RADIUS/ TACACS Authentication

CCNP Lab 4

2018-2019

Nipun Chhajed

Cisco CCNP - Hoffman and Mason - Periods 6 and 7

RADIUS/TACACS Authentication Lab 4

Purpose

The purpose of this lab was to learn:

1. What TACACS+ and RADIUS are.
2. How to implement both TACACS+ and RADIUS based authentication on a router.
3. What the differences between the two are.

Background Information

In this lab, we used two security protocols - TACACS+ native to ubuntu, and RADIUS, native to Windows. What these protocols allow for is secure login to terminals. Both use a client server module, where the client tries to log in to the server/terminal, and the server authenticates their login, where if their login is authenticated, they may access the server/terminal. On routers, you must use the “aaa” framework to use either protocols. “Aaa” stands for authentication, authorization and accounting. The framework is used to allow/deny clients to access network resources, such as remote access of a networking device. Also to define the authority of the client, as to how many and which changes they are allowed to make. And finally it accounts for all the instances where people have tried to login or access the server and it’s resources. RADIUS and TACACS+ are specific types of “aaa” models, because

they are the ones that carry out the “authentication, authorization and accounting” in the network.

Lab Summary

In this lab we set up two virtual machine: one Linux and one Windows Server. We then set up the respective servers’ security protocol (TACACS+ on Linux and RADIUS on Windows).. Next, using aaa commands we configured routers that allowed for authentication using TACACS and RADIUS. Finally we tested the configurations, by logging in to the routers using the username and passwords we set up on each of the Virtual Machine’s security protocols.

Lab Commands

aaa new model	Creates a new aaa model for the router to use when people try to login to the router - allows for RADIUS or TACACS+ to be configured.
tacacs-server host [ip address]	Defines the host TACACS+ sever, where the TACACS+ configuration was done, so that the router can get the information from it.
tacacs-server directed-request	To allow users to send authentication requests to a specific TACACS+ server when logging in
tacacs-server key [key]	Sets the key for the tacacs-server on the router, must match the key defined in the tac_plus.conf file on linux.
aaa authentication login default group [tacacs+ or radius] local	Sets the default security protocol to be used for logging into the router.
aaa authentication enable default group tacacs+ enable	Sets the default security protocol to be used for enabling the user to

	login to the router
aaa authorization config-commands	Configures default authorization commands for USER EXEC commands
radius-server host [address] key [key]	Allows for router to connect to the RADIUS server, and retrieve information for it
aaa authorization commands [level] default group tacacs+ none	Sets the level of authority the client has, meaning which changes they are allowed to make and which information they are allowed to access. Levels go from 0 to 15, where 15 is highest.
Aaa group server radius [name]	Defines the radius server's name that is to be used.
aaa session-id common	To ensure the session ID is maintained across all authentication, authorization, and accounting packets in a session
ping [ip-address]	Shows the connectivity between the device and another one - works for IPv4 and IPv6
ip address [address]	Sets up the IPv4 address in an interface

Network Diagram

Hosts	IP Address
Cisco_2901	
G0/0	192.168.1.254/24
TACACS+	
G0/0	192.168.1.1/24
2016 Server	192.168.1.1/24
Linux Server	192.168.1.3/24

Configurations

Tacacs Router Configuration:

```
tacacs# show run
hostname tacacs
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization config-commands
aaa authorization commands 0 default group tacacs+ none
aaa authorization commands 15 default group tacacs+ none
aaa session-id common
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
tacacs-server host 192.168.1.3
tacacs-server directed-request
```

```
tacacs-server key IPBALANCE
end
```

Radius Router Configuration:

```
Cisco_2901# show run
hostname Cisco_2901
aaa new-model
aaa group server radius RAD_SERVER
aaa authentication login default group radius local
aaa authorization exec default group radius if-authenticated
aaa session-id common
username admin privilege 15 secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
interface GigabitEthernet0/0
 ip address 192.168.1.254 255.255.255.0
 duplex auto
 speed auto
radius-server host 192.168.1.1 key AAARadius
end
```

Screenshots

Tacacs File:

```
# Created by Henry-Nicolas Tourneur(henry.nicolas@tourneur.be)
# See man(5) tac_plus.conf for more details

# Define where to log accounting data, this is the default.

accounting file = /var/log/tac_plus.acct

# This is the key that clients have to use to access Tacacs+

key = IPBALANCE

# Use /etc/passwd file to do authentication

#default authentication = file /etc/passwd


# You can use feature like per host key with different enable passwords
#host = 127.0.0.1 {
#        key = test
#        type = cisco
#        enable = <des|cleartext> enablepass
#        prompt = "Welcome XXX ISP Access Router \n\nUsername:"
#}

# We also can define local users and specify a file where data is stored.
# That file may be filled using tac_pwd
user = fourday {
        default service = permit
        login = cleartext cisco
        enable = cleartext cisco
}

#group = staff {
#       default service = permit
#       service = exec {
#               priv-lvl = 15
#        }
#}

# We can also specify rules valid per group of users.
#group = group1 {
#       cmd = conf {
#               deny
#       }
#}

# Another example : forbid configure command for some hosts
# for a define range of clients
#group = group1 {
#       login = PAM
#       service = ppp
#       protocol = ip {
#               addr = 10.10.0.0/24
#       }
#       cmd = conf {
#               deny .*
#       }
#}
#service tacacs_plus start
#user = DEFAULT {
#       login = PAM
#       service = ppp protocol = ip {}
#}

# Much more features are availables, like ACL, more service compatibilities,
# commands authorization, scripting authorization.
# See the man page for those features.
```

