



Antivirus Software on a Cisco BBSM Server

Problem Statement

Companies using Cisco Building Broadband Service Manager (BBSM) may want to protect their Microsoft Windows-based BBSM servers from virus and worm threats by using third-party antivirus software. This white paper describes the technical processes that are required for adding protection to the Cisco BBSM server with third-party antivirus software. This white paper also addresses the steps that you must take to plan and implement third-party antivirus software on the BBSM server.

The formal documentation for implementing and using third-party antivirus software is available through the respective antivirus vendors. Therefore, you should not rely upon this white paper exclusively to fully implement the third-party antivirus software on BBSM.

Note: Because we do not recommend or support the use of personal firewalls on BBSM servers, this white paper does not provide information pertaining to personal firewalls.

Scope

This white paper discusses some of the antivirus software applications that are available on the market today. Since BBSM is a server product, only software products that comply with server installations are discussed here. This white paper does not provide the following information:

- Pricing
- Recommendation of a specific vendor
- Specific product documentation
- Installation details

Antivirus Software Vendors

There are many antivirus software vendors in the market today. Symantec and Network Associates are well established, but many others, such as Trend-Micro, Panda Software, and Kaspersky Labs, also offer viable alternatives for protecting server products from virus and worm threats. Since the BBSM software is installed only on the Windows 2000 server platform, it is important to choose the appropriate antivirus software that is rated for this server and enterprise environment.

Tasks

We recommend that you perform the following tasks:

Obtain and License the Software

Contact your vendor of choice and obtain the correct application and licenses for your BBSM environment.

Read the Vendor's Documentation

Read and follow the vendor's documentation that explains how to install and protect your BBSM server.

Understand Your BBSM Product and Your Security Needs

The BBSM server ships with 256 MB of RAM. Although this amount of memory is sufficient for small environments with the base software loaded, you could exceed this initial allocation by installing additional Cisco-recommended applications, such as antivirus, remote communication, and other monitoring software. Be sure to install enough RAM to run the BBSM server software as well as the antivirus and other Cisco-recommended software applications.

After you load the antivirus software and update the definitions, we recommend that you initiate a full system scan to verify that no viruses or worms are present on the system. Configure full system scans to run once a week. Because these scans are usually very intensive, select times when the server has the least amount of usage. Configure On-Demand scanners to address common executable files and DLLs; however, do not configure everything through On-Demand scanning.

Installing Other Application Software on a BBSM Server

The BBSM server has been tested with only a small number of antivirus, remote monitoring, and remote communication applications. Antivirus software is discussed in this paper. Cisco Security Agent (CSA) is discussed in a different white paper, *How to Plan and Implement the Cisco Security Agent on the BBSM Server*. BBSM supports Windows Terminal Services remote communication software. If you use any other software applications, be sure to test them in a lab environment before using them in a production environment.

A Warning About Email

Do not use the BBSM server for reading email. Most viruses and worms are contracted and spread through email when users open attachments containing a virus or a worm. By limiting or eliminating the use of email on the BBSM server, your exposure to viruses and worms is significantly reduced.

Updating Virus Definitions on the Antivirus Software

Your antivirus solution is only as good as the latest update. Most vendors offer subscriptions to keep your software and definitions updated. Hundreds of new viruses and worms are discovered monthly. Vendors normally release weekly updates to definitions. They might release updates more often, depending on the threat of a particular strain. Subscriptions keep the engine and other related software updated. We recommend that you configure the software to be updated automatically. In case a reboot is required, schedule the updates to occur during nonpeak times.

Testing the BBSM Server with the Antivirus Software

You must test your BBSM product with the antivirus software. If possible, it is best to perform this test in a nonproduction environment. The tests must emulate, as closely as possible, real-world usage scenarios in which the antivirus software is deployed. Testing should include all aspects of client usage such as web browsing, email, file transfers, VPN, and any other possible usage scenarios. While testing, exercise the use of the BBSM management console, both locally and remotely. While these tests are running, be sure to monitor the performance of your server. Pay particular attention to memory usage and CPU utilization.

Perform these tests initially in a lab environment and then slowly scale to a few production sites. If modification to scanning characteristics or additional memory is required, make these adjustments early in the process, and develop a plan for widespread deployment.

Distributing the Antivirus Software to BBSM Servers

After you test the antivirus software, you can distribute the software to your production servers in various ways. You can load the software directly from the distribution CD. The procedures for installing McAfee (Network Associates) and Symantec AntiVirus software are described in this white paper. Most antivirus software suites can be installed on a central administration server. The server then deploys the software and updates to individual servers while consolidating the scan logs and providing alerting capabilities for all remotely monitored servers.

