

**STONESOFT**

Whitepaper

---

# Multi-Layer Inspection

---

# Table of Contents

---

|                                       |   |
|---------------------------------------|---|
| Executive Overview                    | 1 |
| Components of Multi-Layer Inspection  | 1 |
| The OSI model and TCP/IP              | 1 |
| Packet Filtering                      | 2 |
| Stateful Inspection                   | 2 |
| Application Level Filtering           | 3 |
| Protocol Agents                       | 4 |
| Security Policies and Configurability | 5 |
| Conclusions                           | 6 |

# Executive Overview

Stonesoft's StoneGate™ High Availability Firewall and VPN solution introduces an advanced, hybrid technology for firewalls to the market. Customers wishing to securely connect corporate networks to the Internet, or to reinforce security between corporate LANs, have an even better choice of firewall technologies now than ever before. Combining the best aspects of application proxy firewalls with traditional packet filtering and stateful inspection technologies, Stonesoft developed Multi-Layer Inspection<sup>SM</sup>.

For more information about StoneGate please refer to Stonesoft web page at [www.stonesoft.com](http://www.stonesoft.com)

Multi-layer inspection is a packet and connection verification process developed by Stonesoft to ensure the best security in its StoneGate firewall and VPN product, while minimizing the impact on system throughput. The StoneGate firewalls use administrator-defined security policies to screen connections, and determine when to use stateful connection tracking, packet filtering, or when application-level scrutiny is required. The system expends the resources necessary for application-level security only when the situation demands it—without unnecessarily slowing or limiting network traffic.

Details on packet filtering, stateful inspection, and application proxies are available on the Internet.

This white paper describes Stonesoft's patent-pending multi-layer inspection technology, and discusses how it unites performance and security. The technology is contrasted with existing technologies. Multi-layer inspection is then placed in a business context to show how it addresses your needs and expectations.

## Components of Multi-Layer Inspection

Multi-layer inspection enables a system administrator to call on packet filtering or stateful inspection for performance, yet provides additional application level security—such as traditional application proxy firewalls provide—through the use of protocol agents. This customized security policy inspection results in secure, multi-gigabit throughput using standard Intel® or UltraSPARC™ platforms. This approach contrasts with traditional firewalls that limit the administrator's ability to manage the security process, restricting administrators to set configurations, specific protocols, or expensive and proprietary hardware. Multi-layer inspection provides components of traditional technologies, plus new ideas and approaches that overcome the liabilities other firewalls have.

### The OSI model and TCP/IP

In order to understand the different types of firewall technologies, it is important to understand the basic model upon which each is built. Every firewall, whether it is a packet filter, application proxy, or multi-layer inspection system, examines and controls the flow of TCP/IP traffic. TCP/IP is a set of common communication protocols used on the Internet for connecting systems to each other. The TCP/IP suite is the standard for Internet connections because it provides four layers of abstraction—creating an independence between the applications (such as e-mail programs or Web browsers), and the physical network technologies they communicate over (such as Ethernet, ATM, or FDDI). This model is derived from the standard OSI model, which achieves the same purpose, but defines the levels in seven layers. Figure 1 illustrates the two layers side-by-side.

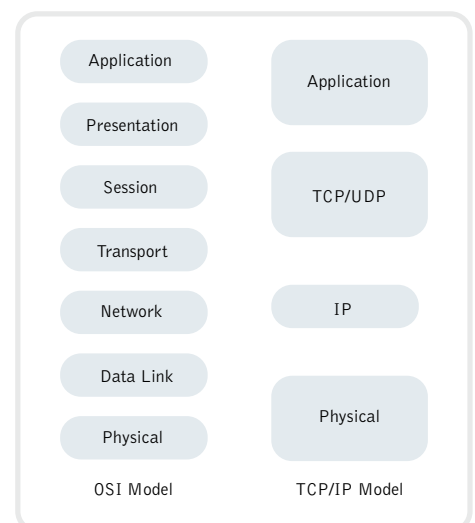


Figure 1. OSI model and TCP/IP layers for communications

Each of the technologies of traditional firewalls and multi-layer inspection described below will reference the OSI model for comparison.

