Confidence in the Connected World

Center for Internet Security®

CIS Controls®

Telework and Small Office Network Security Guide

Contents

Contents

Continued

Telework and Small Office Network Security Guide

Acknowledgments

CIS would like to thank the many security experts who volunteer their time and talent to support the CIS Controls and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

Editors
Joshua M. Franklin, CIS

Contributors
Aaron Piper, CIS
Alan B. Watkins, ABW Consulting, LLC
Stephen Campbell, Non-State Threat Intelligence, LLC
Uros Trnjakov, Oxfam GB
Maurice Turner, Center for Democracy & Technology (CDT)
Michael K. Wicks, CIS
Robin Regnier, CIS
Aaron Wilson, CIS
Phil Langlois, CIS

Introduction

Routers, modems, and other network devices act as the on-ramp for private networks to access the internet. Although these network devices are developed and marketed for home usage, they are often purchased by small to medium-sized organizations and used in a professional enterprise setting. Furthermore, the trend of teleworking is gaining momentum, and employers are increasingly relying upon teleworking employees to safely handle enterprise information at their homes. Employers generally have little visibility into how personal network devices are configured or secured, but a poorly configured home device can affect the entire organization.

The network devices used by small organizations and teleworking employees are significantly less sophisticated, and cost much less than the class of network devices utilized by sophisticated enterprise information technology (IT) environments. Yet these less sophisticated devices are still subject to many of the same threats as their larger and better-funded counterparts. These threats include spying on browsing habits and web activities, harming connected devices, and exploiting vulnerabilities within the routers. Fortunately, security settings can be configured within these network devices to significantly bolster their defenses. Doing so will ultimately help individuals ensure the security of the data they are charged with protecting from other people in their living space, from neighbors, and potentially from other remote attackers on the internet.

Purpose

This Guide is meant to assist individuals and organizations in securing commodity routers, modems, and other network devices. Securing these devices is important as there are serious cybersecurity considerations surrounding the usage of network devices:

- If someone can access your network, they may be able to read sensitive company files like tax information, personally identifiable information (PII) about employees, and other proprietary information that should not be shared with someone outside of the business.
- If routers or computer systems in a network are compromised, they may become part of a botnet, which can be used to attack other computer systems and organizations connected to the internet.
- If a company doesn't keep in line with industry norms in terms of cybersecurity, it may be in some way liable for breaches and data loss caused by insecure computer networks and systems.
- If a company has cybersecurity insurance or is contemplating such insurance, most insurers are requiring the company to have adequate and reasonable security measures in place to protect both company and customer confidential information.

There are many network devices created for small office or home office situations, typically referred to as ***SoHo offices.*** But SoHo network devices are not always equal in terms of security features when compared with more expensive "enterprise class" devices. This document does not cover any "enterprise class" device, since, in addition to having a higher price tag, those devices require specialized technical knowledge in order to properly use and maintain. Paid subscriptions might also be required to download and install applicable updates, as well as for any technical support. Instead, this document is scoped to properly configuring the security options of a commodity network device and does not assist with advanced network features.

Although this Guide is directed toward companies and other organizations, it is completely applicable for personal use. Teleworkers and other individuals are encouraged to configure their home network devices in accordance with this guidance. Users are encouraged to deviate where applicable and as needed.

Document Structure

The general structure of this document is as follows:

- Purchasing a network device
- Basic device setup
- Basic network setup
- Encrypting your traffic
- Network management
- Maintaining security

The following helpful information is also provided:

- A list of acronyms and abbreviations
- Links to online resources for small businesses from external, trusted organizations

Purchasing a Network Device

With few exceptions, once a router, modem, or other network device is purchased, it's generally not possible to add additional security features. This means that the right device for an organization needs to be researched, vetted, and reviewed ***before the device is bought and paid for.*** The following guidance describes features that should be contemplated before the purchase.

Types of Modems, Routers, and Access Points

There are many terms for network devices and they are often used interchangeably. The following helps to define common terminology and ensure that organizations and teleworkers understand what they are purchasing. When considering a purchase, don't be afraid to ask questions of an electronics store employee, and always verify that information on the device manufacturer's website.

