FlexVPN for Carrier Network Security

Alex HONORÉ <ahonore@cisco.com>

Customer Support Engineer, Cisco TAC

Session Agenda

- Overview of FlexVPN
- Case Study: Managed Remote Access
  - Use Case #1: Single Customer, Multiple VRFs
  - Use Case #2: Multiple Customers & VRFs
- Case Study: Mixed Client & Branch Access
- Case Study: MPLS VPN Dynamic Mesh
- Further Information
- Q & A

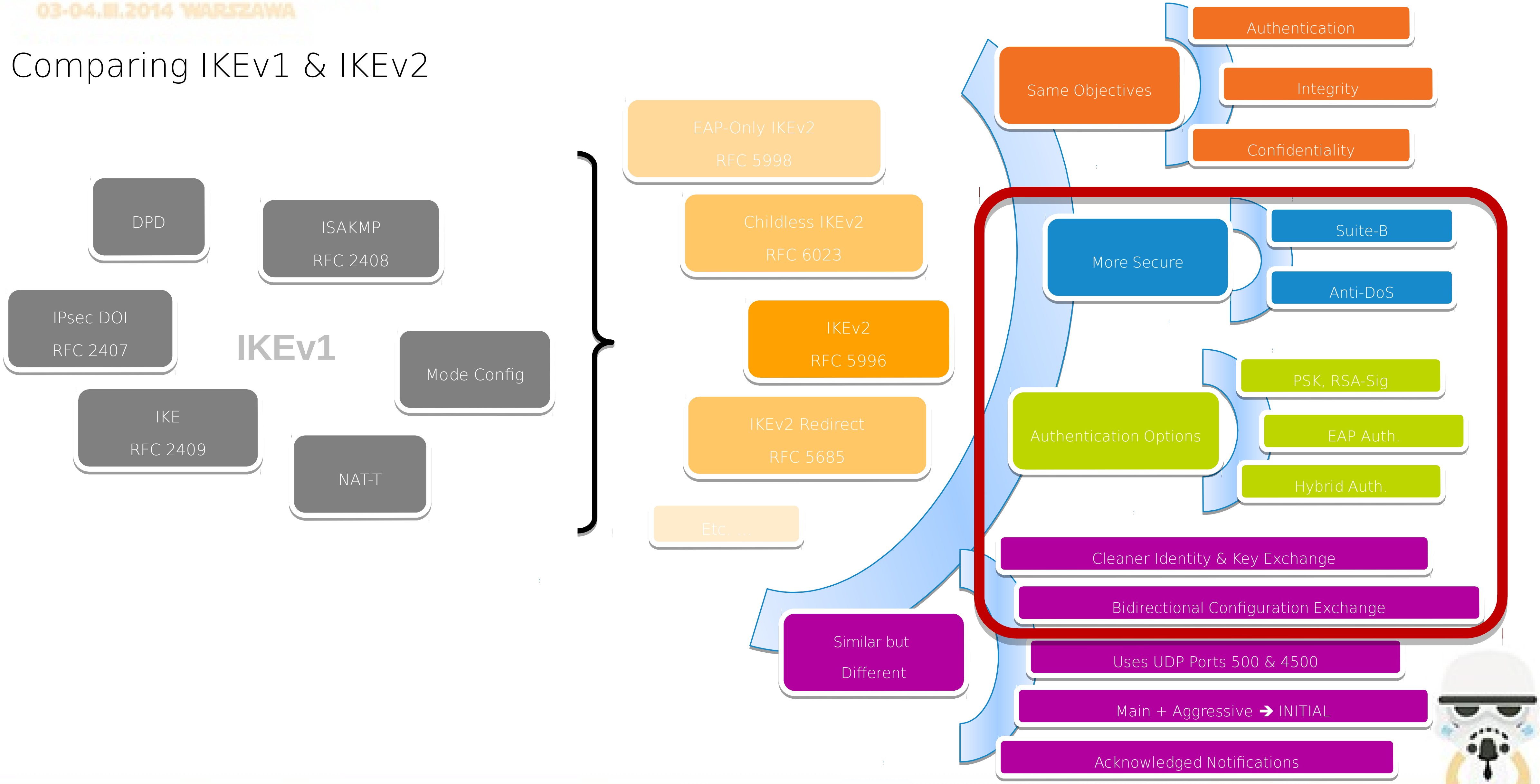
Overview of FlexVPN

Solution Positioning

	Interop.	Dynamic Routing	IPsec Routing	Spoke to Spoke Direct	Remote Access	Simple Failover	Source Failover	Config Push	Per-Peer Config	Per-Peer QoS	Full AAA Mgmt
Easy VPN	No	No	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Complex
DMVPN	No	Yes	No	Yes	No	Partial	No	No	No	Group	No
Crypto Map	Yes	No	Yes	No	Yes	Poor	No	No	No	No	No
FlexVPN	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

- One VPN to learn and deploy
- Everything works – no questions asked

Comparing IKEv1 & IKEv2



IKEv1

DPD

ISAKMP RFC 2408

IPsec DOI RFC 2407

Mode Config

IKE RFC 2409

NAT-T

EAP-Only IKEv2 RFC 5998

Childless IKEv2 RFC 6023

IKEv2 RFC 5996

IKEv2 Redirect RFC 5685

Etc. ...

Same Objectives
- Authentication
- Integrity
- Confidentiality

More Secure
- Suite-B
- Anti-DoS

Authentication Options
- PSK, RSA-Sig
- EAP Auth.
- Hybrid Auth.

