happinetz CAMPUS

AI Powered Internet Filtering

Why DNS Enforcement is Recommended - firewall

DNS enforcement is implemented to ensure that all users within the VLAN utilize the organization's approved DNS service for domain resolution. This guarantees that web filtering, content control, and security policies are consistently applied and cannot be bypassed through manual DNS changes or encrypted DNS protocols.

Without DNS enforcement, users may configure external DNS servers (e.g., public resolvers) to circumvent content filtering controls. Enforcing DNS at the firewall level prevents such bypass attempts by redirecting or blocking unauthorized DNS traffic.

This approach strengthens:

- Content filtering compliance
- Protection against malicious domains
- Prevention of policy circumvention
- Overall network security posture

DNS enforcement ensures:

- All devices use approved DNS servers only
- External DNS bypass attempts are blocked
- DNS over TLS (853) is blocked
- DNS over QUIC (UDP 443) is restricted
- Filtering policies cannot be bypassed using public resolvers

Without enforcement, users can bypass filtering using:

- 8.8.8.8
- 1.1.1.1
- DoT
- QUIC
- Manual DNS override

DNS enforcement is therefore a critical control in maintaining a secure and policy-compliant school network environment.

⚠ *DNS Redirect Capability Warning*

Note: - Interface names, menu paths, and terminology may vary depending on firmware version and model. Consult vendor documentation where required.

Internet will stop working: - Note - Never block TCP 443, or Service: HTTPS (443)

ENFORCEMENT LOGIC (Same for All Firewalls)

Order must be:

1️⃣DNS NAT Redirect (Port 53 → Happinetz DNS)
2️⃣Block DNS (53) to destinations other than HAPPINETZ_DNS
3️⃣Block UDP/TCP (853)
4️⃣Block UDP 443 (Optional but Recommended)
5️⃣Keep TCP 443 OPEN

Below steps show only for 1 group - you can repeat the same for other groups as well.

1.SOPHOS (XG / Sophos Firewall OS)

PART 1 — DNS Redirect Rule

Go to:
Rules & Policies → NAT Rules → Add NAT Rule

Create:

- Rule Type: DNAT
- Original Source: LAN
- Original Destination: Any
- Service: DNS (TCP + UDP 53)
- Translated Destination: HAPPINETZ_DNS_IP
- Translated Service: DNS
- Outbound Interface: WAN

⚠️ Place this rule ABOVE all general LAN→WAN NAT rules.

Save.

PART 2 — Block External DNS

Go to:
Rules & Policies → Firewall Rules → Add Rule

Create rule:

- Source: LAN
- Destination: Any
- Service: DNS
- Destination NOT is not HAPPINETZ_DNS_IP
- Action: Drop

Place BELOW the NAT redirect rule.

PART 3 — Block DoT

Add rule:

- Service: TCP 853 + UDP 853
- Action: Drop

PART 4 — Block QUIC

Create rule:

- Service: UDP 443
- Action: Drop

⚠️ DO NOT block TCP 443.

2.FORTINET (FortiGate)

PART 1 — DNS Redirect (VIP + Policy)

Go to:
Policy & Objects → Virtual IPs → Create New

- Type: Static NAT
- External Interface: LAN
- External IP: 0.0.0.0/0
- Mapped IP: HAPPINETZ_DNS_IP

- Port Forwarding: Enable
- Protocol: TCP/UDP
- External Port: 53
- Map to Port: 53

Save.

In some FortiGate models, DNS redirect may be configured using Central NAT instead of VIP. Follow model-specific guidance if VIP method does not apply. If VIP does not allow 0.0.0.0/0 as External IP, configure DNS redirect using Central NAT with destination port 53 instead.

Now create Firewall Policy:

Policy & Objects → Firewall Policy → Create New

- Incoming Interface: LAN
- Outgoing Interface: WAN
- Source: LAN subnet
- Destination: VIP created
- Service: DNS
- Action: Accept

Place ABOVE general LAN→WAN rule.

PART 2 — Block External DNS

Create deny rule:

- Service: DNS
- Action: Deny
- Place below NAT policy

Block only if:

Destination is not - HAPPINETZ_DNS_IP

PART 3 — Block DoT

Service: TCP 853 + UDP 853
Action: Deny

PART 4 — Block QUIC

Service: UDP 443
Action: Deny

⚠️ Keep TCP 443 allowed.

3.SONICWALL

PART 1 — DNS Redirect

Go to:
Network → NAT Policies → Add

- Original Source: LAN
- Original Destination: Any
- Original Service: DNS
- Translated Destination: HAPPINETZ_DNS
- Translated Service: Original

Move rule to top.

PART 2 — Access Rules

Go to:
Firewall → Access Rules → LAN to WAN

Add:

Rule 1:

- Service: DNS
- Action: Deny

Rule 2:

- Service: TCP/UDP 853
- Action: Deny

Rule 3:

- Service: UDP 443
- Action: Deny

Do NOT deny TCP 443.

4.CISCO FIREPOWER / ASA

PART 1 — DNS NAT

Configure DNAT:

- Source: Inside
- Destination: Any
- Service: DNS
- Translate to: HAPPINETZ_DNS

Ensure rule order is before generic PAT.

PART 2 — Access Control Policy

Block:

- TCP/UDP 53 outbound (Destination NOT equal HAPPINETZ_DNS)
- TCP/UDP 853
- UDP 443

Keep TCP 443 allowed.

Deploy policy.

---

5. PALO ALTO

PART 1 — NAT Policy

Go to:
Policies → NAT → Add

- Source Zone: LAN
- Destination Zone: WAN
- Service: service-53
- Destination Translation: HAPPINETZ_DNS

Move rule to top.

PART 2 — Security Policy

Add Deny Rules:

Application: dns
Service: application-default
Destination: NOT HAPPINETZ_DNS
Action: Deny

2️⃣Service: tcp-853
3️⃣Service: udp-853
4️⃣Service: udp-443

Place deny rules above general allow rule.

Commit.

🔒 IMPORTANT DISCLAIMERS

⚠️ Important Notes

1. NAT redirect rule must be placed ABOVE general outbound rule.
2. Do NOT block TCP 443 in any case.
3. If SSL inspection is enabled, ensure it does not interfere with DNS enforcement.
4. App Control-based DoH blocking (optional advanced step) can be configured separately.

DNS enforcement prevents most bypass techniques. However, advanced tunneling methods (VPN, Tor, encrypted DNS over HTTPS inside TLS inspection bypass) require additional firewall policies and should be addressed separately.