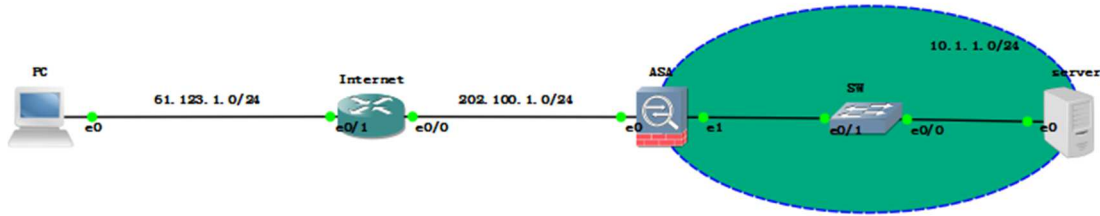


ASA 配置 EZ-VPN

一、拓扑



要求:

PC 充当 EZ-VPN 客户端, ASA 充当 EZ-VPN 服务器端, 在 ASA 上完成相关配置, 使得 PC 可以正常访问 ASA 后面的 Server。

二、配置过程:

1. IP 地址配置

其中 PC 的 IP 为 61.123.1.1/24, Internet 的地址分别为 61.123.1.10/24(e0/1) 和 202.100.1.10/24(e0/0), Server 的地址为 10.1.1.10/24, 现展示 ASA 上的配置:

```
ASA(config)#interface e0
ASA(config-if)#nameif outside
ASA(config-if)#ip address 202.100.1.1 255.255.255.0
ASA(config)#interface e0/1
ASA(config-if)#nameif inside
ASA(config-if)#ip address 10.1.1.1 255.255.255.0
```

2. 默认路由

ASA 上必须配置默认路由, 保证经过 ASA 转换的流量能够正常到达 Internet,

```
ASA(config)#route outside 0 0 202.100.1.10
```

此时, 利用 Server 进行测试:

```
Internet | ASA | server
[root@centos7 network-scripts]# ping 202.100.1.10
PING 202.100.1.10 (202.100.1.10) 56(84) bytes of data:
64 bytes from 202.100.1.10: icmp_seq=1 ttl=255 time=34.6 ms
64 bytes from 202.100.1.10: icmp_seq=2 ttl=255 time=3.85 ms

--- 202.100.1.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 3.853/19.226/34.600/15.374 ms
[root@centos7 network-scripts]#
```

3. 配置 ez-vpn 服务端

当 ASA 充当 ez-vpn 服务端时, 必须按照下面的步骤进行配置如下:

(1) 配置地址池:

当 ez-vpn 请求完成相关的认证后, 分配一个 IP 地址, 必须在 ASA 上定义一个地址池,

```
ASA(config)#ip local pool POOL 123.1.1.100-123.1.1.200
```

(2) 配置 Tunnel-group

当 ez-vpn 请求发起后, 总会对应一个 tunnel-group, 由 tunnel-group 决定其采用什么方式认证, 当然 ez-vpn 中也存在一个默认的 tunnel-group。

①配置类型属性

```
ASA(config)#tunnel-group IPSEC_GROUP type remote-access
```

//定义其类型为 remote-access，其中 remote-access 对应于 ez-vpn 和 ssl-vpn。

②配置加密属性

```
ASA(config)#tunnel-group IPSEC_GROUP ipsec-attributes
```

```
ASA(config-tunnel-ipsec)#pre-shared-key CISCO //有的 ASA 为 ikev1 pre-shared-key CISCO
```

//定义 tunnel-group 的加密属性为预共享密钥

③配置一般属性

※这里之所以将 tunnel-group 的众多属性，如加密属性和普通属性分开，是由于 tunnel-group 不仅可以用于 ez-vpn，还可以用于其它的 vpn，为了一个 tunnel-group 能适应多种 vpn，故将其众多属性分开。

```
ASA(config)#tunnel-group IPSEC_GROUP general-attributes
```

```
ASA(config-tunnel-ipsec)#address-pool POOL
```

④定义加密方式

该加密方式用于第一阶段的加密，和普通的 ipsec-vpn 是一样的。

```
ASA(config)#username IPSECUSER password CISCO
```

```
ASA(config)#crypto isakmp enable outside //这句配置时 ASA 无反应，必须直接配
```

```
ASA(config)#crypto isakmp policy 10
```

```
ASA(config-ikev1-policy)# authentication pre-share
```

```
ASA(config-ikev1-policy)# encryption des
```

```
ASA(config-ikev1-policy)# hash md5
```

```
ASA(config-ikev1-policy)# group 2
```

```
ASA(config-ikev1-policy)# exit
```

