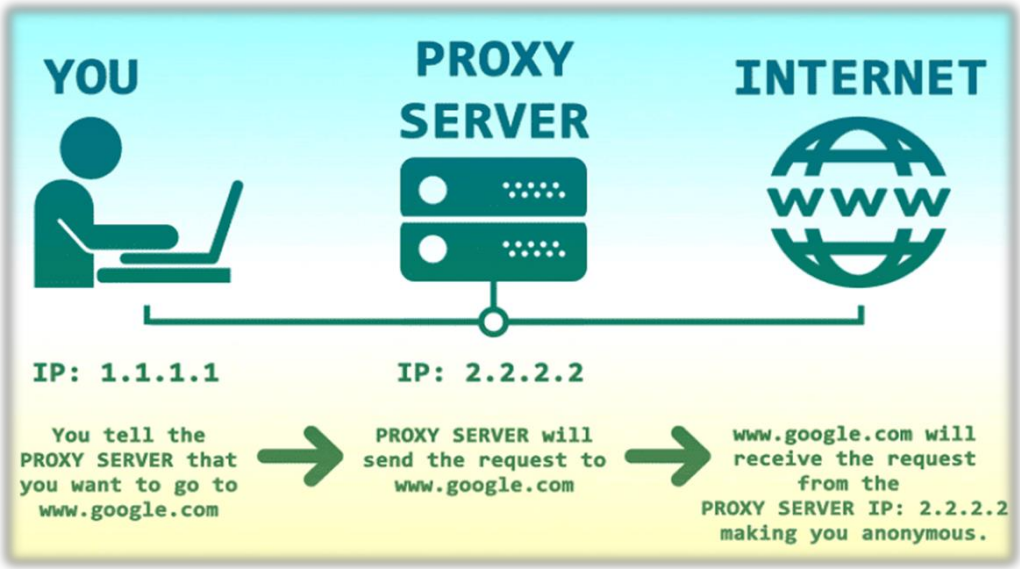
BY- Dashrath Jamadar

Dashrath Jamadar
Sr. Security Analyst at Rimini street india pvt ltd | ISC²-CC | CEH-V12 | SIEM | EDR |

Proxy Server for Monitoring Employee Outgoing Traffic

1. Definition of a Proxy Server

A **Proxy Server** is an **intermediary system** that sits between **user devices (employees)** and the **internet** to monitor, filter, log, and control web traffic. It is used to **monitor employee activity**, **block malicious sites**, **enforce security policies**, and **ensure compliance** with company regulations.



---

2. How a Proxy Server Works

Step-by-Step Process:

1. **User Request** → An employee tries to access a website.
2. **Proxy Interception** → The proxy captures the request.
3. **Policy Enforcement** → The proxy checks company security rules.
   - **Allowed?** → Request is forwarded to the internet.
   - **Blocked?** → The request is denied, and the user gets a block page.
4. **Traffic Logging** → The proxy logs the user's activity.
5. **Response Handling** → If allowed, the website's response is sent back to the employee.

---

3. Types of Proxy Servers

1) Forward Proxy

- **Usage:** Controls and monitors employee outbound internet traffic.
- **Tools:** Squid Proxy, Blue Coat (Symantec ProxySG).

Dashrath Jamadar
Sr. Security Analyst at Rimini street india pvt ltd | ISC²-CC | CEH-V12 | SIEM | EDR |

- **SOC Relevance:** Helps in web traffic filtering, blocking malicious domains, and generating logs forwarded to SIEM for monitoring insider threats or policy violations.

2) Reverse Proxy

- **Usage:** Protects and load-balances internal web servers (e.g., APIs, websites).
- **Tools:** NGINX, Apache HTTPD, F5 BIG-IP, Citrix ADC.
- **SOC Relevance:** Key for hiding backend infrastructure, terminating SSL, and mitigating DDoS. Logs help track external client access to internal resources.

3) Transparent Proxy

- **Usage:** Enforces policies without user configuration.
- **Tools:** Cisco Web Security Appliance (WSA), FortiGate, Palo Alto firewalls (URL filtering).
- **SOC Relevance:** Passive monitoring of web traffic for threat intel, malware callouts, or data exfiltration.

