malware, socially engineered attacks, and other web-based threats, including DDoS attacks. They can also provide preemptive intrusion prevention capabilities for potentially compromised systems.

Intrusion Detection uses known malware signatures to scan both inbound and outbound network traffic for signs of abnormal activity, harmful patterns, and user behavior that reflects malicious intent. Upon detecting a security policy violation or suspect activity, an IDS logs the event and sends an alert to notify security personnel. Intrusion Prevention complements Intrusion Detection because it has the capability to drop malicious traffic, block offending IP addresses, and alert security personnel to potential threats. Having both the capabilities of detection and prevention is vital as detection only identifies and alerts on malicious activity. Further, because IDS/IPS uses a signature database, incorporating a threat intelligence feed is vital to ensure the signature database is up to date.

Application Control

Cloud-based and third-party applications at the core of today's business processes; however, work-from-home and remote access are magnifying web and application attacks. Application-specific and web-application attacks continue to rise and remained the top types of attacks observed. In 2020, application-specific attacks accounted for 35 percent , and web-application attacks accounted for 32 percent, resulting in a combined total of 67 percent of attacks (up from 55 percent in 2019 and 32 percent in 2018).[9]

In 2020, application-specific attacks accounted for 35% of all attacks

Application Control is thus a must-have feature for NGFW. Application Control enables businesses to classify applications into categories based on criteria such as application type, security risk level, business value, and more. Businesses can create granular access policies based on user identity, user role, groups, or the nature of the web application itself to limit or block usage of applications and micro-applications.

Web Control (URL Filtering)

Browsing web pages has become a primary way for people to work and stay informed, but along with the convenience, accessing network resources also brings the risk of malware, phishing attacks, and network abuse. From Facebook and YouTube to TikTok, Instagram and more, the internet continues to offer an untold number of non-work-related websites that draw employees' attention away from work activities – severely affecting productivity, impacting network performance, and potentially opening the door to non-compliance with corporate policies.

Web control – also known as URL filtering – allows or denies access based on URL categories and specific URLs, allowing companies to block access to business-irrelevant, malware, and phishing websites, as well as websites that contain illegal content. URL filtering is enabled by comparing a requested URL with entries in a local URL database or by querying a master cloud-based database. Frequently accessed URLs are cached locally to account for a firm's specific traffic and usage patterns and to reduce latency for the most frequently accessed URLs. Cloud-based databases, supported by threat intelligence feeds, provide wider coverage and protection against the latest threats.

DNS Security (DNS Filtering)

Domain Name System (DNS) Security is widely trusted by organizations as a first line of defense. Integrating DNS security into firewall policies to segment user groups, mapped to allow/deny domain lists for DNS filtering of client queries, can reduce exposure to risk by controlling app access at the earliest point in the flow. DNS domain deny and/or allow lists are seen as very valuable by 43 percent of organizations to improve control over which users can access which apps, and 76 percent of organizations deem it to be critical for their business.[10]

^76%

of organizations deem DNS security
to be critical for their business

^87%

of organizations have experienced
a DNS attack in 2021

DNS, however, remains a prime target for hackers as it enables them to gain first entry into networks. According to IDC Research, 87 percent of organizations have experienced a DNS attack in 2021 compared to 79 percent in 2020. Further, the average number of attacks remains high, with 7.6 attacks per organization.[11]

With enterprise boundaries blurring, DNS security is a critical component of NGFW functionality. Further, because of its ability to provide visibility over client behavior and granular filtering, DNS plays a key role in meeting zero-trust objectives.

Multi-Instance Firewall

Apart from deploying multiple standalone appliances to achieve segmentation and secure different entities, security teams have used multi-tenant technology to logically segment one security appliance into multiple virtual firewalls. Such virtual firewalls will share the same physical resources available on the security appliance, such as CPU, memory, and interfaces. Although this method improves operational efficiency and the ability to deploy more than one firewall on a single security appliance, it has some limitations:

- Virtual firewalls need to have the same software version installed — they cannot have independent versions.
- There is a potential for hardware resource starvation if one of the logical firewalls is oversubscribed.
- Firewall management tenancy is shared, leading to configuration limitations.

By establishing multiple, independent firewall instances using a containerized architecture, organizations can establish complete tenant isolation without having to manage multiple physical appliances. While traditional multi-tenancy architectures suffer from tenant failures that can affect other tenants and cause resource starvation, in a multi-instance paradigm each independent firewall instance provides for customized security policy configuration, independent firmware versions, and dedicated hardware resources.

Network and Cloud Sandboxing

Zero Day threats are constantly growing in quantity and sophistication, making it vital that NGFWs include a way to detect threats that evade traditional email, malware, and virus filters. To aid in the detection and analysis of malware, sandboxing is used to give organizations the ability to run, observe, and analyze code in an isolated environment. Because the environment is not actually connected to a network, any malware that executes in the sandbox environment cannot infect a real device or the host network.

Sandboxing solutions should be evaluated on the ability to analyze every last byte of the code

Network sandboxes monitor network traffic for suspicious objects and automatically extract and submit them to the sandbox environment for testing. Sandbox solutions are able to analyze a broad range of protocols, file types, and file sizes, including executable programs and multiple operating systems.

