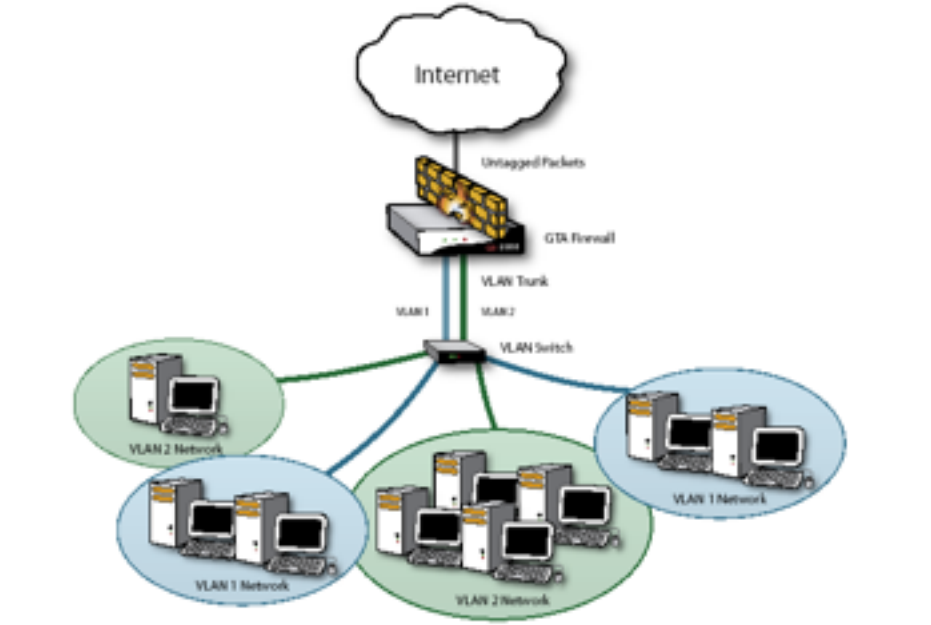
Global Technology Associates, Inc.

Internet Firewall Developer since 1994

Advanced Network VLAN



Course # 3202

VLAN

- Virtual Local Area Network
  - Defined in IEEE 802.1Q
  - Provides the ability to define broadcast domains
  - Number of VLAN's is product dependent.
  - All GTA firewall support VLAN's.
- GB-OS systems using VLAN's are always Trunks and must be connected to another VLAN enabled device or switch configure as a trunk.
  - Firewall expects tagged packets when configure as VLAN Trunk.
- VLAN –Once a VLAN interface is configured on a GTA firewall it is treated like any other interface of the appropriate type.

