Ethical Hacking and Countermeasures

Version 6

Module LX

Firewall Technologies

SonicWall Firewalls Boast Increased Throughput

Company claims a four to five-fold improvement in throughput.

February 19, 2008
By Andy Patrizio: *More stories by this author.*

Firewall vendor SonicWall today introduced the SonicWall Network Security Appliance Series (NSA), a trio of multifunction firewalls aimed at the mid-enterprise.

The NSA Series are multi-core platforms that work with a reassembly-free deep packet inspection engine. Together, they examine all traffic coming in for real-time inspection without slowing down network traffic.

"UTM brings multiple security technologies into a single solution to inspect these packets at a detailed level," said Jon Kuhn, director of product marketing at SonicWall. But it's not easy, he adds. "When you do that level of inspection you will have a dramatic impact on the performance of a network. So while people want all the aspects of protection today, they have the consequence of poor performance."

One way it achieves maximum performance is by scanning the file as it comes in, rather than waiting for an entire file to download before scanning it. That way, if a hint of malware is detected in the first stages of an incoming file, it is more closely inspected as it comes in.

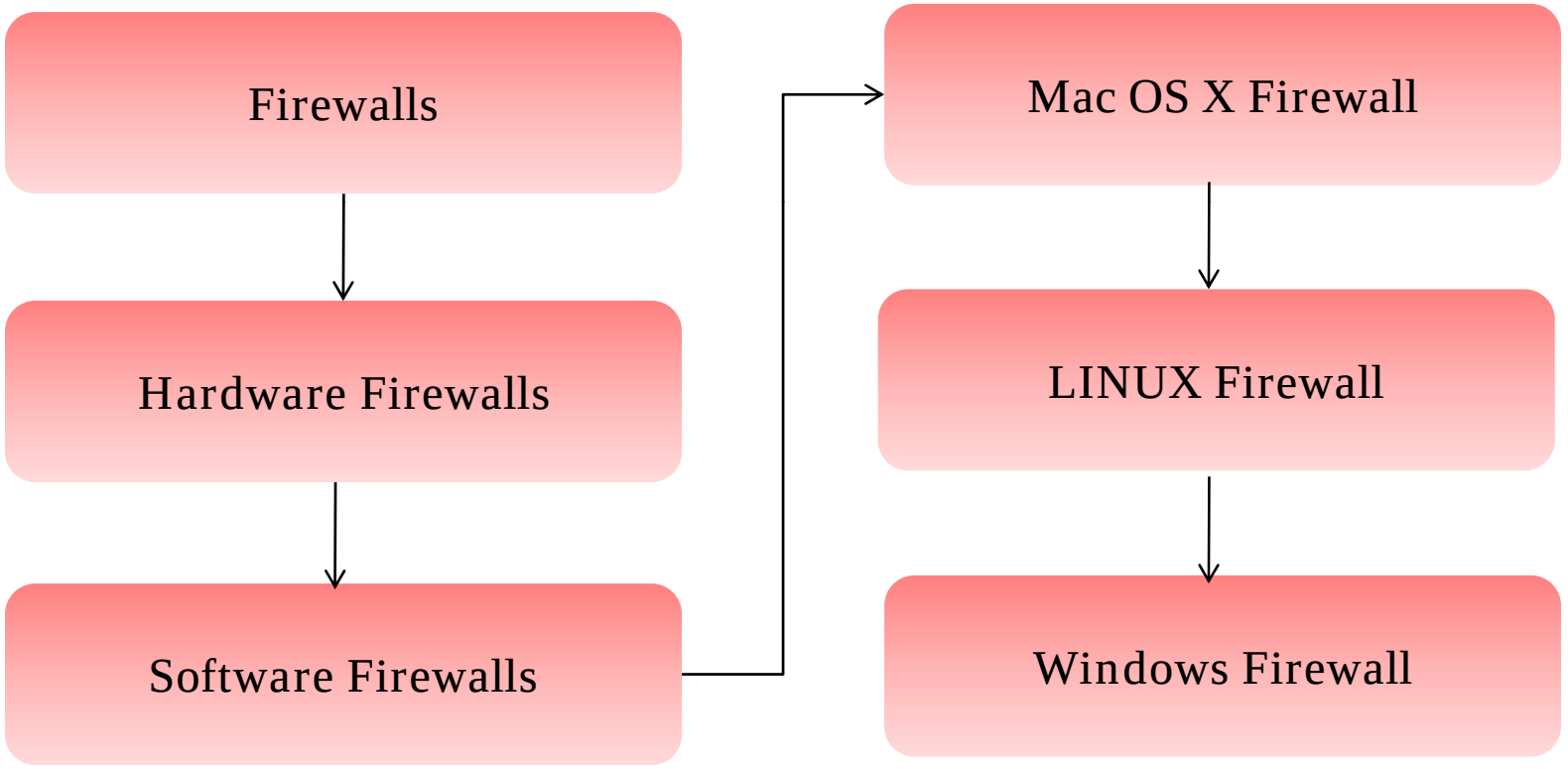
Source: *http://www.internetnews.com/*

Module Objective

This module will familiarize you with:

- Firewalls
- Hardware Firewalls
- Software Firewalls
- Mac OS X Firewall
- LINUX Firewall
- Windows Firewall

Module Flow



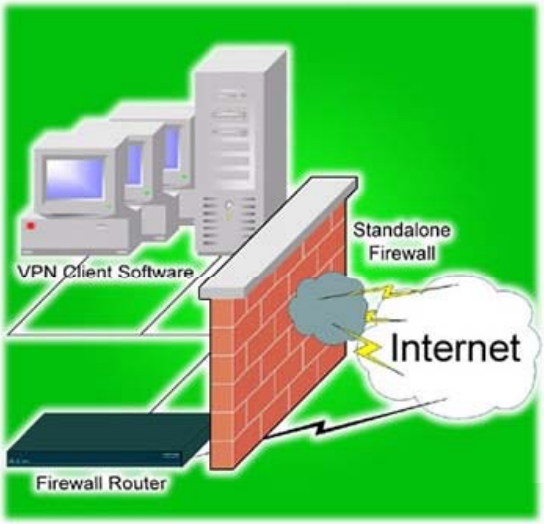
Firewalls: Introduction

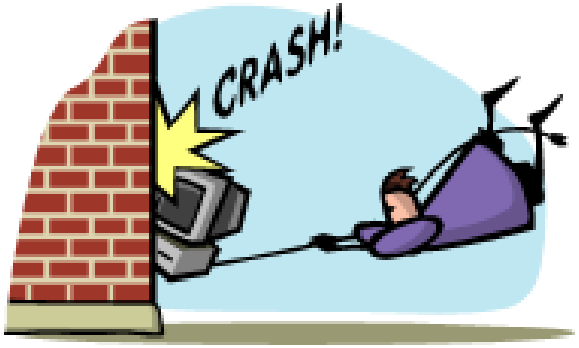
A firewall is a program or hardware device that protects the resources of a private network from users of other networks

It is responsible for the traffic to be allowed to pass, block, or refuse

Firewall also works with the proxy server

It helps in the protection of the private network from the users of the different network

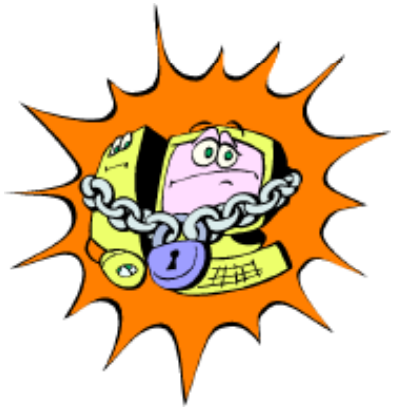




Hardware Firewalls

Hardware Firewall

- Hardware Firewalls are placed in the perimeter of the network
- It employs a technique of packet filtering
- It reads the header of a packet to find out the source and destination address
- The information is then compared with the set of predefined and/or user created rules that determine whether the packet is forwarded or dropped



Netgear Firewall

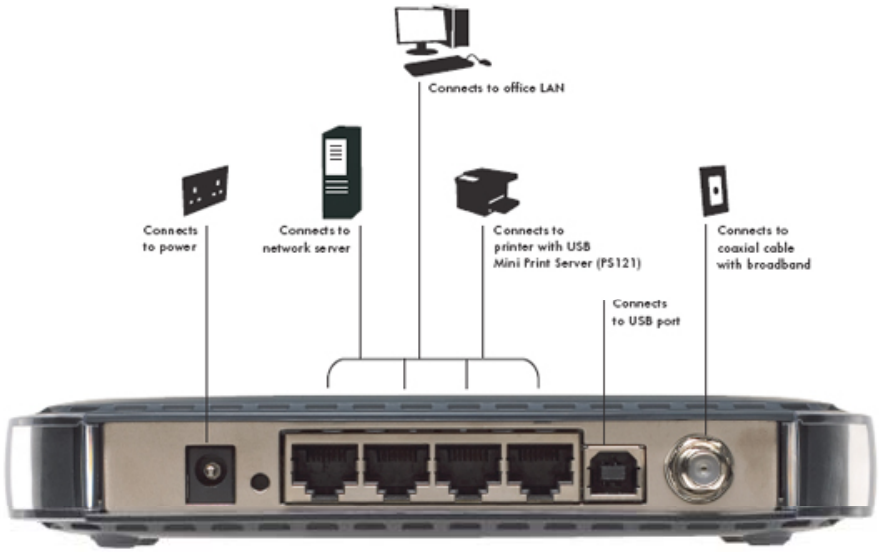
Features:

- Internet sharing broadband router and 4-port switch
- 2x the speed and 4x times the coverage of a Wireless-G router
- Configurable for private networks and public hotspots
- Double Firewall protection from external hackers attacks
- Touchless WiFi Security makes it easy to secure your network

Netgear Firewall: Screenshot

WNR 3300 Firewall

WNR 824 Firewall



Wireless Firewall Router

WNR 3500 Firewall

Personal Firewall Hardware: Linksys

Linksys scans the data travelling in the peer to peer network

It is also known as Ethernet cable/DSL firewall router

The integrated SPI firewall blocks the incoming or outgoing traffic

It works on:

