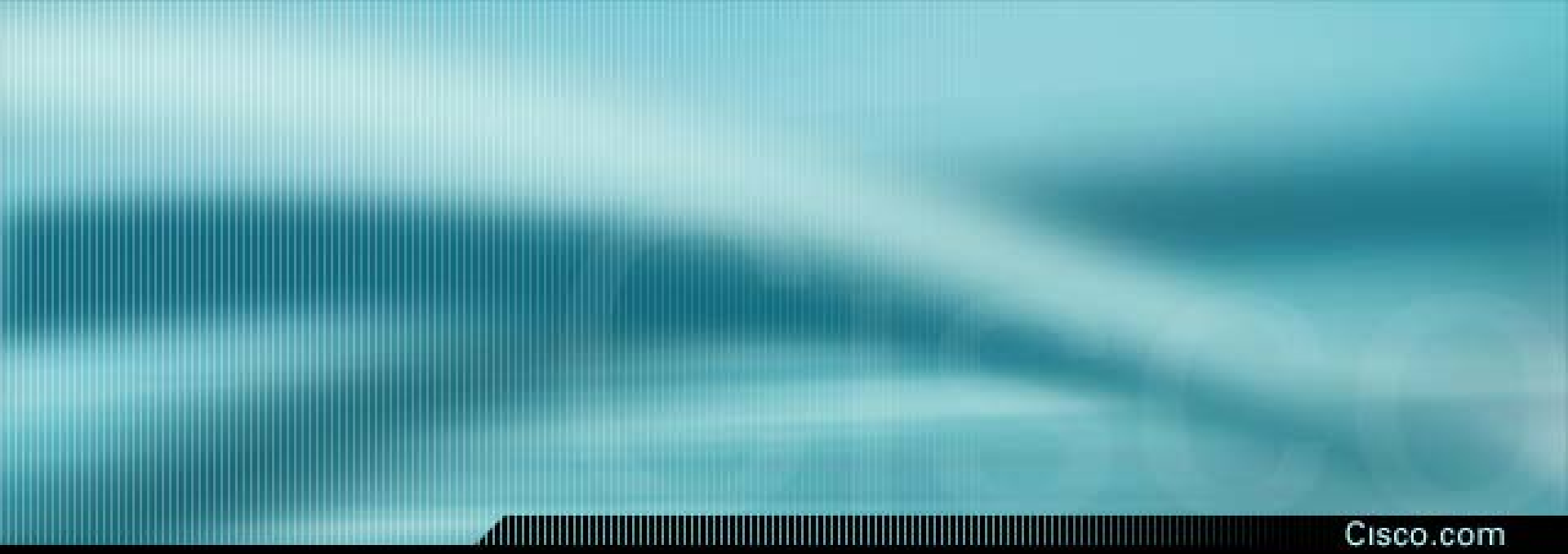


Mobile IP Traversal across IP Sec VPN Gateways

Gopal Dommety

gdommety@cisco.com

Design Team Status Update

- Started about one and a half months ago
- Draft-ietf-mobilip-vpn-problem-statement-req-0.txt
- Team: Recommended by WG chairs
  - *Farid Adrangi*
  - *Gopal Dommety*
  - *Qiang Zhang*
  - *Sami Vaarala*
  - *Nitsan Baider*
  - *Milind Kulkarni*
  - *Eli Gelasco*
  - *Dorothy Gellert*
  - *Henrik Levkowetz*

