Strengthen Your Defenses:

A Guide to DDoS Testing

Author: Michael Smith

WHITE PAPER

Strengthen Your Defenses: A Guide to DDoS Testing

Distributed Denial of Service (DDoS) attacks can undermine availability with little warning, affecting revenue, customer trust, and operational continuity. The most common failure point is not a lack of tools, but untested processes: unclear decision authority, slow diversion, incomplete coverage of new services, or mistuned application controls.

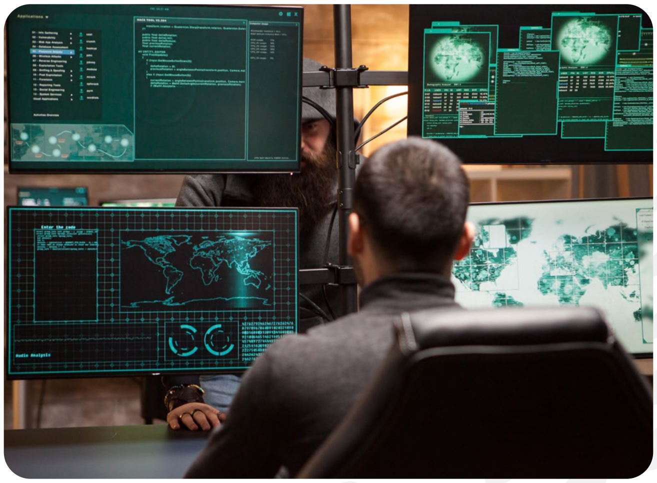
Routine DDoS testing provides measurable assurance that people, procedures, and technology work together under real-world conditions. In the sections that follow, we describe four core testing types—tabletop, diversion, simulation, and application-layer—and how to use them to strengthen resilience.Why You Should Perform DDoS Testing

DDoS activity can fluctuate significantly over time, creating periods of relative quiet followed by concentrated attack campaigns. These shifts make it difficult to rely on historical trends when assessing risk.

Reactive defenses are not sufficient on their own. Infrastructure changes, configuration drift, and evolving attack techniques can introduce gaps that remain invisible until an incident occurs. Proactive testing helps identify those gaps before they affect availability.

Regular DDoS testing validates detection accuracy, traffic diversion procedures, mitigation capacity, and incident response coordination. It confirms that monitoring tools trigger appropriately, escalation paths are clear, and teams can execute under pressure.

By testing consistently, organizations reduce recovery time, minimize operational disruption, and maintain confidence that defensive controls will perform as intended during a real-world event.DDoS Tabletop Exercise: Strategic Planning and Coordination



Understanding and Evaluating Tabletop Exercises

A tabletop exercise simulates a DDoS incident through structured discussion rather than live traffic. Its purpose is to evaluate decision-making, escalation, and cross-functional coordination under realistic conditions.

These exercises test whether incident response plans are actionable, roles are clearly defined, and communication flows effectively across IT, security, leadership, legal, communications, and external partners. They also validate regulatory reporting readiness and stakeholder communication during service disruption.

By exposing gaps in authority, timing, or coordination before a real event occurs, tabletop exercises strengthen overall response maturity. Running Effective Tabletop Exercises

- Align scenarios to business risk. Base exercises on realistic threats targeting critical systems and services.
- Include all response stakeholders. Involve IT, security, legal, communications, executive leadership, and relevant external partners.
- Simulate in phases. Present the scenario in stages, requiring teams to make decisions as conditions evolve.
- Document gaps in real time. Capture unclear roles, escalation delays, communication breakdowns, and procedural weaknesses.
- Assign corrective actions. Establish ownership and timelines to address identified gaps.
- Repeat regularly. Conduct exercises on a defined cadence and introduce new variables to reflect infrastructure and threat changes.

Strategic Exercise Injects

Effective tabletop exercises incorporate realistic complications that test your organization's adaptability. Consider scenarios where primary communication channels become unavailable, key personnel are unreachable, or attacks target multiple systems simultaneously.

