

知 V7路由器和深信服设备对接ipsec

IPSec VPN

程咪

2019-11-28 发表

问题描述

V7路由器和深信服设备对接ipsec

解决方法

```
#
version 7.1.049, Release 0106
#
sysname MS-VPN
#
telnet server enable
#
password-recovery enable
#
vlan 1
#
vlan 37
name NETWORK
#
controller Cellular0/0
#
controller Cellular0/1
#
interface Aux0
#
interface Fcm5/0
#
interface Fcm5/1
#
interface Fcm5/2
#
interface Fcm5/3
#
interface Fcm5/4
#
interface Fcm5/5
#
interface NULL0
#
interface GigabitEthernet0/0
port link-mode route
combo enable copper
#
interface GigabitEthernet0/1
port link-mode route
description inside
combo enable copper
ip address 10.10.7.75 255.255.255.0
#
interface GigabitEthernet0/2
port link-mode route
description outside
ip address 222.76.251.X 255.255.255.248 //配置本端的公网地址
ipsec apply policy ZFT //绑定ipsec策略
#
scheduler logfile size 16
#
line class aux
user-role network-admin
```

```
#
line class tty
  user-role network-operator
#
line class vty
  user-role network-operator
#
line aux 0
  user-role network-admin
#
line tty 81 86
  user-role network-operator
#
line vty 0 4
  authentication-mode scheme
  user-role network-admin
#
line vty 5 63
  user-role network-operator
#
ip route-static 0.0.0.0 0 10.10.7.254
ip route-static 180.153.19.X 32 222.76.251.X //配置到对端的路由
#
acl number 3000 //配置ipsec感兴趣流量
  rule 0 permit ip source 192.168.23.166 0 destination 10.100.12.106 0

#
domain system
#
aaa session-limit ftp 32
aaa session-limit telnet 32
aaa session-limit http 32
aaa session-limit ssh 32
aaa session-limit https 32
domain default enable system
#
role name level-0
  description Predefined level-0 role
#
role name level-1
  description Predefined level-1 role
#
role name level-2
  description Predefined level-2 role
#
role name level-3
  description Predefined level-3 role
#
role name level-4
  description Predefined level-4 role
#
role name level-5
  description Predefined level-5 role
#
role name level-6
  description Predefined level-6 role
#
role name level-7
  description Predefined level-7 role
#
role name level-8
  description Predefined level-8 role
#
role name level-9
```

```
description Predefined level-9 role
#
role name level-10
description Predefined level-10 role
#
role name level-11
description Predefined level-11 role
#
role name level-12
description Predefined level-12 role
#
role name level-13
description Predefined level-13 role
#
role name level-14
description Predefined level-14 role
#
user-group system
#
local-user yyzc class manage
password hash
service-type telnet
authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
#
ipsec transform-set ZFT //配置ipsec安全提议,要是对端相同
esp encryption-algorithm 3des-cbc
esp authentication-algorithm sha1
pfs dh-group5
#
ipsec policy ZFT 10 isakmp //配置ipsec策略
transform-set ZFT
security acl 3000
local-address 222.76.251.X //配置本段的公网地址
remote-address 180.153.19.X //指向对端的公网地址
ike-profile ZFT
sa duration time-based 28800
#
ike keepalive timeout 28800
#
ike profile ZFT
keychain ZFT
local-identity address 222.76.251.X //本端地址
match remote identity address 180.153.19.X 255.255.255.255 //对端地址
proposal 1
#
ike proposal 1
encryption-algorithm 3des-cbc
dh group5
sa duration 28800
#
ike keychain ZFT
pre-shared-key address 180.153.19.X 255.255.255.255 key cipher $c$3$YBS8RjTmxJwUsRMIZoru
vAYIDC55iTBogjywPN9/6g==
#
return
```

设备列表设置 -- 网页对话框

https://180.153.19.141:8023/html/dlan/c 证书错误

设备名称: XM-YiLianZhong

描述:

设备地址类型: 对端是固定IP

固定IP: 222.76.251.203

认证方式

预共享密钥:

确认密钥:

☒ 启用设备 ☒ 启用主动连接

ISAKMP存活时间: 28800 秒

重试次数: 10

支持模式: 主模式

D-H群: MODP1024群(2)

ISAKMP算法列表

认证算法: SHA-1

加密算法: 3DES

ISAKMP存活时间: 28800 秒

重试次数: 10

支持模式: 主模式

D-H群: MODP1024群(2)

ISAKMP算法列表

认证算法: SHA-1

加密算法: 3DES

https://180.153.19.141:8023/html/dlan/policy_oper 证书错误

策略名称: From-XM_YiLianZhong

描述:

源IP类型: 单个IP

源IP地址: 192.168.23.166

对端设备: XM-YiLianZhong

入站服务: 所有服务

生效时间: 全天

☒ 在时间生效范围内允许 ☐ 在时间生效范围内拒绝

☐ 启用过期时间

过期时间: 0-00-00 0 : 0 : 0

☒ 启用该策略

https://180.153.19.141:8023/html/dlan/policy_oper 证书错误

策略名称: TO-XM_YiLianZhong

描述:

源IP类型: 单个IP

源IP地址: 10.100.12.106

对端设备: XM-YiLianZhong

SA生存时间: 28800 秒

出站服务: 所有服务

安全选项: 默认安全选项

生效时间: 全天

☒ 在时间生效范围内允许 ☐ 在时间生效范围内拒绝

☐ 启用过期时间

过期时间: 0-00-00 : 0 : 0

☒ 启用该策略

☒ 启用密钥完美向前保密