TOMORROW
starts here.

Deploying FlexVPN with IKEv2 and SSL

BRKSEC-3013

Tom Alexander – Technical Leader, Cisco Services

#clmel

Agenda

- FlexVPN Introduction
  - Why FlexVPN
  - FlexVPN Positioning
- FlexVPN Building Blocks
- Shortcut Switching (FlexMesh)
- FlexVPN & AAA Integration
- FlexVPN Redundancy
- Remote Access
- Wrap-up

Before We Begin...

For your reference

Additional Info

“For your Reference” slides:

- Just for your reference when back at work.
- Will not be covered in detail

“Additional info” slides:

- Rendered in the presentation PDF (download it through the Cisco Live portal)
- Not shown during the live presentation
- Cover extra details or small additional topics

An Introduction to FlexVPN and IKEv2

EasyVPN, DMVPN and Crypto Maps

```
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp client configura
 key cisco123
 pool dvti
 acl 100
crypto isakmp profile dvti
   match identity group cisco
   client authentication list
   isakmp authorization list l
   client configuration addres
   virtual-template 1
crypto ipsec transform-set dvt
crypto ipsec profile dvti
 set transform-set dvti
 set isakmp-profile dvti
interface Virtual-Template1 ty
 ip unnumbered Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profi
ip local pool dvti 192.168.2.1
ip route 0.0.0.0 0.0.0.0 10.0.
access-list 100 permit ip 192.
```

```
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto ipsec transform-set vpn-ts-set esp-3des esp-s
 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 vpnprof

ip route 192.168.0.0 255.255.0.0 Null0router bgp 1
bgp log-neighbor-changes
redistribute static
 neighbor DMVPN peer-group
 bgp listen range 10.0.0.0/24 peer-group DMVPN
 neighbor DMVPN remote-as 1
 no auto-summary
```

```
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp client configuration group cisco
 key pr3sh@r3dk3y
 pool vpnpool
 acl 110
crypto ipsec transform-set vpn-ts-set esp-3des esp-sha-hmac
crypto dynamic-map dynamicmap 10
 set transform-set vpn-ts-set
 reverse-route
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
```

VPN Technology Selection

Death by a thousand questions…

3rd party and legacy support

Hub & Spoke

AAA Manageability

Failover time

Spoke – Spoke Direct

Solution vs Components

IPv4/IPv6 dual stack

Failure detection method

Design complexity

Route Injection

Dual DMVPN

Dynamic Routing

Crypto Map or Tunnels

Feature order

Multi-Hub Homing

Per peer ACL's

Multicast

Scalability

Multi-ISP Homing

QoS support

High Availability

FlexVPN Unifies

Unified Overlay VPN's

VPN	Interop	Dynamic Routing	IPsec Routing	Spoke-spoke direct (shortcut)	Remote Access	Simple Failover	Source Failover	Config push	Per-peer config	Per-Peer QoS	Full AAA Management
Easy VPN	No	No	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes
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
Flex VPN	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

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

FlexVPN Overview

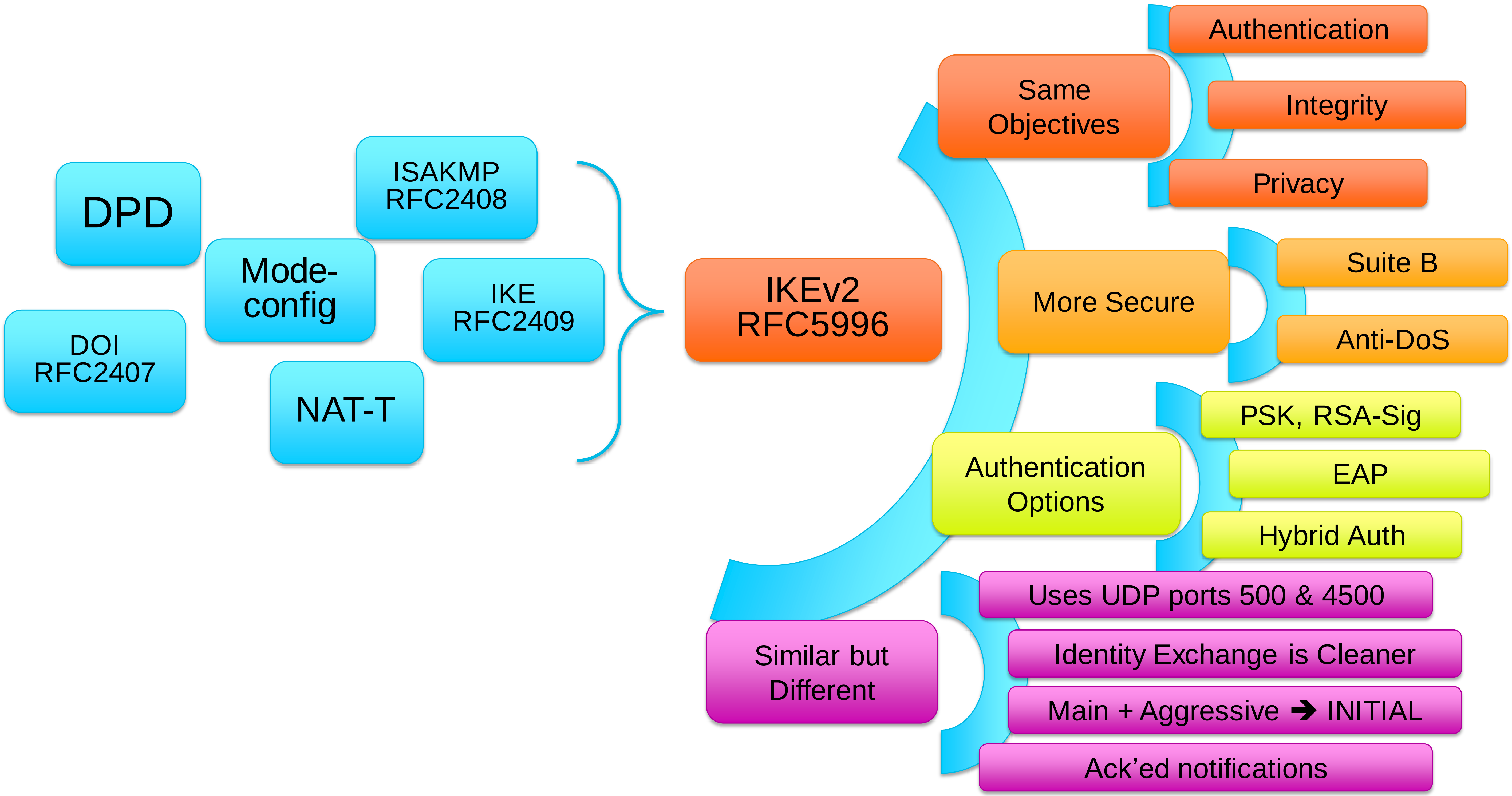
- What is FlexVPN?
  - IKEv2-based unified VPN technology that combines site-to-site, remote-access, hub-spoke and spoke-to-spoke topologies
- FlexVPN highlights
  - Unified CLI
  - Based on and compliant to IKEv2 standard
  - Unified infrastructure: leverages IOS Point-to-Point tunnel interface
  - Unified features: most features available across topologies
  - Key features: AAA, Config-mode, dynamic routing, IPv6
  - Per Spoke level features for QOS, VRF, ZBFW, ACL, etc
  - Simplified configuration using smart-defaults
  - Interoperable with non-Cisco implementations
  - Easier to learn, market and manage

IKEv2 in a Few Words

- Defined in RFC 4306 - updated by RFC 5996
  - No interoperability with IKEv1
  - Usage ramping up rapidly!
- Both are using the same basic structure aiming at:
  - Privacy
  - Integrity
  - Authentication
- Both run over UDP 500/4500

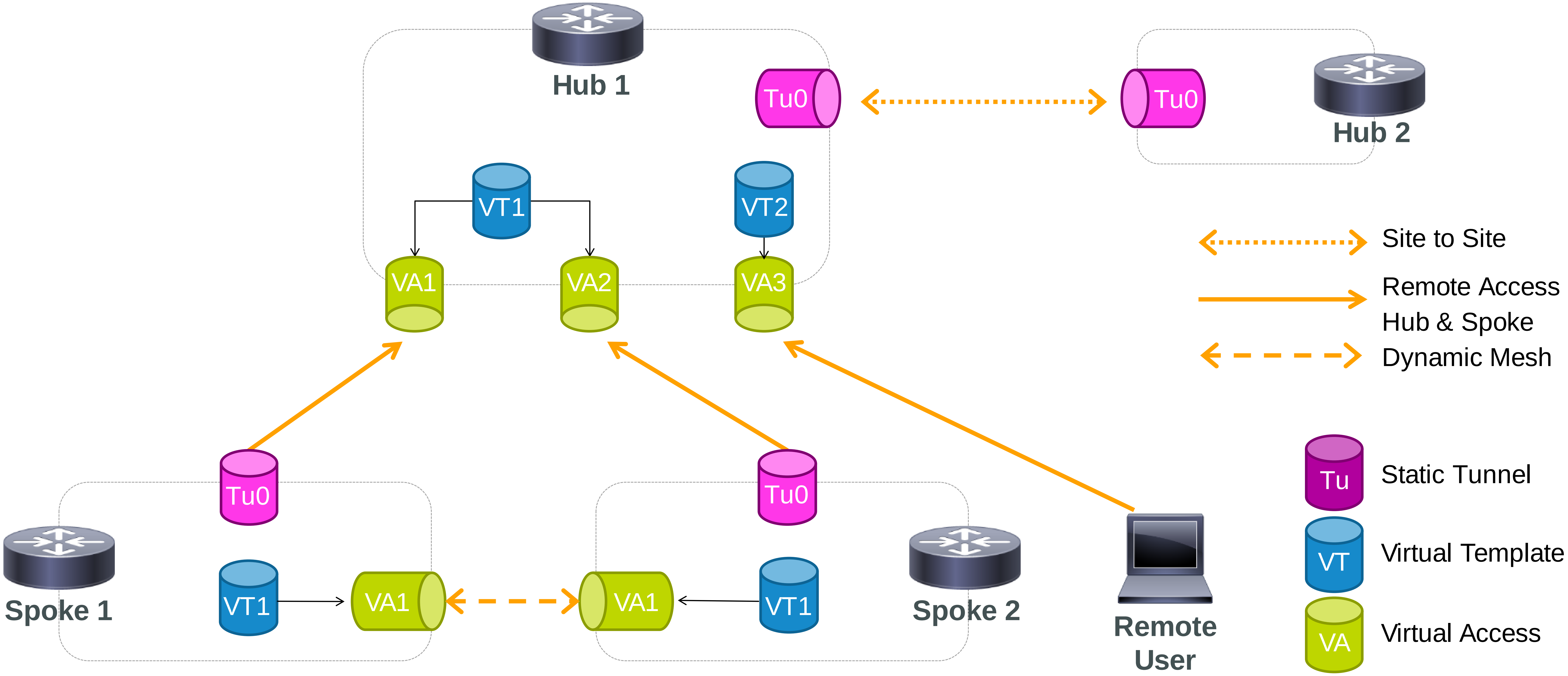
Flex is IKEv2 Only

- Why Flex now?

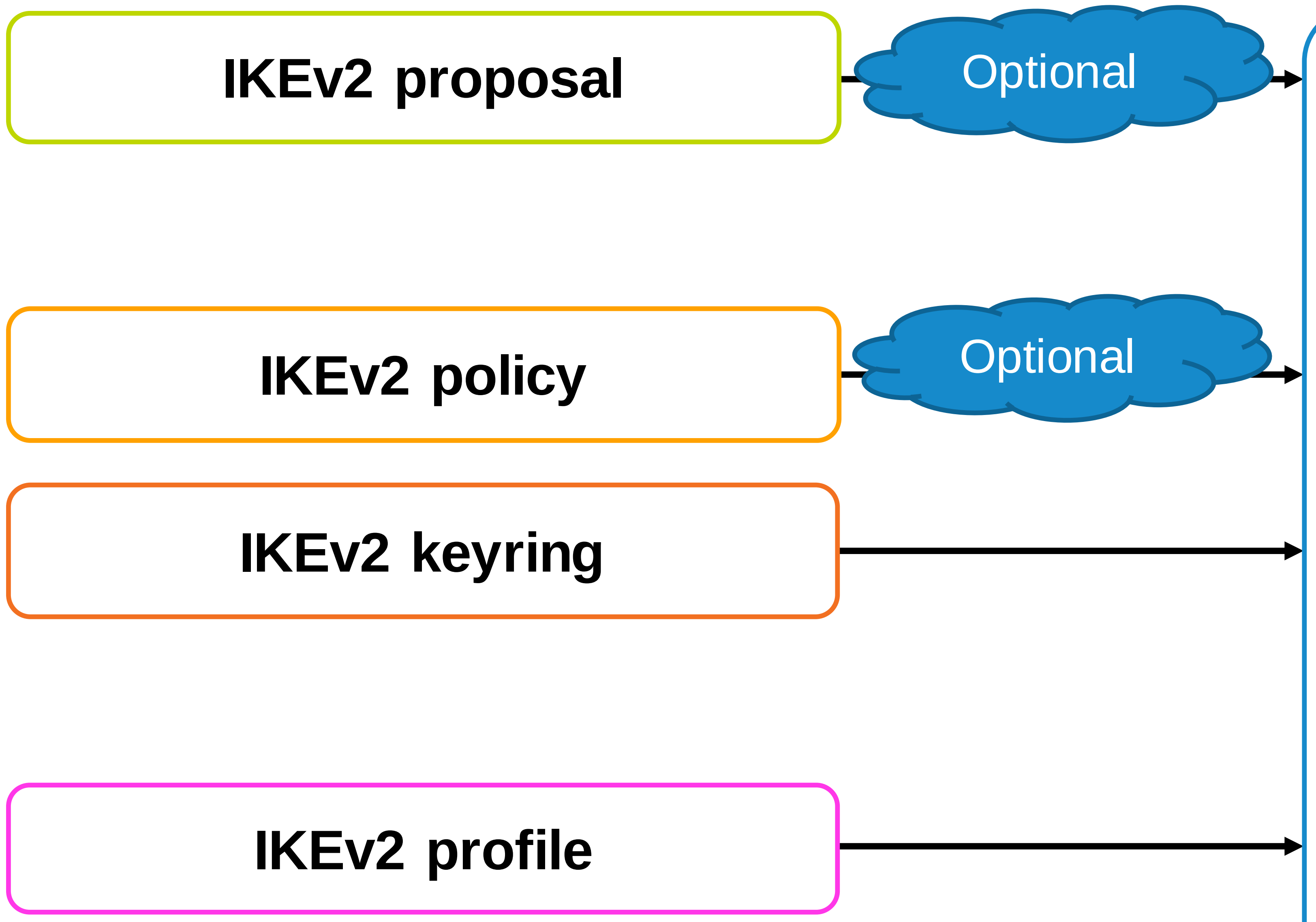


FlexVPN Building Blocks

FlexVPN and Interfaces



IKEv2 Configuration



```
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 cisco123
!
crypto ikev2 profile prof
 match identity remote address 10.0.1.1
 authentication local pre-share
 authentication remote pre-share
 keyring V2-keyring
```

Introduced in15.1(1)T

IKEv2 CLI Overview

IKEv2 Profile – extensive CLI

```
crypto ikev2 profile default
```

Self Identity Control

```
identity local address 10.0.0.1
identity local fqdn local.cisco.com
identity local email local@cisco.com
identity local dn
```

Matching on peer identity or certificate

```
match identity remote address 10.0.1.1
match identity remote fqdn remote.cisco.com
match identity remote fqdn domain cisco.com
match identity remote email remote@cisco.com
match identity remote email domain cisco.com
match certificate certificate_map
```

Matching on local address and front VRF

```
match fvrf red
match address local 172.168.1.1
```

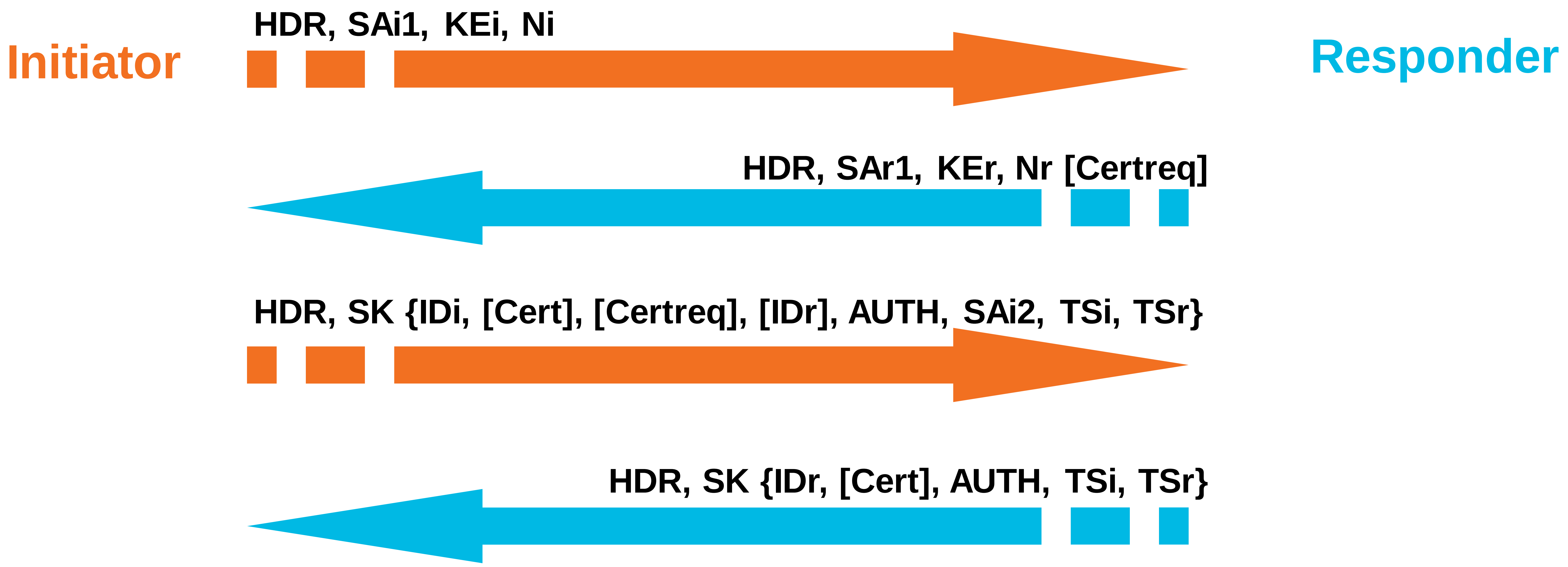
Asymmetric local and remote authentication methods

```
authentication local pre-share [key <KEY>]
authentication local rsa-sig
authentication local eap

authentication remote pre-share [key <KEY>]
authentication remote rsa-sig
authentication remote eap
```

IOS based and AAA based Pre-Shared Keyring

```
keyring local <IOSkeyring>
keyring aaa <AAAlist>

pki trustpoint <trustpoint_name>
```

IKEv2 Basic Negotiation



Initiator

Responder

HDR, SAi1, KEi, Ni

HDR, SAr1, KEr, Nr [Certreq]

HDR, SK {IDi, [Cert], [Certreq], [IDr], AUTH, SAi2, TSi, TSr}

HDR, SK {IDr, [Cert], AUTH, TSi, TSr}

HDR – IKE Header

SA[i/r] – cryptographic algorithms the peer proposes/accepts

KE[i/r] – Initator Key Exchange material

N[i/r] – Initiator/Responder Nonce

SK– payload encrypted and integrity protected

ID[i/r] – Initiator/Responder Identity

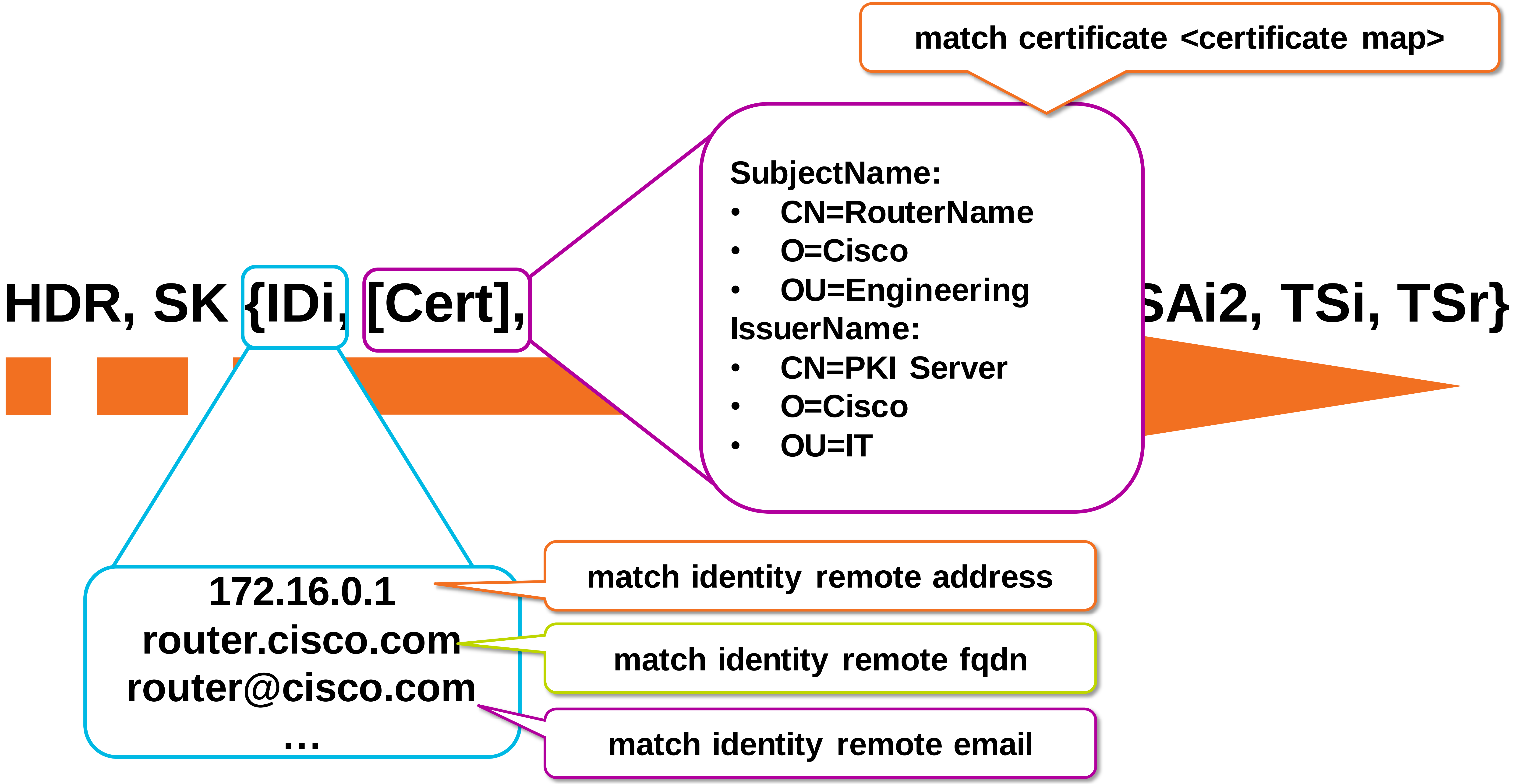
Cert(req) – Certificate (request)

AUTH – Authentication data

SA - Includes SA, Proposal and Transform Info to Create the 1st CHILD_SA

Ts[i/r] – Traffic Selector as src/dst proxies

IKEv2 Profile Match Statements



match certificate <certificate map>

HDR, SK {IDi, [Cert], SAi2, TSi, TSr}

SubjectName:
- CN=RouterName
- O=Cisco
- OU=Engineering

IssuerName:
- CN=PKI Server
- O=Cisco
- OU=IT

172.16.0.1
router.cisco.com
router@cisco.com
…

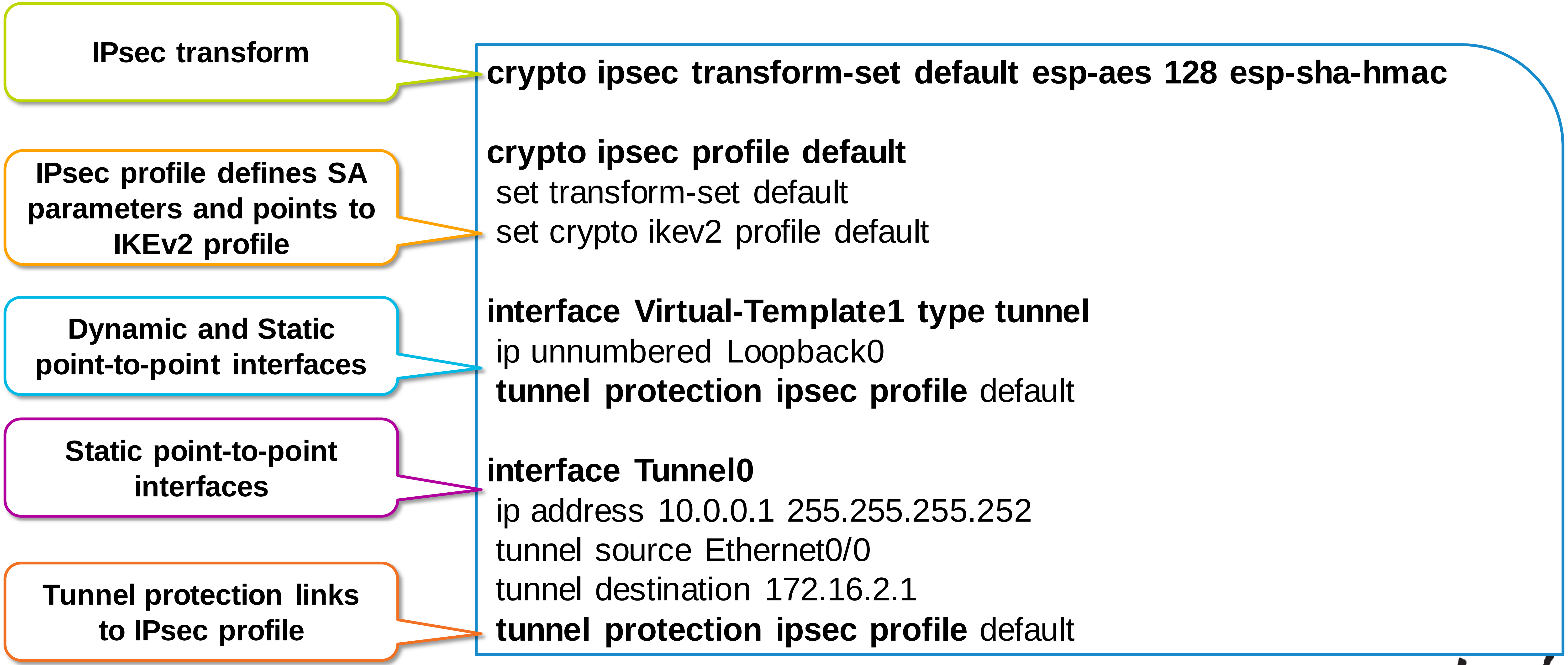
match identity remote address

match identity remote fqdn

match identity remote email

IPsec CLI Overview

Tunnel Protection



IPsec transform

IPsec profile defines SA parameters and points to IKEv2 profile

Dynamic and Static point-to-point interfaces

Static point-to-point interfaces

Tunnel protection links to IPsec profile

```
crypto ipsec transform-set default esp-aes 128 esp-sha-hmac

crypto ipsec profile default
 set transform-set default
 set crypto ikev2 profile default

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

interface Tunnel0
 ip address 10.0.0.1 255.255.255.252
 tunnel source Ethernet0/0
 tunnel destination 172.16.2.1
 tunnel protection ipsec profile default
```

Introducing Smart Defaults

Intelligent, reconfigurable defaults

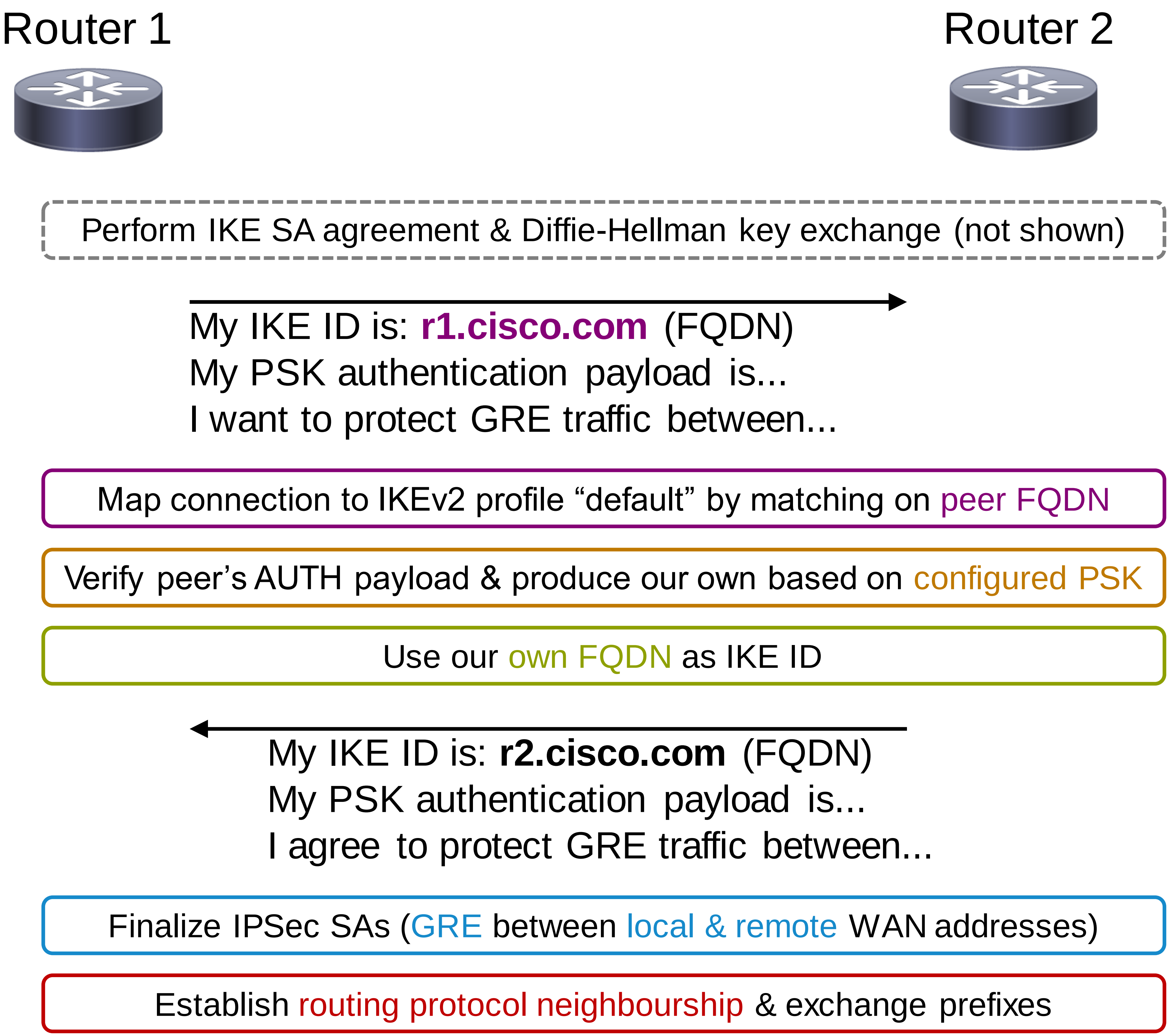
```
crypto ipsec transform-set default
                    esp-aes 128 esp-sha-hmac

crypto ipsec profile default
 set transform-set default
 set crypto ikev2 profile default

crypto ikev2 proposal default
  encryption aes-cbc-256 aes-cbc-128 3des
  integrity sha512 sha 256 sha1 md5
  group 5 2

crypto ikev2 policy default
  match fvrf any
  proposal default

crypto ikev2 authorisation policy default
 route set interface
 route accept any
```

These constructs are the Smart Defaults

```
crypto ikev2 profile default
 match identity remote address 10.0.1.1
 authentication local rsa-sig
 authentication remote rsa-sig
 aaa authorization user cert list default default
 pki trustpoint TP
!
interface Tunnel0
 ip address 192.168.0.1 255.255.255.252
 tunnel protection ipsec profile default
```

What you need to specify

Static Site-to-Site Example



Perform IKE SA agreement & Diffie-Hellman key exchange (not shown)

My IKE ID is: **r1.cisco.com** (FQDN)
My PSK authentication payload is...
I want to protect GRE traffic between...

