msr36 和迈普国密 ike1.0 互通配置

组网图:

MSR36----------MAIPU1800X

组网需求:

按照反馈的迈普配置 (国密 ike1.0), 使用单签名证书, MSR36 和迈普互通 ipsec.
Msr36 需要配置导入 peer 证书, 并且在 ike-profile 中指定 peer 证书的 sn 序号.
Maipu 侧作为发起方, 应该也需要导入 peer 证书, 指定 peer 证书 set peer-id CN=xxx

迈普配置:

```
interface loopback1
 ip address 2.2.2.2 255.255.255.255
 exit

interface vlan1000
 ip address 55.17.15.243 255.255.0.0

crypto ca identity GDFH
 ca type other
 subject-name CN=r2
  key-type sm2
  exit
 exit

crypto sm2-encryption-encode old
crypto sm2-signature old
crypto sm2 hash-e
crypto cert-usage old

crypto ike proposal ikepro
 encryption sm4
 inte sm3
```

```
 exit

crypto ipsec proposal ipsecpro
 esp sm4-old sm3
 exit

crypto tunnel tunnelsm
 local interface vlan 1000
 peer address 172.32.36.41
 set authentication sm2-de-nc
 set ike proposal ikepro
 set ipsec proposal ipsecpro
 set dpd on-demand 10 10 2
 !!set idletime 30 outbound-only
 !!set auto-up
 exit

crypto policy local1
 flow host 2.2.2.2 host 1.1.1.1 ip ipv4-tunnel tunnelsm
 set reverse-route
 exit

ip route 0.0.0.0 0.0.0.0 55.17.15.254
```

MSR36 配置:

```
#
pki domain 1
 public-key sm2 signature name 1
 undo crl check enable
#
acl number 3001
 rule 0 permit ip source 1.1.1.1 0 destination 2.2.2.2 0
#
ipsec transform-set 1
 esp encryption-algorithm sm4-cbc
 esp authentication-algorithm sm3
#
ipsec policy 1 10 isakmp
 transform-set 1
 security acl 3001
```

```
 remote-address 55.17.15.243
 ike-profile 1
#
ike profile 1
 certificate domain 1
 exchange-mode gm-main
 local-identity dn
 match remote identity address 0.0.0.0 0.0.0.0
 proposal 1
 ike gm-main ike-version 1.0
 remote-certificate serial 71
#
ike proposal 1
 authentication-method sm2-de
 encryption-algorithm sm4-cbc
 authentication-algorithm sm3
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 172.32.36.41 255.255.0.0
 ipsec apply policy 1
#
 ip route-static 2.2.2.2 32 172.32.254.254
 ip route-static 55.17.0.0 16 172.32.254.254
```

准备证书文件:

按照前方反馈，准备签名用途的单证书

testca_r1sig_r2sig.zip

```
D:\gmssl\test4\output>gmssl x509 -noout -text -in r1sig.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 111 (0x6f)
    Signature Algorithm: sm2sign-with-sm3
```

```
        Issuer: CN = testca
        Validity
            Not Before: Jun  5 08:20:22 2025 GMT
            Not After : Jun  3 08:20:22 2035 GMT
        Subject: CN = r1
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:89:95:21:44:85:25:d1:45:77:00:ba:f7:2e:69:
                    5f:35:68:0b:37:89:61:9a:24:e1:77:85:04:62:8e:
                    6c:83:6f:7d:89:fa:4e:1c:89:dd:55:c8:ee:ae:b5:
                    4c:bf:4e:05:20:ee:5a:fb:50:e3:fd:b7:cc:9a:60:
                    48:13:34:4b:ad
                ASN1 OID: sm2p256v1
                NIST CURVE: SM2
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Non Repudiation
    Signature Algorithm: sm2sign-with-sm3
         30:44:02:20:59:13:9c:95:df:df:90:dc:36:14:b1:7d:1b:0f:
         f7:de:4e:7e:05:5d:93:c3:8d:5a:ad:b0:fb:9e:cb:7d:82:41:
         02:20:5b:1f:a0:87:f1:a6:96:07:9c:54:e0:77:6b:e6:b5:fc:
         44:2c:53:14:7c:c6:ea:b0:80:97:02:29:b3:0a:99:c8


D:\gmssl\test4\output>gmssl x509 -noout -text -in r2sig.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 113 (0x71)
    Signature Algorithm: sm2sign-with-sm3
        Issuer: CN = testca
        Validity
            Not Before: Jun  5 08:54:59 2025 GMT
            Not After : Jun  3 08:54:59 2035 GMT
        Subject: CN = r2
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:4f:70:bb:45:d0:68:97:4e:3e:0e:e0:e3:58:2f:
```

```
                    3e:c3:17:e1:90:2e:1f:65:94:07:e3:d8:f5:47:22:
                    03:d5:58:eb:52:23:9e:8c:74:b9:c7:9b:4a:73:18:
                    a9:d9:fe:63:e4:e3:5f:9d:48:a5:d8:5e:a2:eb:35:
                    16:13:13:0f:21
                ASN1 OID: sm2p256v1
                NIST CURVE: SM2
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Non Repudiation
    Signature Algorithm: sm2sign-with-sm3
        30:45:02:21:00:ef:53:fa:1b:74:87:e8:1a:ba:75:3f:e6:09:
        9e:8d:9d:73:63:f1:a8:46:4e:26:65:b9:89:c8:dd:55:a1:34:
        2e:02:20:04:64:d0:44:23:4c:ba:78:28:ca:58:f6:57:fb:06:
        39:e7:6e:22:fd:70:a8:d2:31:aa:30:ba:6d:60:3e:39:1e

D:\gmssl\test4\output>
```

