Cisco live!

June 25–29, 2017 · Las Vegas, NV

Designing Remote-Access and Site-to-Site IPSec networks with FlexVPN

Piotr Kupisiewicz

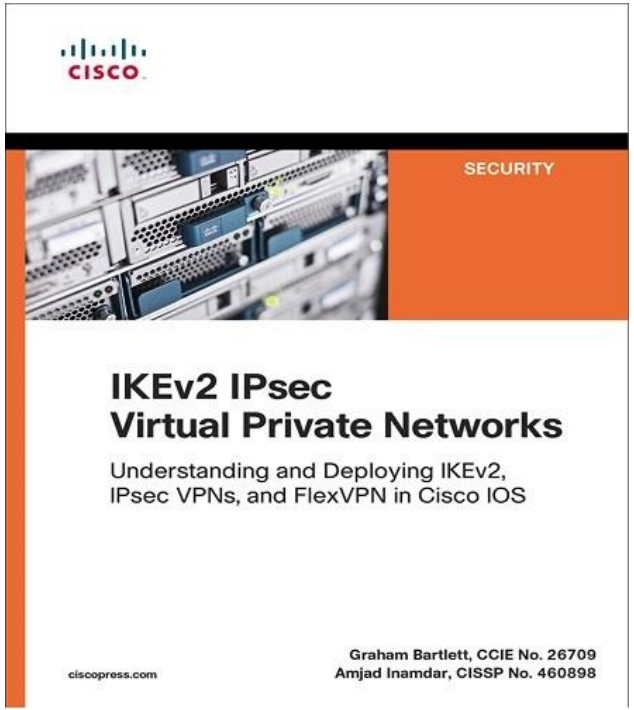
Cisco Services – Customer Support Engineer

Cisco live!

Objectives & Prerequisites

- Session objectives:
  - Introduce IKEv2 & FlexVPN, with a focus on AAA-based management
  - Demonstrate the value-add and possibilities of FlexVPN as a Remote Access solution with a variety of clients (software & hardware)
  - Solve simple & complex use cases using FlexVPN
- It's intermediate session
- Other sessions of interest
  - BRKSEC-3036 – Advanced IPSec with FlexVPN and IKEv2
  - BRKSEC-3005 - Cryptographic Protocols and Algorithms - a review
  - TECSEC-3725 - Advanced Remote-Access and Site-to-Site VPN Design with IOS

Cisco Press Book 'IKEv2 IPsec VPNs' by Amjad Inamdar & Graham Bartlett



https://www.amazon.com/IKEv2-IPsec-Virtual-PrivateNetworks/dp/1587144603/

Listed in the CCIE Security reading list
https://learningnetwork.cisco.com/community/certifications/ccie_security/written_exam/study-material

Customer Reviews ★★★★★

One of the best technical books I've read
This book is the IKEv2 VPN equivalent of Jeff Doyle's Routing T… 2 - a must read for any network security engineer wanting to design and build secure VPN's. One of the best technical books I've read.

Superb book and well worth the money for anyone even thinking about Cisco crypto
This book is the most comprehensive book on IKEv2 for Cisco network engineers that you will find and is all about real-world scenarios.

Definitive guide on modern IPsec VPN theory and practice
Many times I wish I had a book like this to help distill many complex IETF RFCs into "plain English" and provide practical and actionable security best practices.

Brilliant
I bought the Kindle version of this on a bit of an impulse. I'm really glad I did, it's well worth the money. Not only can I establish secure IKEv2 tunnels, I also feel like I know the subject thoroughly now. Even in respect to non-Cisco equipment. The book is a great reference too. I don't usually leave reviews but was motivated to in this instance. Good job, highly recommended.

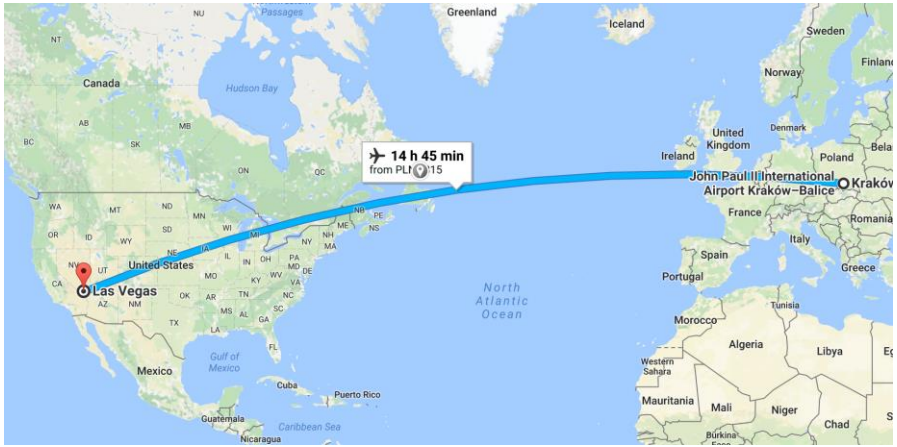
The best book on IKEv2 IPsec VPNs
The book is awesome! I appreciate authors' work on presenting deeply technical topics in extremely easy to understand manner.

Finally, all you need to know about FLEX in one place!
Well written , concise and accurate. An absolute must for anyone designing, supporting or troubleshooting IKEv2 VPNs. You too can become a FLEX expert!

Very good Book on IPsec VPN for Enterprise networks
Very well Written book, This book touches on most important topic on building Dynamic VPN for enterprise networks.

Cisco Press rebate code: ike35

About me



Cisco Spark

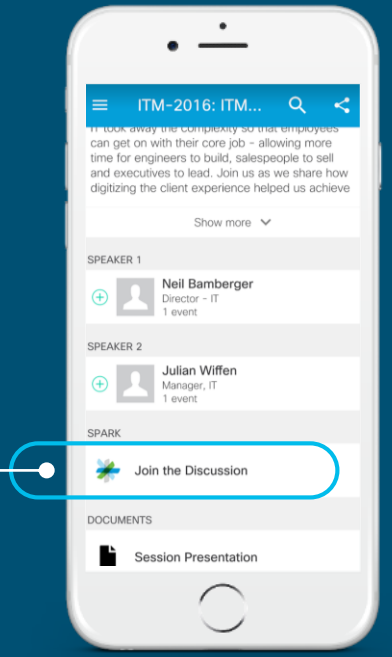
Questions?

Use Cisco Spark to chat with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

Cisco Spark spaces will be available until July 3, 2017.



cs.co/ciscolivebot#BRKSEC-2881

Agenda

- Introduction
- IKEv2 Overview
- Tunnel Interfaces
- Configuration Building Blocks
- FlexVPN AAA Integration
- Remote Access Clients
- Deployment Scenarios & Use Cases
- Wrap-up

Introduction to FlexVPN

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 (AAA, IPv6, Routing…)
  - No IWAN Support
  - Simplified configuration using smart-defaults
  - Interoperable with non-Cisco implementations
  - Easy to learn, market and manage

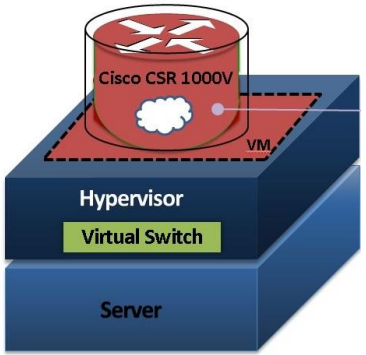
Solution Positioning

	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

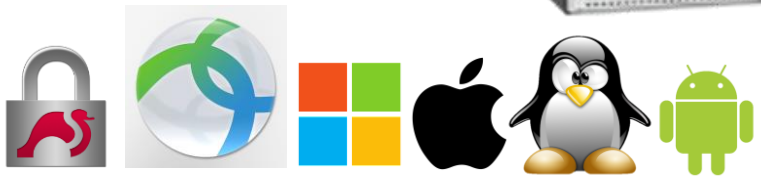
Key Platforms

ASR 1000 series



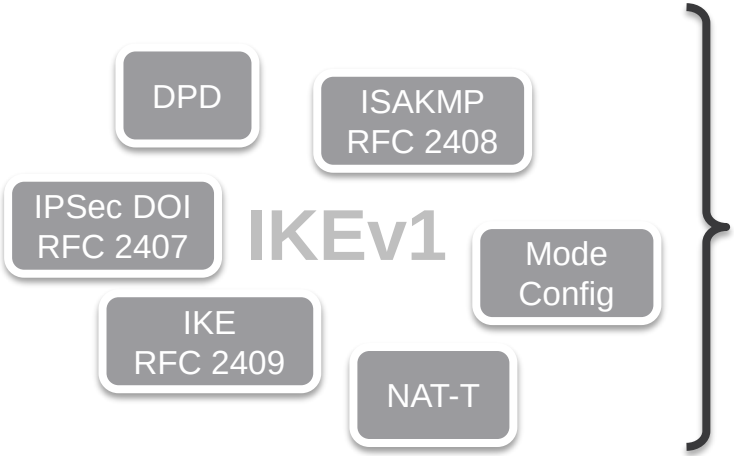
ISR 800 Series

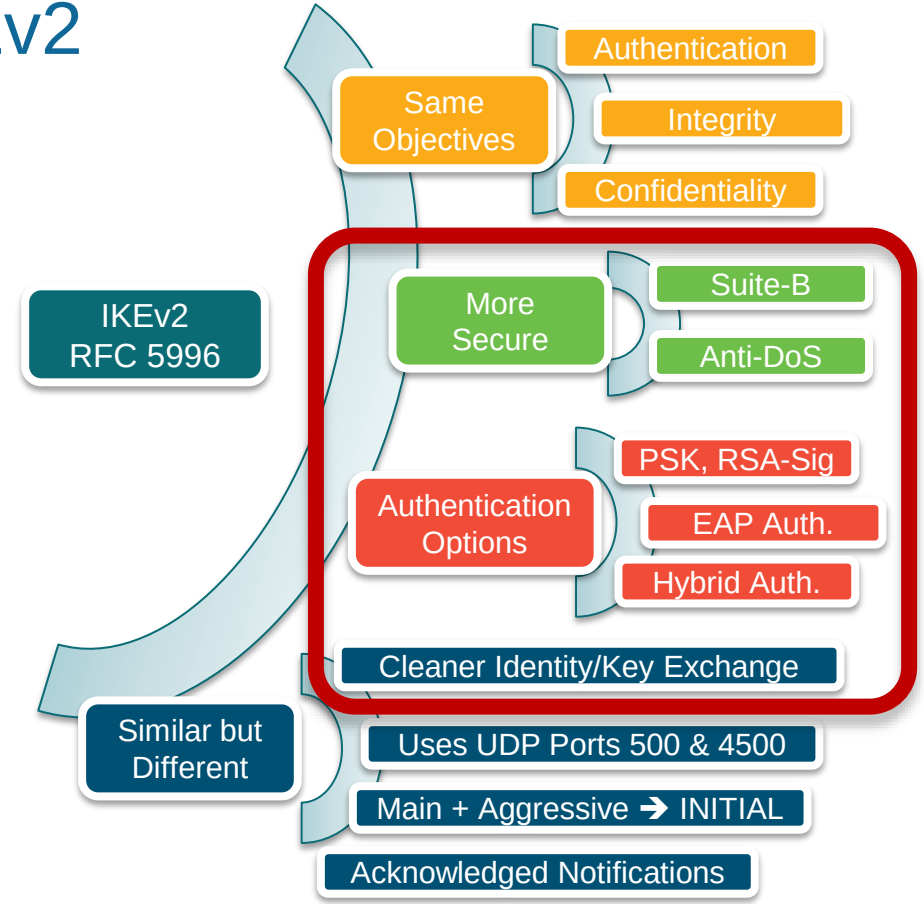
ISR 4000 Series



IKEv2 Overview

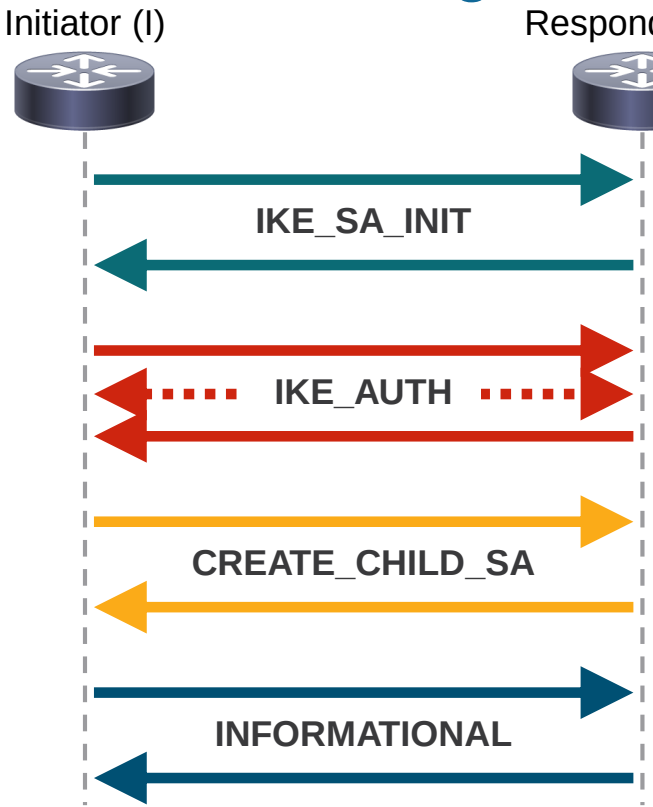
Comparing IKEv1 & IKEv2





IKEv2 Exchanges

Additional info



IKEv2 Security Association (SA) establishment (proposal selection, key exchange)

Mutual authentication & identity exchange
Initial IPSec SAs establishment
Certificate exchange (optional)
Configuration exchange (optional)

Additional IPSec SAs establishment
IKEv2 & IPSec SA rekey

Can be (I → R) with ACK or (R → I) with ACK
Notifications (SA deletion, liveness check, ...)
Configuration exchange (one or both ways)

Key Differentiators

Additional info

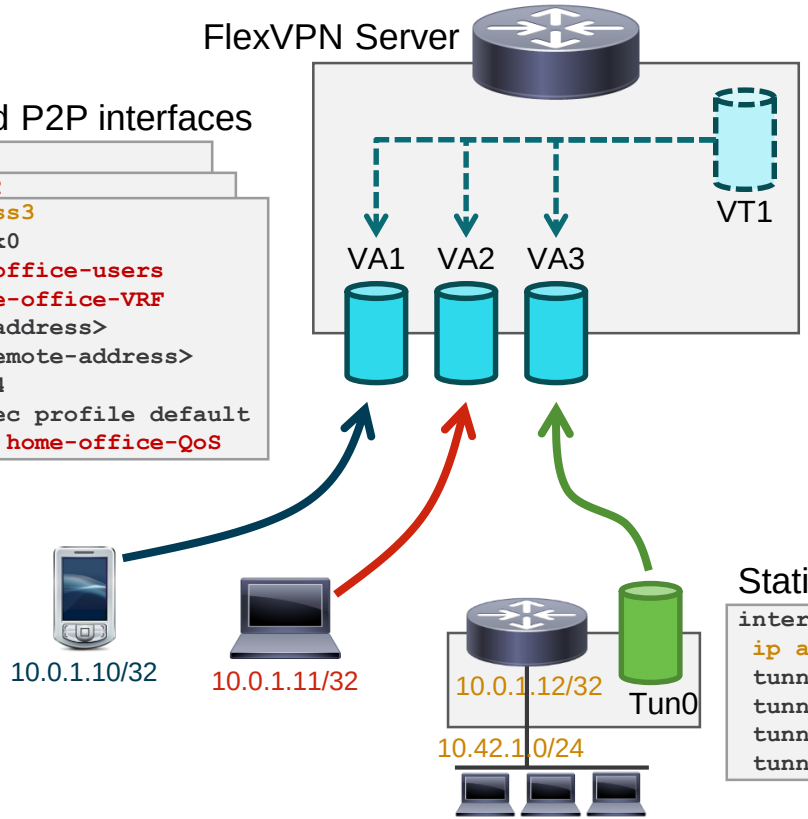
	IKEv1	IKEv2
Auth messages	6 max	Open ended
First IPsec SA	6-9 messages	~ 4-6 messages minimum
Authentication	pubkey-sig, [pubkey-encr], PSK	pubkey-sig, PSK, EAP, asymmetrical authentication
Security	Vulnerable to DOS attacks	Anti-clogging, Suite-B Support, …
IKE rekey	Requires re-auth (expensive)	No Re-auth
Notifies	Fire & Forget	Acknowledged
Message Segmentation	None, relies on IP fragmentation	Protocol built in
NG Cryptography	**Support is stopped***	**Yes**

Tunnel Interfaces

Dynamic Point-to-Point Virtual Interfaces

Dynamically instantiated P2P interfaces

```
interface Virtual-Access1
interface Virtual-Access2
interface Virtual-Access3
 ip unnumbered Loopback0
 ip access-group home-office-users
 ip vrf forwarding home-office-VRF
 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
```

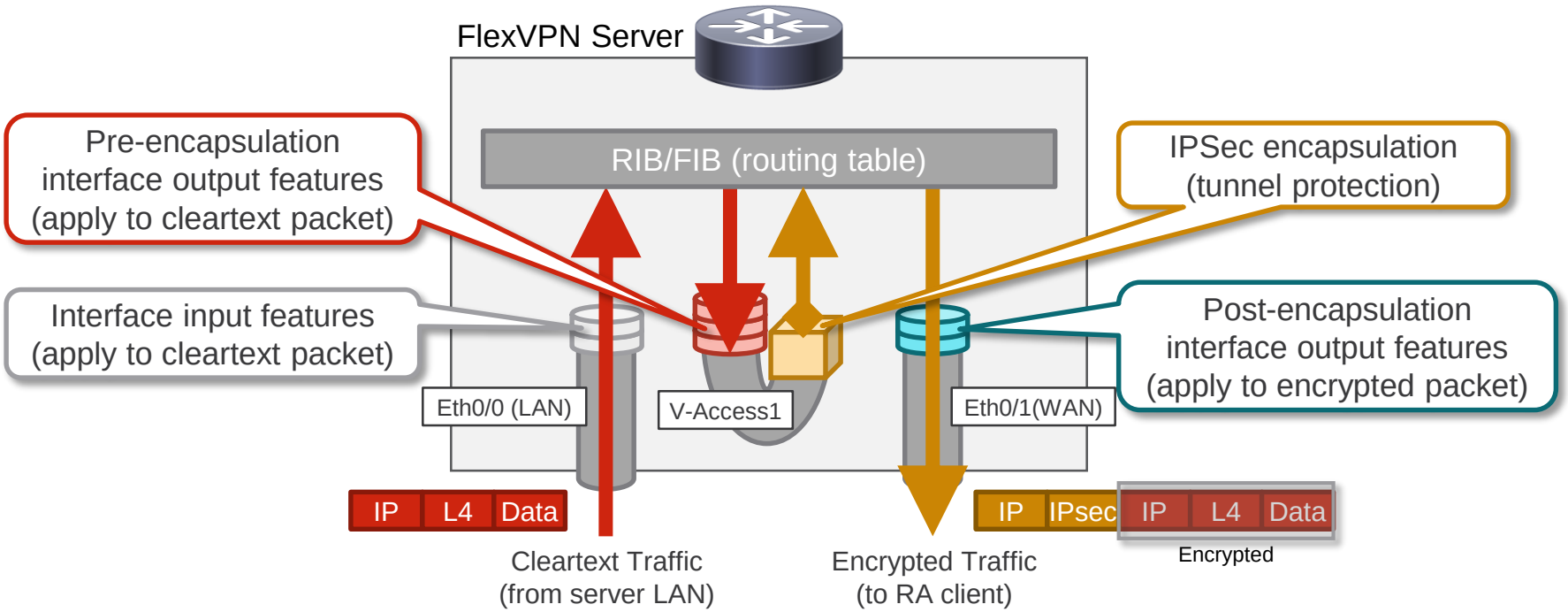
Server routing table (RIB/FIB)

```
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
```

Interface Features



Interface feature (NAT, PBR, QoS, NetFlow, ...)

