GUIDE

Guide de déploiement de Symantec ZTNA

Champ d'application

Ce guide explore l'adoption du ZTNA à travers l'expérience des praticiens, en mettant en lumière les meilleures pratiques pour planifier, intégrer et faire évoluer son déploiement au sein d'une organisation. Chaque organisation suit un parcours qui lui est propre, en fonction des profils utilisateurs, de l'inventaire applicatif et de l'architecture informatique en place. L'un des aspects essentiels abordés dans ce guide est l'identification des groupes et équipes internes à mobiliser pour garantir une mise en œuvre réussie du ZTNA.

Ce guide est conçu pour être utilisé en complément de la documentation technique de Broadcom, afin de s'assurer que chaque étape de mise en œuvre reste alignée avec les capacités actuelles et les configurations les plus récentes.

Ressources techniques de Broadcom: Symantec Zero Trust Network Access

Planification initiale

Le déploiement d'une solution ZTNA implique de nombreux facteurs à anticiper et l'implication de diverses parties prenantes. Les points clés ci-dessous doivent être pris en compte en amont de la mise en œuvre technique, sous peine de provoquer des retards significatifs dans le projet. Pour les étapes générales de planification, veuillez consulter la section suivante Ressource technique

Nom et localisation du locataire ZTNA

Deux paramètres doivent être définis avant de créer le locataire ZTNA dans le portail de gestion des clients (Customer Management Portal, CMP) :

1. La géolocalisation du PoD de gestion (UE/États-Unis) est un paramètre clé, car elle détermine la région de routage des flux de données ainsi que l'emplacement de collecte des journaux. Ce choix est déterminant, car les PoD de connectivité — chargés de l'application des politiques — sont géographiquement associés à leurs PoD de gestion respectifs. Affectation des PoD de gestion et de connectivité
2. Le nom du locataire génère un domaine personnalisé unique, utilisé pour l'accès au Portail des utilisateurs et à l'application sans agent. Il est crucial de choisir avec soin le nom du locataire, afin qu'il reflète fidèlement votre organisation et votre environnement, car ce nom ne pourra plus être modifié une fois défini.

   L'URL complète du locataire est construite en associant le nom de locataire choisi au suffixe « luminatesec.com ».

Fournisseurs d'identité

L'intégration d'un fournisseur d'identité (Identity Provider, IdP) est une étape clé dans Symantec ZTNA, car elle constitue la base du processus d'authentification. Bien que des utilisateurs locaux puissent suffire pour une preuve de concept (PoC), il est indispensable d'impliquer l'équipe en charge de la gestion de l'IdP de l'organisation en tant que partie prenante, afin d'assurer le succès du déploiement en production. Les personnes en charge du déploiement du ZTNA sont souvent également impliquées dans des initiatives liées au Zero Trust, au SSE, ou à l'architecture des proxys et VPN. La collaboration avec l'équipe IdP est indispensable pour comprendre comment les utilisateurs et les groupes sont associés aux applications fournies par ZTNA, ce qui permet ensuite de structurer les politiques d'accès de manière appropriée.

Deux aspects techniques majeurs doivent être pris en compte : l'intégration avec la ou les plateformes SSO de l'organisation, généralement via le protocole SAML (et parfois OIDC), et la résolution de groupe, qui peut s'effectuer par l'analyse des attributs SAML ou par l'utilisation du protocole SCIM

L'option « SAML générique » est la méthode d'intégration IdP recommandée. Ce choix permet à la fois l'intégration SAML et la résolution des groupes, via les options SCIM ou les attributs SAML.

- Ressource technique: Intégrer l'IdP

Si l'IdP du client ne prend pas en charge le protocole SCIM, la résolution des groupes devra s'effectuer via l'option « Attribut SAML ». Cela permet au client de gérer la résolution des groupes directement à partir de la réponse SAML.

