Secure Network Architecture Configuration

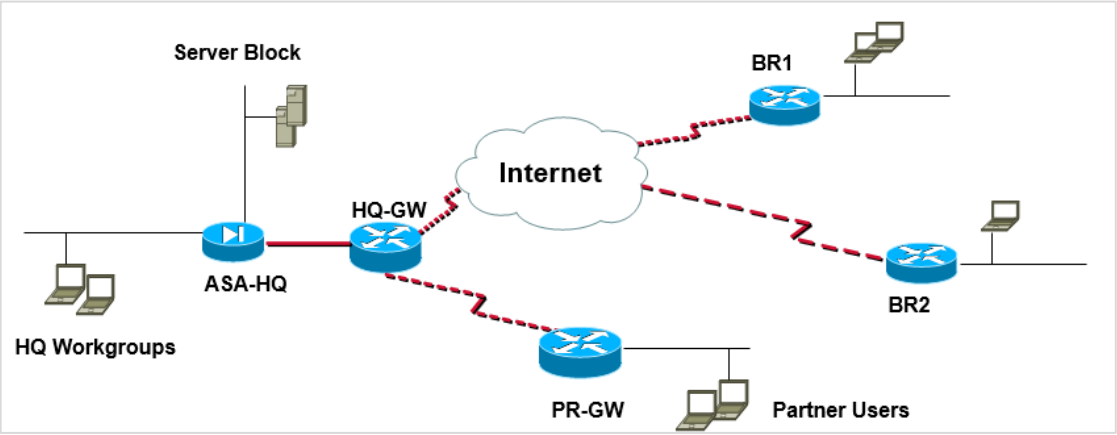
Jordan Patterson

This Document contains an example of the configuration required for the implementation of a secure network including the configuration of IPSEC VPN

Contents

1. Project Requirements

A. IP Address Scheme design.



B. Apply static IP routes on all gateways (you may use OSPF as well).

C. ASA_HQ security level zones, NAT policy creation

D. IPsec VPNs.

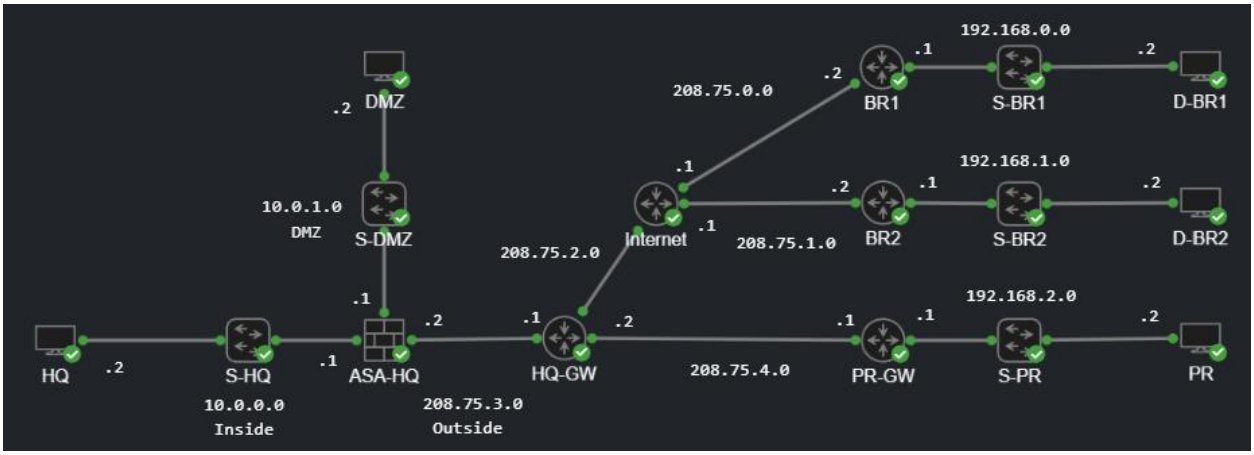
   1. Between HQ-GW and BR1 (ESP)
   2. Between HQ-GW and BR2 (AH)

E. Access Control and conduit policy.

   1. All users access to Server Block
   2. Branch users are allowed to visit HQ workgroups.
   3. Partner users can only visit Server Block.

