

Firewalls and Filtering, Industrial Control Systems (ICS) and SCADA

CS-3113: PRINCIPLES OF CYBER SECURITY

BENJAMIN R. ANDERSON

Definitions

From the *Certified Information Systems Security Professional Official Study Guide, Ninth Edition* by Chapple, Stewart, and Gibson (OSG):

- **Firewalls:** Essential tools in managing, controlling, and filtering network traffic. A firewall can be a hardware or software component designed to protect one network segment from another.
- **Virtual Firewall:** A firewall created for use in a virtualized or hypervisor environment or the cloud. A virtual firewall is a software re-creation of an appliance firewall or a standard host-based firewall installed into a guest OS in a VM.
- **Bastion Host:** A system specifically designed to withstand attacks, such as a firewall appliance. The word bastion comes from medieval castle architecture.
- **Static Packet-Filtering Firewalls:** Filters traffic by examining data from a message header. Usually, the rules are concerned with source and destination IP address (layer 3) and port numbers (layer 4).
- **Stateless Firewall:** Analyzes packets on an individual basis against the filtering ACLs or rules. The context of the communication (that is, any previous packets) is not used to make an allow or deny decision on the current packet.

Definitions

From the *Certified Information Systems Security Professional Official Study Guide, Ninth Edition* by Chapple, Stewart, and Gibson (OSG):

- **Application-Level Firewall:** Filters traffic based on a single internet service, protocol, or application. Application-level firewalls operate at the Application layer (layer 7) of the OSI model. An example is the web application firewall (WAF).
- **Web Application Firewall:** Is an appliance, server add-on, virtual service, or system filter that defines a strict set of communication rules for communications to and from a website. It's intended to prevent web application attacks.
- **Circuit-Level Firewalls:** Also known as circuit proxies are used to establish communication sessions between trusted partners. In theory, they operate at the Session layer (layer 5) of the OSI model (although in reality, they operate in relation to the establishment of TCP sessions at the Transport layer [layer 4]). SOCKS (from Socket Secure, as in TCP/IP ports) is a common implementation of a circuit-level firewall.
- **TCP Wrapper:** An application that can serve as a basic firewall by restricting access to ports and resources based on user IDs or system IDs. Using TCP wrappers is a form of port-based access control.

Definitions

From the *Certified Information Systems Security Professional Official Study Guide, Ninth Edition* by Chapple, Stewart, and Gibson (OSG):

- **Stateful Inspection Firewalls:** Also known as dynamic packet filtering firewalls [they] evaluate the state, session, or context of network traffic. By examining source and destination addresses, application usage, source of origin (i.e., local or remote, physical port, or even routed path/vector), and the relationship between current packets and the previous packet is the same session, stateful inspection firewalls are able to grant a broader range of access for authorized users and activities and actively watch and block unauthorized users and activities. Stateful inspection firewalls operate at OSI layers 3 and up.
- **Deep-packet Inspection:** Also called payload inspection, or content filtering [it] is the means to evaluate and filter the payload contents of a communication rather than only on the header values.
- **Next-Generation Firewalls:** is a multifunction device (MFD) or unified threat management (UTM) composed of several security features in addition to a firewall; integrated components can include application filtering, deep packet inspection, TLS offloading and/or inspection (aka TLS termination proxy), domain name and URL filtering, IDS, IPS...

Definitions

From the *Certified Information Systems Security Professional Official Study Guide, Ninth Edition* by Chapple, Stewart, and Gibson (OSG):

- **Host-based Firewall:** *A local, software, or personal firewall is a security application that is installed on client systems. A host-based firewall provides protection for the local system from the activities of the user and from communications from the network or internet.*
- **Internal Segmentation Firewall:** *A firewall deployed between internal network segments or company divisions. Its purpose is to prevent the further spread of malicious code of harmful protocols already within the private network.*

Definitions

From the *Certified Information Systems Security Professional Official Study Guide, Ninth Edition* by Chapple, Stewart, and Gibson (OSG):

- **Proxy Server:** *A variation of an Application-level firewall or circuit-level firewall. A proxy server is used to mediate between clients and servers. Proxies are most often used in the context of providing clients on a private network with internet access while protecting the identity of the clients.*
- **Forward Proxy:** *A standard or common proxy that acts as an intermediary for queries of external resources. A forward proxy handles queries from internal clients while accessing outside services.*
- **Reverse Proxy:** *Provides the opposite function of a forward proxy; it handles inbound requests from external systems to internally located services. A reverse proxy is similar to the functions of port forwarding and static NAT.*

Definitions

Just a few more definitions:

- **Spam:** In e-mail means “Unsolicited bulk email”. Unsolicited means that the recipient has not granted verifiable permission for the message to be sent. Bulk means that the message is sent as part of a larger collection of messages, all having substantively identical content.
- A message is spam only if it is both unsolicited **and** bulk
 - Unsolicited e-mail (first contact enquiries, job enquiries, sales enquiries) can be normal e-mail
 - Bulk e-mail (subscriber newsletters, customer communications, discussion lists) can also be normal e-mail
- **Filter:** A software program or device that monitors incoming and outgoing packets on a computer network to determine whether the packets should be allowed to enter or leave a computer system.