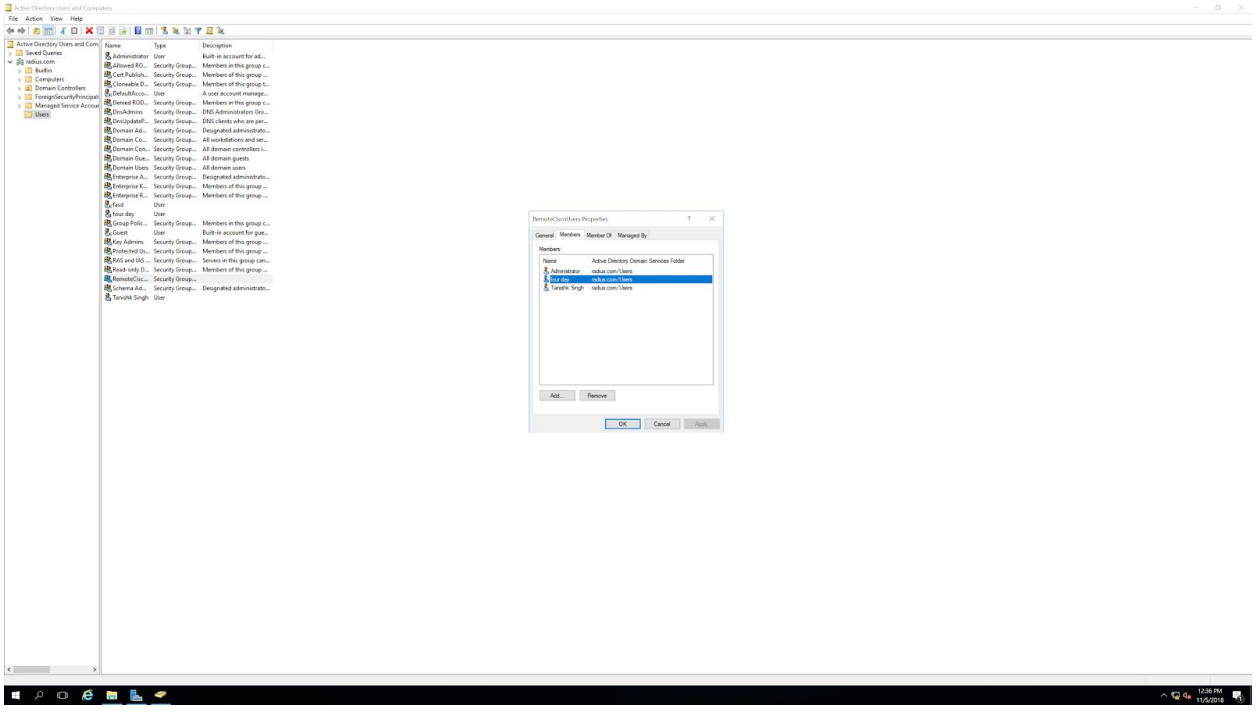
Tacacs Commands:

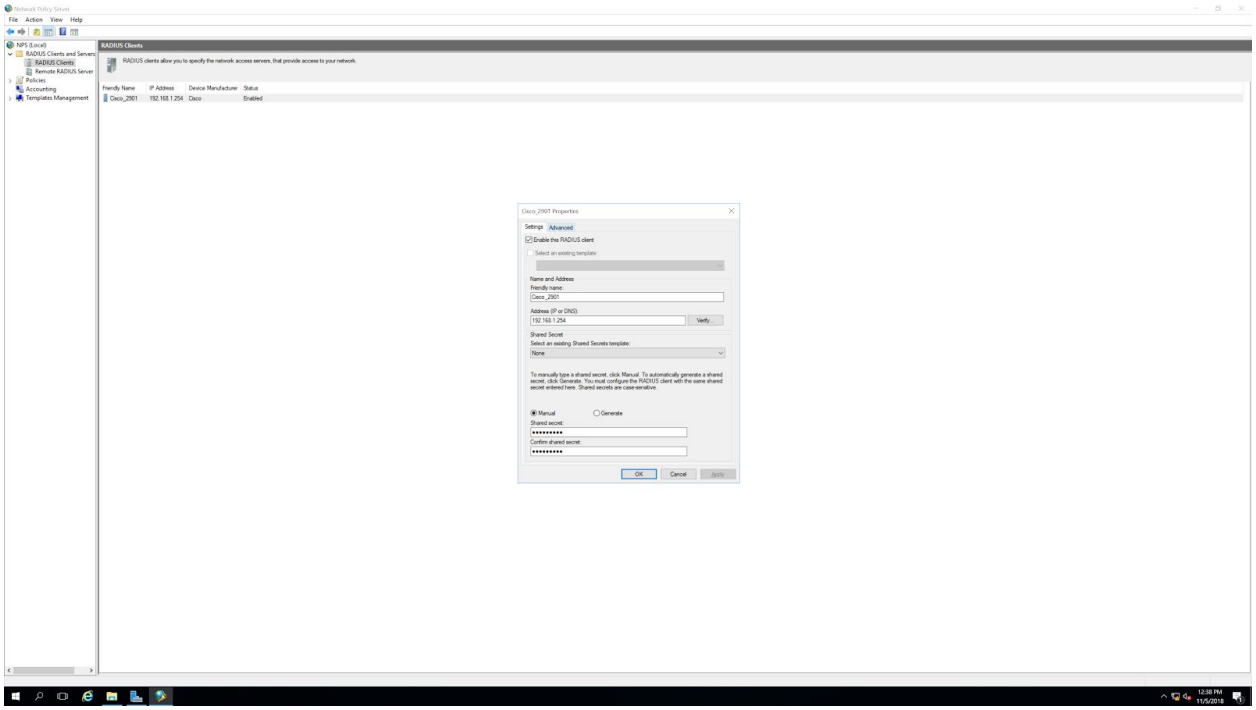
```
tac@ubuntu:~$ sudo /etc/init.d/tacacs_plus start
[ ok ] Starting tacacs_plus (via systemctl): tacacs_plus.service.
tac@ubuntu:~$ sudo /etc/init.d/tacacs_plus restart
[ ok ] Restarting tacacs_plus (via systemctl): tacacs_plus.service.
tac@ubuntu:~$
```

