Examining SSL-encrypted Communications

Sourcefire SSL Appliance
Technology Brief

Executive Summary

SSL traffic (encrypted traffic) in the enterprise is growing rapidly due to the enterprise-wide usage of applications, such as SharePoint, Exchange, WebEx, Salesforce.com and Google Apps. Additionally, most e-mail applications, such as Gmail, Yahoo and Zimbra, all use SSL to encrypt communications.

Although this encrypted traffic protects end user data, it also creates security "blind spots." The security infrastructure put in place to protect your enterprise is blind to SSL traffic, thus causing risks for traffic destined to the enterprise. The same SSL encryption methods used to protect your data provide an easy vehicle for criminals to hide their cyber attack activities, as in the case of several recent well-publicized attacks.

In addition to the risks of incoming threats hiding over SSL channels bypassing security architectures, outbound enterprise traffic is now a growing problem. This is becoming quite a "hot button" for security applications that tackle data loss prevention (DLP), compliance reporting and lawful intercept — solutions that could, at one time, see what was outgoing, but are suddenly "in the dark" to SSL traffic.

This paper explores the drivers behind the increase in SSL usage and the methods used by enterprises to confront the security challenges that SSL creates. The Sourcefire SSL Appliance offers enterprise security appliances or applications unparalleled access to the unencrypted plaintext of SSL flows for these applications to be successful.

SSL Growth

SSL has become the ubiquitous choice to secure web-based transactions. That fact, coupled with the flexibility that SSL provides, has made it the obvious choice for securing a host of additional applications and to enable new services where SSL is used as a secure tunneling mechanism.

Specifically, for end users, SSL has long been used to secure web-based transactions to enable e-commerce and online banking. Over time, the simplicity that SSL provides has made it the perfect vehicle to migrate many applications to a web-based model for new online services like viewing medical records, ordering prescriptions, filing federal, state, and local tax returns and other government uses. New cloud-based and enterprise applications, such as Salesforce.com, Exchange, Sharepoint and most of the web-based email applications on the market, such as Gmail, Yahoo, Zimbra etc., have also adopted SSL encryption.

In the enterprise, SSL is most often used to encrypt traffic leaving the enterprise to provide data security between remote locations across a public network. SSL is also used inside the enterprise to secure sensitive transmissions, such as human resource data, between departments or groups, and to ensure privacy for corporate activities, such as business development, mergers and acquisitions. Enterprises also require encrypted communications to individual mobile users who need remote access, illustrating how SSL-based VPNs are a fast-growing technology for remote-access VPNs.

53% of enterprises have SSL applications today
35% say that SSL makes up more than 25% of traffic
52% CAGR for SSL-based WAN traffic
74% CAGR for SSL VPNs

Table 1. SSL Deployment and Use

While SSL solves many security problems, encrypting sensitive transactions can enable them to pass through security measures unchecked. This fact is exacerbated considering that SSL-encrypted communications constitute a significant and growing percentage of the traffic in enterprise LAN and WAN. Surveys have shown that between 25-35% of enterprise traffic is SSL-encrypted, and can be as high as 70% in select verticals.

Problem Posed By SSL

It is clear that there are legitimate needs for encrypted data within, to and from the enterprise. But this encrypted traffic poses a security risk as SSL also provides a mechanism for more nefarious applications. As many IT managers are aware, the privacy benefits provided by SSL encryption can be overshadowed by the risks SSL brings to the enterprise network. While SSL encryption provides privacy and can protect both corporate and individual user information by ensuring that data is useless to potential interceptors, it can also make it difficult or impossible for network

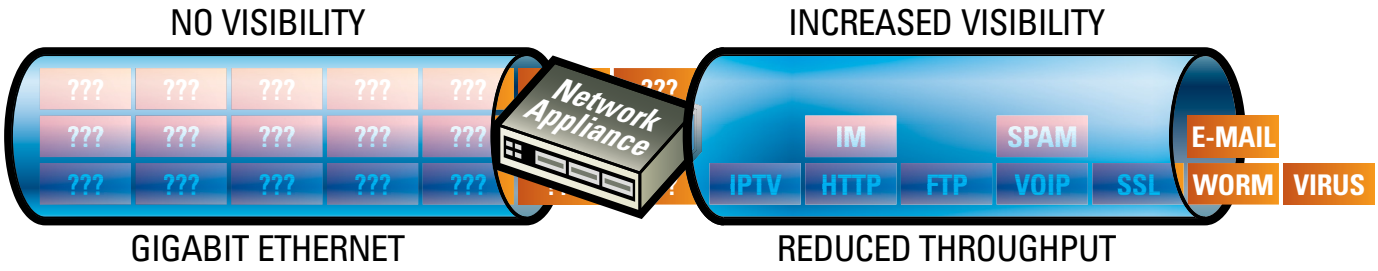

Figure 1. Network appliances have failed to keep pace with improvements in network performance.

administrators to enforce corporate acceptable-use policies. SSL also makes it difficult for IT organizations to ensure that threats, like viruses, spam and malware, are stopped before they reach individual users. Without the ability to examine the contents of SSL communications, network operators leave open the possibility for information to be accidentally leaked out of the enterprise or worse, stolen. Regulatory compliance requirements, including identifying accidental or intentional leakage of confidential information, are also virtually impossible to meet because of SSL encryption.

