SWITCH

REPORT

SCION-basierte Science DMZ

Verbesserung der Leistung und Authentifizierung von grossen Datenströmen

SCION (Scalability, Control, and Isolation On Next-Generation Networks) ist eine zukünftige Internet-Architektur, die den Schweizer Hochschulen bereits heute zur Verfügung steht. Eine SCION-Verbindung kombiniert die Sicherheit, Zuverlässigkeit und Kontrolle privater Netzwerke mit der Flexibilität des öffentlichen Internets. Die Technologie wurde an der Eidgenössischen Technischen Hochschule (ETH) in Zürich entwickelt. SWITCH unterstützt die Entwicklung von SCION an der ETH Zürich seit 2015.

ÜBERBLICK

Science DMZ mit SCION, für hohe Leistung

Eine SCION Science DMZ kombiniert die traditionellen Vorteile einer Science DMZ mit den zusätzlichen Garantien einer starken Quellenauthentifizierung jedes Datenpakets, selbst bei Leitungsgeschwindigkeit, dank der hohen Leistung von LightningFilter, aber ohne die hohen Kosten herkömmlicher IP-Firewalls, wenn Übertragungsraten von über 100 Gigabit pro Sekunde erreicht werden.

LightningFilter kann in Ihre bestehende Firewall-Architektur integriert werden und bietet gleichzeitig eine hohe Leistung für den SCION-Datenverkehr, der Ihre Science DMZ betrifft.

Vorteile einer SCION Science DMZ

Die Aufrüstung Ihrer Konnektivität und die Einrichtung einer SCION Science DMZ bietet mehrere Vorteile:

- Authentifizierung pro Paket dank LightningFilter
- Fähigkeit, auf einem Commodity-Server zu laufen
- Geringere Firewall-Kosten, da der hochvolumige Datei-Übertragungsverkehr vom normalen Verkehr getrennt wird
- Native Multipath-Fähigkeit auf Netzwerkebene
- Erhöhte Denial-of-Service-Resilienz dank der Unterdrückung von Replay und Paketduplikaten durch LightningFilter bei Leitungsgeschwindigkeit

Neben den erweiterten Garantien, die LightningFilter bietet, erbt eine SCION-basierte Science DMZ auch alle Sicherheitsgarantien, die von der sicheren Steuerungsebene der SCION-Architektur geboten werden, und bietet einen Upgrade-Pfad zu weiteren Funktionen wie Pfadkontrolle und niedrige Failover-Latenzen, die eine erhöhte Ausfallsicherheit bieten.

Auf der Anwendungsseite kann die Verwendung der Dateiübertragungsanwendung Hercules die Leistung verbessern, indem die Head-of-Line-Blockierung in TCP-basierten Lösungen und Probleme mit der Staukontrolle bei Verbindungen mit hoher Bandbreite und Verzögerung dank einer verbesserten Staukontrolle und eines Bestätigungsschemas sowie einer effizienten Implementierung unter Umgehung des OS-Netzwerkstacks vermieden werden.
Hercules bietet außerdem eine vollständige Pfadkontrolle und ermöglicht Multipathing über das SCION-Netzwerk.

VORGESCHLAGENER ANSATZ

Intrusion Detection Systeme und Firewalls sind für die Erkennung und Verhinderung einer Reihe von Angriffen in der heutigen Internetumgebung unverzichtbar geworden. Leider ist die Durchsetzung der komplexen Filterregeln moderner Firewalls sehr rechenintensiv. Dies stellt ein Problem für Einrichtungen dar, die hohe Datenübertragungsraten benötigen, wie z. B. in der Wissenschaft und bei Hochleistungsrechnern.
Eine Möglichkeit zur Umgehung des Engpasses besteht darin, bestimmten Datenverkehr um Firewalls herumzuleiten. Ein solcher Ansatz macht das Netz jedoch angreifbar, wenn keine zusätzlichen Schutzmechanismen vorhanden sind.

Die Science DMZ ist eine Netzwerkarchitektur, die genau dieses Problem angeht, indem sie eine spezielle DMZ ausschließlich für hochvolumige Datenübertragungen einrichtet.
Ohne die Komplexität, die mit dem allgemeinen Datenverkehr verbunden ist, kann die dedizierte Science DMZ eine optimale Leistung gewährleisten.
Um die Netzwerkgrenze zu wahren, werden in der Regel Zugriffskontrolllisten (ACLs) verwendet, um den Verkehr durch eine Science DMZ auf eine ausgewählte Gruppe von Quellen/

Zielen zu beschränken. In einigen Fällen wird die Sicherheit durch Intrusion Detection Systeme (IDS) erhöht.

