Cisco RADIUS Auth

Richard Nason <rnason@clusterfrak.com>

Configuring Cisco RADIUS Authentication

For more information on Cisco, visit cisco.com

Description:

This document has been constructed to configure Cisco Routers, Switches, and Aironet devices to allow user authentication via Microsoft RADIUS. This configuration will allow for users to log into the devices using Active Directory credentials and will set their access (Priv 1-15) based on their credentials via Active Directory group membership.

Information on configuring the server for IAS services can be found [[Adding_IAS_Client|here]]

Pre-Requisites:

---

1. RADIUS Server:
Configure your RADIUS server to work with Cisco devices by following the steps outlined in [[Cisco Configure Radius Auth]]

2. Set Secret Enable:
Prior to configuring your devices for RADIUS, ensure you have a secret enable configured on your device so that in the event that RADIUS authentication is down, you will still have access to the device.

```
enable secret
username admin privilege 15 password
```

Warning:
The username configuration will not work while RADIUS authentication is configured, as it is a local username.

Configure RADIUS:

---

1. Login:
Log into the router via Telnet or SSH

```
Telnet 192.168.0.15
```

or

```
ssh 192.168.0.15
```

2. Enter Global Config:
Enter the devices global config mode from the privileged exec prompt **AP#**

```
config t
```

3. AAA Methods:
Configure and enable the following aaa methods

NOTICE:
The following syntax will be input from the Global Config prompt: "'Cisco(config)#"'

```
aaa new-model
aaa authentication login default group radius local
aaa authorization exec default group radius local
```

4. RADIUS PSKs:
Configure the RADIUS server Pre-Shared Keys (This key is the key used when configuring the IAS or NPS RADIUS clients in step 1) [[Adding IAS Client]]

NOTICE:
The following syntax will be input from the Global Config prompt: "'Cisco(config)#"'

```
radius-server host 192.168.79.64 auth-port 1645 acct_port 1646 key ReplaceThisWithKey
radius-server host 192.168.79.69 auth-port 1645 acct_port 1646 key ReplaceThisWithKey
```

Removing RADIUS:

The "no" form of each command will remove the configuration from the running memory

NOTICE:
This snippit assumes you are in Privileged Exec mode: "'Cisco#"'

```
config t
no aaa authentication login default group radius local
no aaa authorization exec default group radius local
aaa authentication login default local
aaa authorization exec default local
```

```
!
no radius-server host 192.168.79.64 auth-port 1645 acct_port 1646 key ReplaceThisWithKey
no radius-server host 192.168.79.69 auth-port 1645 acct_port 1646 key ReplaceThisWithKey
exit
```

