illumio | netskope

North, South, East, West—Securing Your Network with Zero Trust

Lawrence Miller

- Protecting north-south user-to-application communications with ZTNA
- Protecting east-west application-to-application communications with ZTS
- Integrating ZTNA and ZTS to achieve full Zero Trust

PRODUCED BY

ActualTech MEDIA

IN THIS PAPER

In this tech brief, we explore how to implement a zero-trust strategy with ZTNA and ZTS successfully.

Highlights include:

- Protecting north-south user-to-application communications with ZTNA
- Protecting east-west application-to-application communications with ZTS
- Integrating ZTNA and ZTS to achieve full Zero Trust

CONTENTS

INTRODUCTION

More than a decade after it was originally created by John Kindervag, the Zero Trust security strategy has become the de facto standard for organizations aspiring to achieve a robust cybersecurity posture in their multi-cloud and hybrid environments.

The U.S. National Institute of Standards and Technology (NIST) prescribes three Zero Trust Architecture (ZTA) key enforcement points in a Zero Trust Architecture: identity, network access, and workload segmentation. Identity is implemented with identity and access management (IAM) controls that include multi-factor authentication (MFA), biometrics, and attribute-based access controls (ABAC), among others.

In this tech brief, we explain how to implement network access and workload segmentation in a ZTA with Zero Trust Network Access (ZTNA) and Zero Trust Segmentation (ZTS).

ZTNA is a market that offers modern remote-access services built on Zero Trust principles where no user or device, whether inside or outside the network, is implicitly trusted by default.

North and South: ZTNA

North-south traffic broadly refers to network communications which flow in and out of a data center, for example, between a remote workstation on the Internet and a web server in a corporate data center. North-south traffic is generally well understood as it is the focus of traditional perimeter-based security, typically with a network firewall and virtual private network (VPN) protecting the "trusted" corporate data center/network/users from the "untrusted" Internet.

In the past, one of the key advantages of perimeter-based security was its simplicity. However, corporate networks and modern threats have evolved and become far more complex. Today, the proliferation of cloud (89% of organizations have embraced a multi-cloud/hybrid strategy), mobile (global mobile network data traffic now exceeds 140 exabytes per month), and the Internet of Things (IoT, the number of IoT devices worldwide is expected to more than double from nearly 16 billion in 2023 to 32.1 billion in 2030), among others, has effectively extended the corporate perimeter in every direction, and nation-state attackers and cybercrime syndicates with practically unlimited resources are launching increasingly sophisticated cyberattacks from every direction.

Securing east-west traffic begins with extending visibility across environments, workloads, and devices.

ZTNA is a market that offers modern remote-access services built on Zero Trust principles where no user or device, whether inside or outside the network, is implicitly trusted by default. ZTNA mandates verification for every access request to ensure security and compliance with company policies. By strictly allowing only authorized communication or access, organizations can effectively limit unwanted north-south traffic, reducing the risk of breaches and enhancing overall security posture. This approach ensures that every access attempt is scrutinized, creating a robust defense against potential threats. ZTNA is commonly delivered as part of a security service edge (SSE) or secure access service edge (SASE) platform and can be enhanced by combining it with software-defined wide-area networking (SD-WAN).

East and West: ZTS

East-west traffic refers to inter- and intra-application communications, for example, a data transfer between two different applications, or communication between different components (such as web, application, and database servers) within the same application. In legacy data centers where a single application ran on a single physical server, east-west traffic was relatively limited and, in any case, was inside the "trusted" network. Today, these various application components may be running on different physical servers, different virtual machines on different physical servers, or different virtual machines on the same physical server, and east-west traffic now accounts for as much as 70% of all network traffic.

Multi-cloud/hybrid environments and cloud-native applications create further challenges. For example, gaining visibility into and enforcing security policies on virtual machines in a traditional data center typically involves "hairpinning" (that is, backhauling) traffic through a Switched Port Analyzer (SPAN) port on a network switch or a security appliance, such as an internal firewall or intrusion detection/prevention system (IDS/IPS). This configuration creates complexity and inefficiency in traditional data centers, and it only gets worse in the cloud where everything is virtual.

Cloud-native applications built on a microservices architecture create further challenges. Cloud-native applications often rely on hundreds or thousands of discrete components that may be deployed on virtual machines or containers, and may span numerous clouds and traditional data centers. Technically this is east-west application traffic, but because it must also travel between clouds and data centers, the distinction between east-west and north-south quickly gets blurred. Additionally, these microservices often dynamically move to different clouds for optimal workload placement and may be ephemeral, persisting for as little as a few microseconds.

Threat actors take advantage of the relatively flat (that is, unsegmented) attack surface in east-west application traffic to move laterally within the target environment, spreading malware, establishing persistence, and exploiting additional targets. Additionally, insider threats now account for more than one-quarter of all breaches which means the "trusted" perimeter can no longer be implicitly trusted.

Integrating Netskope One and Illumio ZTS creates a robust foundation for a Zero Trust Architecture.