Map connection to IKEv2 profile “default” by matching on peer FQDN

Verify peer’s AUTH payload & produce our own based on configured PSK

Use our own FQDN as IKE ID

My IKE ID is: **r2.cisco.com** (FQDN)
My PSK authentication payload is...
I agree to protect GRE traffic between...

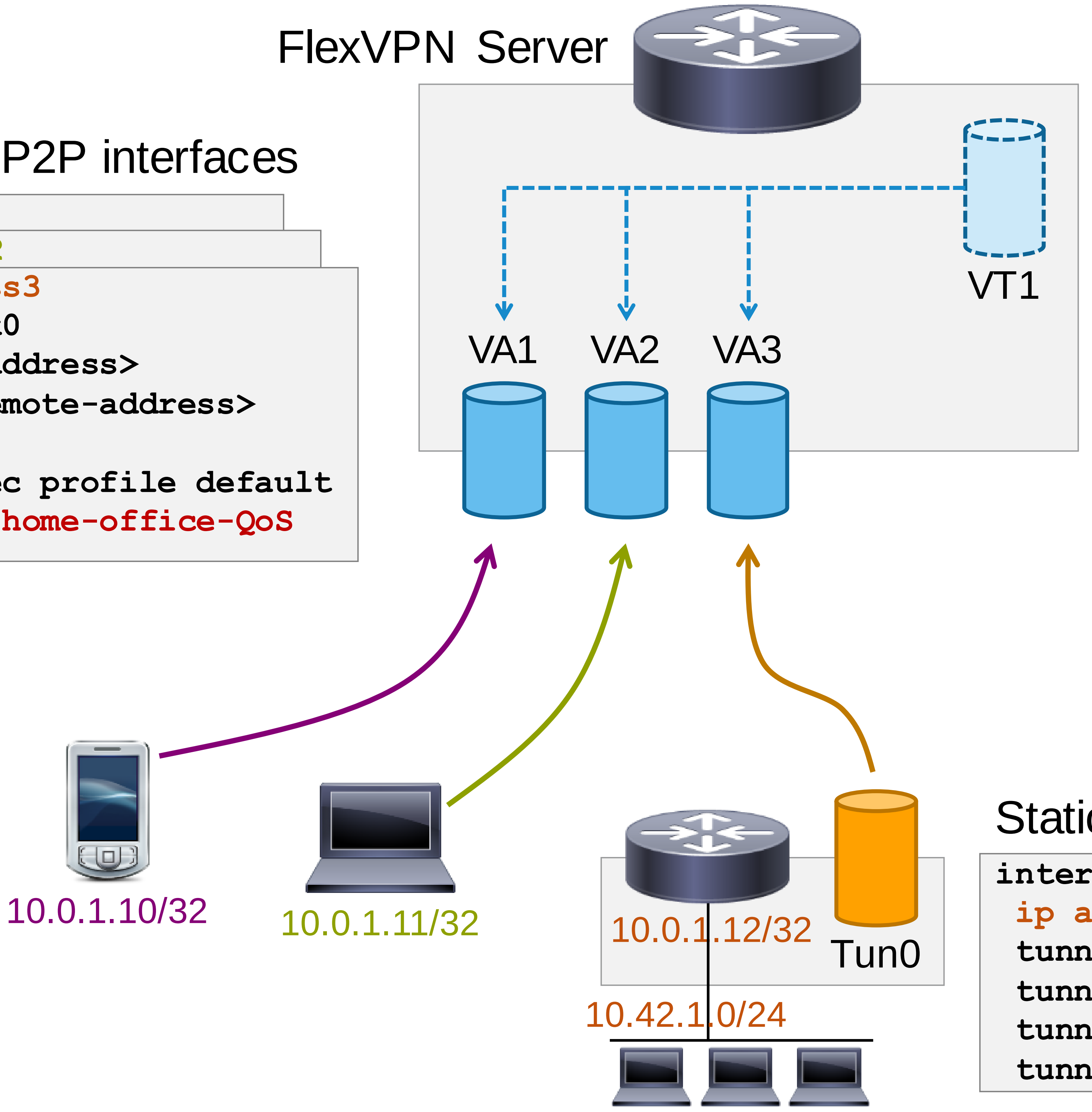
Finalize IPSec SAs (GRE between local & remote WAN addresses)

Establish routing protocol neighbourship & exchange prefixes

```
crypto ikev2 keyring my_keyring
 peer R1
  hostname r1.cisco.com
  pre-shared-key cisco123

crypto ikev2 profile default
 match identity remote fqdn r1.cisco.com
 identity local fqdn r2.cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local my_keyring
!
interface Tunnel0
 ip address 10.0.0.2 255.255.255.252
 tunnel source Ethernet0/0
 tunnel destination 192.0.2.1
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 ip address 192.0.2.2 255.255.255.0
!
router rip
 version 2
 network 10.0.0.0
 ...
```

FlexVPN AAA Integration

Dynamic Point-to-Point Interfaces



Dynamically instantiated P2P interfaces

```
interface Virtual-Access1
 interface Virtual-Access2
  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 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
```

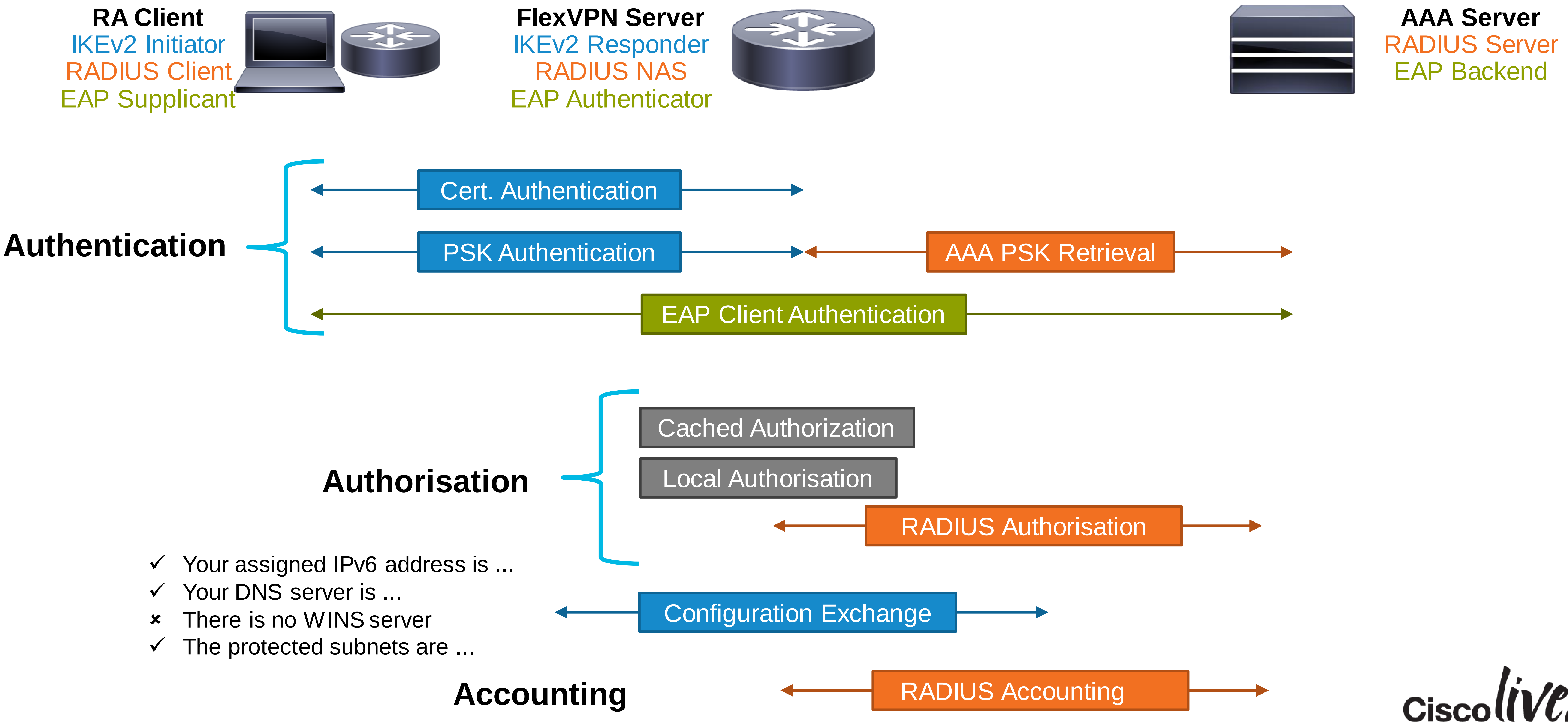
Routing table (RIB/FIB)

```
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 interface

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

High-Level AAA Operations



RA Client
IKEv2 Initiator
RADIUS Client
EAP Supplicant

FlexVPN Server
IKEv2 Responder
RADIUS NAS
EAP Authenticator

AAA Server
RADIUS Server
EAP Backend

Authentication

- Cert. Authentication
- PSK Authentication
- AAA PSK Retrieval
- EAP Client Authentication

Authorisation

- Cached Authorization
- Local Authorisation
- RADIUS Authorisation

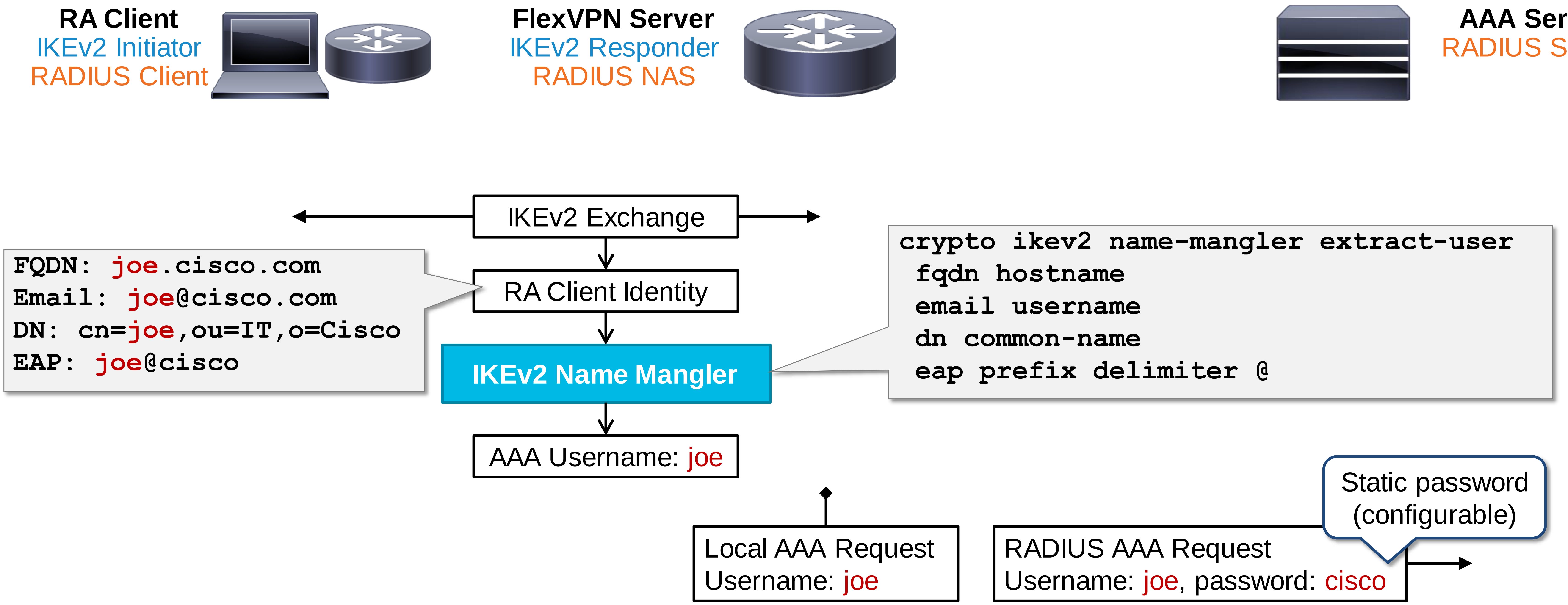
Configuration Exchange

✓ Your assigned IPv6 address is ...
✓ Your DNS server is ...
✗ There is no WINS server
✓ The protected subnets are ...

Accounting

RADIUS Accounting

Building Block – IKEv2 Name Mangler



```
FQDN: joe.cisco.com
Email: joe@cisco.com
DN: cn=joe,ou=IT,o=Cisco
EAP: joe@cisco
```

```
crypto ikev2 name-mangler extract-user
 fqdn hostname
 email username
 dn common-name
 eap prefix delimiter @
```

- Start with the peer’s IKE or EAP identity
- Derive a username that is meaningful to AAA (local or RADIUS)

Authorisation Types

- Not mutually exclusive – May be combined

Implicit User Authorisation

```
crypto ikev2 profile default
 aaa authorization user {psk|eap} cached
```

Uses cached attributes received from RADIUS during AAA PSK retrieval or EAP authentication

Explicit User Authorisation

```
crypto ikev2 profile default
 aaa authorization user {psk|eap|cert} list list [name | name-mangler mangler]
```

Retrieves user attributes from RADIUS (local database not supported)

Explicit Group Authorisation

Reverse order of precedence (group > user)

```
crypto ikev2 profile default
 aaa authorization group {psk|eap|cert} [override] list list [name | name-mangler mangler]
```

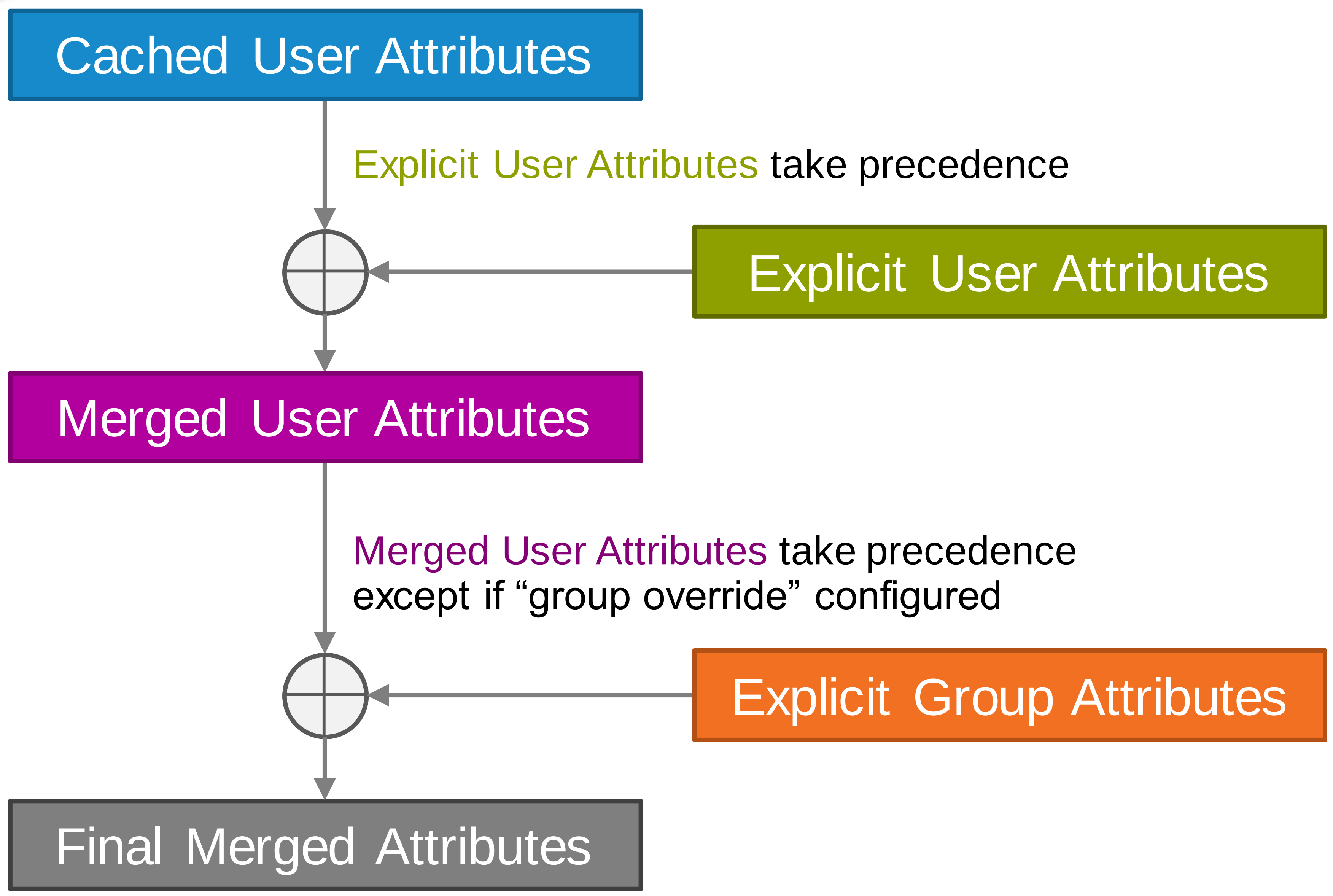
Retrieves group attributes from RADIUS or local database

Attributes – Merging

FlexVPN Server

Received during AAA-based authentication

Attribute	Value
Framed-IP-Address	10.0.0.101
ipsec:dns-servers	10.2.2.2



Cached User Attributes

Explicit User Attributes take precedence

Explicit User Attributes

Merged User Attributes

Merged User Attributes take precedence except if “group override” configured

Explicit Group Attributes

Final Merged Attributes

Attribute	Value
Framed-IP-Address	10.0.0.102
ipsec:dns-servers	10.2.2.2

Attribute	Value
Framed-IP-Address	10.0.0.102
ipsec:dns-servers	10.2.2.2
ipsec:banner	Welcome !

AAA Server

Received during explicit user authorisation

Attribute	Value
Framed-IP-Address	10.0.0.102

Received during explicit group authorisation

Attribute	Value
ipsec:dns-servers	10.2.2.3
ipsec:banner	Welcome !

Authorisation Example

RA Client

FlexVPN Server

My IKE ID is **cn=joe-pc, ou=Eng, o=Cisco**
Here is my **identity certificate**
I need an **IPv4 address**

Map connection to IKEv2 profile “default” by matching on cert-map “cisco”

Perform certificate-based authentication (not shown)

Run client IKE ID through name-mangler “ou” & username output is “Eng”

Invoke AAA with list “here” (local) & username “Eng” & auth policy “Eng”

Allocate IPv4 address from pool “pool-Eng”

Clone V-Template1 into V-Access1, apply VRF & IP unnumbered

Your IPv4 address is: **10.0.1.10/32**

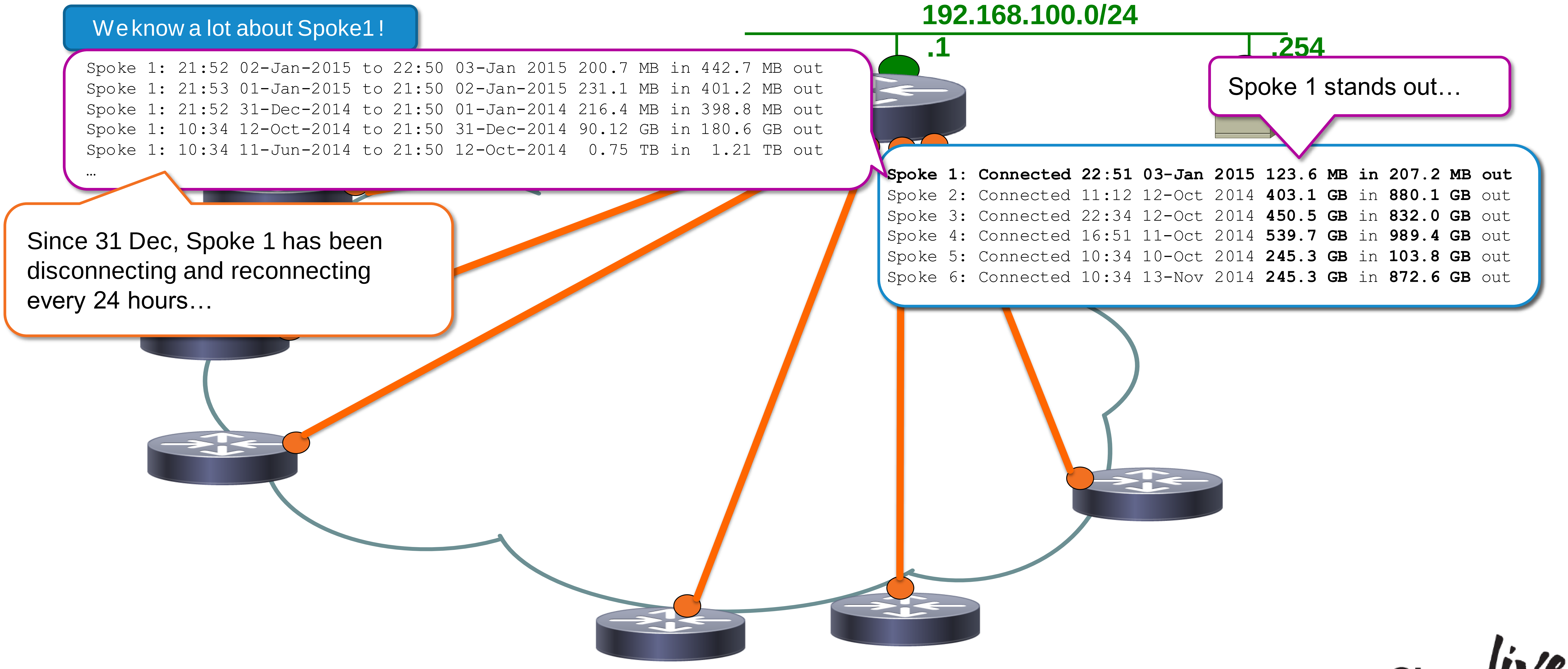
“show derived-config ...”

```
interface Virtual-Access1
 vrf forwarding Eng
 ip unnumbered Loopback1
 tunnel source 192.0.2.2
 tunnel mode ipsec ipv4
 tunnel destination 192.168.221.129
 tunnel protection ipsec profile default
```

```
aaa authorization network AUTHOR local
aaa attribute list attr-Eng
 attribute type interface-config "vrf forwarding Eng"
 attribute type interface-config "ip unnumbered Loopback1"
!
crypto ikev2 authorization policy Eng
 pool pool-Eng
 netmask 255.255.255.255
 aaa attribute list attr-Eng
!
crypto pki certificate map cisco 1
 subject-name co o = cisco
!
crypto ikev2 name-mangler ou
 dn organization-unit
!
crypto ikev2 profile default
 match certificate cisco
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint root
 aaa authorization group cert list AUTHOR name-mangler ou
 virtual-template 1
!
ip local pool pool-Eng 10.0.1.10 10.0.1.99
!
interface Loopback1
 vrf forwarding Eng
 ip address 10.0.1.1 255.255.255.255
!
interface Virtual-Template1 type tunnel
 no ip address
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
```

Accounting and Change of Authorisation

AAA Accounting



We know a lot about Spoke1 !

