SecurityConfigurationCommands

Techroutes
NETWORK

TableofContents

1. AAA Configuration Commands

1.1. User commands

1.1.1. username

Thecommandcanbeusedforaddingtheusertothedatabaseoflocalusers, authentication of local method and authorization.The“no”formatof themethodcanbe usedfordeletingthecorrespondinguser.

Syntas

username*username*[**password**{*password*|[**trust-host***ip_address]*[**user-maxlinks***number*] [**callback-dialstring***string*] [**callback-line***line*][**callback-rotary***rotary*] [**nocallback-verify**] [**autocommand***command*]

no username *username*

Parameter

Parameter	Description
username	CharacterString of User Name
password	Thepassword correspondingtotheuser
password	Plaintext of character string ofpassword
maxlinks	Themaximumlinkstotherouter,thesameusercancreateatthesame time (Statistic ismade onlyto the userpassingthelocalauthentication.
Number	The number of links created at the same time.
callback-dialstring	Callbackthetelephonenumber(not supported).
String	Character stringof telephone number
callback-line	Thelineusedforcallback(not supported).
Line	Linenumber
callback-rotary	Callbackrotaryconfiguration(not supported).
Rotary	rotarynumber
nocallback-verify	Callbackisnotverified.(not supported).
autocommand	When theuser logsin therouter, thedesignated commandwill be executedautomatically.
command	Automatic execution of character string of thecommand.
nohangup	Prevent users from logging in and disconnecting after executing automatic commands (not supported).
noescape	Prevent users from using escape characters after logging in (not supported).

bind-ip	Set the IP address bound by the user.
A.B.C.D	Bind IPv4 addresses.
bind-mac	Set the MAC address bound by the user.
H:H:H:H:H:H	Bind MAC address.
bind-pool	Set the address pool bound by the user, and assign the address from the address pool after the remote user authentication.
WORD	Bind address pool name.
bind-port	Set the user authentication binding port.
INTERFACE	Bind port name. User authentication from other ports fails.
authen-group	Set user local authentication policy group.
WORD	Local user policy group name.
author-group	Set user local authorization policy group.
WORD	Local user authorization policy group name.
pass-group	Set user local password management policy group.
WORD	Local password management policy group name.

Default

No user

Command mode

globalconfigurationmode

Explanation

When there is no password parameter, the password is considered as an empty string.

Maxlinks limits the number of sessions that the same user name can establish with the router at the same time, but when a session of this user is not authenticated by local authentication, it will not be counted. You can use the show aaa users command to check whether each online user has passed the authentication.

At present, the encryption-type supported in our router system includes MD5 encryption and a self-defined encryption algorithm of our company, which correspond to different encryption-type parameter values. The meaning of each parameter value of encryption-type is as follows:

0, no encryption, clear text password will be entered, and clear text will be displayed when show running (equivalent to not using the encryption-type parameter);

4. If MD5 encryption is used, clear text password will be entered, and MD5 encrypted password will be displayed when show running.

Example

The following example adds a local user, whose user name is someone and password is someone, and uses a plaintext password:
username someone password someother

The following example adds a local user, whose user name is someone and password is someone, and uses MD5 encryption:
username someone password 4 someother.

Relevant command

aaaauthenticationlogin aaa

authenticationppp

1.1.2. local user maxlinks

Configure the default maximum number of connections for local users

local user maxlinks*number*
no local usermaxlinks

Parameter

Parameter	Description
number	The default maximum number of simultaneous connections

Default

No maximum connections limit

Command mode

Global configuration status or local user group configuration status

Explanation

When the command is configured in the global configuration state, it is applied to users in the global configuration state; When configured in the local user group configuration state, it is applied to users in the group.
When the user authentication passes, a valid link is calculated, and no other authentication requests will be accepted after the maximum number of connections is reached. Unless the maximum number of connections is specified in the username command, the one configured in this command shall prevail.

Example

The following example sets the local default maximum number of connections to 10.

local user maxlinks 10.

Relevant command

Username

Localgroup

local pass-group

local authen-group

local author-group

1.1.3. local user freeze

Manually freeze local users

local user freeze *username*
no local user freeze *username*

Parameter

Parameter	Description
username	Local user name manually frozen established by local users

Default

Do not freeze any users

Command mode

Global configuration status or local user group configuration status

Explanation

When the command is configured in the global configuration state, it is applied to users in the global configuration state; When configured in the local user group configuration state, it is applied to users in the group.
When a user is manually frozen, AAA requests are not accepted. Only after the user is manually unfrozen can AAA requests be accepted.

Example

The following example sets to freeze the local user guest.

local user freeze guest.

Relevant command

Username

localgroup

local pass-group

local authen-group

local author-group

1.1.4. local pass-group

Configure the default password policy group for local users

local pass-group *WORD*
no local pass-group

Parameter

Parameter	Description
WORD	Default password policy group name for local users

Default

The user does not have a default password policy group

Command mode

Global configuration status or local user group configuration status

Explanation

When the command is configured in the global configuration state, it is applied to users in the global configuration state; When configured in the local user group configuration state, it is applied to users in the group.
After configuring this command, if the user does not specify the password policy group in the username command, the password policy group specified in this command will be used.

Example

The following example sets the default password policy group of local users to A.

local pass-group A.

Relevant command

Username

localgroup

local user

local authen-group

local author-group

1.1.5. local authen-group

Configure the default authentication policy group for local users

local authen-group *WORD*
no local authen-group

Parameter

Parameter	Description
WORD	The default authentication policy group name of the local user

Default

User has no default authentication policy group

Command mode

Global configuration status or local user group configuration status

Explanation

When the command is configured in the global configuration state, it is applied to users in the global configuration state; When configured in the local user group configuration state, it is applied to users in the group.
After configuring this command, if the user does not specifically specify the authentication policy group in the username command, the authentication policy group specified in this command will be used.

Example

The following example sets the local user's default authentication policy group to B.

local authen-group B.

Relevant command

Username
localgroup
local user
local pass-group
local author-group

1.1.6. local author-group

Configure the default authorization policy group for local users

local author-group *WORD*
no local author-group

Parameter

Parameter	Description
WORD	The default authorization policy group name of the local user

Default

User has no default authorization policy group

Command mode

Global configuration status or local user group configuration status

Explanation

When the command is configured in the global configuration state, it is applied to users in the global configuration state; When configured in the local user group configuration state, it is applied to users in the group.
After configuring this command, if the user does not specifically specify the authorization policy group in the username command, the authorization policy group specified in this command will be used.

Example

The following example sets the local user's default authorization policy group to C.

local author-group C.

Relevant command

Username
localgroup
local user
local pass-group
local authen-group

1.1.7. Localgroup

Local User Group Command

localgroup*WORD*

no localgroup*WORD*

Parameter

Parameter	Description
WORD	Local user group name

Default

No local user group

Command mode

Global configuration status

Explanation

Local user groups are used to group and manage local users, and specific management policies can be used within the group.
All local user groups and global user names cannot have the same name.

Example

The following example adds a local user group team, adds two user names user1 and user2 in the group, and freezes user user2.

```
localgroup team
 username user1 password 123
 username user2 password abc
 local user freeze user2
```

Relevant command

username
local user
local authen-group
local author-group
local pass-group

1.1.8. show aaausers

To display thesummary information about all onlineAAAusers, run**showaaausers**.

showaaausers

Parameter

None

Default

None

Command mode

EXEC

Explanation

After thiscommand isrun, thefollowing informationabout onlineusers canbe displayed: port, username, service, online time and peer address.

Example

#showaaa users

Port	User	Service	Duration	Peer-address
console 0	zjl	exec	04:14:03	unknown
vty0	aaa	exec	00:12:24	172.16.20.120
virtual-tunnel 1	admin	ppp(chap)	01:43:09	192.168.20.87

Domain	Explanation
Port	ID of the interfacewhere user lies, or indexnumber of VTY
User	Character stringof username
Service	Serviceappliedbytheuser
Duration	Online durationtime of the user
Peer-address	IPaddress of the remote host where the user lies

Related command

username

1.1.9. show local-users

To display the profile information of all local users, use the show local-users command

show local-users

Parameter

None

Default

None

Command mode

EXEC

Explanation

Use this command to display all online users, including the following information: user name (username), number of current connections (links), password age (pw_present), number of login attempts (login_tries), login attempt time (login_try_time), and user freeze reason (freezing_cause).

Example

```
#show local-users
Local group default:
username        links   pw_presentlogin_trieslogin_try_timefreezing_cause
a               120d3h5m30s 1           0s
b035d         0    0s          command
```

Field	Explain
username	Local user name.
links	Current connections.
pw_present	Password age
login_tries	Number of login attempts.
login_try_time	Login attempt time.
freezing_cause	Reason for user freezing.

Related commands

username

1.2. Password command

This chapter describes password management commands

1.2.1. service password-encryption

Toencryptrelatedpasswordsinthesystem,runservicepassword-encryption.
service password-encryption

noservicepassword-encryption

Parameter

None

Default

Relatedpasswords in the systemisnotencryptedwhen they are displayed.

Command mode

Globalconfigurationmode

Explanation

Thiscommandisrelatedwiththreecommands,**usernamepassword**,**enable password**and**password**.Ifthiscommandisnotconfiguredandthepreviousthree commandsadoptthepasswordplain-textdisplaymode,theconfiguredpassword's plaintextcanbedisplayedafterthe**showrunning-config**commandisrun.Ifthis commandisconfigured,thepasswordsconfiguredforthepreviousthreecommands willbeencryptedandtheconfiguredpassword'splaintextcannotbedisplayedafter the**showrunning-config**command is run; in this case, thepassword plain-text displaycannotberesumedevenifyourun**noservicepassword-encryption**.The**no servicepassword-encryption**commandiseffectiveonlytothepasswordwhichis configuredbythiscommand,whileisnoteffectivetothosepasswordswhichare encryptedbefore this commandis used.

Example

router_config#servicepassword-encryption

Thiscommandisusedtoencrypttheconfiguredplain-textpasswordandalsothe plain-textpassword after this command is used.

Related command

None

1.2.2. Localpass

Local PasswordPolicyGroupCommand

localpass*WORD*

no localpass*WORD*

Parameter

Parameter	Parameter Description
WORD	Local password policy group name.

Default

No local password policy group.

Command mode

Globalconfigurationmode

Explanation

The local password policy group is used to configure password configuration and management policies. It can specify the composition, effective time, minimum length, etc. of the password.
Any password that adopts a password policy group and does not meet the group policy is considered invalid. The user is frozen and will not pass the authentication. The user will be prompted to update the password when logging in.

Example

The following example adds a local password policy group A. The configuration password must contain uppercase and lowercase letters and numbers. The minimum length is 10 and the validity period is 30 days.

```
localpass A
  Elementnumberlower-letterupper-letter
  min-length10
  Validity20d
```

Related command

Element

min-length

validity

1.2.3. Element

Configuration password composition must contain elements

element [number] [lower-letter] [upper-letter] [special-character]

no element

Parameter

Parameter	Parameter Description

number	Password must contain numbers.
lower-letter	Password must contain lowercase letters
upper-letter	Password must contain uppercase letters
Special-character	Password must contain special characters

Default

The password can be in any form, including blank password.

Command mode

Password policy group configuration status

Explanation

After configuring the command, the password complexity must be greater than the command configuration requirements, otherwise it will be considered as invalid password.

Example

In the following example, in the local password policy group A, the configuration password composition must contain lowercase letters and numbers.

```
localpass A
  Elementnumberlower-letter
```

Related command

localpass

min-length

validity

1.2.4. min-length

Configure minimum password length

min-length *number*

no min-length

Parameter

Parameter	Parameter Description
number	Minimum password length value.

Default

The password can be in any form, including blank password.

Command mode

Password policy group configuration status

Explanation

After configuring the command, the password length must be greater than or equal to the command configuration requirements, otherwise it will be considered as invalid password.

Example

In the following example, in the local password policy group A, the minimum length of the configuration password is 5.

```
localpass A
  min-length 5
```

Related command

localpass

element

validity

1.2.5. validity

Configure password validity

validity *1d2h3m4s*

no validity

Parameter

Parameter	Parameter Description
number	Password validity period.

Default

The password can be in any form, including blank password.

Command mode

Password policy group configuration status

Explanation

After configuring this command, the password will be counted from the time of configuration, and will be considered invalid after the expiration date.

Example

In the following example, in the local password policy group A, the configured password validity period is 2 days, 10 hours, 5 minutes and 6 seconds.

```
localpass A
  validity 2d10h5m6s
```

Related command

localpass

min-length

validity

1.3. Authentication Commands

ThisChapterdescribesthecommandsusedforconfiguringtheAAAauthentication method.Authenticationdefinestheaccessrightoftheusersbefore theyareallowedto access the network and networkservices.

Pleasereferto“ConfigurationAuthentication”forinformationonhowtousetheAAA methodtoconfiguretheauthentication.Pleaserefertothelastparttoreviewthe examples configured by the commandsin this Chapter.

1.3.1. aaaauthentication enable default

AAAauthentication shall be enabled soas to determinewhetherauserhastheaccess tothecommandofprivilegedprioritybyusingthecommand “aaaauthentication enabledefault”.Theauthenticationmethodcanbeclosedbyusingthe“no”formatof thesaidcommand.

Syntas

aaaauthenticationenabledefault *method1*[*method2...*]

noaaaauthenticationenabledefault*method1*[*method2...*]

Parameter

Parameter	Parameter Description
method	At least one of the keywords given in Table 1

Default

If the default is not set, the authentication failure result will be returned except that the console can log in successfully.

If the default table is set, if the enable password of the corresponding privilege level does not exist, the authentication process that enters the privilege level will always fail..

Command mode

globalconfigurationmode

Explanation

Thecommand“aaaauthenticationenabledefault”canbeusedtocreateaseriesof authenticationmethods,whichareusedtodeterminewhetherauserhastherightto usetheprivilegedcommands.Thekeyword“method”hasbeenexplainedinform1. Onlywhenthepreviousauthenticationmethodfeedsbackerror,otherauthentication methodsshallbeapplied.Ifthefeedbackresultofthesaidauthenticationmethod informsthefailureoftheauthentication,otherauthenticationmethodshallbe employed.Ifalltheauthenticationmethodisexpectedtofeedbacktheresultoffailure andtheauthenticationstillsucceeds,“none”canbedesignatedasthelast authentication method of command line.

OntopofthatwhenthemethodofRADIUSorTACACS+isavailableformaking authenticationofenable,theusernamesappliedaredifferent.Theusernameshallbe “$ENABLE*level*$”incase“RADIUS”isusedforauthentication.The“level”intheuser namereferstotheprivilegedlevelaccessibletotheuser.WhenTACACS+isusedfor

authentication,theusernameistheoneusedwhentheuserlogontherouter.The relevantspecificconfigurationcanbereferredtoasthepartof“AAAAuthentication Configuration” in the document.

Figuer 1-1 Effective Default Method of AAA Authentication

Keyword	Description
groupWORD	The server group is used for authentication
enable	Theenablepasswordisusedforauthentication.
line	Thepassword line is used forauthentication
none	Authenticatingthepassageofnonecondition
Grouptacacs+	TACACS+ is used for authentication
Groupradius	RADIUS is usedfor authentication.

Example

Anauthenticationlistiscreatedinthefollowingexample.Thelistfirsttriestoconnect withTACACS+server.Ifnoerrorisfedback byTACACS+server or noserver isfound, AAAwilltryusingtheenablepassword.Shouldtheerrorbefedbacktosuchtrial(as noeffectivepasswordisconfiguredontheserver),theuserwillbeallowedtoaccess theserverwithoutauthentication.

aaa authentication enable default group tacacs+ enablenone

Related command

enablepassword

1.3.2. aaaauthentication login

Theglobalconfigurationcommand“aaaauthenticationlogin”shallbeusedforsetting AAA authenticationatthetimeoflogin.The“no”formatofthecommandcanbeused to closeAAAauthentication.

Syntas

aaaauthenticationlogin{**default**|*list-name*}*method1*[*method2...*]

noaaaauthenticationlogin{**default**|*list-name*}

Parameter

Parameter	Description
Default	Itusesthelistedauthenticationmethodfollowingtheparameterasthe default authentication method list atthe time of the user’s login.
list-name	Itisusedtonamethecharacterstringofauthenticationmethodlist.When theuserlogsin,themethodslistedinauthenticationmethodlistwillbe activated.
method	It is one of thekey words described in the Form2 at the least.