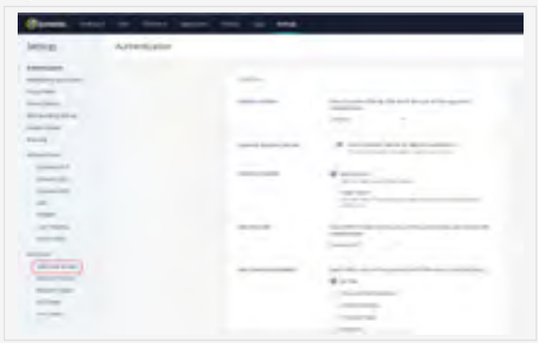
Guide de déploiement de Symantec ZTNA

Planification initiale

Fournisseurs d'identité

Accès sans agent uniquement

Les « utilisateurs locaux » peuvent être utilisés dans le magasin d'entités ZTNA pour les applications sans agent, telles que les applications Web, RDP, SSH ou TCP. Cette option convient pour l'évaluation de services, la réalisation d'une preuve de concept (PoC) ou l'octroi d'un accès restreint à des tiers.



Accès exclusivement via agent

Pour un accès basé sur un agent utilisant les agents WSSA, SES et ESA avec des applications segmentées, l'intégration SAML est indispensable. Cela implique que les utilisateurs locaux ne sont pas supportés. Par ailleurs, l'intégration du fournisseur d'identité (Identity Provider, IDP) à Symantec Cloud SWG implique la mise en place d'une authentification SAML au sein de l'organisation pour accéder à Cloud SWG.

- Ressource technique: Authentification SAML Cloud SWG

Recensement des applications et des méthodes d'accès via ZTNA

La transition vers une architecture ZTNA repose sur une approche descendante, mais nécessite des données provenant du terrain. Contrairement à cela, les VPN et autres solutions d'accès à distance traditionnelles n'ont généralement pas besoin de connaître l'application ciblée par l'utilisateur, cette gestion étant assurée par les propriétaires des applications.

La première décision clé consiste à déterminer si l'organisation souhaite adopter une solution ZTNA avec agent ou sans agent. Même si ces deux composantes coexistent généralement dans les déploiements ZTNA, il est recommandé, dans le cadre d'un projet pilote, de débuter par l'une d'entre elles.

Authentification par le biais d'un agent

L'approche d'accès via agent présente trois principaux atouts

- **Expérience utilisateur fluide :** les utilisateurs finaux ne subissent aucun impact, car aucune modification du domaine ou du réseau n'est requise.
- **S'appuie sur l'infrastructure déjà en place :** cette méthode repose sur le DNS privé de l'organisation, ce qui évite toute modification du flux de travail.
- **Intégration rapide :** des groupes entiers de réseaux peuvent être protégés rapidement à travers une seule application et une politique unifiée. des règles granulaires fondées sur le principe du moindre privilège peuvent ensuite être mises en œuvre sans contrainte de temps.

Pour les clients Symantec déjà utilisateurs des agents WSSA, SEC ou ESA dans le cadre de leurs déploiements SWG, CASB ou EPP, le déploiement de ZTNA s'avère généralement plus simple. Les administrateurs ZTNA peuvent commencer par définir de larges segments du réseau où se trouvent les applications, sans avoir à identifier précisément celles qui sont utilisées. Progressivement, les administrateurs peuvent affiner les politiques afin de les rendre plus précises, en limitant l'accès aux seuls domaines ou adresses IP strictement nécessaires aux utilisateurs.

En revanche, pour les clients qui découvrent Symantec, la méthode d'accès via agent peut représenter un obstacle au déploiement initial, en raison des contraintes liées à l'installation de l'agent Ils privilégient généralement l'approche sans agent lors de la phase initiale.

