Обзор решения FlexVPN. Часть 2

Юрий Дышлевой
Системный инженер, CCIE
23.04.2021

Agenda

- Remote Access VPN
- FlexVPN and SDA
- Mixed Client & Branch Access
- In summary

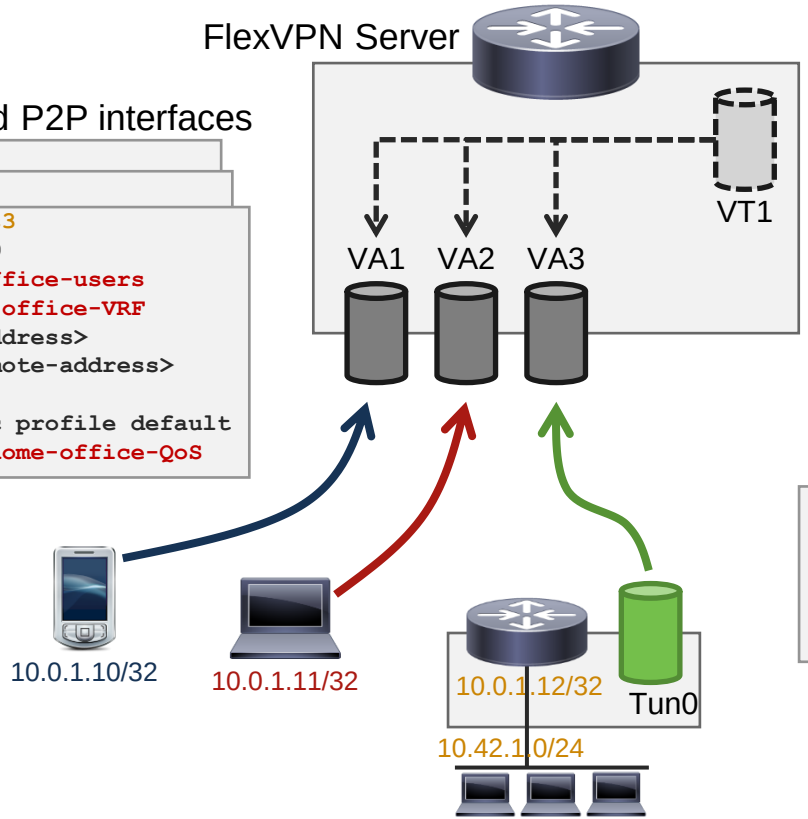
Remote Access

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
```



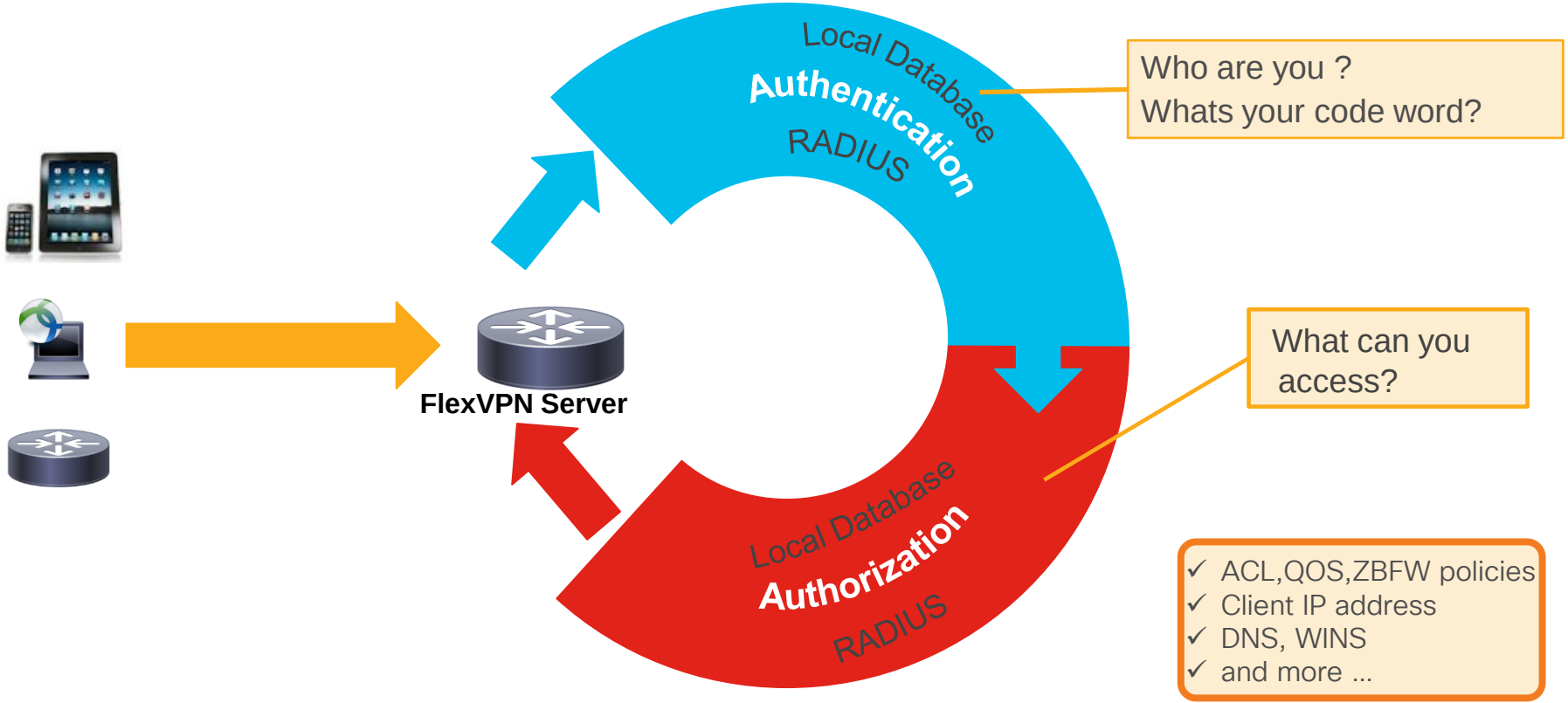
P2P virtual interface template

```
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



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

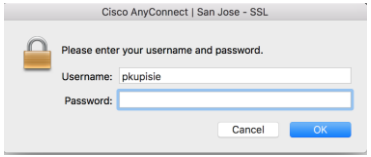
EAP Authentication (Standard Protocols)

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)

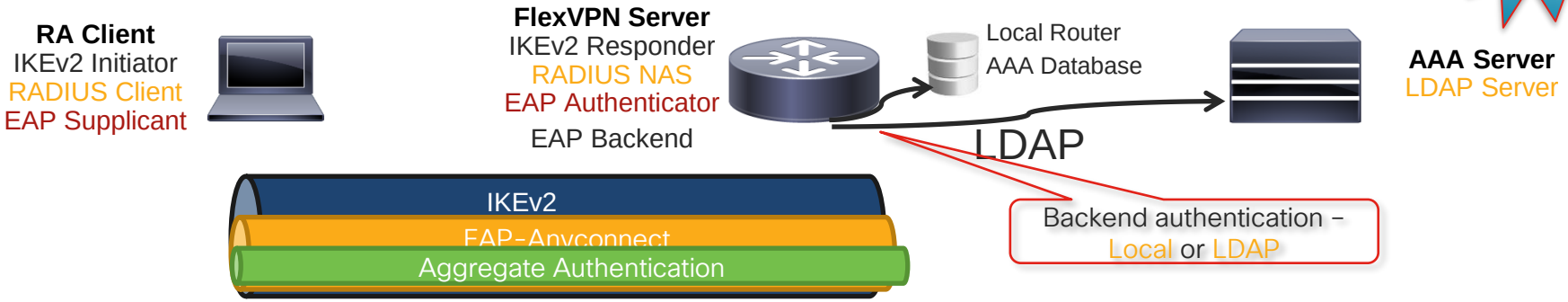
RADIUS (Access-Accept)

