**Network Security Fundamentals**

**and**

**FortiGate Integration**

Asmaa Hazem Ali

Mariam Yasser Mattar

Ahmed Shaaban

Abdelrahman Mohamed

Contents

[**Cybersecurity** 3](#_Toc197989946)

[**Cybersecurity Threats** 3](#_Toc197989947)

[**Cybersecurity Vulnerability** 3](#_Toc197989948)

[**Vulnerability scanning** 3](#_Toc197989949)

[**OWASP Top 10:2021** 4](#_Toc197989950)

[**Network attacks** 5](#_Toc197989951)

[**Types of Network Attacks** 5](#_Toc197989952)

[**FortiGate Basic Configuration** 6](#_Toc197989953)

[**FortiGate Policies and NAT** 10](#_Toc197989954)

# **Cybersecurity**

Cybersecurity is the practice of protecting digital systems, networks, and data from unauthorized access, damage, or attacks. In today’s connected world, it plays a vital role in securing personal information, business operations, and critical infrastructure. With the growing reliance on technology, ensuring the safety of our digital environment has become more important than ever.

As technology advances, so do the methods used by cybercriminals. Cybersecurity threats are malicious attempts to damage, steal, or disrupt data and systems, while vulnerabilities are weaknesses in software, hardware, or processes that attackers exploit. Understanding both threats and vulnerabilities is essential to building effective defenses and maintaining trust in our digital systems. A network attack happens when a threat exploits a vulnerability to gain unauthorized access, steal data, or disrupt services.

# **Cybersecurity Threats**

Cybersecurity threats are deliberate attempts to breach the confidentiality, integrity, or availability of digital systems. These threats can originate from a variety of sources, including individual hackers, organized crime groups, state-sponsored actors, and even insiders within an organization. As digital dependence grows globally, so does the complexity and frequency of cyber threats, making them a major concern for individuals, businesses, and governments.

# **Cybersecurity Vulnerability**

A cybersecurity vulnerability is a weakness or flaw in a system, application, or process that can be exploited by an attacker to gain unauthorized access, disrupt operations, or steal sensitive data. These vulnerabilities can exist in software code, network configurations, or even in user behavior. For example, an unpatched operating system, a misconfigured firewall, or a web form that doesn’t validate user input can all create opportunities for attackers. Vulnerabilities are not threats themselves but become dangerous when discovered and targeted by threat actors. Addressing vulnerabilities through regular updates, secure coding practices, and proper system configuration is essential to prevent cyberattacks and protect digital assets.

# **Vulnerability scanning**

Vulnerability scanning is a cybersecurity process that checks systems for known flaws like outdated software, misconfigurations, or missing patches. It helps identify risks such as injection, broken access control, and weak authentication; allowing organizations to fix issues before attackers exploit them.

## **OWASP Top 10:2021**

The OWASP Top 10 is a list of the most serious security threats to web applications, published by the Open Worldwide Application Security Project. The 2021 update reflects shifts in risk priorities since 2017, ranking the most critical issues, starting with A01 as the highest. It’s a key resource for developers to understand and reduce web security risks.

1. **Broken Access Control**

Users gain access to data or actions they shouldn’t. This includes privilege misuse.

Fix: Use least privilege, strong session handling, regular access reviews, and monitor behavior to block suspicious actions.

1. **Cryptographic Failures**

Sensitive data isn’t properly encrypted or is exposed via weak protocols or keys.

Fix: Use strong encryption, HTTPS, secure cookies, and manage keys safely.

1. **Injection**

Attackers send malicious input (like SQL or scripts) into the app due to poor input validation.

Fix: Validate inputs, use safe APIs, escape characters, and avoid raw queries.

1. **Insecure Design**

Security was never planned into the app's structure.

Fix: Start with secure design, use threat modeling, apply security patterns, and limit access.

1. **Security Misconfiguration**

Weak settings like open ports, default passwords, or verbose errors make the system vulnerable.

Fix: Harden configurations, remove unused features, patch systems, and use security headers.

1. **Vulnerable & Outdated Components**

Old libraries or tools with known flaws expose the app to attacks.

Fix: Update components, remove unused files, use trusted sources, and automate vulnerability checks.

1. **Identification & Authentication Failures**

Login systems are weak or mismanaged, allowing unauthorized access.

Fix: Use MFA, strong passwords, secure sessions, and block brute force attempts.

1. **Software & Data Integrity Failures**

Apps trust code or data without verifying if it’s safe or unchanged.

Fix: Use digital signatures, trusted sources, secure CI/CD pipelines, and avoid sending unsigned data.

1. **Security Logging & Monitoring Failures**

Lack of logging or alerting makes attacks hard to detect or investigate.

Fix: Log key events, protect logs, monitor actively, and have a response plan.

1. **Server-Side Request Forgery (SSRF)**

The app fetches URLs based on user input, letting attackers reach internal systems.

Fix: Validate URLs, block internal access, restrict traffic, and avoid raw responses.

# **Network attacks**

Network attacks are unauthorized actions targeting the applications, systems, or data within a company's network. These attacks are typically carried out by malicious actors aiming to alter, steal, or destroy sensitive information. Some network attacks are passive, meaning they silently monitor or capture data without making any changes—such as eavesdropping or traffic analysis. In contrast, active attacks are more aggressive; they involve actions like data modification, encryption, or system disruption.

## **Types of Network Attacks**

1. **Passive Attacks**

Attacks involve silently monitoring or intercepting data without changing anything. The goal is to gather information without being detected.

1. **Active Attacks**

Attacks involve altering, disrupting, or damaging systems and data. These are more aggressive and easier to detect.

Below is some key network attacks described in more detail:

**DDoS (Distributed Denial of Service):**

DDoS attacks overload a website or server with too much traffic, making it crash or become slow. Hackers use many infected devices (called a botnet) to send the traffic. Big sites like Twitter and Netflix were once taken down this way.

