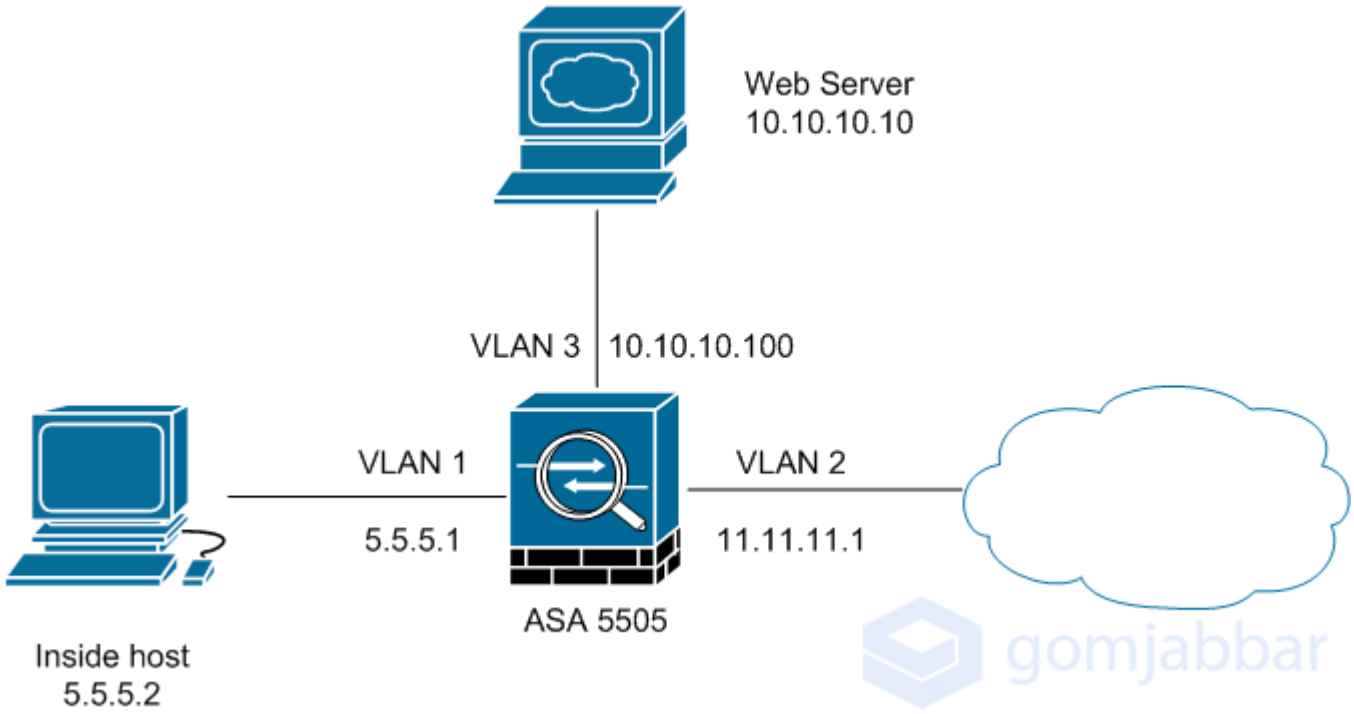
KAK - No Forward Interface Command on the Cisco ASA 5505 with a Base License

By Gom Jabbar | Published: September 11, 2011

The ASA 5505 comes in two flavors: Base License and Security Plus license. Same hardware, but the Security Plus license unlocks more features, such as the number of VLANs that can be configured.

License Type and Mode	Maximum No. of Active VLANs	VLAN Trunking
Base License + Transparent Mode	2 active VLANs in 1 bridge group	Disabled
Base License + Routed Mode	3 active VLANs (3rd VLAN can initiate traffic to only one other VLAN)	Disabled
Security Plus License + Transparent Mode	3 active VLANs (2 active VLANs in 1 bridge group, plus 1 active VLAN for failover)	Enabled
Security Plus License + Routed Mode	20 active VLANs	Enabled

In this post, I am going to look how to configure a third VLAN on a Cisco ASA with a Base License, in Routed Mode. The first two VLANs can be configured to communicate with any of the other three VLANs. The third VLAN, however, can only be configured to **initiate** traffic with one other VLAN. So a good use for this third subnet would be as a DMZ or a guest subnet.



ASA 5505 with 3 VLANs

Let's start with an unconfigured ASA 5505. Right out of the box, with a blank config. (You can also do a **write erase** and **reload** to wipe the config.)

