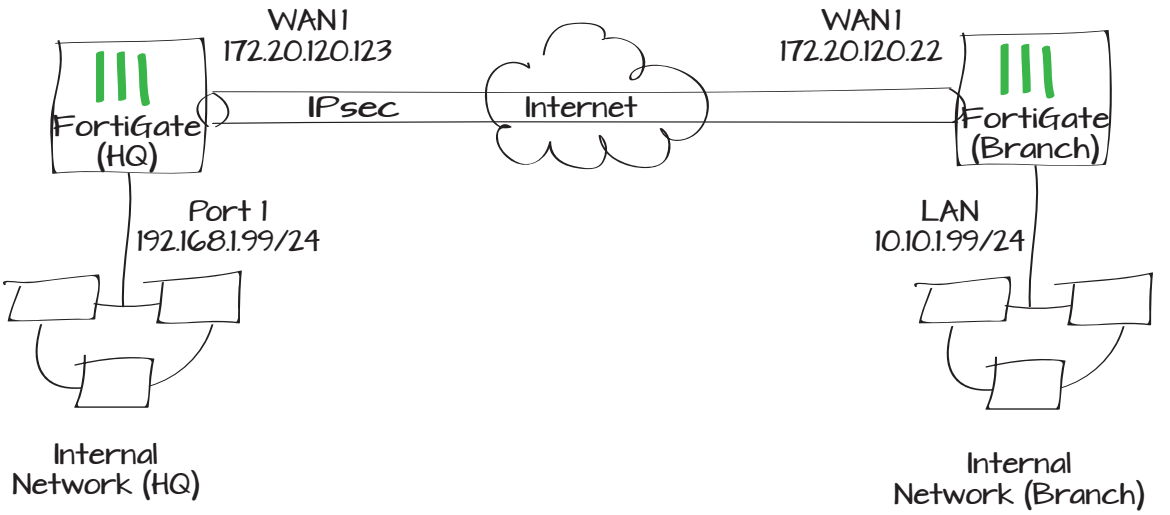
Using IPsec VPN to provide communication between offices

This example provides secure, transparent communication between two FortiGates located at different offices using route-based IPsec VPN. In this example, one office will be referred to as HQ and the other will be referred to as Branch.

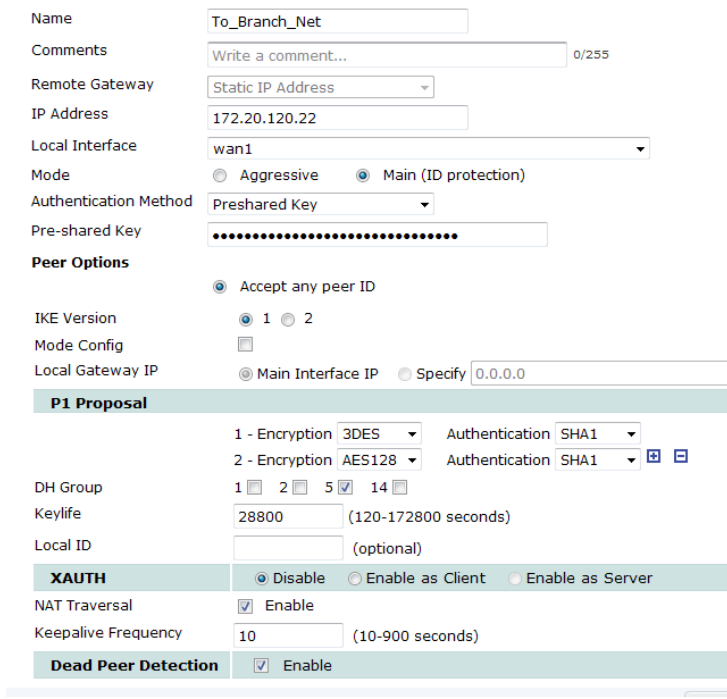
1. Configuring the HQ IPsec VPN
2. Adding firewall addresses for the local and remote LAN on HQ
3. Creating an HQ security policy and static route
4. Configure the Branch IPsec VPN Phase 1 and Phase 2 settings
5. Add Branch firewall addresses for the local and remote LAN
6. Create a branch IPsec security policy and static route
7. Results



