swisscom

InterCloud

ANAPAYA

WHITE PAPER

SCION Technology: Transformation and Optimization of your International Connectivity

This paper summarizes the findings of Swisscom's test of the SCION technology for future optimized international connectivity.

Executive Summary

The Internet as we know it today is outdated. Having no major updates or upgrades since the 90s, it has become an easy target for cyber attackers. The Internet, despite its flaws, is still widely used by governments, businesses, and individuals to transmit highly sensitive information every day.

In a digitalized world like ours, we have become reliant on the Internet, not just as a means to communicate but as a fundamental pillar of a modern lifestyle.

International communication relies heavily on the public Internet. Critical information, digital assets, and interactions are essential today – but they're also ineffective. Long-distance point-to-point MPLS lines are expensive but lack the flexibility required in a fast-moving world of business. They take control away from the sender of data, leaving the communication line vulnerable. The SCION protocol is an effective and efficient alternative to the traditional Internet, offering many benefits that exceed today's connectivity expectations.

Swisscom, the leading telecommunication service company in Switzerland, not only provides Internet services to customers locally but also ensures international connectivity for Swiss-based customers. The current challenges faced by users of the public Internet regarding security, flexibility, and performance, as well as being a staunch promoter of increasing the security of the Internet, have led Swisscom to support the research and development of the SCION protocol. Further, Swisscom have executed Proofs of Concept (PoCs) to showcase the benefits of technologies for our customers.

In this white paper, Swisscom, in close collaboration with Anapaya Systems AG and InterCloud, presents a summary of the findings on international connectivity using the SCION protocol. The goal of this Proof of Concept is to investigate and validate the effect of SCION technology on future international communications over the public Internet.

Today's Connectivity, Tomorrow's Solution

The problems with today's public Internet are rooted in the very approach that made it possible. The Border Gateway Protocol (BGP) is what enables traffic to be routed over the Internet. It is designed to self-correct, selecting the fastest routes possible to connect users.

BGP essentially creates a map for all the destinations on the Internet. Extremely simplified, it has 4 functions:

1. Creating a connection to neighbouring systems (TCP handshake)
2. Share reachable destinations with neighbours
3. Monitor changes and unreachable neighbours
4. Update the Internet map (routing tables)

However, BGP was not designed with security as a main motivator and can easily be taken advantage by unscrupulous individuals. There have been thousands of misconfigurations and attacks on BGP, some of which left the Internet unreachable - while others routed targeted traffic to unwanted locations for malicious purposes. There have been efforts made to secure the BGP (for example, BGPSec). However, most of them rely on updating the current infrastructure and having a full deployment of the changes, requiring other parties to cooperate, which is why BGP is still not as secure as it needs to be.

With international communication between companies or branch offices and cloud service providers across the globe, there is no possibility of managing where traffic is sent to, a crucial point in today's world where we are forced to comply with privacy laws.

SCION is an innovative technology researched and developed at ETH Zürich, Switzerland. One of the key features of the new SCION protocol is the possibility for users to send traffic over the Internet with control, trust, and verification. For international communication between companies or branch offices, this feature could be the key to mitigating current challenges while complying with privacy laws. With a SCION-based international connection, a network administrator can make upfront decisions on how traffic will be routed instead of relying on other parties to securely route the traffic or to go even further, the administrator can purposely match the SCION-based international connection with the needs of a certain application.

In our Proof-of-Concept tests demonstrated below, we put SCION to the test against the Border Gateway Protocol.

PoC – SCION based international connectivity

Setting the Scene

Problem Statement

When the Internet was designed, the focus was on the openness and scalability of the technology. Security was not a priority, and traffic routing security flaws still exists over BGP protocol. One such example led to an incident in 2019, where European traffic was re-routed over China, where traffic inspection and data leakage occurred.

In today's world, where digital information is critical to the development of businesses and governments, this scenario is unacceptable yet all too common. We wanted to find a way to boost the security of the public Internet so that the incidents described above can be avoided.