Tunnel Encapsulation

- IPSec Tunnel Mode (IPv4 or IPv6)
  - Classic dVTI: compatibility with software clients (any-to-any or any-to-assigned-address)
  - Multi-SA dVTI: compatibility with legacy crypto map peers (ASA, other vendors)
  - IPv4 over IPv6 Mixed Mode in IOS-XE3.10

```
interface Virtual-Template1 type tunnel
 tunnel mode ipsec {ipv4 | ipv6}
 tunnel protection ipsec profile default
```

- GRE over IPSec
  - Enables tunneling of non-IP protocols (e.g. MPLS)
  - Required for dynamic mesh scenarios (aka DMVPN, but with the extra flexibility of point-to-point interfaces)
  - “tunnel mode gre ip” is the default on static & dynamic tunnel interfaces

```
interface Virtual-Template1 type tunnel
 tunnel mode gre {ip | ipv6}
 tunnel protection ipsec profile default
```

IPv6 Support Summary

- GRE over IPSec
  - Dual-stack (IPv4 + IPv6 over IPSec) out of the box

Passenger Protocol

Transport Protocol	IPv4	IPv6
IPv4	✓	✓
IPv6	✓	✓

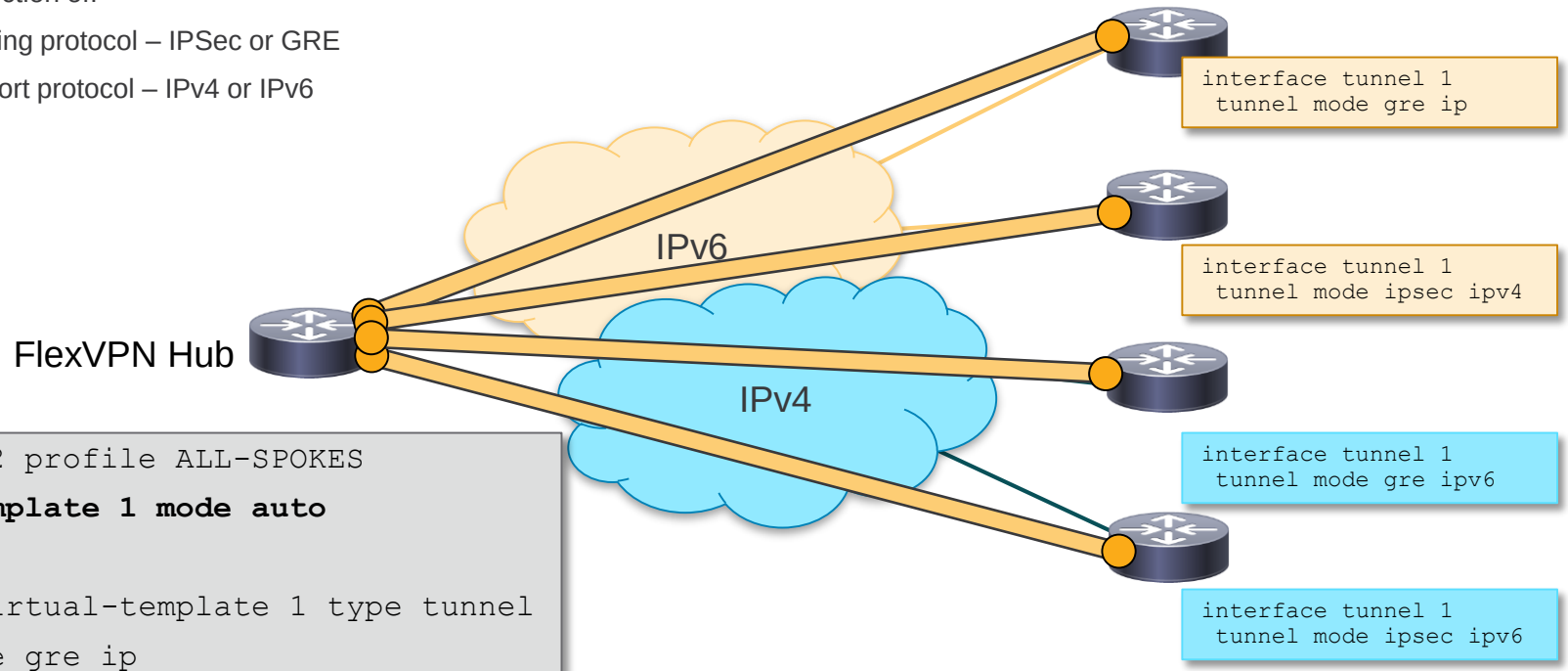
- IPSec Tunnel Mode
  - Dual-stack support
  - IPv4 over IPv6 mixed-mode

Passenger Protocol

Transport Protocol	IPv4	IPv6
IPv4	✓	✓
IPv6	✓ (Since XE3.10)	✓

Auto Tunnel Mode

- Reduces deployment complexity due to different tunnel encapsulations
- Automatic detection of:
  - Tunneling protocol – IPSec or GRE
  - Transport protocol – IPv4 or IPv6




```
crypto ikev2 profile ALL-SPOKES
 virtual-template 1 mode auto
!
interface virtual-template 1 type tunnel
 tunnel mode gre ip
```

Configuration Building Blocks

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

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

IKEv2 identity & profile selection

IKEv2 authentication & certificates

AAA integration (authentication, authorization, accounting)

Dynamic point-to-point interfaces

Native IPSec tunnel or GRE/IPSec

A Simple Site-to-Site Configuration

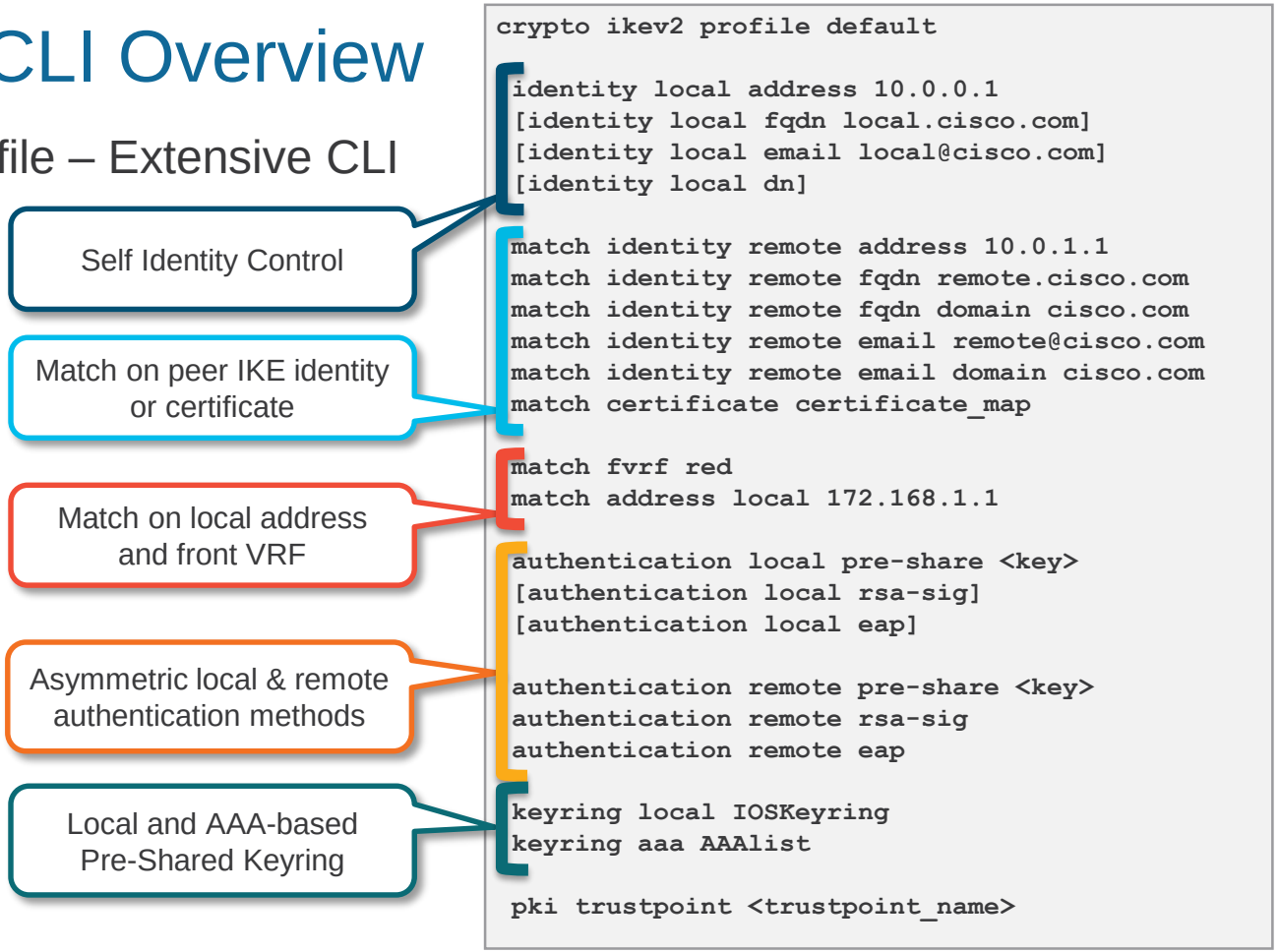
Example with IPv6 over IPv4 tunneling


```
crypto ikev2 profile default
 match identity remote fqdn r2.cisco.com
 identity local fqdn r1.cisco.com
 authentication local pre-shared key cisco123
 authentication remote pre-shared key cisco123

ipv6 unicast-routing

interface Tunnel0
 ipv6 ospf 1 area 0
 tunnel source FastEthernet0/0
 tunnel destination 172.16.2.1
 tunnel protection ipsec profile default

interface E0/0
 ipv6 address 2001:db8:cafe::1/64
 ipv6 ospf 1 area 0
```

```
crypto ikev2 profile default
 match identity remote fqdn r1.cisco.com
 identity local fqdn r2.cisco.com
 authentication local pre-shared key cisco123
 authentication remote pre-shared key cisco123

ipv6 unicast-routing

interface Tunnel0
 ipv6 ospf 1 area 0
 tunnel source FastEthernet0/0
 tunnel destination 172.16.1.1
 tunnel protection ipsec profile default

interface E0/0
 ipv6 address 2001:db8:beef::1/64
 ipv6 ospf 1 area 0
```

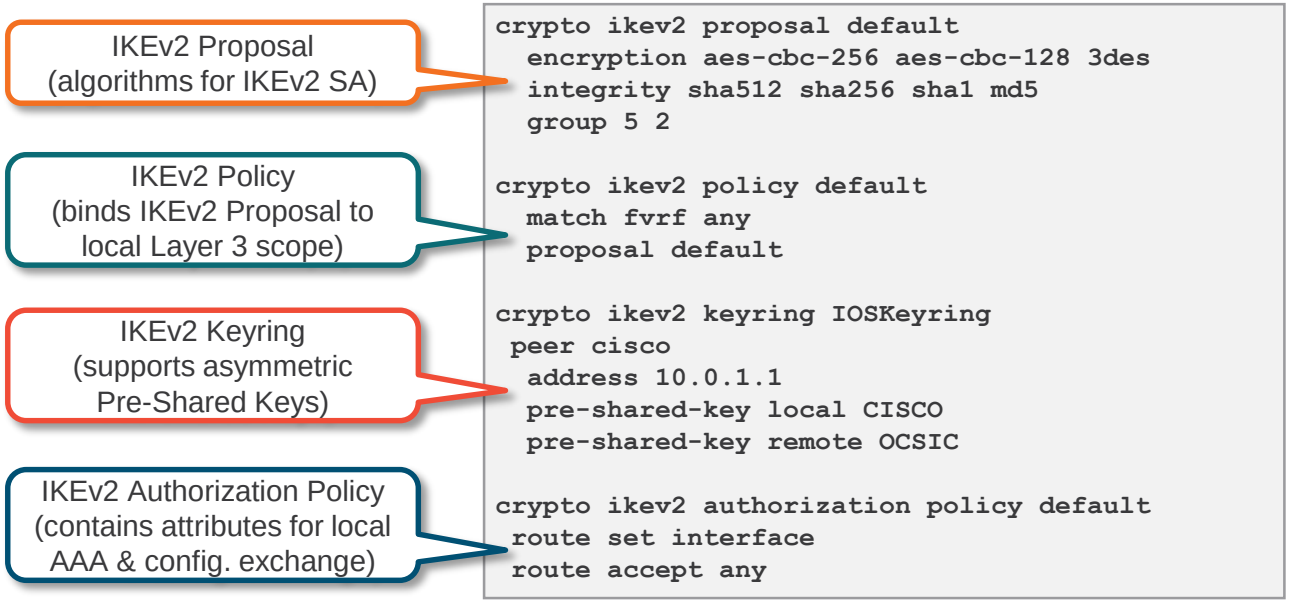
IKEv2 CLI Overview

IKEv2 Profile – Extensive CLI



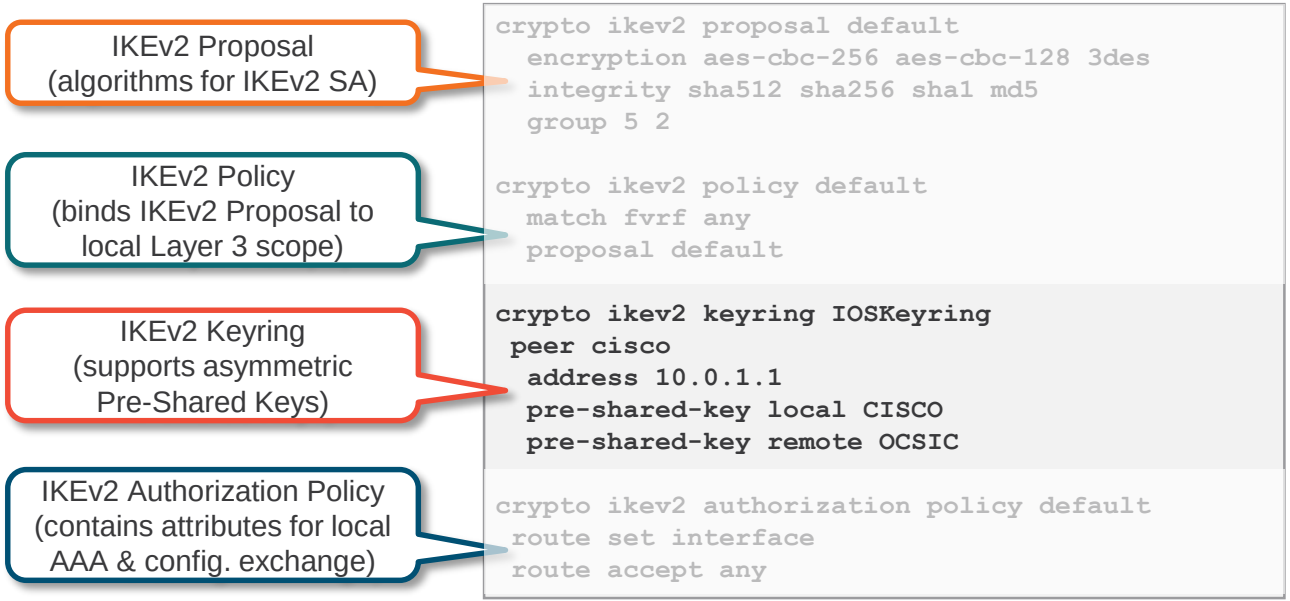
IKEv2 CLI Overview

Proposal, Policy, and Keyring



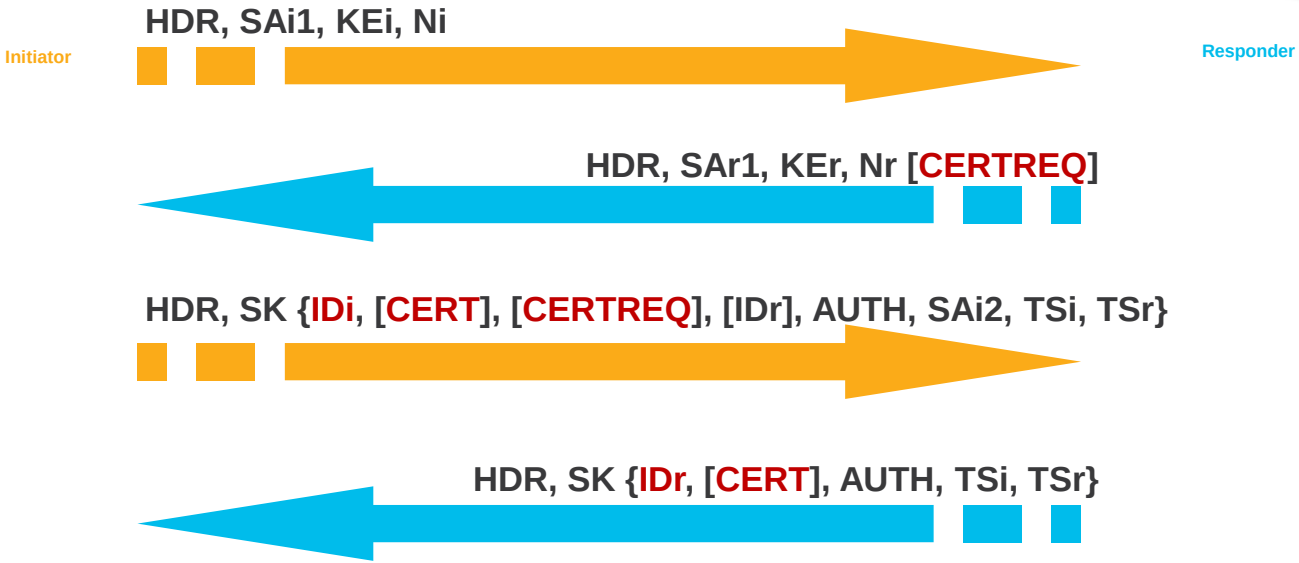
IKEv2 CLI Overview - Smart Defaults

Proposal, Policy, and Keyring



IKEv2 Basic Negotiation

Additional info



HDR – IKE Header

SAi, SAr – Crypto algorithms proposed/accepted by the peer

KEi, KEr – Initiator Key Exchange material

Ni, Nr – Initiator/Responder Nonce

SK {...} – Payload encrypted and integrity protected

IDi, IDr – Initiator/Responder IKE Identity

CERTREQ, CERT – Certificate Request, Certificate Payload

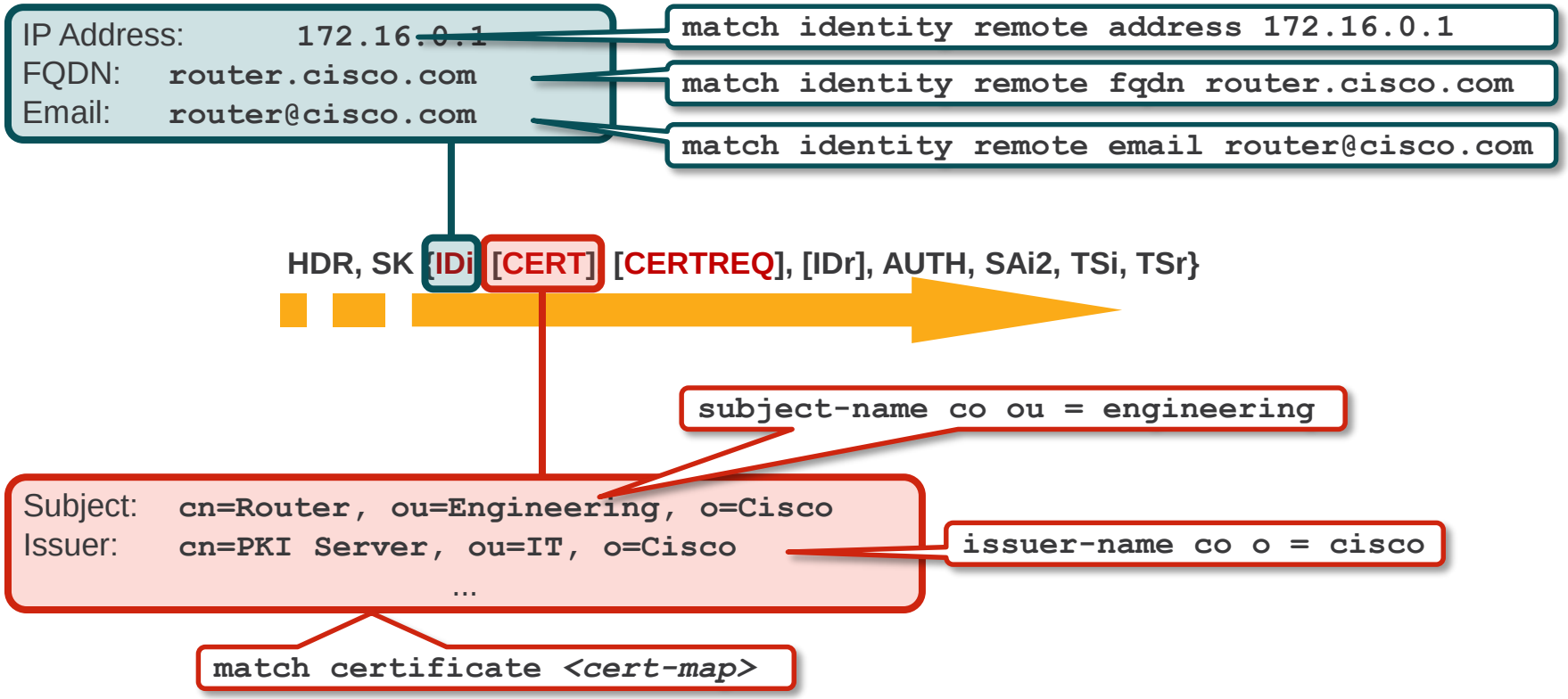
AUTH – Authentication data

SA – Proposal & Transform to create initial CHILD_SA

TSi, TSr – Traffic Selectors (as src/dst proxies)

