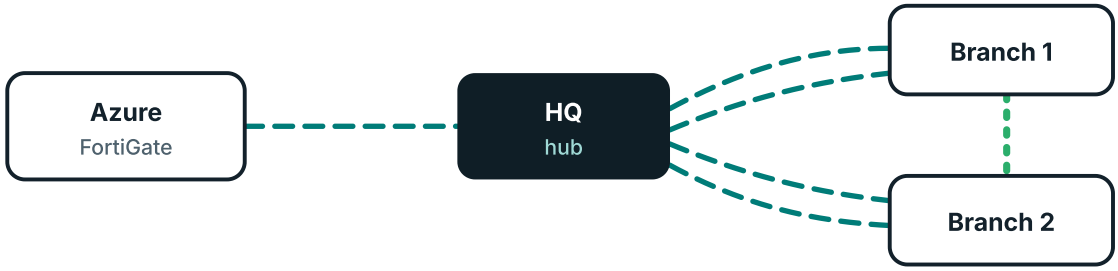
PING MY LAB · LIVE MASTERCLASS

FortiGate Masterclass: Build and Secure a Real Company Network

Guided lab

Ping My Lab · Radhe



IN THIS GUIDE

	What you will build	2
	Before you start	3
Part 1	The internet provider router (ISP-R)	5
Part 2	Head office FortiGate (FGT-HQ)	6
Part 3	Branch 1 FortiGate (FGT-BR1)	11
Part 4	Branch 2 FortiGate (FGT-BR2)	17
Part 5	The test computers	20
Part 6	Internet through the Azure FortiGate	21
Part 7	Tests: shortcut, failover, Azure internet, security checks	28
	Appendix A: the full paste blocks, one per device	40

What you will build

A small company has a head office (**HQ**) and two branches (**BR1** and **BR2**). Each place has its own FortiGate firewall and two internet lines: ISP1 (broadband) and ISP2 (4G). All the lines come from one router, ISP-R, which plays the internet provider.

The branches connect to HQ with encrypted tunnels, one tunnel on each line. If a line fails, the traffic moves to the other line. At the end, all company internet leaves through a licensed FortiGate in Microsoft Azure, which scans it and blocks unwanted sites, attacks, viruses and applications.

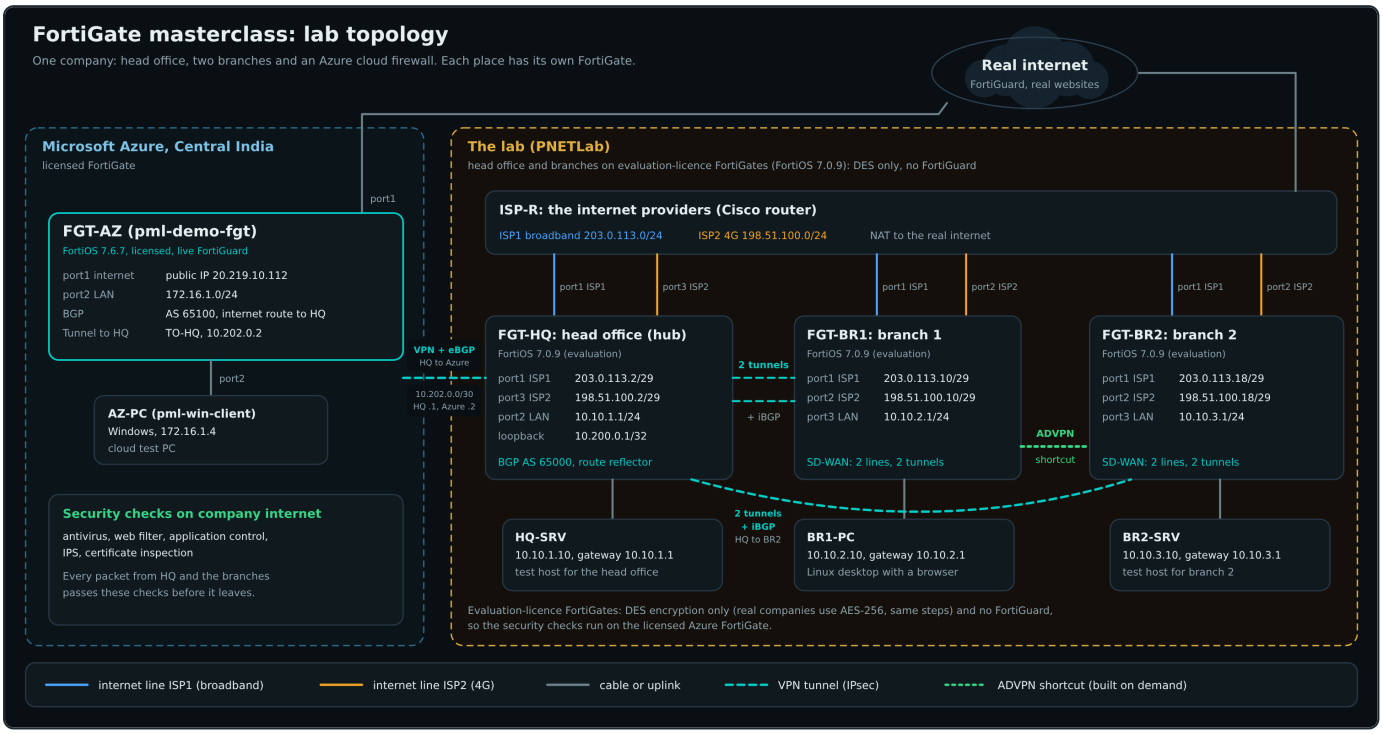


Figure 1: The lab: ISP-R, three lab FortiGates, three test computers and the Azure FortiGate.

IP plan

FORTIGATE	ISP1 LINE: FORTIGATE AND ISP-R	ISP2 LINE: FORTIGATE AND ISP-R	LAN AND TEST COMPUTER	TUNNEL ADDRESSES	MANAGEMENT
FGT-HQ	port1 203.0.113.2/29 ISP-R Gi0/1 203.0.113.1	port3 198.51.100.2/29 ISP-R Gi0/6 198.51.100.1	port2 10.10.1.1/24 HQ-SRV 10.10.1.10	10.201.1.254 10.201.2.254	port4 192.168.122.21/24
FGT-BR1	port1 203.0.113.10/29 ISP-R Gi0/2 203.0.113.9	port2 198.51.100.10/29 ISP-R Gi0/3 198.51.100.9	port3 10.10.2.1/24 BR1-PC 10.10.2.10	10.201.1.1 10.201.2.1	port4 192.168.122.22/24
FGT-BR2	port1 203.0.113.18/29 ISP-R Gi0/4 203.0.113.17	port2 198.51.100.18/29 ISP-R Gi0/5 198.51.100.17	port3 10.10.3.1/24 BR2-SRV 10.10.3.10	10.201.1.2 10.201.2.2	port4 192.168.122.23/24

OTHER NUMBERS	VALUE
Azure FortiGate (pml-demo-fgt)	public address 20.219.10.112 on port1; Azure LAN 172.16.1.0/24 (reached through port2)
Tunnel between HQ and Azure	10.202.0.0/30: TO-AZURE on HQ is 10.202.0.1, TO-HQ on Azure is 10.202.0.2
HQ loopback lo-hc	10.200.0.1/32 (the address that the branches ping for their health check)
COMPANY-NETS (on the branches)	10.10.0.0/16: all three company LANs
BGP	AS 65000: HQ (router ID 10.200.0.1), BR1 (10.10.2.1), BR2 (10.10.3.1). AS 65100: Azure (router ID 10.202.0.2)
DNS servers on the FortiGates	8.8.8.8 and 1.1.1.1

Before you start

What you need

- A lab tool that runs virtual devices. The class lab runs in PNETLab.
- A Cisco router for ISP-R.
- Three FortiGate virtual machines for FGT-HQ, FGT-BR1 and FGT-BR2. They run FortiOS 7.0.9 with the evaluation licence.
- Two small test hosts (VPCS) for HQ-SRV and BR2-SRV, and one Linux desktop with the Firefox browser for BR1-PC.
- For Part 6: a licensed FortiGate in the cloud. In the class it is a FortiGate in Microsoft Azure that runs FortiOS 7.6.7.
- A link from the lab to the real internet, because ISP-R must reach real websites.

How to use this guide

- Do the Parts in order. Each Part starts with its goal and ends with a Check.
- Dark boxes hold commands. Type or paste them in the console of the device named in the step. A console is the text window of a device (**CLI**, command line interface).
- The **GUI** is the web page of a FortiGate. Open it in a browser at the management address, for example http://192.168.122.21 for FGT-HQ.
- A **block** is a group of commands. The full blocks are in Appendix A. Paste the whole block, wait until the prompt comes back, then paste the next block. If you copy a block from this PDF, paste it into a text editor first (for example Notepad). Delete the page footer lines inside the block (they start with *Ping My Lab*). Then copy the block from the editor into the console.
- A box titled *Key lines* shows only the important lines of a block, to read and understand. Never paste it. You paste the full block from Appendix A.
- A Check line says exactly what you must see. If you do not see it, fix it before you go on.
- The pictures (Figure 1, Figure 2 and so on) come from the real lab. Your screen should show the same names and addresses.

Secrets

In the blocks, **YOUR-SECRET** stands for a pre-shared key (**PSK**). This is a secret word that both ends of a tunnel know, so they can prove who they are. Replace YOUR-SECRET with your own secret before you paste.

- Use one secret for the tunnels between HQ and the branches: the same word in block B of FGT-HQ, FGT-BR1 and FGT-BR2.
- Use a second secret for the Azure tunnel: the same word in block C of FGT-HQ and in the block of the Azure FortiGate.
- Do not share your secrets. Do not write them in this guide.

> IMPORTANT **About encryption in this lab.** The lab FortiGates (FGT-HQ, FGT-BR1 and FGT-BR2) run FortiOS 7.0.9 with an evaluation licence. This licence allows only DES encryption for IPsec tunnels. DES is old and weak, so it is used only in the lab. A real network uses AES-256 with strong DH groups (for example group 14, 19, 20 or 21). The steps are the same. Only the proposal and DH group lines change. The lab FortiGates also have no FortiGuard (the Fortinet online service that supplies web categories and attack signatures). That is why the security checks run on the Azure FortiGate. It runs FortiOS 7.6.7 and has a full licence. It accepts DES only so that it can talk to the lab FortiGates.

The ideas in this lab, in plain words

IDEA	WHAT IT MEANS	PARTS
Network size (/24, /29, /32)	The number after the slash tells how big a network is. /24 holds 254 devices, /29 holds 6 devices and /32 is one single address. Example: 10.10.1.0/24 is the head office network.	All
Underlay	The internet lines underneath the tunnels. Here: ISP1 and ISP2.	1 to 4
Overlay	The tunnels on top of the internet lines. Here: one tunnel on each line.	2 to 4
IPsec	A way to build an encrypted tunnel between two firewalls across the internet.	2 to 4
Hub and spoke	HQ is the hub. Each branch is a spoke with its own tunnels to HQ.	2, 3
ADVPN shortcut	A direct tunnel between two branches. HQ tells the branches to build it when they talk to each other. ADVPN means Auto-Discovery VPN.	2, 3, 7
SD-WAN	A feature that puts several links in one group and picks the best link for each kind of traffic.	3
Performance SLA	A health check. The branch measures delay and lost packets on each tunnel and marks the tunnel good or bad.	3
BGP	The way firewalls tell each other which networks they can reach.	2 to 4, 6
Route reflector	A BGP device that passes the routes of one branch on to the other branches. Branches then need a BGP session with HQ only.	2
Default route	The route that is used when no other route matches. It sends traffic to the internet. It is written 0.0.0.0/0.	2, 3, 6
Security profile	A set of checks (antivirus, web filter, DNS filter, application control, IPS) that you add to a firewall policy.	6, 7
URL filter	Your own list of web addresses that the firewall blocks or allows.	6, 7
DNS filter	A check on the name of a website, made when the computer asks for its address. A blocked name gets the address of a block page.	6, 7

PART 1

The internet provider router (ISP-R)

Goal: Build ISP-R, the router that plays both internet providers and connects the lab to the real internet.

ISP-R is a Cisco router. Each FortiGate line connects to it with its own small network. ISP-R also connects the lab to the real internet, so that you can test real websites later.

1 Open the console of ISP-R and paste the block

A console is a text window to a device. You type commands in it (**CLI**, command line interface). ISP-R has no login. Paste the whole block from **Appendix A1**. The first line is `no`. It answers the question about the initial configuration dialog that a new router asks. If your router does not ask it, this line only gives a harmless error.

LINES IN THE BLOCK	WHAT THEY DO
`hostname ISP-R` `no ip domain-lookup`	The router name. The second line stops the router from treating a mistyped word as a host name and looking it up on a DNS server, which makes it hang.
`interface GigabitEthernet0/1` to `0/6`	One interface for each FortiGate line. Each line is a small network of its own (a /29). The router takes the first address and the FortiGate takes the next one. The addresses 203.0.113.x and 198.51.100.x are reserved for examples, so they never clash with a real internet address.
`interface GigabitEthernet0/0`	The link to the real internet. `ip address dhcp` makes the router ask for an address automatically (**DHCP**).

`ip nat inside`
`ip nat outside`
`ip nat inside source list LAB-PUBLIC ... overload`
	NAT (**network address translation**). The first two lines mark which side is the lab (inside) and which side is the real internet (outside). The last line replaces the address of lab traffic with the address of Gi0/0 when it goes to the real internet. LAB-PUBLIC lists the two lab networks. `overload` lets many devices share the one address.

`write memory`	Saves the configuration.

KEY LINES: ONE OF THE SIX FORTIGATE INTERFACES

```
interface GigabitEthernet0/1
 description ISP1 to FGT-HQ port1
 ip address 203.0.113.1 255.255.255.248
 ip nat inside
 no shutdown
```

2 Check ISP-R

```
show ip interface brief
ping 8.8.8.8
```

CHECK

`show ip interface brief` shows an address on GigabitEthernet0/0 (not *unassigned*). `ping 8.8.8.8` gets replies: you see exclamation marks (`!!!!!`) and *Success rate is 100 percent*. If the first ping loses one packet (`.!!!!`), run it again. If Gi0/0 still shows *unassigned* after one minute, the lab link to the real internet is not working: fix that first, because the later parts need it.

PART 2

Head office FortiGate (FGT-HQ)

Goal: Build FGT-HQ: two internet lines, the VPN hub for the branches, routing with BGP, and the firewall policies.

FGT-HQ does four jobs. It connects to the internet on two lines. It is the hub where the tunnels of all branches end. It tells the branches which networks exist (routing). It decides which traffic is allowed (firewall policies). You build it with two blocks: block A for the basics, and block B for the VPN, BGP and policies.

1 Open the console and log in

Open the console of FGT-HQ. Log in as **admin** with an empty password. The FortiGate then asks you to set a new password. Choose your own and keep it private.

2 Paste block A (Appendix A2)

Paste block A and wait until the prompt `FGT-HQ #` comes back. It sets the basics:

PORT	NAME	ADDRESS	JOB
port1	ISP1	203.0.113.2/29	Internet line 1 (broadband). It connects to ISP-R Gi0/1.
port3	ISP2	198.51.100.2/29	Internet line 2 (4G). It connects to ISP-R Gi0/6.
port2	HQ-LAN	10.10.1.1/24	The head office network. Computers there use 10.10.1.1 as their gateway (the address they send everything to when the target is on another network).
port4	MGMT	192.168.122.21/24	Management port. You open the GUI here, and you can use ssh.
lo-hc	loopback	10.200.0.1/32	A virtual interface inside the FortiGate. It is always up. The branches ping it to test their tunnels (hc means health check).

`set allowaccess ping` lets a port answer ping. Port4 also allows http and ssh, so that you can manage the firewall. A DHCP server on port2 gives head office computers an address from 10.10.1.100 to 10.10.1.150. The DNS servers 8.8.8.8 and 1.1.1.1 turn names such as www.example.com into IP addresses.

NEW IDEA

The default route. The default route is the route that is used when no other route matches. It sends traffic to the internet. It is written `0.0.0.0/0`. HQ has two of them: one through ISP1 and one through ISP2. When two routes have the same distance, the route with the lower priority number is used. So ISP1 (priority 1) carries the traffic and ISP2 (priority 10) stays ready as the backup.

KEY LINES: THE TWO DEFAULT ROUTES (EXCERPT OF BLOCK A)

```
config router static
    edit 1
        set gateway 203.0.113.1
        set device "port1"
    next
    edit 2
        set gateway 198.51.100.1
        set device "port3"
        set distance 10
        set priority 10
    next
end
```

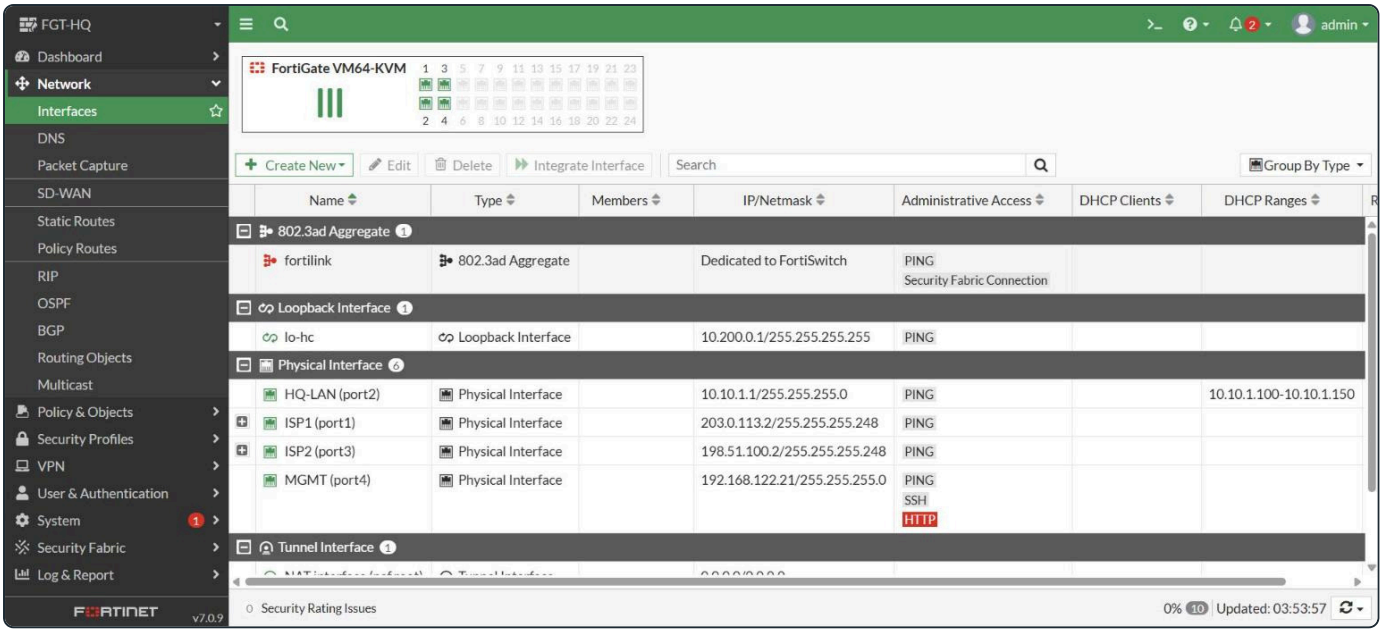


Figure 2: FGT-HQ interfaces (**Network > Interfaces**).

