aruba

a Hewlett Packard Enterprise company

VIA 3.X Deployment Guide

Meggie Yao

Technical Marketing

February 2018

Agenda

- Fully Redundant Deployment
  -Two Regional Domains
- Redundant Deployment
  -Two Data Centers
- Redundant Deployment
  -One Data Center
- General Facts about VIA
- VIA Client Agent Configuration
- VIA Controller Configuration using the ASE Solution
- Troubleshooting

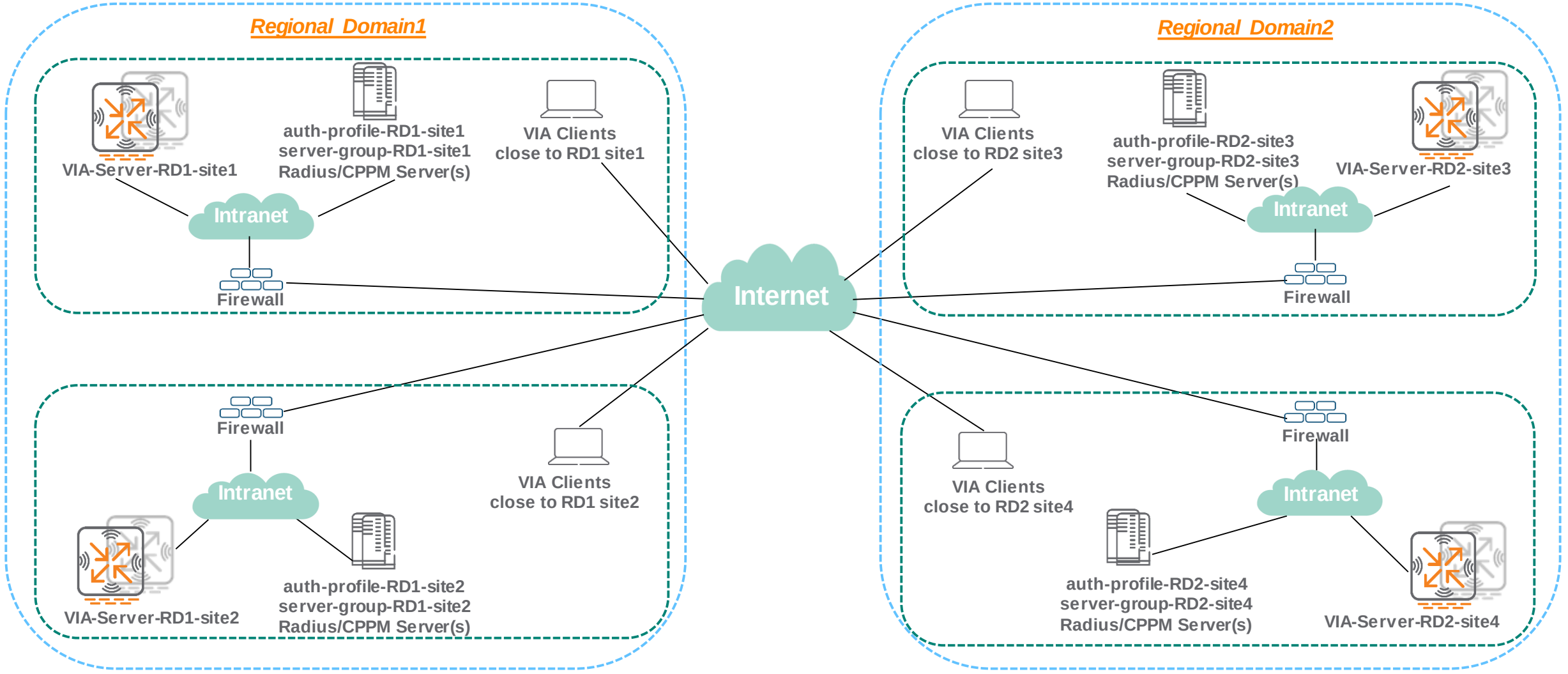
Fully Redundant Deployment

-Two Regional Domains

aruba
a Hewlett Packard Enterprise company

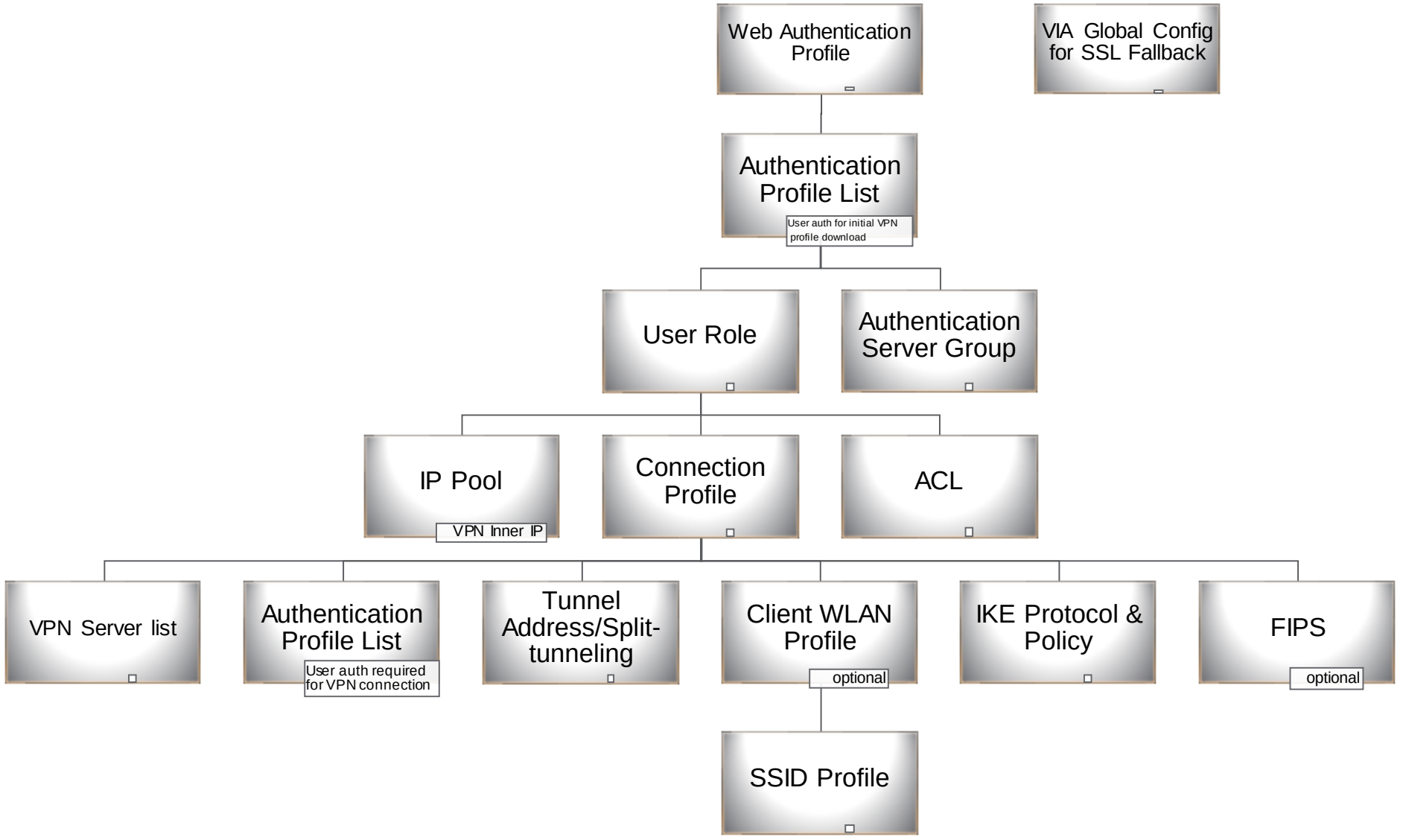
Two Regional Domains Deployment

Full Redundancy Example

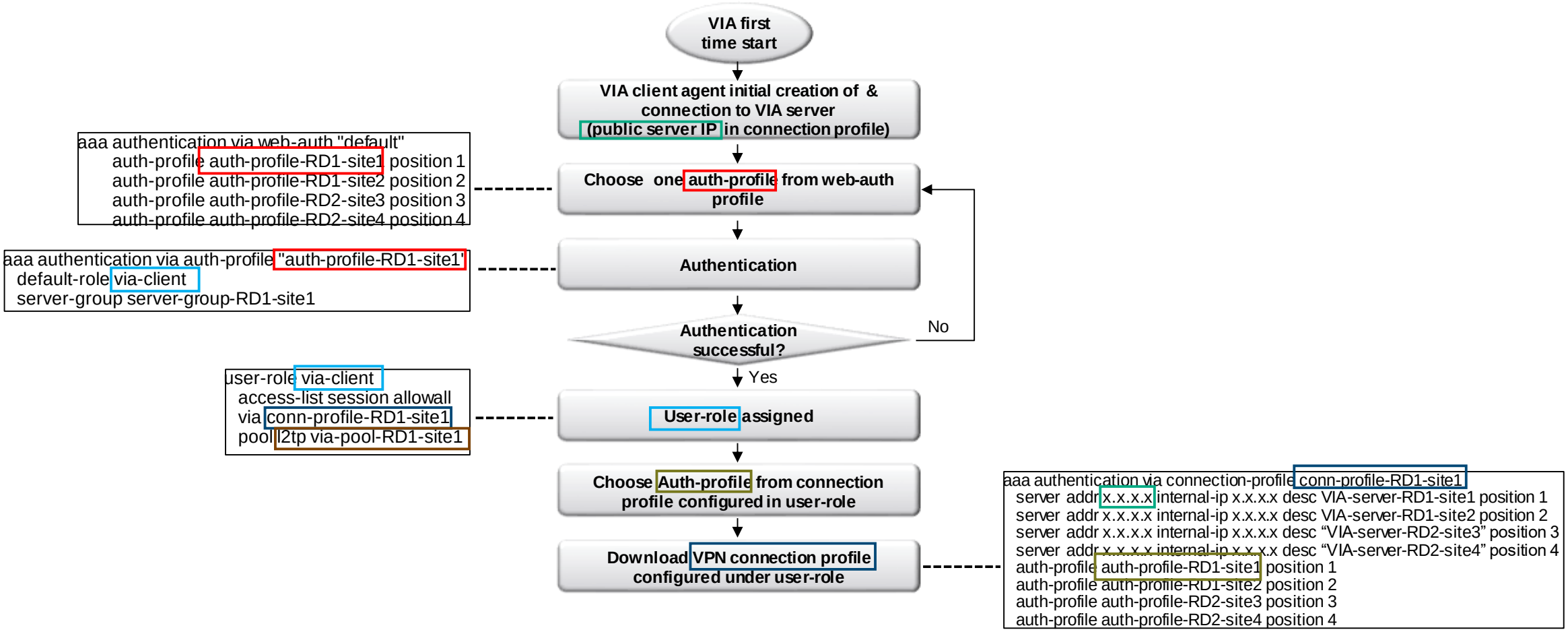


aruba
a Hewlett Packard Enterprise company

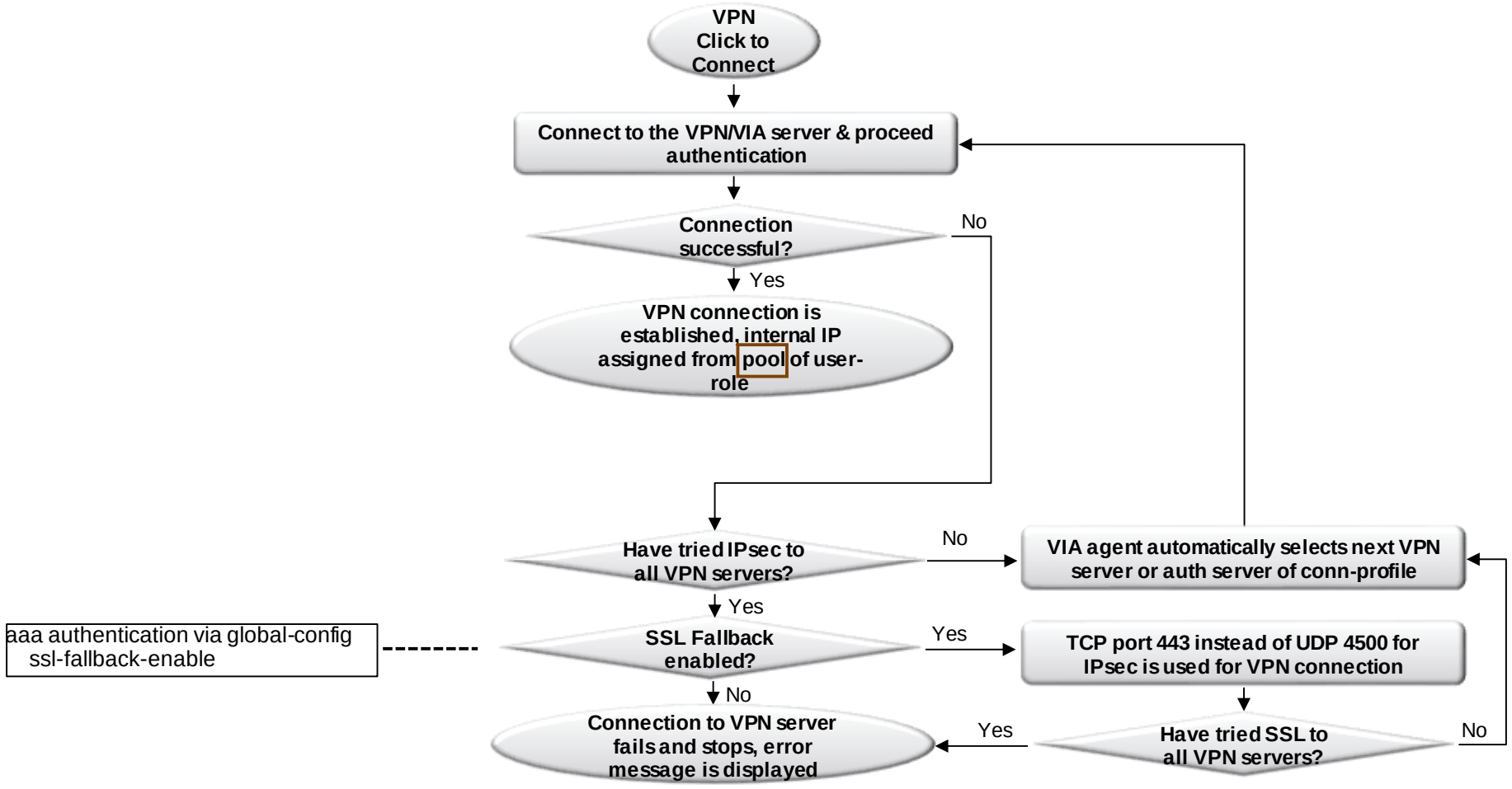
VIA Profile Structure



VIA Client Flow Chart for Initial VPN Profile Downloading



VIA Client Flow Chart for VPN Connection Establishment



Authentication Profile

Authentication server group is configured, multiple servers can be defined for redundancy.

User role assigned to VIA client after successful authentication which links to the VPN connection profile

Used for downloading the VPN profile of VIA connection for the first time

```
aaa authentication via auth-profile "auth-profile-RD1-site1"
   default-role via-client
   server-group server-group-RD1-site1
```

Authentication Mechanisms

Tunnel Authentication

- PSK (Pre shared Key)
- Digital certificate

User Authentication

- User name & password
