
[Scenario]

The part of User Authentication is complex and correlates with lots of function in Netdefend series.

In the current scenario, customers are able to have a charge tariff based on the information provided by build-in function of Netdefend series.

[Test Topology]

PC1(192.168.1.50)------(L1:192.168.1.1/24)DFL-1600(W1:1.1.1.1/24)-----
PC2(1.1.1.60)

[Configuration]

The settings of DFL-1600

1. Configure the WAN1 IP address to "1.1.1.1" with subnet mask "1.1.1.0/24"

```
set Interface Ethernet wan1 DHCPEnabled=No
set Address IP4Address InterfaceAddresses/wan1_ip Address=1.1.1.1
set Address IP4Address InterfaceAddresses/wan1net Address=1.1.1.0/24
```

2. Create a PPTP server on WAN1 interface.

```
add Interface L2TPServer pptp-srv Interface=wan1 IP=10.0.0.1 IPPool=10.0.0.50-
10.0.0.100 ServerIP=InterfaceAddresses/wan1_ip TunnelProtocol=PPTP
```

Solution

3. Create an object for linking to Radius, in current case, the Radius server's IP address is 192.168.1.50, Shared Secret is "testtest".

```
add RadiusServer radius-srv1 IPAddress=192.168.1.50 SharedSecret=testtest
```

4. Create an object for linking to Accounting server, in current case, the Accounting server's ip address is 192.168.1.50, Shared Secret is "testtest".

```
add RadiusAccounting radius-account-srv1 IPAddress=192.168.1.50
SharedSecret=testtest
```

5. Create an User Authentication Rule.

```
add UserAuthRule AuthSource=RADIUS Interface=pptp-srv OriginatorIP=all-nets
RadiusServers=radius-srv1 AccountingServers=radius-account-srv1 Agent=PPP
TerminatorIP=InterfaceAddresses/wan1_ip LogEnabled=Yes Name=pptp-auth
```

6. Create an IP4Object and set the UserAuthGroups to "Group1".

```
add Address IP4Address authenticated-users Address=0.0.0.0/0
UserAuthGroups=Group1
```

7. Create an IP rule to allow the authenticated users can ping to LAN1_IP via PPTP tunnel.

```
add IPRule Action=Allow SourceInterface=pptp-srv SourceNetwork=authenticated-
users DestinationInterface=core DestinationNetwork=InterfaceAddresses/lan1_ip
Service=all_icmp Name=allow-ping-lan1 Index=1 LogEnabled=Yes
```

The settings of PC1

1. Configure the IP address to 192.168.1.50/24.
2. Install a Radius server.
3. In /etc/raddb, edit the file of "clients.conf" and add below parameters:

```
#####  
  
client 192.168.1.1 {  
    secret      =teststest  
    shortname   =DFL-1600  
}
```

```
#####
```

4. To add the Dlink Firewall Vendor Specific attributes create a file called /etc/raddb/dictionary.D-Link. It should contain the information below.

```
#####  
  
VENDOR D-Link      5089  
ATTRIBUTE D-Link-User-Group 1  string  D-Link
```

```
#####
```

5. In /etc/raddb, edit the file of "users" and add below parameters:

```
#####  
  
user1 Cleartext-Password := "user1"  
    D-Link-User-Group = "Group1",  
    Service-Type = Framed-User,  
    Framed-Protocol = PPP,
```

```
#####
```

6. Issue the command of "radiusd -X" to enable the Radius daemon.

The settings of PC2

1. PC2 works as a PPTP client, therefore we have to create a PPTP interface on PC2.

[Test procedure]

1. PC2 tries to build up a PPTP tunnel with DFL-1600.(account name:user1/password:user1)
2. PC2 initials the ICMP traffic to LAN1_IP of DFL-1600.
3. PC2 terminates the PPTP tunnel.

[Result]

After the tunnel established, issue the command of "userauth -list" in CLI, then you will find the user1 with the privilege of "Group1" in DFL.

```
#####
```

```
DFL-1600: /> userauth -list  
Currently authenticated users:
```

Login	Source IP Address	Ses/Idle Interface	Timeouts	Privileges
user1	10.0.0.50	pptp-srv	none/29m	Group1

#####

End of document.
