BLACKBERRY ENTERPRISE SERVER (BES) 5.x SUPPLEMENTAL PROCEDURES

Version 2, Release 9

28 October 2016

Developed by DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. BES SECURITY CONSIDERATIONS

1.1 Setting Up an Application White List Software Configuration

An Application White List is a BES feature that controls which applications can be installed on site-managed BlackBerry devices. More specifically, an Application White List is used to specify which applications are required on all BlackBerrys, specific individual BlackBerrys, or groups of BlackBerrys. In addition, an Application White List is used to control allowable actions of approved applications and access to BlackBerry resources (e.g., microphone, browser, key store, other application data, USB port, etc.).

After a software configuration is assigned to a user, it will be automatically deployed to the user's BlackBerry in about 4 hours unless "Deploy Now" is selected. BlackBerry SAs should verify the delivery of the software configuration.

1.1.1 Setting up and applying an Application White List software configuration on BES 5.x

Listed below are procedures for setting up and applying an Application White List software configuration. Application White List software configurations replace the "Disable download of third party applications" IT policy rule to control the download and installation of malware on DoD BlackBerrys. This change allows the use of third party applications like Google Maps. Configuration of Application White List software configurations is a CAT I requirement. **An Application White List software configuration must be set up on the BES even if the use of third party applications is not approved.**

Procedure:

Step 1 - Determine Applications that will be installed.

- Get AO approval for applications that will be installed.
- Set up an application repository (procedure is in the BES Admin Guide) and save all approved applications to the repository.
- Determine what Application Control Policy should be assigned to each approved application: one of the three default Application Control Policies needs to be selected or a custom Application Control Policy needs to be set up. Determine if each approved application will be required or optional.

Step 2 - Set up custom Application Control Policies, if needed.

- BAS >> BlackBerry solution management menu.
- Expand Software.
- Expand Applications.
- Click "Manage applications".
- Search for the application.
- In the "Application versions" section, click on the application.

- Click the appropriate version of the application.
- Click the "Application control policies" tab.
- Click "Edit application".
- On the "Application control policies" tab, in the settings section, select the use custom Application control policies option.
- In the "Required application name" field, type a name for the application.
- In the "Settings" section, configure the settings required for the application control policy.
- Click the "Add" icon.
- Do not set a priority, unless required by site procedures.
- Click "Save all".

Step 3 - Create an Application White List software configuration.

- In the BlackBerry Administration Service, on the BlackBerry solution management menu, expand Software.
- Click Create a software configuration.
- In the Configuration information section, in the Name field, type a name for the software configuration. The name should be descriptive of the group the software configuration is being assigned to and include "Application White List". Example: Command Staff Application White List.
- In the Description field, type in a description. Example: List of approved applications.
- In the Disposition for unlisted applications drop-down list, set "Disposition for unlisted applications" to "Disallowed" and set "Application control policy for unlisted applications" to "Standard Unlisted Disallowed".
- Click "Save".

Step 4 - Add applications to the Application White List software configuration.

- In the BlackBerry Administration Service, on the BlackBerry solution management menu, expand Software.
- Click Manage software configurations.
- Select an Application White List software configuration.
- Click the "Applications" tab.
- Click Edit software configuration.
- Click the "Applications" tab.
- On the Applications tab, click Add applications to software configuration.
- Search for the BlackBerry Java Applications saved in the application repository.
- In the search results, select an application.
- In the Disposition drop-down list for the BlackBerry Java Application, select either "Required", "Optional", or "Disallowed".

  - To install the BlackBerry Java Application automatically on BlackBerry devices, and to prevent users from removing the application, click "Required".
  - To permit users to install and remove the BlackBerry Java Application, click "Optional".

  - To prevent users from installing a BlackBerry Java Application on BlackBerry devices, click "Disallowed".

- In the Application data section, in the Application control policy drop-down list, click a standard Application Control policy to apply to the application if a custom policy is not being used. Select a pre-configured custom Application control policy if desired and not previously assigned to the application.
- Select the deployment method for the software configuration:
  - To install the application on BlackBerry devices over the wireless network, click "Wireless".
  - To install the application on BlackBerry devices using a USB connection to the user's computer and the BlackBerry Web Desktop Manager, click "Wired".
- Click Add to software configuration.
- Click "Save all".

