illumio | netskope

Norden, Süden, Osten, Westen – Sichern Sie Ihr Netzwerk mit Zero Trust

Lawrence Miller

- Schutz der Nord-Süd-Kommunikation zwischen Anwendern und Anwendungen mit ZTNA
- Schutz der Ost-West-Kommunikation zwischen Anwendungen mit ZTS
- Durch die Integration von ZTNA und ZTS ein vollständiges Zero Trust erreichen

ERSTELLT VON

ActualTech MEDIA

INHALT

In diesem Tech-Brief untersuchen wir, wie eine Zero-Trust-Strategie mit ZTNA und ZTS erfolgreich umgesetzt werden kann.

Zu den Highlights gehören:

- Schutz der Nord-Süd-Kommunikation zwischen Anwendern und Anwendungen mit ZTNA
- Schutz der Ost-West-Kommunikation zwischen Anwendungen mit ZTS
- Durch die Integration von ZTNA und ZTS ein vollständiges Zero Trust erreichen

INHALT

EINFÜHRUNG

Mehr als ein Jahrzehnt nach ihrer ursprünglichen Entwicklung durch John Kindervag ist die Zero-Trust-Sicherheitsstrategie zum De-facto-Standard für Unternehmen geworden, die eine robuste Cybersicherheit in ihren Multicloud- und Hybridumgebungen erreichen wollen.

Das US-amerikanische National Institute of Standards and Technology (NIST) gibt drei zentrale Bereiche vor, die in einer Zero-Trust-Architektur zu berücksichtigen sind: Identität, Netzwerkzugang und Workload-Segmentierung. Der Schutz der Identität wird durch Identitäts- und Zugriffsmanagement-Kontrollen (IAM) gewährleistet, die unter anderem Multifaktor-Authentifizierung (MFA), Biometrie und attributbasierte Zugriffskontrollen (ABAC) umfassen.

In diesem Tech-Brief erklären wir, wie man Netzwerkzugriff und Workload-Segmentierung in einem ZTA mit Zero Trust Network Access (ZTNA) und Zero Trust Segmentation (ZTS) implementiert.

ZTNA ist ein Markt, der moderne Fernzugriffsdienste anbietet, die auf Zero-Trust-Prinzipien basieren, bei denen keinem Benutzer oder Gerät, ob innerhalb oder außerhalb des Netzwerks, standardmäßig implizit vertraut wird.

Nord und Süd: ZTNA

Nord-Süd-Verkehr bezieht sich im Allgemeinen auf Netzwerkkommunikation, die in ein Rechenzentrum hinein- und aus diesem herausfließt, z. B. zwischen einer Remote-Workstation im Internet und einem Webserver in einem Unternehmensrechenzentrum. Der Nord-Süd-Verkehr gilt allgemein als gut verstanden, da er im Mittelpunkt der traditionellen perimeterbasierten Sicherheit steht, bei der in der Regel eine Netzwerk-Firewall und ein virtuelles privates Netzwerk (VPN) das „vertrauenswürdige" Unternehmensrechenzentrum/Netzwerk/ die „vertrauenswürdigen" Unternehmensbenutzer vor dem „nicht vertrauenswürdigen" Internet schützen.

In der Vergangenheit war einer der Hauptvorteile der perimeterbasierten Sicherheit ihre Einfachheit. Unternehmensnetzwerke und moderne Bedrohungen haben sich jedoch weiterentwickelt und sind weitaus komplexer geworden. Heute hat die Verbreitung von Clouds (89 % der Unternehmen haben eine Multi-Cloud-/Hybrid-Strategie eingeführt), Mobilgeräten (der weltweite Datenverkehr im Mobilfunknetz übersteigt jetzt 140 Exabyte pro Monat) und dem Internet der Dinge (IoT, die Zahl der IoT-Geräte weltweit wird sich voraussichtlich von fast 16 Milliarden im Jahr 2023 auf 32,1 Milliarden im Jahr 2030 mehr als verdoppeln), unter anderem den Unternehmensperimeter in alle Richtungen effektiv erweitert. Staatsfeindliche Angreifer und Cyberkriminelle mit praktisch unbegrenzten Ressourcen starten immer ausgefeiltere Cyberangriffe aus allen Richtungen.