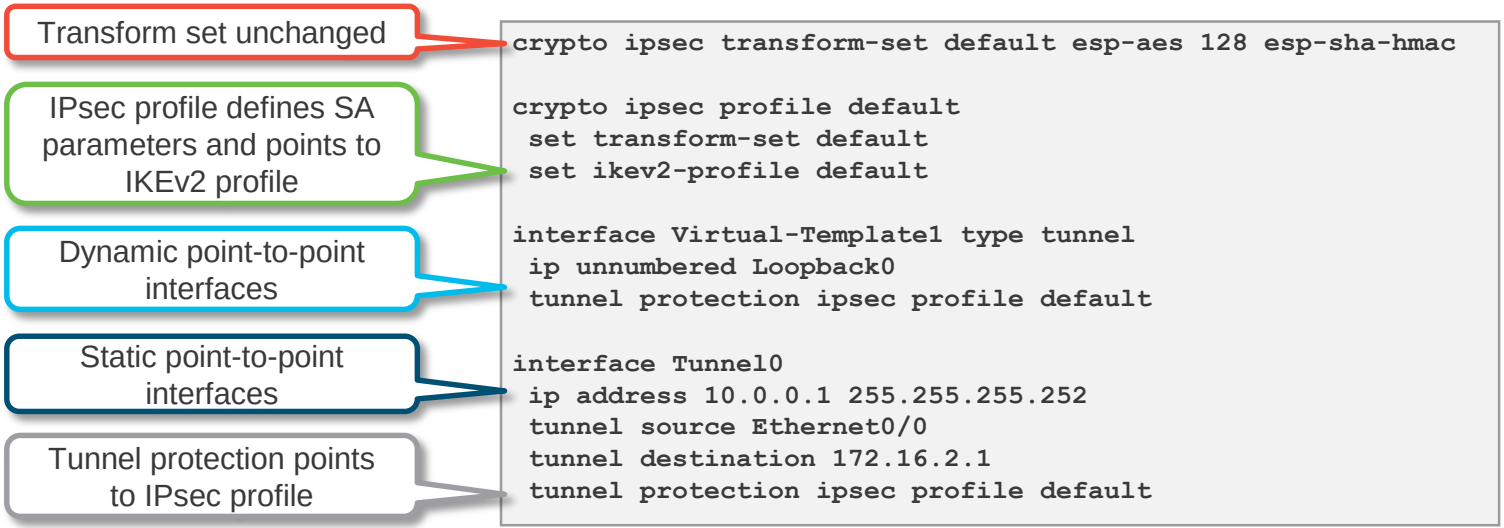
IKEv2 Profile Match Statements

Additional info



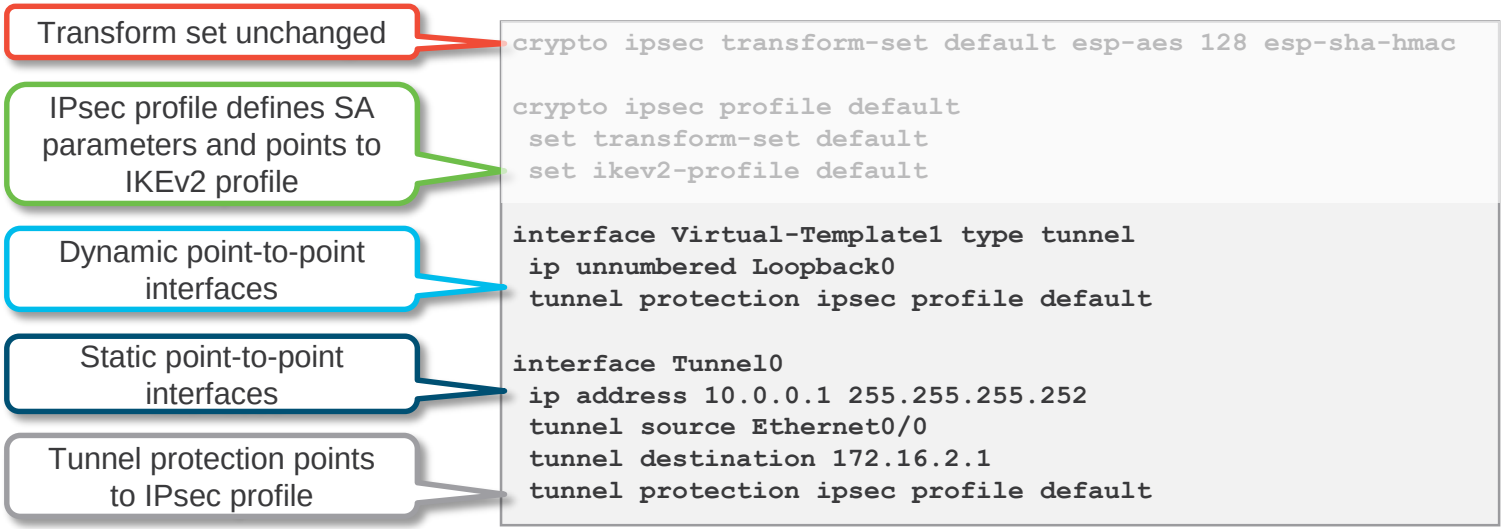
IPSec CLI Overview

Tunnel Protection similar to DMVPN and EasyVPN



IPSec CLI Overview – Smart Defaults

Tunnel Protection similar to DMVPN and EasyVPN



Reconfigurable Defaults

All defaults can be modified, deactivated, or restored

- Modifying defaults:

```
crypto ikev2 proposal default
  encryption aes-cbc-128
  integrity md5

crypto ipsec transform-set default esp-aes 256 esp-sha-hmac
```

- Restoring defaults:

```
default crypto ikev2 proposal

default crypto ipsec transform-set
```

- Disabling defaults:

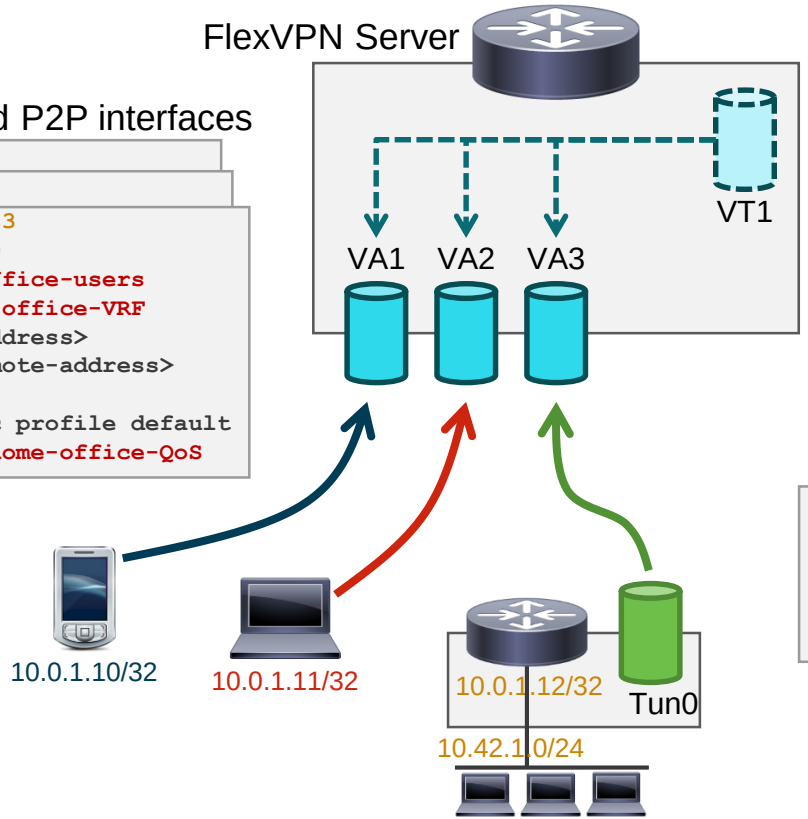
```
no crypto ikev2 proposal default

no crypto ipsec transform-set default
```

FlexVPN AAA Integration

Dynamic Point-to-Point Virtual Interfaces

Dynamically instantiated P2P interfaces

```
interface Virtual-Access1
interface Virtual-Access2
interface Virtual-Access3
 ip unnumbered Loopback0
 ip access-group home-office-users
 ip vrf forwarding home-office-VRF
 tunnel source <local-address>
 tunnel destination <remote-address>
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
 service-policy output home-office-QoS
```



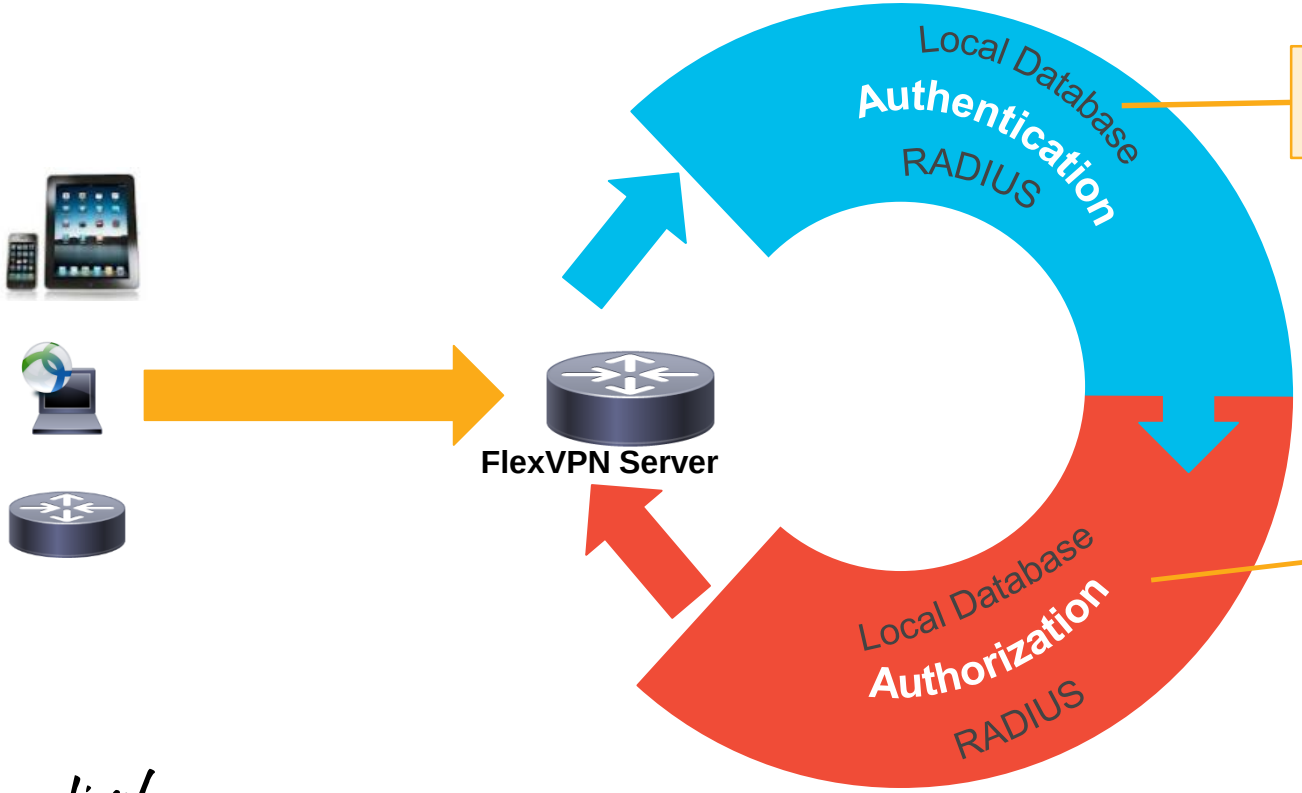
P2P virtual interface template

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

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
```

Authentication and Authorization @ 30,000 ft



Who are you ?
Whats your code word?

What can you access?

- ✓ ACL,QOS,ZBFW policies
- ✓ Client IP address
- ✓ DNS, WINS
- ✓ and more …

High-Level Interactions

RA Client
IKEv2 Initiator
RADIUS Client
EAP Supplicant

FlexVPN Server
IKEv2 Responder
RADIUS NAS
EAP Authenticator

AAA Server
RADIUS Server
EAP Backend

EAP (Username/Password)
Certificates (IKEv2/EAP-TLS)


```
Framed-IP-Netmask = "255.255.255.255",
ipsec:addr-pool=Eng-pool
ipsec:dns-servers=10.0.1.1
ip:interface-config=vrf forwarding Eng-vrf
ip:interface-config=ip unnumbered Loopback1
```

FlexVPN AAA Integration:
› AAA-Based Authentication

Certificate Authentications

RA Client
IKEv2 Initiator
RADIUS Client
EAP Supplicant

FlexVPN Server
IKEv2 Responder
RADIUS NAS
EAP Authenticator

AAA Server
RADIUS Server
EAP Backend

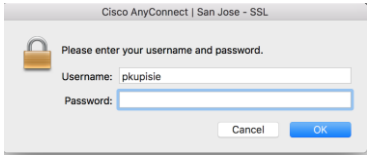
EAP Authentication

Additional info

- Extensible Authentication Protocol (RFC 3748)
  - Provides common functions for a variety of authentication methods
  - Tunneling methods (costly): EAP-TTLS, EAP-PEAP, …
  - Non-tunneling (recommended): EAP-MSCHAPv2, EAP-GTC, EAP-MD5, …
- Implemented in IKEv2 as additional IKE_AUTH packets
  - RA client initiates EAP authentication by omitting AUTH payload in IKE_AUTH
  - RA server must authenticate itself using certificates (mandatory)
  - Authentication takes place between RA client and EAP backend authentication server
- EAP packets are relayed by RA server
  - Between RA client and RA server: tunneled inside IKEv2
  - Between RA server and EAP backend: tunneled inside RADIUS
- EAP method is transparent to RA server
  - Only needs to be supported by RA client and EAP backend

EAP Authentication (Standard Protocols)

RA Client
IKEv2 Initiator
RADIUS Client
EAP Supplicant



FlexVPN Server
IKEv2 Responder
RADIUS NAS
EAP Authenticator

IKE

AAA Server
RADIUS Server
EAP Backend

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

RA server authenticates to client using IKE certificates (mandatory)

IKEv2 (IKE_AUTH)
EAP(CREDENTIALS)

RADIUS (Access-Request)
EAP(CREDENTIALS)

RADIUS (Access-Accept)

IKEv2 | RADIUS
EAP-GTC / EAP-MD5 / EAP-MSCHAPv2 / EAP-AKA / EAP-SIM / ...

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

EAP Authentication – Packet Flow

For your reference

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

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

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

MSK

MSK

IKEv2 (IKE_AUTH)
EAP(Success)
RADIUS (Access-Accept)
EAP(Success), MSK, User-Name;
Other user attributes

EAP Username

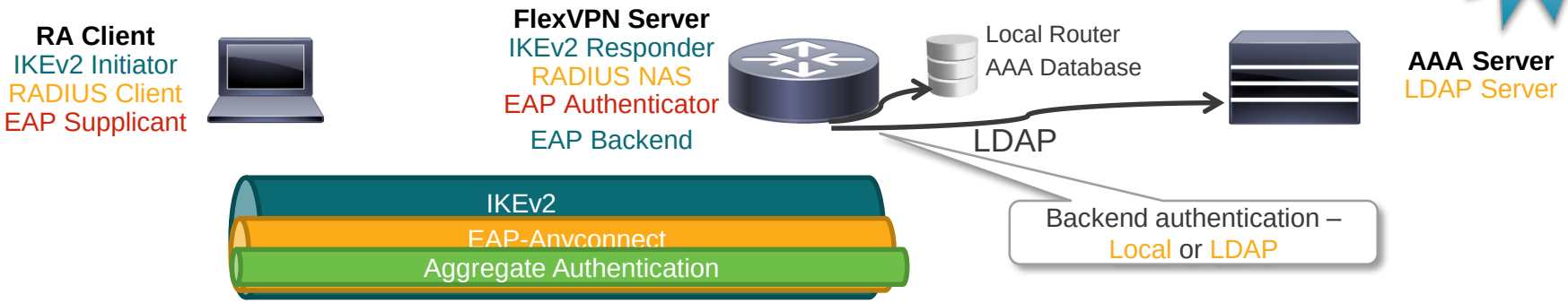
Cached for authorization

IKEv2 (IKE_AUTH)
AUTH(MSK)

IKEv2 (IKE_AUTH)
CFG_REPLY, AUTH(MSK)

Anyconnect-EAP & Aggregate Authentication

15.5(2)S+
15.5(2)T+



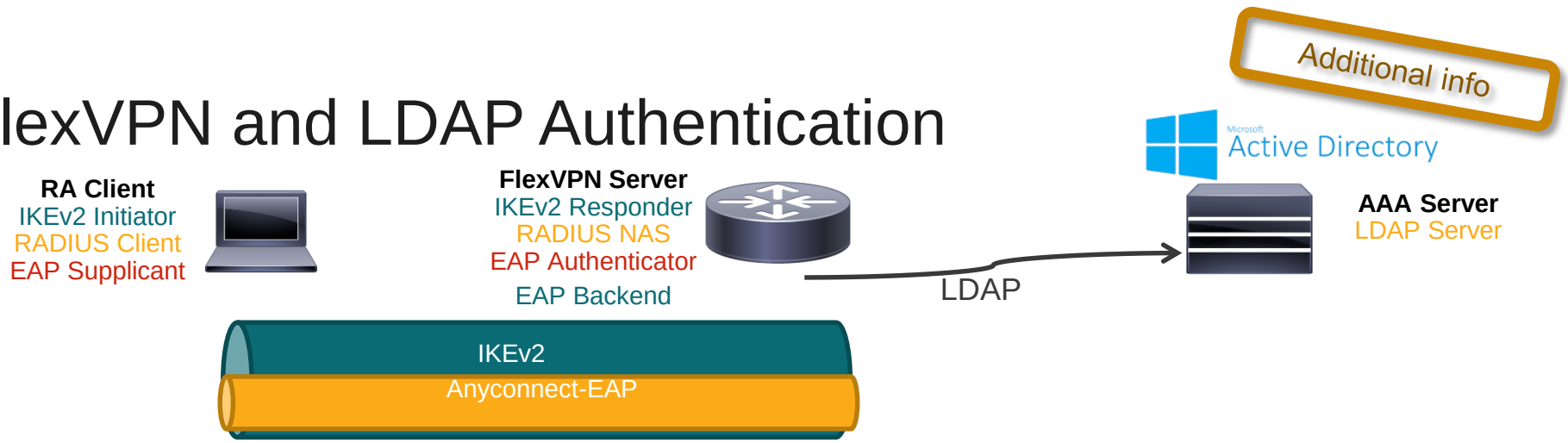
- Platform-independent framework for authentication and config exchange
- Common XML Data format - IKEv2 and SSL
  - Anyconnect support only
- New client side features
  - No headend s/w change required
  - Opaque info can be sent from headend
- Easier Integration of new client features
  - Eg. Double or client Cert Authentication
- Set Bypassdownloader to true in AnyConnectLocalPolicy

Example

```
<config-auth client="vpn" type="auth-request" aggregate-auth-
version="2">
<opaque is-for="sg">
<config-hash>1433410501969</config-hash>
</opaque>
<auth id="main">
<title>Login</title>
<message>Please enter your username and password.</message>
<banner></banner>
<input type="text" name="username" label="Username:"></input>
<input type="password" name="password" label="Password:"></input>
```

