SecureIQlab®

Report

AT&T Dynamic Defense Firewall Validation Report

Test Period: 15 July 2024 – 5 August 2024

Last Revision: 24 October 2024 | Commissioned by: AT&T

Report Contents

1. Executive Summary **2**

2. Introduction **3**

2.1. Policy Enforcement 3

2.2. Security Efficacy 4

2.3. Reporting and Logs 4

2.4. Usability 5

2.5. AI-Driven Policy Generation 5

3. Policy Enforcement **5**

3.1. Application Control 5

3.2. Web / URL Filtering 5

3.3. Service Control Policy 5

3.4. IP Control 6

3.5. Geo Filtering 6

4. Advanced Threat Protection **6**

4.1. Dynamic Defense Shield 6

4.2. Premium Threat Protection / Protection+ 7

4.2.1. Application Threats 7

4.2.2. Post Exploitation Activity 8

4.2.3. Advanced Attacks 8

5. Operational Accuracy Validation **8**

6. Operational Efficiency Validation **9**

7. Conclusion **10**

8. Methodology **11**

8.1. Test Infrastructure 11

8.2. Scenarios Tested & Validation Procedure 12

9. Contact Information **14**

10. Copyright and Disclaimer **14**

1. Executive Summary

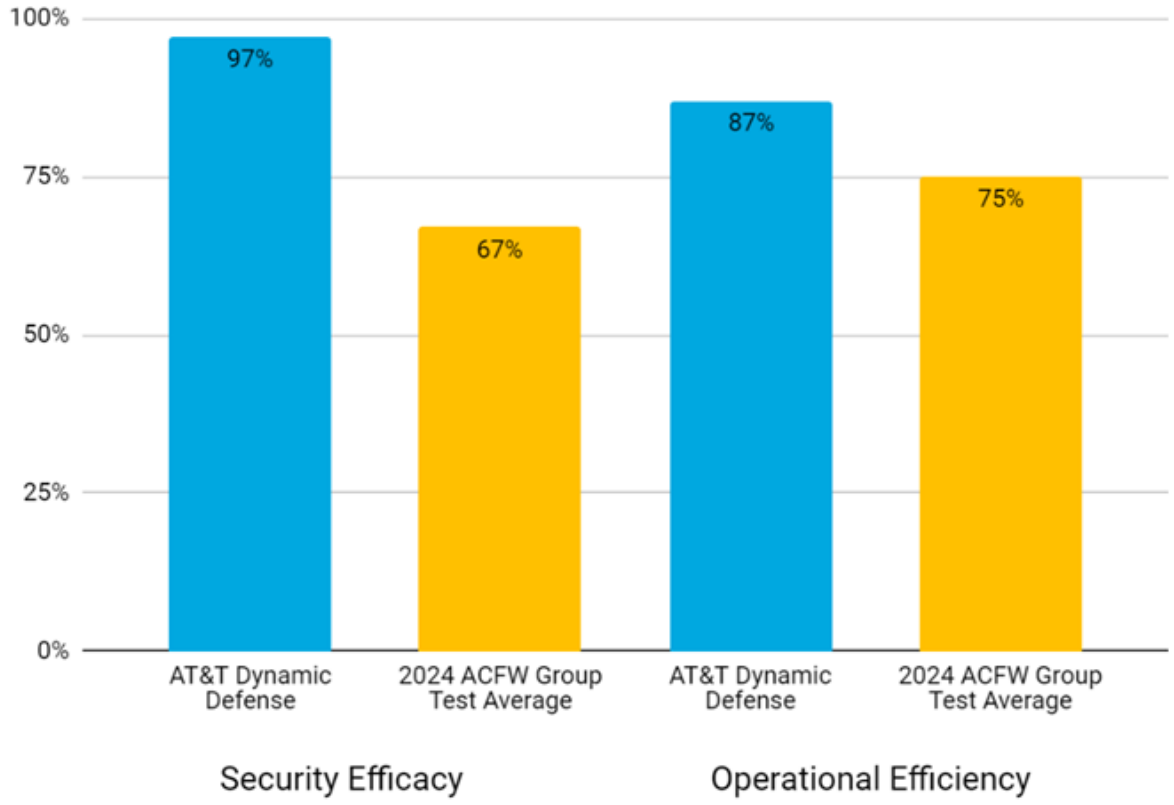

Figure 1. AT&T Dynamic Defense Security and Operational Summary Results

AT&T Dynamic Defense is a network security solution with features like dynamic IP blocking, stateful firewall monitoring, and Geo IP filtering and simple onboarding through AI suggested configuration. It includes web filtering, basic threat detection, and detailed reporting on network health. This report covers SecureIQLab's validation of the AT&T Dynamic Defense software as a service. Figure 1 highlights SecureIQLab's overall findings.

