Proxy-Shim6:
Shim6 deployment tools

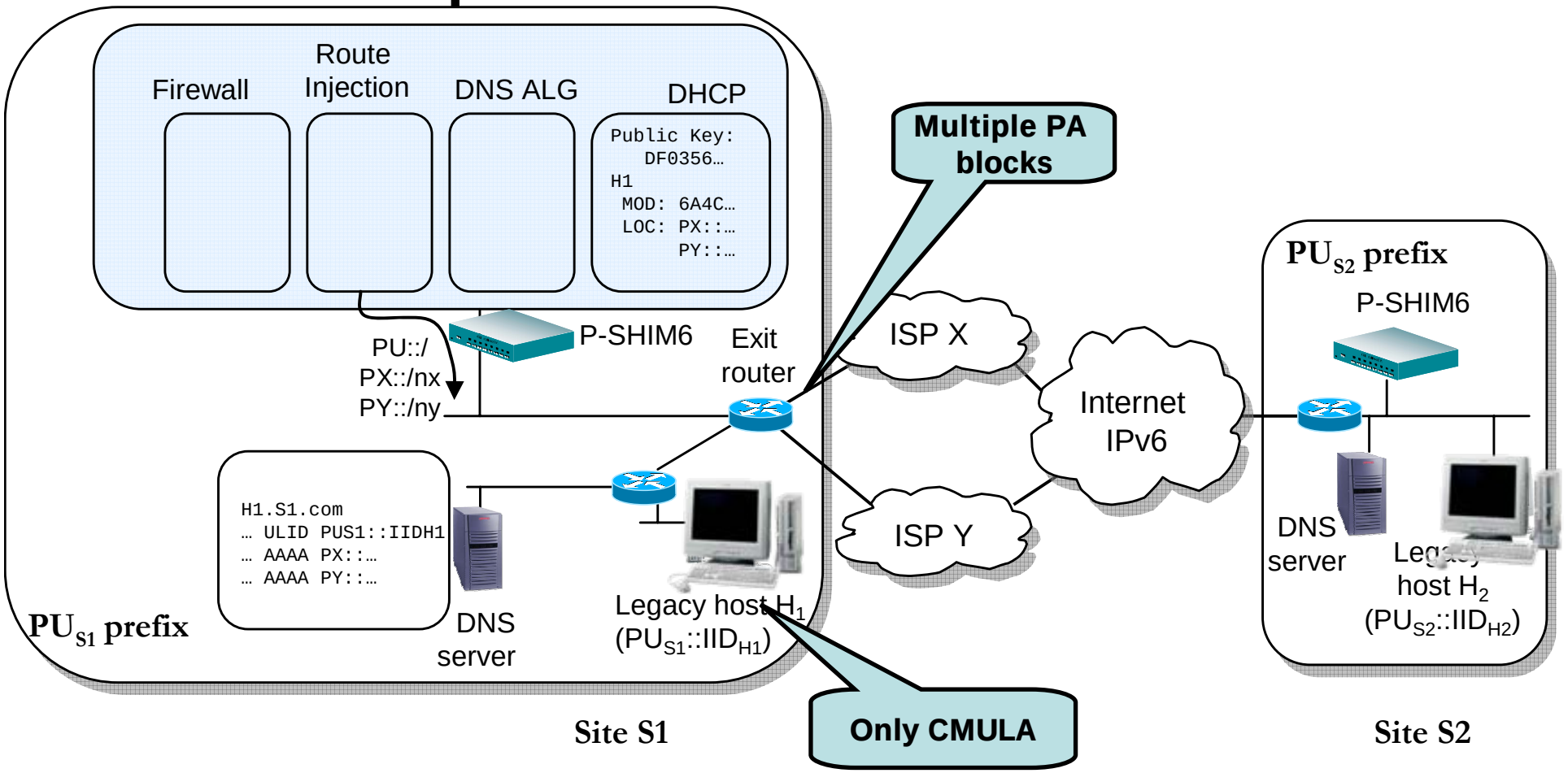
Marcelo Bagnulo

shim6 WG - IETF71

Shim6 Deployment blockers: Key features missing

- Allow off-loading of SHIM6 operation to specialised middle boxes
  - Enable legacy nodes to benefit from multihoming
  - Not require update to all hosts in the mh site
- Capabilities existent in current BGP multihoming missing
  - Portability of the address block
    - Avoid renumbering, that currently results in provider lock-in, available in exist
  - Traffic Engineering (TE) enforcement
    - With SHIM6 is difficult to enforce site-wide TE policies

