

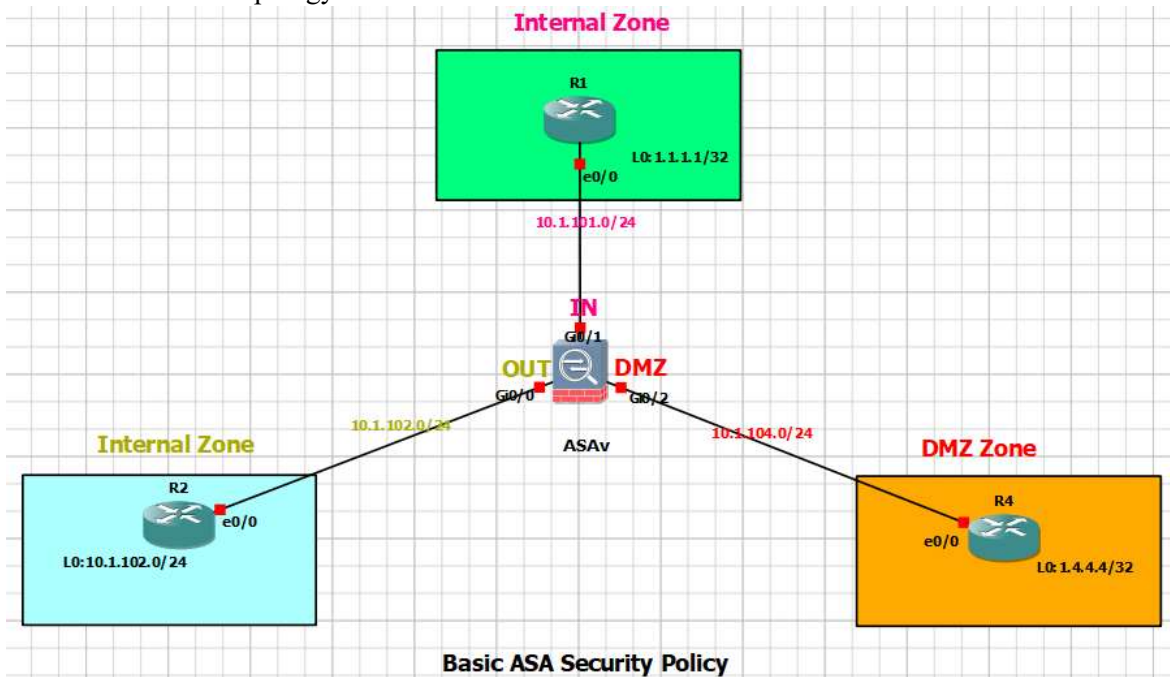
Basic ASA Security Policy

Lab Objective:

The focus of this lab is to understand basic ASA security policy.

Lab Topology:

The lab network topology is illustrated below:



Task 1:

Configure ASA with the following settings:

- Hostname: ASA-FW
- Interface Eth0: name OUT, IP address 10.1.102.10/24, security level 0
- Interface Eth1: name IN, IP address 10.1.101.10/24, security level 80
- On ASA configure default routing pointing to R2 and static routing for the rest of the networks. On routers R1 and R2 configure default routes pointing to the ASA.

Task 2:

Configure interface Eth2 on the ASA so that it will connect to R4's E0/0 interface using IP address of 10.1.104.10/24. Configure static routing on ASA and default routing on R4 to achieve full connectivity

Task 3:

Configure ASA with the policy that Ping and Telnet are allowed from the inside subnet (IN) to the outside subnet (OUT) and DMZ

Task 4:

Allow SSH and TELNET connections from R2's and R4's loopback0 interface to the R1's loopback0 interface. You are allowed to add only one line to the existing access lists.

Solution:

Task 1:

Configure ASA with the following settings:

- Hostname: ASA-FW
- Interface Eth0: name OUT, IP address 10.1.102.10/24, security level 0
- Interface Eth1: name IN, IP address 10.1.101.10/24, security level 80
- On ASA configure default routing pointing to R2 and static routing for the rest of the networks. On routers R1 and R2 configure default routes pointing to the ASA.

Note: AAA will ask the password, just Enter.

Basic configuration of ASA requires port configuration including IP address, interface name and security level. By default, the security level is set up automatically when user tries to name the interface. The ASA will use security level of 100 for interface name "inside" and security level of 0 for other interface name (including "outside"). If you need to configure other security level, use "security-level <level>" command to do so.

What is the security level for? The security level defines what connection will be considered as Inbound and what connection is Outbound.

The Outbound connection is a connection originated from the networks behind a higher security level interface towards the networks behind a lower security level interface.

