Security Strategies: Data and Cloud Monitoring and Protection

Shruti Malik

ITEC5010 – Security & Enterprise Networks

September 7, 2025

Introduction

This report surveys practical tools and methods for monitoring and protecting enterprise networks across on-premises and cloud environments. It focuses on two widely used open-source platforms—pfSense for firewall/router monitoring and Wireshark for packet analysis—and compares them with other common options. The discussion then proposes selection criteria for network monitoring tools and designs a security policy that uses insights from firewall, router, and packet analysis to mitigate risk. Examples and guidance emphasize recent platform capabilities and cloud-native capture features to ensure applicability to modern hybrid architectures.

Analyzing Firewalls and Routers with pfSense

pfSense provides a rich set of built-in monitoring and troubleshooting features that make firewall and router analysis accessible without additional tools. Administrators can inspect the live state table to understand active connections, NAT translations, and session counts, which is essential for identifying asymmetric routing, exhausted states, or policy-routing side effects (Netgate, 2022a). The pfTop utility and States and States Summary views expose per-host and per-rule usage, protocol breakdowns, and top talkers, enabling quick detection of anomalies and rule mis-hits (Netgate, 2022b). For on-box packet inspection, the built-in Packet Capture GUI wraps tcpdump and allows targeted captures by interface, host, port, or protocol with rolling previews and downloadable PCAPs for offline analysis in Wireshark (Netgate, 2024a). pfSense also centralizes log review—firewall logs, DNS Resolver logs, DHCP leases, and VPN events—

while supporting remote syslog and add-on packages such as pfBlockerNG for reputation-based blocking and ntopng and Darkstat for bandwidth monitoring (Netgate, 2022c; Netgate, 2022d). When deeper threat detection is needed, pfSense supports IDS/IPS packages—Snort or Suricata—that can alert and, when configured inline, block traffic by signature, complemented by suppression lists and policy tuning to reduce false positives (Netgate, 2022e; Netgate, 2022f).

pfSense vs. Other Router/Firewall Analysis Tools

Why this matters in practice: pfSense is excellent for one-to-few sites, but it lacks a vendor-supplied, single-pane-of-glass controller to push policy, objects, and updates across hundreds of appliances. In large enterprises this turns into higher operational toil (manual configuration drift, slower incident response, and inconsistent auditing). Cisco FMC and FortiAnalyzer address these pain points with centralized device inventories, role-based admin, API/CLI driven bulk changes, scheduled policy deployments with pre-change validation, and compliance-ready reporting dashboards. They also aggregate and correlate logs/alerts from all edges, enrich with vendor threat intelligence (for example, Cisco Talos or FortiGuard), and support automated ticketing/SIEM forwarding—capabilities that materially reduce mean-time-to-detect (MTTD) and mean-time-to-respond (MTTR). The cost trade-off is clear: pfSense minimizes licensing, but enterprises often offset commercial licensing fees with lower administrative overhead, formal support/SLA, and tighter audit/compliance alignment in Cisco/Fortinet ecosystems.

OPNsense, a close relative of pfSense, offers comparable firewall monitoring with a modern UI and native reporting dashboards for traffic graphs and top talkers, plus integrated Suricata-based IPS and optional plugins like ntopng (OPNsense, n.d.-a; OPNsense, 2025). By contrast, enterprise platforms such as Cisco Secure Firewall Management Center (FMC) aggregate telemetry across managed devices, with dashboards for WAN health, application visibility, VPN topology, device inventory, and audit/syslog correlation—features designed for multi-site fleets and compliance reporting (Cisco Systems, 2025a; Cisco Systems, 2022). Fortinet's FortiAnalyzer similarly centralizes log analytics and reporting, adding integrations (for example, Fluentd log streaming) and enhancements for SD-WAN and OT insights to scale monitoring across large deployments (Fortinet, 2023; Fortinet, 2023b). In short, pfSense excels as a feature-rich, low-cost platform for single-edge or SME environments, while OPNsense offers a polished alternative with similar capabilities. For enterprises that require centralized governance, advanced reporting, and cross-device health monitoring, vendor controllers such as Cisco FMC or FortiAnalyzer are more appropriate.

