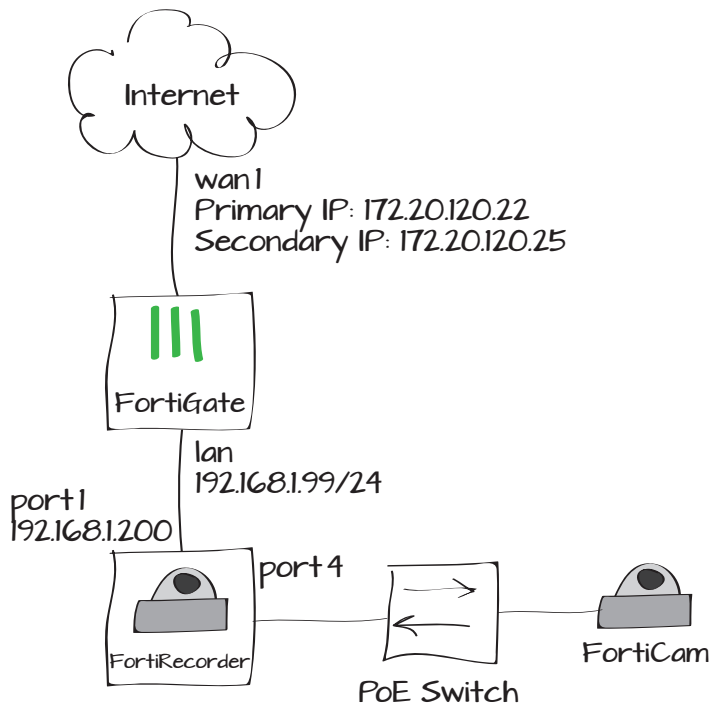


Allowing access from the Internet to a FortiCamera unit

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.

The screenshot shows the 'Edit Interface' configuration page for 'port1 (90:2b:34:58:1d:38)'. The left sidebar shows the 'System' menu with 'Network' selected. The main content area includes the following settings:

- Interface name: port1 (90:2b:34:58:1d:38)
- Discover cameras on this port
- Addressing Mode:**
 - Manual
 - IP/Netmask: 192.168.1.200 / 24
 - IPv6/Netmask: :: / 0
 - DHCP
 - Retrieve default gateway and DNS from server
 - Connect to server

Access settings:

- HTTPS PING HTTP
- SSH SNMP TELNET
- Override default MTU value (1500)

MTU: 1500 (bytes)

Administrative status: Up Down

Set an IP address for port4.

The screenshot shows the 'Edit Interface' configuration page for 'port4 (90:2b:34:58:1d:3b)'. The left sidebar shows the 'System' menu with 'Network' selected. The main content area includes the following settings:

- Interface name: port4 (90:2b:34:58:1d:3b)
- Discover cameras on this port
- Addressing Mode:**
 - Manual
 - IP/Netmask: 192.168.200.2 / 24
 - IPv6/Netmask: :: / 0
 - DHCP
 - Retrieve default gateway and DNS from server
 - Connect to server

Access settings:

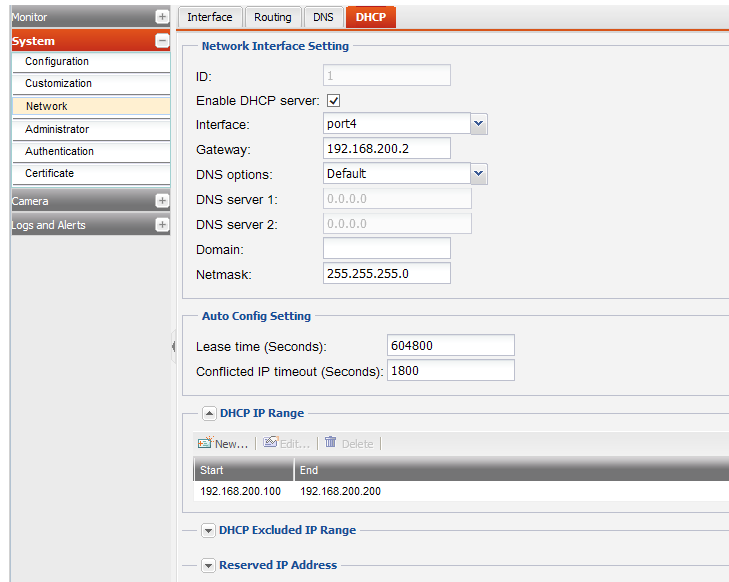
- HTTPS PING HTTP
- SSH SNMP TELNET
- Override default MTU value (1500)

MTU: 1500 (bytes)

Administrative status: Up Down

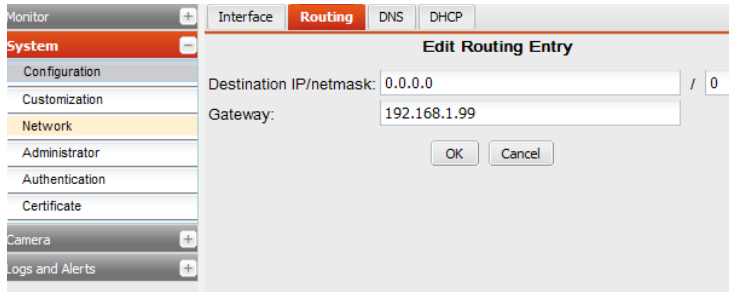
Go to **System > Network > DHCP**.

