Institute for Internet Technologies and Applications

strongSwan News

Prof. Dr. Andreas Steffen

andreas.steffen@strongswan.org

Martin Willi

martin@strongswan.org

EIN INSTITUT DER

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Agenda

Institute for Internet Technologies and Applications

- What is strongSwan?
- News
  - High Availability solution using Cluster IP
  - Virtual IP pools and config attributes for IKEv1 and IKEv2
  - KDE 4 NM Plasma Applet and Android Port
- Outlook
  - Sharing daemon functionality with libhydra:
    pluto inherits kernel netlink interface and dynamic routing
  - EAP-TLS support and probably EAP-PEAP, EAP-TTLS, EAP-FAST
  - Network Endpoint Assessment (NEA, RFC 5209) using
    IKEv2 EAP as a transport protocol
- Questions and discussion

Institute for Internet Technologies and Applications

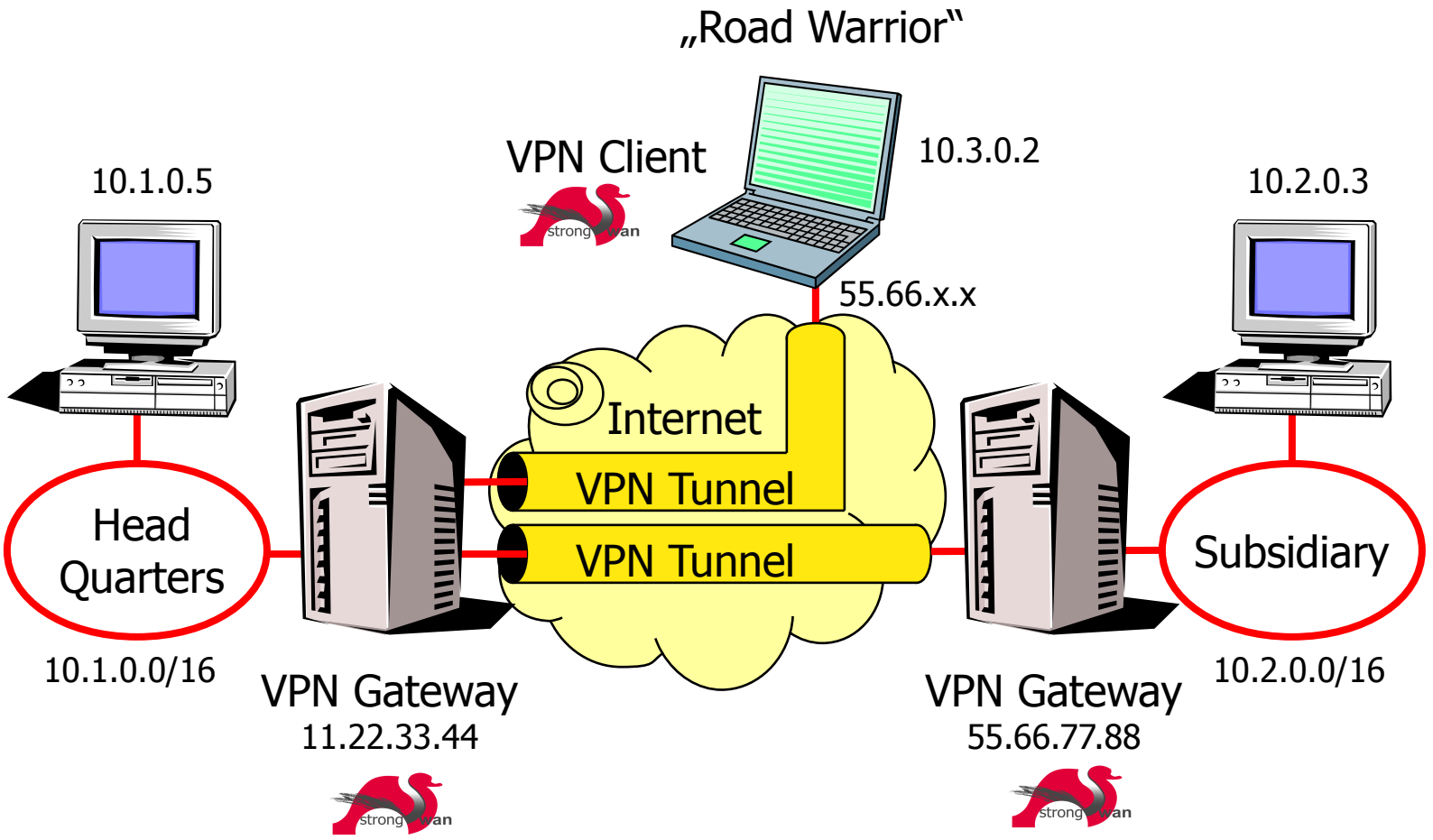
What is strongSwan?

EIN INSTITUT DER

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

VPN Usage Scenarios

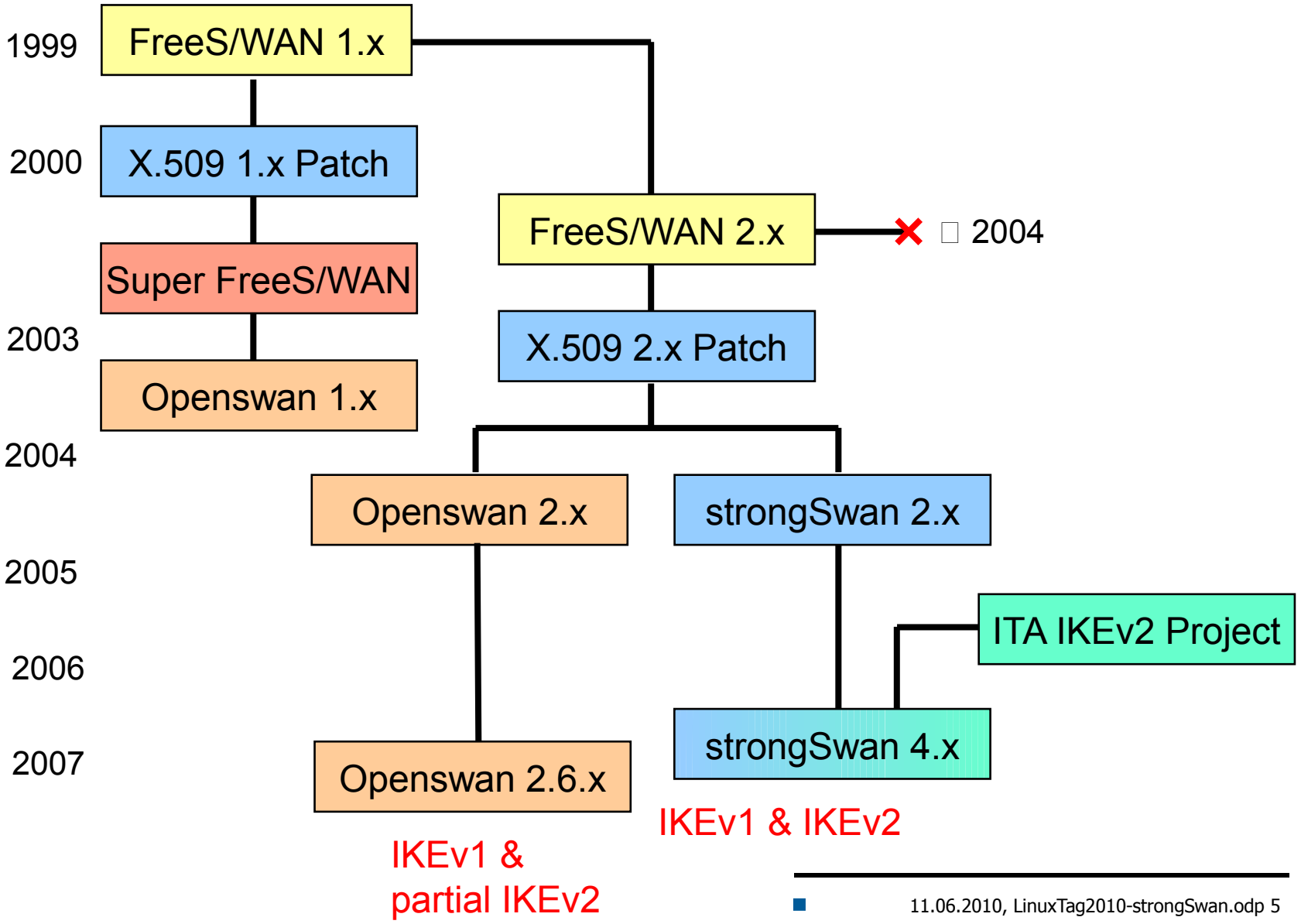
Institute for Internet Technologies and Applications



