waterfall

13 Ways
to Break a Firewall
and what to do about each of them

Introduction

Understanding attacks is essential to defining robust defences. One measure of residual risk in our defensive postures is an evaluation of credible attack scenarios with serious consequences – attacks that we do not (yet) defeat with a high degree of confidence. There are always such attacks – security is a spectrum, not a pair of discrete states. We can never be perfectly secure – there are always attacks our defenses do not defeat. Understanding attacks is essential to evaluating the strength of our defenses and evaluating residual risk.

Since firewalls are almost always the second technical measure[1] deployed to defend industrial control systems, it is important that our understanding of operational technology (OT) / industrial attack patterns starts with attacks on firewalls.

What Is a Firewall, Really?

To understand how to attack firewalls we must first understand what they are and how they work.

We all use firewalls – most of our homes have a firewall built into our wireless router. We all know that firewalls (vaguely) "protect us from the Internet" – to some degree at least. But that's a benefit, not how firewalls work. How do they work?

To start with, all firewalls are software. Most of our laptop computers and even cell phones have firewall software built into the operating system. And while our home firewall and the firewalls we see in industrial settings often look like hardware – they come in a plastic or metal box with network and power connectors – what do we see when we open the lid? A CPU, running software. All firewalls are software, even the ones that ship with their own hardware / CPU.

Why is this important? Because all software can be hacked. All non-trivial software has defects, and firewalls are large, complex pieces of software. Some of those defects are security holes. For evidence of this, go to your favorite firewall vendor's support website and count how many security updates the vendor has issued in the last month.

One level deeper, all firewalls are also routers. They forward network messages from one network to another network (in our homes, from our home Wi-Fi network to the Internet, and vice-versa). Firewalls are routers with filters – software in the firewall that looks at every message and asks the question "is this message allowed?"

First 3 Laws of OT Security

1. Nothing is secure – security is a continuum – we can always be more secure, or less.
2. All software can be hacked – all software has defects, some of which are security holes.
3. All cyber-sabotage is information – and all information flows are attack vectors.

[1]The first measure? Take that password-less HMI off the Internet!

If the message is allowed, then the firewall may modify the message, for example carrying out address translation or encryption/decryption, and then eventually forward the message. Modern firewalls do much more than this, many having built-in anti-virus scanning, remote access capabilities, VPN, deep packet inspection and many other features, each with their own vulnerabilities.

The router nature of firewalls is important because all cyber-sabotage is information. The only way an industrial computer or network (or any computer or network) can change from a normal state to a compromised state is if attack information somehow enters the system. All cyber-sabotage attacks are information, and every information flow can encode cyber attacks. Intrinsically, since firewalls forward messages from one network to another, all firewalls are able to forward attack information from one network to another.

Finally, essentially all firewalls are bi-directional. TCP/IP is the workhorse protocol of the Internet, and TCP/IP is intrinsically bi-directional, exchanging messages, acknowledgements and other information both into and out of a protected network. Even more fundamentally, practically all Internet-based protocols that use TCP/IP are also bi-directional – they send queries (ie: information) in one direction and receive answers to those queries (eg: web pages and other information) back in the other direction. As a general rule, the more complex the protocol, the easier it is to embed attack information into the bi-directional protocol somewhere.

Given these realities, it is therefore not surprising that there are a great many ways to attack firewalls. Let's review a few of these ways and look at what we might do to reduce some of these risks, especially when protecting high-consequence industrial sites.

#1 Steal Firewall Password or Remote Access Password

The simplest, low-tech way to break through a firewall into an OT network is to steal a password. Shoulder surf as the OT firewall administrator enters a password to adjust the firewall, log in to the same firewall later, and add an "allow all" rule. The firewall is now simply a router, permitting all messages to pass. Passwords can also be stolen through phishing attacks rather than by local shoulder surfing, so attackers on the other side of the planet can log in and add the "allow all" rule or otherwise compromise the firewall. Even simpler may be a phishing attack that steals a remote access password, so the attacker can simply log into the OT network remotely with the stolen password, ignoring the firewall completely.

Mitigation: The standard way to address the risk of password theft is to add two-factor authentication (2FA) or multi-factor authentication (MFA) to all firewall administrator accounts and to all remote access accounts. With 2FA/MFA, even when a password is stolen, the attacker cannot use the password to log in because they do not have the other login "factors."