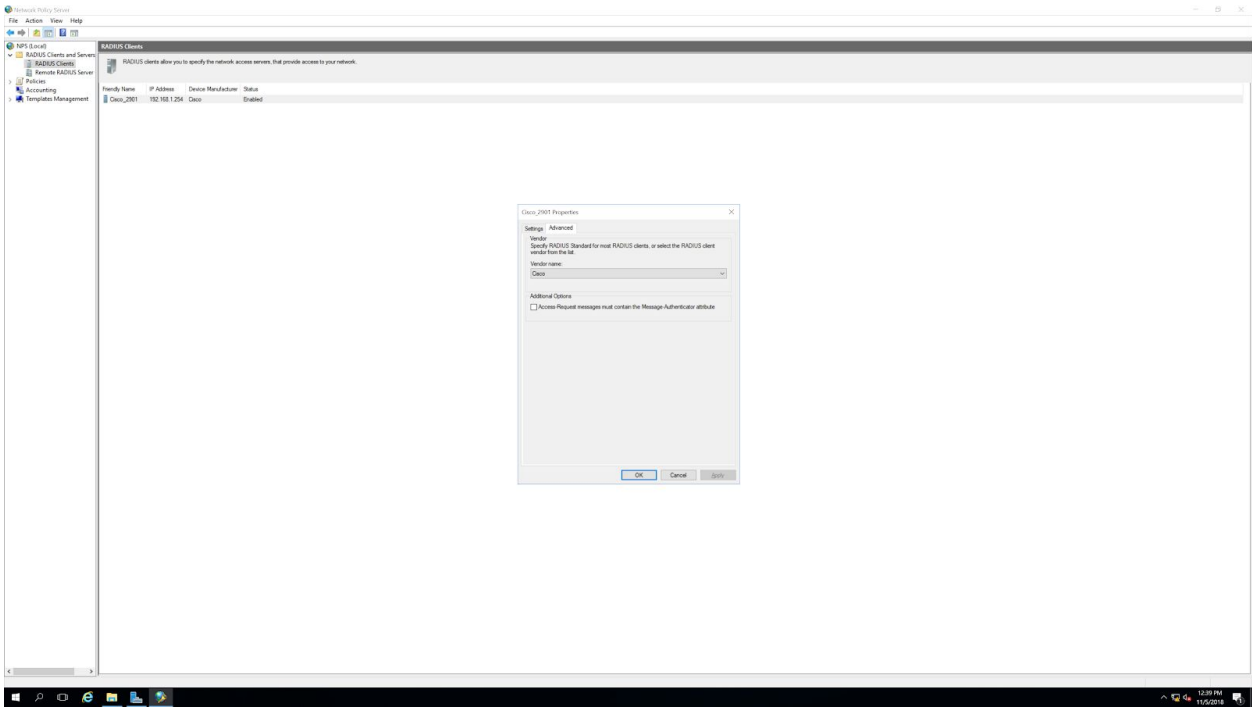
Tacacs Authentication on Router:

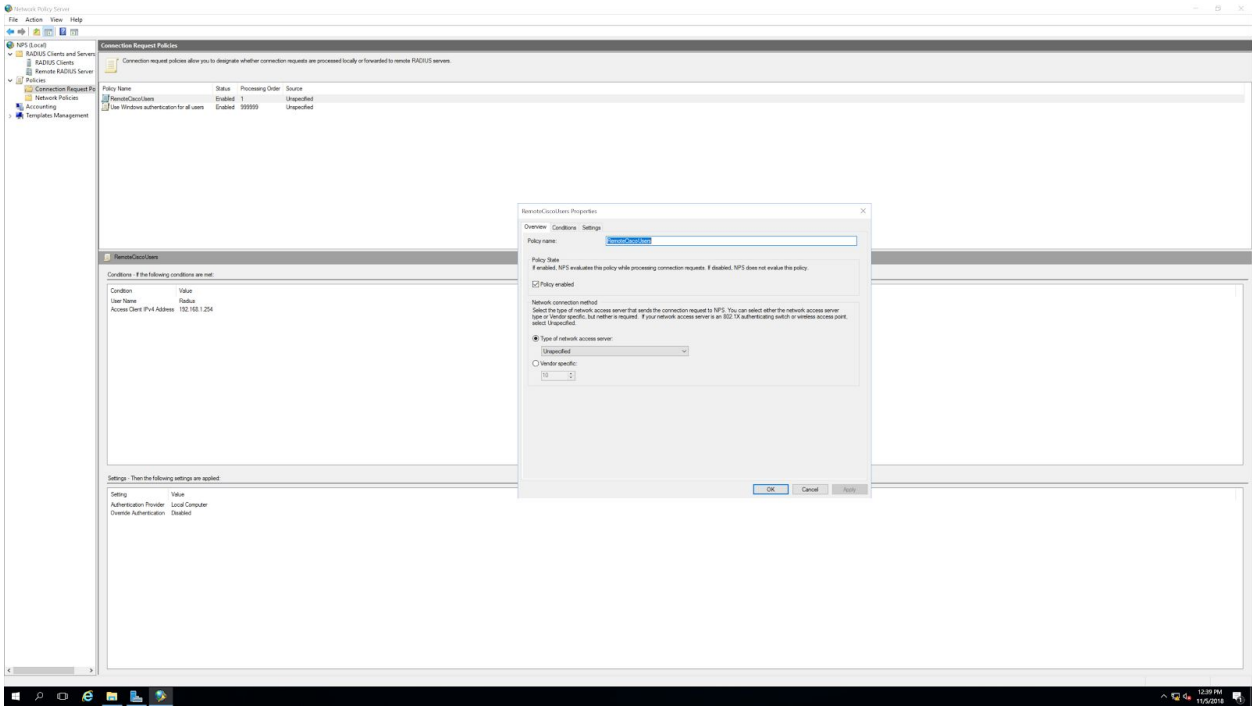
```
User Access Verification

Username: fourday
Password:

tacacs>en
Password:
tacacs#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
tacacs(config)#
```

