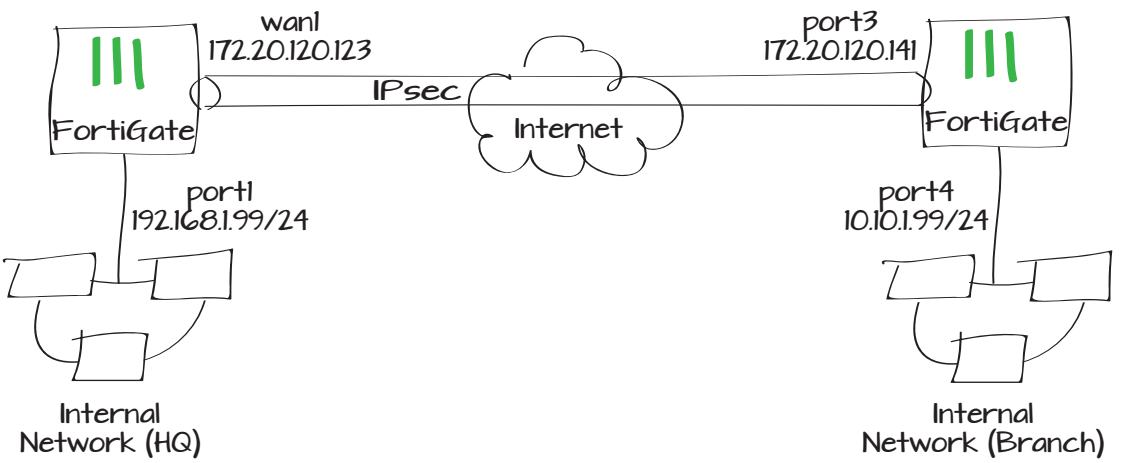
Using policy-based IPsec VPN for communication between offices

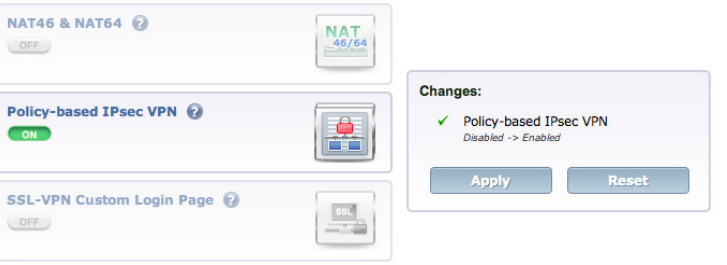
This example uses policy-based IPsec VPN, and assumes that both offices have connections to the Internet with static IP addresses. In this example, one FortiGate unit will be called HQ and the other will be called Branch.

1. Enabling policy-based VPN on the HQ FortiGate unit
2. Configuring the HQ IPsec VPN Phase 1 and Phase 2 settings
3. Adding the HQ firewall addresses for the local and remote LAN
4. Creating an HQ IPsec security policy
5. Configuring the Branch IPsec VPN Phase 1 and Phase 2 settings
6. Adding Branch firewall addresses for the local and remote LAN
7. Creating a branch IPsec security policy
8. Results



Enabling policy-based VPN on the HQ FortiGate unit

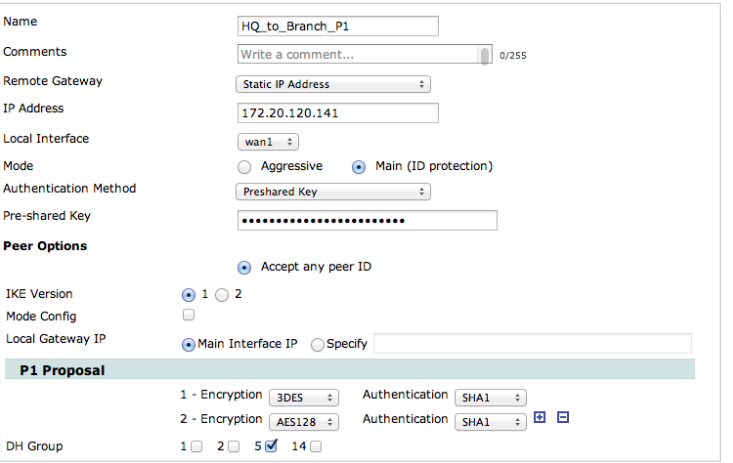
Go to **System > Config > Features**. Select **Show More** and turn on **Policy-based IPsec VPN**.