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

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

Anyconnect-EAP & Aggregate Authentication

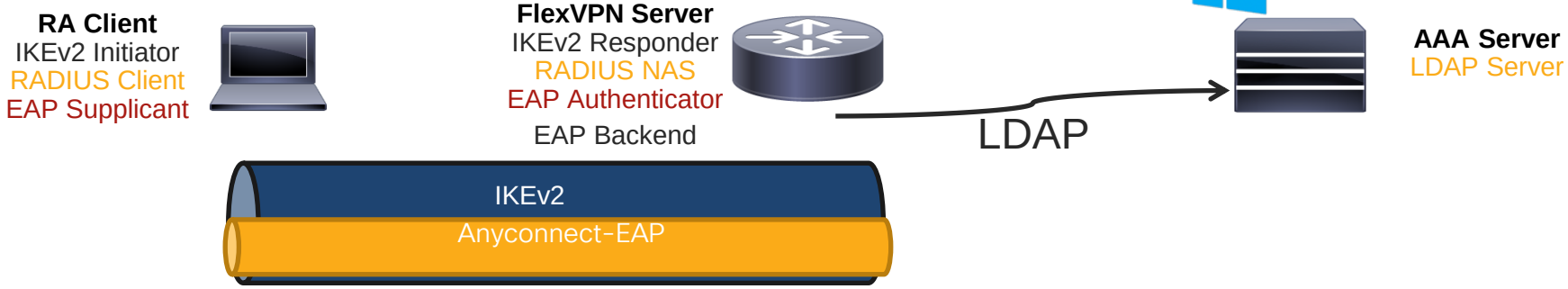
15.5(2)S+
15.5(2)T+



- 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
- Profile download now available!

FlexVPN and LDAP Authentication

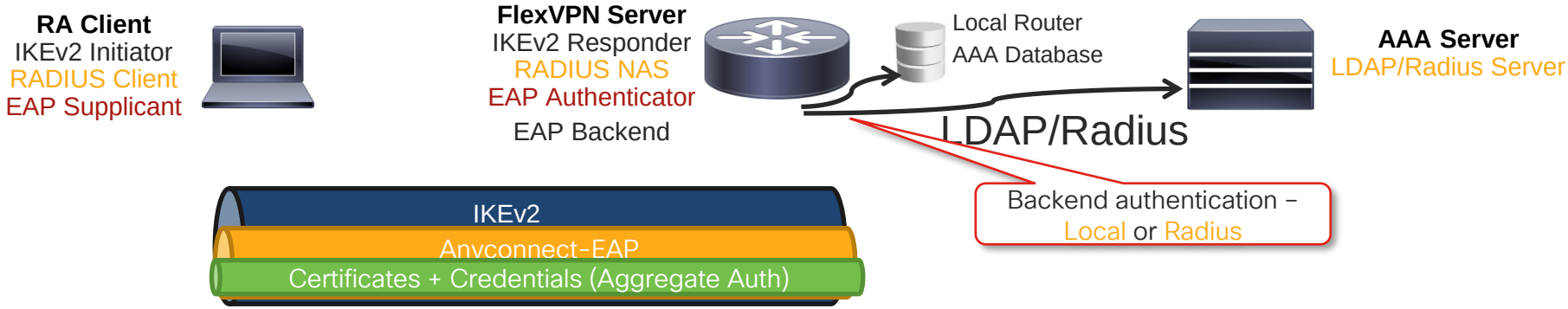
Additional info




```
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
```

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
```

MFA – Duo Security

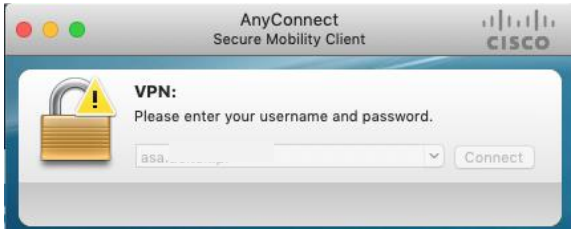
RA Client
IKEv2 Initiator
RADIUS Client
EAP Supplicant

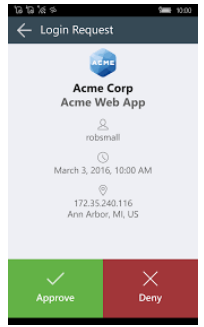
FlexVPN Server
IKEv2 Responder
RADIUS NAS
EAP Authenticator
EAP Backend

AAA Server
Duo Authentication Proxy

RADIUS (Access-Request)
(CREDENTIALS)

Push





Approve

RADIUS (Access-Accept)

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

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

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

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

Explicit User authorization

and

```
crypto ikev2 profile default
 aaa authorization user {psk|eap|cert} list …
```

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

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

Explicit Group authorization

