High Availability and the Barracuda Web Security Gateway

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

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

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 Networks 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 Networks Technical Support for configuration assistance.

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.