2. Logical Network Map

The provided network design was implemented into CML (Cisco Modeling Labs) as follows:



3. System List

The devices configured and their respective IP addresses were configured as follows:

System/Device	Model	Interface	IP Address	Operating System	Memory/ CPU
Desktop/HQ	VM	Eth0	10.0.0.2/24	Alpine Linux 14.2	512M /vCPU
Switch/S-HQ	VSwitch	G0/0	-	IOSv 15.2	722M/vCPU
		G0/1	-		
Server/DMZ	VM	Eth0	10.0.1.2/24	Alpine Linux 14.2	512M /vCPU
Switch/S-DMZ	VSwitch	G0/0	-	IOSv 15.2	722M/vCPU
		G0/1			
ASA/ASA-HQ	ASAv	G0/0	10.0.0.1/24	Cisco ASA 9.16	2048 MB/ Xeon 4100
		G0/1	10.0.1.1/24		
		G0/2	208.75.3.2/24		
Router/HQ-GW	vRouter	G0/0	208.75.2.2/24	IOSv 15.2	449M/vCPU
		G0/1	208.75.3.1/24		
		G0/3	208.75.4.2/24		
Router/Internet	VRouter	G0/0	208.75.2.1/24	IOSv 15.2	449M/vCPU
		G0/1	208.75.0.1/24		
		G0/2	208.75.1.1/24		
Router/BR1	VRouter	G0/0	192.168.0.1	IOSv 15.2	449M/vCPU
		G0/1	208.75.0.2		
Switch/S-BR1	VSwitch	G0/0	-	IOSv 15.2	722M/vCPU
		G0/1	-		
Desktop/D-BR1	VM	Eth0	192.168.0.2	Alpine Linux 14.2	512M /vCPU
Router/BR2	VRouter	G0/0	192.168.1.1	IOSv 15.2	449M/vCPU
		G0/1	208.75.1.2		
Switch/S-BR2	VSwitch	G0/0	-	IOSv 15.2	722M/vCPU
		G0/1	-		
Desktop/D-BR2	VM	Eth0	192.168.1.2	Alpine Linux 14.2	512M /vCPU
Router/PR-GW		G0/0	192.168.2.1	IOSv 15.2	449M/vCPU
		G0/1	208.75.1.2		
Switch/S-PR	VSwitch	G0/0	-	IOSv 15.2	722M/vCPU
		G0/1	-		
Desktop/PR	VM	Eth0	192.168.2.2	Alpine Linux 14.2	512M /vCPU

4. IP Routing Configuration

For the IP routing configuration, OSPF and static routing was configured as follows:

System/Device	OSPF	Static Route
Router/BR1	router ospf 1 network 192.168.0.0 0.0.0.255 area 0 network 208.75.0.0 0.0.0.255 area 0	-
Router/BR2	router ospf 1 network 192.168.1.0 0.0.0.255 area 0 network 208.75.1.0 0.0.0.255 area 0	-
Router/PR-GW	router ospf 1 network 192.168.2.0 0.0.0.255 area 0 network 208.75.4.0 0.0.0.255 area 0	ip route 10.0.0.0 255.255.255.0 208.75.4.2
Router/Internet	router ospf 1 network 208.75.0.0 0.0.0.255 area 0 network 208.75.1.0 0.0.0.255 area 0 network 208.75.2.0 0.0.0.255 area 0	-
Router/HQ-GW	router ospf 1 network 208.75.2.0 0.0.0.255 area 0 network 208.75.3.0 0.0.0.255 area 0 network 208.75.4.0 0.0.0.255 area 0	ip route 10.0.0.0 255.255.255.0 208.75.3.2
ASA/ASA-HQ	-	route outside 0.0.0.0 0.0.0.0 208.75.3.1 1

The routing tables resulting from the configuration in the table above are the following[1]:

System/Device	Routing Table
Router/BR1	10.0.0.0/24 is subnetted, 1 subnets S 10.0.0.0 [10/0] via 208.75.2.2 192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks C 192.168.0.0/24 is directly connected, GigabitEthernet0/0 L 192.168.0.1/32 is directly connected, GigabitEthernet0/0 O 192.168.1.0/24 [110/3] via 208.75.0.1, 01:37:59, GigabitEthernet0/1 O 192.168.2.0/24 [110/4] via 208.75.0.1, 01:37:59, GigabitEthernet0/1 208.75.0.0/24 is variably subnetted, 2 subnets, 2 masks C 208.75.0.0/24 is directly connected, GigabitEthernet0/1 L 208.75.0.2/32 is directly connected, GigabitEthernet0/1 O 208.75.1.0/24 [110/2] via 208.75.0.1, 01:42:26, GigabitEthernet0/1 O 208.75.2.0/24 [110/2] via 208.75.0.1, 01:37:59, GigabitEthernet0/1 S 208.75.3.0/24 [10/0] via 208.75.2.2 O 208.75.4.0/24 [110/3] via 208.75.0.1, 01:37:59, GigabitEthernet0/1
Router/BR2	10.0.0.0/24 is subnetted, 1 subnets S 10.0.0.0 [10/0] via 208.75.2.2 O 192.168.0.0/24 [110/3] via 208.75.1.1, 01:38:45, GigabitEthernet0/2 192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks C 192.168.1.0/24 is directly connected, GigabitEthernet0/0 L 192.168.1.1/32 is directly connected, GigabitEthernet0/0 O 192.168.2.0/24 [110/4] via 208.75.1.1, 01:38:45, GigabitEthernet0/2 O 208.75.0.0/24 [110/2] via 208.75.1.1, 01:38:45, GigabitEthernet0/2 208.75.1.0/24 is variably subnetted, 2 subnets, 2 masks C 208.75.1.0/24 is directly connected, GigabitEthernet0/2 L 208.75.1.2/32 is directly connected, GigabitEthernet0/2 O 208.75.2.0/24 [110/2] via 208.75.1.1, 01:38:45, GigabitEthernet0/2 S 208.75.3.0/24 [10/0] via 208.75.2.2 O 208.75.4.0/24 [110/3] via 208.75.1.1, 01:38:45, GigabitEthernet0/2

