Microsoft® Forefront™ Security for Exchange Server

Microsoft® Forefront™ Security for SharePoint®

The Multiple Scan Engine Advantage and Best Practices for Optimal Security and Performance

Microsoft Forefront Security for Exchange Server
Microsoft Forefront Security for SharePoint

Paul Robichaux
3Sharp LLC
Published: December 2006

Abstract

Microsoft® Forefront™ Security for Exchange Server and Microsoft® Forefront™ Security for SharePoint® provide comprehensive protection against viruses and other types of malware. Because these products are so flexible, administrators look to best practices for deploying and configuring them to get the optimal balance of performance and security. This paper discusses the multiple scan engine support of Forefront Security for Exchange Server and Forefront Security for SharePoint and recommends engine configurations for various server sizes and environments.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2006 Microsoft Corporation. All rights reserved.

Microsoft, Forefront, Antigen, SharePoint, Windows, Windows Server System, and the Windows Server System logo are either registered trademarks or trademarks of Microsoft Corporation or Sybari Software, Inc. in the United States and/or other countries. Sybari Software, Inc. is a subsidiary of Microsoft Corporation.

All other trademarks are property of their respective owners.

Contents

Contents.....2

Forefront Security Products for Exchange Server and SharePoint.....3

Forefront Security and Multi-engine Support.....5

Why Use Multiple Engines?.....5

Which Engines Can I Use?.....6

Scanning Messages.....7

Considerations for Forefront Multi-engine Configuration.....8

Security Considerations.....8

Performance Considerations.....8

Engine Configuration for Specific Environments.....11

Additional Protective Layers.....11

Single-Server vs. Multi-Server Environnent.....12

Conclusion.....13

Related Links.....14

Forefront Security Products for Exchange Server and SharePoint

To address customer demand for well-integrated communications and collaboration systems, Microsoft has been steadily building a complete communications and collaboration platform. Microsoft's strategy in this space is to build a set of unified communications and collaboration solutions that provide easy access to a wide range of work modes—instant messaging, e-mail, calendaring, team workspaces, document libraries—all using a familiar set of tools that let people work without disruption from the desktop, or on the go. These solutions are based on, and take advantage of, infrastructure services like Active Directory and Windows Rights Management Services.

For these services and capabilities to be truly useful in business, they must be properly secured. Each Microsoft messaging and collaboration product includes built-in security features, including encryption, authentication, and auditing. Additional solution-specific security features, such as enhanced server-to-server encryption in Microsoft Exchange Server 2007 and built-in support for Windows Rights Management Services in Microsoft SharePoint Server 2007, are examples of these enhanced security capabilities. However, properly securing a communications and collaboration system depends on protecting the system itself *and* the data it contains. Microsoft Forefront products are designed to complement these capabilities and provide comprehensive protection that integrates with your IT infrastructure and simplifies deployment and management of security.

The recently announced Microsoft® Forefront™ Security for Exchange Server and Microsoft® Forefront™ Security for SharePoint® are an important part of the Microsoft Forefront™ product line, providing advanced security and management services for messaging and collaboration servers. These products represent the next versions of the proven and mature Microsoft Antigen line of antivirus products that Microsoft acquired with the purchase of Sybari in 2005.

Forefront Security for Exchange Server and Forefront Security for SharePoint help provide advanced protection for the valuable data transmitted and stored in mailboxes, document libraries, and team sites. They integrate with Exchange Server 2007 and SharePoint Server 2007 to help optimize effectiveness and performance, and are designed to be easy to deploy and manage.

Microsoft focused their efforts on these Forefront server security products in three primary areas:

- **Comprehensive protection:** Both products include multiple scan engines from industry-leading security firms. These engines work together in a single solution to provide greater protection, faster detection of new threats, reduced exposure to threats, and less likelihood of a single point of failure than single-engine solutions.

- **Optimized performance**: These two server security products take full advantage of the antivirus APIs included in Exchange 2007 and SharePoint Server 2007. They provide a powerful multi-engine manager for automating engine updates and usage, multi-threaded and in-memory scanning for faster processing, and performance controls for balancing the desired levels of server performance and security. Combined, these features help protect messaging and collaboration systems while maintaining server uptime and optimizing server performance.

- **Simplified management**: With an intuitive user interface, compatibility with Microsoft® Forefront™ Server Security Management Console, and features for automating engine updates, scan jobs, and reporting, these two Forefront server security products allow administrators to easily manage and deploy protection services across all their servers.

