Aalto University
School of Electrical Engineering

Master's Thesis Presentation

Cooperative Firewall Signaling over SCION

Author: Dheeraj Chandrashekar
Advisor: Maria Riaz
Supervisor: Raimo Kantola

Communication Engineering
Department of Communication and Networking
School of ELEC, Aalto University

Table of contents

Aalto University
School of Electrical
Engineering

Background and Motivation

Internet

It has evolved at an unprecedented scale and has exceeded initial expectations in terms of capacity, usage, applications and services.

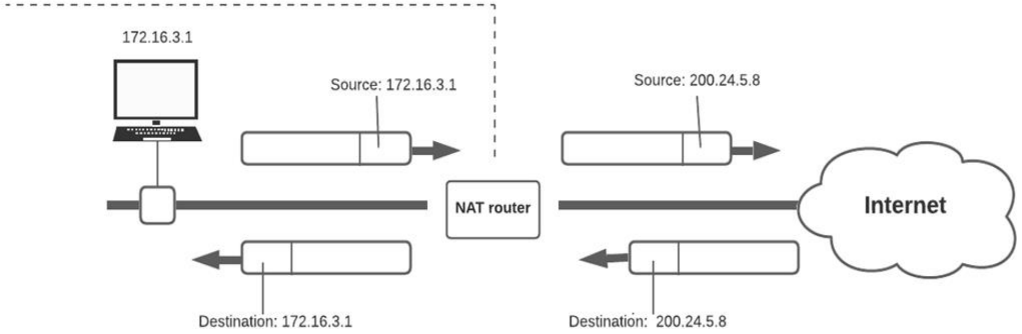
→ New technologies such as 5th Generation (5G) and Internet of Things have contributed to the rise in connected devices.

→ The increase in connected devices has exhausted the available IP addresses used for the purpose of communication.

→ RIPE NCC has announced that they have officially exhausted the available set of IPv4 addresses on 25th Nov.

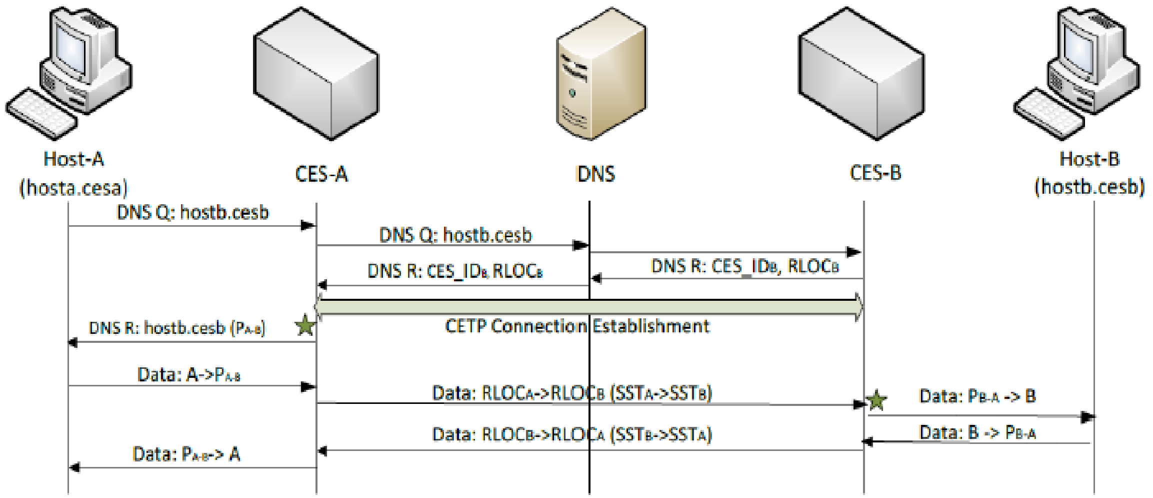
→ Internet Protocol version 6 (IPv6) and Network Address Translation (NAT) are two prominent solutions.

→ While IPv6 is proposed as the long-term solution despite implementation challenges, NAT solution is preferred due to simplicity and minimal implementation efforts.



- NAT was successful in overcoming the IPv4 address exhaustion to some extent.
- However, it suffered from a reachability problem when a host located in the public network tried to reach another in a private network, where no mapping exist.
- Many solutions were proposed to address reachability issue but failed to be promising.
- Customer Edge Switching (CES) is a cooperative firewall solution proposed as an extension and replacement to a traditional NAT—developed at Aalto University by the research group lead by Prof. Raimo Kantola under the department of COMNET.

