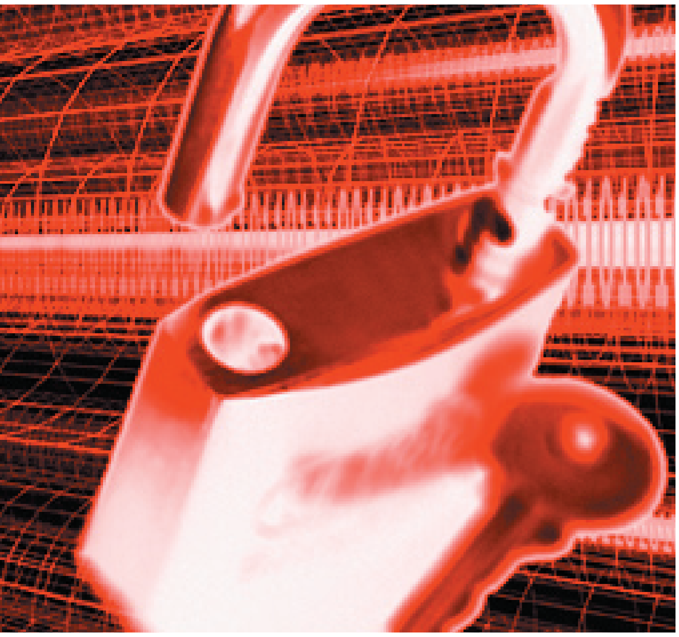


VisNetic Firewall Datasheet

VisNetic Firewall is a packet-filtering software firewall for Windows-based Workstations and Servers. Created by the developer of ConSeal, VisNetic Firewall features sophisticated firewall technology, flexible configuration options and powerful monitoring and reporting capabilities. Unlike its peers however, VisNetic Firewall is priced affordably and quite simple to deploy and maintain. Server licenses start at $249.95 US and VisNetic Firewall's Configuration Wizard steps most users through setup in less than 10 minutes.

"After a flawless install and a painless initial setup, I found VisNetic to be exactly what I was looking for. The interface allowed rules and options to be configured quickly and easily. I was able to create rules for my Dial-Up adapter as well as my broadband cable connection. VisNetic provided the perfect flexibility in ruleset configuration; I was able to allow only the traffic that I needed while blocking and logging everything else. The ability to view logs in real-time was also a big plus because it enables me to analyze attacks as they occur. Additionally, advanced security features such as Sequence Number Hardening and Stateful Packet Inspection were ground-breaking technologies that I now swear by."

Chris Hanaway
Colorado Springs, CO

Advanced Firewall Technology

- **Stateful Inspection** – VisNetic Firewall features stateful inspection, an advanced firewall architecture also known as dynamic packet filtering. Stateful inspection provides enhanced security by keeping track of communications packets over a period of time. Both incoming and outgoing packets are examined. Outgoing packets that request specific types of incoming packets are tracked and only those incoming packets constituting a proper response are allowed through the firewall.
- **Port Scan Detection**– VisNetic Firewall is designed to detect all TCP port scans, a tactic typically employed just prior to hack attempts. VisNetic Firewall detects the most common forms of port scans, alerting you with a log entry and optionally automatically banning the IP address of the scanner, ensuring that they are “cut off” before they can discover any useful information about your system.
- **SYN Flood Protection** – A SYN Flood is a common type of denial of service (DoS) attack used against servers. When launching a SYN Flood, an attacker bombards you with so many connection requests that your computer is unable to accept legitimate connections, effectively shutting down your web, email, FTP or VPN server. VisNetic Firewall employs SYN cookies to protect you from SYN Flood attacks.
- **Tarpits** – VisNetic Firewall allows you to trap hackers, slow down the spread of worms and stall spammers by creating tarpits. A tarpit is a trap for troublesome outsiders. Using tarpits, your system accepts TCP connections but never replies and ignores disconnect requests. This can leave ports scanners and hackers stuck for hours, even days.
- **HTTP Filtering** - Using VisNetic Firewall’s HTTP Filtering, you can prevent intrusion attempts targeted at your web server by screening requests and automatically banning the offender’s IP address, preventing further access.
- **MAC Address Filtering** - VisNetic Firewall now has the ability to filter traffic based on MAC addresses. The ability to allow or deny a computer by its MAC address ensures that malicious or unwanted users on your network are unable to bypass security filters.