Default

Ifnodefaultmethodlistisset,thedefaultwillnotmakeauthentication.Atthismoment, it has the same effect asthe onebelow:

aaa authentication login default group tacacs+ enable none

Command mode

globalconfigurationmode

Explanation

Thedefaultlistorothernaminglistcreatedbythecommand“aaaauthenticationlogin” willactonsomespecific lineusingthecommand“loginauthentication”.

Onlywhenthesaidauthenticationmethodfeedsbackerror,otherauthentication methodswillbeused.Shouldthesaidauthenticationmethodfeedbackthefailure,no otherauthenticationmethodswillbeused.Toensurethesuccessofauthentication evenifallauthenticationmethodsfeedbackerror,“none”shallbedesignatedasthe last method of thecommand line.

Ifnoauthenticationisspeciallysetforaline,noauthenticationwillbeexecutedatthe time of default.

FiguerTheRegistration Method of AAA Authentication

KeyWord	Description
enable	The enablepassword is used for authentication
groupWORD	The server group is used for authentication
line	Thepassword line is used forauthentication
local	The database of local user names is used for authentication.
local-case	The databaseof localuser namesis usedfor authentication(case sensitiveforusername)
none	No authentication is made.
group radius	RADIUS is usedfor authentication
group tacacs+	TACACS+ is used for authentication.

Example

AAAauthenticationmethodslistnamed“TEST”iscreatedinthefollowingexample. ThisauthenticationfirsttriestoconnectwithTACACS+server.Ifnoerrorisfedback byTACACS+ornoserverisfound,AAAwilltryusingtheenablepassword.Should errorbefedbacktosuchattempt(asnoenablepasswordisconfiguredontherouter), theuser willbeallowedtoaccess the networkwithoutauthentication.

aaa authentication loginTESTgroup tacacs+ enable none

The same listis created in the Example below, but the default list is set. If no other lists are designated,thelistwillbeused forallthe loginauthentication.

aaa authentication login default group tacacs+ enable none

Relevant command

username
enable password

1.3.3. aaaauthentication ppp

Theglobalconfigurationcommand“aaaauthenticationppp”canbeusedfor designatingoneormultipleAAAauthenticationmethodsusedforrunningserial interface of PPP.The “no” format of the command isused for closing authentication.

Syntas

aaaauthenticationppp{**default**|*list-name*}*method1*[*method2...*]

noaaaauthenticationppp{**default**|*list-name*}*method1* [*method2...*]

Parameter

Parameter	Description
Default	It usesthe authenticationmethod listfollowing theparameter asthe default authentication methodatthe time of the user’s login.
list-name	It is used to name the character string of authentication method list.
mehod1 [*method2...*]	It is one of the methods described in Form3at the least.

Default

Ifnodefaultisset,thedatabaseoflocalusersshallbeexaminedforauthentication.It hasthesameeffectasthecommandbelow:

aaa authentication ppp default local

Command mode

globalconfigurationmode

Explanation

Thedefaultlistandnaminglistcreatedbythecommand“aaaauthenticationppp”are usedinthecommand“pppauthentication”.Theselistscontainfourauthentication methodsatmost.Theseauthenticationmethodsareusedwhentheuserconnectsthe serialinterface.

Thelistiscreatedbythecommand“aaaauthenticationppplist-namemethod”,of whichthekeyword“list-name”isusedfornaminganycharacterstringofthelist.The parameter“method”designatesthespecificauthenticationmethods.Thesemethods are

used in the authentication process on the sequence ofconfiguration. Fourmethods canbe entered at most.The keywordsofthe methodsis described in Form 3.

Onlywhenthesaidauthenticationmethodfeedsbackerrorwillotherauthentication methodsbeused.Shouldthesaidauthenticationmethodfeedbackthefailure,no otherauthenticationmethodswillbeused.“none”shallbedesignatedasthelast methodofthecommandlinetoensurethesuccessofauthenticationevenifallthe authenticationmethodsfeedbackerror.

Figuer1-3PPPMethodofAAAAuthentication

KeyWord	Description
groupWORD	The server group is used for authentication.
local	The database of local user names is used for authentication.
local-case	The databaseof localuser namesis usedfor authentication(case sensitiveforusername)
none	No authentication is made.
groupradius	RADIUS is usedfor authentication
grouptacacs+	TACACS+ is used for authentication.

Example

AAAauthenticationmethodslistnamed“TEST”iscreatedinthefollowingexamplefor usingtheseriallineofPPP.Thisauthenticationfirsttriesconnectingwith TACACS+server.Iferrorisfedback,theuserwillbeallowedtoaccessthenetwork without authentication.

aaa authentication pppTESTgroup tacacs+ none

Relevant command

pppauthentication

1.3.4. aaaauthentication password-prompt

Theglobalconfigurationcommand“aaaauthenticationpassword-prompt”shouldbe usedforchangingthetextdisplaypromptingtheuserpasswordinput.The“no”format ofthecommandcanbeemployedforreusingthedefault prompt text of thepassword.

Syntas

aaaauthenticationpassword-prompt*text-string*

noaaaauthenticationpassword-prompt

Parameter

Parameter	Description

test-string	Itisusedtoprompttheuserofthetextdisplayedatthetimeofpassword input.

Default

When the user-defined text-string is notused, thepassword promptis “Password”.

Command mode

globalconfigurationmode

Explanation

Thedisplayeddefaultliteralinformationpromptingtheuserpasswordinputcanbe changedbyusingthecommand“aaaauthenticationpassword-prompt”.Thecommand notonlychangesthepasswordpromptoftheenablepassword,italsochangesthe passwordpromptofloginpassword.The“no”formatofthecommandrestoresthe passwordprompt to default value.

Password:

Thecommand“aaaauthenticationpassword-prompt”doesnotchangeanyprompting information provided by remoteTACACS+orRADIUSserver.

Example

ThefollowingExamplewillchangethepassword prompt to “YourPassword:”

aaa authentication password-promptYourPassword:

Relevant command

aaaauthenticationusername-prompt

1.3.5. aaaauthentication username-prompt

Theglobalconfigurationcommand “aaaauthenticationusername-prompt”canbeused forchangingthetextdisplaypromptingtheusernameinput.The“no”formatofthe commandis usedforrestoringthedefaultpromptingcharacter string of theusername.

Syntas

aaaauthenticationusername-prompt*text-string*

noaaaauthenticationusername-prompt.

Parameter

Parameter	Description
text-string	Itisusedtoprompttheuserofthetexttobedisplayedatthetimeofthe user name input.

Default

Whenthereisnouser-definedtext-string,thepromptingcharacterstringoftheuser nameis “Username”.

Command mode

globalconfigurationmode

Explanation

Thecommand“aaaauthenticationusername-prompt”isusedforchangingthe displayedcharacterstringpromptingtheusernameinput.The“no”formatofthe commandchangesthe promptofusernameintodefaultvalue.

Username:

Someprotocols(suchasTACACS+)havethecapabilitytocovertheprompting informationoflocalusername.Undersuchcircumstances,theuseofthecommand “aaaauthenticationusername-prompt”willnotchangethepromptingcharacterstring ofusername.

Note:The command “aaa authentication username-prompt” doesnot change any promptinginformationprovidedbyremoteTACACS+server.

Example

ThefollowingExamplewillchangethepromptofusernameintothedisplayed characterstring.

aaa authentication username-promptYourUsernam:

Relevant command

aaa authenticationpassword-prompt

1.3.6. aaaauthentication banner

Toconfigureapersonalbanner,run**aaaauthenticationbanner**inglobalmode.To deletea personal banner, run **noaaaauthenticationbanner**.

aaaauthenticationbanner*delimiterstringdelimiter*

no aaa authentication banner

Parameter

Parameter	Description
delimiter stringdelimiter	To-be-displayed text**string**when the user logs in The**delimiter**parameterstandsforthedelimterwhichadopts doublequotationmasks.

Default

Ifyoudonotdefinetheloginbanner,thesystemwilldisplaythefollowingdefault banner:

UserAccessVerification

Command mode

Globalconfigurationmode

Explanation

Whencreatingabanner,youneedtoconfigureadelimiterandthentoconfigurethe textstringitself.Thedelimiteristonotifythatthefollowingtextstringwillbedisplayed asthebanner.Thedelimiterappearsreaptedlyattheendofthestring,meaningthe bannerends.

Example

Thefollowingexampleshowsthatthebannerismodifiedto“WelcomtoRouter”when logging on:

aaa authentication banner "Welcome to Router"

Related command

aaaauthentication fail-message

1.3.7. aaaauthentication fail-message

Toconfigureapersonalbannerwhenloginfails,run**aaaauthenticationfail-message** in globalmode.

aaaauthenticationfail-message*delimiter string delimiter*

no aaa authentication fail-message

Parameter

Parameter	Description
delimiter string delimiter	Textstringthat willbedisplayedwhenuserfailstologin Thedelimiteradoptsdoublequotationmarks.

Default

Ifyoudonot definethebannerforloginfailure,thedefaultbanneris: Authentication

failed!

Command mode

Globalconfigurationmode

Explanation

Whencreatingabanner,youneedtoconfigureadelimiterandthentoconfigurethe text string. The delimiter is to notify that the following textstringwillbe displayedas the banner.Thedelimiterappearsreaptedlyattheendofthestring,meaningthebanner ends.

Example

Thefollowingexampleshowsthatusernamepromptischangedtothefollowing characterstring:

aaa authentication fail-message "Seeyou later"

Related command

aaaauthenticationbanner

1.3.8. aaagroup server

Thecommandsbelowareusedtoaccesstotheconfigurationlevelofservergroupfor supportingtheconfigurationofAAAservergroup.The“no”formatofthecommandis usedtodeletetheconfiguredserver group.

Syntas

aaa group server {radius | tacacs+} group-name
no aaa group server {**radius** |**tacacs+**} *group-name*

Parameter

Parameter	Description
group-name	Character stringof the name of the server group.

Default

noserverGroup

Command mode

globalconfigurationmode

Explanation

Accessingtoconfigurationlevelofservergroupbyusingthecommand,thenadding thecorrespondingsevertothegroup.

Example

aaagroup server radius radius-group

Thesaidcommandis usedforaddingaradiusservergroupnamed““radius-group”.

Relevant command

server

1.3.9. server

ThecommandisusedforaddingaserverinanAAA servergroup.The“no”formatof thecommandisusedfor deletingaserver.

Syntas

server ADDR*A.B.C.D*

noserver ADDR

Parameter

Parameter	Description
ADDR	IIP address of the server (v4 or v6).
WORD	The key value required by the server.

Default

noserver

Command mode

Server GroupConfigurationMode

Explanation

20 different servers can beadded toa servergroupat most.

Example

server 12.1.1.1 KEY 1

The above command is used for adding the server whoseaddressis 12.1.1.1 toserver group.

Relevant command

aaagroupserver

1.3.10. Enable

Enter the management status or change the current permission level.

enable [*number***]**

Parameter

Parameter	Description
number	Specify permission level

Default

Adopt the authorization level of the current user

Command mode

Management status or global configuration status

Explanation

If the specified permission level is higher than the user authorization level, you need to enter the high-level enable password to enter after authentication; Otherwise, enter the specified permission level. If no permission level is specified, the default is user authorization level.

Example

In the following example, if the current permission level is 10 and the user authorization level is 15, you can enter the 15 permission level

Router#enable.

Router#<190>Sep 22 12:56:04 Router - 036EE9D0 [Core 0]: User admin enter privilege mode from console 0, level = 15

Relevant command

enable password

enter

1.3.11. enable password

Toconfiguretheprivilege-levelpasswordtoauthenticatetheprivilegeduser,run **enablepassword**.Tocanceltheprivilege-levelpassword,run**enablepassword** **[*level number*]**.

enable password{ ***password***| [**encryption-type**] ***encrypted-password*** }[***level*** *number*]

no enablepassword [***level****number*]

Parameter

Parameter	Description
password	Plain text of the password character string
encryption-type	Typeofpasswordencryption
encrypted-password and**encryption-type**	Cipher textof thepassword whichcorresponds to the limited encryptiontype
level	Privilegelevel
number	Valueoftheprivilegelevel(1-15)

Default

There is nopassword by default.

Command mode

Globalconfigurationmode

Explanation

The password configured by our router cannot contain spaces, that is, when using the enable password command, if you need to enter the password plaintext directly, you cannot enter spaces. The length of password clear text cannot exceed 126 characters.

When the level parameter is not entered, the default is level 15. The higher the privilege level, the greater the privilege. If no password is configured for a privilege level, authentication failure will be returned when the user enters this level.

At present, the encryption-type supported in our router system includes MD5 encryption and a self-defined encryption algorithm of our company, which correspond to different encryption-type parameter values. The meaning of each parameter value of encryption-type is as follows:

0, no encryption, clear text password will be entered, and clear text will be displayed when show running (equivalent to not using the encryption-type parameter);

4. If MD5 encryption is used, the clear text password will be entered, and the MD5 encrypted password will be displayed when show running;.

Example

The following example adds the password of privilege level 10 to clever, and the encryption type is 0, that is, the password is clear text:

enable password 0 clever level 10

The encryption type used is 4, that is, the encryption method, and the password plaintext needs to be entered:

enable password 4 user.

Related command

aaaauthenticationenabledefault enable
servicepassword-encryption

1.3.12. Localauthen

Local authentication policy group command.

localauthen*WORD*

no localauthen*WORD*

Parameter

Parameter	Description
WORD	Local authentication policy group name

Default

No local authentication policy group.

Command mode

Globalconfigurationmode

Explanation

The local authentication policy group is used to configure the authentication restrictions, such as the maximum number of attempts and the maximum time of attempts.

If the user adopts the authentication policy group, the user who exceeds the limit of the authentication policy group during authentication will be frozen, and the restriction will be unfrozen after the expiration of the validity period.

Example

The following example adds a local authentication policy group B, and configures the maximum number of failed authentication attempts within 1 day to 5.

localauthen B

Loginmax-tries5try-duration1d.

Related command

login max-tries

1.3.13. login max-tries

Configure the maximum number of failed login attempts.

login max-tries *number* **try-duration** *1d2h3m4s*

no login max-tries

Parameter

Parameter	Description
number	Maximum number of failed login attempts
try-duration	Limit the maximum number of failed login attempts within the specified time
1d2h3m4s	Specify time duration

Default

No attempt limit.

Command mode

Authentication policy group configuration status

Explanation

After configuring this command, if the maximum number of failed login attempts is exceeded within the specified time, the user will be frozen, and the user can continue to try after the specified time.

Example

In the following example, in the local authentication policy group B, the maximum number of failed authentication attempts within 12 hours is configured to be 3.

localauthen B

Loginmax-tries3try-duration12h.

Related command

localauthen

1.3.14. debugaaaauthentication

Totracktheuserauthenticationprocess,run**debugaaaauthentication**.Toclosethe debuginformation,run**nodebugaaaauthentication**.

debug aaaauthentication

nodebug aaaauthentication

Parameter

None

Default

The debug information is shut down.

Command mode

EXEC

Explanation

Thiscommandcanbeusedtotracktheauthenticationprocessofeachusertodetect thecauseoftheauthenticationfailure.

Related command

debug aaaauthorization

debug aaa accounting

1.4. AAAAuthorizationConfigurationcommand

Thischapterdescribesthecommandsforauthentication,authorizationandaccounting. AAAauthorizationcanlimittheeffectiveservicetoauser.Whentheauthorization resultiseffective,networkaccessserverconfiguresthedialogueprocessoftheuser by using theauthorizationinformation fed back fromauthorization server.

1.4.1. aaaauthorization

Theglobalconfigurationcommand“aaaauthorization”isusedforsettingthe parametertolimittheauthorityoftheuser’saccesstonetwork.The“no”formatofthe commandcanbeusedforclosingtheauthorizationofsomefunction.

Syntas

aaaauthorization network{**default** |*list-name*} [*method1 [method2...*]

no aaa authorization network

Parameter

Parameter	Description
network	Theauthorizationofnetworktypeservice
default	Default authorization methods list
list-name	The character string used for naming authentication methods list.
method1 [method2...]	One of the keywords listed in the form below.
exec	It is applicable to the attributes related to the user's EXEC terminal dialog, which determines whether the user is allowed to start the EXEC shell when registering, or grant the user the privilege level when entering the EXEC shell.

Default

Whentheuserrequestsforauthorizationandtheauthorizationmethodslistrequired foruseisnotdesignatedonthecorrespondinglineortheinterface,thedefault authorizationmethodslistwillbeused.Ifdefaultmethodslistisdefined,no authorizationwilltake place.

