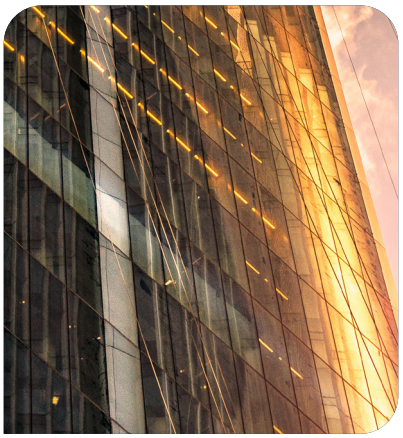
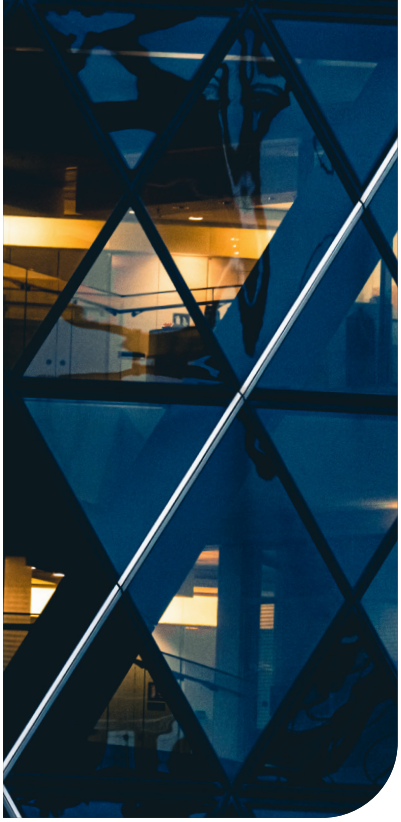
Firewall Logging:
Have you seen enough?

RelianceCyber

THOUGHT LEADERSHIP E-BOOK SERIES





Firewall Logging:
Have you seen enough?

INTRODUCTION

In the context of network security, firewalls provide a critical policing point between network segments, or between internal networks and external threats. While Zero Trust models have expanded the concept of traditional firewalling, it is still at its core one of the fundamental Cyber Security controls.

Modern cloud models, ZTNA, on-premises datacentres, web proxies, and WAFs, ultimately still utilise elements of traffic policing, packet inspection and threat detection. A well-defined policy is crucial to protect organisations' assets and information security.

However, the effectiveness of firewalling is often focused on the ability to control traffic based on the enforcement of identity, access control, and threat detection. Logging and alerting are often lacking in depth and application. A medium sized organisation can produce on average 20-30 GB of logging data per day, with millions of logs generated and stored for a given retention period.

This paper explores the importance of well-defined logging and alerting in the context of Cyber Security, and how to achieve better visibility into potential security issues proactively to enhance the organisation's security posture.

Why do we log traffic?

The need to log traffic generally stems from one or more of the following key drivers:

- Operational – allowing system administrators to check historic logs for troubleshooting or analysis purposes.
- Compliance – satisfying regulatory requirements for frameworks such as DORA, PCI-DSS, GDPR, FOI, and HIPAA.
- Security – integration with other security platforms such as a SIEM, for advanced log correlation, analysis, and proactive security management.

Operationally, logging of traffic plays a big role in the continuous development of network security. Organisations embarking on a Zero Trust journey must first understand what assets exist across their environment and what traffic is being sent from/between those assets. Similarly, the process of network segmentation often starts with understanding existing traffic flows, which relies heavily on analysis of historic traffic logs.

From a compliance perspective, organisations often need to adhere to certain policies and guidelines depending on the industry in which they operate. For example, articles 12 and 23 of the Digital Operational Resilience Act (DORA) cover elements of logging and their application as part of the wider security analytics and alerting. Requirement 10 of the Payment Card Industry Data Security Standard (PCI-DSS) leans heavily on the need to maintain audit logs for a requisite retention period. Failure to comply with such regulations introduces risk of non-compliance, leading to potential fines and/or reputational damage.