Similar but Different
- Cleaner Identity & Key Exchange
- Bidirectional Configuration Exchange
- Uses UDP Ports 500 & 4500
- Main + Aggressive → INITIAL
- Acknowledged Notifications

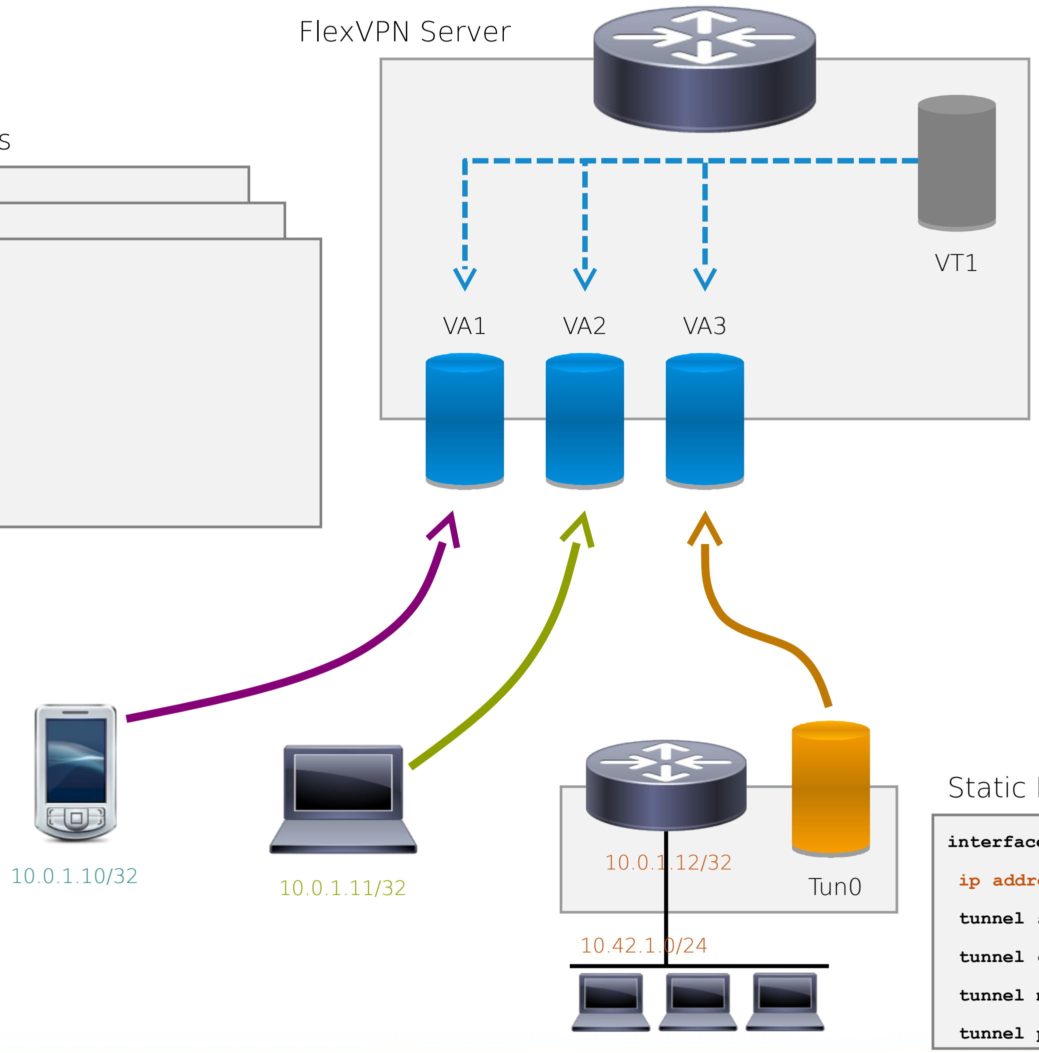
Dynamic Point-to-Point Virtual Interfaces

Dynamically instantiated P2P interfaces

```
interface Virtual-Access1
 i
 t
 t
 t
 t
 s
```

```
interface Virtual-Access2
 i
 t
 t
 t
 t
 t
 s
```

```
interface Virtual-Access3
 ip unnumbered Loopback0
 tunnel source <local-address>
 tunnel destination <remote-address>
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
 service-policy output home-office-QoS
```



P2P virtual interface template

```
crypto ikev2 profile default
 ...
 virtual-template 1
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
```

Server routing table (RIB/FIB)

```
S default via Ethernet0/0
L 10.0.1.1/32 local Loopback0
S 10.0.1.10/32 via Virtual-Access1
S 10.0.1.11/32 via Virtual-Access2
S 10.0.1.12/32 via Virtual-Access3
S 10.42.1.0/24 via Virtual-Access3
```

Static P2P virtual interface

```
interface Tunnel0
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel destination <server-address>
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
```

Configuration Example

```
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn router.cisco.com
 authentication local rsa-sig
 authentication remote eap
 pki trustpoint root sign
 aaa authentication eap default
 aaa authorization user eap
 virtual-template 1
```