Customer Edge Switching (CES)



- CES follows a trust-to-trust communication model to provide global connectivity for hosts in private networks.(mainly devices such as IoT in the edge nodes)
- Security in CES relies on the trust relation created between the network nodes based on the parameters exchanged during the session establishment stage.
- CES enforces a cooperative behavior between hosts within a network served by CES nodes. These nodes act as a connection broker by executing host policies.

CES node depend on a new protocol named Customer Edge Traversal Protocol (CETP) that is not standardized.

CES supports the idea of Identity (ID) for end hosts, routing locator (RLOC) split for routing packets. FQDN is used as ID and proxy addresses as RLOC.

CETP service discovery: figure out if the remote end supports CES with the help Naming Authority Pointer (NAPTR) DNS query and perform cooperative firewall functions towards the destination.

CETP policy negotiation: outbound CES node initiates a three-layered signaling channel – transport, CES-to-CES and host-to-host.

CES nodes allocate a proxy address to represent the remote host within their private network. They also insert flows to the OpenvSwitch, which aids in tunneling the data across the network.

The originating CES node would respond to its host with the proxy address of the remote end and any further communication would use these proxy addresses of the hosts.

CES and IP vulnerabilities

- CES solves the issue of NAT reachability and CES's CETP provides a range of tools to effectively ward off some of the security issues such as ID spoofing, spamming, SYN flooding and MitM attacks.
- CES firewall is backwards compatible with legacy Internet, via NAT and Realm Gateway (RGW) functions that provides application layer filtering with the help of Application Layer Gateway (ALG).
- However, it is still prone to the menaces plaquing the current internet like BGP route hijacking, DDoS attacks and network congestion.
- Root cause of these problems are the use of old protocols such as BGP and IP which have many shortcomings.
- Many ideas for having a new Internet architecture are proposed that is better than the current one.
- SCION (Scalability, Control, and Isolation on Next-Generation Networks) is one such Internet architecture.

Attacks	Routed IP	SCION
Source address authentication	✔	✗
Packet manipulation attacks	✔	✗
Man-in-the-middle attacks	✔	✗
Link DDoS	✔	✗
Address spoofing	✔	✗
Network layer DDoS	✔	✗
Prefix hijacking	✔	✗
Bandwidth exhaustion	✔	✗
Layer 3 DDoS	✔	✗
Outages due to unavailability	✔	✗
Packet replication attacks	✔	✔
Application-layer DoS attacks	✔	✔

- SCION provides defense against trivial attacks by design.
- SCION focuses on security and high availability for point-to-point communication.

SCION

SCION is a clean-state Internet architecture designed to provide highly available and effective point-to-point packet delivery, even in the presence of malicious attackers in the network.

The SCION infrastructure constitutes a network of globally connected Autonomous System (AS) and utilizes an isolation domain (ISD) as its fundamental building block.

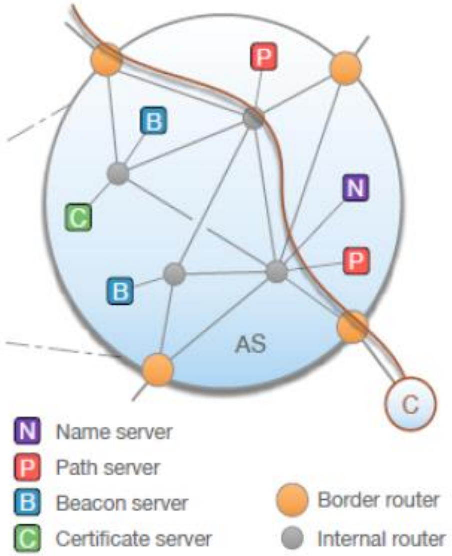
Path exploration phase: Every connected AS within the SCION network would find the cryptographically protected AS-level path information relating to its neighboring ASes.