In Figure 1, The results in blue represent AT&T's Dynamic Defense's Security Efficacy, at an impressive total attack block rate of 97%, and Operational Efficiency of 87%. These are compared to the group test averages from SecureIQLab's 2024 Public Advanced Cloud Firewall Testing, which are shown in orange. Our finding is that the AT&T Dynamic Defense Sheild significantly improves its firewall offering and its Smart Protection, that is, its AI-based configuration assistance significantly improves ease of use.

Our testing of the AT&T Dynamic Defense covered onboarding/offboarding and firewall policy configuration; it also covered the firewall's operational efficiency, scalability, and performance while verifying that it secured small and medium business networks against various cyber threats, such as spyware, data exfiltration, and command-and-control attacks.

AT&T Dynamic Defense simplifies the process of onboarding the product and deployment of the ruleset through Smart Protection, or artificial intelligence (AI) suggestion-based configuration. AI suggestion-based configuration helps the person setting up the firewall choose the appropriate ruleset and deploy it in the targeted environment.

AT&T's high degree of ability to offer clean pipes, that is, clean data channels, along with relevant threat intelligence produced by the AT&T threat Intelligence team form AT&T's Dynamic Defense Sheild. This, along with a managed rule set, are substantial assets.

AT&T commissioned these tests to measure their overall security efficacy and key operational efficiency parameters. These tests were also intended to evaluate the relative security resiliency of the firewall and the firewall's ability to protect the network when well-known protocols are abused to evade detection.

In writing this report, SecureIQLab has made extensive efforts to guarantee the accuracy of the results while straightforwardly presenting them. However, the test results are necessarily aggregated and simplified to present them in a summary format.

2. Introduction

Test Categories	AT&T Dynamic Defense Result
Policy Enforcement	**Pass**
Security Efficacy	**97%**
Reporting and Logs	**High**
Usability	**High**
Ease of Deployment	**High**
Operational Efficiency	**87%**
AI-Driven Policy Generation	**High**

Table 1. AT&T Dynamic Defense Results

The 2024 SecureIQLab AT&T Dynamic Defense Cyber Risk Validation report provides test results for the AT&T Dynamic Defense solution.

Table 1 summarizes the overall validation results of the AT&T Dynamic Defense for the 7 categories tested: policy enforcement, security efficacy, analytics, accessibility, ease of deployment, additional operational efficiency metrics, and AI-driven policy generation.

As can be seen from the table, the AT&T Dynamic Defense generally performs well. One of its biggest strengths is the ease of deployment and usability. There is an opportunity for improvement in additional operational efficiency metrics such as firewall policy scheduling and security recommendations based on security incidents.

2.1. Policy Enforcement

The Dynamic Defense solution's categorized rule management streamlines consistent and centralized enforcement of firewall policies across the network. Organizing protection categories upfront simplifies management and troubleshooting, especially when dealing with version changes.

AT&T Dynamic Defense passed all policy enforcement category testing while effectively managing critical rules and promoting a secure and compliant network environment. Details of these test categories are provided in section 3.

2.2. Security Efficacy

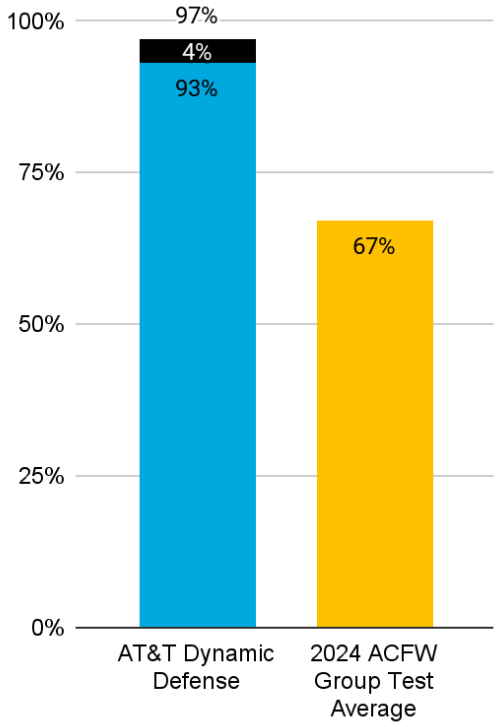

Figure 2. AT&T Dynamic Defense Security Score compared to the 2024 ACFW Group Average

The security efficacy test stressed measuring the effectiveness of Dynamic Defense's threat detection capabilities. As such, this test focused on Dynamic Defense's intrusion prevention system. The attacks launched included exploits targeting lift and shift applications, cloud-native application-centric exploits, post-exploitation activity, and advanced persistent threat (APT) activity. As seen in Figure 2, the overall security efficacy score of the AT&T Dynamic Defense was 97%, which is exceptional. The black bar stacked on top of the blue bar represents the 4% contribution that the AT&T Dynamic Defense Shield provides to the overall security. Details regarding AT&T Dynamic Defense's Advanced threat protection are available in section 4.