```
Spoke 1: 21:52 02-Jan-2015 to 22:50 03-Jan 2015 200.7 MB in 442.7 MB out
Spoke 1: 21:53 01-Jan-2015 to 21:50 02-Jan-2015 231.1 MB in 401.2 MB out
Spoke 1: 21:52 31-Dec-2014 to 21:50 01-Jan-2014 216.4 MB in 398.8 MB out
Spoke 1: 10:34 12-Oct-2014 to 21:50 31-Dec-2014 90.12 GB in 180.6 GB out
Spoke 1: 10:34 11-Jun-2014 to 21:50 12-Oct-2014  0.75 TB in  1.21 TB out
…
```

Since 31 Dec, Spoke 1 has been disconnecting and reconnecting every 24 hours…

Spoke 1 stands out…

```
Spoke 1: Connected 22:51 03-Jan 2015 123.6 MB in 207.2 MB out
Spoke 2: Connected 11:12 12-Oct 2014 403.1 GB in 880.1 GB out
Spoke 3: Connected 22:34 12-Oct 2014 450.5 GB in 832.0 GB out
Spoke 4: Connected 16:51 11-Oct 2014 539.7 GB in 989.4 GB out
Spoke 5: Connected 10:34 10-Oct 2014 245.3 GB in 103.8 GB out
Spoke 6: Connected 10:34 13-Nov 2014 245.3 GB in 872.6 GB out
```

Activating AAA Accounting

And why it is a good idea too…

```
aaa group server radius MyRADIUS
  server-private 192.168.104.101 key cisco

aaa accounting network ACCT start-stop group MyRADIUS

crypto ikev2 profile default
 match identity fqdn domain mycompany.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint TP
 aaa authorization group cert list default default
 aaa accounting cert ACCT
 virtual-template 1
```

Tell IKEv2 to report session status

A Good Idea ?

- Because it is simple!
- Captures even short lived sessions
  ➔ event driven vs. polling (e.g. SNMP)
- Reliable protocol (acknowledged)
  ➔ more reliable than SNMP traps
- Maps the identity to the statistics
  ➔ no more crossing tables (IP→ID)
- You may need it anyway
  - Authorisation, IP pool…

A Simplistic Configuration

RADIUS based Authentication, Authorisation and Accounting

```
aaa group server radius ISE
 server-private 192.168.104.101 key CISCO
!
aaa authentication login ISE group ISE
aaa authorization network ISE group ISE
aaa accounting network ISE start-stop group ISE
!
aaa server radius dynamic-author
 client 192.168.104.101 server-key CISCO
 auth-type all
!

crypto ikev2 profile default
 match identity remote any
 identity local dn
 authentication remote eap query-identity
 authentication local rsa-sig
 pki trustpoint TRUSTPOINT
 aaa authentication eap ISE
 aaa authorization user eap cached
 aaa accounting eap ISE
 virtual-template 1
```

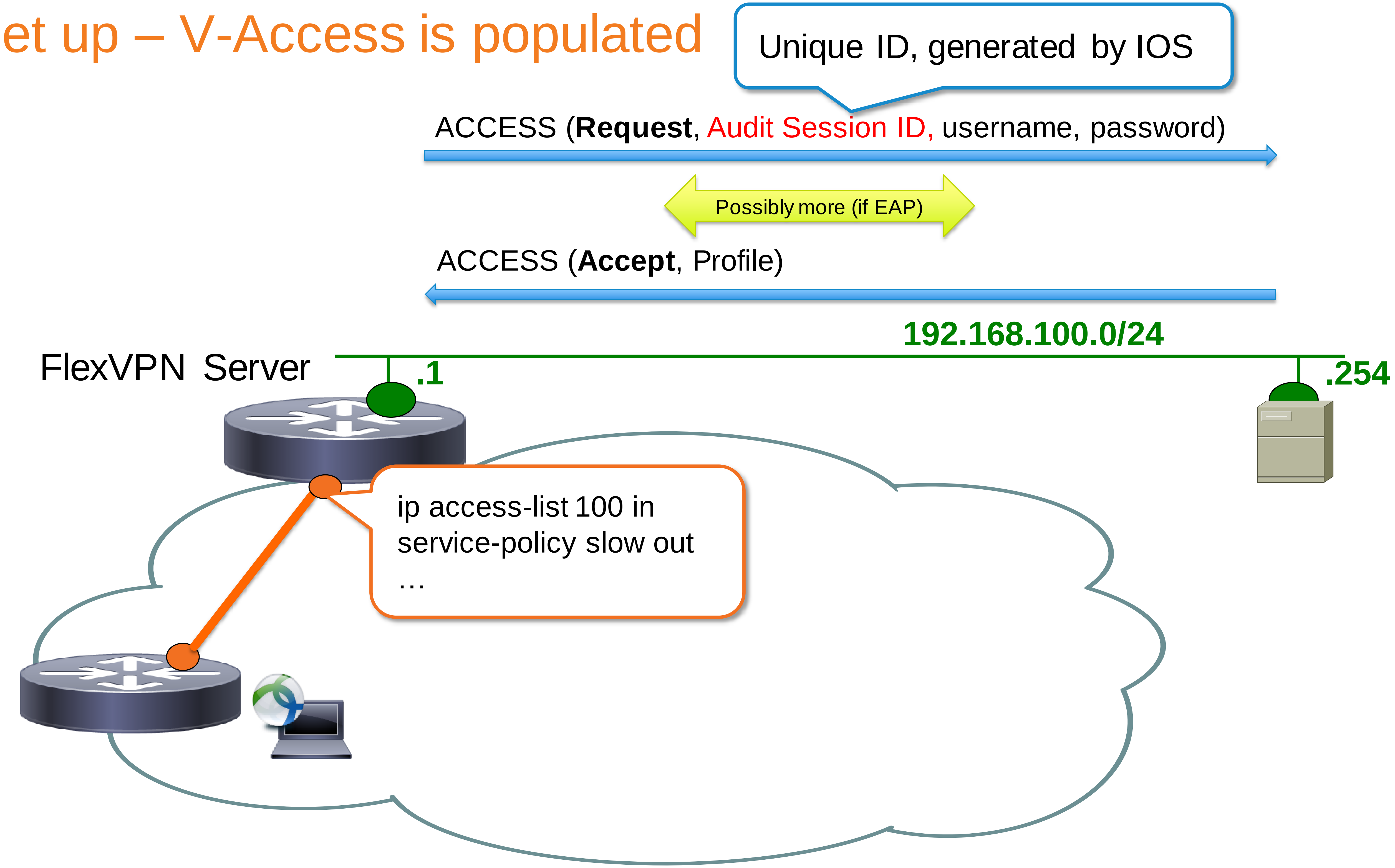
EAP Authentication

Authorization

Accounting (optional but recommended)

How CoA Works

Session is set up – V-Access is populated



Unique ID, generated by IOS

ACCESS (**Request**, Audit Session ID, username, password)

Possibly more (if EAP)

ACCESS (**Accept**, Profile)

192.168.100.0/24

FlexVPN Server

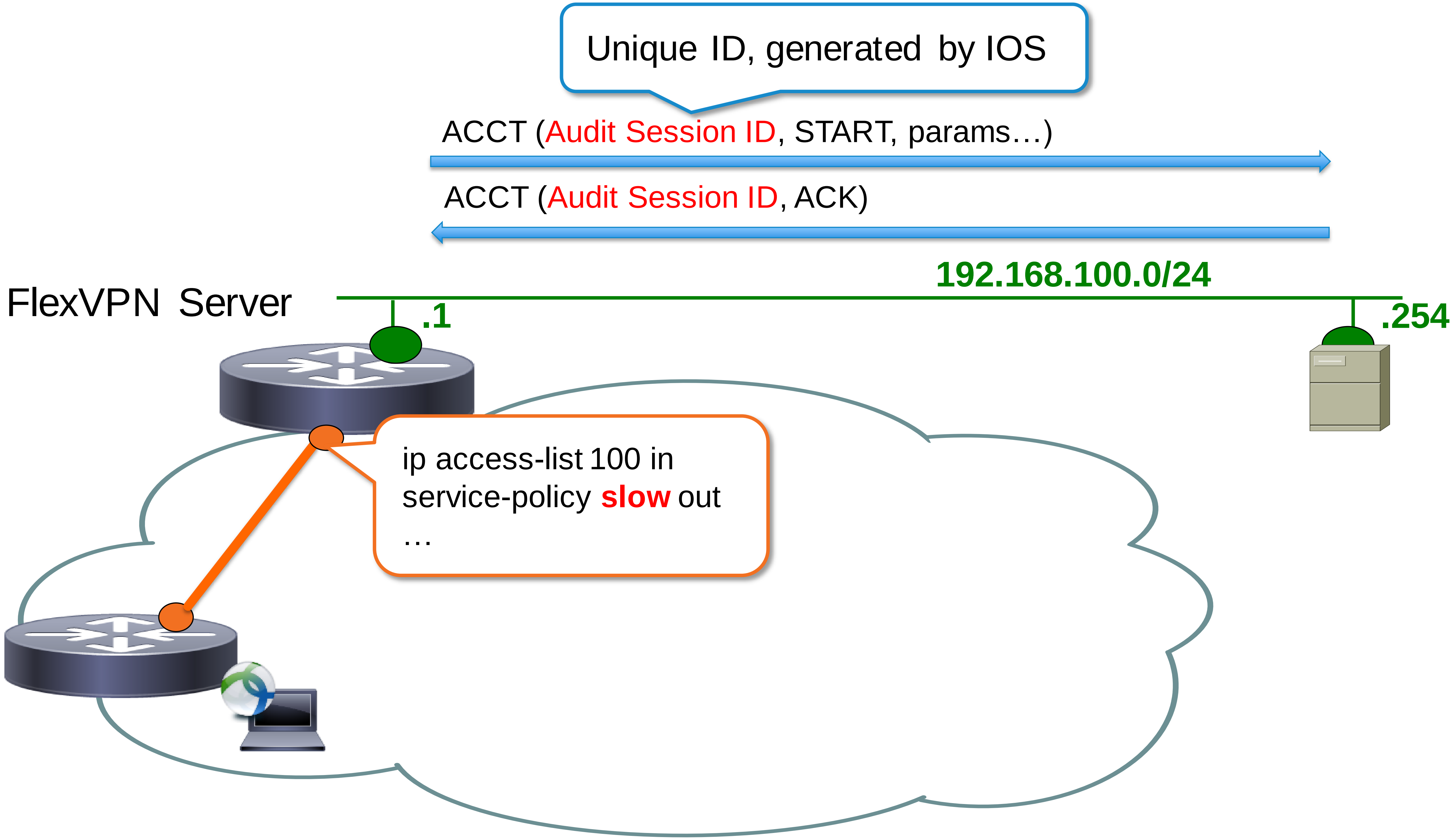
.1

.254

ip access-list 100 in
service-policy slow out
…

Accounting

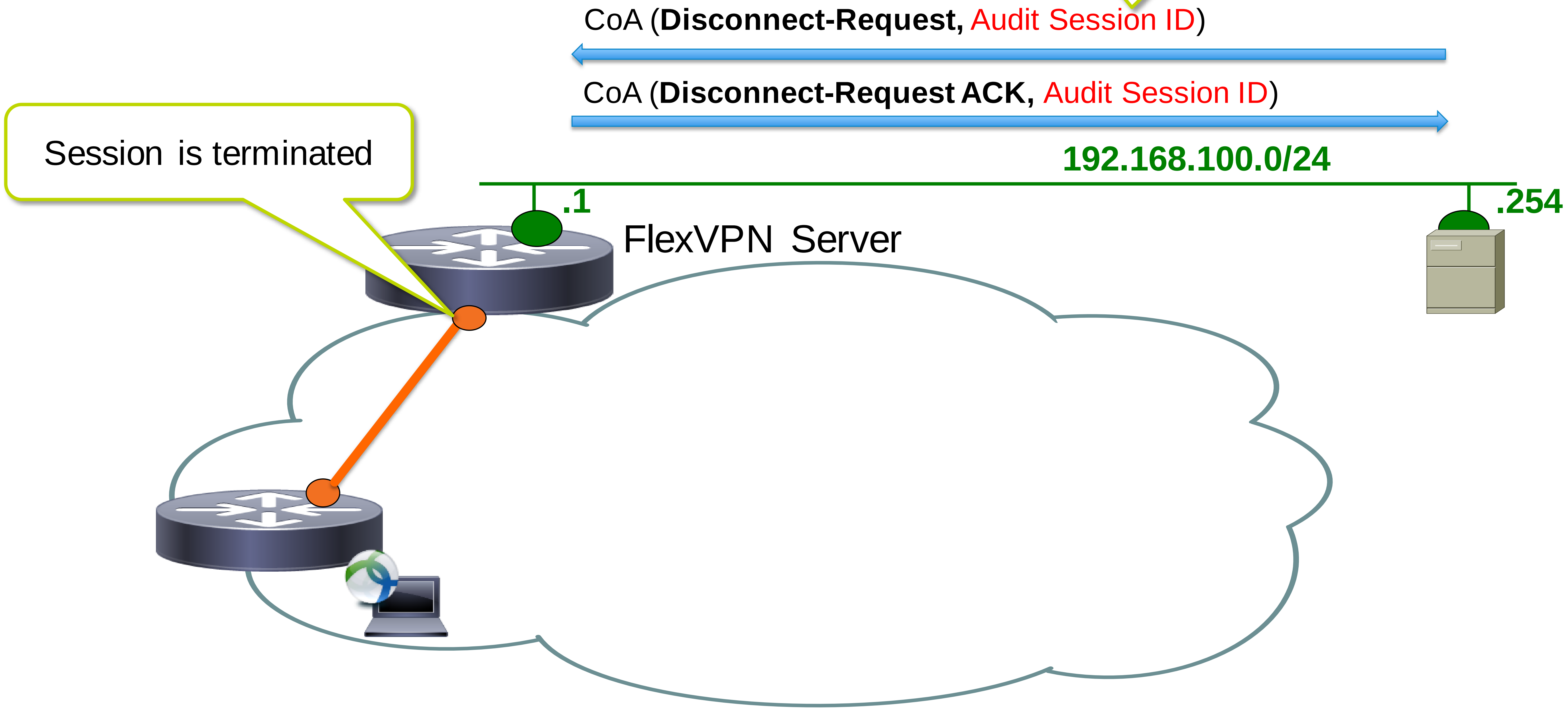
Session is set up – Accounting Starts


Unique ID, generated by IOS
ACCT (Audit Session ID, START, params…)
ACCT (Audit Session ID, ACK)
192.168.100.0/24
FlexVPN Server
.1
.254
ip access-list 100 in
service-policy **slow** out
…

CoA – Packet of Disconnect

Remote clearing of a session

Accounting tells the administrator whether it is worth sending… (session status)

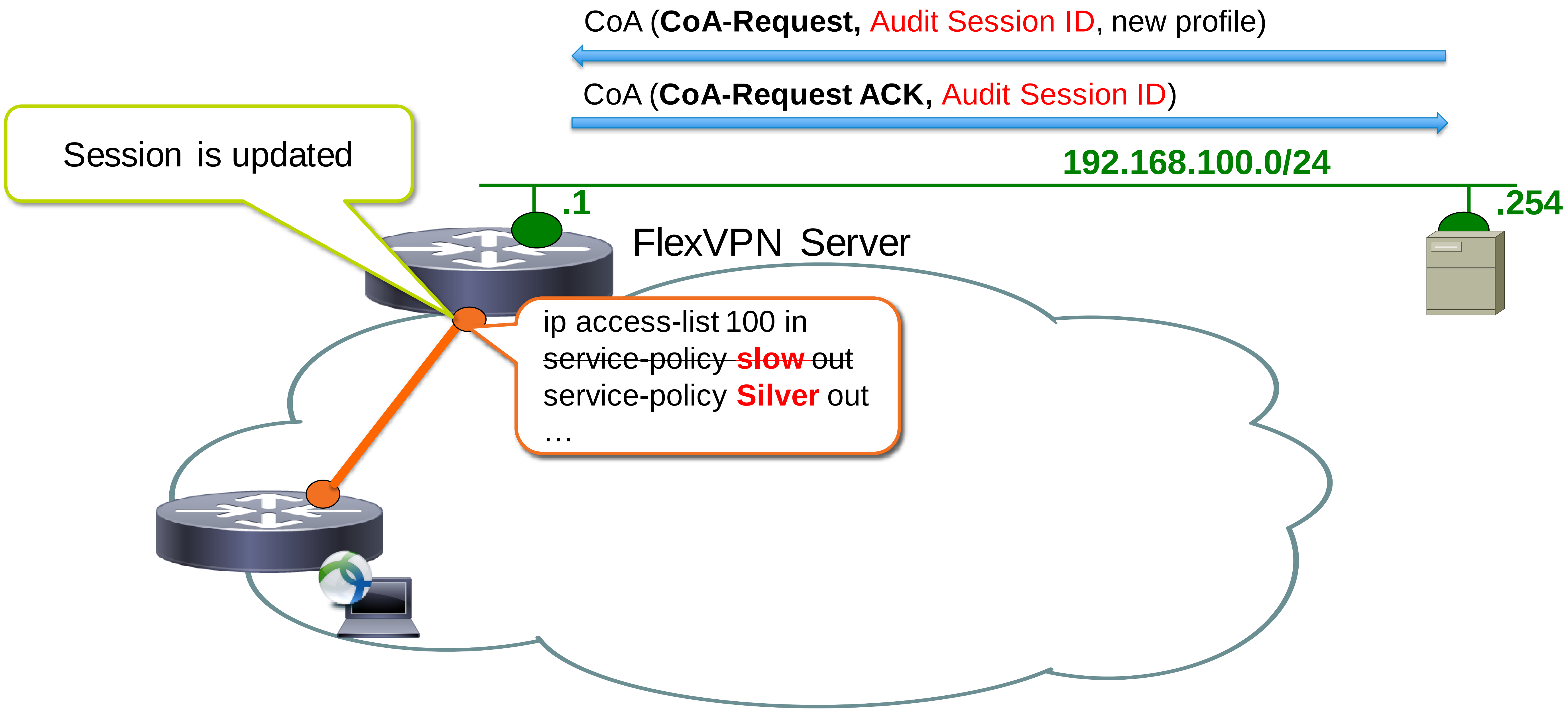

CoA (**Disconnect-Request,** Audit Session ID)

CoA (**Disconnect-Request ACK,** Audit Session ID)

Session is terminated

CoA – Change of Authorisation

The Real Thing ™


CoA (**CoA-Request,** Audit Session ID, new profile)

CoA (**CoA-Request ACK,** Audit Session ID)

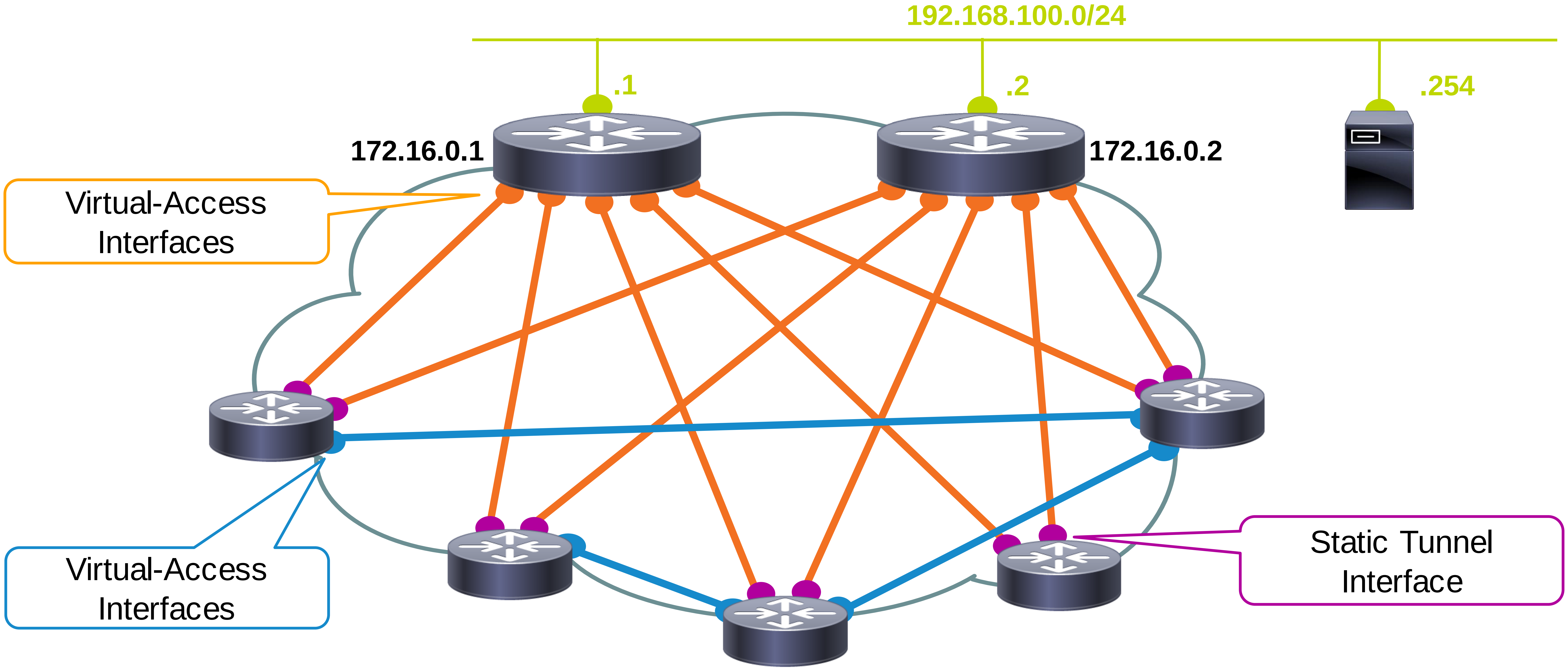
Session is updated

ip access-list 100 in
~~service-policy **slow** out~~
service-policy **Silver** out
…

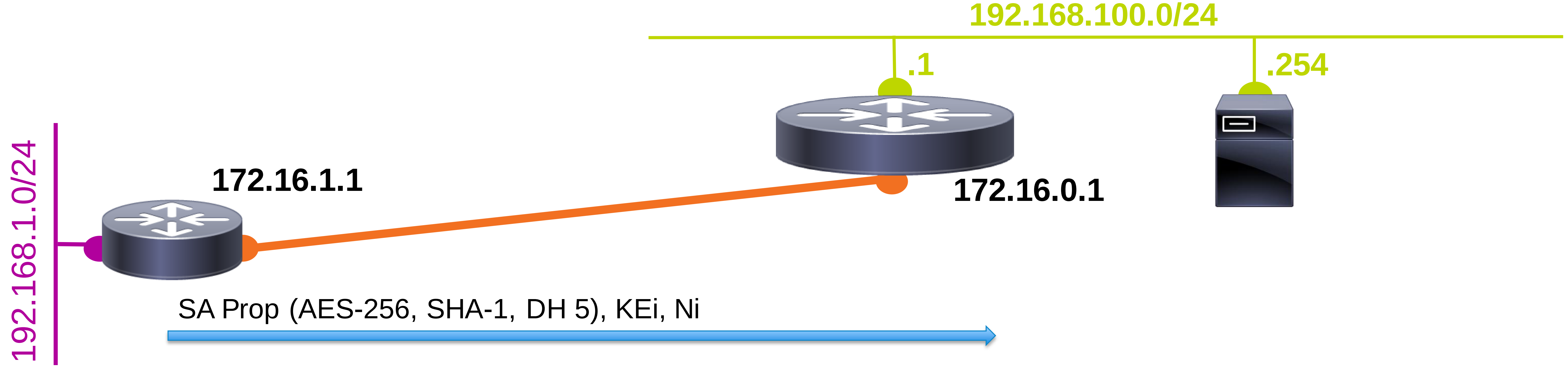
Shortcut Switching With IKEv2 Routing

FlexVPN Mesh

Network Diagram with Hub Resiliency



Hub and Spoke Bootstrap – Config Exchange



SA Prop (AES-256, SHA-1, DH 5), KEi, Ni

SA Prop (AES-256, SHA-1, DH 5), KEr, Nr

IDi=Spoke1.cisco.com, Auth, TSi, TSr,

CFG_Req(IP4_SUBNET…)

IDr, cert, Auth, TSi, TSr,

CFG_Reply(IP4_SUBNET=10.0.0.254/32, 192.168.0.0/16;
IP4_ADDRESS=10.0.0.1)

CFG_set(IP4_SUBNET=10.0.0.1/32, 192.168.1.0/24,
10.0.0.1/32)

CFG_ack()

Interfaces

Ethernet0/0: 172.16.1.1
Ethernet0/1: 192.168.1.1
Tunnel0: **10.0.0.1**

Spoke Assigned Address (optional)

Routing Table

172.16.0.1/32 → 172.16.1.254 (E0/0)
192.168.1.0/24 → Ethernet 0/1
10.0.0.254/32 → Tunnel 0
192.168.0.0/16 → Tunnel 0

Supernet covering all spokes LAN prefixes

Interfaces

Ethernet0/0: 172.16.0.1
Ethernet0/1: 192.168.100.1
Loopback0: **10.0.0.254/32**
VirtualAccess1: 10.0.0.254/32

Routing Table

0.0.0.0/0 → 172.16.0.254 (E0/0)
192.168.100.0/24 → Ethernet 0/1
10.0.0.1/32 → VirtualAccess1
192.168.1.0/24 → VirtualAccess1

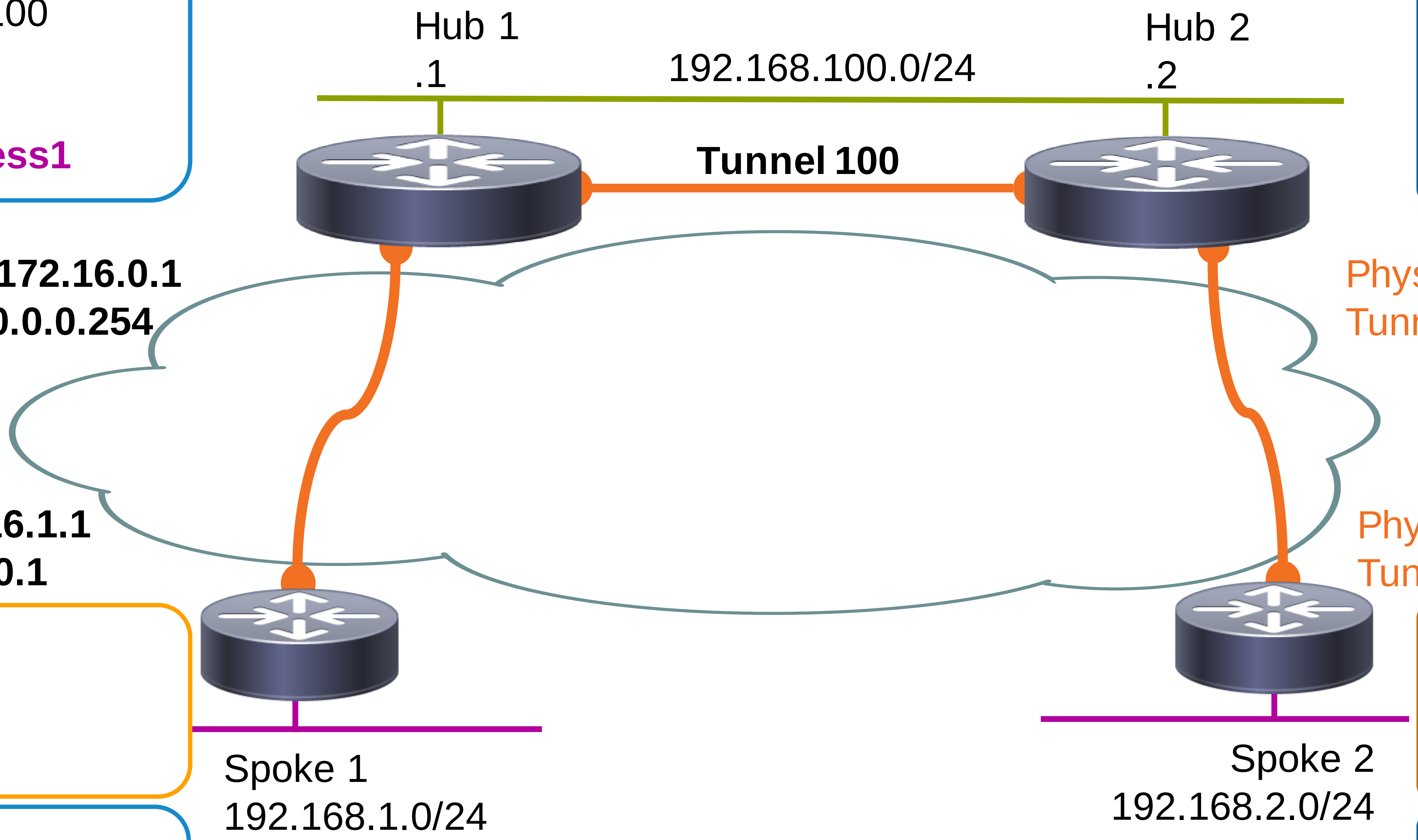
FlexVPN Hub and Spoke – IKE Route Exchange

Routing Table

C 10.0.0.254 → Loopback0
C 192.168.100.0/24 → Eth0
S 192.168.0.0/16 → Tunnel100
S 10.0.0.0/8 → Tunnel100
S 10.0.0.1 → V-Access1
S 192.168.1.0/24 → V-Access1

Routing Table

C 10.0.0.253 → Loopback0
C 192.168.100.0/24 → Eth0
S 192.168.0.0/16 → Tunnel100
S 10.0.0.0/8 → Tunnel100
S 10.0.0.2 → V-Access1
S 192.168.2.0/24 → V-Access1



NHRP Table

-

Routing Table

C 192.168.1.0/24 → Eth0
C 10.0.0.1 → Tunnel0
S 0.0.0.0/0 → Dialer0
S 10.0.0.254/32 → Tunnel0
S 192.168.0.0/16 → Tunnel0

NHRP Table

-

Routing Table

C 192.168.2.0/24 → Eth0
C 10.0.0.2 → Tunnel1
S 0.0.0.0/0 → Dialer0
S 10.0.0.253/32 → Tunnel1
S 192.168.0.0/16 → Tunnel1

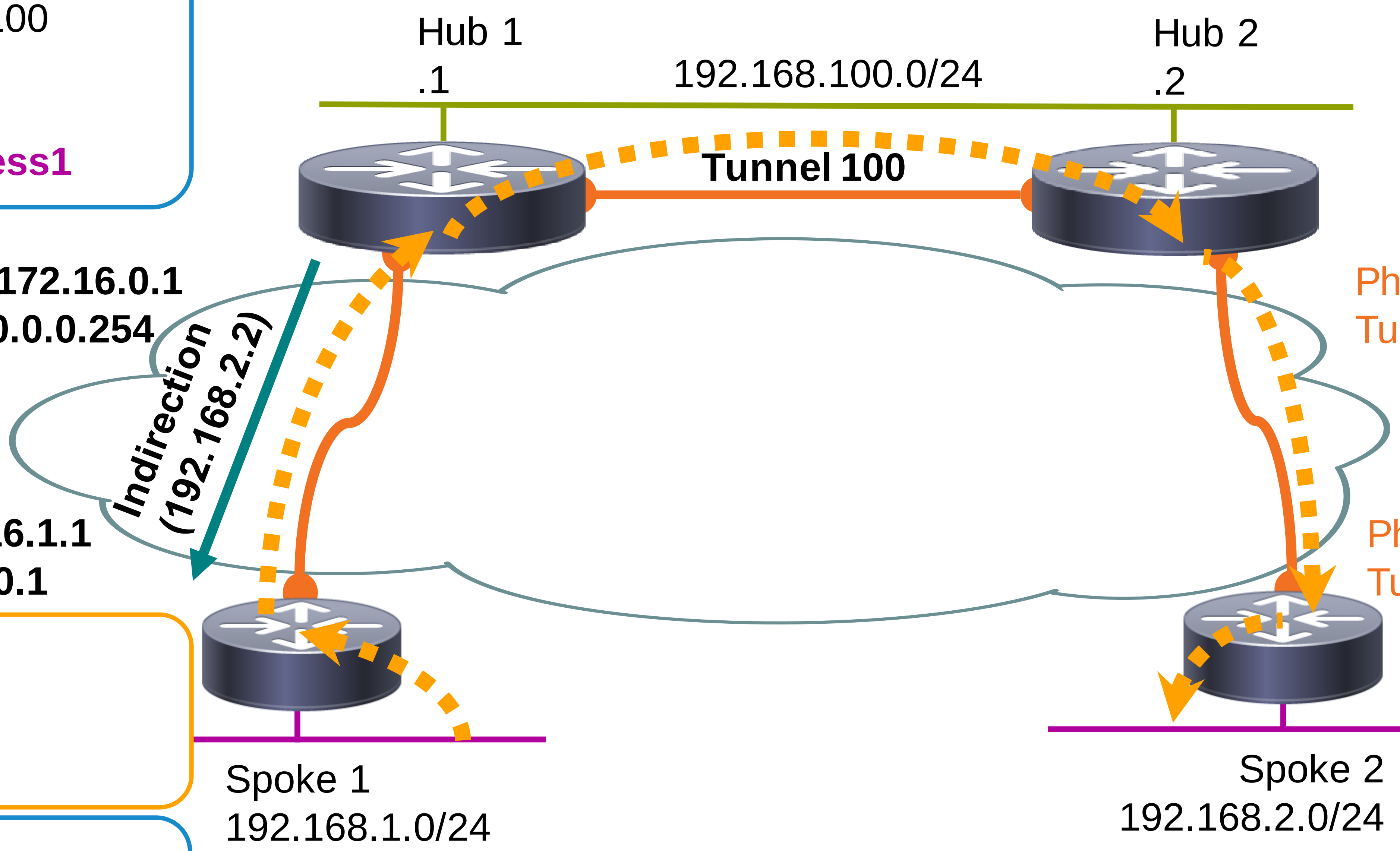
FlexVPN Mesh – Indirection

Routing Table

C 10.0.0.254 → Loopback0
C 192.168.100.0/24 → Eth0
S 192.168.0.0/16 → Tunnel100
S 10.0.0.0/8 → Tunnel100
S 10.0.0.1 → V-Access1
S 192.168.1.0/24 → V-Access1

Routing Table

C 10.0.0.253 → Loopback0
C 192.168.100.0/24 → Eth0
S 192.168.0.0/16 → Tunnel100
S 10.0.0.0/8 → Tunnel100
S 10.0.0.2 → V-Access1
S 192.168.2.0/24 → V-Access1



NHRP Table

-

NHRP Table

-

Routing Table

C 192.168.1.0/24 → Eth0
C 10.0.0.1 → Tunnel0
S 0.0.0.0/0 → Dialer0
S 10.0.0.254/32 → Tunnel0
S 192.168.0.0/16 → Tunnel0

Routing Table

C 192.168.2.0/24 → Eth0
C 10.0.0.2 → Tunnel1
S 0.0.0.0/0 → Dialer0
S 10.0.0.253/32 → Tunnel1
S 192.168.0.0/16 → Tunnel1

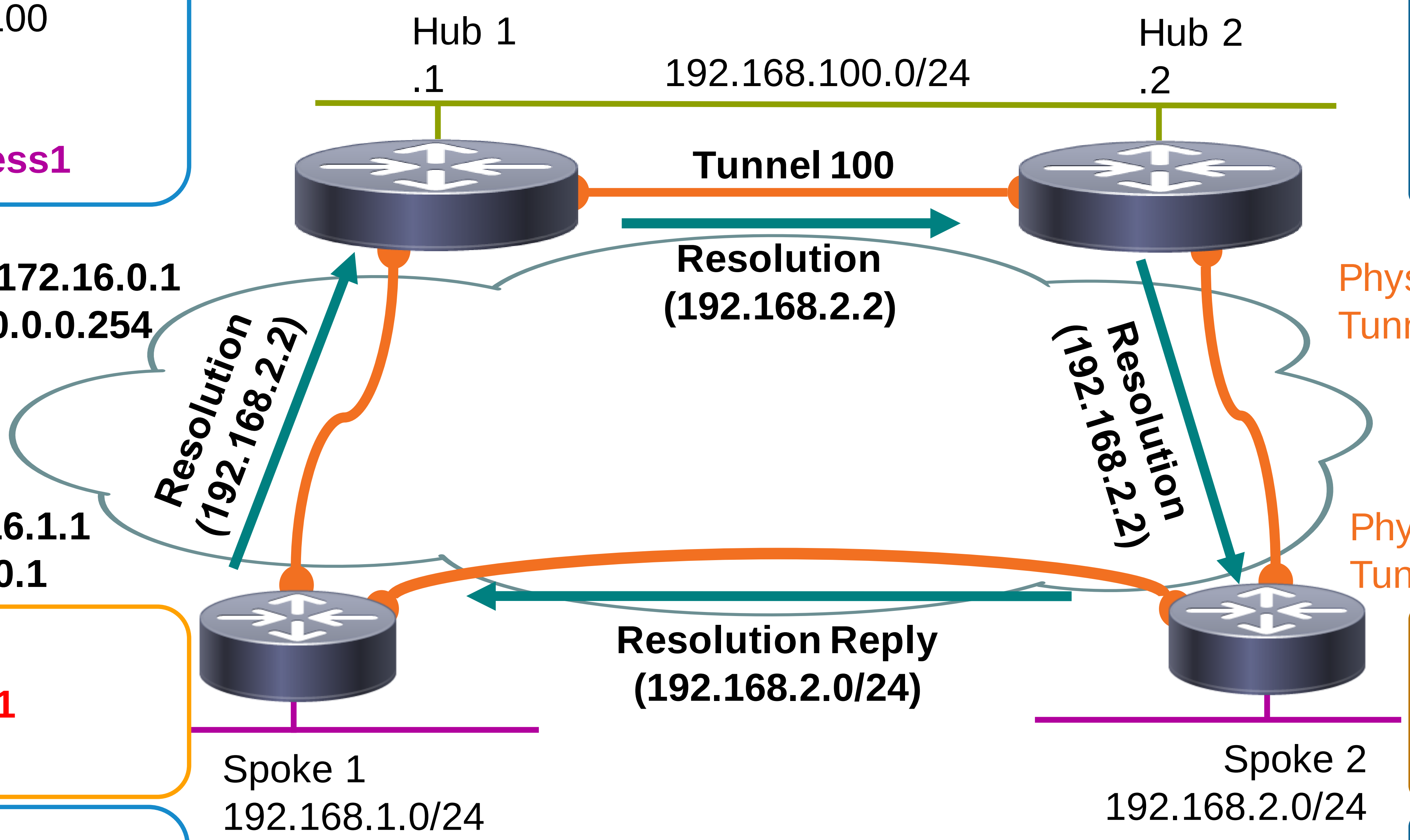
FlexVPN Mesh – Resolution

Routing Table

C 10.0.0.254 → Loopback0
C 192.168.100.0/24 → Eth0
S 192.168.0.0/16 → Tunnel100
S 10.0.0.0/8 → Tunnel100
S 10.0.0.1 → V-Access1
S 192.168.1.0/24 → V-Access1

Routing Table

C 10.0.0.253 → Loopback0
C 192.168.100.0/24 → Eth0
S 192.168.0.0/16 → Tunnel100
S 10.0.0.0/8 → Tunnel100
S 10.0.0.2 → V-Access1
S 192.168.2.0/24 → V-Access1



NHRP Table

10.0.0.2/32 → 172.16.2.1
192.168.2.0/24 → 172.16.2.1

Routing Table

C 192.168.1.0/24 → Eth0
C 10.0.0.1 → Tunnel0
S 0.0.0.0/0 → Dialer0
S 10.0.0.254/32 → Tunnel0
S 192.168.0.0/16 → Tunnel0
H/S 10.0.0.2/32 → V-Access1
H/S 192.168.2.0/24 → V-Access1

NHRP Table

10.0.0.1 → 172.16.1.1

Routing Table

C 192.168.2.0/24 → Eth0
C 10.0.0.2 → Tunnel1
S 0.0.0.0/0 → Dialer0
S 10.0.0.253/32 → Tunnel1
S 192.168.0.0/16 → Tunnel1
H/S 10.0.0.1/32 → V-Access1

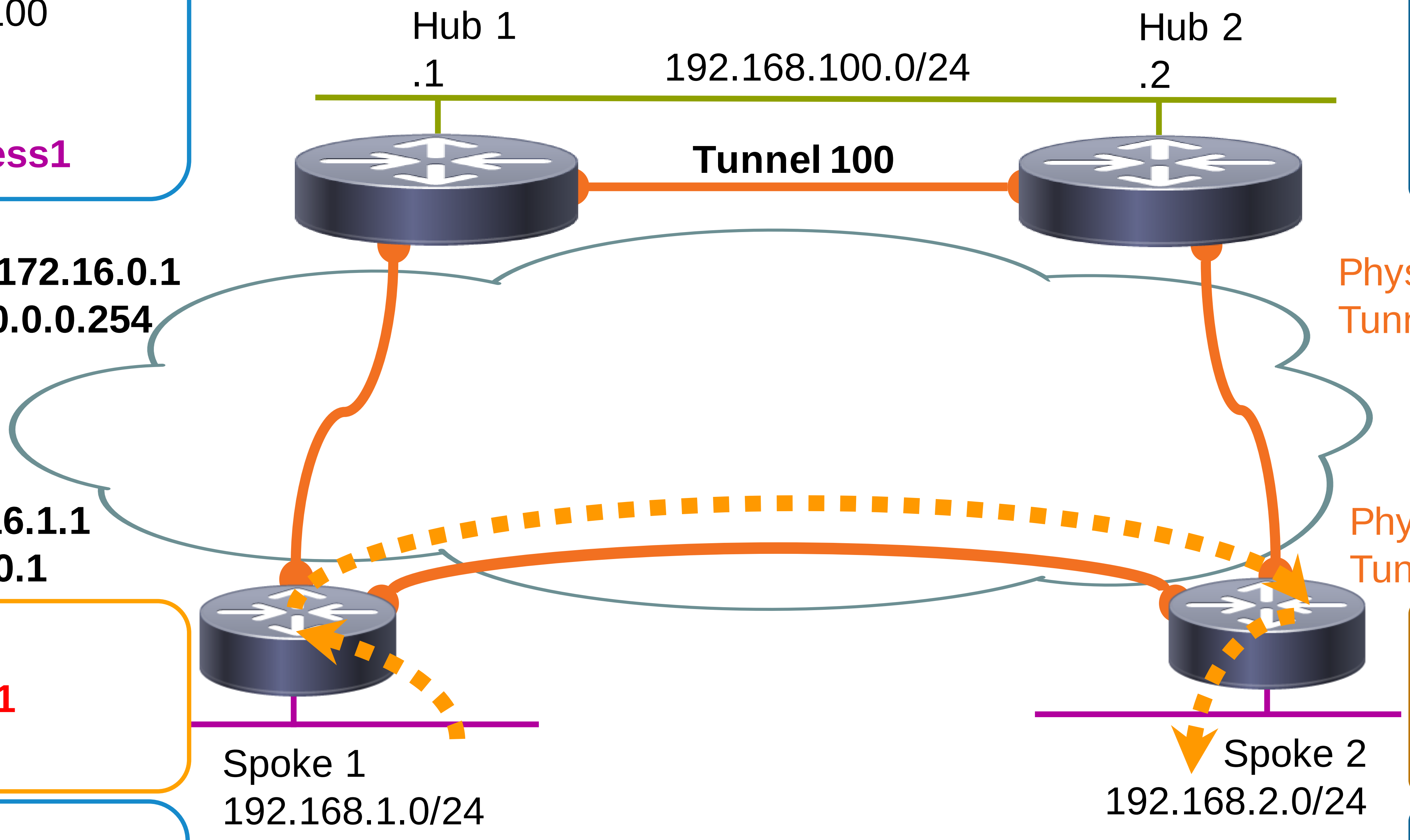
FlexVPN Mesh – Shortcut Forwarding

Routing Table

C 10.0.0.254 → Loopback0
C 192.168.100.0/24 → Eth0
S 192.168.0.0/16 → Tunnel100
S 10.0.0.0/8 → Tunnel100
S 10.0.0.1 → V-Access1
S 192.168.1.0/24 → V-Access1

Routing Table

C 10.0.0.253 → Loopback0
C 192.168.100.0/24 → Eth0
S 192.168.0.0/16 → Tunnel100
S 10.0.0.0/8 → Tunnel100
S 10.0.0.2 → V-Access1
S 192.168.2.0/24 → V-Access1



Physical: **172.16.0.1**
Tunnel: **10.0.0.254**

Physical: **172.16.0.2**
Tunnel: **10.0.0.253**

Physical: **172.16.1.1**
Tunnel: **10.0.0.1**

Physical: **172.16.2.1**
Tunnel: **10.0.0.2**

NHRP Table

10.0.0.2/32 → 172.16.2.1
192.168.2.0/24 → 172.16.2.1

NHRP Table

10.0.0.1 → 172.16.1.1

Routing Table

C 192.168.1.0/24 → Eth0
C 10.0.0.1 → Tunnel0
S 0.0.0.0/0 → Dialer0
S 10.0.0.254/32 → Tunnel0
S 192.168.0.0/16 → Tunnel0
H/S 10.0.0.2/32 → V-Access1
H/S 192.168.2.0/24 → V-Access1

Routing Table

C 192.168.2.0/24 → Eth0
C 10.0.0.2 → Tunnel1
S 0.0.0.0/0 → Dialer0
S 10.0.0.253/32 → Tunnel1
S 192.168.0.0/16 → Tunnel1
H/S 10.0.0.1/32 → V-Access1

FlexVPN Mesh (IKEv2 Routing)

Hub 1 Configuration

