Communications Security Establishment Canada
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

Security considerations for edge devices

Canada

Partnering agencies

Communications Security Establishment Canada
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

Te Tira Tiaki
Government Communications Security Bureau

National Cyber Security Centre
PART OF THE GCSB

National Cyber Security Centre
a part of GCHQ

NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA

Edge devices are an important part of many enterprise computing systems. They allow connection across various devices that aid in productivity. However, as with many technologies they are not without their vulnerabilities. Edge devices require attention and diligence to keep data safe and secure.

Cyber threats actors have increasingly exploited vulnerabilities in edge devices to compromise organizations worldwide. Targeting edge devices has now become a tactic of choice for many cyber threat actors, including state-sponsored actors.

This publication provides organizations with an overview of cyber security considerations and threats relating to edge devices. It also includes examples, recommendations and mitigations that IT professionals can take to reduce the risk of compromise.

This publication is part of a series of complementary publications on cyber security measures and mitigations for edge devices:

- Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC)
- New Zealand's National Cyber Security Centre (NCSC-NZ)
- United Kingdom's National Cyber Security Centre (NCSC-UK)
- United States' (U.S.) Cybersecurity and Infrastructure Security Agency (CISA)
- U.S. National Security Agency (NSA)

Disclaimer:

The information herein is being provided "as is" for information purposes only. The authoring agencies do not endorse or favour any commercial entity, product, company or service, including any entities, products, companies or services linked or otherwise referenced within this document.

Table of contents

List of figures

Introduction

Edge devices are network hardware or software components that bridge internally managed networks and external, untrusted networks such as the Internet. These devices can connect corporate networks to the Internet and provide controlled connectivity to protected internal networks and enable traffic flow.

The terms “boundary” and “perimeter” are also used to refer to the “edge” of a network. The edge of the network is a logical boundary set by administrators to separate internal networks from external networks where malicious actors have unfettered access. Its purpose is to channel all the traffic, whether inbound or outbound, to a device that applies security policies for the protection of the internal network.

The network edge, boundary or perimeter has pathways to the internal network, where the internal services are hosted. All network edges require their own degree of security to not only keep data and the internal network safe, but also to protect the edge devices themselves from being exploited.

Commonly used edge devices

This guidance is limited to virtual private networks, firewalls, and routers as these are commonly used edge devices.

Virtual private network gateways

A virtual private network (VPN) gateway is a secure connection between two points, such as your laptop and your organization's network. A VPN acts as a tunnel that you can use to send and receive secure data across the edge of a network. The encrypted data is sent through a "tunnel" that protects it from threat actors.

For more information, see our publication Virtual private networks (ITSAP.80.101).

Firewalls

Firewalls are security devices (physical or virtual) that control the data entering and exiting a network or security zone. They monitor and control data traffic based on a predefined set of rules. Firewalls are situated at the edge between the network and the user to provide essential security. They inspect traffic going through and either allow or deny connections from reaching their destination. It is important to configure firewalls with a default deny to block unknown traffic.

