New *route-based* IPsec logic ("set net-device disable")

Stéphane HAMELIN – Support Engineering Team

Change Log

Latest version of this document is available at:
https://kb.fortinet.com/kb/documentLink.do?externalID=FD41498

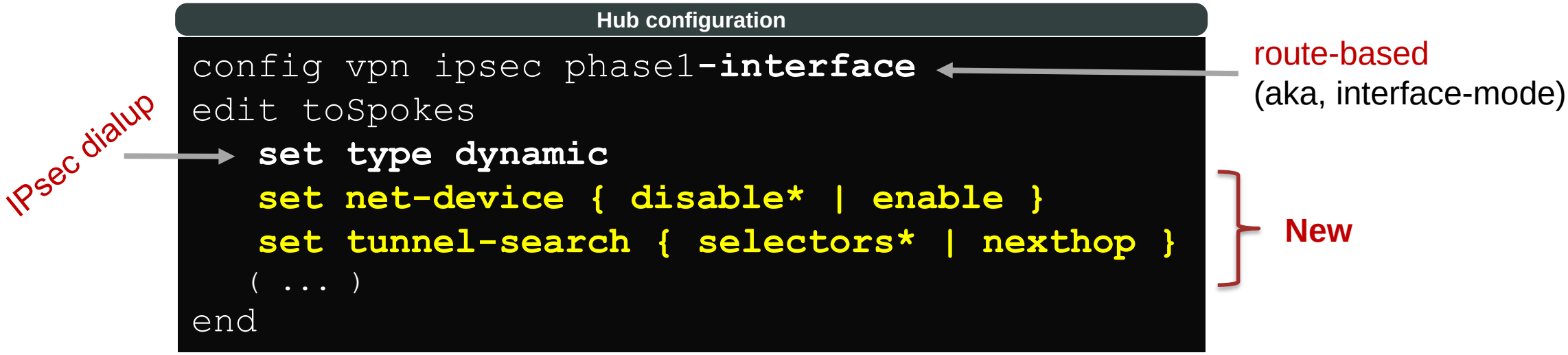
Date	Author	
2020-10-28	S. Hamelin	Added slide for the ip4 route tree Updated the "Upgrade" slide and added a "Restriction" slide As of FortiOS 6.4/6.2.2, tunnel overlay IPs can be provisioned with IKE mode-config As of FortiOS 6.4.3/6.2.6, the tunnel name maximum length is extended
2019-08-23	S. Hamelin	As of FortiOS 6.2.0, "net-device" also applies to static phase1 Document renamed from *"New IPsec dialup logic"* to *"New route-based IPsec logic"*
2019-04-08	S. Hamelin	NATed Spokes are supported with OSPF only as of FortiOS 6.2/6.0.5 IKE route overlap between dialup tunnels is not supported
2018-06-29	S. Hamelin	Initial version for Fortinet *NSE Xperts Academy* event

New *route-based* IPsec logic *('set net-device disable')*

Overview

IPsec dialup

- "`net-device`" for route-based IPsec **dialup** tunnels
  - » As of FortiOS 6.0 & 5.6.3 a new behavior is implemented for routing traffic to IPsec dialup tunnels
  - » This behavior is controlled by new CLI settings



IPsec static

- "`net-device`" for route-based IPsec **static** tunnels
  - » As of 6.2.0, it allows to define an IPsec tunnel has a member of an IPsec aggregate

https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/779544/ipsec-aggregate-to-achieve-redundancy-and-traffic-load-balancing

```
config vpn ipsec phase1-interface
edit <name>
    set type static
    set net-device disable
    set aggregate-member enable
    ( ... )
end
```

IPsec static

  - » As of 6.2.1, similar to dialup IPsec tunnels, it provides a new behavior for routing traffic to ADVPN shortcuts

https://kb.fortinet.com/kb/documentLink.do?externalID=FD39360

```
config vpn ipsec phase1-interface
edit toAdvpnHub
    set type static
    set net-device disable
    set tunnel-search { selectors* | nexthop }
    ( ... )
end
```

Historical IPsec dialup behavior

- A dialup tunnel is created for each successful dial-in negotiation

Hub IKE debug

```
ike 0:Spoke: adding new dynamic tunnel for 198.51.100.4:500
ike 0:Spoke_3: added new dynamic tunnel for 198.51.100.4:500
ike 0:Spoke_3:4: established IKE SA 5dbf5f1070224f9f/19b1a0df8498e2fe
```

- Tunnel name = *phase1Name_index*

FortiOS 5.6.2

```
Hub # diag vpn tunnel list name Spoke_3
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=Spoke_3 ver=1 serial=6 198.51.100.1:0->198.51.100.4:0
bound_if=4 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/0
 parent=Spoke index=3
(...)
```

Historical IPsec dialup behavior (cont.)

- A dynamic interface is created for each dialup tunnel

```
Hub # diag netlink interface list | grep "Spoke_"
if=Spoke_0 family=00 type=768 index=22 mtu=1438 link=16 master=0
if=Spoke_1 family=00 type=768 index=23 mtu=1438 link=16 master=0
if=Spoke_2 family=00 type=768 index=24 mtu=1438 link=16 master=0
if=Spoke_3 family=00 type=768 index=26 mtu=1438 link=16 master=0
```

- Networks accessible over dialup tunnels are bound to the corresponding tunnel interfaces

```
Hub # get router info routing-table bgp
B        192.168.2.0/24 [200/0] via 10.10.10.2, Spoke_0, 00:06:08
B        192.168.3.0/24 [200/0] via 10.10.10.3, Spoke_1, 00:06:05
B        192.168.4.0/24 [200/0] via 10.10.10.4, Spoke_3, 00:06:03
B        192.168.5.0/24 [200/0] via 10.10.10.5, Spoke_2, 00:06:04
```

Historical IPsec dialup behavior (cont.)

- Packets forwarded to dialup IPsec interface `Spoke_3` :

```
B        192.168.4.0/24 [200/0] via 10.10.10.4, Spoke_3, 00:06:03
```

  - When a cleartext packet is sent to `Spoke_3` **interface**, it is actually sent to the IPsec engine
  - The IPsec engine protects the cleartext packets with the IPsec Security Association of **tunnel** `Spoke_3`

Historical IPsec dialup behavior (cont.)

- Packets forwarded to dialup IPsec interface `Spoke_3` (cont.):

FortiOS 5.6.2

```
Hub # diag vpn tunnel list name Spoke_3
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=Spoke_3 ver=1 serial=6 198.51.100.1:0->198.51.100.4:0
bound_if=4 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/0
 parent=Spoke index=3
proxyid_num=1 child_num=0 refcnt=23 ilast=0 olast=0 ad=s/1 itn-status=66
stat: rxp=183 txp=201 rxb=23416 txb=12332
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=Spoke proto=0 sa=1 ref=2 serial=1 ads
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=a26 type=00 soft=0 mtu=1438 expire=42456/0B
replaywin=2048
       seqno=ca esn=0 replaywin_lastseq=000000b8 itn=0
  life: type=01 bytes=0/0 timeout=43190/43200
  dec: spi=a5a66993 esp=aes key=16 ec4c191fd5fc083891b57cfadc1d9516
       ah=sha1 key=20 2b190c304452b488c389a1c532f7e32ada965d25
  enc: spi=c686831a esp=aes key=16 bd6dc3872321d69154c73fdea0e21e09
       ah=sha1 key=20 c5944f9ff812e49d68c99ba2020ad12213553a93
  dec:pkts/bytes=183/11222, enc:pkts/bytes=201/25736
```

  - » Finally, an IPsec packet (ESP) is sent on the wire

New IPsec dialup behavior

- Default settings as of 6.0 & 5.6.3:

Hub configuration

```
config vpn ipsec phase1-interface
edit Spoke
    set type dynamic
    set net-device disable
    set tunnel-search selectors
   ( ... )
end
```

- Configuration required for dynamic routing over IPsec dialup:

```
config vpn ipsec phase1-interface
edit Spoke
    set tunnel-search nexthop
end
```

New IPsec dialup behavior (cont.)

- A dialup tunnel is created for each successful dial-in negotiation

Hub IKE debug

```
ike 0:Spoke: adding new dynamic tunnel for 198.51.100.4:500
ike 0:Spoke_3: added new dynamic tunnel for 198.51.100.4:500
ike 0:Spoke_3:6: established IKE SA 2514224dd6d96aa2/86d700f4961b14e8
```

- Tunnel name = *phase1Name_index*

FortiOS 5.6.4

```
Hub # diag vpn tunnel list name Spoke_3
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=Spoke_3 ver=1 serial=8 198.51.100.1:0->198.51.100.4:0
bound_if=4 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/320
options[0140]=search-nexthop rgwy_chg
 parent=Spoke index=3
(...)
```

New IPsec dialup behavior (cont.)

- No dynamic interface is created

```
Hub # diag netlink interface list | grep "Spoke_"

Hub #
```

  - » `net-device disable` means “do not create interfaces (i.e., network devices)”

- Networks accessible over dialup tunnels are all bound to the same shared (phase1) interface

```
Hub # get router info routing-table bgp
B        192.168.2.0/24 [200/0] via 10.10.10.2, Spoke, 01:04:49
B        192.168.3.0/24 [200/0] via 10.10.10.3, Spoke, 01:04:47
B        192.168.4.0/24 [200/0] via 10.10.10.4, Spoke, 00:35:01
B        192.168.5.0/24 [200/0] via 10.10.10.5, Spoke, 01:04:51
```

New IPsec dialup behavior (cont.)

- Packets forwarded to shared interface `Spoke`

```
B       192.168.4.0/24 [200/0] via 10.10.10.4, Spoke, 00:35:01
```

  - » When a cleartext packet is sent to `Spoke`, it is sent to the IPsec engine
  - » The IPsec engine must find out which tunnel's IPsec Security Association is to be used for protecting this packet
  - » The search logic is controlled by this setting:

```
config vpn ipsec phase1-interface
edit Spoke
    set type dynamic
    set net-device disable
    set tunnel-search { selectors* | nexthop }
   ( ... )
end
```

New IPsec dialup behavior (cont.)

`set tunnel-search selectors`

- This the default setting
- To be used when IPsec routes are learned from the Traffic Selectors of the IPsec SA negotiation
- These routes are called IKE routes `(diag vpn ike route list)`
- This IPsec routing mechanism is also referred as reverse-route injection (*RRI*)

`set tunnel-search nexthop`

- To be used when IPsec routes are learned from a dynamic routing protocol

New IPsec dialup behavior (cont.)

- Packets forwarded to shared interface `Spoke` (cont.):
  - » The IPsec engine checks the search method associated to `Spoke`

```
Hub # diag vpn tunnel list name Spoke
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=Spoke ver=1 serial=1 198.51.100.1:0->0.0.0.0:0
bound_if=4 lgwy=static/1 tun=intf/0 mode=dialup/2 encap=none/64 options[0040]=search-nexthop
proxyid_num=0 child_num=4 refcnt=26 ilast=4159 olast=4159 ad=/0 itn-status=7b
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=4
ipv4 route tree:
10.10.10.2 2
10.10.10.3 0
10.10.10.4 3
10.10.10.5 1
198.51.100.2 2
198.51.100.3 0
198.51.100.4 3
198.51.100.5 1
```

New IPsec dialup behavior (cont.)

- Packets forwarded to shared interface `Spoke` (cont.):
  - » Then it searches the tunnel index associated to next-hop `10.10.10.4`

```
Hub # diag vpn tunnel list name Spoke
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=Spoke ver=1 serial=1 198.51.100.1:0->0.0.0.0:0
bound_if=4 lgwy=static/1 tun=intf/0 mode=dialup/2 encap=none/64 options[0040]=search-nexthop
proxyid_num=0 child_num=4 refcnt=26 ilast=4159 olast=4159 ad=/0 itn-status=7b
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=4
ipv4 route tree:
10.10.10.2 2
10.10.10.3 0
10.10.10.4 3
10.10.10.5 1
198.51.100.2 2
198.51.100.3 0
198.51.100.4 3
198.51.100.5 1
```

Next-Hop

tunnel index → **Spoke_3**

New IPsec dialup behavior (cont.)

