Realtime publishers

The Evolving Threat Landscape and New Best Practices for SSL

sponsored by

Dan Sullivan

Copyright Statement

Chapter 2: Deploying SSL in the Enterprise

Threats to enterprise information, applications, and systems stem from a wide variety of sources from disgruntled employees and unscrupulous competitors to profit-driven cybercriminals and state-sponsored attacks. To protect information systems, one should start with the needs of the business. What infrastructure components need protection? Changes in the way IT services are delivered are also changing the way we implement security controls. Cloud resources, in particular, require careful attention because their use is new and best practices are emerging.

In addition to thinking of security in terms of infrastructure, we must consider business drivers for security controls, such as maintaining compliance, customer trust, and system availability. All of these factors influence the need for broad use of SSL throughout the enterprise.

This chapter first examines the variety of infrastructure components that need SSL, then turns the focus to discuss the business drivers behind comprehensive SSL deployments in the enterprise.

Infrastructure in Need of SSL Protection

IT departments manage an array of infrastructure. There are many ways to categorize components based on their function, location, or business use. For the purposes of this chapter, it helps to categorize infrastructure components into three groups:

- Public servers
- Private internal assets
- Cloud resources

This categorization scheme is used because components within each group have similar SSL requirements and are subject to similar security controls.

Public Servers

Public servers are devices deployed on the Internet for sharing information and applications with customers, business partners, and others outside the corporate boundaries. As Figure 2.1 shows, public servers are accessible from any point on the Internet. This setup puts them in a vulnerable position.

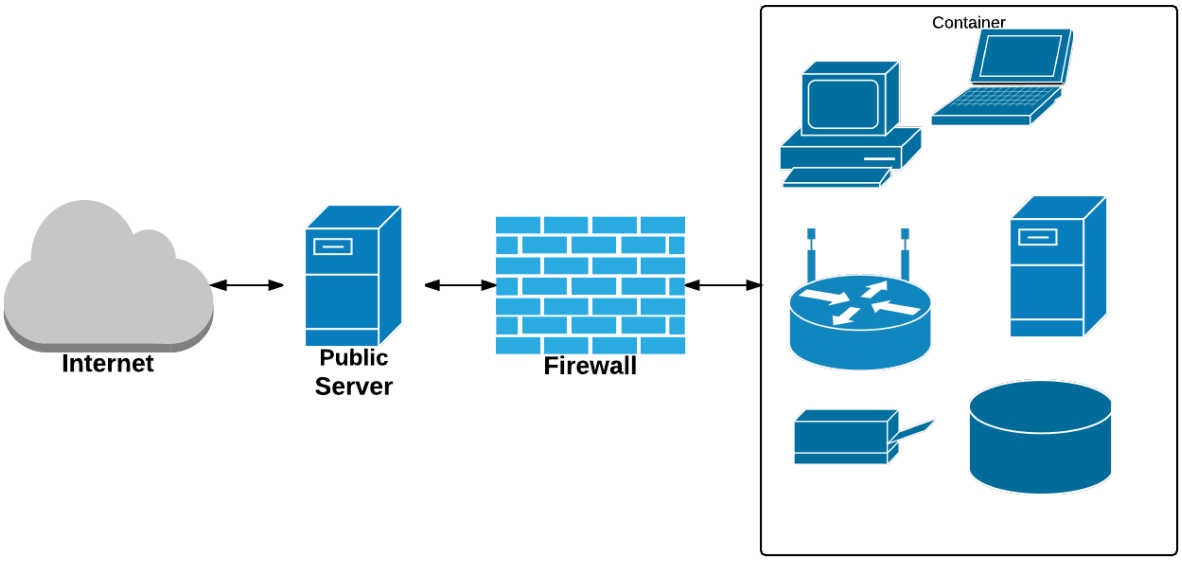

Figure 2.1: Public servers are not protected by network security controls such as firewalls and other traffic filtering and monitoring devices within the enterprise network.

Public servers are more exposed than other devices, making it important to implement as many security controls as possible. This implementation includes using SSL on all public servers.

SSL will enable client devices that connect to the server to verify the identity of the public server. This verification is particularly important for ensuring that customers and other users will trust the device is a legitimate business server and not an attacker's server that has been spoofed to appear like a legitimate server in your business.

Communications to and from public servers can be encrypted when SSL is available on those servers. This setup will further build confidence and trust that information shared with the public server will not be compromised or leaked during transmission.

Within the enterprise network, businesses often run a variety of other security systems including malware filters, vulnerability scanners, and security analytics applications. These all contribute to an increased level of security on the enterprise infrastructure. They are not sufficient to meet all needs, though. Especially when it comes to building trust with customers and users.

