happinetz CAMPUS
AI Powered Internet Filtering

Happinetz Campus – VLAN-Based Policy Segmentation Guide in your router/Firewall

---

1 Purpose

Happinetz campus applies a single DNS filtering policy to the entire campus network based on the registered public IP.

However, many schools use VLAN segmentation to separate:

- Student network
- Staff network/ Admin network / Servers
- CCTV / IoT devices
- Guest WiFi

This document explains how to control where Happinetz filtering applies using VLAN configuration at the router or firewall level.

---

2 Why VLAN-Based Control Is Needed

Without VLAN control:

- All devices inside the campus are filtered equally.
- Admin systems may be unnecessarily restricted.
- Guest WiFi may need different control.

With VLAN control:

- Filtering can apply only to Student VLAN.
- Admin VLAN can bypass filtering (if required).

- Guest networks can have separate control.

Important:

Happinetz campus still uses a single public IP.
Segmentation is controlled at network level, not dashboard level.

---

3 How VLAN-Based Filtering Works (Technical Logic)

Happinetz filtering applies when:

- Device DNS request goes to Happinetz DNS IP
- DNS traffic is redirected and enforced

Therefore:

To apply filtering to a VLAN →
Configure that particular VLAN's DHCP DNS to use Happinetz DNS + enable DNS enforcement.

To exclude a VLAN →
Use alternate DNS + do not apply DNS enforcement rules.

So VLAN control is achieved by:

- DHCP DNS assignment per VLAN
- Firewall/NAT enforcement per VLAN

---

4 Recommended VLAN Architecture (you can choose what you want)

Example VLAN Structure:

VLAN	**Purpose**	**Filtering**
VLAN 10	Students	✅ Enabled
VLAN 30	Admin/Staff	❌ Disabled
VLAN 40	Servers	❌ Disabled
VLAN 50	Guest	Optional

In the above scenario, filtering will apply to Student VLAN only.

---

5 Configuration Logic – Router / Firewall

This section remains vendor-neutral. Check your router or firewall to check the feature.

STEP 1 – Configure VLAN Interfaces

In router/firewall:

Create VLAN interfaces:

- VLAN 10 ⟶ 192.168.10.1/24
- VLAN 20 ⟶ 192.168.20.1/24
- VLAN 30 ⟶ 192.168.30.1/24

Ensure inter-VLAN routing is properly configured.

STEP 2 – DHCP DNS Configuration Per VLAN

For VLANs where filtering is required:

DHCP Settings ⟶ VLAN 10
DNS Server = HAPPINETZ_DNS_IP (both primary and secondary DNS IP)

For VLANs where filtering is NOT required:

DHCP Settings ⟶ VLAN 30
DNS Server = ISP DNS / Internal DNS (example – google – 8.8.8.8 or 1.1.1.1)

This determines who uses filtering.

STEP 3 – DNS Enforcement Rule Scope

Modify DNS enforcement rule to apply only to selected VLANs.

Instead of:

Source: LAN (All)

Use:

Source: VLAN 10 subnet (Students only)

So enforcement rule becomes:

- Source: 192.168.10.0/24
- Redirect Port 53 → Happinetz DNS

For excluded VLANs:

Do NOT apply the redirect rule.

STEP 4 – Block External DNS Per VLAN

For filtered VLAN:

Block:

- TCP/UDP 53 outbound rule
- TCP/UDP 853 block
- UDP 443 block only (not TCP 443)

For excluded VLAN:

Allow normal internet access.

6Important Design Considerations

1 Public IP Binding Remains Same

All VLANs share the same public IP.

Filtering is controlled by:

- Whether their DNS traffic is redirected to Happinetz.
- If that particular VLAN has DNS traffic redirected to Happientz DNS, filtering will happen, if its not directed to happientz DNS, filtering will not happen.

---

2 NAT Rule Order Still Critical

DNS redirect rule must:

- Be above general outbound rule
- Be scoped only to selected VLAN

---

3 Multi-WAN Schools

Ensure filtered VLAN DNS exits from registered public IP.

4Avoid Mixed DNS Environment

Do NOT:

- Give student VLAN internal DNS that forwards to external DNS
- Mix enforcement and non-enforcement rules incorrectly

Keep it clean and segmented.

---

7 When VLAN-Based Filtering Is Recommended

Recommended if:

- School has proper firewall
- Separate student and admin networks
- IT staff available to manage VLANs
- Network already segmented

Not recommended if:

- Flat network
- Basic router only
- No VLAN awareness

---

8 Operational Example

Goal:

Filter only Students.

Implementation:

- VLAN 10 (Students) ⟶ DHCP DNS = Happinetz
- VLAN 10 ⟶ DNS redirect rule applied
- VLAN 30 (Admin) ⟶ ISP DNS
- VLAN 30 ⟶ No redirect rule

Result:

Students filtered
Admin/Staff not filtered
Same public IP
Same dashboard policy

🔐 Final Note

VLAN-based deployment allows controlled filtering without changing the Happinetz dashboard architecture. It is a network-level segmentation approach, not a policy segmentation approach.