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



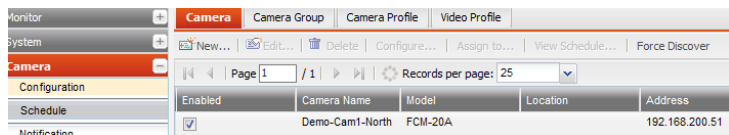
Go to **System > Network > Routing**.

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.

The image shows two screenshots of the FortiGate configuration interface. The top screenshot is for the 'wan1' interface, and the bottom screenshot is for the 'lan' interface.

wan1(00:09:0F:99:39:6A)
Alias: []
Link Status: Up []
Type: Physical Interface

Addressing mode: Manual DHCP PPPoE Dedicate to FortiAP/FortiSwitch

IP/Network Mask: 172.20.120.22/255.255.255.0
IPv6 Address: ::/0

Administrative Access: HTTPS PING HTTP FMG-Access CAPWAP
 SSH SNMP TELNET FCT-Access

IPv6 Administrative Access: HTTPS PING HTTP FMG-Access CAPWAP
 SSH SNMP TELNET

DHCP Server: Enable

Security Mode: None [v]

Device Management: Detect and Identify Devices

Enable Explicit Web Proxy: []
Listen for RADIUS Accounting Messages: []
Secondary IP Address: []

IP/Network Mask	Administrative Access
172.20.120.25/255.255.255.0	

lan
Type: Hardware Switch

Physical Interface Members: port1 [X], port3 [X], port4 [X], port5 [X], port6 [X], port7 [X], port8 [X], port9 [X], port10 [X], port11 [X], port12 [X], port13 [X], port14 [X], port15 [X], port16 [X], port2 [X]

Addressing mode: Manual DHCP PPPoE

IP/Network Mask: 192.168.1.99/255.255.255.0
IPv6 Address: ::/0

Administrative Access: HTTPS PING HTTP FMG-Access CAPWAP
 SSH SNMP TELNET FCT-Access

IPv6 Administrative Access: HTTPS PING HTTP FMG-Access CAPWAP
 SSH SNMP TELNET

DHCP Server: Enable

Address Range: [] []

Starting IP	End IP
192.168.1.100	192.168.1.254

Netmask: 255.255.255.0

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.

Name	FortiRecorder_https	
Comments	Write a comment...	0/255
Color	[Change]	
External Interface	wan1	
Type	Static NAT	
<input type="checkbox"/> Source Address Filter		
External IP Address/Range	172.20.120.25	- 172.20.120.25
Mapped IP Address/Range	192.168.1.200	- 192.168.1.200
<input checked="" type="checkbox"/> Port Forwarding		
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> SCTP	
External Service Port	443	- 443
Map to Port	443	- 443

Name	FortiRecorder_rtsp	
Comments	Write a comment...	0/255
Color	[Change]	
External Interface	wan1	
Type	Static NAT	
<input type="checkbox"/> Source Address Filter		
External IP Address/Range	172.20.120.25	- 172.20.120.25
Mapped IP Address/Range	192.168.1.200	- 192.168.1.200
<input checked="" type="checkbox"/> Port Forwarding		
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> SCTP	
External Service Port	554	- 554
Map to Port	554	- 554

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	wan1
Source Address	all
Outgoing Interface	lan
Destination Address	FortiRecorder_https FortiRecorder_rtsp
Schedule	always
Service	HTTPS RTSP
Action	ACCEPT

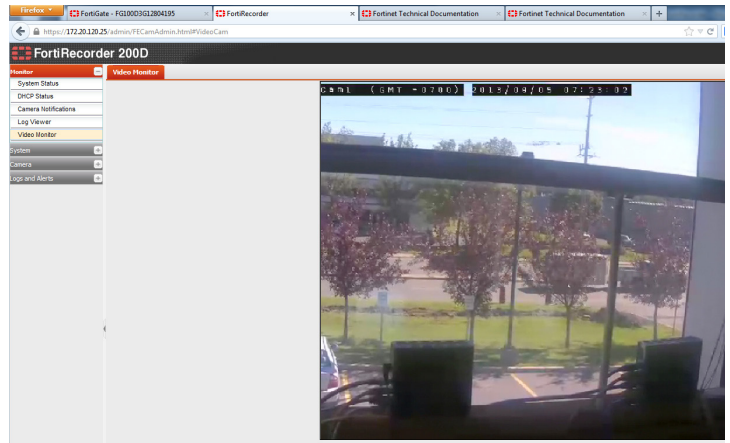
Results

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 through the FortiGate

Select an entry for details.



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	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

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