TREND MICRO™ | Securing Your Web World

InterScan Web Security Virtual Appliance

Sizing Guide for version 6.5

Nov 2014

TREND MICRO INC.
10101 N. De Anza Blvd. Cupertino, CA 95014 •**www.trendmicro.com**
•**Toll free:** +1 800.228.5651 •**Fax:** +1 408.257.2003 •**Phone:** +1 408.257-1500

Contents

Information contained in this document is provided "as-is" and subject to change without notice. This report is for informational purposes only and is not part of the documentation supporting Trend Micro products.

TRENDMICRO MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS REPORT.
[ETM Part No: SG_SVA_201206US]

This document is a product of Trend Micro Technical Sales Solutions.

Executive Summary

Trend Micro conducted tests on Trend Micro™ InterScan™ Web Security Virtual Appliance v6.5 (IWSVA) to obtain performance sizing data for customer deployment.

Several factors impacts the sizing results for an IWSVA deployment, including:

- CPU
- Memory
- Which scanning features are enabled and what percentage of traffic will be scanned by those features

For the latest information about InterScan Web Security Virtual Appliance, including product documentation, server hardware support and the latest software builds, visits the Trend Micro Web site at:

`http://www.trendmicro.com/us/enterprise/network-security/interscan-web-security/index.html`

`http://downloadcenter.trendmicro.com/`

Assumption and Recommendation

Assumption:

- The *user population* is the total number of potential Web users within an organization.
- The number of a*ctive users* is the total number of client workstations that are simultaneously requesting HTTP content at any point in time. This is assumed to be 20% of the user population by default.
- Gigabit network interface cards (NIC) are used throughout the LAN.
- HTTPS scanning is disabled by default.
- When measuring the impact of Application Control performance, it is assumed 35% of the network traffic to be non-HTTP (e.g. UDP, Skype, bitTorrent, etc.)
- Each active user has in average 3.5 opening HTTP connections to the Internet at any one time.
- Each Internet access generates in average 5 log events.
- The Dynamic URL categorization is set to classify 25% of the total traffic in this sizing test.
- The Script Analyzer engine is set to scan 2% of the total traffic in this sizing test.
- There are four configuration of feature set tested:
  - **Basic feature set:** A basic feature set, only Anti-malware scanning
  - **HTTP scan feature set**, including Anti-malware, Web-reputation, URL-filtering and Anti-Botnet
  - HTTP scan feature set + Application Control, which adds Application Control to the HTTP scan feature set
  - HTTP Scan Feature Set + Application Control + Advanced Threat Scanning + Dynamic URL Categorization + DLP

Recommendation:

- Hardware should meet the minimum requirements specified in the Installation Guide. IWSVA requires have adequate memory to establish TCP connections. If there is not enough memory, system performance will be restricted. We recommend the ratio of Memory to the number of CPU Threads shall be larger than the following calculation result:

Memory = CPU_Threads_Num

General Sizing Guidelines

Administrators can obtain the general sizing on a per-server basis if the specification of the available hardware is known. The sizing below shows the four configurations of enabled features in both Forward Proxy mode and Transparent Bridge mode. Content caching was not used in these tests.

IWSVA performance is CPU-bound and the number of CPU threads will affect performance. For multi-core or Hyper-Threading systems, each CPU thread is considered for the purpose of this sizing guide.

Note: A linear increase in allocated CPU GHz does not equate to a linear performance increase.

The sizing information in this guide is the **absolute maximum** the specified hardware configuration can support before the additional latency introduced to average page download times exceeds 2 seconds. The results in the tables below are accurate to within ±5 percent.

Sizing at a Glance – Software Appliance (Bare Metal)

Assuming Virus Scan, Web reputation, Anti-Botnet and URL filtering are active on an IWSVA 6.5 server in Forward Proxy and Transparent Bridge mode deployment; Tables 1, 2, 3 and 4 provide recommendations for bare-metal software appliance general sizing respectively for the four feature set configurations described in Assumptions and Recommendations: 1. Basic feature set, 2. HTTP scan feature set, 3. HTTP scan feature set + App control, 4. HTTP scan feature set + App control + Advanced Threat Scanning + Dynamic URL categorization + DLP

Note: Following test results are all based on IWSVA standalone logging mode. Please refer to “Sizing at a Glance – Central Logging” for the sizing about IWSVA configured to use external IWSVA central log server.

