LET’S BUILD TOMORROW TODAY
An Overview of Site-to-Site VPN Technologies

Nisha Kuruvilla – Technical Leader, Services
Hector Mendoza Jr. – Technical Leader, Services

BRKSEC-1050
Agenda

• VPN Technology Positioning
• SVTI, DVTI, DMVPN, GETVPN, and FlexVPN
  • Technology Overview
  • Why select said technology given network requirements
  • Configuration
  • Advantages/Disadvantages
  • Demos
  • Additional Points to Consider
• Summary
VPN Technology Positioning

Internet/Shared Network

Internet Edge

IPSec Agg.

Data Center Core

GET Encrypted

Remote Access SW Clients

Site-to-Site VPN

EzVPN/FlexVPN Client Spoke

DMVPN/FlexVPN Spoke

WAN Edge

MPLS/Private Network

GETVPN GM

GETVPN GM

GETVPN GM
Virtual Tunnel Interface (VTI)
Virtual Tunnel Interface

- IPsec in tunnel mode between VPN peers
- Simplifies VPN configuration
- Two types - Static VTI and Dynamic VTI (Enhanced EasyVPN)
- Supports Quality of Service (QoS), multicast, and other routing functions that previously required GRE
- Limited VPN interoperability support with non-Cisco platforms
What makes a SVTI a SVTI?

Partner’s Configuration

crypto map VPN 10 ipsec-isakmp
set peer 1.1.1.2
set transform-set TSET
match address 100

access-list 100 permit gre host 1.1.1.1 host 1.1.1.2

interface Tunnel0
ip address 10.1.1.1 255.255.255.0
tunnel source 1.1.1.1
tunnel destination 1.1.1.2

interface Ethernet0/0
ip address 1.1.1.1 255.255.255.0
crypto map VPN

Solution #1

crypto ipsec profile TP
set transform-set TSET

interface Tunnel0
ip address 10.1.1.2 255.255.255.0
tunnel source 1.1.1.2
tunnel destination 1.1.1.1
tunnel protection ipsec profile TP

Solution #2

crypto ipsec profile TP
set transform-set TSET

interface Tunnel0
ip address 10.1.1.2 255.255.255.0
tunnel source 1.1.1.2
tunnel mode ipsec ipv4
tunnel destination 1.1.1.1
tunnel protection ipsec profile TP

Possibilities

A. Solution #1
B. Solution #2
C. Solutions #1 & #2
D. None of the Above
Static VTI

- Statically configured tunnel via ‘tunnel mode ipsec ipv4/ipv6’ and tunnel protection
- Always up
- Interface state tied to underlying crypto socket state (IPsec SA)
- Can initiate and accept only one IPsec SA per VTI
- Routing determines traffic to be protected
- IPsec SA re-keyed even in the absence of any traffic
SVTI Configuration

crypto isakmp policy 1
  authentication pre-share
  encr aes

crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0

crypto ipsec transform-set TSET esp-aes esp-sha-hmac

crypto ipsec profile TP
  set transform-set TSET

interface Tunnel0
  ip address 192.168.100.1 255.255.255.0
  tunnel source FastEthernet0/0
  tunnel destination 1.1.1.2
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile TP

  ip route 192.168.2.0 255.255.255.0 Tunnel0

crypto isakmp policy 1
  authentication pre-share
  encr aes

crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0

crypto ipsec transform-set TSET esp-aes esp-sha-hmac

crypto ipsec profile TP
  set transform-set TSET

interface Tunnel0
  ip address 192.168.100.2 255.255.255.0
  tunnel source FastEthernet0/0
  tunnel destination 1.1.1.1
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile TP

  ip route 192.168.1.0 255.255.255.0 Tunnel0
When do you use it

- Used with site-to-site VPNs – to provide always-on traffic protection
- Need for routing protocols and/or multicast traffic to be protected by IPsec tunnel
- Eliminates the need of GRE
- Need for QoS, firewall, or other security services on a per tunnel basis
- Target Deployment: 2 - 50 sites with point to point connectivity and Cisco and Non-Cisco interoperability
Advantages

- Support for IGP dynamic routing protocol over the VPN (EIGRP, OSPF, etc.)
- Support for multicast
- Application of features such as NAT, ACLs, and QoS and apply them to clear-text or encrypted text
- Simpler configuration
- IPsec sessions not tied to any interface

Disadvantages

- No support for non-IP protocols
- Limited support for multi-vendor
- IPsec stateful failover not available
- Similar scaling properties of IPsec and GRE over IPsec
- Only tunnel mode
Dynamic VTI

- Dynamically instantiated IPsec virtual-access interface (not configurable) cloned from a pre-defined virtual-template
- Created on an incoming IPsec tunnel request
- Interface state tied to underlying crypto socket state (IPsec SA)
- Can support multiple IPsec SAs per DVTI
- Avoids the need for a routing protocol and hence scales better
Dynamic VTI

- Mainly used as Enhanced Easy VPN server for terminating
  - Enhanced Easy VPN Remote
  - Legacy Easy VPN Remote

- Easy VPN Remote supports 3 modes of operation
  - client mode
  - network extension mode
  - network extension plus mode

- A single DVTI can terminate tunnels using static VTIs or crypto map

- Can only terminate and cannot initiate an IPSec tunnel (except in the case of Enhanced Easy VPN Remote)
SVTI To DVTI

interface Tunnel0
- ip unnumbered Loopback1
- tunnel source FastEthernet0
- tunnel destination 192.168.2.1
- tunnel mode ipsec ipv4
- tunnel protection ipsec profile VTI

IKE Identity pkts to 192.168.2.1

Data Plane

Crypto Head End

192.168.2.1

tunnel protect ipsec profile ...

interface Virtual-Access n

Control Plane

Interface Virtual-Template n

crypto isakmp profile

Virtual-Access interface is spawned from the Virtual-Template
When do you use it

• Scalable connectivity for remote-access VPNs
• Need for QoS, firewall, or other security services on a per tunnel basis
• Single touch configuration needed on hub
• No need for routing protocols as it uses reverse route injection
• Target Deployment: 50 – 10,000+ sites with a hub-spoke layout and Cisco and Non-Cisco interoperability
DVTI (SVTI to DVTI)

**Spoke (SVTI)**

```plaintext
crypto isakmp policy 1
  encr aes
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 0.0.0.0

crypto ipsec transform-set TSET esp-aes esp-sha-hmac

crypto ipsec profile TP
  set transform-set TSET

interface Tunnel0
  ip unnumbered Loopback0
  tunnel source 1.1.1.2
  tunnel destination 1.1.1.1
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile TP
```

