Endpoint Security

E80.50

Scalability and Sizing Guide

22 October 2013

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Latest Documentation

The latest version of this document is at:
(http://supportcontent.checkpoint.com/documentation_download?ID=28278)

To learn more, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

For more about this release, see the E80.50 home page
(http://supportcontent.checkpoint.com/solutions?id=sk92965).

Revision History

Date	Description
22 October 2013	First release of this document

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments
(mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Endpoint Security E80.50).

Contents

Introduction

The purpose of this document is to help you plan your Endpoint Security environment. It describes the best practices for server deployment and sizing the Endpoint Security servers.

Overview of the System Architecture

An Endpoint Security environment includes several components that should be configured correctly for the best performance.

Required Components:

- **Endpoint Security Management Server** - Computer that contains the Endpoint Security software and databases. The Endpoint Security Management Server communicates with Endpoint Security clients to manage Endpoint Security client rules and to update protections.
- **SmartEndpoint** - Application installed on a Windows platform that lets you deploy, monitor, and configure Endpoint Security clients and rules. You can install SmartEndpoint on the Endpoint Security Management Server (Windows only) or on a computer that supports the Endpoint Security client installation.
- **Endpoint Policy Server** – Server that manages traffic from the Endpoint Security clients. The Endpoint Security Management Server also acts as an Endpoint Policy Server. You can add external Endpoint Policy Servers to improve performance in large environments.
- **Endpoint Security Management Server for High Availability** – A backup server that is always available for down time situations.
- **Endpoint Security Database** - Contains the policy that enforces security on Endpoint Security clients. This database also contains user and computer objects, licensing and Endpoint monitoring data.
- **Directory Scanner** - Software component that synchronizes the structure and contents of the **Active Directory** with the Endpoint Security database.
- **Endpoint Security Clients** - Endpoint Security client application installed on end-user computers. These Endpoint Security clients monitor the security aspects of your endpoints and enforce security rules.
- **Endpoint Security Blades** - Library of software blades available on the Endpoint Security Management Server. You can install any or all of these blades on individual Endpoint Security clients.

Planning Your Environment

Consider these factors to plan an environment that is best for your organization:

- The number of Endpoint Security clients to be deployed.
- Which Endpoint Security Blades to deploy on the Endpoint Security clients.
- The interval at which the changes in the policies will be enforced on the clients.
- The number of users and computers that you will import to the Endpoint Security Management Server from your organization's existing hierarchy.
- The number of remote sites in the organization.

Centralized Server Deployment

A centralized server deployment has one Endpoint Security Management Server:

- The Endpoint Security Management Server, which is also an Endpoint Policy Server by default, manages all Endpoint Security client requests and communication.
- The Endpoint Security Management Server, which is defined as Log Server by default, saves all Endpoint Security clients logs.

Distributed Server Deployment

In a distributed deployment, additional Policy Servers handle some activities instead of the Endpoint Security Management Server. This provides better performance in larger environments.

External Endpoint Policy Servers can perform these functions:

- Reduce bandwidth between a remote site and the site where the Endpoint Security Management Server is located (the central site).
- Let clients stay connected to the server if connectivity issues occur between a remote site and the central site. Clients can communicate with the local Endpoint Policy Server at the remote site.
- Improve overall system performance by distributing common client messages and policy enforcement between multiple Endpoint Policy Servers.

See more about External Endpoint Policy Servers (on page 8).

High Availability Deployment

A Management High Availability environment includes one Active Endpoint Security Management Server and one or more Standby Endpoint Security Management Servers. The Active Security Management server databases are periodically synchronized with the Standby Endpoint Security Management server databases for full redundancy.

Standby Endpoint Security Management Servers do not handle client or Policy Server requests.

Only one Endpoint Security Management Server can be Active at a time. If the Active server fails, you manually change a Standby server to be an Active server.

Integration with Active Directory

If your organization uses Microsoft Active Directory (AD), you can import Users, Computers, Groups, and Organizational Units (OUs) from multiple AD domains into the Endpoint Security Management Server. After the objects have been imported, you can assign policies that meet the needs of the organization.

