Symantec by Broadcom | Carbon Black. by Broadcom | ARROW

GUIDE

Symantec ZTNA Einrichtungsleitfaden

Umfang

Dieser Leitfaden behandelt die Einführung von ZTNA aus der Perspektive von Praktikern und soll bewährte Verfahren für die Planung, Einführung und Skalierung der ZTNA-Nutzung innerhalb eines Unternehmens veranschaulichen. Jedes Unternehmen ist anders und je nach Endbenutzerprofilen, Anwendungsbeständen und IT-Infrastruktur wird jedes Unternehmen einen eigenen Weg einschlagen. Eine wichtige Funktion dieses Leitfadens besteht darin, die internen Gruppen und Teams zu benennen, die für eine erfolgreiche ZTNA-Implementierung einbezogen werden müssen.

Dieser Leitfaden sollte in Verbindung mit Broadcom TechDocs verwendet werden, um sicherzustellen, dass die technischen Implementierungsschritte stets mit den aktuellen Funktionen und den neuesten Konfigurationen übereinstimmen.

Technische Dokumentation von Broadcom: Symantec Zero Trust Network Access

Vorbereitende Planung

Bei der Planung einer ZTNA-Bereitstellung gibt es viele Dinge zu beachten und zahlreiche Stakeholder zu berücksichtigen. Im Folgenden sind die wichtigsten Punkte aufgeführt, die, wenn sie nicht vor der technischen Umsetzung beachtet werden, zu erheblichen Verzögerungen im Projekt führen können. Allgemeine Planungsschritte finden Sie in diesem TechDoc.

ZTNA Mandantenbenennung und -Standort

ZTNA-Mandant erfordert die Definition von zwei Parametern vor der Mandantenerstellung im CMP (Customer Management Portal)

1. Die Lokalisierung des Management-PoD (EU/USA) ist eine wichtige Einstellung, welche die Region sowohl für das Datenpfad-Routing als auch für die Protokollierung bestimmt. Diese Auswahl ist entscheidend, da Connectivity PoDs, die für die Richtlinienverarbeitung zuständig sind, geografisch mit ihren jeweiligen Management PoDs verknüpft sind. Management PoDs. Management & Connectivity PoDs assignment
2. Der Name des Mandanten erstellt eine eindeutige benutzerdefinierte Domäne sowohl für das Benutzerportal als auch für den agentenlosen Anwendungszugriff. Es ist wichtig, den Mandantennamen sorgfältig auszuwählen, damit er Ihr Unternehmen und Ihre Umgebung genau widerspiegelt, da er nach der Einrichtung nicht mehr geändert werden kann.

Die vollständige Mandanten-URL setzt sich aus dem gewählten „Mandantennamen“ und der Endung „luminatesec.com“ zusammen.

Identitätsanbieter

Die Integration eines Identitätsanbieters (Identity Provider, IdP) ist für Symantec ZTNA von entscheidender Bedeutung und bildet die Grundlage für den Ablauf der Authentifizierung. Während lokale Benutzer für Proof of Concepts (PoCs) ausreichend sind, ist die Einbeziehung des IdP-Managementteams des Unternehmens als Stakeholder für eine erfolgreiche Produktionsbereitstellung von entscheidender Bedeutung. Häufig sind es Personen, die ZTNA einsetzen, die auch für Zero Trust, SSE, Proxy-Architektur oder VPN-Engineering-Initiativen verantwortlich sind. Die Zusammenarbeit mit dem IdP-Team ist unerlässlich, um zu verstehen, wie Benutzer und Gruppen den von ZTNA bereitgestellten Anwendungen zugeordnet werden, was wiederum dabei hilft, die erforderliche Richtlinienstruktur zu definieren.

Technisch gesehen müssen zwei wichtige Aspekte berücksichtigt werden: die Integration in die SSO-Plattform(en) des Unternehmens, die in der Regel mit SAML (und manchmal auch OIDC) bereitgestellt werden, und die Gruppenauflösung, die durch Parsen von SAML-Attributen oder mithilfe des SCIM-Protokolls erfolgen kann.

„Generische SAML“ ist die empfohlene Option für die IdP-Integration. Diese Option unterstützt sowohl die SAML-Integration als auch die Gruppenauflösung über SCIM- und SAML-Attributoptionen.

- TechDoc: Integrate IdP

Wenn SCIM vom IDP des Kunden nicht unterstützt wird, sollte die Option „SAML-Attribut” für die Gruppenauflösung verwendet werden. Dadurch kann der Kunde die Gruppenauflösung direkt aus der SAML-Antwort analysieren.

