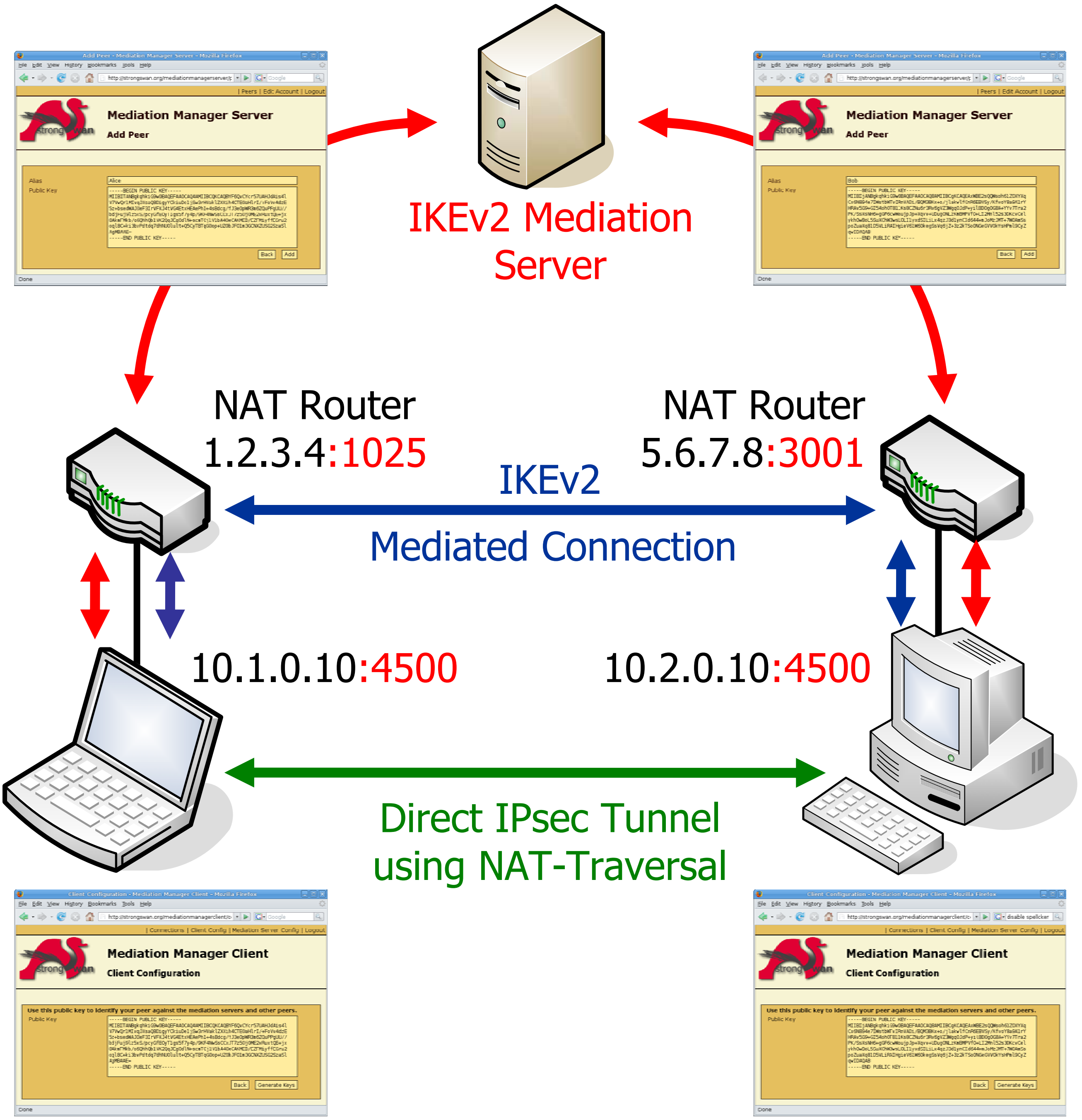
Mediation Service for IPsec

draft-brunner-ikev2-mediation

- Anonymized peer registration (public keyid)
- Endpoint discovery and relaying
- Peer-initiated hole punching



Add Peer - Mediation Manager Server - Mozilla Firefox

http://strongswan.org/mediationmanagerserver/

| Peers | Edit Account | Logout

Mediation Manager Server

Add Peer

Alias: Alice

Public Key:

```
-----BEGIN PUBLIC KEY-----
[illegible]
-----END PUBLIC KEY-----
```

Back | Add

Done

Add Peer - Mediation Manager Server - Mozilla Firefox

http://strongswan.org/mediationmanagerserver/

| Peers | Edit Account | Logout

Mediation Manager Server

Add Peer

Alias: Bob

Public Key:

```
-----BEGIN PUBLIC KEY-----
[illegible]
-----END PUBLIC KEY-----
```

Back | Add

Done

Client Configuration - Mediation Manager Client - Mozilla Firefox

http://strongswan.org/mediationmanagerclient/

| Connections | Client Config | Mediation Server Config | Logout

Mediation Manager Client

Client Configuration

Use this public key to identify your peer against the mediation servers and other peers.

Public Key:

```
-----BEGIN PUBLIC KEY-----
[illegible]
-----END PUBLIC KEY-----
```

Back | Generate Keys

Done

Client Configuration - Mediation Manager Client - Mozilla Firefox

http://strongswan.org/mediationmanagerclient/

| Connections | Client Config | Mediation Server Config | Logout

Mediation Manager Client

Client Configuration

Use this public key to identify your peer against the mediation servers and other peers.

Public Key:

```
-----BEGIN PUBLIC KEY-----
[illegible]
-----END PUBLIC KEY-----
```

Back | Generate Keys

Done

www.strongswan.org

ita Institute for
Internet Technologies
and Applications

The double NAT case - where punching holes counts!

- You are selling automation systems all over the world. In order to save on travel expenses you want to remotely diagnose and update your deployed systems via the Internet. But security counts – thus IPsec is a must! Unfortunately both you and your customer are behind NAT routers so that no direct VPN connection is possible. You are helplessly blocked!
- You own an apartment at home, in the mountains or even abroad. You want to remotely control the heating or your sophisticated intrusion detection system via ADSL or Cable access. But since you and your apartment are separated by two NAT routers your are helplessly blocked.

How it works!

- Two peers want to set up a direct IPsec tunnel using the established NAT traversal mechanism of encapsulating ESP packets in UDP datagrams. Unfortunately they cannot achieve this by themselves because neither host is seen from the Internet under the standard IKE NAT-T port 4500. Therefore both peers need to set up a *mediation connection* with an IKEv2 *mediation server*. In order to prevent unsolicited connection attempts by foreign peers, the mediation connections use randomized pseudonyms as IKE peer identities. With the help of a novel IKEv2 end point payload the mediation server informs each peer under which end point it is visible from the Internet, as soon as both peers are on-line. This allows the peers to initiate a hole punching attempt by simultaneously sending IKE packets to the available selection of UDP end points.

It might become a standard!

- On April 16 2008, strongSwan developer Tobias Brunner registered the Internet Draft <draft-brunner-ikev2-mediation> defining our IKEv2 mediation protocol with the hope that it will become a standard.

EIN INSTITUT DER

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

Prof. Dr. Andreas Steffen
Institute for Internet Technologies and Applications
Oberseestrasse 10
CH-8640 Rapperswil
✉ andreas.steffen@hsr.ch ☎ +41 76 340 25 56