[1] The are additional static routes in the routing table that were added as part of the VPN configuration in section 6.

System/Device	Routing Table
Router/PR-GW	10.0.0.0/24 is subnetted, 1 subnets S 10.0.0.0 [1/0] via 208.75.4.2 O 192.168.0.0/24 [110/4] via 208.75.4.2, 01:39:16, GigabitEthernet0/3 O 192.168.1.0/24 [110/4] via 208.75.4.2, 01:39:26, GigabitEthernet0/3 192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks C 192.168.2.0/24 is directly connected, GigabitEthernet0/0 L 192.168.2.1/32 is directly connected, GigabitEthernet0/0 O 208.75.0.0/24 [110/3] via 208.75.4.2, 01:39:26, GigabitEthernet0/3 O 208.75.1.0/24 [110/3] via 208.75.4.2, 01:39:26, GigabitEthernet0/3 O 208.75.2.0/24 [110/2] via 208.75.4.2, 01:39:26, GigabitEthernet0/3 O 208.75.3.0/24 [110/2] via 208.75.4.2, 00:24:52, GigabitEthernet0/3 208.75.4.0/24 is variably subnetted, 2 subnets, 2 masks C 208.75.4.0/24 is directly connected, GigabitEthernet0/3 L 208.75.4.1/32 is directly connected, GigabitEthernet0/3
Router/Internet	O 192.168.0.0/24 [110/2] via 208.75.0.2, 01:40:35, GigabitEthernet0/1 O 192.168.1.0/24 [110/2] via 208.75.1.2, 01:40:45, GigabitEthernet0/2 O 192.168.2.0/24 [110/3] via 208.75.2.2, 01:40:55, GigabitEthernet0/0 208.75.0.0/24 is variably subnetted, 2 subnets, 2 masks C 208.75.0.0/24 is directly connected, GigabitEthernet0/1 L 208.75.0.1/32 is directly connected, GigabitEthernet0/1 208.75.1.0/24 is variably subnetted, 2 subnets, 2 masks C 208.75.1.0/24 is directly connected, GigabitEthernet0/2 L 208.75.1.1/32 is directly connected, GigabitEthernet0/2 208.75.2.0/24 is variably subnetted, 2 subnets, 2 masks C 208.75.2.0/24 is directly connected, GigabitEthernet0/0 L 208.75.2.1/32 is directly connected, GigabitEthernet0/0 O 208.75.3.0/24 [110/2] via 208.75.2.2, 01:40:55, GigabitEthernet0/0 O 208.75.4.0/24 [110/2] via 208.75.2.2, 01:40:55, GigabitEthernet0/0
Router/HQ-GW	10.0.0.0/24 is subnetted, 1 subnets S 10.0.0.0 [1/0] via 208.75.3.2 S 192.168.0.0/24 [10/0] via 208.75.0.2 S 192.168.1.0/24 [10/0] via 208.75.1.2 O 192.168.2.0/24 [110/2] via 208.75.4.1, 02:10:08, GigabitEthernet0/3 O 208.75.0.0/24 [110/2] via 208.75.2.1, 01:41:14, GigabitEthernet0/0 O 208.75.1.0/24 [110/2] via 208.75.2.1, 01:41:14, GigabitEthernet0/0 208.75.2.0/24 is variably subnetted, 2 subnets, 2 masks C 208.75.2.0/24 is directly connected, GigabitEthernet0/0 L 208.75.2.2/32 is directly connected, GigabitEthernet0/0
ASA/ASA-HQ	S* 0.0.0.0 0.0.0.0 [1/0] via 208.75.3.1, outside C 10.0.0.0 255.255.255.0 is directly connected, inside L 10.0.0.1 255.255.255.255 is directly connected, inside C 10.0.1.0 255.255.255.0 is directly connected, dmz L 10.0.1.1 255.255.255.255 is directly connected, dmz C 208.75.3.0 255.255.255.0 is directly connected, outside L 208.75.3.2 255.255.255.255 is directly connected, outside

5. ASA Configuration

According to the requirements, three zones are connected to the firewall: Inside (HQ Workgroup), DMZ (Server Block) and the outside which connects to the HQ border router.

