Mobile IPv4 Traversal Across VPN or "NAT and VPN" Gateways

Intel Labs

Technical Overview

Agenda

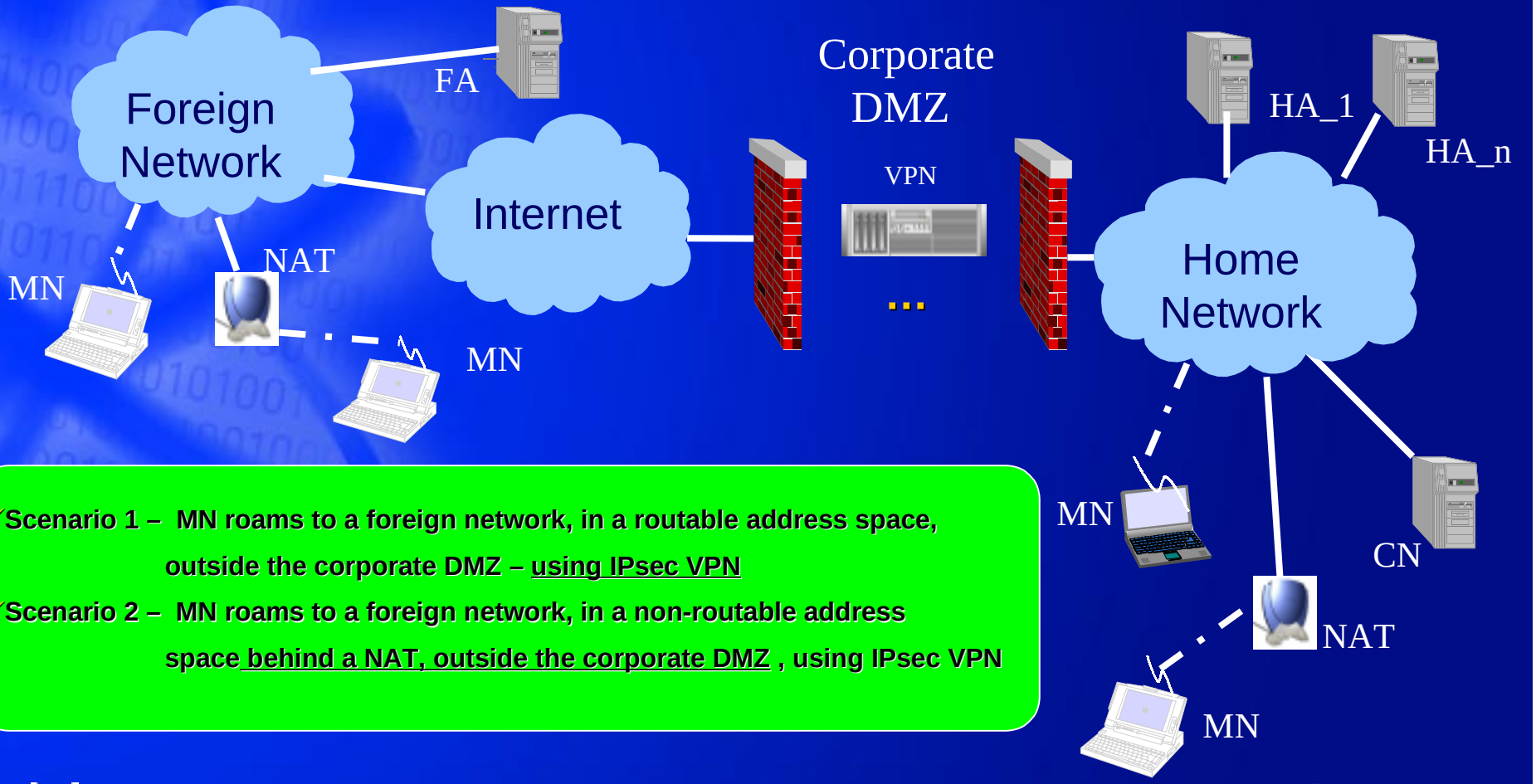
- User scenarios for Mobile IP traversal across VPN or “NAT and VPN” gateways
- Problem Statement for Mobile IP traversal across VPN or “NAT and VPN” gateways
- Solution Overview that enables efficient, seamless Mobile IPv4 traversal across VPN or “NAT and VPN”gateways

