Network Security Buyer's Guide

The Definitive Guide to Creating Security RFPs That Get Results

Table of Contents

The Gathering Storm

Security professionals may differ in their opinions about a lot of things, but there's little disagreement that the threat landscape is getting more virulent and complex by the day. Consider these recent predictions from Unit 42, our internal team that provides threat research and forward-looking analyses of the cybersecurity industry:[1]

- The time to patch vulnerabilities before breaches occur continues to shrink, from days to just hours.
- The skill level required to initiate attacks is lower than ever due to the cheap and easy availability of prebuilt malware on the dark web.
- Difficult economic times could lead to more insiders being willing to explore potential deals with external threat actors.
- Politically motivated incidents, whether so-called hacktivism or state-sponsored attacks, may lead to an increase in incidents where the goal is to damage the brand rather than seek financial gain.

Clearly, the pressure is on to boost cybersecurity measures as a way to mitigate risk and provide additional levels of protection for sensitive information.

Trends in Cybersecurity

Now in its fourth decade—an eternity in the fast-moving world of cybersecurity—the firewall is doing pretty well for its age. After a down year due to COVID-19, the demand for firewalls in the US market is growing at a rate of 23.5% year over year, to reach more than $16 billion by 2027.[2]

This data should come as no surprise. Next-generation firewalls (NGFWs), the current state of the art, continue to be the cornerstone of network security. One key reason is their versatility: today's NGFWs are, in reality, security platforms that can deliver a full range of security services that once required separate appliances, for example intrusion prevention, URL filtering, mobile security, and DNS security. In addition, NGFWs are now available in a range of form factors, both hardware and software, making it easier than ever to architect security solutions based on firewall technology.

Given the importance of NGFWs to cybersecurity, procuring firewalls is a big responsibility. This guide is intended to help you craft your request for proposal (RFP) to ensure a successful procurement and exceptional return on your investment. The main body of the guide is organized alphabetically by security categories such as access control, cloud security, and encryption. For each topic, the guide explains the challenges as well as the general approach to meeting those challenges. In addition, you will find sample questions for each category that you can adapt to your procurement.

As a prelude to the category content, let's briefly look at the important cybersecurity trends that impact network security and NGFWs.

Software Firewalls Take Center Stage

The modern data center is highly virtualized and firewalls are trending that way as well. Software firewalls—such as virtual firewalls and container firewalls—have considerable advantages over physical firewalls. For example, software firewalls run on existing servers and therefore take no additional space in the data center. They are easy to install and upgrade, all of which can be managed from a central location. Flexibility is another key reason because software firewalls can be deployed wherever they are needed, unlike physical firewalls that must reside at key traffic points in the network.

Are hardware firewalls on the way out? Not at all. Physical NGFW appliances continue to be the workhorses of network security because they have much higher capacity than their virtual counterparts. Comprehensive enterprise security requires both hardware and software firewalls to maximize protection without hurting performance.

In addition, a new kind of software firewall is emerging, the container firewall. Introduced by Palo Alto Networks, container firewalls are designed to integrate natively with Kubernetes environments and address some of the security challenges of cloud-native container application development and securing them. Stay tuned for more about this exciting new trend in NGFWs. Learn more.

---

1. *2022 Unit 42 Incident Response Report*, Palo Alto Networks, July 26, 2022, https://start.paloaltonetworks.com/2022-unit42-incident-response-report.
2. *Network Security Firewall Market Research Report by Component (Services and Solution), Type, Deployment, End-User, Region - Cumulative Impact of COVID-19, Russia Ukraine Conflict, and High Inflation - Global Forecast 2023-2030, Research and Markets*, January 2023, https://www.researchandmarkets.com/reports/5470743/network-security-firewall-market-research-report.

Zero Trust Is Catching On

Three recent trends—the move to the cloud, the rise of the hybrid workforce, and the growth in advanced threats—have challenged the security industry's ability to keep up with the needs of its customers. The industry's response has been to roll out yet more tools—one per threat, in some cases. This approach simply cannot be right—a more organized and sustainable approach to network security is desperately needed.

Enter Zero Trust, an architectural philosophy that turns conventional security on its head. The key to Zero Trust is replacing implicit trust with continual verification. In the Zero Trust architecture, trust is enforced through continuous validation at every stage of a digital interaction. Another way to look at Zero Trust is as stateless security, meaning that past validations have no bearing on future security tests—never trust, always verify. In addition to providing stricter security, Zero Trust has the added advantage of simplicity. You are essentially running the same security regardless of the situation (see figure 1). Learn more about Zero Trust.