Spam Filters

Spam is a huge problem – clogging inboxes and often containing links to malicious websites, or having malicious attachments

Google has put a lot of effort to protect their Gmail users from spam

- They claim they: *block more than 99.9 percent of spam, phishing and malware from reaching Gmail inboxes*
- <https://cloud.google.com/blog/products/g-suite/ridding-gmail-of-100-million-more-spam-messages-with-tensorflow>

To do so they have a variety of filters that try to separate valid emails from spam (and malicious) emails

Spam Filters

Read: *Prevent mail to Gmail users from being blocked or sent to spam*, Google Support

- <https://support.google.com/mail/answer/81126>
- You will be responsible for knowing the basic categories that Gmail uses – (Following best practices, Make sure messages are authenticated, Send email to engaged users, etc.)
- You will also need to be generally familiar with the activities in those categories

Also note, some of these filters make it a lot of work to set up and run your own email server

- For example creating SPF records and turning on DKIM signing adds overhead to process
- This is why there are many companies that will provide email hosting (including Google) – they do the administrative work for you

Web Filters

Web filters (or internet filters) are often used to prevent access to websites that contain certain kinds of content

One example is Google SafeSearch. From Google:

- *Whether you use Google Search at work, with children, or for yourself, SafeSearch can help you filter explicit content from your results. Explicit results include sexually explicit content like pornography, violence, and gore.*
- <https://support.google.com/websearch/answer/510>

One issue with web, spam, or other filters is that it is easy to create false-positives

- That's where a legitimate site, email, or other content is blocked or flagged – but is actually legitimate or appropriate
- For example, when signing up for a new website, many of them suggest you check your spam or junk folder for their “confirmation” email

Firewalls

Read: *What is a Firewall?* By Palo Alto Networks:

- <https://www.paloaltonetworks.com/cyberpedia/what-is-a-firewall>

Watch: *What is a Firewall?* By PowerCert Animated Videos

- <https://www.youtube.com/watch?v=kDEX1HXybrU>
- You are responsible for understanding:
 - The components of an Access Control List (permission, (source) IP address, protocol, destination, port)
 - What firewall rules can be based on (IP addresses, domain names, protocols, programs, ports, keywords)
 - How host-based and network-based firewalls work, their differences, and how they can work together
- Also, note that they talk about protecting the network from the internet
 - However, firewalls can also be used inside a corporate network to protect different parts of the network from each other
 - For example, a critical infrastructure organization (like Colonial Pipeline) could use a firewall to separate the business network from the operations network (control for pumping stations, etc.)

Firewall Techniques

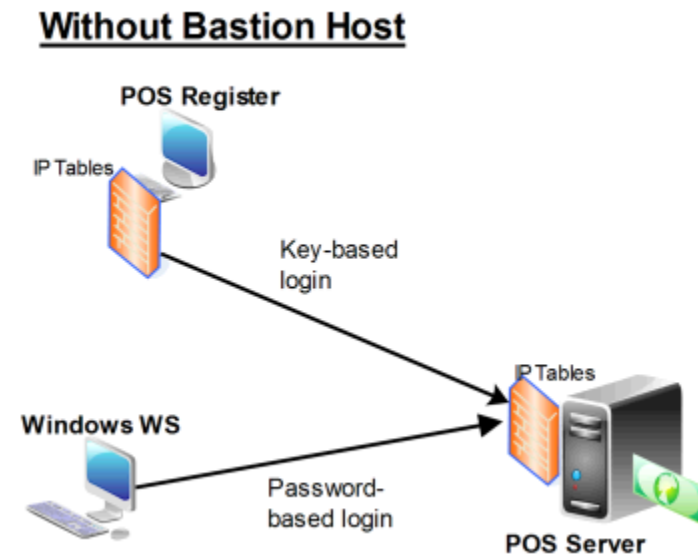
A firewall can base its decisions on whether to allow or deny a packet based on a number of different factors. These include:

- **Service Control:** Specifies the type of Internet services that will be allowed
 - For example, will you allow web traffic, email, or file sharing?
- **Direction Control:** Determines from which "direction" a particular service will be allowed or will be blocked
 - Web traffic (port 80 or 443) may be allowed outbound – someone is trying to access the internet; but not allowed inbound – someone is trying to access a website inside the organization's network
- **User Control:** May control access to a specific service based on the user that requested the service
- **Behavior Control:** Controls how a specific service may be used
 - For example, filter email attachments from unknown sources

Network Architecture

Here is a simple network diagram (of a point-of-sale [POS] network) showing how firewalls can protect various parts of the network

However, notice that there is direct access to the POS server



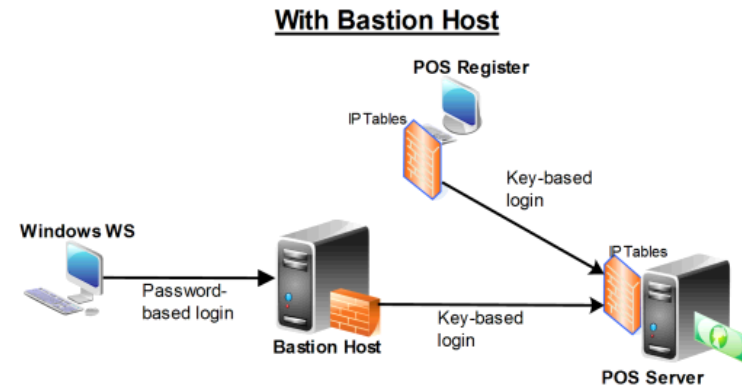
Network Architecture

Notice that, with the bastion host, there are additional protections for the POS server

If the POS server needs certain services active to provide functionality, these could be targeted by an attacker

A bastion host doesn't need to have additional services activated, so it can be a much tougher target for an attacker

- It is better to have a specially hardened and protected host – potentially running a secure operating system – as the access point to your internal network



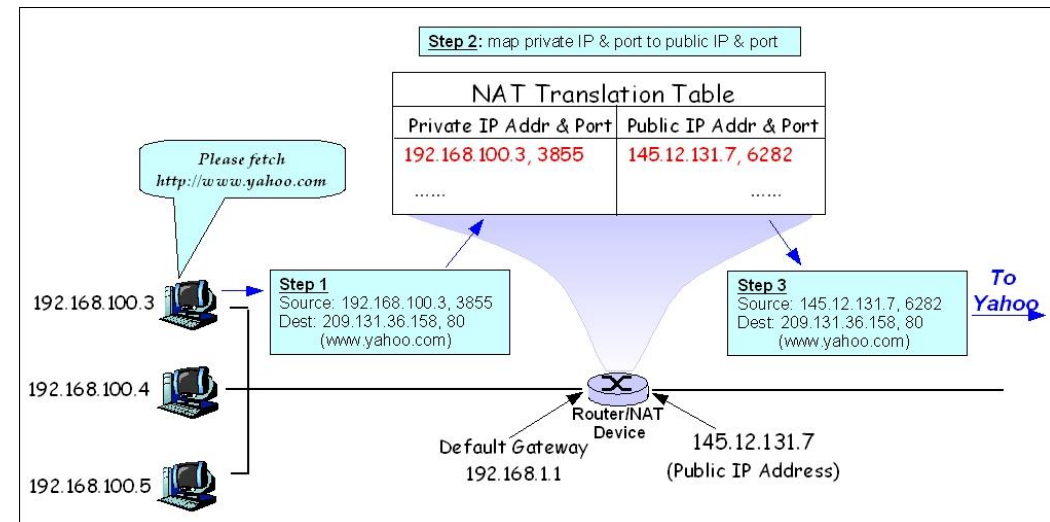
Network Address Translation (NAT)

From Wikipedia:

- **Network address translation (NAT)** is a method of mapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.
- https://en.wikipedia.org/wiki/Network_address_translation

Basically, it is a way of “hiding” your internal network configuration from the internet

- Every device behind your router or firewall gets a “new” source IP address and port – that being the public IP address of the router or firewall, and a port on that device – before being sent out to the internet
- When a packet for that combination of IP address and port returns to the router or firewall, it converts them back to the original source IP and port and sends it into the internal network for delivery to the original host



Network Address Translation (NAT)

Watch: *NAT Explained - Network Address Translation* by PowerCert Animated Videos

- <https://www.youtube.com/watch?v=FTUV0t6JaDA>
- You are responsible for knowing:
 - The initial motivation for creating NAT (IPv4 space exhaustion)
 - Understand the issues with not using NAT (more expensive, unnecessary, waste of public IP addresses)
 - How NAT works in a home environment
 - The number of addresses in IPv6