- Packets forwarded to shared interface `Spoke` (cont.):
  - » the cleartext packet is protected with the IPsec SA of tunnel `Spoke_3`

FortiOS 5.6.4

```
Hub # diag vpn tunnel list name Spoke_3
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=Spoke_3 ver=1 serial=8 198.51.100.1:0->198.51.100.4:0
bound_if=4 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/320 options[0140]=search-nexthop rgwy_chg
 parent=Spoke index=3
proxyid_num=1 child_num=0 refcnt=9 ilast=4 olast=4 ad=s/1 itn-status=7b
stat: rxp=5049 txp=5047 rxb=766344 txb=423108
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=Spoke proto=0 sa=1 ref=2 serial=1 ads
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:0.0.0.0-255.255.255.255:0
  SA:  ref=3 options=a26 type=00 soft=0 mtu=1438 expire=43021/0B replaywin=2048
       seqno=13b8 esn=0 replaywin_lastseq=000013ba itn=0
  life: type=01 bytes=0/0 timeout=43189/43200
  dec: spi=b37926ce esp=aes key=16 63bc7bacf80a7b2c1b1494b0987281b3
       ah=sha1 key=20 3219e7b18950c93d3dc4a933141e963a8387dfec
  enc: spi=aceb1971 esp=aes key=16 850e90ebfa7a3f0b6376128c8433e1d5
       ah=sha1 key=20 082539de75376de4ed16486acd96ae0f7d3c88e5
  dec:pkts/bytes=5049/423083, enc:pkts/bytes=5047/766232
```

  - » Finally, an IPsec packet (ESP) is sent on the wire

New IPsec dialup behavior (cont.)

- The IPv4 route tree
  - » List all overlay next-hop IPs and associated tunnel indexes
  - » List all underlay IPsec tunnel endpoint IPs and associated tunnel indexes

```
Hub # diag vpn tunnel list name Spoke
list ipsec tunnel by names in vd 0
------------------------------------------------
name=Spoke ver=1 serial=1 198.51.100.1:0->…
(…truncated…)
run_tally=4
ipv4 route tree:
10.10.10.2 2
10.10.10.3 0
10.10.10.4 3
10.10.10.5 1
198.51.100.2 2
198.51.100.3 0
198.51.100.4 3
198.51.100.5 1
```

Overlay Next-Hops

Underlay IPsec tunnel endpoints

tunnel indexes

The overlay Next-Hops are automatically learned by the Hub during tunnel negotiation due to the Hub & Spokes being configured with:

"`set exchange-interface-ip enable`"

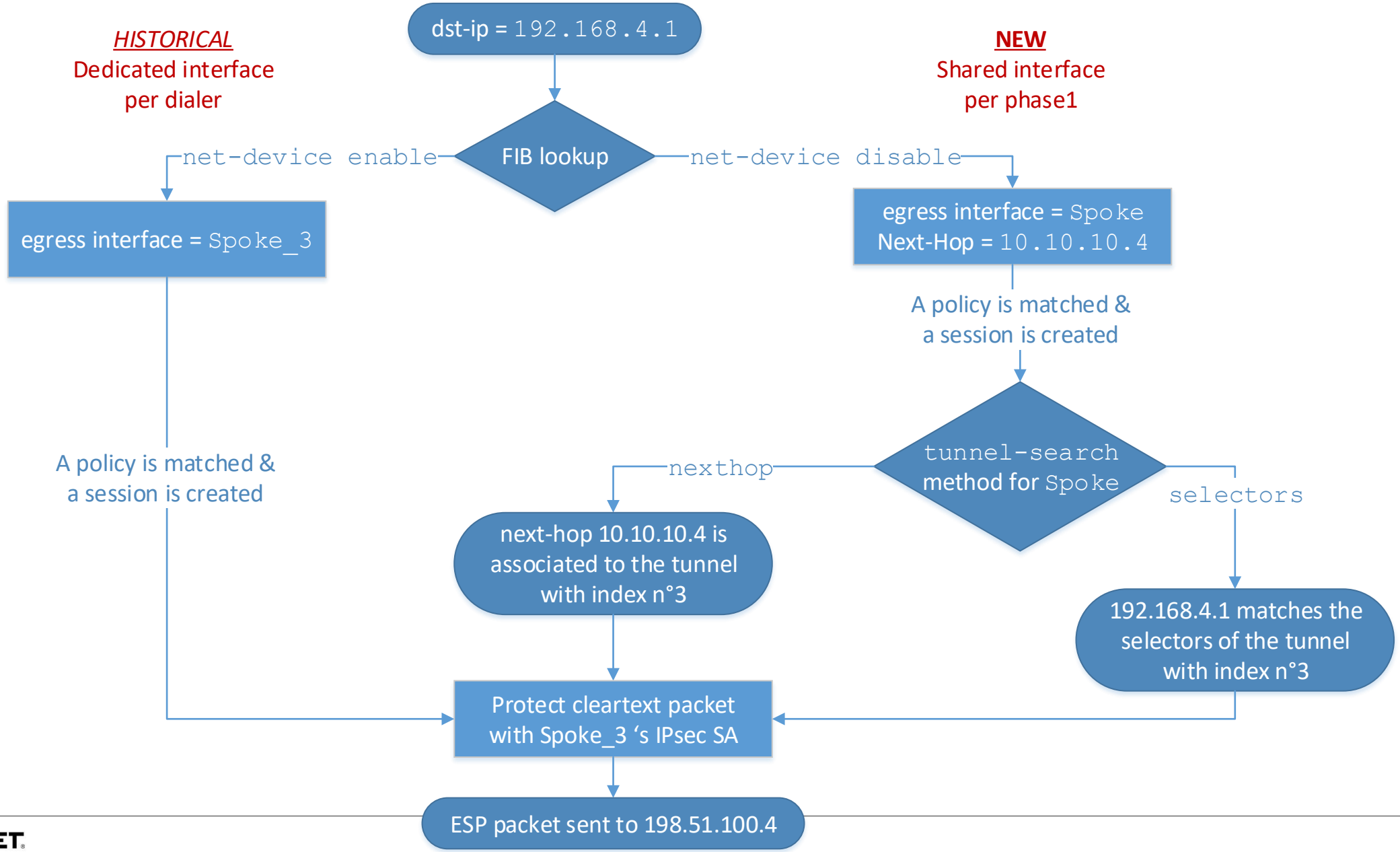
or with

"`set auto-discovery-receiver enable`" [Spoke]
"`set auto-discovery-sender enable`" [Hub]

or with

"`set mode-cfg enable`"

Slow-Path (session setup)

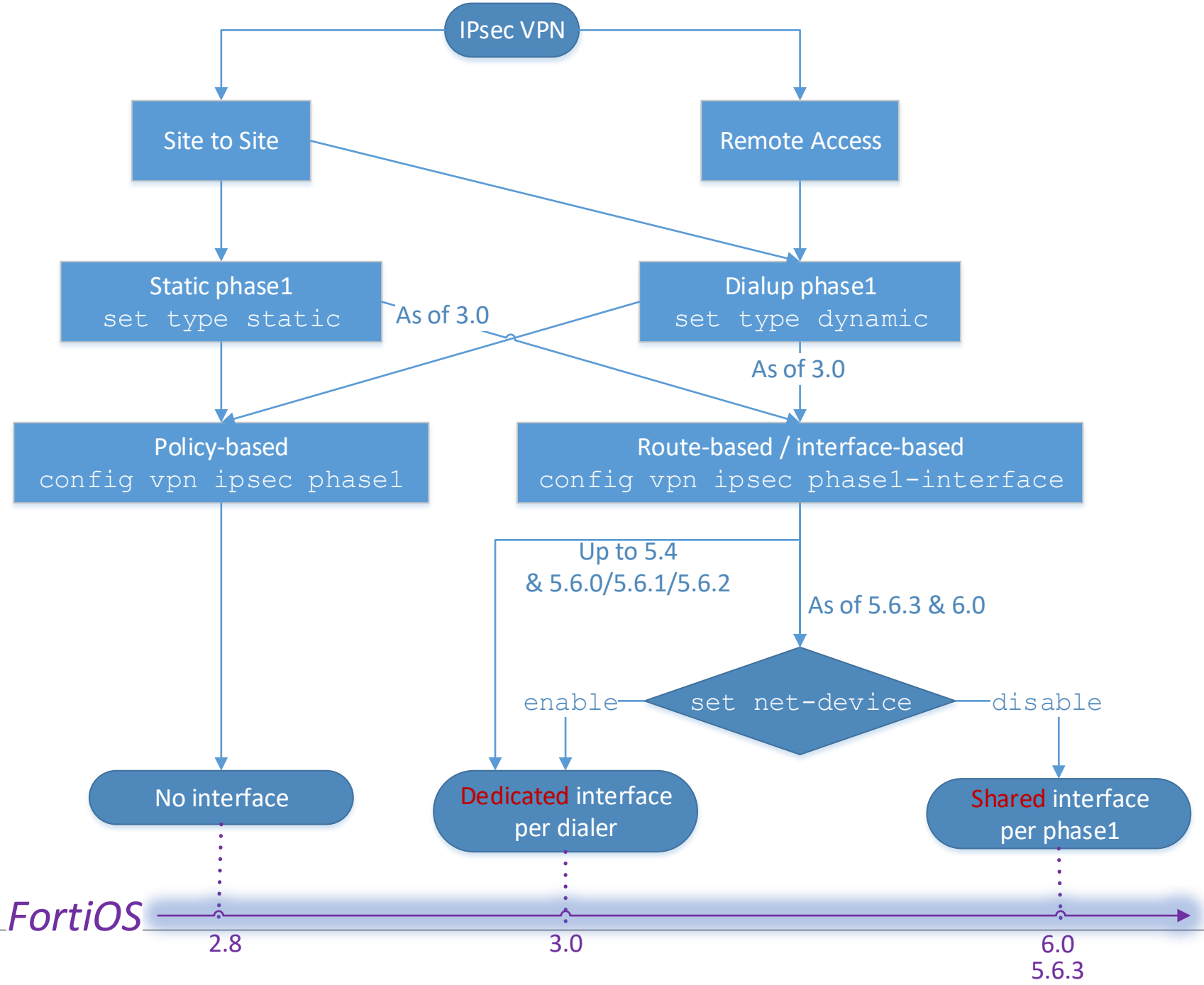


Why this new IPsec dialup behavior ?

- A major kernel upgrade was done between FortiOS 5.2 and 5.4
  - » The new kernel provides reduced latency for session processing which comes with a cost:
    - interface creation is slower (→ lower tunnel setup rate)
    - interface deletion is slower (→ lower tunnel tear-down rate)

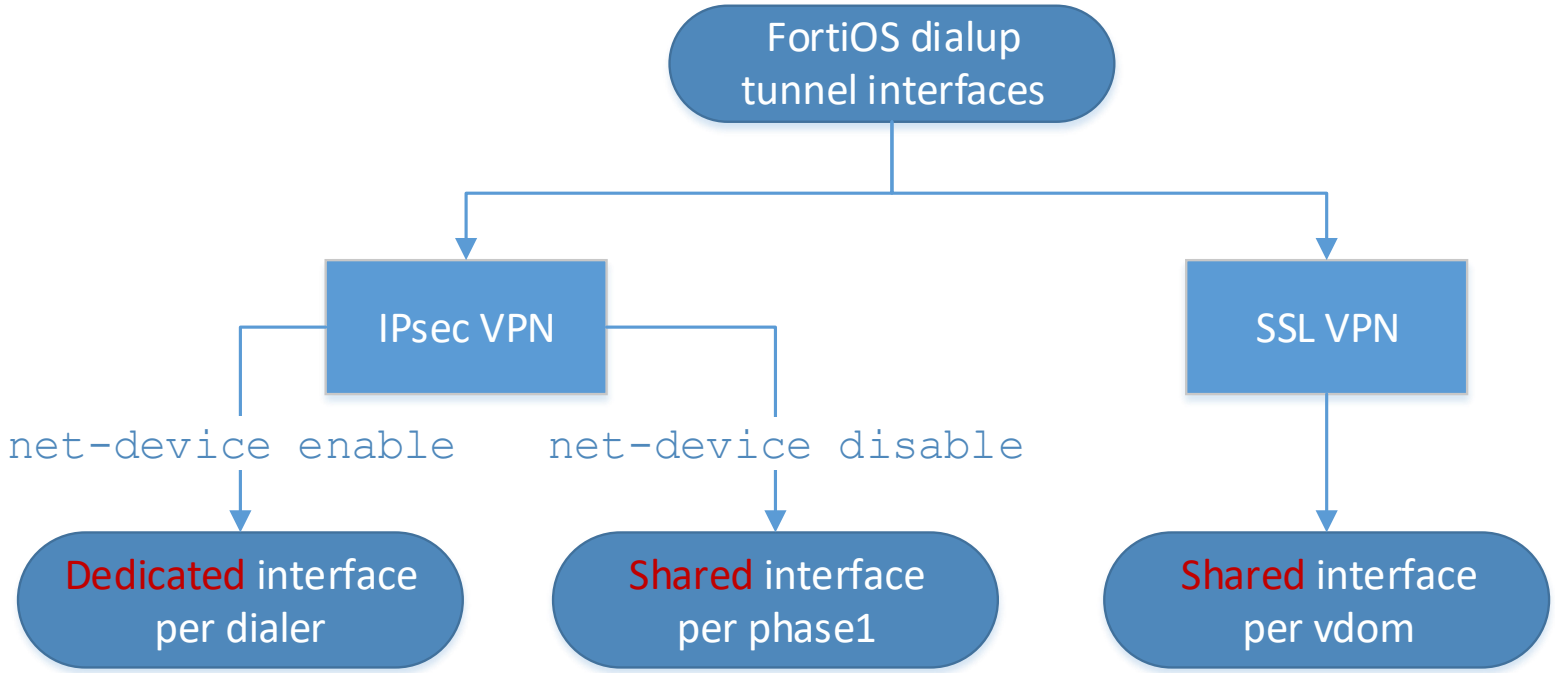
- **`net-device disable`** does not create dynamic interface which:
  - » Provides a tunnel setup/teardown rate close to policy-based VPNs
  - » Eliminates some complexities or limitations