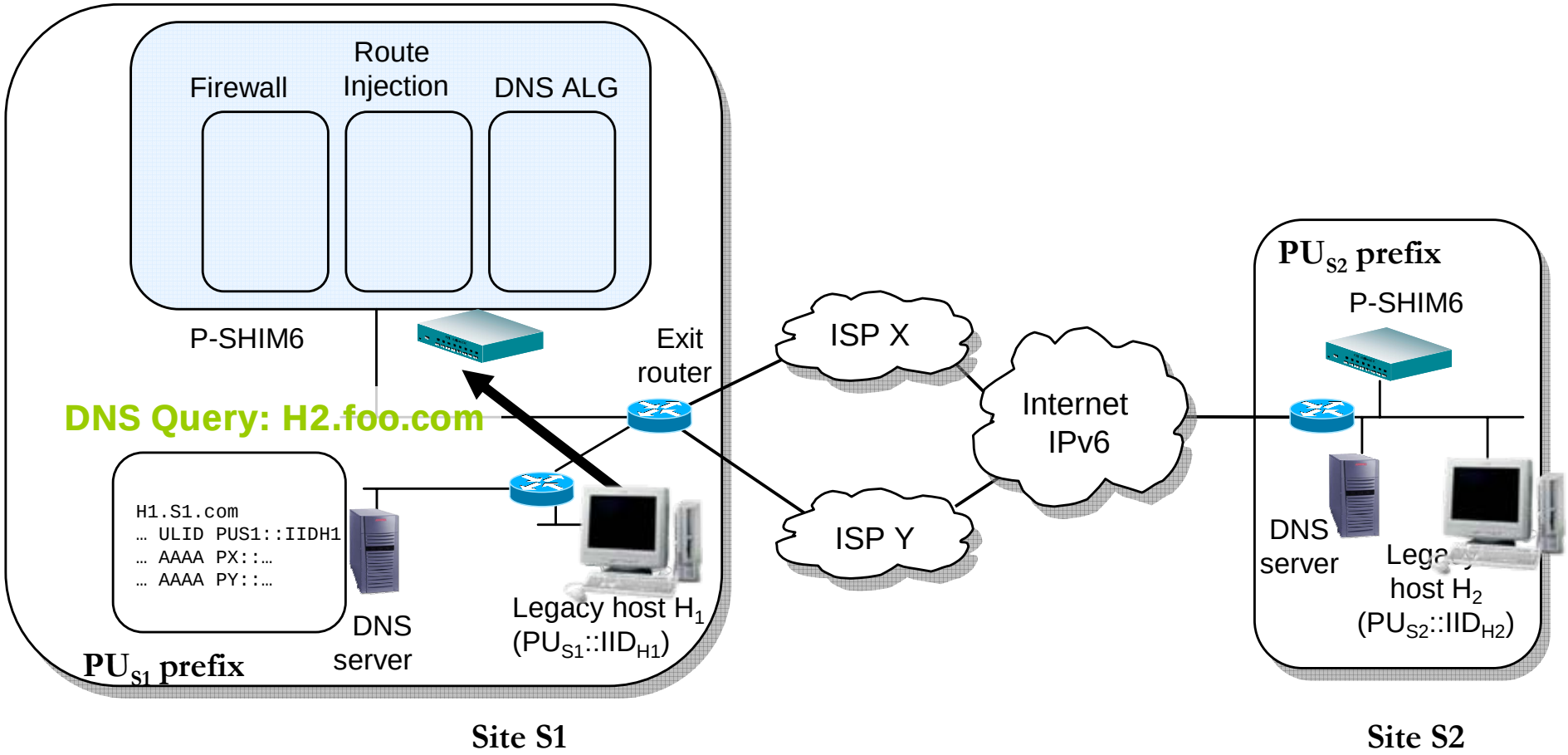
Proposed architecture



Proposed architecture

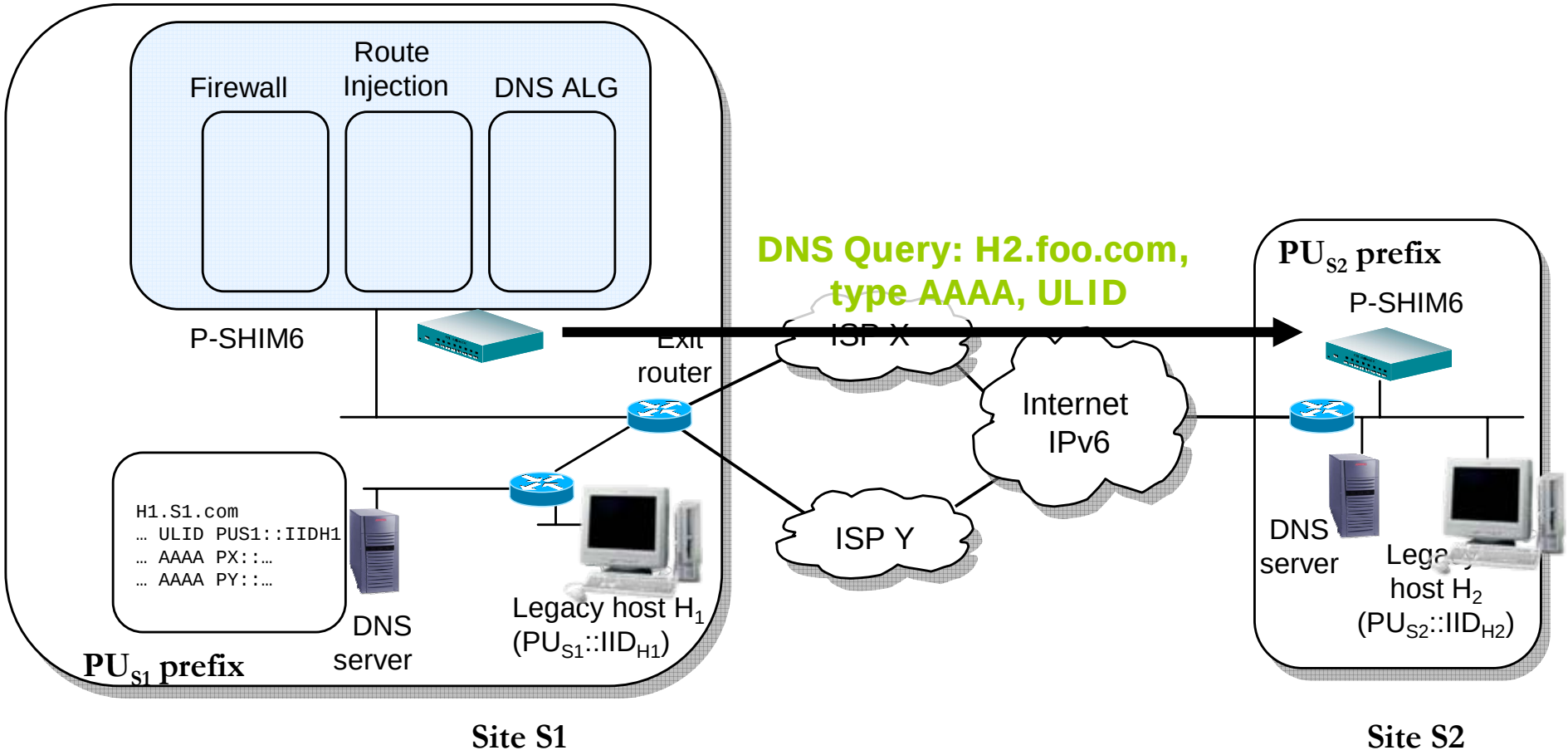
- *P-SHIM6* boxes execute SHIM6 on behalf of internal nodes
- Internal hosts are configured with CMULAs
  - Unique non-routable addresses
  - Objective: avoid internal renumbering when changing ISP
  - Interface Identifier obtained according to rules to built CGAs
- The DNS of the site
  - Show to external nodes
