AVAYA

The Power of We™

Avaya VPN Gateway for VMware

The Avaya VPN Gateway for VMware is a secure access solution that extends enterprise applications and resources to remote employees, partners, contractors and customers. By delivering full-featured SSL and IPSec VPN functionality as software for VMware virtual server environments, the Avaya VPN Gateway dramatically reduces the complexity of deploying a secure access solution. It allows enterprises to quickly provision a flexible and scalable solution that can meet the most challenging secure remote access requirements.

Key VPN Gateway Features

- Easy to deploy software solution for VMware environments
- Flexible, universal secure access for SSL and IPSec users
- Secure access to all applications, including voice and multimedia, from a web browser
- MultiOS endpoint support including Windows, Mac, Linux and smart phones
- Dynamic role-based access to applications and resources
- Strong endpoint security and information protection
- Log and audit trails for compliance

Key Benefits

Easy to deploy, cost-effective solution

The Avaya VPN Gateway is a software-based solution designed to run on VMware compliant hardware. This allows for easy deployment on existing or new servers. A seat based licensing model further allows for secure access services based on an enterprise's need and performance. Along with 10 and 50-user license starter packs, the VPN Gateway is a cost-effective way to get advanced secure access technology at an entry-level price.

Extend access to partners, contractors, customers

The Avaya VPN Gateway leverages browser-based software already available on a user's PC to provide secure remote access. This enables enterprises to extend access without having to distribute or manage client software. An on-demand model helps further ensure that any required client side software is loaded when needed and removed at the end of the session. When connected, end-users are granted access only to the data and applications they require.

Increase employee productivity — teleworkers, day extenders, mobile users

Remote workers can have full network access without losing the functionality they normally have within a traditional office environment. By providing application access over a standard broadband or Internet connection, the Avaya VPN Gateway can provide huge cost savings to the enterprise. It can also be used by mobile workers, enabling them to connect from hotels, hotspots and from within other enterprise networks for convenient anytime, anywhere access.

Protect information, assets, networks

Administrators can guard against information loss or theft without burdening end users with intrusive, hard-to-use security features. Fine-grained access controls help ensure users get access to only what is necessary to perform their job function — nothing more, nothing less. Flexible endpoint security scan and block features allow on-demand validation of unmanaged endpoints. And cache cleaning helps ensure no data remains on the endpoint at the end of the session. VPN Gateway can even prevent users from saving or printing data during the session.

Business continuity services

VPN Gateway VMware servers can be clustered to deliver reliable business continuity services. Clustering allows the VPN Gateway servers to function as a single system with redundancy services. Clusters can also be deployed

in multiple locations to provide site redundancy and optimum performance for a widely-distributed workforce. Avaya also makes it cost-effective to deploy access capacity for worst-case scenarios through Emergency Remote Access (ERA) user licenses that help ensure capacity is available when needed.

Key Capabilities

Flexible, universal secure access

Avaya VPN Gateway offers flexible access options to address a wide range of enterprise requirements and needs. Support for both SSL and IPSec on a common appliance also eliminates the need to deploy and maintain separate VPN devices and/or vendor relationships. Key capabilities include:

- **Clientless web access** enables access to web-based e-mail, file systems and web applications from any web browser through on-the-fly content transformation.
- **Net Direct** provides full network-layer access with no need to pre-install a client. Automatic download of Net Direct to the endpoint enables access to all TCP and UDP applications, including voice, multimedia and collaboration tools from Windows, Macintosh and Linux endpoints.
- **IPSec VPN client** access includes support for the Avaya VPN Client. This allows enterprises to support users with an IPSec requirement on Windows, Mac, smart phone and Unix-based clients.
- **Mobile device support** (both SSL and IPSec VPN) for tablets and smart phones with small device formatting options to support highly mobile user devices and applications such as Outlook Mobile Access.

Dynamic access and policy management

The Avaya VPN Gateway provides dynamic access policy management to help ensure simplified yet highly secure provisioning of users and groups with the enterprise. The gateway also provide granular access control, auditing and logging for both security tracking purposes as well as user/VPN capacity planning. Capabilities include:

- **Role-based policy model** that tightly integrates with existing identity management and directory services to assign user access privileges based on defined roles.
- **Dynamic context-sensitive portal** that enables administrators to control access based on source IP, browser type, digital certificates or other parameters before login is complete.
- **Single sign-on capability** that alleviates the need for end users to enter and maintain multiple sets of credentials for web-based applications.
- **Portal personalization** that allows dynamic generation of the portal based on user profile.
- **Access management** that includes granular control at the URL, server or file level – enabling security policies to be tailored to specific resources.

