poliWall® TIG™

BANDURA® SYSTEMS

DATA SHEET

Benefits

- Significantly reduce your attack surface using threat intelligence to more effectively block known threats and unwanted traffic.
- Reduce staff burden by eliminating alert noise and manual workload.
- Increase the value of threat intelligence by taking action.
- Get more out of your firewall by eliminating noisy known threats ahead of it.

Threat Intelligence-Driven Protection

PoliWall® TIG™ enables companies of all sizes to leverage the power of Threat Intelligence (TI) to more effectively and efficiently protect networks against known threats and unwanted traffic. No longer is Threat Intelligence just a hunt/remediate tool. Now, all the power of massive Threat Intelligence feeds can be deployed ahead of the network — working like a shield to block cyberattacks inbound, preventing data leakage outbound — and significantly reducing the load on the firewall.

The Problem

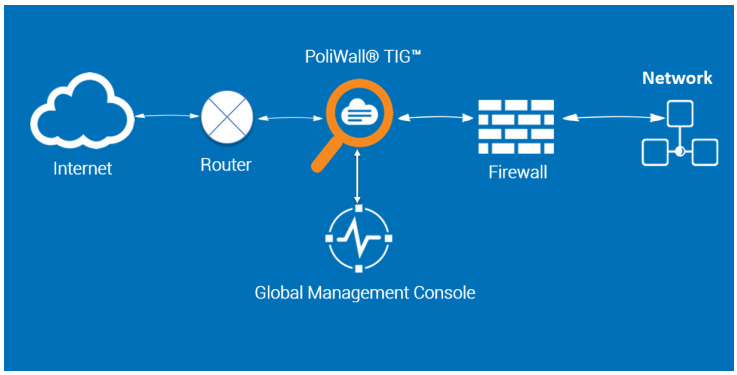
At any moment, there are over 10 million known threats. Existing security controls, like firewalls, can typically only process 100,000 threat indicators before significant performance issues occur. This leads to security coverage gaps with users forced to operate with only a subset of available threat intelligence. This is compounded by the challenges of manually updating and maintaining threat intelligence with firewall rules and Access Control Lists (ACLs).

PoliWall TIG to the Rescue

Bandura pioneered Threat Intelligence Gateway (TIG) technology in partnership with the U.S. Department of Defense. PoliWall TIG is purpose-built to deliver threat intelligence-based protection at scale. PoliWall TIG sits in front of your firewall filtering traffic against a massive volume of threat indicators (IPs and domains) with virtually no latency. PoliWall TIG is easy to deploy and manage enabling organizations of all sizes to harness TI power!

Key Features

- **Threat Intelligence with no limits.** PoliWall TIG comes out of the box with millions of continuously refreshed threat indicators (IPs and domains) from multiple sources and can filter traffic against over 100 million unique threat indicators with virtually no latency. Traffic can be filtered by threat intelligence category (Command & Control, Botnets, Tor/Anonymizers, etc.), Country, Autonomous System Number (ASN) or any combination.
- **Automated Threat Intelligence that is easy to use.** Threat feeds are automatically updated in near real time and policies are automatically applied. PoliWall's automation capabilities improve security and increase staff productivity.
- **Open platform easily integrates with additional threat sources and systems.** Want to integrate existing or additional threat feeds into PoliWall? Not a problem! PoliWall is an open platform that supports STIX and TAXII making it easy to integrate additional threat feeds. PoliWall can also be easily integrated with other systems like Threat Intelligence Platforms and SIEMs.



- **Policy management as granular as you want through an intuitive user interface.** PoliWall TIG has flexible policy management capabilities that scale to the needs of the user. Leveraging PoliWall's automation capabilities, it can be deployed in a low touch "set it and forget it" mode. For more sophisticated enterprises, PoliWall offers robust, granular policy management capabilities. No matter which end of the spectrum you fall on, this is all easily accomplished through an intuitive user interface.
- **Flexible deployment options and centralized management.** PoliWall TIG can be flexibly deployed as a traditional appliance or as a virtual machine (VM) in private and public cloud environments. Our global management console enables centralized management and reporting for multiple PoliWall deployments regardless of form factor.

www.bandurasystems.com
+1.855.765.4925 sales@bandurasystems.com

poliWall® TIG™

MODEL COMPARISON	B-SERIES	E-SERIES	M-SERIES	X-SERIES	Z-SERIES
NETWORKING					
Bridging Interface	Bypass Mode 1 Gbit Copper RJ45	Bypass Mode 1 Gbit Copper RJ45	Bypass Mode 1 Gbit Copper RJ45	Bypass Mode 1 Gbit Copper RJ45 or 1 Gbit Short-Run Fiber	Bypass Mode 10 Gbit Copper RJ45 or 10 Gbit Short-Run Fiber
Redundant Bridge Pairs	Not Available	Not Available	Two Bridge Pairs Active/Standby Active/Active	Two Bridge Pairs Active/Standby Active/Active	Two Bridge Pairs Active/Standby Active/Active
Management Interface	10/100/1000 Copper RJ45	10/100/1000 Copper RJ45	10/100/1000 Copper RJ45	10/100/1000 Copper RJ45	10/100/1000 Copper RJ45
High Reliability	No	No	**Yes**	**Yes**	**Yes**
Throughput Limits	300 Mbps	600 Mbps	1 Gigabit	2 Gigabits	12 Gigabits
Concurrent Connections	500,000	500,000	1,000,000	2,000,000	2,000,000
HARDWARE					
Solid State Drive	No	No	**Yes**	**Yes**	**Yes**
Redundant Power Supplies	No	No	No	**Yes**	**Yes**
RAID	No	No	No	**Yes**	**Yes**
DIMENSIONS & POWER					
Appliance Dimensions	7.25W x 5.5D x 1.7H (in)	17W x 11.5D x 1.7H (in)	17W x 11.5D x 1.7H (in)	17W x 26.5D x 1.7H (in)	17W x 26.5D x 1.7H (in)
Mounting	Desktop	1U rack mount	1U rack mount	1U rack mount	1U rack mount
Shipping Weight	5 lbs.	15 lbs.	25 lbs.	35 lbs.	35 lbs.
AC Power	100-240 VAC	100-240 VAC	100-240 VAC	100-240 VAC	100-240 VAC

About Bandura Systems

Bandura Systems pioneered the Threat Intelligence Gateway (TIG) in part with the U.S. Department of Defense. Bandura's PoliWall™ is the most comprehensive, scalable and granular TIG platform on the market. Organizations worldwide use TIGs for the automation and control needed to operationalize hundreds of millions threat indicators blocking known threats before they even reach the network firewall. Underlying Bandura's robust technology are more than 50 issued and pending patents. To learn more about how Bandura's PoliWall TIG reduces an organization's attack surface, operationalizes threat intelligence and helps get more out of existing security investments, visit https://bandurasystems.com.

www.bandurasystems.com
+1.855.765.4925 sales@bandurasystems.com