FreeRADIUS Version 3.0.26

Copyright (C) 1999-2021 The FreeRADIUS server project and contributors

There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A

PARTICULAR PURPOSE

You may redistribute copies of FreeRADIUS under the terms of the

GNU General Public License

For more information about these matters, see the file named COPYRIGHT

Starting - reading configuration files ...

including dictionary file /usr/share/freeradius/dictionary

including dictionary file /usr/share/freeradius/dictionary.dhcp

including dictionary file /usr/share/freeradius/dictionary.vqp

including dictionary file /etc/freeradius/3.0/dictionary

including configuration file /etc/freeradius/3.0/radiusd.conf

including configuration file /etc/freeradius/3.0/proxy.conf

including configuration file /etc/freeradius/3.0/clients.conf

including files in directory /etc/freeradius/3.0/mods-enabled/

including configuration file /etc/freeradius/3.0/mods-enabled/always

including configuration file /etc/freeradius/3.0/mods-enabled/attr\_filter

including configuration file /etc/freeradius/3.0/mods-enabled/cache\_eap

including configuration file /etc/freeradius/3.0/mods-enabled/chap

including configuration file /etc/freeradius/3.0/mods-enabled/detail

including configuration file /etc/freeradius/3.0/mods-enabled/detail.log

including configuration file /etc/freeradius/3.0/mods-enabled/digest

including configuration file /etc/freeradius/3.0/mods-enabled/dynamic\_clients

including configuration file /etc/freeradius/3.0/mods-enabled/eap

including configuration file /etc/freeradius/3.0/mods-enabled/echo

including configuration file /etc/freeradius/3.0/mods-enabled/exec

including configuration file /etc/freeradius/3.0/mods-enabled/expiration

including configuration file /etc/freeradius/3.0/mods-enabled/expr

including configuration file /etc/freeradius/3.0/mods-enabled/files

including configuration file /etc/freeradius/3.0/mods-enabled/linelog

including configuration file /etc/freeradius/3.0/mods-enabled/logintime

including configuration file /etc/freeradius/3.0/mods-enabled/mschap

including configuration file /etc/freeradius/3.0/mods-enabled/ntlm\_auth

including configuration file /etc/freeradius/3.0/mods-enabled/pap

including configuration file /etc/freeradius/3.0/mods-enabled/passwd

including configuration file /etc/freeradius/3.0/mods-enabled/preprocess

including configuration file /etc/freeradius/3.0/mods-enabled/radutmp

including configuration file /etc/freeradius/3.0/mods-enabled/realm

including configuration file /etc/freeradius/3.0/mods-enabled/replicate

including configuration file /etc/freeradius/3.0/mods-enabled/soh

including configuration file /etc/freeradius/3.0/mods-enabled/sradutmp

including configuration file /etc/freeradius/3.0/mods-enabled/unix

including configuration file /etc/freeradius/3.0/mods-enabled/unpack

including configuration file /etc/freeradius/3.0/mods-enabled/utf8

including files in directory /etc/freeradius/3.0/policy.d/

including configuration file /etc/freeradius/3.0/policy.d/abfab-tr

including configuration file /etc/freeradius/3.0/policy.d/accounting

including configuration file /etc/freeradius/3.0/policy.d/canonicalization

including configuration file /etc/freeradius/3.0/policy.d/control

including configuration file /etc/freeradius/3.0/policy.d/cui

including configuration file /etc/freeradius/3.0/policy.d/debug

including configuration file /etc/freeradius/3.0/policy.d/dhcp

including configuration file /etc/freeradius/3.0/policy.d/eap

including configuration file /etc/freeradius/3.0/policy.d/filter

including configuration file /etc/freeradius/3.0/policy.d/moonshot-targeted-ids

including configuration file /etc/freeradius/3.0/policy.d/operator-name

including configuration file /etc/freeradius/3.0/policy.d/rfc7542

including files in directory /etc/freeradius/3.0/sites-enabled/

including configuration file /etc/freeradius/3.0/sites-enabled/default

including configuration file /etc/freeradius/3.0/sites-enabled/inner-tunnel

main {

security {

user = "freerad"

group = "freerad"

allow\_core\_dumps = no

}

name = "freeradius"

prefix = "/usr"

localstatedir = "/var"

logdir = "/var/log/freeradius"

run\_dir = "/var/run/freeradius"

}

main {

name = "freeradius"

prefix = "/usr"

localstatedir = "/var"

sbindir = "/usr/sbin"

logdir = "/var/log/freeradius"

run\_dir = "/var/run/freeradius"

libdir = "/usr/lib/freeradius"

radacctdir = "/var/log/freeradius/radacct"

hostname\_lookups = no

max\_request\_time = 30

cleanup\_delay = 5

max\_requests = 16384

postauth\_client\_lost = no

pidfile = "/var/run/freeradius/freeradius.pid"

checkrad = "/usr/sbin/checkrad"

debug\_level = 0

proxy\_requests = yes

log {

stripped\_names = no

auth = no

auth\_badpass = no

auth\_goodpass = no

colourise = yes

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

}

resources {

}

security {

max\_attributes = 200

reject\_delay = 1.000000

status\_server = yes

}

}

radiusd: #### Loading Realms and Home Servers ####

proxy server {

retry\_delay = 5

retry\_count = 3

default\_fallback = no

dead\_time = 120

wake\_all\_if\_all\_dead = no

}

home\_server localhost {

ipaddr = 127.0.0.1

port = 1812

type = "auth"

secret = <<< secret >>>

response\_window = 20.000000

response\_timeouts = 1

max\_outstanding = 65536

zombie\_period = 40

status\_check = "status-server"

ping\_interval = 30

check\_interval = 30

check\_timeout = 4

num\_answers\_to\_alive = 3

revive\_interval = 120

limit {

max\_connections = 16

max\_requests = 0

lifetime = 0

idle\_timeout = 0

}

coa {

irt = 2

mrt = 16

mrc = 5

mrd = 30

}

}

home\_server\_pool my\_auth\_failover {

type = fail-over

home\_server = localhost

}

realm example.com {

auth\_pool = my\_auth\_failover

}

realm LOCAL {

}

radiusd: #### Loading Clients ####

client localhost {

ipaddr = 127.0.0.1

require\_message\_authenticator = no

secret = <<< secret >>>

nas\_type = "other"

proto = "\*"

limit {

max\_connections = 16

lifetime = 0

idle\_timeout = 30

}

}

client localhost\_ipv6 {

ipv6addr = ::1

require\_message\_authenticator = no

secret = <<< secret >>>

limit {

max\_connections = 16

lifetime = 0

idle\_timeout = 30

}

}

Debugger not attached

systemd watchdog is disabled

# Creating Auth-Type = mschap

# Creating Auth-Type = digest

# Creating Auth-Type = eap

# Creating Auth-Type = PAP

# Creating Auth-Type = CHAP

# Creating Auth-Type = MS-CHAP

# Creating Autz-Type = New-TLS-Connection

radiusd: #### Instantiating modules ####

modules {

# Loaded module rlm\_always

# Loading module "reject" from file /etc/freeradius/3.0/mods-enabled/always

always reject {

rcode = "reject"

simulcount = 0

mpp = no

}

# Loading module "fail" from file /etc/freeradius/3.0/mods-enabled/always

always fail {

rcode = "fail"

simulcount = 0

mpp = no

}

# Loading module "ok" from file /etc/freeradius/3.0/mods-enabled/always

always ok {

rcode = "ok"

simulcount = 0

mpp = no

}

# Loading module "handled" from file /etc/freeradius/3.0/mods-enabled/always

always handled {

rcode = "handled"

simulcount = 0

mpp = no

}

# Loading module "invalid" from file /etc/freeradius/3.0/mods-enabled/always

always invalid {

rcode = "invalid"

simulcount = 0

mpp = no

}

# Loading module "userlock" from file /etc/freeradius/3.0/mods-enabled/always

always userlock {

rcode = "userlock"

simulcount = 0

mpp = no

}

# Loading module "notfound" from file /etc/freeradius/3.0/mods-enabled/always

always notfound {

rcode = "notfound"

simulcount = 0

mpp = no

}

# Loading module "noop" from file /etc/freeradius/3.0/mods-enabled/always

always noop {

rcode = "noop"

simulcount = 0

mpp = no

}

# Loading module "updated" from file /etc/freeradius/3.0/mods-enabled/always

always updated {

rcode = "updated"

simulcount = 0

mpp = no

}

# Loaded module rlm\_attr\_filter

# Loading module "attr\_filter.post-proxy" from file /etc/freeradius/3.0/mods-enabled/attr\_filter

attr\_filter attr\_filter.post-proxy {

filename = "/etc/freeradius/3.0/mods-config/attr\_filter/post-proxy"

key = "%{Realm}"

relaxed = no

}

# Loading module "attr\_filter.pre-proxy" from file /etc/freeradius/3.0/mods-enabled/attr\_filter

attr\_filter attr\_filter.pre-proxy {

filename = "/etc/freeradius/3.0/mods-config/attr\_filter/pre-proxy"

key = "%{Realm}"

relaxed = no

}

# Loading module "attr\_filter.access\_reject" from file /etc/freeradius/3.0/mods-enabled/attr\_filter

attr\_filter attr\_filter.access\_reject {

filename = "/etc/freeradius/3.0/mods-config/attr\_filter/access\_reject"

key = "%{User-Name}"

relaxed = no

}

# Loading module "attr\_filter.access\_challenge" from file /etc/freeradius/3.0/mods-enabled/attr\_filter

attr\_filter attr\_filter.access\_challenge {

filename = "/etc/freeradius/3.0/mods-config/attr\_filter/access\_challenge"

key = "%{User-Name}"

relaxed = no

}

# Loading module "attr\_filter.accounting\_response" from file /etc/freeradius/3.0/mods-enabled/attr\_filter

attr\_filter attr\_filter.accounting\_response {

filename = "/etc/freeradius/3.0/mods-config/attr\_filter/accounting\_response"

key = "%{User-Name}"

relaxed = no

}

# Loading module "attr\_filter.coa" from file /etc/freeradius/3.0/mods-enabled/attr\_filter

attr\_filter attr\_filter.coa {

filename = "/etc/freeradius/3.0/mods-config/attr\_filter/coa"

key = "%{User-Name}"

relaxed = no

}

# Loaded module rlm\_cache

# Loading module "cache\_eap" from file /etc/freeradius/3.0/mods-enabled/cache\_eap

cache cache\_eap {

driver = "rlm\_cache\_rbtree"

key = "%{%{control:State}:-%{%{reply:State}:-%{State}}}"

ttl = 15

max\_entries = 0

epoch = 0

add\_stats = no

}

# Loaded module rlm\_chap

# Loading module "chap" from file /etc/freeradius/3.0/mods-enabled/chap

# Loaded module rlm\_detail

# Loading module "detail" from file /etc/freeradius/3.0/mods-enabled/detail

detail {

filename = "/var/log/freeradius/radacct/%{%{Packet-Src-IP-Address}:-%{Packet-Src-IPv6-Address}}/detail-%Y%m%d"

header = "%t"

permissions = 384

locking = no

escape\_filenames = no

log\_packet\_header = no

}

# Loading module "auth\_log" from file /etc/freeradius/3.0/mods-enabled/detail.log

detail auth\_log {

filename = "/var/log/freeradius/radacct/%{%{Packet-Src-IP-Address}:-%{Packet-Src-IPv6-Address}}/auth-detail-%Y%m%d"

header = "%t"

permissions = 384

locking = no

escape\_filenames = no

log\_packet\_header = no

}

# Loading module "reply\_log" from file /etc/freeradius/3.0/mods-enabled/detail.log

detail reply\_log {

filename = "/var/log/freeradius/radacct/%{%{Packet-Src-IP-Address}:-%{Packet-Src-IPv6-Address}}/reply-detail-%Y%m%d"

header = "%t"