Command mode

globalconfigurationmode

Explanation

Thecommand“aaaauthorization”isusedforopeningtheauthorization,creating authorizationmethodslistanddefiningtheauthorizationmethodthatcanbeused whentheuseraccessestothedesignatedfunctions.Theauthorizationmethodslist definesthemethodforauthorizationimplementationandsequenceforexecutingthese authorizationmethods.Themethodslistisonlyasimplenaminglistdescribingthe authorizationmethodforinquiryonthesequence(suchasRADIUSandTACACS+). The methodslist candesignate oneor multiplesecurity protocolsused for

authorization.Soitisabletoguaranteeabackupmethodincasealltheabovelisted authorizationmethodsfail.Undergeneralcondition,thelistedfirstmethodisusedat firstinanattempttoauthorizetheusertheauthoritytoaccesstothedesignated networkservice.Ifthemethoddoesnotwork,thenextmethodinthelistshallbe selected.Theprocessshallbecontinuedtillthesuccessfulfeedbackofauthorization resultsbyusingsomeauthorizationmethodor allthedefinedmethodsareusedup.

Oncetheauthorizationmethodslistisdefined,themethodslistshallbeusedonthe designatedlineorinterfacebeforethedefinedmethodisexecuted.Asapartofthe authorization process, theauthorization commandsendsaseriesofrequestpacketsof AVpairsto theprogramofRADIUSorTACACS＋server.Theserverislikelyto execute oneofthefollowingactions:

- Therequestisacceptedcompletely
- Therequestisacceptedandtheattributeisaddedtolimittheauthorityofuser service
- Requestisrefusedandauthorizationfails

Example

ThefollowingExampledefinesthenetworkauthorizationmethodslistnamed“havea try”.ThemethodslistdesignatesRADIUSauthorizationmethodusedontheserialline employingPPP.IfRADIUSservermakesnoresponse,thelocalnetworkauthorization is executed.

```
aaa authorization network have_a_try groupradiuslocal
```

Relevant command

aaaauthentication
aaa accounting
priviledge

1.4.2. localauthor

Local Authorization Policy Group Command.

localauthor*WORD*

no localauthor*WORD*

Parameter

Parameter	Description
WORD	Local authorization policy group name

Default

No local authorization policy group.

Command mode

Global configuration status

Explanation

The local authentication policy group is used to configure the authentication restrictions, such as the maximum number of attempts and the maximum time of attempts.

If the user adopts the authentication policy group, the user who exceeds the limit of the authentication policy group will be frozen,
The restrictions will be unfrozen after the expiration of the validity period

Example

The following example adds a local authentication policy group C, and configures the authorization level of telnet login method to be 15, and the authorization level of ssh login method to be 12.

```
localauthor C
  exec privilege telnet 15
  exec privilege ssh 12
```

Relevant command

exec privilege

1.4.3. exec privilege

Configuration password composition must contain elements.

exec privilege {default | aux | console | ssh | telnet | rtelnet} *number*

no exec privilege {default | aux | console | ssh | telnet | rtelnet}

Parameter

Parameter	Description
default	Default exec authorization level

aux	Authorization level of login through aux port
console	Authorization level of login through console
ssh	Authorization level of login through ssh
telnet	Authorized sectors logged in via telnet
rtelnet	Authorized sectors logged in through reverse telnet
number	Number of authorization levels

Default

No authorization level assignment.

Command mode

Authorization policy group configuration status

Explanation

After configuring this command, logging in with the specified method will use the corresponding authorization level to the user. If there is no corresponding configuration, the default is used. If there is no configuration, the default is 15

Example

The following example configures the telnet login mode authorization level to 14 in the local authorization policy group C.

```
localauthor C
  exec privilege telnet 14
```

Relevant command

localauthor

1.5. Accounting Command

Thissectiondescribes thecommandsforconfiguringAAAauthenticationmethods.The accountingfunctioncantracktheservicesthatusersaccess,andatthesametime tracktheservice-consumednetworkresourcenumber.WhenAAAaccountingis activated,therouterwillreportuser'sactivitiestotheTACACS+serverortheRADIUS serverintheaccountingrecordmethod.Eachaccountingrecordcontainstheattribute valuepeerwhichisstoredontheaccesscontrolserver.Thedataisthenappliedto network management, client'saccounting analysis or audit.

1.5.1. aaaaccounting

ToexecuteAAAaccountingontorequiredservicesonthebasisofaccountingor security,run**aaaaccounting**inglobalmode.Youcanrun**noaaaaccounting**to disable theaccounting function.

aaaaccounting{ network | exec | connection | commands level | ipoe } {default | list-name} {start-stop | stop-only | none} method1 [method2...]

no aaaaccounting{ **network** | exec |connection} {default | *list-name*}

Parameter

Parameter	Description
network	Providesaccountinginformationtoall PPPsessions,includingpackets, bytes and time numbering.
exec	ProvidesinformationaboutEXECterminalsession(itisnotsupported currently).
connection	Providesinformationaboutallegressconnectionsfromrelatedrouter. Currently,onlytheH323sessionissupported.
default	Default accounting method list
list-name	Character stringwhich is usedto name the accounting method list
level	When recording the command execution, specify the command level (1~15)
method1 [method2...]	Accountingmethod For more details, refer to*AccountingConfiguration*.
commands	Record the execution of the command.
ipoe	Provide accounting record information for all IPOE sessions.

Default

Iftheuserrequiresaccountingbuthedoesnotdesignatetheaccountingmethodlist onthecorrespondingpathorinterface,thedefaultaccountingmethodlistwillbe applied. If the default method list is notdefined, the accounting willnot be executed.

Command mode

Globalconfigurationmode

Explanation

Use the aaa accounting command to open accounting, create a list of accounting methods, and define the accounting methods that can be used when users send accounting records. The accounting method list defines how accounting is executed and the order in which these accounting methods are executed. The method list is just a simple named list, which describes the accounting method (RADIUS or TACACS+) to be queried in sequence. The method list can specify one or more security protocols used for accounting. Therefore, it can ensure that there is an alternate method in case the accounting methods listed above fail.

Table 4: Effective default methods for AAA bookkeeping.

keyword	describe
group*WORD*	Use a named server group for billing.
grouptacacs+	Use TACACS+for bookkeeping.
group radius	Use RADIUS for bookkeeping.

Related command

aaaauthentication

aaa accounting

1.5.2. aaaaccounting update

Toperiodicallytransmittemporaryaccountingrecordstotheaccountingserver,run **aaaaccountingupdate**.Youcanrun**noaaaaccountingupdate**todisable temporaryaccounting records.

aaaaccountingupdate{**newinfo**|**periodic***number*}

no aaa accounting update

Parameter

Parameter	Description
update	Activates the router to transmit temporaryaccounting records.
newinfo	Transmitstemporaryaccountingrecordstotheaccountingserverwhen newaccountinginformation need be reported.
periodic	Periodicallytransmitstemporaryaccountingrecords.Theperiodisdefined bythe**number**parameter.
number	A parameterto definethe periodfor temporaryaccounting record transmission

Default

Temporaryaccountingactivity does notoccur.

Command mode

Globalconfigurationmode

Explanation

See*AccountingConfiguration*.

Related command

aaaaccounting

1.5.3. aaaaccounting suppress null-username

Tostopgeneratingaccountingrecordsforthosenon-usersessions,runaaa accountingsuppressnull-usernameinglobalmode.Youcanrunnoaaa accountingsuppressnull-usernameto resume thedefault configuration.

aaaaccountingsuppressnull-username

noaaaaccountingsuppressnull-username

Parameter

None

Default

Theaccountingrecordswillbegeneratedforallsessions,nomatterthesessionshave username or not.

Command mode

Globalconfigurationmode

Explanation

See*AccountingConfiguration*.

Related command

aaaaccounting

2. RADIUSCommands

2.1. RADIUS Configuration Commands

ThischapterintroducesthecommandsforRADIUSconfiguration.RADIUSisa distributedclient/serversystemcapableofdenyingtheunauthorizednetworkaccess. RADIUSclientisrunning ontherouterandsendstherequestofauthentication, authorizationandaccountingtothecentralRADIUSservercontainingthe authentication of all the user and the informationofnetworkserviceaccess.

2.1.1. debug radius

Thecommand“debugradius”canbeexecutedfortracingRADIUSeventorpacket. The“no”formatofthecommandcanbeusedforclosingdebuginformation.

Syntas

debugradius｛event|packet｝

no debug radius｛event|packet｝

Parameter

Parameter	Description
event	TracingRADIUSevent
packet	Tracing RADIUSpacket

Default

none

Command mode

Supervisormode

Explanation

Thecommandcanbeusedfordebuggingnetworksystemtofindoutthecauseof authentication failure.

Router#debugradiusevent

RADIUS:return message toaaa, Give me yourusername

RADIUS:return message toaaa, Give me yourpassword

RADIUS:initaltransmitaccess-request [4] to 192.168.20.126 1812<length=70>

RADIUS:retransmitaccess-request[4]to 192.168.20.1261812<length=70>

RADIUS:retransmitaccess-request[4]to 192.168.20.1261812<length=70>

RADIUS:192.168.20.126isdeadtoresponse[4]

RADIUS:Havetriedallservers，returnerrortoaaa.

Output Information	Explanation
Return packetto aaa, Giveme yourusername	The usernamewantd
Return packetto aaa, Giveme yourpassword	Thepassword corresponding tothe usernamewanted.
initaltransmitaccess-request [4] to 192.168.20.126 1812<length=70>	ThefirstauthenticationrequestissenttotheRADIUS server.Theaddress of the server is 192.168.20.126, the port number is1812, the length ofpacket is 70.
retransmit access-request [4] to 192.168.20.1261812<length=70>	Serverdoesnotechotherequestandauthentication request is retransmitted.
192.168.20.126is dead to response [4]	After repeated retransmission, server is dead to response, the server is markedas dead.
Havetriedallservers，returnerrorto aaa	TheauthenticationiscompletedbyusingRADIUSand the error is returned.

Example

The followingExample opens event trace of RADIUS.

debugradius event

2.1.2. ipradius source-interface

Theglobalconfigurationcommand“ipradiussource-interface”isusedforcompelling RADIUStouseIPaddressofthedesignatedinterfaceforallthepacketstransmitted by RADIUS.The “no” format of the commandisusedfor restoring the default value.

Syntas

ipradiussource-interface *interface-name*

no ip radius source-interface

Parameter

Parameter	Description
interface-name	RADIUS usesIP addressof theinterface forall RADIUSpacket sent.

Default

Thecommandhasnodefaultvaluedesignatedbythemanufacturer,i.e.,thesourceIP addressshouldbedeterminedontherealcondition.

Command mode

globalconfigurationmode

Explanation

Thecommandisusedforselectingthe IPaddressofaninterfaceasthesource addressofsendingoutRADIUSpacket.Solongastheinterfaceisunder“up”state, theaddresswillbeusedcontinuously.Thus,foreachclientaccessingthenetwork, RADIUSserveronlyusesoneIPaddressratherthanmaintaininganIPaddresslist. Thecommandisespeciallyusefulwhentherouterhasmanyinterfacesandintendsto ensurethatallRADIUSpacketscomingfromsomespecificrouterhasthesameIP address.

Thedesignatedinterfaceshallhave IPaddressrelatedtotheinterface.Ifthe designatedinterfacedoesnothaveanIPaddressorisundera“down”state,RADIUS will restore tothe default value. In order to avoidthe case, IPaddress should be added totheinterfaceandtheinterfaceshallbeensuredunder“up”state.

Example

ThefollowingExampleallowsRADIUStouseIPaddressoftheinterfaceG0/2forall RADIUSpacketsused.

ipradius source-interfaceG0/2

Relevant command

iptacacssource-interface

2.1.3. radius-server attribute

Todesignatesomeattributestobetransmitteddu ringradiusauthentication and charging,runradius-serverattribute.Tocancelsomedesignatedattributestobe transmitted, runnoradius-serverattribute.

radius-server attribute{4|*32* |95}

no radius-server attribute{4|*32*|95}

Parameter

Parameter	Description
4	Transmitsthefollowingaddressasattribute4(NASipaddress)during radius operation.
32	Transmits attribute32 (NAS identifier) duringradius authenticationor request.
95	Specify to transfer attribute attribute32 (NAS IPv6 address attribute) in radius authentication or request according to the command following this parameter

Default

None

Command mode

Globalconfigurationmode

Explanation

Thiscommandisusedtodesignateaspecificattributetobetransmitteddu ringradius authenticationorradius request.

The**radius-serverattribute4**commandisusedtoconfigureattribute4(NASipaddress)inradius andtransmititintheRADIUSpackets.

The**radius-serverattribute32**commandisusedtodesignateattribute32(NASID) tobetransmittedinRadiusauthenticationorcharging.

Radius-server attribute 95 specifies to transmit radius attribute 95 (NAS IPv6 address) in RADIUS authentication or billing request message.

Example

The**radius-serverattribute4X.X.X.X**commandisusedwhenattribute4needbe transmittedintheRadiuspacketsandattribute4servesastheattributevalueof X.X.X.X.

The**radius-serverattribute32in-access-req**commandisusedwhentheNAS identifierneed be transmitted in the authentication request.

The**radius-serverattribute32in-account-req**commandisusedwhentheNAS identifier needbetransmittedinthechargingrequest.

Relatedcommand

None

2.1.4. radius-server challenge-noecho

Thecommand“radius-serverchallenge-noecho” shallbeusedfor notshowingtheuser dataundertheAccess-ChallengeMode.

Syntas

radius-serverchallenge-noecho

noradius-serverchallenge-noecho

Parameter

none

Default

The user dataisshown undertheAccess-Challenge.

Command mode

globalconfigurationmode

Explanation

none

Example

radius-serverchallenge-noecho

2.1.5. radius-server deadtime

Theglobalconfigurationcommand“radius-serverdead-time”shallbeusedfor improvingtheechotimeofRADIUSwhensomeserversarenotworkable.The commandallowsthesystemtoskiptheunworkableservers.The“no”formatofthe commandcanbeusedforsettingdead-timeas0,namely,alltheserversarethought tobeworkable.

Syntas

radius-serverdeadtime *minutes*

noradius-serverdeadtime

Parameter

Parameter	Description
minutes	The timelength ofRADIUS serverthought to be unworkable, the maximum length is 1440 minutes (24hours)。

Default

Theunworkabletimeissetas0,meaningthattheserveristhoughttobe workable all the time.

Command mode

globalconfigurationmode

Explanation

Thecommandisusedforlabelingthose RADIUSserversthatdonotrespondtothe authenticationrequest as“dead”, which avoidstoo long waitingfor the response beforeusingthenextserver.TheRADIUSserverlabeledas“dead”isskippedbyall therequestsduringthesetminutesunlessotherwisealltheserversarelabeledas “dead”.

Example

ThefollowingExampledesignates5-minutedeadtimefortheRADIUSserverthat doesnotrespondtotherequest.

radius-server deadtime5

Relevant command

radius-serverhost

radius-server retransmit

radius-server timeout

2.1.6. radius-server host

Theglobalconfigurationcommand“radius-serverhost”isusedfordesignatingIP addressofradiusserver.The“no”formatofthecommandisusedfordeletingthe designated RADIUS host.

Syntas

radius-serverhost*ip-address* [**auth-port***port-number1*] [**acct-port***port-number2*]
no radius-server host *ip-address*

Parameter

Parameter	Description
ip-address	*theipaddressof*RADIUSserver
auth-port	*(optional item) DesignatingUDP destination port for authentication*

	request.
port-number1	*(optionalitem)Theportnumberofauthenticationrequest.Ifthesettingis 0, the host is not used for authentication.*
acct-port	*(optional item) Designating UDPdestination port for accountingrequest.*
port-number2	*(optionalitem)Theportnumberofaccountingrequest.Ifthesettingis0, the host is not used for accounting.*

Default

Any RADIUShost isnot designated.

Command mode

globalconfigurationmode

Explanation

Thecommand“radiusserver”canbeusedrepeatedlyfordesignatingmultipleservers. Thepollingcanbemadeundertheorder ofconfigurationwhennecessary.

Example

TheExamplebelowdesignatesRADIUShostwhoseIP addressis1.1.1.1.Thedefault port isused foraccountingand authentication.

radius-server host 1.1.1.1

ThefollowingExampledesignatesPort12asthedestinationportofauthentication requestontheRADIUShostwhoseIPaddressis1.2.1.2.Port16isusedasthe destinationport of accounting request.

radius-server host 1.2.1.2 auth-port 12 acct-port 16

Relevant command

aaaauthentication
radius-server key
username

2.1.7. radius-server optional-passwords

Theglobalconfigurationcommand“radius-serveroptional-passwords”isusedfor verifyingtheusernamewithoutcheckingpasswordwhenRADIUSauthentication requestistransmittedtoRADIUSserverforthefirsttime.The“no”formatofthe commandcanbeusedforrestoringthedefaultvalue.

