FICHE TECHNIQUE

Zero Trust Device Segmentation

Protection simplifiée contre les menaces latérales pour les réseaux des sites distants, des usines et des campus

Intégrée à Zscaler Zero Trust Networking, la solution de segmentation des dispositifs, Device Segmentation, permet aux équipes informatiques de réduire les risques, d'assurer la conformité et d'améliorer le temps de fonctionnement de l'entreprise en éliminant les sources de déplacement latéral des menaces au sein des réseaux d'entreprise.

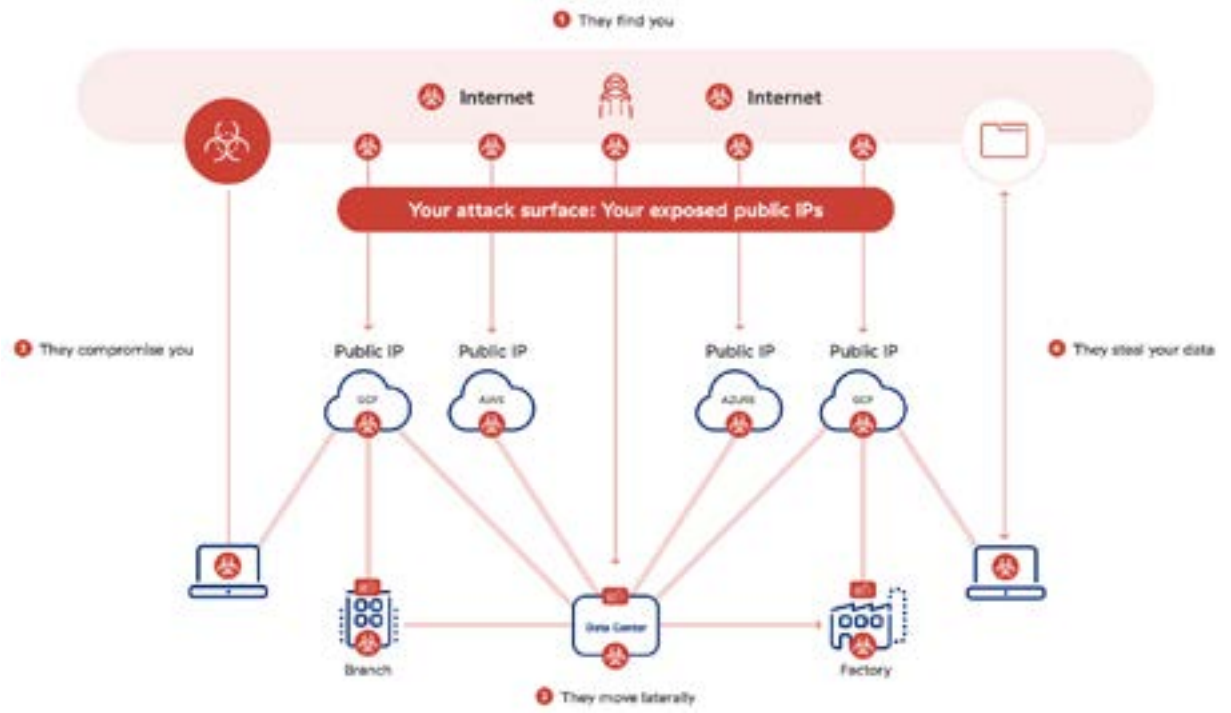
Évolution du paysage des menaces et de la conformité

Récemment, les alertes et mises en garde se sont multipliées concernant les cyberattaques initiées par des États-nations sur des infrastructures critiques aux États-Unis. Le 7 février 2024, le Federal Bureau of Investigation (FBI), la Cybersecurity and Infrastructure Security Agency (CISA), ainsi que la National Security Agency (NSA), ont lancé un avertissement àxl'intention des acteurs du service public et concernant des cybercriminels ciblant des infrastructures critiques (systèmes de transport, oléoducs et gazoducs, usines de traitement des eaux et réseaux électriques) Cette alerte vient en complément d'actions similaires prises par la Transportation Security Administration américaine (sécurisation des aéroports, des opérateurs aériens et de l'industrie ferroviaire), du récent document de référence du Département de l'Énergie des États-Unis (DoE) sur la cybersécurité et de la nouvelle version quasi définitive de la norme CIP-015-1 du NERC.