Most antivirus software suites allow for the repackaging of the distribution software and then deployment of the repackaged software (either manually through CD or over the Internet) or the centralized server can deploy the software to specific machines automatically. If you take this approach, thoroughly test the software in a non-production environment, and make sure that the appropriate communication ports are allowed for communications across firewalls.

Testing the Antivirus Products

The following two products have been tested on a BBSM 5.3 server with 256 MB of RAM:

- McAfee VirusScan Suite 7.1.0
- Symantec AntiVirus Corporate Edition

McAfee VirusScan Suite 7.1.0

You can install the McAfee VirusScan Suite directly from the CD. For additional information about this product, refer to the user guide that ships with the software.

Note: Although it was not tested, you can also install the McAfee VirusScan Suite by creating an administration server and loading the McAfee ePolicy Orchestrator environment. Orchestrator enables you to remotely manage deployed VirusScan software from a central location and create customized software to deploy to servers, handle updates and alerts, and perform other administrative tasks.

To install the McAfee software, insert the CD into the CD-ROM drive and follow the installation wizard. After you insert the CD, the VirusScan Security Suite window appears. Choose **VirusScan v7.1.0 for Win NT/2K/XP**, and follow the installation wizard. When the Select Setup Type window appears, choose either the **Typical** or **Custom** radio button. (The Typical setup type was tested.) After the software installs, a window displays the following message: McAfee VirusScan Enterprise setup has completed successfully.

- If you have an Internet connection, verify that the **Update Now** and the **Run On-Demand Scan** check boxes are checked. These options enable you to update your virus definition (DAT) files and scan your local drives by running On-Demand Scan.
- If you do not have an Internet connection, uncheck both of these check boxes. You can choose these options later, after you establish an Internet connection.

After the installation is complete, refer to the McAfee documentation for information about setting up schedules, running On-Demand scans, automatic updates, and other administrative tasks.

Note: On-Access scanning causes minimum performance impacts based on the types of files being accessed. For additional information, refer to the [Performance](#) section on page 4.

Symantec AntiVirus Corporate Edition

You can install the Symantec AntiVirus Corporate Edition directly from the CD. For additional information about this product, refer to the user guide that ships with the software.

Note: Although untested, you can also install the Symantec AntiVirus Corporate Edition by creating a system control center server and deploying the antivirus image from there. The system control center lets you remotely manage deployed Symantec AntiVirus Corporate Edition software from a central location and create customized software to deploy to servers, handle updates and alerts, and perform other administrative tasks.

To install the Symantec software, insert the CD into the CD-ROM drive and follow the installation wizard. After you insert the CD, the Symantec AntiVirus Corporate Edition window appears. Choose **Install Symantec AntiVirus**, and follow the installation wizard.

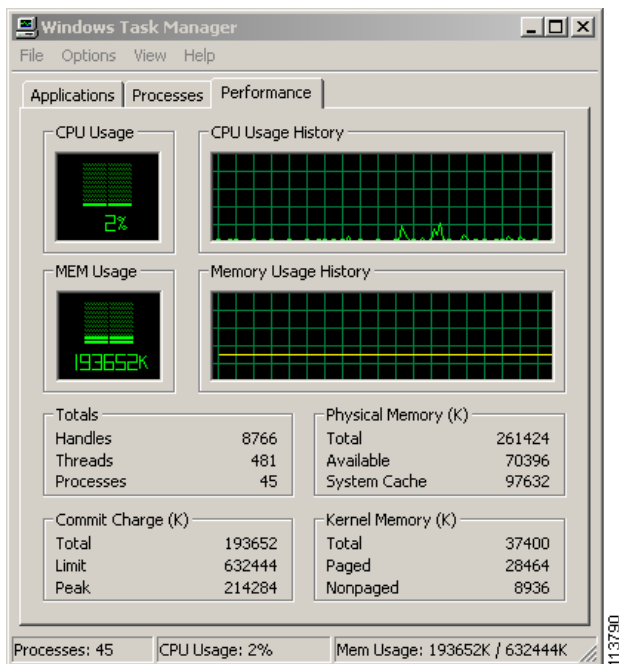
Be careful when choosing the options in the following windows:

- Mail Snap-In Selection—Leave the **Microsoft Exchange/Outlook** and **Lotus Notes** check boxes unchecked. These options do not apply to BBSM.
- Network Setup Type—Click the **Unmanaged** radio button.
- Initial Settings—Check the **File System Realtime Protection** check box.
- Run Options—If you have an Internet connection, verify that the **Run LiveUpdate** check box is checked. If you don't have an Internet connection, uncheck the check box. You can choose this option later, after you establish an Internet connection.

