

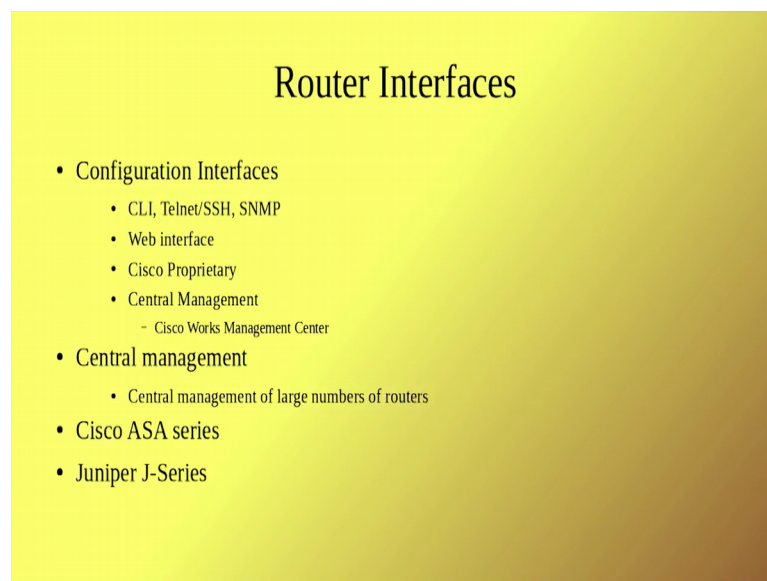
Information security - IV
Prof. M J Shankar Raman
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture – 53
Evidence collection in Routers and Firewalls

So, we were seen that the there are the enterprise routers are very expensive and these routers enterprise routers also actually have their interfaces ok; so, the interfaces how you are going to interact with the router device ok.

And if you remember during our demo of snort we were having most of command line interface for example, when your configuring snort we were actually using the CLI of snort saying that snort minus a console and all those things if you want I mean you can get the nice GUI for snort I mean either you write it or you can get it from open source.

(Refer Slide Time: 01:05)



Similarly all these routers can have a CLI interface command line interface Cisco routers have it juniper routers have it and the command line interface of Huawei routers sometimes resembles Cisco routers due to certain reasons ok.

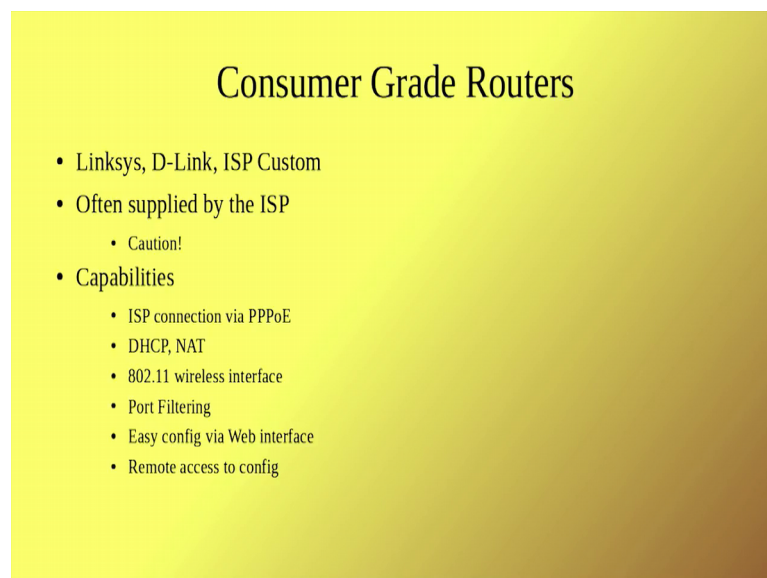
Then what we can do is we will look at telnet and SSH SNMP these are all the ways by which you actually interact with your router. Sometimes this configuration interfaces

could be proprietary Cisco could give their own tools and there is something Cisco work management center. So, the network management console and things like that.

So, these GUI actually make the life of the of the administrator slightly more easy, but if you are looking at convenience and you are an administrator usually CLI clips are much more faster and efficient execute because GUI usually take some time. The other thing is that these routers will also allow you to do some sort of central management ok. And it will be you can have a huge console and in front of you looking at the network where there are lot of routers and then each of them sending some status and all that it will look like a space shuttle launch pad; I mean you can have a network operation center they call it as a network operation center.