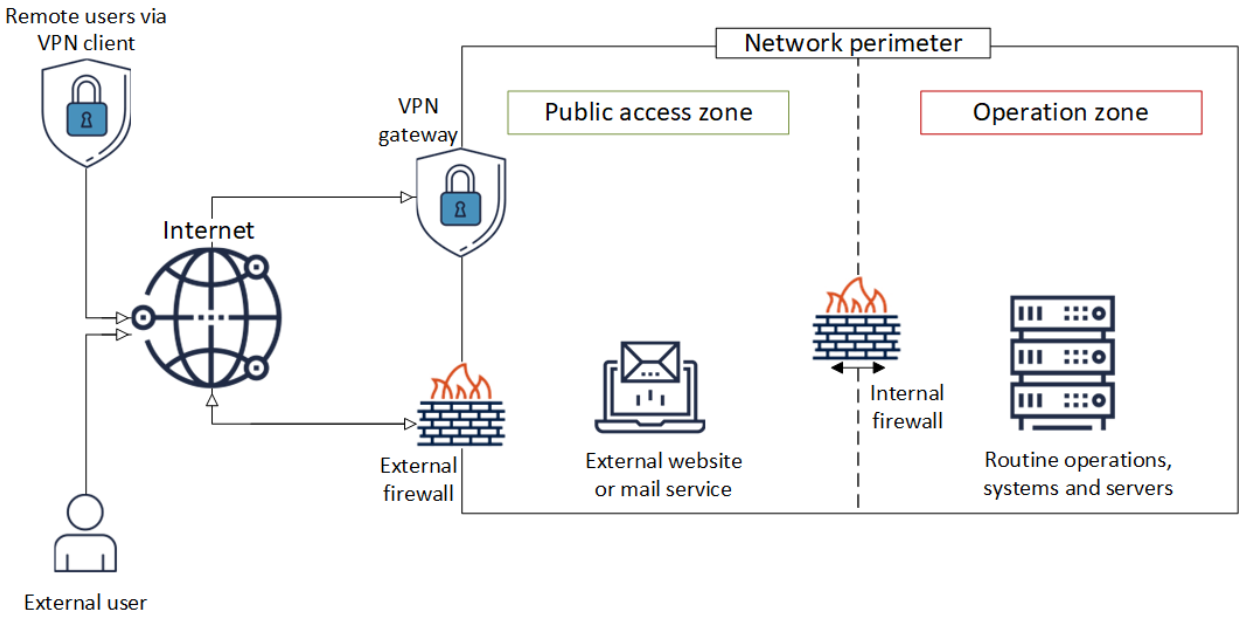
For more information, see our publication Firewall security considerations (ITSAP.80.039).

Routers

Routers direct traffic between internal networks and the Internet but they do not provide the same security as a firewall. The router can direct packets based on routing rules that are either manually configured, dynamically learned from other devices, or both. Routers are essential for any network. It is important for routers to enforce isolation of network segments to minimize their attack surface, such as OT network segments.

For more information, see our publication Router cyber security best practices (ITSAP.80.019).

Figure 1: Placement of edge devices



Long description - Figure 1: Placement of edge devices

Figure 1 illustrates where an edge device is situated. In this case the VPN gateway and the external firewall are sitting on the network perimeter between external users and the organization's network. The network can be accessed by a remote user (an employee, an external user, or a customer) through a client VPN. The traffic flows through the VPN gateway and the external firewall to enter the public access zone to reach the external website or mail service. An internal edge device, the internal firewall, sits at the edge between the organization's public access zone and their operation zone, where their routine operations, systems, and servers reside.

Considerations for edge devices

Your organization requires your corporate devices to access web and email capabilities. This means allowing connectivity between the local network and the Internet. Your organization can secure these connections by using a security-focused edge device, like a firewall, VPN or router. These types of edge devices are built to resist and block malicious traffic coming from the Internet.

Despite advancements in cyber security measures and better visibility of network infrastructures, edge devices are still at a significant risk of compromise. This is mainly due to vulnerabilities in edge devices and how the network (and gateway) architecture is configured.[1]

Some factors your organization should consider when evaluating the security of an edge device include:

- how it is made (the responsibility of the manufacturer)
- how it is configured (a shared responsibility between the manufacturer, through vendor hardening guides and through the organization)
- when the most recent software, firmware, operating system, and security updates and patches were applied

[1] Readers should note that, due to encryption, encoding and complex application protocols, boundary device enforcement alone is inadequate to protect internal systems and data from external threats. Organizations are encouraged to move from overreliance on boundary protections like edge devices by also implementing policy enforcement closer to the protected resources in the context of a zero trust architecture. For more information on implementing a zero trust architecture, see the Cyber Centre's Network and Security Strategy and A zero trust approach to security architecture, the National Institute of Standards and Technology (NIST) SP 800-207, Zero Trust Architecture, and the Cybersecurity and Infrastructure Security Agency's (CISA) Zero Trust Maturity Model.

