

## Best Practices for DNS Filtering Deployment

<https://campus.barracuda.com/doc/94541501/>

See also [Best Practices for Creating DNS Policies](#).

If you are using both DNS Filtering and the [BCS Agent](#):



The BCS agent periodically checks to see if a DNS response is coming from Barracuda Networks DNS Proxies. When it does, the agent tries to route the DNS request to a default public DNS server (8.8.8.8) to prevent multiple filtering. This is to prevent clashing of web policies on the DNS Proxies and the BCS Agent.

In some cases, a request can be made to Barracuda Networks Support to specify a different local DNS to resolve DNS queries when the BCS agent detects that a DNS response is coming from Barracuda Networks DNS Proxies.

### Adding a DNS Location

When you click **ADD LOCATION** on the **DNS Filtering** page, you are initially prompted to select one of two methods of how to specify an outbound IP address for clients. Barracuda Content Shield policies that you configure are then applied according to the outbound IP address associated with each client. The two methods are:

- **Static IP Address** – If the outbound IP address for each client is static (remains the same, as opposed to dynamic), choose **Manually configure outbound IP addresses**. *Barracuda Networks recommends choosing this deployment, if appropriate, since it is the most simple.* Note that if you are entering an IP range, use a 32 bit mask.

Network		
Outbound IP Address ^	Prefix	Remove
192.168.1.1/24	/32	
192.168.1.1	/32	

- **Dynamic IP Address** – If the service provider issues a dynamic IP address (which potentially changes periodically), choose **Automatically update the outbound IP addresses**. This leads

you to the [Barracuda Dynamic IP Address Updater](#) installation at the end of the wizard. The Barracuda Dynamic IP Updater is a tool that installs on a client and runs periodically to inform the BCS DNS proxy server if the outbound IP address for your network has changed.

**Important:** With DNS proxy setups, the user will see an SSL error that they need to accept in order to proceed.

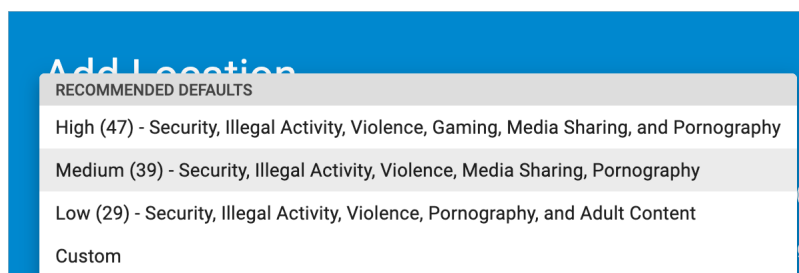
For locations with Dynamic Outbound IP address and DDNS usage:

- For DDNS, install on a machine that doesn't switch networks.
- Install only on one machine that's connected to network you wish you manage.

Note that **you can simulate groups** by segregating users under different external IP addresses. This provides the option to apply different policies to different groups. For example, the *Students* group could be assigned a *High* security policy while the *Faculty* group could have a *Low* security policy.

## Creating Policies

When creating a policy for a location, Barracuda Networks recommends beginning by selecting the *Medium* security option. See [Best Practices for Creating DNS Policies](#) for more details and examples.



## Figures

1. ipRange.png
2. Recommended Medium Policy.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.