Fortinet Auto Discovery VPN (ADVPN)

Stéphane HAMELIN – Support Engineering Team

Change Log

Latest version of this document is available at:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD39360

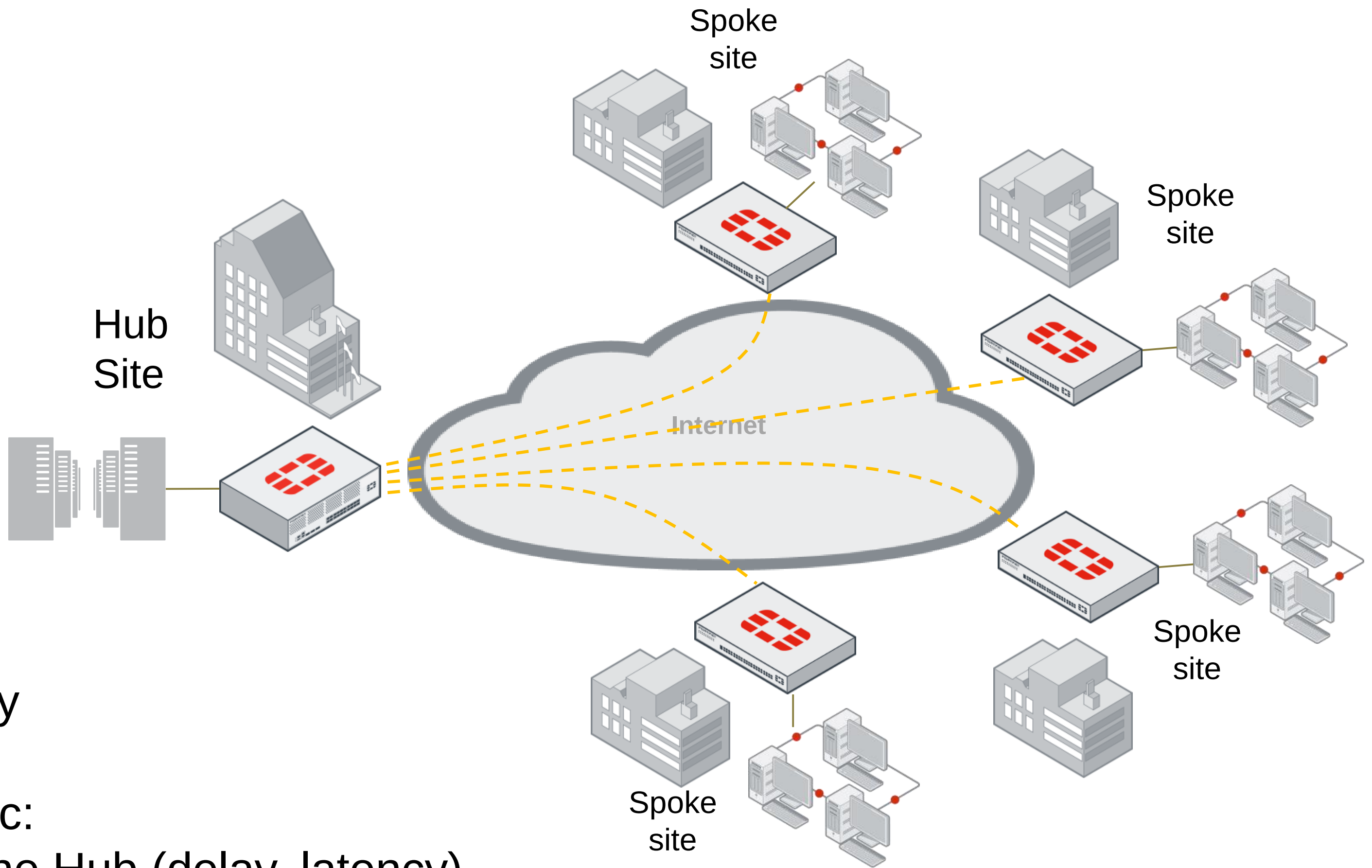
Date	Author	
2020-09-30	S. Hamelin	As of 6.4.3, shortcut tunnels can be automatically brought down when their parent tunnel goes down [link] As of 6.4, shortcuts can be negotiated between two NATed spokes so long as their NAT devices perform EIM NAT [link]
2019-09-16	S. Hamelin	Rework of the document Tunnel overlay IPs can be provisioned with IKE mode-config as of FortiOS 6.2.2 [link] 'net-device' setting available as of FortiOS 6.2.1 for Spokes' shortcuts (static phase1) [link] OSPF is supported as of FortiOS 6.2.0 [link] Additional information added for the Hub-to-Hub tunnel [link]
2018-11-22	S. Hamelin	Added the configuration snippets for *France02* spoke + correction of some config snippets
2018-06-28	S. Hamelin	Added slide and reference for the "net-device" KB article Grey background color used for slides referring to the historical dialup behavior (equivalent to "net-device enable")
2018-05-17	S. Hamelin	IKEv1 aggressive-mode is supported as of FortiOS 6.0.1 As of 5.6.3 and 6.0: new "net-device" setting for dialup phase1 (Hub)
2018-03-16	S. Hamelin	PIM/Multicast is supported as of FortiOS 5.6.1 IKE debug filter supports multiple IP addresses as of FortiOS 6.0 Added the configuration snippets for *Paris* and *Madrid* Hubs
2017-09-14	S. Hamelin	IKEv2 is supported as of FortiOS 5.6.1 ADVPN Hubs can be DNATed as of FortiOS 5.6.1 Added KB reference for this document Added KB reference for scenario mixing ADVPN & non-ADVPN Spokes
2017-02-01	S. Hamelin	Added a setting in ADVPN Spoke configuration
2016-07-01	S. Hamelin	Initial version for Fortinet *Xperts Academy* event

IPsec VPN Topology

How to organize the collection of point-to-point IPsec virtual links between all sites ?

Hub and Spoke

Hub nodes concentrate Spoke nodes in a Star topology



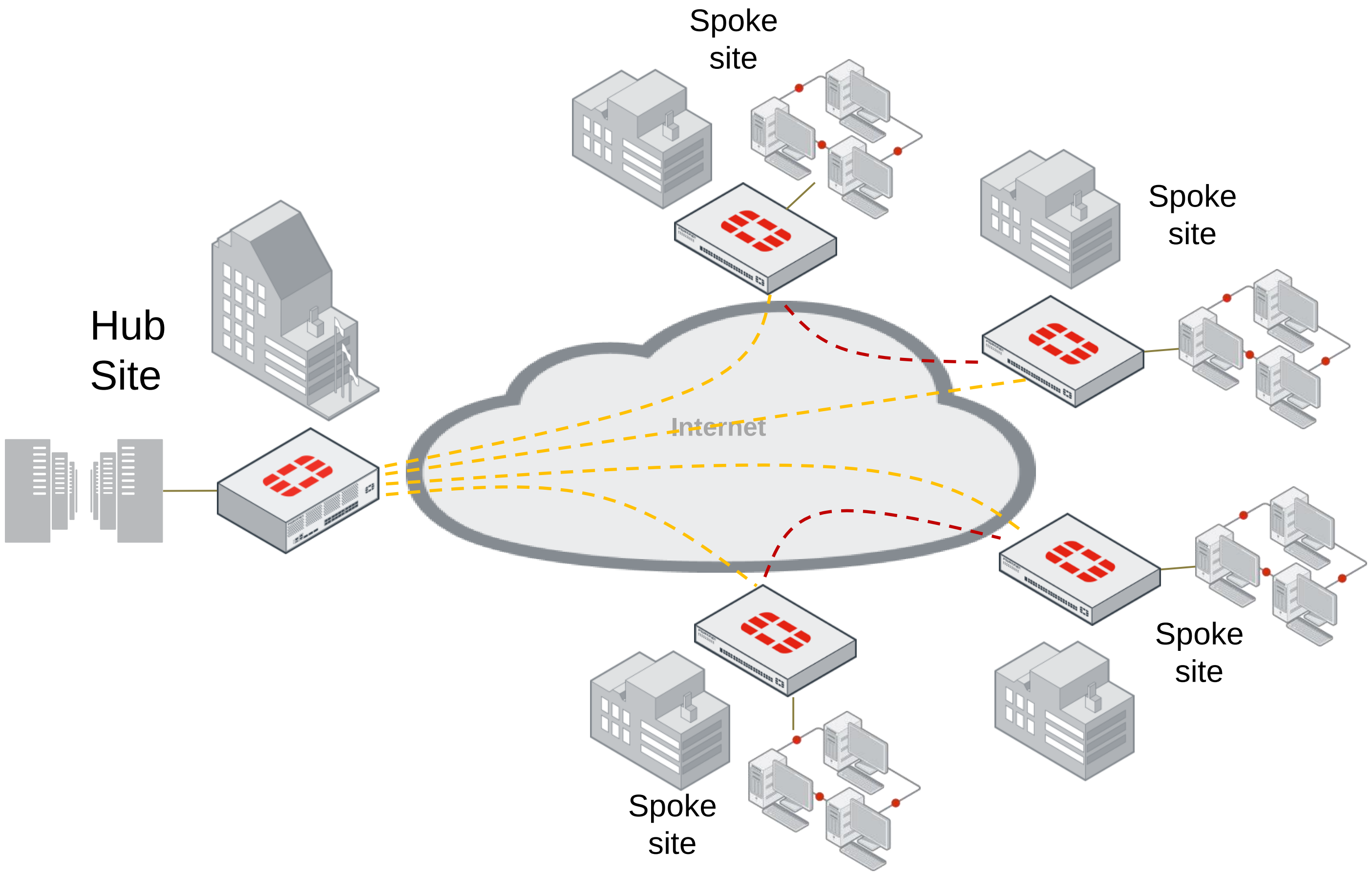
The simplest topology

Spoke to Spoke traffic:

- must go through the Hub (delay, latency)
- needlessly consume resources on Hub site (CPU, memory, Internet link)

Partial Mesh

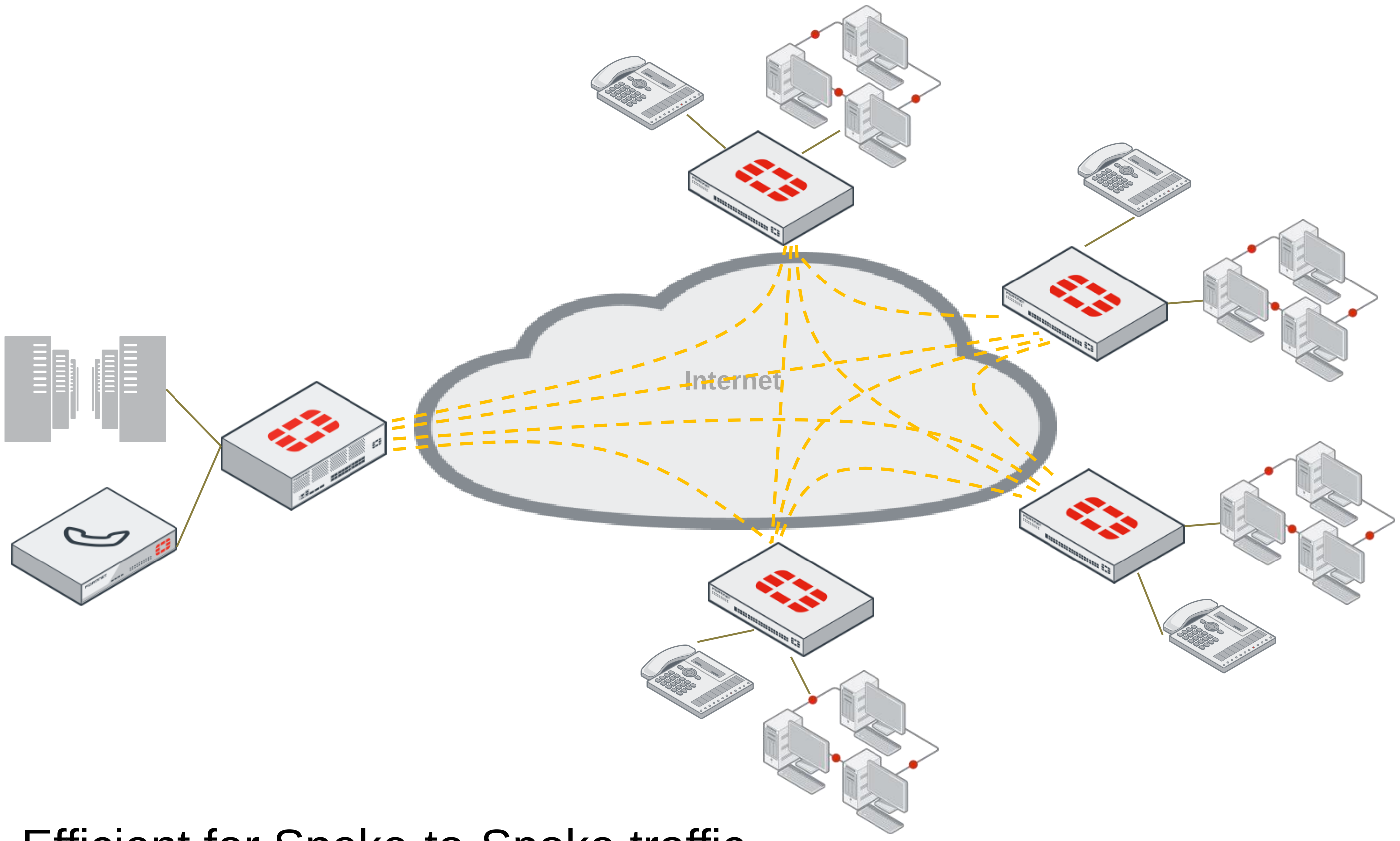
Typically a Hub-and-Spoke topology with additional direct tunnels between some Spokes



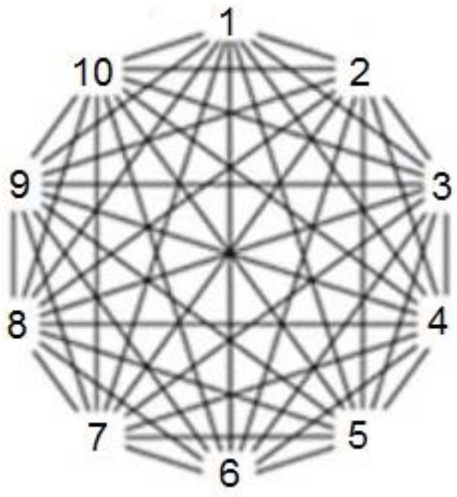
A middle ground between Hub-and-Spoke and Full-Mesh topologies

Full Mesh

Direct connectivity between all sites



N sites = N (N-1) / 2 tunnels

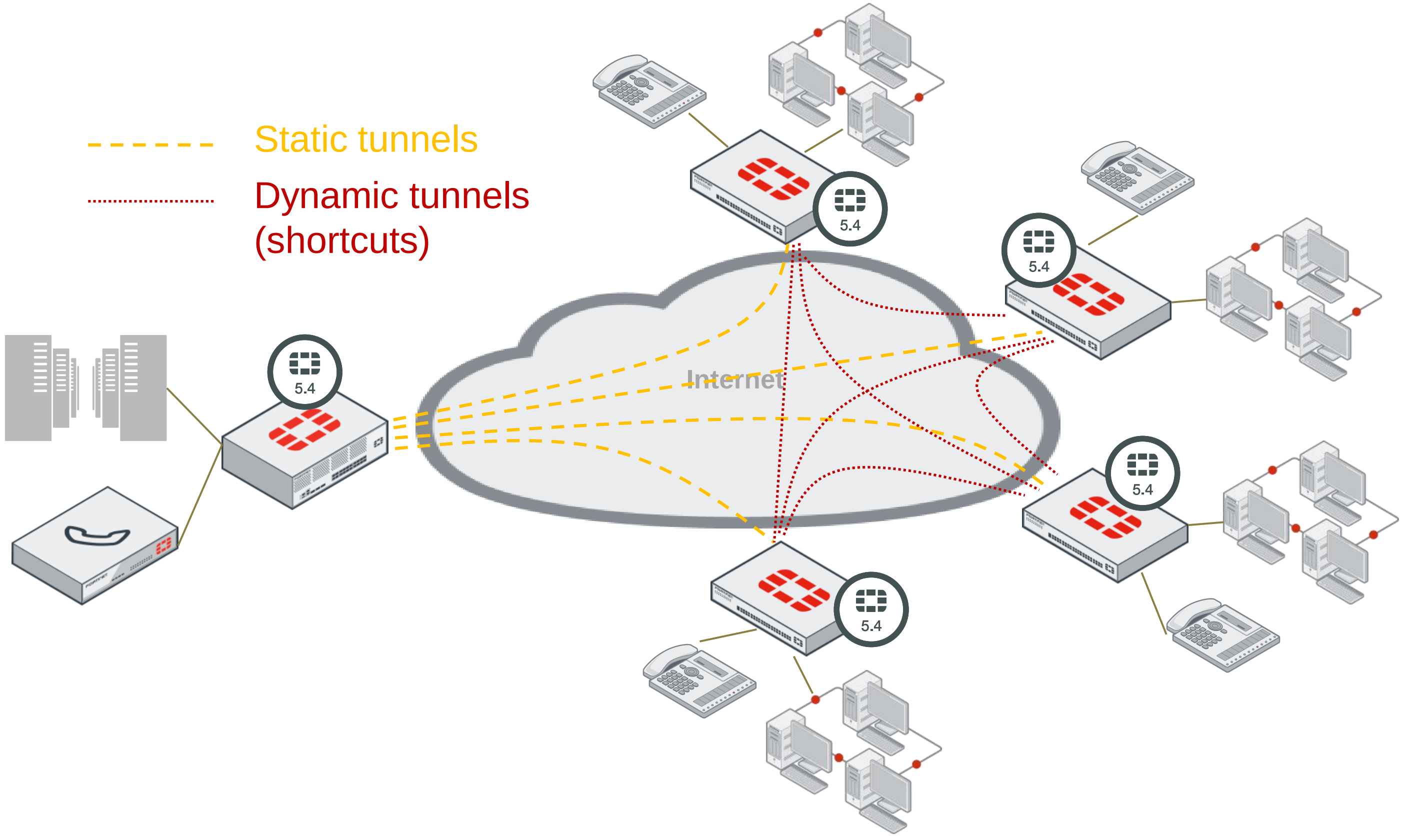


10 sites = 45 tunnels !

Efficient for Spoke-to-Spoke traffic
Complex configuration
Not scalable

Auto-Discovery VPN (as of FortiOS 5.4)

Direct connectivity between all sites



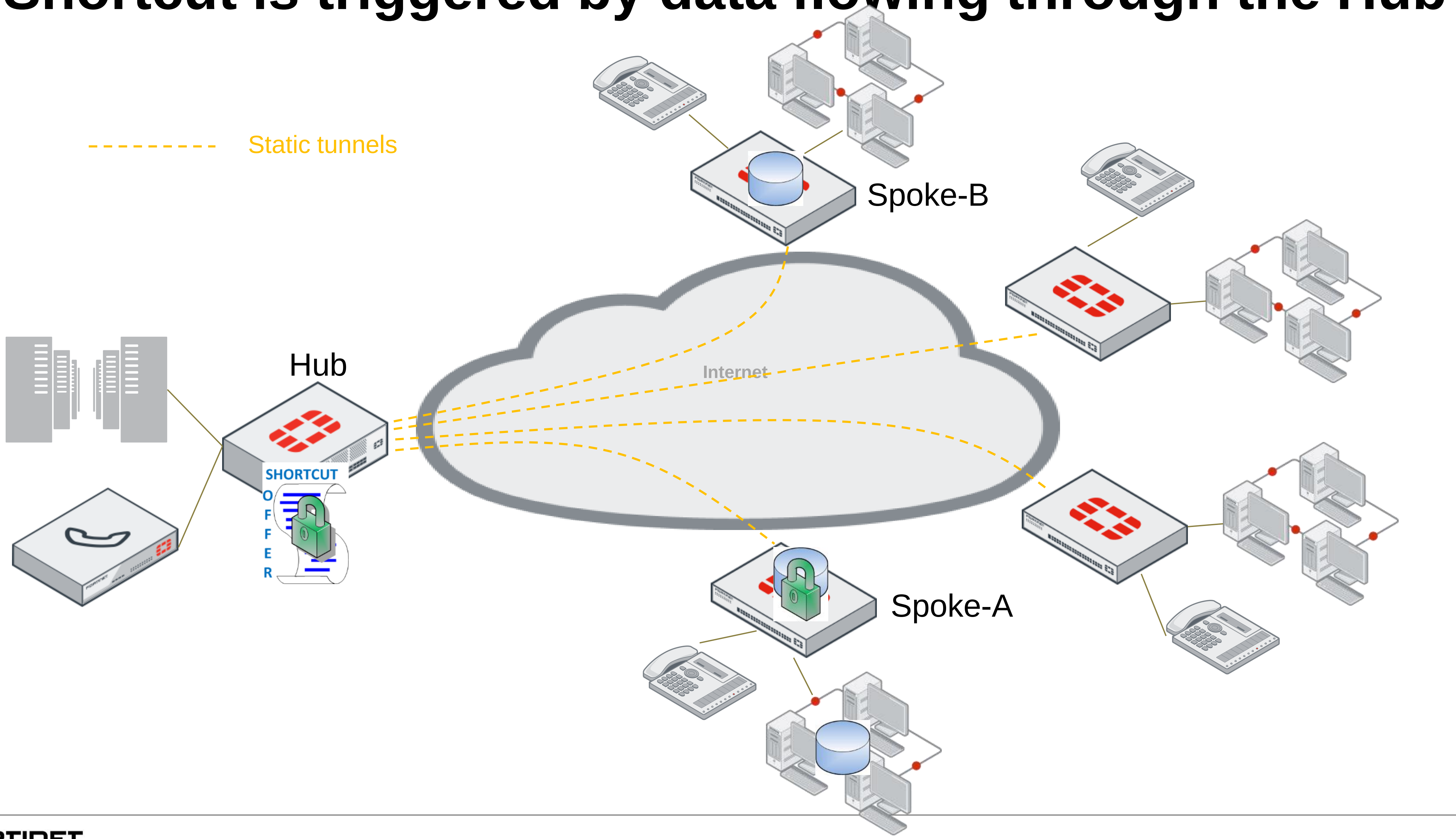
« The simplicity of Hub & Spoke
with the
efficiency of Full-Mesh »

VPN configuration is as simple as configuring a simple Hub & Spoke setup

FortiOS ADVPN

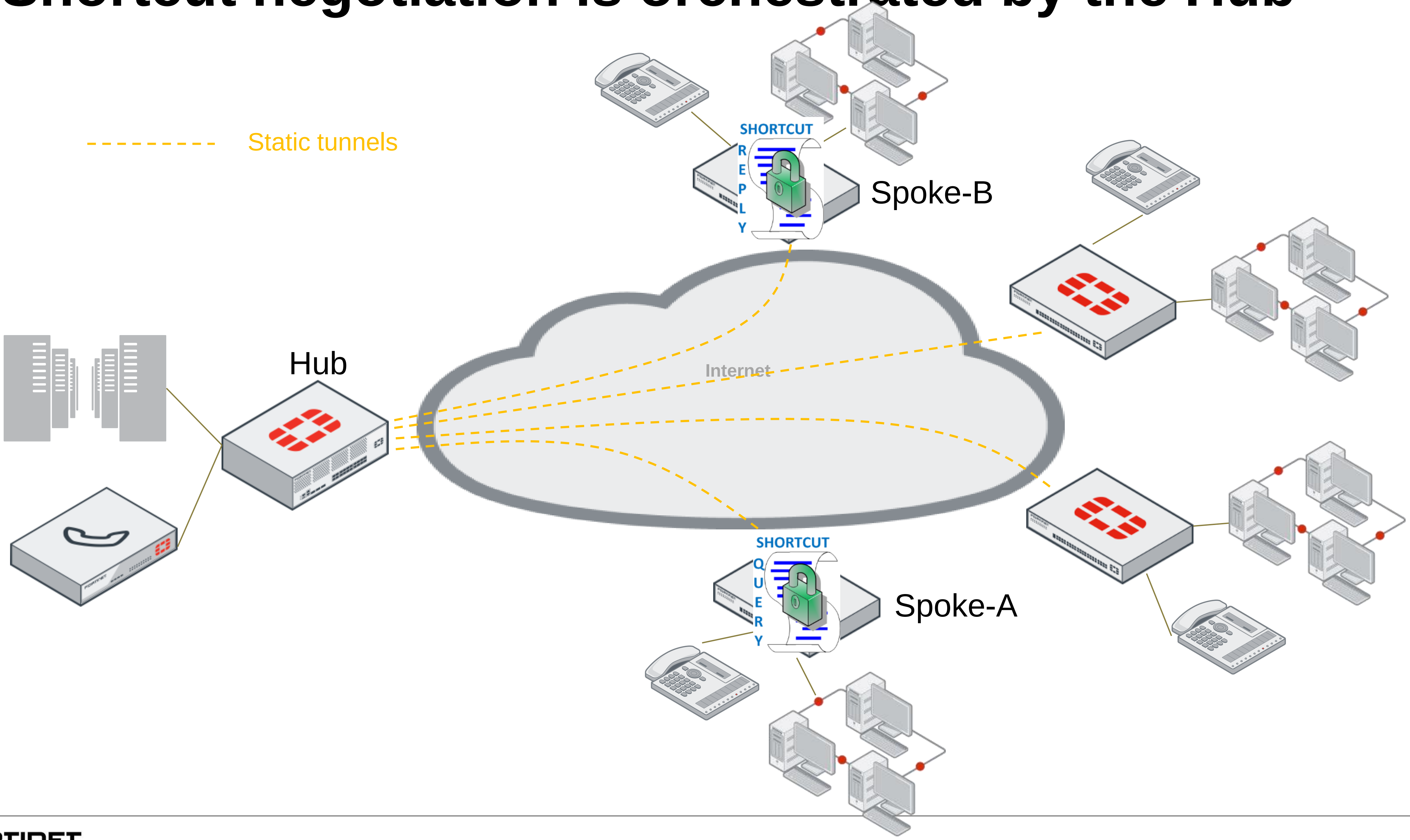
On-demand tunnels between Spokes

1 Shortcut is triggered by data flowing through the Hub



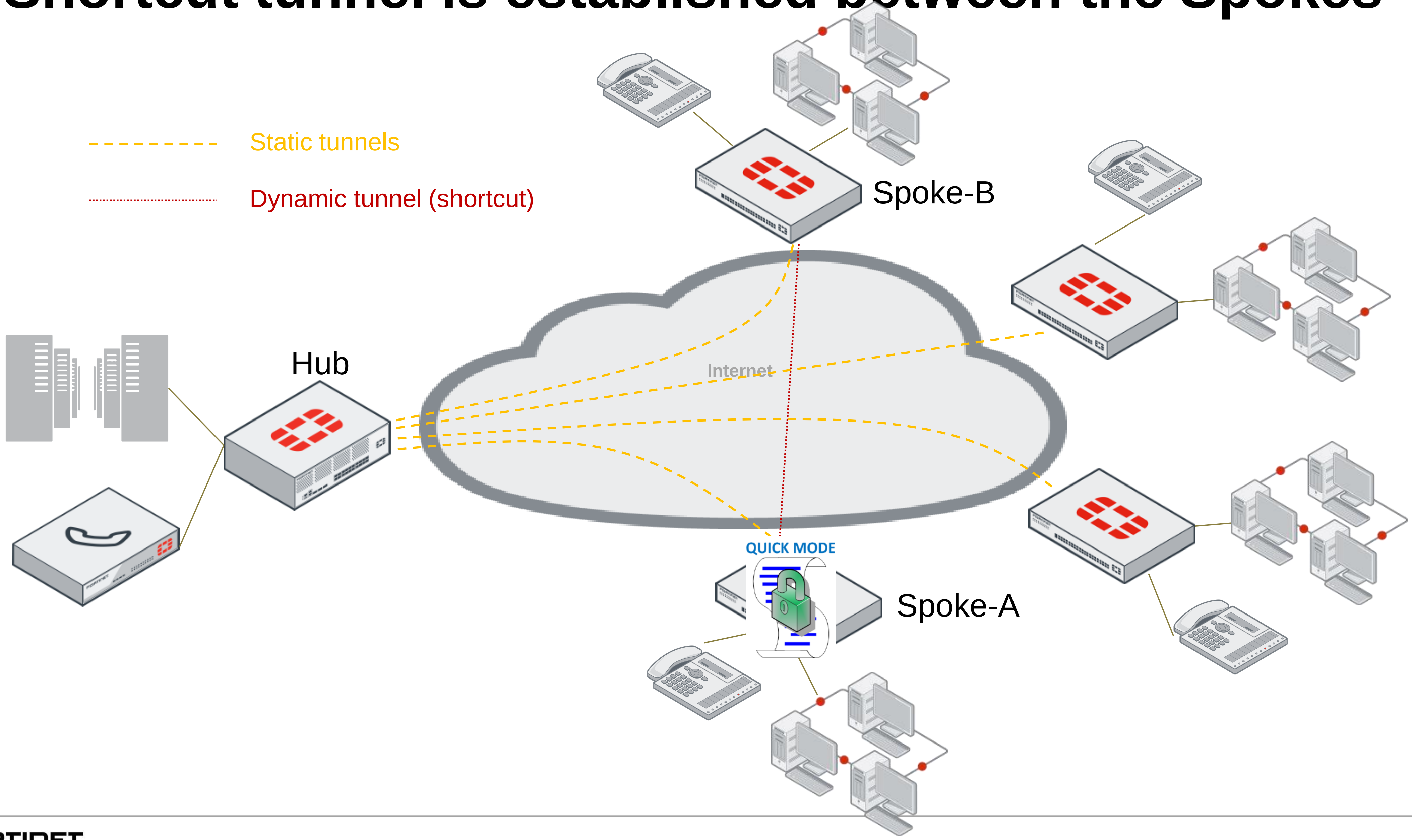
Animated Slide

② Shortcut negotiation is orchestrated by the Hub



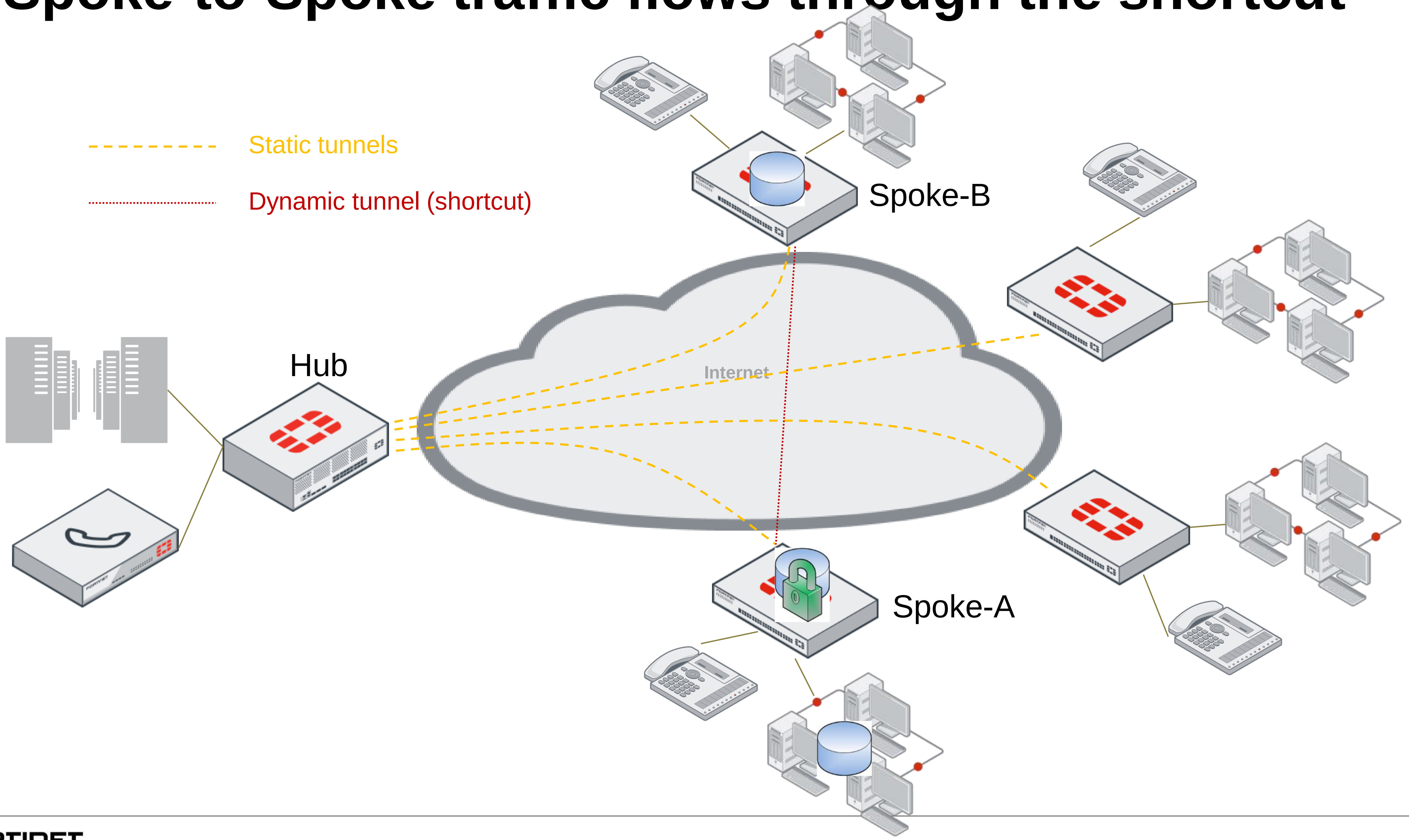
Animated Slide

3 Shortcut tunnel is established between the Spokes



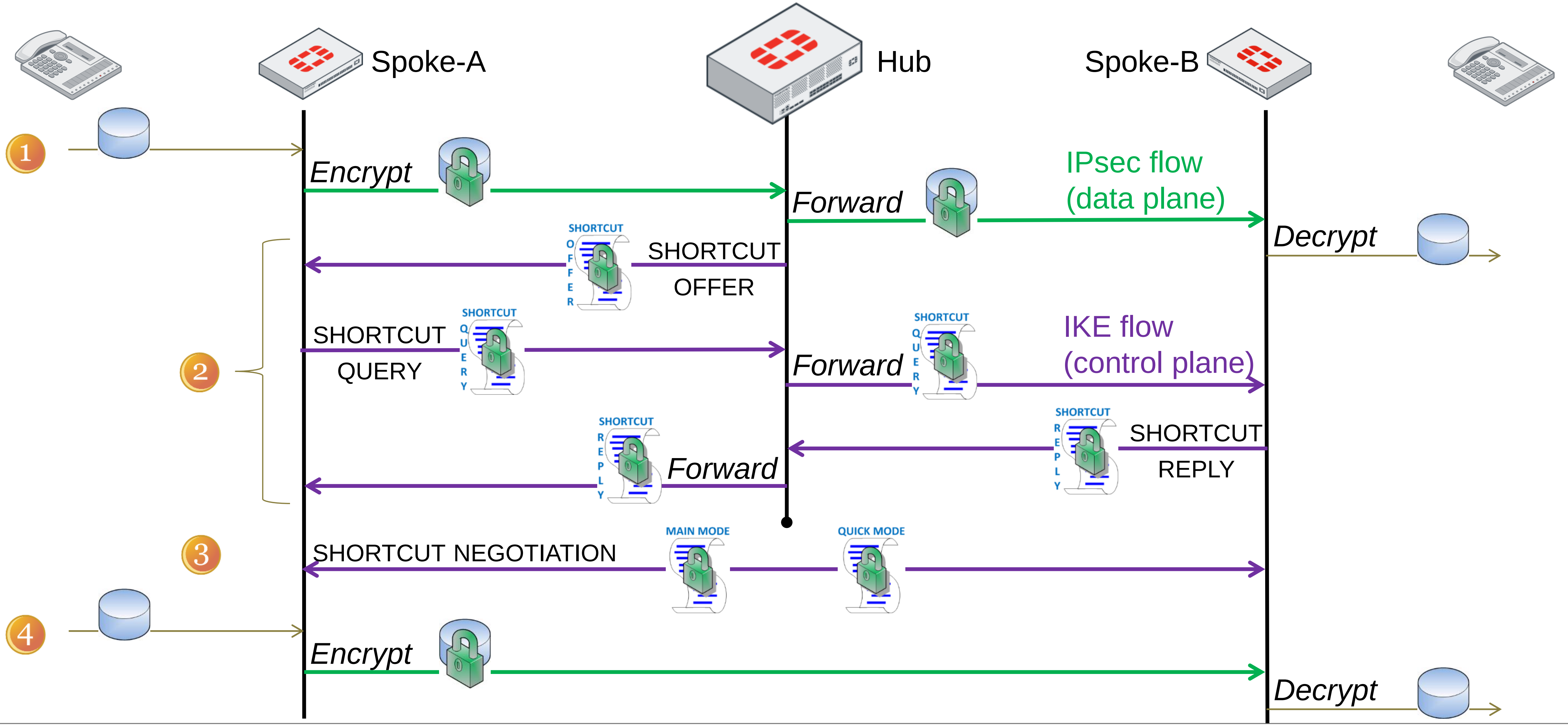
Animated Slide

4 Spoke-to-Spoke traffic flows through the shortcut



Animated Slide

Summary – ADVPN Sequence of Events



[IKE debug details]

Fortinet Auto-Discovery VPN

Fortinet ADVPN is a proprietary solution solely based on IKE & IPsec

It is incompatible with Cisco DMVPN which relies on mGRE-over-IPsec and NHRP

IPsec:

- IKEv1 main-mode is supported (pre-shared key & certificate authentication)
- IKEv1 aggressive-mode is supported as of FortiOS 6.0.1 (pre-shared key & certificate authentication)
- IKEv2 is supported as of FortiOS 5.6.1

- Both IPv4 IPsec & IPv6 IPsec are supported

Dynamic Routing:

- BGP and RIPv2/RIPng are supported
- PIM/Multicast is supported as of FortiOS 5.6.1
- OSPF is supported as of FortiOS 6.2

- IS-IS over IPsec is *not* supported

Fortinet Auto-Discovery VPN

It is mandatory that the Hub runs FortiOS 5.4 (or newer)

The Hub is responsible for triggering the shortcut OFFER and for relaying the shortcut QUERY/REPLY messages between the Spokes. The Hub must run at least FortiOS 5.4 if shortcuts are desired.

It is *not* mandatory that all Spokes be FortiGate running FOS 5.4 (or newer)

If a Spoke runs a firmware older than FortiOS 5.4 or if it is an IPsec Gateway from another vendor, it can still participate to the Hub & Spoke architecture but it will not be able to negotiate shortcuts with other Spokes.

Connecting ADVPN and non-ADVPN IPsec gateways on the same Hub's phase1 requires specific configuration on the Hub and the non-ADVPN gateways:

KB article http://kb.fortinet.com/kb/documentLink.do?externalID=FD40359

A single ADVPN Domain

All interconnected ADVPN tunnels belong to the same ADVPN Domain

Use cases:

- I would like to spread the Spokes between my two ISPs (wan1, wan2)
  Will the Spokes bound to the phase1 on wan1 be able to establish shortcuts with the Spokes bound to the phase1 on wan2 ?

  Yes, no additional configuration is required to cover this scenario.

- I need to connect two independent Hub & Spoke regions. Is it possible to establish cross-region shortcuts ?

  Yes. It requires that an IPsec tunnel be configured between the Hubs of each region.
  This scenario is the *Reference Architecture* used in this document.

- I want to create multiple ADVPN domains. Spokes from a domain can only establish shortcuts with Spokes from the same domain. Cross-domain shortcuts are not allowed.

  FortiOS has no support for ADVPN Domains. All spokes belong to a single ADVPN domain.
  Shortcut negotiations can take place between any Spoke of the ADVPN domain.

NAT with ADVPN

Hub behind NAT

- Support for the Hub being DNATed is supported as of FortiOS 5.6.1

Spokes behind NAT

- *As of FortiOS 6.4*

- An ADVPN shortcut can be negotiated between two NATed Spokes so long as their NAT devices perform *Endpoint Independent Mapping* (EIM) NAT

- EIM NAT = *Destination Independent NAT*

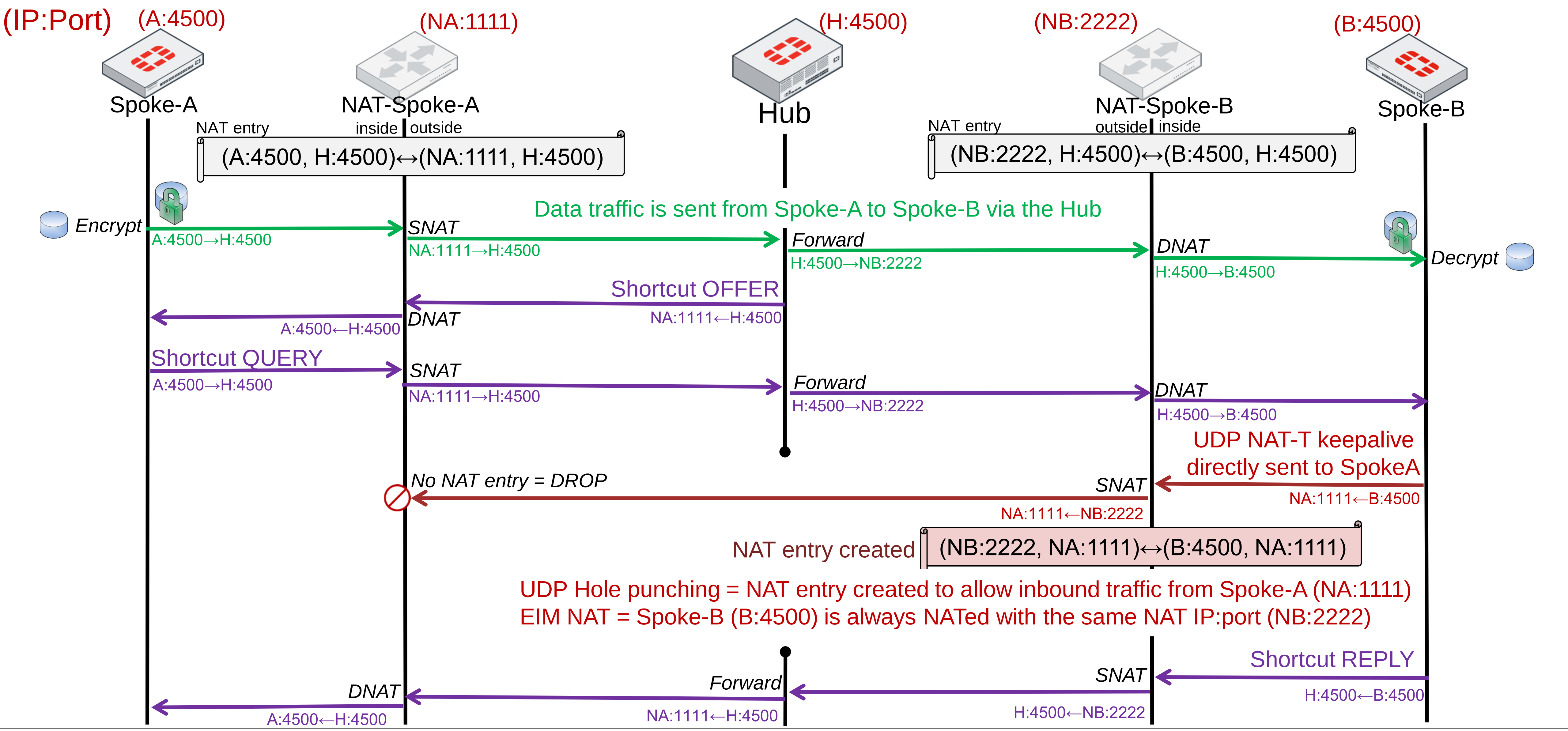
  - An internal host with (src-ip, src-port) is always SNATed with the same (nat-src-ip, nat-src-port) regardless of the (dst-ip, dst-port) being accessed

  - UDP Hole punching is used by FortiOS to open NAT entries on the NAT devices

- *Up to FortiOS 6.2*

- A shortcut can be negotiated between two Spokes only if one of the two Spokes is not NATed.
  A shortcut cannot be established between two Spokes that are both NATed.

