DEFEND AGAINST DENIAL OF SERVICE (DOS AND DDOS) ATTACKS

Protect each IT service layer against exploitation and abuse
Defending Against Denial of Service Attacks

Protect each IT service layer against exploitation and abuse

The Situation
An organization becomes a target of a Denial of Service attack. Hundreds or even thousands of hosts are co-opted by a malicious programmer to strike against a single victim. The service the organization provides becomes unavailable to its customers. The customers start to question the ability of the organization to properly secure information and provide timely access to it. Sound familiar?

Most organizations realize that stopping denial of service (DoS/DDoS) attacks is imperative for business continuity and continued success, but the complexity of these attacks makes it difficult for the IT department to protect the service infrastructure. Until IT identifies and implements security countermeasures at each service layer, most organizations will remain unprepared to handle these threats effectively.

Driving Concerns
Many organizations have experienced lengthy service outages from DoS/DDoS attacks. These attacks can devastate an organization in several ways. First, the business loses any revenue it would have captured during the outage. Second, employees and businesses that utilize or rely on these services lose productive work time or resort to less efficient—and often less secure—means of doing business. Third, some organizations face financial penalties if they fail to meet contractual service level agreements. Fourth, an organizational reputation that has taken years to establish is damaged within hours.

A DoS/DDoS attack can be accomplished in a number of ways. Most commonly today these attacks are originating from Botnets that may contain thousands and in some cases millions of hosts. These Botnets are available for rent and for a nominal fee an individual or group can leverage it against your organization to render your services unavailable.

The fundamental types of attack are: the consumption of computational resources, disruption of configuration information, disruption of state information, disruption of physical components, or obstruction of communications. These different attacks can be used against any of an organization’s IT service layers, including:

- **Network infrastructure.** The network infrastructure includes the physical hardware used to transmit data such as routers and switches and also a variety of other in-line devices such as firewalls and intrusion prevention systems
- **Network services.** Common network services include, but are not limited to, authentication services, DHCP, DNS, email, printing, network file system, and directory services
- **Applications.** This layer consists of business-oriented, data-centric applications such as online shopping and online payment processing, automated billing systems, IT service management, customer relationship management, resource planning, and business intelligence systems
- **Endpoints.** An endpoint is any system that connects to the network and communicates over the network infrastructure. Servers, desktop computers, mobile devices, IP phones, and printers are all examples of a network endpoint.
Since DoS/DDoS attacks can occur at any or all of these different IT service layers, many organizations find that implementing an effective solution can be difficult. The team may have limited knowledge of each layer’s potential reliability and performance issues, as well as possible and appropriate mitigation strategies. Many companies fail to invest because they fear the answer will inevitably require prohibitive capital expenses.

**Solution Description**

To protect against DoS and DDoS attacks, McAfee recommends a defense-in-depth approach. A best of breed set of security technologies should be deployed in multiple layers, but under a common and integrated strategy. This approach addresses specific technical requirements that span the IT service layers to detect and fend off a denial of service attack:

- **Service visibility.** Especially as they move to more sophisticated models of dynamic services and cloud computing, businesses must monitor the real-time status of the services they are providing.
- **Performance and availability.** Today’s attacks can come at multi-gigabit speeds. When choosing a security solution to counter a DoS/DDoS attack, you should not need to sacrifice performance to ensure availability.
- **Protection.** The antiquated approach of simply defending against a DoS/DDoS attack at the network perimeter is short sighted. The sophistication, form, and origination of DoS attacks vary. Security countermeasures should be deployed at each service layer to adequately protect your business and take advantage of real-time reputation based analysis to block dynamic addresses and bots used in DoS/DDoS attacks.
- **Coordination.** Today’s high adoption of broadband connectivity coupled with the availability of freely distributed DDoS software puts a business connection to the Internet at risk. For very large DDoS attacks, organizations can no longer rely on overprovisioning their network as their only DoS/DDoS countermeasure. You should establish a communications plan and technical countermeasures to coordinate your organization’s actions with those of your upstream Internet Service Providers (ISPs).