    - Provider Aggregatable addresses in AAAA records
    - CMULAs in a newly defined ULID record
  - Show to internal nodes
    - Local addresses (CMULAs) in AAAA records
- P-SHIM6 behaves as DNS-ALG, intercepting DNS requests
- P-SHIM6 attracks traffic (by IGP route injection)
  - To the generic CMULA prefix
  - To the PA prefixes of the site

P-Shim6 Operation



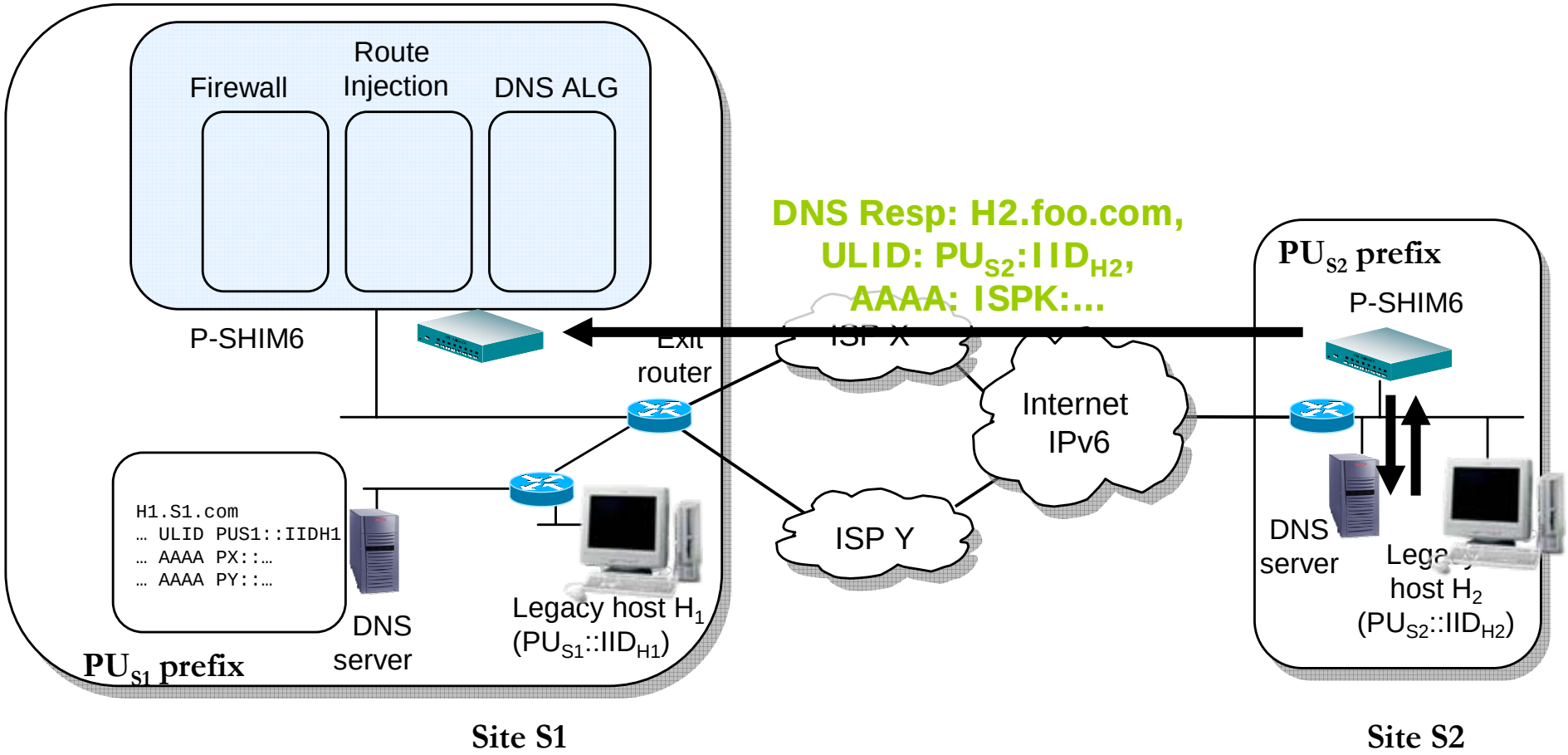
- H1 queries DNS for H2.foo.com
  - Sends query to P-SHIM6, configured as DNS-ALG

