How To Configure Non Local IPSO Radius Authentication

9 May 2012
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=12296
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>9 May 2012</td>
<td>Improved formatting and document layout.</td>
</tr>
<tr>
<td>24 April 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 Non Local IPSO Radius Authentication ).
### 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 Non Local IPSO Radius Authentication</td>
<td>5</td>
</tr>
<tr>
<td>Objective</td>
<td>5</td>
</tr>
<tr>
<td>Supported Versions</td>
<td>5</td>
</tr>
<tr>
<td><strong>Before You Start</strong></td>
<td>5</td>
</tr>
<tr>
<td>Assumed Knowledge</td>
<td>5</td>
</tr>
<tr>
<td>Related Documentation</td>
<td>5</td>
</tr>
<tr>
<td>Impact on the Environment and Warnings</td>
<td>6</td>
</tr>
<tr>
<td>Configuring IPSO</td>
<td>6</td>
</tr>
<tr>
<td>Configuring FreeRadius on FreeBSD</td>
<td>11</td>
</tr>
<tr>
<td>Configuring the Radius Role in Windows Server 2008 R2</td>
<td>15</td>
</tr>
<tr>
<td>How to troubleshoot Non Local IPSO Radius Authentication</td>
<td>18</td>
</tr>
</tbody>
</table>
How To Configure Non Local IPSO Radius Authentication

Objective

This document explains how to configure IPSO to authenticate non-local users as administrators, using Radius protocol, against a FreeRadius server, and a Windows Server 2008 R2 server.

Supported Versions

- IPSO 6.2
- FreeRadius 2.1.9 on FreeBSD
- Windows Server 2008 R2 Standard

Before You Start

Assumed Knowledge

You should have a moderate amount of knowledge about troubleshooting, Unix, and networking.

Related Documentation

sk40129 How to configure FreeRADIUS for non-local user authentication from an IP Security Platform? (http://supportcontent.checkpoint.com/solutions?id=sk40129)
sk44136 IPSO Non local user is not able to run shell commands (http://supportcontent.checkpoint.com/solutions?id=sk44136)
sk40167 Why am I being put into cli mode when I log in as a Non-Local User (http://supportcontent.checkpoint.com/solutions?id=sk40167)
sk38526 AAA Voyager Authentication function fails to initiate connection to Radius Server (http://supportcontent.checkpoint.com/solutions?id=sk38526)
sk43270 ls radius traffic from and edge to radius server encrypted (http://supportcontent.checkpoint.com/solutions?id=sk43270)
sk33579 SPLAT Firewall Admin Authorization via RADIUS (http://supportcontent.checkpoint.com/solutions?id=sk33579)
sk40665 How to configure RADIUS authentication in Network Voyager using AAA (http://supportcontent.checkpoint.com/solutions?id=sk40665)
sk40697 How to configure a SmartConsole admin user to authenticate to an external RADIUS server (http://supportcontent.checkpoint.com/solutions?id=sk40697)
sk13740 Radius authentication fails when using passwords consisting of more than 16 characters (http://supportcontent.checkpoint.com/solutions?id=sk13740)
sk33965 Authentication fails when user tries authenticate using client authentication to the Radius server (http://supportcontent.checkpoint.com/solutions?id=sk33965)
sk40180 How to configure Radius authentication with Microsoft Active Directory (http://supportcontent.checkpoint.com/solutions?id=sk40180)
Configuring IPSO

Impact on the Environment and Warnings

There is a possibility of locking yourself out of the system by misconfiguring authentication. Make a full backup before proceeding. Console access should never be blocked by doing the actions in this document.

You must have end-to-end IP connectivity between the IPSO system and the Radius server, and any firewalls must allow the traffic through.

Configuring IPSO

1. Take a full system backup before you start.
2. Navigate to Voyager > Configuration > Security and Access > AAA

   ![AAA Configuration](image)

   We only need to make changes in the AAA page to support Non Local Radius Authentication

3. First, create a new "Authentication Profile Configuration":

   ![Add New Authentication Profile](image)

   - For "New Auth Profile" enter radius_authprofile
   - For "Type" select RADIUS
   - Leave "File" blank
   - For "Control" select "sufficient"
- Click Save at the bottom

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Control</th>
<th>File</th>
<th>Delete</th>
<th>Server Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>base_file_authprofile</td>
<td>UNIX</td>
<td>required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>base_http_authprofile</td>
<td>UNIX</td>
<td>required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>base_login_authprofile</td>
<td>UNIX</td>
<td>required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>base_other_authprofile</td>
<td>UNIX</td>
<td>required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>base_ssd_authprofile</td>
<td>UNIX</td>
<td>required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>talk_file_authprofile</td>
<td>TALLY</td>
<td>required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>talk_http_authprofile</td>
<td>TALLY</td>
<td>required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>talk&gt;Login_authprofile</td>
<td>TALLY</td>
<td>required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>talk_ssd_authprofile</td>
<td>TALLY</td>
<td>required</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Add New Authentication Profile

New Auth Profile: radius_authprofile
Type: RADIUS
File: 
Control: sufficient

4. Next, click the new "Servers" link next to the Authentication Profile that you created.

Add New Server

Priority:  
Host Address:  
Port: admin  
Secret:  
Timeout: 3  
Max Tries: 3

AAA RADIUS Auth. Servers Configuration

RADIUS Servers for Auth. Profile "radius_authprofile"

5. Under the "AAA RADIUS Auth. Servers Configuration" page, under "Add a New Server:
   - Set the priority to 1
   - Set the IP address of the Radius server  
   - Set the port to 1812
   - Enter the Secret key that will be used to communicate with the Radius server
   - Set the Timeout to 3
   - Set the Max Tries to 3
Click Save at the bottom.