When you first log in to SmartEndpoint, the **Users and Computers** tree is empty. To populate the tree with users from the Active Directory, you must configure the Directory Scanner (see *Directory Scanner* in the *Endpoint Security E80.40 Administration Guide* (http://supportcontent.checkpoint.com/solutions?id=sk82100) for configuration instructions).

The Endpoint Security Management Server communicates with the Directory Scanner and can handle multiple domains.

Note - The Directory Scanner does not scan all objects in the AD. It scans Users, Computers, Groups, and Organizational Units (OUs). For example, printers are not scanned.

Active Directory Size Estimation

You can use the external tool **ADFind** to estimate how many objects will be scanned by the Directory Scanner.

The query for counting the exact number of objects that will be scanned by the Directory Scanner on a given search base is:

```
adfind -b ou=<MyScannedOU>,dc=<MyDomain>,dc=<com> -f
"(|(|(&(objectCategory=container)(|(name=Builtin)(name=Users)(name=Computers)))(obj
ectCategory=organizationalUnit)(objectCategory=organization)(objectCategory=domainD
NS)(objectCategory=builtinDomain))(&(objectCategory=user)(!(objectClass=contact)))(
objectCategory=computer)(&(objectCategory=group)(groupType:1.2.840.113556.1.4.803:=
2147483648)))" -c
```

The query counts:

- Users that are not contacts.
- Computers.
- Groups that are security groups (not distribution groups).
- Organizational Units (including "Users", "Computers" and "Built-in" containers).

For example:

If you want to scan the "marketing" OU in the "company.org" domain the query should be:

```
adfind -b ou=marketing,dc=company,dc=org -f
"(|(|(&(objectCategory=container)(|(name=Builtin)(name=Users)(name=Computers)))(obj
ectCategory=organizationalUnit)(objectCategory=organization)(objectCategory=domainD
NS)(objectCategory=builtinDomain))(&(objectCategory=user)(!(objectClass=contact)))(
objectCategory=computer)(&(objectCategory=group)(groupType:1.2.840.113556.1.4.803:=
2147483648)))" -c
```

If you want to scan the whole "company.org" domain the query should be:

```
adfind -b dc=company,dc=org -f
"(|(|(&(objectCategory=container)(|(name=Builtin)(name=Users)(name=Computers)))(obj
ectCategory=organizationalUnit)(objectCategory=organization)(objectCategory=domainD
NS)(objectCategory=builtinDomain))(&(objectCategory=user)(!(objectClass=contact)))(
objectCategory=computer)(&(objectCategory=group)(groupType:1.2.840.113556.1.4.803:=
2147483648)))" -c
```

Directory Scanner Performance

This table shows the amount of time that the Directory Scanner takes to scan an Active Directory. It also shows a summary of the test environment where these numbers came from.

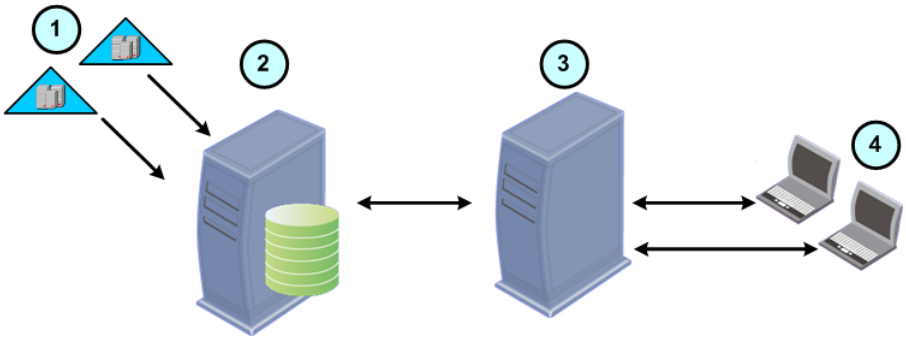
Quantity of Objects	Duration of Scan	Test Environment
44,000	16 minutes	**Endpoint Security Management Server** - Windows 2008 R2 with 2GB RAM **AD server** - Windows 2003 R2 with 2GB RAM
160,000	1.5 hours	**Endpoint Security Management Server** - Windows 2008 R2 with 2GB RAM **AD server** - Windows 2003 R2 with 2GB RAM
540,000	5 hours	**Endpoint Security Management Server** - Windows 2008 R2 with 4GB RAM **AD server** - Windows 2003 R2 with 4GB RAM

External Endpoint Policy Servers

External Endpoint Policy Servers decrease the load of the Endpoint Security Management Server and reduce the bandwidth required between sites. By default, the Endpoint Security Management Server also acts as an Endpoint Policy Server, in addition to the other Endpoint Policy Servers. The work of communication with the Endpoint Security clients is distributed among all of them.