Finally, many organisations have adopted a multi-layer, proactive approach to security. A well-configured security platform should be seen as one layer rather than a complete barrier to threats. Complex attack surfaces, advanced persistent threats, and various entry points into networks mean that most organisations will suffer some sort of compromise. The ability to detect and act on threats proactively is of utmost importance. Security Information and Event Management (SIEM) platforms provide an invaluable resource for handling masses of data and dynamically acting on suspicious traffic.

Logging fine tuning

A busy security device can generate huge amounts of logs on a daily basis. Factors such as industry regulations, available log storage, and compute cost, feed into decisions on what traffic or events should be logged and to what level of detail. All too often, organisations pay little attention to this aspect of security deployments, leading to either too little or too much logging.

There is a vital balance to be met. Logging all traffic and events can lead to an overwhelming amount of data which is operationally challenging, in addition to inherent cost considerations. Conversely, by not logging certain traffic, organisations introduce the risk of threats being undetected, as well as hindering operational troubleshooting. In the event of a security breach or suspected attack, detailed firewall logs are indispensable for forensic investigations. They provide the raw data needed to trace the path of an attacker, understand how they gained access, and assess the extent of the damage.

Addressing this balance should start with analysis of the security platform and policy configuration. Various vendors offer different levels of granularity regarding logging, but generally allow for filtering of certain security events or traffic types, in addition to manipulating the level of verbosity. Some common approaches taken in log tuning are shown below:

- Policy rules split into multiple entities for targeted logging levels
- Ensure high risk traffic flows have full logging enabled (e.g. Internet exposed services)
- Disable logging for internal well-known services such as NetBios
- Email alerts for important but infrequent operational events
- Apply custom filters for log export to SIEM platform

At a fundamental level there are other considerations when deploying logging. Transit paths between the security platform and log server must be examined to understand the risk of sensitive logs being intercepted. Log traffic can be secured using certificates if appropriate, making use of TLS between the endpoints for server or mutual authentication as required. Reliable logging can be configured by making use of syslog over TCP rather than UDP, providing assurance that all logs destined for the server have been received.

Log format must be considered to ensure the server is able to digest and present the data on demand. The rate at which logs are sent may also be a factor which needs to be fine tuned to suit the environment.

There are also various nuances introduced across different platforms. For example, an interesting but often unknown aspect of Cisco ASA firewall logging is seen when configuring the service to utilise TCP as opposed to UDP. Cisco deployed this feature to automatically block all new traffic connections if the TCP connection to the log server is down or can not be established. This creates the potential for an unintended denial of service due to transient or permanent connectivity issues to the log server, but there is a configuration command which overrides the feature.

By approaching logging as a policy refinement exercise, organisations can ensure appropriate diligence as part of the wider cyber security cycle, rather than realising retrospectively that vital logs are missing for analysis and introducing unwanted risk to the environment.

Integration with SIEM Systems

Integrating firewall logs into a SIEM system enhances an organisation's ability to detect, correlate, and automatically respond to security events. Aggregated log data from various security devices, servers, and endpoints, provide a centralised view from which threat monitoring and analysis can take place.

This provides a powerful solution to the problem of "what to do with all those logs". Having a platform which can monitor incoming logs in real time, apply defined logic workflows, allow intelligent queries across the dataset, and automate responses to suspected threats, immediately provides incredible value to the organisation's technical investment. Rather than viewing security platform logs as individual sets of data, the SIEM effectively connects related data to build a picture of what is happening on the network, potential entry points, attack vectors utilised and subsequent compromise. Coupled with AI based machine learning techniques, this makes modern SIEM platforms a must-have for organisations serious about protecting their cyber security posture.

Traditionally, utilising a security platform's logs to analyse potential breaches is often an activity which is performed as a postmortem exercise. SIEM platforms are addressing this as a real time function based on threat detection rules and playbooks. Security Orchestration, Automation and Response (SOAR) utilises automation rules to dynamically apply security controls based on triggers being detected, allowing endpoints to be locked down before further potentially malicious activity can take place. The time to react to security incidents therefore is drastically reduced, in addition to significantly reducing the attack surface in a dynamic way.

By feeding firewall logs into a SIEM system, organisations can benefit from a more comprehensive and proactive approach to threat detection. The prior issue of processing millions of logs / events and being able to act on those of interest, is solved. Analysts can focus on high priority incidents detected by well-defined SIEM rules, and due to automation, the organisation is assured that critical security events are less likely to be missed.

