Laboratory Guide

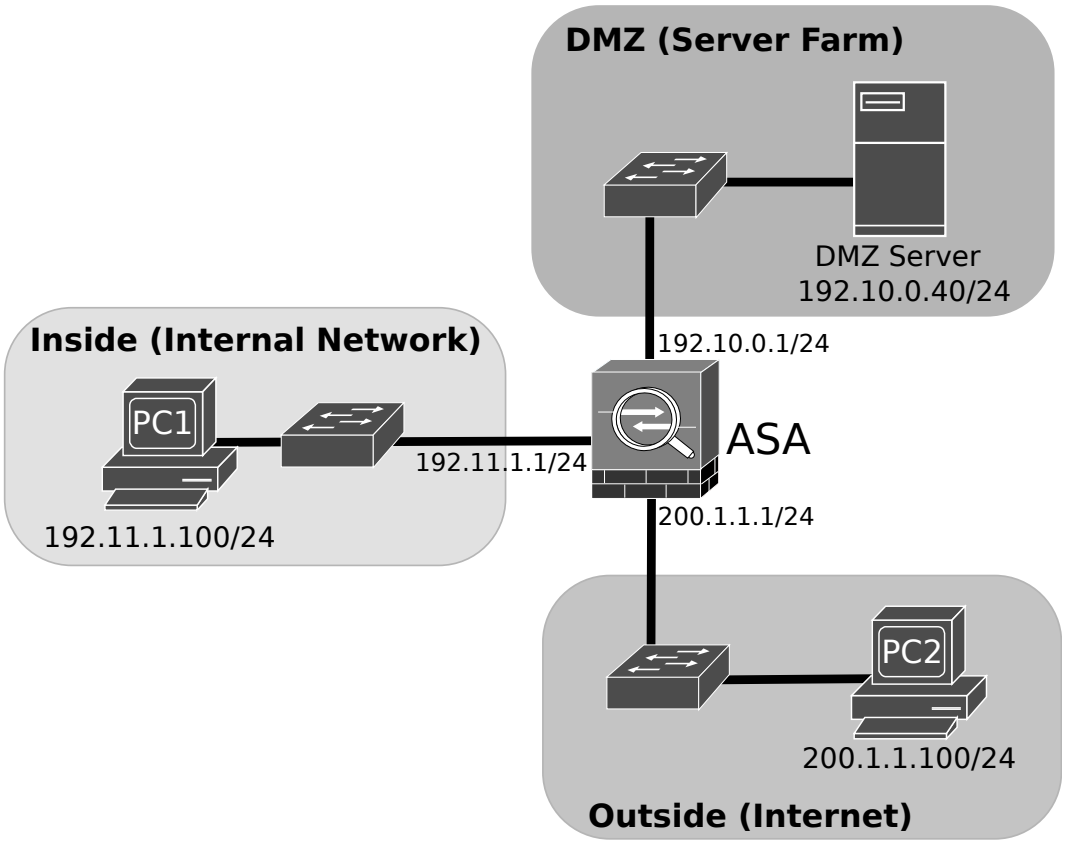
Security Appliances/Firewalls Deployment

Advanced Security Appliance Deployment

1. Using GNS3 configure the network depicted in the following figure, where PC1 and PC2 should be a Linux Vms and the DMZ server a Linux Server VM with an HTTP server. Configure all IP addresses and gateways. Configure the ASA interfaces and routing to achieve full connectivity. Networks 192.11.1.0/24 will be considered the "inside" network zone (maximum trust zone), network 192.10.0.0/24 is the DMZ and network 200.1.1.0/24 is on the "outside" zone (minimum trust zone).

```
interface Ethernet0/0
 nameif inside
 security-level 100                    !maximum trust zone
 ip address 192.11.1.1 255.255.255.0
 no shutdown
interface Ethernet0/1
 nameif dmz
 security-level 50                           !medium trust zone
 ip address 192.10.0.1 255.255.255.0
 no shutdown
interface Ethernet0/2
 nameif outside
 security-level 0                      !minimum trust zone
 ip address 200.1.1.1 255.255.255.0
 no shutdown
```

Verify the connectivity between the PC and Router. Confirm the default ASA security policies.



2. Verify the connectivity between the zones by performing: (i) a ping command at PC1 to the DMZ Server and Internet PC2 and (ii) a ping command at PC2 to the DMZ Server and PC1.

