

Placing the BlackBerry Enterprise Server for Microsoft Exchange in a demilitarized zone

Originally posted: June 2002

Affected software versions

BlackBerry™ Enterprise Server version 2.0 for Microsoft® Exchange

BlackBerry Enterprise Server version 2.1 for Microsoft Exchange

BlackBerry Enterprise Server version 3.5 for Microsoft Exchange

Summary

Some organizations support the placement of Internet-facing servers in demilitarized zones. However, Research In Motion (RIM) recommends against placing a BlackBerry Enterprise Server in a demilitarized zone, and does not support this configuration. This document explains how placing a BlackBerry Enterprise Server in a demilitarized zone can reduce the security level of the zone and can impact BlackBerry Enterprise Server features.

Connecting to the SRP host

Note: The Server Relay Protocol (SRP host) is `srp.xx.blackberry.net`, where “xx” is a variable that represents “na” for a BlackBerry Enterprise Server in North America and “eu” for a BlackBerry Enterprise Server in Europe.

When you start the BlackBerry Enterprise Server service, it makes a persistent Transmission Control Protocol (TCP) connection to the SRP host using one of two methods.

Placing the BlackBerry Enterprise Server behind the firewall

A secure connection requires authentication from both sides of the connection: the BlackBerry Enterprise Server service and the SRP host. The method in which the BlackBerry Enterprise Server is placed behind the firewall is illustrated below (figure 1).

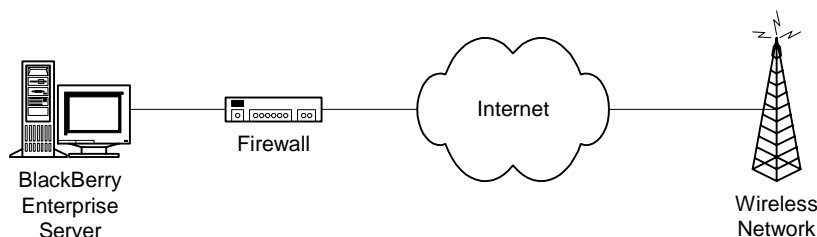


Figure 1: BlackBerry Enterprise Server behind a firewall

In this method, the firewall must be configured so that the BlackBerry Enterprise Server can initiate a TCP connection through the firewall to the SRP host. The connection type is outbound-initiated only; no host can initiate an inbound connection to your BlackBerry Enterprise Server.

Note: When you configure the firewall to enable the connection to the SRP host, RIM recommends that you do not limit the connection to a specific IP address because RIM might add to the SRP host additional IP addresses that provide additional redundancy or fail-over protection.

Placing the BlackBerry Enterprise Server in a demilitarized zone

The second connection method involves installing the BlackBerry Enterprise Server in a demilitarized zone. This method is illustrated below (figure 2).

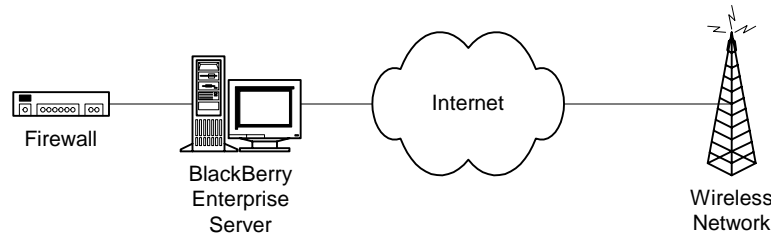


Figure 2: BlackBerry Enterprise Server in a demilitarized zone

Because the BlackBerry Enterprise Server requires a MAPI connection to each Microsoft® Exchange Server that hosts mailboxes for BlackBerry users, this method requires extensive configuration changes. You must reconfigure the firewall and each Microsoft Exchange Server. Because the BlackBerry Enterprise Server connects to each mailbox server using MAPI, the configuration is identical to the configuration that enables Microsoft Outlook® users to connect to their Microsoft Exchange Servers through the firewall. You must complete the following changes:

Microsoft Exchange Server

- ◆ Configure the Microsoft Exchange Server so that it uses static ports.

Firewall

- ◆ Open static ports to enable the BlackBerry Enterprise Server to connect through the firewall to each Microsoft Exchange Server on the static ports.
- ◆ Open the network authentication ports (such as Kerberos) to enable the BlackBerry Enterprise Server to authenticate to a domain controller.

If you use the first connection method, you have to open only one TCP connection. If you use the second connection method, you must open multiple ports, both TCP and User Datagram Protocol (UDP).

If you use the second connection method, the proximity of the BlackBerry Enterprise Server to the mail servers to which it is connecting might affect the stability of the BlackBerry Enterprise Server. MAPI is not a TCP application and performs better with a direct connection to the destination host.