Threats to edge devices

There are several ways in which edge devices can be compromised and leveraged by threat actors to gain access to your environment. A prominent vector is any device directly connected and used as a preventative and detective measure, such as a firewall. Threat actors will spend time and resources looking at all possible vectors to attempt to bypass boundary controls and protections in place.

Misconfigurations and mismanagement of edge devices

Any misconfigured edge device components, such as a misconfigured router or VPN, can lead to a compromise. Configuration and security standards should be set by your organization and each device deployment must follow them. While this can be taxing on resources, you can alleviate some of the pressure by leveraging a centralized configuration management model. By doing so, your organization will be able to monitor and manage security devices across your environment from one point of control.

We strongly recommend your organization's administrators perform all security and configuration related tasks from a dedicated administrative workstation, like a privileged access workstation (PAW) or a secure access workstation (SAW). This will enhance your ability to monitor for potential threats and control the scale of a cyber incident should you be compromised.

For more information on management and architectural zones, see ASD's guidance on secure administration.

Vulnerability exploitation

Threat actors focus their attention on the vulnerabilities of individual devices at the edge of the network. Edge devices are usually connected to the Internet and have public IP addresses that can be reached from anywhere. This makes edge devices particularly susceptible to exploitation as threat actors can leverage the Internet to identify and exploit vulnerabilities in these devices.

Vulnerability exploitation occurs when threat actors leverage vulnerabilities that organizations may not be aware of or have not had the chance to address with updates or patches. Exploitation of known vulnerabilities occurs when threat actors leverage vulnerabilities that have patches available but not applied.

Once zero-day threats leveraging unknown vulnerabilities are used and detected, responsible device manufacturers will release patches quickly. Your organization must keep abreast of released patches, fixes or device updates to mitigate known vulnerabilities. Your organization must have procedures in place to action updates and patches immediately, before threat actors can exploit known vulnerabilities.

Your organization can also be vulnerable if you are not receiving notifications regarding security updates and patches. If a security update is left uninstalled, your device may be vulnerable to compromises. Ensure you configure automatic updates in your environment or designate a mandatory window of time in which updates must be installed. A vulnerability scanner should be used regularly to assist you in identifying missed patches or updates for vulnerabilities in the operating systems of Internet-facing network devices. This will help you mitigate against known vulnerabilities.

Denial of service and distributed denial of service attacks

Denial of service (DoS) attacks look to impede the functionality of services and make networks unavailable. Distributed denial of service (DDoS) means that the threat actors use the many devices connected to the network to achieve their goal.

To be effective, a DDoS attack requires leveraging multiple compromised devices, sometimes referred to as a botnet. Most DoS attacks involve flooding the victim with useless traffic, and a few exploit vulnerabilities specific to the targeted service. Small office, home office or personal Internet routers are popular devices for threat actors to compromise and leave dormant until they're ready to scale up their attack. If these edge devices are not kept patched and updated, threat actors can exploit them to attack other networks.

When the time comes, the malicious actor can trigger all the compromised devices to participate in the DDoS attack. This creates enough requests to slow down, cripple or completely bring down a network by overloading the edge device's capability of defending itself.

Though this will not entirely protect against DoS and DDoS attacks, we recommend keeping edge devices patched to make it more difficult for threat actors to identify and exploit vulnerabilities in edge devices to support these attacks.

For more information on mitigating DDoS attacks, see Defending against distributed denial of service (DDoS) attacks.

Web-based applications

When connected to the Internet, your device can be exposed to intrusion attempts. For business and operational purposes, organizations often need to make a server accessible to the Internet. Such servers could include:

- edge device management servers
- mail or web servers
- servers used to provide connectivity via mobile apps
- remote access servers

This functionality may appear desirable, but it adds additional risks that should be fully considered. The external-facing server is usually put on a separate network, a demilitarized zone (DMZ), that allows connections through the firewall to external networks. Exposed edge devices or external-facing servers may increase the threat surface.