5.1 Security Zones

The mentioned security zones were configured as follows:

Security Zone	Security Level	Interface

Inside	*security-level 100*	`interface GigabitEthernet0/0`
		` nameif inside`
		` security-level 100`
		` ip address 10.0.0.1 255.255.255.0`

Outside	*security-level 0*	`interface GigabitEthernet0/2`
		` nameif outside`
		` security-level 0`
		` ip address 208.75.3.2 255.255.255.0`

DMZ	*security-level 50*	`interface GigabitEthernet0/1`
		` nameif dmz`
		` security-level 50`
		` ip address 10.0.1.1 255.255.255.0`

5.2 Access Control List (ACL)

Additionally, access control list rules were configured to meet the requirements for the connections between Branch 1 users (BR1) and HQ, Branch 2 users (BR2) and HQ, and between Partner Users (PR) and HQ.

Rule	Interface	ACL
Allow incoming connections from any IP address into host 10.0.1.2 (DMZ Server).	`access-group ACL-OUTSIDE in interface outside`	`access-list ACL-OUTSIDE extended permit ip any host 10.0.1.2`
Allow incoming connections from network 192.168.0.0/24 (BR1) into the network 10.0.0.0/24 (HQ Workgroup)	`access-group ACL-OUTSIDE in interface outside`	`access-list ACL-OUTSIDE extended permit ip 192.168.0.0 255.255.255.0 10.0.0.0 255.255.255.0`
Allow incoming connections from network 192.168.1.0/24 (BR2) into the network 10.0.0.0/24 (HQ Workgroup)	`access-group ACL-OUTSIDE in interface outside`	`access-list ACL-OUTSIDE extended permit ip 192.168.1.0 255.255.255.0 10.0.0.0 255.255.255.0`

5.3 Network address translation (NAT)

For the NAT configuration, the following configuration was used:

Translation	Configuration

Translate DMZ server IP address 10.0.1.2/24 into the static public IP address 208.75.3.3/24 on the outside interface.	`object network net-dmz`
	` host 10.0.1.2`
	`object network net-dmz`
	` nat (dmz,outside) static 208.75.3.3`

Translate HQ workgroup network address 10.0.0.0/24 into their same network address facing outside interface (identity nat)	`object network net-inside`
	` subnet 10.0.0.0 255.255.255.0`
	`object network net-inside`
	` nat (inside,outside) static net-inside`

The resulting translation table from the configuration above is the following:

```
ASA-HQ# show xlate
2 in use, 2 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from dmz:10.0.1.2 to outside:208.75.3.3
    flags s idle 3:47:58 timeout 0:00:00
NAT from inside:10.0.0.0/24 to outside:10.0.0.0/24
    flags sI idle 3:48:16 timeout 0:00:00
```

6. IPSec Policy-Based VPN Configuration

According to the requirements, two types of Policy-Based VPN configurations were required: ESP for the VPN between BR1 and HQ, and AH between BR2 and HQ.

6.1 Encapsulating security payload (ESP)

First, we defined an access control list (ACL) to match all the traffic we want to send through the VPN between the two routers.

System/Device	Rule	ACL Configuration

Router/BR1	Allows all IP traffic originating from network 192.168.0.0/24 (BR1) reach any devices in the network 208.75.3.0/27 (ASA HQ outside network) or network 10.0.0.0/24 (HQ Workgroup)	`ip access-list extended BR1_to_HQ`
		` permit ip 192.168.0.0 0.0.0.255 208.75.3.0 0.0.0.255`
		` permit ip 192.168.0.0 0.0.0.255 10.0.0.0 0.0.0.255`

Router/HQ-GW	Allows all IP traffic originating from network 208.75.3.0/27 (ASA HQ outside network) or network 10.0.0.0/24 (HQ Workgroup) to reach any devices in the network 192.168.0.0/24 (BR1)	`ip access-list extended HQ_to_BR1`
		` permit ip 208.75.3.0 0.0.0.255 192.168.0.0 0.0.0.255`
		` permit ip 10.0.0.0 0.0.0.255 192.168.0.0 0.0.0.255`

Later, we configured the routers to authenticate one another (via ISAKMP) using a pre-shared key. To achieve this, we created a keyring to hold our pre-shared keys, which are mapped by peer (public) IP addresses.

System/Device	Keyring Configuration
Router/BR1	`crypto keyring VPN1` `  pre-shared-key address 208.75.2.2 key lerolero`
Router/HQ-GW	`crypto keyring VPN1` `  pre-shared-key address 208.75.0.2 key lerolero`

Next, we created an ISAKMP policy that sets the parameters which will be used by routers during IKE (key exchange) phase one. The policy used in this case employs 256-bit AES using pre-shared key authentication and Diffie-Hellman group five.