Les technologies OT/IoT ont avant tout été conçues pour assurer la vitesse et l'efficacité des transactions, la sécurité n'étant qu'un objectif secondaire. Malheureusement, les environnements OT/IoT sont désormais une cible privilégiée des cybercriminels, comme le souligne ce bond vertigineux de 400 % des attaques en un an, selon une étude de Zscaler ThreatLabz. Le ransomware constitue la stratégie d'attaque la plus populaire, et 61 % de toutes les violations visaient des entreprises connectées à l'OT.

Zscaler Zero Trust Networking

Désigne un moyen de communication plus simple, plus sûr et plus rentable pour les utilisateurs, les appareils et les workloads.



Comment se produisent les attaques de ransomware

L'EPA (Environmental Protection Agency), la CISA et le FBI recommandent fortement aux opérateurs de systèmes d'adopter une approche Zero Trust pour renforcer leur cybersécurité. Cette recommandation peut être mise en œuvre avec Zscaler grâce à sa solution Zero Trust Device Segmentation et à ses atouts :

- Réduction de l'exposition à l'Internet public
- Réduction de l'exposition aux vulnérabilités
- Segmentation du réseau
- Collecte de journaux
- Neutralisation des connexions d'utilisateurs non autorisés
- Aucun service pouvant être ciblé à partir d'Internet
- Limitation des connexions OT/IoT vers Internet
- Détection pertinente des menaces
- Inventaire des actifs OT/IT

Architecture plus sécurisée pour la segmentation des dispositifs

La segmentation a toujours été une pratique essentielle pour les réseaux, avec des outils tels que les listes de contrôle d'accès (ACL) et les pare-feu gérant le trafic entrant-sortant (client vers serveur). Cependant, la segmentation OT se focalise sur le trafic interne plus vulnérable, qui est acheminé latéralement entre les dispositifs et les workloads. Sur les VLAN mutualisés, avec une architecture de commutation traditionnelle, les dispositifs peuvent se voir et communiquer entre eux, ce qui crée un environnement propice à la propagation des malwares. Les solutions faisant appel à des agents, conçues pour les workloads cloud, ne peuvent pas segmenter les machines traditionnelles et headless, courantes dans le domaine de l'OT, tandis que les approches traditionnelles basées sur les listes ACL restent trop complexes.

Tableau de bord de Zero Trust Device Segmentation

Zscaler a introduit Zero Trust Networking pour simplifier, sécuriser et rentabiliser la communication des utilisateurs, des appareils et des workloads. Laxsegmentation des appareils est au cœur de cette approche et constitue l'étape fondamentale pour établir une visibilité et un contrôle granulaires du réseau moderne.

Zscaler simplifie la segmentation intra-VLAN grâce à une solution sans agent qui empêche toute menace de se propager latéralement en isolant chaque terminal IP, y compris les systèmes traditionnels et headless, dans un segment de réseau unique. Cette approche se substitue à la gestion complexe des listes ACL et n'implique aucune modification de l'infrastructure existante, tout en offrant une segmentation granulaire et efficace.

Cas d'utilisation

Voici les cas d'utilisation les plus courants de cette segmentation des dispositifs sans agent :

Segmentation interne du LAN
Étendez le Zero Trust au LAN en appliquant la segmentation sur le trafic est-ouest. Cette approche réduit votre surface d'attaque interne et élimine le risque de déplacement latéral au sein des réseaux OT/IoT critiques, sans recourir à une segmentation basée sur un contrôle NAC ou un pare-feu.

