The F5 SSL Reference Architecture

The demand for data protection is driving SSL growth at 20 percent per year. This significantly impacts the efficiency of networks, and increases the need for visibility, control, and the management of application delivery. Looking ahead, security issues are expected to become more complex—making efficient, innovative solutions a priority for organizations.

White Paper

by F5

Introduction

The cryptographic protocol known as the Secure Sockets Layer (SSL) is quickly becoming the de-facto protocol for all important (and sometimes even casual) communications today. Only a decade ago, SSL was reserved only for financial institutions and for the login pages of the security-conscious. Today SSL is ubiquitous. Even the world's most popular video sites use SSL for streaming. According to the January 2014 Netcraft report, the use of SSL is growing at 20 percent per year.[1]

Although SSL can be an everywhere, all-the-time security protocol, it is not always easy to deploy correctly or without challenges into an architecture. For example, SSL offers protection for data in transit, not at rest. It offers forward secrecy, but usually at the cost of monitoring or diagnostic utilities. SSL also faces numerous attacks, despite being constantly improved and monitored by the Internet Engineering Task Force (IETF). Finally, implementation issues like the OpenSSL group's Heartbleed incident remind the world that cryptography is difficult—even for cryptographers.

The F5 SSL Everywhere reference architecture is centered on the custom-built SSL software stack that is part of every F5 BIG-IP Local Traffic Manager (LTM) deployment. This white paper identifies many of the customer scenarios where visibility, programmability, and management come together to form complete ecosystems for securing data in transit.

The SSL Reference Architecture

SSL is becoming the primary protocol between an organization and its customers. It protects traffic between those customers and the organization's services, whether those services are in the cloud or on premise.

Most of the F5 customer scenarios identified and addressed in the reference architecture are inbound cases. These include:

- Cipher Agility
- The Internet of Things
- Programmatic Control

Enterprises are finding that their outbound traffic is increasingly SSL as well. Outbound SSL has a distinct set of challenges for enterprises and the problems it masks can pose an even greater threat to internal resources than inbound.

- Policy-Based Traffic Steering
- Transformational Services

- Scalability

Reference architecture takes into consideration that many of the same challenges apply to both inbound and outbound traffic.

SSL Customer Scenarios

Since SSL began as an associate of the fundamental web protocol HTTP, it should be no surprise that it continues to find the most usage in service of the World Wide Web today. In the future, the two protocols (HTTP and SSL) will become even more intertwined when HTTP/2.0 requires SSL. But data protection isn't the whole story. Even within just the context of the web, there are several distinctive customer scenarios worth reviewing.

Visibility is important. When services and applications get multiplexed into a data center, the single point of control that decrypts the ciphertext—the application delivery controller (ADC)—becomes the logical place for policy-based traffic steering. This is also the first place than any kind of content-based control can happen.

Although it's not the most exciting topic, certificate management is critical to security administrators. Key management becomes simpler when security services are centralized, either at an ADC or at a network-attached hardware security module.

Data Protection

Data protection is a large umbrella that protects multiple services. The three most significant today include transformational services, cipher agility, and the scalability challenges that will be introduced as the Internet of Things grows larger than the Internet of People.

Transformational services

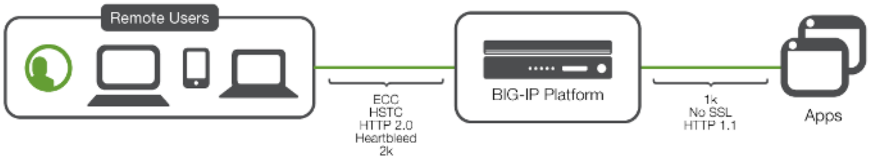


Figure 1: Transformational services convert one form of crypto to another.

The protocol infrastructure of the Internet is showing its age. Companies like Google are tinkering with the HTTP to reduce round-trip times between the client and server as in the SPDY protocol. The global surveillance issue is also spurring designers to build security right into the protocol itself—for example, HTTP/2.0 will require end-to-end cryptography.

These new protocols can be quickly implemented by leveraging an ADC or a similar strategic point of control within the network to speak an enhanced protocol like HTTP/2.0 with the end-user devices—while still speaking a legacy protocol with the back-end servers.