Guide de déploiement de Symantec ZTNA

Planification initiale

Inventario de aplicaciones y método de acceso ZTNA

Accès sans agent

Le ZTNA sans agent adopte une approche plus sécurisée en imposant dès le départ une définition explicite des règles de moindre privilège pour l'accès aux ressources. Cette approche requiert la configuration de l'ensemble des applications dans la console Symantec ZTNA, ainsi que la définition de politiques d'accès pour les utilisateurs et les groupes. Bien que cette méthode modifie le parcours utilisateur — celui-ci devant passer par le DNS global pour accéder à l'application, soit via une publication de l'URL dans le DNS public (mise à jour CNAME), soit par modification de l'URL — les utilisateurs adoptent généralement l'accès sans agent au VPN une fois qu'ils y sont familiarisés.

Au-delà des applications Web, l'approche sans agent est également avantageuse pour les accès SSH et RDP — y compris via les clients natifs — sans perturber les flux de travail des équipes DevOps.

Public cible (Agent Traffic Manager)

Lors de la mise en œuvre de l'accès par agent, il est crucial d'identifier avec soin le public cible afin de limiter les risques de perturbations à grande échelle en cas d'erreurs de configuration. Dans un premier temps, restreignez le déploiement de ZTNA avec Agent Traffic Manager à un nombre limité d'utilisateurs ou de groupes afin de mieux maîtriser la phase initiale.

Conformité des appareils

La conformité des appareils peut être assurée avec Symantec ZTNA grâce à l'agent Symantec Endpoint Protection, sous réserve que l'organisation dispose d'une licence Symantec Enterprise Security. Cette fonctionnalité repose sur les contrôles d'intégrité de l'hôte : Ressource technique

Lors de la planification du ZTNA, il est crucial de déterminer les critères que l'organisation souhaite appliquer pour évaluer les appareils des utilisateurs finaux. Certificats d'appareils ? Niveau de correctif du système d'exploitation ? Processus en cours d'exécution ? Collaborer avec l'équipe en charge de la gestion des terminaux peut faciliter l'identification des réponses à ces questions et permettre une configuration rapide du profil de conformité.

Gestion administrative

En fonction de la manière dont les applications métier sont gérées et distribuées au sein de l'organisation, plusieurs équipes peuvent être amenées à intervenir sur la console d'administration ZTNA. Dans ce contexte, il est recommandé de définir en amont les rôles et responsabilités de chaque équipe afin de mettre en place des politiques RBAC permettant à chacun d'intervenir dans son périmètre sans empiéter sur celui des autres.

Anticiper les groupes impliqués dans la mise en œuvre de ZTNA permet de définir rapidement les rôles RBAC adaptés. Trois rôles clés à prendre en compte :

- **Administrateur de la plateforme ZTNA :** administrateur global responsable de l'intégration de l'IdP (ou des IdPs), de la gestion des journaux, de l'attribution des rôles d'administrateur de politiques, de la création des sites de déploiement et de l'autorisation d'accès à l'API.
- **Administrateur de site :** responsable du déploiement et de la gestion des connecteurs ZTNA sur les sites dont il a la charge.
- **Administrateurs d'application (collection) :** responsables de l'importation des applications dans la plateforme ZTNA et de la définition des politiques d'accès associées.
- **Administrateur des politiques (collection) d'accès :** rôle limité à la gestion des règles d'accès aux applications.

Pour en savoir plus sur l'administration basée sur les rôles (RBAC), vous pouvez consulter la Ressource technique.

Guide de déploiement de Symantec ZTNA

Déploiement initial

Intégration du fournisseur d'identité

Comme mentionné précédemment, une session de travail avec l'équipe d'ingénierie IdP doit être planifiée afin de configurer l'authentification unique (SSO) ainsi que la résolution des groupes dans le cadre de ZTNA. Pour une solution ZTNA reposant sur un agent, le Cloud SWG de l'organisation doit déjà disposer d'un plan d'intégration avec le même fournisseur d'identité (IdP), ce qui implique l'utilisation d'un portail captif compatible SAML. La section ci-dessous dédiée à l'automatisation fournit des recommandations pour adopter l'authentification SAML avec l'agent Symantec.

