Abstract
This document describes best practices for deploying Deep Security and specific configurations and settings used in validating Deep Security on the EMC VSPEX platform in EMC’s VSPEX Labs.

May 2013
Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme file and the latest version of the applicable user documentation.


At Trend Micro, we are always seeking to improve our documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact your Technical Account Manager.
Contents

Recommendations for Deep Security Virtual Appliance (DSVA) ............... 56

Chapter 4 Performance Tuning .......................................................... 58
Disable Stateful Logging of UDP Packets (Especially in a Windows Environment) ........................................................................................................... 59
Performance Profiles ........................................................................... 59
Log Retention Strategy ........................................................................ 59
Database Indexing ............................................................................. 60

Chapter 5 Backup and Disaster Recovery ......................................... 61
Backup and Disaster Recovery ................................................................ 62
Rule and Configuration Backup .......................................................... 62
Back-up an SQL database using Deep Security Manager ...................... 62
Back-up an SQL database using the osql.exe tool ................................ 63
Back-up an SQL database using Enterprise Manager .......................... 64
Restoring an SQL database using the osql.exe tool ............................... 64
Restoring an SQL database using Enterprise Manager ....................... 65
Back-up and Restore an Oracle database using Recovery Manager (RMAN) ........................................................................................................... 65
Disaster Recovery ............................................................................. 66

Appendix A References ........................................................................ 69
Communication Ports .......................................................................... 70
Updates .............................................................................................. 72
Recommended Scan Exclusion List ...................................................... 72
Recommended Scan List ..................................................................... 74
Chapter 1: Introduction

This chapter presents the following topics:

Product Description ...................................................................................................... 7
Terminology ...................................................................................................................... 7
Solution Tested ................................................................................................................. 8
Lab Architecture ............................................................................................................... 8
Lab Reference Architecture .......................................................................................... 11
Validation Methodology ................................................................................................. 13
Validation Results ............................................................................................................ 13
Chapter 1: Introduction

Product Description

Deep Security is a comprehensive, flexible and cost-effective security solution for physical and virtualized environments, enabling customers to achieve and demonstrate compliance, maximize cost savings and minimize business disruptions.

Deep Security combines intrusion detection and prevention, firewall, integrity monitoring, log inspection, web application protection, application control and anti-malware capabilities in a single, centrally managed enterprise software solution.

Beyond standard firewall protection, Deep Security provides true stateful firewall configuration, and deep packet inspection, monitors file system changes and inspects operating system logs, along with delivering advanced application vulnerability protection.

Terminology

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AM</td>
<td>Anti-malware</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>DS</td>
<td>Deep Security</td>
</tr>
<tr>
<td>DSM</td>
<td>Deep Security Manager</td>
</tr>
<tr>
<td>DSVA</td>
<td>Deep Security Virtual Appliance</td>
</tr>
<tr>
<td>EPSec</td>
<td>Endpoint Security</td>
</tr>
<tr>
<td>ESX</td>
<td>Elastic Sky X</td>
</tr>
<tr>
<td>LKM</td>
<td>Loadable Kernel Module</td>
</tr>
<tr>
<td>VC</td>
<td>Virtual Centre</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>VDI</td>
<td>Virtual Desktop Infrastructure</td>
</tr>
</tbody>
</table>
Chapter 1: Introduction

Solution Tested

The purpose of this section is to share the results of the On-Demand Anti-Malware scan performance impact on storage I/O rate and response time latency with EMC for VSPEX validation. The testing was conducted in the EMC VSPEX lab environment to simulate a large-scale deployment. There were 125 VM’s running on three ESX hosts. The lab architecture section provides further details about the distribution of these VM’s across each ESX host. In this testing we analyzed the performance hit of Deep Security Virtual Appliance under stress workload. In our testing, we choose “vdbench” tool to generate a controlled storage I/O workload. Vdbench is an open-source I/O workload generation tool that is available for download on Source Forge Website. The vdbench tool allows control over workload parameters such as I/O rate, LUN or file sizes, transfer sizes, thread count, volume count, volume skew, read/write ratios, read and write cache hit percentages, and random or sequential workloads. In our testing the “vdbench” tool was run for 12 hours to generate a controlled workload while the test VM were scanned for malware presence. Each test client used a workload of random I/O consisting of 67% read and 33% write operations. Each test was run with an I/O request size of 8K. 100 Vdbench worker threads were run for each client VM. The results gathered were then analyzed to identify appropriateness / readiness of a given environment to run Deep Security Virtual Appliance (DSVA) in EMC VSPEX environment.

Lab Architecture

The purpose of this section is to provide a high-level sketch of the various solution components involved in this testing and to detail the additional component that were required to complete this testing. First an architecture overview of each solution component i.e. Deep Security, EMC VSPEX and vdbench tool is presented to introduce the concepts and naming used to describe the overall testing environment, then the specifics of the Lab environment are discussed. This will help the reader of the document to completely understand the entire testing environment.


- **Deep Security Manager (DSM):** This is the management component of the system and is responsible for sending rules and security settings to the Deep Security Agents/appliance. The DSM is controlled using the web-based management console.
Chapter 1: Introduction

- **Deep Security Agents (DSA):** This component is the enforcement point for all protection functionality on a host computer using an agent. The nature of that protection depends on the rules and security settings that each DSA receives from the Deep Security Manager.

- **Deep Security Virtual Appliance (DSVA):** This component is the enforcement point for all protection functionality on a host computer using an appliance. This eliminates the need to have an agent on each guest VM’s. A security Virtual appliance is installed as virtual machines on an ESXi platform to provide protection to each guest VM’s running on the ESX host. The nature of that protection depends on the rules and security settings that are configured for each VM’s at the Deep Security Manager.

- **Deep Security Filter Driver:** This component is loaded into the VMware Kernel to provide network related security (Firewall (FW), Deep Packet Inspection (DPI)). It is integrated with VMSafe API.

- **Database:** The database contains all persistent information that DSM needs to operate. This includes configuration details and event log information for each individual protected host, and other records required for DSM operation.

For agent-less security two additional components are required:

- **vShield Endpoint Driver:** The vShield Endpoint Driver is a part of VMtools and it offload antivirus and anti-malware processing to dedicated security-hardened virtual machines/appliances such as DSVA.

- **vShield Manager:** vShield Manager is a VMware Component and it is used to deploy the EPsec LKM. The Loadable Kernel Module (LKM) is what makes file scanning possible.
Chapter 1: Introduction

The figure below depicts this deep security agent-less architecture, highlighting all of its components, which were described above.

EMC VSPEX Architecture Overview

The figure below depicts a typical EMC VSPEX architecture.
Chapter 1: Introduction

The vdbench tool architecture components are:

- **Vdbench Master**: vdbench runs as two or more Java Virtual Machines (JVMs). The master takes care of the parsing of all the parameters, it determines which workloads should run, and then will also do all the reporting.

- **Vdbench Slave**: vdbench slave works with vdbench master, which instruct vdbench slave to run a specific workload against the storage.

Lab Reference Architecture

The VSPEX lab environment consisted of four ESX servers that were distributed into two datacenter objects (INFRA and VSPEX) configured at VMware vCenter server. The INFRA datacenter object consisted of one ESX host (C210-1) and it was used to host the infrastructure components for this testing. The VSPEX consists of three ESX hosts (C260-01, C260-02 and C260-03) and these were used to host 125 test client VM’s. The workload generation clients were running Windows 2008 R2. The following diagram depicts the lab environment used to perform this testing.

The following table provides greater details on how the hardware and software layouts were used for each server.
### Table 1 - VSPEX Lab - Hardware/software layout

