Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

DoS Attacks:
Response Planning and Mitigation

August 2012

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Contents

softwareblades™

Introduction

This whitepaper provides an overview of Denial of Service attacks, tools and techniques and also describes how DoS attacks can be mitigated with Check Point Software Blades and the DDoS Protector appliance. We'll then take a look at a real-life example of a customer who was under a DoS attack and how their Check Point Account Team helped them mitigate the attack. Note, throughout this paper, the term "DoS" is representative of both Denial of Service and Distributed Denial of Service attacks.

DoS attacks target networks systems and individual services and flood them with so much traffic that they either crash or are unable to operate. What would you do if suddenly your "systems are not responding"?

A DoS Story

We are all familiar with the sci-fi movie scene where the lead characters, already facing overwhelming odds and burdened with the heavy responsibility to triumph over the challenges of the moment, suddenly find "… the systems are not responding…" They've lost control, are running blind and are seemingly unable to save the day.

Such is the case in modern business when IT networks fall prey to DoS attacks. Consider any business today—such as a small regional bank offering services to the public, with account holders, payroll services, mortgage and business loan services, check clearing, and monetary transfers. Suddenly "… the systems are not responding…" Or maybe it's a retailer who generates the majority of their annual business during the holiday season—suddenly "… the systems are not responding…" Or maybe it's a private college for which its online presence is critical to recruiting and enrolling new students—and generating revenue—as well as providing daily services to their current student body: scheduling, resource access for research and class work, emergency campus communication—and suddenly "… the systems are not responding…" Or perhaps a major financial institution whose daily operations are critical to national economic continuity and well-being—and suddenly "… the systems are not responding …"

These are real life examples of how today's DoS attacks have the ability to overwhelm even the most sophisticated and defended networks and cause harm to major businesses.

What Is A DoS Attack?

Denial-of-service (DoS) attacks target networks, systems and individual services, and flood them with so much traffic that they either crash or are unable to operate—which effectively denies the service to legitimate users.

A DoS attack is launched from a single source to overwhelm and disable the target service, whereas a Distributed Denial-of-service (DDoS) attack is coordinated and simultaneously launched from multiple sources to overwhelm and disable a target service. These multiple attack sources are typically part of a "bot-net" (a network of compromised computers) and can be scattered across a region or around the globe. The botnet can act dynamically in terms of which bots are attacking a target at any given moment, making it very difficult to detect and block the attack.

The symptoms of a DoS attack are obvious—slow to unresponsive network performance, and possibly unresponsive or unavailable applications. Collateral impact or damage is to be expected—a DoS attack that floods a network pipe or application can also impact the response time of other services that are on that network segment.

By all definitions, DoS attacks are violations of acceptable conduct and even illegal. They violate the spirit and rules set forth in the IAB RFC 1087, *Ethics and the Internet*, and are against the law in most countries. The bottom line is there is no legitimate use of DoS attacks.

Who Uses DoS Attacks and Why?

DoS attacks have been used by all manner of organizations and groups to further their cause. Who are these groups and what are their motivations? There are three categories of DoS attackers:

1. Hacktivists
2. Nation State Driven
3. Financially Motivated Attackers

Hacktivists are individuals or groups that are organized and motivated to make social and political points primarily through public IT disruption by leveraging DoS and other attack methods. From Wikipedia[1], "The term was first coined in 1996 by a member of the Cult of the Dead Cow hacker collective named Omega." If hacking as "illegally breaking into computers" is assumed, then hacktivism could be defined as "the use of legal and/or illegal digital tools in pursuit of political ends". In addition to social and political motivations, some believe that a small subset of hacktivists are actually tied to organized crime and use hacktivism as a diversion to facilitate stealing information for financial gain.

Nation state driven DoS attacks, presumably sanctioned by one or more governments, are also conducted for many different reasons. These reasons are age old and obvious—from creating havoc and disrupting governmental operations, to good old fashioned spying and stealing national secrets. Note, however, that attacks that might appear as nation state driven can actually be unsponsored acts perpetrated by a few who are motivated to carry out acts under their own perception of patriotism.

Conducting an attack for financial gain is a common denominator in a vast majority of the DoS attacks launched on governments and businesses alike. A for-hire DoS attacker can be paid to conduct a DoS attack against the buyer's competitor, thereby deriving financial gain for both the buyer and the attacker. In other cases the DoS attacks are merely a diversion for the actual objective to steal information—personal records, account records, intellectual property—all to be sold or somehow used for capital gain. Lastly, there have been instances of DoS "ransom attacks" where the target is told to pay a ransom, otherwise they'll be DoS'd and their systems rendered unusable.

Who launches DoS attacks and why? Hacktivists groups organized and motivated to make social and political points. Nation states to create havoc and disrupt governmental operations—and of course to spy and steal national secrets. Organized crime and hacktivists presumably only differ on motive as organized crime is typically driven by financial gain—which is likely the most common denominator across all attack groups.

Types of DoS Attacks

There are two primary categories of DoS attacks today—attacks that target and flood the network, and attacks that target and flood applications. While application attacks have become more common in the last year or two, network flood attacks have remained a commonly used and impactful disruption technique.

