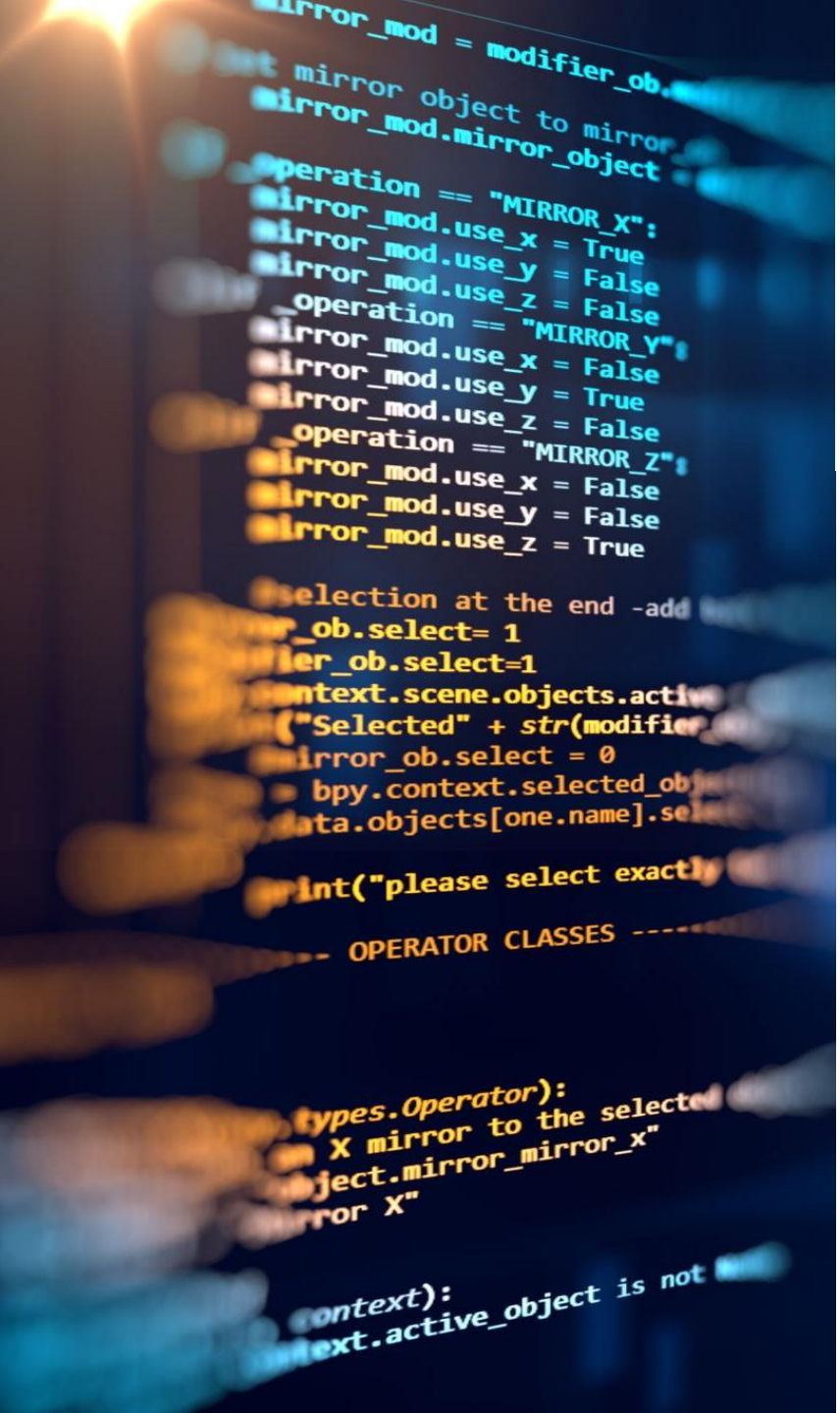
Protecting Remote Access

Lecture 6
Part 2

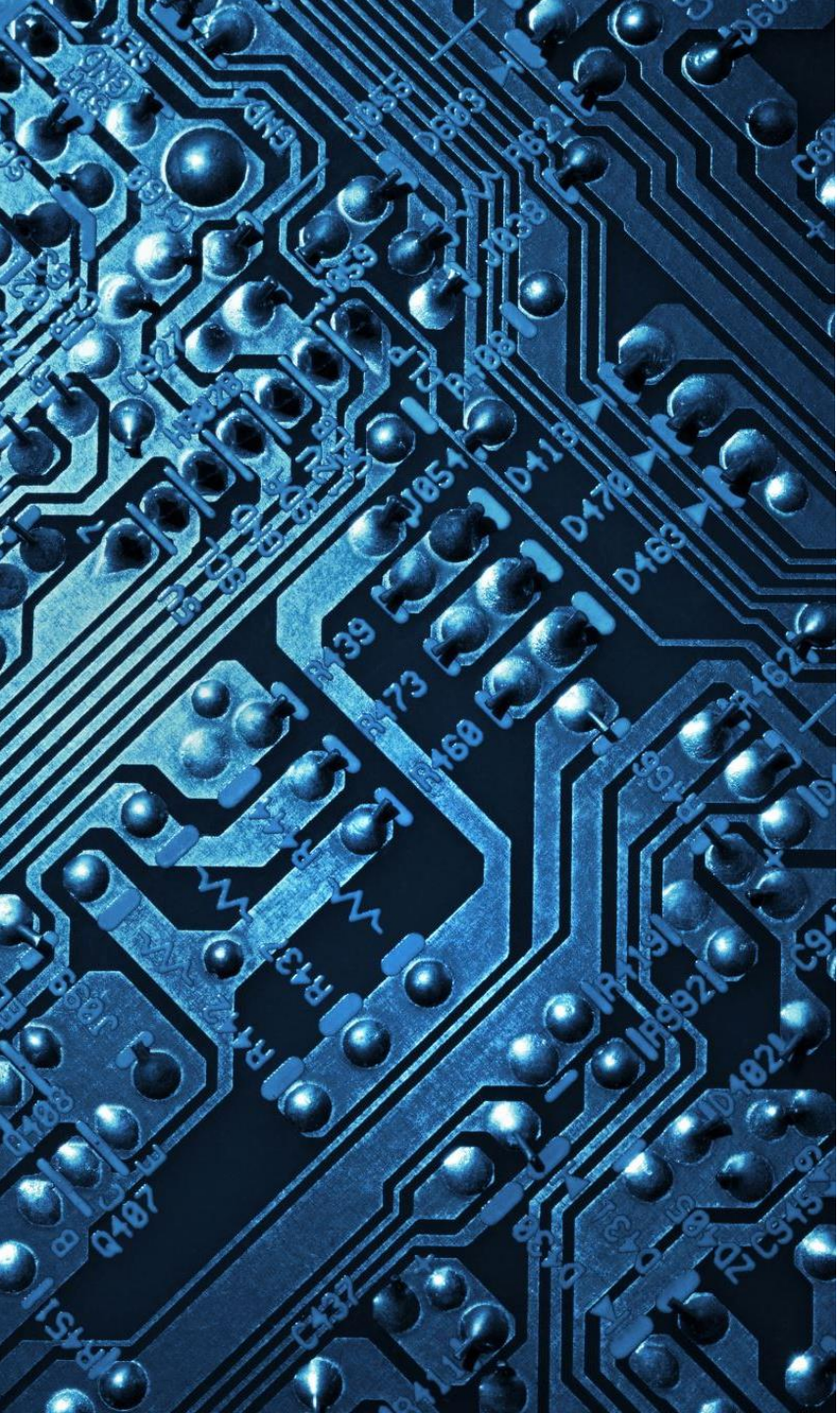
Chapter 9

Professors:
David A. Cass &
Kevin McKenzie



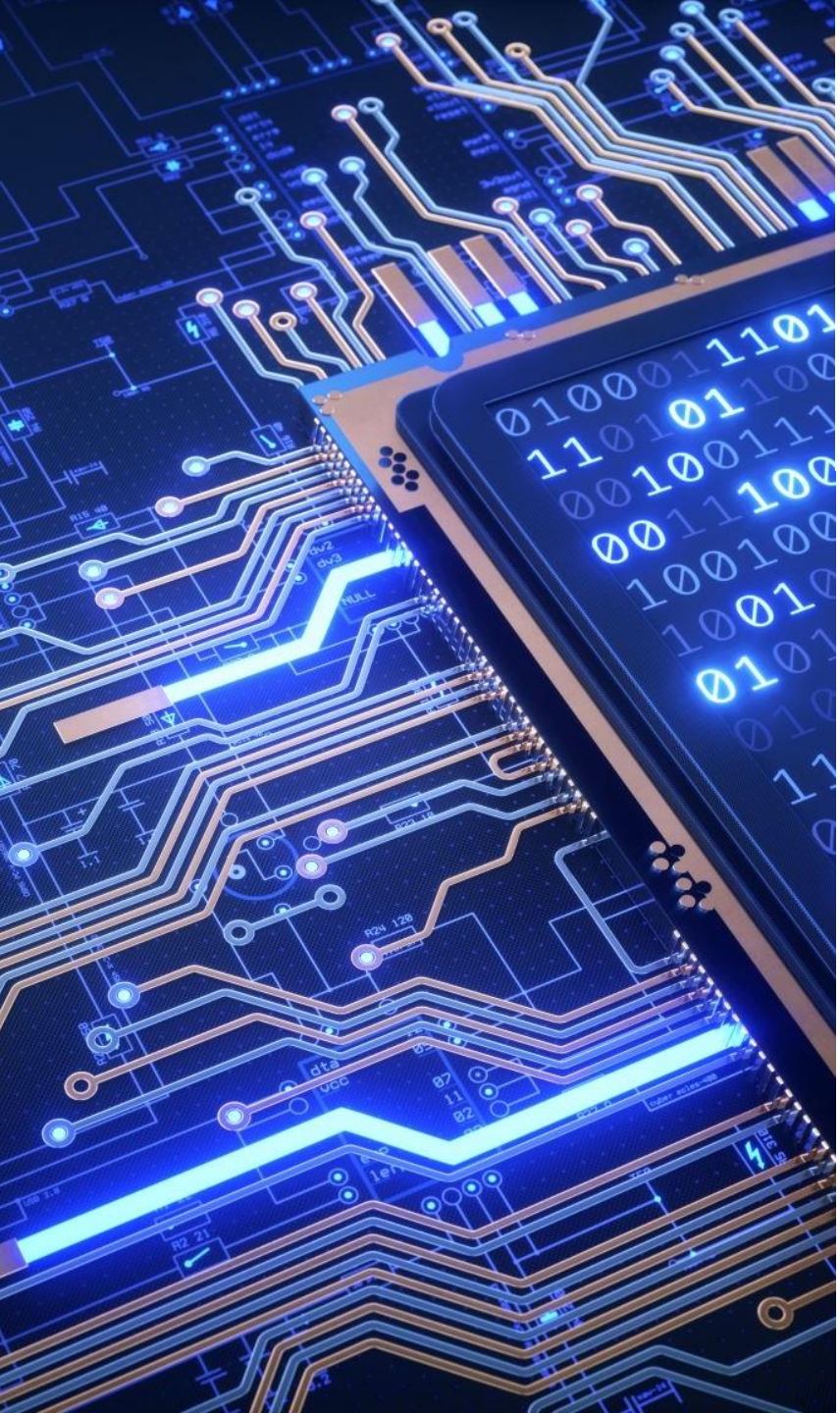
In this chapter, you'll learn to:

- Analyze and Differentiate Between Anti-Virus/Anti-Malware Products.
- Secure the Web Browser of a Standalone Computing Device.
- Configure and Test a Local Firewall Installation.
- Explain the Importance of Application Security.



In this chapter, you'll learn to:

- Audit Local Operating System Services and Events.
- Establish a Local Security policy on a Standalone Host Device.
- Describe the Importance of Conducting Local Updates and Patch Maintenance Activities.

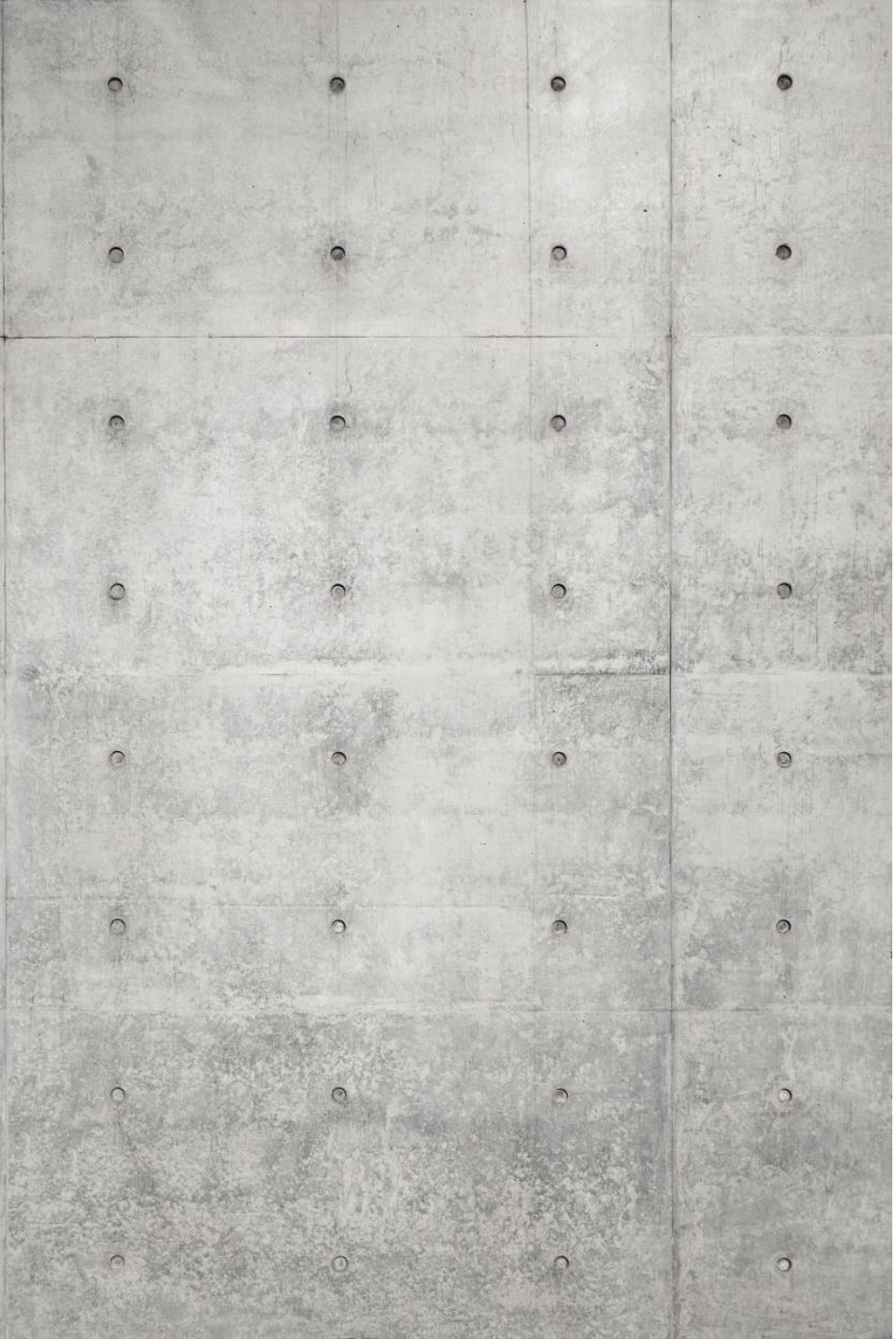


Protecting from Internet-based Threats

1. Use a secure connection.
2. Establish and configure a firewall to control the flow of information between the computing device and the Internet.
3. Install and use anti-malware on the local computer.
4. Remove unnecessary software from the computer.

