appGATE™
NETWORK SECURITY

APPGATE
TECHNOLOGY

UNIFIED

TECHNOLOGY

Introduction

The AppGate solution truly delivers holistic security and access control where other approaches fall short. It is designed to address the security and functionality needs created by two of the most game-changing trends in today's business world - increased workforce mobility and increased collaboration with worldwide partners and customers.

AppGate's security architecture was designed with two principles in mind:
1. Everyone inside the network is not necessarily trustworthy, and
2. Everyone outside the network is not necessarily untrustworthy.

The revolutionary AppGate solution is designed so that protection of IT assets occurs as close as possible to the enterprise assets.

The Difference

The difference between the traditional IT approach to security (one firewall which acts as a perimeter) and the AppGate approach can be described with an analogy to "gated communities." In these neighbourhoods, one cannot just waive their pass to the security guard at the gate and then walk into any house in the community. To get into one's home, one needs to have the right key to open the lock. In just the same way, rather than having a user go through the firewall (i.e. the security guard at the gate) and allowing access to all IT assets (i.e. all homes in the neighbourhood), the AppGate solution puts a lock on each IT asset, such as the CRM system, accounting system, or development application (see figure below). As a result of this method, AppGate safeguards all content inside the network not only from external threats, but also from internal threats. By attaching a security system in front of application servers and treating external security no

differently than internal security, the AppGate solution allows users to request and access corporate assets through an encrypted link from any Internet connection, whether it be from home, office, or a remote wireless connection. Additionally, with the AppGate solution, users may initiate a secure connection directly to their enterprise's application server or other electronic assets through virtually any Internet-connected device, such as a desktop PC,laptop, Smart-phone or PDA. If users change their Internet connection (IP address), the AppGate solution can automatically reconnect the full VPN connection to the AppGate Server. This "Mobile Roaming" capability makes it possible to enable feature-rich applications on a mobile device. For example, checking the enterprise CRM system on a Smart-phone in a taxi becomes not only possible, but also seamless and secure. Furthermore, all settings on a Smart-phone or PDA can be automatically installed via "over-the-air provisioning", enabling true remote administration and support. Unlike "push technologies" which offer only email-centric functionality, AppGate's full mobile VPN solution allows a mobile phone to interact with enterprise application servers the same as a desktop computer interacts with these servers, enabling richer features and access to information on the mobile phone.

Security made Simple

AppGate's complete unified access system is simple and flexible so that system administrators are able to quickly manage the entire network. For example, security rules may be set so that local users on the corporate LAN may access a service such as a network disk during office hours after providing password authentication, but remote

users may be prompted to use a smart card for authentication and be forced to have a personal firewall installed for the same service to be available. Because the AppGate solution is an all-in-one system that is capable of securing any IT asset, systems administrators do not need to learn to maintain multiple point-based security systems. The AppGate solution is always one box and it elegantly solves multiple IT security needs, from mobile accessibility to increased partner collaboration to internal network security. The AppGate solution is designed to protect IT assets by shielding them from all unauthorised traffic. It authenticates users and authorizes them to use specified services, encrypts and decrypts network traffic, performs access control, logs events and is a central point for all security administration. The system can be used to control internal as well as external traffic to servers and with up to 12 interfaces per server, it is an excellent tool for internal segmentation of networks. With an AppGate system in place, the visibility of an IT resource to a user only depends on whether the user is authorized to see and use it, not whether the user is an internal or external user.

Protection at the End Points

AppGate's solution consists of a Server and "connected" Client devices. The AppGate Security Server contains a stateful inspection firewall and clients can have an optional Device Firewall controlled by the AppGate Security Server for protection against unwanted network traffic. This architecture moves protection from the traditional point at corporate boundaries (the firewall) to the actual end-points of the network (the client devices) with much enhanced control of security. The AppGate Client will make sure that all traffic to

TRUST

protected resources is encrypted and enables the AppGate Security Server to fully check the configuration of the client device before granting access to any resources (client check and client command).

The system makes it possible to make detailed decisions about what the user should be allowed to access and controls in detail what applications are useful on the specific client. Traditional "Network Admission Control" is expanded into more than just a question about granting access or not granting access; instead varying access rights can be given depending on the rules associated to each service.

Role and Rights Management

AppGate Servers include a powerful and flexible authorization engine which contains rules for what applications and services should be available to each user or category of users. User accounts and user roles can be stored in third party servers, such as Radius, LDAP and Active Directory, if desired, and support for simultaneous use of different authentication methods offers maximum flexibility. Groups of services can be created and detailed access rules can be assigned to each group such as requirements for authentication method, time of day, type of device, device location and configuration. The services available to the end-users are presented in a portal-like user interface where each icon represents an available service. Clicking an icon enables traffic to the application it represents and also starts an application on the user's workstation, for example the mail reader. This virtually eliminates necessary user training and removes the burden on the help desk to answer common questions from the users.