And there is where there actually use this kind of softer and then monitor the whole network which includes intrusion, detection, provision. How firewalls work and other getting any alerts are you exceeding some band width etcetera. So, the examples of some of these enterprise routers include Cisco A S I series juniper j series. So, usually I mean you buy the enterprises have their own method of buying the routers; so we are not specifying that you have to use this router something. So, in our case for example, you use some of Cisco A S I router; so, some kind of demos.

(Refer Slide Time: 03:04)



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

And if you look at consumer grade routers you have a Linksys D D-Link and you sometimes you can also use your custom routers sometimes the person the ISP itself will provide you the router.

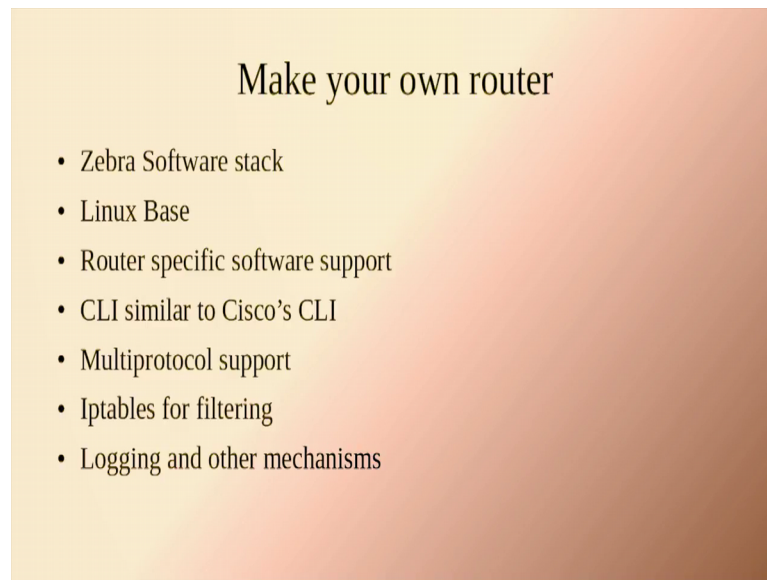
Ok, but then be cautious about it because you do not know what goes inside that router there could be some kind of back doors etcetera. One of the one of the stuff that you could look at is I mean is there any extra data that goes out of the port; I mean this is the small test you could do. You connect to networks routers together inside and then within your own network, send data from one network to another network and then see whether you are getting any data out of any other ports ok; this small test will help you find out whether data is getting leaked etcetera anyway.

So, coming to capabilities the consumer grade routers they provide connection to ISP via PPO over Ethernet and they have DHCP, NAT, 802.11 wireless interface they have port filtering they have MAC address based filtering see if you are using a home router it is always a good idea that even though you might give DHCP and all that.

Our suggestion if you want more security is that you put filtering based on MAC address; that means, record all the MAC addresses of the device that you use in your network ok. And then allow data to flow only from those devices with those MAC addresses ok. So, in that way you will be having a extra round of security in your house itself; otherwise if you are going to use DHCP its totally unsecure anyone can if your network someone attacks your network and opens it up they will get connected.

Many of these consumer get routers provide a web interface because as I told an interface network people would really be certified and. So, they will be some sort of geeks; so, they do not prefer GUI kind of stuff where as in a consumer get routers which is used in your homes you would rather go with a nice GUI set up.

(Refer Slide Time: 05:20)



That it is easy for you to configure you could also make your own router ok. So, sometimes it is needed for forensic expert.

