Trend Micro Proof-of-Concept Deployment Checklist:
Deep Security 7.5

Suggested Test Hardware / Software

Depending on your needs, we recommend at least one virtual server, preferably more. We also recommend testing at least one physical server, one virtual workstation, and one physical workstation. Use the below information as a guide to help set up your environment:

ESXi 4.1 Host 1 (Management Host)	
• Virtual Server running VMware vCenter Server 4.1.0	❑
• Server running Trend Micro Deep Security Manager 7.5 (DSM) (**Memory**: 4 GB, **Disk**: 1.5 GB – 5 GB recommended, **OS**: Windows Server 2003 SP2 or Windows 2008 64-bit). Click here to obtain the required license keys and here to download copies of the product documentation.	❑
• VMware vShield Manager 4.1 Virtual Appliance to enable agentless antivirus (1 per vCenter instance) (**Memory** 1 GB RAM – 8 GB for production environments, **Disk**: 8 GB).	❑
• **Optional** — Trend Micro Smart Protection Server 1.1 Virtual Appliance to enable File Reputation Services (**Memory** 1 GB RAM, **CPU**: 2 vCPUs, **Disk**: 10 GB). Click here to obtain copies of the product documentation.	❑
ESXi 4.1 Host 2 (Test Host)	
• Trend Micro Deep Security Virtual Appliance (DSVA). Enables DPI, IPS, firewall, and agentless antivirus protection at the Hypervisor level. • You must be able to put this ESXi 4.1 host into maintenance mode to deploy the Filter Driver and the vShield Loadable Kernel Module (LKM) • Either suspend or vMotion any VMs on the test host to another host until after you complete the install.	❑
• One (1) test server (**OS**: Windows Server 2003 / 2008) with the latest VMware Tools and the VMware vShield Endpoint Thin Agent.	❑
• One (1) test client (**OS**: Windows XP 32-bit, Windows Vista 32-bit, Windows 7 32- or 64-bit) with the latest VMware Tools and the VMware vShield Endpoint Thin Agent	❑
Additional Recommendations	
Trend Micro also suggests that you set up the following test physical workstations and servers (**Note**: You also can deploy Trend Micro Deep Security to servers running Red Hat Linux, SUSE Linux, Oracle Solaris, and HP-UX): • One (1) test server (**OS**: Windows Server 2003 / 2008) with the with the Trend Micro Deep Security Agent) • One (1) test client (**OS**: Windows XP, Windows Vista, Windows 7 with the Trend Micro Deep Security Agent)	❑