Other valuable injects include the following:

- Hacktivists announce that your organization is a target
- Network saturation reaches 95% of capacity
- Outage of a critical website
- Media inquiries about loss of availability
- Loss of control at the network layer
- Data breach concurrent with DDoS attack
- Attacks that coincide with other business-critical events or system maintenance windows
- DDoS attack on an undefended marketing campaign website
- A traffice surge that is a legitimate flash crowd rather than a malicious attack
- Regulatory reporting requirements under time pressure
- DDoS attack during a major company launch/event

Managing “Lessons Learned”

Post-exercise reviews play a crucial role in improving your organization's incident response strategy. Gather the key stakeholders shortly after the exercise for a debriefing session to discuss findings and document lessons learned. Focus on identifying what went well, what challenges arose, and where improvements are needed. Ensure action items are assigned to specific team members, and set deadlines for implementing changes. Regularly revisit recommendations to track progress and verify that adjustments are effective in enhancing your overall resilience. By integrating continuous learning into your process, your organization will be better equipped to respond to future threats.

Diversion Test: Validating Traffic Management

Understanding Diversion Testing

A diversion test validates your organization's ability to redirect network traffic to a DDoS mitigation provider before an attack can overwhelm your primary systems. It confirms that rerouting mechanisms (e.g., DNS or BGP changes) execute correctly and within defined time thresholds.

The objective is simple: ensure traffic can be redirected quickly and without unintended service disruption.What Diversion Tests Validate

Diversion testing measures:

- Rerouting speed once attack conditions are detected
- Mitigation capacity to handle expected traffic volumes
- Service continuity for legitimate users during diversion
- Monitoring accuracy and alerting triggers
- Operational readiness of teams executing the diversion

It also provides an opportunity to validate automation and reduce reliance on manual intervention.

Diversion Test Process

- Coordinate with your mitigation provider and schedule during lower-traffic periods.
- Define measurable success criteria, including diversion time, latency thresholds, packet loss, and user impact.
- Initiate traffic diversion to scrubbing infrastructure. Monitor performance in real time, documenting timing, configuration changes, and operational issues.
- Conduct a structured post-test review to refine routing procedures and address gaps.

Validating Scrubber Effectiveness

During diversion tests, closely monitor how your scrubbing infrastructure processes different types of traffic. Verify that malicious traffic is filtered effectively while legitimate traffic passes without degradation.

Test various traffic patterns and volumes to ensure your scrubbing capacity matches your organization's actual needs. This validation prevents situations where your mitigation infrastructure becomes overwhelmed during real attacks.

DDoS Attack Simulation Test: Real-World Validation

Understanding Attack Simulation

Attack simulation testing uses controlled DDoS traffic to evaluate defensive performance under realistic conditions. These tests replicate attacker techniques while remaining coordinated and contained.

The goal is to validate detection, mitigation, and recover capabilities across technology and response teams.

What Attack Simulation Tests

Simulation testing evaluates:

- Detection speed across monitoring and alerting systems
- Mitigation effectiveness against multiple attack vectors (volumetric, protocol, application-layer)
- Service availability during active attack conditions
- Recovery time after traffic subsides
- Incident response coordination and escalation execution

Testing can also establish baseline traffic patterns to refine protection thresholds.

The Process for DDoS Simulation Testing

A structured approach to DDoS testing ensures effective results while minimizing risks. Below are the key steps involved:

Planning

Start by clearly defining the goals of your test. Are you testing your system's ability to handle increased traffic, identifying weak points in your infrastructure, or evaluating the effectiveness of your mitigation strategies?

Determine the types of DDoS attacks to simulate, such as volumetric, protocol, or application-layer attacks, and identify the specific systems, applications, or networks to target. If you have staging infrastructure or applications that mimic your production systems but don't have customer traffic on them, it is a good practice to test against this.

You can also install non-customer facing “victim” applications that the test can be run against.

Clearly outline the metrics you will measure (e.g., system performance, recovery time, or impact on user experience). Get approval from all relevant stakeholders, including IT leadership, compliance teams, and legal advisors, and ensure the test aligns with regulations and organizational policies to avoid any unintended consequences.

Preparation

Gather the necessary tools and resources to conduct the test. This could involve using in-house tools, hiring third-party services that specialize in DDoS simulations, or leveraging cloud-based solutions designed for stress testing. Verify that all systems and monitoring tools such as availability monitoring and network utilization monitoring are functioning properly so you can accurately collect data during the test.