```
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Hub1.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint TP
 dpd 10 2 on-demand
 aaa authorization group cert list default default
 virtual-template 1
 !
crypto ikev2 authorization policy default
 route set remote 10.0.0.0 255.0.0.0
 route set remote 192.168.0.0 255.255.0.0
```

Accept connections from Spokes

Local or AAA spoke profiles supported. Can even control QoS, ZBF, NHRP redirect, network-id, …

These prefixes can also be set by RADIUS

Defines which prefixes should be protected

```
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 ip access-group AllowMyBGP in
 tunnel protection ipsec profile default
!
interface Loopback0
 ip address 10.0.0.254 255.255.255.255
!
interface Tunnel100
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel source Ethernet0/1
 tunnel destination 192.168.100.2
```

Static per-spoke features applied here

NHRP is the magic
All V-Access will be in the same network-id

Hub 1 dedicated overlay address

Inter-Hub link (not encrypted)

Same NHRP network-id on v-access and inter-hub link

FlexVPN Mesh (IKEv2 Routing)

Hub 2 Configuration

```
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Hub2.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint TP
 dpd 10 2 on-demand
 aaa authorization group cert list default default
 virtual-template 1
 !
crypto ikev2 authorization policy default
 route set remote 10.0.0.0 255.0.0.0
 route set remote 192.168.0.0 255.255.0.0
```

Dedicated Identity (optional)

```
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 ip access-group AllowMyBGP in
 tunnel protection ipsec profile default
!
interface Loopback0
 ip address 10.0.0.254 255.255.255.255
!
interface Tunnel100
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel source Ethernet0/1
 tunnel destination 192.168.100.2
```

Dedicated Overlay Address

FlexVPN Mesh (IKEv2 Routing)

Spoke Configuration

QoS Everywhere!

```
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Spoke2.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint TP
 dpd 10 2 on-demand
 aaa authorization group cert list default default
 virtual-template 1
```

Needed for tunnel address exchange

```
crypto ikev2 authorization policy default
 route set interface
 route set interface e0/0
```

V-Template to clone for spoke-spoke tunnels

```
interface Loopback0
 ip address 10.0.0.2 255.255.255.255

interface Tunnel0
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source Ethernet0/0
 tunnel destination 172.16.0.1
 tunnel protection ipsec profile default
!
interface Tunnel1
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source Ethernet0/0
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile default

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel protection ipsec profile default
```

Tunnel to Hub 1

Tunnel1 to Hub 2

QoS can be applied here

Shortcut Switching

With a routing protocol (BGP)

FlexVPN Mesh with BGP Routing

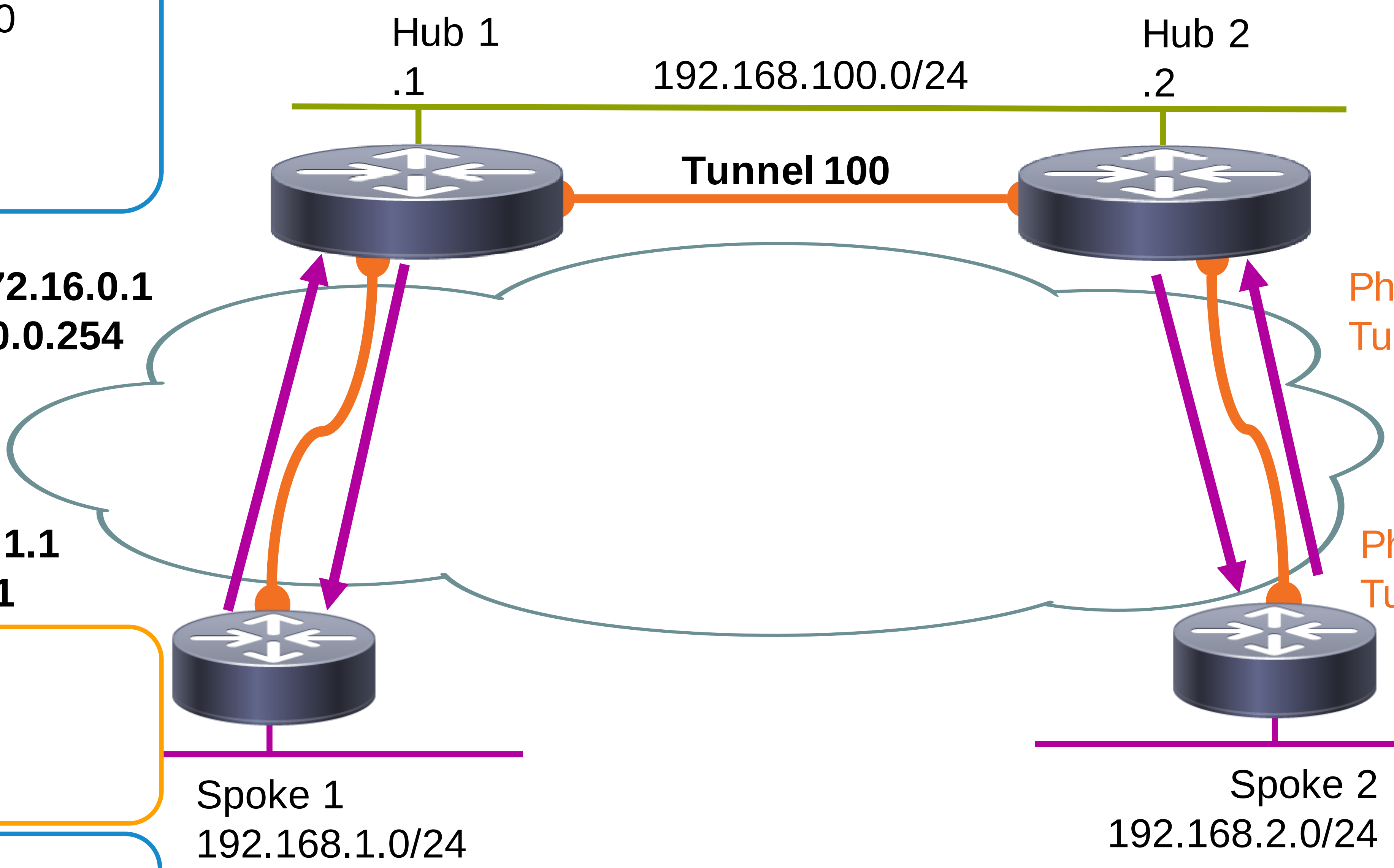
For your reference

Routing Table

C 10.0.0.254 → Loopback0
C 192.168.100.0/24 → Eth0
S 192.168.0.0/16 → Tunnel100
S 10.0.0.0/8 → Tunnel100
S 10.0.0.1 → V-Access1
B 192.168.1.0/24 → 10.0.0.1

Routing Table

C 10.0.0.253 → Loopback0
C 192.168.100.0/24 → Eth0
S 192.168.0.0/16 → Tunnel100
S 10.0.0.0/8 → Tunnel100
S 10.0.0.2 → V-Access1
B 192.168.2.0/24 → 10.0.0.2



NHRP Table

-

Routing Table

C 192.168.1.0/24 → Eth0
C 10.0.0.1 → Tunnel0
S 0.0.0.0/0 → Dialer0
S 10.0.0.254/32 → Tunnel0
B 192.168.0.0/16 → 10.0.0.254

NHRP Table

-

Routing Table

C 192.168.2.0/24 → Eth0
C 10.0.0.2 → Tunnel1
S 0.0.0.0/0 → Dialer0
S 10.0.0.253/32 → Tunnel1
B 192.168.0.0/16 → 10.0.0.253

For your reference

FlexVPN Mesh (BGP)

Hub 1 Configuration

```
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Hub1.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint TP
 dpd 10 2 on-demand
 aaa authorization group cert list default default
 virtual-template 1

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip access-group AllowMyBGP in
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel protection ipsec profile default

interface Loopback0
 ip address 10.0.0.254 255.255.255.255

interface Tunnel100
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel source Ethernet0/1
 tunnel destination 192.168.100.2
```

Accept connections from Spokes

Local or AAA spoke profiles supported. Can even control QoS, NHRP redirect, network-id, …

Static per-per config here…

NHRP is the magic
All V-Access will be in the same network-id

Hub 1 dedicated overlay address

Inter-Hub link
(not encrypted)

Same NHRP network-id on v-access and inter-hub link

```
ip route 10.0.0.0 255.0.0.0 Tunnel100 tag 2
ip route 192.168.0.0 255.255.0.0 Tunnel100 tag 2

router bgp 1
 bgp log-neighbor-changes
 bgp listen range 10.0.0.0/24 peer-group Flex
 !
 address-family ipv4
  neighbor Flex peer-group
  neighbor Flex remote-as 1
  neighbor Flex timers 5 15
  neighbor Flex next-hop-self all
  redistribute static route-map rm
 exit-address-family
!
route-map rm permit 10
 match tag 2
```

Dynamically accept spoke BGP peering!

route-map filters static routes to redistribute in BGP

For your reference

FlexVPN Mesh (BGP)

Hub 2 Configuration

```
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Hub2.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint TP
 dpd 10 2 on-demand
 aaa authorization group cert list default default
 virtual-template 1

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip access-group AllowMyBGP in
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel protection ipsec profile default

interface Loopback0
 ip address 10.0.0.253 255.255.255.255

interface Tunnel100
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel source Ethernet0/1
 tunnel destination 192.168.100.1
```

Dedicated Identity (optional)

Dedicated Overlay Address

```
ip route 10.0.0.0 255.0.0.0 Tunnel100 tag 2
ip route 192.168.0.0 255.255.0.0 Tunnel100 tag 2

router bgp 1
 bgp log-neighbor-changes
 bgp listen range 10.0.0.0/24 peer-group Flex
 !
 address-family ipv4
  redistribute static route-map rm
  neighbor Flex peer-group
  neighbor Flex remote-as 1
  neighbor Flex timers 5 15
  neighbor Flex next-hop-self all
 exit-address-family
!
route-map rm permit 10
 match tag 2
```

- Almost the same as Hub 1 again!

FlexVPN Mesh (BGP)

Spoke Configuration

QoS Everywhere!

For your reference

```
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Spoke2.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint TP
 dpd 10 2 on-demand
 aaa authorization group cert list default default
 virtual-template 1
```

Needed for tunnel address exchange

```
router bgp 1
 bgp log-neighbor-changes
 neighbor 10.0.0.253 remote-as 1
 neighbor 10.0.0.253 timers 5 15
 neighbor 10.0.0.254 remote-as 1
 neighbor 10.0.0.254 timers 5 15
 !
 address-family ipv4
  network 192.168.2.0
  neighbor 10.0.0.253 activate
  neighbor 10.0.0.254 activate
  maximum-paths ibgp 2
```

V-Template to clone for spoke-spoke tunnels

```
interface Loopback0
 ip address 10.0.0.2 255.255.255.255

interface Tunnel0
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source Ethernet0/0
 tunnel destination 172.16.0.1
 tunnel protection ipsec profile default
!
interface Tunnel1
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source Ethernet0/0
 tunnel destination 172.16.0.2
 tunnel protection ipsec profile default

interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel protection ipsec profile default
```

Tunnel to Hub 1

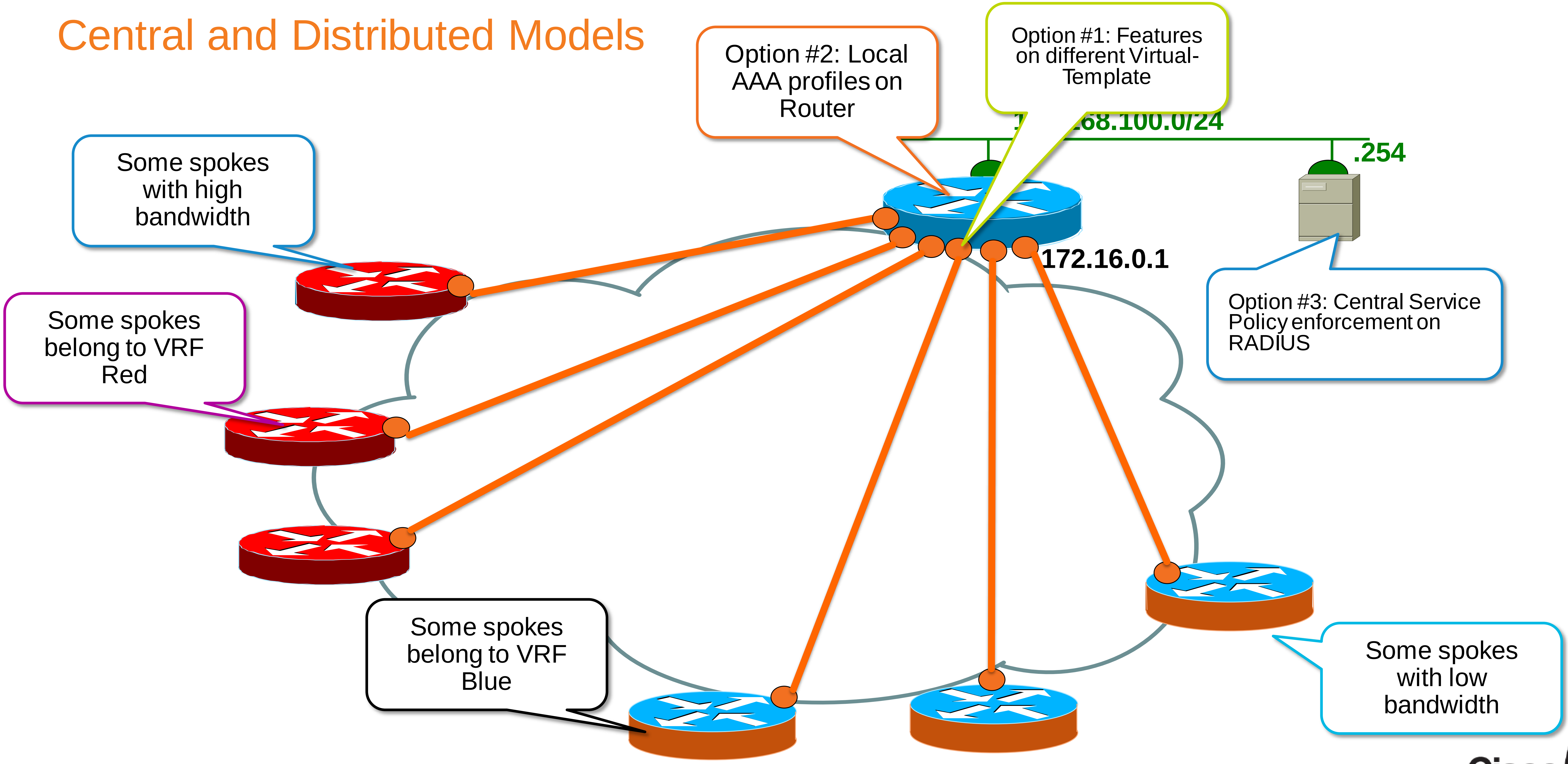
Tunnel1 to Hub 2

QoS can be applied here

Per Session Features: ACL, VRF ,ZBFW, QoS

Provisioning Per-Peer Features

Central and Distributed Models



Option #2: Local AAA profiles on Router

Option #1: Features on different Virtual-Template

Some spokes with high bandwidth

Some spokes belong to VRF Red

Option #3: Central Service Policy enforcement on RADIUS

Some spokes belong to VRF Blue

Some spokes with low bandwidth

VRF Injection

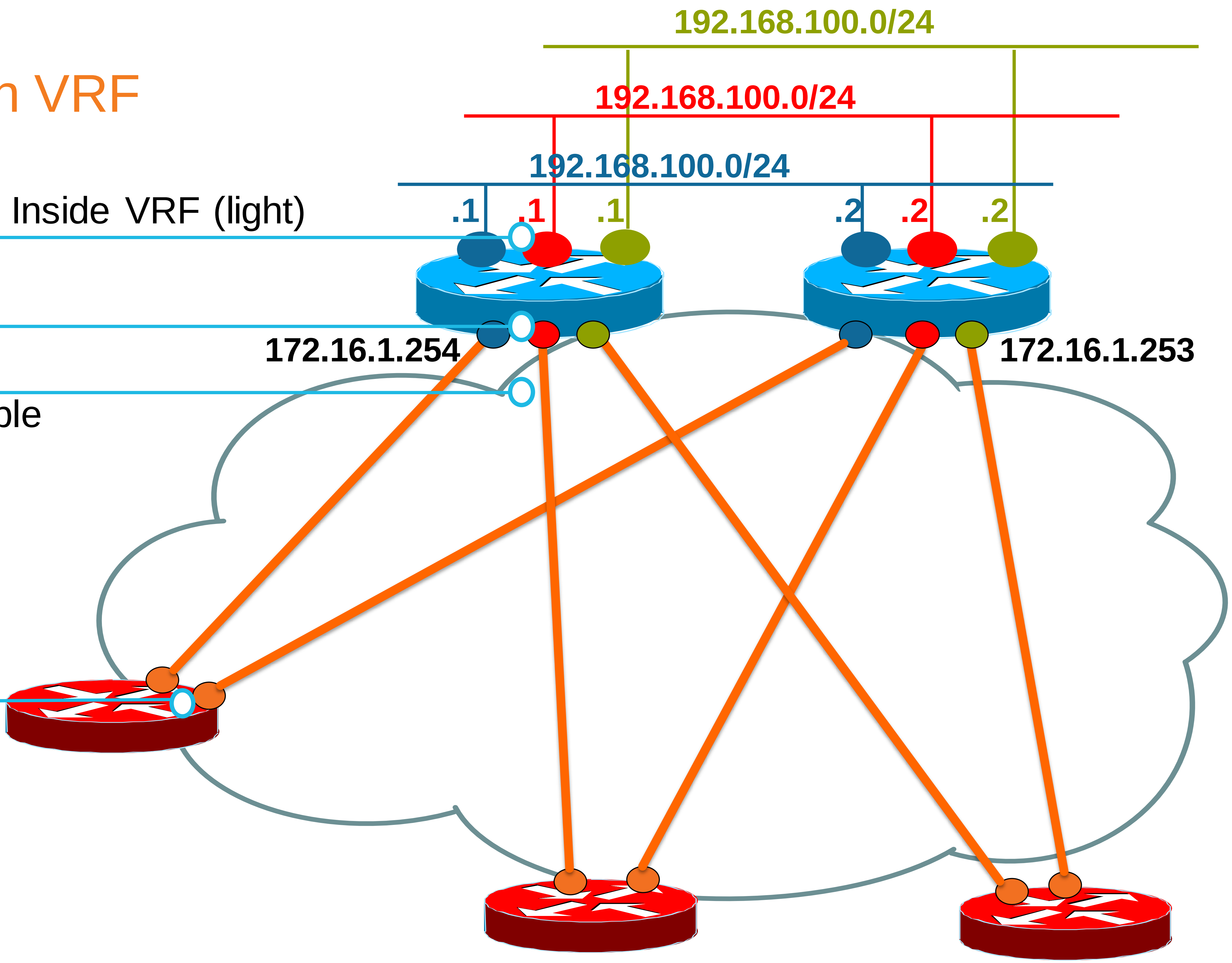
Hub injects traffic in chosen VRF

Hub private interface(s) in Inside VRF (light)

Virtual-Access in iVRF

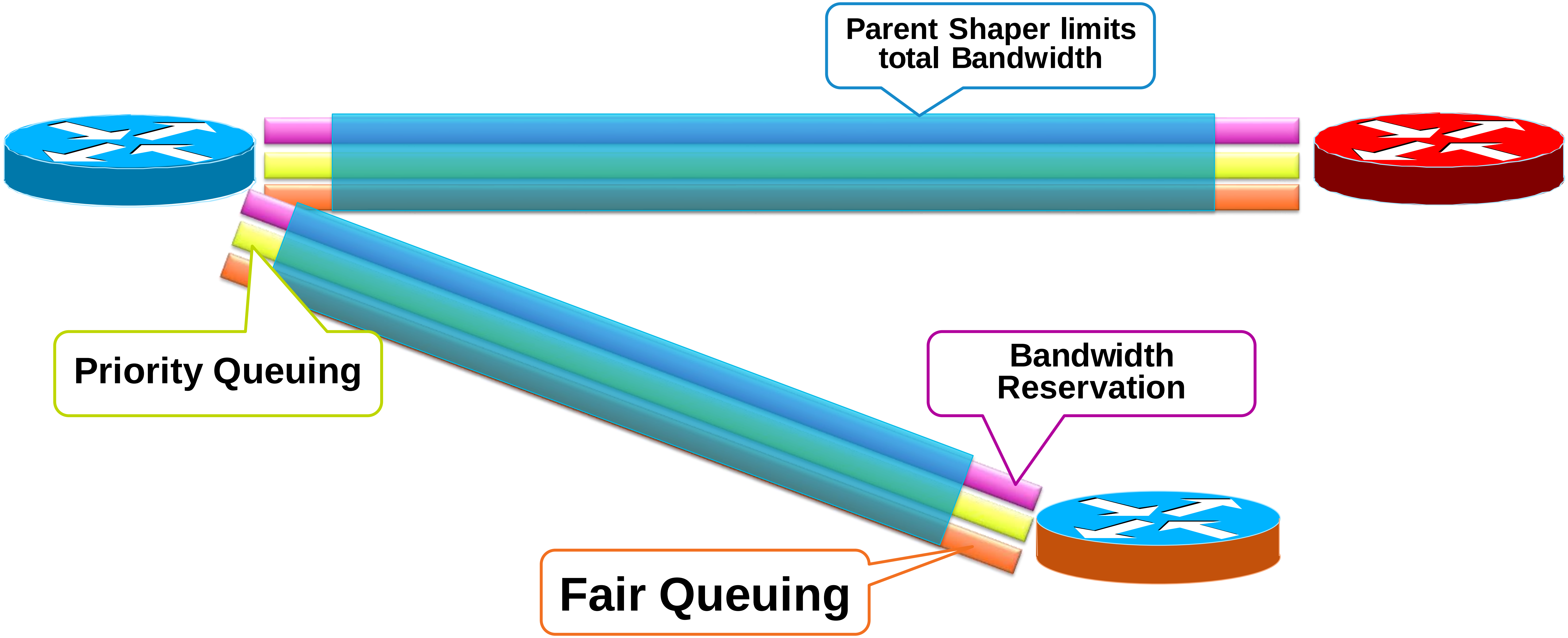
Wan in Global Routing Table
or Front VRF

Optional VRF on spokes
(Not in this example)

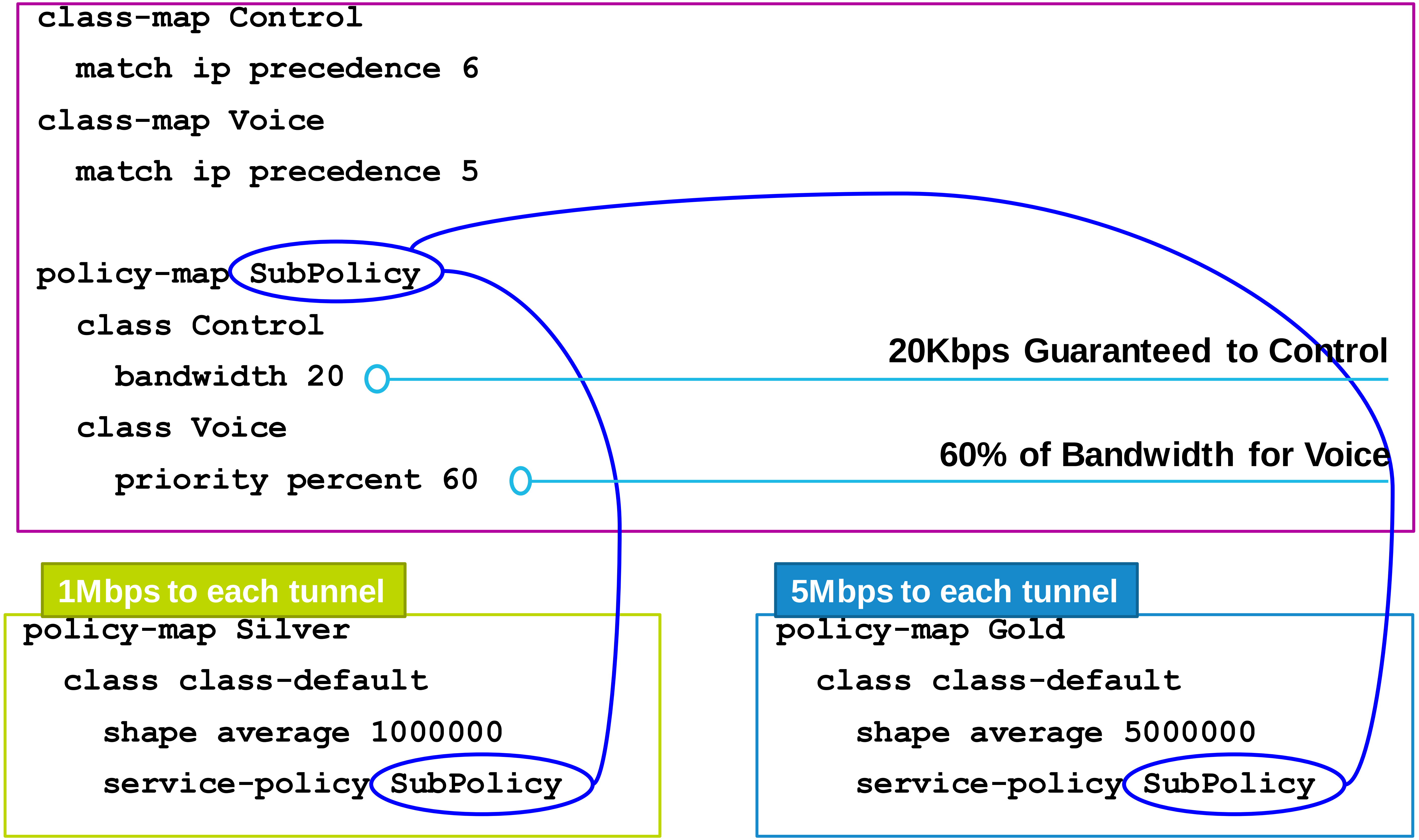


QoS in a Nutshell – Hierarchical Shaper

Each Hub V-Access Needs Its Own Policy



QOS Policy Map(s) Based on Spoke Bandwidth



```
class-map Control
  match ip precedence 6
class-map Voice
  match ip precedence 5

policy-map SubPolicy
  class Control
    bandwidth 20
  class Voice
    priority percent 60
```

20Kbps Guaranteed to Control

60% of Bandwidth for Voice

1Mbps to each tunnel

```
policy-map Silver
  class class-default
    shape average 1000000
    service-policy SubPolicy
```

5Mbps to each tunnel

```
policy-map Gold
  class class-default
    shape average 5000000
    service-policy SubPolicy
```

Heavy Configuration

VRF Injection – Hub Configuration

Option 1: Mapping with In-IOS configuration (without AAA)

Dedicated IKEv2 profile

FQDN Domain is differentiator

Virtual-Template in VRF

Loopback in VRF

```
crypto ikev2 profile BLUE
 match identity fqdn domain blue
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 dpd 10 2 on-demand
 aaa authorization group cert list default default
 virtual-template 1

interface virtual-template1 type tunnel
 vrf forwarding BLUE
 ip unnumbered loopback1
 service-policy Gold out
 tunnel protection ipsec profile default
```

Add NHRP, ACL's,…

```
crypto ikev2 profile RED
 match identity fqdn domain red
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 dpd 10 2 on-demand
 aaa authorization group cert list default default
 virtual-template 2

interface virtual-template2 type tunnel
 vrf forwarding RED
 ip unnumbered loopback2
  service-policy Gold out
 tunnel protection ipsec profile default
```

```
crypto ikev2 profile GREEN
 match identity fqdn domain green
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 dpd 10 2 on-demand
 aaa authorization group cert list default default
 virtual-template 3

interface virtual-template3 type tunnel
 vrf forwarding GREEN
 ip unnumbered loopback3
 service-policy Silver out
 tunnel protection ipsec profile default
```

VRF Injection – Hub Configuration

Option 2: Mapping with AAA group based configuration

Profiles on IOS

Common IKEv2 profile

Profile name extracted from Domain Name

Vanilla Virtual-Template

```
aaa new-model
aaa authorization network default local

crypto ikev2 profile default
 match identity any
 identity local fqdn Hub1.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 dpd 10 2 on-demand
 aaa authorization group cert default name-mangler dom
 virtual-template 1

interface virtual-template1 type tunnel
 tunnel protection ipsec profile default


crypto ikev2 name-mangler dom
  fqdn domain
```

Group profiles on IOS

```
aaa attribute list blue
 attribute type interface-config ”vrf forwarding BLUE”
 attribute type interface-config ”ip unnumbered loopback1”
 attribute type interface-config ”service-policy Gold out”

crypto ikev2 authorization policy blue
 aaa attribute list blue
 route set interface
```

```
aaa attribute list red
 attribute type interface-config ”vrf forwarding RED”
 attribute type interface-config ”ip unnumbered loopback2”
 attribute type interface-config ”service-policy Silver out”

crypto ikev2 authorization policy red
 aaa attribute list red
 route set interface
```

```
aaa attribute list green
 attribute type interface-config ”vrf forwarding GREEN”
 attribute type interface-config ”ip unnumbered loopback3”
 attribute type interface-config ”service-policy GOLD out”

crypto ikev2 authorization policy green
 aaa attribute list green
 route set interface
```

VRF Injection – Hub Configuration

Option 3: RADIUS based profiles

Profiles stored on RADIUS server

Common IKEv2 profile

Profile name extracted from Domain Name

Vanilla Virtual-Template

```
aaa new-model
aaa authorization network default group RADIUS
aaa group server radius RADIUS
  server-private 192.168.100.2 auth-port 1812
                         acct-port 1813 key cisco123

crypto ikev2 profile default
 match identity any
 identity local fqdn Hub1.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 aaa authorization group cert default name-mangler dom
 virtual-template 1

interface virtual-template1 type tunnel
 tunnel protection ipsec profile default

crypto ikev2 name-mangler dom
  fqdn domain
```

Group profiles on RADIUS
Could be per peer profiles
or group+peer (derivation)

RADIUS Group Profiles

Profile “**blue**” / password “cisco”
ipsec:route-accept=any
ipsec:route-set=interface
ip:interface-config=“**vrf forwarding BLUE**”
ip:interface-config=“**ip unnumbered loopback 1**”
ip:interface-config=“**service-policy Gold out**”

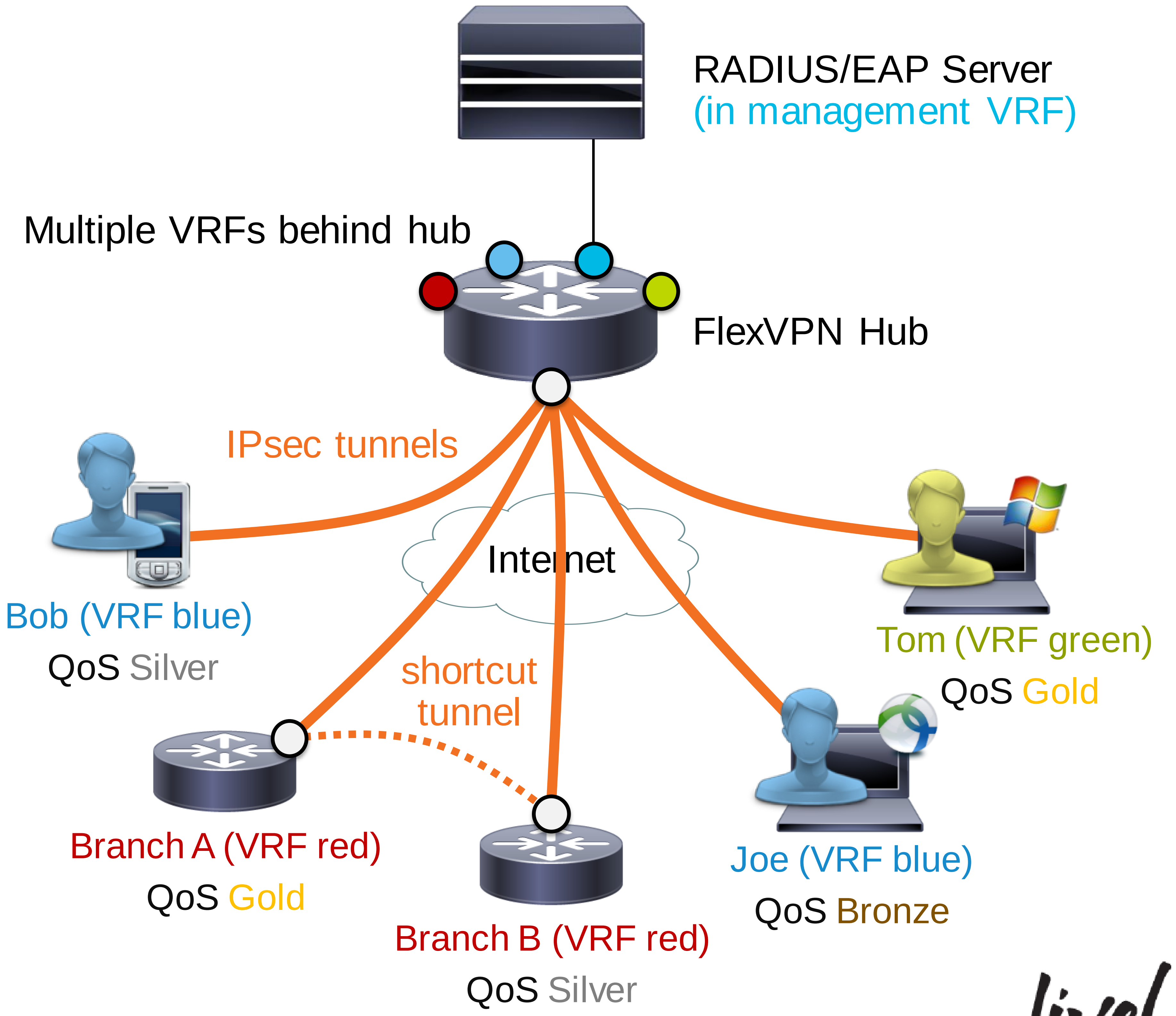
Profile “**red**” / password “cisco”
ipsec:route-accept=any
ipsec:route-set=interface
ip:interface-config=“**vrf forwarding RED**”
ip:interface-config=“**ip unnumbered loopback 2**”
ip:interface-config=“**service-policy Silver out**”

Profile “**green**” / password “cisco”
ipsec:route-accept=any
ipsec:route-set=interface
ip:interface-config=“**vrf forwarding GREEN**”
ip:interface-config=“**ip unnumbered loopback 3**”
ip:interface-config=“**service-policy Gold out**”

Case Study: Multi-tenant Hybrid Access

Use Case: Mixed Client and Branch Access

- Requirements:
  - Single router 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 authorisation depending on authentication method



FlexVPN Server Configuration

RADIUS-based EAP authentication and AAA authorisation

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 authorisation using attributes returned during EAP authentication

Branch authorisation 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 auto mode
!
interface Virtual-Template1 type tunnel
 no ip address
 [no need to specify tunnel mode]
 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 router attributes returned by RADIUS during AAA authorisation step

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

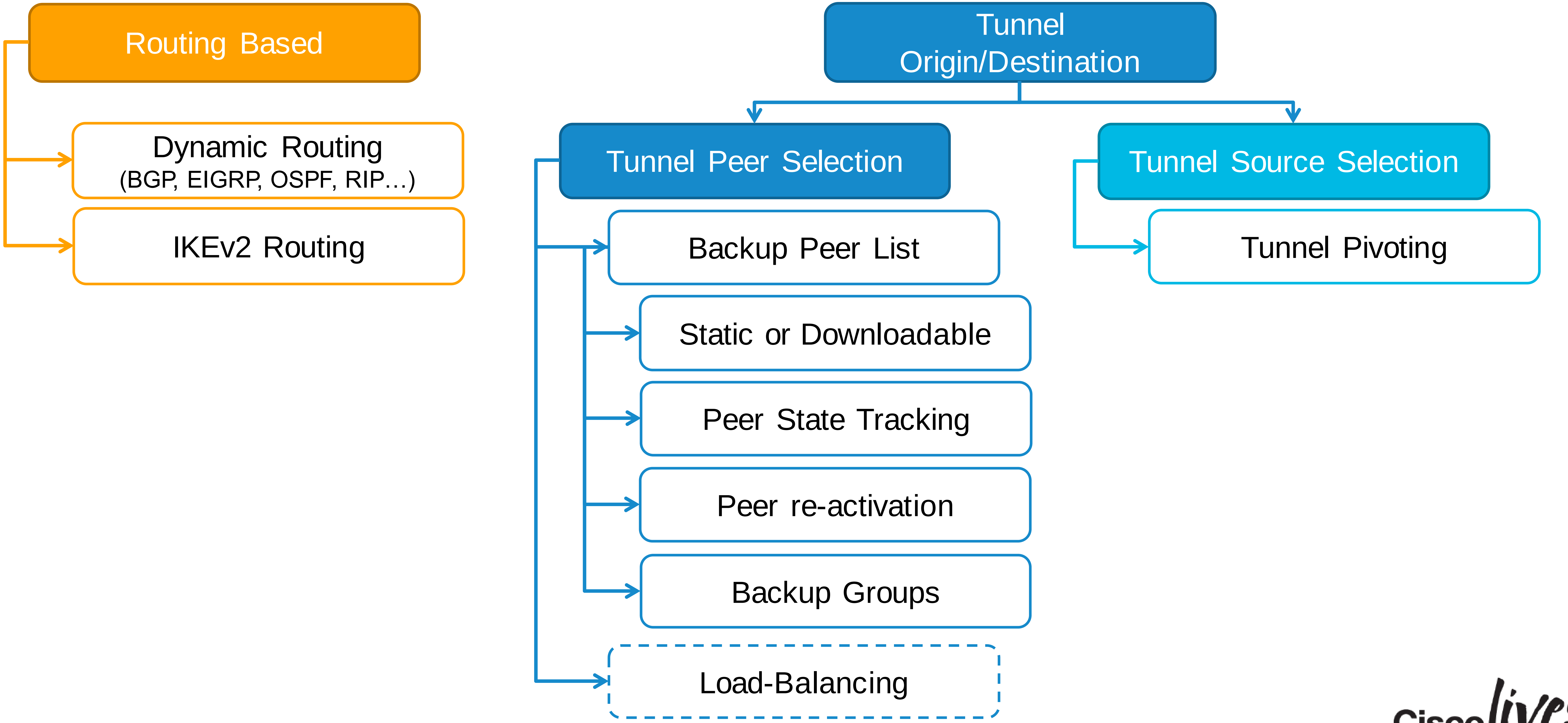
Exchange prefixes via IKEv2 routing, branch prefix(es) controlled by branch

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 Bronze
  ip:interface-config=...

branch1.example.com
  ip:interface-config=vrf forwarding red
  ip:interface-config=ip unnumbered Loopback3
  ip:interface-config=service-policy output Gold
  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
  ip:interface-config=service-policy output Silver
  ipsec:route-set=prefix 192.168.0.0 255.255.0.0
  ipsec:route-set=local 192.168.1.0 255.255.255.0
```

FlexVPN High Availability

FlexVPN Backup Mechanisms



Routing Based

Dynamic Routing (BGP, EIGRP, OSPF, RIP…)

IKEv2 Routing

Tunnel Origin/Destination

Tunnel Peer Selection

Backup Peer List

Static or Downloadable

Peer State Tracking

Peer re-activation

Backup Groups

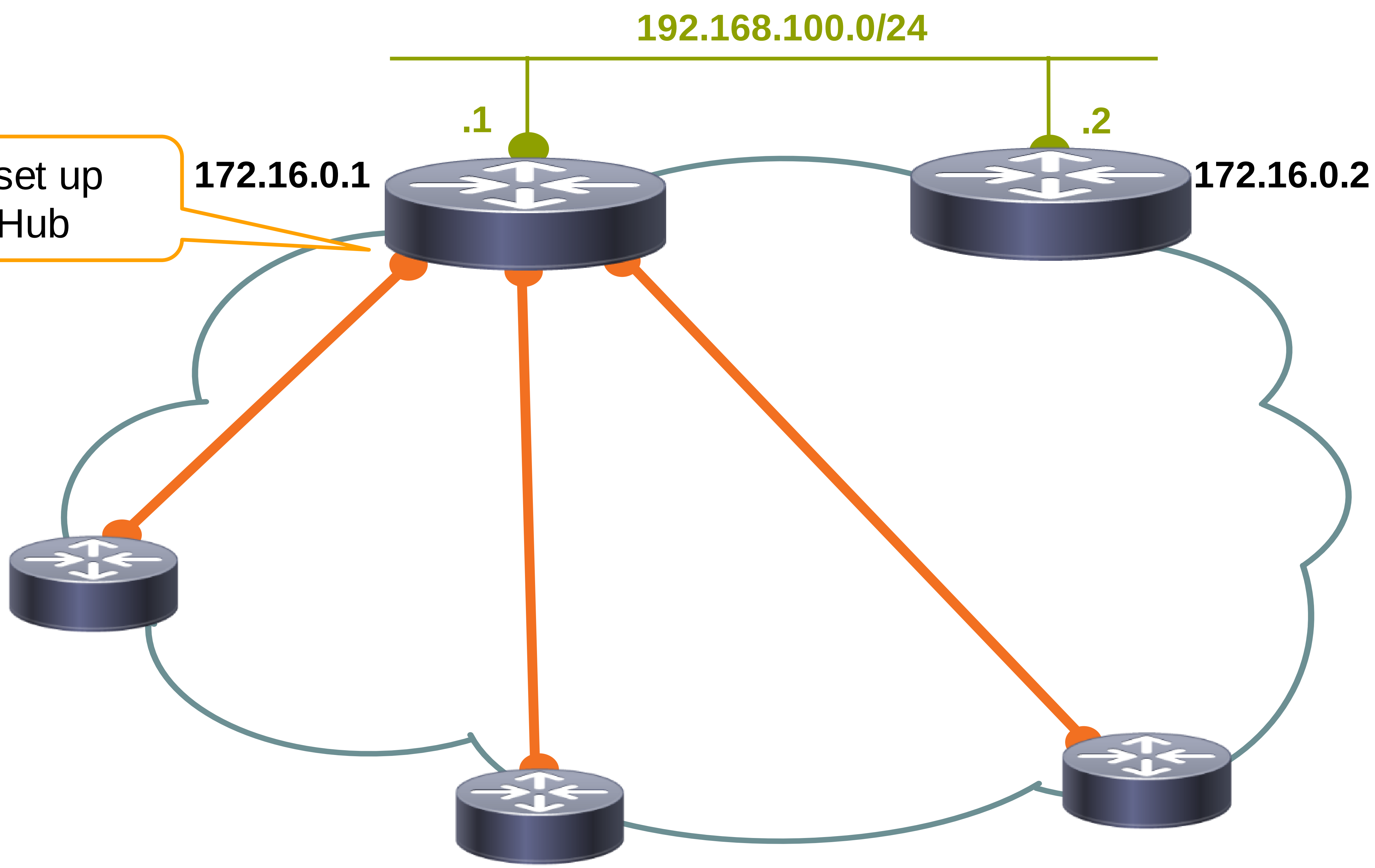
Load-Balancing

Tunnel Source Selection

Tunnel Pivoting

FlexVPN Backup

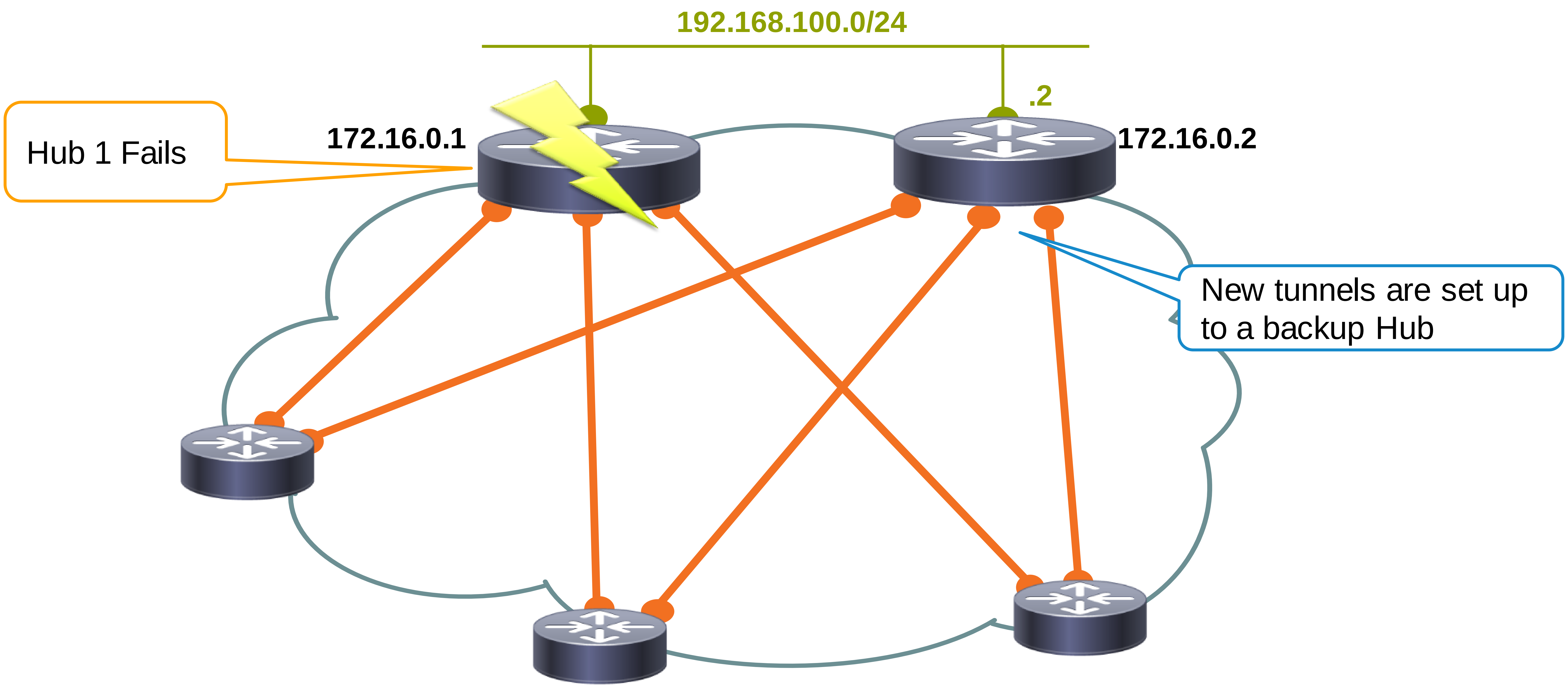
IKE Backup Peers (1)



Tunnels are set up to a primary Hub

FlexVPN Backup

IKE Backup Peers (2)



FlexVPN Backup

IKE Backup Peers (3) – Spoke Config.