ADVPN shortcut negotiation between two NATed Spokes – UDP Hole punching



(IP:Port)

(A:4500) Spoke-A

(NA:1111) NAT-Spoke-A

(H:4500) Hub

(NB:2222) NAT-Spoke-B

(B:4500) Spoke-B

NAT entry inside | outside

(A:4500, H:4500)↔(NA:1111, H:4500)

NAT entry outside | inside

(NB:2222, H:4500)↔(B:4500, H:4500)

Data traffic is sent from Spoke-A to Spoke-B via the Hub

Encrypt A:4500→H:4500

SNAT NA:1111→H:4500

Forward H:4500→NB:2222

DNAT H:4500→B:4500

Decrypt

Shortcut OFFER

NA:1111←H:4500

DNAT A:4500←H:4500

Shortcut QUERY

A:4500→H:4500

SNAT NA:1111→H:4500

Forward H:4500→NB:2222

DNAT H:4500→B:4500

UDP NAT-T keepalive directly sent to SpokeA

NA:1111←B:4500

SNAT NA:1111←NB:2222

No NAT entry = DROP

NAT entry created (NB:2222, NA:1111)↔(B:4500, NA:1111)

UDP Hole punching = NAT entry created to allow inbound traffic from Spoke-A (NA:1111)
EIM NAT = Spoke-B (B:4500) is always NATed with the same NAT IP:port (NB:2222)

Shortcut REPLY

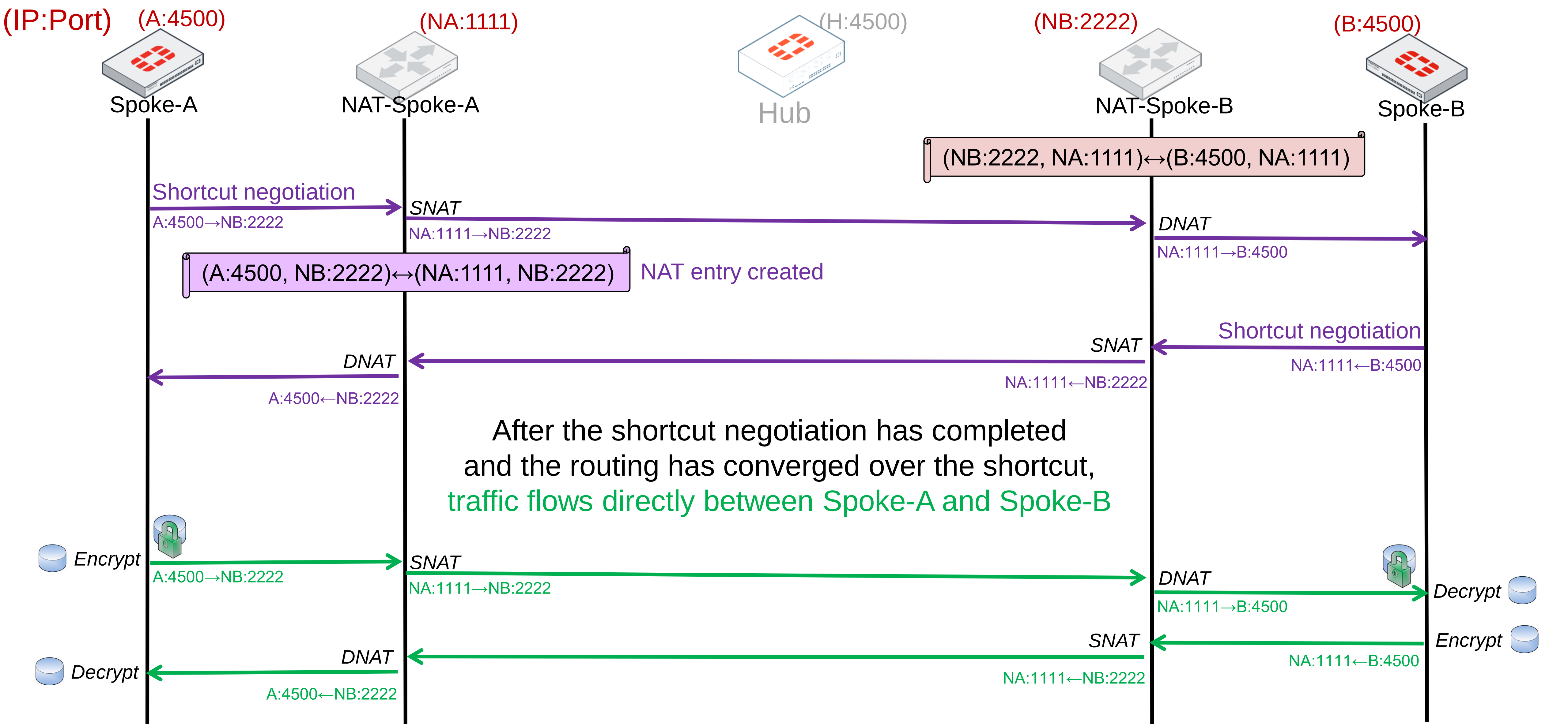
H:4500←B:4500

SNAT H:4500←NB:2222

Forward NA:1111←H:4500

DNAT A:4500←H:4500

ADVPN shortcut negotiation between two NATed Spokes – UDP Hole punching



(IP:Port)

(A:4500) Spoke-A

(NA:1111) NAT-Spoke-A

(H:4500) Hub

(NB:2222) NAT-Spoke-B

(B:4500) Spoke-B

(NB:2222, NA:1111)↔(B:4500, NA:1111)

Shortcut negotiation A:4500→NB:2222

SNAT NA:1111→NB:2222

DNAT NA:1111→B:4500

(A:4500, NB:2222)↔(NA:1111, NB:2222) NAT entry created

Shortcut negotiation NA:1111←B:4500

SNAT NA:1111←NB:2222

DNAT A:4500←NB:2222

After the shortcut negotiation has completed and the routing has converged over the shortcut, traffic flows directly between Spoke-A and Spoke-B

Encrypt A:4500→NB:2222

SNAT NA:1111→NB:2222

DNAT NA:1111→B:4500 Decrypt

Encrypt NA:1111←B:4500

SNAT NA:1111←NB:2222

DNAT A:4500←NB:2222 Decrypt

Lifetime of ADVPN shortcuts

Interplay between a shortcut tunnel (spoke ↔ spoke) and its parent tunnel (spoke ↔ Hub)

As of FortiOS 6.4.3

A shortcut tunnel can be torn down automatically when its parent tunnel goes down :

```
config vpn ipsec phase1-interface
  edit <tunnel-to-the-Hub>
      set auto-discovery-receiver enable
      set auto-discovery-shortcuts dependent
  next
end
```

By default, a shortcut tunnel is independent from its parent tunnel
It is *not* torn down automatically when its parent tunnel goes down

```
config vpn ipsec phase1-interface
  edit <tunnel-to-the-Hub>
      set auto-discovery-receiver enable
      set auto-discovery-shortcuts independent
  next
end
```

Lifetime of ADVPN shortcuts

Interplay between a shortcut tunnel (spoke ↔ spoke) and its parent tunnel (spoke ↔ Hub)

Up to FortiOS 6.4.2

Shortcuts are independent from their parent tunnel
Shortcuts are *not* automatically brought down when their parent tunnel goes down
This behavior is not configurable

Shortcuts can be torn down when they are idle

```
config vpn ipsec phase1-interface
  edit <tunnel-to-the-Hub>
      set idle-timeout enable              // default= disable
      set idle-timeoutinterval <minutes>  // default=15, range=[5 ; 43200]
  next
end
```

Reference Architecture

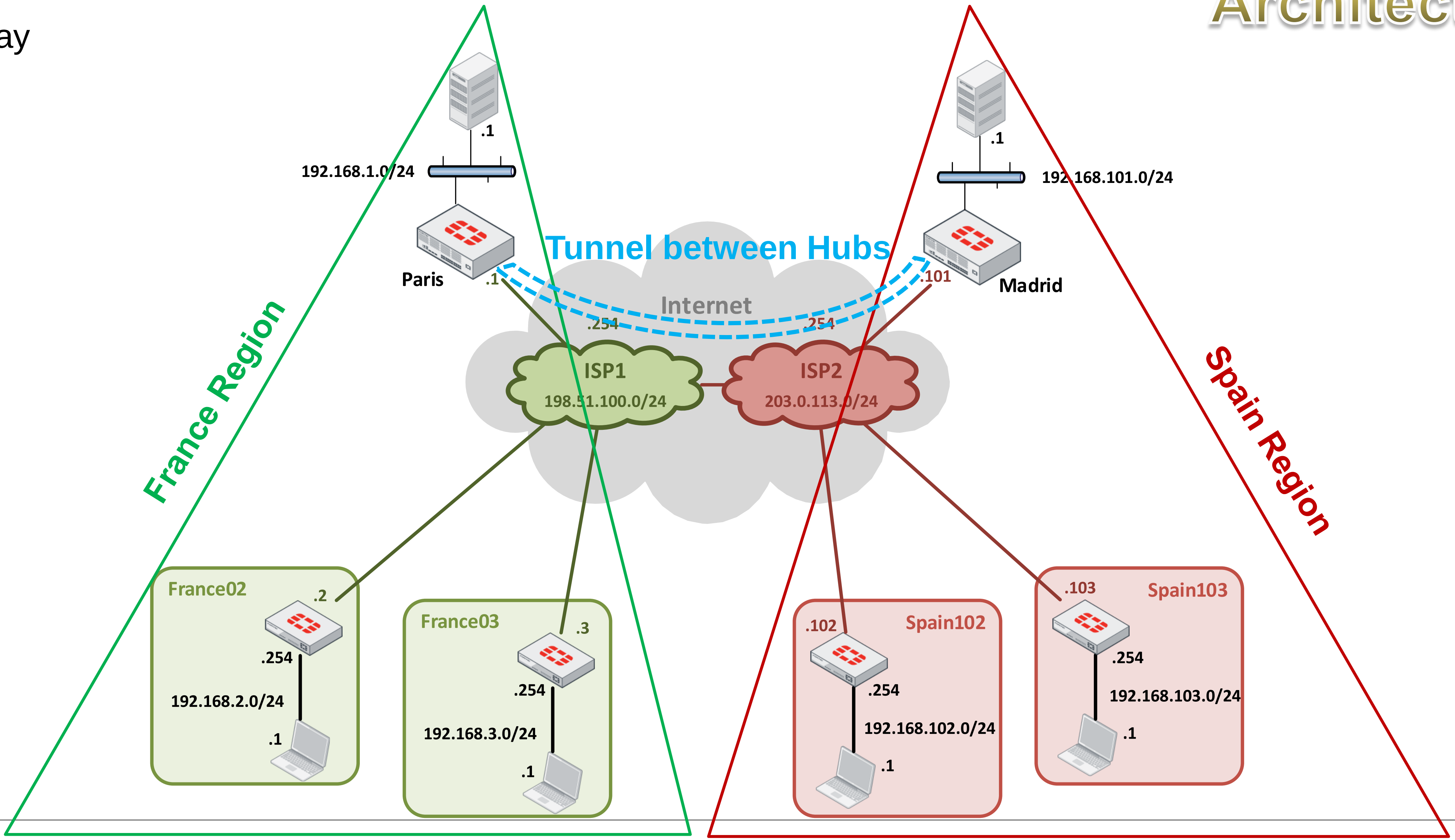
Dual Region

Interconnecting two independent Hub & Spoke Regions

Dual Region

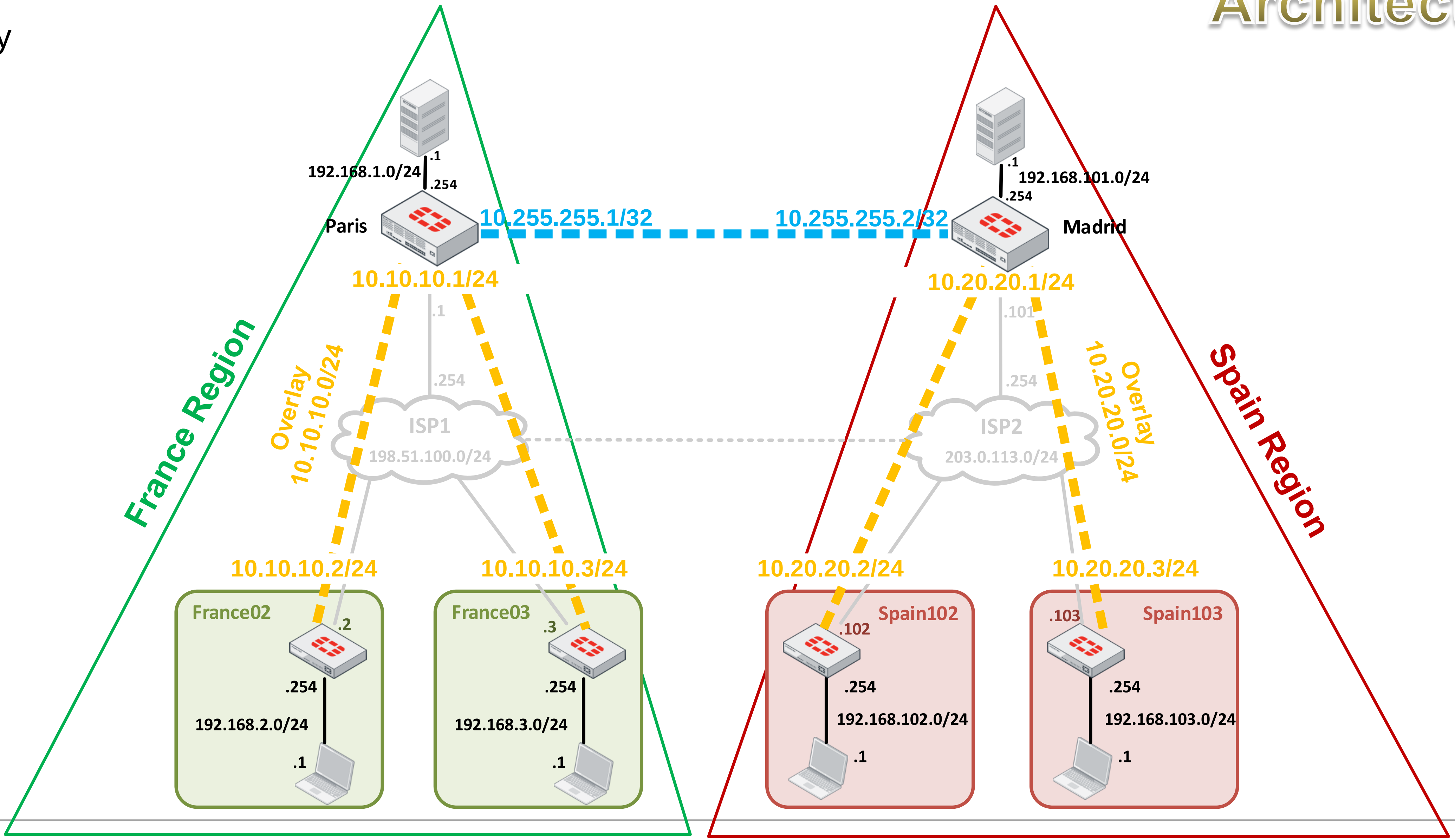
Reference Architecture

Underlay



Dual Region

Overlay



Dual Region

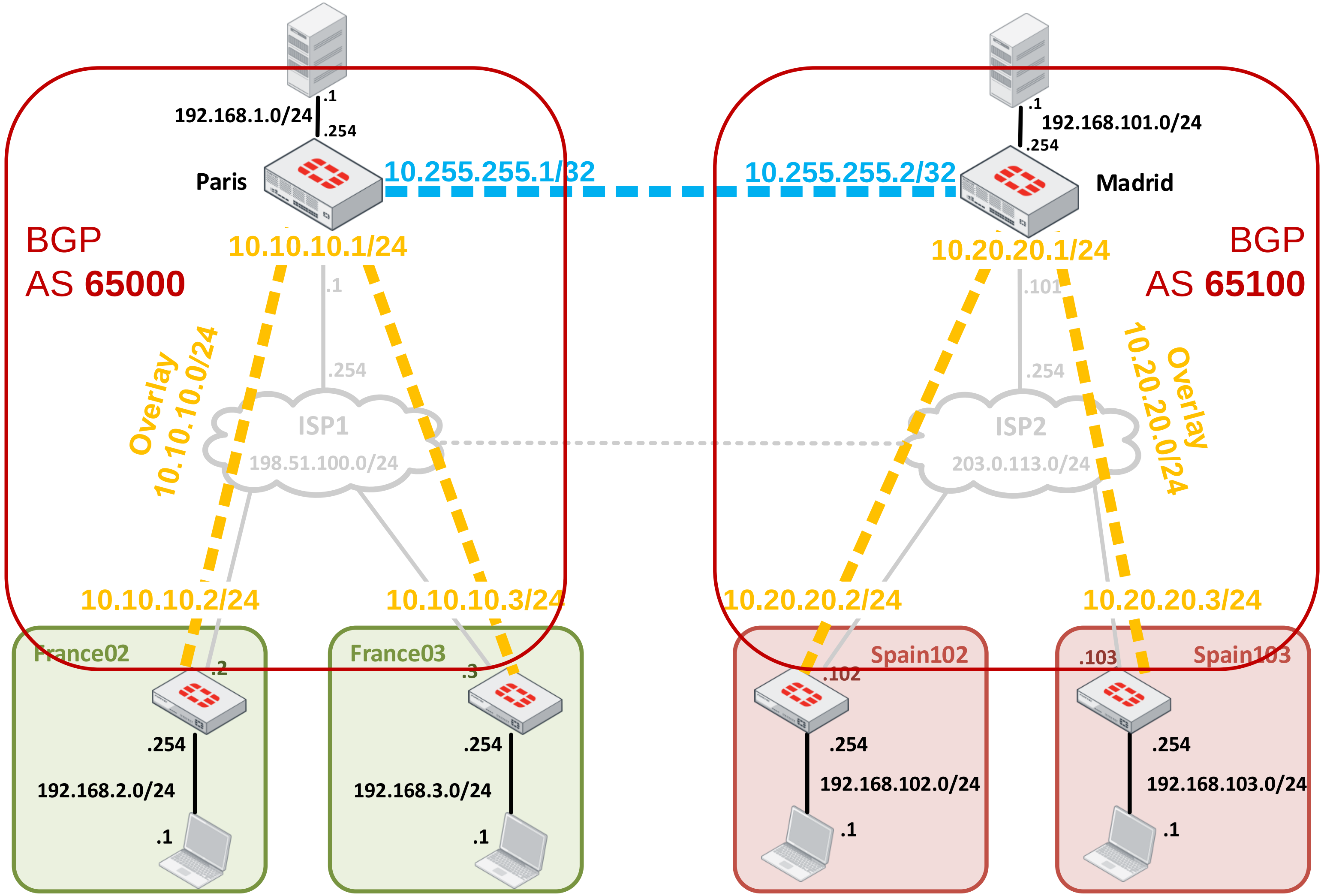
Overlay

Reference Architecture

Each region has a distinct AS

iBGP is used for intra-region routing

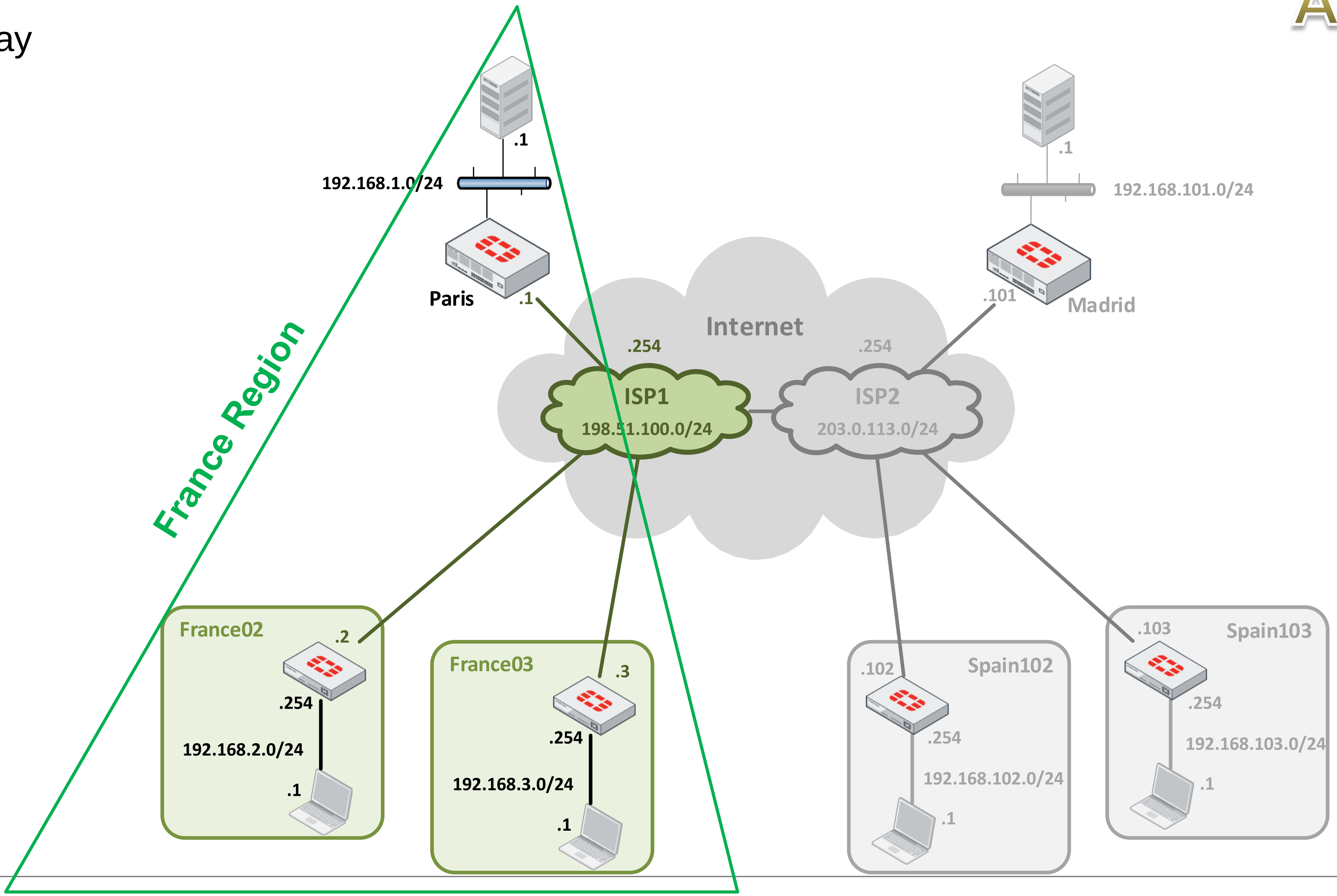
eBGP is used for inter-region routing



France Region

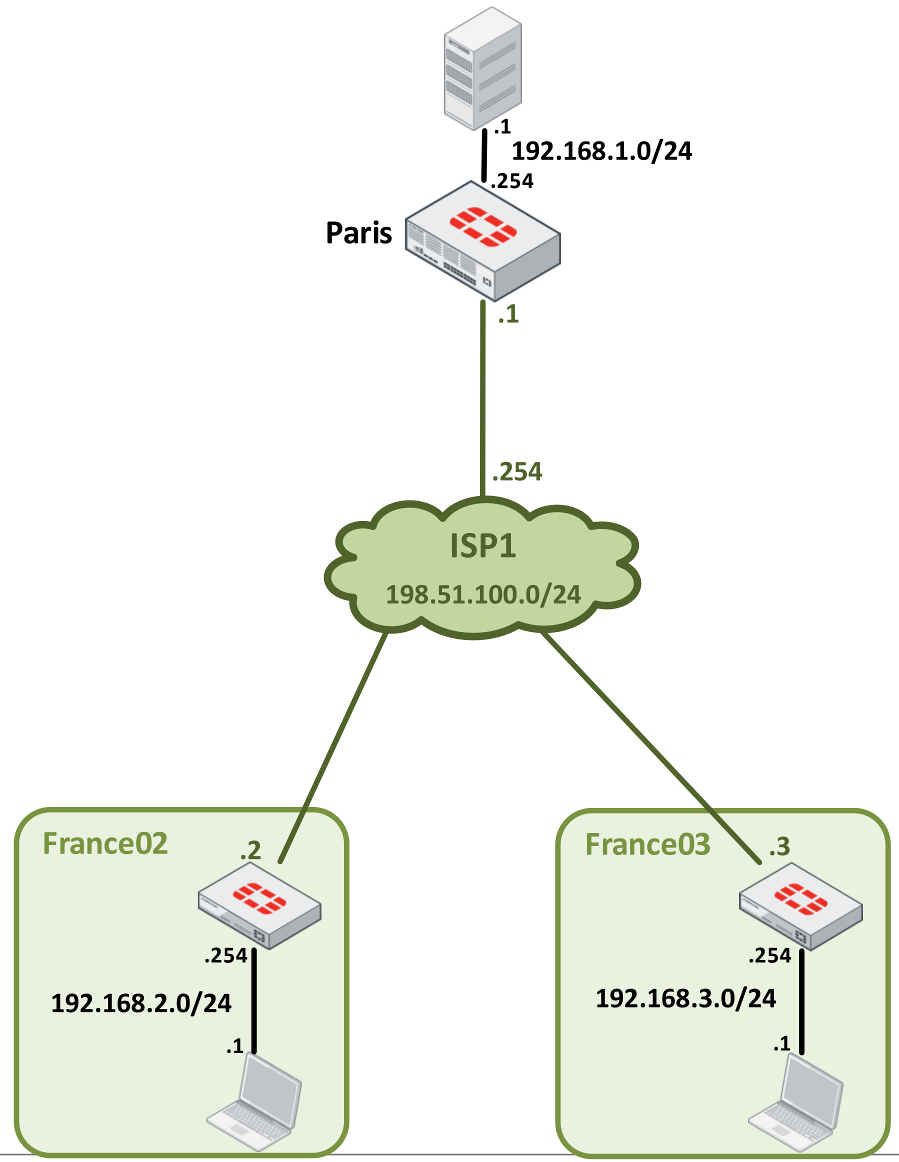
Reference Architecture

Underlay



France Region

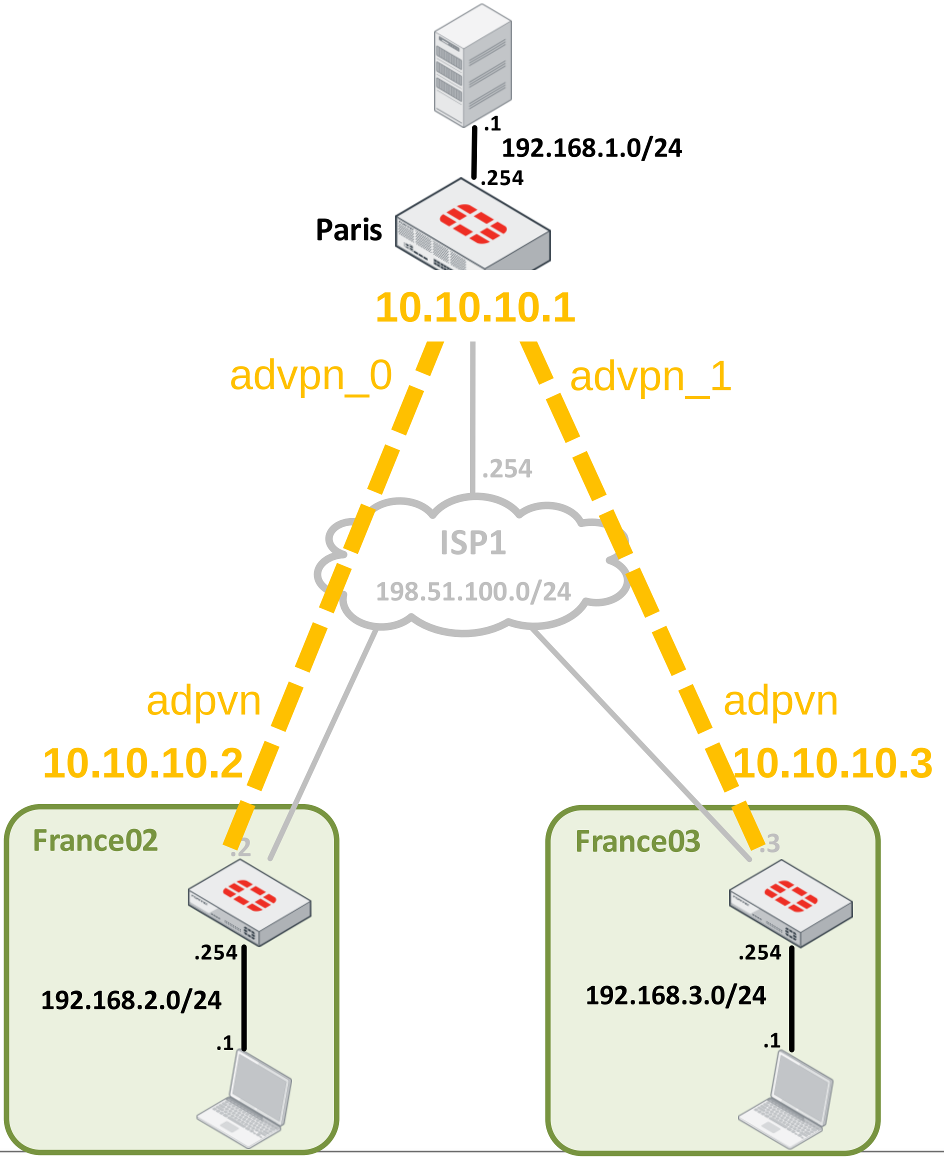
Underlay



France Region

Reference Architecture

Overlay



Overlay IPs

Overlay IPs of the Spokes (10.10.10.x) can be provisioned in two ways:

- Manually on each Spoke

HUB

```
config system interface
  edit "advpn"
    set ip 10.10.10.1/32
    set remote-ip 10.10.10.254/24
  next
end
```

Spoke

```
config system interface
  edit "advpn"
    set ip 10.10.10.2/32
    set remote-ip 10.10.10.1/24
  next
end
```

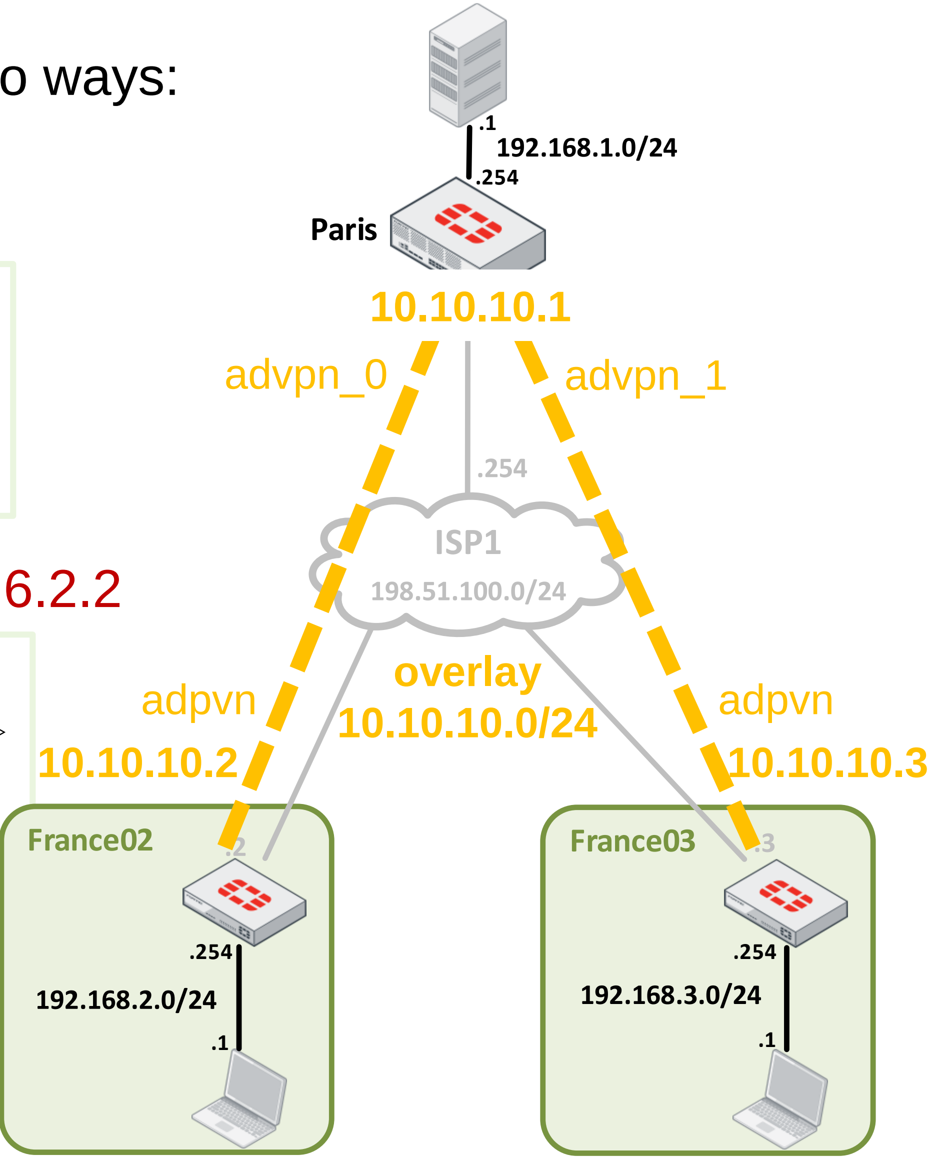
- Automatically from the Hub using IKE mode-config as of FOS 6.2.2

HUB

```
config system interface
  edit "advpn"
    set ip 10.10.10.1/32
    set remote-ip 10.10.10.254/24
  next
end

config vpn ipsec phase1-interface
 edit "advpn"
   set mode-cfg enable
   set ipv4-start-ip 10.10.10.2
   set ipv4-end-ip 10.10.10.253
   set ipv4-netmask 255.255.255.0
 next
end
```

Spoke

```
config system interface
  edit "advpn"
   < do not configure an IP here >
  next
end


config vpn ipsec phase1-interface
 edit "advpn"
   set mode-cfg enable
  next
end
```



IPsec configuration

Hub

ADVPN Hub configuration

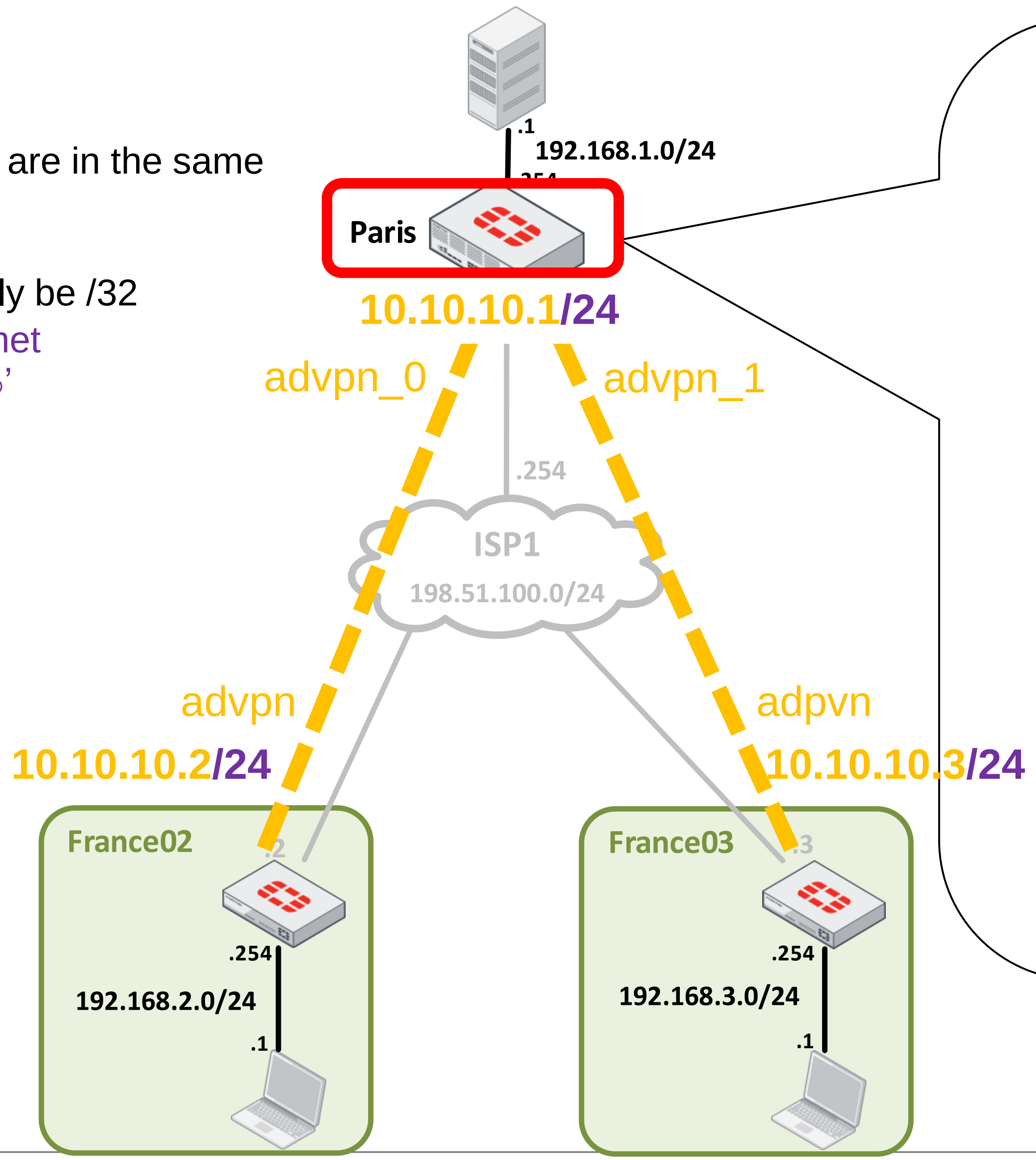
/24

The overlay IPs of all ADVPN participants are in the same subnet

The mask for the local `ip` can only be /32
So, the mask for the overlay subnet must be specified in ‘`remote-ip`’

```
set ip 10.10.10.1/32
Set remote-ip 10.10.10.254/24
```

The `remote-ip` is an unused IP from the overlay subnet



```
config vpn ipsec phase1-interface
    edit "advpn"
        set type dynamic
        set net-device disable
        set tunnel-search nexthop
        set interface "wan"
        set proposal aes128-sha1
        set auto-discovery-sender enable
        set add-route disable
        set psksecret xxxxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "adpvn"
        set phase1name "advpn"
        set proposal aes128-sha1
    next
end

config system interface
  edit "advpn"
    set ip 10.10.10.1/32
    set remote-ip 10.10.10.254/24
  next
end
```

ADVPN Hub configuration

net-device disable

Default setting for dialup phase1 as of FortiOS 6.0 & 5.6.3

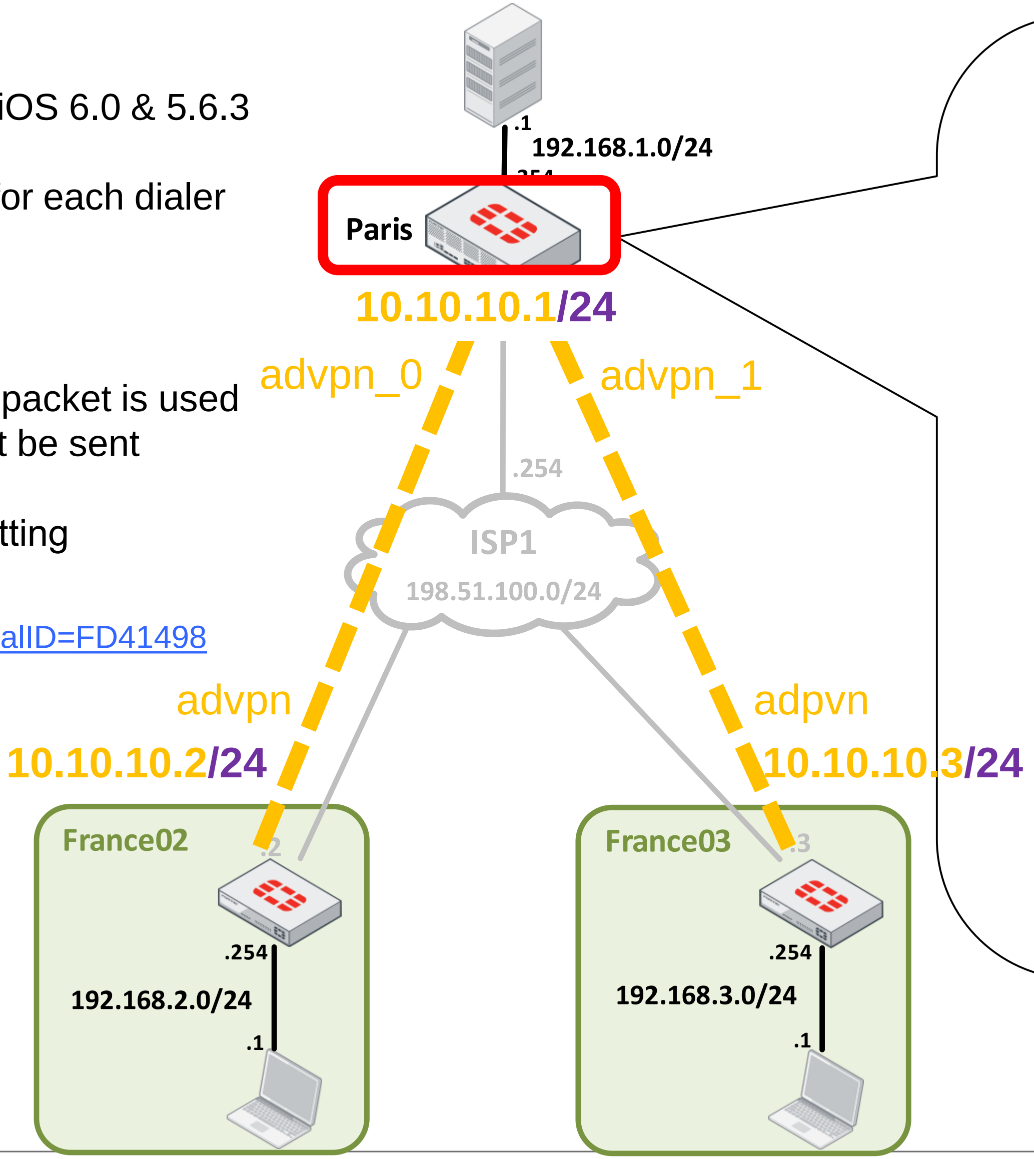
A dedicated interface is no longer created for each dialer
“advpn” is used as a shared interface

tunnel-search nexthop

The next-hop IP of the route matched by a packet is used to decide into which tunnel the packet must be sent

