10 THINGS TO TEST IN YOUR FUTURE NGFW

In the market for your next firewall? How do you navigate the risks and opportunities cybersecurity presents to your organization? How can you determine if the features of your new next-generation firewall are what your organization needs to grow and move forward?

The answer is simple: you test it.

Security professionals agree that organizational security should not be approached with a one-size-fits-all mindset. Every organization has unique needs, and their security architecture should reflect that. Security tools, services and features should be flexible enough to address these individual needs while remaining true to the capabilities advertised.

This paper discusses 10 points to consider and actively test in your current security infrastructure as well as your future NGFW. Using these as guidelines for cross-functional conversations, you will widen the lens through which you can view your NGFW to determine if your potential security investments are easy to implement, alleviate operational burdens, and offer your organization the best protection and value, today and in the future.

PREVENT CREDENTIAL THEFT

1

Users and their credentials are among the weakest links in an organization's security infrastructure. As such, the majority of breaches involve credential theft at some point in the attack lifecycle. With credential abuse as part of the attackers' toolset, their chances of successfully breaching go up, and their risk of getting caught goes down.

Why Should You Advocate and Test This Capability?

Preventing credential theft, such as often occurs via phishing attacks, reduces exposure to one of the most prevalent forms of targeted attacks on organizations. These measures are crucial when dealing with targeted phishing attacks, which typically go after non-technical employees through previously unknown phishing sites.

Move Beyond the Status Quo

Most organizations work to stop these attacks primarily through employee education, which is prone to human error by nature.

Technology products commonly rely on identifying known phishing sites and filtering email, but these methods are easily bypassed as checking for known bad sites will miss newly created ones, and attackers can evade email filtering technology by sending links through social media. A next-generation firewall with machine learning-based analysis can accelerate protection. If the analysis identifies the site as malicious, your firewall should be updated and block it.

Still, there will always be never-before-seen phishing sites that are treated as "unknown." To protect your network and users, it's critical to prevent submission of credentials to unknown sites. By using credential filtering, organizations can whitelist authentication to authorized applications and block credential submission to unknown sites.

Recommended RFP Questions

- □ Can the NGFW prevent use of corporate credentials on unknown websites?
- □ Can the NGFW block users from submitting corporate credentials without storing a copy of the hash in the firewall?
- □ How quickly does the NGFW analyze previously unseen phishing sites and update its protections?
- □ Does the NGFW log user attempts to submit credentials in HTTP post?

PREVENT CREDENTIAL ABUSE

2

Attackers can obtain stolen credentials in many ways: phishing, malware, social engineering, brute force or black market purchase. Once attackers have stolen credentials, they can abuse them to enter an organization, move laterally, and escalate privileges for unauthorized applications and data.

Why Should You Advocate and Test This Capability?

Implementing multi-factor authentication on the firewall helps prevent attackers from moving laterally with stolen credentials. MFA allows your organization to protect all types of applications, including legacy applications and client servers. In addition, authentication that occurs at the firewall, before users connect to applications, moves the line of exposure farther away.

Move Beyond the Status Quo

Many organizations have an MFA solution, but it is often challenging and time-consuming to integrate with all applications. As a result, most organizations only use MFA with a handful of applications, such as a VPN gateway or a few cloud applications, leaving many others vulnerable to credential abuse.

Protection at the Network Layer

MFA is a great tool, but it must be implemented in a way that protects all critical applications. Rather than modifying the applications themselves, use your firewall with MFA policy to control traffic to specific applications. The firewall should be able to control access and require authentication before allowing traffic to pass. Attackers operating inside the organization, even from a compromised endpoint, would not be able to complete the MFA.

Tailored User Experience

Policies for MFA that are created within the firewall should be granular, in terms of both the user and the sensitivity of the application. For example, the policy should match the frequency with which users must reauthenticate to the sensitivity of the application.

Accelerate the Time to Protection for Applications

Multi-factor authentication as a part of firewall policy improves the speed of implementation, as you only need to integrate MFA within network policy, rather than changing applications themselves. This allows for quicker deployment of protections to meet compliance. MFA on the firewall stops attackers from using stolen credentials or moving laterally within an organization, and protects all types of applications, including legacy applications and client servers.

