Large FSI DDoS Protection Reference Architecture

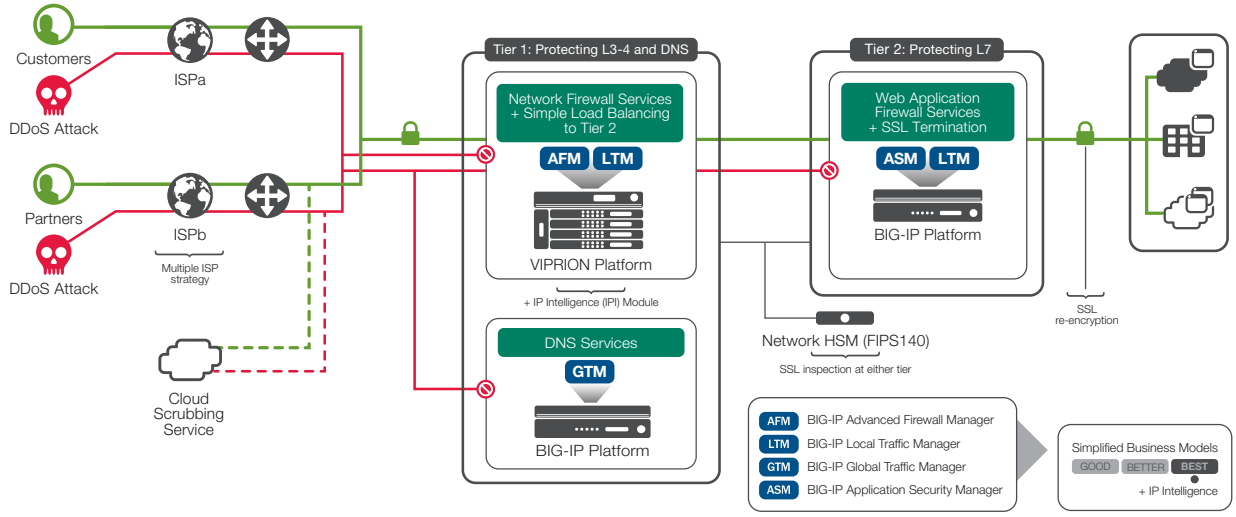

Figure 4: The F5 DDoS protection large FSI data center deployment scenario

FSI customer scenario

The large FSI data center scenario is a mature, well-recognized use case for DDoS. This is what FSIs are building right now. Typically the FSI will have multiple service providers but may forgo those service providers' volumetric DDoS offerings in favor of a cloud-based scrubbing service. The FSI data center often has few corporate staff within it so there is no need for a next-generation firewall.

FSIs have the most stringent security policy outside of the federal/military vertical. For example, nearly all FSIs must keep the payload encrypted through the entire data center. FSIs have the highest-value asset class (bank accounts) on the Internet, so they are frequent targets—not just for DDoS but also for hacking. The two-tier architecture enables FSIs to scale their CPU-intensive, comprehensive security policy at tier 2 independently of their investment in tier 1.

This use case allows FSIs to create a DDoS-resistant solution while retaining (indeed, while leveraging) the security equipment that they already have. The firewalls at tier 1 continue to do their job, and the BIG-IP ASM devices at tier 2 continue to prevent breaches.

Location	F5 Equipment
Tier 1	VIPRION Chassis (Pair)
	VIPRION Add-On: BIG-IP AFM
Tier 2	Mid-Range BIG-IP Appliance
	License Add-On: BIG-IP ASM
DNS	Mid-Range BIG-IP Appliance (Pair)