- Digital Certificate
- Smart card
- RSA SecurID
- MFA (multi-factor authentication)

*Please refer to appendix 8 of VIA v3.0 user guide about the details of MFA.

aruba
a Hewlett Packard Enterprise company

Web-Auth Profile

Authentication redundancy and high availability is required.

VIA users across multi-location, multi Regional domains.

Downloading the VPN profile of VIA connection for the first time

Web-auth profile is skipped if VPN profile has been downloaded earlier

```
aaa authentication  via web-auth  "default"
      auth-profile  auth-profile-RD1-site1  position 1
      auth-profile  auth-profile-RD1-site2  position 2
      auth-profile  auth-profile-RD2-site3  position 3
      auth-profile  auth-profile-RD2-site4  position 4
```

aruba
a Hewlett Packard Enterprise company

User Role

It is post-auth user role which is assigned to VIA client after successful authentication.

VPN connection profile applied which is the VPN profile downloaded by the VIA client for the initial VPN server setup.

IP pool applied where the VIA client VPN IP is assigned from.

Access privilege (ACL) applied

```
user-role via-client
   access-list session allowall
   via conn-profile-RD1-site1
   pool l2tp via-pool-RD1-site1
```

VPN Connection Profile

Multiple Authentication Profile

Provides high authentication redundancy and availability.

Multiple authentication server-group located at different sites.

When server(s) at one site fails, the user can fail over to another site.

