

知 V7防火墙和V3防火墙主模式对接ipsec典型配置举例

IPSec VPN 孙兆强 2018-09-30 发表

组网及说明



F100-A-SI 版本Version 3.40, Release 1662P07

F100-C-G2版本Version 7.1.064, Release 9510P05

配置步骤

V3侧关键配置

```
#
ike proposal 1
  authentication-algorithm md5
#
ike peer 304
  pre-shared-key Sh123456
  remote-address 222.72.136.19
#
ipsec proposal 1
#
ipsec policy 1 1 isakmp
  security acl 3001
  ike-peer 304
  proposal 1
#
acl number 3001
  rule 0 permit ip source 192.168.12.0 0.0.0.255 destination 192.168.0.0 0.0.0.255
  rule 1 permit ip source 192.168.13.0 0.0.0.255 destination 192.168.0.0 0.0.0.255
  rule 2 permit ip source 192.168.14.0 0.0.0.255 destination 192.168.0.0 0.0.0.255
  rule 3 permit ip source 192.168.10.33 0 destination 192.168.0.0 0.0.0.255
acl number 3002
  rule 0 deny ip source 192.168.13.0 0.0.0.255 destination 192.168.0.0 0.0.0.255
  rule 1 permit ip source 192.168.11.0 0.0.0.255
  rule 2 permit ip source 192.168.13.0 0.0.0.255
#
interface Ethernet1/0
  ip address 222.188.87.30 255.255.255.252
  nat outbound 3002
  ipsec policy 1
```

V7侧关键配置

```
acl advanced 3009
  rule 0 permit ip source 192.168.0.0 0.0.0.255 destination 192.168.12.0 0.0.0.255
  rule 1 permit ip source 192.168.0.0 0.0.0.255 destination 192.168.13.0 0.0.0.255
  rule 2 permit ip source 192.168.0.0 0.0.0.255 destination 192.168.14.0 0.0.0.255
  rule 3 permit ip source 192.168.0.0 0.0.0.255 destination 192.168.10.33 0
#
ipsec transform-set ipsec
  esp encryption-algorithm des-cbc
  esp authentication-algorithm md5
#
ipsec policy ipsec 10 isakmp
  transform-set ipsec
  security acl 3009
  local-address 222.72.136.19
  remote-address 222.188.87.30
```

```
ike-profile ipsec
#
ike profile ipsec
  keychain ipsec
  local-identity address 222.72.136.19
  match remote identity address 222.188.87.30 255.255.255.255
  match local address GigabitEthernet1/0/0
  proposal 10
#
ike proposal 10
  authentication-algorithm md5
#
ike keychain ipsec
  match local address GigabitEthernet1/0/0
  pre-shared-key address 222.188.87.30 255.255.255.255 key cipher $c$3$sZn3gVx5zNq5MHil/8fM
hAUa9+WIkEAMlDdQ
#
interface GigabitEthernet1/0/0
  port link-mode route combo enable copper
  ip address 222.72.136.19 255.255.255.0
  nat outbound 3333
ipsec apply policy ipsec
```

配置关键点

- 1、nat的acl将ipsec流量deny掉
- 2、放通相关域间策略。