show running-config

```
: Saved
:
ASA Version 8.4(2)

hostname ARENAASA
domain-name cisco.com
enable password CxOAGVRkNm3Kvjqo encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names

interface Ethernet0/0
nameif outside
security-level 0
ip address dhcp

interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0

interface Ethernet0/2
shutdown
no nameif
no security-level
no ip address

interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address

interface Management0/0
nameif management
security-level 0
ip address 9.9.9.9 255.255.255.0

ftp mode passive
dns server-group DefaultDNS
domain-name cisco.com
access-list hug extended permit ip any any
pager lines 24
mtu outside 1500
mtu inside 1500
mtu management 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
nat (inside,outside) source dynamic any interface
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
http server enable
http 10.78.17.134 255.255.255.255 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
telnet timeout 5
ssh 10.0.76.186 255.255.255.255 outside
ssh 10.78.17.134 255.255.255.255 outside
ssh 10.0.76.170 255.255.255.255 outside
ssh 10.0.0.134 255.255.255.255 outside
ssh 192.168.0.2 255.255.255.255 inside
ssh timeout 60
ssh version 2
console timeout 0
```

```
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 15

class-map inspection_default
match default-inspection-traffic

policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect ip-options
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp

service-policy global_policy global
prompt hostname context
call-home reporting anonymous prompt 2
call-home
profile CiscoTAC-1
no active
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination address email callhome@cisco.com
destination transport-method http
subscribe-to-alert-group diagnostic
subscribe-to-alert-group environment
subscribe-to-alert-group inventory periodic monthly
subscribe-to-alert-group configuration periodic monthly
subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:88b966dfa365bd66c295c1943b1be0da
: end
```

show ip route

```
^
ERROR: % Invalid input detected at '^' marker.
```

show ipv6 route

```
IPv6 Routing Table - 0 entries
Codes: C - Connected, L - Local, S - Static
```

show ip int brief

```
^
ERROR: % Invalid input detected at '^' marker.
```

show ipv6 int brief

```
outside [down/down]
unassigned
inside [down/down]
unassigned
Ethernet0/2 [administratively down/down]
unassigned
Ethernet0/3 [administratively down/down]
unassigned
management [down/down]
unassigned
```

show cdp neighbors

```
^
ERROR: % Invalid input detected at '^' marker.
```

show ipv6 ospf 10

```
^
ERROR: % Invalid input detected at '^' marker.
```

show ipv6 ospf 10 neighbor

```
^
ERROR: % Invalid input detected at '^' marker.
```

show ip bgp summary

```
^
ERROR: % Invalid input detected at '^' marker.
```

show access-lists

```
^
ERROR: % Invalid input detected at '^' marker.
```

show version

```
Cisco Adaptive Security Appliance Software Version 8.4(2)
Detected an old ASDM version.
You will need to upgrade it before using ASDM.

Compiled on Wed 15-Jun-11 18:17 by builders
System image file is "disk0:/asa842-k8.bin"
Config file at boot was "startup-config"

ARENAASA up 22 days 9 hours

Hardware: ASA5510-K8, 1024 MB RAM, CPU Pentium 4 Celeron 1600 MHz
Internal ATA Compact Flash, 256MB
BIOS Flash AT49LW080 @ 0xfff00000, 1024KB

Encryption hardware device : Cisco ASA-55x0 on-board accelerator (revision 0x0)
Boot microcode : CN1000-MC-BOOT-2.00
SSL/IKE microcode : CNLite-MC-SSLm-PLUS-2.03
IPSec microcode : CNlite-MC-IPSECm-MAIN-2.06
Number of accelerators: 1

0: Ext: Ethernet0/0 : address is 0019.e8d9.4908, irq 9
1: Ext: Ethernet0/1 : address is 0019.e8d9.4909, irq 9
2: Ext: Ethernet0/2 : address is 0019.e8d9.490a, irq 9
3: Ext: Ethernet0/3 : address is 0019.e8d9.490b, irq 9
4: Ext: Management0/0 : address is 0019.e8d9.490c, irq 11
5: Int: Not used : irq 11
6: Int: Not used : irq 5

Licensed features for this platform:
Maximum Physical Interfaces : Unlimited perpetual
Maximum VLANs : 100 perpetual
Inside Hosts : Unlimited perpetual
Failover : Active/Active perpetual
VPN-DES : Enabled perpetual
VPN-3DES-AES : Enabled perpetual
Security Contexts : 2 perpetual
GTP/GPRS : Disabled perpetual
AnyConnect Premium Peers : 2 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 250 perpetual
Total VPN Peers : 250 perpetual
Shared License : Disabled perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
UC Phone Proxy Sessions : 2 perpetual
Total UC Proxy Sessions : 2 perpetual
Botnet Traffic Filter : Disabled perpetual
Intercompany Media Engine : Disabled perpetual

This platform has an ASA 5510 Security Plus license.

Serial Number: JMX1108L07Z
Running Permanent Activation Key: 0x7d0e3d41 0xe0922e45 0x30b0a184 0xa1b4285c 0x4935dd9a
Configuration register is 0x1
Configuration last modified by enable_15 at 09:53:24.476 UTC Thu Jan 23 2003
```