2.3. Reporting and Logs

The Reporting functionality offers detailed insights into network traffic, highlighting top talkers, allowed and denied sources, and destinations. It also tracks the most accessed and blocked URLs, applications, and global block list hits that help in identifying potential threats, monitoring compliance, and optimizing security measures. Additionally, the ability to filter data by specific timeframes enables targeted analysis and historical trend tracking, supporting proactive security management and strategic planning.

The logging functionality offers detailed insights into network activities, enabling administrators to filter logs by time, destination, source IP, and actions. Providing categorized logs for traffic, URLs, and threats, helps organizations monitor network behavior, detect anomalies, and ensure compliance. The ability to export logs to Excel, CSV, or JSON formats allows for easy data analysis and sharing, making it a valuable tool for enhancing security and operational efficiency.

2.4. Usability

The AT&T Dynamic Defense Portal offers a highly intuitive user experience and excels in usability across its three key sections.

Overview: The landing page features a network activity graph that provides a clear snapshot of blocked and allowed traffic. Users can easily filter and view blocked events with counts displayed for both inbound and outbound traffic, adjustable by time range. This design ensures that critical network activity insights are readily accessible and understandable.

Policy Management: This section facilitates the categorized management of network security policies, including geo-filtering, web filtering, and IP control. Users can apply AT&T's recommendations and make changes across different categories seamlessly, with the ability to edit drafts and access policy version history. This approach simplifies policy updates and ensures efficient management while maintaining clarity.

Insights: The Insights section not only offers robust reporting and logging but also integrates traffic control features, allowing users to directly allow or block specific traffic from within the reports. This feature streamlines decision-making, enhances efficiency by reducing the number of steps needed to act on insights, and simplifies network security management, making the platform both user-friendly and effective.

2.5. AI-Driven Policy Generation

The AT&T Dynamic Defense Service monitors network traffic for 7 days before generating a tailored policy based on the organization's needs. This process highlights the ease of configuring Dynamic Defense, as it requires minimal human intervention. The automatically generated policies are as effective as those set by network administrators, ensuring strong protection while simplifying policy management.

3. Policy Enforcement

3.1. Application Control

The application control capabilities of the firewall are tested to ensure accurate identification and categorization of applications, effective enforcement of usage policies, and minimal impact on network performance. These tests verify that the firewall can precisely control application behavior, provide detailed reporting and alerts, and remain compatible with various applications and network environments.

Out of 20 tested applications, AT&T Dynamic Defense was able to enforce the policy settings for 17 of them, while 3 of the applications were not detected by Dynamic Defense.

3.2. Web / URL Filtering

Web and URL filtering capabilities of the firewall are rigorously tested to ensure it can effectively block risky categories of URLs and known malicious domains. This process guarantees robust protection against potentially harmful websites and domains. Additionally, the AT&T Dynamic Defense Service offers the option to apply AT&T's recommended block list of website categories. In testing, AT&T Dynamic Defense successfully enforced policies across 77 of the evaluated URL categories.

3.3. Service Control Policy

The Service Control policy of Dynamic Defense is tested to evaluate its ability to accurately identify and classify various network services and applications, including those using both standard and non-standard ports. The assessment involves toggling inbound and outbound connections across these ports to determine the firewall's effectiveness in enforcing rules that allow or block specific services according to security policies.

The tests confirmed that Dynamic Defense successfully enforced policies based on service ports, demonstrating its capability to manage and secure network traffic effectively. Consequently, Dynamic Defense has "PASSED" the test.

3.4. IP Control

The IP control feature of Dynamic Defense is tested to evaluate its capability to block or allow traffic based on custom IP addresses, ports, and protocols. This testing ensures that the firewall can accurately enforce security policies by controlling access to and from specific IP addresses, managing traffic through designated ports, and handling different network protocols.

The tests confirmed that the custom allow and block policy on IP addresses is being enforced by Dynamic Defense resulting in the “PASSED” status for this test.

