



**SOLUTION PAPER
REMOTE ACCESS**

Remote Access with AppGate

SECURE - SIMPLE - FLEXIBLE

Introduction

Gone are the days when different access systems were needed for different users, different devices and different applications.

Remote Access is something all users would like to have. But it also creates a nightmare for the system administrator. Why? Because users do not want to be limited to a particular device or location or even a specific application. They definitely do not want to access applications differently when they work outside the office. Web interface on their e-mail applications? No thanks! From the system administrator's point of view this creates a number of security challenges. How secure are mobile devices? Does the device actually have the required functionality or does it need to be updated? Are the configuration settings O.K.? What kind of information should the user be able to access? It should depend on which type of device and authentication system he/she is using, who the user is, the time of day, type of device, and many other variables. And how can this be done with minimal user interaction so that support calls are held at a minimum? AppGate Remote Access functionality helps to address all those problems and many more in a secure, flexible way.

AppGate – not just another point product

With the AppGate Secure Access Platform, it is possible to get rid of many different products and replace them with a single solution without having sacrifice security or pay more. In fact with an AppGate server the security level will rise and the cost go down. On top of that, it will be possible to manage all accesses from one place! The AppGate server includes the following functionality:

- Replaces existing IPSec, SSL and Mobile VPN's
- Acts as a firewall and protects applications from unauthorised access. This minimises the need for internal firewalls.
- URL-filtering: instead of building multiple web sites, the AppGate server can give users secure access to individual web pages based on their role.
- Single Sign-On enabling
- Network Access Control
- Device Check Management
- Support for VoIP

Intelligent use of technology

Using the AppGate SSL module, normal web browsers and their built-in SSL support can be used to access web based services without having to download or install any software on the client at all. The SSL module makes it possible for users to be able to always reach information from the protected system regardless of location and system being used. The system administrator will also know that all accesses are done in a secure and controlled way. By adding the SSL module to the AppGate security system, instead of having different systems

for different types of access, all accesses will be managed from one system, the AppGate concept of Single-Point of Power. This saves money and effort and by using only one security system it is also possible to know how the system works which will lead to increased security. AppGate's efficient use of bandwidth and possibility to compress traffic also maximises the capacity of the company's Internet connections, further reducing costs. The traffic can run over any transmission, fixed, wireless, GPRS or 3G.

Authentication, Policies, Roles and NAC

One of the biggest problems for a system administrator is how to authenticate people and give them access to the right information based on different criteria. Often the organisation has legacy systems that have to be used and an infrastructure not originally designed to permit Remote Access. AppGate supports many authentication systems out of the box: smart cards, token cards, SMS-authentication, certificates or passwords. Most of them are actually device independent, so with AppGate they can be deployed as an authentication method for all devices: mobile devices, Internet café PC's and for the ordinary laptop. It is even possible to use multiple authentication systems at the same time, enabling the system administrator to define the user's level of access depending on the level of authentication used. And it is of course possible to connect the AppGate server to an existing AD, LDAP or Radius server.

The concept of roles in an AppGate system is very advanced, making it easy to give or deny network access. A Role is defined as a selection of services that a user can access depending on how they authenticate themselves, how secure the device is that they are using, whether it is a mobile, and if the device is owned by the company or not. For example, when a user is using a company PC, visits an Internet café PC or uses a mobile phone, he/she can use the same secure token for authentication but may only get access to some web services on the café PC for security reasons. Using the same authentication method on the mobile phone, he/she may get access to email and the Intranet but many other services such as mounting file shares may not make sense on these devices, and will therefore not be available. All of this happens without the user having to make any decisions. Of course it is possible to give role-based access to groups such as sales people or management.