### AAA RADIUS Auth. Servers Configuration

#### RADIUS Servers for Auth. Profile "radius_authprofile"

<table>
<thead>
<tr>
<th>Priority</th>
<th>Host Address</th>
<th>Port</th>
<th>Secret</th>
<th>Timeout</th>
<th>Max Tries</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>172.28.207.66</td>
<td>1812</td>
<td>✧✦✦✦✦</td>
<td>✦</td>
<td>✦</td>
<td>✦</td>
</tr>
</tbody>
</table>

6. Go back to the main AAA page.
7. Next, update the “Service Profile Configuration”:
   - Create a new Service Profile:
     - Set "Service Profile" to "radius_prof_httpd"
     - Set "Auth Profile" to "radius_authprofile"
     - Set "Acct. Profile" to "base_httpd_acctprofile"
     - Set "Session Profile" to "base_httpd_sessprofile"
How To Configure Non Local IPSO Radius Authentication

- Click Save at the bottom

8. Now we need to add the fallback local authentication:
   - Set "Service Profile" to "radius_prof_httpd".
   - Set "Auth Profile" to "base_httpd_authprofile".
- Click Save at the bottom.
9. The last step to configure IPSO is to set the “Service Module Configuration” at the top.

- Change the Service httpd to use "radius_prof_httpd"
- Click Save at the bottom.

All the IPSO configurations are now complete for HTTP access. The same steps are needed for sshd access, except that you do not need to redefine an "Authentication Profile Configuration" as you can re-use the one you already created.

Configuring FreeRadius on FreeBSD

For the purposes of lab testing, a VMWare image of FreeBSD is perfectly acceptable. This serves as a demonstration of how to do the configuration, which can be equally applied to another BSD flavor like OpenBSD or NetBSD, or a Linux system.

The FreeBSD image that was used

```
freebsd81# uname -a
FreeBSD freebsd81.checkpoint.com 8.1-RELEASE FreeBSD 8.1-RELEASE #0: Mon Jul 19 02:36:49 UTC 2010 root@mason.cse.buffalo.edu:/usr/obj/usr/src/sys/Generic amd64
freebsd81#
```

The FreeRadius server was installed by downloading the package from the FreeBSD packages collection.

The following 4 files were modified:

- `/usr/local/etc/raddb/users`
- `/usr/local/etc/raddb/dictionary`
- `/usr/local/etc/raddb/dictionary.nokia`
- `/usr/local/etc/raddb/clients.conf`

```
/usr/local/etc/raddb/users:
```
Configuring FreeRadius on FreeBSD

How To Configure Non Local IPSO Radius Authentication

```
testing Cleartext-Password := "password"
Nokia-IPSO-User-Role = adminRole,
Nokia-IPSO-SuperUser-Access = 1
```

```
$INCLUDE /usr/local/share/freeradius/dictionary
$INCLUDE dictionary.nokia
```

```
VENDOR          Nokia
BEGIN-VENDOR    Nokia
ATTRIBUTE       Nokia-IMSI                      224     octets
ATTRIBUTE       Nokia-Charging-Id               225     integer
ATTRIBUTE       Nokia-Prepaid-Ind               226     integer
ATTRIBUTE       Nokia-GGSN-IP-Address           227     ipaddr
ATTRIBUTE       Nokia-SGSN-IP-Address           228     ipaddr
ATTRIBUTE       Nokia-IPSO-User-Role             229     string
ATTRIBUTE       Nokia-IPSO-SuperUser-Access     230     integer
END-VENDOR      Nokia
```

```
client 0.0.0.0/0 {
    secret = testing123
    shortname = private-network-1
}
```

Then the server was started up in debug mode:

```
freebsd81# ./radiusd -fX
FreeRADIUS Version 2.1.9, for host amd64-portbld-freebsd8.1, built on Jun 13 2010 at 07:37:24
Copyright (C) 1999-2009 The FreeRADIUS server project and contributors.
There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A
PARTICULAR PURPOSE.
You may redistribute copies of FreeRADIUS under the terms of the
GNU General Public License v2.
Starting - reading configuration files ...
... Listening on authentication address * port 1812
Listening on accounting address * port 1813
Listening on command file /var/run/radiusd/radiusd.sock
Listening on proxy address * port 1814
Ready to process requests.
```