3.5. Geo Filtering

Geo-location filtering is essential for controlling where data is accessed and stored, ensuring compliance with data privacy and sovereignty regulations. By restricting access based on geographic location, organizations can reduce security risks from high-risk regions. It also allows for customized access control, tailoring security policies to specific locations or business needs.

In our test, we adjusted the geo-location settings in the Dynamic Defense policy to block connections to and from specific IP addresses based on their geographic locations. We verified that connections to these blocked IP addresses were successfully prevented, demonstrating that the firewall has "PASSED" the test.

4. Advanced Threat Protection

4.1. Dynamic Defense Shield

The AT&T Dynamic Defense Shield, powered by AT&T’s threat intelligence, automatically blocks traffic to and from malicious IP addresses within your network. It leverages a globally maintained blocklist that is continuously updated to reflect the latest threat landscape.

In our test, we collected a list of malicious IPs and simulated traffic outbound to these IP addresses and found that the Dynamic Defense shield can block the traffic going to these destinations, demonstrating that the firewall has “PASSED” the test.

4.2. Premium Threat Protection / Protection+

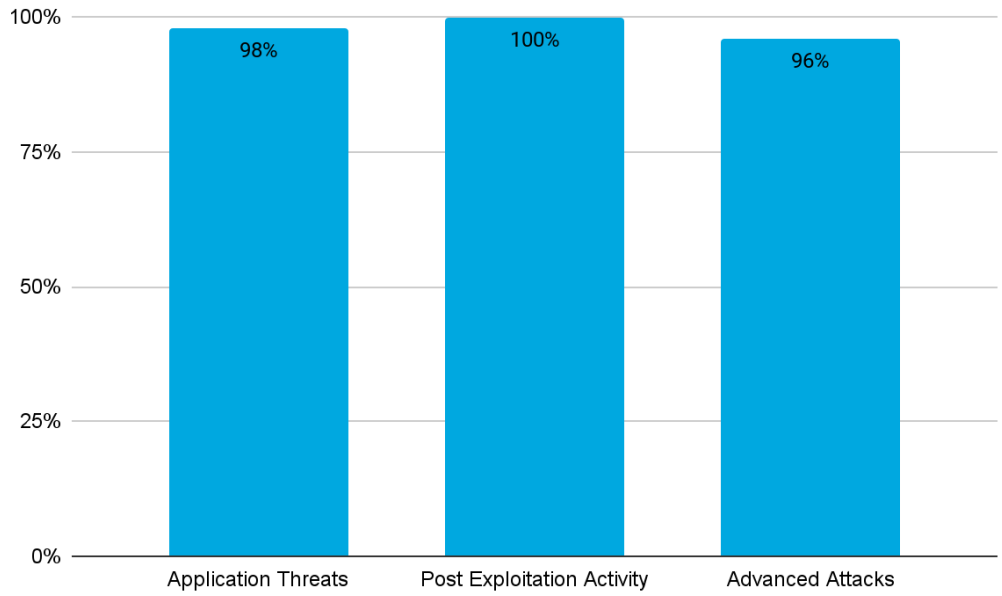

Figure 3. AT&T Dynamic Defense Security Efficacy

The Premium Threat Protection package, previously known as Protection+, is the advanced protection feature offered by Dynamic Defense that adds Next-generation firewall capabilities to the product. It offers virus protection, spyware protection, and vulnerability protection. SecureIQLab ran various categories of tests that evaluate the capabilities of Protection +.

The AT&T Dynamic Defense was tested against 160 attack types within four threat categories. Figure 3 above presents an overview of the SecureIQLab findings during the security effectiveness validation and reporting of the AT&T Dynamic Defense. This includes the application threats, post-exploitation, and APT activity score.

4.2.1. Application Threats

Test Categories	AT&T Dynamic Defense Result
Exploits	100%
Plugin Control	100%
Active Threats	100%
Obfuscated Scripts	100%
Web application attacks	100%
Containerized application attacks	87.5%

Table 2. Application Threats

The AT&T Dynamic Defense was evaluated for its ability to counter application-based attacks, specifically focusing on application threats. The efficacy of the firewall was determined by calculating the average threat scores across various attack categories, which included application-targeted attacks, plugin control capabilities, active cyberattack threats, and evasion techniques. AT&T demonstrated exceptional performance, scoring 100% in all test categories for application threats (as shown in Table 2) except for container-based attacks.

4.2.2. Post Exploitation Activity

Test Categories	AT&T Dynamic Defense Result
Post Exploitation Activity Blocked	**100%**

Table 3. Post-Exploitation Activity

The term post-exploitation refers to any activity performed by threats after the successful exploitation of a resource. While there are various activities that threats could choose to perform, such as data exfiltration, data destruction, and infrastructure lockdown, these activities are performed via various well-known protocols. However, this malicious activity using these protocols is difficult to detect because it looks benign.

