

# FCA - FortiGate Operator Self-Paced

## LAB – Note (Part-1)

Configuring Interface and Routing

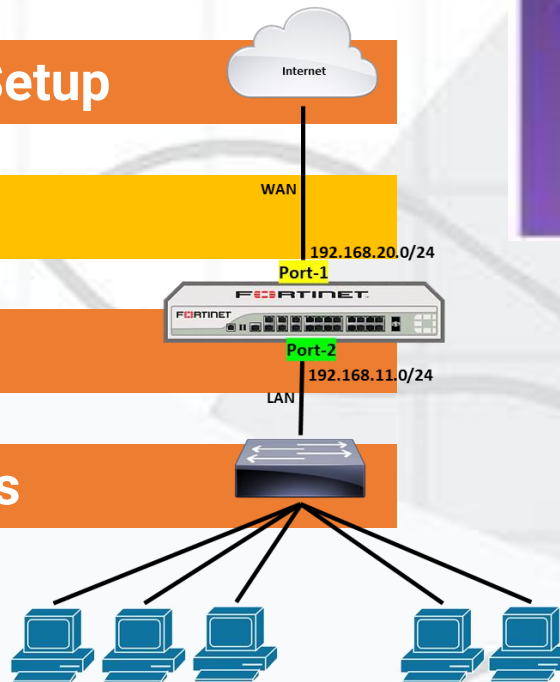
Configuring Firewall Policies

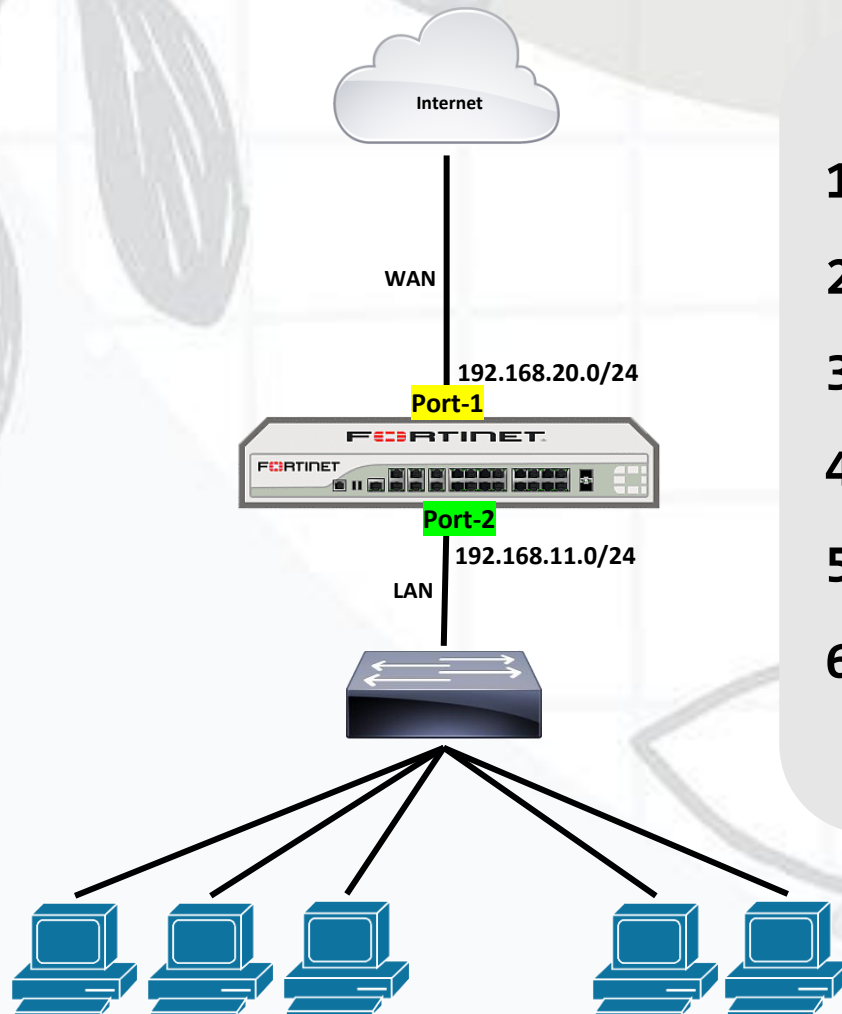
Authenticated Network User Setup

Blocking Malware

Web Filtering

Controlling Application Access





1. Configuring WAN Interface
2. Configuring LAN Interface
3. Configuring DHCP Server
4. Configuring DNS
5. Configuring the default Route
6. Monitoring

Reference

**FORTINET**  
CERTIFIED  
ASSOCIATE  
Cybersecurity

## Configuration LAN Interface and WAN Interface with CLI

### »» WAN Interface Configuration

```
config system interface
  edit port1
  set ip 192.168.20.7 255.255.255.0
  set mode static
  set alias "WAN"
  set role wan
end
```

### »» LAN Interface Configuration

```
config system interface
  edit port2
  set ip 192.168.11.1 255.255.255.0
  set allowaccess ping https ssh http telnet
  set mode static
  set alias "LAN"
  set role lan
end
```

# WAN Interface Configuration (GUI)

- ① Network → Interfaces
- ② Select Port1
- ③ Alias = WAN
- ④ Role = WAN
- ⑤ Address mode = Manual → IP Address = 192.168.20.7/255.255.255.0  
OK

FortiGate-VM64

Dashboard

Network

Interfaces ①

DNS

Packet Capture

SD-WAN

Static Routes

Policy Routes

RIP

OSPF

BGP

Routing Objects

Multicast

Policy & Objects

Security Profiles

VPN

User & Authentication

System 1

Security Fabric

Log & Report

Edit Interface

Name port1 ②

Alias WAN ③

Type Physical Interface

VRF ID 0

Role WAN ④

Estimated bandwidth 0 kbps Upstream

0 kbps Downstream

Address ⑤

Addressing mode Manual DHCP Auto-managed by FortiIPAM

IP/Netmask 192.168.20.7/255.255.255.0

Secondary IP address

Administrative Access

IPv4

☒ HTTPS ☒ HTTP ☒ PING

☐ FMG-Access ☒ SSH ☐ SNMP

☐ FTM ☐ RADIUS Accounting ☐ Security Fabric Connection

Receive LLDP Use VDOM Setting Enable Disable

Transmit LLDP Use VDOM Setting Enable Disable

FortiGate

FortiGate-VM64

Active Administrator Sessions

1 HTTP

Status

Up

MAC address

00:0c:29:e6:0b:f5

Speed Test

Execute speed test

Additional Information

API Preview

References

Edit in CLI

Documentation

Online Help

Video Tutorials

OK Cancel

# WAN Interface Status

- ① Network → Interfaces
- ② Check > WAN (Port1)

FortiGate-VM64

Dashboard

Network

Interfaces

DNS

Packet Capture

SD-WAN

Static Routes

Policy Routes

RIP

OSPF

BGP

Routing Objects

Multicast

Policy & Objects

Security Profiles

VPN

User & Authentication

System

Security Fabric

Log & Report

FortiGate VM64

1 3 5 7 9 11 13 15 17 19 21 23

2 4 6 8 10 12 14 16 18 20 22 24

Create New

Edit

Delete

Integrate Interface

Search

Group By Type

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
				HTTP TELNET			
port3	Physical Interface		0.0.0.0/0.0.0.0				0
port4	Physical Interface		0.0.0.0/0.0.0.0				0
port5	Physical Interface		0.0.0.0/0.0.0.0				0
port6	Physical Interface		0.0.0.0/0.0.0.0				0
port7	Physical Interface		0.0.0.0/0.0.0.0				0
port8	Physical Interface		0.0.0.0/0.0.0.0				0
port9	Physical Interface		0.0.0.0/0.0.0.0				0
port10	Physical Interface		0.0.0.0/0.0.0.0				0
WAN (port1)	Physical Interface		192.168.20.7/255.255.255.0	PING HTTPS SSH HTTP			1

0 Security Rating Issues

100% 11 Updated: 21:46:00

# LAN Interface Configuration (GUI)

- ① Network → Interfaces
- ② Select Port2
- ③ Alias = LAN
- ④ Role = LAN
- ⑤ Address mode = Manual → IP Address = 192.168.11.1/255.255.255.0
- ⑥ Administrative Access = Checked > HTTPS , HTTP , PING , SSH , TELNET
- ⑦ OK

The screenshot displays the 'Edit Interface' configuration page in the FortiGate GUI. The left sidebar shows the navigation menu with 'Network' and 'Interfaces' highlighted. The main configuration area is divided into several sections:

- Name:** LAN (port2)
- Alias:** LAN
- Type:** Physical Interface
- VRF ID:** 0
- Role:** LAN
- Address:**
  - Addressing mode:** Manual (selected), DHCP, Auto-managed by FortiIPAM
  - IP/Netmask:** 192.168.11.1/255.255.255.0
  - Create address object matching subnet:** ☐
  - Secondary IP address:** ☐
- Administrative Access:**
  - IPv4:**
    - ☒ HTTPS, ☒ HTTP, ☒ PING
    - ☐ FMG-Access, ☒ SSH, ☐ SNMP
    - ☒ TELNET, ☐ FTM, ☐ RADIUS Accounting
    - ☐ Security Fabric Connection
  - Receive LLDP:** Use VDOM Setting, Enable, Disable
  - Transmit LLDP:** Use VDOM Setting, Enable, Disable

On the right side, the 'FortiGate' status is shown as 'Up', and the MAC address is '00:0c:29:e6:0b:ff'. There are links for 'API Preview', 'References', 'Edit in CLI', 'Documentation', 'Online Help', and 'Video Tutorials'.

At the bottom, the 'OK' button is highlighted, and the 'Cancel' button is also visible.

# DHCP Server on LAN Configuration

- ① Network → Interfaces → Select and Edit Port (LAN Port)
- ② DHCP Server = [ Enabled ]
- ③ Address Range = 192.168.11.2-192.168.11.100
- ④ Netmask = 255.255.255.0
- ⑤ Default Gateway = [ Same as Interface IP ]
- ⑥ OK

The screenshot shows the FortiGate VM64 web interface. On the left, the 'Network' menu is expanded, and 'Interfaces' is selected, marked with a red circle ①. The main panel is titled 'Edit Interface'. Under the 'DHCP Server' section, the 'DHCP status' is set to 'Enabled' (marked with a red circle ②). The 'Address range' is set to '192.168.11.2-192.168.11.100' (marked with a red circle ③). The 'Netmask' is set to '255.255.255.0' (marked with a red circle ④). The 'Default gateway' is set to 'Same as Interface IP' (marked with a red circle ⑤). The 'Lease time' is set to '604800' seconds. Below this, the 'Advanced' section is expanded, showing 'Network' settings: 'Device detection' is enabled, 'Security mode' is disabled, 'Traffic Shaping' is disabled, and 'Outbound shaping profile' is set to 'None'. At the bottom, the 'OK' button is highlighted with a red circle ⑥. The right sidebar shows the device status as 'Up' and provides links for API Preview, References, Edit in CLI, Documentation, Online Help, and Video Tutorials. The Fortinet logo and version 'v7.0.0' are visible in the bottom left corner.

# DNS Setting Configuration

- ① Network → DNS
- ② DNS Server = [ Specify ]
- ③ Primary DNS Server = 8.8.8.8 , Secondary DNS Server = 8.8.4.4
- ④ DNS (UDP/53) = Enable
- ⑤ Apply

The screenshot shows the FortiGate web interface for DNS Settings. The left sidebar has a menu with 'DNS' highlighted and marked with a red circle ①. The main content area is titled 'DNS Settings' and contains two sections: 'DNS servers' and 'DNS Protocols'. In the 'DNS servers' section, the 'Use FortiGuard Servers' dropdown is set to 'Specify' (marked with a red circle ②), the 'Primary DNS server' is '8.8.8.8' (marked with a red circle ③), and the 'Secondary DNS server' is '8.8.4.4'. The 'DNS Protocols' section has 'DNS (UDP/53)' enabled (marked with a red circle ④), while 'TLS (TCP/853)' and 'HTTPS (TCP/443)' are disabled. At the bottom right, there is a green 'Apply' button marked with a red circle ⑤. On the right side of the interface, there is a 'DNS Servers' table and a list of links for additional information and documentation.