- **IWSVA 6.5 Sizing at a Glance with Basic Feature Set**

Server Type	Memory Size	Concurrent Connections	HTTP Transactions per Second	Throughput (Mbits per second)	Maximum Total User Population per device
1 x Inter® Xeon® E3-1240 (4 Cores, 8 Threads)	8 GB	9,200	6,000	800 Mbps	13,000
2 x Intel® Xeon® E5-2420 (6 Cores, 12 Threads)	16 GB	10,500	6,800	900 Mbps	15,000
2 x Intel® Xeon® E5-2660 (8 Cores, 16 Threads)	32 GB	11,600	7,100	950 Mbps	16,000
2 x Intel® Xeon® E5-2660 (8 Cores, 16 Threads) **Multi-link + Central Logging**	32 GB	22,000	15,000	1,900 Mbps	30,000

Notes:

1. Multi-link is a special deploy mode for transparent bridge, it total use 4 NICs, it can exceed single 1000MB network interface limitation.
2. Central Logging use external IWSVA server to store logs, it can reduce the log cost in disk I/O.

- **IWSVA 6.5 Sizing at a Glance with HTTP Scan Feature Set**

Server Type	Memory Size	Concurrent Connections	HTTP Transactions per Second	HTTP Throughput (Mbits per second)	Maximum Total User Population per device
1 x Inter® Xeon® E3-1240 (4 Cores, 8 Threads)	8 GB	5,000	3,700	500 Mbps	7,000
2 x Intel® Xeon® E5-2420 (6 Cores, 12 Threads)	16 GB	10,400	6,600	870 Mbps	14,000
2 x Intel® Xeon® E5-2660 (8 Cores, 16 Threads)	32 GB	11,100	6,900	920 Mbps	15,000
2 x Intel® Xeon® E5-2660 (8 Cores, 16 Threads) **Multi-link + Central Logging**	32 GB	17,800	11,200	1,430 Mbps	25,000

Notes:

1. Multi-link is a special deploy mode for transparent bridge, it total use 4 NICs, it can exceed single 1000MB network interface limitation.
2. Central Logging use external IWSVA server to store logs, it can reduce the log cost in disk I/O.

- **IWSVA 6.5 Sizing at a Glance with HTTP Scan Feature Set plus Application Control**

Server Type	Memory Size	Concurrent Connections	HTTP Transactions per Second	Throughput (Mbits per second)	Maximum Total User Population per device
1 x Inter® Xeon® E3-1240 (4 Cores, 8 Threads)	8 GB	5,000	3,300	430 Mbps	7,000
2 x Intel® Xeon® E5-2420 (6 Cores, 12 Threads)	16 GB	9,200	5,800	770 Mbps	13,000
2 x Intel® Xeon® E5-2660 (8 Cores, 16 Threads)	32 GB	9,350	6,000	810 Mbps	13,000
2 x Intel® Xeon® E5-2660 (8 Cores, 16 Threads) **Multi-link + Central Logging**	32 GB	14,200	8,800	1,140 Mbps	20,000

Notes:

1. Multi-link is a special deploy mode for transparent bridge, it total use 4 NICs, it can exceed single 1000MB network interface limitation.
2. Central Logging use external IWSVA server to store logs, it can reduce the log cost in disk I/O.

- **IWSVA 6.5 Sizing at a Glance with HTTP Scan Feature Set plus Application Control, Advanced Threat Scanning, Dynamic URL Categorization, and DLP**

Server Type	Memory Size	Concurrent Connections	HTTP Transactions per Second	Throughput (Mbits per second)	Maximum Total User Population per device
1 x Inter® Xeon® E3-1240 (4 Cores, 8 Threads)	8 GB	4,200	2,700	350 Mbps	6,000
2 x Intel® Xeon® E5-2420 (6 Cores, 12 Threads)	16 GB	5,600	4,000	520 Mbps	8,000
2 x Intel® Xeon® E5-2660 (8 Cores, 16 Threads)	32 GB	8,000	5,000	680 Mbps	11,000
2 x Intel® Xeon® E5-2660 (8 Cores, 16 Threads) **Multi-link + Central Logging**	32 GB	8,800	5,500	750 Mbps	12,000

Notes:

1. Multi-link is a special deploy mode for transparent bridge, it total use 4 NICs, it can exceed single 1000MB network interface limitation.
2. Central Logging use external IWSVA server to store logs, it can reduce the log cost in disk I/O.