SCADA Systems Definitions

From Wikipedia:

- **SCADA: Supervisory control and data acquisition** is a control system architecture comprising computers, networked data communications and graphical user interfaces for high-level supervision of machines and processes. It also covers sensors and other devices, such as programmable logic controllers, which interface with process plant or machinery.
 - <https://en.wikipedia.org/wiki/SCADA>
- **Programmable Logic Controller (PLC)**: is an industrial computer that has been ruggedized and adapted for the control of manufacturing processes, such as assembly lines, machines, robotic devices, or any activity that requires high reliability, ease of programming, and process fault diagnosis.
 - https://en.wikipedia.org/wiki/Programmable_logic_controller
- **Distributed Control System (DCS)**: is a computerised [sic] control system for a process or plant usually with many control loops, in which autonomous controllers are distributed throughout the system, but there is no central operator supervisory control.
 - https://en.wikipedia.org/wiki/Distributed_control_system

SCADA Systems Definitions

From Wikipedia:

- **Modbus**: *Is a data communications protocol originally published by Modicon (now Schneider Electric) in 1979 for use with its programmable logic controllers (PLCs). Modbus has become a de facto standard communication protocol and is now a commonly available means of connecting industrial electronic devices.*
 - <https://en.wikipedia.org/wiki/Modbus>
- **Remote Terminal Unit (RTU)**: *A microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA (supervisory control and data acquisition) system by transmitting telemetry data to a master system, and by using messages from the master supervisory system to control connected objects.*
 - https://en.wikipedia.org/wiki/Remote_terminal_unit

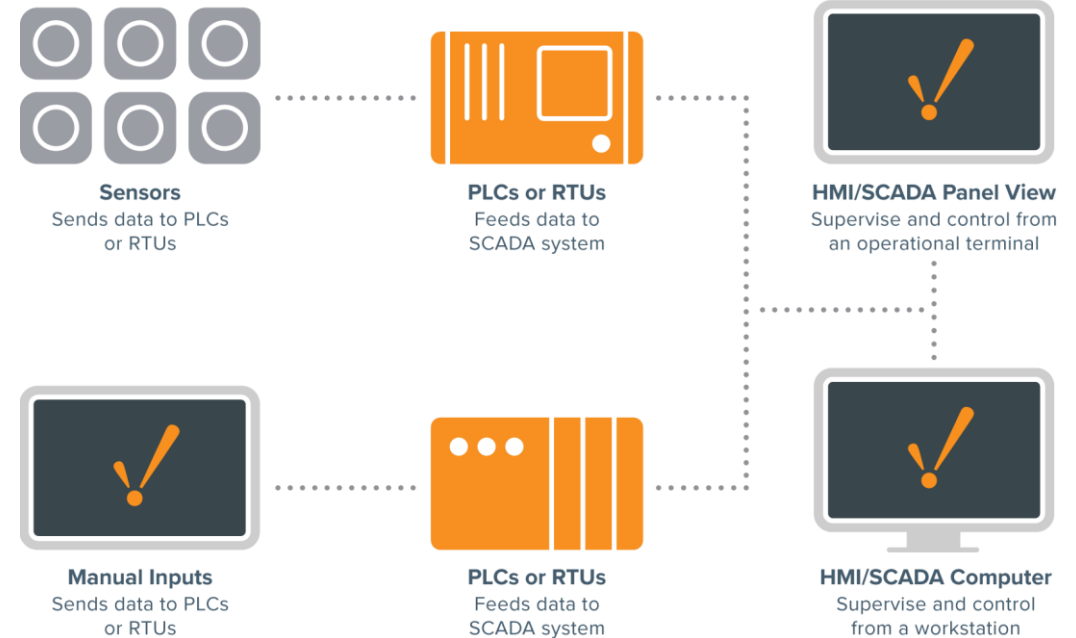
SCADA Systems

Read: *What is SCADA?* By Inductive Automation:

- <https://inductiveautomation.com/resources/article/what-is-scada>
- You are responsible for:
 - The definition of SCADA (First paragraph and bullets)
 - The components of a SCADA architecture (PLCs, RTUs, HMIs, sensors, end devices)
 - Characteristics of Modern SCADA Systems

Watch: *PLC vs SCADA vs DCS* by 4.0 Solutions

- <https://www.youtube.com/watch?v=uhZnVwkWgFw>
- You are responsible for understanding the general differences between the types of systems



SCADA Systems

From: *What is SCADA?* By Inductive Automation

- *Modern SCADA systems allow real-time data from the plant floor to be accessed from anywhere in the world. This access to real-time information allows governments, businesses, and individuals to make data-driven decisions about how to improve their processes.*