<table>
<thead>
<tr>
<th>Server Details</th>
<th>Hardware Specifications</th>
<th>Software Specifications</th>
</tr>
</thead>
</table>
| **Name:** C210-01.vsepx.vdc | **Manufacturer:** Cisco Systems Inc.  
**Model:** R210-2121605W  
**CPU Cores:** 12 CPU x 3.066GHz  
**Processor Type:** Intel Xeon(R) CPU X5675 @3.07GHZ  
**RAM:** 96 GB | • vspe-ad (Domain Controller – 2008R2)  
• vspe-vsm (vShield Manager - 5.1.1.848085)  
• vspe-dsm (Deep Security Manager – 9.0.4017, Deep Security Relay 9.0.0.883)  
• vspe-vc (vCenter Server 5.0.6.23373)  
• vspe-sql (MS SQL – 2008 R2)  
• vdbench Master  
• vdbench Master NFS1  
• vdbench Master NFS2  
• vdbench Master NFS3  
• vdbench Master NFS4  
• vdbench Master NFS5 |
| **Version:** ESXi 5.0.474610 | **Description:** This server was used to host infrastructure components. | |
| **Name:** C260-01.vsepx.vdc | **Manufacturer:** Cisco Systems Inc.  
**Model:** C260-BASE-2646  
**CPU Cores:** 20 CPU x 2.393GHz  
**Processor Type:** Intel Xeon(R) CPU E72870 @2.40GHZ  
**RAM:** 160 GB | • 25 Windows 2008 R2 (2GB RAM and 1 vCPU). Each target desktop was running the vdbench client and vShield Endpoint driver.  
• DSVA-C260-01 (8GB RAM and 2 vCPU) |
| **Version:** ESXi 5.0.821926 | **Description:** This server was used to host the 25 target desktop virtual machines (Trend-NFS1-01 …Trend-NFS1-25) and Deep Security Virtual Appliance (DSVA) to provide security. | |
| **Name:** C260-02.vsepx.vdc | **Manufacturer:** Cisco Systems Inc.  
**Model:** C260-BASE-2646  
**CPU Cores:** 20 CPU x 2.393GHz  
**Processor Type:** Intel Xeon(R) CPU E72870 @2.40GHZ  
**RAM:** 160 GB | • 50 Windows 2008 R2 (2GB RAM and 1 vCPU). Each target desktop was running the vdbench client and vShield Endpoint driver.  
• DSVA-C260-02 (8GB RAM and 2 vCPU) |
| **Version:** ESXi 5.0.821926 | **Description:** This server was used to host the 50 target desktop virtual machines (Trend-NFS2-01 …Trend-NFS2-25 & Trend-NFS3-01…Trend-NFS3-25) and Deep Security Virtual Appliance (DSVA) to provide security. | |
| **Name:** C260-03.vsepx.vdc | **Manufacturer:** Cisco Systems Inc.  
**Model:** C260-BASE-2646  
**CPU Cores:** 20 CPU x 2.393GHz  
**Processor Type:** Intel Xeon(R) CPU E72870 @2.40GHZ  
**RAM:** 160 GB | • 50 Windows 2008 R2 (2GB RAM and 1 vCPU). Each target desktop was running the vdbench client and vShield Endpoint driver.  
• DSVA-C260-03 (8GB RAM and 2 vCPU) |
The vdbench tool was run for 12 hours to write a 45GB file on the target VM’s and each vdbench Master (total of 5) was configured against 25 VM’s to execute this workload. The Deep Security Virtual Appliances were configured to perform 1 concurrent scan and the scan cache expiry was set to 1 day for On-demand scans. Several scheduled tasks were created to perform the on-demand anti-malware scans across these test VM’s.

Validation Methodology

To verify Deep Security in the EMC VSPEX environment, the following tasks were carried out:

1. Installation and configuration of the Deep Security and its required components on a supported platform to conduct the testing. This task include the installation and configuration of these components:
   - MS SQL or Oracle DB Server
   - Deep Security Manager
   - Deep Security Relay
   - VMware vShield Manager
   - Deep Security Virtual Appliance
   - VMware vShield Endpoint
   - vdbench tool component

2. Activation of the Deep Security Virtual Appliance to provide protection to the guest VM’s.

3. Activation and assignment of a Security Profile to each guest VM’s enabled for agent-less anti-malware security.

4. On-demand AM scans execution for each VM.

5. Disk I/O workload generation using vdbench tool.

Note: The validation methodology relates only to the stated scope of this testing. Other aspects/modules of the Deep Security product are beyond the scope of this test.

Validation Results

In order for the validation methodology to be considered successful, the following tests need to be passed:

- Anti-Malware capabilities were enabled and properly detected the presence of a test malware sample.
Running the on-demand scan did not impact the IOPS and response time. The acceptable values for each parameter under consideration were: 25 IOPS for each VM (total rate expected was 25*125=3125) and a response time value less than 20 msec.

Note: The results provided in this document are intended for the purpose of comparing the specific configurations used in our lab environment. The results do not represent the maximum capabilities of any system, software, or storage used in our testing.

There were total 125 VM’s distributed across 3 ESX hosts as listed in the Table 1 above. All VM’s were successfully scanned and all test malware files were quarantined as shown below;

The graph below shows the expected results for “iorate” and “response time” was achieved while running an on-demand scan. The on-demand scan does not impact the overall performance goal of VSPEX architecture.
The test VM’s were cloned VM’s hence the scan duration benefited from the scan cache feature of Deep Security 9.0 release for the subsequent VM scans. Without the scan cache it took us approximately 15 minutes to scan 60,903 files as shown below.
Chapter 1: Introduction

Once the scan cache was built, the scan duration was under 3 minutes but varies per VM and it is expected e.g., in this case, it only took 50 seconds to complete the scan.
Chapter 2: Hardware & Software

This chapter presents the following topics:

Recommended Hardware ............................................................... 18
Software Recommendations ......................................................... 20
Chapter 2: Hardware & Software

Recommended Hardware

* Please note that these are not the minimum system requirements for this product.

<table>
<thead>
<tr>
<th>Component</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deep Security Manager (Windows)</td>
<td>RAM 4GB - 8GB (depending on number of agents)</td>
</tr>
<tr>
<td></td>
<td>Disk Space 5GB recommended-must be on an NTFS partition</td>
</tr>
<tr>
<td></td>
<td>CPU 64 bit Intel Xeon with at least two logical 3.0 GHz CPUs or equivalent</td>
</tr>
<tr>
<td>Deep Security Manager (Linux)</td>
<td>RAM 8GB</td>
</tr>
<tr>
<td></td>
<td>Disk Space 4GB</td>
</tr>
<tr>
<td></td>
<td>CPU 64 bit Intel Xeon with at least two logical 3.0 GHz CPUs or equivalent</td>
</tr>
<tr>
<td>Deep Security Relay</td>
<td>RAM 512 MB</td>
</tr>
<tr>
<td></td>
<td>Disk Space 200 MB</td>
</tr>
<tr>
<td></td>
<td>CPU 300MHz Intel Pentium or equivalent</td>
</tr>
<tr>
<td>Deep Security Agent</td>
<td>RAM 512 MB</td>
</tr>
<tr>
<td></td>
<td>Disk Space 200 MB</td>
</tr>
<tr>
<td></td>
<td>CPU 300MHz Intel Pentium or equivalent</td>
</tr>
<tr>
<td>Deep Security Virtual Appliance</td>
<td>RAM 1 GB (for up to 16 VMs), 4GB (for 33-64 VMs)</td>
</tr>
<tr>
<td></td>
<td>Disk Space 200GB</td>
</tr>
<tr>
<td></td>
<td>CPU 64 bit, Intel-VT present and enabled in BIOS</td>
</tr>
</tbody>
</table>

Table 2 – Hardware Requirements for Deep Security
### Component

<table>
<thead>
<tr>
<th></th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Smart Protection Server (optional)</strong></td>
<td></td>
</tr>
<tr>
<td>RAM</td>
<td>2 GB RAM</td>
</tr>
<tr>
<td>Disk Space</td>
<td>20 GB (For over 10,000 clients, add 5GB for every 5000)</td>
</tr>
<tr>
<td>CPU</td>
<td>Dual 2.0 GHz Intel Core2Duo 64-bit processor supporting Intel Virtualization Technology or equivalent</td>
</tr>
<tr>
<td><strong>Database</strong></td>
<td></td>
</tr>
<tr>
<td>RAM</td>
<td>4 GB or more</td>
</tr>
<tr>
<td>Disk Space</td>
<td>20 GB or more</td>
</tr>
<tr>
<td>CPU</td>
<td>Dual 2.4 GHz processor</td>
</tr>
</tbody>
</table>

*NOTE: We recommend that the database server be installed on a separate machine. Database space should be pre-allocated to avoid autogrowth. Making 20GB available is sufficient for most deployments. The per host storage varies widely but is mostly based on the number of events being generated, and the event purging settings. Therefore, it is better to plan ahead and assign more disk space for DB if possible.*
## Software Recommendations

* Please note that these are not the minimum system requirements for this product.

|------------------|-----------------------|------------------------------------|---------------------|---------------------------------|
| Windows          | • Microsoft Windows 2008 Server (64 bit)  
|                  | • Microsoft Windows 2003 Server SP2 (64 bit)  
|                  | Linux                                | • Microsoft Windows 7 (32- and 64-bit)  
|                  |                                      | • Microsoft Windows 2008 (32- and 64-bit)  
|                  |                                      | • Microsoft Windows 2008 R2 (64-bit)  
|                  |                                      | • Microsoft Windows Vista SP1 (32- and 64-bit)  
|                  |                                      | • Microsoft Windows 2003 SP2 (32- and 64-bit)  
|                  |                                      | • Microsoft Windows XP SP3 (32- and 64-bit)  
|                  | • Microsoft Windows 7 (64-bit)        |                                      | • VMware vCenter 5 and ESXi 5  
|                  | • Microsoft Windows 2008 SP2 (64-bit)  |                                      | • VMware Tools, VMware vShield Manager, VMware vShield Endpoint Security 5.0 (ESXi5 patch ESXi500-201109001 for vShield Endpoint Driver).  
|                  | • Microsoft Windows 2008 R2 (64-bit)  |                                      |                    |
|                  | • Microsoft Windows XP SP3 (64 bit)    | Linux                               |                    |
|                  |                                      | • RHEL 5 (64-bit)                    |                    |
|                  |                                      | • RHEL 6 (64-bit)                    |                    |
|                  |                                      | • VMware vCenter 5 and ESXi 5       |                    |

