FORTINET

Risks That Arise from Digital Transformation

Why Traditional Network Segmentation Fails to Secure the Expanding Attack Surface

Table of Contents

FORTINET

Executive Overview

Digitally transforming networks are characterized by migration of applications and services to the cloud, growing accommodation of user-owned technology ("BYOD"), and increasing deployment of Internet-of-Things (IoT) devices. All these changes have dissolved the traditional network perimeter into numerous microperimeters, which results in a much larger attack surface for the organization.

This broad attack surface makes it easier for rapidly evolving threats to penetrate traditional perimeter defenses and move laterally inside the internal network, which is often flat and consists of network infrastructure that inherently cannot perform threat detection and protection. Network operations teams scramble to patch the gaps with various segmentation techniques, but security effectiveness and cost efficiency are impeded by a lack of deep visibility into traffic and an inability to define access policies in terms of business needs. CIOs also face a persistent trade-off between the need for rigorous traffic inspection to reduce risks and the cost to implement best-of-breed security.

Companies with cybersecurity practices that do not keep pace with their digital transformation initiatives are more likely to see $1 million or more in losses from cyberattacks.[1]

Introduction: The Expanding Attack Surface and Rise in Lateral Threats

When networks were bounded by the walls of the enterprise, and users stayed within the corporate network or on virtual private networks (VPNs) on company-issued devices, strong perimeter security was a reasonable approach. That model began to break down as a result of digital transformation (DX).

DX Fractures the Perimeter

DX allows enterprises to modernize their networks to offer more revenue-generating services, better user experience, and ubiquitous access. DX also enables organizations to adopt multiple cloud services and applications, with assurance of high availability and scale on demand, plus the ability to increase network efficiency and achieve business goals. To support these objectives, networks have needed to absorb IoT and user-owned devices as well as additional traffic volumes and velocity resulting from the growth of business applications and DevOps.

The adoption and growth of these different services and devices—from mobile devices to IoT devices and from multiple cloud services to DevOps initiatives—fractures the traditional network perimeter into many small micro-perimeters that are associated with each user device. This expanded attack surface makes it harder for CIOs to protect against an evolving advanced threat landscape.

Internal Networks Become Increasingly Vulnerable

Even with defenses on every perimeter, bad actors will find a way in. Once inside, they can move with relative ease across the network, launch attacks, and exfiltrate corporate data assets without detection. This is because internal networks are often "flat"—designed with minimal security checkpoints or other network devices that would obstruct throughput and application performance.

Intruders are also harder to detect now that more than 72% of network traffic uses secure sockets layer (SSL) or transport layer security (TLS) encryption protocols.[2] Unsurprisingly, upwards of 50% of malware—such as Zeus, Dridex, and TrickBot—now hides in SSL/TLS encrypted packets. Unless the firewall has SSL/TLS inspection turned on, these attacks go undetected.[3]

More than 72% of network traffic uses SSL/TLS encryption protocols,[4] and 50% of attacks employ SSL/TLS encryption to deliver their malicious payloads.

Reactive Security Drives Network Segmentation

To protect their fragmented and vulnerable network perimeters, organizations are increasingly turning to network segmentation. But traditional network segmentation is ineffective, leaving gaps in network defenses and exposing business-critical information to bad actors.

Network-based Segmentation Results in Security Gaps

Traditional network segmentation falls short when it comes to protecting today's dynamic corporate networks from the evolving advanced threat landscape. In typical segmentation scenarios, the goal is to define groups of IP addresses or segments of virtual local-area networks (VLANs), each of which contains a category of users or resources. Other techniques such as VXLAN segment by workloads and virtualized applications.

These approaches can be highly problematic. Because the business process, compliance requirements, and network access needs of an organization are vastly more complex than the structure of its network, it is very difficult to define secure network-based segments that will be simultaneously accessible to all authorized users and applications and completely inaccessible to all others.

For example, the European Union's General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS) include stipulations that require effective isolation of sensitive data. The problem is that most sensitive data is distributed, and users who are authorized to access the data may reside on the same network segment as other users who are not authorized to access that same data. If segments must be defined in terms of the network architecture, it becomes very difficult to find a segment that includes all the authorized users and none of the unauthorized ones, or includes all the data that falls under the compliance rule and none of that which does not. The end result is reduced visibility.

A best-effort segmentation will inevitably result in security gaps—access scenarios that the network architects did not envision—which bad actors can exploit.

Trusted Today, Rogue Tomorrow

Even if it is possible to create user, application, and data segments that comply with regulations and business requirements, the organization is still vulnerable to attack if access permissions are based on assumed trust in initially vetted users, devices, and applications. The actual trustworthiness of network resources can change unexpectedly; numerous organizations have been surprised by attacks from presumably trusted employees and contractors. External bad actors also use phishing techniques to steal trusted user credentials.

Some organizations choose to block all access pending verification of trust status. While this approach may dramatically minimize risk, the feasibility—in terms of time, resources, and complexity—is virtually impossible to implement and maintain.