---

4. Log Formats Supported by Proxies

Proxy servers generate logs in multiple formats to integrate with **SIEM, DLP, and network monitoring tools**:

- Syslog (RFC 5424 format)
- Common Event Format (CEF)
- Log Event Extended Format (LEEF)
- JSON (JavaScript Object Notation)
- Plain Text (CSV, TXT)

---

5. Logs Generated and Sent to SIEM

Common Proxy Logs Sent to SIEM:

- **Website Access Logs** – Records URLs visited by employees.
- **Blocked Request Logs** – Shows attempts to access restricted websites.
- **Bandwidth Usage Logs** – Logs large file downloads or excessive streaming.
- **User Authentication Logs** – Tracks who accessed which sites.
- **Malware Detection Logs** – Logs access to suspicious or phishing domains.

Dashrath Jamadar
Sr. Security Analyst at Rimini street india pvt ltd | ISC²-CC | CEH-V12 | SIEM | EDR |

6. Advantages of Using a Proxy Server for Monitoring

1. **Enhances Security** – Blocks malicious sites and phishing attempts.
2. **Reduces Data Leakage** – Prevents unauthorized uploads of sensitive data.
3. **Controls Employee Internet Usage** – Limits access to non-work-related websites.
4. **Improves Bandwidth Management** – Restricts excessive streaming or downloads.
5. **Enforces Compliance** – Helps meet **PCI DSS, GDPR, HIPAA** security policies.
6. **Speeds Up Content Delivery** – Uses caching to load frequently visited sites faster.
7. **Protects Against Insider Threats** – Detects unusual web activity.

---

7. Disadvantages of Proxy Servers

1. **May Slow Down Internet Speed** – Extra processing time for filtering traffic.
2. **Bypass Risks** – Users may use VPNs or proxy avoidance tools.
3. **Privacy Concerns** – Employees might feel monitored too much.
4. **Maintenance Overhead** – Requires updates and tuning to keep effective.

---

8. Proxy Log Flow to SIEM

1. **Employee Sends a Request** → Tries to access a website.
2. **Proxy Captures and Logs the Request** → Checks against security rules.
3. **Logs Forwarded to SIEM** → SIEM correlates with other security events.
4. **SOC Team Investigates Anomalies** → If suspicious behavior is detected, action is taken.

Example SIEM Use Case:

- **Scenario:** Employee **uploads sensitive data** to an unknown website.
- **Proxy Server Action:**
  - Detects and **blocks the request**.
  - Sends an alert to **SIEM**.
  - SOC analysts investigate **data exfiltration risk**.

---

9. Top Proxy Vendors in 2025

1. Zscaler Internet Access (ZIA)
2. Blue Coat (Broadcom Symantec)

Dashrath Jamadar
Sr. Security Analyst at Rimini street india pvt ltd | ISC²-CC | CEH-V12 | SIEM | EDR |

3. Palo Alto Prisma Access
4. Cisco Umbrella
5. Forcepoint Web Security
6. McAfee Web Gateway
7. Squid Proxy (Open-Source)
8. Fortinet FortiProxy
9. Sophos Web Gateway
10. Barracuda Web Security Gateway

---

10. Top use-cases for Proxy Server Monitoring

Threat Detection & Web Security

1. **Blocking Malicious Websites** – Prevents access to phishing domains.
2. **Detecting C2 Communications** – Identifies connections to known malware servers.
3. **Preventing Drive-By Downloads** – Blocks sites hosting malware-infected files.
4. **Identifying Anomalous User Behavior** – Detects sudden access to unknown domains.
5. **Blocking VPN and Proxy Avoidance Tools** – Prevents users from bypassing company restrictions.

Employee Monitoring & Productivity Control

6. **Restricting social media Access** – Limits distractions like Facebook, Twitter, Instagram.
7. **Blocking Streaming & Entertainment Sites** – Prevents bandwidth abuse on YouTube, Netflix.
8. **Tracking User Web Activity** – Logs and audits employee browsing history.
9. **Monitoring Unauthorized Data Uploads** – Prevents users from sending sensitive data to personal cloud storage.
10. **Detecting Job-Hunting Activity** – Identifies excessive visits to job portals like LinkedIn, indeed.