## Packet Filtering

One of the oldest, and one of the most common types of firewall technologies are packet filtering firewalls. Packet filters inspect connection traffic at the network layer, and only the network layer. They examine and control traffic based on IP address information and compare the information to access control rules to decide whether the packet should be allowed through the firewall. Packet filtering principles are illustrated in Figure 2.

Packet filters can be very fast; since they do not concern themselves with data in the upper layers—including application information—they can examine and decide packet flow very quickly.

Packet filters have several disadvantages, however. Because every packet of every connection is checked against the access control rules, larger, complex rule bases decrease performance. And because packet filters only check information at the network layer, they are not as secure—malicious code hiding in the other layers can pass through undetected. Because of their limitations, packet filters are often used as a first defense in combination with other fire-wall technologies, and their most common implementation today is seen in the access control lists of routers at the perimeter of networks.

For simple protocols, or one-sided connections, like ICMP or SNMP traps, it is still useful to use packet filtering technology. StoneGate's hybrid approach with multi-layer inspection allows administrators to define specific rules for these instances, where packet filtering is sufficient to meet the demands of the security policy, while still providing the benefits of other firewall technologies.

## Stateful Inspection

Stateful inspection firewalls were developed in the early 1990s to overcome some of the limitations of packet filters. Most of the well-known firewalls in the marketplace today are stateful inspection firewalls. Stateful inspection firewalls also examine packets based on network layer information, as illustrated in Figure 3.

Stateful inspection firewalls only compare the first packets of connections against the defined security policies. Once a connection has been established, it is recorded in a table. This table is checked first when packets arrive at the firewall, and if a packet matches the information there, it is allowed to pass. By using this table of connection data, the overall process of matching and controlling packets is dramatically improved if complex security policies are involved.

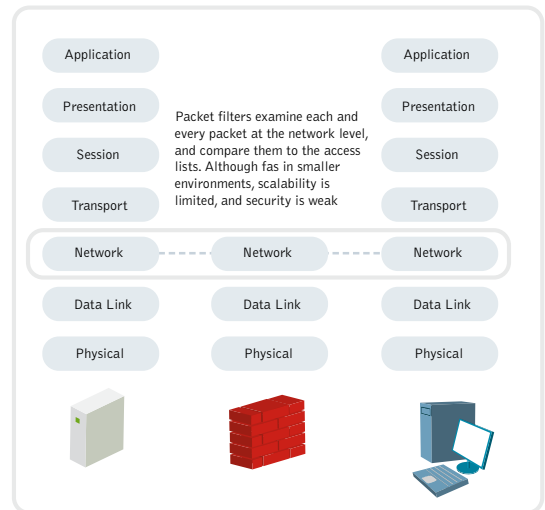


Figure 2. Packet filtering

StoneGate provides a wide range of features out of box that would normally be an additional cost with other products- and some of those features are simply not available with other products. - SC Magazine, October 2001

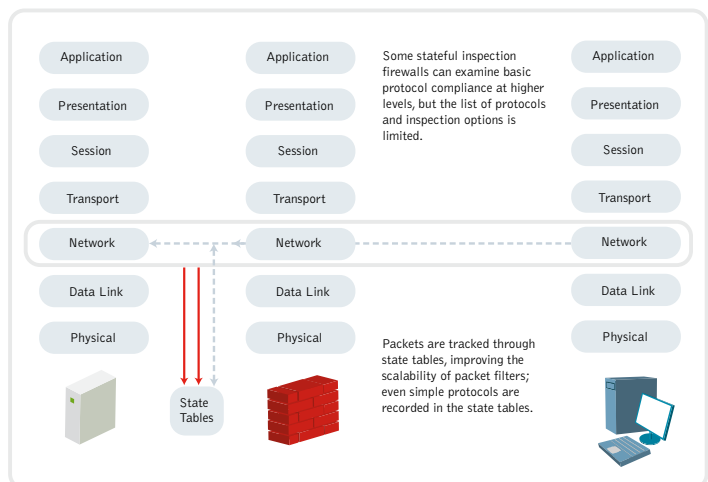


Figure 3. Stateful inspection

Although stateful inspection firewalls have improved the scalability issue inherent to simple packet filters, they still have several disadvantages. In general, stateful inspection systems still provide no application level security; the upper layers are not examined, and malicious code hiding there can still pass undetected. Stateful inspection systems also inspect, record and monitor state tables for every connection protocol, whether it makes sense to do so or not. And for simple protocols where there is no connection (e.g., ICMP or UDP), stateful inspection firewalls lose their advantage over packet filters.

