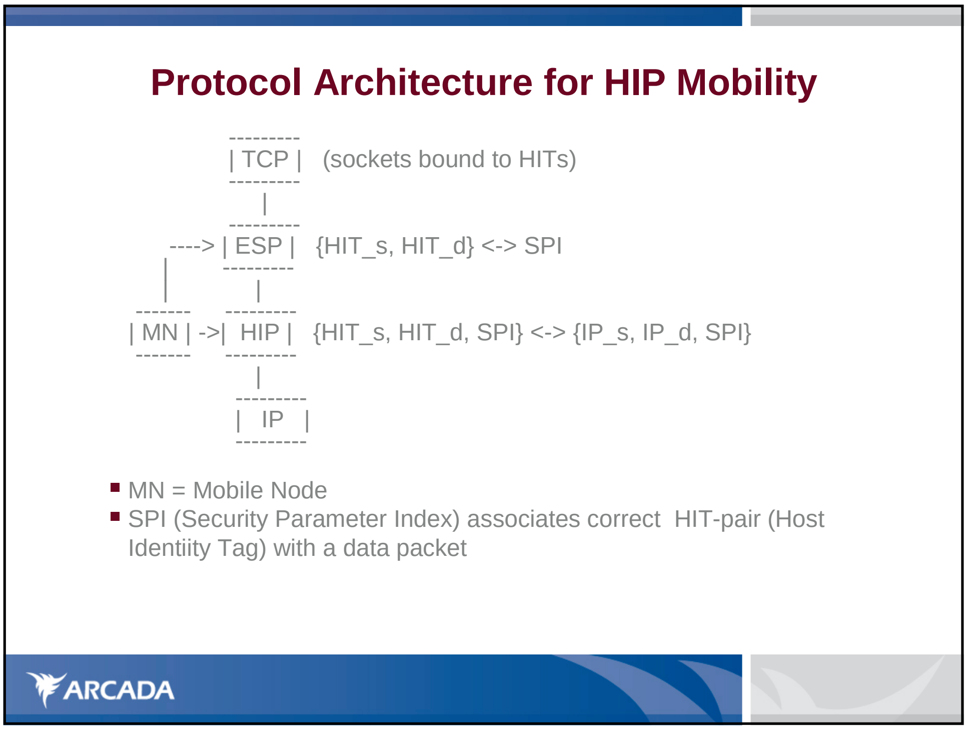
HIP based VPN Mobility

Göran Pulkkis

Arcada University of Applied Sciences

WISEciti Public Seminar 7.5.2009



Protocol Architecture for HIP Mobility

```
              ---------
              | TCP |   (sockets bound to HITs)
              ---------
                 |
              ---------
       ----> | ESP |   {HIT_s, HIT_d} <-> SPI
       |      ---------
       |         |
  -------     ---------
| MN | ->|  HIP |   {HIT_s, HIT_d, SPI} <-> {IP_s, IP_d, SPI}
  -------     ---------
                 |
               ---------
               |   IP   |
               ---------
```

- MN = Mobile Node
- SPI (Security Parameter Index) associates correct HIT-pair (Host Identiity Tag) with a data packet

Standard HIP Mobility

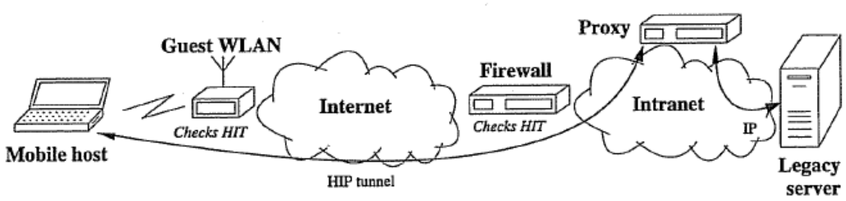
A Rendezvouz Server (RVS) is kept updated on the locality (IP address) of a mobile node (MN)

- DNS name of the RVS is registered in DNS for MN
- MN registers on a RVS with the HIP Registration Protocol, a Base Exchange MN <-> RVS
- A Correspondent Node (CN) wants to communicate with MN
  - In Base Exchange CN <-> MN I1 goes through RVS
  - Communication CN <-> MH uses {HIP SA, ESP SA} (Encapsulated Security Payload)
- MN changes network attachment
  - UPDATE signaling from MN to CN
  - UPDATE signaling from MH to RVS
  - Communication CN <-> MH continues based on {HIP SA, ESP SA}

ARCADA

Virtual Private Networking with HIP

From A. Gurtov, Host Identity Protocol (HIP): Towards the Secure Mobile Internet, ISBN 978-0-470-99790-1,Wiley and Sons, June 2008.



