[NOTE : Use ? for a list of available commands and use tab button to complete the command ]

hostname>en (Enable- In order to go to root privilege)

Password: (No password as default)

hostname # config t ( For configuring the terminal )

hostname (config)# ( # indicates that you are in root )

**For setting up username and password**

hostname (config)# username *username* password *password* encrypted privilege *0-15* ( Higher the value more access you have to the device)

**Configuring vlans**

hostname(config)# interface vlan *1-4090*

hostname(config-if)# nameif outside ( For outside internet )

hostname(config-if)# security-level 0 ( 0-100 where 0 is least trusted )

hostname(config-if)# ip address *ip\_address subnet\_mask* ( for dhcp ip address dhcp setroute )

hostname(config-if)# no shutdown ( To activate the interface )

**Adding vlan to the desired port**

hostname(config)# interface ethernet 0/port (where port is 0 through 7)

hostname(config-if)# switchport access vlan  0-4090 (Assigns this switch port to a VLAN, where number is the VLAN ID, between 1 and 4090

hostname(config-if)# no shutdown

**For creating object group**

hostname (config)# object-group network *obj\_name*

hostname (config-network)# network-object host or subnet *ip\_address*

**For enabling ICMP messages**

hostname (config)# object-group icmp-type *group\_name*

hostname (config-icmp)# icmp-object *type\_of\_message\_you\_want\_to\_add*

hostname (config)# access-list inbound extended permit icmp any any object-group *group\_name*

**For ssh**

hostname (config)# aaa authentication ssh console LOCAL

hostname (config)# crypto key generate rsa modulus *modulus\_size*

hostname (config)# ssh *ip\_address subnet\_mask* inside

hostname (config)# ssh timeout *minutes*

**For DHCP inside LAN**

hostname (config)#dhcpd address *ip\_address\_range* inside

hostname (config)#dhcpd enable inside

ciscoasa(config)# show run

: Saved

:

ASA Version 8.0(2)

!

hostname ciscoasa

domain-name ggt.local

enable password 8Ry2YjIyt7RRXU24 encrypted

names

!

interface Vlan1

nameif inside

security-level 100

ip address 192.168.10.1 255.255.255.0

!

interface Vlan2

nameif outside

security-level 0

ip address dhcp setroute

!

interface Ethernet0/0

switchport access vlan 2

!

interface Ethernet0/1

!

interface Ethernet0/2

!

interface Ethernet0/3

!

interface Ethernet0/4

shutdown

!

interface Ethernet0/5

shutdown

!

interface Ethernet0/6

shutdown

!

interface Ethernet0/7

switchport access vlan 3

!

passwd 2KFQnbNIdI.2KYOU encrypted

ftp mode passive

dns server-group DefaultDNS

domain-name ggt.local

same-security-traffic permit inter-interface

object-group icmp-type ping

description ping group

icmp-object echo

icmp-object echo-reply

icmp-object time-exceeded

icmp-object unreachable

icmp-object traceroute

object-group network net

network-object 192.168.10.0 255.255.255.0

object-group network as

access-list inbound extended permit icmp any any object-group ping

pager lines 24

mtu inside 1500

mtu outside 1500

icmp unreachable rate-limit 1 burst-size 1

asdm image disk0:/asdm-602.bin

no asdm history enable

arp timeout 14400

global (outside) 2 interface

nat (inside) 2 0.0.0.0 0.0.0.0

access-group inbound out interface inside

access-group inbound in interface outside

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 uauth 0:05:00 absolute

dynamic-access-policy-record DfltAccessPolicy

aaa authentication http console LOCAL

aaa authentication ssh console LOCAL

http server enable

http 192.168.10.0 255.255.255.0 inside

no snmp-server location

no snmp-server contact

snmp-server enable traps snmp authentication linkup linkdown coldstart

no crypto isakmp nat-traversal

telnet timeout 5

ssh 192.168.10.0 255.255.255.0 inside

ssh timeout 5

console timeout 0

dhcpd dns 8.8.8.8

dhcpd auto\_config outside

!

dhcpd address 192.168.10.2-192.168.10.33 inside

dhcpd enable inside

!

threat-detection basic-threat

threat-detection statistics access-list

!

class-map inspection\_default

match default-inspection-traffic

!

!

policy-map type inspect dns preset\_dns\_map

parameters

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 netbios

inspect rsh

inspect rtsp

inspect skinny

inspect esmtp

inspect sqlnet

inspect sunrpc

inspect tftp

inspect sip

inspect xdmcp

inspect icmp

inspect icmp error

!

service-policy global\_policy global

username cyberasa password elw9NVFvvkSsuwzy encrypted privilege 15

prompt hostname context

Cryptochecksum:30517293e664190a3721f013a0dfe0a4

: end