> **CHECK** The list shows **HQ-LAN (port2)** 10.10.1.1/255.255.255.0 with the DHCP range 10.10.1.100-10.10.1.150, **ISP1 (port1)** 203.0.113.2/255.255.255.248, **ISP2 (port3)** 198.51.100.2/255.255.255.248, **MGMT (port4)** 192.168.122.21/255.255.255.0, and the loopback **lo-hc** 10.200.0.1/255.255.255.255. The red HTTP label on MGMT is only a warning that http is not encrypted. It is fine on the management port of a lab.



Figure 3: FGT-HQ static routes (**Network > Static Routes**): two default routes.

> **CHECK** Two routes for **0.0.0.0/0** are *Enabled*: gateway **203.0.113.1** on ISP1 (port1) and gateway **198.51.100.1** on ISP2 (port3).

```
execute ping 8.8.8.8
```

> **CHECK** The ping ends with *5 packets transmitted, 5 packets received, 0% packet loss.*

3 Paste block B (Appendix A2)

Replace **YOUR-SECRET** in block B with your ADVPN secret. Then paste block B. It has 173 lines. Wait until the prompt comes back. Block B has three parts: the tunnels, BGP routing and the firewall policies. The next three steps explain them.

4 What the tunnel lines do

> **NEW IDEA** **The tunnel.** An IPsec tunnel is an encrypted connection between two firewalls across the internet. Nobody on the way can read the traffic inside it (**IPsec VPN**).

NEW IDEA **Underlay and overlay.** The internet lines underneath the tunnels are the **underlay**. The tunnels on top of the lines are the **overlay**. HQ has two tunnels: **ADVPN-ISP1** on port1 and **ADVPN-ISP2** on port3.

NEW IDEA **Hub and spoke, and the shortcut.** HQ is the hub. Each branch is a spoke and dials in to HQ. When one branch sends traffic to another branch through HQ, HQ can tell both branches to build a direct tunnel between themselves. This direct tunnel is the **ADVPN shortcut** (ADVPN means Auto-Discovery VPN).

KEY LINES (EXCERPT OF BLOCK B)

```
config vpn ipsec phase1-interface
    edit "ADVPN-ISP1"
        set type dynamic
        set interface "port1"
        set ike-version 2
        set proposal des-sha256
        set dhgrp 14 5 2
        set auto-discovery-sender enable
        set network-id 1
        set psksecret YOUR-SECRET
        ...
    next
    edit "ADVPN-ISP2"
        (the same, with interface "port3" and network-id 2)
    next
end
```

LINE	WHAT IT DOES
`set type dynamic`	HQ accepts a tunnel from any branch address (dial-up). HQ does not need to know the branch addresses.
`set interface "port1"`	The internet line that this tunnel uses. ADVPN-ISP2 uses port3.
`set ike-version 2`	Uses IKE version 2 to set the tunnel up.
`set proposal des-sha256` `set dhgrp 14 5 2`	The encryption and key exchange settings. They are lab settings (see the note **About encryption in this lab** in *Before you start*).
`set psksecret YOUR-SECRET`	The pre-shared key.
`set auto-discovery-sender enable`	Turns on ADVPN on the hub.
`set network-id 1`	A number that tells the ISP1 tunnels (1) apart from the ISP2 tunnels (2).
`set dpd on-idle` `set dpd-retryinterval 5`	Dead peer detection (**DPD**): when no traffic arrives, HQ checks that the other side is alive, and asks again every 5 seconds.
`set add-route disable`	The tunnel adds no routes by itself. BGP gives the routes.

Every tunnel has two parts. Phase 1 (`phase1-interface`) builds the secure channel between the two firewalls. Phase 2 (`phase2-interface`) builds the tunnel that carries your data. Each tunnel also gets an address inside the tunnel: **10.201.1.254** for ISP1 and **10.201.2.254** for ISP2. BGP will use these addresses. The block also puts both tunnels in one zone called **OVERLAY**. A zone is a group of interfaces, so one policy can cover both tunnels.

5 What the BGP lines do

NEW IDEA **BGP.** BGP (**Border Gateway Protocol**) is the way firewalls tell each other which networks they can reach. Every network that one firewall announces is learned by the others.

NEW IDEA **AS number and iBGP.** An **AS number** is the ID of one routing group. HQ and both branches belong to one company, so they all use AS 65000. BGP inside one AS is called **iBGP**.

NEW IDEA **Route reflector.** Normally every iBGP device must talk to every other one. A **route reflector** passes the routes of one device on to the others. HQ is the route reflector, so each branch needs a BGP session with HQ only.

KEY LINES (EXCERPT OF BLOCK B)

```
config router bgp
    set as 65000
    set router-id 10.200.0.1
    set ibgp-multipath enable
    config neighbor-group
        edit "SPOKES-ISP1"
            set remote-as 65000
            set keep-alive-timer 5
            set holdtime-timer 15
            set route-reflector-client enable
            set capability-default-originate enable
        next
        ...
    end
    config neighbor-range
        edit 1
            set prefix 10.201.1.0 255.255.255.0
            set neighbor-group "SPOKES-ISP1"
        next
        ...
    end
    config network
        edit 1
            set prefix 10.10.1.0 255.255.255.0
        next
        edit 2
            set prefix 10.200.0.1 255.255.255.255
        next
    end
end
```

LINE	WHAT IT DOES
`set keep-alive-timer 5` `set holdtime-timer 15`	HQ and each branch send a short keepalive message every 5 seconds. If none arrives for 15 seconds (the hold time), the neighbor is declared dead and its routes are removed. This is how a dead line is noticed fast.
`set route-reflector-client enable`	HQ reflects the routes of this neighbor to the other neighbors.
`set capability-default-originate enable`	HQ sends a default route (0.0.0.0/0) to each branch. It means: send your internet traffic to me.
`config neighbor-range`	Any device in 10.201.1.0/24 (the ISP1 tunnels) or 10.201.2.0/24 (the ISP2 tunnels) may become a neighbor. You do not add each branch by hand.
`set ibgp-multipath enable`	When both tunnels are healthy, HQ keeps the route through both of them.
`config network`	The networks HQ announces: 10.10.1.0/24 (the head office LAN) and 10.200.0.1/32 (the loopback).

6 What the firewall policies do

> **NEW IDEA** **Firewall policy.** A firewall policy is a rule that allows traffic from one interface to another. Traffic that matches no policy is dropped (**implicit deny**, the last row in the list).

#	NAME	FROM	TO	WHAT IT ALLOWS
1	Branch-to-branch	OVERLAY	OVERLAY	Traffic from one branch to the other branch through HQ.
2	Branches-to-HQ	OVERLAY	port2	Branches reach the head office computers.
3	HQ-to-branches	port2	OVERLAY	Head office computers reach the branches.
4	Health-checks	OVERLAY	lo-hc	Only ping, to the loopback 10.200.0.1. The branch health checks use it.
5	HQ-internet	port2	port1	Head office computers go to the internet through ISP1. NAT is on.
6	Branch-internet	OVERLAY	port1	Branch internet traffic leaves through ISP1. NAT is on.

With NAT (network address translation) on, the source address of the traffic is replaced by the address of the outgoing port, here 203.0.113.2. This lets the replies find their way back.

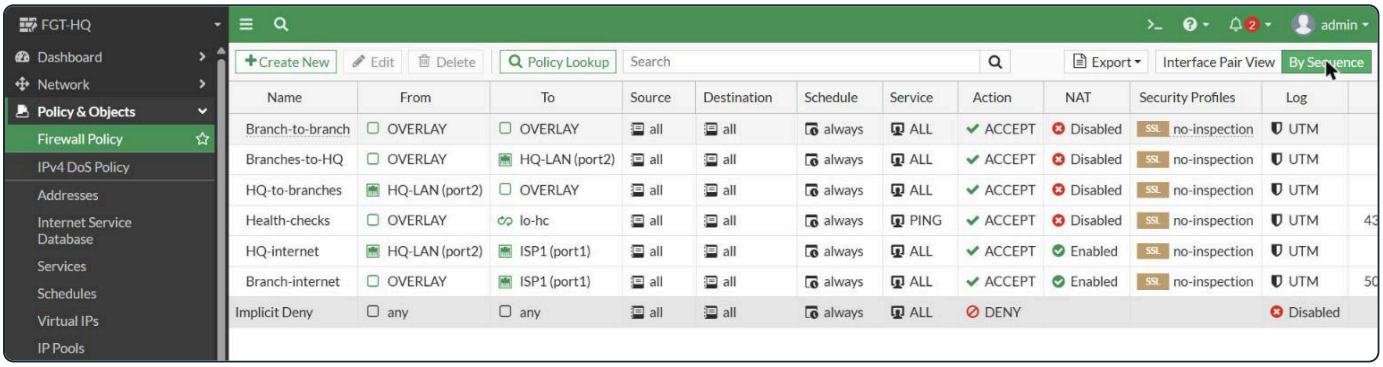


Figure 4: FGT-HQ firewall policies (**Policy & Objects > Firewall Policy**).

> **CHECK** Six policies in this order: Branch-to-branch, Branches-to-HQ, HQ-to-branches, Health-checks, HQ-internet, Branch-internet, then *Implicit Deny*. NAT shows **Enabled** only for HQ-internet and Branch-internet.

7 Check the tunnels later

The tunnels and BGP neighbors of HQ cannot be up yet, because no branch is connected. You check them at the end of Part 4 (Figure 11 to Figure 13).

PART 3

Branch 1 FortiGate (FGT-BR1)

Goal: Build FGT-BR1: two internet lines, two tunnels to HQ, SD-WAN to pick the healthy tunnel, BGP routing and policies.

FGT-BR1 is a spoke. It connects to HQ with one tunnel on each internet line. It measures both tunnels all the time and uses the healthy one. Branch 1 computers use 10.10.2.1 as their gateway.

1 Log in and paste block A (Appendix A3)

Open the console of FGT-BR1. Log in as **admin** with an empty password and set your new password, as you did on HQ. Then paste block A and wait for the prompt. It sets the basics:

PORT	NAME	ADDRESS	JOB
port1	ISP1-broadband	203.0.113.10/29	Internet line 1. It connects to ISP-R Gi0/2.
port2	ISP2-4G	198.51.100.10/29	Internet line 2. It connects to ISP-R Gi0/3.
port3	BR1-LAN	10.10.2.1/24	The branch network. DHCP gives 10.10.2.100 to 10.10.2.150. The address 10.10.2.10 is reserved for BR1-PC. The line `set mac 50:cc:11:03:f9:00` is the network card address (**MAC address**) of BR1-PC in the class lab. If your PC has another one, nothing breaks, because Part 5 sets the address on the PC itself.
port4	MGMT	192.168.122.22/24	Management port (GUI and ssh).

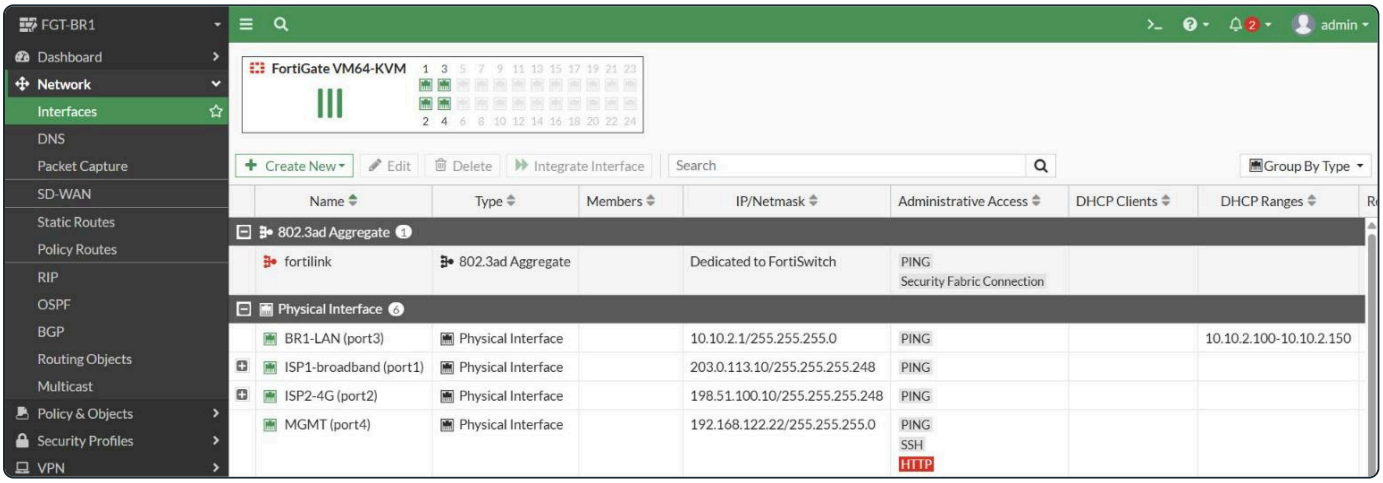


Figure 5: FGT-BR1 interfaces after block A (**Network > Interfaces**).

CHECK **BR1-LAN (port3)** 10.10.2.1/255.255.255.0 with the DHCP range 10.10.2.100-10.10.2.150, **ISP1-broadband (port1)** 203.0.113.10/255.255.255.248, **ISP2-4G (port2)** 198.51.100.10/255.255.255.248 and **MGMT (port4)** 192.168.122.22/255.255.255.0.

Block A also adds five routes. They look strange at first, so read them once:

ROUTE	GOES TO	WHY
1	203.0.113.2/32 through 203.0.113.9 (port1)	The way to HQ over ISP1. The tunnel HUB-ISP1 is built to this address.
2	198.51.100.2/32 through 198.51.100.9 (port2)	The way to HQ over ISP2. The tunnel HUB-ISP2 is built to this address.
3	0.0.0.0/0 through 203.0.113.9 (port1), distance 250	Backup internet if both tunnels are down. **Distance** says how much the firewall trusts a route, and the lowest number wins. Routes that BGP learns from HQ have distance 200, so they win while the tunnels are up.
4	203.0.113.0/24 through 203.0.113.9 (port1)	The whole ISP1 network is reached directly on the internet line.
5	198.51.100.0/24 through 198.51.100.9 (port2)	The same for ISP2.

Routes 4 and 5 keep the underlay traffic on the internet lines. Later, the shortcut tunnel to BR2 is built between the internet addresses of the two branches (for example 203.0.113.10 and 203.0.113.18). Those packets must leave on the internet line, not go into a tunnel.

```
execute ping 203.0.113.2
execute ping 198.51.100.2
```

CHECK Both pings get replies. This proves that the underlay works: BR1 reaches HQ over ISP1 and over ISP2.

2 Paste block B (Appendix A3)

Replace YOUR-SECRET with the **same** ADVPN secret you used on HQ. Then paste block B. It has 184 lines: the tunnels, SD-WAN, BGP and the policies. The branch is the one that dials, so its tunnel lines differ a little from HQ. The other lines (IKE version, proposal, DH group, DPD) are the same as on HQ:

KEY LINES (EXCERPT OF BLOCK B)

```
config vpn ipsec phase1-interface
    edit "HUB-ISP1"
        set interface "port1"
        set auto-discovery-receiver enable
        set network-id 1
        set remote-gw 203.0.113.2
        set psksecret YOUR-SECRET
        ...
    next
    edit "HUB-ISP2"
        (the same, with interface "port2", network-id 2 and remote-gw 198.51.100.2)
    next
end
config vpn ipsec phase2-interface
    edit "HUB-ISP1"
        set phase1name "HUB-ISP1"
        set auto-negotiate enable
        ...
```

LINE	WHAT IT DOES
`set remote-gw 203.0.113.2`	The internet address of HQ on ISP1. The branch dials this address. On ISP2 it is 198.51.100.2.
`set auto-discovery-receiver enable`	The branch accepts the order from HQ to build a shortcut tunnel.
`set auto-negotiate enable`	Phase 2 starts by itself. The tunnel does not wait for traffic.
Tunnel addresses	HUB-ISP1 is 10.201.1.1 and HUB-ISP2 is 10.201.2.1. The other end is HQ at 10.201.1.254 and 10.201.2.254.

3 Check the tunnels

```
get vpn ipsec tunnel summary
```

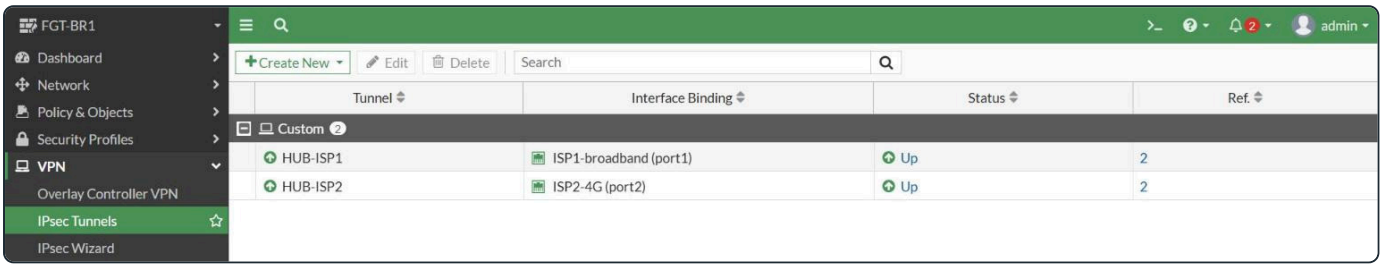


Figure 6: FGT-BR1 IPsec tunnels (**VPN > IPsec Tunnels**).

> **CHECK** **HUB-ISP1** (ISP1-broadband, port1) and **HUB-ISP2** (ISP2-4G, port2) both show *Up*. In the CLI, the summary has a line `'HUB-ISP1' 203.0.113.2:0` and a line `'HUB-ISP2' 198.51.100.2:0`, each with `selectors(total,up): 1/1`.

If a tunnel is not up, check that YOUR-SECRET is the same on HQ and BR1, and repeat the two pings from step 1.

4 Look at the SD-WAN zone

> **NEW IDEA** **SD-WAN.** SD-WAN (**software-defined WAN**) puts several links in one group and picks the best link for each kind of traffic. Here the links are the two tunnels HUB-ISP1 and HUB-ISP2. The group is the SD-WAN zone **OVERLAY**. Policies and rules then use the zone name, not one single tunnel.

