SWITCH

REPORT

SCION-based Science DMZ

Improving performance and authentication of large data flows

SCION (Scalability, Control, and Isolation On Next-Generation Networks) is a future internet architecture already available today to Swiss higher education institutions. A SCION connection combines the security, reliability and control of private networks with the flexibility of the public internet. The technology was developed at the Swiss Federal Institute of Technology (ETH) in Zurich. SWITCH has been supporting SCION's development at ETH Zurich since 2015.

OVERVIEW

Science DMZ with SCION, for high performance

A SCION Science DMZ combines the traditional advantages of a Science DMZ with the additional guarantees provided by strong source authentication of every data packet, even at line rate, thanks to the high performance of LightningFilter, but without the high cost of traditional IP firewalls when reaching transmission rates over 100 Gigabits per second.

LightningFilter can be integrated into your existing firewall architecture, while providing high performance for the SCION traffic involving your Science DMZ.

Benefits of a SCION Science DMZ

Upgrading your connectivity and setting up a SCION Science DMZ provides multiple benefits:

- Per packet authentication thanks to LightningFilter
- Ability to run on a commodity server
- Reduced firewall expenses, since high-volume file transmission traffic is segregated from regular traffic
- Native multipath capability at the network level
- Increased Denial of Service resilience thanks to the replay and packet duplicate suppression of LightningFilter at line rate

Besides the enhanced guarantees provided by LightningFilter, a SCION-based Science DMZ also inherits all the security guarantees provided by the secure control plane of the SCION architecture and provides an upgrade path to further features such as path control and low failover latencies, providing increased resilience to outages.
On the application side, using the file transfer application Hercules can enhance performance by avoiding the head-of-line blocking in TCP-based solutions and issues with congestion control on high bandwidth-delay connections, thanks to an improved congestion control and acknowledgement scheme, as well as an efficient implementation bypassing the OS network stack.
Hercules also provides full path control and enables multipathing over the SCION network.

PROPOSED APPROACH

Intrusion detection systems and firewalls have become indispensable in the detection and prevention of a range of attacks in today's internet environment. Unfortunately, enforcing the complex filtering rules of modern firewalls is very computationally intensive. This creates a problem for setups that require high rates of data transmission, such as in science and high-performance computing.
One way around the bottleneck is to route certain traffic around firewalls. However, such an approach opens the network to attack unless additional protection mechanisms are in place.

The Science DMZ is a network architecture that addresses this very problem by creating a dedicated DMZ exclusively for high-volume data transfers.
Without the complexity associated with general-purpose traffic, the dedicated Science DMZ can ensure optimal performance.
To preserve the network perimeter, access control lists (ACLs) are typically used to restrict traffic through a Science DMZ to a selected set of sources/destinations. In some cases, intrusion detection systems (IDS) enhance security.

The SCION internet architecture provides a high-performance solution for establishing a Science DMZ or complementing a

traditional Science DMZ with enhanced performance and additional security features.
The solution centres around LightningFilter, a high-speed traffic authentication and filtering mechanism.
In addition, SCION's path awareness feature promises performance improvements for applications by avoiding congested paths and aggregating bandwidth across multiple paths.

SCION-based Science DMZ

In a SCION-based Science DMZ network architecture, high-volume data transfers are routed as SCION traffic through LightningFilter instead of the standard firewall.
On the sender side, LightningFilter adds packet and source authenticators, which cryptographically protect the integrity of the packet and authenticate the source address to the receiver.
On the receiver side, LightningFilter verifies the authenticators and blocks malicious traffic.
Address-based filtering and rate limiting further shield the protected services from unknown or misbehaving users.

Our open-source prototype of LightningFilter, implemented purely in software, achieves authentication and filtering at line rate for bandwidths up to 160 Gbps running on commodity hardware. Without the need for specialised hardware, costs are significantly lower compared to enterprise-grade firewalls with a comparable throughput.
The authentication is based on the DRKey system, which enables the creation of a hierarchy of symmetric keys and is used throughout SCION's backbone.

Using SCION not only enables the seamless integration of LightningFilter, but also paves the way for path-aware applications.
In the context of high-volume data transfer, this is particularly useful because it allows bandwidth aggregation over multiple paths.
Hercules, a high-speed file transfer system, transmits its packets over several different paths to make better use of the available bandwidth on the network.
Furthermore, the possibility of actively avoiding congested paths and decreasing recovery time from failed links are other arguments for a SCION-based DMZ network architecture.

Overall, our SCION-based Science DMZ solution offers enhanced security through source authentication and traffic filtering at line rate without impacting the throughput.

Example: High Performance Computing Cluster and universities

Today's research often relies on a high volume of data. While universities cannot always provide the computing resources to process a given amount of data, a high-performance computing cluster (HPCC) offers a cost-effective alternative for researchers.
With a SCION-based Science DMZ, the HPCC and each university operate as independent autonomous system (AS), managing their own cryptographic keys and enforcing their own network rules. Each AS also has its own LightningFilter deployed.
High-volume data transfers between a university and the HPCC are performed using dedicated, SCION-based systems, such as Hercules, which route their traffic through LightningFilter instead of the network's general-purpose firewall.

With LightningFilter, the ASes can control the amount of traffic received from the other ASes or from specific hosts.
For instance, the HPCC can enforce different rate limits for each university while guaranteeing a certain throughput for specific hosts. Such limits are important to protect the services offered from misbehaving hosts that consume more bandwidth than agreed and thus partially or completely block other hosts from reaching the service.