

## Modern Denial of Service Protection



## What is a Denial of Service Attack?

A Denial of Service (DoS) attack is generally defined as a network-based attack that disables one or more resources, such as a network router or server. These attacks may crash servers, tie up services or consume all available network bandwidth, sometimes hampering a network for days to months.

DoS attacks range in complexity. Some attacks are simple in design, such as sending a relentless stream of data. Other attacks have complex logic to break past firewalls and fool network security systems, such as intentionally crafted packets sent in a specific order that target specific vulnerabilities in a network. A Distributed DoS (DDoS) attack uses multiple attacker machines to disable a target.

### Cost to an Organization

DoS attacks threaten any organization with computers connected to a network. Some of the more highly publicized DoS attacks against eBay, Yahoo!, CNN.com and buy.com lasted for extended periods of time, ranging from hours to months. This is not unusual, and occurs frequently against less publicized targets. These attacks can cripple on-line services and create dissatisfied customers. In some cases, attacks with less than 2,000 packets per second are able to disable servers and interrupt services.

During a DoS attack, customers typically experience poor response times and service. The attack incurs costs associated with the degraded service and lost productivity and business. For an e-commerce site like eBay, one day of downtime due to a DoS attack costs approximately 5.5 million dollars in lost revenue. These attacks not only inconvenience potential shoppers, but they engender a loss of faith in the service dependability and corporate identity of an organization.

### How Attacks are Conducted

DoS attacks can vary greatly in their method, ranging from a single packet attack that crashes a server to a coordinated flood attack from multiple hosts. A carefully crafted packet that exploits a known operating system or application vulnerability can be sent through the network to cause a buffer overflow that disables a server and any associated services it performs. A more sophisticated approach makes use of dozens or even thousands of coordinated hosts to attack a single target. Hackers pride themselves in the number of machines, known as zombies, that they have succeeded in compromising and placing under their control. By loading attack scripts on these machines, they can stage large coordinated attacks. As more and more PCs get broadband access from homes, the field of potential zombies has increased dramatically. The sophistication and barrier to launching these DDoS attacks has been greatly reduced through the availability of packaged tools (e.g., Tribe Flood Network and Stacheldrucht) that are freely available on the Internet.

*The goal of Denial of Service (DoS) attacks is to render a network service incapable of communicating by flooding connections and hampering services.*

*Some of the typical DoS attacks include the following:*

- TCP SYN Floods
- TCP Established Connection Attacks
- Worms like Slammer

*For an e-commerce service provider like eBay, one day of downtime due to a DoS attack costs approximately 5.5 million dollars in lost revenue.*

## TippingPoint's Solution

In response to the mounting threat of DoS and DDoS attacks, TippingPoint Technologies has carefully investigated the attack methods attackers employ. The UnityOne™ sits in-line to protect a network and the hosts connected to it by examining every bit of traffic that passes through it and filtering out unwanted traffic. The UnityOne filtering mechanisms include flow filters that detect and block DoS attacks, statistical traffic anomaly filters which can block DDoS attacks, threshold enforcement filters which can shape and mitigate DDoS attacks and SYN flood protection filters to protect against bogus connections and process table overflows. This white paper describes the different types of DoS attacks and further details the solutions provided by the UnityOne Intrusion Prevention Systems and Appliances.

## TCP SYN Flood

One of the most common types of DoS attack is the TCP SYN flood. This attack can be launched from one or more attacker machines to disable access to a target server. The attack exploits the mechanism used to establish a TCP connection. Every connection requires the completion of a three-way handshake before it can pass data:

- **Connection Request** — First packet (SYN) sent from the requester to the server, starting the three-way handshake
- **Request Acknowledgement** — Second packet (SYN+ACK) sent from the server to the requester
- **Connection Complete** — Third packet (ACK) sent from the requester back to the server, completing the three-way handshake

The attack consists of a flood of bogus SYN packets with spoofed source addresses. The spoofed source address causes the target server to respond to the SYN with a SYN-ACK to an unsuspecting or nonexistent source machine. The target then waits for an ACK packet from the source to complete the connection. The ACK never comes and ties up the connection table with a pending connection request that never completes. The table will quickly fill up and consume all available resources with bogus requests. While the number of connection entries may vary from one server to another, tables may fill up with only hundreds or thousands of requests. The result is a denial of service since, once a table is full, the target server is unable to service legitimate requests.