Please refer to Appendix.A or the specific hardware configuration of each server type used above

Note: Features and Modes Impact on Performance:

- The feature with the largest use of system resources is malware scanning and the second is application control.
- The use of Web reputation, URL filtering, and Anti-Botnet, only modestly lowers system performance and does not significantly decrease the supported user population per server.
- For DLP feature, we configured a policy with only a single template (HIPAA compliance). The sizing and capacity numbers in table 1 were reduced by approximately 10%.
- After enabling LDAP authentication, it will cause nearly 14% drop of sizing capacity number in general.
- Enabling HTTPS scanning in a network that contains 15% of all traffic as HTTPS will reduce the performance numbers by approximately 26%. This is normal since HTTPS key negotiation, decryption and re-encryption are CPU-bound activities.
    - Environments with HTTPS scanning requirements should consider hardware acceleration cards for maintaining peak performance. With a Trend approved HTTPS acceleration card, performance numbers are retained with HTTPS scanning enabled. Refer to the “Trend Micro Software Appliance Support” document for certified hardware acceleration cards (http://www.trendmicro.com/certified) and/or the IWSVA Installation Guide and/or Admin Guides.
- The middle and top grade machine has reached the disk I/O limitation because the large amount concurrent connections generate large amount logs and the IWSVA is in log standalone mode, so the disk I/O limit the system performanc

Sizing at a Glance – Virtual Appliance (VMware ESXi 5.5)

Following table provides the general sizing for virtual appliance deployment in VMware ESXi environment.

- **IWSVA 6.5 Sizing at a Glance with HTTP Scan Feature Set**

Server Type	Memory Size	Concurrent Connections	HTTP Transactions per Second	Throughput (Mbits per second)	Maximum Total User Population per device
VM (8 core)	8 GB	5,000	3,200	450 Mbps	7,000

The performance difference of installing IWSVA on a VMware virtual appliance verses installing IWSVA on a bare metal software appliance server is nearly 12%. The performance degradation under VMware is normal and can be attributable to the VMware OS overhead that is required to manage the Virtual Machines (VMs) and the resources being shared.

Sizing at a Glance – Virtual Appliance (Hyper-V 3.0)

Following table provides the general sizing for virtual appliance deployment in Microsoft Windows Server 2012 Hyper-V environment.

- **IWSVA 6.5 Sizing at a Glance with HTTP Scan Feature Set**

Server Type	Memory Size	Concurrent Connections	HTTP Transactions per Second	Throughput (Mbits per second)	Maximum Total User Population per device
VM (8 core)	8 GB	4,500	3,000	400 Mbps	6,000

- **The performance difference of installing IWSVA on a Hyper-V virtual appliance verses installing IWSVA on a bare metal software appliance server (both using 2/4 CPUs and the same amount of memory and disk) is approximately 23%. The performance degradation under Hyper-V is normal and can be attributable to the Hyper-V OS overhead that is required to manage the Virtual Machines (VMs) and the resources being shared.**

Sizing at a Glance – Central Logging

Following table provides the performance comparison between IWSVA with standalone logging and IWSVA configured to use external IWSVA server for central logging.

- **IWSVA 6.5 Sizing at a Glance with HTTP Scan Feature Set plus App Control and Standalone Logging**

Server Type	Memory Size	Concurrent Connections	HTTP Transactions per Second	Throughput (Mbits per second)	Maximum Total User Population per device
2 x Intel® Xeon® E5-2660 (8 Cores, 16 Threads)	32 GB	9,350	6,000	810 Mbps	13,000
2 x Intel® Xeon® E5-2660 (8 Cores, 16 Threads) **Multi-link**	32 GB	13,500	8,500	1,090 Mbps	19,000

- **IWSVA 6.5 Sizing at a Glance with HTTP Scan Feature plus App Control and Using External IWSVA Server for Central Logging**