KEY LINES (EXCERPT OF BLOCK B)

```
config system sdwan
    set status enable
    config zone
        edit "OVERLAY"
    ...
    config members
        edit 1
            set interface "HUB-ISP1"
            set zone "OVERLAY"
        next
        edit 2
            set interface "HUB-ISP2"
            set zone "OVERLAY"
```

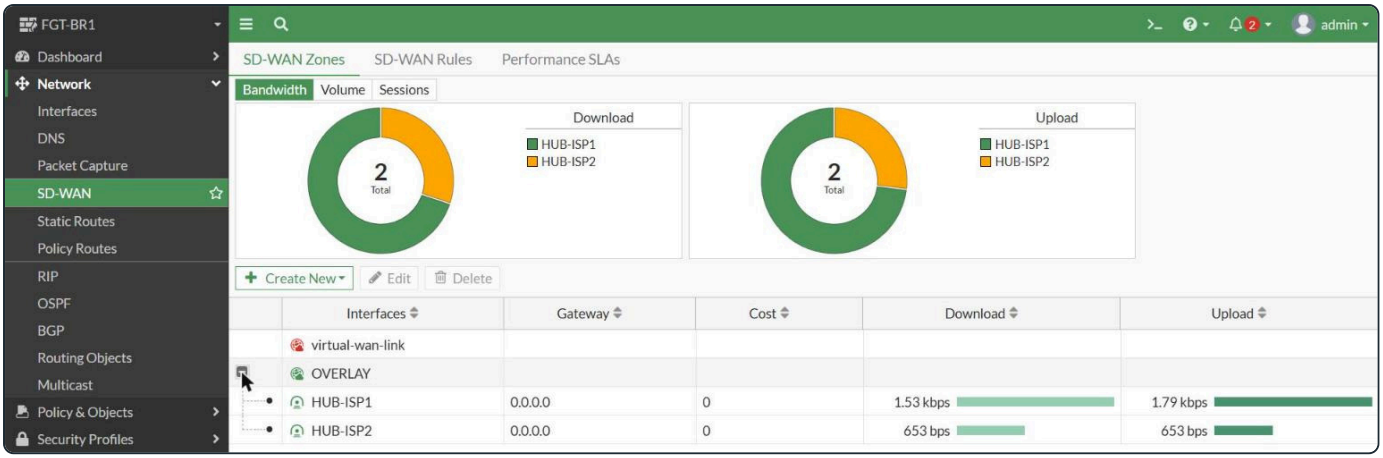


Figure 7: FGT-BR1 SD-WAN zones (**Network > SD-WAN**, tab SD-WAN Zones).

> **CHECK** The zone **OVERLAY** has two members, **HUB-ISP1** and **HUB-ISP2**, both with a green icon. The zone *virtual-wan-link* above it is the default zone. It has no members and the lab does not use it.

5 Look at the performance SLA

> **NEW IDEA** **Performance SLA.** A **performance SLA** is a health check. The branch pings the address 10.200.0.1 (the HQ loopback) through each tunnel and measures the delay (**latency**), the change in delay (**jitter**) and the lost pings (**packet loss**). A tunnel is good when the latency stays under 150 ms and the packet loss stays under 2%. When the checks keep failing, the tunnel is marked dead and SD-WAN stops using it.

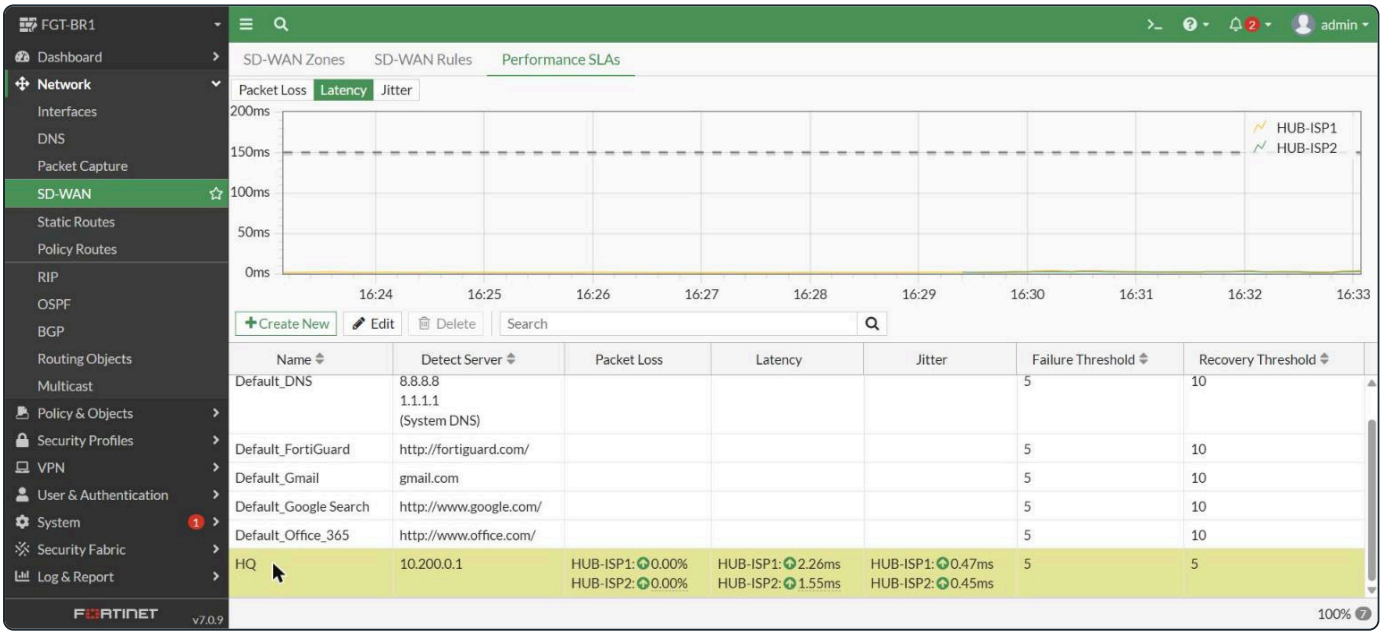


Figure 8: FGT-BR1 performance SLA named HQ (**Network > SD-WAN**, tab Performance SLAs).

> **CHECK** The row **HQ** (the last row of the table) has the detect server **10.200.0.1**. Both HUB-ISP1 and HUB-ISP2 show a green arrow, packet loss **0.00%** and a latency of a few milliseconds (about 2 ms in the figure). The columns *Failure Threshold* and *Recovery Threshold* show 5 and 5. The dashed line in the graph is the 150 ms limit. The rows above HQ (Default_DNS and so on) come with FortiOS. Ignore them.

The check **HQ** comes from these lines of block B:

KEY LINES (EXCERPT OF BLOCK B)

```
config health-check
    edit "HQ"
        set server "10.200.0.1"
        set members 1 2
        config sla
            edit 1
                set link-cost-factor latency packet-loss
                set latency-threshold 150
                set packetloss-threshold 2
```

6 Look at the SD-WAN rules

An SD-WAN rule chooses the tunnel for the traffic that matches it. This branch has two rules. In both, `set mode sla` and `set priority-members 1 2` mean: use HUB-ISP1 while it meets the SLA. If it does not, use HUB-ISP2.

ID	NAME	TRAFFIC IT MATCHES
1	Company-traffic	Traffic to the company networks. The address COMPANY-NETS is 10.10.0.0/16, which covers the three company LANs 10.10.1.0/24, 10.10.2.0/24 and 10.10.3.0/24.
2	Internet-via-HQ	All other traffic, that is the internet. It also goes through HQ.

KEY LINES (EXCERPT OF BLOCK B)

```
config service
    edit 1
        set name "Company-traffic"
        set mode sla
        set dst "COMPANY-NETS"
        set priority-members 1 2
    ...
    edit 2
        set name "Internet-via-HQ"
        set mode sla
        set dst "all"
        set priority-members 1 2
```

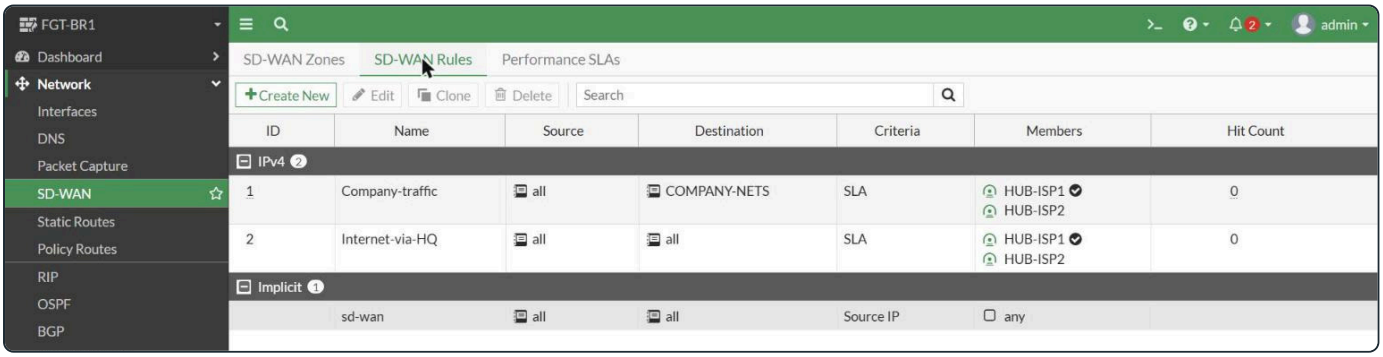


Figure 9: FGT-BR1 SD-WAN rules (**Network > SD-WAN**, tab SD-WAN Rules).

> **CHECK** Two rules, **Company-traffic** and **Internet-via-HQ**, both with the criteria *SLA*. In the Members column, **HUB-ISP1** has a tick. The tick marks the tunnel that the rule uses now.

7 BGP and policies on BR1

BR1 has two BGP neighbors: **10.201.1.254** and **10.201.2.254**. These are the addresses of HQ inside the two tunnels. BR1 announces its own network 10.10.2.0/24. The timers 5 and 15 are the same as on HQ. `set link-down-failover enable` makes BGP drop a neighbor at once when its tunnel goes down.

KEY LINES (EXCERPT OF BLOCK B)

```
config router bgp
    set as 65000
    set router-id 10.10.2.1
    set ibgp-multipath enable
    config neighbor
        edit "10.201.1.254"
            set remote-as 65000
            set keep-alive-timer 5
            set holdtime-timer 15
            set link-down-failover enable
        next
        edit "10.201.2.254"
            ...
    config network
        edit 1
            set prefix 10.10.2.0 255.255.255.0
```

#	POLICY	FROM	TO	WHAT IT ALLOWS
1	LAN-to-company-and-internet	port3	OVERLAY	Branch computers go to the company and to the internet through the tunnels.
2	Company-to-LAN	OVERLAY	port3	Traffic from the tunnels to the branch computers.
3	Backup-internet	port3	port1	Used only when both tunnels are down. Traffic leaves directly through ISP1, with NAT, on the backup route of distance 250.

```
get router info bgp summary
```

CHECK Both neighbors, **10.201.1.254** and **10.201.2.254**, show AS **65000** and a number in the last column (*State/PfxRcd*). A number means the session is up. If you see *Idle*, *Connect* or *Active*, the session is not up yet: check the tunnel first.

PART 4

Branch 2 FortiGate (FGT-BR2)

Goal: Build FGT-BR2 the same way as BR1, then check on HQ that both branches are connected.

FGT-BR2 uses the same steps as FGT-BR1. Only the names and addresses change.

WHAT IS DIFFERENT	FGT-BR1	FGT-BR2
port1, ISP1 (gateway)	203.0.113.10/29 (203.0.113.9)	203.0.113.18/29 (203.0.113.17)
port2, ISP2 (gateway)	198.51.100.10/29 (198.51.100.9)	198.51.100.18/29 (198.51.100.17)
port3, LAN	10.10.2.1/24	10.10.3.1/24
port4, management	192.168.122.22/24	192.168.122.23/24
Tunnel addresses	10.201.1.1 and 10.201.2.1	10.201.1.2 and 10.201.2.2
BGP router ID	10.10.2.1	10.10.3.1
BGP network announced	10.10.2.0/24	10.10.3.0/24
DHCP reservation for a PC	yes (10.10.2.10, BR1-PC)	no

1 Log in and paste block A (Appendix A4)

Open the console of FGT-BR2. Log in as **admin** with an empty password and set your new password. Then paste block A and wait for the prompt. Check the underlay, as you did on BR1:

```
execute ping 203.0.113.2
execute ping 198.51.100.2
```

CHECK Both pings get replies.

2 Paste block B (Appendix A4)

Replace **YOUR-SECRET** with the same secret as on HQ and BR1. Then paste block B (184 lines).

3 Check the tunnels on BR2

```
get vpn ipsec tunnel summary
```

```
FGT-BR2 # get vpn ipsec tunnel summary
'HUB-ISP1' 203.0.113.2:0  selectors(total,up): 1/1  rx(pkt,err): 57061/0  tx(pkt,err): 87047/11
'HUB-ISP2' 198.51.100.2:0  selectors(total,up): 1/1  rx(pkt,err): 53116/0  tx(pkt,err): 53127/9
```

Figure 10: FGT-BR2: both tunnels to HQ are up.

CHECK A line `'HUB-ISP1' 203.0.113.2:0` and a line `'HUB-ISP2' 198.51.100.2:0`, each with `selectors(total,up): 1/1`. The packet counters (rx and tx) are different in your lab.

4 Go back to FGT-HQ: look at the tunnels

Both branches are connected now. On FGT-HQ open **VPN > IPsec Tunnels**.



Figure 11: FGT-HQ IPsec tunnels with both branches connected.

> **CHECK** **ADVPN-ISP1** (ISP1, port1) and **ADVPN-ISP2** (ISP2, port3) both show **2 dialup connection(s)**: one from BR1 and one from BR2.

5 Look at the BGP settings on FGT-HQ

Open **Network > BGP**.

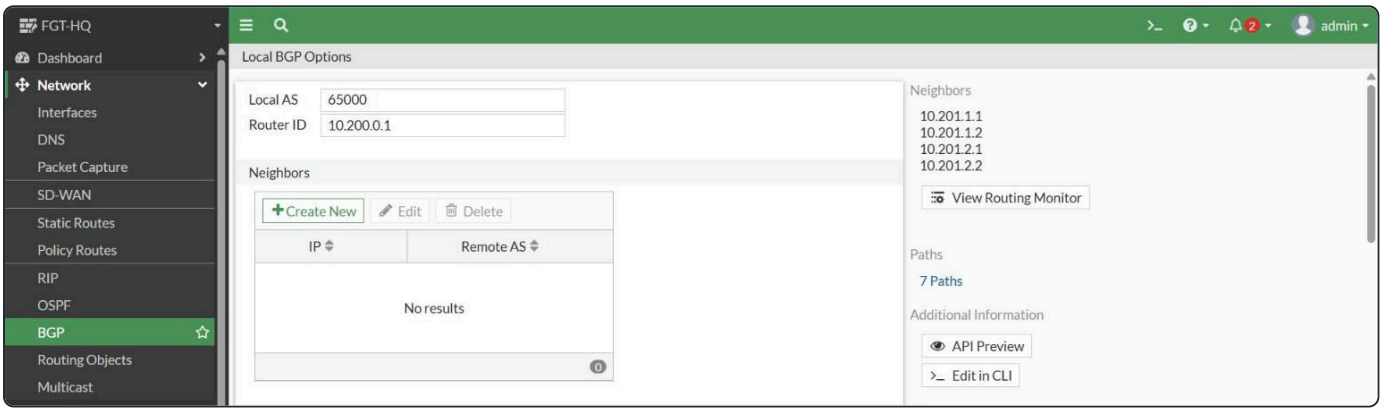


Figure 12: FGT-HQ BGP settings.

> **CHECK** **Local AS 65000** and **Router ID 10.200.0.1**. On the right, the Neighbors list shows **10.201.1.1, 10.201.1.2, 10.201.2.1 and 10.201.2.2**. The Neighbors table on the left says *No results*. This is normal: HQ has no fixed neighbors. It accepts the branches through the neighbor ranges. Below the visible part, the table Neighbor Groups lists SPOKES-ISP1 and SPOKES-ISP2 (remote AS 65000).

6 Look at the BGP neighbors on FGT-HQ

On the same page, click **View Routing Monitor** on the right, and choose **BGP Neighbors** in the list at the top right.

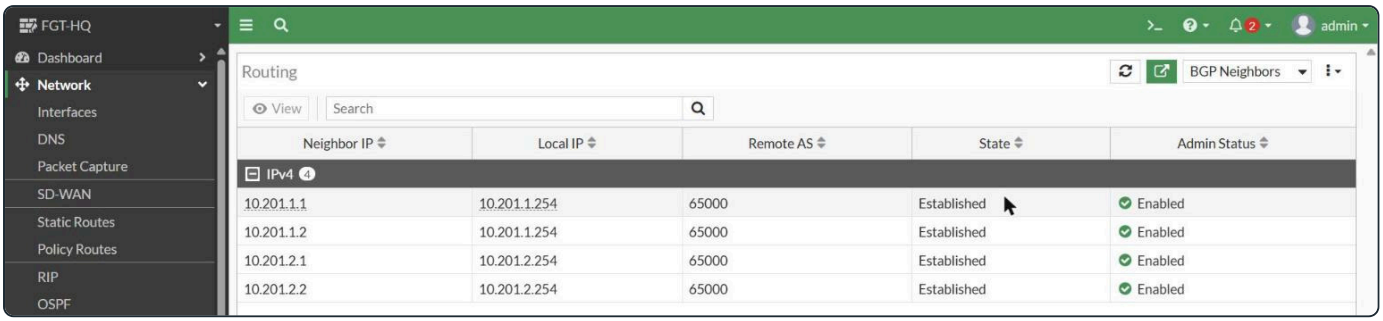


Figure 13: FGT-HQ BGP neighbors.

> **CHECK** Four neighbors, all **Established** and *Enabled*: 10.201.1.1 and 10.201.2.1 (BR1), 10.201.1.2 and 10.201.2.2 (BR2). The local addresses are 10.201.1.254 for the ISP1 neighbors and 10.201.2.254 for the ISP2 neighbors. The remote AS is 65000.

PART 5

The test computers

Goal: Give the three test computers their addresses, so that every office has a user.

HQ-SRV and BR2-SRV are small test hosts (VPCS). They only run network commands such as ping. BR1-PC is a Linux desktop with the Firefox browser. It is the branch user that you will use for the web filter test in Part 7.

