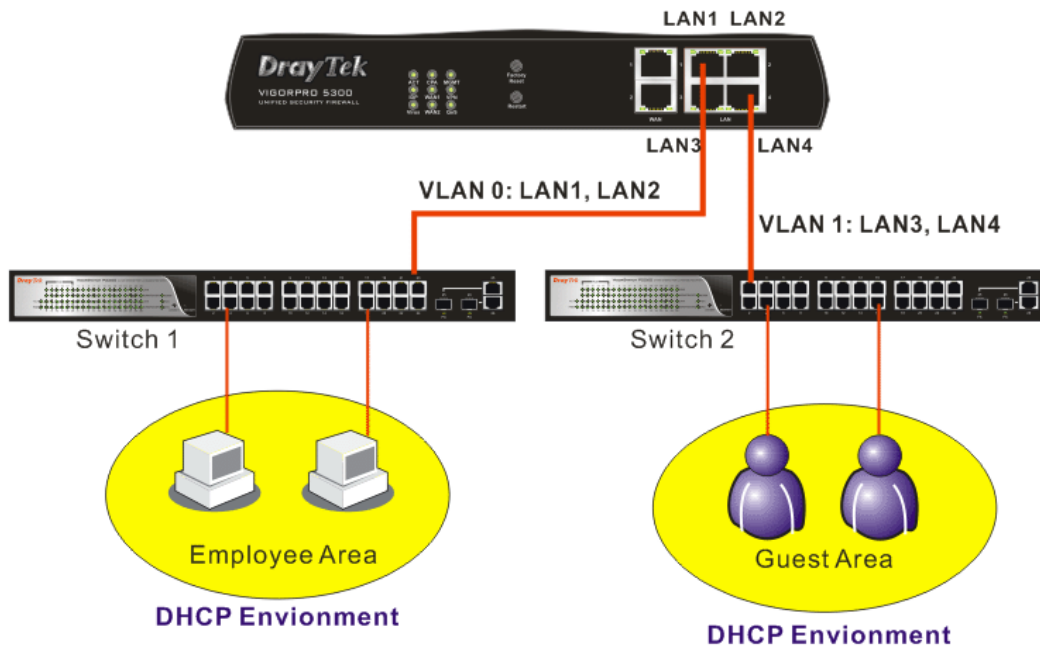


VLAN in Firewall Policy

VLAN in Firewall Policy is a new feature introduced since version 3.3.5 for VigorPro series. With this feature, when LAN VLAN feature is enabled, the firewall rules will check if the packets are received from specified VLAN. Since the VLAN function supported in VigorPro series and Port-based VLAN supported in Vigor 2xxx series, the **VLAN in Firewall Policy** function can achieve the function that specific traffics are restricted to specific switch ports.

This feature is very helpful in DHCP environment for which the source IP addresses can hardly be used to define a firewall policy. Take the following example for explanation:



Suppose there are two areas in your office: **Employee Area** and **Guest Area**. The computers in the Employee Area can access the Internet and the VPN. They are connected to switch 1 which is connected to the LAN 1 port on the router. Guests can access the Internet but not the VPN. They are restricted to connect to switch 2 that connected to LAN 4 port on the router. These two areas are isolated. The guests and the employees are not allowed to access each other. Therefore, **VLAN** is enabled and configured as the following:.

LAN >> VLAN Configuration

VLAN Configuration

<input checked="" type="checkbox"/> Enable				
	P1	P2	P3	P4
VLAN0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VLAN2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VLAN3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

OK Clear Cancel

All the hosts get their IP addresses via DHCP server. Without **VLAN in Firewall Policy** function, you have to define Source IP addresses as match condition. If all the IP addresses are dynamic, it is impossible to create firewall rules because there is no way to distinguish between the employees and the guests. Therefore, you have to open **LAN>> Bind IP to MAC** to assign static IP addresses to employees via DHCP, which is administratively burdensome.

