Switches, Routers, and Firewalls

Storage Media

- ROM
- NVRAM
- DRAM
- CAM
- Hard Drive
- Flash / SSD

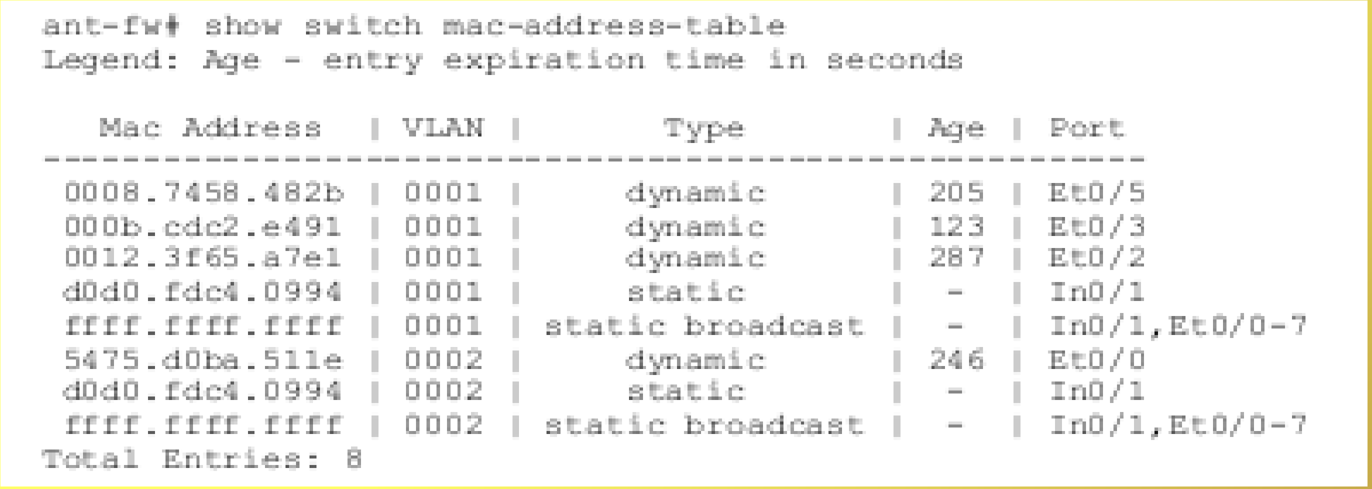
Switches

- Maps MAC addresses to switch ports
- Locate physical location of MACs
- ARP tables
- Data Collection
  - Port Mirroring
  -

CAM Tables

- Very fast memory
- Maps MAC Addresses to physical switch ports
    - Switch looks up MAC in table
    - Writes packet to the correct port
- If an attacker is sniffing local traffic it will show up in the CAM table
- The CAM table is very volatile

CAM Table



```
ant-fw# show switch mac-address-table
Legend: Age - entry expiration time in seconds

   Mac Address    | VLAN |        Type        | Age | Port
-------------------------------------------------------
 0008.7458.482b | 0001 |      dynamic       | 205 | Et0/5
 000b.cdc2.e491 | 0001 |      dynamic       | 123 | Et0/3
 0012.3f65.a7e1 | 0001 |      dynamic       | 287 | Et0/2
 d0d0.fdc4.0994 | 0001 |      static        |  -  | In0/1
 ffff.ffff.ffff | 0001 | static broadcast |  -  | In0/1,Et0/0-7
 5475.d0ba.511e | 0002 |      dynamic       | 246 | Et0/0
 d0d0.fdc4.0994 | 0002 |      static        |  -  | In0/1
 ffff.ffff.ffff | 0002 | static broadcast |  -  | In0/1,Et0/0-7
Total Entries: 8
```

“Age” is the number of seconds left before the entry expires.