Recommended RFP Questions

- □ Does the NGFW support MFA as part of the access-control policy based on the sensitivity of the resource accessed?
- □ Does the NGFW provide choices for a variety of MFA partner technologies?
- □ Can the NGFW support RADIUS and API integrations with MFA partner technologies?
- □ Does the NGFW support MFA policy for any type of application, including web, client-server and terminal applications?
- □ Is the NGFW's MFA capability limited to certain protocols?

PROVIDE DYNAMIC SECURITY POLICIES FOR YOUR DYNAMIC VIRTUAL WORKLOADS

3

When security policies for data center environments are first created and deployed to firewalls, it's assumed that the assigned IP address will remain the same throughout the life of the policy. These policies are static, blanketed and applied in a generic fashion. With data centers transitioning to virtualized environments, workloads are no longer fixed to a particular location or networking schema.

Why Should You Advocate and Test This Capability?

To address security in the virtualized data center, your firewall security policies should be based on the attributes of the workloads rather than tied to static IP addresses, since the data center environment is highly dynamic. This can be done through Dynamic Address Groups on a next-generation firewall.

Move Beyond the Status Quo

Transient workloads are frequently spun up and down to optimize compute resources, repeatedly acquiring new IP addresses. This makes it cumbersome and difficult to manage access-control policies on the firewall when dealing with hundreds or thousands of address groups, each with its own address objects, with constant additions, deletions or changes.

Your firewall should support policies that automatically adapt to the dynamic nature of today's data center, which involves constantly adding, moving or removing workloads for optimal use of compute resources. Adaptive policies help enforce consistent security across your dynamic virtual machines and applications.

Dynamic Address Groups decouple security policies from IP addresses and instead build granular security policies based on the attributes of your virtual workloads. Policies on the firewall use tags mapped to workload attributes. For example, the tag on the firewall may be App-Server, which can be mapped to attributes that identify the specified application server regardless of its IP address. The attributes will continue to place the workload in the desired security policy even if the workload gets relocated.

This helps you build security policies bound to workloads, enhancing your security posture. Dynamic Address Groups lower operational overhead by reducing dependence between applications and security teams.

Recommended RFP Questions

- ☐ How does the NGFW create security policies based on VM attributes of workloads?
- ☐ Can the NGFW create security policies for dynamic workloads in both private and public clouds?
- ☐ Can the NGFW ensure consistent security policies for workloads even when their IP addresses or locations change in the data center?

MANAGE YOUR NGFW USING SIMPLE AND EFFECTIVE TOOLS

4

To be responsive to business needs, security teams need the flexibility to make firewall changes both from a centralized tool and on-site in real time. If a firewall manager allows local administrators to make changes only to a limited set of features, the local team must heavily rely on global teams, potentially located in another region, to make changes. This results in delays, gaps, limited visibility and granular administrator access.

Why Should You Advocate and Test This Capability?

To minimize the delay in making changes locally and keep your security aligned with your organization's guidelines, your firewall should support complete management of all firewall features and offer role-based access control for multiple administrators. Your local firewall managers' tools should support the full feature set on the centralized tool for local administration, allowing local teams to accomplish their respective tasks on time. Your central management tool should augment local data with overarching visibility into the actions of local administrators and, if required, alert and allow for remote override changes to keep the firewall in line with organizational guidelines.

Move Beyond the Status Quo

Ensure Granular Control While Deploying Configuration Changes

In a multi-firewall environment, it is not unusual for multiple administrators to make configuration changes at the same time. It's very likely that one will want to commit recent changes before another is completely done making his or her own. If your firewall manager doesn't allow for selectively committing changes, those incomplete changes will also be deployed. This can have serious security implications, such as users being able to access blocked sites or being blocked from business-critical applications. When selective configuration deployment and rollback isn't possible, administrators would have to manually undo half-baked changes, redo and redeploy them, adding to operational overhead and delaying improvement of security posture.

Manage Logs Effectively at Scale

The central manager acts as a single pane of glass for the organization's security and network, providing a holistic view and context for analyzing security events. In many cases, central firewall managers collect and consolidate firewall logs in multi-firewall deployments. An incoming log rate (generally expressed in logs per second, or LPS) that exceeds the manager's capacity will impact its performance.