Who are you?   **Is your device safe?**   **Do you have access privileges?**   **Is the content carrying any threats?**
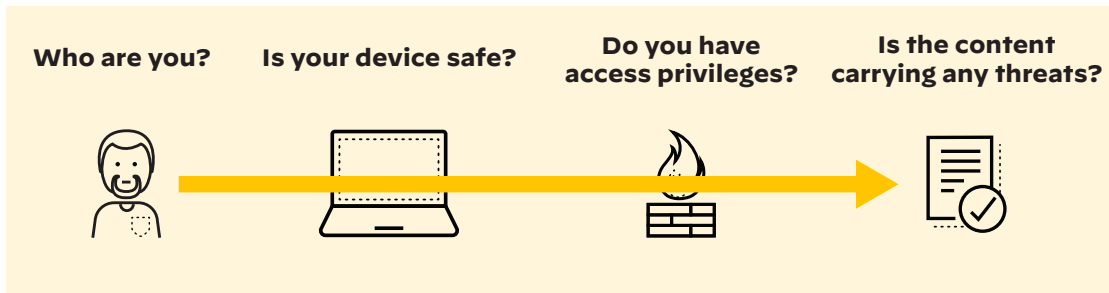
Figure 1: Simplified description of Zero Trust in action

Machine Learning Redefines the NGFW

Just as you would not buy a car without looking under the hood (or bonnet, if you live in the United Kingdom), it pays to understand the key technologies that drive the NGFWs under consideration. In the case of NGFWs from Palo Alto Networks, you are in for a pleasant surprise—machine learning (ML) is at the heart of all our firewalls. ML is an application of artificial intelligence (AI) in which a machine analyzes massive amounts of data, finds meaningful patterns in the data, creates algorithms based on those patterns, and ultimately gets better at the task as time goes on.

NGFWs from Palo Alto Networks employ ML to get ahead of attackers by identifying variations of known threats and patterns, predicting the next steps of an attack, and automatically creating and implementing protections across the organization in near-real time. ML-powered NGFWs from Palo Alto Networks use inline ML models to help prevent previously unknown attacks, the kind that easily elude signature-based security. The "inline" part is important because it assures fast response time to zero-day threats without compromising throughput. ML is a significant differentiator that separates firewalls made by Palo Alto Networks from the pack. Learn more about machine learning.

Cloud-Delivered Security Services Enable Rapid Response

Cybersecurity is above all a foot race, pitting defenders against highly motivated and talented attackers. The attackers have the first-mover advantage—they launch attacks at the time and place of their choosing—and polymorphism, that is, the ability to modify an existing exploit enough to alert its signature and thus turn a known threat into an unknown threat. And remember, it only takes one successful intrusion to seriously compromise your network.

In the race to defeat zero-day threats, our NGFWs are more than up to the challenge. They stop all known threats using signature-based protection and also use a unique process—Cloud-Delivered

File Protections	URL Protections	DNS Protections
5 minutes	**1 minute**	**Instantly**

Figure 2: Typical response times for NGFWs from Palo Alto Networks

Security Services (CDSS)—to detect unknown threats. Combined with threat intelligence gathered from multiple sources, the Palo Alto Networks approach delivers the fastest protection in the industry. Learn more about Cloud-Delivered Security Services.

AIOps Streamlines Network Security Operations

As enterprises expand and the threat landscape evolves, companies invest in new and expensive network security equipment and tools to support their growing infrastructure and prevent threats to maintain a secure workplace. However, these investments alone can't guarantee efficiency or lead to a favorable return on investment (ROI)—network operations come into play as well. Many security teams don't know the best practices to configure various features to effectively maximize their security functionality or have insights into misconfigurations. This leads to gaps in their security posture and puts them at a greater risk of a breach.

Artificial intelligence for IT operations (AIOps) can help. AIOps combines big data and machine learning to automate IT operations processes, including event correlation, anomaly detection, and causality determination. Palo Alto Networks has introduced the industry's first domain-centric AIOps for NGFW that redefines firewall operational experience by predicting, interpreting, and resolving problems before they become business-impacting.

AIOps for NGFW enables security teams to continuously improve security posture by optimizing configuration to their dynamic environment based on best practices and configuration recommendations. It also empowers network security operations teams to become proactive with ML-powered anomaly detection and actionable insights into the health and performance of the entire deployment. AIOps for NGFW proactively addresses the top operational challenges of today, including misconfigurations, human errors, compliance with best practices, resource usage, hardware and software failures, and more. Learn more about AIOps.

Requirements by NGFW Category

This section is organized alphabetically by security category. Each section presents the challenges in that category and the general solution requirements. In addition, you will also find typical RFP questions for each category that you can lift, adapt, and use in your firewall procurements.

Access Control

Challenge: Identify Users and Enable Appropriate Access

The Problem

Employees, customers, and partners—in other words, your network users—connect to the internet as well as different information repositories within your network. To secure these devices, you must be able to identify users and assess the risks of their devices, supported and unsupported.

Network users constantly access information in different physical locations and use multiple devices, operating systems, and application versions. Due to the nature of IP addressing, security policies don't automatically follow users, creating vulnerabilities.

Directory-based access strategies rely solely on an individual's role to determine privileges. However, an accurate risk assessment must include behavioral characteristics such as risky or malicious activity. For that reason, directory-based systems cannot effectively access or mitigate risk.

Solution Requirements

This challenge can only be met by NGFWs that integrate information from multiple sources and assign risk to users based on more than role. Typical information sources include virtual private networks (VPNs), wireless local area network (WLAN) access controllers, directory servers, email servers, and captive portals to determine who is using each application and whether they are transmitting threats.

In addition, the NGFW must rigorously manage access using policies that grant access based on users or groups of users, outbound or inbound—for example, allowing only your IT department to use tools such as SSH, telnet, and FTP. The NGFW also must make sure that policies follow users no matter where they go—at headquarters, branch offices, or home—and on whatever devices they use. Finally, the NGFW must dynamically change user access policies based on information such as new indicators of compromise (IOCs) or need to grant temporary access to a set of users.