P-Shim6 Operation



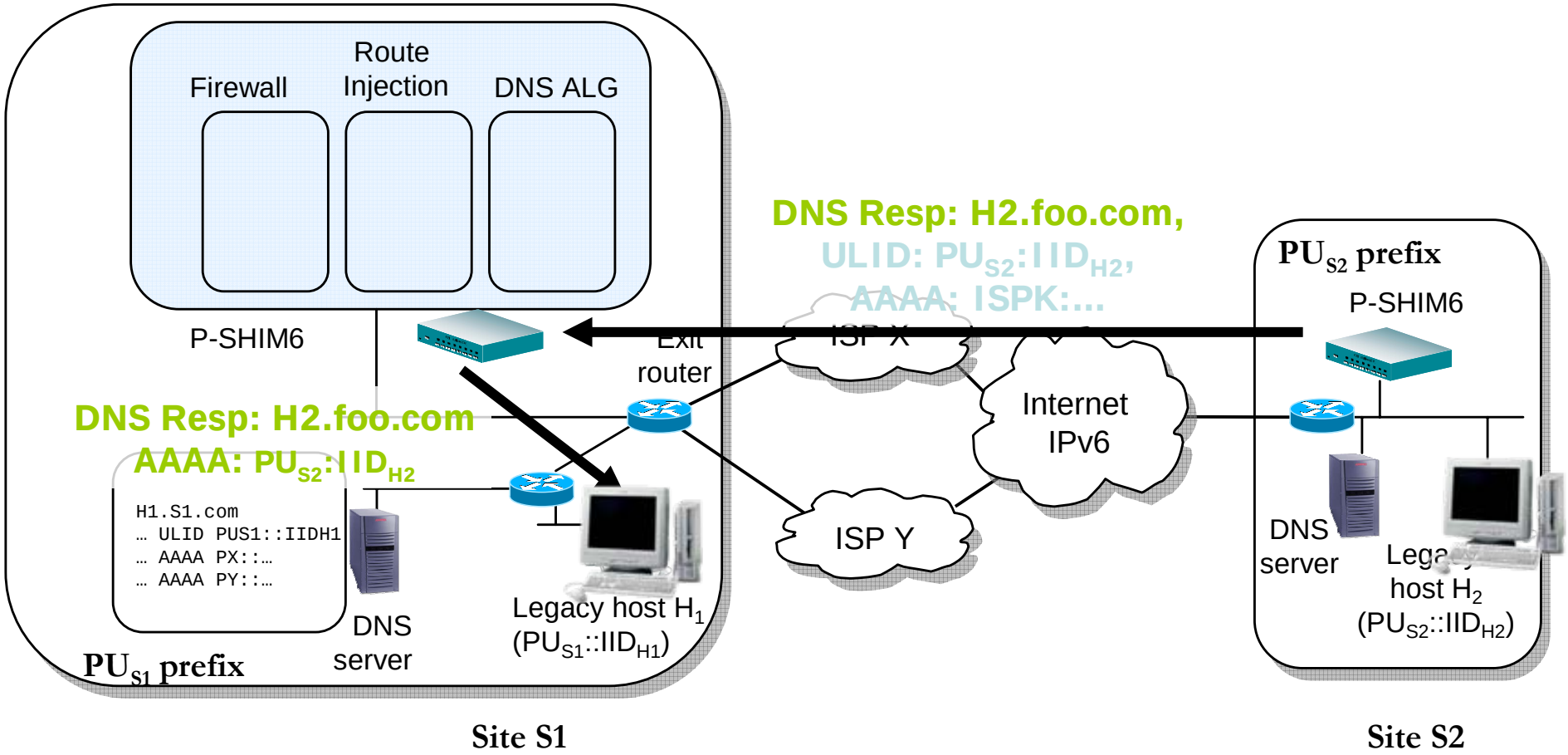
- P-SHIM6 (site S1) queries DNS server at site S2 for both AAAA and ULID RRs
- P-SHIM6 (site S2) intercepts DNS query

