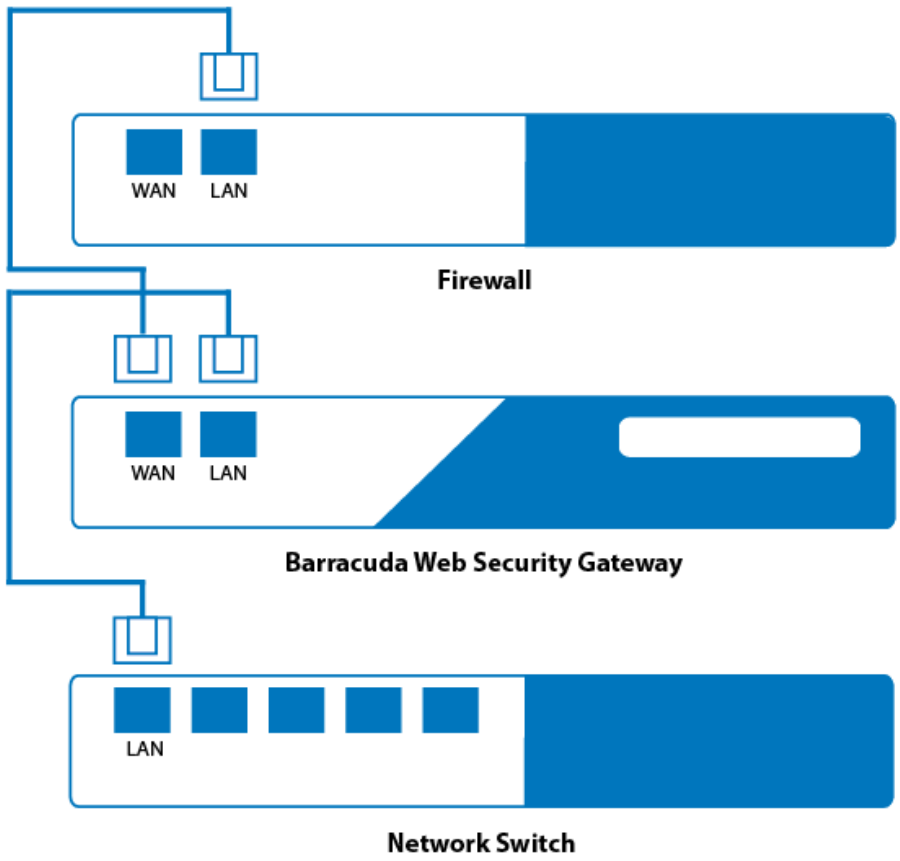
Step 5 - Connect the Barracuda Web Security Gateway to Your Network

https://campus.barracuda.com/doc/6160431/

Begin by choosing either inline or forward proxy deployment. For details about each option, see Inline Pass-Through (Transparent) Mode Deployment and Forward Proxy Deployment of the Barracuda Web Security Gateway.

Inline Deployment

1. Connect the Ethernet cable from your corporate firewall to the WAN port of the Barracuda Web Security Gateway. This step may require disconnecting your internal network switch from the corporate firewall. A crossover cable may be needed if your corporate firewall does not have a switchable port and therefore cannot switch between RX and TX. Another solution is to place a switch between the corporate firewall and the Barracuda Web Security Gateway. You do not need to configure the WAN port. The Barracuda Web Security Gateway creates an Ethernet bridge between the WAN and LAN ports.
2. Connect the LAN port of the Barracuda Web Security Gateway to your internal network switch, router or hub.



3. Select the **BASIC > IP Configuration** page in the web interface, and set the **Operating Mode** to **Audit** and test out your current policy settings as described below in Set the Operating Mode.