The post-exploitation activity average score for the AT&T Dynamic Defense was calculated by averaging the scores for each threat type within their respective attack category. Table 3 showcases that the AT&T Dynamic Defense scored 100% in this category by detecting malicious activity.

4.2.3. Advanced Attacks

Test Categories	AT&T Dynamic Defense Result
Advanced Attacks Blocked	**96%**

Table 4. Advanced Attacks

Advanced Attacks are sophisticated cyberattacks that infiltrate networks using stealthy, persistent methods. They often involve multiple stages, including initial compromise and maintaining long-term access, while avoiding detection. These attacks aim to exfiltrate data or disrupt operations and require advanced defenses to counter; SecureIQLab used PowerShell Empire, Covenant, and Cobalt Strike to run Advanced attack scenarios.

The Advanced Attacks score for the AT&T Dynamic Defense is calculated by averaging the scores for each threat type within their respective attack category. Table 4 highlights AT&T blocked 96% of the Advanced Attacks.

5. Operational Accuracy Validation

Operational Accuracy Test	AT&T Dynamic Defense Result
Resistance to False Positives	**100.0%**

Table 5. Operational Accuracy

False positive testing was included in the scope of this test because a Network Firewall that prevents 100% of malicious attacks but also prevents legitimate (non-malicious) actions can be vastly disruptive. SecureIQLab used appropriate tools and techniques to ensure that the tested firewall products do not generate significant numbers of alerts with legitimate applications and processes in an enterprise environment.

This section of the methodology was performed simultaneously and as part of the validation workflow wherever feasible. It was also performed in other independent sections. The goal of this test was to ensure that the firewall products do not prevent malicious traffic at the expense of operational accuracy.

The AT&T Dynamic Defense was tested for operational accuracy under real-world scenarios during the entire test cycle, and Table 5 above showcases that Dynamic Defense resisted false positives throughout testing.

6. Operational Efficiency Validation

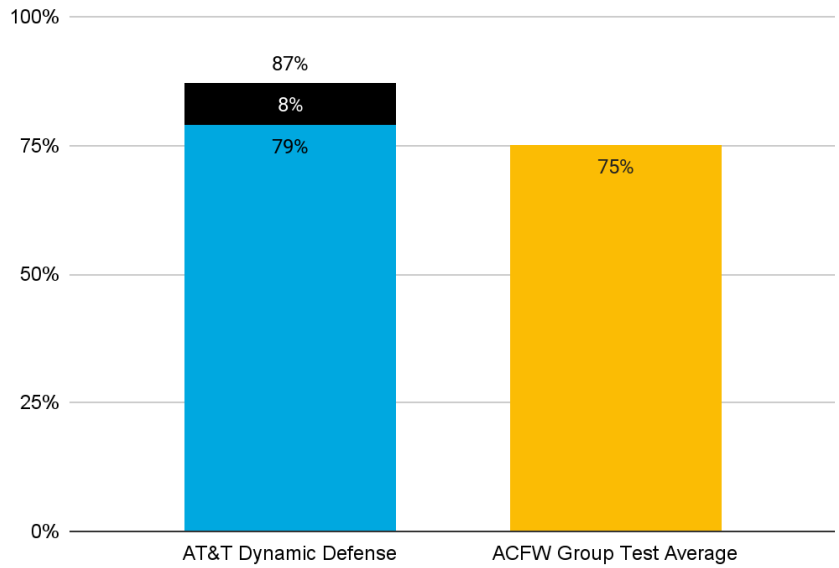

Figure 4. AT&T Operational Efficiency Comparison with Group Average from Recent Public Test

AT&T Dynamic Defenses operational efficiency measures the tested operating burden and complexity of setup and use. As such, the Operational Efficiency Rating measures both the ability of the AT&T Dynamic Defense to detect and respond to cyber-attacks appropriately and ease of use. The operational efficiency was evaluated over the 12 categories listed in Table 6.

Figure 4 illustrates the comparison of Operational Efficiency Ratings between AT&T Dynamic Defense and the ACFW group average. AT&T Dynamic Defense starts with a baseline Operational Efficiency Rating of 79%. Moreover, the integration of AI-driven policy generation enhances this rating by an additional 8%. Furthermore, the firewall's capability to operate effectively out of the box, without requiring any configuration changes, significantly contributes to its improved operational efficiency.

