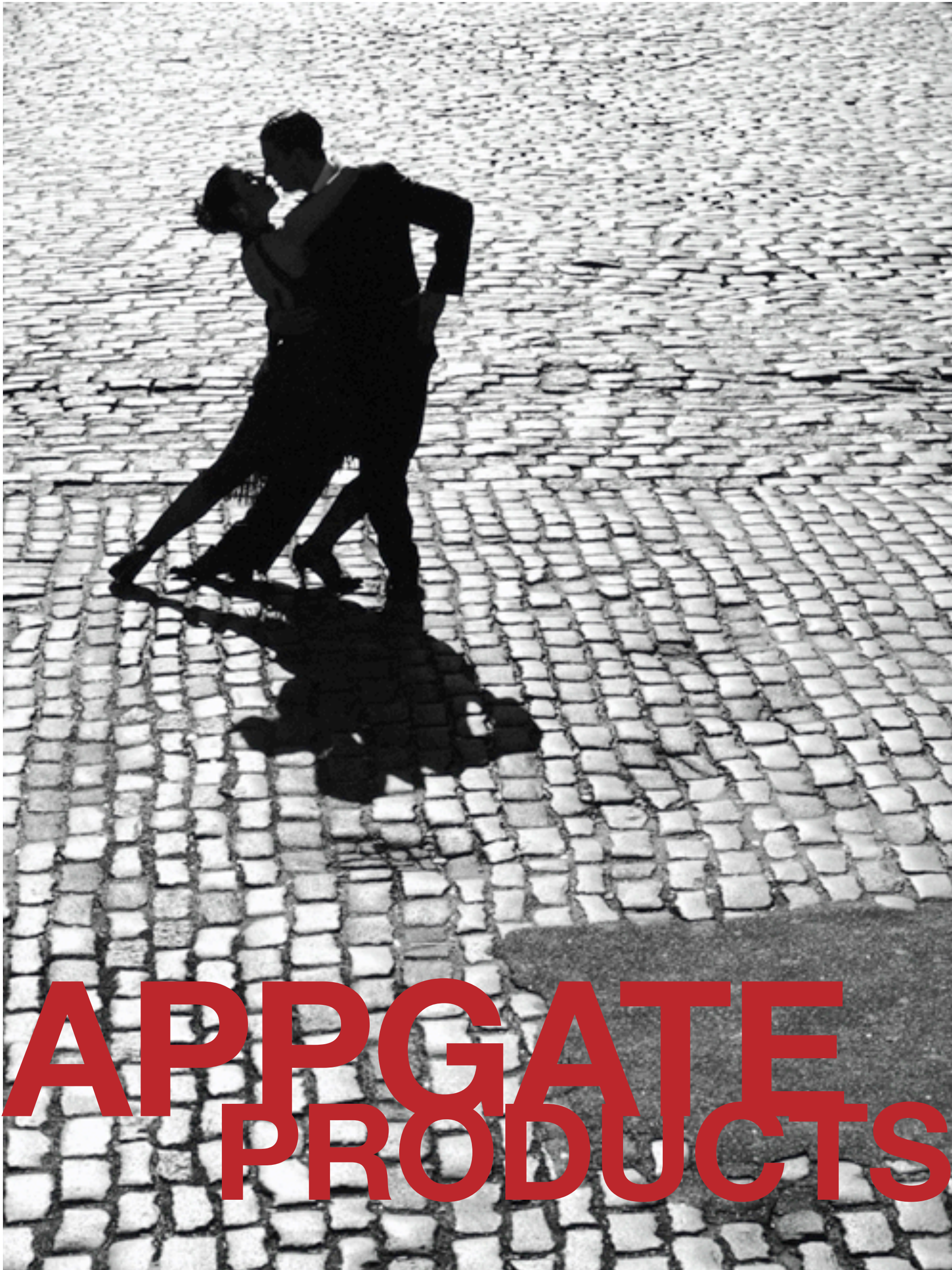


appGATE™
NETWORK SECURITY



APPGATE
PRODUCTS

UNIFIED



SECURITY

Introduction

The AppGate product portfolio is aimed to give customers a comprehensive solution that can be tailored for any customer needs. From small companies in need of remote access to larger organizations which demand total access control, AppGate's products protect company resources from threats inside and outside of the organization's perimeter.