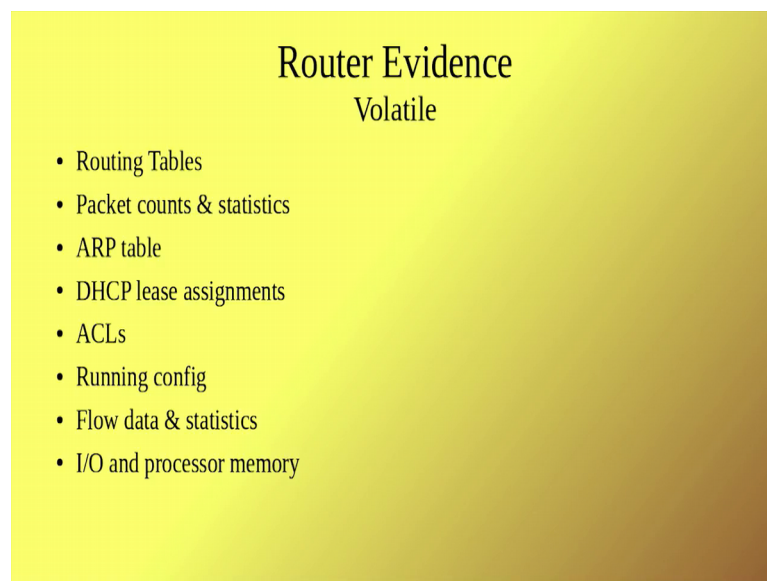
See when I do not trust the router I say let us assume that I found out that one of the routers has been compromised ok. Now I want to really found out find out whether the router has compromised by an attacker. So, what could I do is I could replicate the configuration of the router into my Linux based say router that is my own router replace that router. And then see whether the any differences in behavior between the previous routers that was there and my router that I have put ok.

Because if I had strengthened my router and then things are working fine and you know that the other router is misbehaving; then you could actually identify there is some kind of compromise that would have happened ok. So, under such circumstances its better and plus your own router you could also put get the logs and get whatever logs you want because sometimes if its company specific then there are certain restrictions.

The advantage of using the zebra software based router is that its uses Linux base then the there is very good protocol support it supports protocols such as BGP RIP version one rip version 2 etcetera believe there is also a m p l s support. So, these of embed you might need a fairly powerful box if you were going to deploy it in a large scale.

But if you are debugging at a enterprise level; I think you have enough systems which can provide you support you could use one or more of these routers and then get the data that you want to have. These routers also have a IP table for filtering we will take a look at IP tables firewalls and in next few sections and the advantage of make your own router is that you can bring about your own logging mechanisms ok. So, as forensic expert we need lot of logging to happen; so,, so now looking at routers what are all the evidences that one can get from a routers?

(Refer Slide Time: 07:43)



So, first is the volatile evidences as usual you could get the routing tables there is lot of statistics that routers throughout including band width.

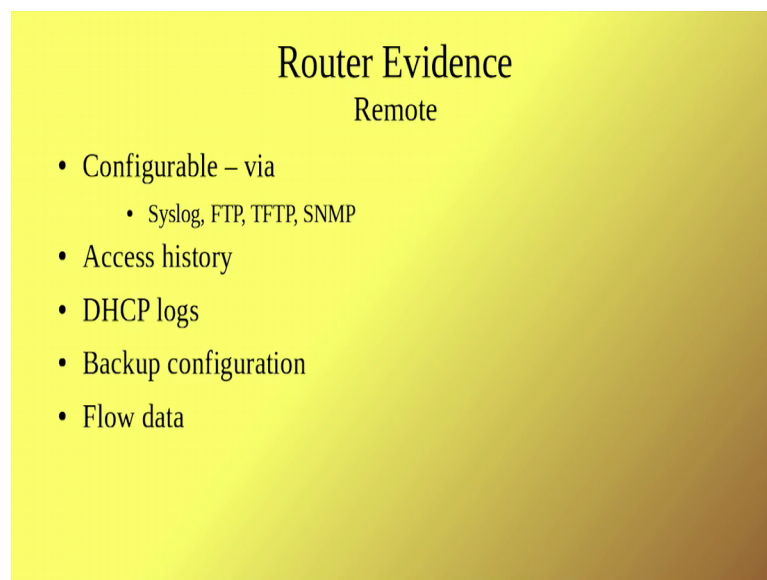
And then if you look at the Cisco's show command it will tell you what kind of statistics the router can dump right from the virtual memory the number of processor that are running in the router etcetera, etcetera, etcetera. Then as usually you can get the a RP table you can get the DHCP lease assignments you can get the access control lease you can get the running configuration of the router you can get lot of flow data and statistics.