Step 5 - Assign the Application White List software configuration to user accounts.

- In the BlackBerry Administration Service, on the BlackBerry solution management menu, expand User.
- Click "Manage users".
- Search for user account.
- In the search results, click the user account display name.
- Click the "Software configuration" tab.
- Click Edit user.
- In the Available software configurations list, click the Application White List software configuration.
- Click "Add".
- Click "Save all".

1.2 Forcing BlackBerry Device Software Updates

A critical component of a DoD BlackBerry system security posture is ensuring all BlackBerry devices have up-to-date software and application loads on the handheld devices. Therefore, BlackBerry SAs will include rules in each IT policy that users are assigned to accept forced upgrades to site-managed BlackBerry devices.

The following IT policy applies to software updates on BlackBerry devices.

- Desktop Only policy group:
  - Force Load Count
  - Force Load Message

1.3 Firewall Requirements

1.3.1 BES Architecture

DoD security policy requires isolation of the BES host server from the site's Internal Local Area Network (LAN) (also referred to as the Internal Enclave LAN) by installing a host-based firewall on the BES host server or installing a firewall between the BES and the Internal Enclave LAN. The BES and Exchange Servers must be placed on the same segment of the Internal Enclave LAN to facilitate communications. The BES also needs to communicate with other resources (e.g., email, LDAP and OSCP servers, authorized back-office web servers, Simple Object Access Protocol (SOAP) web services, and Java 2 Micro Edition (J2ME) applications), which may be located in various segments or security domains within the site's architecture. The following subsection describes the configuration requirements of the host-based firewall located on the BES.

Note: It is the responsibility of each site's IAO to ensure required ports have been registered via the DoD Ports, Protocols, and Services Management (PPSM) process.

1.3.2 BlackBerry Host-Based Firewall Non-Segmented Architecture

In this architecture, all systems used to host BlackBerry services (e.g., email server and LDAP server) are protected behind an Internal Enclave firewall, and added protection is achieved by use of a host-based firewall installed on the BES. The BES is located directly on the Internal Enclave LAN on the same network segment as the Exchange Server.

The Local Gateway Firewall (depicted in Figure 2-1) is an Internal Enclave firewall which creates a separate security domain for the site's Internal Enclave LAN. Specific firewall rules implemented on the BES host-based firewall will vary based on the BES services used. The server will need to communicate with the LDAP server, OSCP, BlackBerry SRP, Exchange Server, Microsoft Structured Query Language (SQL) Server, and any other authorized resources (e.g., back-office application and content servers) not installed directly on the BES. Careful testing prior to BES deployment will be needed to ensure proper operation while remaining compliant with DoD ports, protocols, and services (PPS) policies.

In accordance with DoD policy, the administrator must configure the host-based firewall policy to deny unneeded incoming and outgoing ports and services by default. In addition, connections to internal network back-office application and content servers should be blocked except for connections to authorized servers by implementing a list of trusted IP addresses. Furthermore, firewall-filtering rules must be documented, security alerts must be monitored, and a firewall audit log must be maintained. The firewall used for this functionality must be robust and have the capability to block both incoming and outgoing traffic.

In general, the host-based firewall rules must be configured to implement the following policies.

- Internal traffic from the BES is limited to internal systems used to host the BlackBerry services (e.g., email, LDAP servers, and authorized back-office application and content servers). Communications with other services, clients, and/or servers are not authorized.

- Internet traffic from the BES is limited to only specified BlackBerry services (e.g., BlackBerry SRP server, OCSP, SSL/TLS, HTTP, and LDAP). All outbound connections are initiated by the BlackBerry system and/or service.

Table 1-1 lists the default or standard ports for the needed services used for BES and BlackBerry device communications in a segmented network. Although it is possible to configure Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) to use non-standard or unregistered ports for these communications, this is not recommended since it will cause unexpected results at various internal or external boundaries in the DoD enclave.

Note: Table 1-1 is intended as a starting point and is provided by request of field sites and reviewers to facilitate firewall configuration. Use additional references from BlackBerry, Microsoft, and DISA STIGs to tailor the firewall rule configuration to the site's specific architecture.