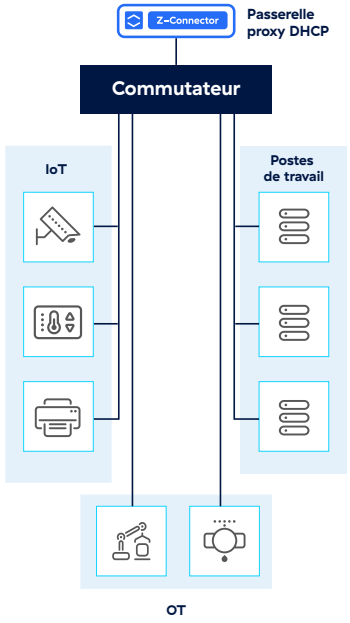
Pour appliquer une segmentation Zero Trust sur votre réseau, procédez comme suit :

- Provisionnez automatiquement chaque dispositif au sein d'un segment unique.
- Regroupez automatiquement les dispositifs, les utilisateurs et les applications en analysant leurs schémas de trafic, empêchant ainsi les dispositifs indésirables d'usurper une adresse MAC pour accéder au réseau.
- Appliquez de manière dynamique des politiques pour le trafic interne en fonction de l'identité et du contexte des utilisateurs et dispositifs.

Segmentation de l'OT

La technologie Zero Trust Device Segmentation de Zscaler agit comme un coupe-circuit anti-ransomware. Elle désactive les communications non essentielles des dispositifs pour prévenir le déplacement latéral des menaces, sans perturber les opérations de l'entreprise. Cette solution neutralise les menaces avancées telles que les ransomwares sur les dispositifs IoT, les systèmes OT et les dispositifs qui ne sont pas compatibles avec un agent logiciel.

- Regroupez et appliquez de manière autonome la politique pour les adresses MAC connues sur n'importe quel dispositif (par exemple, l'accès RDP aux caméras refusé sauf pour les administrateurs).
- Isolez automatiquement les adresses MAC inconnues pour limiter le rayon d'action d'une intrusion sur un dispositif.
- Procédez à une intégration avec les systèmes de gestion d'actifs dans le cadre de politiques de contrôle d'accès sécurisé.



Segmentation OT/IoT automatisée : segment « unique » pour chaque appareil

Identification et classification automatiques des dispositifs

Étant donné qu'une part importante du trafic OT/IoT reste sur le périmètre interne du réseau local, vous devez impérativement disposer d'une visibilité continue sur le trafic interne. Grâce à l'identification et à la classification automatiques des dispositifs, les administrateurs réseau peuvent mieux gérer les performances, le temps de fonctionnement et la sécurité des systèmes IoT/OT, sans subir une gestion complexe de l'inventaire.

Pour la visibilité sur le réseau et les dispositifs, procédez comme suit :

- Identifiez, classifiez et inventoriez les dispositifs OT/IoT sans faire appel à un agent endpoint.
- Établissez une base de référence de vos schémas de trafic et de comportements de vos dispositifs pour identifier les accès autorisés et non autorisés.
- Obtenez des informations précises sur le réseau pour gérer les performances et cartographier les menaces.