By implementing the SCION protocol on an international connection, we are confident that we can enhance security and obtain greater control over how the data is transferred on the public Internet.

Swisscom Cloudlab Ltd.

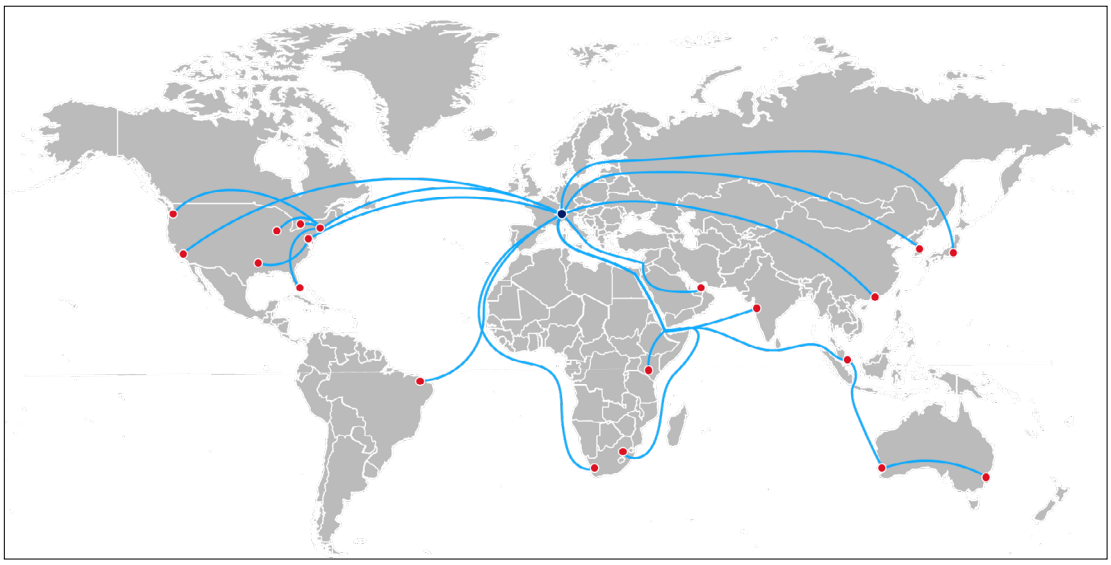
Swisscom Cloudlab Ltd. is based in Palo Alto (close to San Francisco, USA) and is a branch office (Outpost) of Swisscom (Switzerland) AG. This small team works on innovative topics and scouts for new technologies on behalf of Swisscom. Having a local test datacenter, the Swisscom Outpost can also validate new software stacks and versions of Swisscom partners like VMware. This flexibility makes the Outpost an ideal place to run PoCs of new solutions in the areas of IoT, security, telco, data analytics, confidential computing and user experience.

Swisscom's International IP-Plus® Business Internet Backbone

To serve Swiss-based customers, Swisscom maintains a global Internet backbone which is directly connected to essential IXPs. Swisscom customers enjoy direct, high capacity, and fully controlled links throughout the world thanks to this global backbone.

In addition, Swisscom operates its own international network nodes with direct monitoring and control of IP traffic. The network nodes filter unauthorized traffic locally rather than in Switzerland, thus reducing the change of cybercrime uptick.

Overview of Swisscom's International IP-Plus® Internet Backbone in Europe



Overview of Swisscom's International IP-Plus® Internet Backbone globally

swisscom

InterCloud

ANAPAYA

InterCloud

InterCloud is a leading provider of Software-Defined Cloud Interconnect (SDCI), delivering secure, end-to-end managed services to some of the world's leading organizations. InterCloud's API-centred platform helps businesses simplify and accelerate network operation, with a high level of performance and transparency for corporate resources distributed across multiple locations and different cloud providers.

InterCloud uses SCION to power their cloud connectivity and was utilized in the comparison due to cloud connectivity becoming standard in business. With dual SCION and regular networking capabilities, they are good test partner for the purposes of the Proof of Concept.

