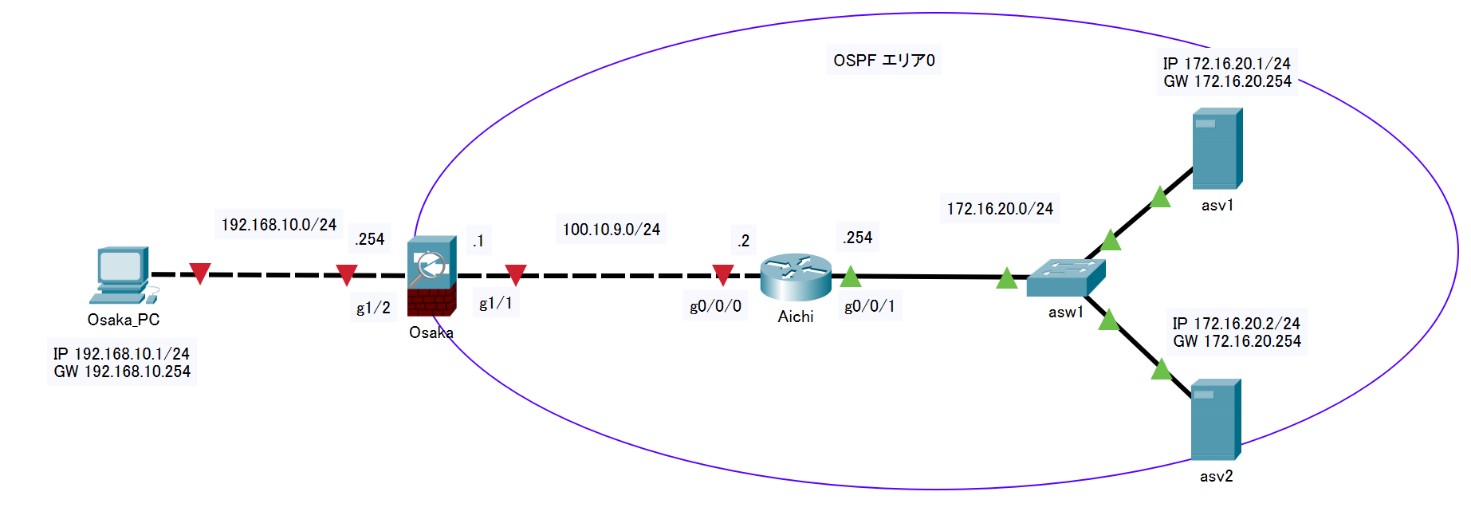
ASA(Firewall)設定

クラス名　　　　　　氏名

次のASAを利用したネットワークを構築しなさい。

＊NT22より、basic\_labo03.pkaをコピーして作成しなさい。PCは設定済み、AichiはIPアドレスのみ設定済み。

＊パスワードは設定していません。



■IPアドレスの設定

1.OsakaにIPアドレスを設定しなさい。IPアドレスは図を参照しなさい。

　g1/1・・・インターフェース名(OUTSIDE)、セキュリティレベル(20)

ciscoasa(config)#int g1/1  
ciscoasa(config-if)#ip address 100.10.9.1 255.255.255.0  
ciscoasa(config-if)#nameif OUTSIDE

ciscoasa(config-if)# security-level 20  
ciscoasa(config-if)#no shutdown

　g1/2・・・インターフェース名(INSIDE)、セキュリティレベル(50)

ciscoasa(config)#int g1/2  
ciscoasa(config-if)#ip address 192.168.10.254 255.255.255.0  
ciscoasa(config-if)#nameif INSIDE

ciscoasa(config-if)# security-level 50  
ciscoasa(config-if)#no shutdown

2.次の接続を確認しなさい。

　①Osaka\_PCとOsakaの接続を確認しなさい。[　確認できた　]

　②OsakaとAichiの接続を確認しなさい。[　確認できた　]

■OSPFの設定

1.OsakaとAichiにOSPFの設定を行いなさい。

　エリアID：0　ルータID：任意　192.168.10.0/24のルート情報はAichiには流さないこと。

Aichi (config)#router ospf 1

Aichi (config-router)#network 100.10.9.0 0.0.0.255 area 0

Aichi (config-router)#network 172.16.20.0 0.0.0.255 area 0

Osaka (config)#router ospf 1

Osaka (config-router)#network 100.10.9.0 255.255.255.0 area 0

Osaka (config-router)#network 192.168.10.0 255.255.255.0 area 0

2.OsakaでOSPFのルート情報があるか確認し、記述しなさい。＊show routeコマンド

|  |
| --- |
| 100.0.0.0/24 is subnetted, 2 subnets  C 100.0.0.0 255.255.255.0 is directly connected, OUTSIDE, GigabitEthernet1/1  C 100.10.9.0 255.255.255.0 is directly connected, OUTSIDE, GigabitEthernet1/1  C 192.168.10.0 255.255.255.0 is directly connected, INSIDE, GigabitEthernet1/2 |

3.次の接続を確認しなさい

　①Osakaとasv1の接続を確認しなさい。[　確認できた　]

　②Osakaとasv2の接続を確認しなさい。[　確認できた　]

　③Osaka\_PCとasv1の未接続を確認しなさい。[　確認できた　]

■NATの設定

1.OsakaでNATの設定を行いなさい。

ネットワークオブジェクト名・・・NAT 変更対象・・・192.168.10.0/24 変換方法・・・ダイナミック

変換先のアドレス・・・インターフェース

Osaka (config)#object network NAT

Osaka (config-network-object)#subnet 192.168.10.0 255.255.255.0

Osaka (config-network-object)#nat (inside,outside) dynamic interface

2.ICMPが通信できるようにポリシーを変更しなさい。

　クラスマップ・・・inspection\_default　　ポリシーマップ・・・global\_policy

関連付けるクラスマップ・・・inspection\_default インスペクション対象・・・icmp

＊service-policyを適用しておく（no service-policy global\_policy globalコマンドを事前に実行すること）

　　<例>service-policy ポリシーマップ名 global

Osaka (config)# policy-map global\_policy

Osaka (config-pmap)#class inspection\_default

Osaka (config-pmap-c)#inspect icmp

Osaka(config)#no service-policy global\_policy global

Osaka (config)#service-policy global\_policy global

3.次のコマンドを使用して設定を確認し、記述しなさい。　＊show xlate

|  |
| --- |
| 0 in use, 0 most used |

4.次の接続を確認しなさい

　①Osaka\_PCとasv1の接続を確認しなさい。[　確認できた　]

　②Osaka\_PCとasv2の接続を確認しなさい。[　確認できた　]

■保存・提出

1. basic\_lab03-クラス名番号.pkaで保存し、sv23に提出しなさい。