Waterfall Security Solutions Ltd.

Waterfall Security Solutions Response to NIST RFI: Developing a Framework to Improve Critical Infrastructure Cybersecurity [Docket Number: 130208119-3119-01]

Lior Frenkel, CEO & Co-Founder, Waterfall Security Solutions
Paul Feldman, Chairman, Midwest ISO & Independent Director, WECC

April, 2013

- Legal Notice & Disclaimer -

The material in this document was prepared for the purpose of potential business and is proprietary to Waterfall Security Solutions Ltd. This document is strictly secret and confidential and is provided with the understanding that it will be held secret and confidential. No part of this document may be disclosed to any third party, copied, reproduced or stored on any type of media or otherwise used in any way without the express, prior, written consent of authorized officers and/or executives of Waterfall Security Solutions Ltd.

Any and all third party intangible and/or proprietary and/or intellectual property rights ("**Third Parties' Rights**"), mentioned herein, whether registered or not, including, without limitation, patents, trademarks, service marks, trade names, copyrights and computer applications, belong to their respective owners. Waterfall Security Solutions Ltd. disclaims any and all interest in all such Third Parties' Rights. It is forbidden to copy, modify, amend, delete, augment, publish, transmit, create derivative works of, create or sell products derived from, display or post, or in any other way exploit or use such Third Parties' Rights without the express authorization of their respective owners.

Except as specified herein, Waterfall Security Solutions Ltd. does not guarantee nor make any representations with regard to any and all third party tangible and/or intangible and/or proprietary and/or intellectual property ("**`Third Party Property`**") mentioned herein. Waterfall Security Solutions Ltd. does not endorse nor makes warranties as to the completeness, accuracy or reliability of such Third Party Property, and all such warranties are hereby expressly and strictly disclaimed.

Waterfall Security Solutions Ltd.
16 Hamelacha St. Afek Industrial Park,
Rosh Ha'ayin, 48091 Israel
Office: +972-3-9003700 ; Fax:+972-3-9003707

North America Offices,
Waterfall Security Solutions USA.
1133 Broadway, Suite 708, New York, NY, 10010
Office: (212) 714-6058 ; Fax: (212) 465-3497

www.waterfall-security.com

- Table of Contents –

Executive Summary

Unidirectional Security Gateways securely integrate control system components with business networks by replicating servers from control networks to business networks. The technology secures safety-critical and reliability-critical networks far better than firewalls can secure such networks. While the gateway technology is widely deployed, it is not yet well-represented in industrial Cybersecurity standards and guidance. Any NIST framework for the security of critical infrastructures must strongly encourage the use of Unidirectional Security Gateways in all applicable network contexts, and should encourage standards developers to reflect the technology in their standards and guidance. This is particularly true of high-risk contexts, such as central vendor monitoring and diagnostics/support for critical infrastructure components.

Introduction

Unidirectional Security Gateways securely integrate control system components with business networks by replicating servers from control networks to business networks. The gateways are a hardware/software combination. The hardware permits information to leave a secured control system network, without allowing any attacks or any information whatsoever back into that network. Gateway software replicates servers from control system networks to business networks through the unidirectional hardware. The

combination of hardware and software provides a secure replacement for firewalls when interconnecting control system networks with business networks.

With a small number of exceptions, Unidirectional Gateway technology is not well-represented in industrial cybersecurity standards and guidance. The technology secures safety-critical and reliability-critical networks far better than firewalls can secure such networks. Any NIST framework for the security of critical infrastructures must strongly encourage the use of Unidirectional Security Gateways in all applicable network contexts. This is particularly true of high-risk contexts, such as central/remote vendor monitoring and operation of critical infrastructure components.

This response to the NIST "Developing a Framework to Improve Critical Infrastructure Cybersecurity" RFI:

- Reviews vulnerabilities of firewall-mediated communications,
- Presents central vendor monitoring and diagnostics/support as a particularly high-risk integration scenario,
- Introduces Unidirectional Security Gateways as a secure alternative for control-to-business and safety-system application integration,
- Reviews standards and guidance coverage of hardware-enforced unidirectional gateways, and
- Recommends that NIST strongly encourage the use of Unidirectional Security Gateways in advice and frameworks for control system cyber-security, especially in high-risk integration scenarios such as central vendor monitoring and diagnostics/support.