An attempt was made to authenticate using the LOCAL user admin:
rad_recv: Access-Request packet from host 172.26.207.60 port 52732, id=73, length=77
  User-Name = "admin"
  User-Password = "password"
  NAS-Identifier = "ipso6-vm-student10"
  NAS-IP-Address = 172.26.207.60
  Service-Type = Login-User
++ entering group authorize {...}
++[preprocess] returns ok
++[chap] returns noop
++[mschap] returns noop
[suffix] No '@' in User-Name = "admin", looking up realm NULL
[suffix] No such realm "NULL"
++[suffix] returns noop
[eap] No EAP-Message, not doing EAP
++[eap] returns noop
++[unix] returns notfound
++[files] returns noop
++[expiration] returns noop
++[logintime] returns noop
[pap] WARNING! No "known good" password found for the user. Authentication may fail because of this.
++[pap] returns noop
No authenticate method (Auth-Type) configuration found for the request: Rejecting the user
Failed to authenticate the user.
Using Post-Auth-Type Reject
++ entering group REJECT {...}
[attr_filter.access_reject] expand: %{User-Name} -> admin
  attr_filter: Matched entry DEFAULT at line 11
++[attr_filter.access_reject] returns updated
Delaying reject of request 0 for 1 seconds
Going to the next request
Waking up in 0.9 seconds.
Sending delayed reject for request 0
Sending Access-Reject of id 73 to 172.26.207.60 port 52732
Waking up in 4.9 seconds.
Cleaning up request 0 ID 73 with timestamp +6
Ready to process requests.

The admin user failed the Radius auth request, but the "fallback" in the IPSO configuration we created is to use local accounts (base_httpd_authprofile after radius_authprofile).

Then the testing NON-LOCAL user logged in:
rad_recv: Access-Request packet from host 172.26.207.60 port 49767, id=24, length=79
  User-Name = "testing"
  User-Password = "password"
  NAS-Identifier = "ipso6-vm-student10"
  NAS-IP-Address = 172.26.207.60
  Service-Type = Login-User
++ entering group authorize {...}
++ [preprocess] returns ok
++ [chap] returns noop
++ [mschap] returns noop
[suffix] No '@' in User-Name = "testing", looking up realm NULL
[suffix] No such realm "NULL"
++ [suffix] returns noop
[eap] No EAP-Message, not doing EAP
++ [eap] returns noop
++ [unix] returns notfound
[files] users: Matched entry testing at line 50
++ [files] returns ok
++ [expiration] returns noop
++ [logintime] returns noop
++ [pap] returns updated
Found Auth-Type = PAP
++ entering group PAP {...}
[pap] login attempt with password "password"
[pap] Using clear text password "password"
[pap] User authenticated successfully
++ [pap] returns ok
++ entering group post-auth {...}
++ [exec] returns noop
Sending Access-Accept of id 24 to 172.26.207.60 port 49767
  Nokia-IPSO-User-Role = "adminRole"
  Nokia-IPSO-SuperUser-Access = 1
Finished request 1.
Going to the next request
Waking up in 4.9 seconds.
Cleaning up request 1 ID 24 with timestamp +29
Ready to process requests.

The testing user was able to log into Voyager as an administrator.
You MUST enable the RADIUS role. After this is done, configure the system in a similar way to the following screenshots:
Configuring the Radius Role in Windows Server 2008 R2

How To Configure Non Local IPSO Radius Authentication
Configuring the Radius Role in Windows Server 2008 R2

How To Configure Non Local IPSO Radius Authentication
How to troubleshoot Non Local IPSO Radius Authentication

Your first step should be tcpdump
How to troubleshoot Non Local IPSO Radius Authentication

Here is a failed session:

| Frame 2 (62 bytes on wire, 62 bytes captured) |
| Ethernet II, Src: NokiaInt_81:70:ee (00:0c:29:00:00:00), Dst: NokiaInt_70:62:6e (00:0c:29:00:00:00) |
| User Datagram Protocol, Src Port: radius (1812), Dst Port: tcp (1112) |
| Radius Protocol |
| Code: Access-Request (3) |
| Packet Identifier: b31 (17) |
| Length: 20 |
| Authenticator: 46221AAA05F3E4B2083DE8805D87F0A0 |
| This is a response to a request in Frame 11 |
| Time from request: 6.014648000 seconds |

And here is a successful session.

| Frame 2 (62 bytes on wire, 62 bytes captured) |
| Ethernet II, Src: NokiaInt_81:70:ee (00:0c:29:00:00:00), Dst: NokiaInt_70:62:6e (00:0c:29:00:00:00) |
| User Datagram Protocol, Src Port: radius (1812), Dst Port: tcp (1112) |
| Radius Protocol |
| Code: Access-Accept (3) |
| Packet Identifier: 0x37 (137) |
| Length: 49 |
| Authenticator: 921D3ED28B303D7F7937A7F7F0F12A |
| This is a response to a request in Frame 11 |
| Time from request: 6.021980000 seconds |

From looking at the tcpdump captures you will be able to see if the problem is with the Attributes or with a simple failed password.