White Paper

Five Network Security Challenges and How to Navigate Them with Zero Trust

For the past few decades, hub-and-spoke networks have extended the corporate network to remote users and locations, including branch offices. They were built and optimized to connect back to a centralized data center, where security resided. Since everything was a part of the flat network, security was designed to place a barrier between the trusted network and the outside world (internet). This model of perimeter security using firewalls was known as castle-and-moat security. This model worked well in the past when all the users and applications were local, but enterprise needs have changed as remote work has exponentially increased and more applications have moved to the cloud.

These changes have created new challenges for organizations that are applying network security architectures to secure a hybrid workforce and cloud-based applications. Let's explore these challenges in detail:

#1

Unknown and uncontrolled risks causing business disruption and losses

Cybersecurity becomes more challenging each day with advanced attacks and threats from sophisticated attackers that are able to find and breach firewalls, VPNs, and cloud-based virtual firewalls. Every internet-facing firewall, whether in the data center, cloud, or branch can be discovered, attacked, and exploited. Once discovered, adversaries will look for vulnerabilities and exploits to gain access. After the device is breached, the doors are open for attackers to steal data and deny access, or they can choose to move laterally to other target devices in the network and look for vulnerabilities.

Traditional security architectures are incapable of preventing these sophisticated attacks. Once a user, good or bad, enters a "secured" network, they become trusted users and get lateral access to all the applications, even when they shouldn't. Virtual firewalls are just as risky as their physical counterparts, because they, too, can be discovered for attacks, often in a much larger number than physical firewalls, increasing the risk further.

Most adversaries don't attack the first machine they encounter. Instead, the threat first surveys the environment to determine how it can move laterally across the network to infect additional resources. It can quickly and quietly move across the network to deposit ransomware into more than one system. Once critical mass has been achieved, the ransomware encrypts all these resources at once, delivering a crippling blow to the organization. This is enabled by the flat nature of network security architectures.

As an analogy, consider burglars breaking into your house through the bathroom window. They don't have anything to steal from the bathroom, but they can move from there to your bedroom or any other location where valuables are kept, and there is nothing to stop them as no room has locked doors or other protection.

How to prevent cyberthreats with zero trust

To better secure the access of applications, you need to eliminate your organization's attack surface and enforce security inline and at the edge. By making apps invisible to adversaries and accessible only by authorized users, the attack surface is practically eliminated, and access to applications—on the internet, in SaaS, or in public or private clouds—is always secure.

How does it tackle lateral movement of threats? Zero trust creates direct connections between authorized entities such as an authenticated user to a specific application.

67% of organizations strongly agree that firewalls are unable to effectively provide fast, secure access for remote users[1]

Only the authenticated user has access to that requested application and no other user can access it. They cannot find the application, which not only eliminates the attack path but also ensures threats cannot propagate laterally to infect other devices or applications.

Relating back to our burglary analogy, in this case it's near impossible for the burglars to find the house because with no attack surface the house cannot be found. Even if they find it somehow, every part of the house – be it a bathroom, living room, or bedroom – is independent and disconnected from each other as each has its own unique access. This way, burglars are incapable of moving from one part of the house to another.

With zero trust, controls are configured to verify identity and context, where context gets continuously checked. A zero trust solution should be able to decrypt all data, identify potential data loss, and stop threats from being exchanged. A secured connection is established through a range of contextual and spatial factors that are continuously validated for a user such as geolocation, IP address, device posture, and time of day. This is done without the user even knowing it so that an approved user is not interrupted while doing their work.

#2

Operational inefficiencies due to complexity

One of the most daunting tasks of securing an organization is policy distribution across scattered infrastructure that includes cloud-based and hardware infrastructure. Companies determine their business policy to designate at a high level what their employees can and cannot access. These business policies are then translated into network policies since the perimeter security model is driven by network access. For distributed infrastructure, where more applications are SaaS or cloud-based than in a data center and users are more likely remote than in office, applying network policies gets increasingly complicated because the network perimeter has now expanded beyond hardware infrastructure in the data center, to all the locations where applications and users reside. Consider an operator defining policies for such a network – they would have to define access policies when the user is in office, policies for SaaS applications, firewall policies, IPS/IDS policies, and many more. In short, it's a nightmare.

Modern applications don't just reside on a single cloud, but may have dependencies spread across a multi-cloud environment that are often required to communicate. Managing applications in multi-cloud environments is particularly more complex than stitching together secure connectivity across multiple clouds and data centers. This requires a patchwork of site-to-site VPNs, firewalls, transit gateways, and peering policies that expand the challenge exponentially.

Network operators must predict future requirements and conduct extensive capacity

75% of organizations agree that it is challenging to manage firewall hardware, upgrades and deployments[1]

planning to accommodate future bandwidth and scaling needs. Underestimating the network needs chokes performance, and on the flip side, overestimating results in unnecessarily high costs and equipment sitting idle. Additionally, there are numerous point products that require regular intervention by security teams to perform tasks like software updates, patch management, troubleshooting etc. These tasks can be critical to keep an organization secure, but may take weeks, or even months, to execute.