With **VLAN in Firewall Policy** function, you can simply define the firewall rules as follows:

Firewall >> Filter Setup >> Edit Filter Set

Filter Set 2
 Comments : Default Data Filter

Filter Rule	Active	Comments	Move Up	Move Down
1	<input checked="" type="checkbox"/>	Block NetBios		<u>Down</u>
2	<input type="checkbox"/>	block all	<u>UP</u>	<u>Down</u>
3	<input type="checkbox"/>	pass employee	<u>UP</u>	<u>Down</u>
4	<input type="checkbox"/>	pass guest	<u>UP</u>	<u>Down</u>
5	<input type="checkbox"/>		<u>UP</u>	<u>Down</u>
6	<input type="checkbox"/>		<u>UP</u>	<u>Down</u>
7	<input type="checkbox"/>		<u>UP</u>	

Next Filter Set: None

OK Clear Cancel

Any traffic that doesn't match rule 3 and rule 4 will match rule 2 "block all" and will be blocked. Keep the Source IP, Destination IP and VLAN option with default settings that imply "any traffic". The action is "**Block If No Further Match**", indicating that a packet will be dropped by this rule only if this packet doesn't match any other rule. Below shows filter rule 2- block all.

Filter Set 2 Rule 2

Check to enable the Filter Rule

Comments: block all

Index(1-15) in Schedule Setup: , , ,

Direction: LAN -> WAN

Source IP: Any

Destination IP: Any

Service Type: Any

Fragments: Don't Care

VLAN: Don't Care

Application **Action/Profile** **Syslog**

Filter: Block If No Further Match

Branch to Other Filter Set: None

Sessions Control: 0 / 8000

MAC Bind IP: Non-Strict

In the rule of pass employee, the VLAN option is set with VLAN 0. Source IP and Destination IP is set with the default value, **Any**. The action is set with **Pass Immediately** which implies that any traffic received from LAN 1 port or LAN 2 port will be passed immediately if matches this rule. Note that LAN 1 port and LAN 2 port are grouped in VLAN 0. If a packet arrives at the router from LAN 3 port or LAN 4 port, it doesn't match this rule because LAN 3 port and LAN 4 port belong to VLAN 1. Below shows filter rule 2- pass employee.

Filter Set 2 Rule 3

Check to enable the Filter Rule

Comments:

Index(1-15) in Schedule Setup: , , ,

Direction:

Source IP:

Destination IP:

Service Type:

Fragments:

VLAN:

Application	Action/Profile	Syslog
Filter:	<input type="text" value="Pass Immediately"/>	<input type="checkbox"/>
Branch to Other Filter Set:	<input type="text" value="None"/>	
Sessions Control	<input type="text" value="0 / 8000"/>	<input type="checkbox"/>
MAC Bind IP	<input type="text" value="Non-Strict"/>	<input type="checkbox"/>

In the rule of pass guest, the VLAN option is set with VLAN 1. Source IP is the set with default value, **Any**. The Destination IP is set with **!(172.16.2.0/255.255.255.0)**. 172.16.2.0/255.255.255.0 indicates the remote VPN network. Please note that the **Inverse Selection** is enabled for this VPN network, which indicates that the destination address is any IP address outside the range 172.16.2.0 ~ 172.16.2.255. Such configuration implies that any traffic received from LAN 3 or LAN 4 port towards the Internet (VPN not included) will be passed immediately if matches this rule.

If a packet (destination is the VPN network) arrives at the router from LAN 3 or LAN 4 port, it doesn't match this rule. Since this is the last rule, the packet is determined to match rule 2 "block all" and will be dropped.

Filter Set 2 Rule 4		IP Address Edit	
<input checked="" type="checkbox"/> Check to enable the Filter Rule		Address Type	Subnet Address
Comments:	pass guest	Start IP Address	172.16.2.0
Index(1-15) in <u>Schedule</u> Setup:		End IP Address	0.0.0.0
Direction:	LAN -> WAN	Subnet Mask	255.255.255.0
Source IP:	Any	<input checked="" type="checkbox"/> Invert Selection	
	Edit	IP Group	None
Destination IP:	!(172.16.2.0/255.255.255.0)	or IP Object	None
	Edit	or IP Object	None
Service Type:	Any	or IP Object	None
	Edit		
Fragments:	Don't Care		
VLAN:	VLAN 1		
Application	Action/Profile	Syslog	
Filter:	Pass Immediately	<input type="checkbox"/>	
Branch to Other Filter Set:	None	<input type="checkbox"/>	
Sessions Control	38 / 8000	<input type="checkbox"/>	
MAC Bind IP	Non-Strict	<input type="checkbox"/>	