**Phishing:**

Phishing is when hackers send fake emails or messages that look real, like from a bank or company, to trick people into giving passwords or personal info. It can also happen through texts (called smishing) or target specific people (called spear phishing).

**Man-in-the-Middle (MITM) Attacks:**

In MITM attacks, hackers secretly get between two people communicating and can read or change what’s being sent. They often do this by setting up fake Wi-Fi or using tricks to make secure websites become insecure.

**Insider Threats:**

These happen when someone inside the company—like an employee—causes harm. It could be on purpose, like stealing data, or by mistake, like clicking a bad link. Even trusted people can be a risk.

**Privilege Escalation:**

Hackers use this to get more control inside a system. They start with limited access and find ways to become admins by using stolen passwords or system bugs. Once they have admin rights, they can do serious damage.

After understanding core network security principles, we applied them by configuring the FortiGate firewall; an essential network device that controls traffic flow, assigns IP addresses, and enforces basic security policies to protect internal networks and manage internet access.

# **FortiGate Basic Configuration**

In this phase, we configured the FortiGate firewall from factory defaults to build a secure and functional network. We connected the firewall to the internet, assigned internal IP addresses using DHCP on LAN interfaces, and configured a default static route for internet access. To secure the network, we created firewall policies with NAT and applied security profiles to control and filter outgoing traffic. Local user accounts were also set up for access control, and we verified that connected devices were detected and online through the Security Fabric. These steps confirm the successful basic setup of the FortiGate system.

**DHCP Server Configuration**

This screenshot shows the internal interface configured with:

* DHCP range: 192.168.2.2 – 192.168.2.100
* DNS: 8.8.8.8
* Gateway: same as interface IP

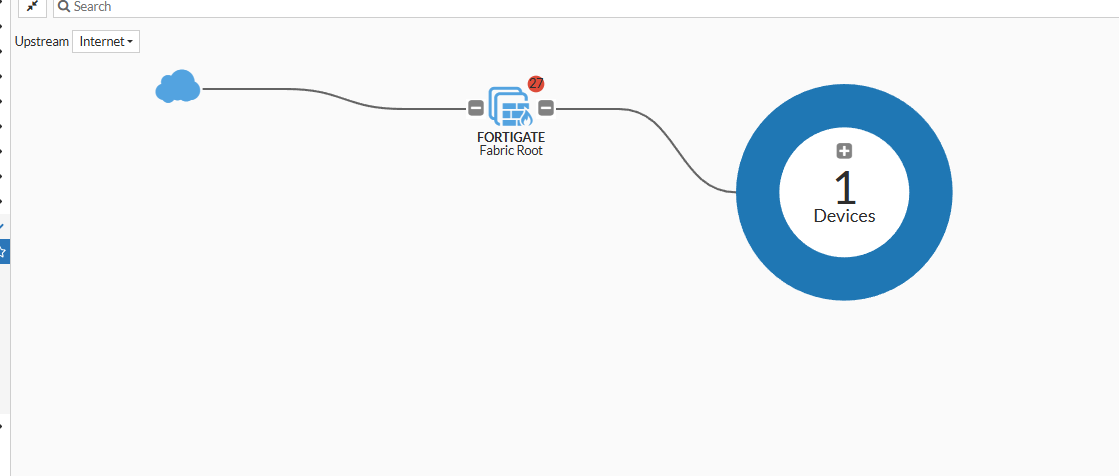
This is the basic step to assign IP addresses automatically to devices.