**Hub (DVTI)**

```plaintext
crypto isakmp policy 1
  encr aes
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 0.0.0.0

crypto isakmp profile VPN
  keyring default
  match identity address 0.0.0.0
  virtual-template 1

crypto ipsec transform-set TSET esp-aes esp-sha-hmac

crypto ipsec profile TP
  set transform-set TSET
  set isakmp-profile VPN

interface Virtual-Template1 type tunnel
  ip unnumbered Loopback0
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile TP
```
Enhanced Easy VPN Client To Server (using DVTI)

Enhanced Easy VPN remote:

```
crypto ipsec client ezvpn EZ
   connect manual
   group cisco key cisco
   local-address Ethernet0/0
   mode network-plus
   peer 1.1.1.1
   virtual-interface 1
   xauth userid mode interactive
!
interface Virtual-Template1 type tunnel
   ip unnumbered Loopback0
   tunnel mode ipsec ipv4
!
interface Ethernet0/0
   ip address 1.1.1.3 255.255.255.0
   crypto ipsec client ezvpn EZ
!
interface Ethernet0/1
   ip address 192.168.3.1 255.255.255.0
   crypto ipsec client ezvpn EZ inside
```
DVTI

Advantages

• Simple configuration of headend once and done
• Scalable
• Support for IGP dynamic routing protocol over the VPN
• Support for IP multicast
• Support for per-branch QoS and traffic shaping
• Centralized Policy Push (Easy VPN)
• Support for x-auth (Easy VPN)
• Cross platform support
• IPsec sessions not tied to any interface

Disadvantages

• Requires ip unnumbered
• No support for non-IP protocols
• No direct spoke to spoke communication
• No IPsec stateful failover
Dynamic Multipoint VPN (DMVPN)
What is Dynamic Multipoint VPN?

DMVPN is a Cisco IOS software solution for building IPsec+GRE VPNs in an easy, dynamic and scalable manner.

- Configuration reduction and no-touch deployment
- Dynamic spoke-spoke tunnels for partial/full mesh scaling
- Can be used without IPsec Encryption (optional)
- Wide variety of network designs and options
DMVPN Components

- **Next Hop Resolution Protocol (NHRP)**
  - Creates a distributed (NHRP) mapping database of all the spoke’s tunnel to real (public interface) addresses

- **Multipoint GRE Tunnel Interface (mGRE)**
  - Single GRE interface to support multiple GRE/IPsec tunnels
  - Simplifies size and complexity of configuration

- **IPsec tunnel protection**
  - Dynamically creates and applies encryption policies (optional)

- **Routing**
  - Dynamic advertisement of branch networks; almost all routing protocols (EIGRP, RIP, OSPF, BGP, ODR) are supported
Dynamic Multipoint VPN (DMVPN)

- Branch spoke sites establish an IPsec tunnel to and register with the hub site
- IP routing exchanges prefix information for each site
- BGP or EIGRP are typically used for scalability
- With WAN interface IP address as the tunnel address, provider network does not need to route customer internal IP prefixes
- Data traffic flows over the DMVPN tunnels
- When traffic flows between spoke sites, the hub assists the spokes to establish a site-to-site tunnel
- Per-tunnel QoS is applied to prevent hub site oversubscription to spoke sites
DMVPN How it works

- Spokes build a dynamic permanent GRE/IPsec tunnel to the hub, but not to other spokes. They register as clients of the NHRP server (hub).
- When a spoke needs to send a packet to a destination (private) subnet behind another spoke, it queries via NHRP for the real (outside) address of the destination spoke.
- Now the originating spoke can initiate a dynamic GRE/IPsec tunnel to the target spoke (because it knows the peer address).
- The dynamic spoke-to-spoke tunnel is built over the mGRE interface.
- When traffic ceases then the spoke-to-spoke tunnel is removed.
“Static” Spoke-Hub, Hub-Hub Tunnels

- GRE, NHRP and IPsec configuration
  - p-pGRE or mGRE on spokes; mGRE on hubs

- NHRP registration
  - Dynamically addressed spokes (DHCP, NAT,…)

- Data traffic on spoke-hub tunnels
  - All traffic for hub-and-spoke only networks
  - Spoke-spoke traffic while building spoke-spoke tunnels
Dynamic Spoke-Spoke Tunnels

- GRE, NHRP and IPsec configuration
  - mGRE on both hub and spokes

- Spoke-spoke unicast data traffic
  - Reduced load on hubs
  - Reduced latency
  - Single IPsec encrypt/decrypt

- On demand tunnel - created when needed

- NHRP resolutions and redirects
  - Find NHRP mappings for spoke-spoke tunnels
DMVPN – Phase3

Data packet
NHRP Redirect
NHRP Resolution

192.168.0.1/24

192.168.0.1/24

Physical: 172.17.0.1

Tunnel0: 10.0.0.1

Physical: (dynamic)

Tunnel0: 10.0.0.11

Spoke A

172.16.1.1

Physical: (dynamic)

Tunnel0: 10.0.0.11

Spoke A

192.168.1.1/24

172.16.2.1

Physical: (dynamic)

Tunnel0: 10.0.0.12

Spoke B

192.168.2.1/24

Data packet
NHRP Redirect
NHRP Resolution
Basic DMVPN Designs

- **Hub-and-spoke – Order(n)**
  - Spoke-to-spoke traffic via hub
    - Phase 1: Hub bandwidth and CPU limit VPN
    - SLB: Many “identical” hubs; increases CPU and bandwidth limits
  - Spoke-to-spoke – Order(n) ≪ Order(n^2)
    - Control traffic; Hub and spoke; Hub to hub
      - Phase 2: (single)
      - Phase 3: (hierarchical)
    - Unicast Data traffic; Dynamic mesh
      - Spoke routers support spoke-hub and spoke-spoke tunnels currently in use.
      - Hub supports spoke-hub traffic and overflow from spoke-spoke traffic.
  - Network Virtualization
    - VRF-lite; Multiple DMVPNs (one per VRF)
    - MPLS over DMVPN (2547oDMVPN); Single DMVPN (many VRFs)
Basic DMVPN Designs

Dual DMVPN Single Hub
Single mGRE tunnel on Hub,
two p-pGRE tunnels on Spokes

Single DMVPN Dual Hub
Single mGRE tunnel on all nodes
Multiple DMVPNs versus Single DMVPN