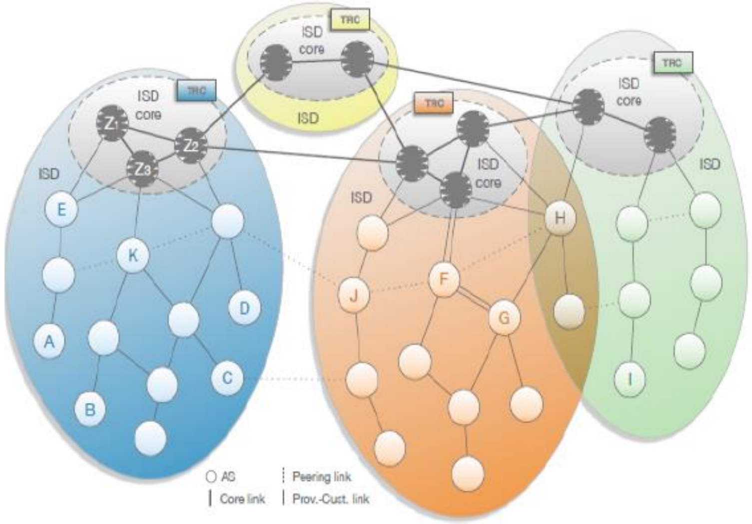
Path registration phase: Discovered path information is registered as Path segments with a dedicated SCION native Path server.

Path lookup phase: End host would get the path segments from the path server and construct a forwarding path to the destination in the path combination phase.

The path information from the source to destination is encrypted placed in the SCION packet's header that traverses the network.

Many ISPs and banks are already using the production version of SCION. Even the Swiss Government utilizes SCION for some of its services, promoting SCION's trust.





CES over SCION

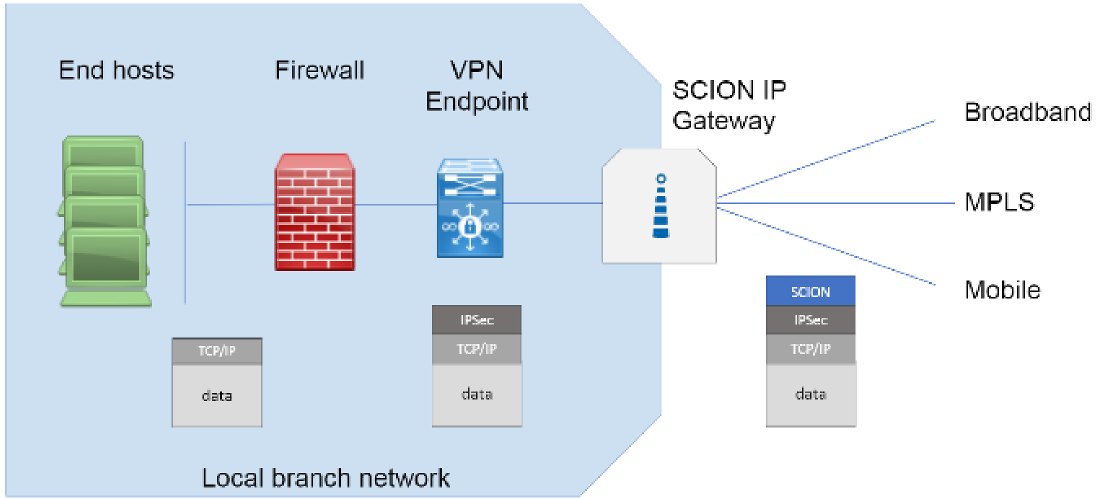
SCION supports SCION-IP gateway (SIG) which enables SCION to interoperate with the legacy IP end hosts benefitting them with SCION infrastructure.

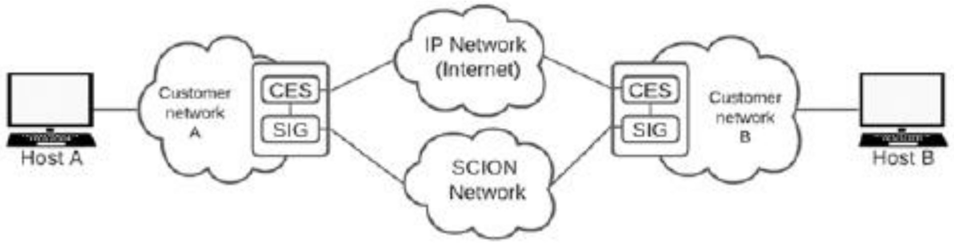
SCION does not provide any defensive mechanism for application-layer DoS attacks.

CES works on the principle of trust-based communication end-to-end and acts as a cooperative firewall preventing application-layer attacks.

Executing the CES solution over the SCION network provides the combined benefits of the SCION network and CES's protection against the application-layer DoS attacks.

Since Control/signaling traffic is critical and CES already uses proxy addresses for data plane, SIG is used only for Signaling traffic.