1. **Network Flood DoS Attack**
   Also known as a volumetric attack, these attacks send enormous volumes of irrelevant UDP, SYN or TCP traffic to consume network bandwidth and flood network equipment, rendering the network segment and even the entire network unusable.
2. **Application DoS Attack**
   Application DoS attacks target applications and flood them with seemingly legitimate requests until they become unresponsive. Most often these attacks go completely unnoticed because they drive a small volume of traffic that slowly consumes resources until the application fails.

Both attack types can fall in these categories:

Asymmetry of resource utilization in starvation
The goal of this attack is to simply overwhelm the target's capacity. It is any network or application DoS attack, where the attacker commands more resources—processing power and/or bandwidth—than the target, and uses it to overwhelm the target.

Diversionary DoS Attack
A DoS attack is sometimes used as a diversion to distract the target's security team while the attackers carry out some other objective.

DoS Attack Methods and Tools

Today there is a wide range of DoS attack techniques and tools, with more being created regularly. Depending on what disruption and impact an attacker wants to inflict, there is probably a technique or tool that will help them accomplish it. It is important to note the lifespan of a tool is often very short—possibly only a few months. This short lifespan highlights the importance and effectiveness of protective actions against DoS attacks—but also highlights how resilient the threat community is in creating new DoS methods and tools.

This section provides an overview of DoS attack techniques and tools, from some of the original and fundamentally simple attack techniques to today's sophisticated, turn-key DoS toolkits. Do note that there are many more DoS attack techniques and tools than are listed here.

SYN Flood Attack
The goal of this attack is to exhaust the target's resources with a flood of half open connections. The attacker repeatedly sends open connection requests (TCP/SYN) to the target with a spoofed source address. The target acknowledges (SYN-ACK) back to the spoofed source, thus opening a connection for each request. However, the standard three-way handshake is never completed because the spoofed source never replies, and the target victim is eventually flooded with half-open connections. Current versions of today's common applications typically protect against this type of DoS attack.

Depending on what disruption and impact an attacker wants to inflict, there is a technique or tool that will help them accomplish it. The lifespan of attack tools are typically very short which highlights the importance and effectiveness of protective actions against DoS attacks—but also highlights how resilient the threat community is in creating new DoS methods and tools.

HTTP Flood

HTTP floods are typically targeted at services that generate a high load like a site search or heavy database activity which consume more resources and cause delayed response and possible failure. There are several types of HTTP flood attacks.

- **Simple "GET" or "PUT" floods**—The attacker sends GET or POST HTTP requests to target main page until the network pipe, the target server or other network equipment is overwhelmed and cannot handle the requests. This attack can be varied by adding a random query string to the HTTP requests which serves to bypass content delivery networks (CDN) or caching services, causing the traffic to hit the web site directly rather than the CDN.
- **"Slow" HTTP attacks**—Similar to SYN floods but at the HTTP level. These attacks cause the web server to exhaust its resources on continually opened new connections. The attackers send a "GET" request then reduce its window size to a small value. This forces the web server to send its response in smaller packets than usual, forcing the connections to remain longer than normal and eventually filling the server's connection table. This attack is slow and silent with no obvious signs of attack like high CPU utilization. This same attack can be done using POST commands where the attacker claims to be sending a large data chunk which is never sent.
- **HTTP flood on a targeted resource**—The attacker profiles the victim site to identify a resource that causes an especially heavy load on servers, such as a site search or heavy database activity. The attacker then attacks that service typically with very small traffic volumes. A server that can typically handle 1000s of connections per second can be completely flooded and rendered unresponsive with merely 20 connections per second of this type of attack. "Slowloris" is an example of a tool that uses this technique.

UDP Flood

The attacker sends packets containing UDP datagrams to the target, which then checks the port for an associated application—finding none, it is forced to reply with an ICMP *Destination Unreachable* packet. This attack continues until the network pipe, the firewall, or other network equipment at the target is flooded. The attacker may also spoof the IP Address of the UDP packets, thus remaining anonymous.

ICMP Flood Attacks

Common in the 1990's, this category of DoS attack is typically blocked by today's firewalls and network equipment policy. There are a couple named techniques in the ICMP flood attack method:

- **Ping Flood**—The goal of this attack is to flood the network with ICMP traffic. An example of this type of attack is where the attacker sends a large volume of "ping" requests and spoofs the source address with the address of the victim, who is then flooded with all the responses to the ping requests.
- **Smurf Attack**—The goal of this attack is to flood the target with ICMP traffic by using the IPS broadcast service. Attackers generate ICMP ping traffic with the victim address spoofed as the source, and send it to the network IP broadcast addresses which broadcast it to all hosts, who then reply to the spoofed source victim, flooding it with traffic.

Application attacks can be slow, silent and go unnoticed. When attacked by the Slowloris tool, a server that can normally handle 1000s of connections per second can be completely flooded and rendered unresponsive with merely 20 connections per second of this type of attack.

Low-rate DoS (LDOS) Attack
The goal of this attack is to slow the TCP throughput of the target system without being detected. An attacker exploits TCP timing weaknesses to cause TCP processing at the victim to repeatedly enter a state of retransmission, thus dramatically impacting TCP throughput.

Peer-to-peer Attack
The goal of this attack is to generate a massive flood of near-simultaneous connection requests to the target. Bugs in peer-to-peer server software allow attackers to hijack clients in peer-to-peer hubs, direct them to disconnect from their peer-to-peer network, and connect to the victim site, thus creating a massive flood of connection requests. Clients in peer-to-peer networks can number in the tens to hundreds of thousands; thus, the scale of these attacks can be immediately overwhelming to the victim.