Note: The versions of the BlackBerry Enterprise Server that are discussed in this document do not require a connection to a Global Catalog Server for remote address lookups.

Mobile Data Service

If you place the BlackBerry Enterprise Server inside the firewall, features that are available in BlackBerry Enterprise Server version 3.5 for Microsoft Exchange, such as Mobile Data Service (MDS), are supported. MDS creates a conduit between the BlackBerry handheld and your intranet and other corporate data.

If the BlackBerry Enterprise Server on which Mobile Data Service is installed is located outside your firewall, you cannot access intranet data unless you open the firewall further to enable access to internal data sources such as the corporate intranet or customer relationship management (CRM) application databases.

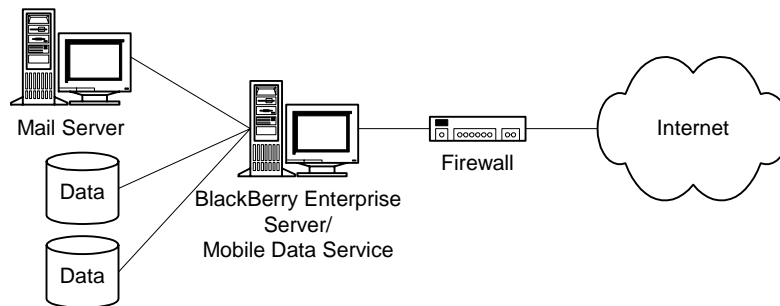


Figure 3: Mobile Data Service enables connectivity to intranet data

Alternatives to placing the BlackBerry Enterprise Server in a demilitarized zone

If strict corporate policy prohibits direct communication between internal servers and Internet hosts, two alternative methods are available. RIM supports both alternative configurations.

Using a proxy server

This connection method uses a proxy server that is located in the demilitarized zone. In this configuration, the BlackBerry Enterprise Server connects to your proxy server only. The proxy server then communicates with the wireless network over the Internet as illustrated below (figure 4).

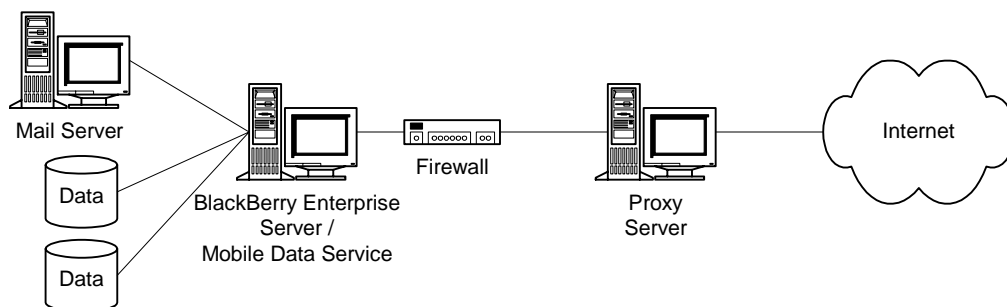


Figure 4: BlackBerry Enterprise Server connects directly to the proxy server

Using a proxy server has the following security characteristics:

- ◆ The proxy server can be configured to enable only the BlackBerry Enterprise Server to make port 3101 requests.
- ◆ The firewall can be configured to enable only the BlackBerry Enterprise Server to connect through port 3101, which prevents all internal servers from communicating to the Internet through port 3101.

Note: The proxy server that is selected must support a transparent proxy. The BlackBerry Enterprise Server does not know how to use a proxy; it requires the appearance of a direct connection to the SRP host. Several proxy servers enable this configuration (for example, Microsoft ISA server and Microsoft Proxy Server). Each server requires the installation of an agent on the client (the BlackBerry Enterprise Server) that gives the appearance of a direct connection.

Using port forwarding (IP port translation)

This connection method uses port forwarding at the firewall. In this configuration, the BlackBerry Enterprise Server is configured to connect to `<firewall.yourdomain>.com` instead of the SRP host. The firewall must be configured to forward port 3101 requests to the SRP host.

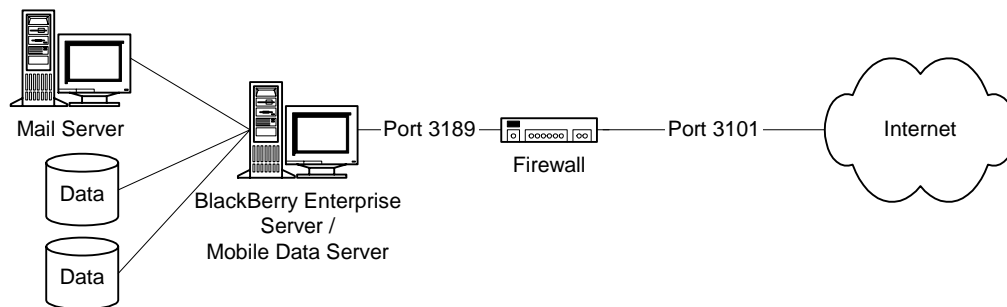


Figure 5: BlackBerry Enterprise Server connected to the firewall

Firewall and proxy configuration

Because many firewalls and proxy solutions exist, RIM does not support any specific firewall or proxy solution. Configuration of proxy servers and firewalls are the responsibility of each individual organization. This document only provides the information that is required to implement a solution.