End-User Inbound	Back-End Server-Bound
HTTP/2.0	HTTP/1.1
SPDY	HTTP/1.1
SSL 4096 bit	SSL 2048 bit
SSL 2048 bit	SSL 1024 bit
SSL 2048 bit	HTTP/1.1
Elliptic Curve Cryptography	RSA 1024 bit

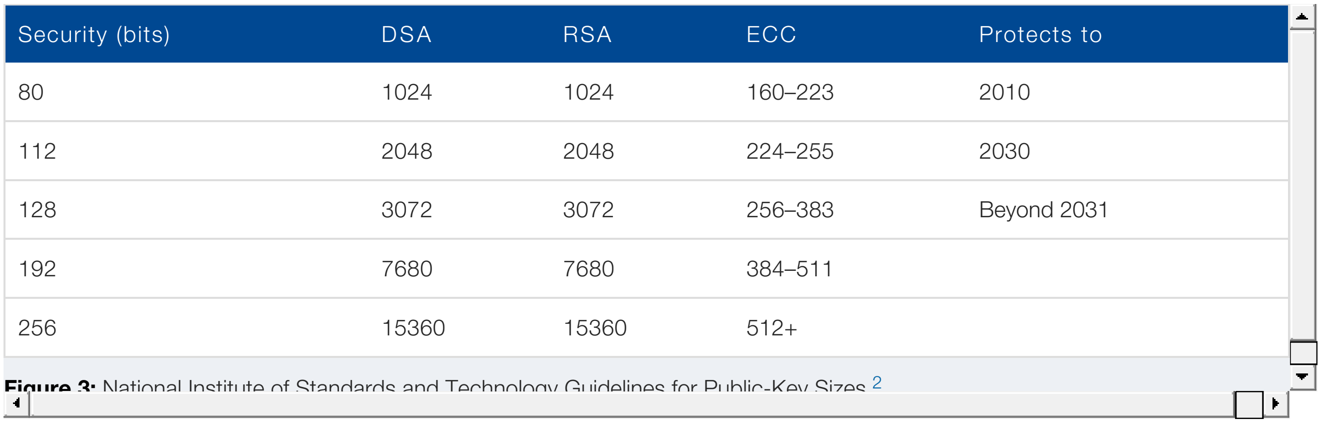
Figure 2: Common transformational services.

The power of transformational services is that they can proxy multiple protocols at the same time. An ADC may be terminating 2048-bit RSA SSL on one application while advertising elliptic curve cryptography (ECC) SSL on another—or even on the same virtual server.

Consider the operational savings when existing servers, services, and virtual machines do not need to be upgraded due to the transformational services in the SSL reference architecture.

Cipher agility

New cryptographic protocols are being introduced and gaining popularity. For instance, elliptic curve cryptography (ECC) offers the same level of security as previous algorithms while requiring less processing. This translates to a protocol that is friendlier to the battery life of mobile devices.



Security (bits)	DSA	RSA	ECC	Protects to
80	1024	1024	160–223	2010
112	2048	2048	224–255	2030
128	3072	3072	256–383	Beyond 2031
192	7680	7680	384–511	
256	15360	15360	512+	

Figure 3: National Institute of Standards and Technology Guidelines for Public-Key Sizes [2]

Organizations don’t want to reconfigure hundreds of servers just to offer these new protocols. This is where transformational services become cipher agility. Cipher agility is the ability of an SSL device to offer multiple cryptographic protocols such as ECC, RSA2048, and DSA at the same time—even on the same virtual server.

Internet of Things

Of course it’s necessary to connect a home computer to the Internet. And in many cases it makes sense to connect a home video camera, baby monitor, alarm system, and thermostat to the Internet as well. The sum of these network-attached devices is called the Internet of Things (IoT). IDC estimates that there will be 30 billion network-attached devices at the end of the decade.[3]

While some of the devices may be “read-only,” some are actionable or provide data that should not be available to third parties. These devices therefore require SSL for confidentiality. A subset of these SSL-enabled devices will use client certificates to identify themselves to the forwarding authority, which for many organizations will be their BIG-IP system.

This is where SSL capacity will become a critical issue. A successful product will produce (hopefully) millions of devices that will call home periodically. Experienced administrators know that the devices can become synchronized and call home at the same time (e.g., when a firmware update is available).

Figure 4 shows the SSL connection capacity of various BIG-IP product platforms, including the virtual edition. This table can be used for capacity planning for a successful IoT product launch.