There may be little apparent evidence that a business routinely scans operating systems (OSs) and applications for vulnerabilities or follows a rigorous patching procedure to ensure software is up to data. It is apparent, however, when SSL is in use on servers. The value of SSL extends beyond just making it obvious to users that SSL is implemented on a server. SSL provides protections that should be deployed on all devices. The next section examines the use of SSL on assets within the enterprise network.

Private On-Premises Infrastructure

Enterprise information infrastructures include a variety of devices performing essential functions. Sometimes the functions are security oriented, such as firewalls, and sometimes they are application-specific functions, such as database servers. Some of the most common include:

- Firewalls
- Load balancers
- Mail servers
- Web servers
- Application servers
- Database servers

All of these benefit from the protections provided by SSL technologies.

Firewalls

Firewalls are used to separate logical sections of networks. For example, Figure 2.2 shows a commonly used configuration known as the demilitarized zone (DMZ) model.

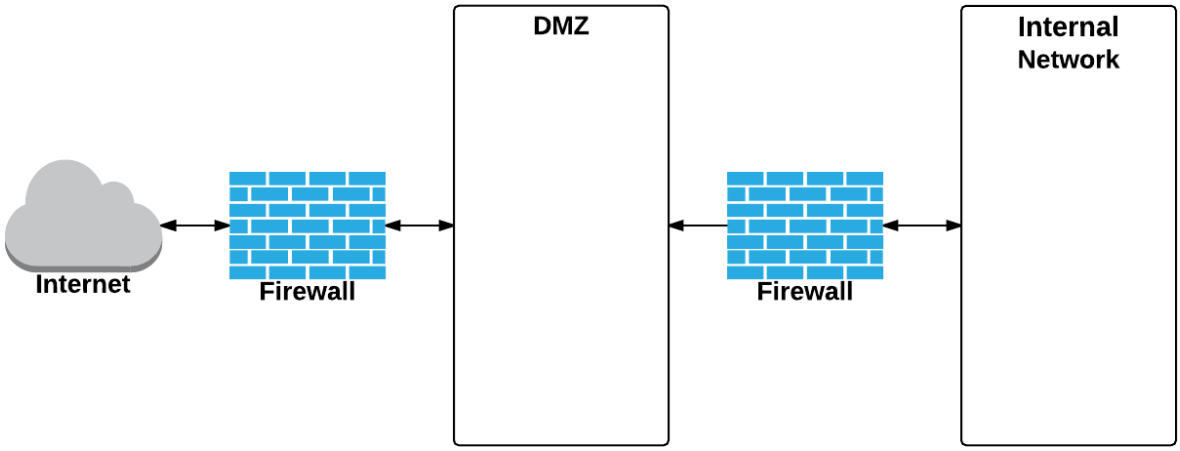

Figure 2.2: The DMZ model isolates sections of the network to limit access to infrastructure within each section.

A firewall can use SSL authentication to verify the identity of devices communicating with it. Similarly, client devices that need to validate the identity of the firewall can do so if the firewall device uses an SSL certificate. A systems administrator, for example, may want to verify the identity of the firewall before performing maintenance on the firewall or changing its configurations.

Firewalls may also be required to encrypt content it receives prior to sending it through to the next network segment. This type of functionality is enabled by using information contained within SSL certificates.

Load Balancers

Load balancers are important tools for helping to ensure scalability and reliability of business applications. A load balancer potentially receives traffic from many sources and distributes that traffic across multiple servers. Load balancers help to optimize server utilization by shifting traffic away from heavily load servers to those with lighter workloads.