Using Wireshark to Identify and Analyze Threats

Wireshark is the de facto standard for packet analysis, providing deep protocol dissectors, expert diagnostics, stream reassembly, and powerful display filters to isolate IOCs and root-cause performance or security issues (Wireshark Foundation, 2025a; Wireshark Foundation, 2025b). Analysts can pivot with Conversations and Endpoints views to find suspicious peers; use Protocol Hierarchy to surface unusual protocols; and rely on the Expert Information and TCP

Analysis flags to spot retransmissions, zero-window events, handshake failures, or malformed packets (Wireshark Foundation, 2025a). Modern releases extend display filter functions and custom columns, speeding up hunting workflows and facilitating repeatable analyses (Wireshark Foundation, 2025c).

Example: Troubleshooting DNS Timeouts with Wireshark

Scenario: Users intermittently experience name-resolution failures for an internal application.

Capture: We captured traffic on the client VLAN gateway (via SPAN/TAP or pfSense Packet Capture) and on the DNS server interface. Interpret: We established a time reference and used Conversations/Endpoints to identify the active client–server pairs and measure query-to-response latency. Filter: We applied display filters such as "(dns.flags.response == 0) || (dns.flags.rcode > 0)" to focus on queries and error responses. Inspect: Drilling into IP headers and ICMP messages revealed MTU mismatch (ICMP 'Fragmentation Needed') causing dropped UDP fragments. Fix: We lowered EDNS0 UDP payload size or enforced TCP fallback and standardized the WAN MTU. Outcome: Post-change captures showed complete query–response cycles with acceptable latency—directly aligning with the prompt's capture → interpret → filter → inspect workflow.

Packet Capture & Traffic Analysis: Wireshark vs. Alternatives

Wireshark (GUI) and TShark (CLI) excel at interactive, host-centric analysis and protocol dissection. For sensor-grade, continuous monitoring, Zeek focuses on protocol-aware metadata logs (for example, conn.log, dns.log, http.log) that enable scalable hunting and enrichment rather than full payload inspection (Zeek Project, 2024; Zeek Project, 2025). Suricata adds signature-

and rule-based IDS/IPS with JSON (EVE) output and performance features like rule grouping and capture-filter offload for high-throughput links (Open Information Security Foundation, 2024; OISF, 2024). For full-packet capture at scale, Arkime provides distributed capture, indexing, and search across PCAPs, complementing tools like Wireshark for deep dives (Arkime, 2024). In cloud environments, native services such as AWS VPC Traffic Mirroring, Azure Network Watcher Packet Capture, and Google Cloud Packet Mirroring export traffic for analysis with your preferred tools, ensuring coverage across hybrid networks (Amazon Web Services, 2024a; Microsoft, 2025; Google Cloud, 2025; Amazon Web Services, 2024b). Together these options cover ad-hoc troubleshooting (Wireshark/TShark), metadata-first detection (Zeek), signature-based prevention (Suricata), forensic recall (Arkime), and cloud telemetry.

Organizational Advantages of Packet Capture Tools

Packet capture capabilities deliver compounding benefits across network management, security, and troubleshooting: (1) Faster mean-time-to-resolution (MTTR) by isolating root causes at the packet layer—translating to reduced outage costs and better customer satisfaction; (2) Objective verification of firewall/NAT/ACL behavior—critical for audit evidence and for proving a policy works as intended; (3) Threat detection/response via signatures, anomaly hunting, and IOC validation—allowing teams to confirm or dismiss alerts quickly; (4) Performance baselining to spot regressions before they become incidents; and (5) Forensics and compliance support

through durable, time-aligned evidence. These benefits reinforce CIS Control 13's emphasis on comprehensive monitoring and reliable telemetry as foundations for resilience.

Selecting a Network Monitoring Tool: Criteria and Rationale

• Coverage & Visibility: Supports on-prem and multi-cloud, required protocols, and encrypted-traffic strategies. Why it matters: Gaps create blind spots that adversaries exploit and make incident scoping unreliable.