Anapaya Systems AG

Anapaya Systems AG is a Swiss company whose goal is to build an international ecosystem providing SCION-based services for a more reliable, secure, and stable networking experience. As the commercial provider of SCION, their solutions provide organizations around the globe with a way to transport critical business data securely and transparently across the network, sending information between corporate sites, trusted partners, and cloud providers.

A comparison will be made between modern Internet connectivity and Anapaya's SCION solution.

SCION protocol

The SCION protocol was researched and developed at the University ETH Zürich (Switzerland), an innovative inter-domain routing technology to control the routing of traffic with confidence and trust. The SCION protocol establishes a secured end-to-end path from source to destination while providing trust between each hop on the way. The SCION protocol can stop BGP hijacking completely and protect against other attacks originating from the Internet (such as DDoS attacks).

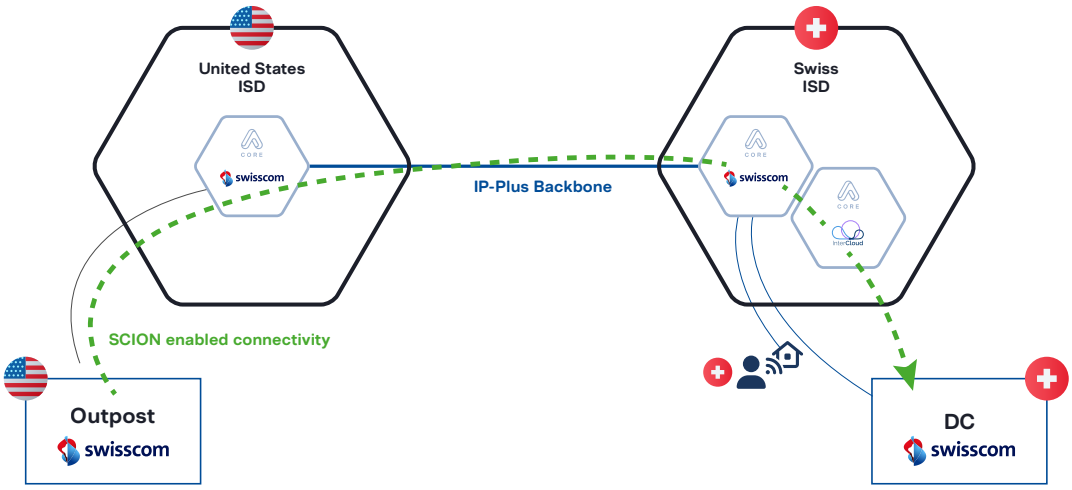
In terms of our Proof of Concept, the SCION protocol will be directly compared to regular Internet connectivity. It was estimated that SCION would be able to provide a superior connectivity experience to the Internet as we know it.

PoC Environment

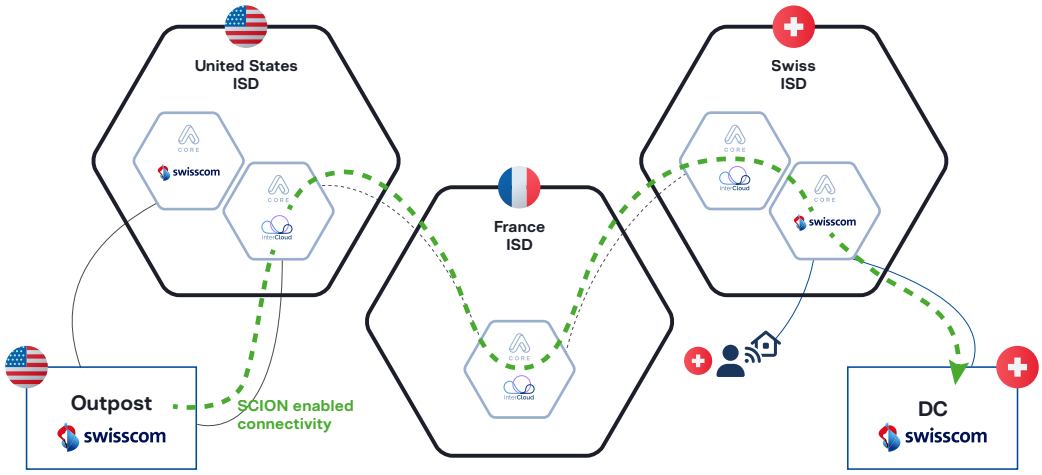
The SCION connection is compared to the traffic sent over the legacy connection, otherwise known as the IP-based public Internet.

