

UNCLASSIFIED



Communications Security
Establishment

Centre de la sécurité
des télécommunications



BlackBerry® Enterprise Server Isolation in a Microsoft Exchange Environment

(ITSG-23)

March 2007

UNCLASSIFIED



Communications Security
Establishment

Centre de la sécurité
des télécommunications



***BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)***

This page intentionally left blank.

March 2007

Canada



***BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)***

Foreword

The *BlackBerry® Enterprise Server Isolation in a Microsoft Exchange Environment (ITSG-23)* is an Unclassified publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

Requests for additional copies or changes in distribution should be directed to your Client Services Representative at CSE.

For further information, please contact CSE's ITS Client Services area by e-mail at client.svcs@cse-cst.gc.ca or call (613) 991-7600.

Effective Date

This publication takes effect on (03/01/2007).

Gwen Beauchemin
Director, IT Security Information Management

© 2007 Government of Canada, Communications Security Establishment

It is not permissible to make copies or extracts from this publication without the written consent of CSE.

UNCLASSIFIED



Communications Security
Establishment

Centre de la sécurité
des télécommunications



***BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)***

This page intentionally left blank.



***BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)***

Executive Summary

This guidance document details how to configure a network so that a BlackBerry Enterprise Server may be isolated from the internal network through the use of a firewall. It describes the changes to the Microsoft Exchange Server and domain controller that are necessary for email and domain interaction through the firewall.

UNCLASSIFIED



Communications Security
Establishment

Centre de la sécurité
des télécommunications



***BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)***

This page intentionally left blank.

UNCLASSIFIED



Communications Security
Establishment

Centre de la sécurité
des télécommunications



***BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)***

This page intentionally left blank.



BlackBerry Enterprise Server Isolation in a Microsoft Exchange Environment (ITSG-23)

Table of Contents

Foreword..... i

Effective Date i

Executive Summary iii

Revision History v

Table of Contents vii

List of Tables ix

List of Figures ix

List of Abbreviations and Acronyms xi

1 Introduction 1

 1.1 Purpose 1

 1.2 Scope 1

 1.3 Stakeholders 2

 1.4 Assumptions 2

2 System Description 3

 2.1 Advantages 3

 2.2 Disadvantages 3

 2.3 Ports Needed 4

 2.3.1 Outbound Ports 4

 2.3.2 Inbound Ports 4

 2.4 Limitations 5

3 System Configuration 7

 3.1 Configuring static MAPI ports 7

 3.1.1 Procedure for statically mapping MAPI ports 7

 3.2 Configuring Active Directory 7

 3.2.1 Procedure for mapping Active Directory 8

 3.3 Configuring the Firewall 8

 3.3.1 Test Network IP Addresses 8

 3.3.2 Set the IP Addresses 9

 3.3.3 Configure routing 9

 3.3.4 Creating the Access List 10

 3.3.5 Creating the Access Group 12

 3.3.6 Saving the configuration 12



BlackBerry Enterprise Server Isolation in a Microsoft Exchange Environment (ITSG-23)

4 Conclusions and Recommendations 15

5 References 17

A. Appendix – Firewall Configuration Script 19

 A.1. Firewall Configuration Script..... 20

B. Appendix – Microsoft Knowledge Base article 270836, *Exchange Server static port mappings* 23

Glossary Error! Bookmark not defined.

Bibliography Error! Bookmark not defined.



***BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)***

List of Tables

Table 1: Outbound Ports 4
Table 2: Firewall Script IPs..... 20

List of Figures

Figure 1: Network Diagram 5

UNCLASSIFIED



Communications Security
Establishment

Centre de la sécurité
des télécommunications



***BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)***

This page intentionally left blank.



***BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)***

List of Abbreviations and Acronyms

ACL	Access Control List
BES	BlackBerry Enterprise Server
CSE	Communication Security Establishment
DMZ	Demilitarized Zone
GoC	Government of Canada
IP	Internet Protocol, also used as short form for IP address
MAPI	Messaging Application Programming Interface
NAT	Network Address Translation
PAT	Port Address Translation
PC	Personal Computer
RIM	Research In Motion, makers of the BlackBerry Handheld Device
TCP	Transmission Control Protocol
TCP/IP	TCP over IP
UDP	User Datagram Protocol

UNCLASSIFIED



Communications Security
Establishment

Centre de la sécurité
des télécommunications



***BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)***

This page intentionally left blank.