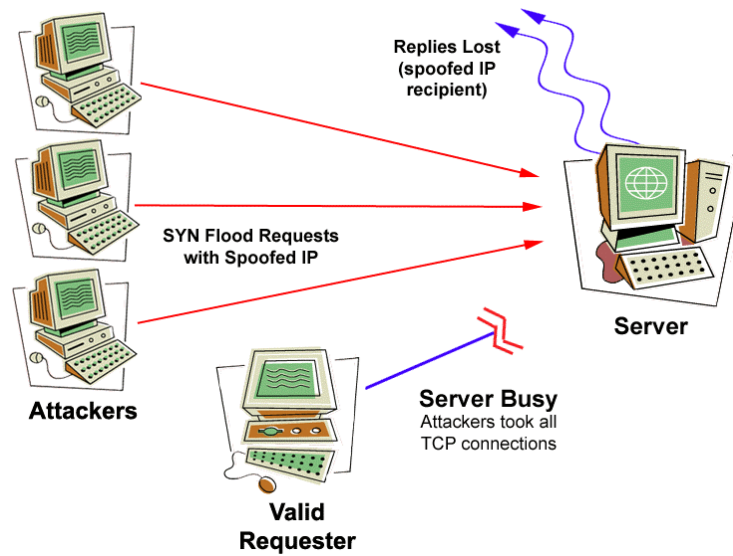
The difficulty with these attacks is that each request in isolation looks benign. A bogus request is very difficult to distinguish from a legitimate one.

*TCP SYN Floods are one of the oldest DoS attacks in existence. Any knowledgeable person can launch a TCP SYN flood, making this attack one of the most common. Without proper protection, SYN floods can place an entire organization at risk.*

*As DoS attacks bombard a network, the requests quickly fill up the connection table of most network security devices.*

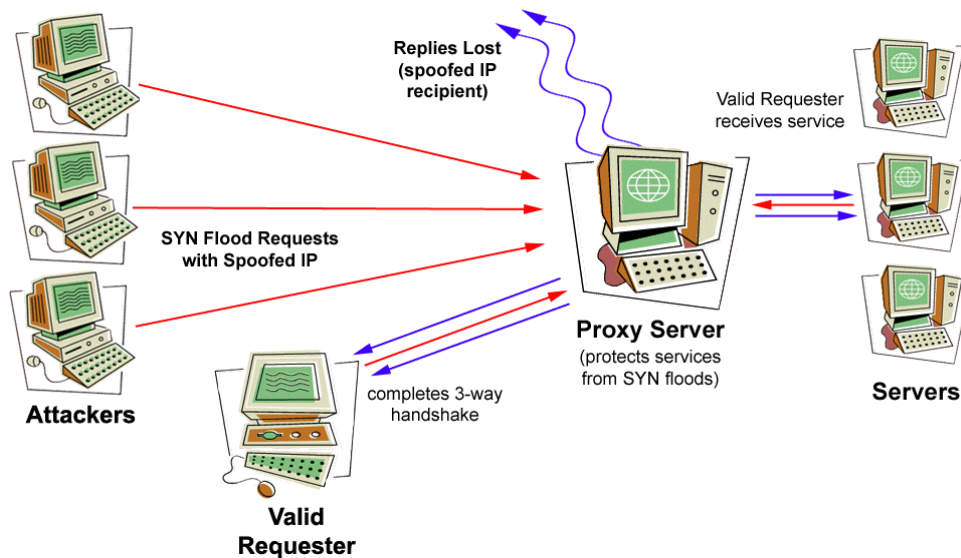
*UnityOne removes DoS attack traffic from the network—the UnityOne drops the requests immediately from the connection table, as in the case of a TCP SYN flood.*

**Figure 1: SYN Flood Attack**



*The SYN flood attack using spoofed IPs prevents a valid requester from accessing a server due to lack of connections.*

**Figure 2: Mitigating SYN Flood Attacks with Proxy Server**



*The addition of a proxy server prevents the SYN flood attack from consuming all TCP connections on the server. A valid request can complete a three-way handshake. This configuration is applicable for small to medium-sized networks.*

## Current Solutions

To protect against TCP SYN floods, network security organizations have developed a number of solutions—each having their limitations. These solutions include the use of Access Control Lists (ACLs) and proxy servers.