To showcase the benefits of the SCION protocol on an international connection over the public Internet, we have set up 2 SCION enabled connections:

1. SCION enabled Swisscom's IP-Plus



2. SCION enabled InterCloud Backbone



The SCION enabled connectivity between the Swisscom Outpost (San Francisco) and HQ in Switzerland sends the same amount of productive data as the legacy connection. We are using this transmission to compare the performance, bandwidth utilization and control of each network.

PoC Test Results

We used the above environment to conduct our tests, using three evaluative parameters:

- Failover capabilities
- Latency
- Parallel connectivity

In this documentation a “SCION connectivity” refers to the time measured in milliseconds (ms) that it takes for a packet to reach (destination) starting from (origin).

Failover Test:

Swisscom Outpost’s Cloudlab conducted a failover test together with Anapaya Systems AG of the SCION connectivity in March 2022.

Test Scenario:

Testing the failover path on two different SCION networks:

1. California (USA) to Bern (CH) over Swisscom SCION enabled IP-Plus connection
2. California (USA) to Paris (FR) over InterCloud’s SCION backbone

Test Results:

The below presented screenshots shows that the failover path was responding to ping requests and did not drop packages during a failover test.

Additionally, the below screenshots show how policies can be configured to customize weighting or selection of connection paths.

swisscom InterCloud ANAPAYA

Red line: Measures the SCION connectivity from Swisscom Cloudlab (California) to Swisscom (Bern) configured to use Swisscom's backbone.

Blue line: Measures the SCION connectivity from Swisscom Cloudlab (California) to Swisscom (Bern) configured to use Swisscom's backbone (preferred) and InterCloud's backbone (secondary).

Orange line: Measures the amount of ping requests that were lost when using Swisscom's backbone to go from Swisscom Cloudlab (California) to Swisscom (Bern).

Purple line: Measures the amount of ping requests that were lost when using Swisscom's (preferred) or InterCloud's (secondary) backbone to go from Swisscom Cloudlab (California) to Swisscom (Bern).

Summary:
The blue line in the graphic will either go over InterCloud or Swisscom's backbone and was constantly responding to pings during the failover test. During the failover test the connectivity was transparently switched from the path via the Swisscom network to the path that goes over InterCloud's network.

Red line: Measures the SCION connectivity from Swisscom Cloudlab (California) to InterCloud (Paris) configured to use InterCloud's backbone (no policy changes during test).

Blue line: Measures the SCION connectivity from Swisscom Cloudlab (California) to InterCloud (Paris) configured to use Swisscom's backbone (before policy modification) and later use InterCloud's backbone (after policy modification).

Orange line: Measures the amount of ping requests that were lost when using InterCloud's backbone (after policy modification) to go from Swisscom Cloudlab (California) to InterCloud (Paris).

Purple line: Measures the amount of ping requests that were lost when using Swisscom's backbone (before policy modification) to go from Swisscom Cloudlab (California) to InterCloud (Paris).

Policy modifications with path control:
The blue line was previously configured to take the longer path over Swisscom (Bern) to reach the destination of InterCloud (Paris), after modifying the configuration the blue line took the faster route over InterCloud's path to Paris.

Red line: Measures the SCION connectivity from Swisscom Cloudlab (California) to Swisscom (Bern) configured to use Swisscom's backbone (preferred) and InterCloud's backbone (secondary).

Blue line: Measures the SCION connectivity from Swisscom Cloudlab (California) to InterCloud (Paris) configured to use Swisscom's backbone (preferred) and InterCloud's backbone (secondary).

Orange line: Measures the amount of ping requests that were lost when using Swisscom's backbone.