```
<BypassDownloader>true</BypassDownloader>
```

FlexVPN and LDAP Authentication




```
aaa group server ldap AD
 server AD_SRV
aaa authentication login AD_AAA group AD
ldap server AD_SRV
 ipv4 192.168.244.123
 attribute map LDAP_AM
 timeout retransmit 20
 bind authenticate root-dn CN=admin, \
        CN=Users,DC=cisco,DC=com password Test123
 base-dn CN=Users,DC=cisco,DC=com
 authentication bind-first
```

```
crypto ikev2 profile default
match identity remote key-id cisco
authentication local rsa-sig
pki trustpoint TRUSTPOINT
aaa authentication anyconnect-eap AD_AAA
aaa authorization group anyconnect-eap list local_list
aaa authorization user anyconnect-eap cached
virtual-template 5
```

EAP Authentication – Initiation

Additional info

RA Client
IKEv2 Initiator
RADIUS Client
EAP Supplicant

FlexVPN Server
IKEv2 Responder
RADIUS NAS
EAP Authenticator

AAA Server
RADIUS Server
EAP Backend

With "query-identity"

"query-identity" recommended
- several clients jam if not configured
- not the default ... but it should be

IKEv2 (IKE_AUTH)
IDi, CFG_REQ, no AUTH

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

IKEv2 (IKE_AUTH)
EAP(ID-Response: ID_{EAP})

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

EAP ID provided by client

Without "query-identity"

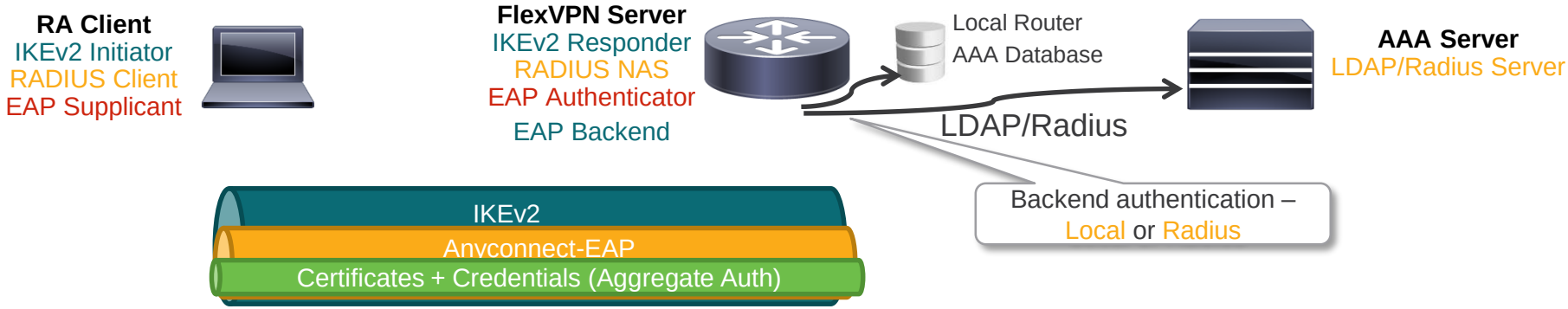
IKEv2 (IKE_AUTH)
IDi, CFG_REQ, no AUTH

IKEv2 (IKE_AUTH)
IDr, AUTH(RSA)

RADIUS (Access-Request)
EAP(ID-Response: IDi)

IKE ID used as EAP ID

Dual Authentication - Certificates + Aggregate auth



- XML-based **aggregate** authentication and configuration protocol transported over the **AnyConnect-EAP** allows dual factor authentication
  - Certificate for device authentication
  - User credentials for user authentication
- Set Bypassdownloader to true in AnyConnectLocalPolicy

```
<BypassDownloader>true</BypassDownloader>
```

Syntax

```
crypto ikev2 profile dual_auth_profile
   authentication remote anyconnect-eap aggregate cert-request
```

FlexVPN AAA Integration:
› User & Group Authorization

Authorization Types

RA Client

FlexVPN Server

AAA Server

IKE_AUTH – EAP-MSCHAPv2
EAP(Username/Password)

RADIUS (Access-Request)
EAP(Username/Password)

RADIUS (Access-Accept)
Framed-IP-Address = ”192.168.100.1"

Implicit/Cached authorization

or

RADIUS (Access-Request)
User-Name: Joe
Password: authorization

RADIUS (Access-Accept)
Framed-IP-Address = ”192.168.100.1"

Explicit User authorization

and

RADIUS (Access-Request)
User-Name: Eng
Password: authorization

RADIUS (Access-Accept)
ipsec:dns-servers=10.0.1.1

Explicit Group authorization

Cisco live!

Attributes – Merging

Additional info

FlexVPN Server

AAA 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

Received during explicit user authorization

Attribute	Value
Framed-IP-Address	10.0.0.102

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

Merged User Attributes

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

Explicit Group Attributes

Received during explicit group authorization

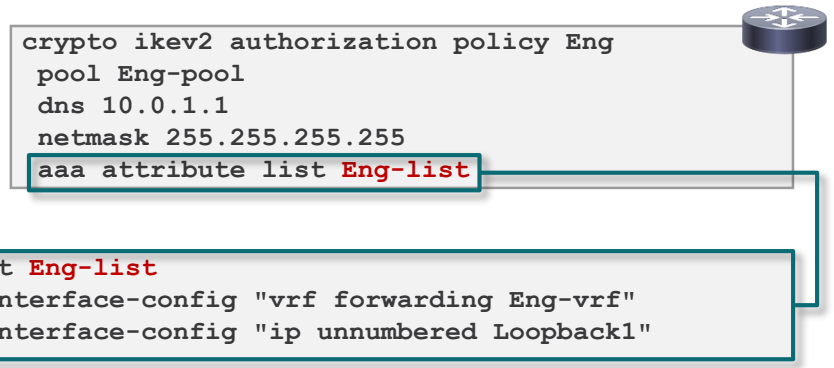
Attribute	Value
ipsec:dns-servers	10.2.2.3
ipsec:banner	Welcome !

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

Final Merged Attributes

Attributes – Local Authorization

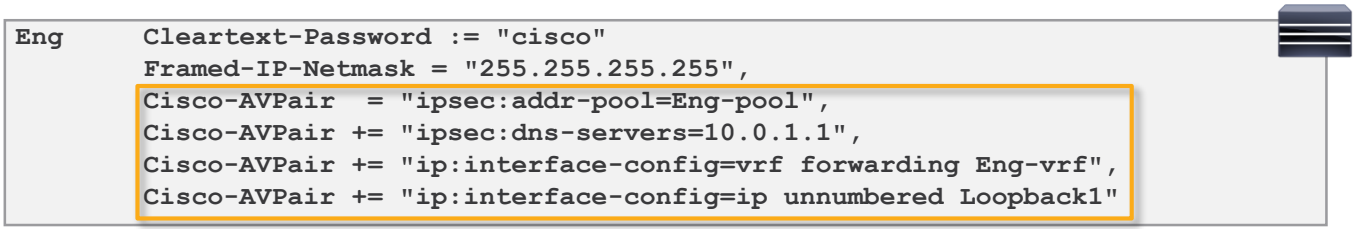
- Local Database
  - IKEv2 Authorization Policy
  - AAA Attribute List (V-Access interface configuration statements)



```
crypto ikev2 authorization policy Eng
 pool Eng-pool
 dns 10.0.1.1
 netmask 255.255.255.255
 aaa attribute list Eng-list
```

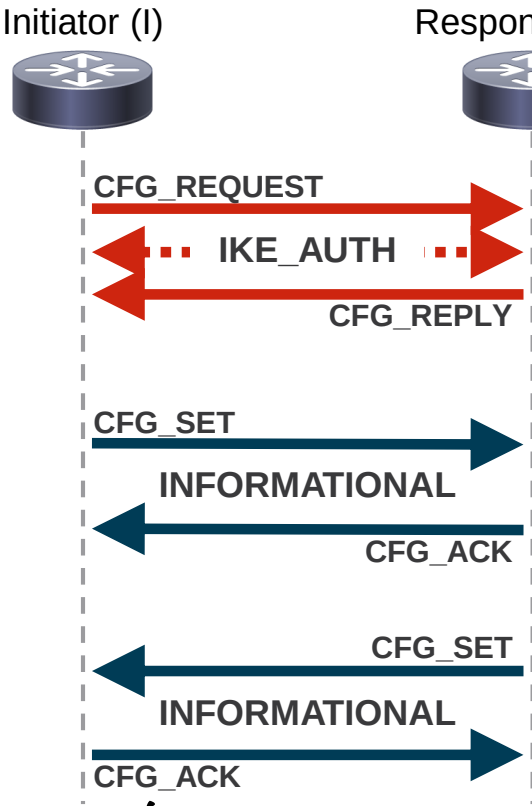
```
aaa attribute list Eng-list
 attribute type interface-config "vrf forwarding Eng-vrf"
 attribute type interface-config "ip unnumbered Loopback1"
```

- Central/Remote Database (on RADIUS Server)
  - Standard IETF Attributes (Framed-IP-Address, etc.)
  - Cisco Attribute-Value Pairs (Cisco-AVPair)



```
Eng     Cleartext-Password := "cisco"
        Framed-IP-Netmask = "255.255.255.255",
        Cisco-AVPair  = "ipsec:addr-pool=Eng-pool",
        Cisco-AVPair += "ipsec:dns-servers=10.0.1.1",
        Cisco-AVPair += "ip:interface-config=vrf forwarding Eng-vrf",
        Cisco-AVPair += "ip:interface-config=ip unnumbered Loopback1"
```

IKEv2 Configuration Exchange



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 protected IPv6 subnets

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

Derived from peer authorization

Derived from peer authorization

- ✓ My local IPv6 protected subnets are ...

- ✓ Acknowledged

Attributes – IP Address Assignment

Additional info

- User-specific statically assigned IP address
  - Returned as RADIUS IETF Framed-IP-Address
  - External DB only, not configurable in IKEv2 Authorization Policy

```
joe
 Framed-IP-Address = "10.0.1.101"
 Framed-IP-Netmask = "255.255.255.255"
```

- IOS-managed address pool
  - Referenced in user or group attributes
  - IOS pool name can be passed by RADIUS server
  - Allocation/deallocation entirely managed by IOS

```
crypto ikev2 authorization policy Eng
 pool Eng-pool
!
ip local pool Eng 10.0.1.10 10.0.1.99
```

```
Eng
 Cisco-AVPair  = "ipsec:addr-pool=Eng-pool"
```

- DHCP-assigned IP addresses
  - Request placed by IOS on behalf of RA client
  - DHCP server can be passed by RADIUS

```
crypto ikev2 authorization policy Eng
 dhcp server 10.2.2.2
```

```
Eng
 Cisco-AVPair  = "ipsec:group-dhcp-server=10.2.2.2"
```

- RADIUS-managed address pool
  - Address allocated by RADIUS server and returned as Framed-IP-Address
  - Accounting must be configured (to release addresses when clients disconnect)

Remote Access Example

RA Client

My IKE ID is type key-id and value: **IT**
Here is my **identity certificate**
I need an **IPv4 address**

FlexVPN Server

Map connection to IKEv2 profile by matching fqdn domain.cisco.com

Perform certificate-based authentication (not shown)

Invoke AAA with list "here" (local authorization) & username "**IT**"

Allocate IPv4 address from pool "**IT**"

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

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

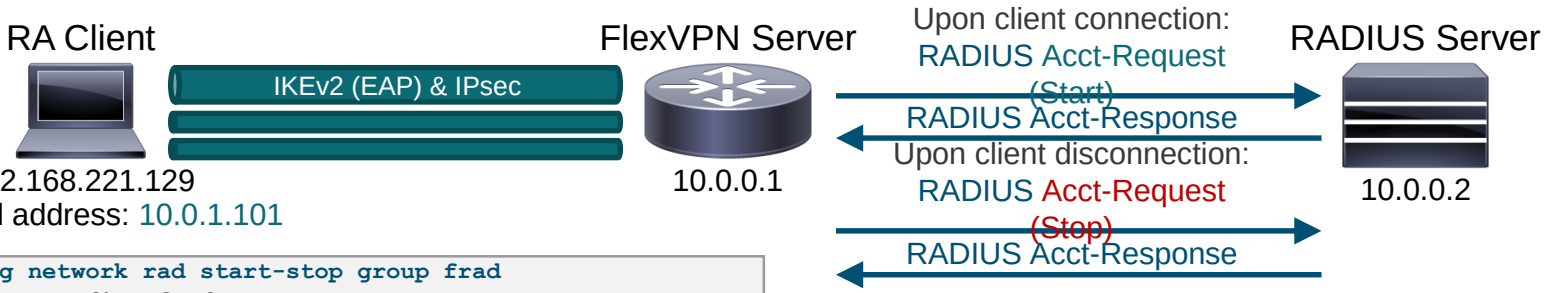
"show derived-config ..."

```
interface Virtual-Access1
 vrf forwarding IT-vrf
 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 flex_local local
aaa attribute list IT-list
 attribute type interface-config "vrf forwarding IT-vrf"
 attribute type interface-config "ip unnumbered Loopback1"
!
crypto ikev2 authorization policy IT
 pool IT-pool
 netmask 255.255.255.255
 aaa attribute list IT-list
!
crypto ikev2 profile default
 match identity remote key-id IT
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint root
 aaa authorization group cert list flex_local
 virtual-template 1
!
ip local pool IT-pool 10.0.1.10 10.0.1.99
!
interface Loopback1
 vrf forwarding IT-vrf
 ip address 10.0.1.1 255.255.255.255
!
interface Virtual-Template1 type tunnel
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
```

FlexVPN AAA Integration › Connection Accounting

AAA Accounting




```
aaa accounting network rad start-stop group frad
aaa group server radius frad
 server-private 10.0.0.2 auth-port 1812 acct-port 1813 key s3cr3t
!
crypto ikev2 profile default
 aaa authentication eap frad
 aaa authorization user eap cached
 aaa accounting eap frad
```

Accounting-Request (Start)

IKE ID

Client public IP address

```
Acct-Session-Id = "0000001B"
Cisco-AVPair = "isakmp-phase1-id=acvpn"
Cisco-AVPair = "isakmp-initator-ip=192.168.221.129"
Framed-IP-Address = 10.0.1.101
User-Name = "joe@cisco"
Cisco-AVPair = "connect-progress=No Progress"
Acct-Authentic = Local
Acct-Status-Type = Start
NAS-IP-Address = 10.0.0.1
Acct-Delay-Time = 0
```

Assigned IP address

EAP username

Accounting-Request (Stop)

Statistics

```
Acct-Session-Id = "0000001B"
Cisco-AVPair = "isakmp-phase1-id=acvpn"
Cisco-AVPair = "isakmp-initator-ip=192.168.221.129"
Framed-IP-Address = 10.0.1.101
User-Name = "joe@cisco"
Acct-Authentic = Local
Cisco-AVPair = "connect-progress=No Progress"
Acct-Session-Time = 104
Acct-Input-Octets = 13906
Acct-Output-Octets = 11040
Acct-Input-Packets = 207
Acct-Output-Packets = 92
Acct-Terminate-Cause = 0
Cisco-AVPair = "disc-cause-ext=No Reason"
Acct-Status-Type = Stop
NAS-IP-Address = 10.0.0.1
Acct-Delay-Time = 0
```

Remote Access Clients

Remote Access Clients – Overview





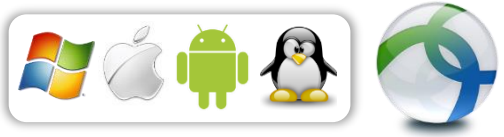
For Your Reference

	AnyConnect (Desktop Version)	AnyConnect (Mobile Version)	Windows Native IKEv2 Client	FlexVPN Hardware Client	strongSwan
Supported OSes	Windows Mac OS X Linux	Android Apple iOS	Windows 7 & 8	Cisco IOS 15.2+ Not on IOS-XE / ASR1k Not on ISR-G1	Linux, Mac OS X, Android, FreeBSD, ...
Supported IKEv2 Authentication Methods	Certificates EAP	Certificates EAP	Certificates EAP	Certificates EAP Pre-Shared Key	Certificates EAP Pre-Shared Key
Supported EAP Authentication Methods	EAP-MSCHAPv2 EAP-GTC EAP-MD5	EAP-MSCHAPv2 EAP-GTC EAP-MD5	EAP-MSCHAPv2 EAP-TLS[1] EAP-PEAP[1] ... and more (Win8)	EAP-MSCHAPv2 EAP-GTC EAP-MD5	EAP-MSCHAPv2 EAP-TLS[1] EAP-PEAP[1] ... and more (plugins)
Security Policy Exchange	Automatic[2] (RRI)	Automatic[2] (RRI)	Automatic[2] (RRI)	Automatic[2] (IKEv2) Dyn. Routing Protocol	Automatic[2] (RRI)
Dual Stack (IPv4 & IPv6)	3.1.05152 (with GRE) IOS-XE planned	Planned (client limitation)	Planned (headend limitation)	Both (with GRE)	Planned (headend limitation)
Split Tunneling	Yes	Yes	Very limited (classful)	Yes	Yes

[1] EAP-TLS, EAP-TTLS, EAP-PEAP and others require (potentially dedicated) TLS certificates on EAP server & RA client
[2] IPSec Reverse Route Injection (RRI) and IKEv2 Route Exchange are enabled by default

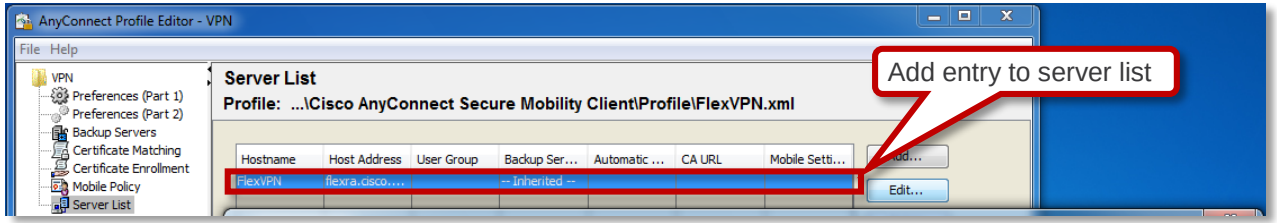
Remote Access Clients
› AnyConnect Secure Mobility Client

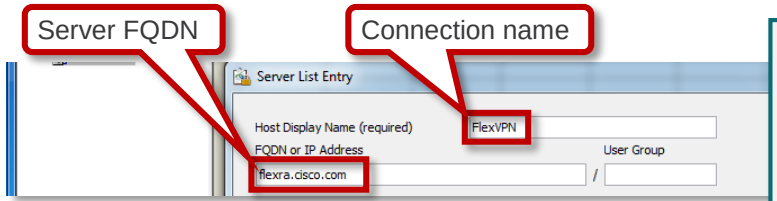
AnyConnect Secure Mobility Client

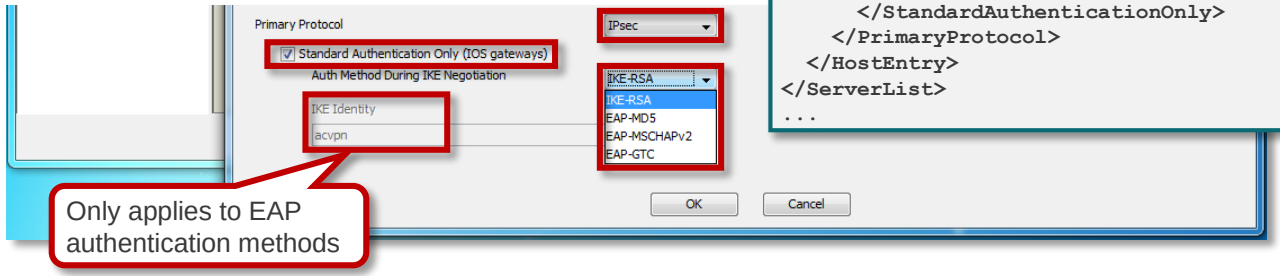


- Since AnyConnect 3.0, IKEv2/IPSec supported
  - Desktop: Windows, Mac OS X, Linux
  - Mobile: Apple iOS, Android
- Supported authentication methods:
  - Machine/User Certificates (RSA signatures)
  - EAP-MSCHAPv2 (password challenge/response, based on MS-CHAPv2)
  - EAP-GTC (cleartext password authentication, used for one-time-passwords/tokens)
  - EAP-MD5 (hash-based authentication)
- Particularities:
  - Requires EAP "*query-identity*" on server (triggers username/password input dialog)
  - Requires "*no crypto ikev2 http-url cert*" on server (aborts the connection otherwise)
  - CSCud96246: incompatibility with IOS when using SHA-2 integrity (resolved in 3.1.05, Dec 2013)

AnyConnect – VPN Profile Editor



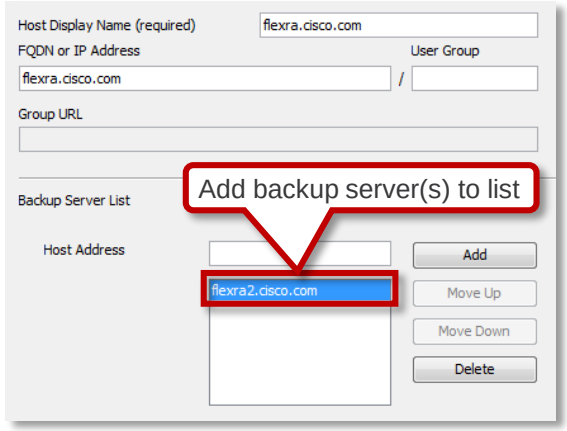


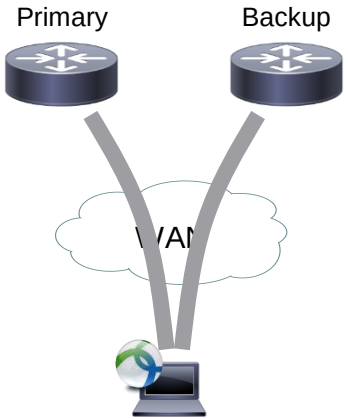


Resulting XML Profile

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

AnyConnect – Backup Server List





Resulting XML Profile

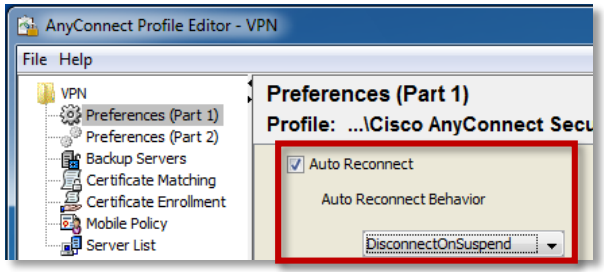
```
...
<ServerList>
  <HostEntry>
    <HostName>FlexVPN</HostName>
    <HostAddress>flexra.cisco.com</HostAddress>
    <BackupServerList>
      <HostAddress>flexra2.cisco.com</HostAddress>
    </BackupServerList>
    ...
```

Primary server stops responding
→ Client will try connecting to backup server(s)

AnyConnect – Seamless Auto-Reconnect

Additional info

- Seamless reconnection after:
  - transient loss of connectivity
  - switching between networks (e.g. moving from 3G to WiFi)
  - suspend/resume computer

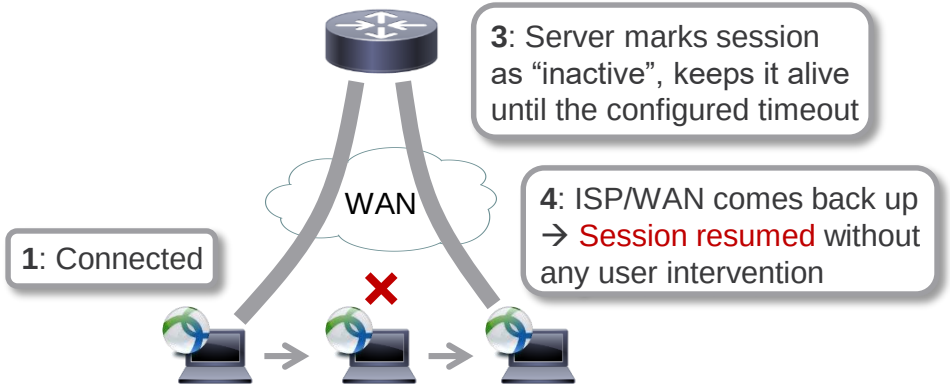


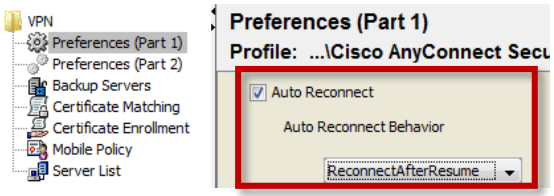

