



AppGate Distributed Device Firewall

The AppGate Distributed Device Firewall from Cryptzone works with the AppGate Security Server to protect the endpoint device and the network by controlling all inbound and outbound traffic on all adapters and network interfaces, and enforcing specific policies. The firewall is centrally managed and easy to install, and is designed for both Windows™ computers and servers.

Protecting workstations, laptops and servers against the viruses, worms and malicious hackers

Overview

Laptops and PCs that are not properly secured are vulnerable to attack every time a VPN connection is set up. They can carry malicious software onto the network, and are potential targets for attackers to use clients as gateways to gain access to the internal network. The AppGate Distributed Device Firewall from Cryptzone works with the AppGate Security Server to protect the user's device and the network.

The AppGate Distributed Device Firewall is a system designed for both Windows computers and servers. It consists of two components, the Device Firewall and a Policy Manager. The Device 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 build and manage a distributed protection system that fits both small and large enterprises.

Device Firewall

The AppGate Device Firewall is a stateful IP filter that protects the endpoint device from network based attacks by ensuring that the client can connect only to specific IP addresses on specific ports and by blocking unwanted connections to the user's workstation. The firewall checks all inbound and outbound traffic according to a well-defined firewall policy.

The firewall can use different policies depending on the circumstances. When used with the AppGate Security Server, the firewall can be configured to only allow network communication to the AppGate server while the user is connected. The AppGate Policy Manager can provide the Device Firewall with different rule sets depending on for example where the client is located. The administrator can also configure a default rule set which is used when the client is not in contact

with either an AppGate Security Server or an AppGate Policy Manager.

No user interaction

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

Policy Manager

The AppGate Policy Manager distributes policies to the AppGate Device Firewall. System administrators can define different policies based on system classes and IP addresses, for example for user workstations and for corporate servers on different networks. Several Policy Managers can also work in parallel. This enables a high degree of redundancy as well as offering load sharing on very large networks.

The AppGate Policy Manager is delivered as a software package. It runs on Windows, Unix and Linux systems and any other platform with 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. It distributes both rule-set #1 and #2 above to all clients. 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 the firewall is used as part of a VPN system that has been implemented with an AppGate Security System, the AppGate server can control the Device Firewall to enforce specific policies when the user connects to a protected application server.

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.

Features and Benefits

- **Centralized control:** Central administration makes it easy to manage large number of Device Firewalls running on user workstations and servers. 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.
- **Easy to use:** Powerful rule syntax allows detailed control of traffic. 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.
- **No user interaction:** The Device Firewall has no GUI, a feature that makes the system ideal for protecting network servers. Users of protected machines do not have to be system administrators and manage their own firewall settings. The Device Firewall can also be installed as a standalone firewall without the Policy Manager, if desired.
- **Protection online and offline:** 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 the device is standalone, for example located outside the corporate network and no connection to a policy server is available.
- **Different policies for different systems:** The Policy Manager distributes policies and updates firewall rules in the network. Different policies can be defined for different groups of systems on the network based on client type and network address.
- **High availability:** Multiple Policy Managers can be used to achieve redundancy and load sharing if needed.
- **System security:** 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. Policies sent to user workstations are signed and time- stamped by the Policy Manager to guarantee their authenticity.
- **Integration with existing firewalls:** The Device 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.
- **Prevents viruses spreading:** The Device 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. If a virus or worm start spreading using a specific port, it can easily be disabled centrally by the system administrator.
- The system automatically protects against malformed and illegal network packets, such as packets with strange IP options and small TCP header fragments.

Application examples

User workstations: The Device Firewall protects workstations by allowing the device to receive and send only the necessary traffic required to run applications. This prevents workstations communicating with each other, making it much harder for viruses and worms to spread between systems.

Application servers: 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 Device Firewall.

Portable computers: Attacks against laptops are a threat to many organizations 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 of the network.

AppGate Distributed Device Firewall Specifications:

AppGate Device Firewall client:

System requirements:	Windows XP, 2003, 2008, 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 an AppGate Policy Manager 3) when VPN connections open to an AppGate Security 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.



Microsoft Partner

Gold Independent Software Vendor (ISV)

Cryptzone solutions mitigate information security risks in the key areas of Policy Compliance, Content Security, Secure Access and Endpoint Security.

International Headquarters

Cryptzone Group AB
Drakegatan 7,
SE-412 50 Gothenburg,
Sweden

www.cryptzone.com
info@cryptzone.com

Regional Offices

Sweden
Tel: +46 (0)31 773 86 00

United States
Tel: +1.949.279.6177

United Kingdom
Tel: +44 (0)370 013 1600

Partner information:

For more information go to
www.cryptzone.com/partners