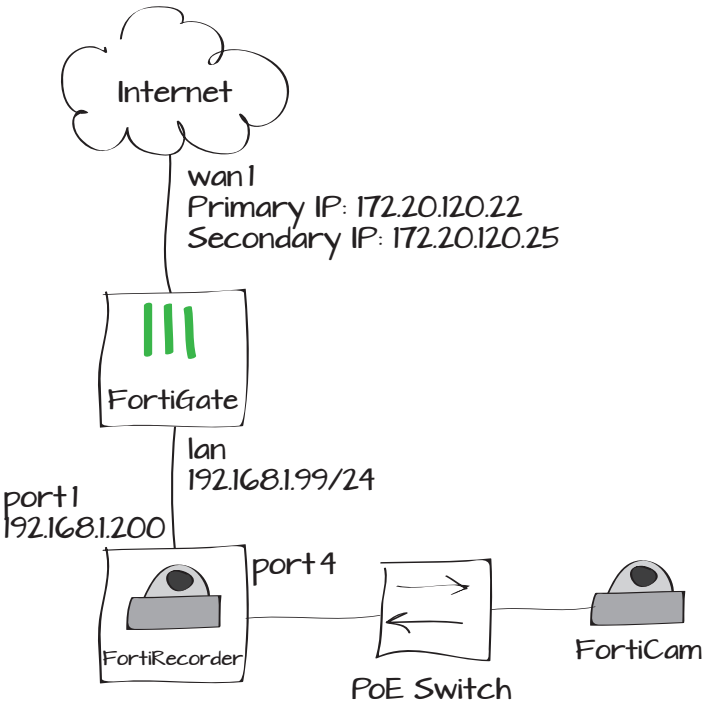
Allowing access from the Internet to a FortiCamera unit

This example sets up a FortiRecorder unit and FortiCamera unit for use with a FortiGate unit. It also allows the FortiCamera unit, which is located on the internal network, to be accessed from the Internet

1. Configuring the FortiRecorder and FortiCamera units
2. Configuring the FortiGate unit's interfaces
3. Adding virtual IPs
4. Adding a security policy to allow access to the FortiCamera
5. Results

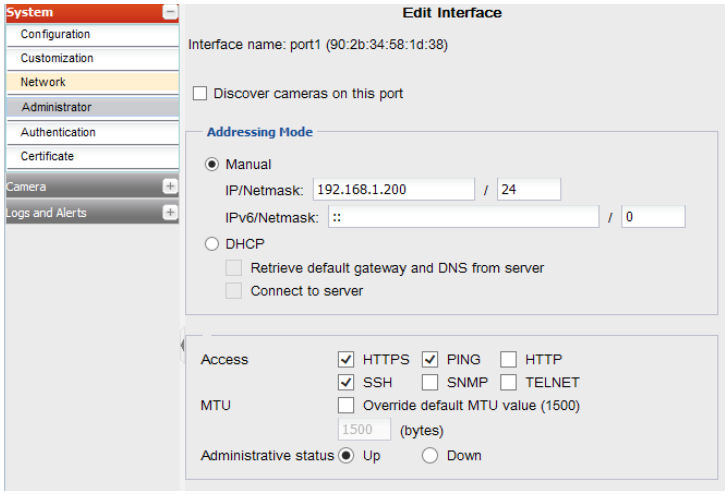


Configuring the FortiRecorder and FortiCamera units

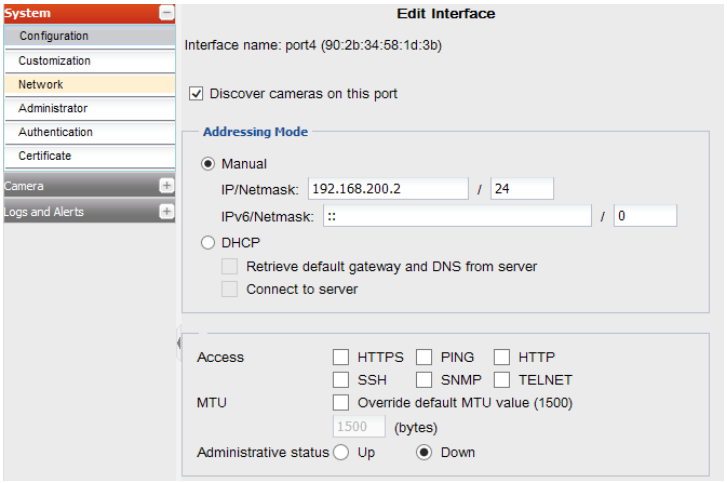
Connect locally to the FortiRecorder.