Firewall Vulnerabilities

Firewalls are intrinsically vulnerable to many kinds of attacks. The most common way through modern firewalls is "phishing" or "drive-by-download" attacks where end-users are tricked into pulling disguised attack code through a firewall. The easiest attack on a firewall is simply to guess a VPN or administrator password. The best-known attack is not to attack the firewall at all, but to attack those servers nominally protected by the firewall with any of a number of kinds of attacks, including SYN floods, buffer overflows, cross-site-scripting and SQL injection. In addition, there are numerous reports showing that industrial firewall misuse and misconfiguration is in practice a serious and widespread problem.

Almost all modern communications and application protocols are bi-directional - eg: HTTP, database client/server communications, data historian client/server communications, OPC, and Modbus. In fact, almost all such protocols use TCP/IP as a transport, and TCP/IP is fundamentally bi-directional. Even UDP/IP-based protocols generally allow bi-directional UDP and ICMP communications. Modern businesses rely

on a timely flow of data from control system components to business systems and users, routed through firewalls via these protocols.

Every one of these common connections through firewalls from control-system networks permits messages to return through those firewalls to those sensitive networks, and any one of those messages could contain an attack. It is widely thought that communications connections initiated from inside a protected network are safer than those initiated outside the network. As a result, some security practitioners require that only systems inside a protected network may open connections through firewalls at the edge of a network. What is less widely appreciated though, is that even though connections originating inside a protected network are, yes, marginally safer than connections originating outside the network, once a bi-directional connection is established, attacks can pass back into the protected network from the outside network over that established connection, no matter who initiated the connection.

What is even more distressing is that large numbers of firewalls nominally deployed to protect control system networks are in fact providing little protection because of the very large numbers of connections allowed through these firewalls. Widely-cited security standards and guidance such as the ISA-SP99 series, the NIST 800-82, NERC-CIP-005, all state that all connections through control system firewalls should be disallowed by default, and only "essential" connections allowed through the firewalls. The problem is that no such standard defines the word "essential."

The most common interpretation of "essential connections" is "essential to the business." Depending on the organization, "essential to the business" can mean almost anything. As a result, in a great many organizations, there are enormous numbers and kinds of bi-directional connections allowed through plant firewalls. Every one of these "essential" connections through a firewall is a channel by which attacks from external networks can reach back into control system networks.

Fundamentally, firewalls are complex software artifacts, and so are intrinsically vulnerable to software compromise, mis-configuration, manipulation by insiders and all of the other vulnerabilities which are fundamental to software artifacts. In practice, the security of even standards-compliant industrial firewall deployments, range anywhere from “as vulnerable as every other software system” to “spectacularly vulnerable because of huge numbers and kinds of allowed connections, and incredible complexity of configuration.”

Central Monitoring and Diagnostics / Support

Turbine vendors and many control system vendors need to receive continuous, online feeds of data from large numbers of control systems networks. These feeds are all sent to these vendors' central “remote monitoring and diagnostic/support” sites. All of these connections are designed to provide vendor personnel at a central site with continuous

remote monitoring capabilities. Many of these connections are also designed to provide vendor personnel with the ability to carry out occasional "support" or "diagnostic" operations – other words for "occasional remote control over critical control system components." The majority of connections to central monitoring and diagnostic/support sites are through a firewall connecting the control system network to the site's business network, and then through the Internet using encrypted communications

These central sites represent prime targets for attackers who wish to cause harm to large numbers of critical infrastructure sites simultaneously, using common technologies and communications systems. These sites represent communications paths by which common malware could migrate from one critical infrastructure site in one organization, to another site in a different organization. They represent communications paths by which targeted attacks could be routed from one customer's site to another, via the shared central monitoring facility. These central sites represent opportunities for disgruntled employees of the central management vendor to deliberately mis-configure or infect dozens of critical infrastructure sites simultaneously.