Detailed information about “**net-device**” setting is available in **KB Article FD41498**

https://kb.fortinet.com/kb/documentLink.do?externalID=FD41498



```
config vpn ipsec phase1-interface
    edit "advpn"
        set type dynamic
        set net-device disable
        set tunnel-search nexthop
        set interface "wan"
        set proposal aes128-sha1
        set auto-discovery-sender enable
        set add-route disable
        set psksecret xxxxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "adpvn"
        set phase1name "advpn"
        set proposal aes128-sha1
    next
end

config system interface
  edit "advpn"
    set ip 10.10.10.1/32
    set remote-ip 10.10.10.254/24
  next
end
```

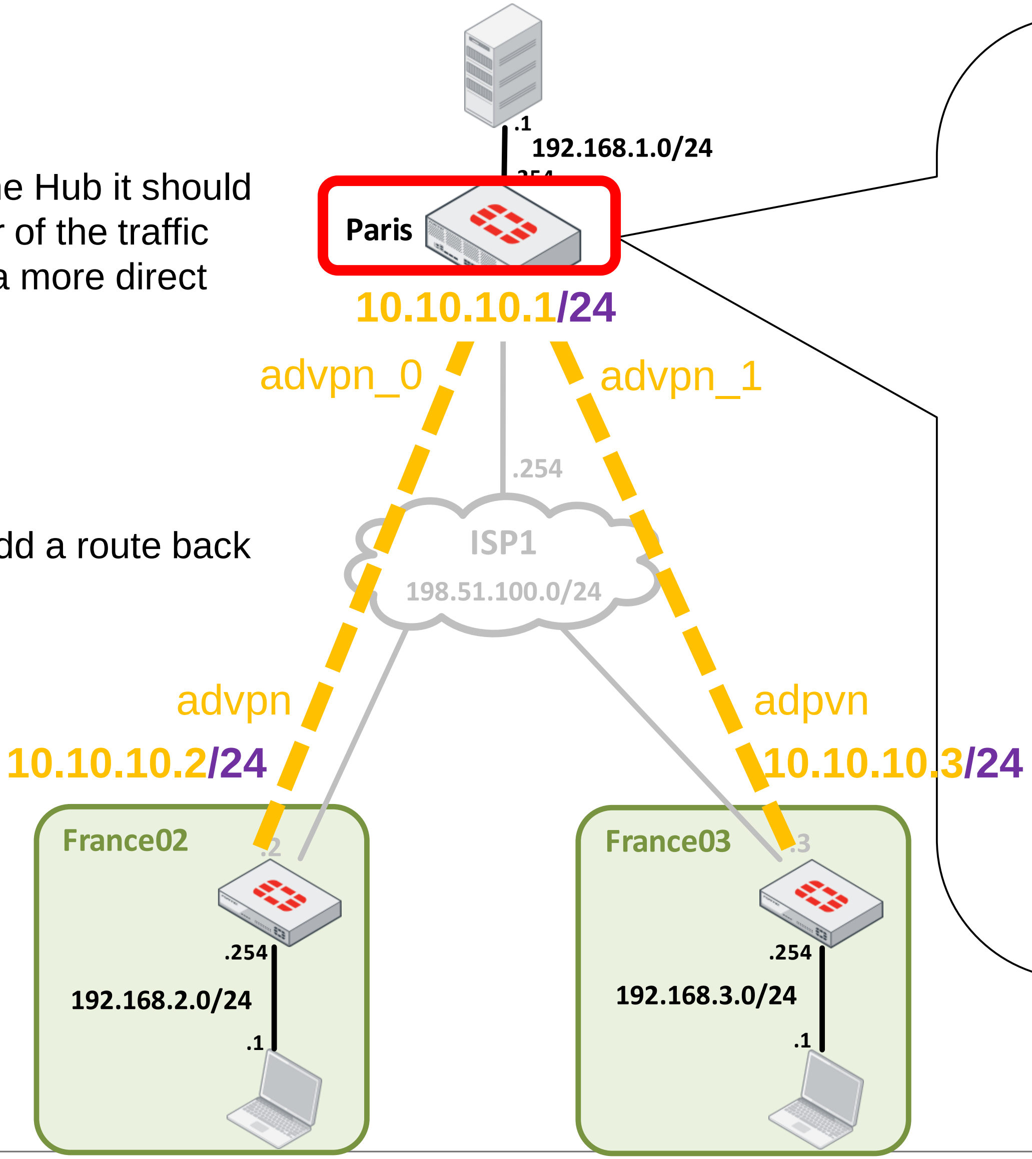
ADVPN Hub configuration

auto-discovery-sender enable

Indicates that when IPsec traffic transits the Hub it should send a SHORTCUT-OFFER to the initiator of the traffic to indicate that it could perhaps establish a more direct connection (shortcut)

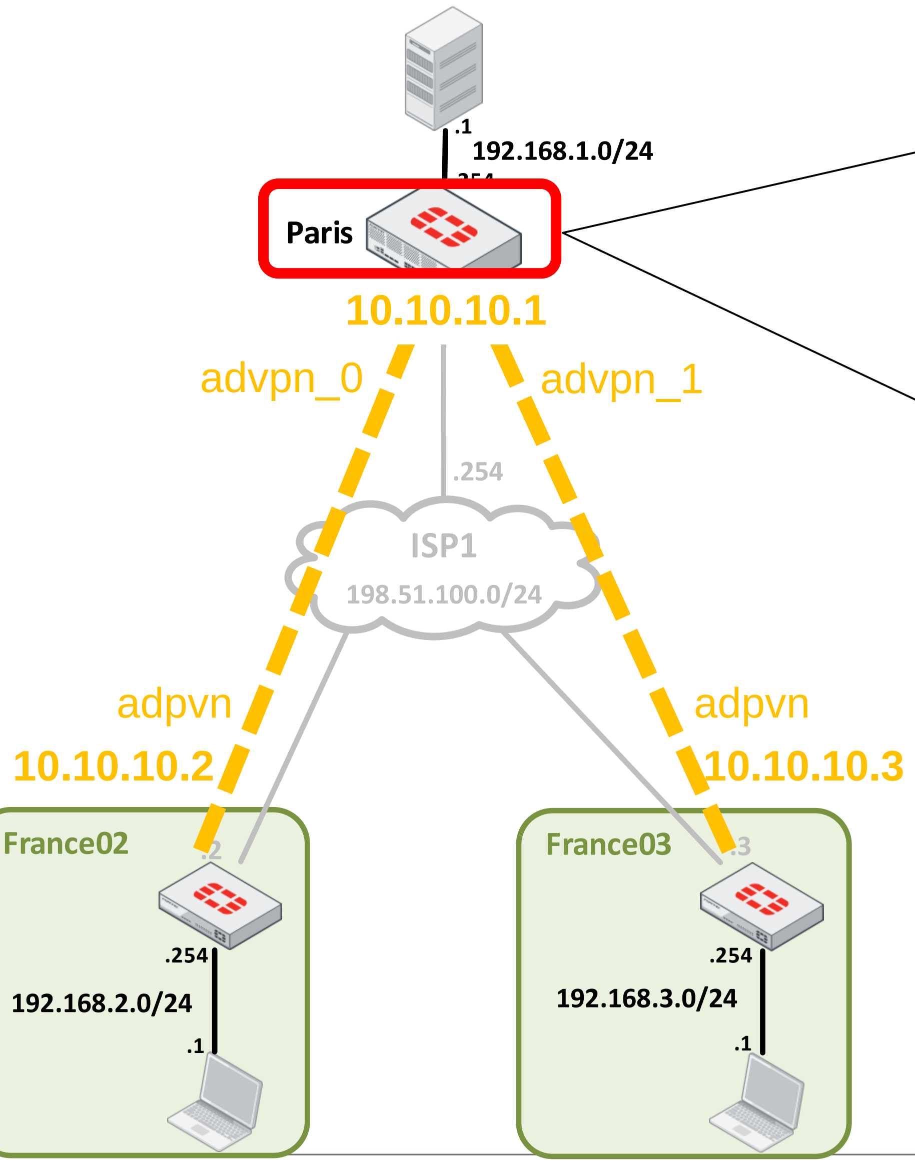
add-route disable

ensures that IKE does not automatically add a route back over the spoke and instead leaves routing to a separately configured routing protocol



```
config vpn ipsec phase1-interface
    edit "advpn"
        set type dynamic
        set net-device disable
        set tunnel-search nexthop
        set interface "wan"
        set proposal aes128-sha1
        set auto-discovery-sender enable
        set add-route disable
        set psksecret xxxxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "adpvn"
        set phase1name "advpn"
        set proposal aes128-sha1
    next
end

config system interface
  edit "advpn"
    set ip 10.10.10.1/32
    set remote-ip 10.10.10.254/24
  next
end
```

ADVPN Hub configuration



```
config firewall policy
    edit 1
        set name "To Spokes"
        set srcintf "internal"
        set dstintf "advpn"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "From Spokes"
        set srcintf "advpn"
        set dstintf "internal"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 3
        set name "Spokes to Spokes"
        set srcintf "advpn"
        set dstintf "advpn"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

ADVPN Hub configuration

Hub configured with "net-device enable"

⚠ This setting is **not recommended** and is **not supported for SD-WAN**

net-device enable

A dedicated interface is created for each dialer

This was FortiOS behavior up to 5.6.2.

As of 5.6.3 & 6.0, this behavior is not the default behavior and is not recommended

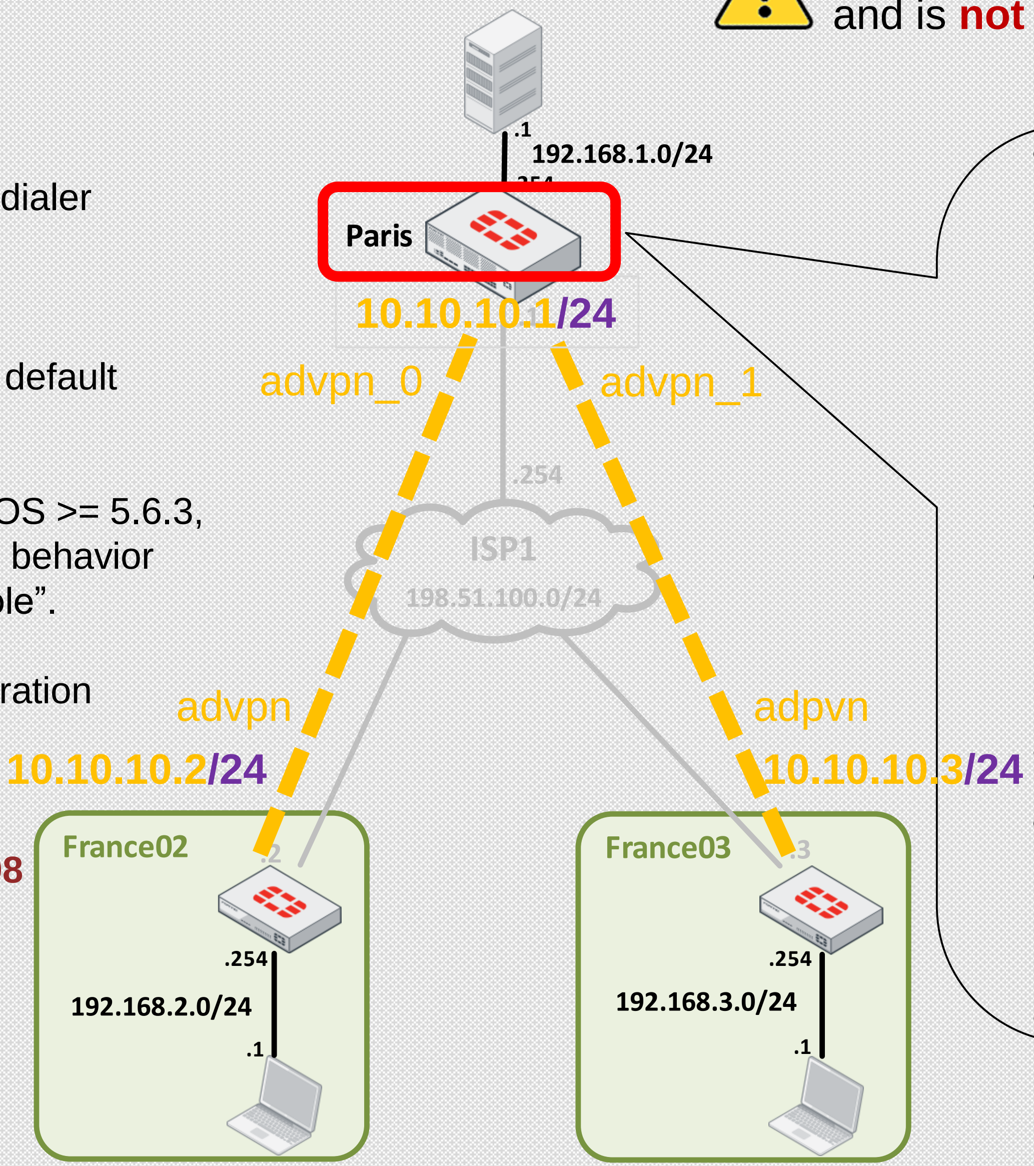
When upgrading from FOS <= 5.6.2 to FOS >= 5.6.3, the upgrade process retains the previous behavior by means of CLI setting "net-device enable".

It is recommended to change the configuration to "net-device disable" after upgrade

Detailed information about "**net-device**" setting is available in **KB Article FD41498**

https://kb.fortinet.com/kb/documentLink.do?externalID=FD41498

The `remote-ip` is dummy
It can be any unused IP



```
config vpn ipsec phase1-interface
    edit "advpn"
        set type dynamic
        set interface "wan"
        set net-device enable
        set proposal aes128-sha1
        set auto-discovery-sender enable
        set add-route disable
        set psksecret xxxxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "advpn"
        set phase1name "advpn"
        set proposal aes128-sha1
    next
end

config system interface
    edit "advpn"
        set ip 10.10.10.1/32
        set remote-ip 10.10.10.254/24
    next
end
```

ADVPN Hub configuration

Hub running FortiOS 5.4.x, 5.6.0, 5.6.1, 5.6.2

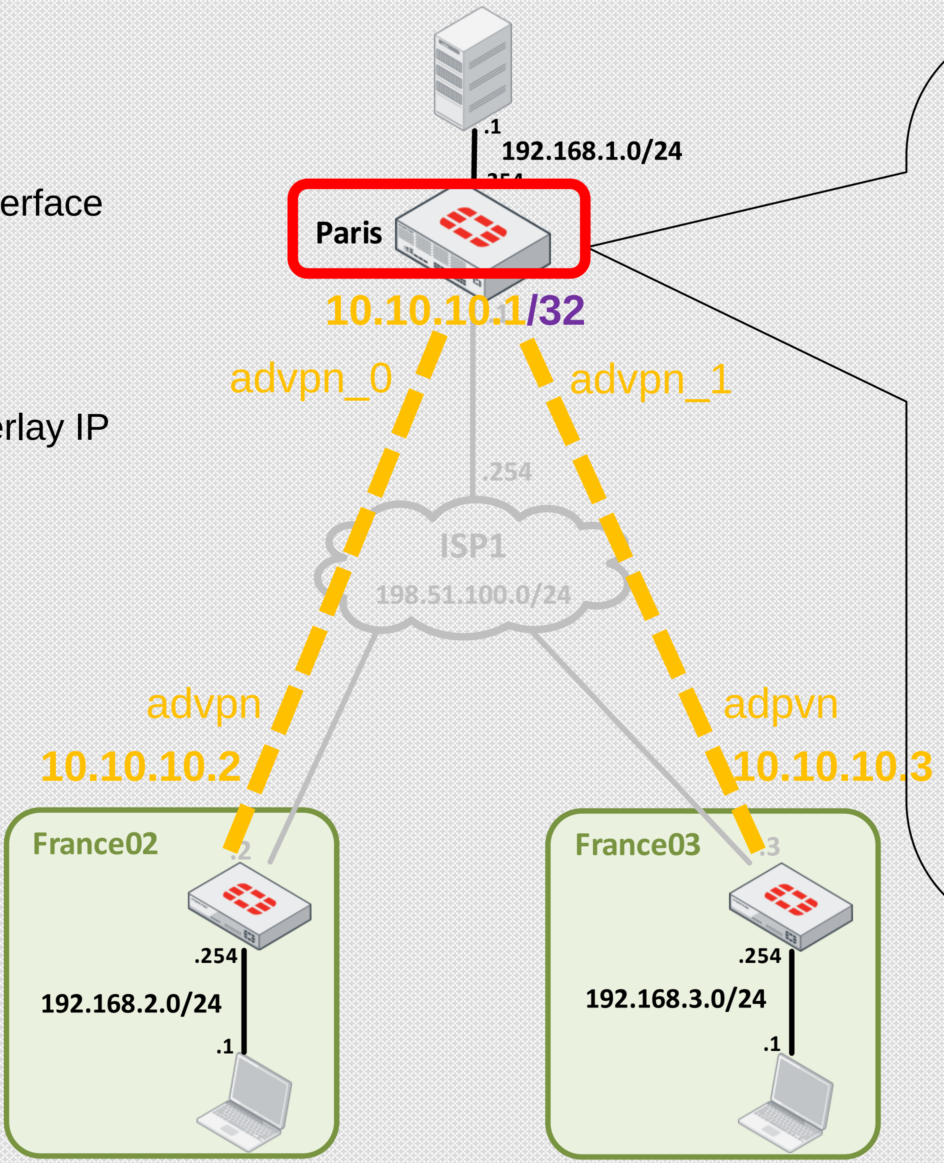
/32

With FortiOS 5.4.x & 5.6.[0-2], a tunnel interface can only be a point-to-point interface.

The only possible mask is /32

A /32 host IP address is configured as overlay IP

The `remote-ip` is dummy
It can be any unused IP



```
config vpn ipsec phase1-interface
    edit "advpn"
        set type dynamic
        set interface "wan"
        set proposal aes128-sha1
        set auto-discovery-sender enable
        set add-route disable
        set psksecret xxxxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "advpn"
        set phase1name "advpn"
        set proposal aes128-sha1
    next
end

config system interface
    edit "advpn"
        set ip 10.10.10.1/32
        set remote-ip 10.10.10.254
    next
end
```

IPsec configuration

Spoke

ADVPN Spoke configuration

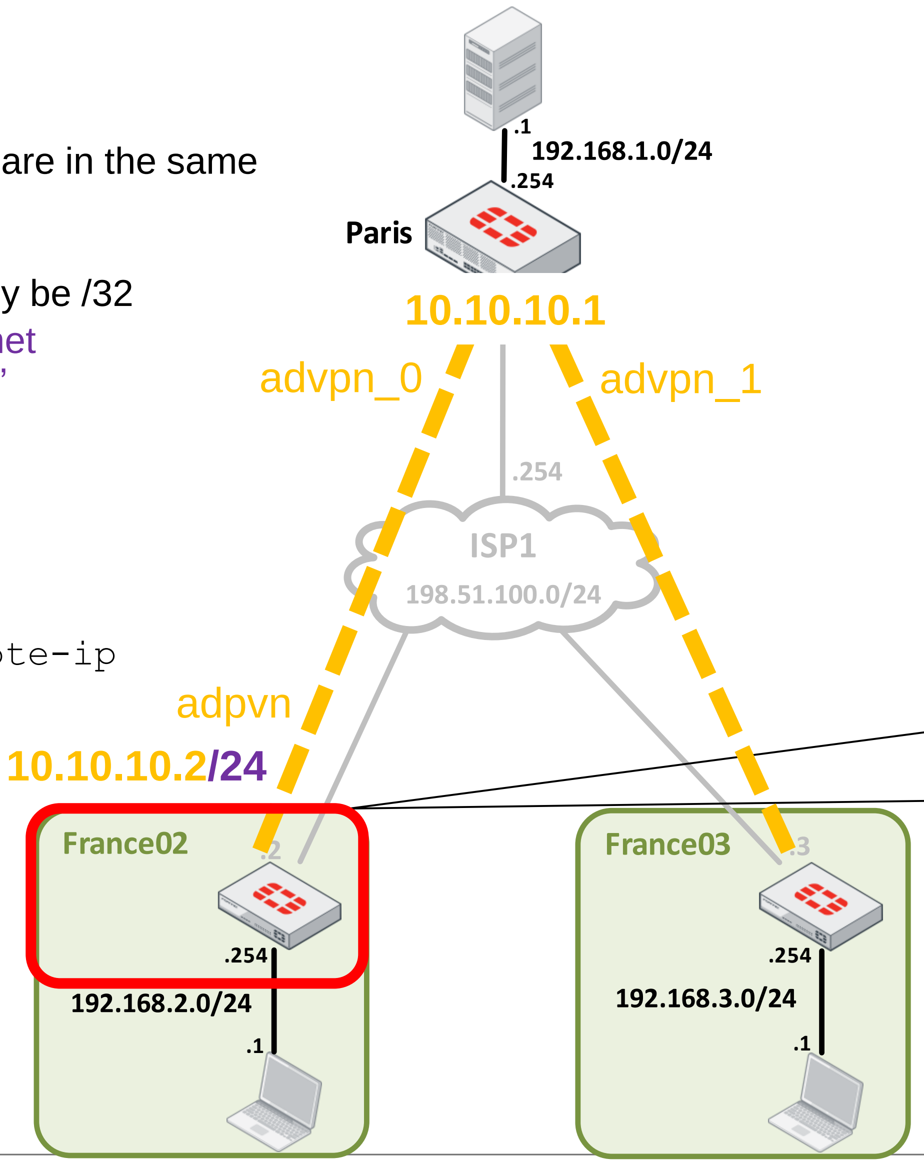
/24

The overlay IPs of all ADVPN participants are in the same subnet

⚠ The mask for the local `ip` can only be /32
So, the mask for the overlay subnet must be specified in ‘`remote-ip`’

```
set ip 10.10.10.2/32
Set remote-ip 10.10.10.1/24
```

The overlay IP of the Hub is used as `remote-ip`



```
config system interface
    edit "advpn"
        set ip 10.10.10.2/32
        set remote-ip 10.10.10.1/24
    next
end
```

ADVPN Spoke configuration

“net-device disable” for shortcuts

⚠ This configuration is **not supported for SD-WAN**

net-device disable

Default setting for static phase1 introduced in FortiOS 6.2.1

A dynamic interface is no longer created for each shortcut
“`advpn`” is used as a shared interface by all shortcuts

This setting is not supported for SD-WAN members
This tunnel is not supported as an SD-WAN member

tunnel-search nexthop

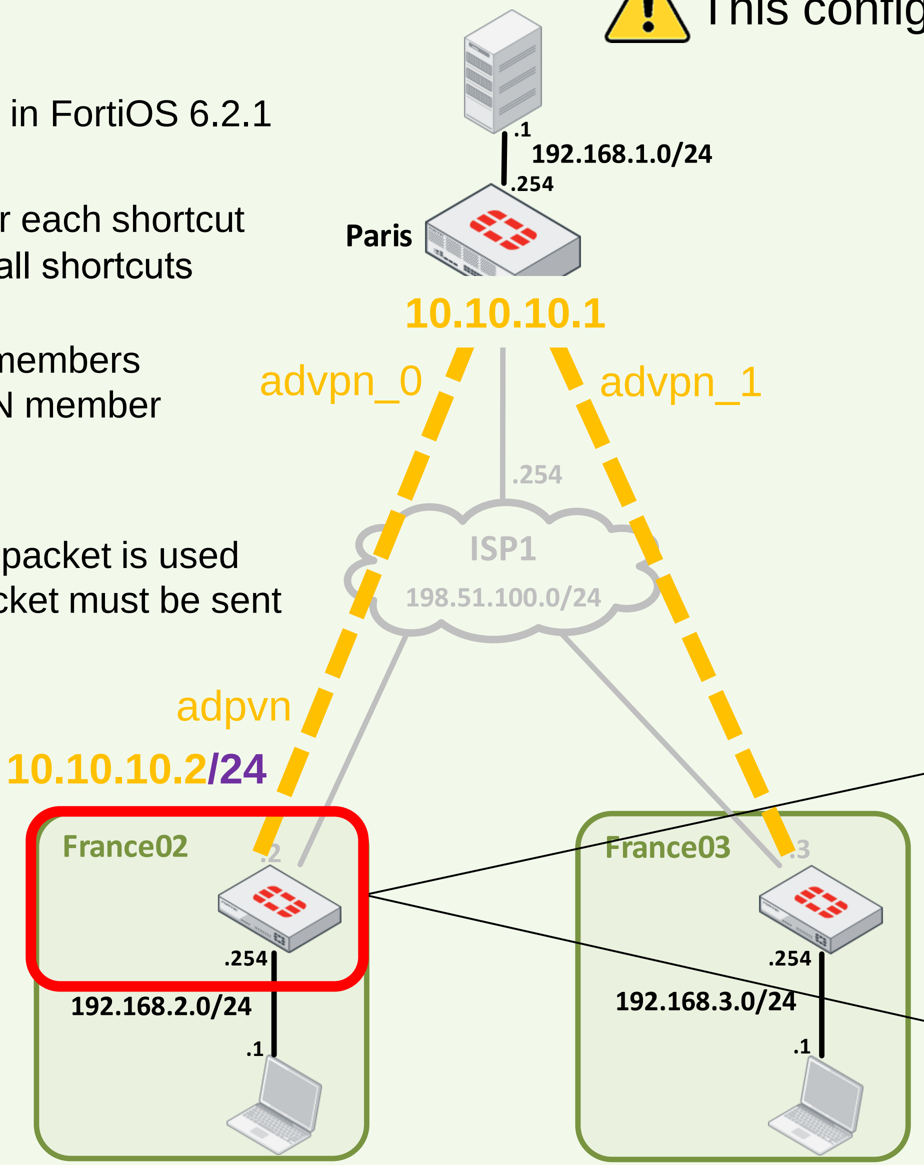
The next-hop IP of the route matched by a packet is used to decide into which tunnel shortcut the packet must be sent

auto-discovery-receiver enable

To indicate that this IPsec tunnel wishes to participate in an Auto-Discovery VPN (i.e., receive SHORTCUT-OFFER)

add-route disable

ensures that IKE does not automatically add a route back over the spoke



```
config vpn ipsec phase1-interface
    edit "advpn"
        set type static
        set interface "wan"
        set net-device disable
        set tunnel-search nexthop
        set proposal aes128-sha1
        set auto-discovery-receiver enable
        set add-route disable
        set remote-gw 198.51.100.1
        set psksecret xxxxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "advpn"
        set phase1name "advpn"
        set proposal aes128-sha1
    next
end

config system interface
    edit "advpn"
       set ip 10.10.10.2/32
       set remote-ip 10.10.10.1/24
    next
end
```

ADVPN Spoke configuration

“net-device enable” for shortcuts

net-device enable

A dedicated interface is created for each shortcut

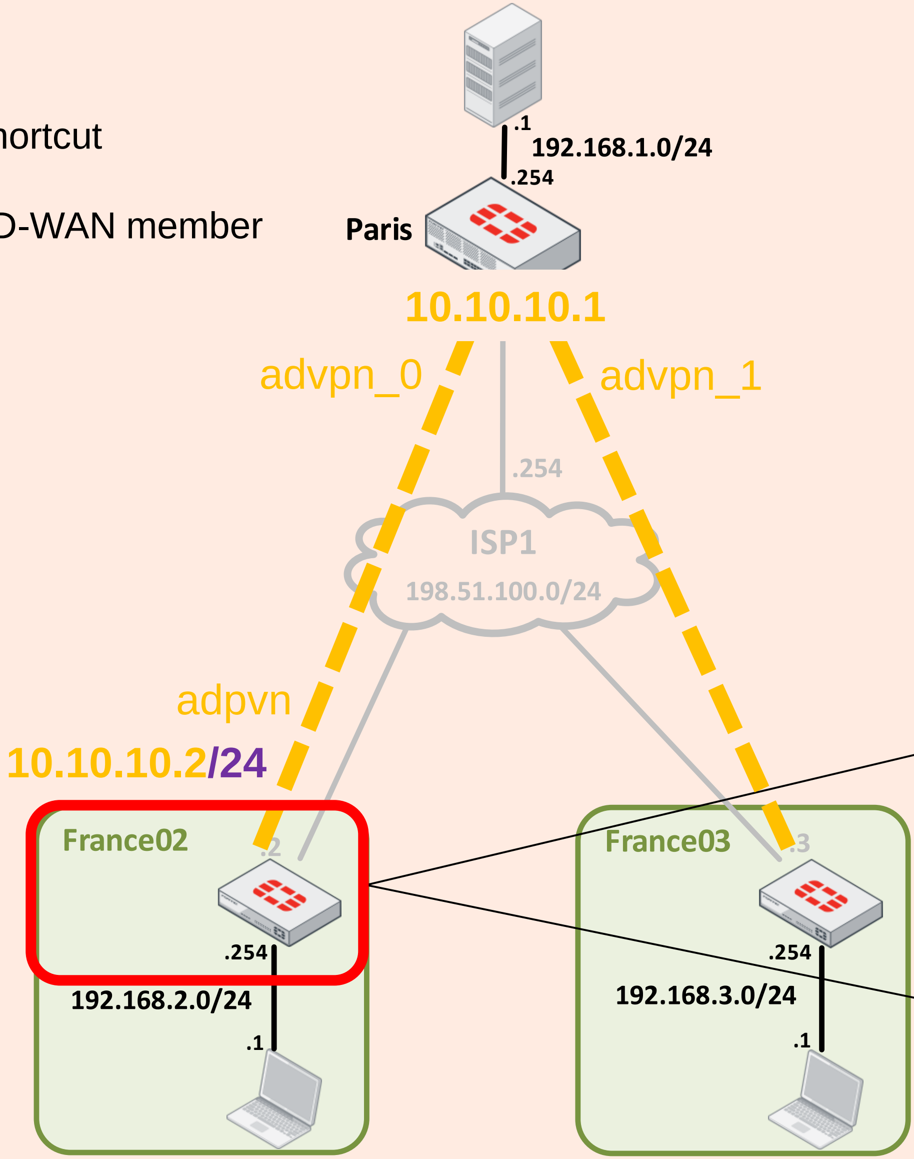
This setting is needed if this tunnel is an SD-WAN member

auto-discovery-receiver enable

To indicate that this IPsec tunnel wishes to participate in an Auto-Discovery VPN (i.e., receive SHORTCUT-OFFER)

add-route disable

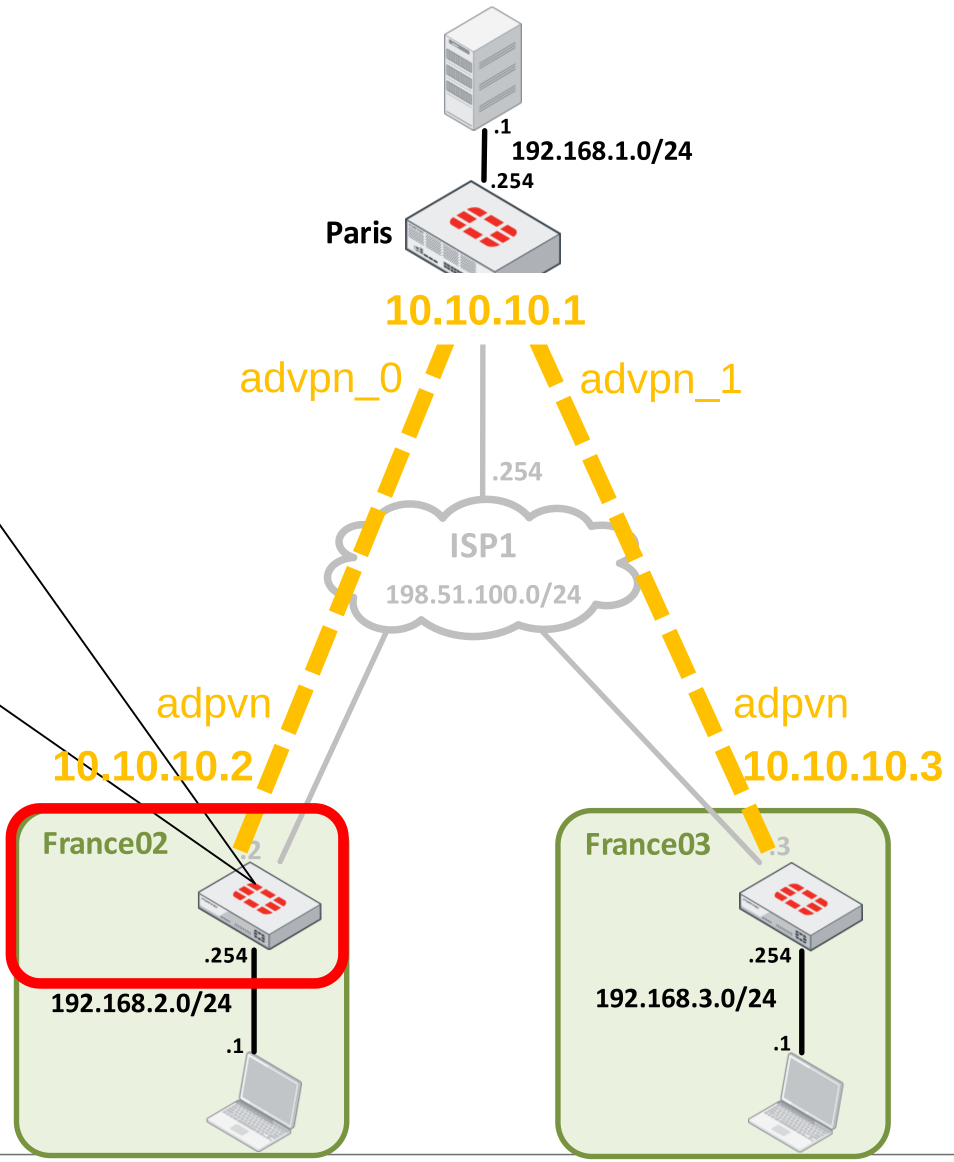
ensures that IKE does not automatically add a route back over the spoke



```
config vpn ipsec phase1-interface
    edit "advpn"
        set type static
        set interface "wan"
        set net-device enable
        set proposal aes128-sha1
        set auto-discovery-receiver enable
        set add-route disable
        set remote-gw 198.51.100.1
        set psksecret xxxxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "advpn"
        set phase1name "advpn"
        set proposal aes128-sha1
    next
end

config system interface
    edit "advpn"
       set ip 10.10.10.2/32
       set remote-ip 10.10.10.1/24
    next
end
```

ADVPN Spoke configuration

```
config firewall policy
    edit 1
        set name "To Hub/Spokes"
        set srcintf "internal"
        set dstintf "advpn"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "From Hub/Spokes"
        set srcintf "advpn"
        set dstintf "internal"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```



No specific policies are needed for traffic to/from other Spokes.

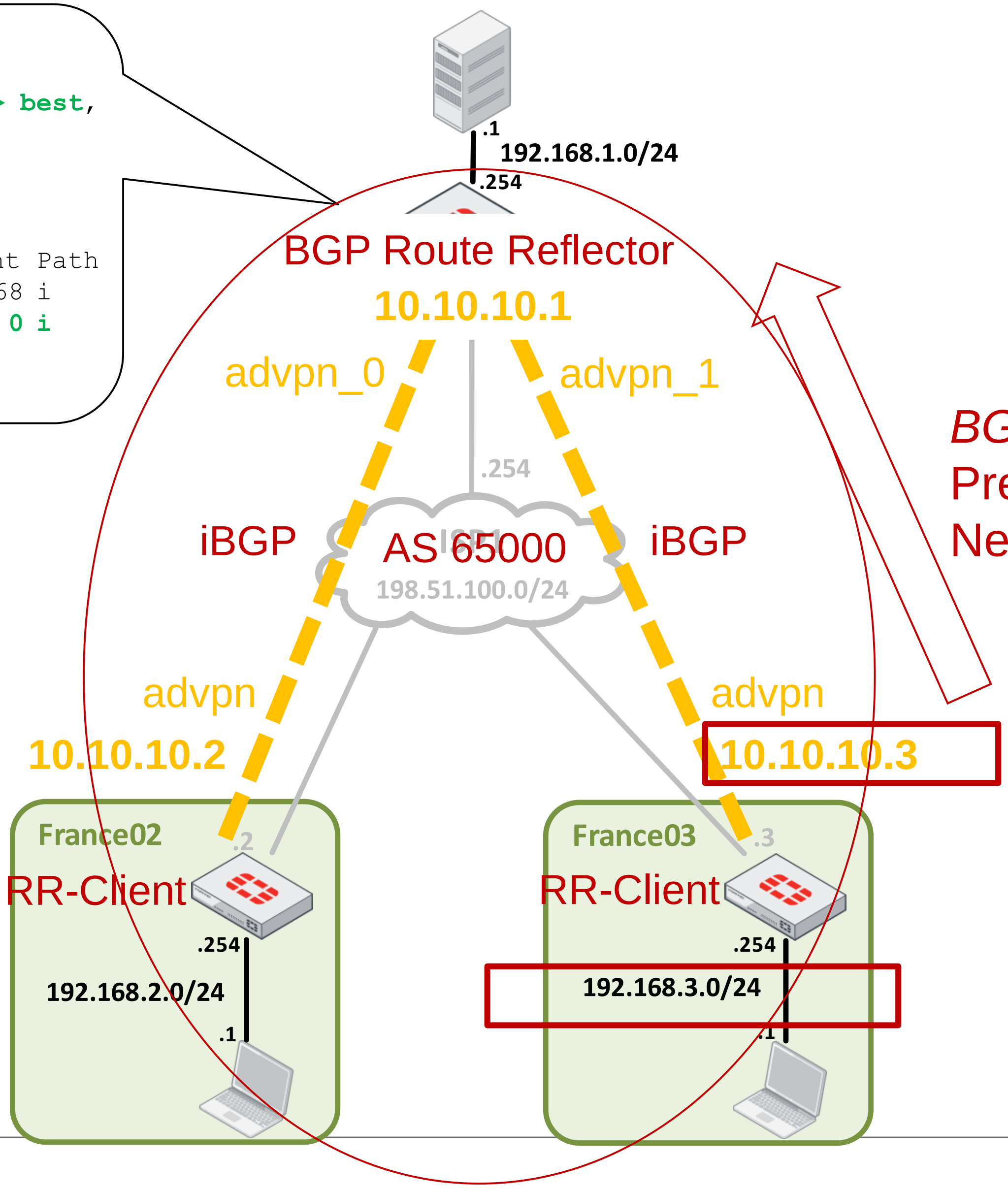
Traffic to/from other Spokes is checked against the policies to/from the Hub

ADVPN with BGP

iBGP with Route-Reflector

iBGP – Route Reflector (RR) and RR-Clients

```
Paris # get router info bgp network
BGP table version is 4, local router ID is 10.10.10.1
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      0.0.0.0                       100  32768 i
*>i192.168.3.0      10.10.10.3               0    100      0 i

Total number of prefixes 2
```

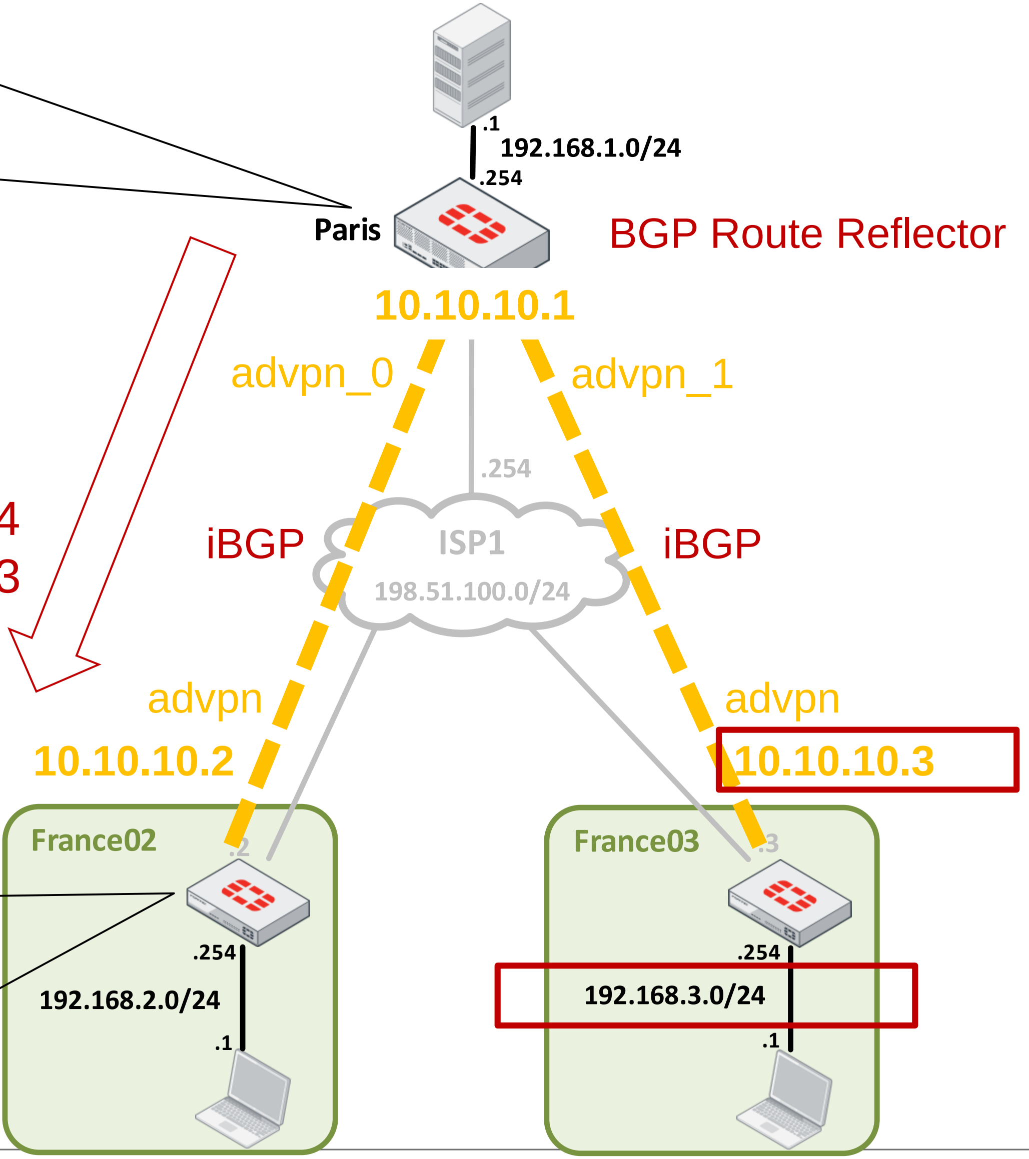


BGP Update:
Prefix= 192.168.3.0/24
Next-Hop = 10.10.10.3

iBGP – Route Reflector (RR) and RR-Clients

```
Paris # get router info bgp network
BGP table version is 4, local router ID is 10.10.10.1
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      0.0.0.0                       100  32768 i
*>i192.168.3.0      10.10.10.3               0    100      0 i

Total number of prefixes 2
```