Table 4: Sizing recommendations for the FSI customer deployment scenario

Enterprise DDoS Protection Reference Architecture

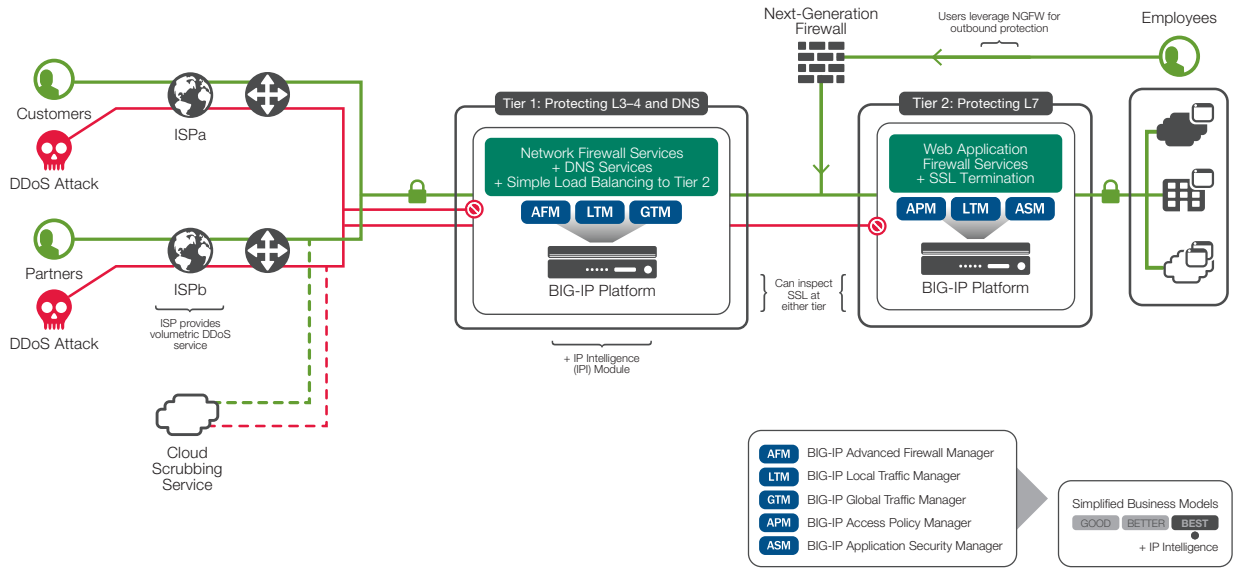

Figure 5: The F5 DDoS protection enterprise data center deployment scenario

Enterprise customer scenario

The enterprise anti-DDoS scenario is similar to the large FSI scenario. The primary difference is that enterprises do have staff inside the data center and therefore need the services of a next-generation firewall (NGFW). They are tempted to use a single NGFW for both ingress and egress, but this makes them vulnerable to DDoS attacks. Another difference is that enterprises will often use the volumetric DDoS service offered by the Internet service provider (ISP).

The recommended enterprise architecture includes a smaller NGFW on a separate path from the ingress application traffic. By using two tiers, the enterprise can take advantage of asymmetric scaling. They can add more BIG-IP ASM devices if they find that their CPU at tier 2 is at a premium.

Different verticals and companies have different requirements. By using F5 equipment at both tiers, the enterprise architecture allows the customer to decide where it makes the most sense for them to decrypt (and optionally re-encrypt) the SSL traffic. For example, an enterprise can decrypt SSL at tier 1 so that they can mirror the decrypted traffic off to a network tap that is monitoring for advanced threats.

Location	F5 Equipment
Tier 1	High-End BIG-IP Appliance (Pair)
	License Add-On: BIG-IP AFM
Tier 2	Mid-Range BIG-IP Appliance
	License Add-On: BIG-IP ASM
DNS	Mid-Range BIG-IP Appliance (Pair)

