



***In a world with fewer borders, the demand for network security changes from security at the gate to security at the source. AppGate is the leader in this space with a solution that protects applications, communication and secures end-point devices. The AppGate solution supports all types of networks, fixed, wireless and mobile and is easily integrated into existing customer environments. The AppGate Security Server unifies all the necessary security elements such as authentication, authorisation, encryption, access control, client control, monitoring and reporting into one easy-to-manage, comprehensive solution.***

Networks are threatened in multiple ways, from virus attacks to unauthorised access. At the same time there is a demand for opening up the network for more flexible access. To be able to balance this equation, AppGate offers a flexible and powerful solution which can be tailored for both small and large enterprises.



The AppGate Security Server provides a wide range of functions:

- Encryption of network traffic with support for multiple simultaneous user authentication methods
- Compatibility with most third party authentication methods
- Roles and Rights Management. Flexible rules makes it possible to specify in detail how and under what circumstances each service should be available.
- User group membership in for example Active Directory can govern what rights users should be entitled to through the AppGate system
- Wide client platform support, from Windows, Mac and Unix/Linux systems to telephones and PDAs
- Client Check enables the security system to check or modify the client's configuration before granting access
- Easy to use portal-like user interface. The system requires virtually no user training.
- Clustering of servers for performance and high availability
- Possibility for remote applications to securely print to locally attached printers
- Roaming functionality in client offers automatic reconnect if the network link goes down. It can even handle change of IP addresses. Roaming is transparent to running applications.
- Single sign-on functionality enables easy authentication to many applications
- AppGate server can function as a firewall in many situations when building networks, reducing deployment costs
- Built-in secure Instant Messaging (IM) functionality

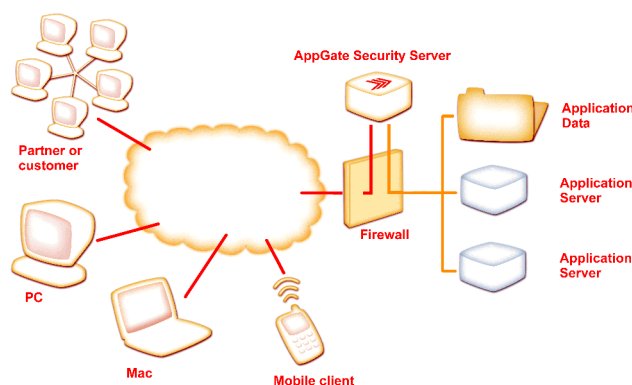
## AppGate Security Server

The AppGate Security Server main function is to control user access to protected resources. It is equally well suited to control remote access to a site as controlling local access to servers on corporate networks. It has a powerful authorisation database that contains rules for what applications and services should be available to users. User accounts and user roles are in larger installations normally defined in external third party servers such as Active Directory, LDAP or Radius servers but can, if desired, also be defined in the AppGate system database. The AppGate Security Server supports simultaneous use of different authentication methods for maximum flexibility.

The powerful authorisation system allows complex rules for access to be defined, for example that users on the corporate LAN may access a service during office hours using password authentication but that remote users need to use a certificate for authentication and must have a personal firewall installed for the same service to be available. It is possible to define for each service exactly what users and under what circumstances it should be available. Services can be grouped in folders and folders may contain other folders, i.e. a tree-like structure can be defined to facilitate administration and to get a comprehensive view of the services offered by the system.

Remote administration of the system is possible and different administrator roles can be defined. All user and administrator activities are logged by the system and system logs can be very detailed, for some protocols it is possible to log everything down to every byte being transferred. Many different types of alarms can be defined and be sent to external systems for immediate action through SNMP, Syslog, email, pagers, etc.

The AppGate Security Server is delivered as an appliance in a turnkey package, a robust server with all necessary AppGate functionality pre-installed. A single unit suits smaller enterprises whereas a cluster of units can support virtually an unlimited number of users. For more information about available models, please see the "AppGate Appliance" product sheet.



The server has built-in firewall functionality for complete protection of itself and the application servers behind it. It is also possible to define firewall rules to allow, for example, an application server on a network behind the AppGate server to access another service located on the other side of the AppGate server. This can in many cases reduce the complexity when building secure networks and reduce deployment costs.

## Clustering and redundancy

The AppGate system supports server clustering for scalability and redundancy. The system scales almost linearly: adding a second server results in twice the performance and so on. Clustering makes the system ideally suited for internal use on corporate networks since high performance is not a problem.