**Decision Elements**

These factors could influence your architecture:

- High speed network links—10 gigabit and higher network links
- Flexible connectivity requirements—Copper or fiber (single mode and multi-mode) interfaces
- Need for bidirectional attack mitigation—The ability to stop not only inbound, but also outbound DoS floods in the event of internal, compromised hosts participating in an outbound attack
- Network high availability or bypass features
- Monitoring of virtual servers
- Comprehensive application and protocol support
- Mixed OS environment
- Centralized monitoring, alerts, and reports
Technologies Used in the McAfee Solution

The McAfee solution is multifaceted, integrated, and built on the real-time sharing of information. It includes intrusion prevention solutions within the network and on the host, reinforced by a next-generation firewall and network threat behavior analysis, and enriched by the proactive analysis of cloud-based McAfee Global Threat Intelligence from McAfee Labs™. These solutions work to reduce the attack surface. Integrated management and database activity monitoring connect to these systems to provide IT staff with visibility into DoS and other network attacks and guide remediation.

McAfee Global Threat Intelligence

McAfee products use real-time data to recognize and block the dynamic addresses used in DoS attacks. McAfee Global Threat Intelligence network connection reputation is McAfee's comprehensive, real-time, cloud-based service that combines IP address, network port, and communications protocol to determine granular reputation intelligence, enabling McAfee products to protect customers against both known and emerging network threats.

McAfee collects data from billions of IP addresses and network ports, providing hundreds of trillions of unique views, and calculates a reputation score based on network traffic, including port, destination, protocol, and inbound and outbound connection requests. The score reflects the likelihood that a network connection poses a threat, such as a connection associated with botnet control. The score is based not only on the collective intelligence from sensors querying the McAfee cloud and the analysis performed by McAfee Labs researchers and automated tools, but also on the correlation of cross-vector

How McAfee products defend against a common DoS/DDoS attack scenario

[Diagram showing the flow of traffic and the steps McAfee takes to defend against DoS/DDoS attacks]
intelligence from file, web, and network threat data. McAfee products, including McAfee Firewall
Enterprise, McAfee Network Security Platform, and McAfee Host Intrusion Prevention, use the score to
determine action based on local policy.

• Protects endpoints from distributed denial-of-service (DDoS) attacks, botnets, command and control
  activity, advanced persistent threats, and risky web connections
• Reduces system and network burden by blocking threats at the network edge
• Decreases downtime and remediation costs associated with network-based attacks

McAfee Global Threat Intelligence is included in the cost of McAfee products that incorporate this
service. In some products, McAfee Global Threat Intelligence is enabled by default. If not, you may
enable it easily in your McAfee product administrative interface.

McAfee Network Security Platform
McAfee Network Security Platform integrates hardware and software for comprehensive protection from
known, first strike (unknown), DoS, and DDoS attacks, processing traffic ranging from several hundred
Mbps to multi-gigabit speeds. The McAfee Network Security Platform architecture combines threshold-
based and self-learning, profile-based detection techniques to detect DoS and DDoS attacks.

With threshold-based detection, you can configure data traffic limits to ensure your servers will
not become unavailable due to overload. You can configure your preferred thresholds based on
desired coverage of different DDoS attacks and the unique performance attributes of your network
infrastructure.

Meanwhile, self-learning methodologies enable McAfee Network Security Platform to study the patterns
of network usage and traffic as they change over time, thus understanding the wide variety of lawful,
though unusual, usage patterns that may occur during legitimate network operations. The learning
algorithm takes into account sudden bursts that are common in all network traffic, and differentiates
these normal intense activities from the real onset of DDoS traffic. In addition to learning the intensity
behavior, it also learns the correlational behavior of different types of packets, such as TCP/IP protocol
behavior and route configuration.

The combination of threshold and learning techniques yields the highest accuracy of detection for DoS
and DDoS attacks. Highly accurate DoS detection techniques are essential because popular websites and
networks do experience legitimate and sometimes unexpected traffic surges during external events, or
for a particularly compelling new program, service, or application.

Integration of real-time, reputation-based intelligence through McAfee Global Threat Intelligence
provides the McAfee Network Security Platform with additional context for enforcing network security
policies, not to mention faster, more accurate threat detection. File, host, geo-location, and network
connection reputation feeds from cloud-based McAfee Global Threat Intelligence allow Network Security
Platform to perform in-line malicious file and botnet prevention based on over 60 million malware
samples and the reputation of hundreds of millions of network connections based on over two billion
IP reputation queries each month. By dropping connections with malicious bots, the system can defuse
DoS attacks.