BlackBerry Enterprise Server Isolation in a Microsoft Exchange Environment (ITSG-23)

1 Introduction

Many government departments rely on Research in Motion's (RIM) BlackBerry Handheld devices and a BlackBerry Enterprise Server (BES) service for wireless communication. However, as with any service, opening ports to the Internet may create security risks.

When a BES service starts, it creates an authenticated TCP session with the RIM Relay over port 3101. All traffic between the BES and a handheld flows over this link and is encrypted during transit. However, since this traffic is encrypted, it is impossible to inspect the packets that flow back and forth between the BES and the handhelds. Therefore, there is a potential security risk in any network that runs a BES since incoming packets cannot be inspected. If the BES can be compromised, then potentially the entire network can be compromised.

At first glance, an easy solution to this is to place the BES in a network Demilitarized Zone (DMZ) and filter traffic to the internal network. Unfortunately, the setup for this is not as simple as it might seem. The BES must also connect to Microsoft Exchange servers which use a Messaging Application Programming Interface (MAPI) connection to send and receive email messages. When the Microsoft Exchange service starts, the MAPI ports are chosen at random. When a client such as the BES initiates a connection, the MAPI ports are communicated through the EndPointMapper which is static on port 135. Having random ports makes it very difficult to put a firewall in-stream of a MAPI connection as it is impossible to know ahead of time which port will be chosen.

1.1 Purpose

This guidance document details how to overcome the problem of random MAPI ports, and how to isolate a BES in its own filtered subnet.

1.2 Scope

This document deals with placing a firewall between a BES and a Microsoft Exchange server. It does not explain how to setup either the MS Exchange server or the BES, or how to administer them. Since the changes are only made to the Exchange server, this should work with all versions of the BES software, past and future. However, only BES version 4.1.0 was tested. This document also does not deal with connectivity to the clients or to the Internet in general.



***BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)***

1.3 Stakeholders

- CSE
- GC Departments

1.4 Assumptions

This guidance document assumes the existence of a working corporate BlackBerry network, including one or more Microsoft Exchange servers and a properly configured BES. A basic knowledge of the TCP/IP protocol suite, Windows administration and Cisco firewall administration is also assumed.



BlackBerry Enterprise Server Isolation in a Microsoft Exchange Environment (ITSG-23)

2 System Description

The solution to this problem is to statically map the MAPI ports by modifying the registry of the Microsoft Exchange server(s) and configuring the firewall to allow outgoing connections on these ports.

The general network setup being discussed in this document is shown at the end of this section in Figure 1 on page 5. The servers running on the network include a domain controller, a single Microsoft Exchange server, and since the BES is S/MIME enabled, a directory server which handles the Public Key Infrastructure (PKI) aspects of the network. If S/MIME is not deployed on the network, the ports pertaining to the directory server may remain closed.

The firewall isolates the BES from the rest of the network and only allows traffic on specific ports to leave. The arrows symbolize the direction of flow of network traffic that the firewall allows. The firewall discussed in this document is stateful, so only the outgoing connections are explicitly allowed, but packets corresponding to existing connections are allowed implicitly.

2.1 Advantages

This setup allows the BES to be isolated from the rest of the internal network. This provides greater security because the BES does not have full access to the internal network. Therefore, if the BES is compromised, there is a far smaller risk of the rest of the network also becoming compromised. Only required ports such as DNS, LDAP and Kerberos are allowed back onto the internal network. As another security measure, traffic bound for the internal network such as email can be inspected for malicious packets since once the packets pass through the BES and are bound for the internal network, they are no longer encrypted¹.

2.2 Disadvantages

Since MAPI uses random port assignments, the Microsoft Exchange server(s) (and optionally the domain controller) must undergo registry modifications to statically map the required ports. This requires a restart of the server (some downtime).

In a large network with multiple Microsoft Exchange servers, all servers that host BlackBerry-enabled mail boxes must be modified since the BES connects to each of them. However, this is derived from the documented behaviour of the BES and was not tested. The tests were performed in a network with only one Microsoft Exchange server.

¹ Packets are no longer encrypted by the BES, but if they are encrypted prior to transmission by a third-party application (e.g.: into S/MIME format), they will still be unreadable.

**BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)**

2.3 Ports Needed

This is a quick reference section for all the ports that are required for full communication with the domain and with the RIM Relays. This is further described in Section 3.