Because these Forefront server security products include support for multiple scan engines, many administrators have questions about why multiple scan engines are important, which scan engines they should use in which combinations and what effect the number of concurrent engines has upon system performance. This paper addresses the most commonly asked questions by describing scenarios that are best suited to particular engine combinations and configurations, and by highlighting IT environment considerations that may impose specific requirements.

Forefront Security and Multi-engine Support

Forefront Security for Exchange Server and Forefront Security for SharePoint support the use of more than one scanning engine at a time. This support is coordinated through the Forefront Security Multiple Engine Manager (MEM), which provides administrators with tools for monitoring the status of installed engines, controlling which engines run, and adjusting the actions taken when an engine needs to be updated or fails during operation.

Why Use Multiple Engines?

The concept of using multiple engines to scan the same set of messages or files for malware might seem odd; after all, if the scan engine is doing its job, you might think that there's no need to scan the same items more than once. However, there are good reasons to use multiple engines in parallel and the ability to run multiple scan engines has long been one of the most popular features of the Antigen product line, now branded as Forefront Security for Exchange Server and Forefront Security for SharePoint.

The primary reason for using multiple engines is that they can help catch more viruses, and do it faster than a single scan engine. A recent set of tests performed by the independent AV-Test.org group found some notable differences in signature update times from various leading anti-virus software vendors. Anti-virus response times were tested for 82 "in the wild" viruses and variants that appeared from April to July 2006. Twenty-six of the viruses were quickly detected by all the scan engines. Of the remaining 56 viruses in the test, some engines didn't protect against viruses for more than 24 hours. In a few cases (notably 0506 Banwarum.C@mm), some vendors didn't update their signatures to provide a block until nearly 5 days had elapsed! Because Forefront Security for Exchange Server and Forefront Security for SharePoint combine multiple engines, the odds that a virus will go unblocked or undetected for long periods are greatly reduced. You benefit from all updates for the set of engines you use, not just from updates to a single engine.

Multiple engines also provide a practical way to implement the security principle of defense in depth. The Forefront Multiple Engine Manager helps ensure that each engine is regularly updated, and that when an engine is being updated, other engines continue to process messages and files.

The additional protection offered by Forefront Security for Exchange Server and Forefront Security for SharePoint multiple engines greatly offsets the minimal impact to server performance. In benchmark tests performed by 3Sharp in October 2006, the results showed that increasing the number of Forefront Security for Exchange Server and Forefront Security for SharePoint scan engines assigned to a transport scan job added a mere 1 – 4% to CPU loads—meaning that using a 5-engine scan can add as little as 4% to the transport server's CPU usage (figure 1).

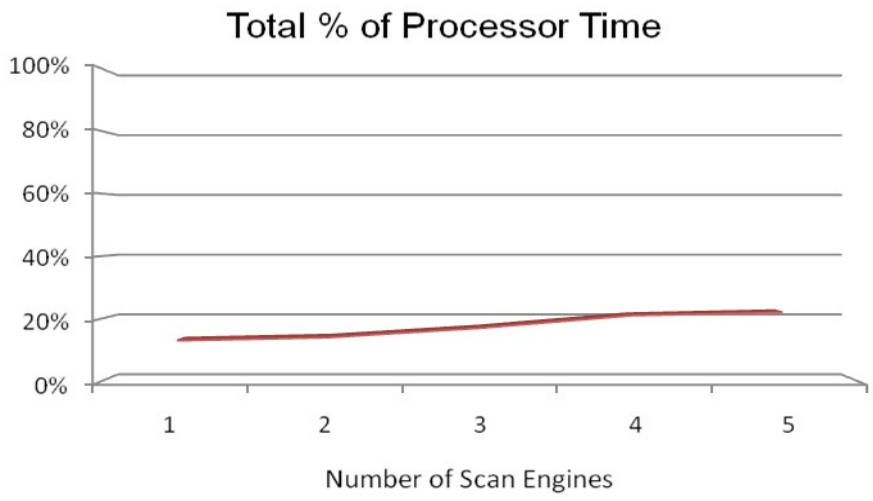

Figure 1 – Forefront Security for Exchange Server / Forefront Security for SharePoint Performance Benchmark Testing

Which Engines Can I Use?

