StoneGate ™

永不间断,安全均衡

StoneGate 安全方案白皮书

(防火墙/VPN/负载均衡/IPS 产品)

CONTENT

一， 序言

在任何一个网络方案当中，防火墙始终是最关键的组成部分，企业一方面访问 INTERNET，得到 INTERNET 所带来的好处，另一方面，却不希望外部用户去访问企业的内部数据库和网络。企业当然没有办法去建立两套网络来满足这种需求。防火墙的基本思想不是对每台主机系统进行保护，而是让所有对系统的访问通过某一点，并且保护这一点，并尽可能地对受保护的内部网和不可信任的外界网络之间建立一道屏障，它可以实施比较惯犯的安全政策来控制信息流，防止不可预料的潜在的入侵破坏。

随着 internet 的飞速发展，以 Internet 为代表的全球性信息化浪潮日益深刻，相应的应用领域从传统的、小型业务系统逐渐向大型、关键业务系统扩展，这就对我们的网络环境提出了更高的要求。面对那些的大型的、关键的业务，除了保证应用的安全之外，业务的高可用性也同样重要。因此，新一代的防火墙必须在保证高度安全的前提下，对应用的连续可用提供保护。

StoneGate 防火墙就是这样的一款防火墙。作为全球知名的安全方案提供商，Stonesoft 公司推出的新一代的防火墙专注与网络的高安全性与高可用性，为企业的应用提供连续的、周到的保护。

二, 关於 Stonesoft 公司

STONESOFT
Real World Business Security™

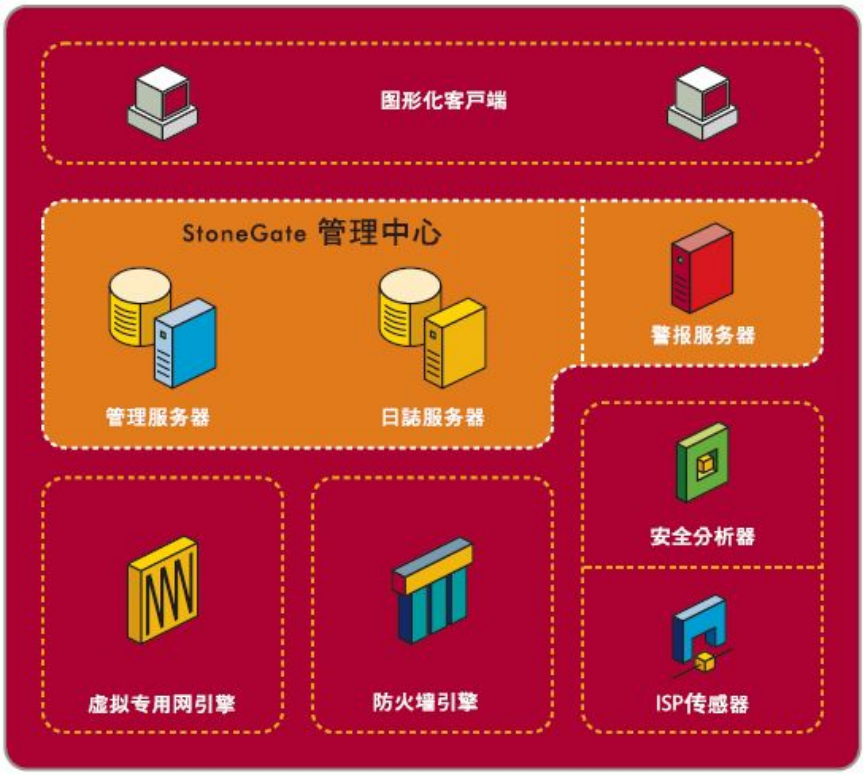
Stonesoft 公司 (HEX: SFT1V) 是一家全球性的公司，她专注于企业级的网络防护和商务连续保证。她自有的 StoneGate(tm) 安全平台整合了防火墙、VPN 和 IPS，给苛刻的商务应用提供了有效灵活的防护。 StoneGate 内置了荣获大奖的采用了负载平衡技术的 StoneBeat

Stonesoft 的产品的构想是构建能互操作的产品，这些产品通过分布式的安全策略的执行，具有集中的管理、有效的分层防护或者深层防护。 这些工具在解决真实的问题是必须要的，这些问题是目前我们的客户在企业网络中所能遇见的。 Stonesoft 提供在那些创建网络的解决方案中必须产品，而这些创建好的网络是安全、有效、可管理和可升级的.

Stonesoft 的全球总部在芬兰的赫尔辛基；美洲总部在美国佐治亚州的亚特兰大；亚太地区总部在新加坡。 Stonesoft 在美洲设有许多办事处，包括墨西哥和巴西。她在欧洲的英国、德国、法国、意大利、荷兰和西班牙都设有办事处。 Stonesoft 在全球拥有超过 250 名员工.

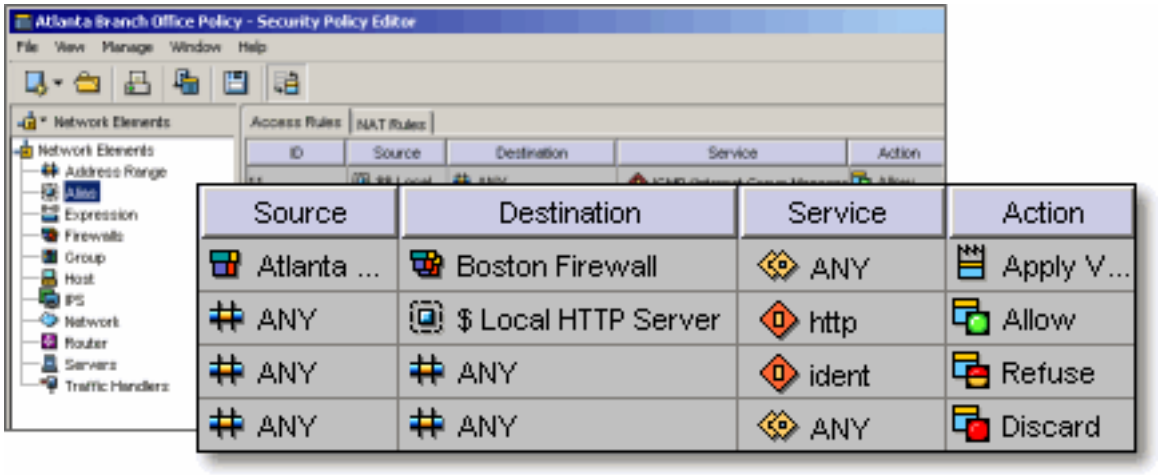
三， STONEGATE 管理中心 (SMC)

为确保较高的安全水准，当前的安全架构通常需要由一小群专业安全人员进行集中化管理，而安全解决方案却需于分布式的杯境下进行部署，但仍需由同一群人进行管理，升级及维护． StoneGate 解决方案提供相应的管理系统，可以一个集中一地点对成千上万的安全执行管理及维护，同时亦允许一定程度的本地管理. StoneGate 架构可对整体安全架构进行管理，包括操作系统级的配置及以某单一地点进行远程软体升级. 该功能可降低管理成本，并可改善整套解决方案的总体拥有成本 (TCO)



