Choosing Your Deployment Mode

https://campus.barracuda.com/doc/4259951/

Reverse Proxy Deployment of the Barracuda Web Application Firewall

Reverse proxy deployments accept traffic on the virtual IP address and proxy the traffic to the back-end server network behind the Barracuda Web Application Firewall. Reverse proxy options include:

- Two-Arm Proxy Deployment
- One-Arm Proxy Deployment

Two-Arm Proxy Deployment

The Barracuda Web Application Firewall is in-line with the web servers; it intercepts and inspects incoming and outgoing traffic, preventing attacks from reaching the web servers and preventing the leak of sensitive data to the requesting clients. Apart from web application security, this mode also allows all delivery acceleration features like server/application load balancing and tcp connection pooling to be employed. For details on configuring this deployment type, see Configuring Two-Arm Proxy Mode. This deployment mode is supported by the Barracuda Web Application Firewall virtual appliance (see Virtual Deployment).

How This Deployment Works

The Two-Arm Proxy deployment is the recommended mode for initial deployment. The Barracuda Web Application Firewall is shipped in Proxy mode. In a Two-Arm Proxy configuration, the Barracuda Web Application Firewall is deployed in-line using both physical ports (WAN and LAN) of the device. This configuration is recommended because it provides the best security and can utilize all traffic acceleration features. Deploying in Two-Arm Proxy requires changes to the existing network infrastructure.

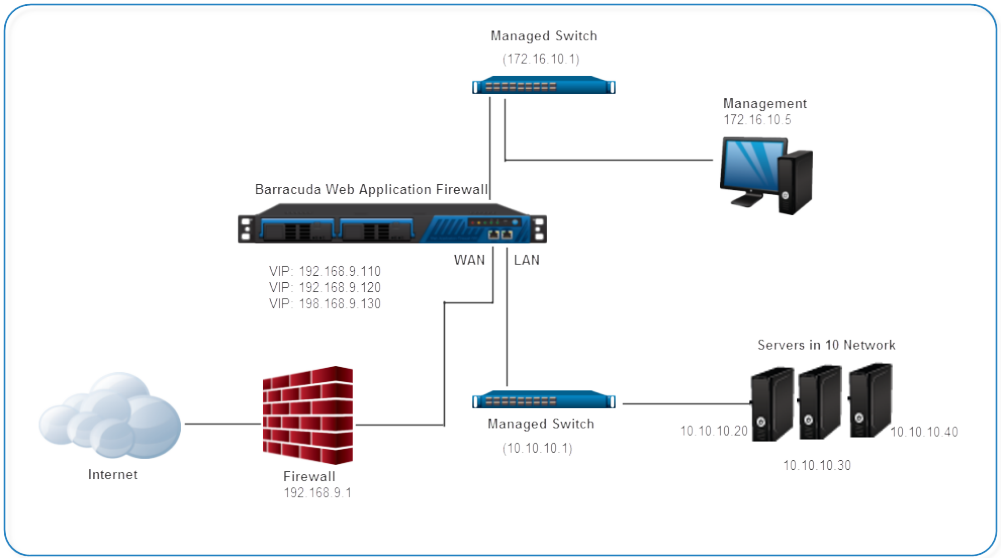
Two-Arm Proxy deployment requires the WAN and LAN interfaces of the Barracuda Web Application Firewall to be on separate logical networks.

- The servers must be on a private network connected through a switch on the LAN port.
- The WAN port connects to the Internet facing switch that connects to a router/network firewall which routes the traffic to the Internet.

Each server in the private network is assigned a virtual IP address on the Barracuda Web Application Firewall (for example, **192.168.9.110**, **192.168.9.120**, and **192.168.9.130** in Figure *Sample Two-Arm Proxy Network Layout*). The virtual IP addresses should be accessible from the Internet, routed to the WAN port via the switch connected to it. When a request is received by the Barracuda Web Application Firewall on a VIP advertised through the WAN port, it inspects and redirects it to the real

server on the private network via the LAN port. For example, the VIPs map to real servers **10.10.10.10**, **10.10.10.20**, and **10.10.10.30**. See Figure: *Sample Two-Arm Proxy Network Layout*.

Sample Two-Arm Proxy Network Layout:



Advantages and Considerations

The following table describes the advantages and considerations of deploying your Barracuda Web Application Firewall in Two-Arm Proxy mode.

Advantages	Considerations
Full feature availability including Load Balancing and Instant SSL.	Requires network changes to Server IP addresses and DNS mappings.
Most secure deployment choice since back-end servers are completely isolated.	Deployment requires cut-over of live services.
Fast High Availability failover.	Network reconfiguration required to restore network to original state.