Server Type	Memory Size	Concurrent Connections	HTTP Transactions per Second	Throughput (Mbits per second)	Maximum Total User Population per device
2 x Intel® Xeon® E5-2660 (8 Cores, 16 Threads)	32 GB	11,000	6,900	920 Mbps	15,000
2 x Intel® Xeon® E5-2660 (8 Cores, 16 Threads) **Multi-link**	32 GB	14,200	8,800	1,140 Mbps	20,000

- **It is highly recommended to use central logging in middle and large enterprise network environment.**

Sizing at a Glance – Log entries V.S. Disk size

Following table provides recommendations for required minimum disk space V.S. Log entries

- **IWSVA 6.5 Sizing at a Glance with disk space V.S. Log entries**

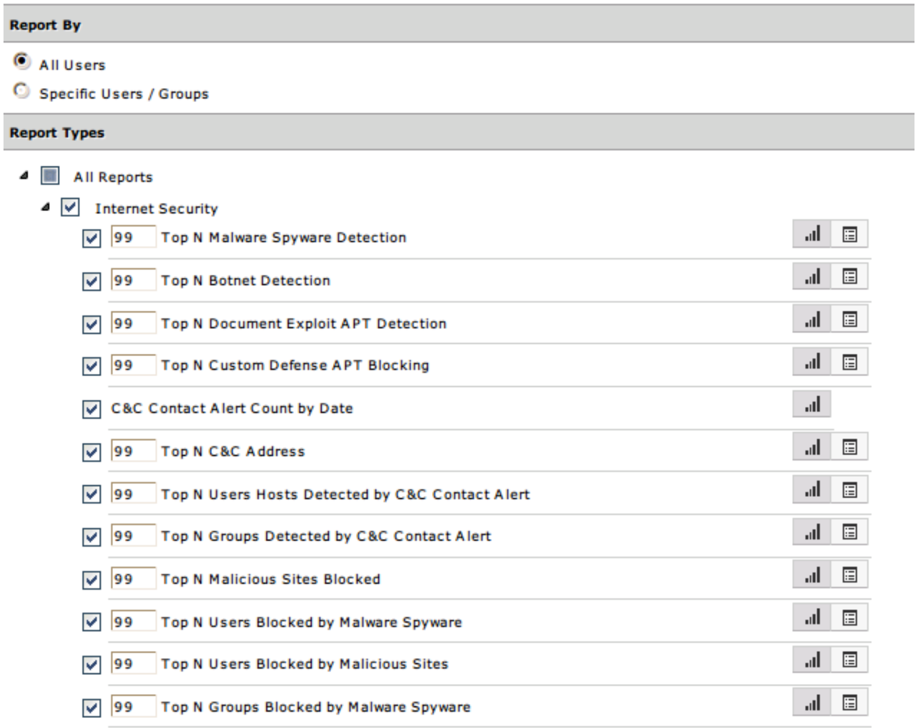
Log Entries	Log Size(GB)	Average Disk Space per million log entries (MB)
3,000,000	0.6 GB	206 MB
110,000,000	11 GB	103 MB
2,200,000,000	134 GB	63 MB
4,400,000,000	256 GB	61 MB

- **The new log storage mechanism makes non-linear relation between log entries and disk space. In general, the average disk space required will be reduced with log entries increasing.**

Note: For simple conversion log size and log entries, please make 140 as ***Average per million entries log size(MB)***

Sizing at a Glance – Report impact

When generating reports, IWSVA need read history data. With the log numbers increases, the report generation time becomes longer. When creating report, the disk IO could be busy, which can impact the system performance, at the same time, user experience may not good for waiting big reports' result.



Report By

● All Users
○ Specific Users / Groups

Report Types

▪ All Reports
☑ Internet Security

☑ 99 Top N Malware Spyware Detection
☑ 99 Top N Botnet Detection
☑ 99 Top N Document Exploit APT Detection
☑ 99 Top N Custom Defense APT Blocking
☑ C&C Contact Alert Count by Date
☑ 99 Top N C&C Address
☑ 99 Top N Users Hosts Detected by C&C Contact Alert
☑ 99 Top N Groups Detected by C&C Contact Alert
☑ 99 Top N Malicious Sites Blocked
☑ 99 Top N Users Blocked by Malware Spyware
☑ 99 Top N Users Blocked by Malicious Sites
☑ 99 Top N Groups Blocked by Malware Spyware

It is recommend scheduling big reports in system idle hours, such like midnight to avoid the resource conflict with content scan functions

Calculating the Number of IWSVA Servers Required

This procedure allows administrator to calculate the number of IWSVA servers required for the deployment based on the number of total users in the organization.