Accès administrateur

Si des rôles ont été définis lors de la phase de planification, la première étape après l'intégration de l'IdP consiste à ajouter les administrateurs supplémentaires. La meilleure pratique consiste à créer un groupe dans l'IdP et à l'associer au rôle d'administrateur global dans ZTNA. Par ailleurs, il peut s'avérer particulièrement pertinent de définir des « collections » regroupant les administrateurs responsables de l'intégration des applications et de la définition des politiques d'accès.

Reproduire les approches internes en matière de « niveaux » ou de « groupes de services » applicatifs peut faciliter l'alignement de l'architecture ZTNA avec les processus internes de l'organisation. Le groupe IdP peut jouer un rôle clé à ce stade, car il a souvent déjà structuré ces groupes de travail.

- Ressource technique: Collections ZTNA

Déploiement du connecteur

Souvent désigné sous le nom de « Sites » dans Symantec ZTNA, le connecteur permet au service cloud ZTNA d'établir une connexion avec les applications hébergées par les clients, que ce soit dans leurs centres de données ou chez des fournisseurs IaaS.

Les connecteurs doivent être déployés au plus près des applications. Le processus d'inventaire applicatif doit inclure la localisation de chaque groupe d'applications. Il est ensuite recommandé d'installer au minimum deux connecteurs sur chacun de ces segments réseau.

Les connecteurs sont disponibles sous plusieurs formats : Docker, Docker Compose, Kubernetes et machines virtuelles pour ESXi.

Outils d'orchestration du cloud

Pour assurer un cycle de vie fluide des connecteurs dans les outils d'orchestration cloud tels que Kubernetes, OpenShift, Fargate, ou autres, il est recommandé d'opter pour le mode d'authentification « Site ». Cela évite d'avoir à préenregistrer un mot de passe à usage unique (OTP) pour chaque connecteur.

- Connecteurs: Ressource technique

Continuité des activités et reprise après sinistre

Lors du déploiement des connecteurs pour un site, il est nécessaire de spécifier la région GCP à laquelle ils doivent se connecter. En cas de défaillance de GCP ou du réseau de l'organisation, un site de secours associé à une autre région peut être utilisé comme solution de reprise.

Pour cela, il convient de créer un nouveau site associé à une autre région, puis de déployer les connecteurs dans une zone différente du réseau de l'organisation, tout en maintenant l'accès aux applications du site principal. En cas d'incident, les applications peuvent être redéployées sur un autre site via l'infrastructure ZTNA.

Ce processus peut être entièrement automatisé grâce à un script exploitant

- API ZTNA. API : lier l'application au site

Guide de déploiement de Symantec ZTNA

Déploiement initial

Agent Traffic Manager

Assurez-vous que les entités concernées par l'application de ZTNA soient clairement identifiées. Par défaut, aucune entité n'est associée à ZTNA, sauf en cas de configuration explicite.

Pour éviter tout impact potentiel, il est recommandé d'attribuer les entités ZTNA dans l'Agent Traffic Manager avant de procéder à la création du Segment d'application.

Catalogue des applications

Comme mentionné précédemment, il est crucial d'avoir une vision claire de l'inventaire des applications prises en charge par ZTNA, qu'elles soient basées sur un agent ou non. Une fois le connecteur déployé, les administrateurs doivent définir les applications individuellement ou par sous-réseaux, selon l'utilisation de l'agent Symantec.

Associer chaque application à une collection adaptée permet de simplifier la définition des politiques d'accès par la suite.

Afin d'éviter tout accès non autorisé avant le déploiement de ZTNA, chaque application dispose d'un bouton « Activer » permettant de contrôler sa mise en service.

Configuración de políticas

Les utilisateurs ne peuvent accéder aux applications que si une politique définit explicitement les entités concernées ainsi que l'application cible. Conformément au principe du moindre privilège, les applications sont inaccessibles par défaut, sauf autorisation explicite. L'accès à une application ne peut être autorisé qu'à travers la mise en place d'une politique dédiée.

Il convient de noter que plusieurs politiques peuvent être définies pour accorder des accès à différentes entités selon les applications ciblées. Dans ce cas, la règle de « résolution des conflits » (définie dans Évaluation de la politique d'accès) détermine quelle politique sera appliquée.