```
crypto ikev2 profile default
 aaa authorization group {psk|eap|cert} …
```

Attributes – Merging

Additional info

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

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

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

Final Merged Attributes

AAA Server

Received during explicit user authorization

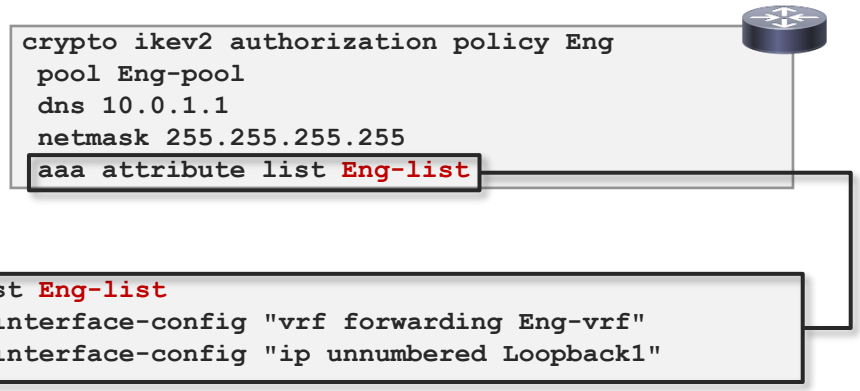
Attribute	Value
Framed-IP-Address	10.0.0.102

Received during explicit group authorization

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

Attributes for Authorization

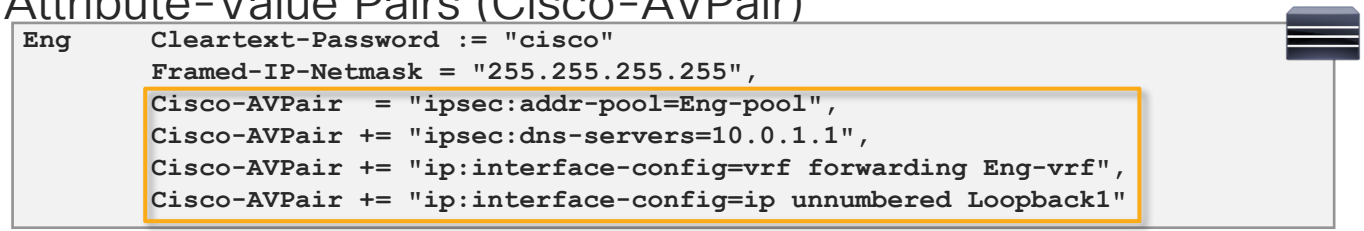
- Local Database
  - IKEv2 Authorization Policy
  - AAA Attribute List (V-Access interface configuration statements)



