Advanced Cloud Firewall Solution CyberRisk Validation Methodology

Version:	1.6
Last Revision:	29 March, 2023
Language:	English

www.secureiqlab.com

AMTSO Standard Compliance Statement

This Test has been designed to comply with the Anti-Malware Testing Standards Organization, Inc. ("AMTSO") Testing Protocol Standard for the Testing of Anti-Malware Solutions, Version [1.3] (the "Standard"). This Test Plan has been prepared using the AMTSO Test Plan Template and Usage Directions, Version [2.4]. SecureIQLab is solely responsible for the content of this Test Plan.

Content

1 INTRODUCTION

The Next Generation Firewall (NGFW) is one of the most ubiquitous security tools in use today with 30% of companies having more than 100 firewalls set up on their network and 60% of companies deploying firewalls in the cloud (Firemon 2019). The Next Generation Firewall Market was valued at USD 2.80 billion in 2020. (Mordor Intelligence 2021). The global Next Generation Firewall (NGFW) market is estimated to reach CAGR 10.8%. Driven by this, the market valuation is set to reach USD 7.97 Billion in 2028. (360 Research Reports 2022).

The NGFW market growth is driven by an increase in attack surface, changes in hacker strategy and more advanced threats. The move to the cloud by many organizations and the surge in IoT devices has expanded attack surfaces. Hackers have historically been noisy and opportunistic, focusing on server-side vulnerabilities. As a consequence, traditional firewalls focused on blocking IP addresses, ports and protocols. But the threat landscape has changed. Today, attackers that once targeted enterprise servers now realize that it is far easier to exploit client machines. Lastly, advanced attack tools are more prevalent.

A new approach to network security is required to counter the emergence of advanced attack vectors, attack strategies and new attack surfaces. This approach must be designed to thwart complex and customized threats. As firewalls evolved to protect against more advanced threats, they naturally moved up the stack. In addition to being “Layer 7 aware” they added capabilities to inspect packet content and search for Indicators of Attack (IOA) within the data stream. As attacks become more complex, detection capabilities with low signal to noise ratio become increasingly important.

Defending against these more complex attack methods requires a new generation of firewall that can also mitigate application-based attacks. As adversaries move up the protocol stack, security devices need to follow suit to be effective. Analysts and their managers, through awareness of their applications and their data, can better examine their traffic and increase overall security. This is the bases of an Advanced Cloud Firewall. More specifically, an **Advanced Cloud Firewall (ACFW)** must be able to:

- Identify permitted applications and block prohibited applications
- Identify and block threats that try to use “known good” ports and protocols
- Identify and block threats that try to use evasive tactics such as non-standard ports or “port hopping”
- Identify and block threats that are encrypted with SSL/TLS
- Identify users, groups and locations and apply policy regardless of IP address
- Identify and block outbound data leaks
- Identify and block outbound botnet command and control communications
- Enable secure business workflow with high detection rate and low signal to noise ratio
- Provide global visibility and granular policy management
- Provide all necessary alerts and configuration recommendations based on best practices

Though many advanced firewalls claim they can properly inspect traffic, not all offer equal protection. Also, Firewalls are not equally able to scale, integrate into security stacks and detect advancements in attack methodologies. This means that IT security staff must carefully test potential solutions before recommending a purchase or renewal. This methodology offers advice on what to expect from a next-generation firewall, features and business needs to consider, and a test methodology for IT and business professionals to use to enhance their investments in security through enhanced firewall capabilities.

2 Objective of this Advanced Cloud Firewall Methodology

This test focuses on three criteria: Security, compliance, and operational capabilities. The criteria were selected with the objective of creating test results that demonstrate the tested product‘s ability to prevent attacks and to quickly resolve incidents.

One industry standard the tests are based on is the MITRE ATT&CK framework. The MITRE ATT&CK framework is a knowledgebase of attack tactics and techniques. This framework is an excellent tool for mapping out tactics, techniques, and procedures (TTPs). The MITRE ATT&CK framework is threat-centric in nature and thus doesn't address all the use cases, various enterprise workflows in different scenarios, or product differentiating factors. It is also slow in adapting to emerging attacks that are evolving in the wild. It lacks a composite scoring mechanism to easily highlight strengths and weaknesses of tested products. Almost every methodology created by other testing firms are also threat-centric in nature. Enterprises struggle to generate actionable strategies from threat-centric tests in order to reduce their true operational risk. In order to help enterprises gain actionable information towards lowering risk, this test incorporates another industry standard, the attacker centric 'Cyber Kill Chain Model". The Cyber Kill Chain Model is useful because it provides a defense model perspective. Combining the MITRE ATT&CK framework with the Cyber Kill Chain Model draws from each of the strengths of these industry standards to effectively measure a product‘s attack prevention capabilities to reduce operational risk.

SecureIQLab has developed an industry-changing paradigm shift towards defining Advanced Cloud Firewalls according to the everyday reality of enterprise use cases and workflows.

2.1 Prevention

The best way to respond to any threat is by preventing it. This is fundamentally the prevention capability of the Advanced Cloud Firewall product. SecureIQLab defines *prevention* as an automated, active response that kicks in 24/7, 365 days a year, without the need for human intervention.

This can be done through a multitude of technologies and mechanisms, for example: Signature-based models, policy-based models, behavior-based models, and ML-based models. This definition is technology-agnostic because it focuses on the *outcomes* of the various analyst workflows and scenarios, rather than the technology used to prevent it.

Advanced Cloud Firewalls are expected to prevent initial and ongoing attacks, without having to triage the threats and while offering reporting capabilities.

2.2 Advanced Cloud Firewall Inclusion Criteria, Setup and Configuration

Vendors with appropriate enterprise firewall products are invited to join this test. Tested firewalls will be in a standalone mode, with each vendor invited to participate in the initial setup, configuration, and baselining aspects. SecureIQLab has compiled a list of popular scenarios requested by enterprises.

Every vendor will be allowed to configure their own product, or review the configuration of their product, to ensure that the deployment aligns with their default configuration that businesses are able to implement when deploying the firewall in their organizations. The firewall configurations will include multiple security and compliance applications—URL filtering, anti-malware, advanced threat protection, vulnerability protection, firewall policy enforcement, data loss prevention and cloud application security.

If there are workflows mentioned in this methodology that require specific configuration changes and/or options, vendors are responsible to provide publicly available documentation of these best practices. If there are any concerns with certain workflows, it is best that the respective vendor discusses these with SecureIQLab, and work with us on these options during the initial setup and baselining phase.

Because this methodology is tailored towards the prevention and reporting capabilities for security and compliance, all vendors are advised to turn on the prevention and protection capabilities (ability to block), so that it emulates the real-world enterprise-class capabilities of these products. Test subject products will be configured with default configuration. Test subject products with default modes enabled as "detect" will be set to "protect" or "block", in order to emulate real-world conditions. Any required tuning will be performed as per publicly available best practices provided by the vendor.

This methodology supports product updates and configuration changes made by a central management console or on-prem device portal. Our intention is to go through and execute all test scenarios from beginning to end, to the greatest extent possible.

2.3 Deployment Overview

Deployment complexity is always a consideration for an enterprise due to labor costs and the "opportunity costs" of dedicating technical and management resources to setting up and maintaining security systems.

Given the nature of test environments, some tuning may be required. Participating vendors are invited to review ACFW deployment to align with default and publicly recommended configurations. Test subject vendors will be configured per default configuration and use publicly available recommendations if any additional tuning is required for test harness compatibility.

The Advanced Cloud Firewall Methodology can include a virtual or a cloud service solution.

