WHITE PAPER

Flat Networks Inevitably Fall Flat When Attacked —Using Secure Segmentation To Protect Your Business

Network and Business Leaders Must Think Differently To Build Effective Enterprise Security

Hybrid IT and the adoption of work-from-anywhere (WFA) strategies have led to the exponential expansion of new network edges. And for many organizations, this has resulted in an expanded and fragmented attack surface that has become a perfect opportunity for bad actors to launch cybersecurity attacks from new attack vectors, undermining the ability of network and security leaders to maintain business operations without disruptions.

Once a perimeter is compromised, the hackers can roam around freely in the flat network and create havoc by stealing data or shutting down business until the ransom is paid off.

Traditional flat networks, including network-based segmentation or even microsegmentation techniques, cannot detect and prevent many of today's more sophisticated attacks. Many of these networks still provide single-time authenticated users and devices with unfettered access to virtually any application. Such an implicit trust policy provides free rein across permitted segments and reduces the visibility across the network, especially into encrypted paths. The lack of integration between security and network constrains their ability to perform essential firewall functions, let alone advanced security inspection, at the growing number of dynamic network edges and junctions, making them unable to contain cyberattacks.

The Challenge of Securing Disparate Networks

To accelerate digital innovation and optimize and develop new products, organizations are deploying new hybrid IT architectures comprised of campuses, data centers, interconnecting branches, home offices, mobile workers, and multi-clouds. And nearly all these networks are being enhanced with 5G, which adds hyperperformance to an already complex network environment.

This challenge has been compounded by the recent transition to a WFA approach. Some employees work from home, others on-site, and many spend part of their time in each location—with their devices following them everywhere. Meanwhile, applications continue to migrate to one or more clouds, especially as organizations consume more and more IaaS and SaaS services. Looking at the mobility of users and the disparate locations of applications, the question facing many IT teams is, "How do network and security leaders deliver consistent security everywhere? And how can users safely consume applications from any location, on any device, at any time?"

Complicating the matter further, these WFA and hybrid IT paradigms have led to an exponential expansion of new network edges, which have expanded the attack surface and fragmented visibility and control. The result has been a perfect platform from which bad actors can successfully launch cybersecurity attacks and undermine the ability of network and security leaders to maintain business continuity. While some of this network transformation has resulted from intentional digital acceleration, including a response to the global pandemic, some of it is also happening organically. Merger and acquisition (M&A) activity, for example, often results in a diverse infrastructure with limited coordination or visibility between different parts of the organization.

One challenge arising from these expanding and fragmenting attack surfaces is they create an array of new paths through which criminals can attack, and new interconnected devices, applications, and network environments for them to target. The need for new devices and software to support digital acceleration efforts has contributed to the growing volume of vulnerabilities being targeted by new or improved cyber threats. CVEs (Common Vulnerabilities and Exposures—the list of publicly disclosed computer security flaws) reached an all-time high in 2021, and that list is only expected to grow.[1] This has caused many IT teams to struggle with keeping their distributed devices and applications patched—especially as home networks leverage personal technologies to access business applications deployed in hybrid cloud and on-premises environments—a fact that cyber criminals have been all too eager to exploit.

And at the same time, threats are increasingly sophisticated, automatically seeking and exploiting vulnerabilities with advanced malware, making security a reactive exercise in many organizations. Increasingly sophisticated threats—many enhanced with automation and artificial intelligence (AI)—regularly target high-priority sectors such as critical infrastructure, healthcare, information technology, financial services, and energy. Ransomware, in particular, has become a significant concern for most organizations. 85% of respondents to a recent survey[2] indicated that they are more concerned about ransomware than any other cyber threat.

For years, network engineering and operations leaders have responded to these challenges by building strong perimeter defenses externally to prevent attacks and then segmenting their networks internally for operational controls.

Difficulty Managing Disparate Networks: Is Segmentation the Answer?

For years, network engineering and operations leaders have responded to these challenges by building strong perimeter defenses externally to prevent attacks and then segmenting their networks internally for operational controls.

Traditional network segmentation techniques based on IP addresses have primarily been augmented with VLANs. More recently, VXLAN-based segmentation techniques support large-scale virtualization deployments and enable granular controls. Other methods include VMware NSX segmentation for virtualized workloads and Cisco ACI Application segmentation using physical switches. And there is a plethora of host-based segmentation techniques that leverage agents running on hosts that need to be segmented.

These microsegmentation techniques enable access control policies to be defined by workloads, applications, or architectural attributes such as the virtual machines (VM) on which the applications, data, and operating systems reside.

However, segmentation and microsegmentation alone are not the panacea they are sometimes hailed to be. Segmented and microsegmented networks must still perform advanced security inspection at each segmentation edge and juncture. Otherwise, they will be unable to prevent intrusions from moving laterally across the devices and applications that connect to and traverse the resulting flat network, whether within a single segment or for the many applications and workflows moving across multiple segments.

Why Traditional Segmentation Fails To Protect the Enterprise

Access control for internal network segments tends to be designed from the architecture up. As a result, security is not intrinsically and deeply integrated into networking. This tactical approach means that security policies, inspection, and enforcement cannot easily adapt to changing business needs, leaving security gaps targeted by cyber criminals.

There are three critical reasons why segmentation alone will not protect today's dynamic hybrid networks.

1. The trust valuations on which access policies are based tend to be static, implicit, and unrestricted. The inability to continually verify users and devices creates compliance and control challenges, especially when a user or device becomes compromised.
2. Access control policies cannot be effectively enforced due to a lack of advanced (Layer 7) security detection and inspection across the hybrid IT. Isolated legacy security solutions cannot see and control these components efficiently or adapt in real time to changes in the network.
3. These problems often stem from network engineering and operations staff planning their segmentation architecture without adequate attention to identity, visibility, and security. Understanding each of these issues and their aggregate impact can lead to a more risk-aware and responsive approach to segmentation.

