IDC
Analyze the Future

I D C A N A L Y S T C O N N E C T I O N

Rob Ayoub
Program Director, Security Products

Segmentation Firewalls: Comprehensive Threat Protection Where and When You Need It

August 2018

Network topographies have changed drastically since the first firewall was introduced. As more applications have moved to the cloud and the number of devices accessing the network has exploded, the perimeter has all but disappeared, while threats have increased exponentially. Application control, URL filtering, and advanced malware detection have become table stakes for network security gateways. Increasingly, deeper ties between network and endpoint technologies, as well as network and analytic technologies, are being created to improve visibility and efficacy across the infrastructure.

The following questions were posed by Fortinet to Rob Ayoub, program director for IDC's Security Products group, on behalf of Fortinet's customers.

Q. What is a segmentation firewall (SFW), and what role does it play in enterprise campus security?

A. SFWs control threats inside the perimeter or within the boundary of a network. This network could be an on-premises private cloud or an off-premises public cloud. While traditional firewalls typically focus on protecting the perimeter as network traffic moves in and out of a company, SFWs focus on traffic inside the perimeter where the default is to trust traffic, users, applications, and data.

We are seeing more and more attacks target resources internally located in the network. A 2016 IDC survey indicated that the top 3 attacks being experienced by organizations were ransomware, phishing, and spyware. These attacks are becoming more difficult to stop at the perimeter because the attacker has to get only one user to click a malicious link to infect an entire organization. With traditional firewalls, once an attack passes the perimeter, the firewall deployed at the edge becomes useless to mitigate it. Segmentation firewalls enable defense in depth, protection that shows up through the network, between sensitive areas. Even if malware penetrates the perimeter, it's not as devastating to the internal organization.

Q. How do organizations benefit from segmentation firewalls?

A. As mentioned previously, SFWs provide organizations with added layers of protection inside the network as opposed to just on the perimeter. Given today's increasing focus on cloud services (a recent IDC survey showed that 50% of security professionals now spend over half their time in the cloud) and the distributed nature of workers, the ability to apply firewall protection across deployment types (on-premises, private, and public clouds) gives organizations a distinct advantage.

Adding internal firewalls is not necessarily an advantage by itself. IDC believes that organizations need to ensure that any solution they are considering also provides highly scalable segmentation and the ability to break a large security policy into smaller sets of distinct security policies based on roles and/or functions (e.g., departments, business units) to segregate traffic, reduce attack surface, and contain threats. The solution also must provide ultra-low latency, which results in improved user experience across delay-sensitive applications and services.

Further, it is important to note that an SFW solution can offer infrastructure consolidation. Segmentation firewalls with sufficient capacity of high-speed interfaces can replace L3 switches and move away from a flat network to a network that offers increased visibility, control, and mitigation while reducing capex and opex.

Q. What are the challenges to SFW deployment?

A. Because most customers' networks are complex, with security policies created by many different stakeholders, deployment presents the following challenges:

- **Concerns about network performance/disruption.** IT organizations are always sensitive about the performance of the internal network. They are sensitive to customers' complaints about the network being slow. In fact, IT bonuses may be tied to network uptime, throughput, and employee satisfaction. Any new security solutions that are added to the network must be proven to deliver wireline performance with extremely high levels of reliability (99.999%).
- **Cost/budget considerations.** Justifying security solutions is always difficult, but attackers long ago recognized the opportunity to take over user accounts and move easily within their victims' internal networks. The recent hacking of the U.S. federal government's Office of Personnel Management (OPM) highlights the sophistication of these kinds of attacks on confidential data.
- **Perceived difficulty with deployment.** Aside from the previously mentioned issues, deployment problems can arise in two areas: time to value and integration. Time to value is often critical because customers want actionable analysis, policy control, and mitigation as fast as possible. Integration means consolidated management across a shrinking number of consoles, with the goal of moving toward a single pane of glass where everything is visible to a security analyst.

Q. What are the features to look for when evaluating SFW solutions?

A. Evaluating SFWs can be challenging for customers. Customers likely already have a traditional firewall solution in place and may be tempted to stay with what they know. However, given the nature of digital transformation occurring in organizations today, along with the focus on cloud and SaaS adoption, organizations should have a security solution that provides fine-grained security policy and better protection within the context of this new paradigm, beyond basic perimeter protection.

As a result, customers should evaluate several areas when they are looking to deploy SFWs. IDC believes that customers should pay attention to the following three key areas:

- **Performance.** This is about not just throughput speed but also throughput of advanced threat protection. In a segmented world, enhanced visibility into internal network traffic without degrading throughput, application performance, or information retrieval is extremely important. Additionally, ensuring the lowest latency possible to maintain line speeds will drastically affect the end user. There is already a good chance that traffic has to leave the corporate network to reach a cloud or SaaS provider offsite; any latency hurts.

- **Manageability.** A key component of SFWs is manageability. Administrators do not want to open a new console to address new functionality. That is one of the key challenges of many of the overlay segmentation solutions available on the market today. An SFW should offer a single pane of glass (to manage segmentation and security policy irrespective of the location of security assets) as well as integrate with existing security functions and management consoles.

- **Incident response.** An SFW should provide full life-cycle protection via prevention through segmentation of critical corporate assets, detection of anomalous behavior, analysis of the validity and severity of the threat, and mitigation of attacks. Because attacks may be trying to navigate the network to get to sensitive information, SFWs must offer quick, nondisruptive deployment that can provide rapid response to administrators. Further, there are many times that files are not immediately known good or bad. An SFW should provide layered defense and the ability to move suspicious samples to sandboxing for detection of advanced malware instead of simply allowing files to pass through the network.

Q. How will segmentation firewalls allow an organization to be future proofed as we move into the cloud?

A. IDC believes that organizational security will be increasingly reliant on segmentation. Making the transition to SFWs and to cloud and SaaS at the same time allows organizations to install security early, getting ahead of potential attacks. We already see organizations moving to lightweight development tools — containers and serverless computing. These fine-grained levels of computing will require more explicit security controls and greater segmentation than those normally applied by organizations. By strategically investing in SFWs today, organizations are investing in a future that addresses deployments from on-premises, into the cloud, and through SaaS providers.

ABOUT THIS ANALYST

Rob Ayoub is a program director in IDC's Security Products program. In this role, he provides thought leadership and guidance for clients on a wide range of security products ranging from traditional network security products such as firewall, IPS, and UTM to emerging products designed to protect the cloud and the Internet of Things (IoT).