Policies are easy to define but traditionally hard to implement. AppGate solves this issue as well and the possibilities are almost endless. It is possible to define almost any rules that control access to applications, for example:

- Whether the client system belongs to the organisation or not
- Whether it has the latest antivirus system (if not the PC can be automatically directed to a site where the latest version can be downloaded)
- The IP-address of the connecting device
- Time-of-day
- Who the user is
- What operating system is on the device
- Or anything else the system owner would like to know about the client system

All of this can be done without having to have a pre-installed client!

So AppGate makes Remote Access easy for the system administrator, but how simple is it for the end user? This is another area where AppGate differs in many ways from other vendors' solutions. First of all, it is possible to check if the connecting device is properly set up using AppGate's diagnostic tool. This tool checks the PC and, based on the results, instructs the user about what to do next. An example of this is checking if a client has the latest version of software installed and instructing the user on how to download the latest version.

Another example of how user friendly the AppGate system is for the end user is the use of the native application. Rather than having to use a web-based version of the application, with AppGate it is possible to work in the same way from home as in the office – very convenient, especially for laptop users. The most important part of the user interface is the dynamic portal interface where all applications that the user can access are shown as icons. If the user cannot see an icon for a service or application, it is not possible to access the application! This reduces the number of calls to the help desk since the users can see what they can access and will in most cases realize that there are reasons for a service to not be available. In most other systems, the user gets no feedback and when the user starts an application and it does not work, then the user does not know whether it is a result of a malfunction of the application, malfunction in the remote access system or if he/she simply does not have the access rights.

Integrated Device Firewall

An issue that is often overlooked is that a single insecure device can make a whole VPN system insecure. When a client is connected to the VPN server it is a good target for attacks. AppGate addresses this problem by offering an integrated device firewall which works in combination with a Policy Server and the AppGate Security Server. The AppGate Device Firewall is not intended to replace an already installed personal firewall. It actually works in conjunction with personal firewalls and is designed to do something they do not do. For the user the Device Firewall should be transparent since it does not have a GUI. This means that the users do not have to be firewall administrators and make decisions about traffic filtering. When the user is connected to the Internet but without any connection to the AppGate server, a simple basic rule set is enforced. When he/she connects to the network, a new rule set is automatically downloaded as determined by the system administrator. An example of a commonly used rule set is to only allow encrypted traffic when the user is connected to the corporate network. And if the user wants to access the Internet when connected to the corporate network, he/she has to go through the company firewall.

Another obstacle with conventional firewalls is what happens when the user moves to the network inside the company's firewall - if there is an active rule set operating this may cause problems with the internal network. With the AppGate device firewall, the rule set is automatically set to zero (or something else that the system administrator decides). Again the user

does not have to interfere at all and does not have to make any security decisions.

Scalability, logging, performance and licensing

The AppGate solution is designed to meet the needs of any enterprise, from small user installations up to large corporate-wide installations with tens of thousands of users. This is solved by using different server sizes and the ability to cluster servers. This approach makes it easy and cost effective to start with a smaller solution and add more users and servers as the requirements change. It also ensures that there is always enough performance even when the most challenging applications are used through the AppGate Server. Most of the time it is just a question of installing a license key when more users need secure access without having to change any hardware.

Logging is an important tool for any system administrator, especially now when compliance with different regulations and laws has become something that everybody needs to care about. AppGate provides an outstanding ability to control and monitor almost everything that happens on the network. Who did access what from where and when? What services have been used last week? What IP addresses have been used in failed login attempts? Everything is logged!

AppGate charges for concurrent users only. Even in an organization with thousands of users, only the ones that connect to the AppGate Server will be charged for. If the users and the servers are at different locations (very common in a distributed network) or one AppGate Server needs to be in one location with another AppGate Server in another location? No problem: from a price perspective this is still treated as one installation.

On top of the license fee AppGate has one of the industry's most generous support agreements. Not only do you get support tailored to your needs but the support cost also includes all new releases and updates from AppGate, minor or major!



For more information please visit us at www.appgate.com or send us an email at sales@appgate.com



appGATE™
NETWORK SECURITY



www.appgate.com