Modem

A modem communicates with an Internet Service Provider (ISP) network and is the main device needed for a small or home office to access the internet. An ISP is the company you pay to access the internet. The modem is often supplied by the ISP, although it can be cheaper over time to purchase and manage one yourself. At that point, the ISP will need to be provided access in order to configure, troubleshoot, and operate the device. Modems may be also referred to as the ***cable box*** or ***digital subscriber line (DSL) modem.***

Router

A router is a network device that typically manages an internal network, acting as an overall network ***hub.*** In a small or home office setting, routers connect directly to the modem via a physical (often blue) Ethernet cable, and will commonly be located ***behind*** the modem (i.e., closer to the internal network). Another similar device, called a network ***switch,*** may be used to create additional Ethernet connections, but the switch does not have router capabilities. Although older routers may only use physical Ethernet cables, modern routers generally also act as a wireless access point (WAP) for devices to wirelessly connect. Modern routers also act as a firewall and manage internet protocol (IP) addresses via the dynamic host control protocol (DHCP). A majority of this document is about router setup, usage, and maintenance.

Modem and Router Hybrids

Although routers and modems were originally distinct devices, most modern store-bought or ISP-provided modems already have a router built into them. These devices may be confusingly referred to as a "modem" or a "router," and research is necessary to identify if a device is a hybrid. They can also be known as a "gateway."

Extender

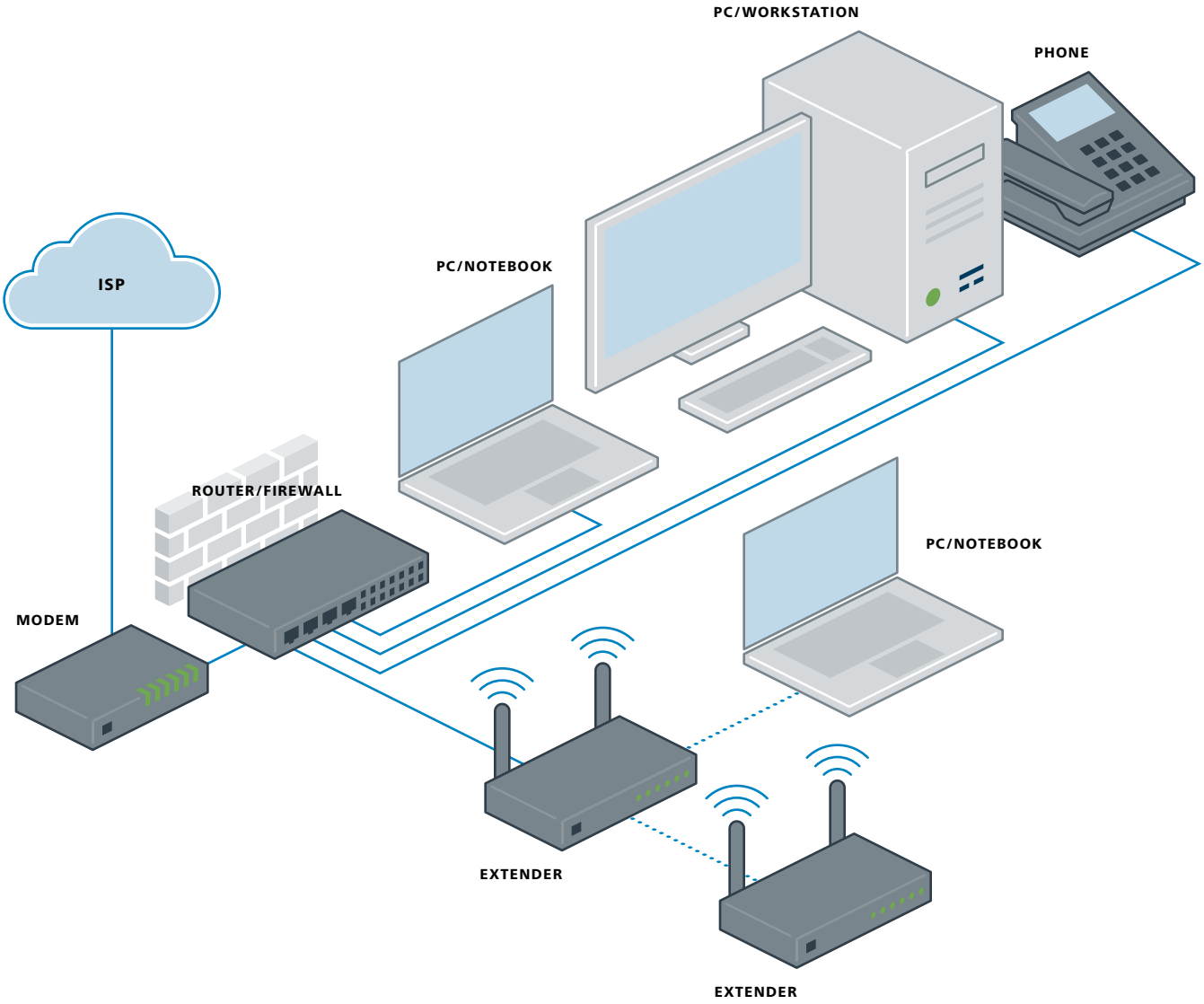
Extenders are WAPs in ***bridge mode,*** meaning they act as a way to send a WiFi network further into a home or office. Extenders are used in areas where there is weak, or no, wireless signal to provide more coverage area. This method of extending a WiFi network offers a variety of advantages for both users and the device owner, such as creating a separate wireless network or running an Ethernet cable back to the modem. One of the main advantages is not needing to have two separate WAPs with slightly different network names, or to configure multiple wireless networks for each device or computer needing a connection. A wireless device will be able to automatically connect to the extender when the signal is strong enough. Extenders may be provided by the ISP, or purchased separately at an electronics store or off the internet. They are sometimes referred to as ***WiFi extenders or range extenders.***