2.3.1 Cloud Deployment

An Advanced Cloud Firewall system requires little effort in terms of deployment, with no hardware or software involved. An administrator simply has to set up either a Generic Routing Encapsulation (GRE) tunnel or IPsec VPN tunnel to connect the traffic from the network to the cloud portal.

- Deployed using a VPN tunnel if required – Specifically, IPsec VPN tunneling using the pre-shared key for authentication. One could potentially forward all traffic destined for any port to the Advanced Cloud Firewall vendor.
- The deployment would emulate an in-line deployment model.
- The VPN tunneling provides visibility into the internal IP addresses, used for security policy and logging by the vendor.
- Protection typically includes control of:
    - Firewall, DNS, mobile applications, file types, URL and cloud applications, browsers, bandwidth and FTP.
    - Configured to provide protection against malware, mobile malware, advanced threats, APTs, and data loss. Decryption and inspection of SSL traffic was also activated.

2.3.2 Virtual Deployment

- Virtual product and Firewall as a Service (FWaaS) vendors can be deployed in-line, in between the router and the client system.

- Protection typically includes control of: Antimalware, endpoint control, application control, data loss protection, web filter and intrusion prevention.

2.3.3 Optional Endpoint Deployment

In order to protect the modern workforce, the convergence of firewall and endpoint solutions has prompted SecureIQLab to take an innovative holistic approach by examining the cybersecurity ecosystem. As a result, this test iteration offers cybersecurity vendors the option to deploy an endpoint-based solution to complement their ACFW solution, if required.

- The cost for the endpoint-based solution will be included in the total cost.
- Metrics for each validated technology implementation will be specifically reported.
- The CyberRisk Ripple implementation WILL include the complete vendor solution set (with the total cost of ownership) represented in this case and not just the ACFW metrics alone.

2.4 Common Cloud firewall Threat Categories

Advanced Cloud firewalls should be designed to protect cloud-based resources and applications from unauthorized access and common cyber threats. They typically use a variety of security measures to detect and prevent different types of common threat categories.

- **Application-based Threats:**

  These include attacks that target web applications and services, such as the following:

  a. **Cross-Site Scripting (XSS) Attacks:** Cloud-based XSS attacks are like traditional XSS attacks but may take advantage of the unique characteristics of cloud-based environments. For example, cloud-based web applications may rely on third-party services or resources that are vulnerable to XSS attacks, such as content delivery networks or advertising networks. Attackers can exploit these vulnerabilities to inject malicious code into a web page or resource that is then served to the user.

  b. **Malicious URL Attacks**: Cloud-based malicious URL-based attacks can be particularly dangerous because cloud-based systems often rely on web-based interfaces and services that can be accessed via URLs. For example, an attacker may create a fake login page that appears to be hosted by a cloud-based service, such as an email or document sharing service, and then trick the user into providing their login credentials.

  c. **SQL Injection Attacks:** Cloud-based SQL injection attack on a cloud firewall is when the attacker attempts to inject malicious SQL statements into the firewall's database or a database protected by it, to bypass security controls or gain unauthorized access to the firewall. For example, the attacker may attempt to inject SQL statements that trick the firewall into allowing access to restricted resources or opening vulnerabilities in the firewall's configuration or the database configuration with sensitive data.

  d. **Buffer Overflow Attacks:** In a cloud-based buffer overflow attack, the attacker may attempt to exploit vulnerabilities in cloud-based systems, such as cloud servers or applications, by overflowing buffers in the system's memory. The attacker may use a variety of techniques to carry out the attack, such as manipulating input fields or sending specially crafted packets.

- **Malware & Botnets:**

These include threats such as viruses, Trojans, and worms that can infect cloud-based systems and devices. Botnets are networks of infected devices that are controlled by a central command-and-control server and used to carry out malicious activities, such as spamming and DDoS attacks.

a. **Malware download over HTTPS:** A malicious file will be sent through an already connected HTTPS session. This test checks to see if the security solution blocks malware encrypted via SSL.
b. **Compressed Malicious Files:** Compressed malicious files are files that have been compressed or archived in a way that conceals their malicious content. Malware authors often use compression techniques to reduce the size of their malware files and make them more difficult to detect by security software. Unzipping takes computational power that can slow traffic down, so many security systems skip analyzing files zipped multiple times. Some examples are Zip files, 7z files, RAR files, Tarballs and very many other types.
c. **Botnets:** Cloud-based botnet attacks are a type of cyber-attack in which a botnet, which is a network of compromised devices, is controlled through a cloud-based command and control (C&C) server. Cloud-based botnets are particularly dangerous because they can be easily scaled and are difficult to track and take down. The attacker can quickly spin up or down cloud instances to control the botnet, making it more difficult to trace and shut down. In this type of attack, the attacker uses the cloud infrastructure to remotely control a botnet, which can then be used to carry out a range of malicious activities, such as distributed denial of service (DDoS) attacks, phishing attacks, or spam campaigns.

- **Browser-based Threats:**

In a browser-based cloud attack, the attacker may attempt to exploit vulnerabilities in a user's web browser to gain access to their cloud account or data. Alternatively, the attacker may target vulnerabilities in a cloud-based application, such as a web-based email client or file-sharing service, to gain access to sensitive data stored in the cloud. Some of the common browser-based threats are as follows,

a. **Browser Exploits**: Type of cyber-attack that targets vulnerabilities in web browsers or browser plugins to gain unauthorized access to a user's system or data. In a browser exploit attack, the attacker may use a malicious website, advertisement, or email to exploit a vulnerability in the browser or a browser plugin, such as Adobe Flash or Java, to install malware or gain unauthorized access to the victim's system.
b. **Cookie Stealing:** Cookie theft is the primary method used to steal personal information such as logins. Different methods of script injection are utilized to accomplish this; specifically, Adobe Flash employed on common, trusted sites (e.g., YouTube or eBay).
c. **Browser version and Plugin-in Control**: Browsers that are not updated with the latest versions, or have missing patches, can entice hackers to exploit these vulnerabilities and infect a user’s computer. Third party plug-ins are also risky and open more vulnerabilities.
d. **Obfuscated JavaScript:** Obfuscated code is when either the entire code, or a piece of it, is masked to hide the true intent of the code. Obfuscation itself is not necessarily malicious, but when its intent is to hide malicious content, it requires detection.

- **Data Loss and Leakage:**

These include threats that target sensitive data stored in the cloud, such as theft, data breaches, and insider threats.

a. **Phishing Site-based Attacks:** Attackers create fake websites that look like legitimate ones and trick users into entering their login credentials or personal information, to steal corporate credentials or sensitive personal data.
b. **Malvertising:** Adware is software supported by advertisements. Malicious code is injected into legitimate advertisements displayed on a website. These ads will automatically infiltrate sites to generate revenue for the author.
c. **Water hole Attacks:** Attackers compromise a legitimate website that is frequently visited by the target group and inject malicious code to exploit vulnerabilities in their browsers.

2.5 Advanced Cloud Firewall Real-World Cloud Performance

Cloud firewall performance refers to the ability of a cloud-based firewall to filter incoming and outgoing network traffic efficiently and effectively. The performance of a cloud firewall is determined by its ability to accurately identify and block unwanted traffic while allowing legitimate traffic to pass through unimpeded. SecureIQLab is taking a new approach towards defining the firewall metrics and workflows mapping key capabilities and workflows of the Advanced Cloud Firewalls to enterprise use-cases subjected under real-world traffic. In other words, the security efficacy of the firewall in terms of threats and the operational efficiency in terms of its ability to perform under normal enterprise operations. Some Common factors that can impact cloud firewall performance include the cloud firewall's processing power, the amount of traffic it needs to process, the complexity of the firewall rules and policies, and the cloud architecture and the supported infrastructure that the firewall is operating on.