Purple line: Measures the amount of ping requests that were lost when using InterCloud's backbone.

Policy modifications and failover test with path weighting:
Similar to the test case above, the red line preferred the route over Swisscom's network to Swisscom (Bern) which is naturally faster while the blue line was configured to prefer the route over Swisscom's network to InterCloud (Paris) which is naturally slower. Both paths went over InterCloud's network as soon as the Swisscom path was manually made unavailable until making the Swisscom's network available again (line crossings).

Latency Test

Swisscom Cloudlab together with Anapaya Systems AG collected the network performance of the SCION enabled international connectivity over a period of 2 months.

Tools:
InfluxDB and Telegraf were used to collect the metrics.

Test Scenario:
Testing the connectivity from Swisscom Cloudlab (Palo Alto, California) to Bern and Paris over 6 different network paths and configurations:

1. California (USA) to Bern (CH) over Swisscom's SCION enabled IP-Plus connectivity
2. California (USA) to Bern (CH) over InterCloud's SCION backbone
3. California (USA) to Bern (CH) over the public Internet
4. California (USA) to Paris – InterCloud (FR) over Swisscom's SCION enabled IP-Plus
5. California (USA) to Paris – InterCloud (FR) over InterCloud's SCION backbone
6. California (USA) to Paris - InterCloud (FR) over the public Internet

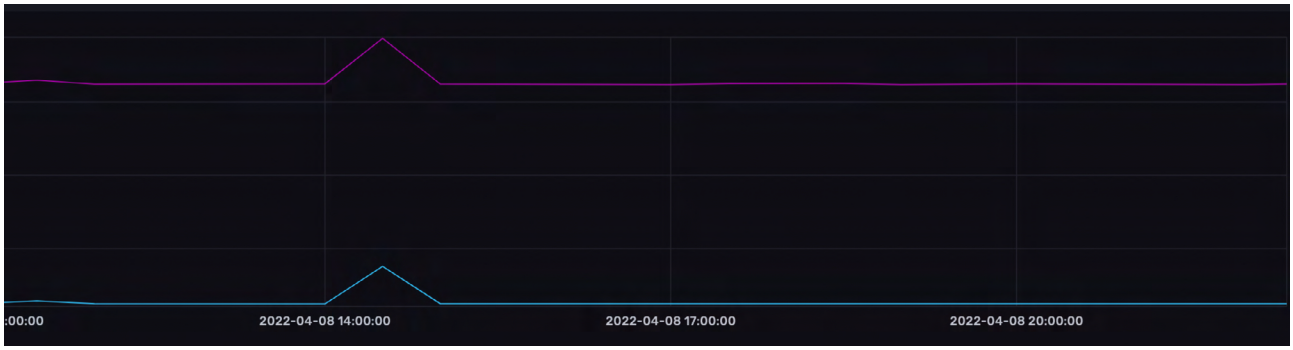
Stipulations:
Because there is no direct SCION gateway on Swisscom Cloudlab's datacenter in California, the SCION connectivity will always carry the last mile over the Internet.

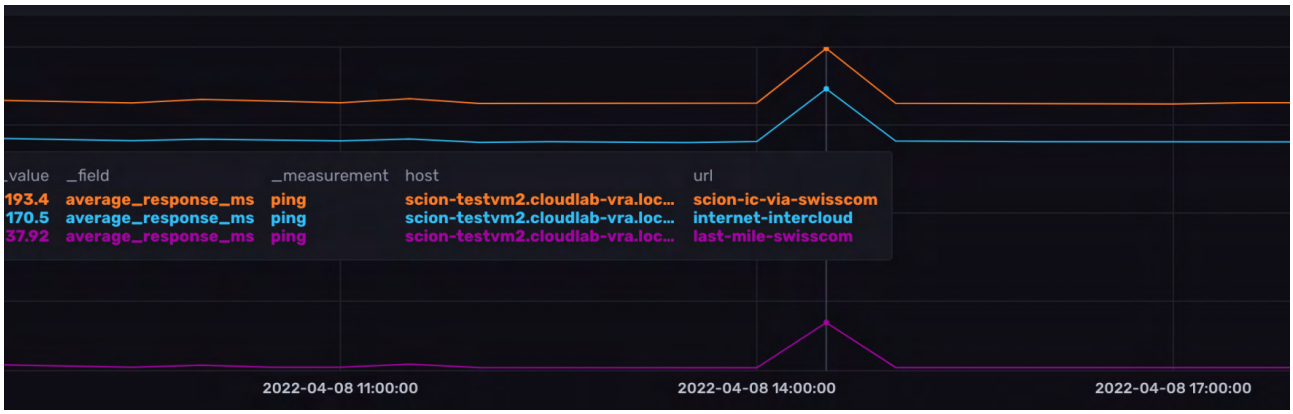
For this we added two additional destination that we collected metrics on:

- Last mile (Internet) using Swisscom's SCION's endpoint
- Last mile (Internet) using InterCloud's SCION's endpoint

This should give a better picture on how the individual routes perform during Internet surges and jitter. Latency is messured in response time (ms).

Finding 1 - During Internet Jitter
We can see in the below example that the SCION connectivity is equally impacted by the jitter (spike in response time) noticed at the last mile level (locally to the datacenter in California).





Orange line: Measures the response time between Swisscom Cloudlab (California) to InterCloud (Paris) over Swisscom's backbone (SCION enabled).

Blue line: Measures the response time between Swisscom Cloudlab (California) to InterCloud (Paris) over Internet connectivity.

Purple line: Measures the "last line" (Internet) response time from Swisscom Cloudlab (datacenter) to Anexia-IT (service provider with SCION enabled router in California).

Finding 2 - Other
The test is stipulated by not having a SCION capable router in the Sunnyvale datacenter of Swisscom Cloudlab, this makes both SCION paths (Swisscom and InterCloud routers) to hop over Los Angeles (Anexia-IT router) before continuing an optimal path forward. The "last-mile" cannot be subtracted comfortably but rather conclude that SCION is on a par with the Internet when it comes to latency.

Parallel Connectivity

Swisscom Cloudlab together with Anapaya Systems AG created a setup where traffic was sent over two different paths but with the same source and destination.

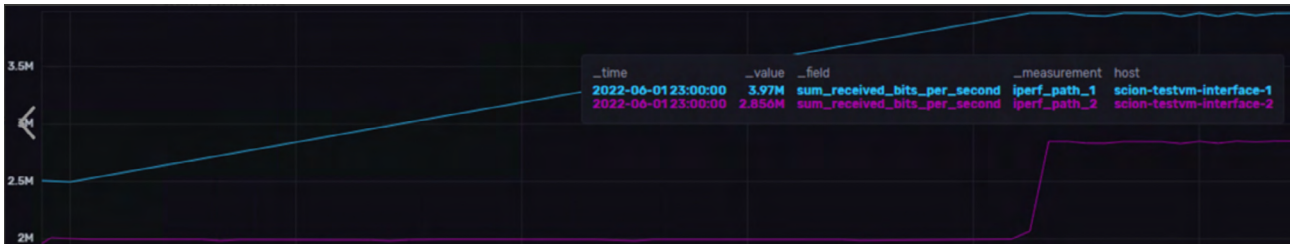
Test-scenario:

Validating that traffic can be sent over two paths simultaneously and validating that traffic can be controlled individually (throughput and routes)

1. California (USA) to Bern (CH) over Swisscom's SCION enabled IP-Plus
2. California (USA) to Bern (CH) over InterCloud's SCION backbone

Test results:

In the below charts we see how metrics of both connections are changing by making modification to through-put (from: 2MB/s and 2.5MB/s, to: 3MB/s and 4MB/s)



Below is a metric collection of both paths with derivation, most likely linked to last-mile interference:

Findings:

The test scenarios and infrastructure are not ideal to find meaningful insights into whether the Internet or SCION based connectivity are faster. However, it does show the amount of configuration flexibility that can be achieved with SCION when it comes to route and traffic control.

