Forward Proxy Deployment of the Barracuda Web Security Gateway

https://campus.barracuda.com/doc/6160394/

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

A key advantage of this deployment is that initial setup does not require any interruptions to your network traffic. However, be aware that, in a forward proxy deployment, only HTTP/HTTPS Internet traffic passes through the Barracuda Web Security Gateway. As such, in this mode the Barracuda Web Security Gateway does not scan non-HTTP traffic for viruses and spyware, nor does it block applications. See the section *Limitations of this Deployment Type* below for more details. **Note that you must use either this deployment or** WCCP Deployment **for the Barracuda Web Security Gateway Vx**.

How This Deployment Works

The Forward Proxy deployment uses a proxy, the Barracuda Web Security Gateway, as an intermediary between a client and the Internet to protect the client from being visible from the Internet. After the Barracuda Web Security Gateway processes clients' HTTP/HTTPS requests, it sends the requests out directly to the Internet. When deployed as a forward proxy, the Barracuda Web Security Gateway shows all HTTP/HTTPS traffic as coming from its own IP address instead of from the individual client IP addresses as is done in the inline pass-through deployment.

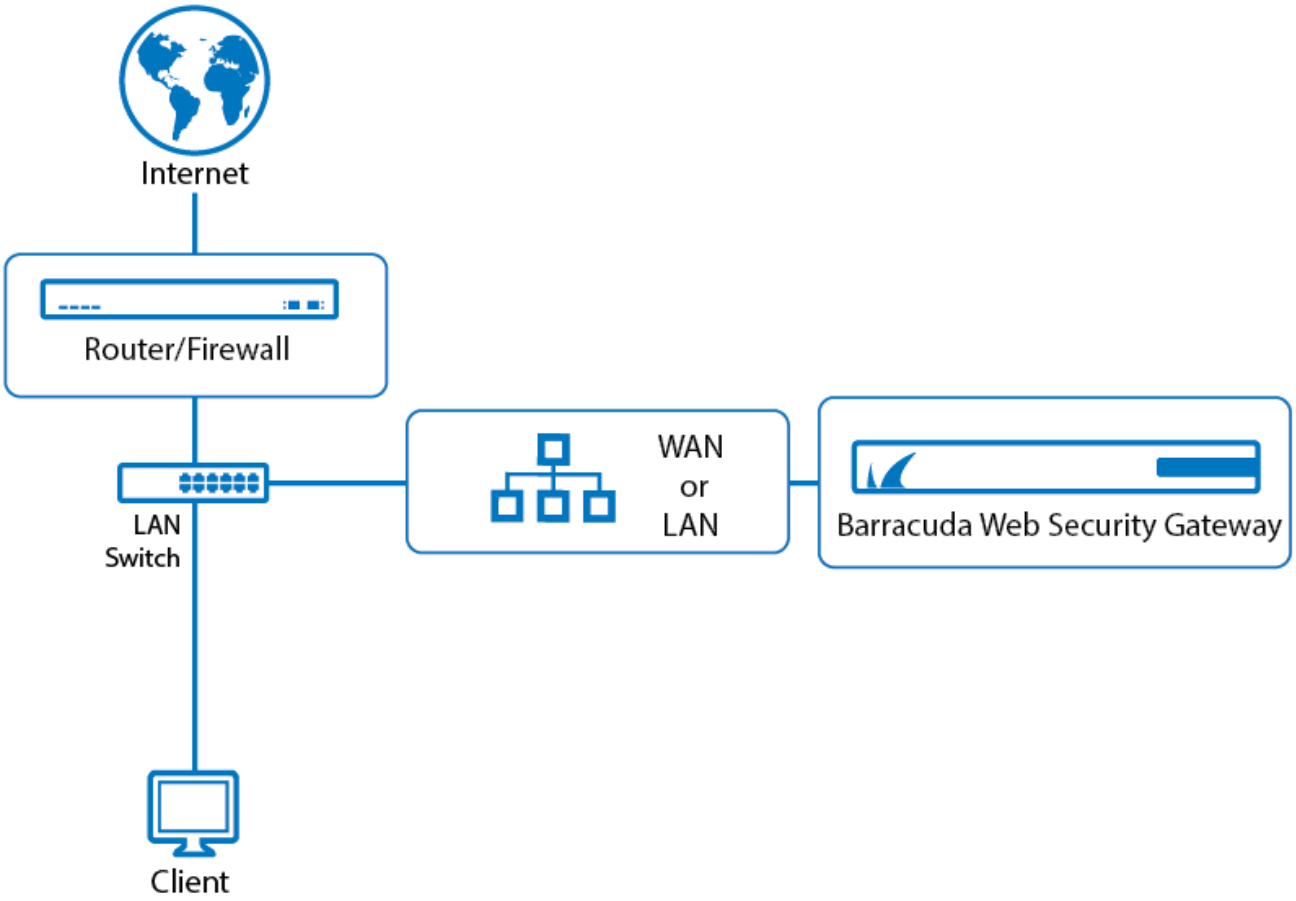
Barracuda Networks recommends deploying the Barracuda Web Security Gateway in forward proxy mode in the following situations:

- You need to replace an existing forward proxy (such as Microsoft ISA Server) with the Barracuda Web Security Gateway.
- You do not want the Barracuda Web Security Gateway to reside inline with all your network traffic and are satisfied with the system **only scanning HTTP/HTTPS traffic** for viruses and spyware.

