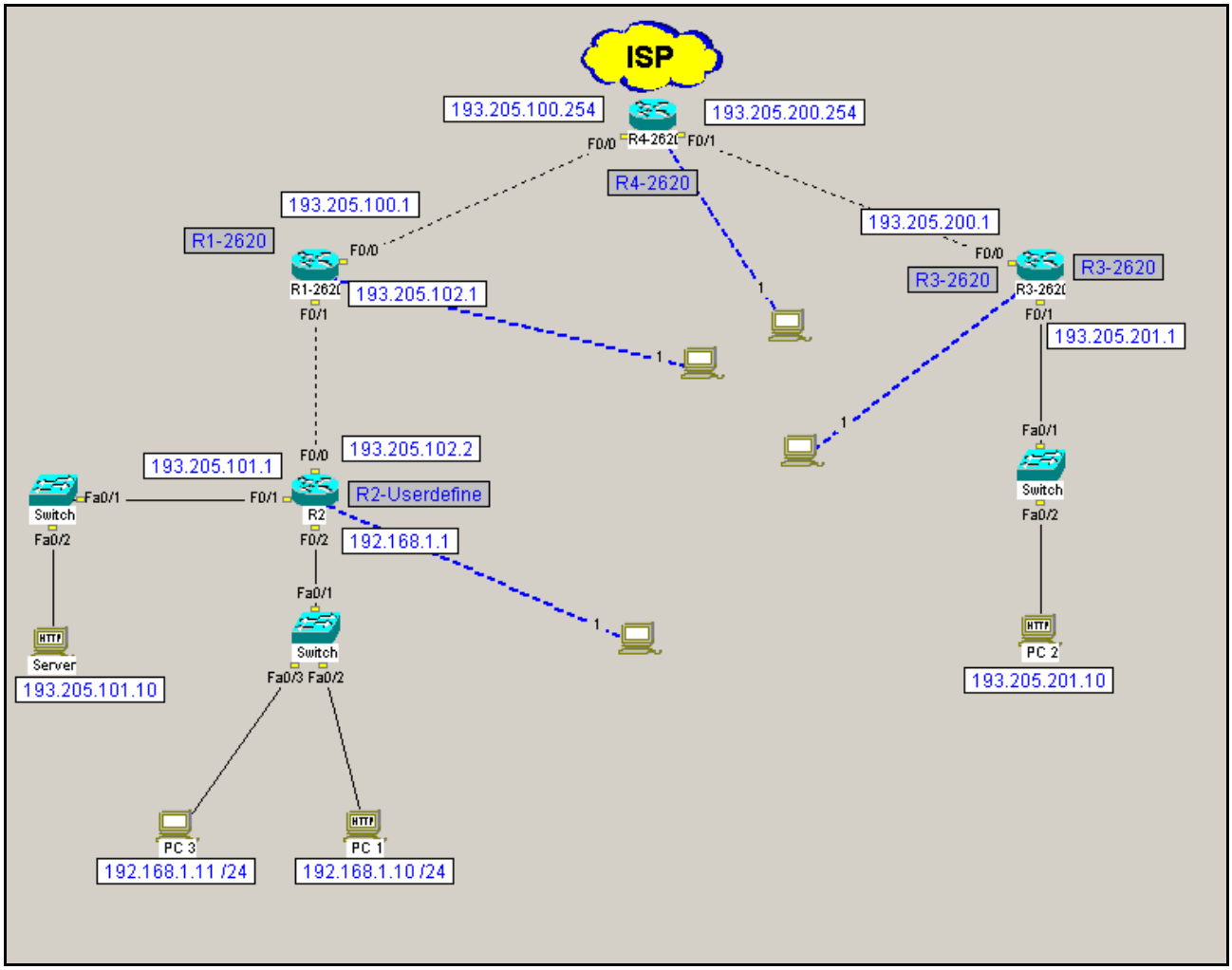
ESERCIZIO – DMZ



Obiettivo:

Si vuole collegare ad Internet una LAN, disegnata a sinistra, composta da:

● un router R2 (Cisco User-Defined con tre interfacce Ethernet e nessuna porta seriale) avente funzionalità di firewall packet filtering

● una Intranet (rappresentata da due PC sulla rete 192.168.1.0 (collegati al router R2 mediante uno switch Cisco 2950), sul PC 1 è disponibile il server web della Intranet

● una DMZ, nella quale è situato un Web server che risponde all'indirizzo IP

193.205.101.10. Tale web server è collegato al router R2 mediante uno switch Cisco 2950

Per eseguire il collegamento ad Internet si è acquistato il router R1 (Cisco 2620) e lo si è connesso alla rete del provider con indirizzo IP 193.205.100.1

Il router del provider ha indirizzo 193.205.100.254

NOTE:

- Per semplicità di configurazione, si rappresenta la rete Internet esterna con il solo router R4 di tipo Cisco 2620, fornito dal provider.