In fact, some course and fine grind the statistics can be got from the routers and also the IO and processor memory utilization. Because sometimes if some computation kind of stuff is running inside the router you will see that there is high processor and memory utilization and you can try to find out what is happening ok. So, these are all the volatile evidences as far as the non volatile evidences in a router is considered, you could look at

the OS image then the boot loader that is being used then what are all the stored configuration previously we had a running configuration. We can also look at stored configuration you can look at access log and then you can look at the DHCP logs.

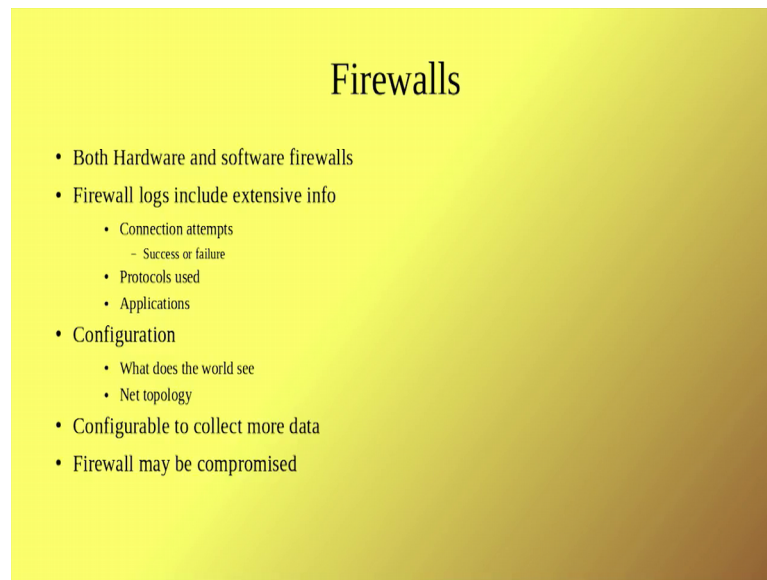
The other way is that now this is if you have the router in your hands suppose what happens if you go for remote access.

(Refer Slide Time: 09:09)



Then most of the evidences will log will come from the Syslog of the routers. So, you might have to log in to the router and then get all these data DHCP log backup configuration flow data etcetera. So, you can log in and get these data.

(Refer Slide Time: 09:24)



Now after routers the next device that will be using I think we had seen enough of firewalls in one of the sections, but we will now look at what is the forensic evidence it provides and especially you will take a look at IP tables which is available in Linux. So, we will also see some demos of how to configure filters and using IP tables ok.

So, in that case we need to have some kind of theory before we go into that ok. So, one of the things with firewall is that you could have both hardware and software based firewalls ok. And firewalls actually provide you lot of information and they provide whether someone has right to connect your network ok.

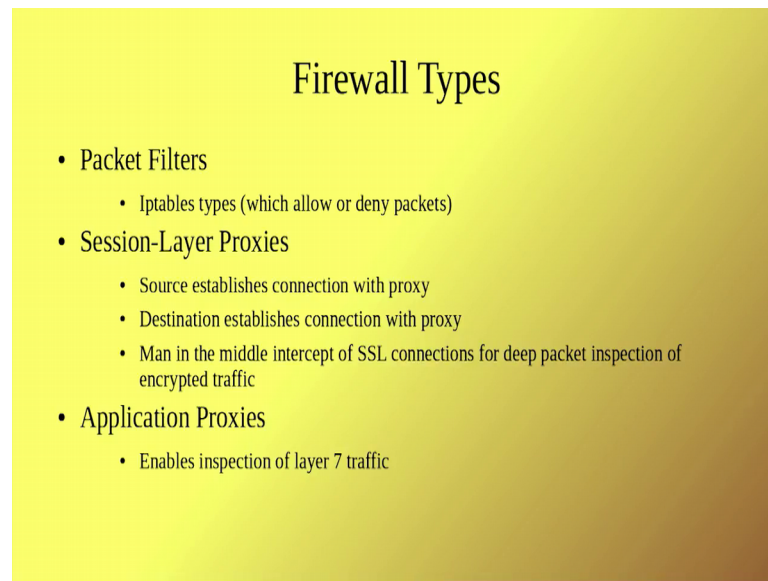
And whether the connection has passed whether the connection has failed, then it also talks about the protocols that are being used for communication and it also has bunch of what are all the applications that are because there something known as application level firewalls ok. So, this tells you what all the applications that are that are the passing through this firewalls etcetera.

