IPsec-VPN（基本構築）

学習内容

1. IKEフェーズ1 (ISAKMP SA) の設定
2. IKEフェーズ2 (IPsec SA) の設定
3. 異機種間接続のためのパラメータ整理
4. PPPoE環境でのVPN構築
5. トラブルシューティングと確認コマンド
6. NAT環境との両立（NAT除外）

01

IKEフェーズ1 (ISAKMP SA) の設定

IKEフェーズ1とは？

IPsec通信の「準備段階」としてISAKMP SAを確立する

IPsec通信を開始するための**最初のステップ**

ISAKMP SA (Security Association) と呼ばれる管理用のセキュアなトンネルを生成する

このトンネルの上で、後のフェーズ2で使われる「鍵」や「パラメータ」が安全に交換される

(config)# crypto isakmp policy [priority] コマンドでポリシーを作成する

priorityは数字が小さいほど優先度が高く、相手と**最初に一致したポリシー**が使用される

ISAKMPポリシーの主要パラメータ

フェーズ1で相手機器と合意する必要がある5つの主要項目

encryption (暗号化)

ISAKMP SAの暗号化方式 (des, 3des, aes 128/192/256)

hash (ハッシュ)

認証や鍵計算に使うハッシュ方式 (md5, sha, sha256など)

authentication (認証方式)

相手を認証する方法 (**pre-share**, rsa-sig, rsa-encr)

ISAKMP SA パラメータとデフォルト値

試験対策としてデフォルト値を覚えておくことが重要

項目	コマンド (config-isakmp)#	選択肢	デフォルト値
暗号化方式	encryption	des, 3des, aes 128/192/256	**des**
ハッシュ方式	hash	sha, md5, sha256/384/512	**sha**
認証方式	authentication	rsa-sig, rsa-encr, pre-share	**rsa-sig**
DHグループ	group	1, 2, 5	**1**
有効時間	lifetime	60〜86400秒	**86400秒 (24時間)**

Pre-shared Key と DPDの設定

認証方式に「pre-share」を選んだ場合の追加設定

Pre-shared Key (事前共有鍵)

`authentication pre-share` を選択した場合、グローバルコンフィグモードで鍵（パスワード）と相手のIPアドレスを指定する

`(config)# crypto isakmp key [password] address [address]`

例: `crypto isakmp key cisco address 100.1.1.1`

DPD (Dead Peer Detection)

相手とのトンネル切断を自動検出する機能。通常は無効

`(config)# crypto isakmp keepalive [seconds] [retries] [periodic | on-demand]`

ダイナミックルーティングを使わない環境では `periodic` の指定が推奨される

IKEフェーズ1 設定例

3DES/SHA/Pre-share/DH2/Lifetime 12時間/DPD 30秒 の場合

```
Cisco(config)# crypto isakmp policy 1
Cisco(config-isakmp)# encryption 3des
Cisco(config-isakmp)# hash sha
Cisco(config-isakmp)# authentication pre-share
Cisco(config-isakmp)# group 2
Cisco(config-isakmp)# lifetime 43200
```

02

IKEフェーズ2 (IPsec SA) の設定

IKEフェーズ2 設定の4ステップ

フェーズ1で確立したISAKMP SAを利用してIPsec SAを生成する

トランスフォームセットの定義

「どのプロトコル」で「どう暗号化・認証するか」の組み合わせ

セキュリティプロトコル	ESP暗号化	ESP認証
AH (認証のみ) または **ESP (暗号化+認証)** を選択。通常はESPが使われる	esp-des, esp-3des, esp-aes などから選択	esp-md5-hmac, esp-sha-hmac などから選択

暗号マップの3要素とACLの役割

フェーズ2設定の中核となる「暗号マップ（Crypto Map）」

ACL (対象トラフィック)

「どの通信を」暗号化するかをACLの **permit** 文で定義。**denyは暗号化対象外**となる

Transform-Set (暗号ルール)

「どのように」暗号化するか (先ほど定義したトランスフォームセットの名前)

Peer (相手アドレス)

「誰と」VPNトンネルを張るか (相手のIPアドレス)

