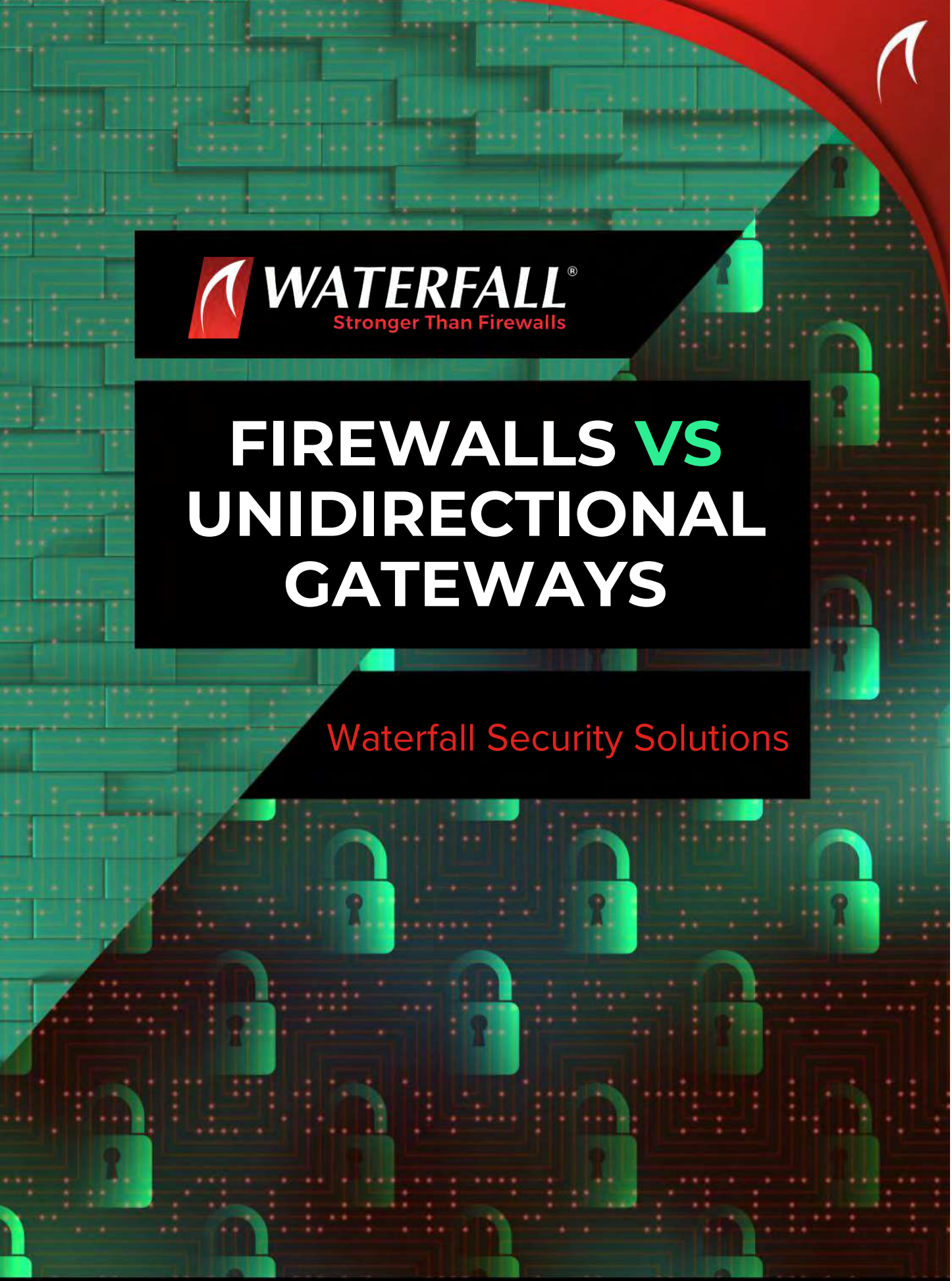

FIREWALLS VS UNIDIRECTIONAL GATEWAYS

Waterfall Security Solutions

TABLE OF CONTENTS

INTRODUCTION

Firewalls are used extensively inside industrial networks and throughout enterprise networks, but best practice demands at least one layer of unidirectional gateway technology in defense in depth architectures, most commonly at the Information Technology / Operations Technology (IT/OT) interface. This advice can be confusing to security practitioners who assume that a unidirectional gateway is some sort of "unidirectional firewall."