MSR36 导入证书:

```
[3620x1]disp clock
09:29:07 bj Mon 06/09/2025
Time Zone : bj add 08:00:00
[3620x1]pki import domain 1 pem local
Enter PEM-formatted certificates.
End with a Ctrl+C on a line by itself.
r1sig.crt


-----BEGIN CERTIFICATE-----
MIIBJTCBzaADAgECAgFvMAoGCCqBHM9VAYN1MBExDzANBgNVBAMMBnRlc3RjYT
Ae
Fw0yNTA2MDUwODIwMjJaFw0zNTA2MDMwODIwMjJaMA0xCzAJBgNVBAMMAnIxMF
kw
EwYHKoZIzj0CAQYIKoEcz1UBgi0DQgAEiZUhRIUl0UV3ALr3LmlfNWgLN4lhmiTh
d4UEYo5sg299ifpOHIndVcjurrVMv04FIO5a+1Dj/bfMmmBIEzRLraMaMBgwCQYD
VR0TBAIwADALBgNVHQ8EBAMCBsAwCgYIKoEcz1UBg3UDRwAwRAIgWROcld/fkNw
2
FLF9Gw/33k5+BV2Tw41arbD7nst9gkECIFsfoIfxppYHnFTgd2vmtfxELFMUfMbq
sICXAimzCpnI
```

-----END CERTIFICATE-----

r1sig.key

ASN1 OID: sm2p256v1
NIST CURVE: SM2
-----BEGIN EC PARAMETERS-----
BggqgRzPVQGCLQ==
-----END EC PARAMETERS-----
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIDp6oY4SSZfP9ezcB8DiR34QPsaat4Q7DiYosBlwrpl7oAoGCCqBHM9V
AYItoUQDQgAEiZUhRIUl0UV3ALr3LmlfNWgLN4lhmiThd4UEYo5sg299ifpOHInd
VcjurrVMv04FIO5a+1Dj/bfMmmBIEzRLrQ==
-----END EC PRIVATE KEY-----

testca.crt

-----BEGIN CERTIFICATE-----
MIIBETCBuAIJAP81IXZFD76JMAoGCCqBHM9VAYN1MBExDzANBgNVBAMMBnRlc3Rj
YTAeFw0yNTA2MDQxMTIxMzdaFw0yNjA2MDQxMTIxMzdaMBExDzANBgNVBAMMBn
Rl
c3RjYTBZMBMGByqGSM49AgEGCCqBHM9VAYItA0IABFXG/PpNyw7T1K2v+edlYzwR
13hrToIw7+n260Lnwb5xofx6JOQGHv1sZ8EtbdT4SjLAe9stP+yi9ed1ufxOMmkw
CgYIKoEcz1UBg3UDSAAwRQIgOV4+tYcggLA7C/oLDZ7XVKykyEllT6itcTmoKZgB
aCgCIQCUhKQ7IVGdmC4XkjA48M1da9bgEKfolW+8Mauix1N+9w==
-----END CERTIFICATE-----

The trusted CA's finger print is:
    MD5   fingerprint:1E64 6F55 6967 BCE0 5D25 6B95 6332 42DA
    SHA1 fingerprint:02BE 2FE0 EC15 F01D D234 4CF7 BB1C 0A29 4712 D824
Is the finger print correct?(Y/N):y
[3620x1]
[3620x1]pki import domain 1 pem peer
Enter PEM-formatted certificates.
End with a Ctrl+C on a line by itself.
-----BEGIN CERTIFICATE-----
MIIBJjCBzaADAgECAgFxMAoGCCqBHM9VAYN1MBExDzANBgNVBAMMBnRlc3RjYTA
e
Fw0yNTA2MDUwODU0NTlaFw0zNTA2MDMwODU0NTlaMA0xCzAJBgNVBAMMAnIyM
Fkw
EwYHKoZIzj0CAQYIKoEcz1UBgi0DQgAET3C7RdBol04+DuDjWC8+wxfhkC4fZZQH
49j1RyID1VjrUiOejHS5x5tKcxip2f5j5ONfnUil2F6i6zUWExMPIaMaMBgwCQYD

VR0TBAIwADALBgNVHQ8EBAMCBsAwCgYIKoEcz1UBg3UDSAAwRQIhAO9T+ht0h+ga
unU/5gmejZ1zY/GoRk4mZbmJyN1VoTQuAiAEZNBEI0y6eCjKWPZX+wY5524i/XCo
0jGqMLptYD45Hg==
-----END CERTIFICATE-----

[3620x1]
[3620x1]disp pki certificate domain 1 local
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 111 (0x6f)
        Signature Algorithm: sm3WithSM2Sign
        Issuer: CN=testca
        Validity
            Not Before: Jun 5 08:20:22 2025 GMT
            Not After : Jun 3 08:20:22 2035 GMT
        Subject: CN=r1
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:89:95:21:44:85:25:d1:45:77:00:ba:f7:2e:69:
                    5f:35:68:0b:37:89:61:9a:24:e1:77:85:04:62:8e:
                    6c:83:6f:7d:89:fa:4e:1c:89:dd:55:c8:ee:ae:b5:
                    4c:bf:4e:05:20:ee:5a:fb:50:e3:fd:b7:cc:9a:60:
                    48:13:34:4b:ad
                ASN1 OID: SM2
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage:
                Digital Signature, Non Repudiation
    Signature Algorithm: sm3WithSM2Sign
         30:44:02:20:59:13:9c:95:df:df:90:dc:36:14:b1:7d:1b:0f:
         f7:de:4e:7e:05:5d:93:c3:8d:5a:ad:b0:fb:9e:cb:7d:82:41:
         02:20:5b:1f:a0:87:f1:a6:96:07:9c:54:e0:77:6b:e6:b5:fc:
         44:2c:53:14:7c:c6:ea:b0:80:97:02:29:b3:0a:99:c8