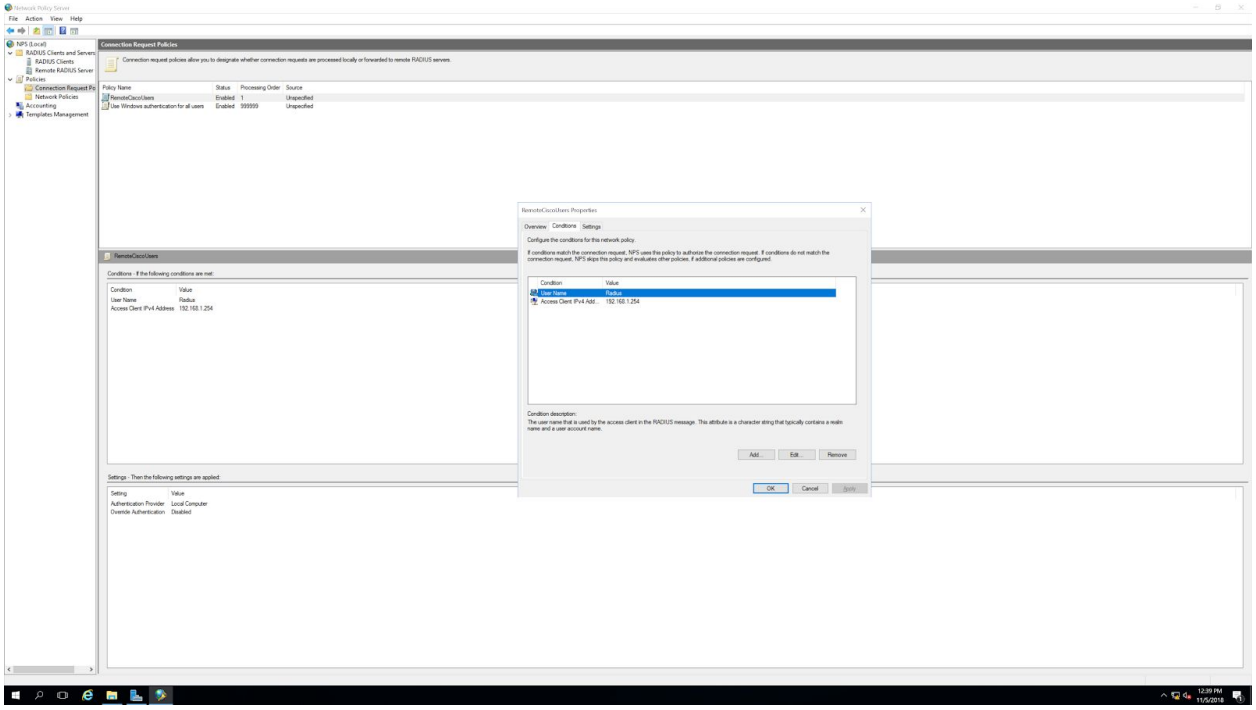
Radius:

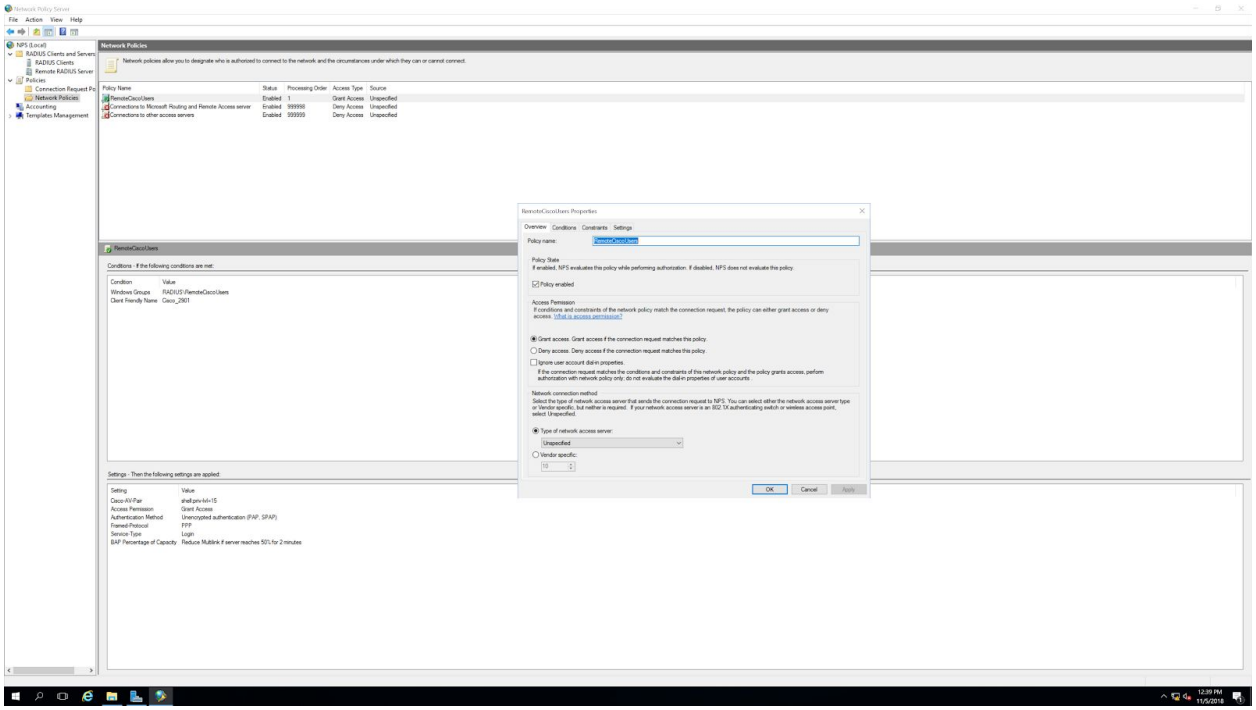


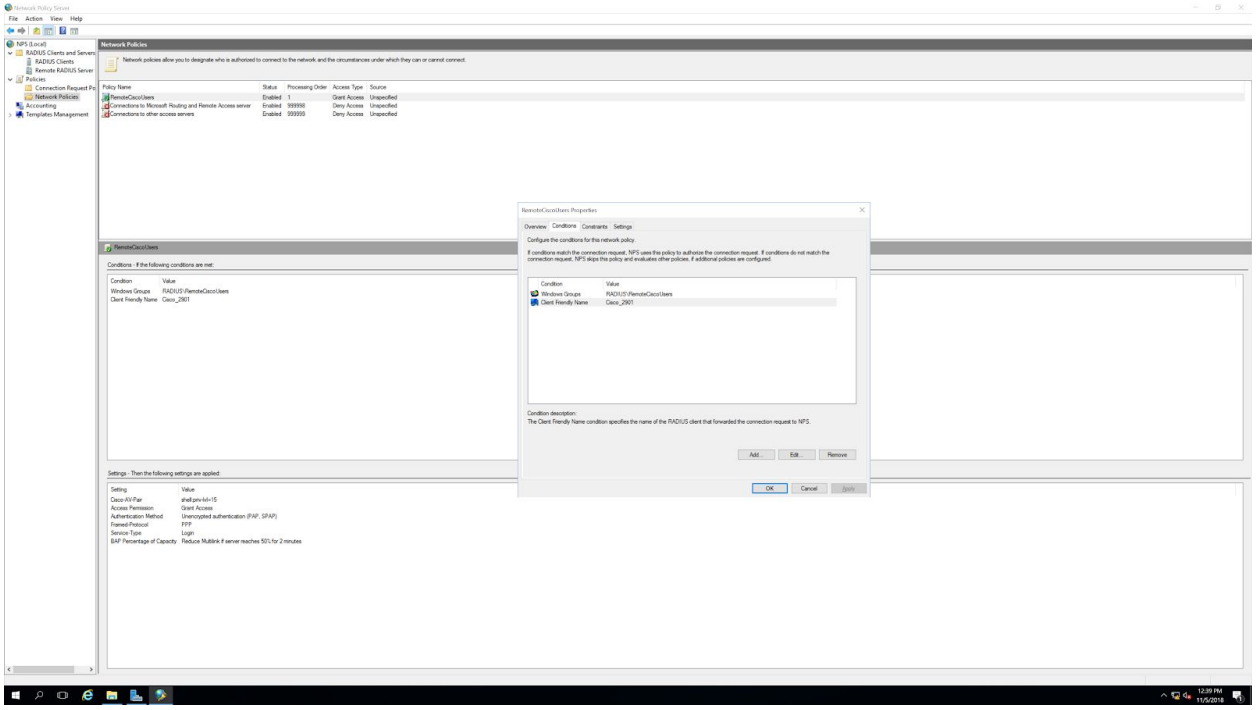

Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server
Policies
Accounting
Templates Management
RADIUS Clients
RADIUS clients allow you to specify the network access servers, that provide access to your network.
Friendly Name
IP Address
Device Manufacturer
Status
Cisco_2901
192.168.1.254
Cisco
Enabled
Cisco 2901 Properties
Settings
Advanced
Enable this RADIUS client
Select an existing template:
Name and Address
Friendly name:
Cisco_2901
Address (IP or DNS):
192.168.1.254
Verify...
Shared Secret
Select an existing Shared Secrets template:
None
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.
Manual
Generate
Shared secret:
Confirm shared secret:
OK
Cancel
Apply
12:38 PM
11/5/2018

