Traffic Shaping

https://campus.barracuda.com/doc/5799962/

The Barracuda Link Balancer allows you to shape incoming and outgoing traffic and link usage in a variety of ways.

> To achieve optimum bandwidth management, ensure that the configuration of your WAN links matches your ISP specifications, such as upstream and downstream speeds. The links can be configured in **BASIC > Links > Link Configuration** (see Step 2: Configure Networking Settings).

Link Usage for Inbound and Outbound Traffic

Outbound Link Balancing

By default, outbound traffic from a client IP address to a new destination IP address inspires comparison of link weights and uses the link with the highest weight. The link weight is the available capacity based on configured link speed and current usage. The weight for each primary and backup WAN link updates on an a continual basis.

Inbound Link Balancing

Inbound link balancing and failover are available only when the Barracuda Link Balancer acts as an authoritative DNS server for domains behind it. When the Barracuda Link Balancer receives a DNS query for a hosted domain, it returns the IP address of a WAN link which the client then uses to reach the hosted domain. The same algorithm is used to select the returned WAN link as is used for outbound link balancing.

Grouping WAN Links for Inbound and Outbound Traffic

You can change how frequently WAN links are used by assigning each link to one of three groups for both inbound and outbound traffic. This feature allows you to reserve links for certain types of traffic or to use higher cost links only if lower cost links fail or become saturated. The supported usage groups are:

- Primary links - Used first for link balancing.
- Backup links - Used only if the primary links are down or if they become saturated. If all primary links are down or saturated, then traffic is distributed across all available backup links until the

primary links become available.
- Private links - Used only for traffic matching IP/Application routing rules or if specified explicitly in the configuration of a VPN. Private links are not used at all for default outbound or inbound link balancing. They are used only if explicitly referenced.

If you want to employ default link balancing policy, where the link with the greatest available capacity is used, set the usage group for each link to **Primary**. To assign each link a usage group, edit the link on the **Basic > Links** page.

Specifying WAN Link for Outbound Traffic

You can override the link balancing algorithm by creating rules that determine which WAN link certain kinds of outbound traffic use. See Specifying the Link Used by Outgoing Traffic.

Creating Quality of Service (QoS) Pipes, Subpipes and Rules

You can control traffic shaping in hierarchical structures of pipes, subpipes and rules. Traffic shaping is executed after determination of the WAN link the traffic will use and applies to all traffic, including VPN traffic, regardless of whether the Barracuda Link Balancer firewall is enabled. Each rule describes a set of traffic based on one or more parameters: source IP address or range, destination IP address or range, application or applications, time, day of the week, and WAN link. Three different hierarchy levels control different aspects of the traffic. If the defined conditions are met, the pipe, subpipe or rule assigns bandwidth shaping and contention shaping. If the traffic on the network exceeds capacity, traffic from high priority applications is allocated a greater share of the bandwidth. The contention shaping subdivides traffic that has the same bandwidth shaping level.

Some examples of traffic shaping:

- Give higher priority to traffic originating from a set of IP addresses.
- Assign lower priority to FTP traffic so that file uploading and downloading does not affect other applications.
- Increase the priority of SIP traffic so that calls are not dropped.
- Give VPN traffic a high priority. You can create a rule with the source IP address of the local VPN endpoint and the destination IP address of the remote VPN endpoint.

Configure QoS on the **POLICY > Bandwidth Mgmt** page.