At present, no standards or guidance refers specifically to this significant threat to critical infrastructures, to how these central sites should be protected or managed in order to protect customer sites, or to how individual sites and organizations should put specific protections in place to protect those sites from this significant threat. This is of course unacceptable.

Here is a specific example. One vendor who provides a remote monitoring and diagnostics / support service does so this way:

- The vendor supplies each site with a firewall with which to connect the vendor's equipment at the site to the vendor's central site via a VPN connection through the site's business network and the Internet.

- The vendor manages that firewall remotely. The site does not have an account which would let them log into the vendor's firewall at the site and review or adjust the firewall's configuration.

- The vendor configures one of the computers at the site as a Remote Desktop server, so that the vendor can at any time log into that server and operate that computer on the customer's network by remote control.

- The vendor uses these technologies to continuously monitor, and occasionally adjust, the vendor's equipment at the customer site, without notifying the customer as to when such adjustments might take place, or what the nature of the adjustments to software or configurations might be.

Customers who have purchased a "monitoring only" service might imagine that they are less exposed to security risks than customers who have purchased the "remote diagnostics and support" package, but they are mistaken. For sake of simplicity and commonality of systems, this vendor deploys its monitoring systems the same way at all customer sites.

This vendor's approach to security is not uncommon.

Unidirectional Security Gateways

Waterfall's Unidirectional Security Gateways are combinations of hardware and software which securely integrate industrial control systems with business networks. The gateway software gathers data from servers and devices on control system networks using conventional communications. The software makes this data available to users and applications on external business networks by replicating industrial servers and devices on those business networks. Business users access the replicas as if they were the original servers and devices.

The gateway hardware consists of a pair of network appliances connected by a fiber-optic cable. The Transmit (TX) appliance in the control system network contains an LED fiber-optic laser. The Receive (RX) appliance in the business network contains a fiber-optic receiver. This pair of appliances can send information from a control system network to a business network, but the RX appliance cannot send anything back. There is no laser in the RX appliance, and even if there was a laser in that appliance, there is no fiber-optic receiver in the TX appliance. As a result, the TX and RX hardware cannot be reconfigured, or hacked, to exchange roles or otherwise behave differently from its design. This hardware-enforced unidirectionality of the Waterfall technology has been verified by both an Idaho National Labs security assessment, and a Common Criteria EAL4+ certification.

Unidirectional Gateways are routinely deployed to transparently replace firewalls and so provide the strongest possible protections for control system networks from attacks originating on external networks. A typical Waterfall gateway installation is illustrated in Figure (1).

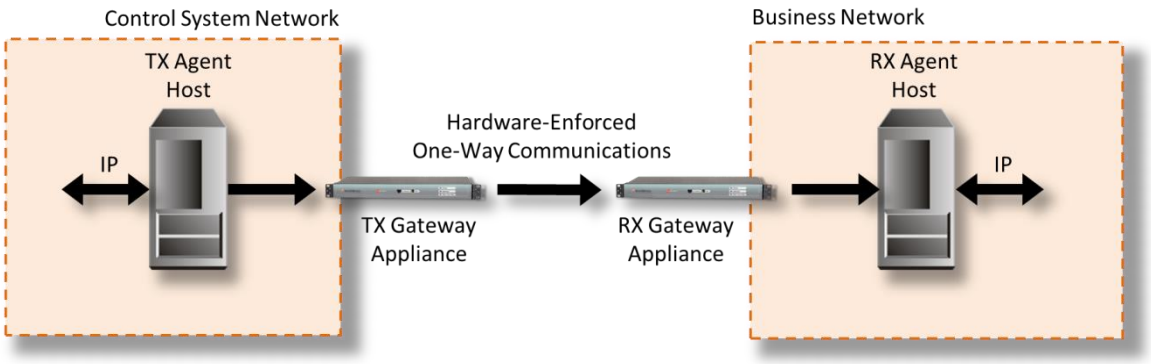

Figure (1) Unidirectional Security Gateways

In the diagram, the gateway agent software running on the TX agent host uses conventional IP communications to gather data from inside the control network. The TX host has two physical network interfaces, one connected to the control network, and one connected to the TX gateway appliance. IP packets received from the control system network have the IP address of the TX host as their destination. That is: the TX host is an endpoint of communications within the control system network, terminating all communications from within the control network. The TX host is not a router and does not permit protocols to be routed to a network outside of the cybersecurity perimeter.