• Multiple DMVPNs
  • Best for Hub-and-spoke only
    • Easier to manipulate RP metrics between DMVPNs for Load-sharing
      • EIGRP – Route tags, Delay; iBGP – Communities, MED; OSPF – Cost
    • Performance Routing (PfR) selects between interfaces
  • Load-balancing over multiple ISPs (physical paths)
    • Load-balance data flows over tunnels → Better statistical load-balancing

• Single DMVPN
  • Best for spoke-spoke DMVPN
    • Can only build spoke-spoke within a DMVPN not between DMVPNs*
    • Slightly more difficult to manipulate RP metrics within DMVPN for Load-sharing
      • EIGRP – Route tags, delay; iBGP – Communities, MED; **OSPF – Can’t do**
  • Load-balancing over multiple ISPs (physical paths)
    • Load-balance tunnel destinations over physical paths → Worse statistical load-balancing
DMVPN Combination Designs (cont)

Hierarchical

Server Load Balancing

Spoke-to-hub tunnels
Spoke-to-spoke tunnels
Hub-to-hub tunnel
Network Virtualization

Separate DMVPN mGRE tunnel per VRF (VRF-lite)

- Hub routers handle all DMVPNs
  - Multiple Hub routers for redundancy and load

- IGP used for routing protocol outside of and over DMVPNs on Spokes and Hubs
  - Address family per VRF
  - Routing neighbor per spoke per VRF

- BGP used only on the hub
  - Redistribute between IGP and BGP for import/export of routes between VRFs
  - “Internet” VRF for Internet access and routing between VRFs

- Global routing table for routing DMVPN tunnel packets
DMVPN Network Virtualization Designs

VRF-lite

2547oDMVPN
Routing

• Supports all routing protocols, except ISIS
• Best routing protocols are EIGRP and BGP
• Hubs are routing neighbors with spokes and other hubs
• Spokes are only routing neighbors with hubs, not with other spokes
Hub Configuration

- **Pre-shared Key**
- **IPsec Profile**
- **NHRP Config**
- **EIGRP Summary**
- **MGRE**
- **Tunnel Protection**

```plaintext
crypto isakmp policy 1
  encr aes
  authentication pre-share
  group 2
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set TSET esp-aes esp-sha-hmac
  mode transport
  crypto ipsec profile TP
  set transform-set TSET

interface Tunnel
  ip address 10.0.0.1 255.255.255.0
  no ip redirects
  ip nhlp authentication cisco
  ip nhlp map multicast dynamic
  ip nhlp network-id 1111
  ip nhlp redirect
  tunnel key 10
  no ip split-horizon eigrp 10
  ip summary-address eigrp 10 192.168.0.0 255.255.0.0
  tunnel source FastEthernet0/0
  tunnel mode gre multipoint
  tunnel protection ipsec profile TP
```
crypto isakmp policy 1
  encr aes
  authentication pre-share
group 2
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set TSET esp-aes esp-sha-hmac
  mode transport
crypto ipsec profile TP
  set transform-set TSET

interface Tunnel
  ip address 10.0.0.2 255.255.255.0
  no ip redirect
  ip nhrp authentication cisco
  ip nhrp map 10.0.0.1 172.17.0.1
  ip nhrp map multicast 172.17.0.1
  ip nhrp network-id 1111
  ip nhrp nhs 10.0.0.1
  ip nhrp shortcut
tunnel key 10
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel protection ipsec profile TP
Advantages

- Dynamic partial or full mesh tunnels
- IP multicast support
- Supports dynamic routing protocols over the hub-and-spoke
- Supported on all Cisco IOS/IOS-XE router platforms
- IWAN Support
- Simplifies and shortens configurations
- Per tunnel QoS possible
- SGT (secure group tagging) with IKEv2
- Cisco Prime Management

Disadvantages

- No support for non-IP protocols
- IGP routing peers tend to limit the design scalability
- No interoperability with non-Cisco platforms or Cisco ASA
- Some added complexity with configuration and troubleshooting of DMVPN
- Multicast replication done on the Hub
## DMVPN Phases

<table>
<thead>
<tr>
<th>Phase 1 – 12.2(13)T</th>
<th>Phase 2 – 12.3(4)T (Phase 1 +)</th>
<th>Phase 3 – 12.4.(6)T (Phase 2 +)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hub and spoke functionality</td>
<td>Spoke to spoke functionality</td>
<td>More network designs and greater scaling</td>
</tr>
<tr>
<td>p-pGRE interface on spokes, mGRE on hubs</td>
<td>mGRE interface on spokes</td>
<td>Same Spoke to Hub ratio</td>
</tr>
<tr>
<td>Simplified and smaller configuration on hubs</td>
<td>Direct spoke to spoke data traffic reduces load on hubs</td>
<td>No hub daisy-chain</td>
</tr>
<tr>
<td>Support dynamically addressed CPEs (NAT)</td>
<td>Hubs must interconnect in daisy-chain</td>
<td>Spokes don’t need full routing table – can summarize</td>
</tr>
<tr>
<td>Support for routing protocols and multicast</td>
<td>Spoke must have full routing table – no summarization</td>
<td>Spoke-spoke tunnel triggered by hubs</td>
</tr>
<tr>
<td>Spokes don’t need full routing table – can summarize on hubs</td>
<td>Spoke-spoke tunnel triggered by spoke itself</td>
<td>Remove routing protocol limitations</td>
</tr>
</tbody>
</table>

- Routing protocol limitations
- NHRP routes/next-hops in RIB (15.2(1)T)
DMVPN Example

**Spoke A**
- Physical: 172.17.0.1
- Tunnel0: 10.0.0.1

**Spoke B**
- Physical: dynamic
- Tunnel0: 10.0.0.12

**LANs can have private addressing**

- **192.168.0.0/24**
- **192.168.1.0/24**
- **192.168.2.0/24**

**Static known IP address**
- **Go to hub tunnels**

**Dynamic unknown IP addresses**
- Spoke A to hub tunnels
- Spoke B to hub tunnels

LANs can have private addressing.
Basic Network Designs

• Hub-and-spoke – \( \text{Order}(n) \)
  • Spoke-to-spoke traffic via hub

• Spoke-to-spoke – \( \text{Order}(n) \ll \text{Order}(n^2) \)
  • Control traffic; Hub and spoke; Hub to hub
  • Unicast Data traffic; Dynamic mesh
    • Spoke routers support spoke-hub and spoke-spoke tunnels currently in use.
    • Hub supports spoke-hub traffic and overflow from spoke-spoke traffic.