Importance of alerting

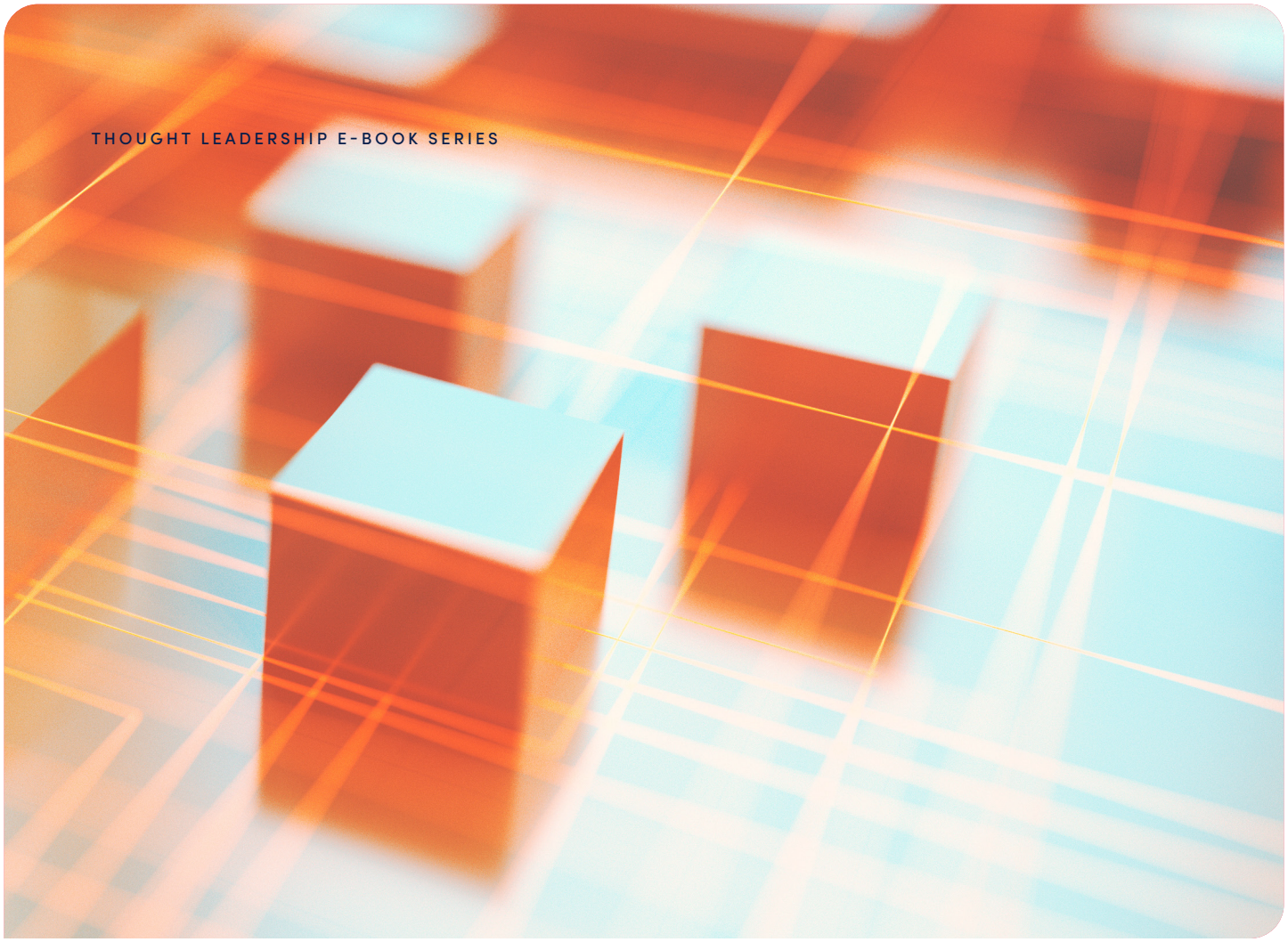
Effective alerting is an essential component of security operations. While logging traffic is crucial for detection and forensic purposes, alerting provides the necessary mechanism for real-time response. When a security event is logged, an alert can be triggered based on predefined thresholds or detected patterns of malicious activity.