Coordination

Before executing the test, notify all relevant teams, including IT, security, help desk, and any business units that might be impacted by the test. Schedule testing for a time when you have less user traffic to minimize service disruptions. Clearly communicate the test schedule, scope, specific objectives, and any potential disruptions that could occur. For example, if the test could temporarily affect a customer-facing system, make sure customer support teams are prepared to manage inquiries. Coordination ensures alignment across the organization, reduces confusion, and prevents unnecessary panic during the test. If possible, designate a point of contact for each team to streamline communication throughout the process.

Execution

Conduct the DDoS test according to your pre-defined plan. Use the tools you prepared to simulate realistic attack scenarios, whether they involve overwhelming your servers with traffic or exploiting protocol vulnerabilities. Continuously monitor network and system performance throughout the test to gauge the impact and your ability to mitigate the attack. Pay close attention to the behavior of your mitigation tools, such as firewalls, load balancers, or intrusion detection systems, and document how they respond to the attack. If any unexpected outages or issues occur, stop the test that is causing the problem and take note of the conditions to address them during the analysis phase.

Analysis

After the test, review the results in detail to identify any weaknesses in your DDoS mitigation strategies. Analyze system logs, performance metrics, and response times to determine how well your defenses held up against the simulated attack. Look for bottlenecks, unresponsive systems, or gaps in your detection mechanisms. Use the data to make targeted improvements, such as updating configurations, implementing new security tools, or refining response protocols. Compare the results to your initial objectives to measure the test's success.

Post-Test Review

Hold a debriefing session with all relevant stakeholders including your mitigation service provider to review the findings, discuss lessons learned, and agree on next steps. Share both successes and areas for improvement to ensure a comprehensive understanding of your organization's DDoS resilience. Document the test results, including any vulnerabilities discovered, actions taken during the test, and recommended changes to your systems or processes. Use this documentation to inform future testing efforts, refine your security posture, and better prepare your organization for real-world DDoS attacks.

Application-Layer DDoS Testing: Advanced Threat Protection

Understanding Application-Layer Testing

Application-layer DDoS testing evaluates attacks that target web applications, APIs, and services rather than the underlying network infrastructure. Unlike traditional volumetric attacks that overwhelm networks with massive amounts of traffic, these attacks often mimic legitimate user behavior and are designed to exhaust application resources without triggering volumetric thresholds.

The objective is to validate that application-layer controls detect and mitigate malicious activity without disrupting legitimate users.

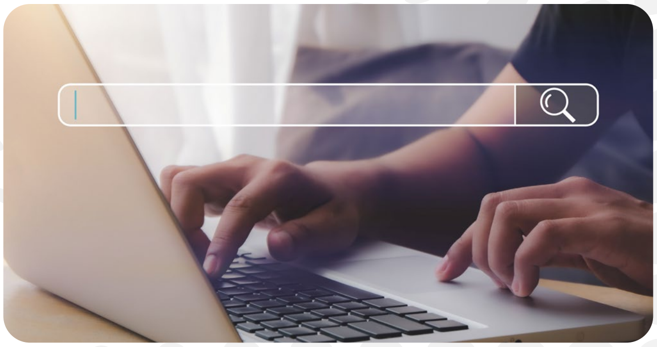
Application-Layer Test Objectives

Testing should validate:

- Accurate differentiation between legitimate user behavior and malicious request patterns
- Rate-limiting effectiveness under burst and distributed low-rate conditions
- WAF detection accuracy, including signature-based and behavioral analysis
- False positive rates to ensure legitimate users are not blocked
- Performance stability during sustained application-layer pressure

Testing HTTP Rate Controls

Evaluate how your systems handle sudden spikes in HTTP requests, as these could signal potential application-layer attacks aimed at overwhelming your infrastructure. Test various request patterns to simulate real-world attack scenarios, including rapid-fire requests from single sources and more sophisticated, coordinated low-rate attacks originating from multiple sources. These scenarios can help identify vulnerabilities that might otherwise go unnoticed.



Ensure that your rate limiting controls are configured to activate appropriately under these conditions, effectively mitigating malicious traffic while still allowing legitimate users to access your applications without interruption. It's crucial to strike the right balance—blocking harmful requests without inconveniencing genuine users.