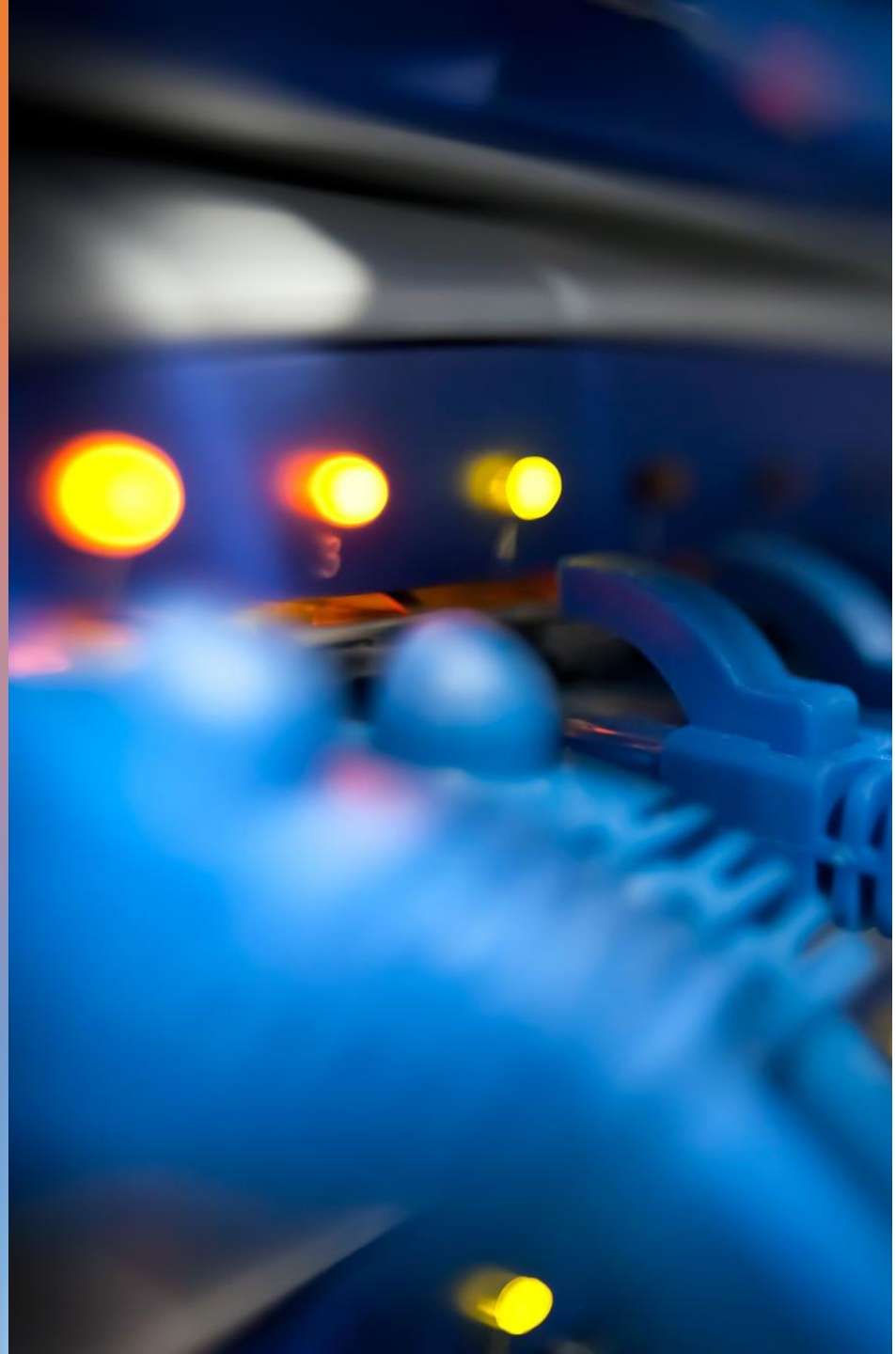
Protecting from Internet-based Threats

5. Disable any nonessential services running on the computer.
6. Disable unnecessary OS default features.
7. Secure the Web browser.
8. Apply operating system and application software updates and patches.
9. Require strong passwords.



Basic Items to consider when securing a router's security features

- Change the login username and default password. (The defaults are published in the user's setup instructions and, therefore, are known to everyone.)
- For wireless network connections, change the default SSID setting.

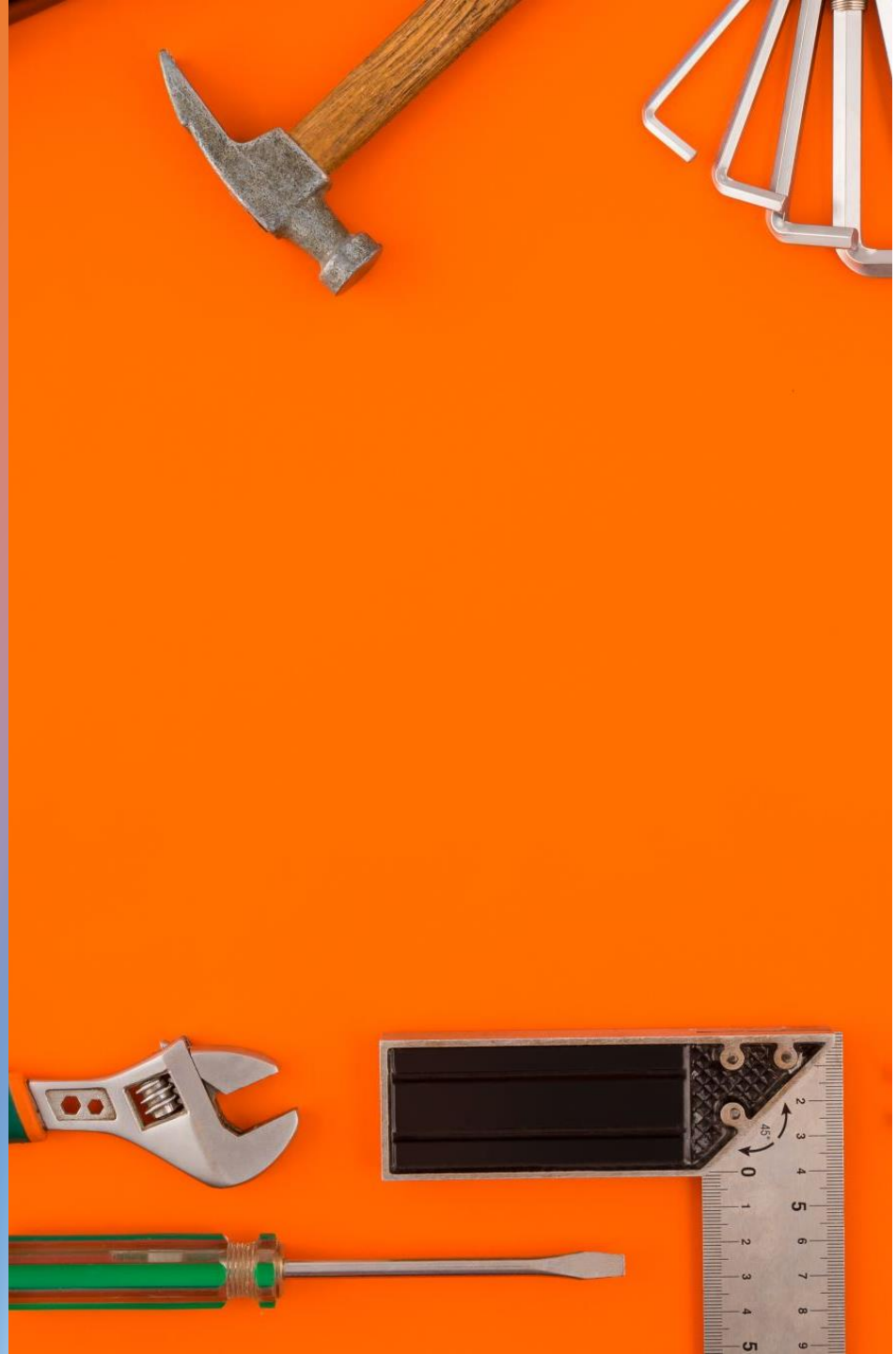


Basic Items to consider when securing a router's security features

- Configure the wireless network with the highest level of encryption available – preferably WPA2-AES for maximum data confidentiality.
- Identify trusted wireless connections by conducting MAC address filtering.

Three Types of User-related Logins

- Logons to the local machine
- Logons to a specific software application
- Network logons



Tools to Protect Computing Devices from exploitation through the Internet

- Local firewalls
- Host-based intrusion-detection systems
- Browser security options
- Antivirus/anti-malware tools
- Software updates and patches

A Word about Firewalls

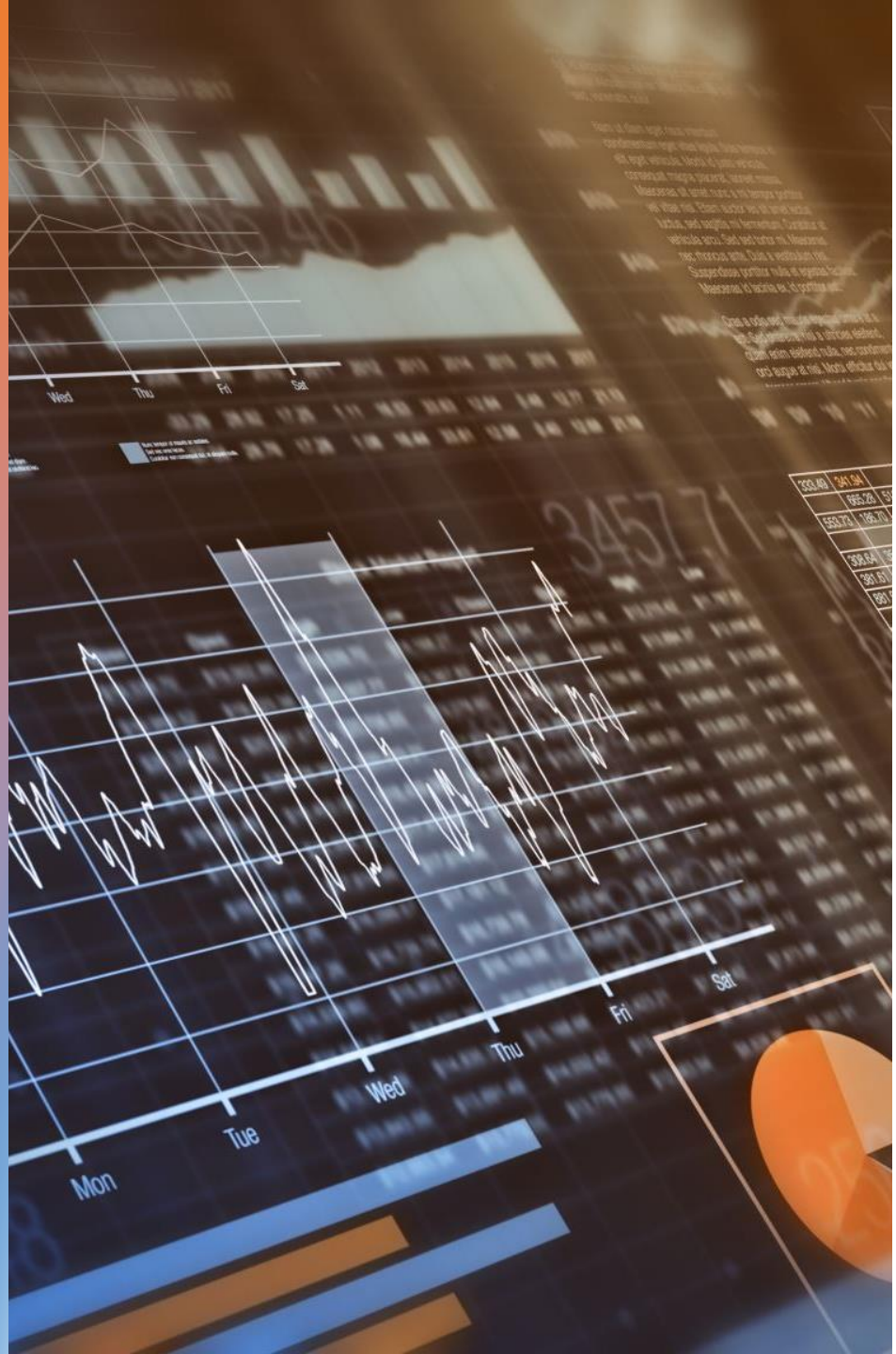
- Local software firewalls are designed to provide protection from outside attacks by preventing unwanted connections from Internet devices. Software-based firewall services are designed to protect individual computers that are directly connected to the Internet through dial-up, LAN, or high-speed Internet connections.

All IDS Devices are Based on One of Two Strategies

- Signature Analysis – Incoming and outgoing traffic is compared to a database of stored specific code patterns that have been identified as malicious threats.
- Anomaly analysis – Incoming and outgoing traffic is compared to an established baseline of normal traffic for the system.

Methods of Implementing Statistical Anomaly Detection

- Profile-based anomaly-detection systems
- Threshold-based anomaly-detection systems



Profile-Based Anomaly Detection Systems

- Rule-based anomaly detection – This detection method analyzes audit records to generate rules based on past usage patterns to generate the “rules” set. The system then monitors the traffic looking for patterns that don’t match the rules.

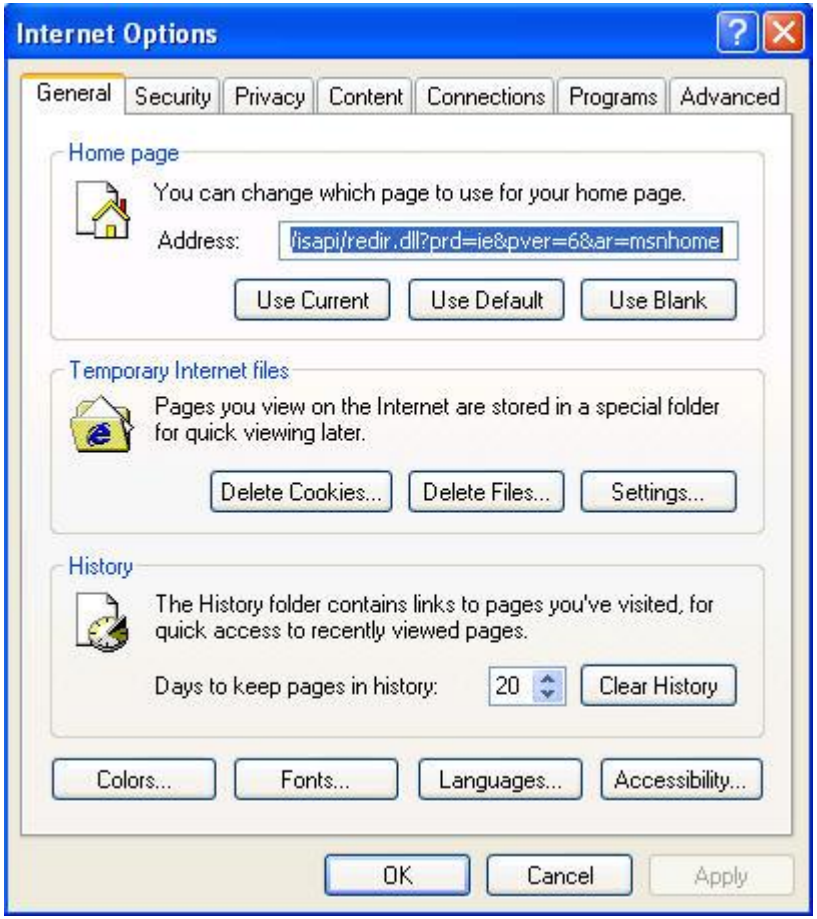
Profile-Based Anomaly Detection Systems

- Penetration detection – These systems generate rules based on known penetration occurrences, system weaknesses, or behavior patterns. For this reason, they are normally specific to a given host system. They also typically include rules generated by security experts that are current with security activities.

IDS Notifications

- In all IDS types, the administrator is notified when a potential attack is detected.