- Filtering traffic from external /internal sources

Personal Firewall Hardware: Cisco's PIX

- Cisco supports Simple Network Management Protocol (SNMP) traps
- Cisco firewall series filters the java applets which is a threat to the corporate resources
- Strong firewall security and proxy authentication functions with NAT and PAT features
- Most valuable feature of Cisco firewall is a Dual NAT

CISCO PIX Firewall

Cisco PIX 501 Firewall

The Cisco PIX 501 is a compact, ready-to-use security appliance that delivers enterprise-class security for small offices and enterprise teleworker environments

It includes an integrated 4-port Fast Ethernet (10/100) switch and a Fast Ethernet (10/100) interface

It delivers upto 60 Mbps of firewall throughput, 3 Mbps of Triple Data Encryption Standard (3DES) VPN throughput, and 4.5 Mbps of Advanced Encryption Standard-128 (AES) VPN throughput

Cisco PIX 501 Series

Cisco PIX 506E Firewall

The Cisco PIX 506E is a robust, purpose-built security appliance that delivers enterprise-class security for remote and branch office environments

It provides two autosensing Fast Ethernet (10/100) interfaces

It delivers upto 100 Mbps of firewall throughput, 16 Mbps of Triple Data Encryption Standard (3DES) VPN throughput, and 30 Mbps of Advanced Encryption Standard-128 (AES) VPN throughput in a cost-effective, high-performance solution

Cisco PIX 506E Series

Cisco PIX 515E Firewall

The Cisco PIX 515E is a modular, purpose-built security appliance that delivers enterprise-class security for small to medium-sized business networks

It supports upto six 10/100 Fast Ethernet interfaces, making it an excellent choice for businesses requiring a cost-effective firewall

It delivers upto 188 Mbps of firewall throughput with the capability to handle more than 130,000 simultaneous sessions

Cisco PIX 515E Series

CISCO PIX 525 Firewall

The Cisco PIX 525 is a reliable, purpose-built security appliance for medium to large enterprise networks

It supports upto eight 10/100 Fast Ethernet interfaces or three Gigabit Ethernet interfaces

It delivers more than 330 Mbps of firewall throughput with the capability to handle more than 280,000 simultaneous sessions

Cisco PIX 525 Series

CISCO PIX 535 Firewall

The Cisco PIX 535 is a high-performance, purpose-built security appliance that delivers enterprise-class security for enterprise and service provider networks

It supports upto ten 10/100 Fast Ethernet interfaces or nine Gigabit Ethernet interfaces

It delivers upto 1.7 Gbps of firewall throughput with the capability to handle more than 500,000 simultaneous sessions

Cisco PIX 535 Series

Check Point Firewall

Check point firewall enables organizations to protect the entire network infrastructure

Different types of Firewall:

- Firewall-1
- Firewall-1 GX

Check Point Firewall (cont'd)

Features of Firewall-1:

- Comprehensive network and application firewall
- Using INSPECT, the most adaptive and intelligent inspection technology, FireWall-1 integrates both network and application-layer firewall protection

Features of Firewall-1 GX:

- Protection for GPRS networks
- Secure connectivity between carriers
- Auditing and tracking of GPRS traffic

Nortel Switched Firewall

The key component of Nortel's Layered Defense strategy is Nortel Switched Firewall

Supports secure access to organizational resources including SIP, VoIP, and other delay sensitive applications

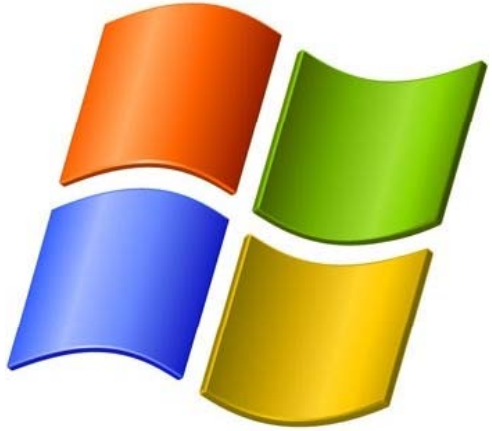
Protects IT data centers, service provider networks, and hosting infrastructures

Uses accelerator technology and Check Point Firewall-1 software, in a compact rack-mount package

Software Firewalls

Software Firewall

- Software firewall is similar to a filter
- It sits between the normal application and the networking components of the operating system
- Software firewall implants itself in the key area of the application/network path
- It analyzes what is going against the rule set



Windows Firewalls

Norton Personal Firewall

Norton Personal Firewall automatically blocks intruders and thieves, and it hides your computer from hackers

Features:

- Automatically detects and blocks viruses, spyware, and worms
- Advanced phishing protection identifies and blocks fraudulent websites
- Rootkit Protection finds and removes hidden threats in the operating system
- Smart firewall blocks the hackers and stops spyware from transmitting unauthorized information
- Intrusion Prevention automatically shields newly discovered security vulnerabilities

Norton Personal Firewall: Screenshot

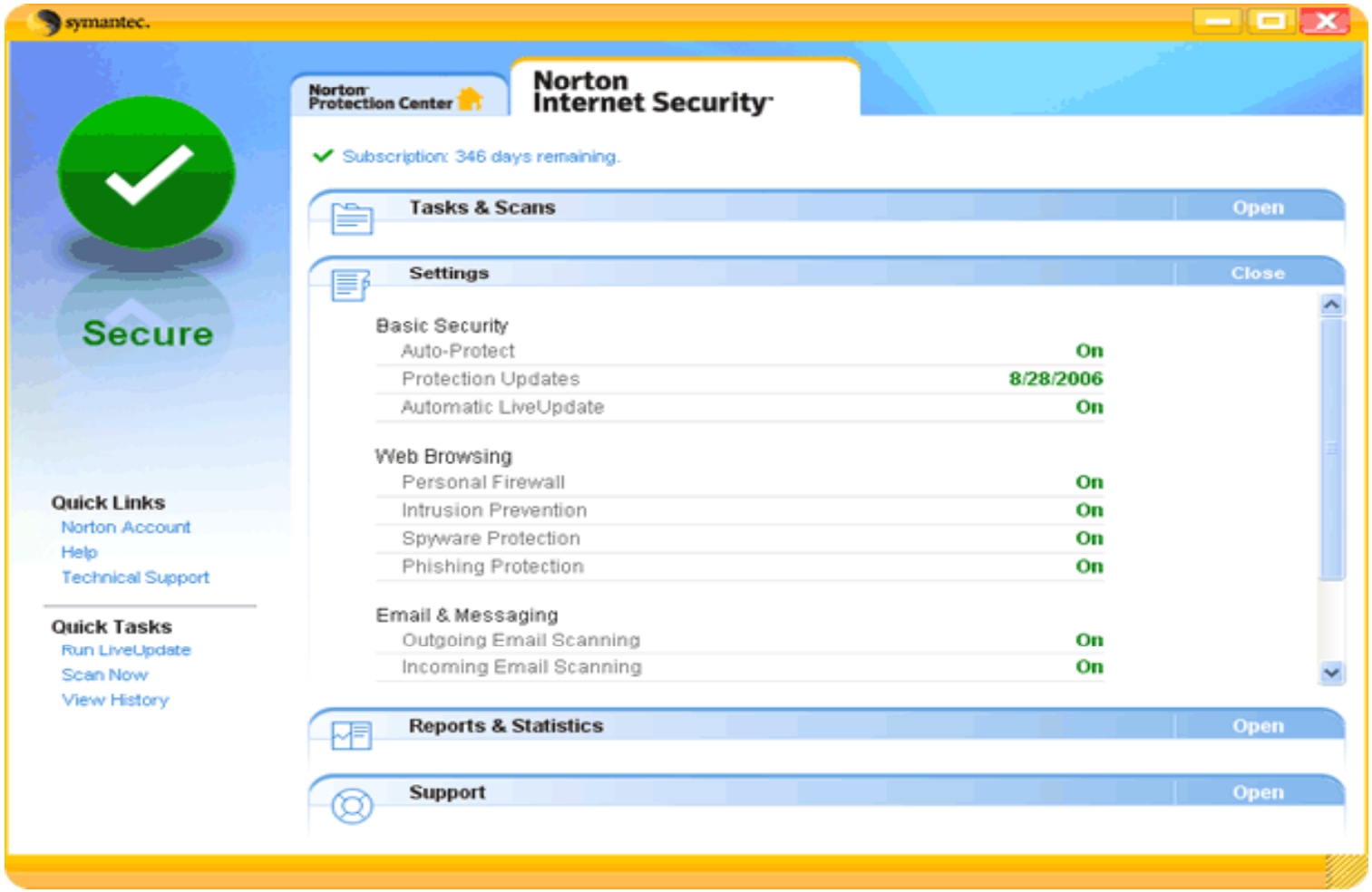


Figure: Norton Personal Firewall

McAfee Personal Firewall

Automatically blocks, cleans, and removes viruses so that you can surf the Web and download files safely

Features:

- Blocks Spyware: Blocks spyware before it is installed in computer and removes existing spyware
- Stops Hackers: Protects and conceals computer from hackers
- Improves PC Performance: Cleans clutter off
- Backs Up & Restores Files: Automated backup and one click restore
- Secures your Identity: Protects your online identity

McAfee Personal Firewall: Screenshot

Figure: Personal McAfee Firewall

Symantec Enterprise Firewall

Symantec Enterprise Firewall gives protection to the assets and data transmission by providing secure connection with the Internet

Features:

- It supports the Advanced Encryption Standard (AES)
- It supports integrated load balancing that allows scalability to more than 1.5 Gbps
- It supports URL filtering technology
- It supports inbound and outbound Network Address Translation (NAT) for both VPN and non-VPN traffic

Kerio WinRoute Firewall

Kerio WinRoute Firewall is a corporate gateway firewall for small and medium-sized businesses