Organizations can use ACLs on their routers to help mitigate TCP SYN flood attacks by blocking invalid source IP addresses. The ACLs block illegitimate IP addresses; however, ACLs do not protect the network against TCP SYN Floods that use legitimate IP addresses and can eventually block legitimate packets. ACLs can also cause performance degradation on many route platforms.

Another approach is to use a proxy server. Proxy servers help protect low bandwidth sites, integrating the proxy server between the requester and the network device providing services. The proxy server becomes the access gateway to the network. It performs the three-way handshake with the requester first. If that handshake succeeds, it starts a connection with the network device.

The proxy solution has its limitations:

- **Scalability & Access Security** — Proxy servers do not scale for medium to large enterprise-grade networks. They have difficulty keeping up with thousands of connections. Proxy server connection tables can only store a small number of connections for tracking: generally a maximum of 15,000 connections/ second, a total of 250,000 connections.
- **Improper TCP Options Handling** — Proxy servers may not properly handle all of the TCP options of a requester. In effect, the connection may perform slowly or improperly. The proxy server may not understand what the requester and network device will negotiate and mishandle the resulting connection.
- **Performance** — After completing the three-way handshake with the proxy server, the requester has to wait on the three-way handshake between the proxy server and the target network device. The idle network time can result in system performance issues.
- **Failure to Block Other Attacks** — Proxy servers do not prevent TCP established connection attacks. It validates the attacks without protecting against them, giving a false sense of security.
- **Failure to Block Other Attacks** — Proxy servers do not prevent TCP established connection attacks. It validates the attacks without protecting against them, giving a false sense of security.

*Attackers may spoof IP addresses of trusted hosts to attack a system. Most network security systems do not provide protection and management options for spoofed, trusted IP addresses.*

*The UnityOne Intrusion Prevention System and Appliances can block attacks from single and multiple spoofed IP addresses. By grouping these attacks, the system detects and handles distributed flood attacks against the system.*

## The UnityOne Solution

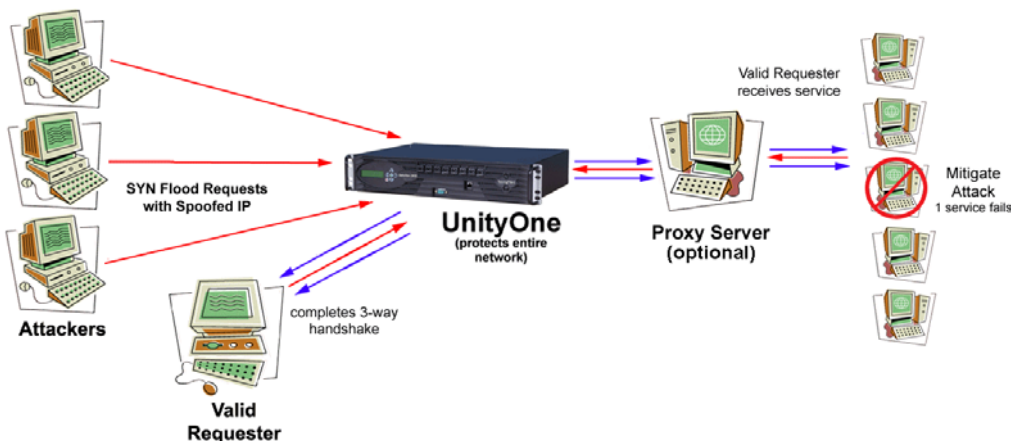
The UnityOne Intrusion Prevention Systems and Appliances use advanced methods and custom hardware to detect and protect enterprise networks against DoS attacks for

enterprise networks. The UnityOne features a connection table capable of handling—at line speed—over one million simultaneous connections.