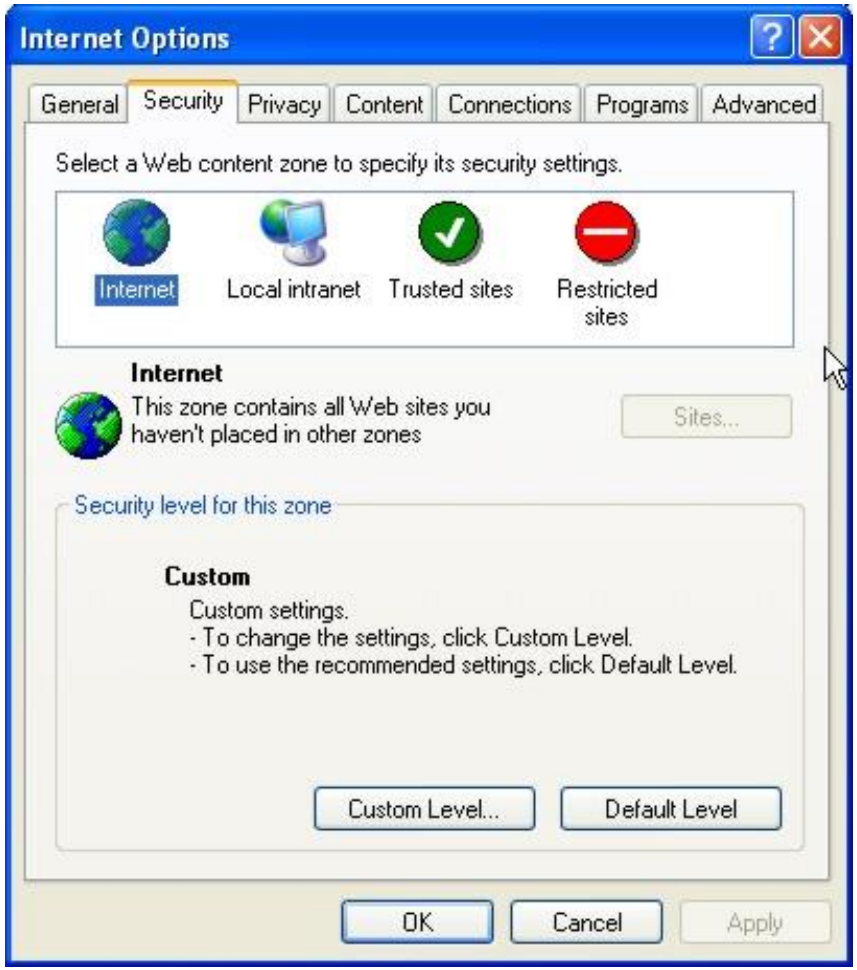
Internet Options

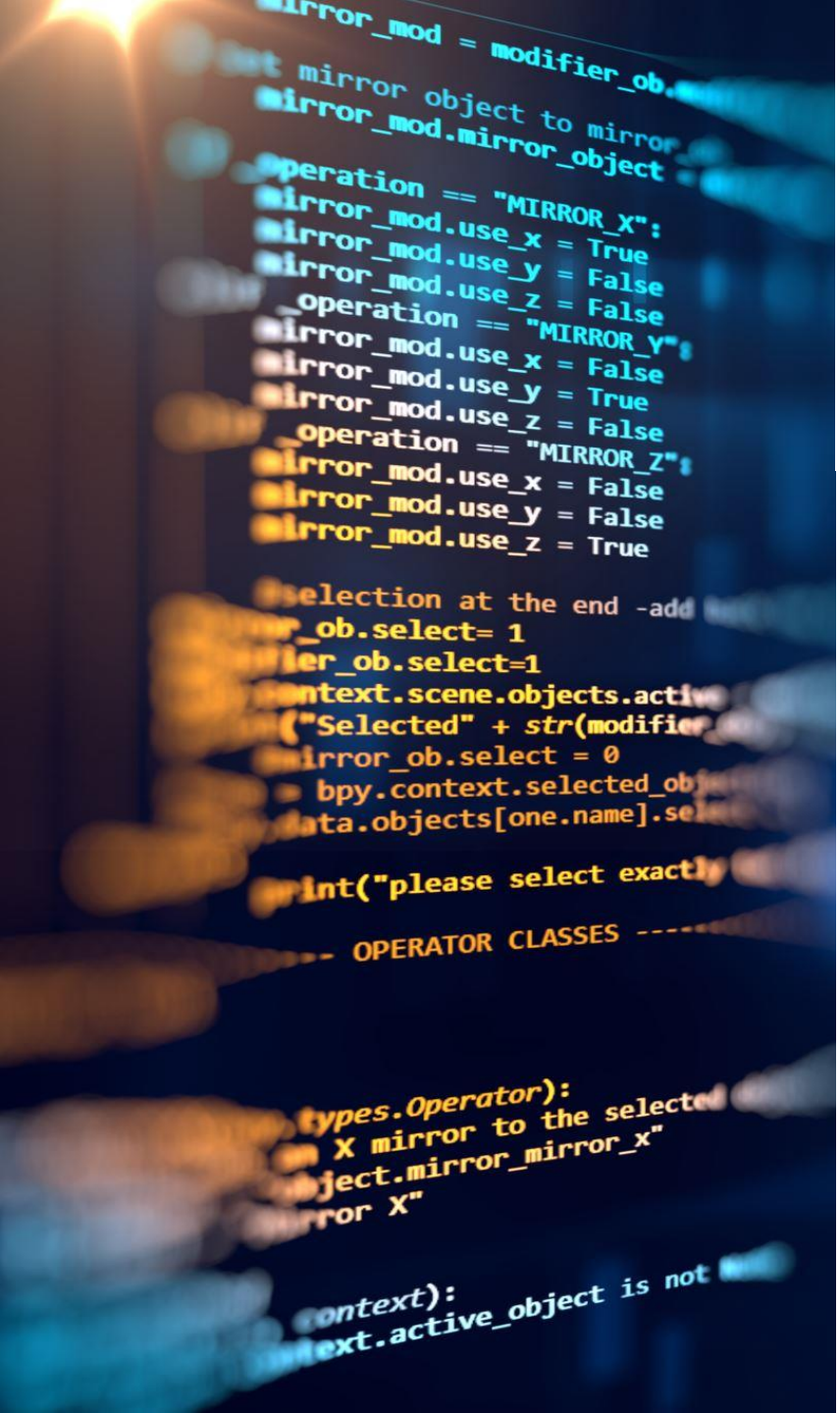


Internet Options

- Configuring security levels
- Configuring scripting
- Configuring proxies
- Controlling cookies

IE Security Tab

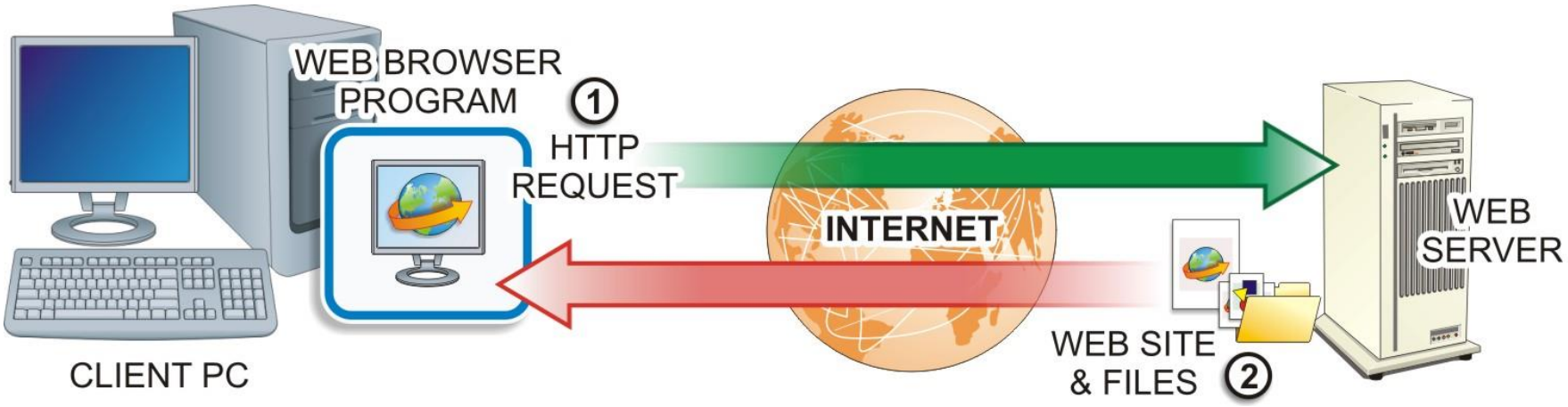




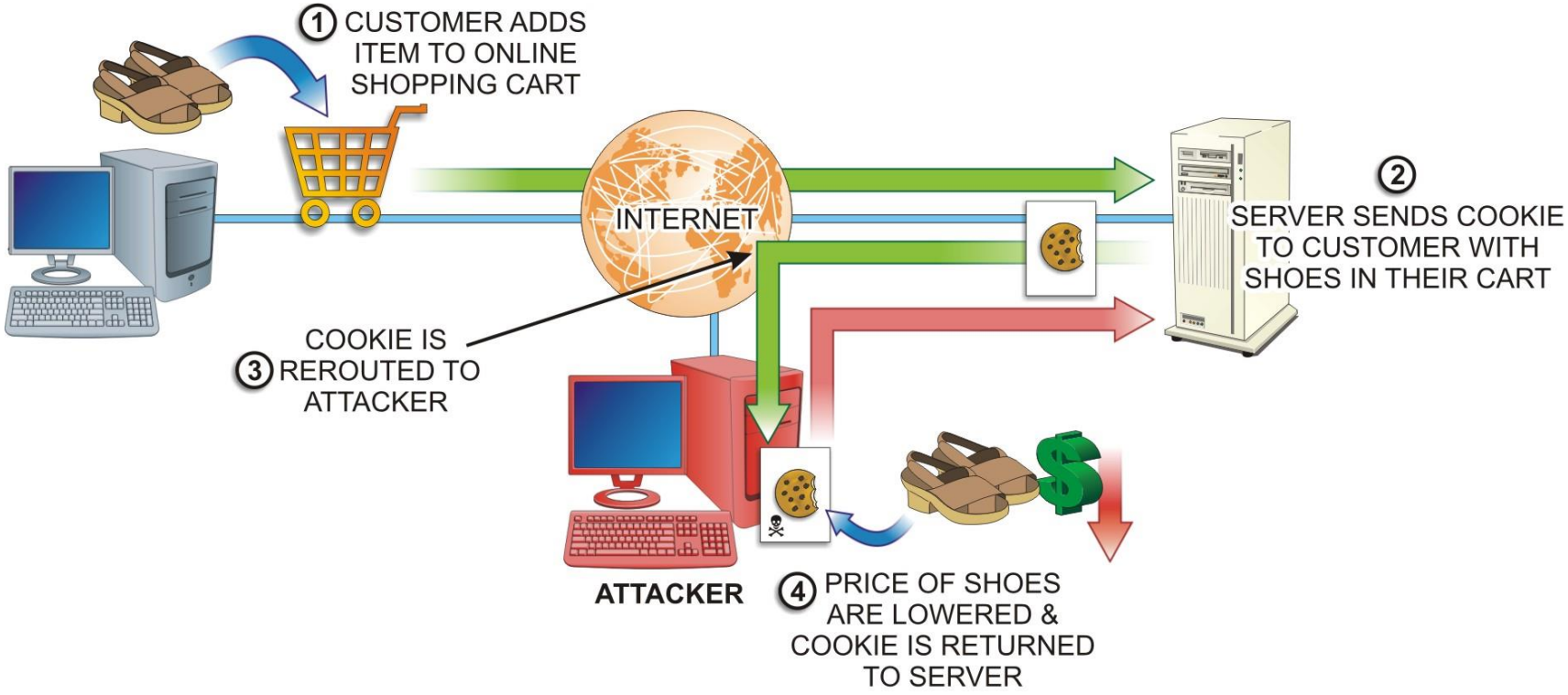
A Word about VBScript

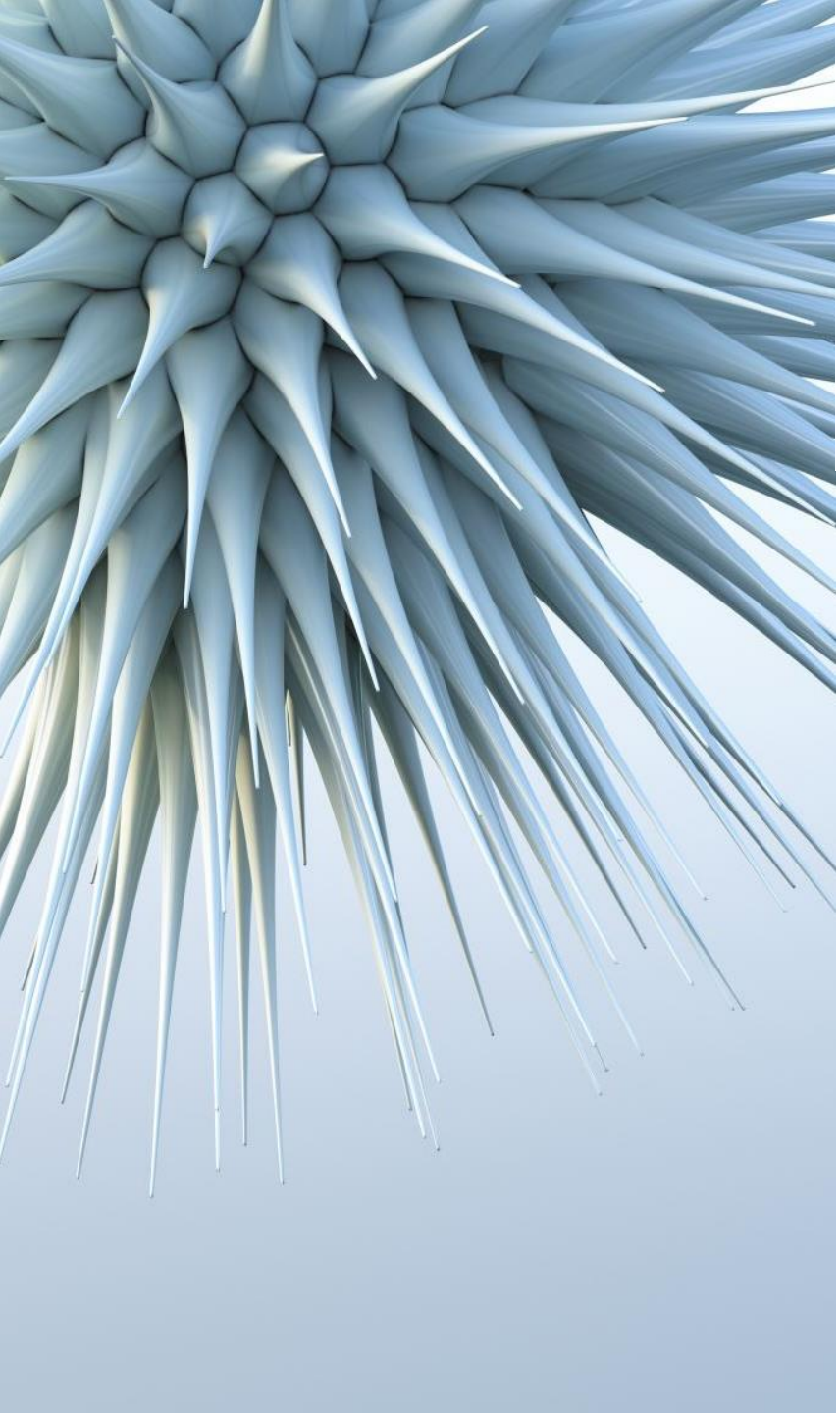
- VBScript is another scripting language that is unique to Microsoft Windows Internet Explorer. VBScript is similar to JavaScript, but it is not as widely used in websites because of limited compatibility with other browsers.

