poliWall® TIG™

Frequently Asked Questions

Can I pre-set Policies on the PoliWall before removing the RiskAnalytics device and then make the switch?

Yes, there are three ports on the PoliWall. An outside port that connects to your incoming traffic, typically your border router; an inside port that connects to your firewall; and a management port. You can connect to the management port and pre-set policies and your resource group configuration prior to installation in your network. The PoliWall also allows you to set the appliance in bypass mode so that traffic simply flows through.

Do I need a designated IP for the PoliWall?

Yes, the PoliWall has an admin port that must be given an internal IP, however the inside and outside ports do not need addressing as they are simply a bridge pair.

I have a firewall, what benefits will a PoliWall add?

- Reduce your cyber risk exposure by leveraging threat intelligence to block massive volumes of known threats in real time on any size enterprise or business network.
- Operationalize threat intelligence easily and in a low touch manner leveraging PoliWall's automated capabilities.
- Free up your security staff to focus on higher priority threats.
- Improve the performance and ROI of your firewalls and intrusion prevention systems.

What happens if there is an equipment failure, will it impact my network?

No, the PoliWall is equipped with a built-in mechanical bypass card. If the PoliWall goes down for any reason the traffic will pass with no impact to your network.

Do I need to reconfigure my network in any way to do the installation?

No, the PoliWall is a Layer 2 bridging device. You do not need to reconfigure anything in your network to use the PoliWall blocking capabilities.

What are the blocking options of the PoliWall?

- Country blocking by simply clicking an interactive world map
- Blocking by threat intelligence by simply clicking a box for the category you wish to block for each Resource Group, 17 different threat categories are available, adjust your acceptable risk tolerance for each group with an intuitive slider bar
- Block industry and government provided blacklists
- PoliWall subscriber based bad domain lists
- Globally apply whitelists and exception lists to allow necessary traffic from blocked areas or lists.

BANDURA® SYSTEMS

bandurasystems.com/cyberedge

+1.855.765.4925 ext. 4 • cyberedge@bandurasystems.com • support@bandurasystems.com