```
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"
```

Remote Access Clients

Remote Access Clients – Overview

For Your Reference



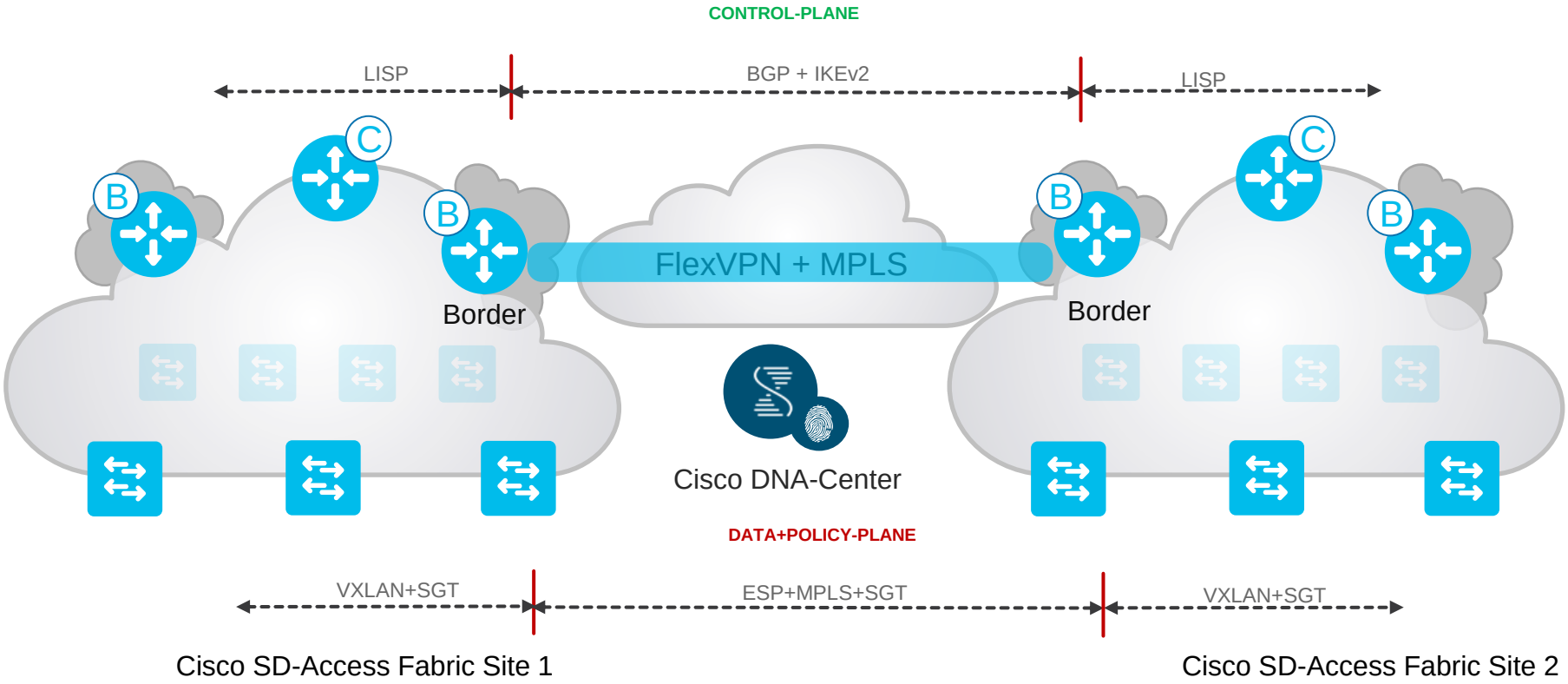


	AnyConnect (Desktop Version)	AnyConnect (Mobile Version)	Windows Native IKEv2 Client	FlexVPN Hardware Client	strongSwan