- La rete esterna è rappresentata dal router R3, che vede collegato, tramite switch Cisco 2950, un Web Server (PC2) avente indirizzo IP 193.205.201.10

- Sempre per semplicità ed evitare l'introduzione di regole di natting,vengono usati, per gli indirizzi del router R2, indirizzi pubblici al posto di indirizzi privati; in una situazione reale l'uso di indirizzi pubblici per host non visibili su Internet è sconsigliato, consentendo le tecniche di natting il risparmio di indirizzi IP pubblici e maggior sicurezza.

- Il firewall, rappresentato dal router R2 con tre schede di rete, va configurato con delle semplici regole di packet filtering. Non si applicano protezioni (consigliate) del tipo stateful inspection o proxy, per esigenze di semplicità dell'esercizio.

- Fare attenzione ai cavi: Netsimk controlla anche che il tipo di cavo di collegamento sia quello corretto. Usare sempre un cavo incrociato per collegare due router ed un cavo seriale per collegare ad un dispositivo di rete il PC da usare per la configurazione. Il bottone "CHECK CONFIGURATION" di Netsimk evidenzia gli eventuali errori.

SCOPO DELL'ESERCIZIO

- Si devono porre in essere delle ACL extended (*) sul router R2, che funge da firewall three-legged di tipo packet filtering, in modo che non sia, in alcun modo, possibile collegarsi, dall'esterno, al server web della rete Intranet .

- Il server web in Intranet deve essere raggiungibile dal solo host della DMZ
- L'host in Intranet deve potersi collegare a qualsiasi host esterno (quindi deve essere consentito il traffico di risposta (**)).
- Tutti i pacchetti ICMP devono essere disabilitati ad eccezione del ping

(*) Con il termine ACL extended si intendono le regole, aventi numerazione compresa fra 100 e 199, che consentono di autorizzare o bloccare i pacchetti in base ai valori di indirizzo IP sorgente, maschera, porta sorgente, indirizzo IP destinatario, maschera, porta destinatario
(**) Non si può applicare l'opzione established che autorizza i pacchetti di ritorno (pacchetti con flag ACK/RST on) in quanto il simulatore non implementa questa possibilità. Per autorizzare il ritorno dei pacchetti si deve far ricorso quindi alle porte efemerali.

SOLUZIONE

R1:

Colleghiamo un pc a R1 con un cavo console e apriamo Hyperterm

```
Router #enable
Router #conf t
Enter configuration commands, one per line. End with CNTL/Z.
```

Impostiamo il nome del Router

```
Router(config)#hostname R1-2620
```

Configuriamo l'interfaccia Fastethernet 0/0

```
R1-2620(config)#interface f0/0
R1-2620(config-if)#ip address 193.205.100.1 255.255.255.0
R1-2620(config-if)#no shutdown
R1-2620(config-if)#exit
```

Configuriamo l'interfaccia Fastethernet 0/1

```
R1-2620(config)#interface f0/1
R1-2620(config-if)#ip address 193.205.102.1 255.255.255.0
R1-2620(config-if)#no shutdown
R1-2620(config-if)#exit
```

Impostiamo il RIP

```
R1-2620 (config)#router rip
R1-2620(config)# network 193.205.102.0
R1-2620(config)# network 193.205.100.0
```

R2:

Colleghiamo un pc a R2 con un cavo console e apriamo Hyperterm

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

Impostiamo il nome del Router

```
Router(config)#hostname R2
```

Configuriamo l'interfaccia Fastethernet 0/0

```
R2(config)#int f0/0
R2(config-if)#ip address 193.205.102.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
```

Configuriamo l'interfaccia Fastethernet 0/1

```
R2(config)#int f0/1
R2(config-if)#ip address 193.205.101.1 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)#exit
R2(config)#
```

Configuriamo l'interfaccia Fastethernet 0/2

```
R2(config)#int f0/2
R2(config-if)#ip address 192.168.1.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
```

Impostiamo il RIP

```
R2(config)#router rip
R2(config-router)#  network 193.205.102.0
R2(config-router)#  network 192.168.1.0
R2(config-router)#  network 193.205.101.0
```

R4:

Colleghiamo un pc a R4 con un cavo console e apriamo Hyperterm

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Configuriamo l'interfaccia Fastethernet 0/0

```
Router(config)#interface F0/0
Router(config-if)#ip address 193.205.100.254 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
%LDXX - Line protocol on Interface FastEthernet0/0, changed state to up
```