* Note: We do not support the Agent to be installed on Windows Server 2008 Core, Windows Server 2008 HyperV, Microsoft Cluster Servers and Microsoft Virtual Server 2005 R2 SP1 systems.
| **Database** | While Deep Security comes bundled with an Apache Derby database, it is not recommended for production use as it can only approximately sufficiently support 10 clients. Apache Derby is not supported for production use and Trend Micro reserves the right to ask the customer to reinstall against a supported database. Migration from Apache Derby to Microsoft is available on best effort basis. Migration from Apache Derby to Oracle is not supported. The recommendation is for customers to use Oracle 10g/11g or Microsoft SQL 2008 SP1 / 2005 SP2 or SP3. |
| **Installing 32-bit or 64-bit Deep Security Manager** | It is generally recommended that customers install the 64-bit version of the Deep Security Manager for production environments. 64-bit systems are not subjected to the memory limits which 32-bit systems are thus making 64-bit systems desired especially for larger deployments and for future expansion. Installing the 32-bit version of Deep Security Manager should only be considered if the system hardware is limited to running 32-bit mode. |
| **Installing Deep Security Manager Linux** | You can install Deep Security Manager on Linux via the Linux GUI or through silent install. For instructions, please refer to the Deep Security Getting Started and Installation Guide. |
Chapter 3: Product Configuration

This chapter presents the following topics:

- **Product Configuration** ................................................................. 23
- **GUI Configuration** ................................................................. 23
- **Dashboard** .............................................................................. 24
- **Alerts** ................................................................................. 24
- **Security Profiles** ................................................................. 24
- **Firewall** ............................................................................... 27
- **Deep Packet Inspection** .......................................................... 32
- **Integrity Monitoring** ............................................................... 34
- **Log Inspection** ..................................................................... 36
- **Deep Security Relay** ............................................................... 38
- **Shared** ................................................................................ 39
- **System Setting Recommendations** ........................................ 41
- **Scheduled and Event-Based Tasks** ........................................ 43
- **Anti-Malware** ....................................................................... 44
- **Web Reputation** ................................................................... 52
- **Recommendation Scans** ......................................................... 53
- **Assigning Rules and Security Profiles** ................................... 54
- **Database** .............................................................................. 54
- **Recommendations for Deep Security Virtual Appliance (DSVA)** .... 56
Product Configuration

There are many ways to architect a Deep Security solution – there is not one correct way of configuring Deep Security. Deep Security is a modular solution. This gives customers the flexibility to use only the features that best suit their needs. A user can start with one or two modules, and then expand their solution later as they grow or their needs mature.

This section does not cover specifics on how to configure each item specifically nor does it intend to provide a mandatory framework for customers to follow. This section aims to present suggested approaches and sample configurations that can be used as reference and/or templates to best suit your environment.

GUI Configuration

Below are the main configuration settings to take note of after installing Deep Security Manager.
Chapter 3: Product Configuration

Dashboard

We recommend that at least the following widgets are included and placed on the area best seen on the dashboard page:

a. Alert Status – to keep you informed on any critical items that may need immediate attention such as security updates and protection on computers getting offline.

b. Computer Status – gives you a good overview of agents’ status.

c. My Account Status – will show information about the user currently logged in. Deep Security Manager (DSM) is a powerful, centralized server that allows users to create and manage comprehensive security policies and track threats and preventive actions taken in response to them. It provides role-based access control (RBAC) and a web-based administrator console for flexible management access.

Alerts

Deep security has default alerts configured on the Alerts section. We recommend that these alerts remain enabled, as they are vital in monitoring events, malware detections, attacks or intrusions.

Security Profiles

"Interface Types" is a very useful feature that is use in conjunction with firewall or DPI rules. We use Interface Types when we need to assign firewall or DPI rules to specific interface on machine that has multiple interfaces.

By default when we assign a firewall or DPI rule, the rule is assigned to all interfaces on a machine. If there are some special rules for instance you want to apply only to the wireless network interface, and not affect the local area network, this is where Interface Types comes into play.

We configure Interface Types via Security Profiles → Interface Types
We can group interfaces into a maximum of 10 different groups. The ones normally used are LAN and Wi-Fi. We specify the group name and underneath the group name we specify all possible interface names that fall under this group, for instance the LAN group we can specify the following matches:

- Local Area Connection
- Local Area Connection.*

When we go to firewall or DPI rules, we can now assign rules to specific interface types. The rule will be applied only to Interface Names that match what we have defined in the LAN group.

When the Security Profile is assigned to host machine, the host machine where its interface name is “Local Area Connection” will now be mapped to the LAN interface type, instead of Global. This allows the rules to be applied only to specific interface.
When we are creating a Security Profile, it is a good idea to consider whether Interface Types can help us in terms of applying rules to specific interfaces we want to protect. Consider populating the Interface Type based on the different networks available to all potential Deep Security Agent protected machines.

Security profiles provide a logical way for replicating security settings to servers and desktops that share similar security requirements. We recommend that machines with similar settings, software installed, application, or function be grouped strategically when placing them in security profiles.

Note that the default profiles built in with Deep Security are meant to be examples and should not be used without prior configuration.

Using security profiles to assign Deep Security rules generally makes it easier to manage as compared to directly assigning rules to individual hosts. This way, you can make changes to the profile settings and testing it first prior to assigning it to the machines. Unlike assigning directly to hosts, there is no quick way (administrators will have to dig into each individual machine to check each setting) to remove any setting configured that may cause conflict or some programs not to run correctly.
Chapter 3: Product Configuration

Using security profiles will allow you to quickly unassign rules by simply taking out a machine from the profile or assigning it an entirely new profile. Administrators will also be able to duplicate profiles and can use these as baseline settings for succeeding profiles to be created.

Below are some recommended machine groupings to effectively take advantage of Security Profiles:

- By Operating System (e.g.: Windows 2008 Servers, Windows XP Machines, and Linux)
- By Server Function (e.g.: Mail Servers, Web Servers, User Laptops, and Point of Sale Systems)
- By Application installed/version (e.g. OfficeScan Servers, Oracle 10 Database Servers, MS SQL 2005 Servers)

Grouping machines properly is key to managing recommendation scans effectively. Recommendation scans provide administrators with a list of areas on a host that need protection. It creates a guide for how to harden a host, based on Deep Security's current ability to protect.

When a Recommendation scan is performed on an individual member of a profile, the recommendations for that particular agent (DSA) will be seen on the profile as well. Accepting (applying) the recommendations at the profile level would apply the rules to all members of the profile. The advantage to this method is ease of maintenance. The disadvantage, however, is the possibility of assigning rules to profile members that do not actually need them.

This is the reason why it is recommended that machines are grouped accordingly if users don't want to see the vulnerability being triggered for machines that should not be affected.

Firewall

Firewall configuration and administration must be performed carefully. There is not one set of rules that will fit all environments and needs. This guide aims to give users best practice tips and recommendations that we hope can be used as reference and serve as guidelines when building your own rules.

It is always recommended that Deep Security be set to run in “In-Line Mode”. When operating Inline, the live packet stream passes through the network engine. Stateful tables are maintained, Firewall Rules are applied and traffic normalization is carried out so that DPI Rules can be applied to payload content.
Chapter 3: Product Configuration

Should there be a need to test the configuration and rules before pushing them out to the production environment, it is suggested that "In-line mode" with "detect" settings are used. This way, the real world process of analyzing the traffic takes place without having to perform any action such as blocking/denying of packets.

Running Deep Security in Tap Mode is generally not recommended and is not the best practice to perform tests or evaluate Deep Security. Tap mode does not actually block traffic, so a lot of traffic that would have otherwise been blocked would continue (e.g., responses to traffic that would have been dropped), so the traffic patterns in this mode are not representative of how the network will behave once the administrator switches to Inline mode.

Traffic analysis takes place with both modes. However, Tap mode only performs analysis on a copy of the incoming packet. Therefore it is not able to block traffic. Only Inline mode provides security functionality.

General list of firewall best practices

• Allow rules explicitly allow traffic that matches it to pass, in addition, it implicitly denies everything else not defined. Be careful when creating allow rules without defining related rules correctly as doing so can cause one to block all traffic apart from what the allow rule is created for.

• If one relies on dynamic ARP include an appropriate rule to allow ARP.

• When using Ethernet, ARP forms the basis of the TCP/IP stack. ARP facilities provide translation from IP addresses to Ethernet addresses, which are essential for sending packets to other systems on the local LAN segment. Without this conversion, there can be no other form of peer-to-peer IP communication.

It is thus very important that Deep Security Manager does not configure a Deep Security Agent to drop ARP packets, unless that is actually desired (configuration uses static ARP tables). To ensure this please follow these guidelines:

1) Enable the Trend Micro-provided ARP force allow rule.

2) Do not prevent broadcast ARP packets.
Chapter 3: Product Configuration

- Stateful Configurations should be used when the Firewall is ON.
- If the UDP stateful option is enabled a Force Allow must be used when running UDP servers (e.g. DHCP).
- If there is not a DNS or WINS server configured for the Deep Security Agents, a Force Allow, Incoming UDP Ports 137 rule may be required for NetBIOS.
- It helps to know the different implications firewall rule actions do when creating your rules. Below are brief descriptions of what each action does:
  - Allow – this action explicitly allows traffic that matches the rule to pass and implicitly denies everything else not defined.
  - Bypass – this allows traffic to bypass both firewall and DPI analysis. Use this setting only for media-intensive protocols. Only the port, direction and protocol can be set with this action.
  - Deny – this action explicitly blocks traffic that matches the rule.
  - Force allow – this forcibly allows traffic that would otherwise be denied by other rules. This action type must be used for UDP and ICMP traffic.
  - Log only – traffic will be only be logged. No other action will be taken.

