

Understanding the Eight Basic Commands on a Cisco ASA Security Appliance

By Don R. Crawley, CCNA Security, Linux+, IPv6 Silver Engineer

There are literally thousands of commands and sub-commands available to configure a Cisco security appliance. As you gain knowledge of the appliance, you will use more and more of the commands. Initially, however, there are just a few commands required to configure basic functionality on the appliance. Basic functionality is defined as allowing inside hosts to access outside hosts, but not allowing outside hosts to access the inside hosts. Additionally, management must be allowed from at least one inside host. To enable basic functionality, there are eight basic commands (these commands are based on software version 8.3(1) or greater):

- interface
- nameif
- security-level
- ip address
- switchport access
- object network
- nat
- route

interface

The interface command identifies either the hardware interface or the Switch Virtual Interface (VLAN interface) that will be configured. Once in interface configuration mode, you can assign physical interfaces to switchports and enable them (turn them on) or you can assign names and security levels to VLAN interfaces.

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 192.168.1.1
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 1
ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 1
ciscoasa(config-if)# █
```

nameif

The *nameif* command gives the interface a name and assigns a security level. Typical names are *outside*, *inside*, or *DMZ*.

security-level

Security levels are numeric values, ranging from 0 to 100, used by the appliance to control traffic flow. Traffic is permitted to flow from interfaces with higher security levels to interfaces with lower security levels, but not the other way. Access-lists must be used to permit traffic to flow from lower security levels to higher security levels. The default security level for an outside interface is 0. For an inside interface, the default security level is 100. In the following sample

configuration, the interface command is first used to name the inside and outside VLAN interfaces, then the DMZ interface is named and a security level of 50 is assigned to it.

```
ciscoasa(config)# interface vlan1
ciscoasa(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)# interface vlan2
ciscoasa(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
ciscoasa(config-if)# interface vlan3
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
```

ip address

The ip address command assigns an IP address to a VLAN interface either statically or by making it a DHCP client. With modern versions of security appliance software, it is not necessary to explicitly configure default subnet masks. If you are using non-standard masks, you must explicitly configure the mask, otherwise, it is not necessary.

In the following sample configuration, an IP address is assigned to VLAN 1, the inside interface.

```
ciscoasa(config-if)# interface vlan 1
ciscoasa(config-if)# ip address 192.168.1.1
```

Configuring interfaces on 55x0 appliances

Notice on the following screen capture from a Cisco ASA 5540 security appliance that the *nameif* command is used to name physical interfaces instead of VLAN interfaces.

```
ciscoasa(config-if)# interface gigabitethernet0/1
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa(config-if)# ip address 10.16.14.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)#
```

switchport access

The switchport access command on the ASA 5505 security appliance assigns a physical interface to a logical (VLAN) interface. In the next example, the interface command is used to identify physical interfaces, assign them to switchports on the appliance, and enable them (turn them on). This command is not used on the ASA 55x0 appliances.

```
ciscoasa(config-if)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 2
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 1
ciscoasa(config-if)# no shutdown
```

object network obj_any

The object network `obj_any` statement creates an object called “obj_any”. (You do not have to name the object “obj_any”; that is a descriptive name, but you could just as easily name it “Juan”.) The network option states that this particular object will be based on IP addresses. The subnet `0.0.0.0 0.0.0.0` command states that `obj_any` will affect any IP address not configured on any other object.

```
ciscoasa(config-if)#object network obj_any  
ciscoasa(config-network-object)#subnet 0.0.0.0 0.0.0.0
```

nat

The `nat` statement, as shown below, tells the firewall to allow all traffic flowing from the inside to the outside interface to use whatever address is dynamically (DHCP) configured on the outside interface.