The Endpoint Policy Servers are located between the Endpoint Security clients and the Endpoint Security Management Server. For most tasks, Endpoint Security clients communicate with the Endpoint Policy Servers and the Endpoint Policy Servers communicate with the Endpoint Security Management Server.

If there are multiple Endpoint Policy Servers in an environment, each Endpoint Security client does an analysis to find which Endpoint Policy Server is "closest" (will be fastest for communication) and automatically communicates with that server.



Item	Description
1	Active Directory Domains
2	Endpoint Security Management Server
3	External Endpoint Policy Server
4	Enterprise workstations with Endpoint Security clients installed

The Endpoint Policy Server handles the most frequent and bandwidth-consuming communication. The Endpoint Policy Server handles these requests without forwarding them to the Endpoint Security Management Server:

- All heartbeat and synchronization requests.
- Policy downloads

- Anti-Malware updates
- All Endpoint Security client logs (the Endpoint Policy Server is configured as Log Server by default).

The Endpoint Policy Server sends this data to the Endpoint Security Management Server:

- All blade-specific messages (which require information to be stored in the database). For example, Full Disk Encryption recovery data.
- Monitoring data. This includes the connection state and other monitoring data for connected clients.
- Policy Server generated messages.
-

Endpoint Policy Server Performance

The maximum number of supported Endpoint Policy Servers in an environment is 25.

- An Endpoint Policy Server on Smart-1 5 can handle up to 5,000 Endpoint Security clients.
- An Endpoint Policy Server on Smart-1 25 can handle up to 27,000 Endpoint Security clients.

Bandwidth Usage

The bandwidth required for communication between servers and between clients and servers in the Endpoint Security environment depends on many factors.

Client to Server Communication

The communication between the Endpoint Security client and the Endpoint Security Management or Policy Server includes:

- Endpoint Security clients send a heartbeat message to the Endpoint Security Server at 60 second intervals (by default) to check if policy updates are necessary.
- Endpoint Security clients send a sync message to the Endpoint Security server when synchronization is necessary. The sync includes monitoring data from the blades installed on the Endpoint Security clients.
- Endpoint Security clients send blade-related payloads to the Endpoint Security server when necessary.
- Endpoint Security clients upload logs to the Endpoint Security server,

Endpoint Security client to Endpoint Security Management or Policy server required bandwidth is based on these factors:

- The Heartbeat interval - The frequency at which Endpoint Security clients communicate with Endpoint Security servers to make sure that all policies are up to date.
- Which Endpoint Security Blades are installed on the Endpoint Security client.

Client to Server Traffic

This table shows the estimated traffic for 1,000 deployed Endpoint Security clients with the default heartbeat interval (60 seconds). The table is organized by Endpoint Security blade.

Component or Blade	**Traffic Inbound to server Kb/s**	**Traffic Outbound from server Kb/s**
Device Agent	236	143
Anti-Malware Updates	0.2	15
Full Disk Encryption	34	3
Media Encryption & Port Protection	3	2
Application Control	15	17

Note - If the Anti-Malware blade is installed, clients must download the Anti-Malware database after installation. The average size of the full database download is 145 Mb for each Endpoint Security client. This database is updated every few hours.

The traffic is linear. To calculate the estimated traffic, multiply the values in the table above by the number of Endpoint Security clients deployed (note that the values above are for 1,000 deployed Endpoint Security clients).

For example:

In an environment with 20,000 Endpoint Security clients with Full Disk Encryption and Media Encryption & Port Protection installed:

Inbound traffic: (20*236) + (20*34) + (20*3) = 5,460 Kb/s

Outbound traffic: (20*143) + (20*3) + (20*2) = 2,960 Kb/s

Policy Server to Management Server Communication

Endpoint Policy Servers communicate with the Endpoint Security Management Server to retrieve system information to answer Endpoint Security client requests.

