Business Case for a DDoS Consolidated Solution

Executive Summary

Distributed denial-of-service (DDoS) attacks are becoming more serious and sophisticated. Attack motivations are increasingly financial or political. Roughly half of all attacks last a day or more, and their costs are estimated to be $2.1 million for every four hours of downtime. Attacks are made at all network layers, and network firewalls by themselves are inadequate to mitigate the attacks.

F5 leverages its unique point of control to deliver a comprehensive DDoS mitigation solution. It starts with a complete contextual understanding of all traffic flowing through the device to make intelligent traffic management decisions. It then applies that context to a two-tier (L3-4 and L7) model that encompasses multilayer protection for Domain Name System, network, SSL, and applications. F5 uses a common hardware and software framework to deliver these services. This simplifies the configuration and management of network resources without any hardware restrictions.

ACG Research analyzed the total cost of ownership (TCO) of a DDoS mitigation use case for a large enterprise. The TCO of the F5 consolidated solution was compared to the TCO of a solution using multiple point products offered by leading DDoS mitigation vendors. It found that the F5 solution has 81 percent lower TCO over five years. Capital expense (CapEx) is 80 percent lower and operations expense (OpEx) is 82 percent lower. Consolidation of all DDoS functions in a two-platform solution eliminates replication of i/o ports (back-to-back) and common costs, such as power supplies, backplanes, and software operating systems. In addition, F5's use of a single management interface eliminates a great deal of the complexity involved in using multiple management interfaces for the alternative point products solution.

KEY FINDINGS

F5 provides a comprehensive DDoS mitigation solution using a two-tier (L3-4 and L7) architecture. As compared to a solution using multiple point products over five years it has:

- 81% lower TCO, 80% lower CapEx and 82% lower OpEx
- Reduced CapEx through elimination of redundant i/o ports and chassis
- Reduced OpEx through use of a single management interface, elimination of multiple vendor service agreements, simplification of operations and maintenance activities
- 94% lower environmental expenses through the elimination of the common costs of multiple chassis

Introduction

Distributed denial-of-service (DDoS) attacks are constantly changing. While the objective is still to cause a service outage, attacks and attackers are becoming more sophisticated. Motivations for attacks are increasingly financial or political—with more serious consequences for the targeted victims. The average downtime caused by a DDoS attack is 54 minutes[1], but roughly half of all attacks last a day or more. This costs $2.1 million for every four hours of downtime[2].

High-profile businesses, such as financial institutions, governments, and service providers, continue to be targets, but a rising number of everyday businesses are also reporting being under attack.

DDoS attacks focused on Layers 3/4 in the past. Network firewalls were able to provide a basic line of defense. In response to that defense, attackers are moving up the stack and focusing on using SSL and application-layer attacks to overwhelm resources. Security solution vendors estimate that today three-quarters of all attacks are at the network layers; one-quarter are at the application layer, where the share of total attacks is increasing.

Network firewalls have failed to keep up with the volume and intelligence of these attacks. These firewalls have no contextual understanding of the traffic they handle, and so they are powerless to defend against multilayered attacks. Consequently, a comprehensive multilayer approach is required to mitigate DDoS attacks. DDoS mitigation requirements include:

- Maintain application availability
- Protect network infrastructure
- Safeguard brand reputation
- Defend against targeted attacks
- Stay one step ahead (scalability)
- Save money (Minimize TCO of DDoS mitigation solution)

F5's Value Proposition

F5 leverages its unique point of control in the network to deliver a comprehensive DDoS protection solution. F5 starts with a complete contextual understanding of all traffic flowing through the device to make intelligent traffic management decisions. It then applies that context to network firewall, web application firewall, and Domain Name System (DNS) security capabilities. The high-performance, stateful, full-proxy network firewall defends against network-layer DDoS attacks such as SYN floods as well as session-layer attacks such as SSL floods[3]. Deep application fluency enables the web application firewall to detect and mitigate HTTP-based attacks. A scalable DNS and DNSSEC solution mitigates DNS-based attacks. Elements of the F5 solution include:

- **Scale and performance:** Scales to up to 100s million concurrent connections, 100s Gbps of throughput, and millions of connections per second.

[1] Ponemon Institute, November 2012

[2] Forester Research, May 2013

[3] A SYN flood attack uses a fake TCP connection to overflow tables in stateful devices. An SSL flood attack uses a connection flood to overflow flow tables within established SSL sessions.