Cellular Signal Boosters

Cellular signal boosters operate in a similar manner to WiFi extenders since they make it easier to access the cellular network. These devices are needed when cellular coverage is not received inside a person's or organization's home or office. This may be because a cellular tower is not close enough or because a room may be constructed with materials that prevent cellular signals from penetrating the walls. Cellular signal boosters often connect directly to the modem. These devices are also referred to as cellular extenders, femtocells, and cellular gateways.

Common Usage

The following graphic shows how these devices are typically set up. The way a device is placed in the network architecture can have an impact on security.



Desired Security Features

The home office router market is quite competitive and new features are often added to help devices stand out from the crowd. The following are examples of security-relevant features that may come with a new home network device. While not all of these are critical to home network security, these items are well worth considering when making a purchase decision.

- **Frequency of software updates:** This feature ensures that security updates are regularly provided by the device manufacturer to fix problems.
- **Auto-update:** This feature ensures that security updates provided by the manufacturer are installed to the device.
- **WPA3:** Wireless Protected Access Version 3 (WPA3) is the latest version of the WiFi standard and contains new authentication and encryption protocols that can help prevent attackers from spying on traffic or successfully attacking a router.
- **Guest network:** Guest networks can act as a dividing line between trusted devices and untrusted devices. They also provide a way to offer network access to individuals without providing the WiFi network password to that user, such as through temporary passwords.
- **Built-in firewall:** A firewall helps to block traffic from reaching any devices on the internal network.
- **Built-in virtual private network (VPN):** A VPN encrypts the traffic from a network device to the VPN provider, which prevents an ISP from viewing the traffic. Note that the VPN provider would be able to view traffic.
- **Allow VPN Access:** This feature can allow or block third-party VPNs from working on a network. Although not critical to the security of the device and network, it is useful in some situations.
- **Parental controls:** While these can be used to ensure that children are unable to access adult or other inappropriate content, they can also be used to ensure that employees don't access unauthorized content. Adult or illegal content sites often contain malware and/or dangerous content that can infect a computer.
- **Two-factor authentication (2FA):** 2FA can be enabled on some network devices to ensure that the person accessing the device is supposed to have access.

