Hub and Spoke (concentrator mode) VPN configuration example

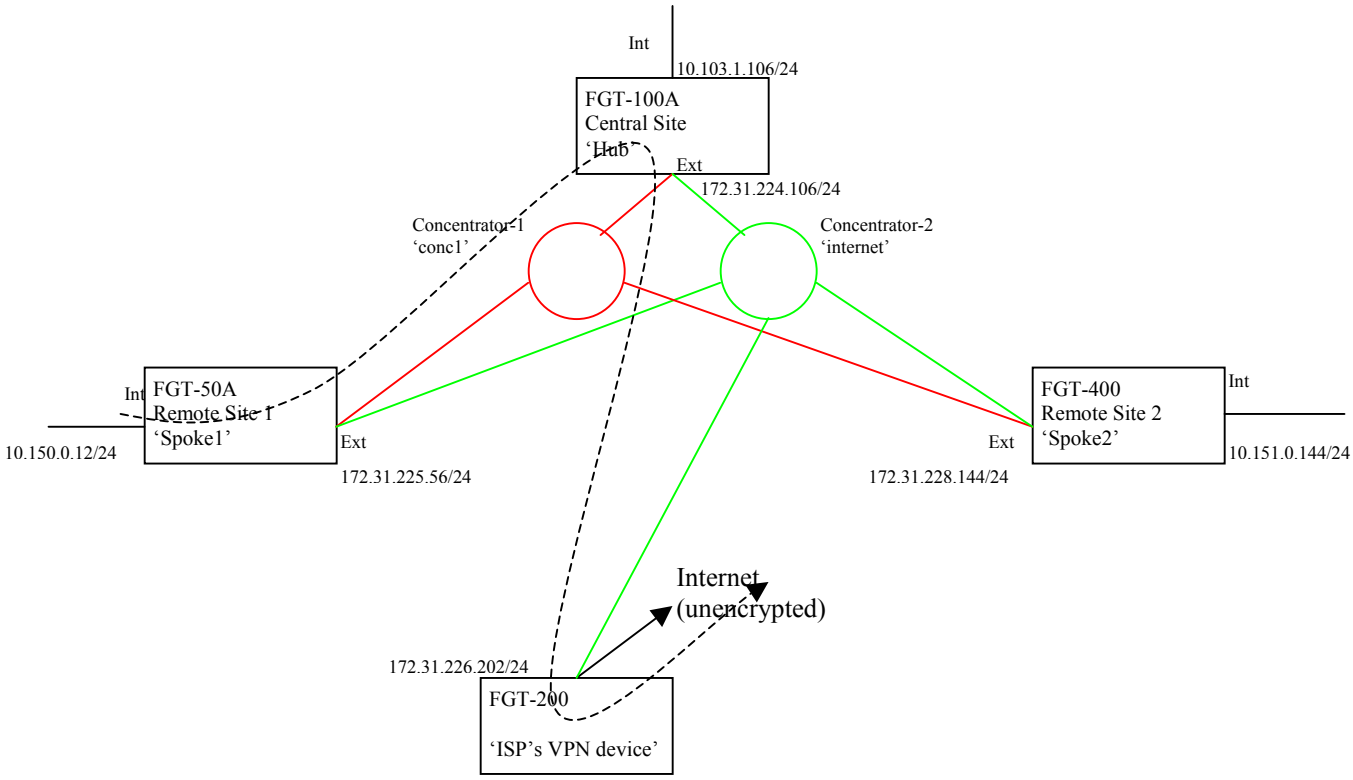
In a typical 'hub and spoke' configuration, the spokes have access to each other via the hub (also known as the Concentrator), and they also access the Internet via the hub. The hub therefore performs the antivirus, content control and any other filtering required for each remote site to access the Internet. The Hub's connection to the Internet is usually a regular (non-VPN) connection.

In this particular example, the hub's connection to the Internet is via another VPN connection. This requires certain changes to the setup, which are particular to this configuration. Particularly, the 'Internet Browsing' feature on the hub will not be used, and two different concentrators will also need to be configured.

Although Internet browsing is required from the remote sites (and this is what normally needs to be configured), this setting will not be required since the connection to the Internet is encrypted via another VPN. The hub's 'Internet Browsing' feature is required when the access to the Internet is not via another VPN.