“NAT and VPN” refers to a Network topology, in which Mobile IPv4 traffic has to traverse one or more NAT gateways followed by a VPN gateway in the path to its final destination

Glossary

FA	Foreign Agent
HA	Home Agent
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
MIP	Mobile IP (RFC2002 + bis)
IPsec	Network Security Protocol
MN	Mobile Node
NAT	Network Address Translator
NAPT	Network Address Port Translator
VPN	Virtual Private Network (IPsec-based)

MIPv4 Traversal Across VPN or "NAT and VPN" Gateways



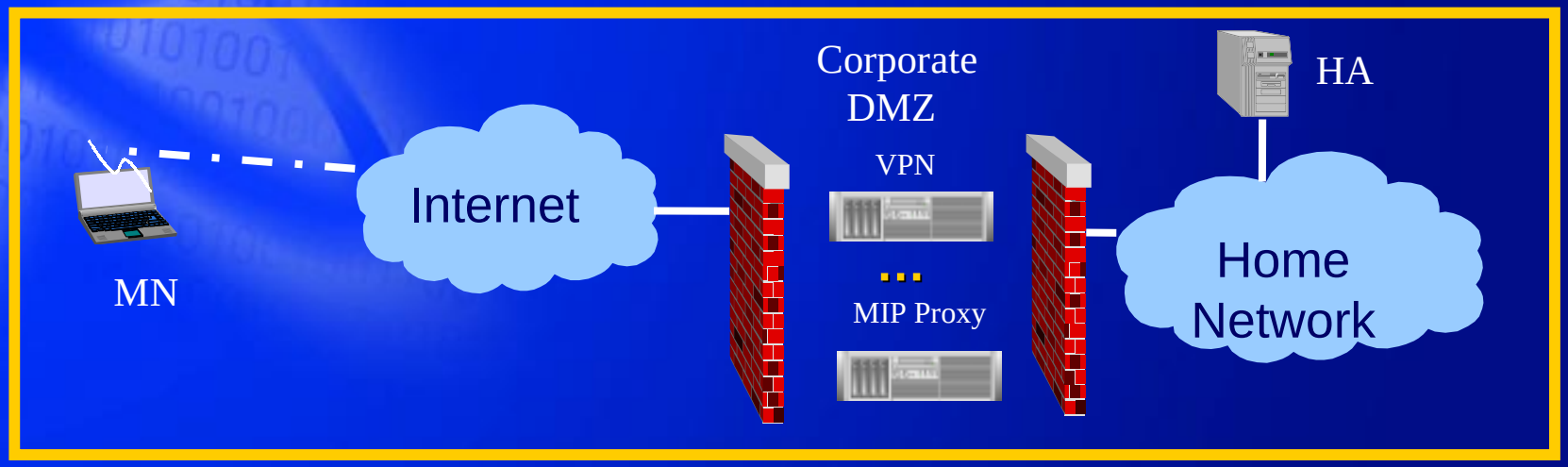
- ✓Scenario 1 – MN roams to a foreign network, in a routable address space, outside the corporate DMZ – using IPsec VPN
- ✓Scenario 2 – MN roams to a foreign network, in a non-routable address space behind a NAT, outside the corporate DMZ , using IPsec VPN

Problem Statement

- MIPv4 is incompatible with IPsec-based VPNs
  - FA assisted routing:
    - IPsec (encrypted) MIPv4 packets can not be processed by FA
  - Non-FA assisted routing
    - VPN tunnel needs to be re-established as the MN moves from one subnet to another (hand-off performance implications)
- MIPv4 is incompatible with NAT gateways
    - Refer to draft-ietf-mobileip-nat-traversal-00.txt

Solution Overview

- Introduce a functional entity called Mobile IP Proxy (MIP Proxy) to help MIPv4 traversal across VPN or “NAT and VPN” gateways
- The MIP Proxy is in the path between an MN and its corresponding HA, and acts as a surrogate MN and HA