Syntas

radius-server optional-passwords

noradius-serveroptional-passwords

parameter

none

Default

optional-password mode is not used.

Command mode

globalconfigurationmode

Explanation

Whentheuserentersloginname,theauthenticationrequestwillincludetheuser nameandzerolengthpassword.Iftheauthenticationrequestisaccepted,thelogin authenticationprocessiscompleted.IfRADIUSserverrefusestherequest,theserver willpromptthepasswordinput.Whentheuserentersthepassword,thesecond authenticationwillbetried.RADIUSservershallsupporttheauthenticationoftheuser of nopassword so as totake advantageof this feature.

Example

The followingExample configuresthe exclusionof userpassword whenthe firstauthentication request is transmitted.

radius-server optional-passwords

Relevant command

host

2.1.8. radius-server key

The global configuration command shall be used for setting encryption key for RADIUS communicationbetweentherouterandRADIUSserver.The“no”formatofcommand can beusedforinvalidatingtheencryptionkey.

Syntas

radius-serverkey *string*

noradius-serverkey

Parameter

Parameter	Description
string	Thesecretkeyusedforencrypting.Thesecretkeyshallmatch with the oneused by RADIUS server.

Default

Thesecretkeyisanullcharacterstring.

Command mode

globalconfigurationmode

Explanation

TheenteredsecretkeyshallmatchwiththeoneusedbyRADIUSserver.Allthezero spacecharacterisneglected.Thesecretkeycontainsnospacecharacter.

Example

ThefollowingExamplesets encryptionkeyas“firstime”.

radius-server keyfirstime

Relevant command

Host

username

2.1.9. radius-server retransmit

Theglobalconfigurationcommandisusedfordesignatingthetimesoftrialbefore abandoningsomeserver.The“no”formatofthecommandcanbeusedforrestoring default value.

Syntas

radius-serverretransmit*retries*

noradius-serverretransmit

Parameter

Parameter	Description
retries	Themaximumtimesofrepeatedtrial,thedefaultvalueis2 trials.

Default

Try 3 times

Command mode

globalconfigurationmode

Explanation

Thecommandisusuallyusedtogetherwiththecommand“radiustimeout”,indicating thetimeofthetimeoutofserverresponseandthetimesofrepeatedtrailsafterthe timeout.

Example

TheExamplebelow designatesthevalueofretrialofcounter as 5.

radius retransmit 5

Relevant command

radius-server timeout

2.1.10. radius-server timeout

Theglobalconfigurationcommand“radius-servertimeout”isusedforsettingthetime towaitfortheserverresponsetotherouter.The“no”formatofthecommandisused forrestoringdefaultvalue.

Syntas

radius-servertimeout*seconds*

noradius-servertimeout

Parameter

Parameter	Description
seconds	Designatingthetimeout(unit:second),thedefaultvalueis3

	seconds.

Default

5 seconds

Command mode

globalconfigurationmode

Explanation

The command is usuallyused together with the command “radius retransmit”.

Example

TheExamplebelowsets thevalueoftimeouttimer as 10seconds.

radius timeout10

2.1.11. radius-server vsasend

Theglobalconfigurationcommand“radius-servervsasend”canbeusedfor configuringtherouterintotheonethatis identifiedandusesspecialattributeof manufacturer(VSA).The“no”formatofthecommandcanbeusedforrestoringthe default value.

Syntas

radius-servervsasend[authentication]

no radius-servervsa send[authentication]

Parameter

Parameter	Description
authentication	(optional item) Theidentified specialattribute ofthe manufactureris limitedtotheauthenticationattribute.

Default

VSAis not used.

Command mode

globalconfigurationmode

explanation

IETFusesspecialattributeofmanufacturer(VSA)(attribute26)anddesignatesthe methodforexchangingthespecialinformationofthemanufacturerbetweentherouter andRADIUSserver.VSAallowsmanufacturerstosupporttheirownextendedattribute notsuitabletouniversalpurposes.Thecommand“radiusvsasend”enablestherouter toidentifyandusethespecialattributeofthemanufacturer(VSA)ofauthentication andaccounting.Thekeyword“accounting”isusedinthecommand“radiusvsasend” tolimittheidentifiedspecialattributeofthemanufacturertotheattributeofaccounting. Thekeyword“authentication”isusedinthecommand“radiusvsasend”tolimitthe identified special attribute of the manufacturer to the attribute of authentication.

Example

The following example configures the router to identify and use vendor-specific authentication:.

radius-server vsa send authentication

Relevant command

host

3. TACACS+ Commands

3.1. TACACS+ Command

ThischapterdescribesthecommandsforconfiguringTACACS+securityprotocols. TACACS+canbeusedforauthenticatingtheidentityoftheuser,authorizationof serviceauthority and theaccounting of theexecutionprocess of user service.

3.1.1. debug tacacs

Thecommand“debugtacacs”canbeusedfortracingTACACS+protocoleventor checkingthepacketsreceivedorsent.The“no”formatofthecommandcanbeused forcancelingthetrace.

Syntas

debugtacacs{event |packet}

nodebugtacacs{event | packet}

Parameter

Parameter	Description
event	***Tracing****TACACS+event*
packet	**Tracing**TACACS+packet.

Default

Closingdebuginformation

Command mode

supervisor

Explanation

Thecommandisonlyusedforthedebuggingofthenetworktofindoutthecauseof failure ofAAAservice.

Example

ThefollowingExamplewillopentheeventtraceofTACACS+

debug tacacs event

Relevant commands

none

3.1.2. iptacacssource-interface

Theglobalconfigurationcommand“iptacacssource-interface”isusedforapplyingIP addressofthedesignatedinterfacetoalltheTACACS＋packets.The“no”formatof thecommandcancelthe usingoftheIPaddress.

Syntas

iptacacssource-interface *subinterface-name*

noiptacacssource-interface

Parameter

Parameter	Description
subinterface-name	InterfacenamecorrespondingtothesourceIPaddressofallTACACS＋ packets.

Default

None

Command mode

globalconfigurationmode

Explanation

Thecommandcanbeusedtosetsource IPaddressforallTACACS ＋ packetsby designatingthesourceinterface.Solongastheinterfaceisunder“up”state,all TACACS+packetswilluseIPaddressoftheinterfaceasthesourceaddress,thus ensuringthatTACACS+packetofeachrouterwillhavethesamesourceIPaddress. SoTACACS＋serverwillnot needto maintainthe addresslist containingthe IP address.Thatistosay,inordertoensureallTACACS＋packetscomingfromthe specificroutertohavethesamesourceIPaddress,thecommandwillworkwhenthe router hasmany interfaces.

Thedesignatedinterfaceshallhavetheipaddresslinkedtotheinterface.Ifthe designatedinterfacehasnoIPaddressorisundera“down”state,thedefaultvalue willberestored,namelythesourceIP addressshallbedeterminedonthereal condition. In order to avoidthe case, the IPaddressshallbeaddedtotheinterfaceand theinterfaceshallbeensuredunderthe“up”state.

Example

ThefollowingExamplewilluseIPaddressoftheinterfaces1/0assourceIPaddress of allTACACS+packets.

iptacacssource-interfaceG0/1

Relevant commands

ipradiussource-interface

3.1.3. tacacs-server

Theglobalconfigurationcommand“tacacsserver”isusedfordesignatingTACACS＋ server.The“no” format of the commandisusedfor deletingthedesignatedserver.

Syntas

tacacs-server hostip-address [**single-connection**|**multi-connection**] [**port** *integer1*] [**timeout** *integer2*] [**key***string*]

notacacs-servehost*ip-address*

Parameter

Parameter	Description
ip-address	IPaddress of server
single-connection	(optional) Designatingrouter tomaintain thesingle andopen TCPconnection for the confirmation fromAAA/TACACS+server.
multi-connection	(Optional)DesignatingroutertomaintainthedifferentTCPconnectionfor thedifferentconfirmation fromAAA/TACACS+server
port	(optional) Designating port number ofserver.The option covers the default port number 49.
integer1	(optional)Theportnumberofserver.Therangeofvalidportnumberis1 to 65536.
timeout	(optional)Designatingthetimeoutofwaitingforserverresponse.Itwill covertheglobaltimeoutsetfortheserverbyusingthecommand“tacacs timeout”
integer2	(optional) Setting the value of timeout timer. It is calculated onsecond.
key	(Optional) Specify authentication and encryption keys. This key must match the key used by the TACACS+server program. Specify this. The key will overwrite the key set for this server using the global command tacacs key.
string	(Optional) Specify the encryption key string.

Default

NoTACACS＋serveris designated.

Command mode

globalconfigurationmode

Explanation

Usemultiplecommandsof“tacacsserver”todesignatemultiplehostsandsearching thehostsonthedesignatedorder.Assomeparametersofthecommandsof“tacacs server”willcovertheglobalconfigurationsetbythecommand“tacacstimeout”and “tacacskey”,thecommandcanbeusedtoconfigurethecommunicationattributeof eachTACACS+serverexclusivelysoastoadvancethesecurityofthenetwork. **Example**

TheExamplebelowdesignatesthenegotiationbetweentherouterand TACACS+serverwhoseIPaddressis1.1.1.1soastomakeAAAauthentication,and designatesTCPserviceportnumber51,setsthevalueoftimeout3seconds.The encryptionkey is “a_secret”.

```
tacacs-server host 1.1.1.1 single-connectport 51
tacacs-server host 1.1.1.1 single-connecttimeout 3
tacacs-server host 1.1.1.1 single-connectkey a_secret
```

Relevant commands

tacacs-serverkey
tacacs-servertimeout

3.1.4. tacacs-server key

The global configuration command“tacacs-serverkey” shall be used for setting the encryption keyusedbyallcommunicationprocessbetweentherouterandTACACS+server.The “no” format ofthe command is used forclosing theencryption key.

Syntas

tacacs-serverkeykey

notacacs-serverkey

Parameter

Parameter	Description
key	Usedforsettingthesecretkeyforencryption.Thesecretkeyshallmatch with the one used bythe program ofTACACS+server.

Command mode

globalconfigurationmode

Explanation

Thecommand "tacacs-server key"shallbeusedforsettingencryptionkeybefore TACACS+protocolis running.Theenteredsecretkey shallmatch withtheone usedby theserviceprogramofTACACS+.Allthedrive-headblanksareignoredandthesecret keycontainsnoblank.

Example

The example below sets encryption keyas "testkey":

tacacs-server keytestkey

Relevant commands

tacacs-server

3.1.5. tacacs timeout

To set the timeout length for TACACS+to wait for a response from a server, use the tacacs timeout global configuration command. Use the no form of this command to restore the default value.

Syntas

tacacs-servertimeout*seconds*

notacacs-servertimeout

Parameter

Parameter	Description
seconds	The valueof timeout calculatedon second (between 1 to 600). The default valueis5seconds.

Default

5seconds

Command mode

globalconfigurationmode

Explanation

Ifsomeserversetsitsowntimeoutvalueofwaitingthroughtheparameterinthe command"tacacs- server",thevaluewillcovertheglobaltimeoutvaluesetbythis command.

Example

The Examplebelowchanges the valueof timeout timeras 10 seconds.

tacacs-server timeout10

Relevant commands

tacacs-server

4. IPSec Commands

4.1. crypto map (global configuration)

4.1.1. crypto map (global configuration)

Theglobalconfigurationcommandcanbeusedforcreatingoramendinganencrypted mapandenteringintotheconfigurationstatusofencryptedmap.The“no”formatof thecommandcanbe usedfordeleting anencryptedmaporset.

Syntas

crypto map*map-nameseq-num***ipsec-isakmpdynamic***dynamic-map-name*

nocryptomap *map-nameseq-num*

Parameter

Parameter	Description
map-name	Thenameofencryptedmapset
seq-num	Serialnumberofencryptedmap.Thedetailedexplanationofhowtouse theparameter can be referred to thepart of “Direction for Use”.
ipsec-manual	IPSecSecurityAssociationissetupthroughmanualworkforprotecting thecommunicationdesignatedbytheencryptedmap.
ipsec-isakmp	IPSec SecurityAssociation isset upthrough IKEfor protectingthe communicationdesignatedbytheencryptedmap.
dynamic-map-name	Theencryptedmapisusedasthenameofdynamicencryptedmapthat serves astemplete.
discovery	Start tunnel endpoint discovery

Default

The encrypted map doesnot exist.

Command mode

globalconfigurationmode.Whenthereisnodynamicanditsparameter,thecommand shall beusedforenteringintotheconfiguration status of encrypted map.

Explanation

Thecommandisusedforcreatinganewencryptedmaporamendinganexisting encrypted map.

Afteranencryptedmapiscreated,theparameterdesignatedunder global configurationmodecannotbechangedbecausetheseparametersdecidewhich commandscanbeusedintheconfigurationstatusofencryptedmap.Forexample, Onceamapiscreatedasipsec-isakmp,itcannotbechangedintoipsec-manual.It shallbedeletedandchangedintoipsec-manualundertheconfigurationstatusofthe encrypted map. After theencrypted mapis defined, thecommand “crypto map（ interfaceconfiguration）canbeusedforapplyingtheencryptedmapsettothe interface.

The functionof the encrypted map

Theencryptedmapbearstwofunctions:Filtratingandclassifyingthecommunication thatneedstobeprotectedanddefiningthepolicyofcommunication.Theencrypted map of IPSec links thedefinitionsbelow together:

The communications that shouldbe protected.

TheoppositeterminalofIPSecaccessibletothedataunderprotectioncansetupa securityassociationwiththelocalrouter.

Howtomanageandusesecretkeyandsecurityassociation(orwhenIKEisnotused, whatissecretkey)

Themultipleencryptedmapswiththesamemapnameformsaencryptedmapset.

Theencryptedmapsetisthegatheringcomposedoftheencryptedmaps,ofwhicheach maphas differentseq-num andsame map-name. Therefore, forthe giveninterface,somesecuritypolicycan be adoptedtothecommunicationtransmittedtothe oppositeterminalofIPSec.

Thedifferentsecuritypoliciesshallbeadoptedtoother communicationstransmittedtothesameorthedifferentoppositeterminalsofIPSec.

Tothisend,twoencryptedmapsshallbecreated,eachmaphasthesamemap-name, but has different seq-num.

Seq-numparameter

Thenumericalvalueofseq-num cannotbedefinedatwill.Thenumericalvalueisused forsequencingthemultipleencryptedmapinanencryptedmapset.Theencrypted mapwithsmallseq-numisjudgedbeforethewithbigseq-num,whichmeansthatthe smallerthe numnumericalvalueis,themore prioritythemapping has.

For instance, Hereis theassumption thatthe encryptedmap setcontains threeencryptedmaps:aaa10，aaa20andaaa30.Theencryptedmapsetnamedaaais usedontheinterfaceSerial0.Whenthecommunicationpassesthroughtheinterface Serial0,itshallbejudgedbyaaa10.Ifthecommunicationmatcheswithapermitin theextendedaccesslistdesignatedbyaaa10,thecommunicationwillbeprocessed onthepolicydefinedinaaa10(includingtheIPSecsecurityassociationestablished whennecessary).Ifthecommunicationdoesnotmatcheswithaaa10accesslist,aaa 20willbeused,theaaa30willjudgethecommunication,tillthecommunication matcheswithapermitsentenceinamap(ifthecommunicationdoesnotmatchwith thepermitsentenceinanyencryptedmap,thecommunicationwillbetransmitted directly without any IPSec protection.

Example

Thefollowingexampleshowstherequiredminimumconfigurationfortheencrypted map when the security association is set up through IKE.

```
crypto map aaa10 ipsec-isakmp
        match addressaaa
        set transform-set one
        set peer 192.2.2.1
```

Thefollowingexampleshowstherequiredminimumconfigurationfortheencrypted mapwhenthesecurityassociationissetupthrough dynamic encryptedmap.

```
cryptodynamic-map aaa22
        match addressaaa
        set transform-set one

crypto map bbb10 ipsec-isakmp dynamicaaa
```

Thefollowingexampleshowstherequiredminimumconfigurationfortheencrypted mapwhenthesecurityassociationissetupthroughmanualwork.

```
crypto IPsec transform-set oneah-md5-hmac esp-des

crypto map aaa 10

  match address aaa

  set transform-set one
  set peer 192.2.2.1
```

Relevant command

crypto map (interface configuration)

cryptomaplocal-address

matchaddress

setpeer

setpfs

set security-associationlifetime

settransform-set

showcrypto map

4.1.2. crypto map(interface configuration)

Thecommand“cryptomap”canbeusedforapplyingtheencryptedmapsetdefinedin advancetotheinterface.The“no”formatofthecommandcanbeusedforremoving the encryptedmap set froman interface.