With StoneGate, the administrator again has a choice. Individual rules in the security policies use stateful inspection technologies by default. Stone-Gate also employs advanced packet handling algorithms that treat connectionless protocols, like ICMP or UDP, as virtual connections. Additionally, administrators can customize a wide range of time-out intervals for connections, and enforce those values on a rule-by-rule basis. In other words, as with packet filters, stateful inspection technology can be applied to just those rules where it makes the most sense to do so.

An example of the customization advantages of StoneGate over stateful inspection firewalls is the use of time-out intervals. In traditional stateful inspection firewalls, if there are no packets transferred as part of a connection for a period of time, the connection information is removed from the state tables, and therefore the connection is dropped. However, an administrator may wish to maintain an SSH (secure shell) connection to a remote Unix server. Such a connection may be open for hours or days for monitoring or troubleshooting purposes. Yet in a stateful inspection firewall, the connection would be dropped. In StoneGate an administrator can explicitly state that connections from the system administrator’s machine to the remote Unix server should have a much greater time-out value; thus ensuring that the connection remains open to collect the troubleshooting data.

### Application Level Filtering

The third type of firewall technology traditionally seen in the market is application level firewalls. These firewalls, also known as application proxies, provide the most secure type of data connection because they can examine every layer of the communication, including the application data, as seen in Figure 4.

A study of attack trends by CERT notes that “sophisticated attack tools...use protocols like IRC or HTTP to send data or commands from the intruder to compromised hosts.”

But to achieve this security, proxies—as their name suggests—actually mediate connections. In other words, a connection from a host to a server is actually opened to the proxy. If the proxy determines that the connection is allowed, it opens a second connection to the server from itself, on behalf of the original host. The data portion of each packet must be stripped off, examined, and rebuilt and sent again on the second connection.

This thorough examination and handling of packets through a second connection means that proxy firewalls are very slow. Proxies are also limited as firewalls, because they must understand the application layer; as new protocols are developed, new proxies must be written and implemented to handle them. Therefore, proxies only support a handful of the more common protocols.

In StoneGate’s multi-layer inspection, a new approach to proxy technology has been taken. In addition to being able

to select packet filtering or stateful inspection technologies, application level security can be applied to specific rules in the security policy when needed. However, multi-layer inspection provides this security without the severe performance penalties normally associated with proxy firewalls, because two separate data connections are no longer required. This is achieved by a new component unique to multi-layer inspection, known as protocol agents.

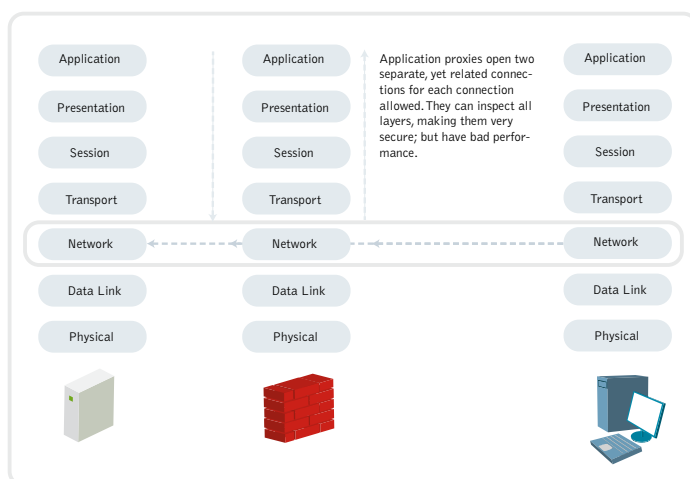


Figure 4. Proxy firewalls

## Protocol agents

Protocol agents are a flexible, configurable, and extensible component of the StoneGate security gateways. When application-level security is required by the administrator, protocol agents can be assigned to perform the additional scrutiny required. They also assist the firewall with handling complex connections, such as Oracle® or FTP, redirection of traffic to content inspection systems (e.g., anti-virus servers), enforcing protocol standards, and modifying the data payload if necessary.