Performance impact on the central manager is generally seen through unresponsive user interface or timed-out database queries. In today's high-throughput digital world, it is not uncommon for a single high-end firewall to exceed the LPS capacity of the central manager acting as a log manager. The likelihood of running into capacity issues in a multi-firewall deployment is very high.

High-throughput log processing needs are generally addressed through a separate log management appliance. A firewall manager, in conjunction with a log manager, is the most appropriate solution for most enterprises. With this setup, the central manager is relieved of log management responsibility and can focus solely on firewall management. When provisioned, the central manager queries the data on the log managers to provide centralized visibility and brings raw logs to the central manager only when required, reducing performance impact.

Keep Your Security Posture Up to Date

Each of the many features of a next-generation firewall is purpose-built to address a specific network security need and empower an organization's growth. In a multi-firewall environment, manual firewall configuration changes are inefficient and often result in security gaps and inconsistent prevention. Automation will provide faster, more accurate responses to ever-changing cybersecurity threats.

The preferred way to act on this is to leverage NGFW APIs to automate changes, alleviating network security teams' operational overhead while reducing human error. For this to be possible, your NGFW APIs should allow for automated changes to all firewall features through a full set of flexible APIs.

Recommended RFP Questions

- ☐ Can local administrators work directly on the appliance, and make configuration changes as needed, without having to log in to a central manager?
- ☐ Can central administrators monitor and view the changes made by local administrators?
- ☐ Can you choose which firewall administrator's configuration changes should be deployed on the firewalls?
- ☐ When deployments go wrong, can you quickly roll back changes from specific users and restore working configuration?
- ☐ Can the central firewall manager separate log management from core configuration management yet still act as single pane of glass for unified visibility?
- ☐ Can your log managers ingest logs at high throughput (e.g., 50,000 LPS)?
- ☐ Does your firewall have APIs for every feature so that you can automate configuration changes?

5 LEAN ON AUTOMATION TO PREVENT DIFFICULT-TO-IDENTIFY AND FAST-CHANGING THREATS

With attackers employing more and more automation, security teams are seeing more security events across their organizations every minute. Someone must sift through these events to identify which are high-risk and determine the point of entry that is likely compromised. Once identified, though, this is still just information. It must be turned into an actionable response to mitigate an attack before it succeeds – and before sensitive data leaves the organization.

Why Should You Advocate and Test This Capability?

Done manually, the process of analyzing and correlating vast numbers of security events is difficult to scale. Security teams can easily drown in alerts and miss the critical, actionable ones. Even actionable information depends on human intervention, slowing mitigation and increasing the likelihood of human error. To move quickly enough to mitigate an attack before it succeeds, security tools and services should be able to identify the attack, then generate and distribute protections automatically, as well as integrate with other tools to set off the next action in your workflow.

Move Beyond the Status Quo

As attacks have become automated, the security tools used to discover them must be agile enough to identify known and never-before-seen threats, as well as prevent them more quickly than they can progress through the attack lifecycle. To do so, every step in the process, from discovery to full prevention, should be automated.

Known threats must be pre-emptively blocked without degrading firewall performance or impacting business productivity. Security tools must also analyze and identify malicious behavior – ideally within a cloud environment, to take advantage of elastic compute and scalability – to prevent never-before-seen threats.

A cloud environment also ensures new techniques for the generation of analytics and prevention can be rolled out without causing service interruption or requiring new hardware or manual updates across an organization. It centralizes decision support in a way that all firewalls, clouds and endpoints can get the latest data from a single, trusted source.

Once a new threat has been identified, protections should be automatically generated and implemented across all technologies to provide consistent coverage across the organization. They should also be distributed to all customers in the shared threat intelligence community to stop the spread of the attack.

With knowledge of the malicious behavior of the newly discovered threat, security tools must also use automation to identify potentially infected endpoints within your environment before any sensitive data can be exfiltrated. Using automated data correlation, the tools should identify and surface hosts on your network exhibiting any of the same malicious behavior as the threat.