Where to Buy Network Equipment

There are many places to purchase network devices, such as a local electronics store, online, or from an ISP. The primary factor is to obtain a device from a *reputable source*. Purchasing a used device is riskier, as someone else may already know the passwords and may have had long-term access to the device. A used device may also be more likely to break and, lacking any vendor support, the office could be left without any way to obtain internet access.

Basic Device Setup

After removing a new device from the packaging, consider registering it with the manufacturer. This will help to ensure the device warranty is properly set up in case there's an issue with the device in the future. It may also be prudent to store any physical media [e.g., digital versatile disc (DVDs), compact disc (CDs), universal serial bus(USB) drives) or credentials that ship with the device, such as device firmware or passwords, in a safe place. They can be useful to reset the router to factory settings, or to help hand off access to a new person in charge of IT in the organization.

If the ISP is installing the device and setting up the service, it will probably reasonably configure the modem and/or router. However, you need to find out how to add, change, or disable administrative accounts and how to change passwords. Otherwise, after plugging the device in a power source, it will likely boot up and activate a wireless network once the ISP connection is active. Otherwise, be sure to investigate and turn off (disable) or immediately proceed to configure all WiFi networks turned on by the manufacturer by default. Finally, there may be some device manufacturers that require the user to sign up for an account in order to use the router.

Initial Access

The device's user manual will specify a method of accessing the *administrative portal*. This is where a router's configuration settings can be modified. The most common methods of accessing the portal are via an application or a webpage. Using an application to control the router limits the computer systems that can access the router, which can be useful. The more common method is to open a browser and access the administrative portal via a specific web address such as 192.168.1.1 or 192.168.0.1. Although it's not imperative to do so, it is more secure to perform administrative activities via a wired connection like Ethernet in lieu of WiFi. More secure web portals will use HTTPS in the browser instead of HTTP. This is the difference between https://cisecurity.org and the less secure http://cisecurity.org.

Internal and External Network Interfaces

Routers and modems are equipped with multiple network cards. A router needs a network card, or *interface*, for each connected network, and routers have an external and internal network. This is because they act as the gateway between your ISP's network (the external interface) and your home network (the internal interface). Some devices have separate passwords for both of these interfaces, but not all will. The ISP will always need to access the external interface. Be aware of the types of access provided by a router, and attempt to control access to the extent possible. Using a firewall in combination with a router (often on the same network device) can help control external devices from accessing the internal network.

Passwords

Passwords are the main credential used to access the network device through a process known as *authentication*. All passwords should be reasonably strong, meaning they are eight characters or greater in length. The administrative password used to configure the network device should be changed from the factory setting to something unique, and not shared with any unnecessary individuals or other service, platform, or application. This is especially important if the network password is used for an organization, but not as imperative if it's solely for home use.

Note that the router administration password is the password for the internal network interface, and is completely separate from the WiFi network password. Different types of passwords used for network devices include:

- **WiFi network password:** Used to access the wireless network. This password will likely be shared with other individuals.
- **Internal router administrative password:** Used to access the internal router configuration dashboard, or the application used to access the mobile application.
- **ISP password:** Used to log into the ISP's online portal and manage your account.
- **Management application password:** Some routers offer a mobile application to control the router and this can be password-protected.

WARNING: Many routers will come preconfigured with a password. The default passwords for most router models are easily available online within a few web searches, making it ***extremely important*** to change the administrative passwords and not use the defaults.

Device and Network Management Apps

Some router manufacturers also provide network management applications for administrative functions. Most commonly, this is a mobile phone application (app). These apps will allow a password to be used to access the router. In certain situations, 2FA will be a possible option, which is significantly more secure. If a mobile device is used to configure a router or perform maintenance activities, the device should have the latest software updates (with auto-update preferred) and be properly configured (such as using a device lockscreen).