BGP Update:
Prefix= 192.168.3.0/24
Next-Hop = 10.10.10.3



```
France02 # get router info bgp network
BGP table version is 4, local router ID is 10.10.10.2
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i192.168.1.0      10.10.10.1               0    100      0 i
*> 192.168.2.0      0.0.0.0                       100  32768 i
*>i192.168.3.0      10.10.10.3               0    100      0 i

Total number of prefixes 3
```

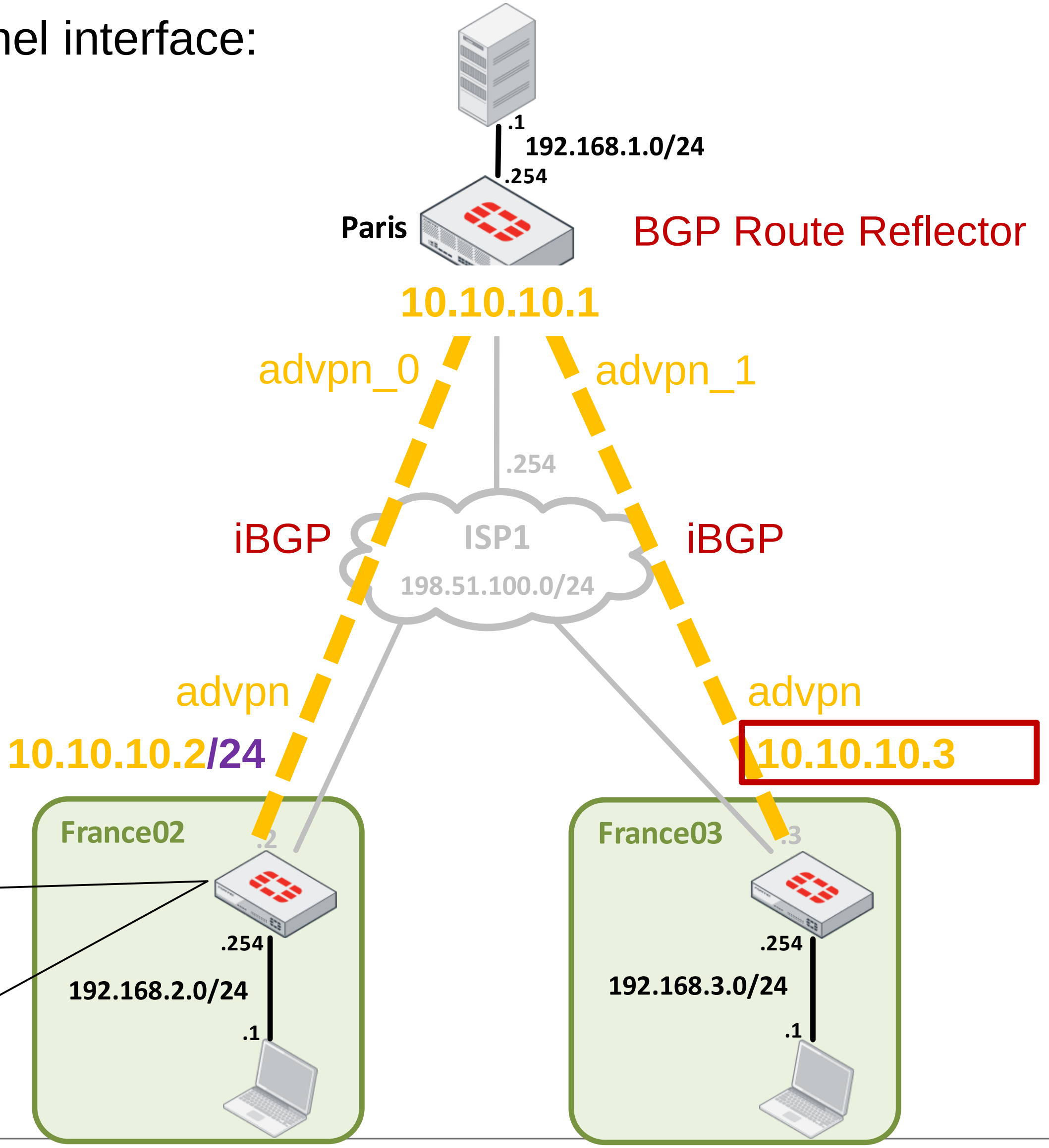
iBGP Next Hop Reachability

- The ADVPN overlay subnet is defined on the tunnel interface:

```
config system interface
    edit "advpn"
        set ip 10.10.10.2 255.255.255.255
        set remote-ip 10.10.10.1 255.255.255.0
    next
end
```

BGP Next-Hop must be accessible through the tunnel

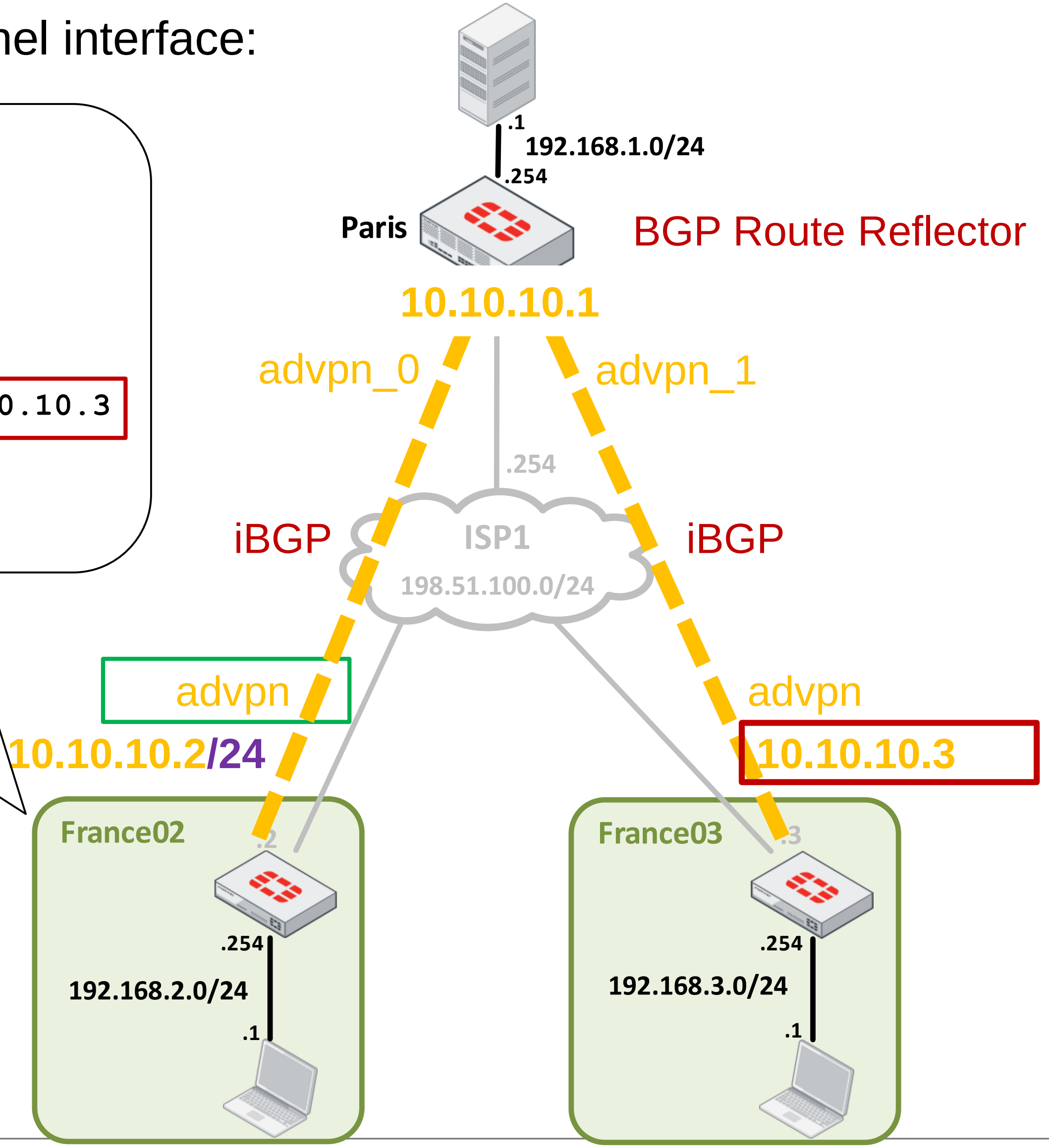
```
France02 # get router info bgp network
BGP table version is 4, local router ID is 10.10.10.2
Status codes: s suppressed, d damped, h history, * valid, > best,
i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i192.168.1.0      10.10.10.1               0    100      0 i
*> 192.168.2.0      0.0.0.0                       100  32768 i
*>i192.168.3.0      10.10.10.3               0    100      0 i

Total number of prefixes 3
```



No shortcut – BGP Next-Hop is reached via the Hub

The ADVPN overlay subnet is defined on the tunnel interface:

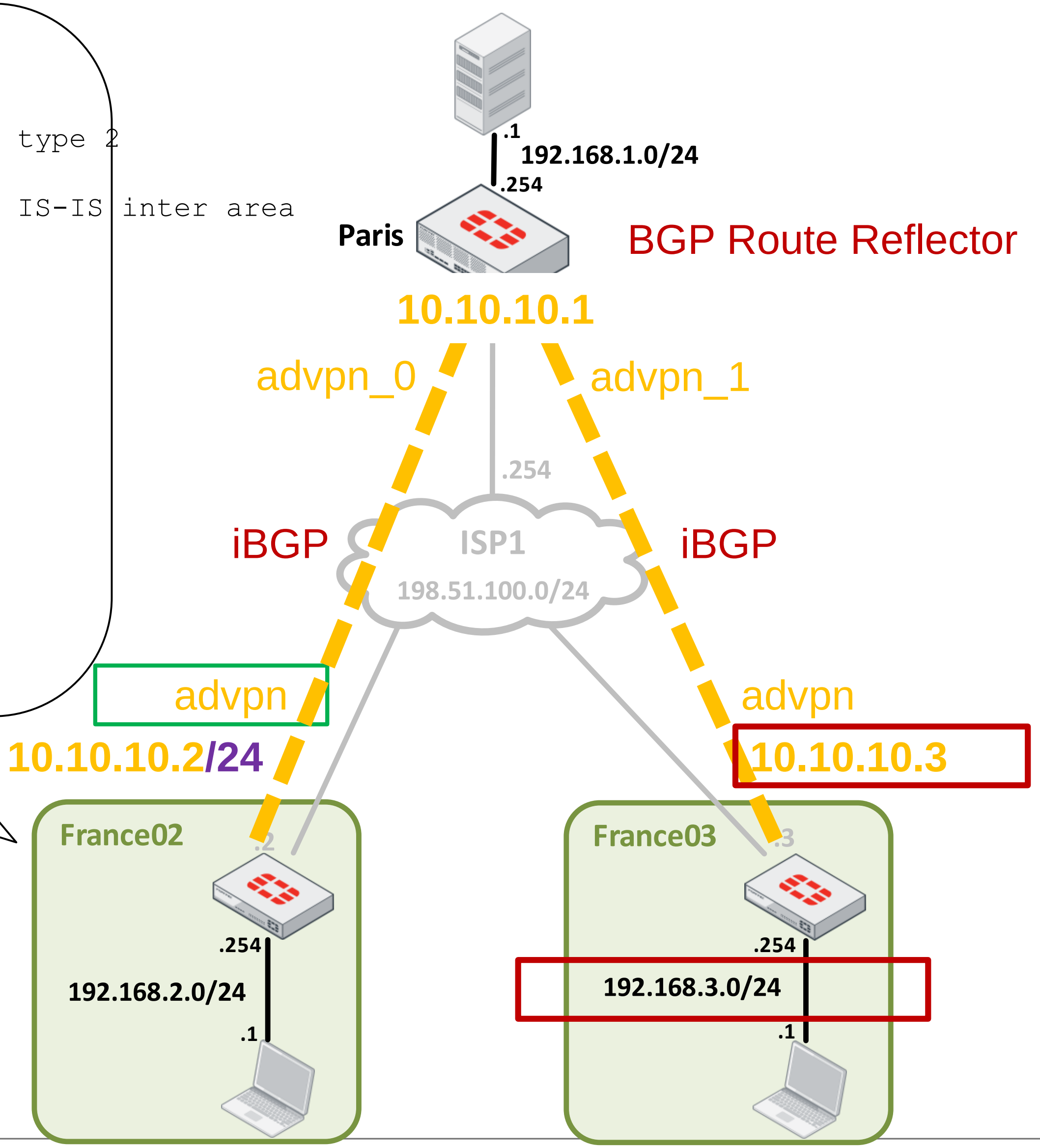
```
France02 # get router info routing-table connected
(…)
C        10.10.10.0/24 is directly connected, advpn
(…)



France02 # get router info routing-table details 10.10.10.3
Routing entry for 10.10.10.0/24
  Known via "connected", distance 0, metric 0, best
  * is directly connected, advpn
```



BGP Next-Hop of France03 Spoke (10.10.10.3) is accessible via advpn connected subnet

No shortcut – RIB lookup

```
France02 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [10/0] via 198.51.100.254, wan

C       10.10.10.0/24 is directly connected, advpn
C       10.10.10.2/32 is directly connected, advpn

B       192.168.1.0/24 [200/0] via 10.10.10.1, advpn, 00:31:43
C       192.168.2.0/24 is directly connected, internal
B       192.168.3.0/24 [200/0] via 10.10.10.3, advpn, 00:31:43

C       198.51.100.0/24 is directly connected, wan
```



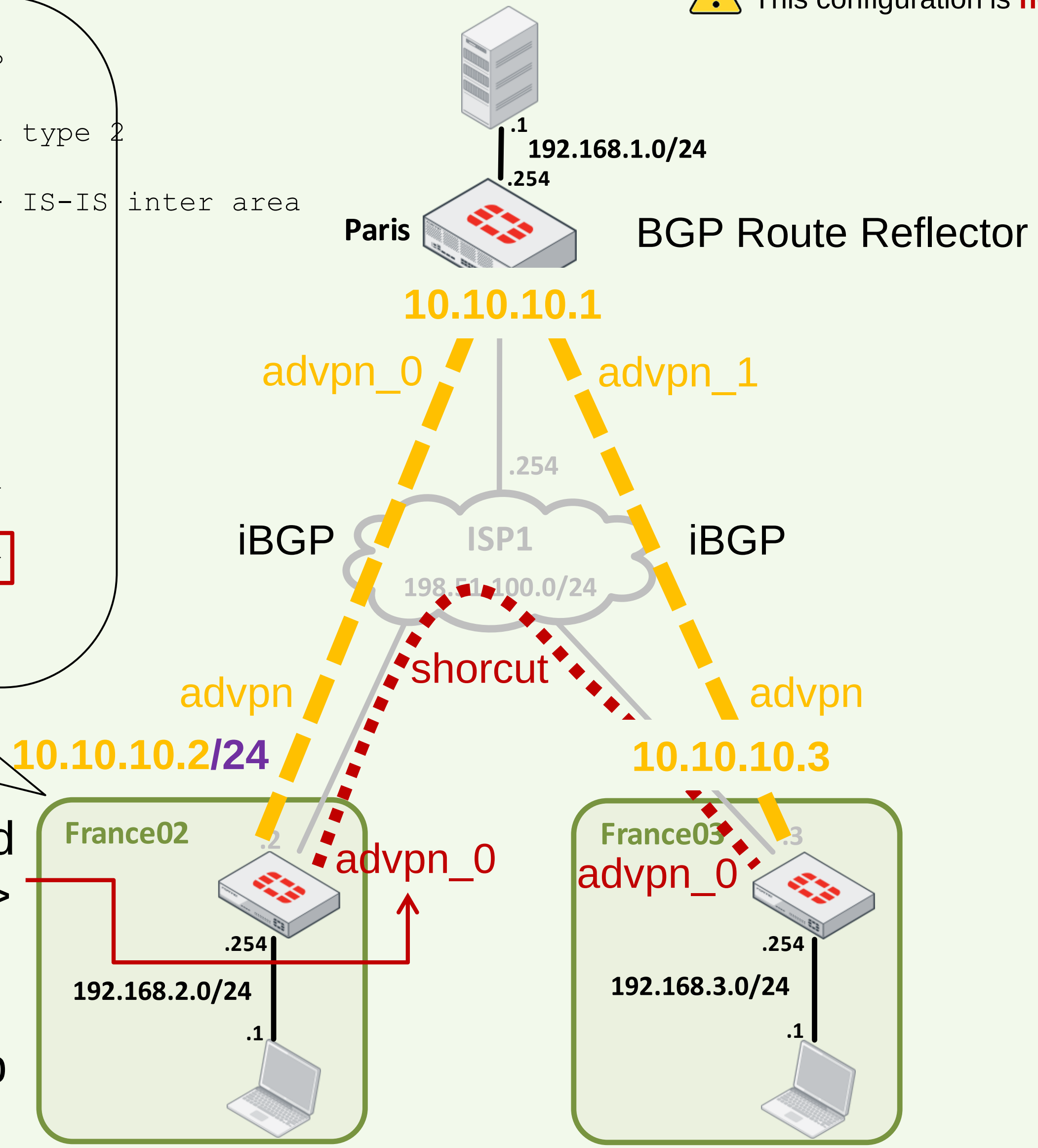
Spoke-to-Spoke traffic flows through the Hub

Shortcut tunnels with a shared interface

“net-device disable” for shortcuts

⚠ This configuration is not supported for SD-WAN

```
France02 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*       0.0.0.0/0 [10/0] via 198.51.100.254, wan

C        10.10.10.0/24 is directly connected, advpn
C        10.10.10.2/32 is directly connected, advpn

B        192.168.1.0/24 [200/0] via 10.10.10.1, advpn, 00:36:51
C        192.168.2.0/24 is directly connected, internal
B        192.168.3.0/24 [200/0] via 10.10.10.3, advpn, 00:36:51

C        198.51.100.0/24 is directly connected, wan
```



A shortcut tunnel is created
name = <phase1name>_<index>

Route to France03 remains unchanged
It stays associated to the interface towards the Hub which is used as well as a shared interface for all shortcuts (‘set net-device disable’)

Shortcut tunnels with a shared interface

"net-device disable" for shortcuts

⚠ This configuration is **not supported for SD-WAN**

```
France02 # get router info routing-table bgp | grep 192.168.3
B       192.168.3.0/24 [200/0] via 10.10.10.3, advpn, 00:36:51

France02 # diag vpn tunnel list name advpn
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=advpn ver=1 serial=1 198.51.100.2:0->198.51.100.1:0 dst_mtu=1500
bound_if=4 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/544 options[0220]=search-nexthop frag-rfc
run_state=0 accept_traffic=1

proxyid_num=1 child_num=1 refcnt=18 ilast=1 olast=1 ad=r/2
stat: rxp=1177 txp=1027 rxb=151752 txb=64843
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=1
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=advpn proto=0 sa=1 ref=2 serial=1 adr
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA:  ref=3 options=32202 type=00 soft=0 mtu=1438 expire=38619/0B replaywin=2048
       seqno=3c0 esn=0 replaywin_lastseq=00000456 itn=0 qat=0
  life: type=01 bytes=0/0 timeout=42903/43200
  dec: spi=93730178 esp=aes key=16 af818f5b74f7acd6bf41d9303757ac41
       ah=sha1 key=20 5dd0e6dbb4dd7b5d0a56ebc02465b575214b03f5
  enc: spi=3292ee38 esp=aes key=16 d1768bc8b7ac5d08a63595c914f377eb
       ah=sha1 key=20 5458ec899ebe5fc680c2ce4290b7a3601272e2e6
  dec:pkts/bytes=1109/67470, enc:pkts/bytes=959/122920
run_tally=2
ipv4 route tree:
10.10.10.3 0
198.51.100.3 0
```

Tunnel 'advpn' contains two types of information:

1- the IPsec Security Association for the tunnel with the Hub

2- the 'route tree' for the shortcut tunnels

Shortcut tunnels with a shared interface

“net-device disable” for shortcuts

⚠ This configuration is **not supported for SD-WAN**

```
France02 # get router info routing-table bgp | grep 192.168.3
B       192.168.3.0/24 [200/0] via 10.10.10.3, advpn, 00:36:51

France02 # diag vpn tunnel list name advpn
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=advpn ver=1 serial=1 198.51.100.2:0->198.51.100.1:0 dst_mtu=1500
bound_if=4 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/544 options[0220]=search-nexthop frag-rfc
run_state=0 accept_traffic=1

proxyid_num=1 child_num=1 refcnt=18 ilast=1 olast=1 ad=r/2
(...)
(... truncated for brevity...)
(...)
  dec:pkts/bytes=1109/67470, enc:pkts/bytes=959/122920
run_tally=2

ipv4 route tree:
10.10.10.3 0
198.51.100.3 0
```

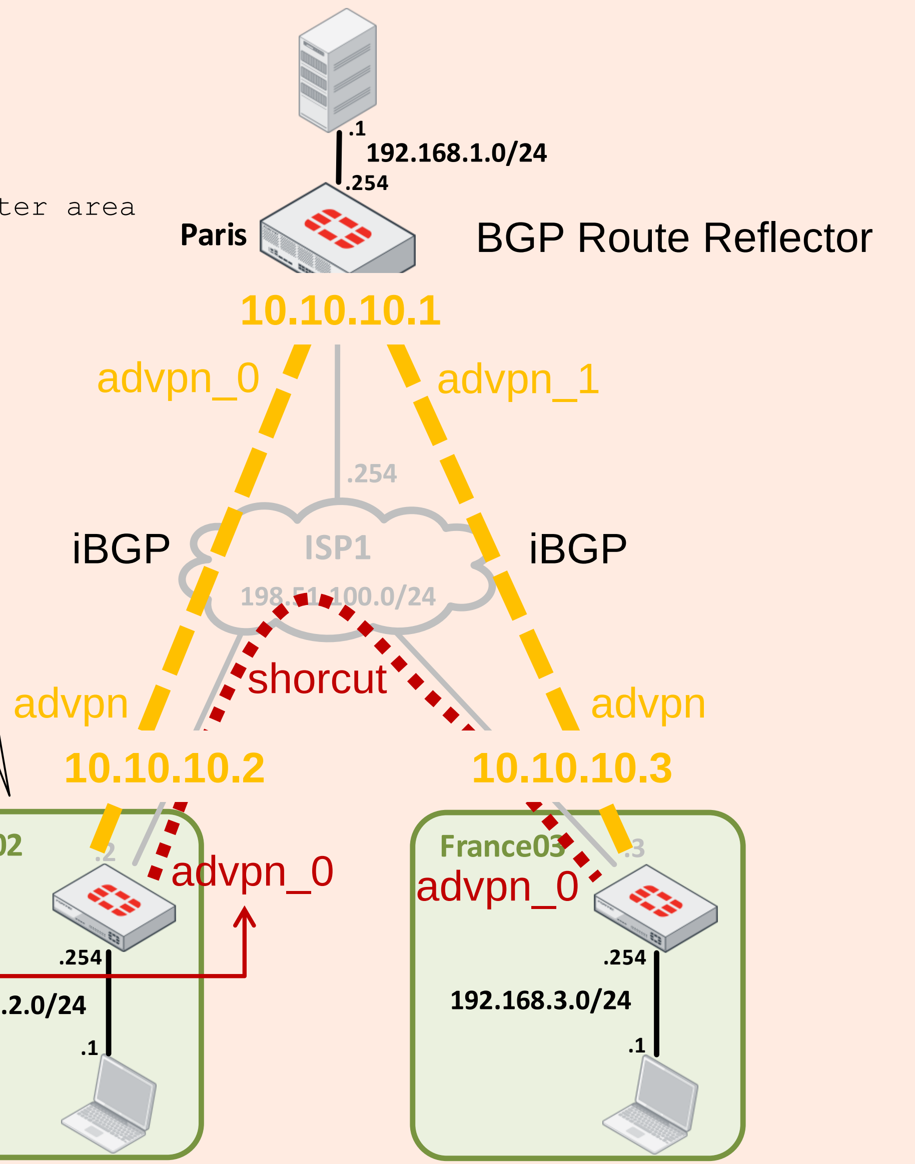
Traffic destined to next-hop 10.10.10.3 is forwarded to shortcut tunnel with index 0 (i.e., adpvn_0)

Spoke-to-Spoke traffic flows through the shortcut

Shortcut tunnels with a dedicated interface

"net-device enable" for shortcuts

```
France02 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [10/0] via 198.51.100.254, wan

C       10.10.10.0/24 is directly connected, advpn
C       10.10.10.2/32 is directly connected, advpn
                      is directly connected, advpn_0
C       10.10.10.3/32 is directly connected, advpn_0


B       192.168.1.0/24 [200/0] via 10.10.10.1, advpn, 02:38:15
C       192.168.2.0/24 is directly connected, internal
B       192.168.3.0/24 [200/0] via 10.10.10.3, advpn_0, 00:00:28

C       198.51.100.0/24 is directly connected, wan
```



A shortcut tunnel is created and

A dynamic interface is created as well ('set net-device enable')

Shortcut tunnel & interface names = <phase1name>_<index>

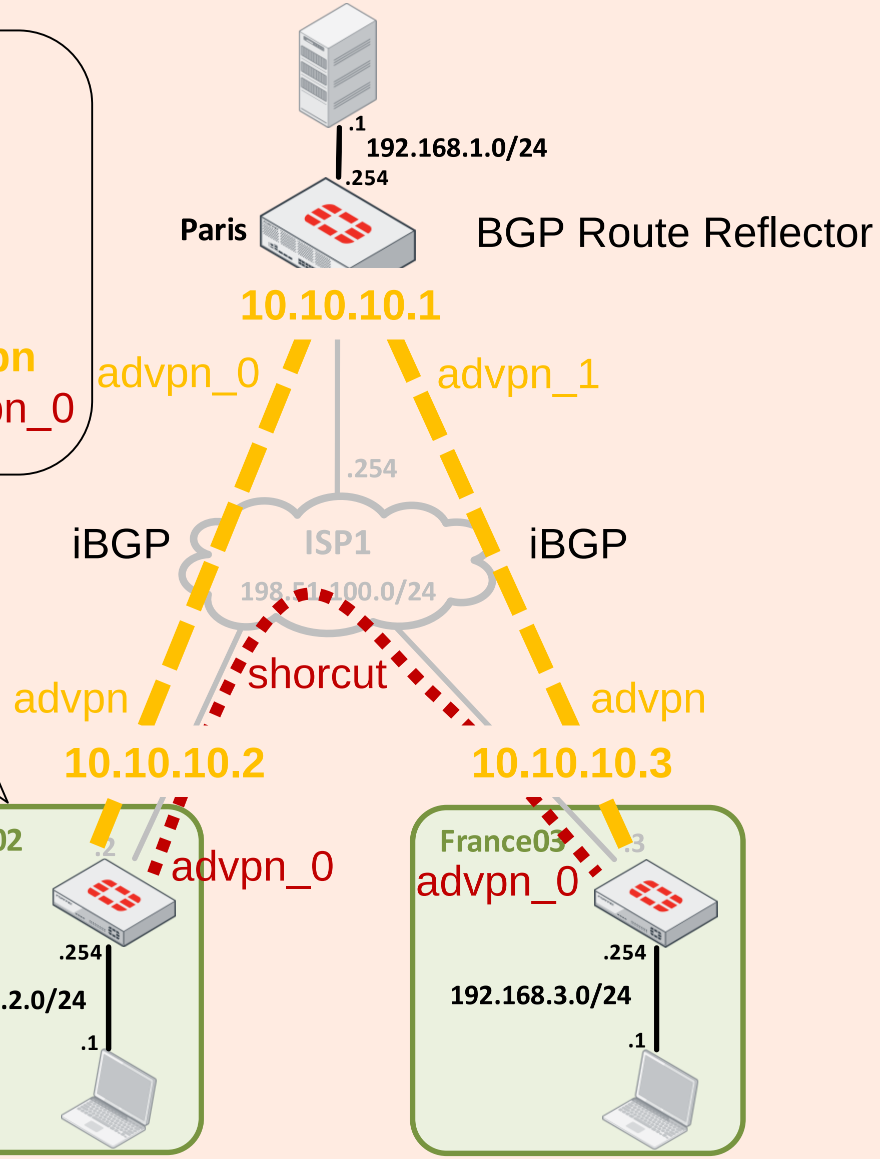
Shortcut tunnels with a dedicated interface

"net-device enable" for shortcuts

```
France02 # get router info routing-table all
(...)
C       10.10.10.2/32 is directly connected, advpn
                      is directly connected, advpn_0
(...)

France02 # diag ip address list | grep advpn
IP=10.10.10.2->10.10.10.1/255.255.255.255 index=15 devname=advpn
IP=10.10.10.2->10.10.10.3/255.255.255.255 index=19 devname=advpn_0
```

The same overlay IP (10.10.10.2) is assigned to:

- the interface towards the Hub (adpvn)
- the interface towards France03 Spoke (adpvn_0)

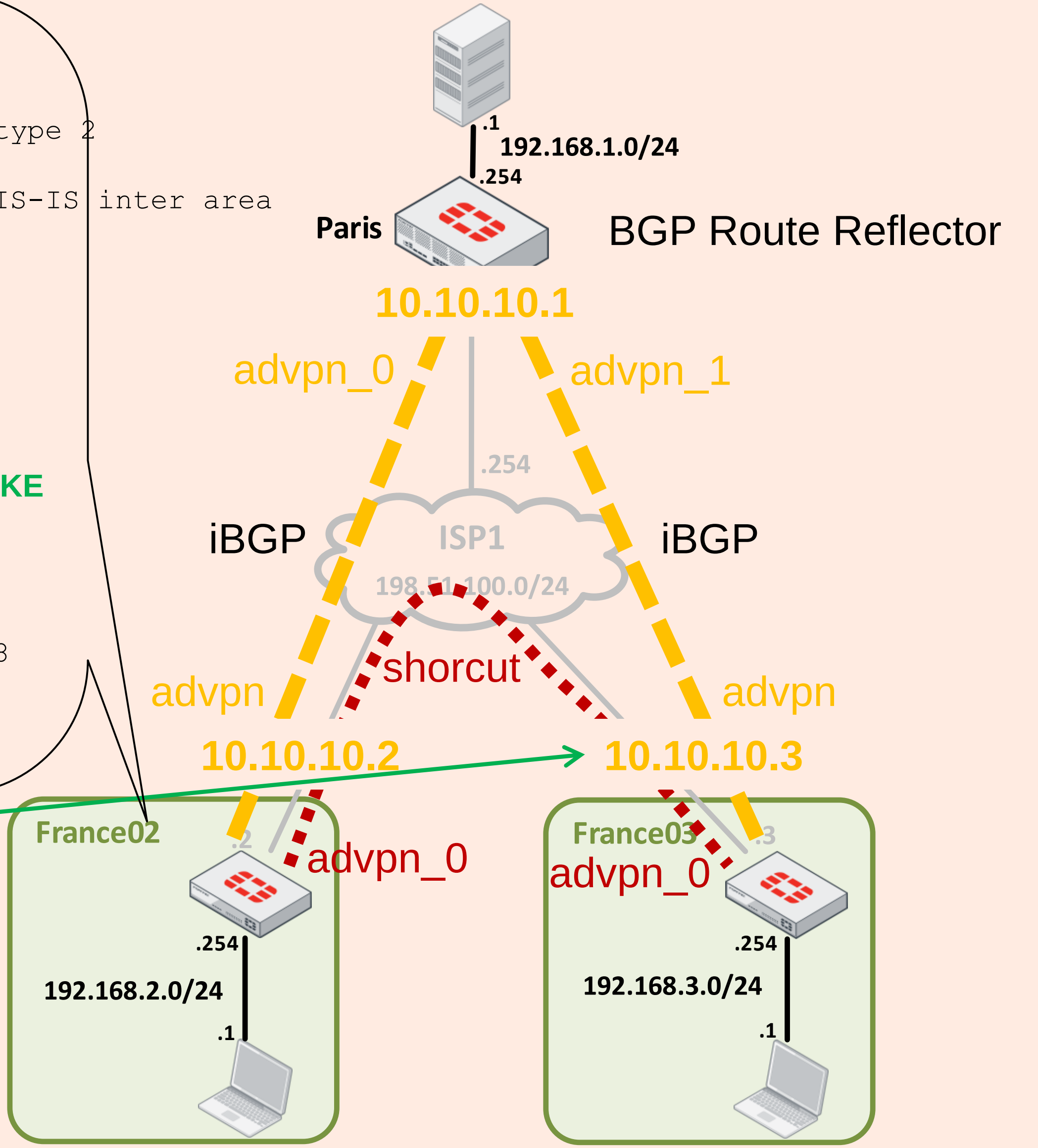


Shortcut tunnels with a dedicated interface

“net-device enable” for shortcuts

```
France02 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [10/0] via 198.51.100.254, wan

C       10.10.10.0/24 is directly connected, advpn
C       10.10.10.2/32 is directly connected, advpn
                      is directly connected, advpn_0
C       10.10.10.3/32 is directly connected, advpn_0


B       192.168.1.0/24 [200/0] via 10.10.10.1, advpn, 02:38:15
C       192.168.2.0/24 is directly connected, internal
B       192.168.3.0/24 [200/0] via 10.10.10.3, advpn_0, 00:00:28

C       198.51.100.0/24 is directly connected, wan
```

Added by IKE



The BGP Next-Hop of France03 (10.10.10.3) is directly connected on the shortcut interface

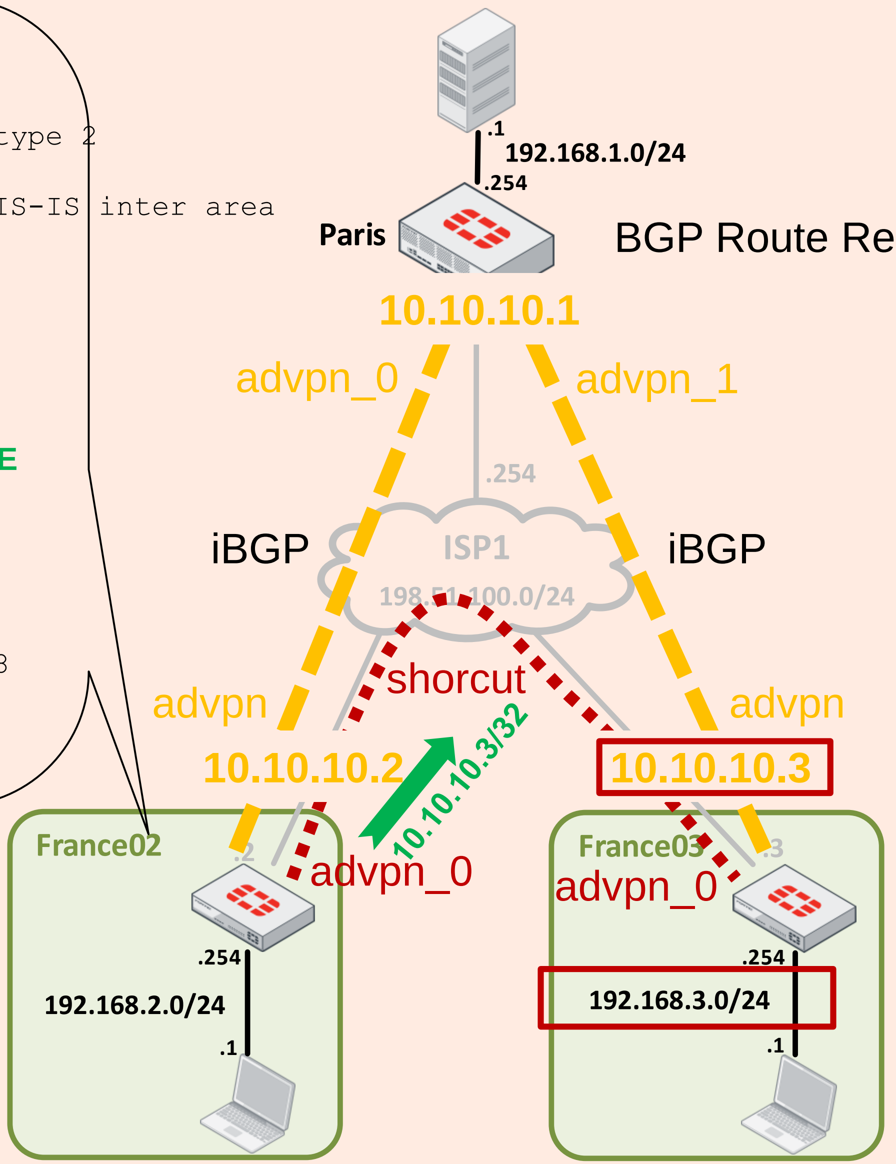
Shortcut tunnels with a dedicated interface

"net-device enable" for shortcuts

```
France02 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*      0.0.0.0/0 [10/0] via 198.51.100.254, wan

C       10.10.10.0/24 is directly connected, advpn
C       10.10.10.2/32 is directly connected, advpn
                      is directly connected, advpn_0
C       10.10.10.3/32 is directly connected, advpn_0


B       192.168.1.0/24 [200/0] via 10.10.10.1, advpn, 02:38:15
C       192.168.2.0/24 is directly connected, internal
B       192.168.3.0/24 [200/0] via 10.10.10.3, advpn_0, 00:00:28

C       198.51.100.0/24 is directly connected, wan
```

Added by IKE

Spoke-to-Spoke traffic flows through the shortcut

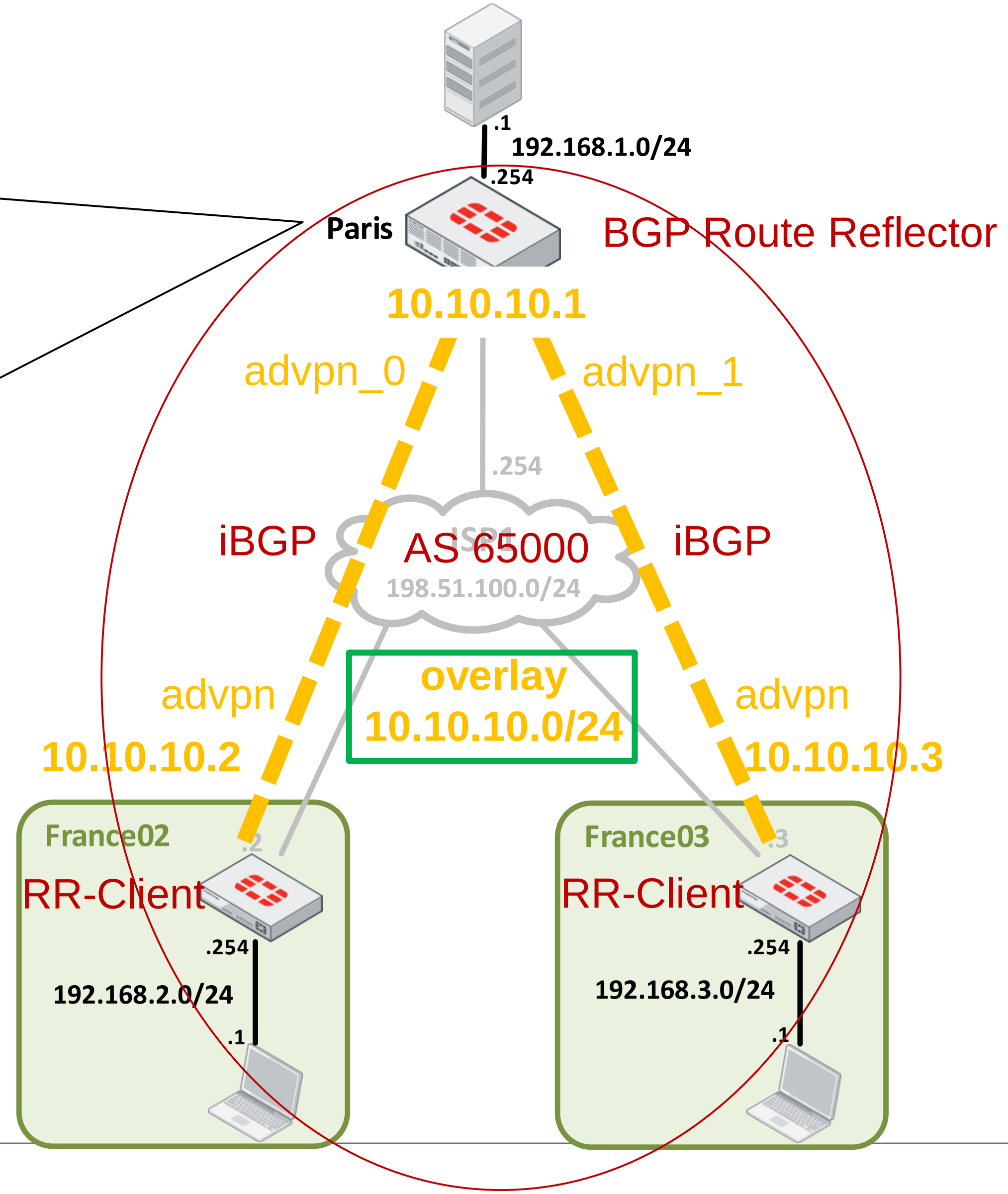


ADVPN with BGP

configuration

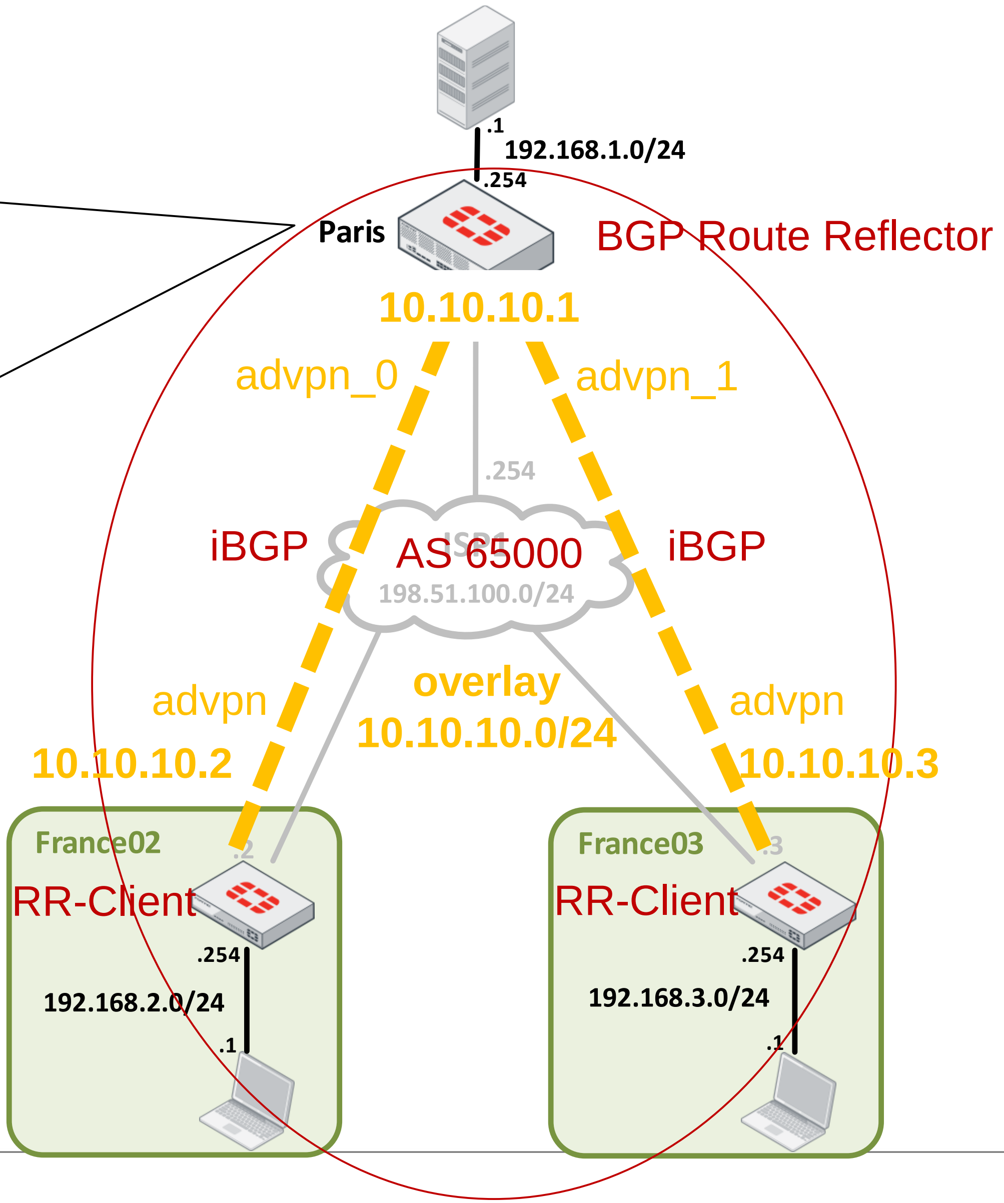
Hub configuration = iBGP Route Reflector (RR)

```
config router bgp
    set as 65000
    set router-id 10.10.10.1
    config neighbor-group
        edit "advn_peers"
            set remote-as 65000
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.10.10.0 255.255.255.0
            set neighbor-group "advn_peers"
        next
    end
    config network
        edit 1
            set prefix 192.168.1.0 255.255.255.0
        next
    end
end
```