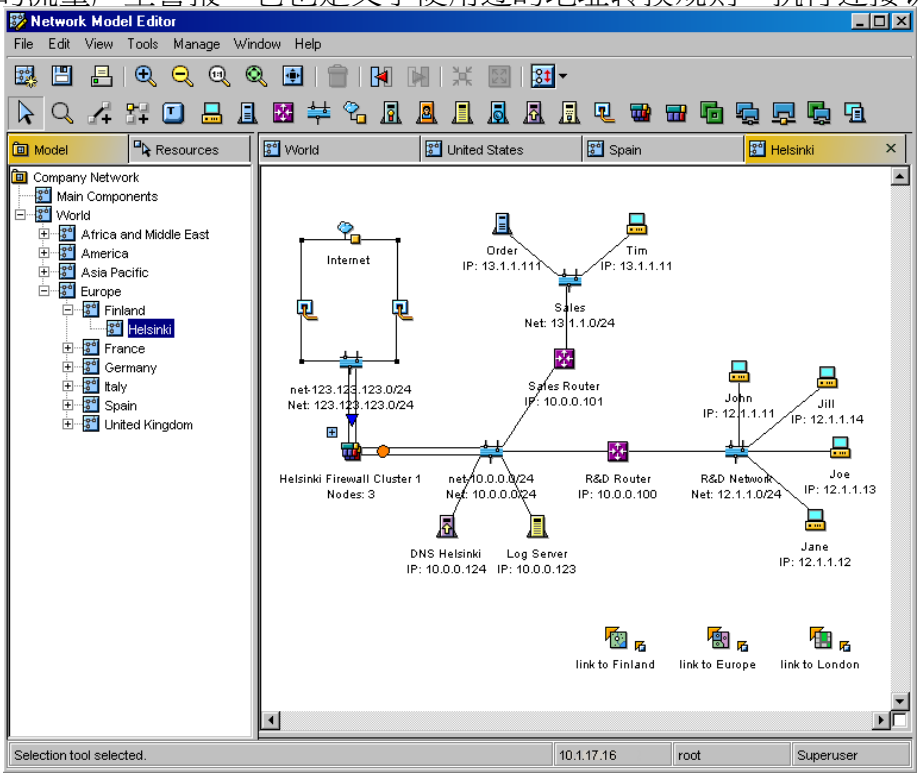
StoneGate 管理中心 (SMC) 可管理所有 StoneGate 防火墙/虚拟专用网, StoneGate IPS (入侵检测及分析) 产品. 以下讲解 StoneGate 管理中心的产品亮点.

◆ 3.1.1 安全策略



防火墙安全策略的主要功能就是实施访问控制规则・在 StoneGate 中，访问控制的主要原则可以表达为“只要没有经过允许都是被禁止的”。 访问控制规则以外，一个防火墙安全策略定义了何种

流量类型登录和基于何种类型的流量产生警报。它也定义了使用过的地址转换规则，执行连接认证，和设定 VPN 是如何使用的



◆ 3.1.2 网络层编辑

管理员们经常需要更新的关于他们网络配置的文档． 然而，任何使用第三方图表工具生成的图表必须经常手工更新，意味着网络图表总是过时的。并且，一旦图表完成后，系统仍然需要配置，需要重复工作。