Platform	SSL Connection Table Size
VIPRION 4480 (4 X B4300)	32 Million
VIPRION 4480 (1 X B4300)	8 Million
VIPRION 4400 (4 X B4200)	5 Million
VIPRION 4400 (1 x B4200)	1 Million
VIPRION 2400 (4 x B2100)	10 Million
VIPRION 2400 (1 x B2100)	2.5 Million
11000 series	2.64-3.9 Million
10200 series	7 Million
8900 series	2.64 Million
7000 series	4 Million
6900 series	660 Thousand
5000 series	4 Million
4200V series	850 Thousand
3900 series	660 Thousand
Virtual Edition	660 Thousand

Figure 4: SSL connection table size by platform.

Visibility and Control

A critical side effect of the confidentiality provided by the SSL protocol is that it can blind many network devices to the content of the traffic that the equipment is steering into the data center. This problem needs to be foremost among the minds of network and security architects as they rebuild for an SSL-everywhere world.

The solution to this problem, in general, is to be strategic about where the initial SSL decryption is taking place. To maximize the efficacy of layer 7 security devices, the SSL decryption should be near the security perimeter.

Once the inbound SSL has been decrypted, the resulting requests can be analyzed, modified, and steered.

Policy-based traffic steering (IDS/IPS, web analytics, NGFW)

Policy-based traffic steering can be in-line with the web data or passive in the case of monitoring and reporting.

Enhancing in-line security solutions

An example of policy-based traffic steering made possible by a programmable SSL decryption device (like an ADC) is the built around the intrusion prevention systems (IPS). A typical IPS excels at matching malicious traffic to thousands of signatures—but is not known for its SSL decryption performance.

The goal is to keep the IPS CPU focused on matching signatures and not performing redundant decryption. An ADC can keep the IPS targeted on its strengths by offloading the SSL decrypting for the IPS. When the IPS determines that a particular data source is sending malicious data, it can signal to the ADC that the source is not to be trusted (for a period of time, perhaps 15 minutes). The ADC can then block that source address at the layer 3 firewall level, thereby saving the intrusion detection system (IDS) from having to monitor more of that traffic and saving the SSL compute cycles on the ADC as well.

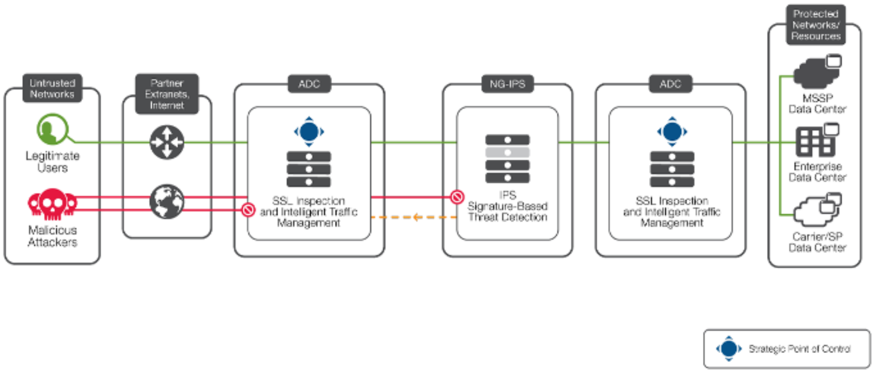

Untrusted Networks
Legitimate Users
Malicious Attackers
Partner Extranets, Internet
ADC
SSL Inspection and Intelligent Traffic Management
NG-IPS
IPS Signature-Based Threat Detection
ADC
SSL Inspection and Intelligent Traffic Management
Protected Networks/ Resources
MSSP Data Center
Enterprise Data Center
Carrier/SP Data Center
Strategic Point of Control

Figure 5: SSL is a key part of an efficient IDS deployment.

Find more details around in-line policy-based traffic steering in the Next-Generation IPS Reference Architecture.

The same approach can be applied to other in-line security technologies such as so-called next generation firewall (NGFW) devices, which are also known to struggle with SSL decryption.

Enabling passive monitoring

While the field of web analytics can encompass multiple subdomains, including security, it more commonly provides usability data for human interface designers. By mapping how users interact with the website—where they linger and how they skip—web analytics provides an essential view into the workings of the website and allows administrators to quantify the value of changes. Web analytics can be critical for revenue-generating web properties.

Clearly, the data examined by web analytics must be decrypted prior to observation. Many customers with advanced security requirements (usually financial) must also re-encrypt data before as it leaves the application delivery controller tier further into the web servers.