The diagram below identifies the various IPSec Phase2 tunnels and concentrators (colored) that are required for this particular setup. The dashed line indicates the traffic flow path from a Spoke to the Internet.

Network setup example:



FortiGate configuration examples (v2.80MR10):

```
#### Central Unit (Hub) - FGT-100A

config system interface
    edit "internal"
        set ip 10.103.1.106 255.255.255.0
        set allowaccess ping https ssh telnet
    next
    edit "wan1"
        set ip 172.31.224.106 255.255.255.0
        set allowaccess ping https ssh telnet
config firewall address
    edit "all"
    next
    edit "int-net"
        set subnet 10.103.1.0 255.255.255.0
    next
    edit "fgt50a-int-net"
        set subnet 10.150.0.0 255.255.255.0
    next
    edit "fgt400-int-net"
        set subnet 10.151.0.0 255.255.255.0
    next
end
config vpn ipsec phase1
    edit "p1-fgt50a"
        set dpd enable
        set nattraversal enable
        set proposal 3des-sha1
        set remotegw 172.31.225.56
        set psksecret ENC 36jKHUy8NhVgj7lDuZ39Cq/
    edit "p1-fgt200"
        set dpd enable
        set nattraversal enable
        set proposal 3des-sha1
        set remotegw 172.31.226.202
        set psksecret ENC Ml9YX23BFlap62GrJqypm7IEz
    next
    edit "p1-fgt400"
        set dpd enable
        set nattraversal enable
        set proposal 3des-sha1
        set remotegw 172.31.228.144
        set psksecret ENC yvFdRQiipy/PibeH3eOuk85653/jUbMoy7+
    next
end
config vpn ipsec phase2
    edit "p2-fgt50a"
        set pfs enable
        set phase1name "p1-fgt50a"
        set proposal 3des-sha1
        set replay enable
    next
    edit "p2-fgt200"
        set pfs enable
        set phase1name "p1-fgt200"
        set proposal 3des-sha1
        set replay enable
    next
    edit "p2-fgt400"
        set concentrator "conc1"
        set pfs enable
        set phase1name "p1-fgt400"
        set proposal 3des-sha1
        set replay enable
    next
    edit "p2-fgt50a-internet"
        set concentrator "internet"
        set pfs enable
        set phase1name "p1-fgt50a"
        set proposal 3des-sha1
        set replay enable
    next
    edit "p2-fgt400-internet"
        set concentrator "internet"
        set pfs enable
        set phase1name "p1-fgt400"
        set proposal 3des-sha1
        set replay enable
```

```
    next
end
config vpn ipsec concentrator
    edit "conc1"
            set member "p2-fgt50a" "p2-fgt400"
    next
    edit "internet"
            set member "p2-fgt200" "p2-fgt50a-internet" "p2-fgt400-internet"
    next
end
config firewall policy
    edit 2
        set srcintf "internal"
        set dstintf "wan1"
        set srcaddr "int-net"
        set dstaddr "fgt50a-int-net"
        set action encrypt
        set schedule "always"
        set service "ANY"
        set inbound enable
        set outbound enable
        set vpntunnel "p2-fgt50a"
    next
    edit 5
        set srcintf "internal"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "fgt50a-int-net"
        set action encrypt
        set schedule "always"
        set service "ANY"
        set inbound enable
        set outbound enable
        set vpntunnel "p2-fgt50a-internet"
    next
    edit 4
        set srcintf "internal"
        set dstintf "wan1"
        set srcaddr "int-net"
        set dstaddr "fgt400-int-net"
        set action encrypt
        set schedule "always"
        set service "ANY"
        set inbound enable
        set outbound enable
        set natinbound enable
        set vpntunnel "p2-fgt400"
    next
    edit 6
        set srcintf "internal"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "fgt400-int-net"
        set action encrypt
        set schedule "always"
        set service "ANY"
        set inbound enable
        set outbound enable
        set vpntunnel "p2-fgt400-internet"
    next
    edit 3
        set srcintf "internal"
        set dstintf "wan1"
        set srcaddr "int-net"
        set dstaddr "all"
        set action encrypt
        set schedule "always"
        set service "ANY"
        set inbound enable
        set outbound enable
        set vpntunnel "p2-fgt200"
    next
end

config router static
    edit 1
        set device "wan1"
        set gateway 172.31.224.254
    next
end
```