2.3.1 Outbound Ports

These ports must be opened for outgoing connections. The Static MAPI port will be unique for each setup.

Table 1: Outbound Ports

Port Number	Protocol Type	Name/Purpose
53	TCP/UDP	DNS
80	TCP	HTTP
88	TCP/UDP	Kerberos
123	UDP	NTP
135	TCP	EndPointMapper
389	TCP/UDP	LDAP
445	TCP	SMB
1026	TCP	Active Directory Logon
<i>variable</i>	TCP	Static MAPI
3101	TCP	RIM Relay

2.3.2 Inbound Ports

Most modern firewalls have stateful inspection. They keep track of outgoing connections and allow traffic that is returning through the firewall. If this is not the case for the firewall being used to create the subnet, then the ports listed in Table 1 above must also be opened for inbound connections.



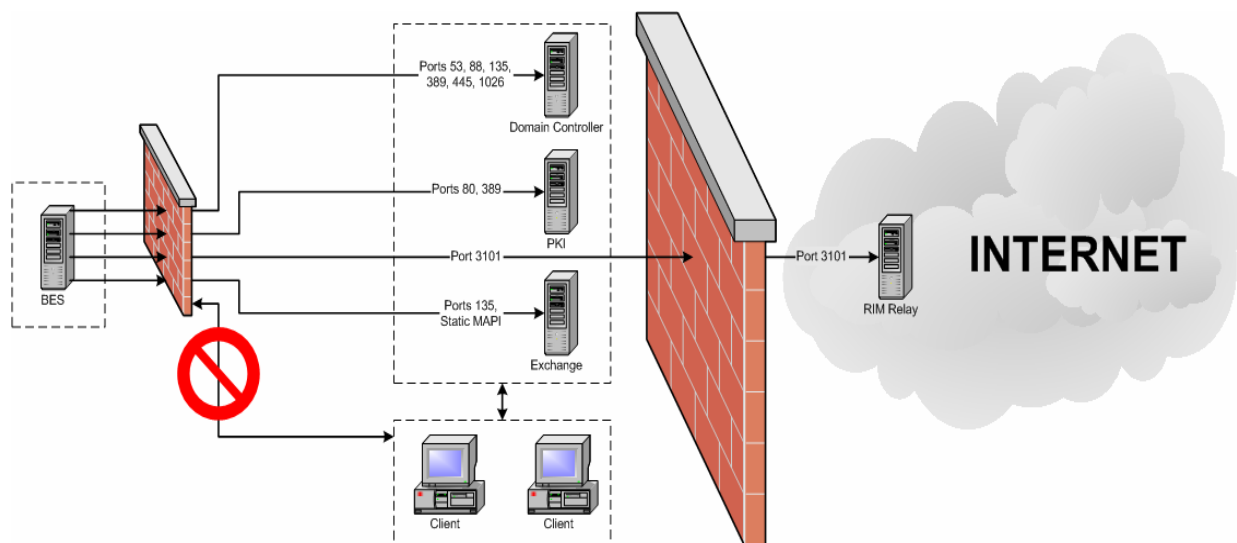
BlackBerry Enterprise Server Isolation in a Microsoft Exchange Environment (ITSG-23)

2.4 Limitations

One limitation found is the inability to use the Microsoft Exchange System Manager from the BES when a firewall is placed between the BES and the Microsoft Exchange server(s). The BES Installation guide suggests that the Microsoft Exchange Administration Tools be installed on the BES prior to installation of the actual BlackBerry Enterprise Server software. However, System Manager (the program used to administer a Microsoft Exchange server) uses different random ports. Static mapping of these ports may not be possible, and thus System Manager cannot be used from behind a firewall.

While this is a limitation, disallowing the System Manager from being installed on the BES is in fact a beneficial and recommended security configuration. This is because if the BES can administer Microsoft Exchange servers, and the BES is compromised, then potentially any Microsoft Exchange server on the network could be compromised as well.

Figure 1: Network Diagram



UNCLASSIFIED



Communications Security
Establishment

Centre de la sécurité
des télécommunications



***BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)***

This page intentionally left blank.



BlackBerry Enterprise Server Isolation in a Microsoft Exchange Environment (ITSG-23)

3 System Configuration

This section describes in detail how to statically map the MAPI ports and configure the firewall for use.