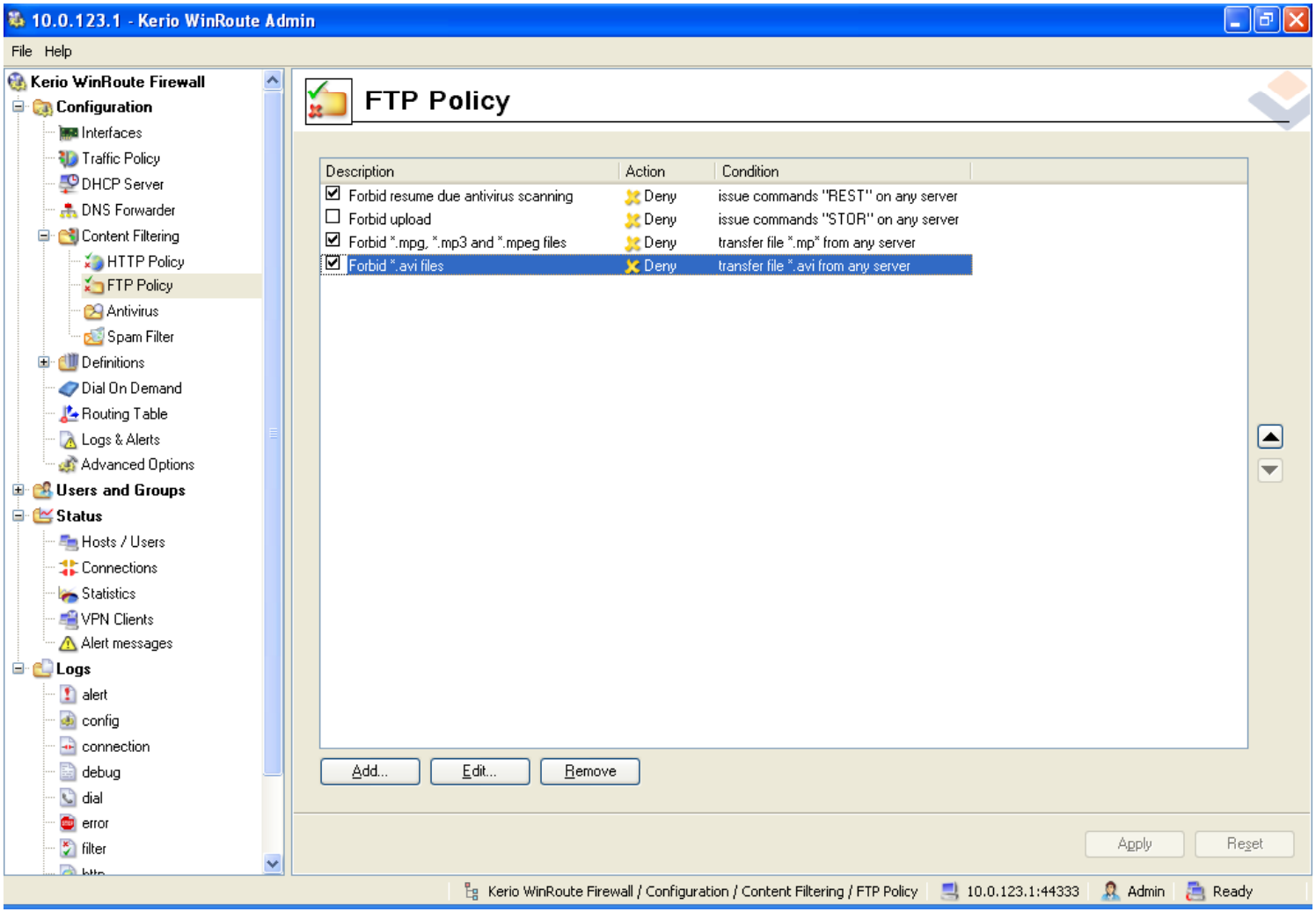
This firewall sets new standards in versatility, security, and user access control

It defends against external attacks and viruses and can restrict access to websites based on their content

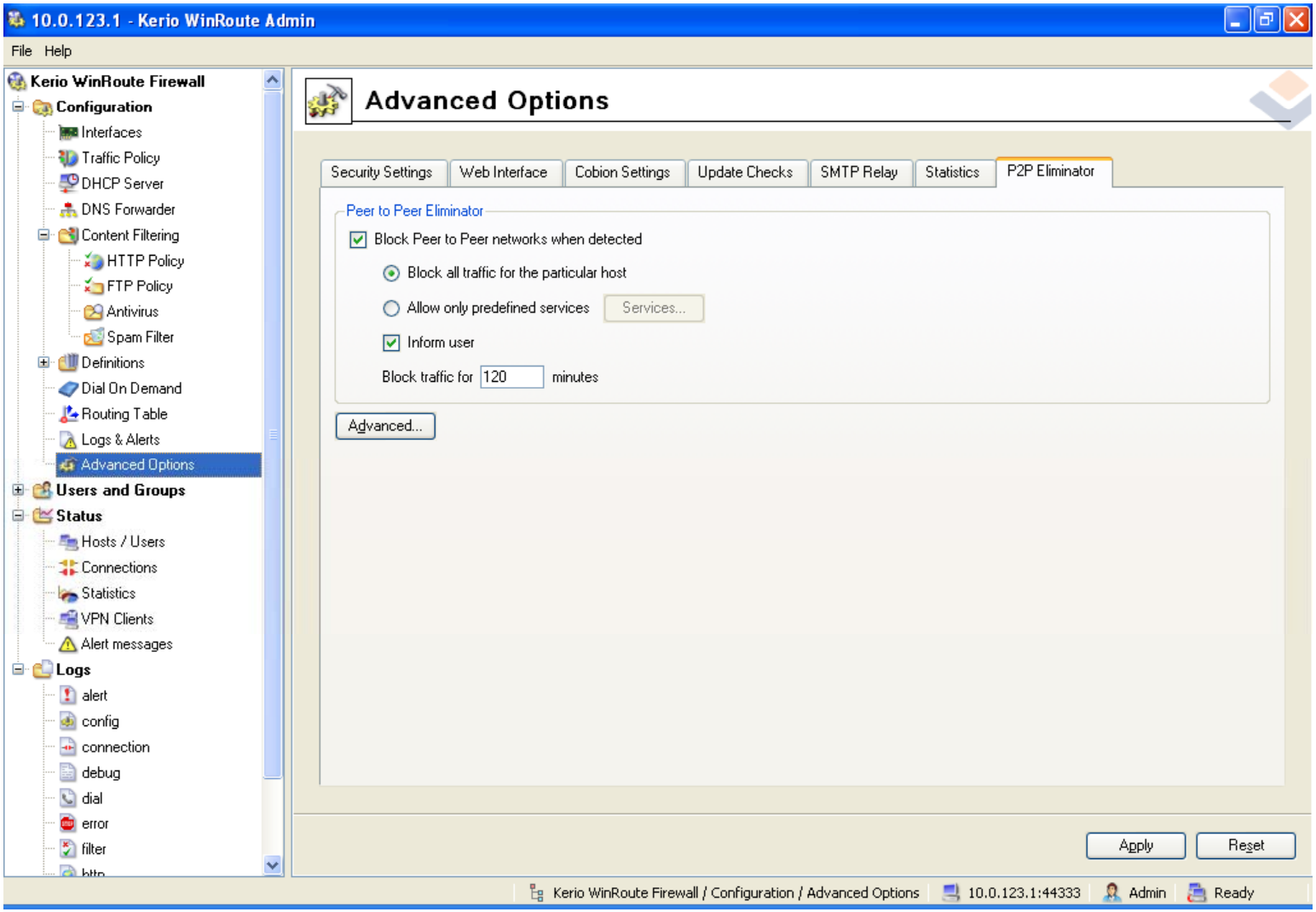
Features:

- Anti-virus Gateway Protection
- Content Filtering
- User Specific Access Management
- Fast Internet Sharing
- Internet Monitoring

Kerio WinRoute Firewall: Screenshot 1



Kerio WinRoute Firewall: Screenshot 2



Sunbelt Personal Firewall

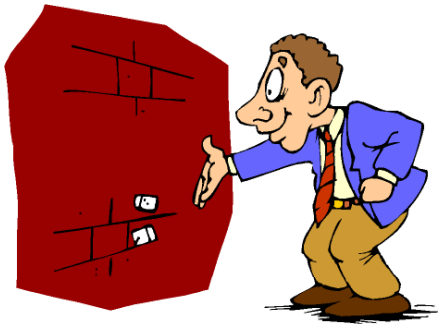
The Personal Firewall controls how computers share information through the Internet or a local network