HTTP Transfer Operations



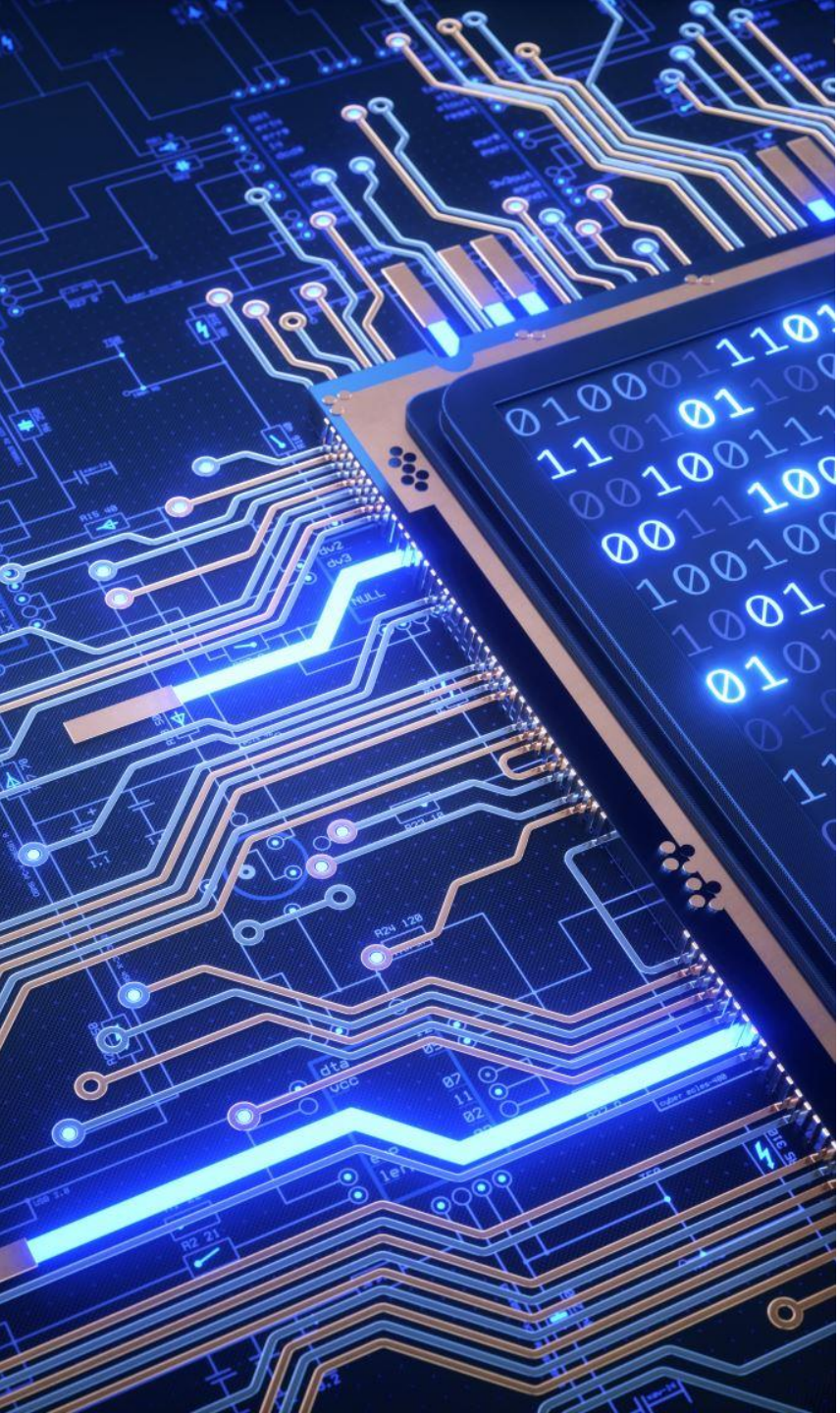
Cookie Poisoning





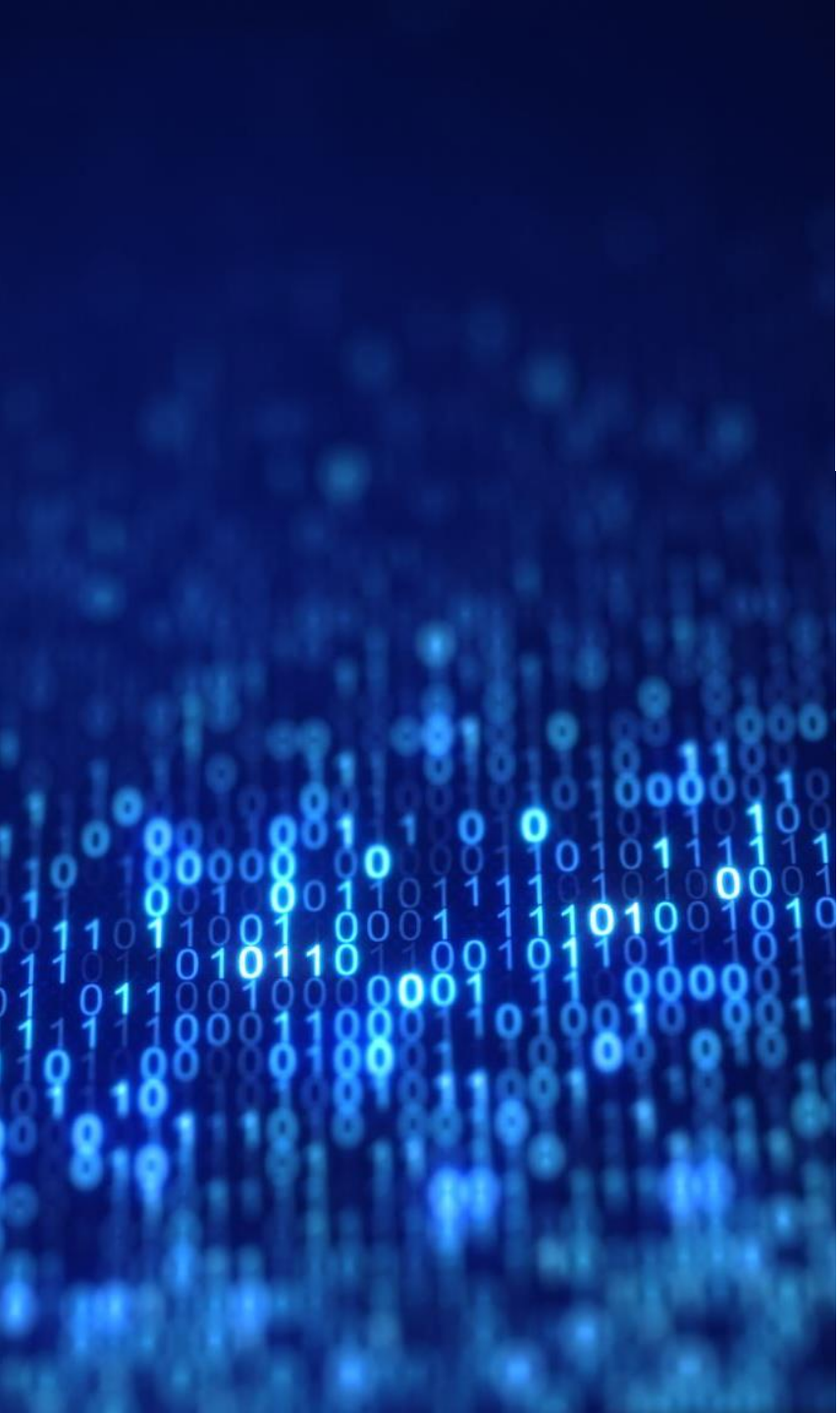
Defending Against Malicious Software

- *Viruses* are destructive programs designed to replicate and spread on their own. Viruses are designed to replicate themselves within a local computer environment. This most often happens when users download programs from the Internet or open email attachments. Many “free” products obtained from the Internet have something attached to them – a virus, spyware, or some other form of malware.



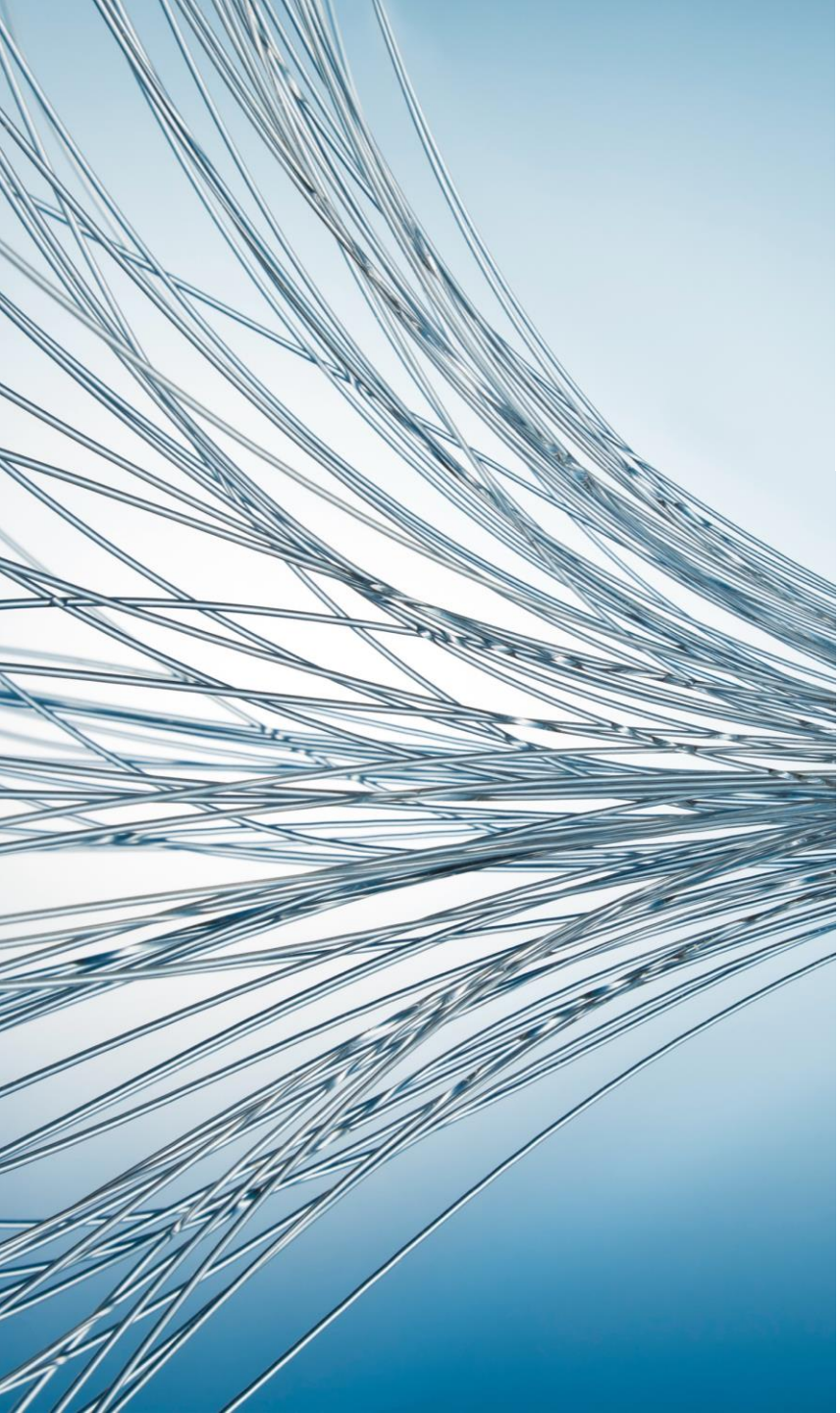
Defending Against Malicious Software

- *Worms* (sometimes referred to as network viruses) are circulated through a network connection. Unlike a virus, worms do not need a host program in order to infect your computer. Worms search for vulnerabilities to exploit in an application. Once the worm has taken advantage of the vulnerability, it seeks to replicate to another computer on the network. While initially intended to slow down network environments, worms often leave payloads on a system to further malicious activity.



Defending Against Malicious Software

- *Trojans* appear to be a legitimate program that might be found on any system. They are made to appear to be actual applications so that users will be tricked into using them. Although they function and work properly, they have malicious code that initiates when the application is launched.



Defending Against Malicious Software

- *Rootkits* are a type of software designed to gain administrative control of a computer system while remaining undetected. Normally, the purpose is to enable malicious operations to occur on a target computer without the knowledge of its users or system administrators. Rootkits can occur in hardware or software by going after the BIOS, boot loader, OS kernel, and sometimes applications or libraries.

Defending Against Malicious Software

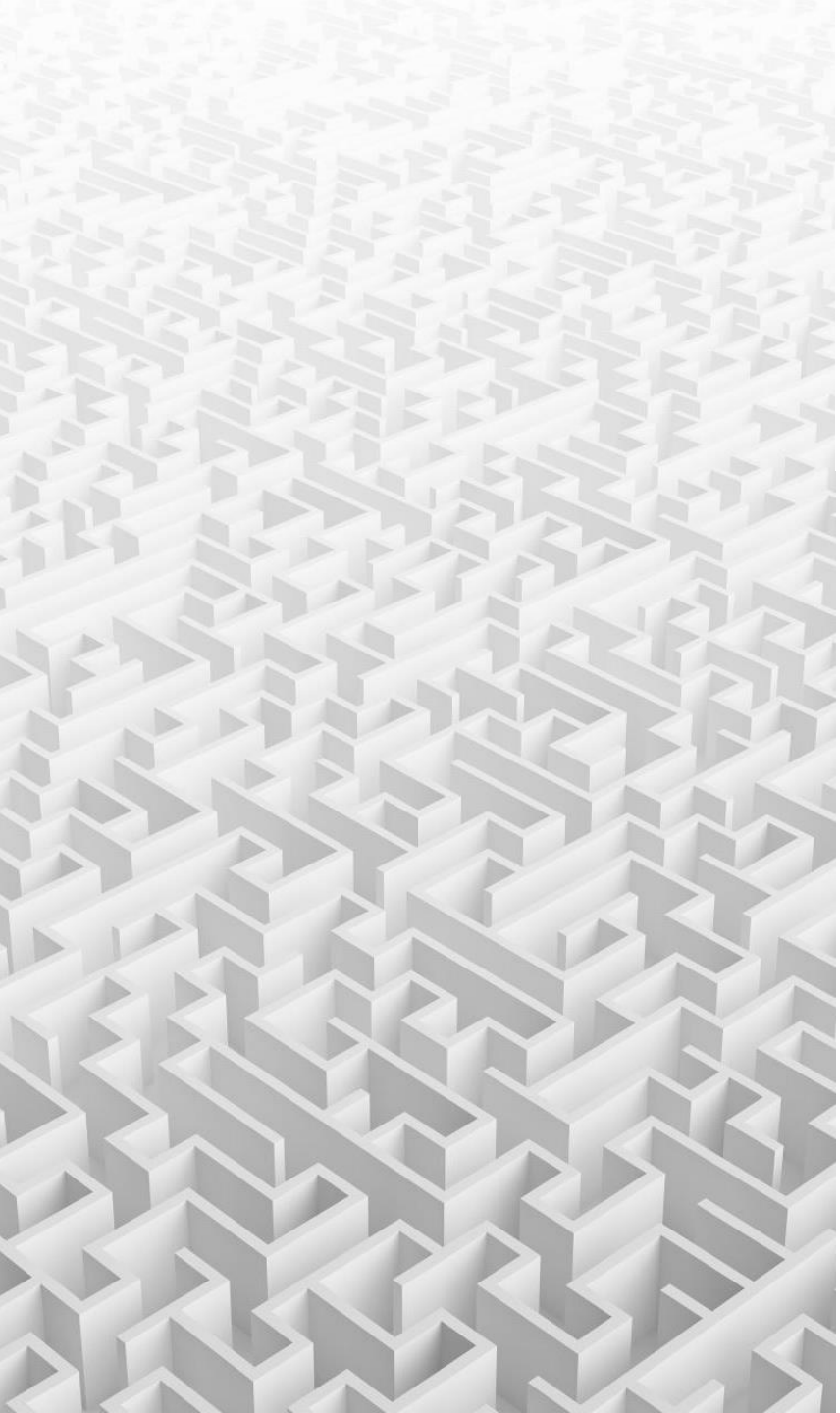
- *Ransomware* is software designed to keep the user from their data and hold it hostage for payment. Spam email is the most common delivery vehicle for spreading the malware. It is then activated by the user clicking an attachment or link in the email message. It then disables essential system services or even locks the computer so that the user cannot gain access to it.

Defending Against Malicious Software

- *Spyware* programs are generally introduced to the system through Internet downloads that appear to be useful programs. Unlike viruses and Trojans, spyware typically does not self-replicate. Once spyware is installed on a system, it monitors the system's operation and collects information such as usernames, passwords, credit card numbers, and other PII.

Defending Against Malicious Software

- *Adware* programs introduce unwanted, unsolicited advertising displays to web browsers. They can also be designed to gather user selection information from the browser, constructing a more personalized advertising scheme. Adware is typically introduced to the system through downloads such as free software (freeware).

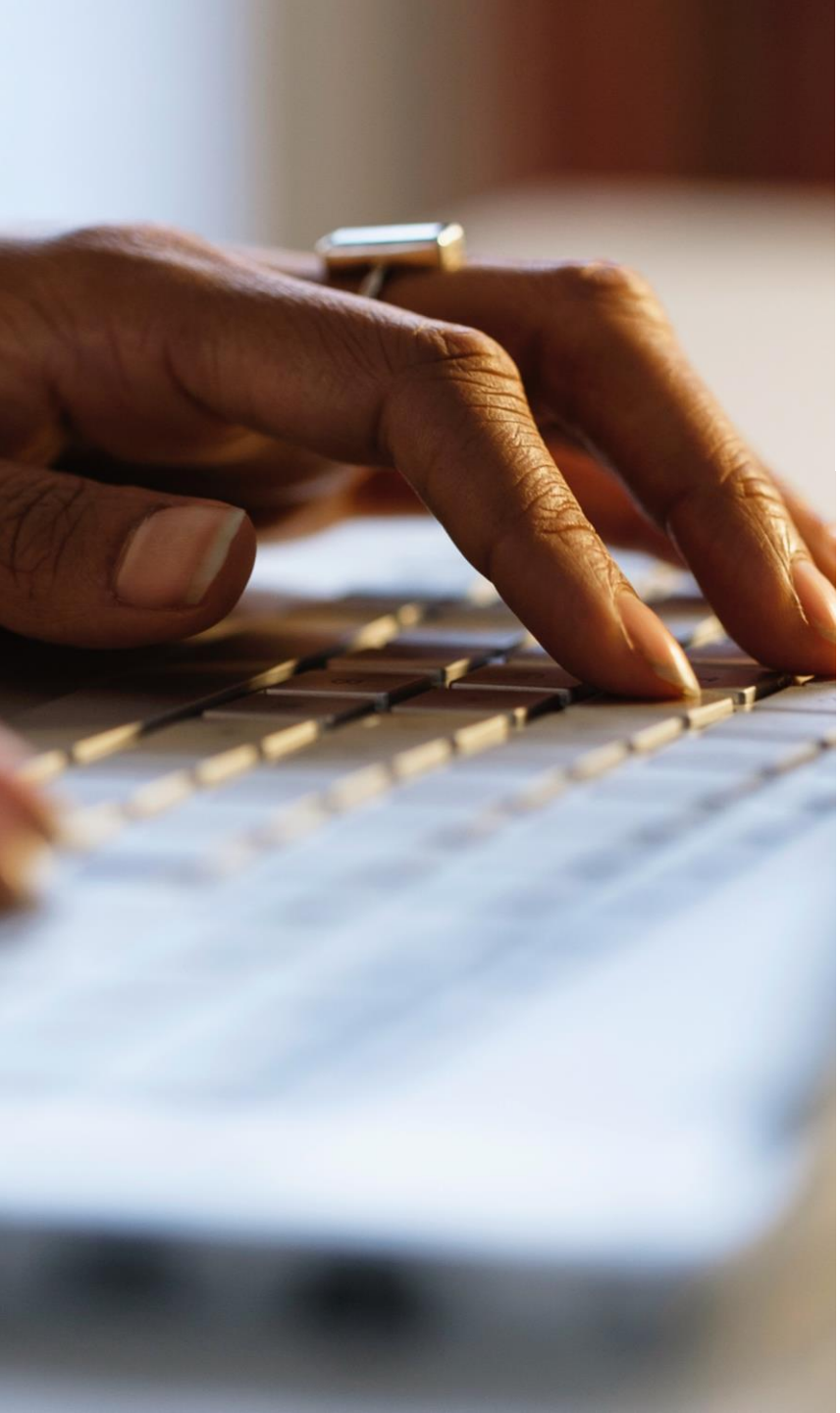


Defending Against Malicious Software

- *Logic bombs* are a type of malware typically used to delete data. A logic bomb is computer code that, much like other malware, is attached to a legitimate program. The code sits idle until a specific logical event is concluded. This includes a number of days passing, a number of programs being opened, or executing a program in a specific manner. Logic bombs are hard to detect because they are often included in large programs with thousands of lines of code.

Defending Against Malicious Software

- *Zombies* are infected computers that can be placed under the remote control of a malicious user. Zombies can be used to create Denial of Service (DoS) attacks that flood targeted networks to slow down and sometimes stop servers completely. Computers are often infected and become zombies by way of viruses, worms, and Trojans.