CATEGORIES	AT&T	ACFW Group Test Average
Security policy configuration	High	Medium
Security Policy Management	Low[1]	Medium
Asset Management	Low[1]	Medium
Access Control	High	High
Compliance Management	High	High
Business Continuity Management	High	Medium
Risk Assessment & Mitigation	High	High
Security Metrics Reporting	High	High
Backup & Restore	High	Medium
Analytics	High	Medium
Customer Support	High	High
License Management	High	High

Table 6. AT&T Dynamic Defense vs ACFW Vendors Operational Efficiency Per Category

The features and functions within each category are awarded scores (integers 0 – 10) based on their capabilities. These scores are then tallied together to form a rating of high, med, or low. The Operational Efficiency Rating is equal to the total number of points scored respectively by the AT&T Dynamic Defense operational efficiency validation over the total number of points. Category ratings were awarded by averaging the scores within a category and using the following criteria:

- High or Yes (Green) = 7 - 10 Points
- Med (Yellow) = 4 - 6 Points
- Low (Orange) =1 - 3 Point
- NA/No (Red) = 0 Points

7. Conclusion

Overall test results show that AT&T Dynamic Defense can detect attacks and block malicious URLs and IP addresses before the traffic even reaches the internal network of the business or organization. In terms of a defense-in-depth approach followed by the organizations, having an easily deployable security perimeter like AT&T Dynamic Defense provided by the network service provider will complement the existing defense mechanisms in place.

The Smart Protection policy (AI-driven policy Generation) offered by AT&T Dynamic Defense automates policy creation based on the traffic observed in the network. In our testing, we observed that the automated policy suggested by AT&T's Dynamic Defense was as effective as the custom policy configured by experienced network administrators. Apart from a straightforward and clean dashboard to monitor the network and administer policy, the automated policy generation further simplifies the ease-of-use aspect of the solution. Thereby significantly reducing the effort needed by the network administrators to manually configure the policy from scratch.

Finally, the Insights section extends beyond standard logs and reports by providing advanced capabilities for analyzing and managing network traffic. It offers a comprehensive view of collated traffic data, categorized by port, application, or service, enabling network administrators to easily identify critical traffic patterns. Moreover, it empowers them to take immediate action by adding firewall rules directly from the report screen, streamlining the process of securing the network.

[1] AT&T reports that these categories are on the roadmap for enhancements.