⑤配置转换集

```
ASA(config)# crypto ipsec transform-set CISCO esp-des esp-md5-hmac
```

⑥配置动态 map，调用转换集

```
ASA(config)# crypto dynamic DYMAP 10 set transform-set CISCO
```

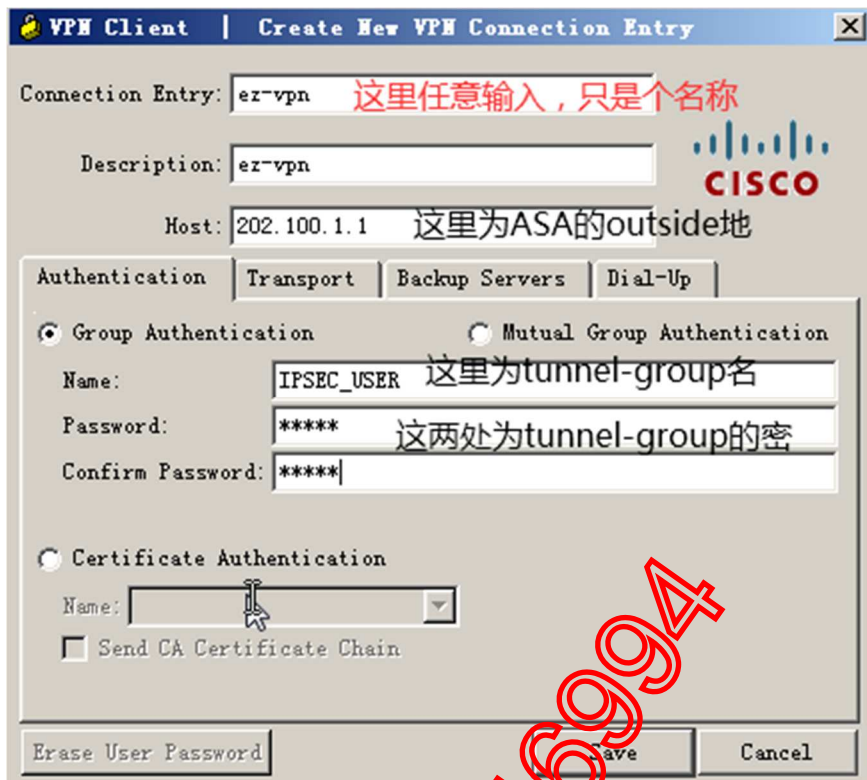
⑦配置静态 map，调用动态 map

```
ASA(config)# crypto map CCIE 10 ipsec-isakmp dynamic DYMAP
```

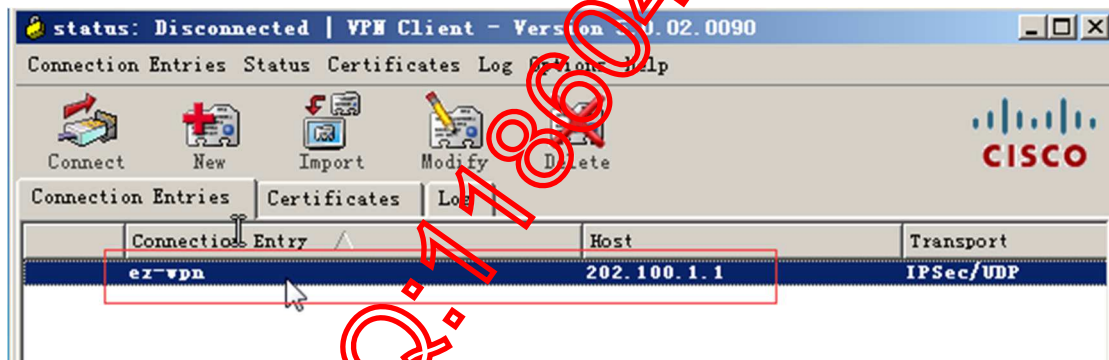
⑧接口调用静态转换集

```
ASA(config)# crypto map CCIE interface outside
```

