Enterprise Remote Access

Overview Historically, organizations have used IPSec VPN solutions to provide employees with remote access to network resources; an expensive, complicated deployment for a handful of users. Originally designed for securing site-to-site communications, IPSec has shown it is unable to keep up with the growing demands of remote access required by today's enterprise organizations. As the Internet becomes the most important method for organizations to provide access to mission critical applications, and web-enabled devices become more prevalent, the limitations plagued by IPSec solutions are proving prohibitive for many enterprises. The FirePass controller from F5 allows organizations to easily provide secure and granular remote access to the internal network and the applications that run there, from any device, in any location.

Challenge Organizations employing IPSec VPNs have to contend with issues regarding IP addressing, network address translation, limited remote device support, and software installation and maintenance required on every client. Because IPSec solutions require client software to secure the transactions, corporate resources can only be accessed through a limited number of systems. This severely limits the ability of end-users to obtain access to important resources from public systems and mobile devices. It also increases the cost of the implementation because it requires organizations to provide and maintain corporate laptops for each employee who travels. Furthermore, as an increasing number of remote users are given access to sensitive information, the integrity and security of the device being used has become a major security issue; is the system secure and free from malicious code?

Also, administrators are faced with the broad security control of these IPSec VPN systems that lack the granularity they need to provide appropriate access to users. Administrators must chose between providing broad access, which compromises network security, or providing very limited access, making it difficult for users to work effectively. IPSec VPN solutions also provide limited auditing, making it difficult for administrators to troubleshoot problems and blinding them from clear insight into user data.

A survey conducted by AT&T/Economist showed that 54% of employees work from home on a regular basis. It is estimated that this number will increase to 80% by 2005. Organizations need a solution that allows them to provide reliable, secure access to multiple applications from a multitude of devices, anywhere in the world.

Solution F5's FirePass® controller enables enterprises to provide secure, reliable and intuitive remote access to corporate applications and data using standard web browser technology, without the headaches associated with time-consuming client software installation and configuration, or changes to server-side applications. The FirePass device also provides robust capabilities for ensuring the integrity of those clients to ensure compliance with corporate standards.

The FirePass device is the first SSL VPN solution with complete cross-platform support. Extending its support for any IP application to Apple® Macintosh®, PocketPC and Linux clients, in addition to Microsoft® Windows®, and expanding client and application security for web, email and file application access, the FirePass controller delivers the industry's most ubiquitous solution for secure network access.

It also offers the only open API and SDK that enables 3rd party application vendors to build seamless, secure remote access into their client applications.

Full Network Access

The corporate laptop user, or "trusted" user, is an employee using company issued and maintained equipment. The trusted user is typically an executive or a member of the sales team who needs the same access to network resources as users in the office.

For these users, the FirePass controller delivers network access for Windows, Macintosh, PocketPC and Linux systems. Standard features across all desktop and laptop platforms include

split tunneling, compression, activity-based timeouts, and automatic application launching.

For administrators, the FirePass device allows the restriction and protection of resources accessible through a connector by instituting rules that limit access to a specific network or port. It uses the standard HTTPS protocol with SSL as the transport, so it works through all HTTP proxies including public access points, private LANs, and over networks and ISPs that do not support traditional IPSec VPNs. And because it utilizes GZIP compression to compress traffic before it is encrypted, it reduces the amount of traffic that is sent across the Internet, improving performance.

To protect against backdoor attacks when accessing the network with split tunneling, the FirePass system provides a dynamic firewall that protects Win2k/XP users when using the full network access feature. This eliminates the ability for a hacker to route through the client to the corporate network or for the user to inadvertently send traffic to the public network.

The FirePass device also increases security by detecting the presence of required processes (e.g. virus scan, personal firewalls, OS patch levels, registry settings and McAfee® anti-virus levels) and the absence of other processes (key logger for example) on the client PC before allowing full network access. Users who fail these primary policies can be connected to a quarantine network where they can update to current corporate security standards.

Portal Access - Secure Access From Public Systems For Employees, Customers and Partners

Enterprises increasingly deploy web-based applications, intranet and extranet portals, as well as web-based email to enable higher employee productivity and increased operational efficiency both internal to their organization as well as with their partners. To maximize the benefits of these applications, organizations should ensure these applications are accessible to employees and partners from any location while ensuring restricted, secure access only to authorized users.

The FirePass controller provides numerous features to ensure secure web-based access to enterprise intranet and extranet portals, web-based email, and applications. The Portal Access capability works on any client OS with a browser - Windows, Linux, Macintosh, Pocket PC's, PDAs and more.

Web Applications

The FirePass device provides access to internal Web servers, including Microsoft Outlook Web Access and Lotus® Domino Web Access (formerly iNotes®), as easily as from inside the corporate LAN. It also delivers granular access control to intranet resources on a group basis. For example, employees can be provided access to all intranet sites; partners can be restricted to a specific web host.

