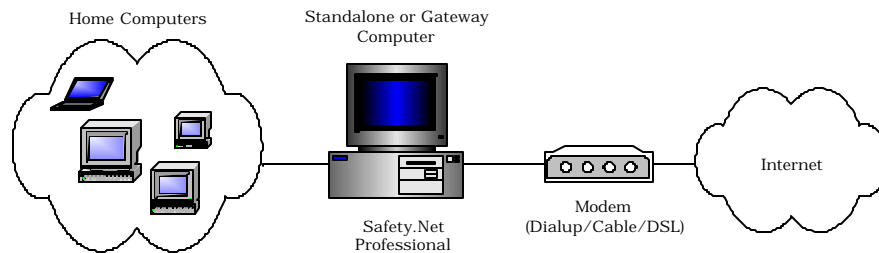




Safety.Net™ Professional offers comprehensive Internet filters, parental controls, time restrictions, activity reports and personal firewall security for all home computers.

Comprehensive Network Policy Management

Safety.Net Professional offers comprehensive Internet filters, parental controls, time restrictions, activity reports and personal firewall security for all home computers. This gateway model solution provides customization, flexibility and scalability to users, and delivers accurate and reliable filtering and security without any impact to overall system performance.



Platforms: Windows 95, 98, ME, NT, 2000 or XP

Low Level Network Driver

Safety.Net Professional operates seamlessly at the lowest level of the protocol stack and performs real time on-the-fly MAC-layer stateful inspection of protocols and content. The kernel-mode NDIS driver implementation delivers high level of performance without memory or processor upgrades.



301 N. Harrison Street, Suite 394, Princeton, NJ 08540
Tel: 877-NetVeda, Fax: 877-271-2133
<http://www.netveda.com>, Email: sales@netveda.com



Flexible Policy Based Management

Customize policies based on user or network computer. Administrators can enforce user specific controls based on logon name and domain for multi-user shared-computers, and computer specific controls based on NetBIOS computer name, MAC or IP address for Internet connection sharing and home office environments.

Web Site Filtering

Allow or block access to up to 65,535 sites by URL, IP address or domain. The web site groups are viewable and editable by the administrator. There are no hidden web site groups. Use the strict web access control option to grant access to explicitly allowed domains and sites only and block all other sites.

Web Content Filtering

Context-sensitive filters block access to a web page based on the appearance of restricted phrases in the head or body of the web page. Through automatic detection of content type, content restriction is only enforced on text (i.e. audio, video and binary streams are not parsed for content). The web content groups are viewable and editable by the administrator. There are no hidden web content groups.

Web Search Restrictions

Block web searches based on restricted phrases. Search engines are a major source of unsolicited adult material through innocuous searches. Restricting searches helps to block objectionable access early and conserve valuable network bandwidth.

Erase Incoming Content

Obliterate whole or partial phrases (words or sentences) in incoming content. There is no limit on the number of phrases that can be erased. Through automatic detection of content type, obliteration is only performed on text (i.e. audio, video and binary streams are not parsed for content). The erase content groups are viewable and editable by the administrator. There are no hidden erase content groups.

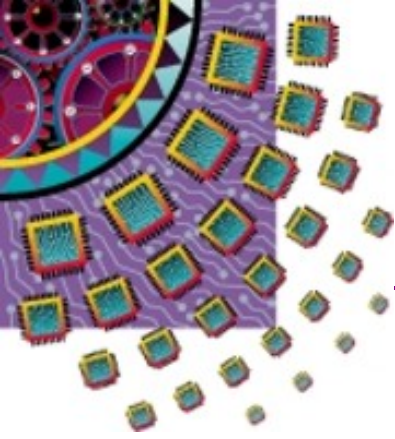
Erase Outgoing Content

Block personal information from being sent out on the Internet (e.g. name, street & school address, credit card & telephone numbers in email, chat, insecure web forms, etc.). This is a valuable feature for parents to protect children from revealing information to strangers on the Internet.

PICS Ratings

Block content based on labels issued by industry standard rating bureaus (RSAC, ICRA, SafeSurf, etc.). While site and content lists are effective filtering techniques, rating's based filtering is rapidly gaining acceptance in the industry and offers greater accuracy and granularity.





User Access Controls

Allow or block specific local users from accessing the Internet.

Application Access Controls

Allow or block specific applications from accessing the Internet, to prevent covert transfer of confidential data by rogue applications to hackers.

Service Access Controls

Allow or block specific services from accessing the Internet (e.g. chat, ftp, etc.)

Restrict Access Time

Restrict Internet access by day-of-week and time-of-day. Planned access schedules help to balance the load, conserve network bandwidth, improve productivity and performance.

Internet Security

Basic security options to:

- Hide computer on the Internet to protect your computer from hackers.
- Block unsolicited incoming network connections from external sources on the Internet.
- Block file and printer sharing on the Internet.
- Block incoming broadcast traffic.

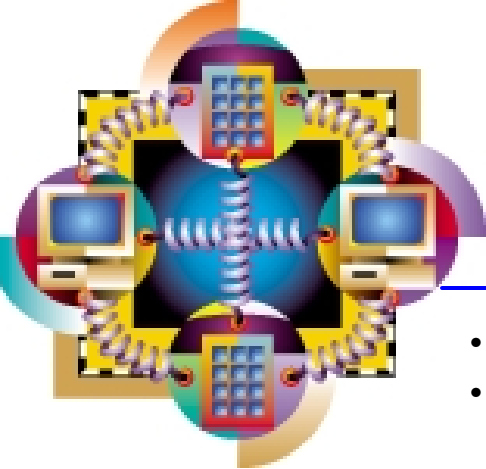
Application & Component Trust

- Allow only trusted applications and components (e.g. DLLs) to access the network.
- Warn when any untrusted application attempts network access directly or indirectly via a trusted application.
- Warn when a trusted application uses any non-trusted component.
- Detect and quarantine unwanted and harmful applications (e.g. malware, spyware, adware, trojans, worms).

Content Security

- Disable content encoding (except for specified sites).
- Hide user identifiable information in web browser requests (except for specified sites). This blocks the transfer of information about your computer and cookies to web sites.
- Disable content filtering for specified file types.





- Enable content filtering for specified content types.
- Disarm (incoming and outgoing) mail attachments for specified file types.

Report Generator

Comprehensive network activity reports include sites and pages accessed by date and time, traffic volume, attempted access violation with in-depth information, application identification, local and remote host addresses and port, protocol and reason for denial. Reports are emailed daily, weekly or monthly as provisioned.

Advanced Internet Firewall

Advanced options for users to build custom filters based on service, application, source network, destination network and hour of day.

Easy Administration

The simple and intuitive graphical user interface and configuration management concepts help administrators master the controls quickly and easily.

Application Activity Monitoring

The real-time application activity monitor reports network application name, port, protocol, and file path information to effectively track an applications use of the network. This feature assists users to detect and identify distrusted applications and block network access with application specific filters.

Robust Design

The solution has been designed to counter common vulnerabilities from hacker attacks and savvy workarounds (such as changing the computer's time-of-day settings, using cached IP addresses or aliases to access a web site, etc.).

System Requirements

Safety.Net Professional works on Microsoft Windows 95, 98, ME, NT, 2000 and XP single/multi-processor platforms, and operates with any compliant Proxy Server, Network Address Translation (NAT) Router, IP Router or Virtual Private Network (VPN) gateway from any provider.