StoneGate 管理中心包含了一个集成的图表化您的网络配置的工具。并且，当你描绘您的网络时，你能同时创建在安全引擎中必须的网络元素。

网络层编辑器使用跟在管理中心的相同的网络元素，意味着改变立刻在任何地方有效．没有重复的修改工作， 你所有的网络/安全架构文档都是最新的。

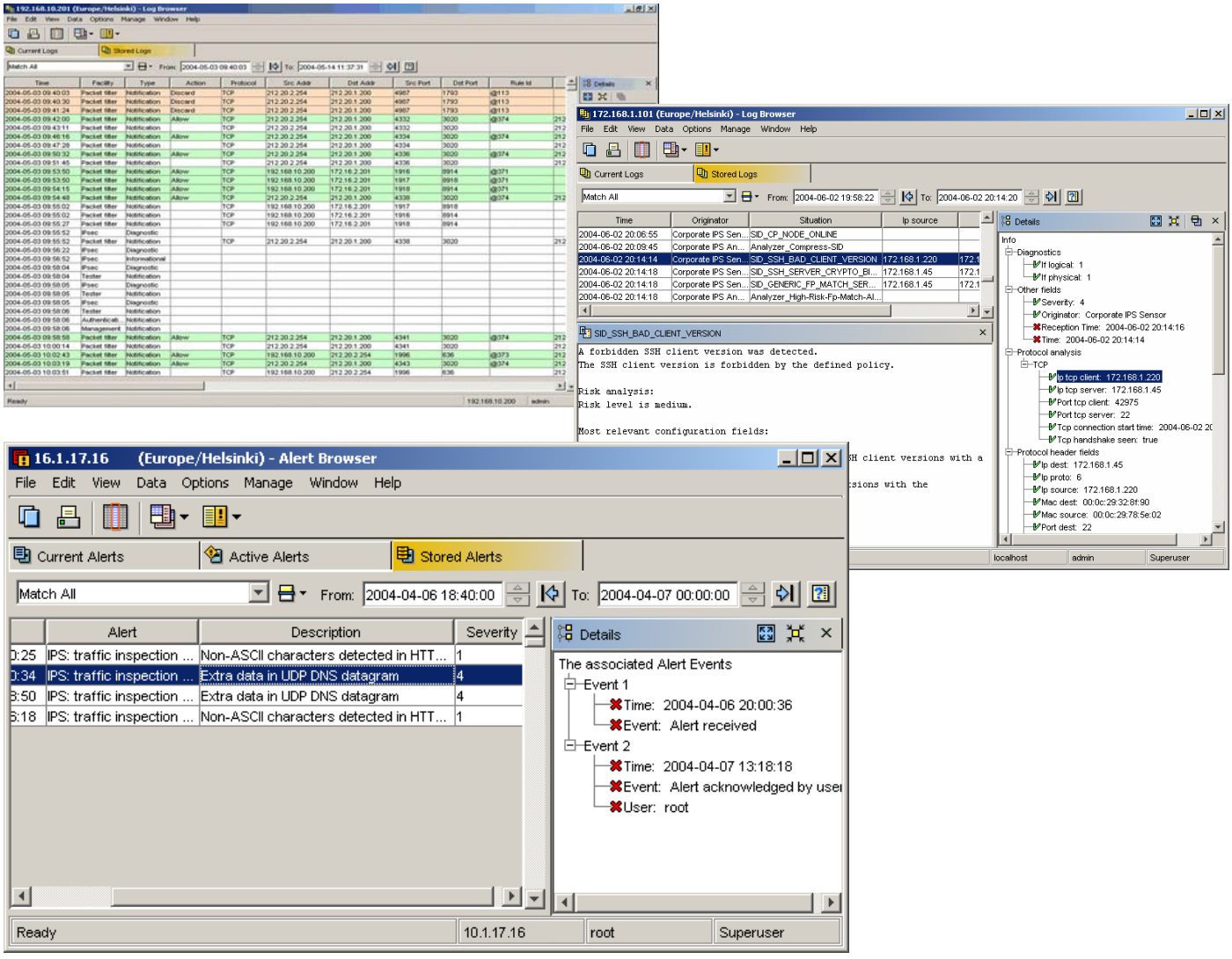
这个工具也通过自动从选定的网络元素创建一个新图表帮助您记录您的现有的配置。

◆ 3.1.3 日志与监控, 警报系统

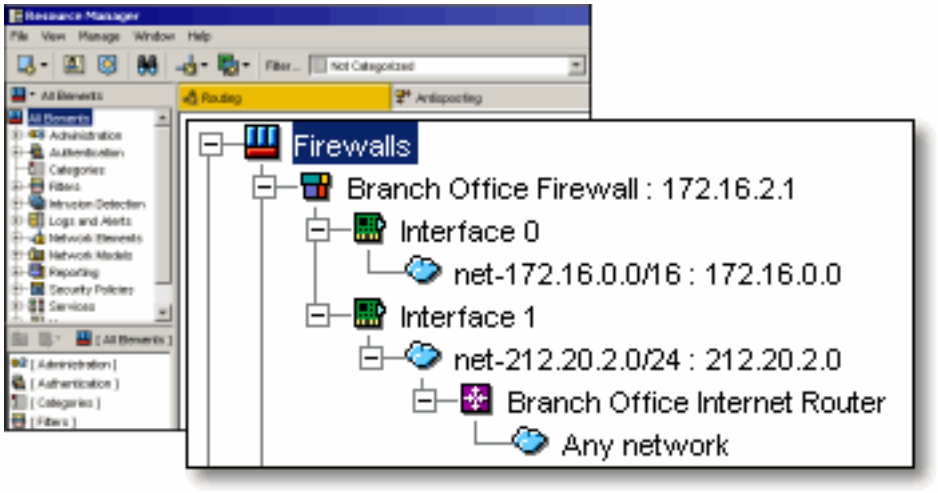
分析日志与监控网络状态是网络管理员的一项重要工作，通过防火墙的监控系统，网络管理员可以分析网络流量习性、吞吐量、防火墙负载以及防火墙的健康状况。StoneGate 日志监控系统是一个非常强大的系统，并且有着非常有好的界面。在 StoneGate GUI 的主面板上，网络管理员可以适时的监视防火墙的每一个节点的状态、负载状况、历史负载曲线图以及当前活动的连接。

如果网络环境当中出现故障，日志系统将会产生故障报警，同样它也将记下来自黑客的攻击记录，以便于日后进行分析。StoneGate 应用专门的数据库来存储、调用日志信息，这样它的访问速度将比一般基于文件的日志系统更快。StoneGate 的日志系统包含所有专门的日志特点，例如日志存档、日志调用、日志删除以及自定义日志安排。

StoneGate 亦可透过内置的警报系统, 把警报透过电邮(SMTP), 短诉(SMS), SNMP, SYSLOG 发送到指定的管理员, 使之可第一时间知道防火墙状态.



◆ 3.1.4 路由和反欺骗



StoneGate 网关的路由通过使用 StoneGate 管理中心的图形化用户接口配置。管理员能使用跟路由配置相同的网络元素在所有的配置中。一个集群网关的路由一次配好，并不单独针对对集群中的元素，因此无需在网关中使用操作系统的命令行工具。

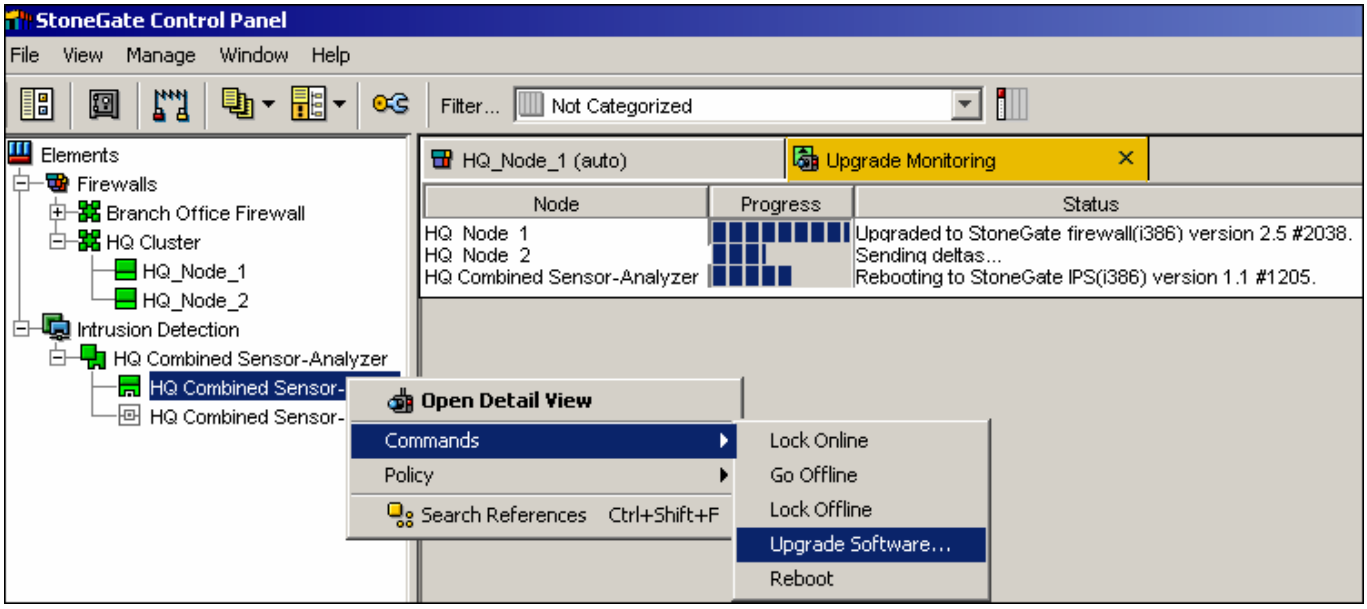
反欺骗规则自动从路由配置中生成和更新。在大多数情况下，无需接触到反欺骗，但是你可以在需要的时候编辑生成的规则。

◆ 3.1.5 中央资源和数据库

组件重用: 作为统一管理的一部分，元件数据库在各个受管理组件和所有工具间共享。这意味着一个元件一旦被创建以后，将在统一管理中所有地方可用。更新一个元件将会更新所有的使用元件的配置，并且将会是用更少的管理员工作和更少的人工错误。

所有的配置信息，包括安全策略、集群、路由、多链路和操作系统都被配置和存储在中央资源库中。这使得对整个系统的单个备份变得可能。当安装在一个安全引擎上的硬件失效时所有您需要做的就是进行软件安装和配置重置和激活。

◆ 3.1.6 远程更新



快速, 可靠, 透明

升级您的网络架构的基础部分将是困难和费时的。StoneGate 的远程更新降低了负担：无须离开您的办公室，整个过程是快速、简单和可信的。

逐步升级

StoneGate 是一个集成的软件包，送到您手上的是全部的集成软件，并且已经经过测试。没有单独的操作系统，没有任何补丁需要执行。仅仅需要简单的下载升级镜像文件，然后通过管理界面把它发送到远程安全引擎。配置信息在升级过程中得到保留，因此您的 StoneGate 安全引擎将在升级完成后立刻恢复到运行状态。

失效保护的可信度

您的 StoneGate 安全引擎载下载升级镜像时保持运行。一旦升级镜像传输，并且完整性得到确认，远程引擎将会重新启动以使升级生效。如果远程引擎不能重新启动，那么升级过程将会回滚。这个机制意味着升级要么成功要么温和得回滚。

