LOLLOJ - FOTOLIA

GET STARTED

1

How to protect enterprise ICS networks with firewalls

ICS network security can be improved using firewalls. Expert Ernie Hayden explains how ICS-specific firewalls can help keep ICS networks strong and protected.

Ernie Hayden, 443 Consulting LLC

Industrial control systems are a ubiquitous and integral part of factories; process industries, such as oil and gas; transportation systems; and critical infrastructure. They are also getting more exposure in the security industry due to the new and continued attacks on these ICS networks and systems.

In the early days of industrial controls, these systems relied on mechanical arrangements that ultimately turned into electromechanical systems. Then, over time, industrial control system (ICS) devices that used proprietary protocols were considered hack-proof by some. Essentially, the ICS systems were kept separate from the IT systems being implemented in the corporate offices.

In the past five to seven years, there has been a rapid convergence of IT and ICS, and the systems are no longer separated from the public internet by an air gap or with security by obscurity. With this new convergence, there is an increased need for data sharing, data acquisition and requirements for business systems -- such as enterprise resource programs -- to communicate between the factory/ICS and the enterprise IT networks.

This convergence has been accelerated by the increased cost to maintain and secure legacy ICS networks, by changes in connection methods used by new control systems from direct serial connections to TCP/IP networking, and by increased demand for remote access to ICS systems and devices by users and vendors.

With all these changes to the ICS networks and enterprise interface, there is an increasing need for defense in depth, and the firewall is an elemental part of this security strategy.

Introduction to firewalls

According to the report "Firewall Deployment for SCADA and Process Control Networks," published by the U.K. Centre for the Protection of National Infrastructure (CPNI), a firewall is:

"… a mechanism used to control and monitor traffic to and from a network for the purpose of protecting devices on the network. It compares the traffic passing through it to a predefined security criteria or policy, discarding messages that do not meet the policy's requirements. "

Firewalls act as guards between different network zones and, if they're not properly configured, they could enable unauthorized or malicious content or users to pass through. Also, firewalls can further restrict ICS subnetwork communications between functional security subnets and devices.

The capabilities of an effectively placed and configured firewall include:

- authenticate users before they are allowed access;
- block all communications between devices with the exception of specifically enabled packets or applications;
- enforce destination authorization;
- establish domain separation;
- monitor and log system events;
- monitor ingress and egress traffic and disallow unauthorized communications; and
- permit ICS to implement operational policies appropriate for the ICS that may not be appropriate in an IT network, such as prohibition of less secure communications, such as email.

Firewalls can also be used to define the separation of ICS and enterprise networks and to outline the boundaries of the DMZ. Firewalls are also expressly mentioned in IEC 62443-3-2, "Security for industrial automation and control systems," when addressing how the separate zones are established within the ICS or operational zone.

Firewalls are an operational imperative to segregate ICS and corporate networks. But firewalls can also be problematic, as they can delay network traffic and are prone to being installed and configured incorrectly.

ICS-specific firewalls

One of the first ICS-specific firewalls on the market was the Tofino Xenon Security Appliance, a small form factor firewall with added features for deep packet inspection and configuration controls specific to ICS protocols. The Xenon Security Appliance is also designed for use and application with the zones and conduits strategy discussed in IEC 62443-3-2.

Vendors such as Fortinet, PaloAlto Networks, Check Point and Cisco claim their firewalls can be used with ICS networks.

ICS network architects should recognize that factory and operational ICS environments can be hostile, dirty and may require intrinsically safe devices due to their explosive atmospheres. An off-the-shelf firewall probably won't work -- or be acceptable -- with these applications.

One potential future alternative to ICS firewalls are data diodes -- unidirectional network devices used as security gateways that enable data to move in only one direction. These are applied at nuclear power plants and are used to separate safety instrumented systems. These unidirectional gateways are effective, but they are also very expensive.

Bypassing a firewall?

Firewalls are not infallible or a panacea for ICS security. Some ways to bypass or circumvent a firewall include:

- using stolen credentials from authorized ICS users;
- attacking an external business web interface and -- if successful -- possibly pivoting into the data historian, a program that collects and stores production and process data, and which is inside the DMZ;
- inserting infected mobile media into a system component of ICS networks; and
- causing a user to upload faulty firewall software or firmware patches from a contaminated server, such as those used in a watering hole attack.

Bypassing or circumventing a firewall may also work if the firewall has not been patched, has been configured incorrectly, or has been positioned or placed improperly in the ICS network. Similarly, a firewall can be made ineffective if its rule sets are out of date or incorrect.