Learn more.

RFQ Questions

Can your NGFW:

· Gather risk-related information from multiple sources?
· Support user-based (as opposed to location-based) policies?
· Change policies on the fly in response to new information?

Advanced Threat Prevention

Challenge: Stop Advanced Threats to Prevent Successful Cyberattacks

The Problem

Ransomware attacks are accelerating—2021 saw an almost 13% rise in ransomware attacks, an increase as big as the last five years combined.[3]
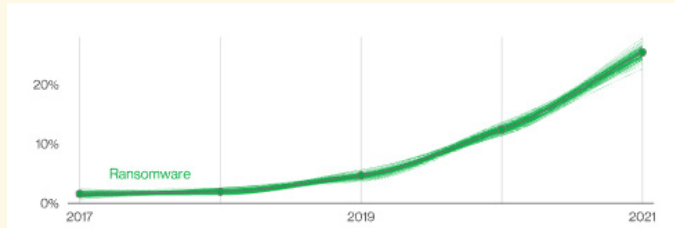
Source: Verizon

Most modern malware, including ransomware variants, uses advanced techniques to elude detection. They employ techniques that scan for valid user activity, system configurations, and indicators of specific virtualization technologies. For example, malicious payloads can be embedded in legitimate files to transport attacks or exploits through network security devices and tools.

The result is a cat-and-mouse game that threatens to overwhelm security systems.

And it gets worse. The technological barrier to entry is falling. Virtually anyone can purchase plug-and-play threats designed to avoid security based on malware analysis.

Solution Requirements

The right NGFW must have both inline analysis and prevention methods based on machine learning to detect unknown threats. Using these tools, the NGFW can identify threats at all points within the cyberattack lifecycle using behavioral analysis and discover command-and-control (C2) activity based on analysis of outbound communication patterns.

In addition, the NGFW must be able to block access to malicious URLs before they compromise your network and scale rapidly using cloud-delivered security enforcement.

To keep up with changing development methodologies, modern firewalls must be able to support DevOps and Kubernetes environments and take advantage of the opportunities these technologies provide. Automation is essential to lessen the load on busy security staff.

Learn more.

RFQ Questions

Can your NGFW:
- Deliver machine learning-based prevention of unknown malware files and variants, including executables as well as fileless attacks leveraging scripts such as PowerShell?
- Deliver inline machine learning-based prevention of malicious website attacks, including JavaScript and credential phishing attacks?
- Block executables and other risky file types from unknown applications and URLs?
- Automatically and dynamically import all known IOCs (i.e., IPs, domains, and URLs) into the block list?
- Integrate with threat intelligence to support dynamic updates for malicious URLs related to ransomware in the malware category of the URL filtering database?

Does your cloud-based malware analysis system:
- Use a custom-coded hypervisor to be effective against sandbox-aware malware?
- Create threat prevention signatures such as 1) content-based AV signatures to prevent known and unknown variants of malware and 2) pattern-based antispyware signatures to detect communications to known and unknown C2 infrastructure?
- Support malware analysis for Windows, Android, Linux, and macOS operating systems?

Can your cloud-based malware analysis system distribute signatures in realtime after a verdict has been reached?

---

3. 2022 *Data Breach Investigations Report*, Verizon, May 24, 2022, https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/.

Application Enablement

The Problem

Applications such as instant messaging applications, peer-to-peer file sharing, and Voice over Internet Protocol often operate on nonstandard ports. In addition, users are accessing diverse types of apps, including software as a service (SaaS), from a range of devices and locations. Some users are increasingly savvy enough to force applications to run over nonstandard ports through protocols such as RDP and SSH.

New applications provide users with rich sets of functions that help ensure user loyalty but may represent high-risk profiles. For example, Webex is a valuable business tool, but using Webex desktop sharing to take over an employee's desktop from an external source may violate internal rules or regulations. Gmail and Google Drive are other good examples. Once users sign in to Gmail, which may be allowed by policy, they can easily switch to YouTube or Google Photos, which may not be allowed.

Security administrators need complete control over usage of these apps and set policy to allow or control certain types of applications and application functions while denying others.

Solution Requirements

NGFWs must be able to classify traffic by application on all ports, all the time, by default—and not burden your staff to research common ports used by each application. The firewall has to provide complete visibility into application usage along with capabilities to understand and control their use. For example, it should understand usage of application functions such as audio streaming, remote access, and posting documents, and be able to enforce granular controls over that usage such as upload versus download permissions, and chat versus file transfer.

Traffic classification must be a continuous process because these commonly used applications share sessions and support multiple functions. If a different function or feature is introduced in the session, the firewall must perform a policy check again. Continuous state tracking to understand the functions each application can support—and the associated risks—is a must for your next firewall.

Learn more.

RFQ Questions

Does your NGFW:
- Defend against applications that evade detection using nonstandard ports, port hopping, or misconfigurations?
- Use mechanisms such as UltraSurf or encrypted P2P to detect purposely evasive applications? Any other mechanisms?
- Prioritize application ID over network port or network destination as basis for classification?
- Track application state to ensure consistent control of the application and associated functions?
- Automatically update the application database? Is it a dynamic update or a system reboot upgrade?
- Allow system managers to work directly on the appliance and change configurations as needed without logging in to a central manager?
- Decrypt SSL and SSH traffic?