    For e.g.:
    - Assignment of an IP address to a dynamic interface
    - Policy-routing towards a dynamic interface
    - Inheritance of all the parent's interface settings (MTU, …) by a dynamic interface


IPsec VPN
Site to Site
Remote Access
Static phase1
set type static
As of 3.0
Dialup phase1
set type dynamic
As of 3.0
Policy-based
config vpn ipsec phase1
Route-based / interface-based
config vpn ipsec phase1-interface
Up to 5.4
& 5.6.0/5.6.1/5.6.2
As of 5.6.3 & 6.0
enable
set net-device
disable
No interface
Dedicated interface
per dialer
Shared interface
per phase1
FortiOS
2.8
3.0
6.0
5.6.3

FortiOS dialup interfaces

- IPsec and SSL VPNs



Upgrade

When upgrading from a FortiOS version which does not have “net-device” setting, “`set net-device enable`” is added to all dialup phase1.

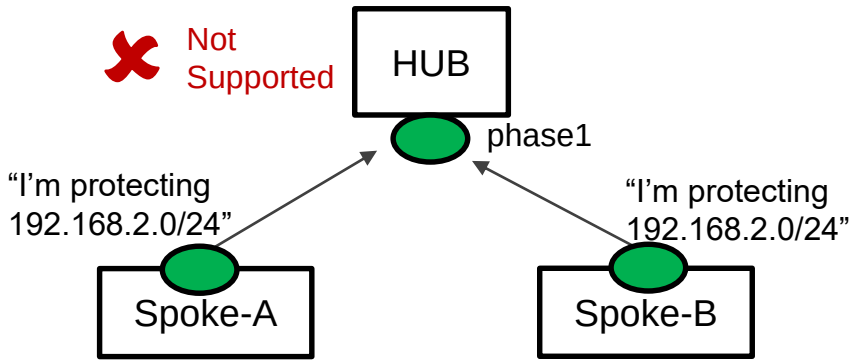
This is done to retain the former dialup behavior of creating a dynamic interface for each dialer.

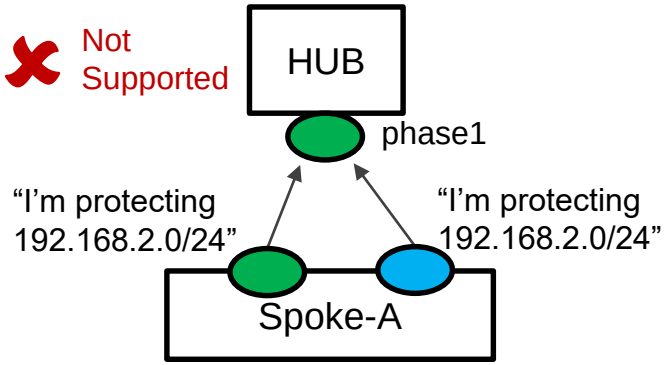
However, for stability reasons, it is **strongly recommended** to switch to using the new dialup behavior with “`set net-device disable`”.

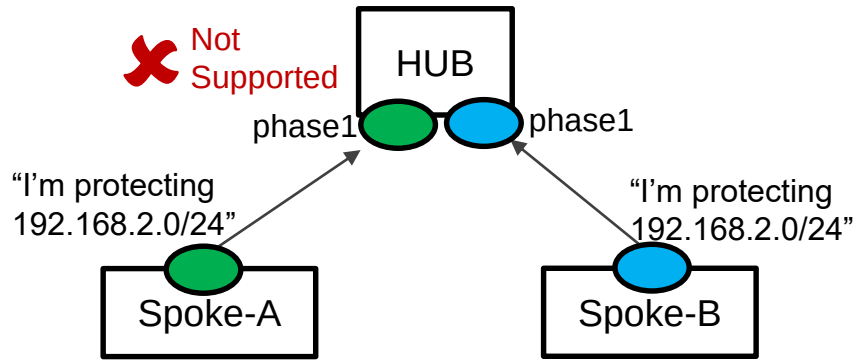
Restrictions for “net-device disable” with IKE routes

The subnets protected by the Spokes are learned from the traffic selectors of the IPsec SA negotiation

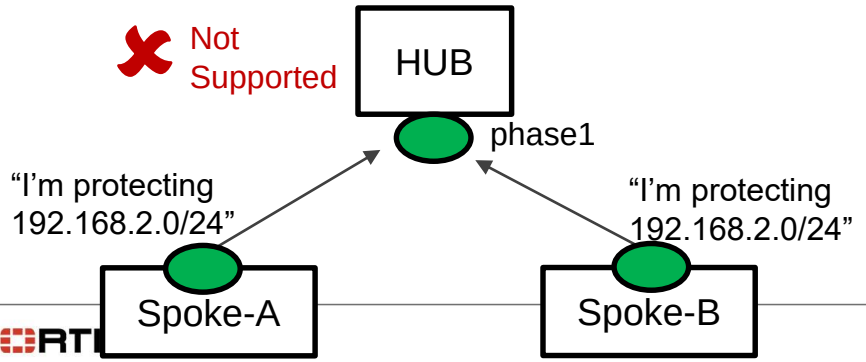
- **Up to FortiOS 6.2.0** The Hub can learn a given subnet **only once**

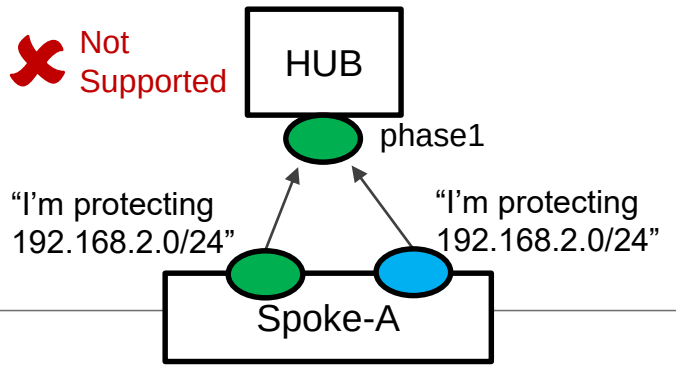


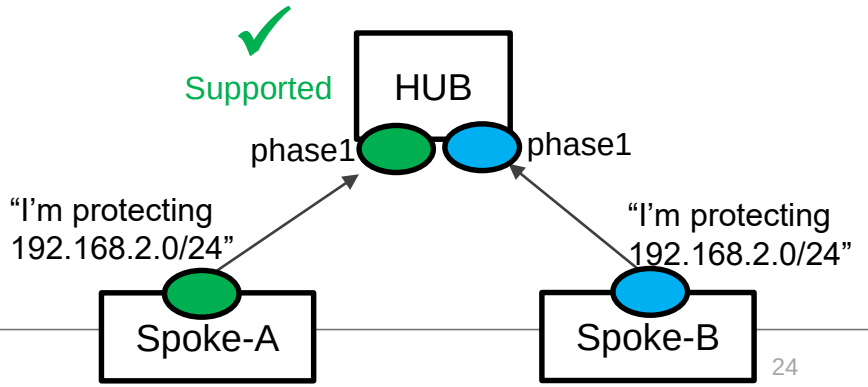




- **As of FortiOS 6.2.1** The Hub can learn a given subnet **once per phase1**







Tunnel name maximum length

- Tunnel name = *phase1name_index*

Each dialup tunnel instance has a unique name made of:
- *The name of the phase1*
- *An arbitrary index*

```
Hub # diag vpn tunnel list name Spoke_3
list ipsec tunnel by names in vd 0
------------------------------------------------
name=Spoke_3 ver=1 serial=8 198.51.100.1:0->...
bound_if=4 lgwy=static/1 tun=intf/0 ...
 parent=Spoke index=3
(...)
```

- Up to 6.4.2/6.2.5, the tunnel name (*phase1name_index*) limit is 15 characters
  - » The length of the phase1 name directly influences the maximum number of concurrent tunnels

  E.g., with a phase1 name of “spn3-inetBB’ (11-char) only 3-char remains for the index itself thereby limiting to [0-999] the index range (spn3-inetBB_XXX): the maximum number of concurrent dialup tunnels is limited to 1000

- As of 6.4.3/6.2.6, the tunnel name (*phase1name_index*) limit is 35 characters
  - » The phase1 name limit is 15-char
  - » Followed by “_” and the index for a total length up to 35-char

New IPsec dialup logic

With BGP

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 "toSpokes"
    set ip 10.10.10.1/32
    set remote-ip 10.10.10.254/24
  next
end
```

Spoke

```
config system interface
  edit "toHub"
    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