Table 1-1: Host-Based Firewall Architecture PPS for Non-Segmented Architecture on BES

Service	Protocol	Default Port	Comments
Outgoing data connections, using SRP, to BlackBerry Infrastructure.	TCP	3101	Both the Local Gateway Firewall and the Enclave Perimeter firewall outbound rules must be configured to allow this port outbound to Internet via NIPRNet. (Must traverse PPS Category Assignment List (CAL) boundaries 12, 10, 6, 4, and 2 when configured in compliance with the requirements of this checklist.)
Incoming and outgoing connections from the Desktop Manager utility installed on a PC with the handheld device attached. Used to sync the BlackBerry to the BES.	TCP	4101	Incoming and outgoing connections on the Internal Enclave (Intranet) to/from the BES (i.e., not outgoing to the Internet).
Incoming and outgoing connection to the Microsoft SQL server for BlackBerry Configuration Database.	TCP	1433	Needed only if SQL server is on a separate server from BES.

Service	Protocol	Default Port	Comments
Outgoing connections to the Enclave web proxy server.	HTTP, HTTPS	8080, 8443	For BlackBerry browser connections to the Internet if permitted by local policy. Some sites have opted to place all application and web proxy services into an Internal Enclave De-militarized Zone (DMZ) network. If the AO has approved access to these applications, then the Firewall Administrator will update all appropriate firewall rules to allow the BES access. List IP address of the web proxy server in the host-based BES firewall list of trusted IP addresses and subnets.
Outgoing connections to Enclave application and content servers (e.g., J2ME servers, SOAP web services, and web content servers).	HTTP, HTTPS	8080, 8443	For approved/authorized connections to Internal Enclave application servers. If the AO has approved access to these applications, then the Firewall Administrator (FA) will update all appropriate host-based BES firewall rules to allow BES access, including listing IP address of the servers in the firewall list of trusted IP addresses and subnets.
Outgoing connection to trusted OCSP.	HTTP	80	To obtain PKI certificate information.
Connections between BES and BlackBerry Messaging Agent: - Incoming data connections to the BlackBerry Dispatcher. - Incoming system log connections to the BlackBerry Controller.	TCP UDP	5096 4070	
Outgoing system log connections from the BlackBerry MDS Connection Service to the Simple Network Management Protocol (SNMP) agent.	UDP	4071	
Outgoing LDAP connection	LDAP	389	

Service	Protocol	Default Port	Comments
For connections between the BES and the Enclave Microsoft Exchange Server			
Remote Procedure Call (RPC) endpoint mapper	TCP	135	
Microsoft Exchange System Attendant service	TCP	135	
Name Service Provider Interface (NSPI)	TCP	135	
Microsoft Exchange Information Store	TCP	135	

1.3.3 Segmented Architecture

In the segmented network architecture (see Figure 2-2), the BES Router is installed in a DMZ of the enclave border firewall. A host-based firewall must be installed on the servers with the BES router and on the BES and configured as described in the Desktop Application STIG.

When the segmented network architecture is used, the host-based firewall on the BES router and the DMZ must be configured as shown in Table 1-2.

Table 1-2: Host-Based Firewall Architecture PPS for Segmented Architecture on BES Router

Service	Protocol	Default Port	Comments
Incoming from the BES locked on the enclave. Outgoing data connections, using SRP, to BlackBerry Infrastructure.	TCP	3101	Both the Local Gateway Firewall and the Enclave Perimeter firewall outbound rules must be configured to allow this port outbound to Internet via NIPRNet (DoD Network) and inbound from the enclave. (Must traverse PPS CAL boundaries 12, 10, 6, 4, and 2 when configured in compliance with the requirements of this checklist.)
Incoming and outgoing connections from the Desktop Manager utility installed on a PC with the handheld device attached. Used to sync the BlackBerry to the BES.	TCP	4101	Incoming and outgoing connections on the Internal Enclave (Intranet) to/from the BES (i.e., not outgoing to the Internet).

Service	Protocol	Default Port	Comments
Outgoing system log connections from the BlackBerry MDS Connection Service to the SNMP agent.	UDP	4071	

When the segmented architecture is used, the host-based firewall on BES should be configured as shown in Table 1-3.

