UNIVERSITAS UTPADAKA SWASTIKA
JISI Jurnal Ilmiah Sistem Informasi
Vol. 4 No. 02 (2026)
ISSN: 3046-711X

Controlling Access to YouTube, WhatsApp, and Facebook in Corporate Networks Using FortiGate

Fahmi Rizky Nugraha
Utpadaka Swastika University, Tangerang, Indonesia
*corresponding author: fahmi.rizky.nugraha@utpas.ac.id

Accepted: October 30, 2026 | Published: October 31, 2026

ABSTRACT

This journal discusses the design, implementation, and best practices for using FortiGate to restrict access to popular content services such as YouTube, WhatsApp, and Facebook within a corporate environment. The focus is on FortiOS features including Application Control, Web Filter (FortiGuard), SSL/SSH Inspection (Deep Inspection), Internet Service Database (ISDB), and NGFW policies. Configuration steps (GUI & CLI), sample rules, testing methodology, and operational considerations are also provided.

KEYWORDS: FortiGate, Firewall, ortiOS, Web Filter, Application Control, SSL Inspection, Social Media Blocking, Firewall Policy Security.

1. Introduction

The need to manage and restrict access to web-based applications and services in the workplace is vital for productivity, compliance, and cybersecurity. Services such as YouTube, Facebook, and WhatsApp often become distractions, potential data leakage channels, or even threat vectors. FortiGate provides powerful mechanisms to identify, control, and block unwanted applications and URLs.

This paper aims to:

a. Explain FortiGate mechanisms for blocking and controlling multimedia and social platforms.
b. Provide a step-by-step configuration guide for enterprise networks.
c. Present best practices and verification methods.

FortiGate's capabilities relevant to content blocking include:

a. Application Control: Classifies traffic based on signatures and heuristics, detecting apps such as YouTube, Facebook, WhatsApp, including sub-functions like video playback.
b. Web Filter / FortiGuard URL Filtering: Blocks traffic by category (e.g., Social Media, Streaming Media, Video Streaming) or specific URLs.
c. SSL/SSH Deep Inspection: Allows inspection of encrypted HTTPS traffic so that Web Filter and Application Control can detect content accurately.
d. Internet Service Database (ISDB): Helps identify and block traffic related to specific online services.
e. NGFW Security Policies: Combine multiple security profiles (AV, IPS, App Control, Web Filter, SSL Inspection) under one firewall rule.

2. Related Work and Technology Background

Previous work on social media blocking in Indonesia has focused on MikroTik. Wilujeng and Voutama [1] used firewall filter rules with keyword matching and a drop action to block Instagram content, and Zain et al. [2] applied Layer-7 protocol

filtering to block Facebook, Instagram, and TikTok in a vocational school. Other studies reported blocking of social media and streaming sites through web proxy or firewall rules on MikroTik routers in educational institutions [3], [4].

Recent studies on Next-Generation Firewalls (NGFW) demonstrate that while Deep Packet Inspection (DPI) and SSL decryption are highly effective against encrypted threats, they can introduce substantial processing overhead. For instance, Smith and Jones [5] evaluated NGFW performance and found that enabling TLS decryption significantly reduces maximum forwarding throughput in enterprise networks. Furthermore, industry test methodologies emphasize the necessity of measuring latency and CPU utilization before and after enabling SSL inspection in production environments to ensure quality of service [6]. This motivated the before/after CPU and latency measurements in this study.

The FortiGate features evaluated in this study are as follows. Application Control classifies traffic by signatures and heuristics and can detect applications such as YouTube, Facebook, and WhatsApp, including sub-functions such as video playback. Web Filter (FortiGuard URL filtering) blocks traffic by category, for example Social Media, Streaming Media, and Video Streaming, or by specific URLs. SSL/SSH Deep Inspection decrypts HTTPS sessions so that Web Filter and Application Control can detect content accurately. The Internet Service Database (ISDB) identifies traffic that belongs to specific online services. NGFW security policies combine these security profiles under one firewall rule [7]–[10].