AppGate's current range of Products includes:

- Security Server
- Mobility Server
- Device Firewall and Policy Manager
- Secure Mobile Office
- MindTerm
- In Case of Emergency (ICE) Server

Customers may also choose to purchase extra functionality through software Modules and Accessories:

- Clustering Module
- USB Client Accessory
- SSL Module
- SMS Authentication Module

The following functionality is included in the cost of an AppGate Server:

- Mobile Client Technologies
- Secure Print
- Secure Instant Messaging

AppGate Security Server

The AppGate Security Server is an all-in-one appliance which is placed as a gateway between the selected IT asset(s) and the rest of the corporate network (or even Internet). Due to AppGate's simple and elegant

technological approach, the AppGate Security Server provides and enables four crucial security features, namely Mobile VPN, Remote Access, Network Access Control and Internal Domain Segmentation, for virtually all application servers without the need for additional point-based solutions or network security infrastructure. In combination with the AppGate Client software which resides on a user's desktop computer, laptop, Smartphone and/or PDA, the AppGate Security Server provides an all-in-one solution for an enterprise's accessibility and security needs. The AppGate Security Server is a rack mounted server and is offered in various sizes based on the number of concurrent users a customer requires. All Servers in the Ax series are built on standard rack-mounted PC hardware, currently servers from Sun Microsystems, and may be clustered using AppGate's unique Clustering Module. The number of concurrent users on a server is controlled by a license key distributed by AppGate. Current AppGate Server models and their respective user capacities are listed below:

- Ax1: 250 concurrent users
- Ax2: 1000 concurrent users
- Ax4: 2,000 concurrent users
- A10: 10,000 concurrent users
- An15: 15,000 concurrent users

AppGate Mobility Server

The Mobility Server is a slimmed version of the Security Server and is designed for use by small and

medium-sized businesses that want to enable just mobile accessibility. It is a pre-configured appliance server that is easy to install as a gateway and can be used either as a stand-alone unit or be combined with an existing VPN system to support mobile phones and PDAs. Used in combination with the AppGate Mobile client which runs on virtually any mobile device, the Mobility Server allows users to securely read and send email, synchronize calendars and access other corporate resources. Its key benefits to system administrators are support of many authentication methods, support for strong encryption and full control of network services based on various factors, such as type of device being used and user role and rights. The Mobility Server also supports AppGate's Mobile Roaming functionality which offers users automatic and seamless reconnection to the Server if the communications link goes down or IP is changed. The AppGate Mobility Server offers small and medium-sized enterprises the flexibility to simply upgrade their existing network infrastructure in order to provide a secure mobile solution based on AppGate's award-winning platform.

AppGate Device Firewall and Policy Manager

The AppGate Device Firewall is a state-of-the-art personal firewall installed on Windows workstations and servers which can be controlled by AppGate Servers for increased

CONTROL

connection and workstation security. The AppGate Device Firewall is designed without a graphical user interface on the client machine as it is meant to be configured remotely by system administrators. It controls all inbound and outbound traffic on all adapters and network interfaces. The firewall system can, for example, make sure that user workstations on a network cannot communicate with each other. Since many viruses and worms spread between systems through bugs or vulnerabilities in the operating systems, this kind of protection also stops users from accessing other users' workstations over the network. The AppGate Device Firewall can also co-exist with other personal firewalls. All firewalls must approve the traffic before it is passed in or out from the system. An existing personal firewall with a graphical user interface can therefore be combined with the centrally administered AppGate Device Firewall that governs the minimum level of protection for the machine, regardless of what action the users take. The Policy Manager makes it possible to set global rules for all stand-alone AppGate Device Firewall installations (i.e. those used without the AppGate Security Server appliance). The Policy Manager distributes two rule-sets to clients, one which is active when the client has contact with a Policy Manager and one, which normally is more restrictive, with allowable IP traffic when no Policy Manager can be contacted (a "default" policy to fall back to). The AppGate Device Firewall and Policy Manager are sold either together with the AppGate Security Server or as a stand-alone offering.

AppGate Secure Mobile Office

In addition to the core Server and Client products, AppGate has recently

launched a related dedicated solution that demonstrates the secure flexibility of the Security Server. The AppGate Secure Mobile Office moves AppGate beyond the enterprise with a revolutionary solution for wireless service providers. It is a lightweight appliance that allows mobile network operators to provide secure mobile VPN solutions for their customers. Announced at the 2008 3GSM World Congress in collaboration with Sun Microsystems, the Secure Mobile Office system enables secure e-mail access, intranet access and calendar/contact synchronization through Smartphones and PDAs. The system creates a new source of revenue for operators by providing an increasingly important service to end-users through the operator's existing connectivity pipe. The AppGate Secure Mobile Office system incorporates an AppGate Security Server at the core of an operator's network, an AppGate Mobile client installed on the Smartphone and an small box the AppGate Satellite at the customer network. The Satellite is placed at the end- customer's network, directly in front of an enterprise's mail, web and calendar application servers. Operators are able to easily support up to 15,000 users AppGate Security Server and the system may be clustered by an operator to support tens of thousands more users. Instead of being limited to the concept of "push email," AppGate's full mobile VPN solution allows a mobile phone to interact with enterprise mail, intranet and calendar servers exactly as a desktop computer interacts with these application servers, enabling richer features and access to information on the mobile phone. The robust connection to the mobile phone can

also provision mobile devices over-the-air, enabling true remote system administration and support. The AppGate SMO is a revolutionary offering which enables operators and internet service providers to deliver a new high-value, next-generation service to enterprises and customers. It enables a operator to offer secure e-mail and application access in a way that is unavailable on the market today. It is a truly disruptive service opportunity.