It protects computers from external or internal attacks by other computers

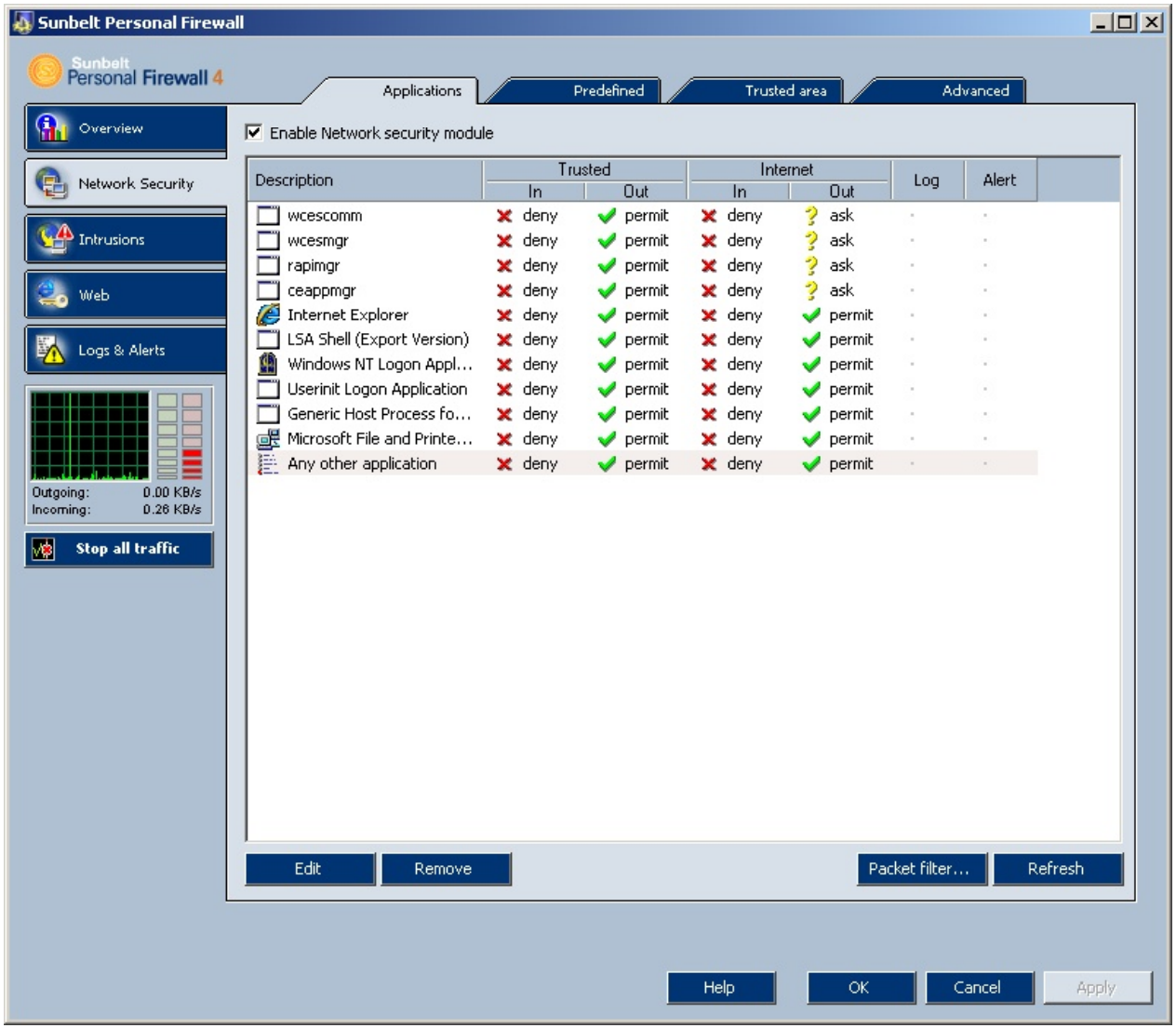
Mostly used in laptops since they are easier to compromise because of the increasing popularity of built-in wireless access

Features:

- Controls all the traffic on the network
- Creates a separate log for firewall modules
- Automatically update the newer version of the software

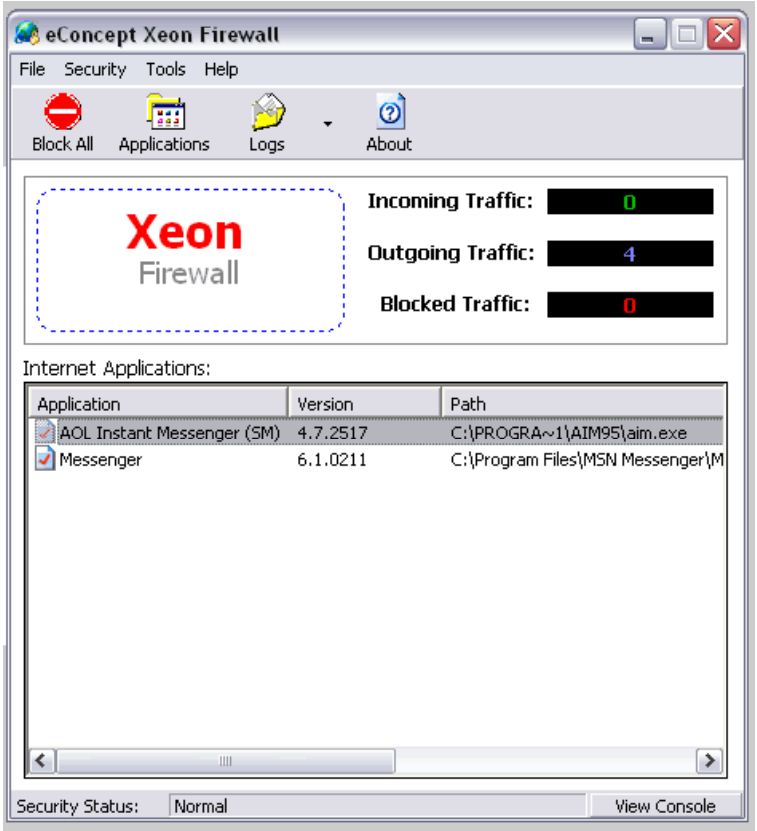


Sunbelt Personal Firewall: Screenshot

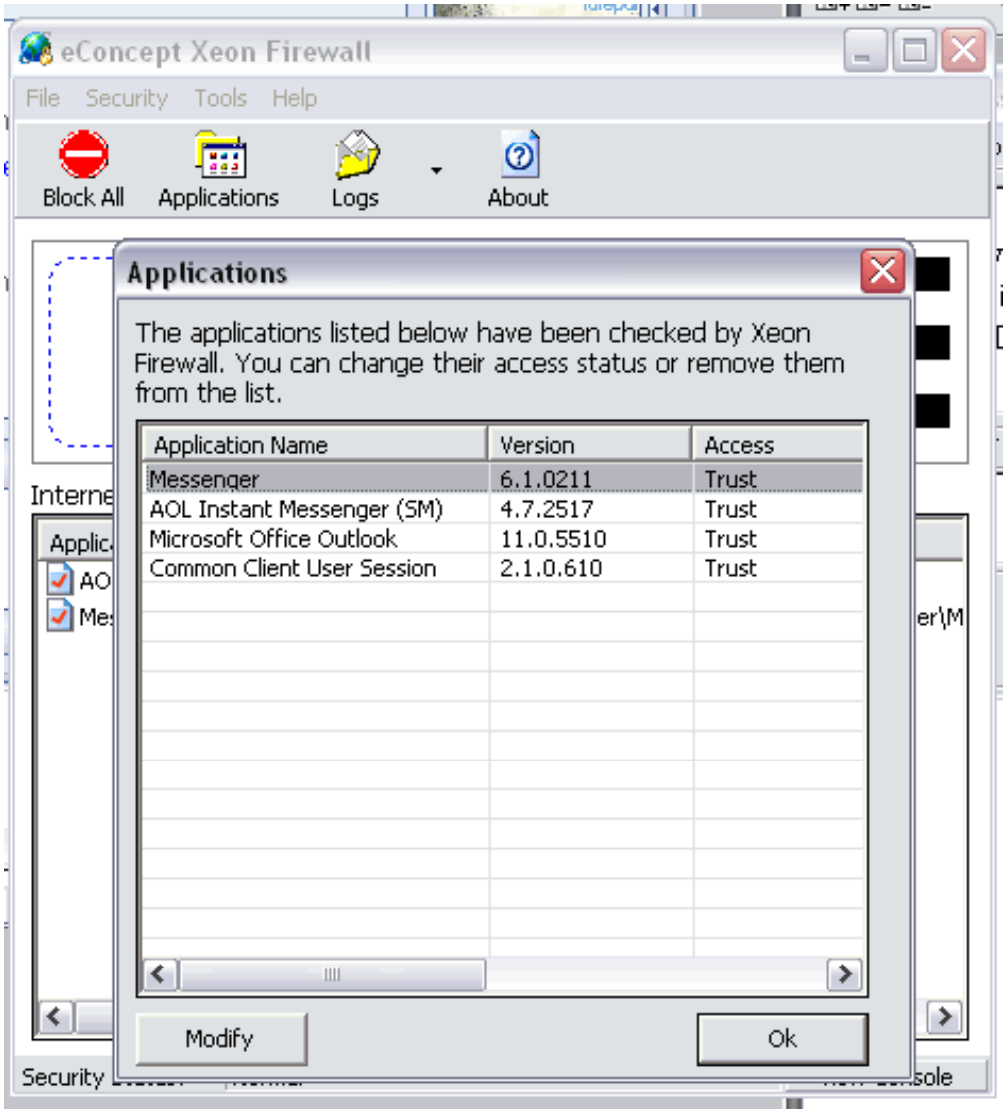


Xeon Firewall

Xeon Personal Firewall scans all your ports to detect possible hacker attempts on your system, and will identify the hacker and his/her location



