SpectraSecure for DDoS Resilience Testing

Verifying Resilience to DDoS Attacks

HIGHLIGHTS

Ease of Use

SpectraSecure's web interface allows authorized users to create DDoS attack scenarios quickly and easily. Built-in Threat Vectors include configurable attack profiles and bandwidth settings.

Flexible Deployment

SpectraSecure can be deployed on virtual machines for maximum flexibility, or on a COTS server with an optional high-performance NICs for high bandwidth testing from a single instance.

DevOps Ready

Use SpectraSecure's REST API to automate DDoS mitigation testing in your DevOps environment.

Multi-Vector

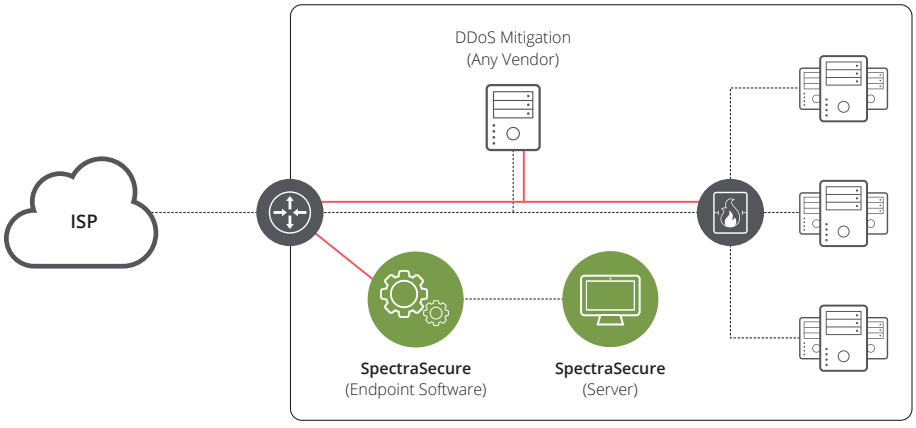
Test resilience to complex DDoS attack scenarios using SpectraSecure's built-in attack vectors and your own custom attack profiles.

Distributed Denial of Service (DDoS) attacks can target any application or service that is reachable from the internet . Web servers, DNS servers, routers, session border controllers, and many other services are constantly subject to attack. Identifying and mitigating these attacks is done using on-premises solutions, cloud-based solutions, or a hybrid solution combing both.

DDoS mitigation is not static. With the power, sophistication, and frequency of DDoS attacks rising, DDoS mitigation must continually evolve in order to protect against the latest attack scenarios. But how can you be sure you are protected? Waiting for an attack to happen to test your resilience is a risky proposition. NETSCOUT's SpectraSecure solution helps you eliminate that risk.

The NETSCOUT Solution for DDoS Mitigation Testing

SpectraSecure tests DDoS resilience in a controlled manner using configurable threat vectors that can mimic the malicious traffic launched by botnets. SpectraSecure utilizes test-botnets to simulate real-world attack scenarios in a customer's controlled environment. Using SpectraSecure, you can validate the resilience of any potential target, including networks, applications, and services. Test attacks launched by SpectraSecure appear massively distributed, even when the test-botnet consists of a small number of Virtual Machines. A single test using a volumetric attack vector may appear to originate from millions of unique endpoints.



War Games

Although traditional lab testing is essential, it cannot assess the organizational readiness required for holistic DDoS attack mitigation. Conducting war games is one of the best ways to verify that the teams, tools, and processes will all be on the same page when an attack occurs.

Blacklist Verification

Maintaining a blacklist of source addresses can present a challenge. Use SpectraSecure in the lab to verify the target can handle high volume DDoS attacks from blacklisted sources. In a production network, SpectraSecure can launch low-bandwidth attacks to verify that blacklisted packets are handled properly.

Deep Packet Inspection Testing

Solutions that use Deep Packet Inspection (DPI) to identify attacks require test traffic with specific content at the application layer. Using SpectraSecure, simulated attacks can contain a mix of traditional attack vectors and packets that contain application-specific content to trigger DPI-based filters.

