Switch

Switch LAN SCION Access

Factsheet

Davantage de sécurité, de fiabilité et de contrôle: grâce à Switch LAN SCION Access, vous créez les conditions idéales pour que vos données ne soient transférées sur Internet que là où vous le souhaitez.

L'architecture Internet sécurisée nouvelle génération

La numérisation exige aujourd'hui plus que jamais des réseaux sécurisés et faciles à contrôler. Toutefois, les fondements d'Internet datent du siècle dernier. Il a été développé sans mécanismes de sécurité particuliers et n'a guère été retravaillé depuis. Et cela le rend vulnérable. Les cybercriminels exploitent aujourd'hui les failles à tel point que la prévention et l'élimination des cybermenaces au sein des entreprises sont désormais des défis informatiques prédominants. Ce constat concerne non seulement les nombreux risques de sécurité, mais aussi les aspects liés au réseau de transport.

Par conséquent, il est grand temps que les choses évoluent. SCION (Scalability, Control, and Isolation On Next-Generation Networks) apporte précisément cette mise à niveau. Switch LAN SCION Access combine les facteurs de sécurité, de fiabilité et de contrôle des réseaux privés avec la flexibilité de l'Internet public. Cette technologie a été mise au point à l'École polytechnique fédérale de Zurich (EPFZ). Switch accompagne le développement de SCION à l'EPF de Zurich depuis 2015 déjà.

Vos avantages

Security by Design

Switch LAN SCION Access vous protège contre les cyberattaques telles que le détournement de préfixe ou certaines attaques DDoS

Nouvelles fonctions de sécurité

Path Control et Path Verification

Path Control

Vous définissez les réseaux que vos données ne sont pas autorisées à quitter. Vous déterminez l'itinéraire emprunté par vos paquets de données

Path Verification

Le chemin et l'intégrité de tous les paquets sont sécurisés par cryptographie et vérifiables

Multipathing

Transmission simultanée fiable des données via plusieurs chemins d'accès réseau

Cybersécurité

Plus de détournement possible de vos données pendant la transmission; protection contre lesattaques DDoS par réflexion

Isolation domains

trust limité aux participants d'un ISD (plus de trust-roots globaux)

Degré élevé de sécurité contre les défaillances

L'architecture de SCION vous offre un degré élevé de sécurité contre les défaillances grâce à diverses caractéristiques et à des concepts novateurs. Cela permet d'éviter certaines attaques en amont: SCION est immunisé contre le détournement de préfixe. Qui plus est, cette technologie limite le risque d'attaques par déni de service distribué (Distributed Denial of Service – DDoS) grâce à des chemins d'accès cachés et à l'authentification de la source. La protection contre l'usurpation d'adresse rend même les attaques DDoS par réflexion totalement impossibles.

Fiabilité et performance grâce au multipathing

Avec le multipathing, le protocole de SCION ouvre plusieurs options de chemins d'accès utilisables simultanément. Cela augmente la capacité utilisable sur le réseau et permet une commutation plus rapide en cas de défaillance du chemin d'accès, à condition que l'application prenne en charge cette fonction.

La granularité du choix du chemin d'accès se limite aux points de transfert entre les réseaux (systèmes autonomes). Le chemin d'accès au sein d'un réseau n'est pas soumis au contrôle de SCION, de sorte qu'il est impossible d'y utiliser des chemins alternatifs.

SCION permet un meilleur contrôle

SCION vous procure un contrôle sur le chemin d'accès emprunté par votre communication de bout en bout. Cela vous permet d'éviter certaines parties du réseau, par exemple les réseaux situés dans des régions peu sûres. Le contrôle du choix du chemin d'accès permet également de sélectionner la bande passante disponible et les temps de latence. De cette manière, vous augmentez la sécurité du traitement de vos données. Vous disposez d'un meilleur contrôle sur l'itinéraire emprunté par vos données sensibles.