8. Methodology

8.1. Test Infrastructure

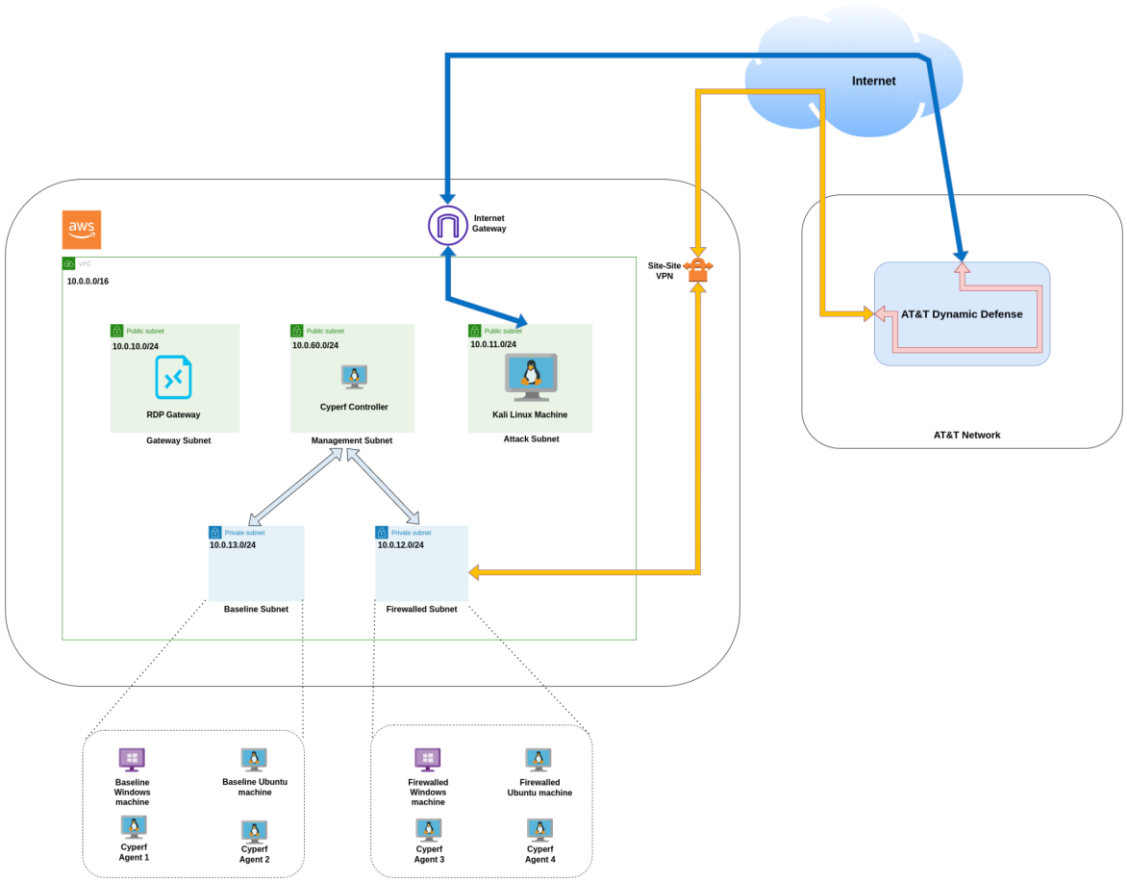

Figure 5. Test Architecture

The test architecture was created and deployed within the AWS environment. Figure 3 provides a diagram of the test architecture. Table 7 highlights certain components of the infrastructure used during testing. Figure 5 above provides an overview of SecureIQLab's test architecture. SecureIQLab ensured that the best practice configurations were used to set up the test network and machines. The site-site VPN and the traffic routing to the AT&T dynamic defense are configured as per the recommended network configuration by the AT&T team. The Ubuntu, Windows, and Kali Linux machines are based on AWS t2.medium configuration. The 4 traffic simulation agents are based on AWS c5.2xlarge configuration.

Operating Systems	Number of Virtual Machines
Ubuntu 20.04 LTS	2
Windows 10 x64 Enterprise Edition	2
Kali Linux (Attacker Machine)	1
Linux x86_64	4

Table 7. Infrastructure Used During Tests

Publicly available best-practice documentation was referred to confirm that the firewall was at least minimally configured to best-practice specifications for all security features/modules ("best-practice or better"). For instance, the default policy for "alert only" configurations were modified to "alert and deny" to ensure the AT&T Dynamic Defense was blocking bad activity. Because product performance is generally highly configuration-dependent, using different settings might yield different results. True positive testing was then performed to confirm the functionality of all configured security policies.

False positive testing was also performed to conservatively tune the policies to what would be appropriate for a typical enterprise. For example, the ability to browse and render general popular websites (e.g., Amazon, Bing, CNN, MSNBC, and Wikipedia) was tested.

The test architecture was designed to evaluate both inbound and outbound traffic flows in the network. The test network is planned in a single VPC with multiple subnets in which various test VMs are deployed. The main subnets used for the test are the Baseline Subnet, the firewall subnet, and the Attack Subnet. The traffic originating from the baseline subnet is routed directly without the interference of the firewall, while the traffic originating from the firewall subnet is routed to the AT&T Dynamic Defense via a Site-Site VPN connection. The attack subnet's traffic is routed to the public IP addresses exposed by the AT&T Dynamic Defense. This ensures that the Dynamic Defense can inspect the inbound simulated malicious traffic. Thus, comprehensively allowing Dynamic Defense to monitor the ingress and egress traffic flows.

The attacker machine was placed within the Attack subnet to conduct a series of targeted exploits. These tests focused on known vulnerabilities, including browser exploits, obfuscated JavaScript, cross-site scripting, and advanced persistent threats. The primary objective was to assess the firewall's capability to inspect and filter traffic between workloads, ensuring it could effectively identify and block these sophisticated attacks.

8.2. Scenarios Tested & Validation Procedure

A business network might contain several key components essential for daily operations, particularly in small to medium-sized businesses (SMBs). These typically include sensitive data and information, such as customer records and financial data, along with IT infrastructure like servers, routers, switches, and potentially cloud services that facilitate connectivity. The network supports various IT systems, including business applications and productivity tools, while connecting user devices such as computers, laptops, and mobile devices.

Given this scenario, it makes sense that a dedicated Internet service provider like AT&T can intercept traffic before it enters the business network and block any malicious activities. By doing so, the provider can proactively filter out threats and prevent them from reaching the internal network, thereby reducing the risk of security breaches and ensuring that sensitive data and critical IT systems remain protected. This early interception helps to safeguard the network from potential attacks, minimizing the need for additional security measures and reducing the overall exposure to cyber threats.

