Implementation of RADIUS group authentication on Check Point appliances

Vložil/a cm3l1k1 [1], 24 Říjen, 2012 - 13:01

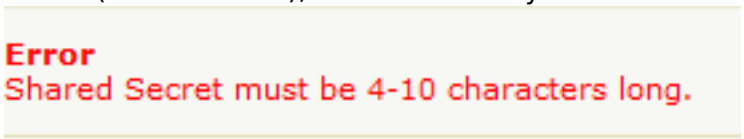
- Check Point [2]
- Networks & Protocols [3]

As usual manuals, knowledge bases and other sources aren't describing this topic very well, so each of us must debug how Check Point implement it in their own way.
I will show you where and how to setup RADIUS authentication on Check Point appliances as well as on RADIUS server itself (FreeRADIUS [4]) step-by-step. This is also some kind of my own notes for further deployments :]

// Mission

First of all we will point Check Point appliances to RADIUS server, setup shared secret and group relation expected in response from RADIUS server. RADIUS group is something what Check Point expecting in successful authentication message from RADIUS in Class attribute. For our purposes we use group name “fwadmins”.

» Notice
There is non-sense limitation on current version of Check Point SecurePlatform for length of shared secret (10 chars max), so be sure that you will not exceed it.

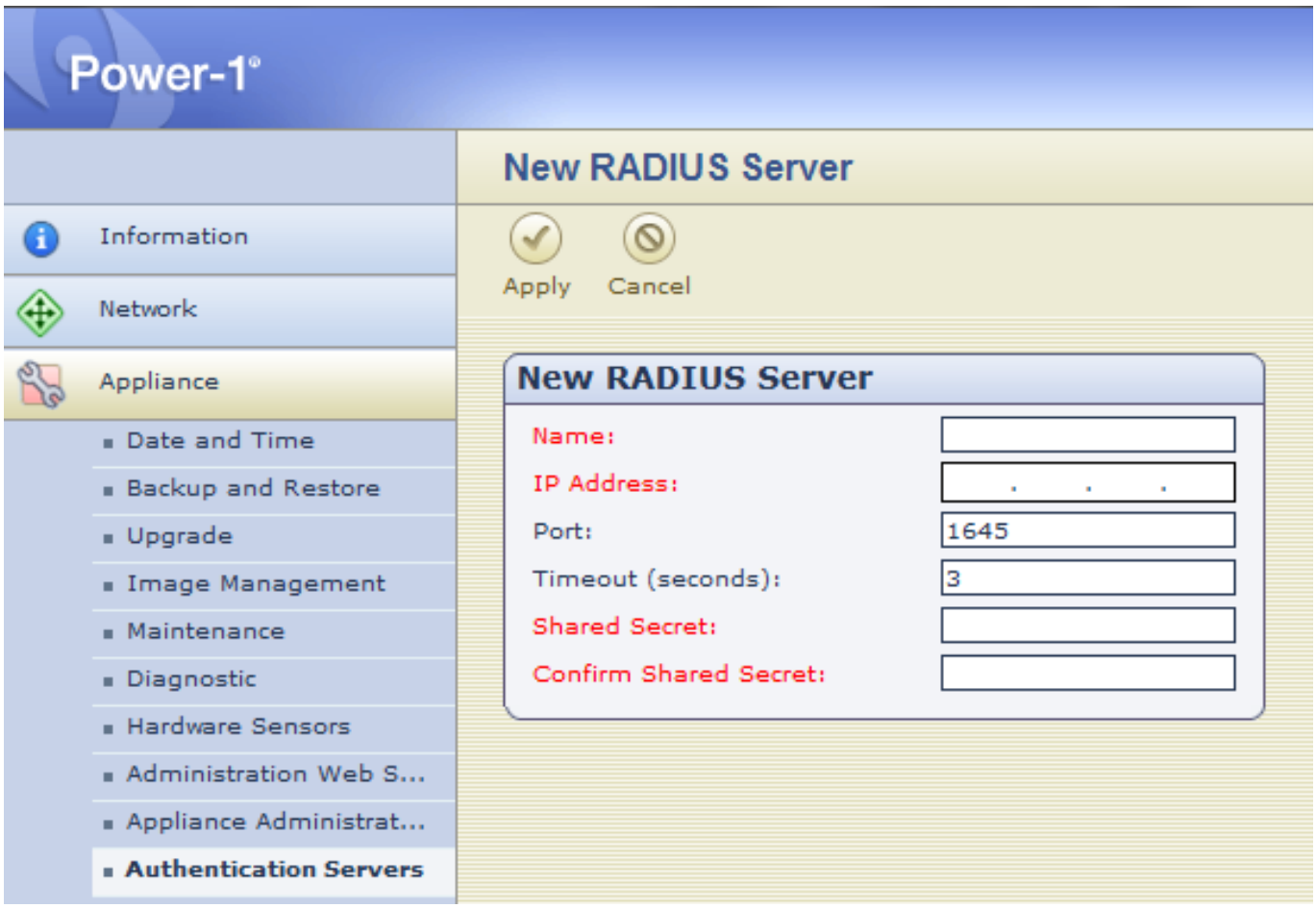


// Setup on Check Point

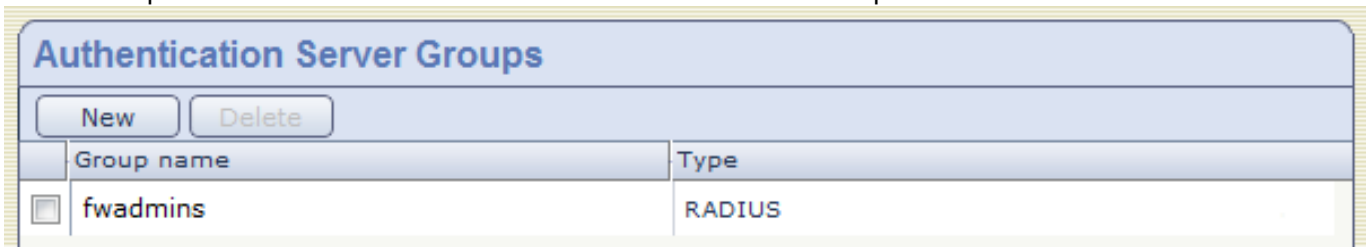
First of all allow access from appliances (and cluster object as well) to RADIUS server.

» Via WebUI

Visit appliance WebUI https://appliance-name.company.com [5], enter credentials and go to Appliance -> Authentication Servers
Click on “New” button in Authentication servers table



When completed add "fwadmins" to "Authentication Server Groups".