Configure the necessary access rules to allow the Inside/DMZ terminals to ping Outside terminals:

```
access-list OUTSIDE_IN extended permit icmp any 192.10.0.0 255.255.255.0 echo-reply
access-list OUTSIDE_IN extended permit icmp any 192.11.1.0 255.255.255.0 echo-reply
access-group OUTSIDE_IN in interface outside
```

Verify the connectivity between the zones by performing: (i) a ping command at PC1 to the DMZ Server and Internet PC2 and (ii) a ping command at PC2 to the DMZ Server and PC1.

Configure the necessary access rules to allow the Inside terminals to ping DMZ terminals:

```
access-list DMZ_IN extended permit icmp 192.10.0.0 255.255.255.0 192.11.1.0 255.255.255.0
                                                                                    echo-reply
access-group DMZ_IN in interface dmz
```

Verify the connectivity between the zones by performing: (i) a ping command at PC1 to the DMZ Server and Internet PC2 and (ii) a ping command at PC2 to the DMZ Server and PC1.

Note: Higher security zones terminals can send ICMP packets to lower security zones by default.

3. Perform a IP Spoofing attack to the Internet PC2 by pinging PC2 from PC1 but using an IP address from network 200.1.1.0/24 (e.g. 200.1.1.200). Define in PC1 a fake IP address in the loopback interface:

```
sudo ifconfig lo 200.1.1.200 netmask 255.255.255.255
```

Start a capture in PC2 and ping it using the fake IP address:

```
ping 200.1.1.100 -I 200.1.1.200
```

Analyze the captured packets in network 200.1.1.0/24.

Configure the ASA to accept only packets where the source address is from a network accessible via the interface where it was received (uses reverse path validation as an anti-spoofing rule).

```
ip verify reverse-path interface inside
ip verify reverse-path interface outside
ip verify reverse-path interface dmz
```

Start a new capture in PC2 and ping it using the fake IP address again:

```
ping 200.1.1.100 -I 200.1.1.200
```

Analyze the captured packets in network 200.1.1.0/24 and the correct implementation of the anti-spoofing rules in the ASA.

4. On the DMZ Server, create three HTML files named *index1.html*, *index2.html* and *index3.html* with random content. The file *index3.html* should contain the word "Attack". Add the three files to the HTTP server default site root.

From the PC2 try to access the HTTP service at the DMZ server, verifying the accessibility to the following web-pages (you may use the command: `wget -q http://192.10.0.40/index1.html -O -`):

- http://192.10.0.40/index1.html
- http://192.10.0.40/index2.html
- http://192.10.0.40/index3.html

Configure the necessary access rules to allow the outside terminals to access the HTTP (port 80 only) service at the DMZ Server.

```
access-list OUTSIDE_IN extended permit tcp any host 192.10.0.40 eq 80
access-group OUTSIDE_IN in interface outside        !if not implemented above
```

Re-verify the accessibility to the following web-pages:

- http://192.10.0.40/index1.html
- http://192.10.0.40/index2.html
- http://192.10.0.40/index3.html

What can you conclude?

5. Implement content filtering rules at the ASA to restrict the access to http://192.10.0.40/index2.html:

```
regex url2 "index2\.html"
access-list http_inspect_list extended permit tcp any host 192.10.0.40 eq www

class-map type inspect http match-all page_block_class
 match request uri regex url2
class-map http_inspect
 match access-list http_inspect_list

policy-map type inspect http http_inspection_policy
 class page_block_class
  drop-connection

policy-map http-outside-policy
 class  http_inspect
  inspect http http_inspection_policy

service-policy http-outside-policy interface outside
```

Re-verify the accessibility to the following web-pages:

- http://192.10.0.40/index.html
- http://192.10.0.40/index2.html
- http://192.10.0.40/index3.html

What can you conclude?

6. Implement content filtering rules at the ASA to restrict the access web pages pages with pattern “ATTACK” in its body:

```
regex attack "ATTACK"
class-map type inspect http match-all page_block_class
 no match request uri regex url2
 match response body regex attack
```

Re-verify the accessibility to the following web-pages:

- http://192.10.0.40/index.html
- http://192.10.0.40/index2.html
- http://192.10.0.40/index3.html

What can you conclude?

7. Implement content filtering rules at the ASA to restrict the access web pages pages with pattern “ATTACK”, independently if letters are lower or upper case, in its body:

```
regex attack2 "[Aa][Tt][Tt][Aa][Cc][Kk]"
class-map type inspect http match-all page_block_class
 no match response body regex attack
 match response body regex attack2
```

Re-verify the accessibility to the following web-pages:

- http://192.10.0.40/index.html
- http://192.10.0.40/index2.html
- http://192.10.0.40/index3.html

What can you conclude?