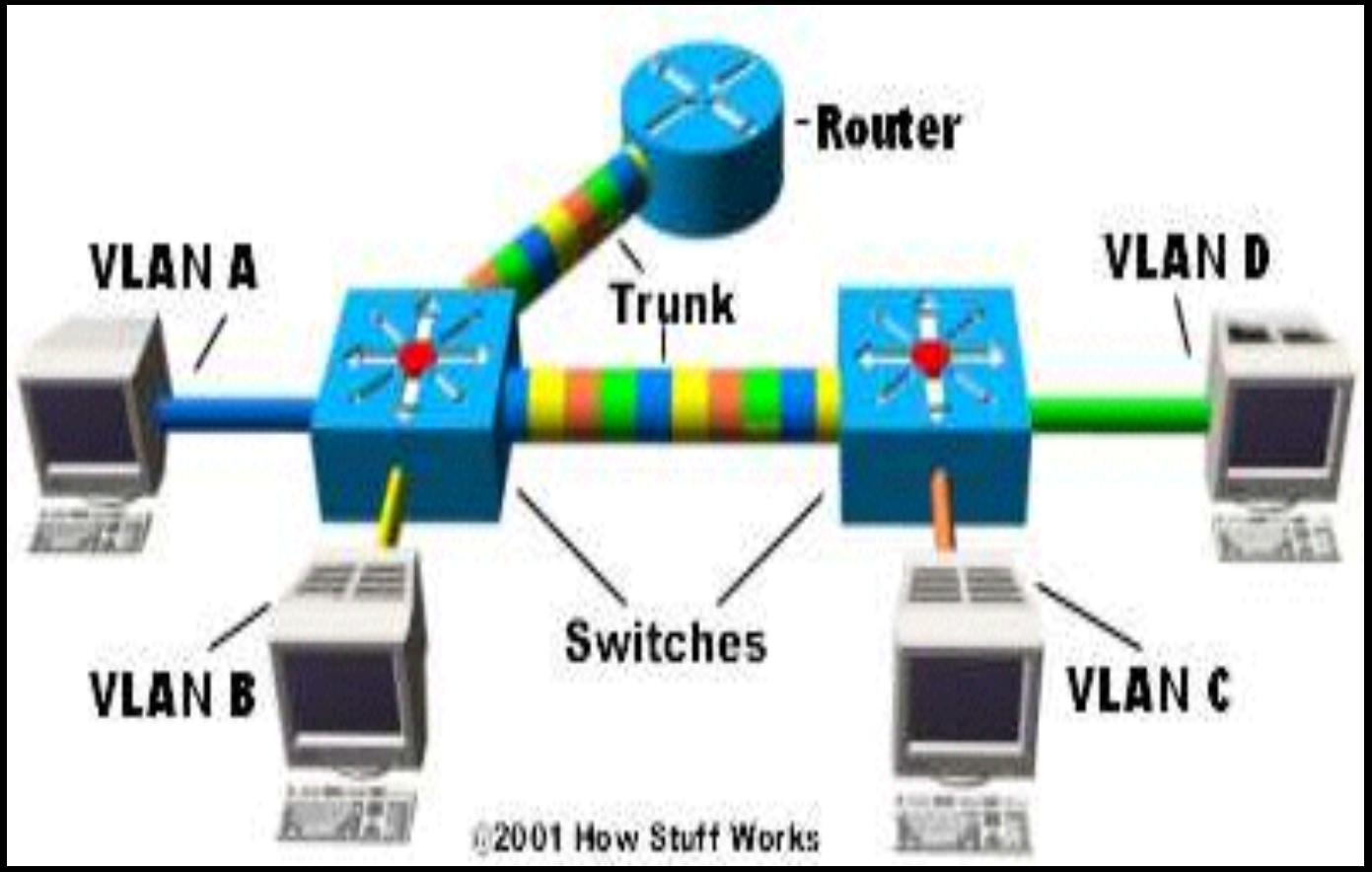
VLAN – Requirements

- VLAN enabled switch
- Basic knowledge of TCP/IP
- Understand of VLAN switch configuration and trunking.
- Administrative privileges on your firewall.
- Does not support a VLAN on a PPP Interface, such as using PPPoE.