Configuring the HQ IPsec VPN Phase1 and Phase 2 settings

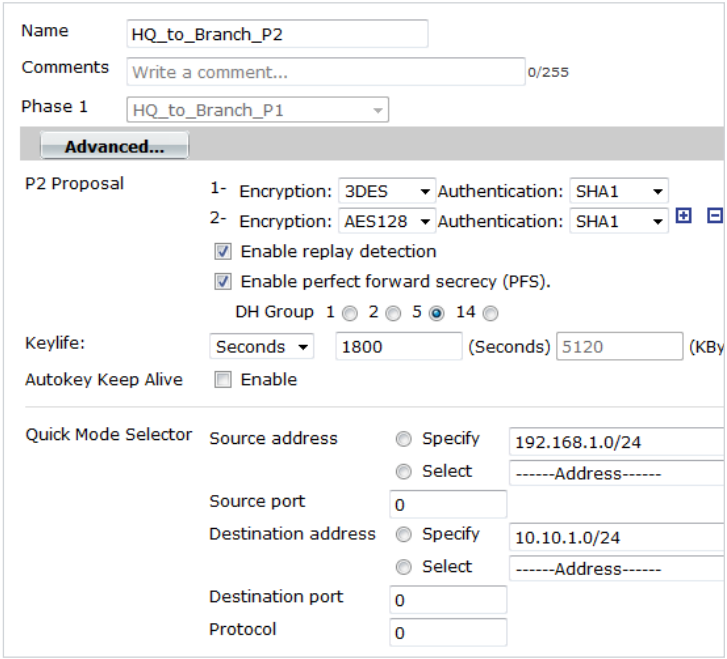
Go to **VPN > IPsec > Auto Key (IKE)**.

Select **Create Phase 1**. Set **IP Address** to the IP of the Branch FortiGate, **Local Interace** 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.

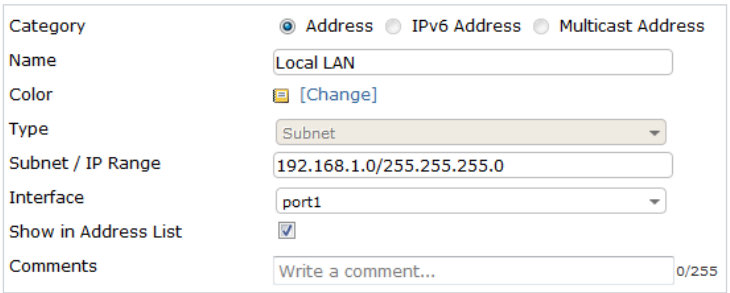
Specify **Source address** as the HQ subnet and **Destination address** as the Branch subnet.



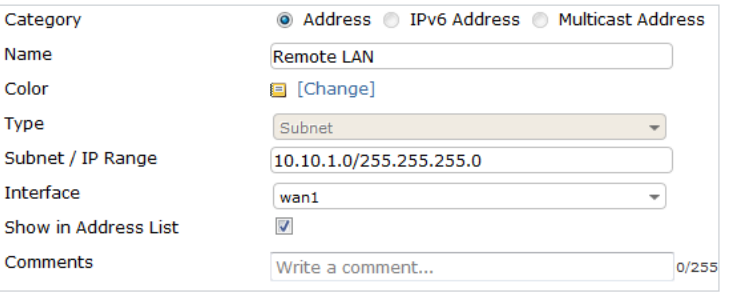
Adding HQ addresses for the local and remote LAN on the HQ FortiGate unit

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

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 Internet-facing interface.

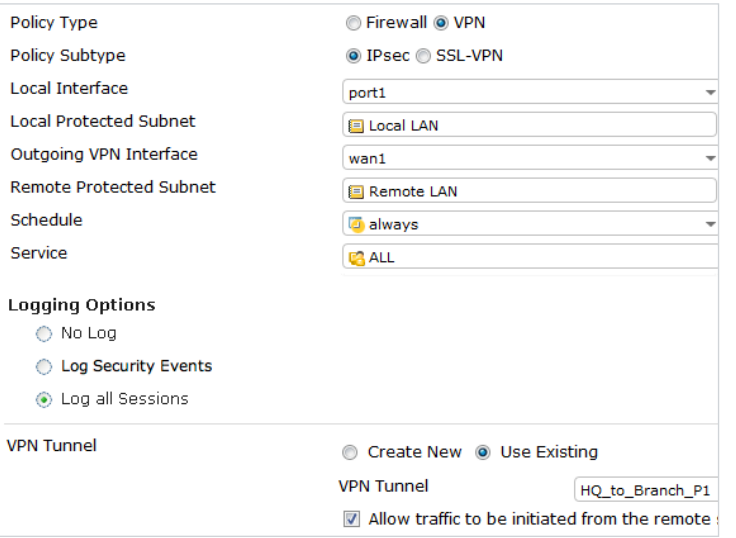


Creating an HQ IPsec security policy

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

Create a new policy. Set **Type** to **VPN** and **Subtype** to **IPsec**. Configure the policy to allow traffic from the local interface to pass through the outgoing VPN interface (in the example, wan1) using the VPN tunnel created in Phase 1.