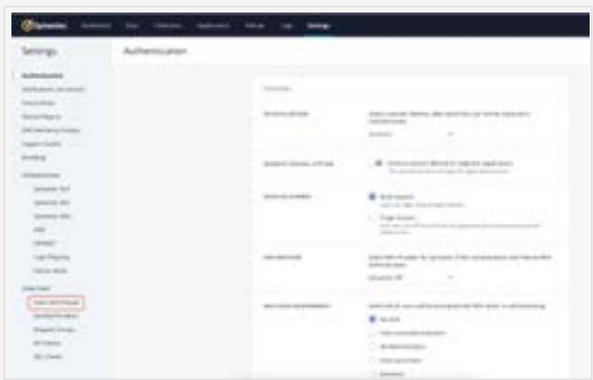
Symantec ZTNA-Einrichtungsleitfaden

Vorbereitende Planung

Identitätsanbieter

Ausschließlich Zugriff ohne Agent

Lokale Benutzer“ können für agentenlose Anwendungen (Web-, RDP-, SSH- und TCP-Anwendungen) innerhalb des ZTNA Entity Store verwendet werden. Dies ist für die Servicebewertung, Proof-of-Concept (PoC) oder den eingeschränkten Zugriff durch Dritte geeignet.



Nur agentenbasierter Zugriff

Für den agentenbasierten Zugriff unter Verwendung von WSSA-, SES- und ESA-Agenten mit Segmentanwendungen ist eine SAML-Integration erforderlich. Das bedeutet, dass lokale Benutzer nicht unterstützt werden. Darüber hinaus muss der Identitätsanbieter (Identity Provider, IDP) in Symantec Cloud SWG integriert sein, was letztendlich eine SAML-Authentifizierung für Cloud SWG innerhalb des Unternehmens erforderlich macht. TechDoc: Cloud SWG SAML Authentication

Anwendungsinventar und ZTNA-Zugangsmethode

Die Migration zu ZTNA ist eine Top-Down-Maßnahme, die Bottom-up-Informationen erfordert. In der Regel müssen VPNs und andere Fernzugriffsprotokolle nicht wissen, auf welche Anwendung ein Benutzer zugreifen möchte, da dies derzeit von den Anwendungseigentümern verwaltet wird.

Die wesentliche Überlegung, die zunächst angestellt werden muss, ist, ob das Unternehmen mit agentenbasiertem ZTNA oder agentenlosem ZTNA beginnen möchte. Obwohl beide in den meisten ZTNA-Implementierungen nebeneinander existieren, ist es aus Sicht der Pilotierung ideal, zunächst mit einem zu beginnen.

Ausschließlich Zugriff ohne Agent

Die agentenbasierte Zugriffsmethode bietet drei Hauptvorteile:

- **Nahtlose Benutzererfahrung:** Endbenutzer sind davon nicht betroffen, da keine Änderungen an der Domäne oder am Netzwerk erforderlich sind.
- **Nutzt bestehende Infrastruktur:** Die Methode beruht auf dem privaten DNS des Unternehmens, sodass keine Änderungen am Workflow erforderlich sind.
- **Schnelle Einarbeitung:** Ganze Netzwerkcluster können schnell innerhalb einer einzigen Anwendung und Richtlinie gesichert werden. Granulare Regeln für geringstmögliche Berechtigungen können dann zu einem späteren Zeitpunkt angewendet werden, wodurch zeitliche Einschränkungen vermieden werden.

Für bestehende Symantec-Kunden, die bereits WSSA-, SEC- oder ESA-Agenten im Rahmen ihrer SWG-, CASB- oder EPP-Bereitstellungen einsetzen, ist ZTNA oft einfacher zu implementieren. Der Grund dafür ist, dass ZTNA-Richtlinienadministratoren zunächst allgemeine Bereiche des Unternehmensnetzwerks definieren können, in denen sich Anwendungen befinden, ohne die spezifischen Anwendungen kennen zu müssen, auf die zugegriffen wird. Im Laufe der Zeit können diese Administratoren die Richtlinien zielgerichteter gestalten, sodass nur noch Zugriff auf die Domänen oder IP-Adressen gewährt wird, die die Benutzer tatsächlich benötigen.

Umgekehrt kann die agentenbasierte Methode für Kunden, die Symantec noch nicht kennen, die anfängliche Bereitstellung innerhalb der Anforderungen für die Agentenbereitstellung erschweren. Für ihre ersten Schritte bevorzugen sie häufig die agentenlose Methode.

Symantec ZTNA-Einrichtungsleitfaden

Vorbereitende Planung

Ausschließlich Zugriff ohne Agent

Agentenloser Zugriff:

Der agentenlose ZTNA bietet einen sichereren Ansatz, da von Anfang an explizite Definitionen für die geringsten Berechtigungen für Ressourcen erforderlich sind. Bei dieser Methode müssen alle Anwendungen auf der Symantec ZTNA-Konsole konfiguriert und Zugriffsrichtlinien für Benutzer und Gruppen festgelegt werden. Obwohl dies den Workflow der Benutzer verändert – da für den Zugriff auf Anwendungen die Nutzung eines globalen DNS erforderlich ist (entweder durch Veröffentlichung der Anwendungs-URL im öffentlichen DNS über eine CNAME-Aktualisierung oder durch Änderung derselben) – bevorzugen Benutzer in der Regel den agentenlosen Zugriff gegenüber VPN, sobald sie sich daran gewöhnt haben.