IKEv2 identity & profile selection

IKEv2 authentication & certificates

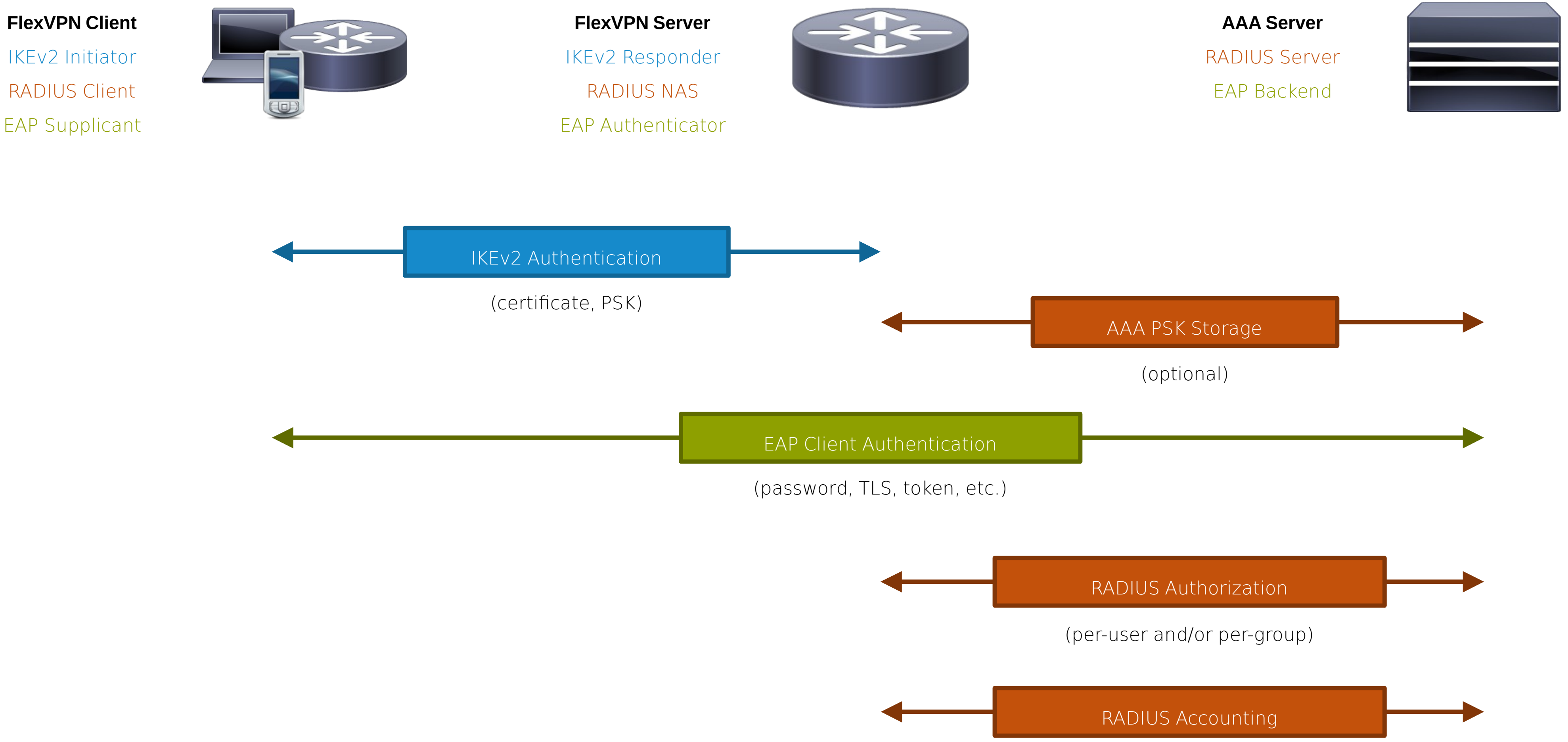
AAA integration (authentication, authorization, accounting)

```
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
```

Dynamic point-to-point interfaces

Native IPsec tunnel or GRE/IPsec

High-Level Functional Interactions



FlexVPN Client
IKEv2 Initiator
RADIUS Client
EAP Supplicant

FlexVPN Server
IKEv2 Responder
RADIUS NAS
EAP Authenticator

AAA Server
RADIUS Server
EAP Backend

IKEv2 Authentication
(certificate, PSK)

AAA PSK Storage
(optional)

EAP Client Authentication
(password, TLS, token, etc.)

RADIUS Authorization
(per-user and/or per-group)