By default, the first auth-profile in the connection profile is always used first.

```
aaa authentication via connection-profile conn-profile-RD1-site1
   auth-profile auth-profile-RD1-site1 position 1
   auth-profile auth-profile-RD1-site2 position 2
   auth-profile auth-profile-RD2-site3 position 3
   auth-profile auth-profile-RD2-site4 position 4
```

aruba
a Hewlett Packard Enterprise company

VPN Connection Profile

Multiple VPN Server Addresses

Provides high availability and redundancy.

When one VPN server fails, the VIA clients fails to another automatically.

The server address is the public IP or DNS hostname address the VIA agent enters as VPN server .

The internal IP is used by the VIA client to determine if the client is connected to a trusted network.

The internal IP will be the VRRP VIP if a pair of redundant VIA servers are installed at one site.

```
aaa authentication  via connection-profile  conn-profile-RD1-site1
   server addr x.x.x.x  internal-ip  x.x.x.x  desc VIA-server-RD1-site1  position 1
   server addr x.x.x.x  internal-ip  x.x.x.x  desc VIA-server-RD1-site2  position 2
   server addr x.x.x.x  internal-ip  x.x.x.x  desc “VIA-server-RD2-site3”  position 3
   server addr x.x.x.x  internal-ip  x.x.x.x  desc “VIA-server-RD2-site4”  position 4
```

VPN Connection Profile

Auto-detection of Trusted & Untrusted VIA Client

The internal IP of the VPN server is used by the VIA client to determine if the client is connected to a trust network.

Client is trusted if it receives an HTTPS response with the X-VIA header.

If VIA client detects untrusted network & auto-connect is enabled, it will connect to VIA automatically.

```
aaa authentication via connection-profile conn-profile-RD1-site1
  server addr x.x.x.x internal-ip x.x.x.x desc VIA-server-RD1-site1 position 1
```

VPN Connection Profile

Tunnel Address & Split-tunneling

When “split-tunneling” is enabled, all traffic destined to “Tunnel address” is forwarded through VIA IPsec tunnel, others is bridged locally on the client.

When “split-tunneling” is disabled, all traffic is forwarded through IPsec tunnel & tunnel address is ignored.

Conn-profile configuration:

```
aaa authentication  via connection-profile "conn-profile-RD1-site1 "
   tunnel address 10.1.1.0 netmask 255.255.255.0
   tunnel address 172.16.200.0 netmask 255.255.255.0
   split-tunneling
```

VIA client routing table:

```
$netstat -nr
Routing tables
Destination        Gateway          Flags     Refs     Use   Netif  Expire
default            15.111.200.1     UGSc       32     113    en0    ===➔ With split-tunnel enabled, other traffic is sent
                                                                        through the default gateway of the client.
10.1.1.0/24        172.16.100.46    UGSc        0       0    utun1  ===➔ both subnets traffic is sent through VIA
172.16.200.0/24    172.16.100.46    UGSc        0       0    utun1        ipsec tunnel.
```

aruba
a Hewlett Packard Enterprise company

VPN Connection Profile

IKEv1 and IKEv2

No separate VIA connection profile required for IKEv1 & IKEv2.

If IKEv2 is enabled in the conn-profile, clients always attempt IKEv2 first.

If IKEv2 connections fails, the clients falls back to IKEv1.

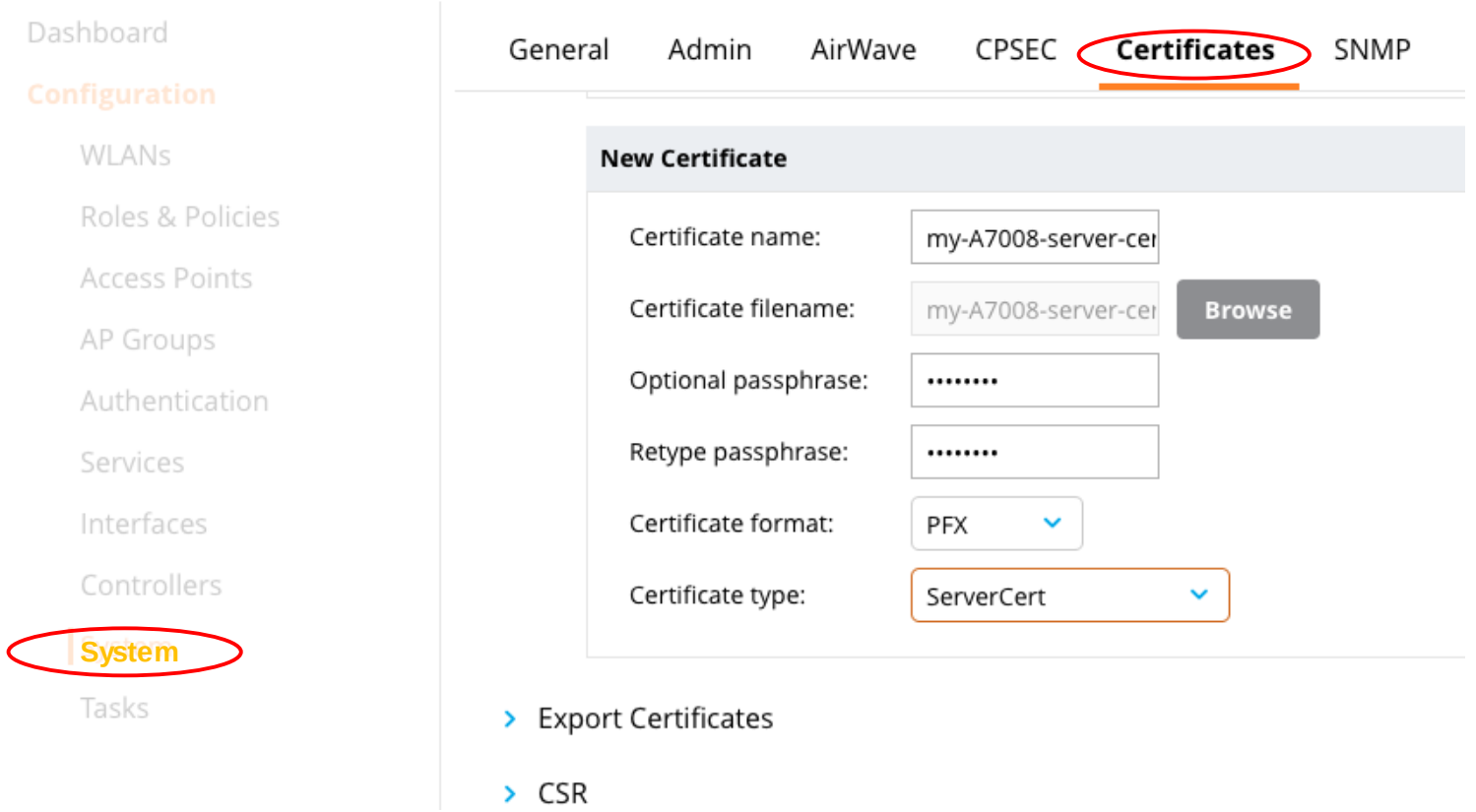
```
aaa authentication via connection-profile conn-profile-RD1-site1
   ikev2-proto
   ikev2auth user-cert
```

IKEv2 with Certificate

Import Certificate

Import server certificate and CA certificate

Under the VIA server device folder, Configuration>System>Certificates>Import Certificates



