SecPath F100-C-G2

域间策略/安全域 zhiliao_28455 2017-11-21 发表

问题描述

客户需求禁用tcp端口， 在命令行里怎么操作呢， 我做了策略 结果VPN互连网都断了

```
[F100]
[F100]dis cur
#
 version 7.1.064, Ess 9504P11
#
 sysname F100
#
context Admin id 1
#
ip vpn-instance management
 route-distinguisher 1000000000:1
 vpn-target 1000000000:1 import-extcommunity
 vpn-target 1000000000:1 export-extcommunity
#
 telnet server enable
#
 irf mac-address persistent timer
 irf auto-update enable
 undo irf link-delay
 irf member 1 priority 1
#
 security-zone intra-zone default permit
#
 dialer-group 1 rule ip permit
#
 dhcp enable
#
 password-recovery enable
#
vlan 1
#
object-group ip address test
 0 network subnet 10.46.16.0 255.255.255.0
#
object-group service group
 0 service tcp source eq 8801 destination eq 8801
 10 service tcp source eq 7776 destination eq 7776
 20 service tcp source eq 7829 destination eq 7829
 30 service tcp source eq 10306 destination eq 10306
 40 service tcp source eq 2800 destination eq 2800
 50 service tcp source eq 8060 destination eq 8060
 60 service tcp source eq 305 destination eq 305
 70 service tcp source eq 8162 destination eq 8162
 80 service tcp source eq 13159 destination eq 13159
 90 service tcp source eq 18200 destination eq 18200
 100 service tcp source eq 17991 destination eq 17991
#
object-group service test1
 0 service tcp source eq 17911 destination eq 17911
 10 service tcp source eq 18200 destination eq 18200
 20 service tcp source eq 13159 destination eq 13159
 30 service tcp source eq 8162 destination eq 8162
 40 service tcp source eq 305 destination eq 305
 50 service tcp source eq 8060 destination eq 8060
 60 service tcp source eq 2800 destination eq 2800
 70 service tcp source eq 10306 destination eq 10306
```

```
 80 service tcp source eq 7829 destination eq 7829
 90 service tcp source eq 7776 destination eq 7776
 100 service tcp source eq 8801 destination eq 8801
#
dhcp server ip-pool vlan10
 gateway-list 10.46.16.254
 network 10.46.16.0 mask 255.255.255.0
 dns-list 222.172.200.68 61.166.150.123
#
dhcp server ip-pool vlan20
 gateway-list 10.46.24.254
 network 10.46.24.0 mask 255.255.255.0
 dns-list 222.172.200.68 61.166.150.123
#
dhcp server ip-pool vlan30
 gateway-list 10.46.32.254
 network 10.46.32.0 mask 255.255.255.0
 dns-list 222.172.200.68 61.166.150.123
#
interface Dialer1
 mtu 1492
 ppp chap password cipher $c$3$fWngv2og31qobdESaYh//m50io0pAfvb11c=
 ppp chap user rdqhmlyyb
 ppp ipcp dns admit-any
 ppp ipcp dns request
 ppp pap local-user rdqhmlyyb password cipher $c$3$Db3yVeEQnaEB46KSzCBYCRxnJ8bYTGrS/7
Q=
 dialer bundle enable
 dialer-group 1
 dialer timer idle 0
 ip address ppp-negotiate
 tcp mss 1024
 nat outbound 3001
 ipsec apply policy Dia1
#
interface NULL0
#
interface GigabitEthernet1/0/0
 port link-mode route
 combo enable copper
 ip address dhcp-alloc
 pppoe-client dial-bundle-number 1
#
interface GigabitEthernet1/0/1
 port link-mode route
 combo enable copper
#
interface GigabitEthernet1/0/2
 port link-mode route
#
interface GigabitEthernet1/0/2.1
 ip address 10.46.16.253 255.255.255.0
 vrrp version 2
 vrrp vrid 10 virtual-ip 10.46.16.254
 vrrp vrid 10 priority 120
 vlan-type dot1q vid 10
 dhcp server apply ip-pool vlan10
#
interface GigabitEthernet1/0/2.2
 ip address 10.46.24.253 255.255.255.0
 vrrp version 2
 vrrp vrid 20 virtual-ip 10.46.24.254
 vrrp vrid 20 priority 120
 vlan-type dot1q vid 20
```

```
 dhcp server apply ip-pool vlan20
#
interface GigabitEthernet1/0/2.3
 ip address 10.46.32.253 255.255.255.0
 vrrp version 2
 vrrp vrid 30 virtual-ip 10.46.32.254
 vrrp vrid 30 priority 120
 vlan-type dot1q vid 30
 dhcp server apply ip-pool vlan30
#
interface GigabitEthernet1/0/3
 port link-mode route
#
interface GigabitEthernet1/0/4
 port link-mode route
#
interface GigabitEthernet1/0/5
 port link-mode route
#
interface GigabitEthernet1/0/6
 port link-mode route
#
interface GigabitEthernet1/0/7
 port link-mode route
#
interface GigabitEthernet1/0/8
 port link-mode route
#
interface GigabitEthernet1/0/9
 port link-mode route
#
interface GigabitEthernet1/0/10
 port link-mode route
#
interface GigabitEthernet1/0/11
 port link-mode route
#
object-policy ip market-database
 rule 0 drop source-ip test service test1
#
object-policy ip pass
 rule 0 pass
#
security-zone name Local
#
security-zone name Trust
 import interface GigabitEthernet1/0/1
 import interface GigabitEthernet1/0/2
