



AppGate Security Server Overview

The AppGate Security Server from Cryptzone provisions secure, controlled access for authorized users working from any device, and from any location. Strong security protects network resources from internal and external threats. The built-in features make AppGate an all-in-one solution that is both easy to use and easy to manage.

Secure access for all users

The AppGate Security Server solution from Cryptzone allows users to access network resources through a secure connection over any type of network connection. Users can initiate the secure connection from virtually any type of device: a Mac or Windows PC/laptop, Unix-based workstation, shared computer, or Smart Phone, using a browser, installed client or USB client.

Employees, home-workers, partners, suppliers, and customers can access the resources they need without any conflicting security or access issues. AppGate creates a secure connection between the endpoint device and the AppGate Security Server. All client-to-server traffic can navigate through any firewall, NAT scheme or any other network component.

Security is treated the same way regardless of the user's location. Access to individual network resources and services is granted to authorized users on a needs-only basis. Roles can be assigned to provide access only to the services that are relevant to the user's job and location.

Controlling user access

The AppGate Security Server's main function is to control user access to protected resources. It is equally well suited to controlling remote access to a site as it is for controlling local (LAN) access to servers on corporate networks.

Features and Benefits

- **Encryption:** All traffic is encrypted between the servers and the endpoint device.
- **Authentication:** The Cryptzone OTP is built-in as standard and AppGate supports most third party authentication systems including LDAP, Radius, or SecurID servers (RSA ACE/Server), and certificate authentication for PKI deployments. It can support multiple, simultaneous authentication methods.
- **Client platform support:** AppGate supports a wide range of client platforms from Windows, Mac and Unix/Linux systems to smartphones and tablets. True client-less access through web browsers' SSL support.
- **Client check:** The security system can check or modify the client's configuration before granting access to services.
- **Single sign-on:** AppGate enables easy authentication to many applications, for example web services, Terminal servers (RDP, Citrix) and file access.
- **Roaming:** The client can automatically reconnect if the network link is lost or changed, or the IP address changes.
- **High availability:** AppGate servers can be clustered to ensure high availability, even across different locations, making the system ideally suited for business continuity.
- **Network segmentation:** Internal security domains can be created to protect critical assets eg. PCI at-risk servers.
- **Data compression:** Data compression reduces the number of data packets transmitted, increasing performance over slower links and reducing costs for mobile devices where users pay per byte sent.
- **Central administration:** AppGate provides a single, central point for defining and managing security policies. Changing user access rights can be done from one central location like Active Directory.
- **Secure mobile access:** Traffic can run over any transmission: fixed, wireless, GPRS or 3G. The solution supports a wide range of mobile platforms including Nokia Series 60 (Symbian), Windows Mobile, Android and Apple's iPhone.

Enabling
all users to
access systems
securely
anywhere,
anytime, from
any device

The powerful authorization database contains rules for controlling which applications and services should be available to each user and under which circumstances: for example, users on the corporate LAN may access a service during office hours using password authentication, while remote users need to use a certificate for authentication and must have a personal firewall installed for the same service to be available.

AppGate integrates with existing infrastructure including Active Directory, LDAP or Radius Servers to streamline administration of users' roles and access rights. Remote administration of the system is possible and different administrator roles can be defined.

Protection from internal and external threats

Instead of relying on network perimeter security, AppGate focuses on protecting the corporate assets. Therefore all users, regardless of their location are authenticated before any access is granted. End to end encryption of all traffic including login details protects the system from phishing or man-in-the-middle attacks.

AppGate can block all access to servers until the user has been authenticated and authorized. If a user is not authorized to use a particular resource, that resource remains invisible thus minimizing the risk should an unauthorized user manager to connect to the network.

Protection of core systems

Many organizations with mission critical systems run two networks to prevent unauthorized access to critical systems. The Appgate access control system simplifies the task of managing access between these two networks.

Up to twelve internal security domains or segments can be created (more with Vlans) to protect specific

assets eg. development data or PCI at-risk servers. All access requests from users to application servers on these networks will be checked and controlled. This reduces the need for internal firewalls and provides more functionality and granular control than traditional firewall technology.