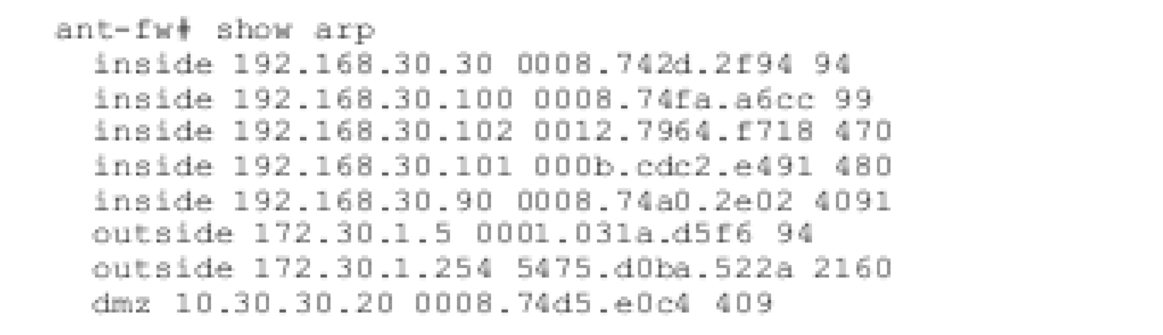
ARP Tables

- MAC address to IP address resolution
- Format of table entry
    - Location of the ARP request
    - IP Address
    - MAC address
    - Age in seconds from initial ARP request

```
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.215                    (incomplete)                              eth0
192.168.1.212                    (incomplete)                              eth0
dlinkrouter.local        ether   3c:1e:04:0b:f6:f4   C                     wlan0
gateway                  ether   74:27:ea:26:28:ea   C                     eth0
192.168.1.214                    (incomplete)                              eth0
192.168.1.213                    (incomplete)                              eth0
Entries: 6      Skipped: 0      Found: 6
```

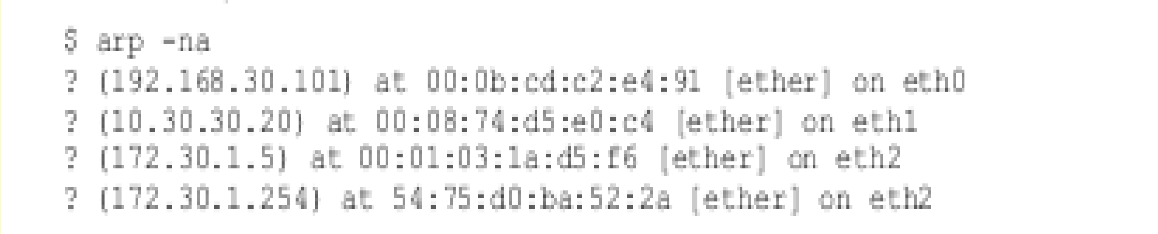
ARP Table

Cisco ASA 5505 firewall



```
ant-fw# show arp
  inside 192.168.30.30 0008.742d.2f94 94
  inside 192.168.30.100 0008.74fa.a6cc 99
  inside 192.168.30.102 0012.7964.f718 470
  inside 192.168.30.101 000b.cdc2.e491 480
  inside 192.168.30.90 0008.74a0.2e02 4091
  outside 172.30.1.5 0001.031a.d5f6 94
  outside 172.30.1.254 5475.d0ba.522a 2160
  dmz 10.30.30.20 0008.74d5.e0c4 409
```

Ubuntu Server



```
$ arp -na
? (192.168.30.101) at 00:0b:cd:c2:e4:91 [ether] on eth0
? (10.30.30.20) at 00:08:74:d5:e0:c4 [ether] on eth1
? (172.30.1.5) at 00:01:03:1a:d5:f6 [ether] on eth2
? (172.30.1.254) at 54:75:d0:ba:52:2a [ether] on eth2
```

Type of Switches

- Managed Switches
- Smart Switches
- Unmanaged Switches

Managed Switches

- Enterprise LANS
  - Support for VLAN, ACLs
  - ARP caching, 802.1 authentication
  - Port mirroring/monitoring
  - Event logging
  - Config Interfaces
    - CLI, SSH/Telnet, SNMP, Web, Proprietary- Cisco
  - Performance Monitoring

Smart Switches

- Subset of Managed Switches
    - VLANs
    - ARP caching
    - Port mirroring
    - Some performance monitoring
- Config Interface
    - Usually Web
    - CLI and remote CLI

Home Switches

- Unmanaged Switches
    - Plug and play
    - No configuration interface
    - No accessible stored data
    - No/limited forensic value

Switch Evidence

- Volatile Data
  - Stored packets (prior to forwarding)
  - CAM tables (MAC to port mappings)
  - ARP Table (MAC to IP address mappings)
  - ACLs, Running configuration
  - Flow data and performance stats
- Non-Volatile Data
  - OS image and Startup configuration
- Off-System
  - Logging data
  - Flow data

Routers - Why?

