2.1.3 Network Connectivity Requirements

Endpoint Secure requires network connectivity between the Endpoint Secure Agent and the Endpoint Secure Manager and between the Endpoint Secure Manager and the cloud server. The required ports and server addresses are as follows.

Source Device	Destination Device	Protocol/Port	Port Function
Endpoint Secure Agent	Endpoint Secure Manager	TCP 443	Endpoint Secure Manager access
		TCP 4430	Endpoint Secure Agent download and database update
		TCP 8083	Service port
		TCP 54120	Endpoint Secure Agent enabling/disabling by Endpoint Secure Manager in emergency scenarios
		ICMP	Connectivity detection
Source Device	Destination Device	Server Addresses Connected Through the Internet	
Endpoint Secure Manager	Cloud server	Patches	https://upd.sangfor.com
		Licensing	https://auth.sangfor.com
		Cloud-Based Engine	https://analysis.sangfor.com
		Terms of Use and Privacy Policy	https://clt.sangfor.com
		IOC rule upgrade	https://intelligence.sangfor.com.cn
		Patches, signatures, and antivirus databases	http://download.sangfor.com https://download.sangfor.com

Table 4: Network Connectivity Requirements

2.1.4 File Whitelist Setting

To avoid false positives during virus scans, collect trusted files such as virus-free business software and previously whitelisted files from other antivirus

products, log in to Endpoint Secure Manager that you have deployed and activated, and add the trusted files in Policies > Detection Policies > File Hashes or Policies > Exclusions. Added trusted files will not be scanned.

IOC Blacklist/ Whitelist	MD5 Hash	Action	Applicable Scope
Security tool	62e153936f09ae701770c5ce014f98ff	Alert	Security department group
IT O&M tool	37bb0bbc1255fdb1693aa45a70bedd91	Allow	IT department group
hacker.exe	6581c35e063322bc6c4f100c4aa48340	Alert and Fix	Security department group
Exclusion	Excluded Path/Suffix		Applicable Scope
The home folder	/home		Server group
Installation packages	.pkg		IT department group

2.2 Endpoint Secure Manager Deployment

2.2.1 Software Deployment

You can implement software deployment for deploying Endpoint Secure Manager in three ways: OVA image-based, ISO image-based, and script-based. Their scenarios are as follows.

1. OVA image-based deployment: Applicable to scenarios involving virtualization platforms such as VMware and HCI.
2. ISO image-based deployment: Applicable to scenarios involving physical servers or virtualization platforms.
3. Script-based deployment: Applicable to environments that do not support OVA and ISO image-based deployment.

Recommendations and differences:

1. Strongly recommended: OVA image-based deployment. As the OVA package contains Endpoint Secure Manager and the underlying Ubuntu system, you can directly use Endpoint Secure Manager after importing the