System/Device	Policy Configuration

Router/BR1	`crypto isakmp policy 10`
	` encr aes 256`
	` authentication pre-share`
	` group 5`

Router/HQ-GW	`crypto isakmp policy 1`
	` encr aes 256`
	` authentication pre-share`
	` group 5`

After this, ISAKMP profiles were created to establish parameters for a particular ISAKMP peer by matching its outside IP address. We specify the keyring to be used for this peer so that the router knows how to locate the correct pre-shared key.

System/Device	Policy Configuration

Router/BR1	`crypto isakmp profile BR_to_HQ`
	`   keyring VPN1`
	`   match identity address 208.75.2.2 255.255.255.255`

Router/HQ-GW	`crypto isakmp profile HQ_to_BR1`
	`   keyring VPN1`
	`   match identity address 208.75.0.2 255.255.255.255`

After finishing the configuration for ISAKMP, the next step is to configure the IPSEC. To do this, we need to define an IPsec transform set that tells the router what protocol, encryption and hashing algorithms to use when forming the IPSEC SA.

According to the requirements, in this case we are using ESP with 256-bit AES and SHA-1 hashing) in tunnel mode.

System/Device	Transform set configuration
Router/BR1	`crypto ipsec transform-set ESP-AES256-SHA1 esp-aes 256 esp-sha-hmac` ` mode tunnel`
Router/HQ-GW	`crypto ipsec transform-set ESP-AES256-SHA1 esp-aes 256 esp-sha-hmac` ` mode tunnel`

Finally, we create a crypto map by tying all the configurations previously defined and applying it to the desired network interface.

System/Device	Crypto map configuration	Interface

Router/BR1	`crypto map VPN1 10 ipsec-isakmp`
	` set peer 208.75.2.2`
	` set transform-set ESP-AES256-SHA`
	` set reverse-route distance 10`
	` set isakmp-profile BR_to_HQ`
	` match address BR1_to_HQ`
	` reverse-route static`
		`interface GigabitEthernet0/1`
		` ip address 208.75.0.2 255.255.255.0`
		` duplex auto`
		` speed auto`
		` media-type rj45`
		` crypto map VPN1`

Router/HQ-GW	`crypto map VPN 1 ipsec-isakmp`
	` set peer 208.75.0.2`
	` set transform-set ESP-AES256-SHA1`
	` set reverse-route distance 10`
	` set isakmp-profile HQ_to_BR1`
	` match address HQ_to_BR1`
	` reverse-route static`
		`interface GigabitEthernet0/0`
		` ip address 208.75.2.2 255.255.255.0`
		` duplex auto`
		` speed auto`
		` media-type rj45`
		` crypto map VPN`

To verify if the VPN connection is correctly established, we generated traffic both ways (Between HQ and BR1) and reviewed the status of the negotiation using *'show crypto ISAKMP SA status'*

System/Device	Crypto ISAKMP SA status

Router/BR1	`BR1#sh cry isa sa`
	`IPv4 Crypto ISAKMP SA`
	`dst  src  state  conn-id status`
	`208.75.2.2  208.75.0.2  QM_IDLE  1001 ACTIVE`

Router/HQ-GW	`HQ-GW#sh cry isa sa`
	`IPv4 Crypto ISAKMP SA`
	`dst  src  state  conn-id status`
	`208.75.2.2  208.75.0.2  QM_IDLE  1001 ACTIVE`

We verified the status of the sessions using *'show crypto session'*

System/Device	Crypto Session
Router/BR1	Interface: GigabitEthernet0/1 Profile: BR_to_HQ Session status: UP-IDLE Peer: 208.75.2.2 port 500 Session ID: 0 IKEv1 SA: local 208.75.0.2/500 remote 208.75.2.2/500 Active IPSEC FLOW: permit ip 192.168.0.0/255.255.255.0 10.0.0.0/255.255.255.0 Active SAs: 0, origin: crypto map IPSEC FLOW: permit ip 192.168.0.0/255.255.255.0 208.75.3.0/255.255.255.0 Active SAs: 0, origin: crypto map
Router/HQ-GW	Interface: GigabitEthernet0/0 Profile: HQ_to_BR1 Session status: UP-IDLE Peer: 208.75.0.2 port 500 Session ID: 0 IKEv1 SA: local 208.75.2.2/500 remote 208.75.0.2/500 Active IPSEC FLOW: permit ip 10.0.0.0/255.255.255.0 192.168.0.0/255.255.255.0 Active SAs: 0, origin: crypto map IPSEC FLOW: permit ip 208.75.3.0/255.255.255.0 192.168.0.0/255.255.255.0 Active SAs: 0, origin: crypto map

