How to Prevent Users from Circumventing Barracuda DNS Servers Using Firewall Rules

https://campus.barracuda.com/doc/78153739/

This article explains steps administrators can take to prevent users on the network from circumventing of Barracudas DNS nameservers.

Savvy internet users may try to bypass Barracuda DNS nameservers you have configured if your network security configuration allows them to change the local DNS IP server from the Barracuda IP address. This would bypass the security policies you have configured in Barracuda Content Shield and may leave your network vulnerable. However, it is possible to not allow those other DNS services through your network firewall to the Internet, which will prevent these users from circumventing policies.

Most routers and firewalls will allow you to force all DNS traffic over port 53, thus requiring everyone on the network to use the DNS settings defined on the router/firewall (in this case, Barracuda DNS nameserver). The preferred recommendation is to forward all DNS requests to go to the Barracuda IP address listed below. This way, you simply forward users' DNS requests without them knowing, instead of having the possibility of someone manually configuring DNS and having it not work.

Create two firewall rules to only allow DNS (TCP/UDP) to Barracuda DNS nameservers and restrict all other DNS traffic to any other IP addresses. Add this policy to the firewall that is at the furthest edge of your network. The rules would look something like this:

> ***ALLOW*** TCP/UDP IN/OUT to <Barracuda DNS nameserver IP> on Port 53
>
> and
>
> ***BLOCK*** TCP/UDP IN/OUT all IP addresses on Port 53

The first rule takes precedence over the second rule. Put simply, any requests to Barracuda will be allowed and any requests to any other IP address will be blocked.

- Depending on your firewall configuration interface, you may need to set up a separate rule for each of these protocols, or one rule which covers both.
- The rule can be applied on either the firewall or the router, but is normally best placed on the device most at network edge. A similar rule could be applied to software firewalls installed on a workstation as well, such as the built-in firewall on Windows or Mac OS X.

For help with creating firewall rules on a Barracuda CloudGen Firewall, see Firewall Access Rules. For the Barracuda NextGen Firewall, see Firewall Rules. If you are not using a Barracuda firewall solution, note that each firewall or router has a unique configuration interface and these vary greatly. If you

are uncertain, you should check your router or firewall documentation or contact the manufacturer to see if this is possible with your device.