While accessing resources, the FirePass controller dynamically maps internal URLs to external URLs so the internal network structure does not reveal them. User cookies are managed at the FirePass device to avoid exposing sensitive information. For applications that require access to cookies, the FirePass controller can pass cookies to the remote browser. User credentials can be passed to web hosts to support automatic login and other user specific access to applications. The FirePass controller also integrates with existing identity management servers (Netegrity® for example) to enable single sign-on to applications.

File Server Access/Email Access

The FirePass controller allows users to browse, upload, download, copy, move or delete files on shared directories. It supports SMB Shares, Windows Workgroups; NT 4.0 and Win2000 domains; Novell 5.1/6.0 with Native File System pack, and NFS servers. For email, the FirePass device provides secure web-based access to POP/IMAP/SMTP email servers from standard and mobile device browsers. This allows users to send and receive messages, download attachments and attach network files to emails.

Mobile Device Support
The FirePass controller allows secure access from PDAs (like Palm OS), and cell phones (like WAP and iMode phones) to email and other applications. It dynamically formats email from POP/IMAP/SMTP email servers to fit the smaller screens of mobile phones and PDAs, and supports the sending of network files as email attachments and the viewing of text/Word documents.

Portal Access -- Comprehensive Security

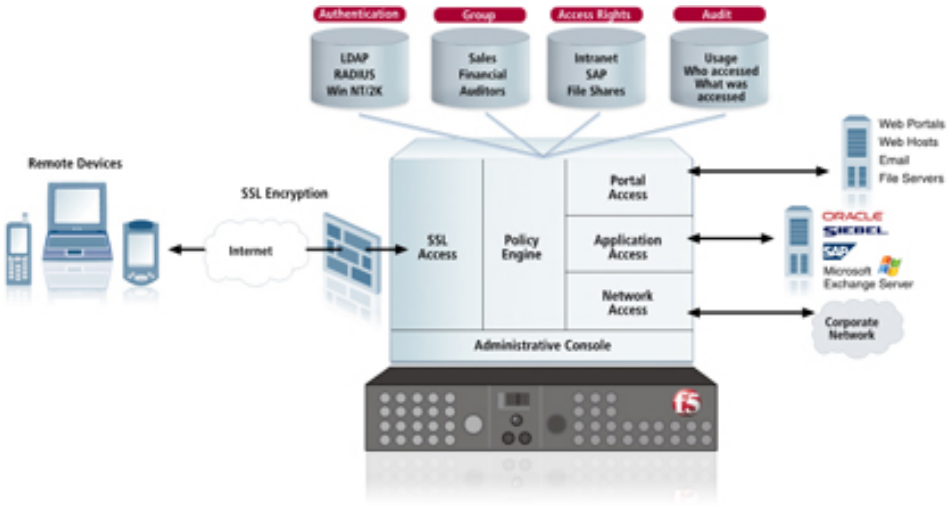
The FirePass controller delivers multiple layers of control for securing information access from public systems. For example, users of Windows 2000/XP can be automatically switched to a protected workspace for their remote access session. In a protected workspace mode, the user cannot write files to locations outside the protected workspace and the temporary folders and all of their contents are deleted at the end of the session. Since the user session is in a separate desktop, users are protected from trojan horses and key loggers.

The FirePass device also includes a cache cleanup control feature that removes cookies, browser history, auto-complete information, browser cache, temp files, and all ActiveX controls installed during the remote access session from the client PC. A secure "virtual keyboard" enables secure password entry from the mouse instead of the keyboard. When engaged, this feature enables users to securely enter a password on a system that has been compromised by a key logger.

For systems unable to install a "cleanup" control, the FirePass controller can be configured to block all file downloads to avoid the issue of inadvertently leaving behind temporary files - yet still allow access to applications. For users accessing web applications on the corporate network, the FirePass product enhances application security and prevents application-layer attacks (such as cross-site scripting, invalid characters, SQL injection, and buffer overflow) by scanning web application access for application-layer attacks - then blocking user access when an attack is detected. The FirePass device can also scan web and file uploads using either an integrated scanner or external scanner via ICAP API. Infected files are blocked at the gateway and not allowed onto email or file servers on the network, heightening protection.

Application Access - Secure Access to Specific Applications

FirePass allows administrators to grant certain users - for example, business partners using equipment not maintained by the company -- access to specific extranet applications and sites. It protects network resources by only allowing access to applications that are specifically cleared by the system administrator. Supported applications include terminal servers, legacy hosts, Windows desktops, and X Windows systems. FirePass logs an audit trail of the specific applications accessed by each user to facilitate security audits.



Client/server Application Access
FirePass enables a native client side application to communicate back to a specific corporate application server via a secure connection between the browser and the FirePass Controller. It does not require the user to preinstall or configure any software. On the network side, FirePass requires no additional enabling software on the application servers being accessed. And because it uses the standard HTTPS protocol, with SSL as the transport, it works through all HTTP proxies including public access points, private LANs, and over networks and ISPs that do not support traditional IPSec VPNs. Supported applications include Outlook to Exchange Clusters; Passive FTP, Citrix Nfuse, and network drive mapping. Compression is also supported for better performance.