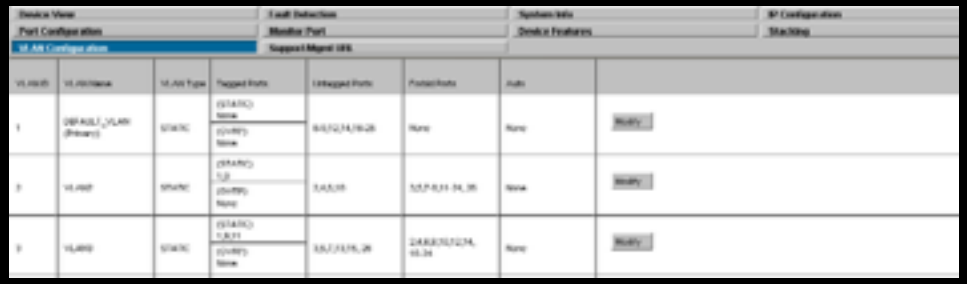
Terms

- **VLAN interface** - is the physical interface that is connected to a VLAN switch. A VLAN interface can be assigned to any physical interface, even if it is not defined in Configure>Network>Settings. For example, a VLAN interface can be assigned to eth0, which may already be assigned to your protected network. Adding a VLAN interface to a physical interface that has already been assigned as an external network, protected network or PSN will not create conflicts. Like physical interfaces, VLANs can be bridged. For more information on bridging interfaces, see Bridging Interfaces.
- **VLAN IDs** - A VLAN segregates devices that are physically separate from each other based upon the IEEE 802.1Q VLAN ID tag that has been sent and received by the devices in the VLAN. For example, packets with a VLAN ID of 1 will only be sent to network devices logically located on the VLAN 1 network. The VLAN ID can be any number between 1 and 4095, and must match the VLAN ID configured on the VLAN switch. When configuring multiple VLANs over one physical interface, it is not possible to have a VLAN interface share the same VLAN ID. It is possible, however, to add a VLAN interface to another physical interface that has the same VLAN ID. For example, a VLAN interface on eth0 with a VLAN ID of 1 and a VLAN interface on eth1 with a VLAN ID of 1 can both be created without conflict.
- **VLAN Trunk** - In a typical configuration, VLAN routers or switches and GTA firewalls add VLAN IDs to packets travelling to or from a VLAN. A VLAN trunk is the physical connection between the two devices. Packets travelling along a VLAN trunk must be handled by a VLAN router, VLAN switch or GTA firewall. VLAN IDs are only added to data packets when travelling along the VLAN trunk. Once the data packet passes through a VLAN network device, such as a GTA firewall or VLAN switch, the VLAN ID is stripped.
- **VLAN Switch** - A VLAN switch is the network device that resides on the other end of a VLAN trunk. When data packets with a VLAN ID travel through the switch, its logic will direct the traffic to the appropriate VLAN. For example, a header with a VLAN ID of 12 will be directed to VLAN 12.