P-Shim6 Operation



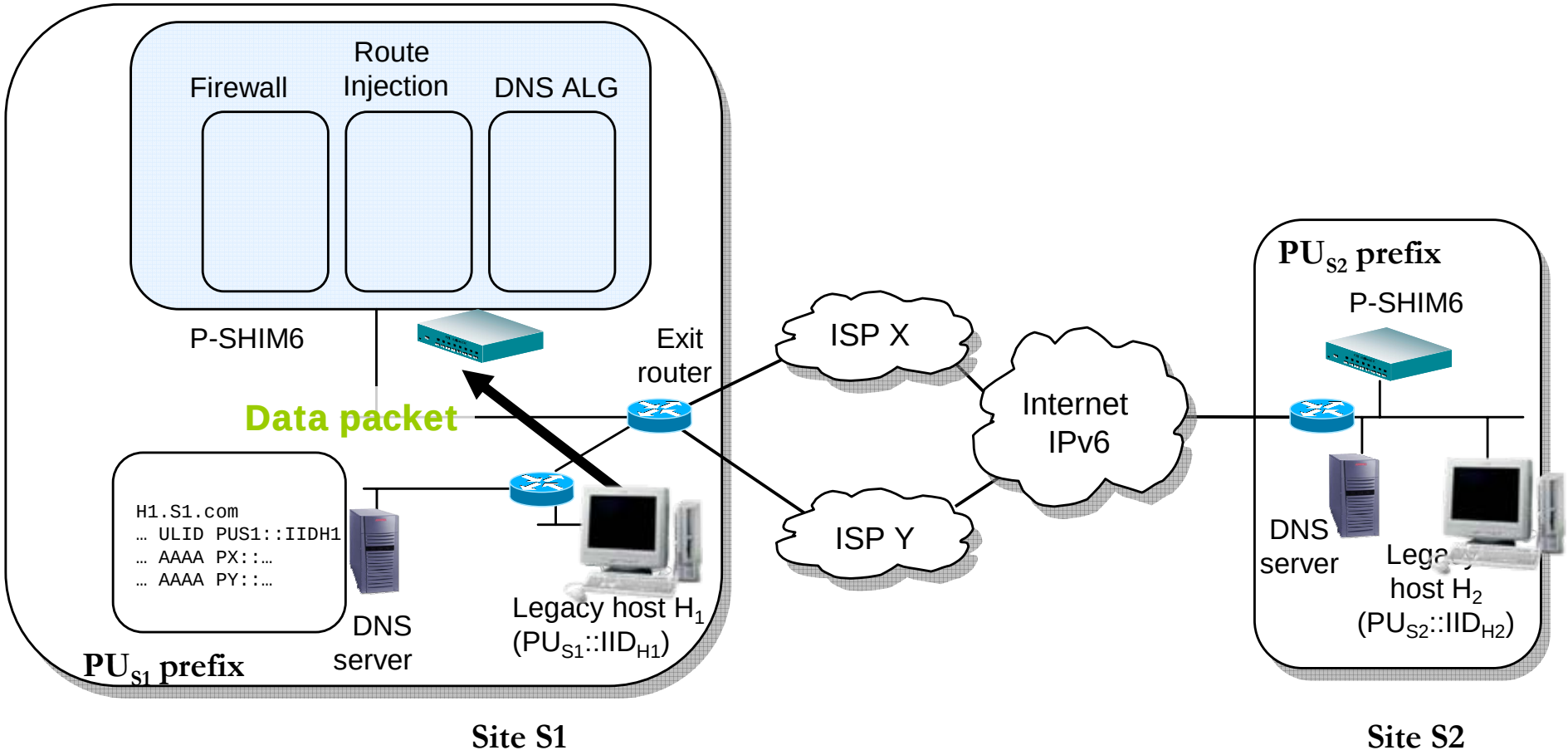
- P-SHIM6 (at S2) intercepts local DNS response