Low-Orbit Ion Canon (LOIC)[2]
This is a DoS attack tool whose goal is to disrupt the target service by flooding it with TCP or UDP packets. Originally an open source stress testing and denial of service attack tool, it was later released into the public domain where it has been put to use as a DoS attack tool. The group Anonymous used the LOIC tool to attack several governmental agencies including the FBI and the Department of Justice as part of their attack campaign to protest the shutdown of file-hosting site MegaUpload, was well as the proposed U.S. SOPA (Stop Online Piracy Act) legislation dealing with online trafficking of copyrighted and PIPA (Preventing Real Online Threats to Economic Creativity and theft of Intellectual Property Act).

An attack called "Operation New Son" (OpNewSon) purportedly driven by Anonymous was scheduled to occur May 25, 2012 and use LOIC as the attack tool of choice. The attack was to target many well-known corporations to cause disruption and outages. The threat caused many of these companies to take actions in preparation for the attack. In the end, it appears no attack was actually launched on that date.[3]

High-Orbit Ion Canon (HOIC)
This DoS attack tool is very new and is the next-generation of LOIC. While LOIC uses TCP, UDP and HTTP attacks, HOIC uses only HTTP attacks. HOIC's goal is to disrupt multiple target services simultaneously by flooding them with HTTP POST and GET requests. HOIC differs from LOIC in two more areas. First, it can attack up to 256 different web addresses simultaneously, or alternatively multiply its attack strength to one target 256 times. Second, it can dynamically change its attack signature, making detection extremely difficult.

The mere threat of DoS attacks forces expense on the targets. The "Operation New Son" DoS attack was scheduled to occur on May 25, 2012 and was publicly stated to target specific, well-known businesses. The threat caused many of these companies to take actions in preparation for the attack. In the end, it appears no attack was actually launched on that date.

Slowloris
This is an application DoS attack tool whose goal is to slowly crash the target web server. The attack slowly opens connections with the victim server and keeps them open by sending additional tidbits of information but without ever completing the request. It continues this tactic until the target web server is overwhelmed with requests—maximum connections, memory exhausted—and can no longer function.

R-U-Dead Yet (RUDY)
This is a web application DoS attack tool whose goal is to consume the target web server's session capacity. Similar to Slowloris, RUDY consumes sessions by repeatedly sending POST transmissions with large content-length headers.

Google+[4]
Less than a year old, this technique leveraged public Google services as a proxy to launch a DoS Attack Response Plan on the target. When automated via a script, the target would be overwhelmed with the number of requests. The Google Security Team quickly responded and fixed the vulnerability that allowed the service to be hijacked.

THC-SSL-DOS (also THC-SSL-DDoS)[4]
This is an application DoS attack tool that targets web servers. In this scenario, a single attacker computer can overwhelm a web server that supports SSL renegotiation. This configuration option allows the web server to create a new secret key on the existing SSL connection which forces renegotiation and consumption of resources. Sending many multiples of these requests can overwhelm the web server.

Apache Killer[4]
This is another short-lived technique that was both born and resolved in the second half of 2011. This technique leveraged vulnerability in Apache HTTPD that caused resource exhaustion, primarily memory, by driving large numbers of incorrect HTTP header ranges to the server. Apache has resolved this vulnerability in the most current versions.

Darkness (Optima) DDoS Bot[5]
A DDoS bot toolkit originally released in 2009 as "Optima" has since evolved to "Darkness Optima" and its 10th version was released in October 2011 as "Darkness X Bot". Described in an ad:

"Darkness X, Powerful DDoS bot with premium admin panel "Optima" (From Russia with Love) 4 types of DDoS attacks / Additional modules / 7 packages / Amazing support"

The toolkit offers HTTP, ICMP, SYN and UDP attack techniques, the ability to attack multiple server URLs simultaneously, methods for bypassing anti-DDoS protections, and real time tech support.

Slowloris is an application DoS attack tool whose goal is to slowly and silently crash the target web server. The attack opens connections with the victim server and keeps them open by sending additional tidbits of information but never completes the request. It continues this tactic until the target is overloaded with requests and has reached its maximum connections or exhausted its memory and can no longer function.

Dirt Jumper and its variations[6,7]

This is another example of a DDoS bot toolkit that has evolved over time. Originally released in 2009 as "Russkill" offering HTTP and SYN flood attack capability, by early 2011 it evolved into "Dirt Jumper" and was initially for sale for $600. "Dirt Jumper September" soon followed in late 2011. The Dirt Jumper toolkit offers multiple DoS attack techniques:

- **HTTP Flood**—Causes server overload from simultaneous sending a large number of HTTP requests
- **Synchronous Flood**—Causes server overload from repeated multiple simultaneous requests
- **Downloading Flood**—Consumes bandwidth of the target via multiple download requests
- **Post Flood**—Consumes bandwidth of the target web server via simultaneous GET and POST commands

The "Dirt Jumper" strain of toolkits continues to evolve and proliferate. "Trojan. Khan" is one named version that appears to be a straight copy, while Di BoTNet is another which adds the ability to kill competitive bot nets.