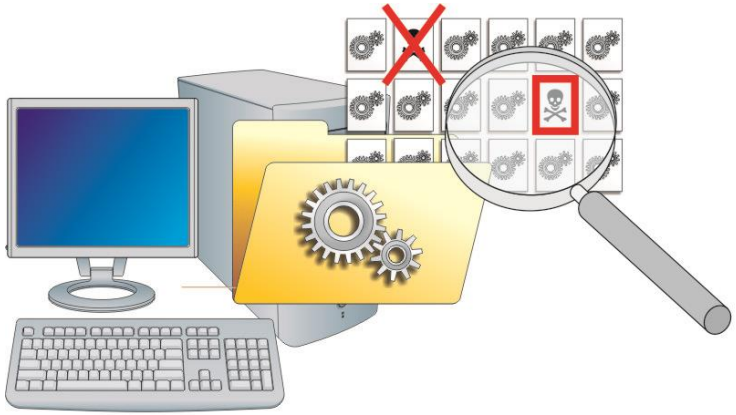
Defending Against Malicious Software

- *Botnets* are a large collection of zombies, or bots, controlled by a bot herder. This type of network can consist of literally millions of unsuspecting computers. Botnets can be used to send out spam (usually through email lists) originating from unsuspecting users' computers. It is estimated that 50 to 80 percent of spam worldwide is created by zombie computers.

Defensive Products to Protect PCs and their Data

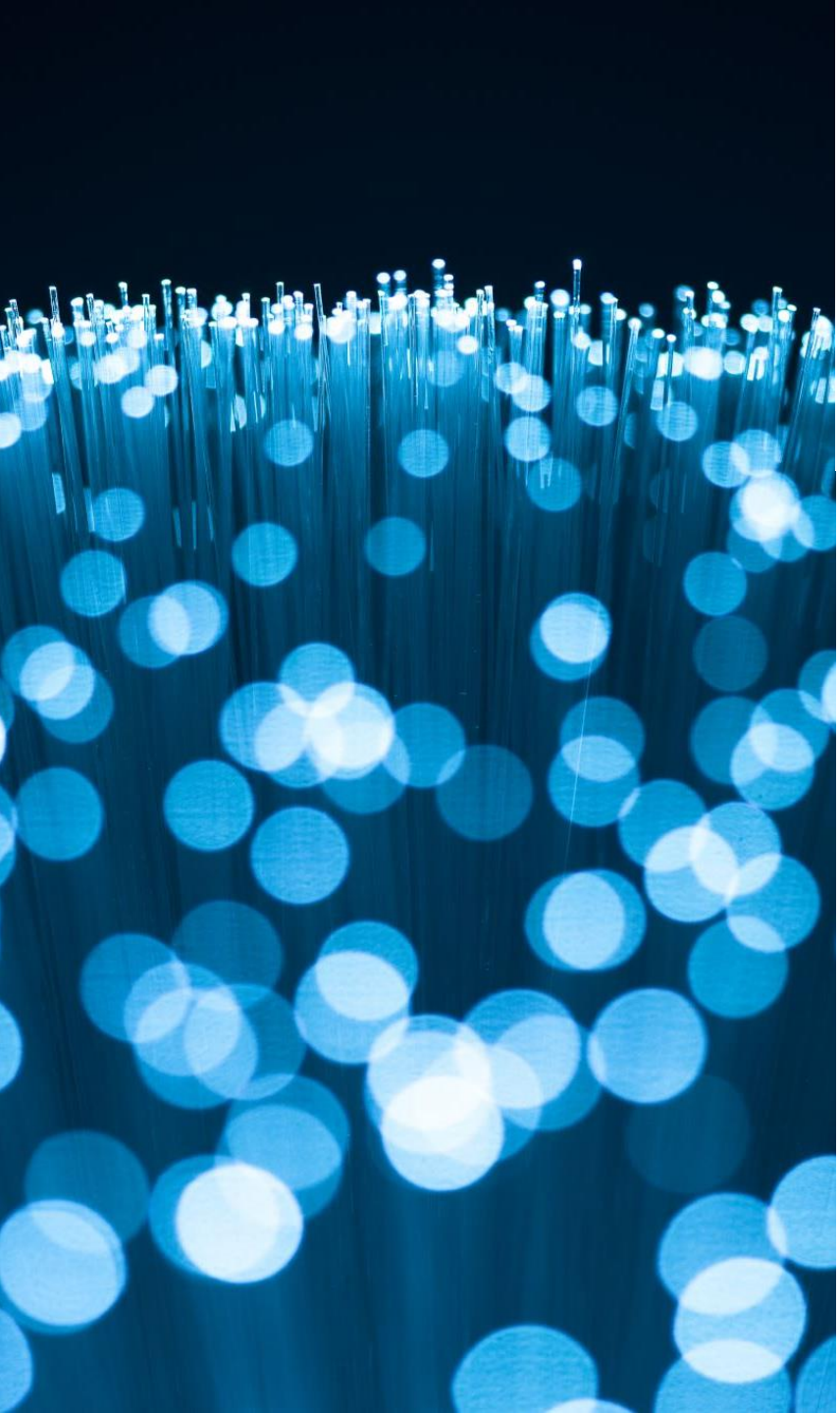
- Antivirus programs
- Antispyware programs
- Spam blockers
- Pop-up blockers

Antispyware Product Types



DETECT & REMOVE

INSTALLATION BLOCKING



Users can Fight Spyware in a Number of Other Ways

- Install a web browser other than Internet Explorer (for example, Chrome or Firefox).
- Download the newest browser version that offers better security features.

Users can Fight Spyware in a Number of Other Ways

- Work with an ISP who uses their firewalls and proxies to block sites that are known to distribute spyware.
- Download only software from reputable sites to prevent spyware that come attached to other programs.

Hardening Operating Systems

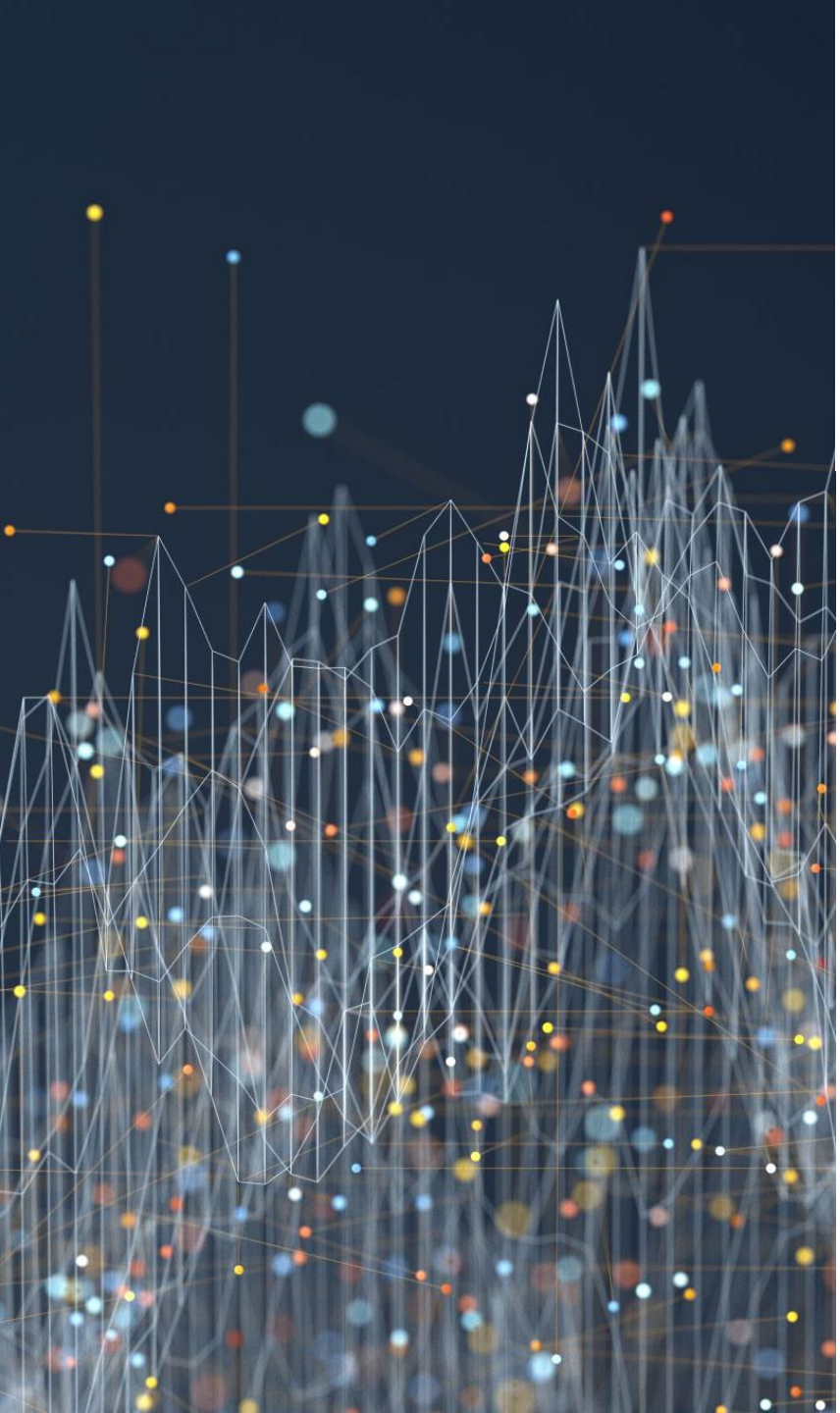
- Service packs
- Patches
- Updates

Conflicting Objectives in the Computer Software Industry

- Make the product as open and easy to use as possible so that otherwise nontechnical users will be able to work with it.
- Make the application bulletproof so that nothing bad can happen to it – ever.

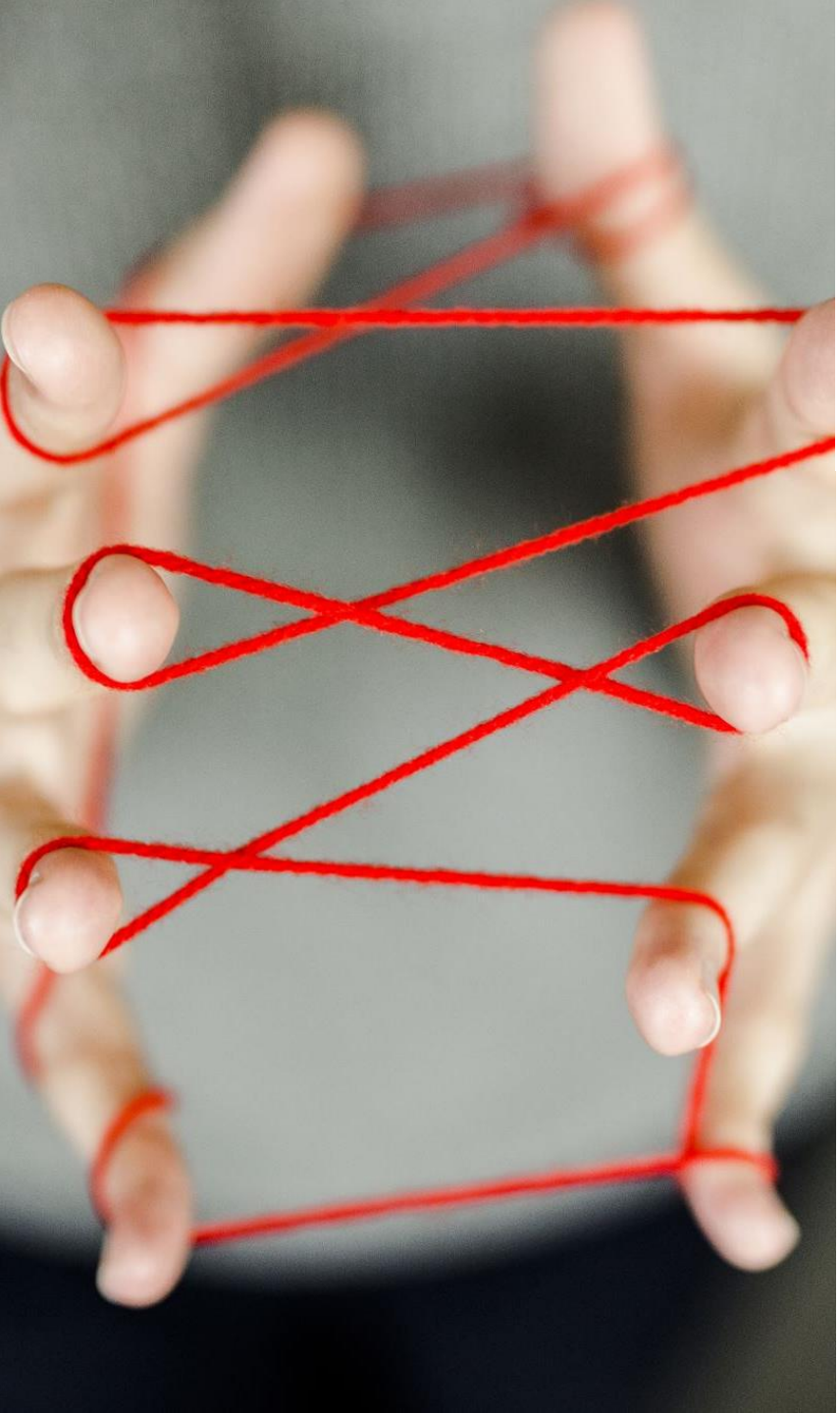
A Word about Black Hat Hackers

- A *black hat hacker* is an individual who possesses extensive programming skills and uses them to breech or bypass network security structures for malicious or criminal purposes. People in this category of hacker are also known as *crackers* or *dark-side hackers*.



A Word about Black Hat Hackers

- There are also *white hat* and *gray hat hackers* who also seek to exploit Internet security vulnerabilities and weaknesses, but not for malicious reasons (for example, to perform security system analysis checks).



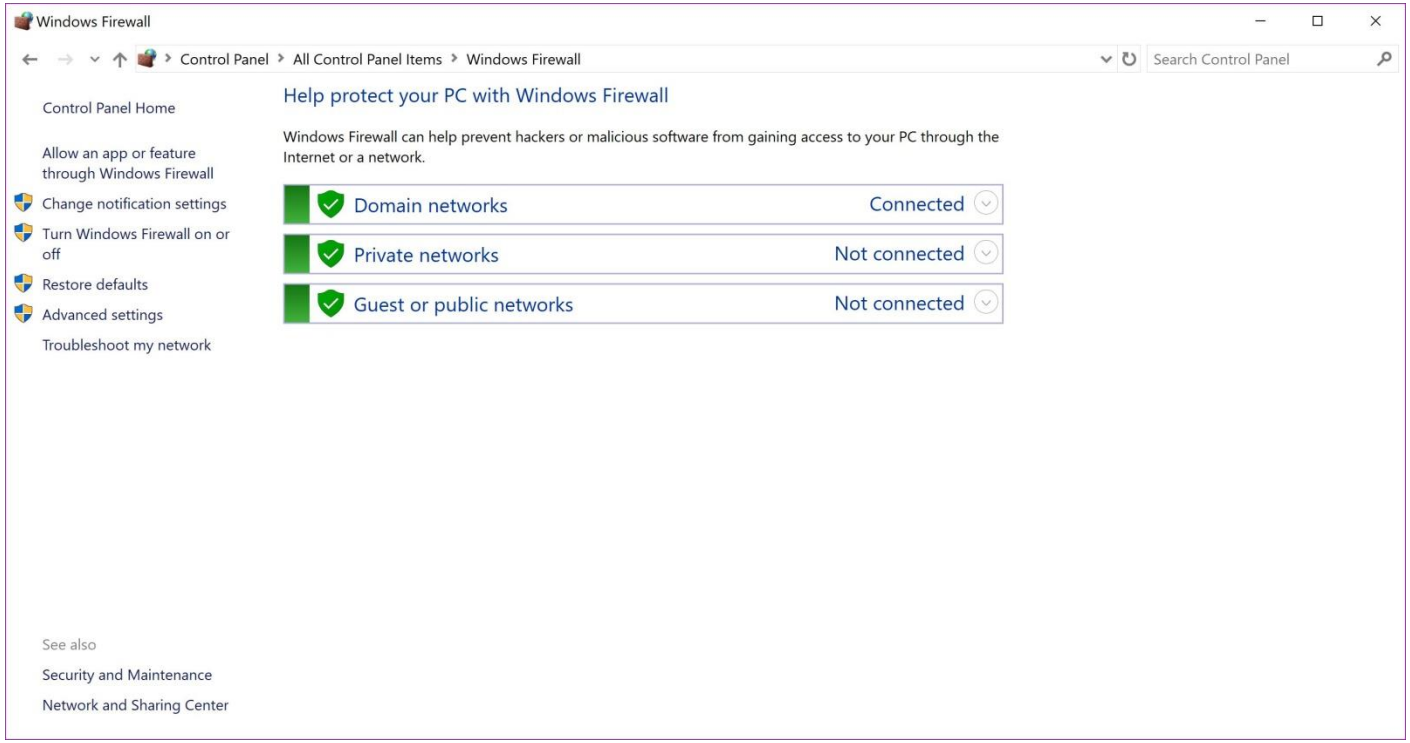
Hands-On Exercises Objectives

- Manage the local firewall configuration.
- Explore Windows Firewall with Advanced Security.
- Recognize the need for outbound filtering.
- Create a port filtering rule.
- Create an ICMP filtering rule.