As for the configuration of firewall is concerned ok; so, we will it similar to what. So, it is it provides a kind of protection therefore, it is see something known as the internal network which earns to protect and then it has something known as external network it wants to protect and there is something known as demilitarized zone where it wants to protect this between the internal and external networks. So, firewall actually does these

job ok; so, if a firewall is compromised I think the whole security of your organization could be very well compromised ok.

Because of this security issue it is configurable to get more and more data from firewalls. There are different types of firewalls the first one is packet filters ok.

(Refer Slide Time: 11:23)



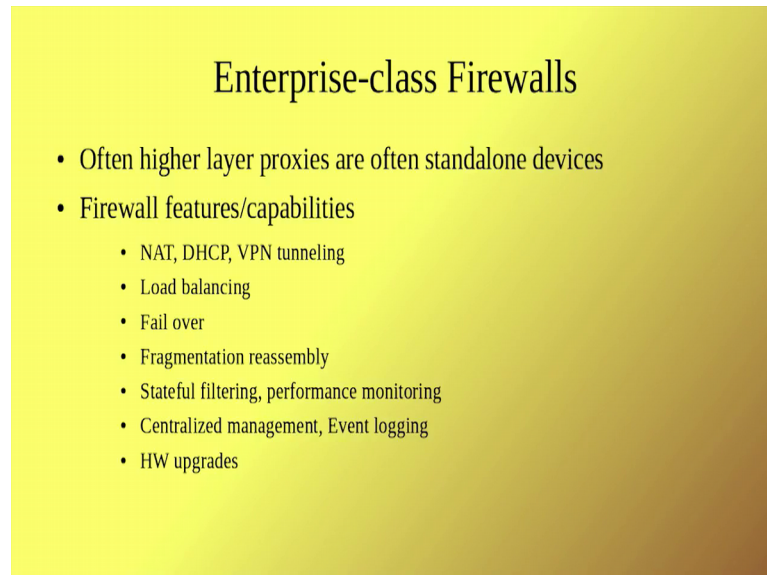
Like which allow or deny packets ok; so we will see an example of IP tables which will we will configure for allowing or denying packets. Then there is this section layer proxies ok; so, essentially what happens is that if instead of a source connecting to destination on the internet straight through the routers, they actually it is a sort of man in the middle this proxy seat in the middle then the connections comes to this proxy then the proxy redirects the connection to the destination ok.

So, the source established connection with the proxy another destination establishes connection with the proxy and then it is the firewall that sits in between these two guys and then it does SSL connections I mean just monitors the SSL connection then it does the deep packet inspection of the traffic etcetera.

Now, now you see how difficult because it is an encrypted traffic you have to do quick description and then intercept the traffic and then study this traffic. So, it is a huge amount of work that is involved in these kind of set up ok. There is this application

proxies. Now this takes a look at application what is happening between two applications. So, this is the layer seven it monitors layer seven traffic.

(Refer Slide Time: 12:43)