**A screenshot of a computer

AI-generated content may be incorrect.**

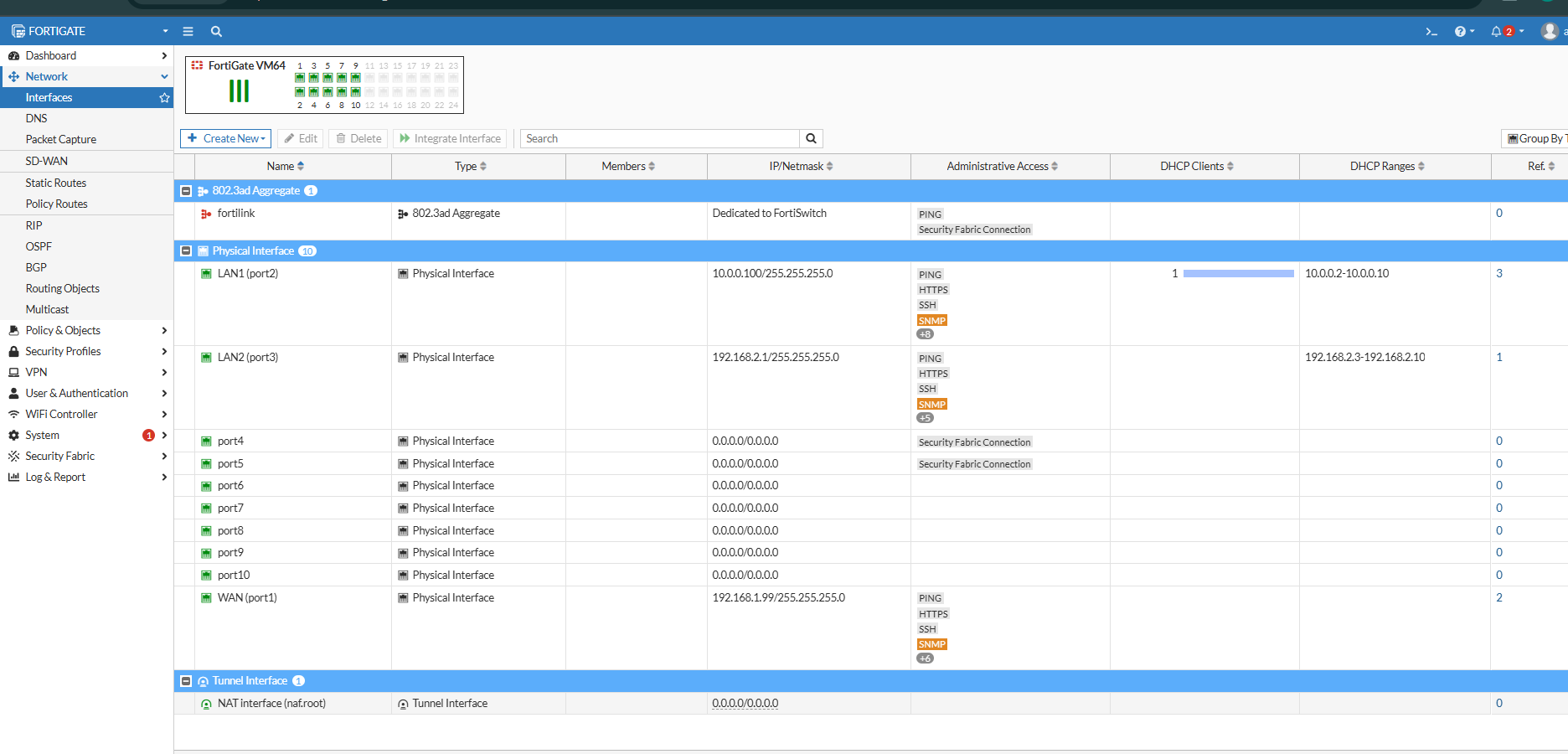
**Security fabric**

Shows the FortiGate connected to the internet and managing 1 internal device.



**Interfaces Configuration**

Port1 is WAN (192.168.1.99), Port2 is LAN1 (10.0.0.1 with DHCP), Port3 is LAN2 (192.168.2.1 with DHCP). Other ports are unused. Admin access (HTTPS/SSH/PING) is enabled on WAN.



**Static Route**

A default route (0.0.0.0/0) is set to 192.168.1.1 via port1, enabling internet access for all outgoing traffic.

A screenshot of a computer

AI-generated content may be incorrect.

**Firewall Policies**

Two policies:

* **Policy 1**: Allows LAN to WAN with security profiles (AV, web filter, app control) and NAT.
* **Policy 2**: Likely blocks or restricts social media usage.

A screenshot of a computer

AI-generated content may be incorrect.

**User Configuration**

Local users “ahmed” and “guest” are created. Groups are set. Can be used for user-based access or portal logins.

A screenshot of a computer

AI-generated content may be incorrect.

**Asset Identity Center**

Detects one active client (10.0.0.2) on the LAN with hostname and OS info. Confirms device tracking and visibility are functioning.

A screenshot of a computer

AI-generated content may be incorrect.

# **FortiGate Policies and NAT**

In this phase, we focused on setting up firewall policies and NAT on the FortiGate firewall to control traffic and secure internet access. We started with a basic NAT policy using the outgoing interface address, then configured dynamic IP pools and fixed port ranges to manage how internal devices use external IPs. We verified all configurations by checking active sessions and testing internet access, like opening Gmail. After that, we enabled Central NAT, created SNAT rules for outgoing traffic, and set up DNAT with Virtual IPs to allow external users to reach an internal web server. We also added WAN-to-LAN firewall policies to complete the setup. All steps were tested and documented with screenshots.

**Basic NAT Policy**

Create firewall policy with NAT which allows internal clients to access the internet with NAT.

* NAT: Enabled

Activates Network Address Translation so internal devices can access the internet.

* Use Outgoing Interface Address

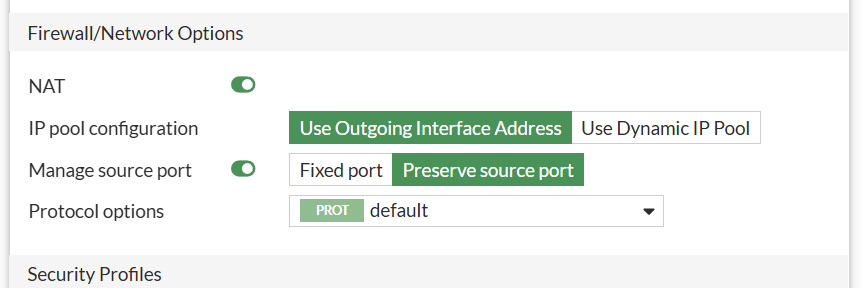
The FortiGate uses the IP of its WAN interface to translate all internal IPs. This is the easiest way to provide internet access when using a single public IP.

* Preserve Source Port

Keeps the original port, useful for applications needing consistent connections.

* Default

Uses standard protocol handling settings.

****

"Open sessions: PAT" appears because the firewall is translating many internal IPs to one external IP using different port numbers.

**Verify internet access and sessions**

BBC Website Opened in Browser which proves that internet is working after firewall configuration. This confirms NAT policy and DHCP setup were successful.



Shows NAT sessions working from internal IP (192.168.2.4) to external IPs. This confirms traffic is being NAT’d properly through FortiGate.

A screenshot of a computer

AI-generated content may be incorrect.

**Dynamic IP Pool – Overload**

* Type: Overload (To simulate PAT but with custom external IPs not the interface IP)

Allows many internal devices to share one or more external IPs using PAT (Port Address Translation).

* External IP Range: 192.168.1.100 – 192.168.1.102

These IPs will be used for NAT instead of the interface IP.

* NAT64: Disabled

You're not translating IPv6 to IPv4 here.