透明

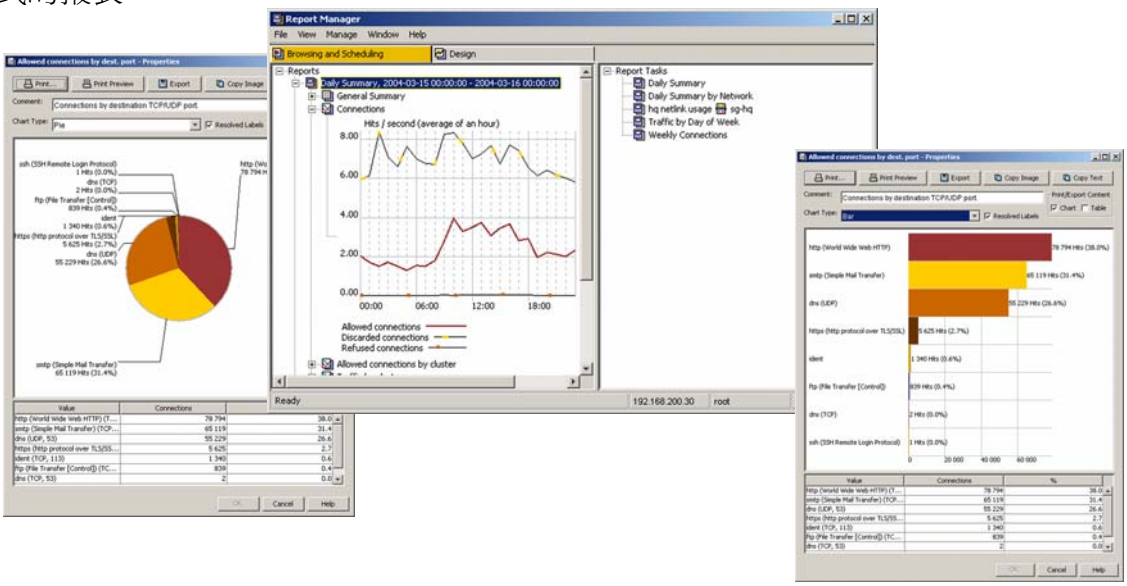
因为 StoneGate 包括了内置的高可用性集群，更新能够通过对用户毫无影响而完成。集群节点一次更新一个，当节点更新重新启动时，剩下的节点自动透明的接过工作。服务保持连续性而无需损失连接。

无需为安全引擎做备份

因为配置信息保存在中央管理系统中，所以无须备份单个的 StoneGate 安全引擎。中央化的备份系统处理了整个安全系统的配置信息。

◆ 3.1.7 报表工具

StoneGate 提供了一个报告工具，它能够概括和可视化系统事件数据以便发现网络使用中的趋势和异常。它有大量的定制化和过滤特性， 因此使它成为研究和记录特定的事件和模式的强力帮助。拥有它你能够：仅仅需要点击几次鼠标就从日志数据中生成图表，并且生成自动化、分布式和多种格式的报表。

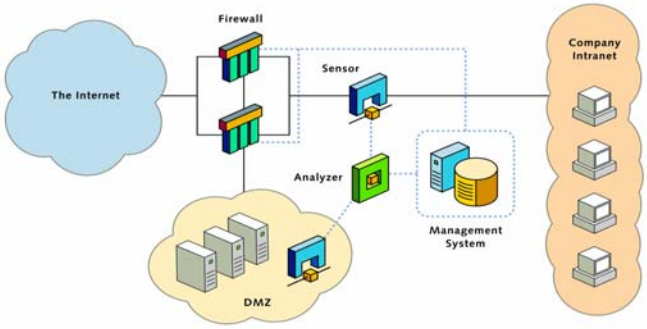


四， STONEGATE 高可用防火墙/VPN 介绍

4.1 基本的防火墙特性

◆4.1.1 访问控制

通过在 SoneGate 上设置相应的访问策略，可以根据网络 IP 地址、用户、服务类型、访问时间等参数对网络流量进行严格的控制。StoneGate 依靠其先进的、多级别的访问规则体系，能够适应任何的复杂的网络环境。同时，网络管理员根据自身网络的实际特点可以对每一个访问规则进行水平或垂直的进行扩展，建立一个新的相关的访问策略。



◆4.1.2 身份验证

防火墙作为外界用户进入企业内部资源的第一道关口，对用户进行认证和授权也将在这里开始实施。SoneGate 内置一个完整的通用的用户管理服务器——LDAP 服务器，可以轻松的实现对用户的管理。同时 SoneGate 也支持外接专门的 LDAP 目录服务器，如果用户本身有自己的 LDAP 目录服务器，SoneGate 将灵活的变成该目录服务器的客户端，便于用户进行统一的管理。

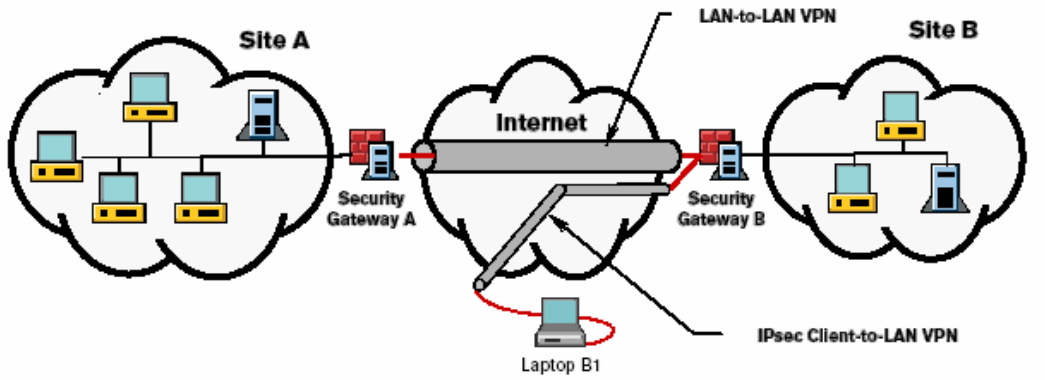
对于那些更为复杂的认证方式，SoneGate 能够全面的支持第三方的认证产品，例如 RADIUS 和 TACTAS+ 等后台协议。SoneGate 可以协同任何第三方的认证产品对用户进行认证授权。

那些经常出差或者是经常在家里通过终端连到企业内部网络访问企业资源的公司员工，如何对他们进行认证呢？为了确保这类移动的用户的认证及数据安全，SoneGate VPN 客户端将对他们进行认证并且通过加密技术建立数据隧道。SoneGate VPN 客户端支持各种连接方式，例如 T-1、xDSL、 Dialup、 ISDN 等等。

◆4.1.3 虚拟专用网 VPN

虚拟专网（VPN）技术是指在公共网络中建立专用网络，数据通过安全的“加密管道”在公共网络中传播。企业只需要租用本地的数据专线，连接上本地的公众信息网，各地的机构就可以互相传递信息；同时，企业还可以利用公众信息网的拨号接入设备，让自己的用户拨号到公众信息网上，就可以连接进入企业网中。使用 VPN 有节省成本、提供远程访问、扩展性强、便于管理和实现全面控制等好处，是目前和今后企业网络发展的趋势。

StoneGate VPN 支持 site to site (两个 LAN 之间)和 client to site（远程用户与 LAN 之间）两种方式。StoneGate VPN 体系遵循 IPSEC 安全构架，这样他能够同其他的任何的 VPN 网关协同操作，包括 CheckPoint VPN、CISCO PIX 等等。