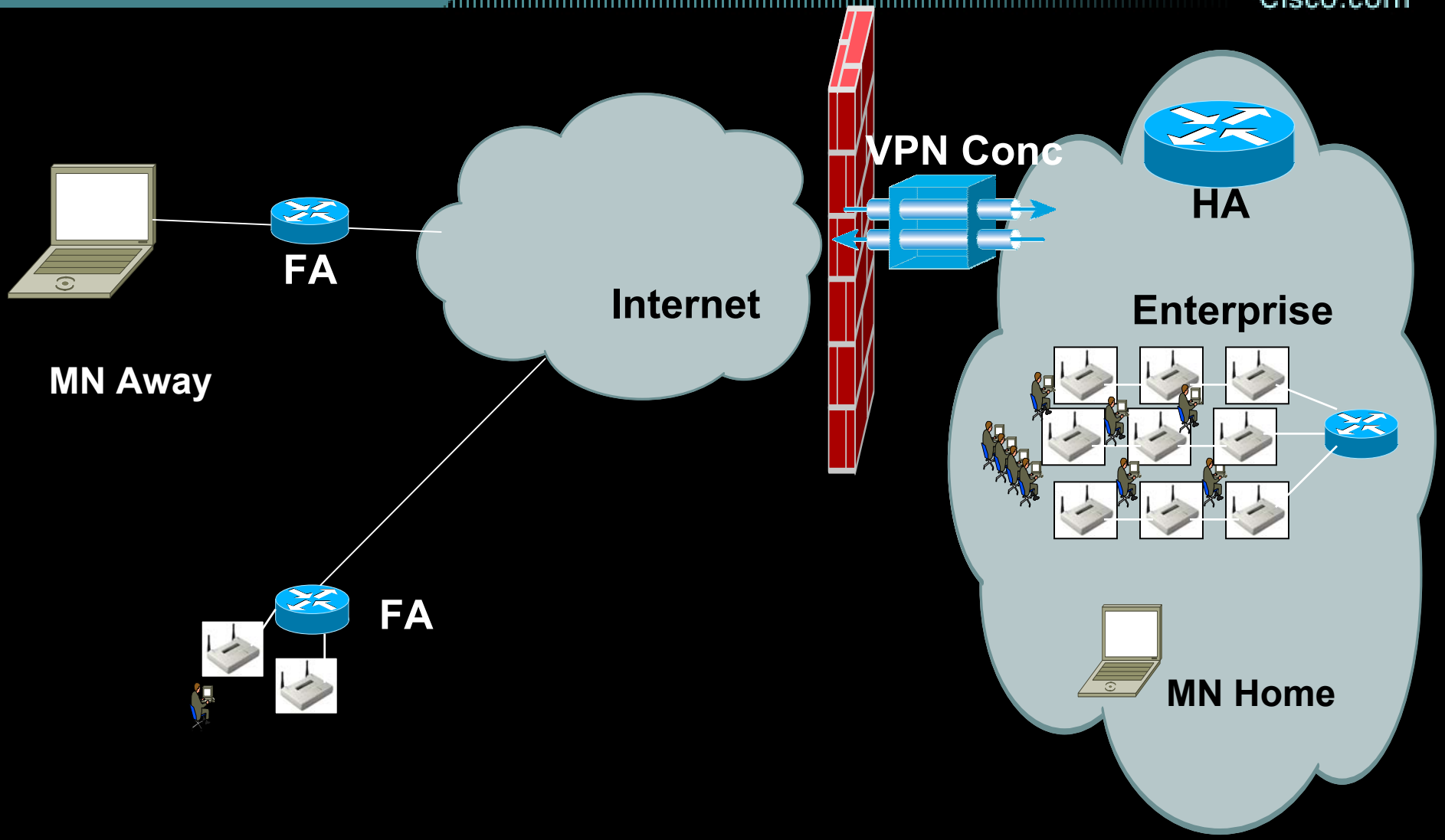
Steps…

- Form the Design Team (Mobile IP/VPN expertise)
- Define the Problem Statement
  - Document all the possible scenarios that could occur
  - Define clearly which of the scenarios we would like to focus on and why?
  - Solution requirements/Guidelines
- Get WG blessings on the Problem Statement
- Work on High level Solution with IPv4 Focus

Objective

- Seamless IP mobility across IPsec-based VPN gateways
- Identified 5 scenarios
  - Problems with these scenarios
  - Usefulness of each of these scenarios

