Encrypted Threat Protection
Network IPS for SSL Encrypted Traffic
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>SSL Encryption Overview</td>
<td>3</td>
</tr>
<tr>
<td>The Need for SSL</td>
<td>3</td>
</tr>
<tr>
<td>SSL Advantages and Disadvantages</td>
<td>3</td>
</tr>
<tr>
<td>Legacy SSL Intrusion Prevention Techniques</td>
<td>3</td>
</tr>
<tr>
<td>The Need for Network IPS in the SSL Environment</td>
<td>4</td>
</tr>
<tr>
<td>Requirements for an Effective SSL Network Intrusion Prevention System</td>
<td>4</td>
</tr>
<tr>
<td>IntruShield SSL Traffic Inspection and Prevention Details</td>
<td>5</td>
</tr>
<tr>
<td>IntruShield Architecture</td>
<td>5</td>
</tr>
<tr>
<td>SSL Inspection Techniques</td>
<td>5</td>
</tr>
<tr>
<td>IntruShield SSL Inspection Coverage</td>
<td>5</td>
</tr>
<tr>
<td>IntruShield SSL Attack Prevention Methods</td>
<td>6</td>
</tr>
<tr>
<td>IntruShield SSL Packet Analysis Options</td>
<td>6</td>
</tr>
<tr>
<td>IntruShield SSL Key Security</td>
<td>6</td>
</tr>
<tr>
<td>Conclusion</td>
<td>7</td>
</tr>
</tbody>
</table>
Introduction

Protecting valuable information assets from network-based attacks is the primary function of any network intrusion prevention system. Until now, protection of assets that use SSL encryption technology (such as Secure HTTP) has been beyond the reach of network IPS or IDS systems. With the introduction of IntruShield v2.1, the power of network IPS now can be extended to protect network servers that use SSL encryption to ensure the confidentiality of their transactions. IntruShield 2.1 is a firmware and software release designed to extend the power of the IntruShield purpose-built sensor. IntruShield 2.1 runs on any IntruShield hardware sensor and provides SSL decryption support on the I-4000 and I-2600 sensor models. This paper is an introduction to the benefits and techniques used to address the problems of inspecting and protecting encrypted traffic on the network.

SSL Encryption Overview

The Need for SSL

As use of the World Wide Web began to grow in the early 1990’s, a secure mechanism to enable commercial Internet transactions became necessary. Two major requirements were identified to enable e-commerce transactions: 1) the ability for internet consumers (clients) to reliably identify the internet vendors (e-commerce servers) with whom they were transacting business, and 2) the need to protect the confidentiality of the clients’ sensitive information as it transited the Internet.

Netscape communications introduced Secure Socket Layer (SSL) v2.0 in 1995 as a solution to fulfill these two requirements. SSL blends Digital Certificate technology for reliable identification of the target server, with encryption for protection of the confidentiality of information as it passes between the client and the server.

SSL Advantages and Disadvantages

The success of SSL in e-commerce is a testament to the advantages of the technology. Using the common Web browser as the primary client software simplifies support requirements by eliminating the need for additional software applications. Authentication of the target SSL Web server is transparent to the end user and is fairly reliable. Encryption algorithms have evolved with the technology to provide a high level of security with the availability of 128-bit and higher keys.

There are some fundamental disadvantages with the technology when examined from a Network or server security perspective. Authentication with SSL is achieved with the identification of the server by the client via a Digital Certificate that is issued and signed by a Certificate Authority (CA) and stored on the server. Identification and authentication of the client accessing the server, although possible, is not practical for the purposes of e-commerce since the vast percentage of clients do not have Digital Certificates that are signed by a registered CA. Without a certificate signed by a CA, reliable identification of the client to the server is not possible. This can lead to a situation where an anonymous client on the Internet can connect to the SSL server, establish an encrypted session and then use this session as a secure channel for attacking the specific Web server associated with the session. The encrypted SSL connection has traditionally prohibited network security or management personnel from inspecting the contents of the session prior to its termination at the SSL concentrator or the Web Server that terminates the SSL session.

Legacy SSL Intrusion Prevention Techniques

Historically the only practical method for protecting against SSL-encrypted attacks has been with the use of host IPS solutions. Host IPS solutions reside on the server itself and either inspect the traffic coming into the host after it has been decrypted, or monitor the behavior of the underlying system to mitigate an attack after it has entered the system. While host IPS provides effective system-level protection for encrypted threats, enterprises need a method to proactively prevent encrypted attacks from compromising critical SSL-enabled infrastructure. This would provide an additional layer of protection and would add flexibility for network security professionals. In order to achieve comprehensive protection against those attacks hidden within encrypted connections, enterprises need to adopt a layered approach that includes proactive network protection for critical infrastructure while assuring business availability and data confidentiality.
The Need for Network IPS in the SSL Environment

By its very nature, information that requires protection via SSL is "critical" data. HTTP is one of the most popular protocols for attackers since it must be made publicly available to be useful. Not only is it important to protect the sensitive data that resides on the Web server itself, but modern e-commerce sites typically access information stored on database servers that live at the very core of the network. Protecting the SSL-enabled Web server from compromise not only safeguards the data local to the Web server, but helps to eliminate a potential attack channel into the heart of the "trusted network". To effectively access data that resides at the core of the network, the Web server must be granted some level of trust through the firewall to the core assets. If the "trusted" Web server is compromised and taken over by an attacker, the trust relationship can be used for penetration of other valuable assets within the network.