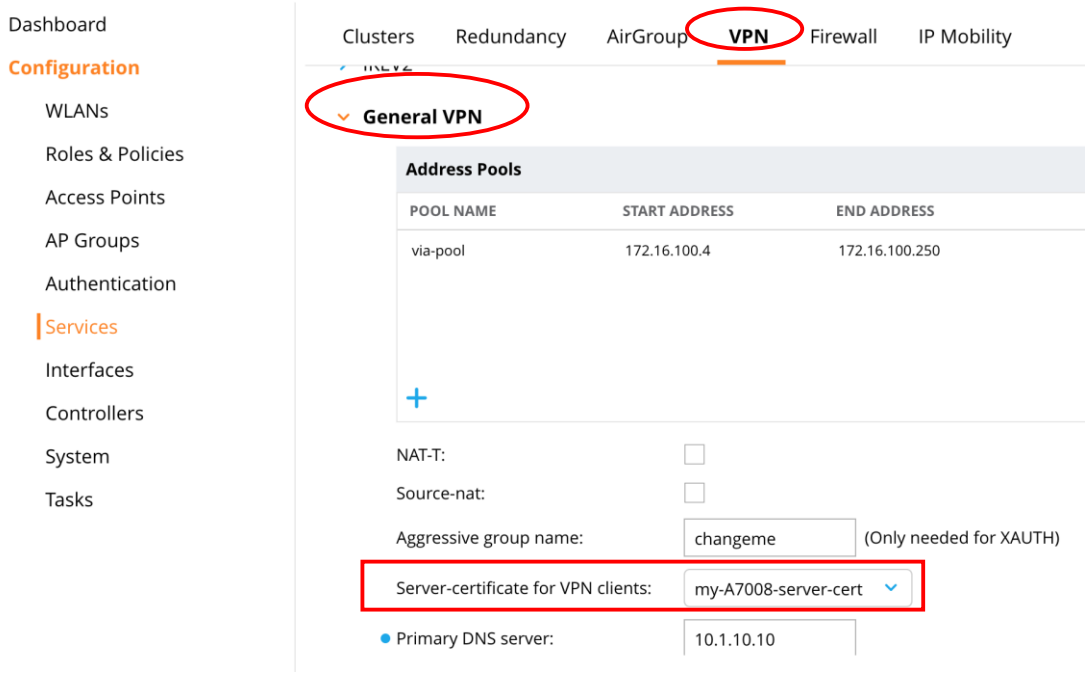
IKEv2 with Certificate

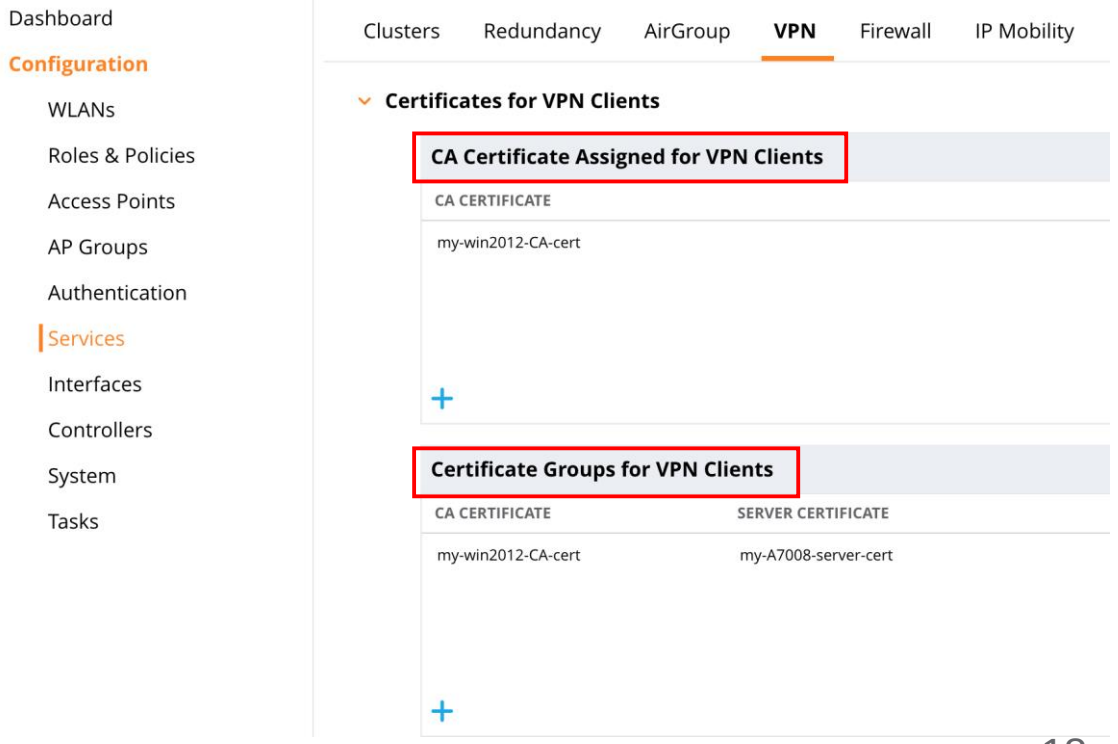
Apply Server Cert & CA Cert to VPN Service

Apply the server certificate and CA certificate

Configuration>Services>VPN>General VPN & Certificates for VPN Clients

Certificate group allows multiple server/CA cert pairs for different clients in one controller.





aruba
a Hewlett Packard Enterprise company

Client WLAN Profile

Used to push WLAN settings on VIA client devices.

It is optional.

```
wlan client-wlan-profile via-wlan
  ssid-profile employee

aaa authentication via connection-profile conn-profile-RD1-site1
  client-wlan-profile via-wlan
```

FIPS Support

Conforms to FIPS 140-2 level certification.

Enabled under connection profile. Disabled by default.

To support FIPS at VIA clients, the controller needs to run AOS FIPS code and have FIPS enabled globally.

```
aaa authentication  via connection-profile  conn-profile-RD1-site1
   enable-fips
```

Downloadable User-Role via CPPM Server

Enable ClearPass acting as a centralized policy & enforcement definition point. Provides greater flexibility and dynamic security.

Supported when VIA users are authenticated against CPPM

Only supported IKE v1 XAuth VIA users

Configured under auth-profile

```
aaa authentication  via auth-profile  "via-auth-prof-US-SanJose"
    download-role
```

SSL Fallback

When UDP port 4500 is blocked in the path, VIA establishes IPsec over SSL using TCP 443.

Port 4500 should not be blocked on Aruba controller port.

With SSL fallback disabled, one VIA client accounts for one IPsec tunnel.
With SSL fallback enabled, one VIA client accounts for two IPsec tunnels.

By default, it is disabled

```
aaa authentication  via global-config
    ssl-fallback-enable
```

Two Regional Domains Deployment

Common Profile Configuration Example for 4 VIA Servers

1 Authentication profile configuration

```
aaa authentication via auth-profile "auth-profile-RD1-site1"
   default-role via-client
   server-group server-group-RD1-site1
aaa authentication via auth-profile "auth-profile-RD1-site2”
   default-role via-client
   server-group server-group-RD1-site2
aaa authentication via auth-profile "auth-profile-RD2-site3"
   default-role via-client
   server-group server-group-RD2-site3
aaa authentication via auth-profile "auth-profile-RD2-site4"
   default-role via-client
   server-group server-group-RD2-site4
```

2 Web Authentication profile configuration

```
aaa authentication via web-auth "default"
      auth-profile auth-profile-RD1-site1  position 1
      auth-profile auth-profile-RD1-site2  position 2
      auth-profile auth-profile-RD2-site3  position 3
      auth-profile auth-profile-RD2-site4  position 4
```

3 Global config if SSL fallback is needed

```
aaa authentication via global-config
   ssl-fallback-enable
```

Two Regional Domains Deployment

Individual Configuration Example of Each VIA Server

1 VIA-Server-RD1-site1

```
lp local pool via-pool-RD1-site1 x.x.x.x x.x.x.x

aaa authentication via connection-profile conn-profile-RD1-site1
  server addr x.x.x.x internal-ip x.x.x.x desc VIA-server-RD1-site1 position 1
  server addr x.x.x.x internal-ip x.x.x.x desc VIA-server-RD1-site2 position 2
  server addr x.x.x.x internal-ip x.x.x.x desc “VIA-server-RD2-site3” position 3
  server addr x.x.x.x internal-ip x.x.x.x desc “VIA-server-RD2-site4” position 4
  auth-profile auth-profile-RD1-site1 position 1
  auth-profile auth-profile-RD1-site2 position 2
  auth-profile auth-profile-RD2-site3 position 3
  auth-profile auth-profile-RD2-site4 position 4

user-role via-client
  access-list session allowall
  via conn-profile-RD1-site1
  pool l2tp via-pool-RD1-site1
```

2 VIA-Server-RD1-site2

```
lp local pool via-pool-RD1-site2 x.x.x.x x.x.x.x

aaa authentication via connection-profile conn-profile-RD1-site2
  server addr x.x.x.x internal-ip x.x.x.x desc VIA-server-RD1-site2 position 1
  server addr x.x.x.x internal-ip x.x.x.x desc VIA-server-RD1-site1 position 2
  server addr x.x.x.x internal-ip x.x.x.x desc “VIA-server-RD2-site3” position 3
  server addr x.x.x.x internal-ip x.x.x.x desc “VIA-server-RD2-site4” position 4
  auth-profile auth-profile-RD1-site2 position 1
  auth-profile auth-profile-RD1-site1 position 2
  auth-profile auth-profile-RD2-site3 position 3
  auth-profile auth-profile-RD2-site4 position 4

user-role via-client
  access-list session allowall
  via conn-profile-RD1-site2
  pool l2tp via-pool-RD1-site2
```