[3620x1]
[3620x1]disp pki certificate domain 1 peer
Total peer certificates: 1

Serial Number: 71
Subject Name: CN=r2

[3620x1]
[3620x1]

MP1800X 导入证书:

mp1800x55(config)#crypto ca import certificate to GDFH
% Input the certificate data, press <Enter> twice to finish:
-----BEGIN CERTIFICATE-----
MIIBETCBuAIJAP81IXZFD76JMAoGCCqBHM9VAYN1MBExDzANBgNVBAMMBnRlc3Rj
YTAeFw0yNTA2MDQxMTIxMzdaFw0yNjA2MDQxMTIxMzdaMBExDzANBgNVBAMMBn
Rl
c3RjYTBZMBMGByqGSM49AgEGCCqBHM9VAYItA0IABFXG/PpNyw7T1K2v+edlYzwR
13hrToIw7+n260Lnwb5xofx6JOQGHv1sZ8EtbdT4SjLAe9stP+yi9ed1ufxOMmkw
CgYIKoEcz1UBg3UDSAAwRQIgOV4+tYcggLA7C/oLDZ7XVKykyEllT6itcTmoKZgB
aCgCIQCUhKQ7IVGdmC4XkjA48M1da9bgEKfolW+8Mauix1N+9w==
-----END CERTIFICATE-----

% Input the private key data, press <Enter> twice after data to finish or press <Enter> without data to ignore:

% The Root CA Certificate has the following attributes:
  Serial Number: ff352176450fbe89
  Subject: CN=testca
  Issuer : CN=testca
  Validity
    Start date: 2025-06-04 11:21:37
    End   date: 2026-06-04 11:21:37
  Usage: General

Fingerprint(sm3) :e88544b261ecfebfac63e87ea5228e1514699d53e90efabf3cd775da34d1c616
  Fingerprint(sha1):02be2fe0ec15f01dd2344cf7bb1c0a294712d824

% Do you accept this root ca-certificate[yes]/[no]:yes
% PKI: Import Certificate success.
mp1800x55(config)#

mp1800x55(config)#crypto ca import certificate to GDFH
% Input the certificate data, press <Enter> twice to finish:
-----BEGIN CERTIFICATE-----
MIIBJjCBzaADAgECAgFxMAoGCCqBHM9VAYN1MBExDzANBgNVBAMMBnRlc3RjYTA
e
Fw0yNTA2MDUwODU0NTlaFw0zNTA2MDMwODU0NTlaMA0xCzAJBgNVBAMMAnIyM
Fkw
EwYHKoZIzj0CAQYIKoEcz1UBgi0DQgAET3C7RdBol04+DuDjWC8+wxfhkC4fZZQH
49j1RyID1VjrUiOejHS5x5tKcxip2f5j5ONfnUil2F6i6zUWExMPIaMaMBgwCQYD
VR0TBAIwADALBgNVHQ8EBAMCBsAwCgYIKoEcz1UBg3UDSAAwRQIhAO9T+ht0h+ga
unU/5gmejZ1zY/GoRk4mZbmJyN1VoTQuAiAEZNBEI0y6eCjKWPZX+wY5524i/XCo
0jGqMLptYD45Hg==
-----END CERTIFICATE-----

% Input the private key data, press <Enter> twice after data to finish or press <Enter> without data to ignore:
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIGzHdWWhv7mrRGwkGLXjBFqrteEYBmmXlWejLdeltJr8oAoGCCqBHM9V
AYItoUQDQgAET3C7RdBol04+DuDjWC8+wxfhkC4fZZQH49j1RyID1VjrUiOejHS5
x5tKcxip2f5j5ONfnUil2F6i6zUWExMPIQ==
-----END EC PRIVATE KEY-----

% PKI: Import Certificate success.
mp1800x55(config)#
mp1800x55(config)#

MSR36 发起协商建立成功:

<3620x1>debug
<3620x1>debugging ike al
<3620x1>debugging ike all
This command is CPU intensive and might affect ongoing services. Are you sure you want to continue? [Y/N]:y
<3620x1>t d
The current terminal is enabled to display debugging logs.
<3620x1>t m
The current terminal is enabled to display logs.