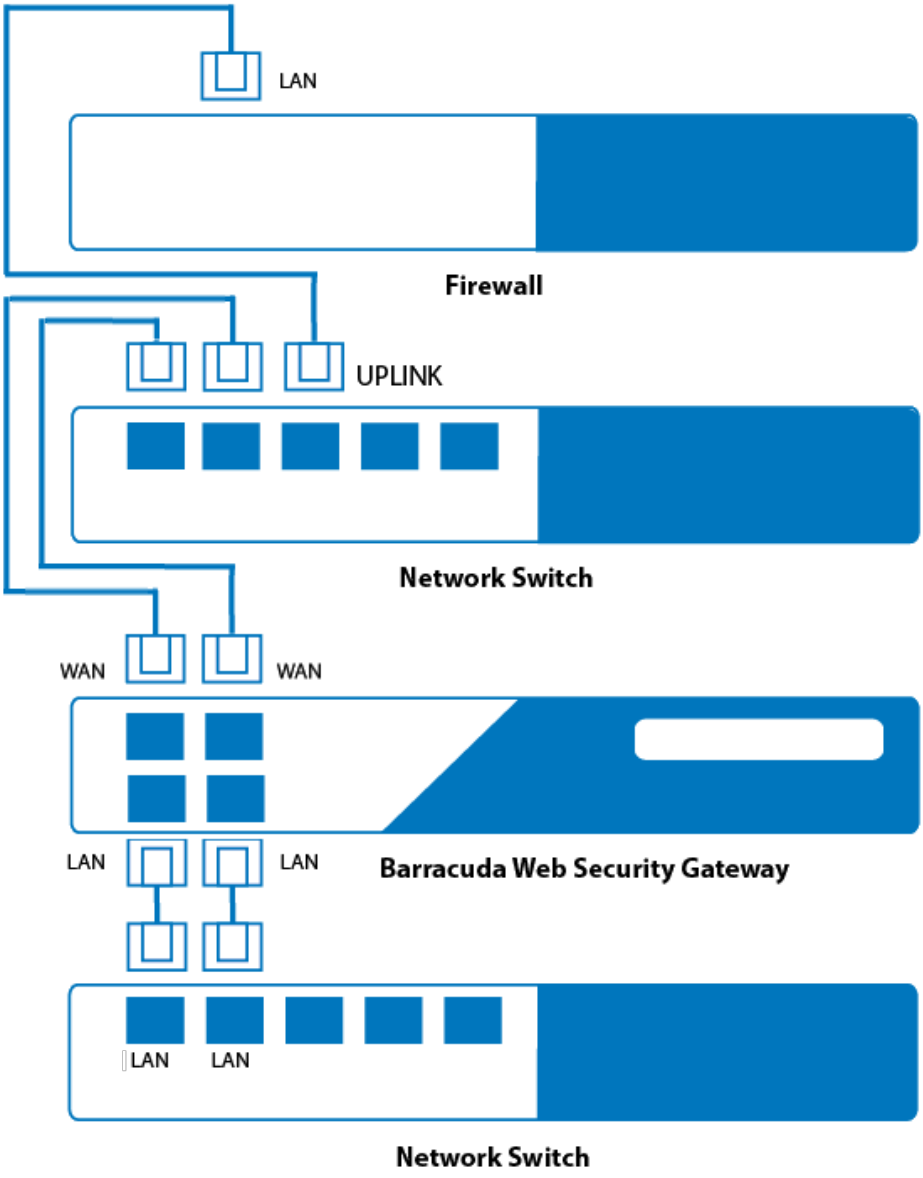
Barracuda Web Security Gateway 810 With Bonded NIC Interfaces

The 810 model offers two 1G interfaces for both WAN and LAN ports that can function as a bonded interface, allowing 2G of ingress/egress traffic in the following configuration:

1. Connect each of the two WAN ports to a separate port on the network switch that connects to the firewall.
2. Connect each of the two LAN ports to a separate port on the switch to the local area network.

For this deployment, be sure to block Spanning-Tree Protocol (STP) on the port-channel used for these connections. For example, with a Cisco Nexus 5000 switch, include '`spanning-tree bpdufilter enable`' in the port-channel configuration.

Example of deployment of Barracuda Web Security Gateway 810 with bonded NIC interfaces:



Forward Proxy Deployment

1. Connect either the WAN or LAN port of the Barracuda Web Security Gateway to the same switch as the network gateway (just one network hop away).
2. Configure your clients' HTTP proxy settings from their browser to access the Internet. See Forward Proxy Deployment of the Barracuda Web Security Gateway for more information.

