

HOWTO: Use ZeroShell as a Radius server for Cisco Radius Authentication

By Paul Taylor

ZeroShell can be obtained from:
<http://www.zeroshell.net/eng/>

This document requires ZeroShell version 1.0 beta 6 or later. (Screenshots were taken with a modified version of beta 5.)

Cisco routers support using Radius servers for user authentication. It is possible to configure the radius server to automatically give certain users (or groups of users) specific access rights on a Cisco router. To do that would require a very specific configuration on the radius server. In most cases, though, that level of detail is not necessary. In most scenarios you will want to authenticate the person when they log into the router with their own individual user ID, then authenticate again when the user switches to Enable mode. Why would this be desirable? Having a centralized point to enable and disable individual user access or globally change the enable password on all of your routers can greatly simplify effectively dealing with employees leaving a department/company. Using only local users and passwords set on routers themselves is generally considered a bad policy.

The following is a skeleton Radius configuration for Cisco routers that works in my test environment. Please do not ask me how to configure Radius on you router. Note that the example router configuration assumes that no user should ever connect via the AUX port.

```
aaa new-model
aaa group server radius radius-group1
  server ZeroShellIP auth-port 1812 acct-port 1813
aaa authentication login radius-vty local group radius-group1
aaa authentication login radius-con local group radius-group1
aaa authentication login aux none
aaa authentication enable default group radius-group1 enable
aaa authorization console
aaa authorization exec radius-vty local group radius-group1
aaa authorization exec radius-con local group radius-group1
aaa accounting exec radius-vty start-stop group radius-group1
aaa accounting exec radius-con start-stop group radius-group1
aaa session-id common
radius-server host ZeroShellIP auth-port 1812 acct-port 1813 key MySharedSecretPhrase
line con 0
  authorization exec radius-con
  login authentication radius-con
line aux 0
  login authentication aux
line vty 0 4
  authorization exec radius-vty
  login authentication radius-vty
```

In the above example, **ZeroShellIP** should be the actual IP Address of the ZeroShell machine, not a FQDN. Please note that the router must have a route to this address. Also, **MySharedSecretPhrase** is where you should put your SharedSecret phrase. This must be the same on both the router and the ZeroShell machine.

This document assumes that you have configured ZeroShell to the point that you are running on your own database, not the Example database that comes with ZeroShell.

To configure ZeroShell to respond to these radius requests, we must first add users to ZeroShell. For this example, we will simply use the default admin user to gain basic access to the router. In addition to this user, we must add a special user for enable access. Cisco routers are hard coded to send the username “\$enab15\$” along with the user supplied password to gain level 15 access. When this user is added, Zeroshell automatically converts the dollar signs to underscores. Simply add the “\$enab15\$” user to ZeroShell with your desired password. You should end up with a screen that looks like this:

The screenshot shows the ZeroShell web interface. The top bar includes the ZeroShell logo, version information (Release 1.0.beta5), and system status (CPU, Uptime, Load). The main content area is titled 'Enable (_enab15_)' and contains several sections:

- Account:** Username: , UID: , Primary Group: , GID: . Home Directory: , Default Shell: bash, sh, tcsh, other,
- User Information:** Firstname: , Lastname: , Organization: , Description: , E-Mail: , Phone:
- User Password:** Password: , Confirm:
- Enabled Services:** Kerberos 5 Authentication , Host-to-Lan VPN (L2TP/IPsec) , 802.1X Access (VLAN:)

The left sidebar contains a navigation menu with categories: SYSTEM (Setup, Logs, Utilities), USERS (Users, Groups, LDAP / NIS, RADIUS, Captive Portal), NETWORK (Hosts, Router, DNS, DHCP, VPN, QoS), SECURITY (Kerberos 5, Firewall, X.509 CA), and ToDo List (Net Balancer, Web Proxy, Wi-Fi AP, IMAP Server, SMTP Server).

Next, select RADIUS in the left pane.

The screenshot shows the ZeroShell web interface. At the top, it displays 'ZEROSHELL Net Services' and 'Release 1.0.beta5'. The system status shows 'CPU (1) Intel(R) Pentium(R) 4 CPU 2.80GHz 2793MHz', 'Uptime 0 days, 0:4', and 'Load 0.02 0.07 0.03'. The main navigation bar includes 'RADIUS', 'Manage', 'Access Points', and 'Proxy'. The left sidebar lists various system components like 'SYSTEM', 'USERS', 'NETWORK', and 'SECURITY'. The main content area is titled 'RADIUS Server for Wireless and Port Based Network Access Applications'. It shows the RADIUS server status as 'ACTIVE' and 'Enabled'. Under '802.1x Configuration', the 'X.509 Host Certificate' is set to 'Local CA' with 'OU=hosts, CN=radius.winn-dixie.com'. There are buttons for 'View', 'Imported', and 'Trusted CAs'. A 'Some Notes' section explains that the RADIUS server supports EAP-TLS, PEAP, and EAP-TTLS.

Now, select the Access Points item (at the top of the RADIUS page).

In the pop-up window that appears, add your router name, IP Address, and Shared Secret that matches the configured shared secret on your router.

Note: You may use very wide IP addressing here. In my example, I'm opening this up for the entire 10.0.0.0/8 network. This encompasses virtually all of my privately addressed routers. Add as many networks here as you need, with the appropriate shared secrets. (You can set the shared secret be the same for multiple networks.)

The screenshot shows the 'Access Point List' pop-up window. It has a 'Close' button in the top right. Below the title bar is a form with three input fields: 'Access Point Name', 'IP or Subnet', and 'Shared Secret'. To the right of these fields are 'Add', 'Change', and 'Delete' buttons. Below the form is a table with the following data:

	Access Point Name	IP or Subnet	Shared Secret
<input type="radio"/>	AllTenDot	10.0.0.1/8	MySharedSecretPhrase

After closing the Access Point configuration page, you'll be returned to the RADIUS page. The process of adding an AP should restart Radius, but just to be sure, I like to restart it by unchecking the "Enabled" box, then checking it again after the screen refreshes. The resulting screen should show a Status of Active. If it doesn't restart, your shared secret may be too long.

Now, just connect to the console of your router (or ssh/telnet there) and log in using the admin user and password of ZeroShell. After you log in, go into enable mode, using the password for the _enab15_ user.

After you have successfully authenticated, select “Show Requests” on the ZeroShell RADIUS screen, and you should get something like this:

The screenshot shows a web interface titled "LOG VIEWER". At the top, there are several filters: a year dropdown set to "2007", a month dropdown set to "Aug", and a day dropdown set to "21". To the right of these are three more filters: "Host" with a dropdown set to "radius (Local)", "Section" with a dropdown set to "radiusd", and an empty "Filter" text box. Further right are navigation buttons: "<<" and ">>" for page navigation, and "Refresh" and "Close" buttons. A "Configure" link is visible in the top right corner. Below the filters, there is a list of log entries. The first entry is "14:09:08 Login OK: [admin] (from client All10Dot port 66 cli 10.214.72.2)". The second entry is "14:09:13 Login OK: [_enab15_] (from client All10Dot port 66 cli 10.214.72.2)".

There should not be any errors here, unless you mistyped your password while logging into the router.