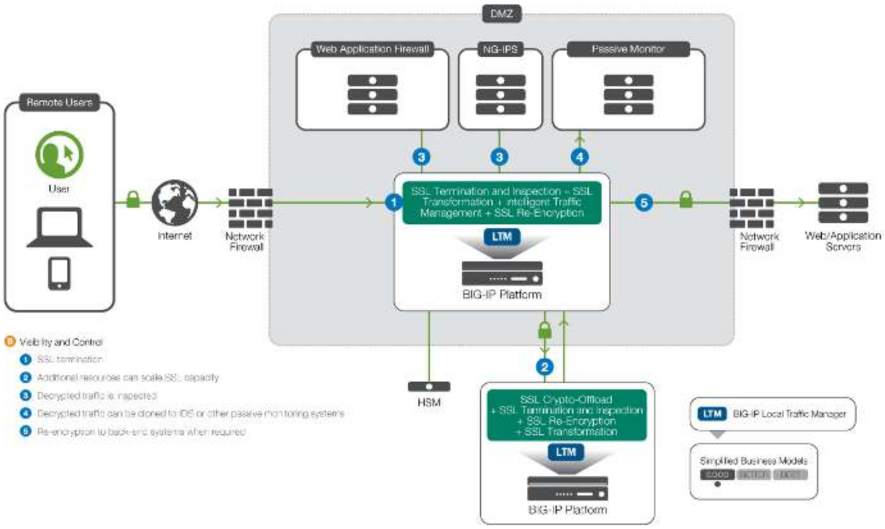

DMZ
Web Application Firewall
NG-IPS
Passive Monitor
Remote Users
User
Internet
Network Firewall
1
3
3
4
5
SSL Termination and Inspection + SSL Transformation + Intelligent Traffic Management + SSL Re-Encryption
LTM
BIG-IP Platform
Network Firewall
Web/Application Servers
2
HSM
SSL Crypto-Offload + SSL Termination and Inspection + SSL Re-Encryption + SSL Transformation
LTM
BIG-IP Platform
LTM BIG-IP Local Traffic Manager
Simplified Business Models
GOOD BETTER BEST
Visibility and Control
1 SSL termination
2 Additional resources can scale SSL capacity
3 Decrypted traffic is inspected
4 Decrypted traffic can be cloned to IDS or other passive monitoring systems
5 Re-encryption to back-end systems when required

Figure 6: Many different systems, including web analytics, benefit from SSL crypto offload.

To enable passive monitoring, a clone pool is configured on the ADC and a copy of the decrypted traffic is sent to the web analytics device.

Clone pools can also be used to direct a copy of decrypted ingress traffic to an IDS. The IDS can then spend its CPU matching signatures. If it ever falls behind, the normal flow of traffic is not impeded since this matching is out of band. For some organizations, this sort of best-effort, maximized-availability posture is sufficient.

Programmatic control

One of the benefits of the F5 SSL reference architecture is the level of programmability it offers. The granularity of attributes in the BIG-IP LTM SSL profiles and the depth of integration of the F5 iRules scripting language let administrators write powerful scripts to patch or enhance even complex environments.

When the Heartbleed vulnerability struck the SSL community, information security personnel were rushed to protect systems. For some, this meant scanning networks and preparing patches for hundreds or thousands of diverse virtual machines across multiple data centers and clouds. During those difficult initial days, administrators were aided by many hastily-crafted tools such open-source IDS signatures, Metasploit modules, and nmap plugins.

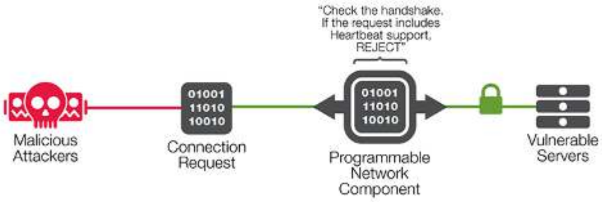


Figure 7: Programmatically defending against Heartbleed.

While the majority of F5 customers were protected from Heartbleed by F5's custom-built SSL stack, there were still corner cases where customers were load-balancing at layer 4 to vulnerable SSL servers. To assist these customers, within hours of the initial announcement, developers at F5 had provided two different iRules to mitigate Heartbleed—one for ingress traffic and the other for egress.