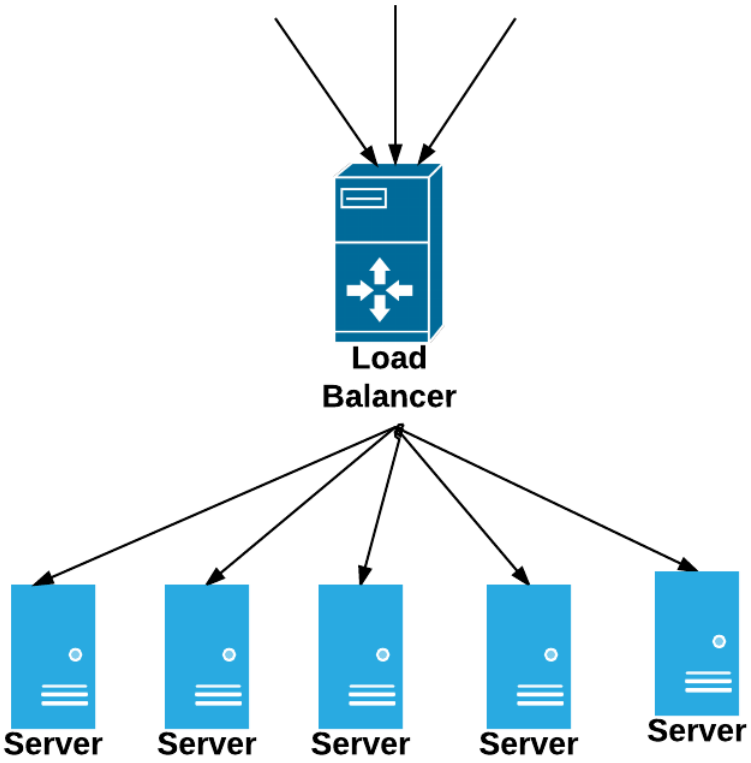

Figure 2.3: Load balancers distribute traffic and workloads across a cluster of servers.

Many applications receive and send sensitive data. In a load-balanced cluster, data may pass through the load balancer on its way to a server. Clearly, client devices sending sensitive data would expect to authenticate any device receiving protected data. By enabling SSL authentication, clients can verify the identity of the load balancer receiving protected data.

Mail Servers

Mail servers are essential for business communications. Email messages, documents, and calendar and appointment information are received, forwarded, stored, and managed on email servers. Large enterprises will often have multiple mail servers communicating with each other.

Email is fundamentally a distributed system. Messages originate at client devices, are sent to local mail servers, and from there, are sent to the destination email server and ultimately to the recipient's device. To ensure trust within the network of collaborating email servers, there must be an ability to authenticate servers. Human resources administrators need to trust that their email system will properly route sensitive messages to the actual recipient and will not be intercepted by a spoofed email server. SSL authentication enables this kind of verification and supports the trust users must have to employ email effectively and efficiently.

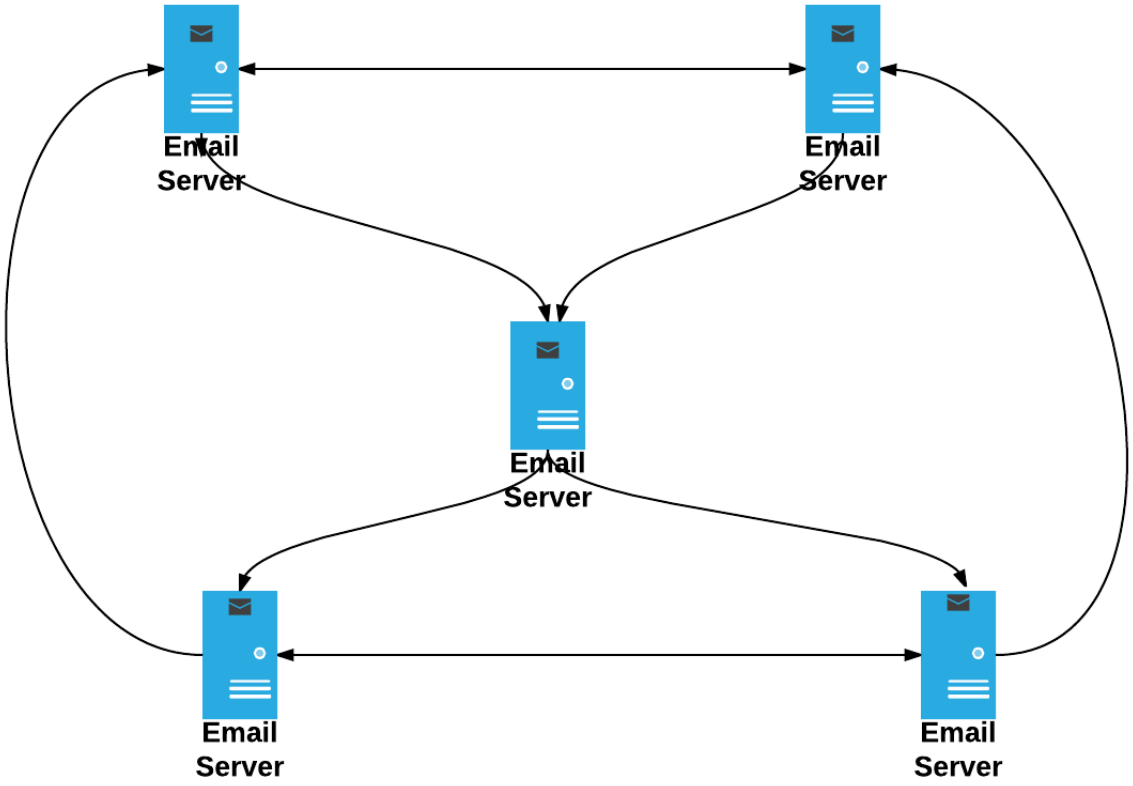

Figure 2.4: Email servers are part of a larger distributed system that requires trust between communicating components. SSL authentication is essential for establishing and maintaining that trust.