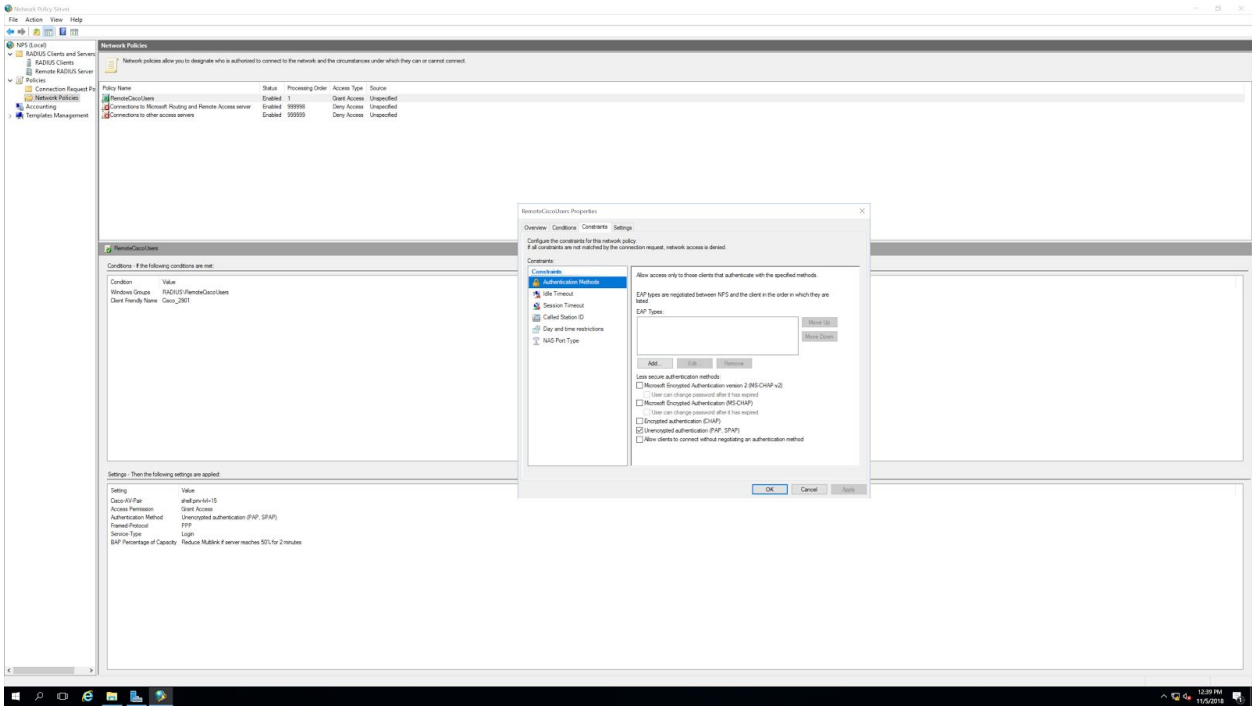

Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server
Policies
Accounting
Templates Management
RADIUS Clients
RADIUS clients allow you to specify the network access servers, that provide access to your network.
Friendly Name
IP Address
Device Manufacturer
Status
Cisco_2901
192.168.1.254
Cisco
Enabled
Cisco 2901 Properties
Settings
Advanced
Vendor
Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.
Vendor name:
Cisco
Additional Options
Access-Request messages must contain the Message-Authenticator attribute
OK
Cancel
Apply
12:39 PM
11/5/2018