```
crypto ikev2 profile default
 ...
 reconnect [timeout <seconds>]
```

- Supported by AnyConnect desktop & mobile for both SSL & IKEv2
  - FlexVPN server-side support introduced in IOS 15.4(1)T & IOS-XE 15.4(1)S / 3.11S
- Suspend/resume client behavior configurable separately:
  - DisconnectOnSuspend: release VPN session resources upon suspend, do not reconnect
  - ReconnectAfterResume: try to reconnect after operating system resumes
- Proprietary method:
  - Session token exchanged during initial session establishment (configuration exchange)
  - Reconnection attempts use session token as pre-shared key in IKE_AUTH
  - Mutually exclusive with PSK configuration in IKEv2 profile
  - Session expires on server after configured timeout (default: 30 minutes)

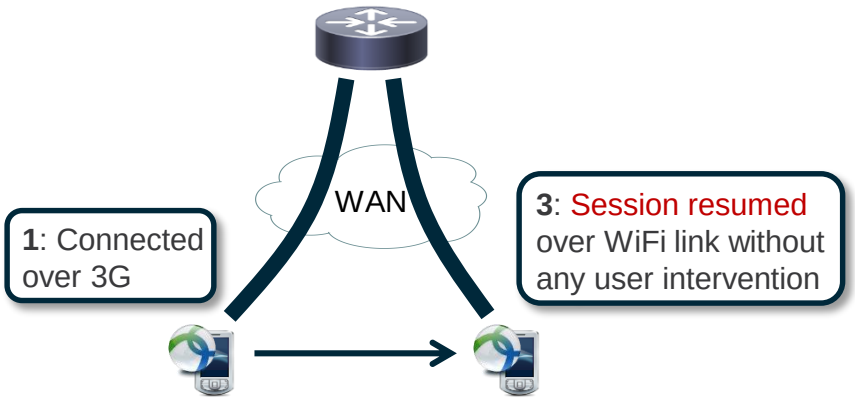
AnyConnect – Seamless Auto-Reconnect

```
crypto ikev2 profile default
 reconnect [timeout <seconds>]
```





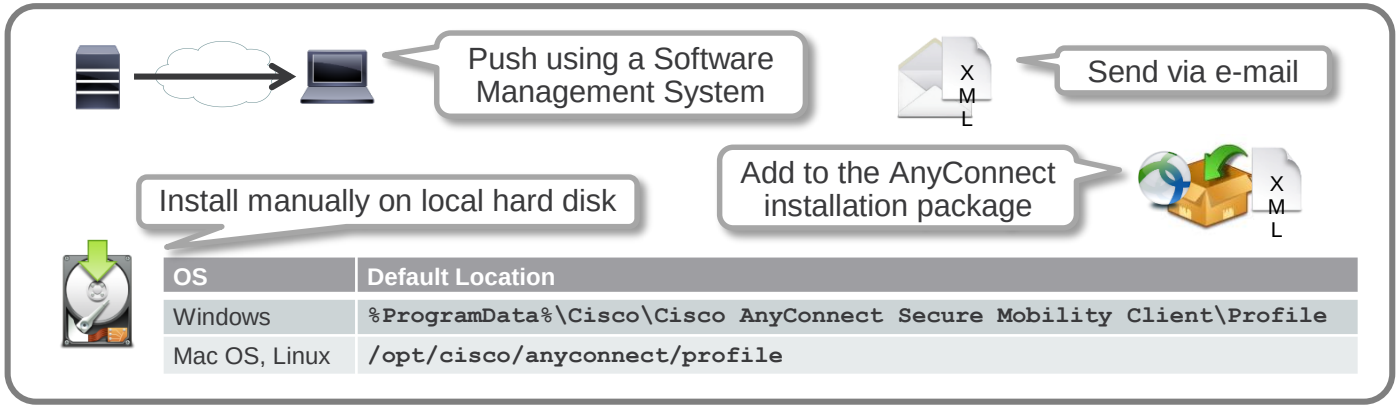

```
crypto ikev2 profile default
 reconnect [timeout <seconds>]
```



Also works when computer suspends & resumes (behavior controllable through XML profile)

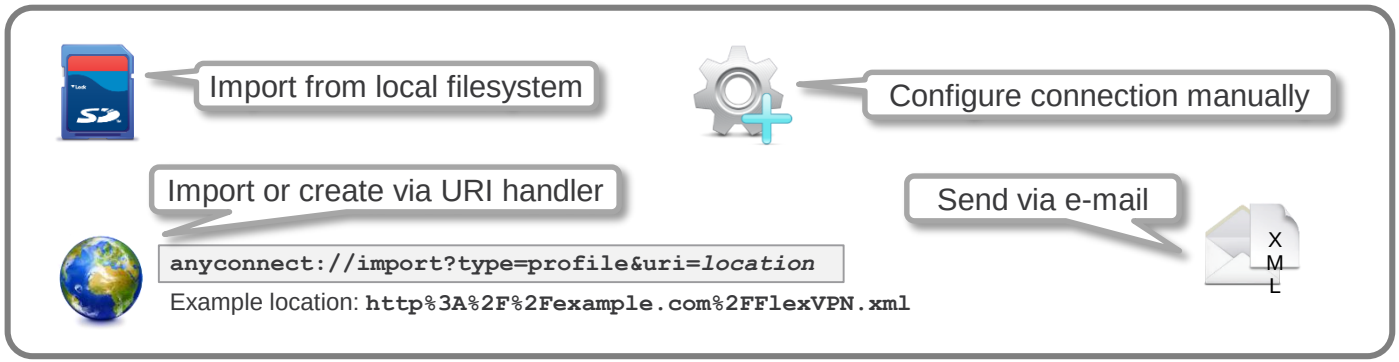
AnyConnect – Profile Deployment Options

AnyConnect Desktop



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

AnyConnect Mobile

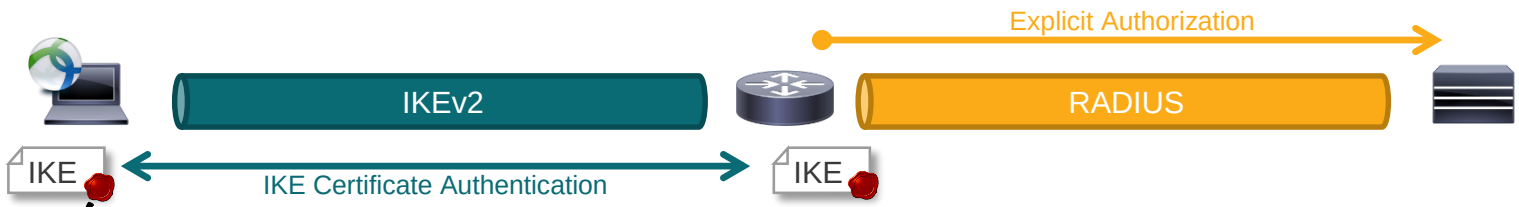


AnyConnect – Mutual RSA Signatures

- Mutual IKE certificate-based authentication
  - AnyConnect picks best available identity certificate
    - Based on selection rules in XML profile (if any)
    - Certificate with EKU preferred over non-EKU
  - Client IKE ID = certificate subject DN
  - Server selects IKE profile based on certificate match
  - Matching is done on certificate itself, not on IKE ID
- Explicit user/group authorization
  - Non-AAA authentication → no cached attributes
  - Extract CN/OU field from DN using name-mangler
  - Retrieve user/group attributes from RADIUS

```
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 frad name-mangler ou
 aaa authorization user cert list frad name-mangler cn
 virtual-template 1
```

```
# Group definition
Eng
  Cleartext-Password := "cisco"
  Cisco-AVPair = "ipsec:dns-servers=10.0.1.1"

# User definition
joe
  Cleartext-Password := "cisco"
  Framed-IP-Address = "10.0.1.101",
  Framed-IP-Netmask = "255.255.255.255"
```

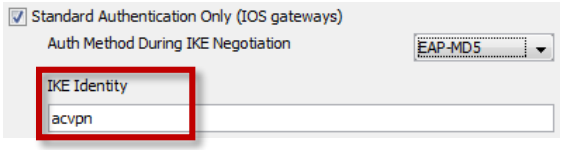


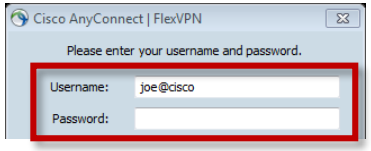
AnyConnect – EAP (All Methods)

- EAP-GTC / EAP-MD5 / EAP-MSCHAPv2
  - Client IKE ID = KEY-ID string configured in XML profile
  - Server selects IKEv2 profile based on KEYID string
  - EAP “query-identity” prompts user for credentials
  - EAP ID = username entered by user
  - Password authentication against AAA user database
  - Returned attributes cached for implicit authorization

```
crypto ikev2 profile default
 match identity remote key-id acvpn
 identity local dn
 authentication remote eap query-identity
 authentication local rsa-sig
 pki trustpoint root sign
 aaa authentication eap frad
 aaa authorization user eap cached
 virtual-template 1
```

