Cisco Router with Cisco ASA for Internet Access

A classic network scenario for many enterprises is to have a Cisco border router for internet access and a Cisco ASA firewall behind this router for protection of the internal LAN or for building a DMZ network. This scenario is shown in the figure below:
Assume that our enterprise is assigned a public IP address range of 50.50.50.0/27 (that is a 32 address subnet). The usable addresses in this subnet range between 50.50.50.1 and 50.50.50.30. In our example we assign 50.50.50.1 to the outside interface of the Cisco router and 50.50.50.2 is the ISP gateway router. Also, we need to use address 50.50.50.3 for accessing a DMZ web server which has a real private address of 10.10.10.1.

Between the Cisco Router and the outside interface of the Cisco ASA we have a private subnet 10.0.0.0/24. Also, the inside internal LAN subnet is 192.168.1.0/24. The inside IP address of the ASA is 192.168.1.1.

**Traffic Flow:**

We need to achieve the following traffic flow:

1) All Internal LAN hosts (192.168.1.0) should be able to access the Internet (outbound communication). No access initiated from the Internet should be allowed towards the Internal LAN network.

2) Also, we need to allow access from the Internet towards our DMZ Web Server (inbound communication).

**Implementation:**

There are a few ways you can follow to achieve the functionality above. For sure we need to perform NAT on the border Cisco Router to translate our internal private addresses to public addresses assigned by our ISP. We have the option also to perform additional NAT on the ASA firewall, which however I wouldn’t recommend.
The way I would configure such a scenario is the following:

- 1) For outbound communication (Internal LAN towards the Internet), **do not** translate the network 192.168.1.0/24 on the Cisco ASA. Rather create a static mapping of 192.168.1.0 to itself (will see this below) and configure NAT overload on the Cisco Router for the network 192.168.1.0/24.
- 2) For inbound communication (Internet towards Web Server), create again a static mapping on the ASA for address 10.10.10.1 to itself, and perform static NAT on the Cisco Router to map 10.10.10.1 to 50.50.50.3

**Configuration:**

Below I will show you snapshots of the configuration for both the Cisco Router and the Cisco ASA that will achieve the functionality above.

**Cisco ASA:**

```bash
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# nameif outside

ciscoasa(config-if)# ip address 10.0.0.2 255.255.255.0

ciscoasa(config-if)# security-level 0

ciscoasa(config-if)# no shutdown

ciscoasa(config)# interface GigabitEthernet0/1

ciscoasa(config-if)# nameif inside

ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0

ciscoasa(config-if)# security-level 100

ciscoasa(config-if)# no shutdown

ciscoasa(config)# interface GigabitEthernet0/3

ciscoasa(config-if)# nameif DMZ

ciscoasa(config-if)# ip address 10.10.10.2 255.255.255.0

ciscoasa(config-if)# security-level 50

ciscoasa(config-if)# no shutdown
```
! Now create a static NAT mapping of 192.168.1.0 to itself
ciscoasa(config)# static (inside, outside) 192.168.1.0 192.168.1.0 netmask 255.255.255.0

! Create also a static NAT mapping of 10.10.10.1 Web Server to itself
ciscoasa(config)# static (DMZ, outside) 10.10.10.1 10.10.10.1 netmask 255.255.255.255

EDIT: NAT Commands For Cisco ASA version 8.3 and later:

object network web_server_static
    host 10.10.10.1
    nat (DMZ, outside) static 10.10.10.1

object network inside_mapped
    subnet 192.168.1.0 255.255.255.0

object network internal-lan
    subnet 192.168.1.0 255.255.255.0
    nat (inside, outside) static inside_mapped

! Create an access-list to allow Inbound traffic to Web server only
ciscoasa(config)# access-list OUTSIDE-IN extended permit tcp any host 10.10.10.1 eq 80
ciscoasa(config)# access-group OUTSIDE-IN in interface outside

ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 10.0.0.1

Cisco Router:

interface ethernet 0
ip address 50.50.50.1 255.255.255.224
ip nat outside
!
interface ethernet 1
ip address 10.0.0.1 255.255.255.0
ip nat inside
!Assume the router uses address 50.50.50.4 for all outbound communication
ip nat pool IP-POOL 50.50.50.4 50.50.50.4 netmask 255.255.255.255
ip nat inside source list 1 pool IP-POOL overload
access-list 1 permit 192.168.1.0 0.0.0.255

!Configure Static NAT to map 10.10.10.1 to 50.50.50.3
ip nat inside source static 10.10.10.1 50.50.50.3

ip route 0.0.0.0 0.0.0.0 50.50.50.2
ip route 192.168.1.0 255.255.255.0 10.0.0.2
ip route 10.10.10.0 255.255.255.0 10.0.0.2

About the Author

Harris Andrea is a Cisco Certified Professional with more than 18 years of experience working with Cisco network technologies. He is the author of two Cisco Books (“Cisco ASA Firewall Fundamentals” and “Cisco VPN Configuration Guide”) which have been embraced by thousands of Cisco professionals all over the world. You can find more Cisco configuration guides and tutorials on his blogs below:
http://www.networkstraining.com
http://www.tech21century.com