

LIVRE BLANC

La technologie SCION: Transformation et optimisation de votre connectivité internationale

Ce document résume les résultats du test par Swisscom de la technologie SCION pour une connectivité internationale optimisée à l'avenir.

Résumé

L'Internet tel que nous le connaissons aujourd'hui est dépassé. Aucune mise à jour ou amélioration majeure n'ayant eu lieu depuis les années 90, il est devenu une cible facile pour les cybercriminels. Pourtant, et malgré ses défauts, l'Internet est encore largement utilisé par les gouvernements, les entreprises et les particuliers pour transmettre chaque jour des informations hautement sensibles.

La numérisation de notre monde nous a rendus dépendants de l'Internet, non seulement comme moyen de communication, mais aussi comme pilier fondamental d'un mode de vie moderne.

Les communications internationales dépendent fortement de l'Internet public. Les informations critiques, les actifs numériques et les interactions sont essentiels aujourd'hui – mais ils sont aussi inefficaces. Les lignes MPLS point à point longue distance sont coûteuses, et manquent de la flexibilité requise

dans un monde des affaires qui évolue rapidement. Elles retirent le contrôle à l'expéditeur des données, ce qui rend la ligne de communication vulnérable. Le protocole SCION est une alternative efficace et efficiente à l'Internet traditionnel, offrant de nombreux avantages qui dépassent les attentes actuelles en matière de connectivité.

Swisscom, la principale société de services de télécommunications en Suisse, fournit non seulement des services Internet à ses clients au niveau local, mais assure également la connectivité internationale des clients basés en Suisse. Les défis actuels auxquels sont confrontés les utilisateurs de l'Internet public en matière de sécurité, de flexibilité et de performance, ainsi que le fait d'être un fervent promoteur de l'amélioration de la sécurité de l'Internet, ont conduit Swisscom à soutenir la recherche et le développement du protocole SCION. Swisscom a en outre réalisé des preuves de concept (PoC) afin de présenter les avantages des technologies à ses clients.

Dans le présent livre blanc, Swisscom, en étroite collaboration avec Anapaya Systems AG et InterCloud, présente un résumé des résultats de la connectivité internationale à l'aide du protocole SCION. La présente démonstration de faisabilité a pour but d'étudier et de valider l'effet de la technologie SCION sur les futures communications internationales par le biais de l'Internet public.

La connectivité d'aujourd'hui, la solution de demain

Les problèmes de l'Internet public d'aujourd'hui trouvent leur origine dans l'approche même qui l'a rendu possible. Le protocole BGP (Border Gateway Protocol) permet d'acheminer le trafic sur l'Internet. Il a été conçu pour s'auto-corriger, en sélectionnant les itinéraires les plus rapides possibles pour connecter les utilisateurs.

Le BGP crée essentiellement une carte de toutes les destinations sur l'Internet. Extrêmement simplifié, il a 4 fonctions:

1. Créer une connectivité avec les systèmes voisins (poignée de main TCP).
2. Partager les destinations accessibles avec les voisins
3. Surveiller les changements et les voisins inaccessibles
4. Mettre à jour la carte Internet (tables de routage)

Cependant, le protocole BGP n'a pas été conçu avec la sécurité comme motivation principale et peut facilement être exploité par des individus peu scrupuleux. Le protocole BGP a fait l'objet de milliers de configurations erronées et d'attaques, dont certaines ont rendu l'Internet inaccessible.

- D'autres ont acheminé un trafic ciblé vers des endroits non désirés à des fins malveillantes. Des efforts ont été faits pour sécuriser le protocole BGP (par exemple, BGPsec). Cependant, la plupart d'entre eux reposent sur la mise à jour de l'infrastructure actuelle et le déploiement complet des changements, ce qui nécessite la coopération d'autres parties, raison pour laquelle le protocole BGP n'est toujours pas aussi sûr qu'il devrait l'être.

Avec les communications internationales entre les entreprises, les succursales et les fournisseurs de services Cloud à travers le monde, il n'est pas possible de gérer la destination du trafic, un point crucial dans le monde d'aujourd'hui où nous sommes obligés de nous conformer aux lois sur la protection de la vie privée.