Key issues:

- **Many SCADA components were not designed to be secure** – they were designed to do their specific task
- **They can be fragile enough that they crash from a simple network scan**

Key issues Cont'd:

- Many protocols used by SCADA systems are inherently insecure
 - No authentication
 - Any system on the network can send a message to request data, or request an action by another component
- Many SCADA systems are deployed for a long time
 - Unlike traditional IT systems, their upgrade cycles may be measured in decades
 - For example, a building control system may be built into the walls and floors of the building – requiring a complete renovation to change (20-30+ year timeframes)
 - This prevents the latest security systems from being integrated into the devices

SCADA Systems

Watch: *What is SCADA?* By RealPars

- <https://www.youtube.com/watch?v=nIFM1q9QPJw>
- You are responsible for knowing:
 - Definition of Human Machine Interface (HMI) (facilitates interaction with field devices)
 - Examples of SCADA devices (pumps, motors, sensors)
 - The biggest advantage to using SCADA (no longer need people on site)
 - The advantage of open communication protocols (can use components from different vendors)

SCADA Systems

There are also other terms used to refer to SCADA systems

- Operational Technology – similar to, but separate from, Information Technology systems
- Industrial Control Systems
- Cyber-Physical Systems

Basically, while some have nuances to the definitions, the general idea for them all is:

- Information systems that control, or are part of, processes that occur in the physical (real) world

The general progression in terms (that I experienced) was:

- SCADA became Industrial Control Systems (ICS)
- Then, because these systems are used in more than just industrial applications, it started to be referred to as Operational Technology or “OT”
- Then, because the systems were connected to corporate networks or the internet, and individuals could receive information at their regular workstations, IT systems got added into the acronym for: IT/OT
- Then, OT/ICS “oh-ticks” became a popular term to emphasize the types of processes involved
- Then, finally, cyber-physical systems became the common term for these systems
- ***Note: This may vary by business sector, or geographic region – but I wanted you to be aware that all of these terms are related***

ICS-CERT

The Industrial Control Systems Cyber Emergency Response Team is a team under the Cybersecurity & Infrastructure Security Agency (CISA) – which is part of the Department of Homeland Security (DHS)

- They provide alerts and support for ICS-related cyberattacks
- <https://www.cisa.gov/ics>
- **Note:** On this page they refer to ICS, and OT environments, and IT and OT

In their report on ICS ransomware, Dragos uses ICS/OT instead of OT/ICS:

- <https://www.dragos.com/blog/industry-news/dragos-industrial-ransomware-analysis-q1-2022/>

Shodan


From Shodan.io:

- *Search Engine for the Internet of Everything*
 - *Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.*

As you can see from their description – Shodan can be used to find a number of SCADA devices in power plants or refrigerators

Even without signing up for a free account, you can get information such as:

- Location
- IP Address
- Open ports
- Certificate information

 **Beyond the Web**

Websites are just one part of the Internet. Use Shodan to discover everything from power plants, mobile phones, refrigerators and Minecraft servers.

Securing ICS – Best Practices

Use network segmentation

- Do not expose your ICS on the Internet
- Do not expose all of your ICS on your internal network
- Use a DMZ or data diode (one-way communication) to export data from ICS to corporate network

Patch your systems

- This is not easy since many devices are hard-coded to communicate with a specific update server
- Can be done during maintenance windows when a plant or process is idle

Use IT Best Practices:

- Change default passwords
- Disable unused services

Security Supervision

- IPS have signatures for ICS
- Create your own signatures

Securing ICS

One project that is working to secure ICS is MOSAICS

- Stands for MOre Situational Awareness for Industrial Control Systems
- Joint effort by multiple government agencies and national labs (including Sandia National Labs)

From: *With MOSAICS, Johns Hopkins APL Brings the Future of Industrial Cybersecurity into Focus:*

- <https://www.jhuapl.edu/NewsStory/220405-mosaics-future-ics-cybersecurity>
- *Known as MOSAICS — from “More Situational Awareness for Industrial Control Systems” — the working prototype has already demonstrated its value to the U.S. Navy, which is expanding its deployment of the system after initial testing demonstrated a 100% success rate with fewer than 1% false positives.*

Also:

- <https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2019/09/20181019-Unclassified-MOSAICS-Slicksheet.pdf>

Summary

Supervisory control and data acquisition (SCADA) is a system of software and hardware elements that allows industrial organizations to:

- Control industrial processes locally or at remote locations.
- Monitor, gather, and process real-time data
- Directly interact with devices such as sensors, valves, pumps, motors, and more through human-machine interface (HMI) software
- Record events into a log file