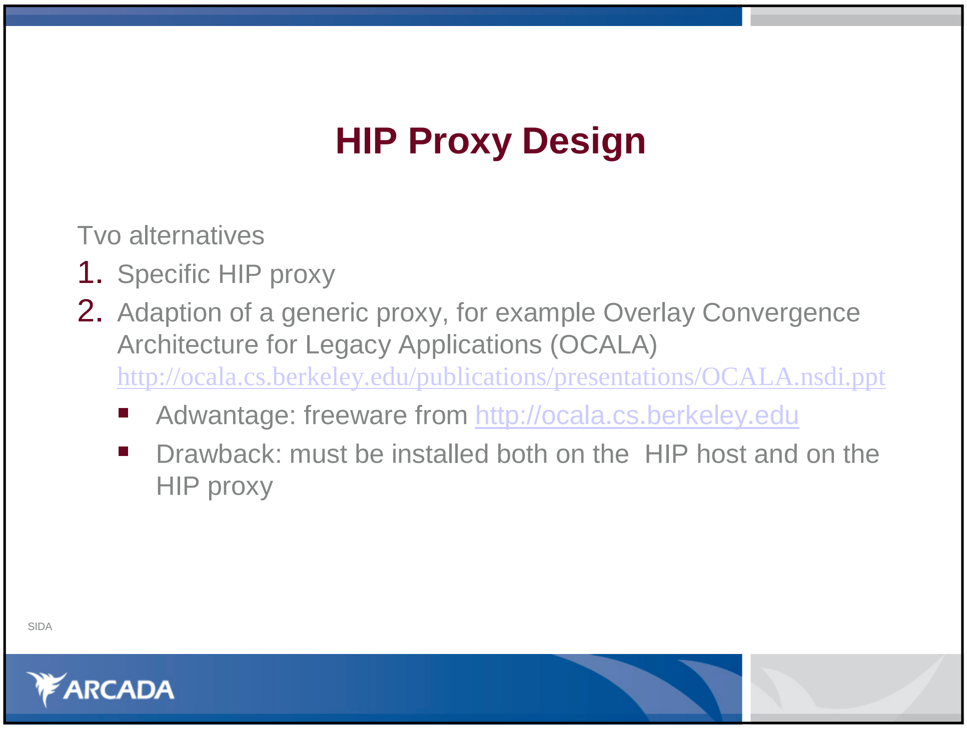
This HIP VPN solution integrates (= HIP VPN GATEWAY)

- HIP firewall
- UDP encapsulation for legacy NAT traversal
- HIP Proxy located in intranet

List of authorized HITs in HIP firewall or PKI integrated with a firewall

ACL (Access Control List)