3.1 Configuring static MAPI ports

The instructions in this section are derived from Microsoft's Knowledge Base Article 270836 *Exchange Server static port mappings*, which can be found in Appendix B. Since the article is intended to describe placing a Microsoft Exchange server in a DMZ, some modifications have been made. However, most of the process remains the same.

It is recommended that the port assigned be in the range of 5000-65535. Running the command `netstat -a` on the Microsoft Exchange server will show all current connections. Ensure that the port chosen does not conflict with current port usage.

3.1.1 Procedure for statically mapping MAPI ports

1. Start Registry Editor on the Microsoft Exchange server
2. Locate the following entry for the Exchange IS Interface:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\ParametersSystem
```

3. Add the following entry for the Exchange IS Interface:

Value name: TCP/IP Port

Value type: REG_DWORD

Value data: *Port number to be assigned in decimal format*

4. Restart the Microsoft Exchange server
5. Repeat for each Microsoft Exchange server that hosts BlackBerry-enabled mail boxes.
Note: the port chosen may be identical on each server.

3.2 Configuring Active Directory

The Active Directory logon and directory replication interface is generally assigned to port 1025 or 1026 during startup. This can also be statically mapped so that only one port need be opened.

However, this is an optional step. If the domain controller is not modified, simply open port 1025 as well (see section 3.3.4).



3.2.1 Procedure for mapping Active Directory

1. Start Registry Editor on the domain controller
2. Locate and click to select the following key:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters

3. Add the following registry value:

Value Name: TPC/IP Port
Value Type: REG_DWORD
Base: Decimal
Value: *Port number to be assigned*

4. Restart Domain Controller

It is possible to use either port 1025 or 1026 as the static port.

3.3 Configuring the Firewall

This section describes how to configure a Cisco PIX 515e firewall to use Network Address Translation (NAT) and how to allow outgoing connections on specified ports. Parts of this section may be specific to Cisco PIX firewalls, but can be generalized to work with any firewall.

In this section, “outside” is used to refer to the interface that leads to the rest of the network and the outside world, generally Ethernet 0. Likewise, “inside” is the interface to which the BES is connected. On firewalls that support interface naming, it is recommended to name the interfaces in this fashion to avoid confusion.

3.3.1 Test Network IP Addresses

In this section, many different IP addresses are used. The network used to test the configuration will likely be different than the production network. Therefore, this is a short description of each IP and how to customize them for each network.

The servers in the test network ran in the 192.168.50.0 255.255.255.0 subnet. When the BES was running without a firewall, it was located on this subnet as well. The gateway that connects to the external network was 192.168.50.1, and the domain controller was 192.168.50.2.

Whenever these addresses are seen, they can be replaced with the gateway and domain controller of the network on which this is implemented. For example, later we will see the `route` command. If the gateway on the network is 192.168.1.1, the command would look like this:



BlackBerry Enterprise Server Isolation in a Microsoft Exchange Environment (ITSG-23)

```
route outside 0 0 192.168.1.1 1
```

Only one Microsoft Exchange server was on the network and had an IP of 192.168.50.4. The directory server had the IP addresses 192.168.50.16. The firewall was given an external IP of 192.168.50.32 so that it was on the same subnet as the other servers. An internal IP space of 10.0.0.0 255.255.255.0 is defined with 10.0.0.1 being the IP of the internal interface, and thus the gateway. This means that the BES could be anywhere on the 10.0.0.0 subnet, and it was placed at 10.0.0.2. All the clients in the test network resided on a different subnet. Their routing rules are defined elsewhere and are beyond the scope of this document.

3.3.2 Set the IP Addresses

The IP Addresses of the two interfaces have to be on separate networks. In this guide, the external address of the firewall is 192.168.50.32 with a mask of 255.255.255.0. The internal address is 10.0.0.1, 255.255.255.0. The external address will vary by network, but the internal one does not have to (unless the external network is a 10.x.x.x network).

1. Connect to the firewall's console
2. Type `en` to enter Enable mode
3. Type `conf t` to enter the configure terminal
4. Enter the command `ip address outside 192.168.50.32 255.255.255.0`
5. Repeat step 4 for the inside interface, replacing `outside` with `inside` and modifying the IP accordingly

3.3.3 Configure routing

In order for routing to work, a default route must be added. NAT routes must also be specified including NAT addresses.

From the configure terminal, enter the following commands

1. `route outside 0 0 192.168.50.1 1`
2. `nat (inside) 1 0 0`
3. `global (outside) 1 192.168.50.50-192.168.50.55`

The first command specifies a default route for traffic. All traffic destined for the outside interface will be routed to 192.168.50.1 with a hop cost of 1. Here, "0 0" is short for "0.0.0.0 netmask 0.0.0.0" which matches any and all traffic.



**BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)**

The `nat` command is similar. It allows all traffic on the inside interface access to that particular NAT rule. The “1” is the rule number, so multiple rules can be specified and matched to their corresponding `global` rule.

The `global` rules specify address pools that the corresponding NAT rules may use. In this case, an address pool of five IPs is designated for NAT rule 1.

Using these two commands together, different subnets inside the firewall can be given access to different external IP pools. In this document, only one pool is needed and only simple default routes are specified since only one host is on the internal network.

Note, if only one address is specified in the global rule, then Port Address Translation (PAT) is used. This means that a single IP is used and random port numbers are used to keep track of different connections. Since we did not want to obfuscate the port numbers, an address pool is specified even though only one is used.

3.3.4 Creating the Access List

The access list is what controls which connections are allowed to proceed through the firewall and which are dropped. All the ports listed in Table 1 on page 4 must be opened for outgoing connections to various hosts in order to ensure connectivity.

The general syntax of a firewall rule is