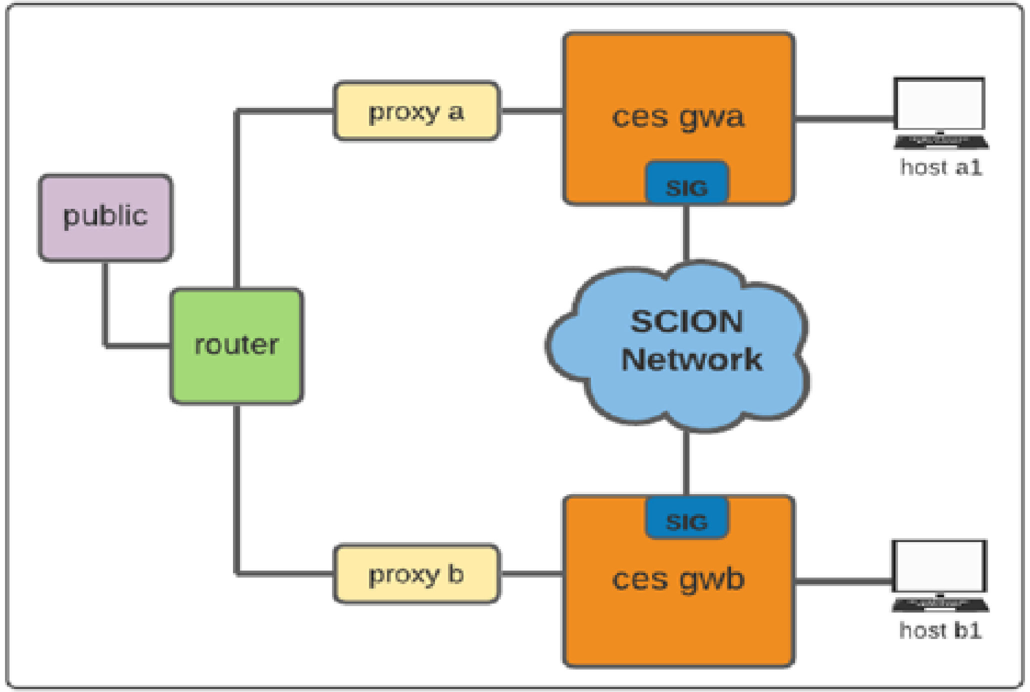
Aalto University
School of Electrical Engineering

Problem Statement:

Add new functionality to the CES firewall solution where the signaling traffic is switched from routed IP (normal Internet) to the SCION network whenever available, using SCION's native SCION-IP-Gateway application.

Methods

Linux container orchestration



Existing CES orchestration is updated to support SCION AS. Each node is a Linux container running Ubuntu 18.

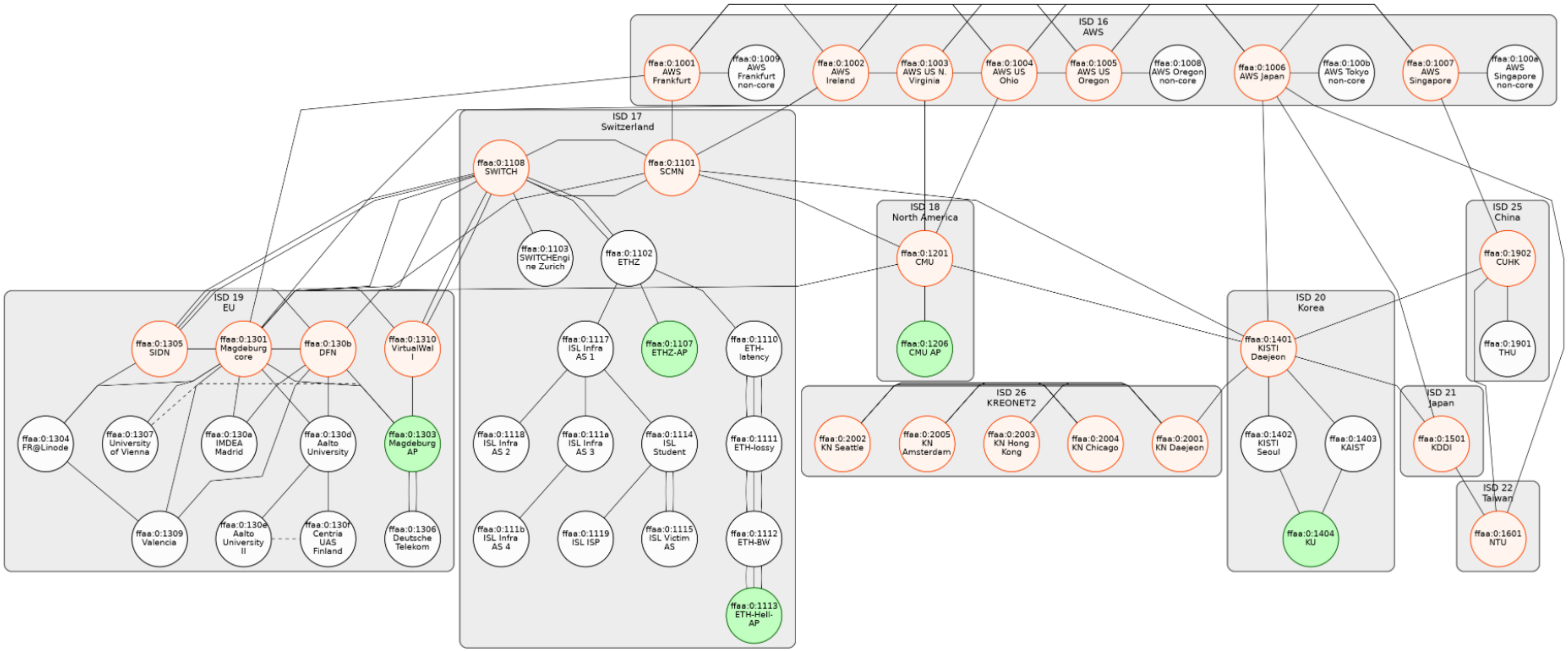
SCIONLab Network is a global research network designed to test and experiment with the SCION architecture.

