



Secure Information Flow

Technical Note

Inspection of Encrypted HTTPS Traffic

StoneGate version 5.0 SSL/TLS Inspection

Table of Contents

Overview	3
Why HTTPS Inspection is Needed	3
Network-based Security Enforcement	3
Risks in HTTP Traffic	4
Browser Attacks	4
Filtering Malicious Content	5
Technical Description	6
What Can Be Inspected	6
Transparency of the Inspection	6
What Information is Included in the Logs	6
Administration of StoneGate Firewall and IPS	7

Inspection of Encrypted HTTPS Traffic

Overview

StoneGate Firewall version 5.0 and StoneGate IPS version 5.0 can open encrypted HTTPS traffic for security inspection. This gives network security administrators the ability to monitor the traffic inside the encrypted TLS/SSL tunnel, and to detect and react if there is any unwanted content. The benefit of the feature is that administrators can ensure that no attacks, viruses, or other unwanted content can enter the organization's network by disguising themselves inside the encryption cloak.

Why HTTPS Inspection is Needed

Before listing the benefits of HTTPS inspection, let us first discuss why the appropriate security enforcement cannot be done solely on the workstation end.

Network-based Security Enforcement

In many organizations, information technology security is enforced in numerous different locations. Some security enforcement may be done on the workstations and the servers, whereas other enforcement must be done in the network. The reasons for network-based security devices include, among other things, cost-effectiveness, and the ability to monitor workstations that lack host-based security. With the increase of virtual hosts within workstation computers, the need for network-based security grows even further.

The encryption used by HTTPS traffic means that under the normal circumstances, the traffic inside of the encrypted tunnel cannot be read or modified. The purpose of the encryption is to ensure the integrity and confidentiality of the data while in transit over the network. The encryption, however, also conceals the encrypted data from the supervision of network-based security devices.

As the organization's security relies heavily on enforcement in the network, the encrypted HTTPS channel acts as a means to bypass the security functions. A controlled way to open the encryption in the network and to submit the encrypted traffic for the same inspection as clear-text HTTP data eliminates the blind spot in the network protection.

Risks in HTTP Traffic

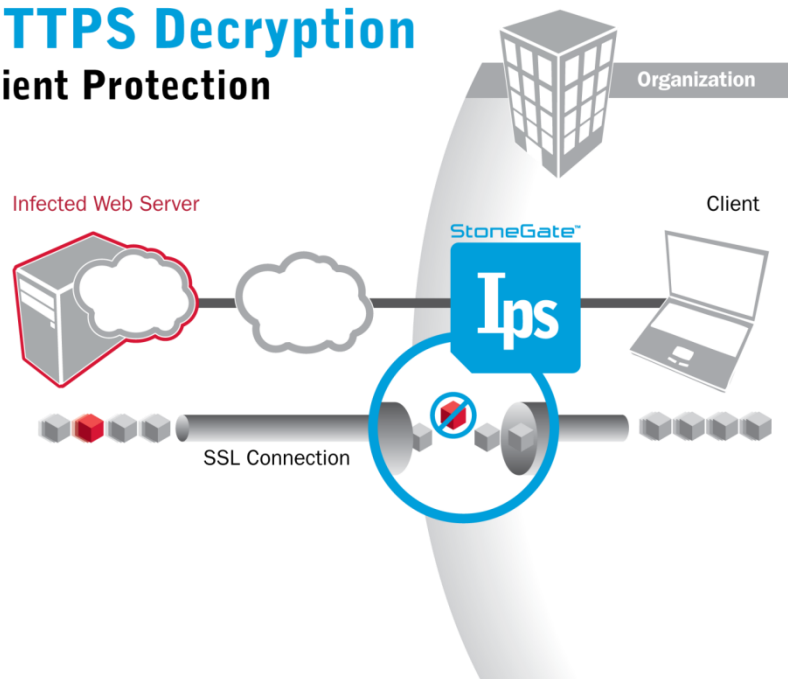
There are many reasons why HTTP traffic inspection increases the organization's security. All these reasons apply to HTTPS traffic as well.