Forefront Security for Exchange Server and Forefront Security for SharePoint each ship with multiple scan engines, and customers can use up to five scanning engines simultaneously. Customers can select from the following scan engines:

- Authentium Command Antivirus engine
- AhnLab engine
- CA Vet
- Kaspersky Labs engine
- Norman Data Defense engine
- Microsoft Antimalware engine, based on technology Microsoft acquired when it purchased GeCAD in 2004
- Sophos Virus Detection engine
- VirusBuster AntiVirus engine

During installation, Forefront Security for Exchange Server and Forefront Security for SharePoint randomly chooses a set of four engines, plus the Microsoft Antimalware engine. You can use this default combination or configure a different set.

Forefront automatically retrieves and installs signature and engine updates for all activated engines. The default schedule checks each engine for updates once per hour, with each engine's start time incremented five minutes from the previous engine's start time. However, you can choose a different schedule update frequency if desired.

Scanning Messages

The Forefront MEM system monitors the performance of each active engine, scoring how well it has performed in the past at identifying new threats and how current its virus definitions are. These scores (or *MEM ratings*) and the administrator-specified bias (performance control) settings are used to determine which engines to use more often. There are five control settings:

- Maximum Performance: For environments where scanning performance is critical, this setting instructs Forefront Security for Exchange Server and Forefront Security for SharePoint to scan each item with only one of the selected engines. The products automatically choose the engine that, based on MEM ratings, appears most likely to catch an incoming threat.
- Favor Performance: Depending on server CPU load, the products adjust the number of scan engines used to scan incoming items. The MEM chooses which engines to use from the set you define according to the engines' MEM ratings.
- Neutral: Each item is scanned by approximately half of the selected engines. Depending on message arrival rates and server resource usage, more engines may be used.
- Favor Certainty: Each item is scanned with all *available* engines; if an engine is offline, it won't be included.
- Maximum Certainty: To get the best possible protection, this setting specifies that each item is to be scanned by *all selected* engines. If one of the engines is offline (for example, getting updated), messages or files will not be processed until that engine has come back online.

To simplify administration, Forefront Security for Exchange Server and Forefront Security for SharePoint enable you to create templates that specify what biases and engines you want applied for a particular type of usage. For example, you could define one template that specifies Neutral bias for transport scanning on Exchange 2007 Hub Transport servers, and a second template that specifies Maximum Certainty bias for scheduled background scans of mailbox servers. Using templates makes it simpler to apply and maintain standardized settings for each type of usage throughout your organization.

Considerations for Forefront Multi-engine Configuration

Two primary considerations influence which scan engine configuration will work best for your environment: your desired level of security and your desired degree of server performance. Forefront Security for Exchange Server and Forefront Security for SharePoint provide significant flexibility to customize the configuration based on which consideration is most important for your particular situation.

Security Considerations

Malware is becoming more and more sophisticated, with attackers increasingly turning to day-zero vulnerabilities in desktop applications as a preferred means of attack. This, and other factors, have elevated the importance of message and content scanning for malware threats.

The primary consideration when planning a Forefront server security product deployment is this: How much protection do you need for the particular situation? Factors to consider when deciding this for your environment include:

- Whether you're already using a perimeter or edge filtering service or appliance. For example, Microsoft's Exchange Hosted Filtering service uses engines from Kaspersky, Sophos, Symantec, and Trend. If you're using this service, you might choose other scan engines for use with Forefront Security for Exchange Server on your Edge or Hub Transport servers to provide additional depth of coverage.
- What your attachment-filtering policies are. Some organizations aggressively block attachments, while others are more permissive. The more attachment types you allow into your organization, the more important malware scanning is at both the network perimeter and on the Store (Mailbox/Public Folder) servers.
- What industry you're in. Specific malware attacks often target industries or companies that rely heavily on information work and valuable intellectual property. In addition, schools, government offices, and other politically sensitive organizations may face a heightened threat.
- How you want to balance server performance (discussed in the next section) with security requirements. Because you can apply different bias settings to different job types and servers, you get fine-grained control over how you manage this tradeoff for each particular use.

The default configuration for these two Forefront server security products (five engines with Neutral bias) provides a good balance of security and performance, and is applicable to many situations. From there, you can adjust the level of security to match your specific needs.

Performance Considerations

One very common question about deploying Forefront Security for Exchange Server or Forefront Security for SharePoint is about what kind of impact using multiple engines has on overall server performance. The exact impact of a given scanning configuration will vary according to several factors. The most important overall factor is how your servers perform under their current workloads. This is critical to understand before deciding how to configure either product. A mailbox, SharePoint, or transport server that's already close to its performance limits won't give you good performance when you add the extra work of scanning content for malware and policy violations. Before you deploy Forefront Security for Exchange Server or Forefront Security for SharePoint, you should understand

the baseline performance of the servers you want to protect, both in normal operation and during peak activity.

