

# 知 V7防火墙ipsec野蛮模式web配置（一对多模式）

IPSec VPN 孙兆强 2021-02-27 发表

## 组网及说明



总部公网地址172.16.0.1，分支无论地址是否固定。两边私网地址用loopback地址替代。

## 配置步骤

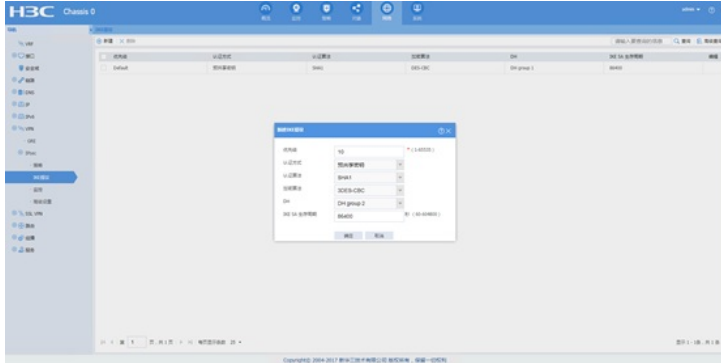
### 地址、安全域及安全策略需自行配置放行

#### 一、总部配置

##### 新建ike提议

网络》VPN》ipsec》IKE提议》新建，选择相应的认证加密等参数

认证加密等参数相同的ike提议建议只配置一个，因为参数相同设备只会去匹配优先级最高的那个ike提议，优先级数值越小越优先。



##### 新建ipsec策略

网络》VPN》ipsec》策略》新建，新建相应的ipsec策略等参数

配置ipsec策略的名称，选择接口及地址，总部设备角色选择中心节点。选择中心节点设备会下发模板方式的配置。模板方式的总部不需要配置acl，由分支配置acl来跟总部协商自动出保护的数据流。

IKE策略选择野蛮模式，IKE提议选择之前配置的ike，本端ID选择ipv4地址。

注意：本端ID一定要选择ipv4地址

基本配置	
策略名称	zongbu (1-46字符)
优先级	1 (1-65535)
设备角色	<input type="radio"/> 对等/分支节点 <input checked="" type="radio"/> 中心节点
IP地址类型	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
智能选路	<input type="checkbox"/> 开启
接口	GE1/0/0 [配置]
本端地址	172.16.0.1
描述	(1-80字符)

IKE策略	
协商模式	<input type="radio"/> 主模式 <input checked="" type="radio"/> 野蛮模式
预共享密钥	(1-128字符)
再次输入预共享密钥	
PKI域	请选择...
证书访问策略	请选择...
IKE提议	10 (预共享密钥; SHA1; 3DES-CBC; DH group 2) [多选]
本端ID	IPv4 地址 172.16.0.1

Ipsec参数选择esp认证加密算法，其他保持默认。



总部采用模板方式无法指定分支的FQDN，总部默认下发配置  
ike profile zongbu\_IPv4\_1  
keychain zongbu\_IPv4\_1  
exchange-mode aggressive  
local-identity address 172.16.0.1  
match remote identity address 0.0.0.0 0.0.0.0  
match local address GigabitEthernet1/0/0  
proposal 10



分支IKE策略--对端ID必须配置ipv4地址，因为分支要主动发起必须知道总部地址，另外如果分支对端ID配置成策略的ipsec策略配置如下。

《网络》>《IPsec策略》新建，新建相应的ipsec策略等参数

注意本端ID留空对端ID选择ipv4地址



密钥会指定为hostname，会报找不到对应的密钥从而ike都无法建立。

命令行配置如下：

```

总部配置
<zongbu-dis cu
#
version 7.1.064, Alpha 7164
#

```

配置ipsec保护的数据流及ipsec参数

```

#
context Admin id 1
#
telnet server enable
#
irf mac-address persistent timer
irf auto-update enable
undo irf link-delay
irf member 1 priority 1
#
ospf 1

```

```

area 0.0.0.0
network 172.16.0.0 0.0.0.255
#
xbar load-single
password-recovery enable
lpu-type f-series
#
vlan 1
#
interface NULL0
#
interface LoopBack0
ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet1/0/0
port link-mode route
combo enable copper
ip address 172.16.0.1 255.255.255.0
ipsec apply policy zongbu
#
interface GigabitEthernet1/0/1
port link-mode route
combo enable copper
ip address 172.16.2.1 255.255.255.0
#
interface GigabitEthernet1/0/2
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/3
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/4
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/5
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/6
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/7
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/8
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/9
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/10
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/11
port link-mode route
combo enable copper