One of the most useful security benefits of protocol agents is the ability to enforce protocol standards. For example, many traditional firewalls can allow SSH connections to pass through the firewall. But because SSH creates encrypted connections, many proxies or stateful inspection firewalls simply examine the destination port to determine that the connection is SSH. Since it is an encrypted connection, it is assumed that there is little else to be done. In other words, an intruder can get malicious code or packets through the firewall by disguising them as an SSH connection. With StoneGate, the SSH protocol agent is called upon at the beginning of the connection. The protocol agent in this case assists the firewall by examining the first few packets and ensuring that they conform to the SSH standard—in other words, that the connection is really SSH, and not something else. Unlike proxies, the protocol agent can be ended once the encryption starts, freeing resources on the firewall gateway for other packet handling operations.

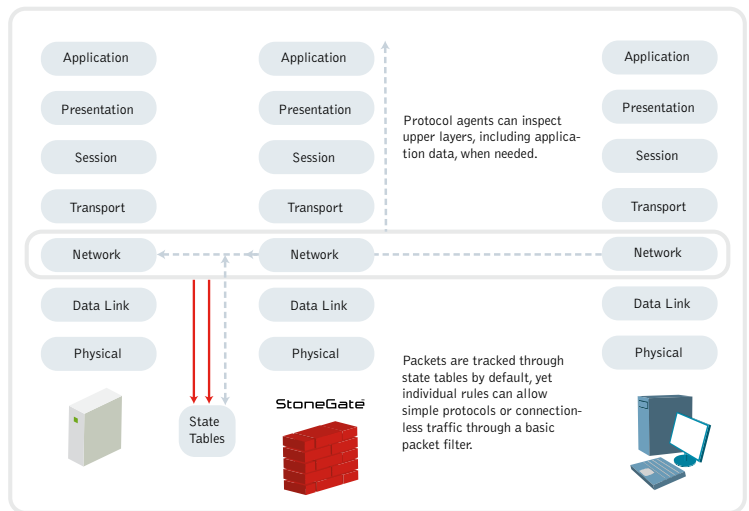


Figure 5. Multi-layer inspection flexibility

Another ability of protocol agents is the ability to redirect traffic to content inspection systems. Content inspection is commonly used to provide anti-virus protection or Web address filtering. They are designed, as a SANS Institute article explains, “to prevent attacks against servers using malicious content that is syntactically correct from a protocol perspective, yet from the perspective of the applications, semantically dangerous.” In StoneGate, protocol agents can be configured at the rule level to redirect traffic to such an inspection system for further analysis; the administrator can choose to only have this redirection take place when it is necessary to do so. Figure 6 illustrates packets being redirected to a content inspection server for Web filtering, as an example.

In addition to inspecting the protocol in more detail than traditional systems provide, and adding the ability to redirect traffic to content inspection systems for further analysis, multi-layer inspection also provides the ability to modify application data through protocol agents. Complex protocols, such as H.323, which is used by voice over IP applications (e.g., Microsoft® NetMeeting®), do not pass through packet filters or stateful inspection firewalls