ARCADA



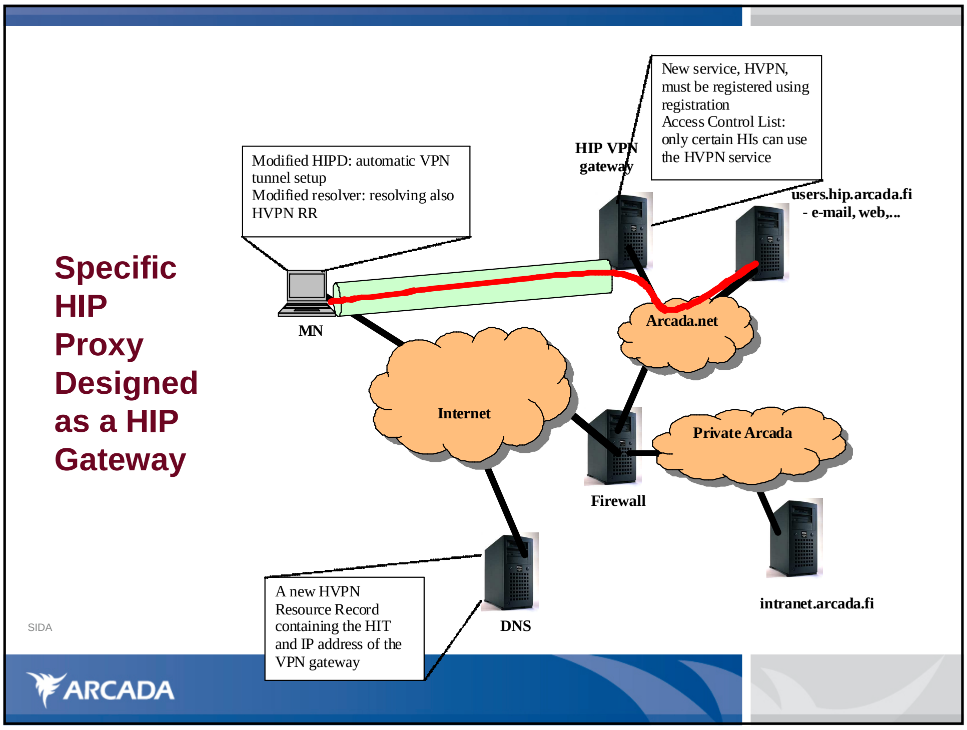
HIP Proxy Design

Tvo alternatives

1. Specific HIP proxy
2. Adaption of a generic proxy, for example Overlay Convergence Architecture for Legacy Applications (OCALA) http://ocala.cs.berkeley.edu/publications/presentations/OCALA.nsdi.ppt
   - Adwantage: freeware from http://ocala.cs.berkeley.edu
   - Drawback: must be installed both on the HIP host and on the HIP proxy

SIDA

ARCADA



Specific HIP Proxy Designed as a HIP Gateway

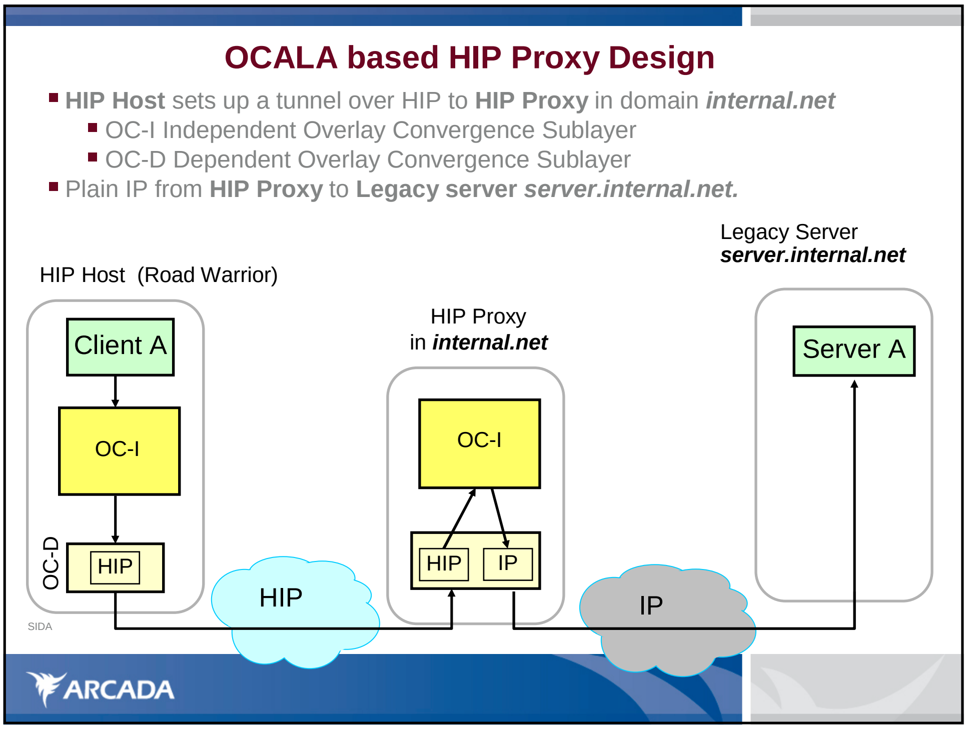
Modified HIPD: automatic VPN tunnel setup
Modified resolver: resolving also HVPN RR

New service, HVPN, must be registered using registration
Access Control List: only certain HIs can use the HVPN service

A new HVPN Resource Record containing the HIT and IP address of the VPN gateway

SIDA

ARCADA



OCALA based HIP Proxy Design

- **HIP Host** sets up a tunnel over HIP to **HIP Proxy** in domain ***internal.net***
  - OC-I Independent Overlay Convergence Sublayer
  - OC-D Dependent Overlay Convergence Sublayer
- Plain IP from **HIP Proxy** to **Legacy server *server.internal.net.***

SIDA

ARCADA