The Inbound connection is a connection originated from the networks behind a lower security level interface towards the networks behind a higher security level interface.

The Outbound connection is automatically being inspected so that it does not require any access list for returning traffic. The Inbound connection is considered unsecure by default and there must be access list allowing that connection.

```
ASA-FW# conf ter
```

```
ASA-FW(config)# int eth0
```

```
ASA-FW(config-if)# ip add 10.1.102.10 255.255.255.0
```

```
ASA-FW(config-if)# no shut
```

```
ASA-FW(config-if)# nameif outside
```

```
INFO: Security level for "outside" set to 0 by default.
```

```
ASA-FW(config-if)# security-level 0
```

```
ASA-FW(config-if)# int eth1
```

```
ASA-FW(config-if)# ip add 10.1.101.10 255.255.255.0
```

```
ASA-FW(config-if)# nameif inside
```

```
INFO: Security level for "inside" set to 100 by default.
```

```
ASA-FW(config-if)# security-level 80
```

```
ASA-FW(config-if)# no shut
```

```
ASA-FW(config)# route outside 0 0 10.1.102.2
```

```
ASA-FW(config)# route inside 1.1.1.1 255.255.255.255 10.1.101.1
```

```
R1(config)#ip route 0.0.0.0 0.0.0.0 10.1.101.10
```

```
R2(config)#ip route 0.0.0.0 0.0.0.0 10.1.102.10
```

Task 2:

Configure interface Eth2 on the ASA so that it will connect to R4's E0/0 interface using IP address of 10.1.104.10/24. Configure static routing on ASA and default routing on R4 to achieve full connectivity

```
ASA-FW# conf t
```

```
ASA-FW(config)# int eth2
```

```
ASA-FW(config-if)# no shut
```

```
ASA-FW(config-if)# ip add 10.1.104.10 255.255.255.0
```

```
ASA-FW(config-if)# nameif DMZ
```

```
INFO: Security level for "DMZ" set to 0 by default.
```

```
ASA-FW(config-if)# security-level 50
```

```
ASA-FW(config-if)# no shut
```

```
ASA-FW(config-if)# route DMZ 4.4.4.4 255.255.255.255 10.1.104.4
```

```
R4(config)#ip route 0.0.0.0 0.0.0.0 10.1.104.10
```

Task 3:

Configure ASA with the policy that Ping and Telnet are allowed from the inside subnet (IN) to the outside subnet (OUT) and DMZ

The main rule on the ASA is to allow traffic coming from the interface with a higher security level towards the interface traffic is blocked in opposite direction by default and there is need for an with a lower security level. However inbound ACL to permit that traffic.

Remember that ICMP traffic is stateless, so there is no session available to track. The ASA has no ICMP inspection enabled by default so that ICMP traffic coming from the interface with higher security level towards the interface with lower security level will be blocked by the lower security level interface (ICMP echo reply will be blocked).

There are two ways to allow that traffic coming through: (1) configure ICMP inspection globally or on the interface or (2) configure inbound ACL on the interface with lower security level.

```
ASA-FW(config)# access-list OUTSIDE_IN permit icmp any any echo-reply
```

```
ASA-FW(config)# access-list DMZ_IN permit icmp any any echo-reply
```

```
ASA-FW(config)# access-group OUTSIDE_IN in interface OUT
```

```
ASA-FW(config)# access-group DMZ_IN in interface DMZ
```

Verify your configuration:

```
R1#ping 2.2.2.2 so lo0
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:

Packet sent with a source address of 1.1.1.1

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms

R1#ping 4.4.4.4

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms

R1#tel 2.2.2.2 /so lo0

Trying 2.2.2.2 ... Open

User Access Verification

Password:

R2>sh users

Line	User	Host(s)	Idle	Location
0 con 0		idle	00:00:49	
* 2 vty 0		idle	00:00:00	1.1.1.1

Interface	User	Mode	Idle	Peer Address
-----------	------	------	------	--------------

R2>exit

[Connection to 2.2.2.2 closed by foreign host]

R2#ping 1.1.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

R2#ping 1.1.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 1.1.1.1, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

Note that the ping is not working for the traffic initiated from the interface with a lower security level. This is because ACL allows only ICMP echo-reply. Also note that Telnet traffic is allowed automatically as the ASA has TCP packet inspection enabled by default so all TCP traffic coming from the interface with higher security level to the interface with lower security level will be statefully inspected (returning traffic will be allowed back).

Task 4:

Allow SSH and TELNET connections from R2's and R4's loopback0 interface to the R1's loopback0 interface. You are allowed to add only one line to the existing access lists.

As this task requires using only one ACL line there is a grouping. This method allows us to group up similar objects (hosts, ports, subnets, etc.) and then use group names in the ACL. There is different object need for object group types:

- icmp-type - specifies a group of ICMP types, such as echo
- network - specifies a group of host or subnet IP addresses
- protocol - specifies a group of protocols, such as TCP, etc
- service - specifies a group of TCP/UDP ports/services