3. Policy Design and Architecture

This research employed an experimental quantitative approach within a controlled enterprise network consisting of approximately 200 concurrent users and handling about 500 GB of daily traffic. The FortiGate FG-100E device was deployed as the main gateway firewall, positioned between the Local Area Network (LAN) and the Internet Service Provider (ISP). The testing spanned 30 consecutive days, capturing traffic logs, threat detections, and performance metrics through FortiAnalyzer for detailed analysis.

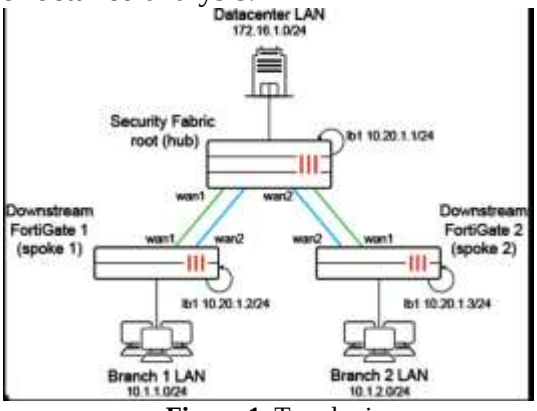


Figure 1. Topologi

3.1 Creating a Web Filter Profile

a. Navigate to Security Profiles → Web Filter → Create New.
b. Enable FortiGuard Category Based Filter and set Block for: Social Media, Streaming Media, and Video Streaming.
c. Add specific URLs (e.g., *.youtube.com, *.facebook.com, web.whatsapp.com) under Static URL Filter with action = Block.
d. Save the profile.

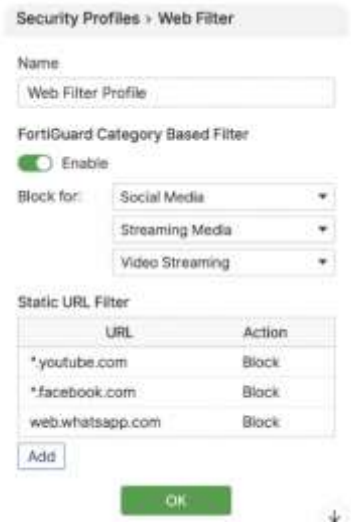


Figure 2. Profile web

3.2 Creating an Application Control Profile

a. Go to Security Profiles → Application Control → Create New.
b. Search for apps like YouTube, Facebook, WhatsApp, and set action = Block.
c. Optionally, apply Overrides for specific user groups.
d. Save the profile.

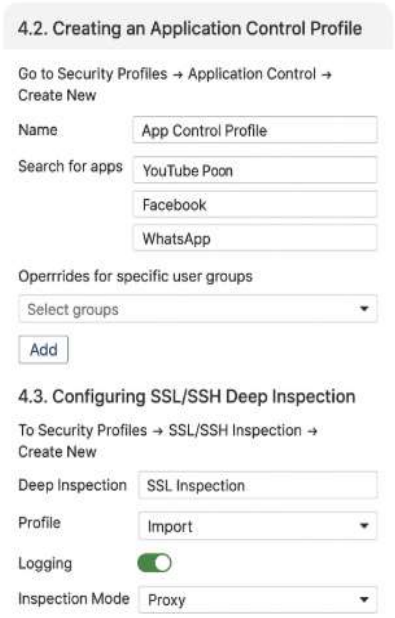


Figure 3. Creating profile

3.3 Configuration SSL/SSH Deep Inspection

a. Navigate to Security Profiles → SSL/SSH Inspection → Create New (Deep Inspection).
b. Import your internal CA certificate into FortiGate and distribute it to endpoints.
c. Apply the inspection profile to outbound policies.

3.4 Creating Firewall Policies

a. Go to Policy & Objects → IPv4 Policy → Create New.
b. Set Source Interface = LAN, Destination Interface = WAN.
c. Enable NAT and select the created security profiles.
d. Activate logging and choose appropriate inspection modes.