SCION est une technologie innovante recherchée et développée à l'ETH Zürich, en Suisse. L'une des principales caractéristiques du nouveau protocole SCION est la possibilité pour les utilisateurs d'envoyer du trafic sur Internet avec contrôle, confiance et vérification. Pour les communications internationales entre les entreprises ou les succursales, cette fonction pourrait être la clé pour atténuer les défis actuels tout en respectant les lois sur la protection de la vie privée. Avec une connectivité internationale basée sur SCION, un administrateur de réseau peut prendre des décisions en amont sur la manière dont le trafic sera acheminé au lieu de compter sur d'autres parties pour acheminer le trafic en toute sécurité ou, pour aller encore plus loin, l'administrateur peut délibérément faire correspondre la connectivité internationale basée sur SCION aux besoins d'une certaine application.

Dans nos tests de validation du concept présentés ci-dessous, nous avons mis SCION à l'épreuve par rapport au protocole Border Gateway.

PoC – Connectivité internationale basée sur SCION

Mise en scène

Énoncé du problème

Lorsque l'Internet a été conçu, l'accent a été mis sur l'ouverture et l'évolutivité de la technologie. La sécurité n'était pas une priorité, et des failles de sécurité dans le routage du trafic existent toujours dans le protocole BGP. L'un de ces exemples a conduit à un incident en 2019, où le trafic européen a été redirigé vers la Chine, où une inspection du trafic et une fuite de données ont eu lieu.

Dans le monde d'aujourd'hui, où l'information numérique est essentielle au développement des entreprises et des gouvernements, ce scénario est inacceptable et pourtant trop courant. Nous voulions trouver un moyen de renforcer la sécurité de l'Internet public afin d'éviter les incidents décrits ci-dessus.

En mettant en œuvre le protocole SCION sur une connectivité internationale, nous sommes convaincus de pouvoir renforcer la sécurité et d'obtenir un meilleur contrôle sur la manière dont les données sont transférées vers l'Internet public.

Swisscom Cloudlab Ltd.

Swisscom Cloudlab Ltd. est basé à Palo Alto (près de San Francisco, États-Unis) et est une succursale (Outpost) de Swisscom (Suisse) AG. Cette petite équipe travaille sur des sujets innovants et recherche de nouvelles technologies pour le compte de Swisscom. Disposant d'un centre de données de test local, l'Outpost de Swisscom peut également valider de nouvelles piles et versions de logiciels de partenaires de Swisscom tels que VMware. Cette flexibilité fait de l'Outpost un endroit idéal pour exécuter des PoC de nouvelles solutions dans les domaines de l'IoT, de la sécurité, des telco, de l'analyse de données, de l'informatique confidentielle et de l'expérience utilisateur.

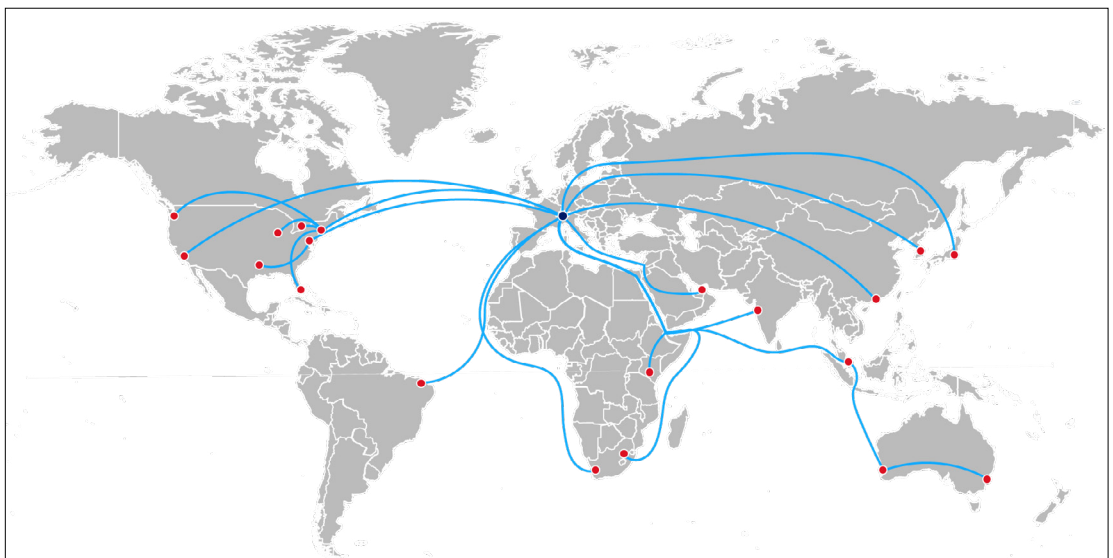
La dorsale (backbone) Internet internationale IP-Plus® Business de Swisscom

Pour servir les clients basés en Suisse, Swisscom entretient une dorsale Internet mondiale qui est directement connectée à des IXP essentiels. Grâce à cette dorsale mondiale, les clients de Swisscom bénéficient de liaisons directes, de grande capacité et entièrement contrôlées dans le monde entier.

