

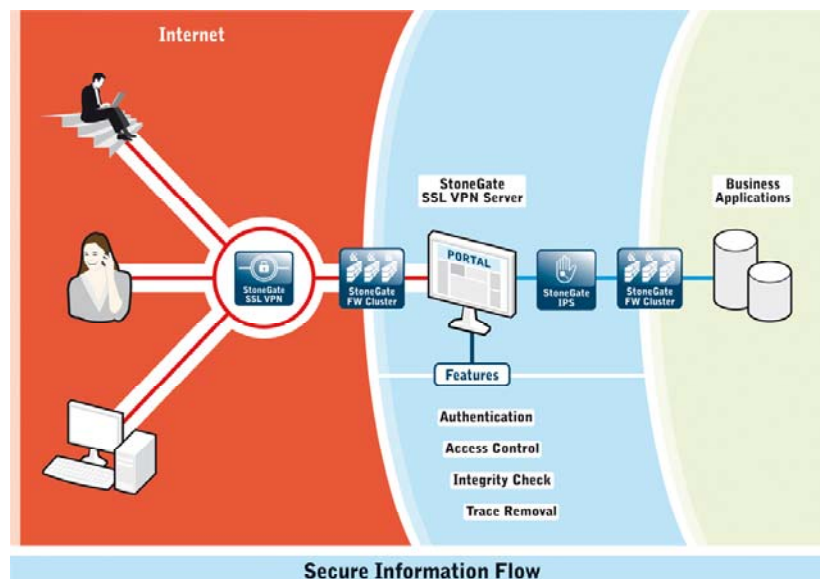
Frequently Asked Questions About StoneGate SSL VPN (April 2008)

Q: When I should use StoneGate SSL VPN and when IPSec VPN?

A: The StoneGate SSL VPN solution is designed for the needs of regular remote/mobile users, while an IPSec VPN solution is targeted for power users and administrators.

StoneGate SSL VPN offers secure, easy to use web portal access to applications from anywhere, at any time, and with any device. It does not require a client, so it is easy to use but also very easy to administer.

While an IPSec VPN solution also offers a direct, unlimited, and secure remote network access, it differs from SSL VPN in the respect that it requires a client.



Security:

Q: What security features are implemented in StoneGate SSL VPN?

A: StoneGate SSL VPN provides proxy access for additional network security. Additionally, it provides inbuilt security features such as two-factor authentication, role based access control, connection trace removal and network access control to prevent unsecured devices entering the network.

Q: Does StoneGate SSL VPN allow end users access back end systems directly?

A: No SSL VPN solution operates in this manner. Instead, a separate connection is established between the client and the gateway, after which the gateway establishes a separate connection from the gateway to the server. Therefore, end users have no direct connection to back end systems. This technology is called proxy access.

Q: Does StoneGate SSL VPN support the full assessment of a user's workstation before allowing them access to an application?

A: Yes, the system can identify the status of anti-virus updates, running applications, installed programs, registry keys and even open network ports. Through this assessment system, it is possible to provide complete security for user workstations. The StoneGate assessment feature is extremely flexible and an API is available for customers that wish to extend this.

Q: Does StoneGate SSL VPN block or stop the up- or download of attachments in Outlook Web Access?

A: Yes, StoneGate SSL VPN can block any upload or download of attachments through the SSL VPN connection. This prevents the user from downloading documents to an insecure workstation.

Q: Does StoneGate SSL VPN clean up the data and Web cache once you logout of the SSL VPN to leave no trace of any documents or files as required?

A: Yes, the StoneGate SSL VPN solution has an abolition feature that can be fine-tuned and configured according to the needs of the situation. You can clean up a Web browser cache, delete downloaded files and even run custom scripts to ensure no trace of data is left on the workstation.

Q: How is network access controlled in StoneGate SSL VPN?

A: StoneGate SSL VPN offers 16 different authentication methods to identify users. Identified users can be granted access separately for each application, or users can be categorized as groups. For example, users who access the network from their home computer using two-factor authentication during off hours can be granted access only to certain applications. This makes user management significantly easier.
In StoneGate SSL VPN portal, users can see only the applications they can access. This way the same portal can be used to host services that are targeted for different user groups like employees, customers and partners.

Q: Does StoneGate support two-factor authentication systems? And do I have to buy a separate module for that?

A: Yes, StoneGate SSL VPN includes an integrated built-in two-factor authentication system that provides strong user authentication. This is available at no extra cost. The client software is available for many platforms, including PDAs and mobile phones, and is free to use with no charges. Additionally, StoneGate SSL VPN supports a number of two-factor authentication systems, pre-configured with the system. Support is available for RSA SecurID, ActivCard, Vasco, and several other systems.

Q: Does StoneGate support single sign-on for applications?

A: Yes, StoneGate includes a sophisticated single sign-on system is possible to allow single sign-on to several applications, regardless of whether they are Web or client-server applications. Combined with the ability to customize the SSL VPN portal, this capability makes the StoneGate SSL VPN solution extremely flexible. For instance, it is possible to completely hide the portal and have your own application transparently accessed through it.

Q: Does StoneGate SSL VPN support a virtual desktop environment for a "sandbox" when users are connecting via an insecure workstation?

A: Yes, StoneGate SSL VPN integrates with the Sygate on-demand system, providing a virtual environment where no traces of the SSL VPN connection remain at the local workstation. This prevents the user from that saving documents, files or other information to the local workstation when it is not allowed.

General issues:

Q: What do I need to access the StoneGate SSL VPN Portal?

A: You need a device with a standard web browser; for example a PC, a mobile phone or a PDA. The StoneGate SSL VPN portal view adapts according to your device.

Q: What if the device I am using doesn't have the needed application installed?

A: If the application has a Web interface available, you can access it over SSL VPN. If the application is a client-server application, the client has to be installed on the local device.

Q: Does StoneGate SSL VPN support network level access through the SSL VPN connection?

A: Yes, it does. StoneGate SSL VPN supports dynamic tunnels for Windows clients. Tunnels enable transparent access over SSL VPN to a range of addresses and TCP or UDP ports.

Integration to other systems:

Q: Does StoneGate SSL VPN integrate with third-party directory services?

A: Yes. StoneGate integrates, for example, with Microsoft Active Directory and Novell eDirectory, among others.

Q: Does StoneGate SSL VPN have tight integration with Citrix so that it handles an application correctly?

A: Yes, StoneGate has a simple wizard that enables you to setup a Citrix Presentation Server and Metaframe members in just a couple of minutes. This configuration correctly handles the sessions and ensures that it is tightly integrated. Single-sign-on is fully supported through to the desktop, if required.