Supported OSes	Windows Mac OS X Linux	Android Apple iOS	Windows 7 & 8	Cisco IOS 15.2+ Not on IOS-XE / ASR1k Not on ISR-G1	Linux, Mac OS X, Android, FreeBSD, ...
Supported IKEv2 Authentication 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

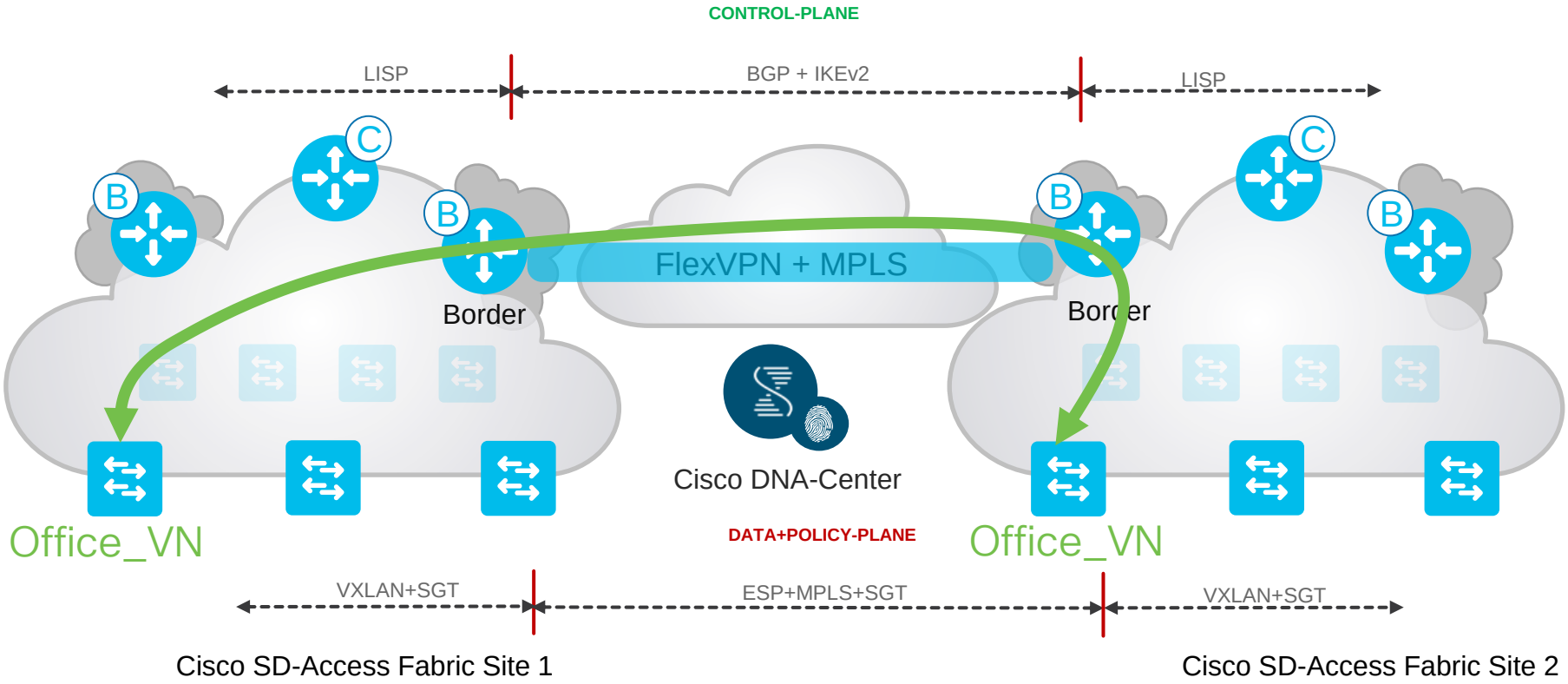