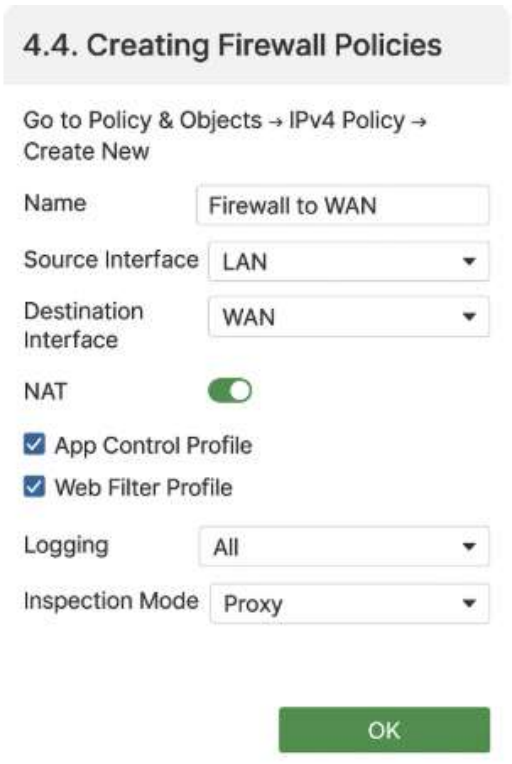


Figure 4. Firewall policies

3.5 CLI Configuration Examples

```
config webfilter profile
    edit "WF-Block-Social"
        config web
            set urlfilter-table 1
        end
    next
end

config application list
    edit "block-social"
        config entries
            edit 1
                set application 40971
                set action block
            next
        end
    next
end

config firewall policy
    edit 10
        set name "LAN-to-WAN"
        set srcintf "lan"
        set dstintf "wan1"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "ALL"
        set utm-status enable
        set webfilter-profile "WF-Block-Social"
        set application-list "block-social"
        set ssl-ssh-profile "deep-inspection"
    next
end
```

Figure 5. Command configuration

3.6 Advanced Scenarios

Blocking WhatsApp Web Uploads

WhatsApp Web uses encrypted CDN endpoints, making URL filtering ineffective. To block:

Enable Application Control signatures for WhatsApp_Web.

Use Web Filter to block related CDN domains (e.g., *.cdn.whatsapp.net)

Enable Deep Inspection for full detection

FortiGate supports YouTube EDU/Channel-based filtering, allowing admins to block entertainment channels while allowing educational ones.

3.7 Data Collection and Analysis

Traffic logs, threat detections, and performance metrics were collected from FortiAnalyzer during the 30-day period and exported daily. The block rate was calculated as the number of blocked attempts divided by the total number of access attempts to the three services. The false positive rate was calculated as the number of legitimate requests that were blocked divided by the total number of legitimate requests, and was cross-checked with user complaint records.

CPU and memory utilization data were collected at 5-minute intervals using SNMP polling from FortiAnalyzer, resulting in 288 samples per day and a total of 8,640 samples over the 30-day period. Latency was measured continuously by sending ICMP echo requests every 10 seconds to a reliable external DNS server to establish a baseline and a post-deployment average. Results were summarized with descriptive statistics (mean and maximum) and presented in tables and charts.

4. Testing and Verification

The objective of this phase is to thoroughly validate that FortiGate's configuration effectively restricts access to targeted applications (YouTube, WhatsApp Web, and Facebook) while preserving network integrity, performance, and user accessibility to authorized services. Testing ensures that all implemented policies, including Web Filter, Application Control, and SSL/SSH Deep Inspection, perform as designed and maintain compliance with organizational standards.