Redundancy and High Availability

The AppGate Server appliances have from four up to 12 network interfaces, making it possible to segment networks and separate application servers from each other without the need for additional network equipment such as routers and firewalls. The server also supports VLAN technology for further segmentation of network traffic. The interfaces are fully symmetrical, which means users and services can be connected to the AppGate Server from any network while at the same time providing network administrators considerable freedom to manage security and devices. AppGate server appliances are available in different hardware configurations, from single processor systems to multiprocessor systems for high performance applications. In addition, the AppGate server solution is built upon a unique clustered architecture which provides for highly scalable and redundant solutions (a system easily supports 30,000 concurrent users). Unlike a traditional clustered architecture, each additional server in a cluster almost linearly increases performance of the entire system. Users are distributed evenly on all available systems in a server cluster, thereby allowing everything from extremely simple to highly advanced and powerful fault-tolerant server solutions to be built.

Mobility Needs Special Attention

To be able to provide a user-friendly experience with full security, AppGate has developed special technology. The Mobile Roaming capability is necessary in a mobile world and, in simple terms, it takes away the problem with poor network coverage. In an ordinary VPN session when a connection to the network is lost, the user may even be completely invisible both to the user and the application, including a change of the user's IP address. Longer outages of network connectivity can also be accepted by the AppGate server and the client may be allowed to reconnect again after several hours without user intervention. AppGate's implementation of roaming is unique in many ways as it works for all types of network connections and not only on mobile devices. To be able to support mobile users, AppGate has developed special clients and support for mobile phones, including over-the-air provisioning of the mobile device. The mobile user receives an SMS message which can automatically set up both the VPN client and individual applications in the mobile phone, for example the user's e-mail client. Due to the full VPN connection, the AppGate Client software enables much more functionality in the mobile phone than traditional solutions. The advantage of using a VPN technology instead of "push-technology" is that it offers not just email functionality, but also the capability to deliver secure network connectivity and feature-rich applications, such as intranet and CRM access, virtually without limitations. With AppGate's full VPN, a mobile phone can truly become a desktop-equivalent device, saving time and money and eliminating the need for "push-applications."

Access from Everywhere – Mobility and Roaming

The AppGate system supports most types of devices, such as desktop computers, servers, mobile phones and PDAs, and is compatible with many common operating systems, including Windows, Mac OS/X, and Linux. This is an important requirement for a system to become an organization's complete unified access system. Instead of having to use multiple security systems with poor integration, this means that the same authorization system is used regardless of the device being used. AppGate performs all functions in one box and requires no modification of applications or application servers. With the AppGate system, the same authorization engine is used to grant

SECURITY

or deny access regardless of the device being used. The secure Mobile Roaming capability in the AppGate Client makes it possible for the user to move between different networks without having to be re-authenticated each time.

Choice of Different Clients

The user can choose to use just a web browser or the AppGate Client when connecting to an AppGate system. When using a web browser, the system can offer true client-less access via the web browser and its built-in SSL support and all web based applications can be accessed through the system. If more applications are needed, the user can use the AppGate Client. The standard AppGate Client is based on Java Web Start technology which means that it can easily be downloaded in a web browser if it is missing on the user's system. In addition, once down-loaded, it will be automatically updated to the latest version available on the AppGate Server if needed. This makes client deployment extremely easy. The only requirement for a Client to be able to connect to an AppGate Server is that it can establish one TCP connection to the AppGate server which will contain a secure encrypted tunnel. It does not matter what underlying networks are being used or whether the network addresses are being translated in the path by outbound firewalls doing NAT or other such things. The client software can also traverse web and Socks proxies when connecting to a server. When a new connection is initiated, the client begins with checking the AppGate Security Server's identity to make sure that no "man in-the-middle" is interfering with the traffic. Next, the client and server agree on session

crypto-keys for their connection. After a connection has been set up and the user is authenticated, an encrypted tunnel is present where traffic can be securely tunnelled. It is also possible to have data compressed before it is encrypted and transmitted in order to increase network bandwidth. On slower links (below 1Mb/s), the performance boost due to compression can be substantial. Compression can not only help to increase performance, it can also decrease connection costs when traffic costs depend on amount of data being transmitted.

Security, Single Sign-on, Web Filters

The AppGate Security Server understands several application-level protocols and can inspect their traffic and in some cases also offer single sign-on functionality. Examples of such applications are remote desktop, RDP and web access and it can also filter access to URLs on a web server. URL filtering is useful, for example, when several user categories share a single web server – then it is possible to use the AppGate server to control what pages each individual user can access. Other areas where the AppGate server offers single sign-on is for example when a user is already authenticated in a Windows domain and the credentials already received to log in to the AppGate Server via the built-in Kerberos protocol support.