True automation goes beyond providing information and allows you to configure automated actions. Some organizations may want to automate the immediate quarantine of potentially infected hosts. This can be done by moving a host to a policy that denies it access to all parts of the network while retaining connectivity for remediation efforts. Others may take a more nuanced approach by automatically applying multi-factor authentication to a potentially infected host so that, if attackers gain access to it, they cannot access corporate data or applications.

Automation enables organizations to act against threats without waiting for human intervention, improving response time and, if implemented appropriately and in conjunction with the right tools, preventing successful attacks. A security vendor that offers automation allows security teams to move away from basic operational tasks and focus on strategic efforts that directly benefit the organization. Reducing human intervention reduces avoidable errors, ultimately enabling a more secure security posture.

Recommended RFP Questions

- ☐ Does your security vendor support the capability to automatically generate prevention signatures across the attack lifecycle for all data relevant to attacks?
- ☐ Can your firewall correlate and identify infected hosts in the network, and quarantine them to limit their access in the network?
- ☐ Can your firewall trigger multi-factor authentication to prevent credential abuse and secure critical applications?
- ☐ Can your firewall correlate the threats seen in the network with information obtained from global threat intelligence?

6 INTEGRATE A NEXT-GENERATION FIREWALL INTO YOUR SECURITY ECOSYSTEM

Security teams are increasingly using application programming interfaces, or APIs, to integrate security devices into their overall security ecosystems and streamline operations, which has the added benefit of reducing avoidable human errors.

Why Should You Advocate and Test This Capability?

Leveraging APIs allows for automation of security workflows that need multiple security devices, often from different vendors, to work together. This moves security teams away from the cumbersome, error-prone processes of operating these workflows manually and increases the speed of effective enforcement.

Move Beyond the Status Quo

Easily Cooperate With Various Data Center Technologies

Data center environments often use infrastructure elements from disparate vendors. APIs offer a mechanism for these elements to share data and kick off appropriate actions required in the workflow. As such, the API your security vendor uses must be able to integrate with a broad list of partners via documented and certified interoperability.

The multivendor integration should also extend beyond the data center to vendors of endpoint security, email gateways, wireless security and more.

Comprehensive Feature Support

The ways many security vendors leverage APIs have introduced challenges that often undo the APIs' original promises of simplicity, such as lack of easy-to-follow documentation or comprehensive support for all security features via API. Many established security products fail to incorporate APIs natively. A firewall with natively integrated APIs would allow firewall administrators to view, access and change the entire feature set.

Single, Unified and Comprehensive Standards-Based API

Security products often employ multiple APIs from different standards to control various mechanisms; for example, one API for the firewall hardware, another for the software running on top of it, and a third for the GUI manager. Multiple APIs must be learned, implemented and maintained individually, amounting to a fragmented, counterintuitive approach to the operational simplicity they're meant to offer. When built appropriately, APIs offer the benefit of zero-touch operations.

Recommended RFP Questions

- □ Can your firewall/manager create a ticket on a change management system based on a malicious event seen on the firewall?
- □ Can your firewall/manager trigger a quarantine action for an infected host on the wireless network?
- □ Can your firewall be completely programmed via API?
- □ Can your firewall collect User-ID information via APIs from wireless controllers about hosts connecting to wireless networks?

PROTECT AGAINST EVASIVE AND NEVER-BEFORE-SEEN ATTACKS

7

Evasive threats have become commonplace in today's threat landscape. Malware developers use various evasive techniques, such as wrapping malicious payloads in legitimate files, packing files to avoid detection or extending sleep calls to wait out potential sandbox environments. As organizations have increasingly deployed virtual sandboxes for dynamic analysis, attackers have evolved to focus on ways to evade them, employing techniques that scan for valid user activity, system configurations or indicators of specific virtualization/emulation technologies. These threats are frequently designed with knowledge gained from open source technology used in most malware analysis tools and hypervisors. With the availability and growth of the cybercrime underground, any attacker, novice or advanced, can purchase plug-and-play threats designed to identify and avoid malware analysis environments. The ability to identify and protect against evasive malware is more crucial now than ever.

Why Should You Advocate and Test This Capability?

The SANS Institute has reported that use of malware programs capable of evading detection rose 2,000 percent between 2014 and 2015. Today, most modern malware leverages these advanced techniques, which can bypass traditional, common network security solutions to transport attacks or exploits through network security devices, firewalls and sandbox discovery tools. Although we can't build individual tools to detect every piece of evasive malware, it's critical to utilize systems that can identify evasive techniques and automatically counteract them.