The SSL Renegotiation attack was also initially mitigated by an iRule, as was documented by Vincent Bernat in a terrific analysis on the difficulty of mitigating cryptographic attacks. The iRule dropped any connection that attempted more than five renegotiations within 60 seconds. Eventually this functionality migrated into the BIG-IP LTM SSL stack itself to provide protection for all users by default.

A new class of cryptographic attacks may be on the horizon. These "no-crypto, brute-force" attacks are similar to the SSL renegotiation attack but are even more pernicious. While they have not been seen in the wild yet, there are already iRules prepared to mitigate them.

Scalability and cryptographic offload

The cryptographic processors at the heart of many ADCs are finding their way out of dedicated appliances and onto the network itself. These new network-attached devices still offload cryptographic operations from a controlling device; they simply perform that function across the network.

Offloading in this fashion provides several benefits. It allows the architect to virtualize more of the infrastructure, including the device that was previously terminating the SSL, such as the ADC. Another benefit is manageability. Most organizations that use network-attached cryptographic devices select a single vendor, allowing them to easily train staff on that vendor's key management solution.

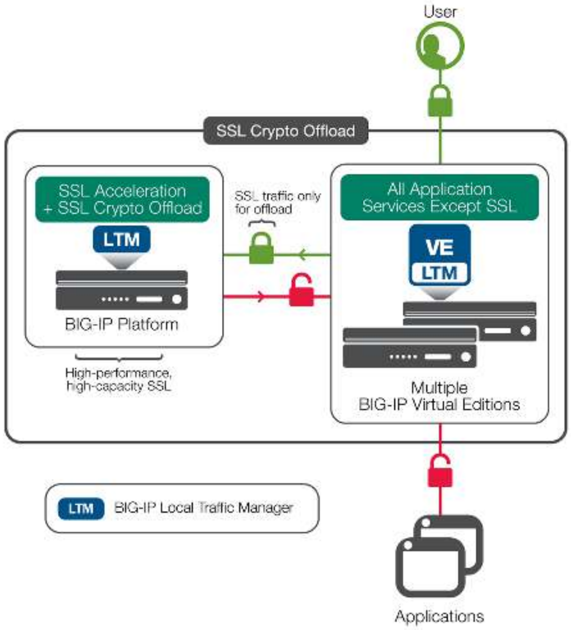


Figure 8: Concentrating SSL crypto to boost virtual editions.

A natural function of the ADC in this environment will be to assist in the scaling up of the overall cryptographic load, since cryptographic offload devices can be loaded into a pool addressed by the virtual ADC. As the need for more cryptographic computation grows, more devices can be simply added to the pool, thereby boosting the scalability of the solution while bounding the cryptographic operations in hardware.

Clearly, the communication channel between the requesting device and the offload device must itself be protected (usually via SSL), and most customers place it in a trusted part of the network as well.

Advanced Topics in Key Management

An idiom from the cryptographic community says, “Cryptography is easy; it is key management that is hard.” This gem is never truer than when applied to the world of public key cryptography, where keys must be trusted in hierarchies and are difficult to revoke and change.

OCSP stapling

In 2011, large parts of the government of the Netherlands ground to a halt when a self-taught teenage hacker hacked into the country’s primary certificate authority (CA), DigiNotar. The chaos that ensued was ultimately too much for DigiNotar and the company imploded, leaving the Dutch government holding the bag. Within months the teenage hacker struck again, this time at the world’s third largest CA, Comodo.

While the whole affair seems tragicomic in retrospect, a significant advancement resulted: the technique known as OCSP stapling. With OCSP stapling, if a public key system is suspected of being compromised, the responsible administrator will “revoke” any certificates associated with the key. These revocations are generally signed lists of revoked certificate serials numbers.

Client software, such as a browsers or email readers, are supposed to double-check these certificate revocation lists by querying an online certificate status protocol (OCSP) server when they establish an SSL connection to a server. In practice, this almost never happens for two reasons: OCSP servers are often provisioned as an afterthought and outages are common. Browser vendors find that when they disallow connections because the OCSP server is unavailable, the result is many “page not found” errors, which are detrimental to users. Even if the servers are available, the additional connection to the OCSP server may add latency significant enough to detract from the user experience.

The solution to all these problems is found in the OCSP stapling technique. An ADC can get its own status message from the OCSP server and then cache it for a period of time. When a client connects to the device, the device can “staple” the response into its own SSL connection with the client. This allows the client to receive and process the status message without having to incur the additional round-trip costs of a separate connection to the OCSP server itself. Problem solved.