How to decrease complexity with zero trust

A zero trust policy enforcer sits in between the entities like mobile devices, IoT, etc. that are trying to connect and the resources like cloud applications, SaaS applications, internet applications, etc. that the entity is trying to access. It applies business policies (what their employees can and cannot access) and context in a variety of ways to come to an enforcement decision, and then brokers authorized connectivity to the requested resource. The inline enforcement of business policies removes the complexity of translating business policies into network policies seen in perimeter based models.

An integrated zero trust solution secures all SaaS, internet, and private applications using a single platform, as opposed to multiple hardware-based or virtual security solutions that are hard to manage and maintain. A unified zero trust platform with a single management console is much quicker to configure, easier to manage, simplifies policies, and offers more security than perimeter security solutions.

A cloud-based zero trust solution places security controls, users, and applications in the cloud, making it easy to scale. As the volume of users and applications increases, it ensures scalability with a consistent, fast and seamless user experience. With increased visibility across users, clouds, and workloads, zero trust simplifies operations and troubleshooting.

#3

Loss of productivity and collaboration due to poor user experience

Users expect applications to work when they need them, whether connecting via corporate Wi-Fi, working at home, or working on the road. They have no interest in how an application is accessed or what networking and security model is used in the back end. When applications are not accessible or slow to respond, there is degradation in productivity and an increase in user frustration.

The hub-and-spoke network architecture requires remote and branch offices to connect back to the central office (data center) through firewalls with MPLS and to remote users with VPN.

300%
increase in the percentage of total employees that are remote users[4]

This architecture creates a flat network that extends to all locations requiring all network traffic to flow to a central security stack. Sending traffic from a remote user through the data center and out to the cloud before returning to the user, and following the same path in reverse, adds unpredictable latency, hence degrading the user experience. The same issue pertains to virtual firewalls, as it is also a part of the flat network architecture that requires all network traffic to flow to the virtual firewall that is located in the cloud – creating a new choke point in the cloud.

It is essential for organizations to provide the best possible user experience to all users—including employees, partners, suppliers, and customers—in any location, as they access applications from any device. But this can prove challenging for IT and security teams as users, data, applications, and devices are more distributed than ever.

How to enhance user experience using zero trust

Zero trust addresses user performance issues by enforcing policies inline, at the edge, so no extra hops are needed, providing direct connections to applications regardless of user location or device. Direct connections eliminate the need to backhaul traffic through centralized security controls that add latency. By operating in the data path, a zero trust platform can also monitor every connection and automatically pinpoint and remediate performance issues.

An edge-delivered zero trust solution scans all content in a single pass without copying packets and adding latency. This approach is starkly different from the chained model of physical or virtual appliances, where each security service independently processes packets, adding incremental latency at each hop. With a single scan, policies can be applied on a variety of security engines with minimal latency.

Critical Unified Communications as a Service (UCaaS) applications, like Microsoft Teams and Zoom, demand low latencies to run effectively. An effective zero trust solution empowers operators to cater to these low latency, high availability demands by directly peering with application companies to enable direct connection based on availability and capacity of the application. For instance, if a M365 user is accessing the application from Texas, he/she will be connected to the closest data center and a security check will be performed inline. It enforces policy inline, at the edge, so no extra hops are needed — a huge transition from hub-and-spoke architecture.

To elevate employee collaboration and productivity, zero trust must monitor these applications and remediate issues quickly with Digital Experience Monitoring (DEM) capabilities. Being an inline solution that operates in the data path, it is way easier to monitor every connection and automatically pinpoint and quickly remediate performance issues.

#4

Siloed IT teams slowing transformation

Business transformation requires IT transformation as well. However, transitioning to a cloud-based, zero trust solution and replacing hardware infrastructure can be a daunting task. It's a challenge for both the organization and teams within IT like security, networking, operations, and others.

One of the primary hurdles to digital transformation in organizations is the lack of communication within IT teams. It's not intentional – these teams have been designed to work on different areas of network and security infrastructure. They work on individual components and not necessarily work toward solving an overall problem. The teams are used to working on their respective solutions—for instance the security team will install firewalls, enable VPNs, and make sure the security stack is up and running, whereas the networking team makes sure routing and switching is working well, and protocols like MPLS, OSPF and others are up and running. The two teams do not collaborate often unless there is something related to interoperability. Cloud-based infrastructure modernization calls for them to work together, which is a big shift from the traditional way of operating. This shift can be difficult to navigate without the right tools, training, and process.

67%
of security professionals agree that cloud security operations is a better long-term career path than firewall administration[1]

On the other hand, organizations have invested in existing network security architectures and need a good justification to move to a new architecture. Changing the mindset of the teams who will champion a transition to the cloud is often a challenge, as security has been done the same way for decades. Network operators who have been operating firewalls and VPNs for years may also fear that they will not have the skills to operate cloud-based security solutions.