Performance

On-Access (or real time) scanning causes minimum performance impacts based on the types of files being accessed. You might see a high spike in process utilization during the scan of a large file. Otherwise, you normally see minimal spikes during actual scans on the fly. (See Figure 1.)

Figure 1. Example of On-Access Scan Performance

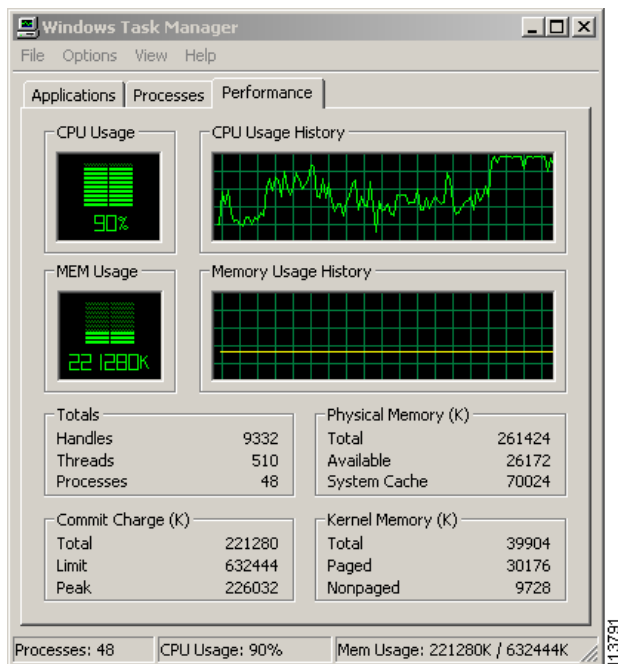


To access the Windows Task Manager, follow these steps:

1. Press **Ctrl + Alt + Delete**. The Windows Security window appears.
2. Click **Task Manager**. The Windows Task Manager window box appears.
3. Click the **Performance** tab.

With On-Demand scanning, every file on the system is accessed during the scan. It is not uncommon to see the processor in the 90% utilization range during the scan. (See Figure 2.) On-Demand scans can take up to 1 hour, depending on the number of files. Run these scans at least once a week during off-peak times to minimize the performance hit users will experience during login.

Figure 2. Example of On-Demand Scan Performance



These tests were run on a BBSM 5.3 server with 256 MB of RAM. We recommend that you install additional RAM to minimize the impact of the antivirus software and other Cisco-recommended applications that you install. Additional RAM increases the overall performance of the BBSM server, especially in high-usage environments.

Final Analysis

Any antivirus solution that is rated for a Windows server installation should work on the BBSM server. Although this white paper discusses the standalone installations for the Symantec and McAfee antivirus software, Cisco Systems does not endorse these products. There are many viable antivirus alternatives; however, it is your responsibility to determine the appropriate product. Antivirus protection is only one component of the overall security strategy. We recommend that you consider other security options, such as firewalls (not the personal software type), Access Control Lists (ACLs), and Intrusion Detection.

The *SAFE Blueprint from Cisco* is a flexible, dynamic blueprint for security and virtual private networks (VPNs). The SAFE blueprint is based on Cisco Architecture for Voice, Video, and Integrated Data (AVVID), which enables businesses to securely and successfully take advantage of electronic business on the Internet. Cisco has significantly enhanced the SAFE blueprint and extended network security and VPN options to small branch offices, teleworkers, and small-to-medium networks.

SAFE White Papers

The following SAFE white papers provide overviews of the extended SAFE blueprint, followed by detailed descriptions of the specific modules that comprise the actual network designs:

- [SAFE: A Security Blueprint for Enterprise Networks](#)
- [SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks](#)
- [SAFE: VPN IPSec Virtual Private Networks in Depth](#)
- [SAFE: Wireless LAN Security in Depth - Version 2](#)
- [SAFE: IP Telephony Security in Depth](#)
- [SAFE: IDS Deployment, Tuning, and Logging in Depth](#)

Note: Not all of the recommendations of SAFE can be implemented on a BBSM network without impacting the overall functionality of the BBSM server.



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0403R)

Copyright © 2004 Cisco Systems, Inc. All rights reserved.

Cisco Systems, Inc.

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Page 6 of 6