



STONEGATE 5.0

FIREWALL/VPN EVALUATOR'S GUIDE

FIREWALL

VIRTUAL PRIVATE NETWORKS

STONESOFT

Secure Information Flow

CONTENTS

Getting Started	3
Installation and Configuration	4
Feature Overview	8

Getting Started

This guide is designed to help you set up StoneGate Firewall/VPN and StoneGate Management Center, and explore the main features of the system. In addition, you will see many of the new features introduced with StoneGate 5.0 including:

- Centralized monitoring of third-party devices.
- Domains for enforcing administrative boundaries within the centrally managed system.
- Automatic geographic pinpointing for IP addresses in various monitoring tasks.
- Web Portal for browser-based access to system information.
- Inspection of SSL-encrypted Web traffic for both client and server protection.
- Rule hit counters for easy clean-up of obsolete rules.

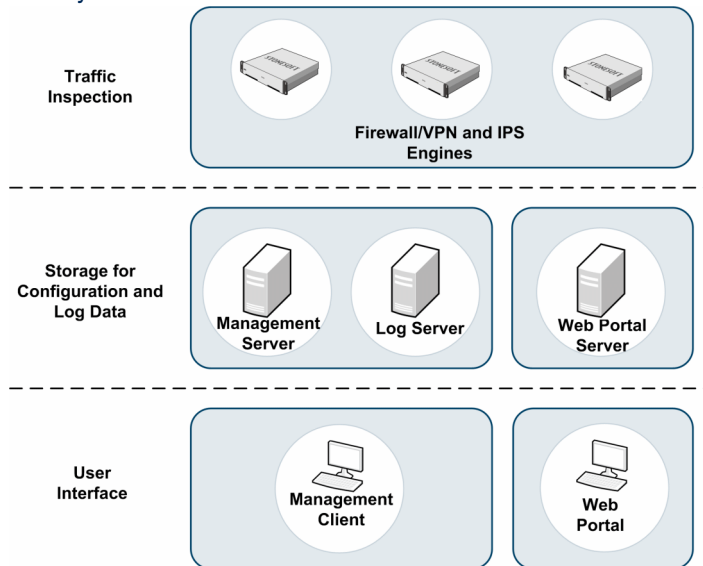
Technical Support

Evaluation support is available with the evaluation Proof of Licence (POL) at <https://my.stonesoft.com/support/supportrequest.do>.

Documentation for all StoneGate products is available for download at http://www.stonesoft.com/en/support/technical_support_and_documents/manuals/.

System Architecture

Illustration 1 StoneGate System Architecture



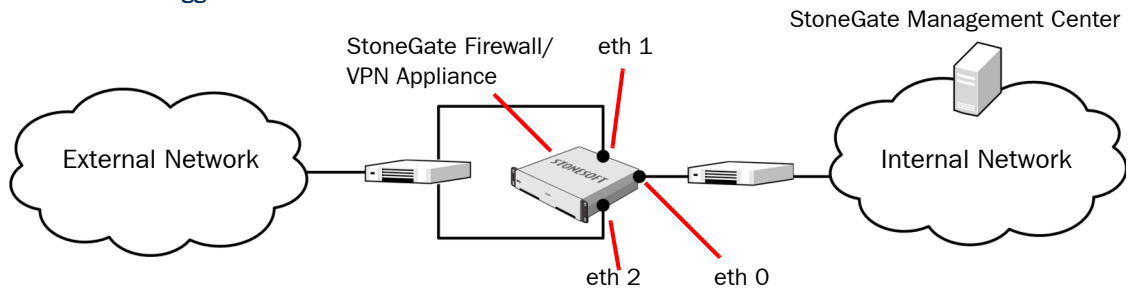
StoneGate is designed for centralized remote management. The Management Center consists of the following components:

- A Management Server, which stores and distributes configuration data.
- One or more Log Servers, which store logs and other monitoring information.
- One or more Management Clients, which administrators use to access the system.
- The optional Web Portal Server allows monitoring the system through a Web browser.

Suggested Evaluation Environment

The suggested evaluation environment, illustrated below, allows you to test most features.

Illustration 2 Suggested Network Environment



In the evaluation network environment, the StoneGate Firewall/VPN appliance is positioned between an internal network and an external network. The firewall has one internal interface that is used for the connection to the internal network and the control connection to the StoneGate Management Center installed on a standard server. There are two external interfaces for the two ISP connections, so that you can test the Multi-Link™ load-balancing and high availability features. In an evaluation configuration, both external interfaces can be connected to the same switch or router, but they must have IP addresses from different (sub)networks.