DNS Servers	
208.91.112.53	220 ms
208.91.112.52	3,310 ms

Additional Information

- API Preview
- Edit in CLI

Setup guides

- DNS Local Domain List
- Using FortiGate as a DNS Server
- FortiGuard DDNS

Documentation

- Online Help
- Video Tutorials



# Default Route Configuration

- ① Network → Static Routes
- ② Destination = [ Subnet ]
- ③ 0.0.0.0/0.0.0.0
- ④ 192.168.20.1
- ⑤ Interface = WAN (port1)
- ⑥ OK

FortiGate-VM64

Dashboard

Network

- Interfaces
- DNS
- Packet Capture
- SD-WAN
- Static Routes ①**
- Policy Routes
- RIP
- OSPF
- BGP
- Routing Objects
- Multicast

Policy & Objects

Security Profiles

VPN

User & Authentication

### Edit Static Route

Destination ⓘ **②** Subnet Internet Service

0.0.0.0/0.0.0.0 **③**

Gateway Address 192.168.20.1 **④**

Interface WAN (port1) **⑤**

Administrative Distance ⓘ 10

Comments Write a comment... 0/255

Status **⑥** Enabled Disabled

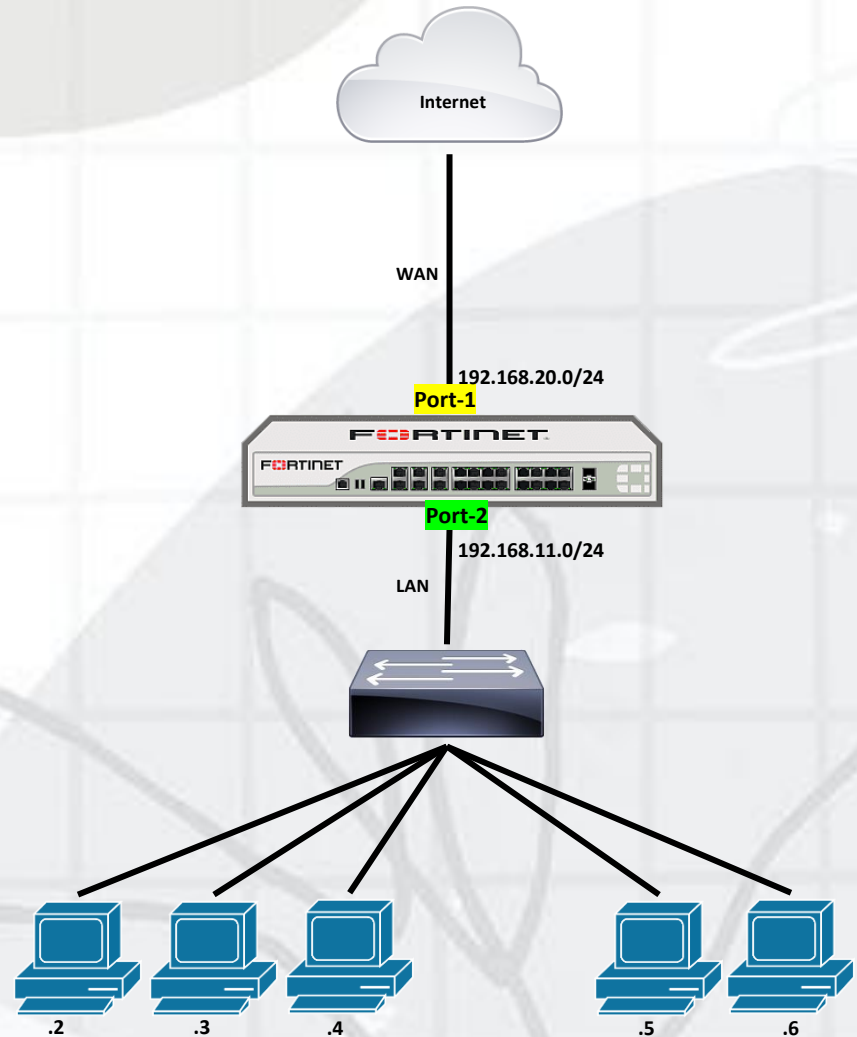
Advanced Options

Priority ⓘ 0

OK Cancel

# Configuration Firewall Policies

1. Create LAN Network Object
2. Configure Firewall policies for Internet Access
3. Monitoring Traffic Log



Reference

# Creating LAN Network Object

- ① Policy & Objects
- ② Address
- ③ Name = [ LAN-Network ]
- ④ IP/Netmask = 192.168.11.0 255.255.255.0
- ⑤ Choose → LAN (Port2)
- ⑥ OK

FortiGate-VM64

Dashboard

Network

**Policy & Objects** ①

Firewall Policy

IPv4 DoS Policy

**Addresses** ② ☆

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles

VPN

User & Authentication

System ①

Edit Address

Name LAN-Network ③

Color Change

Type Subnet

IP/Netmask 192.168.11.0 255.255.255.0 ④

Interface LAN (port2) ⑤

Static route configuration ☐

Comments LAN Network 11/255

⑥ OK Cancel

# Creating Firewall Policy for Internet Access

- ① Policy & Objects → Firewall Policy
- ② Name = [ Internet-Access ]
- ③ Incoming Port = LAN (Port2)
- ④ Outgoing Port = WAN (Port1)
- ⑤ Source = LAN-Network (LAN Network Object)
- ⑥ Destination = All

- ⑦ Schedule = always
- ⑧ Service = DNS , HTTP , HTTPS
- ⑨ Action = Accept
- ⑩ Inspection Mode = Flow-based
- ⑪ NAT = [Enable]
- ⑫ IP Pool = Use Outgoing Interface
- ⑬ OK

The screenshot shows the FortiGate VM64 configuration interface. The left sidebar has 'Policy & Objects' expanded, with 'Firewall Policy' selected and marked with a red circle ①. The main area shows the 'New Policy' configuration for 'Internet-Access'. The configuration is as follows:

- Name: Internet-Access (②)
- Incoming Interface: LAN (port2) (③)
- Outgoing Interface: WAN (port1) (④)
- Source: LAN-Network (⑤)
- Destination: all (⑥)
- Schedule: always (⑦)
- Service: DNS, HTTP, HTTPS (⑧)
- Action: ACCEPT (checked), DENY (unchecked) (⑨)
- Inspection Mode: Flow-based (selected), Proxy-based (⑩)
- NAT: Enabled (checked) (⑪)
- IP Pool Configuration: Use Outgoing Interface Address (selected), Use Dynamic IP Pool (⑫)
- Protocol Options: default (⑬)

A pop-up window titled 'Logging Options' is shown on the right, with a blue arrow pointing to the 'All Sessions' tab. The options are:

- Log Allowed Traffic: Enabled (checked)
- Generate Logs when Session Starts: Disabled (unchecked)
- Capture Packets: Disabled (unchecked)
- Comments: Write a comment... (0/1023)
- Enable this policy: Enabled (checked)

# Viewing Traffic Log

- ① Log & Report
- ② Forward Traffic

Check Traffic Log

FortiGate-VM64

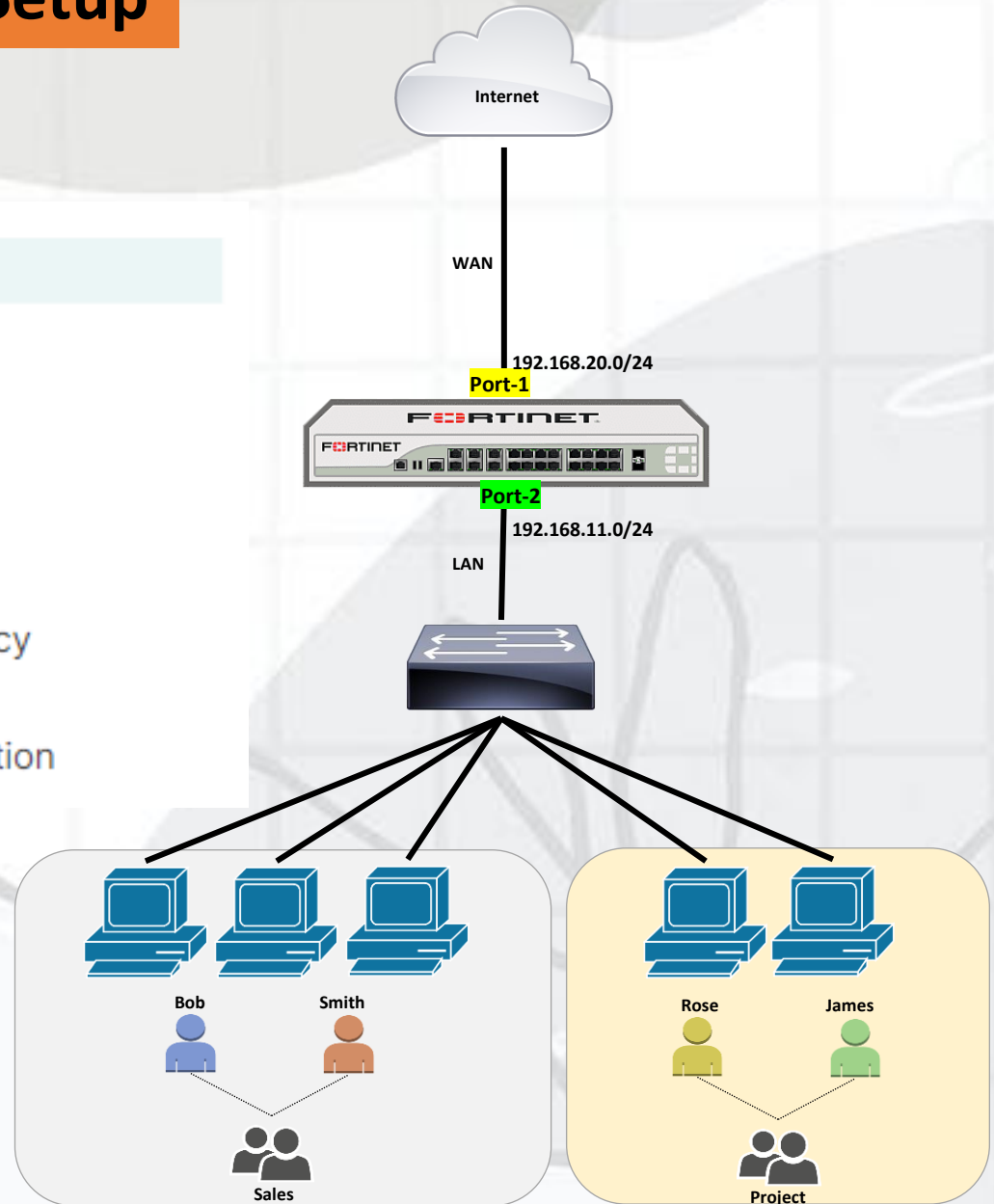
Dashboard  
Network  
Policy & Objects  
Security Profiles  
VPN  
User & Authentication  
System  
Security Fabric  
**Log & Report**  
Forward Traffic  
Local Traffic  
Sniffer Traffic  
Events  
AntiVirus  
Web Filter  
SSL  
DNS Query  
File Filter  
Application Control  
Intrusion Prevention

