High Availability - Linked Management and the Barracuda Web Security Gateway

https://campus.barracuda.com/doc/6160457/

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

Using the Linked Management feature you can cluster, or link two or more Barracuda Web Security Gateways together to provide synchronized configuration and policy settings across all systems. You can also use this feature to provide high availability, or failover, in case one system fails.

For High Availability, the following must be true:

- Multiple Barracuda Web Security Gateways are in the same network
- All Barracuda Web Security Gateways are always active
- Web traffic is only directed through one Barracuda Web Security Gateway at a time
- Failover is handled by other network equipment
- All Barracuda Web Security Gateways must be running the same version of firmware
- Barracuda recommends that all of the Barracuda Web Security Gateways using linked management are the same model. If you wish to link manage mixed models, please contact Barracuda Technical Support for configuration assistance.

For automatically synchronizing most configuration and policy settings across all systems, linked Barracuda Web Security Gateways can be geographically dispersed and do not need to be co-located on the same network. All Barracuda Web Security Gateways must be the same model running the same version of firmware in this use case as well.

Note that Linked Management does not provide load-balancing functionality.

The Barracuda Web Security Gateway uses port 8002 to synchronize configuration between linked systems. Use the **ADVANCED > Linked Management** page to link multiple Barracuda Web Security Gateways. This feature is available on the Barracuda Web Security Gateway 410 and above.

Linked Management Means the Same Policies for Each System

Some network environments may not be suitable to linking multiple Barracuda Web Security Gateway systems together. For example, if you have multiple network segments that each require different policies, it may be better to provide a dedicated, unlinked Barracuda Web Security Gateway for each segment. This way you can configure each Barracuda Web Security Gateway without the configuration settings propagating to the other systems. See How to Set Up Barracuda Cloud Control

for information about managing multiple Barracuda Web Security Gateways (and/or other Barracuda Networks products) with unique configuration and policy settings on each system.

Also see:

- Forward Proxy Deployment
- How to Create and Install a Self-Signed Certificate for SSL Inspection

If you are using a WCCP Deployment, please contact Barracuda Technical Support to confirm that your configuration of linked Barracuda Web Security Gateways is correct.

High Availability Deployment Options

Consider the following methods for deploying linked Barracuda Web Security Gateways for failover and, in some cases, load balancing, depending on your OS and network configuration:

Method 1: Use a PAC file with a GPO. Create a PAC file on your network and use Windows GPO to tell client browsers where to locate the PAC file. The PAC file indicates the proxy server URL (Barracuda Web Security Gateway) to which the browsers are to proxy user requests. In the PAC file you can also specify URL exceptions that won't accept proxied requests. The advantages of this method are:

In the PAC file you can specify a primary and secondary Barracuda Web Security Gateway IP address so that if one is unavailable, the browser will proxy to the other.

You can specify URL exceptions in the PAC file for which you want user requests to bypass the Barracuda Web Security Gateway. These exceptions might include intranet sites or other sites that accept connections from particular 'allowed' IP addresses.

Method 2: Use a PAC file with autodetection via DHCP or DNS. This is an alternative to using a Windows GPO to propagate PAC file information to client browsers.With DHCP, updates to your clients can include PAC file location information along with dynamically assigned IP addresses and other attributes. Configure this in your DHCP server settings. With DNS, you can add a hostname wpad (web proxy auto discovery) to your domain name in the DNS server. The wpad contains the IP address where the PAC file is hosted on the network.

Method 3: Use a Barracuda Load Balancer or Barracuda Load Balancer ADC. This deployment makes sense if your network requires dynamic traffic load balancing. In this case, your client browsers will proxy traffic to a virtual IP address - the load balancing device - which then load balances traffic to the Barracuda Web Security Gateways. The Barracuda Load Balancer provides failover and dynamic traffic

load balancing.

Method 4: Use Multiple A Records. For each Barracuda Web Security Gateway in the cluster, make an A record in your DNS server with the same hostname. Depending on what IP address to which the user',s machine resolved the hostname, they may get a proxy error.

Data Propagated to the Linked Systems

Linking systems together not only makes it easier to manage multiple Barracuda Web Security Gateways, but it also provides 100 percent redundant coverage of the propagated configuration and policy (Block/Accept) data. Table 2.2 identifies the data that is propagated to the other linked systems when a new system joins.

Propagated Data	Data Not Propagated
System settings (global and domain) configured through the web interface. This includes the block/accept filters and, with version 11.0 and higher, SSL Inspection settings.	• System IP configuration (IP address, subnet mask, default gateway, and DNS server) configured on the **BASIC > IP Configuration** page. • System password and time zone as configured on the **BASIC > Administration** page. • Local users. • Cluster hostname and cluster local host map configured on the **ADVANCED > Linked Management** page. • Static route settings as configured on the **BASIC > IP Configuration** page. • Branding image and image URL as configured on the **ADVANCED > Appearance** page. • VLAN configuration settings as configured on the **ADVANCED > Advanced Networking** page. • Source-based routes as defined using the **IP Routing** feature. See the **ADVANCED > Advanced Networking** page. • SSL Inspection Certificates as configured on the **ADVANCED > SSL Inspection** page.

Switching a System to Standby Mode

You can also use the **ADVANCED > Linked Management** page to switch a linked system from *Active* to *Standby* mode. When a system is in *Standby* mode, it does not synchronize its configuration with the other active systems in the cluster, but can pull the configuration from another system that is set to *Active*.

Barracuda recommends switching a system to *Standby* mode when you need to:

- Upgrade the firmware of all systems in a cluster. If a system is part of a cluster, Barracuda recommends changing the system's mode to *Standby* before you upgrade its firmware, and then repeat this process on each system in the cluster. After the firmware on each system has been upgraded, you can then change the mode on each system back to *Active*. Changing a linked system to *Standby* mode before upgrading prevents a system on a more recent firmware version from trying to synchronize its configuration with a system on an earlier firmware version.
- Perform maintenance that requires a system to be powered down or disconnected from your network. For example, if you need to physically move a Barracuda Web Security Gateway, you should change its mode to *Standby* so the other systems in the cluster do not try to synchronize their configuration while the system is down.
- Configure any Barracuda Web Security Gateway to pull its configuration from a system whose mode is set to *Active*, and changes made to this system (on *Standby*) are not synchronized to the cluster. For example, a use case where there is ONE system designated as the 'central controller' of the configuration for all of the systems in the cluster. See the next section regarding this configuration.

Centralized Management Across a Cluster

You can choose to designate one system in the cluster as the 'controller' if you only want to make configuration / policy changes to one system. These changes then automatically propagate to the others in the cluster. For details on this configuration, see Centralized Linked Management of the Barracuda Web Security Gateway.