

SSH - Secure Shell is a network security protocol that allows a secure login from a SSH client to services running on a remote SSH server. The user name/password combination is sent in an encrypted format. The SSH server can be configured to also authenticate the login credentials with a remote Radius account server.

Remote Authentication Dial In User Service (RADIUS) is an AAA (authentication, authorization and accounting) protocol. An SSH Server can optionally validate an SSH Client with a Radius Server before granting remote login access to the SSH Client.

Many networks service providers require that the administration of security credentials (such as usernames and passwords) are handled by a centralized RADIUS server within the provider's network. The importance of this took on greater weight with the creating of the PCI Security Standard by the five major card brands (American Express, Discover, JCB, MasterCard and Visa) in September of 2006. The PCI compliance standards main objective is to stop the cause of online financial and identity theft. They do this by requiring that the systems which process and store customer details and transaction information are secure. As such PCI compliance has become one of the major issues surrounding security.



The Vanguard router's built-in SSH server provides a secure login to allow the establishment of a telnet session between a SSH client and the router's control port. The Vanguard SSH Server can also be configured to authenticate user login credentials with a centralized RADIUS server.

When using RADIUS authentication, the Vanguard SSH server first asks for the user's password and then sends it along with the username to the RADIUS server.

The choices are as follows:

- **Remote-then-Conditional Local** – The Vanguard SSH Server authenticates the SSH Client login via RADIUS. If the authentication fails **solely** because of a disruption of communications with the Radius Server then the SSH Server attempts to authenticate the client locally.
- **Remote-then-Local** – The Vanguard SSH Server authenticates the SSH Client login via RADIUS. If the authentication fails for any reason including denial by the Radius Server then the SSH Server attempts to authenticate the client locally.
- **Local-Only** – SSH Client only authenticates locally via Vanguard Router.
- **Remote-Only** – SSH Client can only authenticates remotely via RADIUS. If the RADIUS server is unavailable then secure login is not possible.

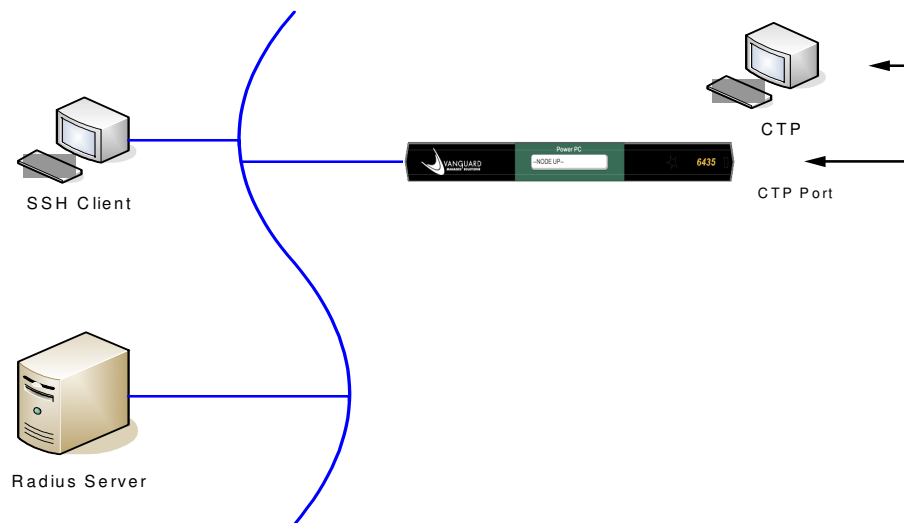
## Benefits & Applications

- Addresses PCI Compliance
- Enables secure remote logins to the Vanguard router control port
- The login and pass word are authenticated before getting to the router
- Secure access to the router means that data can not be read

**Note:** The SSH Server with Radius Authentication is now available on the base Vanguard Application Ware Software license. SSH with Radius Authentication is available on all current Vanguard Networks product through the Applications Ware 7.0 software release.

## Applications

### SSH with Radius Authentication Method



Vanguard Networks ♦ 25 Forbes Blvd. ♦ Foxboro MA 02035 ♦ USA  
Phone +1 (508) 964 6200 ♦ Fax +1 (508) 543 0237  
[www.vanguardnetworks.com](http://www.vanguardnetworks.com)