Default configuration settings

Some edge networking companies have not moved away from the practice of setting default passwords. Credentials must be changed from their default settings to enhance security, as these default passwords can be easily discovered and exploited by threat actors. IT security teams must change default configuration settings on devices before deploying them to enhance security.

We recommended that security teams create a baseline configuration document to use when configuring devices. This baseline should include disabling unneeded services, protocols and ports, and changing default usernames and passwords.

Once deployed, edge devices and their security settings become the responsibility of administrator or operator. We recommend you consult the manufacturer manual and hardening guide included with your product or with external entities such as the Center for Internet Security (CIS) for additional configuration and hardening information.

Some security settings can be locked and controlled at the administrative level, but at times, installation or implementation of security controls or settings can be left to an operator or end user that may not have deep technical understanding of cyber security. Operators and end users should review and follow available guidance on the acceptable configuration and use of edge devices provided by their organization and the manufacturer.

While tailored cyber security and acceptable use policies can assist in mitigating user error attacks, we urge manufacturers to create environments that are user-error tolerant. Adhering to secure by design (SbD) principles will enhance the security of devices and assist users in deploying them more securely.

We encourage manufacturers to follow SbD principles. By implementing SbD principles during the product design phase, manufacturers can significantly decrease the number of exploitable flaws before introducing them to the market for widespread use or consumption. SbD will also ensure products are delivered to consumers in the most secure configuration.

For more information, see the recommendations for edge device manufacturers in this publication.

Examples of edge device compromises

The following examples highlight the methods in which edge devices can be compromised and leveraged by threat actors. They also highlight some of the potential impacts of these types of compromises to organizations.

Fortinet, FortiOS (CVE-2024-21762; CVE-2022-42475)

On February 8, 2024, Fortinet disclosed an out-of-bounds write vulnerability, CVE-2024-21762, that allows a threat actor to connect without providing valid user credentials and run arbitrary commands on the edge device itself. The vulnerability, which is a vendor vulnerability with SSL VPN functionality allowed, enables an unauthenticated threat actor to run arbitrary code via HTTP command.

Furthermore, CISA reported in 2024 that malicious actors Volt Typhoon exploited CVE-2022-42475 in a network perimeter FortiGate 300D firewall that was not patched. The actors used this exploit to compromise a domain admin account stored inappropriately on the device.

Cisco, Cisco IOS (CVE-2023-20198; CVE-2023-20273)

Similar to the Fortinet incident described above, the root cause was the result of leveraging two separate vulnerabilities. The first vulnerability was leveraged to gain “privilege 15” access (administrative access) to create a new user account with a fixed password set by the attacker. Then, a separate vulnerability was allowed to persist within the web configuration interface. This created files on the flash drive to gain additional access and persistence so that restarting the device would not eliminate the backdoor access.

The compromise was a zero-day vendor vulnerability that allowed a threat actor to perform privilege escalation via the web UI configuration interface of devices. We recommend that network management interfaces (NMIs) should not be directly exposed to the Internet.[2] In addition, your organization should review your architecture and determine whether a zero trust approach would be feasible. Robust architecture will help to mitigate this type of vulnerability.

For an in-depth look at a VPN compromise, see the Cyber Centre’s report on Cyber activity impacting CISCO ASA VPNs.

[2] It is possible for vendors to harden their products so that they remain secure with NMIs exposed to the internet. This is a solved problem, and customers should demand vendors harden their devices to secure NMIs.

