poliWall® TIG™

BANDURA® SYSTEMS

ELECTION SYSTEMS PROTECTION

SECURE YOUR INTERNET-FACING ELECTION SYSTEMS

- Use advanced GEO-IP filtering to **block traffic** from unwanted countries like Russia and China, with threats updated daily
- Make your MS-ISAC, EI-ISAC, and other external threat intelligence **actionable and preventative**
- Improve **effectiveness & efficiency** of your network security and your security staff

In a world where government-targeted ransomware campaigns and international cyber-espionage are commonplace, electoral committees and organizations must take the utmost care in protecting the sensitive information they manage.

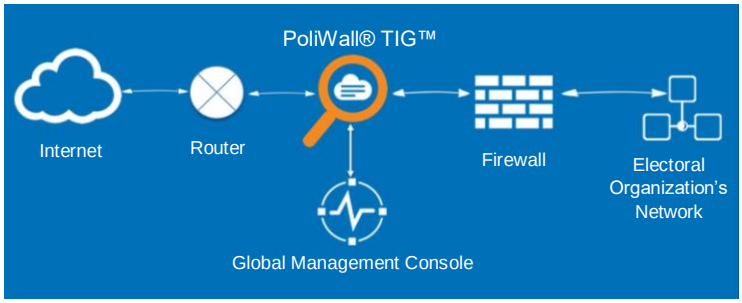
The firewall has long been a standard control point in protecting an electoral organization's network from outside threats. However, the exponentially increasing amount of cyber threats has overwhelmed firewalls leading to security coverage gaps and slower, less efficient firewalls that don't have the bandwidth to identify and block complex threats. This is leaving Internet-facing election systems, such as voter registration databases, open to risk.

While a typical firewall can process approximately 300,000 threat indicators (IPs and domains) at a time, there exist over **10M known threats** at any given moment.

AUTOMATICALLY BLOCK 10 MILLION+ KNOWN THREATS SO FIREWALLS CAN TAKE ON THE COMPLEX STUFF

Developed in part with the U.S. Department of Defense, the Bandura® Threat Intelligence Gateway – PoliWall® TIG™ – identifies and defends against **millions** of potentially harmful IPs and domains at line speeds ahead of firewalls.

By aggregating threat intelligence from ISACs and other threat feeds, the PoliWall identifies and **automatically** blocks threats from reaching your firewall. PoliWall also offers electoral organizations advanced GEO-IP filtering to block traffic from unwanted countries like Russia and China.



IMPROVE THE LIFE & EFFECTIVENESS OF YOUR FIREWALL

Use automated Threat Intelligence and advanced GEO-IP filtering to block:

- Unwanted inbound network scans and probes
- User access to malicious IPs and domains
- Botnets, malware, command & control communications, and sensitive data exfiltration
- Traffic from unwanted countries (updated daily)

Improve network security effectiveness & efficiency while reducing firewall costs:

- Block millions of known threats before they hit the firewall, significantly improving firewall performance
- Focus firewall deep packet inspection cycles on complex threats instead of being overwhelmed by noise
- Get more out of existing firewalls by extending firewall life and deferring expensive upgrades

Improve staff effectiveness & efficiency:

- Reduce alert fatigue from firewalls and other security systems
- Focus scarce staff resources on threats that matter

Get more out of MS-ISAC, EI-ISAC, and other external threat intelligence:

- Automate ISAC threat intelligence ensuring security defenses are up-to-date on the latest threats
- Put ISAC and other threat intelligence to work by proactively detecting and blocking threats

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