En outre, Swisscom exploite ses propres nœuds de réseau internationaux qui surveillent et contrôlent directement le trafic IP. Les nœuds de réseau filtrent le trafic non autorisé localement plutôt qu'en Suisse, réduisant ainsi le changement de la montée de la cybercriminalité.



Aperçu de la dorsale Internet internationale IP-Plus® de Swisscom en Europe



Aperçu de la dorsale Internet IP-Plus® de Swisscom dans le monde

InterCloud

InterCloud est un fournisseur de premier plan de Software-Defined Cloud Interconnect (SDCI), qui fournit des services gérés sécurisés et de bout en bout à certaines des plus grandes organisations au monde. La plateforme d'InterCloud, centrée sur les API, aide les entreprises à simplifier et à accélérer l'exploitation du réseau, avec un haut niveau de performance et de transparence pour les ressources de l'entreprise réparties sur plusieurs sites et chez différents fournisseurs de cloud.

InterCloud utilise SCION pour alimenter sa connectivité Cloud et a été utilisé dans la comparaison en raison de la connectivité Cloud qui devient la norme dans les entreprises. SCION et ses capacités de réseau régulières, ce fournisseur constitue un bon partenaire de test pour les besoins de la démonstration de faisabilité.

Anapaya Systems AG

Anapaya Systems AG est une société suisse dont l'objectif est de construire un écosystème international fournissant des services basés sur SCION pour une expérience de réseau plus fiable, plus sûre et plus stable. Fournisseur commercial de SCION, ses solutions offrent aux organisations du monde entier un moyen de transporter des données commerciales critiques de manière sécurisée et transparente à travers le réseau, en envoyant des informations entre les sites de l'entreprise, les partenaires de confiance et les fournisseurs de cloud.

Une comparaison sera faite entre la connectivité Internet moderne et la solution SCION d'Anapaya.

Le protocole SCION

Le protocole SCION a fait l'objet de recherches et a été développé à l'université ETH Zürich (Suisse), une technologie innovante de routage inter-domaines pour contrôler l'acheminement du trafic en toute confiance. Le protocole SCION établit un chemin sécurisé de bout en bout, de la source à la destination, tout en assurant la confiance entre chaque saut sur le chemin. Le protocole SCION peut arrêter complètement le détournement BGP et protéger contre d'autres attaques provenant d'Internet (telles que les attaques DDoS).

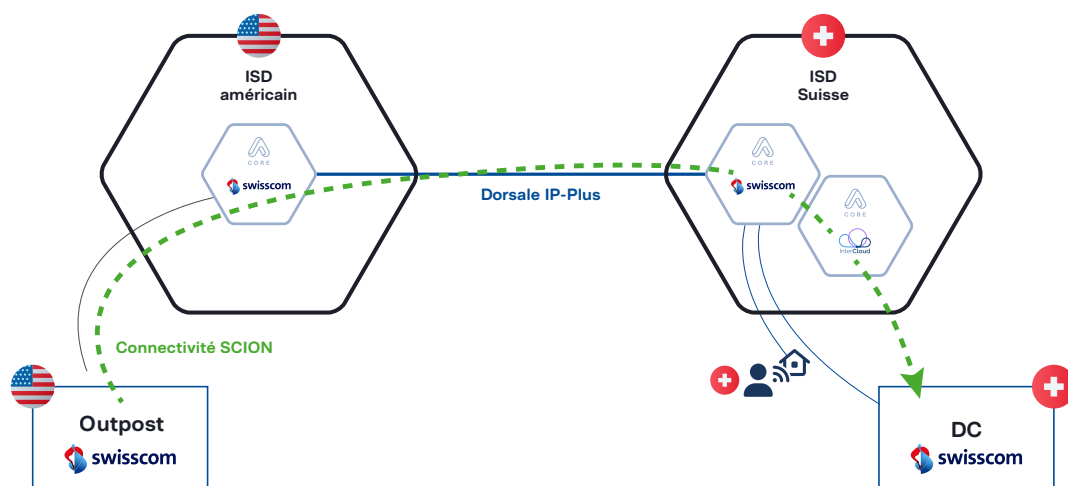
Dans le cadre de notre démonstration de faisabilité, le protocole SCION sera directement comparé à la connectivité Internet traditionnelle. Il a été estimé que SCION serait en mesure de fournir une connectivité supérieure à celle de l'Internet tel que nous le connaissons.