Don’t forget to setup the same on both cluster members!

» Via CLI

As usual via CLI is this operation 10x faster. Just run those two commands:
`radius servers add 2.2.2.256:1812 SHARED-SECRET 3 Radius`
`radius groups add fwadmins`
To double-check your setup run: radius servers show and radius groups show
After that login to second node and execute commands as well.

» Summarize Network information

Imagine this scenario of traffic flow:

```
Management Server (MDS) [1.1.1.256] <---> [1.1.1.1] Check Point appliance cluster
[2.2.2.2] ---> [2.2.2.256] RADIUS server
```

Where CP cluster have 2 interfaces facing RADIUS:
`2.2.2.2 - custer VIP`

```
2.2.2.3 - active node
2.2.2.4 - standby node
```

and 2 interfaces facing MGMT server:

```
1.1.1.1 - cluster VIP
1.1.1.2 - active node
1.1.1.3 - standby node
```

You must distinguish between management IP addresses and addresses from which appliance will contact RADIUS in case of authentication attempt.
Management interface:
Interface for communication with management server. In our example **1.1.1.1**

Routing interfaces (find interface facing RADIUS server):

```
[Expert@cp-firewall-a]# ip route get 2.2.2.256
2.2.2.256 via dev Exp1-2 src 2.2.2.3
   cache  mtu 1500 advmss 1460
```

BUT source of authentication attempt will be cluster interface of 2.2.2.3
To find which one is it, run:

```
[Expert@cp-firewall-a]# cphaprob -a if | grep 2.2.2.

Exp1-2          2.2.2.2
```

So cluster interface in this case is **2.2.2.2**
From this address will be contacted RADIUS, so we have to define it in clients.conf.