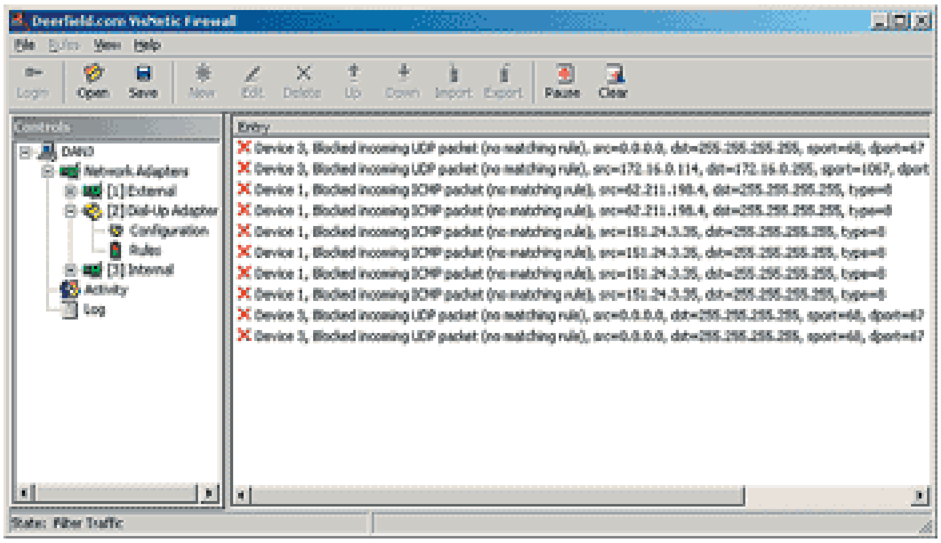
Powerful Administration Tools

Unlike most hardware firewalls, VisNetic Firewall is highly configurable and features a number of powerful administrative tools. These include:

- Remote Administration - VisNetic Firewall for Servers allows access to an entire network or single installation of the Firewall from the Firewall Server or remote locations. This feature gives administrators incomparable freedom and ensures the highest level of security through password protection.

- Granular Access Control - VisNetic Firewall gives the administrator unparalleled control over the traffic passing through the firewall. All traffic is blocked by the firewall, unless you have specifically configured a rule to allow it. Rules are configured per-device, and you have full control over the local and remote IP address(es), local and remote port(s), protocol, and direction of the traffic that you will allow through the firewall.

- Real Time Activity Viewing – The Connections Viewer is a real-time display showing all active connections going through the firewall. For example, with VisNetic Firewall installed on a web server, a quick glance at the Connections Viewer would show the administrator how many visitors are currently at their web site.



```
Entry
Device 3, Blocked incoming UDP packet (no matching rule), src=0.0.0.0, dst=255.255.255.255, sport=68, dport=67
Device 3, Blocked incoming UDP packet (no matching rule), src=172.16.0.114, dst=172.16.0.255, sport=1067, dport
Device 1, Blocked incoming ICMP packet (no matching rule), src=62.211.198.4, dst=255.255.255.255, type=8
Device 1, Blocked incoming ICMP packet (no matching rule), src=62.211.198.4, dst=255.255.255.255, type=8
Device 1, Blocked incoming ICMP packet (no matching rule), src=151.24.3.35, dst=255.255.255.255, type=8
Device 1, Blocked incoming ICMP packet (no matching rule), src=151.24.3.35, dst=255.255.255.255, type=8
Device 1, Blocked incoming ICMP packet (no matching rule), src=151.24.3.35, dst=255.255.255.255, type=8
Device 1, Blocked incoming ICMP packet (no matching rule), src=151.24.3.35, dst=255.255.255.255, type=8
Device 3, Blocked incoming UDP packet (no matching rule), src=0.0.0.0, dst=255.255.255.255, sport=68, dport=67
Device 3, Blocked incoming UDP packet (no matching rule), src=0.0.0.0, dst=255.255.255.255, sport=68, dport=67
```

- Extensive Logging – VisNetic Firewall has full logging capabilities. Administrators have complete control over what to log, how large the log file can become, where to store the logs, and how often to begin a new log file.