More than one-third of reported breaches involve internal users, and 29% involve stolen credentials.[5]

Hard to Justify Cost of High-Performance Security

By 2022, global spending on security products and services is expected to grow 45% from current levels, with privacy regulations and compliance concerns contributing heavily to the increase.[6] This expenditure is justified if CIOs can correlate their investment in increased security with a decreased number of breaches. Indeed, organizations that experienced zero breaches in the past year were four times as likely to increase their cybersecurity budgets as those that experienced more than six breaches that year.[7]

The challenge for CIOs is to identify which investments in threat protection actually increase security without undercutting productivity, customer experience, or other key business metrics. The nearly ubiquitous trade-off seems to be between the rigor of network traffic inspection and the speed at which it can be performed, so as not to create a perceptible slowdown in application performance.

The SSL/TLS Inspection Trade-off

When a firewall inspects data packets, it necessarily delays their progress through the network. The extent of the slowdown—the impact on users and applications—depends on the processing power of the firewall and the configuration of firewalls on the network.

Next-generation firewalls (NGFWs) perform a variety of inspections, but one of the most problematic for throughput is SSL/TLS inspection. A careful review of firewall specification sheets reveals higher performance for basic firewall functionality and reduced performance when SSL/TLS inspection is turned on. This is evidence of the toll that packet decryption and inspection take on the firewall processors. Thus, in many instances when SSL/TLS inspection is turned on, organizations must double or even triple the number of firewalls they have deployed—a dramatic capital expenditure that also increases operational costs. Another alternative is to purchase dedicated SSL/TLS inspection appliances, but this adds both cost and complexity.

As a result of the SSL/TLS inspection performance degradation, some organizations elect to turn off SSL/TLS inspection for throughput-critical network segments. However, as the percentage of encrypted traffic climbs, and as more hackers cloak their malware in encrypted packets, this dramatically ratchets up risk—with nearly three-quarters of network traffic going unchecked when SSL/TLS inspection is turned off.[8]

Throughput a Key Consideration for TCO

Cost-effective security is that which maximizes threat protection while minimizing total cost of ownership (TCO). Solution comparisons would be easier if security products could be matched, either for security effectiveness or for TCO, and compared based on the other characteristic.

Since this is nearly impossible, the independent testing organization NSS Labs has developed a useful metric called TCO per protected Mbps, which relates cost to network throughput.[9] Among the NGFWs that NSS Labs has tested, TCO per protected Mbps ranges from $2 to $57, with an average of $20.86. In large, high-volume networks, the choice of NGFWs and the number of NGFWs required can make a big difference in TCO.

"By 2022, global spending on security products and services is expected to grow 45% from its 2018 levels."[10]

Many organizations still view security and data privacy as an operational expenditure. Furthermore, only about half say their organizations treat security as a strategic asset.[11]

Isolated Remedies Impede Risk Management

Too many firewalls represent more than a cost burden. They also pose a security risk if they operate in isolation from each other. Advanced threats can spread across network segments and target multiple points on the attack surface concurrently. If firewalls across the corporate premises and in public and private clouds cannot automatically share threat information and apply the latest global threat intelligence, they unnecessarily lengthen the time to detect threats and respond to attacks. As it stands, the mean time to identify a breach is 197 days, a number that puts organizations at serious risk.[12]

A significant part of the problem facing CIOs is the lack of integration among security solutions, which impedes their ability to respond automatically to threats, intrusions, and breaches. This is due not to a lack of security assessment tools and services but to the difficulty of collecting and organizing data from multiple disparate sources in a timely manner. And when this data collection and reconciliation is manual, it becomes an overwhelming—and fruitless—effort, which is exacerbated for CIOs with typically lean IT staffs.

Lack of integration and automation is a big reason why it takes 197 days to even detect a breach.[13]

Conclusion: The Idea Is Right, but the Approach Must Change

There is no longer room to doubt that cyberattackers will penetrate perimeter defenses. When they do, if the networks are open and unsegmented, they are ripe for exploitation.

Internal network segmentation is imperative, but traditional methods ultimately fail due to a lack of security efficacy and unjustifiable TCO. If CIOs are to remain accountable for the protection of their organizations' data assets, they will need to adopt a more business-driven, DX-ready approach.

[1] "The Cybersecurity Imperative," securityindustry.org, accessed May 28, 2019.

[2] "Q3 2018 Threat Landscape Report," Fortinet, November 2018.

[3] "Study Reveals Hackers Increasingly Use Encryption to Hide Criminal Activity," Lifeline Data Centers, accessed March 21, 2019.

[4] "Q3 2018 Threat Landscape Report," Fortinet, November 2018.

[5] "2019 Data Breach Investigations Report," Verizon, May 2019.

[6] "New IDC Spending Guide Forecasts Worldwide Spending on Security Solutions Will Reach $133.7 Billion in 2022," IDC, October 4, 2018.

[7] "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, April 26, 2019.

[8] "Q3 2018 Threat Landscape Report," Fortinet, November 2018.

[9] Thomas Skybakmoen, "Next Generation Firewall Comparative Report Security Value Map™ (SVM)," NSS Labs, July 17, 2018.

[10] "New IDC Spending Guide Forecasts Worldwide Spending on Security Solutions Will Reach $133.7 Billion in 2022," IDC, October 4, 2018.

[11] Bill Briggs, et al., "Manifesting legacy: Looking beyond the digital era: 2018 global CIO survey," Deloitte, 2018.

[12] "2018 Cost of a Data Breach Study," Ponemon Institute, July 2018.

[13] Ibid.

www.fortinet.com

339188-0-0-EN

August 2, 2019 12:51 PM

eb-risk-that-arise-from-digital-transformation