permissions = 384

locking = no

escape\_filenames = no

log\_packet\_header = no

}

# Loading module "pre\_proxy\_log" from file /etc/freeradius/3.0/mods-enabled/detail.log

detail pre\_proxy\_log {

filename = "/var/log/freeradius/radacct/%{%{Packet-Src-IP-Address}:-%{Packet-Src-IPv6-Address}}/pre-proxy-detail-%Y%m%d"

header = "%t"

permissions = 384

locking = no

escape\_filenames = no

log\_packet\_header = no

}

# Loading module "post\_proxy\_log" from file /etc/freeradius/3.0/mods-enabled/detail.log

detail post\_proxy\_log {

filename = "/var/log/freeradius/radacct/%{%{Packet-Src-IP-Address}:-%{Packet-Src-IPv6-Address}}/post-proxy-detail-%Y%m%d"

header = "%t"

permissions = 384

locking = no

escape\_filenames = no

log\_packet\_header = no

}

# Loaded module rlm\_digest

# Loading module "digest" from file /etc/freeradius/3.0/mods-enabled/digest

# Loaded module rlm\_dynamic\_clients

# Loading module "dynamic\_clients" from file /etc/freeradius/3.0/mods-enabled/dynamic\_clients

# Loaded module rlm\_eap

# Loading module "eap" from file /etc/freeradius/3.0/mods-enabled/eap

eap {

default\_eap\_type = "md5"

timer\_expire = 60

ignore\_unknown\_eap\_types = no

cisco\_accounting\_username\_bug = no

max\_sessions = 16384

}

# Loaded module rlm\_exec

# Loading module "echo" from file /etc/freeradius/3.0/mods-enabled/echo

exec echo {

wait = yes

program = "/bin/echo %{User-Name}"

input\_pairs = "request"

output\_pairs = "reply"

shell\_escape = yes

}

# Loading module "exec" from file /etc/freeradius/3.0/mods-enabled/exec

exec {

wait = no

input\_pairs = "request"

shell\_escape = yes

timeout = 10

}

# Loaded module rlm\_expiration

# Loading module "expiration" from file /etc/freeradius/3.0/mods-enabled/expiration

# Loaded module rlm\_expr

# Loading module "expr" from file /etc/freeradius/3.0/mods-enabled/expr

expr {

safe\_characters = "@abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789.-\_: /äéöüàâæçèéêëîïôœùûüaÿÄÉÖÜßÀÂÆÇÈÉÊËÎÏÔŒÙÛÜŸ"

}

# Loaded module rlm\_files

# Loading module "files" from file /etc/freeradius/3.0/mods-enabled/files

files {

filename = "/etc/freeradius/3.0/mods-config/files/authorize"

acctusersfile = "/etc/freeradius/3.0/mods-config/files/accounting"

preproxy\_usersfile = "/etc/freeradius/3.0/mods-config/files/pre-proxy"

}

# Loaded module rlm\_linelog

# Loading module "linelog" from file /etc/freeradius/3.0/mods-enabled/linelog

linelog {

filename = "/var/log/freeradius/linelog"

escape\_filenames = no

syslog\_severity = "info"

permissions = 384

format = "This is a log message for %{User-Name}"

reference = "messages.%{%{reply:Packet-Type}:-default}"

}

# Loading module "log\_accounting" from file /etc/freeradius/3.0/mods-enabled/linelog

linelog log\_accounting {

filename = "/var/log/freeradius/linelog-accounting"

escape\_filenames = no

syslog\_severity = "info"

permissions = 384

format = ""

reference = "Accounting-Request.%{%{Acct-Status-Type}:-unknown}"

}

# Loaded module rlm\_logintime

# Loading module "logintime" from file /etc/freeradius/3.0/mods-enabled/logintime

logintime {

minimum\_timeout = 60

}

# Loaded module rlm\_mschap

# Loading module "mschap" from file /etc/freeradius/3.0/mods-enabled/mschap

mschap {

use\_mppe = yes

require\_encryption = no

require\_strong = no

with\_ntdomain\_hack = yes

passchange {

}

allow\_retry = yes

winbind\_retry\_with\_normalised\_username = no

}

# Loading module "ntlm\_auth" from file /etc/freeradius/3.0/mods-enabled/ntlm\_auth

exec ntlm\_auth {

wait = yes

program = "/path/to/ntlm\_auth --request-nt-key --domain=MYDOMAIN --username=%{mschap:User-Name} --password=%{User-Password}"

shell\_escape = yes

}

# Loaded module rlm\_pap

# Loading module "pap" from file /etc/freeradius/3.0/mods-enabled/pap

pap {

normalise = yes

}

# Loaded module rlm\_passwd

# Loading module "etc\_passwd" from file /etc/freeradius/3.0/mods-enabled/passwd

passwd etc\_passwd {

filename = "/etc/passwd"

format = "\*User-Name:Crypt-Password:"

delimiter = ":"

ignore\_nislike = no

ignore\_empty = yes

allow\_multiple\_keys = no

hash\_size = 100

}

# Loaded module rlm\_preprocess

# Loading module "preprocess" from file /etc/freeradius/3.0/mods-enabled/preprocess

preprocess {

huntgroups = "/etc/freeradius/3.0/mods-config/preprocess/huntgroups"

hints = "/etc/freeradius/3.0/mods-config/preprocess/hints"

with\_ascend\_hack = no

ascend\_channels\_per\_line = 23

with\_ntdomain\_hack = no

with\_specialix\_jetstream\_hack = no

with\_cisco\_vsa\_hack = no

with\_alvarion\_vsa\_hack = no

}

# Loaded module rlm\_radutmp

# Loading module "radutmp" from file /etc/freeradius/3.0/mods-enabled/radutmp

radutmp {

filename = "/var/log/freeradius/radutmp"

username = "%{User-Name}"

case\_sensitive = yes

check\_with\_nas = yes

permissions = 384

caller\_id = yes

}

# Loaded module rlm\_realm

# Loading module "IPASS" from file /etc/freeradius/3.0/mods-enabled/realm

realm IPASS {

format = "prefix"

delimiter = "/"

ignore\_default = no

ignore\_null = no

}

# Loading module "suffix" from file /etc/freeradius/3.0/mods-enabled/realm

realm suffix {

format = "suffix"

delimiter = "@"

ignore\_default = no

ignore\_null = no

}

# Loading module "bangpath" from file /etc/freeradius/3.0/mods-enabled/realm

realm bangpath {

format = "prefix"

delimiter = "!"

ignore\_default = no

ignore\_null = no

}

# Loading module "realmpercent" from file /etc/freeradius/3.0/mods-enabled/realm

realm realmpercent {

format = "suffix"

delimiter = "%"

ignore\_default = no

ignore\_null = no

}

# Loading module "ntdomain" from file /etc/freeradius/3.0/mods-enabled/realm

realm ntdomain {

format = "prefix"

delimiter = "\\"

ignore\_default = no

ignore\_null = no

}

# Loaded module rlm\_replicate

# Loading module "replicate" from file /etc/freeradius/3.0/mods-enabled/replicate

# Loaded module rlm\_soh

# Loading module "soh" from file /etc/freeradius/3.0/mods-enabled/soh

soh {

dhcp = yes

}

# Loading module "sradutmp" from file /etc/freeradius/3.0/mods-enabled/sradutmp

radutmp sradutmp {

filename = "/var/log/freeradius/sradutmp"

username = "%{User-Name}"

case\_sensitive = yes

check\_with\_nas = yes

permissions = 420

caller\_id = no

}

# Loaded module rlm\_unix

# Loading module "unix" from file /etc/freeradius/3.0/mods-enabled/unix

unix {

radwtmp = "/var/log/freeradius/radwtmp"

}

Creating attribute Unix-Group

# Loaded module rlm\_unpack

# Loading module "unpack" from file /etc/freeradius/3.0/mods-enabled/unpack

# Loaded module rlm\_utf8

# Loading module "utf8" from file /etc/freeradius/3.0/mods-enabled/utf8

instantiate {

}

# Instantiating module "reject" from file /etc/freeradius/3.0/mods-enabled/always

# Instantiating module "fail" from file /etc/freeradius/3.0/mods-enabled/always

# Instantiating module "ok" from file /etc/freeradius/3.0/mods-enabled/always

# Instantiating module "handled" from file /etc/freeradius/3.0/mods-enabled/always

# Instantiating module "invalid" from file /etc/freeradius/3.0/mods-enabled/always

# Instantiating module "userlock" from file /etc/freeradius/3.0/mods-enabled/always

# Instantiating module "notfound" from file /etc/freeradius/3.0/mods-enabled/always

# Instantiating module "noop" from file /etc/freeradius/3.0/mods-enabled/always

# Instantiating module "updated" from file /etc/freeradius/3.0/mods-enabled/always

# Instantiating module "attr\_filter.post-proxy" from file /etc/freeradius/3.0/mods-enabled/attr\_filter

reading pairlist file /etc/freeradius/3.0/mods-config/attr\_filter/post-proxy

# Instantiating module "attr\_filter.pre-proxy" from file /etc/freeradius/3.0/mods-enabled/attr\_filter

reading pairlist file /etc/freeradius/3.0/mods-config/attr\_filter/pre-proxy

# Instantiating module "attr\_filter.access\_reject" from file /etc/freeradius/3.0/mods-enabled/attr\_filter

reading pairlist file /etc/freeradius/3.0/mods-config/attr\_filter/access\_reject

# Instantiating module "attr\_filter.access\_challenge" from file /etc/freeradius/3.0/mods-enabled/attr\_filter

reading pairlist file /etc/freeradius/3.0/mods-config/attr\_filter/access\_challenge

# Instantiating module "attr\_filter.accounting\_response" from file /etc/freeradius/3.0/mods-enabled/attr\_filter

reading pairlist file /etc/freeradius/3.0/mods-config/attr\_filter/accounting\_response

# Instantiating module "attr\_filter.coa" from file /etc/freeradius/3.0/mods-enabled/attr\_filter

reading pairlist file /etc/freeradius/3.0/mods-config/attr\_filter/coa

# Instantiating module "cache\_eap" from file /etc/freeradius/3.0/mods-enabled/cache\_eap

rlm\_cache (cache\_eap): Driver rlm\_cache\_rbtree (module rlm\_cache\_rbtree) loaded and linked

# Instantiating module "detail" from file /etc/freeradius/3.0/mods-enabled/detail

# Instantiating module "auth\_log" from file /etc/freeradius/3.0/mods-enabled/detail.log

rlm\_detail (auth\_log): 'User-Password' suppressed, will not appear in detail output

# Instantiating module "reply\_log" from file /etc/freeradius/3.0/mods-enabled/detail.log

# Instantiating module "pre\_proxy\_log" from file /etc/freeradius/3.0/mods-enabled/detail.log

# Instantiating module "post\_proxy\_log" from file /etc/freeradius/3.0/mods-enabled/detail.log

# Instantiating module "eap" from file /etc/freeradius/3.0/mods-enabled/eap

# Linked to sub-module rlm\_eap\_md5

# Linked to sub-module rlm\_eap\_gtc

gtc {

challenge = "Password: "

auth\_type = "PAP"

}

# Linked to sub-module rlm\_eap\_tls

tls {

tls = "tls-common"