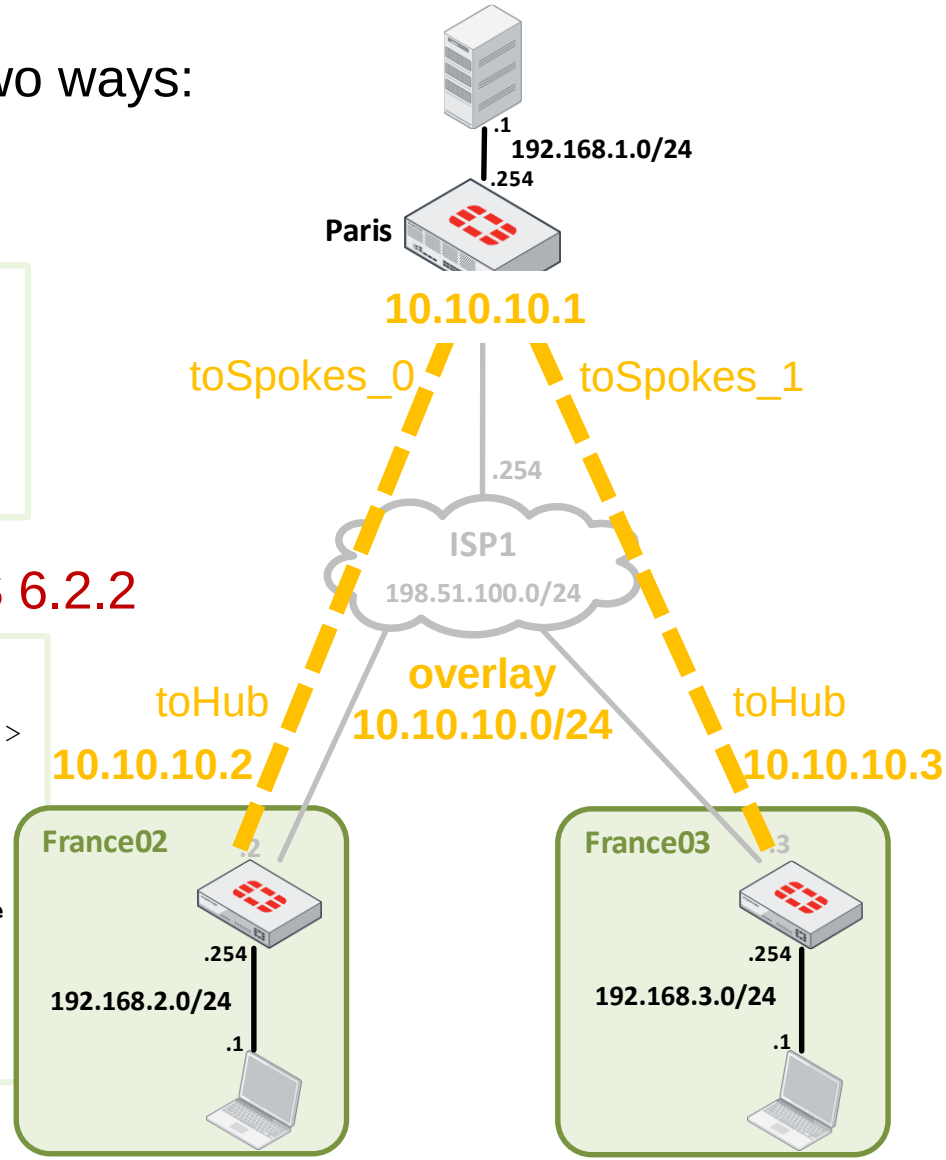
HUB

```
config system interface
  edit "toSpokes"
    set ip 10.10.10.1/32
    set remote-ip 10.10.10.254/24
  next
end
config vpn ipsec phase1-interface
 edit "toSpokes"
   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 "toHub"
   < do not configure an IP here >
  next
end

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



Hub IPsec 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 "`toSpokes`" is used as a shared interface

tunnel-search nexthop

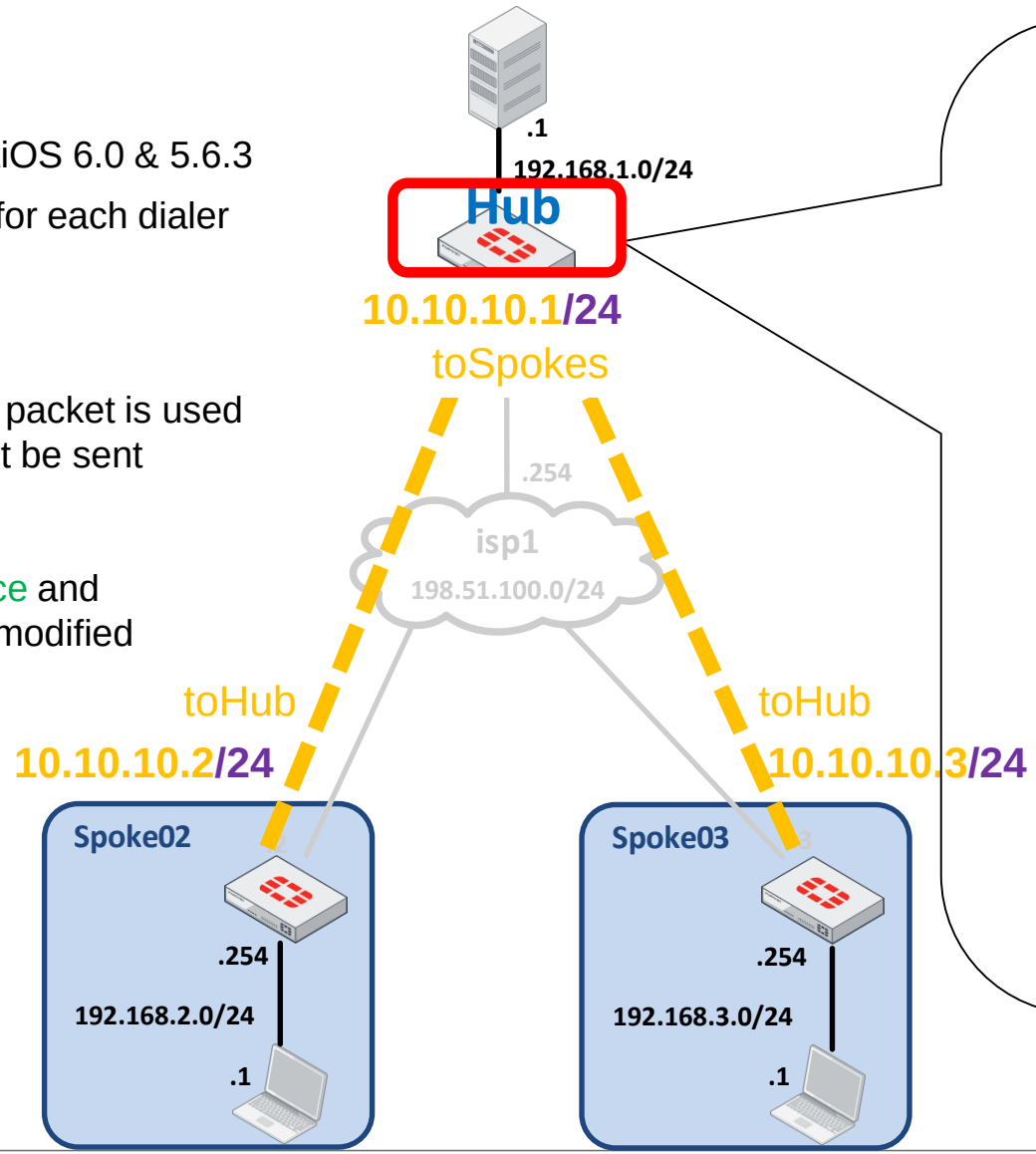
The next-hop IP of the route matched by a packet is used to decide into which tunnel the packet must be sent

In FortiOS 5.6.3 & 5.6.4, net-device and tunnel-search settings cannot be modified after the phase1 was created

This limitation is removed in FortiOS 6.0 and as of FortiOS 5.6.5

add-route disable

Dynamic routing is used for learning the Spokes' protected subnets




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

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

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

Hub IPsec configuration

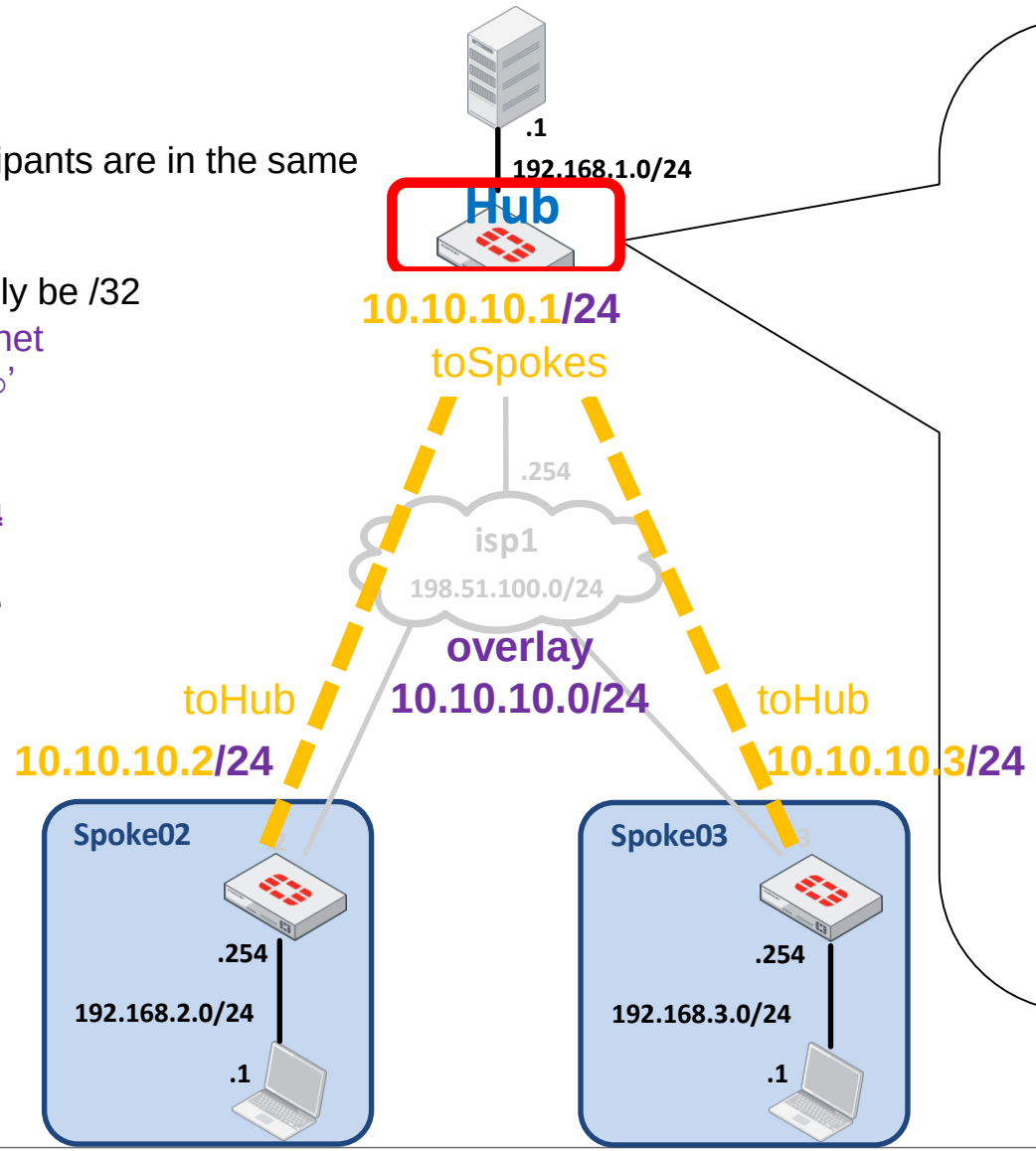
/24

The overlay IPs of all Hub & Spoke 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 "toSpokes"
        set type dynamic
        set net-device disable
        set tunnel-search nexthop
        set interface "wan"
        set proposal aes128-sha1
        set add-route disable
        set exchange-interface-ip enable
        set auto-discovery-sender enable
        set psksecret xxxxxxxx
    next
end

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

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

NEW

Hub IPsec configuration

auto-discovery-sender enable

Required if ADVPN is desired

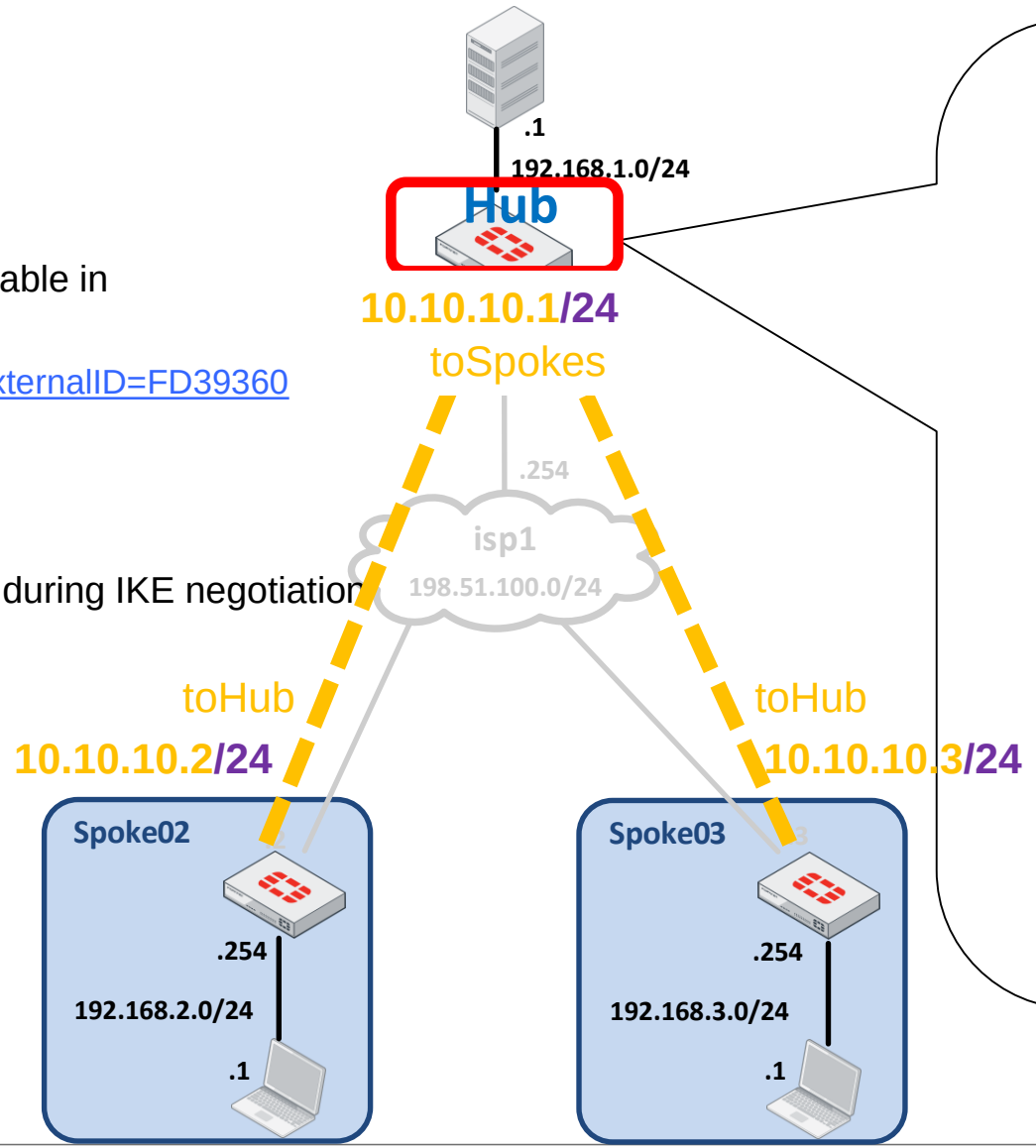
Detailed information about **ADVPN** is available in **KB article FD39360**

https://kb.fortinet.com/kb/documentLink.do?externalID=FD39360

exchange-interface-ip enable

For learning the overlay IPs of the Spokes during IKE negotiation

Automatically enabled when ADVPN is activated with
'auto-discovery-sender enable'




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

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

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

Spoke IPsec configuration

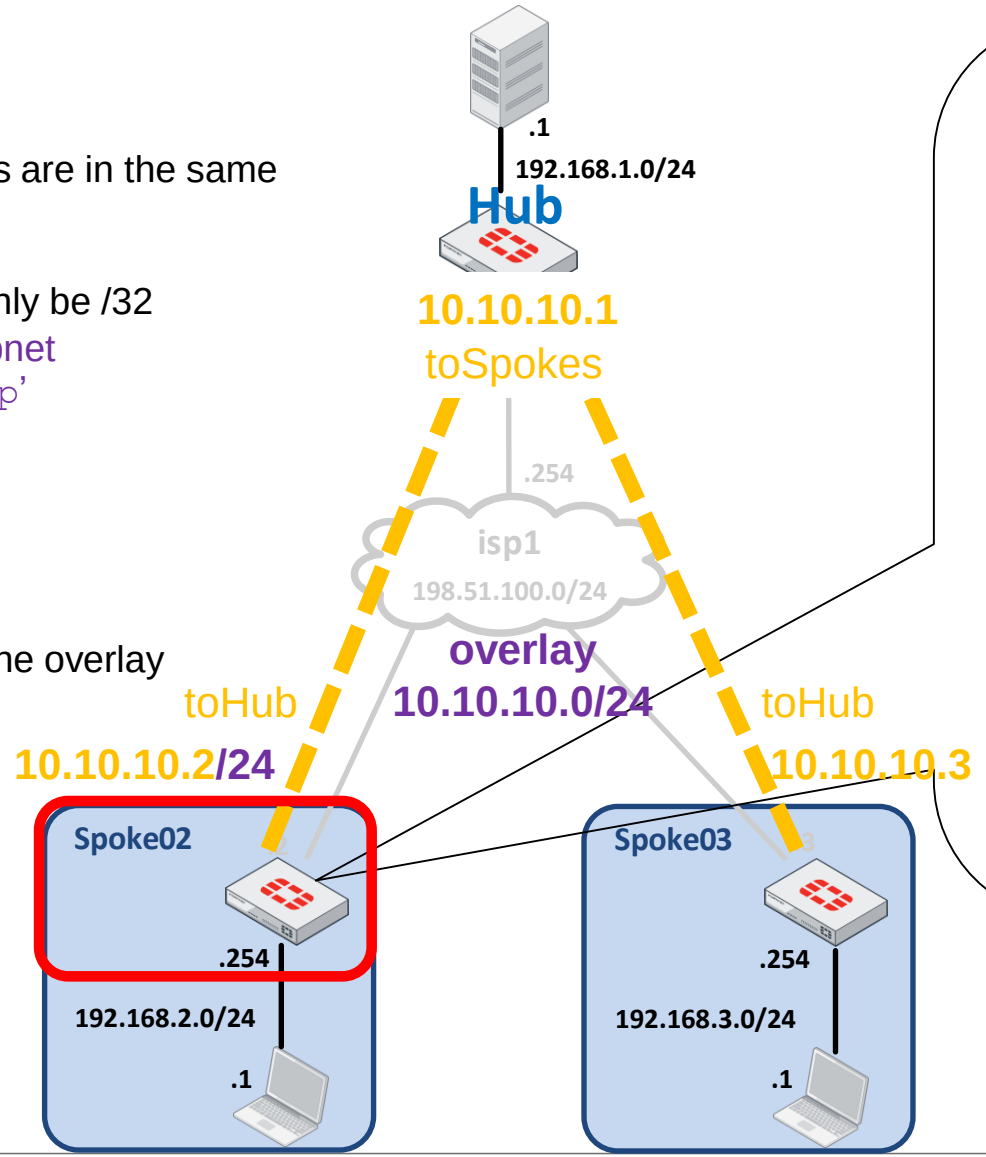
/24

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 `remote-ip` can be any other IP in the overlay
For clarity, the IP of the Hub is used