* ARP Reply: Enabled

Ensures FortiGate responds to ARP requests for these IPs, allowing the pool to be reachable on the network.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Verify session with IP Pool**

Shows NAT sessions using 192.168.1.100 from the configured pool. This confirms Overload NAT method is working.

A screenshot of a computer

AI-generated content may be incorrect.

**IP Pool – Fixed Port Range**

* Type: Fixed Port Range

Assigns specific port ranges per user for NAT translation. This gives more control compared to overload, which dynamically chooses ports.

* External IP Range: 192.168.1.200 – 192.168.1.201

Two external IPs available for NAT.

* Internal IP Range: 192.168.2.2 – 192.168.2.2

Only the device with this IP will be allowed to use this pool.

* Ports Per User: 32

Each internal client gets 32 ports from the pool, which helps manage bandwidth and limits simultaneous connections per user.

* ARP Reply: Enabled

FortiGate responds to ARP requests for these IPs, making them usable on the network.

This is useful for managing traffic load more precisely.

A screenshot of a computer

AI-generated content may be incorrect.

No session appeared because the internal IP range did not include the Windows device IP (192.168.2.4).

**Verify session with fixed port range**

Displays sessions and confirms that traffic is flowing through the NAT using port limits.

A screenshot of a computer

AI-generated content may be incorrect.

**Demonstration of Misconfiguration or IP Mismatch**

Shows gmail.com blocked due to incorrect IP pool or missing route. This is likely from a test before fixing the IP range in the NAT pool.

A screenshot of a computer

AI-generated content may be incorrect.

**Fixed Port Range IP Pool Configuration**

Setting up an IP pool (192.168.1.200–.201) with limited ports per user from specific internal IPs.

A screenshot of a computer

AI-generated content may be incorrect.

**Verifying Firewall Policy + NAT Success**

Gmail works, confirming NAT is working properly using the configured pool.

A screenshot of a computer

AI-generated content may be incorrect.

The session is in putty.

**Central NAT Setup**

Central NAT separates NAT rules from firewall rules, making NAT easier to manage; especially in large or complex networks.

This shows failure when trying to enable Central NAT due to an existing IP pool in use.

**A computer screen with text on it

AI-generated content may be incorrect.**

Central NAT cannot be enabled because it conflicts with an existing firewall policy that uses an IP Pool. Central NAT requires direct NAT configurations and does not support IP Pools.

**Central NAT Enabled Successfully**

A screenshot of a computer

AI-generated content may be incorrect.

**Creating/Editing Policies**

Before enabling central NAT: After enabling central nat: snat ,dnat appear

A screenshot of a computer

AI-generated content may be incorrect. A screenshot of a computer

AI-generated content may be incorrect.

**Configuring Central SNAT**

Central nat: snat

* Incoming Interface: LAN (port2)

Accepts traffic from internal users.

* Outgoing Interface: WAN1 (port1)

Sends traffic out to the internet.

* Source & Destination: all

Applies to any IP address.

* NAT: Enabled

Turns on NAT so devices can access the internet.

* Use Outgoing Interface Address

Uses the WAN IP for NAT (no custom IP pool).

* Protocol: Any

Works for all protocols like web, email, etc.

* Preserve Source Port: Off

Allows FortiGate change ports to avoid conflicts.

* Explicit Port Mapping: Off

Port assignment is automatic.

* Enable this policy: On

The rule is active and working.

A screenshot of a computer

AI-generated content may be incorrect.

**DNAT with Virtual IP**

Maps an external IP 192.168.1.101 to internal web server 192.168.2.15. This enables external users to reach internal services.

A screenshot of a computer

AI-generated content may be incorrect.

**Policy for Accessing Internal Server (DNAT)**

This creates WAN to LAN Firewall Policy. It allows traffic from WAN to reach internal web\_server

A screenshot of a computer

AI-generated content may be incorrect.

**FortiGate Policies**

After configuring NAT, the next step was to create firewall policies to control the traffic flow between network zones. Firewall policies define which types of traffic are allowed or blocked, based on source, destination, service, and schedule. These rules are essential for securing the network, allowing internet access, and enabling services like port forwarding. In this phase, we created policies for LAN-to-WAN traffic, as well as WAN-to-LAN access to internal servers using DNAT.

**Firewall policy**

Enable deep inspection and use proxy-based mode.

Configuration Choices:

* Incoming: port2 (LAN)

This is the internal network interface where user traffic originates. It's selected to allow outgoing traffic from devices in the LAN.

* Outgoing: port1 (WAN)

This is the interface connected to the internet. Traffic is forwarded through it to reach external websites.

* Source & Destination: all

This allows all devices (source) to access all internet addresses (destination). Used during testing or for open internet access.

* Schedule: always

Ensures the policy is always active, 24/7. No time restrictions needed during setup/testing phase.

* Service: all

Allows all types of traffic (HTTP, HTTPS, DNS, etc.). Good for general access when no filtering is applied yet.

* Action: Accept

Permits the traffic to pass through. Required to allow LAN users to access external resources.

* NAT: Enabled, Use Outgoing Interface

This translates internal (private) IPs to the public IP on the WAN interface. Chosen for simplicity and quick internet access.

**A screenshot of a computer

AI-generated content may be incorrect.**

**Logging & Inspection Options**

Applies advanced security features to firewall rules — required for monitoring and HTTPS inspection.

Configuration Choices:

* Inspection Mode: Proxy-based
* SSL Inspection: Enabled (custom profile)
* Logging: All sessions  
  Purpose: Enables deep packet inspection (DPI) and visibility into all allowed traffic

**A screenshot of a computer

AI-generated content may be incorrect.**

**Facebook Access Test**

Verifies that the firewall policy allows real-time internet access. This confirms that the internet\_access policy is functional.

Before deep inspection:

A screenshot of a computer

AI-generated content may be incorrect.