```
access-list <acl name> <permit|deny> <protocol> <source>  
  [options] <destination> [options]
```

There are a few shortcuts that may be used when writing these rules. The keyword “any” can be used to specify any host on the network instead of using 0.0.0.0 0.0.0.0. The keyword “host” can also be used to specify a host on the network by IP instead of using both the IP and netmask. The protocol field can be “tcp”, “udp”, “icmp” or “ip” to refer to any protocol. The options are used here to specify a port number for TCP and UDP connections. Only destination ports are used since source ports are chosen at random and are impossible to determine. A rule such as

```
access-list acl_out permit tcp any host 192.168.50.2 eq 53
```

allows all TCP traffic from any source to the host at 192.168.50.2 on port 53. To specify an entire network, use the syntax

```
access-list acl_out permit tcp 10.0.0.0 255.255.255.0  
192.168.50.0 255.255.255.0 eq 389
```

**BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)**

This rule will allow TCP traffic only from the 10.0.0.x subnet to only the 192.168.50.x subnet on port 389.

If a packet arrives for which there is no rule (rules are inspected one-by-one for a match to the packet in question) the default action is usually to drop it². If this is not the case, simply add the rule

```
access-list acl_out deny ip any any
```

to the end of the rule set. This will drop all packets that do not match a previous rule.

The easiest, but least secure way to configure the firewall is to open each port to the entire server subnet. This will ensure connectivity, but will also allow packets to go to servers that should be off limits.

```
access-list acl_out permit udp any 192.168.50.0 255.255.255.0
eq 53
```

If an intruder were to obtain an IP on the network that this rule inspects (see section 3.3.5) any UDP traffic on port 53 would be allowed into the network, even to hosts that are not running DNS services. This could be used in exploits against the operating system of the target host.

A more secure way is to restrict traffic to only the hosts that are expecting it, or that provide services that are needed.

```
access-list acl_out permit tcp any host 192.168.50.2 eq 389
```

This still leaves the vulnerability of an intruder gaining an IP on the network, but the impact is lessened by restricting the traffic to a single host which can be hardened against attack. Another problem with this style of rule is that the specific IP addresses in the rules must change if the IP of a server is changed (for example the old DNS server is replaced with a new one with a new IP). If the use of names is supported on the firewall, they can be used as a work around for this problem, provided the names remain the same.

The tightest rule possible would be to restrict traffic down to a single source host and a single destination host.

```
access-list acl_out permit tcp host 10.0.0.2 host 192.168.50.2
eq 88
```

However, this has the same problem with changing IP addresses as the previous solution. An intruder could also simply take the BES' IP address in order to gain access to the network.

² While most firewalls drop packets that are not explicitly allowed by default, some firewalls may not. Please consult your firewall documentation for further information



**BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)**

It is up to the reader to decide which rule style is best for each installation. A simple script is included in Appendix A that will configure an access list of the second type for use on the firewall.

3.3.5 Creating the Access Group

Access lists define which packets are allowed to pass, but access groups bind them to specific interfaces. If an access list that only allowed the packet source to be from a 10.0.0.x subnet was placed on an interface with only 192.168.50.x IP addresses, this would effectively block all traffic. When building the access list, one must keep in mind the interface on which it will be used. In the setup for this document, the access list was placed on the inside interface since it is traffic originating from the BES that we are concerned with (note that all connections to internal servers and also the RIM Relays are initiated by the BES).

If no access list is assigned to an interface, usually³ the default is to block all packets that do not match an established connection.

Assigning an access group is a simple one line command