Sécurité

Tous les chemins d'accès sont authentifiés et protégés contre les attaques de routage.

Stabilité

Plusieurs chemins d'accès réseau avec basculement instantané garantissent que les défaillances de chemins d'accès individuels passent inaperçues.

Contrôle

Vous contrôlez l'itinéraire de vos données jusqu'à leur destination.

Protection

Les chemins cachés et la sélection du chemin contrôlée par l'expéditeur renforcent la protection contre les attaques DDoS.

Performance

Une application SCION peut sélectionner les meilleurs chemins d'accès pour le trafic réseau selon des règles de coût ou de latence.

La technologie de SCION

L'Internet d'aujourd'hui est constitué d'une myriade de réseaux interconnectés de manière peu structurée. Et c'est la communication entre les différents réseaux qui rend la transmission vulnérable au détournement d'itinéraire. Un paquet de données peut ainsi être détourné à travers plusieurs pays sur son trajet de Zurich à Genève sans que l'expéditeur ni le destinataire ne puissent l'empêcher. De tels détournements sont souvent découverts avec un certain retard.

Les cybercriminels peuvent rediriger des paquets de données ou désactiver des services web avec des attaques DDoS. C'est précisément là qu'intervient SCION, en minimisant en amont la surface d'attaque au niveau du réseau.

Une équipe de l'EPF de Zurich a repensé de fond en comble l'architecture Internet de SCION. La base du système est formée par ce que l'on appelle des domaines d'isolement (ISD). Ces domaines peuvent être des États, des secteurs industriels ou des entreprises opérant de manière autonome. SCION regroupe plusieurs réseaux dans des ISD, par exemple selon des critères géographiques. Par exemple, tous les réseaux suisses peuvent appartenir à un ISD. La communication entre deux réseaux appartenant à un même ISD ne le quitte jamais. Les données confidentielles ne peuvent donc plus être détournées de manière incontrôlée via d'autres parties du réseau.

Avec SCION, l'expéditeur détermine l'itinéraire des paquets de données, ce qui rend systématiquement impossible les attaques au niveau du routage. Vous pouvez par exemple spécifier que certains fournisseurs ou pays doivent être évités.

Actuellement, le protocole SCION est encore en cours de développement. La spécification n'est pas encore standardisée officiellement et publiquement. L'équipe de développement de l'EPF s'efforce de parvenir à cette standardisation.

Prestations

Switch LAN SCION Access

Cette variante est votre connexion SCION au cœur SCION de Switch LAN (CH-ISD, sans services Edge). Dans ce cas, il vous appartient, en tant que client, de vous procurer et d'exploiter le routeur SCION. Ce dernier peut nécessiter l'acquisition d'une licence logicielle, selon le fournisseur.
Si vous ne disposez pas encore d'une connexion au backbone de Switch LAN, par exemple parce que vous utilisez le service IP Access ou L2VPN, nous nous ferons un plaisir de vous proposer une offre personnalisée.

Switch LAN SCION Edge

La prestation Managed Service constitue un complément optionnel à Switch LAN SCION Access et sert à l'exploitation de votre routeur et de votre connexion SCION (SCION Edge: passerelle IP de SCION).

Contactez-nous

Daniel Bertolo

Head Network

daniel.bertolo@switch.ch
+41 44 268 15 87

Avez-vous des questions? Nous nous ferons un plaisir de vous présenter la nouvelle génération d'architecture Internet.

Switch LAN SCION Access vous intéresse? Appelez-nous ou envoyez-nous un message. Nous vous conseillons avec compétence et engagement, en nous concentrant sur vos besoins individuels.

Diego Tres

Community Account Manager

diego.tres@switch.ch
+41 79 310 48 52

Zurich

Werdstrasse 2
8004 Zurich

info@switch.ch

Lausanne

EPFL Innovation Park
Bâtiment I
1001 Lausanne
info@switch.ch

Linkedin

Website

Newsletter