[1] EAP-TLS, EAP-TTLS, EAP-PEAP and others require (potentially dedicated) TLS certificates on EAP server & RA client
[2] IPSec Reverse Route Injection (RRI) and IKEv2 Route Exchange are enabled by default


FlexVPN as SD-Transit
(Part of MPLS over FlexVPN)

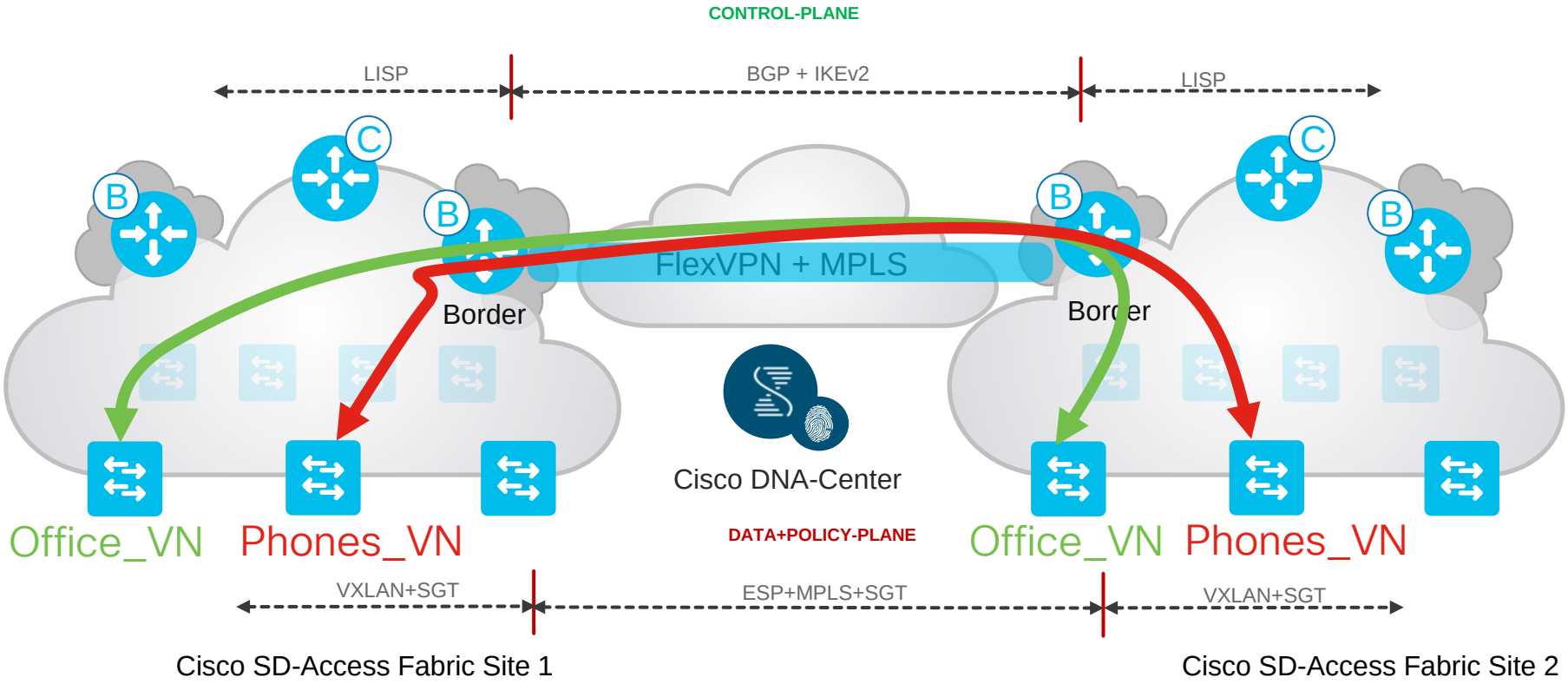
Cisco SD-Access Transit