P-Shim6 Operation



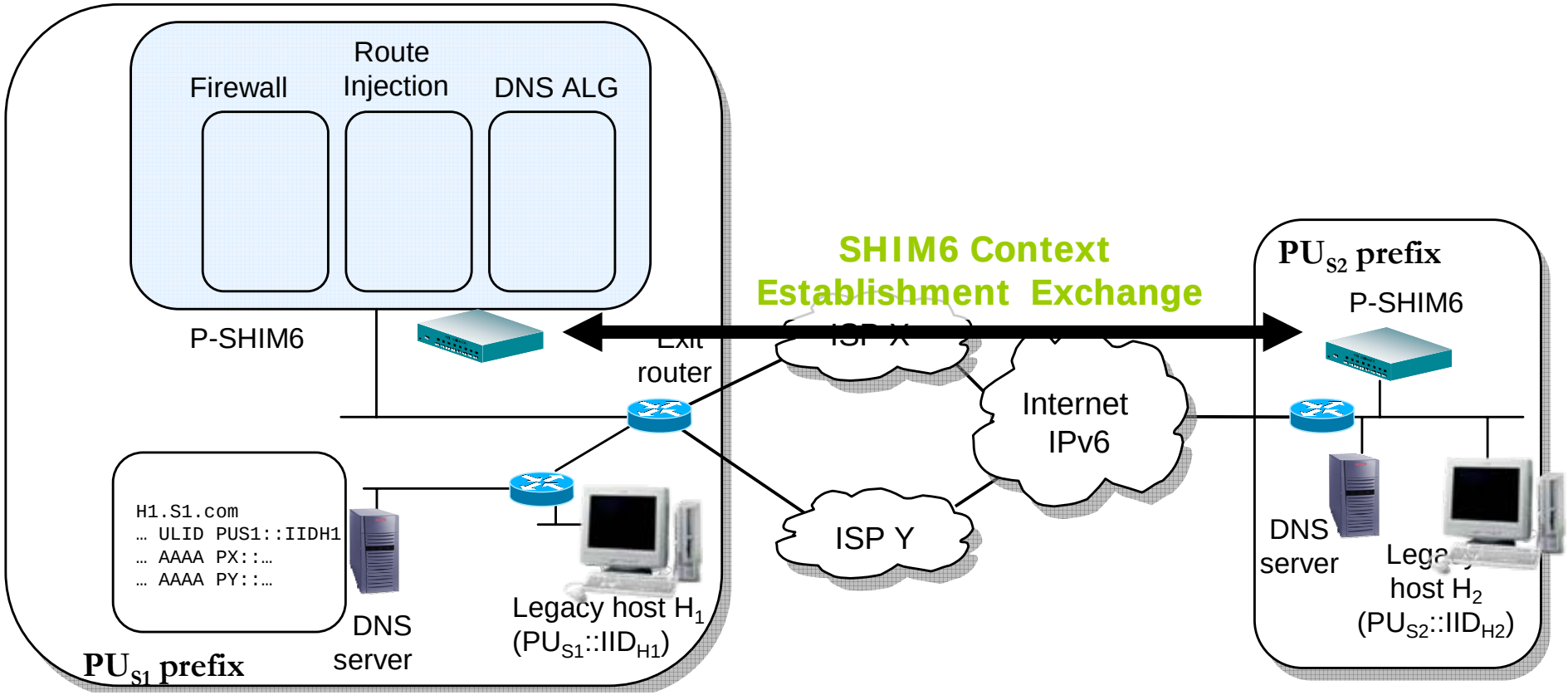
- P-SHIM6 (site S1) stores PA address, and sends ULID in AAAA to host H1

P-Shim6 Operation



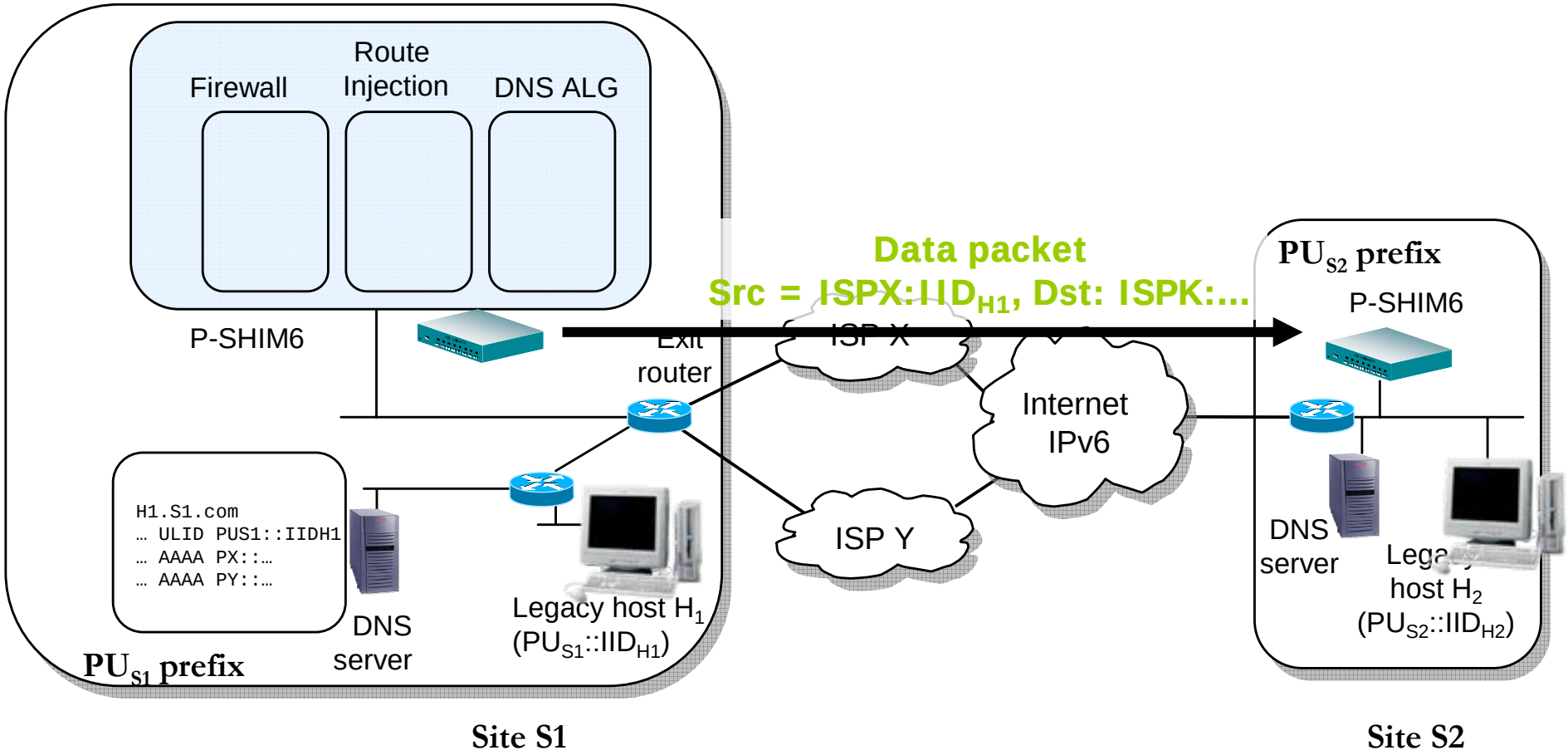
- H1 sends data packet with dst: $PU_{S2}:IID_{H2}$, source: $PU_{S1}::IID_{H1}$
  - P-SHIM6 receives packet

