netskope

WHITE PAPER

Delivering Real-time Cloud Security Without Trading Off Performance

EXECUTIVE OVERVIEW

There has been a long-standing tradeoff between security and performance, and security often gets the short end of the stick. In today's digitally-transforming world, performance is more important than ever. Businesses of all types demand high-speed access to online resources for their employees and customers and slowing things down is not an option. When there are problems accessing the network or applications are slow, it can mean anything from reduced productivity and an overwhelmed IT help desk to lost revenue resulting from downtime.

While network teams focus on performance and availability, security teams are tasked with managing risk tied to data breaches. These two goals have traditionally been at odds, given the impact that delivering security can have on performance. For the most part, user experience and ultimately the speed of the business tend to get a higher priority than security. This unwritten rule forces security teams to severely limit the scope of their security controls to methods that don't impact performance. This ranges from turning off TLS decryption to foregoing inline security altogether and focusing on less intrusive, out-of-band methods of deployment. The result is performance at the expense of security and with the rise of data breaches, this puts the business at risk.

This paper outlines the challenges that impact the ability to deliver high-performant and reliable real-time security and how Netskope addresses these challenges with one of the world's largest and fastest security networks.

PERFORMANCE CHALLENGES WITH DELIVERING INLINE SECURITY

The public internet is great for many things from browsing websites to watching streaming video, but it was not built to deliver fast, reliable, and consistent performance. If you peel back a few layers, the public internet leaves enterprises blind to outages, is comprised of thousands of networks interconnecting with no end to end performance SLAs, and has no notion of capacity management. This is acceptable for most consumer applications, but not ideal for conducting business.

LATENCY IS THE PERFORMANCE KILLER

The problem starts with network latency, or the "round-trip time" of a packet of data, which every networking professional knows has a direct effect on the throughput performance for users accessing resources over a network. Whether accessing Office 365 or Salesforce.com, poor performance equals poor user experience and the network is always the first to be blamed.

ADDITIONAL LATENCY CHALLENGES

The geolocation of the user is only one component of the latency challenge. The latency problem gets worse when additional factors are introduced. These include network congestion, hot-potato routing, and tromboning. Network congestion can result in queuing delays, packet loss, and dropping new connections.

Hot-potato routing is the practice of passing traffic off to another autonomous system as quickly as possible. Hot-potato routing is the normal behavior of most settlement-free peering agreements and has

the effect that the network receiving the data bears the cost of carrying it between cities. The result is a cost savings for the carrier, but at the expense of losing control over the network routing.

The trombone routing effect if when a distributed organization is forced to use a single exit point to the Internet, and vice versa. For example, network traffic from remote locations and mobile users is being backhauled to the corporate data center before exiting the Internet through a firewall appliance. Responses then flow back through the same stack and travel from the data center to the remote user.

All of these factors contribute to increased latency. When you add inline security and are servicing users globally, you have a recipe for poor end user experience and ultimately a failed security deployment.

LIMITED COMPUTE RESOURCES

Traditional appliance-centric approaches with a fixed set of computing resources limit the ability to perform real-time security functionality such as TLS decryption without impacting the performance of the appliance. The result is that security functions are often disabled or appliances are replaced with more expensive models or separate purpose-built appliances, increasing cost and adding complexity.

INTRODUCING NETSKOPE NEWEDGE

Netskope NewEdge is a global network infrastructure that enables Netskope's cloud-native security platform to deliver real-time security without the traditional security and performance trade-off. It enables fast and reliable delivery of advanced security functionality like SSL/TLS inspection, deep inspection (Cloud XD), inline malware scanning, and inline DLP.

NewEdge was built and is run by a world-class platform engineering team who have helped to launch and scale some of the world's largest cloud services, carriers, CDNs and networks including Amazon Web Services (AWS), Level3 Networks, Limelight Networks, VMware, Twitch, Microsoft and CenturyLink.

NewEdge employs the following capabilities to overcome the performance challenges.

Low latency global reach

NewEdge POPs are globally distributed with more than 50 locations worldwide by the end of 2019. Getting closer to where users are is the first step towards addressing latency challenges.

Unrivaled capacity and performance

NewEdge was built to serve the needs of the largest enterprises in the world with the capacity to support hundreds of millions of concurrent users globally, 2Tbps of network throughput per location or 100Tbps globally by the end of 2019, and accessible by most of the world's population with an average latency of only 18.4ms as of July, 2019. Netskope is launching new POPs at a staggering rate of one per week, further reducing the average latency.