In this evaluation environment, all of the standard Management Center components are installed on the same physical server. In production use, the Management Center components are often distributed between separate machines.

Installation and Configuration

The steps in this guide provide an overview of a typical installation and configuration. More detailed installation instructions can be found in the *StoneGate Management Center Installation Guide* and the *StoneGate Firewall/VPN Installation Guide*. Further configuration instructions can be found in the *StoneGate Administrator's Guide* and in the Management Client's *Online Help*.

Installation Checklist

You will need the following for the installation:

- The StoneGate Firewall appliance (preinstalled software is included on all appliances).
- USB mass storage device for saving the firewall's initial configuration.
- Evaluation license file, saved in a location accessible from the computer where you are installing the Management Center. If you do not have the licenses, new evaluation licenses can be requested at http://www.stonesoft.com/en/support/evaluation_licenses/.
- StoneGate Management Center installation CD-ROM. If you do not have an installation CD-ROM, you can download the .iso image file from the Stonesoft Downloads page at <https://my.stonesoft.com/download> and create the installation CD-ROM yourself.
- A server for installing the Management Center (see system requirements on the next page).
- Networking equipment (switches, routers, cables, etc) to set up a small test network such as depicted in [Illustration 2](#) above.

System Requirements for the Management Center

You will need to install the Management Center on your own server hardware. We recommend hardware that meets the following requirements (see the *Release Notes* on the installation CD-ROM for more details):

- Processor: Intel Core family or higher, or equivalent on a non-Intel platform
- Memory: 4 GB RAM
- Disk space: 56 GB

StoneGate Management Center supports the following operating systems and versions:

- Microsoft Windows Server 2008 (32bit)*
- Microsoft Windows Vista SP1 (32bit)*
- Microsoft Windows 2003 SP1 or SP2 (32bit)*
- Microsoft Windows XP SP2 or SP3 (32bit) *
- CentOS 5 (for 32bit x86)
- Fedora 8 and 9 (for 32bit x86)
- Red Hat Enterprise Linux 4 and 5 (for 32bit x86)
- SuSe Linux Enterprise 11 (for 32bit x86)

*) Only the U.S. English language version has been tested, but other locales may work as well.

Installing the StoneGate Management Center

▼ To install the Management Center

1. Insert the StoneGate Management Center installation CD-ROM and run
`\StoneGate_SW_installer\Windows\setup.exe`
or
`/StoneGate_SW_Installer/Linux/setup.sh`
2. Proceed according to the Installation Wizard prompts and accept the default settings until you are prompted to select the installation type.
3. Select **Typical** installation. The Typical installation installs the Management Server, Log Server, and Management Client.
4. Proceed according to the Installation Wizard prompts until the installation is complete.

▼ To install licenses

1. Start the Management Client.
 - In Windows, use the shortcut icon in the location you selected during installation or run the script `<installation directory>/bin/sgClient.bat`.
 - In Linux, run the script `<installation directory>/bin/sgClient.sh`. A graphical environment is needed for the Management Client.
You are automatically prompted to install licenses.
2. Browse to and install all licenses.
3. Start the Log Server:
 - In Windows, use the shortcut icon in the location you selected during installation (default: **Start**→**Programs**→**StoneGate**→**Log Server**) or run the script `<installation directory>/bin/sgStartLogSrv.bat`.
 - In Linux, run the script `<installation directory>/bin/sgStartLogSrv.sh`.

Installing the Firewall

The engine configuration is generated in the Management Client and transferred to the engine. The interface definitions are automatically mapped to the engine's physical interfaces.

▼ To configure a new firewall

1. Right-click **Firewalls** in the left panel Status list and select **New**→**Single Firewall**.
2. **Name** the Firewall and select the **Log Server**.
3. Switch to the **Interfaces** tab.
4. Click **Add** and select **Physical Interface**. The Physical Interface Properties dialog opens with Interface ID 0 automatically selected. Define the following physical interfaces:
 - **Interface ID 0**: for the internal network and the control connection to the Management Server.
 - **Interface ID 1**: for the connection to ISP A.
 - **Interface ID 2**: for the connection to ISP B.
5. Right click each physical interface and select **New**→**IP Address** to enter the appropriate IP address for the interface. The ISP A and ISP B interfaces must have IP addresses from separate networks.
6. Click **OK** to save the changes. You are prompted to open the Routing view. Click **No**.