Xeon Firewall: Screenshot

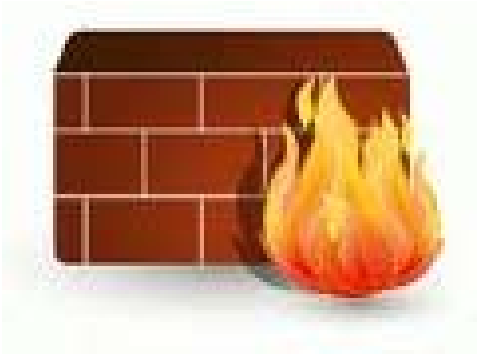


InJoy Firewall

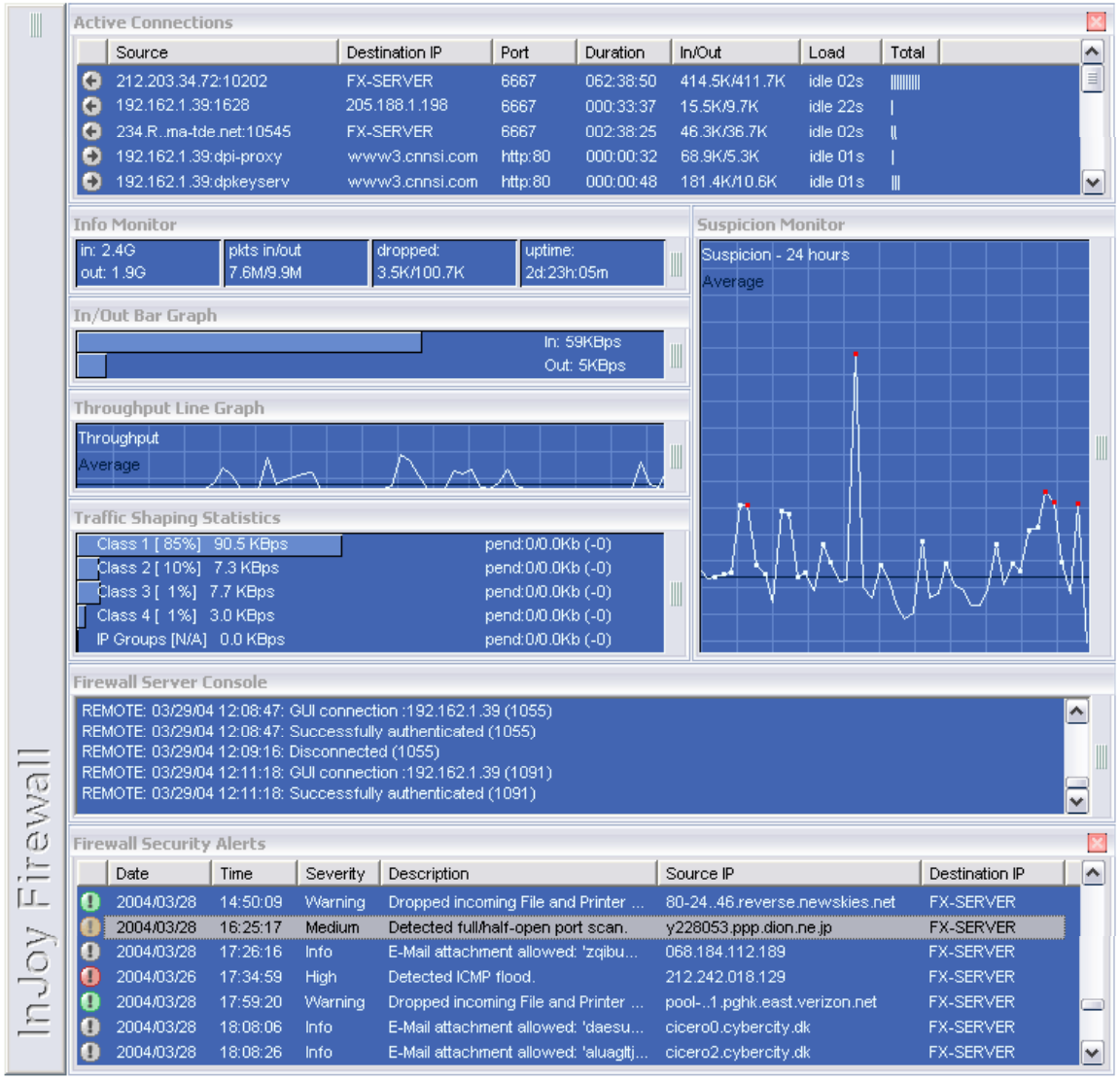
The InJoy Firewall is a firewall security solution for organizations of all sizes

Features:

- Deep Packet Inspection
- Unique MULTI-PLATFORM support
- IPSec VPN support
- Stateful Inspection
- Dynamic Firewall Rules
- Access Control Packet Filtering
- Traffic Accounting
- Traffic Shaping Bandwidth Management
- SafeMail (secure e-mail)
- Web Filtering



InJoy Firewall: Screenshot



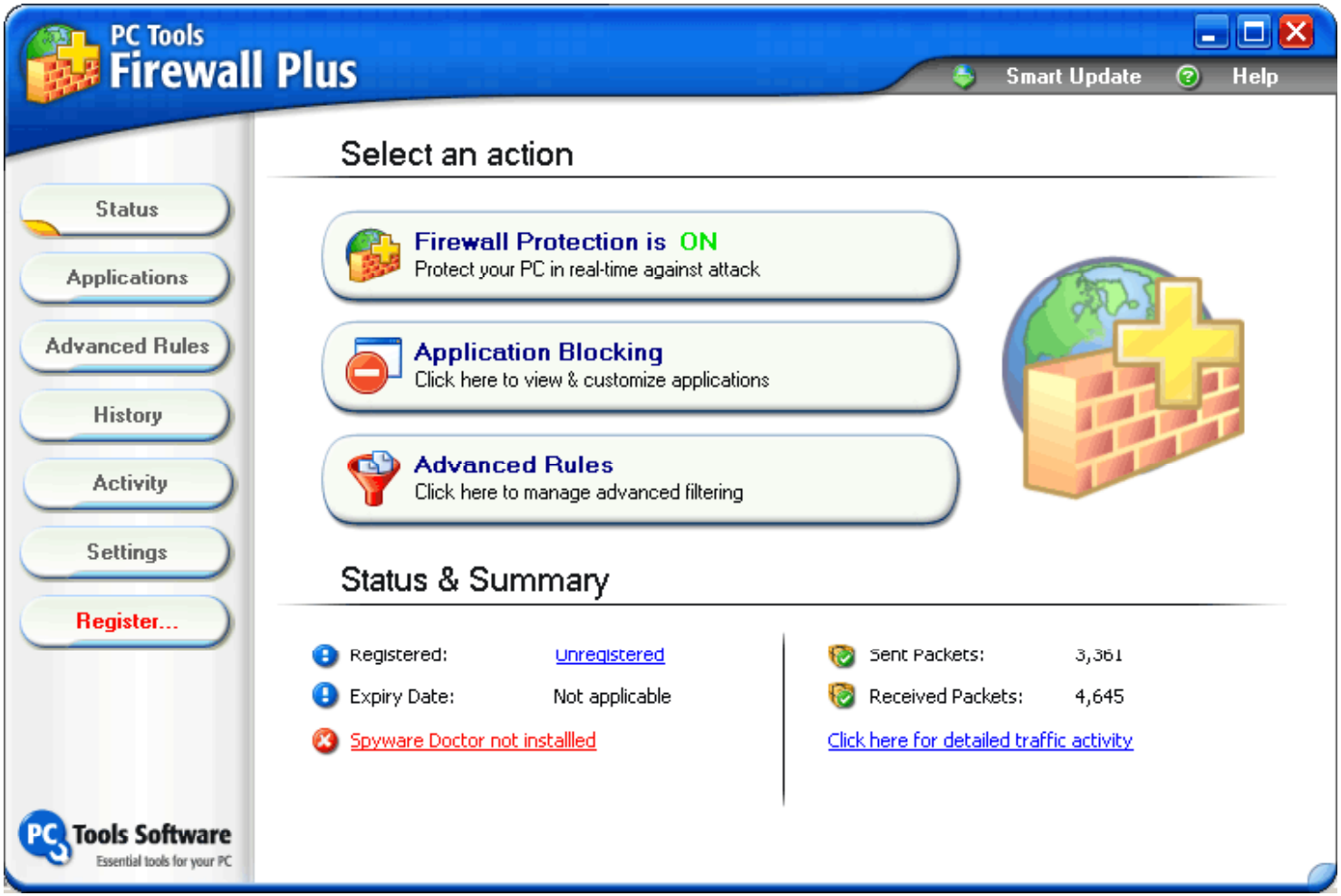
PC Tools Firewall Plus

PC Tools Firewall Plus is a free personal firewall for Windows that protects your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network

Features:

- Protects PC when users are working, surfing, and playing
- Intelligent automatic protection without all the questions
- Advanced rules to protect your PC against common attacks

PC Tools Firewall Plus: Screenshot

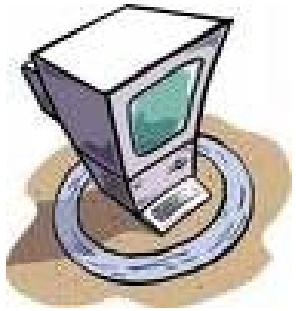


Comodo Personal Firewall

Comodo Personal Firewall protects the system from Hackers, Spyware, Trojans, and Identity theft

Features:

- Clean PC Mode
- Advanced Network Firewall Engine
- Host Intrusion Prevention System
- Powerful and intuitive Security Rules Interface
- Automatic 'Firewall Training' mode
- Windows Security Center Integration
- Self Protection against Critical Process Termination



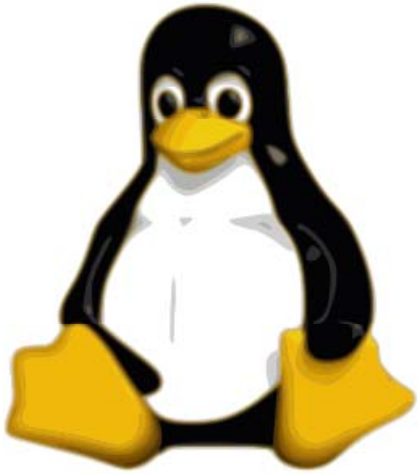
Comodo Personal Firewall: Screenshot

ZoneAlarm

ZoneAlarm is designed to protect your DSL- or cable-connected PC from hackers

The firewall controls the door to your computer and allows traffic that you understand and initiate