Browser Attacks

Attacks against the vulnerable browsers have been on the rise for many years. A typical attack scenario is to send an email that contains a link to a malicious web page to the target user. By clicking the link, the user instructs the browser to connect the web server on the Internet. The server may then attack the browser and even compromise the host if the browser is vulnerable to the attack.

Compromised web sites are another potential source of attacks. Consider this example: an employee visits a familiar web site that uses HTTPS. The employee assumes the web site is secure because it uses encryption. However, the web site has been hacked, and now the hacker can use the web site to attack the employee's browser and exploit a known vulnerability. Once the browser has been compromised, the web site installs malware on the system, which can then "call home". Now the employee's computer can be used, for example, as a part of a botnet, or the malware can be used to disclose confidential company information.

HTTPS Decryption Client Protection



Traditional network security protection systems could not do anything to stop this, as all the traffic between the employee's computer and the web site was encrypted. The HTTPS inspection feature in StoneGate 5.0 eliminates the problem and stops attacks hiding inside encrypted traffic.

Similarly, HTTPS inspection allows administrators to prevent old and vulnerable browsers from connecting to the Internet, decreasing the risk even further.

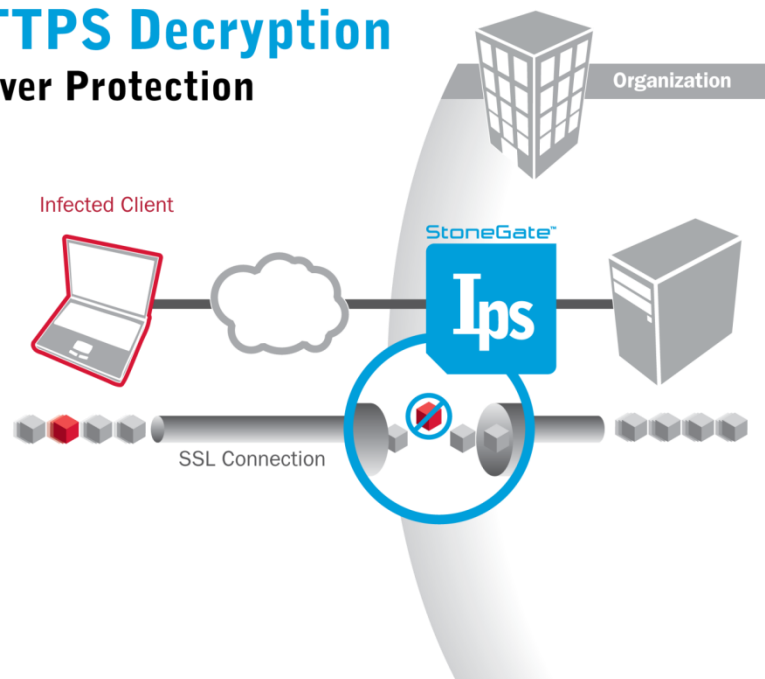
Server Protection

Server protection is needed to protect company servers from being compromised, which in turn may lead to other implications, such as loss of confidential data. In addition to direct financial implications, the loss of valuable data may have indirect consequences, such as the loss of credibility in the eyes of the customers.

Additionally, fulfilling regulatory compliance or a contractual obligation may require the ability to inspect encrypted traffic. For example, the Payment Card Industry Data Security Standard sets clear requirements for protecting the card holder data. To meet these requirements, companies may need to be able to look inside the encrypted traffic.

StoneGate Firewall/VPN and IPS products offer protection against attempts to exploit vulnerabilities in the Web server software on HTTP and inside TLS/SSL encrypted HTTPS.

HTTPS Decryption Server Protection



Known vulnerabilities in major Web server software, such as the Microsoft Internet Information Server and the Apache software are covered. The exploit protection is based on known vulnerabilities, which means that a new exploit variant against an old vulnerability is also detected and blocked by the StoneGate network security device.

Filtering Malicious Content

In addition to attacks, HTTPS inspection allows administrators to control what kind of content is transferred over the network. The organization's security policy may prohibit certain file types, files containing viruses, scripts, active-X or other possibly unwanted content.