In many instances, there are conflicting requirements to both encrypt and examine data within the enterprise. In typical installations, these seemingly incompatible requirements cannot both be met with acceptable performance. This SSL conundrum has wreaked havoc for organizations subjected to industry and government compliance mandates, such as Health Insurance Portability and Accounting Act (HIPAA) and Sarbanes-Oxley (SOX), which require intrusion protection and detection to ensure that only authorized individuals have access to hardware and software resources within the network infrastructure. Other compliance mandates require all organizations with publicly accessible networks to be able to provide law enforcement agencies with documentation of network activity, thus requiring that all traffic be unencrypted.

SSL Control Approaches

Network operators already deploy an array of network and security appliances to protect their enterprises, enforce internal corporate acceptable-use policies and satisfy external government regulation. These devices provide solutions for detecting rogue applications, controlling unrestricted web surfing, firewalling traffic, VPNs, network access control (NAC), intrusion detection (IDS), intrusion prevention (IPS), unified threat management (UTM), regulatory compliance, virus protection and spam control, amongst others. These appliances work almost entirely by providing deep packet inspection and flow analysis, looking for known patterns of mischievous activity and blocking or recording it. Unfortunately, these network and security appliances, in many instances, can only inspect plaintext traffic and are unable to inspect SSL-encrypted communications for attack rules. These solutions are thus becoming less and less effective, as the amount of encrypted SSL communications and traffic continues to grow.

Network operators previously faced two extremes in confronting the issues associated with SSL communications. They could take a draconian approach by blocking SSL communications entirely or, alternatively, enabling SSL communications transparently without inspection (by leaving port 443 open on their security infrastructure), thereby greatly reducing the effectiveness of their network and security appliances that are unable to examine the encrypted flows. Neither of these alternatives is a viable option for enterprise networks.

Besides simply passing all SSL-encrypted payloads or blocking encrypted traffic entirely, several other approaches have been used. These methods share a common goal of providing plaintext inspection of SSL-encrypted flows, enabling the content of encrypted traffic that does not meet corporate acceptable-use policies to be dropped or the logging of suspected attacks to a management station. Just as importantly, these methods also need to identify and permit SSL in legitimate use cases. In many instances, these methods are successful at examining encrypted SSL, but they typically suffer other major problems that limit their effectiveness.

SSL Proxies

Today, in most cases, network operators permit encrypted communications, but only through SSL proxies that enable the IT organization to examine and inspect SSL-encrypted content before entering or exiting the enterprise. These proxies provide the opportunity to examine the contents of network traffic, yet still offer encryption prior to leaving the enterprise.

Unfortunately, traditional SSL proxies create additional problems that become trade-offs to the security benefits that they offer. They are inserted in the network path and create congestion as the performance of the network appliance fails to keep pace with the rate of expansion of network capacity and bandwidth at Gigabits/second and beyond. The network I/O, memory and CPU utilization of these systems all strain at these new performance levels. As a result, these network appliances are rated for use by some amount of aggregate bandwidth or a number of users, sessions and/or flows. When any of these metrics are exceeded, the appliance becomes a bottleneck that can only be relieved by adding capacity with yet more network appliances.

SSL proxies also require network IP address configuration and likely need network topology changes to engineer the appliance into the network as an active network element. As an active network element with IP addresses on the inline interfaces, these SSL proxies are now vulnerable to all attacks just as any other host, server, switch or router would be. Careful consideration needs to be given to the security of the SSL proxy configuration itself in both the data plane and management plane.

Another issue with network designs based on SSL proxies is that these assume that all SSL traffic is blocked except that which goes through the proxy. Network devices redirect traffic on port 443 to the proxy. SSL proxies are incapable of detecting hidden SSL flows on different (non-443) port numbers because such traffic is not directed to the proxy.

Traditional SSL proxies also force costly changes to network topology, firewall and policy configuration, as well as modification of client/server stations and their SSL-capable applications in the enterprise. Applications using SSL require the proxy server's information, such as IP address, port number and, potentially, other security settings.