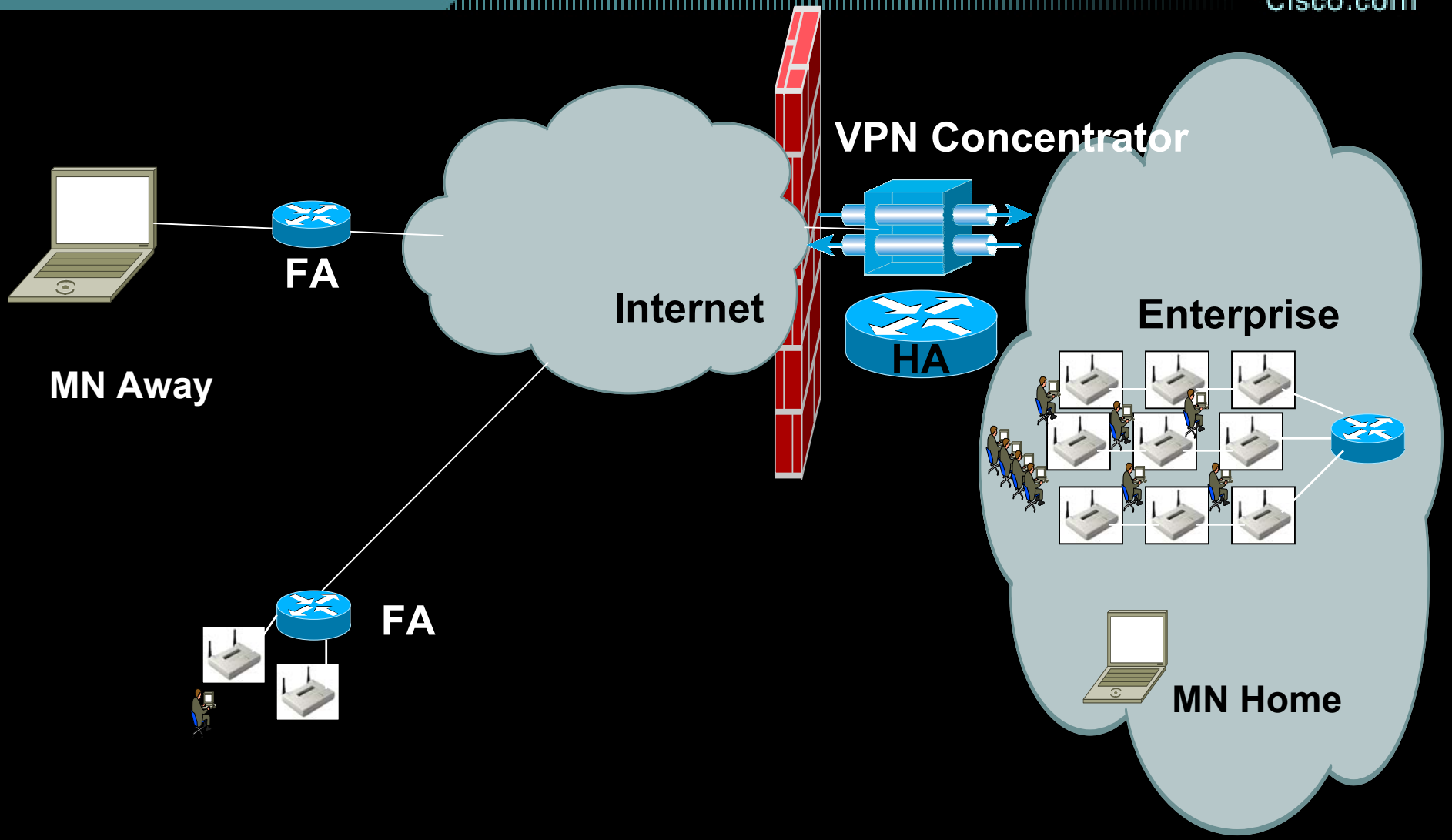
Scenario 1: HA inside the Internet



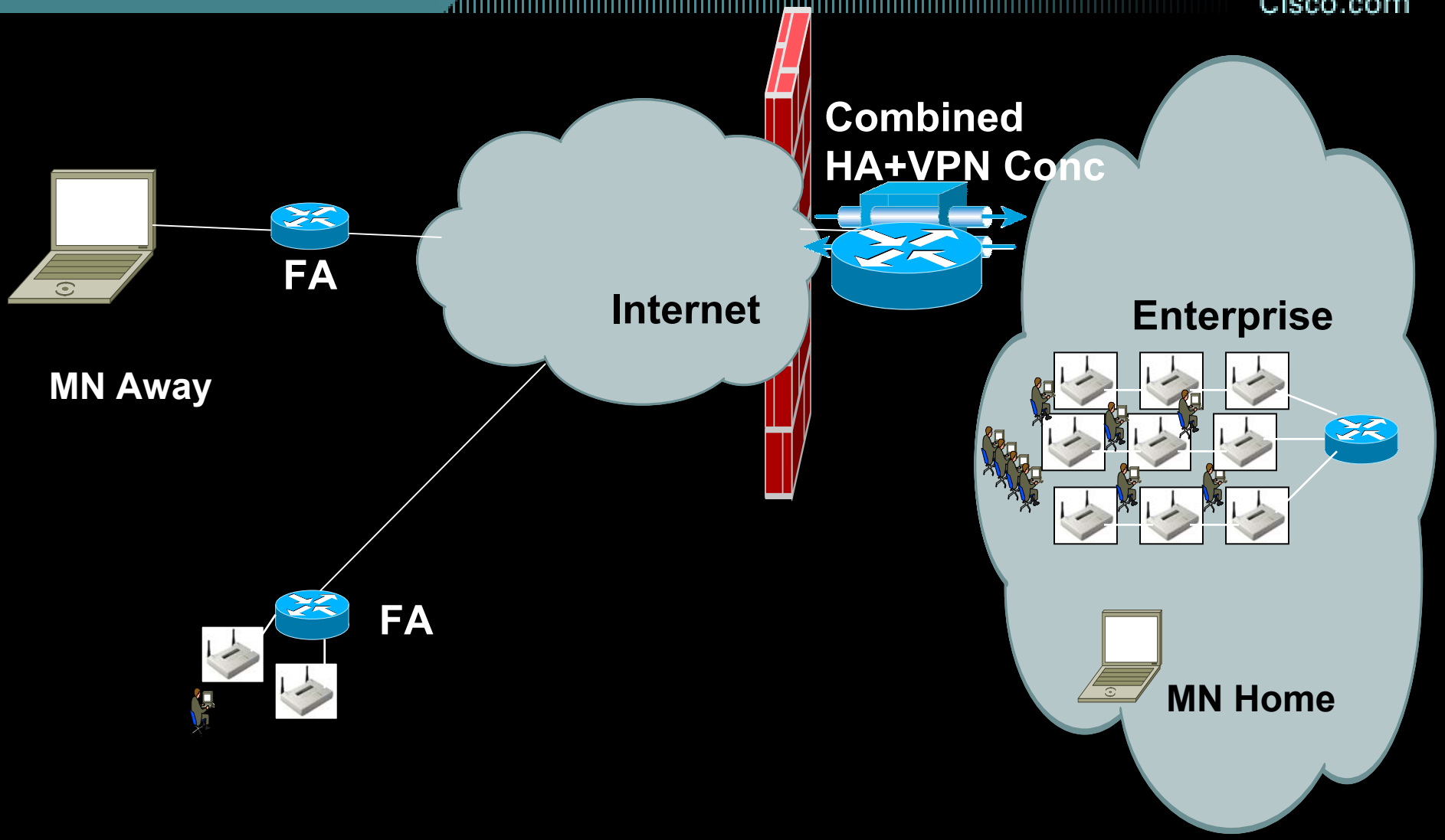
Mobility Support

- Mobility Support while outside the VPN Domain
- Mobility Support while inside the VPN Domain
- Mobility support while traversing between outside and inside the VPN Domain