Email servers also use SSL certificates for encryption. In the post-Snowden era, there is a broad understanding of the value of encryption to protect private and sensitive information. Email users will increasingly expect that protection within systems they use. By deploying SSL-based encryption to all email servers, users will have the option for SSL-based privacy protections if they choose to use it.

Web Servers

Web servers are the backbone of the Web. They receive, process, and transmit HTTP and related protocols to provide much of the collaborative content and information available on the Internet. Web servers are as important to businesses as switchboards and phones have been in the past. Web servers host company Web sites and so much more; they have become an integral part of the software stack.

Many business applications today are built on a multi-tier model. Instead of having a single computer running all parts of an application, which is a common practice with older mainframe and minicomputer applications, applications are distributed over multiple types of servers. Web servers are often tasked with responsibility for the last layer of processing before sending content or other data to an end user. Web development frameworks streamline the process of integrating back-end application code, such as database queries, and front-end user interface code built using HTML, JavaScript, and other Web interface tools.

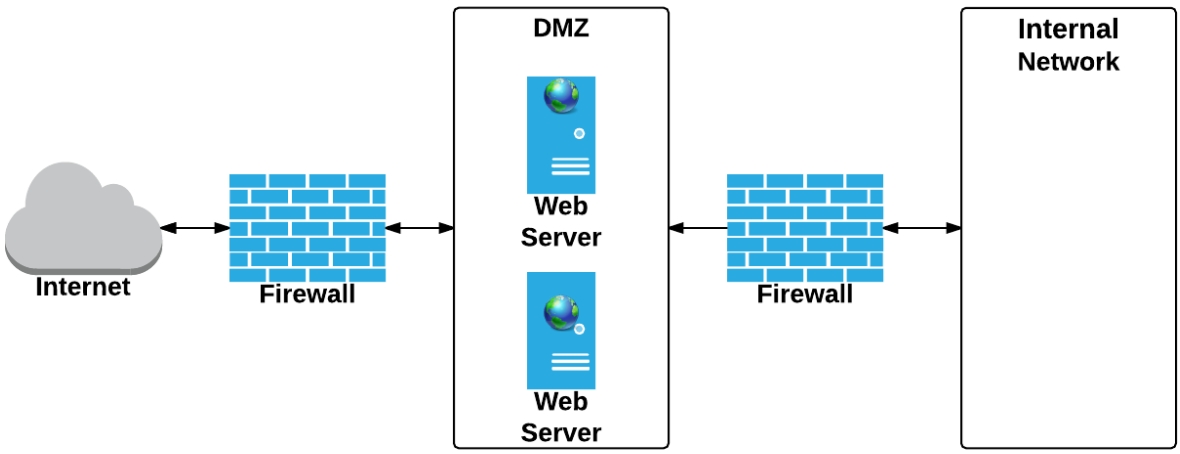

Figure 2.5: Web servers are typically the last layer of the application stack to generate output and the first to receive input.

Web servers are responsible for managing HTTP connections with client devices. SSL certificates on Web servers are used to verify the identity of a Web site. When a Webs site's SSL certificate lists a domain name other than that of the actual server, an error is generated, similar to the one that Figure 2.6 shows. SSL is a first line of defense for customers and other Web site users.

