



Secure Access for Smart Devices



AppGate Client

Mobile devices expose businesses to a number of security threats

Smartphones - an essential business tool

There's been an exponential growth in smartphone sales in recent months as people have recognized the potential benefits of these devices for work as well as personal use. Today's smartphones are effectively mini-computers with more power and capability than the desktop computers still in use in some organizations. They are flexible and convenient, and now have the specialized tools to enable people to browse the Internet or intranet, manage documents, and communicate via email, IM, VoIP and phone. As a result, smartphones are no longer just a 'cool' gadget but are increasingly seen as an essential tool for business.

But how secure are mobile devices?

More and more employees are using smartphones interchangeably for personal use and for work. As a result it is easy for the security risks associated with mobile phones to be overlooked.

The reality is that mobile devices expose businesses to a number of security threats, increasing the risk of unauthorized network access, data loss and compliance failure. Intercepted communications can reveal log-in details or other sensitive information; software downloads can introduce malicious software onto the network; and if the device is lost or stolen, confidential data stored on the phone can fall into the wrong hands.

Organizations need to ensure that mobile phones are not the security exception in the

corporate infrastructure. The AppGate solution from the Cryptzone Group enables businesses to treat security for smartphones such as the Nokia N95 or iPhone in exactly the same way as a PC or laptop on the network, with the same security policies and rules of access applied to all devices.

AppGate enables users to work securely from any smartphone

The AppGate solution can provision secure access from any device including desktop computers, servers, laptops, mobile phones and tablets. With AppGate, users can access data in a secure way from any smartphone device including Apple iPhone and iPad, and Android phones.

The AppGate solution is a complete identity management and access control system, integrating all necessary security, VPN and access management functionality into one easy to manage solution.

Mobile clients

AppGate clients are available for Windows Mobile, Nokia Series 60 (Symbian), Apple iPhone and iPad, and Android devices. All configuration and set up of the phone can be automated and provisioned remotely.

Secure communications

All traffic, including login information, is encrypted end-to-end between the AppGate Security Server and the mobile, protecting the system from phishing or man-in-middle attacks. The information never passes through a third party unlike many common "push" solutions.

Two factor authentication capability is built-in as standard

Strong user authentication

AppGate supports a range of authentication methods including password, Radius and SecurID, and chained authentication.

Two factor authentication capability is built-in as standard, providing another layer of security to your system to reduce the risk of unauthorized access. Automatic SMS authentication using one-time-passwords can be used to streamline the process for users.

Feature-rich mobile working

AppGate's full mobile VPN solution makes it possible to enable feature-rich applications on mobile devices, unlike "push technologies" which offer only email-centric functionality.

Prevent information leaks

When the smartphone is connected to the AppGate Security Server, all traffic flows through the secure VPN connection, avoiding split tunneling and reducing the risk of a data leak. The optional mobile web filter module can be used for Windows Mobile devices to control users' direct access to the Internet without having to pay for a private APN.

Managing user access

Powerful rules & rights management tools give administrators complete control over user access permissions. Policies can be defined to limit access for each individual user depending on criteria harvested from the end-user device. For example: a device that does not have an encrypted disk may only be allowed web access to prevent information from being downloaded and stored unsecured. Restricting user access to specific resources on a server also significantly reduces the security risk should the connection be compromised or any malware be unintentionally introduced via the mobile device.

Technical Specifications

The AppGate solution comprises the AppGate Security Server, which is usually located in the office network, and client software installed on the user's mobile phone. In cases where no specific client exists, then there is also a browser-based SSL-VPN option available for users. The AppGate Security Server controls the access to the host network. It is designed to operate through a single open port in the firewall. Once set up, all connections to the mobile users are effectively multiplexed through this one connection to the AppGate Security Server. This eliminates the need to change firewall rules and makes the mobile solution easier to deploy and maintain. The appliance is available in a range of sizes providing support for just tens of users up to more than a hundred thousand concurrent users.

System Requirements

Currently the AppGate solution supports Windows Mobile Classic, Symbian and Android based mobile phones as well as iOS based devices like iPhone and iPad. The AppGate solution is based on the OpenSolaris operating system allowing customers to choose whether to run AppGate as a virtualized server or purchase an AppGate appliance pre-configured for their business.

Policies can be defined to limit access for each individual user

Key Features

- Easy to use, easy to manage
- Secure communications end-to-end
- Protection against unauthorized access to the network
- Protection against information leaks
- Reduces operating costs
- New apps for iPhone, iPad and Android phones