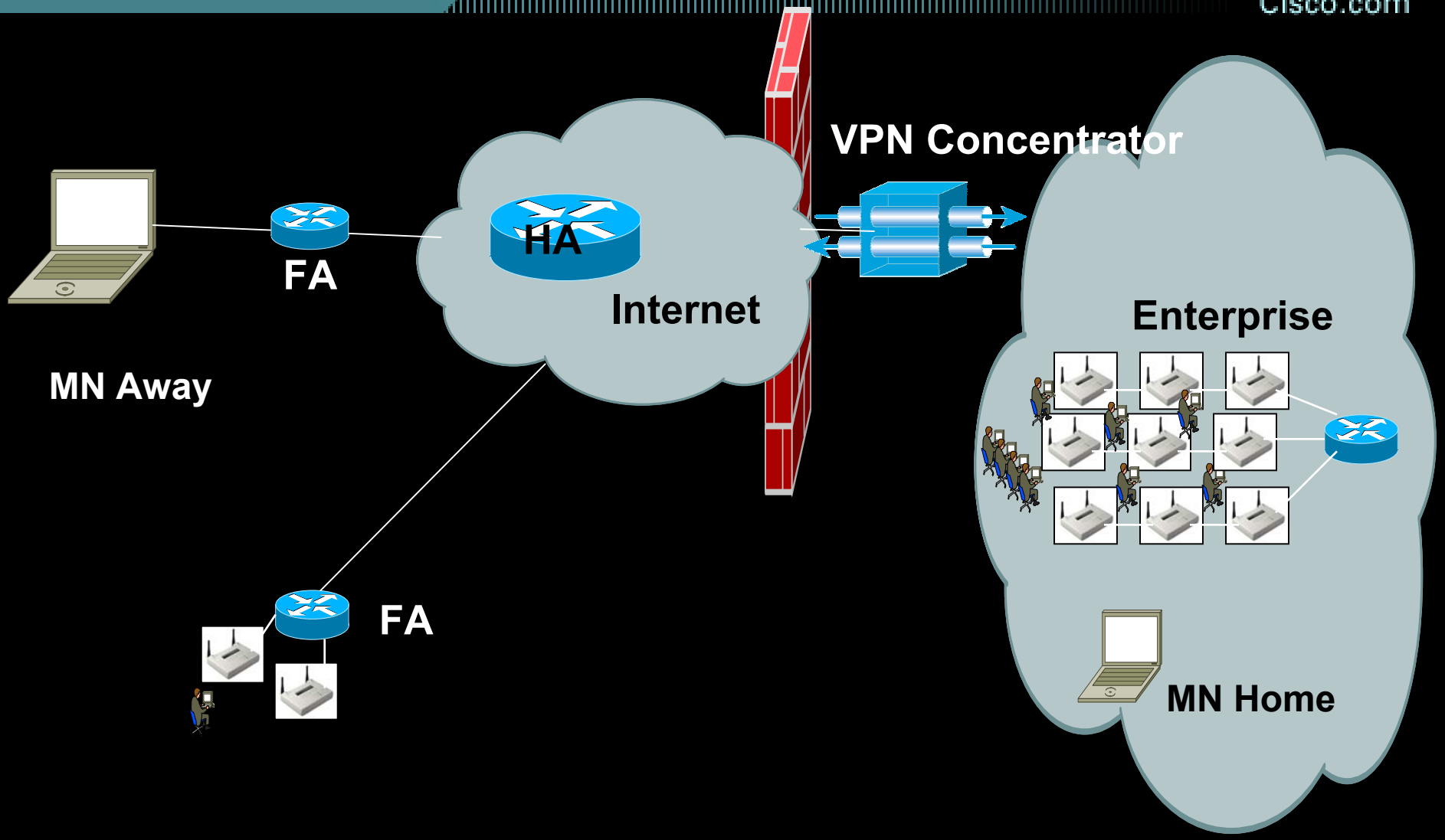
Scenario 2: HA in parallel to the VPN Concentrator