For assistance with the configuration your firewall or proxy, contact your solution vendor.

Conclusion

When you install the BlackBerry Enterprise Server for Microsoft Exchange, RIM recommends that you place the server inside your corporate firewall, as close as possible to the mail server that it services (for example, on the same switch). Placing the BlackBerry Enterprise Server outside the firewall reduces the overall security of your demilitarized zone. If strict corporate policy prohibits direct communication between internal servers and Internet hosts, two alternative methods are available: using a proxy server or Port Address Translation (PAT). RIM supports both alternative configurations.



Appendix A: Relevant Microsoft Q articles

XADM: No Way to Configure Port for UDP New Mail Notification Packets (Q264035)

You can configure a Microsoft Exchange Server computer so that it uses specific TCP ports for the information store, directory, and System Attendant. This configuration enables access to the Microsoft Exchange Server through a firewall, router, or other device that blocks certain TCP or UDP ports. You cannot configure the ports that are used when the Microsoft Exchange Server sends a client a new mail notification packet. In a situation in which UDP traffic from the Microsoft Exchange Server to the client is blocked, clients might not receive new mail notification.

XADM: Setting TCP/IP Ports for Exchange and Outlook Client Connections Through a Firewall (Q155831)

This article explains how to enable the Microsoft Exchange Client so that it connects to the Microsoft Exchange Server over an existing connection to the Internet and through a firewall. To enable this connection, you must verify that the ports that are assigned to these connections are static. This requires that you add entries to the registry.

XCLN: Exchange 2000 Static Port Mappings (Q270836)

This article explains how to enable Microsoft Exchange down-level MAPI clients' computers (either Microsoft Exchange client computers or client computers that are using Microsoft Outlook in Corporate or Workgroup mode on the Microsoft Exchange 2000 Server) so that they connect to the Microsoft Exchange 2000 Server over an existing connection to the Internet through a firewall.

XCLN: How MAPI Clients Access Active Directory (Q256976)

In Microsoft Exchange Server 4.0, 5.0, and 5.5, the directory service is on the server to which MAPI clients log in and look up addresses in the Global Address List. In Microsoft Exchange 2000, the directory service integrates with the Microsoft Windows 2000 operating system (Active Directory). As a result, the directory service might or might not be located on the Microsoft Exchange 2000 Server. In this environment, a MAPI client accesses the directory and logs in mailboxes differently than previous versions of the Microsoft Exchange Server. This article explains how each version of Microsoft Outlook and Microsoft Exchange Client accesses the Active Directory.

Part number: TAE-00038-001

© 2002 Research In Motion Limited. All rights reserved. The BlackBerry and RIM families of related marks, images and symbols are the exclusive properties of Research In Motion Limited. RIM, Research In Motion, 'Always On, Always Connected', the "envelope in motion" symbol and the BlackBerry logo are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries. All other brands, product names, company names, trademarks and service marks are the properties of their respective owners. The handheld and/or associated software are protected by copyright, international treaties and various patents, including one or more of the following U.S. patents: 6,278,442; 6,271,605; 6,219,694; 6,075,470; 6,073,318; D,445,428; D,433,460; D,416,256. Other patents are registered or pending in various countries around the world. Please visit www.rim.net/patents.shtml for a current listing of applicable patents.

RESEARCH IN MOTION LIMITED (RIM) ON BEHALF OF ITSELF AND ITS AFFILIATES MAKES NO REPRESENTATIONS ABOUT THE SUITABILITY OF THE INFORMATION OR GRAPHICS CONTAINED IN THIS ADVISORY FOR ANY PURPOSE. THE CONTENT CONTAINED IN THIS DOCUMENT, INCLUDING RELATED GRAPHICS, ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. RIM HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH REGARD TO THIS INFORMATION, INCLUDING ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL RIM BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF INFORMATION CONTAINED HEREIN. THIS DOCUMENT, INCLUDING ANY GRAPHICS CONTAINED WITHIN THE DOCUMENT, MAY CONTAIN TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. UPDATES ARE PERIODICALLY MADE TO THE INFORMATION HEREIN AND RIM MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED HEREIN AT ANY TIME.