3 VIA-Server-RD2-site3

```
lp local pool via-pool-RD2-site3 x.x.x.x x.x.x.x

aaa authentication via connection-profile conn-profile-RD2-site3
  server addr x.x.x.x internal-ip x.x.x.x desc “VIA-server-RD2-site3” position 1
  server addr x.x.x.x internal-ip x.x.x.x desc “VIA-server-RD2-site4” position 2
  server addr x.x.x.x internal-ip x.x.x.x desc VIA-server-RD1-site1 position 3
  server addr x.x.x.x internal-ip x.x.x.x desc VIA-server-RD1-site2 position 4
  auth-profile auth-profile-RD2-site3 position 1
  auth-profile auth-profile-RD2-site4 position 2
  auth-profile auth-profile-RD1-site1 position 3
  auth-profile auth-profile-RD1-site2 position 4

user-role via-client
  access-list session allowall
  via conn-profile-RD2-site3
  pool l2tp via-pool-RD2-site3
```

4 VIA-Server-RD2-site4

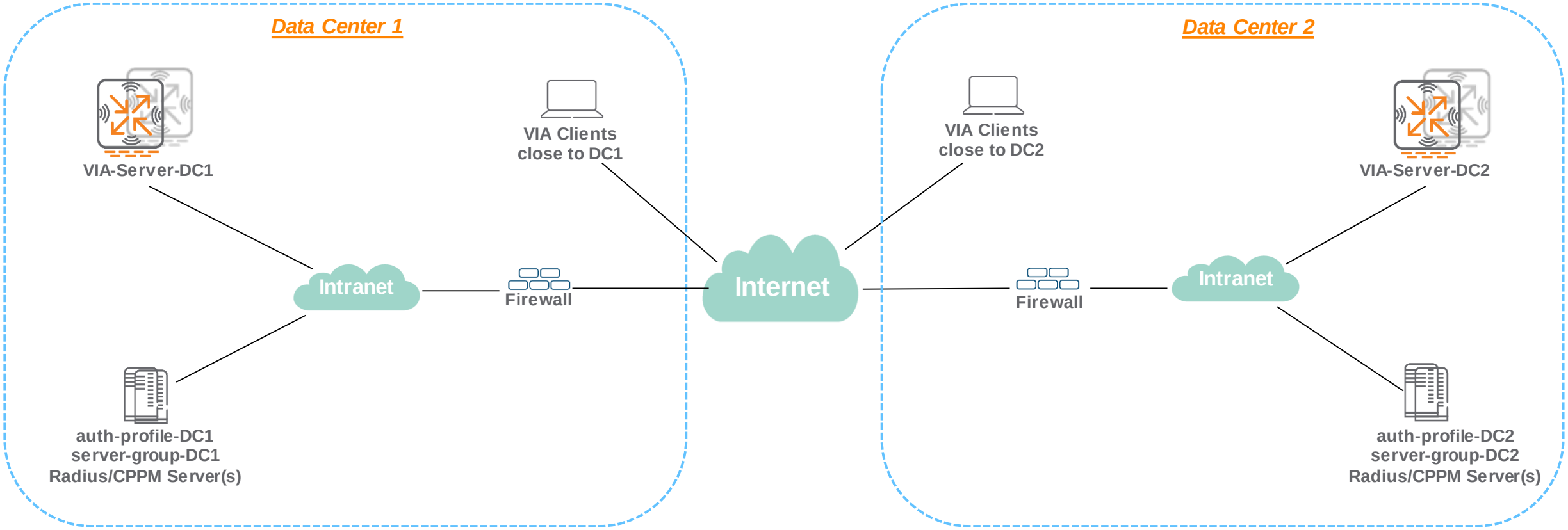
```
lp local pool via-pool-RD2-site4 x.x.x.x x.x.x.x

aaa authentication via connection-profile conn-profile-RD2-site4
  server addr x.x.x.x internal-ip x.x.x.x desc VIA-server-RD2-site4 position 1
  server addr x.x.x.x internal-ip x.x.x.x desc VIA-server-RD2-site3 position 2
  server addr x.x.x.x internal-ip x.x.x.x desc VIA-server-RD1-site1 position 3
  server addr x.x.x.x internal-ip x.x.x.x desc VIA-server-RD1-site2 position 4
  auth-profile auth-profile-RD2-site4 position 1
  auth-profile auth-profile-RD2-site3 position 2
  auth-profile auth-profile-RD1-site1 position 3
  auth-profile auth-profile-RD1-site2 position 4

user-role via-client
  access-list session allowall
  via conn-profile-RD2-site4
  pool l2tp via-pool-RD2-site4
```

aruba
a Hewlett Packard Enterprise company

Redundant Deployment

-Two Data Centers

Redundant Deployment for Two Data Centers



aruba
a Hewlett Packard Enterprise company

Redundant Deployment for Two Data Centers

Common Profile Configuration Example for 2 VIA Servers

1 Authentication profile configuration

```
aaa authentication via auth-profile "auth-profile-DC1"
   default-role via-client
   server-group server-group-DC1
aaa authentication via auth-profile "auth-profile-DC2”
   default-role via-client
   server-group server-group-DC2
```

2 Web Authentication profile configuration

```
aaa authentication via web-auth "default"
      auth-profile auth-profile-DC1 position 1
      auth-profile auth-profile-DC2 position 2
```

3 Global config if SSL fallback is needed

```
aaa authentication via global-config
   ssl-fallback-enable
```

aruba
a Hewlett Packard Enterprise company

Redundant Deployment for Two Data Centers

Individual Configuration Example of Each VIA Server

1 VIA-Server-DC1

```
Ip local pool via-pool-DC1 x.x.x.x x.x.x.x

aaa authentication via connection-profile conn-profile-DC1
  server addr x.x.x.x internal-ip x.x.x.x desc VIA-server-DC1 position 1
  server addr x.x.x.x internal-ip x.x.x.x desc VIA-server-DC2 position 2
  auth-profile auth-profile-DC1 position 1
  auth-profile auth-profile-DC2 position 2

user-role via-client
  access-list session allowall
  via conn-profile-DC1
  pool l2tp via-pool-DC1
```

2 VIA-Server-DC2

```
Ip local pool via-pool-DC2 x.x.x.x x.x.x.x

aaa authentication via connection-profile conn-profile-DC2
  server addr x.x.x.x internal-ip x.x.x.x desc VIA-server-DC2 position 1
  server addr x.x.x.x internal-ip x.x.x.x desc VIA-server-DC1 position 2
  auth-profile auth-profile-DC2 position 1
  auth-profile auth-profile-DC1 position 2

user-role via-client
  access-list session allowall
  via conn-profile-DC2
  pool l2tp via-pool-DC2
```