Die SCION-Internet-Architektur bietet eine leistungsstarke Lösung zur Einrichtung einer Science DMZ oder zur Ergänzung einer herkömmlichen Science DMZ mit verbesserter Leistung und zusätzlichen Sicherheitsfunktionen.
Im Mittelpunkt der Lösung steht LightningFilter, ein Hochgeschwindigkeitsmechanismus zur Authentifizierung und Filterung von Datenverkehr.
Darüber hinaus verspricht die Path-Awareness-Funktion von SCION Leistungsverbesserungen für Anwendungen, indem überlastete Pfade vermieden und die Bandbreite über mehrere Pfade aggregiert wird.

Wissenschaftliche DMZ auf SCION-Basis

In einer SCION-basierten Science DMZ-Netzwerkarchitektur werden hochvolumige Datenübertragungen als SCION-Verkehr durch LightningFilter anstatt durch die Standard-Firewall geleitet.
Auf der Senderseite fügt LightningFilter Paket- und Quellauthentifikatoren hinzu, die die Integrität des Pakets kryptographisch schützen und die Quelladresse gegenüber dem Empfänger authentifizieren.
Auf der Empfängerseite verifiziert LightningFilter die Authentifikatoren und blockiert bösartigen Datenverkehr.Adressbasierte Filterung und Ratenbegrenzung schützen die geschützten Dienste zusätzlich vor unbekannten oder missbräuchlichen Nutzern.

Unser Open-Source-Prototyp von LightningFilter, der rein in Software implementiert ist, ermöglicht die Authentifizierung und Filterung bei einer Bandbreite von bis zu 160 Gbit/s auf handelsüblicher Hardware. Da keine spezielle Hardware benötigt wird, sind die Kosten im Vergleich zu Firewalls der Enterprise-Klasse mit vergleichbarem Durchsatz deutlich geringer.
Die Authentifizierung basiert auf dem DRKey-System, das die Erstellung einer Hierarchie von symmetrischen Schlüsseln ermöglicht und im gesamten SCION-Backbone verwendet wird.

Der Einsatz von SCION ermöglicht nicht nur die nahtlose Integration von LightningFilter, sondern ebnet auch den Weg für pfadabhängige Anwendungen.
Im Zusammenhang mit der Übertragung grosser Datenmengen ist dies besonders nützlich, da es die Aggregation der Bandbreite über mehrere Pfade ermöglicht.
Hercules, ein Hochgeschwindigkeits-Dateitransfersystem, überträgt seine Pakete über mehrere verschiedene Pfade, um die verfügbare Bandbreite im Netz besser zu nutzen.
Weitere Argumente für eine SCION-basierte DMZ-Netzwerkarchitektur sind die Möglichkeit, überlastete Pfade aktiv zu vermeiden und die Wiederherstellungszeit bei ausgefallenen Verbindungen zu verkürzen.

Insgesamt bietet unsere SCION-basierte Science DMZ-Lösung eine verbesserte Sicherheit durch Quellenauthentifizierung und Verkehrsfilterung bei Leitungsgeschwindigkeit ohne Beeinträchtigung des Durchsatzes.

Beispiel: High Performance Computing Cluster und Universitäten

Die heutige Forschung ist oft auf ein großes Datenvolumen angewiesen. Während Universitäten nicht immer die Rechenressourcen zur Verfügung stellen können, um eine bestimmte Datenmenge zu verarbeiten, bietet ein High-Performance-Computing-Cluster (HPCC) eine kostengünstige Alternative für Forscher.
Mit einer SCION-basierten Science DMZ arbeiten das HPCC und jede Universität als unabhängige AS, die ihre eigenen kryptografischen Schlüssel verwalten und ihre eigenen Netzwerkregeln durchsetzen. Jedes AS hat auch seinen eigenen LightningFilter im Einsatz.
Hochvolumige Datenübertragungen zwischen einer Universität und dem HPCC werden über dedizierte, SCION-basierte Systeme wie Hercules abgewickelt, die ihren Datenverkehr über LightningFilter anstatt über die allgemeine Firewall des Netzwerks leiten.

Mit LightningFilter können die AS die Menge des von den anderen AS oder von bestimmten Hosts empfangenen Datenverkehrs kontrollieren.
So kann das HPCC beispielsweise unterschiedliche Ratenlimits für jede Universität durchsetzen und gleichzeitig einen bestimmten Durchsatz für bestimmte Hosts garantieren. Solche Limits sind wichtig, um die angebotenen Dienste vor missbräuchlich handelnden Hosts zu schützen, die mehr Bandbreite als vereinbart verbrauchen und damit andere Hosts teilweise oder ganz vom Zugang zum Dienst abhalten.