Look at what the ASA's default config contains. The only VLAN is VLAN1, and all the physical interfaces belong to it. VLAN1 and all the physical interfaces are administratively down. The **show switch vlan** command displays the VLANs and the physical ports assigned to each VLAN. The **show interface ip brief** command shows all physical and logical interfaces, their IP addresses, whether they are administratively up/down, and whether their line protocol is up/down.

```
ciscoasa# conf t
ciscoasa(config)# sh sw v
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
```

```
1 - down Et0/0, Et0/1, Et0/2, Et0/3
Et0/4, Et0/5, Et0/6, Et0/7
ciscoasa(config)# sh int ip b
Interface IP-Address OK? Method Status Protocol
Internal-Data0/0 unassigned YES unset up up
Internal-Data0/1 unassigned YES unset administratively down up
Loopback0 127.1.0.1 YES unset up up
Vlan1 unassigned YES unset down down
Ethernet0/0 unassigned YES unset administratively down up
Ethernet0/1 unassigned YES unset administratively down up
Ethernet0/2 unassigned YES unset administratively down down
Ethernet0/3 unassigned YES unset administratively down down
Ethernet0/4 unassigned YES unset administratively down down
Ethernet0/5 unassigned YES unset administratively down down
Ethernet0/6 unassigned YES unset administratively down up
Ethernet0/7 unassigned YES unset administratively down up
```

I'll set up the first two VLANs as "inside" and "outside" and give them IP addresses.

```
ciscoasa(config)# int vlan1
ciscoasa(config-if)# ip add 5.5.5.1 255.255.255.0
ciscoasa(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)# no shut
ciscoasa(config-if)# int vlan2
ciscoasa(config-if)# ip add 11.11.11.1 255.255.255.0
ciscoasa(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
ciscoasa(config-if)# no shut
```

However, when I try to do the same for VLAN3, the ASA coughs up an error at the point when I try to name VLAN3. This is because the ASA defines an active VLAN as a VLAN with a **nameif** command configured. So it will accept the **IP address** command, but not the **nameif** command on the third VLAN.

```
ciscoasa(config-if)# int vlan3
ciscoasa(config-if)# ip add 10.10.10.1 255.255.255.0
ciscoasa(config-if)# nameif dmz
ERROR: This license does not allow configuring more than 2 interfaces with
nameif and without a "no forward" command on this interface or on 1 interface(s)
with nameif already configured.
```

So I need to run the **no forward interface vlan** command before the ASA will allow me to name this third VLAN and thus enable it.

```
ciscoasa(config-if)# no forward interface vlan 1
ciscoasa(config-if)# nameif dmz
INFO: Security level for "dmz" set to 0 by default.
ciscoasa(config-if)# no shut
```

Now all three of the VLANs have names and IP addresses.

```
ciscoasa(config-if)# sh sw v
VLAN Name Status Ports
---- -------------------------------- --------- ----------------------------
1 inside down Et0/0, Et0/1, Et0/2, Et0/3
Et0/4, Et0/5, Et0/6, Et0/7
2 outside down
3 dmz down
ciscoasa(config-if)# sh int ip b
Interface IP-Address OK? Method Status Protocol
Internal-Data0/0 unassigned YES unset up up
Internal-Data0/1 unassigned YES unset administratively down up
Loopback0 127.1.0.1 YES unset up up
Vlan1 5.5.5.1 YES manual down down
Vlan2 11.11.11.1 YES manual down down
Vlan3 10.10.10.100 YES manual down down
Ethernet0/0 unassigned YES unset administratively down up
Ethernet0/1 unassigned YES unset administratively down up
Ethernet0/2 unassigned YES unset administratively down down
```

```
Ethernet0/3 unassigned YES unset administratively down down
Ethernet0/4 unassigned YES unset administratively down down
Ethernet0/5 unassigned YES unset administratively down down
Ethernet0/6 unassigned YES unset administratively down up
Ethernet0/7 unassigned YES unset administratively down up
```

All three VLANs are administratively up because I ran the **no shut** command when I configured them. However, their status is shown as down when I ran the **show switch vlan** command because they need to have at least one physical interface assigned to them, and that physical interface needs to be administratively up. You can see that all of the physical interfaces are administratively down. Four of the physical interfaces (E0/0, E0/1, E0/6 and E0/7) show their Line Protocol status as up. This is because those physical interfaces are connected to live devices on my network.