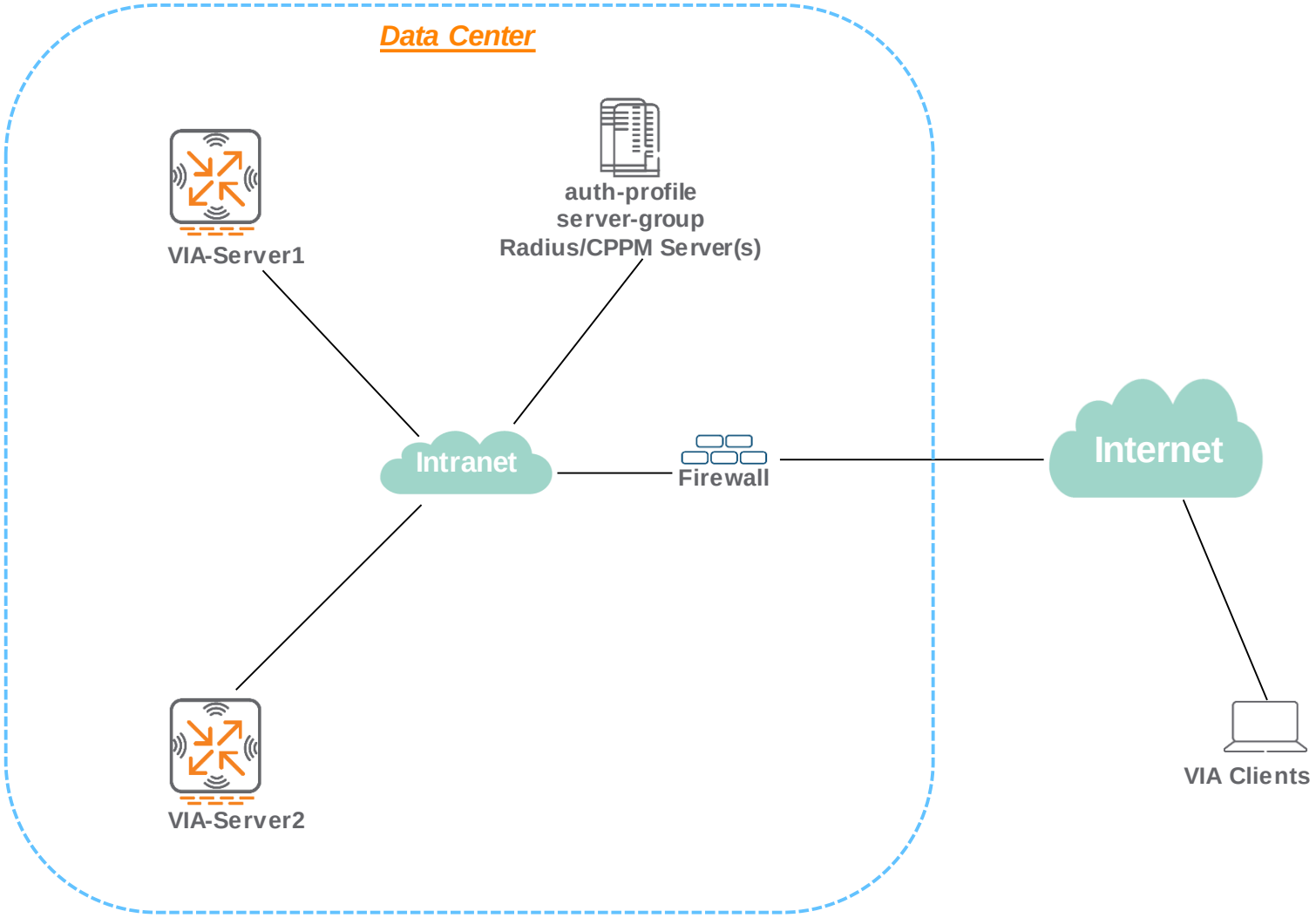
aruba
a Hewlett Packard Enterprise company

Redundant Deployment

-One Data Center

aruba
a Hewlett Packard
Enterprise company

Redundant Deployment for One Data Center



aruba
a Hewlett Packard
Enterprise company

Redundant Deployment for One Data Centers

Common Profile Configuration Example for 2 VIA Servers

1 Authentication profile configuration

```
aaa authentication via auth-profile "auth-profile1"
   default-role via-client
   server-group server-group1
aaa authentication via auth-profile "auth-profile2”
   default-role via-client
   server-group server-group2
```

2 Web Authentication profile configuration

```
aaa authentication via web-auth "default"
      auth-profile auth-profile1 position 1
      auth-profile auth-profile2 position 2
```

3 Global config if SSL fallback is needed

```
aaa authentication via global-config
   ssl-fallback-enable
```

aruba
a Hewlett Packard Enterprise company

Redundant Deployment for One Data Centers

Individual Configuration Example of Each VIA Server

1 VIA-Server1

```
Ip local pool via-pool1 x.x.x.x x.x.x.x

aaa authentication via connection-profile conn-profile1
   server addr x.x.x.x internal-ip x.x.x.x desc VIA-server1 position 1
   server addr x.x.x.x internal-ip x.x.x.x desc VIA-server2 position 2
   auth-profile auth-profile1 position 1
   auth-profile auth-profile2 position 2

user-role via-client
   access-list session allowall
   via conn-profile1
   pool l2tp via-pool1
```

2 VIA-Server2

```
Ip local pool via-pool2 x.x.x.x x.x.x.x

aaa authentication via connection-profile conn-profile2
   server addr x.x.x.x internal-ip x.x.x.x desc VIA-server2 position 1
   server addr x.x.x.x internal-ip x.x.x.x desc VIA-server1 position 2
   auth-profile auth-profile2 position 1
   auth-profile auth-profile1 position 2

user-role via-client
   access-list session allowall
   via conn-profile2
   pool l2tp via-pool2
```

General Facts about VIA

Number of VIA Clients Supported on Mobility Controllers

- One VIA client establishes one IPSEC session with the controller, the number of concurrent VIA clients is equivalent to the number of IPSEC tunnels supported by the platform.

Controller Model	Number of VIA Clients
7280	32,768
7240	32,768
7220	24,576
7210	16,384
7030	4,096
7010	2,048
7005	1,024
7008	1,024

VIA Clients OS Supported on Mobility Controllers

Operating System	Supported VIA OS
Windows	Windows Vista Windows 7 Windows 10
MAC OS X	10.6 – 10.12
Apple iOS	4.2 – 10.x
Android	4.0.2 & above
Linux	RHEL 6 CentOS 6 Debian 7 Ubuntu (>12.04)

Feature Summary

Features	Details
Secure Connectivity	• Native IPsec/NAT-T with automatic SSL fallback • HTTPS proxy support • Optional split-tunnel mode • Supports wired, WLAN, or broadband cellular
Seamless User Experience	• Leverage's SSO so users not aware VPN is in use • User experience "feels" like enterprise LAN
Simplified Administration	• WZC control – Provides IT staff the ability to configure wireless settings for client laptops as part of the profile • Simple "send logs" button packages all diagnostic information and emails to helpdesk, it speeds up troubleshooting
Automatic Trust Detection	• VIA detects whether network connection is "trusted" or "untrusted" • Automatically launches VPN tunnel when on untrusted network
Flexible Authentication	• Tunnel authentication: PSK or digital certificate • User authentication: user/password or token card • Supports RSA SecurID • MFA
Multi-Platform	• Windows 32/64-bit • MacOS • iOS • Android • Linux

aruba
a Hewlett Packard Enterprise company

License

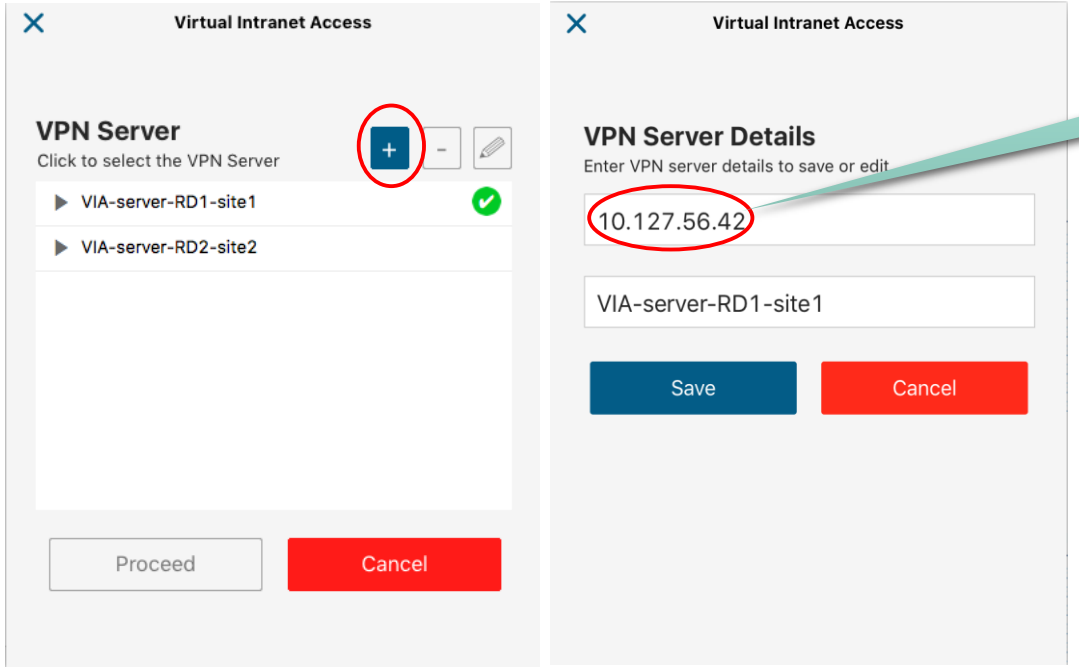
License	Details
LIC-VIA	• Global VIA license installed on Mobility Master, shared by all the VIA clients, supported since AOS 8.2 onwards • VIA Per User License, recommended by Aruba
PEFV	• Policy Enforcement Firewall VPN (PEFV) license • Box License, installed only on the controller the VIA clients terminate on • Optional if global VIA license is available
ACR	• For military-grade security, VIA supports Suite B cryptography which requires Advanced Cryptography (ACR) module. • Used to handle controlled unclassified, confidential and classified information
VMC-TACT-PEFV	• Policy Enforcement Firewall for Aruba “Virtual” Mobility Controller Tactical

VIA Client Agent Configuration

Two Regional Domains Deployment

VIA Agent Setup Example for Clients Close to RD1-site1

1. Add VPN server & proceed to download VPN profile.
2. Multiple VIA VPN server profiles to different destination supported.