```

```
#
interface GigabitEthernet1/0/12
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/13
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/14
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/15
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/16
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/17
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/18
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/19
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/20
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/21
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/22
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/23
port link-mode route
combo enable copper
#
security-zone name Local
#
security-zone name Trust
import interface LoopBack0
#
security-zone name DMZ
#
security-zone name Untrust
import interface GigabitEthernet1/0/0
import interface GigabitEthernet1/0/1
#
security-zone name Management
#
scheduler logfile size 16
#
```

```
line class aux
  user-role network-operator
#
line class console
  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 con 0
  authentication-mode scheme
  user-role network-admin
#
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 0 172.16.0.2
#
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$6$UblhNnPevyKUwfpm$LqR3+yg1ljNct39MkOR0H0iQXLkYB3jMqM4vbAeoXOh
babllFnjJPEGR00YIYA1Sz4LiY3FmEdru2fOLMb1shQ==
service-type telnet terminal http
authorization-attribute user-role level-3
authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
#
ipsec transform-set zongbu_IPv4_1
esp encryption-algorithm 3des-cbc
esp authentication-algorithm sha1
#
ipsec policy-template zongbu 1
transform-set zongbu_IPv4_1
local-address 172.16.0.1
ike-profile zongbu_IPv4_1
#
ipsec policy zongbu 1 isakmp template zongbu
#
ike profile zongbu_IPv4_1
keychain zongbu_IPv4_1
exchange-mode aggressive
local-identity address 172.16.0.1
match remote identity address 0.0.0.0 0.0.0.0
match local address GigabitEthernet1/0/0
proposal 10
#
ike proposal 10
encryption-algorithm 3des-cbc
dh group2
#
ike keychain zongbu_IPv4_1
match local address GigabitEthernet1/0/0
pre-shared-key address 0.0.0.0 0.0.0.0 key cipher $c$3$nw8o7ylcjPSdFyAURIYIKXSd/sFIJgEN
#
ip http enable
ip https enable
#
security-policy ip
rule 1 name test
action pass
#
return
<zongbu>

<zongbu>dis ike sa
```

```
Connection-ID Remote      Flag   DOI
-----
9          172.16.1.1    RD     IPsec
```

Flags:

RD--READY RL--REPLACED FD-FADING RK-REKEY

<zongbu>dis ipse

<zongbu>dis ipsec sa

<zongbu>dis ipsec sa

Interface: GigabitEthernet1/0/0

-----  
IPsec policy: zongbu

Sequence number: 1

Mode: Template

-----  
Tunnel id: 0

Encapsulation mode: tunnel

Perfect Forward Secrecy:

Inside VPN:

Extended Sequence Numbers enable: N

Traffic Flow Confidentiality enable: N

Path MTU: 1444

Tunnel:

local address: 172.16.0.1

remote address: 172.16.1.1

Flow:

sour addr: 1.1.1.1/255.255.255.255 port: 0 protocol: ip

dest addr: 2.2.2.2/255.255.255.255 port: 0 protocol: ip

[Inbound ESP SAs]

SPI: 1511053843 (0x5a10da13)

Connection ID: 12884901891

Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1

SA duration (kilobytes/sec): 1843200/3600

SA remaining duration (kilobytes/sec): 1843199/2576

Max received sequence-number: 5

Anti-replay check enable: Y

Anti-replay window size: 64

UDP encapsulation used for NAT traversal: N

Status: Active

[Outbound ESP SAs]

SPI: 3440085931 (0xcd0b8bab)