Notification Testing

Identifying and mitigating DDoS attacks often involves automatic notification of staff and external systems. Use SpectraSecure to verify these critical steps are occurring as required.

Multi-Vector and Custom Attacks

Use SpectraSecure to stay ahead of threat actors by verifying resilience to multi-vector attacks and custom attack scenarios. SpectraSecure's built-in attack vectors can be modified and combined together to create unique scenarios that exercise all aspects of a mitigation system.

Deployment Options

DDoS Resilience testing with SpectraSecure requires the following components:

Component	Description
SpectraSecure Server	Provides the Web interface, handles REST API commands, and controls the SpectraSecure Endpoint Emulator(s) that serve as the test botnet. No test traffic comes from SpectraSecure Server. A single instance of SpectraSecure Server is required.
SpectraSecure Endpoint Emulator	Emulates a botnet under the control of SpectraSecure Server. One instance of SpectraSecure Endpoint Emulator is required. By combining multiple instances of SpectraSecure Endpoint Emulator running VMs or dedicated servers, users can test high bandwidth DDoS attack scenarios.

TEST SCENARIOS

Testing in the Lab

Lab testing provides a controlled environment to verify DDoS resilience of applications and standalone mitigation systems. Use SpectraSecure's web-based interface to create new attack scenarios and launch them using a high-performance server or one or more VMs to emulate botnets.

Automated Testing and DevOps

Make DDoS resilience testing part of your normal test cycle by integrating SpectraSecure into your DevOps test process. SpectraSecure's REST API makes it a natural fit for automated testing.

Built-in Attack Vectors

Attack Vector	Description
ACK Flood	Flood a target with TCP packets that have the SYN and ACK flags set
BROBOT	Establish TCP sessions with the target and send HTTP GET messages with "AAAAAAA"
CHARGEN	IPV4 Amplification attack using the CHARGEN protocol where all packets are sent using UDP with a source port of 19
DNS Amplification	Flood the target with DNS requests
DNS Flood	Attack a target by repeatedly sending the target the same legitimate DNS query
HTTP Slow	Establish TCP sessions with the target and repeatedly send HTTP GET requests
HTTP Load	Establish TCP sessions with the target and generate a high volume of legitimate and unique HTTP GET requests
ICMP Flood	Send a high volume of ICMP Echo Reply packets to the target
Random GET	Flood the target with HTTP GET messages containing a random sequence appended to the selected URI
NTP Flood	Use the NTP protocol to flood the target
Protocol Flood	An amplification attack where TCP, UDP, or ICMP packets flood the target
TCP RST Flood	An amplification attack where TCP RST messages flood the target
SIP Flood	Use the SIP protocol to flood the target with legitimate SIP messages
SNMP Amplification	Use the SNMP protocol to flood the target
SSDP Amplification	Use the SSDP protocol to flood the target
TCP SYN Flood	An amplification attack where TCP SYN packets are used to attack the target
Tor's Hammer	Establish TCP sessions with the target and send legitimate HTTP POST messages
TCP Space Flood	Establish TCP sessions with the target and send messages containing only " "
TCP Confusion Flood	Flood the target with TCP packets that have all flags set

Custom Attack Vectors

Built-in attack vectors are supplied in XML format and can be customized to meet specific test requirements.

SpectraSecure SERVER

Minimum Specifications

	COTS Server or VM
OS/Hypervisor	Windows x64
Memory	24 GB
Processor	8 cores @ 2.4GHz
Disk Space	64 GB
Network Interfaces	1 Ethernet interface required

SpectraSecure ENDPOINT SOFTWARE

Minimum Specifications

	COTS Server or VM
OS/Hypervisor	Windows x64, Ubuntu 16.04
Memory	24 GB
Processor	4 cores @ 2.4Ghz
Disk Space	32 GB
ODBC Driver	ODBC Driver 13 for SQL Server
Network Interfaces	1 Ethernet interface required for management 1 or more Ethernet interfaces required for test traffic. Interfaces used for test traffic cannot be used for management. Optional High-Performance 1/10G Network Interface Card (NIC) available from NETSCOUT®

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

TOPDS_013_EN-1901 07/2019