1 HQ-SRV and BR2-SRV

Open the console of HQ-SRV. There is no login. Paste the two lines from **Appendix A5**. The first line sets the address, the mask (/24) and the gateway. The second line saves the setting.

HQ-SRV

```
ip 10.10.1.10/24 10.10.1.1
save
```

Then open the console of BR2-SRV and paste its two lines:

BR2-SRV

```
ip 10.10.3.10/24 10.10.3.1
save
```

2 BR1-PC

Log in to the BR1-PC desktop, open **QTerminal** (the terminal program) and run the two lines from Appendix A5. In the class lab this PC first has an address from another lab. The two lines replace it:

```
nmcli con mod lan ipv4.addresses 10.10.2.10/24 ipv4.gateway 10.10.2.1 ipv4.dns 8.8.8.8
nmcli con up lan
```

`nmcli` sets network addresses on Linux, and `lan` is the name of the network connection of this PC. The first line sets the address 10.10.2.10/24, the gateway 10.10.2.1 (port3 of FGT-BR1) and the DNS server 8.8.8.8. The second line switches the new settings on. BR1 keeps the address 10.10.2.10 for this PC in its DHCP settings.

3 Check the test computers

ON HQ-SRV

```
show ip
ping 10.10.1.1
```

ON BR2-SRV

```
ping 10.10.3.1
```

ON BR1-PC (QTERMINAL)

```
ping 10.10.2.1
ping 10.10.1.10
```

CHECK

On HQ-SRV, `show ip` lists **IP/MASK 10.10.1.10/24** and **GATEWAY 10.10.1.1**. On each computer, the ping to its gateway gets replies. On BR1-PC, the ping to 10.10.1.10 (HQ-SRV) also gets replies: it goes through the tunnel to HQ. On a Linux PC, press **Ctrl+C** to stop the ping.

PART 6

Internet through the Azure FortiGate

Goal: Send all company internet through a licensed FortiGate in Azure, where the security checks run: web filter, DNS filter, IPS, antivirus and application control.

Until now, HQ sends the internet traffic of the whole company out on its own line, ISP1. In this part, HQ builds a tunnel to the Azure FortiGate. HQ and Azure then exchange routes with BGP. Azure tells HQ: I am the way to the internet. HQ passes this route on to the branches. From then on, all company internet (HQ and both branches) goes to Azure, is checked there, and then leaves. If Azure is down, HQ goes back to its own lines by itself.

NEW IDEA **eBGP.** In Part 2 all BGP devices were in one AS (65000), so it was iBGP. Between HQ (AS 65000) and Azure (AS 65100) the AS numbers are different. BGP between two different AS is called **eBGP**.

NEW IDEA **Security profile.** A **security profile** is a set of checks that you add to a firewall policy. The Azure policy uses these:

CHECK	WHAT IT DOES
Antivirus	Finds known viruses in the files that pass through the firewall.
Web filter	Allows or blocks websites by category, which is a group of sites such as Social Networking. The categories come from FortiGuard.
URL filter	Your own list of web addresses to block or allow. It is a part of the web filter.
DNS filter	Checks the name of a website when the computer asks for its address (a **DNS lookup**). For a blocked category, the answer is the address of a Fortinet block page, so the site never opens.
Application control	Recognises applications, for example YouTube or file sharing, and allows or blocks them by category.
IPS (intrusion prevention)	Compares the traffic with attack patterns (**signatures**) and blocks the traffic that matches.
Certificate inspection	Reads the site name of an encrypted (https) connection without opening the data inside. The firewall can block a site by name, but it cannot see the page.

1 Start the Azure FortiGate and open its CLI

In the Azure portal, start the virtual machine **pml-demo-fgt** and wait until it runs. The Azure FortiGate has the public address **20.219.10.112**. You open its GUI in a browser at `https://20.219.10.112`. For the CLI, use ssh to `20.219.10.112`, or use the CLI console from the Windows client over RDP (remote desktop). The CLI console does not connect from your own browser.

2 Choose the secret

Choose a new secret for the Azure tunnel. Replace **YOUR-SECRET** with it in **both** blocks before you paste: the Azure block (Appendix A6) and block C of FGT-HQ (Appendix A2). The two words must be the same.

3 Paste the Azure block on the Azure FortiGate (Appendix A6)

Paste the block in the CLI of the Azure FortiGate. It has 185 lines. It sets these things:

PART OF THE BLOCK	WHAT IT DOES
The tunnel **TO-HQ**	A dial-up tunnel: Azure waits and HQ dials in. The address inside the tunnel is 10.202.0.2 on Azure and 10.202.0.1 on HQ.
BGP, AS 65100	The neighbor is HQ (10.202.0.1, AS 65000). `capability-default-originate` makes Azure send HQ a default route. Azure announces its own network 172.16.1.0/24. The timers are 10 and 30.
The web filter	The URL filter list **Company-blocked-sites** blocks `*neverssl.com`. The web filter profile **Company-WF** uses that list, logs every URL, and blocks the FortiGuard categories 37 (Social Networking) and 20 (Games).
The DNS filter	The DNS filter profile **Company-DNS** blocks the FortiGuard category 11 (Gambling) and the names of known botnet servers.
Application control	The application list **Company-APP** blocks the categories 5 (Video/Audio, for example YouTube), 2 (P2P) and 6 (Proxy).
IPS	A test signature **PML.Test.Signature**, and the IPS sensor **Company-IPS**, which blocks this signature and the attacks of severity medium, high and critical.
The policies	Two policies between HQ and the Azure LAN, and the policy **Company-internet**, which sends traffic from the tunnel to the internet through port1 with NAT and with all the security profiles.

The policies **HQ-to-Azure-LAN** and **Azure-LAN-to-HQ** use an address object called **PROTECTED-A**. The block does not create it. In the class lab it already exists on the Azure FortiGate and stands for the protected Azure LAN. If you use your own Azure FortiGate, first create an address object with this name for your Azure LAN, and then paste the block.

One line of the block is very long: the line `set signature` in the IPS part. It is one single line, but the PDF shows it on two rows. When you copy the block, join these two rows into one line, with one space between them, before you paste it in the CLI.

KEY LINES: TUNNEL AND BGP (EXCERPT OF THE AZURE BLOCK)

```
config vpn ipsec phase1-interface
    edit "TO-HQ"
        set type dynamic
        set interface "port1"
        set ike-version 2
        set proposal des-sha256
        set network-id 10
        set psksecret YOUR-SECRET
        ...
config router bgp
    set as 65100
    set router-id 10.202.0.2
    config neighbor
        edit "10.202.0.1"
            set remote-as 65000
            set capability-default-originate enable
            set keep-alive-timer 10
            set holdtime-timer 30
    ...
    config network
        edit 1
            set prefix 172.16.1.0 255.255.255.0
```

4 What the security lines of the block do

Web filter and URL filter. The URL filter list is a list of addresses that you block or allow (a **URL filter**). The star `*` in `*neverssl.com` stands for any text before the name (`type wildcard`).

KEY LINES: URL FILTER LIST (EXCERPT)

```
config webfilter urlfilter
    edit 10
        set name "Company-blocked-sites"
        config entries
            edit 1
                set url "*neverssl.com"
                set type wildcard
                set action block
```

The web filter profile (**web filter**) then uses this list (`urlfilter-table 10`), logs every URL (`log-all-url`) and blocks two FortiGuard categories (`ftgd-wf`). Category 37 is Social Networking and category 20 is Games.

KEY LINES: WEB FILTER PROFILE (EXCERPT)

```
config webfilter profile
    edit "Company-WF"
        set log-all-url enable
        config web
            set urlfilter-table 10
        config ftgd-wf
            config filters
                edit 100
                    set category 37
                    set action block
                edit 101
                    set category 20
                    set action block
```

DNS filter. The DNS filter profile **Company-DNS** checks the names that computers ask the DNS server for (a **DNS lookup**). `category 11` is Gambling, so these names are blocked. For a blocked name, the FortiGate answers with the address of a Fortinet block page, so the real site never opens. `block-botnet enable` also blocks the names of known botnet servers. A **botnet** is a group of infected computers that an attacker controls.

KEY LINES: DNS FILTER PROFILE (EXCERPT)

```
config dnsfilter profile
    edit "Company-DNS"
        set block-botnet enable
        config ftgd-dns
            config filters
                edit 100
                    set category 11
                    set action block
```

Application control. The application list **Company-APP** recognises applications by their traffic. `category 5` is Video/Audio (YouTube is in it). `category 2 6` are P2P (file sharing between users) and Proxy (programs that hide the real website). All of them get the action `block`.

KEY LINES: APPLICATION LIST (EXCERPT)

```
config application list
    edit "Company-APP"
        config entries
            edit 1
                set category 5
                set action block
            next
            edit 2
                set category 2 6
                set action block
```

IPS. IPS (**intrusion prevention system**) compares the traffic with attack patterns called **signatures**. FortiGuard supplies the real signatures. The block adds one harmless signature of its own, **PML.Test.Signature**, so that you can test the IPS. It matches only the word `pingmylab-ips-test` in a web address. These are its parts:

PART OF THE SIGNATURE	WHAT IT DOES
`--name "PML.Test.Signature"`	The name of the signature. It appears in the log.
`--protocol tcp` `--service HTTP`	Look only at web traffic that is not encrypted (http).
`--flow from_client`	Look only at what the computer sends to the website.
`--pattern "pingmylab-ips-test"` `--context uri`	Match this word in the path of the web address (the part after the site name, for example `/pingmylab-ips-test`).
`--no_case`	Capital and small letters count the same.

KEY LINES: TEST SIGNATURE AND IPS SENSOR (EXCERPT). THE SIGNATURE IS ONE SINGLE LINE.

```
config ips custom
    edit "PML.Test.Signature"
        set signature "F-SBID( --name \"PML.Test.Signature\"; --protocol tcp; --service HTTP;
            --flow from_client; --pattern \"pingmylab-ips-test\"; --context uri; --no_case; )"
    ...
config ips sensor
    edit "Company-IPS"
        config entries
            edit 1
                set rule 2354
                set status enable
                set action block
                set log-packet enable
            next
            edit 2
                set severity medium high critical
```

The IPS sensor **Company-IPS** uses the signature in entry 1. `set rule 2354` selects it, `set action block` drops the traffic, and `set log-packet enable` saves the packet that matched. Entry 2 adds the FortiGuard signatures with severity medium, high and critical, each with its default action.

> **IMPORTANT** In the block, `set rule 2354` is the **attack_id** (the number of the signature) that the Azure FortiGate of the class gave to **PML.Test.Signature**. Another FortiGate can give another number. On another FortiGate, run `show ips custom` and use the number shown after `--attack_id` in the line `set rule`.

5 Look at the policy Company-internet

The policy **Company-internet** puts everything together. It sends the traffic from the tunnel TO-HQ out through port1 with NAT. The lines `av-profile`, `webfilter-profile`, `dnsfilter-profile`, `ips-sensor` and `application-list` switch the five checks on. The antivirus profile **default** and the SSL profile **certificate-inspection** already exist on the FortiGate, so the block only names them. In the GUI, open Policy & Objects > Firewall Policy and double-click **Company-internet**.

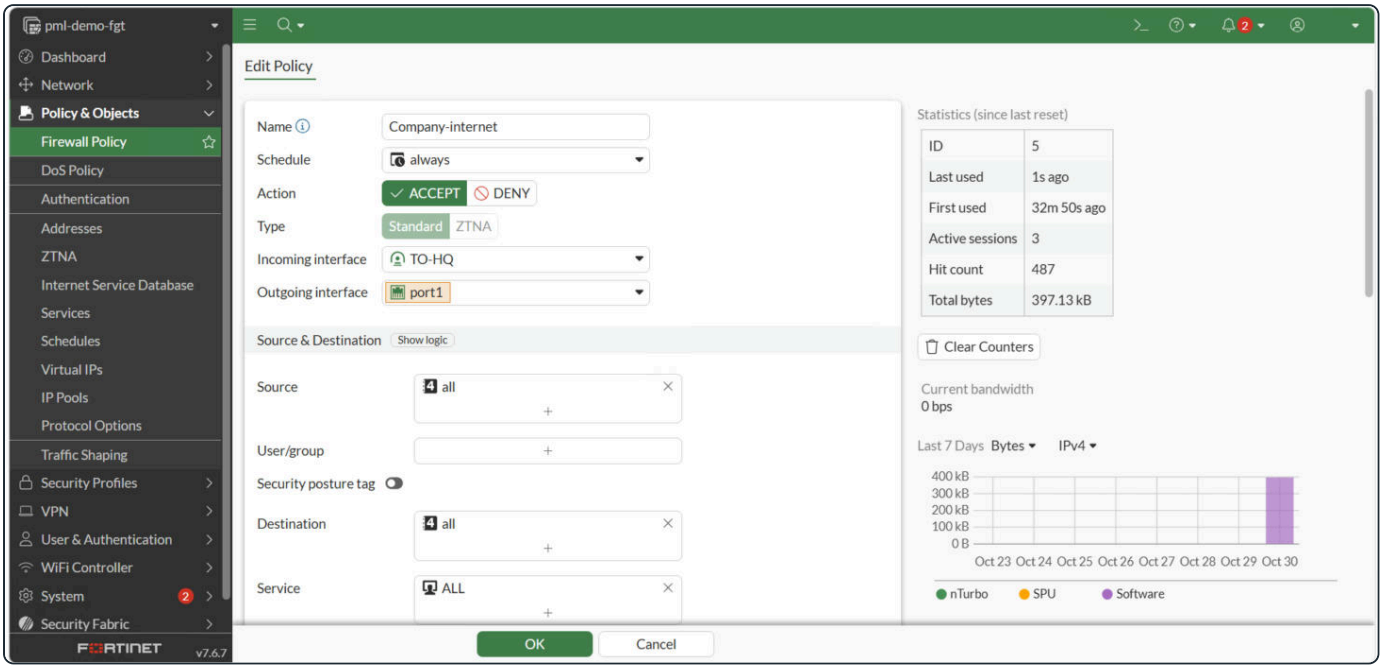


Figure 14: Azure FortiGate, policy Company-internet: from TO-HQ to port1.

> **CHECK** Name **Company-internet**, Action **ACCEPT**, Incoming interface **TO-HQ**, Outgoing interface **port1**, Source **all**, Destination **all**, Service **ALL**.

Now show the whole policy in the CLI of the Azure FortiGate:

```
show firewall policy 5
```

```
pml-demo-fgt # show firewall policy 5
config firewall policy
    edit 5
        set name "Company-internet"
        set uuid cd0728ae-d45a-51f1-9e5e-e04a78250025
        set srcintf "TO-HQ"
        set dstintf "port1"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set av-profile "default"
        set webfilter-profile "Company-WF"
        set dnsfilter-profile "Company-DNS"
        set ips-sensor "Company-IPS"
        set application-list "Company-APP"
        set logtraffic all
        set nat enable
    next
end
```

Figure 15: Azure FortiGate CLI: the policy Company-internet with all its security profiles.

> **CHECK** The policy names the profiles **default** (`av-profile`), **Company-WF**, **Company-DNS**, **Company-IPS** and **Application-APP**, and `ssl-ssh-profile "certificate-inspection"` . The `uuid` line is different on every FortiGate.

6 Paste block C on FGT-HQ (Appendix A2)

Now paste block C in the console of FGT-HQ. It does four things.

First, the underlay routes. Once HQ learns a default route from Azure, all traffic without a more specific route would go to Azure. That includes the tunnel packets to the branches and to Azure itself. These routes are more specific, so they win and keep the tunnels on the internet lines:

KEY LINES: ROUTES 3, 4 AND 5

```
config router static
    edit 3
        set dst 20.219.10.112 255.255.255.255
        set gateway 203.0.113.1
        set device "port1"
    next
    edit 4
        set dst 203.0.113.0 255.255.255.0
        set gateway 203.0.113.1
        set device "port1"
    next
    edit 5
        set dst 198.51.100.0 255.255.255.0
        set gateway 198.51.100.1
        set device "port3"
    next
end
```

Second, the tunnel and BGP. HQ dials the Azure address 20.219.10.112 over ISP1. BGP then runs with the neighbor 10.202.0.2 (AS 65100).

Third, four policies (numbers 7 to 10): HQ-to-Azure, Branches-to-Azure, Azure-to-HQ and Azure-to-branches. They allow traffic between the tunnel TO-AZURE and the LAN or the OVERLAY zone.

Fourth, the local lines become the backup. The two default routes get distance 250. A route learned by eBGP has distance 20, so the Azure route wins while it exists. If Azure is down, BGP loses it, and HQ uses the two static routes again within about 30 seconds. ISP1 is used first because of its priority.

KEY LINES: TUNNEL, BGP AND BACKUP ROUTES (EXCERPT OF BLOCK C)

```
config vpn ipsec phase1-interface
    edit "TO-AZURE"
        set interface "port1"
        set ike-version 2
        set localid "HQ"
        set remote-gw 20.219.10.112
        set network-id 10
        set psksecret YOUR-SECRET
        ...
config router bgp
    config neighbor
        edit "10.202.0.2"
            set remote-as 65100
            set soft-reconfiguration enable
config router static
    edit 1
        set distance 250
    next
    edit 2
        set distance 250
    next
end
```

7 Check the tunnel on both sides

On FGT-HQ open **VPN > IPsec Tunnels**.

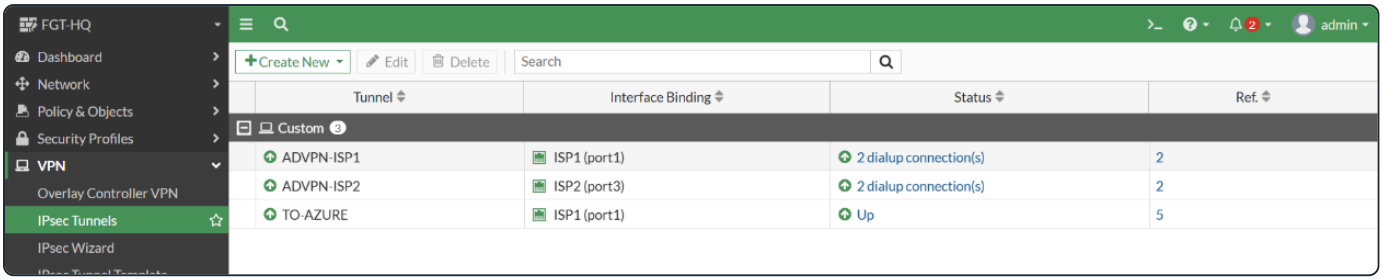


Figure 16: FGT-HQ IPsec tunnels, now with TO-AZURE.

> **CHECK** Besides ADVPN-ISP1 and ADVPN-ISP2, the new tunnel **TO-AZURE** (ISP1, port1) shows **Up**.

On the Azure FortiGate open **VPN > VPN Tunnels**.