Solution Basics

- Can serve multiple MNs and HAs
- Shares SAs with MN and corresponding HA
- Handles all MIP control packets
  - These packets do not go through the VPN gateway
- Allows IPsec tunnel to be bound to invariant MN-Home address, which avoids SA refreshes after each IP subnet hand-off

Solution Basics (Continued)

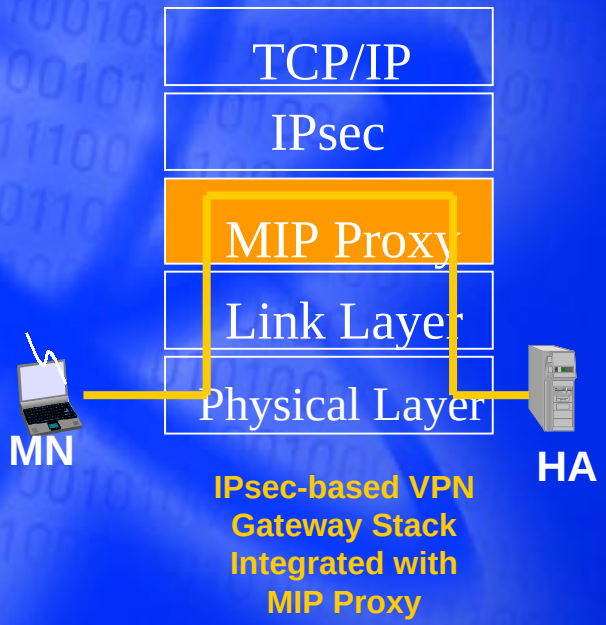
- Can nominally run on a dual-homed host, however, it is possible to instantiate MIP Proxy on a singly homed host
- Leverages NAT traversal protocol extension specified in draft-ietf-mobileip-nat-traversal-00.txt
- supports NAT traversal where the HA is behind a VPN gateway and hence not directly reachable

MIP Proxy Deployment

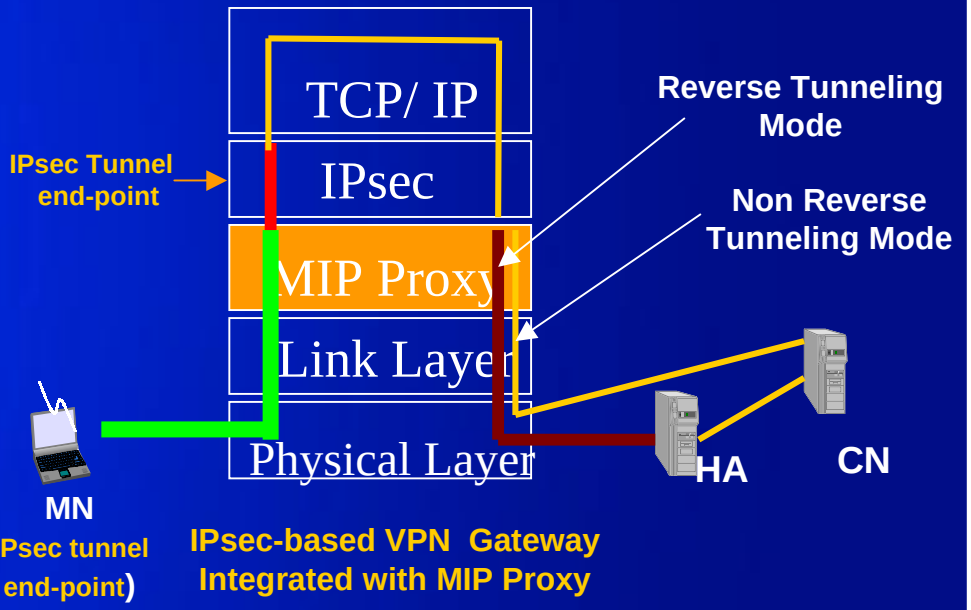
- One Box Solution
  - VPN and MIP proxy integrated on box box
- Two Box Solution
  - VPN and MIP proxy running in parallel on two different boxes