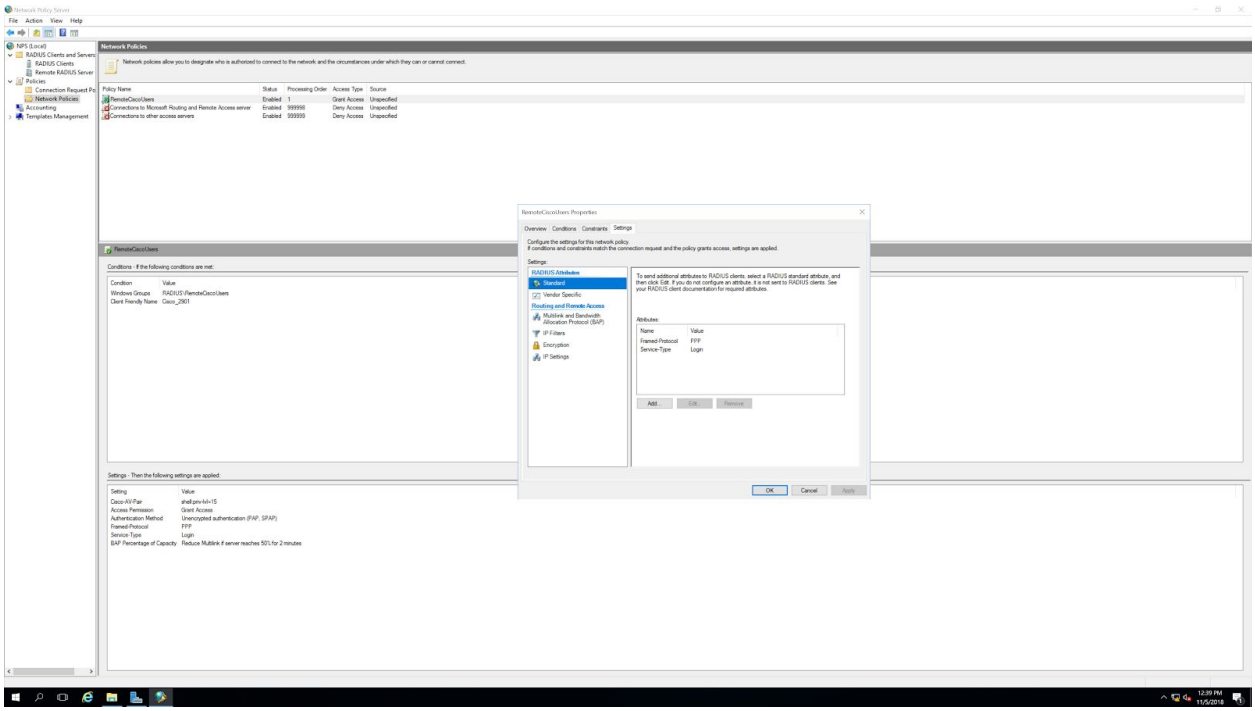


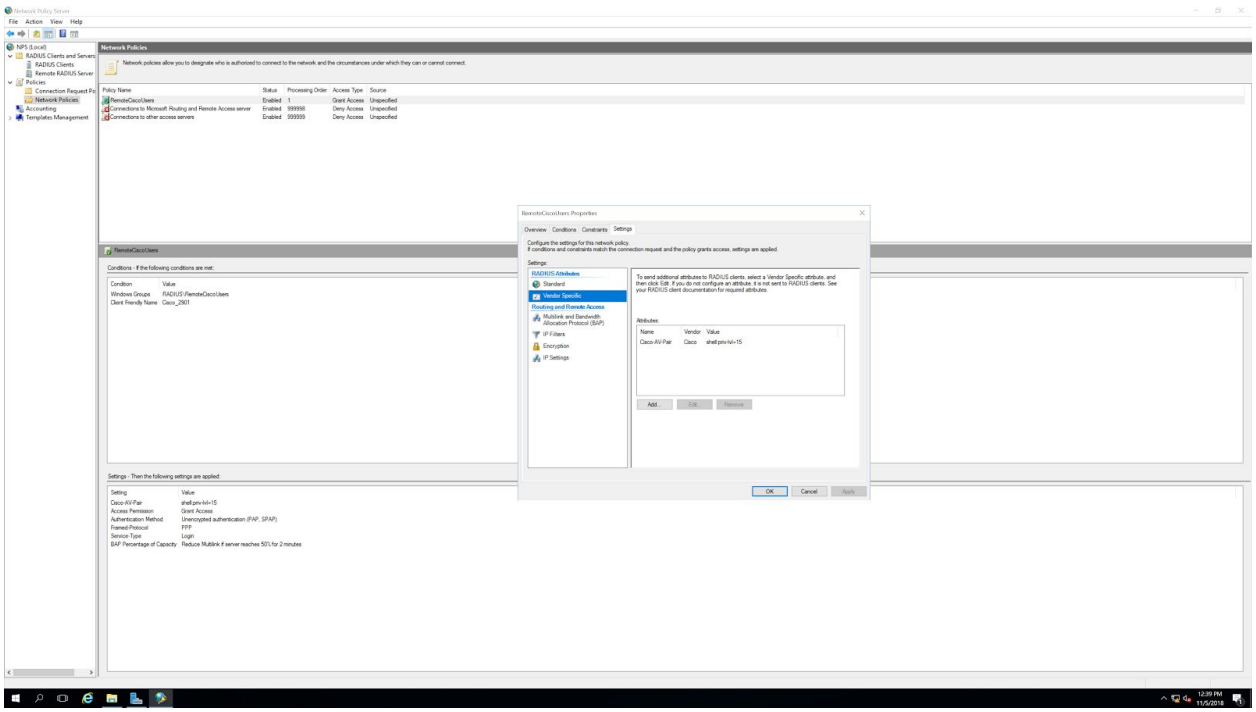


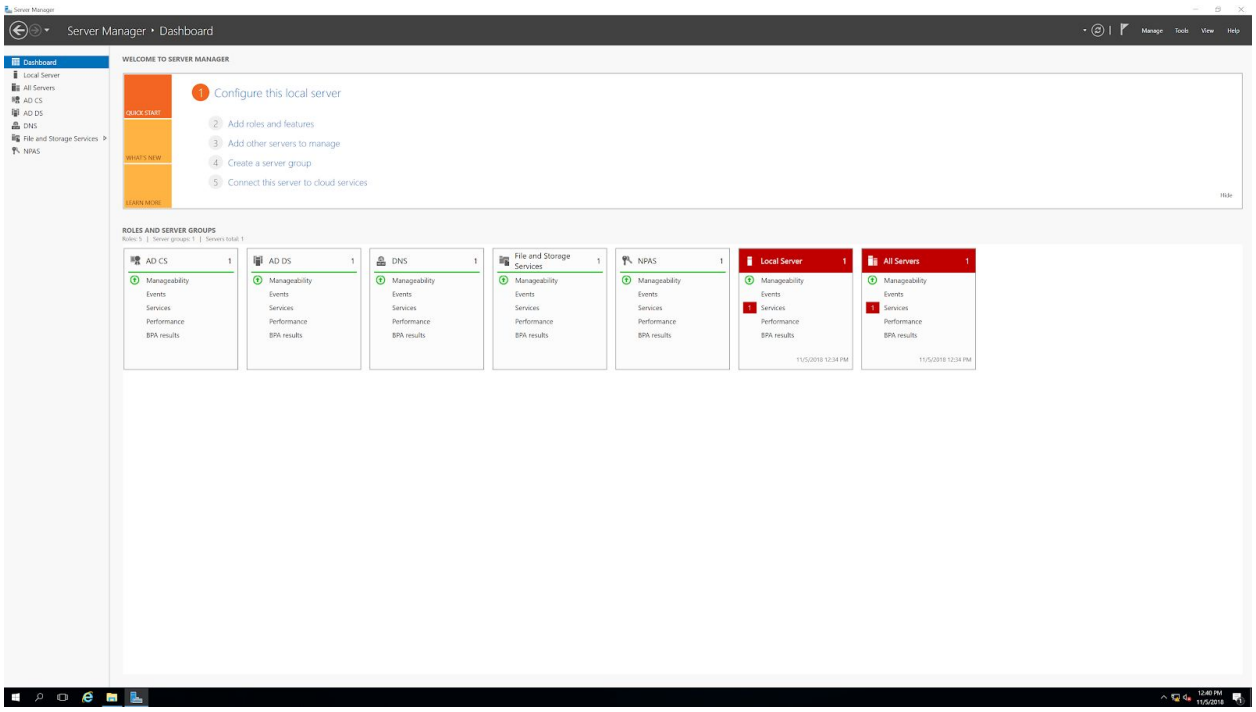





Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server
Policies
Connection Request Policies
Network Policies
Accounting
Templates Management
Network Policies
Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.
Policy Name
Status
Processing Order
Access Type
Source
RemoteCiscoUsers
Enabled
1
Grant Access
Unspecified
Connections to Microsoft Routing and Remote Access server
Enabled
999998
Deny Access
Unspecified
Connections to other access servers
Enabled
999999
Deny Access
Unspecified
RemoteCiscoUsers Properties
Overview
Conditions
Constraints
Settings
Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.
Constraints:
Authentication Methods
Idle Timeout
Session Timeout
Called Station ID
Day and time restrictions
NAS Port Type
Allow access only to those clients that authenticate with the specified methods.
EAP types are negotiated between NPS and the client in the order in which they are listed.
EAP Types:
Move Up
Move Down
Add...
Edit...
Remove
Less secure authentication methods:
Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
User can change password after it has expired
Microsoft Encrypted Authentication (MS-CHAP)
User can change password after it has expired
Encrypted authentication (CHAP)
Unencrypted authentication (PAP, SPAP)
Allow clients to connect without negotiating an authentication method
OK
Cancel
Apply
RemoteCiscoUsers
Conditions - If the following conditions are met:
Condition
Value
Windows Groups
RADIUS\RemoteCiscoUsers
Client Friendly Name
Cisco_2901
Settings - Then the following settings are applied:
Setting
Value
Cisco-AV-Pair
shell:priv-lvl=15
Access Permission
Grant Access
Authentication Method
Unencrypted authentication (PAP, SPAP)
Framed-Protocol
PPP
Service-Type
Login
BAP Percentage of Capacity
Reduce Multilink if server reaches 50% for 2 minutes
12:39 PM
11/5/2018


Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server
Policies
Connection Request Policies
Network Policies
Accounting
Templates Management
Network Policies
Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.
Policy Name
Status
Processing Order
Access Type
Source
RemoteCiscoUsers
Enabled
1
Grant Access
Unspecified
Connections to Microsoft Routing and Remote Access server
Enabled
999998
Deny Access
Unspecified
Connections to other access servers
Enabled
999999
Deny Access
Unspecified
RemoteCiscoUsers Properties
Overview
Conditions
Constraints
Settings
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
RADIUS Attributes
Standard
Vendor Specific
Routing and Remote Access
Multilink and Bandwidth Allocation Protocol (BAP)
IP Filters
Encryption
IP Settings
To send additional attributes to RADIUS clients, select a RADIUS standard attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.
Attributes:
Name
Value
Framed-Protocol
PPP
Service-Type
Login
Add...
Edit...
Remove
OK
Cancel
Apply
RemoteCiscoUsers
Conditions - If the following conditions are met:
Condition
Value
Windows Groups
RADIUS\RemoteCiscoUsers
Client Friendly Name
Cisco_2901
Settings - Then the following settings are applied:
Setting
Value
Cisco-AV-Pair
shell:priv-lvl=15
Access Permission
Grant Access
Authentication Method
Unencrypted authentication (PAP, SPAP)
Framed-Protocol