```
config vpn ipsec phase1-interface
    edit "toHub"
        set interface "wan"
        set proposal aes128-sha1
        set exchange-interface-ip enable
        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 "toHub"
        set phase1name "toHub"
        set proposal aes128-sha1
    next
end

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

NEW

Spoke IPsec configuration

auto-discovery-receiver enable
add-route disable

Required if ADVPN is desired

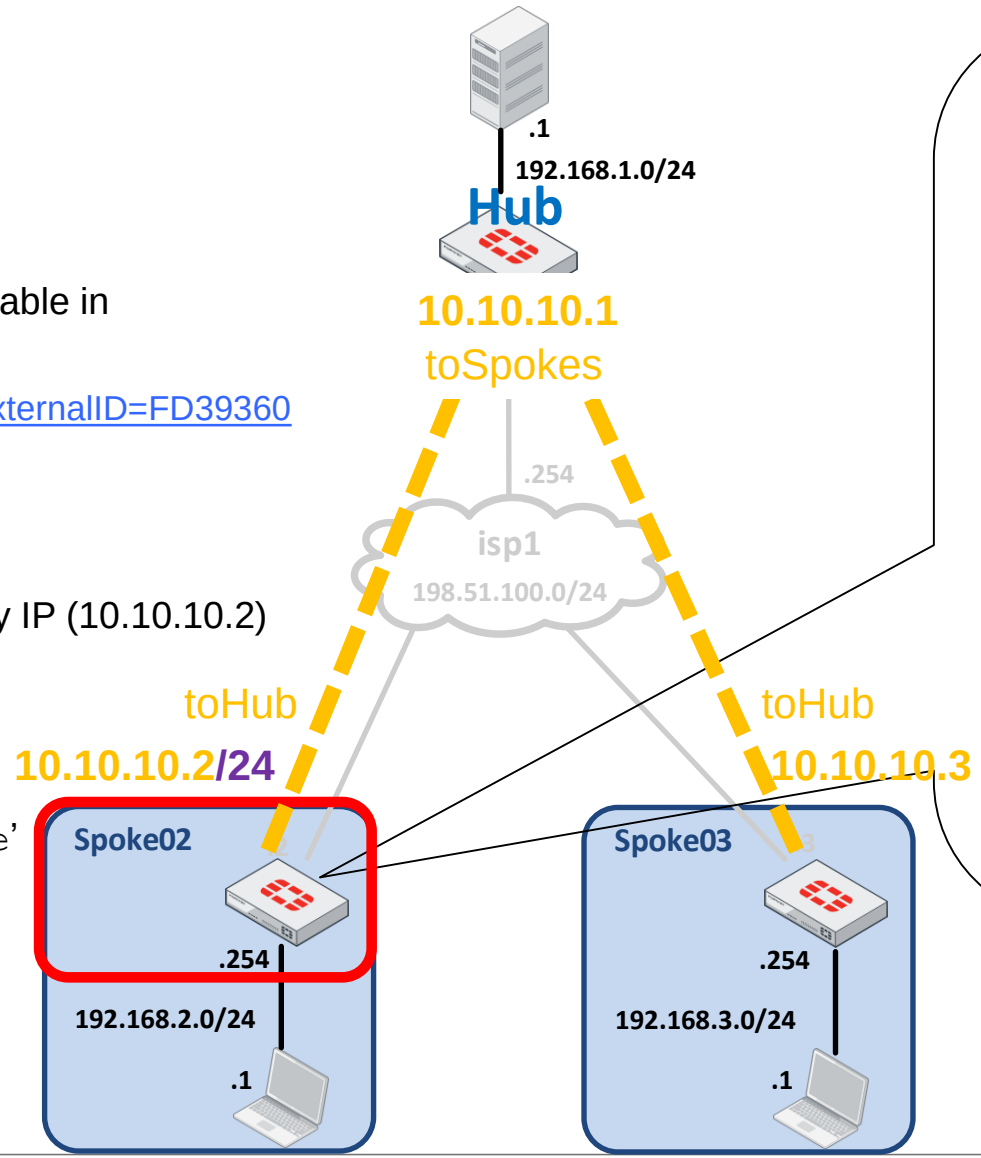
Detailed information about **ADVPN** is available in **KB article FD39360**

https://kb.fortinet.com/kb/documentLink.do?externalID=FD39360

exchange-interface-ip enable

Instructs the Spoke to announce its overlay IP (10.10.10.2) to the Hub during IKE negotiation.

Automatically enabled when ADVPN is activated with '`auto-discovery-sender enable`'