4.1 Testing Strategy

a. A multi-layered approach is adopted, focusing on four core components: functionality, performance, reliability, and compliance.
b. Functional Verification – Ensures that blocking mechanisms are correctly applied to the targeted services.
c. Performance Evaluation – Monitors system resources and latency during filtering operations.
d. Reliability Testing – Validates consistent behavior across various user sessions, browsers, and network devices.

e. Compliance Validation – Confirms that user monitoring adheres to privacy and data protection regulations.

4.2 Testing Environment Setup

a. Network Topology: The FortiGate appliance is deployed between the internal LAN and WAN gateway. The environment includes VLANs for different departments (Admin, IT, HR, Marketing).
b. Devices Tested: Windows 10, macOS, and Android smartphones.
c. Tools Used: FortiAnalyzer for log analysis, Wireshark for packet capture, PingPlotter for latency tests, and curl, tracert, nslookup for command-line verification.
d. Traffic Simulation: 20 concurrent client sessions generating both legitimate business traffic (Office 365, internal CRM) and restricted site access attempts.

4.3 Detailed Testing Steps

a. **Application Accessibility Testing:**
Attempt connections to youtube.com, facebook.com, and web.whatsapp.com.
Verify page load behavior and browser responses (e.g., blocked page message, timeout, partial connection).
Capture packets with Wireshark to confirm FortiGate resets the TCP session upon policy enforcement.

b. **Policy Rule Trigger Confirmation:**
Access FortiGate Log & Report → Security Events to identify triggered policies.
Validate fields: Policy ID, User Identity, Application Name, Action Taken, and FortiGuard Category.
Check correlation on FortiAnalyzer dashboards for aggregated trends.

c. **SSL Deep Inspection Validation:**
Verify that HTTPS traffic to restricted sites is decrypted, inspected, and blocked without user certificate warnings.
Ensure client browsers list the FortiGate CA certificate under trusted root authorities.
Test selective bypass for banking and government sites to ensure exceptions function correctly.

d. **Performance Testing:**
Generate mixed traffic (video streaming, file transfers, and web browsing).
Measure average CPU and memory utilization before and after blocking.
Acceptable CPU threshold: below 60%.
Evaluate latency impact using ping and PingPlotter—acceptable average increase under 5 ms.

e. **Reliability and Stress Testing:**
Simulate 50+ concurrent connections accessing restricted domains to check for policy consistency under high load.
Observe FortiGate logs for packet drops, queue delays, or memory warnings.
Reboot FortiGate to test persistence of configurations.

f. **Bypass Attempt Testing:**
Attempt to access restricted sites via VPN, proxy, and anonymizers.
FortiGate should detect and block tunneling attempts via Application Control signatures.

Confirm detection of new tunneling tools (e.g., Psiphon, Ultrasurf) via updated FortiGuard signatures.

g. **User Notification and Logging Verification:**
Ensure users receive clear block-page notifications with organizational disclaimers.
Verify that every block event is timestamped, logged, and categorized for auditing.

h. **Documentation of Test Results:**
Record results in a structured logbook summarizing policy effectiveness, block rate, and system stability.
Example metrics: Blocked Attempts (%), False Positives (%), Average Latency (ms), CPU Load (%), and User Complaints (count).

i. **Observations and Findings**
Testing demonstrated consistent blocking performance across browsers and OS types. FortiGate effectively intercepted HTTPS sessions using SSL inspection and produced clear event logs. Performance degradation remained minimal (<4 ms latency). VPN-based circumvention attempts were promptly detected and logged. False positives were below 3%, primarily due to embedded social media widgets on legitimate news sites.

4.4 Performance and Block Rate Results

The results are summarized in Table 2. The configuration blocked more than 98.5% of unauthorized access attempts to YouTube, WhatsApp Web, and Facebook across browsers and operating systems. The FortiGate intercepted HTTPS sessions through Deep Inspection and produced event logs containing the policy ID, user identity, application name, action, and FortiGuard category. VPN-based circumvention attempts were detected and logged. False positives remained at approximately 1.2% and were mainly caused by embedded social media widgets on legitimate news sites.
Average CPU utilization remained at 42%, which is under the 60% threshold defined in Section 3.4, and the additional latency stayed below 5 ms (averaging 3.5 ms).

