Inline Pass-Through (Transparent) Mode Deployment

https://campus.barracuda.com/doc/6160452/

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

Inline pass-through is the recommended type of deployment for the Barracuda Web Security Gateway appliance (not supported by the Barracuda Web Security Gateway Vx virtual machine) because it provides the strongest level of protection against spyware. In this deployment, the Barracuda Web Security Gateway is directly inline with your core Internet network components, and all network traffic to the Internet passes through the Barracuda Web Security Gateway. In this mode, your Barracuda Web Security Gateway is able to:

- Filter and scan all Internet traffic requests
- Perform content filtering and scan downloads for spyware and viruses
- Filter web-based and non web-based applications
- Detect and block outbound spyware protocol requests
- Scan all outbound traffic for spyware activity on all ports to detect infected clients
- Perform SSL Inspection – i.e. scanning of HTTPS traffic at the URL level - see Using SSL Inspection With the Barracuda Web Security Gateway for details and requirements. Available on the Barracuda Web Security Gateway 310 and higher.

> **Use case: A hybrid of forward proxy and inline deployment**
>
> Note that you can deploy a hybrid of forward proxy and inline for specific use cases. A typical example is a mixed environment of terminals and desktops. If you want to apply different browsing policies to each group of users, you can proxy traffic from the terminals to the Barracuda Web Security Gateway IP address on port 3128, 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. See also Forward Proxy Deployment of the Barracuda Web Security Gateway. In this scenario you can also use different authentication mechanisms for each group, as described in Hybrid Authentication Mechanisms.

Inline pass-through deployment requires you to have an understanding of your network topology because even though the Barracuda Web Security Gateway acts as a proxy, it does not participate in routing protocols. As a result, you may need to set up static routes in your Barracuda Web Security Gateway so it knows how to properly route traffic. **Do not set the Barracuda Web Security Gateway as a gateway IP address for a PC for this deployment; the Barracuda Web Security Gateway should only be set as a gateway IP address for a PC when using as a direct proxy setup.**
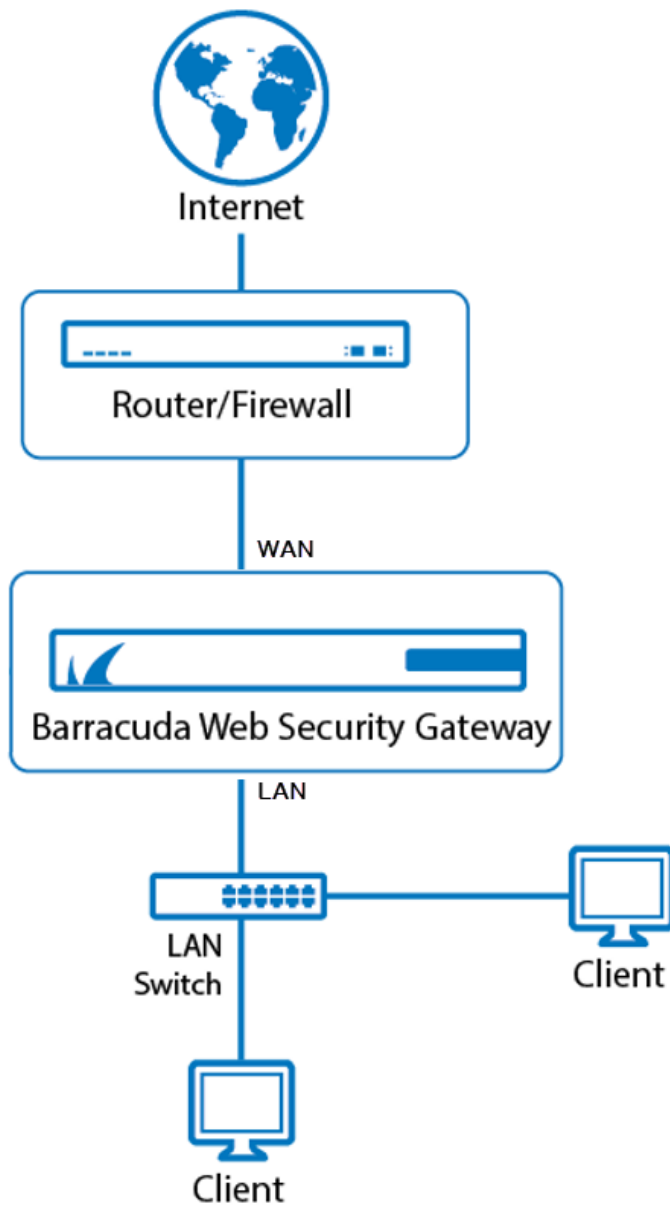
Per Figure 1 below, you'll typically route traffic from your switch or router, via the Barracuda Web Security Gateway, to the internal IP address of your firewall or another device used for routing on the

WAN side of the Barracuda Web Security Gateway.

The following table describes the advantages and disadvantages of deploying your Barracuda Web Security Gateway in inline pass-through mode.

Advantages	Disadvantages
Supports application blocking.	May require setting up static routes in your Barracuda Web Security Gateway.
Supports automatic pass-through mode in the event of a system failure (model 310 and above).	Initial setup requires an interruption to network traffic while you make necessary cabling changes.
Does not require users to configure proxy server settings in their web browser.	
Uses perimeter transparency mode that exposes client IP addresses (supports corporate firewall rules).	

Figure 1: Inline Pass-through Deployment.

Internet

Router/Firewall

WAN

Barracuda Web Security Gateway

LAN

LAN
Switch

Client

Client

Figures

1. inline_BWSG.png