}

tls-config tls-common {

verify\_depth = 0

ca\_path = "/etc/freeradius/3.0/certs"

pem\_file\_type = yes

private\_key\_file = "/etc/ssl/private/ssl-cert-snakeoil.key"

certificate\_file = "/etc/ssl/certs/ssl-cert-snakeoil.pem"

ca\_file = "/etc/ssl/certs/ca-certificates.crt"

private\_key\_password = <<< secret >>>

fragment\_size = 1024

include\_length = yes

auto\_chain = yes

check\_crl = no

check\_all\_crl = no

ca\_path\_reload\_interval = 0

cipher\_list = "DEFAULT"

cipher\_server\_preference = no

reject\_unknown\_intermediate\_ca = no

ecdh\_curve = ""

tls\_max\_version = "1.2"

tls\_min\_version = "1.2"

cache {

enable = no

lifetime = 24

max\_entries = 255

}

verify {

skip\_if\_ocsp\_ok = no

}

ocsp {

enable = no

override\_cert\_url = yes

url = "http://127.0.0.1/ocsp/"

use\_nonce = yes

timeout = 0

softfail = no

}

}

# Linked to sub-module rlm\_eap\_ttls

ttls {

tls = "tls-common"

default\_eap\_type = "md5"

copy\_request\_to\_tunnel = no

use\_tunneled\_reply = no

virtual\_server = "inner-tunnel"

include\_length = yes

require\_client\_cert = no

}

tls: Using cached TLS configuration from previous invocation

# Linked to sub-module rlm\_eap\_peap

peap {

tls = "tls-common"

default\_eap\_type = "mschapv2"

copy\_request\_to\_tunnel = no

use\_tunneled\_reply = no

proxy\_tunneled\_request\_as\_eap = yes

virtual\_server = "inner-tunnel"

soh = no

require\_client\_cert = no

}

tls: Using cached TLS configuration from previous invocation

# Linked to sub-module rlm\_eap\_mschapv2

mschapv2 {

with\_ntdomain\_hack = no

send\_error = no

}

# Instantiating module "expiration" from file /etc/freeradius/3.0/mods-enabled/expiration

# Instantiating module "files" from file /etc/freeradius/3.0/mods-enabled/files

reading pairlist file /etc/freeradius/3.0/mods-config/files/authorize

reading pairlist file /etc/freeradius/3.0/mods-config/files/accounting

reading pairlist file /etc/freeradius/3.0/mods-config/files/pre-proxy

# Instantiating module "linelog" from file /etc/freeradius/3.0/mods-enabled/linelog

# Instantiating module "log\_accounting" from file /etc/freeradius/3.0/mods-enabled/linelog

# Instantiating module "logintime" from file /etc/freeradius/3.0/mods-enabled/logintime

# Instantiating module "mschap" from file /etc/freeradius/3.0/mods-enabled/mschap

rlm\_mschap (mschap): using internal authentication

# Instantiating module "pap" from file /etc/freeradius/3.0/mods-enabled/pap

# Instantiating module "etc\_passwd" from file /etc/freeradius/3.0/mods-enabled/passwd

rlm\_passwd: nfields: 3 keyfield 0(User-Name) listable: no

# Instantiating module "preprocess" from file /etc/freeradius/3.0/mods-enabled/preprocess

reading pairlist file /etc/freeradius/3.0/mods-config/preprocess/huntgroups

reading pairlist file /etc/freeradius/3.0/mods-config/preprocess/hints

# Instantiating module "IPASS" from file /etc/freeradius/3.0/mods-enabled/realm

# Instantiating module "suffix" from file /etc/freeradius/3.0/mods-enabled/realm

# Instantiating module "bangpath" from file /etc/freeradius/3.0/mods-enabled/realm

# Instantiating module "realmpercent" from file /etc/freeradius/3.0/mods-enabled/realm

# Instantiating module "ntdomain" from file /etc/freeradius/3.0/mods-enabled/realm

} # modules

radiusd: #### Loading Virtual Servers ####

server { # from file /etc/freeradius/3.0/radiusd.conf

} # server

server default { # from file /etc/freeradius/3.0/sites-enabled/default

# Loading authenticate {...}

Compiling Auth-Type PAP for attr Auth-Type

Compiling Auth-Type CHAP for attr Auth-Type

Compiling Auth-Type MS-CHAP for attr Auth-Type

# Loading authorize {...}

Ignoring "sql" (see raddb/mods-available/README.rst)

Ignoring "ldap" (see raddb/mods-available/README.rst)

Compiling Autz-Type New-TLS-Connection for attr Autz-Type

# Loading preacct {...}

# Loading accounting {...}

# Loading post-proxy {...}

# Loading post-auth {...}

Compiling Post-Auth-Type REJECT for attr Post-Auth-Type

Compiling Post-Auth-Type Challenge for attr Post-Auth-Type

Compiling Post-Auth-Type Client-Lost for attr Post-Auth-Type

} # server default

server inner-tunnel { # from file /etc/freeradius/3.0/sites-enabled/inner-tunnel

# Loading authenticate {...}

Compiling Auth-Type PAP for attr Auth-Type

Compiling Auth-Type CHAP for attr Auth-Type

Compiling Auth-Type MS-CHAP for attr Auth-Type

# Loading authorize {...}

# Loading session {...}

# Loading post-proxy {...}

# Loading post-auth {...}

# Skipping contents of 'if' as it is always 'false' -- /etc/freeradius/3.0/sites-enabled/inner-tunnel:336

Compiling Post-Auth-Type REJECT for attr Post-Auth-Type

} # server inner-tunnel

radiusd: #### Opening IP addresses and Ports ####

listen {

type = "auth"

ipaddr = \*

port = 0

limit {

max\_connections = 16

lifetime = 0

idle\_timeout = 30

}

}

listen {

type = "acct"

ipaddr = \*

port = 0

limit {

max\_connections = 16

lifetime = 0

idle\_timeout = 30

}

}

listen {

type = "auth"

ipv6addr = ::

port = 0

limit {

max\_connections = 16

lifetime = 0

idle\_timeout = 30

}

}

listen {

type = "acct"

ipv6addr = ::

port = 0

limit {

max\_connections = 16

lifetime = 0

idle\_timeout = 30

}

}

listen {

type = "auth"

ipaddr = 127.0.0.1

port = 18120

}

Listening on auth address \* port 1812 bound to server default

Listening on acct address \* port 1813 bound to server default

Listening on auth address :: port 1812 bound to server default

Listening on acct address :: port 1813 bound to server default

Listening on auth address 127.0.0.1 port 18120 bound to server inner-tunnel

Listening on proxy address \* port 59661

Listening on proxy address :: port 59662

Ready to process requests

(0) Received Access-Request Id 0 from 127.0.0.1:58189 to 127.0.0.1:1812 length 127

(0) User-Name = "steve"

(0) NAS-IP-Address = 127.0.0.1

(0) Calling-Station-Id = "02-00-00-00-00-01"

(0) Framed-MTU = 1400

(0) NAS-Port-Type = Wireless-802.11

(0) Service-Type = Framed-User

(0) Connect-Info = "CONNECT 11Mbps 802.11b"

(0) Called-Station-Id = ""

(0) EAP-Message = 0x025a000a017374657665

(0) Message-Authenticator = 0xcbac7619f7a5de186dd2d7830ac80d53

(0) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default

(0) authorize {

(0) policy filter\_username {

(0) if (&User-Name) {

(0) if (&User-Name) -> TRUE

(0) if (&User-Name) {

(0) if (&User-Name =~ / /) {

(0) if (&User-Name =~ / /) -> FALSE

(0) if (&User-Name =~ /@[^@]\*@/ ) {

(0) if (&User-Name =~ /@[^@]\*@/ ) -> FALSE

(0) if (&User-Name =~ /\.\./ ) {

(0) if (&User-Name =~ /\.\./ ) -> FALSE

(0) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) {

(0) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) -> FALSE

(0) if (&User-Name =~ /\.$/) {

(0) if (&User-Name =~ /\.$/) -> FALSE

(0) if (&User-Name =~ /@\./) {

(0) if (&User-Name =~ /@\./) -> FALSE

(0) } # if (&User-Name) = notfound

(0) } # policy filter\_username = notfound

(0) [preprocess] = ok

(0) [chap] = noop

(0) [mschap] = noop

(0) [digest] = noop

(0) suffix: Checking for suffix after "@"

(0) suffix: No '@' in User-Name = "steve", looking up realm NULL

(0) suffix: No such realm "NULL"

(0) [suffix] = noop

(0) eap: Peer sent EAP Response (code 2) ID 90 length 10

(0) eap: EAP-Identity reply, returning 'ok' so we can short-circuit the rest of authorize

(0) [eap] = ok

(0) } # authorize = ok

(0) Found Auth-Type = eap

(0) # Executing group from file /etc/freeradius/3.0/sites-enabled/default

(0) authenticate {

(0) eap: Peer sent packet with method EAP Identity (1)

(0) eap: Calling submodule eap\_md5 to process data

(0) eap\_md5: Issuing MD5 Challenge

(0) eap: Sending EAP Request (code 1) ID 91 length 22

(0) eap: EAP session adding &reply:State = 0xbba36915bbf86d12

(0) [eap] = handled

(0) } # authenticate = handled

(0) Using Post-Auth-Type Challenge

(0) # Executing group from file /etc/freeradius/3.0/sites-enabled/default

(0) Challenge { ... } # empty sub-section is ignored

(0) Sent Access-Challenge Id 0 from 127.0.0.1:1812 to 127.0.0.1:58189 length 80

(0) EAP-Message = 0x015b0016041040bddd902bbc1f665d1c5179007af55f

(0) Message-Authenticator = 0x00000000000000000000000000000000

(0) State = 0xbba36915bbf86d121edc031d7fd267ce

(0) Finished request

Waking up in 4.9 seconds.

(1) Received Access-Request Id 1 from 127.0.0.1:58189 to 127.0.0.1:1812 length 141

(1) User-Name = "steve"

(1) NAS-IP-Address = 127.0.0.1

(1) Calling-Station-Id = "02-00-00-00-00-01"

(1) Framed-MTU = 1400

(1) NAS-Port-Type = Wireless-802.11

(1) Service-Type = Framed-User

(1) Connect-Info = "CONNECT 11Mbps 802.11b"

(1) Called-Station-Id = ""

(1) EAP-Message = 0x025b00060319

(1) State = 0xbba36915bbf86d121edc031d7fd267ce

(1) Message-Authenticator = 0xb6c364e8349d3c1ff4b9ba621b105e69

(1) session-state: No cached attributes

(1) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default

(1) authorize {

(1) policy filter\_username {

(1) if (&User-Name) {

(1) if (&User-Name) -> TRUE

(1) if (&User-Name) {

(1) if (&User-Name =~ / /) {

(1) if (&User-Name =~ / /) -> FALSE

(1) if (&User-Name =~ /@[^@]\*@/ ) {

(1) if (&User-Name =~ /@[^@]\*@/ ) -> FALSE

(1) if (&User-Name =~ /\.\./ ) {

(1) if (&User-Name =~ /\.\./ ) -> FALSE

(1) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) {

(1) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) -> FALSE

(1) if (&User-Name =~ /\.$/) {

(1) if (&User-Name =~ /\.$/) -> FALSE

(1) if (&User-Name =~ /@\./) {

(1) if (&User-Name =~ /@\./) -> FALSE

(1) } # if (&User-Name) = notfound

(1) } # policy filter\_username = notfound

(1) [preprocess] = ok

(1) [chap] = noop

(1) [mschap] = noop

(1) [digest] = noop

(1) suffix: Checking for suffix after "@"

(1) suffix: No '@' in User-Name = "steve", looking up realm NULL

(1) suffix: No such realm "NULL"

(1) [suffix] = noop

(1) eap: Peer sent EAP Response (code 2) ID 91 length 6

(1) eap: No EAP Start, assuming it's an on-going EAP conversation

(1) [eap] = updated

(1) files: users: Matched entry steve at line 74

(1) [files] = ok

(1) [expiration] = noop

(1) [logintime] = noop

(1) pap: WARNING: Auth-Type already set. Not setting to PAP

(1) [pap] = noop

(1) } # authorize = updated

(1) Found Auth-Type = eap

(1) # Executing group from file /etc/freeradius/3.0/sites-enabled/default

(1) authenticate {

(1) eap: Expiring EAP session with state 0xbba36915bbf86d12

(1) eap: Finished EAP session with state 0xbba36915bbf86d12

(1) eap: Previous EAP request found for state 0xbba36915bbf86d12, released from the list

(1) eap: Peer sent packet with method EAP NAK (3)

(1) eap: Found mutually acceptable type PEAP (25)

(1) eap: Calling submodule eap\_peap to process data

(1) eap\_peap: (TLS) Initiating new session

(1) eap: Sending EAP Request (code 1) ID 92 length 6

(1) eap: EAP session adding &reply:State = 0xbba36915baff7012

(1) [eap] = handled

(1) } # authenticate = handled

(1) Using Post-Auth-Type Challenge

(1) # Executing group from file /etc/freeradius/3.0/sites-enabled/default

(1) Challenge { ... } # empty sub-section is ignored

(1) session-state: Saving cached attributes

(1) Framed-MTU = 994

(1) Sent Access-Challenge Id 1 from 127.0.0.1:1812 to 127.0.0.1:58189 length 64

(1) EAP-Message = 0x015c00061920

(1) Message-Authenticator = 0x00000000000000000000000000000000

(1) State = 0xbba36915baff70121edc031d7fd267ce

(1) Finished request

Waking up in 4.9 seconds.