The UnityOne is able to constantly monitor the number of SYN requests, established connections and active connections on a network. It detects SYN flood attacks when the rate of outstanding SYN requests suddenly exceeds the rate of newly established connections by a configurable threshold on a per source basis. As a result, valid requesters can complete a three-way handshake to access services. The UnityOne prevents the SYN flood from consuming all TCP connections and mitigates the attack.

Because the UnityOne compares the rate of requests to the rate of established connections rather than just counting SYN packets, it accurately detects attacks on busy servers without false positives. This frees busy network administrators from having to spend time carefully tuning the device to their network.

**Figure 3: UnityOne Solution with Optional Proxy Server**



*The addition of the UnityOne to a network prevents the SYN flood attack from consuming all TCP connections on the server. A valid requester can complete a three-way handshake through the UnityOne and an optional proxy server. The system then mitigates the attack, retaining the highest level of available services. This configuration is applicable to large and enterprise networks.*

*When the UnityOne detects a DoS attack, it enacts a series of actions and notifications according to customized settings. Administrators can set the system to block, permit, or generate notifications for the system, users and logs.*

*Every filter in the UnityOne provides protection against a wide variety of attacks. Network administrators can customize the settings for filters, including the following:*

- *Actions for attack responses*
- *Notification contacts for alert messages*
- *Exceptions for specific IP addresses*

Once a SYN flood attack is detected, the UnityOne can respond based on the specified action:

- **Permit + Notify** — Generate an alert
- **Block** — Block the attack
- **Block + Notify** — Block the attack and generate an alert

The system automatically flushes false requests from the connection table, keeping the network ready to accept legitimate requests.

TippingPoint's UnityOne Intrusion Prevention Systems and Appliances provide valuable additional support for detecting and preventing difficult SYN flood attacks.

The UnityOne includes the following:

- **Adaptive Threshold Tuning** — Over time, the traffic profile of a network changes. To better protect a network, UnityOne utilizes adaptive thresholds that are dynamically auto-tuned and calibrated to an organization's unique network traffic patterns.
- **IP Filtering** — The UnityOne includes filters for detecting and blocking attacks from illegal or spoofed IP addresses. Attacks cannot bypass security measures by pretending to have originated from within a network.
- **SYN Traps** — If the UnityOne is configured to block SYN floods, a SYN trap is installed once a SYN flood is detected. SYN traps can block all new TCP connection requests from a single attacker against a host. In the event of a distributed attack with random spoofed source addresses, SYN traps will temporarily block new connections to the server without interfering with existing connections
- **Exceptions** — Some servers are constantly congested and cannot keep up with the number of requests they receive. The UnityOne provides the ability to setup exceptions to SYN flood detection. Administrators can specify a list of IP addresses or subnets that are ignored by the SYN flood detector.
- **Advanced Connection Table** — The UnityOne provides an advanced connection table to handle over one million connections. As traffic increases due to flood attacks, the UnityOne connection table can handle the high amounts of connections and data without performance degradation. The connection table is pipelined with three different states: request, established, and active. After checking these states, a connection is added to the connection table. These settings store and function in the hardware.

*TCP established connection flood attacks can be some of the most difficult to detect and block. These attacks originate from an IP address that is checked and accepted by a proxy server through a complete three-way handshake.*

*Once a TCP established connection flood attack enters a network, it strikes against the proxy server, intending to crash it. Once the proxy crashes, access to systems and servers behind the proxy server is blocked.*

## TCP Established Connection Attack

A TCP established connection attack (also known as a Process Table attack) is an evolution of the SYN flood attack in that it uses completed three-way handshakes to establish bogus connections. The attack employs a multiplicity of attacker zombies to perpetrate a distributed DoS attack on a target. Rather than spoof source addresses, attacker machines use their legitimate addresses to establish connections, but pass no data. The effect is similar to a SYN Flood attack in that it consumes server resources, but is even more difficult to detect.

Proxy servers and ACLs cannot protect against these types of attacks. Most proxy servers can only handle about 15,000 connections/second and have a maximum number of connections or ACLs that is supported (250,000 connections on the larger systems). Once these limits are exceeded, the proxy is overwhelmed and fails. Once it fails, the network can

no longer accept or send requests, effectively dropping an entire network from receiving or initiating connections.

TCP established connection flood attacks are sometimes referred to as “process table attacks.”