AppGate MindTerm

MindTerm is probably the world's most widely used Java-based SSH1 and SSH2 client for desktop and laptop computers. Although free for personal use, some of the world's leading manufacturers of communication equipment have signed OEM contracts to use MindTerm. MindTerm is a small, portable and secure client which contains advanced features such as tunneling support, a file transfer GUI as well as support for HTTP and SOCKS proxies. With the Applet version of the MindTerm client, it is also possible to run a secure terminal session from a Java-enabled web browser.

AppGate In Case of Emergency (ICE) Server

The In Case of Emergency Server is meant to be a part of a customer's business continuity plan, ensuring that employees, customers, partners and support personnel can access the corporate systems from any location when an emergency occurs. The customer buys an ICE Server appropriate for their capacity needs and pays an annual fee for two licenses. The first license is for five concurrent users; the second license is to be used only in case of

SOLUTIONS

emergency. Both licenses are valid for one year. Using the five user license, the ICE Server is set up and tested with special roles defined for the whole user community. The ICE Server is then backed up and left in place for the day that something unexpected happens. When an emergency strikes, the ICE license key enables the company to upgrade the AppGate Server in an instant to support unlimited users for a maximum of 90 days. Since AppGate's unique technology supports secure remote access regardless of device, platform, or transmission - fixed, wireless and mobile - when an emergency strikes, employees can work from home on their PC's, laptops, mobile phones or PDA's; customers and partners can access essential information and applications from their own systems or internet cafés; and support staff can support and maintain systems and servers remotely.

Additional Modules and Accessories

AppGate Clustering Module

AppGate allows for clustering of its Servers to increase the number of concurrent users that may connect securely to an enterprise's network. This feature is unique in the industry as nearly no other vendor's technology supports linearly scaling the number of supported users by simply plugging in another server. In an AppGate cluster, each additional processor (whether in a multi-CPU or clustered AppGate solution) almost linearly increases performance of the entire system because each server in an AppGate cluster is more or less "unaware" of the other servers' existence. User requests are distributed evenly on all available processors, thereby allowing

everything from extremely simple to fault-tolerant, 30,000+ user server solutions to be built.

AppGate USB Client

The AppGate USB client is designed to be used on personal computers when connecting to an AppGate Security Server. It is a client that does not rely on or use the ordinary operating system on the machine. It executes in a secure and trusted environment regardless of the configuration of the original operating system on the computer. In addition, it does not access or store any data on the local hard disk on the PC and will therefore not leave any traces or residues on the computer when the session to the AppGate Server is closed. The AppGate USB Client enables secure flexibility for users and has been deployed in many information-sensitive industries, such as medical doctors that travel from hospital to hospital or review confidential patient information at home.

AppGate SSL Module

AppGate offers an SSL add-on module which supports secure access to all web-based applications without the need to download a client. The SSL module is useful in situations where there is no need for or when it is not possible to use a full client, such as when one needs to read email on an airport or café PC. The SSL module allows users to access web-based corporate assets securely just using a standard web-browser.

AppGate SMS Authentication Module

Through a third party arrangement, AppGate can provide strong two-factor authentication based on a text message being sent to the user's mobile phone. The SMS contains a one-time password that can be used

to log into the AppGate Security Server.

AppGate Mobile Clients

The AppGate Client software supports a wide number of client platforms, from Windows, Mac and Unix/Linux workstations and servers to Smartphones, and PDAs. The client independence of the AppGate solution ensures that no matter where or how a user connects, the corporate network is secure and always reachable. The AppGate solution is designed to give access to an easily-definable degree of network resources based on many different parameters such as the type of client being used or authentication method. AppGate has developed mobile clients for all of the major mobile Smartphone operating systems, including Windows Mobile (compatible with WM2003 and later), S60 3rd Edition, and UIQ 3 devices. These AppGate clients for mobile Smartphones and PDAs feature "over-the-air provisioning," enabling, for example, the client to automatically download a user's personal login settings and set up accounts for mail and Exchange synchronization. The mobile clients are designed from the ground-up to provide desktop-equivalent functionality and security, such as built-in web proxy authentication for "single sign-on" capability and support for load balancing and failover within an AppGate cluster. Each AppGate Client is also capable of "Mobile Roaming," a functionality which offers the ability to automatically reconnect to the AppGate Server if the network connection goes down. It can be done without any user interaction with the client system and can even handle a change of IP address. AppGate's Mobile Roaming functionality enables customers to achieve true workforce mobility.

FUNCTIONS

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	<p>The AppGate system is an application-level VPN system that supports all application protocols, not only web based applications.</p> <ul style="list-style-type: none"> • 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.

app **GATE**TM
NETWORK SECURITY



www.appgate.com