OCSP Stapling isn’t without management overhead though. Ultimately it needs to be configured where the SSL is decrypted, and if that is at a central location, then the management surface is reduced to just that location.

Advanced key protection with hardware security modules

F5 has offered integration with hardware security modules (HSMs) since the year 2000. These modules were developed specifically for ultra-high security environments where keys must not be compromised. High performance of these cryptographic modules was usually not the point. The devices were also quite expensive, often costing 10x the price of the host computer. The modules worked by allowing the hosting system to generate a key within the cryptographic device and then asking for information to be encrypted or decrypted with it. But the key itself could never pass through to the host in an unencrypted form.

As business moved to the Internet, commercial demand for these HSM devices grew rapidly. They were initially deployed in web servers for financial and federal customers all across the world. When SSL decryption was absorbed as an ADC function, the HSM devices moved into the ADCs as well. This movement represented a significant fiscal savings as companies were able to buy fewer HSMs (since a proper ADC can manage thousands of servers).

Today, HSMs are becoming network-attached devices. This enables best-of-all worlds for the high-security environment, as security teams have a single place to manage their keys and organizations can rely and an even smaller number of HSM devices.

The hardware security modules moved from the server to the ADC. Now they are moving to the cloud as network-attached standalone devices.

Enterprise key and certificate management (EKCM and P12)

Many enterprise deployments are staying with a traditional “cryptographic offload at the ADC” strategy. These organizations are effectively centralizing their public-facing SSL keys and certificates at the ADC. Some may use HSM devices embedded in the ADCs.

Either way, security teams are continuously “tightening” their security policies. Policy changes in recent years have included a restriction against plain text private keys on the device, even for those times when a key is being imported into the embedded HSM itself.

This is where the transfer protocol PKCS12 can assist the administrator. PCK12 lets the administrator create a password-protected wrapper for the key. The encrypted key and its associated certificate are imported directly into the BIG-IP system.

The adoption of PKCS12, the integration with the network-attached HSM, and finally the programmability of the F5 TMOS platform via the F5 iControl API are the elements needed to allow true third-party integration to prosper.

Deployment Scenarios

Inbound

For many years, the solitary deployment scenario for SSL on an ADC was the inbound scenario. The ADC provided SSL decryption capabilities. Re-encryption from the ADC to the back-end servers became standard for financial organizations. These were the first SSL transformation services and examples of cipher agility.

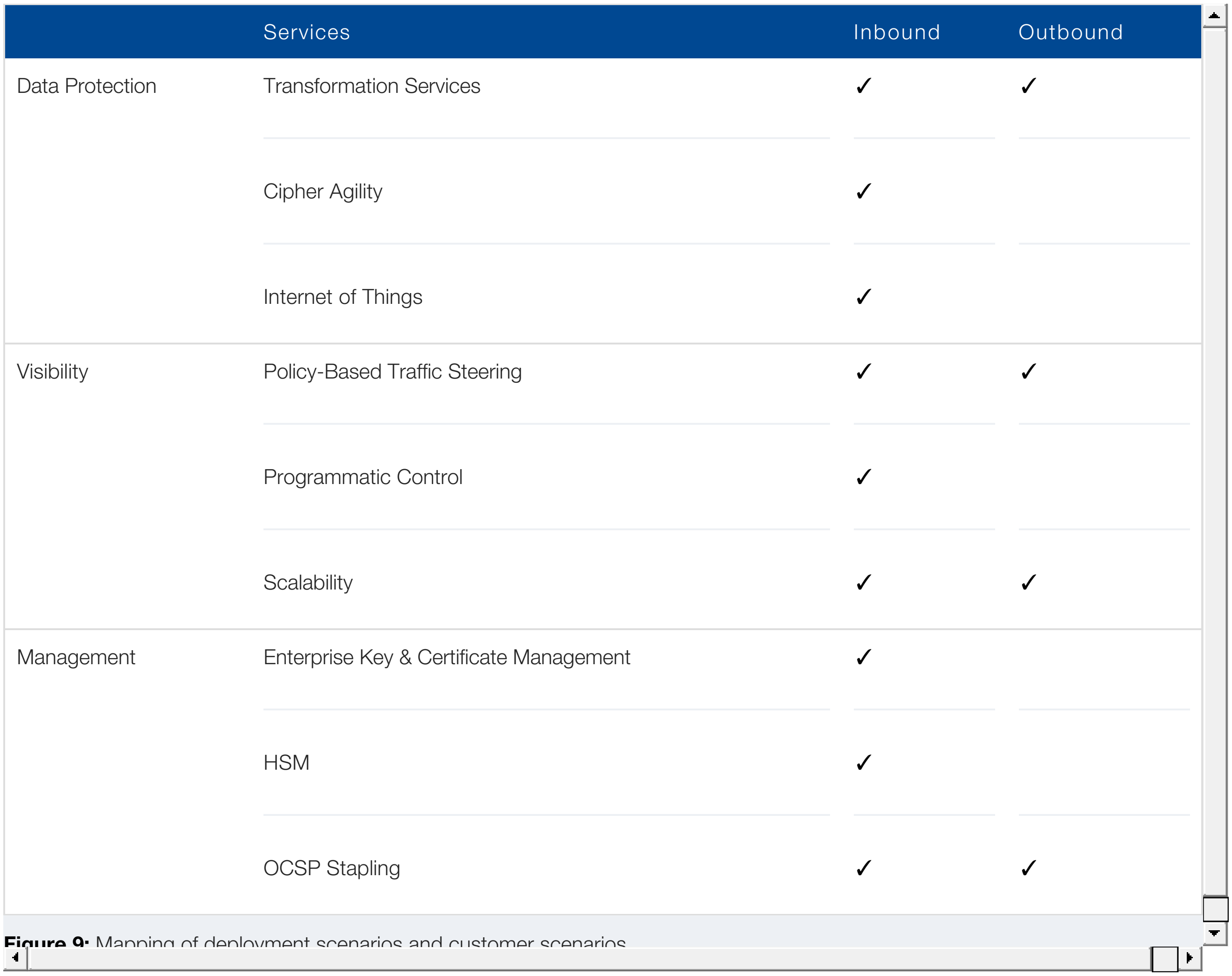
SSL protocol issues like Heartbleed and SSL renegotiation highlighted the need for programmatic control. Now the inbound scenario includes advanced SSL strategies such as OCSP stapling and PKCS12 key import.