The SCIONLab infrastructure comprises a network of globally connected Autonomous Systems (ASes).

SCION AS can be created by using the service provided by the SCION Lab team named as User AS.

A User AS can be created by mentioning an attachment point connecting to an already existing SCION AS present in the SCION research network.

SCIONLab research network



Aalto University
School of Electrical
Engineering

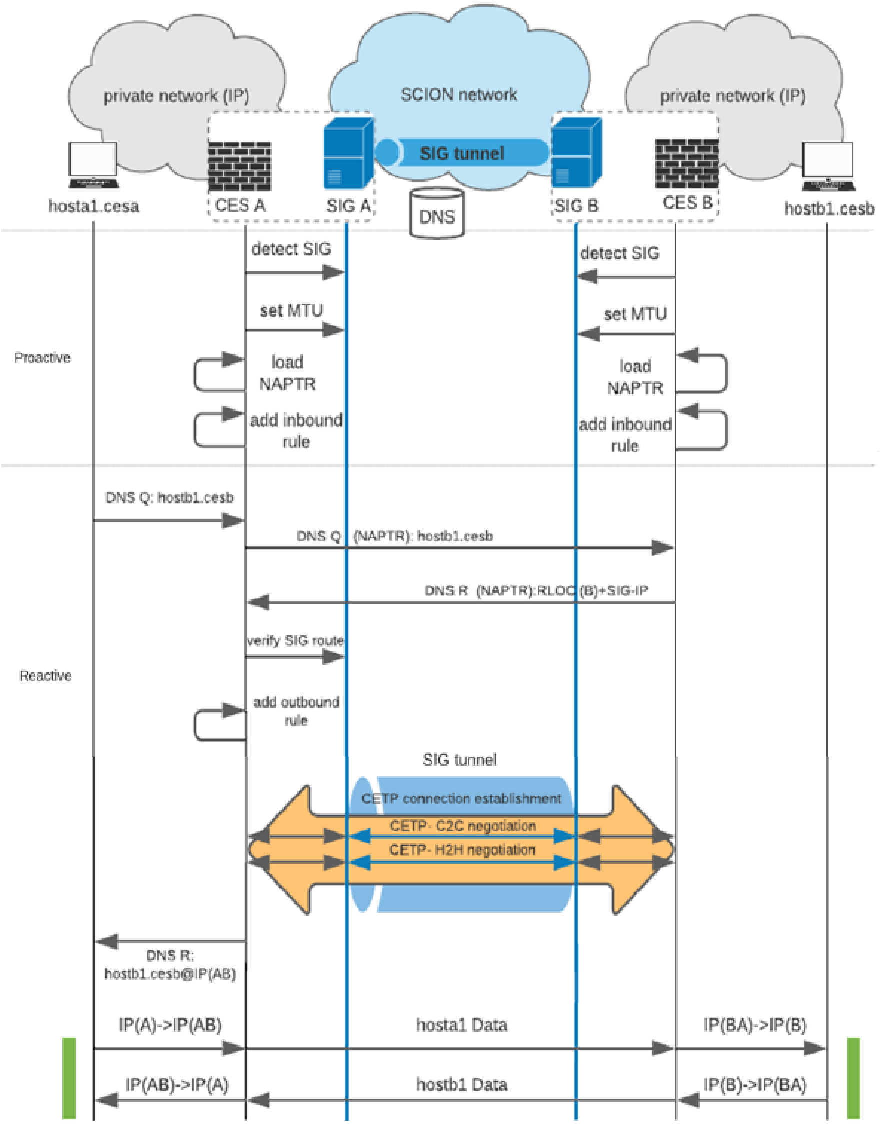
Implementation

CES code

The implementation of the proposed solution involves modifying the CES code base to recognize SIG and switch signaling traffic over to the SCION network. It is divided into three phases:

- **Proactive phase**: CES must receive host SIG IP from the configuration file. It must recognize SIG service running on the host and perform three actions namely: set MTU value on SIG interface, load the DNS NAPTR record with SIG-IP, and set an inbound rule to accept traffic from SIG.