▼ To initialize the appliance

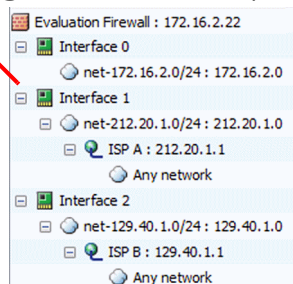
1. In the Management Client, right-click the Firewall and select **Save Initial Configuration**.
2. Select the engine time zone and keyboard layout, and save the initial configuration in the root directory of a USB mass storage device.
3. Connect the appliance's eth 0 interface to the switch or router for internal network. Use a crossover cable if connecting directly to a router.
 - If you have not already connected the computer where you installed the Management Center to this switch or router, connect it now.
4. Connect the appliance's eth 1 interface to the port on the external router used for the ISP A connection and the appliance's eth 2 interface to the port used for the ISP B connection. Use crossover cables if connecting directly to a router.
5. Insert the USB mass storage device in one of the USB ports on the appliance and power on the appliance. The appliance automatically reboots when the configuration is finished.

Configuring Routing and a Basic Policy

▼ To configure Multi-Link routing

1. Select **Configuration**→**Routing** from the menu to open the Routing view.

Expand the routing tree to view all the routing information for the interfaces



- Right-click **Network Elements** and select **New→Router** to define the IP address of the router for the ISP A connection. Repeat for ISP B. The ISP A and ISP B IP addresses must be from two separate networks.
- Right-click **Network Elements** and select **New→Network** to define elements for the networks for the ISP A and ISP B connections.
- Right-click the network under **Interface ID 1** and select **New→Static NetLink**.
- Configure the Static NetLink with the following properties:
 - **Gateway:** ISP A Router.
 - **Network:** ISP A Network.
- Click **OK** to close the NetLink properties. The new NetLink is added to the routing tree.
- Right-click the NetLink and select **New→Any Network** to create the default route.
- Repeat [Step 4-Step 7](#) for Interface ID 2 to configure the route for the ISP B connection.

▼ **Configuring Multi-Link load balancing**

- Right-Click **Network Elements** and select **New→Outbound Multi-Link**.
- Click **Add** and define a Multi-Link Member with the following properties:
 - **NetLink:** ISP A.
 - **Selected Range:** Enter the same IP address in both fields. This address must be from same network as the ISP A router. This is used for translating outbound connections.
- Repeat [Step 2](#) to add the ISP B NetLink, then click **OK** to close the Outbound Multi-Link Properties.

▼ **To define a basic policy**

- Select **Configuration→Configuration→Firewall** from the menu to open the Firewall Configuration view.
- Right-click **Firewall Policies** and select **New→Firewall Policy**.
- Select the **Default** template as the basis for the new policy.
- Double-click the green row and configure a new rule to allow IP addresses in the directly connected internal network to make connections:

Browse to **Network Elements→Networks**. Drag and drop the internal network here.

ID	Source	Destination	Service	Users	Action
14.1	net-192.168.1.0/24	ANY	ANY	N/A	Allow
Discard all					

Right-click and select **Set to ANY**.

Click and select **Allow**.

- Right-click the Access rule you just created and select **Copy Rule**.
- Switch to the **NAT Rules** tab, right-click the green row, and select **Paste**.
- Double-click the empty **NAT** cell in the rule and define the following NAT properties:
 - **Translation Type:** Dynamic.
 - **IP Address Pool:** Click **Select** and browse to **Network Elements→Traffic Handlers**. Select the Outbound Multi-Link element you created.
- Click the Save and Install toolbar icon.





▼ To command the engine online

1. Click the System Status icon to switch to the System Status view.
2. Right-click the Firewall and select **Commands**→**Go Online** to command the engine online.
3. Check the status of the Firewall and SMC on the **Status** tab.
 - The icons should be green, indicating that the Firewall and SMC servers are online.
4. Select the Firewall to view detailed status information the **Info** panel.
5. Switch to the **Connectivity** tab and verify that there is connectivity between the Firewall and the Management Server, and between the Firewall and the Log Server.

Feature Overview

This section outlines the main features of StoneGate Firewall/VPN and StoneGate Management Center. Background information can be found in the *StoneGate Management Center Reference Guide* and the *StoneGate Firewall/VPN Reference Guide*.

StoneGate Management Center Highlights

Centralized Management

A centralized point for managing all firewall, IPS, and VPN components simplifies system administration significantly and allows combining information from different sources without having to integrate the components with an external system. StoneGate has been designed from the start to be centrally managed.

The main centralized management features in StoneGate include the following:

- Sharing of configuration data in different configurations eliminates the need for duplicate work, which reduces the complexity of configurations and the amount of work required for making changes.
- Remote upgrades can be downloaded and pushed automatically to several components. A single remote upgrade operation updates all necessary details on the security engines, including operating system patches and updates.
- The integrated backup feature allows saving all system configurations stored on the Management Server in one manually or automatically run backup.
- Central access point for administrators with centralized access control. Several administrators can be logged in at the same time and simultaneously make changes to the system. Conflicting changes are automatically prevented. Administrator privileges can be easily adjusted in a highly granular way.