Abgesehen von Webanwendungen erweist sich die agentenlose Methode auch für SSH- und RDP-Zugriffe, einschließlich nativer SSH- und RDP-Clients, als vorteilhaft, ohne DevOps-Workflows zu stören.

Zielgruppe (Agent Traffic Manager)

Bei der Implementierung der agentenbasierten Zugriffsmethode ist es entscheidend, die Zielgruppe sorgfältig auszuwählen, um weitreichende Störungen im Unternehmen durch mögliche Fehlkonfigurationen zu vermeiden. Beschränken Sie zunächst die Zielgruppe für die ZTNA-Einführung mithilfe des Agent Traffic Manager auf eine begrenzte Anzahl von Benutzern oder Gruppen.

Gerätekonformität

Die Gerätekonformität kann mit Symantec ZTNA über den Symantec Endpoint Protection-Agenten durchgesetzt werden. Dazu muss das Unternehmen über eine Berechtigung für Symantec Enterprise Security verfügen. Diese Funktion wird über Host-Integritätsprüfungen bereitgestellt Host Integrity Checks - TechDoc.

Während des Planungsprozesses für ZTNA ist es von entscheidender Bedeutung, zu definieren, „was“ das Unternehmen auf den Endgeräten der Benutzer validieren möchte. Gerätezertifikate? Betriebssystem-Patch?

Ebene? Laufende Prozesse? Die Zusammenarbeit mit dem Endpunktmanagement-Team des Unternehmens kann dabei helfen, diese Fragen zu beantworten und sicherzustellen, dass die Konfiguration des Compliance-Profils zügig erfolgen kann.

Verwaltungsmanagement

Je nachdem, wie das Unternehmen Geschäftsanwendungen verwaltet und bereitstellt, kann es erforderlich sein, dass mehrere Teams die ZTNA-Verwaltungskonsole nutzen. In diesem Fall ermöglicht die frühzeitige Festlegung der Rollen und Verantwortlichkeiten jedes Einzelnen die Erstellung von RBAC-Richtlinien, die es jedem ermöglichen, innerhalb seines Bereichs zu arbeiten, ohne einer anderen Gruppe in die Quere zu kommen.

Überlegen Sie sich im Voraus, welche verschiedenen Gruppen für die Bereitstellung von ZTNA erforderlich sind, damit RBAC schnell definiert werden kann. Drei wichtige Rollen sind dabei zu berücksichtigen:

- **ZTNA Platform Administrator** - Der globale Administrator, der für die Integration von IdP(s), die Verwaltung von Protokollen, die Zuweisung von Richtlinienadministratoren, die Erstellung von Bereitstellungsstandorten und die Gewährung des API-Zugriffs verantwortlich ist.
- **Site Administrator** - Sind mit der Verwaltung der ZTNA-Konnektoren und deren Bereitstellung an ihren jeweiligen Standorten betraut.
- **Application (Collection) Administrators** - Sind für das Laden von Anwendungen in ZTNA und die Festlegung der Richtlinien, wer darauf zugreifen darf, verantwortlich.
- **Access Policy (Collection) Administrator** - Ist auf die Verwaltung von Anwendungszugriffsrichtlinien beschränkt.

Weitere Informationen über die RBAC-Verwaltung finden Sie auf den TechDocs.

Symantec ZTNA-Einrichtungsleitfaden

Erste Bereitstellung

Integration von Identitätsanbietern

Wie oben erläutert, sollte eine Arbeitssitzung mit dem IdP-Engineering-Team geplant werden, um SSO und die Gruppenauflösung innerhalb von ZTNA zu konfigurieren. Für agentenbasierten ZTNA sollte die Cloud-SWG des Unternehmens bereits einen Plan für die Integration mit demselben IdP haben – das bedeutet, das SAML Captive Portal zu nutzen. Im Abschnitt „Automatisierung“ unten finden Sie eine Anleitung zur Verwendung der SAML-Authentifizierung für den Symantec-Agenten.

Administrator-Zugriff

Wenn während der Planung Rollen definiert wurden, müssen nach der Integration des IdP zunächst zusätzliche Administratoren hinzugefügt werden. Es empfiehlt sich, innerhalb des IdP eine Gruppe zu definieren und diese als globale ZTNA-Administratoren zuzuordnen. Darüber hinaus kann es sehr hilfreich sein,

„Sammlungen“ mit Administratoren zu definieren, die für die Einbindung von Anwendungen und die Erstellung von Zugriffsrichtlinien verantwortlich sind.