The external/public IP address of VIA-server

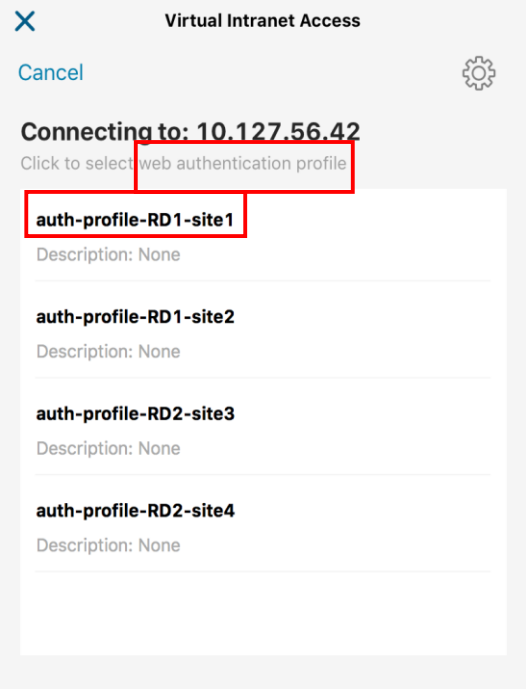
```
aaa authentication via connection-profile conn-profile-RD1-site1
  server addr 10.127.56.42 internal-ip x.x.x.x desc VIA-server-RD1-site1 position 1
  server addr x.x.x.x internal-ip x.x.x.x desc VIA-server-RD1-site2 position 2
  server addr x.x.x.x internal-ip x.x.x.x desc “VIA-server-RD2-site3” position 3
  server addr x.x.x.x internal-ip x.x.x.x desc “VIA-server-RD2-site4” position 4
```

aruba
a Hewlett Packard Enterprise company

Two Regional Domains Deployment

2 Select the closest auth profile/auth server group from Web authentication profile to do authentication & download VIA profile for the first time.

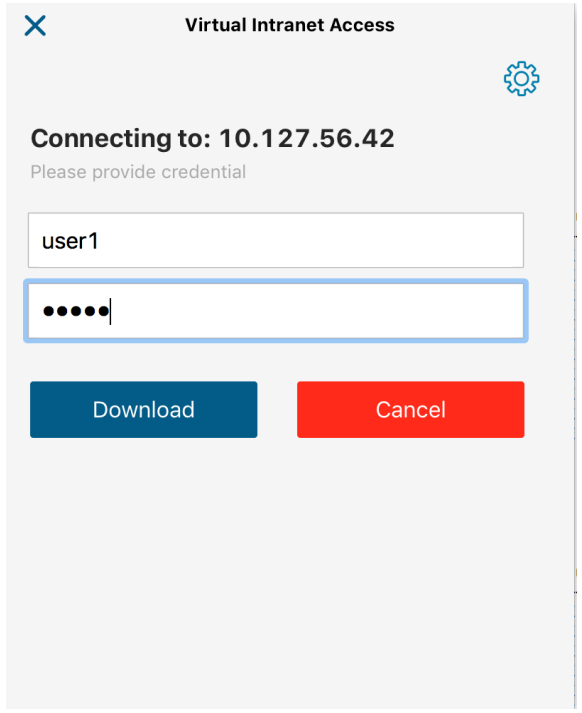
- This process is skipped later on after VPN profile is downloaded successfully at the initial setup.
- Web authentication profile provides high availability for VIA users to download VPN profile in case of any authentication server failure.

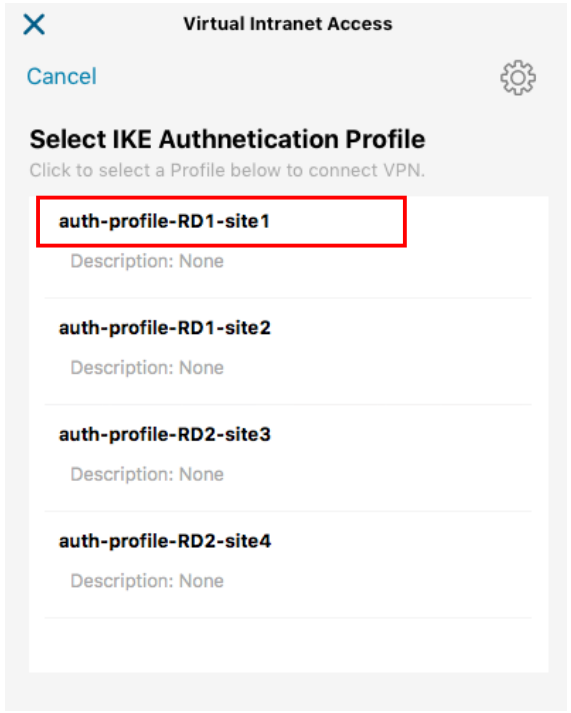


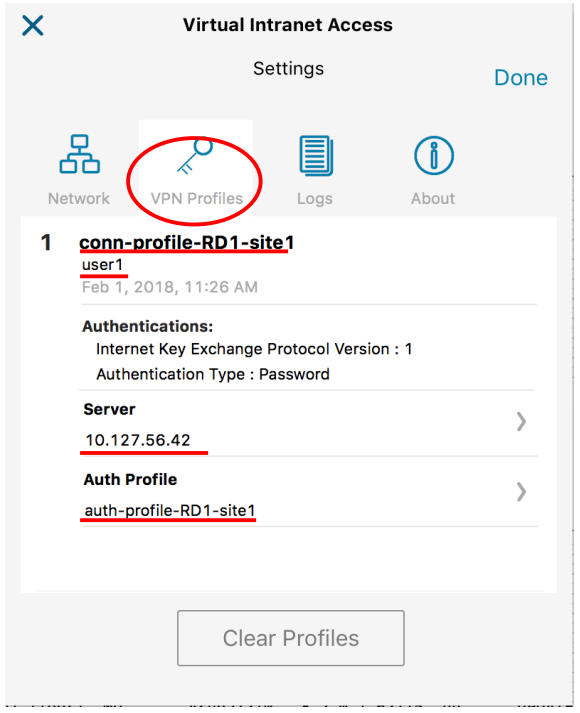

```
aaa authentication via web-auth "default"
    auth-profile auth-profile-RD1-site1  position 1
    auth-profile auth-profile-RD1-site2  position 2
    auth-profile auth-profile-RD2-site3  position 3
    auth-profile auth-profile-RD2-site4  position 4
```

Two Regional Domains Deployment

3. Input user credentials for IKEv1 PSK in this example.
4. Select the auth-profile from the VPN connection profile.
5. VPN Profile is downloaded after successful authentication.





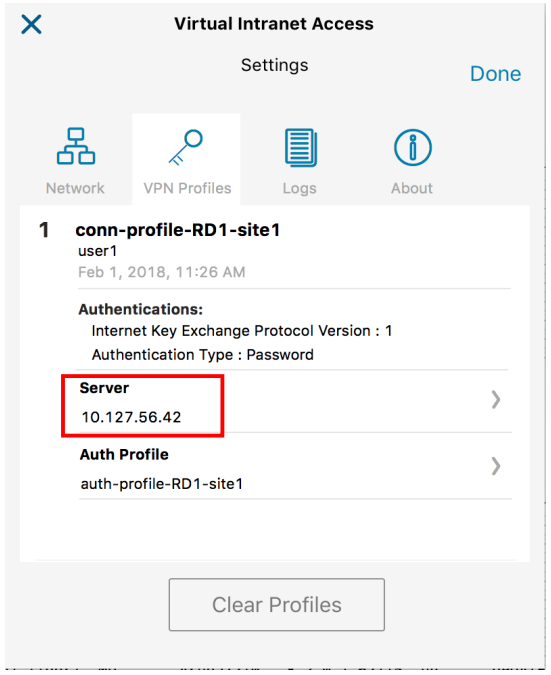


Two Regional Domains Deployment

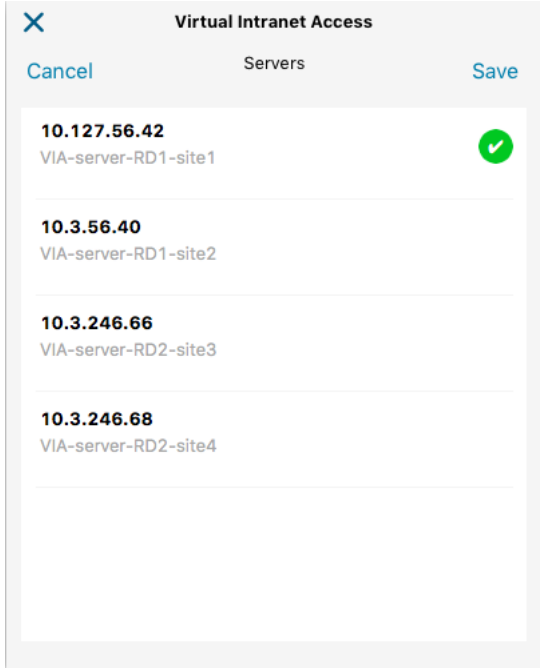
VPN Server Redundancy & SSL Fallback

VIA client will try next VPN server automatically when the current one fails .