Guide de déploiement de Symantec ZTNA

Déploiement initial

Intégration des utilisateurs finaux

Le déploiement de l'accès pour les utilisateurs finaux après une phase de preuve de concept représente l'un des principaux défis de ZTNA, car les équipes de sécurité doivent veiller à minimiser l'impact sur l'expérience utilisateur. Les sections suivantes présentent les meilleures pratiques pour favoriser l'adoption de ZTNA par les utilisateurs finaux.

Déploiement progressif de ZTNA via SAML :

L'utilisation initiale de Symantec Agent for Zero Trust Network Access constitue la méthode la plus fiable pour garantir aux utilisateurs finaux l'accès aux applications habituellement accessibles via VPN. En s'appuyant sur le DNS interne et en opérant au niveau de la couche 3, il permet de prendre en charge les applications existantes.

L'activation du portail captif SAML pour Cloud SWG peut représenter un obstacle majeur à la mise en œuvre de ZTNA, car de nombreuses entreprises craignent de compromettre l'expérience utilisateur. Pour une mise en œuvre efficace de l'accès réseau Zero Trust, il est essentiel d'adopter pleinement le principe Zero Trust dès la phase de conception architecturale.

Le portail captif SAML pour Cloud SWG peut désormais être déployé de manière progressive auprès de groupes ciblés, permettant aux organisations de le tester à petite échelle. Cette approche limite les risques de surcharge du support informatique et facilite une transition fluide

- Ressource technique: Déploiement progressif de SAML

À partir de là, le déploiement de ZTNA peut se faire de manière progressive, en s'appuyant sur l'Agent Traffic Manager de Cloud SWG. Certains utilisateurs ou groupes pour lesquels SAML est activé peuvent commencer à accéder aux applications internes via l'agent Symantec, sans intervention sur le poste client.

- Ressource technique: Agent Traffic Manager

Les organisations utilisant l'agent Symantec Endpoint Security pour la redirection du trafic peuvent facilement créer des groupes d'appareils dans la console ICDm. La politique associée à chaque groupe permet de définir si l'appareil doit rediriger le trafic et, le cas échéant, les modalités d'authentification du trafic..

- Ressource technique: Symantec Endpoint Security: redirection web et du trafic

Intégration rapide :

Pour les organisations utilisant déjà l'authentification SAML avec l'agent Symantec, ZTNA peut être déployé à l'échelle de l'entreprise sans modification des terminaux utilisateurs. Une fois l'intégration entre les locataires Cloud SWG et ZTNA effectuée via un jeton, et le DNS interne configuré, les requêtes internes des utilisateurs sont automatiquement résolues et dirigées vers l'application appropriée, sous réserve des politiques d'accès.

Il est conseillé de définir les politiques liées au DNS, aux segments réseau et aux accès avant d'intégrer le locataire Cloud SWG. Toutefois, Agent Traffic Manager peut être utilisé pour s'assurer qu'aucun agent Cloud SWG ne recourt à ZTNA tant que l'organisation n'est pas prête.

Déploiement progressif des applications :

Pour déployer progressivement une nouvelle application auprès d'un groupe pilote dans un environnement ZTNA déjà en place, suivez les étapes suivantes :

1. Dans Agent Traffic Manager, configurez l'application en mode contournement pour l'ensemble des utilisateurs.
2. Procédez à la création de l'application depuis la console ZTNA.
3. Procédez à la création de l'application depuis la console ZTNA.

Ces étapes assurent que seul le public du groupe de test peut intercepter le trafic des applications.

Accès sans agent

Certaines organisations privilégient dans un premier temps un déploiement sans agent, notamment lorsqu'elles envisagent de gérer un grand nombre d'applications par ce biais à l'avenir.

Cette approche présente un réel avantage : elle est compatible avec les VPN et offre aux organisations une maîtrise totale du rythme de déploiement. Il est conseillé de débuter avec un nombre restreint d'applications, disposant de bases d'utilisateurs bien identifiées, avant de les migrer vers ZTNA.

