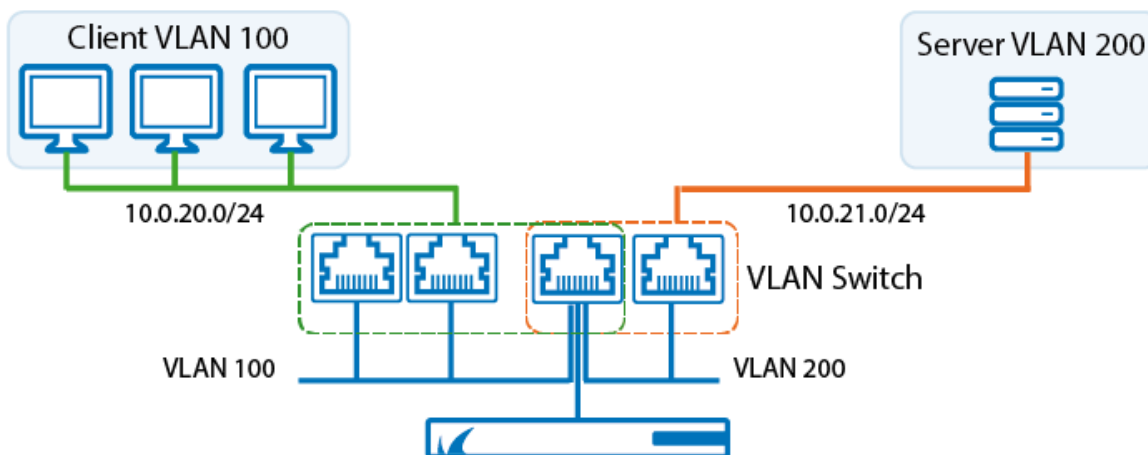


How to Configure VLANs

<https://campus.barracuda.com/doc/72516349/>

VLANs allow you to split one physical network interface into several virtual LANs. The physical interface behaves like several interfaces, and the switch behaves like multiple switches. VLANs allow for layer 2 separation whenever layer 1 separation is not possible. The firewall can use up to 256 VLANs on one physical network interface and a maximum of 4094 VLANs globally. The VLAN interfaces are named **physical interface.VLAN id** (e.g., **eth2.200**). Only tagged traffic is handled by the firewall; untagged traffic sent directly to the physical interface is discarded. You must use a properly configured 802.1q VLAN-capable switch and NICs that use drivers capable of tagging VLAN traffic.

The interface label is formatted as **interface-name.VLAN ID:Virtual Server Name**. Verify that the length of the label does not exceed 15 characters. E.g., **port10.1111:S01** would be a valid 15-character interface label.




Step 1. Add Two VLAN Interfaces

1. Go to **NETWORK > IP Configuration**.
2. In the **Virtual Interface Configuration** section, add the first entry for the VLAN:
 - **VLAN Name** - Enter the name for the VLAN.
 - **Host Interface** - Select the hardware interface.
 - **VLAN ID** - Enter the VLAN ID for differentiating between multiple VLANs.
3. Click **Add**.

VIRTUAL INTERFACE CONFIGURATION				Help
VLAN Name	Host Interface	VLAN ID	MTU	
vlan1	eth2	100	1500	Add


- In the **Virtual Interface Configuration** section, add the second entry for the VLAN.
 - VLAN Name** - Enter the name for the VLAN.
 - Host Interface** - Select the hardware interface.
 - VLAN ID** - Enter the VLAN ID for differentiating between multiple VLANs.
- Click **Add**.

VIRTUAL INTERFACE CONFIGURATION				Help
VLAN Name	Host Interface	VLAN ID	MTU	
vlan2	eth2	200	1500	Add
vlan1	eth2	100	1500	

Step 3. Perform a Network Activation

After you create or change basic network configurations such as routing, you must activate your new network configurations.

- Scroll to the top of the page.
- Click on the link inside of the warning message to execute the new network configuration.

 Some configuration changes made within IP Configuration, Routing or Bridging are not yet in effect. To execute the changes, [click here](#). This will cause a temporary interruption in network traffic. You may have to log into the Barracuda NextGen Firewall again.