Die Sicherung des Ost-West-Verkehrs beginnt mit der Erweiterung der Sichtbarkeit aller Umgebungen, Workloads und Geräte.

ZTNA ist ein Markt, der moderne Fernzugriffsdienste anbietet, die auf Zero-Trust-Prinzipien basieren, bei denen keinem Benutzer oder Gerät, ob innerhalb oder außerhalb des Netzwerks, standardmäßig implizit vertraut wird. ZTNA schreibt die Überprüfung jeder Zugriffsanfrage vor, um die Sicherheit und die Einhaltung der Unternehmensrichtlinien zu gewährleisten. Unternehmen können unerwünschten Nord-Süd-Verkehr effektiv einschränken, indem sie ausschließlich autorisierte Kommunikation oder Zugriffe zulassen. Dadurch wird das Risiko von Sicherheitsverletzungen verringert und die allgemeine Sicherheitslage verbessert. Auf diese Weise wird sichergestellt, dass jeder Zugriffsversuch genau geprüft wird und ein solider Schutz vor potenziellen Bedrohungen entsteht. ZTNA wird in der Regel als Teil einer Security Service Edge (SSE)- oder Secure Access Service Edge (SASE)-Plattform bereitgestellt und kann durch die Kombination mit einem Software-Defined Wide Area Network (SD-WAN) erweitert werden.

Ost und West: ZTS

Der Ost-West-Verkehr bezieht sich auf die Kommunikation zwischen und innerhalb von Anwendungen, z. B. eine Datenübertragung zwischen zwei verschiedenen Anwendungen oder die Kommunikation zwischen verschiedenen Komponenten (z. B. Web-, Anwendungs- und Datenbankservern) innerhalb derselben Anwendung. In älteren Rechenzentren, in denen eine einzelne Anwendung auf einem einzelnen physischen Server ausgeführt wurde, war der Ost-West-Verkehr relativ begrenzt und befand sich in jedem Fall innerhalb des „vertrauenswürdigen" Netzwerks. Heutzutage können diese verschiedenen Anwendungskomponenten auf unterschiedlichen physischen Servern, unterschiedlichen virtuellen Maschinen auf unterschiedlichen physischen Servern oder unterschiedlichen virtuellen Maschinen auf demselben physischen Server ausgeführt werden, und der Ost-West-Verkehr macht inzwischen bis zu 70 % des gesamten Netzwerkverkehrs aus.

Multicloud-/Hybrid-Umgebungen und cloudnative Anwendungen stellen eine weitere Herausforderung dar. Um beispielsweise Einblick in virtuelle Maschinen in einem herkömmlichen Rechenzentrum zu erhalten und Sicherheitsrichtlinien auf diesen durchzusetzen, muss der Datenverkehr in der Regel über einen Switched Port Analyzer (SPAN)-Port auf einem Netzwerk-Switch oder einer Sicherheitsanwendung, wie einer internen Firewall oder einem Eindringlingserkennungs-/Verhinderungssystem (IDS/IPS), geleitet werden. Diese Konfiguration sorgt in traditionellen Rechenzentren für Komplexität und Ineffizienz und wird in der Cloud, in der alles virtuell ist, nur noch schlimmer.

Weitere Herausforderungen stellen Cloud-native Anwendungen dar, die auf einer Microservices-Architektur basieren. Cloud-native Anwendungen basieren oft auf Hunderten oder Tausenden von Einzelkomponenten, die auf virtuellen Maschinen oder Containern bereitgestellt werden können und sich über zahlreiche Clouds und herkömmliche Rechenzentren erstrecken können. Technisch gesehen handelt es sich hierbei um Ost-West-Anwendungsdatenverkehr, aber da dieser auch zwischen Clouds und Rechenzentren übertragen werden muss, verschwimmt die Unterscheidung zwischen Ost-West- und Nord-Süd-Datenverkehr schnell. Darüber hinaus werden diese Mikrodienste häufig dynamisch in verschiedene Clouds verschoben, um eine optimale Platzierung der Arbeitslast zu erreichen, und können kurzlebig sein und nur wenige Mikrosekunden bestehen bleiben.

