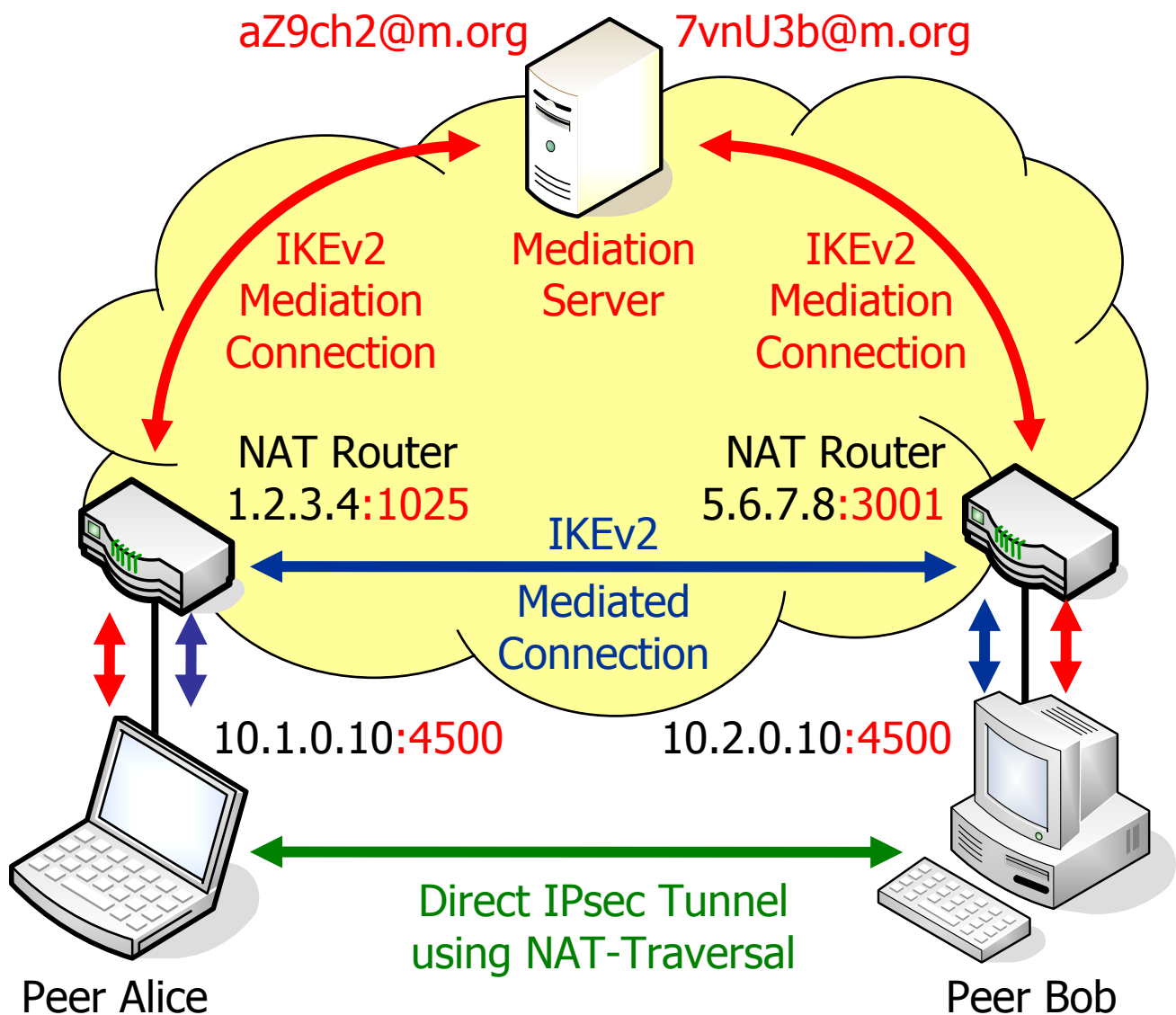




Peer-to-Peer NAT-Traversal for IPsec

- Anonymized peer registration
- Endpoint discovery and relaying
- Peer-initiated hole punching
- IKEv2 Internet draft in preparation



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 you 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.

How we can help you

- We are working on an Internet draft that will allow peers to set up an IPsec connection in double NAT situations by adding client registration, UDP end point discovery and relaying to the IKEv2 standard.