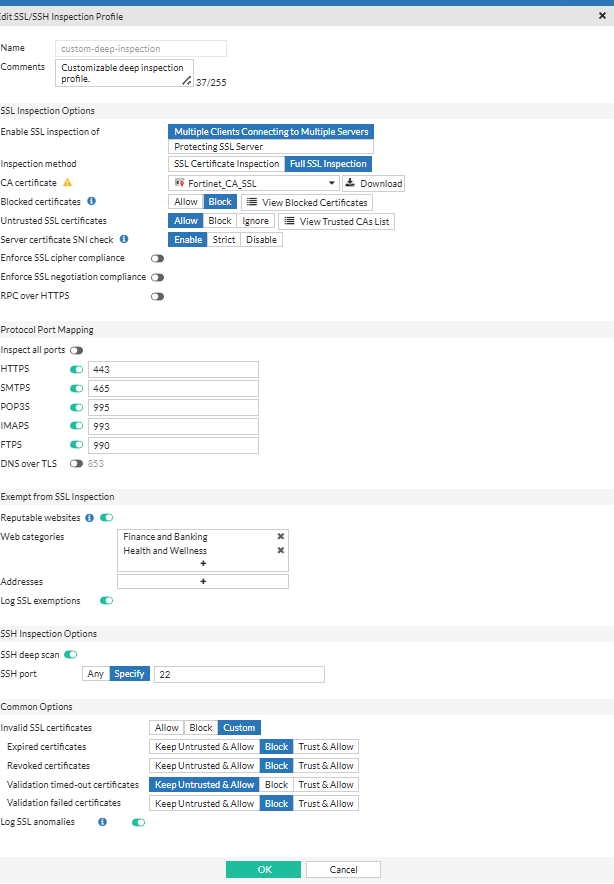
**SSL Inspection Profile**

Scans encrypted traffic for threats.

**Configuration Choices:**

* **Method:** Full SSL Inspection
* **Ports Inspected:** HTTPS, SMTPS, IMAPS, etc.
* **Exceptions:** Banking and health sites
* **Action for invalid certs:** Block

After deep inspection:



**SSL Certificate Error Page**

Client browser doesn't trust FortiGate’s CA certificate. This happens when using Full SSL Inspection without installing the FortiGate root CA on the client.

A screenshot of a computer error

AI-generated content may be incorrect.

**Certificate Viewer**

The certificate is issued by Fortinet. FortiGate's Deep Inspection can cause SSL errors if its CA certificate is not trusted by client devices, leading to blocked HTTPS traffic or certificate warnings. It confirms Full SSL Inspection is intercepting Gmail traffic, which is expected behavior.

A screenshot of a computer

AI-generated content may be incorrect.

After installing the certificate on client devices, HTTPS traffic works without errors or warnings.

**Trusted Root Certificate List**

FortiGate CA certificate added to trusted list.

A screenshot of a computer screen

AI-generated content may be incorrect.

**Gmail Access Restored**

Verifies that after installing the FortiGate certificate, SSL inspection works without browser errors. This confirms firewall + SSL inspection + certificate setup is complete and working.

A screenshot of a computer

AI-generated content may be incorrect.

**Web filter profile**

**Configuration Choices:**

* **Type:** Proxy-based
* **Category Actions:** Warning, Allow, Authenticate
* **Categories Filtered:** Adult, Alcohol, Bandwidth consuming, etc.

Enable the feature in proxy-based mode. Require authentication for Sports Hunting and War Games categories.

**A screenshot of a computer

AI-generated content may be incorrect.**

**Edit Filter – Warning Interval**

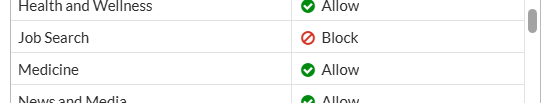
Sets a 2-minute warning for users before applying stricter web filtering. It enforces timed filtering rules for specific user groups using FortiGuard warnings.

A screenshot of a computer

AI-generated content may be incorrect.

**Web Filter Category – Job Search Blocked**

Demonstrates a specific web category (Job Search) set to Block while others like Health and Wellness are allowed. This applies category-based control to restrict access to specific types of websites.

****

**Static URL Filter - Single Keyword (weabons)**

**A screenshot of a computer

AI-generated content may be incorrect.**

Enable blocking of invalid URLs and use the content filter to create a rule that blocks the keyword "weabons".

**Multiple Static Filters – weabons, guns, cat**

Shows extended static filtering. This strengthens control over dangerous or non-productive content using custom word-based filters.