Environnement du PoC

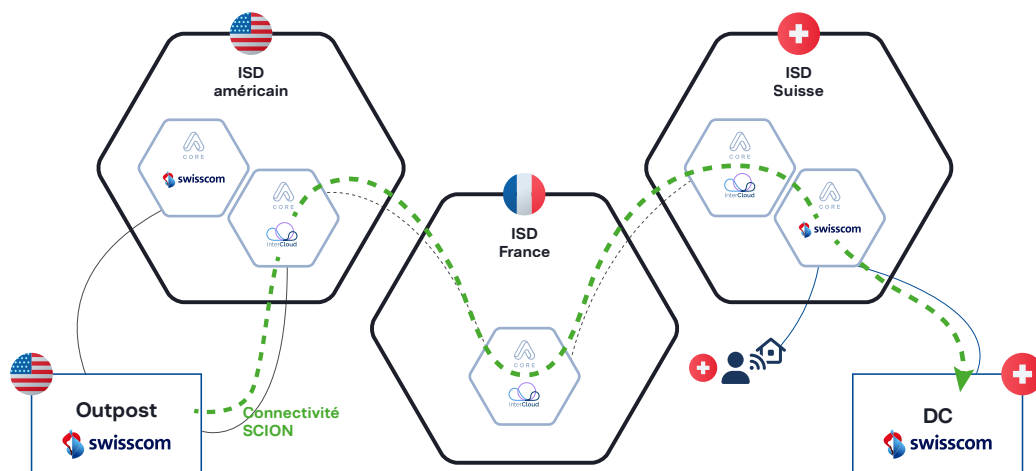
La connexion SCION est comparée au trafic envoyé par la connexion traditionnelle, autrement dit l'Internet public basé sur le protocole IP.

Pour présenter les avantages du protocole SCION sur une connectivité internationale via l'Internet public, nous avons mis en place deux connexions SCION:

1. Connexion IP-Plus de Swisscom activée par SCION



2. Dorsale InterCloud activée par SCION



La connectivité SCION entre l'Outpost de Swisscom (San Francisco) et le siège en Suisse envoie la même quantité de données productives que la connexion traditionnelle. Nous utilisons cette transmission pour comparer les performances, l'utilisation de la bande passante et le contrôle de chaque réseau.

Résultats du test PoC

Nous avons utilisé l'environnement ci-dessus pour effectuer nos tests, en utilisant trois paramètres d'évaluation:

- Capacités de basculement
- Temps de latence
- Connectivité parallèle

Dans cette documentation, une « connectivité SCION » fait référence au temps mesuré en millisecondes (m) qu'il faut à un paquet pour atteindre (la destination) à partir de (l'origine).

Test de basculement:

Le Clouddlab de Swisscom Outpost a effectué un test de basculement avec Anapaya Systems AG de la connectivité SCION en mars 2022.

Scénario du test:

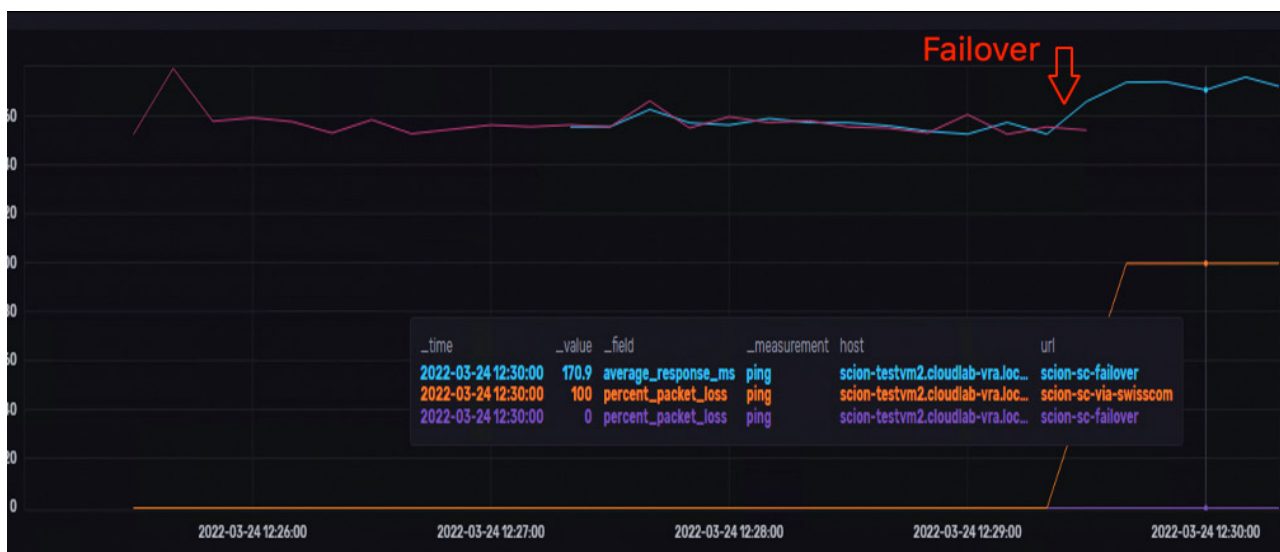
Test du chemin de basculement sur deux réseaux SCION différents:

1. Californie (États-Unis) vers Berne (Suisse) sur une connectivité IP-Plus activée par Swisscom SCION.
2. Californie (États-Unis) vers Paris (France) via la dorsale SCION d'InterCloud.

Résultats du test:

La capture d'écran présentée ci-dessous montre que le chemin de basculement répondait aux demandes de ping et n'a pas laissé tomber de paquets pendant un test de basculement.

De plus, les captures d'écran ci-dessous montrent comment les politiques peuvent être configurées pour personnaliser la pondération ou la sélection des chemins de connectivité.



Ligne rouge: mesure la connectivité SCION de Swisscom Cloudlab (Californie) à Swisscom (Berne) configurée pour utiliser la dorsale de Swisscom.

Ligne bleue: mesure la connectivité SCION entre Swisscom Cloudlab (Californie) et Swisscom (Berne) configurée pour utiliser la dorsale de Swisscom (préférée) et la dorsale d'InterCloud (secondaire)..

Ligne orange: mesure le nombre de demandes de ping perdues lors de l'utilisation de la dorsale de Swisscom pour aller de Swisscom Cloudlab (Californie) à Swisscom (Berne).

Ligne violette: mesure le nombre de demandes de ping perdues lors de l'utilisation de la dorsale de Swisscom (préférée) ou d'InterCloud (secondaire) pour aller de Swisscom Cloudlab (Californie) à Swisscom (Berne).

Résumé:

La ligne bleue du graphique passe soit par la dorsale d'InterCloud, soit par celle de Swisscom, et répondait constamment aux pings pendant le test de basculement. Pendant le test de basculement, la connectivité a été basculée de manière transparente du chemin passant par le réseau de Swisscom au chemin passant par le réseau d'InterCloud.



Ligne rouge: mesure la connectivité SCION de Swisscom Cloudlab (Californie) à InterCloud (Paris) configurée pour utiliser la dorsale d'InterCloud (pas de changement de politique pendant le test).

Ligne bleue: mesure la connectivité SCION entre Swisscom Cloudlab (Californie) et InterCloud (Paris) configurée pour utiliser la dorsale de Swisscom (avant la modification de la politique) et plus tard pour utiliser la dorsale d'InterCloud (après la modification de la politique).

Ligne orange: mesure le nombre de demandes de ping perdues lors de l'utilisation de la dorsale d'InterCloud (après modification de la politique) pour aller de Swisscom Cloudlab (Californie) à InterCloud (Paris).

Ligne violette: mesure le nombre de demandes de ping perdues lors de l'utilisation de la dorsale de Swisscom (avant la modification de la politique) pour aller de Swisscom Cloudlab (Californie) à InterCloud (Paris).

