TREND MICRO™

Securing Your Web World

Trend Micro Advanced Reporting and Management 1.5 for Trend Micro InterScan Web Security

Performance and Sizing Guide

TECHNICAL SALES SOLUTIONS

August 2011

Trend Micro, Inc.
10101 N. De Anza Blvd.
Cupertino, CA 95014
T 800.288.5651 / 408.257.1500
F 408.257.2003
www.trendmicro.com

Contents

Executive Summary

This sizing guide is designed to help customers properly size Trend Micro's Advanced Reporting and Management 1.5 (ARM 1.5) for Trend Micro™ InterScan™ Web Security into their network environments to centrally manage their IWSVA reporting and policy management needs.

Performance testing and sizing examples listed in this sizing guide was conducted with real world environments and represent general sizing concepts approved by Trend Micro. These examples can be used as guidelines for properly sizing ARM for your environment.

The following paragraphs summarize sizing results for a single, 64-bit CPU ARM 1.5 server:

Sizing by Hardware

- **Dual 2.8 GHz Intel Core2Duo processor (4 total cores) with 8 GB RAM** – Supports 2,500 events per second; for environments with up to 10,000 users.
- **Dual 3.16 GHz Intel Xeon processor (8 total cores) with 16 GB RAM** – Supports 6,000 events per second; for environments with over 10,000 users.

Sizing by Number of IWSx Instances

ARM 1.5 can manage up to 50 IWSx instances simultaneously. However, environments with more than 10,000 users' traffic being logged into a single ARM may require modifications to the logging verbosity and grooming setting in IWSx to ensure sustainable performance.

For the latest information about Trend Micro Advanced Reporting and Management 1.5, including documentation, device support, and the latest software builds, visit the Trend Micro Web site:

http://downloadcenter.trendmicro.com/

Impact of Deploying ARM 1.5

Adding ARM 1.5 to an IWSx environment:

- Creates a single common database for all registered IWSx servers.
- Causes each registered IWSx server to send a copy of its logs to the central ARM 1.5 database. ARM 1.5 does not uninstall the local databases on the IWSx instances in case the IWSx instance needs to be unregistered from ARM and managed independently.
- Causes an increase in network traffic between ARM 1.5 and all of its registered IWSx servers. This is because the IWSx servers automatically forward all database communication to ARM 1.5. This includes event logs and reporting information.
- Can potentially reduce the amount of available bandwidth at low bandwidth remote sites. Trend Micro recommends performing a careful evaluation of available network bandwidth if you connect geographically remote IWSx instance to a central ARM 1.5 instance.

Part No: SGEXARM15_110815US

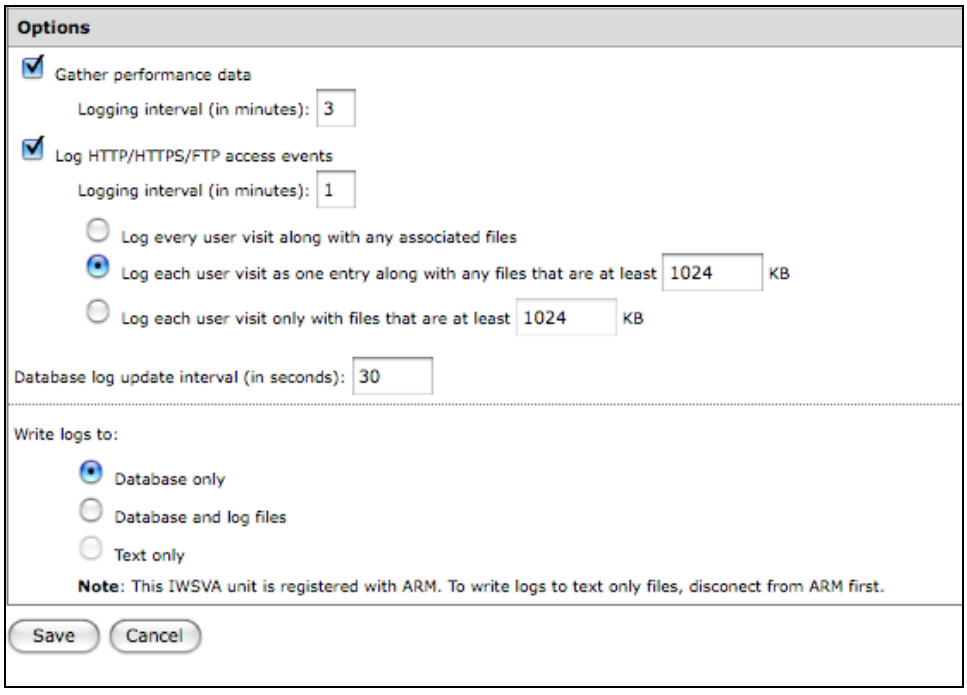
Adding ARM 1.5 to an IWSx environment does not:

- Provide native database clustering or replication. Without redundancy/clustering, ARM 1.5 can become a single point of failure for registered IWSx products. Customers can architect ARM redundancy and fault tolerance with VMware's High Availability features or with fault tolerant hardware solutions (such as NEC's R320a server series).
- Synchronize the time used by IWSx servers in multiple time zones automatically. Customers must manually set IWSx servers in different physical time zones to use the same "global" time (typically, this is the time they set in the ARM 1.5 server). The ARM 1.5 and IWSx servers use the Network Time Protocol (NTP) to ensure the synchronization of events.