### Current Solutions

Protection against a TCP established connection flood is difficult to achieve. Once a source IP address is determined to be real, most network security systems accept all traffic from the IP address. Current solutions for this attack require multiple network security devices to add a layer of misdirection in the proxy. This is done to screen the behavior of sources sending a suspicious amount of requests. However, this causes the same performance degradation as ACLs, impacting the performance of legitimate connections in the process.

### The UnityOne Solution

Using the same advanced hardware to prevent SYN flood attacks, the UnityOne tracks the number of established and active connections on a per IP address basis. The UnityOne detects a process table attack when the number of established connections exceeds the number of active connections by a configurable threshold. Requesters can also be restricted to a maximum number of open connections.

Once an attack is detected, the UnityOne can:

- **Permit + Notify**— Generate an alert
- **Block** — Block the attack
- **Block + Notify** — Block the attack and generates an alert

Optionally, the UnityOne can also reset any inactive connections, freeing resources on the server to satisfy requests from legitimate clients.

### Traffic Anomaly and Threshold Protection

As technology advances, attackers continue to develop new types of attacks. As these attacks seek access to a network, the traffic pattern on a network will typically change. These changes in traffic patterns can be a signal of new attacks or anomalies in a network.

For example, typical networks transmit a majority of one packet type over others. Common packet types include TCP, UDP, and ICMP. A typical network may receive and send 80 percent of TCP packets with the remaining 20 percent a mix of UDP and ICMP packets. An attack against a system can result in a surge of UDP and ICMP packets. This change in traffic mix can indicate an attack, such as the Slammer or Welch worms. Zero-day protection against attacks that exploit undisclosed vulnerabilities requires detection of traffic anomalies that signal the onslaught of such an attack.

*The TippingPoint Threat Management Center (TMC) diligently researches attack trends occurring around the globe.*

*As attacks are discovered, they distribute filters to protect networks. Coupled with traffic pattern analysis and threshold protection, network administrators can identify and track possible attacks and download and install Digital Vaccine™ updates. Most network security companies only provide updates without tracking or threshold protection settings.*

## Current Solutions

Many organizations protect against specific DoS attacks, but few provide general traffic monitoring to protect against packet distribution attacks and anomalous traffic patterns. Some intrusion detection systems are capable of signaling traffic anomalies, but do nothing to control the traffic or stay the attack.

## The UnityOne Solution

The UnityOne provides rate-shaping filters. Rate shaping and statistical anomaly filters guarantee that traffic matching the filter does not exceed or consume more than a preset amount of network bandwidth. This capability is very powerful in controlling excessive bandwidth consumption of non-mission critical applications and ensuring bandwidth availability for mission critical traffic. The aggressive propagation traffic produced by recent worms has resulted in DoS attacks against routers, firewalls, and other network infrastructure elements. Limiting this traffic to a capped bandwidth keeps the network running and stifles the attack.

In addition to pre-defined bandwidth shaping, traffic threshold filters monitor protocol and application traffic patterns over time and detect when there are sudden changes in those patterns. Protocol traffic threshold filters can be created for TCP, UDP, ICMP, and other IP protocols. Application traffic threshold filters monitor traffic to specific TCP and UDP ports.

Traffic threshold filters can measure different aspects of the traffic on a network:

- packets/sec
- bytes/sec
- connections/sec

For each traffic threshold filter, administrators can specify four threshold values and the response to take when the threshold is violated. There are minor and major thresholds when traffic surges above “normal,” as well as minor and major thresholds for when traffic drops below “normal.”

Thresholds are expressed as “percentage of normal” to avoid the tedium of manually configuring and tuning filters for specific networks. The system defines the values for “normal” traffic based on learned traffic patterns of a network over a period of time.

The UnityOne also provides different versions of “normal” for each filter. “Normal” traffic is dynamic and is continually recalibrated to ensure it is current for the actual traffic flowing on a network.