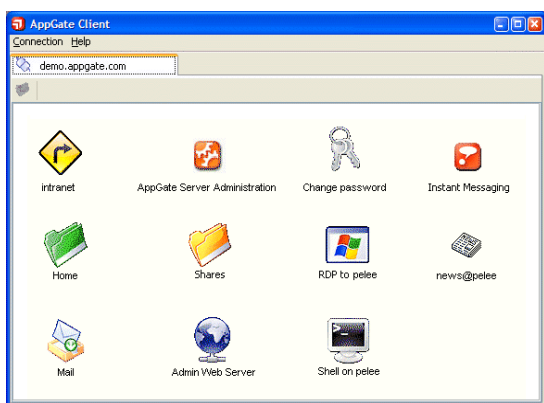
Clustering can also be used for redundancy reasons. It is possible to have two or more network connections for example from the Internet where clients automatically, and invisibly to the user, will try different IP addresses until they succeed to connect to the system. This will take care of all types of communication problems with the system.

The AppGate system is easy to deploy and maintain. Application servers need not be modified and traffic can be compressed to increase performance on slower links and reduce communication costs for devices where users are charged for the amount of data being transferred.

## Clients

The clients support a wide range of system platforms from large servers to desktop computers, telephones and PDAs. There are different clients to choose from: **AppGate Client** which is the "standard" client, an **Applet client** designed for download at Internet kiosks and a **Mobile Client** for PDAs and telephones.

The AppGate Client has a portal-like GUI. It is very intuitive to use and is very appreciated by users since it also displays the currently available services and offers a good overview of what remote resources are available.



All client to server traffic can easily navigate through firewalls, Network Address Translation (NAT) devices, proxy servers or other network components. The AppGate client can be configured to support all kinds of IP traffic such as TCP, UDP and ICMP. For more information about the clients, please consult the "AppGate Clients" product sheet.

## Full client control

The AppGate Security Server can send customised commands to be executed on the client computer. This "client check and client command feature" makes it possible to examine and see and even change how a client is configured before access is granted to all application services.

The AppGate Personal Firewall is an add-on product for Windows workstations. It has no GUI for end-users and is centrally administered through an AppGate Policy server. The AppGate Security Server can also demand that a specific rule-set is active before certain services become available to the user. For more information about the personal firewall, please see the "AppGate Distributed Personal Firewall" product sheet.

## Technical specifications

### General:

Protocol:	SSH v2 with server authentication and integrity protection
NAT	Insensitive to Network address translation (NAT). Only a single TCP connection to the server is needed for the encrypted tunnel.
Proxy traversal:	Support for HTTP and Socks 4/5 proxies
Keep-alive packets:	Can be sent regularly to keep links up
Ciphers:	AES (128, 192 and 256 bit keys), Arcfour/RC4 (128 bits), Blowfish (128 bits), 3-DES-CBC (168 bits)
Server authentication:	1024 bit server keys are verified according to the DSS standard (FIPS-186) or using X.509 certificates
Key exchange:	Diffie-Hellman with SHA-1
Data integrity:	HMAC-SHA1 (RFC-2104) or HMAC-MD5
Compression:	ZLIB LZ77 (RFC-1950/1951)

### Server:

Protocol:	SSH v2 to clients. IPsec encryption to application servers supported.
Administration:	Remote administration through GUI or command line interface. Admin roles with different privileges.
Load sharing:	Server clusters supported
External user DB:	LDAP v3 (RFC 2251-2256, 2829-2830), Active Directory, Radius, SecurID, etc.
Address translation:	Internal IP addresses need not be visible externally
Logging:	Syslog, alarms, AppGate log, SNMP

### Clients:

Operating systems:	Windows (all versions), Unix, Linux, Mac OS X plus other Java enabled platforms such as many PDAs and mobile phones.
Native crypto:	Clients on Windows, Solaris, Linux and HP-UX has native code for increased performance
Tunnelled traffic:	TCP (UDP with IPTD module installed)
Authentication:	Passwords, LDAP, Radius, Token cards, RSA SecurID™, Certificates/PKI from VeriSign, Entrust, etc. Smart cards and biometric authentication may require third party products.
Terminal:	Integrated terminal emulator for secure terminal access to servers

*Specifications may change without notice*