These are only a few examples of DoS techniques and tools, but it is clear that the threat community is resilient and is financially motivated to devise new tools to cause IT disruption and harm. While the Google+, TC-SSL-DDoS and Apache Killer techniques were very short-lived, during their time they were very effective. The Darkness/Optima and the Dirt Jumper families exhibit robust evolution, and even "product management" guidance. Just as the motivation for launching DoS attacks is often financial, it is clear the market for DoS attack techniques and turn-key tools is robust, even resilient—not to mention financially lucrative for their authors.

How Can Organizations Defend Against DoS Attacks?

At this point, it should be clear that defending against DoS and DoS attacks is extremely difficult. In fact, there is no silver bullet solution to fully protect against DoS and DDoS attacks. These attacks typically hit without warning, making them highly impactful. This emphasizes the importance of preparing beforehand. To begin preparing, every organization should ask:

"If a DoS attack hit us right now and our systems were not responding, what would we do?"

Answering this question is the basis for developing a plan of action to help mitigate and defend against DoS attacks. The moment you fall under a heavy DoS attack and your systems are not responding, the situation on the floor will be critically urgent, very confusing, highly stressful and extremely tense. Who is doing it? Why are they doing it? How are they doing it? How long will it last? What should we do? Who should be notified? What partners and vendors can assist? Management is asking "what are you doing about it and when you will have it fixed?!"—via a non-stop open conference line. And so on. Pre-planning is absolutely vital!

Just as the motivation for launching DoS attacks is often financial, it is clear that the market for DoS attack techniques and turn - key tools is robust, even resilient - not to mention financially lucrative for their authors.

Develop a Plan!
Developing a "DoS Attack Response Plan" is truly critical to mitigating and possibly stopping a DoS attack. Further, the entire IT team should be aware of and immediately execute to the DoS Attack Response Plan upon notice.

Consider the following elements of a sound DoS Attack Response Plan:

1. Who is in charge?
From the outset and throughout the DoS ordeal, it is important to have already appointed clear and proper leadership. Who is on the Incident Response Team, what are their roles and who is in charge to direct the team and mitigation efforts?

2. What actions should be taken?
A. Analyze Traffic
Use existing vendor and in-house tools to analyze the traffic and identify the profile of the attack. For example:
- Identify suspicious geographic sources
- Cross reference suspicious IP source addresses with known bad IP addresses
- Identify spikes in traffic types, application traffic, traffic geo sources, etc.
- Identify connection patterns that vary from the norm

B. Implement Blocking Rules
Set rules to block traffic that meets the identified attack profile. For example:
- Block all traffic from the list of suspicious source countries
- Block source IP addresses that are known bad IPs
- Block all identified suspicious traffic/attack types
- Block all traffic based on the identified suspicious connection pattern and/or all connection patterns that vary from the norm
- And any others as needed and appropriate

3. Seek Service Provider Assistance
Contact your Service Providers to understand what DoS protection services and tools they offer to help mitigate and block should you fall under a DoS attack. Understand and document the process for contacting them and implementing their services. What services do they offer, and under what circumstances should they be contacted? How are these services charged—by incident, by amount of data, or by a quarterly or annual premium like a homeowner's fire insurance policy? Service Providers can offer tremendous assistance in mitigating DoS attacks, but the time to understand their services, process and costs are *before* and not during a DoS attack.

4. Contact 3rd Party Mitigators
Beyond Service Providers are 3rd party vendors who offer specialized DoS mitigation services such as what are termed "clean pipes". These services are sometimes the only viable option for mitigating a large, network consuming volumetric DoS attack. Again, as part of your DoS Attack Response Plan, identify and engage these providers to understand what services they offer, their costs and the process and actual steps to engage their services. For example, understand and document the steps to redirect all your internet traffic through their facility for "clean pipes" service should you fall under a volumetric attack.

Developing a "DoS Attack Response Plan" is truly critical to mitigating and possibly stopping a DoS attack. Further, the IT team should be aware of and immediately execute to the DoS Attack Response Plan upon notice.

5. Contact Authorities

Contact authorities, such as the FBI in the U.S. in your country in the event there is an opportunity for legal action. Be sure to retain logs and other evidence that could be useful in identifying and prosecuting the attackers. Federal authorities are working together more and more every day to jointly identify and take down purveyors of spam, bot-nets, DoS and other IT-related crime.

Creating a plan of action against DoS attacks is by far the most important step you can take to defend against an eventual DoS attack. As far as this author is concerned, the importance of this plan cannot be overemphasized. When you fall under DoS you will either know exactly what to do from the instant the attack is identified, or you will be caught under an overwhelming wave of confusion, uncertainty, panic and demanding management because your "systems are not responding".

When you fall under DoS you will either know exactly what to do from the instant the attack is identified, or you will be caught under an overwhelming wave of confusion, uncertainty, panic and demanding management because your "systems are not responding".