(2) Received Access-Request Id 2 from 127.0.0.1:58189 to 127.0.0.1:1812 length 329

(2) User-Name = "steve"

(2) NAS-IP-Address = 127.0.0.1

(2) Calling-Station-Id = "02-00-00-00-00-01"

(2) Framed-MTU = 1400

(2) NAS-Port-Type = Wireless-802.11

(2) Service-Type = Framed-User

(2) Connect-Info = "CONNECT 11Mbps 802.11b"

(2) Called-Station-Id = ""

(2) EAP-Message = 0x025c00c21980000000b816030100b3010000af0303112bf2e6feec867d904587f9e51597a7e8766483eaf2341c55c707611df9f15d000038c02cc030009fcca9cca8ccaac02bc02f009ec024c028006bc023c0270067c00ac0140039c009c0130033009d009c003d003c0035002f00ff0100004e000b000403000102000a000c000a001d0017001e001900180016000000170000000d002a0028040305030603080708080809080a080b080408050806040105010601030303010302040205020602

(2) State = 0xbba36915baff70121edc031d7fd267ce

(2) Message-Authenticator = 0xf3e75a3777fc3b37274559d931953d86

(2) Restoring &session-state

(2) &session-state:Framed-MTU = 994

(2) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default

(2) authorize {

(2) policy filter\_username {

(2) if (&User-Name) {

(2) if (&User-Name) -> TRUE

(2) if (&User-Name) {

(2) if (&User-Name =~ / /) {

(2) if (&User-Name =~ / /) -> FALSE

(2) if (&User-Name =~ /@[^@]\*@/ ) {

(2) if (&User-Name =~ /@[^@]\*@/ ) -> FALSE

(2) if (&User-Name =~ /\.\./ ) {

(2) if (&User-Name =~ /\.\./ ) -> FALSE

(2) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) {

(2) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) -> FALSE

(2) if (&User-Name =~ /\.$/) {

(2) if (&User-Name =~ /\.$/) -> FALSE

(2) if (&User-Name =~ /@\./) {

(2) if (&User-Name =~ /@\./) -> FALSE

(2) } # if (&User-Name) = notfound

(2) } # policy filter\_username = notfound

(2) [preprocess] = ok

(2) [chap] = noop

(2) [mschap] = noop

(2) [digest] = noop

(2) suffix: Checking for suffix after "@"

(2) suffix: No '@' in User-Name = "steve", looking up realm NULL

(2) suffix: No such realm "NULL"

(2) [suffix] = noop

(2) eap: Peer sent EAP Response (code 2) ID 92 length 194

(2) eap: Continuing tunnel setup

(2) [eap] = ok

(2) } # authorize = ok

(2) Found Auth-Type = eap

(2) # Executing group from file /etc/freeradius/3.0/sites-enabled/default

(2) authenticate {

(2) eap: Expiring EAP session with state 0xbba36915baff7012

(2) eap: Finished EAP session with state 0xbba36915baff7012

(2) eap: Previous EAP request found for state 0xbba36915baff7012, released from the list

(2) eap: Peer sent packet with method EAP PEAP (25)

(2) eap: Calling submodule eap\_peap to process data

(2) eap\_peap: (TLS) EAP Peer says that the final record size will be 184 bytes

(2) eap\_peap: (TLS) EAP Got all data (184 bytes)

(2) eap\_peap: (TLS) Handshake state - before SSL initialization

(2) eap\_peap: (TLS) Handshake state - Server before SSL initialization

(2) eap\_peap: (TLS) Handshake state - Server before SSL initialization

(2) eap\_peap: (TLS) recv TLS 1.3 Handshake, ClientHello

(2) eap\_peap: (TLS) Handshake state - Server SSLv3/TLS read client hello

(2) eap\_peap: (TLS) send TLS 1.2 Handshake, ServerHello

(2) eap\_peap: (TLS) Handshake state - Server SSLv3/TLS write server hello

(2) eap\_peap: (TLS) send TLS 1.2 Handshake, Certificate

(2) eap\_peap: (TLS) Handshake state - Server SSLv3/TLS write certificate

(2) eap\_peap: (TLS) send TLS 1.2 Handshake, ServerKeyExchange

(2) eap\_peap: (TLS) Handshake state - Server SSLv3/TLS write key exchange

(2) eap\_peap: (TLS) send TLS 1.2 Handshake, ServerHelloDone

(2) eap\_peap: (TLS) Handshake state - Server SSLv3/TLS write server done

(2) eap\_peap: (TLS) Server : Need to read more data: SSLv3/TLS write server done

(2) eap\_peap: (TLS) In Handshake Phase

(2) eap: Sending EAP Request (code 1) ID 93 length 1004

(2) eap: EAP session adding &reply:State = 0xbba36915b9fe7012

(2) [eap] = handled

(2) } # authenticate = handled

(2) Using Post-Auth-Type Challenge

(2) # Executing group from file /etc/freeradius/3.0/sites-enabled/default

(2) Challenge { ... } # empty sub-section is ignored

(2) session-state: Saving cached attributes

(2) Framed-MTU = 994

(2) TLS-Session-Information = "(TLS) recv TLS 1.3 Handshake, ClientHello"

(2) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHello"

(2) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Certificate"

(2) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerKeyExchange"

(2) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHelloDone"

(2) Sent Access-Challenge Id 2 from 127.0.0.1:1812 to 127.0.0.1:58189 length 1068

(2) EAP-Message = 

(2) Message-Authenticator = 0x00000000000000000000000000000000

(2) State = 0xbba36915b9fe70121edc031d7fd267ce

(2) Finished request

Waking up in 4.9 seconds.

(3) Received Access-Request Id 3 from 127.0.0.1:58189 to 127.0.0.1:1812 length 141

(3) User-Name = "steve"

(3) NAS-IP-Address = 127.0.0.1

(3) Calling-Station-Id = "02-00-00-00-00-01"

(3) Framed-MTU = 1400

(3) NAS-Port-Type = Wireless-802.11

(3) Service-Type = Framed-User

(3) Connect-Info = "CONNECT 11Mbps 802.11b"

(3) Called-Station-Id = ""

(3) EAP-Message = 0x025d00061900

(3) State = 0xbba36915b9fe70121edc031d7fd267ce

(3) Message-Authenticator = 0x3a4001bfdc40abe4e811c905c81c17e4

(3) Restoring &session-state

(3) &session-state:Framed-MTU = 994

(3) &session-state:TLS-Session-Information = "(TLS) recv TLS 1.3 Handshake, ClientHello"

(3) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHello"

(3) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Certificate"

(3) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerKeyExchange"

(3) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHelloDone"

(3) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default

(3) authorize {

(3) policy filter\_username {

(3) if (&User-Name) {

(3) if (&User-Name) -> TRUE

(3) if (&User-Name) {

(3) if (&User-Name =~ / /) {

(3) if (&User-Name =~ / /) -> FALSE

(3) if (&User-Name =~ /@[^@]\*@/ ) {

(3) if (&User-Name =~ /@[^@]\*@/ ) -> FALSE

(3) if (&User-Name =~ /\.\./ ) {

(3) if (&User-Name =~ /\.\./ ) -> FALSE

(3) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) {

(3) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) -> FALSE

(3) if (&User-Name =~ /\.$/) {

(3) if (&User-Name =~ /\.$/) -> FALSE

(3) if (&User-Name =~ /@\./) {

(3) if (&User-Name =~ /@\./) -> FALSE

(3) } # if (&User-Name) = notfound

(3) } # policy filter\_username = notfound

(3) [preprocess] = ok

(3) [chap] = noop

(3) [mschap] = noop

(3) [digest] = noop

(3) suffix: Checking for suffix after "@"

(3) suffix: No '@' in User-Name = "steve", looking up realm NULL

(3) suffix: No such realm "NULL"

(3) [suffix] = noop

(3) eap: Peer sent EAP Response (code 2) ID 93 length 6

(3) eap: Continuing tunnel setup

(3) [eap] = ok

(3) } # authorize = ok

(3) Found Auth-Type = eap

(3) # Executing group from file /etc/freeradius/3.0/sites-enabled/default

(3) authenticate {

(3) eap: Expiring EAP session with state 0xbba36915b9fe7012

(3) eap: Finished EAP session with state 0xbba36915b9fe7012

(3) eap: Previous EAP request found for state 0xbba36915b9fe7012, released from the list

(3) eap: Peer sent packet with method EAP PEAP (25)

(3) eap: Calling submodule eap\_peap to process data

(3) eap\_peap: (TLS) Peer ACKed our handshake fragment

(3) eap: Sending EAP Request (code 1) ID 94 length 192

(3) eap: EAP session adding &reply:State = 0xbba36915b8fd7012

(3) [eap] = handled

(3) } # authenticate = handled

(3) Using Post-Auth-Type Challenge

(3) # Executing group from file /etc/freeradius/3.0/sites-enabled/default

(3) Challenge { ... } # empty sub-section is ignored

(3) session-state: Saving cached attributes

(3) Framed-MTU = 994

(3) TLS-Session-Information = "(TLS) recv TLS 1.3 Handshake, ClientHello"

(3) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHello"

(3) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Certificate"

(3) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerKeyExchange"

(3) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHelloDone"

(3) Sent Access-Challenge Id 3 from 127.0.0.1:1812 to 127.0.0.1:58189 length 250

(3) EAP-Message = 0x015e00c01900f94e9f08c2081be2b2fcb56d99c27072408a9e75a4d904ce749fac6d9a2b788d65fc75c436208fbf7b7019a2e1e1a9fe3700f2c2c713ce6d691396b810818b46329457b2e01321c0384cf9b60f93fae825d5a1fc90e1f311589b47b51c4fa57e2974e62af34bea78f6ab62a4ccede13cd3ddad11b3b7a3dc5106663ead4b879a91a9407820ce83a264b71ef1289194597a30196c0d2c5cb60df600c18a4c4717f1c26852b219e74bdf77ec8884f4f973b016030300040e000000

(3) Message-Authenticator = 0x00000000000000000000000000000000

(3) State = 0xbba36915b8fd70121edc031d7fd267ce

(3) Finished request

Waking up in 4.9 seconds.