Example VLAN Trunks



Example Switch Interface



HP ProCurve 2626

Linksys SRW246

D-Link DSG-3200-10

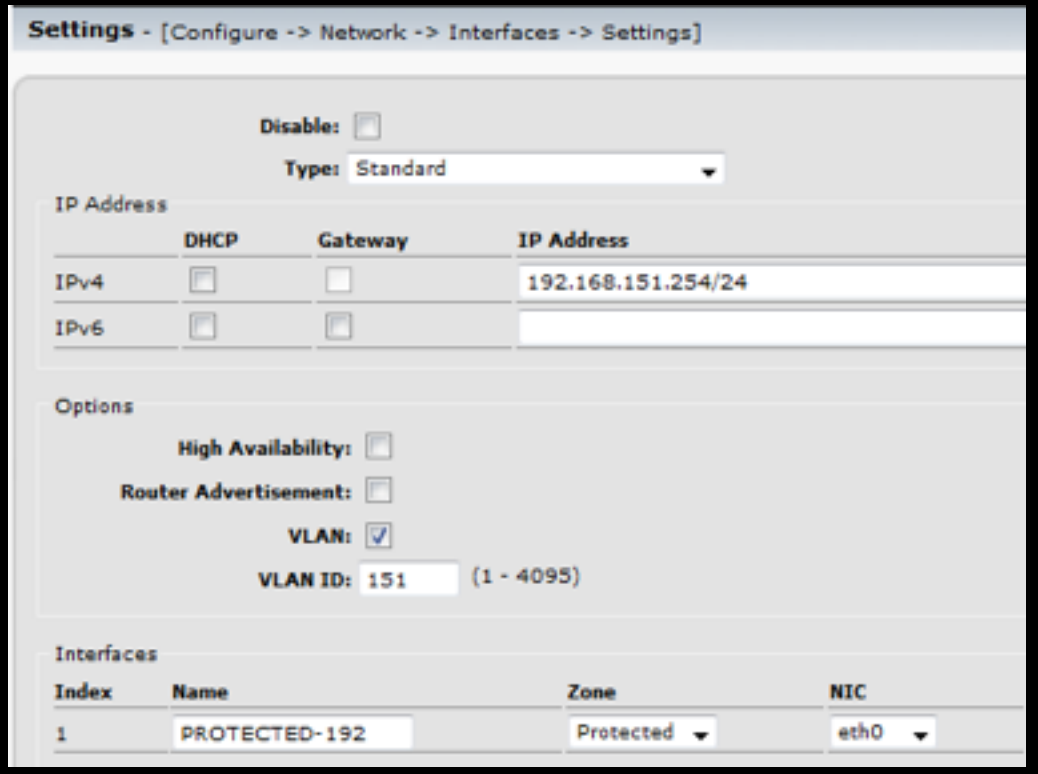
Configure a Basic VLAN

- To configure a VLAN, navigate to Network -> Interfaces -> Settings click the **NEW** icon to create a new Interface
  1. Select a type for the interface. Default is **Standard**. However, all interface types are supported
  2. Enter the VLAN IP address or select DHCP
  3. Select VLAN
  4. Enter the VLAN's VLAN ID. This ID must be matched on the VLAN switch or router.
  5. Interfaces
     1. Enter VLAN Name
     2. For the VLAN's NIC, select the physical interface that will be connected to the VLAN switch or router. For example, **<eth0>**. PPP interfaces are not supported for VLAN's.
     3. Select the interface's Zone, such as **<Protected>**.
  6. Click **OK** and then **SAVE**.

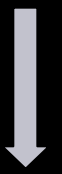
- VLAN Configuration is complete
  - Connect firewall to the trunk port on switch
  - Configure Security Policies based on corporate security policy.