Don't forget the impact of the global supply chain. For instance, recently, there has been a strong focus on using commercial, off-the-shelf firewalls. These devices are often made overseas and could be subject to software or firmware malware, misconfiguration, or other issues.

Attackers can also bypass a firewall by taking advantage of remote access from the internet or the outside world into the ICS and inside the firewall boundary. For example, an intruder can gain access to a user's account at his home or corporate office and then use those stolen credentials to connect to the critical ICS components/systems. Similarly, taking advantage of modems or wireless access points inside ICS networks can enable hackers to bypass a firewall.

Human actions -- whether intentional or unintentional -- can also enable an attacker to bypass a firewall.

The U.S. Department of Homeland Security (DHS) report "DHS ISC-CERT Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies," states, "Do not assume that the implementation of a DMZ is a panacea for preventing threat actors from penetrating deeper into critical environments. The exploitation of transitive trust across a security perimeter is a plausible intrusion vector."

How to protect ICS firewalls

As stated earlier, users need to recognize that no system is 100% secure, and no single security product or technology can protect the ICS by itself.

The CPNI report offers the following actions and objectives to ensure a firewall is properly protecting the ICS:

- Do not allow direct connections from the internet to the ICS network and vice versa.
- Restrict access from the enterprise network to the control network.
- Only allow authorized access from the enterprise network to shared ICS servers in the DMZ -- normally the data historian, maintenance server, patching server and antivirus server.
- Secure the methods used for authorized remote support of control systems.
- Secure connectivity for wireless devices.
- Establish, implement and maintain well-defined rules outlining the type of traffic permitted on the ICS network.
- Monitor traffic on the ICS network and the traffic attempting to enter it.
- Secure connectivity for management of the firewall.

Other key actions to put into place for firewalls include:

- Implement policies and procedures to ensure that firewall software and firmware are patched and up to date. Deferring this patching may give attackers more time to apply new knowledge against ICS and other critical systems.
- Train users and firewall administrators on firewall vulnerabilities, threats and human factors that could result in errors or omissions with firewall configuration, rule sets, etc.
- Back up firewall configurations.
- Establish and closely monitor a subscription to the DHS Industrial Control System Cyber Emergency Response Team alarm and alert notices.
- Institute multifactor authentication for any access -- local or remote -- to firewalls and ICS components/systems.
- Periodically check and verify that the firewall rule sets and placement are correct, up to date, and do not enable an attacker to bypass the firewall.
- Always change the default credentials -- usernames/passwords -- on all ICS and enterprise systems before they go live.
- Implement and practice a strong incident response plan in case a firewall is breached, which can result in damage to the ICS or enterprise networks and data.

Firewall vendor relationships

It behooves the ICS administrator to pressure their firewall vendors to ensure his firewalls do not contain hidden or zero-day vulnerabilities. An admin should also establish a close relationship with his vendor and its security engineering staff in order to stay on top of potential threats, lessons learned, etc. This is especially important because vendors may not necessarily be on top of firewall security engineering strategies and processes.

Ernie Hayden asks:

What tools and services does your organization have in place for ICS network security?

Join the Discussion

This was last published in October 2018

Dig Deeper on Network device security: Appliances, firewalls and switches

Siemens ICS flaws could allow remote exploits

By: Michael Heller

Input validation issues open Cisco firewall vulnerability

Industrial control system cyber security risk high, report warns

By: **Warwick Ashford**

How do newly found flaws affect robot controllers?

By: **Judith Myerson**

Join the conversation

1 comment

Share your comment

☑ Send me notifications when other members comment.

Create Username and Add My Comment

Oldest ▼

[-] **ITKE**

- 25 Oct 2018 9:00 AM

What tools and services does your organization have in place for ICS network security?

Reply

CLOUD SECURITY NETWORKING CIO ENTERPRISE DESKTOP CLOUD COMPUTING COMPUTER WEEKLY

SearchCloudSecurity

How to pass the AWS Certified Security - Specialty exam

Author of 'AWS Certified Security - Specialty Exam Guide' Stuart Scott shares insights on how to prepare for the exam and reap ...

Practice AWS Certified Security - Specialty exam questions

Explore the security and compliance capabilities of the AWS Config service to prepare for the wide-ranging AWS Certified Security...

About Us Meet The Editors Contact Us Videos Photo Stories Definitions

Guides Advertisers Business Partners Media Kit Corporate Site

Contributors CPE and CISSP Training Reprints Events E-Products

Privacy Policy

Do Not Sell My Personal Info