Reducing network complexity

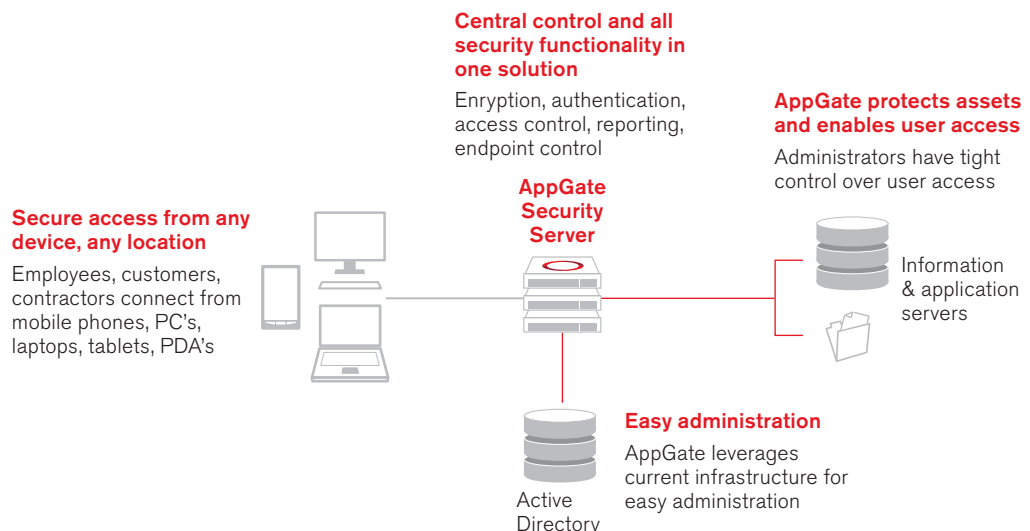
The AppGate Security Server combines strong authentication, authorization, encryption and access control in one system. It replaces many of the point products traditionally used for network security and, as a result, network configuration is simpler and easier to manage.

The server has built-in firewall functionality for complete protection of itself and of the application servers behind it. It is possible to define firewall rules to allow, for example, an application server on one network controlled by an AppGate server to access a service located on another network.

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 demanding environments since high performance is not a problem.

Clustering can also be used to achieve redundancy. If, for example, a corporation has two AppGate servers in two different locations offering access to the same services, the AppGate clients will automatically, and invisibly to the user, try different IP addresses until they succeed to connect to the system. This will take care of communication problems regardless of where the failure occurs.

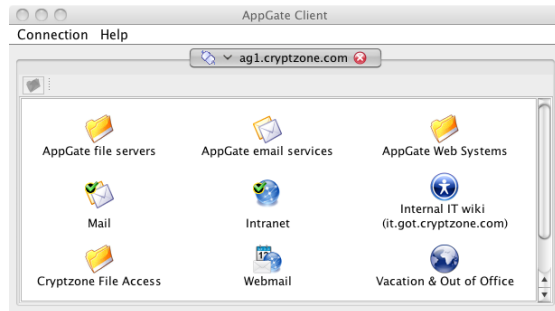


AppGate unifies all the necessary security elements including authentication, authorization, encryption, access control, client control, single sign-on, monitoring and reporting into one easy-to-manage solution.

Clients

The clients support a wide range of system platforms from servers to desktop computers, smartphones and tablets. There are different clients to choose from: The AppGate Client is the standard client; the Mobile Client is designed for mobile devices ranging from PDAs to iPhones, iPads and smartphones; the USB client is pre-packaged on a USB flash drive; and SSL access to web based services is possible through a web browser.

The AppGate Client has a portal-like GUI. It is very intuitive to use and is appreciated by users since it offers a simple overview of what services are available.



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 see the "AppGate Supported Clients" data sheet.