Modifications de la politique avec contrôle du chemin:

La ligne bleue était précédemment configurée pour emprunter le chemin le plus long via Swisscom (Berne) pour atteindre la destination d'InterCloud (Paris) ; après modification de la configuration, la ligne bleue a emprunté le chemin le plus rapide via le chemin d'InterCloud jusqu'à Paris.



Modifications de la politique et tests de basculement avec pondération des chemins:

De manière similaire au cas de test ci-dessus, la ligne rouge privilégiait le chemin passant par le réseau de Swisscom vers Swisscom (Berne), qui est naturellement plus rapide, tandis que la ligne bleue était configurée pour privilégier le chemin passant par le réseau de Swisscom vers InterCloud (Paris), qui est naturellement plus lent. Les deux chemins sont passés par le réseau d'InterCloud dès que le chemin de Swisscom a été rendu manuellement indisponible jusqu'à ce que le réseau de Swisscom soit à nouveau disponible (croisements de lignes).

Test de latence

Swisscom Cloudlab et Anapaya Systems AG ont analysé les performances du réseau de la connectivité internationale activée par SCION sur une période de deux mois.

Outils:

InfluxDB et Telegraf ont été utilisés pour collecter les indicateurs.

Scénario du test:

Test de la connectivité de Swisscom Cloudlab (Palo Alto, Californie) vers Berne et Paris sur 6 chemins et configurations de réseau différents:

1. De la Californie (États-Unis) à Berne (Suisse) via la connectivité IP-Plus de Swisscom, compatible équipé de SCION.
2. De la Californie (États-Unis) à Berne (Suisse) via la dorsale SCION d'InterCloud.
3. De la Californie (États-Unis) à Berne (Suisse) via l'Internet public
4. De la Californie (États-Unis) vers Paris – InterCloud (France) sur l'IP-Plus de Swisscom équipé de SCION
5. De la Californie (États-Unis) à Paris – InterCloud (France) sur la dorsale SCION d'InterCloud
6. De la Californie (États-Unis) à Paris – InterCloud (France) sur l'Internet public

Stipulations:

Comme il n'y a pas de passerelle SCION directe vers le centre de données de Swisscom Cloudlab en Californie, la connectivité SCION assurera toujours le dernier kilomètre sur l'Internet.

Pour cela, nous avons ajouté deux destinations supplémentaires sur lesquelles nous avons collecté des indicateurs :

- Dernier kilomètre (Internet) en utilisant le point d'extrémité SCION de Swisscom.
- Dernier kilomètre (Internet) en utilisant le point d'extrémité SCION d'InterCloud.

Cela devrait vous donner une meilleure idée de la façon dont les routes individuelles se comportent en cas de surtensions et de gigue sur Internet. La latence est mesurée en temps de réponse (ms).

Constatation 1 - Pendant la gigue Internet

L'exemple ci-dessous révèle que la connectivité SCION est également affectée par la gigue (pic de temps de réponse) observée au niveau du dernier kilomètre (localement vers le centre de données en Californie).



Ligne orange: mesure le temps de réponse entre Swisscom Cloudlab (Californie) et InterCloud (Paris) sur la dorsale de Swisscom (SCION activé).

Ligne bleue: mesure le temps de réponse entre Swisscom Cloudlab (Californie) et InterCloud (Paris) sur la connectivité Internet.

Ligne violette: mesure le temps de réponse de la « dernière ligne » (Internet) entre Swisscom Cloudlab (centre de données) et Anexia-IT (fournisseur de services disposant de routeurs SCION en Californie).

Constatation 2 - Autres

Le test est conditionné par l'absence de routeur SCION dans le centre de données Sunnyvale de Swisscom Cloudlab, ce qui oblige les deux chemins SCION (routeurs Swisscom et InterCloud) à

passer par Los Angeles (routeur Anexia-IT) avant de poursuivre un chemin optimal vers l'avant. Il est impossible de soustraire confortablement le « dernier kilomètre », mais il faut plutôt conclure que SCION est au même niveau que l'Internet en ce qui concerne le temps de latence.

Connectivité parallèle

Swisscom Cloudlab et Anapaya Systems AG ont mis en place une configuration dans laquelle le trafic était envoyé sur deux chemins différents, mais avec la même source et la même destination.