Table 5: Sizing recommendations for the enterprise customer deployment scenario

SMB DDoS Protection Reference Architecture

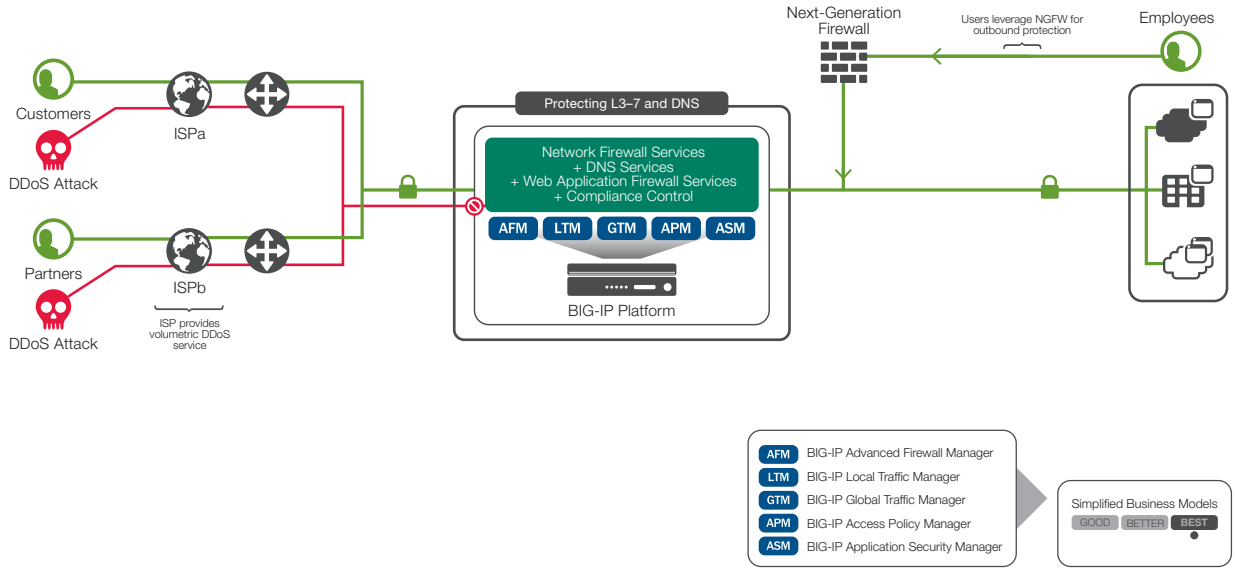

Figure 6: The F5 DDoS protection small-to-medium business data center deployment scenario

SMB customer scenario

The SMB data center use case is all about providing security while maximizing the value of consolidation. These businesses are very serious about getting the most bang for their buck. They would like to do everything from one device if they can, and they are willing to go offline during a DDoS attack.

For this use case, the customer is putting all their eggs in one basket. They will get the most cost-efficient solution but will also have the largest availability challenge. For example, if they have a policy issue with BIG-IP ASM, or if Application Visibility and Reporting cannot keep pace with the traffic, the entire box may become unavailable.

However, a one-tier architecture can actually reduce risk in smaller organizations that do not have the resources to support a larger, two-tier architecture. The organization gains efficiency by focusing specialized resources with deep knowledge on a single platform. F5 provides high availability systems, superior scale and performance, and world-class support that help further offset risk.

Certainly financial savings is the biggest benefit of the single-tier architecture. These customers get a superior DDoS solution with equipment that is already working to deliver their revenue-generating applications every day. The consolidated environment helps save on rack space, power, management, and a range of other costs.

Location	F5 Equipment
Single Tier	Mid- to High-End BIG-IP Appliance Pair
	License Add-On: BIG-IP GTM
	License Add-On: BIG-IP ASM
	License Add-On: BIG-IP AFM
	License Add-On: BIG-IP APM

Table 6: Sizing recommendations for the SMB customer deployment scenario

Sizing Specifications

Table 7 shows specifications for the range of F5 hardware devices that are available to meet customers' scaling requirements.

	Throughput	SYN Flood (per second)	ICMP Flood	HTTP Flood (JavaScript redirect)	SSL Flood (+20k attack requests)	TCP Connections	SSL Connections
VIPRION 2400 4-blade chassis	160 Gbps	196 million	100 Gbps	350,000 RPS	16,000 TPS	48 million	10 million
10200V Appliance High-end appliance	80 Gbps	80 million	56 Gbps	175,000 RPS	16,000 TPS	36 million	7 million
7200V Appliance Mid-range appliance	40 Gbps	40 million	32 Gbps	131,000 RPS	16,000 TPS	24 million	4 million
5200v Appliance Low-range appliance	30 Gbps	40 million	32 Gbps	131,000 RPS	16,000 TPS	24 million	4 million

Table 7: F5 hardware specifications for DDoS protection. See the customer use cases for specific sizing recommendations.

Conclusion

This recommended DDoS protection reference architecture leverages F5's long experience combatting DDoS attacks with its customers. Small- and medium-size businesses are finding success with a consolidated approach. Global financial services institutions are recognizing that the recommended two-tier architecture represents the ideal placement for all of their security controls. Enterprise customers are re-arranging and re-architecting their security controls around this architecture as well. For the foreseeable future, a two-tier DDoS protection architecture should continue to provide the flexibility and manageability that today's architects need to combat the modern DDoS threat.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

Solutions for an application world.