```
# User definition
joe@cisco
  Cleartext-Password := "c1sc0!"
  Framed-IP-Address = "10.0.1.101",
  Framed-IP-Netmask = "255.255.255.255",
  Cisco-AVPair = "ipsec:dns-servers=10.0.1.1"
```





AnyConnect – Certificate Requirements

For Your Reference

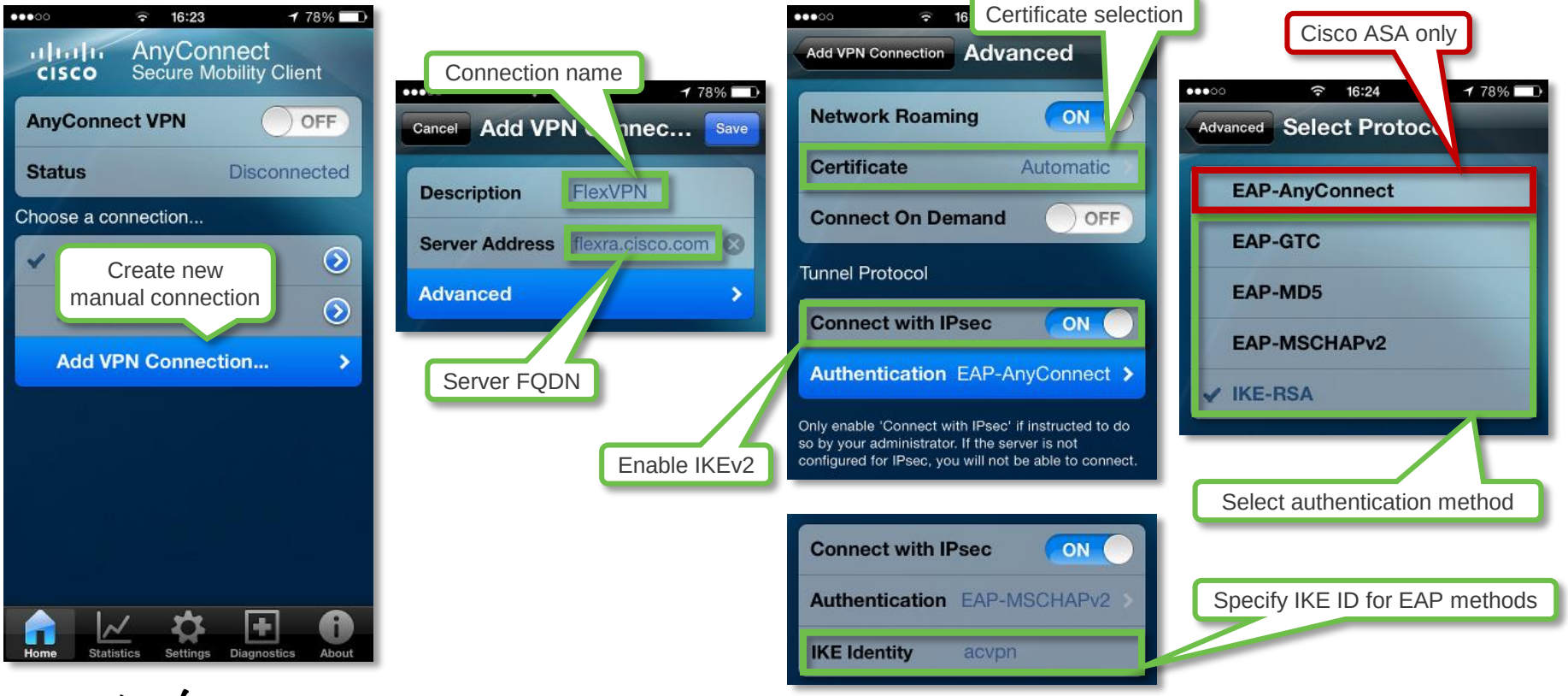
	AnyConnect Client IKEv2 Certificate	FlexVPN Server IKEv2 Certificate
Used for	Mutual RSA-SIG	Mutual RSA-SIG EAP (all types)
Common Name (CN)	Anything	Anything (if SAN field present) Server FQDN (if no SAN field)
Key Usage (KU)	Digital Signature	Digital Signature Key Encipherment or Key Agreement
Extended Key Usage (EKU)	Optional[1,3] If present: TLS Client Authentication	Optional[2,3] If present: TLS Server Authentication or IKE Intermediate
Subject Alternative Name (SAN)	Not required[3]	Optional[3] If present: Server FQDN

- 1 Required in AC 3.0.8 to 3.0.10 (CSCuc07598)
- 2 Required in AC 3.0 (all versions), lifted in 3.1
- 3 Not required: may be omitted or set to any value – Optional: may be omitted or set to the specified value

Demo

Deploying AnyConnect on iPhone via Meraki MDM

AnyConnect Mobile – Manual Connection

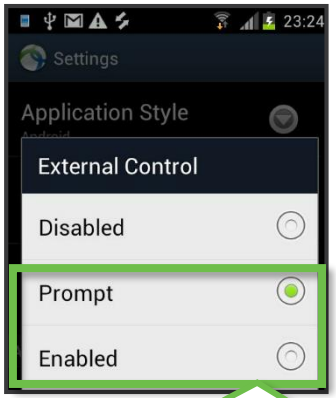


Additional info

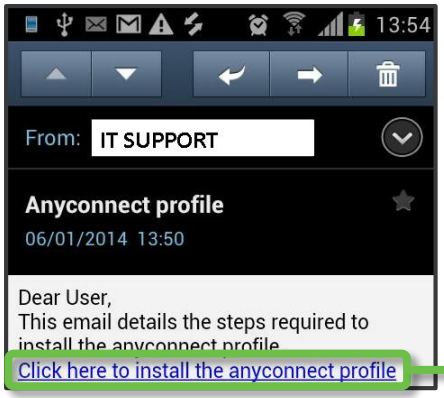
AnyConnect Mobile – URI Handler

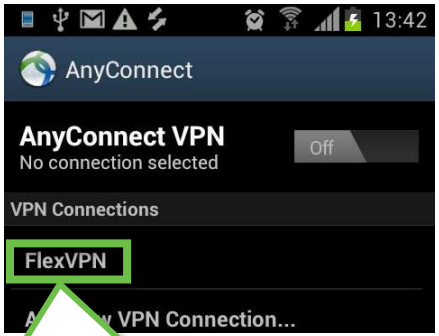
- "anyconnect://" URI handler on Apple iOS & Android
  - Import XML profile
  - Create connection entry
  - Connect & disconnect VPN

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



"Prompt" or "Enabled" required





Connection successfully created

Clients › Piotr's iPad

Client details | Refresh details | Edit details

Name: Piotr's iPad
Model: iPad mini Retina
Serial: F9FMWHSFFCM8
Warranty: Apple
Tags: recently-added
Auto tags: iOS devices
Charge: 23%
Owner: Set an owner

OS

Version: iOS 10.3.1

Security

Encryption: Both file-level and block-level capable
Passcode: Not present
Jailbroken?: No

Management

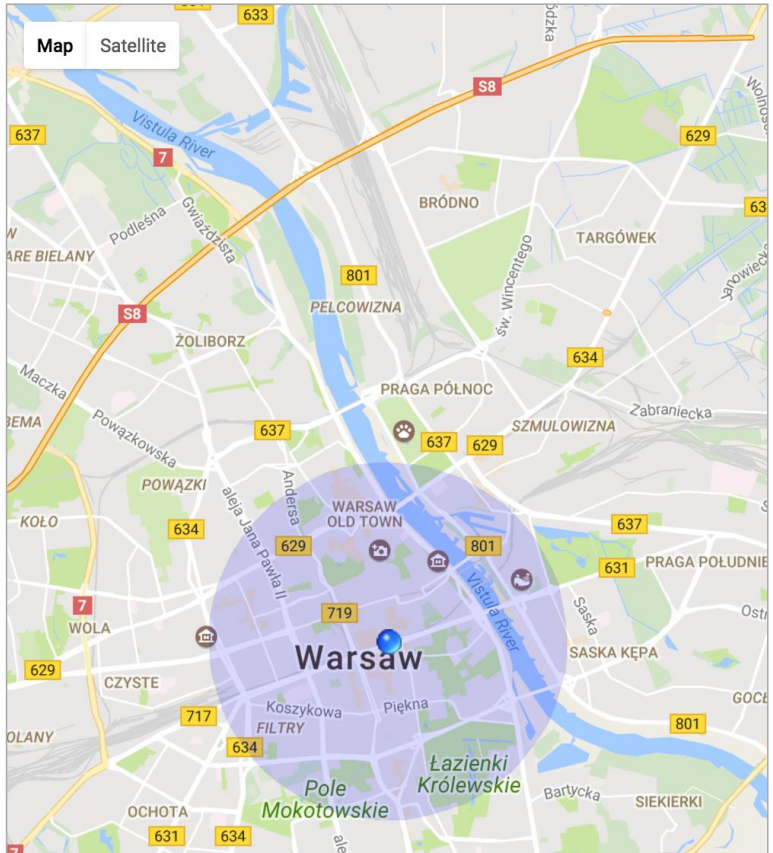
Settings: up-to-date
Apps: up-to-date
Supervised: No
Kiosk application: -
Managed Profile: No
Device Owner: No
Enrollment date: 23:39 Apr 28 2017

Storage

Device storage: 9.0 GB / 11.6 GB 77%

Approximate location | Refresh location

Warszawa, Poland (via IP, updated 10 minutes ago)

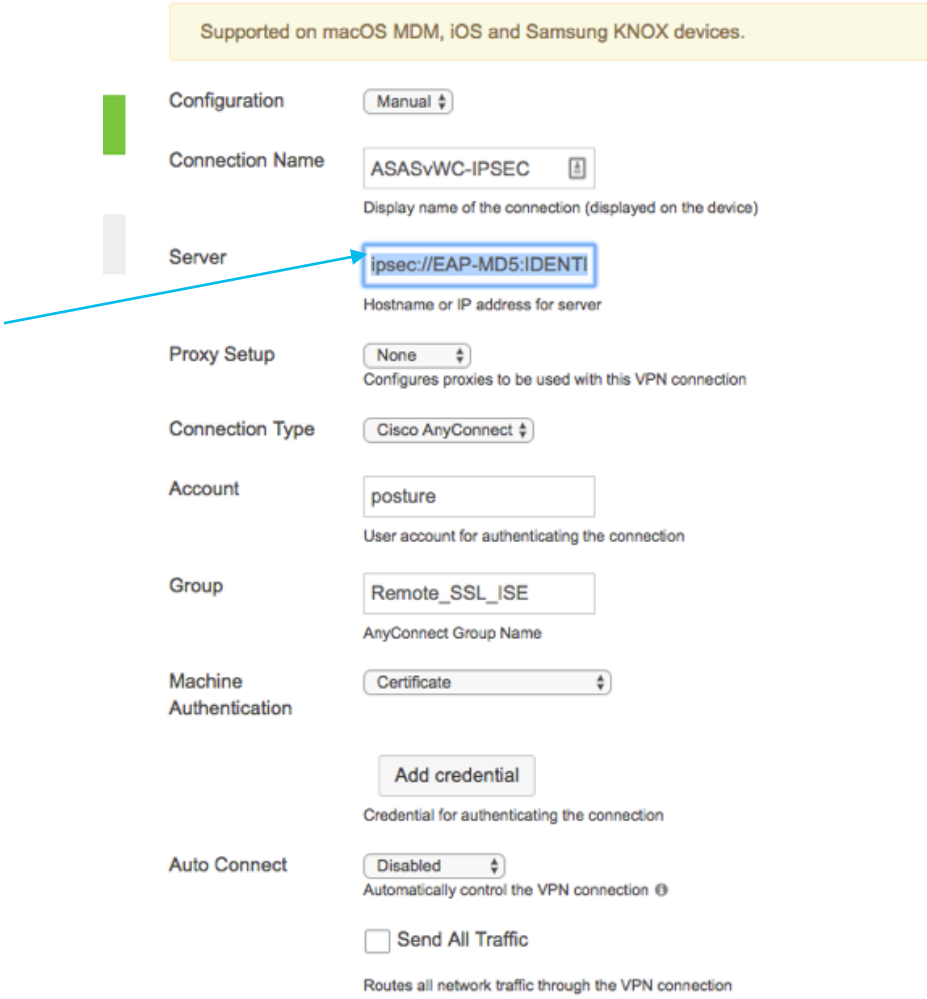


Cisco live!

Creating IPsec AnyConnect profile

[**ipsec**://][<**AUTHENTICATION**>[":"<**IKE-IDENTITY**>"@"]] <**HOST**>[":"<**PORT**>]["/"<**GROUP-URL**>]

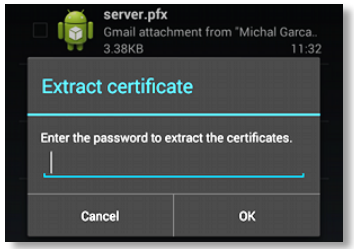
Parameter	Description
ipsec	: Indicates that this is an IPsec connection. If omitted, SSL is assumed.
AUTHENTICATION	Specifies the authentication method for an IPsec connection. If omitted, EAP-AnyConnect is assumed. Valid values are: • EAP-AnyConnect • EAP-GTC • EAP-MD5 • EAP-MSCHAPv2 • IKE-RSA
IKE-IDENTITY	Specifies the IKE identify when AUTHENTICATION is set to EAP-GTC, EAP-MD5, or EAP-MSCHAPv2. This parameter is invalid when used for other authentication settings.
HOST	Specifies the server address. The hostname or IP address to be used.
PORT	Currently ignored, included for consistency with the HTTP URI scheme.
GROUP=URL	Tunnel group name appended to the server name.

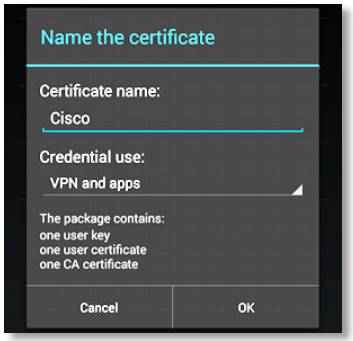


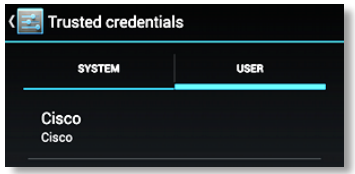
Additional info

AnyConnect Mobile – Certificate Deployment

- Package certificate & keypair into PKCS#12 file
- Apple iOS
  - Import PKCS#12 from URL or email attachment
  - Provision credentials or set up SCEP enrollment using configuration profile (e.g. via iPhone Configuration Utility)
- Android
  - Import PKCS#12 from URL, email or filesystem
  - Use existing credentials from Credential Storage







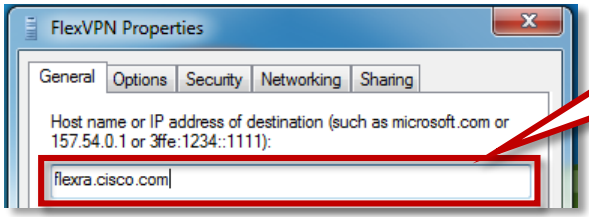
Remote Access Clients
› Windows Native IKEv2 Client

Windows Native IKEv2 Client

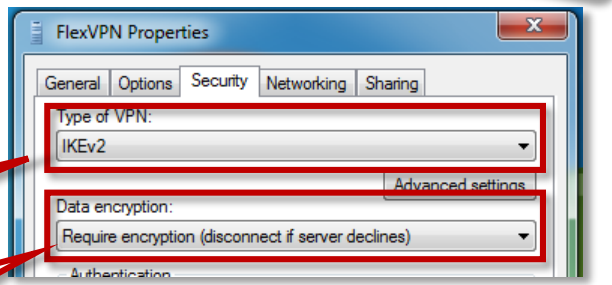
- Since Windows 7, IKEv2/IPsec natively supported for RA connections
- Supported authentication methods:
  - Machine Certificates (RSA signatures)
  - EAP-MSCHAPv2 (password challenge/response, based on MS-CHAPv2)
  - EAP-TLS (certificate authentication, based on TLS handshake)
  - EAP-PEAP (tunnels another EAP method within TLS)
  - EAP-TTLS (Windows 8 – tunnels EAP or non-EAP authentication within TLS)
  - EAP-AKA / EAP-AKA' / EAP-SIM (Windows 8 – SIM card & mobile network authentication)
- Particularities:
  - Requires EAP "*query-identity*" on server (fails to respond to EAP otherwise)
  - Requires *AES-256* in IPsec transform set (current IOS default is AES-128)
  - RSA authentication will fail if more than 100 CA's in client Local Machine Trusted Roots store
  - KB975488: Windows 7 only sends IP address as IKE Identity (except when using certs)
  - KB814394: Certificate requirements for EAP-TLS and PEAP-EAP-TLS
  - KB939616: Certificate keypair lost when copying from user store to machine store

Windows 7 – VPN Connection Settings

For Your Reference



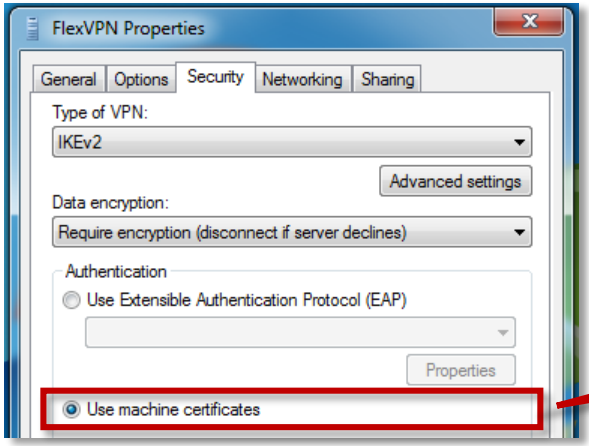
DNS-resolvable FQDN – must be found in:
- ✓ CN/SAN of FlexVPN Server IKE certificate
- ✓ CN of EAP Server TLS certificate



Type of VPN: IKEv2

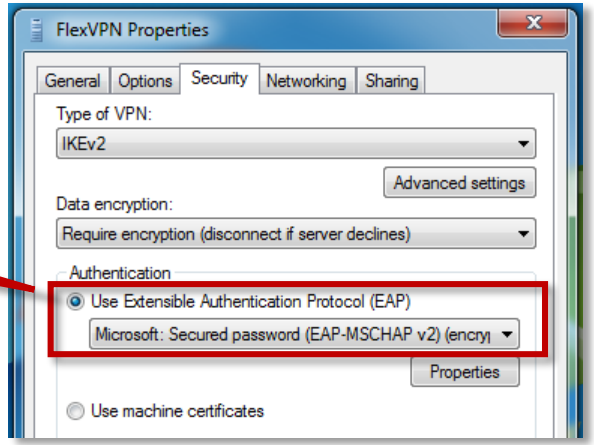
"Require encryption" & "Strongest encryption" require AES-256 in the IPsec transform set

```
crypto ipsec transform-set default esp-aes 256 esp-sha-hmac
```



RSA Signatures

EAP-MSCHAPv2



For Your Reference

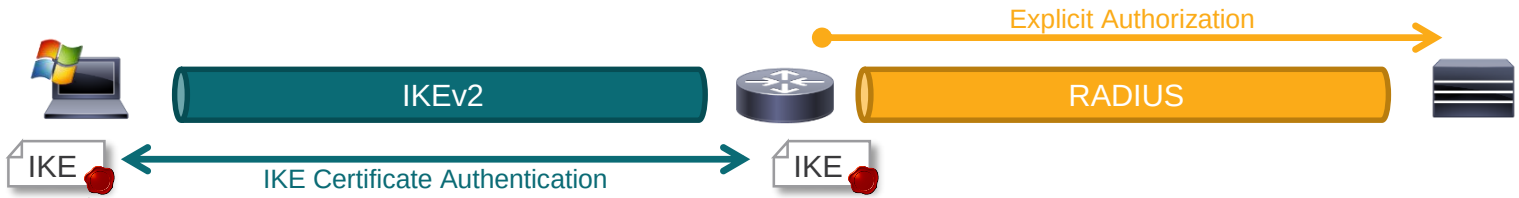
Windows – Mutual RSA Signatures

- Mutual IKE certificate-based authentication
  - Windows can only use local machine certificates
- IKEv2 Profile selection on server
  - Client IKE ID = certificate subject DN
  - Server selects profile based on certificate map
  - Matching is done on certificate itself, not on IKE ID
- Explicit user/group authorization
  - Non-AAA authentication → no cached attributes
  - Extract CN/OU field from DN using name-mangler
  - Retrieve user/group attributes from RADIUS

```
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 frad name-mangler ou
 aaa authorization user cert list frad na      er cn
 virtual-template 1
```

Same as for AnyConnect

```
# Group definition
Eng
  Cleartext-Passwor      "cisco"
  Cisco-AVPair = "ipsec:dns-servers=10.0.1.1"

# User definition
joe
  Cleartext-Password := "cisco"
  Framed-IP-Address = "10.0.1.101",
  Framed-IP-Netmask = "255.255.255.255"
```



Windows – EAP Considerations

- IKEv2 mandates certificate-based server authentication
- Profile selection based on client IKE ID
  - Windows 7 with fix for KB975488: IKE ID = user@domain
    - Selection can be based on “email domain” match
  - Windows 7 w/o fix or 8 w/ regression: IKE ID = client IP address
    - Only option: single IKE profile and VTemplate for all groups
    - Leverage AAA to provide service differentiation
- EAP ID provided by client during authentication
  - Requires “query-identity” (client cannot perform EAP otherwise)
  - EAP server will query AAA database for attributes
  - Attributes can be reused for implicit user authorization
  - Server sends updated EAP ID in final Access-Accept reply (usually same value as the initial client-provided EAP ID)
  - Final EAP ID can be reused for additional authorization if needed

```
crypto ikev2 profile default
 identity local dn
 authentication local rsa-sig
 pki trustpoint root [sign]
```

```
 match identity remote email domain cisco
```

```
 match identity remote address 0.0.0.0
```

```
 authentication remote eap query-identity
 aaa authentication eap frad
 aaa authorization user eap cached
```

```
 aaa authorization group eap list here ...
 ... name-mangler domain
```

Windows 7 – EAP-MSCHAPv2

- EAP-MSCHAPv2
  - EAP ID = user or user@domain
  - Password authentication against EAP server database


```
crypto ikev2 profile default
 match identity remote address 0.0.0.0
 identity local dn
 authentication remote eap query-identity
 authentication local rsa-sig
 pki trustpoint root sign
 aaa authentication eap frad
 aaa authorization user eap cached
 virtual-template 1
```

Same for all EAP

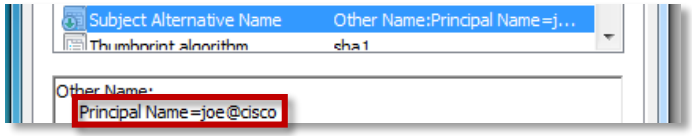
```
# User definition
joe@cisco
  Cleartext-Password := "c1sc0!"
  Framed-IP-Address = "10.0.1.101",
  Framed-IP-Netmask = "255.255.255.255",
  Cisco-AVPair = "ipsec:dns-servers=10.0.1.1"
```

Windows 7 – EAP-TLS

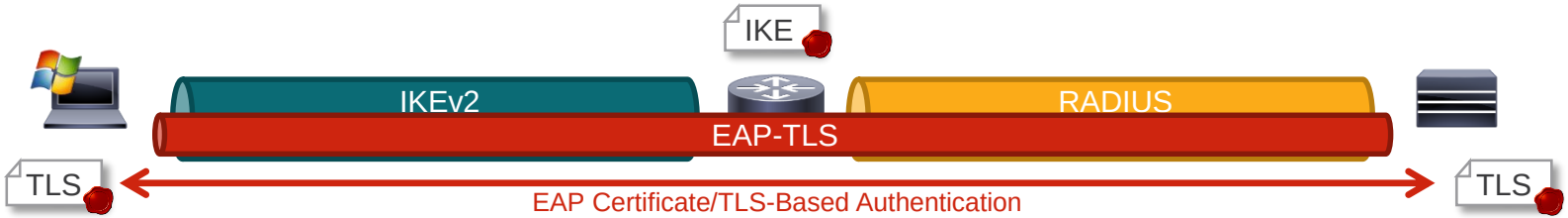
- EAP-TLS
  - Client performs TLS handshake w/ EAP server
  - Mutual authentication using TLS certificates
  - Client authentication mandatory (unlike EAP-PEAP)
  - EAP ID = TLS certificate UPN (or CN if none)

```
crypto ikev2 profile default
 match identity remote address 0.0.0.0
 identity local dn
 authentication remote eap query-identity
 authentication local rsa-sig
 pki trustpoint root sign
 aaa authentication eap frad
 aaa authorization user eap cached
 virtual-template 1
```

Same for all EAP

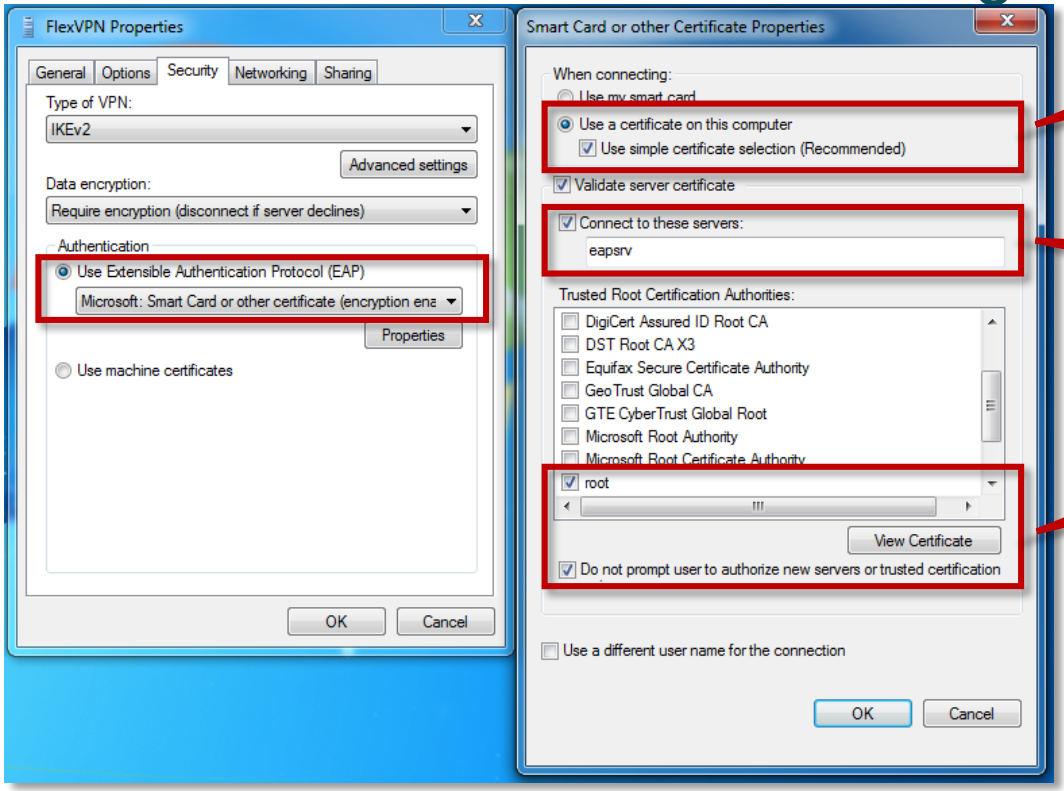