Without HTTPS inspection, content filtering covers only clear-text HTTP traffic. HTTPS inspection adds the coverage for encrypted HTTPS traffic as well.

Technical Description

HTTPS inspection can be implemented in an organization by deploying the StoneGate Firewall or IPS in the organization's network and by enabling the HTTPS inspection feature. The Firewall or IPS comes with a new Certificate Authority (CA) certificate that should be installed in the browsers of all workstations in the organization. Administrators configure what network traffic is subject to the inspection, the list of the unwanted content the firewall or IPS monitors, and finally the level of logging the system provides.

What Can Be Inspected

With the default configuration, the StoneGate Firewall or IPS devices monitor only for clear text attacks, viruses, or similar abuse. HTTPS connections that do not trigger any signature do not provide any logs of the inspection process.

The administrator can optionally configure the system to monitor for other events as well. For example, the administrator may decide that vulnerable browser versions are prohibited from connecting to the Internet, certain file types may not be downloaded, or some other administrator-defined content is terminated.

Transparency of the Inspection

HTTPS inspection creates two separate secure connections: one from the client web browser to the Firewall or IPS engine, and one from the engine to the HTTPS server. Browsers within the organization that contain the new CA certificate of the StoneGate Firewall or IPS do not warn users even though the Firewall or IPS breaks the end-to-end encryption of the HTTPS traffic. A user who knows where to look may study the details of the certificate in the web browser and learn whether a particular connection is being inspected. However, the user cannot confirm how the traffic is being inspected if inspection is enabled.

What Information is Included in the Logs

StoneGate Firewall and IPS provide logs in two levels. Access logs contain information about the connection, such as the IP addresses, ports, and the time when the connection happened. Inspection logs are provided only if the content of the traffic matches any of the signatures that are looked for in the traffic.

Inspection logs contain information about the event that has been detected in the traffic. For example, an inspection log could show that a certain type of attack was detected from the web server to the browser, but was terminated by the Firewall or IPS. Inspection logs in the default configuration contain IP addresses, the event name and description, the URL that triggered the event, and the time when the event occurred. The administrator may also configure the system to provide more detailed information about the traffic in the logs.

Administration of StoneGate Firewall and IPS

StoneGate Firewall and IPS products are professional tools that can be used to significantly reduce the risk level in the organization's computer networks. The same products, however, in the wrong hands may also be used to violate other people's privacy or to cause harm otherwise. Therefore the administrative functions are secured against unauthorized use.

StoneGate Firewalls and IPS devices contain very sophisticated methods to ensure that only the authorized administrators may change the configuration or read the provided logs. These administrative security features include strong authentication for administrators (RADIUS support), encrypted and two-way authenticated connections between the StoneGate components, role-based access control for administrators, detailed audit logs of administrator actions, and dedicated log servers to better enable the securing of the log data.

Note

Traffic that uses HTTPS may be protected by laws related to the privacy of communications. Decrypting and inspecting this traffic may be illegal in some jurisdictions.

About Stonesoft

Stonesoft Corporation (NASDAQ OMX: SFT1V) is an innovative provider of integrated network security solutions to secure the information flow of distributed organizations. Stonesoft customers include enterprises with growing business needs requiring advanced network security and always-on business connectivity.

StoneGate™ Secure Connectivity Solution unifies firewall, VPN, IPS and SSL VPN blending network security, end-to-end availability and award-winning load balancing into a unified and centrally managed system. The key benefits of StoneGate the solution include low TCO, excellent price-performance ratio and high ROI. The StoneGate Virtual Security Solutions protect the network and ensure business continuity in both virtual and physical network environments.

StoneGate Management Center provides unified management for StoneGate Firewall with VPN, IPS and SSL VPN. StoneGate Firewall and IPS work together to provide intelligent defense all over the enterprise network while StoneGate SSL VPN provides enhanced security for mobile and remote use.

Founded in 1990, Stonesoft Corporation is a global company with corporate headquarters in Helsinki, Finland and Americas headquarters in Atlanta, Georgia. For more information, visit www.stonesoft.com.



Copyright July 09 Stonesoft Corporation. All rights reserved. All specifications are subject to change.