Mitigation: A weaker way to protect only the firewall administrator account is to configure the firewall so that administrators can log in only from the protected OT network. This way, even if a password is phished by a distant attacker, the attacker cannot use the password to log into the firewall as an administrator and reconfigure the device. This mitigation does not help with stolen remote access passwords.

In the Wild:

The initial compromise in the Colonial Pipeline attack was via a stolen VPN password

#2 Zero-Day & Other Vulnerabilities

The "high tech" way to break a firewall is to exploit vulnerabilities – defects in the design or implementation of the firewall firmware that allow attackers to take over or otherwise mis-operate the firewall. Known vulnerabilities are those for which patches/security updates and intrusion detection signatures are available. Zero-day vulnerabilities are vulnerabilities for which no patches or signatures are available. While zero days are particularly hard to defend against, even security updates for known vulnerabilities take time to install, time during which attackers may exploit the vulnerabilities. Worse, some security updates are themselves defective, sometimes introducing new and more serious vulnerabilities, and other times simply not preventing exploits of the now public vulnerabilities the updates were intended to repair.

Mitigation: Configure firewalls to auto- update when new security updates are available. This helps reduce the length of time known vulnerabilities can be exploited.

Mitigation: Network engineering techniques such as analog signalling (eg: HART-less 4-20 mA current loops) or OT-to-IT unidirectional gateways (not physically able to send attack information into an OT network) can eliminate the ability of attacks to propagate across network consequence boundaries.

In the Wild:

20,000 Fortinet VPN-firewalls were compromised by Chinese intelligence agencies using CVE-2022-42475

#3 Compromised Management Tools

The "modern" way to break a firewall is to compromise or exploit a management tool. Windows Active Directory controllers manage users and permissions. SolarWinds Orion systems manage firewall configurations throughout an enterprise, and most firewall vendors have their own proprietary firewall management systems. These systems are key targets for modern remote-control attacks. If attackers compromise an Active Directory system, they can create their own legitimate-seeming users with the permissions they need to act within our networks. If attackers compromise a firewall management tool, they can simply reconfigure all firewalls in the enterprise to let the attackers move through networks as they please.

And again, Active Directory controllers and firewall management systems are software. All software has defects. Some of those defects are vulnerabilities. Some vulnerabilities are known to the vendors and updates/patches are available. Some vulnerabilities are zero-days.

In the Wild:

SolarWinds Orion CVE-2021-25275 is a vulnerability that allows attackers to take over SolarWinds Orion software (not the Orion supply chain incident – this is a different vulnerability)

Further reading:
- "pass the hash"
- "golden ticket"

Mitigation: Use separate infrastructures for IT versus OT networks. For example, do not share Active Directory trusts between IT and OT networks. Do not manage OT firewalls from an IT-resident firewall management system. Either use no management systems on OT networks, or use OT-resident management systems, completely disconnected from IT management systems.

Mitigation: Secure the management systems. Most of us imagine that Active Directory systems, identity and access management (IAM) systems, firewall management tools and other management systems are security systems. They are not. These are user and permission management systems that urgently need to be secured and need to be protected from cyber attacks.

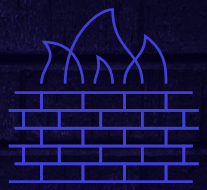
For more information on Unidirectional Gateways as an alternative to firewalls, please contact Waterfall Security to request a free consultation

#4 Attack Through the Firewall

The most widely known way to break a firewall is to ignore it completely and attack OT devices behind the firewall, devices that are exposed through the firewall. It is a widespread misconception that IT/OT firewalls provide external users with access to OT data while protecting the OT systems. In fact, firewalls provide external users with access to some OT systems but not others, so those users can send queries to those OT systems and receive responses.

A legitimate user might for example log into a PI server in an OT DMZ through the IT/OT firewall, logging in with the user's name and password. That same user who has shoulder-surfed a PI admin password can log in through that same firewall impersonating the administrator, to misoperate the PI server, or use the PI server to attack other OT targets reachable by the PI server. This is called "pivoting" – using a compromised machine to attack other machines. An attacker might also launch buffer overflow or other attack messages into OT assets exposed through an IT/OT firewall. In all these cases, the attacker is not attacking the firewall, but the PI server or other devices exposed through the firewall.