P-Shim6 Operation



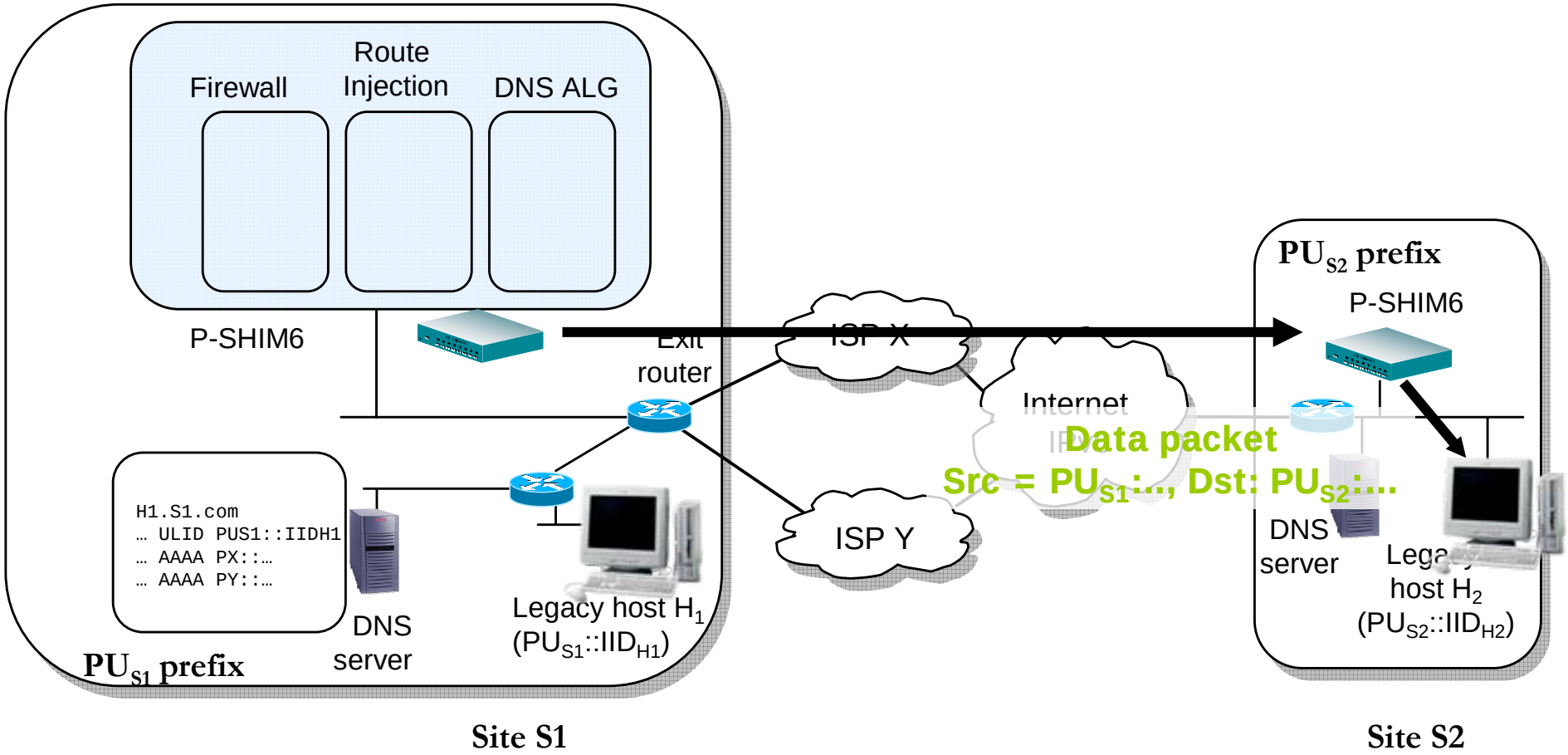
- P-SHIM6 (site S1) initiates a SHIM6 Context Establishment Exchange with P-SHIM6 (site S2)
  - Conveys local CMULA as identifier in the SHIM6 exchange
  - The locator address used as destination is PA remote address (ISPK:…)
    - Signed with public key associated to CMULA (that is a CGA)

P-Shim6 Operation



- Data packets traverse Internet IPv6 using PA addressing
- P-SHIM6 (site S2) attracks traffic sent to PA addresses