How does the firewall accurately identify applications?

How is SSL/SSH decryption implemented in your NGFW?

Automation

Challenge: Reduce Time Spent on Manual Tasks

The Problem

Cybersecurity experts are in high demand, and the supply isn't keeping up. In a recent study of cybersecurity leaders, two-thirds (60%) of participants report that the cybersecurity staffing shortage is placing their organizations at increased risk.[4]

Making matters worse, cybersecurity staff spend much of their day on manual tasks such as investigating false positive alerts and managing remediation. This time drain slows mitigation, increases the chance for error, and is difficult to scale.

Security teams can easily drown in the volume of alerts and miss the critical, actionable ones. Although big data analytics can uncover hidden patterns, correlations, and other insights to provide security teams with actionable intelligence, you still need the right data. That data must be sourced from everywhere—networks, endpoints, SaaS applications, public clouds, private clouds, data centers, and so on—and be ready for analytics.

Solution Requirements

Automation driven by analytics reduces time spent on routine tasks and allows security staff to focus on business priorities such as speeding up applications, improving processes, and hunting for threats. There are three areas where automation can help:

- **Workflow automation**: The firewall must expose standard APIs so it can be programmed from other tools and scripts. It must integrate with tools like Ansible and Terraform and be able to initiate workflows on other devices in your security ecosystem using their APIs, without manual intervention. This automation should extend to operationalization of rules and threat information in open source formats, such as Snort or Suricata.

- **Policy automation**: The firewall must be able to adapt policies to any changes in your environment, such as movement of applications across virtual machines. It must also be able to ingest threat intelligence from third-party sources and automatically act on that intelligence.

- **Security automation**: Your environment must be able to uncover unknown threats and deliver protections to the firewall so new threats are blocked automatically.

Some threats remain hidden in data. By looking deeper into that data across locations and deployment types, you can find threats that may be lurking in plain sight. With automation, you can accurately identify threats, enable rapid prevention, improve efficiency, better utilize the talent of your specialized staff, and improve your organization's security posture.

Learn more.

RFQ Questions

Does your NGFW:
- Correlate, identify, and quarantine infected hosts in the network to limit their access in the network?
- Trigger MFA to prevent credential abuse and secure critical applications?
- Correlate threats in the network with information obtained from global threat intelligence?
- Automatically generate prevention signatures across the attack lifecycle for all data relevant to attacks?

4. *A Resilient Cybersecurity Profession Charts the Path Forward, (ISC)² Cybersecurity Workforce Study, 2021*, (ISC)², October 26, 2021, https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx.

Credential Security

Challenge: Prevent Theft and Abuse of Corporate Credentials

The Problem

Users and their credentials are among the weakest links in an organization's security infrastructure. The human element continues to be a key driver of 82% of breaches, with phishing and pretexting attacks leading the way. Stolen credentials provide a great second step after a social attack gets the actor in the door, which emphasizes the importance of having a strong security awareness program.[5]

When using stolen credentials, an attacker's chances of successfully breaching go up while the risk of getting caught goes down. To prevent credential theft, most organizations rely on employee education, which is prone to human error by nature. Technology products commonly rely on identifying known phishing sites and filtering email.

However, these methods can sometimes be bypassed. Attackers can easily steal credentials through phishing, malware, social engineering, or brute force, and can even buy them on the dark web. In 13% of cases studied by Unit 42, organizations had no mitigations in place to ensure account lockout for brute-force credential attacks.[6] Attackers use these credentials to gain access to a network, move laterally, and escalate their privileges for unauthorized access to applications and data.

Solution Requirements

Organizations should look for a firewall with machine learning-based analysis to identify websites that steal credentials. When the analysis identifies a malicious site, the firewall policies should be updated. Your next firewall must allow you to block submission of corporate credentials to unknown sites as well.

The firewall must also allow you to protect sensitive data and applications by enforcing MFA to prevent attackers from abusing stolen credentials. Research conducted by Unit 42 found that 50% of organizations targeted by cyberattackers lacked MFA on key internet-facing systems such as corporate webmail, virtual private network (VPN) solutions and other remote access methods.[7] By integrating with common MFA vendors, your firewall can protect your applications containing sensitive data, including legacy applications.

Learn more.

RFQ Questions

Does your NGFW:
- Prevent use of corporate credentials on unknown websites?
- Block users from submitting corporate credentials without storing a copy of the hash in the firewall?
- Quickly analyze previously unknown phishing sites and update its protections?
- Log user attempts to submit credentials in HTTP post?

Support MFA as part of access-control policy based on the sensitivity of the resource accessed?

If you do support MFA, does your firewall:
- Provide a variety of choices in MFA technologies?
- Support API integrations with MFA partners?
- Support MFA policy for any type of application, including web, client-server, and terminal applications?
- Support MFA capability on any protocol, rather than be limited to certain protocols?

---

5. *Verizon Data Breach Investigations,* 2022.

6. *Unit 42 Incident Response Report,* 2022.