Additionally, we verified the currently active IPsec SA using *'show crypto ipsec sa'*

System/Device	IPsec security associations
Router/BR1	inbound esp sas: spi: 0x6785797E(1736800638) transform: esp-256-aes esp-sha-hmac , in use settings ={Tunnel, } conn id: 21, flow_id: SW:21, sibling_flags 80004040, crypto map: VPN1 sa timing: remaining key lifetime (k/sec): (4275427/3594) IV size: 16 bytes replay detection support: Y Status: ACTIVE(ACTIVE) outbound esp sas: spi: 0xE75F3B61(3881778017) transform: esp-256-aes esp-sha-hmac , in use settings ={Tunnel, } conn id: 22, flow_id: SW:22, sibling_flags 80004040, crypto map: VPN1 sa timing: remaining key lifetime (k/sec): (4275427/3594) IV size: 16 bytes replay detection support: Y Status: ACTIVE(ACTIVE)
Router/HQ-GW	inbound esp sas: spi: 0xE75F3B61(3881778017) transform: esp-256-aes esp-sha-hmac , in use settings ={Tunnel, } conn id: 37, flow_id: SW:37, sibling_flags 80000040, crypto map: VPN sa timing: remaining key lifetime (k/sec): (4357419/3496) IV size: 16 bytes replay detection support: Y Status: ACTIVE(ACTIVE) outbound esp sas: spi: 0x6785797E(1736800638) transform: esp-256-aes esp-sha-hmac , in use settings ={Tunnel, } conn id: 38, flow_id: SW:38, sibling_flags 80000040, crypto map: VPN sa timing: remaining key lifetime (k/sec): (4357419/3496) IV size: 16 bytes replay detection support: Y Status: ACTIVE(ACTIVE)

6.2 Authentication header (AH)

First, we defined an access control list (ACL) to match all the traffic we want to send through the VPN between the two routers.

System/Device	Rule	ACL Configuration

Router/BR2	Allows all IP traffic originating from network 192.168.1.0/24 (BR1) reach any devices in the network 208.75.3.0/27 (ASA HQ outside network) or network 10.0.0.0/24 (HQ Workgroup)	`ip access-list extended BR2_to_HQ`
		` permit ip 192.168.1.0 0.0.0.255 208.75.3.0 0.0.0.255`
		` permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.0.255`

Router/HQ-GW	Allows all IP traffic originating from network 208.75.3.0/27 (ASA HQ outside network) or network 10.0.0.0/24 (HQ Workgroup) to reach any devices in the network 192.168.1.0/24 (BR1)	`ip access-list extended HQ_to_BR2`
		` permit ip 208.75.3.0 0.0.0.255 192.168.1.0 0.0.0.255`
		` permit ip 10.0.0.0 0.0.0.255 192.168.1.0 0.0.0.255`

Later, we configured the routers to authenticate one another (via ISAKMP) using a pre-shared key. To achieve this, we created a keyring to hold our pre-shared keys, which are mapped by peer (public) IP addresses.

System/Device	Keyring Configuration
Router/BR2	`crypto keyring VPN2` `  pre-shared-key address 208.75.2.2 key lerolero`
Router/HQ-GW	`crypto keyring VPN2` `  pre-shared-key address 208.75.1.2 key lerolero`

Next, we created an ISAKMP policy that sets the parameters which will be used by routers during IKE (key exchange) phase one. The policy used in this case employs 256-bit AES using pre-shared key authentication and Diffie-Hellman group five.

System/Device	Policy Configuration

Router/BR2	`crypto isakmp policy 10`
	` encr aes 256`
	` authentication pre-share`
	` group 5`

Router/HQ-GW	`crypto isakmp policy 2`
	` encr aes 256`
	` authentication pre-share`
	` group 5`

After this, ISAKMP profiles were created to establish parameters for a particular ISAKMP peer by matching its outside IP address. We specify the keyring to be used for this peer so that the router knows how to locate the correct pre-shared key.

System/Device	Policy Configuration

Router/BR2	`crypto isakmp profile BR2_to_HQ`
	`  keyring VPN2`
	`  match identity address 208.75.2.2 255.255.255.255`

Router/HQ-GW	`crypto isakmp profile HQ_to_BR2`
	`  keyring VPN2`
	`  match identity address 208.75.1.2 255.255.255.255`

After finishing the configuration for ISAKMP, the next step is to configure the IPSEC. To do this, we need to define an IPsec transform set that tells the router what protocol, encryption and hashing algorithms to use when forming the IPSEC SA.

According to the requirements, in this case, we are using AH with SHA256 hashing in tunnel mode.