So let's assign the physical interfaces to the VLANs and bring them up.

Ethernet 0/1 is already assigned to VLAN1, so all I have to do is run a **no shut** command. This brings Ethernet 0/1 up. Notice that VLAN1 also shows its status as up immediately.

```
ciscoasa(config-if)# int e0/1
ciscoasa(config-if)# no shut
ciscoasa(config-if)# sh sw v
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 inside up Et0/0, Et0/1, Et0/2, Et0/3
Et0/4, Et0/5, Et0/6, Et0/7
2 outside down
3 dmz down
ciscoasa(config-if)# sh int ip b
Interface IP-Address OK? Method Status Protocol
Internal-Data0/0 unassigned YES unset up up
Internal-Data0/1 unassigned YES unset administratively down up
Loopback0 127.1.0.1 YES unset up up
Vlan1 5.5.5.1 YES manual up up
Vlan2 11.11.11.1 YES manual down down
Vlan3 10.10.10.100 YES manual down down
Ethernet0/0 unassigned YES unset administratively down up
Ethernet0/1 unassigned YES unset up up
Ethernet0/2 unassigned YES unset administratively down down
Ethernet0/3 unassigned YES unset administratively down down
Ethernet0/4 unassigned YES unset administratively down down
Ethernet0/5 unassigned YES unset administratively down down
Ethernet0/6 unassigned YES unset administratively down up
Ethernet0/7 unassigned YES unset administratively down up
```

For a VLAN to be up, it needs:

- An IP address and subnet mask
- A name
- A security level
- To be administratively up
- To have at least one physical interface assigned to it, and that physical interface must be up.

I'll assign some of the other physical interfaces to VLAN2 and VLAN3.

```
ciscoasa(config-if)# int e0/0
ciscoasa(config-if)# switchport access vlan 2
ciscoasa(config-if)# no shut
ciscoasa(config-if)# int e0/6
ciscoasa(config-if)# switchport access vlan 3
ciscoasa(config-if)# no shut
ciscoasa(config-if)# int e0/7
ciscoasa(config-if)# switchport access vlan 3
ciscoasa(config-if)# no shut
```

Now all three VLANs are up.

```
ciscoasa(config-if)# sh sw v
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 inside up Et0/1, Et0/2, Et0/3, Et0/4
Et0/5
2 outside up Et0/0
```

```
3 dmz up Et0/6, Et0/7
ciscoasa(config-if)# sh int ip b
Interface IP-Address OK? Method Status Protocol
Internal-Data0/0 unassigned YES unset up up
Internal-Data0/1 unassigned YES unset administratively down up
Loopback0 127.1.0.1 YES unset up up
Vlan1 5.5.5.1 YES manual up up
Vlan2 11.11.11.1 YES manual up up
Vlan3 10.10.10.100 YES manual up up
Ethernet0/0 unassigned YES unset up up
Ethernet0/1 unassigned YES unset up up
Ethernet0/2 unassigned YES unset administratively down down
Ethernet0/3 unassigned YES unset administratively down down
Ethernet0/4 unassigned YES unset administratively down down
Ethernet0/5 unassigned YES unset administratively down down
Ethernet0/6 unassigned YES unset up up
Ethernet0/7 unassigned YES unset up up
```

So how does the **no forward interface vlan** command affect the flow of traffic?
The inside interface can initiate traffic to the DMZ, and the return traffic is permitted. For example, a host on the inside network can access my web server in the DMZ. The inside host initiates the connection to my web server, and the ASA places the connection in its state table. When my web server replies with the web page, the ASA sees that this is not a new connection, just return traffic from an existing connection, and allows it to reach the inside host who had requested the web page.
However, the DMZ cannot initiate traffic to the inside interface, even when an ACL is configured on the dmz interface, explicitly permitting traffic from the DMZ to the inside. That is because the **no forward interface vlan** command prevents any traffic originating from the DMZ from entering the inside network.
So how is this different from the outside interface? After all, the outside interface has a security level of 0, and it cannot initiate traffic to the inside interface. However, since the outside interface does not have a **no forward interface vlan** command configured, an ACL on the outside interface is all you need to permit all traffic originating from the outside network to reach the inside network.
- See more at: http://www.gomjabbar.com/2011/09/11/no-forward-interface-command-on-the-cisco-asa-5505-with-a-base-license/#sthash.ehQbsSJ6.dpuf