• Network Virtualization
  • VRF-lite; Multiple DMVPNs
  • MPLS over DMVPN (2547oDMVPN); Single DMVPN
Network Designs

Hub and spoke (Phase 1)

Spoke-to-spoke (Phase 2)

VRF-lite

Server Load Balancing

Hierarchical (Phase 3)

2547oDMVPN

Spoke-to-hub tunnels
Spoke-to-spoke tunnels
2547oDMVPN tunnels
Group Encrypted Transport VPN (GETVPN)
Cisco Group Encrypted Transport (GET) VPN

Cisco GET VPN delivers a revolutionary solution for tunnel-less, any-to-any branch confidential communications

- Large-scale any-to-any encrypted communications
- Native routing without tunnel overlay
- Native Multicast support - improves application performance
- Transport agnostic - private LAN/WAN, FR/ATM, IP, MPLS
Header Preservation
IPSec Tunnel Mode vs. GETVPN

**IP Packet**
- IP Header
- IP Payload

**IPSec Tunnel Mode**
- New IP Header
- ESP
- IP Header
- IP Payload
- ▪ IPSec header inserted by VPN Gateway
- ▪ New IP Address requires overlay routing

**GETVPN**
- Preserved Header
- ESP
- IP Header
- IP Payload
- ▪ IP header preserved by VPN Gateway
- ▪ Preserved IP Address uses original routing plane
When should it be used?

- Securing an already secure network
- Efficient secure multicast traffic
- Deploying voice or similar collaborative applications requiring any-to-any encryption
- Encrypting IP packets over satellite links
Main Components of GETVPN

• GDOI (Group Domain of Interpretation,RFC 6407)
  • Cryptographic protocol for group key management

• Key Servers (KSs)
  • IOS devices responsible for creating /maintaining control plane
  • Distributing keys to the group members

• Group Members (GMs)
  • IOS devices used for encryption/decryption

• Group Security Associations
  • Tunnel-less Network
  • No Peer-to-Peer Tunnel required
  • IPsec SAs shared by GM’s

• IP Address Preservation
  • Original IP Address preserved
GDOI Reuses IKE on UDP 848

• Peer to Peer IPsec negotiation:

• IPsec Negotiations with GDOI (GETVPN)
  - Follows the IKE Phase 1

GDOI defines a Re-key exchange for subsequent key updates

– Can use multicast for efficiency
How does it work?

- Group Members (GMs) “register” via GDOI with the Key Server (KS)
  - KS authenticates & authorizes the GMs
  - KS returns a set of IPsec SAs for the GMs to use
How does it work? (cont’d)

- Data Plane Encryption
  - GMs exchange encrypted traffic using the group keys
  - Traffic uses IPSec Tunnel Mode with “address preservation”
How does it work? (cont’d)

• Periodic Rekey of Keys
  • KS pushes out replacement IPsec keys before current IPsec keys expire
  • Unicast rekey or Multicast rekey
Cooperative Key Servers - Redundancy

• A list of trusted key servers
  • Manages common set of keys and security policies for GMs
Group Security Elements

- Group Policy
- Key Encryption Key (KEK)
- Traffic Encryption Key (TEK)
- RFC3547: Group Domain of Interpretation (GDOI)
- Group Policy
- Key Servers
- Proprietary: KS Cooperative Protocol

Routing Members

Group Member

Group Member

Group Member

Group Member

Cisco Live!
Policy Management – ACL

- Permit ACLs can only be pushed from KS
- Deny ACLs can be configured locally on GM or pushed from KS
- Local GM ACL has precedence over downloaded KS ACL
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!
crypto isakmp policy 10
  encrypt aes
  authentication pre-share
!
crypto ipsec transform-set TSET esp-aes esp-sha-hmac
!
crypto ipsec profile GETVPN
  set transform-set TSET
!
access-list 150 permit ip any host 225.1.1.1
!
access-list 160 deny eigrp any any
access-list 160 deny pim any any
access-list 160 deny udp any any eq 848
access-list 160 permit ip any any

Pre-shared Key
ISAKMP Policy
IPSec Transform
IPSec Profile
Access-List used for defining rekey (useful in multicast rekeys only)
Access-list defining the encryption policy pushed to GMs
crypto gdoi group GETVPN
identity number 1234
    server local
        !rekey address ipv4 150 !
        rekey lifetime seconds 14400
        rekey retransmit 10 number 2
        rekey authentication mypubkey rsa GETVPN
        rekey transport unicast
        sa ipsec 1
    profile GETVPN
        match address ipv4 160
            address ipv4 1.1.1.1
        redundancy
            local priority 10
            peer address ipv4 1.1.1.2
!
GM Configuration

Pre-shared Key

crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
!

ISAKMP Policy

crypto isakmp policy 10
  encr aes
  authentication pre-share
!

crypto gdoi group getvpn1
  identity number 1234
  server address ipv4 1.1.1.1
!

crypto map GETVPN 10 gdoi
  set group getvpn1
!

GDOI Group

Crypto map on the interface

interface FastEthernet0/0
  crypto map GETVPN
GETVPN

Advantages
• Any-to-Any large scale (Site-to-Site)
• Multicast replication in IP WAN network
• Route Distribution Model + Stateful
• Group Protection
• Address Preservation - hence works well with QoS and traffic engineering
• SGT support

Disadvantages
• Suited for private IP network infrastructure
• Does not support non-IP protocols
• Cisco routers only
Additional Points Of Interest

• **IPv6**
  - VTI, DMVPN, GETVPN support IPv6 as either **overlay and/or transport protocol**
  - DMVPN needs to use IKEv2 if ipv6 is overlay

• **NAT**
  - IPsec, GRE over IPsec (transport), VTI, DMVPN (spokes- dynamic, hub -static NAT) – work well with NAT
  - GETVPN: NAT does **NOT** work between GM’s

• **VRF**
  - IPsec, GRE over IPsec, VTI, DMVPN are VRF aware
  - KS is **NOT** VRF aware, but GM is VRF aware

• **Management**
  - IPsec, GRE over IPsec, VTI, DMVPN, GETVPN can be managed by Cisco Security Manager and Cisco Prime Infrastructure

• **Suite-B** – Supported by all technologies, based on platform and version
FlexVPN
Flex VPN Overview