```
ciscoasa(config)#nat (inside,outside) dynamic interface
```

route

The `route` command, in its most basic form, assigns a default route for traffic, typically to an ISP’s router. It can also be used in conjunction with `access-lists` to send specific types of traffic to specific hosts on specific subnets.

In this sample configuration, the `route` command is used to configure a default route to the ISP’s router at 12.3.4.6. The two zeroes before the ISP’s router address are shorthand for an IP address of 0.0.0.0 and a mask of 0.0.0.0. The statement *outside* identifies the interface through which traffic will flow to reach the default route.

```
ciscoasa(config-if)# route outside 0 0 12.3.4.6
```

The above commands create a very basic firewall, however, using a sophisticated device such as a Cisco PIX or ASA security appliance to perform such basic firewall functions is overkill.

Other commands to use include *hostname* to identify the firewall, *telnet* or *SSH* to allow remote administration, *DHCPD* commands to allow the firewall to assign IP addresses to inside hosts, and *static route* and *access-list* commands to allow internal hosts such as DMZ Web servers or DMZ mail servers to be accessible to Internet hosts.

Here is a sample base configuration:

Sample Base Configuration

```
ciscoasa(config)# interface vlan1
```

```
ciscoasa(config-if)# nameif inside
```

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

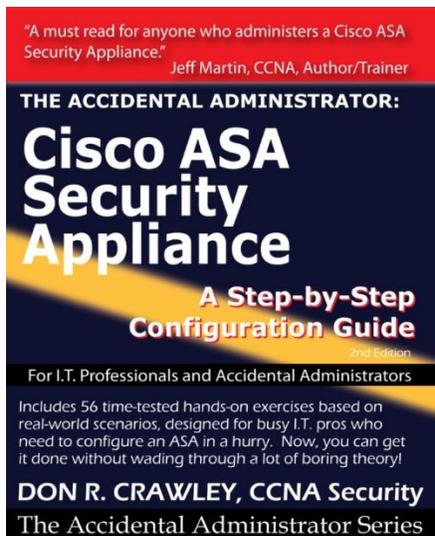
```
ciscoasa(config-if)# interface vlan2
```

```
ciscoasa(config-if)# nameif outside
```

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

```
ciscoasa(config-if)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 2
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 1
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 2
ciscoasa(config-if)# ip address 12.3.4.5
ciscoasa(config-if)# interface vlan 1
ciscoasa(config-if)# ip address 192.168.1.1
ciscoasa(config-if)# route outside 0 0 12.3.4.6
ciscoasa(config-if)#object network obj_any
ciscoasa(config-network-object)#subnet 0.0.0.0 0.0.0.0
ciscoasa(config)#nat (inside,outside) dynamic interface
ciscoasa(config)#exit
```

Excerpted from *The Accidental Administrator: Cisco ASA Security Appliance: A Step-by-Step Configuration Guide* by Don R. Crawley Paperback: 184 pages ISBN-10: 1449596622 ISBN-13: 978-1449596620



About the author



Don R. Crawley author of The Accidental Administrator series of books for IT professionals including *The Accidental Administrator: Cisco ASA Security Appliance: A Step-by-Step Configuration Guide* and President of soundtraining.net a Seattle, Washington-based IT training firm. He is a veteran IT guy with over 35 years' experience in technology for the workplace. He holds multiple certifications on Microsoft, Cisco, and Linux products. Don can be reached at (206) 988-5858 www.soundtraining.net don@soundtraining.net

You have permission to reprint this article in your newsletter, blog, website, or publication if you include the following paragraph (Is it too long? No problem. Just contact us for an edit.):

Don R. Crawley is a longtime geek and President/Chief Technologist of soundtraining.net with more than 35 years in workplace technology. He holds multiple technical certifications and is the author of numerous books on information systems and technology, including *The Accidental Administrator: Cisco ASA Security Appliance*. He has spoken to audiences worldwide on both technical topics and IT customer service. To view this Seattle IT pro's upcoming events or to receive free Cisco tutorials, Linux tutorials, IT customer service tips, and other guides that will help you with Cisco training, Linux training, customer service training, and other skills you need to know to build a great career in IT, visit www.soundtraining.net or contact us at don@soundtraining.net or 206-988-5858.