PPP
Service-Type
Login
BAP Percentage of Capacity
Reduce Multilink if server reaches 50% for 2 minutes
12:39 PM
11/5/2018


Network Policy Server
File Action View Help
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server
Policies
Connection Request Policies
Network Policies
Accounting
Templates Management
Network Policies
Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.
Policy Name
Status
Processing Order
Access Type
Source
RemoteCiscoUsers
Enabled
1
Grant Access
Unspecified
Connections to Microsoft Routing and Remote Access server
Enabled
999998
Deny Access
Unspecified
Connections to other access servers
Enabled
999999
Deny Access
Unspecified
RemoteCiscoUsers Properties
Overview
Conditions
Constraints
Settings
Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.
Settings:
RADIUS Attributes
Standard
Vendor Specific
Routing and Remote Access
Multilink and Bandwidth Allocation Protocol (BAP)
IP Filters
Encryption
IP Settings
To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.
Attributes:
Name
Vendor
Value
Cisco-AV-Pair
Cisco
shell:priv-lvl=15
Add...
Edit...
Remove
OK
Cancel
Apply
RemoteCiscoUsers
Conditions - If the following conditions are met:
Condition
Value
Windows Groups
RADIUS-RemoteCiscoUsers
Client Friendly Name
Cisco_2901
Settings - Then the following settings are applied:
Setting
Value
Cisco-AV-Pair
shell:priv-lvl=15
Access Permission
Grant Access
Authentication Method
Unencrypted authentication (PAP, SPAP)
Framed-Protocol
PPP
Service-Type
Login
BAP Percentage of Capacity
Reduce Multilink if server reaches 50% for 2 minutes
12:39 PM
11/5/2018


Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Services
NPAS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Hide
ROLES AND SERVER GROUPS
Roles: 5 | Server groups: 1 | Servers total: 1
AD CS
AD DS
DNS
File and Storage Services
NPAS
Local Server
All Servers
Manageability
Events
Services
Performance
BPA results
11/5/2018 12:34 PM
12:40 PM
11/5/2018

Problems

During this lab, we encountered many problems. The main problem was getting the configuration on the Virtual Machine itself correct. If the TACACS+ or RADIUS configuration wasn't correct on the Virtual Machines, then the authentication on the routers would fail. We would constantly research how to configure the files correctly, and how to get authentication working. After countless failed attempts, we cracked it and got authentication on both TACACS+ and RADIUS working. Another major problem, was getting the Virtual Machines to connect to internet and ethernet. Internet connectivity, was especially important for linux, since you have to install the tacacs+ packages from the internet using the terminal. Ethernet connectivity was a problem for both, since it took time to figure out how to get the Virtual Machines themselves connected. After a while, we figured out that we just had to bridge the connection between the Virtual Machines and their host computers, and finally, they connected.

Conclusion

In conclusion, we set up two Virtual Machines, one with Linux, and one with Windows Server. We set up RADIUS (on Windows Server) and TACACS+ (on Linux), and set up two routers to specifically authenticate using one of the protocols. In the end, though we faced multiple problems, we ended up figuring out how to configure both security protocols.