• IKEv2 based unified VPN that combines site-to-site, remote-access, hub-spoke and spoke-spoke topologies

• FlexVPN combines multiple frameworks into a single, comprehensive set of CLI and binds it together offering more flexibility and a means to extend functionality in the future

• FlexVPN offers a simple but modular framework that extensively uses the tunnel interface paradigm

• IKEv2 is a major protocol update
VPN Technology Selection

Death by a thousand questions…
EasyVPN, DMVPN and Crypto Maps

crypto isakmp client configuration group cisco
   key cisco123
   pool dvti
   acl 100
crypto isakmp profile dvti
   match identity group cisco
   client authentication list lvpn
   isakmp authorization list lvpn
   client configuration address respond
   virtual-template 1
crypto ipsec transform-set vpn-ts-set esp-3des esp-sha-hmac
   mode transport
crypto ipsec profile vpnprofile
   set transform-set vpn-ts-set
   interface Tunnel0
      ip address 10.0.0.254 255.255.255.0
      ip nhrp map multicast dynamic
      ip nhrp network-id 1
      tunnel source Serial1/0
      tunnel mode gre multipoint
      tunnel protection ipsec profile vpnprofile
crypto isakmp client configuration group cisco
   key pr3sh8r3dk3y
   pool vpnpool
   acl 110
crypto ipsec transform-set vpn-ts-set esp-3des esp-sha-hmac
   crypto isakmp profile vpnpool
   set transform-set vpn-ts-set
   interface Tunnel0
      ip address 10.0.0.254 255.255.255.0
      ip local pool dvti 192.168.2.1 192.168.2.2
      ip route 0.0.0.0 0.0.0.0 10.0.0.2
      access-list 100 permit ip 192.168.1.0 0.0.0.255 any
      access-list 110 permit ip 192.168.1.0 0.0.0.255 10.10.1.0 0.0.0.255
      access-list 110 permit ip 192.168.1.0 0.0.0.255 10.10.1.0 0.0.0.255
   crypto map client-vpn-map client authentication list userauthen
   crypto map client-vpn-map isakmp authorization list groupauthor
   crypto map client-vpn-map client configuration address initiate
   crypto map client-vpn-map client configuration address respond
   crypto map client-vpn-map 10 ipsec-isakmp dynamic dynamicmap
   interface FastEthernet0/0
      ip address 83.137.194.62 255.255.255.240
      crypto map client-vpn-map
      ip local pool vpnpool 10.10.1.1 10.10.1.254
      access-list 110 permit ip 192.168.1.0 0.0.0.255 10.10.1.0 0.0.0.255
Benefits of FlexVPN

- You can run Flex along all your existing IPsec VPNs
- Based on IKEv2 and not IKEv1
- Using GRE over IPsec or VTI as encapsulation
- Utilizing virtual interfaces - allowing per-spoke features like firewall, QoS, ACLs, etc
- Remote access server and client (software and hardware)
- Dynamic spoke to spoke tunnels
- Ease of configuration by using built-in defaults
When do you use it

- Customer requires IKEv2 features
- Customer desires to build site-to-site, remote-access, hub-spoke and spoke-spoke topologies utilizing a unified CLI
- Large Scale deployment (of spoke to spoke and hub and spoke)
- Customer wishes to reduce learning curve of implementing multiple different types of VPN connectivity

• Target Deployment: 50 – 10,000+ sites with a hub-spoke layout and Cisco and Non-Cisco interoperability, IoT
IKEv2 in a few words

• Defined in RFC 4306 - updated by RFC 5996
  • No interoperability with IKEv1
  • Not widespread … yet

• Both are using the same basic structure aiming at:
  • Privacy
  • Integrity
  • Authentication

• Both run over UDP 500/4500
Key Differentiators

<table>
<thead>
<tr>
<th></th>
<th>IKEv1</th>
<th>IKEv2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth messages</td>
<td>6 max</td>
<td>Open ended</td>
</tr>
<tr>
<td>First IPsec SA</td>
<td>9 msgs min</td>
<td>~ 4-6 msgs min</td>
</tr>
<tr>
<td>Authentication</td>
<td>pubkey-sig, pubkey-encr, PSK</td>
<td>Pubkey-sig, PSK, <strong>EAP</strong></td>
</tr>
<tr>
<td>Anti-DOS</td>
<td>Never worked</td>
<td>Works!</td>
</tr>
<tr>
<td>IKE rekey</td>
<td>Requires re-auth (expensive)</td>
<td>No re-auth</td>
</tr>
<tr>
<td>Notifies</td>
<td>Fire &amp; Forget</td>
<td>Acknowledged</td>
</tr>
</tbody>
</table>
IKEv2 Exchanges Overview

IKE_SA_INIT (2 messages)

IKE_AUTH + CREATE_CHILD_SA (2 messages)

CREATE_CHILD_SA (2 messages)

IKE_SA authentication parameters negotiated

IKE Authentication occurs & one CHILD_SA created

Second CHILD_SA created

Protect data

A

B
Complete Configuration

IKEv2 Proposal

IKEv2 Policy binds Proposal to peer

Keyring supports asymmetric PSK’s

IKEv2 profile using PSK for authentication

Local and remote authentication methods supported

crypto ikev2 proposal prop-1
encryption aes-cbc-128 3des
integrity sha1
group 2
!
crypto ikev2 policy site-policy
proposal prop-1
!
crypto ikev2 keyring V2-keyring
peer cisco
address 10.0.1.1
pre-shared-key local CISCO
pre-shared-key remote OCSIC
!
crypto ikev2 profile prof
match identity remote address 10.0.1.1
authentication local pre-share
authentication remote pre-share
keyring V2-keyring
IPsec – no further change

crypto ipsec transform-set TS esp-aes 128 esp-sha-hmac
!  
crypto ipsec profile ipsec_prof
  set transform-set TS
  set crypto ikev2 profile ikev2prof
!
interface Virtual-Template1 type tunnel
  ip unnumbered Ethernet0/0
  tunnel source Ethernet0/0
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile ipsec_prof

IPsec profile points to IKEv2 profile

Tunnel protection links IPsec to tunnel
Introducing Smart Defaults

- Intelligent, reconfigurable defaults
- Pre-existing constructs:
  - crypto ikev2 proposal
    - AES-CBC 256, 192,128, 3DES / SHA-512,384,256, SHA-1, MD5 / group 5, 2
  - crypto ikev2 policy (match any)
  - crypto ipsec transform-set (AES-128, 3DES / SHA, MD5)
  - crypto ipsec profile default (default transform set, ikev2 profile default)
- Only an IKEv2 profile called “default” needs to be created
Reconfigurable Defaults