SecureIQLab has simulated various attacks and malicious traffic patterns across different ingress and egress traffic scenarios, including categories such as spyware, malicious URLs, exploits, advanced persistent threats (APT), and data exfiltration. This approach aims to evaluate the product's ability to detect, respond to, and mitigate a wide range of threats, ensuring comprehensive security coverage and consistent performance in real-world conditions.

Additionally, since AT&T offloads the initial security perimeter from the organization's internal network, it is also important to assess how easy it is to use the product. This evaluation helps estimate operational efficiency and confirms that no additional expertise is required from the IT team to set up and maintain the system, addressing the cost concerns that businesses often face.

The Scenarios tested are as follows:

Policy Enforcement: At the most basic level, a firewall should be able to enforce a firewall policy that would restrict or allow a particular traffic flow based on the configured firewall rules. Additionally, AT&T Dynamic Defense is backed by AT&T's threat intelligence as well as next-generation firewall capabilities that allow the network administrator to enable/disable threat detection and mitigation capabilities of the solution.
Vulnerability Exploits: Exploits and browser-based vulnerabilities were used to evaluate the feasibility of obtaining unauthorized access to the system. An internal attacker machine and various vulnerable versions of Google Chrome and Mozilla Firefox were used to execute the attacks
Obfuscated JavaScript Exploits: Attackers use obfuscated JavaScript to make the malicious JavaScript code more difficult to detect and analyze by security tools. Hence, the test included a set of payloads that were obfuscated to evaluate the firewall's ability to identify and block malicious obfuscated script payloads.
Advanced Persistent Threats: APTs are another set of attacks that impact cloud workloads. These attacks are usually carried out from external networks. A set of tests was run with popular APT tools like Cobalt Strike, Covenant, and PowerShell Empire to test the firewall's ability to identify and block ongoing communications with the C2C server.
Post-Exploitation Techniques: Post-Exploitation Techniques aim to exfiltrate the data from the target cloud workloads. To counter this, behaviors that indicate a potential exfiltration must be identified and stopped by the cloud firewall. Specifically, techniques like DNS tunneling and ICMP tunneling are simulated to verify the firewall's ability to detect malicious activities that are carried out with seemingly normal protocols.
Web/URL Filtering: Web and URL filtering are essential tools that help businesses protect against phishing attacks and malicious websites by controlling and monitoring the online content that users can access. A corpus of malicious URLs and IP addresses is used to test the Web/URL filtering capabilities.
IP Blocking: IP blocking is crucial for maintaining robust network security, as it prevents unauthorized access and mitigates cyberattacks, including Distributed Denial of Service (DDoS) attacks. By ensuring that only trusted IP addresses can access the network, IP blocking reduces the risk of breaches and enforces security policies that restrict access to high-risk regions. Therefore, testing this functionality involves accessing known malicious IPs and evaluating the firewall's ability to leverage both threat intelligence and custom rules to block these threats effectively.
Application Control: Testing application control is crucial for enforcing security policies, mitigating cyber threats, and managing unauthorized software within an organization. By allowing only approved applications to run on the network, application control prevents the execution of potentially harmful software, reduces shadow IT, and enhances productivity by blocking non-essential or distracting applications. This test simulates various application traffic scenarios to evaluate the firewall's ability to accurately identify and enforce policies on application usage, ensuring robust protection and efficient network management.
False Positives: False positive testing was also performed to conservatively tune the policies to what would be appropriate/acceptable for a typical enterprise. For example, the ability to browse and render general popular websites (e.g., Amazon, Bing, CNN, MSNBC, and Wikipedia) was tested.
Operational Efficiency: In the context of AT&T Dynamic Defense, operational efficiency is important because it offloads the security perimeter from the internal network. This approach simplifies the deployment and administration of security measures, allowing businesses to implement robust defenses without placing additional strain on their internal IT teams. With AT&T Dynamic Defense, the ease of setup and management ensures that existing IT staff, regardless of their level of expertise, can effectively oversee security operations. Hence, this test evaluates some key parameters that help determine the operational effectiveness of the product.

9. Contact Information

SecureIQLab, LLC.
9600 Great Hills Trail Suite #150W
Austin, TX 78759 USA
+1.512.575.3457
www.secureiqlab.com
info@secureiqlab.com

10. Copyright and Disclaimer

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

SecureIQLab (October 2024)

19 September 2024 revision corrects typos on pages 3 and 4
14 October 2024 revision simplifies Figure 1 and its accompanying descriptive paragraph. Additional description to Figure 2 have been added to its descriptive paragraph.
Branding has been updated throughout the document and AT&T commentary regarding their Operational Efficiency road map has been added.
24 October 2024 revision adds results details to the 2nd paragraph.