拠点間 IPsecVPN 接続の設定例

実習内容と目標

このラボでは以下のことを学びます：

- IPsec で IKE メインモード、事前共有鍵認証方式を習得します。
- IPsec で IKE アグレッシブモード、事前共有鍵認証方式を習得します。

ネットワーク図

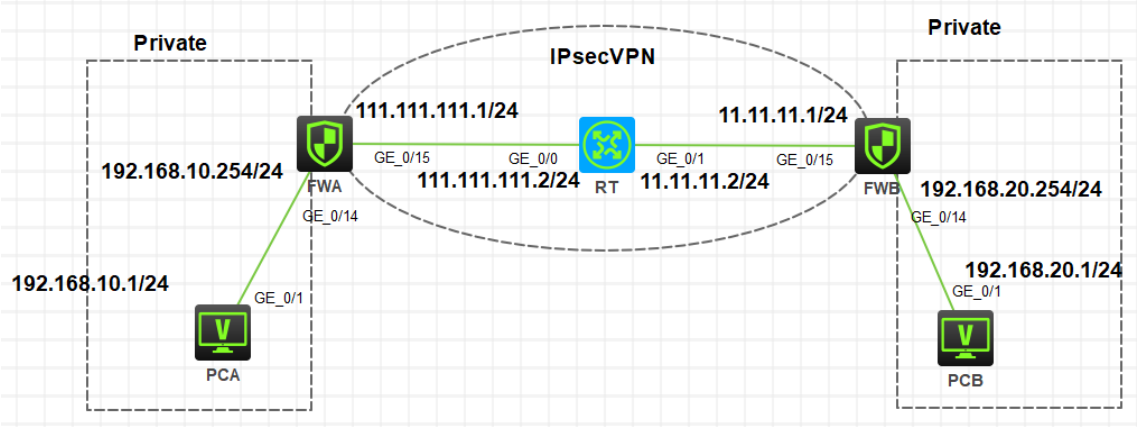

図1 実習ネットワーク

実習装置

本実験に必要な主な設備機材 実験装置名前とモデル番号	バージョン	数量	特記事項
F1060	7.1.064	2	ファイアウォール
MSR36-20	Version7.1	1	ルーター
PC	Windows 7	2	ホスト
V.35 シリアルケーブル		1	
ネットワークケーブルの接続	--	4	ストレートケーブル

IP アドレス割り当て

表 1 IP アドレス割り当て

装置	インターフェイス	IP アドレス	ゲートウェイ
FWA	G1/014	192.168.10.254/24	-
	G/1/0/15	111.111.1111.1/24	-
FWB	G1/0/14	192.168.20.1/24	-
	G1/0/15	11.11.11.1/24	-
RT	G0/0	111.111.111.2/24	
	G0/1	11.11.11.2/24	
PCA		192.168.10.1/24	192.168.10.254/24
PCB		192.168.20.1/24	192.168.20.254/24

実習手順

タスク 1：IPsec+IKE メインモードを設定します

このラボタスクでは、IKE ネゴシエーションを介して RTA と RTB の間に IPsec トンネルを確立する方法と、フェーズ 1 でメインモードを使用するように IKE を構成する方法を示します。

手順 1：両 PC に IP アドレス、ゲートウェイアドレスを設定する

PC に表 1 のように IP アドレス、ゲートウェイアドレスを設定します。

手順 2：基本的な設定をする

FWA を以下のように設定します。

login: admin

Password: admin

<FWB> [FWA]interface GigabitEthernet 1/0/14

[FWA-GigabitEthernet1/0/14]ip address 192.168.10.254 24

[FWA-GigabitEthernet1/0/14]quit

[FWA]interface GigabitEthernet 1/0/15

[FWA-GigabitEthernet1/0/15]ip address 111.111.111.1 24

[FWA-GigabitEthernet1/0/15]quit

[FWA]security-zone name Trust

[FWA-security-zone-Trust]import interface GigabitEthernet 1/0/14

[FWA-security-zone-Trust]quit
[FWA]security-zone name Untrust
[FWA-security-zone-Untrust]import interface GigabitEthernet 1/0/15
[FWA-security-zone-Untrust]quit
[FWA]security-policy ip
[FWA-security-policy-ip]rule 0 name any
[FWA-security-policy-ip-0-any]action pass
[FWA-security-policy-ip-0-any]quit
[FWA-security-policy-ip]quit
[FWA]ip route-static 0.0.0.0 0 111.111.111.2