Go to **System > Network > Interface**.

Set an IP address for port1.

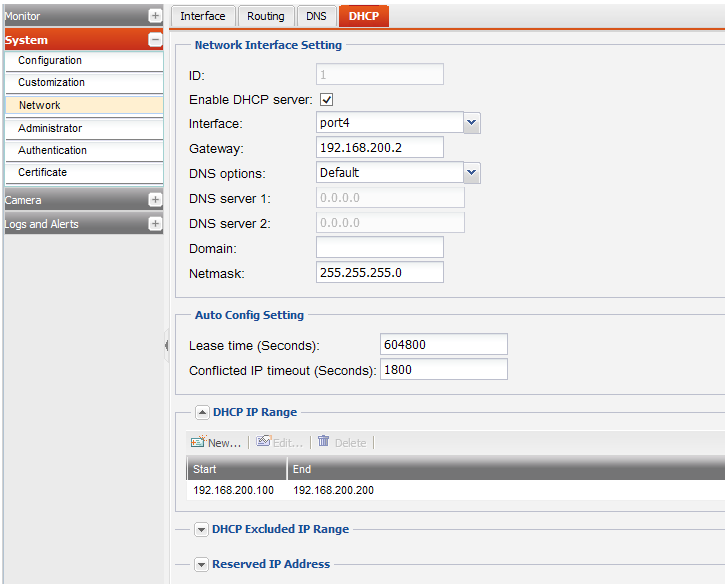


Set an IP address for port4.



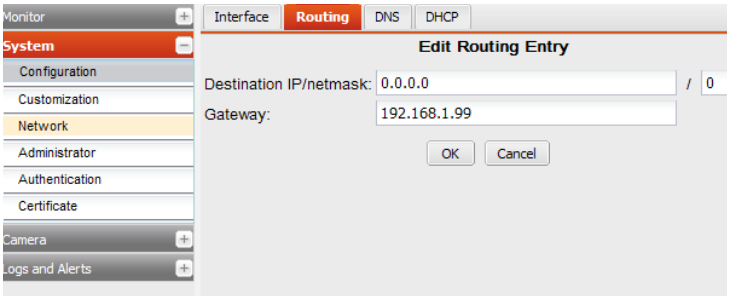
Go to **System > Network > DHCP**.

Create a DHCP server on port4 to lease IPs to FortiCamera.



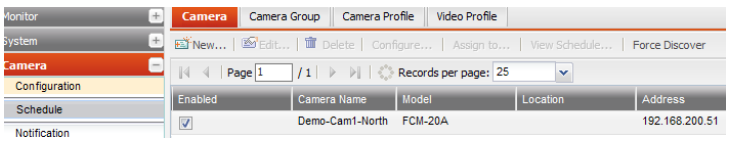
Go to **System > Network > Routing.**

Add a default route.



Go to **Camera > Configuration > Camera**.

Click on **Force Discover** to have connected cameras displayed.

