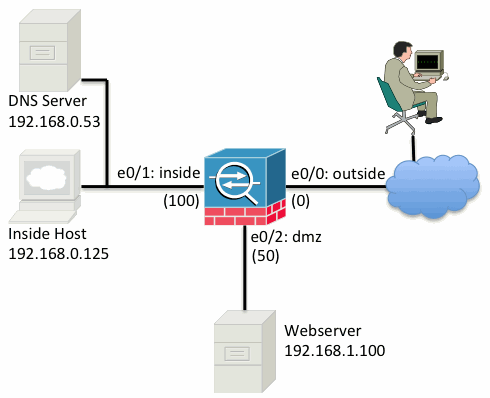
**ASA – DMZ**



### Get Started

interface Ethernet0/0  
 nameif outside  
 security-level 0  
 ip address 198.51.100.100 255.255.255.0  
!  
interface Ethernet0/1  
 nameif inside  
 security-level 100  
 ip address 192.168.0.1 255.255.255.0  
!  
interface Ethernet0/2  
 nameif dmz  
 security-level 50  
 ip address 192.168.1.1 255.255.255.0  
!  
route outside 0.0.0.0 0.0.0.0 198.51.100.1

**Step 1 - Configure NAT to Allow Hosts to Go Out to the Internet**

object network inside-subnet  
 subnet 192.168.0.0 255.255.255.0  
 nat (inside,outside) dynamic interface  
!  
object network dmz-subnet  
 subnet 192.168.1.0 255.255.255.0  
 nat (dmz,outside) dynamic interface

### Step 2 - Configure NAT to Access the Web Server from the Internet

object network webserver-external-ip  
 host 198.51.100.101  
!  
object network webserver  
 host 192.168.1.100  
 nat (dmz,outside) static webserver-external-ip service tcp www www

### Step 3 - Configure ACLs

access-list outside\_acl extended permit tcp any object webserver eq www  
!  
access-group outside\_acl in interface outside

(Até aqui funciona o HTTP)

object network dns-server  
 host 192.168.0.53  
!  
access-list dmz\_acl extended permit udp any object dns-server eq domain  
access-list dmz\_acl extended deny ip any object inside-subnet  
access-list dmz\_acl extended permit ip any any  
!  
access-group dmz\_acl in interface dmz

(Até aqui funciona também o DNS)

**object network HTTPS-WEBSERVER**

While under the "object" configuration mode add the real IP address and the NAT configuration line

**host 192.168.1.14**

**nat (inside,outside) static interface service tcp 443 443**

And then make sure to configure the ACL/Access-list that allows the traffic to the Web server

**access-list OUTSIDE-IN remark Allow HTTPS traffic to the Web Server**

**access-list OUTSIDE-IN permit tcp any object HTTPS-WEBSERVER eq 443**

**access-group OUTSIDE-IN in interface outside**

Acima é para HTTPS(Testar)

<http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/115904-asa-config-dmz-00.html>

Em português

<http://www.cisco.com/c/pt_br/support/docs/security/asa-5500-x-series-next-generation-firewalls/115904-asa-config-dmz-00.html>