eBook

7 Symptoms Your Legacy Firewall Isn’t Fit for Zero Trust

Zero Trust adoption is on the rise...

Today's IT security stakeholders are well aware that zero trust is the right security model for modern digital businesses. Surveys show that as many as 78% of enterprise security programs have either adopted zero trust network access or are planning to do so in the future.[1] They know that focusing directly on securing users, data, and applications—instead of the network—is key to protecting today's data-driven, remote work-enabled enterprises.

Decades ago, when hub-and-spoke network designs were state-of-the-art, firewalls and the networking infrastructures built around them were young, spry, and healthy. They were the right technology choice for that era, serving faithfully and doing their jobs well. In the modern cloud computing era, however, their presence is a burden, and castle-and-moat architecture designs are fundamentally incompatible with the zero trust paradigm.

Here's a diagnostic guide outlining seven symptoms that your firewall is unfit for today's zero trust security world. Any one of these seven symptoms is a sign that your organization needs a cloud security cure.

[1] Source: Cybersecurity Insiders, Zero Trust Adoption Report, 2019.

SYMPTOM #1

A lack of visibility when trying to inspect traffic at scale

Regardless of their form factor, appliance–based firewalls are simply unable to inspect SSL–encrypted sockets layer (SSL) encrypted traffic at scale. This becomes more and more of a problem as the percentage of global internet traffic that's SSL–encrypted increases. Attackers know about this increase and are concealing more and more advanced threats within encrypted traffic.

If your firewall suffers from this condition, you'll notice a performance degradation of 50% or more whenever you try to turn on SSL inspection. You'll have to upgrade to a higher capacity firewall or add more appliances (or virtual firewall instances) just to maintain the performance that's acceptable for your users.

85%

of global internet traffic is encrypted today.[2]

WHAT'S THE CURE?

- Move to a cloud–delivered service that can provide cloud native firewalling capabilities rather than trying to leverage and scale virtual machine (VM) versions of outdated physical appliances. Only true cloud services and solutions are infinitely scalable to meet today's traffic needs.

85%

of network administrators agree that firewall capabilities are best delivered via the cloud.[3]

[2] Source: European Union Agency for Cybersecurity, Encrypted Traffic Analysis

[3] Source: Zscaler, Network Firewall Survey

SYMPTOM #2

Unawareness of lateral movement

Firewalls were designed to protect the perimeter of castle-and-moat style networks. The idea was that once the firewall had made a decision about whether or not to allow its ingress, all traffic within that perimeter could be trusted unconditionally. In such architectures, most users were on-site, more infrastructure was on-premises, and most applications lived within the data center. None of these things hold true any longer.

Today's reality is that 70% of traffic is internal to the network, meaning that it flows between servers and applications within the enterprise's private cloud or data center. Perimeter-based defenses leave few if any means for inspecting or blocking this traffic, giving attackers free rein once they've gotten into the network.

Once you've gained access to this sort of network, it's trivial to discover all the assets to which it's connected. The user needs nothing more than an open-source scanning tool to find every IP address within the network. From there, disseminating ransomware—or exfiltrating valuable data—is a simple matter, and there's nothing a firewall can do to stop it.

64%

of today's network administrators believe that firewalls are ineffective at stopping lateral movement.[4]

57%

of IT decision-makers strongly believe that firewalls cannot stop ransomware attacks.[4]

WHAT'S THE CURE?

- Implement zero trust network access that allows connections only after verifying device and user identities, verifying security status, and enforcing security policies—for every single connection, every time. This makes it possible to establish direct and secure connections between users and applications, rather than unprotected connections to a network.

[4] *Source: Zscaler, Network Firewall Survey*

SYMPTOM #3

Severe policy inflammation

Security teams are attempting to achieve zero trust within legacy network architectures by configuring policies that segment networks into ever-smaller pieces. This is microsegmentation in theory, but the effort and administrative effort required for upkeep quickly become unmanageable in practice.

To protect today's applications, businesses must deploy growing numbers of virtual firewalls all over the network. This results in a tsunami of policies that requires endless configuration and reconfiguration to build something resembling zero trust enforcement.

Like their physical appliance ancestors, virtual firewalls cannot scale beyond a certain point. Eventually, you'll need thousands, if not tens of thousands, of policies, which creates a management nightmare.

WHAT'S THE CURE?

The secret is separating networking from application and resource access control. Zero trust network access makes it possible to grant individual users direct and secure access to applications, not network segments. This means that users can be connected right to the applications they need while traffic follows the shortest possible path, and administrators and security teams no longer need to worry about the underlying plumbing.

It can't be deployed overnight, but its diligent implementation can simplify IT, network, and security management while offering better performance for end users.

SYMPTOM #4

The risk of infection spreading across your public cloud assets

Public cloud providers offer virtual firewalls on their online software marketplaces that are supposedly certified to meet their customers' needs. These firewalls are often nothing more than virtual versions of appliance–based firewalls running as VM instances in the public cloud.

Running one of these firewalls in the cloud essentially extends your legacy network architecture outwards to encompass cloud resources. This gives attackers who can breach your firewall–based defenses the opportunity to move freely within an expanded network and opens access to your cloud assets to anyone inside your network.

Additionally, configuring policies to govern traffic between workloads in the public cloud and virtual private clouds is messy and cumbersome. You'll need virtual firewall instances on every egress and ingress point in your cloud architecture. Think for a moment about the cloud's inherent interconnectivity, and you'll quickly understand why this design is so unwieldy.

Plus, you'll have to manage a convoluted routing and networking infrastructure just to make this cloud architecture work with the rest of your legacy network.