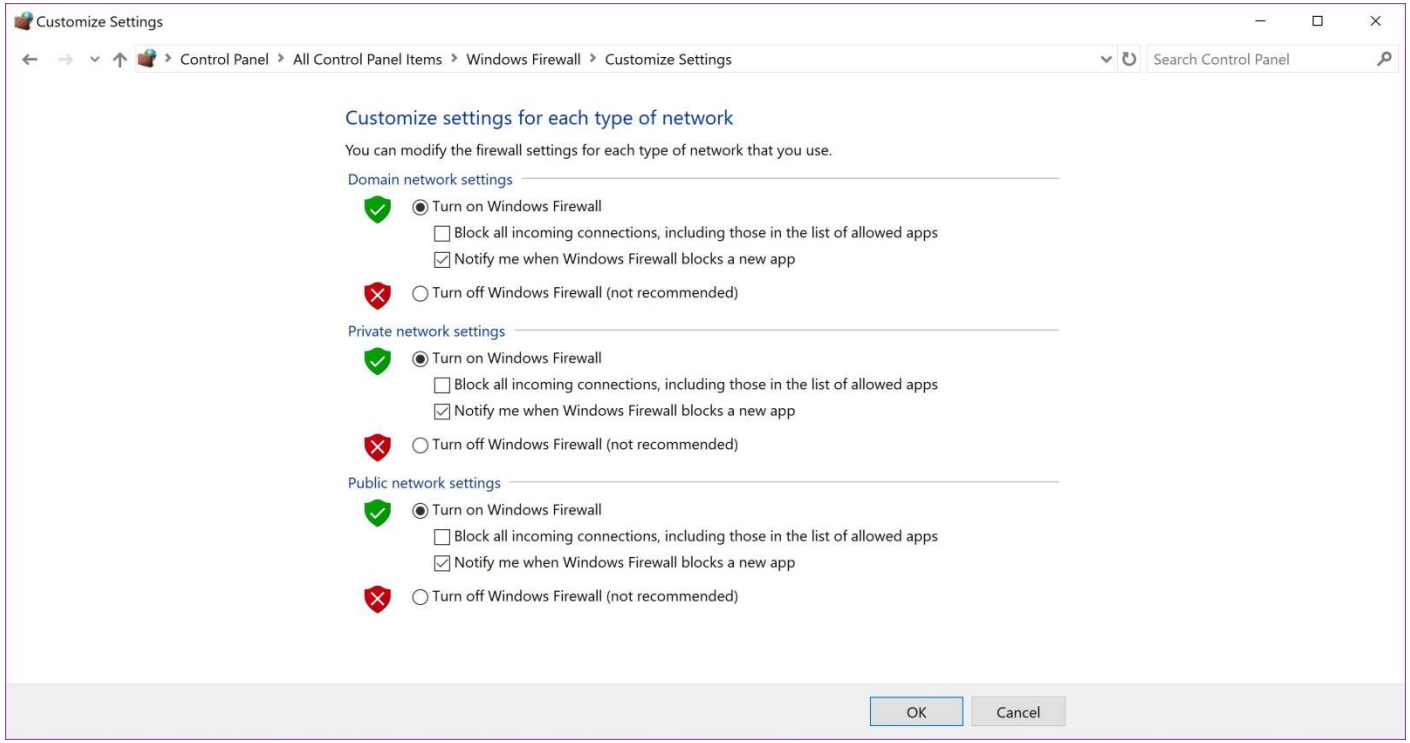
Resources

- PC-compatible desktop/tower computer system
- Windows 10 Professional installed
- User account with Administrative access
- Internet access from a network connection

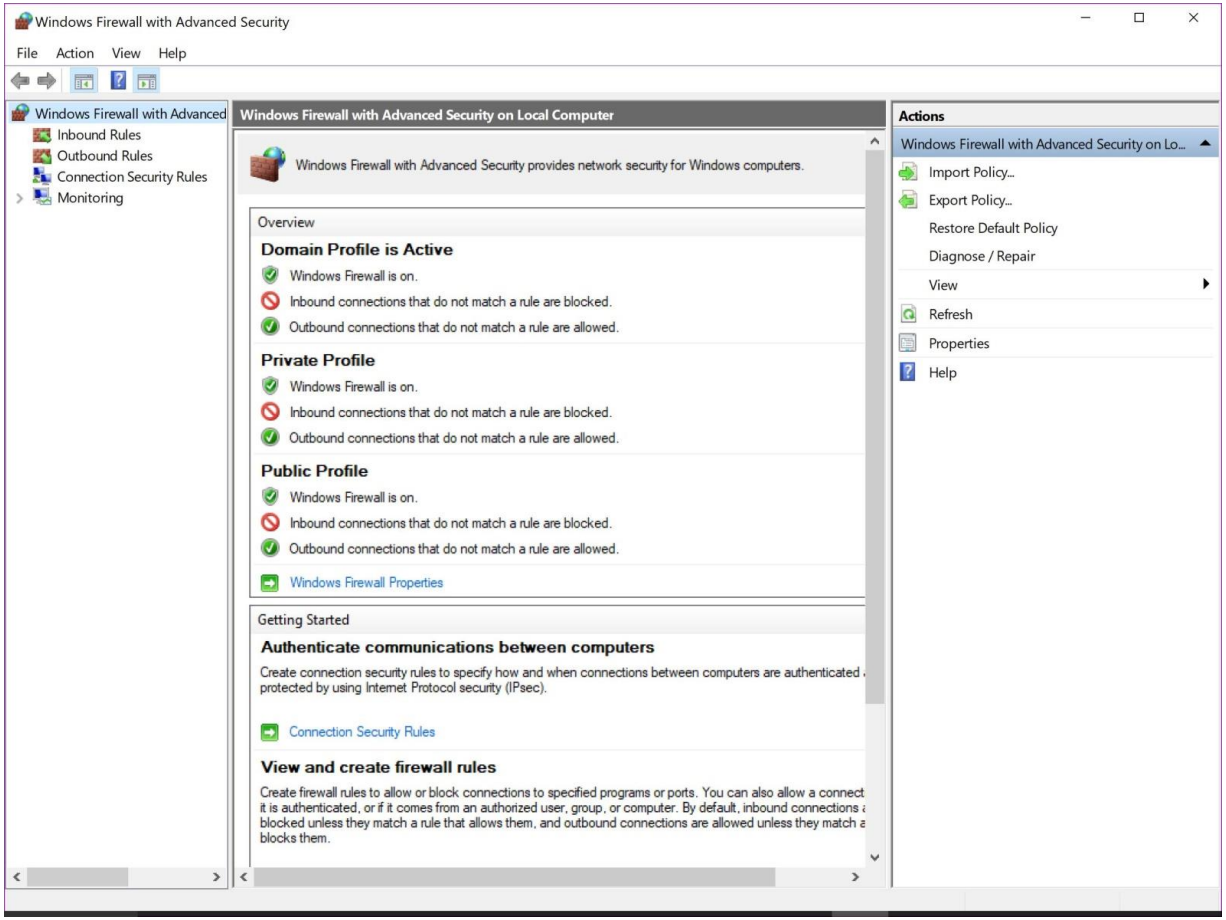
Basic Windows Firewall Settings



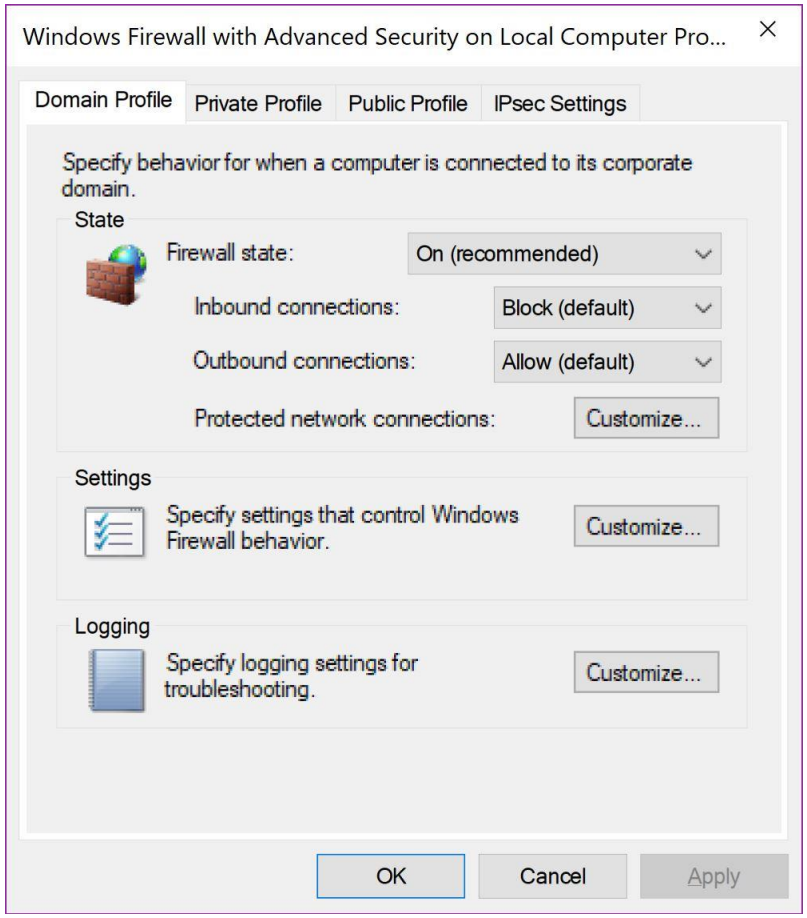
Customize Settings Window for Windows Firewall



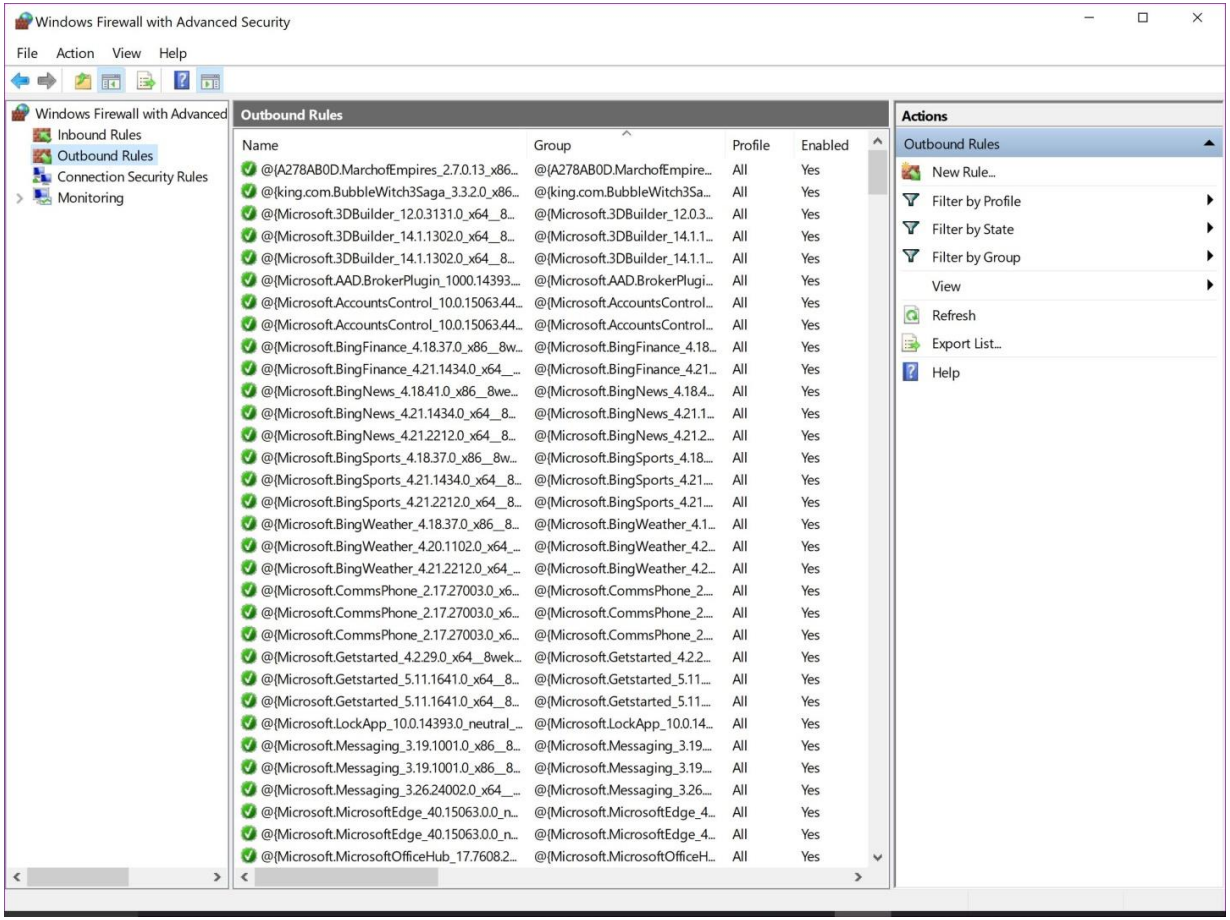
Windows Firewall with Advanced Security Console



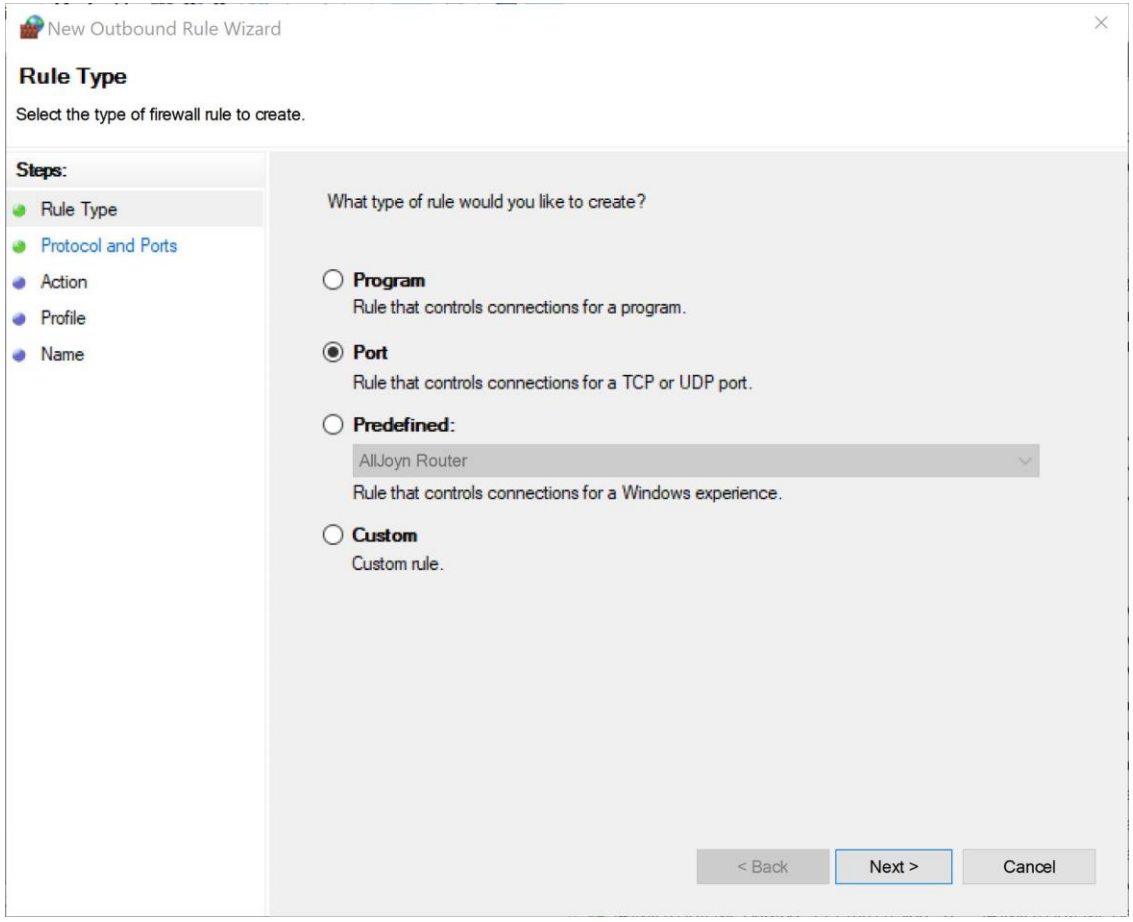
Windows Firewall with Advanced Security on Local Computer Properties