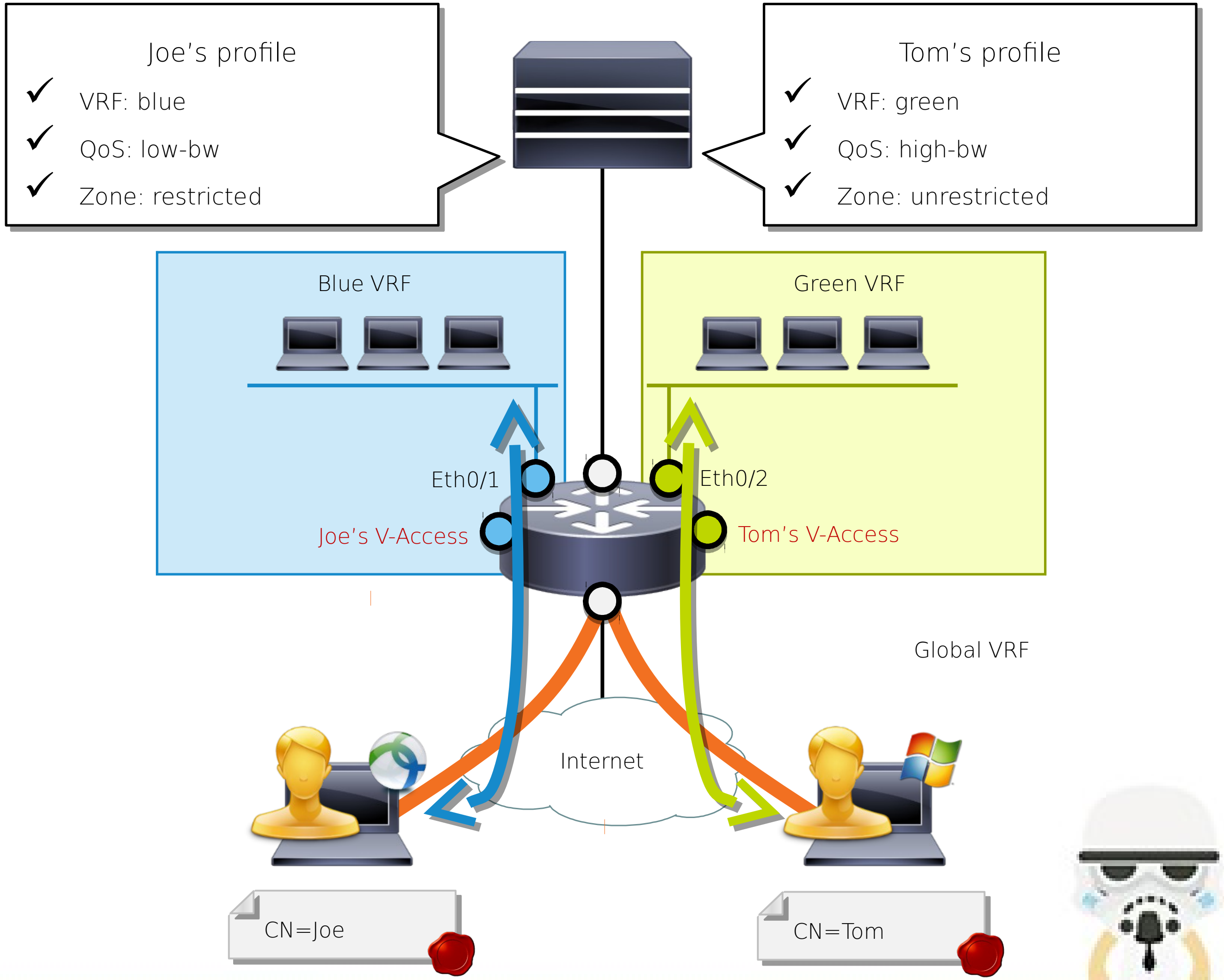
RADIUS Accounting

Case Study:

Managed Remote Access

Use Case #1: Single Customer, Multiple VRFs

- Requirements:
  - Certificate-based authentication
  - Cisco AnyConnect VPN client & Windows native IKEv2 client
  - Per-user features pushed via AAA (VRF, ZBF, QoS, …)
- Proposed solution:
  - Single IKEv2 profile & V-Template
  - RADIUS authorization for certificate CN
  - Per-user interface-config strings



Joe’s profile

✓ VRF: blue

✓ QoS: low-bw

✓ Zone: restricted

Tom’s profile

✓ VRF: green

✓ QoS: high-bw

✓ Zone: unrestricted

FlexVPN Server Configuration

RADIUS-based authorization

Match on peer identity certificate

Extract CN from IKE ID of type DN

Mutual RSA-Sig authentication

Per-user authorization based on CN

Minimal V-Template for all clients

```
aaa new-model
aaa authorization network my-rad group my-rad
!
crypto pki certificate map my-map 1
 issuer-name co o = my-org
!
crypto ikev2 name-mangler cert-cn
 dn common-name
!
crypto ikev2 profile default
 match certificate my-map
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint my-ca
 aaa authorization user cert list my-rad name-mangler cert-cn
 virtual-template 1
!
interface Virtual-Template1 type tunnel
 no ip address
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
```

RADIUS Server Configuration

Client address pool, V-Access & IP unnumbered in VRF blue

Per-user interface commands for QoS & ZBF features

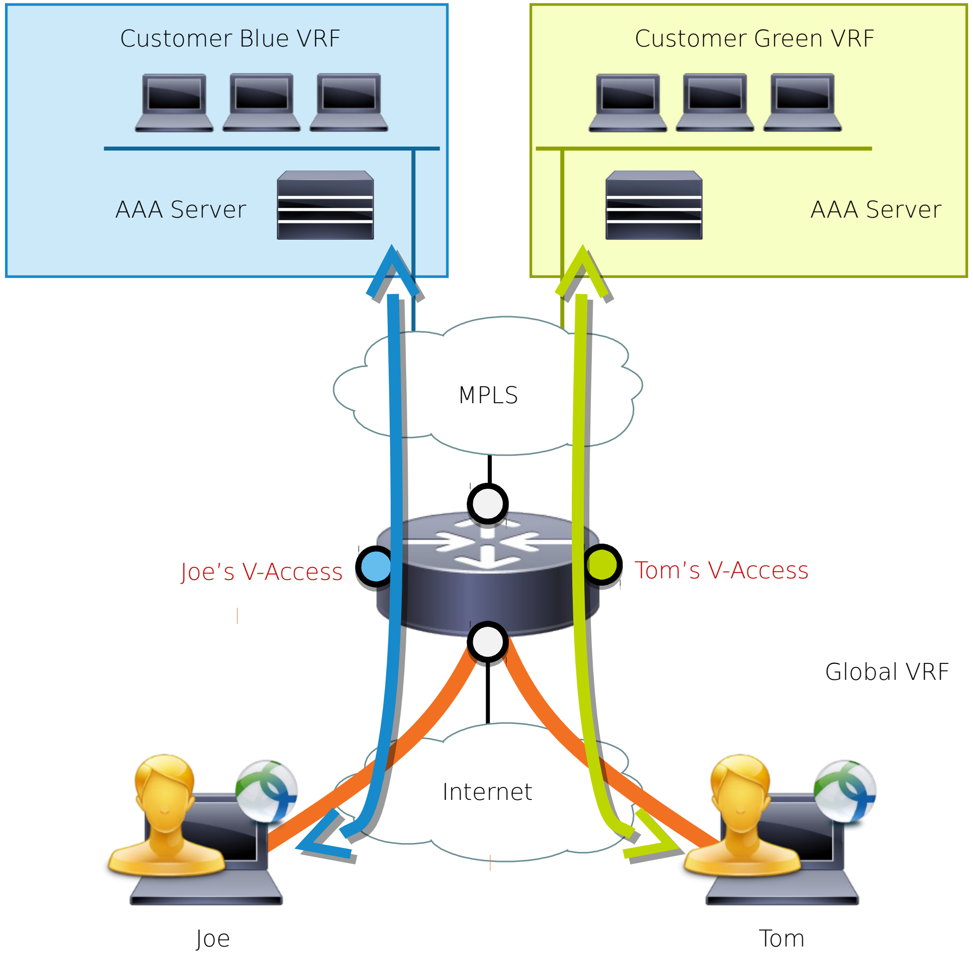
```
Joe
  ipsec:addr-pool=blue
  ip:interface-config=vrf forwarding blue
  ip:interface-config=ip unnumbered Loopback1
  ip:interface-config=service-policy output low-bw
  ip:interface-config=zone-member security restricted

Tom
  ipsec:addr-pool=green
  ip:interface-config=vrf forwarding green
  ip:interface-config=ip unnumbered Loopback2
  ip:interface-config=service-policy output high-bw
  ip:interface-config=zone-member security unrestricted
```