- strongSwan is an Internet Key Exchange daemon needed to automatically set up IPsec-based VPN connections.

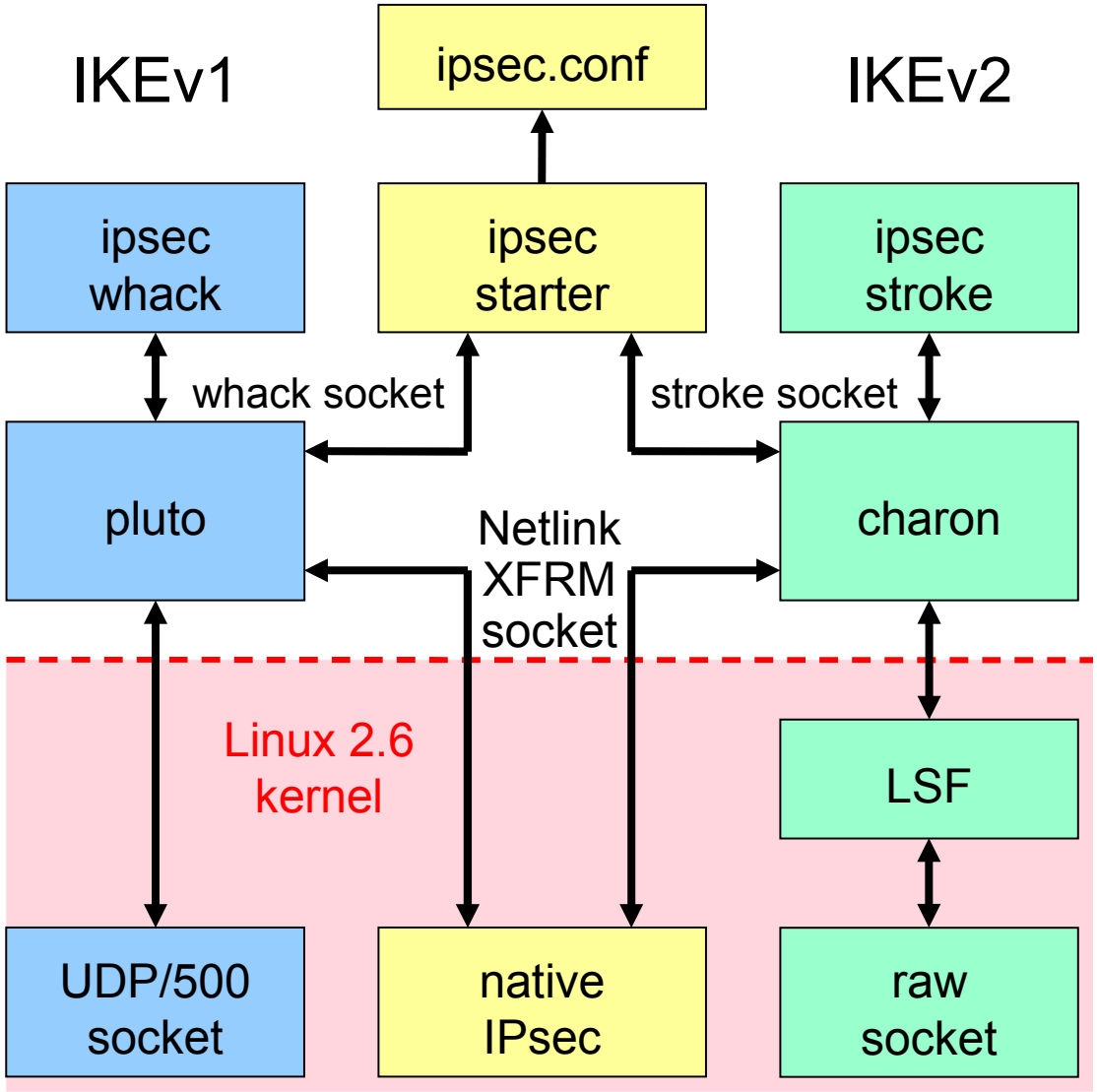
The FreeS/WAN Genealogy

Institute for Internet Technologies and Applications



The strongSwan IKE Daemons

Institute for Internet Technologies and Applications



- IKEv1
  - 6 messages for IKE SA
    Phase 1 Main Mode
  - 3 messages for IPsec SA
    Phase 2 Quick Mode
- IKEv2
  - 4 messages for IKE SA and first IPsec SA
    IKE_SA_INIT/IKE_AUTH
  - 2 messages for each additional IPsec SA
    CREATE_CHILD_SA