The McAfee Network Security Platform (NSP) also includes these capabilities designed to thwart DoS/
DDoS attacks:

• Rate limiting. Controls the rate of egress traffic sent through the ports of the NSP sensor. When
  the NSP sensor is deployed in line, an Administrator can set GTI (location, reputation), application/
  protocol, TCP port, UDP port, and IP protocol number-specific bandwidth limits that are appropriate for
  preventing DoS in a particular network.
• Syn proxy. Ensures that under a SYN flood, all connection requests are screened and only legitimate
  requests are forwarded
• DNS protect. Forces DNS clients to use TCP instead of UDP as their transport protocol. This setting can
  mitigate DNS DoS flood attack: since TCP uses a three-way handshake, IP addresses cannot be spoofed.
• **Dynamic filtering.** Identifies malicious behavior and punishments that behavior by creating a filtering rule (ACL) to block the source of the attack.

• **Static filtering:**
  » **Dark addresses.** Any packets coming from or going to dark addresses—IP addresses that are not yet assigned by IANA—are signs of spoofing. By blocking them, you can block a substantial percentage of spoofed DDoS packets.

  » **Whitelist, blacklist.** In any network, there will always be some IP addresses that you want to deny or allow. Whitelisting and blacklisting are useful during DDoS attacks to ensure that legitimate traffic gets through and known bad traffic is blocked, even while the NSP is inspecting other traffic for possible DDoS behaviors.

• **Application DoS exploits.** Specific signatures can be enabled to prevent exploit-based DoS attacks against applications. The signatures are updated by McAfee multiple times per month and can be implemented automatically, without administrator intervention.

**McAfee Network Threat Behavior Analysis**
This appliance provides a graphical, configurable, real-time view of network traffic. The McAfee Network Threat Behavior Analysis appliance gathers flow and application data from across users, applications, hosts, and devices and stores them in an embedded database. By analyzing netflow traffic from switches and routers from vendors such as Cisco, Juniper, and Extreme Networks, and layer seven application traffic from the McAfee Network Security Platform, McAfee Network Threat Behavior Analysis can pinpoint risky behavior to specific points in the network and effectively prevent internal and external threats. McAfee Network Threat Behavior Analysis rapidly drills down into complex, multi-vector attacks and blended threats. It holistically evaluates network-level threats, identifies the overall behavior of each network element, and enables instant abstraction of potential anomaly or attack type—including distributed denial of service (DDoS), botnets, or worms.

**McAfee Firewall Enterprise**
McAfee Firewall Enterprise allows you to protect your network from unauthorized users and attackers, and to protect internal users as they access the Internet. McAfee Firewall Enterprise combines an application-layer firewall, user-based policy, IPsec VPN capabilities, SSL decryption, and McAfee Global Threat Intelligence into one security appliance for centralized perimeter security. These features provide powerful configuration options that allow you to control your users’ access to almost any publicly available service on the Internet, while mitigating threats to your organization. As a next-generation firewall, advanced capabilities, such as application visualization, reputation-based global intelligence, automated threat feeds, encrypted traffic inspection, anti-virus, and content filtering, block attacks before they occur.

Integrated geo-location in the McAfee Firewall Enterprise allows you to defend against DoS/DDoS attacks by restricting traffic based on geography. You can formally allow or deny both inbound and outbound traffic based on country. This tactic is especially effective when you also restrict communications with countries where your company does not do business.

Another level of protection integrates the McAfee Global Threat Intelligence (GTI) service to analyze the behavior of millions of hosts connected to the Internet. The Firewall Enterprise can leverage the GTI reputation information to block traffic from any host with a bad reputation.

**McAfee Host Intrusion Prevention (with Desktop Firewall)**
McAfee Host Intrusion Prevention is a host-based intrusion detection and prevention system that protects system resources and applications from external and internal attacks. It delivers a manageable and scalable intrusion prevention solution for workstations, notebooks, and critical servers, including web and database servers. It proactively blocks zero-day and known attacks with patented technology.

In addition, Host Intrusion Prevention protects against DoS attacks that exploit vulnerable applications running on the endpoint. It uses a combination of behavioral rules, host and network signatures, and a system firewall to block attacks and reduce the urgency of patches for new threats.
Just like the Firewall Enterprise, the built-in desktop firewall can also leverage reputation information from the McAfee Global Threat Intelligence service and block attacks from hosts that have been identified to have a bad reputation.