```
# User definition
joe@cisco
  Cleartext-Password := "c1sc0!"
  Framed-IP-Address = "10.0.1.101",
  Framed-IP-Netmask = "255.255.255.255",
  Cisco-AVPair = "ipsec:dns-servers=10.0.1.1"
```



For Your Reference

Windows 7 – EAP-TLS Settings



Get certificate from Current User certificate store

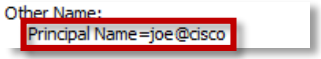
Server name – must be found in CN of EAP Server TLS certificate

Trusted root authorities for EAP server authentication

Windows 7 – EAP-PEAP

Additional info

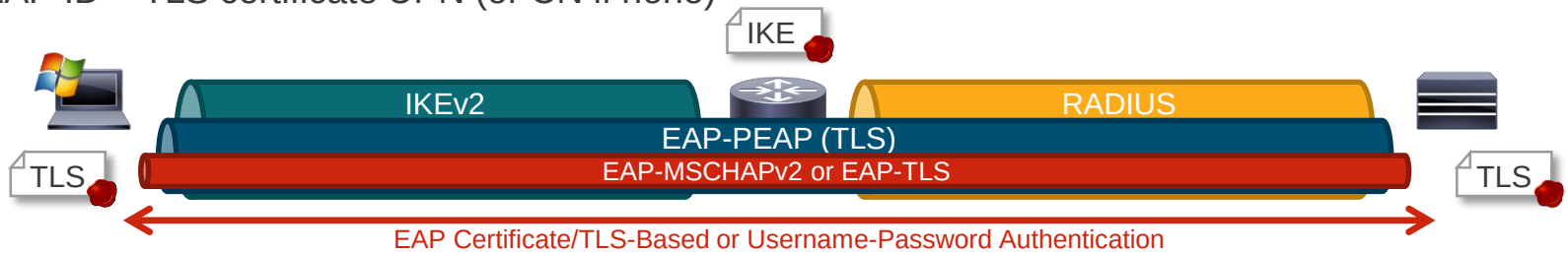
- EAP-PEAP
  - Client performs TLS handshake w/ EAP server
  - Client authenticates EAP server using TLS certificate
  - Provides protection for inner EAP exchange
  - Inner (tunneled) EAP method authenticates the user
  - Outer EAP method returns user attributes to server
- Tunneled EAP-MSCHAPv2
  - EAP ID = user or user@domain
- Tunneled EAP-TLS
  - EAP ID = TLS certificate UPN (or CN if none)




```
crypto ikev2 profile default
 match identity remote address 0.0.0.0
 identity local dn
 authentication remote eap query-identity
 authentication local rsa-sig
 pki trustpoint root sign
 aaa authentication eap frad
 aaa authorization user eap cached
 virtual-template 1
```

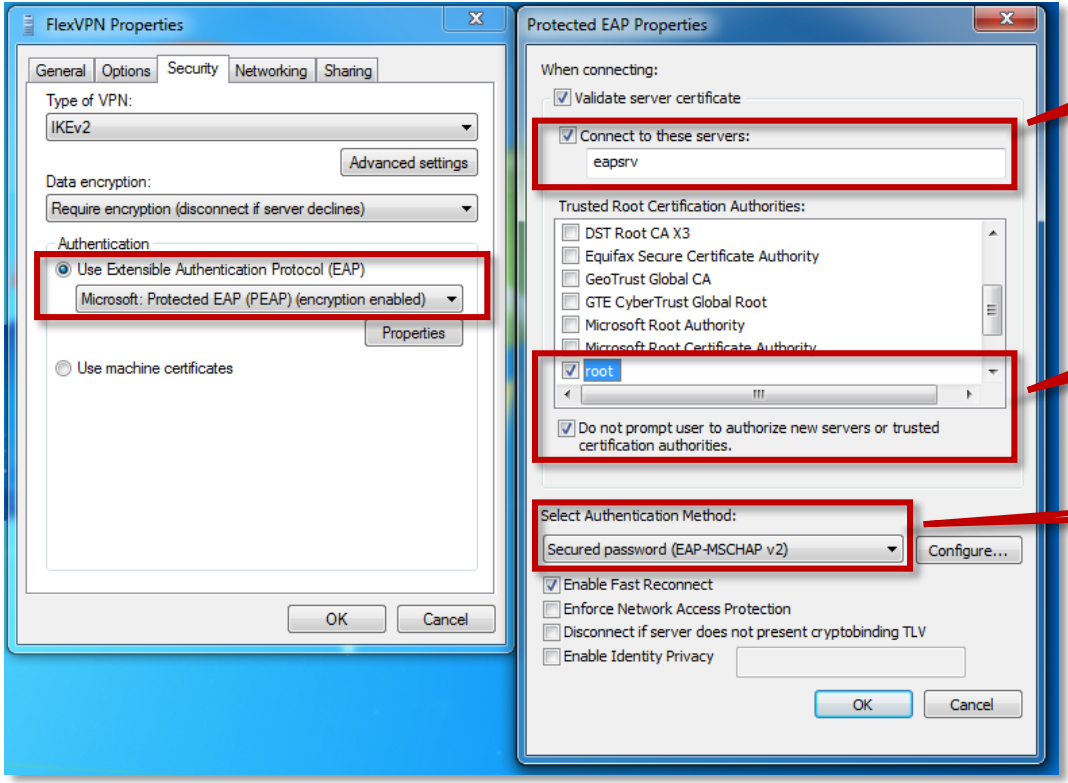
Same for all EAP

```
# User definition
joe@cisco
  Cleartext-Password := "c1sc0!"
  Framed-IP-Address = "10.0.1.101",
  Framed-IP-Netmask = "255.255.255.255",
  Cisco-AVPair = "ipsec:dns-servers=10.0.1.1"
```



Windows 7 – EAP-PEAP Settings

Additional info



Server name – must be found in CN of EAP Server TLS certificate

Trusted root authorities for EAP server authentication

Inner (tunneled) EAP method

For Your Reference

Windows 7 – Certificate Requirements

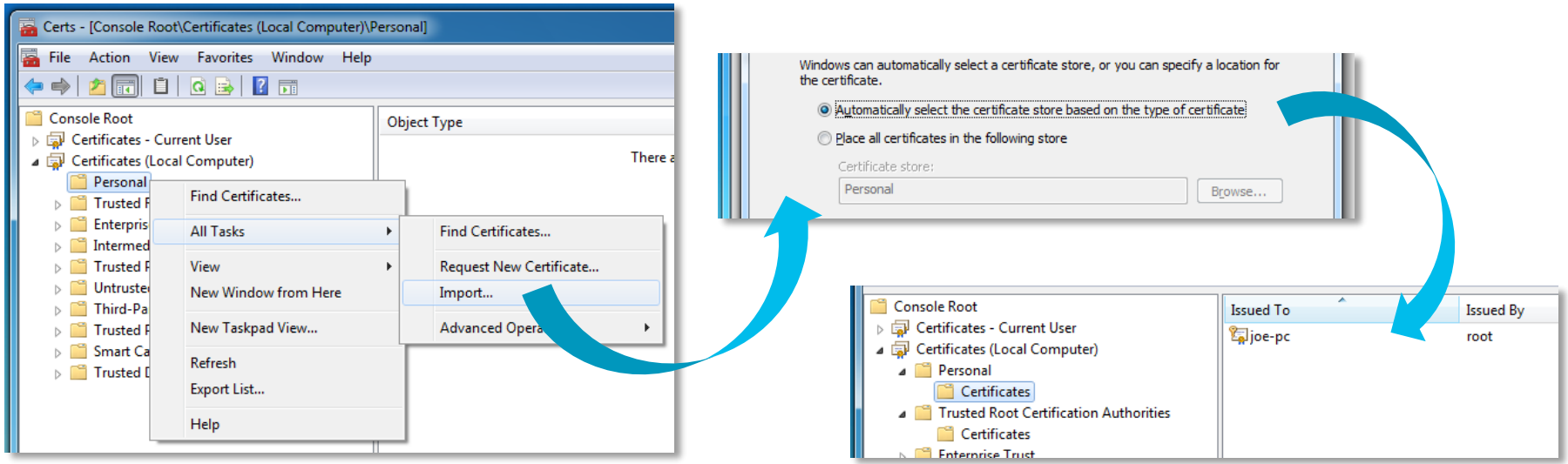



	Win7 Client IKEv2 Certificate	FlexVPN Server IKEv2 Certificate	Win7 Client TLS Certificate	EAP Server TLS Certificate
Used for	Mutual RSA-SIG	Mutual RSA-SIG EAP (all types)	EAP-TLS EAP-PEAP (optional)	EAP-TLS EAP-PEAP
Certificate Store	Local Computer	N/A	Current User	N/A
Common Name (CN)	Anything	Anything (if SAN field present) Server FQDN (if no SAN field)	Anything (if UPN present) user@domain (if no UPN[2])	Server name (as configured in Client EAP Settings)
Key Usage (KU)	Digital Signature	Digital Signature	Digital Signature	Digital Signature Key Encipherment
Extended Key Usage (EKU)	Not required[1]	TLS Server Authentication	TLS Client Authentication	TLS Server Authentication
Subject Alternative Name (SAN)	Not required[1]	Optional[1] If present: Server FQDN	Optional[1] If present: UPN[2]	Server FQDN

- 1 Not required: may be omitted or set to any value – Optional: may be omitted or set to the specified value
- 2 UPN (User Principal Name): Microsoft proprietary “user@domain” SAN extension (OID 1.3.6.1.4.1.311.20.2.3)

Windows 7 – Certificate Import

- Client keypair & certificate can be issued by CA and provisioned to client PC
- Import keypair, identity cert and issuer cert from PFX / PKCS#12 package
- Due to KB939616, machine IKEv2 cert must be imported explicitly into machine store



Remote Access Clients
› FlexVPN Client

FlexVPN Client – Overview

- IKEv2 initiation on IOS can be driven by the FlexVPN Client Profile CLI construct
- Supported authentication methods:
  - Certificates (RSA signatures)
  - EAP-MSCHAPv2 (password challenge/response, based on MS-CHAPv2)
  - EAP-GTC (cleartext password authentication, used for one-time-passwords/tokens)
  - EAP-MD5 (hash-based authentication)
  - Pre-Shared Keys
- Routing on FlexVPN server and client:
  - IKEv2 Routing (bidirectional Configuration Exchange)
  - Dynamic Routing Protocol (optional, bootstrapped through IKEv2 Routing)
- IPv4/IPv6 mixed-mode & dual-stack supported using GRE/IPsec interfaces
- More than a Remote Access client, useful also in hub-and-spoke designs where advanced initiator logic is required (dial backup, object tracking, ...)

FlexVPN Client – Example

- Sample configuration:
  - Static tunnel interface driven by FlexVPN Client Profile
  - Local AAA authorization (default IKEv2 author. policy)
  - Certificate-based mutual authentication (no EAP)
  - Single peer (name resolution of FQDN on connection)
- Tunnel interface configuration:
  - IP address assigned through IKEv2 Configuration Exchange
  - Tunnel destination set dynamically by FlexVPN Client logic
  - IKEv2/IPsec initiation triggered by FlexVPN Client logic
- Default IKEv2 routing between client & server:
  - Client advertises route for Tunnel0 assigned IP address
  - Client installs prefixes advertised by server (egress → Tun0)

```
client#show crypto ikev2 authorization policy default
 IKEv2 Authorization Policy : default
  route set interface
  route accept any tag : 1 distance : 1
```

```
aaa new-model
aaa authorization network flex_local local
!
crypto pki trustpoint root
 rsakeypair root
!
crypto ikev2 profile default
 match identity remote any
 identity local dn
 authentication remote rsa-sig
 authentication local rsa-sig
 pki trustpoint root
 aaa authorization group cert list flex_local default
!
crypto ikev2 client flexvpn flexra
  peer 1 fqdn flexra.cisco.com dynamic
  client connect Tunnel0
!
interface Tunnel0
 ip address negotiated
 tunnel source Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile default
```

FlexVPN Client

For Your Reference

```
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 reactivate
peer <n> <ip>
peer <n> <ip> track <x>
peer <n> <fqdn> [dynamic [ipv6]]
peer <n> <fqdn> [dynamic …] track <x>
```

Switch back

N^{th} source selected only if corresponding track object is up

RADIUS Backup List Attribute

`ipsec:ipsec-backup-gateway`

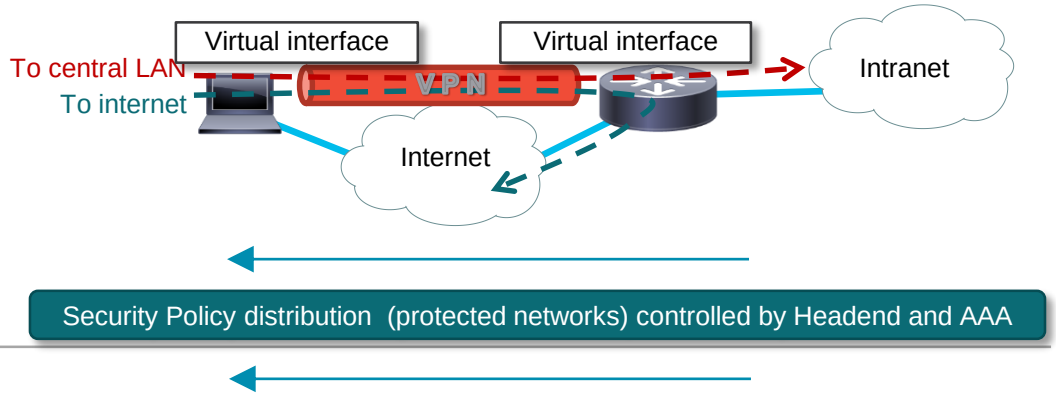
Up to 10 backup gateways pushed by config-exchange

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

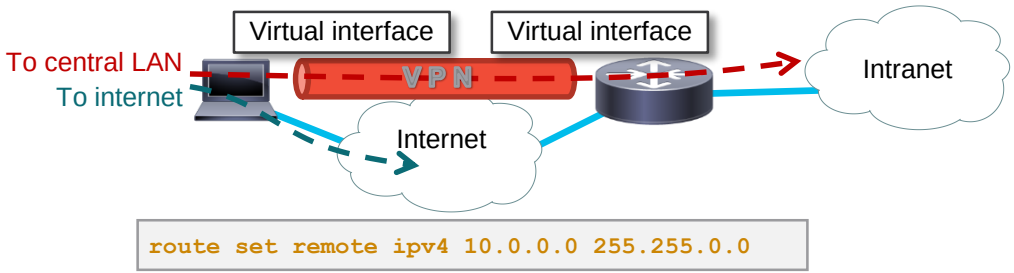
Scenarios & Use Cases
› Full & Split Tunneling

Remote Access Security policy – Full & Split Tunneling

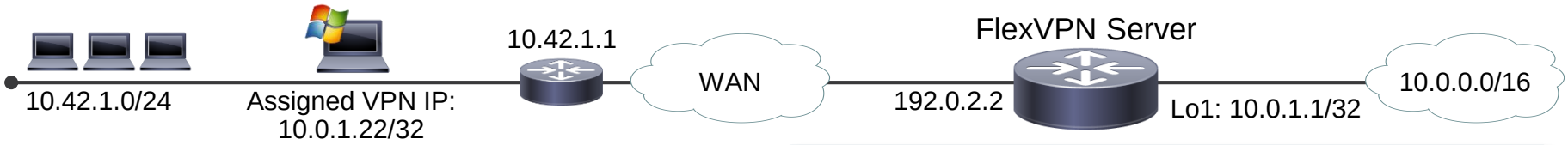
Client Routing Table – Full Tunneling	
Default	Virtual Interface
Local LAN	LAN Interface



Client Routing Table – Split Tunneling	
Default	LAN Interface
Server-Side Networks	Virtual Interface



Scenario: Windows – Full Tunneling




```
IPv4 Route Table
===========================================================================
   Destination        Gateway  Interface
     0.0.0.0/0     10.42.1.1  Local Area Connection
     0.0.0.0/0       On-link  FlexVPN Connection
   192.0.2.2/32   10.42.1.1  Local Area Connection
   10.42.1.0/24      On-link  Local Area Connection
```

Default route changed to point through VPN tunnel

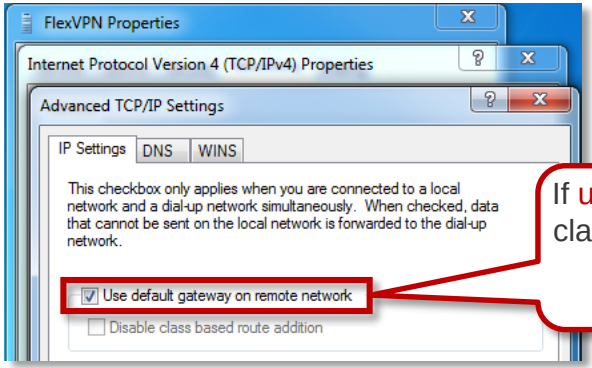
Local LAN still reachable

Server reachable in the clear via ISP

Assigned IP address reachable over client VA (automatic – RRI)

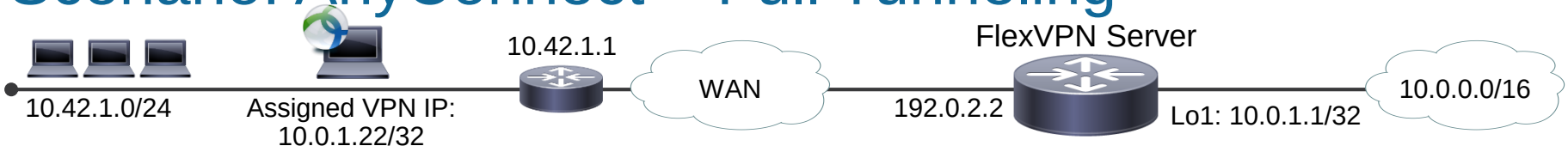
```
S        10.0.1.22/32 is directly connected, Virtual-Access1
```

```
interface Loopback1
 ip address 10.0.1.1 255.255.255.255
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
```



If un-checked: default route replaced with a single classful route based on assigned VPN IP address (e.g. 10.0.0.0/8 → 10.0.1.22) = rudimentary split tunneling

Scenario: AnyConnect – Full Tunneling




```
IPv4 Route Table
===========================================================
   Destination        Gateway  Interface
     0.0.0.0/0      10.42.1.1  Local Area Connection
     0.0.0.0/0        On-link  FlexVPN Connection
   192.0.2.2/32     10.42.1.1  Local Area Connection
   10.42.1.0/24       On-link  Local Area Connection
```

Default route changed to point through VPN tunnel

Local LAN removed from routing table

Server in the clear via ISP

```
S        10.0.1.22/32 is directly connected, Virtual-Access1
```

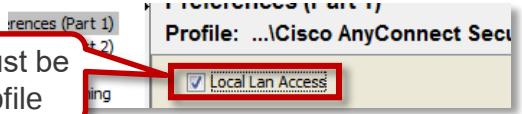
```
interface Loopback1
 ip address 10.0.1.1 255.255.255.255
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
```

To enable full tunneling with local LAN access:
IOS "include-local-lan" attribute not supported by AnyConnect → use RADIUS-only Cisco-AV-Pair "ipsec:split-exclude" with special value 0.0.0.0/32

```
Cisco-AVPair += "ipsec:split-exclude=0.0.0.0/255.255.255.255"
```

(supported in 15.2(4)M6, 15.2(4)S5 and 15.4(2)T/S onwards)

In addition, "Local Lan Access" must be enabled in AnyConnect XML Profile



Scenario: AnyConnect – Split Tunneling

Specific route(s) pointing through VPN tunnel

```
IPv4 Route Table
==========================================================================
   Destination        Gateway  Interface
     0.0.0.0/0      10.42.1.1  Local Area Connection
   10.0.0.0/16        On-link  FlexVPN Connection
  10.42.1.0/24        On-link  Local Area Connection
```

Local LAN still reachable

Authorization: one or more subnets to include in split tunnel