The communication between the Endpoint Policy Server and the Endpoint Security Management Server includes:

- Endpoint Policy Servers get from the Endpoint Security Management Server:
  - Policies and installation packages.
  - Anti-Malware updates.
  - All files that they need for synchronization.
- Endpoint Policy Servers send a Policy Server heartbeat message to the Endpoint Security Management Server at an interval of 60 seconds, by default.
- Endpoint Policy Servers send a sync messages to the Endpoint Security Management Server when synchronization is necessary.
- Endpoint Policy Servers send monitoring events to the Endpoint Security Management Server at 60 second intervals or when there are more than 1,000 events.
- Endpoint Policy Servers send all database-related messages directly to the Endpoint Security Management Server.

Endpoint Policy Servers to Endpoint Security Management Server required bandwidth is based on these factors:

- The Endpoint Policy Server Heartbeat interval
- The Monitoring data upload rate.
- The size of the scanned Active Directory.

Policy Server to Management Server Traffic

This table shows an estimate of the traffic in an environment with:

- One Endpoint Policy Server
- 1,000 deployed Endpoint Security clients
- A default heartbeat interval of 60 seconds
- 5,000 Active Directory objects scanned.

Some values depend on the number of deployed clients and scanned AD objects.

Activity	Inbound to Management Server Kb/s	Outbound from Management Server kb/s	Depends on AD size	Depends on Number of Deployed Clients
Anti-Malware Updates	0.1	0.1	No	No
Monitoring Upload	33	0.02	No	Yes
PAT Download	0.01	137	Yes	No
Control Messages (CP heartbeat, sync)	0.2	0.3	No	No

Note - The Endpoint Policy Server must download the Anti-Malware database after installation. The average size of the full database download is 145 Mb. After the first download, the database is updated every few hours with much smaller downloads.

The traffic is linear. To calculate the estimated traffic, multiply the numbers in the table above by number of Endpoint Security clients deployed or by the Active Directory size, if relevant. Note that the values above are for 1,000 deployed Endpoint Security clients and 5,000 AD objects scanned.

For example:

In an environment with one Endpoint Policy Server, 20,000 Endpoint Security clients deployed, and 80,000 AD object scanned:

Inbound traffic: 0.1 + (20*33) + (16*0.01) + 0.2 = 660.46 Kb/s

Outbound traffic: 0.1 + (20*0.02) + (16*137) + 0.3 = 2,192.8 Kb/s

Endpoint Security Sizing

Hardware requirements depend on:

- The total numbers of deployed Endpoint Security clients.
- The Endpoint Security Blades that are installed on the Endpoint Security clients.
- The size of the portion of the Active Directory that is scanned by the Directory Scanner.

Below are tables with minimum requirements per number of Endpoint Security clients and AD size.

Notes on the sizing information:

- All clients shown in the tables have all Endpoint Security blades (Total Security) installed, unless individual blades are listed.
- The Directory Scanner does not scan all objects in the AD. It scans Users, Computers, Groups, and Organizational Units (OUs). For example, printers are not scanned.
- You can configure the Directory Scanner to scan only relevant parts of the AD. For example, scan only one OU if all deployed Endpoint Security clients reside in the OU.
- An Endpoint Policy Server on Smart-1 5 can handle up to 5,000 Endpoint Security clients.
- An Endpoint Policy Server on Smart-1 25 can handle up to 27,000 Endpoint Security clients.

Servers on Gaia

This table shows the minimum requirements per number of Endpoint Security clients and AD size for Gaia servers.