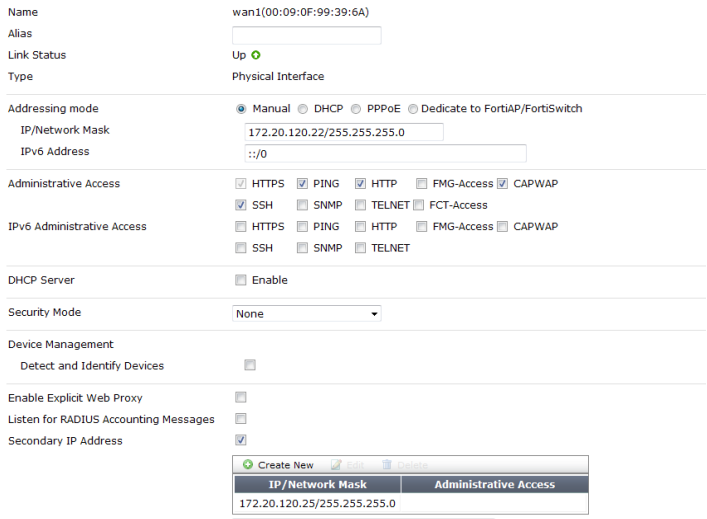


Configuring the FortiGate unit's interfaces

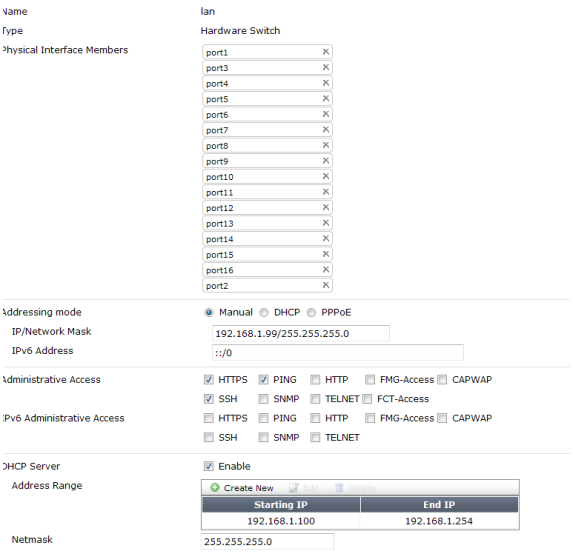
Go to **System > Network > Interfaces**.

Configure your Internet-facing interface. Select **Secondary IP Address** and create a new IP/Network Mask for the interface.

Adding a secondary IP address adds multiple IP addresses to the interface. The FortiGate unit, static and dynamic routing, and the network see the secondary IP addresses as additional IP addresses that terminate at the interface.



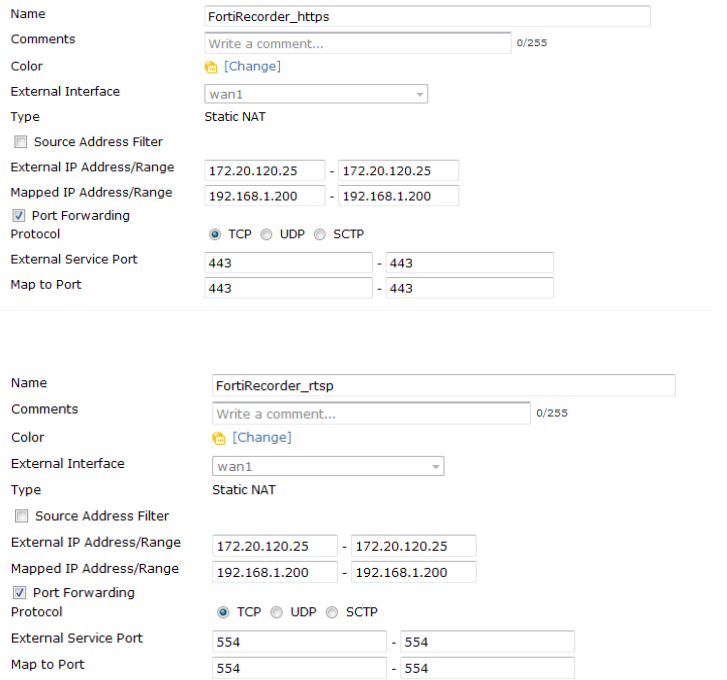
Configure the **lan** interface. Enable **DHCP Server** and create a new IP range.