Step 4. Create a Static Network Interface for the First VLAN

- Go to **NETWORK > IP Configuration**.
- In the **Static Interface Configuration** section, click **Add Static Network Interface**. The **Add Static Interface** window opens.
- From the **Network Interface** list, select the first VLAN port, e.g., eth2.100.
- Enter a **Name** for the first VLAN network interface, e.g., v1anprv1.
- Enter the static WAN **IP address**, e.g., 10.0.20.1.
- Enter the **Netmask** of the interface, e.g., 255.255.255.0.
- From **Services to Allow**, select **Ping** to allow the interface to respond to ping packets.
- From the **Classification** list, select **Trusted**.

Add Static Network Interface ?

Network Interface:

Name:
Maximum 8 characters, no spaces allowed.

IP Address:

Netmask:

Services to Allow: Ping VPN Server SSL VPN
Enable/Disable 'reply to ping' or NTP requests. To be able to enable SSLVPN, you need to select a certificate under VPN > SSLVPN > Server Settings.

Classification:
How this interface is classified within your network. For ISP links, select WAN.

Gateway:
Optional gateway for this interface. Creates a default gateway route (0.0.0.0/0) automatically.

Metric:
Must be unique across all interfaces. The interface with the lowest value is used for outgoing traffic.

Secondary IP Addresses:

IP Addresses	Ping	Barracuda	VPN Server	SSL VPN
<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Other static IP addresses on the same subnet. To be able to enable SSLVPN you need to select a certificate under VPN > SSLVPN > Server Settings.

9. Click **Save**.

Step 5. Create a Static Network Interface for the Second VLAN

1. Go to **NETWORK > IP Configuration**.
2. In the **Static Interface Configuration** section, click **Add Static Network Interface**. The **Add Static Interface** window opens.
3. From the **Network Interface** list, select the first VLAN port, e.g., eth2.200.
4. Enter a **Name** for the first VLAN network interface, e.g., vlanprv2.
5. Enter the static WAN **IP address**, e.g., 10.0.21.1.
6. Enter the **Netmask** of the interface, e.g., 255.255.255.0.
7. From **Services to Allow**, select **Ping** to allow the interface to respond to ping packets.
8. From the **Classification** list, select **Trusted**.

Add Static Network Interface ?


Network Interface:	<input type="text" value="eth2.200"/>																																
Name:	<input type="text" value="vlanprv2"/> <small>Maximum 8 characters, no spaces allowed.</small>																																
IP Address:	<input type="text" value="10.0.21.1"/>																																
Netmask:	<input type="text" value="255.255.255.0 (/24)"/>																																
Services to Allow:	<input checked="" type="checkbox"/> Ping <input type="checkbox"/> VPN Server <input type="checkbox"/> SSL VPN <small>Enable/Disable 'reply to ping' or NTP requests. To be able to enable SSLVPN, you need to select a certificate under VPN > SSLVPN > Server Settings.</small>																																
Classification:	<input type="text" value="Trusted"/> <small>How this interface is classified within your network. For ISP links, select WAN.</small>																																
Gateway:	<input type="text"/> <small>Optional gateway for this interface. Creates a default gateway route (0.0.0.0/0) automatically.</small>																																
Metric:	<input type="text" value="1"/> <small>Must be unique across all interfaces. The interface with the lowest value is used for outgoing traffic.</small>																																
Secondary IP Addresses:	<table><tr><td>IP Addresses</td><td>Ping</td><td>Barracuda</td><td>VPN Server</td><td>SSL VPN</td></tr><tr><td></td><td>NextGen</td><td></td><td></td><td></td></tr><tr><td></td><td>Firewall</td><td></td><td></td><td></td></tr><tr><td></td><td>F-Series</td><td></td><td></td><td></td></tr><tr><td><input type="text"/></td><td><input type="checkbox"/></td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="checkbox"/></td><td><input type="button" value="+"/></td></tr><tr><td colspan="6"><small>Other static IP addresses on the same subnet. To be able to enable SSLVPN you need to select a certificate under VPN > SSLVPN > Server Settings.</small></td></tr></table>	IP Addresses	Ping	Barracuda	VPN Server	SSL VPN		NextGen					Firewall					F-Series				<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="+"/>	<small>Other static IP addresses on the same subnet. To be able to enable SSLVPN you need to select a certificate under VPN > SSLVPN > Server Settings.</small>					
IP Addresses	Ping	Barracuda	VPN Server	SSL VPN																													
	NextGen																																
	Firewall																																
	F-Series																																
<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="+"/>																												
<small>Other static IP addresses on the same subnet. To be able to enable SSLVPN you need to select a certificate under VPN > SSLVPN > Server Settings.</small>																																	

9. Click **Save**.

Step 6. Perform a Network Activation

After you create or change basic network configurations such as routing, you must activate your new network configurations.