Table 1-3: Host-Based Firewall Architecture PPS for Segmented Architecture on BES

Service	Protocol	Default Port	Comments
Outgoing data connections to the BES router located in the DMZ.	TCP	3101	
Incoming and outgoing connections from the Desktop Manager utility installed on a PC with the handheld device attached. Used to sync the BlackBerry to the BES.	TCP	4101	Incoming and outgoing connections on the Internal Enclave (Intranet) to/from the BES (i.e., not outgoing to the Internet).
Incoming and outgoing connection to the Microsoft SQL server for BlackBerry Configuration Database.	TCP	1433	Needed only if SQL server is on a separate server from BES.
Outgoing connections to the Enclave web proxy server.	HTTP, HTTPS	8080, 8443	For BlackBerry browser connections to the Internet if permitted by local policy. Some sites have opted to place all application and web proxy services into an Internal Enclave DMZ network. If the AO has approved access to these applications, then the SA will update all appropriate firewall rules to allow the BES access. List IP address of the web proxy server in the host-based BES firewall list of trusted IP addresses and subnets.

Service	Protocol	Default Port	Comments
Outgoing connections to Enclave application and content servers (e.g., J2ME servers, SOAP web services, and web content servers).	HTTP, HTTPS	8080, 8443	For approved/authorized connections to Internal Enclave application servers. If the AO has approved access to these applications, then the SA will update all appropriate host-based BES firewall rules to allow the BES access, including listing IP address of the servers in the firewall list of trusted IP addresses and subnets.
Outgoing connection to trusted OCSP.	HTTP	80	To obtain PKI certificate information.
Connections between BES and BlackBerry Messaging Agent: - Incoming data connections to the BlackBerry Dispatcher. - Incoming system log connections to the BlackBerry Controller.	TCP UDP	5096 4070	
Outgoing system log connections from the BlackBerry MDS Connection Service to the SNMP agent.	UDP	4071	
For connections between the BES and the Enclave Microsoft Exchange Server			
RPC endpoint mapper	TCP	135	
Microsoft Exchange System Attendant service	TCP	135	
NSPI	TCP	135	
Microsoft Exchange Information Store	TCP	135	
Outgoing LDAP connection	LDAP	389	

1.4 Antivirus Support on BlackBerry Devices

DoDI 8500.2, Information Assurance (IA) Implementation, February 6, 2003, requires virus protection on mobile computing devices. In DoDI 8500.2, IA control ECVP-1 states: "All servers, workstations and mobile computing devices implement virus protection that includes a capability for automatic updates."

For some IT systems, this requirement is met by using anti-virus applications installed on the computer (e.g., IT systems with the Windows operating system). The BES meets the virus protection requirement of DoDI 8500.2 by a combination of IT policies, application control policies, and code signing to contain malware and control its ability to install itself on the BlackBerry device and gain access to device resources, applications, and data and access the DoD network. This document includes specific BES and BlackBerry device configuration requirements to ensure BlackBerry Enterprise System malware controls are implemented.

BlackBerry virus protection features have been tested by National Security Agency (NSA) and DISA and were approved by the Defense Information System Network (DISN) Security Accreditation Working Group (DSAWG) in 2006 as meeting DoD security requirements when the initial release of this Checklist was approved.

Additional information on BlackBerry malware protections can be found in BlackBerry security documents.

1.5 BES System Administrator Training and Certification

Required annual training for the BES System Administrator is listed in vulnerability WIR1220-01 (Vul ID# V0022054), found in the Blackberry Enterprise Server STIG, Part 1.

Administration and security controls on BES 5.x are more sophisticated than those found on previous versions of the BES. The knowledge and skills needed to properly configure and manage security controls are more complex than previously required. It is recommended that DoD sites verify that site BES 5.x system administrators have been trained or have demonstrated proficiency in the minimum skills needed to administer BES 5 security features (listed below). It is also recommended that sites consider requiring BES system administrators be certified as BlackBerry Certified SAs.

- Set up administrator accounts and assign roles to those accounts.
- Determine appropriate roles for various system administrator functions.
- Set up and manage user and group accounts.
- Set up and manage software configurations and assign those configurations to user and/or group accounts.
- Plan what Application White List software configurations are required to meet organizational needs.
- Determine minimal BlackBerry resource requirements for installed applications.
- Set up and manage default and custom application control policies and assign them to applications.
- Set up and manage a host based firewall (e.g., Host Based Security System (HBSS), McAfee, etc.) and configure firewall port, protocol, and IP access control rules.
- Set up and manage IT policies and assign those policies to user and/or group accounts.
- Determine impact on BES operation and site-managed BlackBerry operations when optional IT policy rules are changed to meet organizational needs.
- Set up application repositories and publish applications to the BES.
- Set up and manage BES proxy authentication.
- Configure BES for trusted connections to servers.
- Set up and manage configuration sets.