Configuriamo l'interfaccia Fastethernet 0/1

```
Router(config)#interface F0/1
Router(config-if)#ip address 193.205.200.254 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
Router(config)#
%LDXX - Line protocol on Interface FastEthernet0/1, changed state to up
```

Impostiamo il RIP

```
Router(config)#router rip
Router(config-router)#network 193.205.100.0
Router(config-router)#network 193.205.200.0
Router(config-router)#exit
```

Impostiamo il nome del Router

```
Router(config)#hostname R4-2620
R4-2620(config)#
```

R3:

Colleghiamo un pc a R3 con un cavo console e apriamo Hyperterm

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Impostiamo il nome del Router

Router(config)#hostname R3-2620

Configuriamo l'interfaccia Fastethernet 0/0

R3-2620(config)#interface F0/0
R3-2620(config-if)#ip address 193.205.200.1 255.255.255.0
R3-2620(config-if)#no shutdown
R3-2620(config-if)#exit
R3-2620(config)#
%LDXX - Line protocol on Interface FastEthernet0/0, changed state to up

Configuriamo l'interfaccia Fastethernet 0/1

R3-2620(config)#interface F0/1
R3-2620(config-if)#ip address 193.205.201.1 255.255.255.0
R3-2620(config-if)#no shutdown
R3-2620(config-if)#
%LDXX - Line protocol on Interface FastEthernet0/1, changed state to up
R3-2620(config-if)#exit

Impostiamo il RIP

R3-2620(config)#router rip
R3-2620(config-router)#network 193.205.200.0
R3-2620(config-router)#network 193.205.201.0
R3-2620(config-router)#
Configuriamo ora gli indirizzi ip dei server della Intranet, della DMZ e del server http in Intranet:

Configuriamo il Server http in Intranet

Indirizzo IP del server web in Internet : 192.168.1.10 255.255.255.0
Gateway: 192.168.1.1

Dopo aver configurato l'indirizzo IP attiviamo l'http server.

Da questo host proviamo a pingare tutte le interfacce di rete dei router.

Configuriamo il Server Server http in DMZ

Indirizzo IP del server web in DMZ : 193.205.101.10 255.255.255.0
Gateway: 193.205.101.1

Anche su questo host, configurato l'indirizzo IP, attiviamo l'http server.

Da questo host proviamo a pingare tutte le interfacce di rete dei router ed il server in Intranet. Noteremo che il ping avviene senza problemi.
Proviamo anche ad aprire Internet Explorer (disattivando il proxy se presente usando il bottone PROXY nell'interfaccia del browser) e verifichiamo che sia possibile dalla DMZ connettersi al server web in Intranet (PC 1: 192.168.1.10)

Verifichiamo anche il contrario ossia che da Intranet (PC1 e PC2) sia raggiungibile il server http in DMZ (ricordarsi di disattivare in IE il proxy se impostato)

Configuriamo il Server http in Internet (PC2)

Indirizzo IP da assegnare al server Web in Internet:
193.205.201.10 255.255.255.0
Gateway: 193.205.201.1

Infine attiviamo su questo host l'http server (basta attivare il relativo flag nella finestra richiamabile dall'icona Server Applications).

Da questo host proviamo a pingare tutte le interfacce di rete dei router e i pc.

Noteremo che:

Il ping avviene senza problemi, in quanto le tabelle di routing sono correttamente configurate.