A Traditional Bottom-up, Bolted-on Network Security Approach Is Also Ineffective

Evolving organization needs usually dictate corporate network design, with the rules governing who and what can access which network resources determined by business policies, industry standards, and government regulations. The network operations team uses these rules to configure the access control settings in the routers and switches, permitting users, devices, and applications to access specific network resources. While this approach may seem straightforward, network engineering and operations leaders should immediately recognize two downsides to this approach.

To effectively manage security risks, network engineering and operations leaders must have current and accurate information on the trustworthiness of users, applications, and network assets at all times.

First, the business processes, compliance requirements, and network access needs of an organization are vastly more complex than its network structure. Consequently, it is challenging to use the network architecture to define and secure network segments for those resources that must be simultaneously accessible to all authorized users and applications (and utterly inaccessible to all others). Unfortunately, traditional network connectivity—including more modern intelligent application-driven SD-WAN solutions deployed in hybrid IT architectures—does not include seamless security integration. Other issues, such as the proliferation of unknown IoT devices and ongoing OT and IoT integration, create additional challenges around visibility and security.

In practice, these approaches leave security gaps—access scenarios that the network architects did not envision, especially as security solutions struggle to keep up with automated, adaptive changes to the network—which bad actors are taking advantage of.

Trust Valuations Based On Statistics and Implicit Access Allow Breaches

To effectively manage security risks, network engineering and operations leaders must have current and accurate information on the trustworthiness of users, applications, and network assets at all times. Internal firewalls or other access control mechanisms that manage traffic flows between network segments must constantly identify, verify, and monitor users and devices. If those trust assessments are out of date, segmentation technologies become useless at preventing threats from moving laterally through the network. Many of today's most damaging security breaches are due to compromised user accounts and passwords, and users with inappropriate levels of access exacerbate this problem.

Some organizations have responded to these dangers by practically locking down their networks, trusting no user or application, or creating layers of verification before permitting access. This approach creates its own issues that can be just as counterproductive. While network engineering and operations leaders must protect sensitive assets, users and devices that legitimately require access to assets should not be impacted by unnecessary burdens that affect productivity and user experience.

Security Requires End-to-end Visibility. Without It, Security Controls Mean Little

Most traditional approaches to segmentation assume that all necessary network security components are in place and ready to execute whatever access control policies the IT team defines. However, this assumption may not hold for several reasons.

First and foremost, the rising volume of encrypted web traffic has now reached 95%.[3] While this is great news for organizations looking to provide secure and encrypted access to applications, it also offers an opportunity for bad actors to hide their activities in secure channels. Making things worse, a growing number of network teams intentionally turn off secure sockets layer (SSL)/transport layer security (including TLS 1.3) inspection in their NGFWs to optimize network performance because they fear the impact on performance. The inability of nearly all legacy firewalls to inspect encrypted traffic at digital speeds means that criminals can find their way in and out of an enterprise network undetected to launch ransomware attacks and exfiltrate data.

Second, due to budgetary constraints, or because deployment and management require too many resources, many network engineering and operations teams hesitate to deploy advanced network security and other solutions everywhere they are needed—within the enterprise, in every cloud, and on every endpoint and IoT device. And the ones they do deploy tend to operate in isolation. Unfortunately, point security solutions cannot easily share threat intelligence on known, emerging, or zero-day threats or easily participate in a coordinated response.

Acting promptly is essential to disrupting an attack sequence, as outlined by MITRE.[4] However, the overall effectiveness of security components is severely compromised when they are not tightly integrated. For example, when an isolated firewall detects a suspicious packet, it may take hours (or longer) for the information to be seen by a security administrator and disseminated to the rest of the network.

Third, organizations cannot respond effectively to mitigate the impact of breaches without dealing with malicious websites, known malware, and unknown attacks. This requires integrating XDR, IPS, and sandboxing technologies to automatically quarantine and test suspicious packets. Conversely, the lack of integration between security elements and between security and the network makes orchestration and automation across hybrid networks impossible. And the subsequent reliance on manual operations invariably leads to breaches, as they are far too slow and error-prone.

Segmentation With Network and Security Convergence Becomes Ineffective

What's required is an integrated, coordinated approach to security. A fully integrated and unified security solution is the only way to ensure consistent, adaptable threat detection and response across a segmented hybrid IT architecture.

Without this, network engineering and operations leaders who believe their segmented network is well-protected are likely working under a false sense of security. But without real-time data, it is impossible to know. The best way to determine whether the security strategy being relied on to protect a dynamic, hybrid network is effective is to run ongoing end-to-end security assessments. However, without the end-to-end visibility provided by a fully integrated security platform—a security fabric able to touch and adapt to every edge of the network—a reliable assessment is not possible, preventing IT leaders from accurately reporting on their company's security posture.

It is up to network engineering and operations leaders to ensure that the access control policies applied to internal network segments can withstand today's perpetually expanding and fragmenting attack surfaces. Addressing this challenge starts by converging network and security into the hybrid network architecture. Only with careful attention to segmentation design can a company be confident in its ability to thwart attackers looking to sow destruction by moving laterally across the network.

[1] "A record number of software vulnerabilities was reported in 2021," The Stack, December 7, 2021.

[2] "Fortinet Ransomware Survey Shows Many Organizations Unprepared," Fortinet, September 29, 2021.

[3] "HTTPS encryption on the web," Google, accessed January 15, 2022.

[4] "ATT&CK Matrix for Enterprise," MITRE ATT&CK, accessed January 31, 2022.

February 4, 2022 2:57 PM

1440498-0-0-EN