Step 1: Obtain the Required Data for the Customer Environment

At a minimum, the following information is required to size a customer environment:

- User Population

The following items are recommended but not required because sizing estimates can be made based on User Population:

- Peak number of concurrent users
- Peak throughput (Mbits per second)
- Caching percentage (if present)

Sizing variables are defined in Table 14. Obtain from the customer environment as many of the variables listed in Table 14 as practical and write them down on a worksheet to be used in the calculations or in the Sizing Calculator.

Note: To ensure proper sizing, Trend Micro recommends that customers use peak loads (the highest number of active users and peak throughput) when calculating the number of required IWSVA servers.

All the calculations are based on performance data from IWSVA 6.5.

Environment Variables for IWSVA Sizing

Name	Variable	Description
Number of Users with Internet Access	USER_POPULATION	The total number of users with Internet access that will be supported by the IWSVA deployment.
Number of Users Accessing the Internet Simultaneously	%_CONCURRENCY	The percentage of the USER_POPULATION who are actively making an internet request (clicking a link in a web browser) If unknown, it is common to choose 20% (0.20) concurrency when sizing. For environments with more active users, increase the concurrency percentage to a value such as 0.33 or higher. (%_CONCURRENCY=0.20)
Peak Bandwidth Required	THROUGHPUT_TOTAL	The amount of HTTP traffic passing through the gateway in Megabits per second (Mbps). If unknown, it is common to choose a value of 75% available Internet bandwidth. For example, an organization with a T3 connection would have 44.74 Mbits per second. For this organization THROUGHPUT_TOTAL = 0.75 x 44.74 = 33.6.
Connections per user	CONNECTIONS_USER	The number of HTTP connections per active user. If unknown, the default value is 3.5. For environments with users accessing many Web 2.0 sites, increase the number of connections per user to 5 or higher. (CONNECTIONS_USER=3.5).
Caching %	%_CACHE	If a caching solution is present, the percentage of caching occurring for the environment is required. If unknown yet caching is present, it is common to choose 25% caching (%_CACHE = 0.25) for the environment. If no caching is present, choose %_CACHE = 0.

Name	Variable	Description
Maximum log entries per month	MAX_LOG_MONTH	The maximum log number one month in customer's environment
Total maximum log entries	MAX_LOG_TOTAL	The maximum total log number in customer's environment
Number of days to keep logs	DAYS_OF_LOG	The number of days that log can kept on IWSVA *(IWSVA default use 30 day as default value)*
Number of logs of Internet accesses per user per day	NUM_OF_ACCESS	An estimated number of one user generated log of access the internet in one day. *(If you don't know it, we recommend 6500)*
Average per million entries log size	AVG_LOG_SIZE	*(Average per million entries log size, use 140)*

Step 2: Determine the Number of Required Servers

Identical hardware is assumed for all servers in a multi-server deployment. After calculation, the customer can decide which server type fits their needs best and use the recommended number of servers for that specific hardware configuration.

The options listed below assume IWSVA installed as a Software Appliance (bare metal) with access logging enabled (Table 1, 2, 3 depending on IWSVA enabled features).

Note: It is important to note that only one type of server is used for sizing. Do not add the results from the options below; simply choose one of the results for the sizing.

Option 1: Number of 8 threads server (3.3 GHz Intel E3-1240, 8 GBytes RAM)

Using the variables obtained or assumed from Table 3 and LDAP/HTTPs' impact ratio, calculate the number of servers required

$$Number\ \_Servers = \frac{(\mathrm{CONNECTIO\ NS\_USER} \times \%\_\mathrm{CONCURRE\ \ NT} \times \mathrm{USER\_POPUL\ ATION})}{4,000} \times (1 - \%\ \_CACHE\ )$$

Round **up** the number of IWSVA servers to the nearest whole number.