System/Device	Transform set configuration
Router/BR2	`crypto ipsec transform-set AH-SHA256-HMAC ah-sha256-hmac` ` mode tunnel`
Router/HQ-GW	`crypto ipsec transform-set AH-SHA256-HMAC ah-sha256-hmac` ` mode tunnel`

Finally, we create a crypto map by tying all the configurations previously defined and applying it to the desired network interface.

System/Device	Crypto map configuration	Interface

Router/BR2	`crypto map VPN2 10 ipsec-isakmp`
	` set peer 208.75.2.2`
	` set transform-set AH-SHA256-HMAC`
	` set reverse-route distance 10`
	` set isakmp-profile BR2_to_HQ`
	` match address BR2_to_HQ`
	` reverse-route static`
		`interface GigabitEthernet0/2`
		` ip address 208.75.1.2 255.255.255.0`
		` duplex auto`
		` speed auto`
		` media-type rj45`
		` crypto map VPN2`

Router/HQ-GW	`crypto map VPN 2 ipsec-isakmp`
	` set peer 208.75.1.2`
	` set transform-set AH-SHA256-HMAC`
	` set reverse-route distance 10`
	` set isakmp-profile HQ_to_BR2`
	` match address HQ_to_BR2`
	` reverse-route static`
		`interface GigabitEthernet0/0`
		` ip address 208.75.2.2 255.255.255.0`
		` duplex auto`
		` speed auto`
		` media-type rj45`
		` crypto map VPN`

To verify if the VPN connection is correctly established, we generated traffic both ways (Between HQ and BR2) and reviewed the status of the negotiation using *'show crypto ISAKMP SA status'*

System/Device	Crypto ISAKMP SA status
Router/BR2	BR2#show cry isa sa IPv4 Crypto ISAKMP SA dst src state conn-id status 208.75.2.2 208.75.1.2 QM_IDLE 1001 ACTIVE
Router/HQ-GW[2]	HQ-GW#show cry isa sa IPv4 Crypto ISAKMP SA dst src state conn-id status 208.75.2.2 208.75.0.2 QM_IDLE 1001 ACTIVE 208.75.2.2 208.75.1.2 QM_IDLE 1002 ACTIVE

We verified the status of the sessions using *'show crypto session'*

System/Device	Crypto Session
Router/BR2	Interface: GigabitEthernet0/2 Profile: BR2 to HQ Session status: UP-IDLE Peer: 208.75.2.2 port 500 Session ID: 0 IKEv1 SA: local 208.75.1.2/500 remote 208.75.2.2/500 Active IPSEC FLOW: permit ip 192.168.1.0/255.255.255.0 10.0.0.0/255.255.255.0 Active SAs: 0, origin: crypto map IPSEC FLOW: permit ip 192.168.1.0/255.255.255.0 208.75.3.0/255.255.255.0 Active SAs: 0, origin: crypto map
Router/HQ-GW	Interface: GigabitEthernet0/0 Profile: HQ_to_BR2 Session status: UP-IDLE Peer: 208.75.1.2 port 500 Session ID: 0 IKEv1 SA: local 208.75.2.2/500 remote 208.75.1.2/500 Active IPSEC FLOW: permit ip 10.0.0.0/255.255.255.0 192.168.1.0/255.255.255.0 Active SAs: 0, origin: crypto map IPSEC FLOW: permit ip 208.75.3.0/255.255.255.0 192.168.1.0/255.255.255.0 Active SAs: 0, origin: crypto map

[2] *HQ-GW router is showing two connections because of the previously configured ESP.*

Additionally, we verified the currently active IPsec SA using *'show crypto ipsec sa'*

System/Device	IPsec security associations
Router/BR2	inbound ah sas: spi: 0x862EB2F5(2251207413) transform: ah-sha256-hmac , in use settings ={Tunnel, } conn id: 17, flow_id: SW:17, sibling_flags 80004050, crypto map: VPN2 sa timing: remaining key lifetime (k/sec): (4371815/3591) replay detection support: Y Status: ACTIVE(ACTIVE) outbound ah sas: spi: 0x7DFB20C2(2113609922) transform: ah-sha256-hmac , in use settings ={Tunnel, } conn id: 18, flow_id: SW:18, sibling_flags 80004050, crypto map: VPN2 sa timing: remaining key lifetime (k/sec): (4371815/3591) replay detection support: Y Status: ACTIVE(ACTIVE)
Router/HQ-GW	inbound ah sas: spi: 0x7DFB20C2(2113609922) transform: ah-sha256-hmac , in use settings ={Tunnel, } conn id: 39, flow_id: SW:39, sibling_flags 80000050, crypto map: VPN sa timing: remaining key lifetime (k/sec): (4346040/3541) replay detection support: Y Status: ACTIVE(ACTIVE) outbound ah sas: spi: 0x862EB2F5(2251207413) transform: ah-sha256-hmac , in use settings ={Tunnel, } conn id: 40, flow_id: SW:40, sibling_flags 80000050, crypto map: VPN sa timing: remaining key lifetime (k/sec): (4346040/3541) replay detection support: Y Status: ACTIVE(ACTIVE)

7. Connection Testing

To validate the connection according to the requirements, we are going to generate SSH traffic between BR1, BR2, PR, HQ and DMZ.