<3620x1>ping -c 1 -a 1.1.1.1 2.2.2.2 ?
  <cr>

<3620x1>ping -c 1 -a 1.1.1.1 2.2.2.2
Ping 2.2.2.2 (2.2.2.2) from 1.1.1.1: 56 data bytes, press CTRL_C to break
*Jun 9 09:35:32:965 2025 3620x1 IKE/7/EVENT: Received message from ipsec, message type is 0.
*Jun 9 09:35:32:965 2025 3620x1 IKE/7/EVENT: Received SA acquire message from IPsec.
*Jun 9 09:35:32:965 2025 3620x1 IKE/7/EVENT: IKE thread 1099127030448 processes a job.
*Jun 9 09:35:32:965 2025 3620x1 IKE/7/EVENT: Received SA acquire message from IPsec.
*Jun 9 09:35:32:965 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Set IPsec SA state to IKE_P2_STATE_INIT.
*Jun 9 09:35:32:965 2025 3620x1 IKE/7/EVENT: IKE SA not found. Initiate IKE SA negotiation.
*Jun 9 09:35:32:966 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Obtained profile 1.
*Jun 9 09:35:32:966 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Initiator created an SA for peer 55.17.15.243, local port 500, remote port 500.
*Jun 9 09:35:32:966 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Set IKE SA state to IKE_P1_STATE_INIT.
*Jun 9 09:35:32:966 2025 3620x1 IKE/7/EVENT: IKE thread 1099127030448 processes a job.
*Jun 9 09:35:32:966 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Begin Main mode exchange.
*Jun 9 09:35:32:966 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Pre-shared key matching address 55.17.15.243 not found.
*Jun 9 09:35:32:966 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
  Encryption algorithm is SM4-CBC.
*Jun 9 09:35:32:966 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
  Hash algorithm is HMAC-SM3.
*Jun 9 09:35:32:966 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
  Authentication method is Digital envelope.

*Jun 9 09:35:32:966 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
  Asymmetric public key algorithm is sm2.
*Jun 9 09:35:32:966 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
  Lifetime type is in seconds.
*Jun 9 09:35:32:966 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
  Life duration is 86400.
*Jun 9 09:35:32:966 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Construct transform payload for transform 1.
*Jun 9 09:35:32:966 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Constructed SA payload.
*Jun 9 09:35:32:966 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Construct NAT-T rfc3947 vendor ID payload.
*Jun 9 09:35:32:967 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Construct NAT-T draft3 vendor ID payload.
*Jun 9 09:35:32:967 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Construct NAT-T draft2 vendor ID payload.
*Jun 9 09:35:32:967 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Construct NAT-T draft1 vendor ID payload.
*Jun 9 09:35:32:967 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
IKE SA state changed from IKE_P1_STATE_INIT to IKE_P1_STATE_SEND1.
*Jun 9 09:35:32:967 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Sending packet to 55.17.15.243 remote port 500, local port 500, out-interface 0.
*Jun 9 09:35:32:967 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500

  I-Cookie: d452a4562a294fba
  R-Cookie: 0000000000000000
  next payload: SA
  version: ISAKMP Version 1.0
  exchange mode: Main
  flags:
  message ID: 0
  length: 164

*Jun 9 09:35:32:967 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Sending an IPv4 packet.
*Jun 9 09:35:32:967 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Send udp packet by socket 46 SrcPort 500 ifIndex 0.
*Jun 9 09:35:32:967 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Sent data to socket successfully.
*Jun 9 09:35:32:968 2025 3620x1 IKE/7/EVENT: Received packet successfully.
*Jun 9 09:35:32:968 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Received packet from 55.17.15.243 source port 500 destination port 500.
*Jun 9 09:35:32:968 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500

  I-Cookie: d452a4562a294fba
  R-Cookie: f35e37a46244f13e
  next payload: SA
  version: ISAKMP Version 1.0
  exchange mode: Main
  flags:
  message ID: 0
  length: 124
*Jun 9 09:35:32:969 2025 3620x1 IKE/7/EVENT: IKE thread 1099127030448 processes a job.
*Jun 9 09:35:32:969 2025 3620x1 IKE/7/EVENT: Phase1 process started.
*Jun 9 09:35:32:969 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Received ISAKMP Security Association Payload.
*Jun 9 09:35:32:969 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Received ISAKMP Vendor ID Payload.
*Jun 9 09:35:32:969 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Received ISAKMP Vendor ID Payload.
*Jun 9 09:35:32:969 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Process SA payload.
*Jun 9 09:35:32:969 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Check ISAKMP transform 1.
*Jun 9 09:35:32:969 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500

Encryption algorithm is SM4-CBC.
*Jun 9 09:35:32:969 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
HASH algorithm is HMAC-SM3.
*Jun 9 09:35:32:969 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Authentication method is Digital envelope.
*Jun 9 09:35:32:969 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Asymmetric public key algorithm is sm2.
*Jun 9 09:35:32:969 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Lifetime type is 1.
*Jun 9 09:35:32:969 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Life duration is 86400.
*Jun 9 09:35:32:969 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Attributes is acceptable.
*Jun 9 09:35:32:969 2025 3620x1 IKE/7/EVENT: Oakley transform 1 is acceptable.
*Jun 9 09:35:32:978 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Process vendor ID payload.
*Jun 9 09:35:32:978 2025 3620x1 IKE/7/EVENT: Vendor ID DPD is matched.
*Jun 9 09:35:32:978 2025 3620x1 IKE/7/EVENT: Vendor ID NAT-T rfc3947 is matched.
*Jun 9 09:35:33:003 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Constructed SK payload.
*Jun 9 09:35:33:003 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Constructed Nonce payload.
*Jun 9 09:35:33:004 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Local ID type: DER_ASN1_DN (9).
*Jun 9 09:35:33:005 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Local ID value: DN.
*Jun 9 09:35:33:005 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Constructed ID payload.
*Jun 9 09:35:33:025 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Constructed signature payload by private key.
*Jun 9 09:35:33:025 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote

= 55.17.15.243/500
Construct NAT-D payload.
*Jun 9 09:35:33:025 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Construct DPD vendor ID payload.
*Jun 9 09:35:33:025 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
IKE SA state changed from IKE_P1_STATE_SEND1 to IKE_P1_STATE_SEND3.
*Jun 9 09:35:33:025 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Sending packet to 55.17.15.243 remote port 500, local port 500, out-interface 0.
*Jun 9 09:35:33:025 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500

  I-Cookie: d452a4562a294fba
  R-Cookie: f35e37a46244f13e
  next payload: SK
  version: ISAKMP Version 1.0
  exchange mode: Main
  flags:
  message ID: 0
  length: 692
*Jun 9 09:35:33:026 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Sending an IPv4 packet.
*Jun 9 09:35:33:026 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Send udp packet by socket 46 SrcPort 500 ifIndex 0.
*Jun 9 09:35:33:026 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Sent data to socket successfully.
*Jun 9 09:35:33:098 2025 3620x1 IKE/7/EVENT: Received packet successfully.
*Jun 9 09:35:33:098 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Received packet from 55.17.15.243 source port 500 destination port 500.
*Jun 9 09:35:33:098 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500

  I-Cookie: d452a4562a294fba
  R-Cookie: f35e37a46244f13e
  next payload: SK
  version: ISAKMP Version 1.0
  exchange mode: Main
  flags:

message ID: 0
length: 368
*Jun 9 09:35:33:098 2025 3620x1 IKE/7/EVENT: IKE thread 1099127030448 processes a job.
*Jun 9 09:35:33:098 2025 3620x1 IKE/7/EVENT: Phase1 process started.
*Jun 9 09:35:33:098 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Received ISAKMP SK Payload.
*Jun 9 09:35:33:099 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Received ISAKMP Nonce Payload.
*Jun 9 09:35:33:099 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Received ISAKMP Identification Payload.
*Jun 9 09:35:33:099 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Received ISAKMP Signature Payload.
*Jun 9 09:35:33:099 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Received ISAKMP NAT-D Payload.
*Jun 9 09:35:33:099 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Received ISAKMP NAT-D Payload.
*Jun 9 09:35:33:099 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Started to process SK payload.
*Jun 9 09:35:33:122 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Decrypted SK with local private key successfully.
*Jun 9 09:35:33:122 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Started to process NONCE payload.
*Jun 9 09:35:33:122 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Decrypted nonce payload successfully.
*Jun 9 09:35:33:122 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Started to process ID payload.
*Jun 9 09:35:33:122 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Peer ID type: DER_ASN1_DN (9).
*Jun 9 09:35:33:123 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Peer ID value: DN CN=r2

*Jun 9 09:35:33:123 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Update the profile 1 with Remote identity.
*Jun 9 09:35:33:123 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Started to verify signature payload.
*Jun 9 09:35:33:136 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Signature verification succeeded.
*Jun 9 09:35:33:136 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Received 2 NAT-D payload.
*Jun 9 09:35:33:137 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Nonce Hash:
 95c79240 bc2db828 0160da8b 0a44bbe2 72219010 ea9033e5 97aceac9 13f85057
*Jun 9 09:35:33:137 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
HASH:
 d93e4b15 d5fd6ef9 447a1fe9 9c084825 ac125618 8c122093 99b743a8 e0de4eb1
*Jun 9 09:35:33:137 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Constructed Hash payload.
*Jun 9 09:35:33:137 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Encrypt the packet.
*Jun 9 09:35:33:137 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
IKE SA state changed from IKE_P1_STATE_SEND3 to IKE_P1_STATE_SEND5.
*Jun 9 09:35:33:137 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Sending packet to 55.17.15.243 remote port 500, local port 500, out-interface 0.
*Jun 9 09:35:33:137 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500

  I-Cookie: d452a4562a294fba
  R-Cookie: f35e37a46244f13e
  next payload: HASH
  version: ISAKMP Version 1.0
  exchange mode: Main
  flags: ENCRYPT
  message ID: 0
  length: 76
*Jun 9 09:35:33:138 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote

= 55.17.15.243/500
Sending an IPv4 packet.
*Jun 9 09:35:33:138 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Send udp packet by socket 46 SrcPort 500 ifIndex 0.
*Jun 9 09:35:33:138 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Sent data to socket successfully.
*Jun 9 09:35:33:139 2025 3620x1 IKE/7/EVENT: Received packet successfully.
*Jun 9 09:35:33:139 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Received packet from 55.17.15.243 source port 500 destination port 500.
*Jun 9 09:35:33:139 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500

  I-Cookie: d452a4562a294fba
  R-Cookie: f35e37a46244f13e
  next payload: HASH
  version: ISAKMP Version 1.0
  exchange mode: Main
  flags: ENCRYPT
  message ID: 0
  length: 76
*Jun 9 09:35:33:139 2025 3620x1 IKE/7/EVENT: IKE thread 1099127030448 processes a job.
*Jun 9 09:35:33:139 2025 3620x1 IKE/7/EVENT: Phase1 process started.
*Jun 9 09:35:33:139 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Decrypt the packet.
*Jun 9 09:35:33:140 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Received ISAKMP Hash Payload.
*Jun 9 09:35:33:140 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Started to process HASH payload.
*Jun 9 09:35:33:140 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
HASH:
 19f6fae0 c19714e5 c78ee123 62ded9be 65a2f2e6 c5c91bfa 919073b1 3b9ce36c
*Jun 9 09:35:33:140 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
HASH verification succeeded.
*Jun 9 09:35:33:140 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500