Syntas

crypto map*map-name*

nocryptomap

Parameter

Parameter	Description
map-name	The name of the set of encrypted maps

Default

The encrypted map isnot configured onthe interface.

Command mode

InterfaceConfigurationmode

Explanation

Thecommandisusedforapplyingtheencryptedmapsettotheinterface.An encryptedmapsetshallbeconfiguredbeforetheinterfaceisabletoprovideIPSec service.Onlyanencryptedmapsetcanbesetforaninterface.Ifmultipleencrypted mapshavethesamemap-nameanddifferentseq-num,theywillbeinthesameset andwillappliedtothesameinterface.TheencryptedmapwiththesmallerSeq-num hasthemorepriorityandwillbejudgedbeforehand.Anencryptedmapsetislikelyto contain themix of the encrypted maps ofipsec-isakmp andipsec-manual.

Example

Theexamplebelowcontributestheencryptedmapsetaaatotheinterface S0.When thepacketpassesthroughtheinterfaceS0,alltheencryptedmapsin“mymap”setwill beusedforjudgingthepacket.Whentheoutboundpacketmatcheswiththeaccess listcorrespondingtoalinkageintheencryptedmapsof“mymap”,thelinkage basedon thesecurityassociation(IPSecsupposed)configuredbytheencryptedmapwillbe established(ifthereisnoexistingsecurityassociation).

```
interface G 0/1
  crypto map aaa
```

Relevant command

crypto map (global configuration）

cryptomaplocal-address

showcrypto map

4.1.3. crypto map local-address

Thecommand“cryptomaplocal-address”canbeusedfordesignatinganinterface identifieranddesignatingtheidentifiertobeusedforIPSeccommunicationinthe encryptedmap.The“no”formatofthecommandcanbeusedfordeletingthe command from the configuration.

Syntas

crypto map *map-name* **local-address***interface-id*

nocryptomap *map-name***local-address**

Parameter

Parameter	Description
map-name	The name of the encrypted map set
interface-id	Designatingtheinterfaceidentifierusedbytheencryptedmap set.

Default

none

Command mode

globalconfigurationmode

Explanation

Ifthecommandisconfigured,thelocalterminaladdressofIPSecoftheencrypted map in the encrypted mapset uses IPaddress of the designated interface

Example

none

Relevant command

crypto map (interfaceconfiguration)

4.1.4. crypto map isakmpauthorization

(Xauth command)

4.1.5. crypto map isakmp-profile

Command after entering the crypto map special mode

4.1.6. match address

Thecommand“matchaddress”canbeusedfordesignatinganextendedaccesslist foranencryptedmap.The“no”formatofthecommandcanbeusedforcancelingthe setextendedaccesslistfromanencryptedmap.

Syntas

matchaddress*access-list-name*

nomatchaddress*access-list-name*

Parameter

Parameter	Description
access-list-nam e	Encryptionaccesslist.Thisnameshallmatchwiththenameof theconfiguredaccesslist.

Default

Any access list is configured to the encrypted map.

Command mode

Theconfigurationmodeoftheencryptedmap

Explanation

The command isa must for all the encrypted maps.

Thecommandisusedforcontributingtheextendedaccesslisttoanencryptedmap. The

command “ipaccess-list extended”is used fordefining thisaccess list.

Theextendedaccesslistdesignatedbythecommandisusedby IPSecforjudging whichcommunicationshouldbeprotectedthroughencryptionandwhich communicationsshallnotbeprotectedthroughencryption(Thecommunication allowedbytheaccesslistwillbeprotectedandthecommunicationsrefusedbythe accesslistwillbenotbeprotectedin thecorresponding encryptedmap).

Notes:

Theencryptedaccesslistisnotusedfordecidingwhetherthecommunicationis allowedtopasssomeinterface.Thejobisdonebytheaccesslistthatworksonthe interface.

Theencryptedaccesslistdesignatedbythecommandisusedforjudginginbound communicationandisalsousedforjudgingoutboundcommunication.Theencrypted accesslistcorrespondingtotheencryptedmapofinterfacewillmakejudgmentonthe outboundcommunicationtodecidewhetherthecommunicationshouldbegotunder encryptedprotectionanddecidingtheencryptionpolicyemployedifso(the communicationconfiguresapermit).Afterpassingtheexaminationofcommonaccess listontheinterface,theinboundcommunicationwillbejudgedbytheencrypted accesslistdesignatedbytheencryptedmapsetoftheinterfacetodeterminewhether thecommunicationshouldbegotunderencryptionprotectionandtodecidewhich encryptionpolicyshouldbeadoptedforprotectingthecommunication(Inthecaseof applyingIPSec,theunprotectedcommunicationwillbeabandonedbecauseitshould be protected by IPSec.).

Example

The followingexample is the required minimum configuration of encrypted map createdbyIKE.

```
crypto mapaaa 100ipsec-isakmp
  match addressaaa
  set transform-set one
  set peer 192.2.2.1
```

Relevant command

cryptomap(globalconfiguration)

cryptomap(interface configuration)

cryptomaplocal-address

ip access-list extended

setpeer

set pfs

set security-association lifetime

set transform-set

show crypto map

4.1.7. set peer

Theconfigurationcommandofencryptedmap“setpeer”canbeusedfordesignating theoppositeterminalofIPSecintheencryptedmap.The“no”formatofthecommand canbe used for deleting the opposite terminal of IPSec from the encrypted map.

Syntas

setpeer *ip-address*

nosetpeer *ip-address*

Parameter

Parameter	Description
ip-address	TheoppositeterminalofIPSecdesignatedbyIPaddress.

Default

TheoppositeterminalofIPSecis notdesignatedunderdefaultstate.

Command mode

Configurationmode of Encrypted Map

Explanation

Thecommandisusedfordesignatinganoppositeterminalof IPSecfortheencrypted map.Thecommandisamustforalltheencrypted maps.Oneencryptedmapcanonly designateoneoppositeterminalofIPSec.Iftheoppositeterminalneedstochanged, the new opposite terminalcan be designated, whichwill cover theoriginal settings.

Example

Theexamplebelowshowstheconfigurationofanencryptedmapatthetime IKEis usedforcreatingasecurityassociation.

```
crypto map aaa100ipsec-isakmp
  match addressaaa
  set transform-set one
  set peer 192.2.2.1
```

Relevant command

cryptomap(globalconfiguration)

cryptomap(interface configuration)

cryptomaplocal-address

matchaddress

setpfs

set security-associationlifetime

settransform-set

showcrypto map

4.1.8. set pfs

Whenthenewsecurityassociationisappliedfortheencryptedmap,IPSecshallbe designatedtoapplyingforperfectforwardsystem(PFS),orwhentheapplicationfor settingupnewsecurityassociationisreceived,IPSecwilldemandPFSthatthe configurationcommandofencryptedmap“setpfs”canbeused.The“no”formatofthe commandcanbeusedfordeterminingthatIPSecwillnotapplyforPFS

Syntas

setpfs[group1|group2]

nosetpfs

Parameter

Parameter	Description
group1	WhennewDiffle-Hellmanexchangeisorganized,thedesignatedIPSec willuse768-digitDiffle-Hellmangroup.
group2	WhennewDiffle-Hellmanexchangeisorganized,thedesignatedIPSec willuse1024-digitDiffle-Hellmangroup.
Group5	When organizing a new Diffle-Hellman exchange, specify that IPSec will use the 1536-bit Diffle-Hellman group

Default

Underdefaultstate,PFSisnotrequired.

Command mode

The configuration mode ofencrypted map

Explanation

The command is applicable only to the encrypted map ofipsec-isakmp.

Duringthenegotiationperiod,thecommandenablesIPSectoapplyfornewsecurity

associationfortheencryptedmapandPFSsimultaneously.Whenthelocalterminal startsnegotiationandlocalconfigurationdesignatestheuseofPFS,theopposite terminalsshallorganizePFSexchange,otherwisethenegotiationwillfail.Iflocal configurationdoesnotdesignateagroup,thelocalrouterwillsuggesttheuseof defaultvaluegroup1andeithergroup1orgroup2providedbytheoppositeterminal willbeaccepted.Iflocalconfigurationdesignatesgroup2,theoppositeterminalshall providethisgroup,otherwisethenegotiationwillfail.Iflocalconfigurationdoesnot designatePFS,thelocalrouterwillaccept PFS provided by the opposite terminal.

PFS adds another level of security, because if a key has been unlocked by an attacker, only the data transmitted with this key will be threatened. Without PFS, data transmitted with other keys may also be threatened.

When PFS is used, a new Diffle-Helman exchange will be triggered each time a new security alliance is negotiated (this exchange requires additional processing time).

1024-biteDiffle-Hellmangroup,namelygroup2,offersmoresecuritythangroup1 does. But ittakes more time for processing.

Example

The followingexample designatesthat PFSshould beused atany timewhen encryptedmapaaa100negotiatesnewsecurityassociation.

```
crypto map aaa100 ipsec-isakmp
  set pfsgroup2
```

Relevant command

crypto map(globalconfiguration) **crypto**

map(interface configuration)

cryptomaplocal-address

matchaddress

setpeer

set security-associationlifetime

set transform-set

showcrypto map

4.1.9. set security-association lifetime

Theconfigurationcommandofencryptedmap“Setsecurity-associationlifetime”can beusedforsettinglifetimevalueforanencryptedmap(thisvalueisusedfor negotiatingIPSecsecurityassociation).The“no”formatofthecommandcanbeused forrestoringthelifetimevalueofan encrypted map to the default value.

Syntas

set security-associationlifetime[**seconds** *seconds*|**kilobytes***kilobytes*]

noset security-associationlifetime [seconds|kilobytes]

Parameter

Parameter	Description
seconds*seconds*	Designatingthesurvivingsecondsofasecurityassociationbeforethe timeout terminates.
kilobytes*kilobytes*	Thecommunicationtrafficthatcanbetransmittedbyusingthissecurity associationbeforethetimeoutofasecurityassociationoccurs(calculated on kilobyte)

Default

The security association ofencryptedmap is negotiated on the default lifetime value. The default timeout is 28800 seconds (1 hour), and the default timeout traffic is 2560000 kilobytes.

Command mode

Configurationstatus of encrypted map

Explanation

The command is applicable only to theipsec-isakmpencrypted map.

IPSecsecurityassociationusesthesharedsecretkeys.Thesesecretkeysandtheir correspondingsecurityassociationovertimessimultaneously.Giventheassumption thatthespecifiedencryptedmaphasbeenconfiguredwithnewlifetimewhenthe routerappliesfornewsecurityassociationinthenegotiationofsecurityassociation,it willuseitsownlifetimevalueofencryptedmapintheapplicationmadetotheopposite terminalandusethevalueasthelifetimevalueofnewsecurityassociation.Whenthe routerreceivestheapplicationfornegotiationtransmittedfromtheoppositeterminal,it willtakethesmalleroneofthelifetimevaluesthataresuggestedbytheopposite terminalandconfiguredbythelocalrouterrespectivelyasthelifetimeofnewsecurity association.

Thelifetimecanbeclassifiedintotwo:oneisthesecondslifetime,theotheriskilobyte lifetime.Eitheroneofthetwolifecyclesexpiresfirst,thesecurityassociationwill overtime.

Theformatofthecommand“setsecurity-associationlifetimeseconds”canbeusedfor changingsecondslifetimethatdesignatesthatsecurityassociationandsecretkey overtimesafterthegivenseconds.

Theformatofthecommand“setsecurity-associationlifetimekilobytes”canbeusedfor changingthekilobytelifetimethatdesignatesthatsecurityassociationandsecretkey overtimeswhenthecommunicationtraffic(calculatedonKB)encryptedbythesecret keyofsecurityassociationreachesasetamount.

Theshorter the lifetimevalue is, the more difficult the secretkey isattacked or

decrypted as the data available to the attacker is less.However, the shorter the lifetime is,themoreworkingtimeCPUtakesforestablishingnewsecurityassociation.

Thelifetimevaluewillbeignoredatthetimeofsettingupsecurityassociationthrough manualwork(Theencryptedmapofipsec-manualisusedforcreatingsecurity association).

Howlifetimeworks:

Giventheassumptionthatthespecifiedencryptedmapisnotconfiguredwithnew lifetime,whentherouterappliesfornewsecurityassociation,itwillusethedefault lifetimevalueintheapplicationmadetotheoppositeterminalandwillusethevalueas lifetimevalueofnewsecurityassociation.Whentherouterreceivestheapplicationfor negotiationtransmittedfromtheoppositeterminal,itwilltakethesmalleroneofthe lifetimevaluesthataresuggestedbytheoppositeterminalandconfiguredbythelocal router respectively as the lifetime valueofnewsecurityassociation.

Afteraperiodoftime(designatedbythekeyword“seconds”),agivenbyteof communicationtrafficistransmitted.Eitherofthesaidtwoeventsoccursfirst,the securityassociation(andcorrespondingsecretkey)willovertime.

Newsecurityassociationstartsnegotiationbeforethelifetimelimitoforiginalsecurity associationishitsoastoensureanewsecurityassociationavailablewhentheoriginal securityassociationovertimes.Thenewsecurityassociationstartsnegotiation30 secondsinadvanceoftheovertimeofsecondslifetimeorwhenthecommunication traffictransmittedthroughthetunnelhas256KBawayfromkilobyteslifetime(based onthesequenceoftheoccurrenceoftheevents)

Ifnocommunicationpassesthroughthetunnelduringthewholelifetimeofasecurity association,thenegotiationofnewsecurityassociationwillbecarriedoutwhenthis securityassociationovertimes.Correspondingly,thenegotiationofnewsecurity associationwillbeconductedonlywhenIPSecgainsasubgroupthatshallbe protected.

Example

Thisexampleofencryptedmapsetstheshorterlifetimevaluebecausethesecretkey ofsecurityassociationbelongingtotheencryptedmapislikelytobestolen.Kilobyte lifetimevalueremainsunchangedasthecommunicationtrafficsharingthesesecurity associationisnotsolarge.Thesecondslifetimevalueisshortenedto1800seconds (30minutes).

```
crypto map aaa100 ipsec-isakmp
  set security-association lifetime seconds 1800
```

Relevant command

crypto map(globalconfiguration) **crypto**

map(interface configuration)

cryptomaplocal-address

matchaddress

setpeer

Setpfs

settransform-set

showcrypto map

4.1.10. set security-association idle-time

To set how long the sa expires without receiving any message, you can use the Set security-association idle-time encryption mapping table configuration command. To restore the idle lifecycle value of an encrypted mapping table to the default value, you can use the no format of this command.

set security-association idle-time [**seconds** *seconds*]

no set security-association idle-time [*seconds*]

Parameter

Parameter	Description
seconds*seconds*	Specify the number of seconds for a security alliance to timeout and terminate the survival after not receiving the message.

Default

Turn off this timeout function.

Command mode

Encryption mapping table configuration status

Explanation

When no message about a sa is received for a period of time, the peer corresponding to the sa is considered to have a problem, and the sa is deleted. If the set peer has a default peer set, the subsequent message transmission will use this peer for negotiation and communication.

Example

```
crypto map tohub 1 ipsec-isakmp
  set peer 10.1.1.1
  set peer 10.2.2.2
  set security-association idle-time 120
```

Relevant command

set peer

4.1.11. set security-association level per-host

To establish a security association based on the host address pair in the spacl, you can use the Set security-association leeve per-host encryption mapping table configuration command. To restore to create a sa for each acl, you can use the no format of this command.

set security-association level per-host

no set security-association level per-host

Parameter

None

Default

Turn off this function.

Command mode

Encryption mapping table configuration status

Explanation

This command only supports ipsec-isakmp map and does not support dynamic map
By default, the establishment of a sa corresponds to each access list. If a message belongs to this ACL, the ike negotiation is triggered, and the sa is established, then the next message, even if the source and destination addresses are different, still belongs to the same ACL, will use the sa just now to protect the message and will not restart the negotiation
However, after this command is configured, as long as it conforms to acl, an independent sa will be established between any different host address pairs
When using this command, it is necessary to consider that the increase in the number of sas and the number of negotiations will impose a heavy burden on the system.