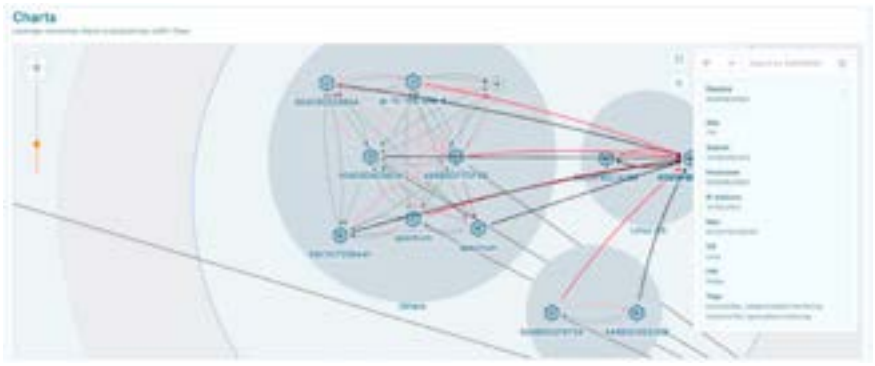
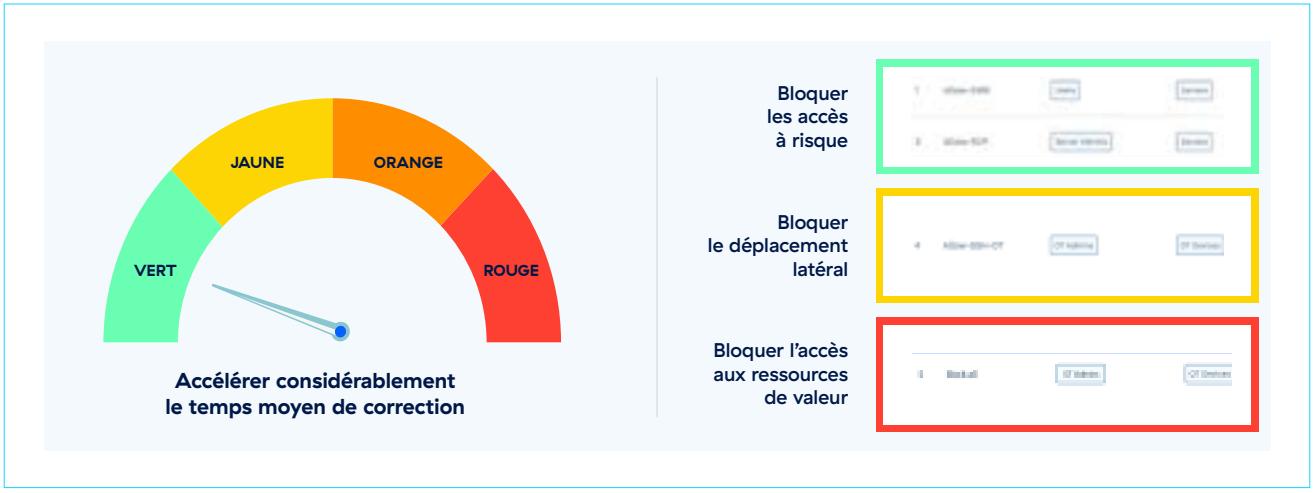


Tableau de bord de la découverte des appareils

Réponse automatisée aux incidents

Grâce au nouveau composant Zscaler Ransomware Kill Switch, entièrement intégré à la solution Zero Trust Device Segmentation, vous pouvez réduire la surface d'attaque en un clic. Verrouillez les protocoles et ports vulnérables connus, et désactivez même instantanément l'accès aux réseaux critiques, comme ceux d'une chaîne de production ou d'un hôpital, le tout avec des niveaux de gravité prédéfinis pour minimiser les temps d'arrêt de l'entreprise.

Le Ransomware Kill Switch agit comme un point d'application de politique multicouche, permettant des niveaux de réponse aux incidents en cas de compromission active, et l'augmentation de l'investissement dans les outils de sécurité existants. Chaque niveau du Ransomware Kill Switch possède des fonctionnalités similaires à des « fusibles virtuels » ou à des niveaux Defcon, avec des chemins d'escalade prédéfinis pour bloquer toutes les communications réseau inutiles ou depuis n'importe quel terminal, empêchant la propagation latérale et réduisant considérablement la surface d'attaque.



Cette solution désactive instantanément les communications non essentielles des dispositifs afin d'arrêter le déplacement latéral des menaces sans interrompre les activités de l'entreprise. Cette solution neutralise les menaces avancées telles que les ransomwares sur les dispositifs IoT, les systèmes OT et les dispositifs qui ne sont pas compatibles avec un agent logiciel.

Zscaler offre un contrôle complet du Ransomware Kill Switch via des API. Grâce à ces interfaces programmables, les entreprises informatiques peuvent activer les outils d'orchestration de la sécurité existants, tels que la gestion des informations et des événements de sécurité (SIEM), l'orchestration de la sécurité, automatisation et réponse (SOAR) ou les solutions EDR/XDR, afin d'automatiser la réponse aux incidents et de mettre immédiatement en quarantaine les terminaux compromis et contenir le rayon d'action de l'infection.