The Waterfall TX agent software on the TX host extracts data from the communication it receives from a server or device inside the control network. The software then packages that data according to Waterfall conventions, and sends the data to the TX hardware appliance. The RX appliance receives the data through the fiber-optic connection and transmits it to the RX host. The content of these messages is simply the data packaged according to Waterfall conventions. The RX host extracts the data from the messages it receives from the RX appliance and sends that data to preconfigured application libraries and communications libraries, which make the data available to the preconfigured applications within the external network. The RX agent communicates within the external network using IP communications which are initiated at the RX agent. The target systems and any API being used are preconfigured in the RX host. No address information is sent from inside the control system perimeter to the RX host.

Correctly-designed, security-certified, hardware-enforced unidirectional gateways, no matter the vendor, provide strong protections for the safety and reliability of control systems, protections against attacks originating on external networks.

Historian Replication

Consider the control system historian replication example reflecting a gateway deployment at an American power plant in Figure (2). An OSIsoft PI Server/data historian is deployed in the power plant, on the plant network, and a replica PI Server is deployed on the business network. After an initial offline synchronization effort where

the database of the historian server was copied to the replica server, the unidirectional solution started its real-time synchronization.

TX Agent software on the control system network queries the production historian, asking for all data since the manual synchronization, and all new data, as that data arrives in the historian. These are standard queries supported by the PI Server product. On the business network, the RX Agent software populates the replica PI Server. The RX Agent registers with the replica as a standard OSIsoft device Interface Node. The RX agent reports to the replica historian all data received via the unidirectional medium, as if that data had just been reported from the original source devices, just as the original Interface Nodes would have reported the same data to the production PI Server.

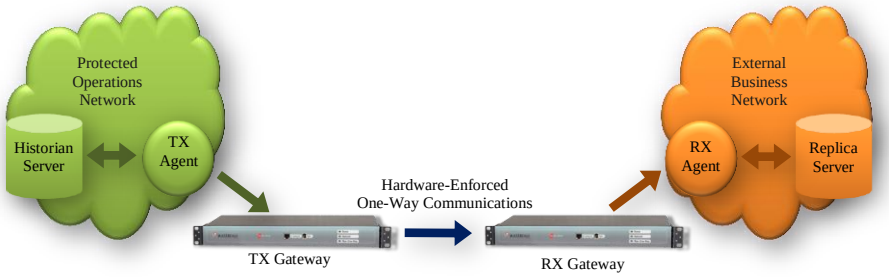

Figure 2: Historian Server Replication with Unidirectional Gateways

Business users and business applications access the replica server(s).

The replica server is maintained in real time as a faithful replica of the original server, identical to that server in almost every way. Business users generally think they are still connected to the original PI Server. As a result, replacing the firewall that originally separated the two PI Servers with a Unidirectional Gateway was a seamless process, and the resulting network integration is without the vulnerabilities associated with firewall technologies.

The unidirectional solution uses conventional two-way protocols and programming interfaces to query the control system PI server, and uses such protocols and interfaces to publish data on the business network to the replica server. What passes on the unidirectional medium is a proprietary, unidirectional protocol, the exact nature of which is irrelevant to users of replica the server.

Industrial Protocols

This same approach can be used to publish Modbus, DNP3 and other data to the business network, data which at first glance appears to be accessible only via query/response type two-way protocols. Take for example the OPC-DA protocol. The protocol is complex and intensely bi-directional, layered on top of DCOM, which rides on DCE, which most commonly uses some form of IP deep in the protocol stack. The unidirectional gateways

do not somehow emulate the OPC protocol across a one-way medium. Instead, just as in the historian replication scenario, the gateways replicate OPC servers [1].

Figure (3) below illustrates how Waterfall Unidirectional Gateways are deployed to protect the control system network on an offshore oil & gas production platform while carrying out OPC server replication. There is both a control system network and a business network on the platform. The gateways are the only connection between the two networks, and the business network on the platform is connected over a radio link to networks on land.