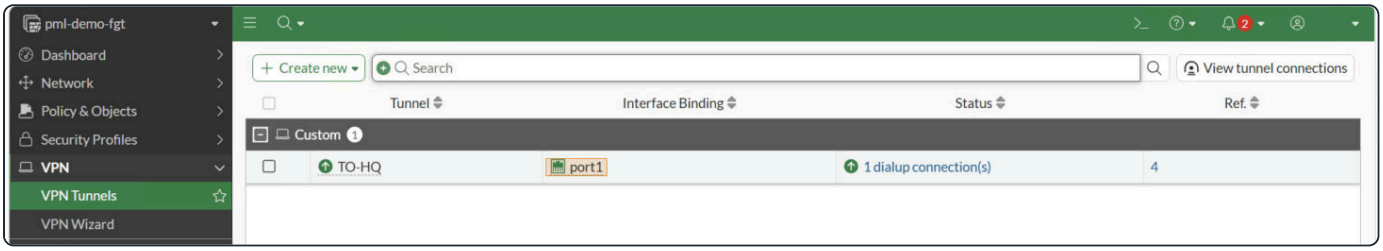


Figure 17: Azure FortiGate VPN tunnels: TO-HQ.

> **CHECK** The tunnel **TO-HQ** (port1) shows **1 dialup connection(s)**.

8 Check BGP on the Azure FortiGate

```
get router info bgp summary
get router info routing-table bgp
```

```
pml-demo-fgt # get router info bgp summary

VRF 0 BGP router identifier 10.202.0.2, local AS number 65100
BGP table version is 1
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.202.0.1 4      65000     228     226        1    0    0 00:32:55        4

Total number of neighbors 1


pml-demo-fgt # get router info routing-table bgp
Routing table for VRF=0
B       10.10.1.0/24 [20/0] via 10.202.0.1 (recursive is directly connected, TO-HQ), 00:32:31, [1/0]
B       10.10.2.0/24 [20/0] via 10.202.0.1 (recursive is directly connected, TO-HQ), 00:32:31, [1/0]
B       10.10.3.0/24 [20/0] via 10.202.0.1 (recursive is directly connected, TO-HQ), 00:32:31, [1/0]
B       10.200.0.1/32 [20/0] via 10.202.0.1 (recursive is directly connected, TO-HQ), 00:32:31, [1/0]
```

Figure 18: Azure FortiGate: BGP neighbor HQ and the routes learned from HQ.

> **CHECK** The neighbor **10.202.0.1** has AS **65000** and a number in *State/PfxRcd* (**4** in the figure). The BGP routing table lists **10.10.1.0/24**, **10.10.2.0/24**, **10.10.3.0/24** and **10.200.0.1/32**, all through **10.202.0.1** (TO-HQ). The routing entries have the form `[20/0]` : distance 20 is the distance of eBGP.

PART 7

Tests: shortcut, failover, internet through Azure, security checks

Goal: Prove that the network does what it should: a direct branch-to-branch shortcut, fast failover, internet through Azure, and security checks that block bad websites, attacks, viruses and applications.

Each step has a command or an action and a Check, and most steps have a figure. Tests 1 to 3 run in the CLI console of the FortiGates. In the GUI of a FortiGate, click the **>_** icon at the top right to open the **CLI Console**. Tests 4 to 8 run on BR1-PC. You read their results on the Azure FortiGate.

Test 1: the ADVPN shortcut (BR1 to BR2)

When BR1 talks to BR2, the first packets go through HQ. HQ then tells both branches to build a direct tunnel. After that, the traffic goes straight between the branches. You see the difference in the **TTL** of the ping replies. TTL (time to live) is a number inside every packet. It starts at 64 on the test host and each firewall that forwards the packet lowers it by 1. In a reply that you see on BR1, a lower number means more firewalls on the way.

1 Ping HQ-SRV and BR2-SRV from BR1, before the shortcut exists

Open the CLI Console of FGT-BR1 and run:

```
execute ping 10.10.1.10
execute ping 10.10.3.10
get vpn ipsec tunnel summary
```

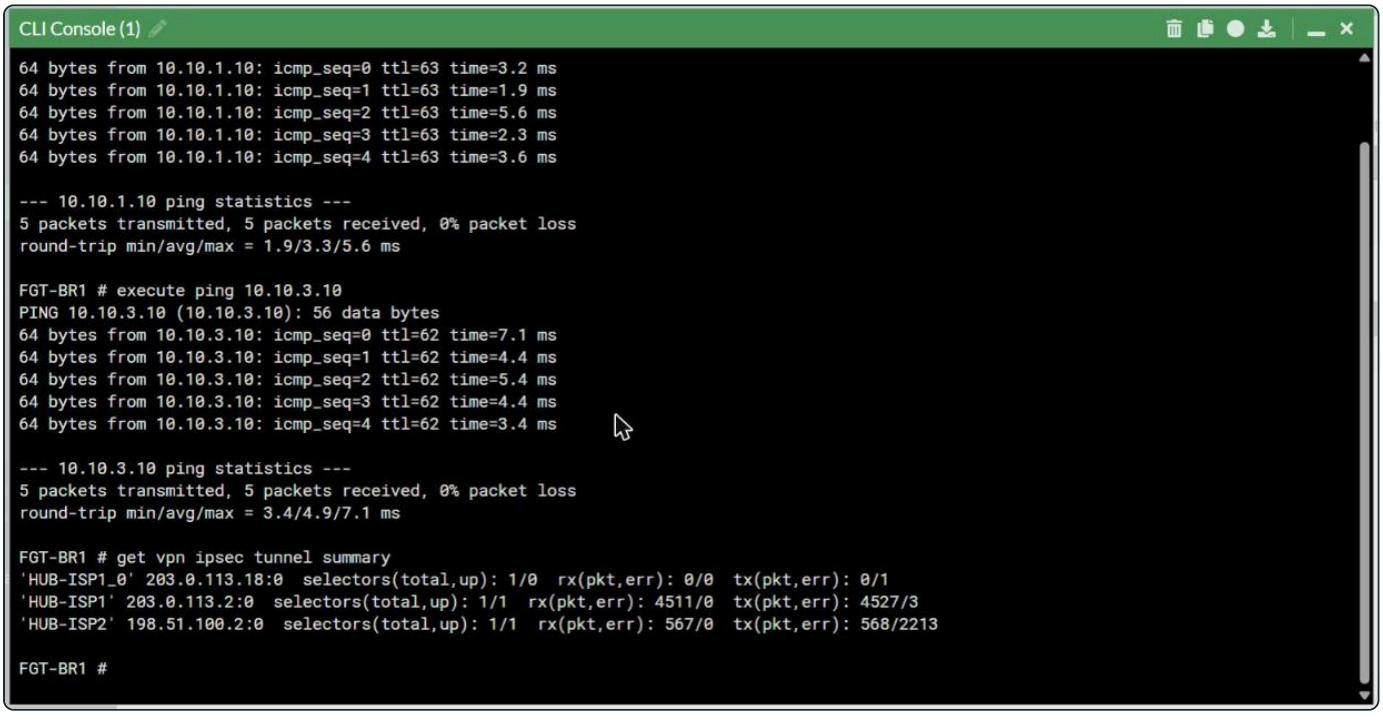


Figure 19: FGT-BR1 CLI: the pings before the shortcut.

> **CHECK** The ping to HQ-SRV (10.10.1.10) shows **ttl=63**: one firewall on the way, HQ. The ping to BR2-SRV (10.10.3.10) shows **ttl=62**: two firewalls, BR2 and HQ. The tunnel summary now has a third line, `'HUB-ISP1_0' 203.0.113.18:0`, with `selectors(total,up): 1/0`. This is the shortcut tunnel to BR2 (203.0.113.18) that is being built.

2 Ping again and look at the shortcut

```
execute ping 10.10.3.10
get vpn ipsec tunnel summary
```

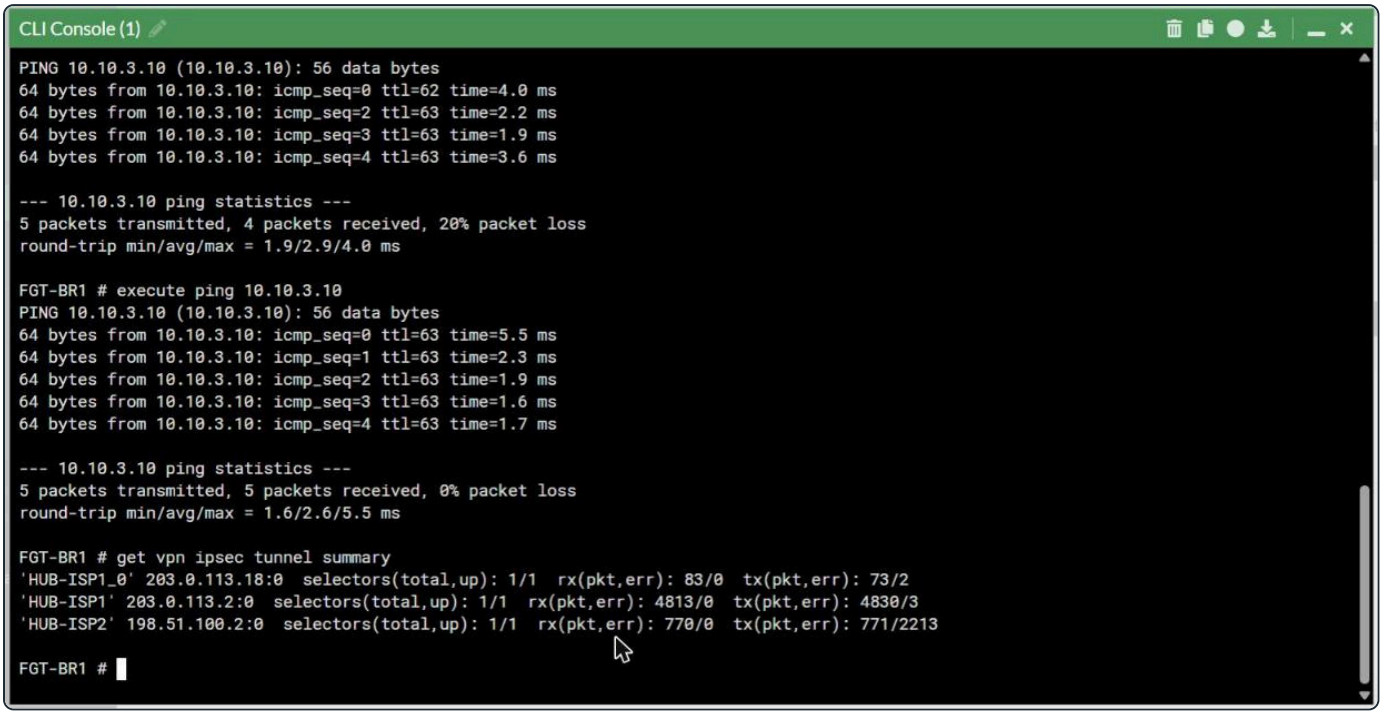


Figure 20: FGT-BR1 CLI: the shortcut tunnel HUB-ISP1_0 is up.

> **CHECK** The ping to BR2-SRV now shows **ttl=63**: only one firewall (BR2) on the way. The line `'HUB-ISP1_0' 203.0.113.18:0` now shows `selectors(total,up): 1/1`. The direct tunnel is up. One reply may be lost while the shortcut is being built (the figure shows 20% loss on the first run). This is normal.

Test 2: failover when ISP1 fails

You switch off the ISP1 line of BR1. The health check sees it, SD-WAN moves the traffic to the 4G tunnel, and BGP removes the dead routes.

3 Switch off port1 of FGT-BR1 and test

```
config system interface
    edit port1
        set status down
end
execute ping 10.10.1.10
get router info routing-table bgp
```

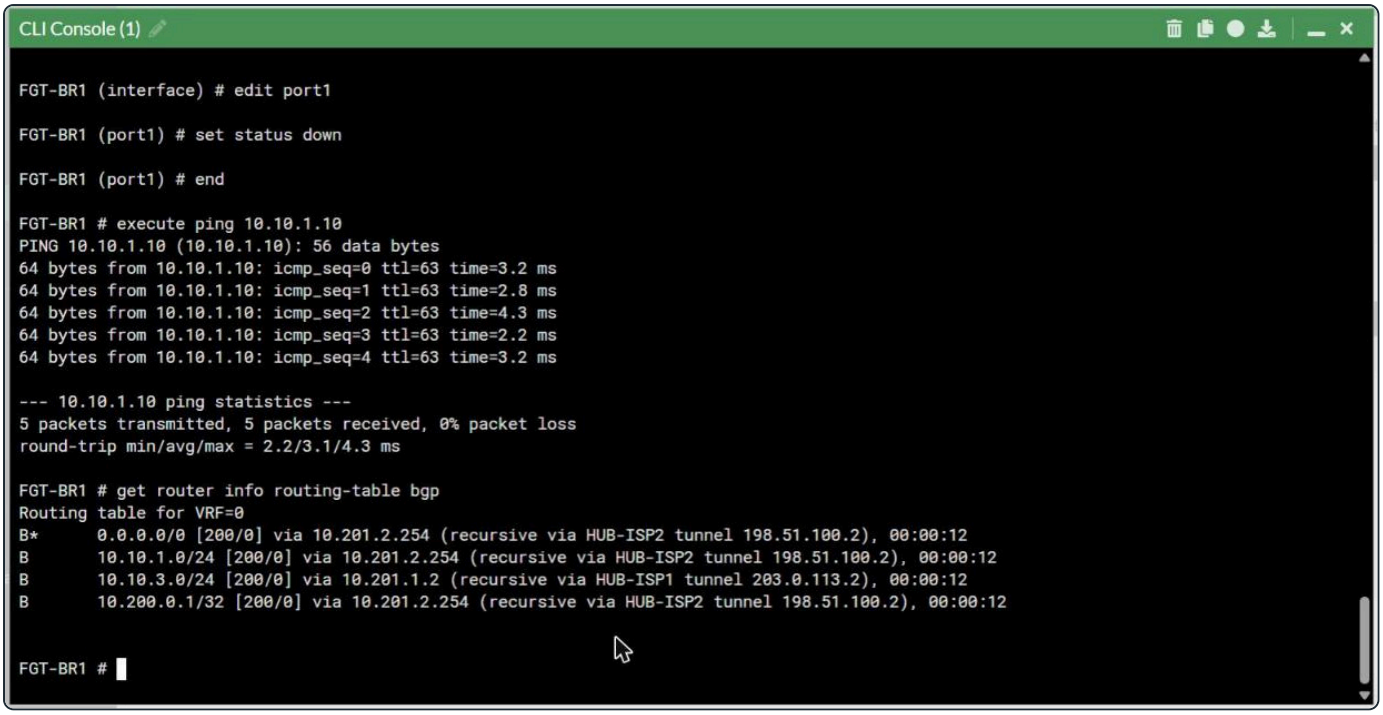


Figure 21: FGT-BR1 CLI: ISP1 (port1) is down, the ping still works.

> **CHECK** The ping to 10.10.1.10 still gets **5 replies**, 0% packet loss. The BGP routes for **0.0.0.0/0**, **10.10.1.0/24** and **10.200.0.1/32** now use the next hop **10.201.2.254**, through **HUB-ISP2** (4G). Look at these three routes. The line for 10.10.3.0/24 can still show the ISP1 tunnel for a few seconds after the failure, because BGP needs a few seconds to react.

4 Look at the SLA and the SD-WAN rules during the failover

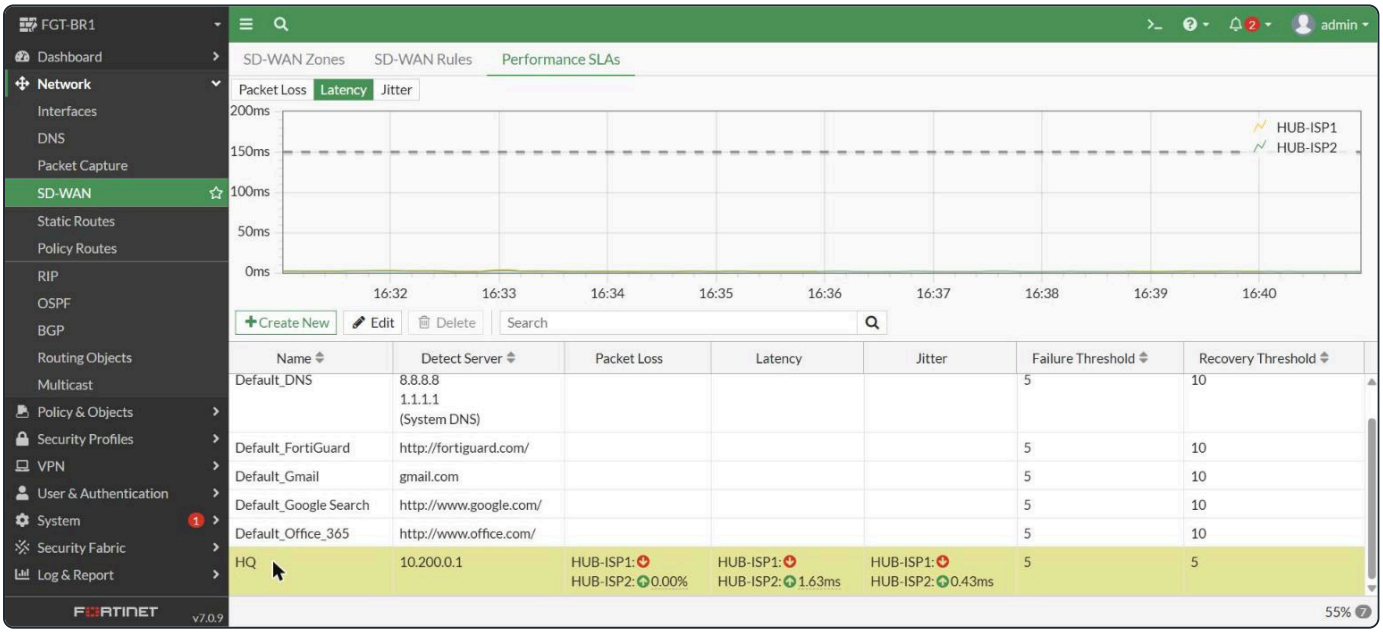


Figure 22: FGT-BR1 performance SLA during the failover.

> **CHECK** In the row **HQ**, **HUB-ISP1** shows a red down arrow and no numbers: the health check gets no replies. **HUB-ISP2** is green with normal numbers.