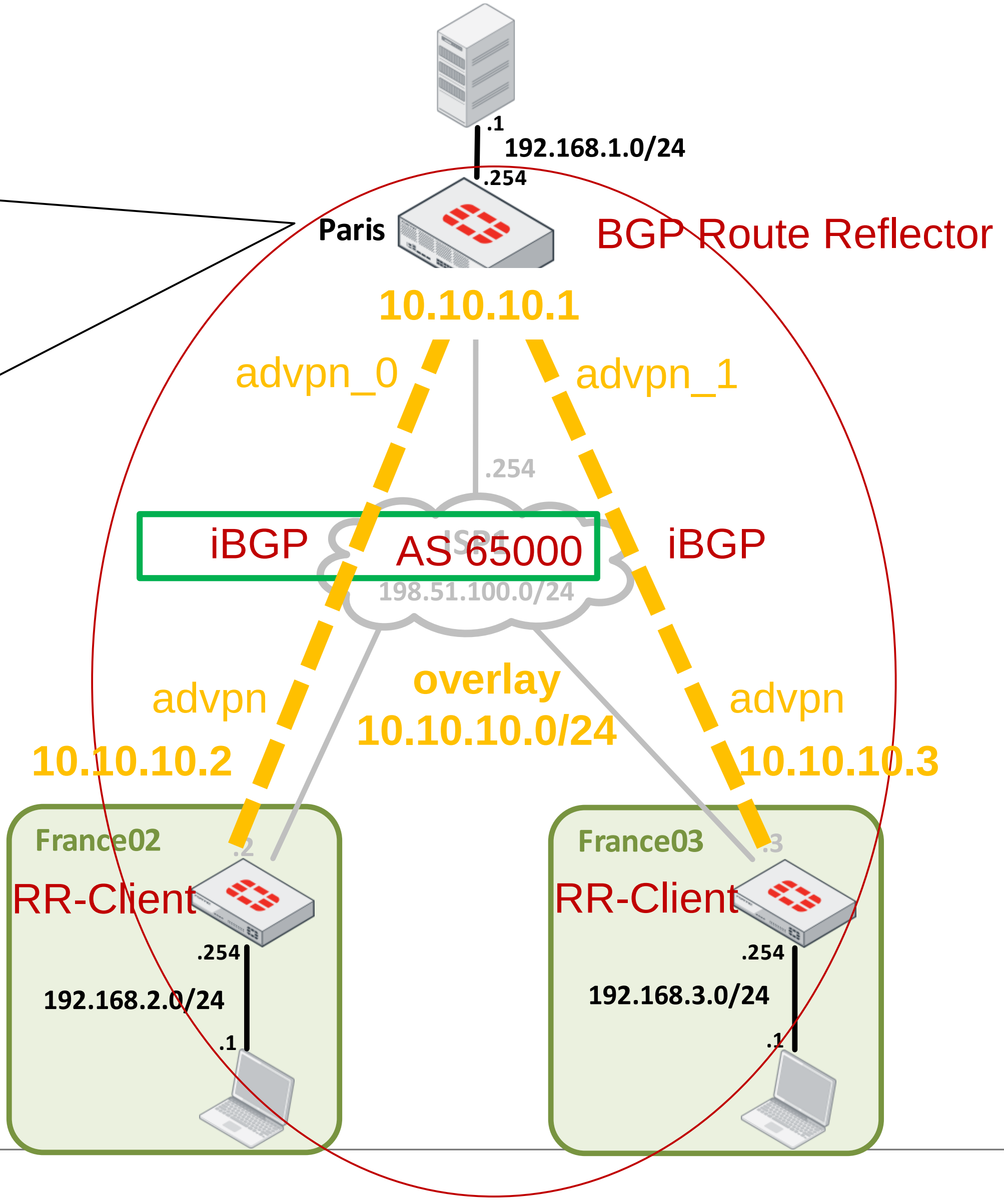
Hub configuration = iBGP Route Reflector (RR)

```
config router bgp
    set as 65000
    set router-id 10.10.10.1
    config neighbor-group
        edit "advn_peers"
            set remote-as 65000
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.10.10.0 255.255.255.0
            set neighbor-group "advn_peers"
        next
    end
    config network
        edit 1
            set prefix 192.168.1.0 255.255.255.0
        next
    end
end
```



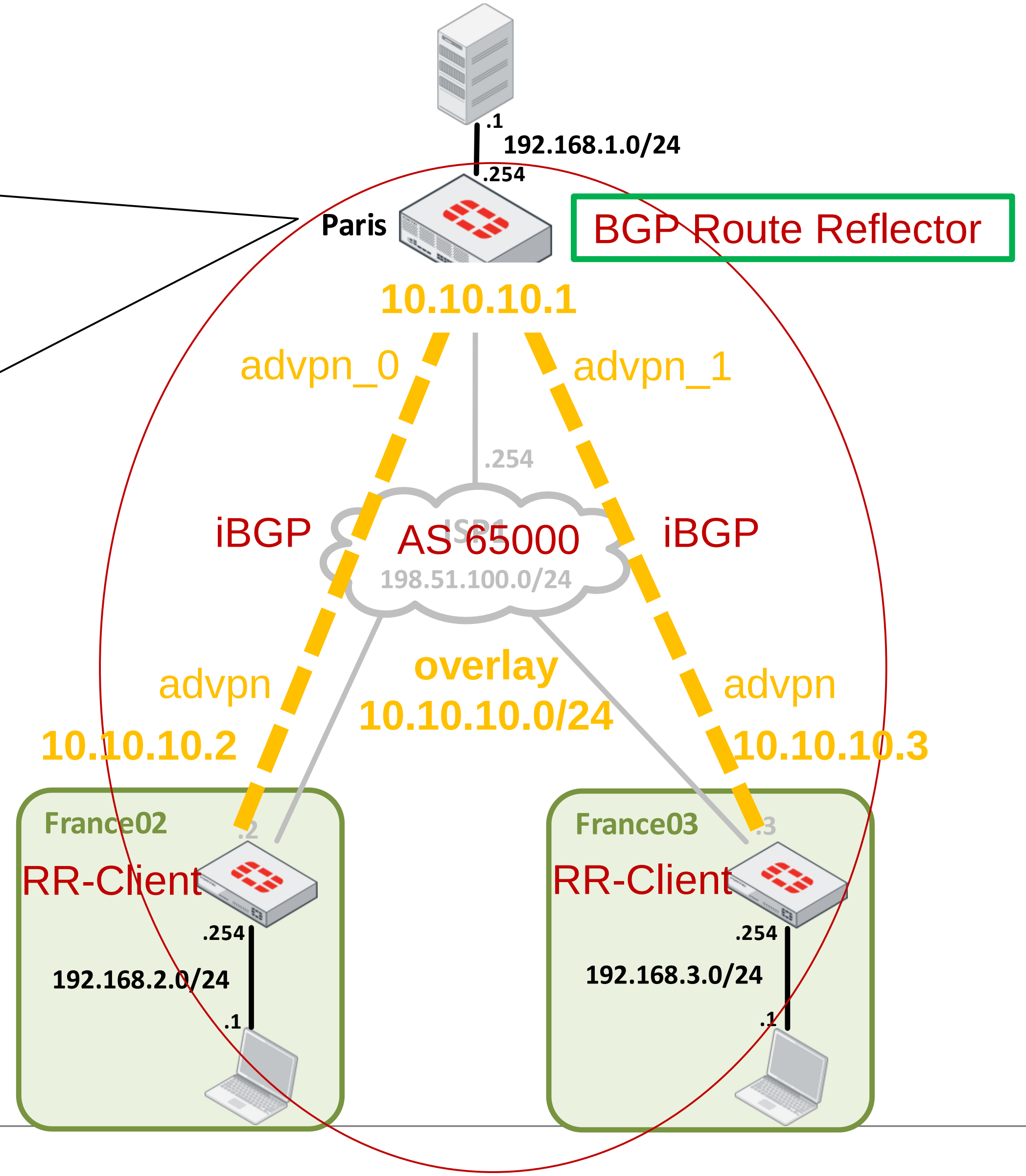
Hub configuration = iBGP Route Reflector (RR)

```
config router bgp
    set as 65000
    set router-id 10.10.10.1
    config neighbor-group
        edit "advn peers"
            set remote-as 65000
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.10.10.0 255.255.255.0
            set neighbor-group "advn_peers"
        next
    end
    config network
        edit 1
            set prefix 192.168.1.0 255.255.255.0
        next
    end
end
```



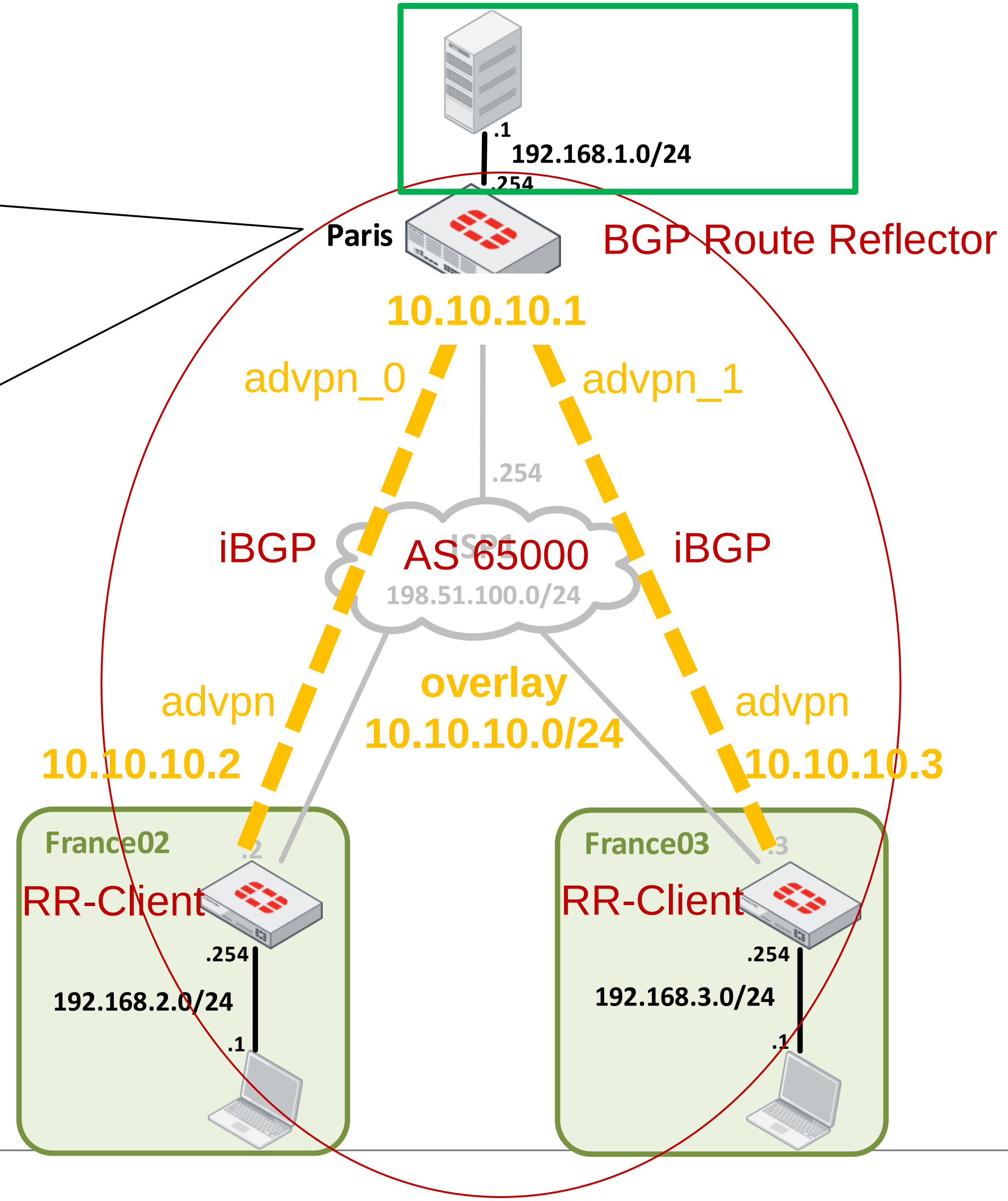
Hub configuration = iBGP Route Reflector (RR)

```
config router bgp
    set as 65000
    set router-id 10.10.10.1
    config neighbor-group
        edit "advn_peers"
            set remote-as 65000
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.10.10.0 255.255.255.0
            set neighbor-group "advn_peers"
        next
    end
    config network
        edit 1
            set prefix 192.168.1.0 255.255.255.0
        next
    end
end
```



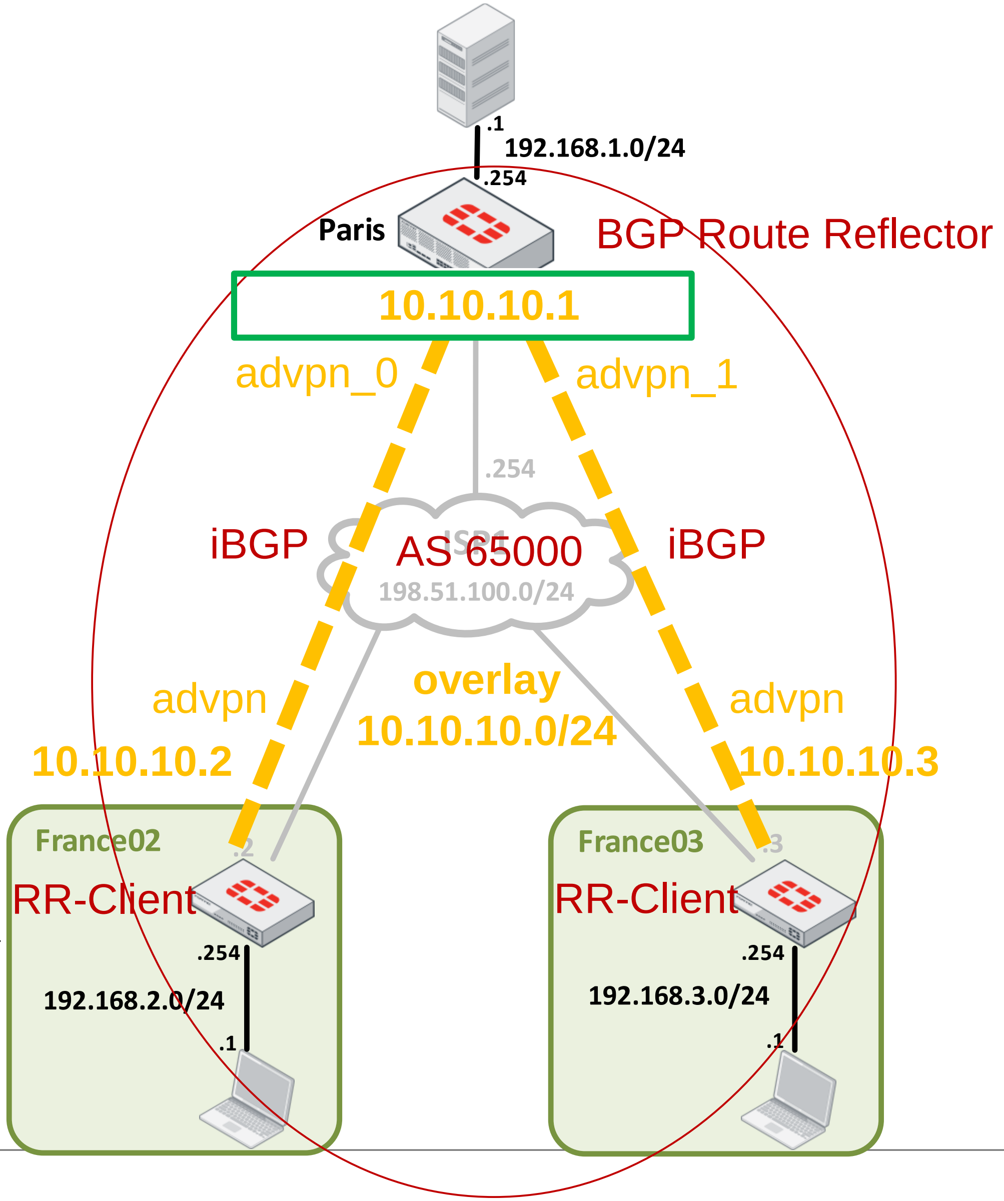
Hub configuration = iBGP Route Reflector (RR)

```
config router bgp
    set as 65000
    set router-id 10.10.10.1
    config neighbor-group
        edit "advn_peers"
            set remote-as 65000
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.10.10.0 255.255.255.0
            set neighbor-group "advn_peers"
        next
    end
    config network
        edit 1
            set prefix 192.168.1.0 255.255.255.0
        next
    end
end
```



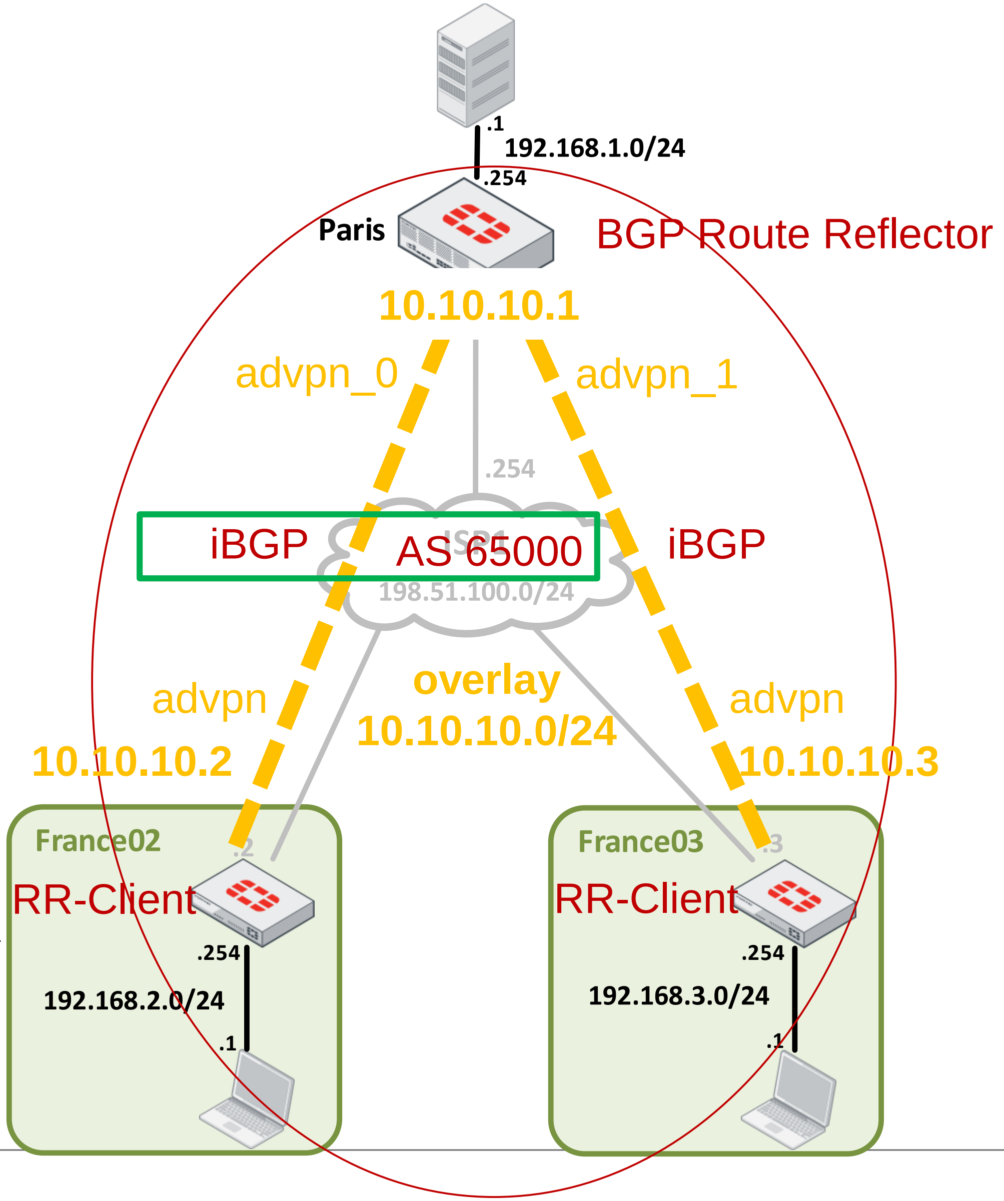
Spoke configuration = iBGP RR-Client

```
config router bgp
    set as 65000
    set router-id 10.10.10.2
    config neighbor
        edit "10.10.10.1"
            set remote-as 65000
        next
    end
    config network
        edit 1
            set prefix 192.168.2.0 255.255.255.0
        next
    end
end
```



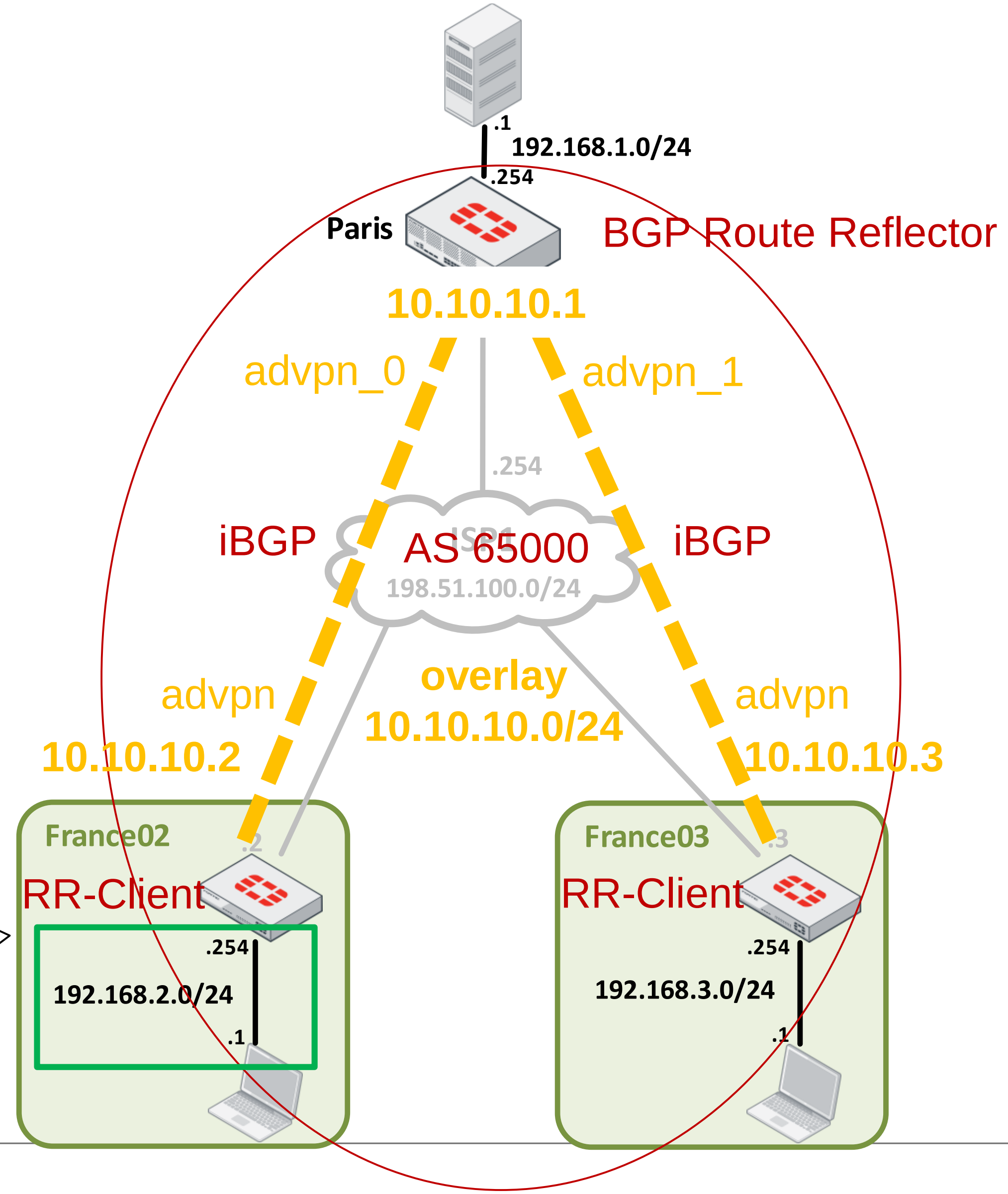
Spoke configuration = iBGP RR-Client

```
config router bgp
    set as 65000
    set router-id 10.10.10.2
    config neighbor
        edit "10.10.10.1"
            set remote-as 65000
        next
    end
    config network
        edit 1
            set prefix 192.168.2.0 255.255.255.0
        next
    end
end
```



Spoke configuration = iBGP RR-Client

```
config router bgp
    set as 65000
    set router-id 10.10.10.2
    config neighbor
        edit "10.10.10.1"
            set remote-as 65000
        next
    end
    config network
        edit 1
            set prefix 192.168.2.0 255.255.255.0
        next
    end
end
```



ADVPN with OSPF

configuration

OSPF configuration

- Filter overlay IPs

Overlay IPs (`10.10.10.x/32`) are exchanged via ADVPN **and** via OSPF

The overlay IPs learned from OSPF must be filtered out from the RIB

```
config router prefix-list
    edit "PFL_filter_overlay_IPs"
        set comments "Filter the overlay IPs 10.10.10.*/32 from LSDB to RIB"
        config rule
          edit 1
              set action deny
              set prefix 10.10.10.0 255.255.255.0
              set ge 32
              set le 32
          next
          edit 2
              set prefix 0.0.0.0 0.0.0.0
              unset ge
              set le 32
          next
        end
    next
end
```

```
config router ospf
(...)
     set distribute-list-in "PFL_filter_overlay_IPs"
(...)
```

OSPF configuration

- Prevent traffic from transiting via Spokes

OSPF adjacencies are established over the shortcut tunnels

Each ADVPN participant has a global view of all the links (Hub↔Spoke and Spoke↔Spoke)

If no care is taken, traffic between two Spokes (A and B) may transit via another Spoke (T)

Only the Hub can orchestrate a shortcut negotiation between two Spokes

If data traffic between two Spokes (A and B) transits via another Spoke (T) then **no shortcut can be established** between A and B

The Hub→Spoke **OSPF cost** and the Spoke→Hub OSPF cost must be configured in such a way that it is less expensive to transit via the Hub than to transit via another Spoke

OSPF configuration

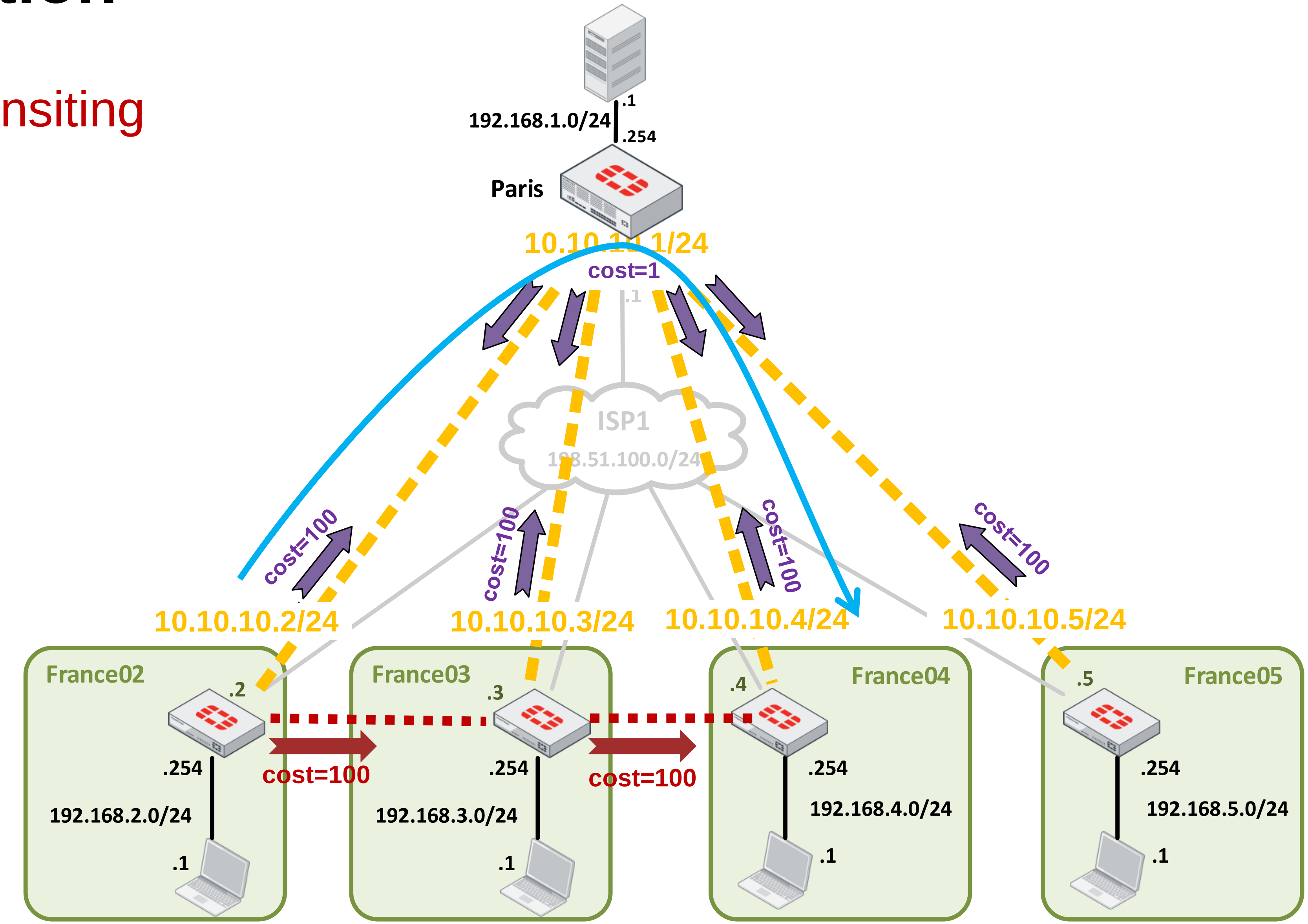
- Prevent traffic from transiting via Spokes

France02 → Hub → France04

The path cost via the Hub is **101**

France02 → France03 → France04

The path cost via France03 is **200**



Hub OSPF configuration

distribut-list-in “PFL_filter_overlay_IPs”

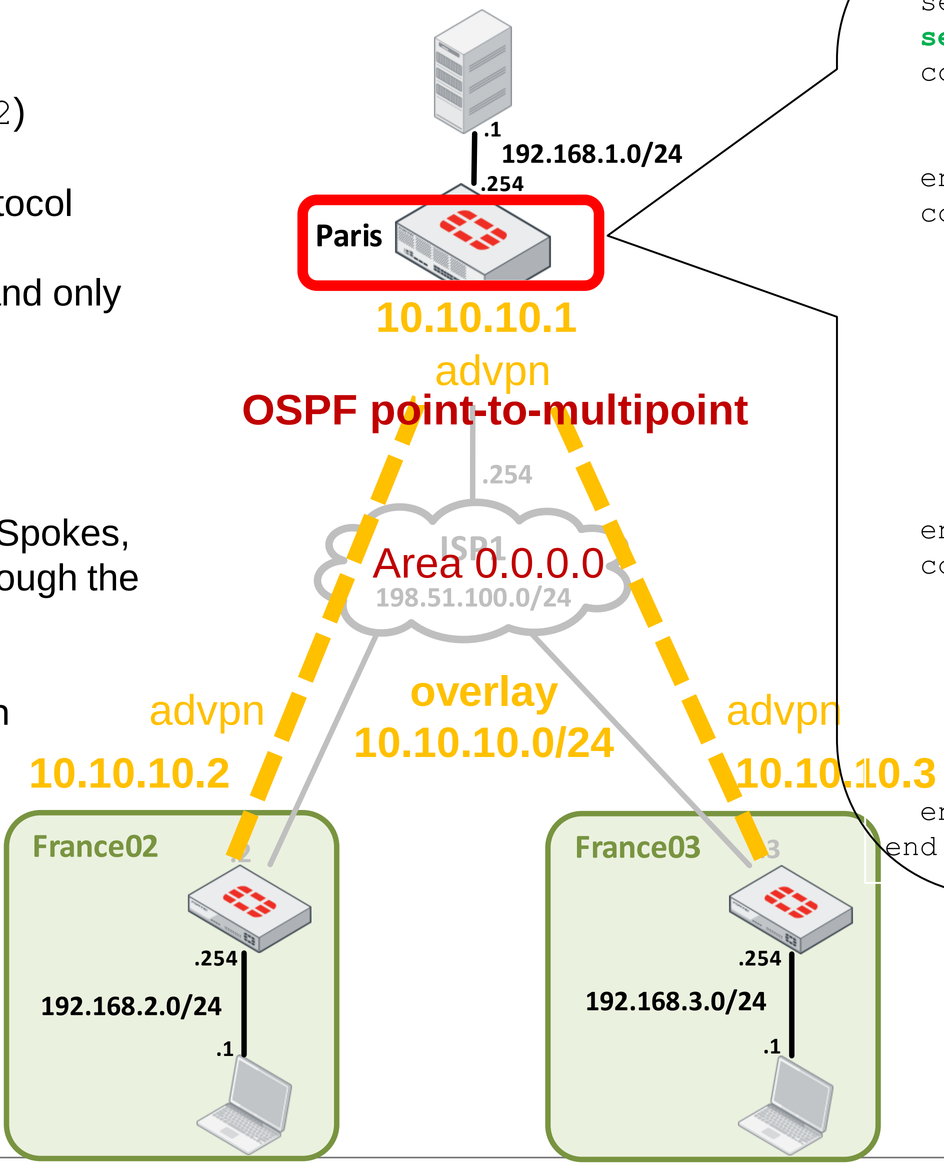
Filter the overlay tunnel IPs (`10.10.10.x/32`)

The overlay IPs are advertised by ADVPN protocol and by OSPF
Filter out the overlay IPs learned from OSPF and only keep those advertised by ADVPN itself

cost 1

When no shortcut is established between two Spokes, Spoke↔Spoke traffic should prefer flowing through the Hub than flowing through another Spoke

OSPF cost of “SpokeA→ Hub → SpokeB” path must be less than the OSPF cost of “SpokeA → SpokeT → SpokeB” path



```
config router ospf
  set router-id 10.10.10.1
  set distribute-list-in "PFL_filter_overlay_IPs"
  config area
      edit 0.0.0.0
      next
  end
  config ospf-interface
      edit "advpn"
          set interface "advpn"
          set network-type point-to-multipoint
          set mtu-ignore enable
          set cost 1
          set hello-interval 10
          set dead-interval 40
      next
  end
  config network
      edit 1
          set prefix 10.10.10.0 255.255.255.0
      next
      edit 2
          set prefix 192.168.1.0 255.255.255.0
      next
  end
end
```

Hub OSPF configuration

network-type point-to-multipoint

With the default of “net-device disable” configured for the phase1, multiple OSPF adjacencies can be established over the “advpn” tunnel interface

OSPF type for this interface is therefore “point-to-multipoint”

mtu-ignore enable

Multiple tunnels with possibly different MTUs (e.g., NATed Spokes) are associated to the same interface

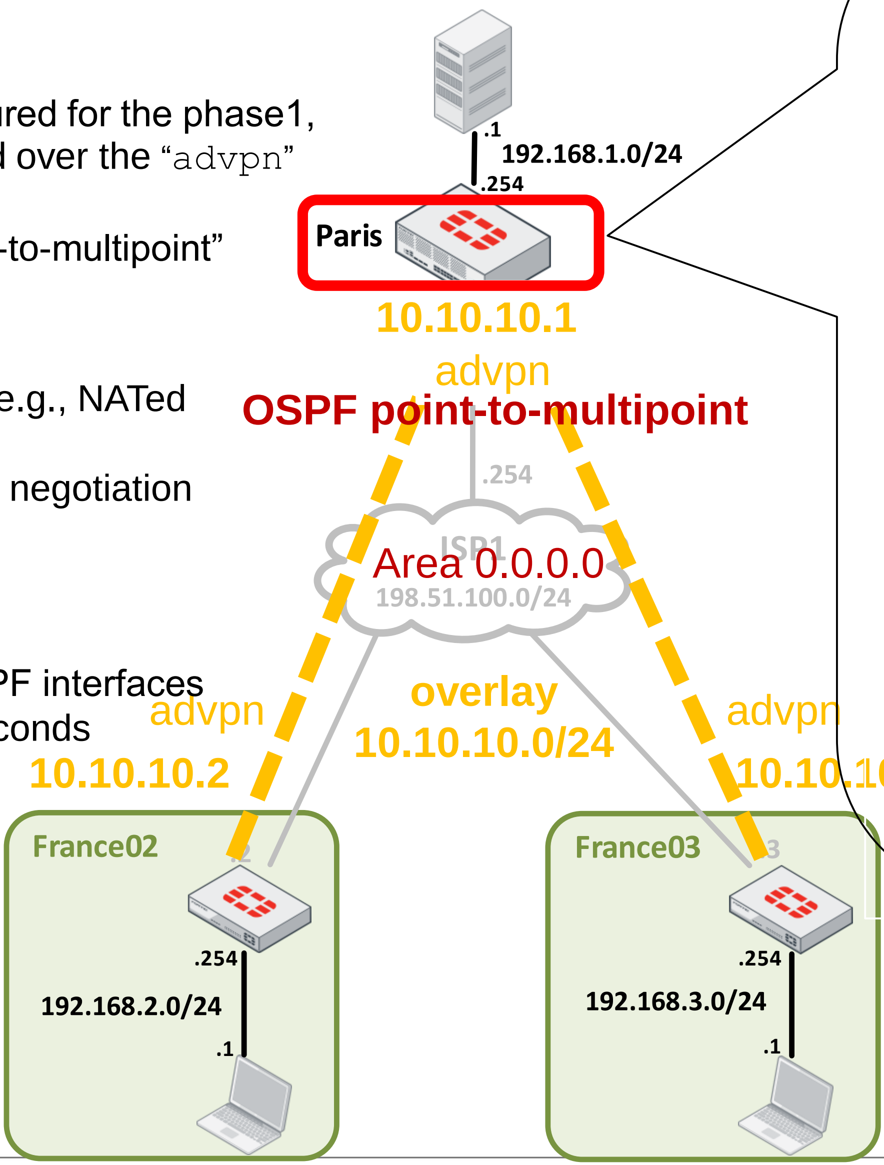
MTU must be ignored during OSPF adjacency negotiation

hello-interval 10 , dead-interval 40

The default timers for “point-to-multipoint” OSPF interfaces are 30 seconds for the Hello timer and 120 seconds for the Dead timer

OSPF timers must match between Peers

These two CLI settings set the timers to the default values used by OSPF “point-to-point” interfaces



```
config router ospf
  set router-id 10.10.10.1
  set distribute-list-in "PFL_filter_overlay_IPs"
  config area
      edit 0.0.0.0
      next
  end
  config ospf-interface
      edit "advpn"
          set interface "advpn"
          set network-type point-to-multipoint
          set mtu-ignore enable
          set cost 1
          set hello-interval 10
          set dead-interval 40
      next
  end
  config network
      edit 1
          set prefix 10.10.10.0 255.255.255.0
      next
      edit 2
          set prefix 192.168.1.0 255.255.255.0
      next
  end
end
```

Hub OSPF configuration

Hub configured with “net-device enable”

⚠ This configuration is **not recommended** and is **not supported for SD-WAN**

distribut-list-in “PFL_filter_overlay_IPs”

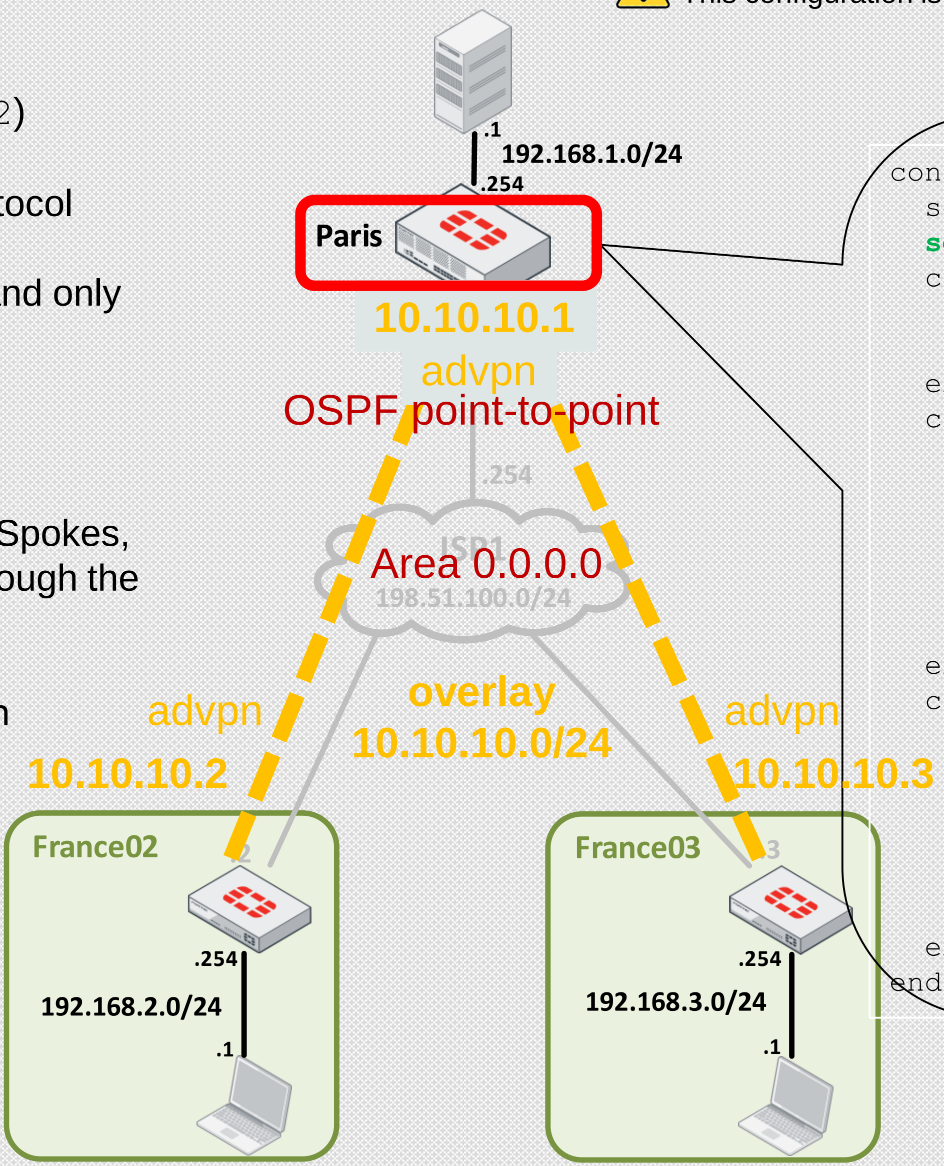
Filter the overlay tunnel IPs (`10.10.10.x/32`)

The overlay IPs are advertised by ADVPN protocol and by OSPF
Filter out the overlay IPs learned from OSPF and only keep those advertised by ADVPN itself

cost 1

When no shortcut is established between two Spokes, Spoke↔Spoke traffic should prefer flowing through the Hub than flowing through another Spoke

OSPF cost of “SpokeA→ Hub → SpokeB” path must be less than the OSPF cost of “SpokeA → SpokeT → SpokeB” path



```
config router ospf
   set router-id 10.10.10.1
   set distribute-list-in "PFL_filter_overlay_IPs"
   config area
      edit 0.0.0.0
      next
   end
   config ospf-interface
      edit "advpn"
         set interface "advpn"
         set network-type point-to-point
         set mtu-ignore enable
         set cost 1
      next
   end
   config network
      edit 1
         set prefix 10.10.10.0 255.255.255.0
      next
      edit 2
         set prefix 192.168.1.0 255.255.255.0
      next
   end
end
```

Hub OSPF configuration

Hub configured with “net-device enable”

⚠ This configuration is **not recommended** and is **not supported for SD-WAN**

network-type point-to-point

With “net-device enable” configured for the phase1, an interface “advpn_xx” is dynamically created along with the “advpn_xx” tunnel itself.