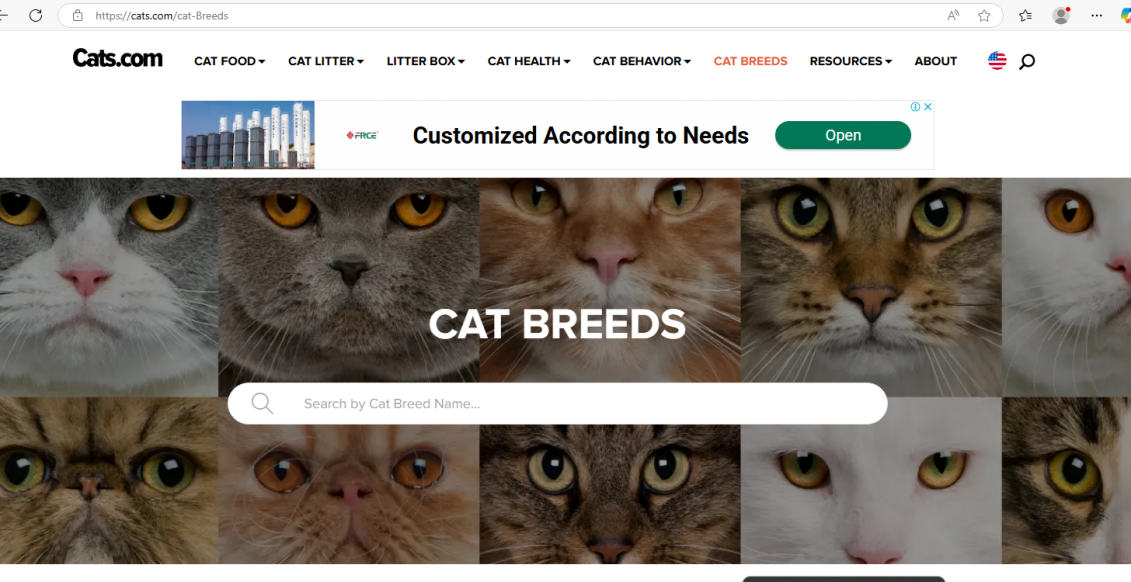
**A screenshot of a computer

AI-generated content may be incorrect.**

**Test Result – Cat Website Accessed**

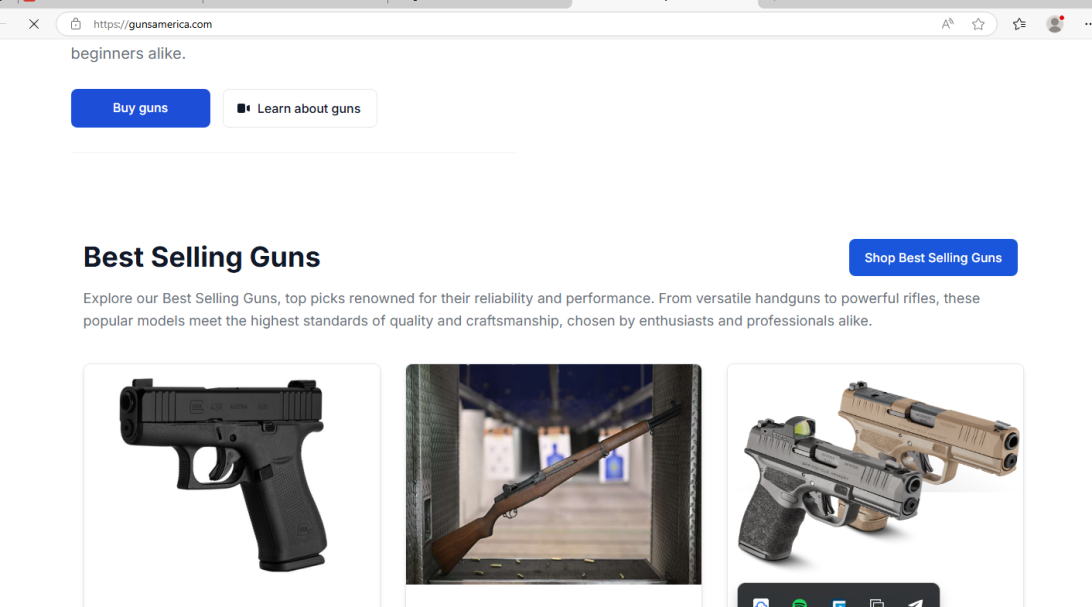
Blocked due to static URL pattern guns. This confirms URL filter is active and working.

Before enabling and applying this web filter profile to the firewall policy:



**Test Result – Guns Website Blocked**

Website blocked successfully. This confirms URL filter is active and working.



**Fishing & Hunting Website Accessed**

A screenshot of a computer

AI-generated content may be incorrect.

Websites like fieldandstream.com or paintballgames.co.uk require authentication due to the applied web filter.

**FortiGuard Block Page – Sports Hunting**

Shows FortiGuard category-based blocking is enforced.

A screenshot of a computer

AI-generated content may be incorrect.

**Web Filter Override Prompt**

After adding the web filter profile, authentication is required. The policy allows manual override by authenticated users.

A screenshot of a computer error

AI-generated content may be incorrect.

**OutdoorLife Website Accessed**

Access granted after override. This confirms override credentials worked, showing policy flexibility.

A screenshot of a computer

AI-generated content may be incorrect.

**Freelancer Blocked Page**

This page shows FortiGuard blocking access to a site in the Job Search category.

**Config Choices Implemented:**

* Web Filter profile has Job Search category set to **Block**.
* This enforces user browsing restrictions based on categories.

A screenshot of a computer

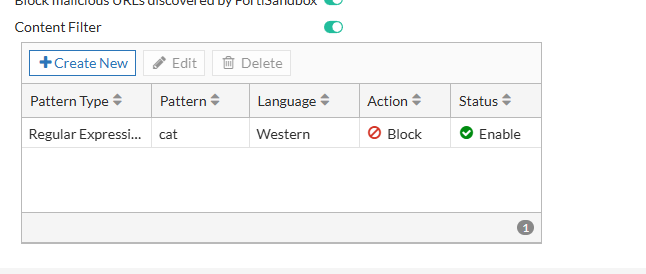
AI-generated content may be incorrect.

**Content Filter**

A content filter with regex blocking the word "cat".