Il est recommandé d'utiliser un nom de domaine personnalisé pour le locataire ZTNA, afin que les utilisateurs identifient clairement qu'ils accèdent à des applications gérées par l'entreprise.

- Ressource technique: Domaine personnalisé

Guide de déploiement de Symantec ZTNA

Déploiement initial

Cumplimiento del dispositivo

Symantec Endpoint Security est requis pour garantir la conformité des appareils dans le cadre d'un accès basé sur un agent. En exploitant les contrôles d'intégrité de l'hôte, les administrateurs peuvent s'assurer que seuls les terminaux autorisés de l'entreprise accèdent aux applications privées.

Il est recommandé de collaborer avec les équipes internes responsables de la gestion des terminaux afin de bien comprendre le profil type des appareils utilisés dans l'entreprise, et de définir une politique de conformité aussi simple que possible pour s'y adapter. Des critères additionnels, tels que la géolocalisation de l'utilisateur ou l'adresse IP source, peuvent également être intégrés afin d'assurer la conformité aux réglementations sur les données, comme le RGPD.

- Ressource technique: Conformité des appareils à ZTNA

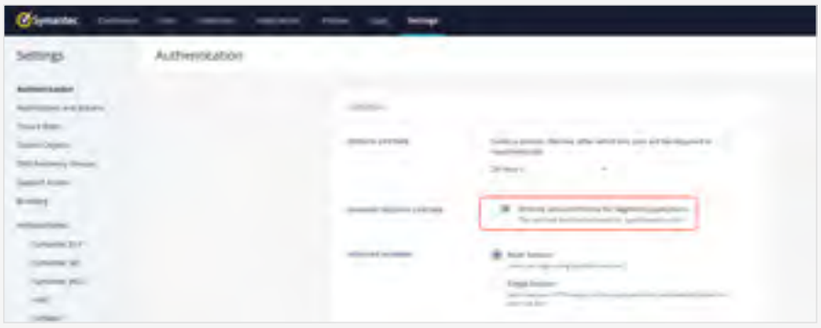
ZTNA « Toujours activé/À la demande »

Certains clients optent pour un fonctionnement en mode « ZTNA permanent ». Cela permet aux utilisateurs de rester connectés via l'agent Symantec tant que leur session auprès du fournisseur d'identité (IdP) reste active, offrant ainsi un avantage notable par rapport aux VPN traditionnels.

Toutefois, certains cas d'usage requièrent une approche plus adaptée et spécifique. Bien que les clients puissent préférer des sessions IdP prolongées pour accéder à Symantec Web Gateway (SWG), afin de limiter les demandes d'authentification lors de la navigation sur Internet, ils peuvent également souhaiter imposer des sessions plus courtes — par exemple de 12 heures — pour ZTNA, nécessitant une authentification distincte pour l'accès aux applications internes.

Pour adopter cette approche « à la demande », il est nécessaire d'activer la fonctionnalité de durée de vie des sessions de segment. Cela permet aux sessions ZTNA de respecter les paramètres de durée configurés, tout en évitant d'imposer une nouvelle authentification pour l'accès général à Internet.

- Ressource technique: Durée de vie de la session de segment



Guide de déploiement de Symantec ZTNA

Automatisation et opérationnalisation

Cumplimiento del dispositivo

Intégration des applications :

Toute application destinée à être distribuée via ZTNA doit être définie dans le moteur de politique, ce qui peut représenter une charge de travail conséquente en raison de la nécessité de préconfigurer l'ensemble des applications ou des emplacements réseau. Les équipes ZTNA doivent collaborer étroitement avec les groupes en charge de l'IdP et de la gestion des services informatiques afin d'avoir une vision claire de l'inventaire des applications. L'idéal est de mettre en place un pipeline automatisé permettant d'intégrer les applications dans ZTNA et de les maintenir à jour. Cette automatisation peut être réalisée via l'API ZTNA.