```
access-group <acl name> in interface <interface name>
```

This command binds the access list specified to the incoming traffic on the interface specified. Therefore, the command

```
access-group acl_out in interface inside
```

binds the access list created in the previous section to the inside interface. It will then inspect any traffic incoming to the interface (both on the wire, and internally) according to the access list and decide if the traffic is valid or not.

Since the firewall used in preparation of this document was stateful, any returning packets from established connections are immediately allowed.

3.3.6 Saving the configuration

In case of a power failure, the running configuration is lost and the firewall will be reset to the last saved configuration (initially the factory defaults). To prevent this, the finished configuration must be written to memory by entering the command

³ While this is the norm, some firewalls may not drop all traffic by default. Please consult your firewall documentation for further information

***BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)***

`write memory`

This will save the current configuration to memory. In case of a catastrophic failure, or firewall replacement, the configuration can also be saved to a TFTP server. The command is

```
write net 192.168.50.2:config.txt
```

This writes the current configuration to the TFTP server running at 192.168.50.2 with the filename “config.txt” which will be saved at the root folder of the TFTP server.

To restore a configuration from a TFTP server (restoration is automatic from internal memory), ensure that the previously saved configuration is in the TFTP root folder (or put it in a folder that you know) and use the command

```
configure net 192.168.50.2:config.txt
```

This has the same form as the write command, but uses “configure” instead.

UNCLASSIFIED



Communications Security
Establishment

Centre de la sécurité
des télécommunications



***BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)***

This page intentionally left blank.



***BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)***

4 Conclusions and Recommendations

The firewall script in Appendix A has been tested with BES version 4.1.0 and a single Microsoft Exchange Server 2003 SP2 (V6.5 Build 4638.2). Since no modifications have to be made to the BES itself, the procedure outlined in this document should work with any version of the BES software that is MAPI compliant. Additionally, any standard firewall should be able to map the connections needed by the BES.

For security reasons, it is recommended that the Microsoft Exchange server(s) be patched regularly with the latest security patches. The procedure to statically map the MAPI ports should work with future versions of Microsoft Exchange, provided that the architecture of the software does not change drastically. Therefore, it is recommended that the Microsoft Knowledge Base be consulted for updated articles pertaining to mapping MAPI connections prior to implementing the procedures in this document.

For additional information on isolating the various BES components into separate subnetworks, please see the RIM technical paper *Placement of the BlackBerry Enterprise Solution in a Segmented Network*.

UNCLASSIFIED



Communications Security
Establishment

Centre de la sécurité
des télécommunications



***BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)***

This page intentionally left blank.



***BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)***

5 References

- a. Microsoft Knowledge Base article 270836, *Exchange Server static port mappings*, July 2006. <http://support.microsoft.com/kb/q270836/>
- b. *Placement of the BlackBerry Enterprise Solution in a Segmented Network*, July 2006. http://www.blackberry.com/knowledgecenterpublic/livelink.exe/1265885/Placement_of_the_BlackBerry_Enterprise_Solution_in_a_Segmented_Network?func=doc.Fetch&nodeid=1265885

UNCLASSIFIED



Communications Security
Establishment

Centre de la sécurité
des télécommunications



***BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)***

This page intentionally left blank.



**BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)**

A. Appendix – Firewall Configuration Script

The script below can be used to automatically configure the interfaces of the firewall, define the default routes, create the NAT, define an access list and bind it to an interface. It can be run by pasting it into a telnet client connected to the firewall's configure terminal. The only customization required is to replace all the IP addresses in the script with the ones present in the network. The IP addresses present in the script and what they correspond to are displayed in Table 2 on page 20. Space is provided to write down the new IP addresses. Note that if there is no directory server on the network, or certificate lookup functionality is not desired on the Handhelds, then the ports for the Directory Server may remain closed.

The static MAPI port used in this script is 8194. Change it to the port chosen in step 3 of section 3.1.1. In an environment with multiple Microsoft Exchange servers the line