**McAfee Database Activity Monitoring**

With McAfee Database Activity Monitoring, organizations gain visibility into all database activity, including local privileged access and sophisticated attacks such as exploit-based DoS attacks from within the database. McAfee Database Activity Monitoring helps you protect your most valuable and sensitive data from external threats and malicious insiders. Database Activity Monitoring monitors activity locally on each database server and alerts or terminates malicious and non-compliant behavior in real time, even when running in virtualized or cloud computing environments. By providing a reliable audit trail, McAfee Database Activity Monitoring can help teams understand attack sequences and implement effective countermeasures.

McAfee Database Activity Monitor is vulnerability aware and can be used to “virtually patch” and prevent databases against attacks attempting to exploit known vulnerabilities as well as common threat vectors. The Database Activity Monitor can be configured to either issue an alert or terminate the session in real time.

**Optional Integrations**

Organizations can install McAfee Firewall Enterprise features on other platforms such as the Riverbed Steelhead equipment, adding network and application visibility to Riverbed’s WAN optimization and server consolidation capabilities. Crossbeam’s X-Series can also be leveraged by the Firewall Enterprise to allow your organization to address all performance and port density requirements, providing up to 40 Gbps of inspected traffic throughput.

Of course, all McAfee products integrate to various degrees with McAfee ePolicy Orchestrator® (McAfee ePO™) software. This provides the organization an “at-a-glance” view of the risks facing an organization and pinpoints areas that need attention. From the McAfee ePO dashboards, you can quickly drill down to get granular details of threats and compliance issues as they relate to specific assets.

McAfee Network Security Platform works with McAfee ePolicy Orchestrator for on-demand visibility to critical host details, threats, and risk relevance. You gain a real-time view of actionable system host details, including host name, user name, OS, patch level, media access control (MAC) address, last scan date, protection details, and the top host intrusion prevention system, anti-virus, and anti-spyware events. With this information, administrators can determine the right response to suspicious events.

**Impact of the Solution**

The McAfee solutions will cover the four IT service layers within your organization to help you reduce the chance of a DoS or DDoS attack damaging your business.

- **Network infrastructure.** McAfee Network Security Products such as the McAfee Firewall Enterprise, Network Security Platform, and Network Behavioral Threat Analysis will help you shut down attacks that try to overwhelm your network infrastructure while you continue to permit approved traffic. These products also allow you to monitor and understand suspicious network traffic so you can fine-tune your policies, rules, and countermeasures.

- **Network services.** Products such as McAfee Host Intrusion Prevention can help you preserve critical network services and overlay application-layer protections against known and unknown exploits, leveraging signature and behavior analysis detection engines

- **Applications.** In addition to using McAfee Host Intrusion Prevention to protect your applications, McAfee Database Activity Monitoring helps protect the databases that underlie many applications to keep business activity flowing.

- **Endpoints.** Robust intrusion prevention and firewall defenses on the host prevent your internal systems from attack, and also participating in or propagating DoS attacks.
All the while, McAfee Global Threat Intelligence provides real-time threat information to McAfee products to keep protections up to date and guard against the ever-dynamic threat landscape.

These solutions can also help you move from a reactive security posture to a proactive security architecture. With a best of breed set of security technologies deployed in multiple layers, but under a common and integrated strategy, you can say “yes” to new business opportunities, processes, and even the latest devices. You can have the security control required for risk management and compliance, while enabling productivity and cost savings from more efficient security operations.

Additional Resources
www.mcafee.com/gti
www.mcafee.com/nsp
www.mcafee.com/firewall
www.mcafee.com/network-threat-behavior-analysis
www.mcafee.com/host-ips-for-desktop
www.mcafee.com/dbactivitymonitoring

For more information about the Security Connected Reference Architecture, visit:
www.mcafee.com/securityconnected

About the Author
Scott Sloan is a Senior Sales Engineer for the U.S. Federal sales group of McAfee. Scott covers technology across the McAfee Network, Endpoint, Mobile and Risk & Compliance product solutions. Scott was previously the Cyber Security Operations Manager of nationwide operations for core IT services for the Department of Energy, providing services to the DOE Chief Information Officer.

Prior to supporting the Department of Energy, Scott was the founder of Palladian Technology, a successful IT professional services firm specializing in cyber security and virtualization services to the U.S. Federal government. He also worked for IntruVert Networks, a pioneer of network intrusion prevention technology, supporting sales of their network IPS sensors. He is also a Navy veteran with five years of service aboard the U.S.S. Enterprise and three years of service at the Pentagon supporting the Chief of Naval Operations.

Scott holds a Bachelor of Science degree in computer science from the University of Maryland University College.