Interface config commands are dynamically applied at run-time upon V-Access instantiation

```
interface Virtual-Access1
 vrf forwarding blue
 ip unnumbered Loopback1
 tunnel source ...
 tunnel mode ipsec ipv4
 tunnel destination ...
 tunnel protection ipsec profile default
 service-policy output low-bw
 zone-member security restricted
```

Use Case #2: Multiple Customers, Shared Headend

- Requirements:
  - Username-password authentication on customer-managed AAA server
  - Cisco AnyConnect VPN client
  - VRF & QoS imposed by headend
- Proposed solution:
  - Multiple IKEv2 profiles & V-Templates
  - EAP authentication



FlexVPN Server Configuration

RADIUS-based EAP authentication with AAA server in the customer VRF

Local authorization attributes

Match on IKE ID configured in AnyConnect XML profile

Allow client to authenticate using EAP

Authenticate to client using RSA-Sig

Get address pool from local authorization policy

Specific tunnel protection profile using default IPsec transform set

Specific V-Template with correct VRF & QoS settings for this customer

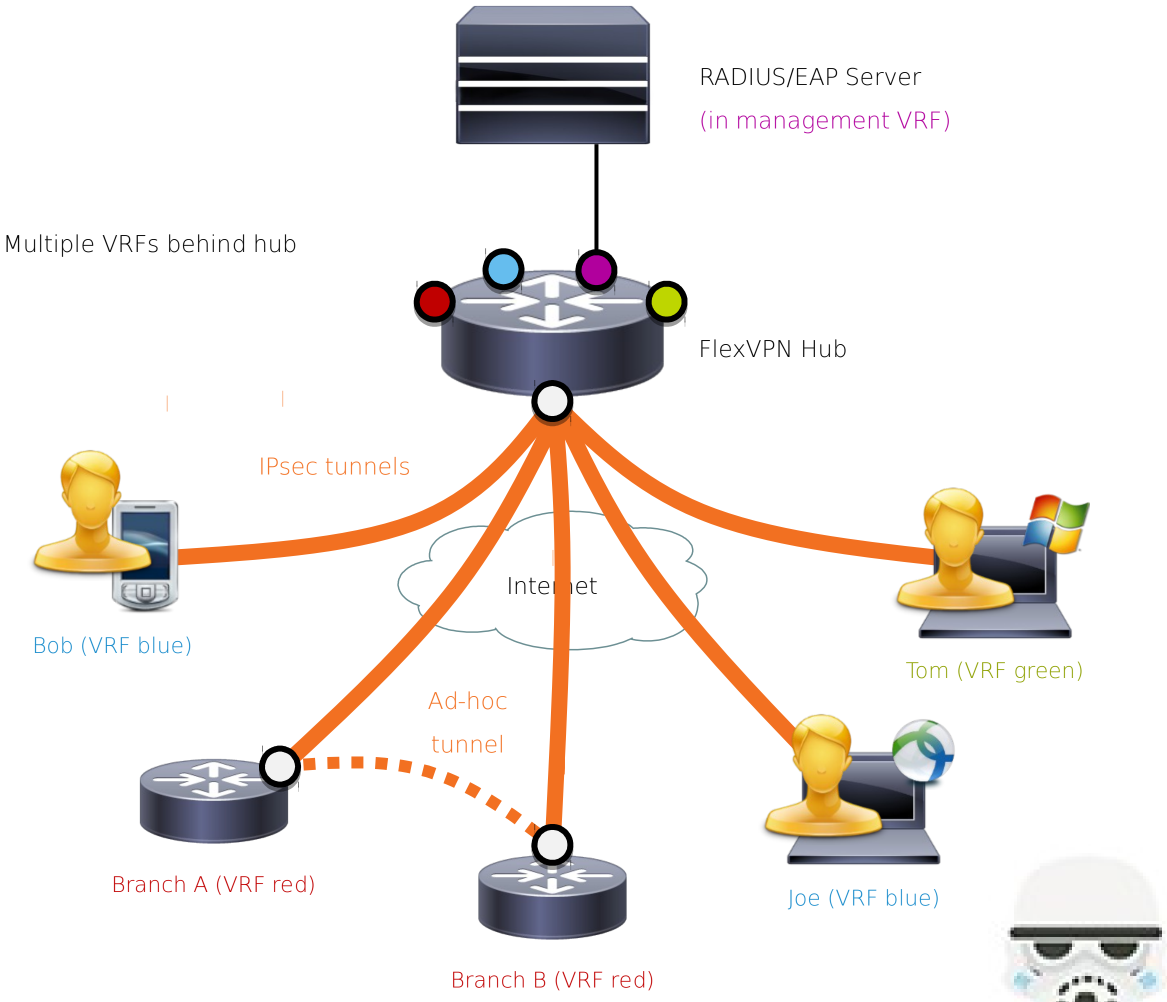
```
aaa new-model
aaa authentication login blue-rad group blue-rad
!
crypto ikev2 authorization policy blue-pol
 pool blue-pool
!
crypto ikev2 profile blue
 match identity remote key-id blue-id
 identity local dn
 authentication remote eap query-identity
 authentication local rsa-sig
 pki trustpoint blue-ca
 aaa authentication eap blue-rad
 aaa authorization group eap list default blue-pol
 virtual-template 1
!
crypto ipsec profile blue
 set ikev2-profile blue
!
interface Virtual-Template1 type tunnel
 vrf forwarding blue
 ip unnumbered Loopback1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile blue
 service-policy output blue-qos
```

