

SonicWALL SSL VPN 2.5 HTTP(S) Reverse Proxy Support

Document Scope

This document describes the implementation of reverse proxy to provide HTTP and HTTPS access to Microsoft Outlook Web Access (OWA) Premium and IBM Lotus Domino Web Access 7 on SonicWALL SSL VPN 2000/4000 appliances running 2.5 firmware.

This document contains the following sections:

- [“HTTP\(S\) Reverse Proxy Overview” section on page 2](#)
 - [“What is HTTP\(S\) Reverse Proxy?” section on page 2](#)
 - [“Benefits” section on page 2](#)
 - [“Platforms” section on page 2](#)
 - [“Supported Standards” section on page 2](#)
 - [“How Does HTTP\(S\) Reverse Proxy Work?” section on page 3](#)
- [“Using Reverse Proxy” section on page 7](#)
 - [“Creating an HTTP or HTTPS User Bookmark” section on page 7](#)
 - [“Creating User/Group/Global Policies for URL Objects” section on page 8](#)
 - [“Policy URL Object Field Elements” section on page 9](#)
 - [“Using HTTP and HTTPS Bookmarks” section on page 10](#)

HTTP(S) Reverse Proxy Overview

This section provides an introduction to reverse proxy. This section contains the following subsections:

- [“What is HTTP\(S\) Reverse Proxy?” section on page 2](#)
- [“Benefits” section on page 2](#)
- [“Platforms” section on page 2](#)
- [“Supported Standards” section on page 2](#)
- [“How Does HTTP\(S\) Reverse Proxy Work?” section on page 3](#)

What is HTTP(S) Reverse Proxy?

A reverse proxy is a proxy server that is deployed between a remote user outside an intranet and a target Web server within the intranet. The reverse proxy intercepts and forwards packets that originate from outside the intranet. An HTTP(S) reverse proxy specifically intercepts HTTP(S) requests and responses.

SonicWALL utilizes HTTP(S) reverse proxy on SonicWALL SSL VPN appliances running 2.5 firmware to provide access to the enhanced versions of commonly-used Web mail interfaces, including Microsoft OWA Premium and Domino Web Access 7.

Benefits

HTTP(S) reverse proxy provides users access to more feature-rich versions of the Microsoft OWA Premium and Domino Web Access 7 Web mail interfaces. These interfaces are easier to use and provide more enhanced features than their basic counterparts. For a full description of features supported using HTTP(S) reverse proxy, refer to [“Microsoft OWA Premium Support” section on page 3](#) and [“Lotus Domino Web Access 7 Support” section on page 5](#).

Platforms

Reverse proxy support is available on the SonicWALL SSL VPN series appliances running firmware version 2.5. Microsoft OWA Premium and Domino Web Access 7 are only available on the SonicWALL SSL VPN 2000/4000 platforms.

Supported Standards

The following requirements must be met in order to access the HTTP(S) reverse proxy features in Microsoft OWA Premium and Domino Web Access 7:

- Internet Explorer 5.0 or later
- Windows 2000, Windows XP, or Windows Server 2003



Note

S/MIME support and bi-directional layout support for Arabic and Hebrew in Microsoft OWA Premium are only available using Internet Explorer 6 SP1. GZip compression supported by Microsoft OWA Premium is not supported through the reverse proxy.

**Note**

Domino Web Access 7 uses ActiveX controls for access using Internet Explorer 5.0 and later. Single sign-on is not supported for Domino Web Access 7 through the reverse proxy.

How Does HTTP(S) Reverse Proxy Work?

SonicWALL SSL VPN 2.5 HTTP(S) reverse proxy provides enhanced application support for Microsoft OWA Premium and Domino Web Access 7. Using HTTP(S) reverse proxy to access Microsoft OWA Premium and Domino Web Access 7 Web-based clients, more features are accessible to users.

This section contains the following subsections:

- “Microsoft OWA Premium Support” section on page 3
- “Lotus Domino Web Access 7 Support” section on page 5

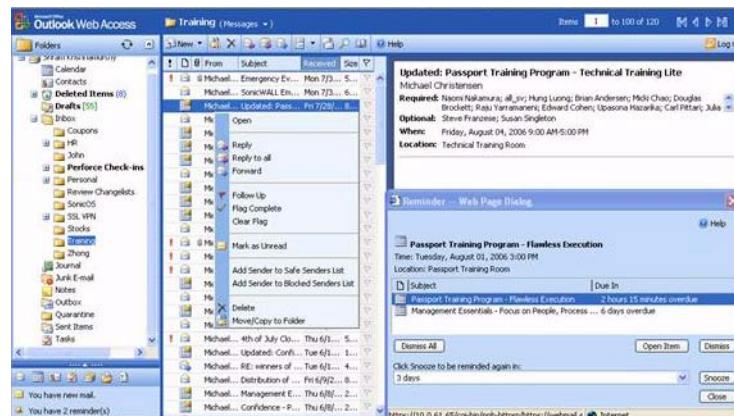
**Tip**

If you are using the correct Web browser and operating system, and a supported application doesn't work, delete the browser session cookies, close and reopen all instances of your browser, clear the browser cache, then try again.