Configuring the HQ's IPsec VPN

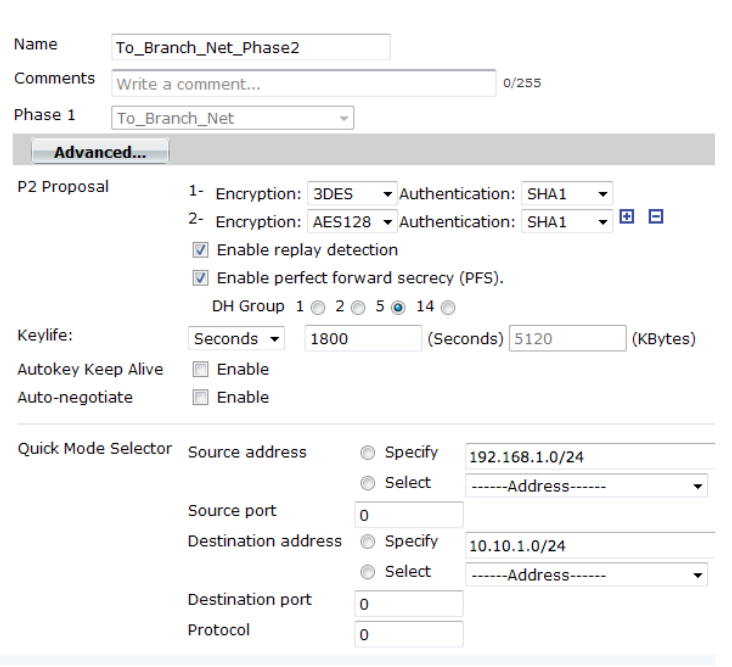
On the HQ FortiGate, go to **VPN > IPsec > Auto Key (IKE)**.

Select **Create Phase 1**. Set **IP Address** to the IP of the Branch FortiGate, **Local Interface** to the Internet-facing interface, and enter a **Pre-shared Key**.



Now select **Create Phase 2,** set it to use the new Phase 1, and expand the **Advanced** options.

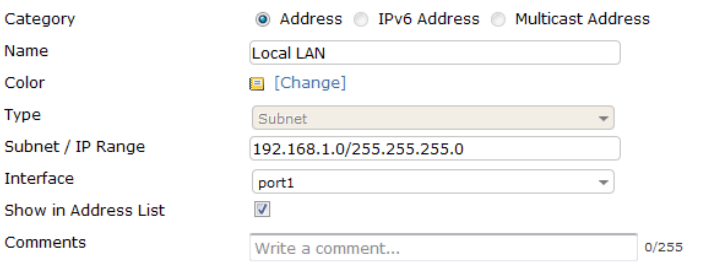
Specify **Source address** as the HQ subnet and **Destination address** as the Branch subnet.



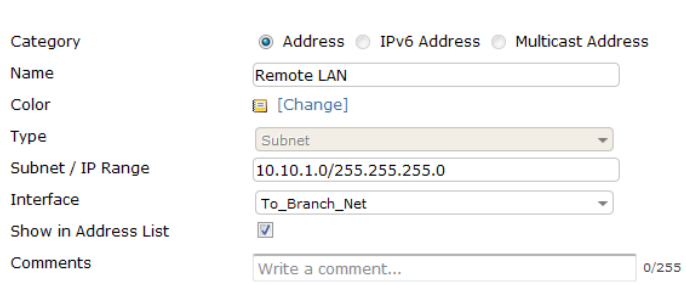
Adding firewall addresses for the local and remote LAN on HQ

Go to **Firewall Objects > Address > Addresses**.

Create a local address. Set **Type** to **Subnet**, **Subnet/IP Range** to the HQ subnet, and **Interface** to an internal port.



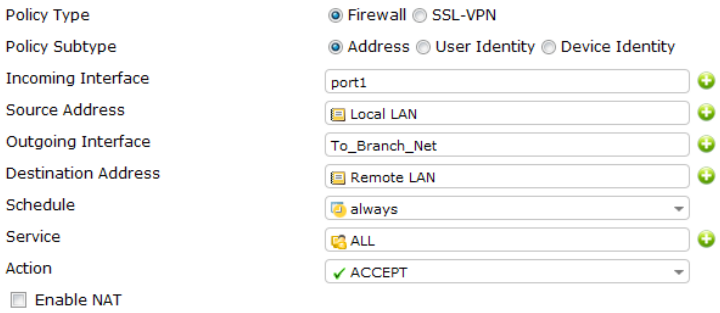
Create a remote LAN address. Set **Type** to **Subnet**, **Subnet/IP Range** to the Branch subnet, and **Interface** to the VPN Phase 1.



