VPN設定(IPSec)

クラス名　　　　　　　NO.　　　　氏名

次の仕様に従いVPNネットワークを構築しなさい。

　＊nt22からbasic\_lab02.pkaをコピーして構築しなさい。

　＊PCとServerについては設定済み。

タイムライン が含まれている画像

自動的に生成された説明

■ルータの設定

1.ホスト名、IPアドレスは図の通り。

■ルート情報設定

1.RAに192.168.2.0/24ネットワークへのスタティックルートを設定しなさい。

2.RBに192.168.1.0/24ネットワークへのスタティックルートを設定しなさい。

3.PCからServer(192.168.2.1)への接続を確認しなさい。[　接続できない　]

■次の仕様に従いVPNの設定を行いなさい。

1.RAとRBに設定するVPN通信用のACLを記述しなさい。VPN通信は192.168.1.1と192.168.2.1間で行われる。

RA(config)#[ int g0/0/0 ]

RA(config)#[ ip add 199.10.1.1 255.255.255.252 ]

RA(config)#[ int g0/0/1 ]

　RA(config)#[ ip add 192.168.1.254 255.255.255.0 　]

RB(config)#[ int g0/0/0 ]

RB(config)#[ ip add 199.10.1.2 255.255.255.252 ]

　RB(config)#[ int g0/0/1 ]

　RB(config)#[ ip add 192.168.2.254 255.255.255.0 　]

2.1で記述したACLを各ルータに設定しなさい。ACLの番号は100とすること。

　RA(config)#[ ip route 192.168.2.0 255.255.255.0 199.10.1.2]

　RA(config)#[ access-list 100 permit ip host 192.168.1.1 host 192.168.2.1 　]

　RB(config)#[ ip route 192.168.1.0 255.255.255.0 199.10.1.1]

　RB(config)#[ access-list 100 permit ip host 192.168.2.1 host 192.168.1.1 　]

3.次の仕様に従いIKEポリシーの設定を行いなさい。

　ポリシー番号：1、　認証：pre-share(事前共有鍵)、　暗号化アルゴリズム：AES(128ビット)

　DHグループ：2、　ハッシュ方式：sha、　有効時間：3600秒

Router(config)#crypto isakmp policy 1  
Router(config-isakmp)#authentication pre-share   
Router(config-isakmp)#encryption aes 128  
Router(config-isakmp)#group 2  
Router(config-isakmp)#hash sha  
Router(config-isakmp)#lifetime 3600

4 .共通鍵とIPアドレスの関連付けを行いなさい。

　RA・・・パスワード：mcato、　対向ルータ：199.10.1.2

RA(config)#crypto isakmp key mcato address 199.10.1.2

　RB・・・パスワード：mcato、　対向ルータ：199.10.1.1

RB(config)#crypto isakmp key mcato address 199.10.1.1

5.トランスフォームセット設定を設定しなさい。

　RA・・・トランスフォームセット名：TFS＿RA、オプション：esp-aes、　esp-sha-hmac

Router(config)#crypto ipsec transform-set TFS\_RA esp-aes esp-sha-hmac

　RB・・・トランスフォームセット名：TFS＿RB、オプション：esp-aes、　esp-sha-hmac

Router(config)#crypto ipsec transform-set TFS\_RB esp-aes esp-sha-hmac

6.ポリシーマップの設定を行いなさい。

　RA・・・マップ名：MAP\_RA、　シーケンス番号：1、　アクセスリスト番号：100、

　　　　　 対向ルータ：199.10.1.2、　トランスフォームセット：TFS\_RA

Router(config)#crypto map MAP\_RA 1 ipsec-isakmp

Router(config-crypto-map)#match address 100  
Router(config-crypto-map)#set peer 199.10.1.2  
Router(config-crypto-map)#set transform-set TFS\_RA   
Router\_B(config-crypto-map)#set security-association lifetime seconds 3600

　RB・・・マップ名：MAP\_RB、　シーケンス番号：1、　アクセスリスト番号：100、

　　　　　 対向ルータ：199.10.1.1、　トランスフォームセット：TFS\_RB

7.6で作成したマップをインタフェースへの適用しなさい。

　RA・・・インタフェース：g0/0/0、　マップ名：MAP\_RA

Router(config-if)#crypto map MAP\_RA

　RB・・・インタフェース：g0/0/0、　マップ名：MAP\_RB

Router(config-if)#crypto map MAP\_RB

■確認

1.PCからServerへの接続を確認しなさい。　[　確認できた　]

2.ISAKMP SAが確立されているか確認しなさい。[　確認できた　・　確認できない　]

　＊show crypto ipsec saコマンドで確認を行う。「dst」など項目が表示されれば確立されている。

3. show crypto isakmp policyコマンドでポリシーを確認しなさい。

RA:

Protection suite of priority 1

encryption algorithm: AES - Advanced Encryption Standard (128 bit keys).

hash algorithm: Secure Hash Standard

authentication method: Pre-Shared Key

Diffie-Hellman group: #2 (1024 bit)

lifetime: 3600 seconds, no volume limit  
  
RB:

Global IKE policy

Protection suite of priority 1

encryption algorithm: AES - Advanced Encryption Standard (128 bit keys).

hash algorithm: Secure Hash Standard

authentication method: Pre-Shared Key

Diffie-Hellman group: #2 (1024 bit)

lifetime: 3600 seconds, no volume limit

　[　確認できた　]

■保存・提出

1.basic\_lab02-クラス名番号.pkaでファイルを保存して、指定されたサーバ(sv23)へ提出しなさい。