CENTRE FOR
CYBERSECURITY
BELGIUM

NETWORK DEVICE

LOGGING RECOMMENDATIONS

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Date: March 2026
Version: 1.0 English
Author: The Centre for Cybersecurity Belgium (CCB)

The Centre for Cybersecurity Belgium (CCB) is the national authority for cybersecurity in Belgium. The CCB was established by Royal Decree of 10 October 2014 and operates under the authority of the Prime Minister.

Based on its legal mission, the CCB tries to inform and advise organisations on improving network device logging and visibility. This document provides technical guidance in response to the current geopolitical landscape and adversarial campaign trends, aiming to detect and be able to respond to attacks against network devices.

Executive summary

This document outlines a logging baseline for network infrastructure such as routers, switches, and firewalls to transform raw data into actionable intelligence. By prioritizing the collection and offloading of authentications, privilege changes, and configuration updates, this recommendations guide ensures staff have the critical visibility needed to:

- Detect unauthorized access in real-time.
- Investigate security incidents with a clear audit trail.
- Remediate threats before they impact operations.

Implementing these recommendations can enable an organisation to move from reactive monitoring to a proactive, defensible network architecture.

Table of contents

1. Importance of good logging

Network infrastructure forms the central nervous system of our business operations. However, unlike workstations and servers, network devices are frequently treated as "black boxes" with limited inherent visibility.

Historically, organisations have often overlooked comprehensive network logging due to storage constraints or operational overhead. This oversight creates a critical blind spot. Many smaller edge devices (such as branch routers) rely on volatile memory; without centralized log offloading, a simple device reboot permanently destroys all forensic evidence of a compromise. In the event of a breach, the absence of these logs can needlessly complicate an incident response effort.

In light of recent high-profile vulnerabilities and sophisticated nation-state campaigns, the importance of this logging baseline is greater than ever.

Advanced persistent threats (APTs) and state-sponsored actors have shifted their focus toward network edge devices, particularly firewalls, VPN concentrators, and routers. Because these devices are directly exposed to the internet and typically cannot run traditional endpoint antivirus software, they are prime targets for zero-day exploits. Attackers use compromised network devices to establish stealthy persistence, bypass access controls, and quietly pivot into the internal network, or use the compromised infrastructure as a proxy to attack other entities.

Without the logging practices defined in this baseline, specifically the immediate offloading of failed logins, unexpected configuration changes, and unauthorized command executions, these advanced compromises can remain undetected for months.

In conclusion, adopting a logging baseline is a vital element of a solid defense-in-depth strategy. By standardizing what to log, where to store it, and how long to keep it, this approach transitions our network infrastructure from a potential blind spot into a proactive layer of security monitoring and incident response capabilities, without overwhelming storage infrastructure.

2. Network device logging setup

2.1. ARCHITECTURAL & CONFIGURATION PREREQUISITES

Before configuring individual devices, these foundational elements must be in place to ensure your logs are accurate and secure.

2.1.1.LOG OFFLOADING (CENTRALIZED LOGGING)

Avoid relying solely on local device storage when possible, especially for smaller devices (like branch routers or edge switches) that use volatile memory (RAM) for logs. A reboot will wipe evidence of a compromise.

- Configure all devices to immediately forward logs to a centralized Syslog server or SIEM (Security information and event management) system.
- Use Syslog over TCP or TLS (if supported) rather than UDP to improve delivery reliability of critical security events.

2.1.2.TIME SYNCHRONIZATION

Logs are ineffective for incident response if the timestamps do not align.

Configure all network devices to synchronize with a minimum of two reliable, internal Network Time Protocol (NTP) servers. Use UTC time across all devices globally to prevent timezone confusion.

2.1.3. DEDICATED MANAGEMENT INTERFACES

Whenever possible, restrict SSH/HTTPS access to a dedicated out-of-band management network or specific jump boxes.

2.1.4. PATCH MANAGEMENT

Establish a risk-based patch management process for network devices with special attention to Internet-facing devices. High-risk vulnerabilities should be assessed and remediated without delay, with compensating controls where immediate patching is not feasible.

This is important, as exploitation in the wild often commences as early as 48 hours (or less) after disclosure of the patch.