Centralized Monitoring and Reporting

Centralized system status monitoring provides an easy way to monitor a large number of components. The StoneGate Management Center provides operating, connectivity, and hardware status information, as well as highly customizable tools for viewing, combining, and processing log information from multiple sources. New in StoneGate Management Center 5.0, the Management Center can monitor the status of any third-party components through various alternative methods, and can now also receive any logs in the syslog format for centralized handling with the built-in tools.

Customizable Overviews can contain information on the system's status, shortcuts to frequently used views, and real-time statistical charts on the system's operation and the traffic flow.

Reports correlate and visualize specific information from large amounts of data into easy-to-read formats to provide an overview of what is happening in the network.

With the launch of StoneGate 5.0, StoneGate now offers geographic pinpointing of IP addresses in logs to show where the source and destination of the traffic are located. Geolocation diagrams can be viewed on a world map in Reports, Statistics, and Overviews.

Support for Large-Scale Installations

The StoneGate Security Platform has been designed to be very scalable and flexible. The StoneGate Management Center has the ability to scale from managing a few security devices to the highly available management of a large enterprise with hundreds of devices.

With the introduction of StoneGate 5.0, Managed Security Service Providers (MSSPs) can separate customer environments into isolated Domains. Domains also allow large enterprises to separate different business units or divisions into their own Domains. To a restricted administrator, working inside a Domain is like managing a separate system, but an administrator who has cross-domain access enjoys the full benefits of centralized management. This unique architecture simplifies environments, makes them easier to maintain, and sets up logical boundaries for administrator access control.

Role-Based Access Control

StoneGate provides flexible role-based administrator access control, which makes it possible to define administrator access rights in fine detail according to the administrator's duties. In addition to defining one or more roles for the administrator, it is also possible to restrict the components to which each role applies.

StoneGate Management Center High Availability

Secondary Management Servers and Log Servers can optionally be installed as backups that can be activated if the active components become unavailable. The high availability solution includes automatic replication of the configuration data stored on the Management Server. This way, manual intervention is kept at a minimum and the system can be fully managed and monitored without going through a manual re-installation and backup restoration process.

Web Portal Server

StoneGate 5.0 also introduced browser-based access to policies, logs and reports anytime, anywhere. The Web Portal Server provides secure, device-independent access for viewing logs, reports, and traffic inspection rules. This is particularly useful for MSSPs for providing customers information about their system. End-users access the information through a standard Web browser without having to install any additional software.

StoneGate Firewall/VPN Highlights

Firewall Clustering

Uniquely, up to 16 StoneGate Firewall/VPN engines can be clustered to provide an unmatched level of high availability and performance needed for today's critical networks. Clustered firewall nodes function as a single, virtual entity. The functioning of the nodes is synchronized, and cluster nodes re-distribute traffic from nodes that become unavailable. The performance of each added node contributes to the total throughput. New firewall nodes can be added flexibly as traffic volumes grow, enhancing the load balancing of traffic.

Multi-Link

Stonesoft's patented Multi-Link technology makes it possible to distribute outbound traffic between two or more Internet connections to provide high availability and load balancing. With the StoneGate Firewall/VPN, Multi-Link is a built-in, and requires no special ISP arrangements or configuration of specialized hardware or software. Multi-Link supports many types of Internet links, such as ISDN, xDSL, leased lines, modem, and satellite connections. Different types of links can be used together. Multi-Link makes it possible to:

- Balance outbound traffic between two or more network links. With each new outbound connection, the firewall selects the fastest route for the connection. Balancing traffic between multiple affordable Internet connections is significantly more affordable than expensive alternatives like MPLS, BGP, or Frame Relay.
- Ensure that outbound network connectivity remains available even if network links fail. If a network link fails, the firewall detects this and directs connections through available links completely automatically.
- Use network links in standby mode so that they are only activated if all the primary network links fail. Using standby network links provides high availability of Internet connectivity, but is less expensive than having multiple network links active at the same time.

Inbound Traffic Management

The StoneGate Firewall/VPN includes built-in server load balancing for the servers a firewall is protecting. Inbound traffic balancing can:

- Balance incoming traffic between several servers to even out their workload.
- Monitor the server's status so that the traffic is not directed to unavailable or overloaded servers.