With many laptops now capable of connecting to both the wired and wireless networks, users need to be aware of the problems that can result from this scenario.

The common problem is a “network bridge” configured between the wired and wireless network. You risk forwarding the internal traffic externally and potentially expose internal hosts to external attacks.

Deep Security allows administrators to configure a set of firewall rules for these types of users to prevent them from creating a “network bridge”.

b. **Create a security profile for wireless laptops**
   - Start with a fresh new profile and choose not to base the profile on an existing Computer’s current configuration. This will allow you to manage the rules and configuration easily without worrying about any pre-existing rules/configuration in use.

c. **Configure Interface Isolation**
   - Interface Isolation allows you to force a Host to use only one interface at any one time. This feature was designed to enable you prevent...
attacker from bridging across two interfaces.

To do so, set the Enable Interface Isolation option and enter string patterns that will match the names of the interfaces on a Computer (in order of priority) and then set the Limit to one active interface per pattern option.

It is not recommended that this be enabled at the global level, so make sure it is enabled through the Security Profile that has just been created. Set the global settings to not use Isolated Interfaces and then override the setting on the Security Profile or the Host.

Note: Interface patterns accept wildcards such as (*) as well as regex expressions such as alternation, or the regex equivalent of "or" (e.g. "Wireless.*|Local.*" will match any interface starting with Wireless OR Local)

d. **Create Firewall Rules**

Once Interface Isolation is in place, connections via the secondary entry (i.e. Wireless Network Connections) should be dropped by Deep Security. Administrators can proceed with creating other custom firewall rules for connections coming in through the Local Area Connection. In addition, one can also configure certain traffic from the restricted interface by creating additional firewall rules using contexts.
A context that uses the Interface Isolation option will apply to interfaces that have been disabled. This is useful for custom Allow and Force Allow rules to allow certain traffic to pass through based on needs.

e. **Configure DPI, Integrity Monitoring and Log Inspection rules as needed.** Interface isolation via the Firewall feature of Deep Security should be enough to prevent network bridging. However, additional security can be further assigned to the profile by configuring DPI rules, Integrity Monitoring and Log Inspection.

**Deep Packet Inspection**

Deep Packet Inspection (DPI) rules should never be modified at the global level as there is no way to restore the default settings once changed. Should there be a need to further configure or modify such rules, it’s suggested this be done at the profile level. (i.e., modify DPI rules needed within the Security Profile). This way, the default master copy of the rules is kept in the global level and can be used as a reference should there be a need to revert back changes.
Double-clicking a DPI rule in Security Profile view or Computers view is the same as editing it in the global level. To edit a DPI rule in the Security Profile or Computer level, open the Security Profile or Computer then right-click on the rule. Select Properties (For This Computer) or Properties (For this Security Profile).

**General Deep Packet Inspection Rules Recommendations**

- If a specific rule is causing false positives, place that rule in Detect Only mode or unassign it.
- Any rule, requiring configuration should be assigned in Detect Only mode until the rule can be configured for that computer.
- For new deployments, we recommend setting DPI rules to Inline Detect mode so it will be easy to identify any false positives.
- Set DPI rules to only log dropped packets to avoid using up too much disk space.
- Only select the Always Include Packet Data option (on the Filter's property sheet) when interested in examining the source of attacks. Otherwise leaving packet data logging on will result in much larger log sizes.
- Application Types under DPI rules should be checked prior to use.
  
  Ex. Trend Micro OfficeScan - Is inspecting incoming ports 8080, 4343 and 46485
  
  - OSCE ports can be changed, specially the random 5 digit client port. So make sure rules such as these are re-configured to match your settings before assigning.

**Recommendations for Cross Site Scripting and Generic SQL Injection rules**

Two of the most common application-layer attacks are SQL injection and cross-site scripting (XSS). Cross Site Scripting and SQL Injection rules are configured to catch majority of attacks by default, the best approach to customizing these rules should be to change the drop score for specific resources that are causing false positives and not the global drop score.

- Both these rules are smart filters and need custom configuration for web servers.
- Customers who have output from Web Application Vulnerability Scanners should leverage that information when applying protection (i.e. if username field on login.asp page is vulnerable to SQL Injection, ensure the SQL Injection rule is configured monitor that parameter with a low threshold to drop on).
Chapter 3: Product Configuration

Recommendations for SSL Configuration

Deep Security Manager supports DPI analysis of SSL traffic and is able to filter SSL encrypted data streams. If this feature is used, it is recommended to disable the inspection of HTTP responses to avoid any performance degradation.

All web attacks that we protect against are included in the HTTP request and not the HTTP response, disabling inspection on responses will improve performance.

- To configure this, go to Deep Packet Inspection > DPI Rules > Web Application Protection.
- Right click on "Web Server Common" application type and choose "Application Type Properties"
- Go to the Configuration tab and uncheck the option called "Monitor Responses from Web Server"
- Update the changes to the host/profile.

Integrity Monitoring

Monitoring the operating system and application files and directories is an excellent way to ensure the integrity of the data on your server. Unexpected changes to these files can be a good indicator that something suspicious has occurred and should be investigated.

It is good to note that rules created for Integrity Monitoring should be as specific as possible to improve performance, avoid conflicts and false positives (Example: Don’t try to create a rule that monitors the entire hard drive)
Integrity Monitoring can be used to monitor files and registries. Malware normally infects a system by modifying certain registry keys and various system files. The default Deep Security rules allow you to monitor the integrity of a machine by monitoring the things most commonly changed by malware in an infected system. Here are a few example rules that are applicable for all types of situation in Windows platform:

- Rule 1002773 – Microsoft Windows – ‘Hosts’ file modified
- Rule 1002776 – Microsoft Windows – ‘All Users’ Startup programs modified
- Rule 1002778 – Microsoft Windows – System dll or exe file modified

Unless new software or a security patch is installed, there is no clear reason any of these files should be modified. When such an event is raised, the administrator can check what's happening on the machine to make sure the machine is not compromised.

It is also possible to create custom rules to monitor specific threats, when a user knows the behavior of a particular virus he is trying to contain in your environment. He can create a special monitoring rule that checks for certain registry keys or files created by the virus. This can help him determine if the spread of the virus is being contained or not.

Integrity Monitoring helps one detect changes made on the system, but it will not remove or prevent the change from taking place. It is a passive monitoring tool that complements anti-malware and intrusion prevention software.

Agentless Integrity Monitoring feature is introduced in Deep Security. It provides agentless Integrity Monitoring for virtual machines implemented by Deep Security Virtual Appliance (DSVA). As same as agentless Anti-Malware feature, vShield Endpoint must be configured to use agentless Integrity Monitoring. Please refer to agentless Anti-Malware section for configuration details.

Following limitations for agentless Integrity Monitoring in current version should be noted.

- Only files can be monitored.
- Manual or Scheduled Integrity Scan is available. Real Time check is not supported.
Log Inspection

Events from the Windows event log and other application specific logs are a great source of information about the health of your server and applications. Have an automated solution to inspect these log files for suspicious events and alert is great functionality to include in your defense in depth strategy.

Log Inspection tracks logs and events in the Operating System Event Log, using an integrated OSSEC Log Inspection Engine. Based on rules defined within the Log Inspection Filter, you can track changes detected by Log Inspection, and send alerts if necessary.

This feature is especially useful in having easier access to important events in log files monitored without having to manually trace through it.

There are a number of available log inspection rules by default that administrators can use to monitor activity on your mail server, including spam activity.

One of these rules is designed to monitor activity on Sendmail servers.

When a recommendation scan is ran against the host with Sendmail, this particular rule should be listed as one of the recommended rules. Enable the rule, along with the dependency rule called Default Rules Configuration.

Log inspection rules need to be properly configured to work correctly. The first thing to change and check is the actual log files to monitor. In this case, that’s the Sendmail log, or the maillog.
After defining the rule location and type, configure the event for detected SPAM messages. This rule is specifically made to monitor spam activity on the server, so for this scenario, we are lowering down the severity level for the other events. Detected Spam Messages and Multiple Spam messages have been set to Critical for this example.

![Image showing rule settings]

Unnecessary alerts for an allowable number of spam messages are not desired, so make sure the Frequency and Time Frame fields are also tweaked correctly.

After these have been modified, switch to the Options section to configure DSM to send alerts when the minimum severity is reached.

![Image showing options settings]

There are 2 more options that can be configured for Log Inspection and can be found in the System Settings section.

*Send Agent/Appliance events to syslog when they equal or exceed the following severity level:* should normally be changed when a syslog server is used. This setting determines which Events triggered by those rules get sent to the syslog server (if syslog is enabled.)

*Store events at the Agent/Appliance for later retrieval by DSM when they equal or exceed the following severity level:* This setting determines which Log Inspection Events are kept in the database and displayed on the Log Inspection Events screen. Custom rules can be made to monitor logs that are not in the built-in set of rules.
Chapter 3: Product Configuration

Deep Security Relay

The Deep Security Relay is a server which relays security updates from the Trend Micro global ActiveUpdate server to the Deep Security system. At least one Relay is required in your Deep Security environment. Multiple Relays can be installed for redundancy or bandwidth optimization.