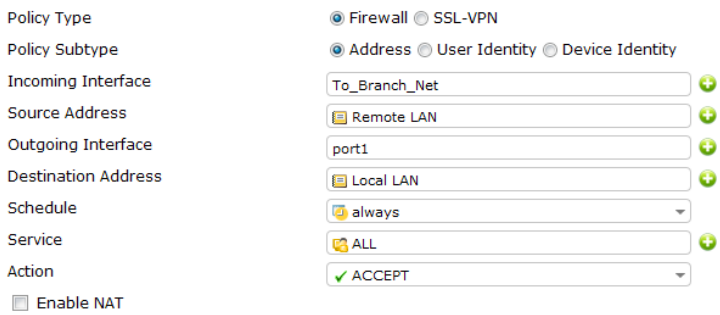
Creating an HQ security policy and static route.

Go to **Policy > Policy > Policy**.

Create a policy for outbound traffic. Set **Incoming Interface** to an internal port, **Source Address** to the local address, **Outgoing Interface** to the VPN Phase 1, and **Destination Address** to the remote LAN address.



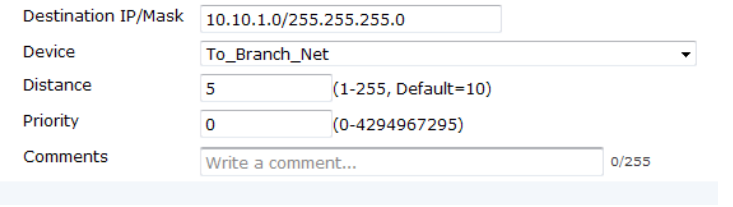
Create a second policy for inbound traffic. Set **Incoming Interface** to the VPN phase 1, **Source Address** to the local address, **Outgoing Interface** to an internal port, and **Destination Address** to the local address.



Go to **Router > Static > Static Routes**.

Create a route for IPsec traffic, setting **Device** to the VPN Phase 1.

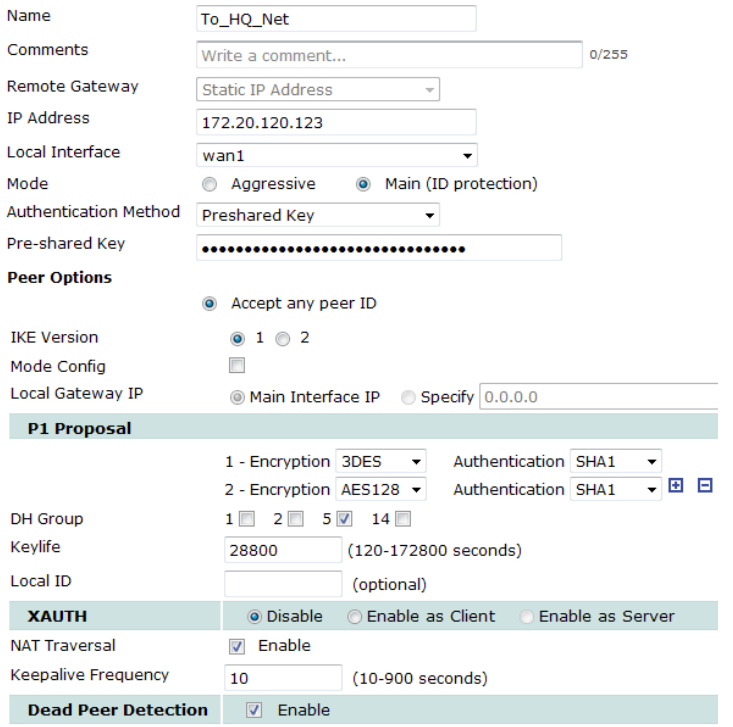
If the **Router** menu is not visible, go to **System > Config > Features** to ensure that **Advanced Routing** is turned on.