Microsoft OWA Premium Support

Microsoft OWA Premium mode is a Web client for Microsoft Outlook 2003/2007 that simulates the Microsoft Outlook interface and provides more features than basic OWA. Microsoft OWA Premium includes features such as spell check, creation and modification of server-side rules, Web beacon blocking, support for tasks, auto-signature support, and address book enhancements. [Figure 1](#) provides a view of the Microsoft OWA Premium interface using SonicWALL SSL VPN 2.5 HTTP(S) reverse proxy.

Figure 1 Microsoft OWA Premium



SonicWALL SSL VPN HTTP(S) reverse proxy application support for Microsoft OWA Premium, using Internet Explorer 5.0 or higher, provides users with full functionality of the following features:

- Access to email, calendar, and tasks
- New Outlook look-and-feel, including right-click functionality
- Ability to mark an email as unread

- Server-side spelling checker (limited to six languages)
- Forms-based authentication (session time-out)
- S/MIME support



Note

S/MIME support for Microsoft OWA Premium is only available on Internet Explorer 6 SP1.

- Two-line view
- Context menus
- Improved keyboard shortcuts
- Ability to forward meeting requests
- Notifications on navigation pane
- Ability to add to contacts
- Ability to pick names from address book
- Ability to set maximum number of messages displayed in views
- Support for bi-directional layout for Arabic and Hebrew



Note

Bi-directional layout support for Arabic and Hebrew for Microsoft OWA Premium is only available on Internet Explorer 6 SP1.

- Option to set message status “mark as read” when using the reading pane
- Public folders display in their own browser window
- Access to GAL property sheets within an email message or meeting request
- Message sensitivity settings on information bar
- Attendee reminder option for meeting request
- Ability to launch the calendar in its own window
- User interface to set common server-side rules
- Outlook style Quick Flags
- Support for message signatures
- Search folders (must be created in Outlook online mode)
- Deferred search for new messages after delete
- Attachment blocking
- Web beacon blocking to make it more difficult for senders of spam to confirm email addresses
- Protection of private information when a user clicks a hyperlink in the body of an email message



Tip

For better performance, it is recommended that the Exchange administrator configure OWA to list at the most 40 items in any page. This can be done in the Outlook Web Access Administration Web-based utility provided part of the Exchange installation. Navigate to **Server Settings > Administration > View Settings**. On the View Settings page, the **Maximum View Rows** attribute defines the maximum row count of items visible in any view. From the drop-down menu, select 40 or less and click **OK**.



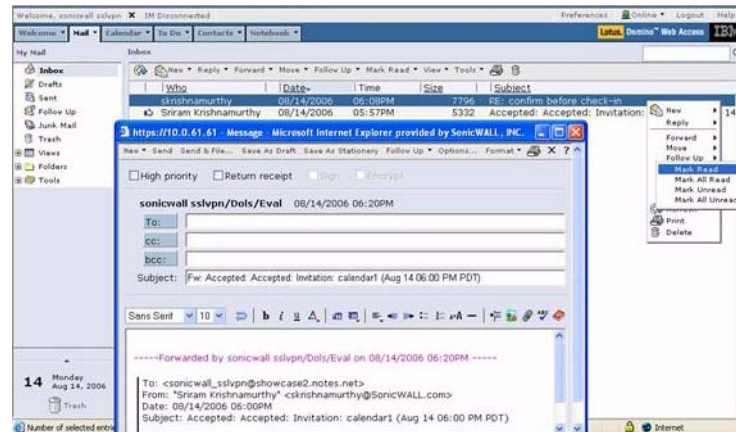
Note

GZip compression supported by Microsoft OWA Premium is not supported through the reverse proxy.