Example

With an access list entry of **permit ip 1.1.1.0 255.255.255.0 2.2.2.0255.255.255.0**and a per-host level:

- A packet from 1.1.1.1 to 2.2.2.1 will initiate a security association request which would look like it originated via **permit ip host 1.1.1.1 host 2.2.2.1**.

- A packet from 1.1.1.1 to 2.2.2.2 will initiate a security association request which would look like it originated via **permit ip host 1.1.1.1 host 2.2.2.2**.

- A packet from 1.1.1.2 to 2.2.2.1 will initiate a security association request which would look like it originated via **permit ip host 1.1.1.2 host 2.2.2.1.**

Without the per-host level, any of the above packets will initiate a single security association request originated via **permit ip 1.1.1.0 255.255.255.0 2.2.2.0255.255.255.0**

Relevant command

crypto dynamic-map
crypto map (global configuration) (IPSec)
crypto map (interface configuration) (IPSec)
crypto map local-address
match address (IPSec)
set peer (IPSec)
set pfs
set security-association lifetime
set transform-set
show crypto map (IPSec)

4.1.12. set security-association replay

To turn off the anti-replay check of SA or set the anti-replay window size, you can use the Set security-association replay encryption mapping table configuration command. To restore the anti-replay window size of an encrypted mapping table to the default value, you can use the no format of this command.

set security-association replay [**window-size**[1024/128/256/64] / **disable**]

no set security-association replay [**window-size**[1024/128/256/64] / **disable**]

Parameter

Parameter	Parameter Description
disable	Cancel anti-replay function
Window-size1024/128/256/64	Specify the size of the anti-replay window

Default

Enable the anti-replay function, and the window size is 64.

Command mode

Encryption mapping table configuration status

Explanation

The role of anti-replay is to prevent attackers from sending the same message continuously, thus forcing the gateway to carry out decryption and other related processing, thus consuming the system resources of the gateway
The usage rules of anti replay are as follows:

If replay windows is not started, the package is always acceptable

After opening the replay window,

The received packet seq is larger than the previously received seq, and the packet is acceptable.
If the received packet seq is smaller than the previously received seq and the difference is greater than the window size, it will be discarded

If the received packet seq is smaller than the previously received packet seq and the gap is smaller than the window size, but the bitmap indicates that the packet has been received, it will be discarded.

Otherwise, the package is acceptable

You must enable authentication to use the replay window,

Because the scope of authentication includes the header of esp/ah. If there is no authentication, the replay window check and update are completed before encryption Attackers can send some packets continuously, occupy some seqs in bitmap, and cause normal packets to fail the replay window check

Or the attack can send a packet with a large seq and move the replay window a large block to the right according to the principle. Then all subsequent packets smaller than this seq may be rejected

All packets that enter the replay window check must be authenticated first, unless AH is not used and the auth function of esp is not used.

Example

router# configure
router(config)# crypto ipsec security-association replay window-size 128

Relevant command

None

4.1.13. set transform-set

Theconfigurationcommandofencryptedmapofsettransform-setcanbeusedfor designatingthetransformsetusedbytheencryptedmap.The“no”formatofthe commandcanbeusedforremovingalltransform setsfrom the encrypted map.

Syntas

set transform-set *transform-set-name1 [transform-set-name2...transform-set-name6]*

no set transform-set

Parameter

Parameter	Parameter Description
transform-set-name	Change the name of the collection. For ipsec-manual encryption mapping tables, only one transformation set can be specified. For ipsec-isakmp, you can specify no more than six sets of encryption mapping tables.

Default

Any transform set is included under default state.

Command mode

Configurationstatus of encrypted map

Explanation

The command isa must for all the encrypted maps.

Thecommandisusedfordesignatingthetransformsetsthatwillbecontainedinan encrypted map

Thecommandcanbeusedforlistingmultipletransformsetsforencryptedmapof ipsec-isakmp.The transform set with top priority will be listed first.

Iflocalrouterstartsnegotiation,thetransformsetwillbeprovidedtotheopposite terminalonthesequencedesignatedintheencryptedmap.Iftheoppositeterminal starts negotiation,thelocalrouterwill accept the first matchable transform.

Thefirstmachabletransformsetfoundatthetwoterminalswillbeusedforcreating securityassociation.Ifnomatchitemisfound,IPSecwillnotsetupsecurity association.Themessagewillbeabandonedbecausenosecurityassociationprotect thesecommunications.

Thesoletransformsetcanbedesignatedfortheencryptedmapofipsec-manual.If thistransformsetisnotabletomatchwiththeoneofencryptedmapoftheopposite terminal,thetwoterminalsofIPSeccannotcommunicatenormallyastheyuse different rules for protectingcommunication.

Ifthecontentoftransformsetneedstobechanged,thecontentofthetransformset shallberesettocovertheoldone.Thischangewillnotaffecttheexistingsecurity associationbutwillbeusedforcreatingnewsecurityassociation.Ifthechangeis neededtotakeeffectassoonaspossible,thecommand“clearcryptosa”canbeused fordeletingthewholeorpartialcontentof security association database.

Any transformset containingin anencrypted mapshall bedefined firstby thecommand“cryptoipsectransform-set”.

Example

Theexamplebelowdefinestwotransformsetsanddesignatingthemtobeusedina sameencryptedmap(theexampleisusedonlywhenIKEisusedforcreatingsecurity association.Fortheencryptedmapusedbythesecurityassociationsetupthrough manual work,a given encrypted map contains onlya transformset.).

```
crypto ipsec transform-set one esp-des esp-sha-hmac
crypto ipsec transform-set twoah-sha-hmacesp-des esp-sha-hmac
crypto map aaa100 ipsec-isakmp
  match addressaaa
  set transform-set one two
  set peer 192.2.2.1
```

Inthisexample,whenthecommunicationmatcheswithaccesslistaaa,thesecurity associationcanusetransformsetone(firstprioritylevel)andset2(secondpriority level),whichdependsonthesetandthematchingwiththetransformsetonthe oppositeterminal.

Relevant command

crypto map(globalconfiguration)

crypto map(interface configuration)

cryptomaplocal-address

matchaddress

setpeer

setpfs

set security-associationlifetime

showcrypto map

4.1.14. set session-key {inbound|outbound}

To manually specify the IPSec key in the encryption mapping table, you can use the set encryption mapping table configuration command. To delete the IPSec key from the encryption mapping table, you can use the no format of this command. This command is only available for ipsec-manual encryption mapping table.

set session-key{*inbound*|*outbound*} *ahspi hex-key-string*

set session-key {*inbound*|*outbound*} *espspi* [**cipher***hex-key-string*] [**authenticator***hex-key-string*]

Parameter

Parameter	Parameter Description
inbound	Set the incoming message IPSec key (both incoming and outgoing message keys must be set).
outbound	Set the outgoing message IPSec key (both incoming and outgoing message keys must be set).
ah	Set IPSec key for AH protocol. Only works if the transformation set of this encrypted mapping table includes AH transformation.
esp	Set IPSec key for ESP protocol. Only works if the transformation set of this encrypted mapping table includes ESP transformation.
spi	Security parameter index value (SPI), which uniquely identifies a security federation. SPI is any given number between 256 and 4294967295 (FFFFFFFF). A security alliance with two directions (out and in) and two protocols (AH and ESP) can be assigned to the same SPI. For a given destination address/protocol combination, a unique SPI value must be used. If it is inbound, the destination address is the router address. If outbound, the destination address is the address of the opposite end.
hex-key-string	Key; Enter in hexadecimal format. This is an arbitrary hexadecimal string of 8, 16, 20, or 24 bytes in length. If the transformation set of the encryption mapping table includes the DES algorithm, each key needs at least 8 bytes. If the transformation set of the encryption mapping table includes the 3DES algorithm, each key needs at least 24 bytes. If the transformation set of the encryption mapping table includes the MD5 algorithm, each key needs at least 16 bytes. If the transformation set of the encryption mapping table includes the SHA algorithm, each key needs at least 20 bytes. Keys longer than the above length will be simply truncated.
cipher	Indicates that this key string is the key of the ESP encryption transformation。
authenticator	(Optional) Indicates that this key string is the key for ESP authentication transformation. This parameter is only required if the transformation set of the encrypted mapping table includes the ESP verification algorithm.

Default

No IPSec key is defined by default.

Command mode

Configurationstatus of encrypted map

Explanation

Use this command to specify the IPSec key for the security alliance established through the ipsec-manual encryption mapping table (for the ipsec-isakmp encryption mapping table, the security alliance and corresponding key are automatically established through IKE negotiation).

If the transformation set of the encryption mapping table includes the AH protocol, the IPSec key must be defined for both the outgoing and incoming communications of the AH. If the transformation set of the encryption mapping table includes the ESP encryption protocol, the IPSec key must be defined for both the ESP encrypted outgoing and incoming communications. If the transformation set of the encryption mapping table includes the ESP authentication protocol, the IPSec key must be defined for both the incoming and outgoing communications of the ESP authentication.

When defining multiple IPSec keys for an encryption mapping table, you can assign the same SPI number to all keys. SPI is used to identify the security federation corresponding to this encryption mapping table. However, not all SPI assignments have the same randomness. It should be ensured that the same SPI assignment is not more than once for the same destination address/protocol combination.

The security alliance established through this command will not time out (different from the security alliance established through IKE).

The local key must match the peer key. If a key is changed, the security alliance using this key will be deleted and re-added.

The ipsec-manual map is not configured with security-association and set pfs.

Example

The following example establishes the encryption mapping table of the security alliance manually. The transformation set one contains only one AH protocol.

```
crypto ipsec transform-set oneah-md5-hmac
crypto map aaa 100 ipsec-manual
  match address aaa
  set transform-set one
  set peer 192.2.2.1
  set session-key inbound ah 300 11111111111111111111111111111111
```

set session-key inbound ah 300 22222222222222222222222222222222

The following example is an encryption mapping table for manually establishing a security alliance. The transformation set one contains an AH protocol and an ESP protocol. In this way, the key must be configured for both outgoing and incoming communications of AH and ESP. This transformation set includes the encryption and authentication transformation of ESP, so you need to use the cipher and authenticator keywords to create the key x for both transformations.
crypto ipsec transform-set oneah-sha-hmacesp-des esp-sha-hmac

crypto map aaa 100 ipsec-manual
match address aaa
set transform-set one
set peer 192.2.2.1
set session-key inbound ah 300 9876543210987654321098765432109876543210
set session-key inbound esp 300 cipher 0123456789012345
set session-key outbound esp 300 cipher abcdefabcdefabcd

Relevant command

crypto map(global configuration)

crypto map(interface configuration)

crypto map local-address

match address

set peer

set transform-set

show crypto map

4.1.15. crypto dynamic-map

Theglobalconfigurationcommand“cryptodynamic-map”canbeusedforcreatingor amendingadynamicencryptedmapandenteringintotheconfigurationstatusof dynamicencryptedmap.The“no”formatofthecommandcanbeusedfordeletinga dynamic encrypted map orset.

Syntas

cryptodynamic-map*map-name*

no cryptodynamic-map*map-name*

Parameter

Parameter	Description

map-name	The name of dynamic encrypted map set

Default

dynamic encrypted map does not exist.

Command mode

globalconfigurationmode.Thecommandisusedforenteringintotheconfiguration status of dynamicencrypted map.

Explanation

Thecommandisusedforcreatinganewdynamicencryptedmaporamendingthe existingdynamicencryptedmap.

Thefunctionsofdynamicencryptedmapandcommonencryptedmaparesimilar.The majordifferencesliesin:

IPaddressoftheoppositeterminaldoesnotneedtobesetinthedynamicencrypted mapandallowsIPSecequipmentofanyaddresstonegotiate,thisfunctioncanbe usedforsupportingtheconnectionwiththemobileusers.Whilecommonencrypted mapshalldesignateIPaddressoftheoppositeterminalandonlyallowsIPSecofthe addresstonegotiate.IPaddresscanbesetindynamicencryptedmap.Undersuch circumstance,thedynamicencryptedmapbasicallyequalstothecommonencrypted map.

Example

Theexamplebelowshowstheconfigurationneededfortheminimumencryptedmap whenIKEisusedforestablishingsecurityassociation.

```
cryptodynamic-map aaa 1
  match address aaa
  set transform-set one
```

Relevant command

crypto map (global configuration)

matchaddress

setpeer

setpfs

set security-associationlifetime

settransform-set

showcrypto map

4.2. Crypto ipsec configuration command

4.2.1. crypto ipsecdf-bit

To specify how to set the df bit in the outer IP header of the ipsec tunnel mode, you can use the crypto ipsecdf-bit global configuration command. Use the no format of this command to restore the default settings.

crypto ipsecdf-bit{clear / set / copy}

no crypto ipsecdf-bit{clear / set / copy}

Parameter

Parameter	Description
clear	No matter how the inner message is set, the outer header does not set df bit
Set	If pmtu is indeed exceeded after the header of tunnel is added, df bit must be set in the outer header
copy	If df bit is set for the inner message header, the outer message header should also be set

Default

df-bit copy

Command mode

Global configuration status

Explanation

The use of this command mainly depends on whether the user wants to send a message larger than Pmtu. If so, it should be set to clear. However, it must be considered that the resulting fragmentation and packet operation will affect the system performance.

Example

```
router# configure
router(config)# crypto ipsecdf-bit clear
```

Related command

crypto ipsec transform-set

mode tunnel

4.2.2. crypto ipsecsecurity-association idle-time

Configure the global security-association idle-time attribute. You can use the crypto ipsec security-association idle-time global configuration command. Use the no format of this command to restore the default settings.

crypto ipsec security-associationidle-time <60-86400>

no crypto ipsec security-associationidle-time

Parameter

Parameter	Description
seconds *seconds*	Specify the number of seconds that all security federations will expire after timeout after no message is received

Default

No idle time configuration

Command mode

Global configuration status

Explanation

Configure the sa idle time globally. If the encryption mapping table does not set the sa idle time, the global setting will be used Otherwise, use the sa idle time configured by the encryption mapping table itself.

See set security-association idle-time for working principle

Example

```
router# configure
router(config)# crypto ipsec security-association idle-time 600
```

Related command

clear crypto ipsecsa
clear crypto saipsec
crypto ipsec security-association lifetime
set security-association idle-time

4.2.3. crypto ipsecsecurity-association lifetime

To configure the global security-association lifetime attribute, you can use the crypto ipsec security-association lifetime global configuration command. Use the no format of this command to restore the default settings.

crypto ipsec security-associationlifetime[**seconds** *seconds*| **kilobytes***kilobytes*]

no crypto ipsec security-associationlifetime[**seconds** | **kilobytes**]

Parameter

Parameter	Descriptio
seconds *seconds*	Specify the number of seconds a security alliance can survive before the timeout expires
kilobytes*kilobytes*	The amount of traffic (in kilobytes) that can be transmitted by using a security alliance before it times out

Default

The default timeout is 28800 seconds (1 hour), and the default timeout traffic is 2560000 kilobytes.

Command mode

Global configuration status

Explanation

Configure the lifetime time of sa globally. If the encryption mapping table does not set the lite time, the global setting will be used Otherwise, use the sa lifetime configured by the encryption mapping table.

See set security-association lifetime for working principle

Example

router# configure.

router(config)# crypto ipsec security-association lifetime seconds 2700

router(config)# crypto ipsec security-association lifetime kilobytes 2304000

Relatedcommand

clear crypto ipsecsa

clear crypto saipsec

crypto ipsec security-association idle-time

set security-association lifetime

4.2.4. crypto ipsecsecurity-association replay

To configure the global security-association replay attribute, you can use the crypto ipsec security-association replay global configuration command. Use the no format of this command to restore the default settings.

crypto ipsec security-association replay [disable| window-size [1024/128/256/64]**]**

no crypto ipsec security-association replay [disable| window-size]

Parameter

Parameter	Parameter Description
disable	Cancel anti-replay function
Window-size1024/128/256/64	Specify the size of the anti-replay window

Default

Enable the anti-replay function, and the window size is 64

Command mode

EXEC

Explanation

Configure the replay configuration of sa globally. If the encryption mapping table does not set the replay, the global settings will be used Otherwise, use the sa replay configured by the encryption mapping table.

See set security-association replay for working principle.

Example

router# configure.
router(config)# cry ipsec security-association replay window-size 512

Related command

clear crypto ipsecsa

clear crypto saipsec
cry ipsec security-association replay

4.2.5. crypto ipsec transform-set

Theglobalconfigurationcommand“cryptoipsectransform-set”isusedfordefiningaipsectransformset---afeasiblemixofsecurityprotocolandalgorithm.The“no”formatofthecommandcanbeusedfordeletingatransformset.

