|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | |
|  | | AAA | | | | |  | |
|  |  | | | | | | |  |
|  | | | |  |  | | | |
|  | | | | Weizhen Chen |  | | | |
|  | | | | —CCNP—Jeffery Mason &Michael Hansen |  | | | |
|  | | |  | | |  | | |

Purpose

The objective of the lab was to use Radius or TACACS+ to configure AAA Protocol and connect the server with the router. The server authenticates the router to access and log in the router.

Background information

The AAA (Authentication, Authorization, and Accounting) server is a network server that is used for access control. Authentication identifies the user, provides a way to identify a user, typically by having the user enter a valid username and valid password before access is granted, then it compares the server with credentials stored in a database. If the credentials match, the user is permitted access to the network. Authorization is the process of enforcing policies determining what types of activities, resources, or services a user is permitted to access. Accounting keeps track of time and data resources that are used for billing and analysis.

Lab summary

Use the virtual box to create a Ubuntu Linux server, download Tacacs+ on the linux server, connect the server to the router. On the router Use theaaa new-model global configuration command to enable AAA. Use the tacacs-server host command with the IP address to specify an encryption key that will be used to encrypt all exchanges between the network access server and the TACACS+. Use the aaa authentication global configuration command to define method lists that use TACACS+ for authentication. use the **aaa** **authorization** global command to configure authorization for the network access server. use the **aaa** **accounting** command to enable accounting for TACACS+ connections. Use the run command to save the configuration and ping the server with the router to show AAA is running.

Lab commands

**AAA new model:** Enables AAA on the router.

**Tacas-server host [*hostname*]**: Enables you to specify the names of the IP host or hosts maintaining a TACACS+ server

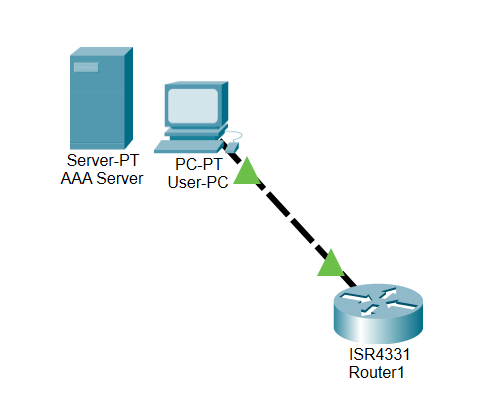
**Radius-server host [*hostname*]**: Enables you to specify the names of the IP host or hosts maintaining a Radius server

**Tacas-server key [*key*]**: Sets the encryption key to match that used on the TACACS+ daemon.

**Radius-server key [*key*]**: Sets the encryption key to match that used on the Radius daemon.

**AAA authentication login:** Defines a method list, “test,” to be used on serial interfaces running PPP. The keyword group Tacacs+or Radius means that authentication will be done through TACACS+

Network diagram



Configurations

**Router 1:**

service timestamps debug datetime msec

service timestamps log datetime msec

no platform punt-keepalive disable-kernel-core

hostname R1

boot-start-marker

boot-end-marker

vrf definition Mgmt-intf

address-family ipv4

exit-address-family

address-family ipv6

exit-address-family

aaa new-model

aaa group server radius linuxaaa

server 10.10.10.5 auth-port 1812 acct-port 1813

server name linux

aaa authentication fail-message "Failed to authenicate remote client"