How to tackle transformation with zero trust

A cloud-based zero trust platform simplifies security management and operations. Network, security, and operations teams can collaborate to transition away from a perimeter based approach to a business policy-based solution that transforms existing networking and security infrastructure with a cloud-based zero trust solution. Reducing that burden allows teams to utilize the time for strategic projects such as data analytics, security optimization, and other activities that more directly support overall business objectives. The organizations are much more secure when teams break down the silos— communicating and working together as one.

Transitioning to a cloud-based zero trust solution also reduces the burden on the IT team to purchase, manage, maintain, and oversee hardware—opening up additional time to focus on other projects. CISOs and CIOs are no longer accountable to accurately predict the future to plan for hardware requirements and bandwidth consumption costs. Through clear communication and a solid plan, organizations can earn the trust and support of their IT and security teams, and succeed with cloud transformation.

#5 High infrastructure costs due to inefficient deployments

The network infrastructure required to support hub-and-spoke architectures—running on protocols like MPLS—is expensive to acquire and deploy, and requires an experienced IT team to maintain it. There is also the additional bandwidth cost incurred due to unnecessarily routing of traffic back to the data center, even when it is not required, like when accessing a cloud-based SaaS application. Beyond the network infrastructure, the cost of security infrastructure—including firewalls, switches, load balancers, access controls, VPNs, sandboxes, and intrusion prevention systems—is high, extending well beyond the considerable price tag attached to these technologies. There is also the cost of installing, configuring, provisioning, testing, and troubleshooting, all accompanied by the added burden of ultimately maintaining these systems. All these costs get multiplied when you have different point products and need highly skilled people to make them work together.

CIOs and CISOs must accurately anticipate future organizational capacity to allow for hardware requirements and the bandwidth consumption costs of sending all traffic over MPLS to the data center for inspection. It is a delicate balance: underplan and you're not able to effectively scale as demand grows; overplan and you have high, unnecessary costs. Additionally, underestimating network needs may impede productivity, but overestimating may result in high costs and unused equipment. Lastly, each location likely needs unique appliance deployment, which can result in an influx of disparate products strung across your infrastructure.

For internet-bound traffic, it makes more sense to use broadband connections, which cost a tiny fraction of network security infrastructure, however, these connections must be secured. But how? Deploying gateway security in every branch office to enable direct connections would be similarly exorbitant.

50% of all corporate data is stored in the cloud[2] and

70% of business apps are SaaS-based[3]

How to reduce costs with zero trust cloud transformation

Switching to a cloud-native zero trust solution enables organizations to cut costs while improving security through elimination of VPNs, public cloud transit costs, and bespoke networking architectures. Zero trust mitigates the extraneous costs associated with an increase in remote access, whereas organizations with perimeter-based solutions have had to scale their existing firewalls and VPNs with a high cost of appliances and infrastructure eating into their IT budgets.

Zero trust eliminates the need for costly MPLS networks that need complex routing, switching, network segmentation etc. with fast, secure, direct-to-cloud access, and secure cloud-to-cloud connectivity. Additionally, a cloud-based zero trust architecture streamlines security and reduces deployment timelines to days rather than months, all while helping to detect, prevent, and avoid expensive data breaches that could cost millions to an organization. A cloud-based zero trust solution is much more cost-efficient and easier for enterprises to scale quickly as they can purchase as they need, removing the need for extensive planning and over-purchasing.

Achieve true zero trust with Zscaler

The Zscaler Zero Trust Exchange delivers zero trust by leveraging the largest security cloud on the planet to provide fast and secure connections allowing your employees to securely work from anywhere, on any device, using the internet as the corporate network. Unlike firewalls and VPNs, the Zero Trust Exchange is founded upon the principle of least-privileged access, meaning no user or application is inherently trusted. Instead, connections are authorized through company policy surrounding user identity and context. Once the business policy is verified and enforced, the Zero Trust Exchange brokers the connection between the intended resources. Users and devices are connected directly to applications, never to the corporate network.

Learn more about the Zero Trust Exchange: www.zscaler.com/platform/zero-trust-exchange

Watch this webinar on why firewalls cannot do zero trust:
info.zscaler.com/webinar-why-firewalls-cannot-do-zero-trust?utm_source=digital

Sources:
[1]Virtual Intelligence Briefing (ViB) Networks Security Survey 2021
[2]Statista. Percent of data and sensitive data stored in the cloud worldwide.
www.statista.com/statistics/1202541/sensitive-data-cloud-location
[3]Better Cloud. (2021). The State of SaaSOps 2021.
stateofsaasops.bettercloud.com/?_ga=2.164919740.241347015.1636678142-1969514686.1636678142
[4]Grady, John. (2021). The State of Zero Trust Security Strategies. Enterprise Strategy Group.
https://info.zscaler.com/resources-industry-report-the-state-of-zero-trust-security-strategies

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 SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com