Transparent SSL Proxies

As network bandwidths expand and the complexity of applications and attacks increases, more networks are employing a multitude of network and security appliances and IP-based applications and services. Accordingly, interest in the use of SSL proxies has surged once again. Despite this and the existence of many SSL products in the market, few solutions exist that can provide a high level of security with little or no effect upon management and performance.

The ultimate solution in ensuring the confidentiality and protection of SSL traffic balances performance, control

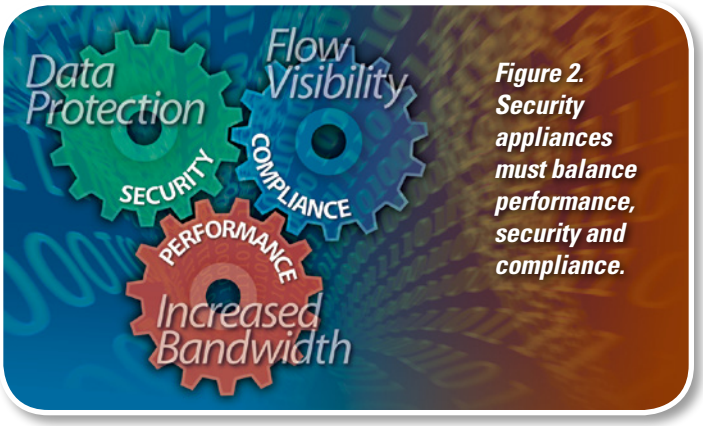

Figure 2. Security appliances must balance performance, security and compliance.

and security. While solutions exist to meet each objective independently, it is difficult to satisfy them simultaneously, resulting in one or more of these critical areas failing to meet expectations. Increasing security at the expense of network performance or compliance is no more acceptable than meeting application bandwidth and compliance requirements while ignoring security. To date, it has been difficult, if not impossible, to satisfy all three of these objectives.

A new class of SSL proxy is entering the market that provides many of the benefits of existing SSL proxies, yet also removes or mitigates the negative impacts that are currently associated with them. These devices, known as transparent SSL proxies, are deployed in the IP network where encrypted SSL traffic can be inspected as plaintext before it enters or exits the LAN, WAN or data center. Their transparency is defined by the fact that they are deployed as a "bump-in-the-wire," meaning they are not active endpoints in the network. As a result, they do not require any IP address assignment or configuration, removing any complicated configuration requirements or IP network topology changes. They can easily be added or removed from the network by simply connecting or disconnecting their input and output network connections. The transparency also means that the SSL proxy function is hidden from the end user, removing the need for time-consuming and costly client device and application configuration.

Transparent SSL proxies see all network traffic, not just SSL, and, thereby, require line-rate network performance and the ability to cut-through non-SSL flows. An effective transparent SSL proxy solution provides great performance at both the network and application levels, as well as multiple-interface support for applications to tap into SSL streams. By providing applications with access to the plaintext in SSL streams, the transparent proxy enables IT managers to implement policy control and regulate network users—often necessary for compliance.

Sourcefire SSL Appliance
Transparent SSL Proxy

The Sourcefire SSL Appliance is the industry's highest-performance transparent proxy for SSL network communications, providing applications with access to the plaintext in SSL-encrypted connections. Beyond industry-defining performance, the SSL Appliance is the first transparent SSL proxy that both increases network security and significantly minimizes deployment and operational costs by removing costly user and network configuration. The SSL Appliance was designed for security and network appliance manufacturers, enterprise IT organizations and system integrators to provide industry-leading performance at a fraction of the cost of other solutions. Without compromising any aspect of enterprise or government-regulated compliance, the SSL Appliance enables network appliances to be deployed with the highest levels of flow analysis while still maintaining multi-gigabit, line-rate network performance.

The Sourcefire SSL Appliance enables existing security and network applications to obtain access to the plaintext within SSL-secured flows, thereby extending the benefits of their applications to SSL-encrypted traffic. Unmodified applications running on the same platform as the SSL Appliance, or on adjacent appliances, can gain visibility into the content of SSL traffic. Sourcefire's network processing and cryptography acceleration hardware are leveraged to forward non-SSL traffic at multi-Gbit/s rates.

The SSL Appliance can be deployed as a "bump-in-the-wire" fully transparent proxy, eliminating the need for costly reconfiguration of network elements. This transparency removes any needed configuration of clients and servers to make them direct SSL traffic towards the proxy. The SSL Appliance just needs to be located inline so that all network flows (including SSL flows) pass through it.

The SSL Appliance can also be deployed in a passive mode of operation with the appliance connected to a span port, tap or mirrored interface where the SSL Appliance is receiving a copy of all network traffic for classification, flow identification and decryption. This mode permits SSL inspection without the need to place an appliance inline.