3 seconds ago 192.168.11.2 00:0c:29:d3:b0:66 152.195.38.76 (fp2e7a.wpc.phicdn.... Internet-Access (1)  
3 seconds ago 192.168.11.2 00:0c:29:d3:b0:66 96.16.102.29 (storeedgefd.dsx.mp.... Internet-Access (1)  
9 seconds ago 192.168.11.2 00:0c:29:d3:b0:66 20.24.121.134 (arc.msn.com) Internet-Access (1)  
10 seconds ago 192.168.11.2 00:0c:29:d3:b0:66 20.24.121.134 (arc.msn.com) Internet-Access (1)  
10 seconds ago 192.168.11.2 00:0c:29:d3:b0:66 20.205.104.58 (ris.api.iris.microsoft.... Internet-Access (1)  
10 seconds ago 192.168.11.2 00:0c:29:d3:b0:66 152.195.38.76 (fp2e7a.wpc.phicdn.... Internet-Access (1)  
14 seconds ago 192.168.11.2 00:0c:29:d3:b0:66 204.79.197.203 (api.msn.com) Internet-Access (1)  
21 seconds ago 192.168.11.2 00:0c:29:d3:b0:66 34.120.158.37 (tracking-protection.... Internet-Access (1)  
23 seconds ago 192.168.11.2 00:0c:29:d3:b0:66 34.120.158.37 (tracking-protection.... 6.57 kB / 333.78 kB Internet-Access (1)  
24 seconds ago 192.168.11.2 00:0c:29:d3:b0:66 20.42.73.28 (v10.events.data.micro... Internet-Access (1)  
24 seconds ago 192.168.11.2 00:0c:29:d3:b0:66 74.125.68.94 (pki-goog.l.google.com) 172 B / 92 B Internet-Access (1)  
24 seconds ago 192.168.11.2 00:0c:29:d3:b0:66 74.125.68.94 (pki-goog.l.google.com) 172 B / 92 B Internet-Access (1)  
24 seconds ago 192.168.11.2 00:0c:29:d3:b0:66 152.195.38.76 (fp2e7a.wpc.phicdn.... 328 B / 92 B Internet-Access (1)  
24 seconds ago 192.168.11.2 00:0c:29:d3:b0:66 34.120.158.37 (tracking-protection.... 12.14 kB / 1.52 MB Internet-Access (1)  
24 seconds ago 192.168.11.2 00:0c:29:d3:b0:66 34.120.158.37 (tracking-protection.... 2.36 kB / 10.43 kB Internet-Access (1)  
24 seconds ago 192.168.11.2 00:0c:29:d3:b0:66 34.120.158.37 (tracking-protection.... 2.37 kB / 5.65 kB Internet-Access (1)

0% 69

# Authenticated Network User Setup

- Task 1. Create a user account
- Task 2. Configure remote authentication
- Task 3. Create a user group
- Task 4. Add authentication to the firewall policy
- Task 5. Verify and monitor firewall authentication



Reference



# Create a Local User Account

- ① User & Authentication → User Definition → Create New
- ② User Type = Local User → Next
- ③ Login Credentials = set (Username , Password) → Next
- ④ Extra Info → User Account Status = [ Enable ] → Submit

The screenshot displays the FortiGate VM64 web interface for the 'Users/Groups Creation Wizard'. The left sidebar shows the navigation menu with 'User & Authentication' expanded and 'User Definition' selected (marked with a red ①). The main content area shows the wizard steps: ① User Type, ② Login Credentials, ③ Contact Info, and ④ Extra Info. Under 'User Type', 'Local User' is selected (marked with a red ②). The 'Login Credentials' step shows the 'Username' field with 'user' and the 'Password' field with masked characters (marked with a red ③). Below this, the 'Two-factor Authentication' option is unchecked. At the bottom, the 'User Account Status' is set to 'Enabled' (marked with a red ④) and the 'User Group' is set to 'None'.

FortiGate-VM64

Dashboard

Network

Policy & Objects

Security Profiles

VPN

User & Authentication

User Definition ①

User Groups

Guest Management

LDAP Servers

RADIUS Servers

Authentication Settings

FortiTokens

System 1

Security Fabric

Log & Report

Users/Groups Creation Wizard

① User Type > ② Login Credentials > ③ Contact Info > ④ Extra Info

Local User ②

Remote RADIUS User

Remote TACACS+ User

Remote LDAP User

FSSO

FortiNAC User

Username user ③

Password

① User Type > ② Login Credentials > ③ Contact Info > ④ Extra Info

Two-factor Authentication

① User Type > ② Login Credentials > ③ Contact Info > ④ Extra Info

User Account Status Enabled ④ Disabled

User Group

# User Account Status

- ① User & Authentication ➔ User Definition
- ② Check User List

FortiGate-VM64

Dashboard

Network

Policy & Objects

Security Profiles

VPN

User & Authentication

User Definition

Create New

Edit

Clone

Delete

Search

Name	Type	Two-factor Authentication	Groups	Status	Ref.
guest	LOCAL	✖	Guest-group	✓ Enabled	1
user	LOCAL	✖		✓ Enabled	0

>\_

?

🔔 2

admin



# Create a User Group

- ① User & Authentication → User Groups → Create New
- ② Name = Sales [ Group Name ]
- ③ Type = Firewall
- ④ Members = user
- ⑤ OK

The screenshot displays the FortiGate VM64 web interface. The left sidebar shows the navigation menu with 'User & Authentication' expanded and 'User Groups' selected (marked with a red circle 1). The main area is titled 'New User Group'. The 'Name' field contains 'Sales' (marked with a red circle 2). The 'Type' dropdown menu is open, showing 'Firewall' selected (marked with a red circle 3). The 'Members' section shows a list with 'user' (marked with a red circle 4). A 'Select Entries' dialog box is open, showing a list of users with 'user' selected. A blue arrow points from the 'user' entry in the dialog to the 'user' entry in the main list. At the bottom, the 'OK' button is highlighted with a red circle 5.

FortiGate-VM64

Dashboard

Network

Policy & Objects

Security Profiles

VPN

User & Authentication

User Definition

User Groups ①

Guest Management

LDAP Servers

RADIUS Servers

Authentication Settings

FortiTokens

System ①

Security Fabric

Log & Report

New User Group

Name Sales ②

Type Firewall ③

Fortinet Single Sign-On (FSSO)

RADIUS Single Sign-On (RSSO)

Guest

Members user ④

Select Entries

Search

+ Create

USER (2)

Local (2)

guest

user

Close

OK ⑤

Cancel

FortiGate

FortiGate-VM64

Additional Information

API Preview

Documentation

Online Help

Video Tutorials

## User Group Status

- ① User & Authentication → User Groups
- ② Check Group List

FortiGate-VM64

Dashboard

Network

Policy & Objects

Security Profiles

VPN

**User & Authentication**

User Definition

**User Groups**

+ Create New Edit Clone Delete Search

Group Name	Group Type	Members	Ref.
Guest-group	Firewall	guest	0
SSO_Guest_Users	Fortinet Single Sign-On (FSSO)		1
Sales	Firewall	user	0

# Add Authentication to the firewall policy

- ① Policy & Object ➔ Firewall Policy ➔ Edit ( Internet Access Rule)
- ② Source = Sales (Add Group)
- ③ OK

The screenshot displays the FortiGate VM64 web interface. The left sidebar shows the navigation menu with 'Policy & Objects' highlighted (marked with a red circle 1). The main area shows the 'Edit Policy' configuration for 'Internet-Access'. The 'Source' field is set to 'LAN-Network' and 'Sales' (marked with a red circle 2). The 'Destination' is set to 'all'. The 'Service' is set to 'DNS', 'HTTP', and 'HTTPS'. The 'Action' is set to 'ACCEPT'. The 'Inspection Mode' is set to 'Flow-based'. The 'Firewall / Network Options' section shows 'NAT' is enabled and 'IP Pool Configuration' is set to 'Use Outgoing Interface Address'. A 'Select Entries' dialog is open, showing the 'User' tab with 'Sales' selected (marked with a red circle 3). The 'OK' button is visible at the bottom.

FortiGate-VM64

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles

VPN

User & Authentication

System

Security Fabric

Log & Report

Edit Policy

Name: Internet-Access

Incoming Interface: LAN (port2)

Outgoing Interface: WAN (port1)

Source: LAN-Network, Sales

Destination: all

Schedule: always

Service: DNS, HTTP, HTTPS

Action: ACCEPT, DENY

Inspection Mode: Flow-based, Proxy-based

Firewall / Network Options

NAT: ON

IP Pool Configuration: Use Outgoing Interface Address, Use Dynamic IP Pool

Select Entries

Address, User, Internet Service

Search

Create

USER (2)

Local (2)

guest

user

USER GROUP (3)

Guest-group

Sales

SSO\_Guest\_Users

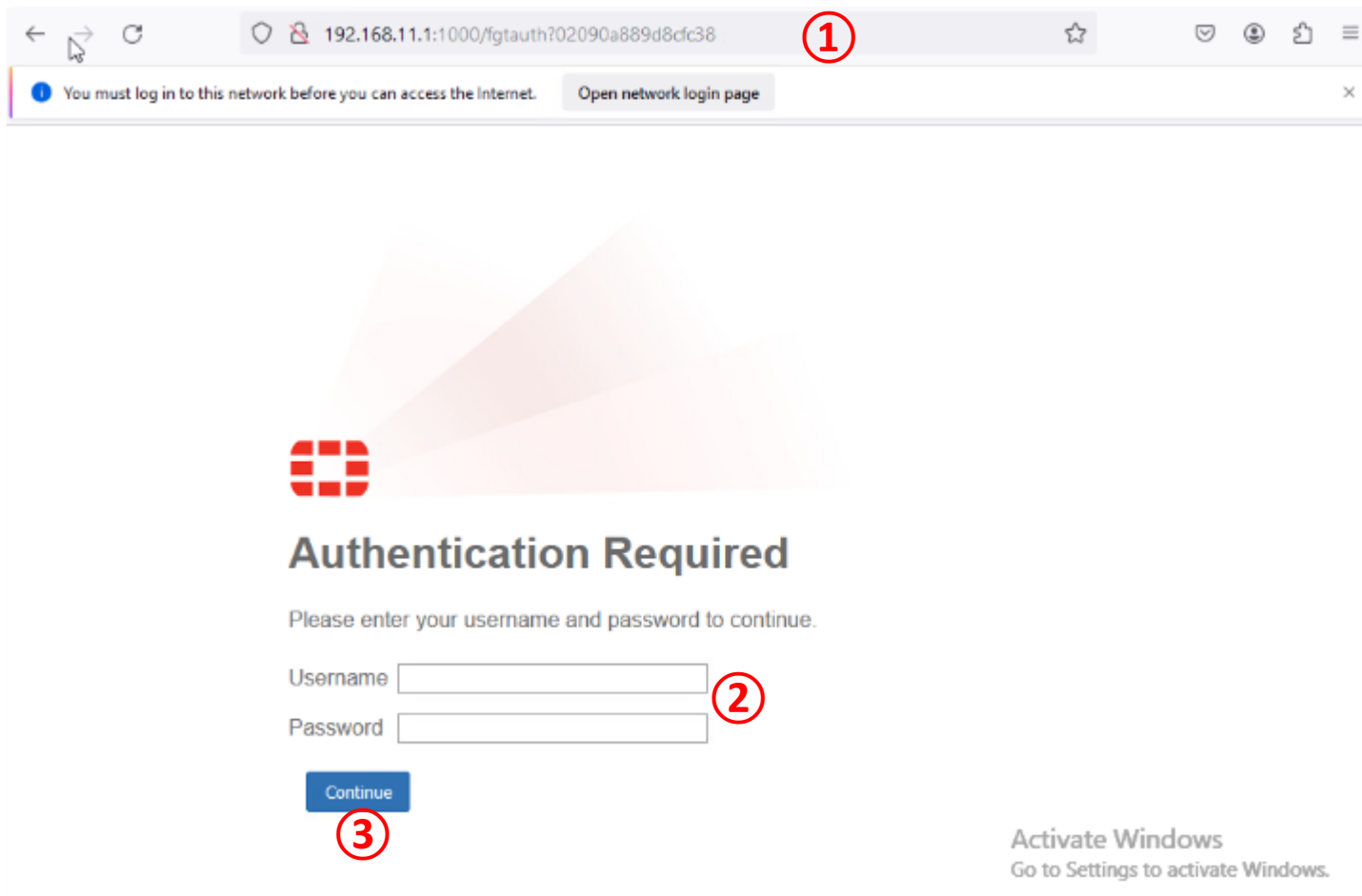
Close

OK

Cancel


# Testing Internet Access with an allowed User Account

- ① Access the Internet ([www.google.com](http://www.google.com))
- ② Login (Username and Password of User in Sales Group)
- ③ Continue



192.168.11.1:1000/fgtauth?02090a889d8dfc38

You must log in to this network before you can access the Internet. Open network login page



## Authentication Required

Please enter your username and password to continue.