Also works with Routing Protocol

```
aaa authorization network default local

crypto ikev2 profile default
 match certificate HUBMAP
 identity local fqdn Spoke1.cisco.com
 authentication remote rsa-sig
 authentication local pre-shared
 keyring local
 pki trustpoint CA
 aaa authorization group cert list default default
 dpd 30 2 on-demand

crypto ikev2 client flexvpn default
 client connect tunnel 0
 peer 1 172.16.1.254
 peer 2 172.16.1.253

interface Tunnel0
 ip address negotiated
 tunnel source FastEthernet0/0
 tunnel destination dynamic
 tunnel protection ipsec profile default
```

Detect Hub Failure

To Primary Hub

To Secondary Hub

Destination managed by FlexVPN

Powerful Peer Syntax

```
peer <n> <ip>
peer <n> <ip> track <x>
peer <n> <fqdn>
peer <n> <fqdn> track <x>
```

Nth source selected only if corresponding track object is up

RADIUS Backup List Attribute

```
ipsec:ipsec-backup-gateway
```

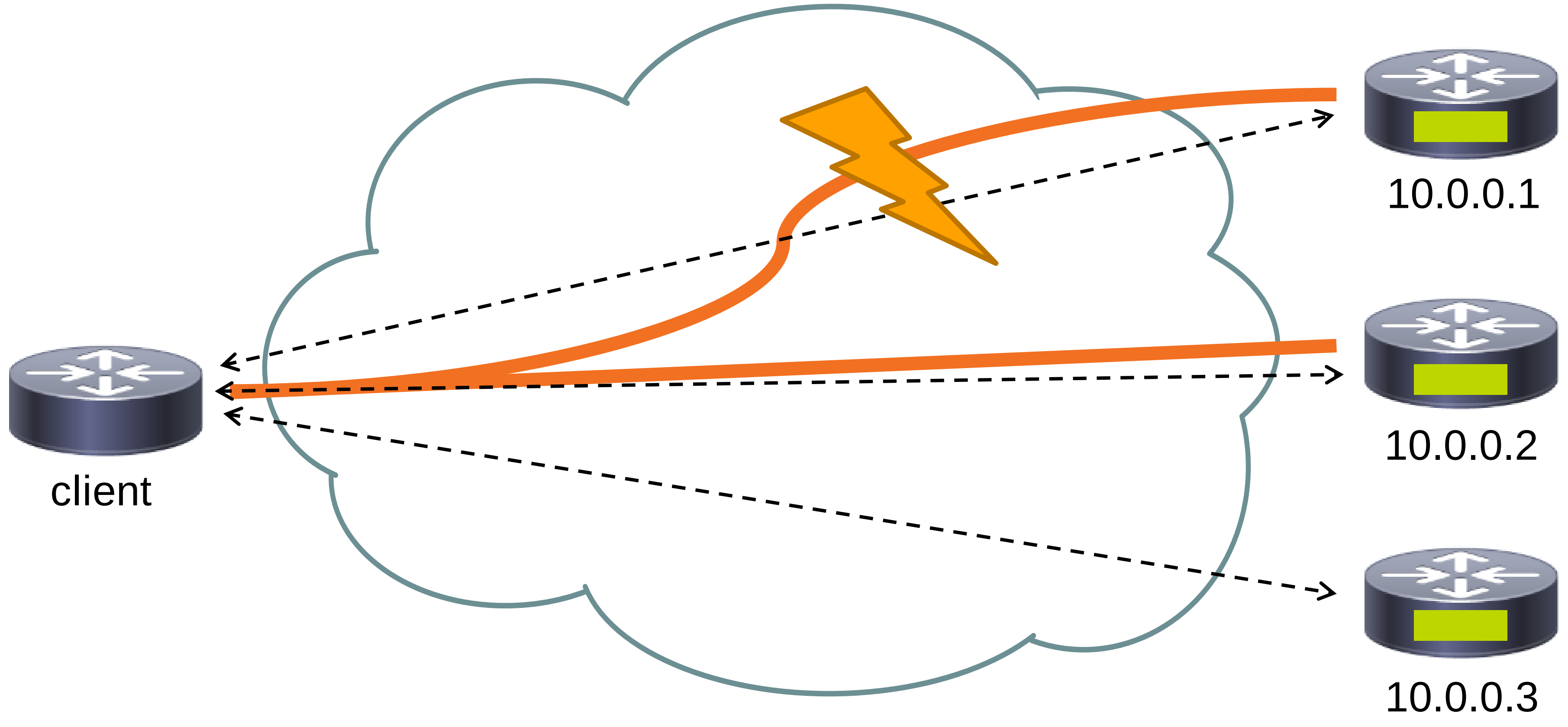
Up to 10 backup gateways pushed by config-exchange

```
crypto ikev2 authorization policy default
 route set interface
 route set access-list 99
```

Cisco live!

FlexVPN Backup – Re-activation of Primary Peer

- Allow re-establishing tunnel directly to preferred peer as soon as it is available again
- **Trackers are required for this feature**



🟩🟥 Tracker state (Up/Down)

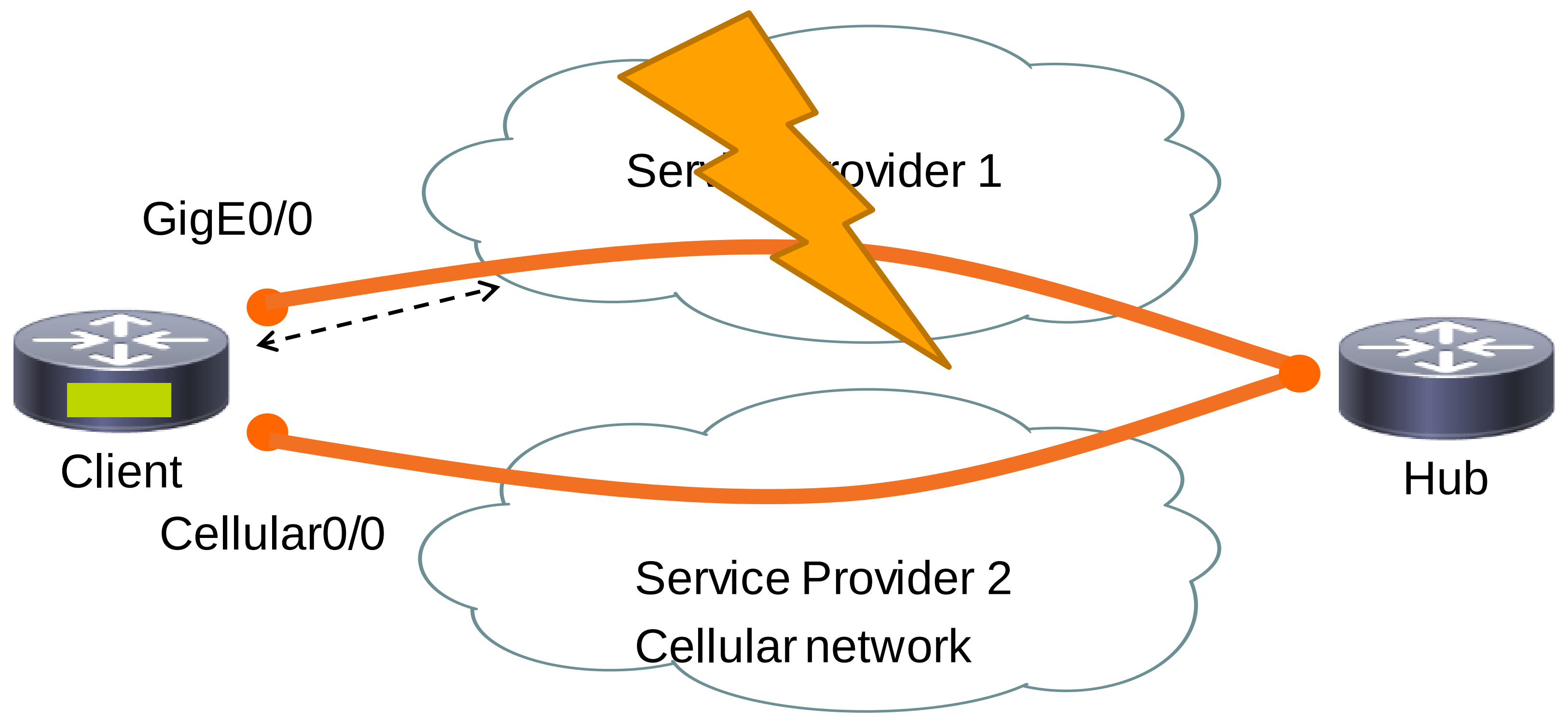
<- - -> ICMP-echo IP SLA probe

━ IPsec Tunnel

```
track 1 ip sla 1 reachability
track 2 ip sla 2 reachability
track 3 ip sla 3 reachability
!
crypto ikev2 flexvpn client remote1
  peer 1 10.0.0.1 track 1
  peer 2 10.0.0.2 track 2
  peer 3 10.0.0.3 track 3
  peer reactivate
  client connect Tunnel0
!
interface Tunnel0
  ip address negotiated
  …
  tunnel destination dynamic
  …
```

FlexVPN Backup – Tunnel Pivoting

- Use when different Service Providers are used to connect to remote host



🟩🟥 Tracker state (Up/Down)

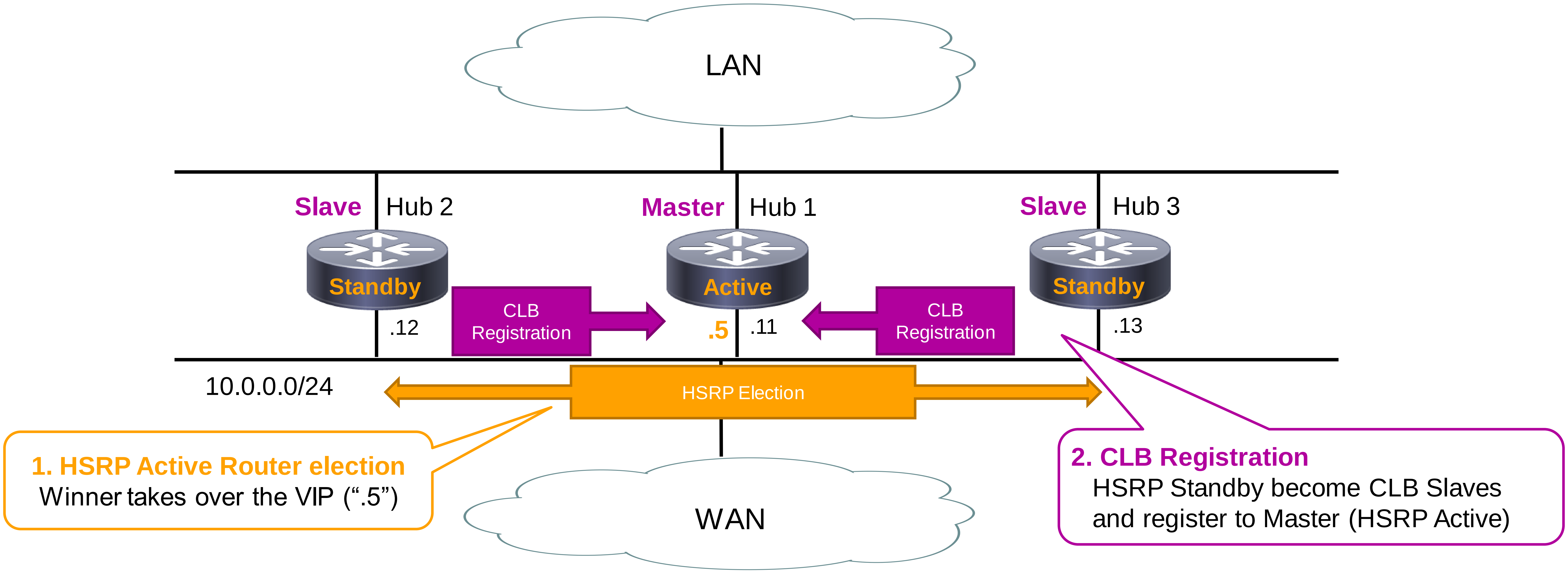
<- - -> ICMP-echo IP SLA probe

▬ IPsec Tunnel

```
track 1 ip sla 1 reachability

crypto ikev2 flexvpn client remote1
  peer 10.0.0.1
  source 1 interface GigabitEthernet0/0 track 1
  source 2 interface Cellular0/0
  client connect tunnel 0

interface Tunnel0
   ip address negotiated
   …
   tunnel source dynamic
   tunnel destination dynamic
   …
```

FlexVPN Backup

IKEv2 Load-Balancer Client Connection



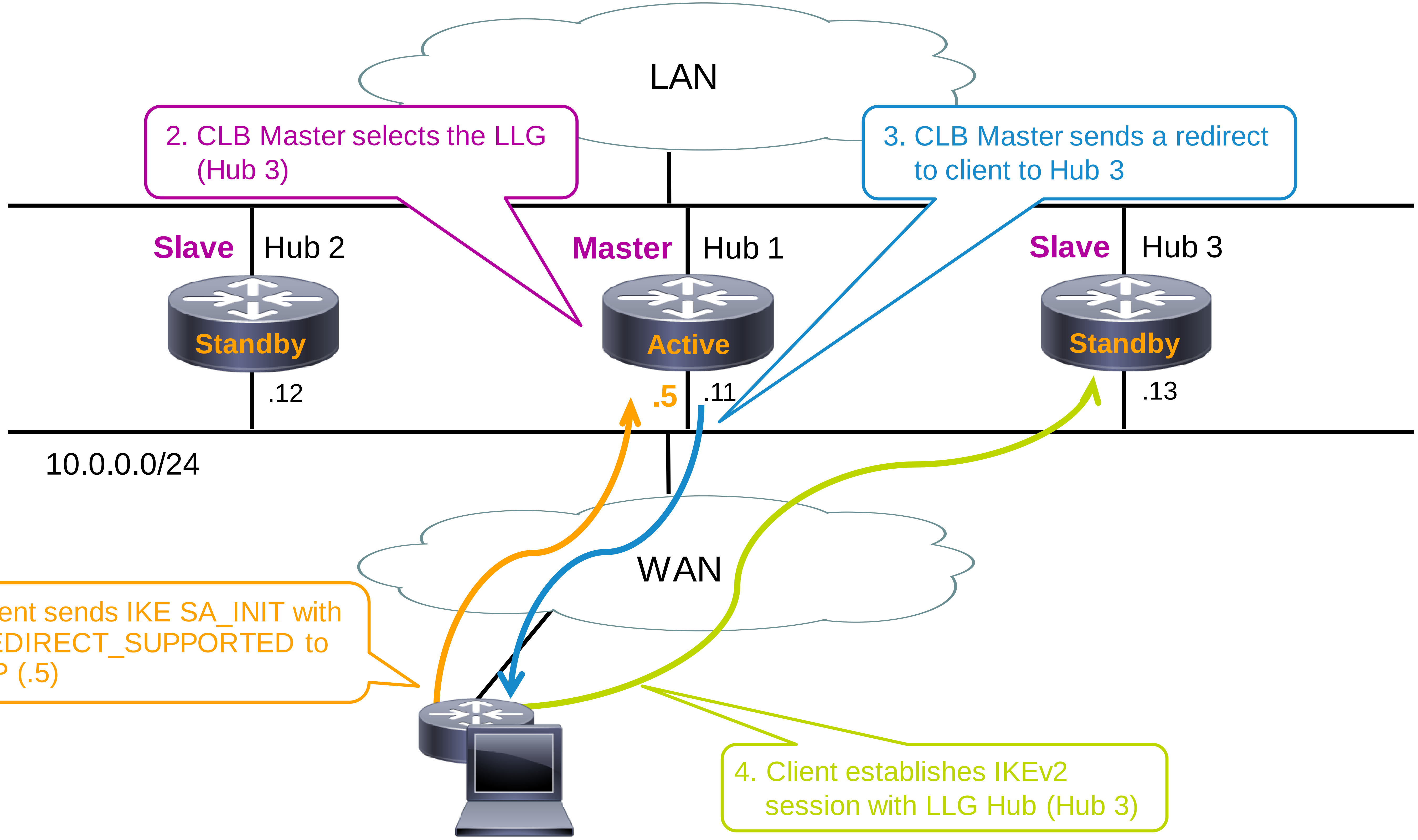
1. HSRP Active Router election
Winner takes over the VIP (".5")

2. CLB Registration
HSRP Standby become CLB Slaves and register to Master (HSRP Active)

```
On Hub 1:
*Nov 20 12:43:58.488: %CLB-6-CLB_SLAVE_CONNECTED: Slave 10.0.0.13 connected.
*Nov 20 12:43:58.493: %CLB-6-CLB_SLAVE_CONNECTED: Slave 10.0.0.12 connected.
```

FlexVPN Backup

IKEv2 Load-Balancer Client Connection



2. CLB Master selects the LLG (Hub 3)

3. CLB Master sends a redirect to client to Hub 3

1. Client sends IKE SA_INIT with REDIRECT_SUPPORTED to VIP (.5)

4. Client establishes IKEv2 session with LLG Hub (Hub 3)

IKEv2 Load-Balancer

Hub 1 Configuration

For your reference

```
crypto ikev2 redirect gateway init
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Hub1.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint TP
 dpd 10 2 on-demand
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ikev2 authorization policy default
 route set interface
!
crypto ikev2 cluster
 standby-group vpngw
 slave max-session 10
 no shutdown
```

Activates the sending of IKEv2 redirects during SA_INIT

```
!
interface Ethernet0/0
 ip address 10.0.0.11 255.255.255.0
 standby 1 ip 10.0.0.5
 standby 1 name vpngw
!
interface Loopback0
 ip address 172.16.1.11 255.255.255.0
!
interface Virtual-Template1 type tunnel
ip unnumbered Loopback0
ip mtu 1400
tunnel source Ethernet1/0
tunnel protection ipsec profile default
```

HSRP Group Name must match IKEv2 Cluster configuration

- Configuration of slave hubs is almost identical (except HSRP priority)!

IKEv2 Load-Balancer

Client Configuration

For your reference

```
crypto ikev2 authorization policy default
 route set interface
!
crypto ikev2 redirect client max-redirects 10
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Spoke2.cisco.com
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint TP
 dpd 10 2 on-demand
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ikev2 client flexvpn VPN_LB
 peer 1 10.0.0.5
 client connect Tunnel0
```

Activates IKEv2 redirection support and limit redirect count (DoS prevention)

```
interface Tunnel0
  ip address 172.16.1.100 255.255.255.0
  ip mtu 1400
  tunnel source Ethernet0/0
  tunnel destination dynamic
  tunnel protection ipsec profile default
```

FlexVPN Peer configured with the VIP address **only**

FlexVPN IKEv2 Remote Access

Anywhere, Any Device Access

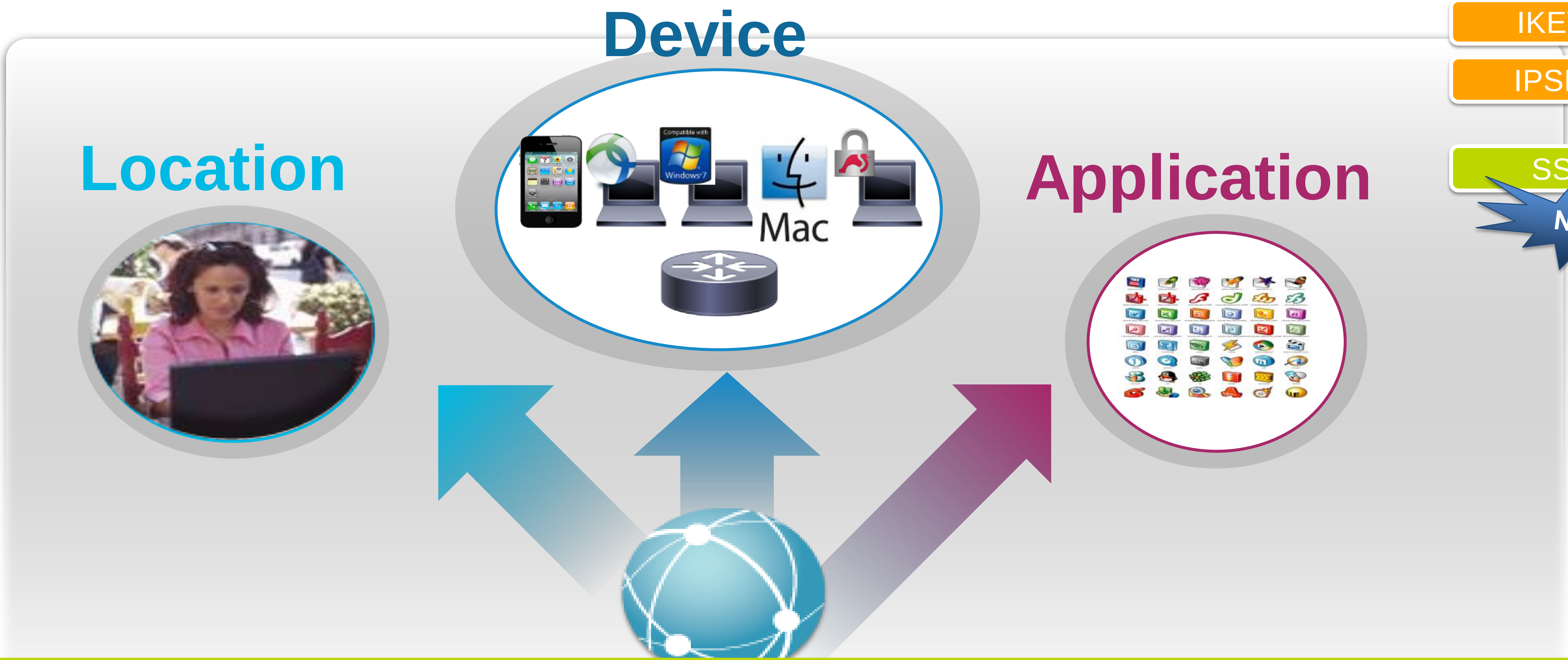
FlexVPN Framework

IKEV2

IPSEC

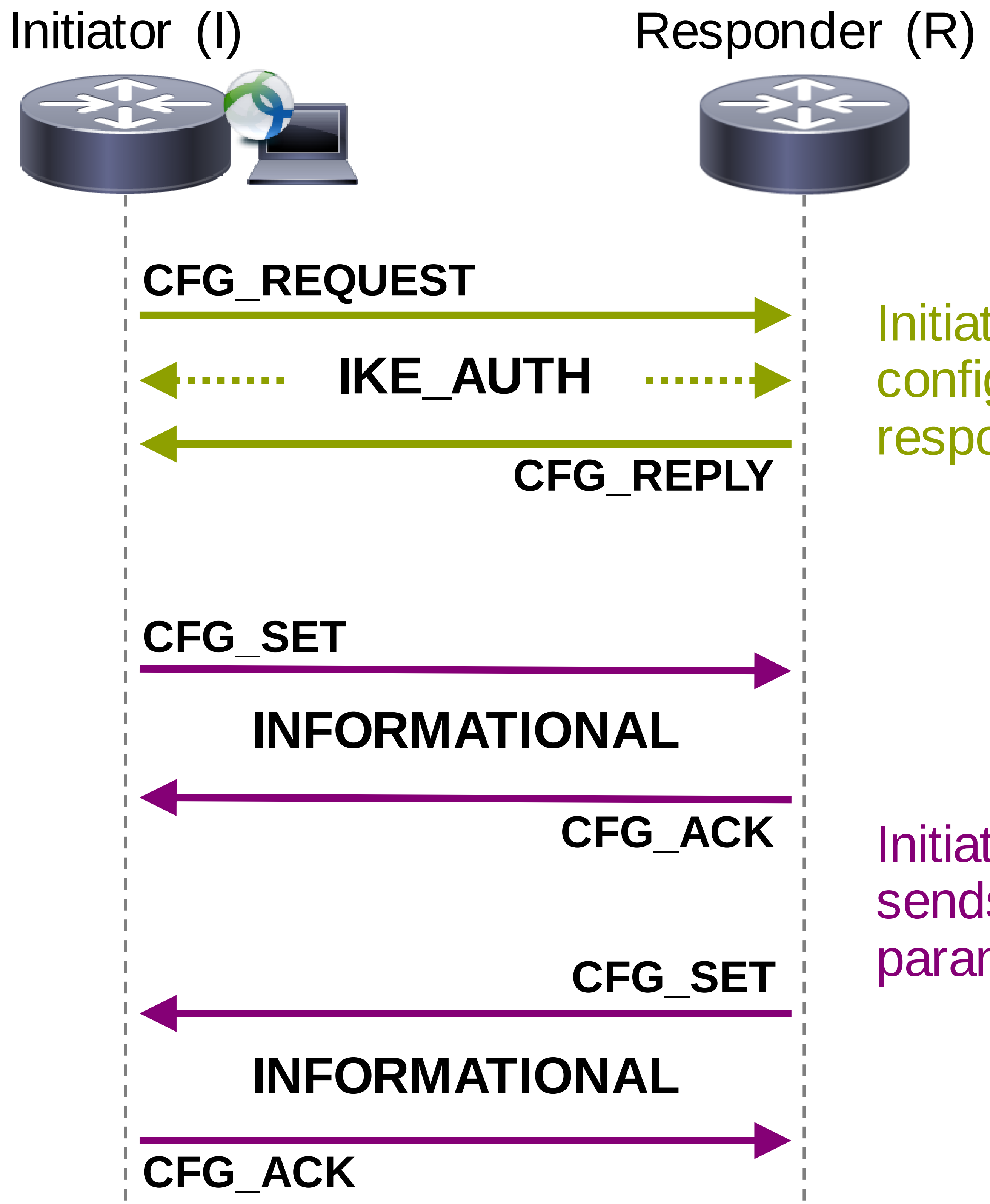
SSL

New !



More Diverse Users, Working from More Places, Using More Devices, Accessing More Diverse Applications, and Passing Sensitive Data

IKEv2 Configuration Exchange



Initiator (I)

Responder (R)

CFG_REQUEST

IKE_AUTH

CFG_REPLY

CFG_SET

INFORMATIONAL

CFG_ACK

CFG_SET

INFORMATIONAL

CFG_ACK

Initiator (RA client) requests configuration parameters from responder (RA server).

Initiator and/or responder sends unsolicited configuration parameters to its peer.

I would like:

- ✓ an IPv6 address
- ✓ a DNS & WINS server
- ✓ a list of IPv6 protected subnets

- ✓ Your assigned IPv6 address is ...
- ✓ Your DNS server is ...
- ✗ There is no WINS server
- ✓ The protected subnets are ...

Derived from peer authorisation

Derived from peer authorisation

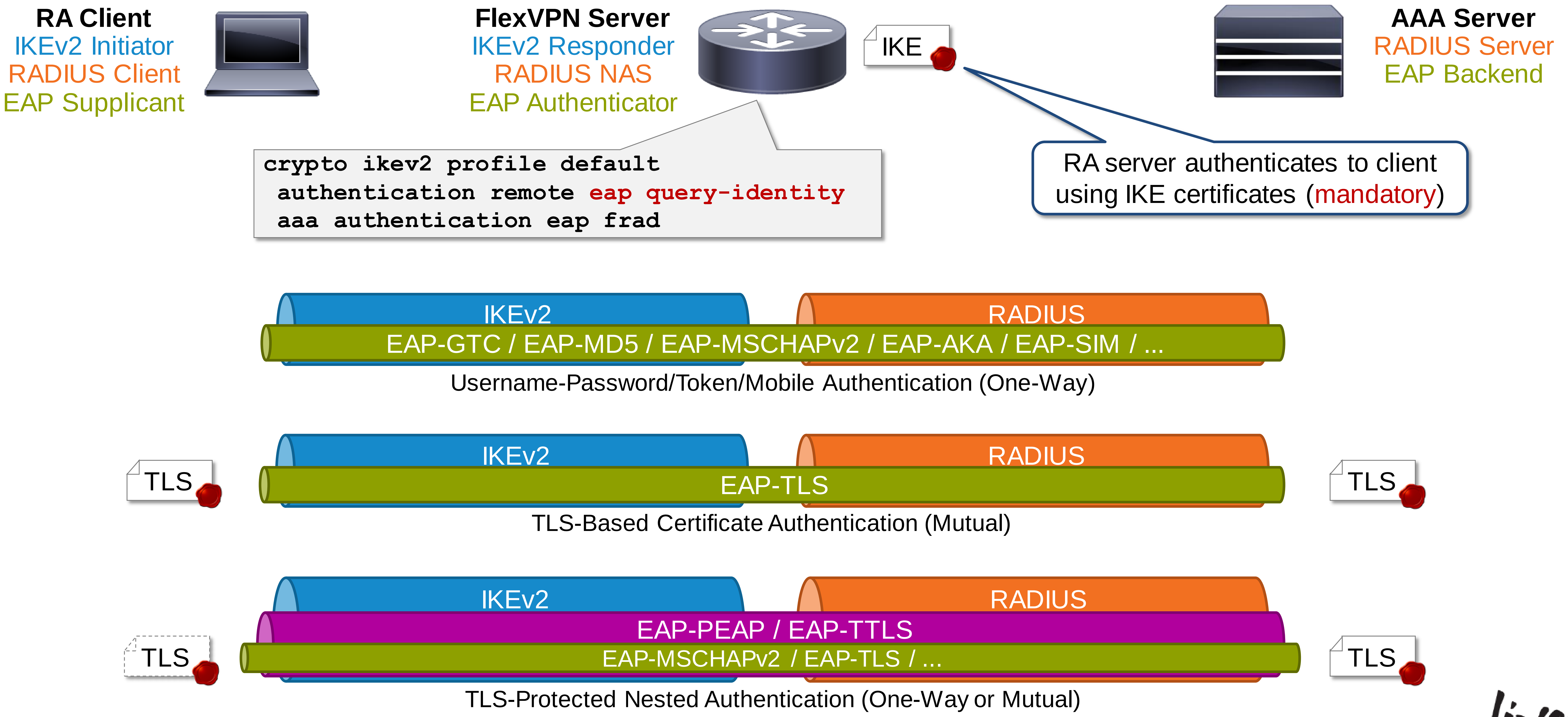
- ✓ My local IPv6 address is ...
- ✓ My local IPv6 protected subnets are ...

- ✓ Acknowledged

Extensible Authentication Protocol (EAP)

- No X-AUTH in IKEv2; EAP instead
- EAP – A General protocol for authentication that support multiple methods:
  - Tunnelling: EAP-TLS, EAP/PSK, EAP-PEAP, …
  - Non-tunnelling (recommended): EAP-MS-CHAPv2, EAP-GTC, EAP-MD5, …
- Implemented as additional IKE_AUTH exchanges
- Only used to authenticate initiator to responder
- Responder **MUST authenticate using certificates**
- Can severely increase number of messages (12-16)
- EAP comes with many caveats – refer to documentation !!

