WATERFALL®

Stronger Than Firewalls

Securing ICCP WANs at Control Centers

Security, NERC CIP compliance, and operating cost benefits

- Stronger than firewall protection for Balancing Authorities and TSO's
- Never forwards messages at all, much less attack messages
- Support for central enterprise Network Operation Centers and SIEM integration
- High Availability and 1Gbps options
- Recognized by NERC CIP V5, draft CIP V6, ANSSI, ISA, IEC 62443, draft NIST 800-82 and other best-practice advice
- Common Criteria EAL4+ certified. Assessed for security by Idaho National Labs

Overview

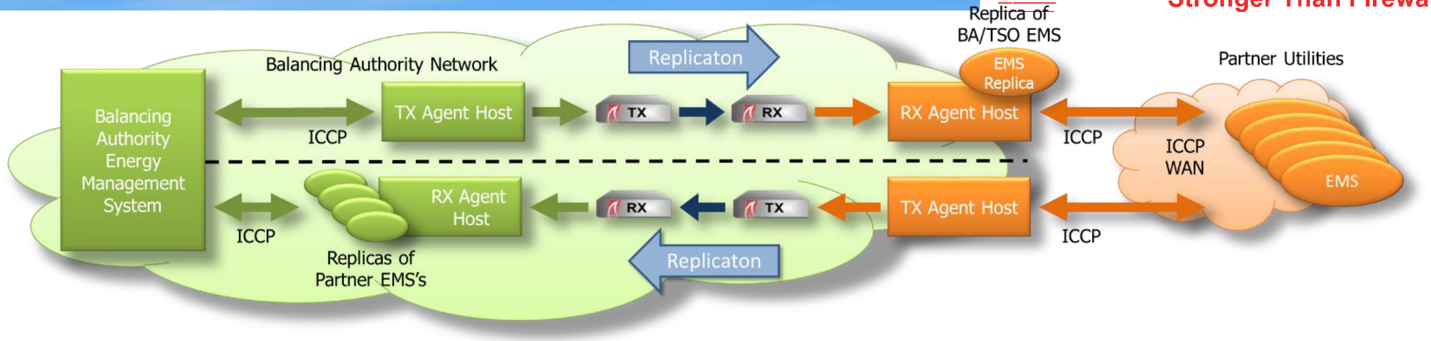
Control center operators rely on continuous communications with partner utilities to balance generating and transmission capacities against load. Partner utilities may be large or small, and may be more or less thoroughly secured against cyber attacks.

It is vital to the reliable operation of the power grid that Balancing Authority Energy Management Systems (EMS) and SCADA systems are protected from attacks originating in wide-area networks and in potentially-compromised partner networks. Waterfall's Unidirectional Security Gateway products provide stronger-than-firewall protections for EMS/SCADA networks, and unlike firewalls, defeat even the most modern, targeted, network-based attacks.

Stronger Than Firewalls

Firewalls are porous by design; they exchange messages between untrusted and trusted networks. While firewalls claim many mechanisms to filter benign messages from messages containing attacks, no such filter can ever be perfect. All firewalls permit attack messages to enter protected networks.

Waterfall's Unidirectional Security Gateways are a combination of hardware and software. Gateway hardware modules are physically able to send information in only one direction. Gateway software emulates the ICCP interfaces of EMS & SCADA servers, without ever forwarding ICCP messages. Two independent channels of hardware-enforced, unidirectional communications, each of which replicate and emulate ICCP servers rather than forwarding messages, together provide unprecedented levels of protection from network attacks to Balancing Authorities and Transmission System Operators.



Secure Communications with Partner Utility ICCP Servers

With Waterfall's Unidirectional Security Gateway solution, partner utilities and the Balancing Authority/TSO's EMS/SCADA systems never exchange messages with each other, but only with the gateways' ICCP replicas. Partner utilities exchange messages with Waterfall's faithful replica of the central, protected EMS/SCADA server, and the central server exchanges messages only with the gateways' replicas of the many partner utilities' ICCP servers. Waterfall maintains the replica servers as faithful, timely replicas of their original ICCP servers using frequent updates of entire snapshots of ICCP points and values, not individual ICCP messages. The replicas are maintained on sets of mutually-inaccessible unidirectional communications channels.

This stronger-than-firewalls solution can be deployed entirely at the Balancing Authority/TSO site, to protect the central EMS/SCADA system. Waterfall's solutions can also be deployed entirely at partner utilities, to protect their ICCP servers. The solution of course supports all of the high availability, management automation, central monitoring and diagnostics, and many other features essential to reliability-critical deployments.

NERC CIP Compliance

The NERC CIP V5 standards recognize the strength of Waterfall's Unidirectional Security Gateways by exempting unidirectionally-protected networks from many CIP V5 requirements. The gateways are hardware-enforced, unidirectional communications, rather than the "bi-directional" communications described in the NERC CIP V5 definition of "External Routable Connectivity" (ERP). In addition, the point-to-point, proprietary, non-routable protocol used across the unidirectional medium never forwards Internet Protocol (IP) messages or any other routable messages. As a result, Waterfall's gateways do not constitute an Electronic Access Point, or External Routable Connectivity, and so does not trigger costly requirements for networks with ERP, including requirements for Network Intrusion Detection systems, and other "malicious traffic inspection" systems.

Evolving Best Practices

Unidirectional Gateways are recognized as a stronger-than-firewalls best practice for defending networks by NERC CIP V5, the draft NERC CIP V6, ANSSI's 2014 Cybersecurity for Industrial Control Systems, ISA/IEC 62443-3-3 and the draft NIST 800-32 standards. The gateway solution is certified Common Criteria EAL4+, and Waterfall's Gateways are only unidirectional solution assessed for security by Idaho National Labs on the DHS National SCADA Security Test Bed.

The difference between control system networks and IT networks is, not surprisingly, control. A compromised Balancing Authority or Transmission System Operator is an unacceptable threat to the reliability of the Bulk Electric System. All software can be hacked, including firewalls, which is why best-practice advice recommends Unidirectional Security Gateways. The time has come to ask:

Which of our control systems are expendable enough to protect with only firewalls?

For further information, please contact us or visit our website: www.waterfall-security.com

USA	V: +1 (703) 840 5452	**International**	V: +972 3-900-3700	Information: info@waterfall-security.com
	F: +1 (703) 840 5401		F: +972 3-900-3707	Sales: sales@waterfall-security.com