◆4.1.4 网络地址转换 NAT

网络地址转换（Network Address Translation）是防火墙当中最常用的一种技术。它有一些显而易见的好处：

- 隐藏网络拓扑信息 ： 通过 NAT 转换的内部企业网，外面的用户将不能知道网络的真实结构。
- 节省紧张的网络 IP 资源 ： 通过使用 NAT，你可以使你的用户通过私人的 IP 地址去访问 INTERNET。

StoneGate 提供静态和动态两种 NAT 服务，并且源地址和目的地址只需在一条 NAT 规则里就可以进行转化。同时，通过 StoneGate 特有的网络管理工具，网络管理员在轻松简单进行 NAT 配置，减少了管理员的工作量。首先，被转换的 IP 地址的 ARP 条目是被 StoneGate 防火墙自动的加上去的；其次，被转换的 IP 地址的相关路由信息也将被 StoneGate 防火墙根据 NAT 规则自动处理。

◆ 4.1.5 内容检测

内容检测可以分为病毒检测和内容过滤两大类，防火墙作为企业内部网的第一道关口，应该为整个被保护的内部网络提供第一道病毒防护及非法内容的过滤检测。

对于 StoneGate 防火墙，将通过协议代理（Protocol agent）来实现这一点。你可以将你要检测的服务重定向到一个第三方的病毒或者是内容检测服务器上，例如趋势公司的 Viruswall 等等；同样也可以通过协议代理应用编程接口来自定义一个基于病毒及内容检测的安全方案。

4.2 STONEGATE 关键特性

◆ 4.2.1 第四代的防火墙——StoneGate 多层检测体系

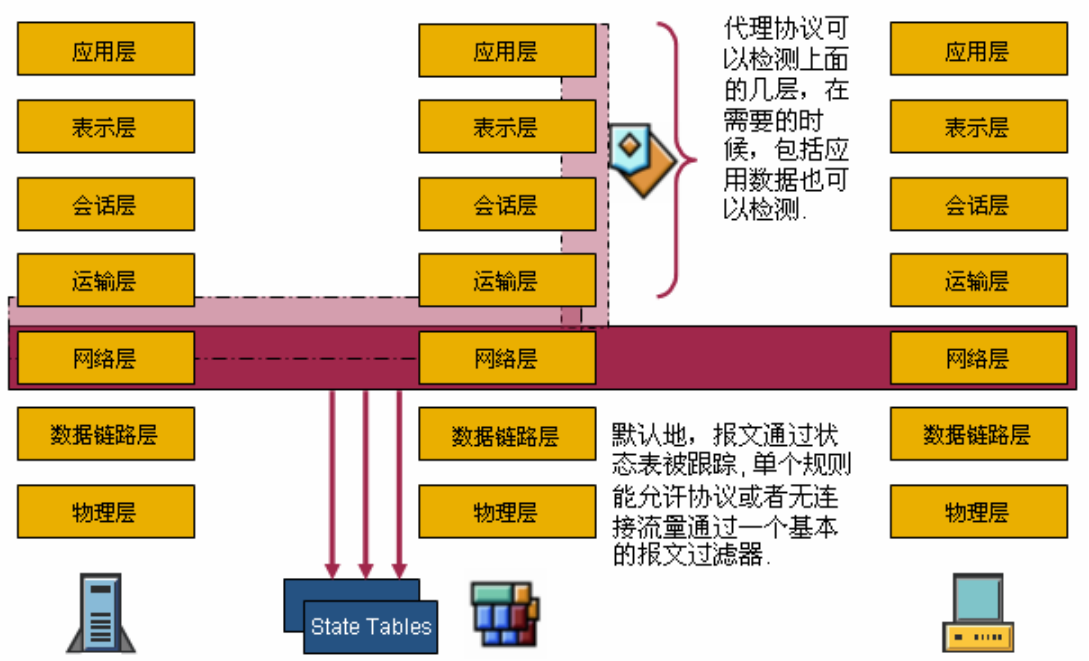
防火墙的工作原理是以 TCP/IP OSI 七层结构为基础的，在防火墙发展到今天，已经有了三种类型的防火墙技术，分别是包过滤、代理及状态检测。StoneGate 在以上三种防火墙技术的基础上，提出了第四代的防火墙——多层检测即应用层的防火墙。

StoneGate 多层检测技术充分吸收了代理防火墙技术和状态将测防火墙技术的优点，从网络层到应用层，多层检测技术都将提供安全检测，尤其是在应用层。

在 StoneGate 的网络层，存在一个状态检测引擎，它将依照设定好了的连接标签和访问规则对数据包进行全面的检查。

从网络层向上直到应用层，在每一层里都相应的有一个已知的协议代理，他们处理每一层的数据包并且根据你定义在每一层的协议规范来作出相应的动作，例如拒绝、允许或者是重定向等等。

当一个数据包到达防火墙的时候，位于网络层里的防火墙引擎将首先依照连接标签和访问规则对该数据报进行检查，当它发现该数据报需要应用层进行处理的时候，数据包将被从网络层转移到应用层，一旦协议代理与这种类型的连接（或协议）建立起密切的联系，所有其它的该类型的流量都将直接被协议代理所控制，协议代理将直接从网络层对数据报进行检测，相关的网络流将不用再一次通过网络层的防火墙引擎。很明显，协议代理实现了应用级的安全控制却并没有牺牲整个网络的性能。



4.2.2 STONEGATE——保证网络的高可用性

为什么需要网络的高可用

IDC 统计显示，导致基于互联网的商业应用停工器的因素主要分布在四个范围：网络、服务器、操作系统和应用本身。对于网络来说，最经常的情况是 ISP 连接出现故障和局域网本身负载过重而瘫痪，导致相应的资源不可访问；在服务器级别里，通常是 CPU 超负荷工作或者是网卡出现故障；对于操作系统来说，系统崩溃是最常见的现象；而数据库的低性能和进程的挂起是应用级别里最可能发生的故障。另外，导致应用出现停工期的另一重要原因是对系统的维护，大部分行业的用户都尽量选择在周末对系统的软硬件精心升级。

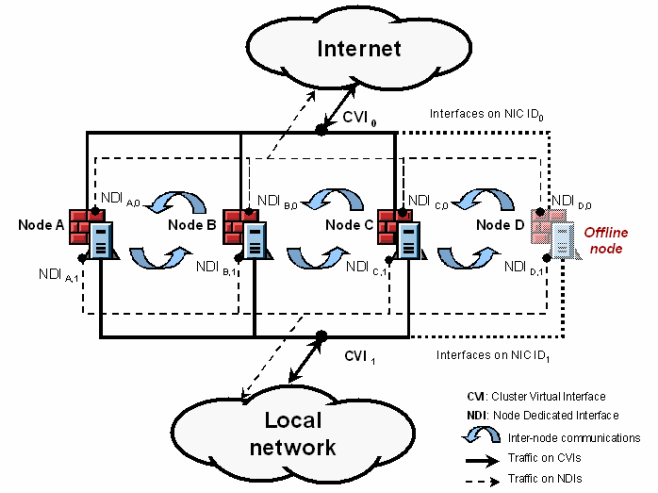
STONEGATE 怎样确保高可用

◆ 防火墙集群 

防火墙集群技术能够在防火墙上实现负载均衡和故障冗余。通过负载均衡和故障冗余，防火墙集群提供更高的伸缩性并且能够对防火墙进行在线的维护。

StoneGate 在集群的各个节点之间进行负载均衡以提高整个防火墙的吞吐量，负载均衡对于用户来说是完全透明的。StoneGate 多节点集群同样提供故障冗余：如果有一个节点发生故障，集群中的

