APPOSITE TECHNOLOGIES

SOLUTION BRIEF

Network Security Testing

INTRODUCTION

In the ever-evolving landscape of digital threats and vulnerabilities, cybersecurity testing is essential to ensure protection for modern networks and systems.

By emulating real-world attack scenarios, evaluating network infrastructures, and validating security measures organizations can proactively identify weaknesses, mitigate risks, and fortify defenses against potential cyber threats.

CHALLENGES

Safely Simulating Attacks at Real-World Scale: Simulating cyber attacks at a very high volume is essential to mirror real-world scenarios, but doing so without causing actual harm or disruption is a significant challenge. Organizations must test security measures in a closed lab environment to avoid risking damage to the network or data.

Avoiding Network Performance Degradation: Organizations must ensure that security infrastructure can identify and block malicious attacks while still allowing valid traffic to pass through at a rate that does not disrupt the network's performance. A significant volume of traffic and attacks can lead to service disruptions, slowdowns, downtime, or poor user experience even if security is not breached.

Staying Up to Date with Evolving Cyber Threats: Cyber threats are continuously evolving, with new attack vectors, tactics, and vulnerabilities emerging regularly. That's why is it is important to find a test solution that maintains an up to date catalog of attacks, to ensure security devices and test methodologies remain effective.

Apposite Test Capabilities

Comprehensive network security tests to evaluate the effectiveness of detecting and stopping security threats

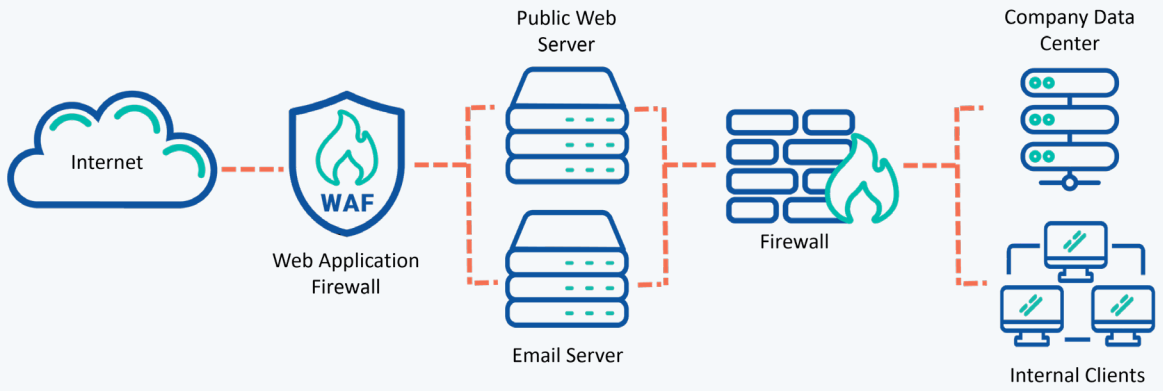
Evaluate the performance of key security devices:

- Next-gen firewalls
- Web application firewalls
- DDoS mitigation systems
- MDR/XDR detection and response systems

Generate a mix of legitimate and malicious traffic at tremendous scale

Ever-expanding Attack Library with 10K+ attacks

TYPICAL NETWORK SECURITY ARCHITECTURE



KEY TESTING AREAS

Evaluating Performance of Security Devices

Continuous testing of security devices such as firewalls, Web Application Firewalls (WAFs), Intrusion Detection Systems (IDS), and Managed Detection and Response (MDR) solutions is critical. This involves examining their effectiveness in filtering and blocking malicious traffic, preventing unauthorized access, and detecting and responding to security incidents. But it also includes measuring their ability to continue letting valid traffic pass through without degrading network and application performance.

Benchmarking the performance of security devices prior to an attack enables more efficient detection of anomalies. Testing with both malicious and valid application traffic helps assess how well these devices handle different types of threats and traffic loads, and increases attack readiness.

Emulating a Variety of Attack Types

Comprehensice cybersecurity testing involves simulating a diverse range of attack types to assess the resilience of network defenses. This includes emulating malware, phishing attempts, spyware, viruses, and common vulnerabilities and exploits (CVEs) in a secure environment to avoid disrupting or corrupting the production network.

By mimicking real attack scenarios, and staying current with evolving cyberthreats, organizations can identify vulnerabilities and weaknesses before they are exploited by an attacker.

Simulating Attacks on Layers 2-7

Understanding the differences between layers is crucial for designing comprehensive security strategies that cover the entire network stack. For example, layers 2-3 attacks focus on network-level vulnerabilities, targeting infrastructure and routing, and may cause network disruption or unauthorized access, while layers 4-7 attacks target higher-level protocols, applications, and user interactions and often aim at compromising data, user sessions, or application functionality.

By generating attacks and testing security at each layer, organizations can identify potential entry points for attackers and fortify defenses accordingly.

