Brocade ICX TACACS+ and Radius Configuration

I todays Cyber environment, security is paramount. Anything we can do to make it harder for an attacker to gain an advantage is a must and if it is really inexpensive or free, it is a no-brainer. Also, accountability is a necessity in a networking environment. Having everyone login with a single account leaves no one accountable for problems and lends to the problem of Insider Threats from angry employees. Now that we have discussed all the bad things that can happen because you have no implemented TACACS+ or Radius, let's discuss them and how to implement them.

Note: Even though you implement TACACS+ or RADIUS, it is still a good practice to have a local username and password configured on the switch. This username and password is not distributed to people to login, but it is locked away in case of an emergency.

Example:
username admin password brocade

Radius vs TACACS+:

RADIUS

You can use a Remote Authentication Dial In User Service (RADIUS) server to secure the following types of access to the Brocade Layer 2 Switch or Layer 3 Switch:

- Telnet access
- SSH access
- Web management access
- Access to the Privileged EXEC level and CONFIG levels of the CLI

RADIUS authentication, authorization, and accounting

When RADIUS authentication is implemented, the Brocade device consults a RADIUS server to verify user names and passwords. You can optionally configure RADIUS authorization, in which the Brocade device consults a list of commands supplied by the RADIUS server to determine whether a RADIUS security user can issue a command he or she has entered, as well as accounting, which causes the Brocade device to log information on a RADIUS accounting server when specified events occur on the device.

TACACS/TACACS+

You can use the security protocol Terminal Access Controller Access Control System (TACACS) or TACACS+ to authenticate the following kinds of access to the Brocade device:

- Telnet access
- SSH access
- Console access
- Web management access
- Access to the Privileged EXEC level and CONFIG levels of the CLI

The TACACS and TACACS+ protocols define how authentication, authorization, and accounting information is sent between a Brocade device and an authentication database on a TACACS/TACACS+ server. TACACS/TACACS+ services are maintained in a database, typically on a UNIX workstation or PC with a TACACS/TACACS+ server running.

NOTE: TACACS+ provides for authentication, authorization, and accounting, but an implementation or configuration is not required to employ all three.

TACACS/TACACS+ authentication, authorization, and accounting

When you configure a Brocade device to use a TACACS/TACACS+ server for authentication, the device prompts users who are trying to access the CLI for a user name and password, then verifies the password with the TACACS/TACACS+ server. If you are using TACACS+, Brocade recommends that you also configure authorization , in which the Brocade device consults a TACACS+ server to determine which management privilege level (and which associated set of commands) an authenticated user is allowed to use. You can also optionally configure accounting, which causes the Brocade device to log information on the TACACS+ server when specified events occur on the device.

Configuration:

!**********RADIUS Configuration**********
enable snmp config-radius
radius-server host x.x.x.x
radius-server key YOURKEY
!
aaa authentication web-server default radius local
aaa authentication enable default enable
aaa authentication login default radius local
aaa authentication login privilege-mode
!
aaa accounting commands 0 default start-stop radius
aaa accounting exec default start-stop radius
aaa accounting system default start-stop radius
!
! If you want the console to have aaa applied
enable aaa console

!**********TACACS+ Configuration**********
!
enable snmp config-tacacs
tacacs-server host x.x.x.x
tacacs-server key YOURKEY
!
aaa authentication web-server default tacacs+ local
aaa authentication enable default enable

```
aaa authentication login default tacacs+ local
aaa authentication login privilege-mode
!
aaa accounting commands 0 default start-stop tacacs+
aaa accounting exec default start-stop tacacs+
aaa accounting system default start-stop tacacs+
!
! If you want the console to have aaa applied
enable aaa console
```

Server Options:

TACACS+

TACACS.net

TAC_Plus

RADIUS

Free RADIUS

Microsoft Network Policy Server (NPS)