- Configure BES Master key.
- Configure allowed email message formats (e.g., block HTML and RTM email).
- Set up and manage Access Control groups and assign them to user and/or group accounts.
- Plan what Access Control groups are required to meet organizational needs.
- Set up Pull URL patterns.
- Configure BAS key store password.
- Configure S/MIME encryption type on BES.
- Configure IT policy resend interval.
- Configure CRL, OCSP, and LDAP properties on BES.
- Configure and manage BlackBerry Web Desktop Manager security features.
- Set up and manage an Enterprise Server Policy to manage lists of authorized BlackBerry devices.

1.6 Setting up and applying an Application White List software configuration on BES 5.x

Listed below are procedures for setting up and applying an Application White List software configuration. Application White List software configurations replace the "Disable download of third party applications" IT policy rule to control the download and installation of malware on DoD BlackBerrys. This change allows the use of third party applications like Google Maps. Configuration of Application White List software configurations is a CAT I requirement. **An Application White List software configuration must be set up on the BES even if the use of third party applications is not approved.**

Procedure:

Step 1 - Determine Applications that will be installed.

- Get AO approval for applications that will be installed.
- Set up an application repository (procedure is in the BES Admin Guide) and save all approved applications to the repository.
- Determine what Application Control Policy should be assigned to each approved application: one of the three default Application Control Policies needs to be selected or a custom Application Control Policy needs to be set up. Determine if each approved application will be required or optional.

Step 2 - Set up custom Application Control Policies, if needed.

- BAS >> BlackBerry solution management menu.
- Expand Software.
- Expand Applications.
- Click "Manage applications".
- Search for the application.
- In the "Application versions" section, click on the application.
- Click the appropriate version of the application.
- Click the Application control policies tab.
- Click Edit application.

- On the "Application control policies" tab, in the settings section, select the use custom Application control policies option.
- In the "Required application name" field, type a name for the application.
- In the "Settings" section, configure the settings required for the application control policy.
- Click the "Add" icon.
- Do not set a priority, unless required by site procedures.
- Click "Save all".

Step 3 - Create an Application White List software configuration.

- In the BlackBerry Administration Service, on the BlackBerry solution management menu, expand Software.
- Click "Create a software configuration".
- In the "Configuration information" section, in the "Name" field, type a name for the software configuration. The name should be descriptive of the group the software configuration is being assigned to and include "Application White List". Example: Command Staff Application White List.
- In the "Description" field, type in a description. Example: List of approved applications.
- In the "Disposition for unlisted applications" drop-down list, set "Disposition for unlisted applications" to "Disallowed" and set "Application control policy for unlisted applications" to "Standard Unlisted Disallowed".
- Click "Save".

Step 4 - Add applications to the Application White List software configuration.

- In the BlackBerry Administration Service, on the "BlackBerry solution management" menu, expand Software.
- Click "Manage software configurations".
- Select an Application White List software configuration.
- Click the "Applications" tab.
- Click "Edit software configuration".
- Click the "Applications" tab.
- On the "Applications" tab, click "Add applications to software configuration".
- Search for the BlackBerry Java Applications saved in the application repository.
- In the search results, select an application.
- In the "Disposition" drop-down list for the BlackBerry Java Application, select either "Required", "Optional", or "Disallowed".

  - To install the BlackBerry Java Application automatically on BlackBerry devices, and to prevent users from removing the application, click "Required".
  - To permit users to install and remove the BlackBerry Java Application, click "Optional".
  - To prevent users from installing a BlackBerry Java Application on BlackBerry devices, click "Disallowed".

- In the "Application data" section in the "Application control policy" drop-down list, click a standard Application Control policy to apply to the application if a custom policy is not being used. Select a pre-configured custom Application control policy if desired and not previously assigned to the application.
- Select the deployment method for the software configuration:

    - To install the application on BlackBerry devices over the wireless network, click "Wireless".
    - To install the application on BlackBerry devices using a USB connection to the user's computer and the BlackBerry Web Desktop Manager, click "Wired".