Network IPS provides protection for the SSL-enabled e-commerce infrastructure from attacks against the underlying Web server software via the encrypted SSL tunnel. Network IPS provides a host platform neutral solution that runs with virtually any SSL-enabled server. By enabling protection at the network level, server resources are conserved for processing of user requests, thereby minimizing the complexity and associated fragility of the server environment.

Requirements for an Effective SSL Network Intrusion Prevention System

The following outline critical requirements for an effective, mission-critical SSL network IPS:

- **Accuracy**—In today’s dynamic threat environment, accurately detecting malicious traffic is critical to network operators. Although false-positives from a network IDS may result in unnecessary alerts and create an annoyance, false-positives from a network IPS are more critical since they can result in the blocking of legitimate network traffic. To reliably block malicious traffic while allowing normal traffic to flow requires a sophisticated system that utilizes and integrates multiple detection technologies, and supports extremely granular security policy applications.

- **Security**—The core tenant of SSL and its constituent authentication and encryption components is the protection of the servers’ private key. If the confidentiality of this key is compromised, the authentication and encryption functions of the system are rendered useless. Any viable solution must preserve the confidentiality and integrity of the private key to be effective. Any system is only as strong as its weakest link. Security must be designed into all aspects of the system. Features that should be present in the system to maximize the overall security posture of the organization include effective audit capabilities, control of operator access, and the encryption of traffic between all components of the system.

- **Performance**—Any solution that is introduced into the data path of critical assets must be capable of performing its function without introducing any significant latency into the system. Although HTTP transactions are more tolerant of delays in the transmission path than many protocols, speed equals capacity for an e-commerce site. Any significant delay will require the deployment of further Web servers to maintain transaction capacity, increasing costs and complexity and decreasing the efficiency of the overall system.

- **Reliability**—Reliability is required for any system designed to be deployed in-line with the data path, particularly with high value SSL based systems. A highly reliable architecture with fail open and redundant high availability capabilities
are critical to ensure minimal down time. Costs for down time on e-commerce systems can often be calculated in the
tens to hundreds of thousands of dollars per minute.

IntruShield SSL Traffic Inspection and Prevention Details

**IntruShield Architecture**

The IntruShield system is designed with a three-tier architecture. The sensor is a highly reliable, purpose-built appliance
designed for wire-speed performance with all detection capabilities enabled. The middle tier consists of a dedicated
management server that provides full configuration and monitoring functions to all sensors deployed in the network. The
Manager can be deployed on the host platform and hardware that best suits the customers’ needs. The Manager supports
both Windows and Sun Solaris platforms. The Manager also supports MySQL with the Intel platform and Oracle with the Sun
or Intel platforms. The client system consists of a fully Web-enabled browser-based client. All components of the system
communicate via secure, encrypted communications links.

**SSL Inspection Techniques**

IntruShield inspects the SSL data stream by securely
storing a copy of the server private key on the sensor.
When a client initiates a connection request to the SSL
server, IntruShield recognizes the SSL session request and
monitors the SSL session initiation transaction between the
client and the server. During the SSL session
establishment phase, IntruShield uses the server’s private
key to decrypt and inspect the data and to determine the
session keys. With these session keys, the IntruShield
sensor can decrypt data packets for the life of the SSL
connection. As an encrypted packet enters the sensor,
IntruShield copies the encrypted packet, decrypts and then
inspects the contents of the packet. The original packet is
temporarily stored in a buffer in the sensor during the
inspection phase.

**IntruShield SSL Inspection Coverage**

Upon conversion of the data into clear text, IntruShield processes the data through its Protocol Normalization processors,
forwards the normalized results to the Protocol and Application anomaly engines, the Statistical DoS and DDoS detection
engines and finally into the signature matching engine. The results of all the engines are correlated to arrive at the final
detection decision. Non-SSL traffic that does not trigger an alert is forwarded from the Normalization engine to the destination
target ensuring “clean” traffic at the protocol level. In the case of non-attack SSL traffic, the original packet is released from the
input buffer to the destination and the data from the Protocol Normalization engine is discarded. This approach ensures the
integrity of the original packet and relieves the sensor from the overhead associated with re-encrypting the packet. This
exhaustive inspection process is implemented in the custom silicon processing engines incorporated into the sensor and is
processed and correlated by the Real Time Operating System (RTOS) resident in firmware on the appliance.

