

McAfee Desktop Firewall

Proactively Defend and Control Corporate Desktops

McAfee® Desktop Firewall™ is an advanced application firewall with intrusion prevention capabilities that proactively defends and controls your desktop and laptops to prevent new threats that anti-virus alone cannot defend against. By providing comprehensive network and application firewall capabilities combined with intrusion prevention technology, Desktop Firewall prevents your systems from sending or receiving threats from unauthorized network traffic or applications. It also prevents your organization's authorized applications from being manipulated in order to send or receive threats across your network.

Reduced Total Cost of Ownership

Integrated Client Security

Desktop Firewall integrates with McAfee VirusScan® Enterprise and McAfee ePolicy Orchestrator® (ePO™), offering your organization integrated virus protection, global management, and reporting for even the largest enterprises. Integrated client security provides your company with smooth interoperability; complete protection against viruses, hackers, and threats; prevention of data theft; and reduced total cost of ownership.

Flexible Policy Management for Remote Systems

Connection-Aware Policies

Desktop Firewall can apply different firewall policies based on how a system connects to the network. For example, an administrator can create a VPN-based connection group, and Desktop Firewall only applies the associated rules when a user tries to connect to a VPN, thus ignoring any associated rules when the user connects to the network via some other connection method. This functionality provides administrators flexibility to define a firewall policy-based range of different connection criteria, including connection type, host IP address, target gateway, DNS, DHCP, and WINS servers.

Stop and Contain New Threats That Anti-Virus Alone Cannot

Packet Filtering Firewall

Desktop Firewall provides a packet-level firewall that can filter all incoming and outgoing network traffic. Desktop Firewall uses rules defined by your administrator and automatically learned rules to either block or allow network traffic. Packet filtering allows Desktop Firewall to prevent your systems from hosting an attack or receiving unauthorized traffic that could be a hostile attack. Desktop Firewall supports multiple network protocols including over 120 IP-based protocols. In addition, your

administrator can create policy for non-IP protocols including Wi-Fi (802.11x), NetBEUI, IPX, and AppleTalk. Multiple protocol rules provide greater levels of network security by filtering a broad range of network traffic.

Control Applications That Access the Network

Application Layer Firewall

Desktop Firewall provides an application layer firewall that can filter all applications that generate network traffic. Your systems administrator can prevent misuse and enforce security policy by controlling the ports and protocols used by trusted applications.

Prevent Unauthorized Programs and Enforce the COE

Application Monitoring

Desktop Firewall includes application monitoring providing the ability for your company to control and monitor applications. This prevents unauthorized applications from running or hooking themselves to other applications. Application rules can be manually configured or automatically learned and locked down to prevent change. Application creation rules prevent unauthorized applications from running.

An example of this is when legitimate software such as Instant Messenger creates a security risk by accessing the network, and threats such as Trojan horses, worms, Remote Access Trojans, or spyware programs result in system damage, loss of productivity, and loss of revenue. Application rules also enable your administrator to enforce the common operating environment (COE) by preventing your users from installing or running unapproved software and introducing additional security vulnerabilities. Application hooking detection prevents sophisticated attacks such as browser hijacking.

Prevent Insecure Systems Connecting to the Network

Quarantine Mode

Quarantine Mode allows Desktop Firewall to be interrogated by ePolicy Orchestrator before the client fully connects to the network. If the client is found to be out-of-date or running old policies, network access is restricted. Desktop Firewall and VirusScan Enterprise policies, software updates, and DAT files can then be enforced and your users released from their quarantine. Quarantine Mode protects your network from out-of-date anti-virus, Desktop Firewall software, and policies that leave your

systems vulnerable to attack. Quarantining your systems until they are updated limits your network security risks by keeping potentially dangerous traffic off your network.

Protect against Known Network Attack Techniques

Signature-Based Intrusion Prevention

Intrusion prevention provides Desktop Firewall with the means to detect behavior within legitimate network traffic, or application activity that indicates an attack on your systems. These are based on rules provided by a McAfee signature definition file. If Desktop Firewall identifies an inbound or outbound attack on your organization it can block the intrusion, alert, and log the event and prevent future attacks. Intrusion prevention allows Desktop Firewall to protect your users from attacks and prevents them from being used to attack others. Desktop Firewall is able to prevent many common attack methods such as IP Spoofing, Ping Flood, WinNuke, SYN Flood, and many more.

Global Policy Enforcement

Centralized Management

Desktop Firewall is available as a stand-alone solution ideal for small businesses or users that need to retain control of their own policies and an ePO solution for the enterprise. Integrated with ePO, your administrator can centrally manage Desktop Firewall from a single console. ePO can deploy and set policies for Desktop Firewall and send out regular product updates and policy changes. Centralized management provided by ePO enables your administrator to save money, time, and bandwidth by leveraging your investment in a single console to manage not only Desktop Firewall, but also your corporate anti-virus and viral vulnerability assessment.

Global Visibility

Graphical Reporting

ePO provides powerful enterprise-wide graphical reporting, including default or customer report templates. Default templates include: all intrusions, intrusion target and source, top ten attack targets, top ten intruders, and summary of intrusion based on type, year, month, or week. The reports allow your administrator to perform detailed analysis on network intrusions and attacks received, and identify the attack origin. In addition, ePO also allows your administrator to highlight issues, thus enabling rapid actions to resolve network security problems.

Simplified Enterprise Deployment and Policy Building

Auto-Learn and Audit Mode

Desktop Firewall can automatically learn activity without prompting your user to allow or deny rules. Your systems administrator can then perform a policy audit of Desktop Firewall to view the rules learned. Your policies can then be modified, locked down, and distributed to your users as a standard set of rules. Also, your administrator can rapidly build custom policies for your organization that may be replicated to your entire enterprise simplifying your policy deployment process.

McAfee PrimeSupport

McAfee PrimeSupport® is essential for optimizing the return on investment in McAfee System and Network Protection Solutions. McAfee's PrimeSupport team is ready to deliver the right resources for any service requirement.

PrimeSupport resources include:

- Delivery of all available maintenance releases and product upgrades
- Access to a comprehensive suite of online self-support capabilities
- Live telephone support 24/7/365
- Available assigned technical support account managers
- A complete range of software and hardware support solutions, tailored to any size organization

System Requirements

Note: The following are general system requirements and may vary depending on the nature of your environment.

Operating systems:

- Windows® 98 SE (Second Edition)
- Windows NT Workstation 4.0, with Service Pack 6 or later
- Windows NT Server 4.0, with Service Pack 6 or later
- Windows 2000 Professional, with Service Pack 2
- Windows 2000 Server, with Service Pack 2
- Windows 2000 Advanced Server, with Service Pack 2
- Windows 2003 Advanced Server
- Windows ME (Millennium Edition)
- Windows XP Home Edition
- Microsoft® Windows XP Professional

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com

McAfee® products denote years of experience and commitment to customer satisfaction. The McAfee PrimeSupport® team of responsive, highly skilled support technicians provides tailored solutions, delivering detailed technical assistance in managing the success of mission-critical projects—all with service levels to meet the needs of every customer organization. McAfee Research, a world leader in information systems and security research, continues to spearhead innovation in the development and refinement of all our technologies.

McAfee, Desktop Firewall, ePolicy Orchestrator, ePO, VirusScan, Protection-in-Depth, and PrimeSupport are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. The color red in connection with security is distinctive of McAfee® brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners. © 2005 McAfee, Inc. All Rights Reserved. 1-sps-f85-002-0405