 import interface GigabitEthernet1/0/2.1
 import interface GigabitEthernet1/0/2.2
 import interface GigabitEthernet1/0/2.3
 import interface GigabitEthernet1/0/3
 import interface GigabitEthernet1/0/4
 import interface GigabitEthernet1/0/5
 import interface GigabitEthernet1/0/6
 import interface GigabitEthernet1/0/7
 import interface GigabitEthernet1/0/8
 import interface GigabitEthernet1/0/9
 import interface GigabitEthernet1/0/10
 import interface GigabitEthernet1/0/11
#
security-zone name DMZ
#
security-zone name Untrust
```

```
 import interface Dialer1
 import interface GigabitEthernet1/0/0
#
security-zone name Management
#
zone-pair security source Any destination Any
 object-policy apply ip pass
#
 scheduler logfile size 16
#
line class aux
 user-role network-operator
#
line class console
 user-role network-admin
#
line class vty
 user-role network-operator
#
line aux 0
 user-role network-admin
#
line con 0
 authentication-mode scheme
 user-role network-admin
#
line vty 0 63
 authentication-mode scheme
 user-role network-admin
#
 ip route-static 0.0.0.0 0 Dialer1
#
 ssh server enable
#
acl advanced 3000
 rule 0 permit ip source 10.46.16.240 0.0.0.15 destination 10.0.0.0 0.0.0.255
 rule 5 permit ip source 10.46.16.240 0.0.0.15 destination 10.0.32.0 0.0.0.255
#
acl advanced 3001
 rule 0 deny ip source 10.46.0.0 0.0.255.255 destination 10.0.0.0 0.0.255.255
 rule 10 permit ip source 10.46.0.0 0.0.255.255
#
acl advanced 3050
 rule 0 deny tcp source-port eq 17991
 rule 5 deny tcp source-port eq 18200
 rule 10 deny tcp source-port eq 13159
 rule 15 deny tcp source-port eq 8162
 rule 20 deny tcp source-port eq 350
 rule 25 deny tcp source-port eq 8060
 rule 30 deny tcp source-port eq 2800
 rule 35 deny tcp source-port eq 10306
 rule 40 deny tcp source-port eq 7829
 rule 45 deny tcp source-port eq 7776
 rule 50 deny tcp source-port eq 8801
 rule 55 deny tcp destination-port eq 17991
 rule 60 deny tcp destination-port eq 18200
 rule 65 deny tcp destination-port eq 13159
 rule 70 deny tcp destination-port eq 8162
 rule 75 deny tcp destination-port eq 350
 rule 80 deny tcp destination-port eq 8060
 rule 85 deny tcp destination-port eq 2800
 rule 90 deny tcp destination-port eq 10306
 rule 95 deny tcp destination-port eq 7829
 rule 100 deny tcp destination-port eq 7776
```

```
 rule 105 deny tcp destination-port eq 8801
#
domain system
#
 aaa session-limit ftp 16
 aaa session-limit telnet 16
 aaa session-limit ssh 16
 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 admin class manage
 password hash $h$6$UbIhNnPevyKUwfpm$LqR3+yg1IjNct39MkOR0H0iQXLkYB3jMqM4vbAeoXOh
babIIFnjJPEGR00YiYA1Sz4LiY3FmEdru2fOLMb1shQ==
 service-type ssh telnet terminal https
 authorization-attribute user-role level-3
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
```

```
ipsec transform-set Dia1_IPv4_1
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
ipsec transform-set ipsec
 esp encryption-algorithm des-cbc
 esp authentication-algorithm sha1
#
ipsec policy Dia1 1 isakmp
 transform-set Dia1_IPv4_1
 security acl 3000
 remote-address 110.86.1.226
 ike-profile Dia1_IPv4_1
#
ipsec policy vpn 1 isakmp
 transform-set ipsec
 security acl 3000
 remote-address 110.86.1.226
 ike-profile vpn
#
 ike identity fqdn honghe
#
ike profile Dia1_IPv4_1
 keychain Dia1_IPv4_1
 exchange-mode aggressive
 local-identity fqdn honghe
 match remote identity address 110.86.1.226 255.255.255.255
 match local address Dialer1
 proposal 65535
#
ike profile proposal
#
ike profile vpn
 keychain k1
 exchange-mode aggressive
 local-identity fqdn honghe
 match remote identity address 110.86.1.226 255.255.255.255
#
ike proposal 65535
 description Dia1_IPv4_1
#
ike keychain Dia1_IPv4_1
 match local address Dialer1
 pre-shared-key address 110.86.1.226 255.255.255.255 key cipher $c$3$6w1mmCywHVUHwCx76c
1FOoEOsXEBeASg6w==
#
ike keychain k1
 pre-shared-key address 110.86.1.226 255.255.255.255 key cipher $c$3$6YKPhZsGILwDozvvkOjjgX
gPeblgmrt3Nw==
#
 ip https enable
#
inspect block-source parameter-profile ips_block_default_parameter
#
ips policy default
#
anti-virus policy default
#
return
[F100]
```

解决方法

http://www.h3c.com/cn/Service/Document_Center/IP_Security/FW_VPN/F1000-E-G2/Configure/Operation_Manual/H3C_CG(V7)(R9313_E9504)-5W201/03/201612/964785_30005_0.htm

要禁用内网到外网的某些TCP端口，可以参考手册配一下，配对象策略后，在域间调用下

答案来自于 **功夫熊猫**