Syntas

cryptoipsectransform-set *transform-set-name*

nocryptoipsectransform-set *transform-set-name*

Parameter

Parameter	Description
transform-set-name	Designating thename of transform set that is to be created (or amended).
ah-md5-hmac| ah-sha-hmac	Set the authentication algorithm used by ah
esp-3des| esp-aes| esp-des| esp-null| esp-seal	Set the encryption algorithm used by esp
esp-md5-hmac| esp-sha-hmac	Set the authentication algorithm used by esp
comp-lzs	Set compression algorithm

Default

None

Command mode

globalconfiguration mode.The command isexecuted forentering the encryption transformconfigurationstatus.

Explanation

Transformsetisthemixofsecurityprotocols,algorithmandothersettingsof communicationssubjecttoIPSecprotection.

Themultiplesetscanbeconfiguredthenoneormultiplesetscanbedesignatedinthe

encryptedmap.Thetransformsetdefinedintheencryptedmapisusedfornegotiating IPSecsecurityassociationwithaviewtoprotectingthepacketsofaccesslistsetby thematchedencryptedmap.Duringthenegotiation,thetwosidessearchforthesame transformsetavailabletothetwosides.Whensuchsetisfound,thesetwillbe selectedasapartofIPSecassociationoftwosidesthatistobeusedontheprotected communication.

IfIKEisnotusedforsettingupsecurityassociation,asoletransformsetshallbe designated.The set shallhavea negotiation.

Only after the transform set is defined byusing the command, the transform set can be set in the encrypted map.

Thecommand“transform-type”canbe usedforconfiguringthetransformtype.

Example

The example below definesa transform set.

crypto ipsec transform-set oneesp-des esp-sha-hmac

Relevant command

mode transform-type

settransform-set

showcrypto ipsectransform-set

4.2.6. mode

Thecommandofencryptiontransformconfiguration“mode”isusedforchangingthe modeofatransformset.The“no”formatofthecommandcanbe usedforrestoringthe mode to thedefault valueof tunnel mode.

Syntas

mode{tunnel|transport}

no mode

Parameter

Parameter	Description
tunnel|transport	Designatingthemodeofatransformset:tunnelmodeortransportmode. Iftunnelandtransportarenotdesignated,thedefaultvalue(tunnelmode) willbeused.

Default

TunnelMode

Command mode

Configurationmode of EncryptionTransform

Explanation

Thecommandisusedforchangingtransformmode.Onlywhenthemessagethatisto beprotectedandtwoterminalsofIPSechavethesameIPaddressvalue(suchkindof communicationcanbeencapsulatedunderbothtunnelmodeandtransportmode),the settingwillbeeffectiveandwillbeineffectiveforalltheothercommunications(allthe othercommunicationsareencapsulatedundertunnelmode).

IfthecommunicationtobeprotectedandtwoterminalsofIPSechavethesameIP addressandthetransportmodeisdesignated,therouterwillapplyfortransportmode duringthenegotiation.Bothtransportmodeandtunnelmodecanbeaccepted.If tunnelmodeisdesignated,therouterwillapplyfortunnelmodeandonlythetunnel modecan beaccepted.

Afterdefiningthetransformset,theconfigurationstatusofencryptiontransformwill follow.Undertheconfigurationstatus,themodecanbechangedintotunnelmodeor transport mode.

Ifthemodeisnotsetatthetimeofdefiningtransformsetandthemodeofthe transform set needs to be changed later, the transformset shall be re-accessed and its modeshallbechanged.

Ifthecommandisusedforchangingthemode,thechangewillonlyaffectthesetupof thesubsequentIPSecsecurityassociationoftheencryptedmapdesignatingthe transformset.Iftheconfigurationofthetransformsetisneededtotakeeffectassoon aspossible,thepartialorwholedatabaseofsecurityassociationcanbecleared.The moredetailscanbesecuredbyreferringtothecommand“clearcryptosa”.

Tunnel Mode:

Under tunnelmode, thewhole original IPmessage willbeprotected(encryption, verificationorbothtwo)andisencapsulatedbyIPSec(ESP,AHorbothtwo).Thenthe newIPheadwillbeaddedtothemessage,theIPheaddesignatesIPSecsourceand destinationaddress.

AnyIPcommunicationcanbetransmittedbytunnelmode.IfIPSecisusedfor protectingthecommunicationofthehostlinkedtothebackoftwoterminalsofIPSec, thetunnelmodeshallbe used.

Undertransportmode,onlytheeffectiveload(data)ofIPsubgroupisprotected (encryption,verificationorbothtwo)andisencapsulatedbyIPSec(ESP,Ahorboth two). Theoriginal IPmessage head remains unchanged and isnotprotected by IPSec. OnlywhenthesourceofIPsubgrouptobeprotectedanddestinationaddressarethe twoterminalsofIPSec,thetransportmodeisused.Forinstance,thetransportmode canbeusedforprotectingroutermanagementcommunication.Designatingthe transportmodeintheapplicationenablestheroutertonegotiatewiththeremote terminal fordeciding the transport modeor tunnel mode shouldbe used.

Example

Theexamplebelowdefinesatransformsetandchangesthemodeintotransport mode.

```
router_config# crypto ipsectransform-set oneesp-des esp-sha-hmac
router_config_crypto_trans #mode transport
router_config_crypto_trans #exit
router_config#
```

Relevant command

cryptoipsectransform-set

4.2.7. crypto ipsec ipsec6-enable

Enable the ipsec function on ipv6. Use the no format of this command to cancel the ipsec function of ipv6.

Syntas

crypto ipsec ipsec6-enable

no crypto ipsec ipsec6-enable

Parameter

None

Default

Do not enable the ipsec function of ipv6.

Command mode

globalconfigurationmode.

Explanation

This command is used to enable the ipsec function on ipv6 and provide ipsec encryption protection.

Example

```
router# configure
router(config)# crypto ipsec ipsec6-enable
```

Relevant command

Techroutes
NETWORK

None

4.3. IPSec Command

ThischapterdescribesthecommandsforIPSecconfiguration.IPSecprovidesthe securityfortransmittingthesensitiveinformationonthepublicnetwork,suchas Internet.ThesecuritysolutionprovidedbyIPSecisverypowerfulandisbasedonthe standards.Asthesupplementtothedataconfidentiality,IPSecalsooffierstheservice of data verification andanti-replay.

4.3.1. show crypto ipsec transform-set

Thecommand“showcryptoipsectransform-set”canbeusedforcheckingallthe configured transform set

Syntas

showcrypto ipsectransform-set [*transform-set-name*]

Parameter

Parameter	Description
transform-set-name	(Optional) Only the transformation sets with the specified transform-set-name are displayed

Default

If the keyword is not used,all the transform set will be shown on the router.

Command mode

Supervisormode

Explanation

none

Example

The example below is anoutput of the command “show cryptoipsectransform-set”.

router# showcrypto ipsec transform-set

Transform setaaa: { esp-des}

will negotiate ={Tunnel }
Transform setbbb: { ah-md5-hmac esp-3des }
will negotiate ={Tunnel }

Relevant command

None

4.3.2. show crypto map

Thecommand“showcryptomap”canbeusedforcheckingtheconfigurationofthe encrypted map.

Syntas

showcrypto map[*map-name*]

Parameter

Parameter	Description
map-name	(optional)Showingtheencrypted map designated bymap-name.

Default

Ifnokeywordisdesignated,alltheencryptedmapconfigurationswillbeshownonthe router.

Command mode

Supervisormode

Explanation

none

Example

The followingexample isan output of the command“show cryptomap”.

```
router# show crypto map map-name
Crypto Map m 1 ipsec-isakmp
acl name :101,   exist : 0
 peer = 172.16.20.101
  no PFS
  Security association ---  idle_time : 0, level_per_host enable:0, lifetime in
kilobyte : 2560000, lifetime in seconds : 28800, replay window size :64,sa repla
y enable :1
          Transform sets={ t1,  }
```

Relevant command

None

4.3.3. show crypto dynamic-map

To view the configured dynamic encryption mapping table, you can use the show crypto dynamic-map command.

show crypto dynamic-map[*map name*]

Parameter

Parameter	Description
map-name	(Optional) Only the dynamic encryption mapping table with the specified map-name is displayed

Default

If keywords are not used, all dynamic encryption mapping tables on the router will be displayed.

Command mode

Management status

Explanation

None.

Example

The following is an output example of the show crypto dynamic-map command.

```
Router_config#show crypto dynamic-map
dynamic map dyn
Crypto Map dyn 10 ipsec-isakmp
acl name :101,   exist : 0
  no PFS
  Security association ---  idle_time : 0, level_per_host enable:0, lifetime in
kilobyte : 2560000, lifetime in seconds : 5000, replay window size :64,sa replay
 enable :1
     Transform sets={}
```

Related command

None

4.3.4. show crypto saisakmp

To view the settings used by the current phase 1 security federation, you can use the show crypto saisakmp command.

show crypto saisakmp

Parameter

None

Default

If no keyword is specified, all security alliances will be displayed

Command mode

Management status.

Explanation

None.

Example

None.

Relatedcommand

None

4.3.5. show crypto saipsec

To view the settings used by the current phase 2 security federation, you can use the show crypto saipsec command.

Syntas

show crypto saipsec

Parameter

Parameter	Description

interface *interface-id*	(Optional) Display the existing security federation created by the encryption mapping table on the identification interface

Default

If no keyword is specified, all security alliances will be displayed.

Command mode

Management status

Explanation

none

Example

The following is an output example of the show crypto saipsec command”

Router_config#show crypto saipsec
sa bundle property
satype : negotiation
diID : 4
local addr : 172.16.20.102
peer addr : 172.16.20.101
mode :1
nat use :0
port :500
refcnt : 0
sa status using
life left : 3491d
kilobytes life left : 4607872d

sa property
protocol id : 51
inbound spi : d0ef8dff
inbound auth id : 1
inbound crypto id : 0
outbound spi : 8696e777
outbound auth id : 1
outbound crypto id : 0
sarecv success bytes 0
sa send success bytes 128
sarecv err bytes 0
sa send err bytes 0

sa bundle property
satype : negotiation
diID : 4
local addr : 172.16.20.102

peer addr : 172.16.20.101
mode :1
nat use :0
port :500
refcnt : 0
sa status using
life left : 3329d
kilobytes life left : 4608000d

sa property
protocol id : 51
inbound spi : db31bbcf
inbound auth id : 1
inbound crypto id : 0
outbound spi : 93d5f2bc
outbound auth id : 1
outbound crypto id : 0
sarecv success bytes 0
sa send success bytes 0
sarecv err bytes 0
sa send err bytes 0

sa bundle property
satype : negotiation
diID : 4
local addr : 172.16.20.102
peer addr : 172.16.20.101
mode :1
nat use :0
port :500
refcnt : 0
sa status using
life left : 28411d
kilobytes life left : 2559756d

sa property
protocol id : 51
inbound spi : eb95a3a7
inbound auth id : 1
inbound crypto id : 0
outbound spi : 5e78e6b9
outbound auth id : 1
outbound crypto id : 0
sarecv success bytes 100
sa send success bytes 144
sarecv err bytes 0
sa send err bytes 0

Related commands

None

4.3.6. clear crypto sa

The command“clear cryptosa” isused fordeleting therelated IPSecsecurity associationdatabase.

Syntas

clearcryptosa[*isakmp* |*ipsec*]

Parameter

Parameter	Description
isakmp	Delete all first stage sa
ipsec	Delete all second stage sa.

Default

Ifthekeywordofpeer,mapandothersarenotused,alltheIPSecsecurityassociation will be deleted.

Command mode

Supervisormode

Explanation

Thecommandisusedforclearing(deleting)IPSecsecurityassociation.Ifsecurity associationaresetupthroughIKE,theywillbedeleted.ThelaterIPSec communicationrequiresare-negotiationofnewsecurityassociation(WhenIKEis used, IPSec security associationis setup only in thetime of need)

Ifthesecurityassociationissetupthroughmanualwork,thesecurityassociationwill be deleted and will re-established.

Ifthekeywordofpeer,mapandothersarenotused,allIPSecsecurityassociationwill bedeleted.TheuseofkeywordpeerwilldeleteallIPSecsecurityassociationof designatedaddressoftheoppositeterminal.Theuseofkeywordmapwilldeleteall IPSecsecurityassociationcreatedbyencryptedmapset.Allthesecurityassociation canbere-establishedbyusingthecommand“clearcryptosa”.Sothesesecurity associationcanusethelatestconfigurationsettings.Underthecircumstanceofsetting upsecurityassociationbymanualwork,thecommand“clearcryptosa”shallbeused beforethe amendmenttomapsettakeseffect

IftherouterisprocessingIPSeccommunication,thecontentsthataremostvulnerable totheeffectinthesecurityassociationdatabasehadbetterbeclearedinapurposeof avoidthesuddeninterruptionoftheon-goingIPSeccommunication.

noted ： thatthecommandonlyclearsIPSecsecurityassociation.Thecommand“clearcrypto isakmp”shallbeusedforclearingIKEstate.

Example

TheExamplebelowclearsallIpsecsecurityassociationontherouter.

clear crypto sa

Relevant command

clear cryptoisakmp

4.3.7. debug crypto

View IPSec debugging information during IPSec processing.

Syntas

debug crypto control
debug crypto isakmp

Parameter

none

Default

Debug information is not displayed by default.

Command mode

Management status

Explanation

Debug crypto control will display errors in the configuration.
Debug crypto isakmp will display the process and errors during IKE negotiation
Some important error messages related to IPSec processing are displayed. The following table lists several common error messages

show information.	Meaning of information
rec'd IPSEC packet from IPADDR has invalid spi.	The spi value of the outbound on the opposite end is different from that of the inbound on the local end or the configured configuration strategy is different (esp, ah)
packet missing policy	The configuration strategy of the outbound on the opposite side is different from that on the local side (esp, ah).

rec'd IPSEC packet from IPADDR has bad pading.	The encryption key of the outbound end is different from the inbound end.
rec'd IPSEC packet mac verify failed	The difference between the ESP or AH authentication key of the outbound peer and the inbound peer.
rec'd IPSEC packet from IPADDR to IPADDR does not agree with policy	The package processed by IPSEC is different from the corresponding access-list. There is a problem with the access list configuration of the sub-MAP

Relevant command

None

5. Internet Key Exchange Security ProtocolCommand

ThischapterdiscussesthecommandsforInternetSecretKeyExchangeSecurity Protocol (IKE).

IKEisakindofthestandardofsecretkeymanagementprotocolandisusedtogether with IPSec protocol.

IPSecisallowednottouseIKE.However,IKEadvancesthefunctionofIPSecby offeringextrafunctions,flexibilityandthesimplificationofIPSecstandard configuration.

IKEisakindofmixedprotocol,itrealizesOakleysecretkeyexchangeandSkeme SecretKeyExchangewithintheframeworkofInternetSecurityAssociationandSecret Key Management Protocol(（ISAKMP）(ISAKMP，OakleyandSkemearethesecurity protocol realized by IKE).

5.1. IKE configuration command

5.1.1. crypto isakmp enable

To choose to enable IKE negotiation to generate SA, use the global configuration command crypto isakmp enable. To disable IKE negotiation, prefix this global configuration command with no.

Syntas

(no) crypto isakmp enable

Parameter

None

Default

By default, IKE is allowed to negotiate, that is, enable IKE

Command mode

Global configuration status

Explanation

Use this command to enable or disable IKE

Example

None

Relevant command

None

5.1.2. crypto isakmpidentity

To define the device identity type used when participating in IKE negotiation, use the crypto isakmp identity command in the global configuration state. When you specify the pre-shared key, it is used to specify the identity of ISAKMP. To reset the ISAKMP identity to the default value (IP address), prefix this global configuration command with no.

Syntas

crypto isakmpidentity{address|hostname}
no crypto isakmpidentity

Parameter

Parameter	Description
address	Set the IP address of the device interface as the ISAKMP identity during IKE negotiation.
hostname	Set the host name or domain name of the device as the ISAKMP identity during IKE negotiation.

Default

By default, the IP address is used as the ISAKMP identity of the device.

Command mode

Global configuration status

Explanation

The address keyword is usually used when only one interface of the device will be used for IKE negotiation and the IP address of this interface is known.

The hostname keyword is usually used when the device may have multiple interfaces for IKE negotiation, or the IP address of these interfaces is unknown (such as the IP address of the interface is dynamically assigned).