VPN Gateway for VMware Recommended Server Configurations

	250 Users	1000 Users	5000 Users
Required CPU	Quad Core (2.0 GHz) with two (2) of the core CPU's allocated	Quad Core (2.0 GHz) with four (4) of the core CPU's allocated	Dual Quad Core (2.0 GHz) with eight (8) of the core CPU's allocated
Memory	512 MB memory allocated	1024 MB (1 GB) memory allocated	4 GB memory allocated
VMware platform	ESX or ESXi Server 3.0 or higher	ESX or ESXi Server 3.0 or higher	ESX or ESXi Server 3.0 or higher
Hard Disk Drive (HDD)	8 GB drive space allocated	16 GB drive space allocated	40 GB drive space allocated
CD/DVD ROM	1 required for software install	1 required for software install	1 required for software install
Ethernet on-board server interfaces	1-4 ports (100 MB or higher)	1-4 ports (100 MB or higher)	1-4 ports (1 GB or higher)
Maximum concurrent VPN sessions **Blended support for SSL and IPSec** **VPN users**	250	1000	5000
Deployment positioning	Entry-level solution	Mid-range solution	High-end solution

Layered security

Designed as a hardened security/web appliance, Avaya's VPN Gateway provides a suite of safeguard features to help protect the enterprise against malicious intent and user negligence. These include:

- **Endpoint Access Control Agent** (for SSL and IPSec) that performs endpoint security checking on both client and clientless VPN endpoints. Enables administrators to define endpoint security policies on the VPN Gateway itself and helps ensure that remote users/devices are inspected for compliance before access is granted.
- **Cache cleaner** for endpoints that helps ensure software downloads and temp files installed at login are erased at logout, allowing no data to be left behind.
- **Strong user authentication** that includes support for best-of-breed options — including secure tokens, smart cards and X.509 certificates.
- **Flexible access controls** that can be tailored to how or from where a user is accessing the network; for example, full network access from a managed PC versus intranet and e-mail access from a less trusted device.
- **Auto log-off** that automatically terminates a session after a configurable period of inactivity to address security in public and shared device situations.
- **Private-side encryption** that meets mandated legislative requirements for data confidentiality and security (HIPPA, GLB, Patriot Act, etc.).
- **Portal Guard** is a unique feature that offloads SSL termination and public key operations from internal servers and provides a low-cost means for secure access to internal enterprise portals.

Avaya VPN Gateway Product specifications

Security features

Authentication

- RADIUS and challenge/response
- LDAP, Windows NT Domain
- Native local user database
- SC SafeWord, RSA SecurID, Entrust IdentityGuard
- Novell NDS/eDirectory
- X.509 Digital Certificate
- Microsoft Active Directory

Single Sign-on (SSO)

- WFS, Web apps HTTP, form based authentication
- HTTP headers
- SSO with CA SiteMinder, RSA ClearTrust
- Domain/network specific sign-on SSO Authorization
- Dual-profile authorization
- Base profile includes network, service and application level information (Layer 3, 4/7)
- Extended profile adds source network, client security and authentication method
- Endpoint security status and access method (Tunnel Guard/SSL) Security protocols
- SSL v2.0, 3.0
- TLS 1.0 (RFC 2246)
- IPsec ESP, AH

Cipher suites

- All ciphers covered by SSLv2.0, 3.0 and TLSv1.0 except the IDEA ciphers and the FORTEZZA ciphers

Accounting

- Syslog/RADIUS account start and stop including user name, gateway address, session ID, session time and cause of termination

Client security

- Avaya Endpoint Access Control Agent (aka Tunnel Guard)
- Auto-logoff with countdown
- Rewriting to no-cache/no-store headers
- Cache cleansing of files/history
- Dynamic access policies
- Malware Detection

Avaya VPN Client Support

- Split Tunneling
- Avaya Endpoint Access Control Agent (for both IPsec and SSL)
- Avaya VPN Client Mobility
- Portal full-access tab
- Certificate-based authentication
- **LT2P/IPSec Client Support, including support for tablets and smart phones**

Other Features & Capabilities

Load balancing

- SSL service load balancing via clustering
- Load balancing of back-end services to include Source IP and round robin session persistence
- Source IP, SSL session ID, cookie information application health checking
- SSL w/TCP/IP/Port
- Scriptable, configurable intervals

Application support

- Access to web-based, client/server and native terminal server applications
- Network-layer native desktop application access via SSL or IPSec mode Web content and protocols
- HTML/DHTML
- JavaScript/Java Applets/XML
- HTTP/HTTPS
- VBScript

Management

- Secure administrative Web GUI (HTTPS)
- Serial port to CLI
- Local logging, external Syslog
- VPN Cluster Manager – Multi-site management and monitoring

Browser support

- Microsoft Windows (2000, XP, Vista, Windows 7)
- Internet Explorer 6 or greater
- Mozilla FireFox 3.0 or greater
- MacOS 10.4 or greater
- Safari 3.0 or higher

Modes of operation

- Clientless—HTML to browser
- Enhanced Clientless—Proxy with Java Applet
- Full Network Extension—SSL Client (Net Direct) delivered via download or Avaya VPN Client access

Feature Licenses

- Portal Guard
- Secure Portable Office Feature

Concurrent User Licenses

- SSL and IPsec User licenses
- Emergency Remote Access (ERA)
- IPSec Only
- Secure Portable Office Client Licenses (per seat)

Learn More

To learn more about the Avaya VPN Gateway please contact your Avaya Account Manager or Avaya Authorized Partner or visit us at **avaya.com**.

About Avaya

Avaya is a global provider of business collaboration and communications solutions, providing unified communications, contact centers, networking and related services to companies of all sizes around the world. For more information please visit **www.avaya.com**.

08/12 • DN5111-04