"Actual enterprise production networks handle thousands of applications, traffic types, and access privileges. To accurately test any advanced firewall, the traffic mix must be as comprehensive and substantive as possible."[1] Test traffic will, where relevant, use mixed traffic that is based on NetSecOPEN's Project *One*, *Testing Using a Real-World Traffic Mix.*

Ultimately, a cloud firewall's performance is critical for maintaining network security and ensuring that business operations run smoothly. It is important to carefully evaluate firewall performance when selecting a cloud-based solution to ensure that it meets your organization's specific needs and requirements.

SecureIQLab believes that the final Advanced Cloud Firewall's security resiliency rating should be a combination of security efficacy along with key operational and cloud-based performance metrics based on a real-world scenario. To this effect, performance evaluation on the firewall will include the following verticals which will include both encrypted and unencrypted traffic.

2.5.1 Performance Traffic Mix Vertical Overview

1. **Enterprise Cloud-based Traffic Mix:** Enterprises primarily use cloud-based services, including cloud storage, computing, and networking. Cloud traffic within this vertical includes the transmission of data between data centers, cloud-based applications, and end-users.

[1] https://www.netsecopen.org/programs
SecureIQLab is an official member of NetSecOPEN

2. **Small-to-Medium Businesses Cloud-based Traffic Mix:** Small-to-medium businesses (SMBs) are increasingly using cloud-based services to reduce costs, increase efficiency, and improve their operations using Data Storage, Data Backup and recovery, collaboration tools, CRM, Accounting and financial mgmt. and E-Commerce.

3. **Remote Office Branch Office (ROBO) Cloud-based Traffic Mix:** With the increasing adoption of cloud-based services and applications, more and more data and workloads are being moved to the cloud. This trend is particularly prevalent in ROBO environments. the percentage of cloud traffic in a typical ROBO environment is expected to grow from around 25% in 2021 to more than 50% by 2024. This growth is being driven by the increasing adoption of cloud-based applications and services, such as collaboration tools, Videoconferencing, file sharing, software-as-a-service (SaaS) applications and most importantly connectivity between ROBO and primary data centers, HQ's and other cloud related services.

4. **Healthcare Organization Cloud-based Traffic Mix:** Healthcare Organizations such as hospitals and clinics, are complex organizations where a broad range of Information Technology (IT), Internet of medical things (IoMT), Operational Technology (OT) and Internet of Things (IoT) devices are increasingly interconnected in their cloud infrastructure. Highly Relying on cloud-based services for storing and managing patient data, as well as for facilitating remote consultations and telemedicine. Cloud traffic within this vertical includes the transmission of sensitive medical information between healthcare providers and patients.

5. **Educational Institution Cloud-based Traffic Mix:** Education institutions are increasingly using cloud-based services to enhance their teaching and learning experiences, streamline their operations using Online learning tools, Collaboration, Data management, administration, research, and security.

6. **Media and Entertainment companies Cloud-based Traffic Mix:** Media and entertainment companies are using cloud-based services for content creation, storage, and delivery. Cloud traffic within this vertical includes the transmission of digital content, such as videos and music, between content creators, distributors, and end-users.

7. **Financial Institution Cloud-based Traffic Mix:** Banks, investment firms, and other financial institutions are using cloud-based services for data storage, risk management, and regulatory compliance. Cloud traffic within this vertical includes the transmission of financial data between financial institutions, as well as between financial institutions and their customers.

8. **Retail Companies Cloud-based Traffic Mix:** Retailers are using cloud-based services for inventory management, supply chain optimization, and e-commerce operations. Cloud traffic within this vertical includes the transmission of customer data, transaction data, and inventory data between retailers and their suppliers, customers, and partners.

2.5.2 Performance Validation Overview

The Advanced Cloud Firewall solution will be evaluated with a common baseline cloud-based firewall traffic followed by the evaluation of the above-mentioned real-world cloud-based traffic mixes. The primary objective of the performance test is NOT to push the cloud security solution under test to its maximum limits but rather ensure that the system is operationally and functionally viable at least at the vendor rated 50% rated throughput-based conditions at least in the above mentioned real-world cloud-based eco systems.

2.6 SSL/TLS Support

HTTP was one of the most important protocols for the web. However, with the advancement in threats and security requirements, there was the need for secure HTTP, i.e., HTTPS. This ensures safer browsing by securely connecting the browsers or applications to the websites. HTTPS uses on encryption, such as SSL or TLS, to provide this safer connectivity. Initially, HTTPS was used with the SSL protocol and with various advancements to this protocol. it led to Transport Layer Security (TLS). Since 2018 all the web browsers made HTTPS the new standard and started specifically would mark HTTP sites as "Not Secure".

Currently, over 60% of the Internet traffic is encrypted. As with any technology, there are always pros and cons. As the industry was securing the web with HTTPS, the external threat actors also improved their game to gradually adapt to exploit this opportunity to become stealthy. In today's threat environment, TLS Inspection by firewall has become very critical to detect and prevent such encrypted threats or behavior.

The following stats indicate the extent of encrypted traffic in use today:

- In January 2021, 89% of pages loaded in Chrome, on all platforms, were over HTTPS[2]
- 93.2% of the browsing time on Chrome is spent on HTTPS pages[2]
- 1 in 10 URLs is malicious[2]
- In January 2021, 89% of pages loaded in Chrome were served over HTTPS[3]

SecureIQLab expects an Advanced Cloud Firewall to provide the features listed below. SecureIQLab will evaluate these capabilities by simulating threat actors and legitimate traffic that leverage these mechanisms.

2.6.1 Cipher Support

To identify the attacks/threats in encrypted connections, it is necessary for the firewall to inspect the encrypted traffic effectively. This is feasible only if the firewall has the capability to support the TLS ciphers and the techniques involved in supporting encrypted connections. To detect a threat that has been encrypted, it is critical that the firewall can decrypt the packets, inspect the content, and take the necessary action based on if the package is a threat or legitimate traffic.

There are 37 TLS 1.2 ciphers and five TLS 1.3 ciphers. SecureIQLab will be test the following cipher suites for support. This cipher list contains those ciphers whose frequency of usage varies from rare to most used. SecureIQLab will also test combinations of ciphers between client and server to analyze firewall behavior with weak ciphers, to analyze how the firewall behaves when two different ciphers are used for communication, and the ability to fall back or enforce secure ciphers for communication.

The cipher suites to be tested are shown below.

2.6.1.1 TLSv1.2 Ciphers

- AES128-GCM-SHA256
- AES128-SHA
- AES256-GCM-SHA384
- AES256-SHA
- AES256-SHA256
- DHE-RSA-AES128-SHA

[2] Google’s Transparency Report
[3] Google HTTPS statistics

- DHE-RSA-AES256-SHA
- DHE-RSA-AES256-SHA256
- DHE-RSA-CHACHA20-POLY1305
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-CHACHA20-POLY1305

2.6.1.2 TLSv1.3 Ciphers

- AES128-GCM-SHA256
- AES256-GCM-SHA384
- CHACHA20-POLY1305-SHA256

2.6.2 TLS Session Reuse

The TLS protocol provides encryption, authentication and data integrity. The server creates a session for each TLS connection and each session requires additional data, such as digital certificates and encryption keys, to be exchanged before any actual web data/payload transfers. This is the TLS handshake negotiation. This additional overhead required to support the TLS protocols and the corresponding encryption techniques has resulted in performance degradation, which may severely affect performance-oriented applications. Hence, the development of TLS session reuse. The additional latency and computational costs for a TLS handshake imposes a serious performance penalty on all applications that require secure communication. To help mitigate some of the costs, TLS session reuse helps resume or share the same negotiated secret key data between multiple connections. This technique is an important optimization deployment. This section will test the session reuse methods supported by the firewall and verify if the methods work properly.