Securing east-west traffic begins with extending visibility across environments, workloads, and devices. Next, granular workload protection with micro-segmentation is needed to effectively establish a "micro-perimeter" around individual workloads and enforce consistent security policies that are mapped to (and move with) individual workloads, rather than traditional network constructs (such as IP addresses or subnets).

Better Together: Netskope and Illumio

ZTNA and workload segmentations are often implemented with different products, effectively creating two distinct cybersecurity silos: north-south and east-west. This creates many new challenges. For example, how are dynamic changes in workloads made visible to ZTNA? If a workload is moved from development to production, how does ZTNA know this information and make dynamic adjustments to its remote access policy? Thus, these two cybersecurity silos need to be integrated and automated.

The integration of Netskope and Illumio offers a robust security solution by merging ZTNA and workload segmentation (see **FIGURE 1**), ensuring that only authenticated users gain network access and restricting them to specific, authorized workloads. By enforcing strict east-west traffic controls, the integration minimizes the risk of unauthorized lateral movement within the network, enhancing overall security and maintaining a Zero Trust posture.

Netskope ZTNA Next, a key component of the Netskope One Zero Trust Engine, defines workload members based on label-IP mappings received from Illumio Zero Trust Segmentation (ZTS). Illumio ZTS manages all workloads using labels to provide app-centric visibility across multi-cloud/hybrid environments. This enables micro-segmentation of every single workload, defining every workload as a dedicated trust boundary and enforcing least-privilege access between all workloads. When integrated with Netskope One, Illumio ZTS identifies a workload compromised by malware, re-labels it as quarantined, and notifies Netskope One of this change. This allows Netskope One to remove the quarantined workload from its remote access permissions.

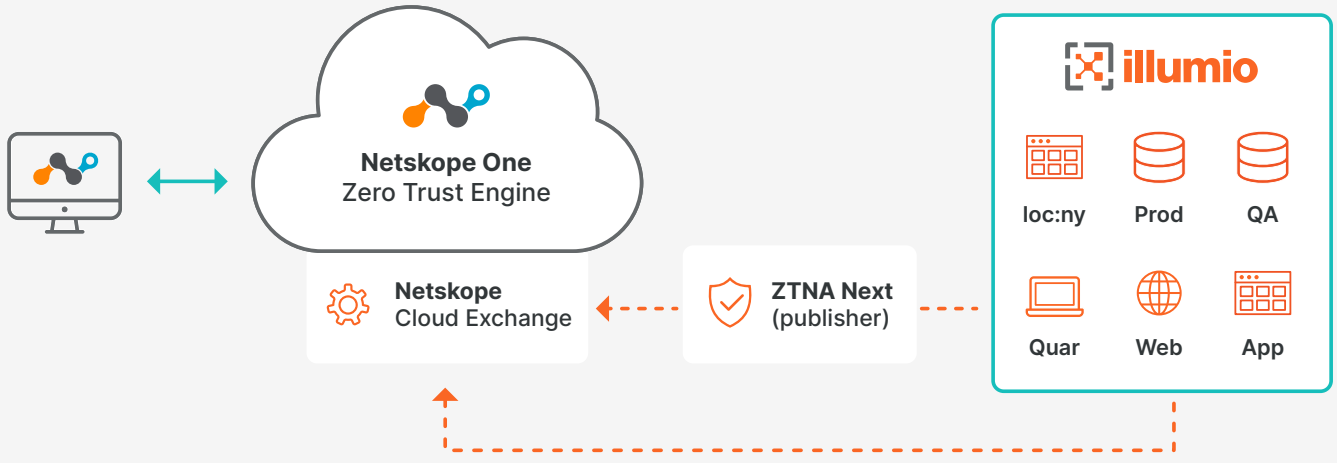

FIGURE 1: Netskope + Illumio integration protects your network in every direction with Zero Trust

Key benefits of the Netskope and Illumio integration include:

1

Enhanced security.
Combining Netskope ZTNA Next with Illumio ZTS creates policies based on least-privilege models for user-to-application and application-to-application connections. This integration effectively mitigates risks by ensuring that only authorized users access specific resources, safeguarding sensitive information and enhancing overall network security.

2

Simplified management.
The integration simplifies managing security policies across the network, enhancing enforcement and compliance monitoring. Illumio's dynamic label updates allow Netskope to map policies to labels instead of IP addresses or subnets, making it effortless to automatically update security measures.

3

Seamless scalability.
The integration is designed to scale seamlessly with growing environments, enabling updates to user access as an environment expands. This process minimizes the need for manual intervention in defining access policies, ensuring efficient and adaptable security management.

Integrating Netskope One and Illumio ZTS creates a robust foundation for a Zero Trust Architecture. This synergy enhances security, scalability, and manageability while effectively preventing lateral movement by unverified and unauthorized entities within the network.

LEARN MORE

Speak to Illumio + Netskope to learn more and get a demo about how to build a ZTA using best-of-breed solutions for ZTNA and ZTS.

illumio | netskope