Basic Network Setup

Once a new network device is plugged into a power source, the device will likely boot and begin broadcasting two WiFi networks automatically. These two WiFi networks will often be labeled with the same network name, or Service Set Identifier (SSID), except they may have the frequency they are operating at attached to the end of the name. For example, 5 Gigahertz (GHz) network names often look like ***SampleNetworkName-5Ghz.*** This is because WiFi operates at two separate frequencies, 2.4 GHz and 5 GHz, and a separate network can be broadcast on each frequency. An example of both networks having similar yet distinct names are ***SampleNetworkName_2*** and ***SampleNetworkName_5.*** Once the login credentials are obtained, both of these networks can be modified and managed as needed.

Device Location

Where a network device is physically located makes a large difference in terms of security. Network devices should be kept in an area away from the public or any house guests. Physical access to the router often means that someone can obtain a high degree of access to the network without a wireless network password. This can be performed by simply plugging an Ethernet cable into the router and then into a computer to access the administrative portal. Finally, not all internal network interfaces are always able to have their passwords changed. In these instances, proper physical security of the router is critical.

Naming a WiFi Network

Naming a network can be a fun activity, but it can also help single out an individual or organization in their neighborhood or office space. This is less of an issue for organizations with stand-alone buildings and more of a problem for teleworking individuals working in dense urban areas. In any case, you should change the WiFi network name from the default to something else because the default name usually identifies the type of network device. Put forethought into whether or not a network name should uniquely identify any specific individual's name, organization's name, street address, or apartment number (e.g., Apartment516WiFi).

Another consideration in naming a WiFi network is refraining from broadcasting the WiFi network name. This is also known as ***SSID cloaking.*** Over a decade ago, hiding the network name was considered a best practice, but popular opinion on this matter has changed since then. SSID cloaking does not prevent attackers from actually noticing that a network is there, as basic wireless hacking equipment can detect these networks. Yet SSID cloaking often poses a problem for ***authorized*** individuals trying to connect to the network. This is for both their primary computers and any ancillary mobile or Internet of Things (IoT) devices. In summation, the security benefit of SSID cloaking is questionable at best, and the usability benefit of broadcasting a network is tangible. Therefore, SSID cloaking is not recommended but reasonable people disagree on this topic.

Creating a Guest Network

Guest networks are useful because they separate devices with sensitive data on them from devices that may not be trustworthy. Guests will often still need a WiFi network connection. This can be accommodated in one of two ways: two separate routers or a router's guest network feature. Remember it's critical to share the WiFi network password with as few trusted people as possible. Using two separate routers, each with its own password and independent connection to the modem (this is a key point), allows for easy separation of trustworthy and untrustworthy devices. The downside of this setup is cost and management. Some routers have a guest network function built right in that can be. This helps provide some separation between devices and doesn't require sharing the network WiFi password. Some guest network features also allow for temporary passwords and schedule restrictions, such as only being available during business hours.

Enable Automatic Updates

Software updates are extremely important in keeping any network device safe. New security flaws and vulnerabilities are constantly discovered, and the main way to defend against these issues is to install updates from the device manufacturer. Unfortunately, some manufacturers will not provide security updates, as it takes time, expertise, and other resources to write software updates and deploy them to network devices. Therefore, it's important to purchase a router from a manufacturer that has a track record of providing software updates. Once a router is in use, it's also important to make sure that these updates are automatically applied. Although it's completely acceptable to manually approve and install updates, for most small office or teleworking needs, ensuring auto-update is enabled will prevent a person from forgetting to perform this critical security task.

Encrypting Your Traffic

Cryptography is the art and science of secure communication methods, such as transforming data in order to hide information from unauthorized access and modification. There are many types of cryptography, some stronger than others, and some devices are still supporting old and ineffective types of cryptography to ensure capability with older devices. Ensuring that the right type of cryptography is in use in a small office or home network can thwart others from viewing sensitive information without authorization. The following are protocols and concepts related to cryptography, and more specifically to encryption and authentication, that should be taken into consideration.

Wired Equivalent Privacy (WEP)

WEP, or Wired Equivalent Privacy, was the first method of encryption built into commodity wireless access points for WiFi. Initially introduced in the late 1990s, it is now considered insecure and ***should never be used under any circumstances.*** It is primarily kept in home network devices for backward compatibility reasons. The cryptography is easily breakable using software that is free and widely available on the internet.