(4) Received Access-Request Id 4 from 127.0.0.1:58189 to 127.0.0.1:1812 length 238

(4) User-Name = "steve"

(4) NAS-IP-Address = 127.0.0.1

(4) Calling-Station-Id = "02-00-00-00-00-01"

(4) Framed-MTU = 1400

(4) NAS-Port-Type = Wireless-802.11

(4) Service-Type = Framed-User

(4) Connect-Info = "CONNECT 11Mbps 802.11b"

(4) Called-Station-Id = ""

(4) EAP-Message = 0x025e006719800000005d16030300251000002120f34072912b4860173a551a191b3ff35476084d3a8e7eb85255de322563883b38140303000101160303002822a33ba6ce9acbcce8f8fb44a1958c572f8f6209c7ae006e06481cd0165a4f93314bf7e0d5555a73

(4) State = 0xbba36915b8fd70121edc031d7fd267ce

(4) Message-Authenticator = 0xcf2c4689295c643119dd594ce3dbfea7

(4) Restoring &session-state

(4) &session-state:Framed-MTU = 994

(4) &session-state:TLS-Session-Information = "(TLS) recv TLS 1.3 Handshake, ClientHello"

(4) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHello"

(4) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Certificate"

(4) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerKeyExchange"

(4) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHelloDone"

(4) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default

(4) authorize {

(4) policy filter\_username {

(4) if (&User-Name) {

(4) if (&User-Name) -> TRUE

(4) if (&User-Name) {

(4) if (&User-Name =~ / /) {

(4) if (&User-Name =~ / /) -> FALSE

(4) if (&User-Name =~ /@[^@]\*@/ ) {

(4) if (&User-Name =~ /@[^@]\*@/ ) -> FALSE

(4) if (&User-Name =~ /\.\./ ) {

(4) if (&User-Name =~ /\.\./ ) -> FALSE

(4) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) {

(4) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) -> FALSE

(4) if (&User-Name =~ /\.$/) {

(4) if (&User-Name =~ /\.$/) -> FALSE

(4) if (&User-Name =~ /@\./) {

(4) if (&User-Name =~ /@\./) -> FALSE

(4) } # if (&User-Name) = notfound

(4) } # policy filter\_username = notfound

(4) [preprocess] = ok

(4) [chap] = noop

(4) [mschap] = noop

(4) [digest] = noop

(4) suffix: Checking for suffix after "@"

(4) suffix: No '@' in User-Name = "steve", looking up realm NULL

(4) suffix: No such realm "NULL"

(4) [suffix] = noop

(4) eap: Peer sent EAP Response (code 2) ID 94 length 103

(4) eap: Continuing tunnel setup

(4) [eap] = ok

(4) } # authorize = ok

(4) Found Auth-Type = eap

(4) # Executing group from file /etc/freeradius/3.0/sites-enabled/default

(4) authenticate {

(4) eap: Expiring EAP session with state 0xbba36915b8fd7012

(4) eap: Finished EAP session with state 0xbba36915b8fd7012

(4) eap: Previous EAP request found for state 0xbba36915b8fd7012, released from the list

(4) eap: Peer sent packet with method EAP PEAP (25)

(4) eap: Calling submodule eap\_peap to process data

(4) eap\_peap: (TLS) EAP Peer says that the final record size will be 93 bytes

(4) eap\_peap: (TLS) EAP Got all data (93 bytes)

(4) eap\_peap: (TLS) Handshake state - Server SSLv3/TLS write server done

(4) eap\_peap: (TLS) recv TLS 1.2 Handshake, ClientKeyExchange

(4) eap\_peap: (TLS) Handshake state - Server SSLv3/TLS read client key exchange

(4) eap\_peap: (TLS) Handshake state - Server SSLv3/TLS read change cipher spec

(4) eap\_peap: (TLS) recv TLS 1.2 Handshake, Finished

(4) eap\_peap: (TLS) Handshake state - Server SSLv3/TLS read finished

(4) eap\_peap: (TLS) send TLS 1.2 ChangeCipherSpec

(4) eap\_peap: (TLS) Handshake state - Server SSLv3/TLS write change cipher spec

(4) eap\_peap: (TLS) send TLS 1.2 Handshake, Finished

(4) eap\_peap: (TLS) Handshake state - Server SSLv3/TLS write finished

(4) eap\_peap: (TLS) Handshake state - SSL negotiation finished successfully

(4) eap\_peap: (TLS) Connection Established

(4) eap\_peap: TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-GCM-SHA384"

(4) eap\_peap: TLS-Session-Version = "TLS 1.2"

(4) eap: Sending EAP Request (code 1) ID 95 length 57

(4) eap: EAP session adding &reply:State = 0xbba36915bffc7012

(4) [eap] = handled

(4) } # authenticate = handled

(4) Using Post-Auth-Type Challenge

(4) # Executing group from file /etc/freeradius/3.0/sites-enabled/default

(4) Challenge { ... } # empty sub-section is ignored

(4) session-state: Saving cached attributes

(4) Framed-MTU = 994

(4) TLS-Session-Information = "(TLS) recv TLS 1.3 Handshake, ClientHello"

(4) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHello"

(4) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Certificate"

(4) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerKeyExchange"

(4) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHelloDone"

(4) TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, ClientKeyExchange"

(4) TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, Finished"

(4) TLS-Session-Information = "(TLS) send TLS 1.2 ChangeCipherSpec"

(4) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Finished"

(4) TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-GCM-SHA384"

(4) TLS-Session-Version = "TLS 1.2"

(4) Sent Access-Challenge Id 4 from 127.0.0.1:1812 to 127.0.0.1:58189 length 115

(4) EAP-Message = 0x015f003919001403030001011603030028e412d7b20c8f7f341a781028eb43c1e2638618a38da9a98ff46eab6867233fc7f873a2888499764b

(4) Message-Authenticator = 0x00000000000000000000000000000000

(4) State = 0xbba36915bffc70121edc031d7fd267ce

(4) Finished request

Waking up in 4.9 seconds.

(5) Received Access-Request Id 5 from 127.0.0.1:58189 to 127.0.0.1:1812 length 141

(5) User-Name = "steve"

(5) NAS-IP-Address = 127.0.0.1

(5) Calling-Station-Id = "02-00-00-00-00-01"

(5) Framed-MTU = 1400

(5) NAS-Port-Type = Wireless-802.11

(5) Service-Type = Framed-User

(5) Connect-Info = "CONNECT 11Mbps 802.11b"

(5) Called-Station-Id = ""

(5) EAP-Message = 0x025f00061900

(5) State = 0xbba36915bffc70121edc031d7fd267ce

(5) Message-Authenticator = 0x98292578e3a4870dec17e2f2b3fa810e

(5) Restoring &session-state

(5) &session-state:Framed-MTU = 994

(5) &session-state:TLS-Session-Information = "(TLS) recv TLS 1.3 Handshake, ClientHello"

(5) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHello"

(5) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Certificate"

(5) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerKeyExchange"

(5) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHelloDone"

(5) &session-state:TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, ClientKeyExchange"

(5) &session-state:TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, Finished"

(5) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 ChangeCipherSpec"

(5) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Finished"

(5) &session-state:TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-GCM-SHA384"

(5) &session-state:TLS-Session-Version = "TLS 1.2"

(5) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default

(5) authorize {

(5) policy filter\_username {

(5) if (&User-Name) {

(5) if (&User-Name) -> TRUE

(5) if (&User-Name) {

(5) if (&User-Name =~ / /) {

(5) if (&User-Name =~ / /) -> FALSE

(5) if (&User-Name =~ /@[^@]\*@/ ) {

(5) if (&User-Name =~ /@[^@]\*@/ ) -> FALSE

(5) if (&User-Name =~ /\.\./ ) {

(5) if (&User-Name =~ /\.\./ ) -> FALSE

(5) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) {

(5) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) -> FALSE

(5) if (&User-Name =~ /\.$/) {

(5) if (&User-Name =~ /\.$/) -> FALSE

(5) if (&User-Name =~ /@\./) {

(5) if (&User-Name =~ /@\./) -> FALSE

(5) } # if (&User-Name) = notfound

(5) } # policy filter\_username = notfound

(5) [preprocess] = ok

(5) [chap] = noop

(5) [mschap] = noop

(5) [digest] = noop

(5) suffix: Checking for suffix after "@"

(5) suffix: No '@' in User-Name = "steve", looking up realm NULL

(5) suffix: No such realm "NULL"

(5) [suffix] = noop

(5) eap: Peer sent EAP Response (code 2) ID 95 length 6

(5) eap: Continuing tunnel setup

(5) [eap] = ok

(5) } # authorize = ok

(5) Found Auth-Type = eap

(5) # Executing group from file /etc/freeradius/3.0/sites-enabled/default

(5) authenticate {

(5) eap: Expiring EAP session with state 0xbba36915bffc7012

(5) eap: Finished EAP session with state 0xbba36915bffc7012

(5) eap: Previous EAP request found for state 0xbba36915bffc7012, released from the list

(5) eap: Peer sent packet with method EAP PEAP (25)

(5) eap: Calling submodule eap\_peap to process data

(5) eap\_peap: (TLS) Peer ACKed our handshake fragment. handshake is finished

(5) eap\_peap: Session established. Decoding tunneled attributes

(5) eap\_peap: PEAP state TUNNEL ESTABLISHED

(5) eap: Sending EAP Request (code 1) ID 96 length 40

(5) eap: EAP session adding &reply:State = 0xbba36915bec37012

(5) [eap] = handled

(5) } # authenticate = handled

(5) Using Post-Auth-Type Challenge

(5) # Executing group from file /etc/freeradius/3.0/sites-enabled/default

(5) Challenge { ... } # empty sub-section is ignored

(5) session-state: Saving cached attributes

(5) Framed-MTU = 994

(5) TLS-Session-Information = "(TLS) recv TLS 1.3 Handshake, ClientHello"

(5) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHello"

(5) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Certificate"

(5) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerKeyExchange"

(5) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHelloDone"

(5) TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, ClientKeyExchange"

(5) TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, Finished"

(5) TLS-Session-Information = "(TLS) send TLS 1.2 ChangeCipherSpec"

(5) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Finished"

(5) TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-GCM-SHA384"

(5) TLS-Session-Version = "TLS 1.2"

(5) Sent Access-Challenge Id 5 from 127.0.0.1:1812 to 127.0.0.1:58189 length 98

(5) EAP-Message = 0x016000281900170303001de412d7b20c8f7f35035baf254407cd1415c2507c6599ae8bb7c50517e3

(5) Message-Authenticator = 0x00000000000000000000000000000000

(5) State = 0xbba36915bec370121edc031d7fd267ce

(5) Finished request

Waking up in 4.9 seconds.

(6) Received Access-Request Id 6 from 127.0.0.1:58189 to 127.0.0.1:1812 length 176

(6) User-Name = "steve"

(6) NAS-IP-Address = 127.0.0.1

(6) Calling-Station-Id = "02-00-00-00-00-01"

(6) Framed-MTU = 1400

(6) NAS-Port-Type = Wireless-802.11

(6) Service-Type = Framed-User

(6) Connect-Info = "CONNECT 11Mbps 802.11b"

(6) Called-Station-Id = ""

(6) EAP-Message = 0x026000291900170303001e22a33ba6ce9acbcd4afc1d4161fd5ecee0b22568f8ad7afe331f5523c818

(6) State = 0xbba36915bec370121edc031d7fd267ce

(6) Message-Authenticator = 0x1b2357013a9f6493c045d9ead1971fe9

(6) Restoring &session-state

(6) &session-state:Framed-MTU = 994

(6) &session-state:TLS-Session-Information = "(TLS) recv TLS 1.3 Handshake, ClientHello"

(6) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHello"

(6) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Certificate"

(6) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerKeyExchange"

(6) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHelloDone"

(6) &session-state:TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, ClientKeyExchange"

(6) &session-state:TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, Finished"

(6) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 ChangeCipherSpec"

(6) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Finished"

(6) &session-state:TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-GCM-SHA384"

(6) &session-state:TLS-Session-Version = "TLS 1.2"

(6) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default

(6) authorize {

(6) policy filter\_username {

(6) if (&User-Name) {

(6) if (&User-Name) -> TRUE

(6) if (&User-Name) {

(6) if (&User-Name =~ / /) {

(6) if (&User-Name =~ / /) -> FALSE

(6) if (&User-Name =~ /@[^@]\*@/ ) {

(6) if (&User-Name =~ /@[^@]\*@/ ) -> FALSE

(6) if (&User-Name =~ /\.\./ ) {

(6) if (&User-Name =~ /\.\./ ) -> FALSE

(6) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) {

(6) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) -> FALSE

(6) if (&User-Name =~ /\.$/) {

(6) if (&User-Name =~ /\.$/) -> FALSE

(6) if (&User-Name =~ /@\./) {

(6) if (&User-Name =~ /@\./) -> FALSE

(6) } # if (&User-Name) = notfound

(6) } # policy filter\_username = notfound

(6) [preprocess] = ok

(6) [chap] = noop

(6) [mschap] = noop

(6) [digest] = noop

(6) suffix: Checking for suffix after "@"

(6) suffix: No '@' in User-Name = "steve", looking up realm NULL

(6) suffix: No such realm "NULL"

(6) [suffix] = noop

(6) eap: Peer sent EAP Response (code 2) ID 96 length 41

(6) eap: Continuing tunnel setup

(6) [eap] = ok

(6) } # authorize = ok

(6) Found Auth-Type = eap

(6) # Executing group from file /etc/freeradius/3.0/sites-enabled/default

(6) authenticate {

(6) eap: Expiring EAP session with state 0xbba36915bec37012

(6) eap: Finished EAP session with state 0xbba36915bec37012

(6) eap: Previous EAP request found for state 0xbba36915bec37012, released from the list

(6) eap: Peer sent packet with method EAP PEAP (25)

(6) eap: Calling submodule eap\_peap to process data

(6) eap\_peap: (TLS) EAP Done initial handshake

(6) eap\_peap: Session established. Decoding tunneled attributes

(6) eap\_peap: PEAP state WAITING FOR INNER IDENTITY

(6) eap\_peap: Identity - steve

(6) eap\_peap: Got inner identity 'steve'

(6) eap\_peap: Setting default EAP type for tunneled EAP session

(6) eap\_peap: Got tunneled request

(6) eap\_peap: EAP-Message = 0x0260000a017374657665

(6) eap\_peap: Setting User-Name to steve

(6) eap\_peap: Sending tunneled request to inner-tunnel

(6) eap\_peap: EAP-Message = 0x0260000a017374657665

(6) eap\_peap: FreeRADIUS-Proxied-To = 127.0.0.1

(6) eap\_peap: User-Name = "steve"

(6) Virtual server inner-tunnel received request

(6) EAP-Message = 0x0260000a017374657665

(6) FreeRADIUS-Proxied-To = 127.0.0.1

(6) User-Name = "steve"

(6) WARNING: Outer and inner identities are the same. User privacy is compromised.