- Network topology
- Traffic through the router – flow data / packet data
- Can do filtering
- Logged data
    - all routers are capable of extensive logging
- The router itself may be compromised!
- Types of Routers
    - Enterprise
    - Consumer
    - Custom – Linux boxes

Enterprise router

- Extensive selection - $ - $$$$$
- Capabilities
    - Stateful packet filtering
    - Supports many routing protocols
    - Multiprotocol Label Switching
    - High-availability, high-throughput
    - DHCP, NAT QoS
    - Performance monitoring
    - Event logging

Router Interfaces

- Configuration Interfaces
    - CLI, Telnet/SSH, SNMP
    - Web interface
    - Cisco Proprietary
    - Central Management
        - Cisco Works Management Center
- Central management
    - Central management of large numbers of routers
- Cisco ASA series
- Juniper J-Series

Consumer Grade Routers

- Linksys, D-Link, ISP Custom
- Often supplied by the ISP
  - Caution!
- Capabilities
  - ISP connection via PPPoE
  - DHCP, NAT
  - 802.11 wireless interface
  - Port Filtering
  - Easy config via Web interface
  - Remote access to config

Make your own router

- Zebra Software stack
- Linux Base
- Router specific software support
- CLI similar to Cisco’s CLI
- Multiprotocol support
- Iptables for filtering
- Logging and other mechanisms

Router Evidence

Volatile

- Routing Tables
- Packet counts & statistics
- ARP table
- DHCP lease assignments
- ACLs
- Running config
- Flow data & statistics
- I/O and processor memory

Router Evidence

Non-Volatile

- OS image
- Boot loader
- Stored configuration
- Access logs
- DHCP logs

Router Evidence
Remote

- Configurable – via
  - Syslog, FTP, TFTP, SNMP
- Access history
- DHCP logs
- Backup configuration
- Flow data

Firewalls

- Both Hardware and software firewalls
- Firewall logs include extensive info
    - Connection attempts
        - Success or failure
    - Protocols used
    - Applications
- Configuration
    - What does the world see
    - Net topology
- Configurable to collect more data
- Firewall may be compromised

Firewall Types

- Packet Filters
  - Iptables types (which allow or deny packets)
- Session-Layer Proxies
  - Source establishes connection with proxy
  - Destination establishes connection with proxy
  - Man in the middle intercept of SSL connections for deep packet inspection of encrypted traffic
- Application Proxies
  - Enables inspection of layer 7 traffic

Enterprise-class Firewalls

- Often higher layer proxies are often standalone devices
- Firewall features/capabilities
    - NAT, DHCP, VPN tunneling
    - Load balancing
    - Fail over
    - Fragmentation reassembly
    - Stateful filtering, performance monitoring
    - Centralized management, Event logging
    - HW upgrades

Configuration Interfaces

- CLI
- Remote CLI via SSH/Telnet
- SNMP
- Web interface
- Proprietary

- Remote access = insecurity!

Consumer Grade Firewalls

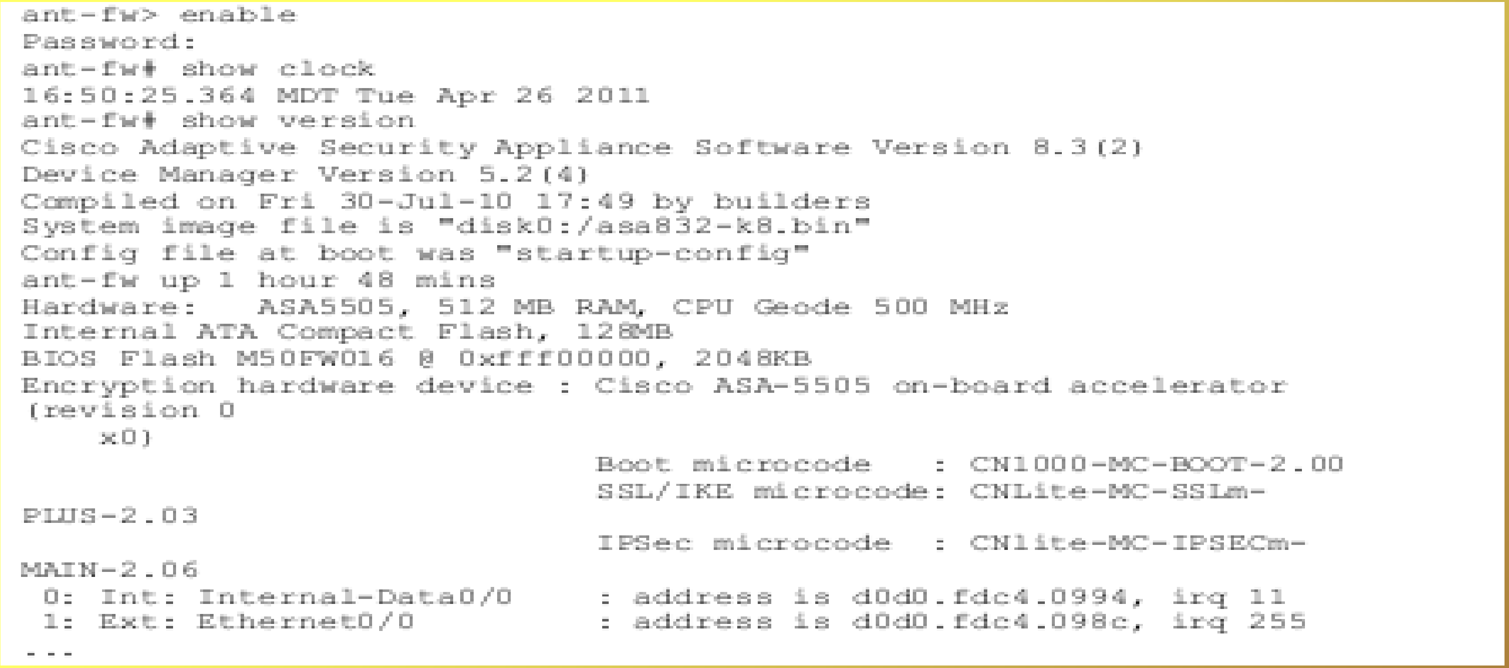
- Provides
  - NAT
  - DHCP
  - WiFi interface
  - Some packet filtering
  - Some logging