- **Reactive phase**: Upon receiving a NAPTR response with SIG-IP, CES must check if a route exists to the remote SIG-IP. If a route exists, then CES must add an outbound rule pointing to the remote SIG-IP instead of remote CES-IP.
- **Monitor phase**: If the switch over was successful, CES must monitor the traffic flowing over SIG and prompt at regular intervals.

Scenarios such as connection error, mismatch configurations and unavailability of service can occur at any point during the implemented phases. The standard response to these scenarios is to clear the previous configurations of the switch over, and fall back to the default behavior i.e., communication over routed IP.



Aalto University
School of Electrical
Engineering

Results

Scenario based verification

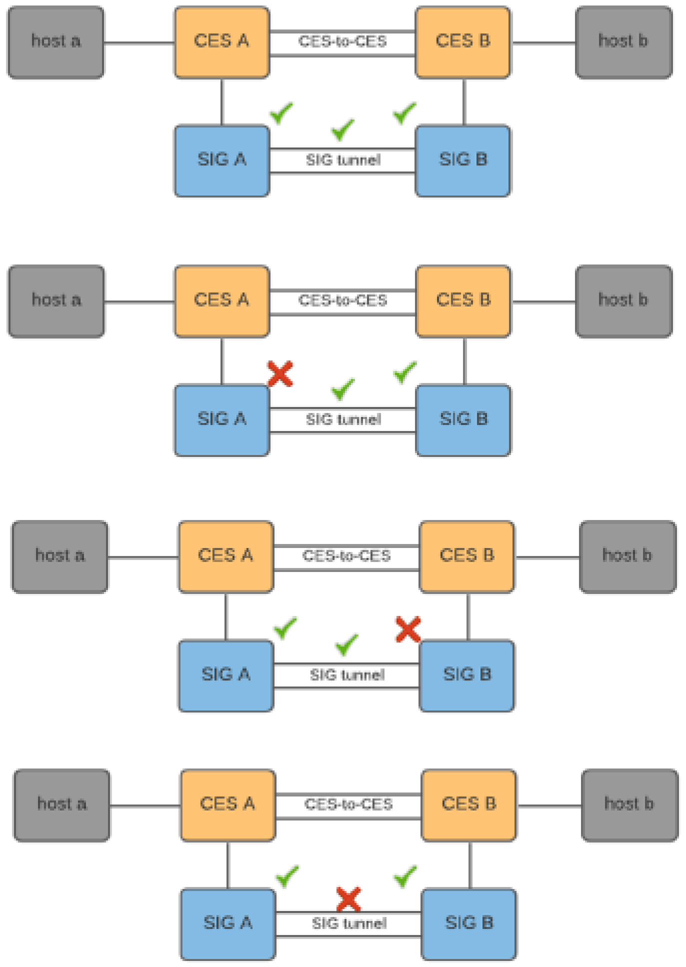
The implemented solution is expected to function smoothly and fall back to the default behavior in cases of discrepancies. Discrepancies can occur either from the host, remote end, or from the network.

Both SIGs are configured and reachable.

SIG A is Not configured/Not running.

SIG B is Not configured/Not running.

Both SIGs are configured but unreachable.