2.6.2.1 Session ID

For every TLS session to be established, there is negotiation between the client and server. Instead of using a new TLS session every time with the client, the server keeps track of recent negotiated sessions using unique session IDs and thus using that to resume an encrypted session. The primary objective in this technique is that when a client reconnects to a server with a session ID, the server can look up the session keys and resume the encrypted communication, rather than starting the negotiation all over again.

2.6.2.2 Session Ticket

In case of the Session ID method, it becomes the responsibility of the servers for remembering the negotiated TLS sessions for a given period of time. This causes severe stress to the servers especially when they have to scale to serve a large load of concurrent connections per second. This puts a burden on the computational cost of the servers to cache sessions for a long time. Hence, the session ticket method is designed to address this issue. Instead of servers managing the session information, it is made the responsibility of the client to handle the same. A session ticket is sent by the server at the end of the TLS handshake and clients supporting session tickets will cache the ticket along with the current session key information to use for their future connections.

3 Advanced Cloud Firewall Metrics and Analyst Workflow

The primary purpose of evaluating any enterprise-grade security firewall product is to come up with quantifiable metrics that provide meaningful data. SecureIQLab is taking a new approach towards defining the firewall metrics and workflows. It is the first testing lab in the industry to showcase individual firewall products' capabilities. SecureIQLab maps these capabilities and workflows to enterprise use-cases. This will allow enterprises to make educated decisions on return on security investment (ROSI), compliance, risk-tolerance (based upon the Advanced Cloud Firewall's ability to cope with threats), total cost of ownership (TCO), and the overall time to prevent threats.

The analyst workflow can be further operationalized using the Cyber Kill Chain and MITRE ATT&CK framework with other security controls.

3.1 Advanced Cloud Firewall Metrics

SecureIQLab has developed the following metrics to accurately assess the capabilities of Advanced Cloud Firewall products:

3.1.1 Reduction in Time to Prevent (TTP)

The ability of the firewall to rapidly identify and prevent a threat and display relevant information is a very important factor. This could include blocking the primary vectors (Web, SMB, applications etc.) and secondary vectors that are typically used for lateral movement. The faster the firewall can prevent a threat and report the relevant information, the sooner the attack can be stopped, and the sooner any damage can be remediated.

TTP will be measured from the time an unknown sample isn't blocked to the time it is blocked. Samples that are not blocked within the TTP test timeframe will be marked as '*missed*'.

SecureIQLab will report the TTP and samples missed for each tested ACFW product.

3.1.2 Threat Classification

Not all threats are of equal severity. The ability to classify attacks according to the risk each one poses is an important feature of an ACFW solution. While reduction in TTP gives time to prevent an incident(s), threat classification gives the users the ability to understand the severity of the threat based on additional research and classification.

If there is a specific threat classification methodology or framework used by the vendor's firewall product, it is best that the vendor discusses this and works with SecureIQLab on those details during the initial setup and baselining phase. This will allow SecureIQLab to map the workflow outcomes to the appropriate threat classification metrics.

- **Advanced Evasive Techniques:**

Advanced evasive techniques refer to tactics used by cyber attackers to avoid detection by security technologies and to make it more difficult for defenders to identify and mitigate cyber threats. These techniques are designed to exploit vulnerabilities in security systems, and to evade detection and analysis by security teams.

- **Known Malicious Files:**

These include known malware that have been in circulation for 30 days or more and consist mostly of viruses and worms. Known samples should not require sandbox analysis. If any pass through an antivirus filter, the sandbox should then have identified it immediately due to the known heuristics of each malware sample.

- **Active Cloud-based Threats:**

Active threat samples that are constantly changing and unknown threats that have been custom-crafted. These undetected samples were acquired from external resources, private honeypots, and APTs that have undergone antivirus evasion techniques such as encryption and payloads that deliver malicious content.

- **Advanced Persistent Threats:**

Cloud-based advanced persistent threats (APTs) refer to sophisticated cyberattacks that specifically target cloud-based infrastructure, applications, and services, and are designed to remain undetected for an extended period. These attacks are often highly targeted, using techniques such as spear-phishing emails, social engineering, and zero-day exploits to gain access to a victim's cloud-based infrastructure. Once inside the system, the attacker can use various techniques to establish persistence, move laterally across the system, and exfiltrate sensitive data without being detected.

Cloud-based APTs often are classified as State-sponsored, Cybercrime, Opportunistic, Hacktivist and Industrial Espionage and are a serious threat and require advanced security measures for the advanced cloud firewall solutions to defend against effectively. Some examples include Cloud Hopper, Silent Fade, Operation Cloudy Omega along with the different APT's with numbering schemes from MITRE ATT&CK ID, Mandiant APT ID, and Kaspersky Lab APT ID.

- **Cloud-centric Post Exploitation Techniques:**

Post-exploitation techniques are used by attackers to maintain access to a compromised system, gather information, and exfiltrate data. Here are some common post-exploitation techniques,

1. **Domain Generation Algorithms (DGA):** DGA is a technique used by malware to create many random domain names that can be used to communicate with a command and control (C2) server. The malware will periodically generate new domain names, making it difficult for security teams to block or detect the C2 traffic.
2. **DNS Tunneling:** DNS tunneling is a technique used by attackers to bypass network security controls and exfiltrate data. The attacker will encode the data they want to exfiltrate into DNS queries or responses, which can be sent over DNS traffic. This technique can be difficult to detect, as DNS traffic is often allowed to pass through firewalls and other security controls.
3. **ICMP Tunneling:** ICMP tunneling is a technique used by attackers to create a covert communication channel over the Internet Control Message Protocol (ICMP). ICMP is typically used for diagnostic purposes, such as testing network connectivity, and is often allowed to pass through firewalls and other security controls. Attackers can use ICMP tunneling to send commands to compromised systems, exfiltrate data, or evade detection.

3.1.3 Compliance Tests

Compliance categories are a way of organizing and classifying various regulatory requirements that organizations must meet to demonstrate their adherence to specific laws and industry standards. Some common compliance categories are around Data Privacy, HIPAA Compliance, PCI DSS compliance and other types of financial reporting and information security.

The primary focus of these compliance-based tests covers the following seven general areas of violated confidentiality and integrity within an organizational cloud infrastructure:

- **Financial Information Exposure:** Organizations requiring payment card industry (PCI) compliance must adhere to data security standards where credit card data is completely protected. Credit card numbers are an obvious target for theft and fraud. Many negative consequences and penalties result from unsecure networks that can cost an enterprise remediation service fees and its reputation.
- **Intellectual Property Exposure:** Intellectual Property is monumental to enterprises of all forms, but especially in technology companies whose property entails incredible amounts of nuances. Hackers are motivated by competitors to steal intellectual property to gain an advantage that could have profound consequences for the vulnerable organization.
- **Restricted Access:** Companies complying with US and European Union (EU) trade laws are obligated to restrict users from visiting websites in countries under embargo. Countries with hostile attitudes towards the US and EU generally host compromised websites and provide low levels of internet security. Blocking specific IP ranges by geography limits can reduce user exposure to threats.
- **Sensitive Information Exposure:** Personal information is targeted by criminals who use it to commit theft and fraud. Breach of confidential data can expose an organization to negative legal consequences and federal actions, in addition to remediation fees to monitor affected consumers
- **Anonymizer Sites:** Employees try to bypass company policies to view blacklisted sites or other harmful content by use of anonymizing proxies. These anonymizers open a backdoor for malware and expose data of an enterprise to untrusted third parties. This may result in a serious depth of negative consequences and legal issues.
- **Insider Threats:** Insider threats can also target integrity by intentionally modifying or destroying data. This can be done through a variety of methods, such as deleting files, modifying data in a database, or introducing malware that corrupts or destroys data.
- **Data Integrity Attacks:** Some types of Man-in-the-middle attacks, Ransomware attacks, Denial of Service(DOS) attacks and SQL injection attacks can lead to unauthorized modifications or deletions of data, and can also enable attackers to gain access to sensitive information such as login credentials which can then prevent legitimate users from accessing critical services, and they can also cause data corruption or loss if the attack is targeted at specific data storage systems.