IKEフェーズ2 設定例 (全体)

フェーズ1の設定に続けて、フェーズ2を設定する流れ

```
! IKE Phase 1 (省略)...

! IKE Phase 2 の設定

Cisco(config)# crypto ipsec transform-set IPSEC esp-3des esp-md5-hmac

! IPsec対象トラフィックの定義 (ACL 101)

Cisco(config)# access-list 101 permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
```

03

異機種間接続とパラメータ

IKEフェーズ1 vs IKEフェーズ2 パラメータ

構築前にパラメータシートを用意し、相手と合意するのが鉄則

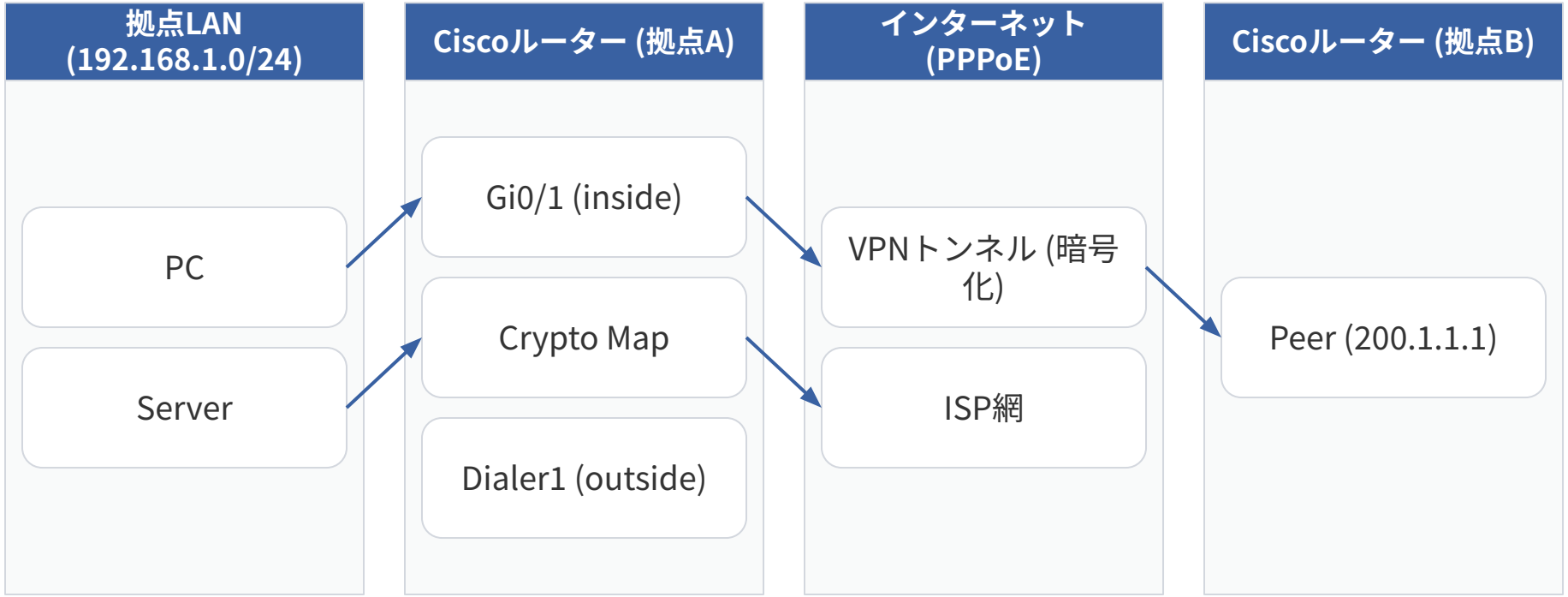
IKE Phase1 (ISAKMP SA)	IKE Phase2 (IPsec SA)
暗号化アルゴリズム (DES/3DES/AES)	セキュリティプロトコル (AH/ESP)
ハッシュ (MD5/SHA)	暗号化 (DES/3DES/AES/Null)
認証方式 (Pre-shared Key / 署名)	認証 (HMAC-MD5 / HMAC-SHA1)
DHグループ (1/2/5)	PFSグループ (任意：1/2/5)
ISAKMP SA ライフタイム	IPsec SA ライフタイム
Pre-shared Key (合言葉)	**IPsec対象トラフィック (ACL)**
DPDの有無	**IPsec通信モード (トンネル/トランスポート)**