Case Study:

Mixed Client & Branch Access

Use Case: Mixed Client & Branch Access

- Requirements:
  - Single responder for software clients & remote branches (spokes)
  - Spoke-to-spoke tunnels enabled on a per-branch basis
  - VRF enforced per user/branch
  - Branches use IKE certificates, clients use EAP (password or TLS certificates)
- Proposed solution:
  - Single IKEv2 profile & V-Template
  - Differentiated AAA authorization depending on authentication method



FlexVPN Server Configuration

RADIUS-based EAP authentication and AAA authorization

Match on FQDN domain for branches

Match statements for clients (depending on allowed client types)

Allow peers to authenticate using either EAP or certificates

User authorization using attributes returned during EAP authentication

Branch authorization using RADIUS

Automatic detection of tunnel mode[1] (pure IPsec tunnel mode for clients, GRE/IPsec for branches/spokes)

```
aaa new-model
aaa authentication login my-rad group my-rad
aaa authorization network my-rad group my-rad
!
crypto ikev2 profile default
 match identity remote fqdn domain example.com
 match identity remote {key-id | email | address} ...
 identity local dn
 authentication remote rsa-sig
 authentication remote eap query-identity
 authentication local rsa-sig
 pki trustpoint my-ca
 aaa authentication eap my-rad
 aaa authorization user eap cached
 aaa authorization user cert list my-rad
 virtual-template 1
!
interface Virtual-Template1 type tunnel
 no ip address
 tunnel mode auto
 tunnel protection ipsec profile default
```

[1] Starting with IOS-XE 3.12S

RADIUS Server Configuration

Clients can perform password-based or TLS-based EAP authentication
(TLS: RADIUS account = CN or UPN)

User attributes returned by RADIUS with successful EAP authentication

Branch attributes returned by RADIUS during AAA authorization step

Add/remove NHRP to enable/disable spoke-to-spoke tunnels per branch

Exchange prefixes via IKEv2 routing, branch prefix(es) controlled by branch

Branch prefix controlled by AAA server (installed as local static route)

```
joe
  cleartext-password=c1sc0!
  ipsec:addr-pool=blue
  ip:interface-config=vrf forwarding blue
  ip:interface-config=ip unnumbered Loopback1
  ip:interface-config=service-policy output blue-pol
  ip:interface-config=...

branch1.example.com
  ip:interface-config=vrf forwarding red
  ip:interface-config=ip unnumbered Loopback3
  ip:interface-config=ip nhrp network-id 3
  ip:interface-config=ip nhrp redirect
  ipsec:route-set=prefix 192.168.0.0 255.255.0.0
  ipsec:route-accept=any

branch2.example.com
  ip:interface-config=vrf forwarding green
  ip:interface-config=ip unnumbered Loopback2
  ipsec:route-set=prefix 192.168.0.0 255.255.0.0
  ipsec:route-set=local 192.168.1.0
```

FlexVPN Branch/Spoke Configuration

Apply default authorization policy:

- route set interface
- route accept any

(if needed, add extra "route set …")

Static tunnel interface (spoke-hub)