3.1.4 Threat Triage

Classifying threats according to how they will be resolved helps enterprises respond to attacks in a fast and meaningful approach. Rather than dealing with each threat individually, the admin can potentially resolve several similar threats together, thus saving time and resources.

3.1.5 Threat Timeline

Advanced attacks typically take place over an extended period. To understand the nature of a threat, it is necessary to find out which actions took place at what time. Hence, it is important to have a detailed timeline of how each attack has progressed from its initial stages to completion, along with any relevant IOCs along the way.

3.2 Scoring Criteria

The different prevention workflow mentioned above, along with prevention and detection avoidance, emerging attacks, and the operational accuracy test, will be used as the scoring mechanism to report the overall prevention and response metrics of the firewall products. We will also be measuring and reporting on the TTP (time to prevent) metrics of each of the participating products.

All this will be included as a part of each product's individual test report, and the comparative test report as well. Only qualifying products will be evaluated and represented in the comparative report. As a part of the test, we will also be reporting on some of the key firewall capabilities of each product from a functional standpoint, so that enterprises are well-informed.

3.3 Return on Security Investment Metrics

Implementation of Advanced Cloud Firewall network security technologies can be an expensive process, in terms of product cost, time to deploy, maintenance and personnel expenditures. These factors should be considered when evaluating any security product.

Return on Security Investment (ROSI) is a financial metric used to measure the effectiveness and value of an organization's security investment. The ROSI of a product is derived from its security effectiveness, operational efficiency, ability to avoid false positives, and pricing.

3.4 Dispute Process

SecureIQLab will make best efforts to resolve disputes regarding scoring. Any changes to scoring resulting from successful disputes will be applied to all vendor results, and not just to the disputing vendor.

All Advanced Cloud Firewall vendors who participate in this test will receive their score. This will include a breakdown of security efficacy and operational efficiency scores. This data set will be shared individually with the Advanced Cloud Firewall vendors and SecureIQLab will work closely to go over the metrics as well as relevant metadata where warranted. Furthermore, SecureIQLab will not share attacks that are missed during the testing window to third parties unless required by law. SecureIQLab will provide vendors up to two weeks for the dispute resolution on the nature of attacks. Any security vulnerabilities that are uncovered during the testing windows related to the Advanced Cloud Firewall under test will be shared based upon responsible disclosure policy and will give the vendors up to 20 days to fix the vulnerability. Vulnerability details will be disclosed to the broader public when a fix is available, or it is in the interest of the public.

SecureIQLab will not entertain disputes or changes to scoring after the Comparative and Individual Test reports have been published.

4 SecureIQLab Advanced Cloud Firewall Test Setup

Based on feedback from enterprise clients, SecureIQLab has developed the following enterprise environments with heterogeneous requirements. While this test setup may not encompass the needs of all existing enterprise networks, they represent a common viable standard for all enterprise class Advanced Cloud Firewall products, it may be virtual or cloud-based and is applicable universally.

SecureIQLab used industry leading test tools, scripts, and databases to provide the most robust, comprehensive, and realistic testing environment possible. The enterprise firewalls were configured to block every security related category available within its administrative console and to use all available defenses.

The test setup can be best summarized by the following diagram in Figure 1.

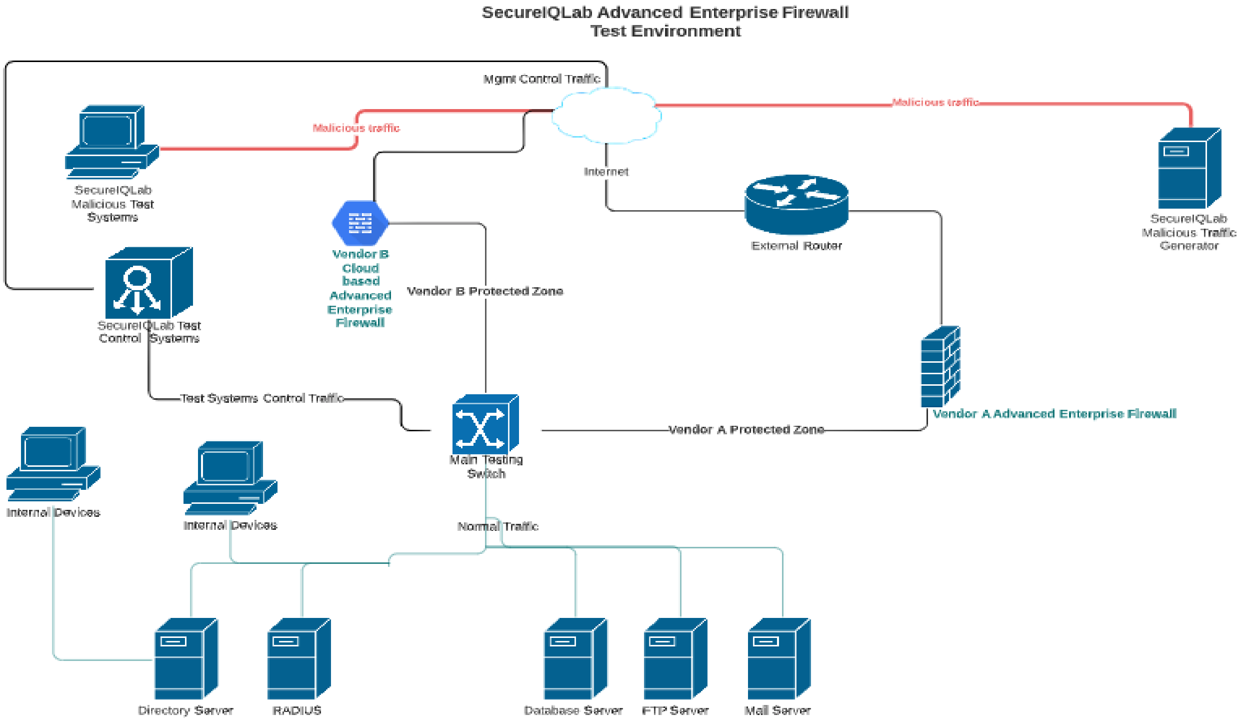

Figure 1. Advanced Cloud Firewall Test Environment

As shown by Figure 1, a firewall product should be able to first identify and prevent attacks using an active response. The advanced capabilities of the firewall should be able to immediately identify the threat and correlate it with its communications to the attackers in real time.

The Analyst Workflow will be triggered by an attack based on the MITRE ATT&CK framework and other methods and can be effectively mapped to the Lockheed Cyber Kill Chain wherever applicable. Given the nature of test environments, some tuning may be required. Participating vendors are invited to review ACFW deployment to align with default and publicly recommended configurations. Test subject vendors will be configured per default configuration and use publicly available recommendations if any additional tuning is required for test harness compatibility.

5 Enterprise Attack Workflow: Prevention Mechanism

An enterprise firewall should be able to first identify and prevent attacks for a specific workflow or an attack scenario.