2.2. GENERAL SECURITY LOGGING (ALL DEVICES)

Regardless of whether the device is a router, switch, or firewall, the following events are critical for tracking unauthorized use. These events should be logged at a notice (level 5) or info (level 6) syslog severity level, depending on the vendor. Consider enabling administrator command logging (Authentication, Authorization, Accounting) on protocols like TACACS+/RADIUS to record privileged session start/stop events and individual command execution.

It is worth noting that uptime monitoring can also be a valuable metric to detect compromise. Root cause analysis should always be performed when a service outage occurs.

Organisations should also monitor the health of the logging pipeline itself, generate alerts for forwarding failures, storage failures, time drift, certificate issues, and unexpected loss of telemetry.

Event Type	**What to Log**	**Security Value**
Authentication	All failed login attempts (SSH, HTTPS, Console).	Detects brute-force attacks and credential stuffing.
Authentication	All successful logins and logoffs.	Establishes a baseline of "normal" access and identifies compromised accounts.
Privilege Escalation	Successful and failed attempts to enter privileged execution mode (e.g., Cisco enable, Juniper configure).	Tracks lateral movement and unauthorized administrative control.
Configuration Changes	Any execution of configuration commands; saving of the configuration.	Identifies unauthorized backdoors, rogue ACLs, or traffic redirection.
System State	Device reboots, OS upgrades, hardware failures (fan/power), clearing of local logs.	Detects attempts to cover tracks (clearing logs), denial-of-service or crashes (potential result of exploitation).
Web interface access logs	Web server access logs for a web UI that the device might expose.	Detect exploitation attempts and potential web shell interaction.

2.3. DEVICE-SPECIFIC LOGGING RECOMMENDATIONS

Beyond basic access control, different devices provide unique telemetry for detecting malicious behavior.

2.3.1. ROUTERS & SWITCHES

Event Type	What to Log	Security Value
Port security violations	Log when an unauthorized MAC address attempts to connect to a switch port (MAC limiting/Sticky MAC violations).	Detect physical rogue devices.
Routing protocol events	Log neighbor state changes (e.g., BGP or OSPF neighbor down/up).	Frequent flapping can indicate network instability or a man-in-the-middle route hijacking attempt.
Spanning tree protocol (STP) Changes	Log root bridge changes or topology change notifications.	Attackers can manipulate STP to intercept VLAN traffic.
Access control list (ACL) Hits	Log drops on infrastructure ACLs (e.g., traffic attempting to reach the router's internal IPs from the outside)	Detect malicious connections to your network devices.

2.3.2. FIREWALLS & VPN CONCENTRATORS

Event Type	What to Log	Security Value
Denied traffic	Log all traffic denied by the implicit deny rule at the bottom of your firewall policy, particularly inbound from the internet.	Detect anomalous disallowed traffic not caught by configured policies.
High-Risk allowed traffic	Log allowed traffic from untrusted zones (Internet) to DMZ resources.	Tracks potential exploitation attempts.
Lateral movement	Log denied inter-zone policy violations (for example: RDP/SSH between segments that are not normally allowed to interact with one another)	Detect an intrusion before actions on objective occur.
VPN authentication	Log all successful and failed VPN connections, including the source IP address, username, and assigned internal IP.	Early detection of brute-force attempts of credential theft/reuse.
Threat intelligence/IDS/IPS	If the firewall has next-gen capabilities, log all triggered intrusion signatures, malware blocks, and connections to known malicious IP addresses.	Detection of exploitation attempts: TTPs can indicate threats the organisation faces.

Event Type	What to Log	Security Value
NAT exhaustion	Log events indicating port/address exhaustion.	Can be an early indicator of a DDoS attack or an internal compromised host scanning outward.

3. Log Retention Recommendations

Retention policies are often dictated by compliance frameworks (like ISO 27001), but if you are establishing a baseline from scratch, follow these industry standards on your centralized logging server:

- Hot storage (Active Search/SIEM): Keep logs for 30 to 90 days in easily searchable, indexed storage. This allows for immediate incident response, dashboarding, and threat hunting.
- Cold storage (Archive): Keep compressed, encrypted logs for 1 year (or longer if mandated). This is crucial for forensic investigations, as many breaches are not discovered until months after the initial compromise.
- Tamper protection: Logs should be protected against unauthorized alteration and deletion. Where feasible: use immutable or tamper-evident storage and preserve raw events.

4. GDPR

Security logging should be implemented in line with GDPR obligations.

Organisations should document the purpose of each log category, limit collection to what is necessary for security and incident response, restrict access on a need-to-know basis, and define retention periods (operational, legal, regulatory).