DDoS Prevention and Mitigation

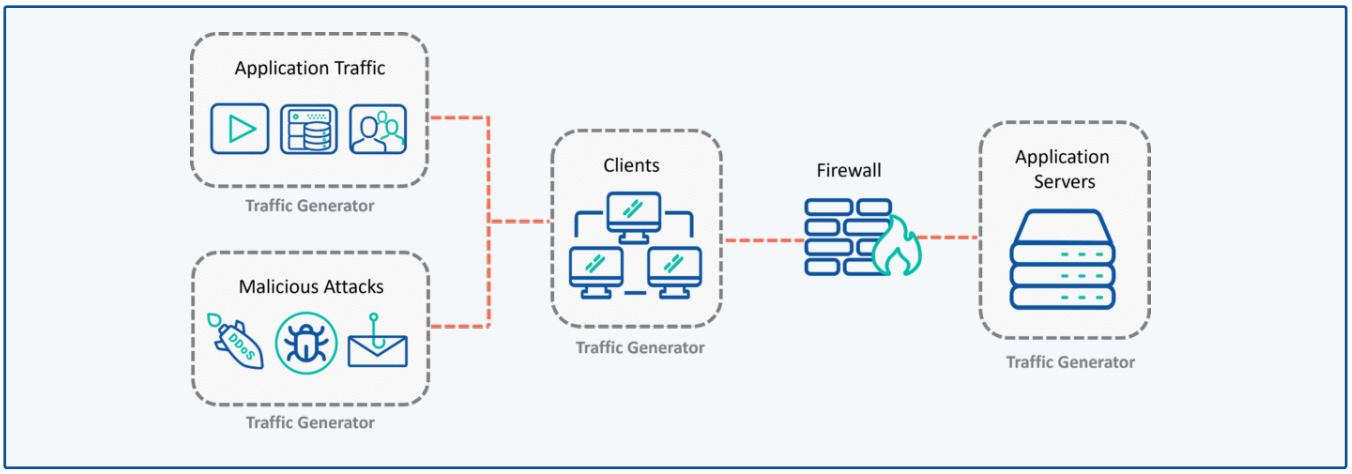
Simulating Distributed Denial of Service (DDoS) attacks is essential to evaluate the effectiveness of DDoS prevention and mitigation strategies. Testing involves generating large volumes of traffic to overwhelm network resources and assess how well DDoS protection mechanisms can detect and mitigate the impact of such attacks. This includes analyzing the ability to identify legitimate traffic amidst the flood of malicious requests and maintain service availability.

Using a tool to emulate large scale DDoS attacks allows security teams to observe how their systems respond under simulated attack conditions, and optimize devices aimed at preventing and mitigating these attacks.

APPOSITE SECURITY TEST SOLUTION HIGHLIGHTS

- An evergreen library of cyber attacks that is constantly updated to include the latest CVEs, malware, viruses etc.
- Support for malicious and valid application traffic
- Security attacks that target layers 2-7
- An intuitive search engine to find CVEs based on vendor name, CVE number, or type of attack
- Browser-based GUI that is platform agnostic
- Interface speeds 1Gbps, 2.5Gbps, 5Gbps, 10Gbps, 25Gbps, 40Gbps & 100Gbps
- Virtual Editions: VMWare, KVM
- Cloud Editions: AWS, Google Cloud, Azure
- Automation through comprehensive RESTful API

TESTING FIREWALL PERFORMANCE



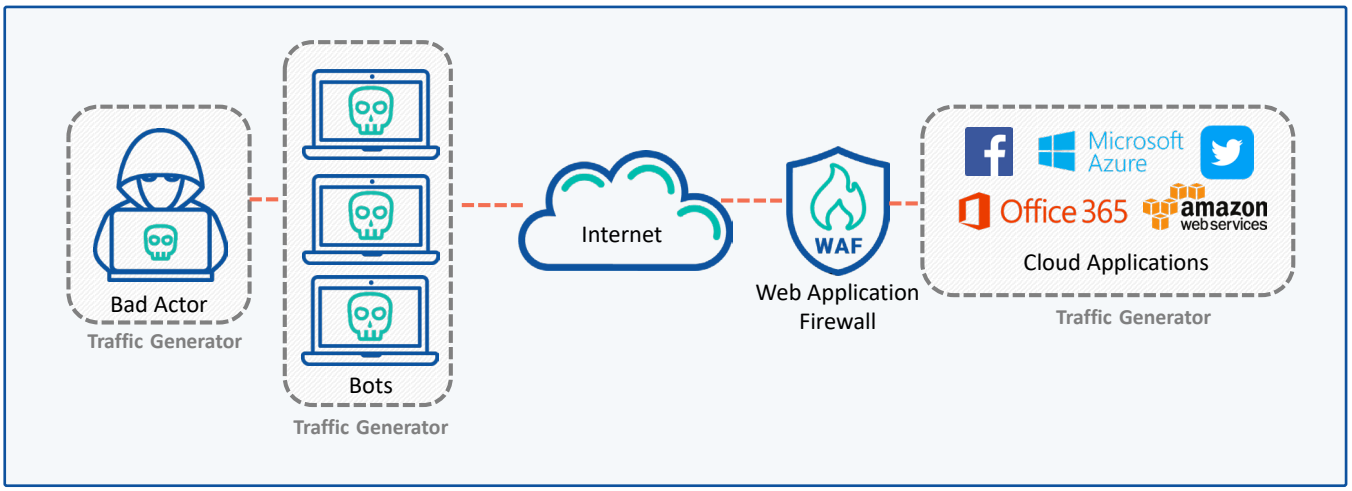
A firewall has three main jobs: to identify traffic types, let legitimate traffic through , and block illegitimate traffic and attacks. Traffic generators can validate the effectiveness of firewalls by simulating various traffic types including both regular application traffic and malicious attack traffic, such as malware, viruses, and common vulnerabilities and exposures (CVEs).