Institute for
Internet Technologies
and Applications

Swans in a Cluster

Image by mozzercork @ flickr | cc-by

strongSwan High Availability

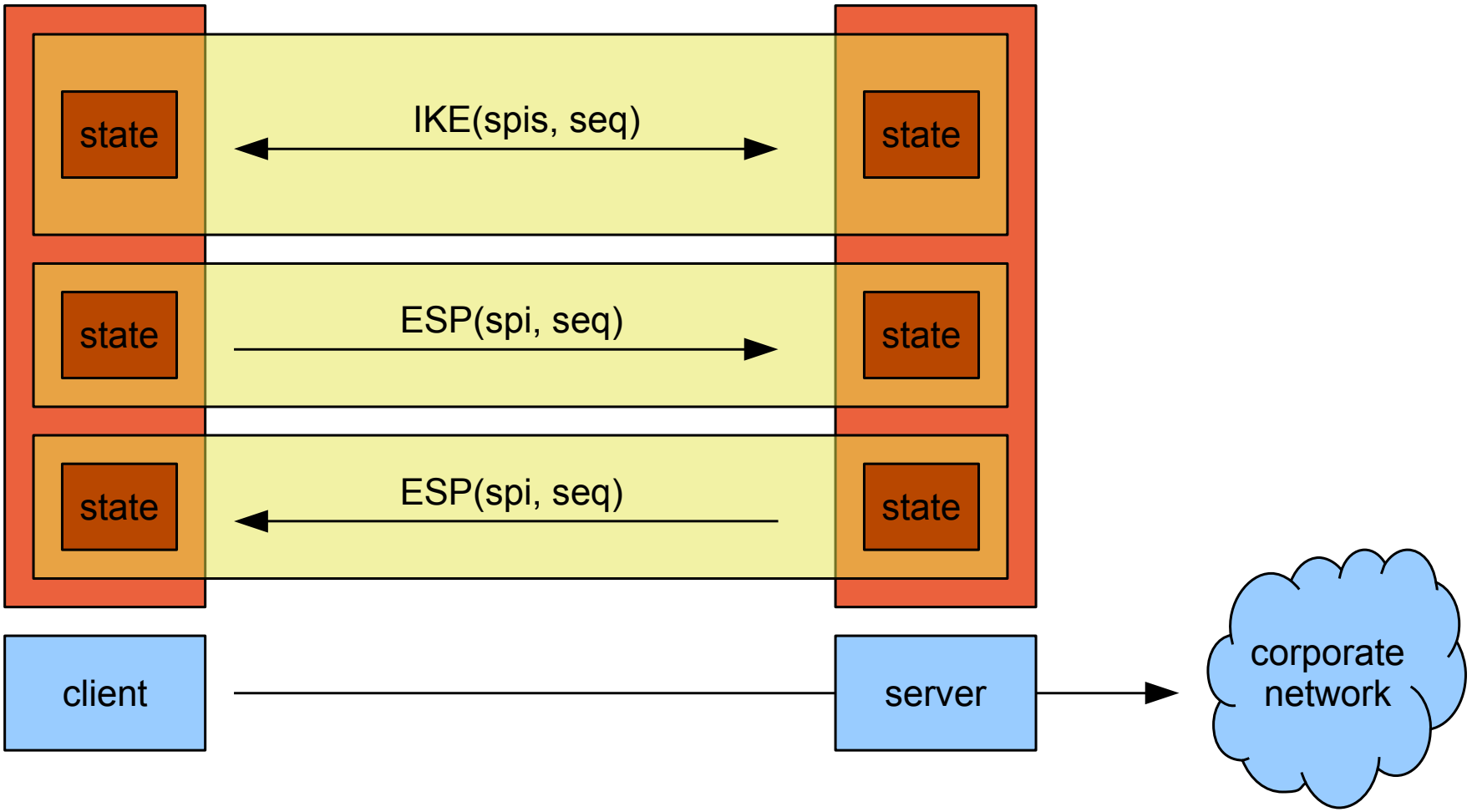
Requirements for a HA Solution

Institute for Internet Technologies and Applications

- **Failure detection -** On power loss, hardware failures, kernel oops or daemon crashes, remove node
- **State synchronization -** Always have IKE/IPsec state of every node synced to another
- **Takeover -** Detect node failure within 1-3 seconds
- **Transparent migration -** TCP or application sessions not interrupted
- **Load sharing -** Share load between all nodes, no idle backup node
- **Reintegration -** Integrate repaired node into running cluster, take over load
- **Legacy clients -** No protocol extension, any client benefits from HA functionality if connected to a cluster