IKE SA state changed from IKE_P1_STATE_SEND5 to IKE_P1_STATE_ESTABLISHED.
*Jun 9 09:35:33:140 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
The default soft lifetime 77760(seconds) was used for the IKE P1 SA.
*Jun 9 09:35:33:140 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Add tunnel, alloc new tunnel with ID [1].
*Jun 9 09:35:33:141 2025 3620x1 IKE/7/EVENT: IKE thread 1099127030448 processes a job.
*Jun 9 09:35:33:141 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Begin Quick mode exchange.
*Jun 9 09:35:33:141 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
IPsec SA state changed from IKE_P2_STATE_INIT to IKE_P2_STATE_GETSPI.
*Jun 9 09:35:33:141 2025 3620x1 IKE/7/EVENT: Received message from ipsec, message type is 9.
*Jun 9 09:35:33:141 2025 3620x1 IKE/7/EVENT: IKE thread 1099127030448 processes a job.
*Jun 9 09:35:33:142 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Set attributes according to phase 2 transform.
*Jun 9 09:35:33:142 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Encapsulation mode is Tunnel.
*Jun 9 09:35:33:142 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
in seconds
*Jun 9 09:35:33:142 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Life duration is 3600.
*Jun 9 09:35:33:142 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
in kilobytes
*Jun 9 09:35:33:142 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Life duration is 1843200.
*Jun 9 09:35:33:142 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Authentication algorithm is HMAC-SM3.
*Jun 9 09:35:33:142 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Transform ID is SM4-CBC.
*Jun 9 09:35:33:142 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote

= 55.17.15.243/500
Construct transform 1.
*Jun 9 09:35:33:142 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Construct IPsec proposal 1.
*Jun 9 09:35:33:142 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Construct IPsec SA payload.
*Jun 9 09:35:33:143 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Construct NONCE payload.
*Jun 9 09:35:33:143 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Construct IPsec ID payload.
*Jun 9 09:35:33:143 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Construct IPsec ID payload.
*Jun 9 09:35:33:143 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Construct HASH(1) payload.
*Jun 9 09:35:33:143 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Encrypt the packet.
*Jun 9 09:35:33:143 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
IPsec SA state changed from IKE_P2_STATE_GETSPI to IKE_P2_STATE_SEND1.
*Jun 9 09:35:33:143 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Sending packet to 55.17.15.243 remote port 500, local port 500, out-interface 0.
*Jun 9 09:35:33:143 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500

  I-Cookie: d452a4562a294fba
  R-Cookie: f35e37a46244f13e
  next payload: HASH
  version: ISAKMP Version 1.0
  exchange mode: Quick
  flags: ENCRYPT
  message ID: 6e28ded7
  length: 172
*Jun 9 09:35:33:143 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Sending an IPv4 packet.
*Jun 9 09:35:33:143 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote =

55.17.15.243/500
Send udp packet by socket 46 SrcPort 500 ifIndex 0.
*Jun 9 09:35:33:144 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Sent data to socket successfully.
*Jun 9 09:35:33:145 2025 3620x1 IKE/7/EVENT: Received packet successfully.
*Jun 9 09:35:33:145 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Received packet from 55.17.15.243 source port 500 destination port 500.
*Jun 9 09:35:33:145 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500

  I-Cookie: d452a4562a294fba
  R-Cookie: f35e37a46244f13e
  next payload: HASH
  version: ISAKMP Version 1.0
  exchange mode: Quick
  flags: ENCRYPT
  message ID: 6e28ded7
  length: 172
*Jun 9 09:35:33:145 2025 3620x1 IKE/7/EVENT: IKE thread 1099127030448 processes a job.
*Jun 9 09:35:33:145 2025 3620x1 IKE/7/EVENT: Phase2 process started.
*Jun 9 09:35:33:145 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Decrypt the packet.
*Jun 9 09:35:33:146 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Received ISAKMP Hash Payload.
*Jun 9 09:35:33:146 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Received ISAKMP Security Association Payload.
*Jun 9 09:35:33:146 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Received ISAKMP Nonce Payload.
*Jun 9 09:35:33:146 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Received ISAKMP Identification Payload (IPsec DOI).
*Jun 9 09:35:33:146 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Received ISAKMP Identification Payload (IPsec DOI).
*Jun 9 09:35:33:146 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Process HASH payload.

*Jun 9 09:35:33:146 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Validated HASH(2) successfully.
*Jun 9 09:35:33:146 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Process IPsec SA payload.
*Jun 9 09:35:33:146 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Check IPsec proposal 1.
*Jun 9 09:35:33:147 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Parse transform 1.
*Jun 9 09:35:33:147 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
  Encapsulation mode is Tunnel.
*Jun 9 09:35:33:147 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
  Lifetime type is in seconds.
*Jun 9 09:35:33:147 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
  Life duration is 3600.
*Jun 9 09:35:33:147 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
  Lifetime type is in kilobytes.
*Jun 9 09:35:33:147 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
  Life duration is 1843200.
*Jun 9 09:35:33:147 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
  Authentication algorithm is HMAC-SM3.
*Jun 9 09:35:33:147 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
  Transform ID is SM4-CBC (127).
*Jun 9 09:35:33:147 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
The proposal is acceptable.
*Jun 9 09:35:33:147 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Process Initiator IPsec IDci payload.
*Jun 9 09:35:33:147 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Process Initiator IPsec IDcr payload.
*Jun 9 09:35:33:148 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500