Packet visualization

CES-to-CES –> CES A

Source	Destination	Protocol	Info
100.64.1.130	100.64.0.1	DNS	Standard query 0xd5b8 NAPTR hostb1.gwb.demo
100.64.0.1	100.64.1.130	DNS	Standard query response 0xd5b8 NAPTR hostb1.gwb.demo NAPTR 100
100.64.1.130	100.64.0.1	DNS	Standard query 0xa1f5 NAPTR hostb1.gwb.demo
100.64.0.1	100.64.1.130	DNS	Standard query response 0xa1f5 NAPTR hostb1.gwb.demo NAPTR 100
100.64.1.130	100.64.2.130	TCP	30760 → 49001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
100.64.2.130	100.64.1.130	TCP	49001 → 30760 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=1460 SACK_
100.64.1.130	100.64.2.130	TCP	30760 → 49001 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=21187293
100.64.2.130	100.64.1.130	TCP	[TCP Window Update] 49001 → 30760 [ACK] Seq=1 Ack=1 Win=65152
100.64.1.130	100.64.2.130	TCP	22690 → 49003 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
100.64.2.130	100.64.1.130	TCP	49003 → 22690 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=1460 SACK_
100.64.1.130	100.64.2.130	TCP	22690 → 49003 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=21187293
100.64.2.130	100.64.1.130	TCP	[TCP Window Update] 49003 → 22690 [ACK] Seq=1 Ack=1 Win=65152
100.64.1.130	100.64.2.130	TCP	23834 → 49002 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
100.64.2.130	100.64.1.130	TCP	49002 → 23834 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=1460 SACK_
100.64.1.130	100.64.2.130	TCP	23834 → 49002 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=21187293
100.64.2.130	100.64.1.130	TCP	[TCP Window Update] 49002 → 23834 [ACK] Seq=1 Ack=1 Win=65152
100.64.1.130	100.64.2.130	TLSv1.3	Client Hello
…. TCP packets ……			
100.64.2.130	100.64.1.130	TLSv1.3	Application Data
100.64.1.130	100.64.2.130	TLSv1.3	Application Data
100.64.2.130	100.64.1.130	TLSv1.3	Application Data
100.64.1.130	100.64.2.130	TCP	30760 → 49001 [ACK] Seq=5924 Ack=6205 Win=64128 Len=0 TSval=211872
40.10.181.107	20.229.20.145	ICMP	Echo (ping) request id=0x0612, seq=1/256, ttl=63 (reply in 64)
20.229.20.145	40.10.181.107	ICMP	Echo (ping) reply id=0x0612, seq=1/256, ttl=63 (request in 63)
100.64.1.130	100.64.2.130	TCP	22690 → 49003 [ACK] Seq=3176 Ack=4747 Win=64128 Len=0 TSval=211872
40.10.181.107	20.229.20.145	ICMP	Echo (ping) request id=0x0612, seq=2/512, ttl=63 (reply in 67)
20.229.20.145	40.10.181.107	ICMP	Echo (ping) reply id=0x0612, seq=2/512, ttl=63 (request in 66)

CES signaling over SCION –> CES A

Source	Destination	Protocol	Info
100.64.1.130	100.64.0.1	DNS	Standard query 0xee77 NAPTR hostb1.gwb.demo
100.64.1.130	100.64.0.1	DNS	Standard query 0x0f36 NAPTR hostb1.gwb.demo
100.64.0.1	100.64.1.130	DNS	Standard query response 0x0f36 NAPTR hostb1.gwb.demo
100.64.0.1	100.64.1.130	DNS	Standard query response 0xee77 NAPTR hostb1.gwb.demo
150.221.76.201	2.114.82.182	ICMP	Echo (ping) request id=0x058b, seq=1/256, ttl=63 (re
2.114.82.182	150.221.76.…	ICMP	Echo (ping) reply id=0x058b, seq=1/256, ttl=63 (re
150.221.76.201	2.114.82.182	ICMP	Echo (ping) request id=0x058b, seq=2/512, ttl=63 (re
2.114.82.182	150.221.76.…	ICMP	Echo (ping) reply id=0x058b, seq=2/512, ttl=63 (re

