REMOTE ACCESS VPN NETWORK DIAGRAM
HQ ASA Firewall As Remote Access VPN Server

Notes:

________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________

From Cisco VPN Reference Guide For Field Engineer

Configuring ASA Firewall As Remote Access VPN Server
Scenario 2 - (configuration is based on Figure 7)

1.1 Configuring ASA Firewall as Remote Access VPN Server

HQ ASA Firewall Configuration

Objective 1: Configuring ISAKMP Policy

Step 1

Enabling ISAKMP command

HQ-ASA(config)# isakmp enable outside

Step 2

Define authentication for pre-shared keys

HQ_Firewall(config)# isakmp policy 10 authentication pre-share

Step 3

Define encryption type DES, 3DES or AES (AES default value is 128. You may adjust it to AES-192 or AES-256 for higher security but it will affect your router CPU performance. DES encryption is not secure and do not use AES-192 as Cisco VPN Client unable to support this encryption.

HQ_Firewall(config)# isakmp policy 10 encryption aes

Step 4

Define hashing method either using md5 or sha. In this scenario, we will use sha as the hashing method.

HQ_Firewall (config)# isakmp policy 10 hash sha

Step 5

Define a pre-shared key and netmask for remote access VPN client. In this scenario, we will use “cisco” as the pre-shared key.

HQ_Firewall(config)# isakmp key cisco address 0.0.0.0 netmask 0.0.0.0
Objective 2: Configuring Local DHCP Pool For Remote VPN Client

Step 1
Define the local pool for remote access VPN clients.

HQ_Firewall(config)# ip local pool vpnpool 192.168.1.10 – 192.168.1.254
HQ_Firewall(config)# tunnel-group MYGROUP general-attributes
HQ_Firewall(config-general)# address-pool vpnpool

Objective 3: Configuring Attributes For Remote Access VPN Client

Step 1
Define the tunnel group name and type for remote access group VPN users. In this scenario, we will use the group name as MYGROUP with the pre-shared key of “cisco”. The type of tunnel group is “ipsec-ra” or IPSec remote access.

HQ_Firewall(config)# tunnel-group MYGROUP type ipsec-ra
HQ_Firewall(config)# tunnel-group MYGROUP ipsec-attributes
HQ_Firewall(config-ipsec)# pre-shared-key cisco

Objective 4: Configuring Username For Remote Access VPN Client

Configure users credentials for remote access VPN client. Remote users will use this local credentials for authentication. In this scenario, we will configure two user names and password with local authentication of LOCAL.

Step 1
HQ_Firewall(config)# username gizmo password cisco
HQ_Firewall(config)# username blade password cisco
HQ_Firewall(config)# tunnel-group MYGROUP general-attributes
HQ_Firewall(config-group-policy)# authentication-server-group LOCAL
Objective 5: Configuring IPSec Policy For Remote Access VPN Client

Define the IPSec policy name, encryption type and hashing method. The data flow between remote sites will be encrypted by the IPSec policy. In this scenario, we will use “HQSET” as the transform set name and the encryption used is as follow.

Step 1

HQ_Firewall(config)# crypto ipsec HQSET esp-aes esp-sha-hmac

Objective 6: Configuring Dynamic Crypto Map For Remote Access VPN Client

Home users or telecommuters are always able to establish connection to the HQ by using VPN client regardless of where they are. However, for home users and telecommuters that get internet connection from ISPs always get dynamic IP addresses. Unlike site to site VPN, static IP addresses are compulsory in order for it to work. Dynamic crypto map is very powerful as it can learn home user and telecommuters dynamic IP addresses. In this scenario, we will use “HQDYNMAP” as the dynamic crypto map name and bind it to transform set created at Objective 5.

Step 1

HQ_Firewall(config)# crypto dynamic-map HQDYNMAP 10 set transform-set HQSET

Objective 7: Configuring Crypto Map For Remote Access VPN

The crypto map will bind to dynamic map as shown below. In this scenario, we will use “MYMAP” as the crypto map name with the sequence number of 10

Step 1

HQ_Firewall(config)# crypto map MYMAP 10 ipsec-isakmp dynamic HQDYNMAP
Step 2

Apply the crypto map to the outside interface.

HQ_Firewall(config)# crypto map MYMAP interface outside

Objective 7: Creating Access-List To Exempt NAT

Exempt the VPN clients pool from being NAT to the ASA local LAN IP addresses. Nat 0 will prevent NAT process.

HQ_Firewall(config)# access-list 100 extended permit ip 172.16.50.0 255.255.255.0 192.168.1.0 255.255.255.0

HQ_Firewall(config)# nat (inside) 0 access-list 100

Objective 8: Configuring Explicit Permit Of IPSEC Traffic

Allow the IPSec traffic from being filter by the firewall.

HQ_Firewall(config)# sysopt connection permit-ipsec
**Objective 8: Configuring Client PC for Cisco VPN Client**

Notes: Cisco VPN Client software must be downloaded from Cisco official Website. CCO account is needed in order to download Cisco VPN Client.

**Step 1**

Run the Cisco VPN client setup file as shown below

![File List](image)
Step 2
Click “next” to proceed

Step 3
Accept the license agreement and click “next”
**Step 4**

Confirmed the destination folder and click “next”

![Destination Folder Dialog](image1)

**Step 5**

Click “next” to proceed

![Application Ready for Installation Dialog](image2)
**Step 6**

Allow the system update to run

![System update window](image1)

**Step 7**

The software is installing network components for Cisco VPN client to work

![Network components installation window](image2)

*Configuring ASA Firewall As Remote Access VPN Server*
**Step 8**

Click “Finish”

![Image of Cisco Systems VPN Client installation completion](image1)

**Step 9**

The system will prompt user to restart the PC after installation is completed. Click “yes” to restart

![Image of Installer Information window](image2)
Step 10

Select the Cisco VPN Client folder and start the Cisco VPN Client program

Step 11

Click “New” to create a new connection
Step 12

Insert the info accordingly as configured in the router and click “save”

Step 13

Key in the username and password. You may use “nemo” or “shrek” as configured in the router
Step 14

Go to the VPN “statistics” and under the tunnel details, VPN Client shows that packets are decrypted and encrypted successfully

* The above output shown that the encrypted traffic between both sides has been successful.