EAP Authentication



```
crypto ikev2 profile default
 authentication remote eap query-identity
 aaa authentication eap frad
```

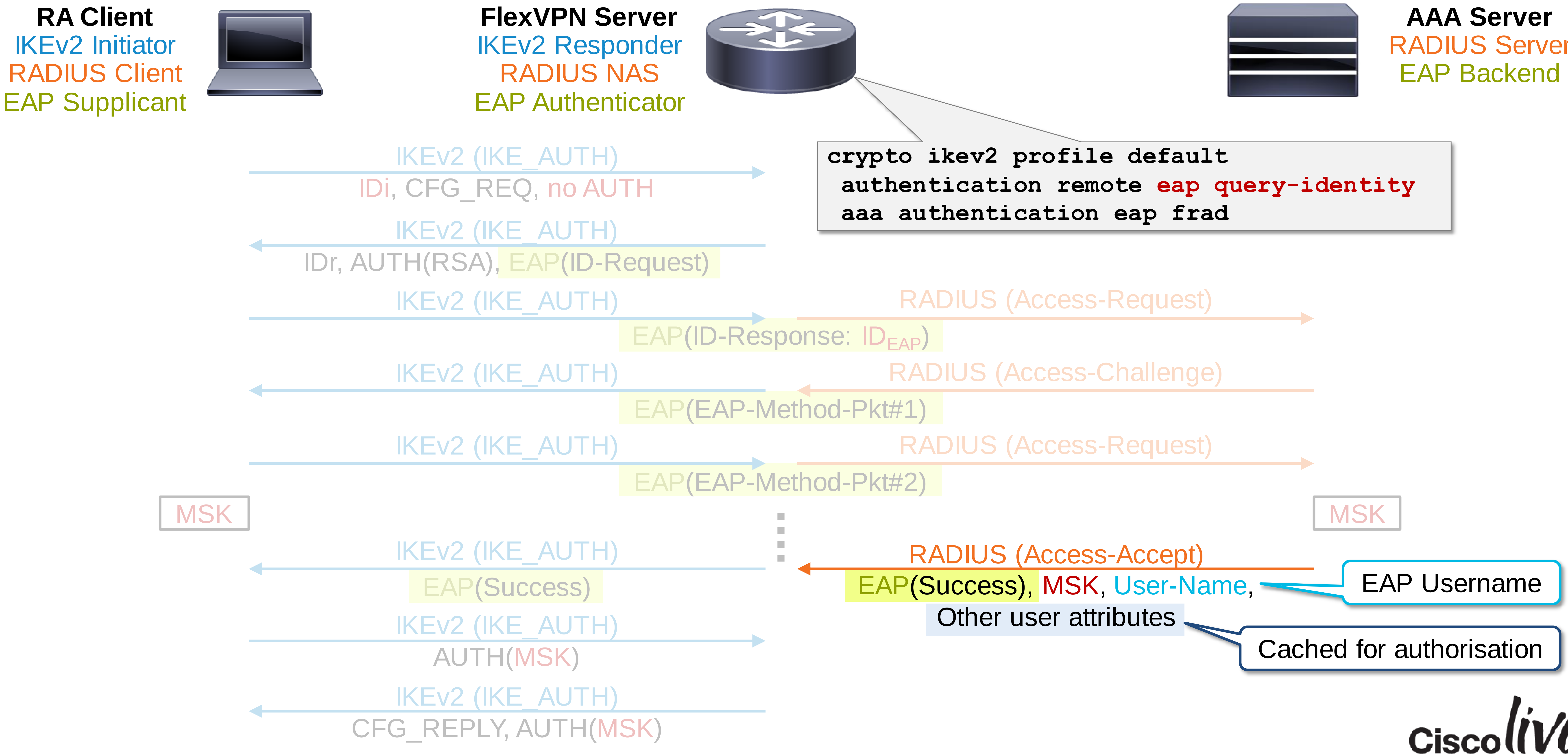
RA server authenticates to client using IKE certificates (mandatory)

Username-Password/Token/Mobile Authentication (One-Way)

TLS-Based Certificate Authentication (Mutual)

TLS-Protected Nested Authentication (One-Way or Mutual)

EAP Authentication – Packet Flow



RA Client
IKEv2 Initiator
RADIUS Client
EAP Supplicant

FlexVPN Server
IKEv2 Responder
RADIUS NAS
EAP Authenticator

AAA Server
RADIUS Server
EAP Backend

```
crypto ikev2 profile default
 authentication remote eap query-identity
 aaa authentication eap frad
```

IKEv2 (IKE_AUTH)
IDi, CFG_REQ, no AUTH

IKEv2 (IKE_AUTH)
IDr, AUTH(RSA), EAP(ID-Request)

IKEv2 (IKE_AUTH) — RADIUS (Access-Request)
EAP(ID-Response: ID_{EAP})

IKEv2 (IKE_AUTH) — RADIUS (Access-Challenge)
EAP(EAP-Method-Pkt#1)

IKEv2 (IKE_AUTH) — RADIUS (Access-Request)
EAP(EAP-Method-Pkt#2)

MSK — MSK

RADIUS (Access-Accept)
EAP(Success), MSK, User-Name, Other user attributes

EAP Username

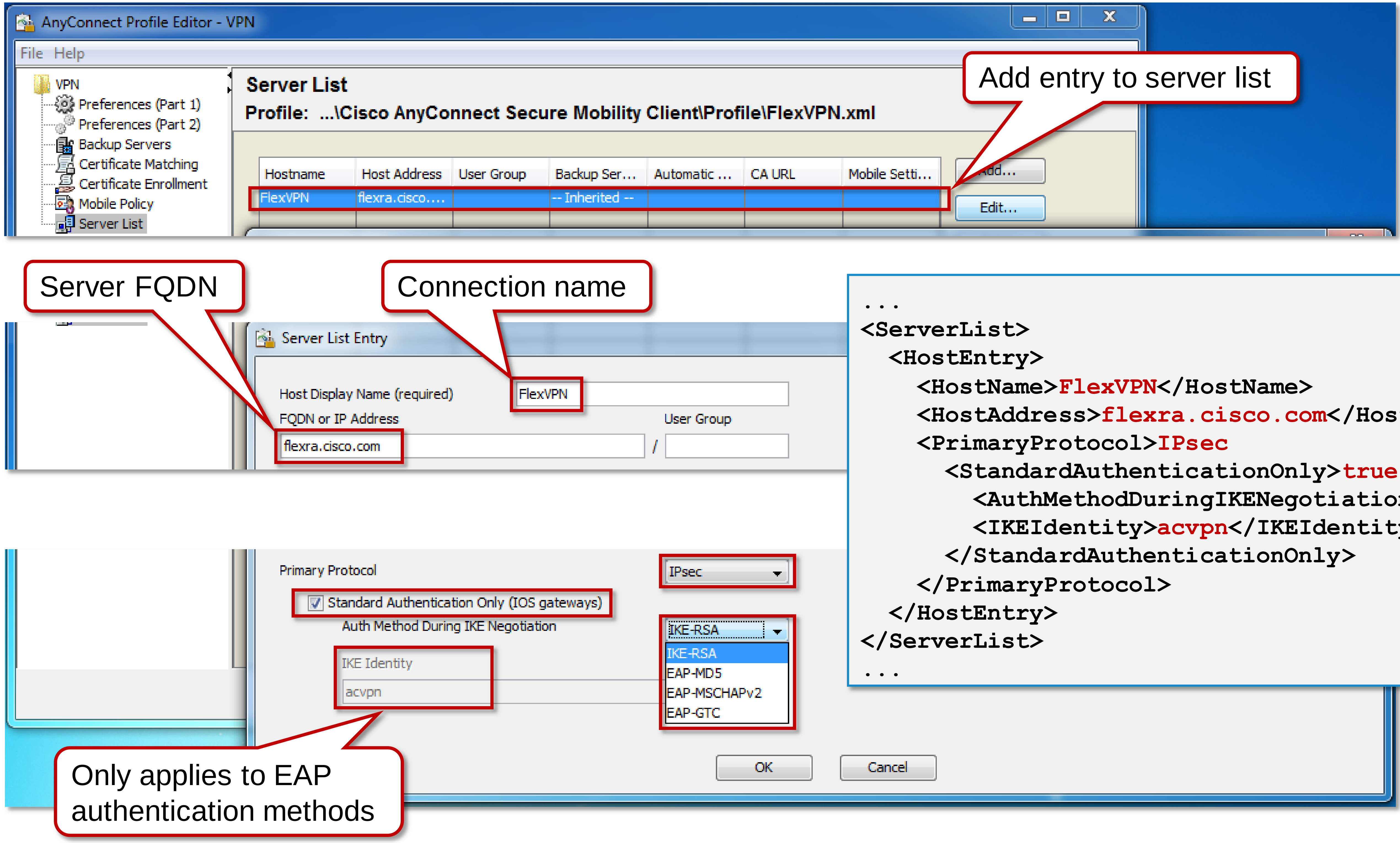
Cached for authorisation

IKEv2 (IKE_AUTH)
EAP(Success)

IKEv2 (IKE_AUTH)
AUTH(MSK)

IKEv2 (IKE_AUTH)
CFG_REPLY, AUTH(MSK)

AnyConnect – VPN Profile Editor



Server List

Profile: ...\Cisco AnyConnect Secure Mobility Client\Profile\FlexVPN.xml

Hostname	Host Address	User Group	Backup Ser...	Automatic ...	CA URL	Mobile Setti...
FlexVPN	flexra.cisco....		-- Inherited --			

Add entry to server list

Server FQDN

Connection name

Host Display Name (required): FlexVPN

FQDN or IP Address: flexra.cisco.com / User Group:

Primary Protocol: IPsec

☑ Standard Authentication Only (IOS gateways)

Auth Method During IKE Negotiation: IKE-RSA

- IKE-RSA
- EAP-MD5
- EAP-MSCHAPv2
- EAP-GTC

IKE Identity: acvpn

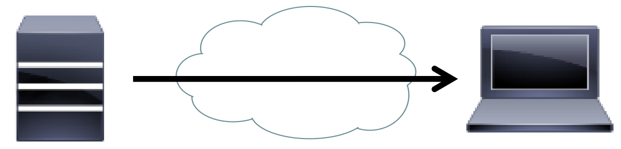
Only applies to EAP authentication methods

Resulting XML Profile

```
...
<ServerList>
  <HostEntry>
    <HostName>FlexVPN</HostName>
    <HostAddress>flexra.cisco.com</HostAddress>
    <PrimaryProtocol>IPsec
      <StandardAuthenticationOnly>true
        <AuthMethodDuringIKENegotiation>EAP-GTC</AuthMethodDuringIKENegotiation>
        <IKEIdentity>acvpn</IKEIdentity>
      </StandardAuthenticationOnly>
    </PrimaryProtocol>
  </HostEntry>
</ServerList>
...
```

AnyConnect Desktop – Profile Deployment Options

Use a Software Management System



Add the profile to the AnyConnect package

Send the profile via email

Download the profile to the file system

OS	Default Location
Windows	`%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile`
Mac OS, Linux	`/opt/cisco/anyconnect/profile`

AnyConnect Mobile – Profile Deployment Options

Send the profile via email

XML

Install the profile via a URI handler

```
anyconnect://import?type=profile&uri=location
```

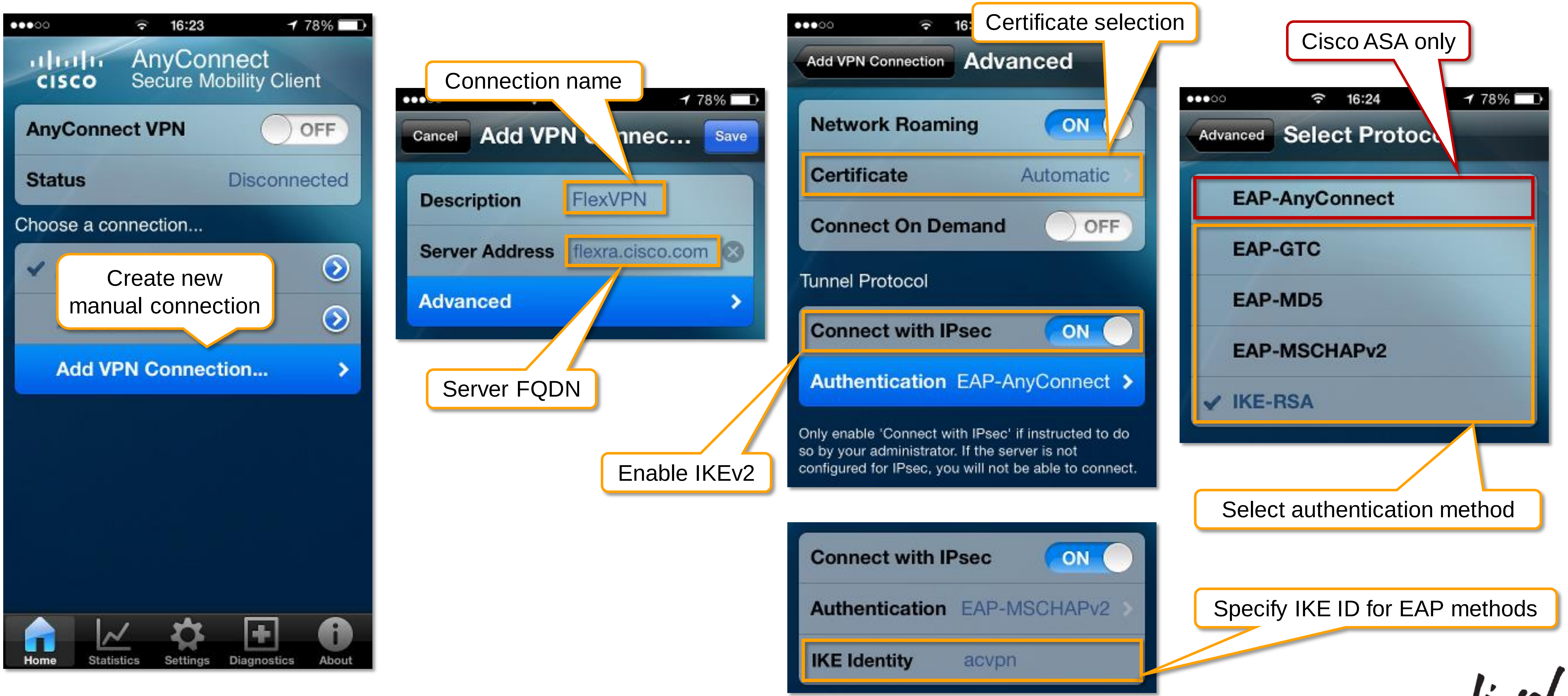
Example location: http://example.com/profile.xml

Import it from Local File system or URI

Manual Connection Creation

MDM (Mobile Device Management)

AnyConnect Mobile – Manual Connection



AnyConnect Secure Mobility Client

AnyConnect VPN: OFF

Status: Disconnected

Choose a connection...

Add VPN Connection...

Create new manual connection

Connection name

Add VPN Connection

Description: FlexVPN

Server Address: flexra.cisco.com

Advanced

Server FQDN

Certificate selection

Advanced

Network Roaming: ON

Certificate: Automatic

Connect On Demand: OFF

Tunnel Protocol

Connect with IPsec: ON

Authentication: EAP-AnyConnect

Only enable 'Connect with IPsec' if instructed to do so by your administrator. If the server is not configured for IPsec, you will not be able to connect.

Enable IKEv2

Cisco ASA only

Select Protocol

- EAP-AnyConnect
- EAP-GTC
- EAP-MD5
- EAP-MSCHAPv2
- ✓ IKE-RSA

Select authentication method

Connect with IPsec: ON

Authentication: EAP-MSCHAPv2

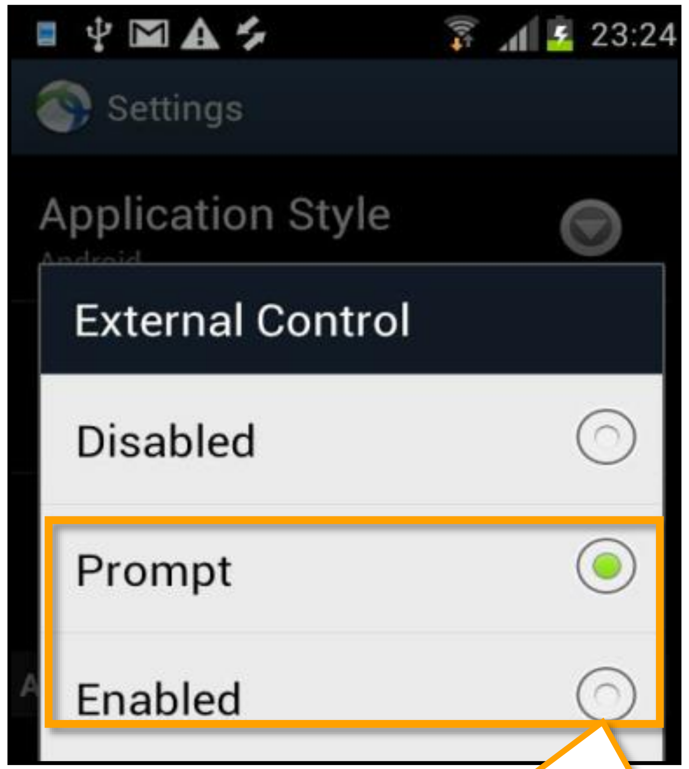
IKE Identity: acvpn

Specify IKE ID for EAP methods

AnyConnect Mobile – URI Handler Profile Deployment

- Import profiles, certificates, and create connection entries
- Apple iOS & Android
  - Import via URL, email, device storage
  - Also connect & disconnect VPN using URI Handler

```
anyconnect://create/?name=FlexVPN&host=flexra.cisco.com&protocol=IPsec&authentication=EAP-MD5&ike-identity=acvpn
```



Settings

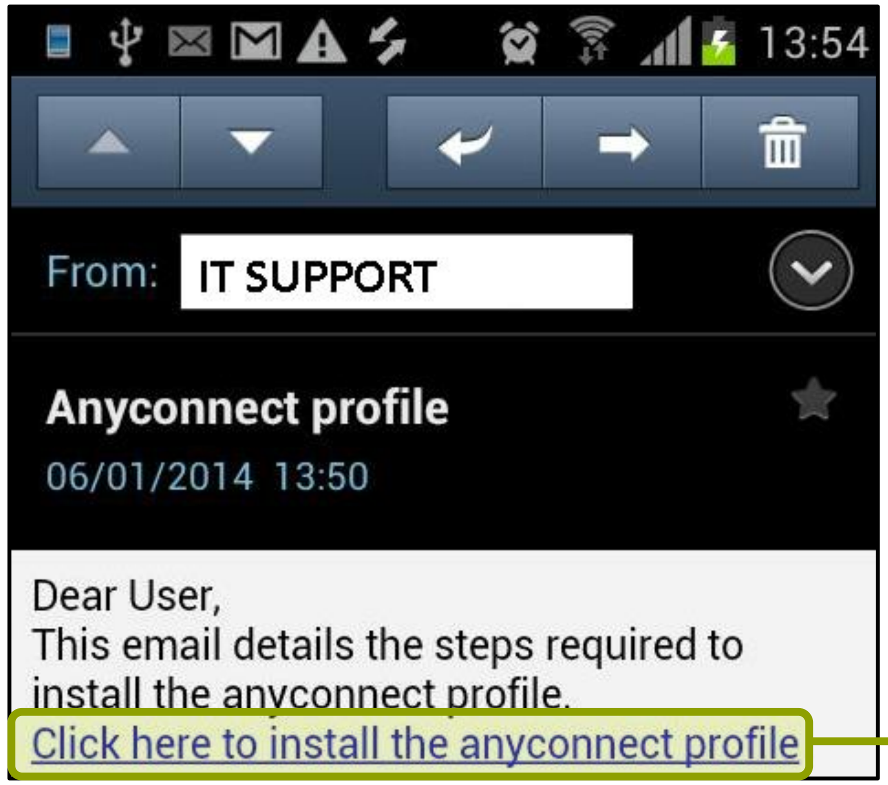
Application Style

Android

External Control

- Disabled ○
- Prompt ●
- Enabled ○

Prompt or Enabled - Required for URI Handler



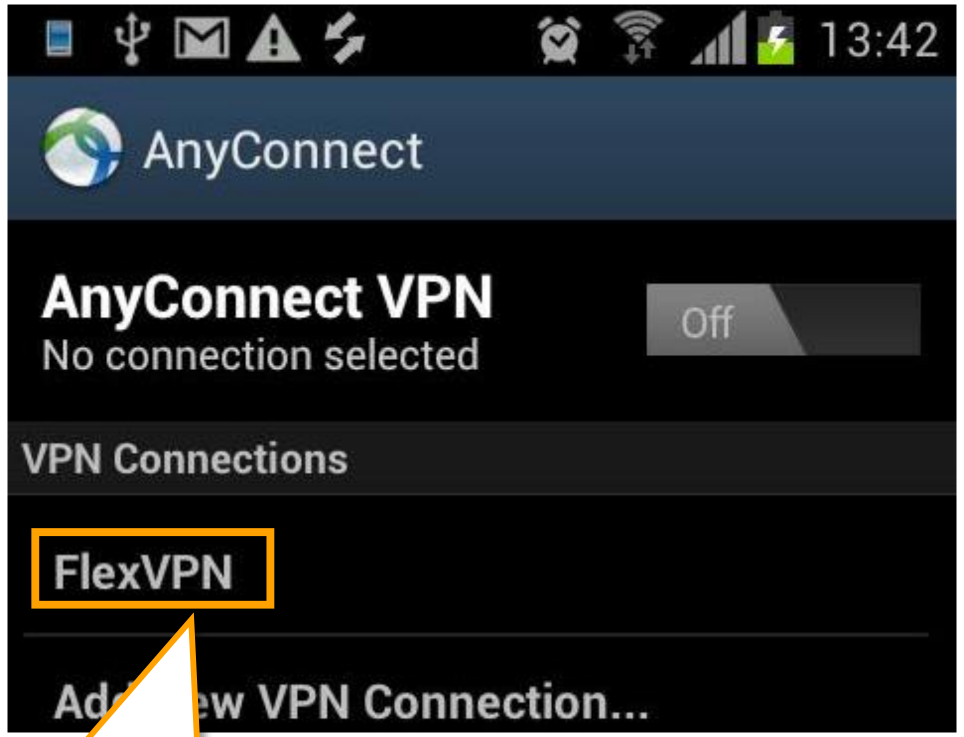
From: IT SUPPORT

Anyconnect profile

06/01/2014 13:50

Dear User,
This email details the steps required to install the anyconnect profile.

Click here to install the anyconnect profile



AnyConnect

AnyConnect VPN
No connection selected
Off

VPN Connections

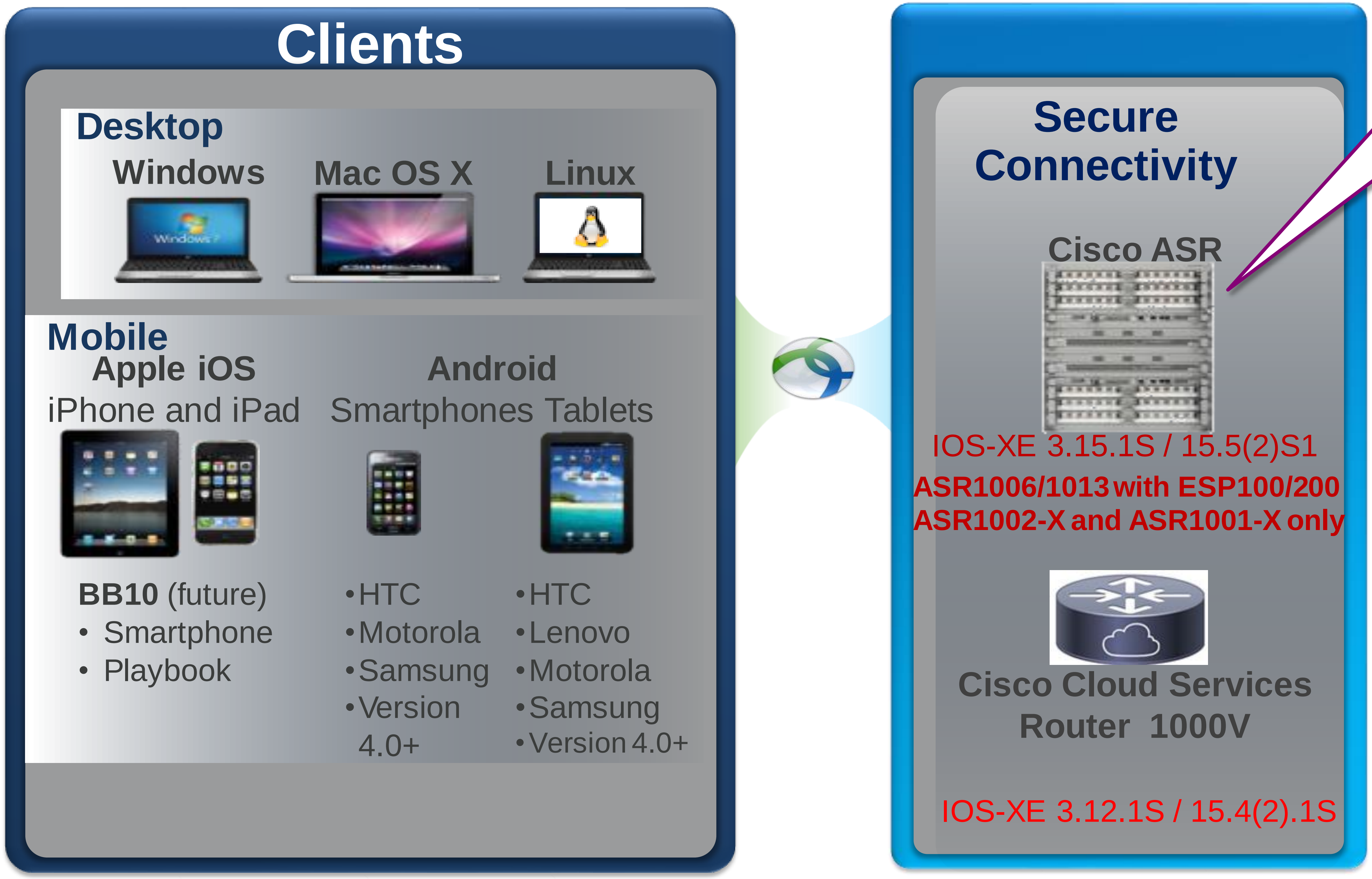
FlexVPN

Add new VPN Connection...