Firewall Evidence

- Volatile
  - Similar to routers
  - Command history
- Persistent
  - Boot load, startup config
  - Access logs, DHCP logs
  - Firewall rules and exceptions
  - **TURN IT ON**
- Remote
  - Usual logs

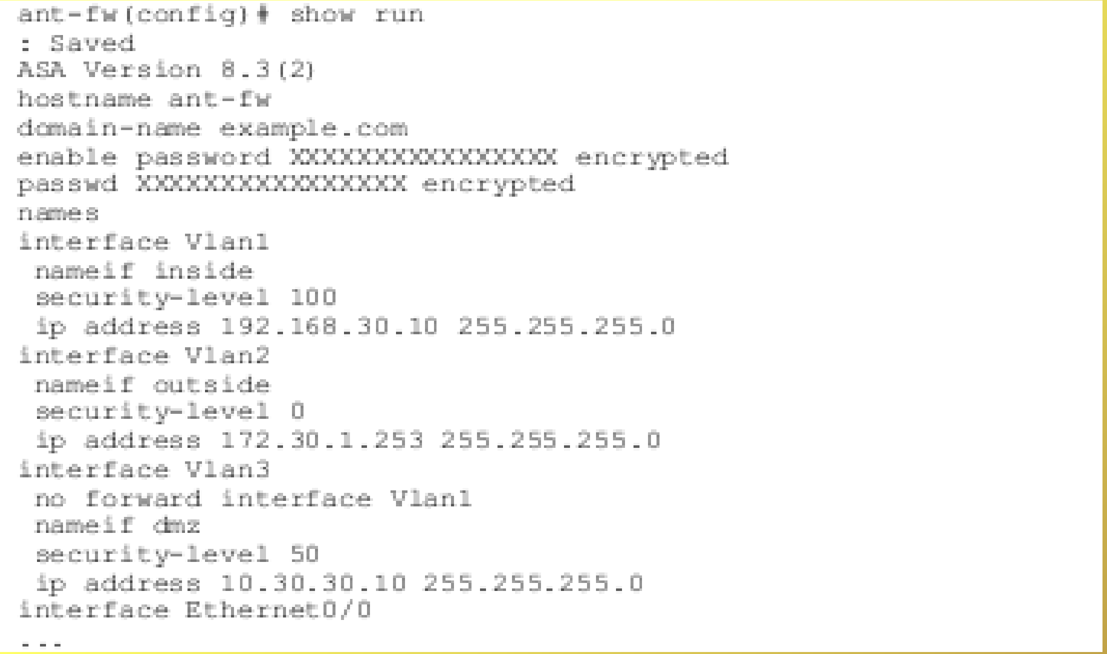
Interfaces

- CLI
  - Cisco ASA 5505 is typical



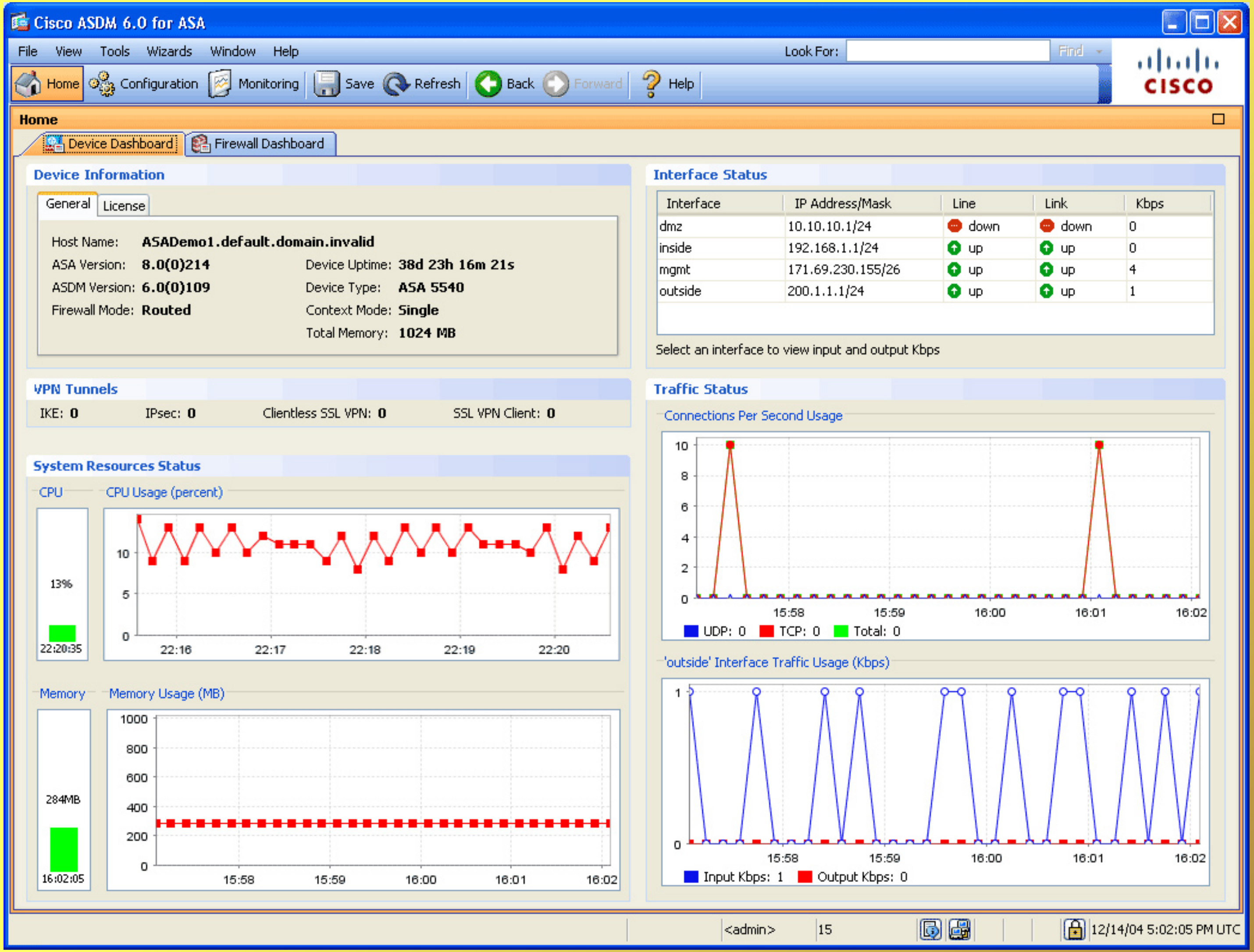
```
ant-fw> enable
Password:
ant-fw# show clock
16:50:25.364 MDT Tue Apr 26 2011
ant-fw# show version
Cisco Adaptive Security Appliance Software Version 8.3(2)
Device Manager Version 5.2(4)
Compiled on Fri 30-Jul-10 17:49 by builders
System image file is "disk0:/asa832-k8.bin"
Config file at boot was "startup-config"
ant-fw up 1 hour 48 mins
Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 128MB
BIOS Flash M50FW016 @ 0xfff00000, 2048KB
Encryption hardware device : Cisco ASA-5505 on-board accelerator
(revision 0
    x0)
                             Boot microcode   : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode: CNLite-MC-SSLm-
PLUS-2.03
                             IPSec microcode  : CNlite-MC-IPSECm-
MAIN-2.06
 0: Int: Internal-Data0/0    : address is d0d0.fdc4.0994, irq 11
 1: Ext: Ethernet0/0         : address is d0d0.fdc4.098c, irq 255
...
```