Use the traffic generator to evaluate the firewall's ability to detect and block common security threats and measure the firewall's performance in terms of throughput, latency, and packet loss to ensure it allows valid traffic through at a rate that does not recduce network or application performance.

Another important consideration when testing firewalls, is session testing. When the firewall is overwhelmed with sessions, its ability to process requests slows down, resulting in performance degradation. By using a traffic generator to set up and tear down TCP and UDP sessions at a high very high rate you can:

- Assess the firewall's session limitations
- Determine the maximum number of simultaneous connections it can withstand
- Measure how fast the firewall is setting up and tearing down sessions
- Recognize and resolve issues that arise in real-world scenarios

TESTING AGAINST DDOS ATTACKS



Web Application Firewalls (WAFs) can be great tools for preventing DDoS attacks, but they must be tested to verify performance. Using a traffic generator, simulate DDoS attacks by generating a large scale of bot traffic from different regions simultaneously. Attacks can be launched against actual devices like WAFs, by using IP addresses, or a simulated target to avoid disrupting production defenses. They can also be used to evaluate a prospective new solutions prior to purchase.

DDoS attacks are now targeting every layer of the network including the application layer, so it is especially important to be able to simulate multi-layer attacks such as:

- Layer 7, Application Layer or HTTP Flooding
- Layer 3-4, UDP Amplification
- DNS Flooding

Test protection, alert, and mitigation of DDoS attacks by creating realistic attack scenarios. A good test solution should allow for configuration of specific details of the attack including the regions it's launched from, the number of compromised devices, how fast the attack ramps up, and how often it repeats.

SUMMARY

Cybersecurity testing is a vital component of digital defense. The proactive identification, evaluation, and fortification of security measures is the best way to counter the relentless evolution of cyber threats. By emulating real-world attack scenarios, scrutinizing vulnerabilities across network layers, and assessing the efficacy of security devices and protocols, organizations can protect themselves against potential breaches and disruptions. Conducting these tests with knowledge and access to the most current cyber threats and CVEs helps identify weaknesses, fine-tune defenses, and better protect networks from the ever-evolving threat landscape.

SOLUTION OVERVIEW

ATTACK LIBRARY

- Generate legitimate application traffic and malicious attacks simultaneously
- Validate DDoS defenses, protect against zero-day attacks, and increase attack readiness
- Optimize security devices and systems such as next-generation firewalls, WAFs, MDR Solutions, IPS and IDS systems, and SD-WAN gateways
- Emulate large-scale botnet attacks to stress test your network and discover hidden weaknesses
- Simulate realistic threat scenarios for cyber range training environments

Attack Library and Traffic Generators

Apposite's Attack Library consists of 10k+ cybersecurity threats including viruses, malware and other attacks for comprehensive network security testing. By ensuring our solution is always up to date, it delivers the cutting-edge intelligence needed to protect your network and devices from ever-evolving cybersecurity threats.

Apposite's Attack Library integrates seamlessly with our AppStorm and AppPlayback traffic generation solutions to deliver unmatched ease of use. By simulating real-world attacks and valid application traffic at scale, organizations can optimize security devices like next-generation firewalls, validate DDoS defenses, improve security performance, and ensure network resiliency.

Supported Threats

- Fuzzing
- Backdoor
- DoS
- Exploits/Vulnerabilities
- Generic
- Reconnaisance/Spyware
- Malware/Ransomware
- Worms/Viruses

WHY APPOSITE?

Apposite has been in business for over 15 years and has helped customers around the globe from telecoms to system integrators, technology vendors and large enterprises. Our modern, easy-to-use test solutions enable teams to set up performance tests quickly and easily and trust the results.

Apposite Technologies

4223 Glencoe Ave b121, Marina del Rey, CA 90292 USA

www.apposite-tech.com | TEL: 1.310.477.9955 | info@apposite-tech.com