Lotus Domino Web Access 7 Support

Lotus Domino Web Access 7 is a Web client for IBM Lotus Domino server with an easy-to-use interface. It provides features such as advanced Web messaging and rich-text messages, scheduling meetings, managing tasks, collaboration, and managing personal information. Domino Web Access 7 also provides increased server capability and reduced CPU usage to boost performance and response time. [Figure 2](#) provides a view of the Lotus Domino Web Access 7 interface using SonicWALL SSL VPN 2.5 HTTP(S) reverse proxy.

Figure 2 Lotus Domino Web Access 7



Note

Domino Web Access 7 uses ActiveX controls for access using Internet Explorer 5.0 and later.

SonicWALL SSL VPN HTTP(S) reverse proxy application support for Domino Web Access 7, using Internet Explorer 5.0 or higher, provides users with full functionality of the following features:

- Email
 - Send and receive email
 - Send and receive attachments
 - Delete messages
 - Open attachment from reading and preview panes
 - Spell check
 - Quick Flags and message flags
 - Set message importance
 - Send and receive HTML mail
 - Mark messages as read or unread
- Navigation
 - Navigate folder hierarchy in navigation pane
 - Sort message list by standard fields
 - Search capabilities
 - Logout
- Calendar

- Calendar views of different time periods
- Create a meeting
- Check schedule
- Use address book to pick attendees
- Search for resource
- Change invitee list
- Delete meeting
- Folders and storage
 - Create a folder
 - Move messages using drag and drop
 - Recover from trash
 - Empty trash
- Contacts
 - View by options
 - Add and edit contacts
 - Delete contact
- Tasks and options
 - Create a to-do list
 - View to-do list
 - Use notebook to create a new note.
 - Delegation
 - Change password
 - Display options
 - Change notes ID
 - Out of office settings
- Rules
 - Create new mail and quick rules
 - Delete rules
 - Test created rules



Note

Single sign-on is not supported for Domino Web Access 7.

Using Reverse Proxy

The SSL VPN administrator can configure Web (HTTP) or Secure Web (HTTPS) bookmarks to allow user access to Web-based resources and applications such as Microsoft OWA Premium or Domino Web Access 7 with HTTP(S) reverse proxy support. When user or group bookmarks are defined, the user or group member will see the defined bookmarks on the SonicWALL SSL VPN appliance Virtual Office home page.

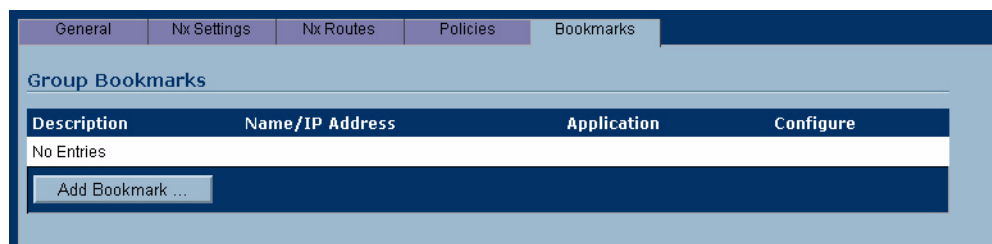
This section contains the following subsections:

- “Creating an HTTP or HTTPS User Bookmark” section on page 7
- “Creating User/Group/Global Policies for URL Objects” section on page 8
- “Using HTTP and HTTPS Bookmarks” section on page 10

Creating an HTTP or HTTPS User Bookmark

To create HTTP or HTTPS user bookmarks, perform the following steps:

-
- Step 1** Log into your SonicWALL SSL VPN.
- Step 2** From the **Users** tab, select either **Local Users** or **Local Groups**.
- Step 3** Click the **Configure** icon next to the user or group for which you want to create the bookmark.
- Step 4** Select the **Bookmarks** tab.



- Step 5** Click **Add Bookmark**. The **Add Bookmark** dialog box displays.

- Step 6** Type the name of the bookmark in the **Bookmark Name** field.
- Step 7** Enter the HTTP or HTTP(S) address of your Web mail server in the **Name or IP Address** field. For example, webmail.company.com or company.notes.net/example/mail.



Note

For HTTP and HTTPS bookmarks you can specify custom ports and paths, for example “www.mycompany.com:8080”.

- Step 8** If you are creating the bookmark for a **Local User**, you have the option to allow or deny users the ability to edit or delete this bookmark.
- Select **Allow** from the **Allow user to edit/delete** drop-down menu to allow them to edit or delete the bookmark.
 - To prevent users from editing or deleting the bookmark, select **Deny**.
 - To allow or deny based on the individual user policy, select **Use user policy**.