Option 2: Number of 24 threads server (2 x 1.9 GHz Intel E5-2420, 16 GBytes RAM)

Using the variables obtained or assumed from Table 3 and LDAP/HTTPs' impact ratio, calculate the number of servers required:

$$Number\ \_Servers = \frac{(\mathrm{CONNECTIO\ NS\_USER} \times \%\_\mathrm{CONCURRE\ \ NT} \times \mathrm{USER\_POPUL\ ATION})}{5,500} \times (1 - \%\ \_CACHE\ )$$

Option 3: Number of 32 threads server (2 x 2.2 GHz Intel E5-2620, 24 GBytes RAM)

Using the variables obtained or assumed from Table 3 and LDAP/HTTPs' impact ratio, calculate the number of servers required (IWSVA 6.5 used in this example):

$$Number\ \_Servers = \frac{(\mathrm{CONNECTIO\ NS\_USER} \times \%\_\mathrm{CONCURRE\ \ NT} \times \mathrm{USER\_POPUL\ ATION})}{8,000} \times (1 - \%\ \_CACHE\ )$$

Round **up** the number of IWSVA servers to the nearest whole number.

IWSVA 6.5 Sizing Example

For a customer with:

- USER_POPULATION = 10,000
- %_CONCURRENT = 0.20
- CONNECTIONS_USER = 3.5
- %_CACHE = 0.20
- THROUGHPUT_TOTAL=180 Megabits per second

Who desires sizing using the following existing server configuration:

- Two CPU (two, dual-core, 3.0 GHz Intel Xeon 5160 CPU's)
- Memory per server is 4 GB

The number of required servers is as follows:

$Number\ \_Servers = \frac{(3.5\times 0.20\times 10,000)}{1,700}\times (1-0.20)$= 3. With rounding **up**, this equals 3.0

For this network, three (3) servers are required to meets their needs to ensure scanning capacity meets environmental conditions.

Note: If throughput information is also available, the throughput capabilities of the solution should be compared to the environment needs prior to making a recommendation.

Simply compare the THROUGHPUT_TOTAL variable (if available) to the calculated throughput for the recommended solution. The calculated throughput should be greater than the THROUGHPUT_TOTAL variable. If it is not, the number of recommended servers should be adjusted accordingly.

Conclusion: For customers using IWSVA version < 6.0, if no need to enable new features and just keep legacy features enable, customers only need to adopt memory = number of CPU threads x 0.5 + 3.

If they want to enable new features in IWSVA 6.5, suggest use calculation above to adopt hardware resource.

For new customers using IWSVA 6.5, just use calculation above to adopt hardware is enough.

Step 3: Determine the Storage

The administrator can use the information described below to calculate the required disk space for log storage.

For storage type, it is recommended using a fast disk subsystem. *(For example, SAS 15000rpm disk in RAID 1+0 configurations, even use SSD disk is more powerful.)*

Note: As the number of users and events increases, the DISK_IO will more busy even 100%; it becomes more important to use a fast disk subsystem to increase Log performance.

Dimensions 1: How much disk space is needed if I have XXX record logs?

From above sizing about Log entries V.S. Disk size, we get Average per million entries log size (MB) = 140, so we can calculate needed disk size (GB):

$$Disk\_Size(GB) = \frac{MAX\_LOG\_TOTAL}{1{,}000 \times 1{,}000 \times 1{,}024} \times AVG\_LOG\_SIZE$$

IWSVA 6.5 Storage Sizing Example

For a customer with:

- MAX_LOG_TOTAL = 2,200,000,000

The number of required disk size is as follows:

$Disk\_Size = \frac{2,200,000,000}{1{,}000 \times 1{,}000 \times 1{,}024} \times 140$ = 300.78125 with rounding **up**, this equals 301 GB

Dimensions 2: How much disk space is needed if I have XXX users?

$$Disk\_Size(GB) = \frac{USER\_POPULATION \times NUM\_OF\_ACCESS \times DAYS\_OF\_LOG}{1{,}000 \times 1{,}000 \times 1{,}024} \times AVG\_LOG\_SIZE$$

IWSVA 6.5 Storage Sizing Example

For a customer with:

- *USER_POPULATION = 10,000*

Following is IWSVA default value:

- *NUM_OF_ACCESS = 6,500* ***(default)***
- *DAYS_OF_LOG = 30* ***(default)***
- *AVG_LOG_SIZE = 140* ***(default)***

The number of required disk size is as follows:

$Disk\_Size = \frac{10,000 \times 6,500 \times 30}{1,000 \times 1,000 \times 1,024} \times 140$ = 266.6015625 with rounding **up**, this equals 267 GB

Dimensions 3: How many days of log can be kept on IWSVA?