VIA client will switch to SSL connection if none of the VPN servers are reachable via UDP 4500 and SSL fallback is enabled.



When the connection to one VPN server fails, VIA client switches to another VPN server automatically

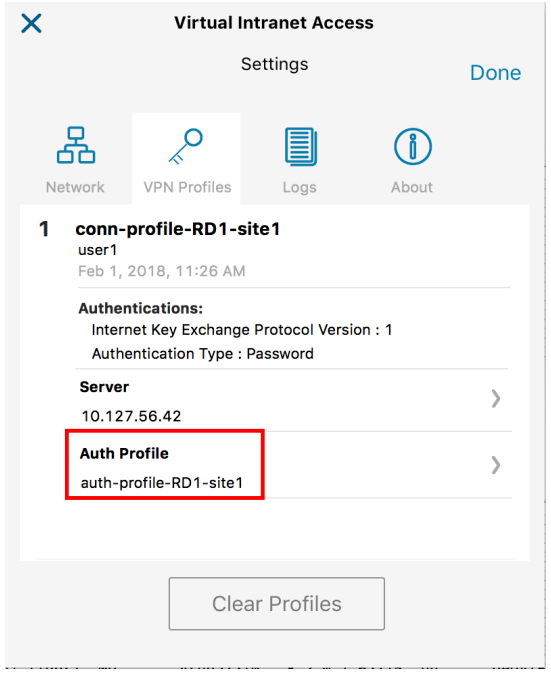


aruba
a Hewlett Packard Enterprise company

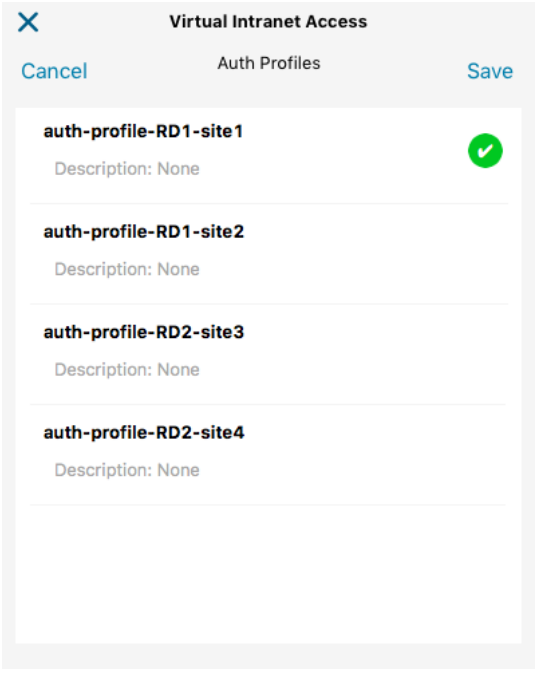
Two Regional Domains Deployment

Auth Profile Redundancy

VIA client will switch to another auth profile automatically when the current one fails .



When the authentication fails with one auth-profile, the VIA client switches to another one automatically.

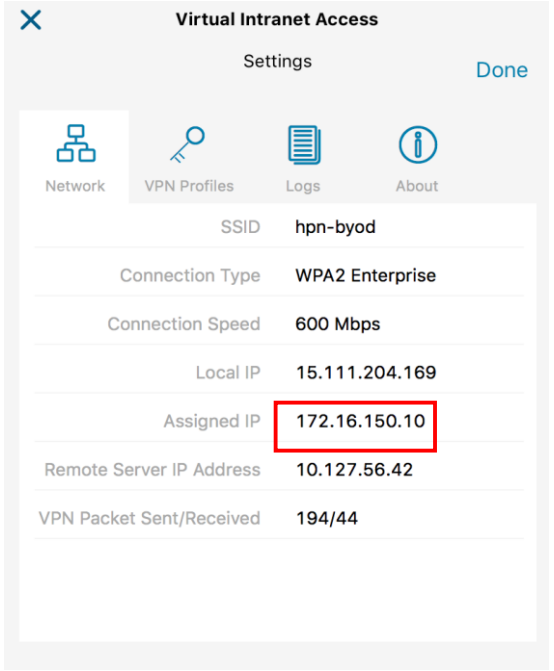


aruba
a Hewlett Packard Enterprise company

Two Regional Domains Deployment

6 Click to connect.

7 VPN/IPsec tunnel is established, VPN internal IP is assigned.



aruba
a Hewlett Packard
Enterprise company

VIA Controller Configuration using the ASE Solution

VIA Solution in Aruba Solutions Exchange

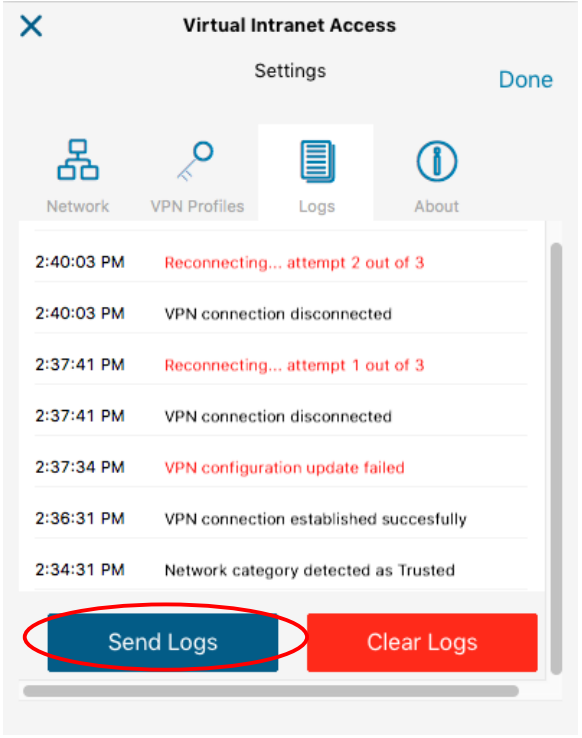
Follow the link and complete the ASE solution to get VIA configuration for AOS 8.x

https://ase.arubanetworks.com/solutions/id/190

Troubleshooting

Troubleshooting

Collect logs from VIA client



Enable ISAKMP packet dump

(VIA-server) #crypto isakmp packet-dump
(VIA-server) #write memory

2018-01-19 15:21:12,416 INFO - viaplugin_proto_isakmp:log_mocana:3035 #SEND 371 bytes to 10.127.62.42[4500] (18.17)
2018-01-19 15:21:15,421 ERROR - viaplugin_proto_isakmp:ikestat_cbh:1984 status = VIA_ERROR_IKESA_FAILED using [v1 I] (id=0x5c2e873c)
2018-01-19 15:21:15,421 ERROR - viaplugin_proto_isakmp:ikestat_cbh:1987 status = VIA_ERROR_IKESA_FAILED reason = -8949
2018-01-19 15:21:15,422 INFO - viaplugin_proto_isakmp:try_ssl_fallback:450 **Trying SSL Fallback**. InternalAddress - 10.127.62.42 ExternalAddress - 10.127.62.42
2018-01-19 15:21:15,422 ERROR - viaplugin_proto_isakmp:try_ssl_fallback:472 Remote server address - 10.127.62.42
2018-01-19 15:21:15,422 DEBUG - viaplugin_proto_isakmp:try_ssl_fallback:480 Creating read and write stream for ssl socket
2018-01-19 15:21:15,424 DEBUG - viaplugin_proto_isakmp:setup_arubassl_tunnel:411 **start SSL Session**

Thank You

aruba
a Hewlett Packard
Enterprise company