P-Shim6 Operation

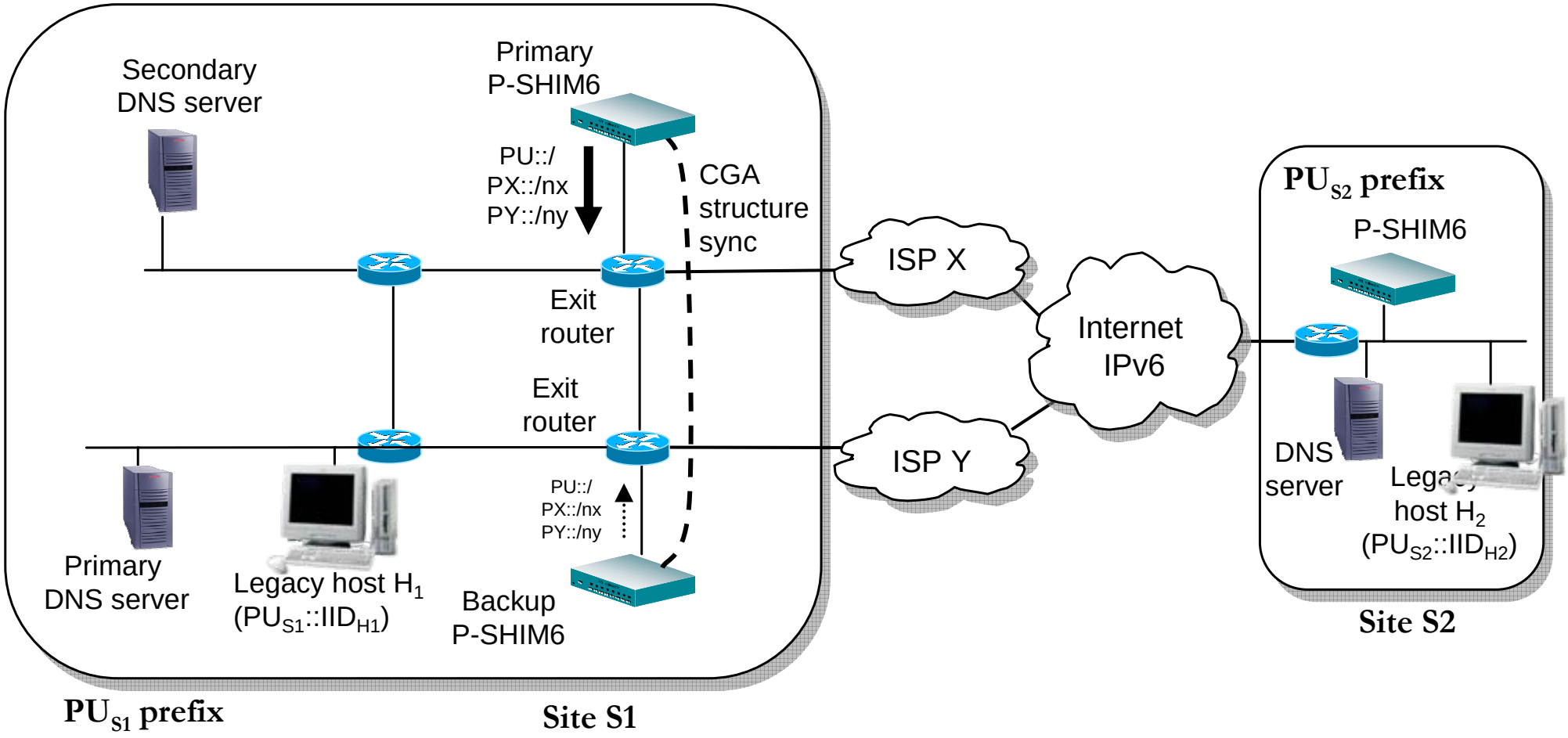


- P-SHIM6 (S2) changes addresses so that legacy host only sees CMULAs

Note that…

- Communications are protected against failures by SHIM6
- End points see the same addresses
  - P-SHIM6 do not need to rewrite application data
- P-SHIM6 are not used in intrasite communication
  - CMULAs can be used locally
- Reverse DNS is used to start a communication when direct DNS is not used
  - Host uses CMULA to initiate a communication
  - P-SHIM6 obtains PA addressing associated to the CMULA in the reverse DNS
- P-SHIM6 uses DHCPv6 to configure the CMULAs (CGAs) on each host
  - P-SHIM6 generates the address and manages the keys for the SHIM6 Context Establishment Exchange

Fault tolerance: multiple P-SHIM6



Fault tolerance: multiple P-SHIM6

- Primary / secondary configuration
  - Primary injects routes with higher preference, so it receives all traffic (until it fails)
- P-SHIM6s must share address configuration parameters
  - Keys for SHIM6 operation, CGAs
- On-going communications can be preserved
  - Incomming data packet with unknown Context Tag:
    - Use SHIM6 Context Recovery facilities to ask remote P-SHIM6 about the context lost
  - Outgoing data packet without existing context:
    - Ask reverse DNS to find addresses, initiate SHIM6 Context Establishment Exchange

Design choices

- A set of components are required exclusively due to address protabilify support, namely
  - CMULAs or similar
  - DNS ALG
  - New ULID RR
  - Firewall component
  - CGAs and not HBAs
  - If address portability is not needed, these components can be avoided
- Other repository (other than reverse DNS) could be used to recover locator information associated to lost sessions

Questions?