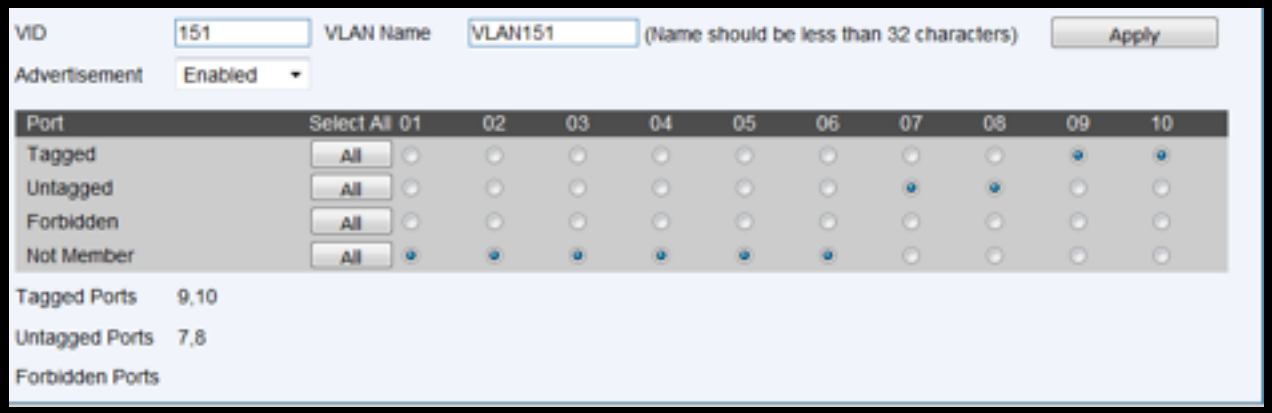
VLAN Configuration

Firewall VLAN Interface Configuration

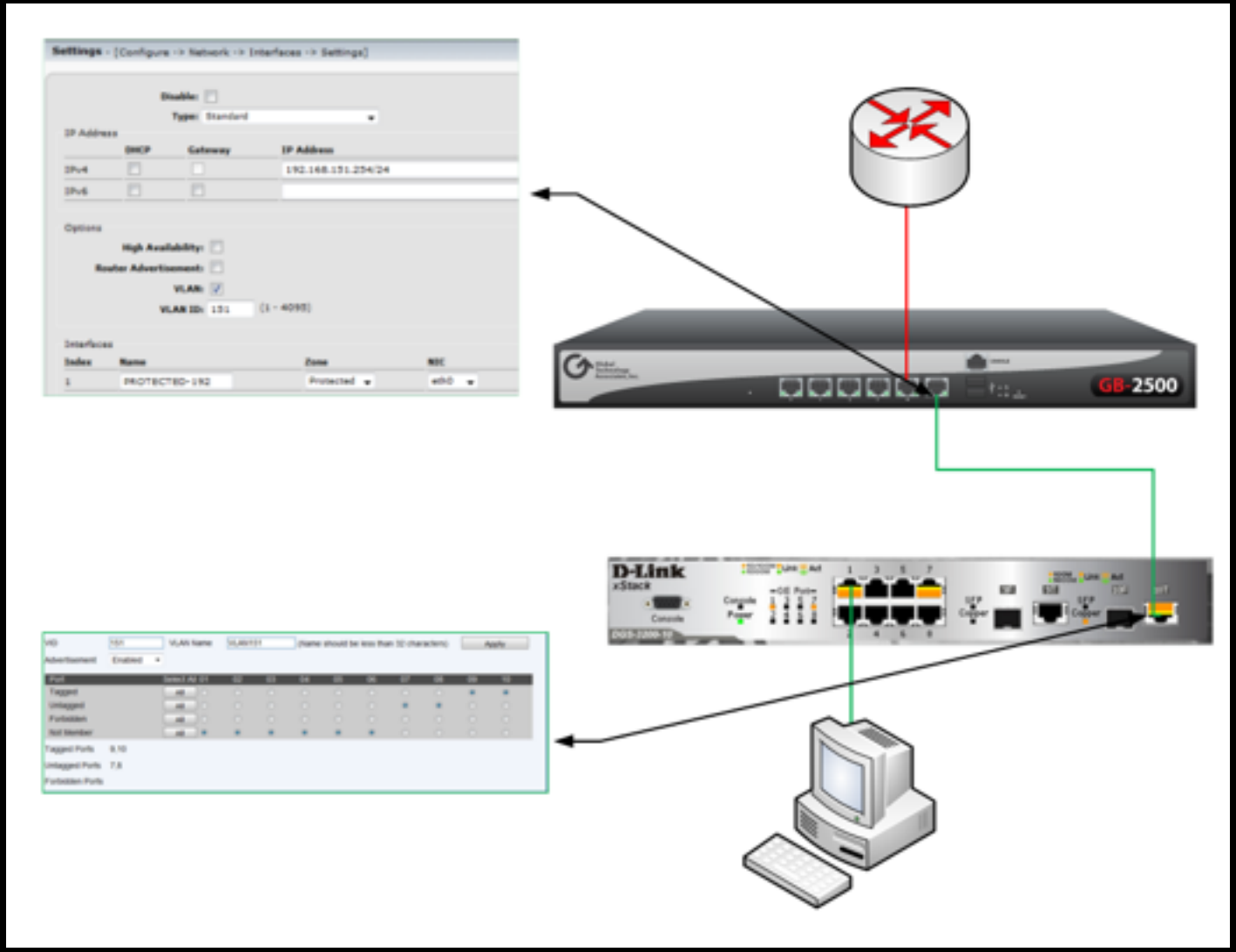


