Step 1: configure privileged level password

(config)# enable password PASSWORD

Step 2: Enable Command Line Management

(config)# username blah password blah

(config)#aaa authentication ssh console local

(config)#crypto key generate rsa modulus 1024

(config)#ssh x.x.x.x x.x.x.x inside

(config)#ssh x.x.x.x x.x.x.x outside

Step 3: Configure a firewall hostname\

(config)#hostname blah

Step 4: Configure interface commands int g0/0… on 5510, on 5505 interface vlan x

(config)#Nameif “interface name”

#Ip address address mask

#Security level 0 to 100 – 0 default outside 100 default inside

#No shut

Step 5: Configure NAT control

(config)#nat-control –only if all traffic from high interfaces to lower interfaces need nat

These are dynamic and the “1” binds them together with the global

(config)# nat inside 1 x.x.x.x x.x.x.x – inside subnet

#global outside 1 x.x.x.x x.x.x.x – outside subnet

#Nat dmz 1 x.x.x.x x.x.x.x – ip of dmz

#Global dmz 1 x.x.x.x x.x.x.x – dmz addresses of inside hosts

Show xlate – to monitor

If mask of global outise is 255.255.255.255 then PAT

If using pat and ip of outside interface then the command can use the ip or int name

STATIC NAT

(config)#static(source interface name, Mapped interface name) mapped ip real ip netmask mask

STATIC PORT REDIRECTION

(config)#Static (DMZ, outside) tcp 100.1.1.1 80 x10.0.0.1 80 netmask 255.255.255.255 – ips are outside and then inside

#Static (DMZ, outside) tcp 100.1.1.1 25 x10.0.0.2 25 netmask 255.255.255.255 – ips are outside and then inside

IF inside uses nat but DMZ does not and you used the nat-control statement earlier then :

#Nat(DMZ) 0 100.1.1.0 255.255.255.0 – so that DMZ going to lower will skip the nat process

Step 6: Configure routing

(config)#route outside 0.0.0.0 0.0.0.0 x.x.x.x – default route out

Route inside ip mask IpOfNextHop – static route back inside

Step 7: ACLs

(config)# access-list “name” [line line\_number] [extended]{deny|permit} protocol “source\_address” “mask” [operator source\_port] “dest\_address” “mask” [operator dest\_port]

Access-group to apply acl to int

#Access-group “name”(same from acl) in/out interface “int name”

Examples

Example 1---

Allow inbound to dmz

(config)#Static (DMZ, outside) 100.1.1.1 10.0.0.1 netmask 255.255.255.255

#Static(DMZ, outside) 100.1.1.2 10.0.0.2 netmask 255.255.255.255

#Access-list OUTSIDE-IN extended permit tcp any host 100.1.1.1 eq 80

#Access-list OUTSIDE-IN extended permit tcp any host 100.1.1.2 eq 25

#Access-group OUTSIDE-IN interface outside

#Access-list DMZ-IN extended deny ip any any log

#Access-group DMZ-IN interface DMZ

Allows the world to get to our web and email but if these servers are hacked they cannot get back into the inside…should be this way anyway

Example 2-----

Access-list NO-NAT extended permit ip “inside-ip” “inside mask” “DMZ subnet” “DMZ mask”

(config)#Nat (inside) 0 NO-NAT

#Nat (inside) 1 “ip address of inside” “mask of inside”

#Global (outside) 1 interface

This allows inside to dmz without nat, but uses nat to go from inside to outside

Example 3---

(config)#Access-list INSIDE-IN extended permit tcp x.x.x.x x.x.x.x host x.x.x.x eq 25

#Access-list INSIDE-IN extended deny ip x.x.x.x x.x.x.x host x.x.x.x

#Access-list INSIDE-IN extended permit ip x.x.x.x x.x.x.x any –ips are same for these 3

#Access-group INSIDE-IN interface inside

#Access-list NO-NAT extended permit x.x.x.x x.x.x.x x.x.x.x x.x.x.x –ips are inside and dmz