> Remember, firewalls were not designed to stop lateral movement.

WHAT'S THE CURE?

- Invest in a modern platform that acts as an exchange between workloads, no matter where they're located. This both prevents attackers from moving laterally to access network resources and simplifies management and troubleshooting. Plus, it gives admins granular, conditional access control that can be revoked if context is changed.

SYMPTOM #5

“Permit any-any” addiction spiraling out of control

Cloud transformation is changing business on a global scale, and organizations across all industries are leveraging the agility and freedom to innovate offered by the cloud. If you’re part of an IT or security team, it’s simply a matter of time until you deal with a cloud migration project—if you aren’t already doing so.

The problem is that it’s taxing and cumbersome to configure legacy firewall-based architectures to secure cloud assets. Policies proliferate, complexities abound, and what’s more, users need access to applications to be productive. What can you do?

90% of IT and security administrators admit that they have applied highly permissive policies* —at least temporarily—to speed up projects and give users the access that they need. Over time, permissive policies add up and are eventually ignored or forgotten, increasing the organization’s risk of suffering a breach or falling victim to a devastating ransomware attack. Of course, these practices directly contradict those of a zero trust, least-privileged access approach.

85%

of organizations will have adopted a cloud-first strategy by 2025.[5]

95%

of new digital workloads today are being deployed on cloud native platforms.[5]

WHAT’S THE CURE?

Seek out a cloud based zero trust solution that’s simple to implement and operate. Not only will a unified zero trust platform with a single management console be easier to configure and manage, but it will offer more robust security than a legacy perimeter firewall.

[5] *Source: Gartner, “Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences”*

SYMPTOM #6

Potentially infectious internet exposure

Perimeter firewalls were designed to serve as network front ends. They're internet-exposed assets by nature, allowing direct access to internal networks and resources if they're breached. This means that using a legacy firewall as a gateway to deploy virtual private network (VPN) services inherently puts your network at risk.

The severity of these risks is evidenced by a string of recent successful breaches by attackers who exploited vulnerabilities in legacy VPNs. The Colonial Pipeline ransomware attack, the largest publicly disclosed cyberattack against critical infrastructure ever to take place within the US, occurred when attackers "exploited a legacy VPN that shouldn't have been in use," according to the company's CEO.[6]

Firewall based VPNs offer no way to implement granular access controls or restrict which users can connect to particular resources. Hence, relying on VPNs is an all-or-nothing approach that extends your network's attack surface from the cloud all the way to individual employees' home wireless routers and networks. And, the further out your network expands, the more damage attackers can do, and the faster they can do it.

Firewall-based VPNs offer no way to implement granular access controls or restrict which users can connect to particular resources.

WHAT'S THE CURE?

- Look for a VPN alternative that enables secure access to applications by establishing one-to-one connections between users and applications on a dynamic identity- and context-aware basis. Such solutions use inside-out connections that make apps invisible to the public internet, delivering better performance than VPNs alongside dramatic improvements in security.

[6] Source: "Colonial Pipeline hack explained: Everything you need to know," TechTarget, April 2022.

SYMPTOM #7

Traffic congestion

The distributed enterprise has entered the mainstream, and most companies are embracing hybrid and remote working models to keep up. But when a large number of users are remote and you're still relying on a legacy castle–and–moat network architecture, you'll need to backhaul large amounts of traffic back to the corporate data center for an inspection by your firewall.

Needless to say, this architecture is illogical and complex. Legacy firewalls and appliance–based security stacks are time–consuming and cumbersome to manage. If you're using leased MPLS lines, you're paying a premium for a complex routing, switching, and traffic segmentation infrastructure. This is why interest in software–defined wide area networking (SD–WAN) is increasing—but adding network overlays only serves to increase the complexity and costs associated with firewall management.

Application performance and end user experiences both suffer when you're backhauling traffic. Not to mention latency, a perennial problem that becomes even more of an issue as organizations rely more heavily on bandwidth–intensive communications apps like Zoom and Microsoft Teams.

WHAT'S THE CURE?

A cloud–based zero trust solution places security controls where today's users and applications reside—in the cloud. It enforces policy inline and at the edge so traffic doesn't need to make any extra hops. And because it operates in the data path, a zero trust platform can monitor every connection and automatically pinpoint and remediate performance issues.

THE ZERO TRUST CURE

How Zscaler can heal your network and its architecture

The Zscaler Zero Trust Exchange™ is a cloud native platform purpose-built for zero trust. The Zero Trust Exchange allows direct and secure connections based on the principle of least-privileged access, and it inspects content deeply and verifies access rights based on identity and context before permitting any connection to be made.

Zscaler's AI/ML-based policy engine, powered by the world's largest security cloud, understands context based on user, device, and application information and uses this context to make intelligent decisions about access levels and restrictions to keep users and data safe. And the Zero Trust Exchange brokers direct one-to-one connections between users and applications, ensuring that applications are invisible to the internet, eliminating the attack surface.

Our approach makes zero trust security accessible and simple for our customers. That's why industry leaders and expert analysts agree that the Zero Trust Exchange is the most mature, easiest-to-use zero trust platform.

Deploying the Zscaler Zero Trust Exchange is fast and easy, and it offers a comprehensive array of integrated inline security that supercharges its leading security service edge (SSE) capabilities. These include:

- **Cloud-gen firewall**
- **Advanced cloud sandboxing**
- **Secure web gateway (SWG)**
- **Data loss prevention (DLP)**
- **CASB**
- **and more**

For more information, visit:
https://www.zscaler.com/technology/cloud-firewall

zscaler™ | **Experience your world, secured.™**

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.