**Config Choices Implemented:**

* Pattern Type: **Regular Expression**
* Pattern: cat
* Action: **Block**
* Status: **Enabled**

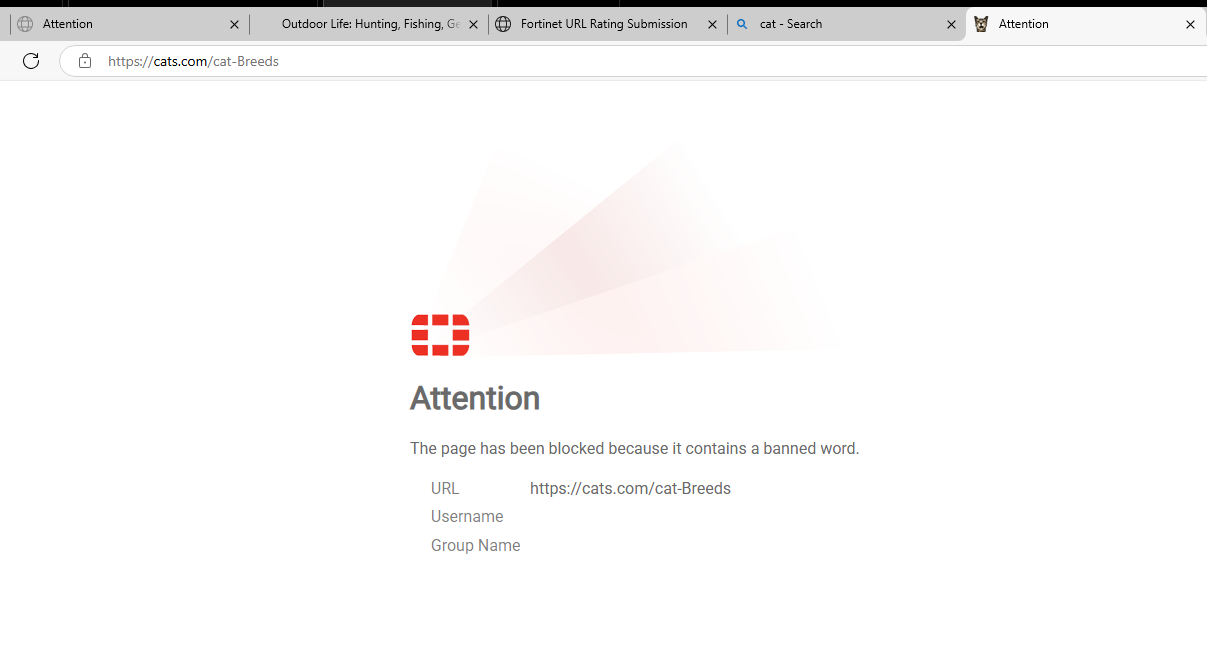


**Blocked Page**

This page shows the site **cats.com** blocked due to the banned word **"cat".**

**Config Choices Implemented:**

* Regular expression cat matched in the URL.
* Enforced by the Content Filter profile in the applied firewall policy.

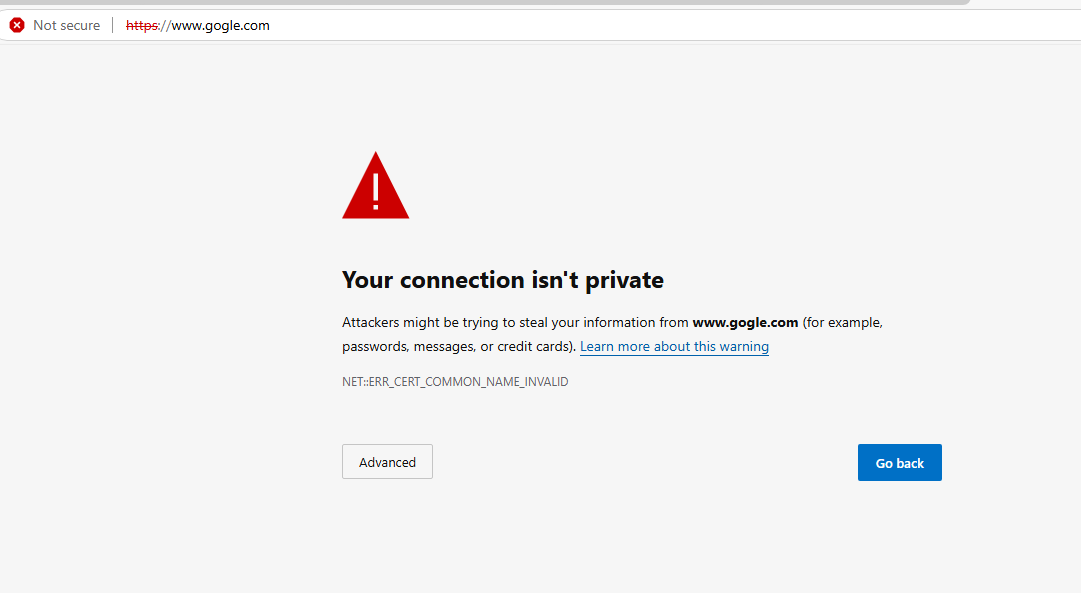


**Certificate Error**

Browser warning due to invalid SSL certificate (name mismatch).

**Config Choices Implemented:**

* FortiGate is doing **Full SSL Inspection**, but the website has a **bad cert.**
* Certificate validation failed → browser flagged it as unsafe.



**Video Filter – Music Block**

**Relation to Firewall Policy:**

* FortiGuard Video Filter profile blocks the **Music** category.
* **Config Choices Implemented:**
  + Category: **Music**
  + Action: **Block**
  + Filter Type: **Proxy-based** or **Flow-based**

A screenshot of a computer

AI-generated content may be incorrect.

**YouTube Channel ID in Source**

* YouTube channel identified in page source.
* Useful for Custom Filtering if blocking specific channel IDs.
* Not directly applied yet, but can be added to URL filter patterns.

A computer screen shot of a computer code

AI-generated content may be incorrect.

Antivirus Profile Config

Shows antivirus profile antivirus\_new used in security inspection.

Config Choices Implemented:

* Scans HTTP, FTP, SMTP, etc.
* Virus Outbreak Prevention using virus\_total
* Block action for malware and viruses.

A screenshot of a computer

AI-generated content may be incorrect.

**WICAR – Malware Testing Site**

Site used to test AV filtering.

Config Choices Implemented:

* EICAR test file used.
* Should trigger block if FortiGate antivirus is working.

