Deployment Best Practices

https://campus.barracuda.com/doc/55312401/

Deployment Considerations

For best security, deploy the Barracuda Web Application Firewall behind a firewall and consider limiting access to the admin interface. For more information, refer to the **Controlling and Restricting Access** section in the Configuring Access to the Barracuda Web Application Firewall article.

The Barracuda Web Application Firewall can be deployed in 3-modes:

Proxy Mode	
Two-Arm Proxy	In Two-arm proxy mode, the Barracuda Web Application Firewall is deployed in-line, using both the physical ports (WAN and LAN) of the device. This is the recommended configuration as it provides the best security.
One-Arm Proxy	Deployed in One-armed proxy mode, incoming and outgoing network traffic to the Application Firewall passes through the WAN port. Virtual IP addresses of the services on the Web Application Firewall and back-end real server IP addresses are on the same subnet. A high level of security is achieved with this configuration, but a network firewall is recommended to restrict direct access to the back-end servers.
Bridge Mode	
Bridge Path	Deployed as an in-line Bridge Path, the Barracuda Web Application Firewall uses the same address for the VIP and back-end server, so data is passed through to the Web Application, including potential attacks, even as the security checks are performed. This configuration does not require changes to the existing network infrastructure but the WAN and LAN need to be on a different switch.

For more information on deployment modes, see Choosing Your Deployment Mode.

Deploy in Proxy mode, preferably as a Two-Arm Proxy

Two-Arm Proxy is the industry accepted best practice and is inherently more secure than bridge mode deployments. Proxy mode deployments give administrators the ability to protect against critical attacks like session spoofing, etc. The key capabilities of Barracuda Web Application Firewall Proxy deployments that are not available in Bridge Mode architectures include:

- Real Server Load Balancing
- Connection Pooling
- Content Rules
- Caching

- Compression

Cluster for High Availability (HA) and redundancy

Due to the 24/7 nature of web traffic, it is important that any deployments in line with the data path have added redundancy. The Barracuda Web Application Firewalls configured in HA clusters will automatically synchronize security and network configurations between the clusters to provide seamless failover in response to disruptions. For more information on clustering, see High Availability.