• Scalability & Performance: Handles expected throughput/retention and distributed capture. Why it matters: Tools that can't keep up will drop packets and miss alerts, eroding trust in telemetry.

• Detection & Analytics: IDS/IPS, behavioral analytics, ATT&CK mappings, and flexible filtering/scripting. Why it matters: Rich analytics shorten investigations and reduce false positives, improving MTTR.

• Integration & Ecosystem: Syslog/JSON exports, SIEM/SOAR connectors, cloud mirroring (AWS, Azure, GCP). Why it matters: Seamless data flow enables automation, case management, and end-to-end visibility.

• Usability & Skill Fit: Intuitive UI plus automation/CLI; strong docs/training. Why it matters: Tools that require niche skills become shelf-ware and lead to missed threats.

• Security & Compliance: RBAC, tamper-evident logging, privacy controls, and clear retention policies. Why it matters: Minimizes legal exposure and audit findings while protecting sensitive payloads.

• Cost & Licensing: Account for storage (especially PCAP) and support. Why it matters: Under-estimating storage or support leads to surprise costs or unsafe retention cuts.

Security Policy Informed by Firewall, Router, and Packet Analysis

Purpose: Establish a monitoring-driven defense for hybrid networks that uses firewall/router telemetry and packet analysis to detect, contain, and remediate threats while respecting privacy and compliance.

Scope: Applies to all network segments, data centers, branch offices, and cloud VPCs/VNETs connected to the enterprise network.

1) Telemetry & Data Collection

• Firewalls/Routers: Enable detailed firewall logs, state/NAT logs, DNS resolver logs, and VPN events. Forward to a central log platform. Maintain pfSense packages (for example, IDS/IPS, ntopng) as needed.

• Packet Capture: Deploy tiered capture—on-demand PCAP at edges (pfSense Packet Capture), continuous metadata (Zeek) for all segments, targeted full-packet capture (Arkime) on critical chokepoints.

• Cloud: Use AWS VPC Traffic Mirroring, Azure Network Watcher, and GCP Packet Mirroring to export traffic from workloads to approved sensors.

2) Detection & Triage

• Signatures & Metadata: Run Suricata IDS/IPS with tuned rules and suppression. Ingest Zeek logs for behavior analytics (DNS tunneling, unusual user-agents, beaconing). • Threat Hunting: Use Wireshark/TShark for deep dives on priority incidents with standard display-filter playbooks (for example, TLS handshake failures, suspicious DNS, SMB anomalies). • Alert Routing: Integrate with SIEM/SOAR; define severity-based SLAs and escalation paths.

3) Response

• Containment: Automate block/deny actions via firewall APIs (for example, pfSense tables for dynamic blocks) and NAC where feasible. • Forensics: Preserve PCAPs and related logs with chain-of-custody; capture memory/disk as required by incident-response procedures.

4) Privacy, Legal, and Retention

• Limit payload capture by default; prefer metadata except during an approved investigation. • Define retention periods (for example, Zeek logs 180 days; full PCAP 7–30 days on critical links) aligned with regulation and storage budgets. • Access control: RBAC, least privilege, and audit trails for all query/download operations.

5) Governance & Continuous Improvement

• Metrics: MTTD/MTTR, false-positive rate, packet loss on sensors, coverage of critical segments. • Reviews: Quarterly rule and pipeline tuning; post-incident lessons learned;

validation against CIS Controls and cloud-security best practices.

Systematic Risk Mitigation: This policy translates observed network behavior into prioritized controls—blocking known bad, baselining normal traffic, and instrumenting the environment so that anomalies are quickly detectable and investigable. Packet-level evidence drives confident decisions, reduces downtime, and creates durable feedback loops to harden controls over time.

Additional Telemetry: In addition to packet-level data, enable flow telemetry (NetFlow/sFlow or cloud flow logs such as AWS VPC Flow Logs, Azure NSG Flow Logs, and Google VPC Flow Logs) to provide scalable, low-overhead coverage of all segments. Use flows for baselining and anomaly detection and pivot to PCAP only when needed.