- Click "Add to software configuration".
- Click "Save all".

Step 5 - Assign the Application White List software configuration to user accounts.

- In the BlackBerry Administration Service, on the BlackBerry solution management menu, expand User.
- Click "Manage users".
- Search for user account.
- In the search results, click the user account display name.
- Click the "Software configuration" tab.
- Click "Edit user".
- In the "Available software configurations" list, click the "Application White List software configuration".
- Click "Add".
- Click "Save all".

2. NETWORK ARCHITECTURE

Figure 2-1: Example BlackBerry Network Architecture

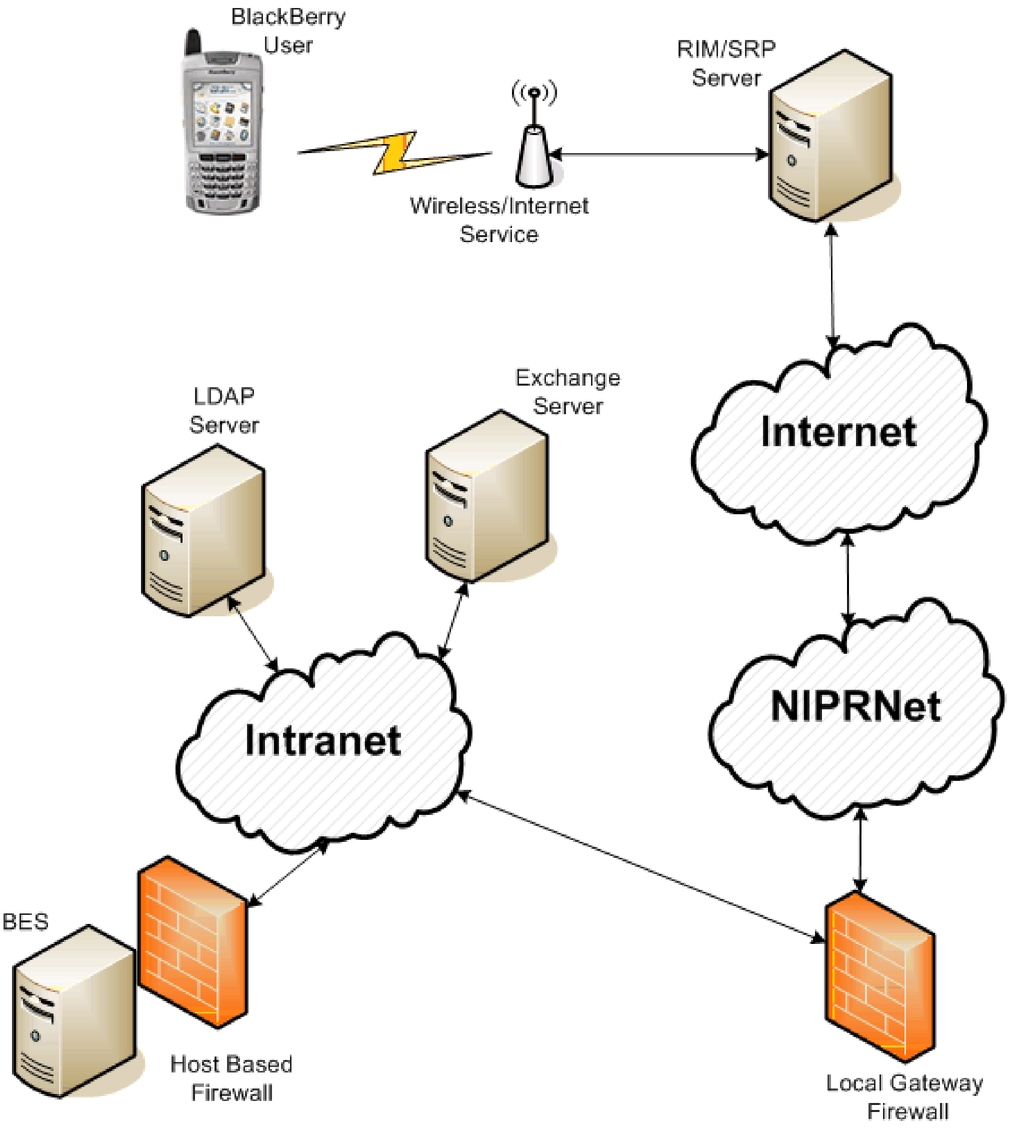
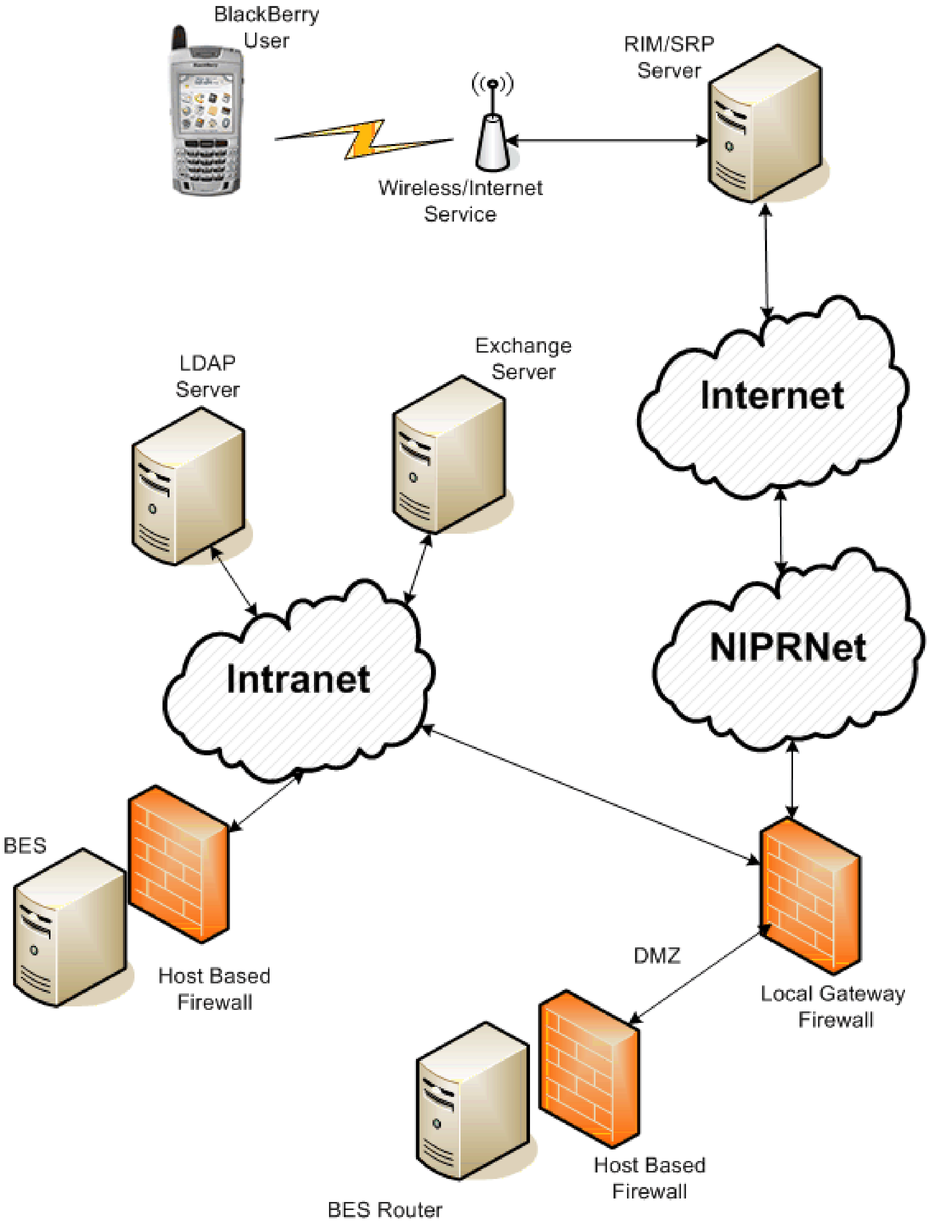


Figure 2-2: Segmented BlackBerry Network Architecture


BlackBerry User
Wireless/Internet Service
RIM/SRP Server
LDAP Server
Exchange Server
Internet
Intranet
NIPRNet
BES
Host Based Firewall
DMZ
Local Gateway Firewall
BES Router
Host Based Firewall