Username

Password

Continue

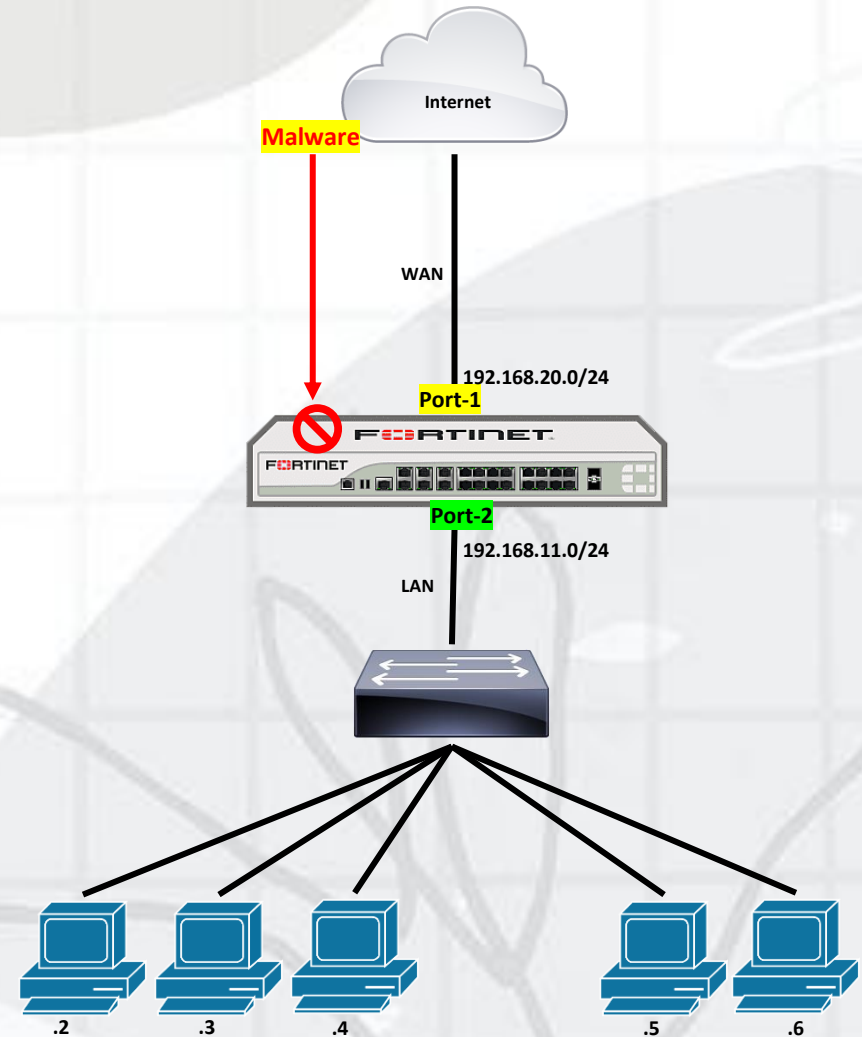
Activate Windows  
Go to Settings to activate Windows.

# Blocking Malware

Task 1 : Create a Antivirus Profile

Task 2 : Apply antivirus to Firewall policy

Task 3 : Verify antivirus



Reference

## Create a Antivirus Profile

- ① Security Profiles
- ② Antivirus
- ③ Default
- ④ Edit

The screenshot displays the FortiGate web interface for configuring Antivirus profiles. The left sidebar contains the navigation menu, where 'Security Profiles' is marked with a red circle ① and 'AntiVirus' is marked with a red circle ②. The main content area shows a table of antivirus profiles. The 'default' profile is highlighted with a red circle ③. A yellow circle ④ highlights the 'Edit' button in the top toolbar. A purple callout bubble points to the 'default' profile with the text 'Click default.'

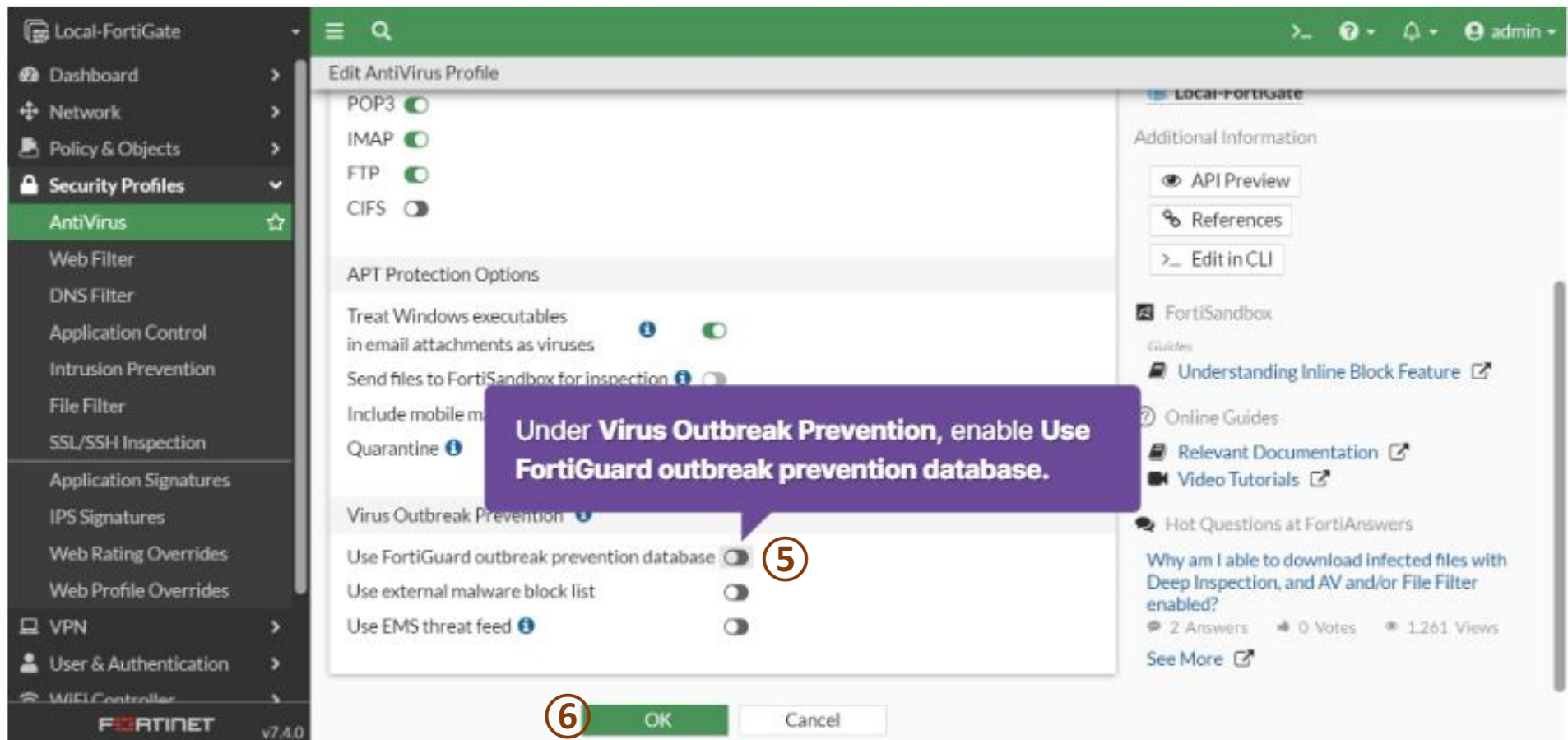
Name	Comments	Ref.
AV default	Scan files and block viruses.	0
AV wifi-default	Default configuration for offloading WiFi traffic.	1

FortiGate v7.4.0

## Create a Antivirus Profile - Continue

⑤ Use FortiGuard outbreak prevention database = [ Enable ]

⑥ OK



# Apply antivirus to Firewall policy

- ① Policy & Objects
- ② Firewall Policy
- ③ Select → Internet Access Rule
- ④ Edit

Local-FortiGate

Dashboard > Network > Policy & Objects (1) > Firewall Policy (2)

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles > VPN > User & Authentication > WiFi Controller >

FortiGate v7.4.0

4 Security Rating Issues

Create new Edit Delete Export Interface Pair View By Sequence Classic layout

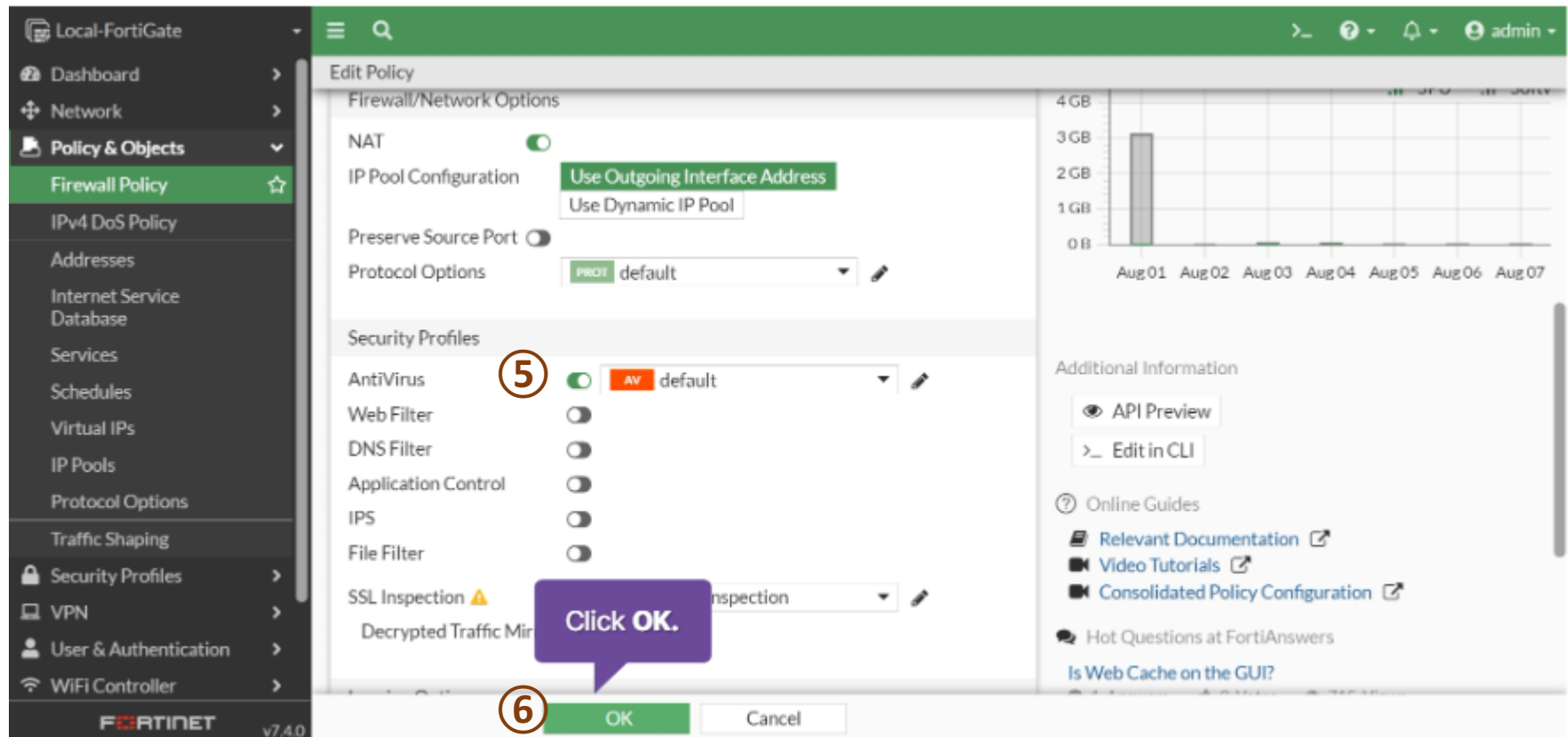
Policy

Name	From	To	Source	Destination	Schedule	Service	Action	IP P
Uncategorized (2)								
Internet Access (3)	port3	port1	Internal Network (4)	all	always	DNS HTTP HTTPS	ACCEPT	
vpn_RemoteVPN_remote_0	RemoteVPN	port3	RemoteVPN_range	Internal Network	always	ALL	ACCEPT	
Implicit (1)								
Implicit Deny	any	any	all	all	always	ALL	DENY	