Move Beyond the Status Quo

Fight Automation With Automation

Attackers often make slight modifications to malicious code, resulting in malware variants and/or polymorphic malware. Threat signatures that rely on specific variables, such as a hash, filename or URL, get one-to-one matches only against known threats. This "new" malware is considered unknown, as protections have only been created for the original malware, not its modified variant.

Rather than use signatures based on specific attributes, NGFWs should use content-based signatures to detect variants, polymorphic malware, or command-and-control activity. Content-based signatures detect patterns that allow them to identify known malware that has been modified. This results in signatures capable of automatically preventing tens of thousands of variants created from the same malware family, rather than trying to create signatures for individual variants.

Command and control can pose a challenge, with malware authors creating C2 communications that automatically change the DNS or URL. Automated signatures based on these artifacts quickly become outdated and ineffective. C2 signatures based instead on analysis of C2 outbound communication patterns are much more effective protections that can scale at machine speed when created automatically.

Validate With More Than One Analysis Method

More determined, skilled attackers will create entirely new threats with purely new code, the costliest method for attackers. Any such threat will be treated as an unknown and go undetected.

When an entirely unknown threat enters an organization, the clock begins ticking. Protections must be created and distributed across all security products more quickly than a threat can spread. This can be accomplished by automating various aspects of the analysis, including static analysis with machine learning, dynamic analysis and bare metal analysis. Implementing automation results in accurate identification of threats, enables rapid prevention, improves efficiency, makes better use of the talent of your specialized staff, and improves your organization's security posture.

Create Knowledge Gaps for Attackers

Purpose-built virtual analysis environments add challenges and costs for attackers as they work to avoid discovery. The targeted environment would require different techniques from those of other commonly known analysis environments, making it more likely for you to identify the threat.

Move Beyond Virtual Environments

There are a number of ways to counter threats built to evade analysis environments, and a modern, effective security platform should combine multiple techniques. For example, combining dynamic analysis in a sandbox environment with bare metal analysis has proven effective in countering malware that assesses the environment to determine if it is being analyzed. When employing bare metal analysis, if the file successfully evades virtual analysis, it can be steered to a real hardware environment for detonation and observation. The malicious activity of the file, which would otherwise have remained dormant in the virtual environment, will fully execute in the bare metal environment.

Prevent the Spread of an Attack, Share Threat Intelligence

Threat intelligence sharing allows organizations to benefit not only from their own intelligence but from that of other organizations globally. Should an organization identify an entirely new threat and share that information, other organizations in the sharing network would be able to identify and treat this new threat as “known.” This intelligence should come from multiple sources and be correlated and validated for necessary context, in addition to the generation and distribution of an actionable response, further contributing to rapid, automated prevention.

Recommended RFP Questions

- □ Does your cloud-based malware analysis system support multiple analysis techniques, including bare metal analysis for detecting evasive, sandbox-aware malware?
- □ Does your cloud-based malware analysis system use a custom-coded hypervisor to be effective against sandbox-aware malware?
- □ Does your malware analysis system, after analyzing malware, create threat prevention signatures, such as:
  - Content-based AV signatures to prevent known and unknown variants of malware?
  - Pattern-based anti-spyware signatures to detect communications to known and unknown C2 infrastructure?
- □ Does your cloud-based malware analysis system support malware analysis for file types of Windows®, Android® and macOS® operating systems?

INCORPORATE EXTERNAL THREAT INTELLIGENCE IN THE NGFW

8

Firewalls have the ability to import lists of predetermined rules and policies that, once consumed, allow the firewall to act against the objects outlined in the list. Afterward, firewall administrators are responsible for updating the firewall to reflect newfound threats, protections and policy roles. With attackers employing more advanced methods, such as automation and evasion, having the most updated security posture possible requires moving at machine speed.

Why Should You Advocate and Test This Capability?

Incorporating automation and dynamic lists into your next-generation firewall is the most effective and efficient way to improve your organization’s security posture. Dynamic lists are often provided by your NGFW vendor, and can be updated manually or by integrating third-party threat intelligence. As a result, changes to rules and policies only need to be made to the list, and all firewalls tied to the dynamic lists will regularly and automatically import the most updated protections.