Install IPsec SAs.
*Jun 9 09:35:33:148 2025 3620x1 IKE/7/EVENT: Inbound flow: 2.2.2.2/32->1.1.1.1/32
*Jun 9 09:35:33:148 2025 3620x1 IKE/7/EVENT: Outbound flow: 1.1.1.1/32->2.2.2.2/32
*Jun 9 09:35:33:148 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Lifetime in seconds: 3600
*Jun 9 09:35:33:148 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Lifetime in kilobytes: 1843200
*Jun 9 09:35:33:148 2025 3620x1 IKE/7/EVENT:
Protocol: 50
Inbound SPI: 0xd4f3b0e5
Outbound SPI: 0x3e017472
*Jun 9 09:35:33:149 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
IPsec SA state changed from IKE_P2_STATE_SEND1 to IKE_P2_STATE_SA_CREATED.
*Jun 9 09:35:33:149 2025 3620x1 IKE/7/EVENT: Received message from ipsec, message type is 11.
*Jun 9 09:35:33:149 2025 3620x1 IKE/7/EVENT: IKE thread 1099127030448 processes a job.
*Jun 9 09:35:33:149 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Construct HASH(3) payload.
*Jun 9 09:35:33:149 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Encrypt the packet.
*Jun 9 09:35:33:151 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
IPsec SA state changed from IKE_P2_STATE_SA_CREATED to IKE_P2_STATE_SA_SWITCH.
*Jun 9 09:35:33:151 2025 3620x1 IKE/7/EVENT: Received message from ipsec, message type is 15.
*Jun 9 09:35:33:151 2025 3620x1 IKE/7/EVENT: IKE thread 1099127030448 processes a job.
*Jun 9 09:35:33:151 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
IPsec SA state changed from IKE_P2_STATE_SA_SWITCH to IKE_P2_STATE_ESTABLISHED.
*Jun 9 09:35:33:151 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Sending packet to 55.17.15.243 remote port 500, local port 500, out-interface 0.
*Jun 9 09:35:33:151 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote

= 55.17.15.243/500

I-Cookie: d452a4562a294fba
R-Cookie: f35e37a46244f13e
next payload: HASH
version: ISAKMP Version 1.0
exchange mode: Quick
flags: ENCRYPT
message ID: 6e28ded7
length: 76
*Jun 9 09:35:33:151 2025 3620x1 IKE/7/PACKET: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Sending an IPv4 packet.
*Jun 9 09:35:33:151 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Send udp packet by socket 46 SrcPort 500 ifIndex 0.
*Jun 9 09:35:33:152 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Sent data to socket successfully.
*Jun 9 09:35:33:152 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Got time-based lifetime settings for IKE P2 SA:
Role : Initiator.
Configured soft lifetime buffer : 0 seconds.
Hard lifetime after negotiation : 3600 seconds.
Default soft lifetime : 2700 seconds.
Actual soft lifetime : 2700 seconds.
*Jun 9 09:35:33:152 2025 3620x1 IKE/7/EVENT: vrf = 0, local = 172.32.36.41, remote = 55.17.15.243/500
Add P2 SA to triple successfully.
Request time out

--- Ping statistics for 2.2.2.2 ---
1 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
<3620x1>%Jun 9 09:35:35:168 2025 3620x1 PING/6/PING_STATISTICS: Ping statistics for 2.2.2.2: 1 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss.

<3620x1>ping -c 1 -a 1.1.1.1 2.2.2.2
Ping 2.2.2.2 (2.2.2.2) from 1.1.1.1: 56 data bytes, press CTRL_C to break
56 bytes from 2.2.2.2: icmp_seq=0 ttl=255 time=1.055 ms

--- Ping statistics for 2.2.2.2 ---
1 packet(s) transmitted, 1 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.055/1.055/1.055/0.000 ms

<3620x1>%Jun 9 09:35:36:089 2025 3620x1 PING/6/PING_STATISTICS: Ping statistics for 2.2.2.2: 1 packet(s) transmitted, 1 packet(s) received, 0.0% packet loss, round-trip min/avg/max/std-dev = 1.055/1.055/1.055/0.000 ms.

<3620x1>
<3620x1>disp ike sa

Connection-ID	Local	Remote	Flag	DOI
4	172.32.36.41	55.17.15.243/500	RD	IPsec

Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY
<3620x1>disp ike sa v

Connection ID: 4
Outside VPN:
Inside VPN:
Profile: 1
Transmitting entity: Initiator
Initiator cookie: d452a4562a294fba
Responder cookie: f35e37a46244f13e
Output interface name:

Local IP/port: 172.32.36.41/500
Local ID type: DER_ASN1_DN
Local ID: CN=r1

Remote IP/port: 55.17.15.243/500
Remote ID type: DER_ASN1_DN
Remote ID: CN=r2

Authentication-method: SM2-DE
Authentication-algorithm: SM3
Encryption-algorithm: SM4-CBC

Life duration(sec): 86400
Remaining key duration(sec): 86393
Exchange-mode: GM-main
Diffie-Hellman group:
NAT traversal: Not detected

