iBoss Network Deployment Configuration Options

The iBoss provides its filtering functionality in a completely transparent fashion on the network. It does not segment a network, nor does it provide firewall or NAT capability which allows for easy deployment. The iBoss filters traffic passing between the LAN and WAN port. The iBoss will actively scan traffic applying filtering rules and intercepting traffic when necessary. This allows the iBoss to achieve very high filtering performance without affecting network topology. If using the iBoss in an Active Directory environment, NTLM can be used to transparently identify the user using their Active Directory credentials.

**Transparent Inline Filter (Recommended) - Figure 1**

Out of the box, the iBoss Web Filter is a true in line filter analyzing multiple streams for optimum performance. The iBoss Web Filter typically sits inline between your existing firewall and switch. With throughput speeds capable of reaching 1 Gbps on the models with Gigabit interfaces, iBoss Web filters can ensure powerful filtering without sacrificing network performance. In addition, optional Fiber, 10G, and Fail-Safe Bypass Interfaces are available.

**Tap Mode (Mirrored Span Port) - Figure 2**

In this mode, the iBoss Web Filter is connected to a mirrored span port on the network switch. This allows you place the iBoss off the network and still filter traffic.

**Inline Proxy Filter - Figure 3**

In this mode, requests made by the computers on the network are sent through the iBoss at which point the request is made by the iBoss on their behalf with filtering applied. This can be done by configuring the proxy settings within the browser through an Active Directory Group Policy Object or manually. In this mode, the proxy will analyze web requests. For applications to be analyzed, the iBoss must be placed inline on the network so that the iBoss can see the network streams. For Web 2.0 streams, the policy for that computer will be applied instead of the Active Directory proxy user.
**Non-Inline Proxy Filter** - Figure 4

In this mode, requests made by the computers are sent to the iBoss at which point the request is made by the iBoss on their behalf with filtering applied. This requires the proxy settings to be configured within the browser through an Active Directory Group Policy Object or manually. In this mode, the iBoss Web Filter is not inline and attached to the switch.

![Diagram of Non-Inline Proxy Filter](image)

**Multiple iBoss Web Filters on Redundant Firewall Paths** - Figure 5

Corporations with secondary networks for redundancy can implement one iBoss Web Filter inline behind each firewall path. The filtering settings can be synced between the two for redundancy using the remote management services (see figure 7 for example).

![Diagram of Multiple iBoss Web Filters](image)

**Dual-WAN Router Transparent Inline Filter** - Figure 6

When using a Dual-WAN Router with two Internet connections, simply implement the iBoss Web Filter inline between the Dual-WAN Router and the switch.

![Diagram of Dual-WAN Router Transparent Inline Filter](image)
Multiple iBoss Web Filters with External Enterprise Reporter - Figure 7
The iBoss Web Filters can be implemented deeper within the network to filter portions of the network. This clustered method allows for better performance as it offloads the tasks to multiple units. The filtering settings can be synced between the two for redundancy using the remote management services (see figure 7 for example).

Multiple Locations with Filters Synchronized Through Remote Management - Figure 8
Filtering settings between devices can be synced with each other using the Remote Management Interface. This allows you to quickly and easily manage multiple locations using the iBoss Web Filters.
Distributed Filtering Platform (DFP) Clustering - Figure 9

The iBoss distributed filtering platform (DFP) provides support for the most distributed complex networking topologies. When deployed using the DFP, several iBosses across unsecure Internet connections can be clustered to a central iBoss master. All settings are configured within the master typically located at a datacenter or co-location facility. Settings from the primary master are automatically distributed to members of the cluster over a secure AES encrypted connection using push real-time technology.

It is not necessary for the primary iBoss to be at a central datacenter. Any iBoss in the cluster can be designated a master and central policy configuration point. Although locations may be distributed across the globe, policies can be applied via groups to iBosses that are part of the cluster. This provides a seamless and centralized control of policies as well as consolidated reporting across the enterprise.
Additional Management Interface - Figure 11

An additional management network interface can be added to allow for configuration of the iBoss settings. This is useful for having the iBoss filter a different subnet than the one that you will be managing the settings from. In this configuration, the two on-board network ports will be filtering traffic for the network and the additional management interface would be connected to the network which you will be able to access the configuration of the iBoss.

![Management Interface Diagram](Continued)

Additional Bypass Interface - Figure 12

An additional management network interface can be added to allow for configuration of the iBoss settings. This is useful for having the iBoss filter a different subnet than the one that you will be managing the settings from.

![Bypass Interface Diagram](Continued)

Small Business iBoss Pro Series Firewall Deployment - Figure 13

Small Business networks can use the iBoss Pro as a firewall for their network. In this mode, the iBoss is the firewall/router and gateway for the network. iBoss Pro units can also have their settings synced using Remote Management (as shown in Figure 7).

![Firewall Deployment Diagram](Continued)

Small Business iBoss Pro Series Transparent Deployment - Figure 14

Small Business network already setup with a firewall/router can implement the iBoss Pro transparently between their existing firewall and switch. This allows for easy deployment without having to change any network settings for the computers already connected to the network. In this mode, the iBoss Pro works as a transparent bridge and filters the traffic that passes through it.

![Transparent Deployment Diagram](Continued)