Current setup of Relays and Relay Groups are shown at System > Updates > Relays.

Relay Groups can be configured at System > System Settings > Updates > View Relay Groups.

Each Agent/Appliance is configured to have one Relay Group assigned at Computer Details screen.
Chapter 3: Product Configuration

Setup Relay Group for redundancy

If one Relay Group has multiple Relay members, each Relay acts as a backup for the others. Each Agent/Appliance assigned to a Relay Group automatically chooses a member Relay at random to connect to. If one of the Relays in a Group fails, the other Relays will continue to serve updates to the Agents/Appliances.

Setup Relay Group for bandwidth optimization

If you have multiple sites, that is geographic region or office, it is recommended to setup Relay Groups for each site.

1. Install Relay at each site and activate it.
2. Create Relay Groups for each site (Such as “East Relay Group” and “West Relay Group”).
3. Add Relay to corresponding Relay Groups. (add Relays at east office to “East Relay Group”, ones at west office to “West Relay Group”)
4. Configure Agent/Appliance at each site to use each site Relay Group. (Agent/Appliance at East office to use “East Relay Group”, ones at West office to “West Relay Group”)

Shared IP Lists

Properly segregating the network allows one to maximize the potential how security rules can be configured to help protect the network. To make it easier to build firewall rules and to avoid constantly typing in individual IP Addresses, one can group IP Addresses using IP Lists. The IP Lists can be re-used on various configuration items in the Deep Security Manager.
Chapter 3: Product Configuration

Updating the IP Lists automatically updates security rules using this list. This allows the administrator to update multiple rules immediately and can help avoid inconsistency among rules.

**MAC Lists**

Same as with IP Addresses, one can also group MAC Addresses under MAC Lists. This avoids unnecessary re-typing of MAC Addresses when they need to be added to multiple rules.

Updating the MAC Lists automatically updates security rules using this list. This allows the administrator to update multiple rules immediately and can help avoid inconsistency among rules.

**Port Lists**

The Port Lists by default contain comprehensive information on ports used by different applications. Before one adds custom ports in here, check first if the application is already listed and if the port is not there, continue to add the port into the said application. Otherwise, consider adding a new custom Port List entry with a short and descriptive name.

**Contexts**

Context rules allow administrators to create firewall rules that only apply in specific circumstances. Use context to assign rules depending on the location of the machine in relation with its Domain Controller. Context can also be created to apply to a restricted interface by using the apply to restricted interface check box.

**Schedules**

The schedules here do not have anything to do with updates and deployment. The schedules defined here are used for when certain rules should be enabled only on a limited basis. (e.g. daily: Weekdays from 8am to 4pm, nightly: Everyday from 10pm to 2am or weekends: Saturday and Sunday 8am to 4pm)

**Directory Lists**

Directory lists allow administrators to create lists of directories used for anti-malware configurations. This avoids unnecessary re-typing of directories when they need to be added to multiple rules.

Updating the Directory Lists automatically updates security rules using this list. This allows the administrator to update multiple rules immediately and can help avoid inconsistency among rules.

For recommended lists of directories for exclusion, refer to section 8.4.

**File Lists**

File Lists is used for anti-malware configuration. File lists can be used in excluding specific files and specific process images from anti-malware scanning.

Updating the File Lists automatically updates security rules using this list. This allows the administrator to update multiple rules immediately and can help avoid inconsistency among rules.
Chapter 3: Product Configuration

For recommended lists of files for exclusion, refer to section 8.4.

**File Extension Lists**

Same with Directory Lists, File Extension Lists is used for anti-malware configuration. File Extension Lists can be used to define which file extensions should be scanned and can also be used in specifying exclusions.

Updating the File Extension Lists automatically updates security rules using this list. This allows the administrator to update multiple rules immediately and can help avoid inconsistency among rules.

**System Setting Recommendations**

- **Computers > Communication Direction**

![System Settings](image)

This option can be set at the global, security profile and host level. We recommend selecting the default value of “Bidirectional” method, which is used in most production deployments.

Manager Initiated should typically only be used for DMZ hosts that can’t reach the Manager in the Datacenter.

Agent Initiated method is good for environments where the Agent is behind a firewall such as mobile workstations.

- **Computers > Automatically Update**

![Automatically Update](image)

Computers We recommend disabling this option and instead, use scheduled tasks to update computers or to update hosts manually.

- **Computers > Agent Self Protection**
Chapter 3: Product Configuration

We recommend to enable and set password for local override of Agent self protection. By default Agent self protection is enabled to block unauthorized change for Agent. However it can be disabled at Agent side by “dsa_control /H 0” command or reset Agent by “dsa_control /r” command. By configuring password, it requires this password to disable the protection at Agent side or reset Agent. (“dsa_control /H 0/p <password>” or “dsa_control /r/p <password>”)

- Scan > Scanning for Recommendations

This setting is disabled by default and should be left off. Setting ongoing scans to automatically start will mean administrators have no control over when it will occur, best practice is to create a new scheduled task with type “Scan Computers for Recommendations” to take place once a week instead.

It’s strongly recommend against deploying program updates automatically. Make sure ample machines have been tested on new product versions before they are rolled out to the whole enterprise.

Also, automatic update of rule updates is the default but not recommended in production environments as the administrator loses control over when updates occur. Manual updates allow more control for an administrator to follow their existing change control process. Scheduled Tasks can be used to update hosts during maintenance windows, off hours, etc.

To monitor when hosts were last updated and when update was requested, administrators can use the information on the Computer Properties screen.

Recommendations for Quarantined Files

With agentless Anti-Malware feature, quarantined files are stored in the Deep Security Virtual Appliance (DSVA). Therefore, always make sure that the DSVA disk is not full. The default quarantined file settings are the recommended settings.

Trend Micro Confidential. Non-disclosure Agreement is required for non-Trend Micro employees to view this document
Quarantined files will be automatically deleted from a Virtual Appliance under the following circumstances:

- If a virtual machine (VM) undergoes vMotion, quarantined files associated with that VM will be deleted from the Virtual Appliance.
- If a VM is deactivated from the Deep Security Manager, quarantined files associated with that VM will be deleted from the Virtual Appliance.
- If a Virtual Appliance is deactivated from the Deep Security Manager, all the quarantined files stored on that Virtual Appliance will be deleted.
- If a Virtual Appliance is deleted from the vCenter, all the quarantined files stored on that Virtual Appliance will also be deleted.

Scheduled and Event-Based Tasks

Tasks can be configured to automate certain common tasks by schedule or event.

We recommend configuring the following scheduled tasks:

- Component Update (Frequency: Once Daily)
- Check for New Software (Frequency: Once every Week)
  
  Note: Check for New Software only checks if there is a new version available in Trend Micro Download Center. The software is not automatically downloaded. If there is a new software available, it has to be downloaded manually then imported to the Deep Security Manager via the console (System > Updates > Import Software).
- Scan Computers for Malware (Frequency: Once every Week)
- Scan Computers for Recommendations (Frequency: Once every Week)
  
  Note: When scheduling recommendation scans, it is best practice to set the task by group (i.e. per security profile, or for a group of computers, no more than 1,000 hosts per group) and spread it in different days.

E.g. Database server scans are scheduled every Monday; Mail server scans are scheduled every Tuesday, and so forth.
Chapter 3: Product Configuration

Recommendation scans can be CPU intensive on the DSM (Manager) so setting different schedules per group will help avoid any performance issues.

Schedule recommendation scans more frequently for systems that change often.

- Update Computers (Frequency: Once every week)
- Discover Computers (Frequency: Once Daily)
- Backup (Frequency: Once Every Week during off hours)

**Recommended Event-Based Tasks to Set Up**

If you have Deep Security Virtual Appliance to protect virtual machines, we recommend configuring the following event-based tasks:

- **Computer Created (by System) – Activate Computer and Assign Security Profile**

This will let you keep baseline security policy for newly created virtual machines.

**Anti-Malware**

Anti-Malware is a new feature introduced in Deep Security 7.5 (agentless) and 8.0 (agent). Anti-malware functionality provides agentless anti-malware protection for virtual machines implemented by the Deep Security Virtual Appliance (DSVA), and agent anti-malware protection for physical and virtual servers implemented by Deep Security Agent (DSA).

This DSVA/DSA version can:

- Perform manual, schedule, and real-time scanning
- Support different scanning configurations for each scan type
- Use conventional or Smart scanning

**Configuring Smart Scan**

By default, Smart Protection is turned off for DSVA, on for DSA. This is the suggested setting when using Anti-malware protection for servers. This setting will optimize the performance of Anti-Malware Protection in the virtual environment. For Virtual Desktop (VDI) environments, to achieve the more timely protection against threats that Smart Protection provides, this setting should be turned on. Smart Protection Server for File Reputation Service needs to be configured.