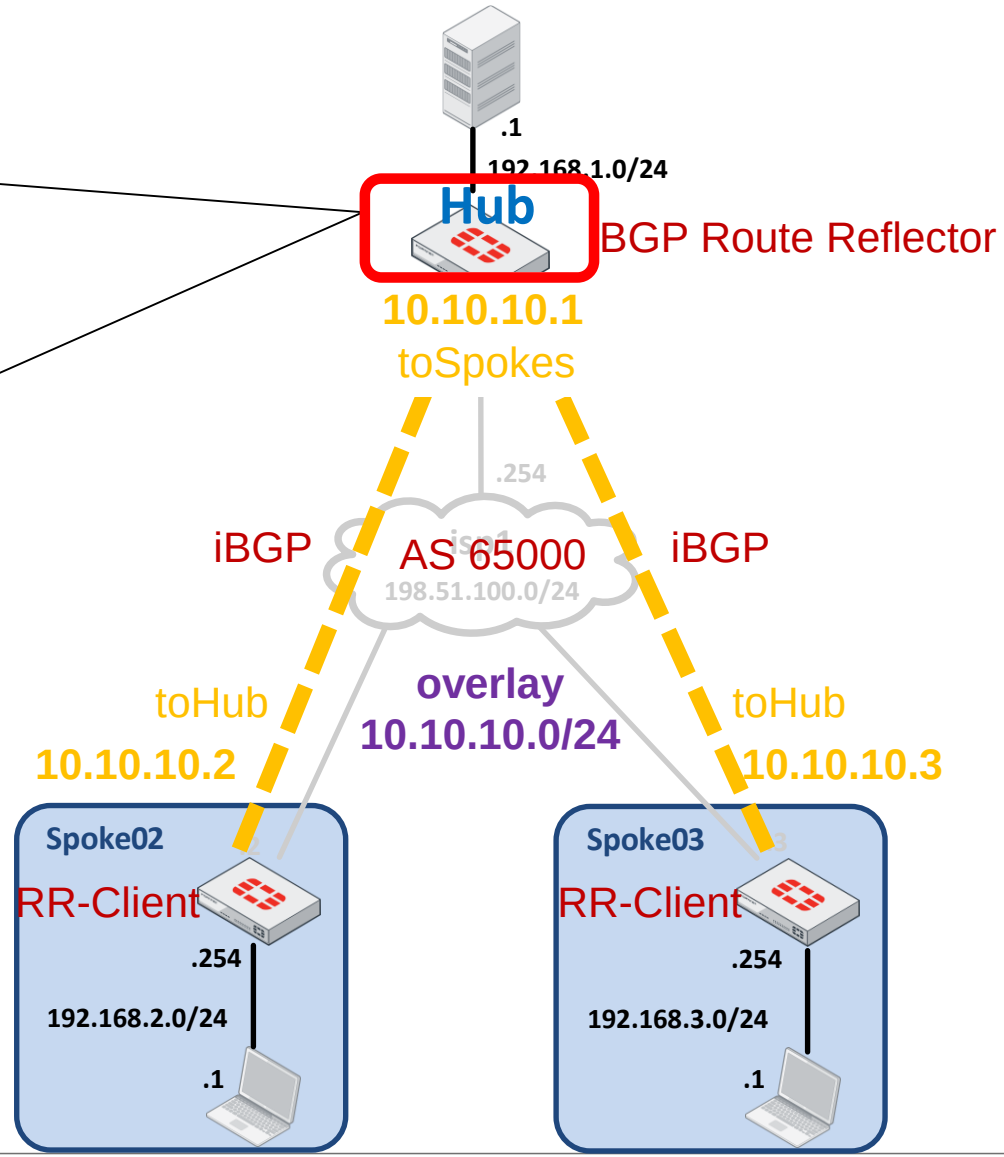

```
config vpn ipsec phase1-interface
    edit "toHub"
        set interface "wan"
        set proposal aes128-sha1
        set exchange-interface-ip enable
        set auto-discovery-receiver enable
        set add-route disable
        set remote-gw 198.51.100.1
        set psksecret xxxxxxxx
    next
end

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

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

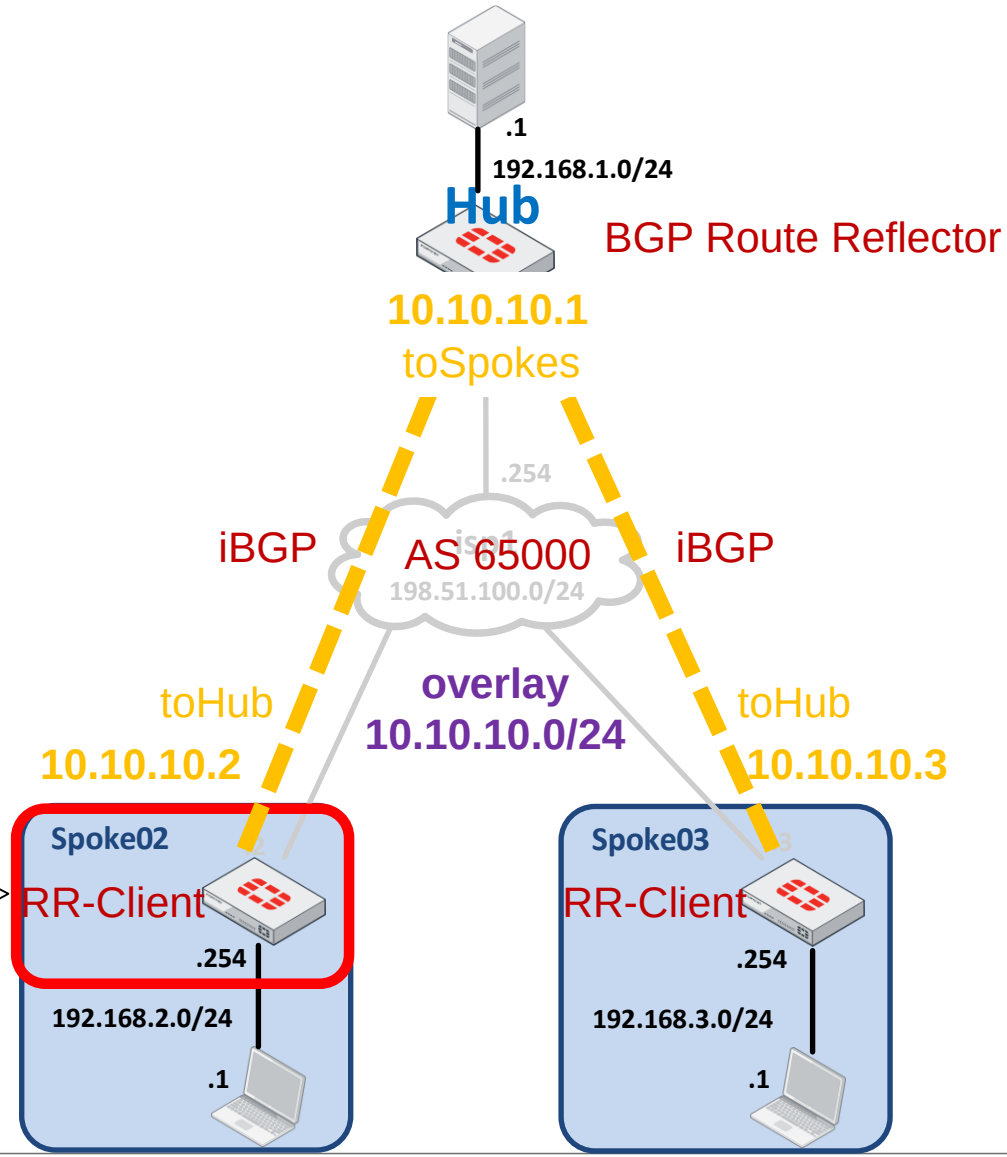
Hub BGP configuration

```
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 BGP configuration

```
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
```



New IPsec dialup logic

With OSPF

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 "toSpokes"
    set ip 10.10.10.1/32
    set remote-ip 10.10.10.254/24
  next
end
```

Spoke

```
config system interface
  edit "toHub"
    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

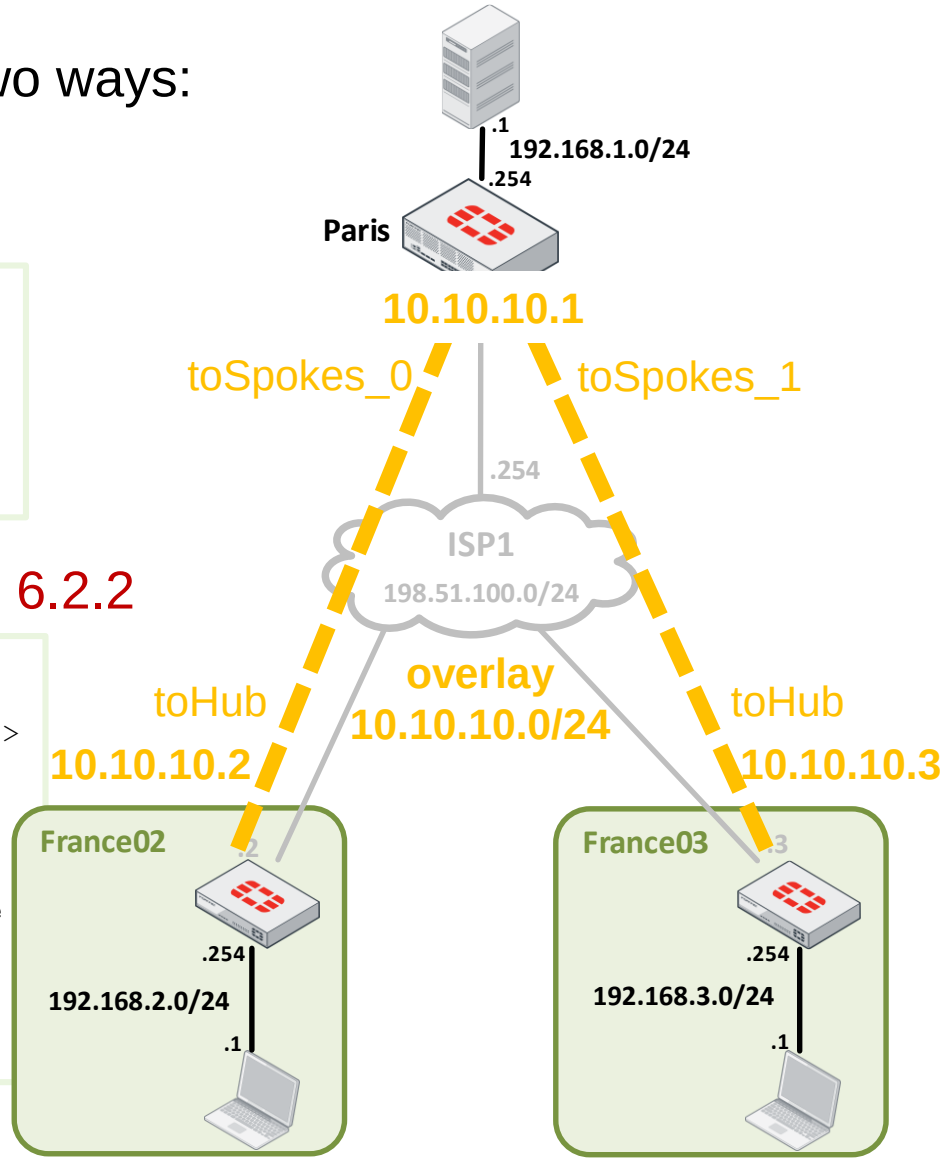
HUB

```
config system interface
  edit "toSpokes"
    set ip 10.10.10.1/32
    set remote-ip 10.10.10.254/24
  next
end
config vpn ipsec phase1-interface
 edit "toSpokes"
   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

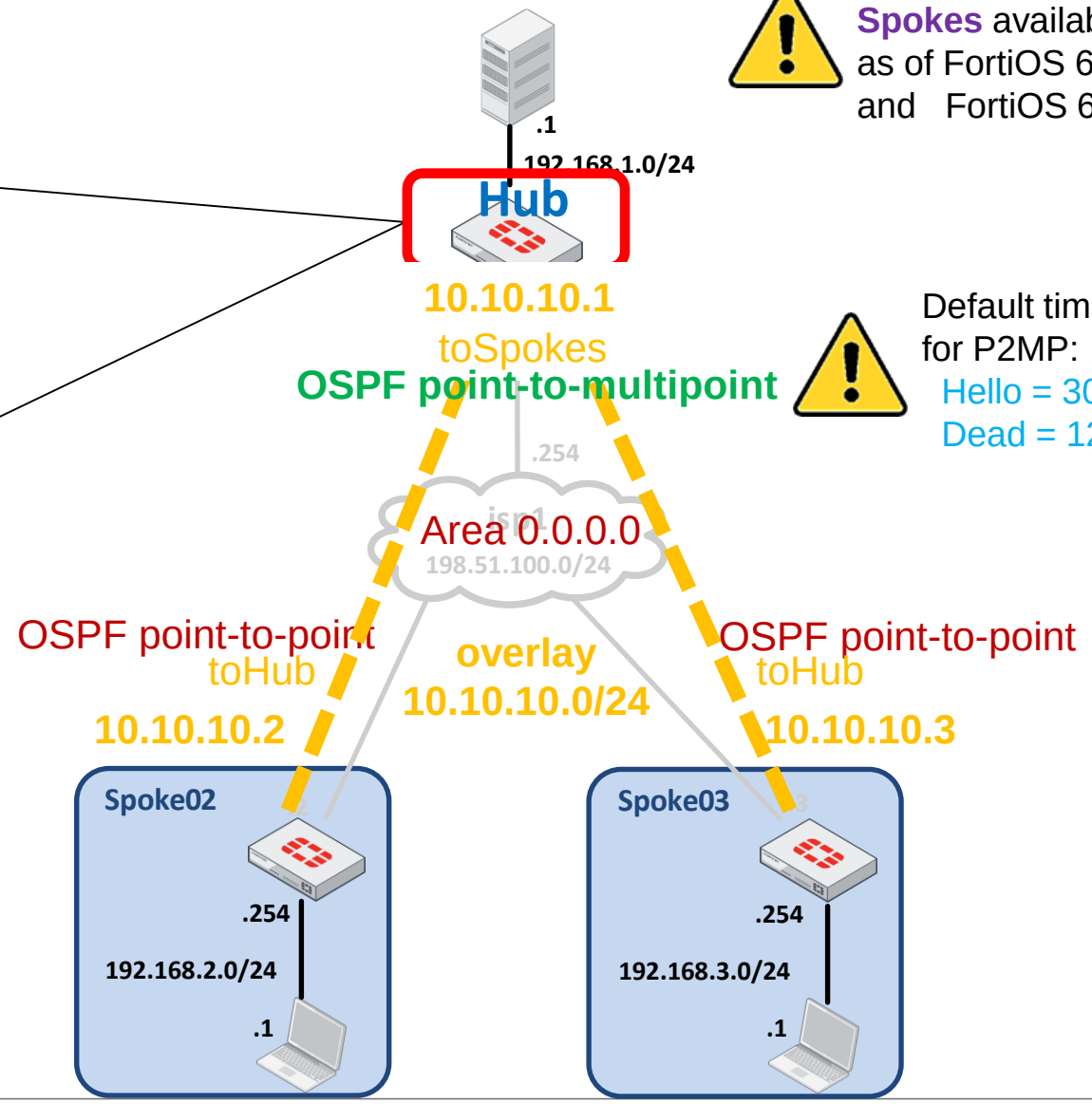
```
config system interface
  edit "toHub"
   < do not configure an IP here >
  next
end