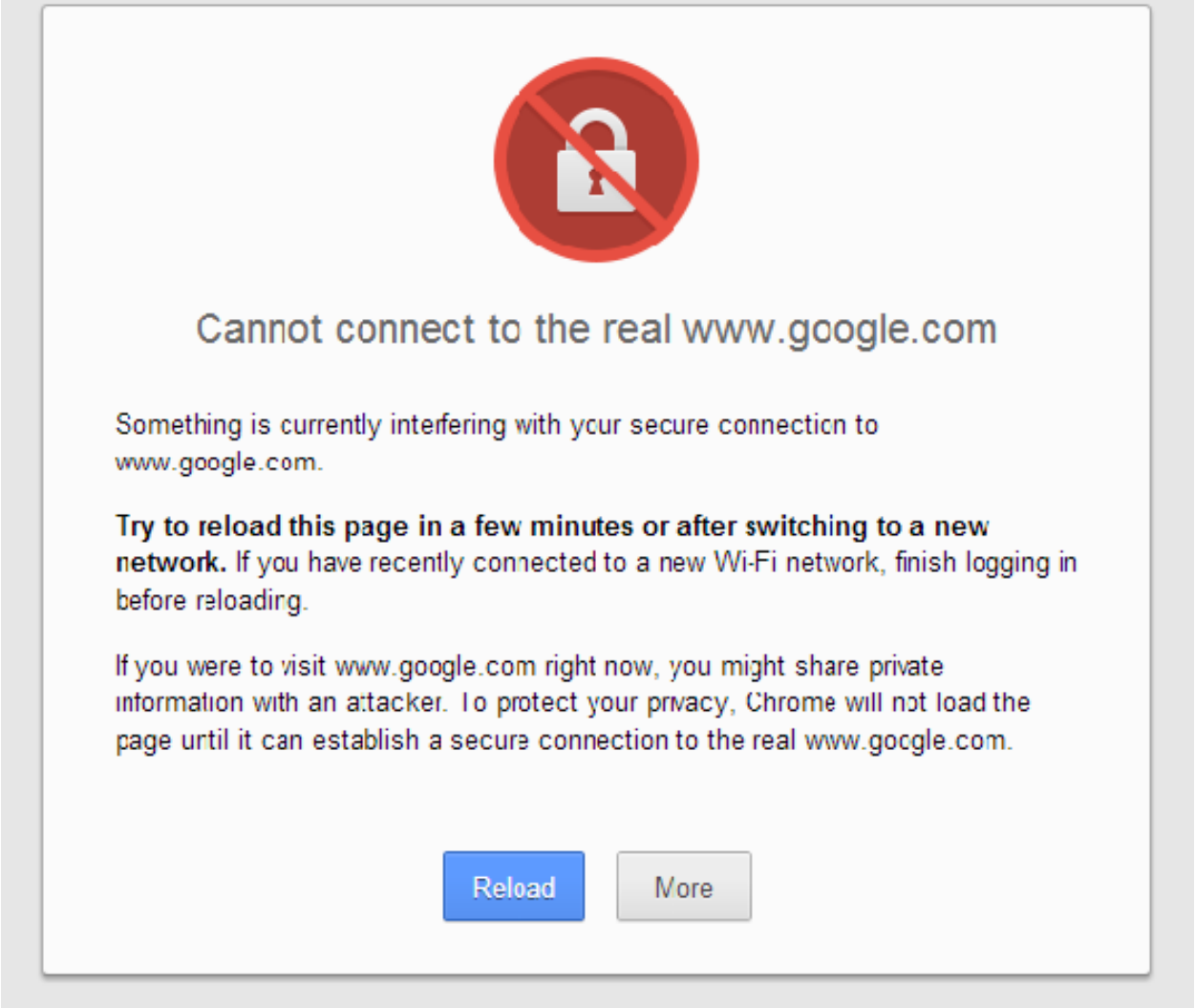

Figure 2.6: Error messages such as this indicate a problem verifying the identity of a Web server.

Application Servers

Another type of server that is integral to the modern software development is the application server. These servers implement much of the processing and business logic needed within an application. As Figure 2.7 shows, application servers are between Web servers and database servers, indicating the application servers communicate with each of the other types of servers.

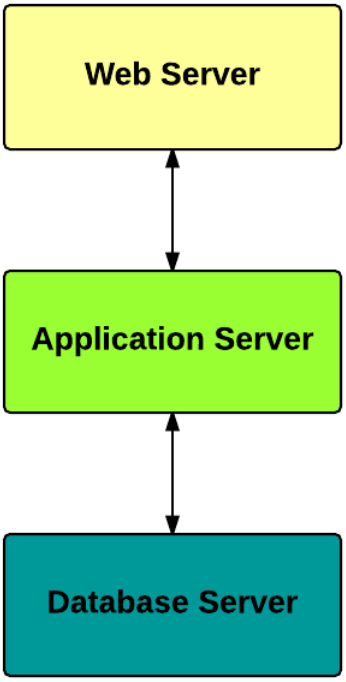

Figure 2.7: Application servers communicate with both database servers and Web servers.

As with email systems, described earlier, software designed using the multi-tier model depends on being able to coordinate communication between components. Application servers must be able to establish communication with Web servers that are sometimes in a network DMZ. As a DMZ segment allows for more access from the Internet than an internal network, servers in the DMZ may become targets for attack.

If attackers were able to compromise the security of a DMZ and re-route traffic from the legitimate Web server, they could install a spoofed server that appears to be the legitimate Web server. They would not, however, have a valid SSL certificate vouching for the identity of the server. For this reason, it is important to deploy SSL certificates to Web servers. For similar reasons, application servers should be protected with SSL authentication as well. Even when application servers are located in more hardened segments of the network, compromises can still occur. Multiple defensive measures are called for in this case.