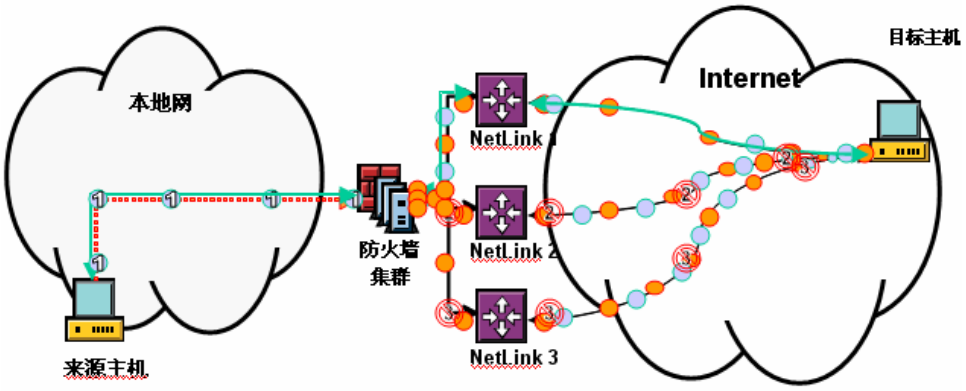
其它节点将自动的接管发生故障的那一个节点的应用任务，不需要管理员对其进行任何的干预；集群技术可以使用户随时添加一个新的防火墙节点到防火墙集群当中，以用来增强防火墙的性能；它同样也支持对防火墙进行在线维护：可以在任意时刻（包括正常运营时间）将一个或几个节点从集群当中分离（Offline）出来，以对其进行一些包括软件、硬件之类的升级或维护工作，而不影响其业务的应用。



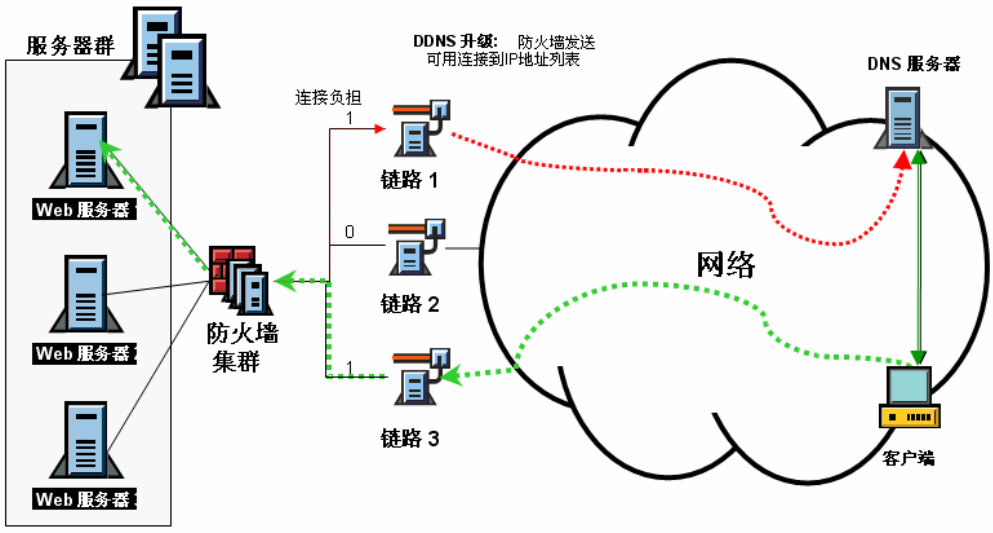
◆ 4.2.3 Multi-link 技术

StoneGate Multi-link 技术使得单个的防火墙集群可以连接到多个 ISP(网络服务提供商)上，这样，StoneGate 将在与之相连的多个 ISP 之间提供负载均衡和故障冗余，消除了在连接到一个 ISP 的时候因 ISP 不可用而导致的单点故障。在 VPN（虚拟专用网）的情况下，StoneGate 同样也支持多条并行的专线连接到互联网上，并且在这些并行的专线之间进行负载均衡和故障冗余。

对于从企业内部网到外面的互联网的数据包（outbound traffic），它总是选取最短的路由线路来到达目的地，在连有多个 ISP 的 StoneGate 集群体系里面，将通过路由负载均衡（Load Balanced Routing）来解决这个问题，当数据包到达防火墙的时候，路由负载均衡将为每一个数据包选择一条最优的路由线路，这样也大大增强了整个网络的性能。

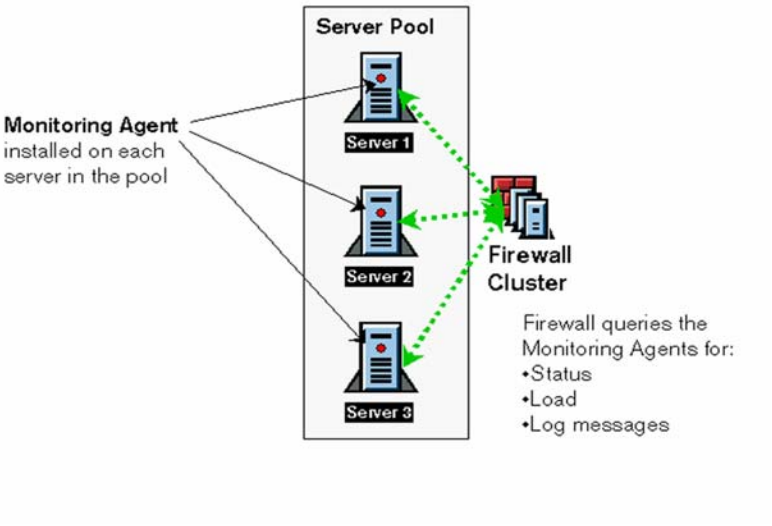


对于从互联网到达企业内部网的数据包（inbound traffic），远程客户端将通过动态的 DNS 来找出目前最合适的 ISP 连接，将数据包发到相应的内部网上。