## Apply antivirus to Firewall policy - Continue

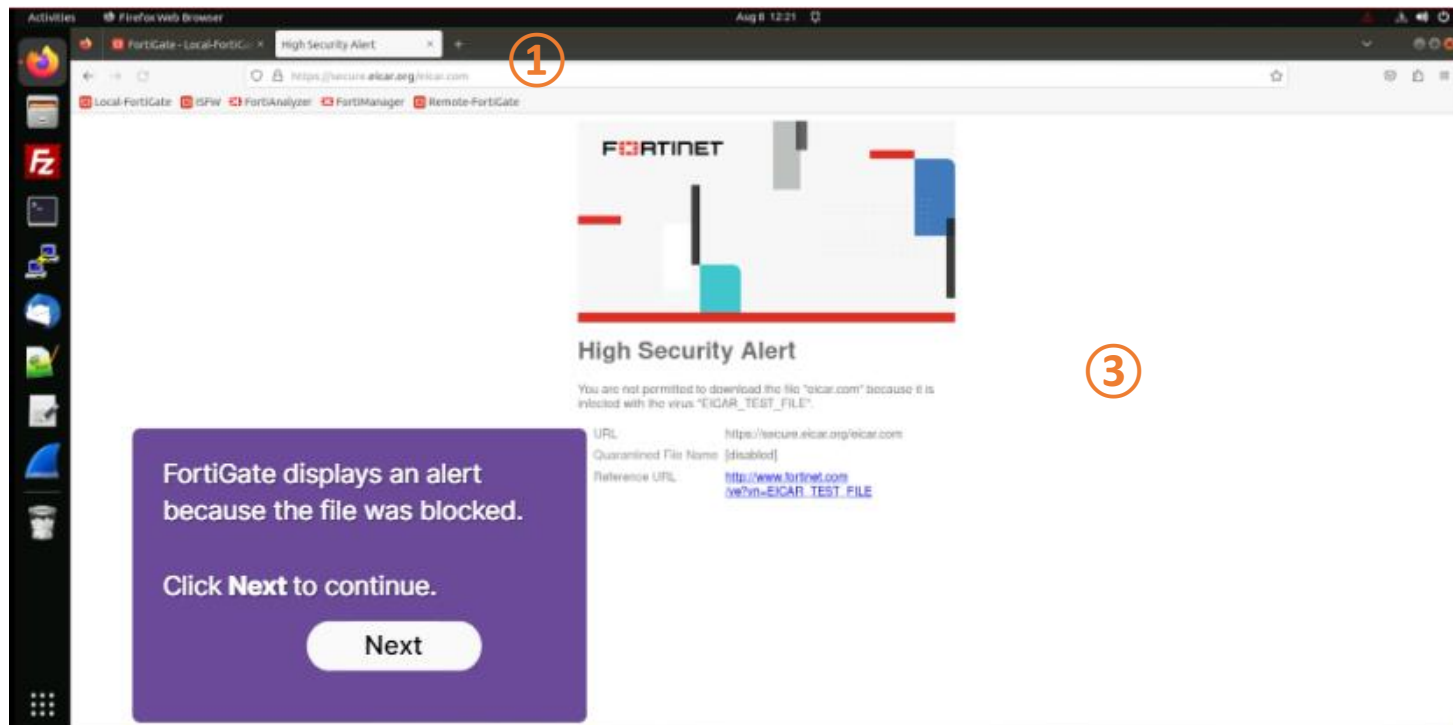
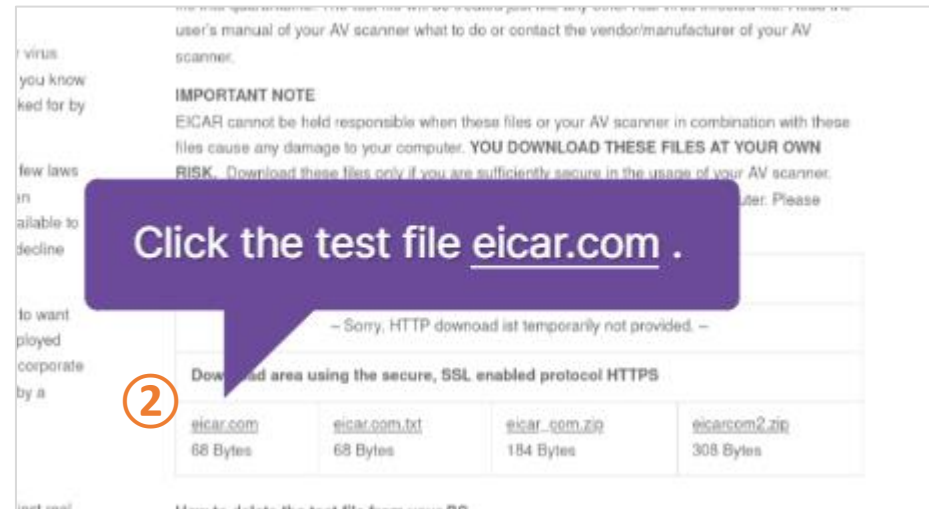
- ⑤ Antivirus = [ Enable ] and Select Profile
- ⑥ OK



# Verify antivirus

- ① Browse → [www.eicar.org/download-anti-malware-testfile/](http://www.eicar.org/download-anti-malware-testfile/)
- ② Click → [eicar.com](http://eicar.com)
- ③ Check Security Alert Message

Type [www.eicar.org/download-anti-malware-testfile/](http://www.eicar.org/download-anti-malware-testfile/)



# Verify antivirus - Continue

- ① Log & Report
- ② Security Events
- ③ Inspect the logs

The screenshot shows the FortiGate Web UI interface. The left sidebar contains a menu with items: Local-FortiGate, Dashboard, Network, Policy & Objects, Security Profiles, VPN, User & Authentication, WiFi Controller, System, Security Fabric, Log & Report (marked with ①), Forward Traffic, Local Traffic, Sniffer Traffic, System Events, Security Events (marked with ②), Reports, and Log Settings. The main content area is titled 'Summary' and 'Logs'. It features a search bar and filters for 'AntiVirus', 'Disk', and '1 hour'. Below this is a table of logs with columns: Date/Time, Service, Source, File Name, Virus/Botnet, User, Details, and Action. Three log entries are visible, all showing 'EICAR TEST FILE' as the virus and 'Blocked' as the action. A callout box (marked with ③) points to the 'Blocked' action in the third row.

Date/Time	Service	Source	File Name	Virus/Botnet	User	Details	Action
2023/08/08 12:21:57	HTTPS	10.0.1.10	eicar.com	EICAR TEST FILE		URL: https://secure.eicar.org/eicar.com	Blocked
2023/08/08 12:17:20	HTTPS	10.0.1.10	eicar.com	EICAR TEST FILE		URL: https://secure.eicar.org/eicar.com	Blocked
2023/08/08 12:17:20	HTTPS	10.0.1.10	eicar.com	EICAR TEST FILE		URL: https://secure.eicar.org/eicar.com	Blocked

Under **AntiVirus**, an **EICAR\_TEST\_FILE** entry appears, with the **Action** shown as **Blocked**.

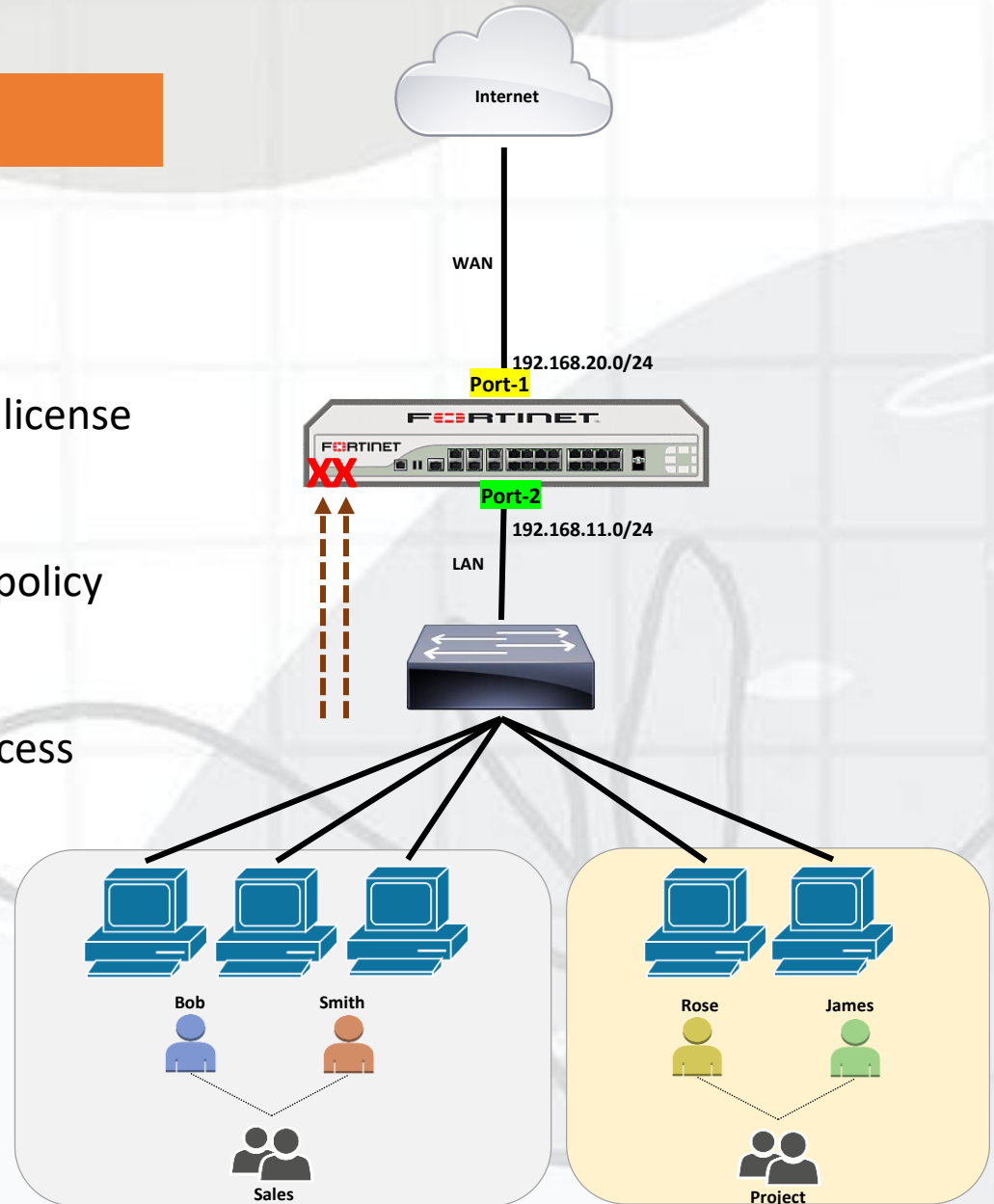
Antivirus inspection is verified.

Click **Next** to continue.

Next

# Web Filtering

1. Validate FortiGuard Security Subscription license
2. Create an Web Filter profile
3. Add the Web Filter profile to the firewall policy
4. Verify the configuration.
5. Monitor the logs regarding application access



# Control Web Access Using Web Filter

Task 1:

Validate FortiGuard security subscription license.



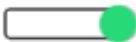
Task 2:

Identify how FortiGuard categorizes the website.



Task 3:

Configure a web filtering security profile.