Data Protection & Compliance Enforcement

11. **Blocking File Sharing Services** – Restricts unauthorized use of Dropbox, Google Drive.
12. **Preventing Unauthorized API Calls** – Blocks suspicious web-based API requests.
13. **Ensuring SSL Inspection** – Analyzes encrypted traffic for hidden threats.
14. **Compliance Reporting** – Generates reports for **GDPR, PCI DSS, HIPAA** adherence.

BY- Dashrath Jamadar

Dashrath Jamadar
Sr. Security Analyst at Rimini street india pvt ltd | ISC²-CC | CEH-V12 | SIEM | EDR |

Backend Process of a Proxy Server (Focus: Web Security in SOC)

Applies to tools like: Zscaler, Bluecoat (Symantec ProxySG), Forcepoint, Squid, Palo Alto (URL Filtering Proxy), Cisco Umbrella, etc.

---

1. Client Request Handling (Intercept or Explicit Mode)

When a user accesses a website (e.g., https://example.com), the proxy server acts as a **middleman** between the user and the internet.

Modes:

- **Explicit Proxy**: Browser/device is configured with proxy IP and port (e.g., 8080).
- **Transparent Proxy (Intercepting)**: Traffic is silently redirected (via WCCP, PBR, etc.).

Captured Info:

- Source IP, Username (if auth integrated)
- Request method (GET, POST)
- URL, domain, destination IP/port
- User-Agent and browser headers

📌 *Initial stage where the proxy decides to allow, block, or scan the request.*

---

2. Authentication & User Identification

If the proxy is integrated with identity providers (e.g., **Active Directory**, SAML, or Okta):

- It identifies **who the user is** behind the request.
- Assigns **user groups, policies**, and logs the user session.

Methods:

- NTLM/Kerberos (for domain-joined devices)
- Captive portal (for guest devices)
- SAML/OpenID (for cloud proxies)

📌 *User identity is essential for access control, audit logs, and policy enforcement.*

---

3. URL Filtering & Web Category Check

The requested URL is checked against a **web categorization database** to decide if it falls into allowed/disallowed categories.

Categories include:

- Security: Malware, Phishing, Command & Control

Dashrath Jamadar
Sr. Security Analyst at Rimini street india pvt ltd | ISC²-CC | CEH-V12 | SIEM | EDR |

- Business Use: SaaS, Cloud Storage, News
- Non-Business: Gambling, Pornography, Social Media

Policies may vary by user group:

- Finance: Allowed to access banking sites.
- Interns: Denied access to cloud storage or dev tools.

📌 *Stops users from reaching unsafe or non-compliant destinations.*

---

4. Threat Intelligence & Real-Time Reputation Checks

If the URL/IP/Domain is suspicious or unknown:

- Proxy checks against threat feeds and **reputation databases**.
- It may invoke **cloud sandboxing** (Zscaler, Bluecoat Intelligence Cloud, etc.).

Checks:

- Is the domain recently registered?
- Is the IP part of a known botnet or malware C2?
- Is the URL similar to known phishing domains (typosquatting)?

📌 *Helps detect advanced threats and zero-day web-based attacks.*

---

5. SSL Inspection / HTTPS Decryption (Optional)

For **HTTPS traffic**, if SSL inspection is enabled:

- Proxy terminates the SSL session from the client.
- Decrypts the traffic (acts as MITM with org certificate).
- Scans the payload (e.g., file download, post request data).
- Re-encrypts and forwards to destination.

Used to:

- Detect malware in downloads
- Prevent credential theft via phishing
- Log/search query contents (optional)

📌 *Critical for deep packet inspection of encrypted web traffic.*

---

6. File Type Control, DLP, and Malware Scanning

If the user downloads/upload files (e.g., .exe, .doc, .zip):

- File is **scanned inline** using:

Dashrath Jamadar
Sr. Security Analyst at Rimini street india pvt ltd | ISC²-CC | CEH-V12 | SIEM | EDR |

- AV engines
- Sandboxing
- DLP policies

Checks:

- File hash (known malware?)
- Sensitive data (e.g., credit card numbers in uploads)
- Behavior analysis (detonation in sandbox)

📌 *Prevents both inbound and outbound data threats.*

---

7. Response Handling & Client Delivery

Once allowed:

- Proxy **fetches the content from the destination server**.
- Applies **caching, compression**, or **response filtering** (e.g., strip headers).
- Forwards it back to the client browser securely.