Die Spiegelung interner Ansätze für Anwendungsebenen oder Dienstgruppen kann dabei helfen, die ZTNA-Architektur an die internen Prozesse des Unternehmens anzupassen. Die IdP-Gruppe kann hier eine große Hilfe sein, da sie diese Arbeitsgruppen oft bereits definiert hat.

- TechDoc: ZTNA Collections

Bereitstellung von Konnektoren

Der Konnektor, in Symantec ZTNA oft als „Sites“ bezeichnet, ist die Schnittstelle, über die der Cloud-ZTNA-Dienst eine Verbindung zu vom Kunden verwalteten Anwendungen in Rechenzentren oder bei Cloud-IaaS-Anbietern herstellt.

Die Konnektoren sollten so nah wie möglich an den Anwendungen eingesetzt werden. Im Rahmen der Anwendungsinventarisierung sollte die Position jeder Anwendungsgruppe protokolliert werden. Außerdem wird empfohlen, mindestens zwei Konnektoren in diesen Netzwerksegmenten einzusetzen.

Die Konnektoren sind in den Formaten Docker, Docker Compose, Kubernetes und VM ESXi verfügbar.

Cloud Orchestrator

Für einen nahtlosen Lebenszyklus von Konnektoren innerhalb von Cloud-Orchestratoren wie K8S und OpenShift, Fargate (und anderen) wird die Verwendung des Authentifizierungsmodus „Site“ empfohlen. Dadurch entfällt die Notwendigkeit einer Vorabregistrierung mit einem einmaligen Passwort (OTP) für jeden Konnektor.

- Konnektoren: TechDoc

Geschäftskontinuität und Notfallwiederherstellung

Wenn Sie Konnektoren für eine Website bereitstellen, müssen Sie die Region angeben, mit der die Konnektoren verbunden werden sollen – dies bezieht sich auf die GCP-Region. Im Falle eines Ausfalls von GCP oder eines Netzwerkausfalls im Unternehmen kann ein Backup-Standort in einer anderen Region als Wiederherstellungsschritt dienen.

Zu diesem Zweck sollte ein neuer Standort eingerichtet werden, der einer anderen Region zugeordnet ist. Diese Konnektoren sollten in einem anderen Teil des Netzwerks des Unternehmens bereitgestellt werden, der nach wie vor Zugriff auf die Anwendungen am primären Standort hat. Im Falle eines Ausfalls können Anwendungen innerhalb von ZTNA von einem Standort zu einem anderen verschoben werden.

Dieser Prozess kann mithilfe eines Skripts automatisiert werden, indem die

- API: Bind Application to Site

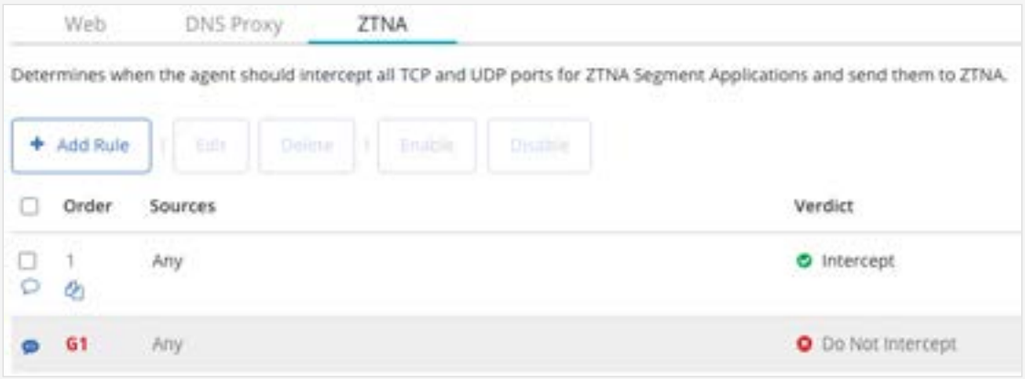
Symantec ZTNA-Einrichtungsleitfaden

Erste Bereitstellung

Agent Traffic Manager

Stellen Sie sicher, dass die Einheiten, auf die ZTNA angewendet werden soll, definiert sind. Standardmäßig sind ZTNA keine Einheiten zugewiesen, sofern dies nicht ausdrücklich konfiguriert wurde.

Um mögliche Auswirkungen zu vermeiden, weisen Sie Einheiten für ZTNA in ATM zu, bevor Sie die Segmentanwendung erstellen.



Anwendungskatalog

Wie oben erläutert, ist es von entscheidender Bedeutung, den Anwendungsbestand zu kennen, den ZTNA unterstützen wird – sowohl agentenlos als auch agentenbasiert. Nach der Bereitstellung des Konnektors müssen Administratoren Anwendungen entweder einzeln oder als Subnetze definieren, wenn sie den Symantec Agent verwenden.

