





# Client To Gateway

## Add a New Tunnel

Tunnel  Group VPN

Tunnel No. 1  
Tunnel Name :   
Interface : WAN1   
Enable :

## Local Group Setup

Local Security Gateway Type : IP Only   
IP Address : 0.0.0.0  
Local Security Group Type : Subnet   
IP Address : 192.168.1.0  
Subnet Mask : 255.255.255.0

## Remote Client Setup

Remote Security Gateway Type : IP Only   
IP Address  :

## IPSec Setup

[ãf^ãf³ãf◆ãf«ç•ã◆(Tunnel  
Number)]ã◆ã€◆ãf^ãf³ãf◆ãf«ã◆@ç•ã◆ã,èj¨ çºã◆™ã,è†ã◆ç"Yæ^◆ãf•ã,£ãf¼ãf«ãf%ã◆Sã◆™

### Client To Gateway

Add a New Tunnel

Tunnel
  Group VPN

Tunnel No.

Tunnel Name :

Interface :

Enable :

---

#### Local Group Setup

Local Security Gateway Type :

IP Address :

Local Security Group Type :

IP Address :

Subnet Mask :

---

#### Remote Client Setup

Remote Security Gateway Type :

IP Address :

---

#### IPSec Setup

2. Tunnel Name: tunnel\_1

3. Interface: WAN1

4. Enable: checked

### Local Security Gateway

1. Local Security Gateway Type: IP Only

IP Address: 0.0.0.0

Local Security Group Type: Subnet

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

Remote Client Setup

Remote Security Gateway Type: IP Only

IP Address:

IPSec Setup





VPN Client Configuration (Only)]

### Client To Gateway

**Add a New Tunnel**

Tunnel     Group VPN

Tunnel No. : 1

Tunnel Name : tunnel\_1

Interface : WAN1

Enable :

---

**Local Group Setup**

Local Security Gateway Type : IP Only

IP Address : 0.0.0.0

Local Security Group Type : Subnet

IP Address : 192.168.1.0

Subnet Mask : 255.255.255.0

---

**Remote Client Setup**

Remote Security Gateway Type : IP Only

IP Address :

IP Only

IP Only

IP + Domain Name(FQDN) Authentication

IP + Email Address(USER FQDN) Authentication

Dynamic IP + Domain Name(FQDN) Authentication

Dynamic IP + Email Address(USER FQDN) Authentication

---

**IPSec Setup**

Keying Mode : IKE with Preshared key

- IP Address (WAN)
- IP Address (Subnet)
- IP + Domain Name (FQDN) Authentication
- IP + Email Address (User FQDN) Authentication
- Dynamic IP + Domain Name (FQDN) Authentication
- Dynamic IP + Email Address (User FQDN) Authentication

IP Address (IP Only) [IP + Domain Name (FQDN)] [IP + E-mail Address (User FQDN) Authentication] [IP Address]

IP Address (IP Only) [IP + Domain Name (FQDN)] [IP + E-mail Address (User FQDN) Authentication] [IP Address]

IP Address (IP Only) [IP + Domain Name (FQDN)] [IP + E-mail Address (User FQDN) Authentication] [IP Address]







**Remote Client Setup**

Remote Security Gateway Type : IP Only

IP Address : 192.168.1.2

---

**IPSec Setup**

Keying Mode : Manual

Incoming SPI : 100A

Outgoing SPI : 1BCD

Encryption : DES

Authentication : MD5

Encryption Key :

Authentication Key :

3.1.4 [Encryption]

Encryption is a process of converting plain text into cipher text using an algorithm and a key. It is used to protect data from unauthorized access.

- DES: Data Encryption Standard (DES) is a symmetric-key algorithm for encrypting and decrypting data. It uses a 56-bit key and a Feistel network to perform the encryption process.
- 3DES: Triple Data Encryption Standard (3DES) is a symmetric-key algorithm for encrypting and decrypting data. It uses three 56-bit keys and three DES encryption processes.

**IPSec Setup**

Keying Mode : Manual

Incoming SPI : 100A

Outgoing SPI : 1BCD

Encryption : DES

Authentication : MD5

Encryption Key :

Authentication Key :

3.1.5 [Authentication]

Authentication is a process of verifying the identity of a user or system. It is used to ensure that the data is being sent by the intended sender.

- MD5: Message Digest Algorithm-5 (MD5) is a cryptographic hash function that takes an input and produces a fixed-size output called a hash value. It is used for data integrity and authentication.
- SHA1: Secure Hash Algorithm version 1 (SHA1) is a cryptographic hash function that takes an input and produces a fixed-size output called a hash value. It is used for data integrity and authentication.



**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : **Group 1 - 768 bit**

Phase 1 Encryption : DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 28800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter :

Phase 1 Encryption]

1 Encryption]

- DES:Data Encryption  
Standard(DES) 56 bit
- 3DES:Triple Data Encryption  
Standard(3DES) 168 bit
- AES-128:Advanced Encryption  
Standard(AES) 128 bit
- AES-192:Advanced Encryption  
Standard(AES) 192 bit
- AES-256:Advanced Encryption  
Standard(AES) 256 bit

**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 bit

Phase 1 Encryption : DES

Phase 1 Authentication : DES

Phase 1 SA Life Time : 3600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter :

3.1.4 [Phase 1 Authentication]

- MD5: Message Digest Algorithm-5 (MD5)
- SHA1: Secure Hash Algorithm version 1 (SHA1)

**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 bit

Phase 1 Encryption : DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 3600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter :

Advanced +

Phase 1 Authentication :

MD5

Phase 2 Authentication :

MD5



**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : DES

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 27600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : **Group 1 - 768 bit**

Phase 2 Encryption : MD5

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter :

Phase 2 Encryption

Phase 2 Encryption is used to encrypt the Phase 2 traffic. The encryption algorithm and key length are configured in the Phase 2 Encryption settings. The available options are:

- DES:Data Encryption Standard(DES) is a symmetric key algorithm. It uses a 56-bit key to encrypt and decrypt data.
- 3DES:Triple Data Encryption Standard(3DES) is a symmetric key algorithm. It uses a 168-bit key to encrypt and decrypt data.
- AES-128:Advanced Encryption Standard(AES) is a symmetric key algorithm. It uses a 128-bit key to encrypt and decrypt data.
- AES-192:Advanced Encryption Standard(AES) is a symmetric key algorithm. It uses a 192-bit key to encrypt and decrypt data.
- AES-256:Advanced Encryption Standard(AES) is a symmetric key algorithm. It uses a 256-bit key to encrypt and decrypt data.

**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : DES

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 27600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

Phase 2 Authentication : **DES**

Phase 2 SA Life Time :

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter :

Advanced +

Phase 2 Authentication

VPN

- MD5:Message Digest Algorithm-5(MD5)
- SHA1:Secure Hash Algorithm version 1(SHA1)
- Null

**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : DES

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 27600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time :

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter :

Advanced +

Phase 1

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : DES

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 27600 seconds

Phase 2

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time :

Preshared Key

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter :

Advanced +







ã"ã"ã¾ãšã¯ã€RV016ã€RV042ã€RV042Gã€ãšã,^ã³RV082  
VPNãf«ãf¼ã,¿ã,šãšã,ãf©ã,ãã,çãf³ãf^ã<ã,%ã,²ãf¼ãf^ã,|ã,šã,ãã,ãã®ãfªãfçãf¼ãf^ã,çã,¯ã,»ã,¹V

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。