Mitigation: It helps somewhat to configure the IT/OT firewall to permit connections only from OT assets out to external IT assets, and not vice-versa. In such configurations there is less opportunity to attack OT assets through the firewall.



Mitigation: Using a so-called "next gen" firewall can help somewhat, to prevent some systems' administrators from logging in from unusual sources, or to detect some of the suspicious traffic passing through the firewall.

Mitigation: Network engineering techniques such as analog signalling (eg: HART-less 4-20 mA current loops) or OT-to-IT Unidirectional Gateways (not physically able to send attack information into an OT network) can eliminate the ability of attacks to propagate across network consequence boundaries.

In the Wild:

The Galil irrigation system was shut down by mis-operation of an HMI exposed to the Internet through a firewall

#5 Dependencies & "Abundance of Caution"

Most ransomware attacks that shut down industrial operations do so by encrypting and shutting down IT assets, not even touching any OT assets behind the IT/OT firewall. When industrial operators are not confident of the strength of their IT/OT firewall, and they see that ransomware has crippled the IT network, those industrial operations often decide to shut down safety-critical physical operations "out of an abundance of caution." In other cases, when continuous industrial operations depend on the correct operation of IT resources such as container tracking systems, custody transfer systems, or just-in-time order processing systems, then ransomware crippling those systems gives businesses no choice but to shut down physical operations.

Mitigation: Network engineering techniques can increase our confidence in the defenses at our IT/OT consequence boundary to the point where we can confidently continue operating, even if IT networks are compromised – no more "abundance of caution" shutdowns.

Mitigation: Risk assessments, table-top exercises and other cyber attack planning should include a report of OT dependencies on IT, cloud and other external services. If we need physical operations to continue when these services are crippled, we need plans, processes and technology in place to enable such operations.

In the Wild:

The Colonial Pipeline was shut down in "abundance of caution" when ransomware impaired the IT network.

Maersk Shipping was shut down because IT systems for tracking containers crippled by NotPetya

#6 Pivot Through a Compromised IIoT Cloud

The cloud is coming – cloud in the most general sense. Not necessarily the Amazon cloud where you rent CPUs, but cloud in the sense of "any connection from an OT system to any industrial vendor's service across the Internet." Such connections are commonplace in most industries, most often for predictive maintenance, such as for large rotating equipment – turbines and pipeline pumps / compressors. Those predictive maintenance servers may be hosted on Amazon or Google or may be hosted in the vendor's own offices. Either way, they are regularly connected to "IIoT" equipment deep in OT customer networks.

These industrial vendors' Internet-based systems and services are exposed to attacks from the Internet. If attackers want to break into a heavily firewalled industrial site that uses such services, and today most sites do use these vendor services, then the attackers target the industrial vendors' Internet services. Some vendors' systems will be thoroughly protected and others not. Attackers need only find a weakly-defended vendor, compromise that vendor's Internet-facing services, and pivot through those services' connections into the real OT target network. Once in control of Internet-connected equipment in the target network, attackers can mis-operate that equipment, or further pivot through the compromised OT equipment to other even more sensitive OT equipment in the (otherwise) heavily defended target.

In the Wild:

The Kesaya cloud service distributed ransomware to hundreds of customer sites over the course of 45 minutes (IT impact)

Cloud-based pivoting can reach and compromise hundreds of heavily defended industrial sites at once. And the attacks most often arrive inside of heavily encrypted "secure" connections, to which intrusion detection systems are largely blind.

Mitigation: Network engineering techniques such as the EPRI Industrial Internet of Things (IIoT) methodology can help. EPRI recommends deploying monitor-only IIOT devices that are physically incapable of control and hosting those devices on a separate IIoT monitoring network that has no access whatsoever to the main OT control network. Other network engineering techniques can help as well, the most common of which are Waterfall's Unidirectional Gateway products.

For more information on Unidirectional Gateways as an alternative to firewalls, please contact Waterfall Security to request a free consultation

#7 Break the VPN

Remote access makes life easier for people working at a site, and for people attacking the site. Instead of breaking the firewall, attackers can reach through the firewall inside a VPN connection. Many VPNs provide an experience to users that is similar to driving to site and plugging the laptop into the site's network. Plugging in lets a device access any other device on that segment of the OT network – as does the VPN. This means that if a remote laptop has been compromised with malware, that malware can access OT devices through the VPN the same as it could access OT devices if the laptop were physically connected to the OT network.