Mobile VPN

Traffic can be run over any transmission: fixed, wireless, GPRS, or 3G. AppGate supports a wide range of mobile platforms including Nokia Series 60 (Symbian) and Windows Mobile and will support Apple's iPhone®.

By using the most efficient standard protocols, as well as compressing all traffic, AppGate ensures efficient use of bandwidth, reducing costs and creating a very good user experience. Configuration and set up of mobile devices is automated and can be provisioned remotely.

End Point Control

It is possible to send customized commands to be executed on the client computer. This "client check and client command" functionality makes it possible to examine and even change how a client device is configured before access is granted to all application services.

The AppGate Device Firewall is an add-on product for Windows workstations. The firewall has no GUI for end-users and is centrally administered through an AppGate Policy server. The AppGate server can also demand that a specific rule-set is active before selected services become available to the user.

For more information about the firewall, see the "AppGate Device Firewall" data sheet.

Secure local printing

Secure printing can be a problem if the user is on a different network to the one hosting the application. AppGate's Secure Local Print module enables users to print on their local printer wherever they are working.

Full reporting for monitoring and compliance

All servers in an AppGate cluster are administered as one entity. The system can be remotely administered using a powerful GUI-based console application that offers graphical views of the system, its configuration and status.

All user and administrator activities are logged by the system and these logs can be very detailed. Many different types of alarms can be defined and be sent to external systems for immediate action through SNMP, Syslog, email, SMS, etc.

Appliances

The AppGate Security Server is available in different forms, including virtualized appliances, small rack mountable units for small/mid sized enterprises and clusters of multi-core units that can support a virtually unlimited number of users. For more information about available appliances, please see the "AppGate Security Server Appliances" datasheet.

AppGate Security Server Technical Specifications

General

Protocols:	SSL 3.0/TLS and SSH v2.
Proxy traversal:	Supports Socks 4/5 proxies and HTTP proxies. Also supports Basic and NTLM authentication in proxies (e.g. ISA servers).
Keep-alive packets:	Can be sent regularly to keep links up.
Supported ciphers:	AES (128, 192 and 256 bit keys), Arcfour/RC4 (128 bits), Blowfish (128 bits), 3-DES-CBC (168 bits).
Server auth.:	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 and HMAC-MD5 (RFC-2104).
Compression:	ZLIB LZ77 (RFC-1950/1951).

Server

Protocols:	SSL 3.0/TLS and SSH v2 to clients. IPSec to application servers are supported.
Administration:	Remote administration through GUI and command line interface and administrator roles with different privileges.
Clustering:	For load sharing and redundancy.
External user account databases:	LDAP v3 (RFC 2251-2256, 2829-2830), Active Directory, Radius, SecurID, etc.
NAT support:	Internal IP addresses on protected networks need not be visible externally.
Logging:	Syslog, alarms, AppGate log, SNMP.

Clients

Operating systems:	Windows, Unix/Linux, Mac OS X, tablets, smartphones and most Java enabled platforms. For details, please see "AppGate Clients" product sheet.
Native crypto:	Clients on Windows, Solaris, Linux and many mobile platforms have native code clients.
Tunnelled traffic:	TCP (and UDP with IPTD module installed).
Authentication:	Passwords, LDAP, Radius, token cards, RSA SecurIDTM, Kerberos, certificates from VeriSign, Entrust, etc., one-time SMS passwords.
Smart card support:	Support for MSCAPI and PKCS #11 certificates. Third party software to interface with smart card may be required.
Client-less access:	Web browsers' built-in SSL support can be used for client-less access to web-based services.

Specifications may change without notice

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

The AppGate solution from Cryptzone enables organizations to provide controlled access for all authorized users regardless of their location whilst also ensuring network resources are protected against internal and external threats. This award-winning technology combines an application layer firewall with device security and granular access control system in one easy to use, cost effective system.

Cryptzone Group AB
Drakegatan 7,
SE-412 50 Gothenburg,
Sweden
Tel: +46 (0)31 773 86 00

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

United States
Tel: +1.949.279.6177

info@cryptzone.com
www.cryptzone.com