(6) server inner-tunnel {

(6) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/inner-tunnel

(6) authorize {

(6) policy filter\_username {

(6) if (&User-Name) {

(6) if (&User-Name) -> TRUE

(6) if (&User-Name) {

(6) if (&User-Name =~ / /) {

(6) if (&User-Name =~ / /) -> FALSE

(6) if (&User-Name =~ /@[^@]\*@/ ) {

(6) if (&User-Name =~ /@[^@]\*@/ ) -> FALSE

(6) if (&User-Name =~ /\.\./ ) {

(6) if (&User-Name =~ /\.\./ ) -> FALSE

(6) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) {

(6) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) -> FALSE

(6) if (&User-Name =~ /\.$/) {

(6) if (&User-Name =~ /\.$/) -> FALSE

(6) if (&User-Name =~ /@\./) {

(6) if (&User-Name =~ /@\./) -> FALSE

(6) } # if (&User-Name) = notfound

(6) } # policy filter\_username = notfound

(6) [chap] = noop

(6) [mschap] = noop

(6) suffix: Checking for suffix after "@"

(6) suffix: No '@' in User-Name = "steve", looking up realm NULL

(6) suffix: No such realm "NULL"

(6) [suffix] = noop

(6) update control {

(6) &Proxy-To-Realm := LOCAL

(6) } # update control = noop

(6) eap: Peer sent EAP Response (code 2) ID 96 length 10

(6) eap: EAP-Identity reply, returning 'ok' so we can short-circuit the rest of authorize

(6) [eap] = ok

(6) } # authorize = ok

(6) Found Auth-Type = eap

(6) # Executing group from file /etc/freeradius/3.0/sites-enabled/inner-tunnel

(6) authenticate {

(6) eap: Peer sent packet with method EAP Identity (1)

(6) eap: Calling submodule eap\_mschapv2 to process data

(6) eap\_mschapv2: Issuing Challenge

(6) eap: Sending EAP Request (code 1) ID 97 length 43

(6) eap: EAP session adding &reply:State = 0xd7d95441d7b84e51

(6) [eap] = handled

(6) } # authenticate = handled

(6) } # server inner-tunnel

(6) Virtual server sending reply

(6) EAP-Message = 0x0161002b1a016100261064390bd0f9d0c65a458d4b68a2e21ccc667265657261646975732d332e302e3236

(6) Message-Authenticator = 0x00000000000000000000000000000000

(6) State = 0xd7d95441d7b84e5173423a5242b003f7

(6) eap\_peap: Got tunneled reply code 11

(6) eap\_peap: EAP-Message = 0x0161002b1a016100261064390bd0f9d0c65a458d4b68a2e21ccc667265657261646975732d332e302e3236

(6) eap\_peap: Message-Authenticator = 0x00000000000000000000000000000000

(6) eap\_peap: State = 0xd7d95441d7b84e5173423a5242b003f7

(6) eap\_peap: Got tunneled reply RADIUS code 11

(6) eap\_peap: EAP-Message = 0x0161002b1a016100261064390bd0f9d0c65a458d4b68a2e21ccc667265657261646975732d332e302e3236

(6) eap\_peap: Message-Authenticator = 0x00000000000000000000000000000000

(6) eap\_peap: State = 0xd7d95441d7b84e5173423a5242b003f7

(6) eap\_peap: Got tunneled Access-Challenge

(6) eap: Sending EAP Request (code 1) ID 97 length 74

(6) eap: EAP session adding &reply:State = 0xbba36915bdc27012

(6) [eap] = handled

(6) } # authenticate = handled

(6) Using Post-Auth-Type Challenge

(6) # Executing group from file /etc/freeradius/3.0/sites-enabled/default

(6) Challenge { ... } # empty sub-section is ignored

(6) session-state: Saving cached attributes

(6) Framed-MTU = 994

(6) TLS-Session-Information = "(TLS) recv TLS 1.3 Handshake, ClientHello"

(6) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHello"

(6) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Certificate"

(6) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerKeyExchange"

(6) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHelloDone"

(6) TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, ClientKeyExchange"

(6) TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, Finished"

(6) TLS-Session-Information = "(TLS) send TLS 1.2 ChangeCipherSpec"

(6) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Finished"

(6) TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-GCM-SHA384"

(6) TLS-Session-Version = "TLS 1.2"

(6) Sent Access-Challenge Id 6 from 127.0.0.1:1812 to 127.0.0.1:58189 length 132

(6) EAP-Message = 0x0161004a1900170303003fe412d7b20c8f7f36e3127590b5f4475ee61292a80f40f3c1d545337245101c02b308baa8808b1d712fbee85ba19555035d88311dd974cd3d6a0d2a645ba79f

(6) Message-Authenticator = 0x00000000000000000000000000000000

(6) State = 0xbba36915bdc270121edc031d7fd267ce

(6) Finished request

Waking up in 4.9 seconds.

(7) Received Access-Request Id 7 from 127.0.0.1:58189 to 127.0.0.1:1812 length 230

(7) User-Name = "steve"

(7) NAS-IP-Address = 127.0.0.1

(7) Calling-Station-Id = "02-00-00-00-00-01"

(7) Framed-MTU = 1400

(7) NAS-Port-Type = Wireless-802.11

(7) Service-Type = Framed-User

(7) Connect-Info = "CONNECT 11Mbps 802.11b"

(7) Called-Station-Id = ""

(7) EAP-Message = 0x0261005f1900170303005422a33ba6ce9acbce6640d785078050775c2fb944d5cef0382dcc791a2bf1e4bd6fab8af14067be91c263ce51160a6187c01ea806bc6734be5510d5b3497ff49d6c42b31b5928b65ee87ce0887ee6af0c743abc1d

(7) State = 0xbba36915bdc270121edc031d7fd267ce

(7) Message-Authenticator = 0x3357d9b554c129a462554016524d96bc

(7) Restoring &session-state

(7) &session-state:Framed-MTU = 994

(7) &session-state:TLS-Session-Information = "(TLS) recv TLS 1.3 Handshake, ClientHello"

(7) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHello"

(7) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Certificate"

(7) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerKeyExchange"

(7) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHelloDone"

(7) &session-state:TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, ClientKeyExchange"

(7) &session-state:TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, Finished"

(7) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 ChangeCipherSpec"

(7) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Finished"

(7) &session-state:TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-GCM-SHA384"

(7) &session-state:TLS-Session-Version = "TLS 1.2"

(7) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default

(7) authorize {

(7) policy filter\_username {

(7) if (&User-Name) {

(7) if (&User-Name) -> TRUE

(7) if (&User-Name) {

(7) if (&User-Name =~ / /) {

(7) if (&User-Name =~ / /) -> FALSE

(7) if (&User-Name =~ /@[^@]\*@/ ) {

(7) if (&User-Name =~ /@[^@]\*@/ ) -> FALSE

(7) if (&User-Name =~ /\.\./ ) {

(7) if (&User-Name =~ /\.\./ ) -> FALSE

(7) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) {

(7) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) -> FALSE

(7) if (&User-Name =~ /\.$/) {

(7) if (&User-Name =~ /\.$/) -> FALSE

(7) if (&User-Name =~ /@\./) {

(7) if (&User-Name =~ /@\./) -> FALSE

(7) } # if (&User-Name) = notfound

(7) } # policy filter\_username = notfound

(7) [preprocess] = ok

(7) [chap] = noop

(7) [mschap] = noop

(7) [digest] = noop

(7) suffix: Checking for suffix after "@"

(7) suffix: No '@' in User-Name = "steve", looking up realm NULL

(7) suffix: No such realm "NULL"

(7) [suffix] = noop

(7) eap: Peer sent EAP Response (code 2) ID 97 length 95

(7) eap: Continuing tunnel setup

(7) [eap] = ok

(7) } # authorize = ok

(7) Found Auth-Type = eap

(7) # Executing group from file /etc/freeradius/3.0/sites-enabled/default

(7) authenticate {

(7) eap: Expiring EAP session with state 0xd7d95441d7b84e51

(7) eap: Finished EAP session with state 0xbba36915bdc27012

(7) eap: Previous EAP request found for state 0xbba36915bdc27012, released from the list

(7) eap: Peer sent packet with method EAP PEAP (25)

(7) eap: Calling submodule eap\_peap to process data

(7) eap\_peap: (TLS) EAP Done initial handshake

(7) eap\_peap: Session established. Decoding tunneled attributes

(7) eap\_peap: PEAP state phase2

(7) eap\_peap: EAP method MSCHAPv2 (26)

(7) eap\_peap: Got tunneled request

(7) eap\_peap: EAP-Message = 0x026100401a0261003b31691a0e1f159beae45ae8529cc4ea3f3d0000000000000000d38e43ef75819f17f883e8ef3e02913c7f86eef18adebfd9007374657665

(7) eap\_peap: Setting User-Name to steve

(7) eap\_peap: Sending tunneled request to inner-tunnel

(7) eap\_peap: EAP-Message = 0x026100401a0261003b31691a0e1f159beae45ae8529cc4ea3f3d0000000000000000d38e43ef75819f17f883e8ef3e02913c7f86eef18adebfd9007374657665

(7) eap\_peap: FreeRADIUS-Proxied-To = 127.0.0.1

(7) eap\_peap: User-Name = "steve"

(7) eap\_peap: State = 0xd7d95441d7b84e5173423a5242b003f7

(7) Virtual server inner-tunnel received request

(7) EAP-Message = 0x026100401a0261003b31691a0e1f159beae45ae8529cc4ea3f3d0000000000000000d38e43ef75819f17f883e8ef3e02913c7f86eef18adebfd9007374657665

(7) FreeRADIUS-Proxied-To = 127.0.0.1

(7) User-Name = "steve"

(7) State = 0xd7d95441d7b84e5173423a5242b003f7

(7) WARNING: Outer and inner identities are the same. User privacy is compromised.