The Sourcefire solution enables the identification and elimination of risks, such as regulatory compliance violations, viruses/malware and intrusion attempts normally hidden within SSL. The privacy and integrity of SSL-encrypted communications are maintained by making the plaintext available only within a controlled environment while also exempting certain traffic from inspection based on user preference.

Deployment

The SSL Appliance is deployed adjacent to existing security and networking appliances to provide these devices with visibility into SSL flows. The plaintext of SSL flows can be fed to existing applications via a dedicated gigabit Ethernet link while non-SSL flows are mirrored to the security appliance, firewalled or cut-through, bypassing the security appliance altogether. This enables SSL visibility to be added to existing network security infrastructure with no integration effort. The system is configured and managed via a web-based graphical user interface.

Operating Modes

In the network security appliance space, due to its nascent nature, the market segmentation is somewhat malleable as the market is still developing. New threats emerge, security and compliance requirements evolve and enabling technologies adapt. This is visible today, considering the numerous categories of network and content security appliances available on the market. Some of the more common products (and product categories) include firewalls, intrusion detection

Figure 3.
Sourcefire SSL Appliance

systems, intrusion prevention systems, anti-virus scanners, unified threat management systems, network capture, network monitoring, network forensics, network analysis, network access control, spam/spyware and web filters. There are also as many analysis techniques employed as there are product categories in the content and security appliance space. These systems use methods like packet filters, rule detection, traffic/packet anomaly detection, protocol monitoring and packet capture to alleviate security threats.

Even though the network security appliance market is complex and constantly changing, these devices share several common deployment modes. They are either installed inline with respect to traffic flow, and actively filter traffic to block attacks, or they are deployed on a mirrored interface, span port or tap port and only monitor network traffic as it passes through the network to identify attacks or record traffic. These device configurations are referred to in the SSL Appliance as filtering and sniffing configurations, respectively.

The SSL Appliance is either deployed inline to offer the plaintext of SSL-encrypted communications to sniffing or filtering applications for analysis, or it can be installed in a passive or "offline" mode for packet capture applications. The choice between modes is a global system setting configured by the network administrator.

Sniffing/IDS Inline Mode

In sniffing inline mode, also known as IDS inline, the Sourcefire SSL Appliance sits as a "bump-in-the-wire" and will receive all inbound and outbound traffic to/from the computing resources behind it. The SSL Appliance forwards all traffic to the egress network port while simultaneously copying both non-SSL flows and decrypted plaintext to an attached sniffing application for examination/logging.

SSL plaintext flows may be marked by the SSL Appliance with either a configurable source MAC, VLAN ID or DSCP to identify plaintext decrypted flows from non-SSL flows sent to the attached security appliance. It is assumed that the sniffing device is monitoring only and, therefore, no data will be transferred from the IDS or sniffing application back to the SSL Appliance.

Sniffing/IDS Passive Mode

In passive mode, the SSL Appliance is deployed off a span port, tap or mirrored interface where the appliance is receiving a copy of all network traffic for classification, flow identification and decryption. Packets are classified and, based on policy, are forwarded to an adjacent packet capture security appliance, such as an IDS or network forensics appliance. In passive configuration, no data is ever forwarded back toward the network; the SSL Appliance and adjacent security appliance are capturing traffic for analysis.

Filtering/IPS Inline Mode

In filtering mode, both the SSL Appliance and filtering appliance are inline and all network traffic may traverse both devices. Similar to IDS inline mode, the SSL Appliance will receive inbound traffic and can pass both non-SSL flows and unencrypted plaintext to the host application or adjacent filtering device. SSL plaintext flows will be marked by the SSL Appliance with either source MAC, DSCP or VLAN ID to distinguish decrypted plaintext flows from non-SSL flows sent to the IPS. The filtering application/appliance will parse the plaintext and non-SSL flows against its rule database to identify and counteract threats and/or data leakage.

Unlike sniffing mode, in a filtering configuration, there is an active communications path back from the security appliance. For each SSL packet, a plaintext packet will be generated and sent to the filtering appliance where it will be bridged and sent back. The original encrypted SSL data packets of inspected flows will be held back in a queue in the SSL Appliance. If the flow is validated by the security appliance and packets are received back by the SSL Appliance, the returned plaintext packet will trigger the release of the original SSL data packet, which has been re-encrypted, to the egress network interface. Any non-SSL traffic received back from the security appliance is cut-through to the egress port of the SSL Appliance.