In fact, a best practice in information security is known as defense in depth. This approach to security assumes some security controls will fail and other overlapping controls must be in place to protect information and system assets. SSL technologies are frequently used in defense-in-depth implementations because they support both authentication and encryption.

Encryption is an important element of defense in depth when working with distributed systems. By encrypting data in motion between application servers, Web servers, and other system components, the data is protected from compromise if other security controls fail. For example, an attacker might break into a network and install a packet sniffer, which collects network packets transmitted over the network. Any unencrypted data would be revealed to the attacker. Encrypted data, however, would appear to be a randomly generated stream of incomprehensible data. Of course, databases are used to store and manage data at rest and encryption is a vital element of defense in depth for databases as well.

Database Server

Database servers store increasingly large volumes of data. Multiple applications may use the same database server (see Figure 2.8). In this scenario, multiple application servers will need to authenticate the database server. Similarly, the database server will need to authenticate multiple application servers.

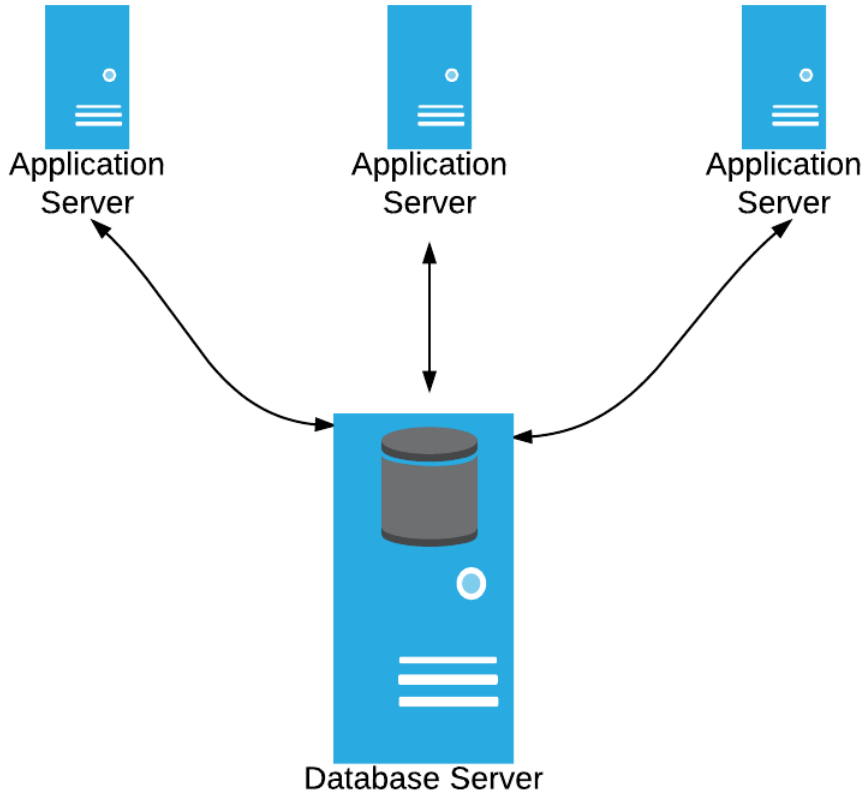

Figure 2.8: Once again distributed systems require SSL certificates to support authentication and encryption.

Encryption helps protect data from outside attackers as well as supports another security best practice: separation of duties. Database administrators have comparable abilities to control database software that OS administrators have with servers and desktops. By the nature of their responsibilities, they have to be able to perform any task on a database, such as allocating space for data, creating database data structures, and changing access controls. This set of abilities also allows them to view data, any data, on the database.

This situation is not a problem in many use cases. Database administrators help developers create data-driven applications and routinely see test data. In other cases, database administrators have other non-administrative roles, such as a software developer, in which case they need to work with data directly. There are also times that the data saved in a database is not sufficiently sensitive to warrant additional measures. However, there are cases where regulations or business policy require that only a limited number of people with actual business needs for sensitive data have access to it.

This situation creates a difficulty for database administrators. Policy dictates that they not have access to data on their database, but their role provides them with the ability to view all data on the database. One way to address this challenge is to encrypt the data in the database. Someone other than the database administrator should control encryption keys.

There is a broad array of system types in an enterprise information infrastructure, and they all benefit from the use of SSL for authentication and encryption. This reality stems from the fact that modern applications are often distributed and data is exchanged between multiple servers and across a variety of networks, including the Internet. SSL technologies solve two crucial problems: (1) the need to authenticate devices before sending them data or interacting with them in other ways, and (2) the need to encrypt data so that it cannot be viewed or captured during transmission. Databases have the additional need to encrypt data at rest.