```
route set remote ipv4 10.0.0.0 255.255.0.0
```

```
S        10.0.1.22/32 is directly connected, Virtual-Access1
```

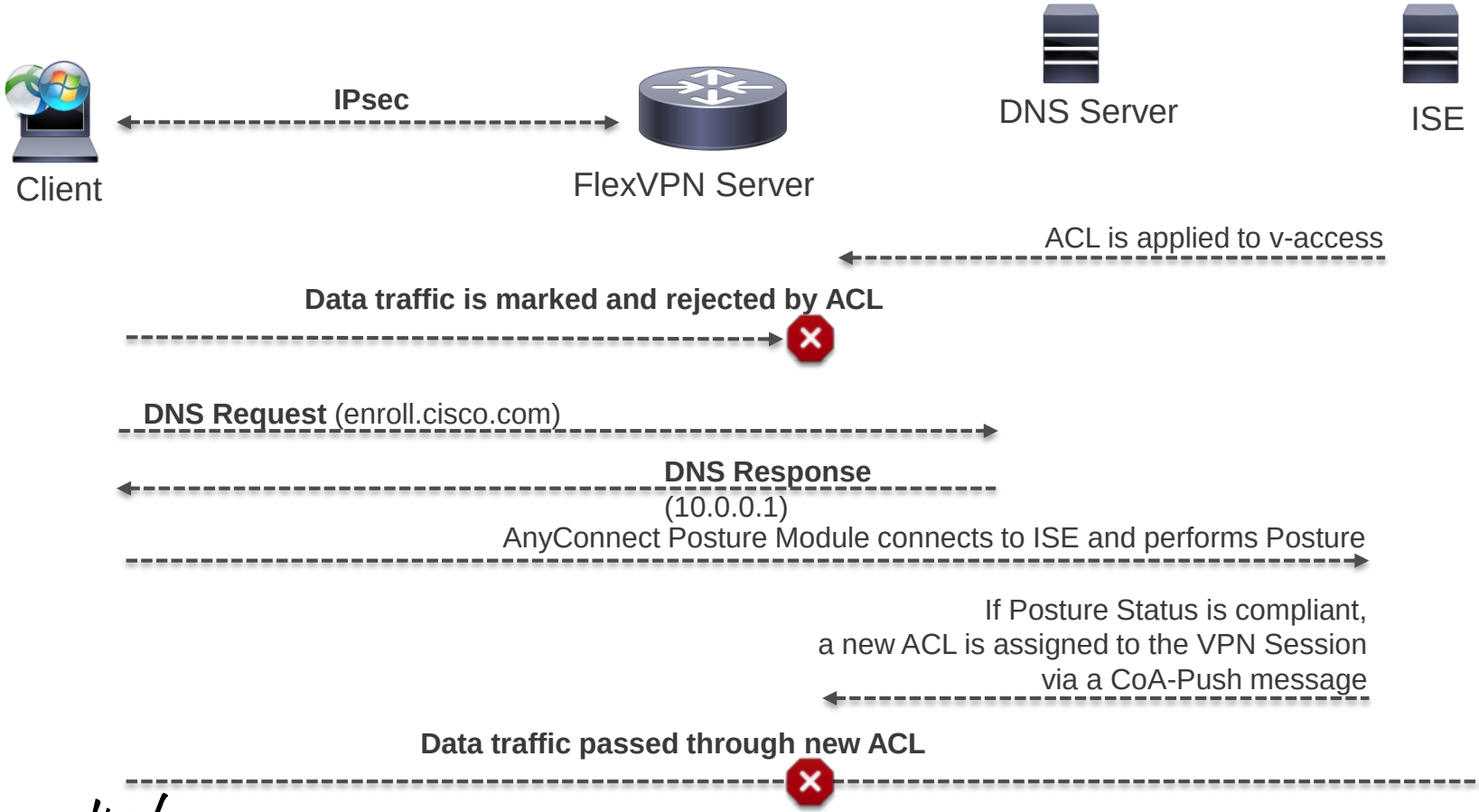
```
interface Loopback1
 ip address 10.0.1.1 255.255.255.255
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback1
```

Split tunnel policy pushed by server within IKEv2 Config Exchange

Original default gateway used for internet traffic + server reachability

Scenarios & Use Cases
› Posture

Posture Flow



COA-PUSH=TRUE

Other Attributes

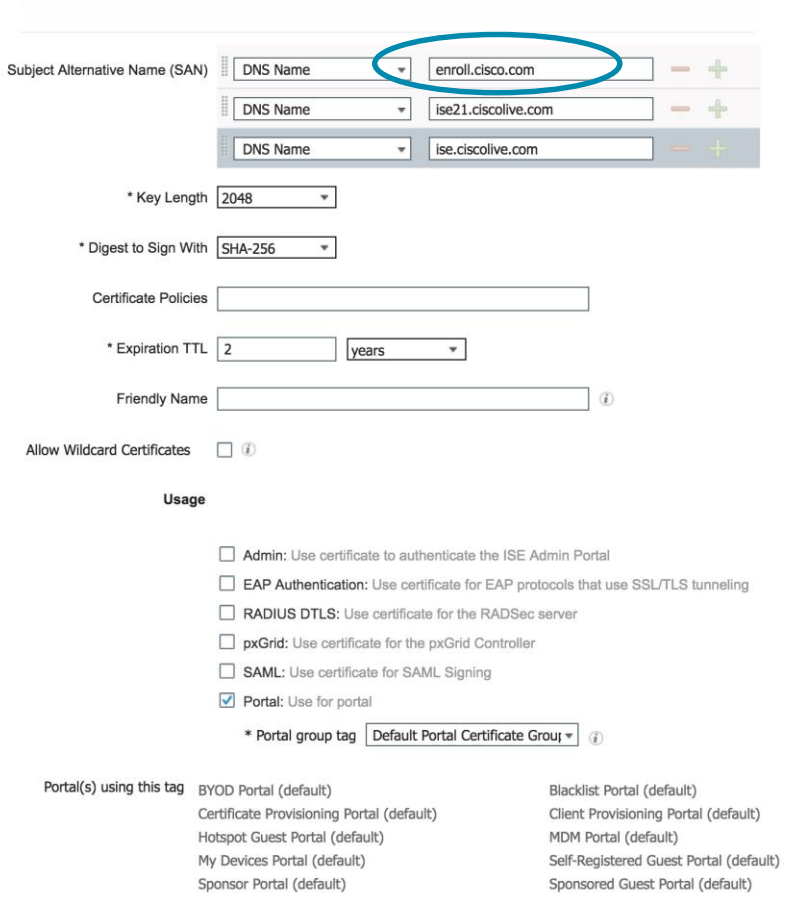
ConfigVersionId	144
Acct-Session-Id	00000FF0
Event-Timestamp	1494755828
NetworkDeviceProfileName	Cisco
Device CoA type	Cisco CoA
Device CoA port	1700
NetworkDeviceProfileId	403ea8fc-7a27-41c3-80bb-27964031a08d
IsThirdPartyDeviceFlow	false
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
Device IP Address	172.16.140.101
CiscoAVPair	ip:interface-config=cts role-based sgt-map sgt 3, ipsec:addr-pool=LOCAL_POOL, ipsec:dns-servers=1.1.1.1, audit-session-id=L2L4AC108C65ZO2L4AC108CDAZH1194C17AZN59

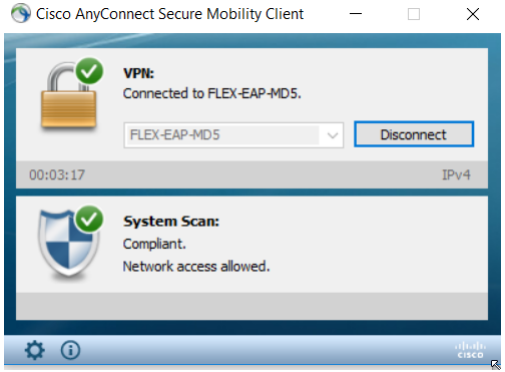
Authorization Policy	Authorization Profiles
Authorization Policy	Authorization Profiles
	RA_COMPLIANT
VPN >> RA_NOT_COMPLIANT	RA_NOT_COMPLIANT

POSTURE – AAA Requirements

- Accounting (!)
- DNS: enroll.cisco.com -> one of PSNs (*working only since ISE 2.2)
- VPN Downloader needs to be enabled (for Compliance Module download)
- enroll.cisco.com in SAN of Posture Certificate
- For TrustSec on IOS we need to have aaa-group ISE with PAC inside

Certificate requirements

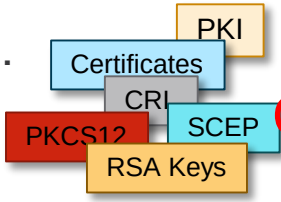




Scenarios & Use Cases
› Certificates or PSK ?

RSA or PSK ?

Certificates sometimes might be complicated …



Complicated!!

- How to renew certificates?
- How to revoke certificates ?
- How to grant certificates ?
- How to backup keys and certificates ?
- Should I use ECDSA (which EC curve) or RSA certificate ?

Pre-Shared Keys are secure if unique keys are used per spoke …

Possible with FlexVPN!

BAD!!

```
peer all-of-my-peers
  address 0.0.0.0 0.0.0.0
  pre-shared-key cisco123
```

AAA Pre-Shared Keys – Packet Flow

FlexVPN Client
IKEv2 Initiator
RADIUS Client

```
crypto ikev2 profile default
 identity local fqdn r1.cisco.com
```

FlexVPN Server
IKEv2 Responder
RADIUS NAS

```
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 keyring aaa list radius
```

AAA Server
RADIUS Server

IKEv2 (IKE_AUTH)
IDi, AUTH(PSK), ...

IKEv2 ID: r1.cisco.com → **AAA** → AAA Username: r1.cisco.com

RADIUS (Access-Request)
User-Name: r1.cisco.com
Password: cisco

configurable

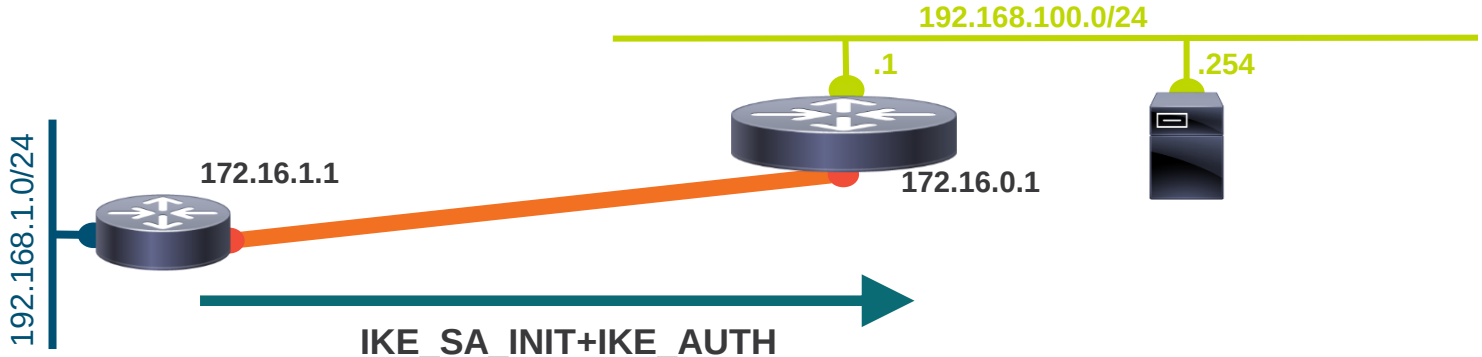
IKEv2 (IKE_AUTH)
IDr, AUTH(PSK), ...

RADIUS (Access-Accept)
Local PSK = cisco!
Remote PSK = !ocsic
Other user attributes for r1.cisco.com

Cached for authorization

Scenarios & Use Cases
› Hub & Spoke

Hub & Spoke – IKEv2 Routing



IKE_SA_INIT+IKE_AUTH

CFG_REQUEST

CFG_REPLY

CFG_SET

CFG_SET_ACK

Interfaces

Ethernet0/0: 172.16.1.1
Ethernet0/1: 192.168.1.1
Tunnel0: **10.0.0.2**

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
192.168.0.0/16 → Null0
10.0.0.1/32 → VirtualAccess1
192.168.1.0/24 → VirtualAccess1

Hub & Spoke – HUB's configuration

Accept connections from Spokes

```
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn Hub.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 access-list ike-policy
 !
ip access-list regular ike-policy
 permit 192.168.0.0 0.0.255.255
```

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

Defines which prefixes should be protected

Virtual-Template configuration

```
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 tunnel protection ipsec profile default
!
interface Loopback0
 ip address 10.0.0.254 255.255.255.255
!
```

Hub & Spoke – Spoke's configuration

```
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
```

Needed for tunnel address exchange

```
crypto ikev2 authorization policy default
 route set interface
 route set interface e0/1
```

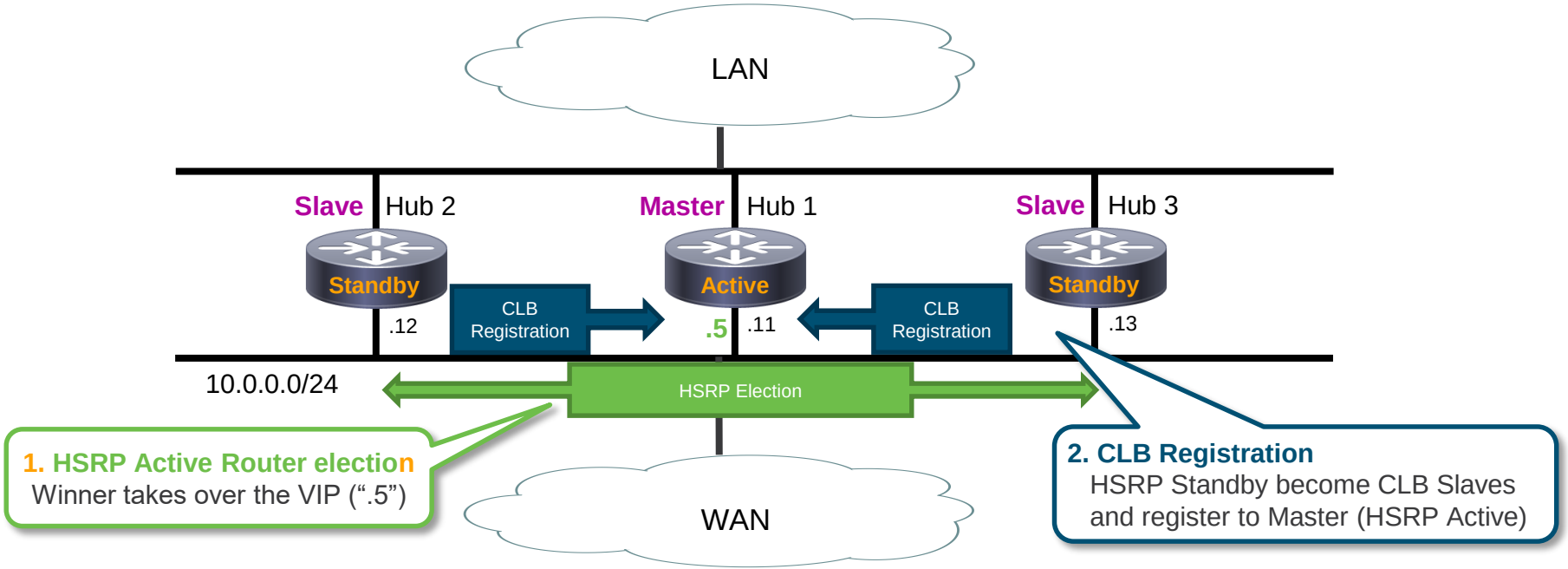
Advertising it's LAN Interface (192.168.1.0/24)

Tunnel to Hub

```
interface Tunnel0
 ip address 10.0.0.2 255.255.255.255
 tunnel source Ethernet0/0
 tunnel destination 172.16.0.1
 tunnel protection ipsec profile default
!
```

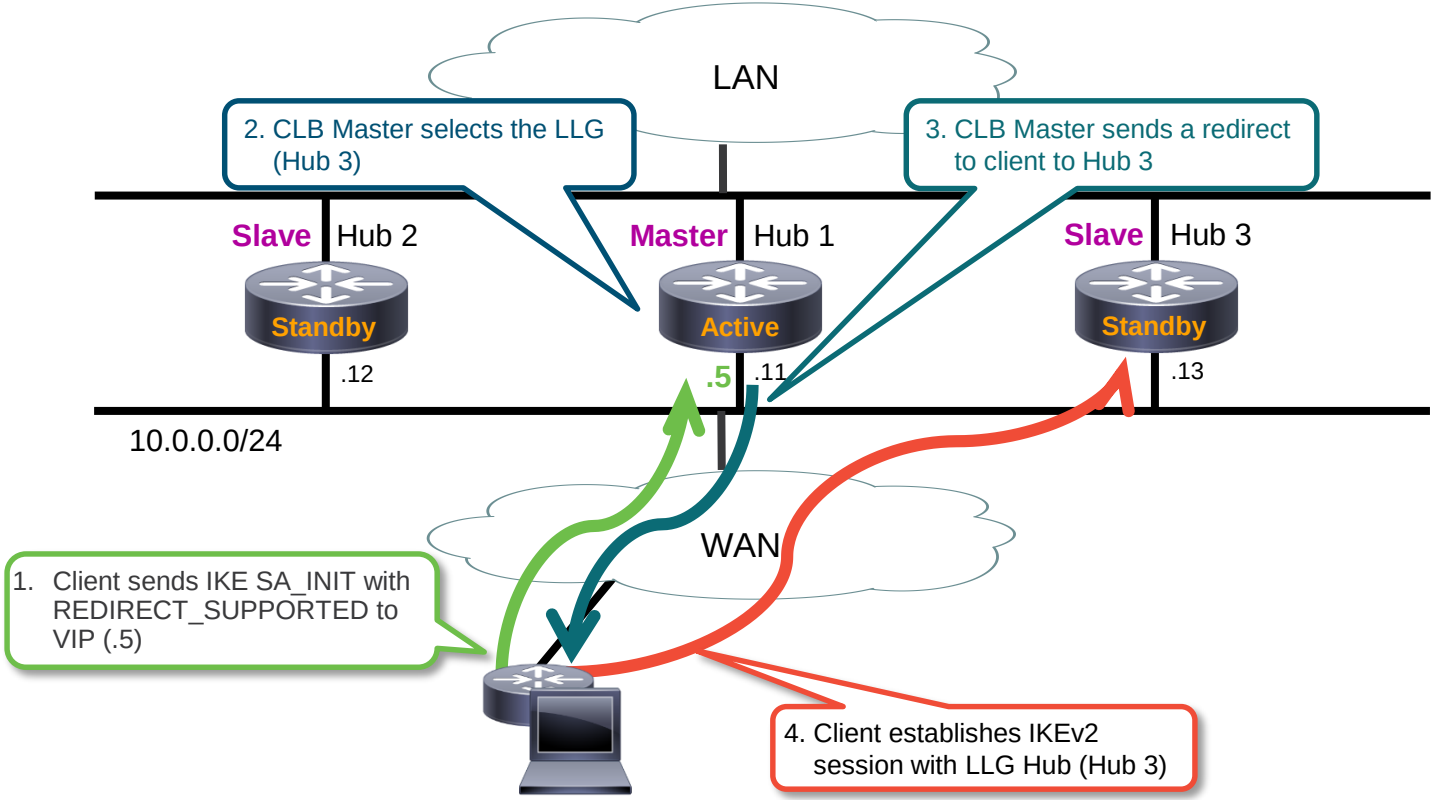
Scenarios & Use Cases
› FlexVPN Load Balancer

FlexVPN Load-Balancer Bootstrap




```
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 Load-Balancer Client Connection



For Your Reference

FlexVPN Load-Balancer – Hub 1 Configuration

```
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

FlexVPN 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
```

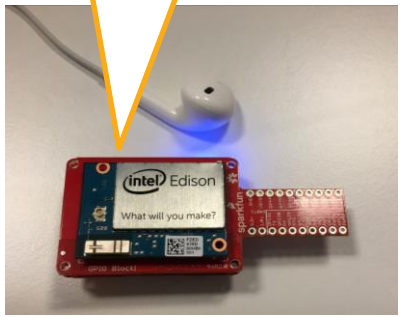
FlexVPN Peer configured with the VIP address **only**

Wrapping up...

Spotlight on ESR & IR platforms

- ESR – Embedder Services Routers
- Regular IOS
- Mobile networks in vehicles, mobile users, harsh environments
- 3 ESR models – 5915, **5921** (runs on Linux!) and 5940
- 3 IR models – IR 809, IR819 & IR 829 – ruggedized fog-computing platforms

ESR5921 Bring Your Own Hardware



IR 809

IR 829

ESR5915

Complete Your Online Session Evaluation

- Give us your feedback to be entered into a Daily Survey Drawing. A daily winner will receive a $750 gift card.
- Complete your session surveys through the Cisco Live mobile app or on www.CiscoLive.com/us.

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

Cisco live!

Thank you


cisco
You're
Cisco live!