Worked Example – Port Scan → SSH Brute Force: Detection: Zeek flags high-fan-out connection attempts; Suricata raises ‘ET SCAN NMAP’ then ‘ET POLICY Possible SSH Brute-Force’; pfSense firewall logs show repeated denies to tcp/22. Triage: Pivot to Wireshark/TShark on an edge capture using filters like “tcp.port == 22 && tcp.flags.syn == 1” to verify rate/source distribution; use flow logs to confirm volume and path. Response: SOAR playbook adds offending IPs to a dynamic blocklist (pfSense tables) and hardens SSH (restrict to VPN, enforce MFA on bastions, consider port-knocking). Lessons: Tune Suricata thresholds, add Zeek notices for scan heuristics, and validate that blocks propagate via API across all edges.

Conclusion

Effective network defense depends on visibility. pfSense offers granular, low-cost firewall and router analytics suitable for many environments, while Wireshark provides unmatched depth for packet-level investigation. Combined with scalable platforms—Zeek, Suricata, Arkime—and cloud-native mirroring and capture, organizations can achieve comprehensive coverage across hybrid networks. Applying clear selection criteria and a monitoring-driven security policy ensures that telemetry is actionable, privacy-aware, and aligned with recognized controls, improving both security outcomes and operational efficiency.

References

Amazon Web Services. (2024). Work with open-source tools for traffic mirroring. https://docs.aws.amazon.com/vpc/latest/mirroring/tm-example-open-source.html

Amazon Web Services. (2024). What is Traffic Mirroring? https://docs.aws.amazon.com/vpc/latest/mirroring/what-is-traffic-mirroring.html

Amazon Web Services. (2025). Logging IP traffic using VPC Flow Logs. https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

Arkime. (n.d.). Arkime – Open-source full packet capture. (Accessed September 3, 2025). https://arkime.com/

Center for Internet Security. (2024, June 24). CIS Critical Security Controls v8.1. https://www.cisecurity.org/insights/white-papers/cis-critical-security-controls-v8-1

Cisco Systems. (2025, June 18). Cisco Secure Firewall Management Center Administration Guide, 7.6. https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/760/management-center-admin-76.html

Fortinet. (2024, July 11). FortiAnalyzer 7.4.1 Administration Guide. https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/ef4bde1e-412e-11ee-8e6d-fa163e15d75b/FortiAnalyzer-7.4.1-Administration_Guide.pdf

Google Cloud. (2025, August 29). VPC Flow Logs. https://cloud.google.com/vpc/docs/flow-logs

Google Cloud. (2025). Packet Mirroring. https://cloud.google.com/vpc/docs/packet-mirroring

Microsoft. (2025, March 21). Manage packet captures – Azure Network Watcher. https://learn.microsoft.com/azure/network-watcher/packet-capture-manage

Microsoft. (2025, May 19). NSG Flow Logs overview – Azure Network Watcher. https://learn.microsoft.com/azure/network-watcher/nsg-flow-logs-overview

Netgate. (2024). Packet Capture GUI. https://docs.netgate.com/pfsense/en/latest/diagnostics/packetcapture/webgui.html

Netgate. (2022). Firewall States. https://docs.netgate.com/pfsense/en/latest/monitoring/status/firewall-states.html

Netgate. (2022). pfTop. https://docs.netgate.com/pfsense/en/latest/monitoring/status/pftop.html

OPNsense. (n.d.). Reporting: Traffic. (Accessed September 3, 2025). https://docs.opnsense.org/manual/reporting_traffic.html

Open Information Security Foundation. (2024, July 2). Suricata Engine’s 20x performance upgrade on rule grouping. https://suricata.io/2024/07/02/suricata-engines-20x-performance-upgrade-on-rule-grouping/

Open Information Security Foundation. (2025). Eve JSON Output.

https://docs.suricata.io/en/latest/output/eve/eve-json-output.html

Wireshark Foundation. (n.d.). Wireshark User's Guide – Expert Information & TCP Analysis.

(Accessed September 3, 2025). https://www.wireshark.org/docs/wsug_html_chunked/

Zeek Project. (n.d.). Logs — Book of Zeek. (Accessed September 3, 2025).

https://docs.zeek.org/en/master/logs/index.html