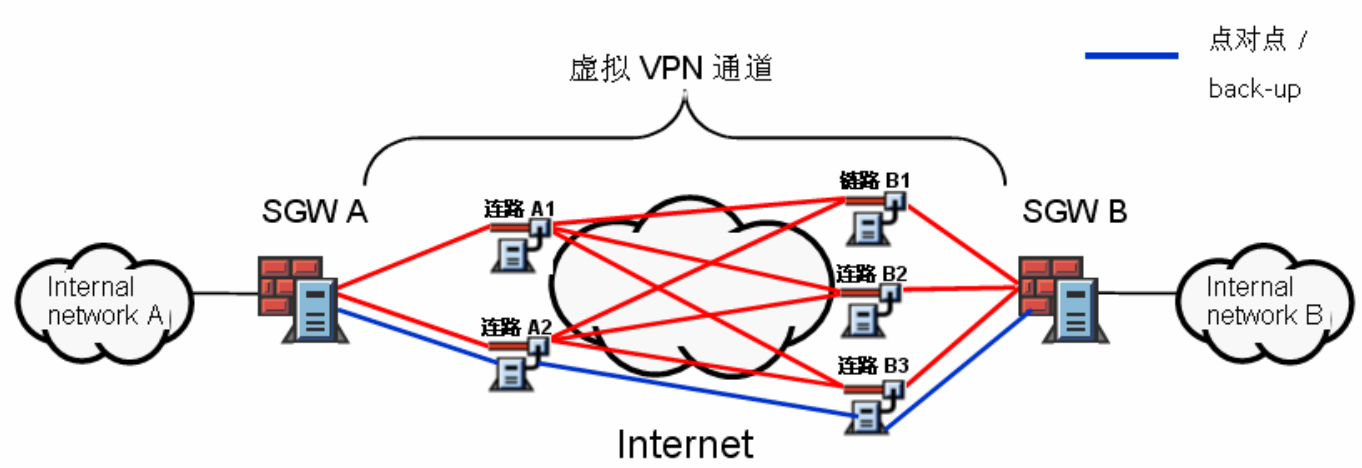
◆ 4.2.4 服务器群负载分配

StoneGate 会对一组服务器进行负载分配, 它可以透过 ICMP 或代理跟踪来进行服务器可以性评估及分配



◆ 4.2.5 多链路虚拟专用网 (VPN)

对于多个 ISP 情况下的 VPN 连接，StoneGate 通过在每一个 ISP 上建立一个 VPN 连接，然后将这些 VPN 联合形成一个具有故障冗余和负载均衡功能的 VPN 隧道。



StoneGate 监视每一个 ISP 的可用性和带宽状况来决定将一个数据包分配个哪一个 ISP 连接，在每一个 ISP 都可用的情况下，StoneGate 将把连接分配给拥有最好的带宽的那一个 ISP。当用户需要更多的带宽来访问互联网时，在传统上，用户只有通过在现有的 ISP 上购买更多的带宽来实现这一要求，因为改变 ISP 将导致公用 IP 的更改，给用户带来极大的不方便。但是对于多 ISP 的 StoneGate 体系，用户除了在现有的 ISP 上购买更多的带宽以外，StoneGate 通过在线的增加一个新的 ISP 同样可以达到这一要求。

4.3 STONEGATE 防火墙设备

StoneGate 安全应用设备产品系列包括名种不同的网关设备，均用于在分散的安全架构下执行企业网络安全任务. 根据客户的需要, StoneGate 安全应用设备可作为防火墙/虚拟专用网解决方案式仅作为虚拟专用网解决方案进行部署. 所有设备均由 StoneGate 管理中心(SMC) 进行管理

◆ 4.3.1 SG-200

StoneGate SG-200 专为小型远程办公室设计的固态安全网关，提供可靠的企业级安全及业务持续性. StoneGate 网关拥有三个 10/100 以太网端口, 可处理最多达 20Mbps 的吞吐量并进行远程升级及进行中央管理.

SG-200 Appliance Specifications	
Software	StoneGate Firewall Engine (preloaded)
Network Interfaces	3 x 10/100BASE-TX, autosensing
Licensed firewall Performance	20 Mbps
Licensed 3DES VPN Performance	6 Mbps
Licensed AES-128 VPN Performance	8 Mbps
Maximum Connection Establishment Rate (connections/sec.)	1 600
Sustained Concurrent Connection	50, 000
Concurrent IPsec tunnels	1 000
High Availability	Yes, active/active with up to 16-node, clusters, stateful failover (including VPN connections)
ISP Multihoming	Yes, high availability and load balancing between multiple ISPs (including VPN connections)
# of protected IPs	Unlimited users

◆ 4.3.2 SG-500

SG-500 防火墙/虚拟专用网网关致力于满足拥有几十名员工的远程办公室的安全需求. 透过 5 个 10/100Mbps 的高速从太网接口, SG-500 支持小型网络分段, 以不断操作为日的群集及多重连接配置.

SG-500 Appliance Specifications		
Software	StoneGate Firewall Engine (preloaded)	
Network Interfaces	5 x 10/100 FE, autosensing	
	SG-500-50	SG-500-100
Licensed Firewall Performance	50 Mbps	100 Mbps
Licensed 3DES VPN Performance	8 Mbps	11 Mbps
Licensed AES-128 VPN Performance	10 Mbps	22 Mbps
Maximum Connection Establishment Rate (connections/sec.)	4 200	4 200
Sustained Concurrent Connection	75,000	100,000
Concurrent IPsec tunnels	1 500	2 000
High Availability	Yes, active/active with up to 16-node, clusters, stateful failover (including VPN connections)	
ISP Multihoming	Yes, high availability and load balancing between multiple ISPs (including VPN connections)	
# of protected IPs	Unlimited users	
Hardware Specifications		
Serial console	One RS-232 serial port	
Dimensions (W x H x D)	220 x 50 x 254 mm (8.8" x 2" x 10.16")	
Weight	2.06 kg (4.5 lbs.)	
Power Supply	Full range AT 44W PSU, 100–240V, 47 –63 Hz	

◆ 4.3.3 SG-570

SG-570 防火墙/虚拟专用网网关致力于满足拥有几十名员工的远程办公室的安全需求. 透过 7 个 10/100Mbps 的高速从太网接口, SG-570 支持小型网络分段, 以不断操作为日的群集及多重连接配置.

SG-570 Appliance Specifications	
Software	StoneGate Firewall Engine (preloaded)
Network Interfaces	7 x 10/100BASE-TX, autosensing
Licensed firewall Performance	200 Mbps
Licensed 3DES VPN Performance	24 Mbps
Licensed AES-128 VPN Performance	40 Mbps
Maximum Connection Establishment Rate (connections/sec.)	4 200
Sustained Concurrent Connection	100,000
Concurrent IPsec tunnels	2 000
High Availability	Yes, active/active with up to 16-node, clusters, stateful failover (including VPN connections)
ISP Multihoming	Yes, high availability and load balancingbetween multiple ISPs (including VPN connections)
# of protected IPs	Unlimited users
Hardware Specifications	
Serial console	One RS-232 serial port
Dimensions (W x H x D)	220 x 50 x 254 mm (8.8" x 2" x 10.16")
Weight	2.06 kg (4.5 lbs.)
Power Supply	Full range AT 44W PSU, 100–240V, 47–63 Hz

◆ 4.3.4 SG-1000

SG-1000 防火墙虚拟专用网网关适用于大型企业及拥有数百人的分公司办公室. 大型办公室拥有广泛的网络，互联网使用率高，且通常在非罕事区(DMZ)寄存网站. SG-1000 拥有八个可自动调节的10/100/1000Mbps 接口，从进行网络分段，群集设置及多重连接.

StoneGate 1000-Q Appliance Specifications	
Software	StoneGate Firewall Engine (preloaded)
Network Interfaces	8 x 10/100/1000 FE, autosensing
Licensed Firewall Performance	1 Gbps
Licensed 3DES VPN Performance	90 Mbps
Licensed AES-128 VPN Performance	160 Mbps
Maximum Connection Establishment Rate (connections/sec.)	30,000
Sustained Concurrent Connection	250,000
Concurrent IPsec tunnels	5 000
High Availability	Yes, active/active with up to 16-node, clusters, stateful failover (including VPN connections)
ISP Multihoming	Yes, high availability and load balancing between multiple ISPs (including VPN connections)
# of protected IPs	Unlimited users
Hardware Specifications	
Serial console	One RS-232 serial port
Dimensions (W x H x D)	19" rack unit, 425 x 44 x 625 mm (16.8" x 1.7" x 25.7")
Weight	10.8 kg (23.7 lbs.)
Power Supply	400 W cold-swap, 100–240 V, 50–60 Hz, 8 A max.