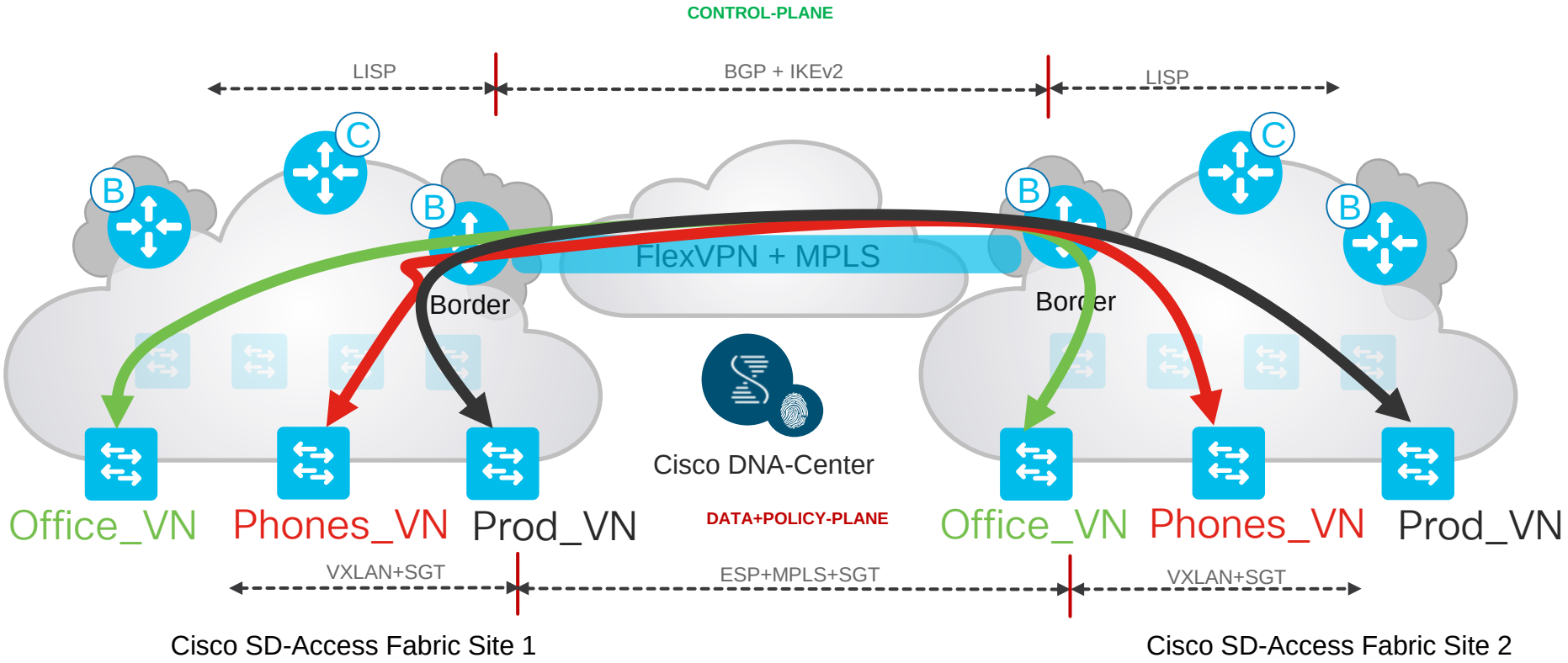
Cisco SD-Access Transit



Cisco SD-Access Transit



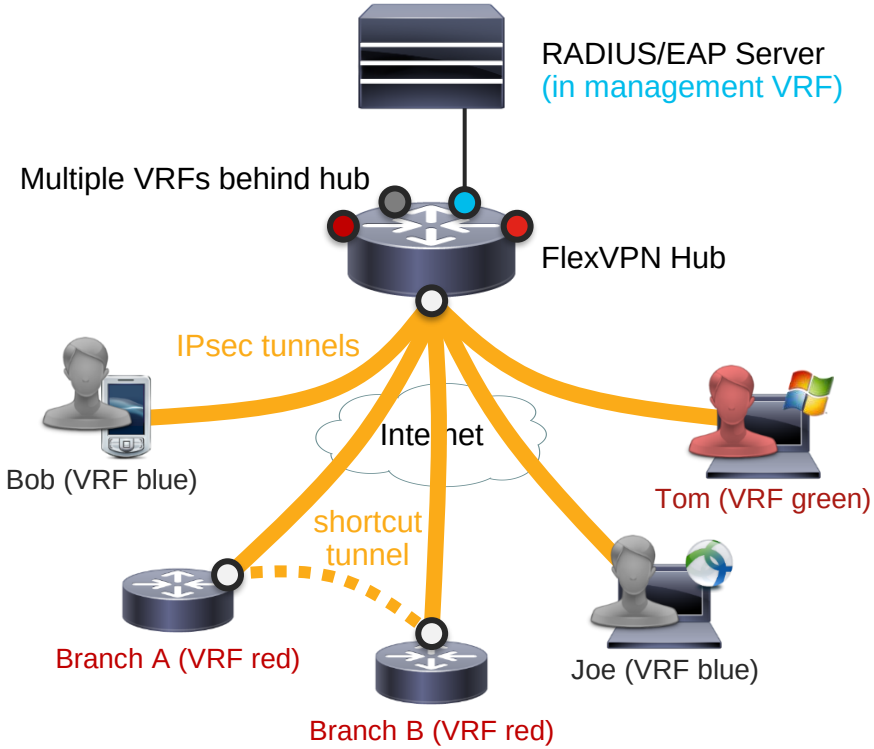
Cisco SD-Access Transit



COVID-19 response – Mixed Client & Branch Access

Use Case: Mixed Client & Branch Access

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



Tunnel modes made easy