The attack scenario in this workflow typically goes through a 3-phased approach: first, the initial compromise and gaining of a foothold by the attacker; second, internal propagation; and third, active asset breach. These three phases of the prevention workflow are illustrated in Figure 2 below and are documented in detail.

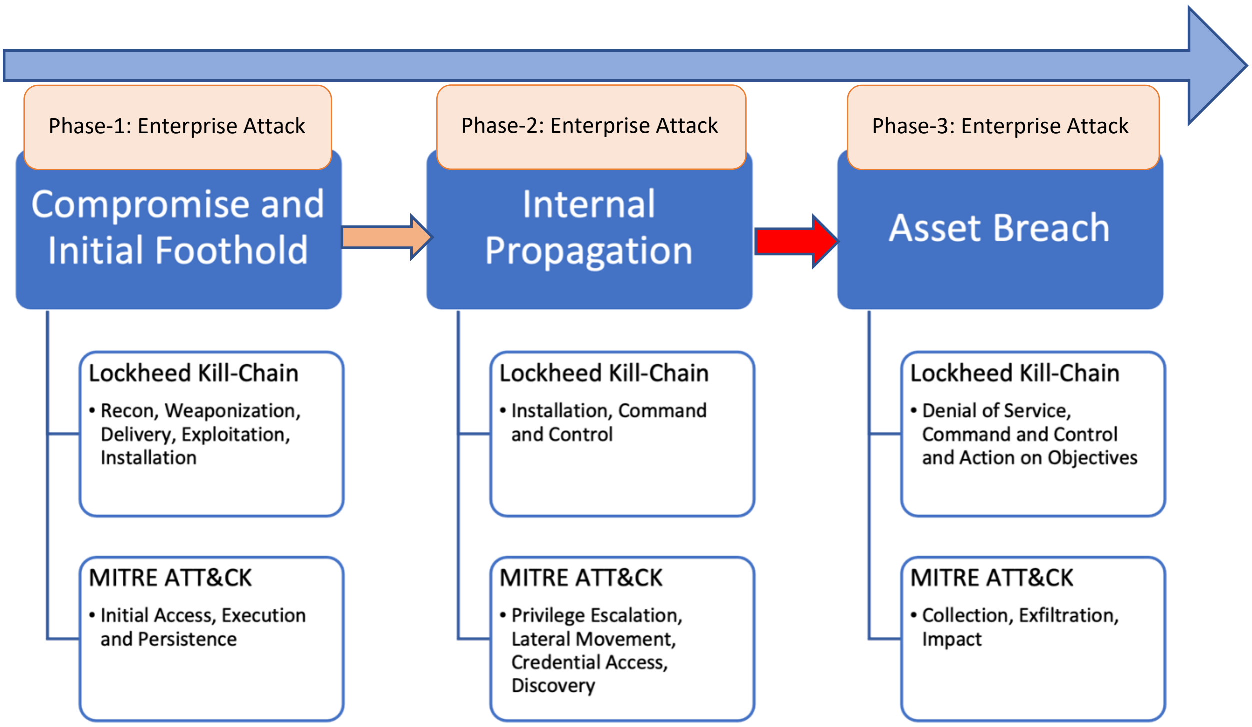
Phase-1: Enterprise Attack
Compromise and Initial Foothold
Lockheed Kill-Chain
• Recon, Weaponization, Delivery, Exploitation, Installation
MITRE ATT&CK
• Initial Access, Execution and Persistence
Phase-2: Enterprise Attack
Internal Propagation
Lockheed Kill-Chain
• Installation, Command and Control
MITRE ATT&CK
• Privilege Escalation, Lateral Movement, Credential Access, Discovery
Phase-3: Enterprise Attack
Asset Breach
Lockheed Kill-Chain
• Denial of Service, Command and Control and Action on Objectives
MITRE ATT&CK
• Collection, Exfiltration, Impact

Figure 2. Enterprise Attack Prevention Workflow: Phases 1, 2 and 3

5.1 PHASE 1: COMPROMISE AND INITIAL FOOTHOLD

An enterprise firewall should be first able to identify and prevent a threat in the shortest possible time window. Because this is the first phase of the attack, the faster the prevention, the more effective the firewall. This will enable organizations to defend against the attacker before a compromise and a foothold is achieved within the enterprise infrastructure. This compromise can be triggered by an attack based on the MITRE ATT&CK and other methods and can be effectively mapped to Lockheed's Cyber Kill Chain.

5.1.1 Initial Access

Initial access is the method used by the attacker to get a foothold inside the environment that is being targeted. Attackers may use a single method, or a combination of different techniques. Threats may come from compromised servers, databases, websites, email attachments, insider threats or removable media.

5.1.2 Execution

The next goal of the attacker is to execute their own code inside the target environment. Depending upon the circumstances, this could be done locally or via remote code execution.

5.1.3 Persistence

Once the attacker gets inside the target environment, they will try to establish a persistent presence there. Depending upon the target operating system, an attacker typically uses operating system features to plant inside the environment. These include registry manipulation, specifying dynamic-link-library values in the registry, shell scripts that can contain shell commands, application shimming, and account manipulation.

5.2 Phase 2: Internal Propagation

In this phase, the firewall should be able to prevent internal propagation. This phase is triggered when the initial identification and prevention of the threat fails. The firewall in this phase should be able to enable the analyst to immediately identify and correlate the internal propagation of threat in real time. The analyst should be able not only to perform the necessary actions to identify, detect, classify, and triage a threat, based on the data collection and analysis, but also initiate the response using the firewall or an integrated solution as a specific workflow tied to this phase.

This workflow can be triggered by an attack based upon MITRE ATT&CK or other methods and can be effectively mapped to Lockheed Kill-Chain[4]. This phase of attack can be operationalized by the attacker using the steps described below.

5.2.1 Privilege Escalation

In enterprise networks, it is standard practice for users, including system admins on their own personal computers, to use standard user accounts without administrator privileges. If an enterprise endpoint is attacked, the logged-on account will not have the permissions the attacker requires to launch the next phase of the attack. In these cases, privilege escalation must be obtained, using techniques such as user-access token manipulation, exploitation, application shimming, hooking, or permission weakness.

5.2.2 Discovery for Lateral Movement

Once the attacker has gained access to the target network, they will explore the environment, with the aim of finding those assets that are the potential target of the attack. This is typically done by scanning the network.

5.2.3 Credential Access

This is a method used by the attacker to ensure their further activities are carried out using a legitimate network user account. This ensures that they can access the resources they want and will not be flagged by the system's defenses as an intruder. Different credential access methods can be used, depending on the nature of the targeted network. Credentials can be obtained on-site, using a method such as input capture (e.g., keyloggers). Alternatively, it might be done using the offline method, where the attacker copies the entire password database off-site, and can then use any method to crack it without fear of discovery.

5.2.4 Lateral Movement

The attacker will move laterally within the environment to access those assets that are of interest. Techniques used to move laterally include pass the hash, pass the ticket, and exploitation of remote services and protocols like RDP.

5.3 Phase 3: Asset Breach

The final phase of the workflow is asset breach. This is the stage where an attacker truly starts acting on its true objective. This workflow can be triggered by an attacker based upon MITRE ATT&CK or other methods and can be effectively mapped to Lockheed Kill Chain. This phase of attack can be operationalized by the attacker through the steps described below.

5.3.1 Collection

This involves gathering the target information – assuming of course that information theft, rather than sabotage, is the object of the exercise. The data concerned could be in the form of documents, emails, or databases.

5.3.2 Exfiltration

Once the attacker has reached the objective of collecting the target information, they will want to copy it covertly from the targeted network to their own server. In almost all cases, exfiltration involves the use of a command-and-control infrastructure.