**WEB** default → 

**FortiGuard Category Based Filter**

Name	Action
+ Local Categories	<input checked="" type="checkbox"/> Allow
+ Potentially Liable	<input type="checkbox"/> Monitor
+ Adult/Mature Content	<input checked="" type="checkbox"/> Block
Bandwidth Consuming	<input type="checkbox"/> Warning
File Sharing and Storage	<input type="checkbox"/> Authenticate
Internet Telephony	

Task 4:

**Security Profiles**

Antivirus ☐

Web Filter ☒

Video Filter ☐

DNS Filter ☐

Application Control ☐

IPS ☐

File Filter ☐

SSL Inspection ☒

**WEB** default

**SSL** certificate-inspection

**Logging Options**

Log allowed traffic ☒ **Security events**

Generate logs when session starts ☐ **All sessions**

Capture packets ☐

Task 5:



**FortiGuard - Access Blocked**

You have tried to access a web page, which is in violation of your Internet usage policy.

Category: Personal Web Sites and Blogs  
URL: http://www.example.com/  
Username: Guest  
Group Name: Guest-group

To have the rating of this web page re-evaluated, please [click here](#)

## Validate FortiGuard Security Subscription license

- ① Dashboard
- ② Status
- ③ Web Filter
- ④ Check Web Filter License

The screenshot displays the FortiGate web interface with the following components:

- Left Sidebar:** Contains navigation links. 'Dashboard' is highlighted with a red circle ①, and 'Status' is highlighted with a red circle ②. Other links include Security, Network, Assets & Identities, WIFI, FortiView Sources, FortiView Destinations, FortiView Applications, FortiView Web Sites, FortiView Policies, FortiView Sessions, Network, Policy & Objects, Security Profiles, and VPN.
- Main Content Area:**
  - System Information:** Displays details for 'Local-FortiGate', including serial number FGVM010000064692, firmware v7.4.0 build2360 (Feature), mode NAT, system time 2023/08/22 15:46:56, uptime 12d 2h 50m 33s, and WAN IP 34.145.253.29.
  - Licenses (10.0.1.241):** A grid of license status tiles. The 'Web Filter' tile is highlighted with a red circle ③. A tooltip for the 'Web Filter' license shows: License: Web Filter, Status: ④ Licensed (with a green checkmark), and Expires on: 2026/01/18.
  - Virtual Machine:** Shows 'FGVM01 License' with 1/1 vCPUs at 100% and 2 GB RAM. Auto scaling is disabled.
  - FortiGate Cloud:** Status is 'Not Activated'.
  - Security Fabric:** Shows 'LAN Edge' with 1 FortiGate, 0 FortiSwitch, 0 FortiAP, and 0 FortiExtender. 'Fabric Connectors' include Logging and FortiSandbox.
  - Administrators:** Lists 'FortiExplorer' (0), 'HTTP' (2), and 'HTTPS' (2) with associated users 'admin' and 'super\_admin'.



# Create or Edit an Web Filter profile

- ① Security Profiles
- ② Web Filter
- ③ Edit [ Web filter Profile (default) ]
- ④ Social Networking (Right-Click)
- ⑤ Choose Block
- ⑥ OK

Name	Comments
default	Default web filtering.
monitor-all	Monitor and log all visited URLs, flow-based.
wifi-default	Default configuration for offloading WIFI traffic.

FortiGate

board

rk

& Objects

ty Profiles

Filter

Filter

ation Control

on Prevention

ter

H Inspection

ation Signatures

natures

ating Overrides

rofile Overrides

Authentication

ontroller

FORTINET v7.4.0

Edit Web Filter Profile

Name

default

Comments

Default web filtering.

22/255

FortiGuard Category Based Filter

Allow

Monitor

Block

Warning

Authenticate

Name	Action
Job Search	Allow
Medicine	Allow
News and Media	Allow
Social Networking	Allow
Political Organizations	Allow
Reference	Allow
Global Religion	Allow
Shopping	Allow
Society and Lifestyles	Allow

OK

Cancel

Additional Information

API Preview

References

Edit in CLI

Online Guides

Relevant Documentation

Video Tutorials

Hot Questions at FortiAnswers

Join the Discussion

- Allow
- Monitor
- Block
- Warning
- Authenticate

# Add the Web Filter profile to the firewall policy

- ① Policy & Object → Firewall Policy
- ② Web Filter [ Enable ]
- ③ Choose Web Filter Profile [Default]
- ④ OK

FortiGate-VM64

Dashboard

Network

Policy & Objects

Firewall Policy ①

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles

VPN

User & Authentication

System

Security Fabric

Edit Policy

Firewall / Network Options

NAT ☒

IP Pool Configuration **Use Outgoing Interface Address**

Preserve Source Port ☐

Protocol Options **PROT** default

Security Profiles

AntiVirus ☐

Web Filter ② ☒ **WEB** default ③

DNS Filter ☐

Application Control ☐

IPS ☐

File Filter ☐

SSL Inspection **SSL** certificate-inspection

Logging Options

Log Allowed Traffic ☒ Security Events **All Sessions**

OK ④ Cancel

Last 7 Days Bytes

2 GB

2 GB

1 GB

500 MB

0 B

Jul 07 Jul 08

Additional Information

API Preview

Edit in CLI

Documentation

Online Help

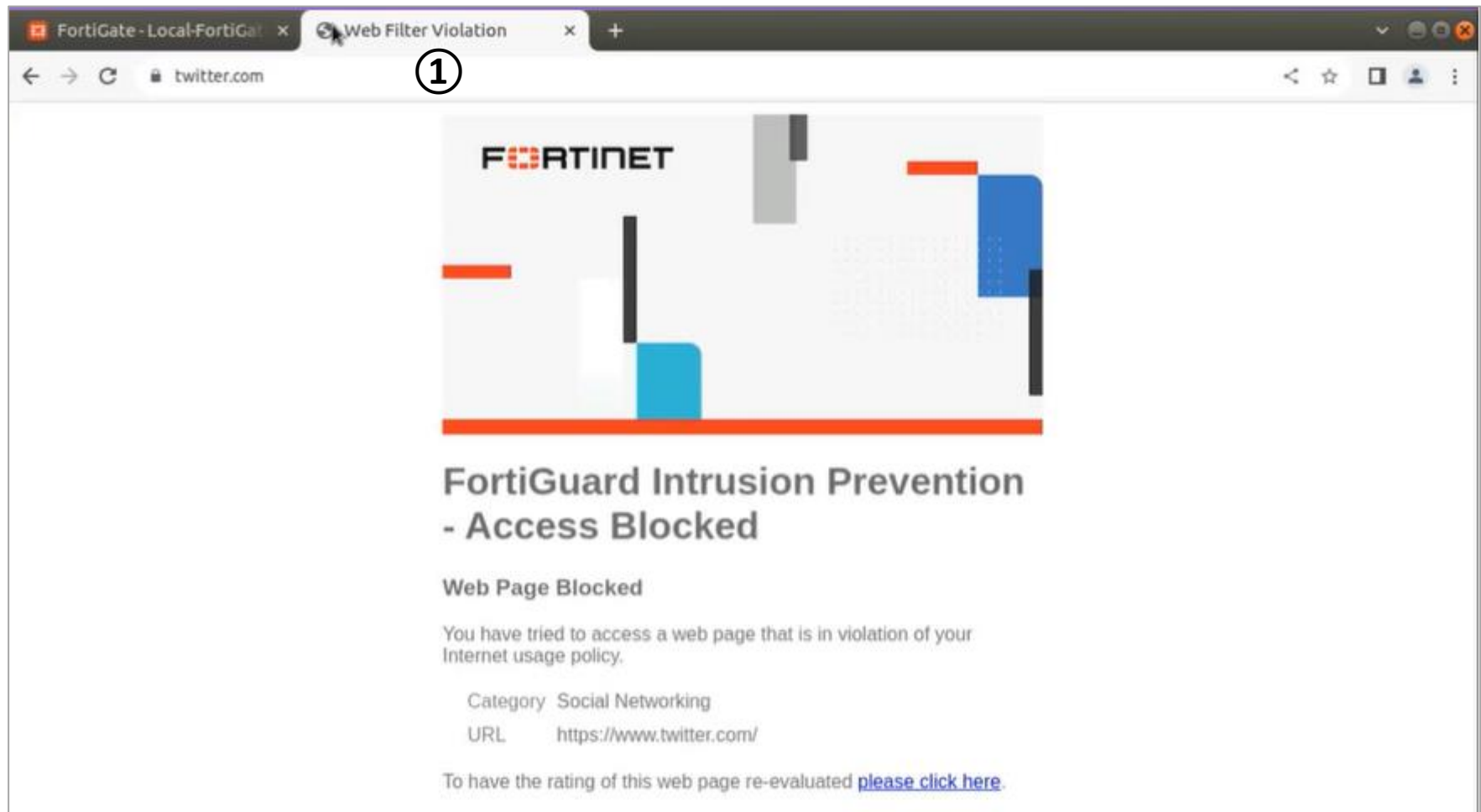
Video Tutorials

Consolidated Policy Configuration



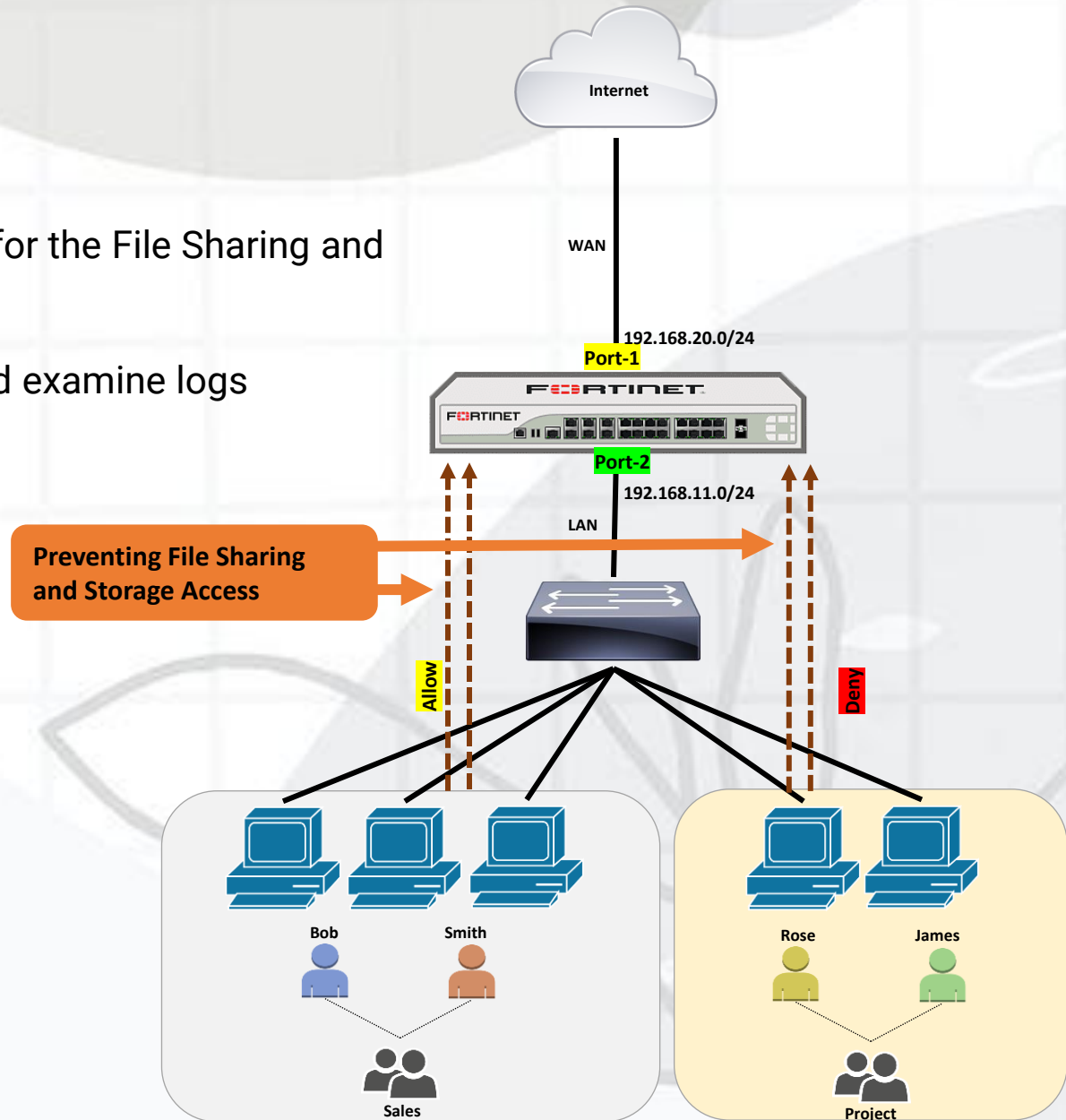
# Verify Web Filter

① Open Browser → [www.twitter.com](https://www.twitter.com)