Configuring the Branch's IPsec VPN

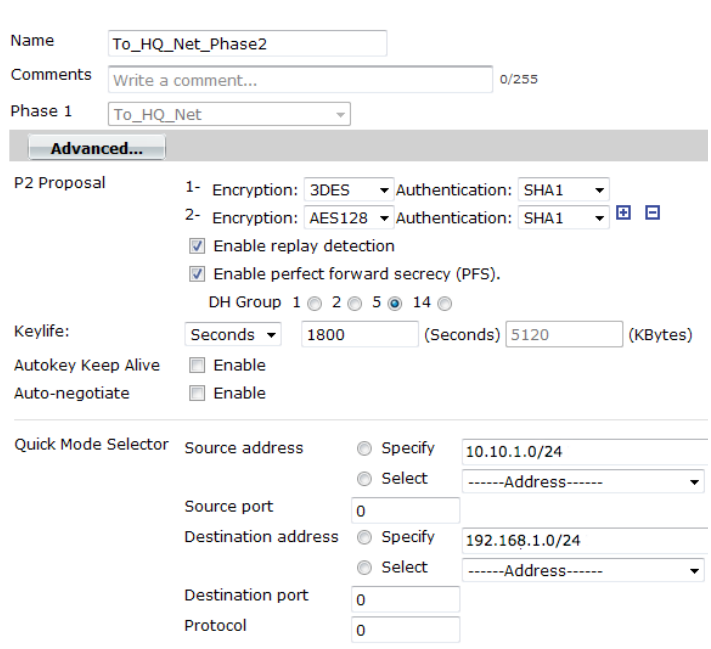
One the Branch FortiGate, Go to **VPN > IPsec > Auto Key (IKE)**.

Select **Create Phase 1**. Set **IP Address** to the IP of the HQ FortiGate, **Local Interface** to the Internet-facing interface, and enter the same **Pre-shared Key** used previously.



Now select **Create Phase 2,** set it to use the new Phase 1, and expand the **Advanced** options.

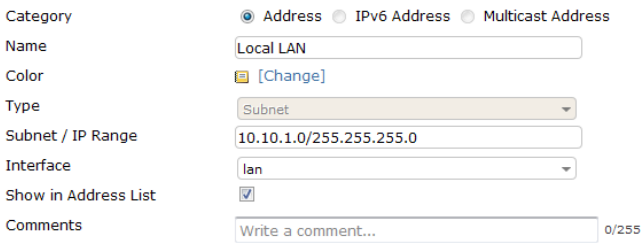
Specify **Source address** as the Branch subnet and **Destination address** as the HQ subnet.



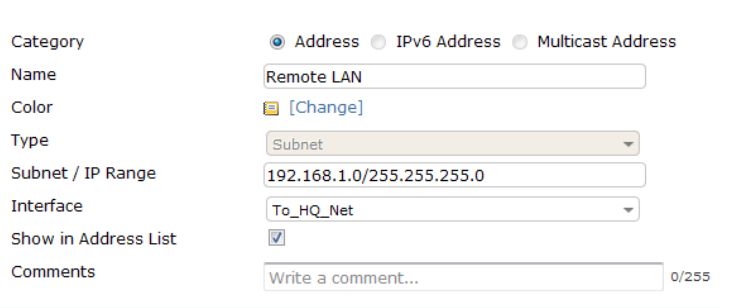
Adding firewall addresses for the local and remote LAN on HQ

Go to **Firewall Objects > Address > Addresses.**

Create a local address. Set **Type** to **Subnet**, **Subnet/IP Range** to the Branch subnet, and **Interface** to an internal port.



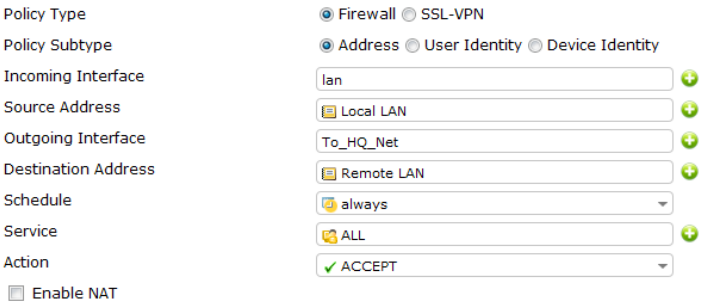
Create a remote LAN address. Set **Type** to **Subnet**, **Subnet/IP Range** to the HQ subnet, and **Interface** to the VPN Phase 1.