One-Arm Proxy Deployment

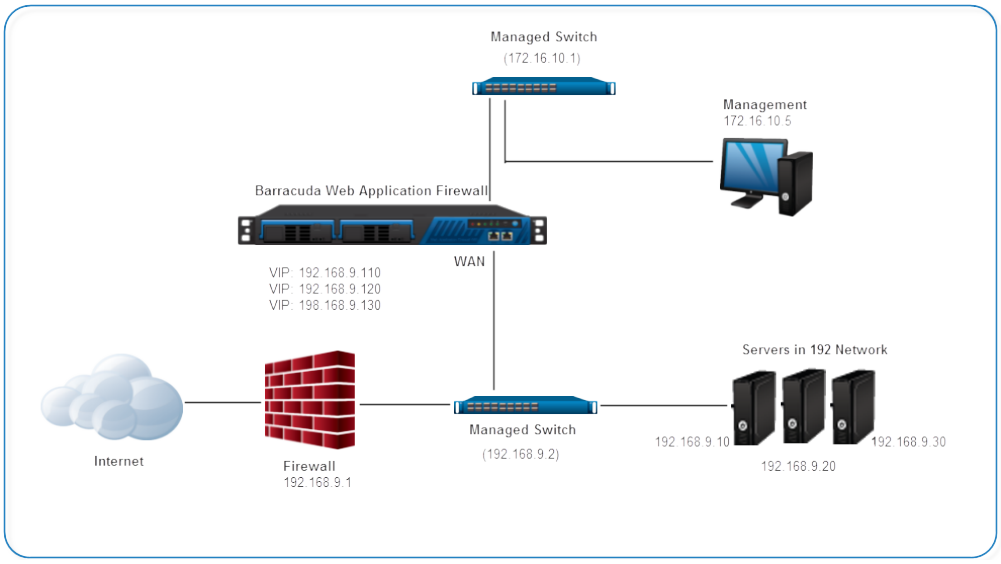
Allows the deployment of the Barracuda Web Application Firewall with minimal changes to the network configuration of the web servers. However, traffic from the upstream devices will have to explicitly pass through the Barracuda Web Application Firewall. For details on configuring this deployment type, see Configuring One-Arm Proxy Mode. This deployment mode is supported by the Barracuda Web Application Firewall virtual appliance (see Virtual Deployment).

How This Deployment Works

One-Arm proxy deployment requires minimal changes to the existing infrastructure. In this

deployment, the WAN port is used for both incoming and outgoing traffic passing through the Barracuda Web Application Firewall. One-Arm Proxy deployment allows the retention of alternate paths to access the servers. For example, this deployment configuration can be used to load balance HTTP/HTTPS traffic at the application layer, while letting SMTP and other traffic go directly to the server.

Sample One-Arm network layout:



Advantages and Considerations

The following table describes the advantages and considerations of deploying your Barracuda Web Application Firewall in One-Arm Proxy mode.

Advantages	Considerations
Requires fewer network configuration changes than Two-Arm Proxy. Network infrastructure and partitioning unchanged.	Requires DNS, IP address changes.
Allows multiple access paths to servers for testing.	Decreased throughput with only one port (WAN) used.
Integrates easily with existing enterprise load balancers.	Potentially compromises server security by providing direct server access, unlike Two-Arm Proxy configuration.

Bridge Mode Deployment of the Barracuda Web Application Firewall

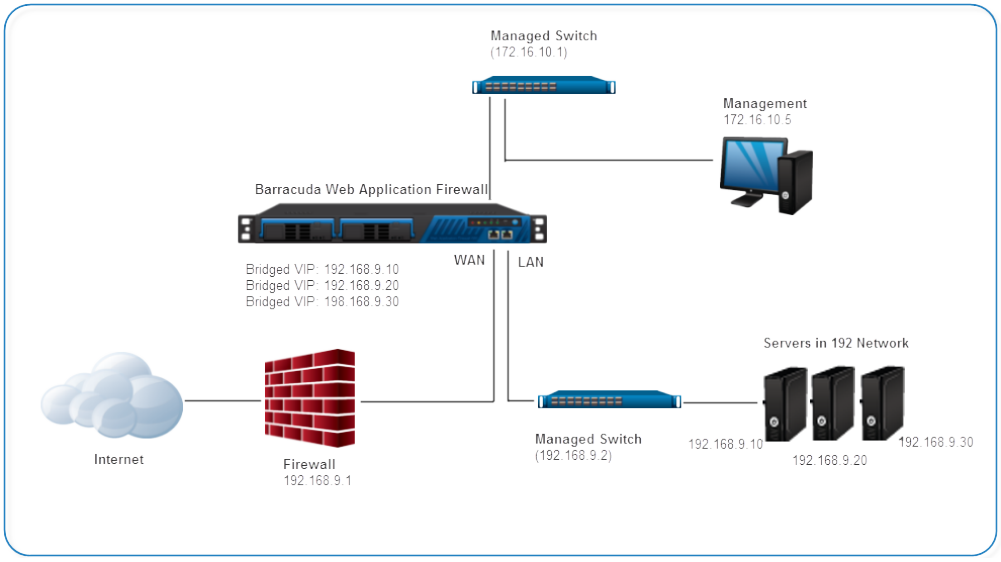
The Barracuda Web Application Firewall is inline with the web servers and acts as an L2 transparent bridge. It inspects only the traffic that is configured for inspection while bridging all other traffic.

Bridge mode deployment can be achieved with no changes to the network configuration of the upstream devices or web servers. For details on configuring this deployment type, see Configuring Bridge-Path Mode . **This deployment mode is *not* supported on the Barracuda Web Application Firewall virtual appliance** (see Virtual Deployment).

How This Deployment Works

In Bridge-Path deployment the Barracuda Web Application Firewall is located inline between the network firewall and the web servers, inspecting configured traffic and bridging any other traffic to the servers. Bridge-Path provides the easiest configuration scenario because it uses the same IP address for the VIP and back-end server, so it does not require changing the server IP addresses or DNS mappings. You can place the Barracuda Web Application Firewall inline with the existing IP address infrastructure and add servers without changing IP addresses. In a Bridge-Path deployment, the WAN and LAN interfaces must be on physically separate networks and the LAN interface must be on the same logical switch as the servers.

Sample Bridge-Path network layout:



Advantages and Considerations

The following table describes the advantages and considerations of deploying your Barracuda Web Application Firewall in Bridge mode.

Advantages	Considerations
Minimal network changes since the existing IP address infrastructure is reused.	Sensitive to broadcast storms and address resolution looping errors.
Real Servers keep existing IP addresses.	Less resilient to network misconfiguration.

	Features like Load balancing and TCP pooling are not available.

Figures

1. two-arm-proxy-mode.png
2. one-arm-proxy-mode.png
3. bridge-mode.png