Mitigating threats to edge devices

Your organization can reduce the risk of compromise to your edge devices by implementing the following mitigation recommendations:

- Subscribe to security notifications from the device's vendor and to advisories provided by the Cyber Centre
- Follow vendor hardening guides
- Install security patches on edge devices as quickly as possible after testing for reliability on a standby or test device
    - Establish an automated or monitored patch management schedule to ensure patches are applied when they become available
- Enable centralized (off-device) logging and configure log levels to be as detailed as possible
- Use strong, phishing-resistant multi-factor authentication (MFA) for all administrative access to devices
- Alert on successful administrative log-ons, configuration changes and hardware changes
- Detect hardware changes using vendor-specific detection tools or commands
- Follow industry standard change management processes for all configuration changes of security
    - Require two (or more) people to review a change before it can be implemented
- Deactivate any functionality that is not required
- Routinely review security rules for relevancy
    - The more dynamic the network, the more frequent this review should be performed
- Maintain an inventory of edge devices and their respective support timelines
    - Manage the lifecycle of any end-of-life (EoL) device and end-of-life service (EoSL) as any discovered vulnerability on a device will remain unpatched
    - Periodically review which edge devices have an upcoming EOL date and plan to remove or replace them before EOL occurs
    - Investigate and implement compensating controls for EoSL your organization is unable to remove
- Leverage centralized authentication with role-based access control to minimize the risks associated with local accounts and to help with access management
    - Consider the risks associated with deploying authentication services and approaches within your environment[3]

[3] Central authentication systems, such as Active Directory, increase an organization's attack surface when edge device authentication is linked to the primary corporate identity store or when one Identity Provider (IDP) is used across multiple security zones. It is critical to segregate edge devices from an organization's corporate AD forest or an equivalent authentication, authorization and accounting (AAA) solution.

- Use an out-of-band management network or administrative workstation that is physically separated from the operational data flow network
    - Ensure the management of the network infrastructure devices can only come from an out-of-bound management network
- Use a hardened host to reduce the risk of administrative credentials and MFA being exploited by a compromise of the local host
- Include edge device compromise as part of your organization's incident response plan
    - Conduct practice exercises to ensure the plan is effective and will allow your organization to identify, contain, remediate and recover with limited impact to your operations
    - Consider vendor diversification when selecting vendors for edge device functions to reduce and mitigate the supply chain integrity threat surface

For more information on additional ways organizations can secure their devices, see the following publications:

- Network security logging and monitoring (ITSAP.80.085)
- Preventative security tools (ITSAP.00.058)
- How updates secure your device (ITSAP.10.096)

Although these risks are prevalent, central authentication systems also offer a range of security advantages, including fine-grained access control, device management plane isolation, and robust hardening of centralized authentication services. These measures can limit lateral movement risks and provide benefits like individual accountability, synchronized account revocation, efficient credential management, logging and anomaly detection. To effectively manage these risks, organizations should consider both the vulnerabilities and the security strengths of centralized authentication, and tailor their approach accordingly.

Alternative AAA solutions beyond Active Directory may offer similar benefits while addressing specific vulnerabilities. For a detailed approach to secure centralized AAA configurations, refer to NSA's Network Infrastructure Security Guide."

Recommendations for edge device manufacturers

The authors encourage all edge device manufacturers to make their products secure by design by including security considerations throughout the product design and development process, with the goal of reducing the prevalence of vulnerabilities in edge devices. Secure-by-design principles describe how manufacturers should improve security outcomes for their customers by taking ownership of the security of their products.

For more information, manufacturers should review the joint guidance Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software (published by the Cyber Centre and international cyber security partners).

For guidance for manufacturers to implement secure features by default in edge device products, see CISA's Secure by Design Alert: Security Design Improvements for SOHO Device Manufacturers.

We also encourage manufacturers to join CISA's Secure by Design Pledge, which outlines specific goals for manufacturers to meet to make their products more secure, including goals to reduce the presence of vulnerabilities in their products and transparently report on vulnerabilities.

Additional information

This publication only addresses your organization's corporate boundary security. For more information about protecting your organization and your remote workers, please see the following publications:

- Security tips for organizations with remote workers (ITSAP.10.016)
- End user device security for Bring-Your-Own-Device (BYOD) deployment models (ITSM.70.003)
- Known Exploited Vulnerabilities Catalog
- CISA Tabletop Exercise Packages