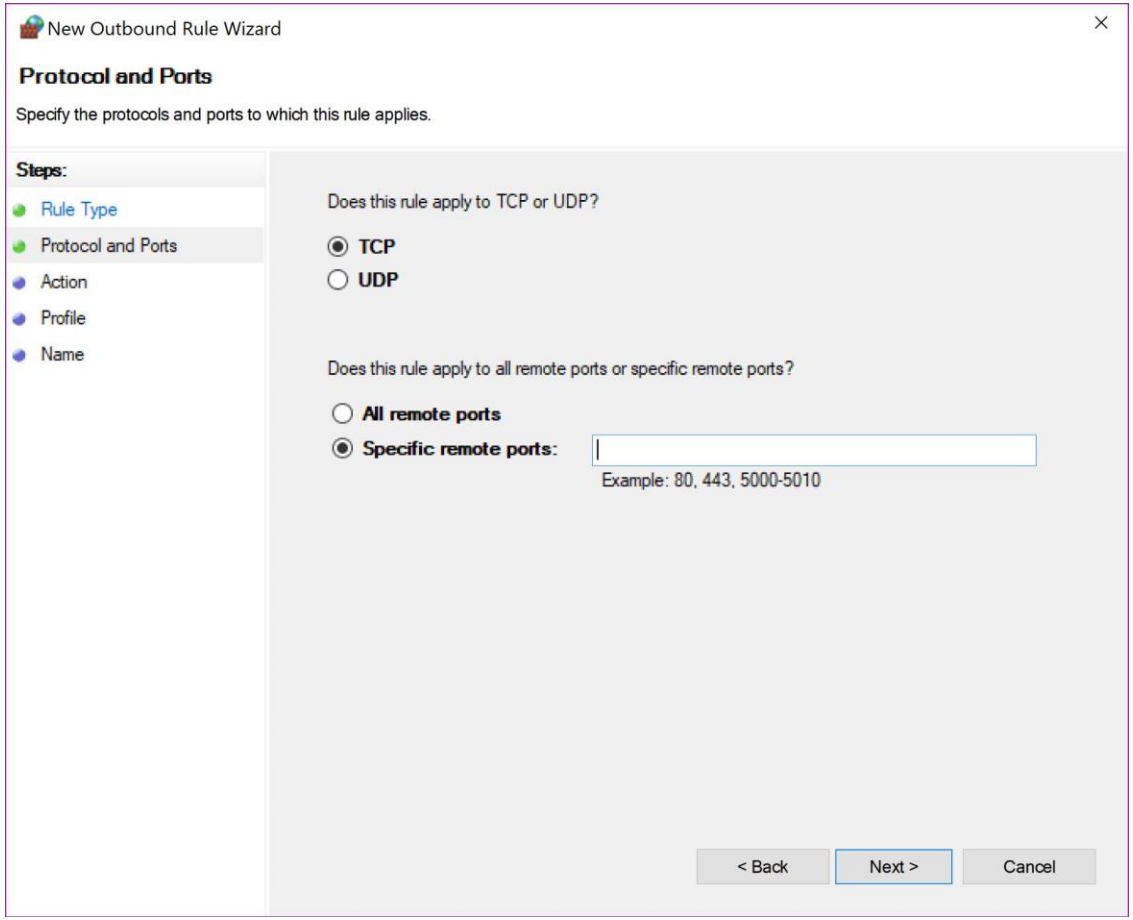
Outbound Rules in Windows Firewall with Advanced Security



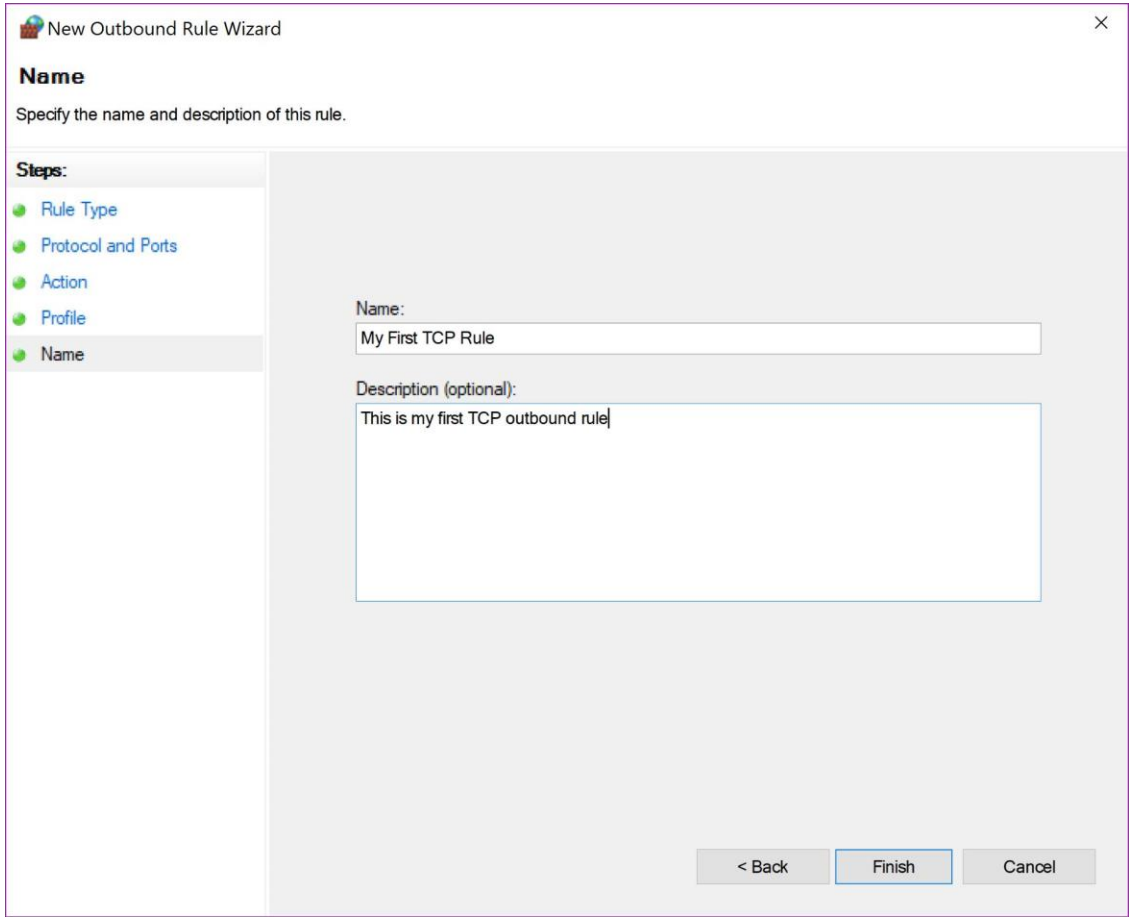
New Outbound Rule Wizard



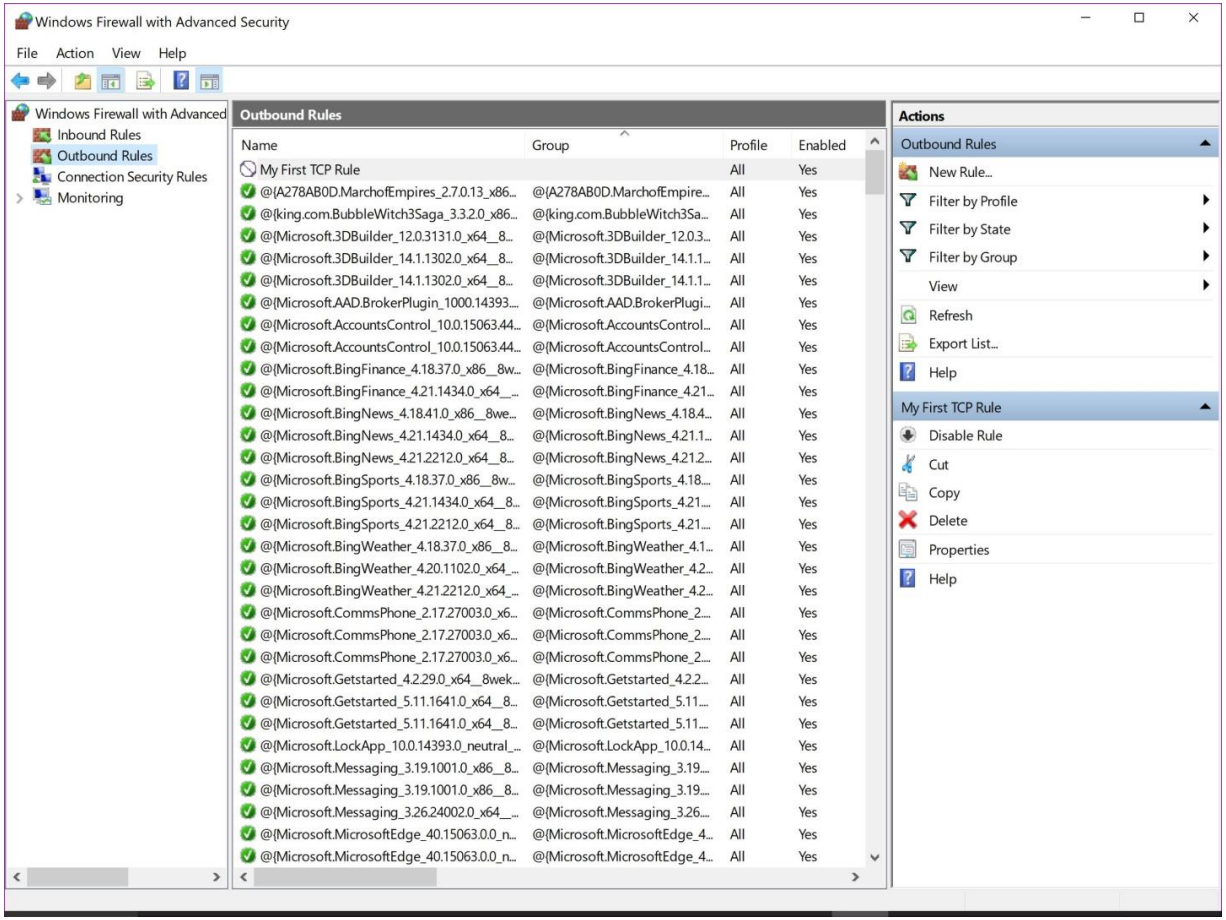
New Outbound Rule Wizard Steps: Protocol and Ports



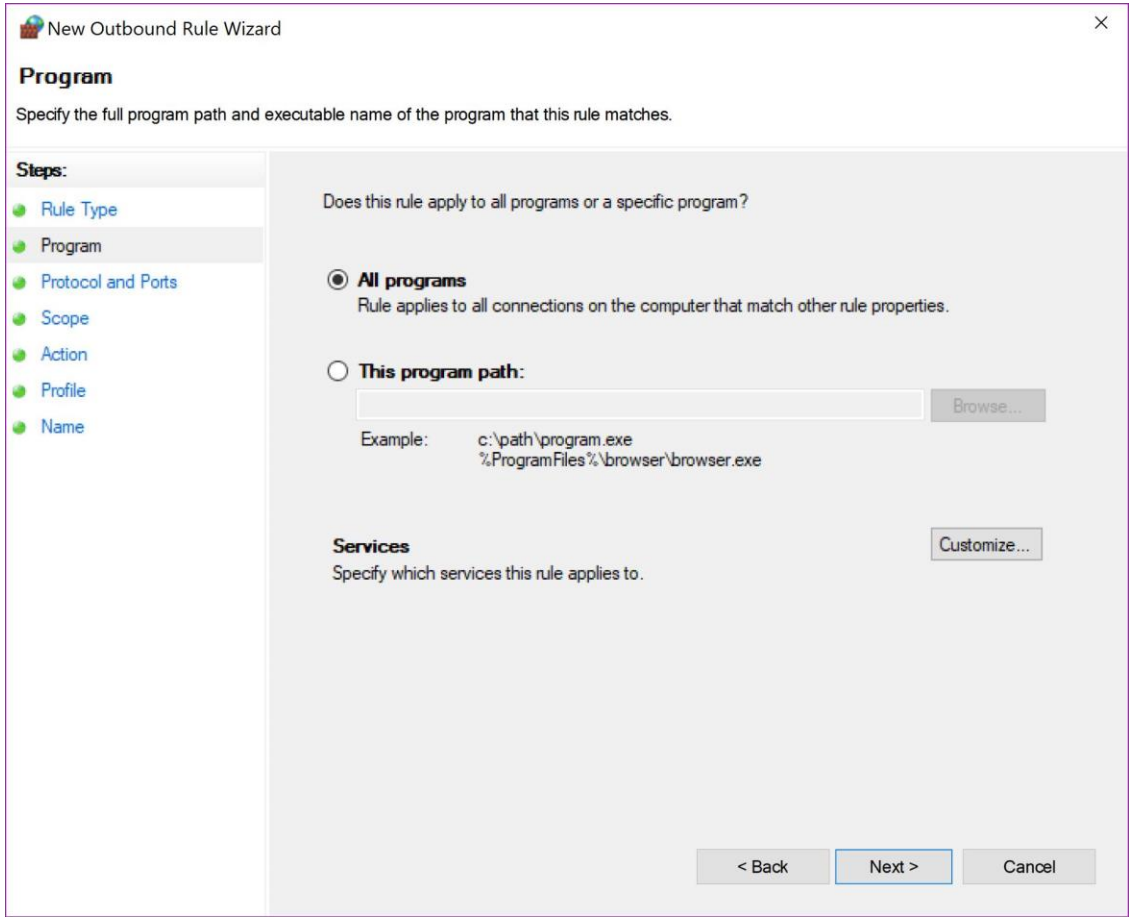
New Outbound Rule Wizard Steps: Name Page



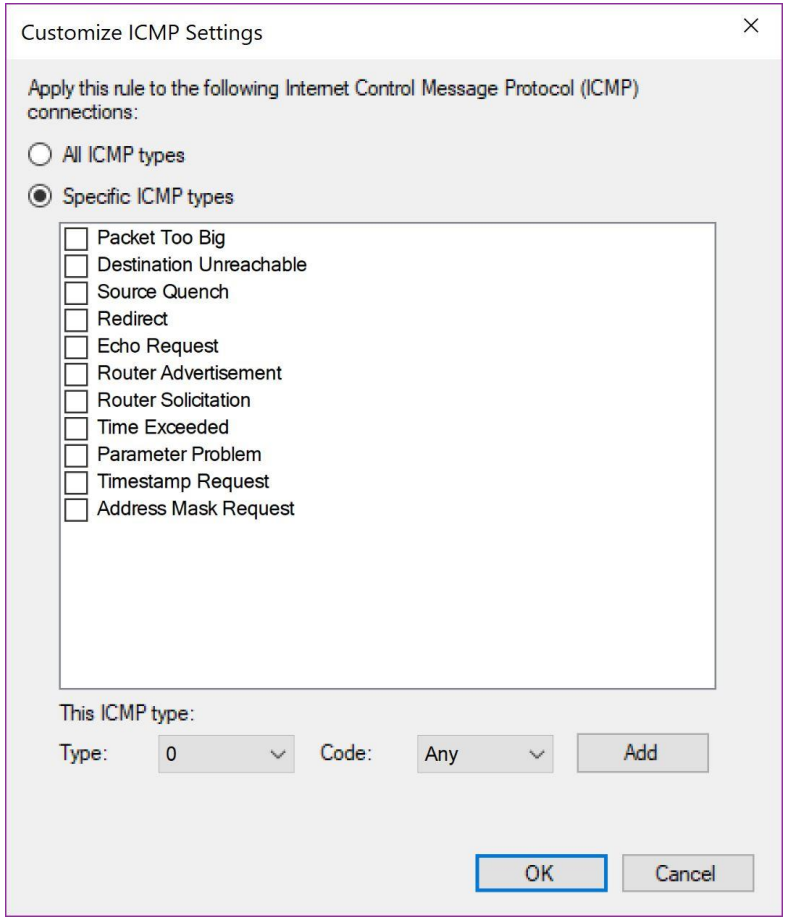
Windows Firewall with Advanced Security New Outbound Rule



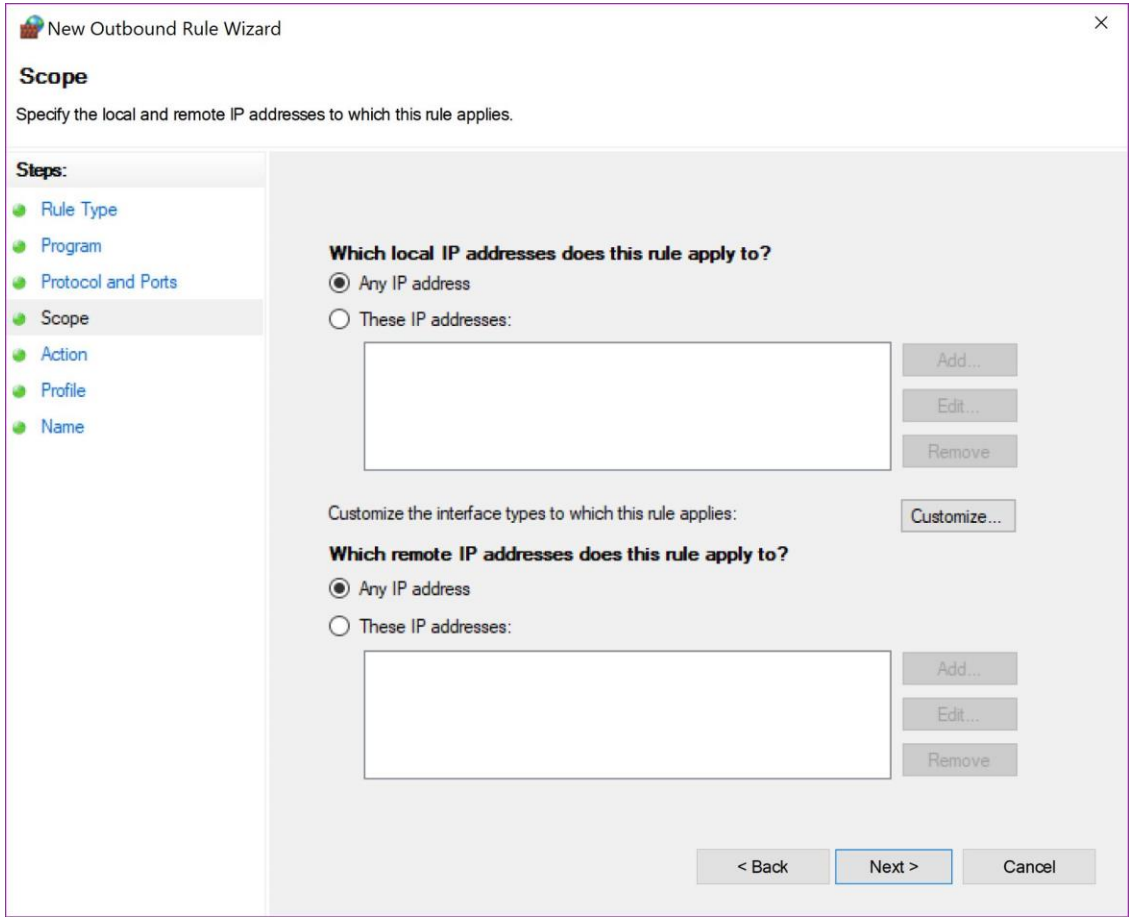
New Outbound Rule Wizard Steps: Program Page