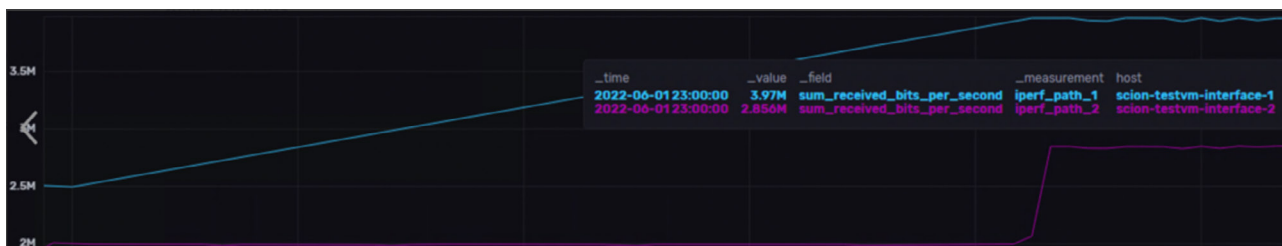
Scénario du test:

Valider que le trafic peut être envoyé sur deux chemins simultanément et valider que le trafic peut être contrôlé individuellement (débit et itinéraires).

1. De la Californie (États-Unis) à Berne (Suisse) via le réseau IP-Plus de Swisscom équipé de SCION.
2. De la Californie (États-Unis) à Berne (Suisse) via la dorsale SCION d'InterCloud.

Résultats du test:

Dans les graphiques ci-dessous, nous voyons comment les indicateurs des deux connexions changent en modifiant le débit (de : 2 Mo/s et 2,5 Mo/s, à : 3 Mo/s et 4 Mo/s).



Vous trouverez ci-dessous un ensemble d'indicateurs des deux chemins avec une dérivation, très probablement liée à l'interférence du dernier kilomètre:



Constatations:

Les scénarios de test et l'infrastructure ne sont pas idéaux pour déterminer si la connectivité Internet ou la connectivité basée sur SCION est plus rapide. Cependant, ils montrent la souplesse de configuration que l'on peut obtenir avec SCION en ce qui concerne le contrôle des routes et du trafic.

Conclusion

Swisscom a entrepris de créer un environnement PoC pour montrer et prouver que la technologie SCION est supérieure à l'Internet traditionnel pour la connectivité internationale.

La conclusion du PoC que nous avons réalisé est la suivante:

1. Il peut être difficile de comparer les vitesses de l'Internet traditionnel. Cependant, la collecte d'indicateurs sur une longue période montre que SCION est plus stable en général et qu'il est au moins à la hauteur de la vitesse d'Internet.

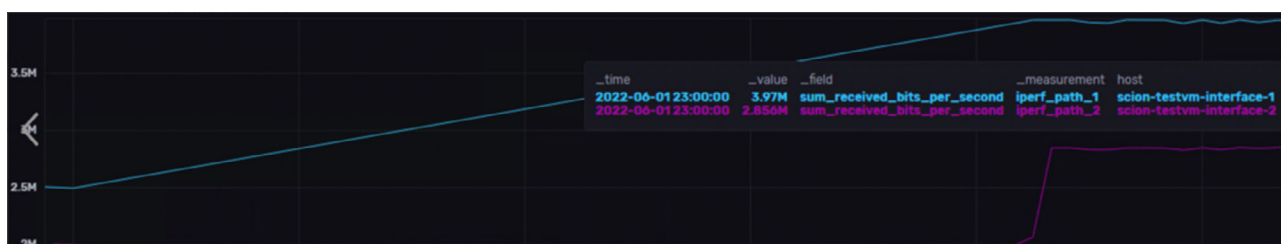
Mais le PoC ne peut pas conclure ou infirmer cela pour diverses raisons (charge, matériel dédié, portée, connectivité du dernier kilomètre).

Ce qui a été confirmé pendant le PoC et validé, c'est que SCION et BGP peuvent coexister. La présence de routeurs SCION dans la dorsale permet d'activer SCION et de transmettre les paquets à l'Internet normal (BGP) en tant que dernier kilomètre, et vice versa

2. SCION kann auf verschiedene Arten konfiguriert werden, um:

- » **Inclure ou exclure les chemins d'acheminement** – Ceci peut être utilisé pour éviter certaines juridictions et se conformer aux déclarations de confidentialité.
- » **Envoyer le trafic sur deux chemins différents en parallèle avec la même source et la même destination** – Ceci n'est pas possible avec BGP à l'échelle mondiale et peut théoriquement augmenter le débit.
- » **Restreindre le débit d'un chemin donné** – Une autre configuration que BGP ne peut pas prendre en charge
- » **Mettre en place des décisions de basculement en amont** – permettant le basculement instantané du chemin. Alors que BGP ferait tomber les paquets jusqu'à ce qu'une tâche programmée soit exécutée pour mettre à jour les tables de routage.