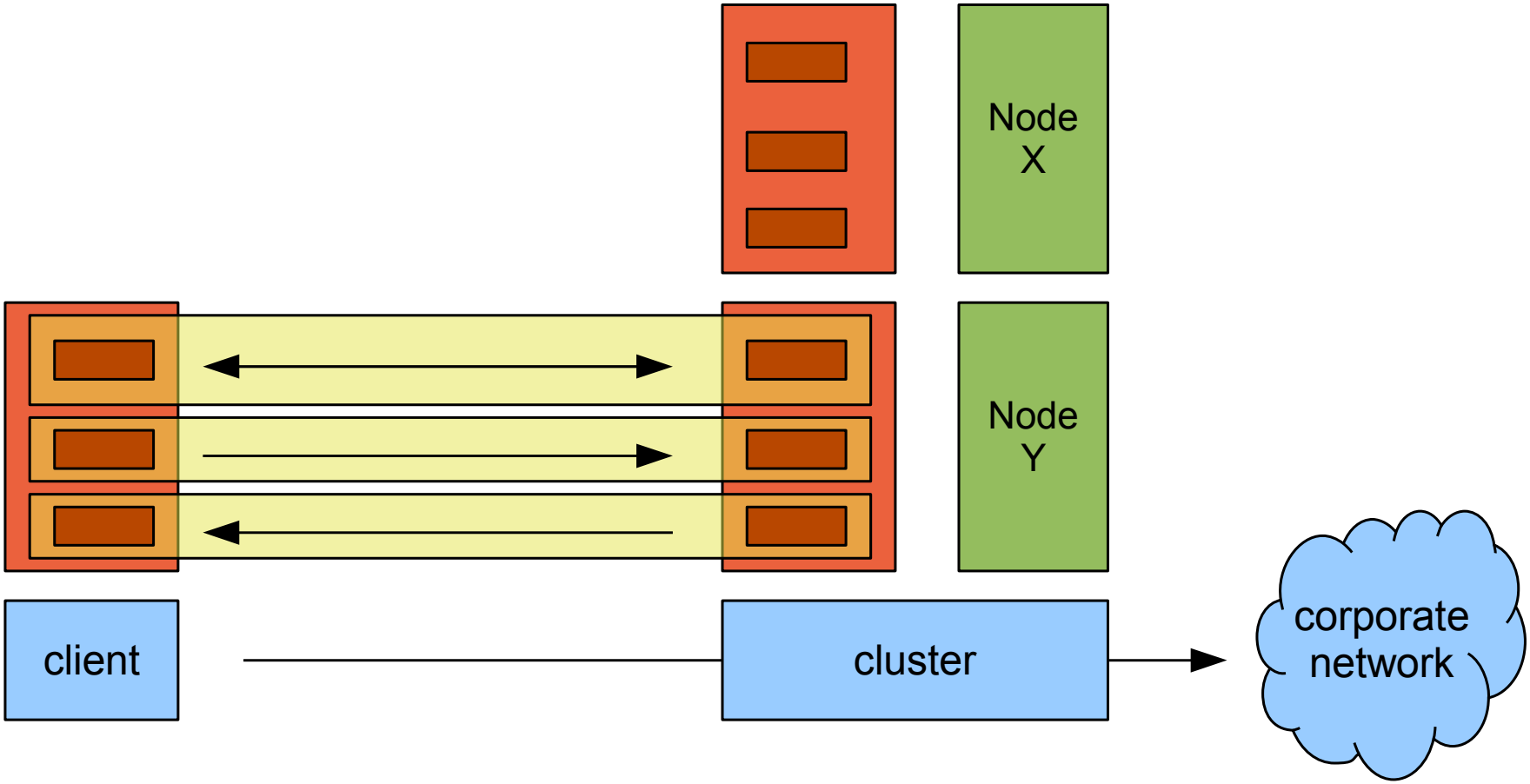
IPsec and IKE State

Institute for Internet Technologies and Applications



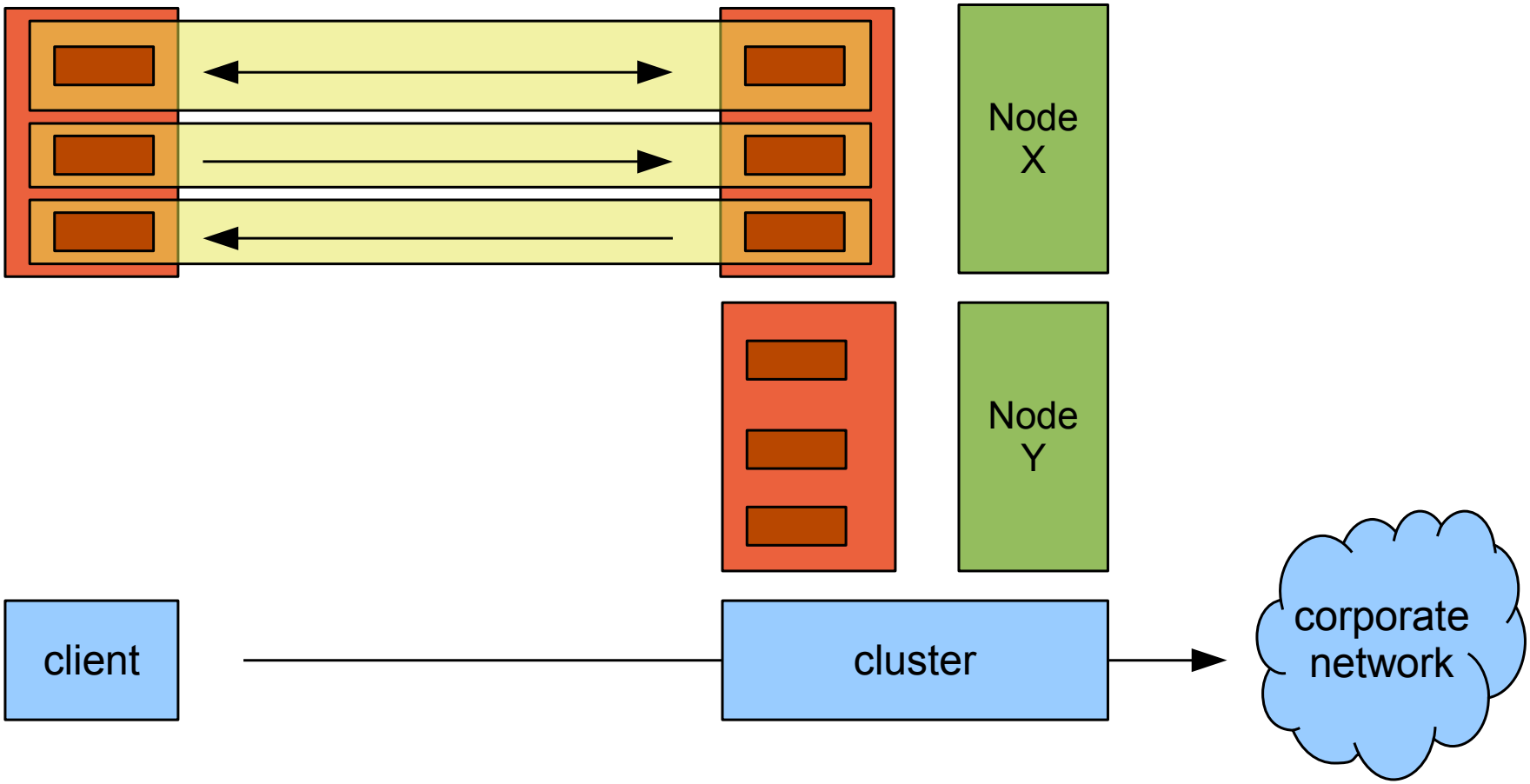
Adding Failover Node

Institute for Internet Technologies and Applications



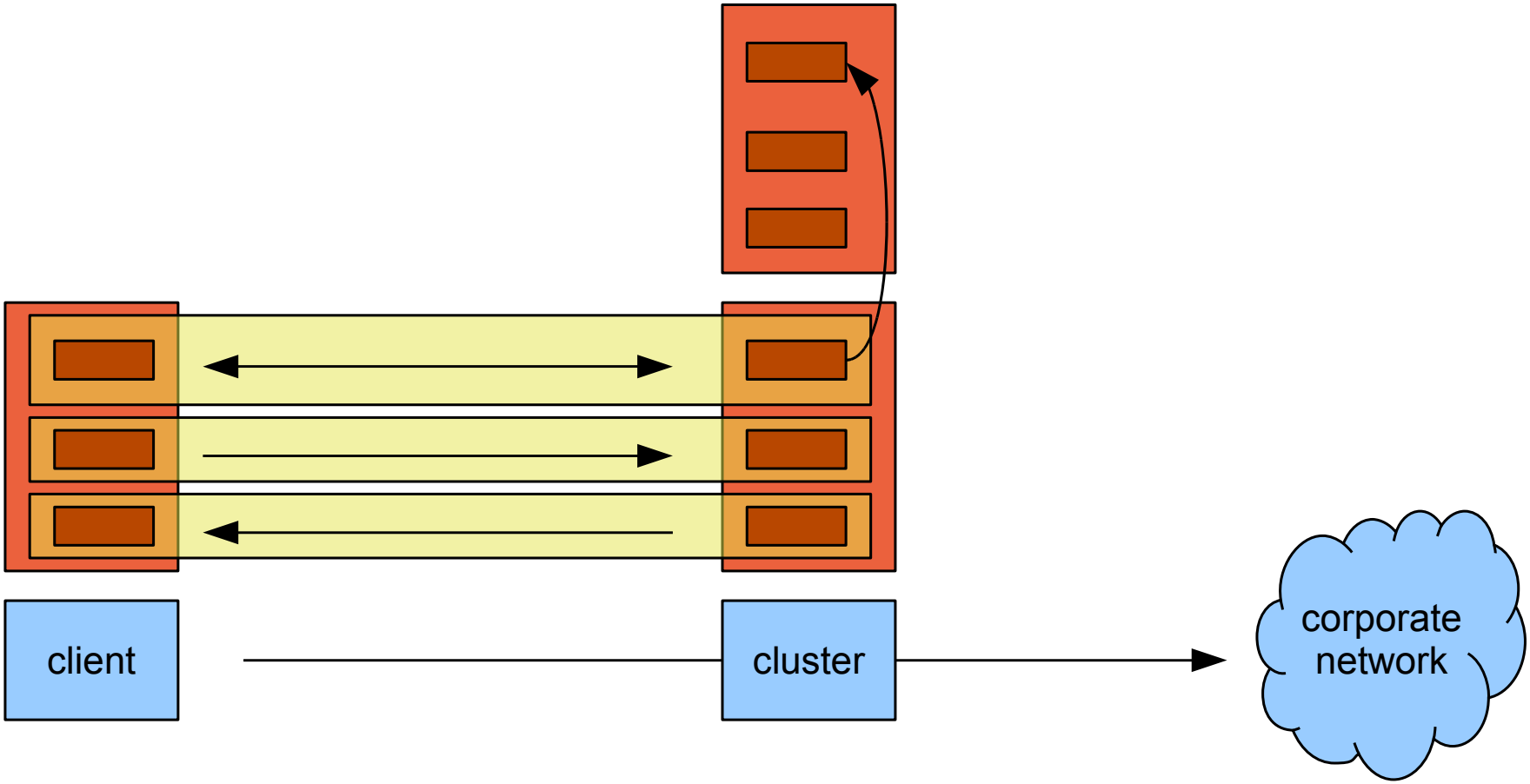
Failover

Institute for Internet Technologies and Applications



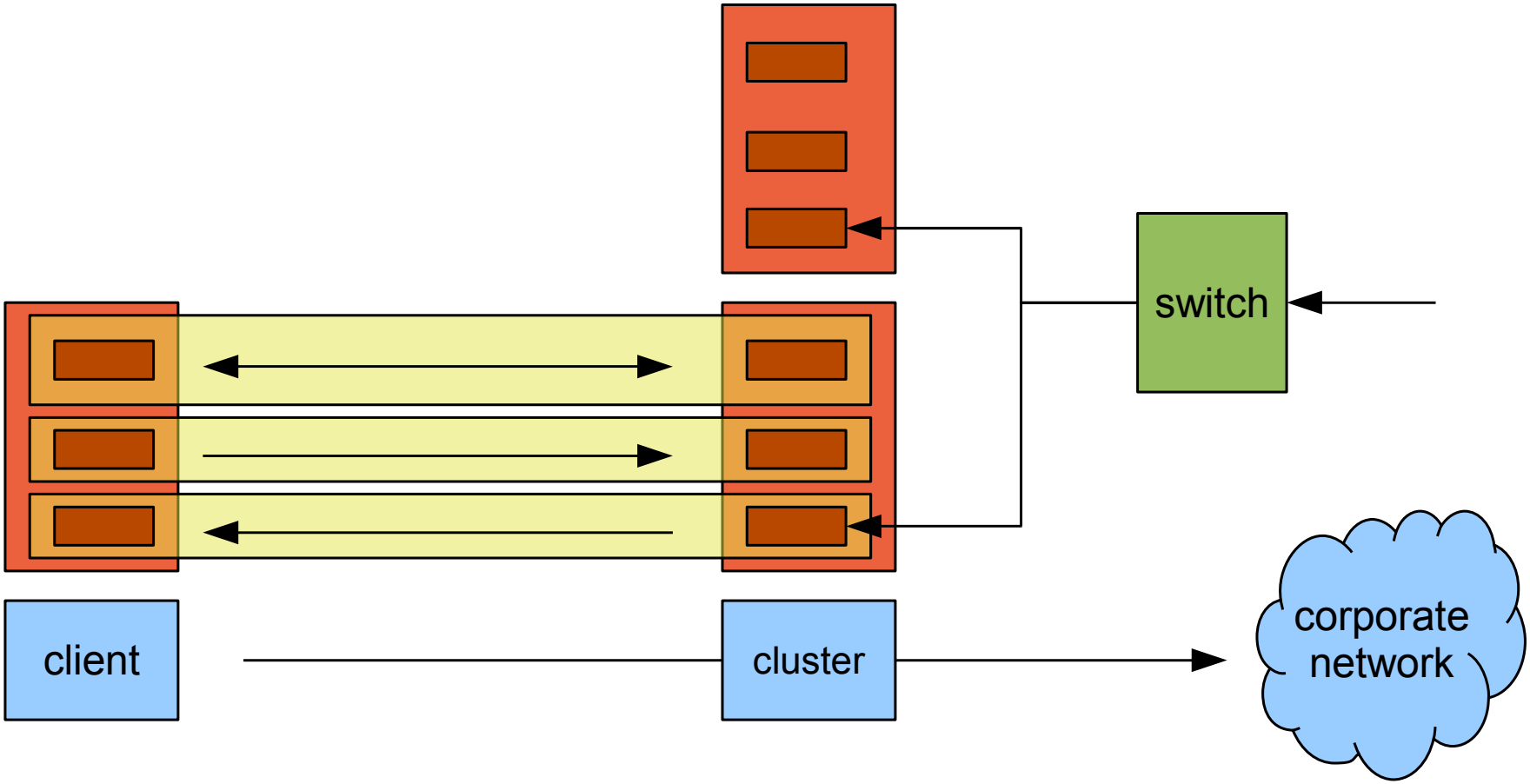
Synchronizing State - IKE

Institute for Internet Technologies and Applications



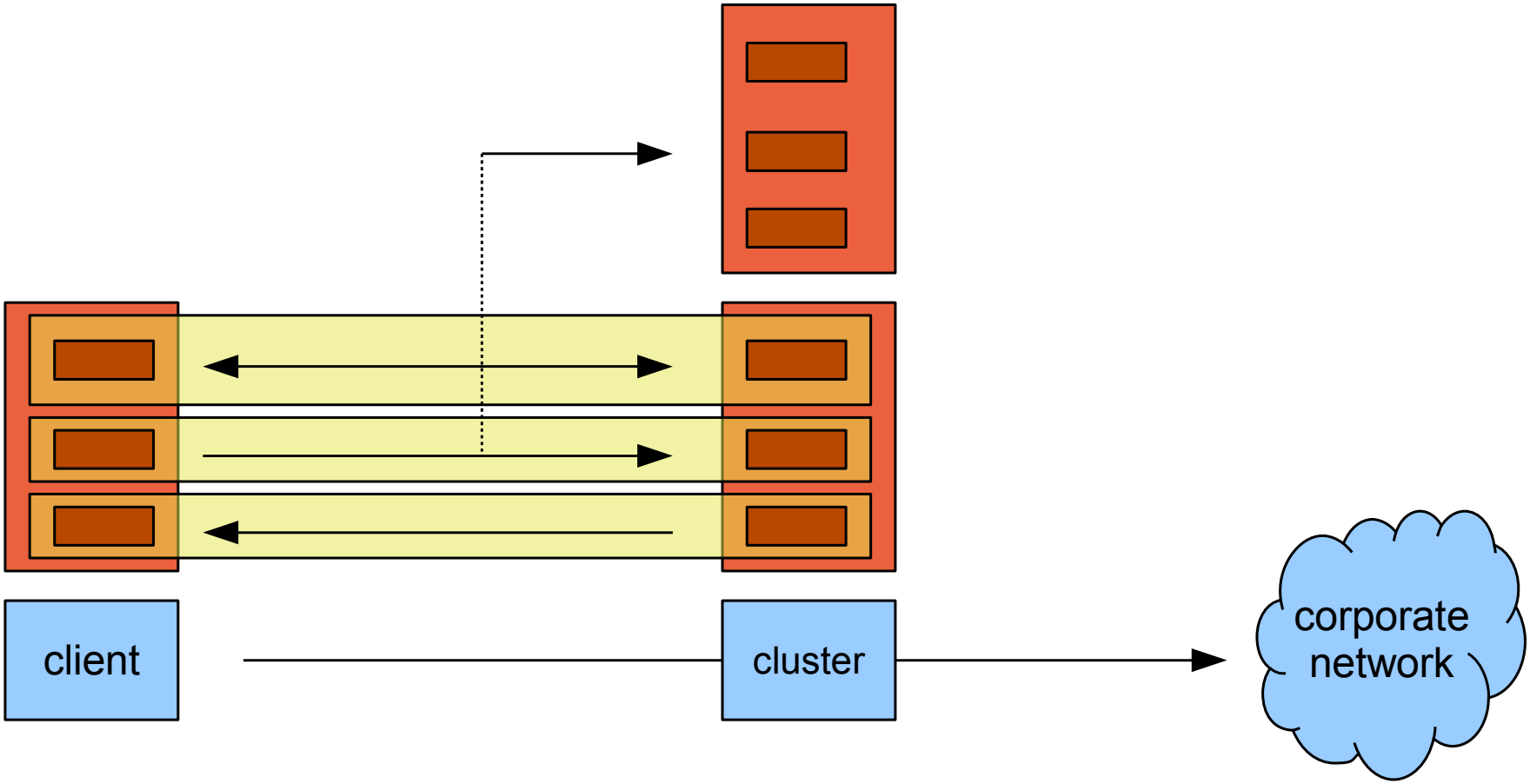
Synchronizing State – ESP Outgoing

Institute for Internet Technologies and Applications



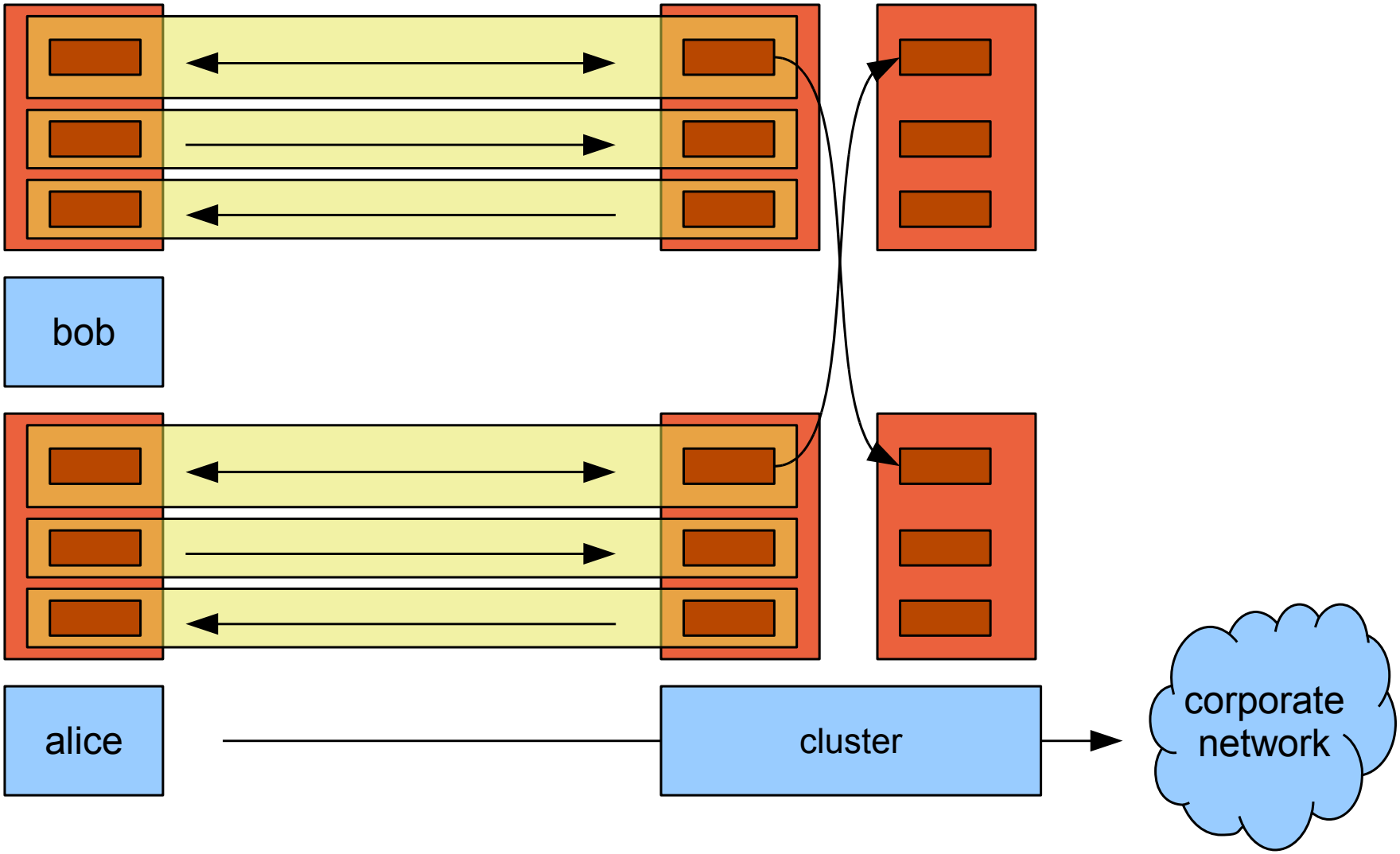
Synchronizing State – ESP Incoming

Institute for Internet Technologies and Applications



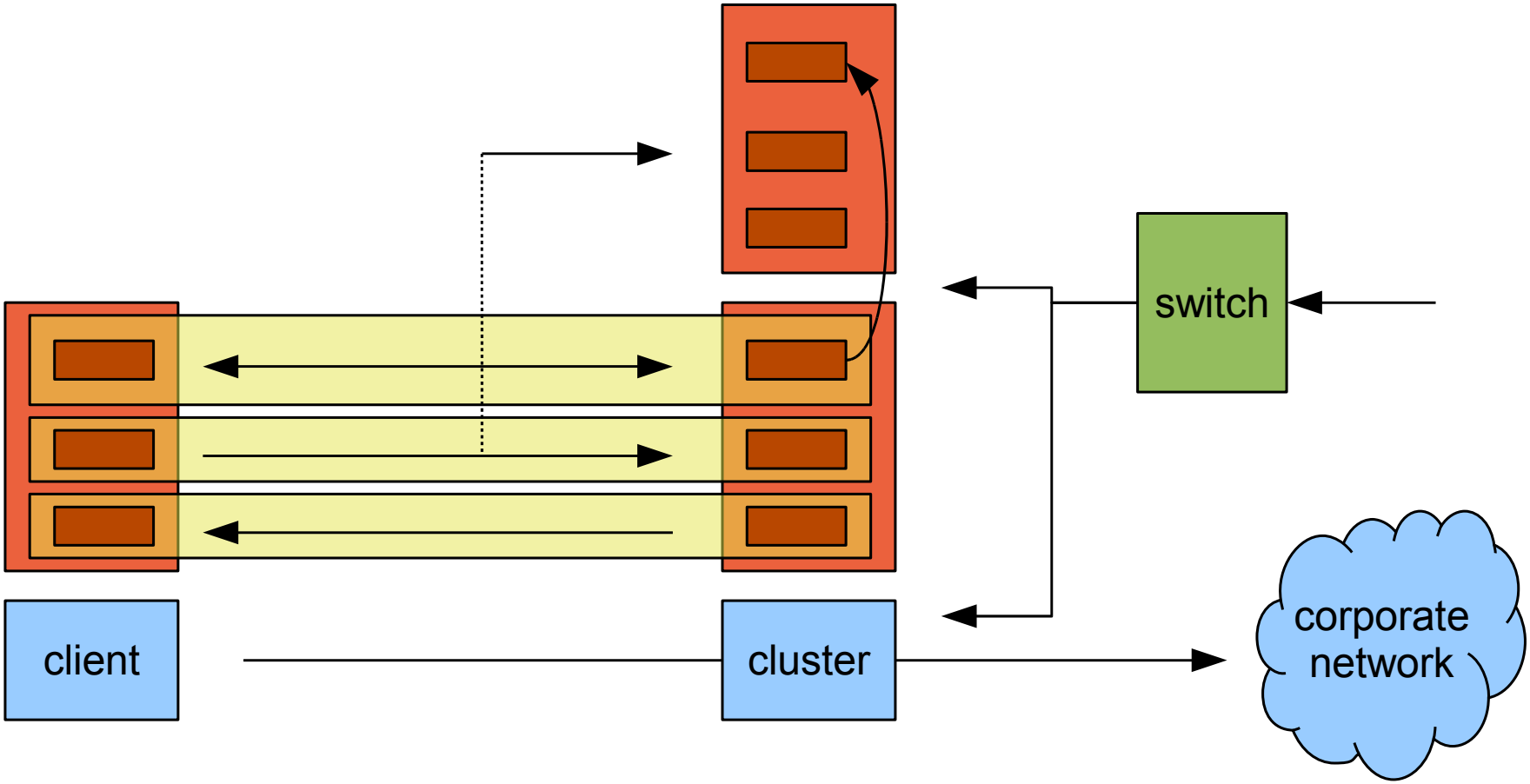
Going Active/Active – Multiple Clients

Institute for Internet Technologies and Applications



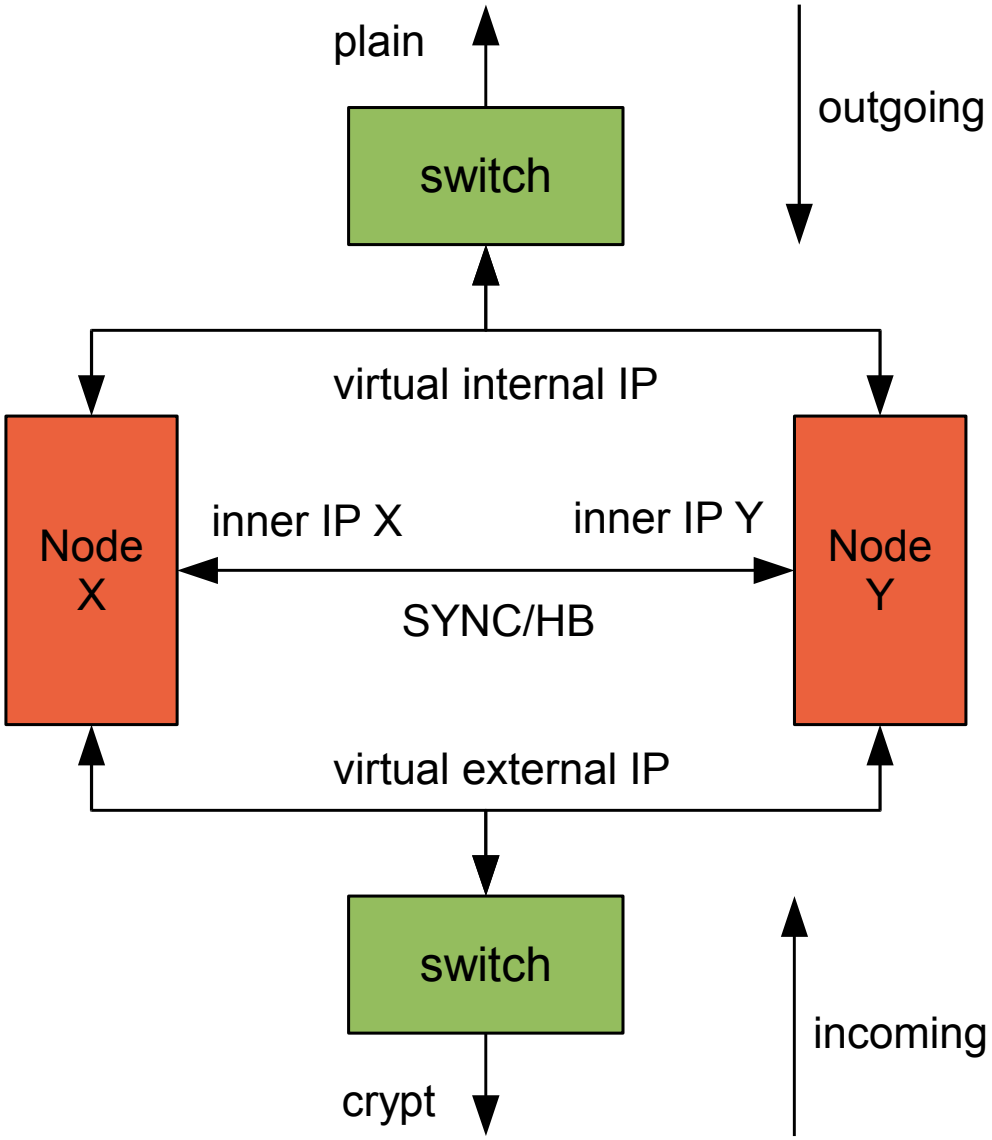
Going Active/Active – Single SA