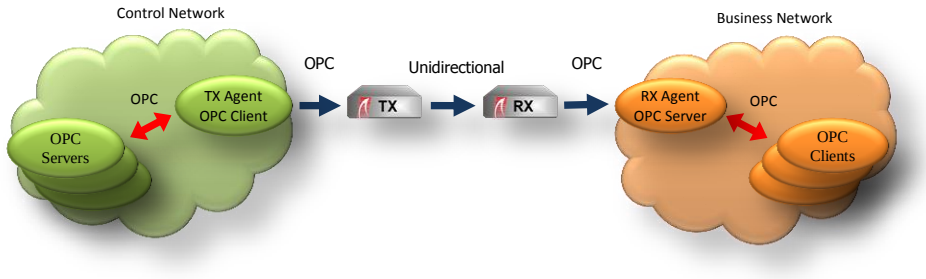

Figure 3: OPC-DA Server Replication with Unidirectional Gateways

OPC is an open specification, and so anyone can write an OPC client, and anyone can write an OPC server. The gateway TX Agent in Figure (3) is a true OPC client, and that client is configured to use the true OPC protocol to query control network OPC servers for the data which is to be shared with business users and applications. The TX Agent sends that data across the unidirectional medium, using a proprietary one-way protocol, to the RX agent. The RX Agent is a true OPC server. That server holds the received data until an OPC client on the business network requests the data. Again, OPC clients on the business network interact exclusively with the OPC-DA server replica. This same approach can be applied to emulate Modbus "slave" devices and DNP3 "slave" devices, devices which in TCP terminology act as TCP servers.

Remote Assistance: Remote Screen View

Security practitioners new to Unidirectional Security Gateways often assume that the gateways frustrate all remote monitoring and diagnostics/support capabilities. In fact, unidirectional Remote Screen View [2] is often used for remote vendor support and emergency vendor support. The screen images are made available to business network users via a server of some sort, for example a password-protected web server. Remote administrators can access the screen image / video feeds to see what is occurring on monitored equipment on the protected control system network, but of course cannot directly influence the monitored equipment in any way. Instead, they communicate with personnel who have access to the protected equipment, usually by telephone.

In a power generation turbine management scenario for instance, the turbine vendor's monitoring applications at a central location gathering data from replica servers may alert the vendor's personnel to a turbine vibration problem requiring adjustment. The vendor's support personnel call personnel at the unidirectionally-protected generation site and ask for assistance. Site personnel verify the caller's identity and route the call to an authorized equipment administrator.

That administrator logs into the appropriate equipment, often an engineering workstation, is guided by turbine vendor support personnel to the appropriate applications and dialogs needed to diagnose the problem and to adjust the turbine to correct the vibration problem. The turbine vendor sees this interaction as "supervising site personnel in correct resolution of a problem." The site personnel see the interaction as "supervising vendor personnel in their adjustment of the site's equipment." Each perception is legitimate, and each set of needs is met.

Secure Manual Uplink

When there are no qualified personnel at a site, there may still be a need for occasional remote access into the critical network. A variety of ad-hoc solutions support this need, and a commercial solution exists in the form of Waterfall Security Solutions' Secure Manual Uplink product. Whether ad-hoc or off-the-shelf, the solution lies in temporarily, physically connecting protected control system networks to business networks for remote management. Figure (4) illustrates the Waterfall solution as applied to the turbine management problem.

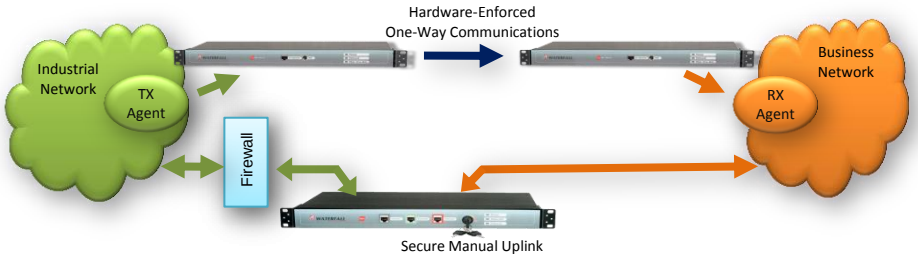

Figure 4: Secure Manual Uplink

The Waterfall solution consists of a network appliance with two conventional copper connectors, and a physical key. When the key is turned, the device electrically connects the "input" and "output" copper connections and so connects the business network to the industrial network for a pre-programmed period of time. After the time expires, or in the event of an unanticipated failure such as a power failure, the device automatically disconnects the two networks. The mechanism provides temporary remote control for remote vendors or for central SOC, NOC or other support personnel to the protected ICS network.