**Recommended Scan Settings**

It is suggested to create duplicates of the default scan configurations made available on the console. This will help administrators retain the default scan configurations for future reference and use them as templates for new configurations.
Chapter 3: Product Configuration

a. **Real Time Scan Configuration Recommendations**:  
   Scan Settings: All Folders  
   Files to scan: All files  
   Note: Selecting “File types scanned by Intelliscan” slightly improves performance by only scanning types known to potentially carry malicious code. Using this setting also allows you to utilize True File Type scanning.  
   Exclusions: Refer to section 8.4 (Recommended Scan Exclusion list)  
   **Actions**  
   Upon Detection: Use action determined by Active Action  
   Possible Malware: Pass  
   Note: Selecting “Quarantine” is also suggested so a copy of the possible malware detection can be sent out to Trend Micro for further evaluation. Using this setting will move and quarantine the detected file and should be used with caution if false positive detections are frequent. Quarantined files may also be deleted in certain circumstances (refer to section 5.1.9.3 for details). For cases where losing quarantined files is unacceptable, Deny Access action is recommended.  
   **Options**  
   Enable Spyware/Grayware Scan: On  
   Scan Compressed files: On  
   Maximum size of individual extracted files: 30MB  
   Maximum levels of compression from which to extract files: 2  
   Scan Embedded Microsoft Office Objects: On  
   Scan for exploit code in Microsoft Office Objects: On  
   OLE Layers to scan: 15  
   Enable Intellitrap: On  
   Enable Network Directory Scan: Off  
   Scan files when: Read/Write  
   Note: Intellitrap detects/removes malware on compressed files packed as executable files. Turn off this setting on special cases where users regularly exchange real-time compressed executable files.  
   Alert when this Anti-Malware configuration logs an event: On  

b. **Scheduled Scan Configuration Recommendations**  
   Scan Settings: All Folders  
   Files to scan: Intelliscan
Chapter 3: Product Configuration

Exclusions: Refer to section 8.4 (Recommended Scan Exclusion list)

**Actions**

Upon Detection: Use action determined by Active Action
Possible Malware: Pass

Note: Selecting “Quarantine” is also suggested so a copy of the possible malware detection can be sent out to Trend Micro for further evaluation. Using this setting will move and quarantine the detected file and should be used with caution if false positive detections are frequent. Quarantined files may also be deleted in certain circumstances (refer to section 5.1.9.3 for details). For cases where losing quarantined files is unacceptable, Deny Access action is recommended.

**Options**

Enable Spyware/Grayware Scan: On
Scan Compressed files: On
Maximum size of individual extracted files: 60MB
Maximum levels of compression from which to extract files: 2
Scan Embedded Microsoft Office Objects: On
Scan for exploit code in Microsoft Office Objects: On
OLE Layers to scan: 15
CPU Usage (Agent only): Medium

c. **Manual Scan Configuration Recommendations:**

Scan Settings: All Folders
Files to scan: All files
Exclusions: Refer to section 8.4 (Recommended Scan Exclusion list)

**Actions**

Upon Detection: Use action determined by Active Action
Possible Malware: Pass

Note: Selecting “Quarantine” is also suggested so a copy of the possible malware detection can be sent out to Trend Micro for further evaluation. Using this setting will move and quarantine the detected file and should be used with caution if false positive detections are frequent. Quarantined files may also be deleted in certain circumstances (refer to section 5.1.9.3 for details). For cases where losing quarantined files is unacceptable, Deny Access action is recommended.

Trend Micro Confidential. Non-disclosure Agreement is required for non-Trend Micro employees to view this document
Chapter 3: Product Configuration

**Options**

Enable Spyware/Grayware Scan: On  
Scan Compressed files: On  
Maximum size of individual extracted files: 60MB  
Maximum levels of compression from which to extract files: 2  
Scan Embedded Microsoft Office Objects: On  
Scan for exploit code in Microsoft Office Objects: On  
OLE Layers to scan: 15  
CPU Usage (Agent only): Medium

Agentless Anti-Malware (DSVA)  
In order for agentless anti-malware feature to work, the following software and licenses are required:

**VMware Related:**

- vCenter v5.0 *
- ESXi v5.0 with ESX 5.0 Patch 01(ESXi500-201109001) or later *
- vShield Manager v5.0 including vShield Endpoint v5.0 *
- vShield Endpoint v5.0 Thin Agent included in VMware Tools

**Trend Micro Related:**

- Deep Security Manager (DSM) v8.0 or later *
- Deep Security Virtual Appliance (DSVA) v8.0 or later  
- Deep Security Filter Driver (Filter Driver) v8.0 or later

* License Required

After installing all the requirements, the following items need to be checked in order for anti-malware feature to work:

1. vCenter Server is configured and registered in vShield Manager.
2. Inventory is retrieved from vCenter

3. vShield Endpoint status for ESX is installed

4. vShield Endpoint Thin Agent in VMware Tools is installed. You need to choose “Custom” setup and select VMCI Driver -> vShield Drivers
5. After installing vShield Endpoint Thin Agent, check driver status in guest OS (vmci and vsepflt)

Note: In vShield Endpoint Thin Agent 1.0 Update 2 and above, these drivers are named vsepflt and vsepscs.

6. Check ESX status in DSM console.

7. Check DSVA status in DSM console.

8. Check guest OS status in DSM console. Aside from checking if Anti-Malware status is On, take note of the green or blue icon as well. The icon will only turn green if a security profile with Anti-Malware set to On.
9. Check if anti-malware is working by downloading eicar test file. Alert and event should be generated in the DSM console and download should fail.

10. Always make sure that anti-malware components are always up-to-date. Creating a scheduled task to download component updates daily is highly recommended.
Chapter 3: Product Configuration

If you deploy Agent Anti-Malware into vSphere environment, you should care for "Scan Storm" caused by running multiple on-demand scans at virtual machines on a single ESXi server at the same time.

Deep Security has a feature to avoid Scan Storm:

1. Open Manager properties from System > System Information > Managers...

2. Select “Limited Agent Disk & Network Usage” and click OK.

This configuration limits maximum concurrent on-demand scans at one ESXi server to 3.

For Anti-Malware (and Integrity Monitoring) features, the coordinated protection by both DSA and DSVA does not work automatically like Firewall and DPI. If you activate DSA, Anti-Malware protection by DSVA is
disabled. To switch to DSVA Anti-Malware protection, you need to deactivate DSA manually.

Web Reputation

The Web Reputation module blocks web pages based on their reputation ratings by querying the Trend Micro Smart Protection Network servers. Web Reputation is available for both Agent(DSA) and Agentless(DSVA).

The default security level “Medium” is suitable for most users. However if you want further security, you can adjust it to “High” level.

If you have specific web pages to be allowed or blocked, they can be configured at [Exceptions] tab.

By default, Web Reputation is enabled to port 80 and 8080. If you have HTTP proxy server using other ports, you need to configure it at [Advanced] tab.

1. Create a new Port List from Shared > Port Lists including your proxy port. (Such as 3128)
2. Choose the created Port List at Web Reputation > Advanced > Ports.
Chapter 3: Product Configuration

Recommendation Scans

The recommendation engine is a framework that exists within Deep Security Manager, which allows the system to suggest and automatically assign security configuration. The goal is to make configuration of hosts easier and only assign security required to protect that host.

- Recommended best practice is to set weekly recommendation scans.
- Recommendation Scans can heavily tax the DSM so scanning too frequently can result in poor DSM performance. Hence, systems that don’t change often (servers) can be scanned less frequently.
- Systems that lack control over when changes occur (workstations) should be scanned more frequently.
- Scans should be performed after major changes to the computer to determine any additional required protection.

Automatic Assignment of DPI rules for Single Host

By default the automatic assignment of DPI rules is turned off. We do not recommend enabling this option on the host level except under special circumstances where the host machine is on its own and cannot be associated with other machines in a group. When this rule is enabled, DPI rules will automatically be enabled on the host machine when the rule is found to be applicable or a matching application is found on the machine related to the DPI rule.
Chapter 3: Product Configuration

Assigning Rules and Security Profiles

We do not recommend assigning Firewall or DPI rules directly to individual hosts. After a series of changes made to individual machines, it will become impossible to track which configuration machines have. Not only is this confusing, but it makes it impossible for machines to have a consistent set of rules and configuration.

Security Profiles should be used as much as possible to assign rules to machines or groups.

It is important to group machines that have common functionalities together. For example, SQL servers should be under its own group and Web Servers under its own separate group.

For automatic assignment of DPI rules, under “Scan for Recommendation” → “Automatic Assignment of DPI rules”, it is recommended that this be disabled to give administrators better control over assigning and unassigning recommended DPI rules.

Note: Refer to section 5.1.3.2 for more details on grouping machines.

Database

Deep Security Manager must be able to maintain a database PING time of less than 2 million nanoseconds. Any figure higher than this can cause unpredictable problems. We recommend that the database time skew be kept as close to 0 as possible. Although not 100% necessary, keeping the database time in sync would help prevent confusion in reading logs and reports, this is also especially important for multi-node environments.
The DSM System Information screen provides information about connection speed and time skew on the database.

For this reason, the DSM must be co-located on the same network as its database, ideally with a 1GB LAN connection. Connections over WAN are discouraged.

By default, database communication is not encrypted. However, if DSM uses a remote database, and the SQL server is protected by a DSA, the contents of DPI rules may cause false alarms when the DSM saves these rules to its database.

The following workarounds are available to avoid this condition:

**Option 1:** Create a bypass firewall rule for traffic between the database and DSM servers. In this scenario, a static IP address for the DSM would be preferred.