Conclusion

Swisscom set out the task to create a PoC environment to showcase and prove that SCION technology is superior to the traditional Internet for international connectivity.

Our conclusion of the PoC we have run are as follows:

1. Comparing regular Internet speeds can be difficult. However, the metric collection over a long period of time shows SCION to be more stable in general and at least on par with Internet speed.

   But the PoC can't conclude or disprove this for various reasons (load, dedicated hardware, scope, last-mile connectivity).

   What was confirmed during the PoC and validated is that SCION and BGP can co-exist. Having SCION enabled routers in the backbone will give the ability to enable SCION and then pass the packets to "normal Internet" (BGP) as "last-mile" and vice-versa.

2. SCION can be configured in various ways to:

   - **Include or exclude routing paths** -This can be used to avoid certain jurisdictions and comply with privacy declarations.
   - **Send out traffic over two different paths in parallel with the same source and destination** - This isn't possible with BGP on a global scale and can theoretically increase the throughput.
   - **Throttle the throughput of a given path** - Another configuration that BGP can't support
   - **Set up failover decisions upfront** - leading to instantaneous path failover. While BGP would make packets drop until a scheduled task is run to update the routing tables.

Picture above shows: Path configuration, throttling throughput 2.) Sending traffic over two paths at the same time)

swisscom InterCloud ANAPAYA

Red line: Measures the SCION connectivity from Swisscom Cloudlab (California) to Intercloud (Paris) configured to use InterCloud's backbone.

Blue line: Measures the SCION connectivity from Swisscom Cloudlab (California) to Intercloud (Paris) configured to use InterCloud's backbone (preferred) and Swisscom's backbone (secondary).

Orange line: Measures the amount of ping requests that were lost when using InterCloud's backbone (connection became unstable)

Purple line: Measures the amount of ping requests that were lost when using Swisscom's backbone to go from Swisscom Cloudlab (California) to InterCloud (Paris).

Picture above shows a failover test with instant failover to secondary path after the preferred path became unstable (manual interference).

About Swisscom

Swisscom is the leading telecommunications company and one of the leading IT companies in Switzerland. The Swisscom Enterprise Customers business unit is the largest integrated ICT provider for major customers in Switzerland. Swisscom is uncompromisingly geared towards customer needs, focuses on service and quality, and invests massively in the networks of the future.

The network of tomorrow is virtualized, omnipresent and secure with high performance. The global network between people, organisations, machines, and things is the most important driver for modern, economic, and social development. For this, Swisscom offers complete solutions for mobile working and telephony, secure solutions for corporate networks, Internet, and telephony as well as global network solutions together with our partners. Swisscom is highly interested in increasing the security of communications on the Internet, is offering the SCION technology to its customers and continues to actively support the further development of SCION technology.

About Anapaya Systems

Anapaya Systems, a spinoff of ETH Zurich, develops and supports an industrial-grade implementation of SCION and builds the SCION-Internet, the international ecosystem of service providers enabled with this protocol.

With cybercrime on the rise and individual incidents costing businesses and service providers tens of millions of dollars each to resolve, the time is right for the next evolutionary step in the Internet.

Anapaya and its partnering Service Providers offer today the next-generation Internet: reliable, secure and trustworthy. Multinational companies, regulated industries such as financial services, healthcare, public sectors and other industries can now regain a real control on where their sensitive data goes, and how it gets there.

About InterCloud

InterCloud is a leading Software-Defined Cloud Interconnect (SDCI) provider that transforms global connectivity, reduces network complexity and accelerates growth and innovation for global business – securely, quickly and easily. Its end-to-end global connectivity platform eliminates the complexity of deploying the cloud, giving businesses full control over the security, sovereignty and performance of their critical data traffic with complete peace of mind. The company's platform is underpinned by its team of cloud experts who guide customers to implement effective strategies to leverage the power of the cloud across their organization – giving customers the ultimate peace of mind that their business will be fit for the future.

Public document · 02.23 · ANA-23:0000.EN | V1.0