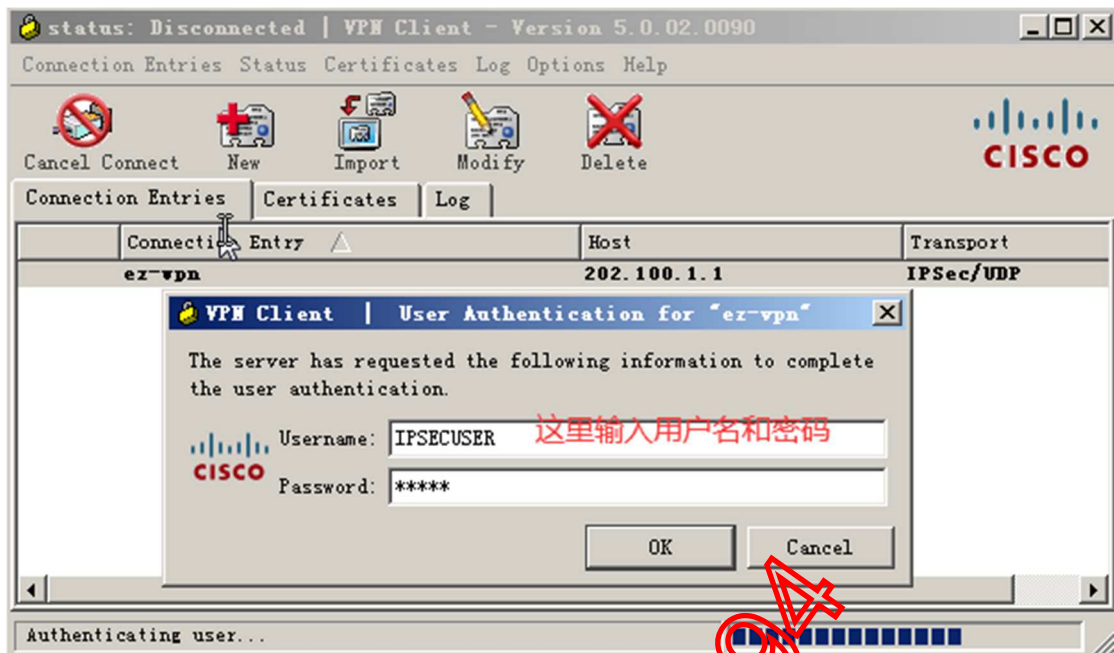
此时，在 PC 上可以登录到 ez-vpn，



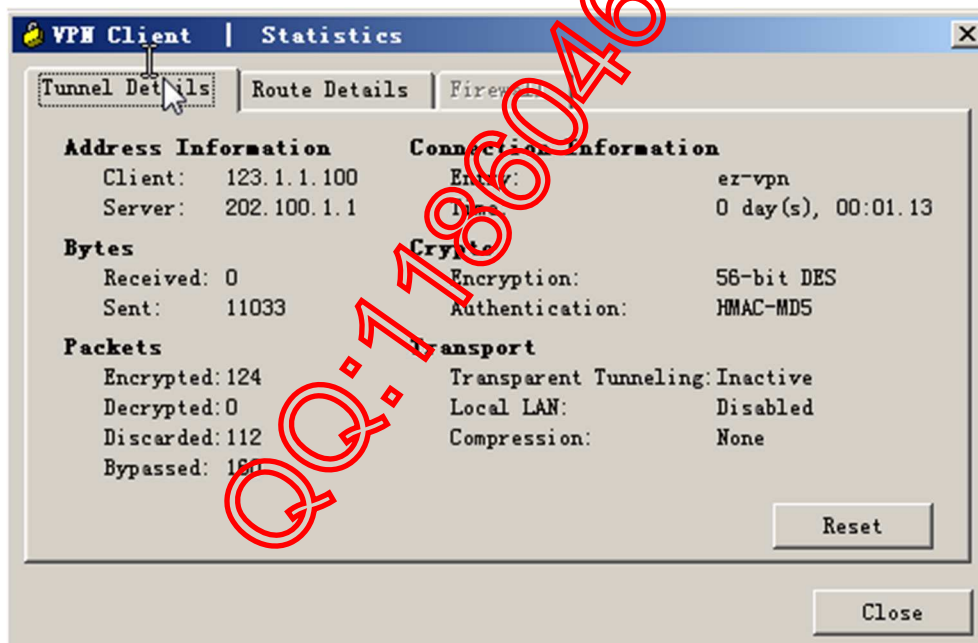
当输入对应的 tunnel-group 名称和密钥之后，就会生成



然后双击上面的 ez-vpn 条目“ez-vpn”，出现



输入相应的用户名和密码后，则 ez-vpn 会拨号成功。



可以看到拨号成功的相关信息，此时再访问内部的服务器 10.1.1.1/24，



※经过测试，发现如果在 ASA 上做了针对 Server 的 NAT 后，则无法用 PC 访问 Server。