*Most network security systems cannot handle a tremendous number of attack traffic and connection loads that can flood a network. The UnityOne provides a unique, advanced connection table to handle over one million simultaneous connections.*

*To provide greater protection of a network, The UnityOne incorporates advanced traffic pattern monitoring and filters to watch for and react to possible traffic anomalies. These sudden changes in traffic could indicate an attack. With these advanced features, the UnityOne provides the best protection of an organization's assets.*

Traffic threshold filters provide settings for traffic comparisons. The system compares current traffic levels against “normal” levels using historical data for the last:

- 60 seconds
- 60 minutes
- 24 hours
- 7 days
- 30 days
- 35 days

Once a threshold is crossed, the system can be configured to take different actions, including the following:

- **Monitor Only** — Collect data for reporting purposes only
- **Permit + Notify** — Generate a notification
- **Rate Limit** — Dynamically install a rate shaping filter
- **Block** — Block the protocol or application
- **Block + Notify** — Block the protocol/ application and generate a notification

Traffic threshold filters are edge-triggered. These filters fire when the threshold is exceeded and again when the threshold is no longer being exceeded. These triggers provide information on the duration of each change in traffic patterns.

## Client Protection

Communications between a server system and its clients is another route for sending flood attacks. Attackers can infiltrate a network with programs to launch attacks from workstations within an organization. These attacks can initiate behind the firewall and proxy server.

*Attacks against networks can originate within an organization's network. Most intrusion protection and prevention systems do not consider an organization's internal computers and services as possible attackers.*

*The UnityOne considers every possible attack angle for DoS attacks, including as organization's internal network.*

Most intrusion prevention systems protect the incoming, but not outgoing, traffic on the edge of the network. Once within a network, an attacker can launch multiple attacks at any time without triggering a response in an edge network security device.

These attacks can use one of the various DoS tools that exist to flood a system and evade protection techniques of a network or firewall.

These tools include:

- **Tribe Flood Network (TFN)** — Focuses on Smurf, UDP, SYN, and ICMP echo request floods.
- **Tribe Flood Network 2000 (TFN2K)** — The updated version of TFN.
- **Trinoo** — Focuses on UDP floods. Sends UDP packets to random destination ports. The size is configurable.

- **IRC** — A client-server chat system popular worldwide, which can be a path for attacks to follow.
- **Zombies** — System that is used to send attacks, such as requests to random destination ports and packets that appear to be responses to requests from a specific target.
- **Stacheldraht** — Software tool that focuses on TCP, ACK, TCP NULL, HAVOC, DNS floods, and TCP packet floods with random headers.

In effect, a user can turn the network into the attacker, sending out hundreds if not thousands of attacks. In order to detect the communications channels used to orchestrate Distributed Denial of Service (DDoS) attacks, network administrators need protection that blocks these tools, provides signature-based detection techniques, and monitors outgoing as well as incoming traffic.

In general, DDoS tools are maturing both in terms of covert channel implementation and in DDoS flooding techniques. New tools rely heavily on encrypted communications channels that utilize arbitrary port numbers or work across IRC. Further, smarter tools intelligently disguise flooding packets as legitimate service requests and/or introduce a high degree of randomness. These enhancements make it increasingly difficult for a port-filtering device to separate attack packets from legitimate traffic.

### **Current Solutions**

Most DoS systems protect the network at the outer perimeter. They do not consider that internal traffic could be malicious. They protect every connection coming in, but not all connections initiated and sent out. As a result, the organization's network becomes an attacker, ignored by the network security system.

### **The UnityOne Solution**

The UnityOne offers complete protection by scanning and protecting every single connection and packet on a network, including internal traffic. With specialized filters and advanced traffic anomaly detection algorithms, the UnityOne solution prevents both external and internal attacks and provides total protection against all possible threats.

### **The Bottom Line**

To obtain full protection for DoS attacks, organizations typically need to purchase multiple proxy servers, network security devices, intrusion prevention systems, as well as software packages, updates, and expanded licenses as an organization grows.

TippingPoint Technologies provides the answer in a single system. The UnityOne is an easy, affordable, and scalable solution, equipped with a broad range of protection mechanisms including, application anomaly filters, protocol anomaly filters, exploit signature filters, statistical traffic anomaly filters and threshold rate-shaping filters.

Attacks continue to evolve and increase in sophistication. The flexibility of the UnityOne platform offers state-of-the-art protection against today's attacks and the power to protect against tomorrow's.