Additionally, monitor for false positives during testing to ensure that legitimate traffic isn't mistakenly flagged or blocked by your security measures. Regularly review your system's performance under these conditions, as well as your logging and alerting mechanisms, to ensure you can quickly detect and respond to abnormal patterns and maintain seamless service during potential attacks.

WAF and CDN Validation

Test your web application firewall (WAF) to ensure it can effectively identify and block malicious requests while still allowing legitimate traffic to flow through without interruption. Assess its signature-based detection capabilities to detect known attack patterns and evaluate its behavioral analysis features to identify and mitigate more sophisticated or evolving threats. Additionally, confirm that your WAF can adapt to new vulnerabilities and provide customizable rules for fine-tuned protection.

Validate that your content delivery network (CDN) is capable of absorbing and filtering attack traffic, preventing it from overwhelming your origin servers. Test the CDN's caching effectiveness to ensure that static content is delivered seamlessly during high-traffic periods or attacks. At the same time, verify that dynamic content remains accessible and properly routed to users, even during incidents, maintaining an uninterrupted experience for legitimate visitors.

Implementing Comprehensive DDoS Testing

Effective DDoS testing requires an ongoing, risk-aligned strategy rather than isolated exercises. Begin with tabletop sessions to validate roles and execution paths, then progress to diversion and simulation testing to confirm technical controls perform as expected.

Establish a recurring testing cadence tied to business risk, infrastructure changes, and continuity planning. Carefully document results, track remediation efforts, and measure improvement using defined metrics such as detection time, diversion speed, mitigation effectiveness, and recovery duration.

Engage qualified third-party security professionals where appropriate to provide independent validation and identify blind spots. Integrate testing outcomes into broader disaster recovery and business continuity planning to strengthen overall operational resilience.

Introducing DigiCert UltraDDoS Protect

DigiCert UltraDDoS Protect is a robust solution designed to help organizations safeguard their infrastructure against the growing threat of distributed denial-of-service (DDoS) attacks. By leveraging advanced traffic monitoring, real-time data analysis, and scalable mitigation tactics, UltraDDoS Protect ensures your systems stay online even under heavy attack. Its cutting-edge technology identifies malicious traffic patterns quickly, blocking them before they can disrupt operations, all while allowing legitimate users uninterrupted access. With DigiCert UltraDDoS Protect, you can strengthen your defenses and build confidence in your ability to respond to and recover from DDoS attacks effectively.

Protecting Web Applications with UltraWAF

For organizations seeking an additional layer of protection, DigiCert offers the UltraWAF (Web Application Firewall) module. UltraWAF complements UltraDDoS Protect by safeguarding web applications against a wide range of threats, including application-layer DDoS attacks, SQL injection, cross-site scripting (XSS), and zero-day vulnerabilities.

This advanced module provides granular traffic inspection, ensuring only legitimate requests reach your applications while malicious payloads are effectively neutralized.

UltraWAF integrates seamlessly into your existing security framework, offering robust policy customization and automated responses to DDoS attacks. By incorporating UltraWAF alongside UltraDDoS Protect, you can ensure comprehensive protection for both your network and web applications, delivering an unrivaled defense against evolving cyber threats.

UltraDDoS Protect's DDoS Testing Policy

Here at DigiCert, we encourage you to test your network, services, and websites to ensure they remain robust under any circumstances. Our generous DDoS testing policy, described in the service guide for UltraDDoS Protect, allows you to evaluate the full capabilities of UltraDDoS Protect against simulated attacks. By conducting these tests, you can gain confidence in the protection we provide, ensuring your systems are equipped to handle real-world scenarios. Testing not only validates the effectiveness of our solution but also helps identify areas for optimization, ultimately enhancing your overall resilience.

If you're interested in scheduling a DDoS test or have any questions about protecting your systems, we're here to help. Contact us today to discuss your needs and learn how UltraDDoS Protect can safeguard your organization from evolving threats. And if you are a customer already, you can request a test in any of the following ways:

1. Log into the UltraSecurity Support Portal - security.ultraproducts.support/hc/en-us

2. Email us at ultrasecuritysupport@vercara.com

3. Call our toll free number: +1 (844) 929-0808 Select option 1 > option 1 For international customers call: +1 540-835-5462.

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management, to secure infrastructure, software, devices, messages, AI content and agents. Learn why more than 100,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com.