5.3.3 Impact

Having found and extracted the target information, the attacker will try to delete or destroy all the evidence of the attack that remains within the target network. An ideal scenario for the attacker may well be one in which the victim does not even realize that the attack has taken place. Whether or not this is possible, the attacker will try to manipulate data inside the target environment to ensure that their tracks are covered as far as possible. This will ensure that the victim does not have the forensic information needed to understand the attack or trace the attacker. Data manipulation, deletion, and encryption (as used in ransomware) are the typical techniques that are used to do this.

6 Advanced Cloud Firewall Operational Efficiency

Cloud firewall operational efficiency refers to the effectiveness and efficiency with which a cloud firewall can provide security to an organization's cloud infrastructure while minimizing operational costs and complexity.

Operational efficiency in the context of Advanced cloud firewalls will be measured on the following areas,

- **Security Policy Configuration:** This helps in the understanding of the environment that organizations are working on, specifically the different persona categories and types deploying, managing, or monitoring the ACFW solution with vendor recommended configuration.
- **Security Policy Configuration-Ongoing**: The is the ability to deploy, maintain, change and monitor the shift in policy over time. This is a very critical aspect of day-to-day firewall operations.
- **Asset Management:** This refers to the ability of the cloud firewall to provide effective visibility and control over the assets that are protected by the FW.
- **Access Control:** This refers to the ability of the cloud firewall to have the required administrative control levels, role-based access for admins and users.
- **Incident Management:** This refers to the ease with which the cloud firewall can be for activity, identify and detect the existence of a security threat followed by a defined mitigation process against it.
- **Compliance Management:** This refers to the ease with which the cloud firewall can be for activity, identify and detect lack of compliance followed by a process to manage it.
- **Business Continuity Management:** This in the context of the ACFW solution simply refers to how services are restored during and post attack or a disaster.
- **Risk Assessment & Mitigation:** The process for understanding risks and the ability to reduce or mitigate them completely from the ACFW solution.
- **Security Metrics Reporting:** This is a metric to validate if the ACFW solution has sufficient logging and documentation around security events that are reported with the right timeline and context.

- **Configuration and Policy Backup and Restoration:** This refers to the ability of the cloud firewall to consistently backup configuration and policy parameters are able to restore on-demand.

7 Reporting Capability

Admins should also be able to use the firewall management systems to review past incidents and the action taken at the time to decide if the same actions are applicable to the current threat. While providing maximum flexibility to senior analysts, the firewall should support predefined but configurable workflows for less experienced personnel, who may be assigned specific tasks during an investigation.

A firewall platform should have the ability to unify data. That is to say, bring together information from disparate sources, and present it all within its own user interface (UI) as a coherent picture of the situation. Technical integration with the operating system and third-party applications (syslog, Splunk, SIEM or via API) is an important part of this.

7.1 Standard Firewall Security Reporting

Standard firewall security reporting consists of the detection of known threats that have been in circulation and have already been researched. These are the simpler security tests, and although basic, having detection against these tests is vital for a firewall.

Vendors will be evaluated against SecureIQLab's threat categories such as, legacy files, malicious URL testing, botnets, phishing, compressed malicious files, exploits, cookie stealing, script injection and adware.

7.2 Advanced Cloud Firewall Security Reporting

Advanced security tests require more sophisticated methods to protect against threats that either have a more convoluted form of attack or extract highly sensitive data.

This could range from advanced malware samples, APT's, AET's, malware downloaded over SSL/TLS, obfuscated JavaScript detection and browser/plugin related vulnerabilities.

This also includes various types of data loss and compliance-based tests.

8 Resiliency

Attackers will obviously make every effort to ensure that their attacks will not be prevented by the firewall product, or any of the victim's security measures. SecureIQLab will make use of common content-masquerading techniques and employ trusted apps and processes to mimic detection avoidance. This will determine whether the tested Advanced Cloud Firewall products can prevent attacks that deliberately use obfuscation techniques. This will give a better understanding of the products' prevention capabilities in realistic enterprise scenarios. This section will be independent of the workflow listed above and will focus on testing resiliency of the products against more advanced attacks.

9 Operational Accuracy Test

A security product that reports 100% of malicious attacks, but also reports legitimate (non-malicious) actions, can be hugely disruptive/noisy. SecureIQLab will use appropriate tools and techniques to ensure that the tested firewall products do not raise significant numbers of alerts with legitimate applications and processes. This section of the methodology will be performed in conjunction with *Workflow* and other independent sections as much as possible. This will ensure that the firewall products aren't heavily biased towards prevention by sacrificing operation accuracy in an enterprise environment.

10 General Evaluation Approach

10.1 Advanced Cloud Firewall Vendor Participation Selection Criteria

We select ACFW vendors based on three following criteria:

1. Market Leaders – Either in terms of revenue generated, customer numbers globally, or strong channel play
2. Analyst and Enterprise challengers – Small-mid-large enterprise security professional surveys, direct 1:1 inquiries and engagement with enterprises, organizations, MSP's, MSSP's and Gartner MQ, buyers guide, Forrester Wave, and IDC reports
3. New market entrants and interested participating vendors with breakthrough technology offerings

There are no known conflicts of interest.

10.2 Scope

The scope of this iteration of the test will be limited to ACFW solutions that are available in cloud marketplace, Cloud-ready/SaaS based deployment. Examples of cloud marketplace include Azure, Amazon Web Services, Google Cloud, SaaS and FWaaS offerings. Vendors can choose to include different product for different Cloud offering.

Subsequent iteration of this test will include physical as well as hybrid deployments.

Here is the list of considered vendors at the time of this publication:

Vendor	Product Name	Process Used
AgniGate	AAA NGFW	Test to be evaluated utilizing Blackbox Security and Greybox Security Tasks
Barracuda Networks	CloudGen Firewall	
CATO	Next Generation Firewall as a service	
Check Point	CloudGuard Network Security NGFW	
Cisco	Firepower NGFWv	
Forcepoint	Forcepoint Next Generation Firewall	
Fortinet	FortiGate NGFW	
Hillstone Networks	CloudEdge	
Juniper Networks	vSRX	
Netskope	Netskope Cloud Firewall	
Palo Alto Networks	VM-Series NGFW	
Perimeter81	FWaaS	
Qi-AnXin	LegendSec Next-Generation Smart Firewall	
Sangfor Technologies	Sangfor NGAF	

SonicWall	NSv
Sophos	Sophos Firewall
Stormshield	NGFW
Valtix	NGFW + WAF Service
Versa Networks	NGFWaaS
VMware	NSX Distributed Firewall
Voleatech GmbH	VT AIR Cloud Firewall
WatchGuard	Firebox Cloud
Microsoft	Azure Firewall

10.3 Advanced Cloud Firewall Test Life Cycle

The Advanced Cloud Firewall test plan is within scope if the project remains within four weeks of the below timeline. This methodology was finalized on 29 March 2023. Feedback is encouraged for future iterations.

SecureIQLab will execute the test in seven phases:

- **Phase 1: Reconnaissance**
  - We will start the initial validation with basic and advance level reconnaissance.
- **Phase 2: Evaluating Operational Efficiency Capabilities**
  - As a part of the validation, we will perform evaluation of Operational Efficiency capabilities.
- **Phase 3: Evaluating Standard Firewall Threat Capabilities**
  - We will start the initial validation with Standard Firewall Threat Capabilities.
- **Phase 4: Evaluating Advanced Threat Capabilities**
  - As a part of the validation, we will perform evaluation of Advanced Threat capabilities.
- **Phase 5: Evaluating Compliance Capabilities**
  - As a part of the validation, we will perform evaluation of Compliance capabilities.
- **Phase 6: Evaluating Prevention Avoidance Capabilities**
  - As a part of the validation, we will perform evaluation of Prevention Avoidance capabilities.
- **Phase 7: Post Assessment Phase**
  - We will review, assess, and document the discovered vulnerabilities and the issues and will be tabulating the scorecard and prepare the final report.