- **DDoS protection for all layers:** Provides security at all layers: network, DNS, SSL, and application. The solution protects not only protocols but also applications.

- **SSL termination:** Offloads and inspects SSL traffic, making it the only place in the network where early content analysis and mitigation can be performed for SSL attacks. The SSL proxy also can mitigate SSL floods and renegotiation attacks.

- **Extensible security and dynamic threat mitigation:** Provides the means to react to DDoS threats and vulnerabilities for which an associated patch has not yet been released.

Two-Tier DDoS Mitigation Use Case

The TCO advantages of the F5 solution are illustrated by making a TCO comparison between the F5 unified DDoS mitigation solution and a solution where each DDoS mitigation function is hosted on a separate system produced by a leading vendor of DDoS mitigation (alternative point products) solutions. A two-tier (L3/4, L7) DDoS mitigation use case applicable for a large enterprise is used to make the comparison.

The two-tier DDoS mitigation use case incorporates multilayer protection for:

- **Domain Name System:** Attacks designed to disrupt the DNS. This is the most critical (and public) of all web services.

- **Network:** Basic DDoS attacks designed to flood and disrupt the L3/4 network. The L3/4 network is the weakest link in the network chain.

- **SSL:** Attacks designed to overwhelm a web server that is terminating SSL connections.

- **Applications:** Attacks designed to flood web servers with fake HTTP web requests or take over web server network and memory resources.

The two-tier architecture allows the application layer (Tier 2) to scale independently of Tier 1. It also allows different code versions, platforms and even security policies to exist within the two tiers.

The first tier is built around the network firewall. At this tier Layer 3 and Layer 4 (IP and TCP) defenses are provided.

Tier 2 provides application-aware defense mechanisms such as login walls, web application firewall policy and load balancing rules. This also is where SSL termination takes place. SSL termination is rare at Tier 1 because of the sensitivity of SSL keys and policies against keeping them at the perimeter.

Traffic Model

TCO is estimated by configuring the F5 unified solution and the alternative point products solution to meet traffic requirements defined as throughput (Gbps) and TCP connections per second (CPS) for Tiers 1 and 2. Millions of packets per second (Mpps) also is used to configure the Tier 1 network elements.

Table 1 and Table 2 show the value of the traffic requirements used for the Tier 1 and Tier 2 network configurations.

Metric	Value
Throughput (Gbps)	50
Connections per Second (million)	0.25
Millions Packets per Second	12

Table 1 – Tier 1 Traffic Requirements

Metric	Value
Throughput (Gbps)	39
Connections per Second (million)	0.1

Table 2 – Tier 2 Traffic Requirements

These values are used to configure each network element of the F5 and alternative point products solutions described below. They have been chosen to be representative of the values used by a large enterprise.

50 Gbps Tier 1 throughput provides 20 Gbps to support the expected sustained production load on the data center; 30 Gbps additional throughput is provisioned to provide the capacity needed to absorb traffic generated by a DDoS attack. 39 Gbps Tier 2 throughput provides the capacity to support expected production capacity plus DDoS attack traffic that was not mitigated at Tier 1.

F5 DDoS Mitigation Solution

Figure 1 provides a network schematic for the F5 solution, which is hosted by two F5 BIG-IP application delivery controllers.

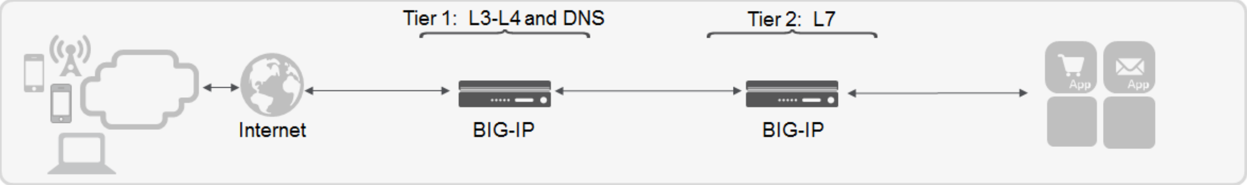

Figure 1 – F5 Two-Tier DDoS Mitigation Solution

The BIG-IP platform provides a unified solution that simplifies the network by hosting all software applications on a single platform and provides a single unified management interface. It features a scalable architecture that includes:

- On-demand scaling: Software license upgraded on demand
- Operational scaling: Multitenant device virtualization, role-based access
- Application scaling: Scale across device and service clusters

For Tier 1 the F5 software applications are:

