SWITCHlan SCION Access

Factsheet

More security, reliability and control: SWITCHlan SCION access provides the best conditions for ensuring that your data is only transferred to the parts of the internet that you want it to reach.

The secure internet architecture of the next generation

These days, digitalisation requires secure networks that are easy to control. However, the foundation of the internet was laid last century without any special security mechanisms, and it has hardly been updated since. That makes it vulnerable. Nowadays, cybercriminals exploit vulnerabilities to such a degree that IT departments spend the majority of their time trying to prevent and eliminate cyber threats. This observation concerns not only the multitude of security risks, but also aspects of the transport network. It's high time for an upgrade. SCION (Scalability, Control, and Isolation On Next-Generation Networks) is that upgrade. SWITCHlan SCION access 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 supported SCION's development at ETH Zurich since 2015.

How you benefit

- **Security by design:** SWITCHlan SCION access protects against cyber attacks such as prefix hijacking and specific DDoS attacks
- **New security features:** path control and path verification
- **Path control:** you define the networks to which your data is confined; you define the route your data packets take
- **Path verification:** the path and integrity of all packages is cryptographically secured and verifiable
- **Multi-pathing:** reliable data transfer via multiple network paths at the same time
- **Cybersecurity:** your data can no longer be redirected during transfers; protection against DDoS reflection attacks
- **Isolation domains:** trust limited to participants of an ISD (no more global trust roots)

High degree of reliability

SCION's architecture gives you a high degree of reliability with various features and new concepts. As a result, some attacks can be prevented from the very outset: SCION is immune to prefix hijacking. What is more, the technology reduces the risk of exposure to distributed denial of service (DDoS) attacks through hidden paths and source authentication. The protection provided against address spoofing even prevents susceptibility to DDoS reflection attacks.

Reliability and performance through multi-pathing

Multi-pathing allows the SCION protocol to open up multiple potential paths that can be used simultaneously. This increases the usable capacity in the network and enables faster switching in the event of path failures, provided that the application supports this function.

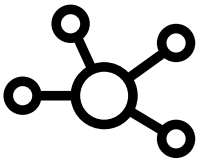
In this instance, the granularity of the path selection is restricted to the transfer points between networks (autonomous systems). The path within a network is not subject to the control of SCION, meaning alternative paths cannot be used there.

More control with SCION

SCION gives you path control over your end-to-end communication, allowing you to avoid certain network sections such as networks in unstable regions. Control over path choice also allows you to make selections regarding available bandwidths and latencies. This increases the security of your data in terms of how it is handled. You get more control over the transport route of your sensitive data.

SWITCH

Security
All the paths are authenticated and protected against routing attacks.



Stability
Multiple network paths with instant failover ensure that individual path failures go unnoticed.

Control
You control the route of your data to its destination.

Protection
Hidden paths and the path selection controlled by the sender increase protection against DDoS attacks.

Performance
A SCION application can select the best paths for network traffic based on cost or latency rules.

The technology of SCION

Today's internet is made up of a multitude of loosely interconnected networks. Communication between the different networks makes transfers vulnerable through route hijacking. For example, a data packet could be diverted across several countries on its way from Zurich to Geneva and the sender and recipient would be helpless to prevent this from happening. Such hijackings are often detected well after the event.

Cybercriminals can redirect data packets or disable internet services with DDoS attacks. This is where SCION comes in – and minimises the area of attack to network level from the outset.

A team from ETH Zurich has redesigned SCION's internet architecture from scratch. The foundation is formed by 'isolation domains' (ISDs). These domains can be states, industries or autonomous companies. SCION combines several networks (geographical, for example) to form ISDs. All the Swiss networks can belong to one ISD, for instance. Communication between two networks in the same ISD never goes anywhere else. As a result, confidential data can no longer be diverted unchecked via other network sections.

With SCION, the sender determines what transport route the data packets take, making attacks at routing level essentially impossible. For example, you can specify certain providers or network paths to avoid.

At present, the SCION protocol is still in development. Officially, the specification has not yet been publicly standardised. The development team at ETH is actively seeking to obtain this standardisation.

Services

SWITCHlan SCION Access

This variant is your SCION connection to SWITCHlan's SCION Core (CH-ISD, without Edge services). Here, you the customer are responsible for procuring and operating the SCION router. You will need a software licence for this, depending on the provider.

If you are not connected to the SWITCHlan backbone yet, for example because you are using the IP access or L2VPN service, we will be happy to provide you with a tailored quotation.

SWITCHlan SCION Edge

The managed service is an optional addition to SWITCHlan SCION access and is used to operate your SCION router and connection (SCION Edge: SCION IP gateway).

Do you have any questions? We would be happy to help you understand the next generation of internet architecture.
Are you interested in SWITCHlan SCION access? Call us or send us a message. We advise you with expertise, commitment and a focus on your individual requirements.

Daniel Bertolo
Head Network
daniel.bertolo@switch.ch
+41 44 268 15 87

Diego Tres
Community Account Manager
hello@switch.ch
+41 44 268 16 57

SWITCH
PO Box
8021 Zurich
switch.ch/SCION

SWITCH