If blocked:

- User sees a **custom block page** (URL category violation, malware found, etc.)

📌 *Client receives content or block notification with full traceability.*

---

8. Logging, SIEM Integration, and SOC Visibility

All activities are **logged centrally** and forwarded to SIEM (e.g., QRadar, Exabeam, Splunk) for correlation and alerting.

📁 Logs typically include:

- Timestamp, User, Source IP
- Requested URL/domain
- Destination IP
- Action taken (Allowed/Blocked)
- Threat category or malware detection (if any)
- File download/upload activity
- SSL inspection results (if applied)

📌 *SOC analysts use these logs to investigate phishing, malware access, data exfiltration, and insider threat activity.*

Final Flow Summary:

- [User Request] ➜

BY- Dashrath Jamadar

Dashrath Jamadar
Sr. Security Analyst at Rimini street india pvt ltd | ISC²-CC | CEH-V12 | SIEM | EDR |

- [Authentication] ➜
- [URL Categorization & Policy Match] ➜
- [Threat Intelligence Lookup] ➜
- [SSL Decryption (Optional)] ➜
- [Payload/File Inspection] ➜
- [Access Decision (Allow/Block/Quarantine)] ➜
- [Response to Client] ➜
- [Logging & SIEM]

Use Cases

Use Case 1: User Accessed Malware-Hosting Domain Detected in Proxy Logs

Question: A SIEM correlation rule triggered — a user accessed a known malware-hosting domain. How do you handle this?

Step 1: Validate the SIEM Alert

"As soon as the SIEM alert comes in, I check the log source — it's from the proxy server, in our case that's Zscaler. I open the alert and note the key details: the destination domain is marked *malicious* by our threat intel feed, and the action in the log says 'allowed', which is a concern."

- I copy down the **source IP**, **username**, **timestamp**, and the **URL**.
- I also note the **category** assigned by Zscaler — in this case, it shows 'Malware Sites'.
- First thing I check is whether this is **actually malicious**. I paste the domain into **VirusTotal** and **Talos Intelligence** — both show this is known for hosting malware.

📌 "Now I know this is not a false positive — it's a valid alert."

Step 2: Understand How the User Reached the Domain

"Next, I want to understand how the user landed on this domain."

- I go back to the proxy logs and look for the **referrer URL** — sometimes it shows if they clicked a link from another page or email.
- In this case, I see the referrer is from a **shortened link** (bit.ly/...), which could've come from a phishing email or social media.

📌 "This gives me context — it might be a phishing campaign or adware link."

Step 3: Check the User's Activity and Scope

"Now I pivot — I pull all proxy logs for that user in the last **30 minutes to 1 hour**."

- I look for:
    - Other suspicious domains

Dashrath Jamadar
Sr. Security Analyst at Rimini street india pvt ltd | ISC²-CC | CEH-V12 | SIEM | EDR |

- Multiple blocked attempts
- Signs of scripted traffic or automated access

"I also check if other users accessed the same domain — using the SIEM, I run a search for the same destination IP/domain across all proxy logs."

📌 "If more users accessed it, this may be a broader campaign."

Step 4: Check for Impact on the Endpoint

"I check the EDR (CrowdStrike in our environment) to see if there's any suspicious behavior on the user's machine around the time of access."

- I search by hostname or username.
- Look for:
  - Suspicious processes
  - Unknown executables
  - Connections to strange IPs

📌 "This tells me whether anything was downloaded or executed."

Step 5: Containment and Blocking

"Since the domain is confirmed malicious, I immediately take action:"

- I **block the domain** and its IP on the proxy/firewall.
- I check if it's part of a known malware campaign — if yes, I also block related IOCs.
- I reach out to the **user** and ask them if they noticed anything unusual or clicked anything.

📌 "If there's suspicion of infection, I inform the desktop team to isolate the device or perform a scan."

Step 6: Escalation and Documentation

- I create an **incident case** in our ticketing system.
- Add:
  - Alert summary from SIEM
  - Proxy log entries
  - Domain intelligence reports
  - EDR findings (if any)
  - Actions taken (block, notify, scan)
- I also inform the **Threat Intel** team to enrich the domain and look for related indicators.

📌 "This ensures we can use the intel in future detections."