Many organizations are choosing to deploy some of their applications in public clouds such as Amazon Web Services, Microsoft Azure, and Google Compute Engine. All of the issues described for on-premises systems apply to the cloud as well. There are, however, additional challenges that come with moving applications to the cloud.

Securing Cloud Resources with SSL

When assessing your security requirements with regards to cloud computing, it helps to distinguish three types of cloud services (see Figure 2.9):

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

Each of these share the basic feature of the cloud: the ability to acquire and use resources for only as long as they are needed and to scale up and down according to your workload requirements.

Infrastructure as a Service

IaaS cloud providers offer customers access to virtual or physical machines, storage of various types, and networking services. Servers are usually offered in a variety of sizes with a range of CPUs, memory, and I/O operations per second (IOPs). IaaS cloud providers offer a variety of storage types, including long-term object storage as well as storage attached to compute servers, which may be either disk or solid-state device storage.

Managing servers in an IaaS cloud is similar to managing them on-premises. Systems administrators are responsible for choosing OSs, installing packages and libraries, patching as needed, and other management tasks. The primary advantages of IaaS is that the cloud provider is managing the physical hardware, providing machine images, and maintaining all supporting systems, such as networking, cooling, and power.

Platform as a Service

PaaS providers extend the set of services offered to include software services for application developers. The services are typically targeted to application-layer functionality, such as messaging services for communicating between application subsystems, support for application deployment with configuration management tools, and identity management services for user authentication and authorization.

With PaaS providers, developers do not need to manage servers directly; the PaaS provider does that for them. The advantage of this model is that it allows developers the chance to focus more on application coding and less on systems administration.

Software as a Service

SaaS delivers complete application functionality to users. Some of the best-known SaaS providers are Salesforce.com, a customer relationship management service, and Workday, an enterprise resource planning and human resources management service. Unlike PaaS, which offers services targeted to application developers, SaaS providers deliver full application services for business end users.

SaaS services are appealing to many. There is no need to procure hardware, develop software, or hire technical support staff. All of that is the responsibility of the SaaS provider. At the same time, it leaves control of security measures in the hands of the SaaS provider. Customers could demand that all data transmitted to and from a SaaS service be encrypted, but customers do not typically dictate infrastructure security controls. Of the three types of public clouds, IaaS clouds require the most attention to security.

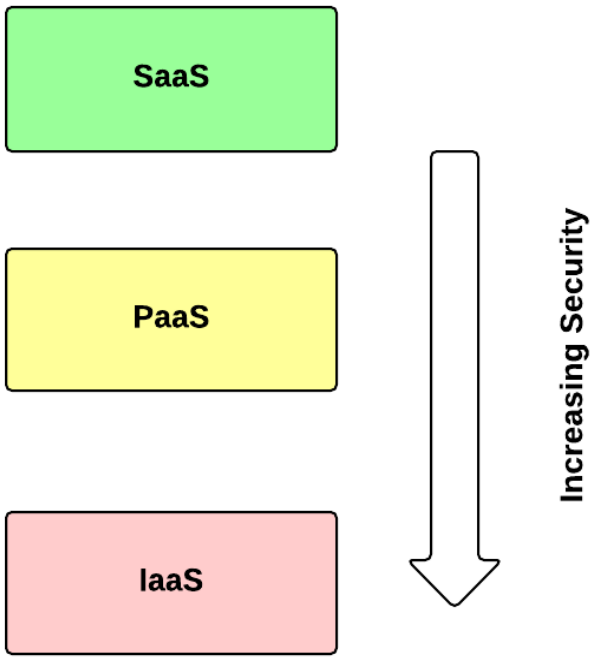

Figure 2.9: Different types of cloud services offer varying levels of management and different levels of control and responsibility for security.

Issues with IaaS Security

There are many issues that systems administrators and others have to address when using IaaS resources. Many are the same issues one would encounter in on-premises deployments. There are three, however, that are particular to using SSL to protect your cloud resources:

- Dynamic use of servers
- Challenges to managing SSL certificates
- Appropriate SSL type for cloud resources

One of the advantages of using cloud services is that you can add and remove servers as you need them. There is no long procurement delay; servers can be started in a matter of minutes. Although this functionality is helpful in terms of adjusting your resources to meet varying workloads, it does require additional planning when using SSL with each of these servers. If all of your servers will be using SSL (and they should be), you will probably want to use an SSL server that works with multiple servers. For customer-facing Web servers, consider using Extended Validation (EV) certificates.

Also, plan for certificate management in the cloud. Cloud providers have created tools, such as command-line utilities, for uploading and managing certificates. It is best to become familiar with these tools as you are planning your cloud deployment.

