

SAVI Protocol Framework

draft-vogt-savi-framework

Christian Vogt

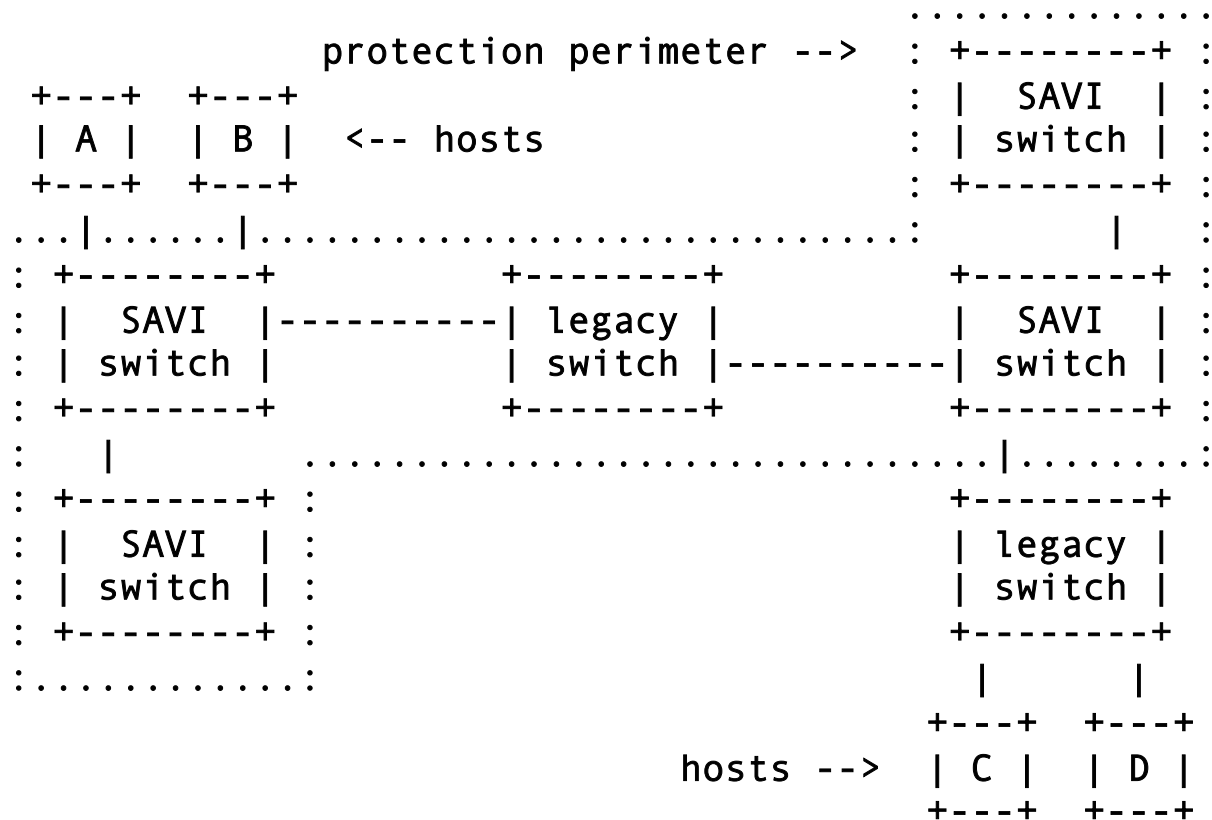
Outline of Document

- protocol model
 - requirements
 - validation approach
- scalability optimizations
 - protection perimeter
- deployment options
 - address assignment methods
 - binding anchor types