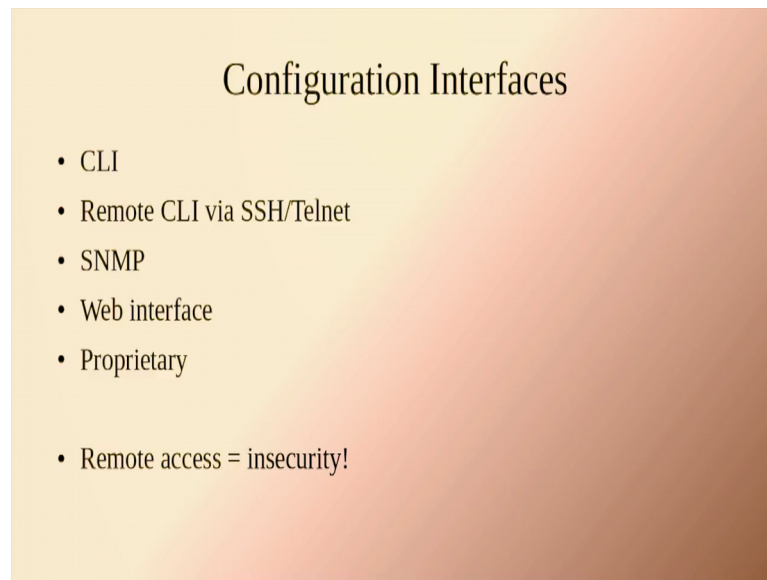


Different types of firewalls that one could deploy the network the enterprise class firewalls ok usually are standalone devices and they have provide the they can provide the lot of features like VPN tunneling which will private network tunneling and it can provide DHCP, it can provide NAT facilities it can do load balancing because performance is one of the important criteria with respect to firewalls ok.

So, fail tardyons and load balancing will be two features that you expect out of a firewall because these are supposed to be 99 percent 99.9969 and systems ok. These firewalls also do fragmentation and reassembly of packets because since it works as a proxy there could be a different packet length on one side of proxy and different packet length and other sides. So, this guys can do this kind of a fragmentation and reassembly of packets.

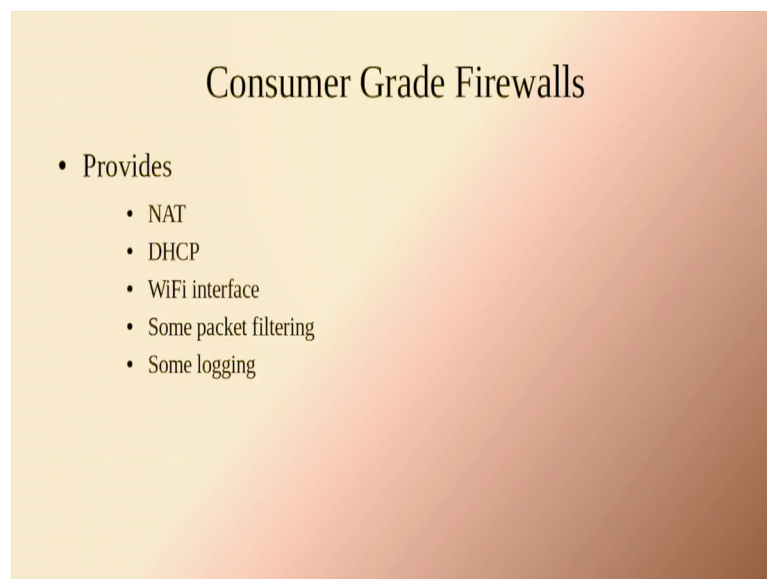
Then, you could have something like stateful filtering ok. So, what suppose I only want to see what all the states are particular connection goes through and I do not want to just go through certain number of states; I can filter all those states I can do event logging and centralized management of firewalls. And then it also includes hardware upgrades because you have to cope up with feed and the data speed that comes. So, any remote access leads to insecurity, but firewalls and other devices actually allow remote access.

(Refer Slide Time: 14:13)



But you need to be extremely careful when you do this kind of remote access. So, as usual like other devices provides the CLI, SNMP, Web Interface and some proprietary interfaces.

(Refer Slide Time: 14:25)



Ok with coming down to consumer grade firewalls they are provide much less feature than the enterprise firewalls they have NAT, DHCP and they have Wi-Fi interface.

(Refer Slide Time: 14:38)

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

Some kind of packet interface and log; so, looks I mean it similar. So, if you remember all these three device that we have been looking at firewalls routers all these three devices that we have been looking at; they all more or less have volatile evidence, they have a persistence evidence then you can collect remote evidence.

One of the important things that you should do is as a network administrator person you should enable the logs I mean many of the time if you forget to enable the logs you are not going to collect any more evidence.