Sample Running-Config:

```
APCF01P#show run
Building configuration...

Current configuration : 6408 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname APCF01P
!
enable secret 5 $1$6NLA$ZzXylh4pR/GJCDGIifWoC0
!
ip subnet-zero
ip domain name clusterfrak.com
ip name-server 192.168.79.64
ip name-server 192.168.79.32
ip name-server 192.168.79.254
!
!
aaa new-model
!
!
aaa group server radius rad_eap
 server 192.168.79.69 auth-port 1645 acct-port 1646
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default group radius local
aaa authentication login mac_methods group rad_mac
aaa authentication login eap_methods group rad_eap
aaa authorization exec default group radius local
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
dot11 association mac-list 700
dot11 vlan-name Clusterfrak vlan 79
dot11 vlan-name Public vlan 100
!
dot11 ssid CFGuest
   vlan 100
```

```
   authentication open
   authentication key-management wpa
   guest-mode
   mbssid guest-mode
   wpa-psk ascii 7 12100918040E0A082B3B343139342118145742
!
dot11 ssid Clusterfrak
   vlan 79
   authentication open eap eap_methods
   authentication network-eap eap_methods
   authentication key-management wpa
   infrastructure-ssid optional
!
!
crypto pki trustpoint TP-self-signed-1195232396
 subject-name cn=IOS-Self-Signed-Certificate-1195232396
 revocation-check none
 rsakeypair TP-self-signed-1195232396
!
!
crypto ca certificate chain TP-self-signed-1195232396
 certificate self-signed 01
  3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 31313935 32333233 3936301E 170D3032 30333031 30313331
  35385A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 31393532
  33323339 3630819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100C12A 863463FE 57045A2A 7F19FB29 26D9F7F5 4BB06A4F 625FCB70 8933A92D
  9A0FA852 FE391C05 DBC7300B 3E87CEEC 54124EE8 EEE2D885 1E2F6F07 6BBA5894
  26737685 C4B48764 59A1AFBF 7A22F15A 01415672 A88987B5 E3CBE53D 0EB95903
  197C44C6 F6C39042 E8B2C07D EF06898F 70F9512E 28E87D84 C82121D6 B877B877
  3E490203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
  551D2304 18301680 14119CE8 6948D67F 7F5C23F9 0A5A2413 7C80B3B8 99301D06
  03551D0E 04160414 119CE869 48D67F7F 5C23F90A 5A24137C 80B3B899 300D0609
  2A864886 F70D0101 04050003 81810036 4F6002CD 03A1836F FE2ACCFD 829F7796
  B7C34E20 002B5F6C 74BE5EBB BF7E9348 96B42C45 9B8C1E99 42487D60 2263D006
  41D41274 6CB73CAA 3092482C 1C9B5A92 35562340 7B325051 F4A094A0 8DF7AEFA
  C9CD5A08 C0FC5D9B 6BE30228 387D8DC7 A21C0569 8127955E 7E670749 EC4DA51C
  9EA47756 84D71D6F B5860683 EE7EC4
  quit
username rnason privilege 15 secret 5 $1$WKnq$iGrwQh/8RFkXkxIsHEroL.
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 79 mode ciphers tkip
 !
 encryption vlan 100 mode ciphers tkip
 !
 ssid CFGuest
 !
 ssid Clusterfrak
 !
 mbssid
 speed basic-11.0 basic-54.0
 channel 2442
 station-role root
```

```
 l2-filter bridge-group-acl
!
interface Dot11Radio0.79
 encapsulation dot1Q 79 native
 ip helper-address 192.168.79.64
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 input-address-list 700
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0.100
 encapsulation dot1Q 100
 no ip unreachables
 no ip proxy-arp
 no ip route-cache
 no cdp enable
 bridge-group 100
 bridge-group 100 subscriber-loop-control
 bridge-group 100 block-unknown-source
 no bridge-group 100 source-learning
 no bridge-group 100 unicast-flooding
 bridge-group 100 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
!
interface FastEthernet0.79
 encapsulation dot1Q 79 native
 no ip route-cache
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface FastEthernet0.100
 encapsulation dot1Q 100
 no ip route-cache
 bridge-group 100
 no bridge-group 100 source-learning
 bridge-group 100 spanning-disabled
!
interface BVI1
 ip address 192.168.79.253 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.79.254
ip http server
ip http authentication local
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
!
access-list 700 permit 0023.6c80.2cf5   0000.0000.0000
access-list 700 permit 0026.4acd.6ad3   0000.0000.0000
access-list 700 permit 041e.64c8.645d   0000.0000.0000
access-list 700 permit 0026.08ae.d1d6   0000.0000.0000
access-list 700 permit 0026.4acc.dfc0   0000.0000.0000
```

```
access-list 700 permit 001f.a749.be9f   0000.0000.0000
access-list 700 permit 0021.29b0.1755   0000.0000.0000
access-list 700 permit 001f.a736.ff30   0000.0000.0000
access-list 700 deny   0000.0000.0000   ffff.ffff.ffff
snmp-server community Clusterfrak RO 1
snmp-server host 192.168.79.69 version 2c Clusterfrak
radius-server host 192.168.79.69 auth-port 1645 acct-port 1646 key 7 04782D5156115E471F4850121C1F3E5
radius-server deadtime 60
radius-server vsa send accounting
!
control-plane
!
bridge 1 route ip
!
!
banner motd ^CC
**************************************************************
*     WARNING --- WARNING --- WARNING --- WARNING              *
*                                                              *
*   UNAUTHORIZED ACCESS IS STRICTLY FORBIDDEN        *
*                                  *
*   Unauthorized access to this network, its systems,     *
*   hosts, or any other resources is strictly forbidden.  *
*   Violators will be prosecuted to the fullest extent    *
*   of the law.                     *
*                                  *
**************************************************************
^C
!
line con 0
 password 7 06041E731B4B021E0616
 logging synchronous
 transport preferred all
 transport output all
line vty 0 3
 transport preferred all
 transport input all
 transport output all
line vty 4
 transport preferred all
 transport input ssh
 transport output ssh
line vty 5 15
 transport preferred all
 transport input ssh
 transport output ssh
!
end

APCF01P#
```

Post Requisites:

None

References:

Cisco Configuration Guide