FWB を以下のように設定します。
login: admin
Password: admin
[FWB]interface GigabitEthernet 1/0/14
[FWB-GigabitEthernet1/0/14]ip address 192.168.20.254 24
[FWB-GigabitEthernet1/0/14]quit
[FWB]interface GigabitEthernet 1/0/15
[FWB-GigabitEthernet1/0/15]ip address 11.11.11.1 24
[FWB-GigabitEthernet1/0/15]quit
[FWB]security-zone name Trust
[FWB-security-zone-Trust]imp
[FWB-security-zone-Trust]import interface GigabitEthernet 1/0/14
[FWB-security-zone-Trust]quit
[FWB]security-zone name Untrust
[FWB-security-zone-Untrust]import interface GigabitEthernet 1/0/15
[FWB-security-zone-Untrust]quit
[FWB]security-policy ip
[FWB-security-policy-ip]rule 0 name any
[FWB-security-policy-ip-0-any]action pass
[FWB-security-policy-ip-0-any]quit
[FWB-security-policy-ip]quit
[FWB]ip route-static 0.0.0.0 0 11.11.11.2

RT を以下のように設定します。
[RT]interface GigabitEthernet 0/0

[RT-GigabitEthernet0/0]ip address 111.111.111.2 24

[RT-GigabitEthernet0/0]quit

[RT]interface GigabitEthernet 0/1

[RT-GigabitEthernet0/1]ip address 11.11.11.2 24

[RT-GigabitEthernet0/1]quit

FWA と FWB には隣接する Prive ネットワークへのルートが必要です。

[FWA]ip route-static 192.168.20.0 24 111.111.111.2

[FWB]ip route-static 192.168.10.0 24 11.11.11.2

手順 3:接続性をチェックする

<PCA>ping 192.168.20.1

Ping 192.168.20.1 (192.168.20.1): 56 data bytes, press CTRL_C to break

Request time out

Request time out

Request time out

Request time out

Request time out

<PCB>ping 192.168.10.1

Ping 192.168.10.1 (192.168.10.1): 56 data bytes, press CTRL_C to break

Request time out

Request time out

Request time out

Request time out

Request time out

手順 4:IKE Proposal の設定をする

FWA を以下のように設定します。

[FWA]ike proposal 1

[FWA-ike-proposal-1]authentication-method pre-share

[FWA-ike-proposal-1]authentication-algorithm md5

[FWA-ike-proposal-1]encryption-algorithm 3des-cbc

[FWA-ike-proposal-1]quit

FWB を以下のように設定します。

[FWB]ike proposal 1
[FWB-ike-proposal-1]authentication-method pre-share
[FWB-ike-proposal-1]authentication-algorithm md5
[FWB-ike-proposal-1]encryption-algorithm 3des-cbc
[FWB-ike-proposal-1]quit

手順 5：IKE Keychain の設定をする

FWA を以下のように設定します。
[FWA]ike keychain 1
[FWA-ike-keychain-1]pre-shared-key address 11.11.11.1 32 key simple 123456
[FWA-ike-keychain-1]quit

FWB を以下のように設定します。
[FWB]ike keychain　1
[FWB-ike-keychain-1]pre-shared-key address 111.111.111.1 32 key simple 123456
[FWB-ike-keychain-1]quit

手順 6：IKE Profile の設定をする

FWA を以下のように設定します。
[FWA]ike profile 1
[FWA-ike-profile-1]local-identity address 111.111.111.1
[FWA-ike-profile-1]match remote identity address 11.11.11.1 32
[FWA-ike-profile-1]keychain 1
[FWA-ike-profile-1]proposal 1
[FWA-ike-profile-1]quit