• All defaults can be modified, deactivated and restored
• Default proposals pre-configured
  • for IKEv2
  • for IPsec
• Modifying defaults

- Restoring defaults
- Disabling defaults

crypto ikev2 proposal default
  encryption aes-cbc-128
  hash md5

crypto ipsec transform-set default aes-cbc 256 sha-hmac

default crypto ipsec transform-set

no crypto ikev2 proposal default

no crypto ipsec transform-set default
Modular Building Blocks

<table>
<thead>
<tr>
<th>Tunneling</th>
<th>Authentication Method</th>
<th>Tunnel Config</th>
<th>Config Mode Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRE/IPsec</td>
<td>Certificate</td>
<td>Static</td>
<td>Local config</td>
</tr>
<tr>
<td>Pure IPsec</td>
<td>Pre-shared Key</td>
<td>Dynamic</td>
<td>RADIUS</td>
</tr>
<tr>
<td></td>
<td>EAP (initiator)</td>
<td>crypto map</td>
<td>Hybrid</td>
</tr>
</tbody>
</table>

**Security policy & routing**
- IKEv2 “routing”
- BGP
- Static routes
- Reverse-Route Injection
- EIGRP or anything else!
Sample Configurations

- FlexVPN Site-to-Site Configuration using Crypto Maps
- FlexVPN Site-to-Site SVTI-SVTI Configuration using Digital Certificates
- FlexVPN Site-to-Site IPv6 over IPv4 using GRE Encapsulation (in reference slides)
- FlexVPN Hub & Spoke DVTI-SVTI using IKEv2 Routing
- FlexVPN Hub & Spoke using Flex Client
- FlexVPN Dynamic Spoke to Spoke
FlexVPN Site-to-Site Configuration using Crypto Maps

crypto ikev2 keyring ASA
peer ASA address 1.1.1.2 pre-shared-key cisco

crypto ikev2 profile PROF
match identity remote address 1.1.1.2 255.255.255.255 authentication local pre-share authentication remote pre-share keyring ASA

crypto ipsec transform-set TSET esp-aes esp-sha-hmac

crypto map VPN 10 ipsec-isakmp
set peer 1.1.1.2 set transform-set TSET set ikev2-profile PROF match address CRYPTOACL

ip access-list extended CRYPTOACL
permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
ip route 0.0.0.0 0.0.0.0 1.1.1.2

ASA requires local-authentication

crypto ipsec ikev2 ipsec-proposal IPROP
protocol esp encryption aes
tenprocol esp integrity sha-1

crypto map VPN 10 match address CRYPTOACL
crypto map VPN 10 set peer 1.1.1.1
crypto map VPN 10 set ikev2 ipsec-proposal IPROP crypto map VPN interface outside
crypto ikev2 policy 1 encryption aes integrity sha group 5 prf sha

crypto ikev2 enable outside
tunnel-group 1.1.1.1 type ipsec-l2l tunnel-group 1.1.1.1 ipsec-attributes ikev2 remote-authentication pre-shared-key cisco ikev2 local-authentication pre-shared-key cisco
access-list CRYPTOACL extended permit ip 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
route outside 192.168.1.0 255.255.255.0 1.1.1.1 1
FlexVPN Site-to-Site IPv6 over IPv4 using GRE Encapsulation

Asymmetric PSKs

Tunneling IPv6 over IPv4 Tunnel

Could use a routing protocol (IGP/BGP)

crypto ikev2 keyring KR
peer SPOKE2
address 2.2.2.1
pre-shared-key local CISCO
pre-shared-key remote CISCO

crypto ikev2 profile default
match identity remote address 2.2.2.1 255.255.255.255
authentication remote pre-share
authentication local pre-share
keyring local KR

interface Tunnel0
ip address 10.1.1.1 255.255.255.0
disable ipv6 address FE80::1
link-local
tunnel source Ethernet0/0
tunnel destination 2.2.2.1
tunnel protection ipsec profile default
ip route 192.168.2.0 255.255.255.0 Tunnel0
disable ipv6 route 2001::/64 Tunnel0

crypto ikev2 keyring KR
peer SPOKE1
address 1.1.1.1
pre-shared-key local CISCO
pre-shared-key remote CISCO

crypto ikev2 profile default
match identity remote address 1.1.1.1 255.255.255.255
authentication remote pre-share
authentication local pre-share
keyring local KR

interface Tunnel0
ip address 10.1.1.2 255.255.255.0
disable ipv6 address FE80::2
link-local
tunnel source Ethernet0/0
tunnel destination 1.1.1.1
tunnel protection ipsec profile default
ip route 192.168.1.0 255.255.255.0 Tunnel0
disable ipv6 route 2001::/64 Tunnel0

192.168.1.0/24
192.168.2.0/24
2001::1/64
2001::2/64
192.168.1.0/24
2001::1/64

Asymmetric PSKs

Tunneling IPv6 over IPv4 Tunnel

Could use a routing protocol (IGP/BGP)
FlexVPN Hub & Spoke DVTI-SVTI using IKEv2 Routing – Network Diagram
FlexVPN Hub & Spoke DVTI-SVTI using IKEv2 Routing – Hub configuration

aaa authorization network FLEX local
crypto ikev2 keyring SPOKES
peer ALL
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco123
crypto ikev2 authorization policy FLEXAUTHOR
  pool FLEXPOOL
  route set interface
  route set access-list 99
crypto ikev2 profile default
  match identity remote address 0.0.0.0
  authentication remote pre-share
  authentication local pre-share
  keyring local SPOKES
  dpd 10 2 periodic
  aaa authorization group psk list FLEX FLEXAUTHOR
  virtual-template 1

interface Virtual-Template1 type tunnel
  ip unnumbered FastEthernet0/1
  tunnel protection ipsec profile default
  ip local pool FLEXPOOL 10.1.1.1 10.1.1.10
  access-list 99 permit 192.168.0.0 0.0.255.255

Spoke Tunnel IP Pool
IKE v2 Route
FlexVPN Hub & Spoke DVTI-SVTI using IKEv2 Routing – Spoke Configuration

**Spoke Configuration**

```
interface Tunnel0
  ip address negotiated
tunnel source Ethernet0/0
tunnel destination 200.1.1.2
tunnel protection ipsec

aaa authorization network FLEX local

crypto ikev2 keyring HUB
  peer HUB
  address 200.1.1.2
  pre-shared-key cisco123

crypto ikev2 authorization policy FLEXAUTHOR
  route set interface
  route set access-list 99

crypto ikev2 profile default
  match identity remote address 200.1.1.2 255.255.255.255
  authentication remote pre-share
  authentication local pre-share
  keyring local HUB
  dpd 10 2 periodic
  aaa authorization group psk list FLEX FLEXAUTHOR

access-list 99 permit 192.168.2.0 0.0.0.255
```

**Advertisement**

- Interface IP: 192.168.2.0/24
- Local Authorization
- IKE v2 Route
FlexVPN Server

- FlexVPN Server is an IKEv2 RA Server that provides the IKEv2 headend functionality for Remote Access and Hub-Spoke topologies.