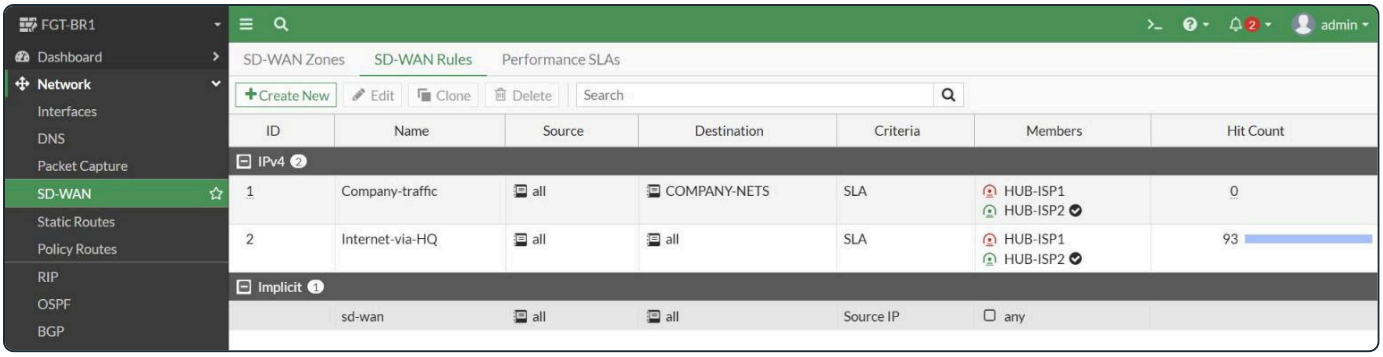


Figure 23: FGT-BR1 SD-WAN rules during the failover.

> **CHECK** In both rules, **HUB-ISP1** has a red icon, and the tick is now on **HUB-ISP2**. The hit count of **Internet-via-HQ** has grown (93 in the figure): the traffic uses the 4G tunnel.

5 Switch ISP1 on again

```
config system interface
    edit port1
        set status up
end
```

> **CHECK** After a short time, **HUB-ISP1** turns green again in the SD-WAN pages and the tick can return to it.

Test 3: internet through Azure

Now check that the internet traffic of HQ and the branches leaves through the Azure FortiGate.

6 Look at the default route on FGT-HQ

```
get router info routing-table all
```

```
FGT-HQ # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
B*      0.0.0.0/0 [20/0] via 10.202.0.2 (recursive via TO-AZURE tunnel 20.219.10.112), 00:00:54
C       10.10.1.0/24 is directly connected, port2
B       10.10.2.0/24 [200/0] via 10.201.1.1 (recursive is directly connected, ADVPN-ISP1), 00:58:42
                     [200/0] via 10.201.2.1 (recursive is directly connected, ADVPN-ISP2), 00:58:42
B       10.10.3.0/24 [200/0] via 10.201.1.2 (recursive is directly connected, ADVPN-ISP1), 01:02:29
                     [200/0] via 10.201.2.2 (recursive is directly connected, ADVPN-ISP2), 01:02:29
C       10.200.0.1/32 is directly connected, lo-hc
C       10.201.1.0/24 is directly connected, ADVPN-ISP1
C       10.201.1.254/32 is directly connected, ADVPN-ISP1
C       10.201.2.0/24 is directly connected, ADVPN-ISP2
C       10.201.2.254/32 is directly connected, ADVPN-ISP2
S       10.202.0.0/30 [5/0] via TO-AZURE tunnel 20.219.10.112, [1/0]
C       10.202.0.1/32 is directly connected, TO-AZURE
S       20.219.10.112/32 [10/0] via 203.0.113.1, port1, [1/0]
B       172.16.1.0/24 [20/0] via 10.202.0.2 (recursive via TO-AZURE tunnel 20.219.10.112), 00:00:54
C       192.168.122.0/24 is directly connected, port4
S       198.51.100.0/24 [10/0] via 198.51.100.1, port3, [1/0]
C       198.51.100.0/29 is directly connected, port3
--More--
```

Figure 24: FGT-HQ routing table: the default route is learned from Azure.

> **CHECK** The first route is `B* 0.0.0.0/0 [20/0] via 10.202.0.2 (recursive via TO-AZURE tunnel 20.219.10.112)`. **B*** is a BGP route that is the default route. The route `B 172.16.1.0/24` (the Azure LAN) is also learned from Azure. The two static default routes (distance 250) are not shown. The BGP route wins, so they are only kept as the backup.

7 Ping and trace the internet from FGT-HQ

```
execute ping 8.8.8.8
execute traceroute 8.8.8.8
```

```
64 bytes from 8.8.8.8: icmp_seq=0 ttl=112 time=41.6 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=112 time=42.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=112 time=41.8 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=112 time=40.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=112 time=42.0 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 40.1/41.6/42.8 ms

FGT-HQ # execute traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 32 hops max, 3 probe packets per hop, 84 byte packets
 1  10.202.0.2  36.108 ms  35.987 ms  37.163 ms
 2  * * *
```

Figure 25: FGT-HQ: ping and traceroute to 8.8.8.8 go through Azure.

> **CHECK** The ping gets replies (5 received, 0% packet loss). The traceroute shows **10.202.0.2** as hop 1: this is the Azure FortiGate. Hop 2 shows `* * *`: the device behind Azure does not answer the probes. This is normal.

8 Trace the internet from FGT-BR1

A branch computer would send its traffic with its LAN address as the source. The first command makes the FortiGate test the same way:

```
execute traceroute-options source 10.10.2.1
execute traceroute 8.8.8.8
```

```
FGT-BR1 # execute traceroute-options source 10.10.2.1

FGT-BR1 # execute traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 32 hops max, 3 probe packets per hop, 84 byte packets
 1  10.201.1.254  1.570 ms  2.154 ms  1.745 ms
 2  10.202.0.2  35.975 ms  40.759 ms  50.204 ms
 3  * * *
```

Figure 26: FGT-BR1: the internet path goes through HQ and then Azure.

> **CHECK** Hop 1 is **10.201.1.254** (HQ, through the tunnel). Hop 2 is **10.202.0.2** (Azure). Hop 3 shows `* * *`. So the branch traffic goes branch, HQ, Azure, internet.

9 Optional: Azure down

Stop the Azure FortiGate virtual machine in the Azure portal. Skip this test if other people use the Azure FortiGate at the same time. Wait about 30 seconds: the tunnel to Azure stops answering, and HQ drops the BGP neighbor 10.202.0.2. Then run on FGT-HQ:

```
get router info routing-table all
```

```
FGT-HQ # get router info routing-table all
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

Routing table for VRF=0
S*      0.0.0.0/0 [250/0] via 203.0.113.1, port1, [1/0]
                  [250/0] via 198.51.100.1, port3, [10/0]
C       10.10.1.0/24 is directly connected, port2
B       10.10.2.0/24 [200/0] via 10.201.1.1 (recursive is directly connected, ADVPN-ISP1), 05:52:46
                     [200/0] via 10.201.2.1 (recursive is directly connected, ADVPN-ISP2), 05:52:46
B       10.10.3.0/24 [200/0] via 10.201.1.2 (recursive is directly connected, ADVPN-ISP1), 05:52:51
                     [200/0] via 10.201.2.2 (recursive is directly connected, ADVPN-ISP2), 05:52:51
C       10.200.0.1/32 is directly connected, lo-hc
C       10.201.1.0/24 is directly connected, ADVPN-ISP1
C       10.201.1.254/32 is directly connected, ADVPN-ISP1
C       10.201.2.0/24 is directly connected, ADVPN-ISP2
C       10.201.2.254/32 is directly connected, ADVPN-ISP2
S       10.202.0.0/30 [5/0] via TO-AZURE tunnel 20.219.10.112, [1/0]
C       10.202.0.1/32 is directly connected, TO-AZURE
S       20.219.10.112/32 [10/0] via 203.0.113.1, port1, [1/0]
C       192.168.122.0/24 is directly connected, port4
S       198.51.100.0/24 [10/0] via 198.51.100.1, port3, [1/0]
C       198.51.100.0/29 is directly connected, port3
```

Figure 27: FGT-HQ routing table with Azure down: the default route is a static route again.

> **CHECK** The default route is now `S* 0.0.0.0/0 [250/0] via 203.0.113.1, port1` : the static route to ISP1. The second line, `via 198.51.100.1, port3` , is ISP2. **S*** is a static route that is the default route. The routes learned from Azure (the BGP default route and `172.16.1.0/24`) are gone.

```
execute ping 8.8.8.8
```

```
FGT-HQ # execute ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=126 time=12.0 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=126 time=12.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=126 time=10.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=126 time=10.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=126 time=10.7 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 10.3/11.1/12.1 ms
```

Figure 28: FGT-HQ: the internet works without Azure.

> **CHECK** The ping gets **5 replies**, 0% packet loss. HQ now reaches the internet through its own ISP1 line.

The branches keep their internet too, through HQ. On FGT-BR1 run the same trace as in step 8:

```
execute traceroute-options source 10.10.2.1
execute traceroute 8.8.8.8
```

```
FGT-BR1 # execute traceroute-options source 10.10.2.1

FGT-BR1 # execute traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 32 hops max, 3 probe packets per hop, 84 byte packets
 1  10.201.1.254  1.654 ms  2.113 ms  1.471 ms
 2  203.0.113.1  3.318 ms  3.107 ms  3.466 ms
 3  10.0.137.254  4.471 ms  3.798 ms  4.425 ms
 4  192.168.122.2  6.064 ms  4.993 ms  3.844 ms
```

Figure 29: FGT-BR1 with Azure down: the internet path goes through HQ and then ISP1.

> **CHECK** Hop 1 is **10.201.1.254** (HQ, through the tunnel), as before. Hop 2 is now **203.0.113.1**, the ISP1 router of HQ, and not Azure (10.202.0.2). The next hops are the way out of the lab to the internet, so in your lab they can be different. Stop the trace with **Ctrl+C**.

Start the Azure virtual machine again. After a few minutes the tunnel and the BGP neighbor are up again, and `get router info routing-table all` shows the BGP default route from Azure again, as in Figure 24.

Test 4: the web filter, from BR1-PC

The Azure policy **Company-internet** checks every connection. The URL filter blocks `*neverssl.com`, and the web filter blocks the category Social Networking.

---

10 Open neverssl.com on BR1-PC

On BR1-PC open **Firefox** and type `http://neverssl.com`. Type the `http://` part. neverssl.com is a plain http site, which is not encrypted.

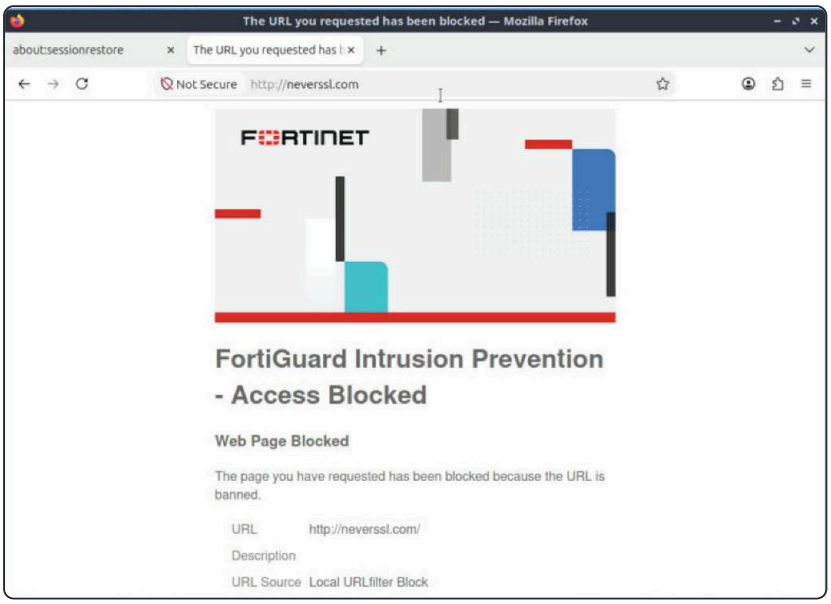


Figure 30: BR1-PC, Firefox: the block page of the Azure FortiGate.

> **CHECK** Firefox shows the clean **Fortinet block page** with the words **Web Page Blocked**. The big heading says *FortiGuard Intrusion Prevention - Access Blocked*. Do not worry about these words: the line **URL Source: Local URLfilter Block** tells you the real reason. Our own URL filter list stopped the page.

---

11 Open facebook.com on BR1-PC

In the same Firefox open `facebook.com`. This site is blocked too (category Social Networking). But facebook.com uses https, which is encrypted. The firewall stops the encrypted connection, so Firefox shows a **security warning**, not the clean block page. This is expected: the block worked.

12 Find the blocked websites in the web filter log

Open Log & Report > Security Events, tab **Logs**. Choose **Web Filter** and add the filter `Action == blocked`.

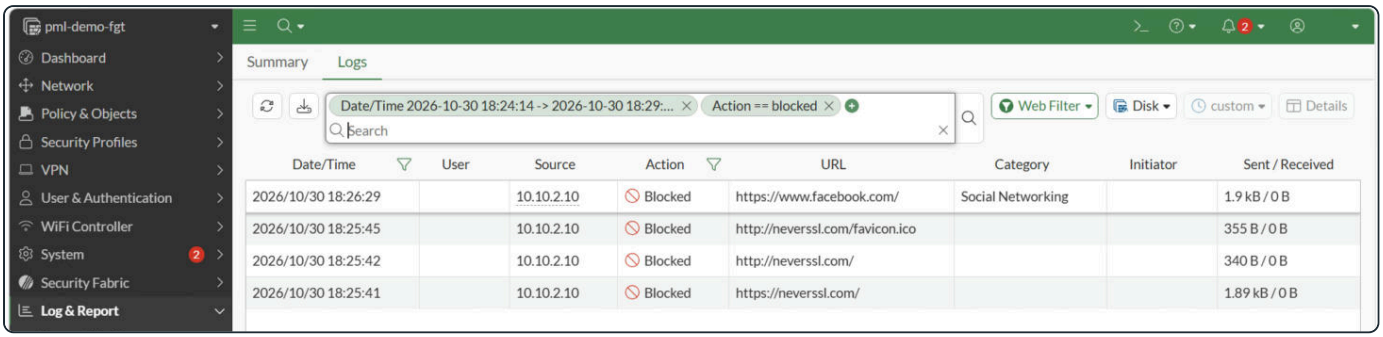


Figure 31: Azure FortiGate: web filter log with the blocked requests of BR1-PC.

> **CHECK** The list shows requests from the source **10.10.2.10** (BR1-PC) with the action **Blocked**: `https://www.facebook.com/` with the category **Social Networking**, and `http://neverssl.com/`. The browser itself also asked for `https://neverssl.com/` and `http://neverssl.com/favicon.ico` (the page icon). They are blocked too.

13 See the overview of the security events

Click the tab **Summary**. It shows what each security profile saw.

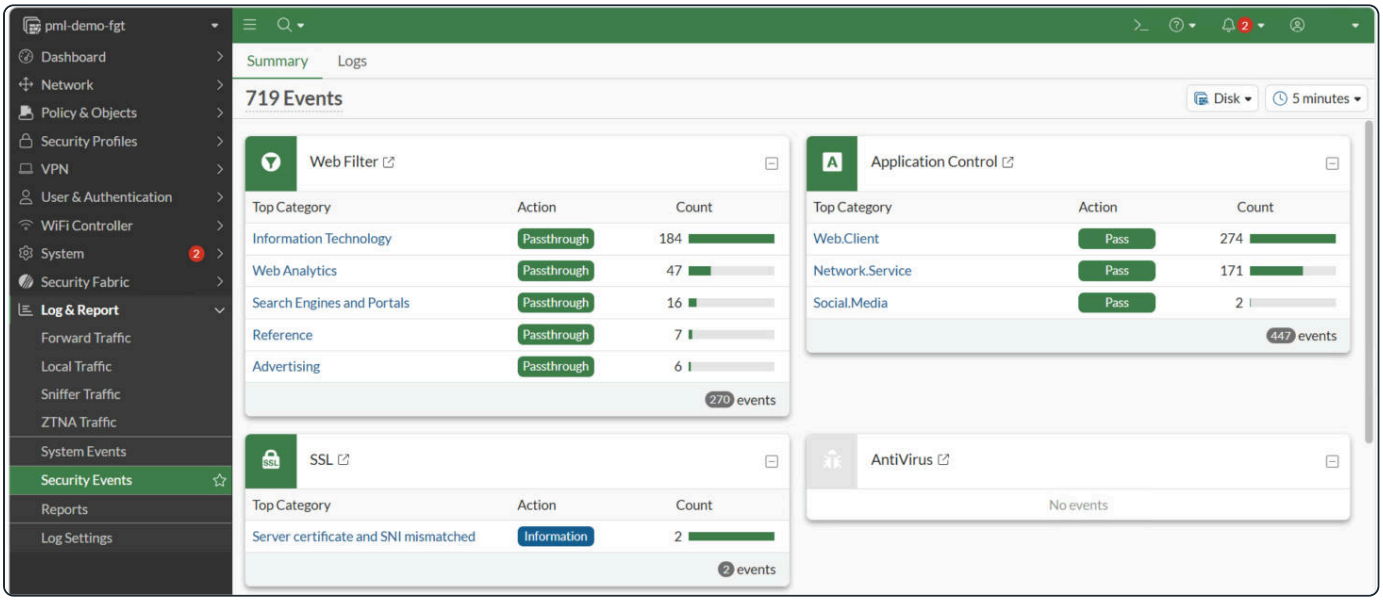


Figure 32: Azure FortiGate: security events summary.

> **CHECK** The summary lists the profiles **Web Filter**, **Application Control**, **SSL** and **AntiVirus**, each with its events. AntiVirus shows *No events*, because no virus has been sent yet (you send one in Test 7). The blocked websites are in the Logs tab (previous step).

Test 5: the DNS filter, from BR1-PC

The DNS filter looks at the name of a site when the computer asks for its address. The profile **Company-DNS** blocks the category Gambling. For a gambling site, the answer is not the real address.

14 Ask for the address of a gambling site

On BR1-PC open **QTerminal**, the terminal from Part 5. The command `nslookup` asks the DNS server for the address of a name. Run:

```
nslookup www.bet365.com
```

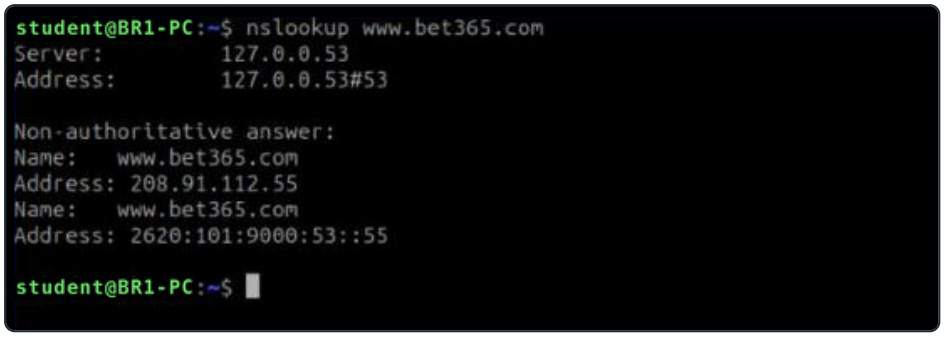


Figure 33: BR1-PC, QTerminal: the answer for www.bet365.com.