Move Beyond the Status Quo

Dynamic Lists

When new threats are identified, it falls to the firewall administrator to create a new rule or policy so that the firewall can respond appropriately. This must be done for each risk object and potentially each firewall in the network – a labor-intensive, often error-prone, manual process.

Working with dynamic lists dramatically reduces manual efforts and improves response time. Modern dynamic lists include protections against known, and high-risk, malicious IP addresses validated by your NGFW vendor. They also protect against high-risk IP addresses drawn from correlated third-party data that has not been validated by your vendor, which you can opt in to at the level of policy enforcement appropriate for your organization.

Third-Party Threat Intelligence Feeds

Organizations subscribe to third-party threat intelligence feeds for access to continuously updated data on potential threats and attack sources, ultimately increasing their knowledge base. These feeds provide massive amounts of data on raw indicators of compromise, or IoCs, which is used to turn unknown threats into known before attackers have a chance to compromise an organization.

Turning threat intelligence into actionable protections, much like creating new rules and policies based on activity seen on the firewall, is a time-consuming, manual process that many security teams struggle to manage.

The data from threat intelligence feeds must be current and formatted, potentially requiring the data format to be changed to a consumable form. The data must also be correlated to validate whether a given IoC is malicious, correlating multiple IoCs to reveal larger patterns of malicious behavior, and adding necessary context, such as the priority and relevance of newly identified threats. Once the data has been validated and enriched with context, security teams can much more efficiently create and distribute protections to address specific threats across various security enforcement points. Alternatively, vendors can push protections out to enforcement points, but consolidation with local traffic isn’t as effective. Without completing these steps, threat feeds remain inert reams of data.

Automation is necessary to rapidly improve your security posture with the latest threat intelligence, alleviate manual intervention and eliminate human error. Based on context collected from outside your organization, automation can turn unknown threats into known protections more quickly than attackers can successfully complete the attack lifecycle.

Recommended RFP Questions

- □ Can your NGFW dynamically incorporate third-party or custom threat intelligence feeds in the firewall without policy commits?
- □ Does your security architecture support threat feed aggregation, consolidation and deduplication of threat feeds before pushing the indicators to your firewall?
- □ Does your security architecture integrate with your NGFW to automate timeout of expired threat indicators to avoid using stale threat intelligence?
- □ Does your security architecture allow you to target threat indicators from recent APT campaigns and incorporate threat feeds proactively on your NGFW?
- □ Does your security architecture allow you to enrich threat intelligence based on a confidence rating to reduce the operational overhead from dealing with false positives?

PREVENT SUCCESSFUL RANSOMWARE ATTACKS

9

Ransomware is top of mind for organizations these days, and rightfully so – it has brought many organizations' operations to a halt. This not only forces organizations to pay to regain access to the encrypted data but also incurs costs from lost opportunities or customers, equipment replacement, new security technologies, damaged reputations, and so on. This is not a new development, and to address the ransomware problem, security vendors have updated products with tacked-on ransomware prevention features.

Why Should You Advocate and Test This Capability?

No single security product can successfully prevent ransomware on its own. As there are multiple stages in the attack lifecycle, there should be multiple layers of defense to prevent ransomware attacks. Your organization's ability to effectively protect against ransomware lies in the natively engineered automation and integration among your security products to proactively detect and prevent ransomware. A multilayered defense is the most effective way to disrupt possible ransomware attacks, and new additions to the security architecture should complement protections throughout the network.

Move Beyond the Status Quo

There Is No Silver Bullet

Protecting against ransomware requires visibility into network traffic and enforcement of applications, as well as user- and content-based policies. It also requires security products to protect against known and unknown exploits, malware, and command-and-control traffic, as well as prevent access to known malicious and phishing URLs.

Ransomware Is Time-Sensitive

Automation is the only way for prevention to move more quickly than a ransomware attack can transition through the full attack lifecycle within your organization. To identify and block unknown threats, malicious files and URLs must be detonated, analyzed and observed for malicious activity. Once a file or URL is identified as malicious, protections must be created and automatically distributed throughout the security infrastructure – across the network, cloud and endpoint. This ensures all points of entry are informed and capable of protecting against the latest version of the ransomware.