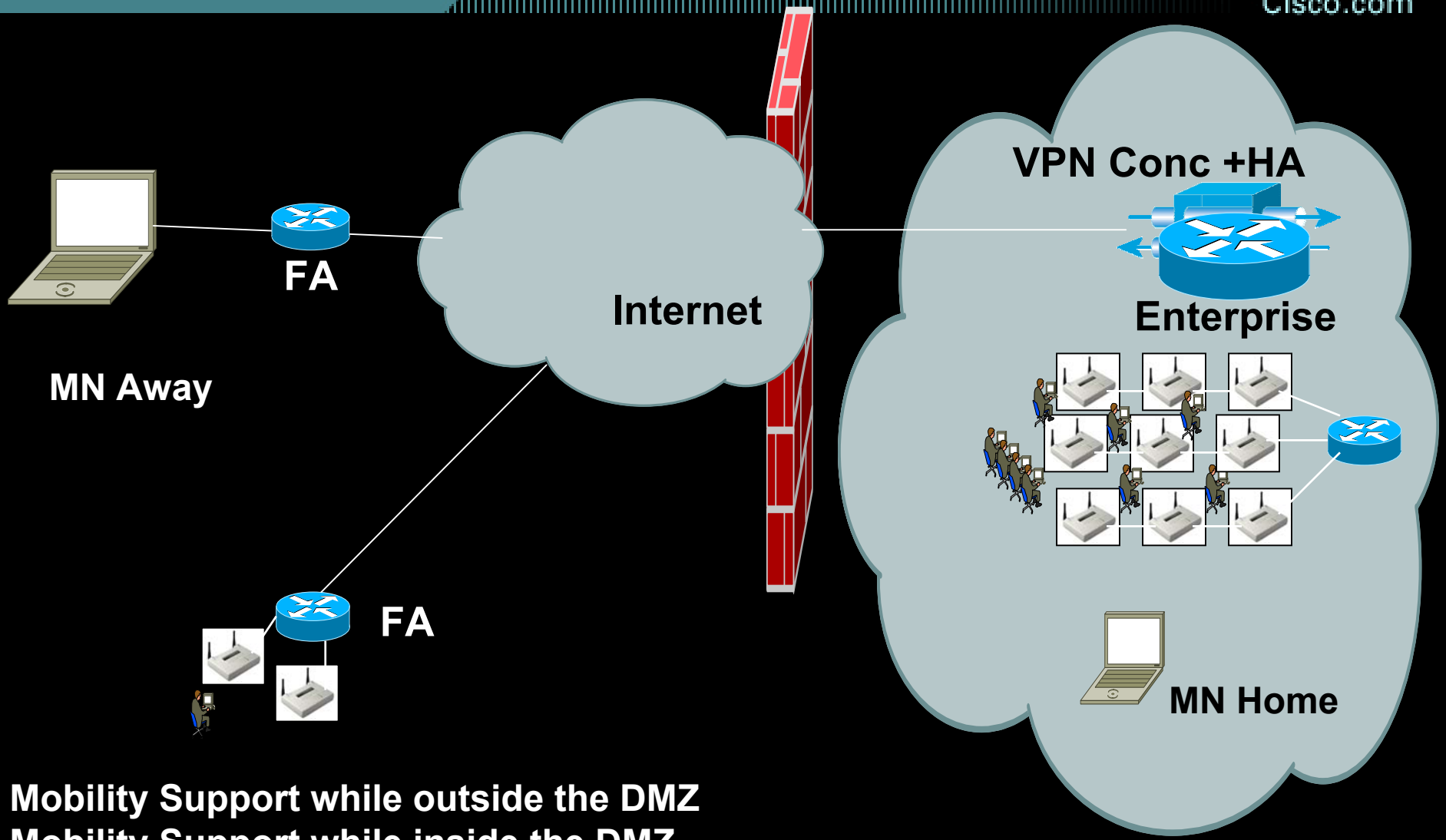
Scenario 3: Combined HA and VPN Gateway



Scenario 4: HA Outside the VPN Domain



Scenario 5: Combined HA + IP Sec conc on the local Link



Mobility Support while outside the DMZ
Mobility Support while inside the DMZ
Mobility support while traversing between outside and inside the DMZ

Solution Guidelines

- **VPN Requirements**
  - None or minimal IPSec changes
  - No Changes to existing VPN/DMZ Architecture/Design
  - Minimize Software upgrades to VPN concentrator
- **Mobile IP**
  - MUST adhere to Mobile IP Protocol
  - MAY Propose extensions
  - MAY require multiple Layers of Mobile IP Tunneling
  - MAY introduce multiple Mobile IP compliant entities
- **MUST NOT introduce any new Security Vulnerabilities**

Solution Guidelines

- Must Support Handoffs
- Scalability, Availability, Reliability, and Performance requirements
- MUST work with NAT Traversal

Promising Solution Options

- Dual Mobile IP Layering/Optimized Single Layer
  - Use of Two Home Agents
  - Use of Mobile IP signaling to VPN gateway (use of Update message to update the MN binding)
- Use of Proxy entity which is Mobile IP aware in conjunction with VPN concentrator
- Making VPN concentrator accept outer IP address changes with out breaking IP security
- Use of IP Sec tunnel instead of GRE/IPIP tunnel for Mobile IP Tunneling

Other Solutions

- Host Routing and End-to-End Security
- Explicit IP Sec Signaling to change IP address of the Outer IP Sec Header
- Explicit IP Sec signaling to include FA