Institute for Internet Technologies and Applications



Setup with Segmentation

Institute for Internet Technologies and Applications



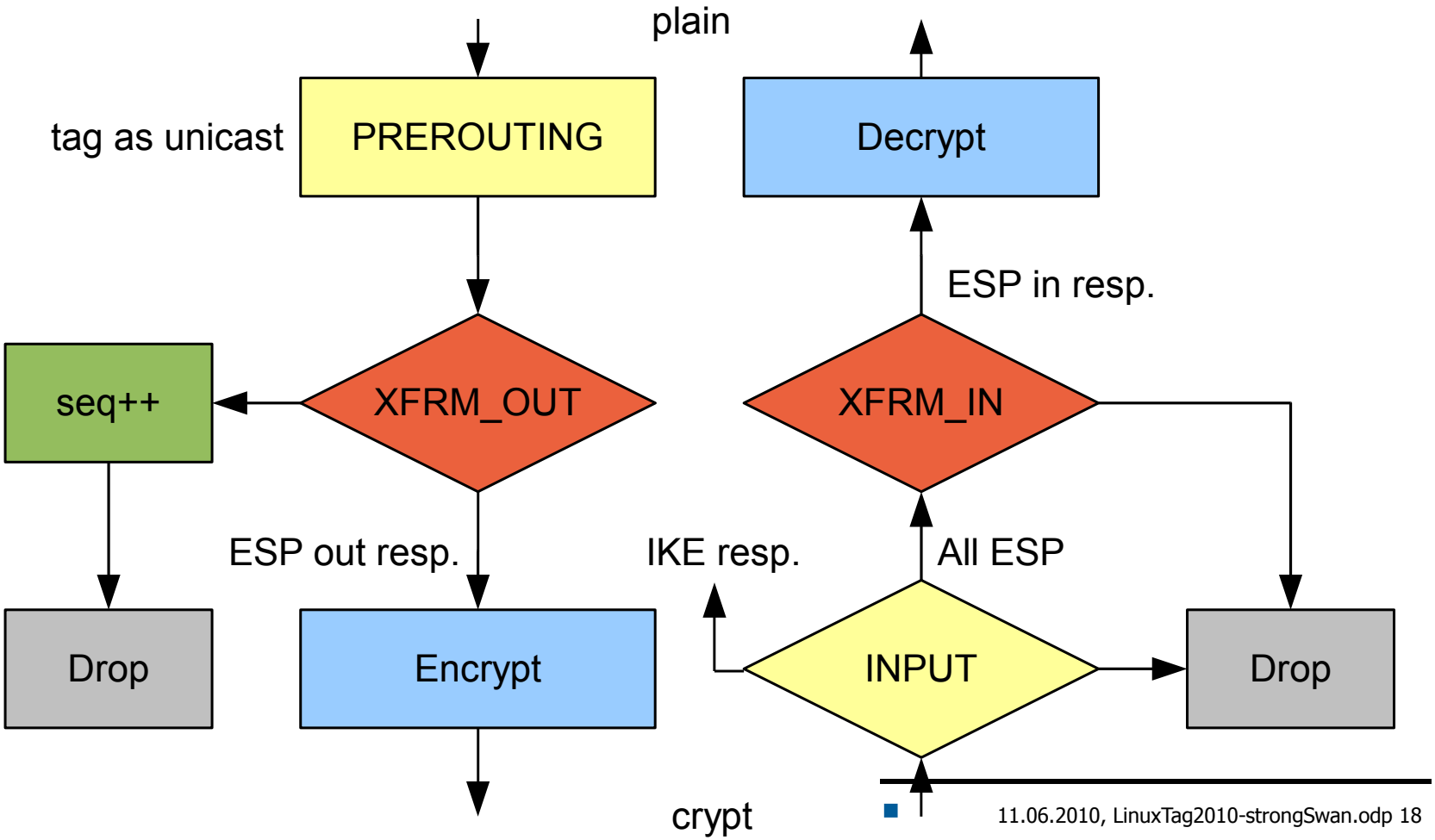
- 2 Nodes
- 4 Segments s (n = 4)
- X serves 1+2
- Y serves 3+4
- Anti-reorder mask: d = 16
- Segment calculation outgoing:
  - s = hash(spi, ip) % n
- Segment calculation incoming:
  - s = hash(spi, ip, seq / d) % n
- Segment calculation IKE:
  - s = hash(ip) % n

- SYNC: exchange IKE state using UDP messages, IPsec protected
- HB: Heartbeat, announces served segments

Kernel Implementation

Institute for Internet Technologies and Applications

- Introducing two new Netfilter hooks
  - XFRM_IN: Before XFRM decryption
  - XFRM_OUT: After policy lookup, before encryption
- Functionality implemented in ClusterIP



Institute for Internet Technologies and Applications

Virtual IP Address Pools

EIN INSTITUT DER

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Volatile RAM-based IP Address Pools