Die Zuordnung jeder Anwendung zu einer geeigneten Sammlung kann später die Erstellung von Zugriffsrichtlinien vereinfachen.

Um sicherzustellen, dass vor der Einführung von ZTNA kein unerwünschter Zugriff erfolgt, gibt es für jede Anwendung einen „Aktivieren“-Schalter.

Konfiguration der Richtlinien

Der Zugriff auf Anwendungen wird Benutzern nur gewährt, wenn eine Richtlinie vorhanden ist, die die relevanten Einheiten und die Zielanwendung definiert. Gemäß dem Prinzip der „“Least Privilege“ sind Anwendungen standardmäßig nicht zugänglich. Um den Zugriff auf die Anwendung zu gestatten, muss für diese Anwendung eine bestimmte Richtlinie vorhanden sein.

Es ist zu beachten, dass mehrere Richtlinien verschiedenen Einheiten Zugriff auf unterschiedliche Anwendungen gewähren können. In solchen Fällen bestimmt die Regel „Konfliktlösung“ (definiert in „Access Policy Evaluation“), welche Richtlinie angewendet wird.

Symantec ZTNA-Einrichtungsleitfaden

Erste Bereitstellung

Einbindung der Endnutzer

Die Einführung des Zugangs für Endbenutzer nach einem Proof-of-Concept ist eine der größten Herausforderungen für ZTNA, da Sicherheitsexperten oftmals die Aufgabe haben, die Benutzererfahrung so wenig wie möglich zu beeinträchtigen. In den folgenden Abschnitten werden bewährte Vorgehensweisen beschrieben, um Endbenutzer für ZTNA zu gewinnen.

Langsame Einführung von ZTNA (SAML):

Die Verwendung des Symantec Agent for Zero Trust Network Access ist die beste Möglichkeit, um sicherzustellen, dass Endbenutzer Zugriff auf alle Anwendungen haben, auf die sie normalerweise über VPN zugreifen würden, da er interne DNS verwendet und auf Layer 3 arbeitet, sodass auch ältere Anwendungen unterstützt werden können.

Die Aktivierung des SAML Captive Portals für Cloud SWG kann eines der größten Hindernisse für ZTNA darstellen, da viele Unternehmen zögern, die Endbenutzererfahrung zu stören. Letztendlich ist es entscheidend, Zero Trust sowohl aus architektonischer Sicht wirklich umzusetzen als auch Zero Trust Network Access zu implementieren.

Das Cloud SWG SAML Captive Portal kann nun schrittweise für bestimmte Gruppen eingeführt werden, sodass Unternehmen es mit ausgewählten Benutzern testen können. Dadurch wird das Risiko verringert, dass der IT-Support mit Supportanfragen überlastet wird, und es wird ein reibungsloser Übergang gewährleistet.

- TechDoc: SAML Slow Rollout

Anschließend kann ZTNA mithilfe des Cloud SWG Agent Traffic Managers schrittweise eingeführt werden. Ausgewählte Benutzer oder Gruppen, für die SAML aktiviert ist, können über den Symantec Agent auf interne Anwendungen zugreifen, ohne den Endpunkt überhaupt berühren zu müssen.

- TechDoc: Agent Traffic Manager

Unternehmen, die den Symantec Endpoint Security-Agenten für die Umleitung des Datenverkehrs verwenden, können in der ICDm-Konsole ganz einfach Gerätegruppen erstellen, in denen über Gruppenrichtlinien festgelegt werden kann, ob das Gerät den Datenverkehr umleiten soll und wenn ja, wie die Authentifizierung erfolgen soll.

- TechDoc: Symantec Endpoint Security - Web and Traffic Redirection

Schnelle Einarbeitung:

Für Unternehmen, die bereits SAML-Authentifizierung mit ihrem Symantec Agent durchführen, kann ZTNA unternehmensweit ohne Änderungen an den Endgeräten der Benutzer implementiert werden. Sobald der Cloud SWG-Mandant und der ZTNA-Mandant mit einem Token integriert und das interne DNS definiert sind, werden interne Anfragen der Benutzer sofort aufgelöst und an die richtige Anwendung weitergeleitet – sofern die Richtlinien dies zulassen.

Es wird empfohlen, DNS, Netzwerksegmente und Zugriffsrichtlinien vor der Integration mit dem Cloud SWG-Mandanten zu definieren. Agent Traffic Manager kann jedoch auch verwendet werden, um sicherzustellen, dass keine Cloud SWG-Agenten ZTNA nutzen, bis das Unternehmen dazu bereit ist.