IntruShield can protect multiple SSL servers that use different private keys automatically. All SSL sessions are processed and
tracked in separate input queues in the sensor. The sensor tracks these connections via the IntruShield State tables and a
relationship is maintained between the active session and the private key associated with that session. Incoming packets are
automatically matched to the appropriate key for decryption and inspection.

www.mcafee.com
Multiple security policies with the ability to support multiple, unique configurations of SSL hosts are supported via the Virtual IPS capabilities of the system. A single physical interface within the sensor may be logically subdivided by assigning sub-interface designations to the physical interface. Sub-interfaces can be defined by 802.11q VLAN tags, CIDR address blocks, or even by individual IP addresses. This allows for greater accuracy when supporting a heterogeneous SSL infrastructure. Policies may be created to detect and prevent attacks that are targeted at the specific operating system or Web Server applications resident on the protected servers.

Dedicated Management Domains can be assigned at the sub-interface level. This allows for greater control of the personnel tasked with managing the security infrastructure. For example, operators can have rights assigned to one Management Domain while being restricted from having access to any other defined system Domains. This granularity in operator control increases the overall accountability and security of the installed system and may be of particular interest to organizations that provide SSL enabled E-Commerce services to external customers.

**IntruShield SSL Attack Prevention Methods**

Upon detection of an attack, IntruShield can be configured to block the attack packet, allow the packet to pass while raising an alert, or allow the packet to pass without raising an alert. If an attack is detected within the packet and the system is configured to block the attack, the original packet stored in the buffer is dropped and the sensor sends notification to the Manager to log and/or send an alert to the designated operator(s).

**IntruShield SSL Packet Analysis Options**

The sensor can be configured to capture and store copies of decrypted packets associated with an alert or block action on the IntruShield Manager. Capture configuration is available on a per-signature basis, providing extremely fine control of which packets are captured for future analysis. The SSL Packet Log feature is disabled by default. Access to the packets stored on the Manager can be controlled by the Manager’s Multiple Administrative Domain feature. Creation of a separate Administrative Domain for the sensor segment associated with the SSL Protection feature restricts access to the captured packets to personnel assigned access to this specific Management Domain.

**IntruShield SSL Key Security**

Protection of the SSL Private Key is paramount, and IntruShield uses a number of mechanisms to ensure key confidentiality. Private keys are encrypted and exported from the SSL Server in PKCS #12 format and are imported into the IntruShield Manager via portable media, writable CD, floppy disk, etc. The encrypted key is imported into the IntruShield Manager and is encrypted again with the public key of the IntruShield sensor on which it will be used. When the Sensor is configured to perform SSL inspection, the Manager pushes the encrypted key to the sensor. The sensor decrypts the key with its private key and stores the resulting clear text SSL Private Key in volatile memory in the sensor. If someone gains unauthorized access to the IntruShield Manager the value of the SSL Key can not be determined without the possession of the Sensor Private Key that is generated and stored on the Sensor itself. If the Sensor is physically stolen, the unencrypted copy of the Private SSL Key is lost as soon as power is removed from the Sensor, or a re-boot of the Sensor is performed. The Private SSL Key is never transmitted or stored in unencrypted format and only exists in an unencrypted format in volatile RAM within the Sensor.
Conclusion

The ability to inspect and protect SSL-encrypted traffic represents a major milestone in the Network Intrusion Prevention field. IntruShield is the first IPS solution to provide this capability while fulfilling the four major requirements for the protection of critical SSL encrypted information.

- **Accuracy**—By integrating all aspects of attack detection—including Protocol and Application Anomaly inspection, multi-field, multi token signature inspection, and Self Learning Statistical Anomaly DoS and DDoS Detection—IntruShield’s accurate detection technology forms the foundation for the most accurate attack prevention solution for today’s mission-critical in-line IPS deployments

- **Security**—Extending the benefits of Intrusion Prevention to SSL-encrypted traffic represents an unprecedented increase in the security of critical network assets. By ensuring the Private SSL Key is never exposed in an unencrypted form, IntruShield ensures that the confidentiality and integrity of the SSL Key is not compromised. This added security enables high-confidence adoption and deployment of the technology.

- **Performance**—IntruShield sensors are powered by programmable security-focused hardware for mission-critical performance and attack prevention. As a result, IntruShield sensors can support thousands of signatures at wire-speed traffic rates without any packet loss, while protecting against known, zero-day, and DoS attacks for both clear-text and encrypted traffic. IntruShield delivers compelling price and performance for needs ranging from 100’s of Mbps to multi-gigabit bandwidth rates

- **Reliability**—IntruShield appliances are equipped with redundant fans and optional redundant power supplies and have no internal hard disk drives that may be prone to premature failure. This advanced and unique architecture provides the highest reliability in the industry. As well, fully redundant configurations with automated optical bypass capability provide full fail-open and fail-over support and are uniquely suited for mission-critical in-line deployments.