If the attached IPS device decides to drop the flow, it will send a TCP RST and/or silently drop all packets of the flow. The Sourcefire SSL Appliance assumes that all buffered flows are invalid until their packet headers are returned from the IPS. After a timeout period, the buffered flows are discarded under the assumption that the security application has blocked them.

SSL Policies

The main function of the SSL Appliance is to expose the plaintext of encrypted flows to third-party security appliances or applications. In addition to processing SSL traffic, the SSL Appliance can act as an intelligent and programmable traffic-capturing and mirroring device, optionally reducing load on the attached security appliance and/or replacing costly network switch span ports. There are several policy and filtering stages that control access to overall SSL inspection.

Traffic Diversion Policy

The Traffic Diversion Policy (TDP) is a list of global rules in the form of 7-tuple IP filters and associated actions. The goal of the TCAM-based rules table is to reduce the processing requirements on the SSL Appliance system and the associated security appliance or application by providing a classification, filtering and forwarding mechanism for flows to be steered to the IPS/IDS, cut-through to the egress interface or other actions to be performed (such as drop). These rules are applied to all incoming flows (SSL and non-SSL) via basic 7-tuple classification rules that enable the IT administrator to invoke policies, such as "never decrypt traffic from host w.x.y.z, or network w.x.0.0." The SSL Appliance system defaults to a single TDP wildcard rule that indicates that all packets should be cut-through and not mirrored at system startup.

SSL Inspection Policy

An integral part of the SSL Appliance is identifying SSL traffic in order to separate it from non-SSL traffic. SSL traffic is identified based on content (pre-SSL, SSL Handshake and SSL Data) and does not rely on it being on port 443. Based on the SSL Inspection Policy, traffic is optionally decrypted and forwarded as plaintext to an external IPS/IDS network appliance. The SSL Inspection Policy provides the network operator with a quick and easy way to alert the SSL Appliance to valid or acceptable uses of SSL encryption that should not be decrypted further, such as personal banking or other online transactions. Once identified, these flows are immediately cut through to the egress network interface without further inspection. Individual SSL site URLs can be specified as exempt and set to be cut through or marked for inspection. The SSL Inspection Policy contains a default entry for all flows. The default SSL Inspection Policy is that all flows are exempt from further SSL processing/decryption and should be cut-through at system startup. Administrators must specifically enable SSL inspection.

SSL Session Log

The SSL Appliance Session Log provides a mechanism for logging all SSL communications through the system. It contains the learned information that was passively gathered from the flows through the system. This database is for the network administrator to view details of SSL flows so that certain trends or patterns can be identified as data traverses the system. The SSL Appliance Session Log is a repository where data detailing the SSL flows through the system is maintained and can be accessed by the network administrator.

SSL Session Log Classification Fields

The SSL Session Log contains data from flows that are being actively inspected, as well as those that are not. These flows are uniquely identified so that the network administrator can identify activity that needs to be inspected. The flow identification is based on classification of the certificate fingerprint. From the fingerprint, fields of interest are:

- Certificate Subject
- 5-tuple
- Date
- Flow Start Time
- SSL_Inspect_On/Off (status)
- Certificate Issuer
- Fingerprint Hex
- Time
- Flow End Time

Traffic Mirroring

In sniffing mode, inbound traffic has the option of being mirrored to the connected security appliance or application. Traffic Mirroring is necessary to configure the profile of non-SSL traffic to be forwarded to the security appliance and other traffic that should be cut-through without further examination.

Traffic Bypass

In filtering mode, inbound traffic can be classified and passed directly from the ingress to egress network-facing interfaces in hardware to bypass the filtering appliance entirely for flows not requiring further inspection. This bypass mechanism saves resources on the filtering appliance. It also enables the security appliance to be removed from service or updated without affecting network throughput and availability.

SSL Connection Establishment

Oftentimes, SSL connections are passively ignored or actively dropped by "bump-in-the-wire" security appliances. To decrypt SSL, the SSL Appliance sits inline and acts a transparent proxy to SSL flows traversing the system to provide plaintext of encrypted SSL sessions to adjacent security appliances.

As previously described, the SSL Appliance is deployed as a "bump-in-the-wire" directly inline with flows to and from protected computing resources. This transparent proxy does not require IP interface configuration on the SSL Appliance's Ethernet interfaces. This enables the original IP address of the client to communicate with the original IP address of the server without further administrative intervention, such as SSL proxy configuration on clients. The SSL Appliance acts as a "man in the middle" and intercepts SSL sessions as they are established/negotiated between the SSL client and server.

By intercepting these sessions, the SSL Appliance transparently establishes two SSL sessions: one between the SSL client and the SSL Appliance; and another between the SSL Appliance and SSL server.

