© 2017 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page http://www.checkpoint.com/copyright.html for a list of our trademarks.

Refer to the Third Party copyright notices http://www.checkpoint.com/3rd_party_copyright.html for a list of relevant copyrights and third-party licenses.
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 Version of this Document
Download the latest version of this document
To learn more, visit the Check Point Support Center

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>23 July 2017</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>
Introduction

The SMP (Security Management Portal) is a web-based management solution to easily manage Small and Medium Business security appliances. You can configure, monitor and provide services to thousands of customers.

Please read this document carefully before you use the R12.30 Check Point SMP.

Important Solutions


What's New in R12.30

Manage Firewall Access Policy from the SMP

- Configure rules for outgoing, incoming, internal and VPN traffic for gateway or plan.


VPN Community Enhancements

- Allow a gateway to participate in multiple VPN communities.
- Support routing traffic to other satellites through the center.
- Support routing traffic to the internet through an externally managed center.

SandBlast Zero-day Protection Threat Emulation

- Threat Emulation analyzes potentially malicious files, stopping dangerous attacks before malware has an opportunity to deploy.
- SandBlast Threat Emulation uses OS-level inspection to examine a broad range of file types, including executables and data files.
- Files are inspected in a virtual sandbox to discover malicious behavior and suspect files are blocked before they enter your network.
SMP Server Requirements

Make sure that you meet the server and network requirements before you install SMP Server.

Windows Server Requirements

  - CPU - At least 4 cores
  - Memory - Minimum 8GB, recommended 16 GB
- Disk space
  - Minimum 100GB
  - Additional disk space is required to store gateway logs. The amount depends on: number of managed gateways, amount of time that logs are stored, and the amount of logs generated by each gateway
    For example, to store one month of logs for 100 typical gateways requires 100 GB of additional disk space.
- The SMP Server log receiving module supports up to 2000 gateways. For SMP deployments that manage more than 2000 gateways, it is necessary to use additional SMP servers.
- VMs (virtual machines) are fully supported by the SMP.

Dynamic DNS Requirements

For deployments that use Dynamic DNS, the interface that communicates with the gateways must have two IP addresses: external and Dynamic DNS. The SMP uses the Dynamic DNS IP address to communicate with the gateways.

When there are multiple IP addresses on an interface, Windows 2008 Server automatically selects which one connects to the gateways. The SMP must use the external IP address to connect to the gateways.

- Make sure that the external IP address is closer to the default Gateway IP address than the Dynamic DNS IP address.
- We recommend that the external IP address is on the same subnet as the default Gateway. The Dynamic DNS IP address uses a different subnet.

For more about how Windows uses multiple IP addresses on one interface, go to Microsoft kb969029 https://support.microsoft.com/en-us/kb/969029.

Note - The previous link is to the Microsoft Support web site. Check Point is not responsible for the information on that web site.
Configuring the Firewall for SMP Server

SMP Server is protected by the Windows firewall and sometimes by a corporate firewall as well. For both firewalls, make sure these ports are open and allow connections between the gateways and the SMP. For the Windows firewall, the ports for outbound traffic are open by default.

### Open Ports for Inbound Traffic

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>SmartDashboard Object</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>53</td>
<td>DNS</td>
<td>domain-tcp</td>
<td>TCP traffic</td>
</tr>
<tr>
<td>257</td>
<td>N/A</td>
<td>FW1_log</td>
<td>TCP traffic - Security logs</td>
</tr>
<tr>
<td>443</td>
<td>SSL</td>
<td>ssl_v3</td>
<td>TCP traffic</td>
</tr>
<tr>
<td>514</td>
<td>N/A</td>
<td>syslog</td>
<td>UDP traffic - System logs</td>
</tr>
<tr>
<td>18191</td>
<td>N/A</td>
<td>CPD</td>
<td>TCP traffic - SIC</td>
</tr>
<tr>
<td>18192</td>
<td>N/A</td>
<td>CPD_amon</td>
<td>TCP traffic - SIC</td>
</tr>
<tr>
<td>18210</td>
<td>N/A</td>
<td>FW1_ica_pull</td>
<td>TCP traffic - SIC</td>
</tr>
<tr>
<td>18211</td>
<td>N/A</td>
<td>FW1_ica_push</td>
<td>TCP traffic - SIC</td>
</tr>
<tr>
<td>18264</td>
<td>N/A</td>
<td>FW1_ica_services</td>
<td>TCP traffic - SIC</td>
</tr>
</tbody>
</table>

### Open Ports for Outbound Traffic

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>SmartDashboard Object</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>SMTP</td>
<td>smtp</td>
<td>TCP traffic - Standard ports for outgoing SMTP. If the port in your network is different, make sure that it is open</td>
</tr>
<tr>
<td>443</td>
<td>SSL</td>
<td>ssl_v3</td>
<td>TCP traffic - HTTPS traffic that connects to the Check Point UserCenter and other Web services</td>
</tr>
<tr>
<td>18191</td>
<td>N/A</td>
<td>CPD</td>
<td>TCP traffic - SIC</td>
</tr>
</tbody>
</table>
Active Directory on SMP Server

SMP uses AD to store the information and data about the gateways that it manages. You must install AD on the server before you install the SMP.

For deployments that use more than one SMP Server, make sure that the AD is installed on the primary server.

Network Requirements

Make sure that these network requirements are met before you install SMP Server:

- Access to an SMTP server (can be in an external network)
- The Windows server DNS name is able to delegate from smbservice.pnt.com to SMP Server
- The SMP uses AD to help manage the gateways. There must be an AD user that is used only for the SMP and define it as:
  - schema admin
  - domain admin
  - Enable feature Password never expires

- Optional - File with the company logo for the Custom Reports feature
- Optional - FTP server to backup the gateway settings

Configuring IIS Ports on SMP Server

Before you install SMP on the server, make sure that Microsoft IIS (Internet Information Services) does not use ports 80 and 8080. The Installation wizard cannot complete the process if IIS uses these ports.

For more about how to configure the IIS ports, go to Microsoft kb149605 https://support.microsoft.com/en-us/kb/149605.

Note - The previous link is to the Microsoft Support web site. Check Point is not responsible for the information on that web site.