Row #	Number of Endpoint Security Clients	AD Objects Scanned	Endpoint Security Management Server	Policy Servers
1	2,500	12,500	Smart-1 5	none
2	5,000	25,000	Smart-1 25	none
3	10,000	50,000	Smart-1 25	1 Smart-1 5
4	20,000	100,000	Smart-1 50 with extended RAM (16GB)	1 Smart-1 25
5	30,000	150,000	Smart-1 50 with extended RAM (16GB)	2 Smart-1 25
6	40,000	200,000	Smart-1 50 with extended RAM (16GB)	2 Smart-1 25
7	50,000	250,000	Smart-1 50 with extended RAM (16GB)	2 Smart-1 25
8	60,000	300,000	Smart-1 50 with extended RAM (16GB)	3 Smart-1 25
9	70,000	350,000	Smart-1 50 with extended RAM (16GB)	3 Smart-1 25
10	80,000	500,000	Smart-1 50 with extended RAM (16GB)	3 Smart-1 25
11	150,000 Full Disk Encryption and Media Encryption & Port Protection	800,000	Smart-1 50 with extended RAM (16GB)	3 Smart-1 25

To calculate the minimum hardware requirements for your environment:

1. Find the row that has a **Number of Endpoint Security Clients** that is closest to but no less than the number in your environment . For example, if you have 52,000 clients, look at row 8 and not row 7.
2. In the same row, look at the number of **AD Objects Scanned**.
   - If the number of **AD Objects Scanned** is equal to or more than the number in your environment, the hardware requirements in that row apply to your environment.

- If the number of AD Objects Scanned is less than the number in your environment, find the row that has the number of AD Objects Scanned that is closest to but no less than the number in your environment . The hardware requirements in that row apply to your environment.

For example, row 3 shows that an Endpoint Security Management Server on Smart-1 25 with one Endpoint Policy Server on Smart-1 5 supports up to 10,000 clients and up to 50,000 scanned AD objects. If you are deploying more than 10,000 clients or intend to scan more than 50,000 AD objects, then the requirements of row 3 are not enough for your environment. Look in the lower rows to find a better match.

If you have 15,000 clients but 350,000 scanned AD objects, the requirements of row 9 apply to your environment. However, each Endpoint Policy Server can handle 27,000 clients, so only 1 Smart-1 25 Endpoint Policy Server is required.

Notes:

- To learn how to extend the RAM on Smart-1 50, see the *Smart-1 50 Installing and Removing Memory Guide.* http://downloads.checkpoint.com/dc/download.htm?ID=18942

-In addition to recommended number of Endpoint Policy Servers, you can add more Endpoint Policy Servers for redundancy. If one Endpoint Policy Server is down, clients will connect to a different Endpoint Policy Server and not the Endpoint Security Management Server.

Servers on Windows

Number of Endpoint Security Clients	AD Objects Scanned	Endpoint Security Management Server	Policy Servers
60,000	300,000	Windows 2008 R2 8 CPUs: Intel Xeon E5620 @ 2.27GHz 16GB RAM DDR3, 4 Hard Disks in RAID 10 configuration	3 Servers Windows 2008 R2 4 CPUs: Intel Xeon E5220 @ 2.27GHz 4GB RAM DDR3

Alternative Sizing Calculator

You can use the questions below to help you calculate the minimum hardware requirements for your environment. The information and recommendations here are the same as in the tables above.

Endpoint Security Management Server

Answer these questions and see the corresponding Endpoint Security Management Server hardware recommendation. If you get two different hardware recommendations, choose the stronger one.

How many clients do you intend to deploy?

a) Up to 2,500 Total Security clients > Smart-1 5

b) 2,500 – 10,000 Total Security clients > Smart-1 25

c) 10,000 – 80,000 Total Security clients > Smart-1 50 with extended RAM (16GB)

d) 10,000 – 150,000 FDE+ME clients > Smart-1 50 with extended RAM (16GB)

What is the AD scanned size?

Note - You can configure the Directory Scanner to scan only relevant parts of the AD. For example, scan only one OU if all deployed Endpoint Security clients reside in the OU.

a) Up to 12,500 objects > Smart-1 5

b) 12,500 – 50,000 objects > Smart-1 25

c) 50,000 – 500,000* objects > Smart-1 50 with extended RAM (16GB)

d) 500,000 – 800,000** objects > Smart-1 50 with extended RAM (16GB)

* The maximum number of scanned AD objects that is supported for Total Security is 500,000.

** The maximum number of scanned AD objects that is supported for FDE+ME only is 800,000

Endpoint Policy Servers

Answer this question to see the recommended quantity of Endpoint Policy Servers and hardware.