The technical aspects of your infrastructure shape how you use SSL certificates. You need to assess and deploy these certificates to a wide range of devices to enable comprehensive SSL protection. Technical issues are not the only concern, however. In fact, the most important drivers to using SSL technologies are based on business, not technical, needs.

SSL Deployment Driven by Business Requirements

It is easy to focus on the technical aspects of implementing SSL technologies, but organizations should always remember the reasons to implement such security controls ultimately rest on business requirements. Thee key business drivers to SSL adoption are to maintain:

- Compliance
- User trust
- System availability

These drivers have distinct characteristics but all are supported with the use of SSL technologies.

Compliance

Businesses have always been subject to regulation, but the rash of accounting improprieties in the early 2000s led to stricter reporting requirements, such as the Sarbanes-Oxley Act (SOX). Growing concerns about privacy protection have led to national governments around the globe legislating privacy and confidentiality regulations. Of course, governments are not the only institutions driving new regulations. Industry institutions and governing bodies are establishing regulations to protect their industries. The banking industry and Basel Accords are just one example. Individual businesses themselves establish their own policies and procedures to ensure business operations are executed appropriately.

Compliance issues are an ongoing operational concern, particularly in information technology areas, and especially in security. The specific security issues will vary by industry. For example, in the healthcare industry, there is significant effort to protect private health information.

Doctors, hospitals, insurance companies, and others have to follow directives that mitigate the risk of exposing patient information while facing significant changes in the way healthcare is delivered. In the United States, the recent adoption of federal legislation governing healthcare has enabled millions of individuals to acquire health insurance. Cost controls and efficiencies are essential to improving overall care while limiting the cost to consumers and providers. Healthcare, like any industry, can benefit from innovation, but new products and services must comply with existing regulations.

Innovation is driven by a wide range of factors:

- Legislation
- Changing demographics
- New knowledge
- Evolving market conditions
- Shifting consumer preferences

To realize the benefits of innovative ideas without running afoul of regulations, it is important for regulated industries to build from a strong foundation of compliant information systems. SSL technologies are integral to establishing that foundation.

In spite of varying industry specifics, regulations regarding privacy and data integrity often require that companies:

- Protect data at rest
- Protect data in motion
- Demonstrate compliance

To protect data at rest, encrypt sensitive data in databases, file systems, and other applications. As noted earlier, if a database is compromised and records are stolen, they will be of no use to anyone without the encryption key.

Data in motion should be protected by encryption as well. Many applications are designed to encrypt sensitive information, such as credit card data, but allow other data to transmit in clear-text form. A better practice is to encrypt all data in motion. Small bits of information collected from multiple sources might give a determined, persistent attacker the pieces needed to draw conclusions about business process, operations, or controls that could help further other efforts to breach your systems.

When deploying SSL, keep in mind that you want to be able to demonstrate compliance. This ability will include showing that all relevant servers, applications, and data are protected; SSL certificates are kept up to date; and appropriate encryption algorithms and key sizes are in use.

Maintaining User Trust

Maintaining user and customer trust is difficult when the news has all too frequent stories of major banks or large, international conglomerates losing the data of millions of customers. It is not difficult to imagine a customer wondering why she should trust her data to a midsized company or even an established enterprise when some of the largest businesses in the world have been breached. There is no simple way to address these realistic concerns; however, whatever the solution may be, it will entail multiple types of security measures.

One of these measures should include the comprehensive use of SSL: encrypt all data in motion, even between internal systems. Sensitive information should be encrypted at rest. There may be times when this is not practical. For example, a legacy system may not support encrypted data, and the data used by that system might not contain private or confidential information.

Another important step to establishing user trust is to demonstrate your security measures. For example, EV certificates display a green bar in browsers when rendering content from an EV-enabled site.

Maintaining Data Availability

SSL technologies also play a pivotal role in protecting IT infrastructure. SSL protocols can authenticate servers to other devices. Applications running on one server, for example, may authenticate a database server prior to uploading any data. Doing so can help mitigate the risk of inadvertently transmitting sensitive data to the wrong device.

A best practice to protecting systems and data is to require encryption of all data transmissions even within an internal corporate network. It does not take much searching to find news stories of businesses with sophisticated IT systems that have been breached and data stolen. No matter how confident we may be in our existing security measures, we should work with the assumption that some of them will fail. Rather than think "My data is safe because it is behind a firewall" it is better to reason "My data is safer if it is behind a firewall and encrypted in motion and while at rest."

Summary

More business applications are using distributed architectures to deliver new services, take advantage of existing applications, and control costs. The benefits of distributed systems also come with risks. Data is spread across multiple devices and databases. Even with sound network and server security practices, breaches can occur. SSL technologies deployed throughout the IT infrastructure can help meet business objectives while protecting the confidentiality, integrity, and availability of your systems and data.