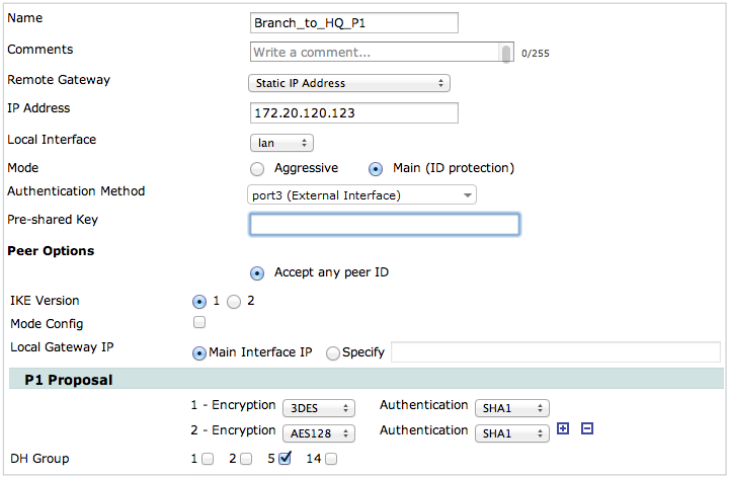
When the policy is created, ensure that it is placed at the top of the policy list by clicking on the policy sequence number and dragging the row to the top of the policy table.



Configuring the Branch IPsec VPN Phase 1 and Phase 2 settings

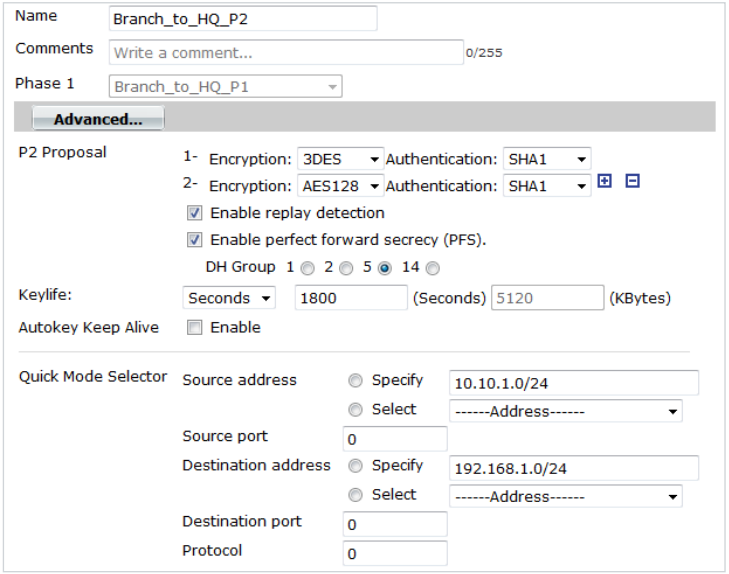
Go to **VPN > IPsec > Auto Key (IKE)**.

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



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

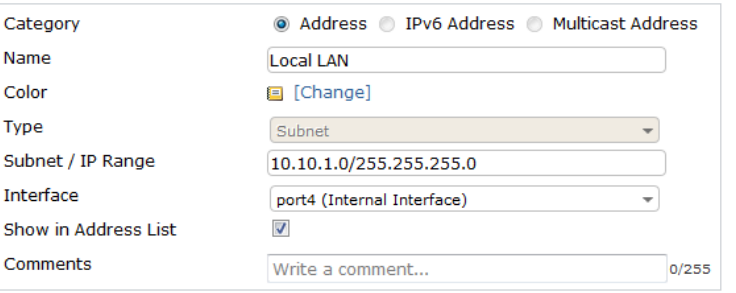
Specify **Source address** as the Branch subnet and **Destination address** as the HQ subnet.



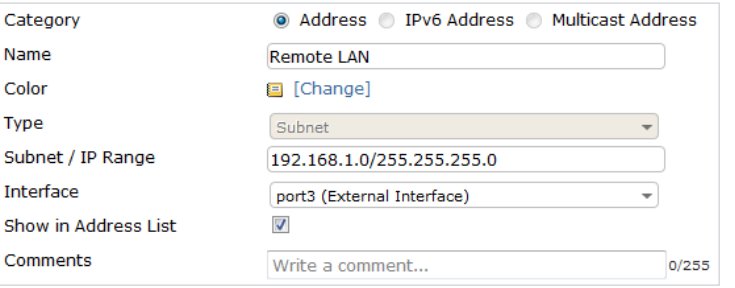
Adding Branch addresses for the local and remote LAN on the HQ FortiGate unit

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

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 Internet-facing interface.