Langsame Einführung für Anwendungen:

Um eine neue Anwendung langsam für eine Testgruppe einzuführen, wenn Ihr Unternehmen bereits auf ZTNA umgestellt ist, gehen Sie wie folgt vor:

1. Konfigurieren Sie in ATM die Umgehung der Anwendung für alle Benutzer

2. Erstellen Sie die Anwendung in der ZTNA-Konsole

3. Schließen Sie die Anwendung für die festgelegte Testgruppe von der Umgehung in ATM aus

Diese Schritte gewährleisten, dass der Anwendungsdatenverkehr ausschließlich von der Testgruppe abgefangen wird.

Agentenloser Zugriff

Einige Unternehmen entscheiden sich zunächst für eine agentenlose Bereitstellung, insbesondere wenn sie davon ausgehen, dass sie in Zukunft viele Anwendungen über die agentenlose Methode unterstützen werden.

Dieser Ansatz ist ausgezeichnet, da er mit VPNs koexistieren kann und Unternehmen die vollständige Kontrolle über die Geschwindigkeit der Einführung ermöglicht. Es wird empfohlen, mit einer kleinen Anzahl von Anwendungen mit klar definierten Benutzergruppen zu beginnen und diese auf ZTNA umzustellen.

Eine bewährte Vorgehensweise besteht darin, einen benutzerdefinierten Domänennamen für Ihren ZTNA-Mandanten zu verwenden, damit die Benutzer wissen, dass sie sich bei vom Unternehmen verwalteten Anwendungen anmelden.

- TechDoc: Custom Domain

Symantec ZTNA-Einrichtungsleitfaden

Erste Bereitstellung

Gerätekonformität

Symantec Endpoint Security ist für die Gerätekonformität für den agentenbasierten Zugriff erforderlich. Durch die Nutzung von Host-Integritätsprüfungen können Administratoren sicherstellen, dass nur autorisierte Unternehmensendpunkte auf private Anwendungen zugreifen.

Es wird empfohlen, mit internen Endpoint-Management-Teams zusammenzuarbeiten, um das Basisprofil der Unternehmensgeräte zu verstehen und eine Compliance-Richtlinie zu entwerfen, die so einfach wie möglich auf sie ausgerichtet werden kann. Zusätzliche Kriterien wie die Lokalisierung des Benutzers und die Quell-IP können ebenfalls genutzt werden, um die Einhaltung von Datenstandards wie etwa der DSGVO usw. sicherzustellen.

- TechDoc: ZTNA Device Compliance

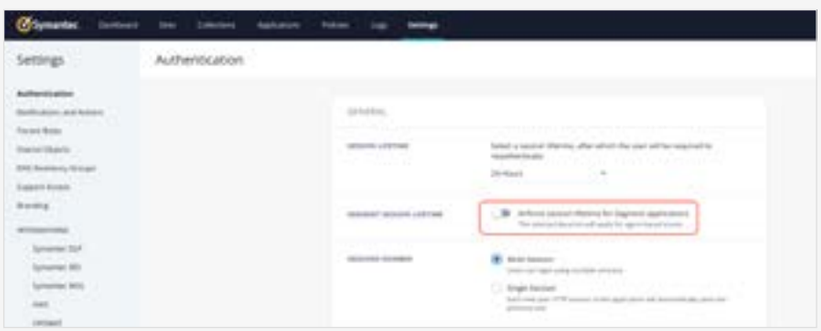
ZTNA „Immer aktiviert/Auf Abruf“

Einige Kunden entscheiden sich für den Modus „ZTNA immer aktiviert“. Dadurch können Benutzer über den Symantec-Agenten verbunden bleiben, solange ihre Identity Provider (IDP)-Sitzung aktiv ist, was einen erheblichen Vorteil gegenüber herkömmlichen VPNs darstellt.

Bestimmte Szenarien erfordern jedoch einen differenzierteren Ansatz. Während Kunden möglicherweise längere IDP-Sitzungen für den Zugriff auf Symantec Web Gateway (SWG) bevorzugen (um häufige Authentifizierungsaufforderungen beim Surfen im Internet zu vermeiden), müssen sie möglicherweise gleichzeitig kürzere Sitzungen (z. B. 12 Stunden) für ZTNA durchsetzen, was eine erneute Authentifizierung speziell für den Zugriff auf interne Anwendungen erfordert.

Um diesen „Auf Abruf“-Ansatz zu ermöglichen, sollte die Funktion „Segment Session Lifetime“ aktiviert werden. Dadurch wird sichergestellt, dass ZTNA-Sitzungen den konfigurierten Einstellungen für die Sitzungsdauer entsprechen, ohne dass eine erneute Authentifizierung für den allgemeinen Internetzugang erforderlich wird.