Note that you can deploy a hybrid of forward proxy and inline for specific use cases such as, for example:

- A mixed environment of terminals and desktops. You can proxy traffic from the terminals to the Barracuda Web Security Gateway IP address as described below, while connecting the desktops inline using the LAN/WAN bridge, enabling filtering of application traffic from the desktops as well as HTTP and HTTPS traffic from both the desktops and the terminals. See Inline Pass-Through (Transparent) Mode Deployment for more information on inline deployment.

The figure below illustrates a basic installation using the Forward Proxy Deployment.



Configuring Forward Proxy Mode

To set up the Barracuda Web Security Gateway as a forward proxy without placing it inline, you must manually direct all outgoing web traffic you want filtered through the Barracuda Web Security Gateway. You can specify specific types of traffic to bypass the Barracuda Web Security Gateway either manually in the browser proxy settings, or by pushing out a PAC file with a GPO.

To configure Forward Proxy Mode:

1. Connect either the WAN or LAN port of the Barracuda Web Security Gateway to the same switch as the network gateway (just one network hop away).
2. Do one of the following to proxy traffic from client computers to the Barracuda Web Security Gateway:
    1. In the Advanced/Network settings of client browsers, using the manual proxy setting, enter the IP address of the Barracuda Web Security Gateway as the HTTP Proxy and 3128

for the port. If you wish to use a different port, you can change the **Proxy Port** setting on the **ADVANCED > Proxy** page of the Barracuda Web Security Gateway web interface.
OR

2. Create a PAC file and use a GPO to push it out to all client browsers. The PAC file provides lots of flexibility as to which traffic is filtered and can provide load balancing. See Using a PAC File below.

3. From the **BASIC > IP Configuration** page of the web interface, set the **Operating Mode** to **Active**. Note that **Audit** mode **does not apply to this deployment**; in either **Audit** or **Active** modes, traffic will be logged and policy will be applied.

Limitations of this Deployment Type

Because the Barracuda Web Security Gateway only scans outbound HTTP/HTTPS traffic in this deployment, the system *cannot* perform the following functions in Forward Proxy mode:

- Block access to applications listed on the **BLOCK/ACCEPT > Applications** pages.
- Block access to applications that use the destination IP address specified on the **BLOCK/ACCEPT > IP Block/Exempt** page.
- Block access to applications that use the destination port specified on the **BLOCK/ACCEPT > IP Block/Exempt** page.
- Inspect outbound traffic for spyware infection activity.
- Scan non-web based traffic for viruses and spyware.

Proxying Web Traffic Using a WPAD or PAC File

You can use a WPAD or PAC file with your Barracuda Web Security Gateway instead of setting the client browser proxy to the Barracuda Web Security Gateway IP address on port 3128. You can create a custom Web Proxy Auto-Discovery (WPAD) or Proxy Auto-Configuration (PAC) file that specifies a URL to use for the proxy, and either:

- Use a windows GPO to push out proxy settings for some or all HTTPS traffic to client browsers.
- OR -
- Upload the WPAD or PAC file to the Barracuda Web Security Gateway. This feature is available with the Barracuda Web Security Gateway version 14.1 and higher.

This method of proxying web traffic to the Barracuda Web Security Gateway has the following advantages:

- You can automatically configure all client browsers with proxy instructions rather than manually configuring them.
- A PAC file affords lots of flexibility since you can optionally proxy specific traffic - domains,

URLs, internal versus external traffic - to a specific Barracuda Web Security Gateway, or directly to the internal or external internet.
- You can set up load balancing of web traffic and failover (with multiple Barracuda Web Security Gateways) in case one system is not available.

If you are running version 14.1 or higher, you can upload your WPAD or PAC file: specifies a URL to use for the proxy.

1. Go to the **ADVANCED > Proxy** page.
2. In the **WPAD/PAC Configuration** section, click **Browse** to find the file on your system to upload.
3. Click **Upload Now** to upload the file to the Barracuda Web Security Gateway.
4. To access the file you uploaded:
   - For a PAC file, use `http://IP of the Barracuda Web Security Gateway:8000/proxy.pac`
   - For a WPAD file, use `http://IP of the Barracuda Web Security Gateway:8000/wpad.dat`

See also Proxying Web Traffic Using a PAC File for details and examples of what you can do with a PAC file, and https://findproxyforurl.com for more info. on how to create a WPAD or PAC file.

Figures