(Refer Slide Time: 15:14)

Interfaces

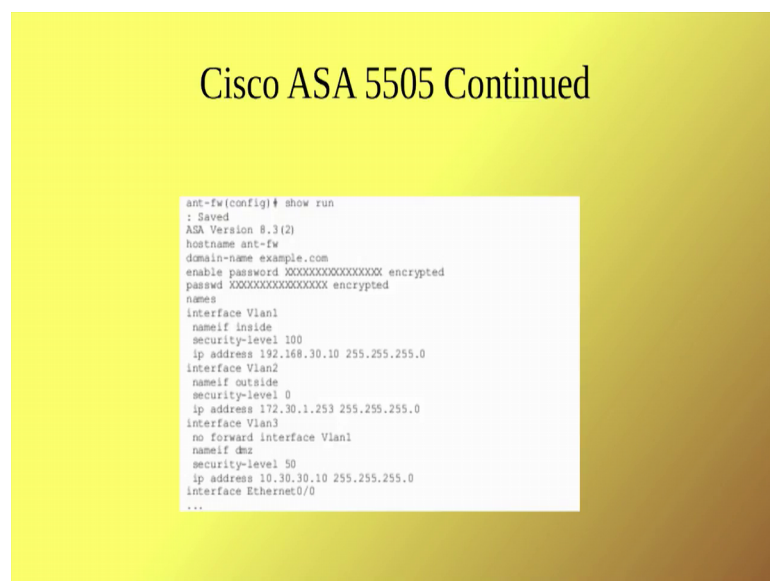
- CLI
 - Cisco ASA 5505 is typical

```
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: ASAS505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 128MB
BIOS Flash M50FW016 @ 0xffff0000, 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
...
```

So, firewall evidence is important; so, here is a typical interface that you can get. So, this is the Cisco interface CLI for a ASA 5505. So, here is something like I mean it tells you what is the version and all that; so, it show clock show a version.

So, all these all these are evidences that you can collect ok. So, if you look at this evidence it tells you how much time this was up what was the start up configuration that reduced and then what is the image file it has and what is the boot code where is the boot code what all the external interface internet interface and so on.

(Refer Slide Time: 15:53)

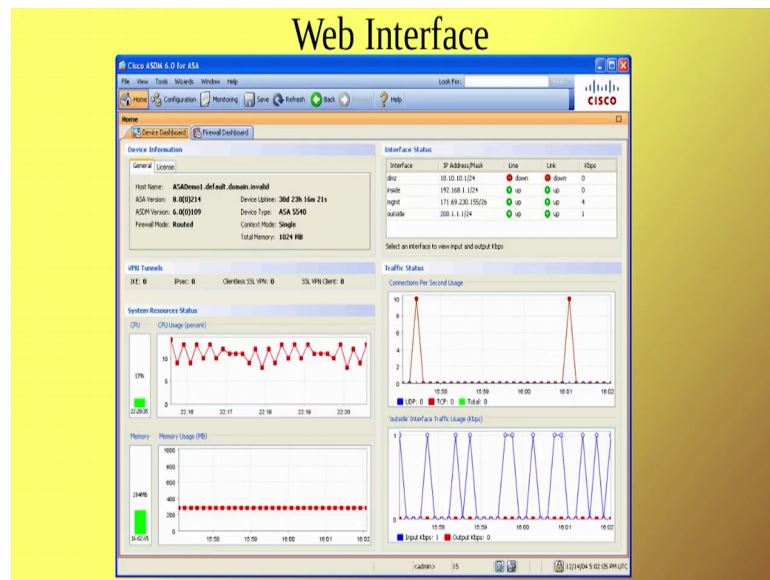


The slide features a yellow-to-brown gradient background. At the top center, the text "Cisco ASA 5505 Continued" is displayed in a black serif font. Below this, a white rectangular box contains a screenshot of a Cisco ASA CLI session. The text in the box is as follows:

```
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
...
```