FWB を以下のように設定します。
[FWB]ike profile 1
[FWB-ike-profile-1]local-identity address 11.11.11.1
[FWB-ike-profile-1]match remote identity address 111.111.111.1 32
[FWB-ike-profile-1]keychain 1
[FWB-ike-profile-1]proposal 1
[FWB-ike-profile-1]quit

手順 7：セキュリティ ACL の設定をする

FWA を以下のように設定します。

```
[FWA]acl advanced 3500
[FWA-acl-ipv4-adv-3500]rule 0 permit ip source 192.168.10.0 0.0.0.255 destinatio
n 192.168.20.0 0.0.0.255
[FWA-acl-ipv4-adv-3500]quit
```

FWB を以下のように設定します。

```
[FWB]acl advanced 3500
[FWB-acl-ipv4-adv-3500]rule 0 permit ip source 192.168.20.0 0.0.0.255 destinatio
n 192.168.10.0 0.0.0.255
[FWB-acl-ipv4-adv-3500]quit
```

手順 8：IPsec security proposal の設定をする

FWA を以下のように設定します。

```
[FWA]ipsec transform-set 1
[FWA-ipsec-transform-set-1]esp authentication-algorithm sha1
[FWA-ipsec-transform-set-1]esp encryption-algorithm aes-cbc-128
[FWA-ipsec-transform-set-1]quit
```

FWB を以下のように設定します。

```
[FWB]ipsec transform-set 1
[FWB-ipsec-transform-set-1]esp authentication-algorithm sha1
[FWB-ipsec-transform-set-1]esp encryption-algorithm aes-cbc-128
[FWB-ipsec-transform-set-1]quit
```

手順 9：IPsec セキュリティポリシーを設定する

FWA を以下のように設定します。

```
[FWA]ipsec policy 1 1 isakmp
[FWA-ipsec-policy-isakmp-1-1]remote-address 11.11.11.1
[FWA-ipsec-policy-isakmp-1-1]security acl 3500
[FWA-ipsec-policy-isakmp-1-1]transform-set 1
[FWA-ipsec-policy-isakmp-1-1]ike-profile 1
[FWA-ipsec-policy-isakmp-1-1]quit
[FWA]interface GigabitEthernet 1/0/15
```

[FWA-GigabitEthernet1/0/15]ipse apply policy 1
[FWA-GigabitEthernet1/0/15]quit

FWB を以下のように設定します。
[FWB]ipsec policy 1 1 isakmp
[FWB-ipsec-policy-isakmp-1-1]remote-address 111.111.111.1
[FWB-ipsec-policy-isakmp-1-1]security acl 3500
[FWB-ipsec-policy-isakmp-1-1]transform-set 1
[FWB-ipsec-policy-isakmp-1-1]ike-profile 1
[FWB-ipsec-policy-isakmp-1-1]quit
[FWB]interface GigabitEthernet 1/0/15
[FWB-GigabitEthernet1/0/15]ipsec apply policy 1
[FWB-GigabitEthernet1/0/15]quit

手順 10：設定をチェックする

```
<FWA>display ike proposal
  Priority Authentication Authentication Encryption    Diffie-Hellman Duration
                     method           algorithm       algorithm           group          (seconds)
-------------------------------------------------------------------------------
  1             PRE-SHARED-KEY        MD5             3DES-CBC       Group 1             86400
  default    PRE-SHARED-KEY        SHA1            DES-CBC        Group 1             86400

<FWA>display ipsec transform-set
IPsec transform set: 1
   State: complete
   Encapsulation mode: tunnel
   ESN: Disabled
   PFS:
   Transform: ESP
   ESP protocol:
      Integrity: SHA1
      Encryption: AES-CBC-128

<FWA>display ipsec policy
-----------------------------------------
IPsec Policy: 1
```

```
Interface: GigabitEthernet1/0/15
-----------------------------------------
  ----------------------------
  Sequence number: 1
  Mode: ISAKMP
  ----------------------------
  Traffic Flow Confidentiality: Disabled
  Security data flow: 3500
  Selector mode: standard
  Local address:
  Remote address: 11.11.11.1
  Transform set:    1
  IKE profile: 1
  IKEv2 profile:
  smart-link policy:
  SA trigger mode: Traffic-based
  SA duration(time based): 3600 seconds
  SA duration(traffic based): 1843200 kilobytes
  SA soft-duration buffer(time based): --
  SA soft-duration buffer(traffic based): --
  SA idle time: --
```