Installation Notes

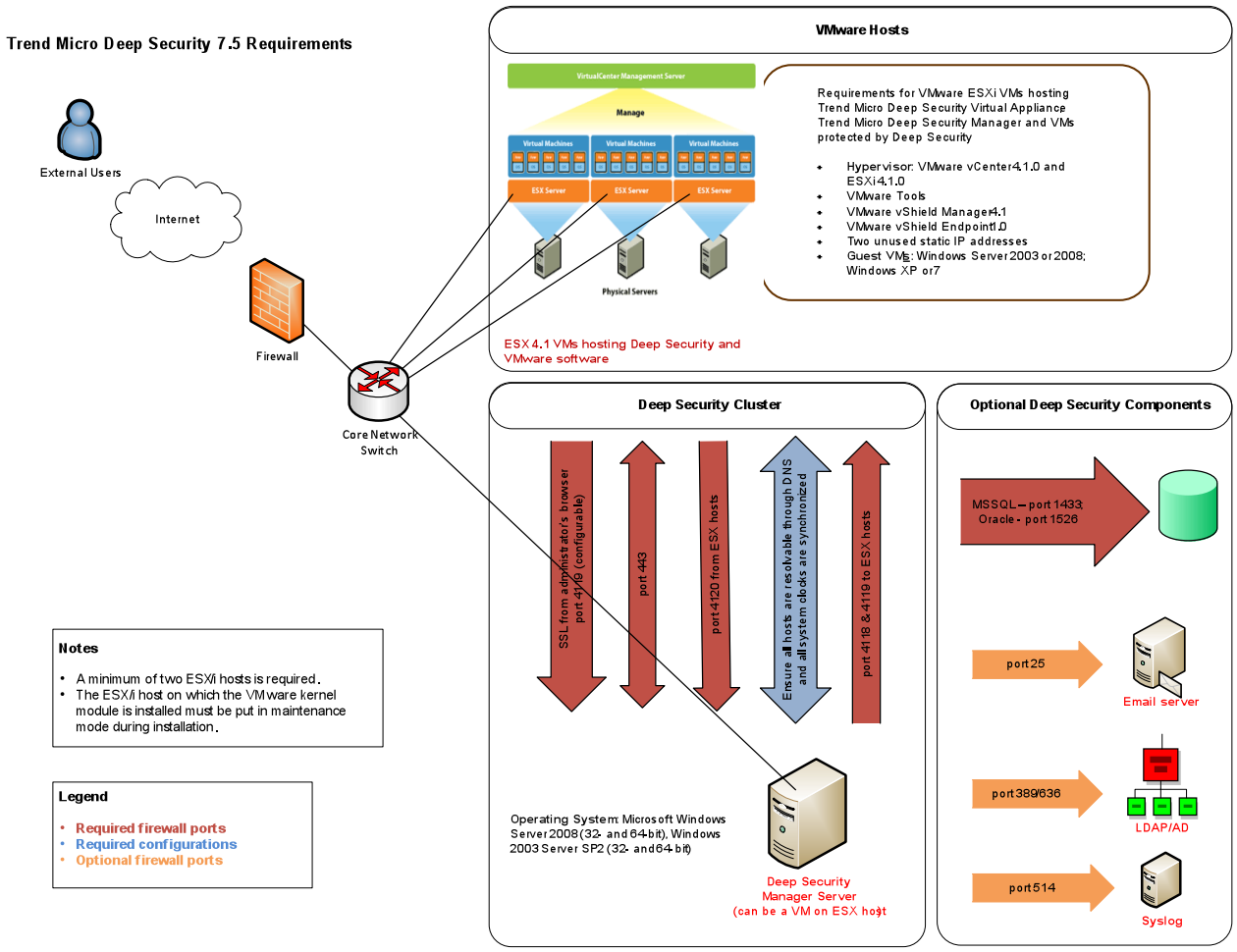
VMware vCenter	
• Be sure to obtain a VMware vCenter Administrator username and password before beginning the install process.	❑
Deep Security Virtual Appliance	
• You must have one (1) unused static IP address (plus gateway, netmask and DNS servers) must be available for use by Deep Security Virtual Appliance.	❑
Deep Security Manager	
• You must have a Windows administrator username and password for the physical or virtual server hosting Deep Security Manager to install the DSM software. • **Port 4118:** Deep Security Manager uses this port to communicate with Deep Security agents and appliances. (Not configurable.) • **Port 4119**: Microsoft Internet Explorer (7.0+) and Mozilla Firefox (3.0+) use this port to communicate with Deep Security Manager. (Configurable.) • **Port 4120**: Deep Security agents and appliances use this port to communicate with Deep Security Manager. (Configurable.)	❑
Deep Security Manager Database (Recommended but Optional)	
• **Supported Databases**: Oracle 11g, Oracle 10g, Microsoft SQL Server 2008 SP1, Microsoft SQL Server 2005 SP2 • **Port 1433**: Must be open to use Microsoft SQL Server as your DSM database. • **Port 1526**: Must be open to use Oracle as your DSM database.	❑
Microsoft Active Directory (Optional)	
• **Port 389/636:** Active Directory uses this port to communicate with Deep Security Manager (**Note**: If you use Active Directory, the AD server must running and available.) • You must have one (1) Active Directory user with read-only privileges for synchronizing users with target systems.	❑
Email Server (Optional)	
• **Port 25**: Must be open for Deep Security Manager to issue email notifications	❑
VMware vShield Manager 4.1	

• **Static IP Address**: You must have one unsused static IP address (plus gateway, netmask, and DNS servers) available for use by vShield Manager .
• **Port 443**: vShield Manager uses this port to communicate with vCenter and Deep Security Manager.
• The VMware vShield API supports only the following SCSI drivers. Ensure your SCSI hardware is compatible with one of them:
  ○ LSI Logic Parallel (Default for Windows Server 2003)
  ○ LSI Logic SAS (Default for Windows Server 2008 and Windows 7)
  ○ LSI Logic Para Virtual (new driver from VMware)
  ○ BusLogic SCSI controllers are **not supported**
	❑