SecureIQLab will execute the project in five phases that are listed in table format below:

Schedule Summary for Test Project

Index	Test Activity	Date Range	Dependencies
1	Test Commencement	1 May 2023	Vendor Voluntary participation (or) procurement of vendor software
2	Confirm Vendor Configuration Feedback	8 May 2023 to 16 May 2023	All required vendors installed, smoke tested, and configurations validated by vendors where possible.
3	Testing	17 May 2023 to 14 June 2023	Based on smoke test result disputes and resolution
4	Feedback and Dispute Resolution Time – Retests as Needed	15 June 2023 to 12 July 2023	Based on report feedback and final dispute resolution.
5	Publish results	18 July 2023	Dependent on ACFW solution disclosure requirements

10.4 Risk and Risk Management:

No additional risks are known at this time.

10.5 Geo-Limitations:

SecureIQLab will make every effort to use only attacks that are not geo-location centric when necessary. SecureIQLab will ensure that attacks also originate from as wide a range of IP addresses as possible.

10.6 Distribution of Test Data:

Upon the completion of the five phases of this validation project, the resulting data will be organized into individual test reports and one comparative report. These results will be available for vendors to purchase for marketing and will also be publicly available to download at https://secureiqlab.com/publications/.

10.7 Funding Agreement

This is a non-commissioned test funded by SecureIQLab.

10.8 Opt-Out Policy

Opt-Out: Opt-out will only be considered for the following reasons:

1. The product, solution (or) technology is found to be outside of scope in the context of the methodology as determined by SecureIQLab.
2. Any technology, product or a solution that is NOT generally available nor ready for deployment.
3. Publishing the test would not serve the public interests as deemed by SecureIQLab.

Opt-out requests must be provided in writing. Emailed opt-ops must be sent to info@secureiqlab.com. Mailed opt-outs must be sent to:

SecureIQLab
9600 Great Hills Trail #150W
Austin, Texas 78759
USA

Mailed opt-outs are effective by the date received, not the date posted. We do not accept opt-outs through phone, voice, social media or similar. ***The opt-out must contain the name, title, email and phone number of the individual authorized to request an opt-out on behalf of the vendor. To be considered a completed opt-out, the request must state under which of the reasons above the request should be considered and provide details to support the request***. All vendors have a limited right to opt-out for the designated reasons listed above. The opt out period begins at the *Test Commencement* and continues through the end of the *Dispute Phase [Section 2.2]*. Vendors will be contacted by SecureIQLab within 3 business days of receiving the opt-out request to discuss feasibility. If a vendor opts out before the end of the *Configuration Phase*, the vendor will be listed as 'Participant, not tested '. If a vendor opts out after testing has been performed for their product, their product will be marked in the results 'Tested, not published '.

11 Attestations

I understand and agree that I am submitting this Test Plan, and the following Attestations, on behalf of the entity listed below, and I represent and warrant that I have authority to bind such entity to these Attestations. All references to "I" or "me" or similar language refer to such entity. I represent and warrant that the following Attestations are true, to the best of my knowledge and belief, and each of the following commitments will be upheld to the best of my ability.

I will provide public notification on the AMTSO website covering my obligation for notification of a Public Test, regardless of whether a potential Participant is in actual receipt of such notification prior to the Commencement Date of a Test.

All products included in this Test will be analyzed fairly and equally.

I will disclose any anticipated or known imbalance or inequity in the Test design to all Participants in the Test.

Although I may charge for participation in a Test, I will not charge any additional fees for a vendor to be a test subject under the Standards.

I will disclose any material conflicts of interest or other information that could materially impact the reliability of the Test.

I will disclose how the Test was funded.

I hereby affirm, to the best of my knowledge and belief that this Test Plan complies with the AMTSO Testing Standards, as of the date hereof.

Signature: /s/ David Ellis
Name: David Ellis

12 Appendix

12.1 Glossary of Terms

12.1.1 Cyber Kill Chain

The Cyber Kill Chain® framework is part of the Intelligence Driven Defense® model for the identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete to achieve their objective.

12.1.2 MITRE ATT&CK®

MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

12.2 Sample Selection, Curation, and Sourcing

Sample selection and sourcing will be based on the realities of the threat landscapes during the testing window. Publicly and privately available threat intelligence reports, sources, and techniques will be collected and assessed to determine the viability of inclusion for the test. Enterprise feedback is also solicited for sample selection and the curation purpose.

12.3 Proposed Attack Types

Testing will demonstrate the effectiveness of the PUT to protect vulnerable assets from targeted threats and exploitation. This asset/target and threat-based approach forms the basis from which the PUT security effectiveness is measured.

Attack types and test configuration: The SecureIQLab threat and attack suite contains attacks, including mutations of the same underlying attacks, and proprietary exploits. These attacks and exploits are either harvested through our test harness or crafted by our threat research team. Crafted exploits are intended to simulate attacks in the wild. Groups of exploits used in testing are carefully selected from the attack based on the intended attack. Each exploit has been validated to compromise the vulnerable target host(s). Targeted assets may include web servers, web applications or sites. In this iteration, attacks will primarily target cloud-based assets.

ACFWs will defend a number of networks that have also been constructed to include known vulnerabilities and coding errors.

SecureIQLab includes attacks that have a definite outcome i.e., an attacker establishing a reverse connection, file uploads or proof of concept (PoC) attacks are all part of the test set. This ensures that the ACFW under test's ability is stressed for outcome-based testing.

The level of compromise can vary between instigating a Denial of Service (DoS) condition, providing administrator/root access to the host server, allowing malicious users to amend system parameters or application data before submission, browse and/or retrieve files stored on the host server, escalating user privileges and so on.

12.4 Document Revisions:

Version	Section	Revision overview
V1.1	2.5	Added Advanced Cloud Firewall Real-World Traffic section
V1.1	3.1.3	Removed Test Overview column
V1.1	9.2	Added Microsoft Azure Firewall into scope of test vendors
V1.5	2.4	Renamed "COMMON CLOUD FIREWALL THREAT CATEGORIES" and rewritten
V1.5	2.5	Updated with additional details provided
V1.5	3.1.2	Section rewritten and additional details provided
V1.5	3.1.3	Section rewritten to seven areas of compliance
V1.5	3.3	Section renamed "RETURN ON SECURITY INVESTMENT METRICS and rewritten
V1.5	6-12	Sections incremented plus one with the creation of a new section 6 "ADVANCED CLOUD FIREWALL OPERATIONAL EFFICIENCY"
V1.5	10.2	Edits to vendor products
V1.5	10.3	Tests phases, test project, and test timeline edited
V1.5	11	Updated attestation
V1.6	Title	Advanced Cloud Firewall Solution CyberRisk Validation Methodology
V1.6	2.3.3	Added Optional Endpoint Deployment
V1.6	2.5	Section renamed and split into two subsections with additional details
V1.6	10.3	Updated dates and timeline

13 Copyright and Disclaimer

This publication is Copyright © 2023 by SecureIQLab®. Any use of the results, etc., in whole or in part, is ONLY permitted after the explicit written agreement of SecureIQLab prior to any publication. SecureIQLab and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but liability for the correctness of the test results cannot be taken by any representative of SecureIQLab. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For more information about SecureIQLab and the testing methodologies, please visit our website www.secureiqlab.com.

SecureIQLab (March 2023)