Inoltre a questo punto non sono state ancora attivate delle ACL.

```
C:>ping 193.205.201.1

Pinging 193.205.201.1 with 32 bytes of data:

Reply from 193.205.201.1 on Eth, time<10ms TTL=80
Reply from 193.205.201.1 on Eth, time<10ms TTL=80
Reply from 193.205.201.1 on Eth, time<10ms TTL=80
Reply from 193.205.201.1 on Eth, time<10ms TTL=80



C:>ping 193.205.200.254

Pinging 193.205.200.254 with 32 bytes of data:

Reply from 193.205.200.254 on Eth, time<10ms TTL=79
Reply from 193.205.200.254 on Eth, time<10ms TTL=79
Reply from 193.205.200.254 on Eth, time<10ms TTL=79
Reply from 193.205.200.254 on Eth, time<10ms TTL=79



C:>ping 193.205.100.1

Pinging 193.205.100.1 with 32 bytes of data:

Reply from 193.205.100.1 on Eth, time<10ms TTL=78
Reply from 193.205.100.1 on Eth, time<10ms TTL=78
Reply from 193.205.100.1 on Eth, time<10ms TTL=78
Reply from 193.205.100.1 on Eth, time<10ms TTL=78



C:>ping 193.205.102.2

Pinging 193.205.102.2 with 32 bytes of data:

Reply from 193.205.102.2 on Eth, time<10ms TTL=77
Reply from 193.205.102.2 on Eth, time<10ms TTL=77
Reply from 193.205.102.2 on Eth, time<10ms TTL=77
Reply from 193.205.102.2 on Eth, time<10ms TTL=77



C:>ping 193.205.101.1

Pinging 193.205.101.1 with 32 bytes of data:

Reply from 193.205.102.2 on Eth, time<10ms TTL=77
Reply from 193.205.102.2 on Eth, time<10ms TTL=77
Reply from 193.205.102.2 on Eth, time<10ms TTL=77
```

```
Reply from 193.205.102.2 on Eth, time<10ms TTL=77



C:>ping 193.205.101.10

Pinging 193.205.101.10 with 32 bytes of data:

Reply from 193.205.101.10 on Eth, time<10ms TTL=124
Reply from 193.205.101.10 on Eth, time<10ms TTL=124
Reply from 193.205.101.10 on Eth, time<10ms TTL=124
Reply from 193.205.101.10 on Eth, time<10ms TTL=124



C:>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Ping request timed out.
Reply from 192.168.1.11 on Eth, time<10ms TTL=124
Reply from 192.168.1.11 on Eth, time<10ms TTL=124
Reply from 192.168.1.11 on Eth, time<10ms TTL=124



C:>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Ping request timed out.
Reply from 192.168.1.10 on Eth, time<10ms TTL=124
Reply from 192.168.1.10 on Eth, time<10ms TTL=124
Reply from 192.168.1.10 on Eth, time<10ms TTL=124
```

Verificata la corretta configurazione della rete andiamo ora ad impostare le ACL che soddisfino i requisiti di sicurezza richiesti dall'esercizio.

Andiamo quindi a configurare il nostro firewall (R2), in modo da consentire l'accesso al solo server web della DMZ isolando completamente la rete Internet.

Inoltre disabilitiamo completamente il protocollo ICMP ad eccezione delle risposte (echo-reply) al comando ping inviato da Intranet e DMZ.

L'interfaccia che considereremo è quella che invia/riceve il traffico a/da Internet ossia l'interfaccia f0/0 che ha indirizzo IP 193.205.102.2.

Le regole che verranno definite saranno applicate (con comando access-group .. in) al

traffico in ingresso su questa interfaccia.

Quando si definiscono delle ACL è sempre importante non far confusione sul senso del traffico. Per traffico di tipo in si intende quello che entra nel router; analogamente il traffico di tipo out è quello che lascia il router.

Per il traffico in uscita dal router sull'interfaccia f0/0, non vengono definite, in questo esercizio, delle regole di filtering e quindi tutto il traffico in uscita verso Internet sarà permesso.

Prima di iniziare verifichiamo di riuscire a pingare la intranet dall'esterno:

C:>ping 192.168.1.11

```
Pinging 192.168.1.11 with 32 bytes of data:

Ping request timed out.
Reply from 192.168.1.11 on Eth, time<10ms TTL=124
Reply from 192.168.1.11 on Eth, time<10ms TTL=124
Reply from 192.168.1.11 on Eth, time<10ms TTL=124
```

```
C:>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10 on Eth, time<10ms TTL=124
Reply from 192.168.1.10 on Eth, time<10ms TTL=124
Reply from 192.168.1.10 on Eth, time<10ms TTL=124
Reply from 192.168.1.10 on Eth, time<10ms TTL=124
```

Andiamo quindi su R2

```
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

Impostiamo l'ACL per i pacchetti tcp in entrata sull'interfaccia f0/0 (inbound) permettiamo tutto il traffico http, qualsiasi sia l'host di provenienza, diretto al server web in DMZ avente indirizzo 193.205.101.10

```
R2(config)# access-list 110 permit tcp any host 193.205.101.10 eq www
```

E' importante ricordare che il router applica, per ogni pacchetto, le regole, nello stesso ordine con il quale sono state scritte e che se nessuna delle regole è soddisfatta il pacchetto viene scartato.

Applichiamo infine l'ACL all'interfaccia Fastethernet 0/0 per il traffico inbound

```
R2(config)#interface F0/0
```

applichiamo le regole identificate dalla chiave 110 al traffico inbound (in), ossia ai pacchetti che arrivano da altre reti su questa interfaccia ed entrano nel router; se invece si trattasse di applicare delle regole ai pacchetti uscenti la parola da usare sarebbe out (outbound)

```
R2(config-if)#ip access-group 110 in
R2(config-if)#exit
```

Gia così non riusciremo più a pingare la Intranet, in quanto avendo messo la regola precedente, implicitamente blocchiammo tutto il traffico restante.