04

PPPoE環境でのVPN構築

PPPoE + IPsec VPN 構成イメージ

暗号マップ（Crypto Map）を物理インターフェースではなくDialerへ適用



PPPoE環境 サンプル構成 (拠点A)

Dialer1インターフェースに暗号マップとPPPoE設定を共存させる

```
! (Phase1, Phase2, ACL, Crypto Map設定は省略)...
interface GigabitEthernet0/0
 pppoe-client dial-pool-number 1
!
interface GigabitEthernet0/1
 ip address 192.168.1.254 255.255.255.0
!
interface Dialer1
 ip unnumbered Loopback1  (※固定IP運用の場合)
 ip mtu 1454
 encapsulation ppp
 dialer pool 1
 ppp authentication chap callin
 ppp chap hostname ...
 ppp chap password ...
 crypto map M-ipsec
!
ip route 0.0.0.0 0.0.0.0 Dialer1
```

05

トラブルシューティング

フェーズ1 (ISAKMP SA) の切り分け

`show crypto isakmp sa` コマンドの出力で判断する

Q. 何も表示されない

A. トラフィック未発生かACL不一致。対象間でPing疎通確認

Q. MM_NO_STATE

A. 交渉失敗。**PSK不一致**やISAKMP到達不可。鍵とACLを要確認

Q. QM_IDLE

A. **フェーズ1成功**。フェーズ2 (`show crypto ipsec sa`) を確認

フェーズ2 (IPsec SA) の確認

`show crypto ipsec sa` で暗号化・復号の統計情報を確認

`show crypto ipsec sa` を実行し、統計情報を確認する

#pkts encaps / #pkts encrypt (暗号化された送信パケット数)

#pkts decaps / #pkts decrypt (復号された受信パケット数)

VPN対象の通信 (Pingなど) を行い、**これらのカウンタが増加**すれば、フェーズ2は正常に動作している

カウンタが増加しない場合、フェーズ2のパラメータ（トランスフォームセット、ACL）の不一致が疑われる

主要な確認コマンド

各コマンドの目的を正確に把握する

コマンド	目的・確認内容
`show crypto isakmp policy`	設定されているIKEフェーズ1ポリシー（暗号、ハッシュ、認証など）の確認
`show crypto isakmp sa`	IKEフェーズ1のSA状態（MM_NO_STATE / QM_IDLEなど）の確認
`show crypto ipsec transform-set`	設定されているIKEフェーズ2トランスフォームセットの定義確認
`show crypto ipsec sa`	IKEフェーズ2のSAと統計値（暗号化・復号のパケット数）の確認
`show crypto session detail`	現在の暗号化セッションの詳細状態と切り分け材料の確認

06

NATとの両立 (NAT除外)

NAT除外設定の正しい順序

NAT用ACLで「deny (除外)」→「permit (変換)」の順序が最重要

IPsec対象ACL (A-ipsec)	NAT用ACL (A-nat)	NAT用ACL (A-nat)	NAT設定
`permit ip [自LAN] [宛先LAN]` (暗号化する通信を定義)	`deny ip [自LAN] [宛先LAN]` (VPN通信を**NAT除外**)	`permit ip [自LAN] any` (上記以外を**NAT対象**)	`ip nat inside source list A-nat ...` (NAT用ACLを適用)

VPN (Dialer) とNAT (GIP) の設定

PPPoE環境で固定IP (Loopback) を持つ場合のNAT設定

VPN設定 (Dialer IF)

interface Dialer1

ip unnumbered Loopback1

ip mtu 1454

ip nat **outside**

crypto map M-ipsec

NAT設定 (GIP/LAN IF)

ip nat inside source list **A-nat** interface **Loopback1** overload

interface Loopback1

ip address [固定GIP] ...

interface GigabitEthernet0/1

ip nat **inside**