Determine if You Need to Set Up Static Routes

If necessary, set up Static Routes on the **BASIC > IP Configuration** page. Setting up static routes is

often required in more complex networks so that the Barracuda Web Security Gateway knows the proper route for returning client traffic to your network's next device (which the Barracuda Web Security Gateway is connected to), in order for that device to route the traffic back to the client(s).

Using static routes enables the Barracuda Web Security Gateway to protect any client machines that have IP addresses outside of the native subnet of the Barracuda Web Security Gateway. For example, if the Barracuda Web Security Gateway is assigned an IP address of 172.20.0.6 and a subnet mask of 255.255.255.0 and uses the default gateway at 172.20.0.9, you will need to create a static route to reach client machines in the range of 192.168.2.x with a netmask value of 255.255.255.0. The Gateway Address should be inside 172.20.0.x. See Using Static Routes for more information.

Test and adjust the Barracuda Web Security Gateway

After connecting your Barracuda Web Security Gateway to the network, verify connectivity. Open your web browser from a machine on your network. If you cannot browse the web, review the installation steps to make sure your Barracuda Web Security Gateway is properly configured and connected to your corporate firewall and network switch.

If you can browse the web without any issues, you are ready to adjust the settings on the Barracuda Web Security Gateway. The most common adjustment to make is to create filters that determine what traffic and applications the Barracuda Web Security Gateway blocks and accepts. For more information about the available filters, refer to Monitoring the System.

Set the Operating Mode

Inline deployment:

1. Set the **Operating Mode** to **Audit** from the **BASIC > IP Configuration** page, and note how traffic is logged. In **Audit** mode, traffic is only logged, not blocked. As you configure policies on the **BLOCK/ACCEPT** pages, with the Barracuda Web Security Gateway in **Audit** mode, you can see how your users surf the web and then adjust policies accordingly.
2. When you are ready to block traffic based on those policies, for an inline deployment, change the **Operating Mode** to **Active**. Now traffic will be blocked per polices you have set, as well as being logged.

Forward proxy deployment:

In this deployment, **Audit** and **Active** modes behave the same way; traffic is logged and is blocked per policies you set. See **Understanding Operating Modes** in Step 3 - Configure the Barracuda Web Security Gateway for more information on these modes.

Exempt Specific IP Addresses or Clients

Go to the **BLOCK/ACCEPT > IP Block/Exempt** page and use the **IP and Port Exemption** section to bypass scanning or filtering for clients or targeted servers. To avoid accidentally specifying a broader than intended exemption range, be sure to apply the proper subnet mask. For example, if you wanted to exclude a Windows Update server (WSUS) from filtering, use a /32 (255.255.255.255) subnet mask.

Filtering HTTPS Traffic

HTTPS traffic can be detected by content category filters and domain filters, as well as by exceptions you might create for all web traffic, content category filters, and domain filters (see the **BLOCK/ACCEPT > Exceptions** page). The **HTTPS Filtering** option is configured on the **BLOCK/ACCEPT > Configuration** page, and is disabled by default. Note that the Barracuda Web Security Gateway relies on DNS responses when filtering HTTPS traffic. In order for the rules to be applied properly for HTTPS requests, DNS queries and responses should go through Barracuda Web Security Gateway. This requires doing the following:

1. On the **BASIC > IP Configuration** page, set the primary DNS server to an external one.
2. Set the DNS server in all clients to the same primary DNS server.

When first enabling HTTPS filtering, any client PCs that had previously established an HTTPS session will not be blocked. In this situation, the HTTPS website's IP address remains in the user's local DNS cache (as well as in the DNS table on the core router or domain controller) until the DNS request time-to-live (TTL) expires. This can take up to a day or two, depending upon how the HTTPS sites configure TTL. What this means is that, until the user performs another DNS lookup of a website's domain name, the Barracuda Web Security Gateway won't automatically know which domain is associated with the IP address and won't be able to perform any domain blocks on those connections.

To avoid this issue, you can manually clear the DNS cache on your network's DNS servers.

For a secure deployment, Barracuda Networks recommends reviewing Securing the Barracuda Web Security Gateway.

Figures

1. InlineDeployWSG.png
2. 810_BondedNICWSG.png