1. Scroll to the top of the page.
2. Click on the link inside of the warning message to execute the new network configuration.




 Some configuration changes made within IP Configuration, Routing or Bridging are not yet in effect. To execute the changes, [click here](#). This will cause a temporary interruption in network traffic. You may have to log into the Barracuda NextGen Firewall again. ?

Step 7. Verify the New Configuration

There are two places to verify that the two VLAN interfaces have been configured as expected:

Go to **NETWORK > IP Configuration**. If no errors occurred during the configuration, you can see the two VLAN interfaces both in the **Network Interface Configuration** and **Static Interface Configuration** tables.

NETWORK INTERFACE CONFIGURATION									Help
Interface Name	Application Link		MAC Address	MTU	Speed	Use QoS	Duplex	Status	Action
	TCP Port	Type/Name							
eth0			00:0c:29:9f:b2:54		10000 Mbps	No	Full	Unknown	
eth1			00:0c:29:9f:b2:5e		10000 Mbps	No	Full	Unknown	
eth2			00:0c:29:9f:b2:68		10000 Mbps	No	Full	Unknown	
eth2.100		VLAN interface			10000 Mbps	No	Full	Unknown	
eth2.200		VLAN interface			10000 Mbps	No	Full	Unknown	
eth3			00:0c:29:9f:b2:72			No	Unknown	Down	

STATIC INTERFACE CONFIGURATION					Help
<input type="button" value="Add Static Network Interface"/>					
Name	IP Address/Mask	Interface Name	Classification	Action	
dmz	172.16.0.241/255.255.255.0	eth1	DMZ	Edit 	
vlanprv1	10.0.20.1/255.255.255.0	eth2.100	Trusted	Edit 	
vlanprv2	10.0.21.1/255.255.255.0	eth2.200	Trusted	Edit 	

Go to **NETWORK > Routing**. If no errors occurred during the configuration, you can see the two VLAN interfaces in both the **Network Routes** and the **Network Interfaces** tables.

NETWORK ROUTES Help

Table	From	State	To	Gateway	Source	Interface Na...	Name	Trust Level	Metric
[-] main		✔	172.16.0.0/24		172.16.0.241	eth1	dmz	DMZ	11
		✔	10.0.20.0/24		10.0.20.1	eth2.100	vlanprv1	Trusted	11
		✔	10.0.21.0/24		10.0.21.1	eth2.200	vlanprv2	Trusted	11
		✔	10.17.68.0/24		10.17.68.130	eth0	boxnet	Trusted	
[-] default		✔	0.0.0.0/0	10.17.68.1	10.17.68.130	eth0		Unclassified	

NETWORK INTERFACES Help

Interface Name	IP Addresses	MAC Address	Link	MTU	Speed	Duplex	Transferred	Errors
[+] eth0	10.17.68.130	00:0c:29:9f:b2:54	✔	1500	10000M...	Full	5.34 MB	0
[+] eth1	172.16.0.241	00:0c:29:9f:b2:5e	✔	1500	10000M...	Full	3.32 MB	0
[+] eth2		00:0c:29:9f:b2:68	✔	1500	10000M...	Full	3.31 MB	0
[+] eth2.100	10.0.20.1	00:0c:29:9f:b2:68	✔	1500	10000M...	Full	1.35 KB	0
[+] eth2.200	10.0.21.1	00:0c:29:9f:b2:68	✔	1500	10000M...	Full	1.35 KB	0
[+] eth3		00:0c:29:9f:b2:72		1500	?	?	0.00 kB	0

Figures

1. vlan_config01.png
2. add_vlan.png
3. add_2nd_vlan.png
4. network_activation.png
5. add_static_network_interface_vlan1.png
6. add_static_network_interface_vlan2.png
7. network_activation.png
8. two_vlans_added_nw_itfc_sect.png
9. two_vlans_added_nw_static_itfc_sect.png
10. two_vlans_added_nw_route.png

© Barracuda Networks Inc., 2020 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.