Enable spoke-spoke tunnel creation

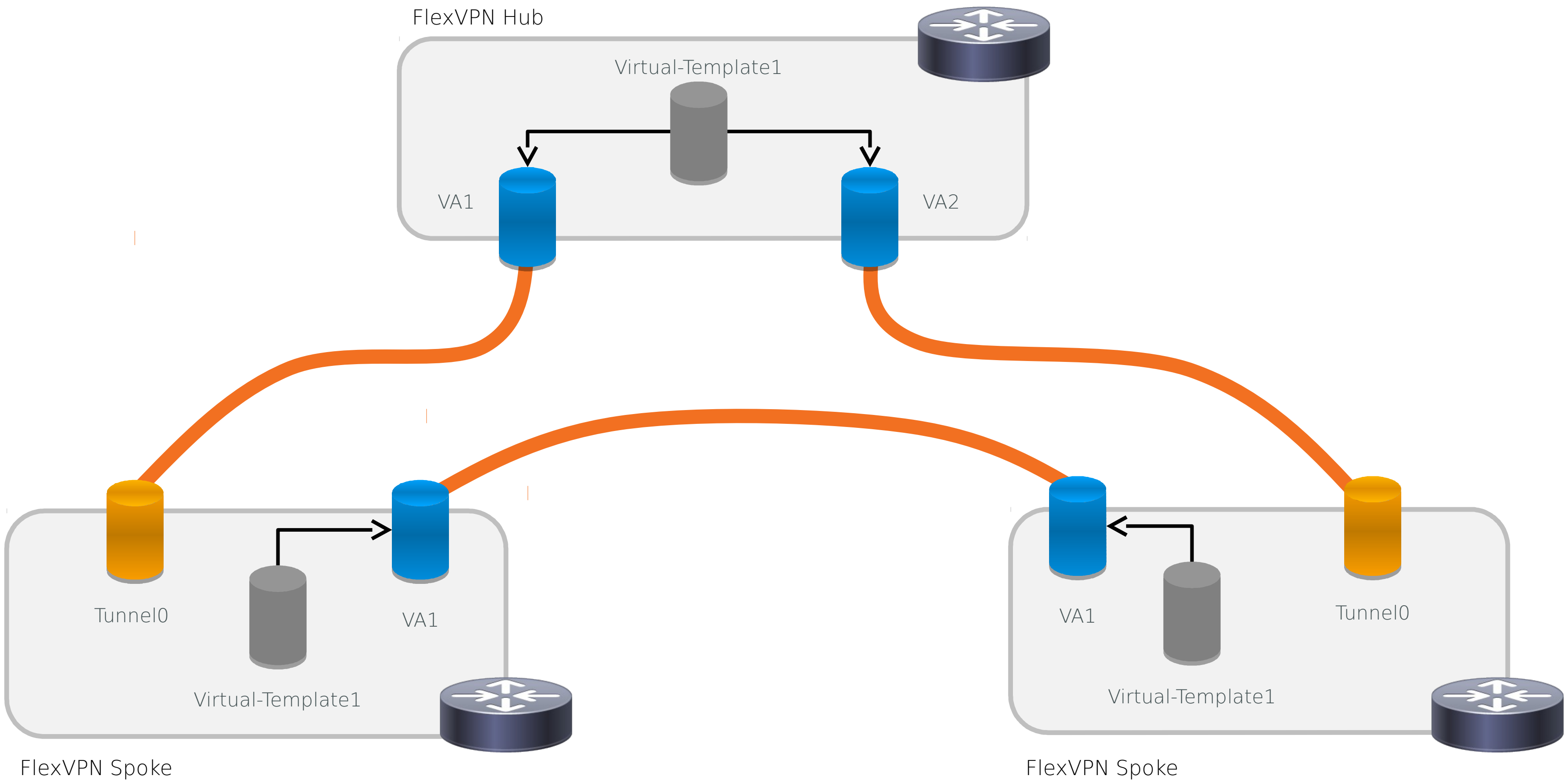
(also requires hub-side VA config)

V-Template (spoke-spoke)

with same NHRP config as Tunnel0

```
crypto ikev2 profile default
 match identity remote fqdn domain example.com
 identity local fqdn branch1.example.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint my-ca
 dpd 10 2 on-demand
 aaa authorization group cert list default default
 virtual-template 1
!
interface Tunnel0
 ip unnumbered Loopback1
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source Ethernet0/0
 tunnel destination 192.0.2.10
 tunnel protection ipsec profile default
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel protection ipsec profile default
```