The default value for log days on IWSVA is 30 days. Sometimes user wants to modify the log days on IWSVA to fits the hardware. If the user has known the disk space available for logs and the number of users, then he can get the number of days to keep log on IWSVA by one of the following formulas:

$$DAYS\_OF\_LOG = \frac{Disk\_Size \times 1,000 \times 1,000 \times 1,024}{NUM\_OF\_ACCESS \times USER\_POPULATION \times AVG\_LOG\_SIZE}$$

IWSVA 6.5 Storage Sizing Example

For a customer with:

- *USER_POPULATION = 5000*
- *Disk_Size = 128 (GB)*

Following is IWSVA default value:

- *NUM_OF_ACCESS = 6,500* ***(default)***
- *AVG_LOG_SIZE = 140* ***(default)***

The days of log can be kept is as follows:

$DAYS\_OF\_LOG = \frac{120 \times 1,000 \times 1,000 \times 1,024}{6,500 \times 5000 \times 140}$ = 27.00659340659341 with rounding **up**, this equals 27 days

Step 4: Determine the Standalone log server

Recommendations:

- We recommend use bare-metal for standalone log server because in our test compare the IO performance, bare-metal is better than the virtual platform.

Standalone log server can receive multi IWSVA's log. It replaces central log. Use standalone log server can also avoid log query and generated report's impact to system performance.

Recommend Configuration:

CPU: *8 Threads (8 cores CPU or 4 cores CPU with Hyper Thread supported)*

MEM: *16G*

Disk Size/Disk IO: *Please refer to section "Determine the storage"*

Max Users support for 1 log server: *20,000*

Max logs support for 1 log server: *2.2 billion*

Note: *If the users > 5000 or log entry >1 billion per month, it is recommended to only keep* ***2 months*** *logs for better performance.*

Appendix A

How Tests Were Conducted

Product performance was determined based on a workload where each active user accesses 12 Web sites sequentially. This workload was deemed representative of that of an actual enterprise. The range of object sizes (.jpg, .png, .css, .gif, and .js) ranged between 9 and 174 KBytes, with .htm pages ranging between 3 and 143 KBytes. Think time was maintained at 5 seconds, making this a test of moderately aggressive Internet surfing behavior. For the application control's impact for IWSVA 6.5, we use one scenario, which is to use pure HTTP traffic to check application control's impact for features.

The use of ICAP or caching in general greatly improves the capacity of the environment by reducing the amount of network communication to the IWSVA server.

Note: IWSVA also includes a *Web Reputation* feature. This feature relies on DNS queries to Trend Micro data centers for each new URL request. Reputations are cached for a period of 35 minutes by default and new reputation requests for that URL are provided without the need for additional queries.

This Sizing Guide assumes that the customer environment has sufficient DNS infrastructure to handle the query load that results from deploying one or more IWSS units.

What Configuration Changes do to Sizing

Configuration changes to IWSVA affect sizing in a number of ways. These impacts are summarized below:

Reporting

- Real-time reports can take a significant amount of time to complete in high-workload environments if there are inadequate amounts of free CPU to process each request. For this reason, reports should be scheduled for non-peak workload periods.
- Environments requiring efficient real-time reporting during high-workload periods are advised to size their servers for less than 100% CPU utilization to keep the end-user and administrative experiences positive. Alternatively, the standalone log server can be deployed on a separate host/vm to handle all log processing and reporting actions. This frees up the IWSVA instance to dedicate its resources to processing traffic.

- Using high-performance RAID arrays with fast hard disks (SAS 15000rpm or SSD disk) will improve performance significantly.