7. Ibid.

DNS Security

Challenge: Stop Attacks That Use DNS to Penetrate Defenses

The Problem

DNS is a massive internet protocol that carries a tremendous amount of data and is absolutely essential for any business to operate, yet, most organizations fail to properly secure it. The majority of organizations have solutions in place to secure the web and email, but they do nothing to protect their DNS traffic, leaving it wide open for attackers to use for malicious activity such as data exfiltration, C2, ransomware and phishing. Since 85% of modern malware abuses DNS for malicious activity, it is imperative that companies monitor and analyze their DNS traffic.[8]

Solution Requirements

Some organizations try to combat DNS attacks with a block list of known bad domains, which only solves part of the problem. The need is for a way to predict highly dynamic malicious domains. Stopping DNS-based attacks requires a next-generation firewall equipped with best-in-class security services that can use predictive analytics and machine learning-powered detections to instantly identify and block known and unknown DNS-layer threats.

Learn more.

RFQ Questions

Does your NGFW:
- Use predictive analytics and detections powered by machine learning to identify unknown bad domains?
- Integrate threat intelligence to improve detection capabilities?
- Automatically add bad domains to the block list?
- Identify newly registered domain names and block them to lower the risk of type squatting or phishing attacks?

Encryption

Challenge: Secure Encrypted Traffic

The Problem

Most enterprise web traffic today is encrypted, and attackers take advantage of this fact to hide threats from security surveillance. Even businesses with mature, comprehensive security measures in place can be breached if they are not closely monitoring encrypted traffic. Additionally, TLS/SSL encryption is used nearly universally, and end users can easily configure it to hide non-work-related activity.

Solution Requirements

The ability to decrypt TLS/SSL-encrypted traffic is a foundational security function. Key elements to look for include recognition and decryption on any port, inbound or outbound; policy control over decryption; and the necessary hardware and software elements to perform decryption across tens of thousands of simultaneous SSL connections without compromising performance.

Your next firewall must be flexible enough to easily decrypt certain types of encrypted traffic (e.g., HTTPS from unclassified websites) via policy, while leaving other types (e.g., web traffic from known financial services organizations) alone in compliance with privacy standards. The next-generation firewall should apply security and load balancing to decrypted flows across multiple stacks of security devices for additional enforcement. This approach eliminates dedicated SSL offloaders, reducing network complexity and making decryption simpler to operate. It must also offer support for decryption of modern protocols that are gaining widespread adoption such TLS 1.3 and HTTP/2.

RFQ Questions

Does your NGFW:
- Include policy controls to selectively decrypt, inspect, and control SSL-based applications?
- Support bidirectional SSL identification, decryption, and inspection?
- Incorporate SSL decryption as a standard feature?
- Automatically identify applications which cannot be decrypted due to MITM mitigation techniques such as certificate pinning?
- Support SSH control as a means of accessing remote devices? If so, what is the depth of control?

What is the process by which encrypted applications are identified on all ports, including nonstandard ports?

What mechanisms are used to identify evasive applications such as UltraSurf and Tor?

---

8. Unit 42 threat research, Palo Alto Networks, 2022.

Hybrid and Multicloud Security

Challenge: Secure Hybrid and Multicloud Environments

The Problem

Data and applications increasingly reside in the cloud. In a recent study, almost half (48%) of the respondents said they plan to migrate 50% or more of their applications to the cloud in the coming year, with 20% planning to migrate all of their applications.[9]

Organizations must now secure sensitive data in the network and a variety of cloud environments, including SaaS. In addition, legacy security tools and techniques designed for static networks were not designed to work with cloud-native tools or capabilities. Moreover, native security services from the cloud providers themselves typically offer only Layer 4 protections and are specific to that cloud provider resulting in low threat blocking effectiveness.

Solution Requirements

Organizations need cloud security that extends policy consistently from the network to the cloud, stops malware from accessing and moving laterally (east-west) within the cloud, simplifies management, and minimizes the security policy lag as cloud workloads change. The ideal firewall must protect the resident applications and data with the same security posture you may have established on your physical network.

To ensure your ability to secure multicloud deployments, the firewall must support a variety of cloud and virtualization environments:

- **Public Cloud Service Providers**: Amazon Web Services, Microsoft Azure, Google Cloud Platform, Oracle Cloud, AliCloud, and IBM Cloud
- **Software-Defined Network (SDN) Integration**: Nutanix Flow, VMware NSX, and Cisco ACI
- **Hypervisors**: VMware ESXi, Microsoft Hyper-V, Linux KVM, and Nutanix AHV hypervisors
- **Kubernetes Containers**: VMware Tanzu, Rancher, Amazon EKS, Azure Kubernetes Services (AKS), Google Kubernetes Engine, and OpenShift

Learn more.

RFQ Questions

Does your NGFW:
- Create security policies for dynamic workloads in both private and public clouds?
- Ensure consistent security policies for workloads, even when their IP addresses or locations change?
- Track virtual machine and container moves, adds, and changes?

What is the process of building security policies for newly created virtual machines or app containers?

What features are available for integration with automation and orchestration systems?

In virtualized environments, how is traffic classified throughout the virtual machine and among Kubernetes containers (east-west, north-south)?

What are the points of integration within the virtualized/cloud environment?