ZoneAlarm: Screenshot



Linux Firewalls

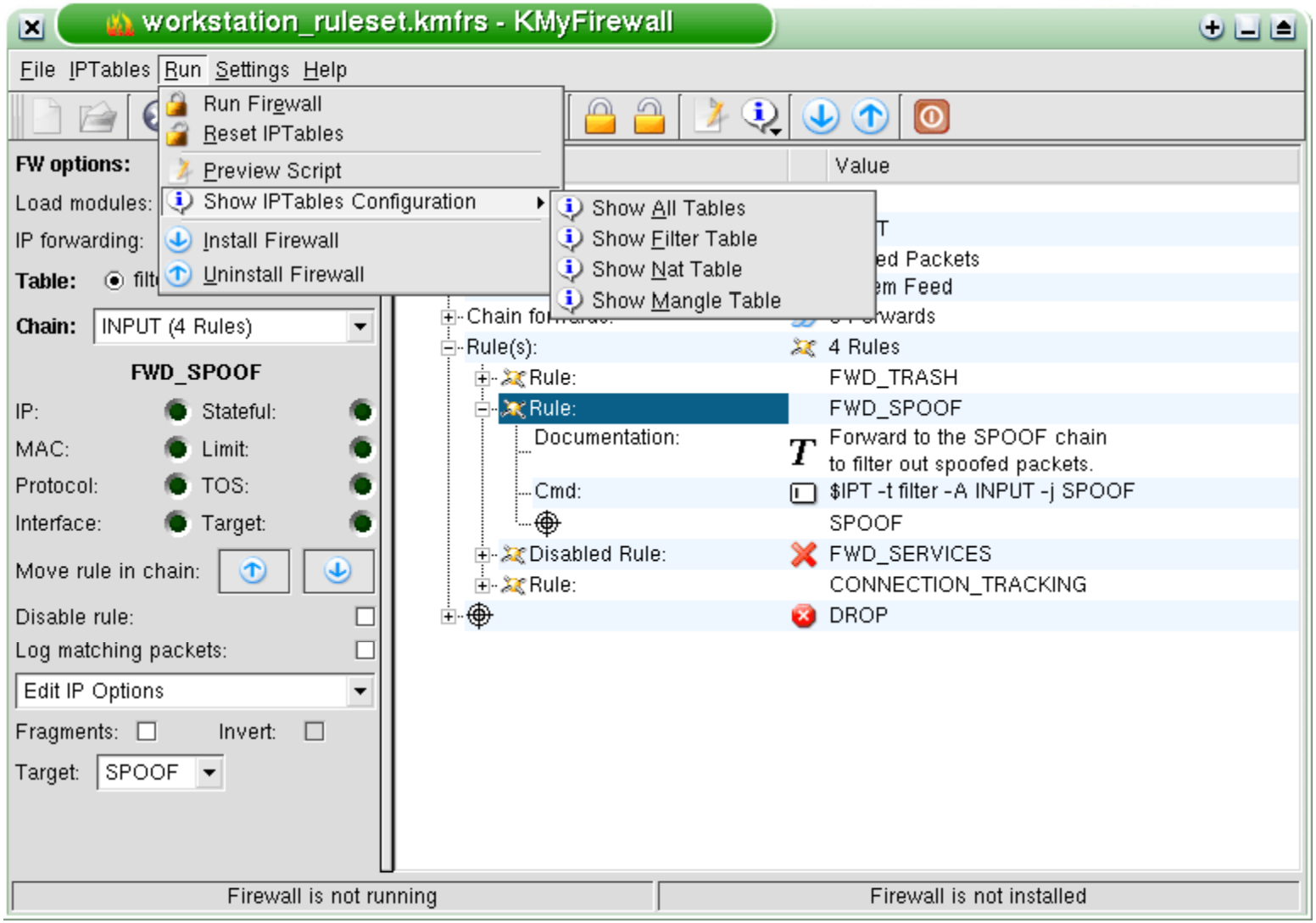
KMyFirewall

KMyFirewall attempts to make it easier to setup IPTables based firewalls on Linux systems

The firewall has the ability to save entire rulesets

You only have to configure your ruleset one time, and then you can use it on several computers giving each of them a similar configuration

KMyFirewall: Screenshot



Firestarter

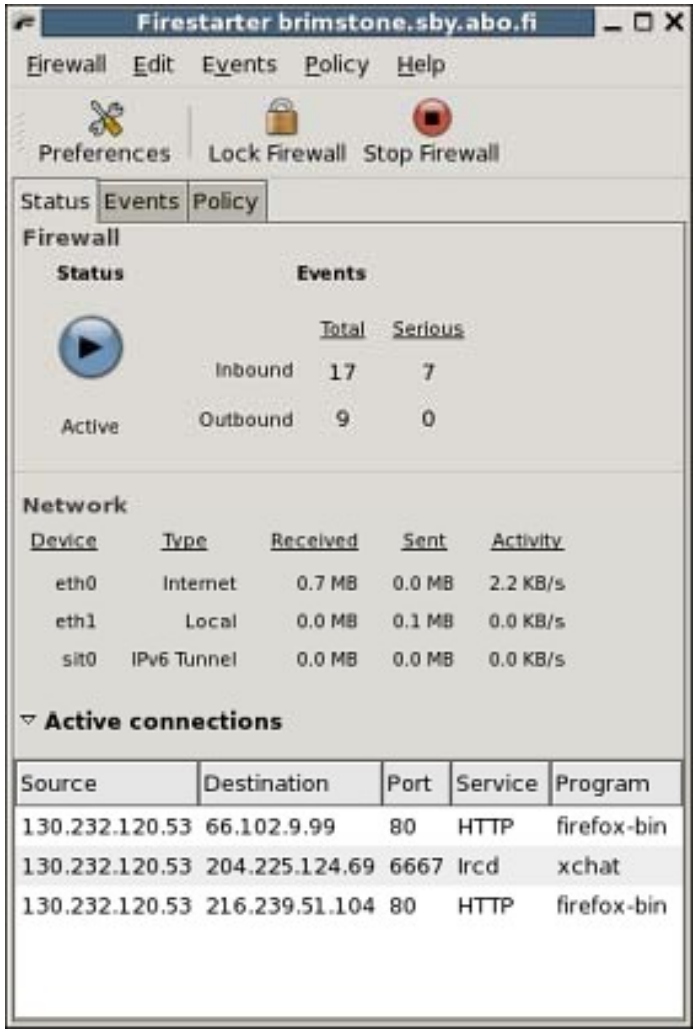
Firestarter is an Open Source visual firewall program

The software serves both Linux desktop users and system administrators

Features:

- Real-time firewall event monitor shows intrusion attempts as they happen
- Allows you to define both inbound and outbound access policy
- Option to whitelist or blacklist traffic

Firestarter: Screenshot



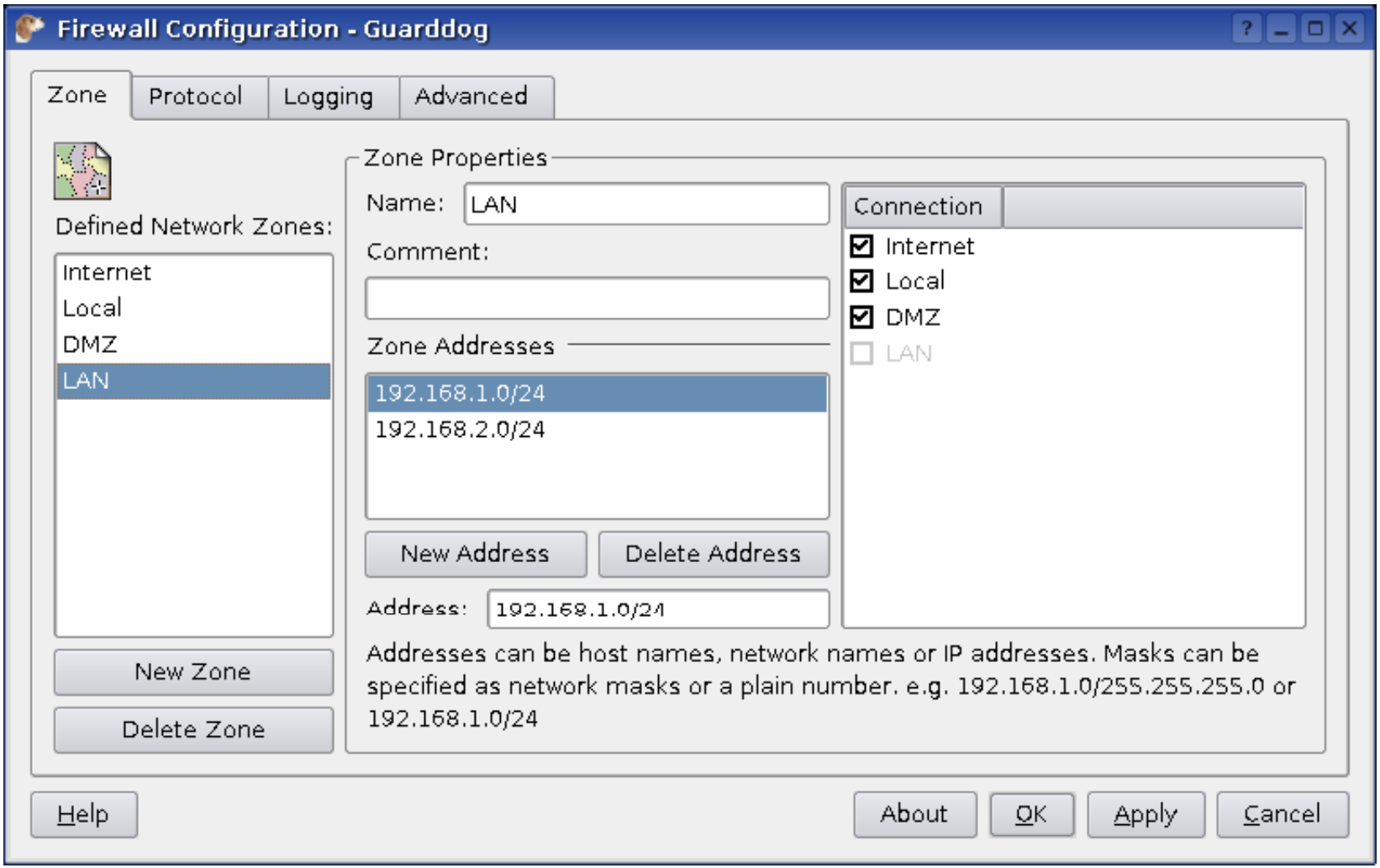
Guarddog

Guarddog is a firewall configuration utility for Linux systems

Features:

- Supports router configurations
- Firewall scripts can be imported/exported to be used on machines other than the current one
- Hosts/networks can be divided into zones
- It reduces the chances of configuration mistakes being made which are a prime source of security holes