Cisco ASA 5505 Continued



```
ant-fw(config)# show run
: Saved
ASA Version 8.3(2)
hostname ant-fw
domain-name example.com
enable password XXXXXXXXXXXXXXXX encrypted
passwd XXXXXXXXXXXXXXXX encrypted
names
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.30.10 255.255.255.0
interface Vlan2
 nameif outside
 security-level 0
 ip address 172.30.1.253 255.255.255.0
interface Vlan3
 no forward interface Vlan1
 nameif dmz
 security-level 50
 ip address 10.30.30.10 255.255.255.0
interface Ethernet0/0
...
```

Web Interface



Device Information

General | License

Host Name: **ASADemo1.default.domain.invalid**

ASA Version: **8.0(0)214** Device Uptime: **38d 23h 16m 21s**

ASDM Version: **6.0(0)109** Device Type: **ASA 5540**

Firewall Mode: **Routed** Context Mode: **Single**

Total Memory: **1024 MB**

Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
dmz	10.10.10.1/24	down	down	0
inside	192.168.1.1/24	up	up	0
mgmt	171.69.230.155/26	up	up	4
outside	200.1.1.1/24	up	up	1

Select an interface to view input and output Kbps

VPN Tunnels

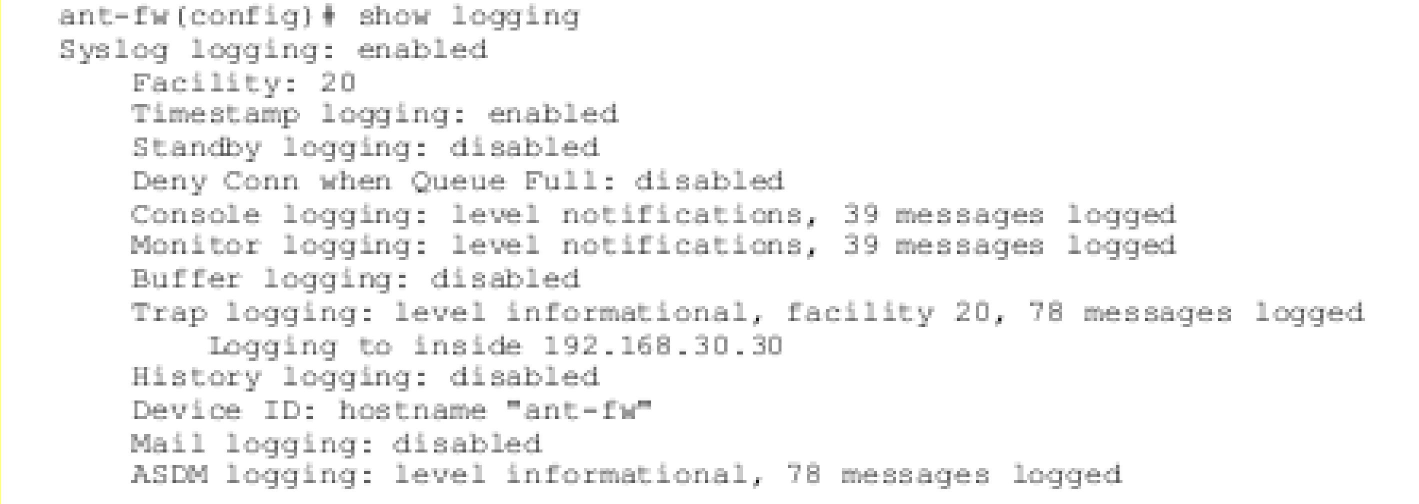
IKE: **0** IPsec: **0** Clientless SSL VPN: **0** SSL VPN Client: **0**

Traffic Status

System Resources Status

Logging

- Cisco ASA 5505



```
ant-fw(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: enabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: level notifications, 39 messages logged
    Monitor logging: level notifications, 39 messages logged
    Buffer logging: disabled
    Trap logging: level informational, facility 20, 78 messages logged
        Logging to inside 192.168.30.30
    History logging: disabled
    Device ID: hostname "ant-fw"
    Mail logging: disabled
    ASDM logging: level informational, 78 messages logged
```

Other Logs

- Syslog, rsyslog, etc.
- AAA logs
    - Authentication
    - Authorization
    - Accounting
- Files usage logs
- Console logs
- Terminal logs
-