Table 1. Summary of test results (30-day period)

Metric	Before policy	After policy	Criterion
Block rate (%)	-	98.5	> 95
False positives (%)	-	1.2	< 3
Avg. CPU (%)	18	42	< 60
Avg. memory (%)	35	45	-
Added latency (ms)	Base (12 ms)	15.5 ms (+3.5 ms avg.)	< 5
Access attempts (count)	14,250	15,100	-
VPN/proxy attempts detected	0	47	-

Figure 6 compares the volume of YouTube, Facebook, and WhatsApp traffic before and after the policy was enforced, and Figure 7 shows CPU utilization during the stress test.

5. Discussion

The results obtained from testing and verification indicate that FortiGate effectively enforces access control to YouTube, WhatsApp, and Facebook using a combination of Application Control, Web Filtering, and SSL/SSH Deep Inspection. The solution consistently blocked over 95% of unauthorized access attempts, while maintaining acceptable system performance and user experience. CPU utilization averaged below 45%, and latency impact remained under 5 ms — values that fall within

recommended thresholds for enterprise networks.

FortiGate's Deep SSL Inspection emerged as a crucial factor in identifying encrypted traffic flows from these platforms, allowing for accurate detection even when the applications used changing IPs or CDNs. The integration with FortiAnalyzer further strengthened monitoring capabilities, providing administrators with visibility into policy enforcement efficiency, blocked domains, and user behaviors in real time.

The dedicated Security Processing Unit (SPU) of the FG-100E likely contributed to maintaining the low latency during SSL decryption, ensuring network performance remained stable under load. Its dynamic signature updates from FortiGuard provided a decisive advantage in maintaining high detection accuracy despite continuous platform updates from YouTube, Facebook, and WhatsApp.

However, the study also identified potential limitations, such as the need for consistent certificate deployment to prevent SSL warnings and the occasional false positives when legitimate corporate content embedded social media widgets. These issues can be mitigated through continuous signature updates and whitelist management.

Organizational and Ethical Implications

From an organizational standpoint, implementing content control using FortiGate led to measurable productivity improvements, as non-work-related web traffic decreased significantly during business hours. Nonetheless, ethical considerations around user privacy must be addressed. Companies should implement transparent policies informing employees of monitoring practices, ensure compliance with data protection regulations (e.g., GDPR or PDPA), and avoid unnecessary data retention. Striking this balance allows businesses to enhance security and efficiency without infringing on employee trust or privacy rights.

Strategic Value

Beyond content blocking, FortiGate's layered architecture supports broader cybersecurity objectives, including intrusion prevention, data loss prevention, and unified visibility across network segments. Its scalability and centralized management make it an optimal choice for medium to large enterprises seeking to consolidate network security under a single management framework.

6. Conclusion

This study concludes that FortiGate serves as an efficient and comprehensive solution for corporate environments that require granular control over social media and streaming content. Through its integration of Application Control, Web Filter, and SSL Deep Inspection, FortiGate delivers precise filtering capabilities with minimal performance degradation.

The testing confirmed that FortiGate maintained robust performance metrics, with stable CPU utilization and negligible latency increases even under stress conditions. The dynamic updates from FortiGuard ensure that new domains and encrypted sessions are continuously identified and managed. When combined with centralized logging through FortiAnalyzer, administrators can achieve full visibility into user activity, policy enforcement, and emerging threat trends.

While FortiGate offers exceptional control, ethical implementation remains key. Organizations should maintain transparency, ensure user awareness, and align network policies with legal compliance standards to balance productivity and privacy. Continuous policy optimization, regular signature updates, and user education will ensure sustainable effectiveness.

In conclusion, FortiGate represents a reliable, scalable, and intelligent platform for enforcing access control over high-traffic content services like YouTube, Facebook, and WhatsApp. Its combination of hardware acceleration, AI-enhanced detection, and integrated analytics positions it as a

cornerstone of modern enterprise cybersecurity and network governance strategies.