WiFi Protected Access (WPA)

Once WEP was broken, WiFi Protected Access (WPA) was introduced as a temporary fix to help protect WiFi communication. WPA may also be listed as ***WPA-Personal*** or ***WPA-PSK (Pre-Shared Key)*** within a network device. Although WPA is not broken, attacks exist that harm the security of a network using WPA. This is especially true if a short password is used. Breaking WPA is not overly difficult, but it often requires specialized knowledge and equipment, making it much stronger than WEP. It is not recommended to use basic WPA encryption and instead, refer to WPA2 and WPA3 below.

WiFi Protected Access Version 2 (WPA2)

WPA2 is the de facto standard for networks across the globe. The cryptography within has stood strong for many years. WPA2 uses the Advanced Encryption Standard (AES), a form of cryptography employed by the U.S. government. There are multiple types of WPA2, some meant for enterprise use that are more difficult to set up. One of the main differences between WPA2-Personal and WPA2-Enterprise is the password distribution method. WPA2-Personal is sufficient for small and home office needs.

WiFi Protected Access Version 3 (WPA3)

WPA3 is the newest form of wireless security for WiFi and is currently being deployed in new devices across the world. In a nutshell, some of the main security benefits of WPA3 include longer key sizes (most likely desired by larger organizations) and forward secrecy. Among other things, forward secrecy prevents those who obtain the WiFi password in the future from reading a person's past internet activity. Most network devices will not be able to download a software patch or software update to use WPA3. Instead, a new WPA3-enabled device will need to be purchased.

WiFi Protected Setup (WPS)

WPS is a button that can be pushed on some routers to help make connecting to the router easier. WPS was designed as a way to make it easier for users to connect to a WiFi network, offering four distinct connection methods. Unfortunately, multiple major security flaws were discovered in WPS. Some of these flaws were fairly easy to exploit, and can allow attackers to connect to the WiFi network without authorization. WPS is still included in major name-brand devices. ***WPS should be disabled if possible.*** The inclusion of WPS on a router means that if someone has physical access to a router, they can connect without the network password and read network traffic.

Additional Network Configuration

Routers and other network equipment can be further configured in a number of ways. The exact configuration options and how they function will vary with different manufacturers, but the following options will be present within most commodity network devices.

Firewalls

Firewalls help prevent malicious network traffic and other information that attempts to enter a network from reaching certain devices. Firewalls generally come built-in to most home routers, but the utility and effectiveness from one device to the next can be difficult to understand. A router with a firewall built-in may be more expensive, and organizations should decide for themselves if a firewall is worth this resource expenditure. As a general rule, organizations with larger, more complex networks, or with internet facing services (e.g., FTP, SSH), should consider obtaining a model with a firewall. Most of the firewall functionality within routers can be set to multiple levels such as "low security," "medium security," and "high security." This Guide recommends utilizing the most stringent settings available during initial configuration. If these settings do not permit users to access the appropriate web resources, lower the security settings until they meet the needs of the small or home office.

Most routers also provide a benefit known as Network Address Translation (NAT). NAT works to hide devices and networks located behind a router and can make it significantly more difficult to attack. The usage of NAT is sometimes referred to as ***IP masking,*** or a ***NAT firewall.*** Regardless, NAT should always be enabled.

Device Hardening

A large part of device hardening consists of removing ports and services that are active on a device. Services can be thought of as "programs" on a router that are meant to communicate with external computer systems. Ports can be conceptualized as doors to the outside world, and they are identified via a number and sometimes a protocol (e.g., UDP 53, TCP 80). Generally, each service uses a dedicated port to communicate. Removing running services and closing ports can go a long way to securing a home network device.

Domain Name System (DNS)

DNS is a method of associating IP addresses to website names, also known as *domain names.* Essentially, whenever a computer in the internal network requests a webpage, a DNS server is used to look up where to find the page on the internet. Home network devices will generally use a pre-configured DNS server, and in most cases the ISP's DNS server is used. Alternative DNS options exist, and certain nonprofits and other organizations offer DNS servers that can help to prevent computer systems from reaching out to known dangerous websites. Using DNS filtering, if your network requests access to a dangerous website, the request will not be completed. Other DNS servers may also not track you in the same way as an ISP's DNS would.