How does your NGFW create security policies based on VM or container attributes of workloads?

---

9. Mike Loukides, "The Cloud in 2021: Adoption Continues," O'Reilly, December 7, 2021, https://www.oreilly.com/radar/the-cloud-in-2021-adoption-continues/.

IoT Security

Challenge: Reduce Exposure to IoT Security Risks

The Problem

While IoT devices can help organizations increase productivity, efficiency, and revenue, they are also the weakest link of the network for attackers. In a 2021 study, 78 percent of information technology decision-makers saw an increase in the number of IoT security incidents over the previous year. [10]

Existing security strategies fail to protect the vulnerable IoT devices for several reasons. The most important is lack of clear ownership. The IT security team may not be fully aware of the scope and nature of IoT deployments and thus not include these components in the SOC workflow. Many existing tools for asset and endpoint management are not up to date for the need of IoT security. In addition, IoT security products often take a static, signature-based approach to identify devices. This approach cannot scale to keep up with the massive proliferation of new devices or variants of devices being launched every day. Others only provide visibility and lack the native, built-in policy enforcement capabilities required to actually secure these devices.

Solution Requirements

When evaluating your next firewall, consider a solution that can identify and classify all IoT devices on your network, including those never seen before. Your firewall solution should empower security teams to make decisions quickly with full context for each device, understanding device identity, risk level, and any behavioral anomalies. The firewall should then offer segmentation and other policy recommendations based on risk assessment that can be automatically enforced natively. The firewall should also be able to block known and unknown threats to the IoT devices.

Learn more.

RFQ Questions

Does your NGFW:
- Identify and classify all IoT devices on the network, including those never seen before?
- Assess IoT-specific risk and threats?
- Offer and enforce policy recommendations based on risk assessment?
- Share IoT device context with your other IT and security technologies such as asset management, SIEM, EPP, XDR, and NAC?

Mobile Security

Challenge: Protect Mobile Workforce

The Problem

The mobile workforce continues to grow along with the use of mobile devices to connect to business applications, often through public networks and devices that are open to advanced threats. This process increases risk when users are off-premises because there is no network firewall to stop attacks, and the issue becomes even more complex when considering the effects of cloud and bring-your-own-device (BYOD) practices. In addition, remote locations and small branch offices often lack consistent security because it is operationally inefficient and costly to ship firewalls to them or backhaul traffic to headquarters.

Solution Requirements

The mobile workforce and remote locations need access to applications from places far beyond your network. They also need protection from targeted cyberattacks, malicious applications and websites, phishing, C2 traffic, and other unknown threats.

Your next firewall must consistently enable the required levels of visibility, threat prevention, and security policy enforcement to protect your distributed users and locations by delivering next-generation firewall capabilities from the cloud, securing them without the need to deploy physical hardware.

Learn more.

RFQ Questions

Does your NGFW:
- Keep users connected to ensure consistent policy enforcement whether users are on external or internal wireless?
- Safely enable both corporate and BYOD laptops, phones, and tablets?

What are the available options for securing remote users, including all necessary components?

If a client component is included, how is it distributed?

How many users can be supported simultaneously?

Is the remote user security feature set transparent to the client?

How is policy control over remote users implemented (in firewall policy, in a separate policy/device, etc.)?

Which features and protections are provided by the remote capabilities (for example, SSL, application control, and IPS)?

---

10. *The Connected Enterprise: IoT Security Report 2021*, Palo Alto Networks, October 20, 2021, https://www.paloaltonetworks.com/resources/research/connected-enterprise-iot-security-report-2021.

Policy Consistency

Challenge: Maintain Consistent Policies Across the Hybrid Cloud Environment

The Problem

Complexity in security management is on the rise, and company leaders are not happy about it. A recent study found that nearly half (46%) of organizations are consolidating or plan on consolidating the number of vendors they do business with as a way to reduce the complexity of their security systems.[11]

This complexity is often a result of legacy decisions. Organizations have adopted a wide range of point products to address different network and security requirements for applications hosted on-premises, in cloud environments, or both. However, with each product comes a separate policy and interface to manage, creating extra costs, complexity, and gaps in security. Additionally, these products are not integrated and cannot share insights into network access, application access, or policy violations, nor can they provide consolidated logs.

Organizations also find it challenging to onboard new firewall appliances at scale, maintain consistent security policies, and deploy policy changes across thousands of firewalls. This approach causes gaps in security and network performance, leading to staff and cost shortages.

Solution Requirements

To be successful, firewall solutions must deliver security capabilities in a variety of form factors—hardware, software, and containerized—to integrate security protections into the optimal parts of the environment. You must be able to operationalize the deployment of consistent, centralized security policies across tens of thousands of firewalls spanning on-premises and cloud deployments—including remote locations, mobile users, and SaaS applications—through centralized management, consolidated core security tasks, and streamlined capabilities.

For example, you should be able to use a single console to view all network traffic, manage configurations, push global policies, and generate reports on traffic patterns or security incidents. Your reporting capabilities must let your security personnel drill down into network, application, and user behavior for the context they need to make informed decisions.

When these capabilities are delivered from the cloud, your teams can get the networking and security needed in an architecture designed for everything: traffic, applications, and users, no matter their location. In today's constantly changing threat landscape, using a single security vendor to address the vast spectrum of your security and business needs may not be practical. In this case, the ability to integrate with and consume third-party insight and innovation is critical.