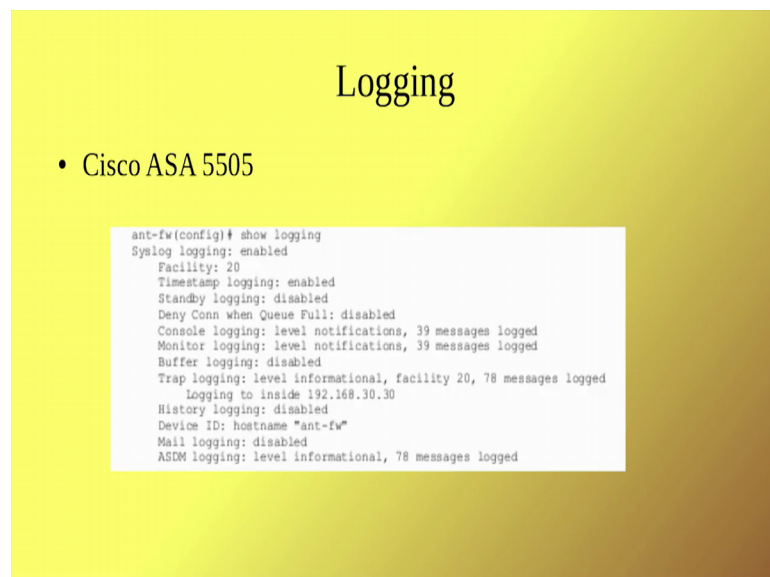
Then it also shows something like what is the running configuration. So, what all the wheel LAN and so, if you see the inside network you can see the outside network what is the IP address of the demilitarized zone and where is this wheel are connected and all those; so, you see all these addresses ok.

(Refer Slide Time: 16:13)



And this is a typical web interface. So, so it shows I mean what is the device dashboard then you can have the firewall dashboard etcetera; so, what are all the tunnels? So, you look at the traffic status and all that it is just to see I mean as I told you there is there is the big screen that you will have to monitor all these.

(Refer Slide Time: 16:37)

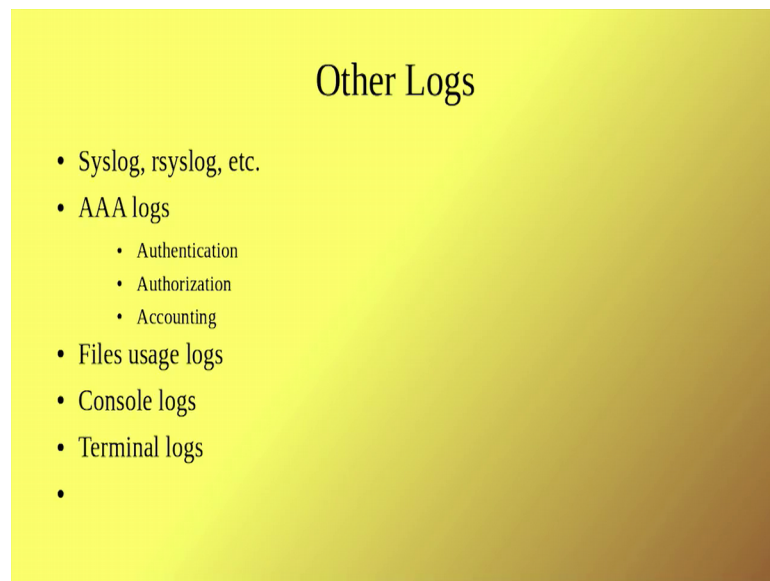


Then you can also if you can find out what are all the logging ok; so, if you say show logging it says that the timestamp logging enables the standby logging is enabled console

logging is there. So, all these logs will be using if you see there are. So, many logs that can come out and these logs can be gathered for forensic evidence ok.

There are other types of logs that we look at; we will take a look at many of these logs and done how to analyze some of these logs say probably will for one session we will allocate to analyze some logs look at some logs.

(Refer Slide Time: 17:14)



And then guess what information we are getting out of the logs that will be a separate section that will be having. In general these are all the types of log you will get you will get Syslog then remote Syslog I mean it includes remote logging into a remote system and getting it ok.

Then you have a authentication authorization and accounting law which basically radius tacacs and diameter ok. You can look at file usage; statistics console logs and logs that you will get out of terminal. Anyhow we will going to the details of all these logs some of the format of some of these logs and how to do some forensic analysis based on some of these logs.

What we will do now is that we will now look at how to configure a firewalls ok; some example of how to configure a firewall especially using IP tables. So, IP tables as you know the packet filters. So, the next section we will take a look at how to configure a packet filter.

Thank you very much.