Extend authentication: Disabled
Assigned IP address:
Vendor ID index: 0xffffffff
Vendor ID sequence number: 0x0

```
<3620x1>disp ipsec sa
-------------------------------
Interface: GigabitEthernet0/0
-------------------------------

  -----------------------------
  IPsec policy: 1
  Sequence number: 10
  Alias: 1-10
  Mode: ISAKMP
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Transmitting entity: Initiator
    Path MTU: 1428
    Tunnel:
        local    address/port: 172.32.36.41/500
        remote address/port: 55.17.15.243/500
    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: 3572740325 (0xd4f3b0e5)
      Connection ID: 115964116994
      Transform set: ESP-ENCRYPT-SM4-CBC ESP-AUTH-SM3
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3593
      Max received sequence-number: 2
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: Active

    [Outbound ESP SAs]
      SPI: 1040282738 (0x3e017472)
      Connection ID: 107374182403
      Transform set: ESP-ENCRYPT-SM4-CBC ESP-AUTH-SM3
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/3593
```

Max sent sequence-number: 1
UDP encapsulation used for NAT traversal: N
Status: Active
<3620x1>

MSR36 作为发起方协商一次后，迈普侧可以看到 peer 证书: (和导入 peer 证书差不多)
mp1800x55#show crypto ca certificates
Root CA Certificate:
Status: Valid
Serial Number: ff352176450fbe89
Subject: CN=testca
Issuer : CN=testca
Validity
Start date: 2025-06-04 11:21:37
End date: 2026-06-04 11:21:37
Key Type: SM2(256 bit)
Usage: General

Fingerprint(sm3):e88544b261ecfebfac63e87ea5228e1514699d53e90efabf3cd775da34d1c616
Fingerprint(sha1):02be2fe0ec15f01dd2344cf7bb1c0a294712d824
Associated Identity: GDFH
index: 3

My Certificate:
Status: Valid
Serial Number: 71
Subject: CN=r2
Issuer : CN=testca
Validity
Start date: 2025-06-05 08:54:59
End date: 2035-06-03 08:54:59
Key Type: SM2(256 bit)
Usage: Sign

Fingerprint(sm3):3a47bf29a170ebdac468cfa849c1d4c74c20c0a4d818ad5dc706d7ffc5b3e66a
Fingerprint(sha1):bf5cb989da8b2d7b2bd7d92982963ea5d77c5802
Associated Identity: GDFH
index: 4

Remote Certificate:
    Status: Valid
    Serial Number: 6f
    Subject: CN=r1
    Issuer : CN=testca
    Validity
      Start date: 2025-06-05 08:20:22
      End   date: 2035-06-03 08:20:22
    Key Type: SM2(256 bit)
    Usage: Sign

Fingerprint(sm3):b5434ea083d4c8443940a8db07aded3dcf6bd5e659f6c361087274d07f
454e8f
    Fingerprint(sha1):1b6f0009b78486940e8e80434848a70b182eb999
    Associated Identity: GDFH
        index: 5

mp1800x55#

测试版本:

[3620x1-probe]display system internal version
H3C MSR3620 V600R007B02D071SP32
Comware V700R001B64D086SP82
[3620x1-probe]
<3620x1>disp version
H3C Comware Software, Version 7.1.064, Feature 6749L40

H3C MSR3620 uptime is 0 weeks, 2 days, 14 hours, 48 minutes
Last reboot reason : User reboot
Boot image: flash:/msr36x1-cmw710-boot-f6749l40.bin
Boot image version: 7.1.064P80, Feature 6749L40
  Compiled May 16 2025 15:00:00
System image: flash:/msr36x1-cmw710-system-f6749l40.bin
System image version: 7.1.064, Feature 6749L40
  Compiled May 16 2025 15:00:00
Feature image(s) list:
  flash:/msr36x1-cmw710-escan-f6749l40.bin, version: 7.1.064
    Compiled May 16 2025 15:00:00
  flash:/msr36x1-cmw710-security-f6749l40.bin, version: 7.1.064

Compiled May 16 2025 15:00:00
flash:/msr36x1-cmw710-voice-f6749l40.bin, version: 7.1.064
Compiled May 16 2025 15:00:00
flash:/msr36x1-cmw710-data-f6749l40.bin, version: 7.1.064
Compiled May 16 2025 15:00:00

mp1800x55(config)#do show version
MyPower (R) Operating System Software
MP1800X system image file (flash0: /flash/rp37-g-8.11.32.65(R).pck), version 8.11.32.65, Compiled on Apr 01 2023, 20:33:59
Copyright (C) 2023 Maipu Communication Technology Co.,Ltd.All Rights Reserved.

MP1800X Version Information
System ID : ccd81fc37e60
Hardware Model : MP1800X-55(V12) with 512 MBytes SDRAM, 128 MBytes flash
Hardware Version : 2(Hotswap Unsupported)
Bootloader Version : 1.0.8.04
Software Version : 8.11.32.65
Software Image File : flash0: /flash/rp37-g-8.11.32.65(R).pck
Compiled : Apr 01 2023, 20:33:59

Local MPU Uptime is 1 day 20 hours
System Uptime is 1 day 20 hours

mp1800x55(config)#

注意事项:

1). 国密 ike1.0 迈普侧要求 id-type 为 dn, msr36 侧需要配置为 id-type dn; 如果 msr36 使用默认的 id-type address, msr36 做发起方，发送完第三个包 SK 后，迈普侧应答证书编码错误.

2). 测试互通的版本一阶段算法配置为 sm3 可以建立起来; 配置为 sha1 算法建立不起来，第三个包签名 SIG 字段两边互相验证不过.