Two common DNS servers that offer security benefits are Quad 9 (**https://www.quad9.net**) and OpenDNS (**https://www.opendns.com**). Organizations can choose to configure Quad9 or OpenDNS for each computer workstation, tablet, and mobile device individually, or configure the router to protect the entire network. Devices that are used outside of the workplace should be configured individually. Regardless of the device in question, there will be a location within the administration area of most devices to configure the DNS settings. Quad 9's IP address is 9.9.9.9 and the OpenDNS IP address is 208.67.222.222. Either will work to protect your network. Simply use one of those IP addresses for the DNS server and this item will be resolved.

The *CIS Controls Microsoft Windows 10 Cyber Hygiene Guide* provides additional information for correctly configuring DNS filtering on Microsoft Windows 10 workstations. It is listed under Sub-Control 7.7 on page 23, located at: **https://www.cisecurity.org/white-papers/cis-controls-microsoft-windows-10-cyber-hygiene-guide/**.

Remote Configuration

ISPs will often ***need*** to do remote maintenance for modems connected to their network. They may need to update passwords, digital certificates, and other credentials. Data and other configuration information to access the ISP's network will also need to be verified and configured on a regular basis. If you are concerned about the ISP having access to your network's modem, it's always possible to place a router that you have complete control of immediately behind the ISP's modem. Then connect all devices to that router and only use the modem to connect to the internet.

Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP) is a network protocol suite that allows devices on a network to easily communicate. It is often used to share data between devices, such as computers, printers, and even gaming devices, with zero configuration necessary. Over the years, numerous security issues have been found within the UPnP protocol suite. The number and severity of these critical security flaws mean that ***UPnP should always be disabled,*** even if certain devices cease to function properly (e.g., gaming devices). In fact, UPnP intentionally creates holes in firewalls in order to allow devices to connect. If UPnP is absolutely necessary to an organization's operation, attempt to only utilize the most up-to-date version of UPnP, which can be difficult to verify before purchasing the device. In most cases you should be able to find manual configuration settings for most devices, to replace what UPnP does.

Media Access Control (MAC) Address Whitelisting

MAC address whitelisting can be used to restrict devices from accessing a WiFi or wired network. MAC addresses are like serial numbers for any device that has a wired or wireless connection. Whitelisting MAC addresses requires the MAC address of each device to be listed within the router's management dashboard. Unfortunately, MAC addresses can be easily spoofed, leading to a false sense of security, which can be compounded by the difficulty of managing the router. The way WiFi is designed, attackers with very basic equipment can track the MAC addresses of all devices connected to a network—even if the network is encrypted. With a few short commands, a valid MAC address can be cloned and reused by someone wishing to access a WiFi network without authorization. Because of the ease of defeating, and the large amount of upkeep needed to maintain MAC address whitelisting, this Guide does not recommend its usage.

Small Business Guidance

Many individuals and organizations have guidance for both small businesses and teleworkers. The following is a collection of related guidance that can be useful.

- *5 Steps to Better Business Cybersecurity,* Better Business Bureau.
  https://www.bbb.org/council/for-businesses/cybersecurity
- *10 Cybersecurity Mistakes Your Small Business Cannot Afford to Make,* webinar on YouTube by the Federal Trade Commission (FTC) and Small Business Administration (SBA).
  https://www.youtube.com/watch?v=KLrnI5ZEl9Y
- *CyberSecure My Business, Stay Safe Online* (website by NCSA, the National Cyber Security Alliance).
  https://staysafeonline.org/resources/?filter=.topic-cybersecure-my-business.resource-item
- *Guide to Enterprise Telework and Remote Access Security,* National Institute of Standards and Technology (NIST).
  https://csrc.nist.gov/publications/detail/sp/800-46/rev-1/archive/2009-06-16
- *Secure Router Configuration – The Short List,* Router Security (website by Michael Horowitz).
  https://routersecurity.org/#StartHere
- *Small Business Information Security: The Fundamentals,* National Institute of Standards and Technology (NIST).
  https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
- *Start with Security: A Guide for Business,* Federal Trade Commission (FTC).
  https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