手順 11:トンネルの動作状態をチェックする

```
<PCA>ping 192.168.20.1
Ping 192.168.20.1 (192.168.20.1): 56 data bytes, press CTRL_C to break
Request timed out
56 bytes from 192.168.20.1: icmp_seq=0 ttl=253 time=4.000 ms
56 bytes from 192.168.20.1: icmp_seq=1 ttl=253 time=8.000 ms
56 bytes from 192.168.20.1: icmp_seq=2 ttl=253 time=8.000 ms
56 bytes from 192.168.20.1: icmp_seq=3 ttl=253 time=9.000 ms
56 bytes from 192.168.20.1: icmp_seq=4 ttl=253 time=9.000 ms

<FWA>display ike sa
      Connection-ID     Remote                        Flag              DOI
-----------------------------------------------------------------------
```

```
    1                   11.11.11.1              RD              IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY

<FWA>display ipsec sa
------------------------------
Interface: GigabitEthernet1/0/15
------------------------------

  ------------------------------
  IPsec policy: 1
  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: 1428
    Tunnel:
        local    address: 111.111.111.1
        remote address: 11.11.11.1
    Flow:
        sour addr: 192.168.10.0/255.255.255.0    port: 0    protocol: ip
        dest addr: 192.168.20.0/255.255.255.0    port: 0    protocol: ip

    [Inbound ESP SAs]
      SPI: 1465250511 (0x5755f2cf)
      Connection ID: 4294967296
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843197/1407
      Max received sequence-number: 29
      Anti-replay check enable: Y
```

Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active

[Outbound ESP SAs]
SPI: 4148267663 (0xf7418a8f)
Connection ID: 4294967297
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843197/1407
Max sent sequence-number: 29
UDP encapsulation used for NAT traversal: N
Status: Active

手順 12：次のラボのために今までの FWA, FWB の設定を元に戻します

FWA の IPsec VPN 設定を削除します。

```
[FWA]interface GigabitEthernet 1/0/15
[FWA-GigabitEthernet1/0/15]undo ipsec apply policy
[FWA-GigabitEthernet1/0/15]quit
[FWA]undo ipsec policy 1
[FWA]undo ipsec transform-set 1
[FWA]undo ike profile 1
[FWA]undo ike keychain 1
[FWA]undo ike proposal 1
[FWA]undo acl advanced 3500
[FWA]quit
```

FWB の IPsec VPN 設定を削除します。

```
[FWB]int GigabitEthernet 1/0/15
[FWB-GigabitEthernet1/0/15]undo ipsec apply policy
[FWB-GigabitEthernet1/0/15]quit
[FWB]undo ipsec policy 1
[FWB]undo ipsec transform-set 1
[FWB]undo ike profile 1
```

[FWB]undo ike keychain 1

[FWB]undo ike proposal 1

[FWB]undo acl advanced 3500

タスク 1：IPsec+IKE アグレッシブモードを設定します

このラボタスクでは、IKE ネゴシエーションを介して RTA と RTB の間に IPsec トンネルを確立する方法と、フェーズ 1 でアグレッシブモードを使用するように IKE を構成する方法を示します。