Beyond that general rule, there are some more specific principles to be aware of.

First, the performance impact of using multiple engines may be less than you expect. 3Sharp recently performed a series of benchmark tests using pre-release builds of Exchange Server 2007 and Forefront Security for Exchange Server. We tested various combinations of Forefront scan engines to measure the performance impact of adding engines to transport scans. In our tests, we found that moving from one to two engines added about 1% of CPU usage; adding a third engine added about 3%, while adding a fourth increased CPU load on average by about 4%. However, moving to five engines added, on average, less than 1%.

Second, bear in mind that Forefront product performance will always be tied to the level of activity on the server. For example, a Forefront Security for SharePoint installation that's configured to scan newly checked-in documents will have more work to do as more files are checked in. Spikes in activity may result in temporary slowdowns in message or file processing and delivery.

Next, you should consider the question of what control settings are applied. The Favor Certainty and Maximum Certainty selections apply more engines, on average, than Favor Performance and Maximum Performance, so naturally they will require more server resources to run. However, using one of the Certainty settings adds a good deal of additional security, so many administrators choose to do so.

For scans run on the Edge Transport or Hub Transport servers (*transport scanning*), message arrival rate is an important factor. Forefront Security for Exchange Server and Forefront Security for SharePoint let you set up multiple scanning threads to efficiently process messages by allowing multiple engines to run multiple iterations against a queue of messages. For example, if you've selected four engines, a Maximum Certainty bias, and four scanning threads, and ten messages are waiting to be scanned, thread 1 will scan message 1 with all engines; at the same time, thread 2 will scan message 2 with all engines; thread 3 will scan message 3 with all engines, and thread 4 will scan message 4 with all engines. As soon as a scan finishes, it moves on to scan another message that has not yet been scanned. The Multiple Engine Manager coordinates all this scanning activity to ensure that every message is scanned by configured engines, in accordance with the selected control settings, before it's released for delivery.

Every time a message is scanned (either while in transit or after being delivered to a mailbox), it is stamped with a property indicating that it was previously scanned. This eliminates duplicate scanning; for example, a message that is scanned after arrival on an Edge Transport server won't be rescanned by the same engines on a Hub Transport server.

For Store (Mailbox/Public Folder) server scans, the Exchange virus scanning API (VSAPI) supports two types of scans. Messages can be scanned when they're opened (*on-access scanning*), or the scanner can check messages in mailboxes and public folders as a background task (*background scanning*). Exchange always uses on-access scanning on messages that are not tagged as having been scanned; this helps ensure that a message will be scanned at least once before a user opens it. Background scanning runs on a schedule you specify; as messages are scanned, they're flagged to indicate the time and circumstances of the scan.

There are several options you can set to control how background scans use your server resources; these options apply to both Forefront Security for Exchange and Forefront Security for SharePoint:

- You can optionally configure on-access scanning to rescan previously scanned messages or files if the signature or engine used to scan an item in the past has been updated since the scan took place. This adds overhead to user requests to open messages or files, but it helps ensure that all items are fully scanned before users open them.
- By default, the background scanning task scans items that have arrived in the last two days, but you can lengthen or shorten the scan depth to match your requirements.
- Background scans run in the background, and you can schedule when they start to let them run during non-peak periods.

Engine Configuration for Specific Environments

Microsoft's recommendation for engine configurations are simple: choose the setting that best fits your security requirements and your server performance needs. The Neutral setting, which is on by default, is a sound choice that balances a high degree of protection with moderate resource usage. However, you still have to choose which engines you use, and you may want to consider using different settings and engine sets at various places in your environment. There are two primary environmental issues to consider when planning a set of engines and a bias configuration:

- Which existing protective layers you have in place, like hosted e-mail filtering or desktop antivirus scanners
- How many Exchange or SharePoint servers you have, and what roles they play

In general, when you consider these factors, your goal should be to use discrete sets of engines whenever possible. There isn't much benefit from scanning the same messages or files more than once with the same engine; instead, you want to maximize protection by covering each message or file with distinct engines whenever possible.

Additional Protective Layers

The traditional idealized anti-malware protective model involves three layers: perimeter or ingress scanning that checks content as it enters and leaves the network; server-based scanning that checks content as it's submitted to a server for permanent storage; and desktop-based scanning that checks items as they are retrieved or accessed on individual users' computers. Not every organization has all three layers, or deploys unique engines across all three layers. The type of protection you have will affect how you deploy Forefront Security for Exchange Server and Forefront Security for SharePoint.