In this eBook we define what is a firewall, we review firewall principles, introduce unidirectional gateways, and compare the effectiveness of these two network perimeter protection technologies at the IT/OT interface. We conclude that unidirectional gateways are much stronger than firewalls. The gateways are also simple to deploy and reduce perimeter protection operating costs quite dramatically at the boundary between control-critical and business-critical networks.

FIREWALLS ARE ROUTERS

The term “firewall” can be confusing. In Internet Protocol (IP) terminology, all firewalls are routers – they forward network traffic from one IP network to another. Firewalls are not just routers though, what makes a firewall a security device is that all firewalls include a filter function. The filtering software looks at each IP message passing through the firewall and asks the question “is this message allowed?” If the message is allowed, it is forwarded to the destination network. If the message is not allowed, then it is dropped.

All firewalls are intrinsically bi-directional as well, despite some security practitioners using the term “unidirectional firewall.” A “unidirectional firewall” is one that is configured to permit industrial hosts to create connections to enterprise destinations, but not vice-versa. Such configurations prevent attackers from creating connections from enterprise networks into industrial targets.

The term is misleading, though. For example, such a firewall configuration would let a web browser on an industrial network connect out to a document server on the enterprise network and access a PDF file. But - if the PDF file contains malware, then the browser has just pulled that malware back into the industrial network right through the “unidirectional” firewall.

All firewalls are bi-directional. Once a connection is created through a firewall, no matter what kind of firewall, and no matter which network asked for the connection initially, the firewall passes messages that belong to that connection in both directions.

Even more fundamentally, all firewalls are software. All software has defects, both discovered and undiscovered, and some of those defects are software vulnerabilities. In practice then, all firewalls can be compromised. The simplest compromise steals passwords. The most sophisticated compromise exploits otherwise undiscovered “zero-day” vulnerabilities.

In short, firewalls are routers, they are vulnerable software, and they are intrinsically bi-directional

Firewalls are intrinsically bi-directional, passing all the messages their rules allow, whether or not those messages contain attack information.

UNIDIRECTIONAL GATEWAYS

Unidirectional Gateways are simple: the hardware can move data in only one direction, and the software makes copies of servers.

Firewalls have a role to play inside industrial networks, and throughout enterprise networks, but these intrinsic limitations mean that firewalls are almost always less secure than is needed at the critical IT/OT interface – the interface between the industrial and enterprise networks.

The alternative to firewalls at the IT/OT interface is unidirectional gateways. The National Institute of Standards and Technology (NIST) 800-82r2 Guide to ICS Security defines unidirectional gateways as:

Unidirectional gateways are a combination of hardware and software. The hardware permits information to flow in only one direction. The software replicates databases and emulates devices.

Let's look deeper at the gateways:

1. Unidirectional gateway hardware allows information to flow in only one direction, most often from the industrial network out to the enterprise network. The hardware does not control just connection requests, it controls the direction of all information flows.
2. The gateway software is not a router – it does not forward network packets from one network to another.
3. Instead, the gateway software gathers snapshots of industrial state information, packages up those snapshots for transmission through the unidirectional hardware, and makes the information available to enterprise users and applications on the destination network.

The first characteristic above means that the gateway absolutely prevents any attack information from passing back into the industrial network. The hardware is physically able to send information in only one direction. It does not matter how sophisticated malware is, or how capable the threat actors are, all cyber attacks on industrial operations are information. If no information can reach back into the industrial network through the unidirectional hardware, no attacks can reach back either.

Unidirectional Gateway software makes integration easy – providing enterprise networks with copies of industrial servers and other data sources.

The second and third items above may be new to practitioners familiar with firewalls. The concept is simple though – for example, a common IT/OT integration design stores all industrial data that is allowed to be shared with the enterprise in a database, such as a SQL Server database. In such designs, the unidirectional gateway software logs into the industrial SQL Server and watches for new or changed data. When software sees a change, it extracts the changed data and sends that data through the unidirectional hardware.

On the enterprise network, the gateway software inserts the data into an identical SQL Server database. Any enterprise user or application that needs access to the data simply connects to and queries the enterprise database.

Server replication makes it clear why unidirectional gateways are not router, like firewalls. The interaction between the gateway software and the database in the industrial network is query/response. The interaction in the enterprise network is update/response. These are entirely different sets of messages. It makes no sense to forward any of the query or response messages from the industrial network out to the enterprise network.

In short, unidirectional gateways are not routers. The gateways are intrinsically unidirectional and make copies of industrial datasets available to enterprise users, rather than forwarding network traffic from industrial to enterprise networks.