Switch VLAN configuration





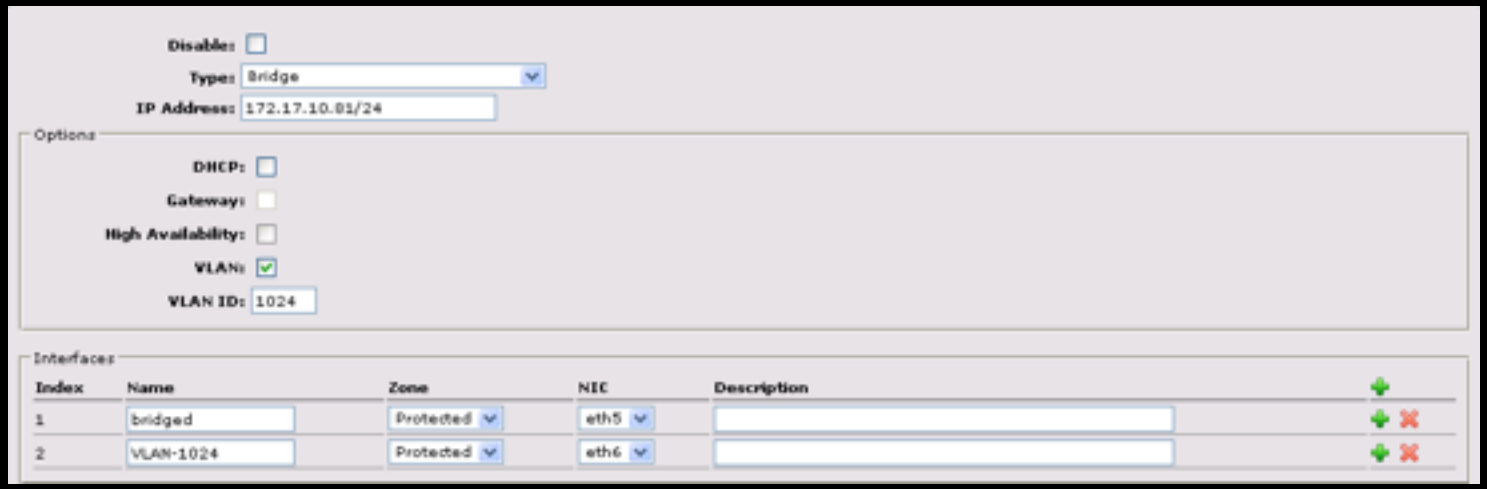
Switch Port will be connected to the firewall Tagged Port