Each individual SSL session terminates on the SSL Appliance, but TCP connections are retained end-to-end via TCP splicing. The SSL stream is parsed, terminated, decoded and regenerated on the other side. The TCP ACK loop continues to operate between the main client and server, not to the SSL Appliance. Terminating and re-originating SSL enables the appliance to get hold of the plaintext in the encrypted payload that can be sent to the adjacent security appliance in a valid, regenerated TCP stream. This stream can be made available via an internal API, sent to a host interface (VNIC) or sent to an attached security appliance. Although the unmodified sniffing or filtering application will see the contents of the unencrypted SSL flows, the data remains encrypted on both the connection from the client to the SSL Appliance and from the SSL Appliance to the web server.

Certificates

During SSL session establishment, the SSL Appliance acts as a Certificate Authority (CA). The server certificate that would be usually stored in the server and transmitted to the client as part of the SSL protocol is transparently re-signed by the SSL Appliance. The name of the server in the certificate remains unchanged, but the rule of the CA belonging to the SSL Appliance is applied. A key is maintained for the SSL server in which all of the details are known to the SSL Appliance. The modified certificate is transmitted to the SSL client. Instead of the original server key, a different key is used between the SSL Appliance and SSL client. Since the private key associated with the modified certificate is known to the SSL Appliance, the whole SSL handshake can proceed successfully. If the SSL clients are configured to use the SSL Appliance as a trusted Certificate Authority the SSL client will see the server certificate as a valid CA-signed certificate. This process is called "re-signing," and enables the SSL Appliance to transparently intercept SSL communications.

SSL Proxy Modes

The Sourcefire SSL Appliance can work simultaneously in two modes with respect to SSL certificates and private keys. These modes are called "server-controlled" and "client-controlled." The primary difference between these modes is the location of the SSL Appliance relating to the SSL client/server.

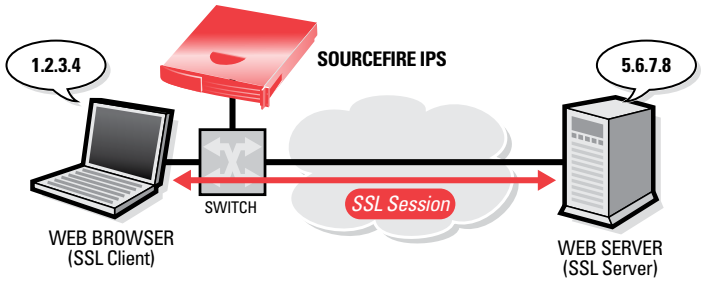

Figure 4. Sourcefire IPS cannot inspect encrypted SSL flows and has no access to decrypted plaintext in this configuration.

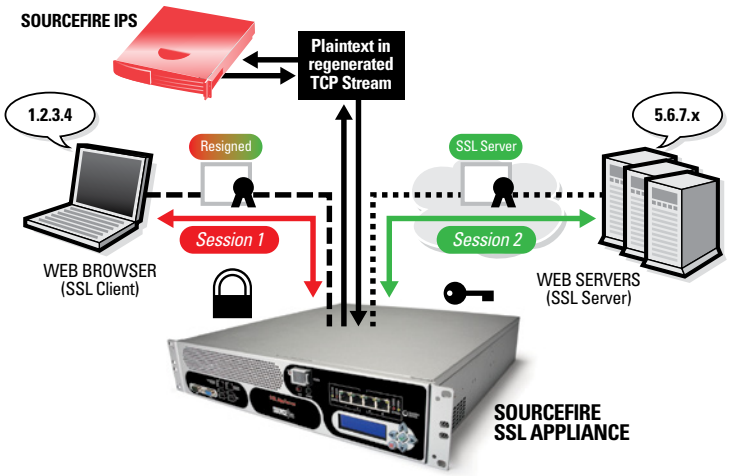

Figure 5a. The SSL Appliance can be deployed inline. The adjacent Sourcefire IPS is passed plaintext of decrypted SSL flows and (optionally) non-SSL data for analysis.

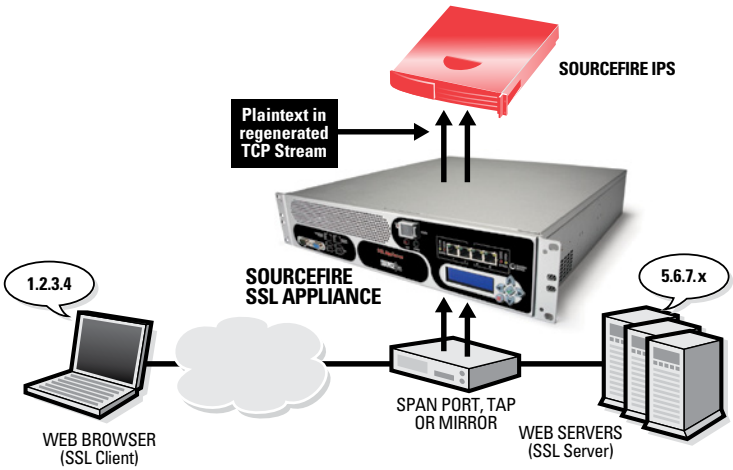

Figure 5b. The Sourcefire SSL Appliance can also be deployed in a passive mode of operation connected to a span port, tap or mirrored interface.