- BIG-IP Local Traffic Manager (LTM): Provides traffic management, load balancing, and application delivery
- BIG-IP Advanced Firewall Manager (AFM): Provides a network firewall, SSL visibility at scale, and network-layer and session-layer distributed DDoS mitigation
- BIG-IP Global Traffic Manager (GTM): Scales and secures DNS responses geographically to survive DDoS attacks

For Tier 2 the F5 software applications are:

- BIG-IP Local Traffic Manager (LTM): Provides traffic management, load balancing, and application delivery
- BIG-IP Access Policy Manager (APM): Provides access management, secure remote access, and user context
- BIG-IP Application Security Manager (ASM): Delivers application security, web scraping and bot prevention, and HTTP DDoS mitigation

The routers and other network elements shown in the diagram are common to both solutions and, therefore, are excluded from the analysis.

Alternative Point Products Solution

Figure 2 provides the network schematic for the alternative point products solution:

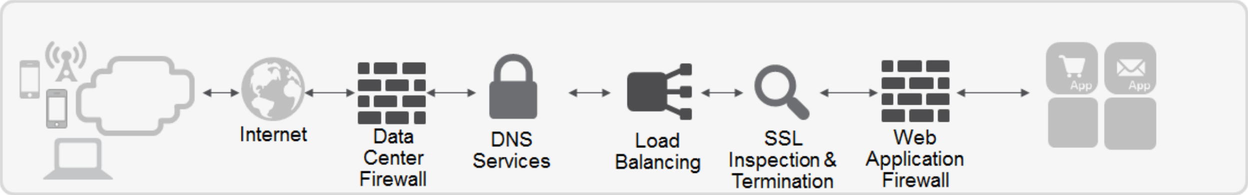

Figure 2 – Alternative Point Products Two-Tier DDoS Mitigation Solution

In this solution each function is hosted on a separate appliance. The study incorporates the configuration, performance characteristics and market pricing of each appliance type of a leading vendor.

TCO Results for Two-Tier DDoS Mitigation Use Case

Figure 3 shows the TCO comparison for the network simplification use case.

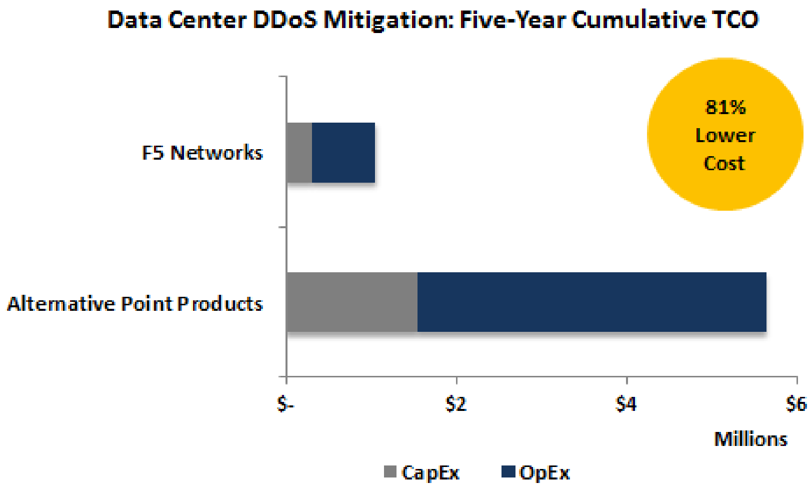

Figure 3 - Five-Year TCO Comparison

The F5 unified solution has 81 percent lower TCO over five years as compared to the alternative point products solution. Capital expense (CapEx) is 80 percent lower and operations expense (OpEx) is 82 percent lower. Unification of all five functions in a single solution eliminates replication of i/o ports (back-to-back) and replication of chassis common costs, such as power supplies, backplanes, and software operating systems. This is the primary source of the CapEx savings produced by the F5 unified solution.

Vendors' service contract expense is a very large portion of total OpEx for this use case. The F5 unified solution has 81 percent lower service contract expense than the alternative point products solution. The use of a single management interface by the F5 unified solution eliminates a great deal of the complexity involved in using five different management interfaces for the alternative point products solution. Also, one service contract consolidates much of the administrative and staffing overhead incurred when five separate contracts are required.

Figure 4 provides a comparison of all other OpEx items (service contracts excluded) for the F5 unified solution and alternative point products solution.