Step 7: Post-Incident Improvement

- I work with the proxy policy team to ensure **newly registered or uncategorized domains are not allowed by default**.
- Suggest **alert tuning** — if similar domains are missed, we tweak the SIEM use case.

Dashrath Jamadar
Sr. Security Analyst at Rimini street india pvt ltd | ISC²-CC | CEH-V12 | SIEM | EDR |

- Share a **security bulletin** internally warning users about links from shortened URLs or suspicious redirects.

📌 "Every alert like this is a learning opportunity to tighten controls."

Use Case 2: Suspicious Data Exfiltration via Proxy Logs

Question: A SIEM alert triggers for potential data exfiltration — a user uploaded a large amount of data to an unknown external file-sharing website. Walk me through your investigation and response using proxy logs and related tools.

Step 1: SIEM Alert Validation

"As soon as I get the SIEM alert, I check the event details — it came from the proxy log (Zscaler) and flagged a high volume of outbound data to an unusual domain, something like fileshare-unknown.net."

- I check the **source IP, username, timestamp**, and **destination URL**.
- I note the **action** in the log: it says *POST allowed* with over **500 MB of data uploaded** in less than 2 minutes.

📌 "This kind of high-volume upload to an unclassified site is definitely suspicious."

Step 2: Look Deeper into Proxy Logs

"Now I dive into proxy logs manually. I pull the user's entire activity for the last 1 hour."

- I filter by action=POST, method=PUT, and large bytes_out.
- I also look for **repeat connections** to cloud storage or file transfer services like WeTransfer, Mega, or custom FTP/SFTP services.

📌 "This helps me confirm if it's an isolated upload or part of a broader data transfer pattern."

Step 3: Validate the External Site

"I check the destination domain with threat intel tools:"

- I use **VirusTotal**, **Talos**, and **AbuseIPDB** to check if the domain is flagged.
- Also verify whether the domain is **newly registered**, **uncategorized**, or **parked** (which is risky).

📌 "Even if it's not a known malicious domain, it's suspicious if it bypassed category filtering and is not business-related."

Step 4: Check the File Upload Type (If Available)

"If file metadata is captured in the proxy logs or headers, I try to extract details."

- Sometimes you'll see .zip, .csv, .txt, or even .bak files.
- I also check the **User-Agent string** — sometimes it's a browser, sometimes it's a custom script or CLI tool like curl.

📌 "Custom tools uploading sensitive data are a red flag."

Dashrath Jamadar
Sr. Security Analyst at Rimini street india pvt ltd | ISC²-CC | CEH-V12 | SIEM | EDR |

Step 5: Check Endpoint Activity

"I correlate the activity with EDR logs (CrowdStrike/SentinelOne):"

- Look for:
  - Files accessed or zipped
  - Script execution
  - Network activity matching the external domain
- If possible, I check **process-to-domain mapping**: which process initiated the connection?

📌 "If a script or tool ran, I flag it for possible insider threat or credential abuse."

Step 6: Containment Actions

"Based on the volume and destination, I start containment immediately:"

- I **block the domain** or IP in the proxy/firewall.
- Add the domain to the **blacklist** under 'Suspicious Uploads'.
- If the upload is ongoing, I ask the **network team** to terminate the session.
- Inform the **endpoint team** to isolate the host for forensic review.

📌 "I also reach out to the user to understand if this was a legitimate action — sometimes devs use personal services for testing, which still violates policy."

Step 7: Escalation and Reporting

- I open an incident ticket with **'Potential Data Exfiltration'** tag.
- Add:
  - Proxy logs (upload size, time, domain)
  - Threat intel results
  - EDR findings (process, file access, etc.)
  - User justification (if any)
- I escalate to **legal or HR** if sensitive files are involved or policy violation is confirmed.

📌 "This step is key for auditing and future legal hold if it's insider threat."

Step 8: Post-Incident Action and Awareness

- Work with the **proxy team** to:
  - Block uncategorized file-sharing services by default
  - Set thresholds on upload size alerts per user/session
- Update **SIEM use cases** to better correlate large uploads + unknown domains + rare destinations.
- Share awareness with the SOC team and notify **compliance** or **data protection** teams.

📌 "The goal is to prevent data loss and enhance behavioral detection for insiders."