L'image ci-dessus illustre cette situation : Configuration du chemin, limitation du débit 2.) L'envoi de trafic sur deux chemins en même temps)





Ligne rouge: mesure la connectivité SCION de Swisscom Cloudlab (Californie) à InterCloud (Paris) configurée pour utiliser la dorsale d'InterCloud.

Ligne bleue: mesure la connectivité SCION entre Swisscom Cloudlab (Californie) et Intercloud (Paris) configurée pour utiliser la dorsale d'InterCloud (préférée) et celle de Swisscom (secondaire).

Ligne orange: mesure le nombre de demandes de ping perdues lors de l'utilisation de la dorsale d'InterCloud (la connectivité est devenue instable).

Ligne violette: mesure le nombre de demandes de ping qui ont été perdues lors de l'utilisation de la dorsale de Swisscom pour aller de Swisscom Cloudlab (Californie) à InterCloud (Paris).

L'image ci-dessus représente un test de basculement avec basculement instantané sur le chemin secondaire après que le chemin préféré soit devenu instable (interférence manuelle).

À propos de Swisscom

Swisscom est la principale entreprise de télécommunications et l'une des principales entreprises informatiques de Suisse. La division Swisscom Enterprise Customers est le plus grand fournisseur intégré de TIC pour les grands clients en Suisse. Swisscom est résolument orientée vers les besoins des clients, se concentre sur le service et la qualité et investit massivement dans les réseaux de l'avenir.

Le réseau de demain est virtualisé, omniprésent et sécurisé avec des performances élevées. Le réseau mondial entre les personnes, les organisations, les machines et les objets est le moteur le plus important du développement moderne, économique et social. Swisscom propose donc des solutions complètes pour le travail mobile et la téléphonie, des solutions sécurisées pour les réseaux d'entreprise, l'Internet et la téléphonie, ainsi que des solutions de réseau globales en collaboration avec ses partenaires. Swisscom s'intéresse de près à l'amélioration de la sécurité des communications sur Internet, propose la technologie SCION à ses clients et continue à soutenir activement le développement de cette technologie.

À propos d'Anapaya Systems

Anapaya Systems, une entreprise dérivée de l'ETH Zürich, développe et soutient une mise en œuvre industrielle de SCION et construit l'Internet SCION, l'écosystème international de fournisseurs de services utilisant ce protocole.

La cybercriminalité étant en hausse et les incidents individuels coûtant aux entreprises et aux fournisseurs de services des dizaines de millions de dollars à résoudre, le moment est venu de franchir la prochaine étape de l'évolution de l'Internet.

Anapaya et ses partenaires fournisseurs de services offrent aujourd'hui l'Internet de la prochaine génération : fiable, sécurisé et digne de confiance. Les multinationales, les industries réglementées telles que les services financiers, les soins de santé, les secteurs publics et d'autres industries peuvent maintenant reprendre le contrôle réel de la destination de leurs données sensibles et de la manière dont elles y parviennent.

À propos d'InterCloud

InterCloud est un fournisseur leader de Software-Defined Cloud Interconnect (SDCI) qui transforme la connectivité mondiale, réduit la complexité des réseaux et accélère la croissance et l'innovation pour les entreprises mondiales – en toute sécurité, rapidement et facilement. Sa plateforme de connectivité mondiale de bout en bout élimine la complexité du déploiement du cloud, donnant aux entreprises un contrôle total sur la sécurité, la souveraineté et la performance de leur trafic de données critiques, en toute tranquillité d'esprit. La plateforme de l'entreprise est étayée par son équipe d'experts en Cloud qui aide ses clients à mettre en œuvre des stratégies efficaces pour tirer parti de la puissance du Cloud au sein de leur organisation – donnant aux clients l'ultime tranquillité d'esprit que leur entreprise sera prête pour l'avenir.