- Tech Doc: Segment Session Lifetime



Symantec ZTNA-Einrichtungsleitfaden

Automatisierung und Operationalisierung

Einführung von Anwendungen

Anwendungs-Onboarding:

Jede Anwendung, die über ZTNA bereitgestellt werden soll, muss in der Richtlinien-Engine definiert werden. Dies kann einen hohen Arbeitsaufwand bedeuten, da alle Anwendungen oder Netzwerkstandorte vordefiniert werden müssen. ZTNA-Engineering-Teams sollten mit IdP- und ITSM-Gruppen innerhalb des Unternehmens zusammenarbeiten, um sich einen Überblick über den Anwendungsbestand zu verschaffen. Ideal ist es, eine Pipeline einzurichten, um Anwendungen automatisch in ZTNA zu integrieren und auf dem neuesten Stand zu halten. Dies kann mit der ZTNA API automatisiert werden.

- API: Manage Applications

Für die Ersteinrichtung mit agentenbasiertem Zugriff können Unternehmen zunächst die Definition breiter Subnetze in Betracht ziehen, auf die Benutzer zugreifen können. So können sie sicherstellen, dass den Benutzern keine Anwendungen fehlen. Dadurch erhalten sie außerdem Zugriff auf Anwendungen, auf die sie sonst keinen Zugriff benötigen – die ZTNA-Richtlinie folgt dem Prinzip „Longest Prefix Match“ (längste Präfixübereinstimmung), sodass Administratoren überlappende Netzwerksegmentdefinitionen erstellen können und die genaueste davon die Zugriffsrichtlinie ausführt. Je mehr Anwendungen mit hoher Auswirkung definiert werden, desto strengere Zugriffsrichtlinien können für sie festgelegt werden.

- Longest Prefix Match: Wikipedia

Überwachung:

Die allgemeine Dienstüberwachung ist zwar wichtig, kann jedoch größtenteils automatisiert werden, indem in der ZTNA-Konsole Benachrichtigungseinstellungen für den Verbindungsstatus und den Anwendungsstatus festgelegt werden. Eine weitere Überwachungsebene, die Unternehmen berücksichtigen sollten, ist der Benutzerzugriff – die ZTNA-API kann so abgefragt werden, dass nur Protokolle für fehlgeschlagene Verbindungsversuche bereitgestellt werden. Dies kann Aufschluss darüber geben, ob Benutzer und Gruppen Zugriff auf Anwendungen benötigen, der derzeit von den ZTNA-Richtlinien nicht unterstützt wird. Dies kann in IAM-Überprüfungen einbezogen werden, um die ZTNA-Richtlinien in Zukunft besser zu rationalisieren.

- API: Forensic Logs

Verhinderung von Datenverlust:

DLP Cloud Detection ist für agentenloses ZTNA verfügbar und schließt eine Lücke beim Zugriff auf private Anwendungen von nicht verwalteten Geräten. Vor der Bereitstellung sollte das ZTNA-Team gemeinsam mit dem DLP-Administrationsteam ein Governance-Framework erstellen, um zu ermitteln, welche DLP-Richtlinien welchen Anwendungen zugewiesen werden sollten. DLP-Administratoren verwenden die DLP Enforce-Konsole zum Erstellen von DLP-Richtlinien. Das ZTNA-Team muss lediglich festlegen, welchen agentenlosen Anwendungen DLP-Richtlinien zugewiesen werden sollen.

DLP-Richtlinien werden einer „Anwendungserkennungsgruppe“ zugewiesen, und diese Gruppen-ID wird der ZTNA-Richtlinie zugewiesen. DLP-Richtlinien für Anwendungserkennungsgruppen sind eine Viele-zu-Viele-Zuordnung, aber einer Anwendung in ZTNA kann nur eine Anwendungserkennungsgruppe zugewiesen werden. Das Erstellen von Anwendungs-„Ebenen“ oder „Datenbereichen“ kann dabei helfen, die ZTNA-Richtlinie einmalig einzurichten und es dem DLP-Team dann zu ermöglichen, Richtlinien bei Bedarf zu aktualisieren und neu zuzuweisen, ohne dass das ZTNA-Engineering-Team eingreifen muss.

DevSecOps:

ZTNA bietet eine enorme Chance, die Abhängigkeit der Softwareentwicklung von VPN auf eine echte Microservice-Architektur für die CI/CD-Pipeline zu verlagern. ZTNA-Planungsteams sollten mit ihren internen Entwicklungsteams zusammenarbeiten, um zu prüfen, ob diese in ZTNA integriert werden können. So müssten Entwickler nicht mehr von bekannten Netzwerken aus auf Cloud-Ressourcen zugreifen – was die typische Sicherheitsrichtlinie der meisten Unternehmen ist.

Symantec ZTNA verfügt über einen vorgefertigten Terraform-Anbieter, der in die CI/CD-Pipeline integriert werden kann, aber die ZTNA-API unterstützt jeden Anbieter.