Adding virtual IPs

Go to **Firewall Objects >Virtual IPs > Virtual IPs.**

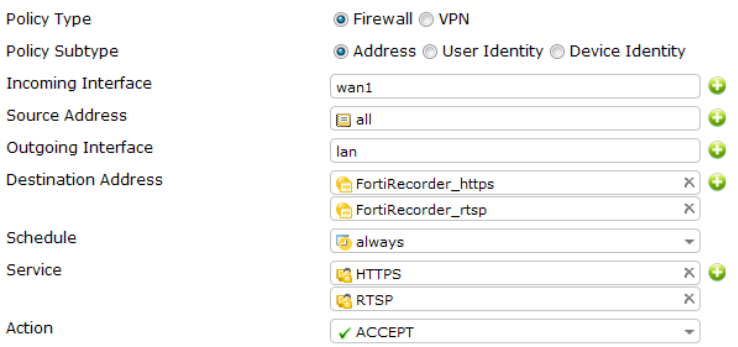
Create the two virtual IPs: one for HTTPS traffic and one for RTSP traffic. For both virtual IPs, set **External IP Address/ Range** to the secondary IP of the Internet-facing interface and the **Mapped IP Address/Range** to the IP of port1 on the FortiRecorder unit.



Adding a security policy

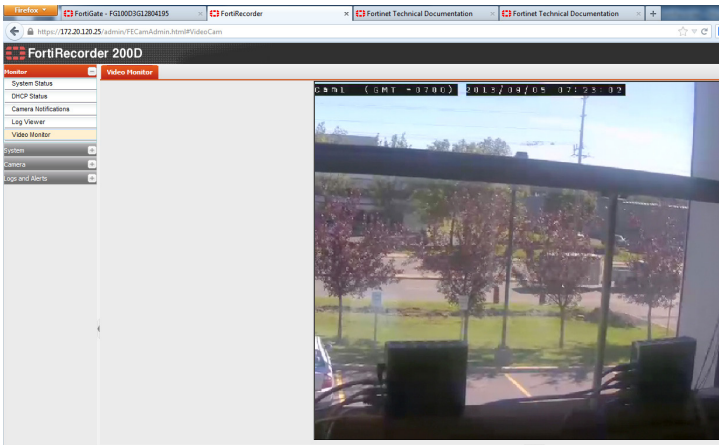
Go to **Policy > Policy > Policy**.

Create a policy allowing access to the FortiRecorder from the Internet. Set **Incoming Interface** to your Internet-facing interface, **Outgoing Interface** to lan, and **Destination Address** to the new virtual IPs.



Results

From the Internet, go to the IP address of the FortiGate unit's secondary IP (in the example, https://172.20.120.25) and you should be able to see securely live video feed using HTTPS and RTSP (Real Time Streaming Protocol)



Go to **Log & Report > Traffic > Forward Traffic.**

Verify https and RTSP traffic trough the FortiGate

Dst	Src Interface	Dst Interface	Service
172.20.120.25	wan1	lan	HTTPS
172.20.120.25	wan1	lan	HTTPS
172.20.120.25	wan1	lan	HTTPS
172.20.120.25	wan1	lan	HTTPS
172.20.120.25	wan1	lan	HTTPS
172.20.120.25	wan1	lan	HTTPS
172.20.120.25	wan1	lan	RTSP
172.20.120.21	lan	wan1	RTSP
172.20.120.25	wan1	lan	RTSP
172.20.120.25	wan1	lan	HTTPS
172.20.120.25	wan1	lan	HTTPS
172.20.120.25	wan1	lan	HTTPS
172.20.120.25	wan1	lan	HTTPS

Select an entry for details.

Application Details		**Date/Time**	10:28:03 (1378376883)
Destination Country	Reserved	**Dst**	172.20.120.25
Dst Interface	lan	**Dst NAT IP**	192.168.1.200
Dst NAT Port	554	**Dst Port**	554
Duration	5899	**Level**	notice
Log ID	13	**Policy ID**	5
Protocol	6	**Received**	1617
Received Packets	8	**Sent**	1819
Sent / Received	1.78 KB / 1.58 KB	**Sent Packets**	9
Sequence Number	25233	**Service**	RTSP
Source Country	Reserved	**Src**	172.20.120.21
Src Interface	wan1	**Src Port**	63004
Status	close	**Sub Type**	forward
Threat		**Timestamp**	September-05-13 10:28:03 AM
Tran Display	dnat	**Virtual Domain**	root