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



Hub OSPF configuration

```
config router ospf
    set router-id 10.10.10.1
    config area
        edit 0.0.0.0
        next
    end
    config ospf-interface
        edit "toSpokes"
            set interface "toSpokes"
            set mtu-ignore enable
            set network-type point-to-multipoint
            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
```

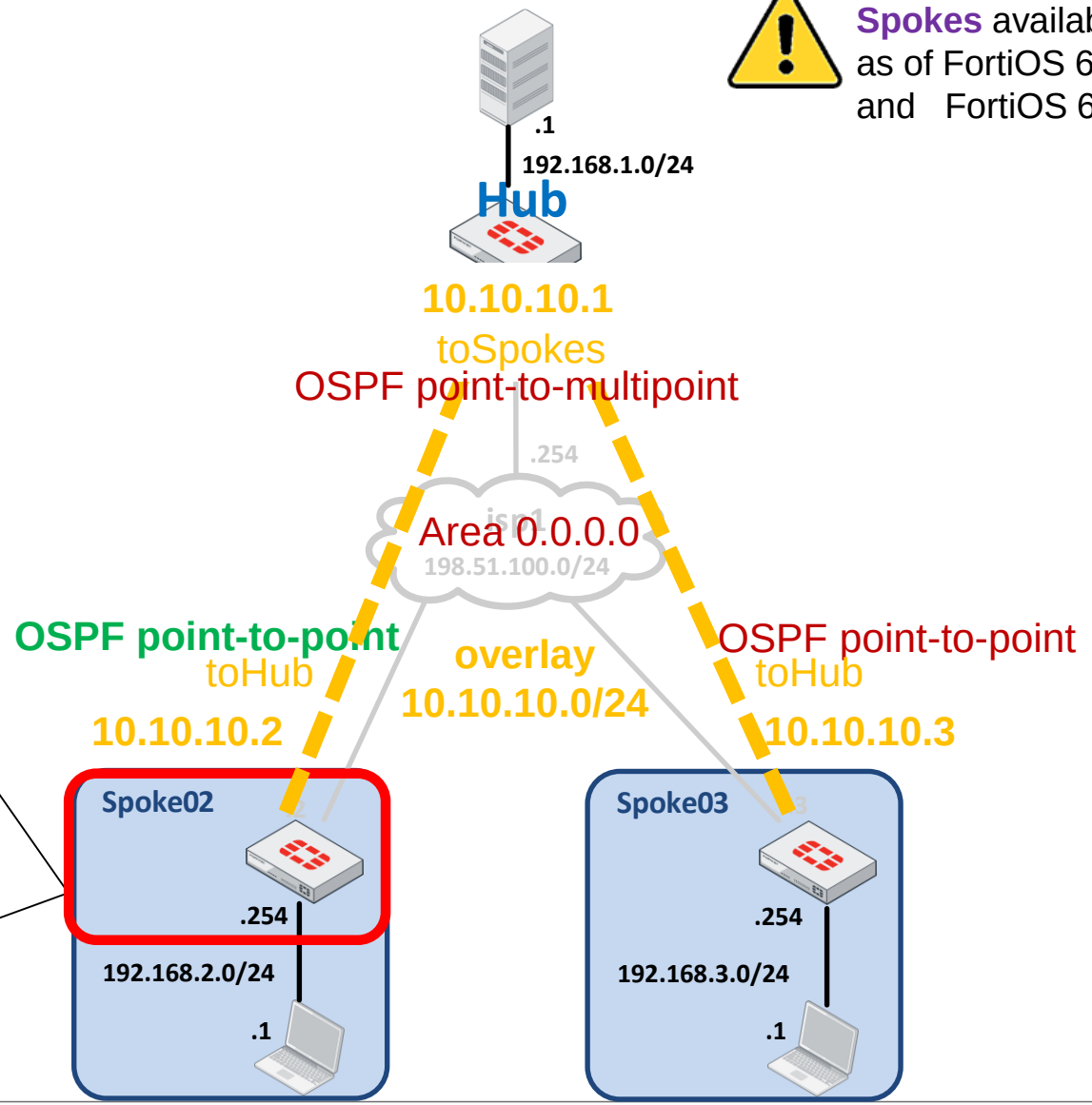


Support for NATed Spokes available only as of FortiOS 6.2 and FortiOS 6.0.5

Default timers for P2MP:
Hello = 30 sec
Dead = 120 sec

Spoke OSPF configuration

```
config router ospf
    set router-id 10.10.10.2
    config area
        edit 0.0.0.0
        next
    end
    config ospf-interface
        edit "toHub"
            set interface "toHub"
            set network-type point-to-point
            set mtu-ignore enable
        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
```



Support for NATed Spokes available only as of FortiOS 6.2 and FortiOS 6.0.5

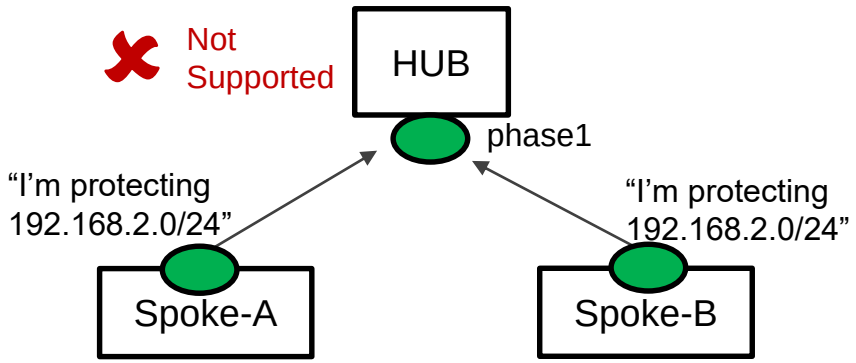
New IPsec dialup logic

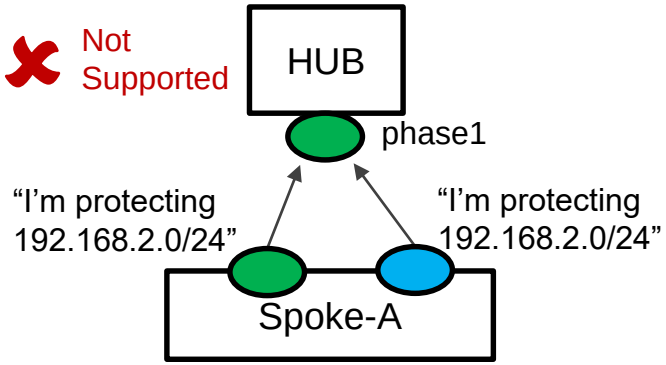
With IKE routes (a.k.a, reverse-route injection - *RRI*)

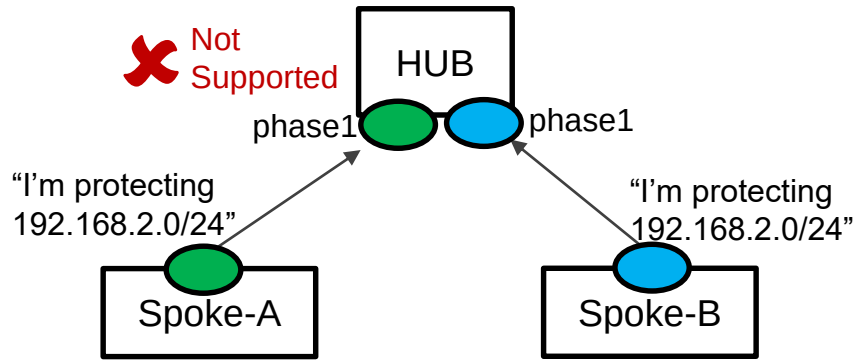
Restrictions for “net-device disable” with IKE routes

The subnets protected by the Spokes are learned from the traffic selectors of the IPsec SA negotiation

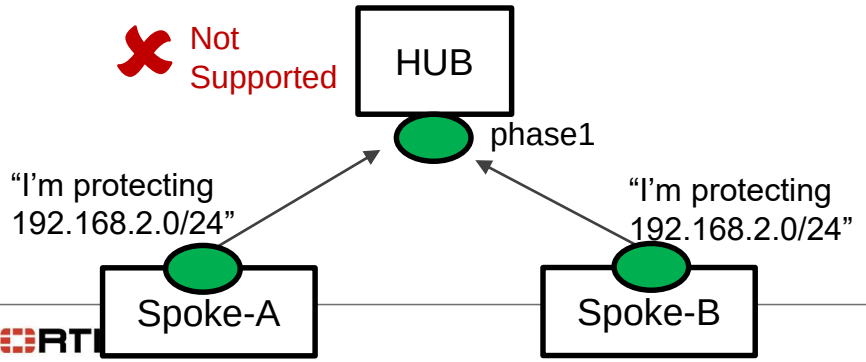
- **Up to FortiOS 6.2.0** The Hub can learn a given subnet **only once**

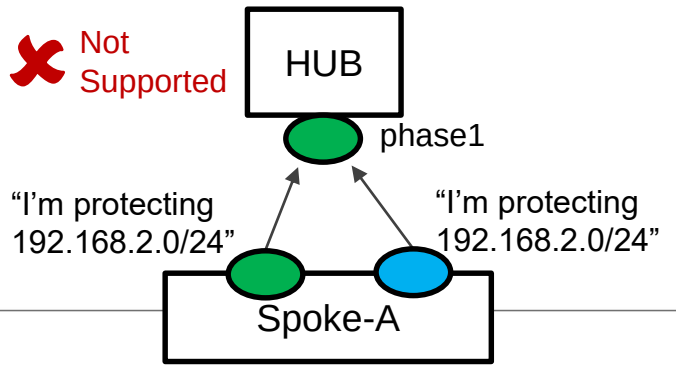


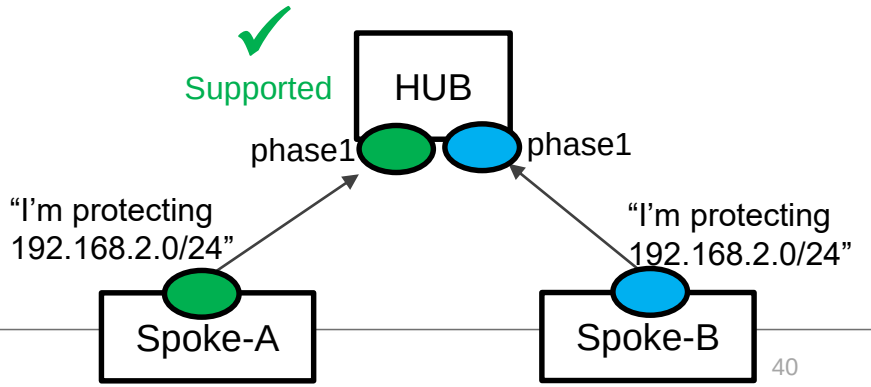




- **As of FortiOS 6.2.1** The Hub can learn a given subnet **once per phase1**







Hub IPsec configuration

add-route enable

The subnets protected by the Spokes are learned from the traffic selectors of the IPsec SA negotiation

These routes are submitted to the routing table manager (RTM)

