VPN As A Service

Michael Ko
Edward Wang
Robert Raszuk
November 16, 2011
Dynamic Secure Interconnect

Internet

A1

B1

B2

B3

B4

A2

A3

A4

NAT

CGN
Issues to Address

• Connectivity Issues
  – Need for automated discovery of authorized node
  – Traversing network boundaries such as NATs, IPv4-to-IPv6 coexistence technologies, firewalls, etc.
  – Existing standards include SLP, TURN, ICE, etc.

• Security Issues
  – Creating security tunnels
    • No consistent end-to-end security policy
  – Existing standards include Kerberos, IPsec, TLS, SSH, PKCS, etc.

• Management Issues
  – Managing large virtual networks
    • Having to configure virtual network parameters on every node
  – Existing standards include SNMP, NETCONF, etc.
Need For a Central Server

- A network node consults a central server for information related to connection establishment with another node
  - Likely involves authentication
- Central server acts as information broker for both ends of the connection
  - Local IP address, address list for peer, STUN server address, credentials for secure tunnel, etc.
- A network then establishes a connection with the target node
  - Uses IPsec tunnel, DTLS, etc.
  - May use ICE, STUN or other mechanisms as needed to establish connectivity
- A protocol is needed for communicating between a network node and the central server and between central servers
  - Use or extend existing protocols if practicable
Dynamic, On-Demand Connection

- Node A interacts with central server to discover Node B
- Central server coordinates the parameter exchange of the connectivity and security policies for Nodes A & Node B
- Node A establishes a secure connection with Node B
• DSI Server manages all clients and resources in the cloud
  – Responsible for access authentication, resource monitoring and network addressing
• Changes in resource attributes are updated in DSI Server
Other Use Case

• DSI concept can be used to provide VPN As A Service (VAAS)
  – For applications with a need to establish VPN

• Central server is then the VAAS server
  – Manages and coordinates VPN service
Missing Pieces

• IETF has no generic service provisioning protocol to use for node-to-server communication

• Existing management protocols have different model
  – “Configure yourself”, rather than “provision me”
  – No ability to trigger provisioning of service across multiple nodes

• Existing data models (MIBs, Yang modules) could be used to hold data