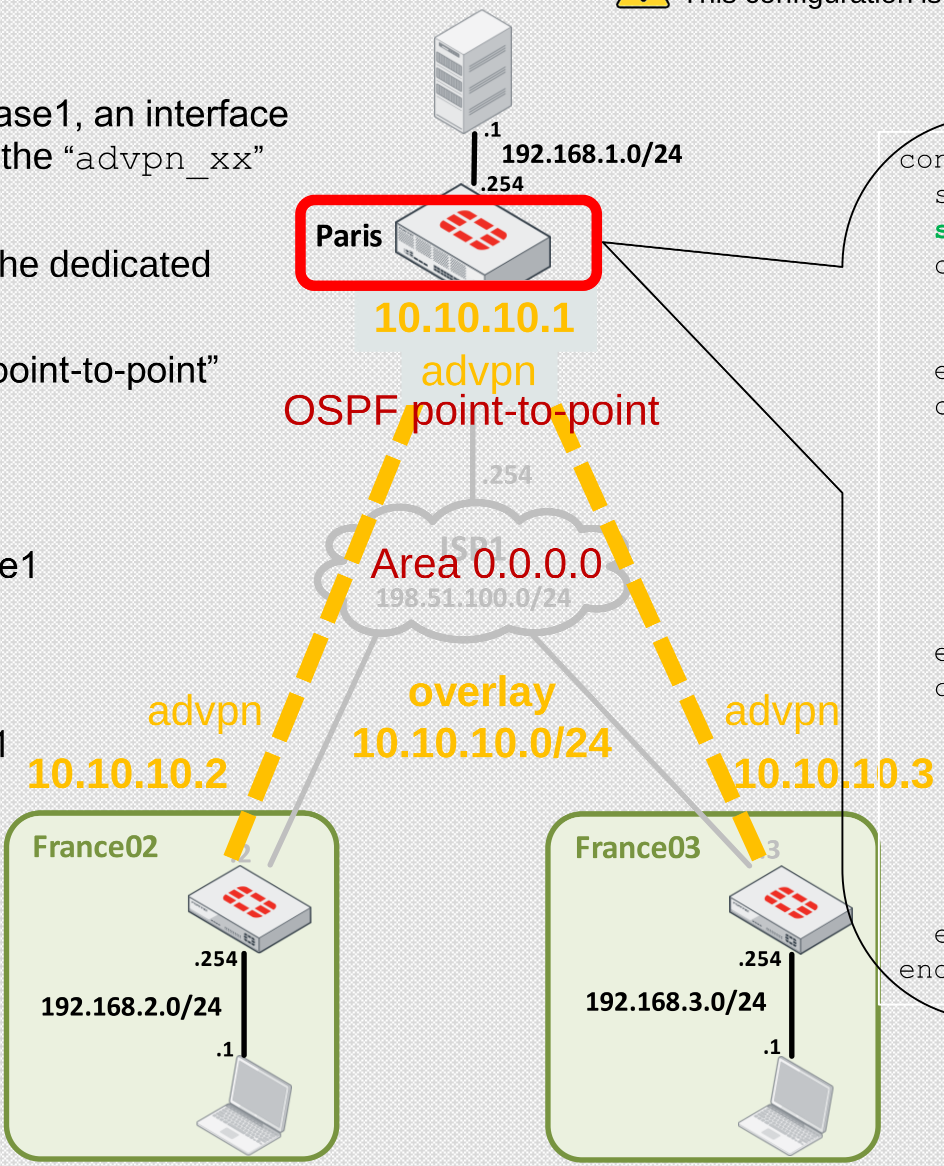
A single OSPF adjacency is established over the dedicated tunnel interface “advpn_xx”.

The OSPF type for this interface is therefore “point-to-point”

mtu-ignore enable

If all the ADVPN Spokes are configured with “net-device enable” for their ADVPN phase1 then this setting is not needed

If at least one ADVPN Spoke is configured with “net-device disable” for its ADVPN phase1 then it is recommended to ignore the MTU during OSPF negotiation



```
config router ospf
  set router-id 10.10.10.1
  set distribute-list-in "PFL_filter_overlay_IPs"
  config area
      edit 0.0.0.0
      next
  end
  config ospf-interface
      edit "advpn"
          set interface "advpn"
          set network-type point-to-point
          set mtu-ignore enable
          set cost 1
      next
  end
  config network
      edit 1
          set prefix 10.10.10.0 255.255.255.0
      next
      edit 2
          set prefix 192.168.1.0 255.255.255.0
      next
  end
end
```

Spoke OSPF configuration

"net-device disable" for shortcuts

⚠ This configuration is **not supported for SD-WAN**

distribut-list-in "PFL_filter_overlay_IPs"

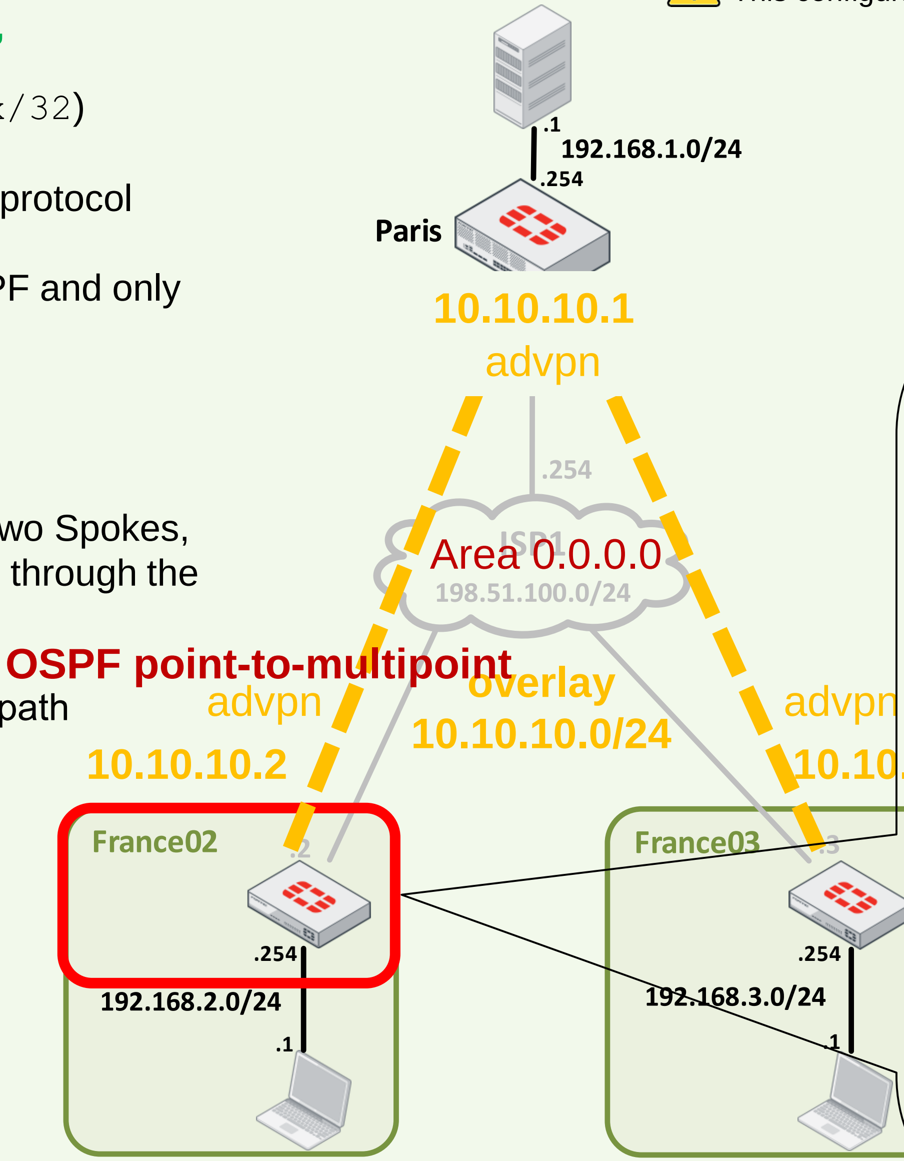
Filter the overlay tunnel IPs (`10.10.10.x/32`)

The overlay IPs are advertised by ADVPN protocol and by OSPF
Filter out the overlay IPs learned from OSPF and only keep those advertised by ADVPN itself

cost 100

When no shortcut is established between two Spokes, Spoke↔Spoke traffic should prefer flowing through the Hub than flowing through another Spoke

OSPF cost of "SpokeA→ Hub → SpokeB" path must be less than the OSPF cost of "SpokeA → SpokeT → SpokeB" path



```
config router ospf
  set router-id 10.10.10.2
  set distribute-list-in "PFL_filter_overlay_IPs"
  config area
      edit 0.0.0.0
      next
  end
  config ospf-interface
      edit "advpn"
          set interface "advpn"
          set network-type point-to-multipoint
          set mtu-ignore enable
          set cost 100
          set hello-interval 10
          set dead-interval 40
      next
  end
  config network
      edit 1
          set prefix 10.10.10.0 255.255.255.0
      next
      edit 2
          set prefix 192.168.2.0 255.255.255.0
      next
  end
end
```

Spoke OSPF configuration

"net-device disable" for shortcuts

⚠ This configuration is **not supported for SD-WAN**

network-type point-to-multipoint

With the default of "net-device disable" configured for the phase1, multiple OSPF adjacencies can be established over the "advpn" tunnel interface
OSPF type for this interface is therefore "point-to-multipoint"

mtu-ignore enable

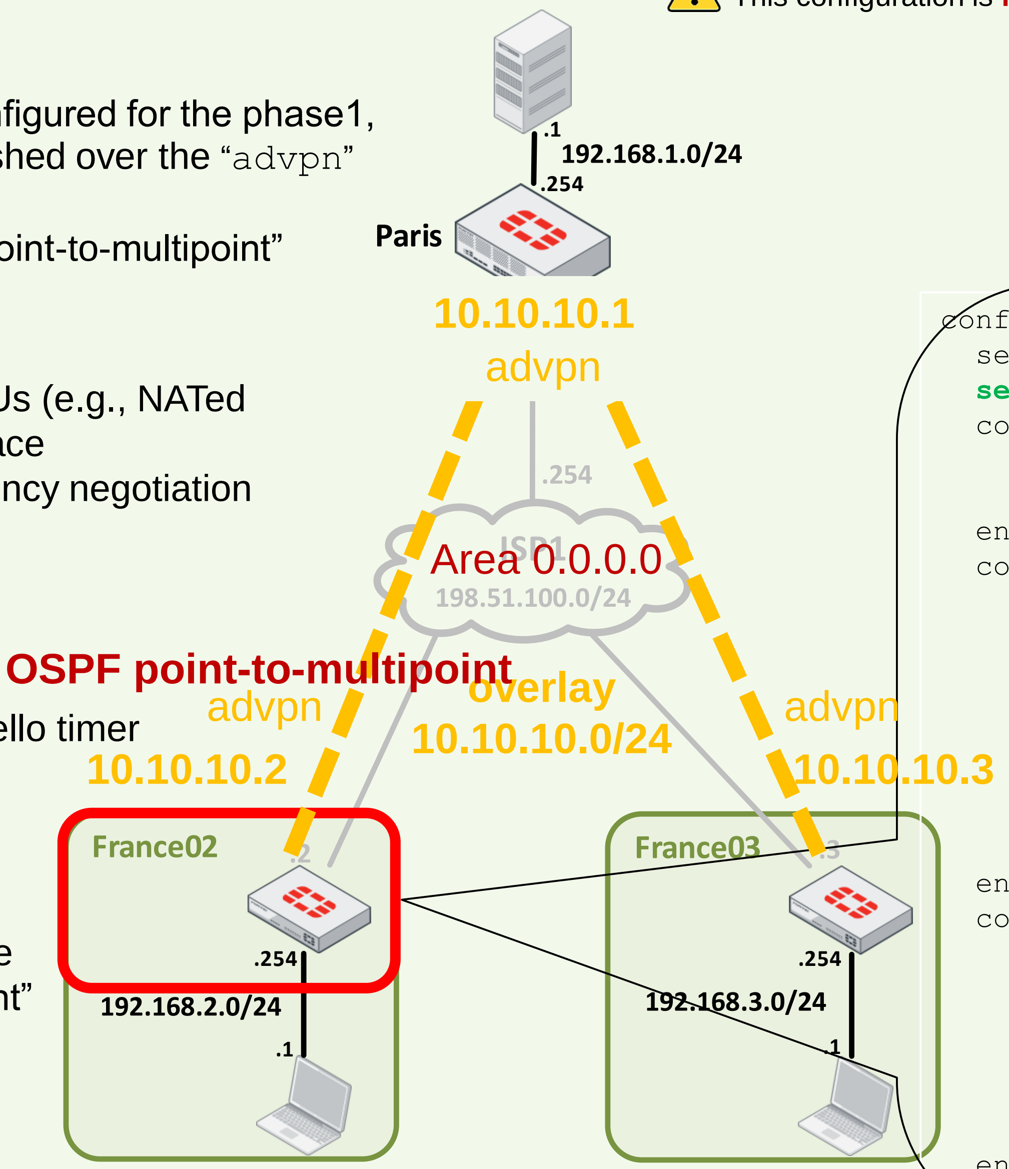
Multiple tunnels with possibly different MTUs (e.g., NATed Spokes) are associated to the same interface
MTU must be ignored during OSPF adjacency negotiation

hello-interval 10 , dead-interval 40

The default timers for "point-to-multipoint" OSPF interfaces are 30 seconds for the Hello timer and 120 seconds for the Dead timer

OSPF timers must match between Peers

These two CLI settings set the timers to the default values used by OSPF "point-to-point" interfaces



```
config router ospf
  set router-id 10.10.10.2
  set distribute-list-in "PFL_filter_overlay_IPs"
  config area
      edit 0.0.0.0
      next
  end
  config ospf-interface
      edit "advpn"
          set interface "advpn"
          set network-type point-to-multipoint
          set mtu-ignore enable
          set cost 100
          set hello-interval 10
          set dead-interval 40
      next
  end
  config network
      edit 1
          set prefix 10.10.10.0 255.255.255.0
      next
      edit 2
          set prefix 192.168.2.0 255.255.255.0
      next
  end
end
```

Spoke OSPF configuration

"net-device enable" for shortcuts

distribut-list-in "PFL_filter_overlay_IPs"

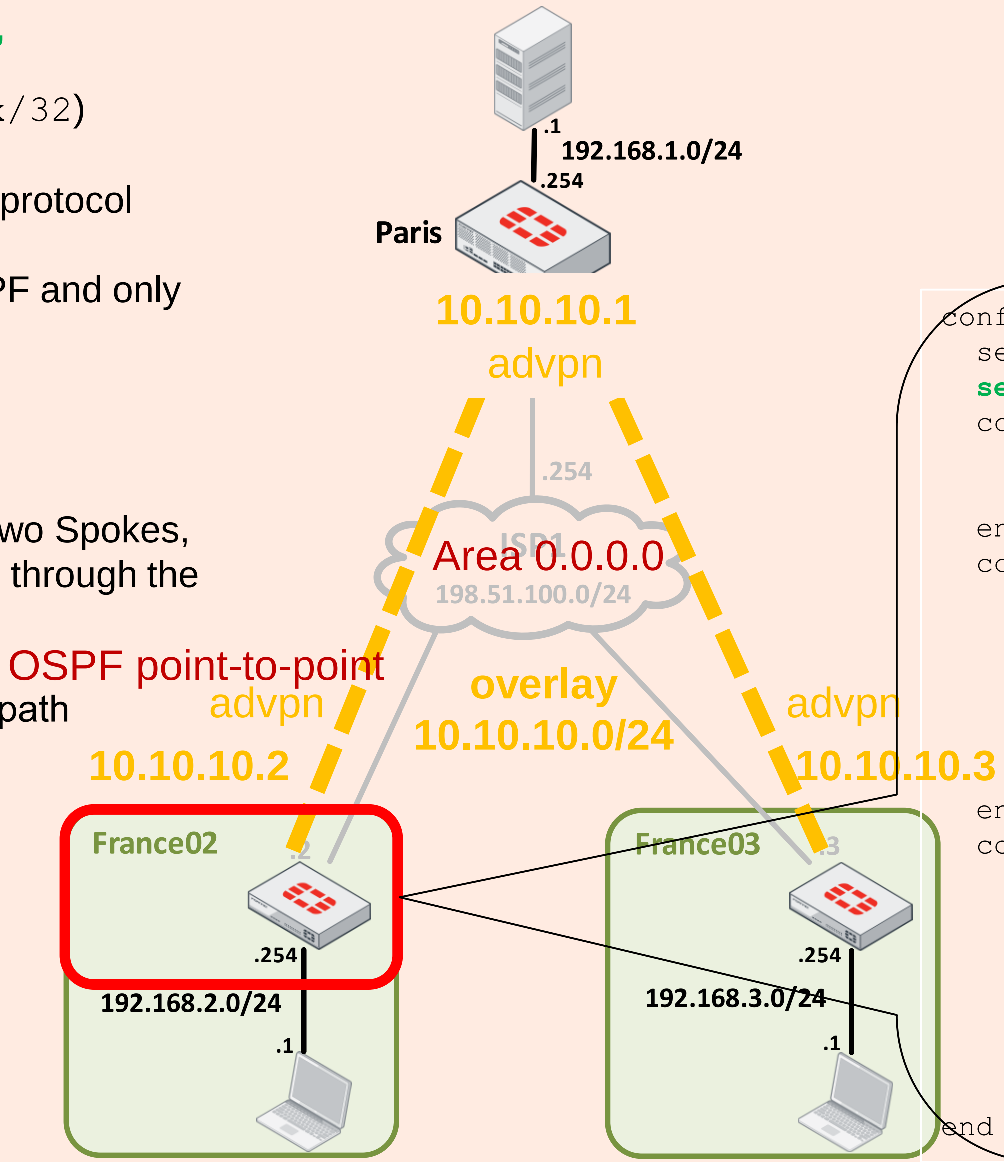
Filter the overlay tunnel IPs (`10.10.10.x/32`)

The overlay IPs are advertised by ADVPN protocol and by OSPF
Filter out the overlay IPs learned from OSPF and only keep those advertised by ADVPN itself

cost 100

When no shortcut is established between two Spokes, Spoke↔Spoke traffic should prefer flowing through the Hub than flowing through another Spoke

OSPF cost of "SpokeA→ Hub → SpokeB" path must be less than the OSPF cost of "SpokeA → SpokeT → SpokeB" path



```
config router ospf
  set router-id 10.10.10.2
  set distribute-list-in "PFL_filter_overlay_IPs"
  config area
      edit 0.0.0.0
      next
  end
  config ospf-interface
      edit "advpn"
          set interface "advpn"
          set network-type point-to-point
          set mtu-ignore enable
          set cost 100
      next
  end
  config network
      edit 1
          set prefix 10.10.10.0 255.255.255.0
      next
      edit 2
          set prefix 192.168.2.0 255.255.255.0
      next
    end
end
```

Spoke OSPF configuration

"net-device enable" for shortcuts

network-type point-to-point

With "net-device enable" configured for the phase1, an interface "`advpn_xx`" is dynamically created along with the "`advpn_xx`" tunnel itself.

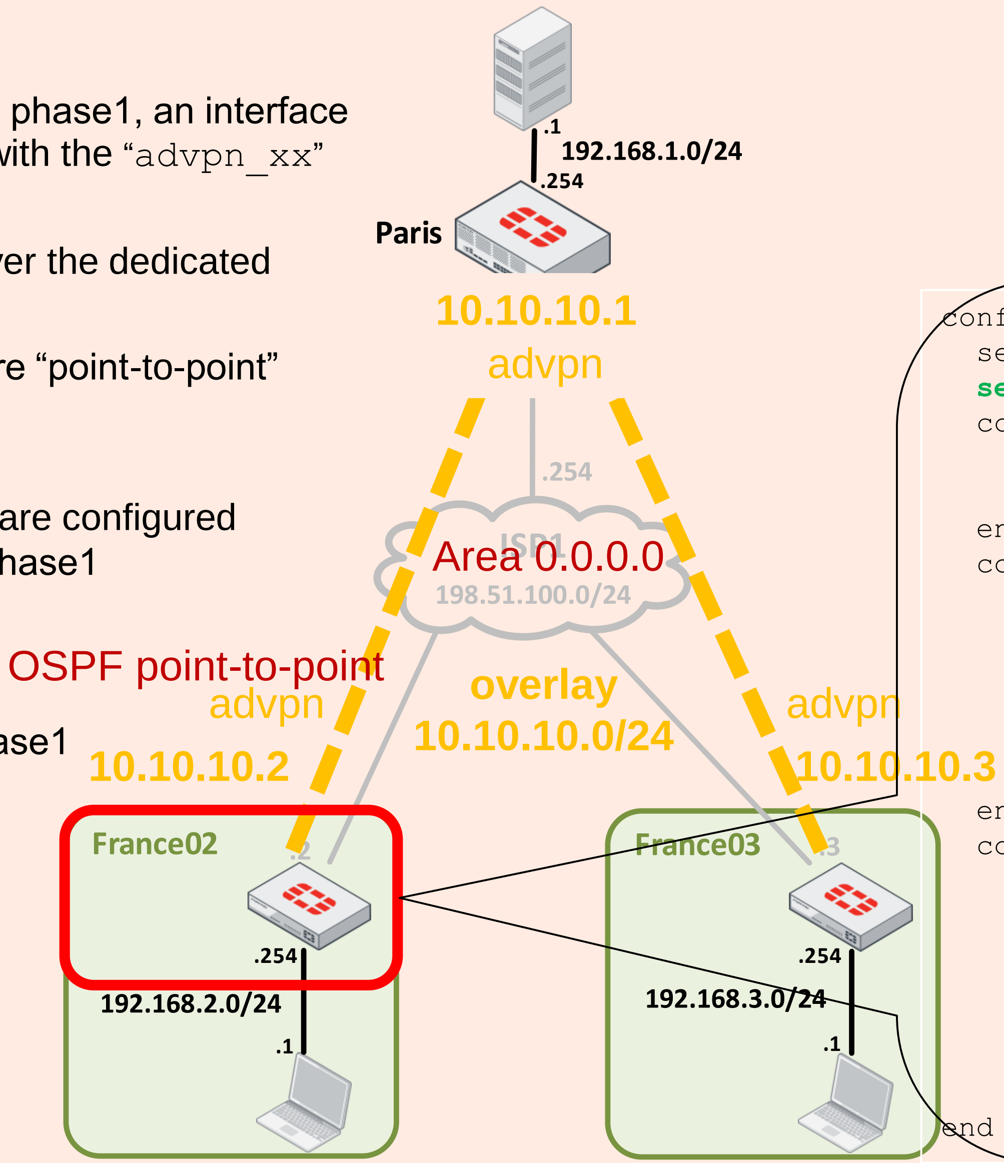
A single OSPF adjacency is established over the dedicated tunnel interface "`advpn_xx`".

The OSPF type for this interface is therefore "point-to-point"

mtu-ignore enable

If the ADVPN Hub and all ADVPN Spokes are configured with "net-device enable" for their ADVPN phase1 then this setting is not needed

If at least one ADVPN Spoke is configured with "net-device disable" for its ADVPN phase1 then it is recommended to ignore the MTU during OSPF negotiation



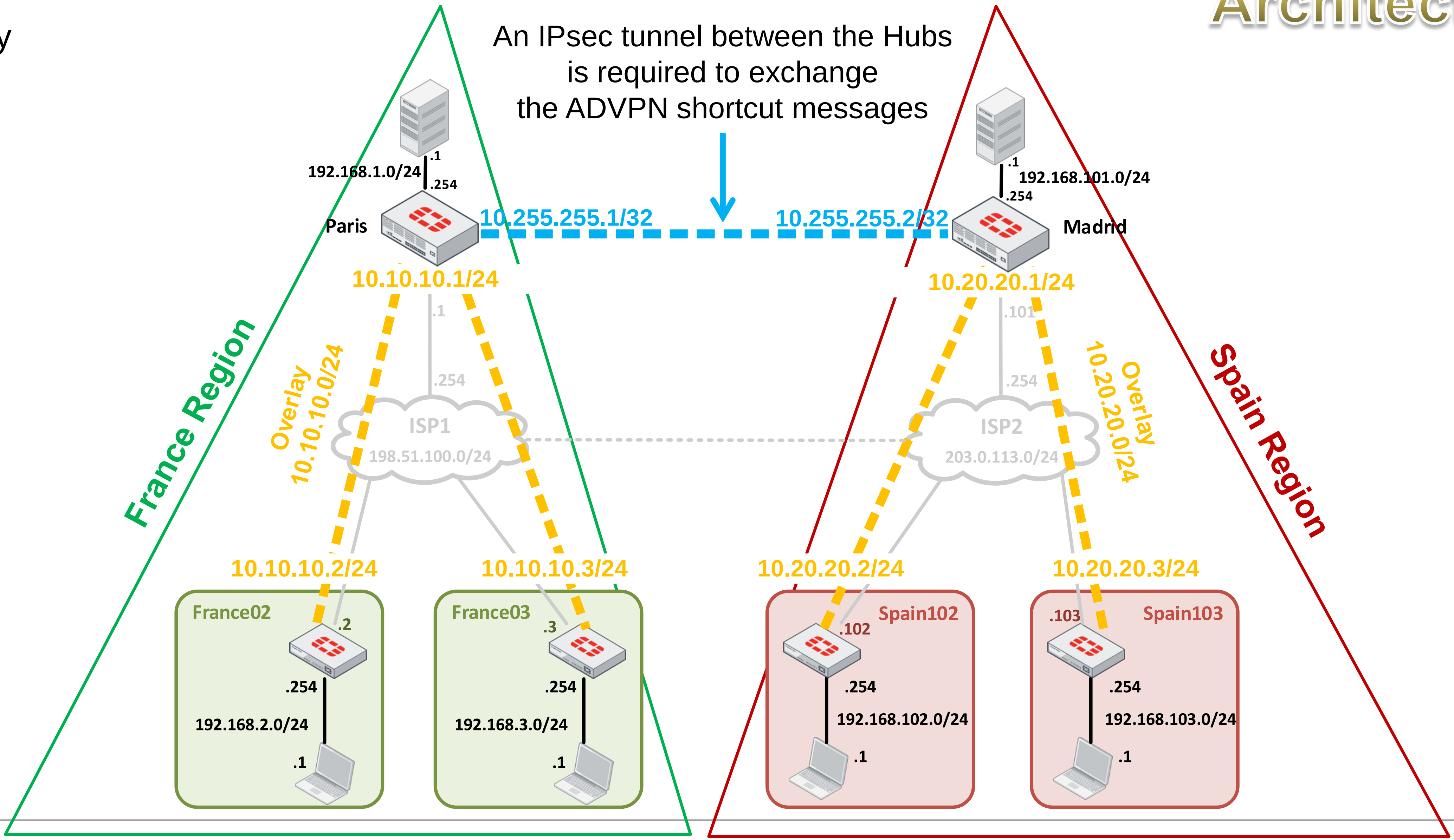
```
config router ospf
  set router-id 10.10.10.2
  set distribute-list-in "PFL_filter_overlay_IPs"
  config area
      edit 0.0.0.0
      next
  end
  config ospf-interface
      edit "advpn"
          set interface "advpn"
          set network-type point-to-point
          set mtu-ignore enable
          set cost 100
      next
  end
  config network
      edit 1
          set prefix 10.10.10.0 255.255.255.0
      next
      edit 2
          set prefix 192.168.2.0 255.255.255.0
      next
    end
end
```

Dual Region (BGP)

Interconnecting two independent Hub & Spoke Regions

Dual Region (BGP)

Overlay



An IPsec tunnel between the Hubs is required to exchange the ADVPN shortcut messages

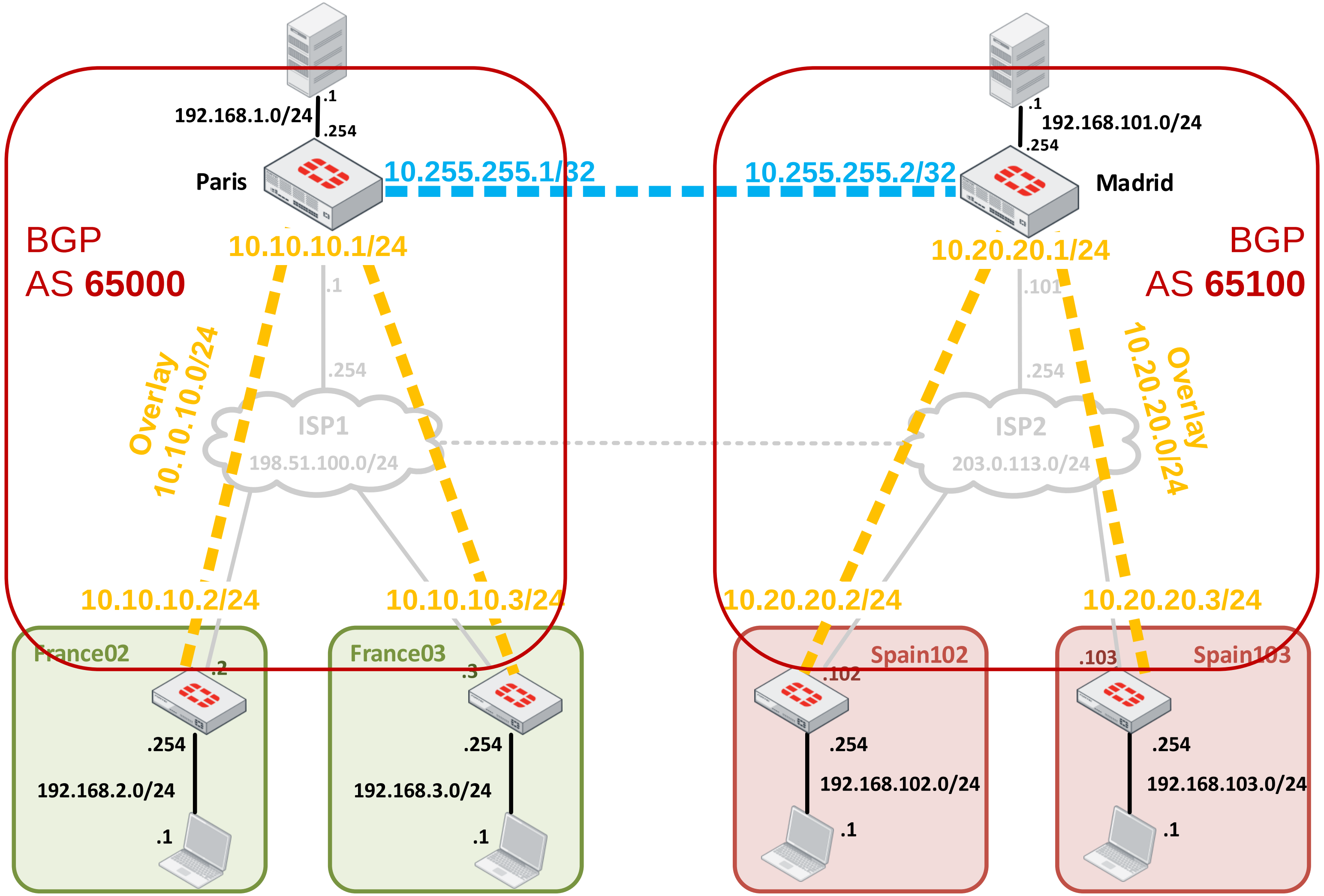
Dual Region (BGP)

Overlay

Each region has a distinct AS

iBGP is used for intra-region routing

eBGP is used for inter-region routing



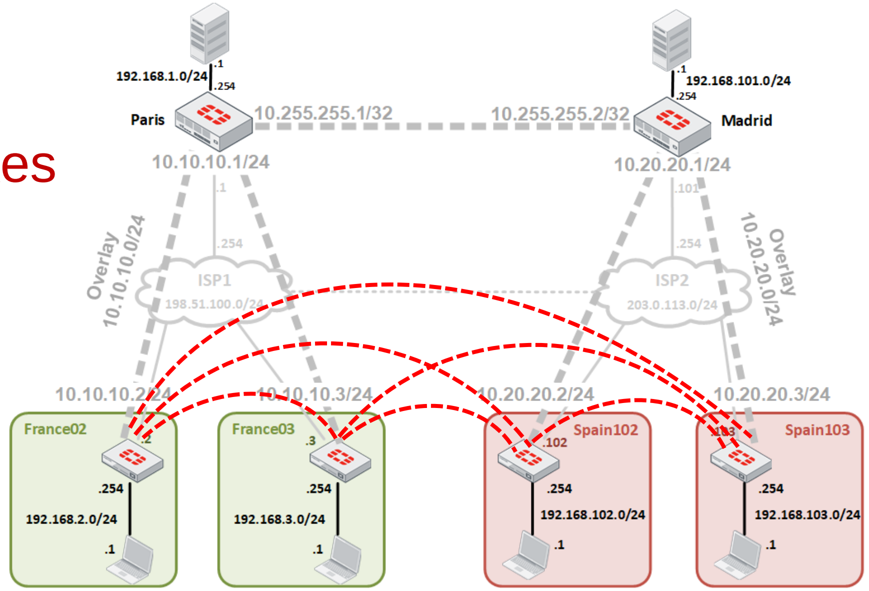
Dual Region (BGP)

IPsec configuration

Dual Region (BGP)

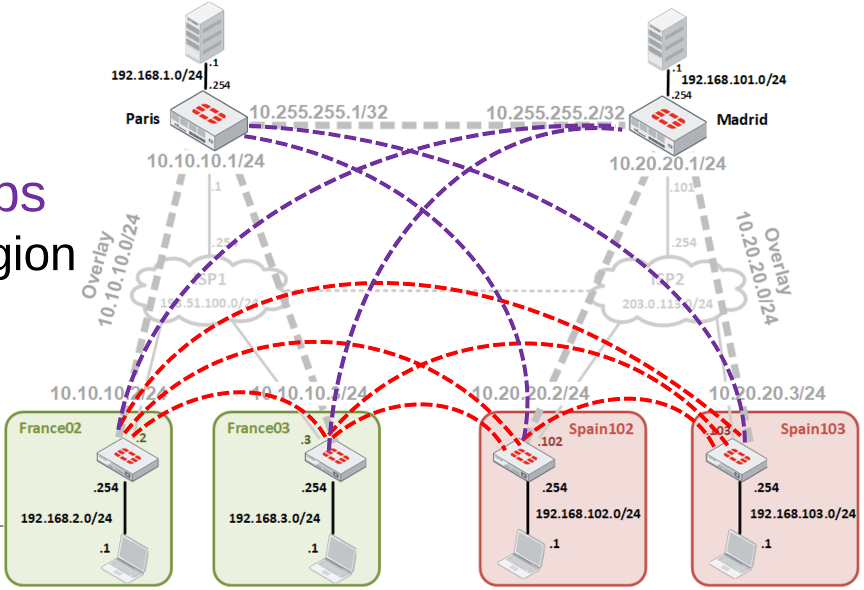
Two use cases:

- Shortcuts are established only between Spokes
  - » Shortcuts are established between Spokes within the same region and across region



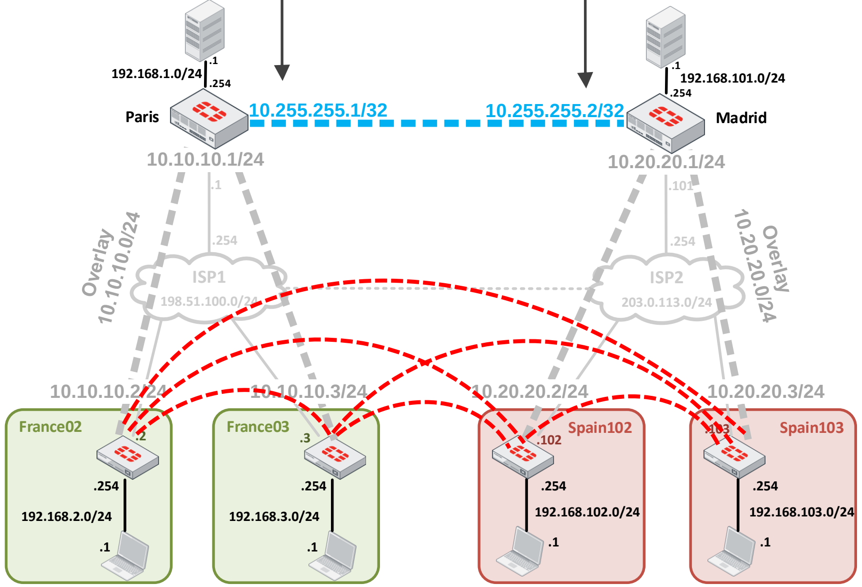
As of FortiOS 6.2.1

- Shortcuts are established between Spokes and with the Hubs
  - » Shortcuts are established between Spokes within the same region and across region
  - » Shortcuts are established between Spokes of one region towards the Hub of the other region



Dual Region (BGP)

```
config vpn ipsec phase1-interface
    edit "toMadrid"
        set interface "wan"
        set proposal aes128-sha1
        set auto-discovery-forwarder enable
        set remote-gw 203.0.113.1
        set psksecret xxxxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "toMadrid"
        set phase1name "toMadrid"
        set proposal aes128-sha1
    next
end

config system interface
    edit "toMadrid"
        set ip 10.255.255.1/32
        set remote-ip 10.255.255.2/32
    next
end
```



```
config vpn ipsec phase1-interface
   edit "toParis"
     set interface "wan"
     set proposal aes128-sha1
     set auto-discovery-forwarder enable
     set remote-gw 198.51.100.1
     set psksecret xxxxxxxx
   next
end

config vpn ipsec phase2-interface
    edit "toParis"
        set phase1name "toParis"
        set proposal aes128-sha1
    next
end

config system interface
    edit "toParis"
        set ip 10.255.255.2/32
        set remote-ip 10.255.255.1/32
    next
end
```

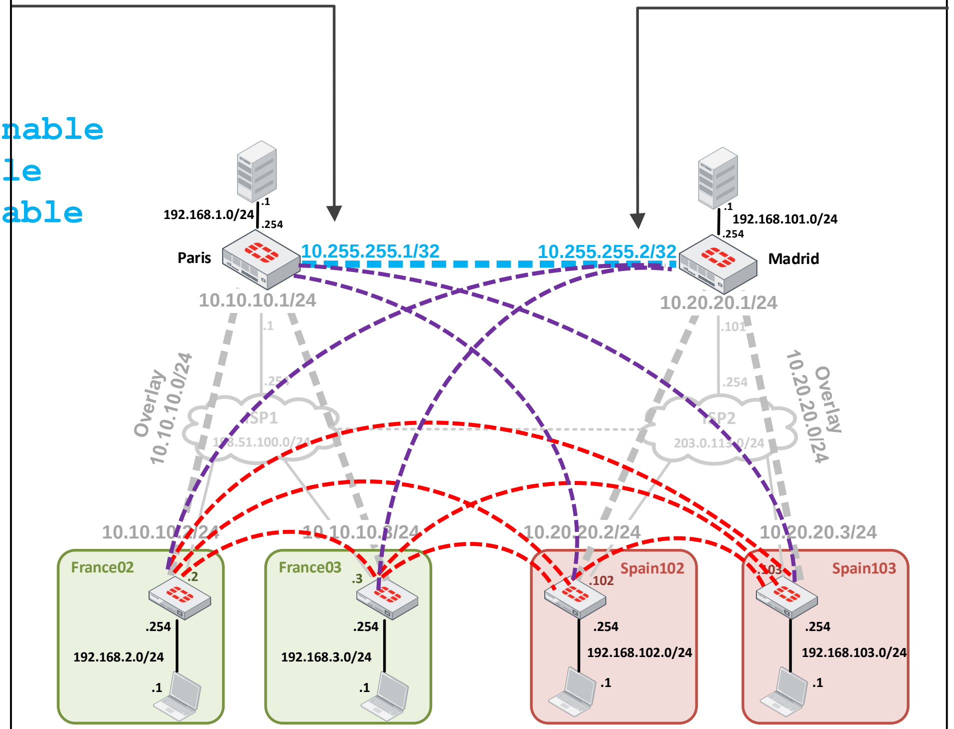
Shortcuts are established only between Spokes