Note Only **Local Users** bookmarks have the option of allowing users edit/delete privileges. Bookmarks created in the **Local Groups** tab are permanently displayed on portals for all users in the group and can only be removed or edited by the administrator.

- Step 9** Select **Web (HTTP)** or **Secure Web (HTTPS)** the service type in the **Service** pull-down menu.

- Step 10** Click **Add** to add the bookmark. Once the configuration has been updated, the new user bookmark will be displayed in the **Edit User Settings** window.

Creating User/Group/Global Policies for URL Objects

To create object-based HTTP or HTTPS user policies, perform the following steps:

- Step 1** Navigate to **Users > Local Users**.
- Step 2** Click the configure icon next to the user you want to configure.
- Step 3** Select the **Policies** tab.
- Step 4** Click **Add Policy...**
- Step 5** In the **Apply Policy To** drop-down menu, select the **URL Object** option.

- Step 6** Define a name for the policy in the **Policy Name** field.
- Step 7** In the **Service** pull-down menu and choose either **Web (HTTP)** or **Web (HTTPS)**.

Step 8 In the **URL** field, add the URL string to be enforced in this policy.



Note In addition to standard URL elements, the administrator may enter port, path and wildcard elements to the URL field.

If a path is specified, the URL policy is recursive and applies to all subdirectories. If, for example “www.mycompany.com/users/*” is specified, the user is permitted access to any folder or file under the “www.mycompany.com/users/” folder.

For more information on using these additional elements, refer to the [“Policy URL Object Field Elements” section on page 9](#).

Step 9 In the **Status** pull-down menu, click on an access action, either **PERMIT** or **DENY**.

Step 10 Click **Add**.

Policy URL Object Field Elements

When creating an HTTP/HTTPS policy, the administrator must enter a valid host URL in the **URL** field. In addition, the administrator may enter port, path and wildcard elements to this field. The following chart provides an overview of standard **URL** field elements:

Element	Usage
Host	Can be a hostname that should be resolved or an IP address. Host information has to be present.
Port	If port is not mentioned, then all ports for that host are matched. Specify a specific port or port range using digits [0-9], and/or wildcard elements. Zero “0” must not be used as the first digit in this field. The least possible number matching the wildcard expression should fall within the range of valid port numbers i.e. [1-65535].
Path	This is the file path of the URL along with the query string. A URL Path is made of parts delimited by the file path separator ‘/’. Each part may contain wildcard characters. The scope of the wildcard characters is limited only to the specific part contained between file path separators.
Username	%USERNAME% is a variable that matches the username appearing in a URL requested by a user with a valid session. Especially useful if the policy is a group or a global policy.
Wildcard Characters	The following wildcard characters are used to match one or more characters within a port or path specification. * – Matches one or more characters in that position ^ – Matches exactly one character in the position. [!<character set>] – Matches any character in that position not listed in character set. E.g. [!acd], [!8a0] <range> – Matches any character falling within the specified ASCII range. Can be an alphanumeric character. E.g.) [a-d], [3-5], [H-X]



Note Entries in the **URL** field can not contain (“http://”, “https://”) elements. Entries can also not contain fragment delimiters such as “#”.

Using HTTP and HTTPS Bookmarks

HTTP or HTTPS bookmarks are accessed directly from the Virtual Office. To use HTTP(S) bookmarks, perform the following steps:

-
- Step 1** Log into the SonicWALL Virtual Office.
- Step 2** Click on the **Web (HTTP)** or **Secure Web (HTTPS)** bookmark.

A new window is launched in your default browser that connects to the domain name or IP address specified in the bookmark.



Note

Microsoft OWA Premium and Lotus Domino Web Access are supported in SSL VPN 2.5. For information about non HTTP(s) bookmarks, refer to the *SonicWALL SSL VPN 2.5 Administrator's Guide*.

Glossary

GAL: Global Address List maintained by MS Exchange server.

HTTP(S) Reverse Proxy: A reverse proxy that intercepts HTTP(S) requests and responses.

Reverse Proxy: A reverse proxy is a proxy server that is deployed between a remote user outside an intranet and a target Web server within the intranet. The reverse proxy intercepts and forwards packets that originate from outside the intranet.

Web beacon: A Web beacon is an often-transparent graphic image that is used to monitor the behavior of the user visiting the Web site or sending the email. It is used to send back information such as the IP address of the client, the browser type and any cookies that may have been set before.

Solution Document Version History

Version Number	Date	Notes
2	11/06/2007	Updated for 2.5, added Policy URL Field section (PL, SK).
1	10/11/2006	This document was created.

P/N 232-001308-00