Alternately, attackers could steal VPN keys, passwords and other credentials, and log into the VPN from their own devices, or attackers could exploit a vulnerability in the VPN to gain access as if the attackers were legitimate users.

Mitigation: 2FA and Auto-updating VPN servers helps defeat some of these scenarios.

Mitigation: The latest advice from many national security agencies is to stop using VPNs and jump hosts, switching to hardware-enforced unidirectional remote access for high-consequence OT networks.

In the Wild:

The CVE-2024-3661 "Tunnel Vision" vulnerability was evident in practically all VPNs in 2024 – it's not clear how often it was exploited

#8 Supply Chain Attacks

We generally trust our OT hardware and software suppliers, but should we trust their web sites?

Attackers breaking into those websites or into the software development networks in industrial vendors can create malware or ransomware that looks and feels like a normal security update. Install the update and the software might act autonomously to encrypt everything it can reach, or more often connects to a command and control (C2) center on the Internet for further instruction.

Or hiding in plain sight – USB keyboards and mice purchased at the local computer store each have tiny CPUs and firmware in them. If attackers can compromise that firmware during the manufacture or delivery of the devices, the keyboards or mice can communicate malware into whatever computers we connect to the devices.

More commonly, well-meaning industrial vendors often install DSL routers, cable modems or cellular access points as part of automation for large equipment, so that the vendor has access to the equipment over the Internet. When attackers find those access points through Shodan or a similar search engine, they can try to use the Internet connections to bypass the IT/OT firewalls.

Mitigation: Security audits should include walk-throughs to try to discover rogue / vendor Internet connections, and vendor contracts should include heavy penalties for installation of such devices.

Mitigation: When installing software updates, test them thoroughly – not only for correct operation, but for any symptoms of connecting out to a C2 on the Internet.

Mitigation: Configuring firewalls for deny-by-default helps defeat malware calling out to the Internet. Network engineering measures such as unidirectional gateways help more.

In the Wild:

The SolarWinds Orion software update included malware.

NotPetya malware disguised as a security update shut down dozens of industrial sites

#9 Wireless Leave-Behind Attack

When someone breaks into an electric substation or other remote site, we inspect the site to see if anything has been stolen or damaged. Do we look to see if anything new has been left behind? Attackers can steal a little copper, so defenders think they understand the attack, and then leave behind a laptop or other device taped underneath or behind other equipment. Alternately, leave behind a small device labeled with a bright red notice saying "Important! Do not remove!" and the device becomes effectively invisible to technicians servicing the site.

Attackers can then return to the site days or weeks later, connect to their device using a wireless network the device starts broadcasting at that time, and operate the OT-connected device from the safety of a van parked around the corner, out of sight from cameras at the site.

Mitigation: Raise alerts and investigate when new devices / MAC addresses appear in OT networks.

Mitigation: Deny-by-default configuration of the small firewalls in remote sites helps somewhat.

In the Wild:

There are no public reports of such attacks on OT networks in the wild, but this technique is a favorite of cyber/physical penetration testers

#10 Cell-Phone War Driving Attack

Cell phones are walking wireless attack vectors – walking past firewalls.

Attackers invest in writing a useful free cell phone app and hundreds of thousands of users install the app. In addition to the stated purpose of the app, it also monitors Wi-Fi usage. When the cell phone is not connected to a Wi-Fi network, the trojan app uses the Wi-Fi capability to scan for SSID's and report the identifiers and their geographic location across the cellular Internet – effectively "war driving."

Then when attackers want to target a site, they consult their database, asking which SSID's exist within the geographic boundaries of the site. Attackers use phishing attacks to steal the passwords and other credentials for the Wi-Fi networks at the site. Then - the next time any compromised cell phone is carried into the site, the attackers use that cell phone and their stolen credentials to connect to IT and OT Wi-Fi networks at the site and attack through those connections. Many defenders believe that Wi-Fi networks located physically deep into heavily defended sites are low risk because those networks cannot be reached by external attackers. This is not the case.

Mitigation: Avoid OT Wi-Fi and other OT wireless networks

Mitigation: Asusme all Wi-Fi networks everywhere in the site are constantly compromised and design the site to tolerate constant attack from wireless networks.

In the Wild:

This attack has never been reported in the wild, but government authorities are concerned about the possibility.

