WATERFALL®
Stronger Than Firewalls

Simplifying Network Segmentation for the TSA Pipeline Security Directive

Simplifying Network Segmentation for the TSA Pipeline Security Directive

The Colonial Pipeline outage was a shock to senior decision-makers – the pipeline was shut down “in an abundance of caution” in the face of a compromised IT network, with no evidence that the OT network was affected by the ransomware. Before the outage, senior decision-makers had assumed that industrial and OT cybersecurity initiatives that pipelines and other critical infrastructures had deployed over the past fifteen years were sufficient to ensure that physical operations were independent of cyber attacks on Internet-connected IT networks. The Colonial incident proved that this was not the case.

The Directive

A month after the incident, the TSA issued Security Directive *Pipeline-2021-02: Pipeline Cybersecurity Mitigation Actions, Contingency Planning and Testing*. The directive was confidential, but a redacted version was subsequently released to the Washington Post in response to a Freedom of Information request. The redacted directive ordered large pipeline operators to address many topics, but the most pertinent directive was II.2(b):

> *Implement network segmentation sufficient to ensure that the Operational Technology system can operate at necessary capacity, even if the Information Technology system is compromised, ...*

The directive continues, requiring a number of measures, including II.2(b).vii:

> *Developing workarounds or manual controls to ensure industrial control system networks can be physically isolated when the Information Technology system creates risk to the safe and reliable Operational Technology system processes.*

These directives directly addressed the concern regarding pipeline outages due to compromised IT networks.

Unidirectional Gateways

The TSA directive includes many far-reaching requirements, and Waterfall’s Unidirectional Security Gateway products and technologies are powerful tools for compliance with the directive, and for strengthening pipeline OT cybersecurity programs.

When deployed as recommended, Unidirectional Gateways directly address network segmentation and other provisions in the directive. Waterfall recommends that Unidirectional Security Gateway products be deployed as the sole connection between operations-critical OT networks and all external networks, such as IT networks, the Internet and/or connections to external vendors and/or service providers. Waterfall further recommends that the gateways be oriented to send data exclusively from OT networks to IT networks.

Such configuration is of tremendous benefit to security programs, because Waterfall's Unidirectional Security Gateways are physically able to send information in only one direction – from the protected OT network out to external networks such as IT networks. No online attacks can traverse the Unidirectional Gateway hardware back into protected OT networks.

When deployed as recommended, the gateways assure pipeline operators that no stolen remote access credentials, malware, ransomware, hacktivist attacks, nation-state attacks or any other online attacks can pass through the gateway hardware into a protected OT network.

How Gateways Work

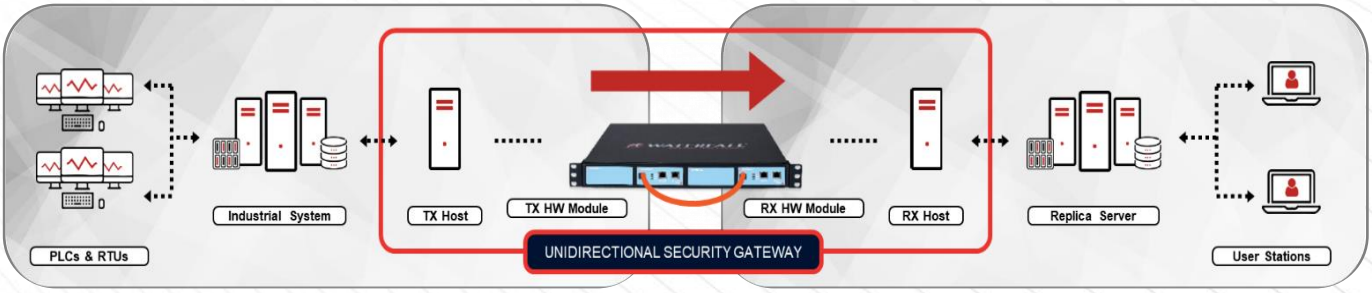
Waterfall's Unidirectional Security Gateways are a combination of hardware and software. The hardware consists of separate Transmit (TX) and Receive (RX) hardware modules - the TX module contains a fiber-optic transmitter (a laser), the RX module contains a fiber-optic receiver (a photocell,) and a short segment of fiber-optic cable connects the two modules. Since there is no fiber-optic laser in the RX hardware module, there is physically no way to send any optical signal from the receiving hardware back to the sending hardware.