7.1 Access from BR1 to DMZ

For testing the connection from BR1 to DMZ, we established an SSH connection to the IP address 208.75.3.3 which is the static NAT public IP address assigned to the DMZ server. The results show a successful connection.

```
D-BR1:~$ ip addr | grep eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    inet 192.168.0.2/24 scope global eth0
D-BR1:~$ ssh 208.75.3.3
cisco@208.75.3.3's password:
Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <http://wiki.alpinelinux.org/>.

You can setup the system with the command: setup-alpine

You may change this message by editing /etc/motd.

DMZ:~$ ip addr | grep eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    inet 10.0.1.2/24 brd 10.0.1.255 scope global eth0
DMZ:~$
```

7.2 Access from BR1 to HQ

For testing the connection from BR1 to DMZ, we established an SSH connection to the IP address 10.0.0.2 which is the IP address of the HQ workgroup machine. In this case, the private IP addresses are being translated to their same value (identity NAT). The results show a successful connection.

```
D-BR1:~$ ip addr | grep eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    inet 192.168.0.2/24 scope global eth0
D-BR1:~$ ssh 10.0.0.2
cisco@10.0.0.2's password:
Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <http://wiki.alpinelinux.org/>.

You can setup the system with the command: setup-alpine

You may change this message by editing /etc/motd.

HQ:~$ ip addr | grep eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    inet 10.0.0.2/24 scope global eth0
HQ:~$
```

7.3 Access from BR2 to DMZ

For testing the connection from BR2 to DMZ, we established an SSH connection to the IP address 208.75.3.3 which is the static NAT public IP address assigned to the DMZ server. The results show a successful connection.

```
D-BR2:~$ ip addr | grep eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    inet 192.168.1.2/24 scope global eth0
D-BR2:~$ ssh 208.75.3.3
cisco@208.75.3.3's password:
Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <http://wiki.alpinelinux.org/>.

You can setup the system with the command: setup-alpine

You may change this message by editing /etc/motd.

DMZ:~$ ip addr | grep eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    inet 10.0.1.2/24 brd 10.0.1.255 scope global eth0
DMZ:~$
```

7.4 Access from BR2 to HQ

For testing the connection from BR1 to DMZ, we established an SSH connection to the IP address 10.0.0.2 which is the IP address of the HQ workgroup machine. In this case, the private IP addresses are being translated to their same value (identity NAT). The results show a successful connection.

```
D-BR2:~$ ip addr | grep eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    inet 192.168.1.2/24 scope global eth0
D-BR2:~$ ssh 10.0.0.2
cisco@10.0.0.2's password:
Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <http://wiki.alpinelinux.org/>.

You can setup the system with the command: setup-alpine

You may change this message by editing /etc/motd.

HQ:~$ ip addr | grep eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    inet 10.0.0.2/24 scope global eth0
HQ:~$
```

7.5 Access from PR to DMZ

For testing the connection from PR to DMZ, we established an SSH connection to the IP address 208.75.3.3 which is the static NAT public IP address assigned to the DMZ server. The results show a successful connection.

```
PR:~$ ip addr | grep eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    inet 192.168.2.2/24 scope global eth0
PR:~$ ssh 208.75.3.3
cisco@208.75.3.3's password:
Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <http://wiki.alpinelinux.org/>.

You can setup the system with the command: setup-alpine

You may change this message by editing /etc/motd.

DMZ:~$ ip addr | grep eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    inet 10.0.1.2/24 brd 10.0.1.255 scope global eth0
DMZ:~$
```

7.6 Access from PR to HQ

For testing the connection from PR to DMZ, we established an SSH connection to the IP address 10.0.0.2 which is the IP address of the HQ workgroup machine. In this case, the private IP addresses are being translated to their same value (identity NAT).

```
PR:~$ ip addr | grep eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    inet 192.168.2.2/24 scope global eth0
PR:~$ ssh 10.0.0.1
```

The connection was unsuccessful due to the ACL rule configuration that allows the PR machines to access only the DMZ but not the HQ machines. The following image shows the ASA logs that indicate the connection was denied.

```
%ASA-4-106023: Deny tcp src outside:192.168.2.2/38796 dst inside:10.0.0.1/22 by access-group "ACL-OUTSIDE" [0x0, 0x0]
%ASA-4-106023: Deny tcp src outside:192.168.2.2/38796 dst inside:10.0.0.1/22 by access-group "ACL-OUTSIDE" [0x0, 0x0]
```