SWITCH

REPORT

Science DMZ basée sur SCION

Améliorer la performance et l'authentification des flux de données volumineux

SCION (Scalability, Control, and Isolation On Next-Generation Networks) est une architecture Internet du futur d'ores et déjà mise à la disposition des établissements d'enseignement supérieur suisses. Une connexion SCION 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.

PRÉSENTATION GÉNÉRALE

Science DMZ avec SCION, pour un haut niveau de performance

Une Science DMZ (ou DMZ scientifique) basée sur SCION associe les avantages traditionnels d'une Science DMZ aux garanties supplémentaires apportées par l'authentification forte de la source de chaque paquet de données, même au débit de ligne, grâce aux hautes performances de LightningFilter, mais sans le coût élevé des pare-feu IP classiques lorsque les vitesses de transmission dépassent 100 Gbps.

LightningFilter peut être intégré à votre architecture de pare-feu existante, tout en assurant des performances élevées pour le trafic SCION associé à votre Science DMZ.

Avantages d'une Science DMZ basée sur SCION

Une mise à niveau de connectivité avec mise en place d'une Science DMZ basée sur SCION offre de nombreux avantages:

- Authentification par paquet grâce à LightningFilter
- Possibilité d'utiliser un serveur standard
- Réduction des dépenses de pare-feu, le trafic de transmission de fichiers volumineux étant séparé du trafic classique
- Capacité native de multipathing au niveau du réseau
- Résilience accrue au déni de service grâce à la suppression du rejeu et de la duplication de paquets par LightningFilter au débit de ligne

Au-delà des garanties améliorées apportées par LightningFilter, une Science DMZ basée sur SCION hérite également de l'ensemble des garanties de sécurité fournies par le plan de contrôle sécurisé de l'architecture SCION et facilite l'adoption de nouvelles fonctionnalités (Path Control, faibles latences de basculement...) pour une résilience accrue aux pannes.

Côté applicatif, l'utilisation de l'application de transfert de fichiers Hercules peut augmenter les performances en évitant le blocage en tête de file (HOL) dans les solutions basées sur TCP, ainsi que les problèmes de contrôle de congestion sur les connexions à haut produit bande passante-délai, et ce, grâce à un meilleur mécanisme de reconnaissance et de contrôle de congestion, de même qu'une implémentation efficace contournant la pile réseau de l'OS.
Hercules fournit par ailleurs un contrôle complet du routage tout en permettant le multipathing sur le réseau SCION.

APPROCHE PROPOSÉE

Les systèmes de détection d'intrusion et les pare-feu sont devenus indispensables à la détection et à la prévention d'un large éventail d'attaques dans l'environnement Internet actuel. Malheureusement, l'application des règles de filtrage complexes des pare-feu modernes demande des capacités de calcul considérables. Une situation qui pose problème dans les déploiements nécessitant des vitesses élevées de transmission des données, comme dans le secteur de la science et du calcul de haute performance.
On peut imaginer qu'une partie du trafic contourne les pare-feu pour échapper à ce goulet d'étranglement. Mais à moins de mettre en place des mécanismes de protection supplémentaires, cette approche expose le réseau à des attaques.

La Science DMZ est une architecture réseau qui remédie précisément à ce problème en créant une zone DMZ dédiée exclusivement aux transferts de données volumineux.
Débarrassée de la complexité associée au trafic général, la Science DMZ dédiée peut garantir des performances optimales. Afin de préserver le périmètre de réseau, on recourt généralement à des listes de contrôle d'accès (ACL) pour restreindre à

une sélection de sources/destinations le trafic transitant par une Science DMZ. Dans certains cas, des systèmes de détection d'intrusion (IDS) améliorent la sécurité.

L'architecture internet SCION apporte une solution haute performance pour mettre en place une Science DMZ ou pour améliorer les performances et enrichir les fonctions de sécurité d'une Science DMZ traditionnelle.
LightningFilter, un mécanisme d'authentification et de filtrage du trafic à haut débit, est au centre de la solution.
Par ailleurs, en évitant les itinéraires congestionnés et en agrégeant la bande passante sur plusieurs chemins, la fonction SCION de contrôle du choix du chemin d'accès promet des gains de performance pour les applications.

Science DMZ basée sur SCION

Dans une architecture réseau de Science DMZ basée sur SCION, les transferts de données volumineux sont acheminés en tant que trafic SCION via LightningFilter au lieu du pare-feu standard.
Côté expéditeur, LightningFilter ajoute des authentifiants de paquet et de source qui, par cryptographie, protègent l'intégrité de chaque paquet et authentifient l'adresse de la source pour le destinataire. Côté destinataire, LightningFilter vérifie les authentifiants et bloque le trafic malveillant.
Le filtrage basé sur l'adresse et la limitation de débit renforcent encore la protection des services contre les utilisateurs inconnus ou irrespectueux.

Notre prototype open source de LightningFilter, exclusivement implémenté au niveau logiciel, exécute, sur matériel standard, l'authentification et le filtrage au débit de ligne pour des bandes passantes pouvant atteindre 160 Gbps. Parce qu'il ne requiert pas de matériel spécialisé, ses coûts sont considérablement inférieurs à ceux des pare-feu d'entreprise pour une vitesse comparable.
L'authentification repose sur le système DRKey, qui permet la création d'une hiérarchie de clés symétriques et est utilisé dans toute la dorsale de SCION.

L'utilisation de SCION facilite non seulement l'intégration de LightningFilter, mais ouvre également la voie à des applications exerçant un contrôle sur le choix des chemins.
Une fonction particulièrement utile dans le contexte des transferts de données volumineux dans la mesure où la bande passante peut ainsi être agrégée sur plusieurs chemins d'accès.

Hercules, un système de transfert de fichiers à haute vitesse, transmet ses paquets sur différents chemins pour mieux mettre à profit la bande passante disponible sur le réseau.
En outre, la possibilité d'éviter délibérément les chemins congestionnés et la réduction du délai de basculement en cas de liaisons défaillantes s'ajoutent aux arguments en faveur d'une architecture réseau DMZ basée sur SCION.

En conclusion, notre solution Science DMZ basée sur SCION offre une sécurité renforcée grâce à l'authentification de la source et au filtrage du trafic au débit de ligne sans aucune perte de vitesse.

Exemple: cluster de calcul de haute performance et hautes écoles

Aujourd'hui, le secteur de la recherche s'appuie bien souvent sur un volume considérable de données. Les hautes écoles n'étant pas toujours en mesure de fournir les ressources de calcul nécessaires au traitement de ces quantités de données, le cluster de calcul de haute performance (HPCC) offre une alternative économique aux chercheurs.
Avec une Science DMZ basée sur SCION, le HPCC et chaque haute école fonctionnent comme un système autonome indépendant, qui gère ses propres clés cryptographiques et fait appliquer ses propres règles réseau. Chaque système autonome possède également son propre déploiement LightningFilter.
Les transferts de données volumineux entre une haute école et le HPCC sont exécutés à l'aide de systèmes basés sur SCION dédiés, comme Hercules, qui acheminent leur trafic via LightningFilter au lieu du pare-feu général du réseau.

Avec LightningFilter, les systèmes autonomes peuvent contrôler le niveau de trafic reçu des autres systèmes autonomes ou d'hôtes précis.
Par exemple, le HPCC peut imposer différentes limites de débit pour chaque haute école tout en garantissant un débit particulier pour certains hôtes. Ces limites sont importantes pour protéger les services offerts contre les hôtes irrespectueux qui consomment davantage de bande passante que convenu, empêchant en partie ou totalement les autres hôtes d'accéder au service.