Connection successfully created

FlexVPN SSL

FlexVPN SSL Overview



Clients

Desktop

Windows **Mac OS X** **Linux**

Mobile

Apple iOS
iPhone and iPad

Android
Smartphones Tablets

BB10 (future)
- Smartphone
- Playbook

- HTC
- Motorola
- Samsung
- Version 4.0+

- HTC
- Lenovo
- Motorola
- Samsung
- Version 4.0+

Secure Connectivity

Cisco ASR

IOS-XE 3.15.1S / 15.5(2)S1

ASR1006/1013 with ESP100/200 ASR1002-X and ASR1001-X only

Cisco Cloud Services Router 1000V

IOS-XE 3.12.1S / 15.4(2).1S

Tentative date – June 2015

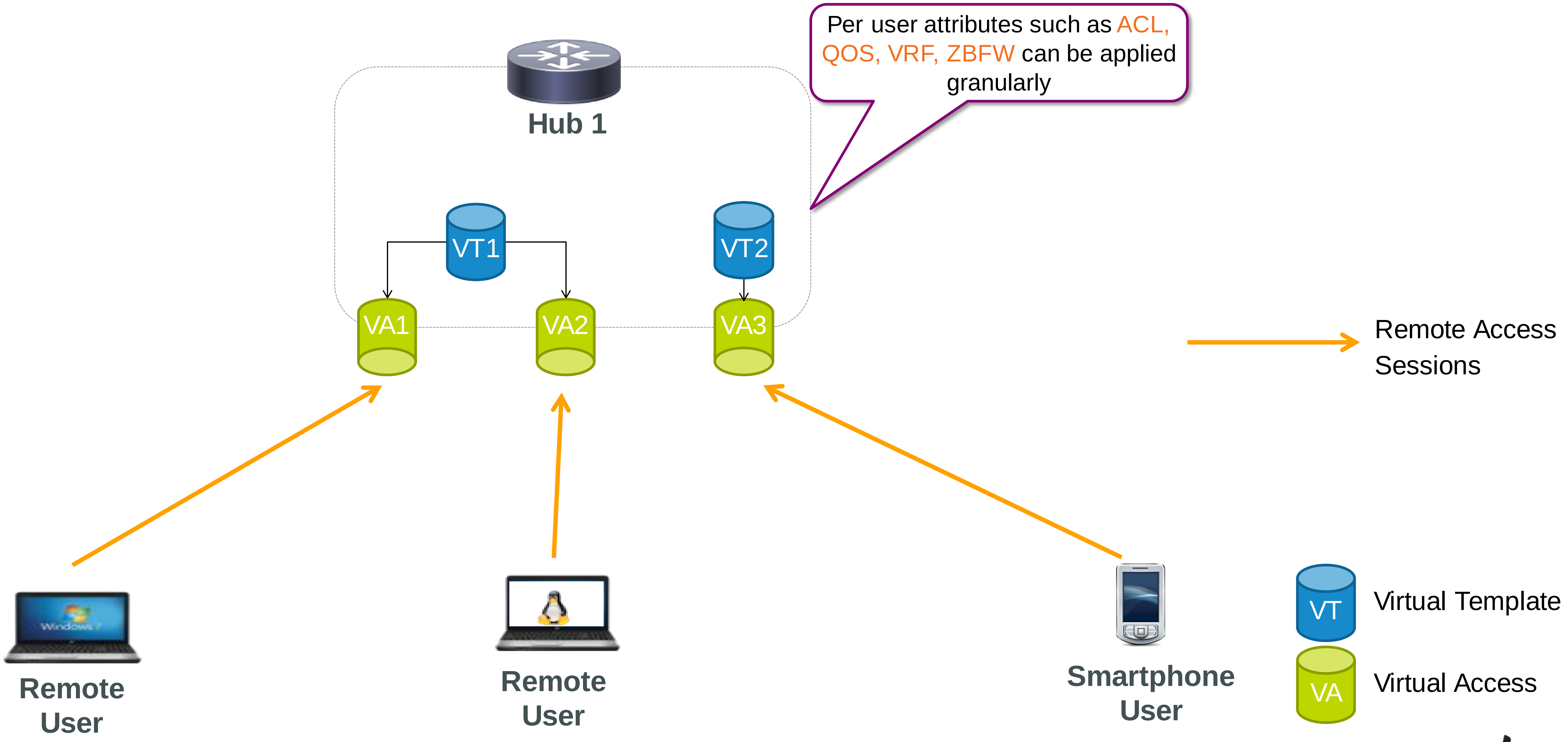
- First release of SSLVPN support (on ASR / CSR)
- Client-based only (AnyConnect)
  - No clientless support
- Integrated into FlexVPN framework
  - AAA integration
  - Virtual tunnel interfaces
  - Smart defaults
  - CLI consistency
- ASR not supported on previous ESP (ESP 2.5 up to 40 due to lack of crypto engine support)

Features Not Supported In Initial Release

Slated for Future Releases

- Automatic anyconnect software upgrade from headend
- Web Launch for anyconnect (from browser)
- Client side certificates
- Hostscan and Posture
- Name mangler
- Two-Factor & Double Authentication
- IPv6 Mixed-Mode / Dual-Stack
- DTLS

FlexVPN SSL and Interfaces



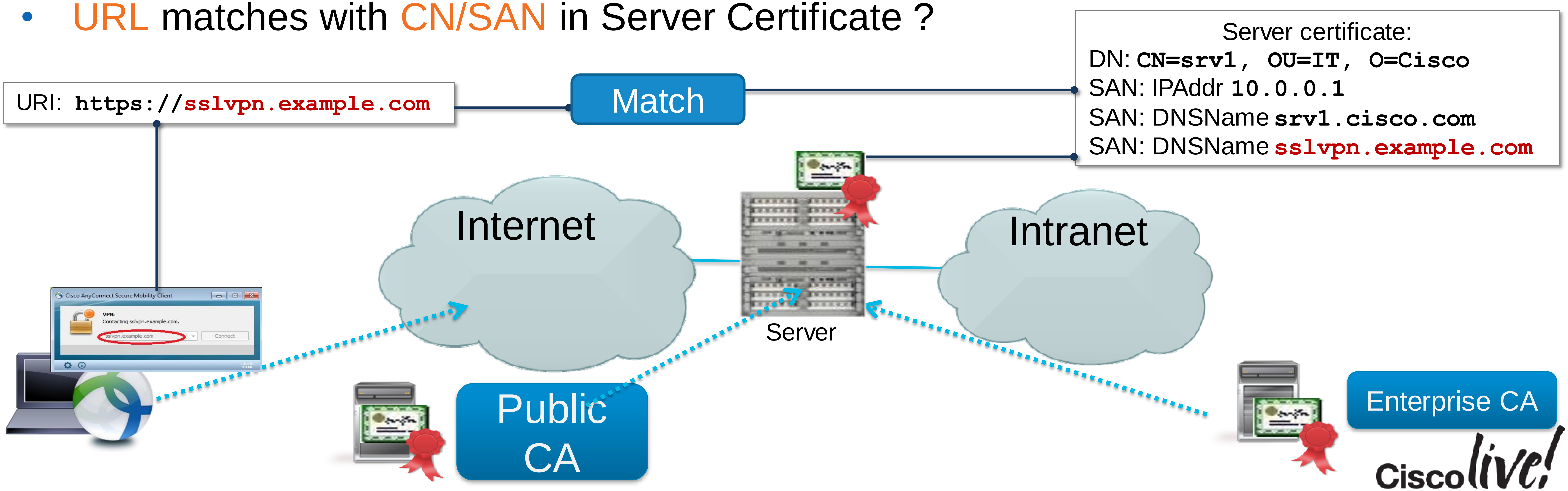
Per user attributes such as ACL, QOS, VRF, ZBFW can be applied granularly

SSL and Certificates: Server Certificate Validation

- Router certificate should be trusted by clients
  - Public (well-known) Certificate Authority (e.g. Verisign)
  - Enterprise Certificate Authority, e.g. Microsoft AD
  - Self-Signed (need to import certificate to all clients)

Prevents man-in-the-middle attacks

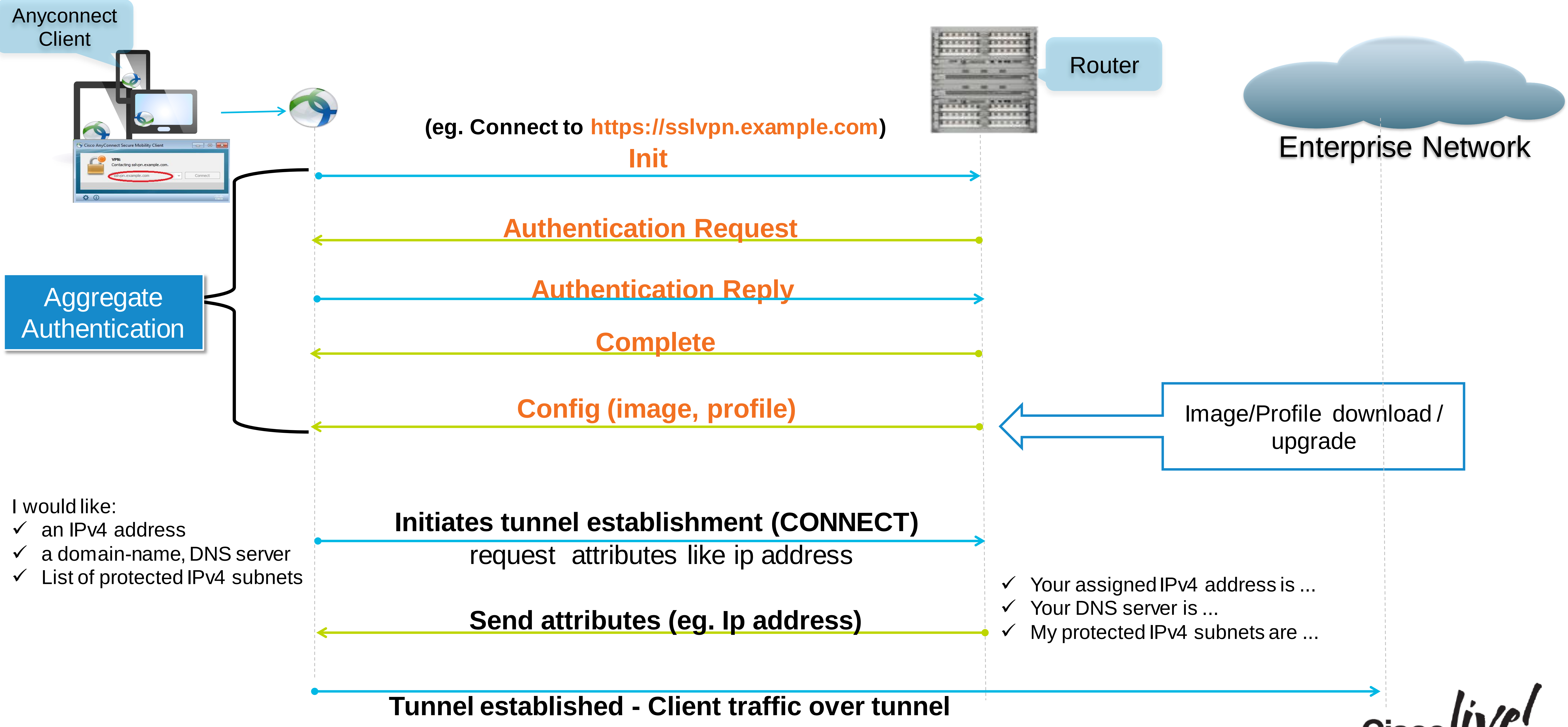
- Has the certificate expired or revoked **(OCSP or CRL)?**
- URL matches with CN/SAN in Server Certificate ?



URI: **https://sslvpn.example.com**

Server certificate:
DN: **CN=srv1, OU=IT, O=Cisco**
SAN: IPAddr **10.0.0.1**
SAN: DNSName **srv1.cisco.com**
SAN: DNSName **sslvpn.example.com**

Aggregate Authentication High level Flow



(eg. Connect to https://sslvpn.example.com)

Init

Authentication Request

Authentication Reply

Complete

Config (image, profile)

Image/Profile download / upgrade

I would like:
- ✓ an IPv4 address
- ✓ a domain-name, DNS server
- ✓ List of protected IPv4 subnets

Initiates tunnel establishment (CONNECT)

request attributes like ip address

- ✓ Your assigned IPv4 address is ...
- ✓ Your DNS server is ...
- ✓ My protected IPv4 subnets are ...

Send attributes (eg. Ip address)

Tunnel established - Client traffic over tunnel

FlexVPN SSL Configuration Example

```
crypto ssl proposal my-proposal
 protection rsa-aes128-sha1 rsa-aes256-sha1
```

- ✓ Cryptographic algorithms
- ✓ Key exchange method

```
crypto ssl policy my-policy
 ip interface GigabitEthernet0/0/0 port 443
 pki trustpoint my-cert sign
 ssl proposal my-proposal
 no shutdown
```

- ✓ Local endpoint matching criteria
- ✓ Apply SSL proposal
- ✓ Configure SSL server certificate

```
crypto ssl profile my-profile
 match policy my-policy
 match url https://sslvpn.example.com
 authentication remote user-pass
 aaa authentication user-pass list my-radius
 aaa authorization user user-pass cached
 virtual-template 1
 no shutdown
```

- ✓ Match on SSL policy
- ✓ Match on URL (FQDN, hostname, path, ...)
- ✓ Authentication (certificate, username/password)
- ✓ Authorisation (cached, user, group)
- ✓ Accounting
- ✓ Virtual interface template (ASR only)

CLI Experience: FlexVPN **IPsec** vs SSL

```
crypto ikev2 proposal prop-1
  encryption aes-cbc-128 3des
  integrity sha
  group 2
 !
 crypto ikev2 policy site-policy
   proposal prop-1
 !
crypto ikev2 authorization policy default
 pool mypool
 !
 crypto ikev2 profile v2-profile
  match identity remote address 10.0.1.1
  authentication local rsa-sig
  authentication remote rsa-sig
  pki trustpoint CA
  aaa authorization cert list default default
  virtual-template 1
 !
 interface Virtual-Template1 type tunnel
  ip unnumbered Loopback0
  tunnel source Ethernet0/0
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile ipsec-prof
```

Both use the FlexVPN CLI Framework

Minor differences unavoidable due to protocol differences IKE2 vs SSL

```
Crypto ssl proposal sslvpn1
 protection rsa-aes128-sha1 rsa-aes256-sha1
!


crypto ssl policy sslvpn1
 ssl proposal sslvpn1
 pki trustpoint SSLVPN sign
 ip address local 10.48.67.251 port 443
  !
crypto ssl authorization policy default
 pool mypool
  !
crypto ssl profile sslvpn1
 match policy sslvpn1
 match url https://flexssl.cisco.com
 aaa authentication user user-pass list SSLUSERS
 aaa authorization group user-pass list SSLAUTHOR
 authentication remote user-pass
 virtual-template 1
!
interface Virtual-Template1 type vpn
 ip unnumbered Loopback1
 ip mtu 1400
 ip nat inside
 vpn mode ssl
```

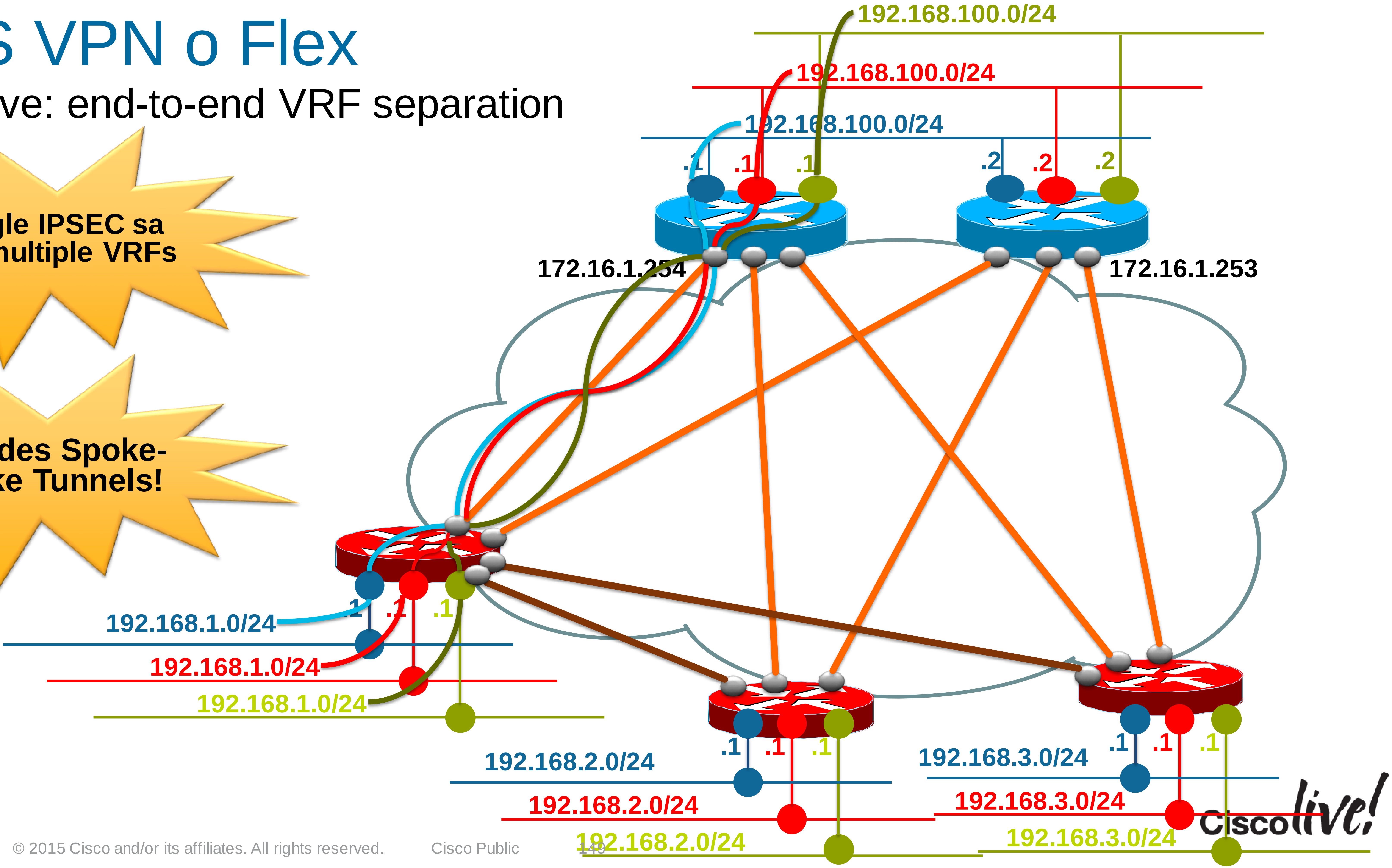
Advanced Features…

MPLS VPN o Flex

- Objective: end-to-end VRF separation

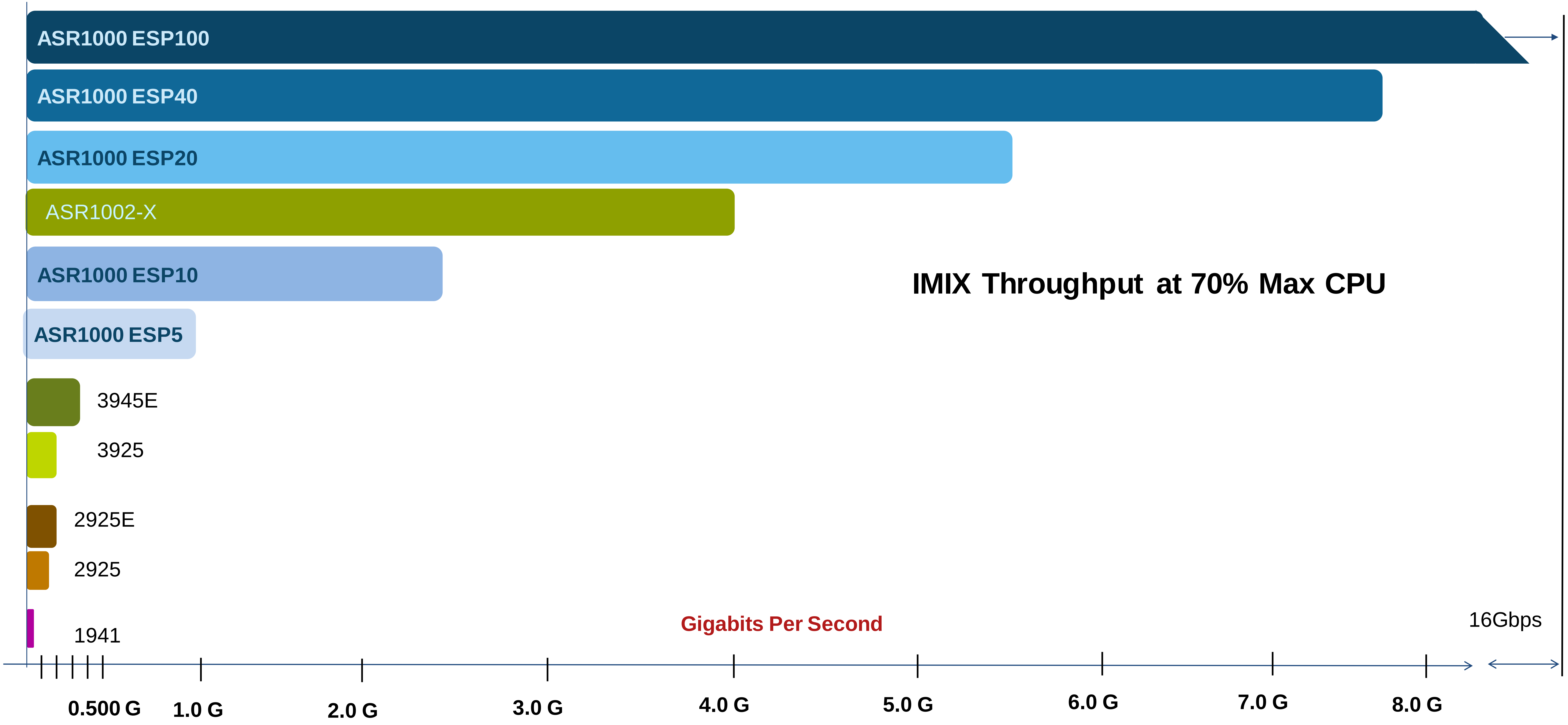
Single IPSEC sa
for multiple VRFs

Includes Spoke-
Spoke Tunnels!



Performances and Scalability

IPSec Forwarding Performance



Route Exchange Protocol Selection

Branch-Hub		Use case				
IKEv2 Recommended	Simple, large scale	Static (No redistribution IGP→IKE)	Simple branches (< 20 prefixes)	Identity-based route filtering	Lossy networks	High density hubs
BGP Recommended	Simple to complex, large scale	Dynamic (Redistribution IGP → BGP)	Complex branches (> 20 prefixes)	Powerful route filtering – not identity based	Lossy networks	High density hubs up to 350K routes
EIGRP not recommended at large scale	Simple to complex	Dynamic (Redistribution IGP → IGP)	Semi-complex branches (> 20 prefixes)	Intermediate route filtering – not identity based	Lossless networks (very rare)	< 5000 prefixes at hub

Hub-Hub	Use case		
BGP Recommended	Large amount of prefixes (up to 1M)	Road to scalability	Powerful route filtering
IGP (EIGRP, OSPF)	< 5000 prefixes total	Perceived simplicity	

Tentative

FlexVPN – High-end Scalability & Performances

Release 3.5+ w/out QoS	ISR 4451	ASR1001	ASR1000-ESP5	ASR1000-ESP10	ASR1000-ESP20	ASR1000-ESP40	ASR1000-ESP100
Throughput (Max / IMIX)	1.2 / 0.8Gbps	1.8 / 1Gbps	1.8 / 1 Gbps	4 / 2.5 Gbps	7 / 6 Gbps	11 / 7.4 Gbps	29 / 16 Gbps
Max tunnels (RP1 / RP2)	4000	4000	1000	1000 / 4000	1000 / 4000	1000 / 4000	-- / 4000
EIGRP neighbors	4000 (1000 recommended)	4000 (1000 recommended)	1000	1000 / 4000 (1000 recommended)	1000 / 4000 (1000 recommended)	1000 / 4000 (1000 recommended)	-- / 4000 (1000 recommended)
BGP neighbors	**4000**	**4000**	**1000**	**1000 / 4000**	**1000 / 4000**	**1000 / 4000**	**-- / 4000**

Bumping from 4,000 to 10,000 spokes/hub with FlexVPN in 3.12 (RP2, ESP10 & above)

Release 3.10 w/ QoS	ISR 4451	ASR1001	ASR1000-ESP20	ASR1000-ESP40
Throughput (Max / IMIX)	1.2/0.8 Gbps	1.8 / 1Gbps	7 / 6 Gbps	11 / 7.4 Gbps
Max tunnels (RP2 only)	2000	4000* (16K Queues)	4000 (128K Queues)	4000 (128K Queues)

High-End Scalability & Performances – 3.12+

Tentative

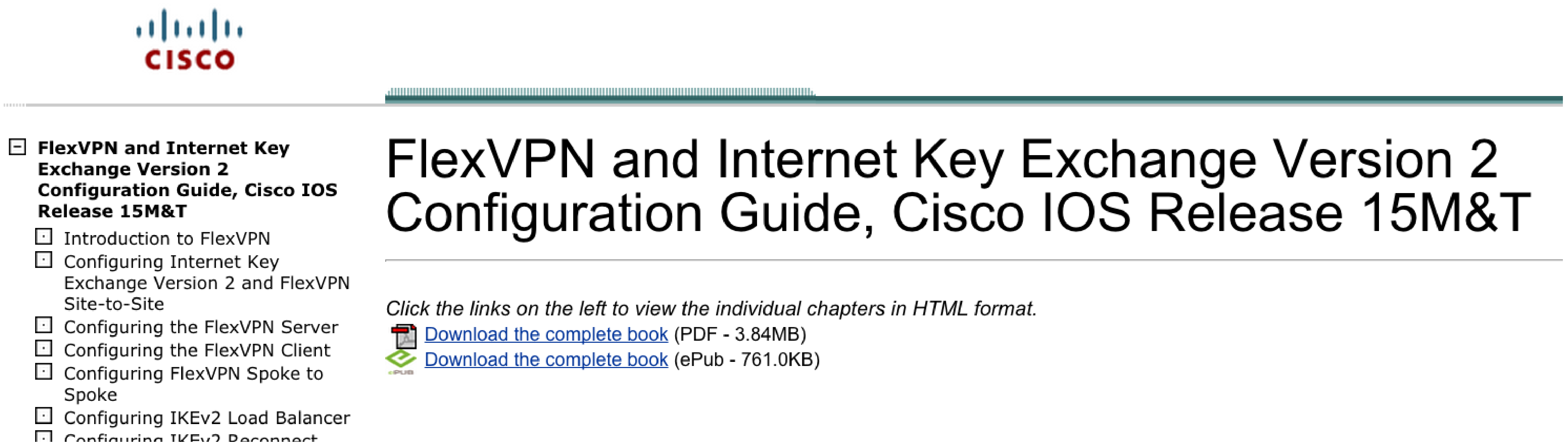
3.12+ w/out QoS	ISR 4451	ASR 1001	ASR 1001-X	ASR 1002-X	ASR 1000 ESP5	ASR 1000 ESP10	ASR 1000 ESP20	ASR 1000 ESP40	ASR 1000 ESP100	ASR 1000 ESP200
Throughput (Max / IMIX)	1.2 / 0.8Gbps	1.8 / 1 Gbps	1.8 / 1 Gbps	4 / 4 Gbps	1.8 / 1 Gbps	4 / 2.5 Gbps	7 / 6 Gbps	11 / 7.4 Gbps	29 / 16 Gbps	59 / 78 Gbps
Max tunnels (RP2)	2,000	4,000	4,000	**10,000**	4,000 RP1: 1,000	4,000 RP1: 1,000	**10,000** RP1: 1,000	**10,000**	**10,000**	**10,000**
EIGRP neighbours	2,000 1000 recommended	4,000 1000 recommended	4,000 1000 recommended	4,000 1000 recommended	4,000 1000 recommended	4,000 1000 recommended	4,000 1000 recommended	4,000 1000 recommended	4,000 1000 recommended	4,000 1000 recommended
IKE Routing	2,000	4,000	4,000	**10,000**	4,000	4,000	**10,000**	**10,000**	**10,000**	**10,000**
BGP neighbours	2,000	4,000	4,000	**10,000**	4,000	4,000	**10,000**	**10,000**	**10,000**	**10,000**
QoS	10% crypto throughput decrease	16K Q No crypto impact	16K Q No crypto impact	128K Q No crypto impact	128K Q No crypto impact	128K Q No crypto impact	128K Q No crypto impact	128K Q No crypto impact	128K Q No crypto impact	128K Q No crypto impact

Bumping from 4,000 to 10,000 spokes/hub
with FlexVPN in 3.12 (RP2 only)

For your reference

FlexVPN CCO Documentation

- CCO doc link
  - http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_ike2vpn/configuration/15-mt/sec-flex-vpn-15-mt-book.html
  - Reflects latest release (currently 15.4(1)T)
- Doc organized into chapters
  - FlexVPN Site-Site
  - FlexVPN Server
  - FlexVPN Client
  - FlexVPN Spoke-Spoke
  - FlexVPN Load-Balancer
  - FlexVPN Reconnect
  - Appendix-1: FlexVPN Radius Attributes
  - Appendix-2: Legacy VPNs
- Changes across releases
  - Documentation reflects latest release
  - Behaviour/CLI changes noted in corresponding sections



cisco

⊟ **FlexVPN and Internet Key Exchange Version 2 Configuration Guide, Cisco IOS Release 15M&T**
- ⊡ Introduction to FlexVPN
- ⊡ Configuring Internet Key Exchange Version 2 and FlexVPN Site-to-Site
- ⊡ Configuring the FlexVPN Server
- ⊡ Configuring the FlexVPN Client
- ⊡ Configuring FlexVPN Spoke to Spoke
- ⊡ Configuring IKEv2 Load Balancer
- ⊡ Configuring IKEv2 Reconnect

FlexVPN and Internet Key Exchange Version 2 Configuration Guide, Cisco IOS Release 15M&T

Click the links on the left to view the individual chapters in HTML format.

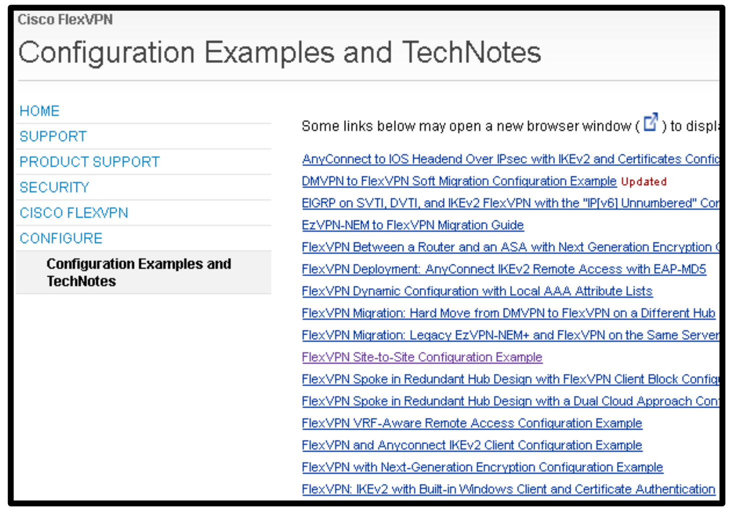
Download the complete book (PDF - 3.84MB)

Download the complete book (ePub - 761.0KB)

For your reference

FlexVPN CCO Documentation

- FlexVPN Sample Configurations
  - http://www.cisco.com/c/en/us/support/security/flexvpn/products-configuration-examples-list.html



Cisco FlexVPN

Configuration Examples and TechNotes

- HOME
- SUPPORT
- PRODUCT SUPPORT
- SECURITY
- CISCO FLEXVPN
- CONFIGURE
- **Configuration Examples and TechNotes**

Some links below may open a new browser window ( ) to displ

- AnyConnect to IOS Headend Over IPsec with IKEv2 and Certificates Confic
- DMVPN to FlexVPN Soft Migration Configuration Example Updated
- EIGRP on SVTI, DVTI, and IKEv2 FlexVPN with the "IP[v6] Unnumbered" Cor
- EzVPN-NEM to FlexVPN Migration Guide
- FlexVPN Between a Router and an ASA with Next Generation Encryption C
- FlexVPN Deployment: AnyConnect IKEv2 Remote Access with EAP-MD5
- FlexVPN Dynamic Configuration with Local AAA Attribute Lists
- FlexVPN Migration: Hard Move from DMVPN to FlexVPN on a Different Hub
- FlexVPN Migration: Legacy EzVPN-NEM+ and FlexVPN on the Same Server
- FlexVPN Site-to-Site Configuration Example
- FlexVPN Spoke in Redundant Hub Design with FlexVPN Client Block Configu
- FlexVPN Spoke in Redundant Hub Design with a Dual Cloud Approach Con
- FlexVPN VRF-Aware Remote Access Configuration Example
- FlexVPN and Anyconnect IKEv2 Client Configuration Example
- FlexVPN with Next-Generation Encryption Configuration Example
- FlexVPN: IKEv2 with Built-in Windows Client and Certificate Authentication

- Past FlexVPN sessions from Ciscolive
  - BRKSEC-3036 - Advanced IPsec designs with FlexVPN (2015 Milan)

  https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=82068
  - BRKSEC-2881 - VPN Remote Access with IOS & Introduction to FlexVPN (2015 Milan)

  https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=81929

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2015 T-Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mob App
- By visiting the Cisco Live Mobile Site http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com

Thank you.

cisco