When evaluating security vendors, be sure to evaluate the flexibility, extensibility, and programmability of what they offer. Read this e-book to learn about a new approach to securing cloud-enabled organizations as well as delivering speed and agility to enterprise networking and security.

RFQ Questions

Can your NGFW:
- Deliver consistent network security and threat prevention for applications running on-premises and in virtualized and container environments?
- Natively deploy within Kubernetes environments?
- Provision into a continuous integration/continuous development (CI/CD) process?
- Integrate into software-defined networking (SDN) solutions to extend security protections to remote locations for branch segmentation and to meet PCI compliance?
- Automate configuration changes using APIs for every feature?

Does your NGFW allow central administrators to:
- Work directly on the appliance and change configurations as needed without logging in to a central manager?
- Monitor and view changes made by local administrators?
- Quickly roll back changes from specific users and restore working configuration?

Can your central firewall manager:
- Separate log management from core configuration management?
- Ingest logs for throughputs as high as 50,000 LPS?
- Act as a single pane of glass for unified visibility?

---

11. Jon Oltsik, *Technology Perspectives from Cybersecurity Professionals*, ESG, July 2022, https://www.issa.org/wp-content/uploads/2022/07/ESG-ISSA-Research-Report-Security-Process-and-Technology-Trends-Jul-2022.pdf.

Policy Gap Management

Challenge: Close Dangerous Policy Gaps

The Problem

Legacy firewalls allow and block traffic based on ports and IP addresses. This approach is inadequate as port-based rules allow both good and bad applications through the firewall. Applications can easily go through a port-based firewall by hopping between ports, using SSL and SSH, or using well-known open ports such as 80 and 443.

Over time, customers accumulate thousands of port-based rules on their firewalls, and often migrate these rules as-is to their next-generation firewalls. These rules leave dangerous policy gaps. Customers realize that they must migrate to application-based rules for effective security, but this requires significant manual effort—and due to the cybersecurity skills shortage, most organizations do not have the resources. This becomes a high security risk that may cause a business disruption.

Solution Requirements

When evaluating your next firewall, look for one that reduces the complexity of rule and policy management. One way is to discover applications that are running on your network, map them to the legacy rules, and help replace the legacy rules. Your next-generation firewall should help your security team easily replace legacy rules with intuitive, application-based policies. Because rules based on application identification are easy to create, understand, and modify as business needs evolve, they minimize configuration errors that leave you vulnerable to data breaches. These policies strengthen security and take significantly less time to manage. Finally, your next firewall should aggregate telemetry information and apply machine learning to automatically identify required policy and configuration changes. These capabilities can improve security policy optimization to eliminate breaches due to misconfiguration.

RFQ Questions

Can your NGFW:
- Perform stateful inspection for traffic classification prior to application identification?
- Allow port-based controls to be implemented for all applications in the application database?
- Allow administrators to enforce, by policy, the application and port relationship? For example, ensure that IT personnel are the only ones who are allowed to use SSH and RDP?
- Collect telemetry data for ML-based security policy optimization to eliminate breaches due to misconfiguration?
- Offer an API available for custom or nonstandard identity-infrastructure integration?

Once an application is identified, how are changes in application state monitored, tracked, and used within policy?

How does the application database hierarchy expose functions within the parent application for more granular enablement policies?

What levels of control can be exerted over individual applications and their respective functions?

Which enterprise identity repositories are supported for user-based controls?

How are policy-based controls implemented by users and groups for terminal services environments?

What are the differences in application enablement options for hardware and virtualized instances?

Secure Branch Connectivity

Challenge: Securely Connect Branches to Headquarters

The Problem

As enterprises continue to move applications to the cloud, IT teams are challenged to quickly, reliably, and securely connect corporate locations and branches to critical business resources. Software-defined wide area networking (SD-WAN) promises to increase bandwidth while improving connectivity and performance, and organizations are taking note.

However, while SD-WAN offers many benefits, it also brings many challenges such as degraded or bolted-on security, unforeseen architecture and deployment complexity, and unpredictable performance.

Solution Requirements

Your next firewall should extend to your branches the same consistent security that protects your data center and cloud environments. Organizations can adopt SD-WAN safely by implementing a firewall that natively integrates with the SD-WAN to consolidate connectivity and security. This can also help maintain consistent security policies from the network core out to branches. With SD-WAN configuration and monitoring as well as firewall user and application policy workflows available through a single pane of glass, organizations can avoid gaps in their security posture as well as benefit from improved security, simplicity, and efficiency. Read this e-book to learn how to achieve consistent security with SD-WAN.

Learn more.

RFQ Questions

Can your NGFW:
- Natively integrate with your SD-WAN?
- Maintain consistent security policies from the network core out to branches?
- Consolidate SD-WAN configuration and monitoring as well as firewall user and application policy workflows available through a single pane of glass?