> **CHECK** The answer is **208.91.112.55**, and the IPv6 address `2620:101:9000:53::55`. This is the FortiGuard block address, not the real address of the site. The DNS filter sent it instead of the real answer, so the gambling site never opens. The line *Server: 127.0.0.53* is the small DNS service inside the PC. Ignore it.

Test 6: IPS, from BR1-PC

A real attack is not safe to try in a lab. So the lab uses the test signature **PML.Test.Signature**. It matches only one thing: the word `pingmylab-ips-test` in the path of a web address. A normal web address does not contain this word. The test address starts with `http://` because the IPS can read http traffic, which is not encrypted.

15 Send the test word, then a normal request

In QTerminal on BR1-PC run the first command. The command `curl` fetches a web address. The option `-m 10` makes it give up after 10 seconds.

```
curl -m 10 http://example.com/pingmylab-ips-test
```



Figure 34: BR1-PC, QTerminal: the request with the test word times out.

> **CHECK** After 10 seconds curl stops with `curl: (28) Operation timed out after 10002 milliseconds with 0 bytes received`. The number of milliseconds can be a little different. The Azure FortiGate dropped the request, so no answer came back.

Now run the second command. The option `-I` asks only for the first lines of the answer. This address has no test word in it.

```
curl -m 10 -I http://example.com/
```

> **CHECK** The first line of the answer is `HTTP/1.1 200 OK`. Only the test word is blocked. The same site works.

16 Find the dropped request in the IPS log

Open the CLI of the Azure FortiGate (see Part 6, step 1). The option `category 4` chooses the IPS log, and `view-lines 5` shows at most five entries. Run:

```
execute log filter reset
execute log filter device disk
execute log filter category 4
execute log filter view-lines 5
execute log display
```

```
pml-demo-fgt # execute log display
1 logs found.
1 logs returned.

1: date=2026-10-30 time=20:40:16 eventtime=1793373017214911745 tz="+0530" logid="0419016384" type="utm" subtype="ips" eventtype="signatu
re" level="alert" vd="root" severity="critical" srcip=10.10.2.10 srccountry="Reserved" dstip=172.66.147.243 dstcountry="United States" s
rcintf="TO-HQ" srcintfrole="undefined" dstintf="port1" dstintfrole="undefined" sessionid=47749 action="dropped" proto=6 service="HTTP" p
olicyid=5 poluuid="cd0728ae-d45a-51f1-9e5e-e04a78250025" policytype="policy" attack="PML.Test.Signature" srcport=55846 dstport=80 hostna
me="example.com" httpmethod="GET" direction="outgoing" attackid=2354 profile="Company-IPS" incidentserialno=266342268 msg="custom: PML.T
est.Signature" crscore=50 craction=4096 crlevel="critical" url="/pingmylab-ips-test" agent="curl/8.5.0"
```

Figure 35: Azure FortiGate CLI: the IPS log entry for the test signature.

> **CHECK** One log entry with `subtype="ips"`, `attack="PML.Test.Signature"`, `srcip=10.10.2.10` (BR1-PC) and `action="dropped"`. The entry also shows `attackid=2354`, the number from the block, and `url="/pingmylab-ips-test"`.

Test 7: antivirus, from BR1-PC

Every antivirus knows one harmless test text, the **EICAR test string**. It is not a virus, but every antivirus treats it as one. This guide writes it in a coded form (**base64**). The command `base64 -d` turns it back into the test string.

17 Send the EICAR test string

On BR1-PC run these commands. The first one writes the test string into the file `e.txt`. It is one command on two rows: the first row ends with the pipe sign `|`, and the second row continues it. The second command sends the content of the file to a website.

```
echo WDVPIVAlQEFQWzRcUFpYNTQoUF4pN0NDKTd9JEVJQ0FSLVNUQU5EQVJELUFOVElWSVJVUy1URVNULUZJTEUhJEgrSCo= |
    base64 -d > e.txt
curl -m 10 --data-binary @e.txt http://example.com/
```

```
    <body><div class="message-container">
    <div class="logo"></div>
    <h1>High Security Alert</h1>
    <p>You are not permitted to transfer the file "" because it is inf
ected with the virus "EICAR_TEST_FILE".</p>
    <table><tbody>
        <tr>
            <td>URL</td>
            <td>http://example.com/</td>
        </tr>
```

Figure 36: BR1-PC, QTerminal: part of the answer, the High Security Alert page.

> **CHECK** Curl prints the answer as text: the source of a web page. It contains `<h1>High Security Alert</h1>` and the words `infected with the virus "EICAR_TEST_FILE"`. The antivirus of the Azure FortiGate found the test string and blocked the transfer. The figure shows only a part of the answer. Delete the file when you are done: `rm e.txt`.

Test 8: application control, from BR1-PC

Application control recognises an application, for example YouTube, by its traffic. The list **Company-APP** blocks the category Video/Audio.

18 Open YouTube on BR1-PC

On BR1-PC open **Firefox** and go to `www.youtube.com`.

> **CHECK** The page **never loads**. Firefox stays stuck on the TLS handshake (the first exchange of an encrypted connection) and shows no block page. This is the expected result. YouTube uses https, and with certificate inspection the firewall cannot show a page inside an encrypted connection. So it only stops the connection. There is no figure, because Firefox shows no page.

19 Find the blocked application in the log

On the Azure FortiGate open **Log & Report > Security Events**, tab **Logs**, and choose **Application Control**. Figure 37 shows the log entries as the CLI prints them with `execute log display`.

```
3 logs found.
3 logs returned.

1: date=2026-10-30 time=20:45:17 eventtime=1793373316549817045 tz="+0530" logid="1059028705" type="utm" subtype="app-ctrl" eventtype="si
gnature" level="warning" vd="root" appid=31077 srcip=10.10.2.10 srccountry="Reserved" dstip=142.251.151.4 dstcountry="United States" src
port=44368 dstport=443 srcintf="TO-HQ" srcintfrole="undefined" dstintf="port1" dstintfrole="undefined" proto=6 service="SSL" direction="
outgoing" policyid=5 poluuid="cd0728ae-d45a-51f1-9e5e-e04a78250025" policytype="policy" sessionid=49038 applist="Company-APP" action="bl
ock" appcat="Video/Audio" app="YouTube" hostname="142.251.151.4" incidentserialno=266342377 msg="Video/Audio: YouTube" apprisk="elevated
"

2: date=2026-10-30 time=20:44:19 eventtime=1793373258376483045 tz="+0530" logid="1059028705" type="utm" subtype="app-ctrl" eventtype="si
gnature" level="warning" vd="root" appid=31077 srcip=10.10.2.10 srccountry="Reserved" dstip=142.251.151.4 dstcountry="United States" src
```

Figure 37: Azure FortiGate CLI: the application control log with the blocked YouTube requests.

> **CHECK** The entries show `srcip=10.10.2.10` (BR1-PC), `appcat="Video/Audio"`, `app="YouTube"`, `action="block"` and `applist="Company-APP"`. The figure has three entries, because Firefox tried more than once.

Live demo: SSL deep inspection

In Test 4, Firefox showed a security warning for facebook.com. The firewall cannot show a page inside an encrypted connection. With **deep inspection** the firewall opens the encrypted connection, looks inside, and closes it again with its own certificate. Then it can show its own block page. The browser must trust the certificate of the firewall for this. Radhe shows this live in the class, so it has no figure.

20 SSL deep inspection (live demo)

On the Azure FortiGate, download the certificate **Fortinet_CA_SSL**. This is the certificate that the firewall uses to sign the connections that it opens. Open **Security Profiles > SSL/SSH Inspection** and double-click the profile **deep-inspection**. In the line **CA certificate** (Fortinet_CA_SSL), click **Download**.

On BR1-PC, import the file in Firefox as a trusted authority: Settings, Privacy & Security, **View Certificates**, tab **Authorities**, **Import**. Choose the file and tick *Trust this CA to identify websites*.

On the Azure FortiGate, change the SSL inspection of the policy Company-internet to **deep-inspection**:

```
config firewall policy
    edit 5
        set ssl-ssh-profile "deep-inspection"
    next
end
```

Open `facebook.com` in Firefox again.

> **CHECK** Firefox shows the clean **Fortinet block page** for facebook.com, not the security warning of Test 4.

This is why companies push the certificate of the firewall to every PC. Without it, every encrypted site that the firewall opens shows a warning. When you finish, put `certificate-inspection` back in the line `set ssl-ssh-profile`, because the other tests in this guide expect it.

What this lab tested

WHAT	HOW IT WAS TESTED	WHERE
IPsec IKEv2 hub and spoke	The tunnels from BR1 and BR2 to HQ are up on both internet lines.	Parts 2 to 4
ADVPN shortcuts	The ping from BR1 to BR2 first shows TTL 62, through HQ. After the shortcut tunnel is built it shows TTL 63.	Test 1
SD-WAN with SLA and failover	ISP1 of BR1 is switched off. The SLA marks HUB-ISP1 down, the traffic moves to the 4G tunnel, and the ping still works.	Part 3, Test 2
iBGP route reflector	HQ has both branches as BGP neighbors and passes their routes on. BR1 learns the networks of HQ and BR2.	Parts 2 and 4, Test 2
eBGP to Azure	HQ learns the default route from Azure (distance 20), and the traceroute goes through 10.202.0.2.	Part 6, Test 3
Backup default route	With the Azure FortiGate stopped, HQ uses its static route to ISP1 again (distance 250), and HQ and BR1 still reach the internet.	Test 3, step 9
NAT	ISP-R and the policies on HQ and on Azure use NAT, and the pings and websites work.	Parts 1, 2 and 6, Test 3
DHCP	ISP-R gets its address by DHCP, and the LAN ports of HQ, BR1 and BR2 give addresses to the computers.	Parts 1 to 4
DNS	Names turn into addresses: BR1-PC opens websites by name, and the FortiGates use 8.8.8.8 and 1.1.1.1.	Parts 2 and 5, Tests 4 and 5
Web filter	neverssl.com is blocked by the URL filter, facebook.com by its category. The log shows both.	Test 4
DNS filter	The lookup of a gambling site answers with the block address 208.91.112.55.	Test 5
IPS	The request with the test word is dropped and logged. A normal request to the same site works.	Test 6
Antivirus	The EICAR test string is stopped, and the High Security Alert page comes back.	Test 7
Application control	YouTube never loads, and the log shows the application YouTube blocked.	Test 8
Certificate inspection	The firewall blocks facebook.com by its site name without opening the data. Deep inspection, with the certificate of the firewall in Firefox, is the live demo.	Test 4, live demo

APPENDIX A

The full paste blocks

These are the exact blocks used to build the lab, one section per device. Paste a whole block at once, then wait for the prompt.

BEFORE YOU PASTE In every block, **YOUR-SECRET** stands for the pre-shared key. Replace it with your own secret before you paste (see **Secrets** in *Before you start*). The boxes titled *Key lines* in the Parts show only some lines of a block. Do not paste them. The blocks below are complete: paste each one whole.

A1 ISP-R (Part 1)

A1 ISP-R: the whole router — 48 lines

```
no
enable
configure terminal
hostname ISP-R
no ip domain-lookup
interface GigabitEthernet0/0
 description NAT to the real internet
 ip address dhcp
 ip nat outside
 no shutdown
interface GigabitEthernet0/1
 description ISP1 to FGT-HQ port1
 ip address 203.0.113.1 255.255.255.248
 ip nat inside
 no shutdown
interface GigabitEthernet0/2
 description ISP1 to FGT-BR1 port1
 ip address 203.0.113.9 255.255.255.248
 ip nat inside
 no shutdown
interface GigabitEthernet0/3
 description ISP2 4G to FGT-BR1 port2
 ip address 198.51.100.9 255.255.255.248
 ip nat inside
 no shutdown
interface GigabitEthernet0/4
 description ISP1 to FGT-BR2 port1
 ip address 203.0.113.17 255.255.255.248
 ip nat inside
 no shutdown
interface GigabitEthernet0/5
 description ISP2 4G to FGT-BR2 port2
 ip address 198.51.100.17 255.255.255.248
 ip nat inside
 no shutdown
interface GigabitEthernet0/6
 description ISP2 4G to FGT-HQ port3
 ip address 198.51.100.1 255.255.255.248
 ip nat inside
 no shutdown
exit
ip access-list standard LAB-PUBLIC
 permit 203.0.113.0 0.0.0.255
 permit 198.51.100.0 0.0.0.255
exit
ip nat inside source list LAB-PUBLIC interface GigabitEthernet0/0 overload
end
write memory
```

A2 FGT-HQ (Parts 2 and 6)

A2 Block A: basics, two internet lines, routes (Part 2, step 2) 74 lines

```
config system global
    set hostname "FGT-HQ"
    set admintimeout 480
    set admin-https-redirect disable
end
config system interface
    edit "port1"
        set mode static
        set ip 203.0.113.2 255.255.255.248
        set allowaccess ping
        set alias "ISP1"
        set role wan
    next
    edit "port2"
        set mode static
        set ip 10.10.1.1 255.255.255.0
        set allowaccess ping
        set alias "HQ-LAN"
        set role lan
    next
    edit "port3"
        set mode static
        set ip 198.51.100.2 255.255.255.248
        set allowaccess ping
        set alias "ISP2"
        set role wan
    next
    edit "port4"
        set mode static
        set ip 192.168.122.21 255.255.255.0
        set allowaccess ping http ssh
        set alias "MGMT"
    next
end
config system dns
    set primary 8.8.8.8
    set secondary 1.1.1.1
end
config router static
    edit 1
        set gateway 203.0.113.1
        set device "port1"
        set comment "Internet via ISP1 (preferred: priority 1)"
    next
    edit 2
        set gateway 198.51.100.1
        set device "port3"
        set distance 10
        set priority 10
        set comment "Internet via ISP2 (backup: priority 10, always ready)"
    next
end
config system dhcp server
    edit 1
        set dns-service default
        set default-gateway 10.10.1.1
        set netmask 255.255.255.0
        set interface "port2"
        config ip-range
            edit 1
                set start-ip 10.10.1.100
                set end-ip 10.10.1.150
            next
        end
    next
end
```

```
config system interface
    edit "lo-hc"
        set vdom "root"
        set type loopback
        set ip 10.200.0.1 255.255.255.255
        set allowaccess ping
    next
end
```

A2 Block B: VPN hub, BGP, policies (Part 2, step 3) 173 lines

```
config vpn ipsec phase1-interface
    edit "ADVPN-ISP1"
        set type dynamic
        set interface "port1"
        set ike-version 2
        set peertype any
        set net-device disable
        set exchange-interface-ip enable
        set proposal des-sha256
        set dhgrp 14 5 2
        set add-route disable
        set dpd on-idle
        set auto-discovery-sender enable
        set tunnel-search nexthop
        set network-overlay enable
        set network-id 1
        set psksecret YOUR-SECRET
        set dpd-retryinterval 5
    next
    edit "ADVPN-ISP2"
        set type dynamic
        set interface "port3"
        set ike-version 2
        set peertype any
        set net-device disable
        set exchange-interface-ip enable
        set proposal des-sha256
        set dhgrp 14 5 2
        set add-route disable
        set dpd on-idle
        set auto-discovery-sender enable
        set tunnel-search nexthop
        set network-overlay enable
        set network-id 2
        set psksecret YOUR-SECRET
        set dpd-retryinterval 5
    next
end
config vpn ipsec phase2-interface
    edit "ADVPN-ISP1"
        set phase1name "ADVPN-ISP1"
        set proposal des-sha256
        set dhgrp 14 5 2
    next
    edit "ADVPN-ISP2"
        set phase1name "ADVPN-ISP2"
        set proposal des-sha256
        set dhgrp 14 5 2
    next
end
config system interface
    edit "ADVPN-ISP1"
        set ip 10.201.1.254 255.255.255.255
        set remote-ip 10.201.1.253 255.255.255.0
        set allowaccess ping
    next
    edit "ADVPN-ISP2"
        set ip 10.201.2.254 255.255.255.255
        set remote-ip 10.201.2.253 255.255.255.0
        set allowaccess ping
    next
```

```
end
config system zone
    edit "OVERLAY"
        set intrazone allow
        set interface "ADVPN-ISP1" "ADVPN-ISP2"
    next
end
config router bgp
    set as 65000
    set router-id 10.200.0.1
    set ibgp-multipath enable
    config neighbor-group
        edit "SPOKES-ISP1"
            set remote-as 65000
            set keep-alive-timer 5
            set holdtime-timer 15
            set route-reflector-client enable
            set capability-default-originate enable
            set soft-reconfiguration enable
        next
        edit "SPOKES-ISP2"
            set remote-as 65000
            set keep-alive-timer 5
            set holdtime-timer 15
            set route-reflector-client enable
            set capability-default-originate enable
            set soft-reconfiguration enable
        next
    end
    config neighbor-range
        edit 1
            set prefix 10.201.1.0 255.255.255.0
            set neighbor-group "SPOKES-ISP1"
        next
        edit 2
            set prefix 10.201.2.0 255.255.255.0
            set neighbor-group "SPOKES-ISP2"
        next
    end
    config network
        edit 1
            set prefix 10.10.1.0 255.255.255.0
        next
        edit 2
            set prefix 10.200.0.1 255.255.255.255
        next
    end
end
config firewall policy
    edit 1
        set name "Branch-to-branch"
        set srcintf "OVERLAY"
        set dstintf "OVERLAY"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "Branches-to-HQ"
        set srcintf "OVERLAY"
        set dstintf "port2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 3
        set name "HQ-to-branches"
        set srcintf "port2"
        set dstintf "OVERLAY"
```

```
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 4
        set name "Health-checks"
        set srcintf "OVERLAY"
        set dstintf "lo-hc"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "PING"
    next
    edit 5
        set name "HQ-internet"
        set srcintf "port2"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
    edit 6
        set name "Branch-internet"
        set srcintf "OVERLAY"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

A2 Block C: underlay routes, tunnel to Azure, BGP, policies, local internet becomes backup (Part 6, step 6) 111 lines

```
config router static
    edit 3
        set dst 20.219.10.112 255.255.255.255
        set gateway 203.0.113.1
        set device "port1"
        set comment "Azure FortiGate over ISP1"
    next
    edit 4
        set dst 203.0.113.0 255.255.255.0
        set gateway 203.0.113.1
        set device "port1"
        set comment "Branches ISP1 side (keeps tunnels on the underlay)"
    next
    edit 5
        set dst 198.51.100.0 255.255.255.0
        set gateway 198.51.100.1
        set device "port3"
        set comment "Branches ISP2 side (keeps tunnels on the underlay)"
    next
end
config vpn ipsec phase1-interface
    edit "TO-AZURE"
        set interface "port1"
        set ike-version 2
        set peertype any
        set proposal des-sha256
        set dhgrp 14 5 2
        set localid "HQ"
        set remote-gw 20.219.10.112
        set network-overlay enable
```