The same is true for non-malicious activity which can still introduce risk to the environment. How many people reading this whitepaper have experienced a service outage due to an expired certificate or license? One part of the battle is ensuring important security or operational events are being logged, but without this log either triggering an automation flow or alerting an engineer, the value is potentially lost.

Most security platforms come with pre-defined out-of-the-box alerts which may or may not be applicable or of use in each organisation's deployment. It is vital to consider the scenarios which are relevant and assess when / how these events will be acted upon.

Feeding into the theme discussed throughout this paper, security platforms generating logs for events such as threat detection, denial of service, or indeed operational events such as certificate expiry, may not be doing anything other than storing the event to a long list of logs, only visible if an engineer happens to search for it specifically. By the time this happens it may be too late to act upon in a proactive manner.

Organisations should decide how various alerts should be handled accordingly. For example, operational events such as upcoming certificate expiry may be configured to email the engineering team whereas a spike in threat logs on the security device can be configured to trigger a detection rule on the SIEM. The faster a security team can identify and respond to a potential threat, the more likely they are to mitigate potential damage. Real-time alerts based on firewall traffic logs enable security teams to immediately investigate suspicious activity and take appropriate action, such as blocking an IP address or isolating affected systems.

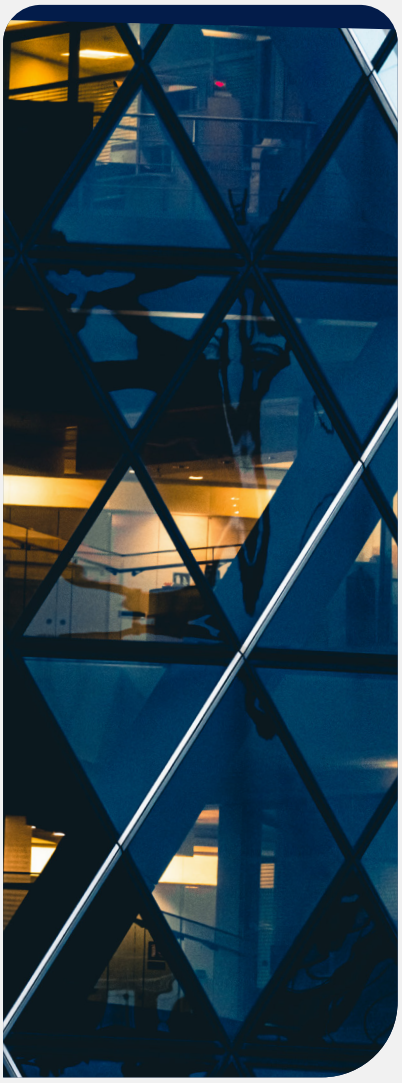


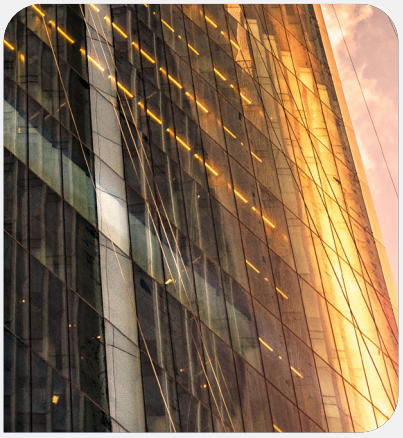
Conclusion

In an era of increasing cyber threats, logging security platform traffic is a critical component of a robust security strategy. The collection and analysis of security logs provides valuable visibility into network activity but should only be seen as the root in a multi-layer structure. Integrating with SIEM systems vastly improves cyber security posture by providing enhanced threat detection, correlation, and automated response capabilities, enabling early detection of security incidents to mitigate risks and strengthening an organisation's security posture. Ultimately there is no 'one-size-fits-all' and organisations need to address logging and alerting with as much diligence as they would afford the platform's underlying security and threat policies.

Get in touch with our experts

+44 (0)845 519 2946
contact@reliancecyber.com
reliancecyber.com





Firewall Logging:
Have you seen enough?

Explore the leadership series

RelianceCyber

reliancecyber.com