A screenshot of a computer

AI-generated content may be incorrect.

**EICAR Blocked Alert**

**Relation to Firewall Policy:**

* FortiGate successfully blocks EICAR test virus.
* **Config Choices Implemented:**
  + Detected by AV engine.
  + Action: **Blocked**
  + Severity: High/Critical.

A screenshot of a computer

AI-generated content may be incorrect.

**AV Log Entry for EICAR**

Log shows virus blocked.

Config Choices Implemented:

* Detailed AV event shown.
* Action: Blocked
* Profile: antivirus\_new

A screenshot of a computer

AI-generated content may be incorrect.

IPS Signature Filter Configuration

* **Type: Filter** – Applies a group of IPS signatures based on criteria.
* **Action: Default** – Uses each signature’s default action (usually Block).
* **Packet Logging: Disable** – Reduces system load, logs not saved.
* **Status: Enable** – Activates the IPS filter.
* **Filter: Client** – Targets client-side attacks (e.g., browsers, apps).
* **Signatures: Block actions** – Blocks traffic matching known CVEs.
* **Purpose** – Protects internal users from exploits during web/app usage.
* **Use in firewall** – Applied in security profiles within firewall policy.

A screenshot of a computer

AI-generated content may be incorrect.

IPS (Intrusion Prevention): Use "Filter: Client" to protect client devices without overloading the system with unnecessary signatures.

**IPS Sensor**

To detect and block client-side attacks such as buffer overflows, browser exploits, and known vulnerabilities targeting end-user devices.

Configuration:

* IPS profile named protect\_client
* Default action applied to detected signatures
* Logging disabled (can be enabled later for forensic analysis)
* Block malicious URLs is off, so no URL-based blocking

A screenshot of a computer

AI-generated content may be incorrect.

**Ping Attack Attempt (from Kali)**

Simulates a large ICMP packet attack to test if IPS blocks oversized packets or malformed traffic. This shows how IPS drops malformed packets (e.g., large ICMP sizes) — verified with 100% packet loss and session logs showing IPS inspection.

A computer screen with white text

AI-generated content may be incorrect.

**Debug Log: IPS Session Output**

Shows FortiGate intercepted and forwarded the session to IPS. This confirms IPS is enabled and actively inspecting — session marked with send to ips.

A black screen with white text

AI-generated content may be incorrect.

Add the Kali to Port3.

**Routing Table Check**

Ensures routing is correct so IPS and other policies can act on reachable traffic. This confirms LAN and WAN are correctly connected (192.168.1.x, 192.168.2.x, 10.0.0.x), so policies apply cleanly to expected zones.

A screenshot of a computer screen

AI-generated content may be incorrect.

**Forward Traffic Logs**

Shows that packets from kali and other clients to the destination were blocked due to policy violation and IPS detection.

* Blocked by IPS or Application Control
* Confirms enforcement of policy

A screenshot of a computer

AI-generated content may be incorrect.

**Application Control Profile**

To block social media and high-bandwidth-consuming apps while allowing monitoring of others like LinkedIn.

**Configuration:**

* Blocks categories: Social Media, P2P, Proxy
* Monitors LinkedIn (instead of blocking)
* Blocks excessive bandwidth usage

A screenshot of a computer

AI-generated content may be incorrect.

**LinkedIn Application Override**

To specifically allow tracking and control of LinkedIn usage across file uploads, logins, posts, etc.

Configuration:

6 LinkedIn app signatures are set to “Monitor” in Application Control.

**A screenshot of a computer

AI-generated content may be incorrect.**

**Firewall Policy (test\_application\_control)**

Main rule to apply IPS, Application Control, SSL Inspection, DNS filtering, etc. between LAN interfaces.

Configuration:

* Source: port2 (LAN), Destination: port3 (LAN2)
* Enabled IPS, custom SSL inspection, App Control (block\_social\_large\_bandwidth)
* Proxy-based inspection to enable deep packet inspection

**A screenshot of a computer

AI-generated content may be incorrect.**

**Facebook Blocked (ERR\_CONNECTION\_CLOSED)**

Blocked by Application Control due to Social Media category being denied. This is enforced by the block\_social\_large\_bandwidth profile assigned in the firewall policy.

A screenshot of a computer

AI-generated content may be incorrect.

**LinkedIn Verification Page**

LinkedIn not blocked, but traffic is being monitored (possibly redirected to verification puzzle due to policy restrictions or LinkedIn detection of inspection). This shows that LinkedIn is monitored, not blocked, as configured in the application control override.

A screenshot of a computer

AI-generated content may be incorrect.

**YouTube Buffering**

The video is still loading and not playing because "Excessive-Bandwidth" is blocked in the Application Control profile. This blocks high-bandwidth apps like YouTube, causing buffering or failure to load.

A screenshot of a video chat

AI-generated content may be incorrect.

After completing all firewall configurations, we tested each setup using session monitoring, browser-based verification, and policy behavior checks. Internet access was successfully achieved through different NAT methods, including interface-based and IP pool NAT. Central NAT, SNAT, and DNAT were also configured and validated with internal and external traffic. The use of deep inspection and proxy-based mode enhanced traffic control and visibility. All outcomes were documented with screenshots to confirm correct implementation.

To conclude, this project demonstrated the practical application of FortiGate firewall configurations to secure and manage network traffic effectively. We began with basic NAT policies using the outgoing interface and expanded to advanced techniques like dynamic IP pools, fixed port ranges, and Central NAT. Deep inspection and proxy-based mode were enabled to improve traffic visibility and enforce security controls such as web filtering and antivirus scanning. All configurations were tested and verified using real-time browsing and session monitoring. This setup reflects essential firewall practices and highlights how FortiGate can be used to build a secure, well-managed network.