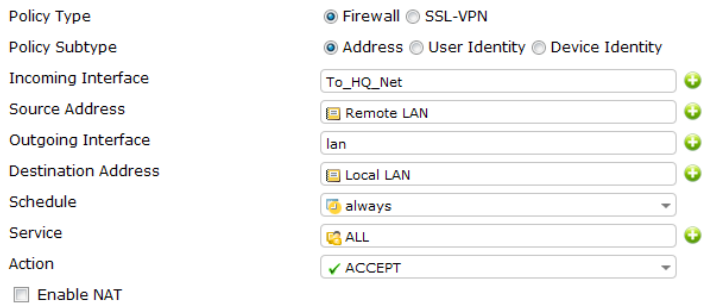
Creating an HQ security policy and static route.

Go to **Policy > Policy > Policy**.

Create a policy for outbound traffic. Set **Incoming Interface** to an internal port, **Source Address** to the local address, **Outgoing Interface** to the VPN Phase 1, and **Destination Address** to the remote LAN address.

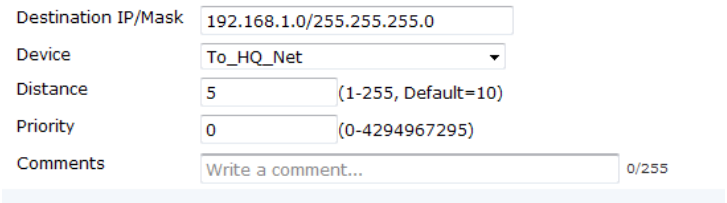


Create a second policy for inbound traffic. Set **Incoming Interface** to the VPN phase 1, **Source Address** to the local address, **Outgoing Interface** to an internal port, and **Destination Address** to the local address.



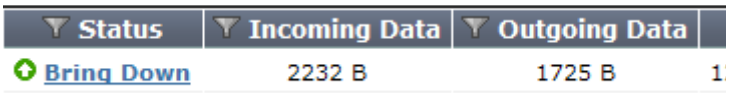
Go to **Router > Static > Static Routes**.

Create a route for IPsec traffic, setting **Device** to the VPN Phase 1.



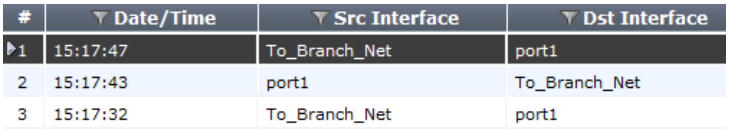
Results

Go to **VPN > Monitor > IPSec Monitor** to verify the status of the VPN tunnel. It should be up.



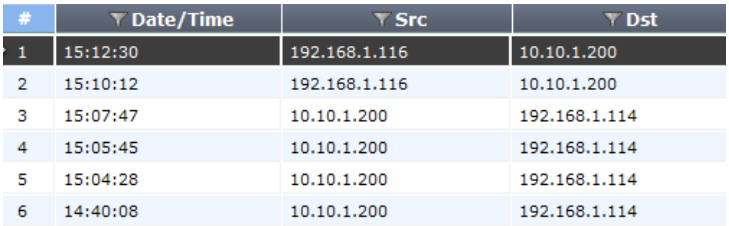
A user on either of the office networks should be able to connect to any address on the other office network transparently.

From the HQ FortiGate unit go to **Log & Report > Traffic Log > Forward Traffic** to verify that both inbound and outbound traffic is occurring**.**



#	Date/Time	Src Interface	Dst Interface
1	15:17:47	To_Branch_Net	port1
2	15:17:43	port1	To_Branch_Net
3	15:17:32	To_Branch_Net	port1

To verify traffic on the Branch FortiGate unit as well, go to **Log & Report > Traffic Log > Forward Traffic.**



#	Date/Time	Src	Dst
1	15:12:30	192.168.1.116	10.10.1.200
2	15:10:12	192.168.1.116	10.10.1.200
3	15:07:47	10.10.1.200	192.168.1.114
4	15:05:45	10.10.1.200	192.168.1.114
5	15:04:28	10.10.1.200	192.168.1.114
6	14:40:08	10.10.1.200	192.168.1.114