How many clients do you want to deploy?

a) Up to 5,000 Total Security clients > no Endpoint Security Policy server is needed*

b) 5,000 – 10,000 Total Security clients > 1 Endpoint Security Policy server Smart-1 5

c) 10,000 – 27,000 Total Security clients > 1 Endpoint Security Policy server Smart-1 25

d) 27,000 – 54,000 Total Security clients > 2 Endpoint Security Policy servers Smart-1 25**

e) 54,000 – 80,000 Total Security clients > 3 Endpoint Security Policy servers Smart-1 25**

f) 54,000 – 150,000 FDE+ME clients > 3 Endpoint Security Policy servers Smart-1 25**

* You can install Endpoint Policy Server to improve overall system performance by load-balancing common client messages

** The Endpoint Security Management Server should not be configured as an Endpoint Policy Server.

Note - In addition to recommended number of Endpoint Policy Servers, you can add more Endpoint Policy Servers for redundancy. If one Endpoint Policy Server is down, clients will connect to a different Endpoint Policy Server and not the Endpoint Security Management Server.

Large-Scale Environments (20,000 +)

E80.50 supports large-scale environments of up to 80,000 clients with all Endpoint Security blades (Total Security) or150,000 clients with Full Disk Encryption and Media Encryption & Port Protection.

In a large-scale environment (20,000+ seats), we recommend these configurations:

1. Do not configure the Endpoint Security Management Server as an Endpoint Policy Server. See *Enabling the Management Server to be an Endpoint Policy Server* in the Endpoint Security E80.40 Administration Guide (http://supportcontent.checkpoint.com/solutions?id=sk82100).

   Install external Endpoint Policy Servers to handle requests from Endpoint Security clients.

   Explanation: This makes the Endpoint Security Management Server resources available for other tasks and reduces bandwidth between sites.
2. Install the Endpoint Security Management Server on a 64-bit server.

   Note: If the Endpoint Security Management Server is on Gaia, do the procedure in SK83640 (http://supportcontent.checkpoint.com/solutions?id=sk83640) to convert the system to 64-bit.

   Explanation: This allows memory consumption of more than 4GB per process.
3. If more than 80,000 Endpoint Security clients are deployed, increase the Client Heartbeat Interval to 2 minutes.

   Explanation: This reduces the database activity rate.

4. Do not configure Log forwarding (transferring logs from one Log Server to another).
   Explanation: This distributes the load of log handling between the various servers.

Disk Space Requirements

The Endpoint Security Management Server contains a database that stores all rules, configurations, Endpoint Security client information, monitoring data, and Endpoint Security client logs.

The size of the database depends on these factors:

- The size of the monitoring data and for how long the monitoring history is saved.
- The number of endpoint events in the system and for how long they are saved.
- The Endpoint Security Blades that are installed on the Endpoint Security clients. This affects the amount of data that is saved for each Endpoint Security client
- The amount of AD objects that are scanned by the Directory Scanner.

Database Purging

There is a scheduled purge task that runs on the database and deletes monitoring data that is out of date. This prevents the database from growing too big and helps to reduce database response times. By default the purge task runs every 24 hours and purges monitoring data older than 30 days.

Note - It is important to pay attention to available disk space on the Endpoint Security Management Server.

Calculating Minimum Disk Space

Minimum Disk Space for the Database

You can calculate the minimum disk requirements for the database by using the table below. The Database growth is approximately linear, so to calculate minimum disk requirements multiply the minimum disk requirement by the number of clients.

- The Active Directory size is assumed to be 5 times the number of Endpoint Security clients.
- All clients shown in the tables have all Endpoint Security blades (Total Security) installed.

Number of Clients	Minimum disk requirements for the database
2,500	1.2GB
5,000	2.4GB
10,000	4.2GB
80,000	30GB

Minimum Disk Space for Storing Logs

Endpoint Security servers are configured as Log servers by default, therefore additional disk space is required for storing logs.

On average, each Endpoint Security client sends 50 logs per hour. 200 bytes of disk space is required per log. Therefore 240KB is required to store one day of logs from one Endpoint Security client.