(7) server inner-tunnel {

(7) session-state: No cached attributes

(7) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/inner-tunnel

(7) authorize {

(7) policy filter\_username {

(7) if (&User-Name) {

(7) if (&User-Name) -> TRUE

(7) if (&User-Name) {

(7) if (&User-Name =~ / /) {

(7) if (&User-Name =~ / /) -> FALSE

(7) if (&User-Name =~ /@[^@]\*@/ ) {

(7) if (&User-Name =~ /@[^@]\*@/ ) -> FALSE

(7) if (&User-Name =~ /\.\./ ) {

(7) if (&User-Name =~ /\.\./ ) -> FALSE

(7) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) {

(7) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) -> FALSE

(7) if (&User-Name =~ /\.$/) {

(7) if (&User-Name =~ /\.$/) -> FALSE

(7) if (&User-Name =~ /@\./) {

(7) if (&User-Name =~ /@\./) -> FALSE

(7) } # if (&User-Name) = notfound

(7) } # policy filter\_username = notfound

(7) [chap] = noop

(7) [mschap] = noop

(7) suffix: Checking for suffix after "@"

(7) suffix: No '@' in User-Name = "steve", looking up realm NULL

(7) suffix: No such realm "NULL"

(7) [suffix] = noop

(7) update control {

(7) &Proxy-To-Realm := LOCAL

(7) } # update control = noop

(7) eap: Peer sent EAP Response (code 2) ID 97 length 64

(7) eap: No EAP Start, assuming it's an on-going EAP conversation

(7) [eap] = updated

(7) files: users: Matched entry steve at line 74

(7) [files] = ok

(7) [expiration] = noop

(7) [logintime] = noop

(7) pap: WARNING: Auth-Type already set. Not setting to PAP

(7) [pap] = noop

(7) } # authorize = updated

(7) Found Auth-Type = eap

(7) # Executing group from file /etc/freeradius/3.0/sites-enabled/inner-tunnel

(7) authenticate {

(7) eap: Expiring EAP session with state 0xd7d95441d7b84e51

(7) eap: Finished EAP session with state 0xd7d95441d7b84e51

(7) eap: Previous EAP request found for state 0xd7d95441d7b84e51, released from the list

(7) eap: Peer sent packet with method EAP MSCHAPv2 (26)

(7) eap: Calling submodule eap\_mschapv2 to process data

(7) eap\_mschapv2: # Executing group from file /etc/freeradius/3.0/sites-enabled/inner-tunnel

(7) eap\_mschapv2: authenticate {

(7) mschap: Found Cleartext-Password, hashing to create NT-Password

(7) mschap: Creating challenge hash with username: steve

(7) mschap: Client is using MS-CHAPv2

(7) mschap: Adding MS-CHAPv2 MPPE keys

(7) eap\_mschapv2: [mschap] = ok

(7) eap\_mschapv2: } # authenticate = ok

(7) eap\_mschapv2: MSCHAP Success

(7) eap: Sending EAP Request (code 1) ID 98 length 51

(7) eap: EAP session adding &reply:State = 0xd7d95441d6bb4e51

(7) [eap] = handled

(7) } # authenticate = handled

(7) } # server inner-tunnel

(7) Virtual server sending reply

(7) EAP-Message = 0x016200331a0361002e533d37433437334538383646463045424434424330383845463244444341433530464335323843463835

(7) Message-Authenticator = 0x00000000000000000000000000000000

(7) State = 0xd7d95441d6bb4e5173423a5242b003f7

(7) eap\_peap: Got tunneled reply code 11

(7) eap\_peap: EAP-Message = 0x016200331a0361002e533d37433437334538383646463045424434424330383845463244444341433530464335323843463835

(7) eap\_peap: Message-Authenticator = 0x00000000000000000000000000000000

(7) eap\_peap: State = 0xd7d95441d6bb4e5173423a5242b003f7

(7) eap\_peap: Got tunneled reply RADIUS code 11

(7) eap\_peap: EAP-Message = 0x016200331a0361002e533d37433437334538383646463045424434424330383845463244444341433530464335323843463835

(7) eap\_peap: Message-Authenticator = 0x00000000000000000000000000000000

(7) eap\_peap: State = 0xd7d95441d6bb4e5173423a5242b003f7

(7) eap\_peap: Got tunneled Access-Challenge

(7) eap: Sending EAP Request (code 1) ID 98 length 82

(7) eap: EAP session adding &reply:State = 0xbba36915bcc17012

(7) [eap] = handled

(7) } # authenticate = handled

(7) Using Post-Auth-Type Challenge

(7) # Executing group from file /etc/freeradius/3.0/sites-enabled/default

(7) Challenge { ... } # empty sub-section is ignored

(7) session-state: Saving cached attributes

(7) Framed-MTU = 994

(7) TLS-Session-Information = "(TLS) recv TLS 1.3 Handshake, ClientHello"

(7) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHello"

(7) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Certificate"

(7) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerKeyExchange"

(7) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHelloDone"

(7) TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, ClientKeyExchange"

(7) TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, Finished"

(7) TLS-Session-Information = "(TLS) send TLS 1.2 ChangeCipherSpec"

(7) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Finished"

(7) TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-GCM-SHA384"

(7) TLS-Session-Version = "TLS 1.2"

(7) Sent Access-Challenge Id 7 from 127.0.0.1:1812 to 127.0.0.1:58189 length 140

(7) EAP-Message = 0x0162005219001703030047e412d7b20c8f7f37ed37ed98a47350992eaabfe499dc5a75b5a899a5da0e63e38c8658be73ae0a0052aaf068524c61e5ba6afd1225dc53a6167038575ff7b148d82d6f95935d35

(7) Message-Authenticator = 0x00000000000000000000000000000000

(7) State = 0xbba36915bcc170121edc031d7fd267ce

(7) Finished request

Waking up in 4.9 seconds.

(8) Received Access-Request Id 8 from 127.0.0.1:58189 to 127.0.0.1:1812 length 172

(8) User-Name = "steve"

(8) NAS-IP-Address = 127.0.0.1

(8) Calling-Station-Id = "02-00-00-00-00-01"

(8) Framed-MTU = 1400

(8) NAS-Port-Type = Wireless-802.11

(8) Service-Type = Framed-User

(8) Connect-Info = "CONNECT 11Mbps 802.11b"

(8) Called-Station-Id = ""

(8) EAP-Message = 0x026200251900170303001a22a33ba6ce9acbcfc671ad85164d76e9482f98badc187c335b8d

(8) State = 0xbba36915bcc170121edc031d7fd267ce

(8) Message-Authenticator = 0x626521a8b204766eaf80b7732443cd52

(8) Restoring &session-state

(8) &session-state:Framed-MTU = 994

(8) &session-state:TLS-Session-Information = "(TLS) recv TLS 1.3 Handshake, ClientHello"

(8) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHello"

(8) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Certificate"

(8) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerKeyExchange"

(8) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHelloDone"

(8) &session-state:TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, ClientKeyExchange"

(8) &session-state:TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, Finished"

(8) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 ChangeCipherSpec"

(8) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Finished"

(8) &session-state:TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-GCM-SHA384"

(8) &session-state:TLS-Session-Version = "TLS 1.2"

(8) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default

(8) authorize {

(8) policy filter\_username {

(8) if (&User-Name) {

(8) if (&User-Name) -> TRUE

(8) if (&User-Name) {

(8) if (&User-Name =~ / /) {

(8) if (&User-Name =~ / /) -> FALSE

(8) if (&User-Name =~ /@[^@]\*@/ ) {

(8) if (&User-Name =~ /@[^@]\*@/ ) -> FALSE

(8) if (&User-Name =~ /\.\./ ) {

(8) if (&User-Name =~ /\.\./ ) -> FALSE

(8) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) {

(8) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) -> FALSE

(8) if (&User-Name =~ /\.$/) {

(8) if (&User-Name =~ /\.$/) -> FALSE

(8) if (&User-Name =~ /@\./) {

(8) if (&User-Name =~ /@\./) -> FALSE

(8) } # if (&User-Name) = notfound

(8) } # policy filter\_username = notfound

(8) [preprocess] = ok

(8) [chap] = noop

(8) [mschap] = noop

(8) [digest] = noop

(8) suffix: Checking for suffix after "@"

(8) suffix: No '@' in User-Name = "steve", looking up realm NULL

(8) suffix: No such realm "NULL"

(8) [suffix] = noop

(8) eap: Peer sent EAP Response (code 2) ID 98 length 37

(8) eap: Continuing tunnel setup

(8) [eap] = ok

(8) } # authorize = ok

(8) Found Auth-Type = eap

(8) # Executing group from file /etc/freeradius/3.0/sites-enabled/default

(8) authenticate {

(8) eap: Expiring EAP session with state 0xd7d95441d6bb4e51

(8) eap: Finished EAP session with state 0xbba36915bcc17012

(8) eap: Previous EAP request found for state 0xbba36915bcc17012, released from the list

(8) eap: Peer sent packet with method EAP PEAP (25)

(8) eap: Calling submodule eap\_peap to process data

(8) eap\_peap: (TLS) EAP Done initial handshake

(8) eap\_peap: Session established. Decoding tunneled attributes

(8) eap\_peap: PEAP state phase2

(8) eap\_peap: EAP method MSCHAPv2 (26)

(8) eap\_peap: Got tunneled request

(8) eap\_peap: EAP-Message = 0x026200061a03

(8) eap\_peap: Setting User-Name to steve

(8) eap\_peap: Sending tunneled request to inner-tunnel

(8) eap\_peap: EAP-Message = 0x026200061a03

(8) eap\_peap: FreeRADIUS-Proxied-To = 127.0.0.1

(8) eap\_peap: User-Name = "steve"

(8) eap\_peap: State = 0xd7d95441d6bb4e5173423a5242b003f7

(8) Virtual server inner-tunnel received request

(8) EAP-Message = 0x026200061a03

(8) FreeRADIUS-Proxied-To = 127.0.0.1

(8) User-Name = "steve"

(8) State = 0xd7d95441d6bb4e5173423a5242b003f7

(8) WARNING: Outer and inner identities are the same. User privacy is compromised.

(8) server inner-tunnel {

(8) session-state: No cached attributes

(8) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/inner-tunnel

(8) authorize {

(8) policy filter\_username {

(8) if (&User-Name) {

(8) if (&User-Name) -> TRUE

(8) if (&User-Name) {

(8) if (&User-Name =~ / /) {

(8) if (&User-Name =~ / /) -> FALSE

(8) if (&User-Name =~ /@[^@]\*@/ ) {

(8) if (&User-Name =~ /@[^@]\*@/ ) -> FALSE

(8) if (&User-Name =~ /\.\./ ) {

(8) if (&User-Name =~ /\.\./ ) -> FALSE

(8) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) {

(8) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) -> FALSE

(8) if (&User-Name =~ /\.$/) {

(8) if (&User-Name =~ /\.$/) -> FALSE

(8) if (&User-Name =~ /@\./) {

(8) if (&User-Name =~ /@\./) -> FALSE

(8) } # if (&User-Name) = notfound

(8) } # policy filter\_username = notfound

(8) [chap] = noop

(8) [mschap] = noop

(8) suffix: Checking for suffix after "@"

(8) suffix: No '@' in User-Name = "steve", looking up realm NULL

(8) suffix: No such realm "NULL"

(8) [suffix] = noop

(8) update control {

(8) &Proxy-To-Realm := LOCAL

(8) } # update control = noop

(8) eap: Peer sent EAP Response (code 2) ID 98 length 6

(8) eap: No EAP Start, assuming it's an on-going EAP conversation

(8) [eap] = updated

(8) files: users: Matched entry steve at line 74

(8) [files] = ok

(8) [expiration] = noop

(8) [logintime] = noop

(8) pap: WARNING: Auth-Type already set. Not setting to PAP

(8) [pap] = noop

(8) } # authorize = updated

(8) Found Auth-Type = eap

(8) # Executing group from file /etc/freeradius/3.0/sites-enabled/inner-tunnel

(8) authenticate {

(8) eap: Expiring EAP session with state 0xd7d95441d6bb4e51

(8) eap: Finished EAP session with state 0xd7d95441d6bb4e51

(8) eap: Previous EAP request found for state 0xd7d95441d6bb4e51, released from the list

(8) eap: Peer sent packet with method EAP MSCHAPv2 (26)

(8) eap: Calling submodule eap\_mschapv2 to process data

(8) eap: Sending EAP Success (code 3) ID 98 length 4

(8) eap: Freeing handler

(8) [eap] = ok

(8) } # authenticate = ok

(8) # Executing section post-auth from file /etc/freeradius/3.0/sites-enabled/inner-tunnel