#Nat (inside) 0 access list NO-NAT

#Nat (inside) 1 x.x.x.x x.x.x.x

#Global(outside) 1 interface

This lets inside traffic to email in dmz, then deny all else to dmz, and then allow all other out

And does not nat to email but nats to outside

OBJECT GROUPS

4 types:

Network – used to group ips

Service – used to group tcp or udp ports

Protocol – used to group protocols

ICMP-type – used to group icmp message types

NETWORK

(config)#Object-group network “group\_name”

#Network-object host x.x.x.x –host

#Network-object “net\_address netmask” – subnet

EXAMPLE

(config)#Object-group network WEB\_SRV

#Network-object host 10.1.1.1

#Network-object host 10.1.1.2

#Object-group network DMZ\_SUBNET

#Network-object 10.1.1.0 255.255.255.0

#Access-list OUTSIDE-IN extended permit tcp any object-group WEB-SRV eq 80

--creates an object group for the web servers and an object group for all dmz addresses and then applies an acl to allow access from anywhere

SERVICE

Object-group service “group-name” {tcp | udp | tcp-udp}

Port-object {eq | range}

Exit

EXAMPLE

(config)#Object-group service DMZ\_SERVICES tcp

#Port-object eq http

#Port-object eq https

#Port-object range 21 23

#Object-group DMZ\_SUBNET

#Network-object 10.0.0.0 255.255.255.0

#Access-list OUTSIDE-IN extended permit tcp any object-group DMZ\_SUBNET object group DMZ\_SERVICES

--This allows outside traffic into the DMZ from any address to the DMZ subnet on ports 21,22,23,80, and 443

VLANS and SUBINTERFACES

EXAMPLE

(config)#Interface gi0/0

(config)#No nameif

#no security-level

#no ip address

#exit

(config)#int gi0/0.10

#vlan 10

#nameif inside1

#security-level 80

#ip address 192.168.1.1 255.255.255.0

(config)# int gi0/0.20

#vlan 20

#nameif inside2

#security-level 90

#ip address 192.168.2.0 255.255.255.0

--creates different security levels for 2 vlans, asa port must be plugged into a trunk port on the switch

CLOCK and NTP

(config)#Clock set hh:mm:ss [day month | month day] year

Show clock to check

Time zone and DST

(config)#clock timezone [zone name] [offset hours from utc]

(config)#clock summer-time [zone name] recurring [week weekday month hh:mm week weekday month hh:mm] [offset]

NTP

(config)#ntp server [ip address of NTP] source [interface name]

(config)#ntp server 10.1.1.1 source inside

IF AUTHENTICATE

(config)#ntp authenticate

#ntp authentication-key [key ID] md5 [ntp key]

#ntp trusted-key [key ID]

#ntp server [ip of server] key [key ID] source [int name]

LOGGING

(config)#logging enable -----MUST DO

(config)#logging timestamps ---adds timestamp

(config)#logging monitor ---for ssh and telnet

(config)#logging console ---for console cable

(config)#logging adsm

(config)#logging host [int name] [syslog ip] ---external syslog server

(config)#logging trap [logging level]

#logging host inside 192.1.1.1

#logging trap errors

(config)#snmp-server host inside 10.1.1.1 trap community [community name] –to send to snmp

#snmp-server enable traps syslog

#logging history warnings

LEVELS – each level auto includes lower number levels

0-emergencies

1-alerts

2-critical

3-errors

4-warnings

5-notifications

6-informational

7-debugging

LOCAL AUTHENTICATION

(config)# username blah password blah

(config)#aaa authentication [serial/telnet/ssh/http/enable] console LOCAL -serial=console cable

#aaa local authentication attempts max-fail 5

#clear aaa local user lockout all

MODULAR POLICY FRAMEWORK

Traffic match with class-map, then actions applied with policy-maps, finally policy is applied to interface with service-policy

(config)#class-map [class name]

#match access-list [ACL name] -or

#match port [tcp/udp] [eq port\_no/ range port port] -or

#match any -or

#match default-inspection-traffic

#show run class-map

By default there is a default class-map and default-inspection-traffic

----page 98