strongSwan News

Prof. Dr. Andreas Steffen
andreas.steffen@strongswan.org

Martin Willi
martin@strongswan.org
Agenda

• 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
What is strongSwan?
strongSwan is an Internet Key Exchange daemon needed to automatically set up IPsec-based VPN connections.
The FreeS/WAN Genealogy

1999
- FreeS/WAN 1.x

2000
- X.509 1.x Patch
- Super FreeS/WAN

2003
- Openswan 1.x

2004
- X.509 2.x Patch
- FreeS/WAN 2.x
- Openswan 2.x
- strongSwan 2.x
- ITA IKEv2 Project
- IKEv1 & IKEv2

2005
- strongSwan 4.x

2006

2007
- Openswan 2.6.x
- IKEv1 & partial IKEv2
The strongSwan IKE Daemons

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

IKEv1
- IKEv1
- IKEv2

ipsec.conf

pluto

ipsec starter

Netlink XFRM socket

LSF

UDP/500 socket

native IPsec

raw socket

ipsec stroke

charon
Swans in a Cluster

strongSwan High Availability
Requirements for a HA Solution

- **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

IKE (spis, seq)

ESP (spi, seq)

State

Client

Server

corporate network
Adding Failover Node

client → cluster → corporate network

Node X

Node Y
Failover

Node X

Node Y

client

cluster

corporate network
Synchronizing State - IKE
Synchronizing State – ESP Outgoing
Synchronizing State – ESP Incoming

client

cluster

corporate network
Going Active/Active – Multiple Clients

corporate network

alice
bob

cluster
Going Active/Active – Single SA

[Diagram showing connections between client, cluster, switch, and corporate network.]
Setup with Segmentation

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

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

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

Diagram:
- Introducing two new Netfilter hooks
  - XFRM_IN: Before XFRM decryption
  - XFRM_OUT: After policy lookup, before encryption
- Functionality implemented in ClusterIP
Virtual IP Address Pools
Volatile RAM-based IP Address Pools

- **Configuration in ipsec.conf**

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

- **Statistics**

```plaintext
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**

```plaintext
conn rw1
...
right=%any
rightsourceip=%rw
auto=add
```
Persistant SQL-based IP Address Pools I

- SQLite database table definitions

  [Link](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

● 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
```
Persistant SQL-based Config Attributes

- 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
  
  ```
<table>
<thead>
<tr>
<th>type</th>
<th>description</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>INTERNAL_IP4_DNS</td>
<td>62.2.17.60</td>
</tr>
<tr>
<td>3</td>
<td>INTERNAL_IP4_DNS</td>
<td>62.2.24.61</td>
</tr>
<tr>
<td>4</td>
<td>INTERNAL_IP4_NBNS</td>
<td>10.10.0.1</td>
</tr>
<tr>
<td>4</td>
<td>INTERNAL_IP4_NBNS</td>
<td>10.10.1.1</td>
</tr>
</tbody>
</table>
  | 28672      | UNITY_BANNER          | "Welcome to LinuxTag"
  | 28676      | UNITY_SPLIT_INCLUDE   | 10.10.0.0/255.255.0.0 |
  ```
Network Endpoint Assessment
Network Endpoint Assessment (NEA)

Posture Collectors (1 .. N)

Posture Broker Client

Posture Transport Clients (1 .. K)

NEA Client

PA

Posture Validators (1 .. N)

Posture Broker Server

Posture Transport Servers (1 .. K)

NEA Server

IKEv2 EAP