**Option 2:** Enable encryption for the database channel. To accomplish this, add the following line to the dsm.properties file:

For **MS SQL** - Add the following line to dsm.properties:

```
database.SqlServer.ssl=require
```

For **Oracle** - Add the following lines to dsm.properties:

```
database.Oracle.oracle.net.encryption_types_client=(3DES168)
database.Oracle.oracle.net.encryption_client=REQUIRED
database.Oracle.oracle.net.crypto_checksum_types_client=(MD5)
database.Oracle.oracle.net.crypto_checksum_client=REQUIRED
```
Chapter 3: Product Configuration

Recommendations for Deep Security Virtual Appliance (DSVA)

The Virtual Appliance uses VMware's VMsafe-NET API to intercept network traffic at the hypervisor. Anti-malware feature which is added in this version also uses the new vShield Endpoint API to detect malware in the files or I/O events that were intercepted by the vShield Endpoint driver. Because of this, when installing the driver, the ESX server must be put into maintenance mode (with the running VMs either vMotioned to another ESX server or all turned off).

- Make sure to schedule the deployment of DSVA carefully because of these requirements.
- It is best practice to download the filter driver and DSVA installer packages onto Deep Security Manager prior to deploying DSVA and adding the vCenter server onto DSM.
- Ensure that the ESX server is able to connect to the DSM hostname at port 4119. There will be issues installing the driver and DSVA if ESX cannot do so.
- When preparing the ESX box, allow the Deep Security Manager to automatically bring the server into and out of maintenance mode.

- Default password for the deployed DSVA image is “dsva” and we recommend users to change this after the install. To do so, press <F2> and select the option “Configure Password” on the console.
## Chapter 3: Product Configuration

### System Configuration

<table>
<thead>
<tr>
<th>System Information</th>
<th>Configure Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Password</td>
<td>Password set</td>
</tr>
<tr>
<td>Configure Management Network</td>
<td>This will change the password</td>
</tr>
<tr>
<td>Configure Time Zone</td>
<td></td>
</tr>
</tbody>
</table>

### Virtual Agents

### Reset Appliance

### Reboot System

### Change Password

**Old Password:**  
**New Password:**  
**Confirm:**  

*Enter* or *ESC* to Exit
Chapter 4: Performance Tuning

This chapter presents the following topic:

- Disable Stateful Logging of UDP Packets (Especially in a Windows Environment) ................................................................. 59
- Performance Profiles ........................................................................................................................................................................... 59
- Log Retention Strategy ...................................................................................................................................................................... 59
- Database Indexing ............................................................................................................................................................................. 60
Disable Stateful Logging of UDP Packets
(Especially in a Windows Environment)

The network creates a lot of noise because of stateful inspection being enabled which results in the creation of a lot of events that can be largely ignored from a management perspective. So it is recommended that the stateful logging of UDP packets be turned off.

Note: ICMP Stateful logging should also be turned off if it is generating a lot of firewall events.

Performance Profiles

The new optimized concurrent scheduler considers the impacts of each job on CPU, Database and Agent/Appliance.

By default it is set to an “Aggressive” performance profile which is optimized for a dedicated Manager.

The performance profile can be changed by navigating to System > System Information and clicking the Managers... button in the toolbar. From this screen select the desired Manager node and open the Properties window. From here the Performance Profile can be changed via the drop-down menu.

The Performance Profile also controls the amount of Agent/Appliance-initiated connections that the Manager will accept. The default of each of the performance profiles effectively balances the amount of accepted, delayed and rejected heartbeats.

Log Retention Strategy

There are different types of logs stored in the Deep Security Manager database.

- AntiMalware logs
Chapter 4: Performance Tuning

- Firewall logs
- DPI logs
- Integrity Monitoring logs
- Log Inspection logs
- System Events

It is recommended to delete logs older than 7 days. Depending on audit purposes, sometimes it may be necessary to store logs longer than usual. However, if the requirement is to keep the logs, it is recommended to use third-party SIEM products.

Make sure that log purge is enabled in Deep Security Manager and log deletion is configured for all types of log (System → System Settings → System Tab → Prune).

Also note that the bigger the database, SQL related queries can often times slow down in relation to the size of the database, so we want to purge logs as much as possible and keep only the logs we need.

Database Indexing

Indexes are specialized data structures that operate on tables (and sometimes views) in the database engine used to aid in the searching for and sorting of data. Indexes are vital to the database engine returning results quickly. As data is modified in the underlying tables that the indexes operate on, the indexes become fragmented. Fragmentation is when the logical ordering of an index does not match the physical ordering of the underlying table or view. As the indexes become more and more fragmented, query times can begin to suffer. The remedy to this situation is to either reorganize or rebuild the index in SQL.

It’s recommended to periodically rebuild the index of the database to improve performance. Below are some useful links with additional information on how to do this:

- Rebuilding SQL Server Indexes (Fragmented data can cause SQL Server to perform unnecessary data reads, slowing down SQL Server’s performance)
- Index Rebuilding Techniques
  http://www.remote-dba.net/t_tuning_index_rebuilding.htm
Chapter 5: Backup and Disaster Recovery

This chapter presents the following topics:

Backup and Disaster Recovery ................................................................. 62
Rule and Configuration Backup ............................................................. 62
Chapter 5: Backup and Disaster Recovery

Backup and Disaster Recovery

Deep Security utilizes a database for all of its configurations and settings. It is highly recommended that the database be backed up periodically. This provides the best chance of successfully recovering a production environment in the quickest amount of time in case there is a disaster situation. Deep Security is compatible with both Oracle and Microsoft SQL database.

Rule and Configuration Backup

All of Deep Security’s configuration and rules are stored in the database. This is essentially the only data that needs to be backed up for disaster/recovery purposes. However, there is another file, called dsm.properties. The file is inside the folder: Program Files\Trend Micro\Deep Security Manager\webclient\webapps\ROOT\WEB-INF.

We recommend users to save a copy of this file. The dsm.properties contains most of the information used by Deep Security to connect to the database. It includes access information such as the database name and credentials.

Back-up an SQL database using Deep Security Manager

NOTE: This feature is available but is not the recommended way of backing up the database. It is better to use the database backup software recommended by Microsoft or Oracle.

1. Go to Start > Programs > Trend Micro > Deep Security Manager to launch the console.
2. Log into Deep Security Manager.
3. Choose System > Tasks
4. Click on “New” on top left corner of Right Pane window
5. Under Type choose Backup and select the Schedule. Click Next.
6. Choose date, start time and frequency. Click Next.
7. Choose the path on the Server for DB backup. Click Next.

8. Confirm and Click Finish.

9. This will create daily backups of SQL server on the specified directory.

**Back-up an SQL database using the osql.exe tool**

2. On the machine where the database is installed, open a commandshell (cmd.exe) and then type "osql.exe -U sa"
3. Type the sa password.
4. The backup itself is performed using the “backup” command:
   1> backup database dsm to disk="C:\dsm.bak"
   2> go

Notes:
Chapter 5: Backup and Disaster Recovery

- The administrator can specify any other disk file / path as a backup destination.
- Replace “dsm” with the database name used when Deep Security was installed.
- Length of time to back up depends on the size of the database. The larger the size, the longer the time to backup.

5. Exit from the osql.exe utility:
   1> quit


---

**Back-up an SQL database using Enterprise Manager**

2. Open Enterprise Manager and connect to the server.
3. Expand the Databases folder, then right-click the database that you want to back up. (Example: ‘dsm’)
4. Select All Tasks, then select Backup Database.
5. Provide a name for the backup in the Name text box. Leave the Database – complete radio button selected and make sure that the correct database to backup is selected in the Database drop-down menu.
6. Select the Overwrite existing media check box to save a new copy of the database either to disk or to tape.
7. To select a destination for the backup, click the Add button. Select an existing file or enter a new file name (eg. C:\Backup\dsm.bak) . Click OK after selecting a file.
8. Click the Options tab and select the Verify backup upon completion check box to verify the backup upon completion.
9. Once all the necessary options are selected, either click the OK button to start performing the backup, or check the Schedule check box to schedule this operation for periodic execution.

---

**Restoring an SQL database using the osql.exe tool**

2. Open up a commandshell (cmd.exe) and then type “osql.exe -U sa”
3. Type the sa password.

---

Trend Micro Confidential. Non-disclosure Agreement is required for non-Trend Micro employees to view this document
Chapter 5: Backup and Disaster Recovery

4. Restore the database from backup, using the “restore” command:
   1> restore database dsm from disk='C:\dsm.bak'
   2> go
   Specify another file name / location, if it is different from C:\dsm.bak

5. Exit from the osql.exe utility:
   1> quit

Restoring an SQL database using Enterprise Manager

2. Open SQL Server Enterprise Manager and connect to the server where
   the backup is to be restored.
3. Right-click the database and select All Tasks, then select Restore
   Database.
4. In the Restore as database list box, enter the name of the new
   database that the backup process will create and restore the backup
   to or from the list of databases, select the database for which the
   backup has to be restored.
5. Select the From device radio button and click the Select Devices...
   button
6. In the Choose Restore Devices dialog box, select either the Disk or the
   Tape radio button.
7. Click the Add button and enter the file name of the backup file that is
   to be restored. If the file exists on a network share, provide the UNC
   share name in the File name text box.