Caching

Using caching in an environment affects system performance. With a properly sized ICAP 1.0 solution in

The place, the capacity of the environment increases proportionally to the cache percentage:

- A 25 percent cache allows each server to increase capacity by a factor of 1.3.
- A 50 percent cache allows each server to increase capacity by a factor of 2.
- A 75 percent cache allows each server to increase capacity by a factor of 4.
- A 90 percent cache allows each server to increase capacity by a factor of 10.

These performance factors are based on an off box external ICAP server.

Performance Criteria for Tests

Trend Micro conducted the tests with the requirement that all test results and sizing recommendations meet the following conditions:

- Hosts and servers have zero TCP Connection failures
- Hosts and servers have zero HTTP Transaction failures
- Hosts must experience an average page load time of no more than 2000ms (2 seconds)

Although the IWSVA servers can provide more connections and transactions than listed in the sizing tables, the page load latency will be above 2 seconds and will not reflect real-world expectations where users expect faster Internet response times.

Scalability and Accuracy

The performance ability of IWSVA depends on the quantity and type of CPU being used and also the feature sets enabled. Higher MHZ and more CPU can bring better performance results. However, when the Application Control feature is enabled, performance increases flatten out above 12 CPU cores. Since 12 cores can support up to 12,000 users in a single IWSVA instance, it is unlikely that a customer would have more than that many users' traffic flowing through a single instance. Segmenting the network to have Internet traffic from separate sub-nets flowing to multiple concurrent IWSVA instances is one way to address this potential scalability issue.

The testing procedure and methodology used in this report is accurate, reproducible and well documented. The results are precise by ±5 percent.

Hardware Tested

Tables 16-22 provide details of the hardware used in this Sizing Guide.

- **4 thread Server**

Component Type	Value
Chassis	Dell R210II
CPU	Intel® Xeon® Processor E3-1240
CPU Speed	3.30 GHz
Cores per CPU	4
Threads per cores	2

Number of physical CPU	1
Total Threads	8
Memory	8 GB
Storage	SATA SSD, SAS
Network	Broadcom BCM 5716

- **24 thread Server**

Component Type	Value
Chassis	Dell R420
CPU	Intel® Xeon® Processor E5-2420
CPU Speed	1.9 GHz
Cores per CPU	6
Threads per cores	2
Number of physical CPU	2
Total Threads	24
Memory	16 GB
Storage	SAS SSD, SATA SSD, SAS
Network	Broadcom® NetXtreme 5709c

- **32 thread Server**

Component Type	Value
Chassis	Dell R720
CPU	Intel® Xeon® Processor E5-2660
CPU Speed (Total Allocated)	2.2 GHz
Cores per CPU	8
Threads per cores	2
Number of physical CPU	2
Total Threads	32
Memory	32 GB
Storage	SAS SSD, SATA SSD, SAS
Network	Broadcom® BMC5709C

Glossary

Active Users – The number of actual users requesting Web content through an HTTP Web browser (such as Microsoft Internet Explorer) at any time.

Connection Latency – The amount of time between the user’s first click in a Web browser until the time data begins appearing on the screen.

Default Configuration – The default configuration of IWSVA is with antivirus, Web-reputation, URL filtering, and Anti-Botnet (enabled in IWSVA 6.5 by default) active.

HTTP 1.1 Connection – A method that makes one connection can send or receive multiple HTTP requests or responses. HTTP 1.1 allows multiple requests to be made through a single connection.

Requests per second – The rate at which HTTP objects (for example .jpg, .gif or .html files) are requested and processed.

Think Time – The time between browser clicks for an active user.

Throughput – The amount of digital data per time unit that is delivered over a physical or logical link or that is passing through a gateway scanning device. This is expressed as either Bytes per second or bits per second (8 bits = 1 Byte).

Total Page Download Latency – The average total time to download a workload-specific Web site after initial connection.

User Population – The total number of users with Internet access to be supported by the IWSVA deployment.

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. Trend Micro's flexible solutions, available in multiple form factors, are supported 24/7 by threat intelligence experts around the globe. A transnational company, with headquarters in Tokyo, Trend Micro's trusted security solutions are sold through its business partners worldwide.

For more information, please visit www.trendmicro.com.