



appGATE™
NETWORK SECURITY

AppGate Distributed Device Firewall For Windows™ systems

The AppGate Distributed Device Firewall is a system designed for both Windows™ workstations and servers. It consists of two components, the Device Firewall and a Policy Manager. The firewall is designed for remote administration and has no GUI for end users. The Policy Manager allows system administrators to define and distribute global policies for all AppGate firewalls in a network. With the Distributed Device Firewall, it is easy to manage and build a distributed protection system that fits both small and large enterprises.

Benefits

AppGate Device Firewall in combination with the Policy Manager offers many benefits:

- Central administration of a large number of firewalls running on user workstations and servers. Users of protected machines do not have to be system administrators and manage their own firewall settings.
- Two different policies can be distributed: one to use when the protected machine is connected to a Policy Manager and one that is used when it is standalone, for example when it is located outside the corporate network.
- Different policies can be defined for different groups of systems on the network.
- System administrators can make sure application servers only offer the services they are intended to. For example an internal web server should offer access only to the web server, not to any other services the operating system may want to publish to the network.
- The firewall can co-exist with other personal firewalls. All firewalls must approve the traffic before it is passed in or out from the system. An existing personal firewall with a graphical user interface can be combined with the centrally administered AppGate Device Firewall that governs the minimum level of protection for the machine regardless of what action the users take.
- If a virus or worm start spreading using a specific port, it can easily be disabled centrally by the system administrator.
- The firewall system can make sure that user workstations cannot communicate with each other. Many viruses and worms spread between systems through bugs or vulnerabilities in the operating systems. This kind of protection also stops users from accessing other users' workstations over the network.
- Policies sent to user workstations are signed and time-stamped by the Policy Manager to guarantee their authenticity.

Key features

- Easy to use and install with minimal end-user interaction.
- Controls all inbound and outbound traffic on all adapters and network interfaces.
- Powerful rule syntax allows detailed control of traffic.
- Automatic protection against malformed and illegal network packets, such as packets with strange IP options and small TCP header fragments.
- Rules allow "related states" to be defined, i.e. to allow new traffic based on whether other TCP sessions are established or not. This makes it easy to define rules for complex protocols.
- The firewall has no GUI, a feature that also suits well for network servers. The firewall can also be installed as a standalone firewall without the Policy Manager, if desired.
- The Policy Manager distributes policies and updates firewall rules in the network. Workstations can have different policies based on client type and network address.
- Mobile computers can have a restrictive default rule-set with rules guarding the workstation when no connection to a policy server is available, for example when it is used outside the corporate network.
- Multiple policy managers can be used to achieve redundancy and load sharing, if needed.
- Rules can generate both log entries and alarms. Alarms are entries sent to the Windows event log system, which can be inspected by remote system administrators.



No GUI for user interaction

The AppGate Device Firewall is designed without a graphical user interface on the client machine (user's workstation or network server). It is normally remotely configured by system administrators through the Policy Manager instead of letting local users be firewall administrators that have to make decisions about traffic filtering. Administration is normally done from one or more Policy Managers, although local administration is possible by local system administrator on standalone systems.

The AppGate Distributed Device Firewall system is ideal to use on public systems and systems used by many users, in schools and large organisations, on internal and external corporate workstations as well as on application servers.

The Policy Manager

System administrators have the possibility to define different policies based on system classes and IP addresses, for example to distribute different policies for user workstations and corporate servers on different networks. Several policy managers can also work in parallel. This enables a high degree of redundancy as well as offers load sharing on very large networks.

The policy manager is delivered as a software package. It runs on Windows, Unix and Linux systems and any other platform having Java version 1.4 or later installed. The policy manager should preferably run on a dedicated server and must, of course, have proper protection either by an external firewall or by the AppGate Device Firewall.

All configuration information and policies are text files. This makes the system easy to manage and scripts can be created to generate automated policies. All policies downloaded to clients are signed by the policy manager to prevent spoofing. The clients are able to verify that the policies they receive are current and authentic before installing and using them.

Policies and rule-sets

There are two different rule-sets that are distributed by the Policy Manager:

1. A rule-set that is active when the client has contact with a Policy Manager.
2. A rule-set which is used when no Policy Manager can be contacted ("a default policy" to fall back to).

The Policy Manager is normally placed on an internal corporate network to manage all internal workstations and Windows servers. To all clients, it distributes both rule-set #1 and #2 above. If a computer is moved outside this network and the contact with the policy server is lost, the default rule-set (#2) which normally is more restrictive, will automatically become active on that particular computer.

Use together with VPN systems

If used together with an AppGate VPN system, the Device Firewall can also be controlled by an AppGate Security Server to enforce specific policies when the user connects to a protected application server. It is, for example, possible for the AppGate Security Server to demand that all connections except the secure VPN tunnel should be closed before certain resources become available to the user.

The Distributed Device Firewall system can also be used together with non-AppGate VPN systems. If a policy manager becomes visible when the user connects to a remote network, the firewall will immediately request a policy from that server and start using it.



PC. Firewall

Application examples

User workstations should be protected and only allowed to receive and send the necessary traffic required to run its applications. This prevents internal hackers from gaining access to other users workstations and makes it much harder for viruses and worms to spread between workstations and servers.

Application servers: Servers connected to the Internet and all servers on the internal network need protection. Systems connected to the Internet are often controlled by the corporate firewall, but internal systems containing vital and possibly sensitive information are normally placed on the internal network without any protection. These systems can be attacked by users, viruses, worms and any other malicious software if not protected by a firewall.

Portable users: Attacks against portable users is a threat to many organisations since these computers are often moved between internal networks and the Internet. If not properly protected, they can carry malicious software from the outside to the inside. In addition, if the VPN system can verify that the firewall is running a specific rule-set, it can be the enabler that makes it possible to offer new applications to external users.

Specifications

AppGate Device Firewall client:

System requirements: Windows™ NT4, 2000 with SP2, XP, 2003 Vista and Windows 7. Administrator rights are needed for installation.

Supported adapters: All NDIS drivers that appears as connection-less 802.3 devices (Ethernet type): LAN, Microsoft® RAS (except on NT4), WLAN, etc.

Performance: Normally no noticeable performance degradation

Filtered protocols: IPv4, TCP, UDP, ICMP

Logs and alarms: Logs and alarms can be sent to a local file or to Windows event system.

Policies (rule-sets):
 1) Default
 2) when connected to a Policy Manager
 3) when VPN connections open to AppGate server

Policy Manager: Can update both rule-set (1) and (2) above

Compatibility: Can co-exist with other personal firewall products, if needed

Policy manager:

Server system: Windows, Unix, Linux or other systems. Requires server with Java 1.4 or later. The distribution for Windows platforms contains the Java environment.

Cluster support: Many policy managers can work together to support a large number of clients

Number of clients: One policy server can support more than 1000 clients

Administration: Administration is possible both through GUI and text files

Specifications may change without notice