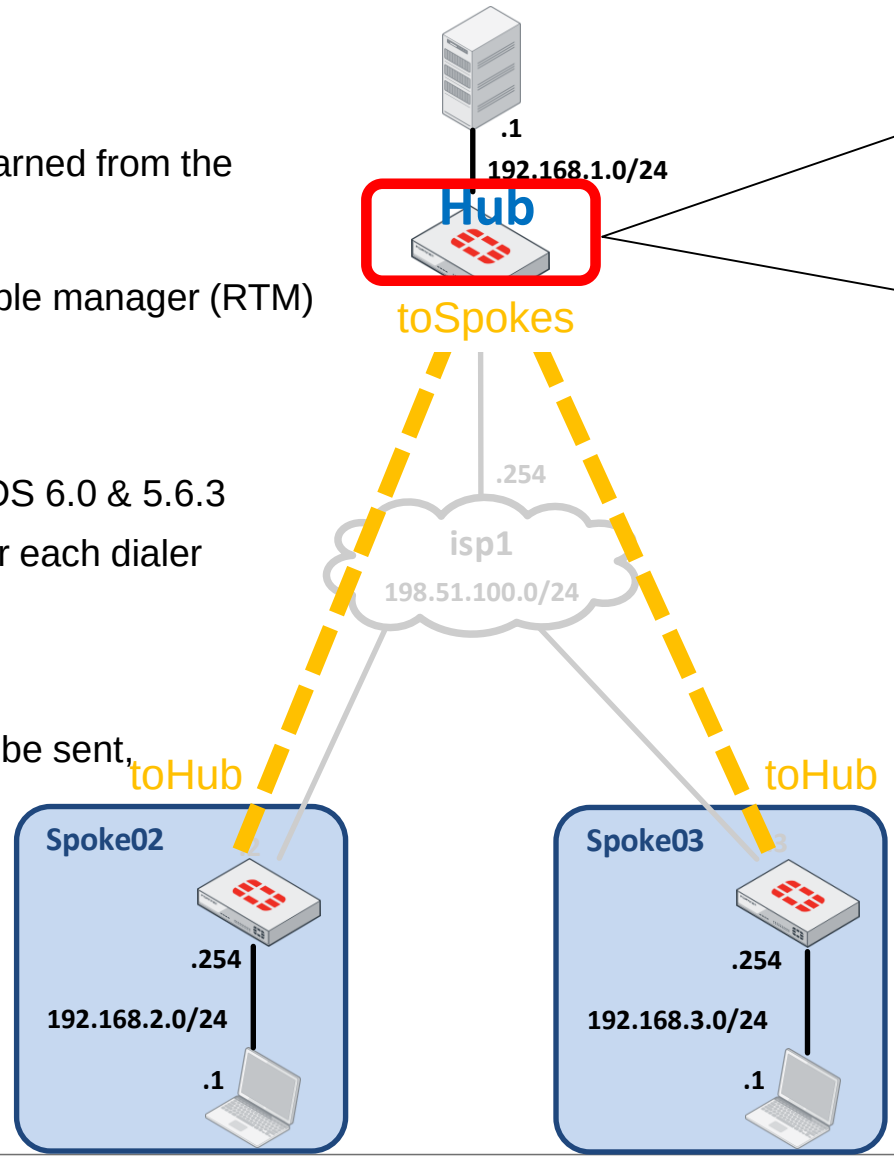
net-device disable

Default setting for dialup phase1 as of FortiOS 6.0 & 5.6.3

A dedicated interface is no longer created for each dialer "`toSpokes`" is used as a shared interface

tunnel-search selectors

To decide into which tunnel the packet must be sent, the dst-ip of the packet is checked against the list of IPsec SA selectors



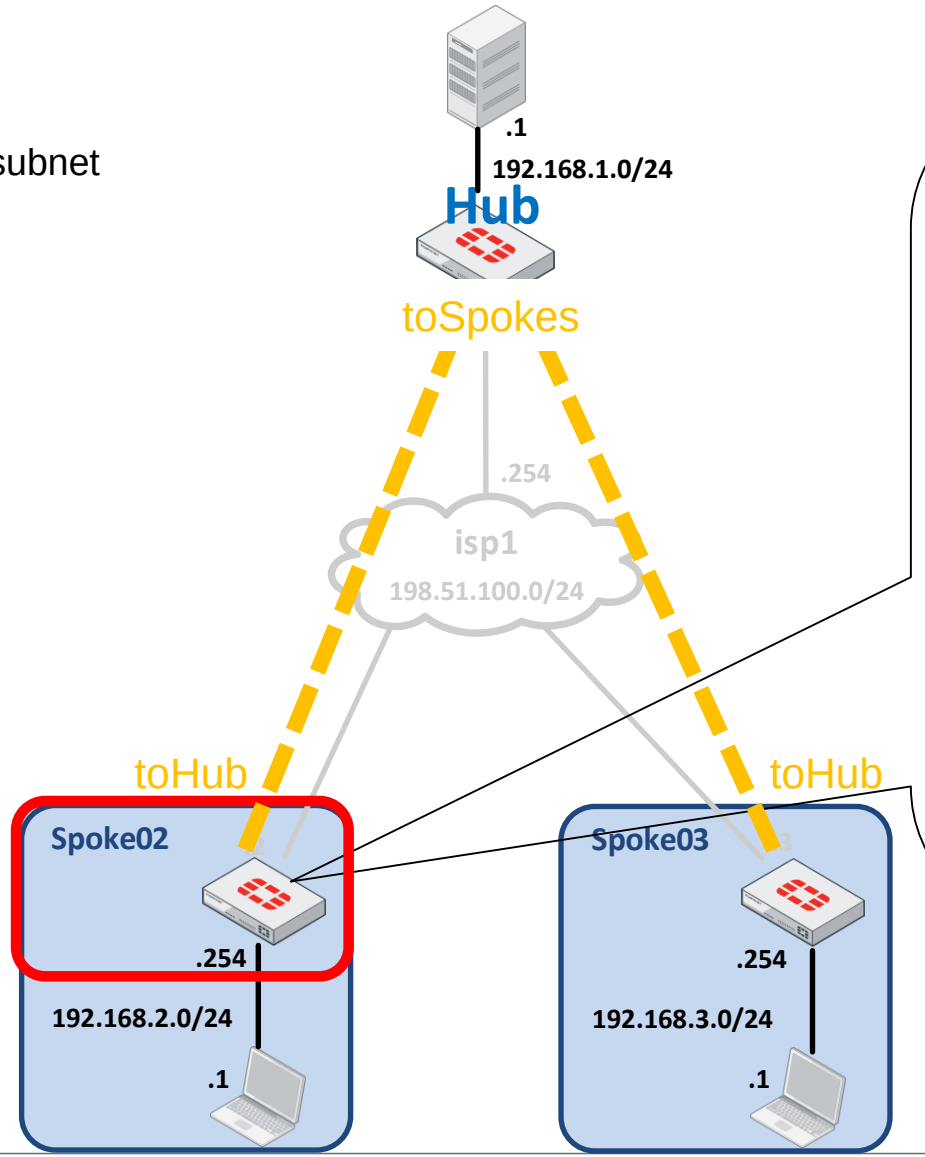

```
config vpn ipsec phase1-interface
    edit "toSpokes"
        set type dynamic
        set net-device disable
        set tunnel-search selectors
        set interface "wan"
        set proposal aes128-sha1
        set add-route enable
        set psksecret xxxxxxxx
    next
end

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

Spoke IPsec & routing configuration

src-subnet <protected-subnet>

The Spoke must announce each protected subnet during IPsec SA negotiation




```
config vpn ipsec phase1-interface
    edit "toHub"
        set interface "wan"
        set proposal aes128-sha1
        set remote-gw 198.51.100.1
        set psksecret xxxxxxxx
    next
end

config vpn ipsec phase2-interface
    edit "toHub"
        set phase1name "toHub"
        set proposal aes128-sha1
        set src-subnet 192.168.2.0/24
    next
end

config router static
    edit <id>
        set dst 192.168.1.0/24
        set device "toHub"
    next
end
```

Static route(s) to reach the Hub's subnet(s)

Spoke IPsec & routing configuration

Announcing multiple protected subnets with IKEv1

```
config vpn ipsec phase2-interface
 edit "net2"
    set phase1name "toHub"
    set proposal aes128-sha1
    set src-subnet 192.168.2.0/24
 next
 edit "net22"
    set phase1name "toHub"
    set proposal aes128-sha1
    set src-subnet 192.168.22.0/24
 next
 edit "net222"
    set phase1name "toHub"
    set proposal aes128-sha1
    set src-subnet 192.168.222.0/24
 next
end
```

Announcing multiple protected subnets with IKEv2

```
config firewall address
 edit "internal_net2"
   set subnet 192.168.2.0 255.255.255.0
 next
 edit "internal_net22"
   set subnet 192.168.22.0 255.255.255.0
 next
 edit "internal_net222"
   set subnet 192.168.222.0 255.255.255.0
next
end

config firewall addrgrp
edit "internal_subnets"
    set member "internal_net2" "internal_net22" "internal_net222"
next
end

config vpn ipsec phase2-interface
 edit "toHub"
    set phase1name "toHub"
    set proposal aes128-sha1
    set src-addr-type name
    set src-name "internal_subnets"
    set dst-addr-type name
    set dst-name "all"
next
end
```

IKE routes (reverse route injection)

- The Hub learns the Spokes' subnets during IPsec SA negotiation

Hub IKE debug

```
ike 0: comes 198.51.100.2:500->198.51.100.1:500,ifindex=4....
(...)
ike 0:toSpokes_3:5:7: responder received first quick-mode message
ike 0:toSpokes_3:5:7: peer proposal is: peer:0:192.168.2.0-
192.168.2.255:0, me:0:0.0.0.0-255.255.255.255:0
(...)
ike 0:toSpokes_3:5:toSpokes:7: IPsec SA selectors #src=1 #dst=1
ike 0:toSpokes_3:5:toSpokes:7: src 0 7 0:0.0.0.0-255.255.255.255:0
ike 0:toSpokes_3:5:toSpokes:7: dst 0 7 0:192.168.2.0-192.168.2.255:0
ike 0:toSpokes_3:5:toSpokes:7: add dynamic IPsec SA selectors
ike 0:toSpokes:7: add route 192.168.2.0/255.255.255.0 gw 198.51.100.2
oif toSpokes(16) metric 15 priority 0
(...)
```

static route
is dynamically created

Next-Hop is the Spoke's
tunnel endpoint address

IKE routes (reverse route injection)

- Networks accessible over dialup tunnels are all bound to the same shared (phase1) interface

```
Hub # get router info routing-table static
S        192.168.2.0/24 [15/0] via 198.51.100.2, toSpokes
S        192.168.3.0/24 [15/0] via 198.51.100.3, toSpokes
S        192.168.4.0/24 [15/0] via 198.51.100.4, toSpokes
S        192.168.5.0/24 [15/0] via 198.51.100.5, toSpokes
```

static routes dynamically created

Spokes' networks

The Next-Hop is the tunnel endpoint address of the corresponding Spoke

IKE routes overlap is not supported with 'net-device disable'

IKE routes (reverse route injection)

- Packets forwarded to shared interface `toSpokes`

```
S       192.168.2.0/24 [15/0] via 198.51.100.2, toSpokes
```

  - » When a cleartext packet is sent to `toSpokes`, it is sent to the IPsec engine
  - » The IPsec engine searches for the tunnel index matching the packet's `dst-ip`

```
Hub # diagnose vpn tunnel list name toSpokes
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=toSpokes ver=1 serial=1 198.51.100.1:0->0.0.0.0:0
bound_if=4 lgwy=static/1 tun=intf/0 mode=dialup/2 encap=none/0
proxyid_num=0 child_num=4 refcnt=22 ilast=2940 olast=2940 ad=/0 itn-status=1f
stat: rxp=0 txp=0 rxb=0 txb=0
dpd: mode=on-demand on=0 idle=20000ms retry=3 count=0 seqno=0
natt: mode=none draft=0 interval=0 remote_port=0
run_tally=4
ipv4 route tree:
192.168.2.0->192.168.2.255 3
192.168.3.0->192.168.3.255 0
192.168.4.0->192.168.4.255 2
192.168.5.0->192.168.5.255 1
```

tunnel index → **toSpokes_3**

Spokes' selectors

IKE routes (reverse route injection)

- Packets forwarded to shared interface `toSpokes` (cont.):
  - » the cleartext packet is protected with the IPsec SA of tunnel `toSpokes_3`

```
Hub # diag vpn tunnel list name toSpokes_3
list ipsec tunnel by names in vd 0
------------------------------------------------------
name=toSpokes_3 ver=1 serial=2 198.51.100.1:0->198.51.100.2:0
bound_if=4 lgwy=static/1 tun=intf/0 mode=dial_inst/3 encap=none/256 options[0100]=rgwy_chg
 parent=toSpokes index=3
proxyid_num=1 child_num=0 refcnt=7 ilast=0 olast=0 ad=/0 itn-status=1f
stat: rxp=269 txp=269 rxb=40888 txb=22596
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=Spoke proto=0 sa=1 ref=2 serial=1 add-route
  src: 0:0.0.0.0-255.255.255.255:0
  dst: 0:192.168.2.0-192.168.2.255:0
  SA:  ref=3 options=2a6 type=00 soft=0 mtu=1438 expire=40260/0B replaywin=2048
       seqno=10e esn=0 replaywin_lastseq=0000010e itn=0
  life: type=01 bytes=0/0 timeout=43190/43200
  dec: spi=900ff680 esp=aes key=16 117f19309cc32ef183b7973b6e2f6f4d
       ah=sha1 key=20 c54d3053af167264dc24050ff4f1fa82d1993cbb
  enc: spi=fd617a96 esp=aes key=16 8921a03db5ee144f4eae94deab321c5d
       ah=sha1 key=20 02a6aee085cc3323a799ff643dcdf5760d461158
  dec:pkts/bytes=269/22596, enc:pkts/bytes=269/40888
```

  - » Finally, an IPsec packet (ESP) is sent on the wire


FORTINET