Step 1 - Network Considerations

https://campus.barracuda.com/doc/6160460/

The Barracuda Web Security Gateway is designed for low-risk deployment because it is intended to be a bridge within your network. The Barracuda Web Security Gateway can view Internet traffic that passes through the network but does not affect its routing. To reduce the risk of interfering with important network traffic, initially set the Barracuda Web Security Gateway to monitor and log the spyware activity only. Determine which internal servers and clients to exclude from spyware and virus scans.

> For maximum security, Barracuda Networks recommends placing your Barracuda Web Security Gateway behind a corporate firewall.

The following pre-installation considerations may help you understand some of the issues that may occur, and Barracuda Networks recommends reading and understanding the Deployment Options for the Barracuda Web Security Gateway before proceeding.

Routers

Make sure the default gateway is properly set to reach the Internet. Also, if you are testing the Barracuda Web Security Gateway in one portion of your network and move to another portion of the network for deployment, make sure that you check the default gateway and make changes as necessary.

VLANs

If you have a trunk port for a VLAN setup, you may need to set up a virtual host interface (VIF) to be able to talk to the network. A VIF enables the router to send and receive IP multicast packets on several different interfaces at once, as dictated by the multicast routing tables on the router.

External DNS

Some of the considerations regarding DNS include the following issues:

Optimal DNS query response time: When the Barracuda Web Security Gateway is in Active mode, it proxies all Internet requests for the clients. As a result, the Barracuda Web Security Gateway needs to resolve website hostnames to IP addresses while proxying the HTTP requests made by the users. The response for web server DNS queries needs to be optimal to allow the Barracuda Web Security Gateway to look up and quickly process these requests. A slow DNS server will cause the Barracuda

Web Security Gateway to respond slowly to clients, which adds latency to their Internet access.

Requests for fully qualified Web application server names: If a user attempts to browse to a website by specifying a web server name which is not a fully qualified name that includes the domain name, the Barracuda Web Security Gateway automatically appends the string barracuda.com to the unqualified name in order to resolve the request. For example, if the user enters the server name myserver instead of myserver.mydomain.com, the Barracuda Web Security Gateway resolves the request using the hostname myserver.barracuda.com.

HTTPS Filtering: 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.

Internal DNS

If you have an internal server that is only resolvable via an internal DNS, make sure that this DNS server is used by the Barracuda Web Security Gateway as a secondary DNS.

Enterprise class Layer 3 switch, VLANS, VPN concentrators

These device types are normally capable of handling multiple subnets and providing default routes to clients. However, they may affect the Barracuda Web Security Gateway deployment in the following ways:

- A Layer 3 switch can also be set up to have multiple VLANs (Virtual Local Networks) using port assignments. There is no side effect by having VLAN tags in the traffic that is visible to the Barracuda Web Security Gateway (see also VLAN Deployments). However, when the Barracuda Web Security Gateway is set up to a single subnet, it needs to have routes to process requests for other subnets. Although all VLAN operations are in Layer 2, most of the Layer 3 switches have better control since they offer a management user interface. Layer 2 "Smart" switches offer VLAN support as well. Layer 3 switches primarily differ from their capabilities of routing in IPv4 and IPv6, so it acts more like a router which is beyond normal switching hardware can do.
- A standard solution is to add static routes to these foreign subnets. All Layer 3 switch subnets should use its IP address as the gateway. In the case of a VPN concentrator, use the IP of the concentrator as the default gateway for all the networks aggregated by that VPN concentrator.
- If you have a trunk port for a VLAN setup, you may need to set up a virtual host interface (VIF) to be able to talk to the network. A VIF enables the router to send and receive IP multicast

packets on several different interfaces at once, as dictated by the multicast routing tables on the router.

Other considerations:

- On the **Basic > IP Configuration** page, set **Enable proxy on WAN** to **Yes** if you are routing traffic through the WAN interface of the Barracuda Web Security Gateway.
- In the case of a VPN concentrator, you should typically use the IP address of the core switch as the default gateway for all the networks aggregated by that VPN concentrator. Alternatively, you may need to use the IP address of the concentrator (or firewall) as the default gateway for all the networks aggregated by that VPN concentrator. This will allow all of the VPN traffic to be filtered with the Barracuda Web Security Gateway being on the internal network.

To filter VPN traffic when the Barracuda Web Security Gateway is deployed inline:

1. Go to the **ADVANCED > Configuration** page.
2. Set **Pass Client IP addresses through WAN port** to *No*, effectively enabling the Barracuda Web Security Gateway as the source IP for all outbound packets.

Firewall DMZ

Servers in the demilitarized zone (DMZ) are accessible from the internet. Servers inside this zone, such as mail servers, for example, may be configured to access certain servers within an internal network with their own security rules set up. The Barracuda Web Security Gateway should not be deployed to protect these machines. **The Barracuda Web Security Gateway is not designed to protect servers but, rather, to protect end user machines. For maximum security, Barracuda Networks recommends placing your Barracuda Web Security Gateway behind a corporate firewall.**

Internal Servers

In most organizations, internal servers are protected by corporate firewalls that use port forwarding rules to limit access to the servers. Port forwarding rules define the ports that can be used to access the servers (such as HTTP, FTP, and mail servers). These servers should have optimal response time.

As a result, the server traffic must not be interrupted. Barracuda Networks recommends that you exempt or bypass these servers from the Barracuda Web Security Gateway. To reduce Layer 2 bridging overhead, place a switch between the firewall and the Barracuda Web Security Gateway and connect your server farm on a different port on the switch. In this case, set up the servers parallel to the Barracuda Web Security Gateway instead of behind it, and then configure the **IP and Port Exemptions** feature on the **BLOCK/ACCEPT > IP Block/Exempt** page to exclude these IP addresses from filtering

Caching and the Current Time Setting

Caching provides faster access to repeatedly requested content by storing content locally on the Barracuda Web Security Gateway. Data is handled using an LRU (Least Recently Used) algorithm. You can enable or disable content caching, and specify domains to exempt from content caching, on the **ADVANCED > Caching** page. Note that the time value entered in the Current Time field on the **BASIC > Administration** page must be accurate since the Barracuda Web Security Gateway uses the current time to ensure accurate cache updates.

QoS/Packet Reconfiguration (Quality of Service, Packet Shapers)

There are many products available that can control traffic in a LAN environment, specify priorities, and size these different traffic types. Normally, this is done using a Layer 7 device on different types of applications. The Barracuda Web Security Gateway deployment is affected when the Barracuda Web Security Gateway is placed in front of these devices to benefit from the shaped data. Place the Barracuda Web Security Gateway close to the Internet to help reduce noise and overhead on both the Layer 2 bridging and HTTP proxy.

Mounting and cabling considerations

To install the Barracuda Web Security Gateway you need to:

- Mount it on a rack or shelf, unless you have a desktop model and don't need to rack it.
- Cable it to other network devices

The Barracuda Web Security Gateway is designed to be installed in a data center with other networking devices and servers. Depending on the model, its dimensions are suitable for a 19-inch rack, or can be adapted to a rack with the mounting kit. You must position it within cabling distance of any switches or other devices that access the network segments that you want to protect. The appliance can be mounted facing either direction in your rack, so consider which side will have access to the ports. You may need access to the ports during installation, and you may need to use the back panel during initial configuration.

Continue with Step 2 - Installation.