If you're already using perimeter filtering, familiarize yourself with the anti-malware filters it uses. In general, you'll want to maximize your use of those filters because they intercept messages before they cross over to your servers, saving you bandwidth and server resources. You'll still want to use the filtering of Forefront Security for Exchange Server on your Edge or Hub Transport servers to check outbound messages and messages submitted by internal clients, as well as to provide additional security for inbound messages from the Internet. Because Forefront Security for Exchange Server stamps messages as it scans them, you can enable scanning on your Edge and Hub Transport servers to give you layered protection: scanning at the Edge server will exempt scanned messages from being re-scanned at the Hub Transport server, but the Hub Transport server can still scan messages sent between servers in the organization, or sent to external users.

If you aren't using perimeter filtering, you should use as many engines as possible, with a bias towards certainty. The Edge Server role is not computationally intensive, so your servers are likely to have more than enough spare CPU capacity to support running four or five engines; this will give you a better chance at intercepting infected messages before they reach mailbox servers or clients.

If you're using a desktop scanning solution in a collaboration environment, you'll probably want to choose a set of engines for use with Forefront Security for SharePoint that doesn't overlap with your desktop scanning engine. This helps ensure maximum coverage for files and documents in the library. SharePoint servers that are used for message archiving won't need to rescan messages that have been previously scanned by Forefront Security for Exchange. However, SharePoint document

libraries should be regularly scanned, and you may want to consider using Forefront Security for SharePoint as a content policy enforcement tool even if your organization feels the risk of malware intrusion is low.

Single-Server vs. Multi-Server Environnent

If you have a single Exchange 2007 server, you can install the same set of content filtering tools that are included with the Edge Transport role. However, you will want to perform both transport and background scanning on the server. Depending on the load imposed on your server by your users and the rate of message arrival, you may need to reduce the number of engines you're using or change the bias settings to provide adequate performance. The meaning of "adequate" will vary from installation to installation; it all depends on how many concurrent users you have, what type of server hardware you're using, and how active users are.

When you use one server for transport scanning functions, and another server for mailbox scanning functions, you can apply separate scanning parameters for each operation. You'll get the best protection if you aggressively scan during the transport stage, using the Max Certainty or Favor Certainty settings and five engines whenever possible. Adding more engines has an impact on transport server performance. However, because Exchange transport is essentially a store-and-forward process, this performance impact will be mostly invisible to users.

In this scenario, background scanning on the mailbox server is primarily a backstop for the intensive transport scans. If you have enough performance headroom, you can use a certainty setting that applies four or five engines; if not, you can probably maintain adequate security with the Favor Performance setting and two or three active engines. Because you can adjust the number of days for which messages are scanned and how many background scan processes are used, you can fine-tune the background scanning process to meet your needs. You should monitor the Microsoft Forefront Server Security object in Performance Monitor; specifically, the Messages Tagged, Total Messages Tagged, Messages Scanned, and Total Messages Scanned will give you useful information on how Forefront is performing on your server under normal load.

The relationship between server counts and deployment of Forefront Security for SharePoint is less well defined. SharePoint servers generally operate as stand-alone entities; the workload on one server doesn't have much effect on other servers in the organization. Some SharePoint servers may be much busier than others, depending on whether they're used for file archival, message archival, or ordinary end-user file and document storage and management. Because you can control the timing of background scans, you will probably want to adjust the Forefront scan time window so that scans occur when the server is lightly loaded, and when no backup or maintenance tasks are scheduled to run.

Conclusion

The ability to use multiple engines helps give you a significant security advantage because it increases the odds of quickly catching new malware before it affects your network. To make the most of this advantage, you should configure Forefront Security for Exchange Server and Forefront Security for SharePoint to use multiple engines for transport and background scanning. As you deploy Forefront Security for Exchange Server and Forefront Security for SharePoint, you can control how they use server resources by adjusting the scan engine settings and controlling which engines you use and where they’re applied in the scanning pipeline. This process of adjustment, which should include both baseline and ongoing performance monitoring, will help you find the optimal balance of security and performance for your specific needs. You can choose a set of scan engines that will help complement other existing protective measures that you now have in place, taking advantage of the advanced multi-engine support in these Forefront server security products to give you better coverage and more protection.

Related Links

For the latest information about Microsoft Forefront security products, see the Microsoft Forefront Web site at http://www.microsoft.com/forefront.