Risk Mitigations for Devices on UW Networks

Intended audience

- IT Staff
- Anyone who has received a notice of a publicly exposed and vulnerable device

Purpose

This document describes the security risks posed by devices on UW networks, and best practices for mitigating these risks.

Scope

This document applies to all computing devices with a network connection: desktop computers, IoT devices, printers, cameras, managed network switches, and more. The focus is on network configuration and initial deployment; ongoing system management practices (particularly software updates) are critical, but they are out of scope for this document.

Summary of best practices

The safest solution to protect a device from attacks is a defense-in-depth approach. This means layers of defense, so that if one layer fails or is inadequate, other layers will still offer protection.

1. Actively block all connections except those from computers that are required to talk to this device. This usually means using a network firewall to control access to your devices if possible, and using the device's built-in ("host-based") firewall if it has one.
2. Do not make the device public (by giving the device a public IP address) unless you know you need to. Use private (internal, UW-only) IP addresses unless you know you need a public IP address.

3. Don't make unauthorized access easy by leaving default passwords in place or by using weak, easily guessable passwords. Ensure that even if the device is reachable by a bad actor, only authorized users are able to log in.

In the remainder of this document, we will expand on the above goals and provide some suggestions for meeting them.

Ideal: Use a UW-IT managed firewall

This addresses best practice #1 above: Actively block all connections except those from computers that are required to talk to this device.

A firewall allows you to specify which computers are allowed to communicate with your device. This gives you a high degree of confidence that only authorized computers can access it. This solution is equally effective for both IPv4 and IPv6 addresses, the latter of which may be automatically configured and are often overlooked.

Some departments choose to use their own non-UW-IT managed firewalls. This confers the same security benefits to your device as a UW-IT managed firewall, but with additional risks. Using your own firewall requires you to be responsible for managing everything that is protected by it. UW-IT networking and security teams cannot directly see or block devices causing problems behind it. Consequently, they must often choose between blocking the firewall itself—which interrupts connectivity for everything behind it—or waiting for its owner to figure out which computer is problematic.

We recommend you install and use a UW-IT managed firewall rather than installing and managing your own device. The UW-IT Managed Firewall Service requires some technical knowledge to implement correctly, and we can help. Please contact the Office of the CISO if you'd like guidance on how to do this for your department.

Alternative: Host-based firewalls

This also addresses best practice #1: Actively block all connections except those from computers that are required to talk to this device.

Host-based firewalls include Windows Defender Firewall, Linux iptables, and MacOS Firewall; these add another layer of protection and are especially important for devices which are not always on networks that you control, or where network firewalls cannot be installed.

An advantage of host-based firewalls is that rules can be quite granular. There's no need to trust all hosts on your network; you can precisely control which computers are allowed to communicate with your device.

Host-based firewalls may be the best option for wireless devices as well.

Host-based firewalls do have some disadvantages:

1. They are sometimes modified by software or operating system updates without your knowledge. This may be merely undesirable, or, in some cases, malicious.
2. Host-based firewalls may be more cumbersome to manage if you don't have a configuration management system (such as Windows computers in an Active Directory OU).
3. Many devices, particularly printers and IoT devices, have no built-in firewalling mechanism. Worse, these tend to be the least robust and most commonly exploited devices. So, if you have any devices other than general purpose computers on your network, it's probably not possible to rely on host-based firewalls alone.

Consult your device's documentation for instructions on enabling a host-based firewall.

Another layer of defense: Private IP addresses

This addresses best practice #2: Do not make the device public (by giving the device a public IP address) unless you know you need to.

If you're unable to use a firewall of any kind, you can reduce the exposure of your device by choosing its IP address carefully and paying close attention to its configuration.

"Private" IP addresses for IPv4

For IPv4 addresses, you can choose to put your device in "private" IP address space. Previously known as "p172" addresses, they now include addresses starting with 10, and within the UW are referred to as "10net," such as 10.xx.yyy.z. (More information about 10net addressing can be found on this page on IT Connect.) A "private" IP address is one that may reach out to the internet but cannot be reached directly from the internet. For IPv6 addresses, you can choose to put your device on a ULA (Unique Local Address). This is an IPv6 address which can only reach hosts on its own network.

Be aware that many devices will automatically configure IPv6 for you if your network supports that (through a protocol called SLAAC), and that IPv6 should not be ignored. You must either configure IPv6 correctly or disable it. Private IPv4 addresses may use Network Address Translation (NAT), which allows them to reach out to, but not receive connections from, the internet. Addresses of this type are most suitable for desktop computers and any device which does not need to be accessed from computers on the internet. There is no NAT feature available for IPv6 addresses.

It is critical to note that “private” IP addresses are still vulnerable. Since the UW is a very large open network, other compromised UW computers can still attack yours. Further, if your computer is compromised, it can still attack any other UW computer, and, if it uses NAT, it can also attack computers anywhere in the world. This is why you should avoid relying on private addressing alone as a means of access control—or understand its limitations if you have no other choice.

In summary, a “private” IP address can reduce the number of computers that are able to attack yours, but it does not prevent attacks entirely. This option should not be considered as a security mitigation unless there is no firewalling option available to you.

If you need help determining whether you are using public or private IP addresses, or determining which type of IP addressing you need, please contact ciso@uw.edu.

Always change default passwords

This addresses best practice #3: Don't make unauthorized access easy by leaving default passwords in place or by using weak, easily guessable passwords.

Many devices, particularly those such as cameras, network switches, and medical and IoT devices, ship with default, published "admin" passwords. It is critical to change default passwords immediately when deploying a new device. Attackers are aware of the default passwords on these devices, and frequently use them to gain easy access to them for abuse or data theft.

Get Help

If you have questions about implementing these services, contact ciso@uw.edu for a consultation.

References

IT Connect:

https://itconnect.uw.edu/connect/uw-networks/firewall/
https://itconnect.uw.edu/connect/uw-networks/network-addresses/private-address-routing/
https://itconnect.uw.edu/connect/uw-networks/network-addresses/ipv6/
UW Network Port Blocking | IT Connect

UW IP address blocks