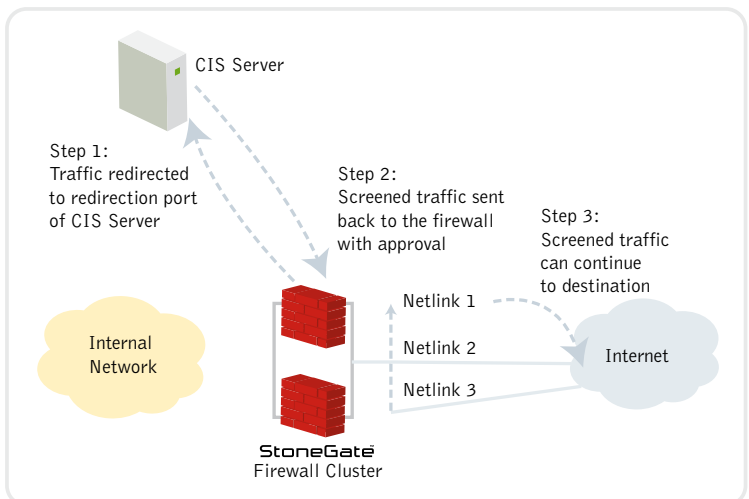


Figure 6: Protocol agents and content inspection

when the IP addresses are translated using network address translation (NAT). Such protocols often contain address information about associated voice gateways and call

"StoneGate offers firewalling beyond stateful inspection, scalability, high availability, and hierarchical grouping of firewall components that no other vendor approaches." - Ned Schumann, CEO, Townsend Communications Inc.

endpoints within the data of the packet—data which is not translated by firewalls because they are not designed to do so. With StoneGate's multi-layer inspection, protocol agents can examine and modify such application data, yet because the system does not establish two separate connections the performance and translation problems associated with application proxies do not affect the firewall. In the same way, other complex protocols, which require multiple, yet related connections, such as Oracle® database connections or even FTP are also handled more efficiently with multi-layer inspection. Protocol agents monitor connections for these protocols, and can instruct the firewall to allow related connections. With such assistance, the firewall does not need to perform additional checks against the security policy, and all connections required for the protocol are handled without the firewall inadvertently rejecting them.

## Security Policies and Configurability

With StoneGate and multi-layer inspection, the best aspects of each type of firewall technology, from basic packet filters to stateful inspection and robust, high performance application proxy technologies have been combined. Each of these can be implemented in security policies, giving today's network administrators the highest level of configurability to meet the needs of 21st century networks.

By default, most rules in StoneGate security policies implement stateful inspection methods to ensure robust security with great performance. Unlike traditional firewalls, however, multi-layer inspection gives the administrator the ability to use packet filtering methods where it makes sense to do so. For example, SNMP traps from server systems and network devices can pass through the firewall to a management network for monitoring conditions, using packet filtering because it is faster, and the level of security and the overhead of stateful inspection is not required.

Since stateful inspection methods are the default, however, large complex rule bases do not slow down the system as would normally happen with traditional packet filters.

Yet, when necessary, the administrator can implement application-level security by setting protocol agents for specific services and rules in the security policies, ensuring that certain connections meet the additional scrutiny necessary.

Because all of these options, and the options configurable in each protocol agent, are set at an individual rule level, the security requirements can be controlled to a level beyond what traditional firewalls offer.

# Conclusions

---

StoneGate's multi-layer inspection technology provides the best features of packet filters and stateful inspection firewalls, while removing the disadvantages. When application proxy technologies are desired for maximum security benefits, they can be applied to specific rules and policies, yet are implemented in such a way that they remove performance bottlenecks. Because protocol agents, a key component of multi-layer inspection, are extensible and flexible, they can be customized at the rule level as well.

With multi-layer inspection, administrators can have the best firewall technologies in the market in a single system, with centralized management, high availability, scalability and performance built-in.

---

**STONESOFT**

**Stonesoft Corp.**

Itälahdenkatu 22 A  
00210 Helsinki  
Finland  
tel. +358 9 476 711  
fax. +358 9 476 712 34

**Stonesoft Inc.**

1050 Crown Pointe Parkway  
Suite 900  
Atlanta, GA 30338, USA  
tel. +1 770 6681 125  
fax. +1 770 6681 131

Copyright 2006 Stonesoft Corp. All rights reserved. Registered or unregistered trademarks in this document are property of their respective owners. The products described in this document are protected by one or more of U.S. patents and European patents: U.S. Patent No. 6,650,621, European Patents No. 1065844, 1289202, and may be protected by other U.S. patents, foreign patents, or pending applications. Specifications subject to change without notice.