5. Build effective alerting and detection rules

To catch a compromise before it spreads, an organisation must shift from simply storing logs to actively monitoring them. Meaningful alerting requires a strict focus on high-risk security events.

Establishing a baseline for anomaly detection requires formalized operations. Fragmented workflows and ad hoc tooling create 'noise' that obscures threats and triggers false positives. Standardising day-to-day operations ensures legitimate activity is predictable, allowing malicious intrusions to stand out rather than hide within undocumented practices.

The approach to configuring alerting depends on the setup of the centralized logging platform. It is worth mentioning that both approaches have their use cases, and the choice between them has to be evaluated on a per-case basis, depending on the organisation’s needs and resources.

5.1. SYSLOG SERVER

The main benefit of a syslog server is that it is relatively cheap to set up, and not very resource-intensive to maintain. For organisations constrained by resources, it is an excellent starting point.
However, since a standard syslog server lacks analytical capabilities to correlate events, alerting must be simple and binary.
To avoid alert fatigue, only the most critical events should be selected to fire an alert. An example would be configuration changes outside a maintenance window, or an admin user login in the middle of the night.

5.2. SIEM

For organisations that already have a SIEM (and ideally a SOC to monitor it), it makes perfect sense to forward network device logs to it.
With a SIEM, an organisation is able to set up correlated alerts using log events that would not, by themselves, warrant investigation.
It is worth noting that, while bringing considerable benefits to the table, setting up and continuously tuning and maintaining a SIEM is resource intensive.

Annex A: References to Cyber Fundamentals (CyFun)

https://cyfun.eu/sites/default/files/2026-03/CyFun2025_Booklet_ESSENTIAL_E.pdf

- ID.AM-03-3 The organisation's network communication and external data flows shall be mapped, documented, authorised and updated when changes occur.
- ID.AM-08.11 Remote maintenance and diagnostic activities of organisational assets shall be pre-approved and the performance logged.
- PR.IR-01.5 The organisation shall implement, where feasible, authenticated proxy servers or firewalls with URL filtering and threat intelligence capabilities for defined communications traffic between its critical systems and external networks.

PR.PS-04 Log records are generated and made available for continuous monitoring

- PR.PS-04.1 Logs shall be maintained, documented, and monitored.
- PR.PS-04.2 The organisation shall ensure that logbook records contain an authoritative time source or internal clock time stamp that is compared and synchronised with an authoritative time source.
- PR.PS-04.3 Audit data from the organisation's critical systems shall be moved to an alternative system.
- PR.PS-04.4 The organisation shall ensure that audit processing failures on the organisation's systems generate alerts and trigger defined responses.
- PR.PS-04.5 The organisation shall ensure that authorised personnel can extend or enhance audit logging and monitoring capabilities when needed to support investigations or incident response

DE.AE-03 Information is correlated from multiple sources

- DE.AE-03.1 The logging functionality of protection and detection tools shall be enabled. Logs shall be backed up and retained for a predefined period and regularly reviewed to identify unusual or potentially harmful activity
- DE.AE-03.2 The organisation shall ensure that event data from critical systems is collected and correlated using information from multiple relevant sources.
- DE.AE-03.3 The organisation shall combine event analysis with information from vulnerability scans, system performance data, monitoring of critical systems, and facility monitoring, where feasible.

DISCLAIMER

“This document and its annexes have been prepared by the Centre for Cybersecurity Belgium (CCB), a federal administration created by the Royal Decree of 10 October 2014 and under the authority of the Prime Minister.

This document contains technical information written mainly in English. Indeed, this technical information is taken directly from reports communicated to the CCB by various international partners (European network of CSIRTs, international organisations, foreign companies, etc.), which are written in English. Moreover, this information related to the security of networks and information systems is addressed to the organisations concerned under the benefit of urgency and to IT services which use the English terms of computer language.

A translation into Dutch, French or German of this technical information can nevertheless be requested from the CCB.

The CCB accepts no responsibility for the content of this document.

The information provided:

- are exclusive of a general nature and do not intend to take into consideration all particular situations;
- are not necessarily exhaustive, precise or up to date on all points;

Responsible editor:
Centre for Cybersecurity Belgium
Mr. De Bruycker, General Director
Rue de la Loi, 1 !
1000 Brussels

Legal Deposit:
D/2026/14828/003