- API: Gérer les applications

Pour la configuration initiale de l'accès basé sur un agent, les organisations peuvent envisager de définir des sous-réseaux larges, afin de garantir aux utilisateurs un accès complet et de s'assurer qu'aucune application ne leur échappe. Cela peut également permettre aux utilisateurs d'accéder à des applications qui ne leur sont pas nécessairement destinées. La politique ZTNA repose sur le principe de la correspondance de préfixe la plus longue, ce qui autorise la création de segments réseau qui se chevauchent ; dans ce cas, c'est la définition la plus précise qui détermine la politique d'accès appliquée. Ainsi, lorsque des applications critiques sont identifiées, elles peuvent être soumises à des politiques d'accès renforcées.

- Correspondance de préfixe la plus longue : Wikipedia

Surveillance :

Bien que la surveillance globale des services soit essentielle, la majorité de ces tâches peuvent être automatisées en configurant les notifications dans la console ZTNA, notamment pour le suivi de l'état des connecteurs et des applications. L'accès utilisateur constitue un niveau supplémentaire de surveillance que les organisations devraient considérer : l'API ZTNA peut être interrogée pour extraire uniquement les journaux des tentatives de connexion échouées. Cela peut aider à déterminer si certains utilisateurs ou groupes ont réellement besoin d'accéder à certaines applications, et si la politique ZTNA est correctement définie en ce sens.

Si la politique ZTNA actuelle ne le permet pas, ces informations peuvent être intégrées aux revues de gestion des identités et des accès, afin d'optimiser les politiques ZTNA à l'avenir.

- API: Journaux médico-légaux

Prevención de pérdida de datos:

La détection DLP dans le cloud est disponible pour le ZTNA sans agent, comblant ainsi une lacune en matière de sécurité lors de l'accès à des applications privées depuis des appareils non gérés. Avant le déploiement, l'équipe ZTNA doit collaborer avec l'équipe en charge de la prévention des pertes de données afin de définir un cadre de gouvernance permettant d'associer les politiques DLP appropriées aux différentes applications. Les administrateurs DLP utiliseront la console Enforce pour rédiger les politiques de prévention des pertes de données. De leur côté, l'équipe ZTNA n'a qu'à spécifier les applications sans agent auxquelles ces politiques doivent être appliquées.

Les politiques de prévention des pertes de données seront associées à un groupe nommé « Détection d'application », dont l'identifiant sera ensuite intégré à la politique ZTNA. Les politiques de prévention des pertes de données peuvent être associées à plusieurs groupes de détection d'application.

Toutefois, dans le cadre de ZTNA, une application ne peut être liée qu'à un seul groupe de détection d'application. La définition de « Niveaux » d'application ou de « Champs d'application des données » permet de configurer une politique ZTNA unique. Elle offre ensuite à l'équipe de prévention des pertes de données la flexibilité nécessaire pour mettre à jour et réattribuer les politiques selon les besoins, sans solliciter l'équipe d'ingénierie ZTNA.

DevSecOps:

ZTNA représente une excellente opportunité pour réduire la dépendance du développement logiciel au VPN, en favorisant l'adoption d'une véritable architecture microservices au sein du pipeline CI/CD. Les équipes en charge de la planification ZTNA doivent collaborer étroitement avec les équipes de développement internes pour évaluer leur intégration potentielle à ZTNA. L'objectif est de permettre aux développeurs d'accéder aux ressources cloud sans passer par des réseaux connus, en conformité avec les politiques de sécurité généralement adoptées par les organisations.

Symantec ZTNA propose un fournisseur Terraform préconfiguré, facilement intégrable dans le pipeline CI/CD. Toutefois, son API est suffisamment flexible pour prendre en charge n'importe quel fournisseur.

- Terraform: Github
- Symantec ZTNA: Passerelles SSH

Mise à l'échelle automatique :

Les connecteurs d'application Symantec ZTNA assurent automatiquement l'équilibrage de charge des sessions au sein d'un site. En cas de besoin accru en bande passante, il est possible de déployer des connecteurs supplémentaires pour répartir la charge de manière dynamique, sans interruption de service.