Shortcuts are established between Spokes
within the same region and across region

Dual Region (BGP)

As of FortiOS 6.2.1

```
config vpn ipsec phase1-interface
  edit "toMadrid"
     set interface "wan"
     set proposal aes128-sha1
     set auto-discovery-forwarder enable
     set auto-discovery-sender enable
     set auto-discovery-receiver enable
     set net-device disable
     set tunnel-search nexthop
     set add-route disable
     set remote-gw 203.0.113.1
     set psksecret xxxxxxxx
  next
end

config vpn ipsec phase2-interface
    edit "toMadrid"
        set phase1name "toMadrid"
        set proposal aes128-sha1
    next
end

config system interface
    edit "toMadrid"
        set ip 10.255.255.1/32
        set remote-ip 10.255.255.2/32
    next
end
```



Shortcuts are established between Spokes and with the Hubs

Shortcuts are established between Spokes within the same region and across region

Shortcuts are established between Spokes of one region towards the Hub of the other region

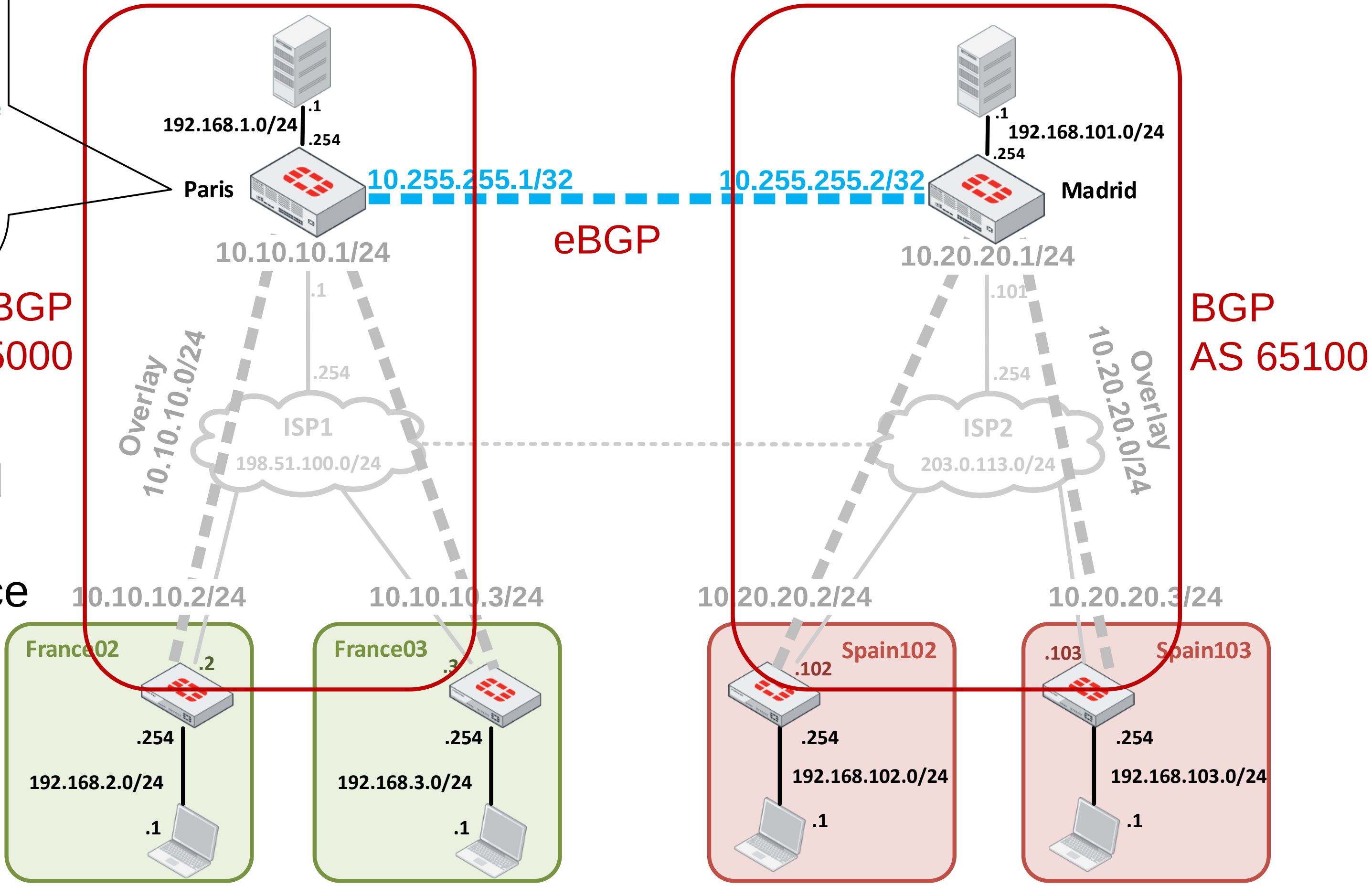
```
config vpn ipsec phase1-interface
  edit "toParis"
    set interface "wan"
    set proposal aes128-sha1
    set auto-discovery-forwarder enable
    set auto-discovery-sender enable
    set auto-discovery-receiver enable
    set net-device disable
    set tunnel-search nexthop
    set add-route disable
    set remote-gw 198.51.100.1
    set psksecret xxxxxxxx
  next
end

config vpn ipsec phase2-interface
    edit "toParis"
        set phase1name "toParis"
        set proposal aes128-sha1
    next
end

config system interface
    edit "toParis"
        set ip 10.255.255.2/32
        set remote-ip 10.255.255.1/32
    next
end
```

Dual Region (BGP)

BGP configuration

Dual Region (BGP)

```
config router bgp
    set as 65000
    set router-id 10.10.10.1
    config neighbor
        edit "10.255.255.2"
            set attribute-unchanged next-hop
             set ebgp-enforce-multihop enable
            set remote-as 65100
        next
    end
end
```



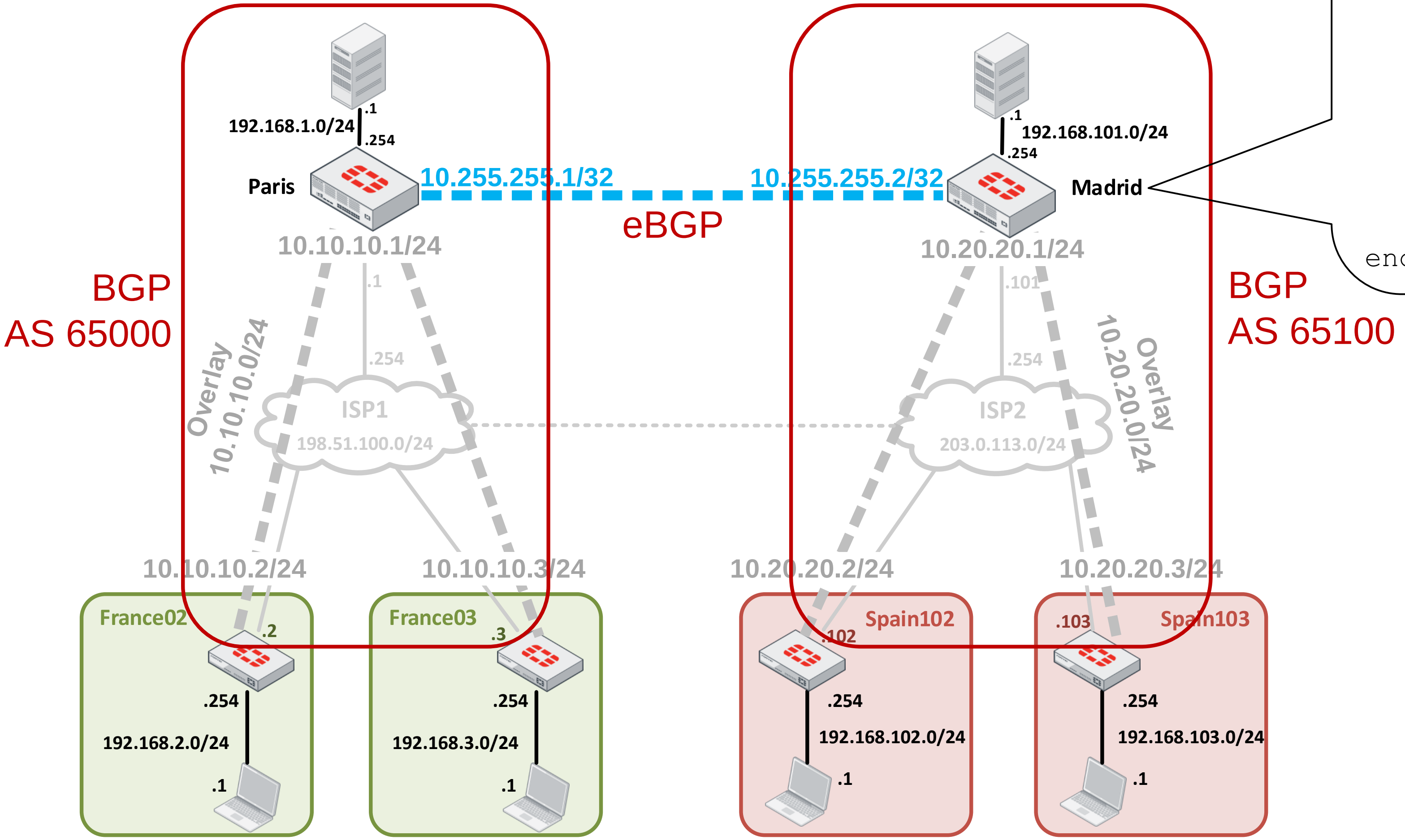
attribute-unchanged next-hop

keep the BGP Next-Hop attributes unchanged when BGP routes exit the AS.
This is mandatory to allow routing convergence over the ADVPN shortcuts.

ebgp-enforce-multihop

is required to keep the next-hop unchanged

Dual Region (BGP)



```
config router bgp
    set as 65100
    set router-id 10.20.20.1
    config neighbor
        edit "10.255.255.1"
            set attribute-unchanged next-hop
            set ebgp-enforce-multihop enable
            set remote-as 65000
        next
    end
end
```

Dual Region (BGP)

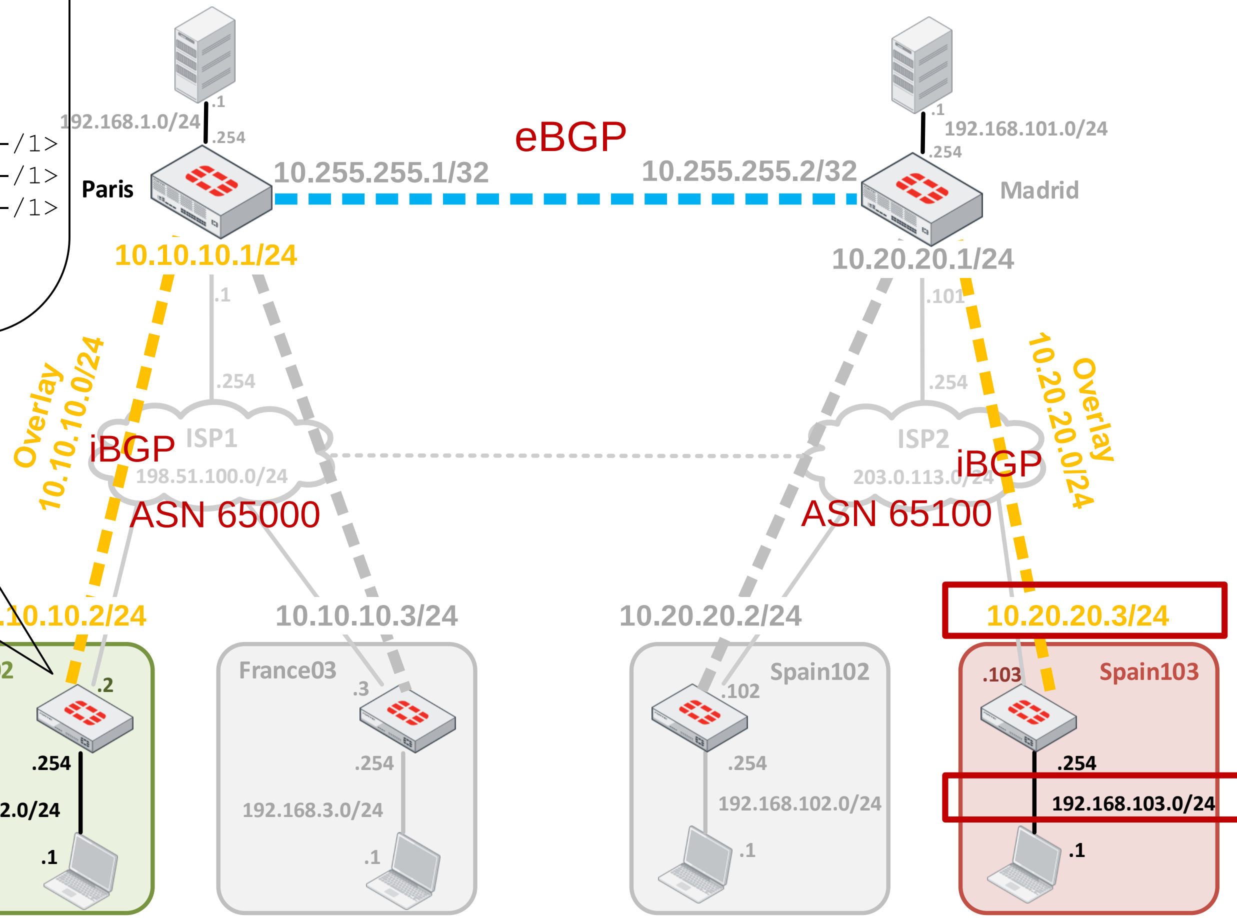
BGP Next-Hop Reachability

Dual Region - BGP Next Hop Reachability

```
France02 # get router info bgp network
France02 # get router info bgp network
BGP table version is 2, local router ID is 10.10.10.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight RouteTag Path
*>i192.168.1.0      10.10.10.1               0    100      0        0 i <-/1>
*> 192.168.2.0      0.0.0.0                       100  32768        0 i <-/1>
*>i192.168.3.0      10.10.10.3               0    100      0        0 i <-/1>
*>i192.168.101.0    10.255.255.2             0    100      0        0 65100 i <-/1>
*>i192.168.102.0    10.20.20.2               0    100      0        0 65100 i <-/1>
*>i192.168.103.0    10.20.20.3               0    100      0        0 65100 i <-/1>

Total number of prefixes 6
```

BGP Next-Hop must be accessible through the tunnel

```
config router static
    edit …
        set dst 10.20.20.0 255.255.255.0
        set device "advpn"
        set comment "Spain overlay subnet"
    next
end
```



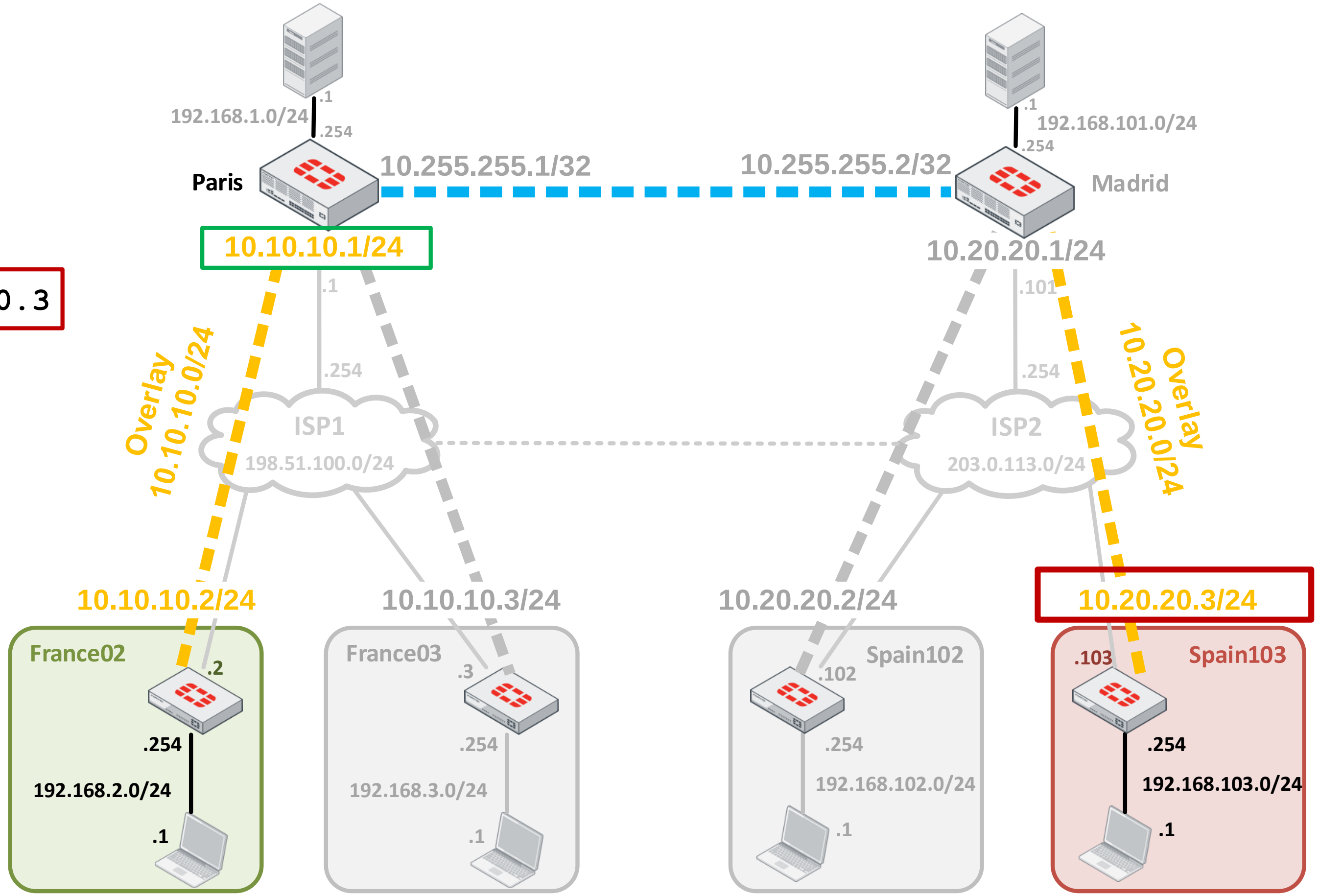
Dual Region - BGP Next Hop Reachability

No shortcut is established between France02 and Spain103

```
France02 #
config router static
    edit …
        set dst 10.20.20.0 255.255.255.0
        set device "advpn"
        set comment "Spain overlay subnet"
    next
end
```

```
France02 # get router info routing-table details 10.20.20.3
Routing table for VRF=0
Routing entry for 10.20.20.0/24
  Known via "static", distance 10, metric 0, best
  * 10.10.10.1, via advpn
```

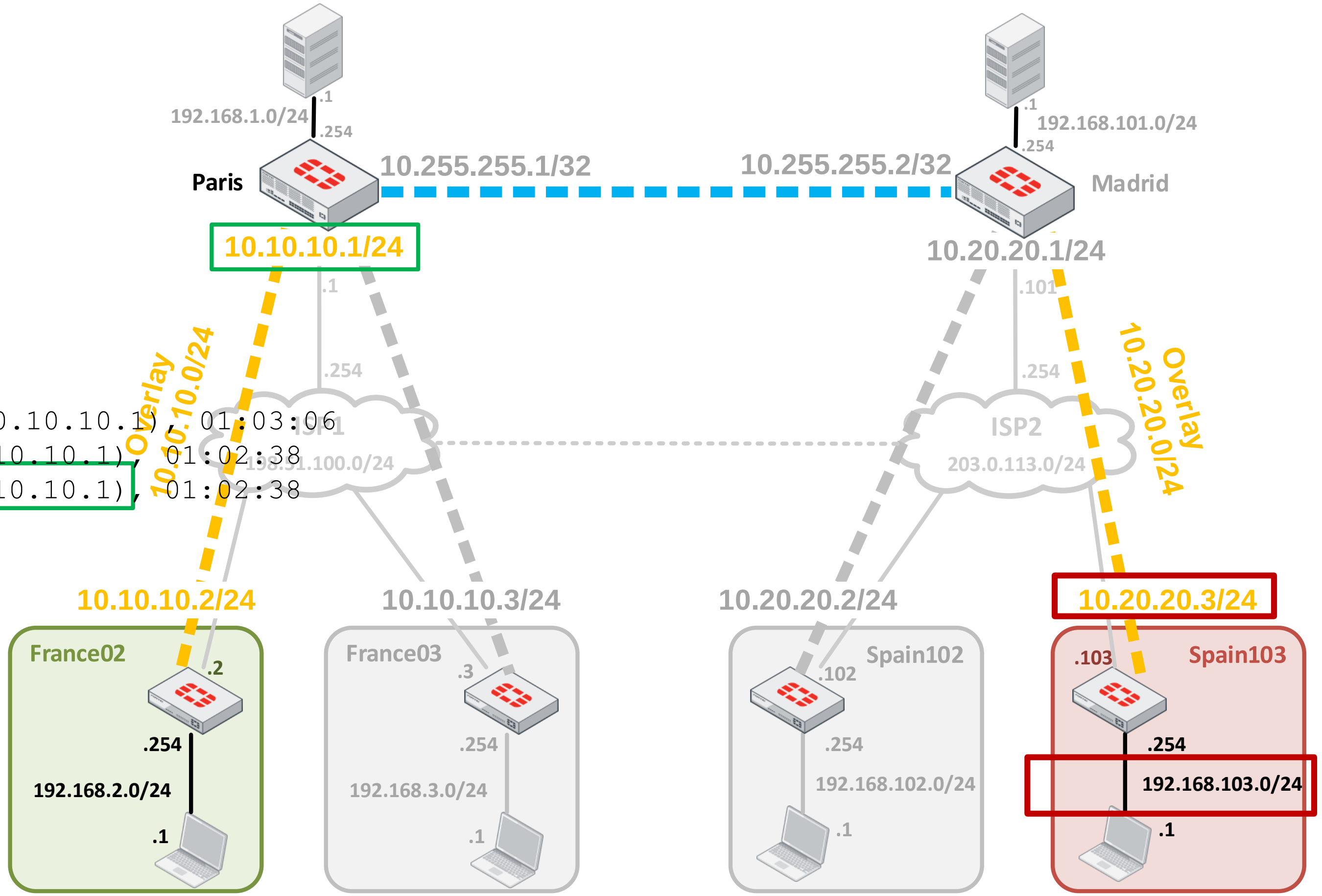
BGP Next-Hop of Spain103 Spoke (10.20.20.3) is accessible via Paris Hub (10.10.10.1)



Dual Region - BGP Next Hop Reachability

No shortcut is established between France02 and Spain103

```
France02 # get router info routing-table all
Routing table for VRF=0
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       (...)
       * - candidate default

S*      0.0.0.0/0 [10/0] via 198.51.100.254, wan

C       10.10.10.0/24 is directly connected, advpn
C       10.10.10.2/32 is directly connected, advpn
S       10.20.20.0/24 [10/0] via 10.10.10.1, advpn
S       10.255.255.0/30 [10/0] via 10.10.10.1, advpn

B       192.168.1.0/24 [200/0] via 10.10.10.1, advpn, 01:03:34
C       192.168.2.0/24 is directly connected, internal
B       192.168.3.0/24 [200/0] via 10.10.10.3, advpn, 01:03:06
B       192.168.101.0/24 [200/0] via 10.255.255.2 (recursive via 10.10.10.1), 01:03:06
B       192.168.102.0/24 [200/0] via 10.20.20.2 (recursive via 10.10.10.1), 01:02:38
B       192.168.103.0/24 [200/0] via 10.20.20.3 (recursive via 10.10.10.1), 01:02:38

C       198.51.100.0/24 is directly connected, wan
```



France02↔Spain103 traffic flows through the Hubs

Dual Region - BGP Next Hop Reachability

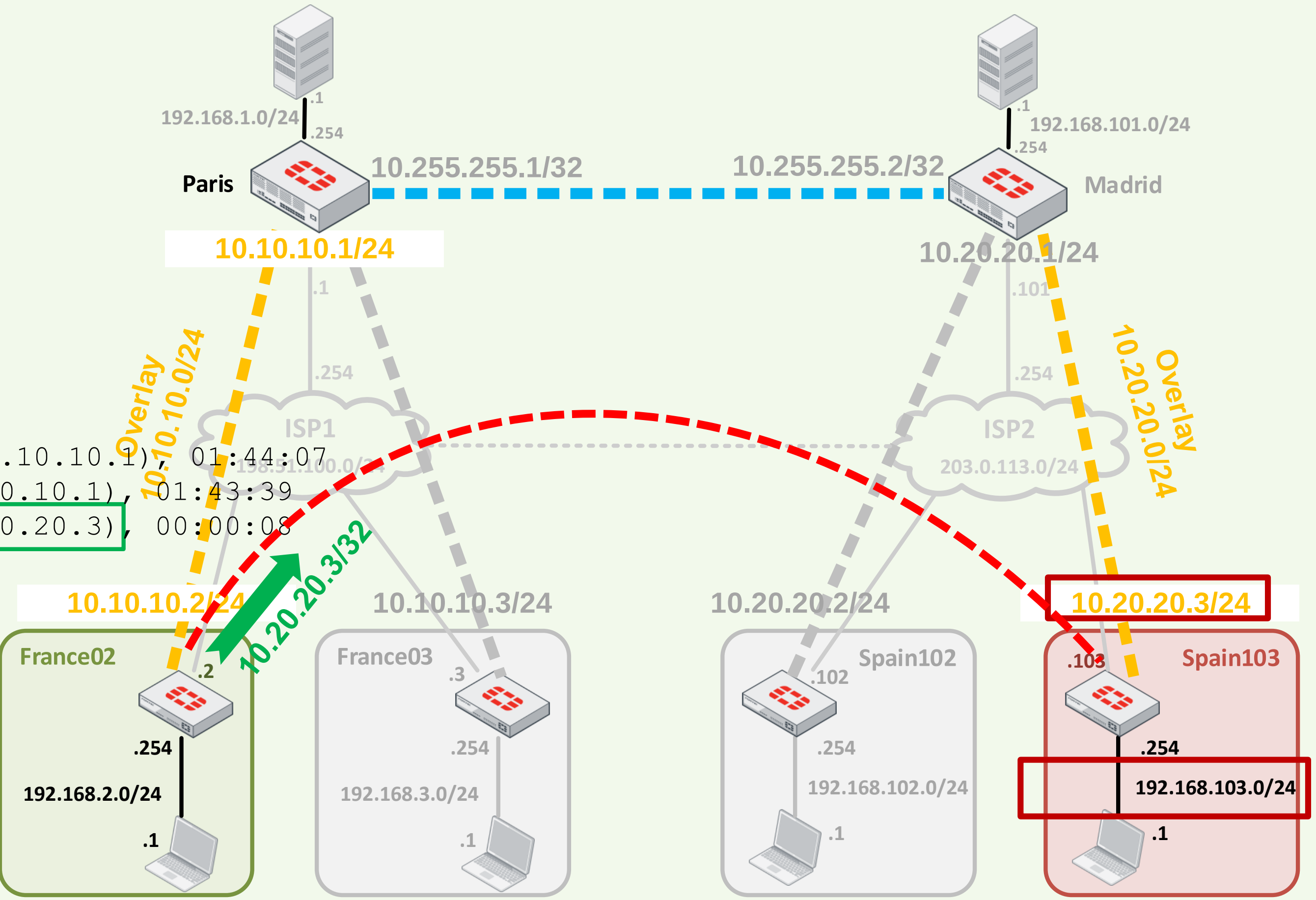
“net-device disable” for shortcuts

⚠ This configuration is **not supported for SD-WAN**

Shortcut is established between France02 and Spain103

```
France02 # get router info routing-table all
Routing table for VRF=0
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       (...)
       * - candidate default

S*      0.0.0.0/0 [10/0] via 198.51.100.254, wan

C       10.10.10.0/24 is directly connected, advpn
C       10.10.10.2/32 is directly connected, advpn
S       10.20.20.0/24 [10/0] via 10.10.10.1, advpn
S       10.20.20.3/32 [15/0] via 10.20.20.3, advpn
S       10.255.255.0/30 [10/0] via 10.10.10.1, advpn

B       192.168.1.0/24 [200/0] via 10.10.10.1, advpn, 01:44:35
C       192.168.2.0/24 is directly connected, internal
B       192.168.3.0/24 [200/0] via 10.10.10.3, advpn, 01:44:07
B       192.168.101.0/24 [200/0] via 10.255.255.2 (recursive via 10.10.10.1), 01:44:07
B       192.168.102.0/24 [200/0] via 10.20.20.2 (recursive via 10.10.10.1), 01:43:39
B       192.168.103.0/24 [200/0] via 10.20.20.3 (recursive via 10.20.20.3), 00:00:08

C       198.51.100.0/24 is directly connected, wan
```

Added by IKE



France02↔Spain103 traffic flows through the shortcut

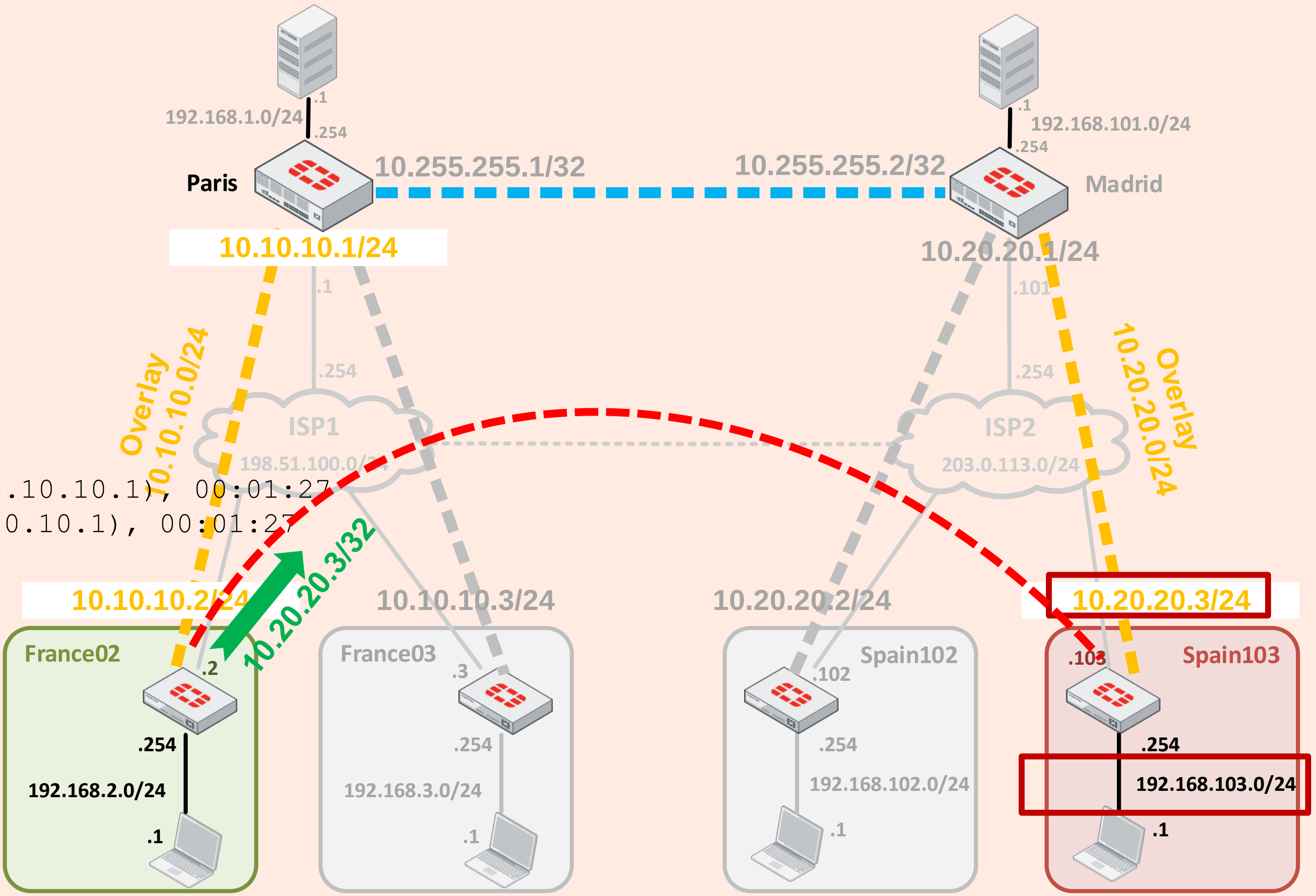
Dual Region - BGP Next Hop Reachability

"net-device enable" for shortcuts

Shortcut is established between France02 and Spain103

```
France02 # get router info routing-table all
Routing table for VRF=0
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       (...)
       * - candidate default

S*      0.0.0.0/0 [10/0] via 198.51.100.254, wan

C       10.10.10.0/24 is directly connected, advpn
C       10.10.10.2/32 is directly connected, advpn
                      is directly connected, advpn_0
S       10.20.20.0/24 [10/0] via 10.10.10.1, advpn
C       10.20.20.3/32 is directly connected, advpn_0
S       10.255.255.0/30 [10/0] via 10.10.10.1, advpn

B       192.168.1.0/24 [200/0] via 10.10.10.1, advpn, 00:01:27
C       192.168.2.0/24 is directly connected, internal
B       192.168.3.0/24 [200/0] via 10.10.10.3, advpn, 00:01:27
B       192.168.101.0/24 [200/0] via 10.255.255.2 (recursive via 10.10.10.1), 00:01:27
B       192.168.102.0/24 [200/0] via 10.20.20.2 (recursive via 10.10.10.1), 00:01:27
B       192.168.103.0/24 [200/0] via 10.20.20.3, advpn_0, 00:00:22

C       198.51.100.0/24 is directly connected, wan
```

Added by IKE



France02↔Spain103 traffic flows through the shortcut

ADVPN troubleshooting

IPsec & Routing

Troubleshooting

IPsec

Troubleshooting – IPsec

```
France02 # diag ip address  list | grep advpn
IP=10.10.10.2->10.10.10.1/255.255.255.0 index=15 devname=advpn
```

overlay `local-ip` and `remote-ip`

Overlay IP address

Tunnel to Hub

Shortcut tunnel

```
France02 # get vpn ipsec tunnel summary
'advpn' 198.51.100.1:0  selectors(total,up): 1/1  rx(pkt,err): 1606/0  tx(pkt,err): 1539/0
'advpn_0' 198.51.100.3:0  selectors(total,up): 1/1  rx(pkt,err): 1136/0  tx(pkt,err): 1051/0


France02 # diag vpn ike status detailed
vd: root/0
name: advpn
version: 1
used-index: 0
connection: 2/6
IKE SA: created 2/6  established 2/5  times 0/1858/9010 ms
IPsec SA: created 2/7  established 2/6  times 0/13/40 ms
```

Tunnels summary

Troubleshooting – IPsec

Initial State = no shortcut yet

```
[root:~]# ping 192.168.3.1
PING 192.168.3.1 (192.168.3.1): 56 data bytes
64 bytes from 192.168.3.1: icmp_seq=0 ttl=252 time=1.1 ms
64 bytes from 192.168.3.1: icmp_seq=1 ttl=253 time=0.6 ms
64 bytes from 192.168.3.1: icmp_seq=2 ttl=253 time=0.5 ms
64 bytes from 192.168.3.1: icmp_seq=3 ttl=253 time=0.3 ms
64 bytes from 192.168.3.1: icmp_seq=4 ttl=253 time=0.4 ms

--- 192.168.3.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.5/1.1 ms
```

TTL change

Ping from France02 LAN to France03 LAN

```
France02 # get vpn ipsec tunnel summary
'advpn_0' 198.51.100.3:0  selectors(total,up): 1/1  rx(pkt,err): 6/0  tx(pkt,err): 6/0
'advpn' 198.51.100.1:0  selectors(total,up): 1/1  rx(pkt,err): 125/0  tx(pkt,err): 113/0
```

New

Shortcut to France03

```
[root:~]# ping 192.168.102.1
PING 192.168.102.1 (192.168.102.1): 56 data bytes
64 bytes from 192.168.102.1: icmp_seq=0 ttl=251 time=1.8 ms
64 bytes from 192.168.102.1: icmp_seq=1 ttl=253 time=0.7 ms
64 bytes from 192.168.102.1: icmp_seq=2 ttl=253 time=0.7 ms
64 bytes from 192.168.102.1: icmp_seq=3 ttl=253 time=0.8 ms
64 bytes from 192.168.102.1: icmp_seq=4 ttl=253 time=0.7 ms

--- 192.168.102.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.7/0.9/1.8 ms
```

TTL change

Ping from France02 LAN to Spain102 LAN

```
France02 # get vpn ipsec tunnel summary
'advpn_0' 198.51.100.3:0  selectors(total,up): 1/1  rx(pkt,err): 7/0  tx(pkt,err): 7/0
'advpn_1' 203.0.113.102:0  selectors(total,up): 1/1  rx(pkt,err): 5/0  tx(pkt,err): 5/0
'advpn' 198.51.100.1:0  selectors(total,up): 1/1  rx(pkt,err): 134/0  tx(pkt,err): 121/0
```

New

Shortcut to Spain102

Troubleshooting – IPsec

Bringing down a shortcut

```
France02 # get vpn ipsec tunnel summary
'advpn' 198.51.100.1:0  selectors(total,up): 1/1  rx(pkt,err): 1606/0  tx(pkt,err): 1539/0
'advpn_0' 198.51.100.3:0  selectors(total,up): 1/1  rx(pkt,err): 1136/0  tx(pkt,err): 1051/0

France02 # diag vpn ike gateway flush name advpn_0

France02 # get vpn ipsec tunnel summary
'advpn' 198.51.100.1:0  selectors(total,up): 1/1  rx(pkt,err): 1606/0  tx(pkt,err): 1539/0
```

Shortcuts cannot be flushed via the GUI

Troubleshooting – IPsec

List of all IKE SA (“phase1 up”)

```
France02 # diag vpn ike gateway list

vd: root/0
name: advpn
version: 1
interface: port2 4
addr: 198.51.100.2:500 -> 198.51.100.1:500
virtual-interface-addr: 10.10.10.2 -> 10.10.10.1
created: 71630s ago
auto-discovery: 2 receiver
IKE SA: created 1/1  established 1/1  time 9010/9010/9010 ms
IPsec SA: created 1/2  established 1/2  time 0/10/20 ms

  id/spi: 1 bdd67d1022a0408e/4fba5ba5ee388f62
  direction: initiator
  status: established 71630-71621s ago = 9010ms
  proposal: aes128-sha1
  key: da232c99ba37b1a7-d9d1b33065f6594f
  lifetime/rekey: 86400/14478
  DPD sent/recv: 00000001/00000004

(... Continuation in next slide ...)
```

Tunnel towards the Hub (10.10.10.1)

Troubleshooting – IPsec

List of all IKE SA (“phase1 up”)

```
France02 # diag vpn ike gateway list

(...  Continuation from previous slide ...)

vd: root/0
name: advpn_0
version: 1
interface: port2 4
addr: 198.51.100.2:500 -> 198.51.100.3:500
virtual-interface-addr: 10.10.10.2 -> 10.10.10.3
created: 2535s ago
auto-discovery: 2 receiver
IKE SA: created 1/1  established 1/1  time 10/10/10 ms
IPsec SA: created 1/1  established 1/1  time 0/0/0 ms

  id/spi: 5 6ad21160f21d3a42/f1e5376a7a798d78
  direction: initiator
  status: established 2535-2535s ago = 10ms
  proposal: aes128-sha1
  key: db059962e3c581e5-da2462527694dcde
  lifetime/rekey: 86400/83564
  DPD sent/recv: 00000000/00000000
```

Shortcut tunnel towards France03 (10.10.10.3)

Troubleshooting – IPsec

List of all IPsec SA (“phase2/tunnel up”)

```
France02 # diag vpn tunnel list
list all ipsec tunnel in vd 0
------------------------------------------------------
name=advpn ver=1 serial=1 198.51.100.2:0->198.51.100.1:0 dst_mtu=1500
bound_if=4 lgwy=static/1 tun=intf/0 mode=auto/1 encap=none/544 options[0220]=search-nexthop frag-rfc  run_state=0 accept_traffic=1

proxyid_num=1 child_num=1 refcnt=18 ilast=2 olast=2 ad=r/2
stat: rxp=198 txp=226 rxb=25744 txb=15412
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=1
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=advpn proto=0 sa=1 ref=2 serial=1 adr
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA:  ref=3 options=32202 type=00 soft=0 mtu=1438 expire=42212/0B replaywin=2048
       seqno=d5 esn=0 replaywin_lastseq=000000b9 itn=0 qat=0
  life: type=01 bytes=0/0 timeout=42903/43200
  dec: spi=9373017c esp=aes key=16 2041c61a6ca346ee46829edffbd5f4c9
       ah=sha1 key=20 895da8e9f1d63e4aea5df5db78fdb62eb93b9473
  enc: spi=9b5f61d6 esp=aes key=16 3ac31ca155083a66dfecd4d9abac2df6
       ah=sha1 key=20 aca591a29dae6d104f87a81a9effa8b9e593b55f
  dec:pkts/bytes=184/11347, enc:pkts/bytes=212/28416
run_tally=2
ipv4 route tree:
10.10.10.3 0
198.51.100.3 0
------------------------------------------------------

(... Continuation in next slide ...)
```

Tunnel towards the Hub
(198.51.100.1)

Troubleshooting – IPsec

List of all IPsec SA (“phase2/tunnel up”)

```
France02 # diag vpn tunnel list

(...  Continuation from previous slide ...)

-------------------------------------------------------
name=advpn_0 ver=1 serial=4 198.51.100.2:0->198.51.100.3:0 dst_mtu=1500
bound_if=4 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/672 options[02a0]=search-nexthop rgwy-chg frag-rfc  run_state=1
accept_traffic=1

 parent=advpn index=0
proxyid_num=1 child_num=0 refcnt=5 ilast=10 olast=531 ad=r/2
stat: rxp=14 txp=14 rxb=2128 txb=1176
dpd: mode=on-demand on=1 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
proxyid=advpn proto=0 sa=1 ref=2 serial=1 adr
  src: 0:0.0.0.0/0.0.0.0:0
  dst: 0:0.0.0.0/0.0.0.0:0
  SA:  ref=3 options=32202 type=00 soft=0 mtu=1438 expire=42366/0B replaywin=2048
       seqno=f esn=0 replaywin_lastseq=0000000f itn=0 qat=0
  life: type=01 bytes=0/0 timeout=42900/43200
  dec: spi=9373017d esp=aes key=16 8aa4b75b3c8e1ad94ba4878b1548cb5c
       ah=sha1 key=20 449af1d85bb99cd953633949488f70aa652a172d
  enc: spi=21a001a1 esp=aes key=16 6179d7db568e80f19763bd6d5ec57604
       ah=sha1 key=20 8ed691ed67476a350d81b182eeb27c1a95e98ba6
  dec:pkts/bytes=14/1176, enc:pkts/bytes=14/2128
```

Shortcut tunnel towards France03 (198.51.100.3)