# Configure the Authenticate Action for FortiGuard Category Filter

- Apply the Authenticated action for the File Sharing and Storage sub-category
- Test the Authenticate action and examine logs



# Apply the Authenticated action for the File Sharing and Storage sub-category

- ① Security Profiles ➔ Web Filter ➔ Edit [ Web filter Profile (default) ]
- ② Select File Sharing and Storage
- ③ Click Authenticate
- ④ Add User and Group
- ⑤ OK
- ⑥ OK

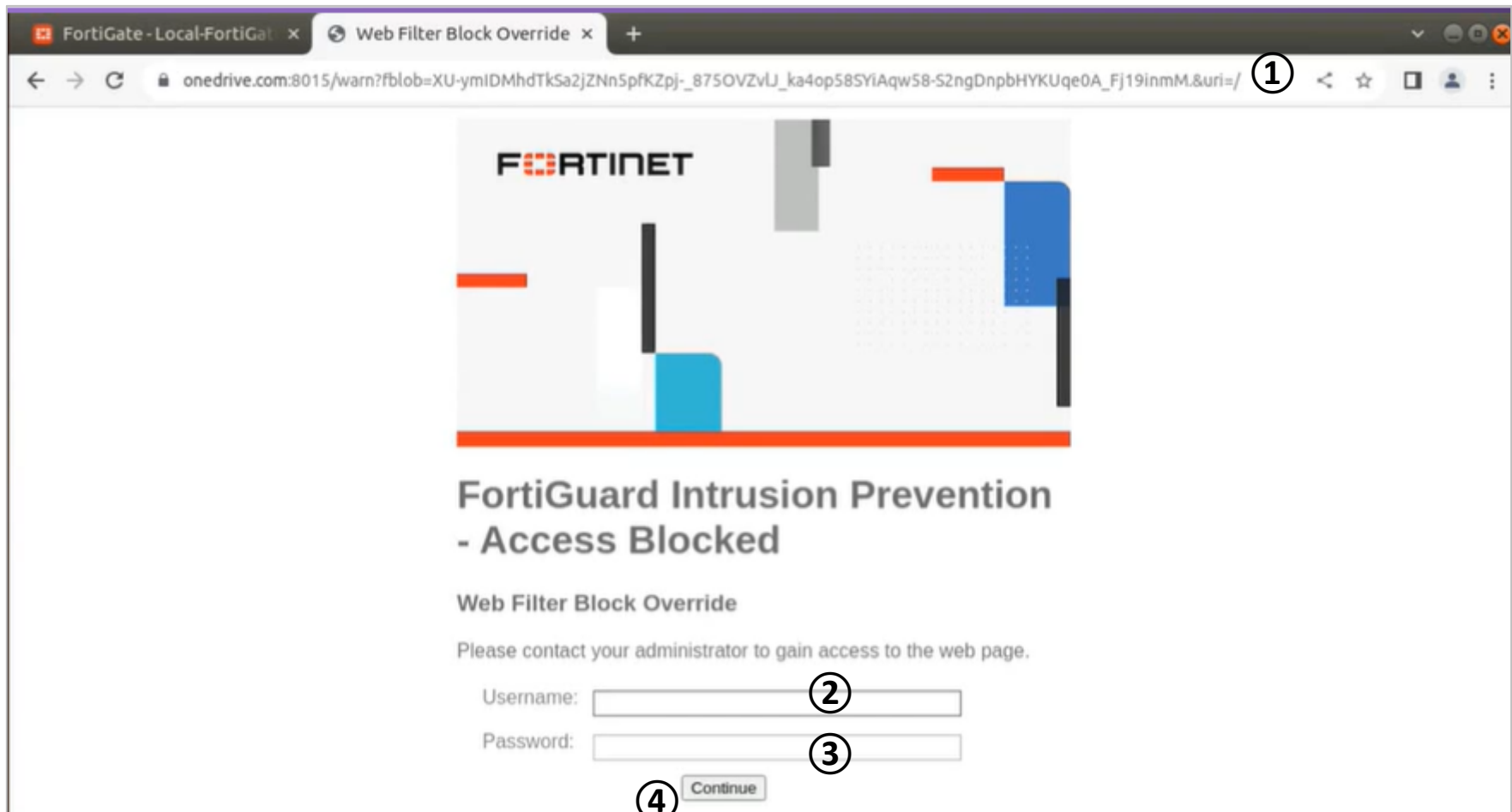
The screenshot shows the FortiGate VM64 interface. The left sidebar contains the navigation menu with the following items: Dashboard, Network, Policy & Objects, Firewall Policy, IPv4 DoS Policy, Addresses, Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, Protocol Options, Traffic Shaping, Security Profiles (marked with ①), VPN, User & Authentication, System (marked with ①), and Security Fabric. The main content area displays the 'Edit Web Filter Profile' window. At the top, there is a warning message: 'Traffic may be blocked if this option is enabled.' Below this, there are five action buttons: Allow, Monitor, Block, Warning, and Authenticate (marked with ③). A table lists various categories and their actions:

Name	Action
terrorism	Block
Adult/Mature Content 15	Allow
Bandwidth Consuming 6	Allow
Freeware and Software Downloads	Allow
File Sharing and Storage ②	Allow
Streaming Media and Download	Allow
Peer-to-peer File Sharing	Allow
Internet Radio and TV	Allow
Internet Telephony	Allow
Security Risk 6	Allow

An 'Edit Filter' dialog box is open, showing the 'Warning Interval' set to 0 hours and 5 minutes. The 'Selected User Groups' list includes 'Sales' (marked with ④). A 'Select Entries' dialog box is also open, showing a list of entries: 'Guest-group', 'Sales' (marked with ④), and 'SSO\_Guest\_Users'. The 'OK' button in the 'Edit Filter' dialog is marked with ⑤. At the bottom of the main window, there is a green 'OK' button (marked with ⑥) and a 'Cancel' button. The bottom status bar shows '22% 90' and 'Activate Windows Go to Settings to activate Windows.'

## Test the Authenticate action and examine logs

- ① Open file sharing and storage website (www.onedrive.com)
- ② Username = User in Sale-Group
- ③ Password = [ Password ]
- ④ Continue



# Monitoring Web Filter

Local-FortiGate

Dashboard

Network

Policy & Objects

Security Profiles

VPN

User & Authentication

WiFi Controller

System

Security Fabric

Log & Report

Forward Traffic

Local Traffic

Sniffer Traffic

System Events

Security Events

Reports

Log Settings

SummaryLogs

Web Filter

Disk

custom

Details

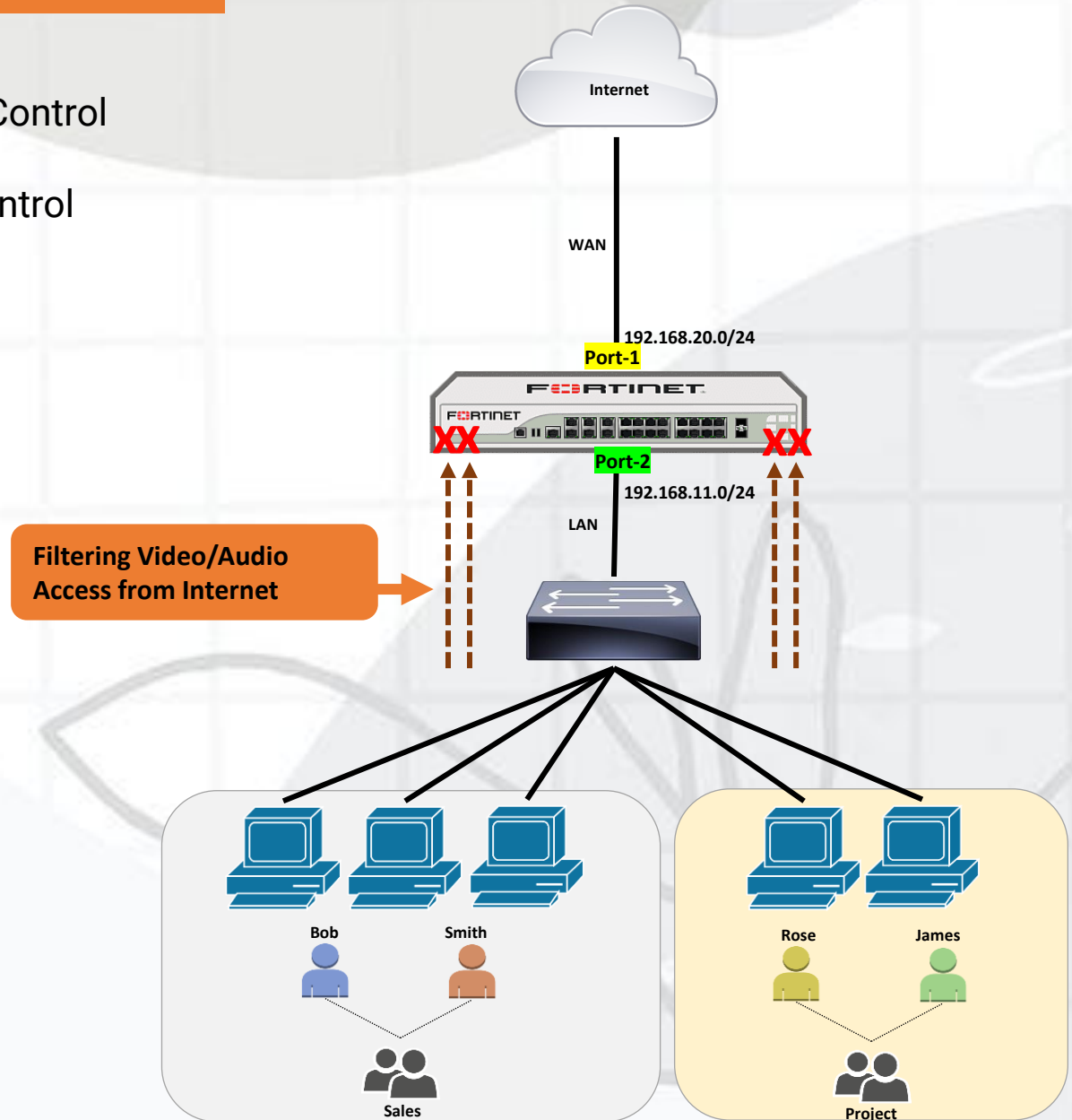
Date/Time 2023-08-22 15:18:56 -> 2023-08-22 16:18:56 x Search

Date/Time	User	Source	Action	URL	Category	Initiator
2023/08/22 16:16:34		10.0.1.10	Blocked	https://www.facebook.com/tr?id=1770...	Social Networking	
2023/08/22 16:16:34		10.0.1.10	Blocked	https://www.facebook.com/tr?id=1770...	Social Networking	
2023/08/22 16:16:26		10.0.1.10	Passthrough	https://onedrive.live.com/	File Sharing and Storage	
2023/08/22 16:15:07		10.0.1.10	Passthrough	https://onedrive.live.com/	File Sharing and Storage	
2023/08/22 16:15:06		10.0.1.10	Passthrough	https://www.onedrive.com/	File Sharing and Storage	
2023/08/22 16:14:27		10.0.1.10	Blocked	https://www.onedrive.com/favicon.ico	File Sharing and Storage	
2023/08/22 16:14:27		10.0.1.10	Blocked	https://www.onedrive.com/favicon.ico	File Sharing and Storage	
2023/08/22 16:14:26		10.0.1.10	Blocked	https://www.onedrive.com/	File Sharing and Storage	
2023/08/22 16:07:32		10.0.1.10	Passthrough	https://www.skype.com/en/	Internet Telephony	
2023/08/22 16:07:32		10.0.1.10	Passthrough	https://www.skype.com/	Internet Telephony	
2023/08/22 16:07:30		10.0.1.10	Blocked	https://www.skype.com/favicon.ico	Internet Telephony	
2023/08/22 16:07:30		10.0.1.10	Blocked	https://www.skype.com/favicon.ico	Internet Telephony	