Guarddog: Screenshot



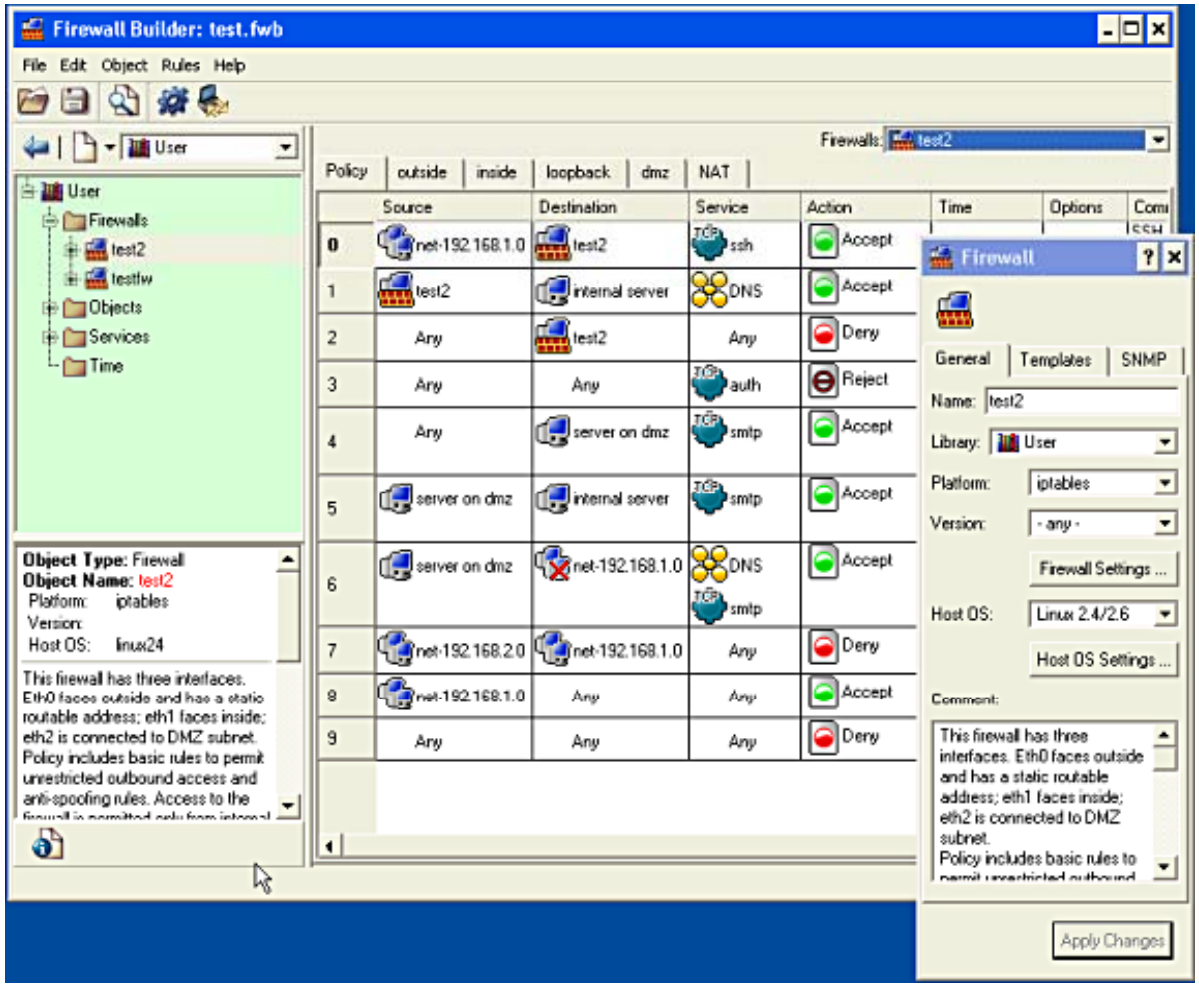
Firewall Builder

Firewall Builder is multi-platform firewall configuration and management tool

Firewall Builder currently supports iptables, ipfilter, and OpenBSD PF as well as Cisco PIX and Cisco IOS extended access lists

Firewall Builder can generate configuration file for any supported target firewall platform from the same policy created in its GUI

Firewall Builder: Screenshot



Mac OS X Firewalls

Flying Buttress

Advanced firewall configuration, logging, and IP sharing options are found in Flying Buttress

Features:

- Includes qualifiers on host or network addresses
- Operates on protocols other than TCP or UDP protocols
- NAT port forwarding or other custom NAT configuration
- Ability to switch between different firewall configuration sets quickly and easily

Flying Buttress: Screenshot

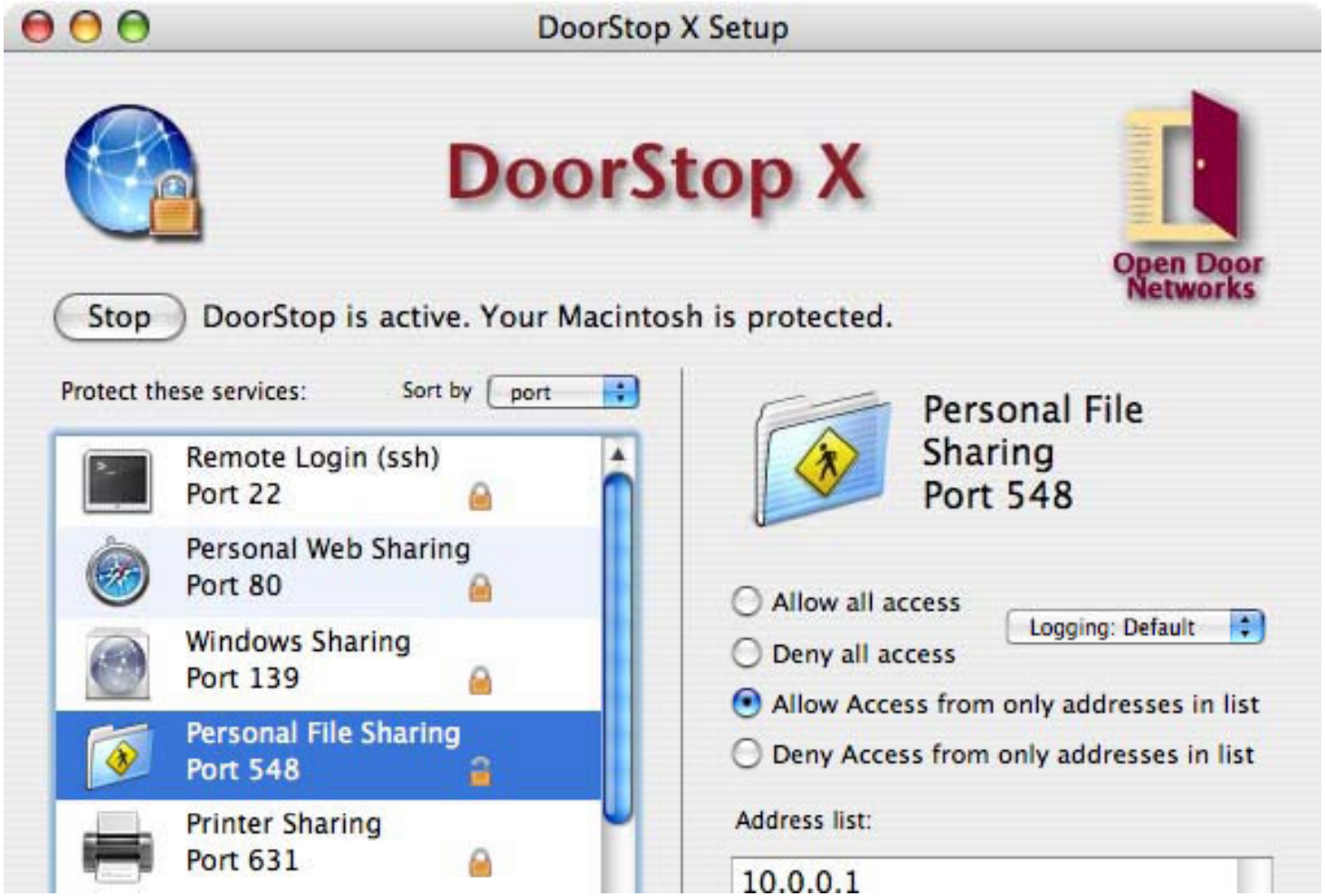
DoorStop X Firewall

Protects your Mac from outside attack, including specific Leopard protection

Features:

- All TCP services are protected by default
- Ability to tune protection on a service-by-service and address-by-address basis
- Protects services by name or port number
- Four protection modes: deny all, allow all, allow by address, and deny by address
- Setup assistant to help you best secure your Mac's services