As a general rule, you should usually set the identity of all devices participating in IKE negotiation to the same type.

Example

The following example configures the pre-shared key on the devices at both ends and uses the IP address as the ISAKMP identity:
Local terminal (10.0.0.1)
crypto isakmp identity address
crypto isakmp key 0sharedkeystring address 192.168.1.33

Far end (192.168.1.33)

crypto isakmp identity address
crypto isakmp key 0 sharedkeystring address 10.0.0.1

The following example configures the pre-shared key on both devices and uses the host name as the ISAKMP identity:
Local terminal (10.0.0.1)

crypto isakmp identity hostname
crypto isakmp key 0 sharedkeystringhostname remote.aacom.com
ip host name remote.aacom.com 192.168.1.33 192.168.1.34

Local terminal (192.168.1.33 192.168.1.34)
crypto isakmp identity hostname
crypto isakmp key 0 sharedkeystringhostname local.aacom.com
ip host name local.aacom.com 10.0.0.1

Relevant command

crypto isakmp identity
crypto isakmp key
ip host name

5.1.3. crypto isakmpinvalid-spi-recovery

To configure the device to notify the peer IPSec device of an "illegal SPI" error through

IKE SA, use the global configuration command crypto isakmp invalid-spi-recovery command. To prevent notification of this situation, prefix the global configuration command with no.

Syntas

crypto isakmpinvalid-spi-recovery

no crypto isakmpinvalid-spi-recovery

Parameter

None

Default

This notification is prohibited by default

Command mode

Global configuration status

Explanation

When IPsec processes messages, "illegal SPI" may occur. Invalid SPI Recovery requires IKE to re-establish SA to ensure IPsec can process messages normally. Before re-establishing the SA, IKE will send a notification with the error number of "Invalid SPI" to the IPsec terminal that caused the "illegal SPI". The terminal will delete the local SA (the SA has expired) after receiving such an error number, and then both ends of IPsec will renegotiate a new SA through IKE. Once the SADB of the devices at both ends is resynchronized, the data packets can communicate normally and are no longer discarded.

Example

None

Relevant command

None

5.1.4. crypto isakmpkeepalive

To configure IPSec dead peer detection(DPD), run**cryptoisakmpkeepalive**inglobal configurationmode.Thecommandisusedtopromptlydetectandclearthe locally-stored informationaboutthepeernodewhenthepeernodecannotbereached. TocancelIPSecDPD,run**nocryptoisakmpkeepalive**.

cryptoisakmp keepalive *seconds types*

nocryptoisakmpkeepalive

Parameter

Parameter	Description
Seconds	SpecifiestheintervalofPDPmessageforwarding.Itrangesfrom10to 3600seconds.
types	SpecifiestheconditionsthattriggertheDPDmessagetransmission.The defaultconditionis**on-demand**. <2-69>: retrytimes after the DPD detection failure On-demand: means thatthe DPDmessage issent onlywhen themessage fails tobe sent. Periodic: meansthe DPD message is sentwhen thepath is free.

Default

The default value of theparameter **seconds**is 10.

The default value of the**types**parameteris**on-demand**.

ThedefaultretrytimesaftertheDPDdetectionfailsis5.

Command mode

Globalconfigurationmode

Explanation

When the function isstarted, the peermust support DPD.

Example

ThefollowingexampleshowsthataDPDwhoseintervalis10,whosefailedresending times is 5 and whose type is **periodic**is specified:

crypto isakmpkeepalive10 5periodic

The followingexample showsthat the DPD configuration is canceled: no

crypto isakmpkeepalive

Related command

None

5.1.5. crypto isakmp key

Theglobalconfigurationcommand“cryptoisakmpkey”isusedforconfiguring pre-sharedauthenticationsecretkey.Thesecretkeyshallbeconfiguredfor designatingpre-sharedsecretkeyinIKEpolicyatanytime.The“no”formatofthe commandcanbeusedfordeletingpre-sharedauthenticationsecretkey.

Syntas

cryptoisakmp key0 *keystringpeer-address*

no cryptoisakmp key0 *keystringpeer-address*

Parameter

Parameter	Description
keystring	Designatingpre-sharedsecretkeybyusingletter,numberandcharacter to forma random mixwith 128 bytes at the most.
address	Use IP address as ISAKMP identity of remote device
peer-address	Designating IPaddress of remote terminal
mask	(Optional) Specify the subnet mask of the remote device. The subnet mask can be configured only when the ISAKMP identity of the remote device is set to the IP address
hostname*hostname*	Specify the FQDN of the remote device

Default

Pre-sharedauthenticationsecret key without default

Command mode

globalconfigurationmode

Explanation

IfIKEpolicyincludespre-sharedsecretkeythatisusedasauthenticationmethod, thesepre-sharedsecretkeyshallbeconfiguredonthetwoterminals.Otherwise,the policy shallnot be adopted (The policy willnot be submitted inIKE processfor configuration).

Example

Designatingpre-sharedsecretkeyanddesignatingremoteterminalbyusingIP address.

crypto isakmpkey0 1 address 192.2.2.1

Relevant command

authentication (IKE policy)

5.1.6. crypto isakmpnat keepalive

To allow the device to send NAT keepalive messages, use the global configuration command crypto isakmpnat keepalive. To prevent the device from sending NAT keepalive messages, prefix this global configuration command with no.

Syntas

crypto isakmpnat keepalive *seconds*
no crypto isakmpnat

Parameter

Parameter	Parameter Description
seconds	Time interval for sending nat keepalive message, unit: seconds, value range: 5-3600.

Default

Nat keepalive closed.

Command mode

Global configuration status

Explanation

The crypto isakmpnat keepalive command allows users to keep dynamic NAT mapping valid during the communication between two IPSec peer devices. When IPSec does not send or receive data packets within a specified time interval, it will send NAT keepalive messages

If this command is configured, the user should ensure that the idle time value is less than the valid time of NAT mapping

Example

The following example specifies that NAT keepalive messages are sent every 20 seconds

crypto isakmpnat keepalive 20

Relevant command

None

5.1.7. crypto isakmppeer

To define the IKE policy, use the global configuration command crypto isakmp policy. IKE policy defines a set of parameters to be used during IKE negotiation. Use the no form of this command to delete the IKE policy.

Syntas

crypto isakmppeer{**ip-address** *ip-address*|**fqdn***fqdn*}
no crypto isakmppeer{**ip-address** *ip-address*|**fqdn***fqdn*}

Parameter

Parameter	Parameter Description
ip-address *ip-address*	IP address of the peer device.
fqdn*fqdn*	FQDN of peer device

Default

None.

Command mode

Global configuration status

Explanation

Use this command to configure RADIUS tunnel properties of peer IPSec devices during ISAKMP negotiation

Use this command to enter the ISAKMP peer attribute configuration state (represented by IKE peer).

Example

The following example shows how to specify a pair of segment addresses using RADIUS:

crypto isakmppeer address 1.1.1.1

Relevant command

None

5.1.8. crypto isakmppolicy

Theglobalconfigurationcommand“cryptoisakmppolicy”isusedfordefiningIKE policy.IKEpolicydefinesasetofparametersusedduringIKEnegotiation.The“no” format of the commandis used for deleting IKE policy.

Syntas

cryptoisakmp policy*priority*

no cryptoisakmp policy*priority*

Parameter

Parameter	Description
priority	IdentifyingtheprioritylevelofIKEpolicybyemployingtheintegerfrom1 to10000.1representstopprioritylevelland10000representsbottom prioritylevel.

Default

There isa default policy. The policy is alwayson the bottom priority level. In this default policy,encryption,hash,authentication,Diffie-Hellmangroupandlifetimeparameter areallsetasdefaultvalue.

IfnovalueisdesignatedforthespecificparameterincreatinganIKEpolicy,the default valuewill be applied to theparameter.

Command mode

globalconfigurationmode

Explanation

ThecommandisusedfordesignatingtheparameterthatistobeusedduringIKE negotiation (Theseparameters areused for creating IKE SA).

ThecommandisusedforaccessingtheconfigurationstatusofISAKMP.Underthe configurationstatusofISAKMPpolicy,thefollowingcommandsareeffectivein designatingparametervalueinthepolicy.

- encryption(IKE policy); default value =56 byte DES-CBC

- hash(IKE policy); default value =SHA-1
- authentication(IKE policy);default value=Pre-SharedKey
- group(IKE policy); default value =768 byte Diffie-Hellman
- lifetime(IKE policy); default value =86400 seconds.

Ifoneofthesecommandsarenotdesignatedforthepolicy,thedefaultvalueofthe parameter will be employed.

MultipleIKEpoliciescanbeconfiguredtothetwoterminalsofIPSec.WhenIKE negotiationstartsinanattempttofindthecommonpolicyconfiguredonthetwo terminals,itwillsetoutfromthepolicyoftoppriorityleveldesignatedontheopposite terminal.

Example

The example belowconfigures two ISAKMPpolicies

```
crypto isakmppolicy 10
   hash md5
   authenticationpre-share
   group2
   lifetime 5000
crypto isakmppolicy 20
   authenticationpre-share
   lifetime 10000
```

Theresultofaboveconfigurationisthepolicybelow:

Relevant command

authentication(IKE policy)

encryption(IKE policy)

group(IKE policy)

hash(IKE policy)

lifetime(IKE policy)

showcrypto isakmp policy

5.1.8.1. authentication(IKE policy)

To specify the authentication method in the IKE policy, use the ISAKMP policy configuration command authentication (IKE policy). IKE policy defines a set of parameters used during IKE negotiation. Use the no form of this command to restore the default value of the authentication method.

Syntas

authentication { **pre-share**|**rsa-sig**|**rsa-encr**}

no authentication{ **pre-share**|**rsa-sig**|**rsa-encr**}

Parameter

Parameter	Description
pre-share	Specify the pre-shared key as the authentication method.
rsa-sig	Specify RSA signature as authentication method.
rsa-encr	Specify RSA real-time encryption as the authentication method.

Default

Pre-shared key authentication method

Command mode

ISAKMP policy configuration status

Explanation

Use this command to specify the authentication method used in the IKE policy
If you specify pre-shared keys, you must configure these pre-shared keys separately at the same time (crypto isakmp key command)

Example

This example configures the IKE policy and uses the pre-shared key as its authentication method (all other parameters are the default values):

router_config#cryptoisakmp policy 10

router_config_isakmp# authentication pre-share

router_config_isakmp# exit

router_config #

Relevant command

crypto isakmp key

crypto isakmp policy

encryption(IKE

policy)group(IKE policy)

hash(IKE policy)

lifetime(IKE policy)

5.1.8.2. encryption(IKE policy)

To specify the encryption algorithm in the IKE policy, use the ISAKMP policy configuration command encryption (IKE policy). IKE policy defines a set of parameters that are used during IKE negotiation. Use the no form of this command to restore the encryption algorithm to the default value.

Syntas

encryption {aes|des|3des}

no encryption

Parameter

Parameter	Description
aes	Specify AES as encryption algorithm.
des	Specify DES as encryption algorithm.
3des	Specify 3DES as the encryption algorithm.

Default

DES encryption algorithm

Command mode

ISAKMP policy configuration status

Explanation

Use this command to specify the encryption algorithm used in the IKE policy

Example

This example configures the encryption algorithm in IKE policy as DES encryption algorithm (all other parameters are set to default values):

router_config# crypto isakmp policy 10

router_config_isakmp# encryption des

router_config_isakmp# exit

router_config#

Relevant command

authentication(IKE

policy)

crypto isakmp policy

group(IKE policy)

hash(IKE policy)

lifetime(IKE policy)

5.1.8.3. group(IKE policy)

To specify the Diffie-Hellman group in the IKE policy, use the ISAKMP policy configuration command group (IKE policy). IKE policy defines a set of parameters that are used during IKE negotiation. Use the no form of this command to restore the Diffie-Hellman group to the default value

Syntas

group {**1**|**2**|**5**}
no group

Parameter

Parameter	Parameter Description
1	Specify 768-bit Diffie-Hellman group.
2	Specify 1024-bit Diffie-Hellman group.
5	Specify 1536-bit Diffie-Hellman group.

Ddfuale

768-bit Diffie-Hellman group (group 1)

Command mode

ISAKMP policy configuration status.

Explanation

Use this command to specify the Diffie-Hellman group used in the IKE policy.

Example

This example configures the IKE policy as a 1024 bit Diffie-Hellman group (all other

parameters are set to default values):

router_config# crypto isakmp policy 10
router_config _isakmp# group 2
router_config _isakmp# exit
router_config#

Relevant command

crypto isakmp policy

authentication(IKE

policy)

encryption(IKE policy)

hash(IKE policy)

lifetime(IKE policy)

5.1.8.4. hash(IKE policy)

TheconfigurationcommandofISAKMP policy“hash(IKEpolicy)”isused for designatinghashalgorithminIKEpolicyIKEpolicydefinesasetofparametersthat areusedduringIKEnegotiation.The“no”formatofthecommandcanbeusedfor restoringhashalgorithm as defaultSHA-1hashalgorithm.

Syntas

hash{**sha**|**md5**}

nohash

Parameter

Parameter	Description
sha	Designating SHA-1(HMACvariant)ashashalgorithm.
md5	Designating MD5(HMAC variant)as hash algorithm

Default

SHA-1hash algorithm

Command mode

ConfigurationStatus of ISAKMPpolicy

Explanation

Thecommandisusedfordesignating hashalgorithmusedinIKEpolicy

Example

The Exampleconfigures IKEpolicy asusing MD5 hashalgorithm (all theother parametersare set as default value):

router_config #crypto isakmppolicy 10
router_config _isakmp#hashmd5
router_config _isakmp#exit
router_config#

Relevant command

authentication(IKE policy)

cryptoisakmp policyencryption(IKEpolicy)

group(IKE policy)

lifetime(IKE policy)

crypto isakmp policy

5.1.8.5. lifetime(IKE policy)

TheconfigurationcommandofISAKMPpolicy“lifetime(IKEpolicy)”isusedfor describinglifetimeofIKESA.The“no”formatofthecommandcanbeusedfor restoring SAlifetime as default value.

Syntas

lifetime*seconds*

no lifetime

Parameter

Parameter	Description
seconds	DesignatingthelastingsecondsbeforeIKESAisdisabled.

Default

28800seconds

Command mode

Configuration mode of ISAKMPpolicy

Explanation

Thecommandisusedfordesignatingtheexistingtimeof IKESAbeforeIKESAis disabled.

WhenIKEstartsnegotiation,theagreementisreachedfirstonthesecurityparameters foritsdialogue.Theseaccordantparametersisreferred bySA.IKESA isreservedtill thelifetimeloseseffect.BeforeIKESAloseseffect,itcanbere-usedbythe consequentIKEnegotiation,whichcansavetimeinsettingnewIPSecSA.NewIKE SAisnegotiatedbeforeIKESAloseseffect.Inordertosavethetimeofsetting IPSec, therelativelongIKESAlifetimeshallbeset.Theshortertheconfiguredlifetimeis,the moresecuretheIKEnegotiationis.

Notes:

WhenthelocalterminalstartsIKEnegotiationwiththeoppositeterminal,thepolicy canbechosenonlyontheconditionthatthelifetimeofoppositeterminalpolicyis shorter than or equals to that of local terminalpolicy.

If the lifetime isunequal,choose the shorter one.

Example

TheExampleconfiguresthelifetime ofsecurityassociationofIKEpolicy as600 seconds(alltheotherparametersaresetasdefaultvalue)

```
router_config# crypto isakmppolicy 10
router_config_isakmp# lifetime 600
router_config_isakmp# exit
router_config#
```

Relevant command

authentication(IKE policy)

cryptoisakmp policy

encryption(IKE policy)

group(IKE policy)

hash(IKE policy)

5.1.9. crypto isakmp ikev2 enable

Thecommand“showcryptoisakmpsa”isusedforshowingallthecurrentIKESA.
Enable IKEv2

Syntas

crypto isakmpikev2 enable

no crypto isakmpikev2 enable

Parameter

None

Default

The default is IKEv1; The device will not respond to IKEv2 requests from other devices

Command mode

Global configuration status

Explanation

Use this command to configure IKEv2 for negotiation during ISAKMP negotiation.

When the IKE version is modified through the command, all tunnels established by the current device will be cleared.

When IKEv2 is configured, the device will not respond to IKEv1 requests from other devices

Example

The following example enables the IKEv2 function of the device:

crypto isakmpikev2 enable

Relevant command

The device supports configuration of up to 150 IPsec tunnels with an IPsec throughput of 300 Mbps.