Spoke 1 - FGT-50A

```
config system interface
    edit "internal"
        set ip 10.150.0.56 255.255.255.0
        set allowaccess ping https ssh telnet
    next
    edit "external"
        set ip 172.31.225.56 255.255.255.0
        set allowaccess ping https ssh telnet
    next
end
config firewall address
    edit "all"
    next
    edit "central"
        set subnet 10.103.1.0 255.255.255.0
    next
    edit "int-net"
        set subnet 10.150.0.12 255.255.255.0
    next
    edit "fgt400-int"
        set subnet 10.151.0.0 255.255.255.0
    next
end
config vpn ipsec phase1
    edit "p1-fgt100a"
        set dpd enable
        set nattraversal enable
        set proposal 3des-sha1
        set remotegw 172.31.224.106
        set psksecret ENC zYCSJDY+NcGcvVO6DnMxG7AkQkMGz
    next
end
config vpn ipsec phase2
    edit "p2-fgt100a"
        set pfs enable
        set phase1name "p1-fgt100a"
        set proposal 3des-sha1
        set replay enable
    next
    edit "p2-fgt100a-internet"
        set pfs enable
        set phase1name "p1-fgt100a"
        set proposal 3des-sha1
        set replay enable
    next
end
config firewall addrgrp
    edit "central-and-fgt400"
            set member "central" "fgt400-int"
    next
end
config firewall policy
    edit 2
        set srcintf "internal"
        set dstintf "external"
        set srcaddr "int-net"
        set dstaddr "central-and-fgt400"
        set action encrypt
        set schedule "always"
        set service "ANY"
        set inbound enable
        set outbound enable
        set vpntunnel "p2-fgt100a"
    next
    edit 3
        set srcintf "internal"
        set dstintf "external"
        set srcaddr "int-net"
        set dstaddr "all"
        set action encrypt
        set schedule "always"
        set service "ANY"
        set inbound enable
        set outbound enable
        set vpntunnel "p2-fgt100a-internet"
    next
end
```

```
config router static
    edit 1
        set device "external"
        set gateway 172.31.225.254
    next
end



#### Spoke 2 - FGT-400

config system interface
    edit "port1"
        set ip 10.151.0.144 255.255.255.0
        set allowaccess ping https ssh telnet
    next
    edit "port2"
        set ip 172.31.228.144 255.255.255.0
        set allowaccess ping https ssh telnet
    next
end

config firewall address
    edit "all"
    next
    edit "central"
        set subnet 10.103.1.0 255.255.255.0
    next
    edit "int-net"
        set subnet 10.151.0.0 255.255.255.0
    next
    edit "fgt50a-int"
        set subnet 10.150.0.0 255.255.255.0
    next
end
config vpn ipsec phase1
    edit "p1-fgt100a"
        set dpd enable
        set nattraversal enable
        set proposal 3des-sha1
        set remotegw 172.31.224.106
        set psksecret ENC vsd5BBvu9D8ZRZHk3Inaxg4aCEodd0lAv6sGhc
    next
end
config vpn ipsec phase2
    edit "p2-fgt100a"
        set pfs enable
        set phase1name "p1-fgt100a"
        set proposal 3des-sha1
        set replay enable
    next
    edit "p2-fgt100-internet"
        set pfs enable
        set phase1name "p1-fgt100a"
        set proposal 3des-sha1
        set replay enable
    next
end
config firewall addrgrp
    edit "central-and-fgt50a"
            set member "central" "fgt50a-int"
    next
end
config firewall policy
    edit 1
        set srcintf "port1"
        set dstintf "port2"
        set srcaddr "int-net"
        set dstaddr "central-and-fgt50a"
        set action encrypt
        set schedule "always"
        set service "ANY"
        set inbound enable
        set outbound enable
        set vpntunnel "p2-fgt100a"
    next
    edit 2
        set srcintf "port1"
        set dstintf "port2"
        set srcaddr "int-net"
        set dstaddr "all"
```

```
        set action encrypt
        set schedule "always"
        set service "ANY"
        set inbound enable
        set outbound enable
        set vpntunnel "p2-fgt100-internet"
    next
end
config router static
    edit 1
        set device "port2"
        set gateway 172.31.228.254
    next
end
```