Unidirectional Gateway software makes copies of servers and emulates devices. For example - consider an OT network where an OPC server or process historian server contains all the industrial data that is permitted to be shared with external users via the IT network. In this case, the Waterfall software connects to the source server, logs in, and asks for a snapshot of all recent data. The software receives that data, converts it to Waterfall's proprietary unidirectional formats and protocols, and sends the data through the unidirectional hardware to the Waterfall software on the receiving network.

That software receives the snapshot and logs into an identical server on the IT network. That is, if the source was OPC, then the destination is OPC. If the source was a historian server, then the destination is an identical historian server.

The software logs into the destination server and inserts the latest data snapshot. All IT users and applications that need access to real-time industrial data interact normally with the destination or “replica” server. No queries or other communications can be sent through the gateway to the source server, and since all data allowed to be shared with IT is already in the destination/replica server, no queries or other communications need to be sent through the gateway back into the protected OT network.

Waterfall’s unidirectional replication software already supports a very wide range of industrial servers, software, protocols, systems, and requirements. For that matter, Waterfall’s Unidirectional Security Gateways already serve many petrochemical pipeline operators, so pipeline operators can be confident that the systems and protocols they need to replicate to external networks have already been proven in the field.



Benefits

Using Waterfall's Unidirectional Gateways has many benefits:

- Per directive II.2(b), there is physically no way for online attacks to propagate from compromised IT or other external networks into OT targets through Unidirectional Gateways, ensuring that OT networks continue operating un-interrupted when IT networks are compromised,
- Per II.2(b).vii, with Unidirectional Gateways there is no need for emergency workarounds to ensure physical isolation of OT networks in cyber emergencies, because OT networks are permanently, physically isolated and protected from cyber attacks, and
- The deployment of Unidirectional Gateways makes obvious any OT dependencies on IT services, such as corporate Active Director controllers or other servers, so that those dependencies can be addressed in security designs, rather than being discovered in dismay during emergencies and triggering "abundance of caution" shutdowns.

The gateways also simplify other requirements in the TSA directive, such as requirements for controlling OT connectivity with the Internet, blocking connections to OT networks from post-exploitation tools, isolating IT from OT systems in the event of cyber emergencies, and many others.

Future-Proof Protection

Better yet, the benefits of deploying Unidirectional Gateways endure for many years to come, even as cyber attacks continue to evolve and become more sophisticated over time. All cyber-sabotage attacks able to affect OT networks are, by definition, information – the only way for an OT network to change from an uncompromised state to a compromised state is for attack information to somehow enter that OT network. Unidirectional Gateway hardware is, and will always remain, physical protection against the online movement of such attack information, no matter how sophisticated that attack information becomes as years pass.

The world's most secure petrochemical pipelines already use Waterfall's Unidirectional Security Gateways, as do a much greater number of power plants, refineries, water treatment plants, rail systems and other critical infrastructures. Unidirectional Security Gateways are recommended or required by IEC 62443, ANSSI Critical Infrastructure Cybersecurity standards, and other national standards, such as Israeli and South Korean standards. In North America, the gateways are recognized by CISA and the NERC CIP standards as providing stronger protection than do firewalls.

Please consider Unidirectional Security Gateways when seeking strong assurances of the continuity of physical operations in the face of rapidly evolving ransomware and other threats to IT networks.

To learn more about how Waterfall's Unidirectional Security Gateways can contribute to your cybersecurity program, please contact Waterfall at
https://waterfall-security.com/contact

ABOUT WATERFALL

Waterfall Security Solutions is the OT security company, producing a family of Unidirectional Gateway technologies and products that enable enterprise-wide visibility for operations, with disciplined control. Waterfall products represent an evolutionary alternative to firewalls. The company's growing list of customers includes national infrastructures, power plants, nuclear plants, off and on shore oil and gas facilities, refineries, manufacturing plants, utility companies, and many more. Deployed throughout North America, Europe, the Middle East and Asia, Waterfall products support the widest range of leading industrial remote monitoring platforms, applications, databases, and protocols in the market. For more information, please visit https://www.waterfall-security.com/