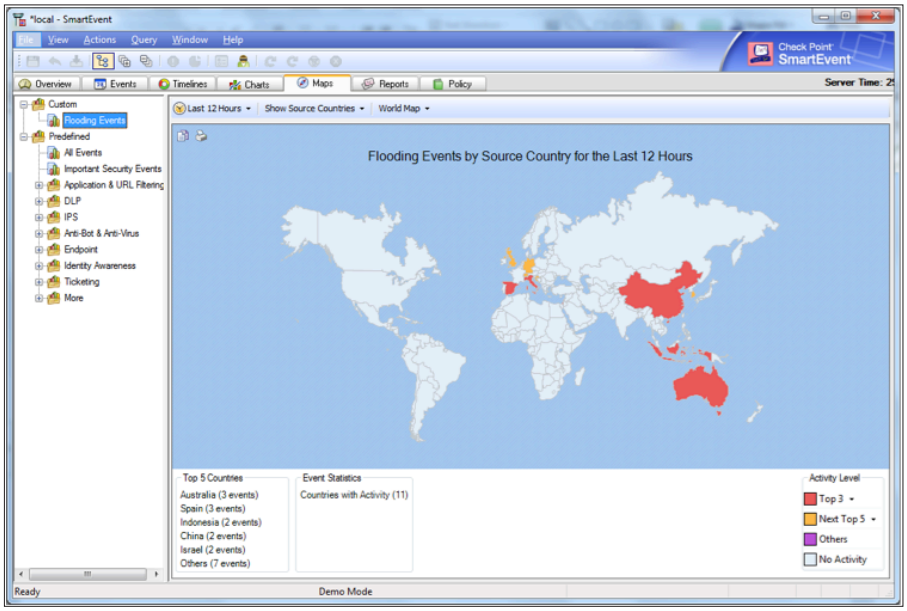
Check Point Software Blade Tools for Mitigating DoS Attacks

While there is no silver bullet solution against DoS attacks, a subset of Check Point Software Blades can be very effective tools to help mitigate DoS attacks. Customers who have these Blades deployed can easily leverage their capabilities during a DoS attack to help identify the attack sources, attack patterns and other identifying elements to assist in mitigating the attack.

SmartEvent

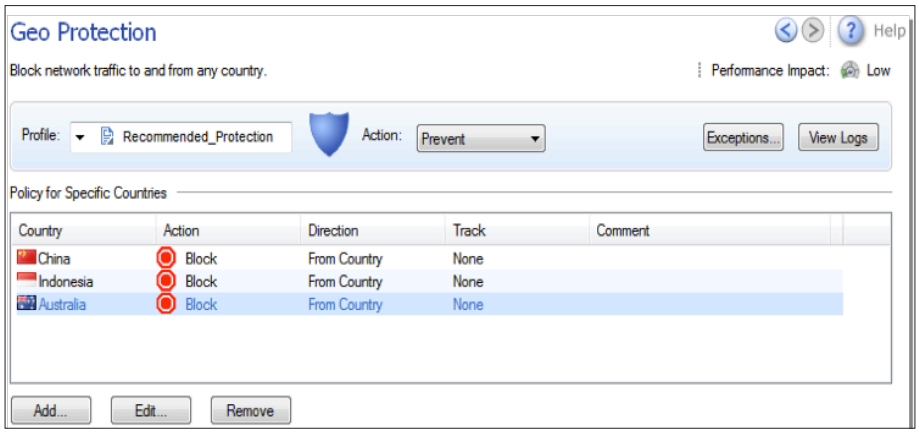
The SmartEvent Blade is the key tool to quickly identify the attack profile and patterns. From a single pane of glass that presents a graphical view of the leading geographical attack sources, to the alert analysis screen where automatic sorting and correlation will identify patterns, SmartEvent is an essential tool for analyzing and identifying DDoS traffic patterns.

For example, the screenshot below highlights the top flooding events by source country.



It is easy to block the offending countries permanently or just for the duration of the attack.

SmartLog feature of Logging and Status Blade



The SmartLog feature of the Logging and Status Blade can help quickly identify DoS attacks profiles and patterns. SmartLog provides deep log analysis with split-second search results from billions of log records from multiple log files, time periods, gateways, domains, actions, users, time period or geographic data.

Firewall Software Blade

The Firewall is a front-line tool to help mitigate DoS attacks based on certain attack elements. Examples of features that can be employed are:

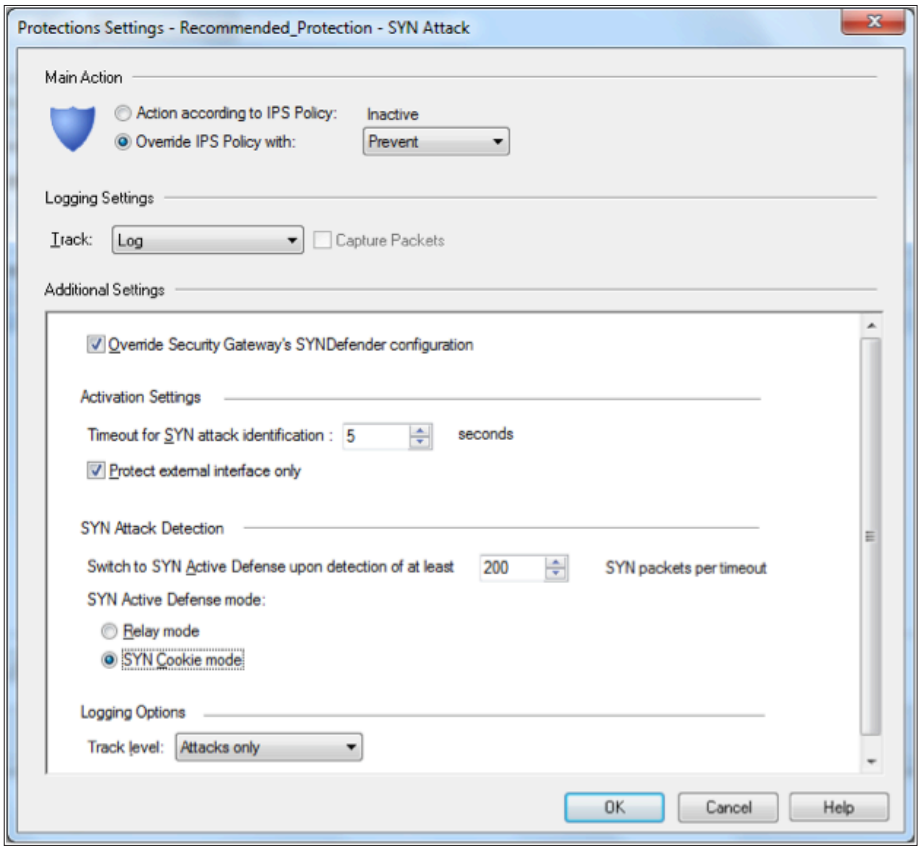
- **Aggressive Aging**—If connections are idle for longer than the defined threshold, the connections are marked eligible for deletion from the gateway's connections table. This technique helps protect against slow, connection consuming attacks. The default is 60 seconds, but in the case of an attack it can be lowered to a much smaller time period.
- **Network Quota**—Enforces a limit upon the number of connections that are allowed from the same source IP address. When a source address exceeds the number of allowed connections, the Network Quota can either block all new connection attempts from that source or track the event.
- **Block ICMP/UDP** traffic at the perimeter with a rule early in the rule set
- **Stateful Inspection timers**—Lower Stateful Inspection Timers to defend against slow, resource consuming DoS attacks:
  - TCP Start, Session and End Timeout
  - UDP, ICMP and IP Virtual Session Timeout
- Create a custom service with more aggressive session timeouts