# Controlling Application Access

**Task 1 :** Configure Application Control

**Task 2 :** Monitor Application Control



Reference

# Create Application Control Profile

- ① Security Profiles
- ② Application Control
- ③ Create New

FortiGate-VM64

Dashboard

Network

Policy & Objects

**Security Profiles**

AntiVirus

Web Filter

Video Filter

DNS Filter

**Application Control**

③

+ Create New

View

Clone

Delete

Search

Name	Comments	Ref.
APP block-high-risk		0
APP default	Monitor all applications.	0
APP wifi-default	Default configuration for offloading WiFi traffic.	1

## Create Application Control Profile - Continue

- ④ Write [ Application Control Name ]
- ⑤ Block Video /Audio
- ⑥ OK

FortiGate-VM64

Dashboard

Network

Policy & Objects

Security Profiles

AntiVirus

Web Filter

Video Filter

DNS Filter

Application Control

Intrusion Prevention

File Filter

SSL/SSH Inspection

Application Signatures

IPS Signatures

Web Rating Overrides

Web Profile Overrides

VPN

User &

FortiGate-VM64

New Application Sensor

Name: Video\_Block

Comments: 0/255

Categories

All Categories

Business (179, 6)

Collaboration (293, 6)

Game (124)

Mobile (3)

P2P (85)

Remote.Access (91)

Storage.Backup (296, 16)

Video/Audio (206, 13)

Web.Client (18)

Cloud.IT (31)

Email (87, 12)

General.Interest (241, 9)

Network.Service (332)

Proxy (106)

Social.Media (150, 31)

Update (48)

VoIP (31)

Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

OK

Cancel

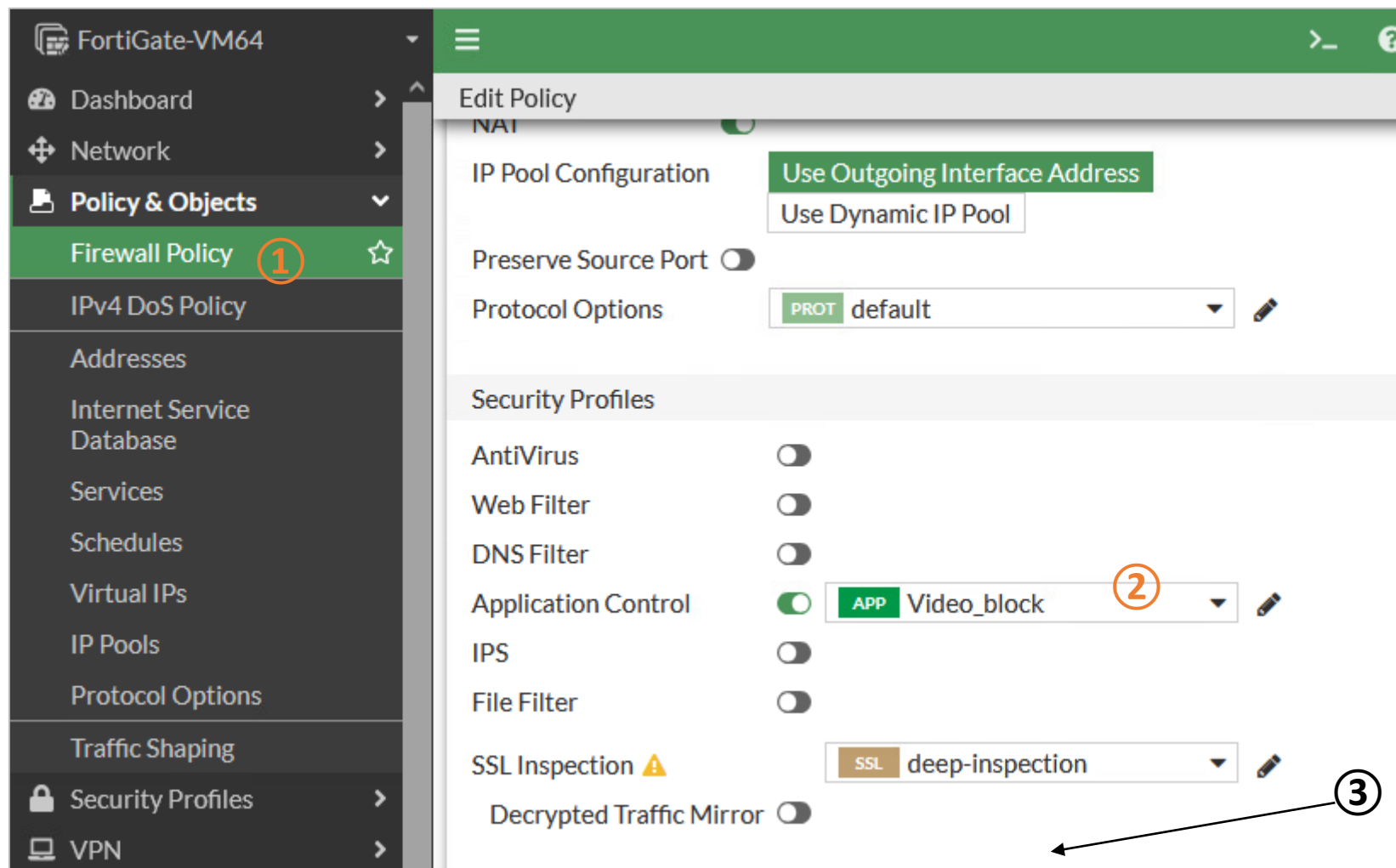
Activate Windows

Go to Settings to activate Windows.



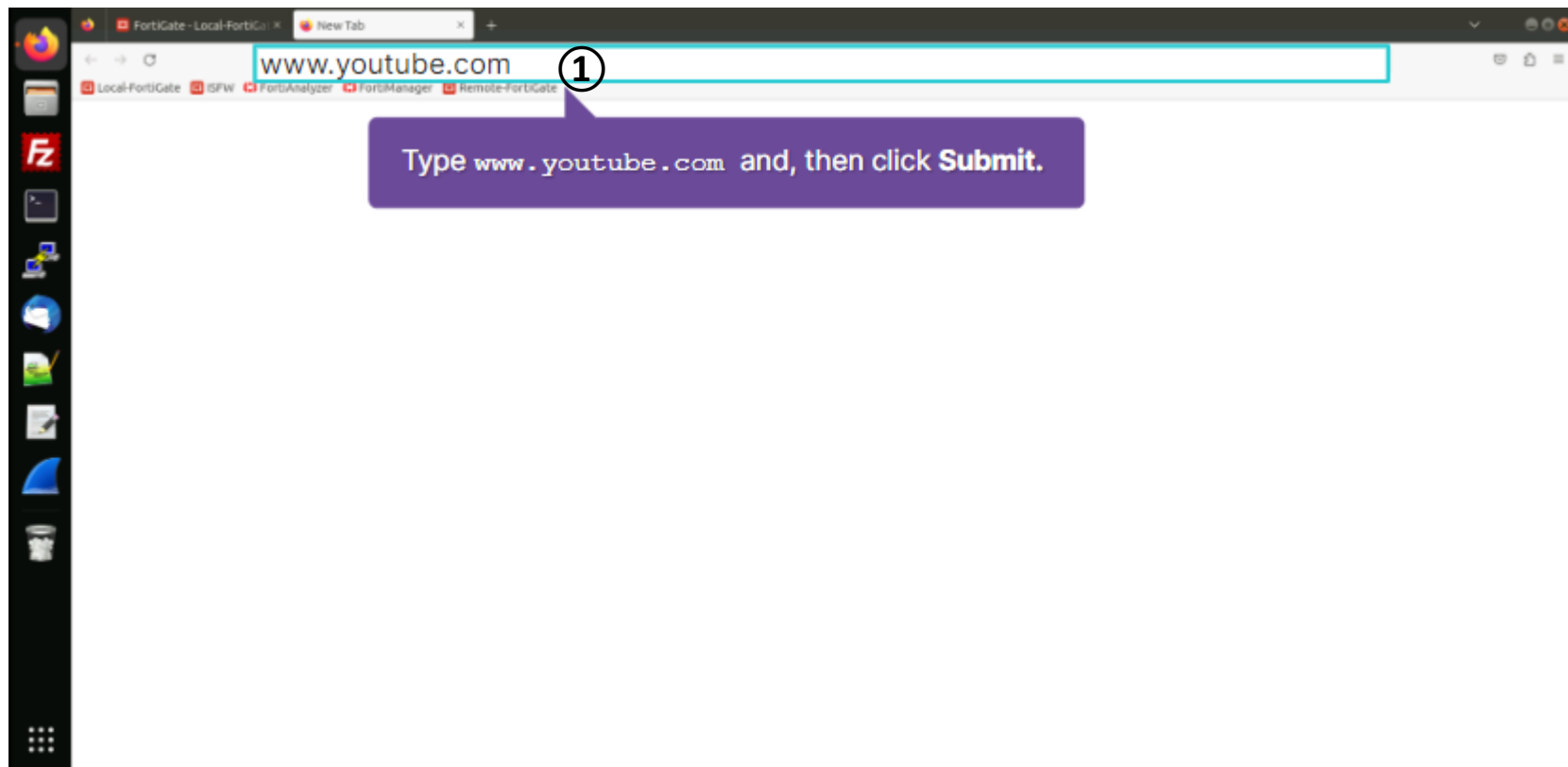
## Add Application Control Profile in Firewall Policy

- ① Policy & Objects ➔ Firewall Policy ➔ [Edit] Internet Access Policy
- ② Application Control [ Enable ] and Choose Video\_block
- ③ OK



# Verify Application Control

① Browse → [www.youtube.com](http://www.youtube.com)



# Monitoring Application Control

- ① Log & Report
- ② Application Control (or) Security Event ➔ Application Control
- ③ Confirm the Application Control Sensor was used, meaning Block\_Video for YouTube

FortiGate-VM64

User & Authentication

System

Security Fabric

Log & Report

Forward Traffic

Local Traffic

Sniffer Traffic

Events

AntiVirus

Web Filter

SSL

DNS Query

File Filter

Application Control

Intrusion Prevention

Anomaly

Log Settings

Threat Weight

admin

3

Details

Date/Time	Source	Destination	Application Name	Action
2024/07/14 02:16:16	192.168.11.66	172.253.118.136 (youtube-ui.l...	YouTube	block
2024/07/14 02:16:15	192.168.11.66	54.177.212.176 (fortinet.com)	HTTPS.BROWSER	pass
2024/07/14 02:16:13	192.168.11.66	54.177.212.176 (fortinet.com)	HTTPS.BROWSER	pass
2024/07/14 02:15:55	192.168.11.66	172.253.118.136 (youtube-ui.l...	YouTube	block
2024/07/14 02:15:54	192.168.11.66	172.253.118.136 (youtube-ui.l...	YouTube	block
2024/07/14 02:15:54	192.168.11.66	172.253.118.136 (youtube-ui.l...	YouTube	block
2024/07/14 02:15:54	192.168.11.66	172.253.118.136 (youtube-ui.l...	YouTube	block
2024/07/14 02:15:54	192.168.11.66	172.253.118.136 (youtube-ui.l...	YouTube	block
2024/07/14 02:15:53	192.168.11.66	74.125.24.105 (www.google.co...	HTTPS.BROWSER	pass
2024/07/14 02:15:53	192.168.11.66	74.125.24.105 (www.google.co...	HTTPS.BROWSER	pass
2024/07/14 02:15:53	192.168.11.66	64.233.170.94 (pki-goog.l.googl...	OCSP	pass
2024/07/14 02:15:53	192.168.11.66	74.125.24.105 (www.google.co...	HTTPS.BROWSER	pass
2024/07/14 02:15:53	192.168.11.66	64.233.170.94 (pki-goog.l.googl...	OCSP	pass

13



# Thank You

 Min Zaw Oo



Reference