For more information on Unidirectional Gateways as an alternative to firewalls, please contact Waterfall Security to request a free consultation

#11 C2 Beacons Defeat "Deny By Default"

Malware that activates in an OT network should not be able to connect to a C2 on the Internet if an intervening firewall has a "deny by default" rule, forbidding connections to arbitrary networks and IP addresses. The problem lies in OT networks with connections to industrial cloud services. When cloud services are hosted on public server farms, attackers can purchase capacity in those same server farms to host their C2's.

In these server farms, jobs can move around between parts of the farm, or between instances of the farm in different cities or different countries, changing IP addresses. This means that from time to time, the malicious C2 may have the same IP address as the legitimate industrial service.

Modern firewalls have the ability to set DNS-based firewall rules saying that a connection to the industrial vendor's DNS address is allowed. Firewalls resolve these DNS names into IP addresses, typically once per minute, and permit packets through the firewall destined for those IP addresses. As loads move around the public cloud acquiring different IP addresses, the firewall rules update to reflect the new permitted IP addresses. This means that from time to time, the firewall will permit connections from OT malware to a C2 service hosted on the same cloud service as a legitimate industrial service – when those loads migrate in such a way as to give them both the same IP address, at least temporarily.

Mitigation: Network engineering techniques such as the EPRI IIoT methodology can help. EPRI recommends deploying monitor-only devices that are physically incapable of control and hosting those devices on a separate IIoT monitoringc network, with no access whatsoever to the main OT control network. Other network engineering techniques can help as well, the most common of which are Waterfall's Unidirectional Gateway products.

In the Wild:

Never observed in the wild, but financial institutions are worried about this for their IT networks

#12 Sneakernet

Firewalls are tools designed to control the movement of online attacks. Offline attacks bypass firewalls – carrying malware into the site on a thumb drive or in a compromised laptop for example.

Mitigation: AV scanning kiosks at physical security checkpoints help somewhat to detect compromised devices

Mitigation: The Secure Operations Technology (SEC-OT) methodology seeks to physically control the flow of all online and offline attack information.

In the Wild:

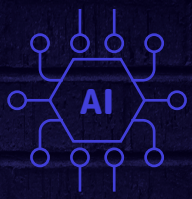
Stuxnet moved between sites on USB keys.

Sogu spreads on USB keys exfiltrating data from firewalled sites

#13 Autonomous AI

Stuxnet was the most sophisticated autonomous malware ever to cause physical consequences in OT systems. Many of us have wondered when we would see the "next Stuxnet." AI may provide an answer.

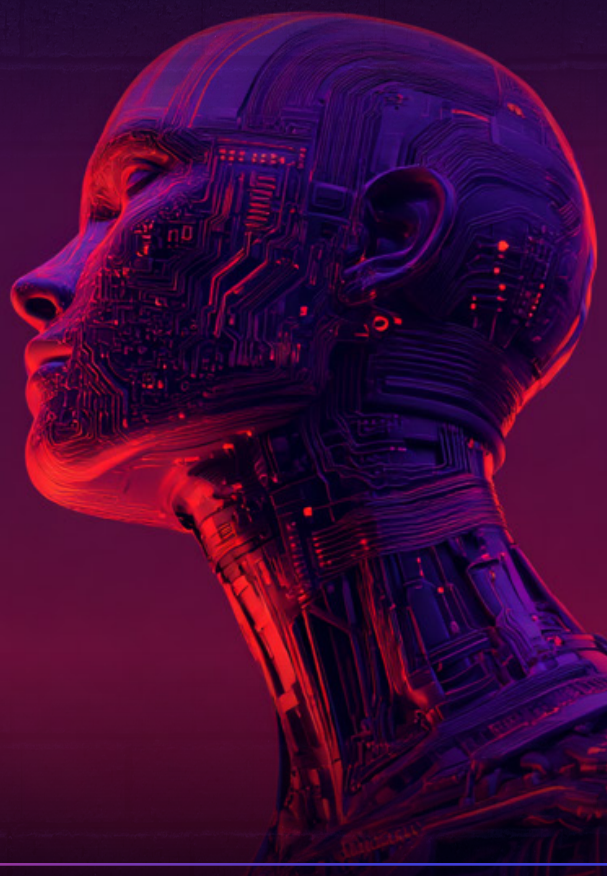
Penetration testers routinely use Kali Linux tools to test the security of OT networks and demonstrate breaking into those networks. AI models can be trained on the commands and outputs used by such penetration testers to attack OT testbeds and bring about simulated physical consequences. Attackers can then bundle a Kali Linux CD image with the AI model trained to attack OT systems, wrapping the whole thing in enough code to animate the Linux image and the AI model. If someone drops this 3-5GB of attack code on an OT asset, activates it and then walks away, the malware will start launching its attacks autonomously. Attackers can also train an AI on using Kali Linux and their own custom attack tools to break through IT and IT/OT firewalls autonomously, dropping the above autonomous AI into OT networks and activating it.