手順 1：IKE proposal を設定します

FWA の設定は以下の通りです：

[FWA]ike proposal 1

[FWA-ike-proposal-1]authentication-method pre-share

[FWA-ike-proposal-1]authentication-algorithm md5

[FWA-ike-proposal-1]encryption-algorithm 3des-cbc

[FWA-ike-proposal-1]quit

FWB の設定は以下の通りです：

[FWB]ike proposal 1

[FWB-ike-proposal-1]authentication-method pre-share

[FWB-ike-proposal-1]authentication-algorithm md5

[FWB-ike-proposal-1]encryption-algorithm 3des-cbc

[FWB-ike-proposal-1]quit

手順 2：IKE identity 情報を設定します

FWA の設定は以下の通りです：

[FWA]ike identity fqdn fwa

FWB の設定は以下の通りです：

[FWB]ike identity fqdn fwa

手順 3：IKE keychain を設定します

FWA の設定は以下の通りです：

[FWA]ike keychain 1

[FWA-ike-keychain-1]pre-shared-key address 11.11.11.1 32 key simple 123456

[FWA-ike-keychain-1]quit

FWB の設定は以下の通りです:

```
[FWB]ike keychain 1
[FWB-ike-keychain-1]pre-shared-key hostname fwa key simple 123456
[FWB-ike-keychain-1]quit
```

手順 4:IKE profile を設定します

FWA の設定は以下の通りです:

```
[FWA]ike keychain 1
[FWA-ike-keychain-1]pre-shared-key address 11.11.11.1 32 key simple 123456
[FWA-ike-keychain-1]quit
[FWA]ike profile 1
[FWA-ike-profile-1]exchange-mode aggressive
[FWA-ike-profile-1]match remote identity fqdn fwb
[FWA-ike-profile-1]keychain 1
[FWA-ike-profile-1]proposal 1
[FWA-ike-profile-1]quit
```

FWB の設定は以下の通りです:

```
[FWB]ike profile 1
[FWB-ike-profile-1]exchange-mode aggressive
[FWB-ike-profile-1]match remote identity fqdn fwa
[FWB-ike-profile-1]keychain 1
[FWB-ike-profile-1]proposal 1
[FWB-ike-profile-1]quit
```

手順 5:セキュリティ ACL を設定します

FWA の設定は以下の通りです:

```
[FWA]acl advanced 3500
[FWA-acl-ipv4-adv-3500]rule 0 permit ip source 192.168.10.0 0.0.0.255 destinatio
n 192.168.20.0 0.0.0.255
[FWA-acl-ipv4-adv-3500]quit
```

FWB の設定は以下の通りです:

```
[FWB]acl advanced 3500
[FWB-acl-ipv4-adv-3500]rule 0 permit ip source 192.168.20.0 0.0.0.255 destinatio
n 192.168.10.0 0.0.0.255
```

