Virtual Local Area Network (VLAN)

A VLAN (Virtual Local Area Network) is a logical construct, similar to a LAN, which defines a broadcast domain. While a LAN requires all hosts to be physically connected to the same switch, a VLAN allows hosts not connected to the same switch to belong to the same broadcast domain. In addition, the ports on a switch with VLAN capabilities can be divided into multiple independent broadcast domains. Network reconfiguration can be done through software instead of physically relocating devices.

When a VLAN spans multiple switches, the VLAN traffic is routed over trunk ports on the switches. The link between two trunk ports is known as the trunk link. Usually a trunk link is implemented between fast switch ports on two different switches using a crossover cable. A VLAN might have 3 ports on one switch, and 7 ports on another; the inter-switch traffic is routed on the trunk ports.

Traffic for multiple VLANs can be transferred across a single trunk link. This works using VLAN tagging, which tags Ethernet packets with the VLAN ID to which the packet belongs. Alternatively, VLAN ports on the VLAN switch belong to a single VLAN and therefore only see the broadcast traffic of that VLAN.

VLAN Configuration

To route a VLAN through the WAN, LAN, or MGMT interface, a VLAN interface must be added to receive the broadcast traffic from the VLAN and route traffic to the VLAN. To add a VLAN interface, you must specify the VLAN ID, and the IP address and subnet mask for the interface. Based on the destination IP address of network packets, the Barracuda Web Application Firewall routes the packets to the appropriate VLAN interface.

Adding a VLAN interface makes the Barracuda Web Application Firewall aware of that VLAN, and allows it to perform explicit VLAN tagging functions for traffic routed to the VLAN, and to remove VLAN tagging when routing packets from the VLAN to non-VLAN networks.

For example, if all Real Servers reside in VLAN 100, then the LAN port may be connected to a port on the VLAN switch belonging to VLAN 100. Correspondingly a VLAN interface must be added to the LAN interface with VLAN ID 100 and have an available IP address belonging in the VLAN broadcast domain.

A VLAN rule can be added in the **NETWORKS > VLAN** page. In the **Add VLAN** section, specify values for the fields and click **Add**. Click **Help** for more information.

Routing to Multiple VLANs over an Interface

If any interface on the Barracuda Web Application Firewall has to route to multiple VLANs, it must be connected to the VLAN switch via a trunk (or hybrid) link, since VLAN traffic to multiple VLANs can only be transported over trunk links. In order to route to multiple VLANs via any of the physical interfaces, one VLAN interface must be added to the relevant physical interface per VLAN. If the Real Servers are distributed across multiple VLANs, say 100, 105, and 111, then the LAN port must be connected to a trunk port on the VLAN switch. A VLAN interface must be added for each VLAN on the LAN interface with the corresponding VLAN IDs, 100, 105 and 111. This allows the Barracuda Web Application Firewall to route to the correct VLAN by inserting appropriate VLAN IDs before forwarding on to the trunk link.

Bridge Mode

In Bridge mode, if VLANs are being used, both the LAN and WAN ports must be on the same VLAN and a corresponding VLAN interface must be added on either the WAN or LAN interface. Bridge mode does not currently support configurations with the LAN and WAN connected to different VLANs. If the MGMT port is part of one or more VLANs, then VLAN interfaces must be added on to the MGMT port for the respective VLANs.