Bedrohungsakteure nutzen die relativ flache (d. h. nicht segmentierte) Angriffsfläche im Ost-West-Anwendungsverkehr, um sich lateral innerhalb der Zielumgebung zu bewegen, Malware zu verbreiten, Persistenz zu etablieren und zusätzliche Ziele auszunutzen. Dazu kommt, dass Insider-Bedrohungen mittlerweile für mehr als ein Viertel aller Sicherheitsverletzungen verantwortlich sind. Das bedeutet, dass dem „vertrauenswürdigen" Perimeter nicht mehr implizit vertraut werden kann.

Die Integration von Netskope One und Illumio ZTS schafft eine solide Grundlage für eine Zero-Trust-Architektur.

Die Sicherung des Ost-West-Verkehrs beginnt mit der Erweiterung der Sichtbarkeit aller Umgebungen, Workloads und Geräte. Als Nächstes ist ein granularer Workload-Schutz mit Mikrosegmentierung erforderlich. So können Sie einen „Mikroperimeter" um einzelne Workloads herum einrichten und konsistente Sicherheitsrichtlinien durchsetzen, die einzelnen Workloads zugeordnet sind (und sich mit diesen bewegen), anstatt herkömmliche Netzwerkkonstrukte (wie IP-Adressen oder Subnetze) zu verwenden.

Gemeinsam stärker: Netskope und Illumio

ZTNA- und Workload-Segmentierungen werden oft mit unterschiedlichen Produkten implementiert, wodurch effektiv zwei verschiedene Cybersicherheitssilos entstehen: Nord-Süd und Ost-West. Dies bringt viele neue Herausforderungen mit sich. Wie werden beispielsweise dynamische Änderungen in Workloads für ZTNA sichtbar gemacht? Wenn ein Workload von der Entwicklung in die Produktion verlagert wird, woher weiß ZTNA davon und wie nimmt es dynamische Anpassungen an seiner Richtlinie für den Fernzugriff vor? Daher müssen diese beiden Cybersicherheitssilos integriert und automatisiert werden.

Aus der Kombination von Netskope und Illumio ergibt sich eine robuste Sicherheitslösung, die ZTNA und Workload-Segmentierung (siehe **ABBILDUNG 1**) zusammenführt und sicherstellt, dass nur authentifizierte Benutzer Netzwerkzugriff erhalten und auf bestimmte, autorisierte Workloads beschränkt sind. Strenge Ost-West-Verkehrskontrollen minimieren das Risiko unbefugter lateraler Bewegungen innerhalb des Netzwerks, erhöhen die Gesamtsicherheit und sorgen für eine Zero-Trust-Haltung.

Netskope ZTNA Next, eine Schlüsselkomponente der Netskope One Zero Trust Engine, definiert Workload-Mitglieder auf der Grundlage von Label-IP-Zuordnungen, die von Illumio Zero Trust Segmentation (ZTS) empfangen werden. Illumio ZTS verwaltet alle Workloads mithilfe von Labels, um eine anwendungsorientierte Transparenz in Multicloud-/Hybridumgebungen zu gewährleisten. Dies ermöglicht eine Mikrosegmentierung jeder einzelnen Arbeitslast, wobei jede Arbeitslast als dedizierte Vertrauensgrenze definiert wird und der Least-Privilege-Zugriff zwischen allen Arbeitslasten erzwungen wird. Bei der Integration in Netskope One identifiziert Illumio ZTS eine durch Malware gefährdete Arbeitslast, kennzeichnet sie als unter Quarantäne gestellt und benachrichtigt Netskope One über diese Änderung. Dadurch kann Netskope One die unter Quarantäne gestellte Arbeitslast aus seinen Fernzugriffsberechtigungen entfernen.