// Configuration on RADIUS

- **2.2.2.2** - is cluster VIP making connection to RADIUS (doesn't matter if you're authenticating against active or standby node) which has to be defined in RADIUS **clients.conf**
- **1.1.1.2 and 1.1.1.3** - are management IPs which has to be defined in RADIUS **huntgroups** file because authentication is provided to them and not to cluster VIP making connection

Example in clients.conf:
we will use Check Point cluster IP facing RADIUS server

```
client 2.2.2.2 {
        secret          = SHARED-SECRET
        shortname       = cp-firewall-vip
        vendor          = CheckPoint
}
```

Example in huntgroups:
we will use Check Point cluster management IP

```
CHECKPOINT NAS-IP-Address == 1.1.1.2
CHECKPOINT NAS-IP-Address == 1.1.1.3
```

"fwadmin" class value is taken from freeradius "**/etc/raddb/users**" file where we define relation of Class attribute to user account.

Example of users:

```
martin.cmelik Huntgroup-Name == CHECKPOINT
              Class = fwadmins
```

So when I try login to CP firewall, appliance will send my username and password to RADIUS, where will be authenticated against LDAP/PAM/SQL/whatever and when it is OK from "users" file add Class attribute "fwadmins" if authentication client match huntgroup "CHECKPOINT".
In fact "fwadmins" can be attribute in LDAP as well, you just need to correctly filter and translate response from LDAP server on RADIUS. It's up to you.

// Appendix

» Traffic visible on RADIUS

```
radius ~# tcpdump -s 0 -X -nni bond0 host 2.2.2.2

14:26:42.898208 IP 2.2.2.2.26367 > 2.2.2.256.1812: RADIUS, Access Request (1), id:
0x94 length: 90
        0x0000:  4580 0086 481b 4080 ff81 083d a588 d281  E..cT.@....=.H..
        0x0010:  a548 0c0c 668f 0714 0062 821f 0194 005a  .G..f....b.....Z
        0x0020:  680f 9a35 989b 15ab 3893 f514 956d db86  e..5....9....m..
        0x0030:  0109 6863 6d65 6c69 6b02 121f a279 db36  ..martin.cmelik.
        0x0040:  7849 b873 3835 e877 6834 7384 0602 fc3f  kI.s12.dt2s....?
        0x0050:  0520 0673 7368 6405 0600 003b 273d 0600  ...sshd....;'=..
        0x0060:  0000 0586 0600 0800 881f 1831 3618 2137  ...........1.2.3
        0x0070:  312e 382e 3838                           .4...

14:26:42.932269 IP 2.2.2.256.1812 > 2.2.2.2.26367: RADIUS, Access Accept (2), id:
0x94 length: 41
        0x0000:  4500 0045 ab07 0000 4011 a682 a548 0c0c  E..E....@....H..
        0x0010:  a548 d281 0714 66ff 0031 d43e 0294 0029  .H....f..1.>...)
        0x0020:  28c8 384f 58ca 71f3 d02c 719c 7d0a 5aa9  (.8OX.q..,q.}.Z.
        0x0030:  0b0b 5650 4e52 454d 4f54 4119 0166 7161  ..VPNREMOTE..fwa
        0x0040:  616d 616e 73                             dmins
```

» RADIUS log

Tue Oct 23 14:26:42 2012 : Auth: Login OK: [martin.cmelik] (from client cp-firewall-vip port 15143 cli 1.2.3.4)

EOF

URL článku:
https://security-portal.cz/clanky/implementation-radius-group-authentication-check-point-appliances

Odkazy:
[1] https://security-portal.cz/users/cm3l1k1
[2] https://security-portal.cz/category/tagy/check-point
[3] https://security-portal.cz/category/tagy/networks-protocols
[4] http://freeradius.org/
[5] https://appliance-name.company.com