aaa authentication login default group radius

aaa session-id common

no ip domain lookup

ip domain name nhstechnet.edu

ipv6 unicast-routing

subscriber templating

multilink bundle-name authenticated

license udi pid ISR4321/K9 sn FDO214421CF

spanning-tree extend system-id

redundancy

mode none

vlan internal allocation policy ascending

interface GigabitEthernet0/0/0

no ip address

negotiation auto

interface GigabitEthernet0/0/1

ip address 10.10.10.1 255.255.255.192

negotiation auto

ipv6 address 2001:DB8:ACAD:1::1/64

interface Serial0/1/0

no ip address

interface Serial0/1/1

no ip address

interface GigabitEthernet0

vrf forwarding Mgmt-intf

no ip address

negotiation auto

interface Vlan1

no ip address

ip forward-protocol nd

no ip http server

no ip http secure-server

ip tftp source-interface GigabitEthernet0

ip ssh version 2

ip ssh server algorithm authentication password

radius server linux

address ipv6 2001:DB8:ACAD:1::10 auth-port 1812 acct-port 1813

address ipv4 10.10.10.5 auth-port 1812 acct-port 1813

timeout 30

retransmit 5

key password

control-plane

line con 0

stopbits 1

line aux 0

stopbits 1

line vty 0

transport input ssh

line vty 1 4

end

**Linux Server:**

**Clients Configuration:**

client 10.10.10.1 {

ipv4addr = 10.10.10.1

ipv6addr = 2001:DB8:ACAD:1::1

secret = password

nastype = cisco

shortname = R1

proto = \*

secret = testing123

require\_message\_authenticator = no

nas\_type = other # localhost isn't usually a NAS...

limit {

max\_connections = 16

lifetime = 0

idle\_timeout = 30

}

Users Configuration:

admin MD5-Password := "5f4dcc3b5aa765d61d8327deb882cf99"

Service-Type = NAS-Prompt-User

hacksore MD5-Password := "5f4dcc3b5aa765d61d8327deb882cf99"

Service-Type = NAS-Prompt-User

earls MD5-Password := "915fa686e4e3d12877bfbb273723b495"

Service-Type = NAS-Prompt-User

**Free Radius Configuration:**

prefix = /usr

exec\_prefix = /usr

sysconfdir = /etc

localstatedir = /var

sbindir = ${exec\_prefix}/sbin

logdir = /var/log/freeradius

raddbdir = /etc/freeradius/3.0

radacctdir = ${logdir}/radacct

libdir = /usr/lib/freeradius

pidfile = ${run\_dir}/${name}.pid

correct\_escapes = true

max\_request\_time = 60

cleanup\_delay = 5

max\_requests = 50

hostname\_lookups = no

log {

destination = files

colourise = yes

file = ${logdir}/radius.log

syslog\_facility = daemon

stripped\_names = no

auth = yes

auth\_accept = yes

auth\_reject = no

auth\_badpass = yes

auth\_goodpass = yes

msg\_denied = "You are already logged in - access denied"

}

checkrad = ${sbindir}/checkrad

security {

user = freerad

group = freerad

allow\_core\_dumps = no

max\_attributes = 200

reject\_delay = 1

status\_server = yes

}

proxy\_requests = yes

$INCLUDE proxy.conf

$INCLUDE clients.conf

thread pool {

start\_servers = 5

max\_servers = 32

min\_spare\_servers = 3

max\_spare\_servers = 10

max\_requests\_per\_server = 0

auto\_limit\_acct = no

}

$INCLUDE mods-enabled/

}

policy {

$INCLUDE policy.d/

}

$INCLUDE sites-enabled/

Problems

One of the biggest Problem that I faced in the lab was that I did not know how to configure a AAA, Tacacs+ and configure a ubuntu Linux server, so I looked at AAA, Tacacs+ and ubuntu videos along with a website on them to understand how to properly create the AAA system. During the process of creating AAA, I encountered some minor problems, like not understanding that you have to use the AAA new model command to start the AAA configuration for routers

Conclusion

The objective of the lab was to be able to configure an AAA system for a router using Tacas+ or Radius. During this prosses of creating the AAA it allowed us to review Authentication, Authorization, Accounting and allowed us to better understand and familiarize ourselves with how to configure a virtual box or physical server. During the lab we encountered some small troubles that we learned from, but We were able to config the AAA system correctly by the end. This lab was straight forward, and I was able to gain experience in setting up the server router system by the end of the lab.