All cyber attacks are information. Unidirectional Gateways enable visibility into industrial operations while physically preventing the movement of attack information.

COMPARING SECURITY

Best practice advice strongly encourages unidirectional gateways at IT/OT interfaces because of the strong security the gateway hardware provides. Some examples:

Threat	Firewall	UGW
Errors & omissions	Simple misconfigurations can open attack paths into control system targets	Even if the software is misconfigured, the hardware still protects industrial operations
Credential theft	Stolen firewall administrator credentials can be used to reconfigure firewalls to suit of attackers	Even if credentials are stolen, no software change can affect the unidirectional hardware
Vulnerabilities and zero-days	Firewall software vulnerabilities can be exploited to attack industrial networks	No compromise of gateway software can affect the unidirectional hardware
Denial of service attacks	When firewalls permit connections from external networks, connection floods can overwhelm industrial servers	Unidirectional gateways are physically unable to transmit any attack back into the protected network

Unidirectional gateway hardware is physically unable to send any information back into protected industrial networks. No attack originating on external networks – neither stolen passwords, nor connection floods, nor exploited vulnerabilities – can propagate through the unidirectional hardware back into protected networks.

In short, firewalls are intrinsically software, with all the limitations of software security mechanisms. Unidirectional gateways have software components, but even if the software is compromised or deliberately misconfigured, the unidirectional hardware physically prevents attacks from reaching industrial networks.

OPERATING COST SAVINGS

What surprises many security practitioners is how little unidirectional gateways cost to deploy, manage and operate. IT/OT firewall configurations typically include between one hundred and one thousand firewall rules. IT and engineering best practices both dictate that every one of those rules be configured, tested, reviewed, documented and managed. All takes time and effort.

Worse, firewall rules change regularly over the life of the firewall, as communications needs evolve, as users come and go, and as enterprise IP address schemes evolve. In addition, because firewalls are vulnerable software, close and continuous monitoring of firewall logs and communications is vital to security. All of these activities represent significant labour costs.

Unidirectional gateways require none of these labour-intensive activities. A typical unidirectional gateway is configured to make a copy of a database, a copy of an OPC server, and copies of possibly one or two other servers. Each copying connection takes a few minutes to configure and test. Furthermore, once the copies are synchronized to the enterprise network, monitoring of the gateways is a low priority. Unlike firewalls, no change in the configuration, no error in the configuration, and no online attack whatsoever, no matter how sophisticated, can penetrate through the gateway hardware back into the protected industrial network.

In short, firewalls are labour-intensive, while unidirectional gateways are not.

INDUSTRIAL NETWORKS

Industrial networks are important. Compromised industrial networks risk long, unplanned shutdowns of physical operations, long-term damage to very costly physical equipment and threats to worker and public safety.

Software-based security controls, such as security updates, encryption, anti-malware systems and intrusion detection monitoring are all important protections, but of themselves are not sufficient to protect industrial networks. All software can be compromised or defeated, even security software and intrusion detection software. Worse, modern cyber attacks exploit permissions and stolen credentials more often than they compromise known software vulnerabilities.

This is why best practice guidance demands at least one layer of unidirectional gateways in a defense in depth network architecture, most commonly at the IT/OT interface.

CONCLUSION

Firewalls are intrinsically bi-directional routers and forward into industrial networks all network traffic that the configured rules permit, along with any attacks embedded in that traffic. While firewalls and other software-based security mechanisms do have a role in protecting industrial networks, best practice advises at least one layer of hardware-based unidirectional protection for important industrial systems, most often at the IT/OT interface.

Unidirectional gateways:

- Are intrinsically unidirectional and are physically unable to send any message or attack back into protected networks,
- Are cost effective, requiring much less effort to configure, operate and manage than IT/OT firewalls, and
- Are simple to deploy, making real-time copies of industrial servers available to enterprise users and applications.

Industrial control networks need more than IT class software protections. Nobody who works every day within the impact radius of an “industrial incident”, nor anyone who lives downwind of such potential incidents, wants to trust their lives or livelihoods to software alone. Unidirectional gateways provide physical protection from online attacks to industrial networks, no matter how simple or how sophisticated those attacks are or might become in the future.

Cyber-sabotage attacks will always be information, no matter how those attacks evolve into the future. Unidirectional gateways enable visibility into industrial operations, while physically preventing attack information from reaching industrial networks.

WATERFALL SECURITY SOLUTIONS

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, visit www.waterfall-security.com.