Il est judicieux pour une organisation d'envisager l'automatisation du déploiement de nouveaux connecteurs via une plateforme de gestion des services informatiques. Les sites étant préconfigurés, l'ajout de nouveaux connecteurs peut ainsi être déclenché automatiquement selon les besoins.

Lorsqu'un nouveau connecteur est requis, l'API ZTNA peut être sollicitée pour générer un mot de passe à usage unique, permettant le lancement immédiat d'un nouveau conteneur.

- API de ZTNA: Créer un connecteur

Guide de déploiement de Symantec ZTNA

Automatisation et opérationnalisation

Accès juste à temps

De nombreuses organisations éprouvent des réticences à accorder des droits d'accès aux applications en amont de l'application elle-même. Avec ZTNA, les administrateurs doivent définir à quelles applications les utilisateurs peuvent accéder avant même que ceux-ci ne s'authentifient, ce qui constitue un changement par rapport aux pratiques de sécurité traditionnelles.

C'est pourquoi les organisations devraient envisager une intégration avec leur plateforme de gestion des services informatiques, afin de permettre aux utilisateurs de soumettre des demandes d'accès automatisées. L'accès juste-à-temps permet aux utilisateurs d'obtenir des droits d'accès temporaires, limités à la durée nécessaire pour accomplir leurs tâches métier. Une fois cette période écoulée, l'accès est automatiquement révoqué, et l'équipe en charge de la gestion des identités et des accès peut alors examiner les demandes d'accès permanent.

- API de ZTNA: Mettre à jour la politique d'accès

Résilience commerciale

Symantec ZTNA est déployé comme une véritable plateforme SaaS basée sur une architecture microservices sur Google Cloud Platform, garantissant une redondance intégrée à tous les niveaux du service. Le principal point de vulnérabilité réside dans la connexion entre le connecteur d'application et Symantec Enterprise Cloud. Les connecteurs sont associés à des régions spécifiques de Google Cloud Platform, principalement pour répondre aux exigences de confidentialité des données et de conformité en matière de sécurité.

Chaque région GCP comprend trois zones de disponibilité, parmi lesquelles le connecteur ZTNA fonctionne en mode actif-actif sur deux zones. En cas de défaillance d'une zone de disponibilité GCP, le connecteur redirige automatiquement toutes les connexions vers la zone restante opérationnelle, tout en établissant une nouvelle connexion avec la troisième zone pour restaurer la redondance. Toutes les connexions restent confinées à la région concernée.

Si toutes les zones d'une région GCP deviennent indisponibles, les administrateurs ZTNA sont immédiatement alertés de l'incident. L'API ZTNA peut également être interrogée pour vérifier cet état.

Le service peut être rapidement restauré en basculant vers une autre région GCP. Pour cela, il convient de déployer deux sites ZTNA au même emplacement d'hébergement des applications (centre de données, IaaS, etc.). Le site A, utilisé comme site principal en conditions normales, peut être configuré pour se connecter soit à la région GCP la plus proche afin d'optimiser les performances, soit à une région spécifique pour répondre aux exigences de conformité des données. Le site B est ensuite configuré pour se connecter à une autre région GCP. Ainsi, bien que les deux connecteurs soient déployés côte à côte sur le réseau de l'organisation, chacun est relié à une région GCP distincte.

Les applications ZTNA associées à cet emplacement seront configurées pour se connecter via le connecteur du site A, tandis qu'aucune application ne sera rattachée au site B. En cas de panne, toutes les applications peuvent être reconfigurées via l'interface utilisateur ZTNA ou l'API pour se connecter au site B, qui redirigera autovmatiquement vers une région GCP disponible.

Puisque tout cela est géré en arrière-plan par le service ZTNA, aucune modification DNS n'est nécessaire et le flux de travail de l'utilisateur final reste inchangé.

- API de ZTNA: Mettre à jour l'application