```
crypto ikev2 profile prof1
 …
 virtual template 1
interface virtual-template 1
 …
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
```

```
crypto ikev2 profile prof2
 …
 virtual template 2
interface virtual-template 2
 …
 tunnel mode ipsec ipv6
 tunnel protection ipsec profile default
```

```
crypto ikev2 profile prof3
 …
 virtual template 3
interface virtual-template 3
 …
 tunnel mode gre ip
 tunnel protection ipsec profile default
```

```
crypto ikev2 profile prof4
 …
 virtual template 4
interface virtual-template 4
 …
 tunnel mode gre ipv6
 tunnel protection ipsec profile default
```

```
crypto ikev2 profile default
 …
 virtual template 1 mode auto

interface virtual-template 1
 …
```

In summary

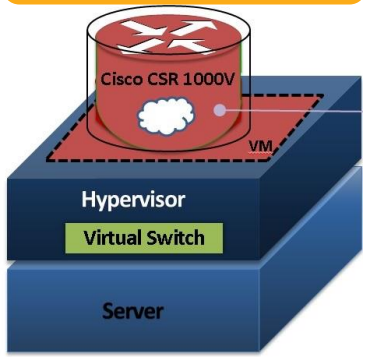
Key Platforms

Catalyst 8000 Edge Platforms

ISR 900 series

ISR 1000 series

CSR 1000v



ASR 1000 series

ISR 800, 1100
& 4000 Series

Some additional scenarios

- Multicast over FlexVPN
- Profile download
- TrustSec
- Change of Authorization

Thank you