◆ 4.3.5 SG-3000

SG-3000 防火墙虚拟专用网网关乃专为满足数据中心及大型网络中央站点的性能及扩展要求而麦计. SG-3000 拥有 4 个光纤 1000Mbps 和 10 个铜制 10/100/1000 Mbps 的以太网接口, 此外 SG-3000-C 配备有 14 个铜制 10/100/1000 以太网接口.

SG-3000-F and SG-3000-C Appliance Specifications		
Software	StoneGate Firewall Engine (preloaded)	
	SG-3000-F	**SG-3000-C**
Network Interfaces	10 x 10/100/1000 FE copper autosensing 4 x fiber 1 Gbps w/G-0 connectors	14 x 10/100/1000 FE autosensing
Licensed Firewall Performance	2.3 Gbps	
Licensed 3DES VPN Performance	180 Mbps	
Licensed AES-128 VPN Performance	340 Mbps	
Maximum Connection Establishment Rate (connections/sec.)	50,000	
Sustained Concurrent Connection	500,000	
Concurrent IPsec tunnels	10,000	
High Availability	Yes, active/active with up to 16-node, clusters, stateful failover (including VPN connections)	
ISP Multihoming	Yes, high availability and load balancing between multiple ISPs (including VPN connections)	
# of protected IPs	Unlimited users	
Hardware Specifications		
Serial console	One RS-232 serial port	
Dimensions (W x H x D)	19" rack unit, 425 x 88 x 652 mm (16.8" x 3.4" x 25.7")	
Weight	15.8 kg (34.76 lbs.)	
Power Supply	400 W cold-swap, 115/10A 230/5A, 50 – 60 Hz	

五， STONEGATE 核心优势

◆ 5.1.1 最高的安全性

多层检测

保证最高的安全性是 StoneGate 最基本的思想，它以其特有的多层检测技术来实现这一目标。多层检测技术吸收了包过滤技术、代理防火墙技术、状态检测技术的优点，是第四带的防火墙技术。

嵌入的防火墙操作系统

StoneGate 运行一个专门的 LINUX 操作系统，该操作系统包含在 StoneGate 分布式的结构当中。运行一个专门的操作系统将有效地减少因为对操作系统不适当的配置而导致的一些安全隐患。

多连接的 VPN 隧道

StoneGate 的 VPN 技术是以 IPSEC 的认证和数据加密为标准的，IPSEC 的认证和数据加密使得在 VPN 隧道中的数据很难被未经授权的用户截取伙攥改。

StoneGate 的每一个 VPN 通道经由多条线路穿过互联网，这更增加了黑客偷听得难度，因为一个偷听者在一个位置不可能偷听属于这个 VPN 的每一个数据包。

无懈可击的管理系统

StoneGate 有一套有效地企业管理系统。StoneGate 的管理系统是有着非常人性化的、易于使用的特点，相比于目前市场上的主流的防火墙的管理系统，StoneGate 管理系统大大降低了人为错误的机率，也减小了因为错误的配置而导致存在安全漏洞的可能。

◆ 5.1.2 最高的性能

多层检测提升性能

StoneGate 特有的几种先进的技术能够确保 StoneGate 业界领先的防火墙性能。多层检测技术本身就能够提高防火墙的整体性能。

改进的嵌入式防火墙操作系统

StoneGate 引擎内嵌在一个 LINUX 操作系统当中，在处理器的速度和资源分配上能够得到更高的优先权。另外，StoneGate 的操作系统是一种专门针对于防火墙的流线型的操作系统。StoneGate 的操作系统也支持更高一级的硬软件特性，例如支持多个处理器、专门的高性能的安全检测算法。

◆ 5.1.3 可支持多种硬件平台

StoneGate 可在以下硬件上执行:

StoneGate 设备　　Intel® based 平台　　IBM iSeries　　IBM zSeries

◆ 5.1.4　网络的高可用性

Multi-link 技术

StoneGate Multi-link 技术使得单个的防火墙集群可以连接到多个 ISP(网络服务提供商)上，这样，StoneGate 将在与之相连的多个 ISP 之间提供负载均衡和故障冗余，消除了在连接到一个 ISP 的时候因 ISP 不可用而导致的单点故障。在 VPN（虚拟专用网）的情况下，StoneGate 同样也支持多条并行的专线连接到互联网上，并且在这些并行的专线之间进行负载均衡和故障冗余。

防火墙集群

防火墙集群技术能够在防火墙上实现负载均衡和故障冗余。通过负载均衡和故障冗余，防火墙集群提供更高的伸缩性并且能够对防火墙进行在线的维护，StoneGate 在集群的各个节点之间进行负载均衡以提高整个防火墙的吞吐量。

服务器的负载均衡

对服务器实现负载均衡也是 StoneGate 防火墙的重要特点。StoneGate 自己特有的 inbound traffic 管理技术使得被防火墙保护的服务器如 WEB、FTP 等可以实现负载均衡，避免网络连接造成的单点故障的同时，也可以消除因为服务器的单点故障而造成的应用中断。

◆ 5.1.5 可伸缩的管理

集中的管理系统

集中的、企业级的管理是 StoneGate 防火墙的重要特征。通过位于中心的管理系统，可以简单的管理多套防火墙或防火墙集群，包括穿过广域网去管理分公司的防火墙设备。其强大的日志系统、备份系统大大减少了系统管理员的工作负担。

防火墙的配置与网络的配置相结合

管理系统同样也包括对防火墙引擎操作系统的管理，在对防火墙引擎进行初始化以后，对防火墙引擎的所有的操作都可以在位于中心的管理系统上进行，而不需要在防火墙引擎上进行任何的操作。这不仅减少了管理员的工作负担，也降低了人为因素导致出错的可能性。

全面易用的管理工具

StoneGate 管理系统为系统管理员提供了一套强大的管理工具来提高系统管理员的工作效率。例如：安全策略模板、子规则、多个管理员级别、强大的日志过滤、日志修剪工具。另外可以同时的从多个 GUI 对防火墙进行管理也极大的方便了系统管理员的工作。

◆ 5.1.6 降低用户成本

Multi-link ISP

StoneGate 通过其高可用技术提高了 ISP 的可靠性，使得用户可以将那些关键的应用从昂贵的专线连接移植到相对便宜的 VPN 上，这种移植将降低有户的线路成本，还能提升现有互联网的利用率。

管理费用的节省

StoneGate 强大的管理工具最大的减少了管理工作，薪金昂贵的系统管理员可以将精力放到比日常的防火墙维护工作更重要的工作当中；另外，StoneGate 不会因为要达到高的性能而要求顶级的硬件平台。对于 StoneGate 来说，一般的 INTEL 构架的硬件平台就能达到企业级的吞吐性能。

内嵌的集群技术

有了 StoneGate 防火墙的高可用技术，用户不用再去实施专门的负载均衡和高可用的方案，StoneGate 的 Multi-link 、防火墙集群、服务器负载均衡技术将完成这一切，减少了额外的硬件与软件开支，以减少了相应的机房的维护费用、操作管理费用。