DoorStop X Firewall: Screenshot



Intego NetBarrier X5

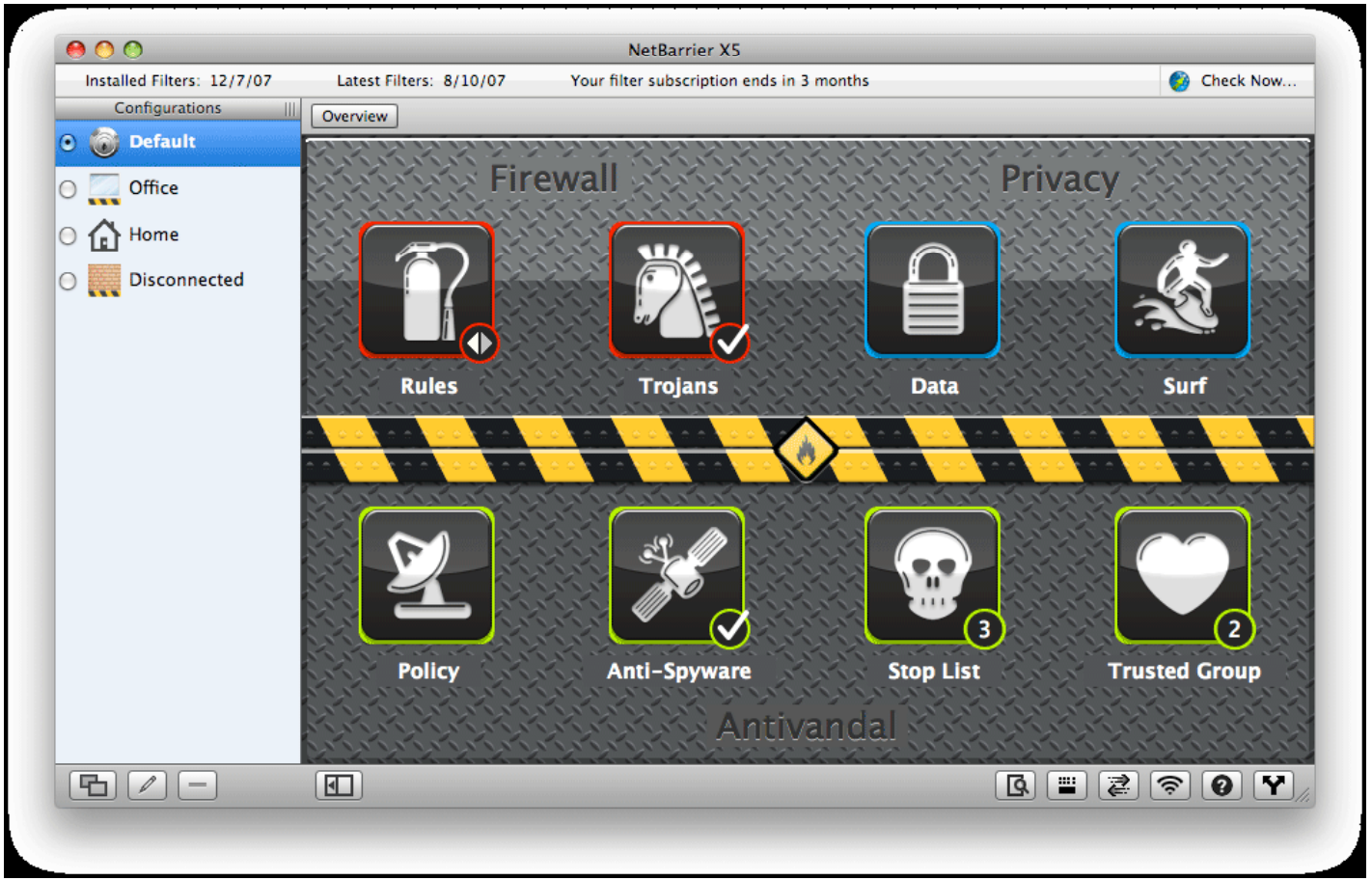
Intego NetBarrier X5 is the Internet security solution for Macintosh computers running Mac OS X

It offers thorough protection against intrusions coming across the Internet or a local network

NetBarrier X5 has four lines of defense to protect your Mac and data from intrusions and attacks

- Personal firewall
- Antivandal
- Privacy protection
- Monitoring

Intego NetBarrier X5: Screenshot



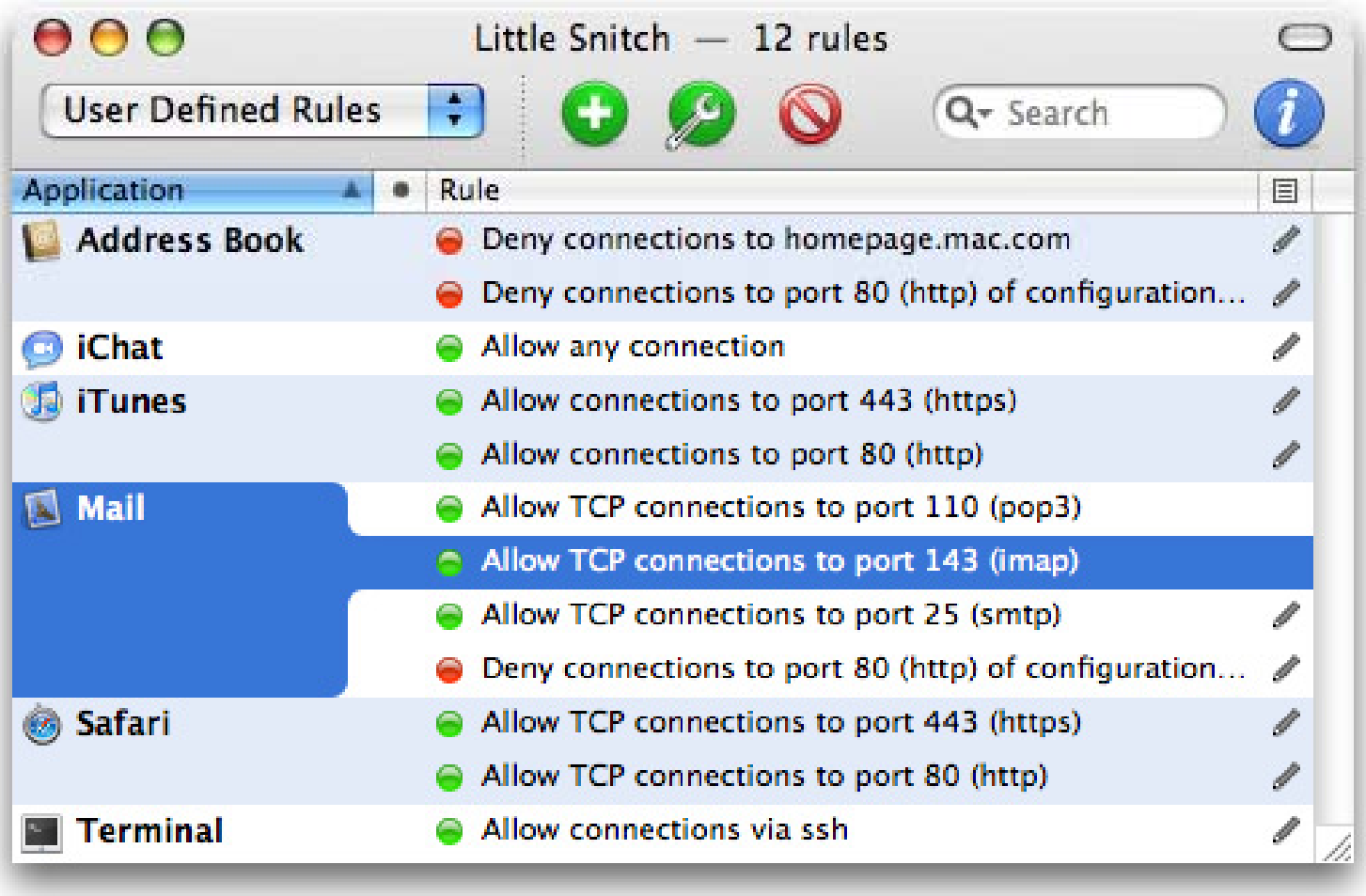
Little Snitch

Little Snitch provides flexible configuration options, allowing you to grant specific permissions to your trusted applications or to prevent others from establishing particular Internet connections

Little Snitch introduces a new network monitor, showing detailed information of all incoming and outgoing network traffic

Little Snitch allows you to intercept unwanted connection attempts, and lets you decide how to proceed

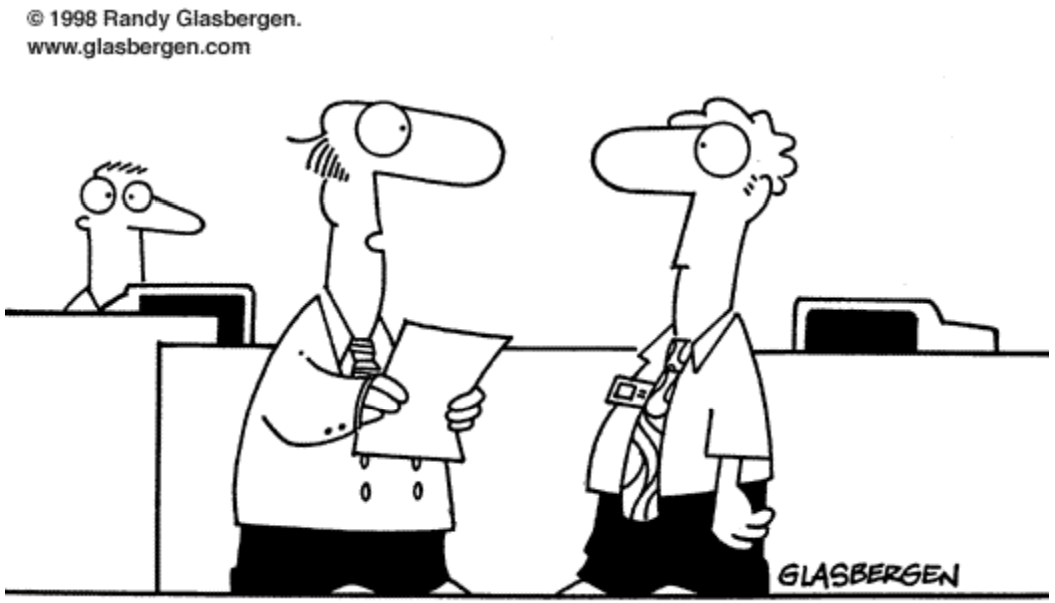
Little Snitch: Screenshot



Summary

- Firewall is a program which is placed at the network's gateway server
- Linksys scans the data travelling in the peer to peer network
- Cisco firewall series allows filtering the java applets which is a threat to the corporate resources
- Intego NetBarrier X5 is the Internet security solution for Macintosh computers running Mac OS X
- Guarddog is a firewall configuration utility for Linux systems
- Firewall Builder is a multi-platform firewall configuration and management tool

"According to new government safety regulations, employees must wear goggles and protective clothing when exposed to sharp criticism or cutting remarks."



"I believe it's important to be sensitive to the needs of our employees...but do we really need a paper cut support group?"