[FWB-acl-ipv4-adv-3500]quit

手順 6：IPsec Security proposal を設定します

FWA の設定は以下の通りです：

[FWA]ipsec transform-set 1

[FWA-ipsec-transform-set-1]esp authentication-algorithm sha1

[FWA-ipsec-transform-set-1]esp encryption-algorithm aes-cbc-128

[FWA-ipsec-transform-set-1]quit

FWB の設定は以下の通りです：

[FWB]ipsec transform-set 1

[FWB-ipsec-transform-set-1]esp authentication-algorithm sha1

[FWB-ipsec-transform-set-1]esp encryption-algorithm aes-cbc-128

[FWB-ipsec-transform-set-1]quit

手順 7：IPsec Security policy を設定します

FWA の設定は以下の通りです：

[FWA]ipsec policy 1 1 isakmp

[FWA-ipsec-policy-isakmp-1-1]remote-address 11.11.11.1

[FWA-ipsec-policy-isakmp-1-1]security acl 3500

[FWA-ipsec-policy-isakmp-1-1]transform-set 1

[FWA-ipsec-policy-isakmp-1-1]ike-profile 1

[FWA-ipsec-policy-isakmp-1-1]quit

[FWA]interface GigabitEthernet 1/0/15

[FWA-GigabitEthernet1/0/15]ipsec apply policy 1

[FWA-GigabitEthernet1/0/15]quit

FWB の設定は以下の通りです：

[FWB]ipsec policy-template 1 1

[FWB-ipsec-policy-template-1-1]security acl 3500

[FWB-ipsec-policy-template-1-1]transform-set 1

[FWB-ipsec-policy-template-1-1]ike-profile 1

[FWB-ipsec-policy-template-1-1]quit

[FWB]ipsec policy 1 1 isakmp template 1

[FWB]interface GigabitEthernet 1/0/15

[FWB-GigabitEthernet1/0/15]ipsec apply policy 1

[FWB-GigabitEthernet1/0/15]quit

手順 8：設定をチェックします

```
[FWA]display ike proposal
  Priority Authentication Authentication Encryption    Diffie-Hellman Duration
                     method           algorithm       algorithm           group          (seconds)
------------------------------------------------------------------------------
  1             PRE-SHARED-KEY        MD5             3DES-CBC       Group 1             86400
  default    PRE-SHARED-KEY        SHA1            DES-CBC        Group 1             86400

[FWA]display ipsec transform-set 1
IPsec transform set: 1
   State: complete
   Encapsulation mode: tunnel
   ESN: Disabled
   PFS:
   Transform: ESP
   ESP protocol:
      Integrity: SHA1
      Encryption: AES-CBC-128

[FWA]display ipsec policy
-----------------------------------------
IPsec Policy: 1
Interface: GigabitEthernet1/0/15
-----------------------------------------
   ----------------------------
   Sequence number: 1
   Mode: ISAKMP
   ----------------------------
   Traffic Flow Confidentiality: Disabled
   Security data flow: 3500
   Selector mode: standard
   Local address:
   Remote address: 11.11.11.1
   Transform set:    1
```

```
  IKE profile: 1
  IKEv2 profile:
  smart-link policy:
  SA trigger mode: Traffic-based
  SA duration(time based): 3600 seconds
  SA duration(traffic based): 1843200 kilobytes
  SA soft-duration buffer(time based): --
  SA soft-duration buffer(traffic based): --
  SA idle time: --

[FWB]display ike proposal
  Priority Authentication Authentication Encryption    Diffie-Hellman Duration
                     method           algorithm       algorithm           group          (seconds)
------------------------------------------------------------------------------
  1             PRE-SHARED-KEY        MD5             3DES-CBC       Group 1             86400
  default    PRE-SHARED-KEY        SHA1            DES-CBC        Group 1             86400

[FWB]display ipsec transform-set
IPsec transform set: 1
  State: complete
  Encapsulation mode: tunnel
  ESN: Disabled
  PFS:
  Transform: ESP
  ESP protocol:
    Integrity: SHA1
    Encryption: AES-CBC-128

[FWB]display ipsec policy-template
-----------------------------------------
IPsec Policy Template: 1
-----------------------------------------
  ----------------------------
  Sequence number: 1
  ----------------------------
  Traffic Flow Confidentiality: Disabled
```

Security data flow : 3500

Selector mode: standard

Local address:

IKE profile: 1

IKEv2 profile:

Remote address:

Transform set: 1

IPsec SA local duration(time based): 3600 seconds

IPsec SA local duration(traffic based): 1843200 kilobytes

SA idle time: --

[FWB]display ipsec policy

IPsec Policy: 1

Interface: GigabitEthernet1/0/15

Sequence number: 1

Mode: Template

Policy template name: 1

手順 9：設定をチェックします

PCB で PCA への接続性をチェックします

<PCB>ping 192.168.10.1

Ping 192.168.10.1 (192.168.10.1): 56 data bytes, press CTRL_C to break

Request time out

Request time out

Request time out

Request time out

Request time out

PCA で PCB への接続性をチェックします

<PCA>ping 192.168.20.1

Ping 192.168.20.1 (192.168.20.1): 56 data bytes, press CTRL_C to break

Request time out

56 bytes from 192.168.20.1: icmp_seq=1 ttl=253 time=7.000 ms
56 bytes from 192.168.20.1: icmp_seq=2 ttl=253 time=6.000 ms
56 bytes from 192.168.20.1: icmp_seq=3 ttl=253 time=7.000 ms
56 bytes from 192.168.20.1: icmp_seq=4 ttl=253 time=6.000 ms