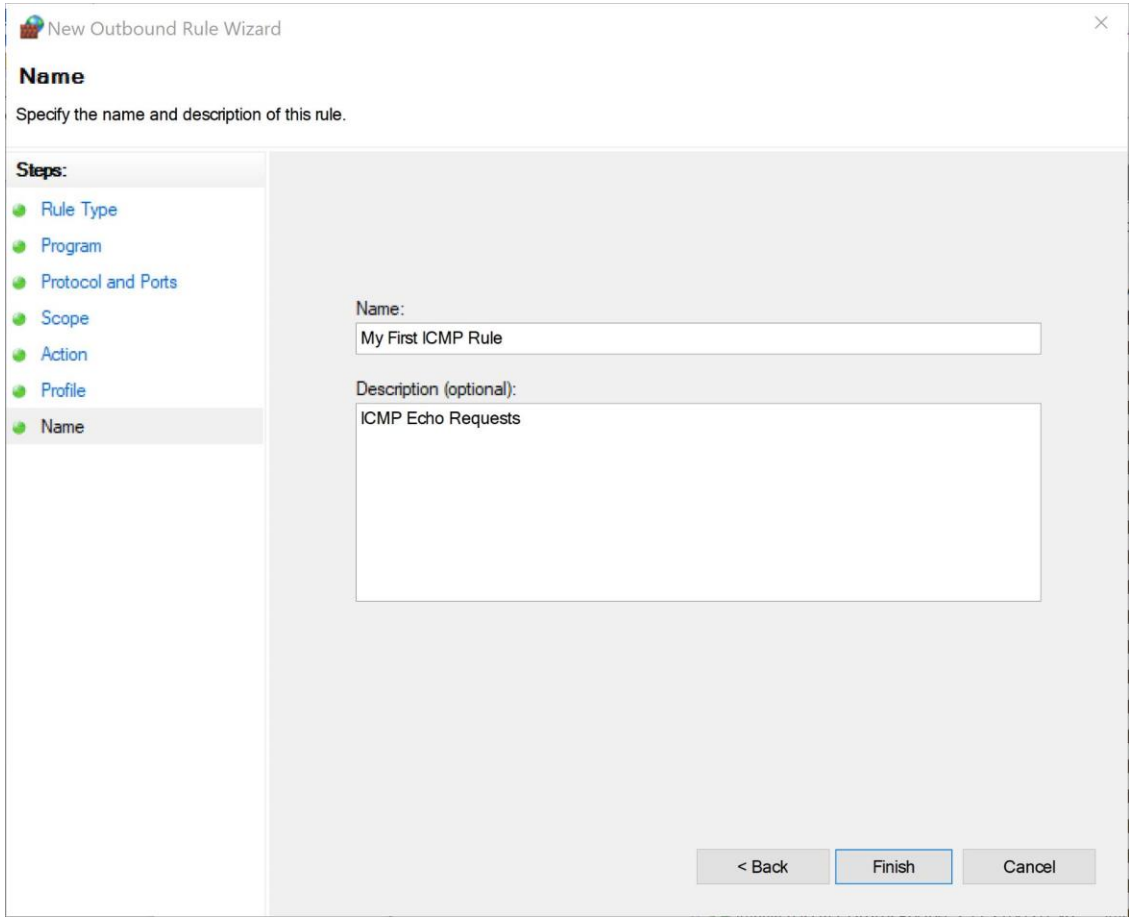
Customize ICMP Settings



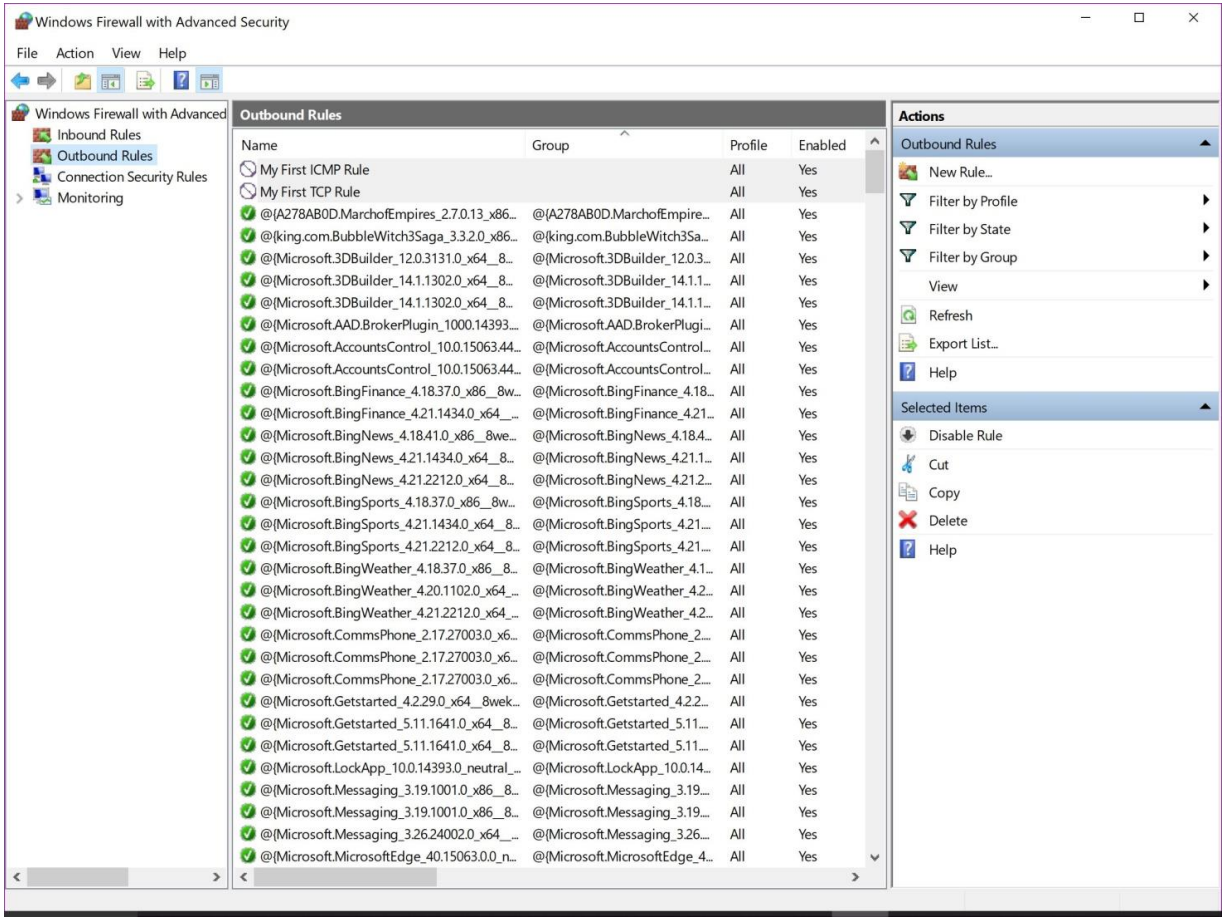
New Outbound Rule Steps: Scope Page



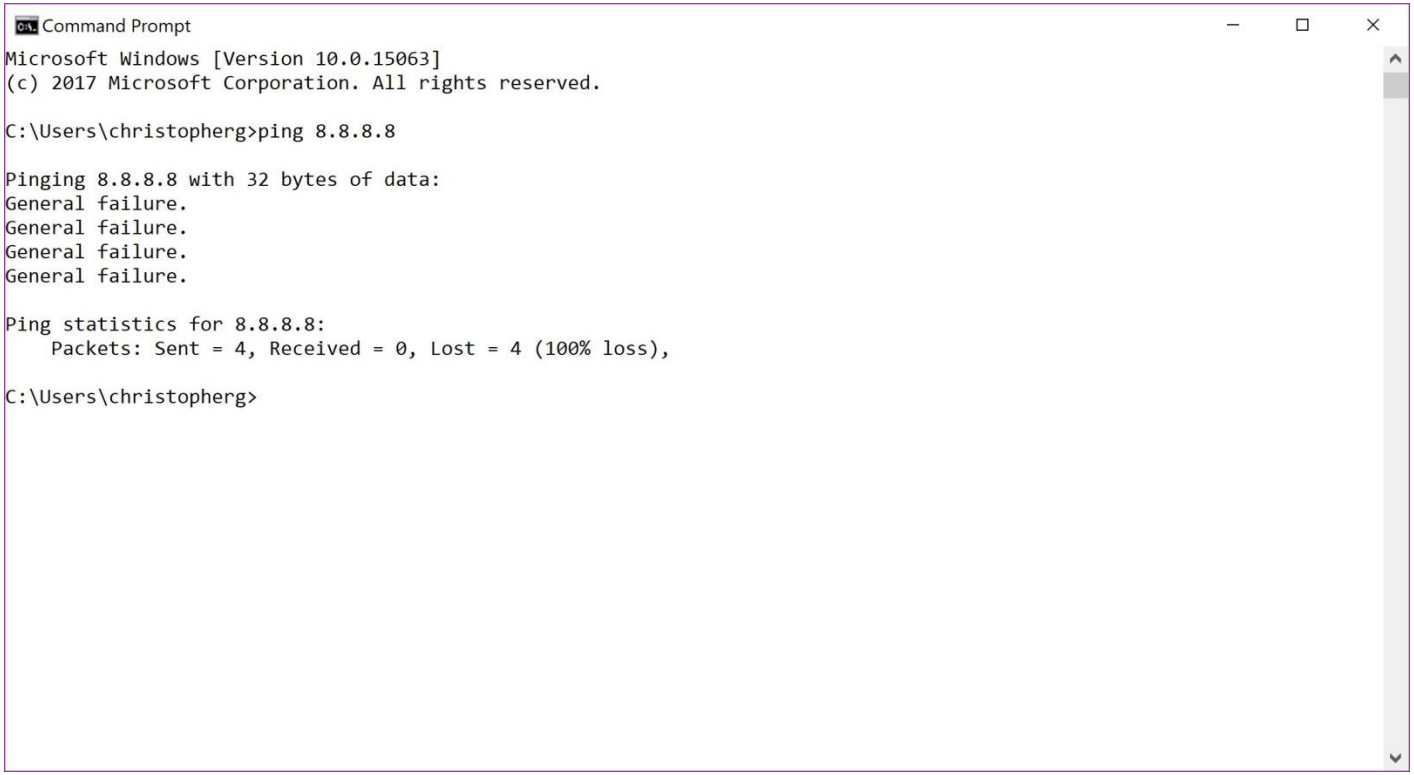
New Outbound Rule Wizard Steps: Name Page



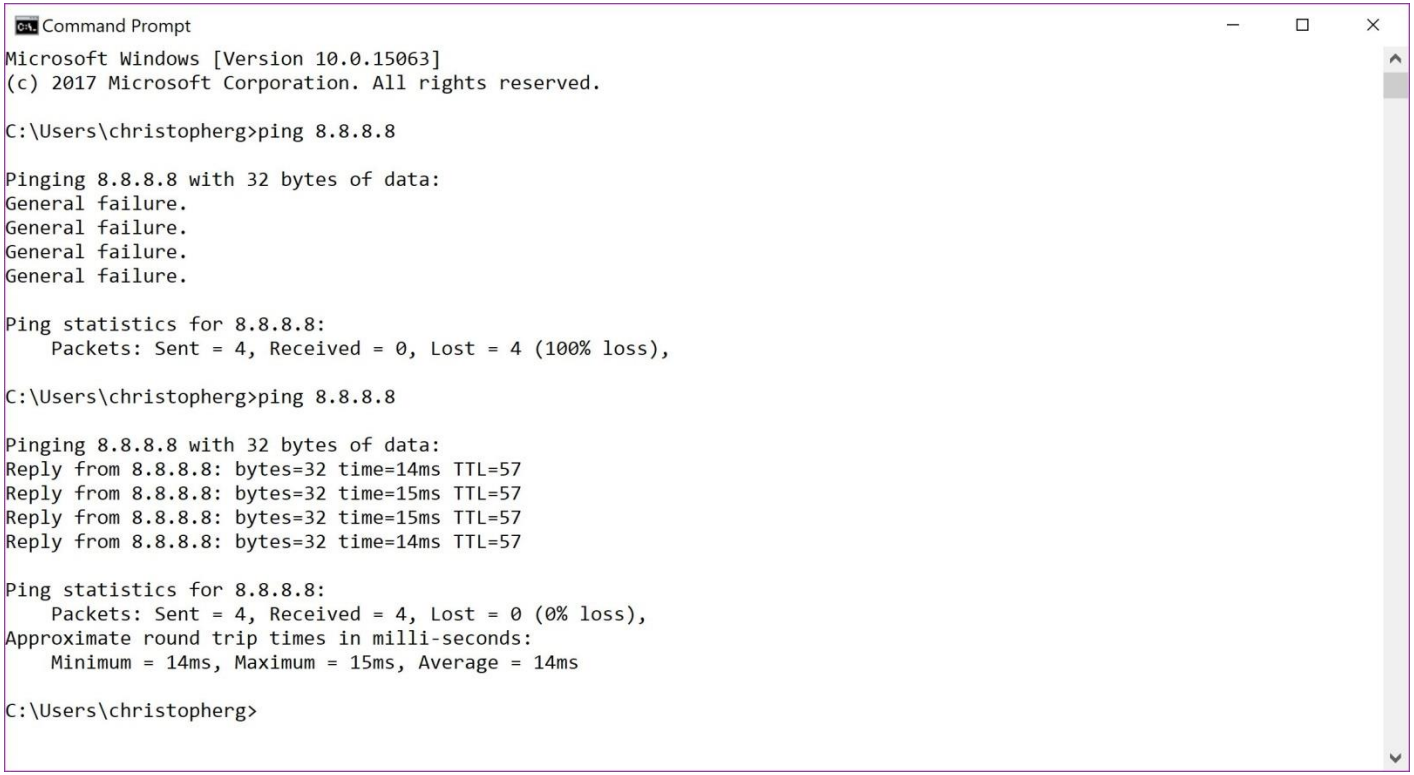
New Outbound Rule in Windows Firewall with Advanced Security



Ping Failure



Ping Success



Types of Networks

Domain Networks	Home or work (private) networks	Public Networks

Recommended Ports to Close

Port Name	TCP or UDP	Port Number(s)	Reason for Closure
MS RPC	Both	135	Windows systems use these ports to send out queries. This can leak information or be construed as an attack by another network.
NetBIOS/IP	Both	137-139	Windows systems use these ports to send out queries. This can leak information or be construed as an attack by another network.
SMB/IP	TCP	445	Windows systems use these ports to send out queries. This can leak information or be construed as an attack by another network.
Trivial File Transfer Protocol	UDP	69	Closing this prevents a hacker from moving their toolkit onto your system.
Syslog	UDP	574	Sends out information about the network topology, which is something to avoid.
Simple Network Management Protocol	UDP	161-162	Sends out information about the network topology, which is something to avoid.
SMTP (all but your mail server)	TCP	25	This prevents your network information from being turned into a Spam relay, which could get your network on one or more blacklists.
Internet Relay Chat	TCP	6660-6669	These are used by hackers to send and receive communications from the systems that they infect.

Recommended ICMP Types and Codes to Close

ICMP Name	Type	Code	Reason for Closure
Echo – Replies	0	0	These are used for covert communications.
Host Unreachables	3	1	Host Unreachables are used by hackers to map out networks and to identify which hosts are online and offline.
Time Extended in Transit	11	0	Closing these prevents some network-mapping tools from functioning.

Lab Question 1

What are the three main types of networks that Windows Firewall handles?

Lab Question 2

It is important to turn Windows Firewall off. True or False?

Lab Question 3

What are the four Rule types that you can create with the New Rule Outbound Wizard?

Lab Question 4

What is an easy way to test ICMP echo requests?

Lab Question 5

You have the option to block all incoming traffic. True or False?