Les entreprises bénéficient ainsi d'une protection de l'investissement dans leur réseau et leur infrastructure de sécurité en place, tout en améliorant immédiatement leur posture de sécurité.

Avantages

Confinement granulaire pour limiter la propagation latérale

Réponse aux incidents pré-planifiée et automatisée dans le chaos d'une violation

Confinement strict aux couches limites clés, par exemple entre les réseaux informatiques de l'entreprise et les réseaux centraux

Arrêt progressif des ports et protocoles suspects pour maximiser la disponibilité de l'entreprise

Éliminer le déplacement latéral des menaces sur le réseau local

Réduisez la surface d'attaque en isolant chaque périphérique dans son propre réseau unique, éliminant ainsi la surface d'attaque et le risque de propagation des menaces. Même les appareils compromis ne peuvent plus infecter leurs voisins.

Réduire la complexité opérationnelle et les coûts associés aux outils de segmentation traditionnels

Segmentez chaque terminal IP sans la complexité des technologies de réseau vieillissantes et centrées sur l'IP, telles que NAC et les pare-feu internes (est-ouest), ou des constructions complexes telles que les ACL et la segmentation VLAN manuelle.

Améliorer la visibilité sur le trafic interne (est-ouest)

Grâce à la découverte et à la classification automatiques des périphériques, les administrateurs réseau peuvent mieux gérer les performances, le temps de fonctionnement et la sécurité de tous les périphériques, même ceux qui ne sont pas compatibles avec un agent.

Déploiement sans perturbation du réseau

Cette technologie sans agent se déploie rapidement sans perturber les opérations actuelles des clients et ne requiert pas de modification de l'architecture du réseau ni de réattribution des adresses IP des appareils.

Mise en conformité plus rapide

Les normes fédérales de cybersécurité dans tous les secteurs d'activité considèrent désormais la segmentation comme la pierre angulaire de Zero Trust. L'approche sans agent de Zscaler se déploie rapidement et améliore instantanément la mise en conformité.

Fonctionnalités

Isolation cloisonnée (sous air gap)

- Isolation des appareils sans agent
- Mise en quarantaine des appareils en un clic
- Détection des violations et isolation cloisonnée (sous air gap)
- Filtrage basé sur l'adresse MAC

Segmentation Zero Trust

- Segmentation basée sur le réseau

Segmentation basée sur les appareils

- Groupement et politique autonomes
- Contrôle des politiques intra-VLAN et inter-VLAN
- Politique basée sur des balises dynamiques
- Politique basée sur l'identité de l'appareil et de l'utilisateur
- Politique en fonction d'une période
- Politique par zones
- Cadre politique hiérarchique

Découverte et profilage des actifs

- Découverte des terminaux et du réseau
- Empreinte des dispositifs
- Catégorisation des appareils basée sur le profil
- Décodage des protocoles ICS/médicaux

Haute disponibilité

- Cluster à deux nœuds avec VRRP
- VRRP avec synchronisation de session
- Synchronisation de la configuration et de l'état
- Agrégation de liens
- Suivi de l'activité de l'interface
- Mises à niveau logicielles sans discontinuité
- Remplacement du matériel en service

Services de routage et de réseau

- Routage dynamique : BGP, OSPF
- Routage multicast : IGMP, PIM
- Serveur DHCP, relais/proxy
- VLAN à branche unique
- Traduction d'adresses réseau
- Routage basé sur des politiques
- Chemins multiples à coût égal (ECMP)
- VPN de site à site

Réponse aux incidents

- Ransomware Kill Switch

Visibilité et journalisation

- Carte de trafic avec corrélation des politiques
- Lac de données Elastic intégré
- Journaux d'initialisation de session pour toutes les communications au sein et entre les segments
- Exportation des journaux vers SIEM/Collecteur de journaux