Mitigation: When this kind of AI-based autonomous malware becomes a credible threat, OT sites will need to adopt equally sophisticated defenses, including Cyber-Informed Engineering, SEC-OT and all of the NIST Cybersecurity Framework.

In the Wild:

Not yet seen in research efforts nor in the wild



Six More Attacks

Previous versions of this report described additional attacks able to defeat firewalls, including:

1. Steal the IP address of a host allowed to pass through the firewalls, such as an OT engineer's laptop, and start connecting through the firewall the way that authorized device would have.
2. Hijack existing connections to OT networks, such as via a fake Wi-Fi access point in an airport or coffee shop.
3. Errors & omissions – modern firewalls are complicated, and IT/OT firewalls especially can have a lot of rules. Any mistake in the configuration risks attacks passing through the device.
4. Unsecured Wi-Fi access points in OT networks, or even simple network cables connecting IT to OT cables bypassing firewalls, are sometimes deployed by well-meaning insiders, for what they think are good reasons.
5. Gain physical access to the firewall device – often there is a documented, supported way to take over the device for administrator with physical access.
6. Daisy-chain C2 connections through cooperating malware in an IT network – when breaking into OT networks unable to rout packets directly to the Internet.

These and other attacks still work.

In the Wild:

Misconfiguration of complex IT/OT firewalls is a constant concern for OT defenders

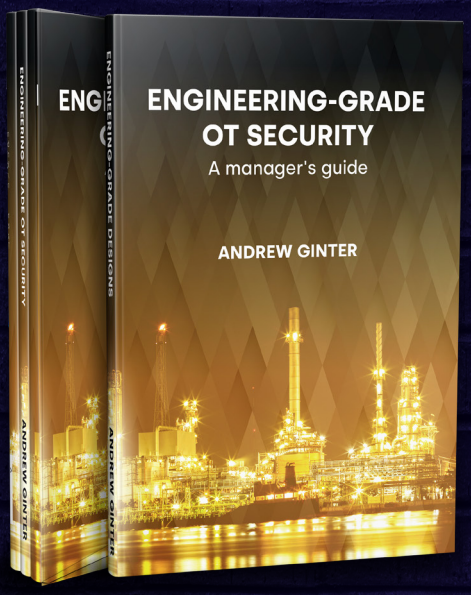
Conclusion

Understanding the limitations of firewalls is important, but even with these limitations, firewalls play important roles in most OT networks and in IT networks. That said, firewalls may not be sufficiently strong protection at consequence boundaries – connections between networks with dramatically different worst-case consequences of compromise. Today's most common consequence boundaries are IT/OT interfaces in high-consequence industrial installations.

Waterfall's Unidirectional Gateways are alternatives to firewalls at such boundaries. Unidirectional Gateways are combinations of hardware and software.

The hardware is physically able to send information in only one direction – usually out of the OT network – and not physically able to send any attack/information at all back in. The gateway software makes copies of servers, such as PI servers and OPC servers. Users and programs on IT networks use the copies of servers normally to access OT data. The gateway hardware means no questions or queries can be sent back into the OT network to put that network at risk. The gateway software means no questions need to be sent back into the OT network, because all the data that is allowed to be shared with the IT Network is already in the IT replica servers.

More generally, unidirectional gateways are the most widely-used example of network engineering – a collection of designs to deterministically prevent the propagation of cyber attacks through consequence boundaries.



Owners & operators who would like more information on network engineering and other modern approaches to OT security can request a free copy of Andrew Ginter's most recent book, 'Engineering-Grade OT Security'.

For more information on Unidirectional Gateways as an alternative to firewalls, please contact Waterfall Security to request a free consultation