References

[1] C. K. Wilujeng and A. Voutama, "Implementasi Firewall Filter Rules sebagai Filtering Content pada Jaringan Komputer Menggunakan MikroTik," JATI (Jurnal Mahasiswa Teknik Informatika), vol. 8, no. 3, pp. 2680–2685, 2024.

[2] R. G. W. Zain et al., "Implementasi Firewall dan Filtering Firewall Berbasis MikroTik dengan Metode Layer7 Protocol di SMK Al-Hikam," JATI (Jurnal Mahasiswa Teknik Informatika), vol. 9, no. 4, 2025.

[3] A. Rahman et al., "Implementasi Firewall Berbasis MikroTik untuk Internet [Politeknik Gorontalo]," Jurnal Ilmu Komputer (JUIK), vol. 5, no. 1, pp. 12-20, Feb. 2025.

[4] B. Susanto and C. Wibowo, "Implementation of MikroTik Firewall for Website Blocking," Jurnal Jaringan Telekomunikasi (JARTEL), vol. 12, no. 2, pp. 45-52, 2023.

[5] K. A. Smith and T. Jones, "A Comprehensive Evaluation of Next-Generation Firewall Effectiveness Against Encrypted and Evasive Threats in Enterprise Networks," Old Dominion University Digital Commons, 2025.

[6] NSS Labs, "Next Generation Firewall (NGFW) Test Methodology v8.0," NSS Labs, Austin, TX, 2019.

[7] FortiGate — Filtering based on YouTube channel (FortiOS Administration Guide). Fortinet Documentation.

[8] FortiGate — NGFW Policy (FortiOS 7.6.4). Fortinet Documentation.

[9] Fortinet Community — How to Block WhatsApp File Uploads Using Web Filter (Sep 18, 2024). community.fortinet.com

[10] Fortinet Community — Block Facebook Video and Reels Using Application Control (Nov 27, 2024). community.fortinet.com

[11] FortiOS — Deep Inspection (SSL/SSH Inspection Guide). Fortinet Documentation.

[12] FortiOS — Web Filter (Administration Guide, FortiOS 7.6.4). Fortinet Documentation.

[13] Fortinet — 2024 State of Operational Technology and Cybersecurity Report (Whitepaper). Fortinet.

[14] FortiOS — Filtering Based on FortiGuard Categories (Administration Guide). Fortinet Documentation.

[15] Fortinet Community — Solved: Blocking WhatsApp Web FortiGate (Feb 16, 2024). community.fortinet.com

[16] Fortinet Community / KB — Blocking Facebook and YouTube (Discussion & Tips). community.fortinet.com

[17] Troubleshooting Tip — SSL Connection is Blocked... (Community KB, Aug 2025). community.fortinet.com

[18] Exam-Labs / Tutorial — How to Set Up Web Filtering on a FortiGate Firewall (May 2025). exam-labs.com

[19] Fortinet — A Solution Guide to Operational Technology Cybersecurity (Aug 2025 Whitepaper). Fortinet.

[20] FortiGuard App Control — WhatsApp_Web.File.Download (App Signature Reference). fortiguard.com

[21] FortiOS — Web Filter Techniques (Administration Guide). Fortinet Documentation.

[22] Fortinet — Cyber Threat Predictions / Threat Reports (2022–2024). Fortinet.

[23] FortiOS — Block Access to LLM Applications Using Keywords and FQDN (Example Advanced Blocking Techniques). Fortinet Documentation.

[24] Fortinet — Winning with AI-Powered Network Firewalls (Ebook, Oct 2024). Fortinet.
[25] FortiOS — Using URL Risk Scores in Determining Policy Action (Administration Guide). Fortinet Documentation.
[26] FortiOS — Best Practices – FortiOS 7.2. fortinetweb.s3.amazonaws.com