- Terraform: Github
- Symantec ZTNA: SSH Gateways

Automatische Skalierung:

Symantec ZTNA-Anwendungskonnektoren sorgen automatisch für einen Lastenausgleich zwischen den Sitzungen innerhalb einer „Site“. Sollte dennoch mehr Bandbreite benötigt werden, kann durch die Bereitstellung zusätzlicher Konnektoren die Last aktiv verteilt werden, ohne Ausfallzeiten zu verursachen.

Unternehmen sollten die Automatisierung der Bereitstellung neuer Konnektoren über eine ITSM-Plattform in Betracht ziehen. Die Sites sind bereits eingerichtet, und wenn ein neuer

Konnektor benötigt wird, kann die ZTNA-API nach einem Einmalpasswort abgefragt und sofort ein neuer Container gestartet werden.

- ZTNA API: Create Connector

Symantec ZTNA-Einrichtungsleitfaden

Automatisierung und Operationalisierung

Just-in-Time-Zugriff

Viele Unternehmen haben Schwierigkeiten damit, den Zugriff auf Anwendungen über die eigentliche Anwendung hinaus zuzuweisen. Bei ZTNA müssen Administratoren bereits vor der Authentifizierung der Benutzer bei der Anwendung entscheiden, auf welche Anwendungen diese zugreifen dürfen.

Aus diesem Grund sollten Unternehmen eine Integration mit einer ITSM-Plattform in Betracht ziehen, damit Benutzer Anfragen einreichen können, um automatisch Zugriff zu erhalten. Just-in-Time-Zugriff bedeutet, dass Benutzer für einen kurzen Zeitraum Zugriff erhalten, um ihren Geschäftsprozess abzuschließen, und dass dieser Zugriff automatisch widerrufen werden kann – zu diesem Zeitpunkt sollte das IAM-Team die Anfrage für einen dauerhaften Zugriff prüfen.

- ZTNA API: Update Access Policy

Widerstandsfähigkeit von Unternehmen

Symantec ZTNA wird als echte Microservice-SaaS-Plattform zusätzlich zur Google Cloud Platform bereitgestellt. Das bedeutet, dass auf allen Ebenen des Dienstes Redundanz integriert ist. Der primäre Punkt eines potenziellen Ausfalls ist die Verbindung des Application Connector mit der Symantec Enterprise Cloud. Die Konnektoren sind bestimmten GCP-Regionen zugeordnet, in erster Linie aus Gründen des Datenschutzes und der Einhaltung von Sicherheitsvorschriften.

Jede GCP-Region verfügt über drei Verfügbarkeitszonen, von denen der ZTNA- Konnektor mit zwei der Zonen aktiv-aktiv sein wird. Im Falle eines Ausfalls einer GCP-Verfügbarkeitszone leitet der Konnektor automatisch alle Verbindungen über die verfügbare Verfügbarkeitszone weiter und stellt eine neue Verbindung mit der dritten Verfügbarkeitszone her. So werden alle Verbindungen innerhalb der Region aufrechterhalten.

Wenn eine GCP-Region in keiner der Zonen verfügbar wäre, würden ZTNA-Administratoren über einen Ausfall benachrichtigt werden. Zusätzlich könnte die ZTNA API abgefragt werden, um ebenfalls diesen Status zu ermitteln.

Der Dienst kann schnell wiederhergestellt werden, indem eine andere GCP-Region genutzt wird. Die Konfiguration hierfür würde so aussehen, dass zwei ZTNA-„Sites“ am selben Anwendungsbereitstellungsort (Rechenzentrum, IaaS usw.) bereitgestellt werden. „Site A“ wäre die primäre Site für die normale Nutzung und würde aus Leistungsgründen entweder mit der nächstgelegenen GCP-Region oder aus Gründen der Datenkonformität mit einer bestimmten Region verbunden werden. Dann würde „Site B“ so konfiguriert werden, dass sie eine andere GCP-Region nutzt. Diese beiden Konnektoren würden also nebeneinander im Netzwerk des Unternehmens angeordnet, aber jeweils mit unterschiedlichen GCP-Regionen verbunden sein.

ZTNA-Anwendungen für diesen Standort würden so konfiguriert, dass sie über den ZTNA- Konnektor „Site A“ verbunden werden, und keine Anwendung würde mit „Site B“ verbunden werden. Im Falle eines Ausfalls können über die ZTNA-Benutzeroberfläche und über die API alle Anwendungen so aktualisiert werden, dass sie die Verbindung über „Site B“ herstellen – der zur GCP-Region weiterleitet, die online ist.

Da dies alles hinter dem ZTNA-Dienst geschieht, sind keine DNS-Änderungen erforderlich und es sind keine Änderungen am Workflow der Endbenutzer notwendig.

- ZTNA API: Update Application