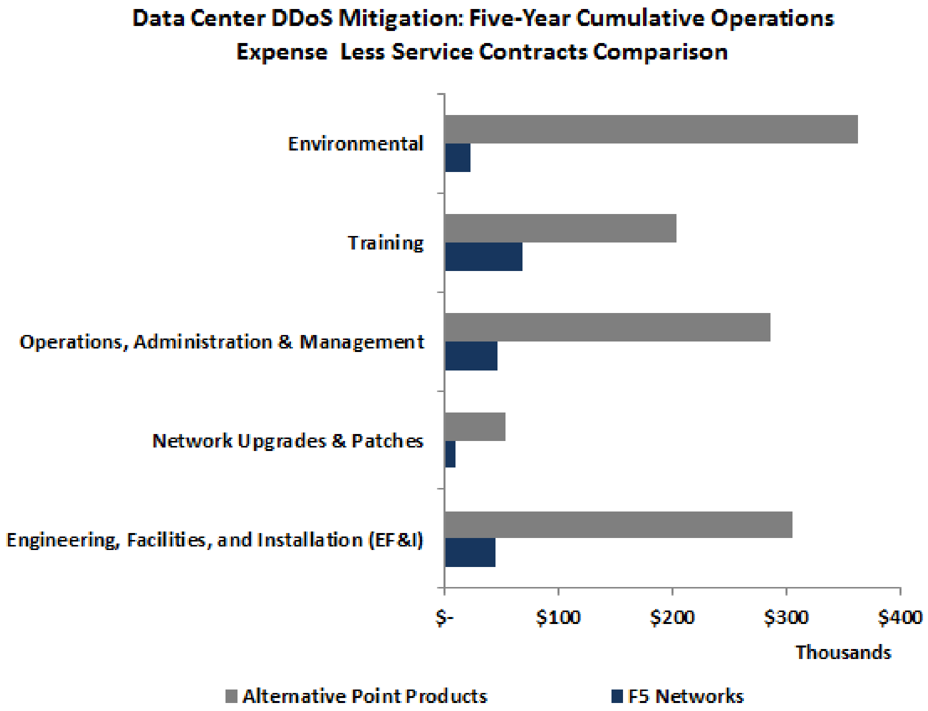

Figure 4 - Five-Year Cumulative OpEx Comparison (Service Contracts Excluded)

Environmental expense is the second largest OpEx category. It is 94 percent lower than the environmental expense of the alternative point products solution. Environmental expense is lower because one chassis requires less power, cooling and floor space than five chassis. Engineering, facilities, and installation; and operations, administration and management expenses are lower because 1) it is only necessary to learn a single management interface for the unified solution, and 2) there is much less equipment under management with the consolidated solution versus the point products solution.

Conclusion

DDoS attacks are becoming more serious and sophisticated. Attacks are made at all network layers, and network firewalls by themselves are inadequate to mitigate the attacks.

A comprehensive multilayer approach is required for DDoS attack mitigation. It includes:

- Maintain application availability
- Protect network infrastructure
- Safeguard brand reputation
- Defend against targeted attacks
- Stay one step ahead (scalability)
- Save money (Minimize TCO of DDoS mitigation solution)

F5 provides a unique point of control in the network to deliver a comprehensive DDoS mitigation solution. Its solution includes:

- **Scale and performance:** Scales to up to 100s million concurrent connections, 100s Gbps of throughput, and millions connections per second.

- **DDoS protection for all layers:** Provides security at all layers: network, DNS, SSL, and application. The solution protects not only protocols but also applications.

- **SSL termination:** Offloads and inspects SSL traffic, making it the only place in the network where early content analysis and mitigation can be performed for SSL attacks. The SSL proxy also can mitigate SSL floods and renegotiation attacks.

- **Extensible security and dynamic threat mitigation:** Provides the means to react to DDoS threats and vulnerabilities for which an associated patch has not yet been released.

F5 employs a two-tier (L3/4 and L7) solution hosted on two BIG-IP application delivery controllers.

The TCO of the F5 solution was compared to an alternative point products solution where each DDoS mitigation function is provided on a separate platform of a leading DDoS mitigation vendor. The F5 solution has 81 percent lower TCO over five years as compared to the alternative point products solution. CapEx is 80 percent lower and OpEx is 82 percent lower. Unification of all five functions in a single solution eliminates replication of i/o ports (back-to-back) and replication of chassis common costs, such as power supplies, backplanes, and software operating systems. In addition, F5's use of a single management interface eliminates a great deal of the complexity involved in using five different management interfaces for the alternative point products solution. These are the primary sources of the savings produced by the F5 solution.