Check Point Software Blades can be very effective tools to help mitigate DoS attacks. These Blades can easily be leveraged to help identify the attack sources, attack source countries, attack patterns and other identifying elements to assist in mitigating the attack.

IPS Software Blade

The IPS Software Blade provides additional capabilities to help mitigate and block DoS attacks. Here are some examples:

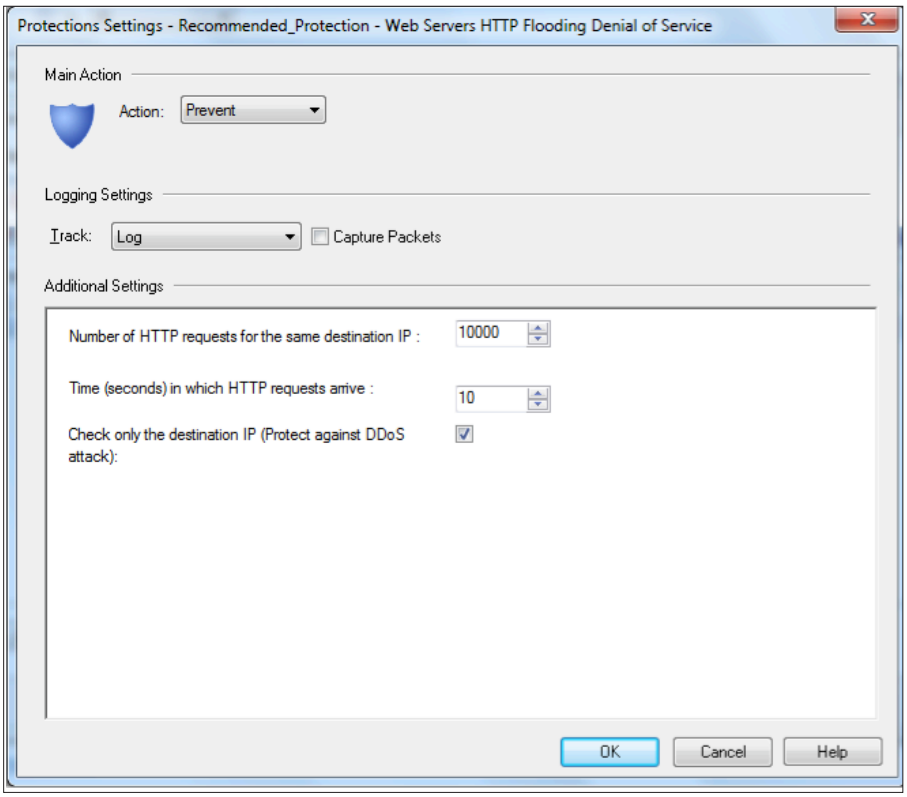
- **Block by Country**—Block all traffic from countries that appear to be the attack source and also countries from which your company does not do business
- **Worm Catcher Signature**—Enable the Worm Catcher signature to block the identified attack URLs
- **TCP Window Size Enforcement**—Protects against two specific Windows TCP vulnerabilities often exploited in DoS attacks the first vulnerability involves setting the TCP receive window to a small size or zero then flooding with TCP connections. The second exploit involves flooding the system with connections that have an infinite wait state.
- **SYN Flood Protection**—Provides additional and specific protection against SYN Flood attacks. Per the screenshot below, the SYN Attack protection is being enabled and defined in the "Recommended Profile". Specifically, when the IPS Blade detects at least 200 SYN packets per 5 second interval, then the SYN Attack protection intercedes to block the offending traffic.