Terminal Server Access
FirePass provides secure Web-based access to Microsoft Terminal Servers, Citrix® MetaFrame® applications, Windows XP Remote Desktops, and VNC servers. It supports group access options, user authentication and automatic logon capabilities for authorized users, and supports automatic downloading and installation of the correct Terminal Services or Citrix remote-platform client component, if it is not currently installed on the remote device.

Host Access
Host Access features enable FirePass to secure web-based access to legacy VT100, VT320, Telnet, X-Term, and IBM 3270/5250 applications without requiring modifications to the applications or application servers from Web browsers supporting Java or ActiveX downloads.

Desktop Access
By combining the features of the FirePass controller and existing functionality for remote desktop access imbedded in Windows XP or through functionality which can be added using freely available software for virtually any desktop operating system, the FirePass can provide seamless, virtually transparent access to almost any desktop environment from Web browsers supporting Java or ActiveX downloads.

Authentication and Authorization

The FirePass controller provides a Visual Policy Editor (VPE) that allows an organization to determine what the client requirements are before even being allowed to login. The VPE provides an easy to understand, self-documenting process to define and show the company policy and provides for user-based remediation in the event a client fails to satisfy the policy. This allows a company to not only prevent systems that might cause harm to the network from connecting, but also intrinsic documentation of that process and a way for users to "fix themselves" without needing help-desk support.

The FirePass controller also includes a dynamic policy engine that enables administrators to easily manage user authentication and authorization privileges. Dynamic policy based access gives administrators quick and granular control over their network resources. Through rules support, administrators can authorize access to applications based on the user and device being used (based on any of the pre-logon check results). For example, administrators can configure a user's permission to allow email-only access from a public kiosk with active cache and temporary file cleanup, but provide them full network access from a corporate laptop with active firewall and virus detection software.

By default, users are authenticated against an internal FirePass database, using passwords. But the FirePass device can also be easily configured to work with RADIUS, Active Directory (Kerberos) and LDAP authentication methods, basic and form-based HTTP authentication, identity management servers (e.g. Netegrity),and Windows Domain Servers. For authentication, many organizations require "two-factor" authentication, which uses something beyond knowledge of a user ID and password. FirePass fully supports both RSA SecurID® and VASCO Digipass® token-based authentication systems.

In addition, the FirePass controller enables the administrator to restrict or permit access based on the device being used to access the FirePass device. The FirePass controller can also check for the presence of a client-side digital certificate during user login. This certificate will only be present on the laptop. Based on the presence of this digital certificate, the FirePass device can support access to a broader range of applications. The FirePass controller can also use the client-side certificate as a form of two-factor authentication and prohibit all network access for users without a valid client-side certificate. The FirePass device can act as a certificate authority and auto-generate and distribute client certificates. This drastically reduces the additional costs to purchase and manage certificates for each of the clients.

Client-Integrity The FirePass controller includes a suite of components for providing client-integrity verification of the remote client prior to even allowing login. Integrity checks allow organizations to verify that the remote host complies with a set of defined standards. In windows based systems, for example, the FirePass supports 16+ anti-virus and 7+ personal firewall vendors providing an organization the flexibility to define the need for these applications without having to dictate specific vendors or acquire and install one. In addition, the VPE allows organizations to check for files, processes, client certificates, source IP, patch level, SSL characteristics, OS, etc. This information can be used to prevent a user from logging in entirely or can be used restrict access to specific systems.

Access Privileges
Access privileges can be granted to individuals or to groups of users (for example: "Sales", "Partners", "IT"). This allows the FirePass device to restrict individuals and groups to particular resources. Partners may be allowed access only to an extranet server, while Sales staff can connect to email, the company Intranet, and the CRM system. Access Policies can be defined to a group of resources as opposed to individual resources. New resources can be simply added to a resource group without modifying individual access policies manually. In addition, resources can be defined as an alias so that any changes to resource definitions are automatically updated in all resource aliases. These capabilities significantly reduce the policy management complexity in an enterprise environment with a large number of user groups and resources.

The FirePass controller also gives organizations flexibility in providing some administrative functions (enrolling new users, terminating sessions, re-setting passwords) to some administrator-users, without exposing all functions to them (for example, shutting down the server, deleting a certificate). In addition, the authorities can be restricted to particular groups of end users: the administrator in Finance, for example, would not be allowed to delete a user in Sales.

Auditing
The FirePass device provides reports from the session and activation logs. Summary reports aggregate usage by day of the week, time of day, accessing OS, features used, web sites accessed, session duration, session termination type, and other information for a user-specified time interval.

iControl SSL VPN Client API for Secure Application Access

As the only SSL VPN product with an open API and SDK, FirePass Controller enables automated, secure access for rich Win32 client applications by providing secure system-to-system or application-to-application communication. Now, applications can automatically start and stop network connections transparently without requiring users to log into the VPN. This enables faster, easier connections for end users while reducing client application installation.