Combine Preventive Efforts

For effective prevention, you must employ automation and share information among various security tools that work together to identify known and unknown malware and exploits in your environment, and subsequently identify and quarantine any infected host, preventing the attack from spreading.

Threat intelligence should always be a component of your organization's threat prevention efforts, and your firewall should be capable of dynamically updating preventions against malicious IPs, domains and URLs based on information gathered from the threat intelligence cloud and IoCs.

Recommended RFP Questions

- □ Can your NGFW block executables and other risky file types from unknown applications and URLs to prevent ransomware attacks?
- □ Can your NGFW automatically and dynamically import all known IoCs (i.e., IPs, domains and URLs) into the blacklist to be proactive against all known ransomware families?
- □ Does the threat intelligence cloud integration with the NGFW support dynamic updates for malicious URLs related to ransomware in the malware category of the URL filtering database?
- □ Does the threat intelligence cloud integration with the NGFW support dynamic updates for malicious domains related to ransomware as DNS signatures to be automatically blacklisted or sinkholed?
- □ Can your NGFW learn about threats or ransomware behavior from your endpoint protection software and vice versa?

OFFER CONSISTENT PROTECTION, NO MATTER WHERE USERS OR APPLICATIONS ARE

10

Users are becoming more mobile, and they need access to applications from remote locations around the globe. With the growth of cloud usage, the applications may not always reside in the data center. However, many organizations do not have visibility into traffic when users access the internet and cloud applications off-premise, and thus security is often compromised.

Why Should You Advocate and Test This Capability?

Your organization should be able to protect all users in the same manner, without the need for different security profiles depending on the user's location. Since security policies are more effective when they can be administered in a consistent manner, a single set of tools and a common policy framework will give security teams greater control.

Move Beyond the Status Quo

Many companies use VPNs solely for remote access (bringing traffic back to headquarters). When users are not connected, organizations often use other products for off-premise users. However, those products only solve a fraction of the security issues users encounter. For example, products based on DNS filtering block connections to some known bad domains, and web security products block some known bad URLs. Both measures are easily bypassed. Thus, these add-on products add administrative complexity to the environment with fragmented policy, more consoles, steeper learning curves and heavier workloads.

Your organization should maintain the same protection wherever your users work, whether on-premise or off. Deployment options should provide flexibility to support consistent coverage for all users and locations. This way, no matter where users are, they can easily connect to the cloud service or a firewall for security and receive the same protections from known and unknown threats.

Recommended RFP Questions

- □ Can your NGFW provide consistent security policy for mobile users?
- □ Can you protect users who are not behind an NGFW?
- □ Can your NGFW use multiple physical/virtual firewalls to support an always-on VPN connection?
- □ Can your NGFW utilize the cloud to bring protection closer to the user?

Attackers and their techniques are more sophisticated than ever, enabling advanced attacks that are targeted, automated, evasive and span multiple environments.

Your future firewall, as well as the various security products that make up your security infrastructure, should be comprehensive and include:

- The best technology with the ability to rapidly, automatically prevent attacks at every step of the attack lifecycle for known and unknown threats. These products should deliver consistent, risk-appropriate protection for data and users regardless of location. Your security ecosystem should offer agile, flexible updates, allowing you to adapt to changing risks and workloads.
- Operational efficiency delivered by automation and API integrations, reducing time spent on error-prone, manual tasks. Security should be operationalized over various environments without straining resources or budget, and without adding complexity, allowing security teams to focus on strategic efforts that are more critical to the organization.
- Knowledgeable, responsive service and support teams to minimize your learning curve and keep improving your security posture long after the initial migration. You should be able to maximize your investment over time and achieve higher levels of security.

When planning your next purchase or assessing your current firewall deployment, it's important to test the capabilities and features of your firewall with all security teams in your organization. The 10 points of consideration discussed in this paper, when tested, will help determine if your next firewall purchase matches the needs of your organization in its current and planned states by keeping future innovation in mind.

For more information, as well as live conversations with peers and technical advisers on these topics, visit our **Test Your Firewall Overview page**.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com