Check Point solutions that can help you fight against DoS attacks include

- SmartEvent Software Blade
- Firewall Software Blade
- IPS Software Blade
- DDoS Protector

- **HTTP Flooding**—Enable the "Web Servers HTTP Flooding Denial of Service" protection for more protection against HTTP flood attacks. Per the screenshot below, the protection is enabled and defined in the Recommended Profile. Specifically, when more than 10,000 HTTP requests to the same destination IP address occur within 10 seconds, the protection intercedes to block the offending traffic.



This protection can be tuned to specifically fit your environment. Start out in detect mode and at 10 HTTP requests per second. Assess your logs, adjust the thresholds, and when no logs appear from normal traffic, increase the number to allow headroom and switch the protection to block mode.

Check Point Software Blades offer many capabilities to help combat DoS attacks—from analysis tools that can identify the profile of the violating traffic, to security functions that help detect and block varieties of DoS traffic. To be prepared to mitigate a DoS attack, it is important to understand and document in your DoS Attack Response Plan all the DoS mitigation tools and techniques available in your Check Point and other security products. Your existing security products will be your first line of defense against and in detecting DoS attacks and your all-important tool box to analyze traffic and then extend security actions to mitigate the attack.

To be prepared to mitigate a DoS attack, it is important to understand and document in your DoS Attack Response Plan all the DoS mitigation tools and techniques available in your Check Point and other security products. Your existing security products will be your first line of defense against and in detecting DoS attacks and your all-important tool box to analyze traffic and then extend security actions to mitigate the attack.

Check Point DDoS Protector

Check Point DDoS Protector is a DoS mitigation solution that employs specialized software running on a hardware-accelerated platform. It is deployed outside the perimeter firewall to detect and mitigate DoS attacks before they can impact the production network. Protector leverages three protection techniques to defend against DoS attacks:

- **Network Flood Protection** - Protector uses behavioral analysis to provide network flood protection. By baselining normal daily and weekly traffic patterns for both network and application traffic, Protector then identifies abnormal traffic—especially spikes from network floods.
- **Server Flood Protection** - Protector protects against misuse of resources with automatic signature generation capability—it automatically generates new signatures to mitigate suspected attacks, while pre-defined signatures prevent known bad behavior. Key signature elements include source IPs, protocol, threshold, SSL renegotiation and others.
- **Application Layer Protection** - Protector blocks automated tools and fake users with challenge/response techniques, while legitimate users are transparently redirected to the desired destination.

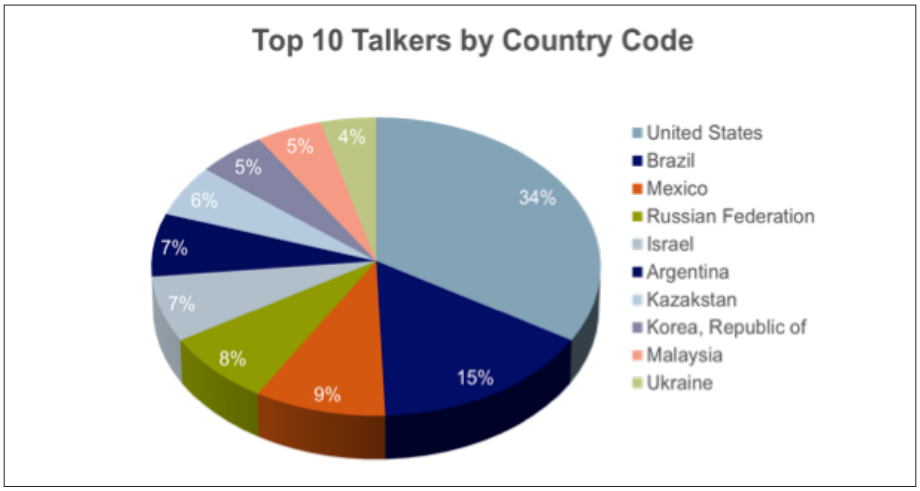
DDoS Protector combines these techniques to deliver extremely effective DoS mitigation, especially for the "slow and quiet" type of application DoS attacks.

DoS Mitigation Case Example

U.S Regional Bank

A small, regional bank in the U.S. fell under a DoS attack and contacted their Check point Account Team to assist. The attack had already been underway a few hours when Check Point was contacted and the customer had ramped up their staff and had contacted authorities. They did not have a DoS Attack Response Plan in place, so the mitigation actions were being defined and determined on the spot.

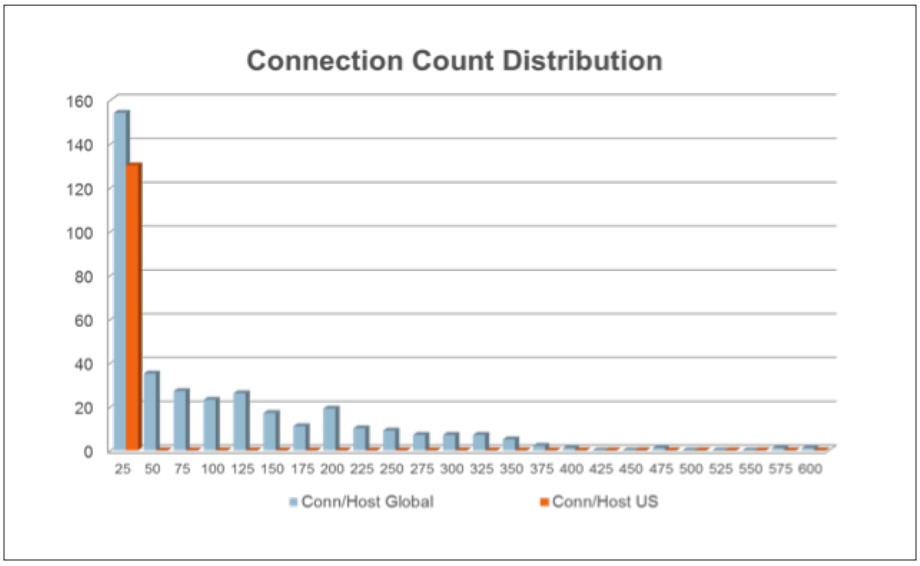
When the Check Point Account Team arrived, the first thing the Security Engineer did was leverage SmartEvent to analyze logs for patterns—IP addresses, geographic, URL, TCP and connection patterns. The analysis through SmartEvent took mere minutes and was very revealing on a number of fronts. First, simply sorting on the "Source Country" in the SmartEvent event screen yielded immediate insight that geographic distribution was all over the map:



When a small, regional bank in the U.S. fell under DoS attack, they did not have a DoS Attack Response Plan in place, so the mitigation actions were determined and defined on the spot.

Recall this is a small, U.S. regional bank, yet 66% of the traffic originated offshore and 35% of the traffic originated from the European and Asian continents.

Second, analysis of the logs revealed a correlation of connection count by country.



Again, this is a U.S. regional bank and the chart above clearly shows that typical connections from U.S. hosts (Y-axis) are never more than 25 (x-axis) while connection counts from global hosts are clearly out of the norm.

Third, the Check Point IPS Protection Team wrote a custom IPS signature to analyze TCP fingerprints. This signature revealed there were a number of TCP zero windows which correlated to known bad IP addresses (See IPS Software Blade, TCP Window Size Enforcement, in this paper):

Mitigation Actions

The analysis revealed several behavior patterns of the DoS attack being carried out against the bank. With this information, the Account Team and the customer were able to implement rules to block traffic with the suspicious traits. Specifically, the following mitigation actions were taken:

- **Firewall Software Blade**—Add IP quota rule to limit connections to certain servers < 25.
- **IPS Software Blade**—Set rules to block traffic from approximately 40 countries.
- **IPS Software Blade**—Deploy a custom IPS signature to blacklist user who close connections with zero windows.

In this instance, the Check Point Firewall, IPS and SmartEvent Software Blades provided the tools that were necessary to analyze the mass of traffic and properly discern and expose the identifying patterns of the DoS attack. With this information and behavior profile in hand, the Check Point Account Team and the customer's technical staff were able to define and deploy new rules which successfully mitigated the DoS attack. Note, however, that had the bank 's network been protected by a Check Point DDoS Protector appliance, it's likely that they would've automatically been protected from the attack without needing to involve the Check Point account team.

Tools in Check Point Software Blades helped to quickly identify that the attacks had specific geographic, connection and fingerprint patterns for which Firewall and IPS rules could be defined to block them.

Summary

The DoS threat is real and the problem is not going away. The threat community is alive with innovation driven by robust demand for tools to cause IT disruption and harm in the name of national and social causes—and of course, financial gain. While there is no silver bullet solution that protects against all forms of DoS attacks, there are many actions that can be taken to help mitigate the attack when it comes. First and foremost is preparing a DoS Attack Response Plan that outlines the leadership, tools, analysis steps and mitigation actions that should be taken when under DoS attack. Absent such a plan, the security team will be left to improvise a plan in real time in an attempt to mitigate an attack.

For more information on the Check Point products mentioned in this white paper, please go to the following links:

SmartEvent Software Blade

Firewall Software Blade

IPS Software Blade

DDoS Protector

Be sure to prepare a DoS Attack Response Plan so that your security team is not left to improvise a plan in real time in an attempt to mitigate an attack.

[1] Wikipedia

[2] Alert (TA12-024A) "Anonymous" DDoS Activity—US-Cert

[3] threatpost.com

[4] DoS Attack Response Plan in H1 2011—SecureList

[5] "A Peek Inside the Darkness (Optima) DDoS Bot"—Webroot Threat Blog

[6] ProLexic Threat Advisory

[7] "A DDoS Family Affair: Dirt Jumper Bot Family Continues to Evolve"—Arbor Networks

About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com), worldwide leader in securing the Internet, is the only vendor to deliver Total Security for networks, data and endpoints, unified under a single management framework. Check Point provides customers uncompromised protection against all types of threats, reduces security complexity and lowers total cost of ownership. Check Point first pioneered the industry with FireWall-1 and its patented Stateful Inspection technology. Today, Check Point continues to innovate with the development of the software blade architecture. The dynamic software blade architecture delivers secure, flexible and simple solutions that can be fully customized to meet the exact security needs of any organization or environment. Check Point customers include tens of thousands of businesses and organizations of all sizes including all Fortune 100 companies. Check Point award-winning ZoneAlarm solutions protect millions of consumers from hackers, spyware and identity theft.

CHECK POINT OFFICES

Worldwide Headquarters
5 Ha'Solelim Street
Tel Aviv 67897, Israel
Tel: 972-3-753 4555
Fax: 972-3-624-1100
email: info@checkpoint.com

U.S. Headquarters
800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391 ; 650-628-2000
Fax: 650-654-4233
URL: **http://www.checkpoint.com**

August 10, 2012