Sizing Assumptions

The sizing calculations in this document:

- Require a properly sized IWSx environment. While ARM 1.5 reduces local IWSx I/O requirements and thus frees system resources for an increase in local scanning capacity, Trend Micro does not recommend adding ARM 1.5 solely to increase scanning capacity in borderline performance situations.
- Assume that 20% of your user population accesses the Internet at the same time (i.e., are active users) if the true number is unknown.
- Set the IWSx logging parameters to their default values. For IWSVA 5.x this means only logging the initial session information and objects over a specified size (1024 KB by default). If you use verbose logging (all objects, initial sessions, and objects over a specified size), it may affect sizing and you should consider the use of this feature separately. The IWSx default logging options appear below and are discussed more completely in Appendix B:



Customer-based Reference Sizing

Trend Micro used ARM 1.5 in actual customer environments to validate sizing. The results from these sizing validations appear below.

- Sample manufacturing company:
  - 8,000 employees
  - Two IWSx servers registered to a single ARM 1.5 server
  - ARM 1.5 server specification: IBM 3650 with 2x146 GB HD, 8 GB RAM, 2x Quad Core Intel Xeon 5300 3.0 GHz

Sizing at a Glance

Table 1 provides general sizing recommendations for readily available hardware. URL "events per second" is the most accurate measurement available for sizing ARM 1.5. If a customer exceeds any of the thresholds in Table 1, Trend Micro recommends that they purchase the next higher performing server to ensure proper sizing.

Table 1 *Sizing at a Glance*

CPU / RAM	Dual 2.8 GHz Intel Core2Duo 64-bit Processor	Dual 3.16 GHz QuadCore 64-bit processor
4 GB	• **Up to 4,000 User Population** • 1,000 URL events per second • 20 total active dashboards between all administrators • Requires 4,800 Kbits/sec bandwidth	-
8 GB	• **Up to 10,000 User Population** • 2,500 URL events per second • 40 total active dashboards between all administrators • Requires 12,000 Kbits/sec bandwidth	• **Up to 10,000 User Population** • 2,500 URL events per second • 40 total active dashboards between all administrators • Requires 12,000 Kbits/sec bandwidth
12 GB	-	• **More than 10,000 User Population** • 4,000 URL events per second • 60 total active dashboards between all administrators • Requires 19,200 Kbits/sec bandwidth
16 GB	-	• **More than 10,000 User Population** • 6,000 URL events per second • 80 total active dashboards between all administrators • Requires 28,800 KB/sec bandwidth

Part No: SGEXARM15_110815US

Note:

- Trend Micro calculates ARM 1.5 sizing primarily on database read/write events. Since ARM 1.5 acts as a remote database for the logs from IWSx instances, these events have an impact on the physical network and customers should evaluate them carefully..
- As the number of users and events increases, it becomes essential to use a fast disk subsystem to increase system performance (for example, a SCSI disk array in a RAID 1+0 configuration with 10,000+ RPM hard disks)
- Trend Micro has configured ARM 1.5 Dashboard components to refresh every 60 seconds over a period of 4 hours.

Advanced Reporting and Management 1.5 Sizing

Step 1: Obtain the Required Data for Sizing ARM

At a minimum, you need the following information to size your environment (use Table 1):

- User population (including planned growth)

If you require more accurate sizing, you must also attempt to gather the following information as well.

- Log events per second

Table 2 shows the sizing variables for ARM 1.5. Obtain from your environment as many of the variables in Table 2 as practical and write them down for use in the calculations.

Note: To ensure proper sizing, Trend Micro recommends that customers use peak loads (the highest number of active users) to calculate the hardware required for an ARM 1.5 server.

Table 2 *Environment Variables for ARM 1.5 Sizing*

Name	Variable	Description
Number of Users with Internet Access	USER_POPULATION	The total number of users with Internet access that this IWSx + ARM 1.5 deployment supports. Ensure that this number includes any planned growth.
Log Events per second	CONNECTIONS	This is the most accurate statistic available to size the ARM 1.5 environment. See Step 2 below for how to measure the log events per second by using the Log Query feature of IWSx.

Part No: SGEXARM15_110815US

Step 2: Size the Environment

Calculate if only user population is Known

If you only know the User Population (i.e. the number of seats), simply compare the User Population value to the sizing guidelines in Table 1 to find the best fit for the environment.

It is best if you can install the maximum amount of RAM possible as ARM 1.5 makes use of RAM for its dashboard views and management components. The RAM sizes provided in this sizing guide are general recommendations and installing more RAM can help improve real-time dashboard performance and overall user experience.