Figure 6. The Sourcefire SSL Appliance supports the following ciphers and encryption standards:

Encryption	TLS 1.0, TLS 1.1, SSL3, partial SSL2
Proxy Mode	Transparent
Public Key Algorithms	RSA, DSA, DH
Symmetric Key Algorithms	AES, 3DES, DES, RC4
Hashing Algorithms	MD5, SHA-1
RSA Keys	512, 1024, 2048, 4096, 8172 bits

Client-controlled

Also known as "re-sign mode" or "outbound SSL recrypt" in client-controlled operation, the SSL client and the SSL Appliance are under common administration by an enterprise IT organization. The SSL Appliance would be deployed to inspect outgoing client traffic to protect confidential information from leaking out of the enterprise. In this mode, the SSL Appliance does not have access to the destination SSL server private key(s). Instead, the certificate key that the SSL server would store and transmit to the client as part of the SSL protocol handshake is intercepted and transparently re-signed by a Certificate Authority (CA) in the SSL Appliance. The name of the SSL server in the certificate remains unchanged, but the rule of the CA belonging to the SSL Appliance is applied. A key for the SSL server is maintained in the SSL Appliance.

When the SSL Appliance intercepts a connection, it presents a "re-signed" server certificate to the SSL client. Provided that the certificate issued by the SSL Appliance is installed as a trusted root in the SSL client's certificate store, the SSL connection proceeds normally. If the certificate was not imported by the client, the client browser issues a security window to the user because the browser does not trust the certificate issuer. The user could accept the security warning pop-up box in the browser for the SSL connection to proceed.

The administrator does not need to have access to the server private key; he only needs to make the modification to the SSL client by installing the CA certificate to be used for re-signing (which is a common one-time configuration task for IT organizations). Optionally, a CA certificate that is a subordinate to the Root CA within the enterprise Public Key Infrastructure may be used for re-signing. This enables minimal administration if the Root CA certificate has already been installed in the client certificate store.

During resigning, the SSL Appliance will only modify the CA that issued the site's certificate. All other attributes present in the re-signed certificate are retained from the original certificate. In the case that a certificate that has expired, or contains a common name that does not match the host to which the certificate was issued, the client will be presented with a warning as though the SSL Appliance were not inline.

Server-controlled

In the server-controlled mode, or "key-known mode," the SSL server(s) and the SSL Appliance are in the same administrative domain. In this mode of operation, the SSL Appliance can be deployed to protect e-commerce or other SSL-server infrastructure from incoming web threats, as well as protect enterprise resources from threats originating over SSL-based VPNs. In server-controlled mode, the SSL-server private key is installed directly in the SSL Appliance. This enables the SSL Appliance to participate transparently during SSL session establishment between the SSL client and the SSL server.

High Availability

In order to ensure network uptime and enable the SSL Appliance to be installed and removed from the system with minimal network disruption, various forms of high availability measures are supported in the SSL Appliance system. The system supports both hardware and software features to reduce network downtime.

Network Interface High Availability

The SSL Appliance was designed to ensure that organizations retain network connectivity and guarantee traffic flow in failure scenarios, including loss of power to the appliance. Available with both copper- and fiber-based SFPs, the SSL Appliance supports a hardware relay-based interface card that can connect ingress and egress ports in case of power loss or any other failure of the SSL Appliance. Failure monitoring is accomplished by means of an active heartbeat from the PCIe acceleration card and CPU to the Ethernet relay interface card. If the heartbeat packets are no longer received, the Ethernet relay card will revert to one of two modes of operation:

- "Fail-open," where ingress and egress ports are connected via mechanical relay when a failure is detected in the SSL Appliance system. This will enable traffic to continue flowing and bypass the SSL Appliance, as well as any connected security appliances. The system defaults to this configuration.

- "Fail-closed," where the ingress and egress ports are no longer connected during a failure. Fail-closed is the preferred failure mode for highly secure applications that would prefer that no traffic be sent across the network (through the SSL appliance) when the adjacent application is unavailable to manage or inspect traffic.