Connection ID: 12884901890

Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1

SA duration (kilobytes/sec): 1843200/3600

SA remaining duration (kilobytes/sec): 1843199/2576

Max sent sequence-number: 5

UDP encapsulation used for NAT traversal: N

Status: Active

<zongbu>

### 分支配置

<fenzhi>dis cu

#

version 7.1.064, Alpha 7164

#

sysname fenzhi

#

context Admin id 1

#



```
telnet server enable
#
irf mac-address persistent timer
irf auto-update enable
undo irf link-delay
irf member 1 priority 1
#
ospf 1
area 0.0.0.0
network 172.16.1.0 0.0.0.255
#
xbar load-single
password-recovery enable
lpu-type f-series
#
vlan 1
#
interface NULL0
#
interface LoopBack0
ip address 2.2.2.2 255.255.255.255
#
interface GigabitEthernet1/0/0
port link-mode route
combo enable copper
ip address 172.16.1.1 255.255.255.0
ipsec apply policy fenzhi
#
interface GigabitEthernet1/0/1
port link-mode route
combo enable copper
ip address 172.16.2.2 255.255.255.0
#
interface GigabitEthernet1/0/2
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/3
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/4
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/5
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/6
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/7
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/8
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/9
port link-mode route
combo enable copper
```

```
#
interface GigabitEthernet1/0/10
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/11
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/12
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/13
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/14
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/15
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/16
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/17
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/18
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/19
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/20
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/21
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/22
port link-mode route
combo enable copper
#
interface GigabitEthernet1/0/23
port link-mode route
combo enable copper
#
security-zone name Local
#
security-zone name Trust
import interface LoopBack0
#
security-zone name DMZ
#
```

```
security-zone name Untrust
import interface GigabitEthernet1/0/0
import interface GigabitEthernet1/0/1
#
security-zone name Management
#
scheduler logfile size 16
#
line class aux
user-role network-operator
#
line class console
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 con 0
authentication-mode scheme
user-role network-admin
#
line vty 0 4
authentication-mode none
user-role network-admin
#
line vty 5 63
authentication-mode none
user-role network-operator
#
ip route-static 0.0.0.0 0 172.16.1.2
#
acl advanced name IPsec_fenzhi_IPv4_1
rule 1 permit ip source 2.2.2.2 0 destination 1.1.1.1 0
#
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$6$UblhNnPevyKUwfpm$LqR3+yg1IjNct39MkOR0H0iQXLkYB3jMqM4vbAeoXOh
babllFnjJPEGR00YiYA1Sz4LiY3FmEdru2fOLMb1shQ==
service-type telnet terminal http
authorization-attribute user-role level-3
authorization-attribute user-role network-admin
authorization-attribute user-role network-operator
#
ipsec transform-set fenzhi_IPv4_1
esp encryption-algorithm 3des-cbc
esp authentication-algorithm sha1
#
ipsec policy fenzhi 1 isakmp
transform-set fenzhi_IPv4_1
security acl name IPsec_fenzhi_IPv4_1
remote-address 172.16.0.1
ike-profile fenzhi_IPv4_1
#
ike profile fenzhi_IPv4_1
keychain fenzhi_IPv4_1
exchange-mode aggressive
match remote identity address 172.16.0.1 255.255.255.255
match local address GigabitEthernet1/0/0
proposal 10
#
ike proposal 10
encryption-algorithm 3des-cbc
dh group2
#
ike keychain fenzhi_IPv4_1
match local address GigabitEthernet1/0/0
pre-shared-key address 172.16.0.1 255.255.255.255 key cipher $c$3$0D8k6aHsDCIx2d/siPNHdmC
MjeDjWHJR
#
```

```
ip http enable
ip https enable
#
security-policy ip
rule 1 name test
action pass
#
return
<fenzhi>
```

```
<fenzhi>dis ike sa
Connection-ID Remote Flag DOI
-----
37 172.16.0.1 RD IPsec
```

```
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
```

```
<fenzhi>dis ipse
<fenzhi>dis ipsec sa
<fenzhi>dis ipsec sa
```

```
-----
Interface: GigabitEthernet1/0/0
-----
```

```
-----
IPsec policy: fenzhi
Sequence number: 1
Mode: ISAKMP
-----
```

```
Tunnel id: 0
Encapsulation mode: tunnel
Perfect Forward Secrecy:
Inside VPN:
Extended Sequence Numbers enable: N
Traffic Flow Confidentiality enable: N
Path MTU: 1444
Tunnel:
local address: 172.16.1.1
remote address: 172.16.0.1
```

```
Flow:
sour addr: 2.2.2.2/255.255.255.255 port: 0 protocol: ip
dest addr: 1.1.1.1/255.255.255.255 port: 0 protocol: ip
```

```
[Inbound ESP SAs]
```

```
SPI: 3440085931 (0xcd0b8bab)
Connection ID: 12884901891
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/2400
Max received sequence-number: 5
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active
```

```
[Outbound ESP SAs]
```

```
SPI: 1511053843 (0x5a10da13)
Connection ID: 12884901890
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/2400
Max sent sequence-number: 5
UDP encapsulation used for NAT traversal: N
Status: Active
```