All Systems	
• The system time must be the same for all physical machines, VMs, and all Deep Security Manager, and vCenter instances • All servers and VMs must be able to resolve one another by DNS or via host files	❑

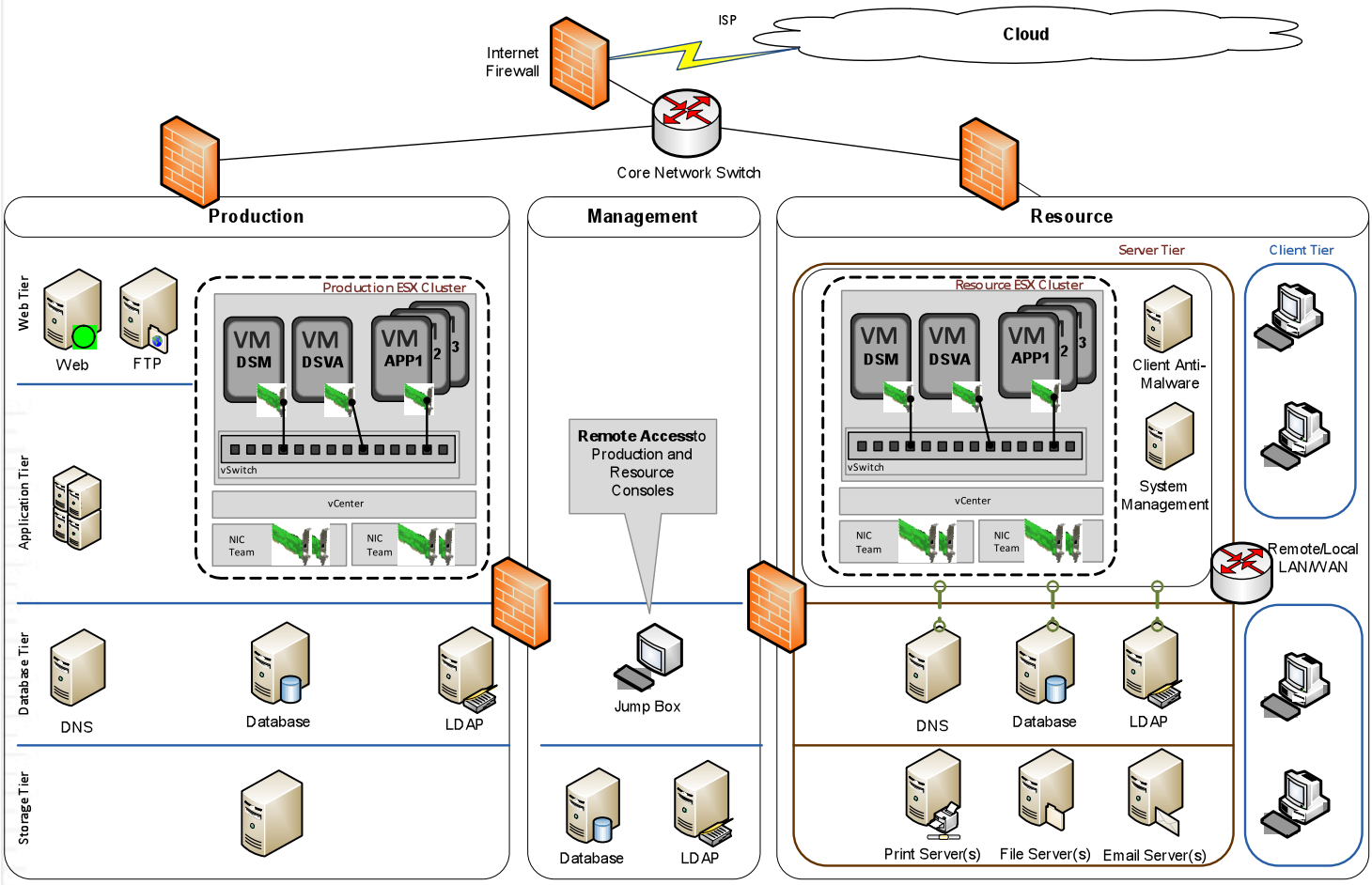
©Trend Micro, Inc. — December 2010

Figure 1: Deep Security 7.5 Port Requirements



©Trend Micro, Inc. — December 2010

Figure 2: Deep Security 7.5 in an N-tier Environment



©Trend Micro, Inc. — December 2010