After VLAN is configured

- Acts like a normal physical interface
- All rules apply per type of interface

Advanced VLAN
Bridged

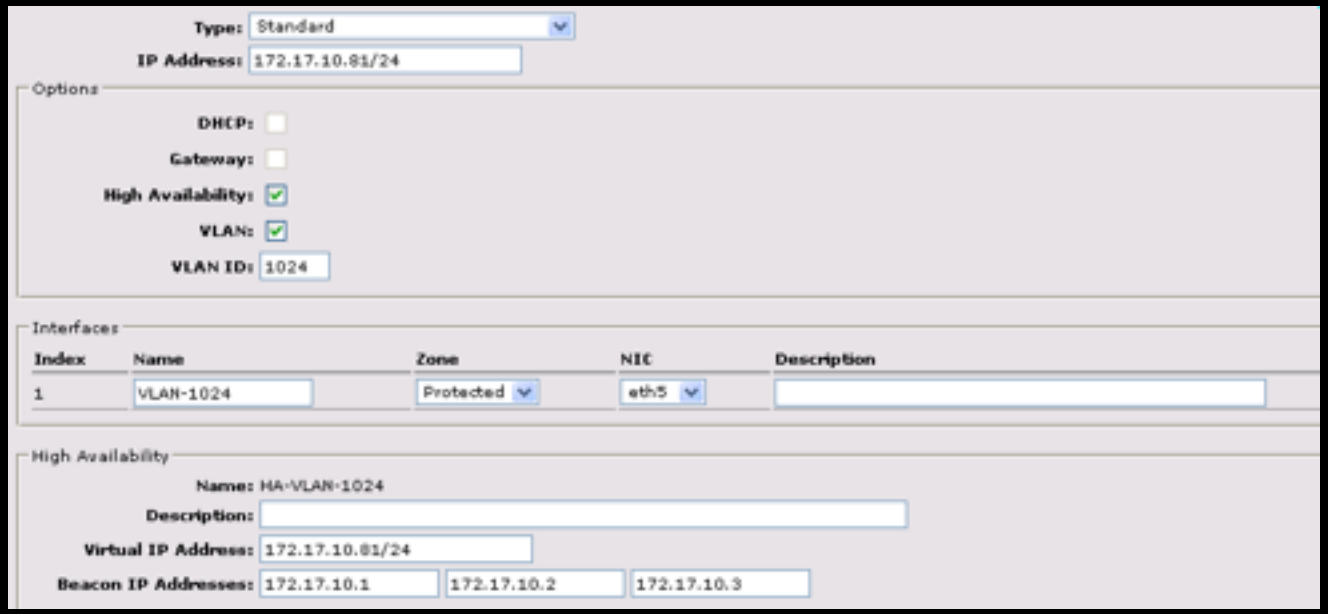


- V5.2 Bridged mode was added to the VLAN's
- Select Type Bridge when configuring VLAN.
- Use Green **Plus** or Red **X** to add or remove from the bridge.
- Once VLAN bridge is enabled VLAN interfaces will act like typical bridged interfaces on a firewall. Configure Security Policies using IP Pass Through Policies.

Standard VLAN and High Availability (HA)

- A VLAN interface of type Standard with High Availability uncheck on an HA system is not an HA interface.
- During Update Slave the VLAN interface will be pushed to the Slave firewall.
- VLAN will only be active on the firewall in Master mode. When in init or slave mode the VLAN interface will not bind to the firewall.
- To have a VLAN act as a standard HA interface configure a VLAN as an HA interface in an High Availability group enabled the High Availability option on the interface.

Advanced VLAN
High Availability



- Set up standard VLAN Interface and then check the HA option. This will display the HA configuration section.
- Add Virtual IP used on the VLAN and the beacon addresses.
- Complete the High Availability configuration in the Service section.

VLAN and High Availability

- When HA Option is enabled the VLAN will be always active for standard IP. HA IP will be assumed only in Master mode.
- VLAN IP address will need to be added to the HA Nodes object.
- Since the VLAN interface has High Availability enabled. During update slave the Interface IP will not be pushed to the slave system.
- VLAN interface will be treated like any other HA interface.

FAQ

- Do you need to purchase an upgrade OS for VLAN trunks?
  - No VLAN trunk support is standard on all GTA firewalls.
- How many VLAN's does GTA firewalls support?
  - Number of VLAN's is dependent on the firewall model.
- What GB-OS versions support VLAN's?
  - VLAN support was added in v4.0 and improved on in subsequent releases.

Trouble Shooting

- Confirm VLAN TAGS on Firewall match VLAN switch.
- Possible Network Diagram
- Confirm ports connected to switch
- Get Syslog data, you may wish to enable logging of unexpected or invalid packets in the Policy Preferences section.
- Firewall Configuration and switch configuration (If possible)
- SNIFFER
- Find out switch information
  - Version
  - Model

References

- http://www.networknewz.com/networknewz-10-20030725IntroductiontoVLANs.html
- http://www.ieee802.org/1/pages/802.1Q.html
- http://computer.howstuffworks.com/lan-switch16.htm

If you require additional assistance or have additional questions please contact GTA Technical Support.

- Email: support @gta.com
- Support Line Phone: 1.407.482.6925
- Normal Hours – 0830-1900 EST U.S.
- Free User Support – http://forum.gta.com

References

- GTA Online Documentation - http://www.gta.com/support/documents
- FreeBSD LAG Information - http://www.freebsd.org/doc/en/books/handbook/network-aggregation.html