(8) post-auth {

(8) if (0) {

(8) if (0) -> FALSE

(8) } # post-auth = noop

(8) } # server inner-tunnel

(8) Virtual server sending reply

(8) MS-MPPE-Encryption-Policy = Encryption-Allowed

(8) MS-MPPE-Encryption-Types = RC4-40or128-bit-Allowed

(8) MS-MPPE-Send-Key = 0x34f4cc08ed7b38eefaa789e688414db5

(8) MS-MPPE-Recv-Key = 0x954e35bdc2ea1f687cd5653d97dc18ea

(8) EAP-Message = 0x03620004

(8) Message-Authenticator = 0x00000000000000000000000000000000

(8) User-Name = "steve"

(8) eap\_peap: Got tunneled reply code 2

(8) eap\_peap: MS-MPPE-Encryption-Policy = Encryption-Allowed

(8) eap\_peap: MS-MPPE-Encryption-Types = RC4-40or128-bit-Allowed

(8) eap\_peap: MS-MPPE-Send-Key = 0x34f4cc08ed7b38eefaa789e688414db5

(8) eap\_peap: MS-MPPE-Recv-Key = 0x954e35bdc2ea1f687cd5653d97dc18ea

(8) eap\_peap: EAP-Message = 0x03620004

(8) eap\_peap: Message-Authenticator = 0x00000000000000000000000000000000

(8) eap\_peap: User-Name = "steve"

(8) eap\_peap: Got tunneled reply RADIUS code 2

(8) eap\_peap: MS-MPPE-Encryption-Policy = Encryption-Allowed

(8) eap\_peap: MS-MPPE-Encryption-Types = RC4-40or128-bit-Allowed

(8) eap\_peap: MS-MPPE-Send-Key = 0x34f4cc08ed7b38eefaa789e688414db5

(8) eap\_peap: MS-MPPE-Recv-Key = 0x954e35bdc2ea1f687cd5653d97dc18ea

(8) eap\_peap: EAP-Message = 0x03620004

(8) eap\_peap: Message-Authenticator = 0x00000000000000000000000000000000

(8) eap\_peap: User-Name = "steve"

(8) eap\_peap: Tunneled authentication was successful

(8) eap\_peap: SUCCESS

(8) eap: Sending EAP Request (code 1) ID 99 length 46

(8) eap: EAP session adding &reply:State = 0xbba36915b3c07012

(8) [eap] = handled

(8) } # authenticate = handled

(8) Using Post-Auth-Type Challenge

(8) # Executing group from file /etc/freeradius/3.0/sites-enabled/default

(8) Challenge { ... } # empty sub-section is ignored

(8) session-state: Saving cached attributes

(8) Framed-MTU = 994

(8) TLS-Session-Information = "(TLS) recv TLS 1.3 Handshake, ClientHello"

(8) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHello"

(8) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Certificate"

(8) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerKeyExchange"

(8) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHelloDone"

(8) TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, ClientKeyExchange"

(8) TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, Finished"

(8) TLS-Session-Information = "(TLS) send TLS 1.2 ChangeCipherSpec"

(8) TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Finished"

(8) TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-GCM-SHA384"

(8) TLS-Session-Version = "TLS 1.2"

(8) Sent Access-Challenge Id 8 from 127.0.0.1:1812 to 127.0.0.1:58189 length 104

(8) EAP-Message = 0x0163002e19001703030023e412d7b20c8f7f3892d3e4f0c538c85f7e7dbdd46829bffb72b6f9c7962b995b5d8b0c

(8) Message-Authenticator = 0x00000000000000000000000000000000

(8) State = 0xbba36915b3c070121edc031d7fd267ce

(8) Finished request

Waking up in 4.9 seconds.

(9) Received Access-Request Id 9 from 127.0.0.1:58189 to 127.0.0.1:1812 length 181

(9) User-Name = "steve"

(9) NAS-IP-Address = 127.0.0.1

(9) Calling-Station-Id = "02-00-00-00-00-01"

(9) Framed-MTU = 1400

(9) NAS-Port-Type = Wireless-802.11

(9) Service-Type = Framed-User

(9) Connect-Info = "CONNECT 11Mbps 802.11b"

(9) Called-Station-Id = ""

(9) EAP-Message = 0x0263002e1900170303002322a33ba6ce9acbd0954975bdd927db9b64b93ad6e898d2e6550c8ccbcd29378a0af8a7

(9) State = 0xbba36915b3c070121edc031d7fd267ce

(9) Message-Authenticator = 0x1cefc61c2acd150876896926aedea139

(9) Restoring &session-state

(9) &session-state:Framed-MTU = 994

(9) &session-state:TLS-Session-Information = "(TLS) recv TLS 1.3 Handshake, ClientHello"

(9) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHello"

(9) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Certificate"

(9) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerKeyExchange"

(9) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, ServerHelloDone"

(9) &session-state:TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, ClientKeyExchange"

(9) &session-state:TLS-Session-Information = "(TLS) recv TLS 1.2 Handshake, Finished"

(9) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 ChangeCipherSpec"

(9) &session-state:TLS-Session-Information = "(TLS) send TLS 1.2 Handshake, Finished"

(9) &session-state:TLS-Session-Cipher-Suite = "ECDHE-RSA-AES256-GCM-SHA384"

(9) &session-state:TLS-Session-Version = "TLS 1.2"

(9) # Executing section authorize from file /etc/freeradius/3.0/sites-enabled/default

(9) authorize {

(9) policy filter\_username {

(9) if (&User-Name) {

(9) if (&User-Name) -> TRUE

(9) if (&User-Name) {

(9) if (&User-Name =~ / /) {

(9) if (&User-Name =~ / /) -> FALSE

(9) if (&User-Name =~ /@[^@]\*@/ ) {

(9) if (&User-Name =~ /@[^@]\*@/ ) -> FALSE

(9) if (&User-Name =~ /\.\./ ) {

(9) if (&User-Name =~ /\.\./ ) -> FALSE

(9) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) {

(9) if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) -> FALSE

(9) if (&User-Name =~ /\.$/) {

(9) if (&User-Name =~ /\.$/) -> FALSE

(9) if (&User-Name =~ /@\./) {

(9) if (&User-Name =~ /@\./) -> FALSE

(9) } # if (&User-Name) = notfound

(9) } # policy filter\_username = notfound

(9) [preprocess] = ok

(9) [chap] = noop

(9) [mschap] = noop

(9) [digest] = noop

(9) suffix: Checking for suffix after "@"

(9) suffix: No '@' in User-Name = "steve", looking up realm NULL

(9) suffix: No such realm "NULL"

(9) [suffix] = noop

(9) eap: Peer sent EAP Response (code 2) ID 99 length 46

(9) eap: Continuing tunnel setup

(9) [eap] = ok

(9) } # authorize = ok

(9) Found Auth-Type = eap

(9) # Executing group from file /etc/freeradius/3.0/sites-enabled/default

(9) authenticate {

(9) eap: Expiring EAP session with state 0xbba36915b3c07012

(9) eap: Finished EAP session with state 0xbba36915b3c07012

(9) eap: Previous EAP request found for state 0xbba36915b3c07012, released from the list

(9) eap: Peer sent packet with method EAP PEAP (25)

(9) eap: Calling submodule eap\_peap to process data

(9) eap\_peap: (TLS) EAP Done initial handshake

(9) eap\_peap: Session established. Decoding tunneled attributes

(9) eap\_peap: PEAP state send tlv success

(9) eap\_peap: Received EAP-TLV response

(9) eap\_peap: Success

(9) eap: Sending EAP Success (code 3) ID 99 length 4

(9) eap: Freeing handler

(9) [eap] = ok

(9) } # authenticate = ok

(9) # Executing section post-auth from file /etc/freeradius/3.0/sites-enabled/default

(9) post-auth {

(9) if (session-state:User-Name && reply:User-Name && request:User-Name && (reply:User-Name == request:User-Name)) {

(9) if (session-state:User-Name && reply:User-Name && request:User-Name && (reply:User-Name == request:User-Name)) -> FALSE

(9) update {

(9) &reply::Framed-MTU += &session-state:Framed-MTU[\*] -> 994

(9) &reply::TLS-Session-Information += &session-state:TLS-Session-Information[\*] -> '(TLS) recv TLS 1.3 Handshake, ClientHello'

(9) &reply::TLS-Session-Information += &session-state:TLS-Session-Information[\*] -> '(TLS) send TLS 1.2 Handshake, ServerHello'

(9) &reply::TLS-Session-Information += &session-state:TLS-Session-Information[\*] -> '(TLS) send TLS 1.2 Handshake, Certificate'

(9) &reply::TLS-Session-Information += &session-state:TLS-Session-Information[\*] -> '(TLS) send TLS 1.2 Handshake, ServerKeyExchange'

(9) &reply::TLS-Session-Information += &session-state:TLS-Session-Information[\*] -> '(TLS) send TLS 1.2 Handshake, ServerHelloDone'

(9) &reply::TLS-Session-Information += &session-state:TLS-Session-Information[\*] -> '(TLS) recv TLS 1.2 Handshake, ClientKeyExchange'

(9) &reply::TLS-Session-Information += &session-state:TLS-Session-Information[\*] -> '(TLS) recv TLS 1.2 Handshake, Finished'

(9) &reply::TLS-Session-Information += &session-state:TLS-Session-Information[\*] -> '(TLS) send TLS 1.2 ChangeCipherSpec'

(9) &reply::TLS-Session-Information += &session-state:TLS-Session-Information[\*] -> '(TLS) send TLS 1.2 Handshake, Finished'

(9) &reply::TLS-Session-Cipher-Suite += &session-state:TLS-Session-Cipher-Suite[\*] -> 'ECDHE-RSA-AES256-GCM-SHA384'

(9) &reply::TLS-Session-Version += &session-state:TLS-Session-Version[\*] -> 'TLS 1.2'

(9) } # update = noop

(9) [exec] = noop

(9) policy remove\_reply\_message\_if\_eap {

(9) if (&reply:EAP-Message && &reply:Reply-Message) {

(9) if (&reply:EAP-Message && &reply:Reply-Message) -> FALSE

(9) else {

(9) [noop] = noop

(9) } # else = noop

(9) } # policy remove\_reply\_message\_if\_eap = noop

(9) if (EAP-Key-Name && &reply:EAP-Session-Id) {

(9) if (EAP-Key-Name && &reply:EAP-Session-Id) -> FALSE

(9) } # post-auth = noop

(9) Sent Access-Accept Id 9 from 127.0.0.1:1812 to 127.0.0.1:58189 length 173

(9) MS-MPPE-Recv-Key = 0xe12493812a87a9653222e3b0cd95159bd03b70d315053aa2c17e0b203b87eaa8

(9) MS-MPPE-Send-Key = 0xac7143995f971ae676db1c43de1225c52f596eebf65953c314ce3dfaceba5669

(9) EAP-Message = 0x03630004

(9) Message-Authenticator = 0x00000000000000000000000000000000

(9) User-Name = "steve"

(9) Framed-MTU += 994

(9) Finished request

Waking up in 4.9 seconds.

(0) Cleaning up request packet ID 0 with timestamp +52 due to cleanup\_delay was reached

(1) Cleaning up request packet ID 1 with timestamp +52 due to cleanup\_delay was reached

(2) Cleaning up request packet ID 2 with timestamp +52 due to cleanup\_delay was reached

(3) Cleaning up request packet ID 3 with timestamp +52 due to cleanup\_delay was reached

(4) Cleaning up request packet ID 4 with timestamp +52 due to cleanup\_delay was reached

(5) Cleaning up request packet ID 5 with timestamp +52 due to cleanup\_delay was reached

(6) Cleaning up request packet ID 6 with timestamp +52 due to cleanup\_delay was reached

(7) Cleaning up request packet ID 7 with timestamp +52 due to cleanup\_delay was reached

(8) Cleaning up request packet ID 8 with timestamp +52 due to cleanup\_delay was reached

(9) Cleaning up request packet ID 9 with timestamp +52 due to cleanup\_delay was reached

Ready to process requests