Troubleshooting – IPsec

As of 6.0, multiple IP addresses can be specified to filter the IKE debug (**mdst-addr4**)
It simplifies the debugging of Spoke-to-Spoke shortcut negotiations:

```
# From Spoke-A, check the shortcut negotiation with Spoke-B (which initially passes through the Hub)
diag debug console timestamp enable
diag vpn ike log filter clear
diag vpn ike log filter mdst-addr4 <ip.of.Hub> <ip.of.Spoke-B>
diag debug application ike -1
diag debug enable
```

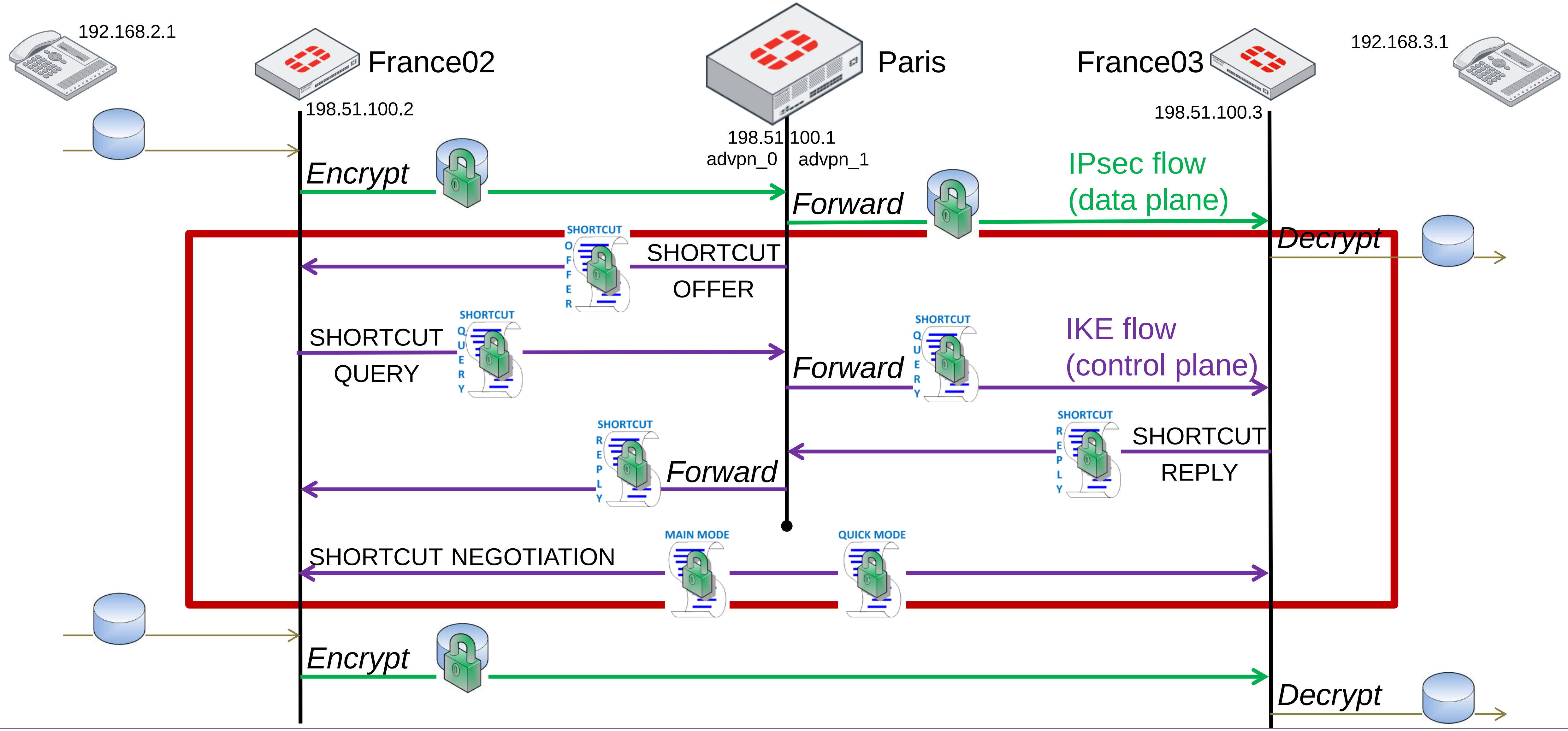
IKE debug

Up to 5.6, a single IP address can be specified to filter the IKE debug (dst-addr4)
Spoke-to-Spoke shortcut negotiations must therefore be investigated in two phases:
- 1st phase: investigate the Spoke-to-Hub negotiation which takes place at the beginning of the shortcut setup
- 2nd phase: investigate the Spoke-to-Spoke negotiation during another failing shortcut setup

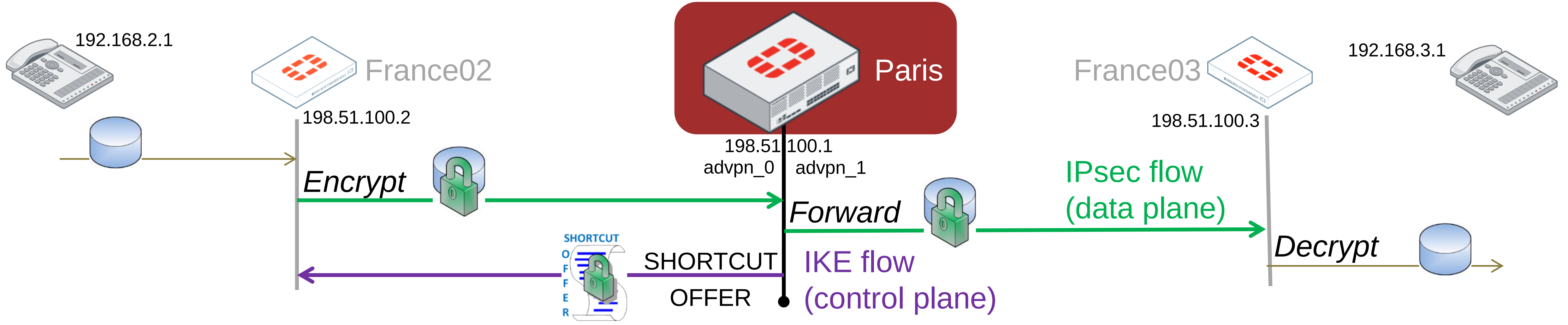
```
diag debug console timestamp enable
diag vpn ike log filter clear
diag vpn ike log filter dst-addr4 <ip.of.Hub or ip.of.Spoke-B>
diag debug application ike -1
diag debug enable
```

IKE debug

Troubleshooting – IKE debugs for shortcut negotiation



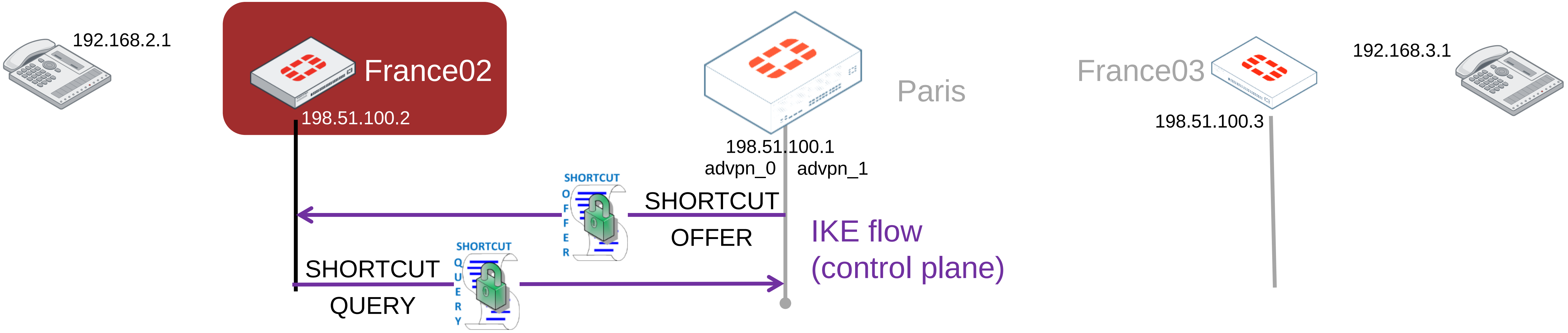
Troubleshooting – IKE debugs for shortcut negotiation



# IKE process is notified by IPsec kernel that data traffic from 192.168.2.1 to 192.168.3.1 was forwarded from advpn_0 to advpn_1
ike 0: shortcut **advpn_0**:198.51.100.2:0 **to advpn_1**:198.51.100.3:0 for 192.168.2.1->192.168.3.1

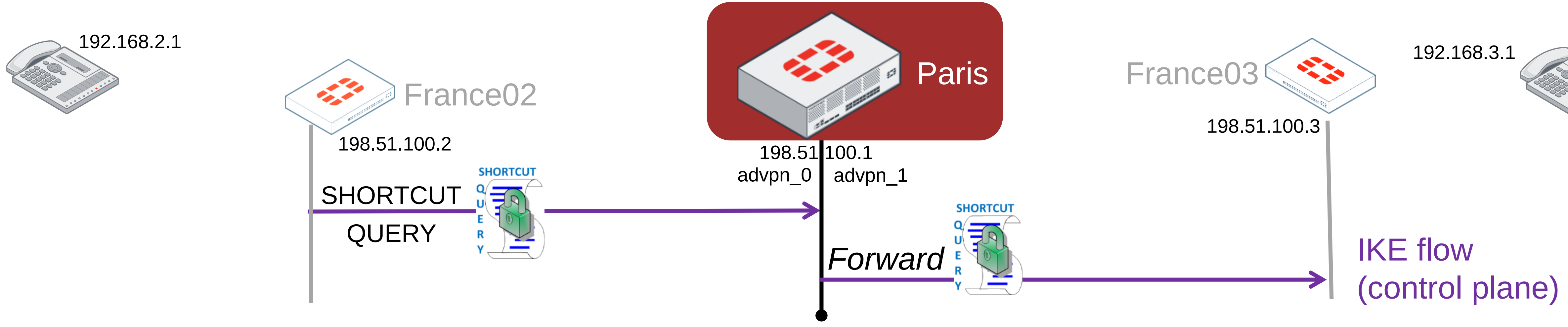
# IKE process sends a shortcut-offer to France02 (advpn_0)
ike 0:advpn_0:1: **sent** IKE msg (**SHORTCUT-OFFER**): 198.51.100.1:500->198.51.100.2:500, len=188, id=67a5828ff8216c8d/37b349b57406cb19:e8f7caf4

Troubleshooting – IKE debugs for shortcut negotiation



```
# IKE receives a shortcut-offer, accepts it and replies with a shortcut-query

ike 0: comes 198.51.100.1:500->198.51.100.2:500,ifindex=4....
ike 0: IKEv1 exchange=Informational id=67a5828ff8216c8d/37b349b57406cb19:e8f7caf4 len=188
ike 0:advpn:12: notify msg received: SHORTCUT-OFFER
ike 0:advpn: shortcut-offer 192.168.2.1->192.168.3.1 psk 64 ppk 0 ver 1 mode 0

ike 0 looking up shortcut by addr 192.168.3.1, name advpn

ike 0:advpn: send shortcut-query 3402812622499100305 cd1adf65f3afde0d/0000000000000000 198.51.100.2 192.168.2.1->192.168.3.1 psk 64 ttl 32 nat 0 ver 1 mode 0
ike 0:advpn:12: sent IKE msg (SHORTCUT-QUERY): 198.51.100.2:500->198.51.100.1:500, len=220, id=67a5828ff8216c8d/37b349b57406cb19:6d47b15b
```

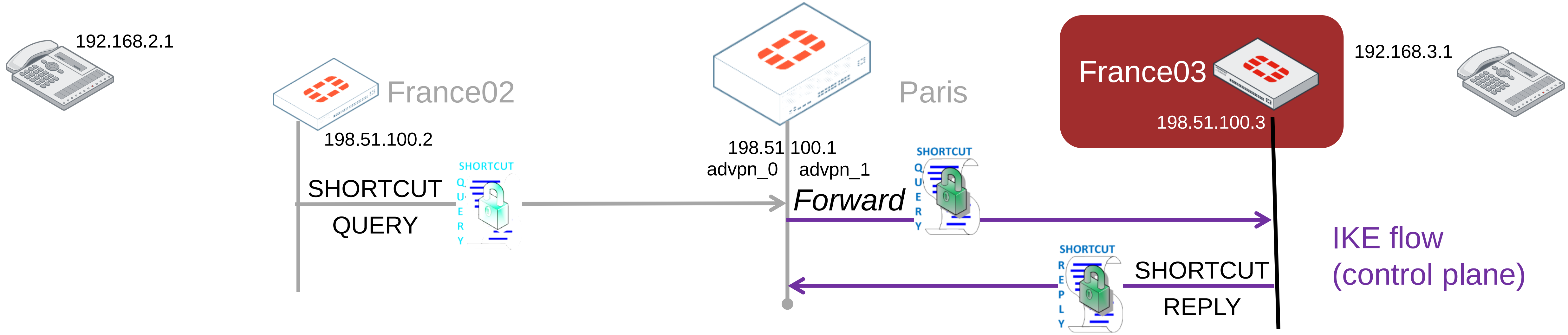
Troubleshooting – IKE debugs for shortcut negotiation



# IKE receives a shortcut-query related to data traffic (192.168.2.1→192.168.3.1)
# A routing lookup is done for 192.168.3.1 in order to find the tunnel into which the shortcut-query must be forwarded
# shortcut-query is forwarded to advpn_1 (France03)

```
ike 0: comes 198.51.100.2:500->198.51.100.1:500,ifindex=4....
ike 0: IKEv1 exchange=Informational id=67a5828ff8216c8d/37b349b57406cb19:6d47b15b len=220
ike 0:advpn_0:1: notify msg received: SHORTCUT-QUERY
ike 0:advpn_0: recv shortcut-query 3402812622499100305 cd1adf65f3afde0d/0000000000000000 198.51.100.2 192.168.2.1->192.168.3.1 psk 64 ppk 0 ttl 32 nat 0 ver 1 mode 0

ike 0:advpn: iif 15 192.168.2.1->192.168.3.1 route lookup oif 15

ike 0:advpn_1: forward shortcut-query 3402812622499100305 cd1adf65f3afde0d/0000000000000000 198.51.100.2 192.168.2.1->192.168.3.1 psk 64 ppk 0 ttl 31 ver 1 mode 0
ike 0:advpn_1:2: sent IKE msg (SHORTCUT-QUERY): 198.51.100.1:500->198.51.100.3:500, len=220, id=dca96501f2b0dec0/14d8345a3ddf87e5:391b1f83
```

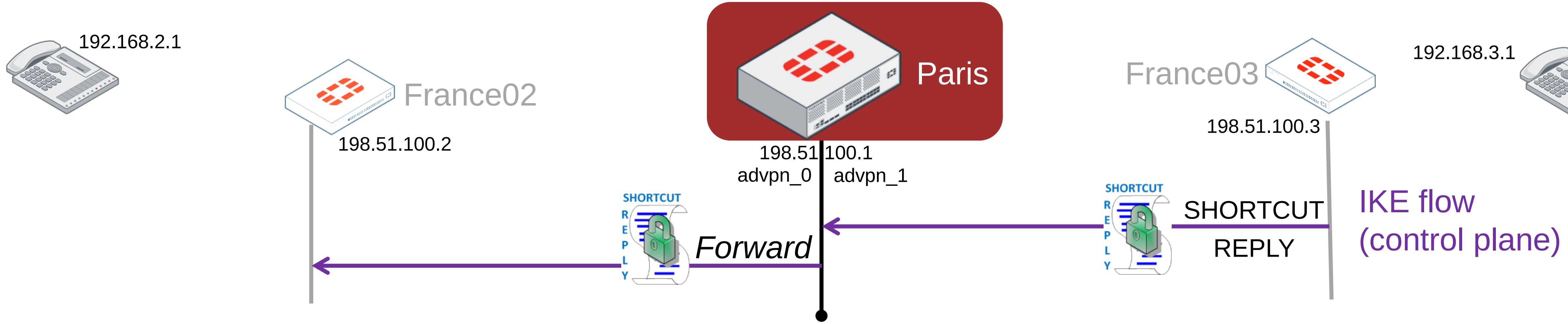
Troubleshooting – IKE debugs for shortcut negotiation



# IKE receives a shortcut-query, accepts it and replies with a shortcut-reply

```
ike 0: comes 198.51.100.1:500->198.51.100.3:500,ifindex=4....
ike 0: IKEv1 exchange=Informational id=dca96501f2b0dec0/14d8345a3ddf87e5:391b1f83 len=220
ike 0:advpn:13: notify msg received: SHORTCUT-QUERY
ike 0:advpn: recv shortcut-query 3402812622499100305 cd1adf65f3afde0d/0000000000000000 198.51.100.2 192.168.2.1->192.168.3.1 psk 64 ppk 0 ttl 31 nat 0 ver 1 mode 0

ike 0:advpn: iif 15 192.168.2.1->192.168.3.1 route lookup oif 3

ike 0:advpn: send shortcut-reply 3402812622499100305 cd1adf65f3afde0d/d525765a5a0840ba 198.51.100.3 to 192.168.2.1 psk 64 ppk 0 ver 1 mode 0
ike 0:advpn:13: sent IKE msg (SHORTCUT-REPLY): 198.51.100.3:500->198.51.100.1:500, len=220, id=dca96501f2b0dec0/14d8345a3ddf87e5:12037459
```

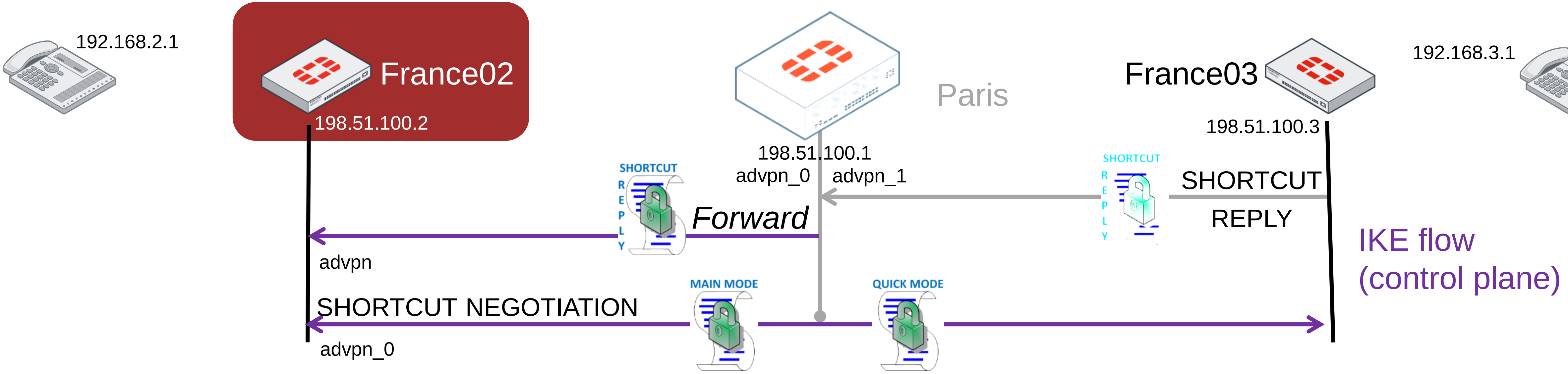
Troubleshooting – IKE debugs for shortcut negotiation



# IKE receives a shortcut-reply related to data traffic (192.168.3.1→192.168.2.1)
# A routing lookup is done for 192.168.2.1 in order to find the tunnel into which the shortcut-reply must be forwarded
# shortcut-reply is forwarded to advpn_0 (France02)

```
ike 0: comes 198.51.100.3:500->198.51.100.1:500,ifindex=4....
ike 0: IKEv1 exchange=Informational id=dca96501f2b0dec0/14d8345a3ddf87e5:12037459 len=220
ike 0:advpn_1:2: notify msg received: SHORTCUT-REPLY
ike 0:advpn_1: recv shortcut-reply 3402812622499100305 cd1adf65f3afde0d/d525765a5a0840ba 198.51.100.3 to 192.168.2.1 psk 64 ppk 0 ver 1 mode 0

ike 0:advpn: iif 15 192.168.3.1->192.168.2.1 route lookup oif 15

ike 0:advpn_0: forward shortcut-reply 3402812622499100305 cd1adf65f3afde0d/d525765a5a0840ba 198.51.100.3 to 192.168.2.1 psk 64 ppk 0 ttl 31 ver 1 mode 0
ike 0:advpn_0:1: sent IKE msg (SHORTCUT-REPLY): 198.51.100.1:500->198.51.100.2:500, len=220, id=67a5828ff8216c8d/37b349b57406cb19:ead55273
```

Troubleshooting – IKE debugs for shortcut negotiation



# IKE receives a shortcut-reply and initiates a tunnel (shortcut) negotiation with 198.51.100.3 (France03)

```
ike 0: comes 198.51.100.1:500->198.51.100.2:500,ifindex=4....
ike 0: IKEv1 exchange=Informational id=67a5828ff8216c8d/37b349b57406cb19:ead55273 len=220
ike 0:advpn:12: notify msg received: SHORTCUT-REPLY
ike 0:advpn: recv shortcut-reply 3402812622499100305 cd1adf65f3afde0d/d525765a5a0840ba 198.51.100.3 to 192.168.2.1 psk 64 ppk 0 ver 1 mode 0
ike 0:advpn: iif 15 192.168.3.1->192.168.2.1 route lookup oif 3
ike 0:advpn: created connection: 0xd29ba30 4 198.51.100.2->198.51.100.3:500.
ike 0:advpn: adding new dynamic tunnel for 198.51.100.3:500
ike 0:advpn_0: added new dynamic tunnel for 198.51.100.3:500
ike 0:advpn_0:13: initiator: main mode is sending 1st message...
ike 0:advpn_0:13: cookie cd1adf65f3afde0d/d525765a5a0840ba
ike 0:advpn_0:13: sent IKE msg (ident_i1send): 198.51.100.2:500->198.51.100.3:500, len=372, id=cd1adf65f3afde0d/d525765a5a0840ba
```

Troubleshooting

Routing

Troubleshooting – BGP Routing

```
France02 # get router info bgp summary
BGP router identifier 10.10.10.2, local AS number 65000
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.1      4      65000   10009   10007        1    0    0 04:02:20        5

Total number of neighbors 1
```

BGP peers

```
France02 # get router info bgp network
BGP table version is 2, local router ID is 10.10.10.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight RouteTag Path
*>i192.168.1.0      10.10.10.1               0    100      0        0 i <-/1>
*> 192.168.2.0      0.0.0.0                       100  32768        0 i <-/1>
*>i192.168.3.0      10.10.10.3               0    100      0        0 i <-/1>
*>i192.168.101.0    10.255.255.2             0    100      0        0 65100 i <-/1>
*>i192.168.102.0    10.20.20.2               0    100      0        0 65100 i <-/1>
*>i192.168.103.0    10.20.20.3               0    100      0        0 65100 i <-/1>

Total number of prefixes 6
```

BGP table

Troubleshooting – BGP Routing

```
France02 # get router info bgp network 192.168.102.0
BGP routing table entry for 192.168.102.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Not advertised to any peer
  65100
    10.20.20.2 from 10.10.10.1 (10.10.10.1)
      Origin IGP metric 0, localpref 100, valid, internal, best
      Last update: Wed Aug 28 10:59:58 2019
```

BGP details of a specific prefix

```
France02 # get router info routing-table bgp
Routing table for VRF=0
B       192.168.1.0/24 [200/0] via 10.10.10.1, advpn, 04:05:36
B       192.168.3.0/24 [200/0] via 10.10.10.3, advpn, 04:04:45
B       192.168.101.0/24 [200/0] via 10.255.255.2 (recursive via 10.10.10.1), 04:05:36
B       192.168.102.0/24 [200/0] via 10.20.20.2 (recursive via 10.10.10.1), 04:03:56
B       192.168.103.0/24 [200/0] via 10.20.20.3 (recursive via 10.10.10.1), 04:03:56
```

BGP routes in the RIB

```
France02 # get router info routing-table static
Routing table for VRF=0
S*      0.0.0.0/0 [10/0] via 198.51.100.254, wan
S       10.20.20.0/24 [10/0] via 10.10.10.1, advpn
S       10.255.255.0/30 [10/0] via 10.10.10.1, advpn
```

Static routes in the RIB

```
France02 # get router info routing-table connected
Routing table for VRF=0
C       10.10.10.0/24 is directly connected, advpn
C       10.10.10.2/32 is directly connected, advpn
C       192.168.2.0/24 is directly connected, internal
C       198.51.100.0/24 is directly connected, wan
```

Connected routes in the RIB

Troubleshooting – BGP Routing

```
France02 # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*       0.0.0.0/0 [10/0] via 198.51.100.254, wan
C        10.10.10.0/24 is directly connected, advpn
C        10.10.10.2/32 is directly connected, advpn
S        10.20.20.0/24 [10/0] via 10.10.10.1, advpn
S        10.255.255.0/30 [10/0] via 10.10.10.1, advpn
B        192.168.1.0/24 [200/0] via 10.10.10.1, advpn, 04:10:56
C        192.168.2.0/24 is directly connected, internal
B        192.168.3.0/24 [200/0] via 10.10.10.3, advpn, 04:10:05
B        192.168.101.0/24 [200/0] via 10.255.255.2 (recursive via 10.10.10.1), 04:10:56
B        192.168.102.0/24 [200/0] via 10.20.20.2 (recursive via 10.10.10.1), 04:09:16
B        192.168.103.0/24 [200/0] via 10.20.20.3 (recursive via 10.10.10.1), 04:09:16
C        198.51.100.0/24 is directly connected, wan
```

All active routes in the RIB

```
France02 # get router info routing-table details 192.168.102.1
Routing table for VRF=0
Routing entry for 192.168.102.0/24
  Known via "bgp", distance 200, metric 0, best
  Last update 04:10:52 ago
  * 10.20.20.2 (recursive via 10.10.10.1)
```

Details of a specific route in the RIB

Troubleshooting – BGP Routing

```
[root:~]# ping 192.168.3.1
[root:~]# ping 192.168.102.1
[root:~]# ping 192.168.103.1
```

Bring up shortcuts to France03, Spain102 & Spain103

```
France02 (root) # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

S*        0.0.0.0/0 [10/0] via 198.51.100.254, wan

C         10.10.10.0/24 is directly connected, advpn
C         10.10.10.2/32 is directly connected, advpn
S         10.20.20.0/24 [10/0] via 10.10.10.1, advpn

S         10.20.20.2/32 [15/0] via 10.20.20.2, advpn
S         10.20.20.3/32 [15/0] via 10.20.20.3, advpn

S         10.255.255.0/30 [10/0] via 10.10.10.1, advpn

B         192.168.1.0/24 [200/0] via 10.10.10.1, advpn, 00:01:17
C         192.168.2.0/24 is directly connected, port1
B         192.168.3.0/24 [200/0] via 10.10.10.3, advpn, 00:01:00
B         192.168.101.0/24 [200/0] via 10.255.255.2 (recursive via 10.10.10.1), 00:01:17
B         192.168.102.0/24 [200/0] via 10.20.20.2 (recursive via 10.20.20.2), 00:01:17
B         192.168.103.0/24 [200/0] via 10.20.20.3 (recursive via 10.20.20.3), 00:01:17

C         198.51.100.0/24 is directly connected, internal
```

BGP next-hop of shortcuts established with Spain region
(automatically added by IKE)

Routes via the shortcuts

Troubleshooting – BGP Routing

```
France02 # diag sniffer packet any 'tcp port 179' 6 0 l
```

Capture BGP traffic

```
diag debug reset
diag debug console timestamp enable
diag ip router bgp all enable
diag ip router bgp level info
diag debug enable
```

Start BGP debugs

```
diag ip router bgp all disable
diag debug disable
```

Stop BGP debugs

```
exec router clear bgp ip <peer-ip>
```

Reset BGP peering

```
exec router clear bgp ip <peer-ip> soft
exec router clear bgp ip <peer-ip> soft in
exec router clear bgp ip <peer-ip> soft out
```

Route Refresh

Troubleshooting – OSPF Routing

```
France02 # get router info ospf neighbor

OSPF process 0, VRF 0:
Neighbor ID      Pri   State           Dead Time   Address         Interface

10.10.10.1         1   Full/ -         00:00:31    10.10.10.1      advpn

10.10.10.3         1   Full/ -         00:00:34    10.10.10.3      advpn
10.10.10.4         1   Full/ -         00:00:35    10.10.10.4      advpn
```

Hub

shortcuts

Point-to-multipoint

OSPF neighbors

```
France02 # get router info ospf database brief

            OSPF Router with ID (10.10.10.2) (Process ID 0, VRF 0)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#      CkSum Flag Link count
10.10.10.1      10.10.10.1      794  80000048 7083  0002 6
10.10.10.2      10.10.10.2      21   80000034 d256  0021 5
10.10.10.3      10.10.10.3      443  80000022 7aba  0002 5
10.10.10.4      10.10.10.4      22   8000000f 182a  0002 5
10.10.10.5      10.10.10.5      970  8000000d 9613  0002 3
```

OSPF LSDB summary

Troubleshooting – OSPF Routing

```
France02 # get router info ospf status
 Routing Process "ospf 0" with ID 10.10.10.2
 Process uptime is 1 hour 3 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Do not support Restarting
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Refresh timer 10 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 1
 Number of LSA received 85
 Number of areas attached to this router: 1
    Area 0.0.0.0 (BACKBONE)
        Number of interfaces in this area is 2(2)
        Number of fully adjacent neighbors in this area is 3
        Area has no authentication
        SPF algorithm last executed 00:12:39.320 ago
        SPF algorithm executed 45 times
        Number of LSA 5. Checksum 0x026bd0
```

OSPF status

Troubleshooting – OSPF Routing

```
France02 # get router info ospf interface advpn
advpn is up, line protocol is up
  Internet Address 10.10.10.2/24, Area 0.0.0.0, MTU 1438
  Process ID 0, VRF 0, Router ID 10.10.10.2, Network Type POINTOMULTIPOINT, Cost: 100
  Transmit Delay is 1 sec, State Point-To-Point
  Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Neighbor Count is 3, Adjacent neighbor count is 3
  Crypt Sequence Number is 9
  Hello received 559 sent 362, DD received 112 sent 139
  LS-Req received 24 sent 25, LS-Upd received 159 sent 72
  LS-Ack received 10 sent 81, Discarded 162
```

OSPF interface details

```
France02 # get router info ospf neighbor 10.10.10.1
OSPF process 0, VRF 0:
 Neighbor 10.10.10.1, interface address 10.10.10.1
    In the area 0.0.0.0 via interface advpn
    Neighbor priority is 1, State is Full, 5 state changes
    DR is 0.0.0.0, BDR is 0.0.0.0
    Options is 0x42 (*|O|-|-|-|-|E|-)
    Dead timer due in 00:00:37
    Neighbor is up for 00:45:08
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0
    Crypt Sequence Number is 0
    Thread Inactivity Timer on
    Thread Database Description Retransmission off
    Thread Link State Request Retransmission off
    Thread Link State Update Retransmission off
```

Neighbor details

Troubleshooting – OSPF Routing

```
France02 # get router info ospf route

OSPF process 0:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

C  10.10.10.0/24 [100] is directly connected, advpn, Area 0.0.0.0
O  10.10.10.1/32 [100] via 10.10.10.1, advpn, Area 0.0.0.0
O  10.10.10.3/32 [100] via 10.10.10.3, advpn, Area 0.0.0.0
O  10.10.10.4/32 [100] via 10.10.10.4, advpn, Area 0.0.0.0
O  10.10.10.5/32 [101] via 10.10.10.1, advpn, Area 0.0.0.0
O  192.168.1.0/24 [101] via 10.10.10.1, advpn, Area 0.0.0.0
C  192.168.2.0/24 [1] is directly connected, port1, Area 0.0.0.0
O  192.168.3.0/24 [101] via 10.10.10.3, advpn, Area 0.0.0.0
O  192.168.4.0/24 [101] via 10.10.10.4, advpn, Area 0.0.0.0
O  192.168.5.0/24 [102] via 10.10.10.1, advpn, Area 0.0.0.0
```

Routes announced & received via OSPF

```
France02 # get router info routing-table ospf

Routing table for VRF=0
O       192.168.1.0/24 [110/101] via 10.10.10.1, advpn, 00:33:09
O       192.168.3.0/24 [110/101] via 10.10.10.3, advpn, 00:33:19
O       192.168.4.0/24 [110/101] via 10.10.10.4, advpn, 00:20:20
O       192.168.5.0/24 [110/102] via 10.10.10.1, advpn, 00:33:09
```

OSPF routes in the RIB

Troubleshooting – OSPF Routing

```
France02 # diag sniffer packet any 'ip proto 89' 6 0 l
```

Capture OSPF traffic

```
diag debug reset
diag debug console timestamp enable
diag ip router ospf all enable
diag ip router ospf level info
diag debug enable
```

Start OSPF debugs

```
diag ip router ospf all disable
diag debug disable
```

Stop OSPF debugs

```
exec router clear ospf process
```

Restart OSPF

ADVPN Dual Region (BGP)

Configuration

Hub “*Paris*” [1/3]

Tunnels:

```
config vpn ipsec phase1-interface
    edit "advpn"
        set type dynamic
        set interface "port2"
        set proposal aes128-sha1
        set auto-discovery-sender enable
        set add-route disable
        set psksecret xxxxxxxx

        set net-device disable
        set tunnel-search nexthop

    next

    edit "toMadrid"
        set interface "port2"
        set proposal aes128-sha1
        set auto-discovery-forwarder enable
        set remote-gw 203.0.113.101
        set psksecret fortinet
    next
end
```

As of FortiOS 6.0 and 5.6.3

```
config vpn ipsec phase2-interface
    edit "advpn"
        set phase1name "advpn"
        set proposal aes128-sha1
    next
    edit "toMadrid"
        set phase1name "toMadrid"
        set proposal aes128-sha1
    next
end
```

Hub “*Paris*” [2/3]

Interfaces:

```
config system interface
    edit "port1"
        set ip 192.168.1.254 255.255.255.0
        set allowaccess ping https ssh
        set alias "LAN"
    next
    edit "port2"
        set ip 198.51.100.1 255.255.255.0
        set allowaccess ping https ssh
        set alias "INTERNET"
    next
    edit "toMadrid"
        set ip 10.255.255.1 255.255.255.255
        set remote-ip 10.255.255.2
        set remote-ip 10.255.255.2 255.255.255.255
        set allowaccess ping
    next

    edit "advpn"
        set ip 10.10.10.1 255.255.255.255

        set remote-ip 10.10.10.254
        set remote-ip 10.10.10.254 255.255.255.0

        set allowaccess ping
    next
end
```

For FortiOS 5.4
and 5.6.0/5.6.1/5.6.2

As of FortiOS 6.0 and 5.6.3

Policies:

```
config firewall policy
    edit 1
        set name "To Spokes"
        set srcintf "port1"
        set dstintf "advpn"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "From Spokes"
        set srcintf "advpn"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 3
        set name "Spokes to Spokes"
        set srcintf "advpn"
        set dstintf "advpn"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
```

Hub *“Paris”* [3/3]

Policies:

```
(cont.)
edit 4
        set name "To Madrid"
        set srcintf "port1" "advpn"
        set dstintf "toMadrid"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 5
        set name "From Madrid"
        set srcintf "toMadrid"
        set dstintf "advpn" "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

Routes:

```
config router static
    edit 1
        set gateway 198.51.100.254
        set device "port2"
    next
    edit 2
        set dst 10.20.20.0 255.255.255.0
        set device "toMadrid"
    next
end
```

BGP:

```
config router bgp
    set as 65000
    set router-id 10.10.10.1
    config neighbor
        edit "10.255.255.2"
            set attribute-unchanged next-hop
            set ebgp-enforce-multihop enable
            set remote-as 65100
        next
    end
    config neighbor-group
        edit "advn_peers"
            set remote-as 65000
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.10.10.0 255.255.255.0
            set neighbor-group "advn_peers"
        next
    end
    config network
        edit 1
            set prefix 192.168.1.0 255.255.255.0
        next
    end
end
```

Hub “*Madrid*” [1/3]

Tunnels:

```
config vpn ipsec phase1-interface
    edit "advpn"
        set type dynamic
        set interface "port2"
        set proposal aes128-sha1
        set auto-discovery-sender enable
        set add-route disable
        set psksecret xxxxxxxx

        set net-device disable
        set tunnel-search nexthop

    next

    edit "toParis"
        set interface "port2"
        set proposal aes128-sha1
        set auto-discovery-forwarder enable
        set remote-gw 198.51.100.1
        set psksecret xxxxxxxx
    next
end
```

As of FortiOS 6.0 and 5.6.3

```
config vpn ipsec phase2-interface
    edit "advpn"
        set phase1name "advpn"
        set proposal aes128-sha1
    next
    edit "toParis"
        set phase1name "toParis"
        set proposal aes128-sha1
    next
end
```

Hub “*Madrid*” [2/3]

Interfaces:

```
config system interface
    edit "port1"
        set ip 192.168.101.254 255.255.255.0
        set allowaccess ping https ssh
        set alias "LAN"
    next
    edit "port2"
        set ip 203.0.113.101 255.255.255.0
        set allowaccess ping https ssh
        set alias "INTERNET"
    next
    edit "toParis"
        set ip 10.255.255.2 255.255.255.255
        set allowaccess ping
        set remote-ip 10.255.255.1
        set remote-ip 10.255.255.1 255.255.255.255
    next

    edit "advpn"
        set ip 10.20.20.1 255.255.255.255

        set remote-ip 10.20.20.254
        set remote-ip 10.20.20.254 255.255.255.0

        set allowaccess ping
    next
end
```

For FortiOS 5.4
and 5.6.0/5.6.1/5.6.2

As of FortiOS 6.0 and 5.6.3

Policies:

```
config firewall policy
    edit 1
        set name "To Spokes"
        set srcintf "port1"
        set dstintf "advpn"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "From Spokes"
        set srcintf "advpn"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 3
        set name "Spokes to Spokes"
        set srcintf "advpn"
        set dstintf "advpn"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
```

Hub “*Madrid*” [3/3]

Policies:

```
(cont.)
 edit 4
        set name "To Paris"
        set srcintf "port1" "advpn"
        set dstintf "toParis"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 5
        set name "From Paris"
        set srcintf "toParis"
        set dstintf "advpn" "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

Routes:

```
config router static
    edit 1
        set gateway 203.0.113.254
        set device "port2"
    next
    edit 2
        set dst 10.10.10.0 255.255.255.0
        set device "toParis"
    next
end
```

BGP:

```
config router bgp
    set as 65100
    set router-id 10.20.20.1
    config neighbor
        edit "10.255.255.1"
            set attribute-unchanged next-hop
            set ebgp-enforce-multihop enable
            set remote-as 65000
        next
    end
    config neighbor-group
        edit "advn_peers"
            set remote-as 65100
            set route-reflector-client enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.20.20.0 255.255.255.0
            set neighbor-group "advn_peers"
        next
    end
    config network
        edit 1
            set prefix 192.168.101.0 255.255.255.0
        next
    end
end
```

Spoke “*France02*” [1/3]

Tunnel:

```
config vpn ipsec phase1-interface
    edit "advpn"
        set interface "port2"
        set proposal aes128-sha1
        set auto-discovery-receiver enable
        set add-route disable
        set net-device disable
        set tunnel-search nexthop
        set remote-gw 198.51.100.1
        set psksecret xxxxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "advpn"
        set phase1name "advpn"
        set proposal aes128-sha1
    next
end
```

As of FortiOS 6.2.1

Interfaces:

```
config system interface
    edit "port1"
        set ip 192.168.2.254 255.255.255.0
        set allowaccess ping https ssh
        set alias "LAN"
    next
    edit "port2"
        set ip 198.51.100.2 255.255.255.0
        set allowaccess ping https ssh
        set alias "INTERNET"
    next

    edit "advpn"
        set ip 10.10.10.2 255.255.255.255
        set remote-ip 10.10.10.1 255.255.255.0
        set allowaccess ping
    next
end
```

Spoke “*France02*” [2/3]

Overlay routes:

```
config router static
    edit 1
        set gateway 198.51.100.254
        set device "port2"
    next

    edit 2
        set dst 10.10.10.0 255.255.255.0
        set device "advpn"
        set comment "France overlay subnet"
    next

    edit 3
        set dst 10.20.20.0 255.255.255.0
        set device "advpn"
        set comment "Spain overlay subnet"
    next
    edit 4
        set dst 10.255.255.0 255.255.255.252
        set device "advpn"
        set comment "Paris-Madrid overlay subnet"
    next
end
```

Only required
for FortiOS 5.4
and 5.6.0/5.6.1/5.6.2

Spoke “*France02*” [3/3]

BGP:

```
config router bgp
    set as 65000
    set router-id 10.10.10.2
    config neighbor
        edit "10.10.10.1"
            set remote-as 65000
        next
    end
    config network
        edit 1
            set prefix 192.168.2.0 255.255.255.0
        next
    end
end
```

Policies:

```
config firewall policy
    edit 1
        set name "to ADVPN"
        set srcintf "port1"
        set dstintf "advpn"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "from ADVPN"
        set srcintf "advpn"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

Spoke “*Spain102*” [1/3]

Tunnel:

```
config vpn ipsec phase1-interface
    edit "advpn"
        set interface "port2"
        set proposal aes128-sha1
        set auto-discovery-receiver enable
        set add-route disable
        set net-device disable
        set tunnel-search nexthop
        set remote-gw 203.0.113.101
        set psksecret xxxxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "advpn"
        set phase1name "advpn"
        set proposal aes128-sha1
    next
end
```

As of FortiOS 6.2.1

Interfaces:

```
config system interface
    edit "port1"
        set ip 192.168.102.254 255.255.255.0
        set allowaccess ping https ssh
        set alias "LAN"
    next
    edit "port2"
        set ip 203.0.113.102 255.255.255.0
        set allowaccess ping https ssh
        set alias "INTERNET"
    next

    edit "advpn"
        set ip 10.20.20.2 255.255.255.255
        set remote-ip 10.20.20.1 255.255.255.0
        set allowaccess ping
    next
end
```

Spoke “*Spain102*” [2/3]

Overlay routes:

```
config router static
    edit 1
        set gateway 203.0.113.254
        set device "port2"
    next

    edit 2
        set dst 10.20.20.0 255.255.255.0
        set device "Madrid"
        set comment "Spain overlay subnet"
    next

    edit 3
        set dst 10.10.10.0 255.255.255.0
        set device "Madrid"
        set comment "France overlay subnet"
    next
    edit 4
        set dst 10.255.255.0 255.255.255.252
        set device "Madrid"
        set comment "Paris-Madrid overlay subnet"
    next
end
```

Only required
for FortiOS 5.4
and 5.6.0/5.6.1/5.6.2

Spoke “*Spain102*” [3/3]

BGP:

```
config router bgp
    set as 65100
    set router-id 10.20.20.2
    config neighbor
        edit "10.20.20.1"
            set remote-as 65100
        next
    end
    config network
        edit 1
            set prefix 192.168.102.0 255.255.255.0
        next
    end
end
```

Policies:

```
config firewall policy
    edit 1
        set name "to ADVPN"
        set srcintf "port1"
        set dstintf "advpn"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "from ADVPN"
        set srcintf "advpn"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

FORTINET®