```
access-list acl_out permit tcp any host 192.168.50.4 eq 8194
```

must be duplicated for each server, replacing 192.168.50.4 with each server IP.

Also note that the two North American RIM Relays are provided in the script. For networks in Europe, Australia or New Zealand, different RIM IP addresses will be needed. Duplicate the

line

```
access-list acl_out permit tcp any host <RIM Relay> eq 3101
```

as many times as needed, replacing <RIM Relay> with one of the Relay IPs.

**BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)****Table 2: Firewall Script IPs**

Script IP	Description	My IP
192.168.50.1	Gateway to Internet	
192.168.50.2 Port 53	DNS Server	
192.168.50.2 Other ports	Domain Controller	
192.168.50.4	MS Exchange Server	
192.168.50.16	Directory Server (PKI)	
192.168.50.32	Firewall External IP	
192.168.50.50 – 192.168.50.55	Firewall External Address Pool	
10.0.0.1	Firewall Internal IP	
204.187.87.33	RIM Relay	
206.51.26.33	RIM Relay	

A.1. Firewall Configuration Script

For each section of the script, follow the instructions laid out above to replace all the IP addresses with custom addresses specific to your network.

The first two lines of the script define the IP addresses of the outside and inside interface. If the interfaces are not named this way (or the firewall does not support naming), these lines will fail. However, the rest of the script will continue. Consult the usage guide on how to configure the IP address of interfaces for your firewall.

The next three define the routing rules and the NAT and global rules. Again, if the interfaces are not (or cannot be) named outside and inside, these rules will fail. Consult the usage guide on how to configure routes and NAT rules for your firewall.

The next line of the script ensures that there is not already an access list named `acl_out`, thus ensures that only the desired rules are entered and no old rules remain.

The next section defines all the firewall rules individually.

**BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)**

The final line binds the newly created access list to the interface “inside”. If a different name has been given to the interface logically on the inside of the firewall, replace the word “inside” with the interface name, or consult the usage guide for your firewall for instructions on how to bind an access list to an interface.

```
ip address outside 192.168.50.32 255.255.255.0
ip address inside 10.0.0.1 255.255.255.0

route outside 0 0 192.168.50.1 1
nat (inside) 1 0 0
global (outside) 1 192.168.50.50-192.168.50.55

no access-list acl_out

access-list acl_out permit udp any host 192.168.50.2 eq 53
access-list acl_out permit tcp any host 192.168.50.2 eq 53
access-list acl_out permit tcp any host 192.168.50.16 eq 80
access-list acl_out permit udp any host 192.168.50.2 eq 88
access-list acl_out permit tcp any host 192.168.50.2 eq 88
access-list acl_out permit udp any host 192.168.50.2 eq 123
access-list acl_out permit tcp any host 192.168.50.2 eq 135
access-list acl_out permit tcp any host 192.168.50.4 eq 135
access-list acl_out permit udp any host 192.168.50.2 eq 389
access-list acl_out permit tcp any host 192.168.50.2 eq 389
access-list acl_out permit tcp any host 192.168.50.16 eq 389
access-list acl_out permit tcp any host 192.168.50.2 eq 445
access-list acl_out permit tcp any host 192.168.50.2 eq 1026
access-list acl_out permit tcp any host 192.168.50.4 eq 8194
access-list acl_out permit tcp any host 204.187.87.33 eq 3101
access-list acl_out permit tcp any host 206.51.26.33 eq 3101

access-group acl_out in interface inside
```

UNCLASSIFIED



Communications Security
Establishment

Centre de la sécurité
des télécommunications



***BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)***

This page intentionally left blank.



***BlackBerry Enterprise Server Isolation in a
Microsoft Exchange Environment (ITSG-23)***

B. Appendix – Microsoft Knowledge Base article 270836, Exchange Server static port mappings

The following Knowledge Base article describes the process of putting a Microsoft Exchange server behind a firewall, not a BES, so it is not to be followed exactly. However, it provides good guidance on statically mapping MAPI ports.

The section of most interest is *Static port mappings for MAPI client computers to connect to Exchange 2000 Server or Exchange Server 2003 through a firewall*. Since the BES is essentially another MAPI client, only the Microsoft Exchange Information Store (MSEExchangeIS) port must be statically mapped. The other ports are used for Exchange synchronization and are not used by the BES.

An up to date version of this Knowledge Base article can be found online at

<http://support.microsoft.com/kb/q270836>