Interconnect with consumer and commercial last mile providers

NewEdge POPs are collocated in data centers and connected to all the major consumer and commercial

networks, to leading cloud service providers, to private exchanges and to SaaS application providers. Traffic from Netskope customers is routed via the fastest path to the Netskope security cloud and to the cloud application or web site being accessed.

Latency optimizations

NewEdge employs a variety of optimizations to overcome the effects of TCP congestion control and routing inefficiencies, increasing throughput and improving response time.

Auto-failover

Netskope customers can be served by any POP globally and in the event that unexpected issues occur with their default POP, they are automatically routed to another POP in their configured zone.

Cloud-scale

NewEdge benefits from cloud-scale with a virtually unlimited number of cloud-based resources available for compute-intensive, real-time functions such as line rate TLS decryption, deep inspection, DLP, and malware scanning. With NewEdge, there is no need to upgrade or deploy purpose-built security appliances. Deliver real-time security from the cloud at cloud-scale.

ENABLING REAL-TIME, PROACTIVE SECURITY

Not all security impacts user experience. Cloud security use cases that use an out-of-band API deployment method do not impact user experience as they are not deployed between the users and the online resources they are accessing. While the out-of-band deployment method is needed for covering important use cases such as protecting data at rest in cloud services, the security method is reactive, providing visibility and control after a security event has already happened and it is only focused on a small number of cloud services that are managed by IT.

A comprehensive approach to cloud security involves employing both out-of-band and inline, real-time, methods. You need to be deployed inline to provide real-time security that is proactive for all traffic accessed by users, whether that is cloud resources, general web access, or zero-trust access to private apps hosted in the cloud or corporate datacenter.

TOP 10 REAL-TIME CLOUD SECURITY USE CASES ENABLED BY THE NETSKOPE'S SECURITY CLOUD RUNNING ON NEWEDGE

Use Case #1

Real-time inspection of TLS / SSL traffic

Netskope safely decrypts TLS-encrypted traffic for inspection and performs this function from the cloud, using a virtually unlimited amount of cloud-based resources.

Use Case #2

Real-time deep inspection and behavioral analytics (Cloud XD)

Netskope's CloudXD is a patented technology that enables real-time inspection of all cloud traffic in real-time, decoding rich, contextual details about the user, group, location, app, app instance, activity, and content for thousands of cloud services.

Use Case #3

Real-time, granular control of managed SaaS and IaaS

Netskope provides real-time, granular control for cloud services managed by IT. From Office 365 and Box to IaaS environments like AWS and Azure, apply real-time policy enforcement to proactively stop risky activities.

Use Case #4

Real-time, granular control for unmanaged SaaS and IaaS

Netskope also provides real-time, granular control for the thousands of cloud services not managed by IT. From rogue deployments of Slack to the dev team using Github, apply real-time policy enforcement to ensure safe use of these applications adopted by lines of business and users.

Use Case #5

Real-time cloud DLP

Inspect all cloud and web traffic for sensitive data movement and apply real-time policies to ensure sensitive data does not get in the wrong hands.

Use Case #6

Real-time threat protection

Inspect all cloud and web traffic for the presence of threats such as zero-day malware and ransomware downloads or abnormal behavior that may signal the presence of an external, bad actor or a malicious insider.

Use Case #7

Stop data exfiltration to personal devices

Inspect traffic going from cloud apps managed by IT to personal devices and block sensitive data from going to the personal device.

Use Case #8

Stop data exfiltration to unmanaged cloud services

Inspect traffic going from a managed device to cloud services that are not managed by IT and block sensitive data being exfiltrated to these personal cloud apps like Dropbox and Slack.

Use Case #9

URL filtering and acceptable use policies for web

Inspect all web traffic from all devices on corporate networks or from managed devices on any network, even for mobile and remote office users. Apply acceptable use policies based on the needs of your organization.

Use Case #10

Zero-trust secure access to private apps

Provide zero-trust, secure access to private apps hosted in the public cloud and corporate datacenter.

SUMMARY

Delivering proactive, real-time security is a critical requirement for mitigating risk and protecting against data loss and threats. You not only need a security platform that can address your real-time use cases, you need a solution that can cover your use cases while not impacting user performance. The Netskope security cloud running on NewEdge addresses this need.

netskope

Netskope is the leader in cloud security. We help the world's largest organizations take advantage of cloud and web without sacrificing security. Our patented Cloud XD technology targets and controls activities across any cloud service or website and customers get 360-degree data and threat protection that works everywhere. We call this smart cloud security.

To learn more visit, https://www.netskope.com.