Security Coordination

Challenge: Coordinate Detection and Analytics with Other Security Tools

The Problem

Advanced adversaries don't limit themselves to one part of your architecture. Instead, their goal is to move laterally from endpoints to your network, clouds, and other data structures to access and exfiltrate valuable data. Research conducted by Unit 42 found that clients tend to underestimate how long a given threat has been active. In some cases, threat actors have been found to have been active and moving laterally through an environment for a period of six months or more.[12]

With this in mind, siloed security approaches that can only see and understand one slice of your infrastructure produce suboptimal results. They limit the application of analytics and force security analysts to bounce between interfaces to try to manually piece together attacks—a process that is both time-consuming and prone to error.

Solution Requirements

As the number of needed security functions increases, so does the potential value of platforms/devices that can provide meaningful integration between them. If your firewall can act as a sensor and enforcement point for a more comprehensive, machine learning-driven analytics platform (such as an extended detection and response or XDR solution), your security team will gain both efficacy and efficiency in uncovering, remediating, and preventing sophisticated attacks.

Your next firewall should integrate with XDR to allow both your network and security teams to understand the full scope of an attack, share threat context and intelligence, and drive automated response as well as enforcement between the firewall and other enforcement points.

RFQ Questions

Can your NGFW:
- Create a ticket on a change management system based on a malicious event seen on the firewall?
- Trigger a quarantine action for an infected host on the wireless network?
- Be completely programmed via API?
- Collect User-ID information via APIs from wireless controllers about hosts connecting to wireless networks?
- Dynamically incorporate third-party or custom threat intelligence feeds in the firewall without policy commits?
- Support threat feed aggregation, consolidation, and deduplication of threat feeds before pushing the indicators to your firewall?
- Integrate with your next-generation firewall to automate timeout of expired threat indicators to avoid using stale threat intelligence?
- Allow you to target threat indicators from recent APT campaigns and incorporate threat feeds proactively on your next-generation firewall?
- Allow you to enrich cloud-based threat intelligence and IOCs with intelligence based on a confidence rating to reduce the operational overhead from dealing with false positives?

---

12. *Unit 42 Incident Response Report*, 2022.

Zero Trust

Challenge: Adopt a Zero Trust Strategy for Security

The Problem

Conventional security models operate on the outdated assumption that everything inside an organization's network can be trusted. These models are designed to protect the perimeter. Meanwhile, threats that get inside the network go unnoticed and are left free to compromise sensitive, valuable business data. In the digital world, trust is nothing but a vulnerability.

Consider the risk due to insider threats. While not a major cause of intrusions—Unit 42 research cited insider threats in just 5.4% of incidents studied[13]—a deliberate insider attack can be devastating because these malicious actors know exactly where to look to find sensitive information. Seventy-five percent of insider threat cases reported were caused by disgruntled ex-employees who left with company data, destroyed company data, or accessed company networks after their departure.[14]

Solution Requirements

Zero Trust is a cybersecurity strategy that eliminates the notion of trust. In a Zero Trust world, there are no trusted devices, systems, or people. You identify the data, assets, applications, and services most critical to the business, determine who or what should have access based on their specific job function, and enforce a least-privileged access model through network segmentation, granular Layer 7 security policy, user access control, and threat prevention.

When evaluating NGFWs, look for one that can act as a segmentation gateway to enable a Zero Trust architecture. Your next firewall should directly align with Zero Trust, including enabling secure access for all users irrespective of location, inspecting all traffic, enforcing policies for least-privileged access control, and detecting and preventing advanced threats. Zero Trust significantly reduces the pathways for adversaries, whether they are inside or outside your organization, to access your critical assets.

Learn more.

RFQ Questions

Does your next-generation firewall enable you to write context-based policy to determine who or what can access your protect surface?

How does the next-generation firewall leverage network segmentation, prevent lateral movement, provide Layer 7 threat prevention, and simplify granular user access control?

Does the next-generation firewall inspect all traffic for malicious content, unauthorized activity, and data leakage as well as log through Layer 7, both inside and outside, across the network and public or private cloud environments?

---

13. *Unit 42 Incident Response Report*, 2022.
14. Ibid.

Six Reasons to Choose Palo Alto Networks

Best-in-Class Portfolio

Our industry-leading solutions work together intelligently to strengthen security, simplify operations, and improve ROI. Learn more.

Commitment to Zero Trust

Palo Alto Networks is the only company that enables comprehensive Zero Trust throughout your entire digital ecosystem of users, applications, and infrastructure, with continual verification of every interaction. Learn more.

Excellence in Secure Access

We empower and protect the global hybrid workforce with the industry's most complete SASE solution and ZTNA 2.0. Learn more.

Multicloud Protection

Palo Alto Networks offers the only comprehensive cloud-native application protection platform (CNAPP) that provides full-lifecycle, full-stack protection across all clouds. Learn more.

Driving the Autonomous SOC

By leveraging the benefits of today's most advanced AI and automation, Palo Alto Networks empowers security teams to be prepared for what's next. Learn more.

World-Class Threat Intelligence and Incident Response

Our Unit 42 threat intelligence enhances everything we do. Our team is the preferred breach response company for 70+ cyber insurance carriers. Learn more.

Your Next Move

This guide should help you craft a comprehensive RFP to navigate the dozens of possible vendors and find the right fit for your organization. Palo Alto Networks believes that our solutions offer the best value in the industry—and we can prove it. Sign up for the Ultimate Test Drive—right now!

Partner Text Area/CTA