Calculate if log events per second is known

If you desire more accurate sizing and an existing IWSx deployment exists, you can use the IWSx logs over peak time periods to estimate it.

On each IWSx instance that will be reporting into ARM 1.5:

1. Go to each of the logs in the **Logs → Log Query** section (except for the Audit Log) and run a report for the last full day for each log type.
2. Look at the peak hours and see how many events each log generated per hour.
3. Add these up from each log report per instance and calculate the total. This is the total number of events for this hour.
4. Do this for each of the IWSx instance in the cluster and add up the total. If you do this for several "heavy traffic" days, determine which hour is the heaviest for each server and then add 15 – 25% on top of that for safe measure. This figure is the rough events per hour for the system as a whole. Divide this by 3,600 to calculate the average number of events per second for your environment's peak time.

Once you have determined the peak log events per second, you can use Table 1 to find the best hardware fit for the environment. Remember to size up instead of down to handle any growth the environment may need.

Part No: SGEXARM15_110815US

Appendix A – Hardware Tested

Hardware Specifications

Tables 3 and 4 provide the details of the hardware Trend Micro used in this Sizing Guide. Similar CPU and hard disk configurations from other vendors will offer similar results, as results are not specific to the vendor and model of the hardware.

Table 3 *Hardware and Operating System Specifications – Server 1*

Hardware	Specifications
Server	Dell 1950
Processor	Dual 2.8 GHz Intel Core2Duo 64-bit Processor
Total Cores	4
Memory	4, 8, 12 GB RAM (depending on test)
Disk	2 x 73 GB 15K RPM SAS on Dell Perc 5/I SAS Controller
Network	1 Gigabit Ethernet (2)
Operating System	CentOS 5.1

Table 4 *Hardware and Operating System Specifications – Server 2*

Hardware	Specifications
Server	Dell 2950
Processor	Dual 3.16 GHz QuadCore 64-bit Intel Xeon processor
Total Cores	8
Memory	8, 12, 16 GB RAM (depending on test)
Disk	3 x 73 GB 15K RPM SAS on Dell Perc 6/I SAS Controller
Network	1 Gigabit Ethernet (2)
Operating System	CentOS 5.1

Appendix B – IWSx Logging Settings and Traffic Impact

Default Configuration of IWSx for use with ARM 1.5

This document presents sizing estimates that assume the IWSx servers use a specific configuration. If your IWSx server deviates from this configuration, you may have to adjust sizing capacity accordingly. This section describes the configuration Trend Micro recommends for registered IWSx servers.

By default, IWSx version before 5.1 SP1 does not log HTTP/FTP access events. Access events are essential for proper reporting in ARM 1.5 and so you must manually enable HTTP/FTP logging on the IWSx servers version before 5.1 SP1 you register with ARM 1.5.

Note: Enabling user access logging on IWSx servers will affect IWSx performance directly. A minimum degradation in performance of 10% is to be expected for servers running faster harddrives and controllers. Servers with slower disk controllers and harddrives may see up to 20% degradation.

Please refer to the *InterScan Web Security Virtual Appliance Sizing Guide* for further discussion on the affects of logging.

Below is a summary of the logging configuration settings that must be in place on each IWSx instance registered to ARM.

- Log into the IWSx unit as the **Admin** user.
- Go to **Logs → Settings** menu screen.
- Under the options section, enable the check box for "**Log HTTP/FTP access events**"
- Set the logging interval to **1 minute.**
- Select the option to "**Log each user visit as one entry along with files over 1024 KB**". This reduces the number of logging events and logs only high-level access information. Use the size setting to adjust the volume of logs saved. Increasing the size of the objects logged will reduce the number of log events saved in the database, but will affect the accuracy of the Internet volume and time used reports.
- Save the settings and exit.
- Repeat for each IWSx unit registered with the ARM 1.5.

Estimating the Network Traffic Impact of Deploying ARM 1.5

If you want to estimate the additional network traffic ARM 1.5 introduces, follow these steps.

- Estimate the total number of events per second for your environment. This document includes guidelines for this process in the "Calculate if log events per second is known" section.
- Each logging event is typically 600 bytes in size. Multiply the total number of events per second by 0.600 KB to obtain KB/second network requirements.
    - Example: For a 2,500 event per second environment, this equates to 600 x 2,500 = 1,500 KB/sec network load.
- If calculating the number of events per second is not possible, then refer to refer to Table 1 for a recommendation on the bandwidth requirements for ARM based on the number of users in the environment.

Part No: SGEXARM15_110815US

About Trend Micro Incorporated

Trend Micro Incorporated, a global leader in Internet content security, focuses on securing the exchange of digital information for businesses and consumers. A pioneer and industry vanguard, Trend Micro is advancing integrated threat management technology to protect operational continuity, personal information, and property from malware, spam, data leaks and the newest Web threats. Its flexible solutions, available in multiple form factors, are supported 24/7 by threat intelligence experts around the globe.

Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware, and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at http://www.trendmicro.com/.

Part No: SGEXARM15_110815US