```
        set network-id 10
        set dpd on-idle
        set dpd-retryinterval 5
        set psksecret YOUR-SECRET
    next
end
config vpn ipsec phase2-interface
    edit "TO-AZURE"
        set phase1name "TO-AZURE"
        set proposal des-sha256
        set dhgrp 14 5 2
        set auto-negotiate enable
    next
end
config system interface
    edit "TO-AZURE"
        set ip 10.202.0.1 255.255.255.255
        set remote-ip 10.202.0.2 255.255.255.252
        set allowaccess ping
    next
end
config router bgp
    config neighbor
        edit "10.202.0.2"
            set remote-as 65100
            set soft-reconfiguration enable
        next
    end
end
config firewall policy
    edit 7
        set name "HQ-to-Azure"
        set srcintf "port2"
        set dstintf "TO-AZURE"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 8
        set name "Branches-to-Azure"
        set srcintf "OVERLAY"
        set dstintf "TO-AZURE"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 9
        set name "Azure-to-HQ"
        set srcintf "TO-AZURE"
        set dstintf "port2"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 10
        set name "Azure-to-branches"
        set srcintf "TO-AZURE"
        set dstintf "OVERLAY"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
config router static
    edit 1
```

```
        set distance 250
        set comment "Backup internet via ISP1 if Azure is down"
    next
    edit 2
        set distance 250
        set comment "Backup internet via ISP2 (priority 10)"
    next
end
```

A3 FGT-BR1 (Part 3)

A3 Block A: basics, two internet lines, routes, DHCP (Part 3, step 1) 91 lines

```
config system global
    set hostname "FGT-BR1"
    set admintimeout 480
    set admin-https-redirect disable
end
config system interface
    edit "port1"
        set mode static
        set ip 203.0.113.10 255.255.255.248
        set allowaccess ping
        set alias "ISP1-broadband"
        set role wan
    next
    edit "port2"
        set mode static
        set ip 198.51.100.10 255.255.255.248
        set allowaccess ping
        set alias "ISP2-4G"
        set role wan
    next
    edit "port3"
        set mode static
        set ip 10.10.2.1 255.255.255.0
        set allowaccess ping
        set alias "BR1-LAN"
        set role lan
    next
    edit "port4"
        set mode static
        set ip 192.168.122.22 255.255.255.0
        set allowaccess ping http ssh
        set alias "MGMT"
    next
end
config system dns
    set primary 8.8.8.8
    set secondary 1.1.1.1
end
config router static
    edit 1
        set dst 203.0.113.2 255.255.255.255
        set gateway 203.0.113.9
        set device "port1"
        set comment "HQ over ISP1"
    next
    edit 2
        set dst 198.51.100.2 255.255.255.255
        set gateway 198.51.100.9
        set device "port2"
        set comment "HQ over ISP2"
    next
    edit 3
        set gateway 203.0.113.9
        set device "port1"
        set distance 250
        set comment "Backup internet if both tunnels are down"
    next
    edit 4
```

```
        set dst 203.0.113.0 255.255.255.0
        set gateway 203.0.113.9
        set device "port1"
        set comment "ISP1 network direct (underlay for tunnels)"
    next
    edit 5
        set dst 198.51.100.0 255.255.255.0
        set gateway 198.51.100.9
        set device "port2"
        set comment "ISP2 network direct (underlay for tunnels)"
    next
end
config system dhcp server
    edit 1
        set dns-service default
        set default-gateway 10.10.2.1
        set netmask 255.255.255.0
        set interface "port3"
        config ip-range
            edit 1
                set start-ip 10.10.2.100
                set end-ip 10.10.2.150
            next
        end
        config reserved-address
            edit 1
                set ip 10.10.2.10
                set mac 50:cc:11:03:f9:00
                set description "BR1-PC"
            next
        end
    next
end
```

A3 Block B: VPN, SD-WAN, BGP, policies (Part 3, step 2) 184 lines

```
config vpn ipsec phase1-interface
    edit "HUB-ISP1"
        set interface "port1"
        set ike-version 2
        set peertype any
        set net-device enable
        set exchange-interface-ip enable
        set proposal des-sha256
        set dhgrp 14 5 2
        set add-route disable
        set dpd on-idle
        set auto-discovery-receiver enable
        set network-overlay enable
        set network-id 1
        set remote-gw 203.0.113.2
        set psksecret YOUR-SECRET
        set dpd-retryinterval 5
    next
    edit "HUB-ISP2"
        set interface "port2"
        set ike-version 2
        set peertype any
        set net-device enable
        set exchange-interface-ip enable
        set proposal des-sha256
        set dhgrp 14 5 2
        set add-route disable
        set dpd on-idle
        set auto-discovery-receiver enable
        set network-overlay enable
        set network-id 2
        set remote-gw 198.51.100.2
        set psksecret YOUR-SECRET
        set dpd-retryinterval 5
    next
end
```

```
config vpn ipsec phase2-interface
    edit "HUB-ISP1"
        set phase1name "HUB-ISP1"
        set proposal des-sha256
        set dhgrp 14 5 2
        set auto-negotiate enable
    next
    edit "HUB-ISP2"
        set phase1name "HUB-ISP2"
        set proposal des-sha256
        set dhgrp 14 5 2
        set auto-negotiate enable
    next
end
config system interface
    edit "HUB-ISP1"
        set ip 10.201.1.1 255.255.255.255
        set remote-ip 10.201.1.254 255.255.255.0
        set allowaccess ping
    next
    edit "HUB-ISP2"
        set ip 10.201.2.1 255.255.255.255
        set remote-ip 10.201.2.254 255.255.255.0
        set allowaccess ping
    next
end
config firewall address
    edit "COMPANY-NETS"
        set subnet 10.10.0.0 255.255.0.0
    next
end
config system sdwan
    set status enable
    config zone
        edit "OVERLAY"
        next
    end
    config members
        edit 1
            set interface "HUB-ISP1"
            set zone "OVERLAY"
        next
        edit 2
            set interface "HUB-ISP2"
            set zone "OVERLAY"
        next
    end
    config health-check
        edit "HQ"
            set server "10.200.0.1"
            set members 1 2
            config sla
                edit 1
                    set link-cost-factor latency packet-loss
                    set latency-threshold 150
                    set packetloss-threshold 2
                next
            end
        next
    end
    config service
        edit 1
            set name "Company-traffic"
            set mode sla
            set src "all"
            set dst "COMPANY-NETS"
            config sla
                edit "HQ"
                    set id 1
                next
            end
            set priority-members 1 2
        next
```

```
        edit 2
            set name "Internet-via-HQ"
            set mode sla
            set src "all"
            set dst "all"
            config sla
                edit "HQ"
                    set id 1
                next
            end
            set priority-members 1 2
        next
    end
end
config router bgp
    set as 65000
    set router-id 10.10.2.1
    set ibgp-multipath enable
    config neighbor
        edit "10.201.1.254"
            set remote-as 65000
            set keep-alive-timer 5
            set holdtime-timer 15
            set link-down-failover enable
            set advertisement-interval 1
            set soft-reconfiguration enable
        next
        edit "10.201.2.254"
            set remote-as 65000
            set keep-alive-timer 5
            set holdtime-timer 15
            set link-down-failover enable
            set advertisement-interval 1
            set soft-reconfiguration enable
        next
    end
    config network
        edit 1
            set prefix 10.10.2.0 255.255.255.0
        next
    end
end
config firewall policy
    edit 1
        set name "LAN-to-company-and-internet"
        set srcintf "port3"
        set dstintf "OVERLAY"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "Company-to-LAN"
        set srcintf "OVERLAY"
        set dstintf "port3"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 3
        set name "Backup-internet"
        set srcintf "port3"
        set dstintf "port1"
```

```
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

A4 FGT-BR2 (Part 4)

A4 Block A: basics, two internet lines, routes, DHCP (Part 4, step 1) 84 lines

```
config system global
    set hostname "FGT-BR2"
    set admintimeout 480
    set admin-https-redirect disable
end
config system interface
    edit "port1"
        set mode static
        set ip 203.0.113.18 255.255.255.248
        set allowaccess ping
        set alias "ISP1-broadband"
        set role wan
    next
    edit "port2"
        set mode static
        set ip 198.51.100.18 255.255.255.248
        set allowaccess ping
        set alias "ISP2-4G"
        set role wan
    next
    edit "port3"
        set mode static
        set ip 10.10.3.1 255.255.255.0
        set allowaccess ping
        set alias "BR2-LAN"
        set role lan
    next
    edit "port4"
        set mode static
        set ip 192.168.122.23 255.255.255.0
        set allowaccess ping http ssh
        set alias "MGMT"
    next
end
config system dns
    set primary 8.8.8.8
    set secondary 1.1.1.1
end
config router static
    edit 1
        set dst 203.0.113.2 255.255.255.255
        set gateway 203.0.113.17
        set device "port1"
        set comment "HQ over ISP1"
    next
    edit 2
        set dst 198.51.100.2 255.255.255.255
        set gateway 198.51.100.17
        set device "port2"
        set comment "HQ over ISP2"
    next
    edit 3
        set gateway 203.0.113.17
        set device "port1"
        set distance 250
        set comment "Backup internet if both tunnels are down"
    next
    edit 4
```

```
        set dst 203.0.113.0 255.255.255.0
        set gateway 203.0.113.17
        set device "port1"
        set comment "ISP1 network direct (underlay for tunnels)"
    next
    edit 5
        set dst 198.51.100.0 255.255.255.0
        set gateway 198.51.100.17
        set device "port2"
        set comment "ISP2 network direct (underlay for tunnels)"
    next
end
config system dhcp server
    edit 1
        set dns-service default
        set default-gateway 10.10.3.1
        set netmask 255.255.255.0
        set interface "port3"
        config ip-range
            edit 1
                set start-ip 10.10.3.100
                set end-ip 10.10.3.150
            next
        end
    next
end
```

A4 Block B: VPN, SD-WAN, BGP, policies (Part 4, step 2) 184 lines

```
config vpn ipsec phase1-interface
    edit "HUB-ISP1"
        set interface "port1"
        set ike-version 2
        set peertype any
        set net-device enable
        set exchange-interface-ip enable
        set proposal des-sha256
        set dhgrp 14 5 2
        set add-route disable
        set dpd on-idle
        set auto-discovery-receiver enable
        set network-overlay enable
        set network-id 1
        set remote-gw 203.0.113.2
        set psksecret YOUR-SECRET
        set dpd-retryinterval 5
    next
    edit "HUB-ISP2"
        set interface "port2"
        set ike-version 2
        set peertype any
        set net-device enable
        set exchange-interface-ip enable
        set proposal des-sha256
        set dhgrp 14 5 2
        set add-route disable
        set dpd on-idle
        set auto-discovery-receiver enable
        set network-overlay enable
        set network-id 2
        set remote-gw 198.51.100.2
        set psksecret YOUR-SECRET
        set dpd-retryinterval 5
    next
end
config vpn ipsec phase2-interface
    edit "HUB-ISP1"
        set phase1name "HUB-ISP1"
        set proposal des-sha256
        set dhgrp 14 5 2
        set auto-negotiate enable
    next
```

```
    edit "HUB-ISP2"
        set phase1name "HUB-ISP2"
        set proposal des-sha256
        set dhgrp 14 5 2
        set auto-negotiate enable
    next
end
config system interface
    edit "HUB-ISP1"
        set ip 10.201.1.2 255.255.255.255
        set remote-ip 10.201.1.254 255.255.255.0
        set allowaccess ping
    next
    edit "HUB-ISP2"
        set ip 10.201.2.2 255.255.255.255
        set remote-ip 10.201.2.254 255.255.255.0
        set allowaccess ping
    next
end
config firewall address
    edit "COMPANY-NETS"
        set subnet 10.10.0.0 255.255.0.0
    next
end
config system sdwan
    set status enable
    config zone
        edit "OVERLAY"
        next
    end
    config members
        edit 1
            set interface "HUB-ISP1"
            set zone "OVERLAY"
        next
        edit 2
            set interface "HUB-ISP2"
            set zone "OVERLAY"
        next
    end
    config health-check
        edit "HQ"
            set server "10.200.0.1"
            set members 1 2
            config sla
                edit 1
                    set link-cost-factor latency packet-loss
                    set latency-threshold 150
                    set packetloss-threshold 2
                next
            end
        next
    end
    config service
        edit 1
            set name "Company-traffic"
            set mode sla
            set src "all"
            set dst "COMPANY-NETS"
            config sla
                edit "HQ"
                    set id 1
                next
            end
            set priority-members 1 2
        next
        edit 2
            set name "Internet-via-HQ"
            set mode sla
            set src "all"
            set dst "all"
            config sla
                edit "HQ"
```

```
                    set id 1
                next
            end
            set priority-members 1 2
        next
    end
end
config router bgp
    set as 65000
    set router-id 10.10.3.1
    set ibgp-multipath enable
    config neighbor
        edit "10.201.1.254"
            set remote-as 65000
            set keep-alive-timer 5
            set holdtime-timer 15
            set link-down-failover enable
            set advertisement-interval 1
            set soft-reconfiguration enable
        next
        edit "10.201.2.254"
            set remote-as 65000
            set keep-alive-timer 5
            set holdtime-timer 15
            set link-down-failover enable
            set advertisement-interval 1
            set soft-reconfiguration enable
        next
    end
    config network
        edit 1
            set prefix 10.10.3.0 255.255.255.0
        next
    end
end
config firewall policy
    edit 1
        set name "LAN-to-company-and-internet"
        set srcintf "port3"
        set dstintf "OVERLAY"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "Company-to-LAN"
        set srcintf "OVERLAY"
        set dstintf "port3"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
    next
    edit 3
        set name "Backup-internet"
        set srcintf "port3"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

A5 The test computers (Part 5)

A5 HQ-SRV (VPCS) 2 lines

```
ip 10.10.1.10/24 10.10.1.1
save
```

A5 BR2-SRV (VPCS) 2 lines

```
ip 10.10.3.10/24 10.10.3.1
save
```

A5 BR1-PC (Linux, run in QTerminal) 2 lines

```
nmcli con mod lan ipv4.addresses 10.10.2.10/24 ipv4.gateway 10.10.2.1 ipv4.dns 8.8.8.8
nmcli con up lan
```

A6 Azure FortiGate (Part 6)

IMPORTANT The line `set rule 2354` in this block is the **attack_id** that the Azure FortiGate of the class gave to the test signature. On another FortiGate, run `show ips custom` and use the number shown after `--attack_id` (see Part 6, step 4). The line `set signature` is one single line, shown on two rows here. Join the two rows before you paste.

A6 Azure FortiGate: tunnel to HQ, BGP, security profiles, policies (Part 6, step 3) 185 lines

```
config vpn ipsec phase1-interface
    edit "TO-HQ"
        set type dynamic
        set interface "port1"
        set ike-version 2
        set peertype any
        set net-device disable
        set proposal des-sha256
        set dhgrp 14 5 2
        set add-route disable
        set network-overlay enable
        set network-id 10
        set dpd on-idle
        set dpd-retryinterval 5
        set psksecret YOUR-SECRET
    next
end
config vpn ipsec phase2-interface
    edit "TO-HQ"
        set phase1name "TO-HQ"
        set proposal des-sha256
        set dhgrp 14 5 2
    next
end
config system interface
    edit "TO-HQ"
        set ip 10.202.0.2 255.255.255.255
        set remote-ip 10.202.0.1 255.255.255.252
        set allowaccess ping
    next
end
config router static
    edit 3
        set dst 172.16.1.0 255.255.255.0
        set gateway 172.16.0.65
        set device "port2"
        set comment "Azure LAN (protected subnet)"
    next
end
config router bgp
```

```
    set as 65100
    set router-id 10.202.0.2
    config neighbor
        edit "10.202.0.1"
            set remote-as 65000
            set capability-default-originate enable
            set keep-alive-timer 10
            set holdtime-timer 30
            set soft-reconfiguration enable
        next
    end
    config network
        edit 1
            set prefix 172.16.1.0 255.255.255.0
        next
    end
end
config webfilter urlfilter
    edit 10
        set name "Company-blocked-sites"
        config entries
            edit 1
                set url "*neverssl.com"
                set type wildcard
                set action block
            next
        end
    next
end
config webfilter profile
    edit "Company-WF"
        set comment "Masterclass: company internet through Azure"
        set log-all-url enable
        config web
            set urlfilter-table 10
        end
        config ftgd-wf
            config filters
                edit 100
                    set category 37
                    set action block
                next
                edit 101
                    set category 20
                    set action block
                next
            end
        end
    next
end
config application list
    edit "Company-APP"
        set comment "Masterclass: block video streaming, P2P and proxies"
        set other-application-log enable
        config entries
            edit 1
                set category 5
                set action block
            next
            edit 2
                set category 2 6
                set action block
            next
        end
    next
end
config dnsfilter profile
    edit "Company-DNS"
        set comment "Masterclass: block gambling at DNS level"
        set block-botnet enable
        config ftgd-dns
            config filters
                edit 100
```

```
                    set category 11
                    set action block
                next
            end
        end
    next
end
config ips custom
    edit "PML.Test.Signature"
        set signature "F-SBID( --name \"PML.Test.Signature\"; --protocol tcp; --service HTTP;
            --flow from_client; --pattern \"pingmylab-ips-test\"; --context uri; --no_case; )"
        set comment "Masterclass IPS test"
    next
end
config ips sensor
    edit "Company-IPS"
        set comment "Masterclass: default protection plus a test signature"
        config entries
            edit 1
                set rule 2354
                set status enable
                set action block
                set log-packet enable
            next
            edit 2
                set severity medium high critical
            next
        end
    next
end
config firewall policy
    edit 3
        set name "HQ-to-Azure-LAN"
        set srcintf "TO-HQ"
        set dstintf "port2"
        set srcaddr "all"
        set dstaddr "PROTECTED-A"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
    edit 4
        set name "Azure-LAN-to-HQ"
        set srcintf "port2"
        set dstintf "TO-HQ"
        set srcaddr "PROTECTED-A"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set logtraffic all
    next
    edit 5
        set name "Company-internet"
        set srcintf "TO-HQ"
        set dstintf "port1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set ssl-ssh-profile "certificate-inspection"
        set av-profile "default"
        set webfilter-profile "Company-WF"
        set dnsfilter-profile "Company-DNS"
        set ips-sensor "Company-IPS"
        set application-list "Company-APP"
        set logtraffic all
        set nat enable
    next
end
```