Endpoint Security Client Deployment

Endpoint Security supports up to 1,000 concurrent deployments. At a given time, up to 1,000 Endpoint Security clients can be in the deployment phase.

As a result of the large load on the Endpoint Security Management Server during the deployment phase, we recommend that you wait 15 minutes between deployments of 1,000 clients.

Two packages are installed on each endpoint as part of the Endpoint Security client deployment:

- **Initial Endpoint Security client** - This package includes the Endpoint Agent that communicates with the Endpoint Security Management Server.
- **Software Blade Package** - This package includes the specified Software Blades to be installed on the Endpoint Security client.

After the Initial Endpoint Security client is deployed, clients download the Software Blade package from the Endpoint Security Management Server or Endpoint Policy Server. The Initial Client is 10MB. The size of Software Blade package varies between 10MB and 200MB.

When a new Endpoint Security client is deployed or an existing Endpoint Security client is upgraded, these steps occur:

1. The Endpoint Security client downloads the Software Blade package from the Endpoint Security Management Server.
2. The relevant data for the Endpoint Security client is saved in the database on the Endpoint Security Management Server.
3. The Endpoint Security client gets its Container/Blade licenses from a pool of available licenses.
4. When the Endpoint Security client is installed with the Anti-Malware blade it must download the Anti-Malware database. The average size of the database download is 145 Mb.

Troubleshooting

If you have connectivity problems, (for example Endpoint Security clients fail to communicate with an Endpoint Security server or SmartEndpoint fails to connect to the Endpoint Security Management Server) do these steps on the problematic Endpoint Security server to find the issue.

Checking for Java Errors

Check `%UEPMDIR%\logs\server_messages.log` on Windows and `$UEPMDIR/logs/server_messages.log` on Gaia for errors.

If there is a **java.lang.OutOfMemoryError** error, Tomcat is out of Java space. You can increase the Java heap space on a 64-bit platform (JVM should be 64-bit).

To make sure that JVM is 64-bit:

In the command line, run:

- **Windows** - `"%UEPMDIR%\engine\jre\bin\java" –version`
- **Gaia** - `"$UEPMDIR/engine/jre/bin/java" -version`

If necessary, see sk83640 (http://supportcontent.checkpoint.com/solutions?id=sk83640) to upgrade JVM to 64-bit on a 64-bit server.

To increase the Java Heap Memory on Windows:

1. On the 64-bit Windows server, stop the **Check Point Endpoint Security Server** Service.
2. Change the value of the `JvmMx attribute` found under **HKEY_LOCAL_MACHINE -> SOFTWARE -> Wow6432Node -> Apache Software Foundation -> Procrun 2.0 -> CPEndpointServer -> Parameters -> Java** according to the RAM on the server:
   - If RAM <= 2G leave the default (1024)
   - If 2G < RAM < 8G change the JvmMx to 2048
   - If RAM > 8G change the JvmMx to 4096

Note - Use Decimal (not Hex) values.

3. Start the **Check Point Endpoint Security Server** Service.

To increase the Java Heap Memory on Gaia:

1. On the 64-bit Gaia server, do the instructions in sk83640 (http://supportcontent.checkpoint.com/solutions?id=sk83640) if you have not done them.
2. Run `cpstop`.
3. Backup `$CPDIR/registry/HKLM_registry.data.`
4. In `$CPDIR/registry/HKLM_registry.data,` change the value of `EPS_SERVER_PARAM_JVMMX` attribute found under `CPuepm` according to the RAM on the server:
   - If RAM <= 2G leave the default (1024)
   - If 2G < RAM < 8G change the JvmMx to 2048
   - If RAM > 8G change the JvmMx to 4096
5. Run `cpstart`.

Checking for Apache Errors

Check `%UEPMDIR%\logs\mod_jk.log` on Windows or `$UEPMDIR\logs\mod_jk.log` on GAIA for errors. If there are errors that Apache fails to forward requests to the Tomcat, do the procedure below.

To fix errors between Apache and Tomcat:

1. Check that Tomcat is listening on 8009.
   a) Run on the CMD:
      - On Windows - `netstat -an | find "8009"`
      - On Gaia - `netstat -an | grep "8009"`
2. Check `server_messages.log` for errors.