Institute for Internet Technologies and Applications

- Configuration in ipsec.conf

```
conn rw
     ...
     right=%any
     rightsourceip=10.3.0.0/24
     auto=add
```

- Statistics

```
ipsec leases

Leases in pool 'rw', usage: 2/255, 2 online
      10.3.0.2   online   'dave@strongswan.org'
      10.3.0.1   online   'carol@strongswan.org'
```

- Referencing and sharing a volatile pool

```
conn rw1
     ...
     right=%any
     rightsourceip=%rw
     auto=add
```

Persistant SQL-based IP Address Pools I

Institute for Internet Technologies and Applications

- SQLite database table definitions

```
http://wiki.strongswan.org/repositories/entry/strongswan/
        testing/hosts/default/etc/ipsec.d/tables.sql
```

- Creation of SQLite database

```
cat /etc/ipsec.d/table.sql | sqlite3 /etc/ipsec.d/ipsec.db
```

- Connecting to the SQLite database

```
# /etc/strongswan.conf - strongSwan configuration file

libhydra {
  plugins {
    attr-sql {
      database = sqlite:///etc/ipsec.d/ipsec.db
    }
  }
}
```

Persistant SQL-based IP Address Pools II

Institute for Internet Technologies and Applications

- Pool creation

```
ipsec pool --add bigpool --start 10.3.0.1 --end 10.3.0.254 --timeout 48
allocating 254 addresses... done.
```

- Configuration in ipsec.conf

```
conn rw
     ...
     right=%any
     rightsourceip=%bigpool
     auto=add
```

- Statistics

```
ipsec pool --status
name      start      end          timeout  size    online    usage
bigpool   10.3.0.1   10.3.0.254   48h      254     1 ( 0%)   2 ( 0%)

ipsec pool --leases --filter pool=bigpool
name     address  status start                end                  identity
bigpool  10.3.0.1 online Oct 22 23:13:50 2009                    carol@strongswan.org
bigpool  10.3.0.2 valid  Oct 22 23:14:11 2009 Oct 22 23:14:25 2009 dave@strongswan.org
```

Persistant SQL-based Config Attributes

Institute for Internet Technologies and Applications

- Add DNS and NBNS Servers

```
ipsec pool --addattr dns -server 62.2.17.60
```

- Add Unity Banners

```
ipsec pool --addattr banner -string "Welcome to LinuxTag"
```

- Add Unity Split Subnetworks

```
ipsec pool -addattr unity_split_include --subnet 10.10.0.0/255.255.0.0
```

- Statistics

```
ipsec pool -statusattr
 type  description           value
    3  INTERNAL_IP4_DNS      62.2.17.60
    3  INTERNAL_IP4_DNS      62.2.24.61
    4  INTERNAL_IP4_NBNS     10.10.0.1
    4  INTERNAL_IP4_NBNS     10.10.1.1
28672  UNITY_BANNER          "Welcome to LinuxTag"
28676  UNITY_SPLIT_INCLUDE   10.10.0.0/255.255.0.0
```

Institute for Internet Technologies and Applications

Network Endpoint Assessment

EIN INSTITUT DER

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Network Endpoint Assessment (NEA)

Institute for Internet Technologies and Applications