   Note: It is recommended that the backup be copied to the server and
   a local path be used to restore the database.
8. Click OK and Restore the database.

Back-up and Restore an Oracle database using Recovery Manager (RMAN)

Recovery Manager (or RMAN) is an Oracle provided utility for backing-up,
restoring and recovering Oracle Databases. There are several methods
and strategies available for performing backups in Oracle. We suggest
users choose the method that best fit their needs. For this guide, we shall
only cover basic backup method using RMAN. RMAN ships with the
database server and doesn't require a separate installation. The RMAN
executable is located in your ORACLE_HOME/bin directory.

RMAN can be operated from command line:

   [oracle@localhost oracle]$ rman
Chapter 5: Backup and Disaster Recovery

Whenever a backup is created with RMAN, RMAN records the action in the RMAN repository. One can also record copies of files you create outside of RMAN (such as copies of datafiles created with host operating system commands) in the repository. When you attempt to restore the backups using the RESTORE command, RMAN queries the repository for information about available backups, then chooses among them to perform the restore efficiently.

Additional references for RMAN and other methods can be found below:

Oracle database Backup and Recovery FAQ
http://www.orafaq.com/wiki/Oracle_database_Backup_and_Recovery_FAQ#Why_and_when_shoud_I_backup_my_database?

Oracle Database Backup and Recovery Basics
http://download.oracle.com/docs/cd/B19306_01/backup.102/b14192/toc.htm

Overview of Database Backup and Recovery Features
http://download.oracle.com/docs/cd/B19306_01/server.102/b14220/intro.htm#sthref159

Backup and Recovery
http://download.oracle.com/docs/cd/B19306_01/server.102/b14220/backrec.htm#g1023042

Making Backups with Recovery Manager
http://download-west.oracle.com/docs/cd/B12037_01/server.101/b10735/bkup.htm#1005571

Disaster Recovery

Deep Security in its default form has a single point of failure with respect to Database. It is recommended to implement database clustering to create a redundant system in addition to using a full database backup. There are two options available:

a. Restore on the same Server

Once the database has been restored, simply restart the Trend Micro Deep Security service and re-connect with the database. All previous data will be available from the Deep Security Manager.
Chapter 5: Backup and Disaster Recovery

b. Restore on another Server

1. Install Deep Security Manager using your original license on the new box.

2. At this point, you can use the same hostname as the old server or choose another hostname.

3. If a different hostname is used, make sure that the deployed agents are able to contact and reach the server.

4. Choose embedded database to complete the installation.


7. Open the following file in notepad:
   [install Directory]\webclient\webapp\ROOT\WEB-INF\dsm.properties
   It will look something like:
   
   database.name=dsm
   database.directory=C:\Program Files\Third Brigade\Deep Security Manager\dbs
   database.type=Embedded
   mode.demo=false

8. Replace the contents of the file with the following values:
   Note: Replace the <values> with information corresponding to the restored environment (point it to the restored database). Make sure to use “sa” username and password.
   
   database.type=SqlServer
   database.name=<database_name>
   database.SqlServer.server=<hostname>
   database.SqlServer.user=<username>
   database.SqlServer.password=<password>
   database.SqlServer.namedPipe=false
   mode.demo=false


10. Open the dsm.properties file to confirm that the password is encrypted. If the password is still in clear text then open server0.log under the DSM directory to see what are the exceptions.

11. If the password is encrypted, it means the connection to SQL server was successful.

12. Login to the Deep Security Manager console.

13. You can change the hostname of the DSM at this point, provided communication method is not using “agent-initiated” communications and the Manager can contact all the agents.
Chapter 5: Backup and Disaster Recovery

14. Go to System > System Information > Click on DSM name
15. Update the hostname/ip/fqdn for DSM
16. All the agents will now be updated to report to the new Deep Security Manager.
Appendix A References

This appendix presents the following topic:

Communication Ports.......................................................... 70
Updates .................................................................................. 72
Recommended Scan Exclusion List ...................................... 72
Recommended Scan List ...................................................... 74
Communication Ports

Before deployment, make sure that the ports used by Deep Security for communication are open.

The table below lists ports commonly used by different Deep Security components when communicating with each other.
## Appendix A: References

### Deep Security Manager

<table>
<thead>
<tr>
<th>Port</th>
<th>Direction</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>4118 (TCP/UDP)</td>
<td>From Manager to the Agent</td>
<td>Manager to Agent communication</td>
</tr>
<tr>
<td>4120 (TCP/UDP)</td>
<td>From the Agent to the Manager</td>
<td>Agent to Manager communication</td>
</tr>
<tr>
<td>4119 (TCP/UDP)</td>
<td>Going towards the Deep Security Manager Console</td>
<td>DSM console</td>
</tr>
<tr>
<td>443 (TCP/UDP)</td>
<td>From Manager to VMware vCenter</td>
<td>Retrieval of virtual environment information from the vCenter server</td>
</tr>
<tr>
<td>389 (TCP)</td>
<td>From Manager to LDAP (Active Directory Synchronization)</td>
<td>LDAP Clear Text</td>
</tr>
<tr>
<td>636 (TCP)</td>
<td>From Manager to LDAP (Active Directory Synchronization)</td>
<td>LDAP SSL</td>
</tr>
</tbody>
</table>

### Deep Security Agent

<table>
<thead>
<tr>
<th>Port</th>
<th>Direction</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>4118 (TCP/UDP)</td>
<td>From Manager to the Agent</td>
<td>Manager to Agent communication</td>
</tr>
</tbody>
</table>

### Deep Security Relay

<table>
<thead>
<tr>
<th>Port</th>
<th>Direction</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>4122 (TCP/UDP)</td>
<td>From network members to the Relay.</td>
<td>Relay listening port</td>
</tr>
<tr>
<td>443 (TCP/UDP)</td>
<td>From Relay to the Internet</td>
<td>iAU Security Updates</td>
</tr>
</tbody>
</table>

### Database Communication

<table>
<thead>
<tr>
<th>Port</th>
<th>Bi-directional</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1433 (TCP/UDP)</td>
<td>Microsoft SQL server</td>
<td>Bi-directional</td>
</tr>
<tr>
<td>1434 (TCP/UDP)</td>
<td>Microsoft SQL server</td>
<td>Bi-directional</td>
</tr>
<tr>
<td>1521 (TCP/UDP)</td>
<td>Oracle SQL Server</td>
<td>Bi-directional</td>
</tr>
</tbody>
</table>

### Virtual Appliance Communication

<table>
<thead>
<tr>
<th>Port</th>
<th>Bi-directional</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>4118 (TCP/UDP)</td>
<td>From Manager to the virtual appliance (DSVA)</td>
<td>Manager to DSVA communication</td>
</tr>
<tr>
<td>443 (TCP/UDP)</td>
<td>From DSVA to VMware vShield Manager</td>
<td>Sending Anti-Malware functionality status information to the vShield Manager</td>
</tr>
</tbody>
</table>
Appendix A: References

Updates

- Deep Security Rule Updates are typically released once a week, on Tuesdays, inline with Microsoft’s Patch Tuesday.
- Automatic download of Component Updates is recommended
- Automatic download and apply of Deep Security Rule Updates is not recommended
- Automatic download and apply of Anti-Malware Updates is recommended
- It is a best practice to perform a Recommendation Scan after applying a new Deep Security Rule Update
- Create a scheduled task to check new software or turn it on from the System > Updates page.
- Software Packages are not automatically downloaded.
- Check the System > Updates page to determine if there is a new software available in Download Center.
- Software download has to be done manually then imported to the DSM.


Recommended Scan Exclusion List

When you have the Anti-Malware feature enabled, there are certain files and folders that should not be scanned, the reason could be the files are unscannable due to implementing certain encryptions as well as being locked at all times, other times scanning these files would cause performance or cause software using these files to become unstable.

Refer to this KB article for recommended exclusion lists when using Trend Micro products:

Here are some additional information from external sources:

- General Exclusions for all Windows platforms
  - http://support.microsoft.com/kb/822158/

Active Directory Domain Controllers
Appendix A: References

- http://support.microsoft.com/kb/822158/en-us

Microsoft IIS Servers
- http://support.microsoft.com/kb/817442

Microsoft SQL Servers
- http://support.microsoft.com/kb/309422

Microsoft SharePoint Servers
- http://support.microsoft.com/kb/952167

Microsoft Operations Manager Server (MOM)
- SMS 2.0 / 2003
  - http://support.microsoft.com/kb/327453

Microsoft Exchange Server 2000
- http://support.microsoft.com/kb/328841
- http://support.microsoft.com/kb/245822

Microsoft Exchange Server 2003
- http://support.microsoft.com/kb/823166
- http://support.microsoft.com/kb/245822

Microsoft Exchange Server 2007

Microsoft Exchange Server 2010
Recommended Scan List

Refer to this KB article for recommended exclusion lists when using Trend Micro products:

Recommended files and folders to scan with Deep Security Anti-Malware feature.

Realtime Scan
- `<drive>\ Program Files`
- `<drive>\ Windows`
- `<drive>\ Documents and Settings`
- `<drive>\ Users`

Scheduled Scan and Manual Scan
- All Folders and Files