Remote Administration, Logs and Alarms

All servers in an AppGate cluster are administered as one entity. From the system administrator's point of view, there is almost no difference in administering a single server or a large cluster of servers. The system can be remotely administered using a

powerful GUI-based console application and it offers graphical views of the system, its configuration and status. The system includes a log server for audit capabilities. It captures events such as users logging in and out from the system, services or applications accessed by the users, security-related events such as denied requests and protocol errors, system related information and events from the operating system (disk quota problems, hardware errors). The log can be examined using the AppGate Console GUI or be exported to external systems for further analysis. Alarms can be generated by specifying the kind of event to look for and an arbitrary command can be executed for each such event. This way, alarms can easily be sent through email, syslog, SMS, or SNMP.

The Server

The AppGate server currently runs on Solaris 10 and OpenSolaris on standard PC and Sun Sparc hardware. The AppGate server can also be virtualized and is available as a software package running under VMware Server and VMware ESX Server. The server also uses FIPS 140-2 certified OpenSSL libraries for encryption of network traffic. In addition, the server is currently undergoing a Common Criteria certification. The clients are developed mostly in Java with the exception of the mobile clients which are developed in C to overcome platform dependencies with Java and to be in maximum control of the devices.

CONTROL

Security Advantages in the AppGate System	
Appliances with Multiple Network Interfaces	The AppGate server is delivered a ready-to-run appliance and depending on selected hardware, it can have from four up to twelve independent network interfaces.
Authentication & Encryption	Offers strong encryption of network traffic with support for multiple simultaneous user authentication methods. The system is compatible with most third party authentication methods. Even one-time passwords sent over SMS are supported via the built-in authentication module.
Automatic Client Updates	When a newer version of the client software becomes available on the AppGate Server, all clients can automatically be updated with the new version. This makes deployment of client software extremely easy.
Built-in Firewall	The AppGate server has a built-in stateful inspection firewall for complete protection of itself and the application servers behind it.
Client Check and Client Command	The Client Check feature enables the security system to check the client's configuration before granting access to selected services. Similar functionality is often called NAC or NAP. Client commands can be used to reconfigure and make server controlled checks on the client.
Client Provisioning	Mobile devices such as PDAs and mobile phones can be automatically configured from SMS messages being sent from the AppGate server.
Clustering	Several servers can be clustered for enhanced performance or for high availability solutions.
Distributed Device Firewall	Windows clients can have an optional firewall installed which is controlled from the AppGate server when the user connects to a system. This gives the systems administrator full control over the configuration of the clients when they connect to the system.
Full Application Protocol Support	The AppGate system is an application-level VPN system that supports all application protocols, not only web based applications. • The user uses the real application interface without modification • Even supports multi-user systems such as terminal server solutions • It does not have any NAT or other network traversal problems
Logs and Alarms	All important system events are logged and alarms can be triggered and sent to administrators, for example by email, SMS, SNMP or other means.
Portal-like Graphical Client User Interface	The AppGate Client has a nice graphical client interface. It is highly configurable and offers a portal-like experience of currently available services. User can simply click on icons to start applications.
Proxy Server Traversal Support	The client can traverse firewalls and proxies such as HTTP and Socks proxies including those requiring NTLM authentication for SSO functionality.
Remote Administration	Even distributed clustered solutions can be remotely administered with the AppGate Server GUI.
Roaming	Automatic reconnects to the network if the connection is lost. Can even transparently move between networks and even accepts a change of IP address. This means that users can seamlessly switch between different carrier networks.
Roles & Rights Management with Granular Access Control	Flexible authorization rules can specify in detail how and under what circumstances individual services should be available. Services can be grouped together or placed in folders to facilitate administration in larger environments.

USABILITY

Security Advantages in the AppGate System	
Secure Single Sign-on	Today it is common for users to have to log in several times in order to access an application. With the AppGate system, in many cases it is possible to avoid additional logins resulting in easier access of information.
Secure Print	Possibility for remote applications to securely print to locally attached printers, for example printers at local offices or even at home.
Secure Instant Messaging	Secure Instant Messaging for authorized users with single sign-on functionality.
Single Sign-on functionality	The AppGate system can offer single sign-on functionality for many applications including web and RDP and can accept Kerberos tickets from clients (obtained from Windows Domains).
SSL Support	The built-in SSL module allows users to connect to web-based services behind the AppGate server in a true client-less fashion just using a standard web browser.
Traffic Compression	Clients can compress traffic to enhance performance on slower links and reduce traffic cost on other.
Universal client support	Clients exist for virtually all types of hardware and operating systems, including Windows, Linux/Unix, Solaris, Mac OS/X, PDAs and mobile phones.
URL Filtering	Instead of building multiple web sites, the AppGate server can give users secure access to individual web pages based on their role.