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=TBD
For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/24/2012</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

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 How To Configure IPSO as a DHCP Server ).
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>How To Configure IPSO as a DHCP Server</td>
<td>5</td>
</tr>
<tr>
<td>Objective</td>
<td>5</td>
</tr>
<tr>
<td>Supported Versions</td>
<td>5</td>
</tr>
<tr>
<td>Supported Operating Systems</td>
<td>5</td>
</tr>
<tr>
<td>Supported Appliances</td>
<td>5</td>
</tr>
<tr>
<td>Before You Start</td>
<td>5</td>
</tr>
<tr>
<td>Related Documents and Assumed Knowledge</td>
<td>5</td>
</tr>
<tr>
<td>Impact on the Environment and Warnings</td>
<td>5</td>
</tr>
<tr>
<td>Overview</td>
<td>6</td>
</tr>
<tr>
<td>Configuring IPSO as a DHCP Server</td>
<td>6</td>
</tr>
<tr>
<td>Completing the Procedure</td>
<td>11</td>
</tr>
<tr>
<td>Verifying the Procedure</td>
<td>11</td>
</tr>
<tr>
<td>Index</td>
<td>15</td>
</tr>
</tbody>
</table>
How To Configure IPSO as a DHCP Server

Objective

Dynamic Host Configuration Protocol (DHCP) for Check Point IPSO provides a complete DHCP Client and DHCP Server capabilities for your Check Point appliance.

This document explains how to configure IPSO to serve as a DHCP Server.

Supported Versions

IPSO 3.8 and later

Supported Operating Systems

IPSO

Supported Appliances

Any appliance that is operated by IPSO

Before You Start

Related Documents and Assumed Knowledge

- Client host unable to obtain address from IPSO DHCP Server (DHCPREQUEST) - SK40456
  http://supportcontent.checkpoint.com/solutions?id=SK40456
- Please explain why the DHCP Server accepts and processes a DHCP Request even if a FireWall-1 rule blocks DHCP traffic - sk41541 (http://supportcontent.checkpoint.com/solutions?id=SK41541)
- How should I configure a DHCP server with VRRP? - sk44366 (http://supportcontent.checkpoint.com/solutions?id=SK4436)
- Where can I see what IPs the DHCP Server has leased? - sk41194 (http://supportcontent.checkpoint.com/solutions?id=SK41194)

Impact on the Environment and Warnings

Since DHCP operates over UDP and IP, it provides a security risk. For instance, one could use IPSec at layer three to provide authentication. The solution to these risks is to provide security at lower layers. For example, one of the most important techniques to prevent unauthorized servers and clients is careful control over physical access to the network, layer one security. Security techniques implemented at layer two may also be of use.
Overview

DHCP was first defined as a standard track protocol in RFC 1531 in October 1993.

Dynamic Host Configuration Protocol automates network-parameter assignment to network devices from one or more DHCP Servers. Even in small networks, DHCP is useful because it makes it easy to add new machines to the network. When a DHCP-configured client (a computer or any other network-aware device) connects to a network, the DHCP Client sends a broadcast query that requests necessary information from a DHCP Server. The DHCP Server manages a pool of IP addresses and information about client configuration parameters such as, default gateway, domain name, the name servers, and other servers such as, time servers, and so on. When the server receives a valid request, it assigns the computer an IP address, a lease (length of time for which the allocation is valid), and other IP configuration parameters such as, the subnet mask and the default gateway. The query is typically initiated immediately after you boot, and must complete before the client can initiate IP-based communication with other hosts.

Configuring IPSO as a DHCP Server

1. Log into Voyager.
2. In the Voyager tree view, select Configuration > System Configuration > DHCP. The DHCP Configuration window opens.
3. Select the network interface for the server to listen on. The **DHCP Interface Configuration** window opens.
4. Select **Server**, enter the details in the **Client ID**, **Timeout**, **Retry**, **Lease**, and **Reboot** fields, and click **Apply**. The **DHCP Configuration** window opens.
5. In **DHCP Server Subnet Configuration**, select **Add a New Subnet Entry**. The **Add New Entry** window opens.
6. In New Subnet Entry and IP-Pool Configuration, select the Enable check boxes, and enter the details in the Subnet, Mask Length, and Start fields. Click Apply. The DHCP Configuration window opens.

Add New Entry

- **New Subnet Entry**
  - Subnet: 10.10.30
  - Mask Length: 24
  - Enable: 
  - Default Lease: 
  - Maximum Lease: 

- **IP-Pool Configuration**
  - New Pool: Enable: 
  - Start: 10.10.100
  - End: 10.10.150

- **Initial Root Configuration**
  - TFTP Server: 
  - File Name: 
  - Extensions Path: 
  - Root Filename: 

- **System Setup Configuration**
  - Default Gateway: 10.10.1
  - Domain: 
  - Time Offset: 
  - Swap Server: 
  - DNS Servers: 4.2.2.2
  - NTP Servers: 
  - SMTP Servers: 

---

How To Configure IPSO as a DHCP Server | 10
Completing the Procedure

To make sure that the DHCP traffic is accepted by the firewall rules, check SK41541 (http://supportcontent.checkpoint.com/solutions?id=SK41541) - Please explain why the DHCP Server accepts and processes a DHCP Request even if a FireWall-1 rule blocks DHCP traffic.

Verifying the Procedure

There are several ways to verify the success of the procedure.

- Add a client PC to make a DHCP request to the network.
- On the server, to check if DHCP operates, run: `ps -auwx. It shows: /bin/dhcpd -d -cf /var/etc/dhcpd.conf running`
Verifying the Procedure

- In Wireshark, you can see the client with a source IP of 0.0.0.0 to destination 255.255.255.255.

In the dhcp.leases file, to check what IPs are given out, run: `pwd`

```
slim[admin]# pwd
/preserve/var/etc
slim[admin]# more dhcpd.leases
# All times in this file are in UTC (GMT), not your local timezone. This is
# not a bug, so please don't ask about it. There is no portable way to
# store leases in the local timezone, so please don't request this as a
# feature. If this is inconvenient or confusing to you, we sincerely
# apologize. Seriously, though - don't ask.
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-V3.0.1rc11
lease 172.16.100.148 {
    starts 5 2007/03/02 16:42:33;
    ends 6 2007/03/03 04:42:33;
    tstp 6 2007/03/03 04:42:33;
    binding state free;
    hardware ethernet 00:0c:29:f3:e3:81;
}
lease 172.16.100.149 {
    starts 5 2007/03/23 19:19:56;
    ends 6 2007/03/24 07:19:56;
    tstp 6 2007/03/24 07:19:56;
    binding state free;
    hardware ethernet 00:11:25:16:fc:c5;
```
uid "\001\000\021\026\374\305";
}
lease 172.16.100.150 {
    starts 1 2007/05/21 12:56:57;
    ends 2 2007/05/22 00:56:57;
    binding state active;
    next binding state free;
    hardware ethernet 00:0e:7b:21:f2:1e;
    uid "\001\000\016!/\362\036";
    client-hostname "KOT-GLP";
}
slim[admin]#