In practice though, the control system and business networks are never directly connected. Instead, as illustrated in Figure (4), the business network is generally connected to a control system firewall, and other kinds of security technologies such as VPNs and remote access servers often intervene

This remaining firewall exposure is a much smaller risk than a full-fledged plant firewall, both because the exposure is of such limited duration, and because the firewall deployed behind a Secure Manual Uplink appliance tends to be very simple. Advanced threats use manual remote control or "Remote Administration Tools" (RATs) to manipulate compromised networks. Such remote control intrusions tend to require weeks of interaction with compromised networks in order to achieve their objectives. Such attacks are very much frustrated if the attackers can only interact with compromised equipment for 30 minutes at a time, at long intervals.

In addition, simple configurations are a significant asset when it comes to keeping firewalls reasonably secure. If the vast majority of connections allowed through a firewall have been diverted to secure server replications via Unidirectional Gateways, what tends to remain configured on the firewall behind an SMU is handful of VPN connections. These connections are much easier to scrutinize, test and understand thoroughly, than are hundreds or thousands of "essential" connections through a conventional plant firewall.

When comparing the security of the Unidirectional Security Gateway + Secure Manual Uplink solution to that of a firewall, critical infrastructure sites conclude that it is better to be 100% secure from online attacks 99% of the time, than it is to be 99% secure, 100% of the time.

Widespread Deployment

In the USA, Unidirectional Gateways are deployed widely to protect electric power generators in the Bulk Electric System. For example, all nuclear generators in the United States have plans in place to deploy unidirectional gateway technology to protect their control system equipment from their business networks and from the Internet beyond their business networks. A growing number of conventional generators, oil and gas facilities, and water and wastewater facilities, are using Unidirectional Security Gateways. Chemical facilities in the US are also showing growing interest, with pilot projects being planned.

Unidirectional Gateways are not meant to replace every firewall in a defense-in-depth architecture. The gateways are best suited to replace “operational to business” perimeter firewalls, thus breaking the remote-control / online attack chain of bi-directional communications which would otherwise extend all the way from the Internet to life-critical safety systems, equipment protection systems, and industrial control systems. The single most common deployment of Unidirectional Gateways is to replicate data historian servers from plant-wide networks to business networks, or to replicate OPC servers to

business networks. The second most-common deployment model is to replicate monitoring systems and information from critical systems or safety systems out to local monitoring teams or remote monitoring and diagnostic facilities.

Securing Central Monitoring and Diagnostics/Support

Some organizations have determined that the central monitoring and diagnostics/support connections described earlier represent an unacceptable security risk, and have deployed Unidirectional Security Gateways to address this risk. These organizations deploy Unidirectional Gateways between the vendor's equipment at their sites and an external DMZ protected by the vendor's firewalls. This effectively creates a "replica servers DMZ" between the gateways and the vendor's firewall.

The vendor is thus able to continuously monitor equipment at the organization's sites by accessing the replica servers. When the vendor needs to adjust some setting, the site provides one of two mechanisms:

- Some sites deploy Remote Screen View to a web server on the replicas DMZ, and require the vendor to call the site and supervise the site making required changes to configurations or software.

- Other sites deploy Secure Manual Uplink and require the vendor to call the site and request a temporary connection to their Remote Desktop server on the real control network. The SMU is activated by a certified site employee, following an identification and authorization process.

Both of these mechanisms provide strong protections against viruses and targeted attacks propagating through the vendor's central site.