Modèles de déploiement flexibles

- Provisionnement de passerelle cloisonnée (sous air gap) sans intervention
- Modèles et profils de sites
- Déploiement autonome en cluster à haute disponibilité ou en cluster multiple
- Passerelles cloisonnées (sous air gap) basées sur des machines physiques ou virtuelles

Surveillance et dépannage

- Console de débogage à distance
- CLI locale sur les passerelles cloisonnées (sous air gap)
- Prise en charge du SNMP

Gestion centralisée basée sur le cloud

- Authentification unique (SSO) et MFA
- Pistes d'audit pour les événements de connexion et les modifications de configuration
- Contrôle d'accès basé sur les rôles
- Plateforme multi-entité fournie dans le cloud
- Accès basé sur l'API

Intégrations tierces

- Microsoft Active Directory
- Intégration SIEM
- Fournisseurs EDR : Crowdstrike, SentinelOne
- Gestion d'actifs : Armis
- SSE : Zscaler ZIA

Dimensionnement de l'appliance de passerelle Zscaler

Vous trouverez ci-dessous diverses estimations de dimensionnement pour les passerelles Zscaler matérielles ou virtualisées.

Spécifications matérielles pour les déploiements de passerelles physiques						
	XS	**S1**	**S2**	**M**	**L**	**XL**
Disponibilité	Juin 2024	Juin 2024	Maintenant	Maintenant	Maintenant	1QFY25
Modèle de matériel	ZT 400	ZT 600	Dell VEP4600	Dell VEP4600	Dell VEP4600	À DÉTERMINER
UC	4C Atom	8C Atom	4C Xeon	8C Xeon	16C Xeon	16C Xeon
Mémoire	16 Go	16 Go	16 Go	32 Go	64 Go	64 Go
Stockage	64 Go	64 Go	128 Go	256 Go	960 Go	256 Go
Ports	4x 1 GbE	4x 1 GbE	6x 1 GbE 2x 1 GbE (SFP)	4x 1 GbE 2x 10 GbE	4x 1 GbE 6x 10 GbE	4x 25 GbE
Facteur de forme	Bureau	Bureau	1U	1U	1U	1U
Autres caractéristiques	Sans ventilateur		RPS	RPS	RPS	RPS
Débit (HTTP 64 Ko)	4 Gbit/s	8 Gbit/s	10 Gbit/s	20 Gbit/s	40 Gbit/s	80 Gbit/s
Sessions	250 000	500 000	500 000	1 M	2 M	2 M
Nombre de terminaux	200	500	1	2 000	4 000	À DÉTERMINER

Guide de dimensionnement des appliances virtuelles				
	XS	**S1**	**S2**	**M**
Disponibilité	Maintenant	Maintenant	Maintenant	Maintenant
UC	2 vCPU	4 vCPU	8 vCPU	16 vCPU
Mémoire	8 Go	16 Go	32 Go	64 Go
Stockage	256 Go	256 Go	256 Go	256 Go
Ports	4x vNIC	4x vNIC	4x vNIC	4x vNIC
Débit (HTTP 64 Ko)	5 Gbit/s	10 Gbit/s	20 Gbit/s	40 Gbit/s
Sessions	250 000	500 000	1 M	2 M
Nombre de terminaux	200	500	2 000	4 000

Contacter un expert technique

Vous souhaitez en savoir plus sur la manière dont Zscaler peut aider à protéger l'infrastructure critique de votre entreprise ? Prenez rendez-vous avec l'un de nos experts techniques.

zscaler™ | Experience your world, secured.™

À propos de Zscaler
Zscaler (NASDAQ : ZS) accélère la transformation numérique pour améliorer l'agilité, l'efficacité, la résilience et la sécurité de ses clients. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et les pertes des données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quel que soit leur emplacement. Distribué dans plus de 150 data centers dans le monde, Zero Trust Exchange, basé sur le SASE, constitue la plus grande plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur **zscaler.com/fr** ou suivez-nous sur Twitter **@zscaler**.

+1 408 533 0288 Zscaler, Inc. (siège) • 120 Holger Way • San Jose, CA 95134 zscaler.com/fr