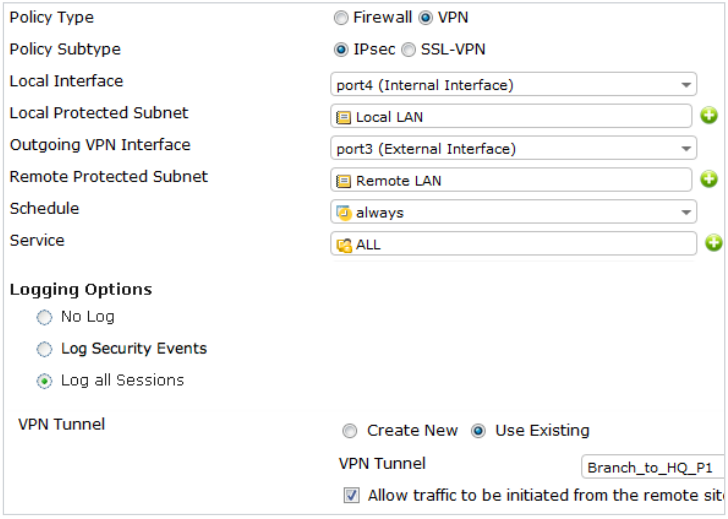


Creating a Branch IPsec security policy

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

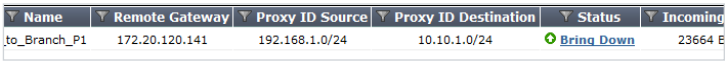
Create a new policy. Set **Type** to **VPN** and **Subtype** to **IPsec**. Configure the policy to allow traffic from the local interface to pass through the outgoing VPN interface (in the example, wan1) using the VPN tunnel created in Phase 1.

When the policy is created, ensure that it is placed at the top of the policy list by clicking on the policy sequence number and dragging the row to the top of the policy table.



Results

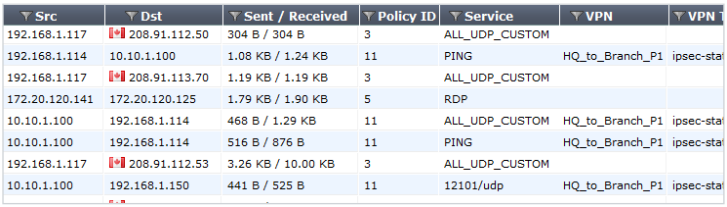
Go to **VPN > Monitor > IPSec Monitor** to verify the status of the VPN tunnel. It should be up.



Name	Remote Gateway	Proxy ID Source	Proxy ID Destination	Status	Incoming
to_Branch_P1	172.20.120.141	192.168.1.0/24	10.10.1.0/24	Bring Down	23664 B

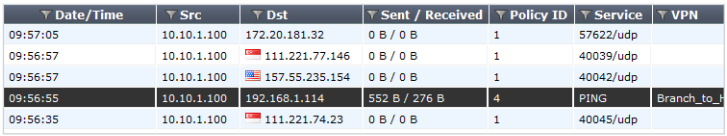
A user on either of the office networks should be able to connect to any address on the other office network transparently.

From the HQ FortiGate unit go to **Log & Report > Traffic Log > Forward Traffic.**



Src	Dst	Sent / Received	Policy ID	Service	VPN	VPN T
192.168.1.117	208.91.112.50	304 B / 304 B	3	ALL_UDP_CUSTOM		
192.168.1.114	10.10.1.100	1.08 KB / 1.24 KB	11	PING	HQ_to_Branch_P1	ipsec-sta
192.168.1.117	208.91.113.70	1.19 KB / 1.19 KB	3	ALL_UDP_CUSTOM		
172.20.120.141	172.20.120.125	1.79 KB / 1.90 KB	5	RDP		
10.10.1.100	192.168.1.114	468 B / 1.29 KB	11	ALL_UDP_CUSTOM	HQ_to_Branch_P1	ipsec-sta
10.10.1.100	192.168.1.114	516 B / 876 B	11	PING	HQ_to_Branch_P1	ipsec-sta
192.168.1.117	208.91.112.53	3.26 KB / 10.00 KB	3	ALL_UDP_CUSTOM		
10.10.1.100	192.168.1.150	441 B / 525 B	11	12101/udp	HQ_to_Branch_P1	ipsec-sta

From the Branch FortiGate unit go to **Log & Report > Traffic Log > Forward Traffic.**



Date/Time	Src	Dst	Sent / Received	Policy ID	Service	VPN
09:57:05	10.10.1.100	172.20.181.32	0 B / 0 B	1	57622/udp	
09:56:57	10.10.1.100	111.221.77.146	0 B / 0 B	1	40039/udp	
09:56:57	10.10.1.100	157.55.235.154	0 B / 0 B	1	40042/udp	
09:56:55	10.10.1.100	192.168.1.114	552 B / 276 B	4	PING	Branch_to_H
09:56:35	10.10.1.100	111.221.74.23	0 B / 0 B	1	40045/udp	