CES signaling over SCION –> SIG A

Source	Destination	Protocol	Info
11.0.0.1	12.0.0.1	TCP	55188 → 49001 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSva
11.0.0.1	12.0.0.1	TCP	19774 → 49003 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSva
11.0.0.1	12.0.0.1	TCP	22348 → 49002 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSva
12.0.0.1	11.0.0.1	TCP	49001 → 55188 [SYN, ACK] Seq=0 Ack=1 Win=64896 Len=0 MSS=1260 SACK_
11.0.0.1	12.0.0.1	TCP	55188 → 49001 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=630219423 TSe
12.0.0.1	11.0.0.1	TCP	49003 → 19774 [SYN, ACK] Seq=0 Ack=1 Win=64896 Len=0 MSS=1260 SACK_
11.0.0.1	12.0.0.1	TCP	19774 → 49003 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=630219423 TSe
12.0.0.1	11.0.0.1	TCP	49002 → 22348 [SYN, ACK] Seq=0 Ack=1 Win=64896 Len=0 MSS=1260 SACK_
11.0.0.1	12.0.0.1	TCP	22348 → 49002 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=630219423 TSe
11.0.0.1	12.0.0.1	TLSv1.2	Client Hello
11.0.0.1	12.0.0.1	TLSv1.2	Client Hello
11.0.0.1	12.0.0.1	TLSv1.2	Client Hello
12.0.0.1	11.0.0.1	TCP	49001 → 55188 [ACK] Seq=1 Ack=518 Win=64384 Len=0 TSval=3698352536
12.0.0.1	11.0.0.1	TCP	49003 → 19774 [ACK] Seq=1 Ack=518 Win=64384 Len=0 TSval=3698352536
12.0.0.1	11.0.0.1	TCP	49002 → 22348 [ACK] Seq=1 Ack=518 Win=64384 Len=0 TSval=3698352536

CETP connection establishment

CETP connection delay

- The CETP connection establishment occurs between two CES nodes. Hence, the hosts connected to them are unaware of whether the traffic is routed over IP or SCION.
- To measure the delay introduced by the CES-to-SCION switchover, the time difference between the DNS query and the DNS response of the host is calculated.
- Delay is calculated for both the scenarios: CES-to-CES and CES Signaling over SIG.

Case	Delay
CES-to-CES	0.04sec
CES Signaling over SIG	0.67sec

CETP policy

The SIG-to-SIG connection between two nodes confirms the authenticity of the hosts running them (Only if both CES and SIG are run on the same host).

- CES validation can be skipped when SIG is available. Due to this, CA parameters from the policies can be eliminated.
- SIG itself provides encapsulation, thereby making it possible to avoid encrypting CETP messages.
- CETP can include payload with the SIG option, providing the host an option to send data plane traffic over SIG. (Current implementation does not support this)

SCION-IP-Gateway performance

Round-Trip-Time

Packet count	Avg RTT	Loss %	Total time
1	112.76ms	0	0ms
5	100.78ms	0	4s
10	113.48ms	0	9s
15	112.46ms	0	14s
20	110.72ms	0	19s
50	117.05ms	0	49s

Bandwidth

Attempted BW(bps)	Achieved BW(bps)	
	C ->S	S ->C
1M	1M	0.99M
10M	9.83M	9.91M
50M	49M	49.5M
100M	98M	98.9M
200M	196M	198M
500M	490M	495M
1G	981M	990M
10G	9.92G	9.96G

Throughout the tests, the SIG tunnel was stable and provided uniform results.

Aalto University
School of Electrical
Engineering

Conclusion and Future work

Conclusion

- Customer Edge Switching (CES) is a firewall solution intended to replace the traditional NAT along with some extensions.
- CES can still be plagued by some of the common attacks present on the current Internet.
- SCION is proposed as a new Internet architecture, which provides defenses against some of the commonly seen attacks on the Internet by design.
- SCION provides a feature for the end-hosts in an IP network to connect to SCION using SCION-IP-Gateway.
- End-domains can benefit from the integration of CES and SCION, where CES provides host-level authenticity by cooperative behavior concept, and SCION can provide network-level security by design.
- Implementation of the solution is carried out in three phases: Reactive, Proactive and Monitor phases.
- Evaluation of the implemented solution is performed by a range of tests: design verification, packet visualization, CETP optimization and SIG performance

Future work

- Provide an option to CES, allowing it to switch not only Signaling traffic but any traffic of choice.
- CES can make use of the SIG-to-SIG trust and optimize the connection establishment procedures.
- End-host can mention in its policy to inform CES to use SIG for all traffic originating from that host.
- SCION ASes configured on the Linux containers use OpenVPN to connect to the parent AS, and this causes performance issues. OpenVPN can be eliminated if the SCION AS can have a publicly reachable IP address.
- SCION AP used in the solution is in Switzerland. Selecting a closer AP would perform well.
- Performing different types of attacks against the SIG and verifying its credibility.

Aalto University
School of Electrical Engineering

Questions ?