Sandboxes can be deployed as on-premises appliances or as a cloud-delivered solution. Beyond being free of hardware limitations in terms of scalability and geography, cloud-based sandboxes can track malware over longer periods of time to uncover 'time bomb' attacks. Testing should be combined with threat intelligence data to help determine whether the malware is part of a targeted attack, advanced persistent threat, or an automated or mass distributed attack. Lastly, sandboxing solutions should be evaluated on the ability to analyze every last byte of the code with deep memory inspection and hold files until a final verdict to block or allow is determined.

Dedicated Threat Intelligence

Next-generation firewalls remain an important foundational component of network security. However, without a way to keep up to date on the latest threats and signatures, NGFWs operate with a narrow a view of the threat landscape. Critical to their effectiveness in defending against Zero Day and evolving attacks is timely, accurate, and actionable threat intelligence that provides constant updates and global visibility across the entire threat spectrum. Because NGFWs are only as effective as the threat intelligence infrastructure and researchers that support them, telemetry should be gathered from across the world and vetted by dedicated, expert research teams.

The combination of layer 3 to layer 7 controls into a single policy reduces rule management overhead

Manageability

Individually accessing multiple firewalls and other components to make changes or view activity can burden already constrained resources. A centralized system that enables you to remotely configure, deploy, view, and run reports on all on-prem and cloud-based firewall activity through a single pane of glass is vital. Important central management and ease-of-use functionality includes:

- **On-prem and Cloud.** Flexible management allows for the configuration and management of NGFW through an on-prem system or via the cloud.
- **Unified Policy.** The combination of layer 3 to layer 7 controls into a single policy reduces rule management overhead and provides a centralized location for easier and more intuitive policy configuration for both users and assets.
- **Policy Tuning.** The automation of provisioning, tuning, and enforcement of policies helps security teams optimize security effectiveness and respond to changing conditions and new attacks in real-time.
- **Monitoring.** Continuous and passive monitoring provides real-time insight that helps security teams to identify and address security gaps, identify and remediate risks, and fine-tune controls.
- **High Scalability.** Elasticity allows for seamless scaling in physical, virtual, or cloud environments and configuration of NGFW as topology, sites, or workloads change, while being able to manage hundreds of firewalls from a central location.

Programmability

Despite its multiple, robust capabilities, a next-generation firewall still needs to operate with other systems that are installed on the network it is expected to protect. It should, therefore, be able to integrate seamlessly and transparently with the entire network infrastructure and third-party security solutions. It should also be able to integrate with all major IaaS providers to support multi-cloud deployments across AWS or Azure. Critical technology integrations include:

- Vulnerability management systems
- Security information and event management (SIEM)systems
- Trouble ticketing and synchronized event-response workflow systems
- Threat intelligence

Summary

With the disruption of the traditional office-centric workforce, the new normal is that everyone is remote and unsecure. The huge shift toward work-from-anywhere and increased adoption of cloud-based services and applications have created micro-perimeters at on-premises, in-the-cloud, branch office, and home office locations.

Threat actors are becoming more powerful, more aggressive, and more numerous, increasingly abandoning the tendency to look for the biggest quarry in favor of attacking the least

SonicWall firewalls are designed to meet your specific security and usability needs

defended. The abrupt shift to remote working, for example, precipitated a dramatic increase in cyber threats as threat actors capitalized on the COVID-19. Taking advantage of hyper-distributed networks, threat actors exploited a multitude of new vulnerabilities, with ransomware and IoT attacks taking the lead as preferred tools. In the new, boundary-less reality, it's imperative that businesses move away from traditional, makeshift security strategies and adopt a comprehensive, integrated cybersecurity model that combines malware analysis, encrypted traffic inspection, cloud app security, and reputation services.

With the power and flexibility of a NGFW, enterprises can protect devices and companies from a much broader spectrum of intrusions, more effectively reduce cyber risk, and achieve greater protection across new perimeters and network segments more easily while lowering costs of ownership.

SonicWall Empowers You to Defend the Newly Defined Network

Whether you're a small business or a large enterprise, whether in your home or in the cloud, SonicWall next-generation firewalls provide the security, control, and visibility you need to maintain an effective cybersecurity posture. SonicWall's award-winning hardware and advanced technology are built into each firewall to give you the edge on evolving threats. With solutions designed for networks of all sizes, SonicWall firewalls are designed to meet your specific security and usability needs , all at a cost that will protect your budget while securing your network.

[1] *SonicWall, 2021 SonicWall Cyber Threat Report, March 2021.*

[2] *SonicWall, 2021 SonicWall Cyber Threat Report, March 2021.*

[3] *Ponemon Institute, Rethinking Firewalls: Security and Agility for the Modern Enterprise, November 2020.*

[4] *Ponemon Institute, Rethinking Firewalls: Security and Agility for the Modern Enterprise, November 2020.*

[5] *Ponemon Institute, Rethinking Firewalls: Security and Agility for the Modern Enterprise, November 2020.*

[6] *Ponemon Institute, Rethinking Firewalls: Security and Agility for the Modern Enterprise, November 2020.*

[7] *Ponemon Institute. 2021 Global Encryption Trends Study. April 2021.*

[8] *Zscaler. 2020 State of Encrypted Attacks. September 2020.*

[9] *NTT Ltd., 2021 Global Threat Intelligence Report Technical Report, May 2021.*

[10] *IDC Research, 2021 Global DNS Threat Report, June 2021.*

[11] *IDC Research, 2021 Global DNS Threat Report, June 2021.*

Learn more about SonicWall Next-Generation Firewalls

www.sonicwall.com/firewalls

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 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 PROFITS, 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.