Outbound

The outbound SSL deployment scenario for the ADC is a relatively new phenomena. This deployment scenario has been driven by enterprises with a need to monitor the activity or sanitize their outbound web traffic.

Typically SSL had been deployed by adjacent security devices, but like many security functions that sit adjacent to an ADC, its functionality was getting subsumed. The ADC began to function as both an inbound security and an outbound security gateway.

The regular deployment scenario for outbound SSL at the enterprise will include URL-filtering and SSL interception. These technologies, known together as Web Security, have matured with the Internet and are now being consolidated into security gateways like the ADC.



	Services	Inbound	Outbound
Data Protection	Transformation Services	✓	✓
	Cipher Agility	✓	
	Internet of Things	✓	
Visibility	Policy-Based Traffic Steering	✓	✓
	Programmatic Control	✓	
	Scalability	✓	✓
Management	Enterprise Key & Certificate Management	✓	
	HSM	✓	
	OCSP Stapling	✓	✓

Figure 9: Mapping of deployment scenarios and customer scenarios

Conclusion

The customer scenarios documented in this paper can be viewed as trends from the past into the future. For example, organizations are doing what they can to protect data in transit. This overall requirement of data protection is what drives the 20 percent growth in SSL usage every year. Going forward, organizations will be able to affect some efficiencies by using the transformational services (such as from SPDY to HTTP). Ultimately, the increasing requirement for data protection will mean that the SSL inbound deployment scenario will continue to grow in importance—but will also consume more computation resources.

Gains may be made when cipher agility can promote a computationally cheaper key establishment algorithm such as ECC. Customers may gain additional ground by leveraging efficient architecture for scenarios such as an SSL decryption offload for IDS and web analytics.

Hybrid architectures of embedded and network-attached HSM devices will gain ground, leading to more complex software architecture. Conversely, key management will get easier as cryptographic offload is consolidated to fewer and fewer points in the network.

Looking further into the future, the situation becomes more complex when the Internet of Things takes the number of Internet-attached devices to another order of magnitude. As organizations continue to use SSL as their primary communications protection, they may find an even greater need for innovative, efficient network security architecture.

[1] http://news.netcraft.com/archives/2014/01/03/january-2014-web-server-survey.html

[2] http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf

[3] http://www.businesswire.com/news/home/20131003005687/en/Internet-Poised-Change-IDC#.U-4pIPldUg8

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

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com