System High Availability

NPU-based Bypass

The SSL Appliance supports bypass of all traffic received by the system, based on a Traffic Diversion Policy rule-set that assures that all traffic is cut-through the system and not forwarded to the attached IDS or IPS device entirely. This will enable traffic to continue flowing in the network in case of a failure in the attached security appliances. These pre-defined TDP rules do not protect from a failure in the SSL Appliance itself, but rather can be quickly applied to the SSL Appliance to keep traffic flowing in case of a failure of an attached security appliance. They also enable changes to be made to an attached network security appliance with minimal network disruption.

Link State Control

Ethernet link status is a common method used to identify network infrastructure failures from fiber cuts to system hardware or software problems. If Ethernet link or "carrier" is flagged as down, the network device connected to the interface reporting the error is unreachable. When an interface's link state changes, it is useful to report these state changes to adjacent devices. Inserting the SSL Appliance into the network architecture as a "bump-in-the-wire" enables it to report link failures on the network-connected ports, as well as state changes to and from the adjacent security appliance (filtering or sniffing modes). The SSL Appliance supports configurable behavior to mirror link state between pairs of ports that form a virtual "bump-in-the-wire." This enables the system to function in high availability deployment scenarios which rely on detecting the link state to determine the path through the system.

The SSL Appliance enables the administrator to remotely control the link state to force link down or enable auto-detection of each GigE interface through the web UI. In addition to manually controlling link state through the user interface, the SSL Appliance supports several link state mirroring modes where state on an interface can optionally be indicated on adjacent interfaces.

Link State Mirroring Modes

- Mirroring by Direct Coupling: In direct coupling mode, when link is lost on one GigE interface, link is immediately forced down on the paired GigE interface. Link indication will always mirror the state of the paired interface.
- Latching Mirroring: In latching mode, when link is lost, link is immediately forced down on the paired GigE interface. An administrator must manually configure the interface to again automatically sense link.
- Mirroring with Hysteresis: to avoid needlessly propagating a fluctuating link state, when link on an interface goes down, the system waits for a configurable time before bringing the paired link down. Once the link on an interface is restored, the system waits for an additional configurable time before configuring the paired link to automatically sense link state again.

Performance

Using SSL to encrypt data over a network ensures that the data was only read by its intended recipient and not intercepted during transmission. The SSL protocol is computationally intensive, though. Depending on the cipher suite chosen, SSL can slow down a web server or application substantially.

The SSL protocol is slow because public key cryptography is extremely CPU intensive. The time and number of CPU cycles required to establish an SSL session and encrypt/decrypt data are much higher than similar metrics for symmetric encryption and certainly for an unencrypted TCP connection.

Accordingly, inline SSL decryption is a potential bottleneck in network performance. Most SSL proxy devices in the industry only operate at hundreds of Mbps. Considering that they are almost exclusively deployed inline on Gigabit Ethernet interfaces, it takes many devices operating in parallel to keep up with network speeds, not to mention the additional hardware required to optionally load-balance flows across a large number of SSL proxies.

SSL Inspection Performance

The Sourcefire SSL Appliance is the industry's highest-performance transparent SSL proxy, supporting line-rate network performance, scalable flow-based processing, flexible cipher support and extremely high connection rates; metrics that enable the SSL Appliance to be installed in a network without becoming a bottleneck adversely affecting network performance.

Figure 7. Sourcefire SSL Appliance Performance

SSL Throughput	1 Gbps
Total Flows	1,000,000
Concurrent SSL Flow States	50,000
SSL Flow Inspection Per Second	30,000
SSL Flow Setups / Teardowns Per Second	2,900
Traffic Diversion Policies	32,000
SSL Session Log	10,000,000 entries
Cut-through Latency	<40us

Conclusion

With the amount of SSL-encrypted traffic forecasted to continue to increase, IT network operators are looking for new solutions that satisfy their need for information security for the enterprise and individual users, as well as the requirement for corporate compliance, acceptable-use policies and government regulations for both security and privacy. The solution must also be provided without impact to network performance, because providing compliance at the expense of throughput is no more acceptable than meeting user and application bandwidth requirements while ignoring security. To date, it has been difficult, if not impossible, to satisfy these competing requirements for security, performance and control. Thankfully, for enterprise network operators, a next generation of high-speed, transparent SSL proxies is now poised to deliver it.

The Sourcefire SSL Appliance is the industry's highest-performance SSL proxy of any type, providing IT administrators with visibility into the contents of encrypted flows at the highest speeds, largest number of flows and highest connection rate. Beyond industry-defining performance, the Sourcefire SSL Appliance is unique by being the first transparent SSL Proxy that both increases security and significantly minimizes deployment and operation costs by removing costly user and network configuration.