FlexVPN Static & Dynamic Interfaces

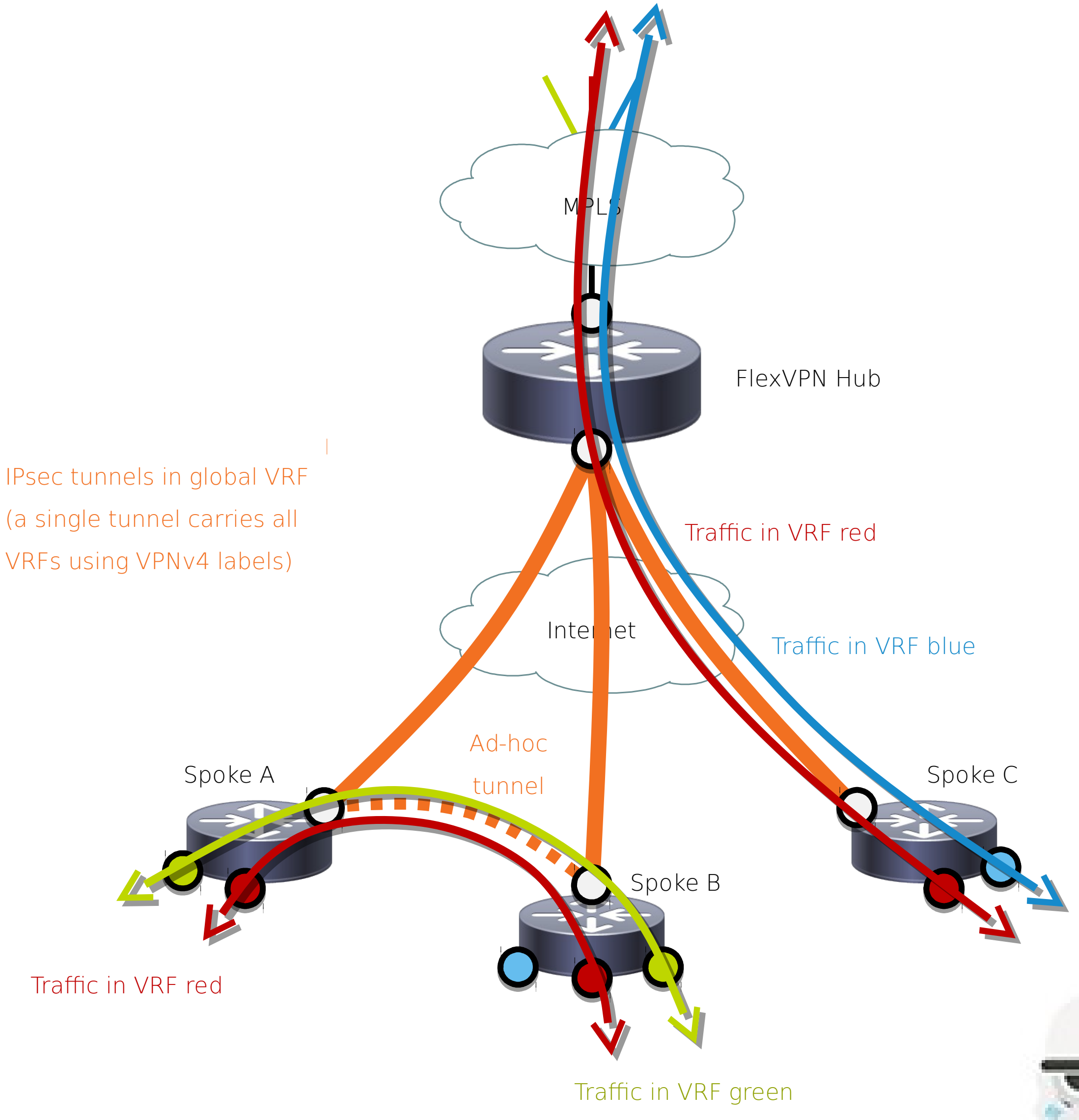


Case Study:

MPLS VPN Dynamic Mesh

Use Case: MPLS VPN over FlexVPN

- Requirements:
  - Traffic segregation using MPLS VPN
  - Dynamic spoke-to-spoke tunnels
  - Certificate-based authentication
- Proposed solution:
  - MPLS-enabled GRE/IPsec tunnels
  - Spokes peer with hub using MP-iBGP
  - NHRP carries label information for spoke-to-spoke direct forwarding



FlexVPN Hub Configuration (1)

```
crypto ikev2 profile default
 match identity remote fqdn domain example.com
 identity local fqdn hub.example.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint my-ca
 dpd 10 2 on-demand
 aaa authorization group cert list default default
 virtual-template 1
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
 ip nhrp network-id 1
 ip nhrp redirect
 mpls nhrp
 tunnel protection ipsec profile default
```

Apply default authorization policy

V-Template & V-Access in global VRF

Enable NHRP on V-Template

Enable spoke-spoke redirection
& give NHRP control over MPLS

FlexVPN Hub Configuration (2)

Use BGP Dynamic Neighbor feature to listen for incoming connections

Use V-Template unnumbered IP address as the update-source

Exchange VPNv4 prefixes with spokes

Send summary route to all spokes within each VRF

```
router bgp 65001
 bgp listen range 10.0.0.0/16 peer-group spokes
 neighbor spokes peer-group
 neighbor spokes remote-as 65001
 neighbor spokes update-source Loopback1
 !
 address-family vpnv4
  neighbor spokes activate
  neighbor spokes send-community extended
 !
 address-family ipv4 vrf blue
  network 192.168.0.0 mask 255.255.0.0
 exit-address-family
 !
 ...
!
ip route vrf blue 192.168.0.0 255.255.0.0 Null0
```

FlexVPN Spoke Configuration (1)

Apply default authorization policy

Static tunnel interface (spoke-hub) located in global VRF

Enable spoke-spoke tunnel creation & give NHRP control over MPLS

V-Template (spoke-spoke) with same NHRP config as Tunnel0

```
crypto ikev2 profile default
 match identity remote fqdn domain example.com
 identity local fqdn spoke1.example.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint my-ca
 dpd 10 2 on-demand
 aaa authorization group cert list default default
 virtual-template 1
!
interface Tunnel0
 ip unnumbered Loopback1
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 mpls nhrp
 tunnel source Ethernet0/0
 tunnel destination 192.0.2.10
 tunnel protection ipsec profile default
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 mpls nhrp
 tunnel protection ipsec profile default
```

FlexVPN Spoke Configuration (2)

Configure hub as static iBGP neighbor
(with Tunnel0 unnumbered IP address as the update-source)

Exchange VPNv4 prefixes with hub

Send local prefixes to hub for all VRFs

```
router bgp 65001
 neighbor 10.0.0.10 remote-as 65001
 neighbor 10.0.0.10 update-source Loopback1
 !
 address-family vpnv4
  neighbor 10.0.0.10 activate
  neighbor 10.0.0.10 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf blue
  network 192.168.1.0
 exit-address-family
 !
 ...
```

Further Information

Further Information

- Cisco Live recordings/slides (www.ciscolive365.com)
  - Milan 2014: BRKSEC-2881: FlexVPN Remote Access
  - Milan 2014: BRKSEC-3036: FlexVPN Advanced Site-to-Site
  - London 2013: BRKSEC-3013: Advanced IPsec with FlexVPN & IKEv2
- IOS & IOS-XE Configuration Guide (www.cisco.com)
- More literature is in the works… ☺

Thank you !