```
ASA-FW(config)#object-group network MGMT-HOSTS
ASA-FW(config-network-object-group)#network-object host 2.2.2.2
ASA-FW(config-network-object-group)#network-object host 4.4.4.4
ASA-FW(config)#object-group service TELNET-and-SSH tcp
ASA-FW(config-network-object-group)#port-object eq telnet
ASA-FW(config-network-object-group)#port-object eq ssh
ASA-FW(config)#access-list OUTSIDE_IN extended permit tcp object-
group MGMT-HOSTS host 1.1.1.1 object-group TELNET-and-SSH
ASA-FW(config)#access-list DMZ_IN extended permit tcp object-group
MGMT-HOSTS host 1.1.1.1 object-group TELNET-and-SSH
```

Verify your Configuration:

```
ASA-FW#sh run object-group
object-group network MGMT-HOSTS
network-object host 2.2.2.2
network-object host 4.4.4.4
object-group service TELNET-and-SSH tcp
port-object eq telnet
port-object eq ssh
```

```
ASA-FW#sh access-list OUTSIDE_IN
access-list OUTSIDE_IN; 5 elements; name hash: 0xe01d8199
access-list OUTSIDE_IN line 1 extended permit icmp any any echo-
reply (hitcnt=3) 0xc857b49e
```

```
access-list OUTSIDE_IN line 2 extended permit tcp object-group MGMT-  
HOSTS host 1.1.1.1 object-group TELNET-and-SSH (hitcnt=1) 0xb422f490
```

```
access-list OUTSIDE_IN line 2 extended permit tcp host 2.2.2.2  
host 1.1.1.1 eq telnet (hitcnt=1) 0x939bf78d
```

```
access-list OUTSIDE_IN line 2 extended permit tcp host 2.2.2.2  
host 1.1.1.1 eq ssh (hitcnt=0) 0x8d022728
```

```
access-list OUTSIDE_IN line 2 extended permit tcp host 4.4.4.4  
host 1.1.1.1 eq telnet (hitcnt=0) 0xbf14a304
```

```
access-list OUTSIDE_IN line 2 extended permit tcp host 4.4.4.4  
host 1.1.1.1 eq ssh (hitcnt=0) 0x04c16117
```

```
ASA-FW#sh access-list DMZ_IN
```

```
access-list DMZ_IN; 5 elements; name hash: 0x229557de
```

```
access-list DMZ_IN line 1 extended permit icmp any any echo-reply  
(hitcnt=2) 0x7fb4c5b2
```

```
access-list DMZ_IN line 2 extended permit tcp object-group MGMT-  
HOSTS host 1.1.1.1 object-group TELNET-and-SSH (hitcnt=1) 0x909d621e
```

```
access-list DMZ_IN line 2 extended permit tcp host 2.2.2.2 host  
1.1.1.1 eq telnet (hitcnt=0) 0x231b90e2
```

```
access-list DMZ_IN line 2 extended permit tcp host 2.2.2.2 host  
1.1.1.1 eq ssh (hitcnt=0) 0x4284ac66
```

```
access-list DMZ_IN line 2 extended permit tcp host 4.4.4.4 host  
1.1.1.1 eq telnet (hitcnt=1) 0xfd96744e
```

```
access-list DMZ_IN line 2 extended permit tcp host 4.4.4.4 host  
1.1.1.1 eq ssh (hitcnt=0) 0x44528edd
```

```
R2#tel 1.1.1.1
```

```
Trying 1.1.1.1 ...
```

```
% Connection timed out; remote host not responding
```

```
R2#tel 1.1.1.1 /so 100
```

```
Trying 1.1.1.1 ... Open
```

User Access Verification

Password:

```
R1>exit
```

```
[Connection to 1.1.1.1 closed by foreign host]
```

```
R4#tel 1.1.1.1
```

```
Trying 1.1.1.1 ...
```

```
% Connection timed out; remote host not responding
```

```
R4#tel 1.1.1.1 /so 100
```

```
Trying 1.1.1.1 ... Open
```

User Access Verification

Password:

```
R1>exit
```

```
[Connection to 1.1.1.1 closed by foreign host]
```

```
R4#
```