FWA と FWB の IPsec/IKE に関する情報を表示します。

```
<FWA>display ike sa
      Connection-ID      Remote                    Flag              DOI
-------------------------------------------------------------------------
      1                  11.11.11.1                RD                IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY

<FWA>display ike sa verbose
    ----------------------------------------------
    Connection ID: 1
    Outside VPN:
    Inside VPN:
    Profile: 1
    Transmitting entity: Initiator
    Initiator cookie: c0a04d6fb37cd7ab
    Responder cookie: 2dbc80efadda0768
    ----------------------------------------------
    Local IP: 111.111.111.1
    Local ID type: IPV4_ADDR
    Local ID: 111.111.111.1

    Remote IP: 11.11.11.1
    Remote ID type: IPV4_ADDR
    Remote ID: 11.11.11.1

    Authentication-method: PRE-SHARED-KEY
    Authentication-algorithm: MD5
    Encryption-algorithm: 3DES-CBC

    Life duration(sec): 86400
```

```
    Remaining key duration(sec): 81618
    Exchange-mode: Main
    Diffie-Hellman group: Group 1
    NAT traversal: Not detected

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

<FWA>display ipsec sa
-------------------------------
Interface: GigabitEthernet1/0/15
-------------------------------
  -----------------------------
  IPsec policy: 1
  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: 1428
    Tunnel:
        local    address: 111.111.111.1
        remote address: 11.11.11.1
    Flow:
        sour addr: 192.168.10.0/255.255.255.0    port: 0    protocol: ip
        dest addr: 192.168.20.0/255.255.255.0    port: 0    protocol: ip

    [Inbound ESP SAs]
      SPI: 3086555129 (0xb7f917f9)
      Connection ID: 12884901889
```

Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3380
Max received sequence-number: 4
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active

[Outbound ESP SAs]
SPI: 1724385507 (0x66c808e3)
Connection ID: 12884901888
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3380
Max sent sequence-number: 4
UDP encapsulation used for NAT traversal: N
Status: Active

<FWB>display ike sa

Connection-ID	Remote	Flag	DOI
1	111.111.111.1	RD	IPsec

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

<FWB>display ike sa verbose

Connection ID: 1
Outside VPN:
Inside VPN:
Profile: 1
Transmitting entity: Responder
Initiator cookie: c0a04d6fb37cd7ab
Responder cookie: 2dbc80efadda0768

Local IP: 11.11.11.1
Local ID type: IPV4_ADDR
Local ID: 11.11.11.1

Remote IP: 111.111.111.1
Remote ID type: IPV4_ADDR
Remote ID: 111.111.111.1

Authentication-method: PRE-SHARED-KEY
Authentication-algorithm: MD5
Encryption-algorithm: 3DES-CBC

Life duration(sec): 86400
Remaining key duration(sec): 81453
Exchange-mode: Main
Diffie-Hellman group: Group 1
NAT traversal: Not detected

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

<FWB>display ipsec sa

Interface: GigabitEthernet1/0/15

IPsec policy: 1
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: 1428
Tunnel:
    local address: 11.11.11.1
    remote address: 111.111.111.1
Flow:
    sour addr: 192.168.20.0/255.255.255.0 port: 0 protocol: ip
    dest addr: 192.168.10.0/255.255.255.0 port: 0 protocol: ip

[Inbound ESP SAs]
  SPI: 1724385507 (0x66c808e3)
  Connection ID: 12884901889
  Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
  SA duration (kilobytes/sec): 1843200/3600
  SA remaining duration (kilobytes/sec): 1843199/3226
  Max received sequence-number: 4
  Anti-replay check enable: Y
  Anti-replay window size: 64
  UDP encapsulation used for NAT traversal: N
  Status: Active

[Outbound ESP SAs]
  SPI: 3086555129 (0xb7f917f9)
  Connection ID: 12884901888
  Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
  SA duration (kilobytes/sec): 1843200/3600
  SA remaining duration (kilobytes/sec): 1843199/3226
  Max sent sequence-number: 4
  UDP encapsulation used for NAT traversal: N
  Status: Active