Existing Standards

Hardware-enforced unidirectional communications technologies are described to one degree or another in some existing or proposed standards:

- NERC CIP V5 (draft) inserted the word "bi-directional" into the definition of External Routable Connectivity, thus deliberately exempting unidirectionally-protected equipment from 37 of 103 requirements [3].

- NERC CAN-0024 (withdrawn) described "data diodes" and how they related to the CIP-V3 standards.

- NRC 5-71 and NEI 08-09 describe reduced compliance obligations when Unidirectional Gateways form at least one layer of a layered defense-in-depth strategy.

- The DHS Catalog of Controls mentions "data diodes" very briefly.

- ISA SP-99-03-03 (draft) mentions unidirectional gateways as an accepted network segmentation mechanism.

A great many industrial cyber-security standards and guidance documents do not yet describe Unidirectional Security Gateways, including NIST 800-82, NIST 800-53, the NISTIR 7628, all published ISA SP-99 standards, API 1164, INGAA guidelines, and a variety of DHS documents including CFATS Guidance, procurement language guidance, and defense-in-depth guidance. Given the widespread deployment of Unidirectional Gateway technology by many critical infrastructures, these and other standards should be updated to reflect this new technology as an alternative to firewalls.

Recommendations

Any NIST framework intended to further develop standards should include:

- Strong recommendations to a variety of standards bodies to include Unidirectional Security Gateways in their advice, and

- Strong recommendations to industry stating that unidirectional gateways be regarded as the preferred mechanism for protecting connections between networks.

Any NIST framework should recommend that if a firewall is to be used instead of a gateway, then for every connection permitted through that firewall, the organization deploying the firewall should consider seriously risks and business benefits. Specifically, when choosing a firewall over a unidirectional gateway, or when permitting yet another "essential" connection through a firewall, the organization should ask “is the benefit to the organization of that choice greater than the risk that choice represents to the organization, to its employees and to society?”

National critical infrastructures will be measurably safer, more secure and more reliable when Unidirectional Security Gateways are deployed more widely to separate safety, protection, and control networks from less-trusted networks, from central vendor monitoring site, from business networks, and from the Internet.

Bibliography

[1] L. Frenkel, D. Berko and A. Ginter, "Experience with Unidirectional Security Gateways Protecting Industrial Control Systems," November 2012. [Online]. Available: http://www.waterfall-security.com/category/resources/.

[2] L. Frenkel, "Advanced Protection for Advanced Threats: Securing Turbine Management Connections," Waterfall Security Solutions, September 2011. [Online]. Available: http://www.waterfall-security.com/category/resources/.

[3] Waterfall Security Solutions Ltd., "Unidirectional Security Gateways: Non-Routable, By Design," April 2013. [Online]. Available: http://www.waterfall-security.com/category/resources/.

About Waterfall Security Solutions

Waterfall Security Solutions Ltd. is the leading provider of Unidirectional Security Gateways™ for industrial control networks and critical infrastructures. Waterfall's Unidirectional Gateways reduce the cost and complexity of compliance with NERC-CIP, NRC, NIST, CFATS and other regulations, as well as with cyber-security best practices. Waterfall's products are deployed in utilities and critical national infrastructures throughout North America, Europe, Asia and Israel. Frost & Sullivan describe Waterfall's solutions as ensuring "optimum security for networks across user verticals" and awarded Waterfall the 2012 Network Security Award for Industrial Control Systems Entrepreneurial Company of the Year. Waterfall's offerings include support for leading industrial applications, including the ISOFT PI™ Historian, the GE Prophecy™ historian, Siemens SIMATIC™/Spectrum™ solutions and GE OSM™ remote monitoring platforms, as well as OPC, Modbus, DNP3, ICCP and other industrial protocols. More information about Waterfall can be found on the company's website at: www.waterfall-security.com.

Waterfall Security Solutions Ltd.
16 Hamelacha St. Afek Industrial Park,
Rosh Ha'ayin, 48091 Israel
Office: +972-3-9003700 ; Fax:+972-3-9003707

North America Offices,
Waterfall Security Solutions USA.
1133 Broadway, Suite 708, New York, NY, 10010
Office: (212) 714-6058 ; Fax: (212) 465-3497

www.waterfall-security.com