Quality of Service

The Quality of Service (QoS) features make it possible to manage bandwidth and prioritize connections on the firewall. The bandwidth management features make it possible to set a limit, a guarantee or both for any given type of outbound traffic.

Traffic prioritization is used either independently or in addition to bandwidth management to ensure quick delivery of time-critical communications, such as streaming audio or video. StoneGate has its own internal traffic prioritization scheme, but StoneGate can also read and write DiffServ Code Point (DSCP) markers (type of service (ToS) fields).

Deep Packet Inspection

Deep packet inspection uses detailed protocol analysis and fingerprinting to check whether traffic contains a malicious pattern. Additionally, the StoneGate IPS components can complement the StoneGate Firewall/VPN inspection and command the firewall to block traffic based on real-time IPS traffic analysis.

Antivirus

A virus scanner is available. The virus scanner can inspect HTTP, HTTPS, IMAP, POP3, and SMTP protocol traffic.

SSL Inspection

StoneGate version 5.0 introduced SSL/TLS inspection capabilities in the Firewall/VPN and IPS products. StoneGate can decrypt and re-encrypt HTTPS traffic so that it can be inspected in the same way as plain HTTP traffic. The HTTPS Inspection feature covers both server protection to inspect incoming HTTPS connections to protected servers, and client protection to inspect outgoing HTTPS connections initiated by internal users.

CIS Redirection

The StoneGate Firewall/VPN can be set up to redirect traffic to an external content inspection server (CIS). Using an external CIS expands the capabilities of the firewall with virtually any type of content screening.

Customizable User Responses

User Responses define custom responses that are sent when a connection is not allowed to continue. User Responses differentiate cases where a connection was blocked from cases where a technical problem prevented the connection from going through.

Assisted Routing and Anti-Spoofing

Routes to directly connected networks are configured automatically based on the IP addresses of the firewall's network interfaces. Other routes can be added manually. Automatic anti-spoofing defines which addresses are allowed for each interface and enforces correct traffic direction. For example, a packet with a legitimate internal address sent to a firewall's external interface would be automatically blocked by anti-spoofing.

Efficient Rule Organization

The StoneGate Firewall/VPN rules can be organized efficiently with hierarchical Firewall Policies. Template Policies and Sub-Policies can be used to make it easier to read the rules and to assign editing rights to administrators.

Template Policies contain rules that are inherited into any template or policy below it in the policy hierarchy. All firewall policies are based on the ready-made Default Template Policy or a copy of it. Templates reduce the need for creating the same or similar rule in several policies, and reduce the likelihood of mistakes affecting important communications.

Firewall Sub-Policies are sections of Access rules that can be inserted into Policies, Template Policies, and even other Sub-Policies to make the engine process traffic more efficiently.

Additionally, Aliases can be used at all levels of the policy hierarchy to add variable values to the rules. The Aliases are assigned a different value for each firewall, which allows the administrators to install the same rules on different firewalls. There is no need to create several separately managed rule sets for similar installations.

Policy Tools

The same policy can be installed on several security engines at the same time. Fail-safe policy installation with automatic rollback prevents policies that prevent management connections from being installed. A policy snapshot is created each time a policy is uploaded to the engine.

The policy validation tool runs various types of validation checks, including, for example, searches for duplicate rules and rules that can never match traffic. StoneGate 5.0 further assists administrators with a rule counter tool that helps detect obsolete rules and optimize rule order to enhance network and security performance.

In addition, rules can be created directly from logs for faster incident management.

IPsec VPN

VPNs in StoneGate Firewall/VPN are implemented according to the IPsec standard. In StoneGate, there are two main types of VPNs:

- A VPN between two or more gateway devices that provide VPN access to several hosts in their internal networks.
- A VPN between a gateway device at a site and a VPN client running on an individual computer, such as the laptop of a travelling user, or a desktop PC at a home office.

Clustering and Multi-Link provide load balancing between nodes and networks links, as well as the possibility to recover connections lost due to node or network link failure.

StoneGate Guides

Administrator's Guides - step-by-step instructions for configuring and managing the system.

Installation Guides - step-by-step instructions for installing and upgrading the system.

Reference Guides - system and feature descriptions with overviews to configuration tasks.

User's Guides - step-by-step instructions for end-users.

For more documentation, visit
www.stonesoft.com/support/

Stonesoft Corporation

Itälahdenkatu 22 A
FI-00210 Helsinki
Finland

Tel. +358 9 476 711
Fax +358 9 4767 1234

STONESOFT

Secure Information Flow

Stonesoft Inc.

1050 Crown Pointe Parkway
Suite 900
Atlanta, GA 30338
USA

Tel. +1 770 668 1125
Fax +1 770 668 1131