# 13.9.2 Wired Network Security Facts

As a system administrator, there are several best practices that you can employ to increase the security of a wired network. The goal is to make the network more difficult to compromise and accordingly less attractive to an attacker. These best practices are listed in the following table:

| Best Practice | Description |
|---|---|
| Maintain Physical Security | Technological security measures can be circumvented if the computer systems connected to the wired network are not physically secure. Consider the following physical security measures:<br>▪ Keep server systems in a locked server room where only authorized persons who have the appropriate keys or access codes are allowed in.<br>▪ Ensure that the screen savers on workstations and notebook systems have a very short timeout period and require a password whenever a user tries to resume the session.<br>▪ Ensure workstation and notebook systems require the user to authenticate before they're allowed to resume a session from sleep or hibernation.<br>▪ Control access to work areas where computer equipment is used. For example, you could use a proximity badge reader on a locked door to regulate access.<br>▪ Ensure computers in low security areas (such as a receptionist's desk) are secured with a cable lock.<br>▪ Disable external ports on desktop and servers systems, especially USB and FireWire ports. This can be done in the BIOS/UEFI configuration or using Windows Group Policy.<br>▪ Disable or completely remove optical disc burners.<br>▪ Uninstall any software from servers and workstations that isn't necessary. |
| Protect User Accounts and Passwords | Consider implementing the following measures to increase the security of user accounts and passwords:<br>▪ Require strong passwords. A strong password is at least 8 characters long, uses upper- and lower-case letters, and includes numbers or non-alphabetic characters.<br>▪ Don't allow users to write down their passwords.<br>▪ Ensure all user accounts have passwords assigned.<br>▪ Disable guest user accounts.<br>▪ Change default user names (such as Administrator) to something less obvious (such as Winifred).<br>▪ Immediately disable or remove accounts when users leave the organization.<br>▪ Change default usernames and passwords. Many network devices, such as routers and switches, use a default user name and password for initial setup. These default user names and passwords are widely posted on the internet. |
| Implement MAC Address Filtering | MAC address filtering restricts access to the wired network switch to hosts that have specific MAC addresses. This can be done in two different ways:<br>▪ Use a whitelist, which defines a list of MAC addresses that are allowed to connect to the switch.<br>▪ Use a blacklist, which defines a list of MAC addresses that are not allowed to connect to the switch.<br><br>With MAC address filtering enabled, a switch checks a computer's MAC address when it connects to the wired network. If the switch has been configured to use a whitelist, it will compare the computer's MAC address to the whitelist. If its address is listed in the whitelist of allowed MAC addresses, then the switch will allow the host to connect to the wired network. If the computer's MAC address is not in the whitelist, then the host will be denied access.<br><br>If the switch is configured to use a blacklist, the opposite occurs. If the computer's MAC address is on the blacklist, the switch will not allow the host to connect to the network. If its MAC address is not listed in the blacklist, the switch will allow the computer to connect to the network.<br><br>For security reasons, whitelists are usually the preferred option. This configuration locks out all hosts except for those specifically allowed in the whitelist. However, MAC address filtering provides only a basic level of network security and can be defeated by a determined attacker. However, it does make the network harder to compromise and hopefully less attractive to an attacker. |

| | |
|---|---|
| Implement Static IP Addressing | In order to use IP addresses efficiently, most networks use a DHCP server to automatically assign an IP address to hosts whenever they connect to the network. However, this configuration presents a security weakness. If attackers are able to successfully connect a system to an open network jack in your wired network, they automatically receive all the configuration information they need to communicate with other hosts on the network.<br>To prevent this, use static IP addressing instead of DHCP. In this configuration, an attacker who manages to successfully connect to your wired network won't receive any IP addressing information. Be aware that using static IP addressing isn't a fool-proof security measure. Determined attackers will eventually be able to determine the IP addressing scheme used on your network and configure their system appropriately. However, it does make your network more difficult to compromise. |
| Disable Unused Switch Ports | The security of a wired network can be increased by disabling unused network wall jacks and switch ports. If an unused network jack is left in an active state, it can be used to connect to the wired computer network. Likewise, an unused port on the switch that is left in an active state can provide an attacker with an easy way to connect to the wired network.<br>To prevent this from happening, disable all unused switch ports. This is especially true for switch ports connected to network jacks located in insecure areas of your organization, such as the reception area. |
| Install Firmware Updates | It is important that you keep the firmware of your network devices updated, including:<br>▪ Switches<br>▪ Routers<br>▪ Firewalls<br><br>The firmware contains software instructions that allow these devices to run. It's not unusual for security weaknesses to be discovered in the firmware of these devices when they are deployed in production environments. To address these weaknesses, the hardware vendor should release updates to the firmware. Unlike standard software, which can be automatically updated over a network connection, firmware updates must usually be installed manually. You should watch for updates for your devices to be released and install them when they become available. |
| Maintain Firewalls | You should ensure that network hosts are protected by a firewall. A firewall monitors incoming and outgoing network traffic to make sure it is allowed by the organization's security policy. Firewalls should be implemented:<br>▪ On each individual host<br>▪ On the network itself<br><br>The validity of network traffic is determined by the access control list (ACL) configured on the firewall. To increase the security of your wired network, ensure your firewall ACLs are configured to allow only authorized traffic on the network. The best way to do this is to start with all traffic blocked. This is usually enabled by default on most network firewalls using a preconfigured *implicit deny* rule in all ACLs. Then add ACL rules that allow specific types of traffic through the firewall that are permitted by your organization's security policy. If network traffic that does not match any allow rules in the ACL tries to go through the firewall, it will be denied by default. |
| Implement a Demilitarized Zone (DMZ) | If internet users need to access internal network resources (such as a web server), do not allow their traffic to flow into the internal network. Instead, use a high-end router or network security appliance to create a DMZ and place the resource to which they need access within it. This divides the network into three areas of differing levels of security:<br>▪ **External network**: Little or no security<br>▪ **DMZ**: Moderate security<br>▪ **Internal network**: High security<br><br>In this configuration, external traffic enters the DMZ instead of the internal network. If a server in the DMZ is compromised by an external attacker, the rest of the network is not affected. |
| Use Content Filters | The internet contains illicit and illegal content. If your users access this type of content from your organization's network, then your organization could be held liable for their actions. To keep this from happening, implement a content filter that inspects network traffic to ensure that it meets your organization's Acceptable Use Policy (AUP). This prevents users from: |

| | |
|---|---|
| | ▪ Wasting time accessing content that is not work-related<br>▪ Accessing content that could be construed as creating a hostile work environment<br>▪ Engaging in illegal activities<br><br>Most content filters can be configured to use pre-defined blacklists of websites categorized according to content. However, there will always be unapproved sites that slip past these pre-defined blacklists. When this happens, most content filters allow you to manually add specific sites to the blacklists. As with network firewalls, content filters can be implemented for an entire network or on individual network hosts:<br><br>▪ A network-wide content filter usually sits near the network firewall and router, inspecting the contents of all incoming and outgoing network traffic.<br>▪ A host-based content filter is implemented as software on a specific host. |
| Do Not Allow Port Forwarding | Because of the wide-spread use of NAT routing to conserve registered IP addresses, some organizations implement port forwarding to allow access to internal network resources (such as a web server) from the internet.<br>However, when you enable port forwarding you allow untrusted traffic into the internal network, which should be an area of high security. In this configuration, you must rely on the security configuration of the internal host that is being accessed externally to protect the rest of the network. For this reason, port forwarding implementations should be avoided. |