- FlexVPN Server Features include
  - Peer Authentication Using EAP
  - Per-user Attributes allows fetching per-user session attributes from AAA via IKEv2 authorization
  - IKEv2 Multi-SA dVTI

- Supported Remote Access Clients include Microsoft Windows 7/8 IKEv2 Client, Cisco IKEv2 AnyConnect Client, and Cisco IOS FlexVPN client
FlexVPN Client

- FlexVPN Client provides the IKEv2 Remote Access Client functionality
- FlexVPN Client Highlights
  - GRE encapsulation support that allows IPv4/IPv6 over IPv4/IPv6
  - Dynamic routing protocol support
  - Route exchange via config mode
  - Dynamic BGP peering
- FlexVPN Client Features
  - Backup Gateways
  - Dial backup
  - Split DNS
  - NAT
FlexVPN Hub & Spoke using Flex Client – Network Diagram

- Virtual-Access Interfaces
- Static Tunnel Interface with FlexVPN client

Network Diagram:
- 192.168.1.0/24
- 200.1.1.2
- 192.168.2.0/24
- Static Tunnel Interface with FlexVPN client
FlexVPN Hub & Spoke using Flex Client – Hub configuration

192.168.1.0/24

Spoke

192.168.2.0/24

crypto ikev2 keyring SPOKES
peer ALL
address 0.0.0.0 0.0.0.0
pre-shared-key cisco123

crypto ikev2 profile default
match identity remote address 0.0.0.0
authentication remote pre-share
authentication local pre-share
keyring local SPOKES
dpd 10 2 periodic
virtual-template 1

interface Virtual-Template1 type tunnel
ip unnumbered Ethernet0/1
tunnel source Ethernet0/0
tunnel protection ipsec profile default
router eigrp 1
network 192.168.1.1 0.0.0.0

IGP Routing

Wildcard PSK Keyring
IKEv2 profile named default

Creates Virtual-Access from Virtual-Template
FlexVPN Hub & Spoke using Flex Client – Spoke Configuration

```
interface Tunnel0
ip unnumbered Ethernet0/1
tunnel source Ethernet0/0
tunnel destination dynamic
tunnel protection ipsec profile default

crypto ikev2
match identity remote address 0.0.0.0
authentication remote pre-share
authentication local pre-share
keyring local HUBS
dpd 10 2 periodic

crypto ikev2 profile default
match identity remote address 0.0.0.0
authentication remote pre-share
authentication local pre-share
keyring local HUBS
dpd 10 2 periodic

crypto ikev2 client flexvpn FLEXCLIENT
peer 1 200.1.1.1
peer 2 200.1.1.2
client connect Tunnel0
```

- **Crypto IKEv2 Keyring**
  - HUBS
    - Peer HUB1
      - Address 200.1.1.1
      - Pre-shared-key cisco123
    - Peer HUB2
      - Address 200.1.1.2
      - Pre-shared-key cisco123

- **Crypto IKEv2 Profile Default**
  - Match identity remote address 0.0.0.0
  - Authentication remote pre-share
  - Authentication local pre-share
  - Keyring local HUBS
  - DPD 10 2 periodic

- **Crypto IKEv2 Client FlexVPN**
  - Peer 1 200.1.1.1
  - Peer 2 200.1.1.2
  - Client Connect Tunnel0

- **Interface Tunnel0**
  - IP Unnumbered Ethernet0/1
  - Tunnel Source Ethernet0/0
  - Tunnel Destination Dynamic
  - Tunnel Protection IPsec Profile Default

- **Client FlexVPN Construct**
  - Tunnel Destination Selected from flexvpn client

```
router eigrp 1
network 192.168.1.0 0.0.0.0
```
Spoke – Dynamic Tunnel Source/Destination

```
interface Tunnel0
  ip unnumbered Loopback0
tunnel source dynamic
tunnel destination dynamic
tunnel protection ipsec profile default

crypto ikev2 keyring PEERS
  peer ALL
    address 0.0.0.0 0.0.0.0
    pre-shared-key cisco

crypto ikev2 profile PROF
  match identity remote address 0.0.0.0
  authentication remote pre-share
  authentication local pre-share
  keyring local PEERS
dpd 30 2 on-demand

crypto ikev2 client flexvpn FLEXCLIENT
  peer 1 200.1.1.1 track 1
  peer 2 200.1.1.2
  peer reactivate
  source 1 Ethernet0/0 track 2
  source 2 Ethernet0/1 track 3
  client connect Tunnel0

crypto ipsec profile default
  set ikev2-profile PROF

track 1 ip sla 1
  delay down 10 up 10

track 2 ip sla 2
  delay down 10 up 10

track 3 to interface Ethernet0/1

ip sla 1
cmd-echo 200.1.1.1
  frequency 5
  ip sla schedule 1 life forever start-time now

ip sla 2
cmd-echo 209.1.2.2 source-interface Ethernet0/0
  frequency 5
  ip sla schedule 2 life forever start-time now

interface Ethernet0/0
  ip address 209.1.2.1 255.255.255.0

interface Tunnel0
  ip route 0.0.0.0 0.0.0.0 209.1.2.2 track 2

interface Ethernet0/1
  ip address 209.1.3.1 255.255.255.0

ip route 0.0.0.0 0.0.0.0 209.1.3.2 track 3
```
FlexVPN Spoke to Spoke

- **FlexVPN Hub-Spoke, Spoke-Spoke**
  - Uses sVTI/dVTI, NHRP and routing protocol
  - No NHRP registrations from spokes to hub
  - No GRE multipoint interface