MIP Proxy and VPN Integration – 1 Box Solution

MIP Control Traffic Flow

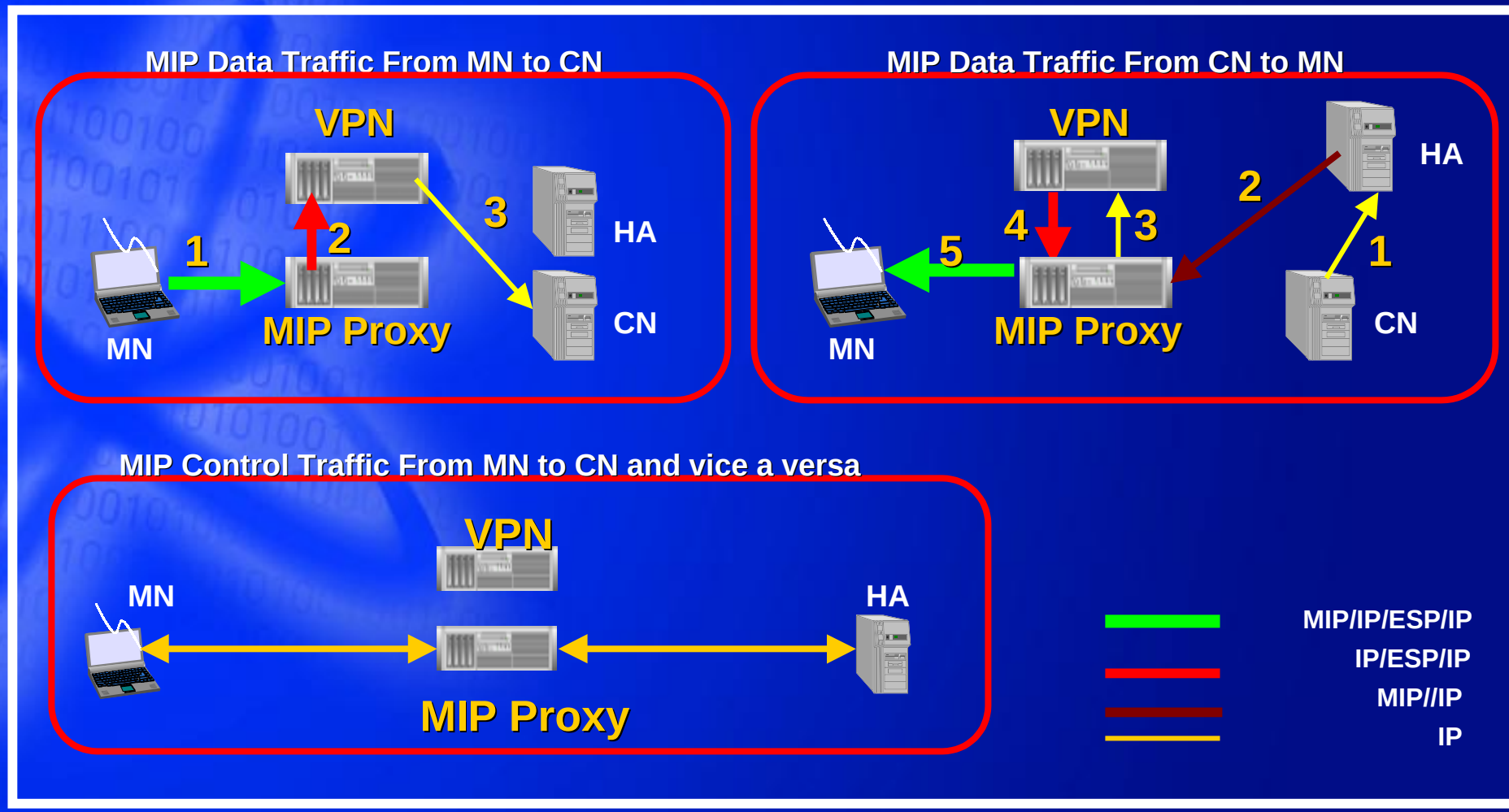


MIP Data Traffic Flow



MIP/IP/ESP/IP
IP/ESP/IP
MIP//IP
IP

MIP Proxy and VPN Integration – 2 Box Solution



References

- *Draft-adrangi-mobileip-nat-vpn-problem-stat-req-00.txt*
- *draft-adrangi-mobileip-natvpn-traversal-01.txt*
- *draft-ietf-mobileip-nat-traversal-00.txt*