Firewall da usare: 5506-X

1-Impostare indirizzi ip e gateway dei pc collegati

PC1: 192.168.0.1 (INSIDE)

PC2: 192.168.1.1 (OUTSIDE)

Collegare i pc al firewall sulle Gig 1/1 e 1/2

2-Configurare le Gigabit Ethernet (gateway, subnetmask e no shutdown)

3-Definizione rete inside e outside

Rete inside (interface gig1/1): nameif inside (livello di sicurezza 100, max)

Rete outside (interface gig1/2): nameif outside (livello di sicurezza 0 min)

Rete dmz (interface gig1/3): nameif dmz (livello di sicurezza medio (50), ci sono i server di solito)

Per cambiare il livello di sicurezza: security level n (show route per visualizzare le connsessioni);

4-Definizione ACL firewall

ACL generale: access-list “nome” extended “permit/deny” “protocollo” ipM wildCardM ipD wildCardD “echo-reply/niente”

Access-group “nome” in/out interface inside/outside

//echo-reply: permette solo le risposte

ACL1: deve permettere al pc sulla rete outside di rispondere al pc della rete inside

-Semplice: ACL gig1/1: access-list prima_acl extended permit icmp any any echo-reply

(Interface gig1/1): access-group prima_acl out interface inside

-Più complessa: ACL gig1/1: access-list prima_acl extended permit icmp 192.168.1.0 255.255.255.0 192.168.0.1 255.255.255.255 echo-reply

(Interface gig1/1): access-group prima_acl out interface inside

Configurazione wildcard mask: è il contrario, 0 non controlla mentre 1 si.

Rete Outside: Default routing

route inside/outside ip ipD subnetMask nexthop/

Esempio: route outside 0.0.0.0 0.0.0.0 100.1.1.1

Rete Inside: Static routing

route inside 192.168.2.0 255.255.255.0 192.168.1.1

AAA

Con il termine AAA si indica un insieme di protocolli usati per gestire gli accessi a una rete informatica. Gli accessi vengono di solito distinti nelle fasi di autenticazione, autorizzazione e accounting.

Autenticazione: consiste nel verificare l'identità dell'entità che richiede l'accesso alla rete.

Autorizzazione: ha a che fare con le azioni che l'utente può compiere una volta che si è autenticato.

Accounting: permette di tenere traccia dei comportamenti e delle risorse consumate dall'utente e permette di conoscere quali servizi sono stati usati ed è utile sia per stimare l'uso delle risorse da parte degli utenti e quindi per prevedere i bisogni futuri sia per identificare tempestivamente eventuali problemi di sicurezza.

1-Configuriamo indirizzi ip, gateway e le fastEthernet del router.

2-Configuriamo il servizio AAA sul router:

Router(config)# aaa new-model

Router(config)# aaa authentication enable default group radius

Router(config)# aaa authentication login default group radius

Router(config)# aaa authorization exec default group radius

Router(config)# radius-server host 192.168.0.253 (a quale server radius si riferisce) key cisco

Router(config)# hostname casa

casa(config)#

3-Attivare il servizio AAA sul server

-Client name: casa

-Client IP: 192.168.0.254 (gateway del router)

-Secret: cisco (key)

-ServerType: Radius

-Username: Marco

-Password: password

4-Dal pc, bisogna andare in desktop/command prompt e pingare

telnet 192.168.0.254

DHCP

Il protocollo DHCP viene usato per automatizzare l'assegnazione la configurazione di TCP/IP dei diversi client in una intranet: è possibile infatti assegnare indirizzo IP, i due DNS, i due server WINS e l'eventuale Gateway che il client dovrà utilizzare.

1-Attivare fastEthernet e impostare indirizzi ip e gateway

2-Configurare il dhcp sul router

Router(config)# ip dhcp pool pool_sx

Router(dhcp-config)# network 192.168.0.0 255.255.255.0 (rete dove agisce il dhcp)

Router(dhcp-config)# default-router 192.168.0.254 (gateway)

Router(dhcp-config)# ip dhcp excluded-address 192.168.0.254

Router(config)# ip dhcp pool pool_dx

Router(dhcp-config)# network 192.168.1.0 255.255.255.0 (rete dove agisce il dhcp)

Router(dhcp-config)# default-router 192.168.1.254 (gateway)

Router(dhcp-config)# ip dhcp excluded-address 192.168.1.254

3-Andare sul pc e spuntare DHCP sulla fastEhternet (oppure su ip-configuration)

Access point-WLC-VLAN

1-Collegare tutto e impostare gli ip/gateway

2-Creare i dhcp

Router(config)#ip dhcp pool mng;

Router(config)#ip dhcp pool 10;

Router(config)#ip dhcp pool 20;

3-Creare le Vlan sul router e sullo switch

Router (config)# int g/0/0.10

Router (config-subif)# encapsulation dot1q 10

Router (config-subif)# ip address 192.168.10.254 255.255.255.0

Router (config-subif)# int g/0/0.20

Router (config-subif)# encapsulation dot1q 20

Router (config-subif)# ip address 192.168.20.254 255.255.255.0

Router (config-if)# no shutdown

Switch(config)# vlan 10

Switch(config)#exit

Switch(config)# vlan 20

Switch(config)#int fa2/1

Switch(config-if)#switchport mode trunk

Switch(config)#int eth6/1 7/1

Switch(config-if)#switchport mode trunk

4-Andare sul WLC

Wireless LANs

-Name: wlan10; vlan 10, SSID (wlan10); WPA2-PSK (cisco123)

-Name: wlan20; vlan 20, SSID (wlan20); WPA2; 192.168.0.252 (server); cisco123.

Su management:

-ip: 192.168.0.253; subnet mask: 255.255.255.0; gateway: 192.168.0.254.

5-Andare nel server

-AAA. Client name: WLC; secret: cisco123; ip: 192.168.0.253; username: marco; password: marco.

6-Access Point: Collegare l'alimentazione.

7-Andare sui laptop:

Laptop2:

-Mettere il wireless;

-Andare su wireless0:

- SSID: wlan10;
- WPA2-PSK: cisco123

Laptop1:

-Mettere il wireless;

-Andare su wireless0:

- SSID: wlan20;
- WPA2- id: marco, password: marco.