- **Routing Protocol**
  - Routing protocol run over FlexVPN hub-spoke tunnels
  - Allows spokes to learn networks behind other spokes

- **NHRP**
  - Resolves spoke overlay addresses to transport addresses

- **IPSec Virtual-Access Interface (VA)**
  - IPSec VA created on either side, per spoke tunnel
FlexVPN Spoke to Spoke Protocol Flow

- **Hub-Spoke tunnels**
  1. Spokes connect to hub, IPSec-VA created on hub for each spoke
  2. IPSec-VAs for all spokes share network id
  3. Hub learns spoke networks via routing protocol over hub-spoke tunnels
  4. Hub advertizes summarized route (via hub) to all spokes

- **NHRP redirect**
  1. Spoke to spoke traffic forwarded to hub
  2. Hub detects ingress and egress interfaces (IPSec-VAs) share NHRP network id
  3. Hub sends NHRP traffic redirect indication to source spoke with destination spoke overlay address
FlexVPN Spoke to Spoke Protocol Flow

- **NHRP Resolution**
  1. Spoke receiving redirect initiates NHRP resolution via hub to resolve destination spoke
  2. Hub forwards resolution request to destination spoke
  3. Destination spoke receives resolution request, creates VA and crypto tunnel to source spoke
  4. Destination spoke sends resolution reply over spoke-spoke direct tunnel
  5. Destination spoke adds NHRP cache entry for source spoke

- **NHRP Shortcut**
  1. Source spoke receives NHRP resolution reply
  2. Source spoke adds NHRP cache entry and shortcut route for destination spoke
FlexVPN Spoke to Spoke – Network Diagram
FlexVPN Spoke to Spoke – Hub configuration

crypto ikev2 keyring SPOKES
  peer ALL
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco123

crypto ikev2 profile default
  match identity remote address 0.0.0.0
  authentication remote pre-share
  authentication local pre-share
  keyring local SPOKES
  virtual-template 1

router eigrp 100
distribute-list EIGRP_SUMMARY out Virtual-Template1
network 172.16.0.0 0.0.0.0
redistribute static metric 1500 10 10 1 1500
ip route 172.16.0.0 255.255.0.0 Null0
ip access-list standard EIGRP_SUMMARY
permnit 172.16.0.0 0.0.255.255
**FlexVPN Spoke to Spoke – Spoke configuration**

```
import interface Virtual-Template1

    type tunnel
eip unnumbered FastEthernet0/1

    ip nhrp network-id 1
eip nhrp holdtime 300
eip nhrp shortcut virtual-template 1
tunnel source FastEthernet0/0
tunnel destination 200.1.1.2
tunnel protection ipsec profile default

```

```
interface Tunnel0

eip unnumbered FastEthernet0/1
eip nhrp network-id 1
eip nhrp holdtime 300
eip nhrp shortcut virtual-template 1
tunnel source FastEthernet0/0
tunnel destination 200.1.1.2
tunnel protection ipsec profile default

```

```
cryptokeykeyring SPOKES
    peer ALL
    address 0.0.0.0 0.0.0.0
    pre-shared-key cisco123

```

```
cryptokeykeyring SPOKES
    match identity remote address 0.0.0.0
    authentication remote pre-share
    authentication local pre-share
    keyring local SPOKES
    virtual-template 1

```

```
router eigrp 100

```

```
network 172.16.2.0 0.0.0.0
passive-interface default
no passive-interface Tunnel0
no passive-interface Ethernet0/1
```

**Virtual-Template is used for Spoke-Spoke Communication**

**Tunnel0 is used for Hub-Spoke Communication**

**Shortcut switching**

**Prevent EIGRP Neighbors on VAI**

---

172.16.0.0/24

172.16.2.0/24
Summary Route Advertisement

• Redistributing a static route pointing to null0 (Preferred option). This option allows to have control over summary and redistribution without touching hub’s VT configuration.

  ip route 172.16.0.0 255.255.0.0 Null0
  ip access-list standard EIGRP_SUMMARY
    permit 172.16.0.0 0.0.255.255
  router eigrp 100
  distribute-list EIGRP_SUMMARY out Virtual-Template1
  redistribute static metric 1500 10 10 1 1500

• DMVPN-style summary address on Virtual-template. This configuration is not recommended because of internal processing and replication of said summary to each virtual access. It is shown here for reference:

  interface Virtual-Template1 type tunnel
  ip summary-address eigrp 100 172.16.0.0 255.255.0.0
Advantages

• Leverages IKEv2 Protocol
• Large Scale Hub-Spoke with dynamic spoke-to-spoke
• VPN Concentrator for Remote Access
• Can be deployed either on public or private networks
• Centralized Policy Management with AAA
• Failover (dynamic and IKEv2 based routing)
• Multicast
• Per-tunnel QoS at Hub
• 3rd Party Compatible

Disadvantages

• Not backward compatible with IKEv1
• Currently supported only on ISR-G2s, ASR1k and 8xx routers)
### Summary

<table>
<thead>
<tr>
<th>Features</th>
<th>Standard IPsec</th>
<th>GRE over IPsec</th>
<th>Easy VPN/DVTI</th>
<th>SVTI</th>
<th>DMVPN</th>
<th>GETVPN</th>
<th>FlexVPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>3rd Party Compatibility</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>AAA attributes support</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Dynamically addressed spoke</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Dynamic Routing</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Dynamic Spoke to Spoke tunnel</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>IKEv2</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>PublicTransport</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>IPv6</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>IP Multicast</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>NAT</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Inline tagging (IKEv2)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>QoS</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>VRF</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Complete Your Online Session Evaluation

- Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a $750 Amazon gift card.

- Complete your session surveys though the Cisco Live mobile app or your computer on Cisco Live Connect.

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online

Note: This slide is now a Layout choice
Participate in the “My Favorite Speaker” Contest

Promote Your Favorite Speaker and You Could Be a Winner

• Promote your favorite speaker through Twitter and you could win $200 of Cisco Press products (@CiscoPress)

• Send a tweet and include
  • Your favorite speaker’s Twitter handle
  • Two hashtags: #CLUS #MyFavoriteSpeaker

• You can submit an entry for more than one of your “favorite” speakers

• Don’t forget to follow @CiscoLive and @CiscoPress

• View the official rules at http://bit.ly/CLUSwin
Continue Your Education

• Demos in the Cisco campus
• Walk-in Self-Paced Labs
• Table Topics
• Meet the Engineer 1:1 meetings
• Related sessions
Thank you
TOMORROW starts here.