Acronyms and Abbreviations

2FA	Two-Factor Authentication
AES	Advanced Encryption Standard
CD	Compact Disc
CIS	Center for Internet Security
DHCP	Digital Host Control Protocol
DNS	Domain Name System
DSL	Digital Subscriber Line
DVD	Digital Versatile Disc
FTC	Federal Trade Commission
FTP	File Transfer Protocol
GHz	Gigahertz
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IoT	Internet of Things
IP	Internet Protocol
ISP	Internet Service Provider
IT	Information Technology
MAC	Media Access Control
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
SoHo	Small Office / Home Office
SP	Special Publication
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
USB	Universal Serial Bus
VPN	Virtual Private Network
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity
WPA	WiFi Protected Access
WPA2	WiFi Protected Access Version 2
WPA3	WiFi Protected Access Version 3
WPAN	Wireless Personal Area Network
WPA-PSK	WiFi Procted Access – Pre-Shared Key
WPS	WiFi Protected Setup

Network Security Checklist

The following checklist contains the configurations that should be put into place after the correct network device is purchased. It is possible that some of the steps below are not applicable to your situation.

- [ ] **Register your device with the manufacturer**
- [ ] **Change the default administrative password of all routers and modems to something unique**
- [ ] **Use a unique password to access your ISP's web portal**
- [ ] **Enable two-factor authentication wherever possible. This may include accessing the ISP web portal, the router/modem, or a mobile app**
- [ ] **Change the WiFi network name (i.e., SSID) password to something unique**
- [ ] **Ensure the WiFi network (i.e., SSID) name does not provide any identifying information**
- [ ] **Carefully guard who has knowledge of the WiFi network password**
- [ ] **Turn off the 2.4 GHz or 5GHz network if you're not using one of them**
- [ ] **Move all routers and modems to a location not accessible by the general public or passersby**
- [ ] **Enable automatic updates for all routers and modems**
- [ ] **Turn on WPA2 or WPA3**
- [ ] **Disable WPS if possible**
- [ ] **Enable the router and modem firewall**
- [ ] **Enable network address translation (NAT)**
- [ ] **Enable DNS filtering on the router and/or modem**
- [ ] **Disable UPnP**

Mapping to the CIS Controls

The following maps the security configurations to the CIS Controls. Not all of the items below can be fully mapped to a CIS Control.

CIS Control	Defense
N/A	Register your device with the manufacturer.
4	Change the default administrative password of all routers and modems to something unique.
4	Use a unique password to access your ISP's web portal.
4	Enable two-factor authentication wherever possible. This may include accessing the ISP web portal, the router/modem, or a mobile app.
N/A	Change the WiFi network (e.g., SSID) password to something unique.
N/A	Ensure the WiFi network (e.g., SSID) name does not provide any identifying information.
4	Carefully guard who has knowledge of the WiFi network password.
13	Turn off the 2.4 GHz or 5GHz if you're not using one of them.
N/A	Move all routers and modems to a location not accessible by the general public or passersby.
3	Enable automatic updates for all routers and modems.
15	Turn on WPA2 or WPA3.
11	Disable WPS if possible.
12	Enable the router and modem firewall.
11	Enable NAT.
7	Enable DNS filtering on the router and/or modem.
11	Disable UPnP.

About This Document

In this document, guidance is provided on how to apply the security best practices found in telework and small office network security environments. As a nonprofit driven by its volunteers, we are always in the process of looking for new topics and assistance in creating cybersecurity guidance. If you are interested in volunteering and/or have questions, comments, or have identified ways to improve this Guide, please write us at controlsinfo@cisecurity.org.

All references to tools or other products in this document are provided for informational purposes only, and do not represent the endorsement by CIS of any particular company, product, or technology.

Contact Information

CIS
31 Tech Valley Drive
East Greenbush, NY 12061
518.266.3460
controlsinfo@cisecurity.org