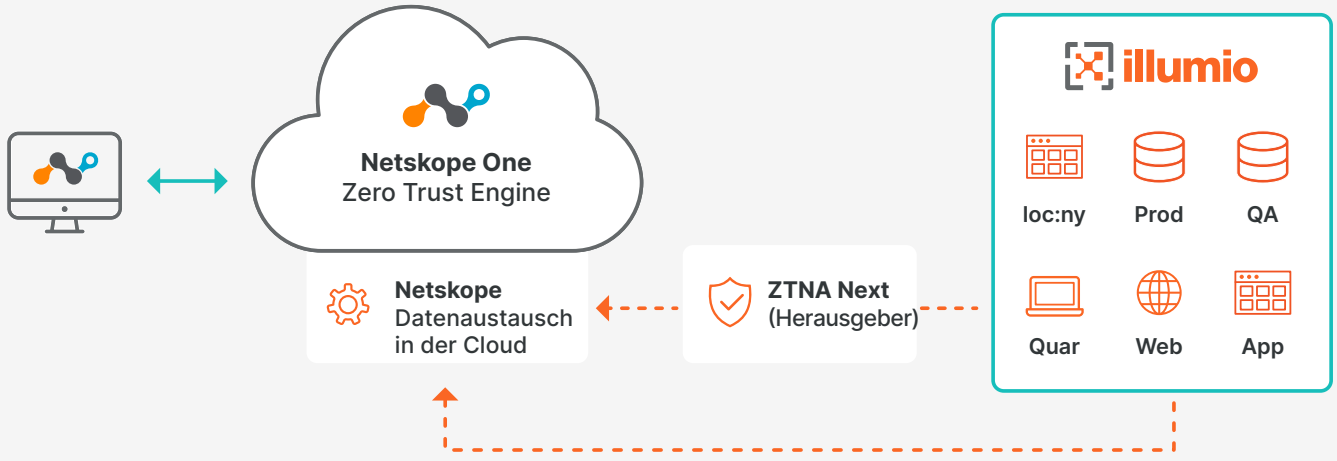

ABBILDUNG 1: Die Integration von Netskope und Illumio schützt Ihr Netzwerk in alle Richtungen mit Zero Trust.

Zu den wichtigsten Vorteilen der Integration von Netskope und Illumio gehören:

1

Verbesserte Sicherheit.
Durch die Kombination von Netskope ZTNA Next mit Illumio ZTS werden Richtlinien auf der Grundlage von Least-Privilege-Modellen für Verbindungen zwischen Benutzern und Anwendungen sowie zwischen Anwendungen erstellt. Diese Integration mindert Risiken effektiv, indem sie sicherstellt, dass nur autorisierte Benutzer auf bestimmte Ressourcen zugreifen, sensible Informationen geschützt werden und die allgemeine Netzwerksicherheit verbessert wird.

2

Einheitliche Verwaltung.
Die Integration vereinfacht die Verwaltung von Sicherheitsrichtlinien im gesamten Netzwerk und verbessert die Durchsetzung und Überwachung der Einhaltung von Vorschriften. Mithilfe der dynamischen Label-Updates von Illumio kann Netskope die Richtlinien Labeln statt IP-Adressen oder Subnetzen zuordnen, sodass Sicherheitsmaßnahmen problemlos automatisch aktualisiert werden können.

3

Nahtlose Skalierbarkeit.
Die Integration ist so konzipiert, dass sie sich nahtlos an wachsende Umgebungen anpasst und Aktualisierungen des Benutzerzugriffs ermöglicht, wenn eine Umgebung erweitert wird. Dadurch wird der Bedarf an manuellen Eingriffen bei der Definition von Zugriffsrichtlinien minimiert und ein effizientes und anpassungsfähiges Sicherheitsmanagement gewährleistet.

Die Integration von Netskope One und Illumio ZTS schafft eine solide Grundlage für eine Zero-Trust-Architektur. Diese Synergie verbessert die Sicherheit, Skalierbarkeit und Verwaltbarkeit und verhindert gleichzeitig effektiv die laterale Ausbreitung durch nicht verifizierte und nicht autorisierte Entitäten innerhalb des Netzwerks.

MEHR ZUM THEMA

Wenden Sie sich an Illumio + Netskope, um weitere Informationen und eine Demoversion zum Aufbau einer ZTA mit erstklassigen Lösungen für ZTNA und ZTS zu erhalten.

illumio | netskope