Protocol Model

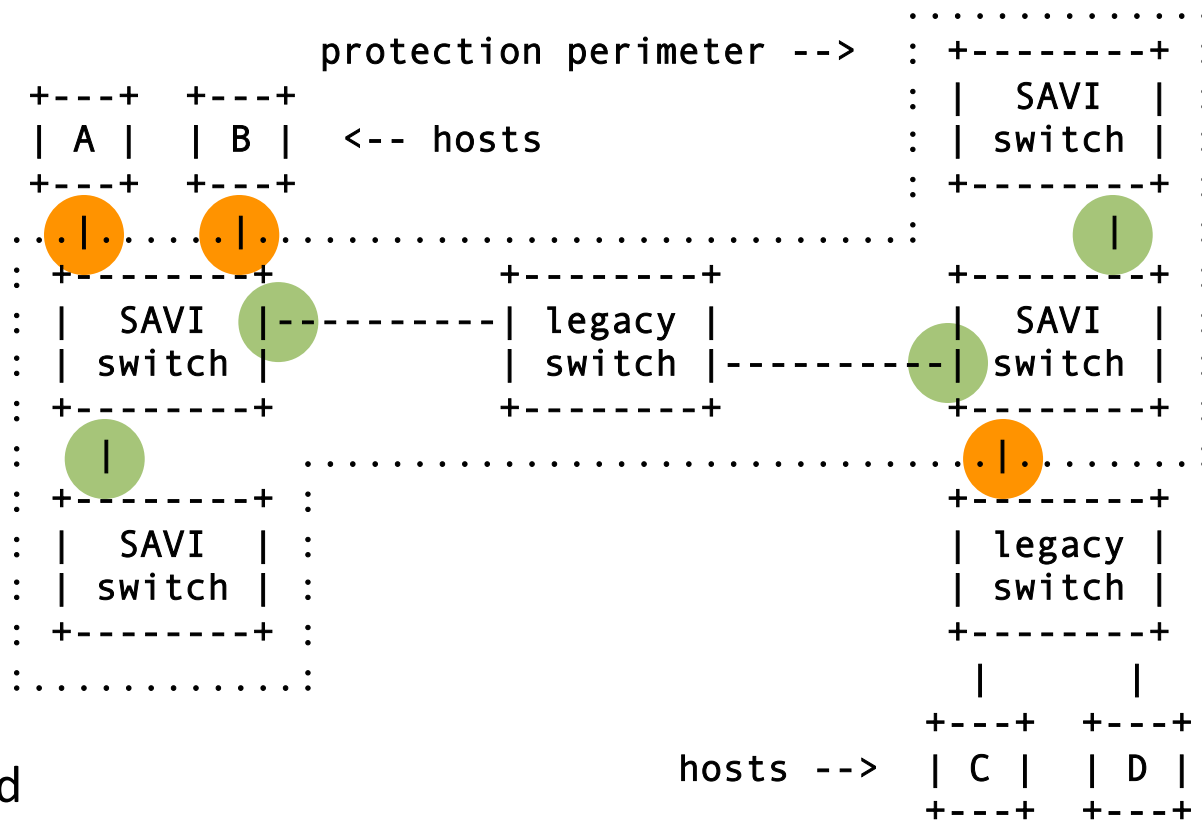
- network-based + on path of packets
- three-step validation
 1. identify legitimate addresses
 2. bind legitimate addresses to binding anchor
 3. enforce address legitimacy through binding anchor verification
- validate close to hosts
 - easier to guarantee on-path property
 - binding anchor easier to find
 - \Rightarrow validate on switch if possible

Scalability Optimizations



reduce memory requirements
on links with multiple SAVI devices

Scalability Optimizations



 untrusted

 trusted

reduce memory requirements
on links with multiple SAVI devices

Deployment Options

- SAVI partly deployment-specific
 - identification of legitimate addresses depends on address assignment
 - binding anchors depend on link layer
- requires modularity
- modules have different security properties
 - calls for deployment guidance
 - need to explain co-existence (prioritization)

Security Properties of Address Assignment Methods

address assignment method	examples
via address authority	DHCP
autonomous	SLAAC or manual configuration
autonomous with legitimacy proof	SeND

Security Properties of Address Assignment Methods

address assignment method	examples	security strength
via address authority	DHCP	spoofing impossible
autonomous	SLAAC or manual configuration	spoofing impossible for used addresses
autonomous with legitimacy proof	SeND	spoofing impossible

Security Properties of Binding Anchor Types

binding anchor method	examples
bound to network attachment	switch port
bound to attached host	MAC address
bound to legitimate user	SEND key, security association

Security Properties of Binding Anchor Types

binding anchor method	examples	security strength
bound to network attachment	switch port	strong
bound to attached host	MAC address	weak
bound to legitimate user	SEND key, security association	strong