Enterprise Connectivity using MIPv4 and MOBIKE

Vijay Devarapalli and Pasi Eronen

MIP4 WG, IETF 63

Enterprise connectivity

- Enterprise networks
  - A typical enterprise networks has users connecting from trusted and untrusted networks
  - The trusted and untrusted networks are separated by a DMZ
  - Access to the intranet is controlled by a firewall and VPN gateway in the DMZ

- Tools to enable secure connectivity and mobility for enterprise users
  - IPsec VPNs
  - Mobile IPv4
  - Mobility extensions to IKEv2 (MOBIKE)

Available Solutions

- draft-ietf-mip4-vpn-problem-solution-01
  - Describes how MIPv4 and IPsec VPNs can be used together
  - Uses dual MIP due to many reasons
    - Non IPsec VPNs
    - IPsec VPNs that don't survive MN movements
    - IKEv1 based IPsec VPNs

- Our proposal
  - If MOBIKE supported, use it
  - Eliminates the need for one MIP4 tunnel and the external Home Agent
  - Three access modes
    - 'f' – MIP with FA-CoA
    - 'c' – MIP with CCoA
    - 'mc' – mobile enhanced VPN with VPN_TIA as the CCoA

MN inside the Enterprise network

- The MN uses regular MIPv4 for subnet mobility
- Traffic does not go through the DMZ
- Confidentiality protection maybe required between the MN and the FA/access router, if the MN uses a wireless link to connect to the trusted network

MN outside the Enterprise

- MN has an IPsec VPN tunnel with the VPN GW in the DMZ
  - If the MN moves, it uses the MOBIKE protocol to update the tunnel end point at the VPN GW
- MN also has a binding cache at the HA
  - The MN uses the VPN Tunnel Inner Address (TIA) as the CCoA for MIP registration
  - If the VPN TIA changes, the MN must send a registration request to update the binding at the HA
  - If the MN connects to a new VPN GW, the MN must send a registration request to update the binding at the HA

Crossing Security Boundaries

- Based on the reachability of the HA from the MN's current point of attachment
- Whenever the MN moves, it sends a Registration Request to the HA without VPN encapsulation
  - If the HA responds, then the MN is inside the enterprise network
  - Otherwise, it is not
- The MN at the same time also contacts the VPN GW
  - If a VPN tunnel already exists, the MN sends a MOBIKE message message
  - If a VPN tunnel doesn't exist already, the MN sends a IKEv2 message to setup a VPN tunnel
  - If the VPN GW responds and the HA does not, the MN is outside the enterprise
- More details in the draft

An Optimization

- Send agent discovery message and DHCP request message at the same time
  - This avoids the delay involved in first discovering if there is an FA available and then performing DHCP
  - Some implementations already do this
  - Recommend this for all mobile node implementations; should be configurable to turn it off

NAT Traversal

- MIP4 NAT traversal should be used if there is a NAT between the MN and the HA
- IPsec NAT traversal should be used if there is a NAT between the MN and the VPN GW
- If VPN TIA is from a private address space associated with the VPN GW, then both MIPv4 and IPsec NAT traversal should be used together in the access mode, ‘mc’