```
C:>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Ping request timed out.
Ping request timed out.
Ping request timed out.
Ping request timed out.
```

```
C:>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:

Ping request timed out.
Ping request timed out.
Ping request timed out.
Ping request timed out.
```

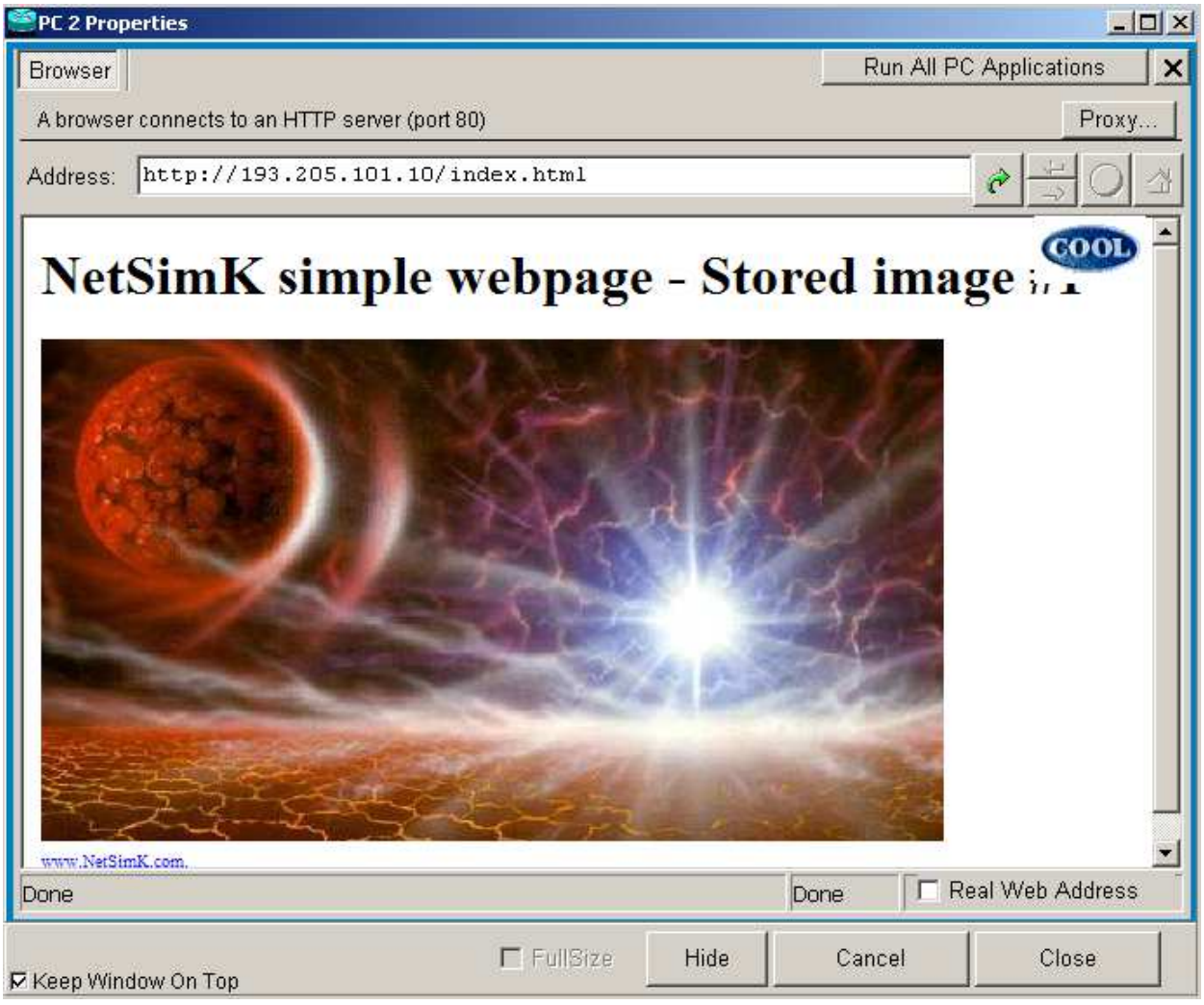
Non si riesce però a pingare neanche il server web della DMZ.

```
C:>ping 193.205.101.10

Pinging 193.205.101.10 with 32 bytes of data:

Ping request timed out.
Ping request timed out.
Ping request timed out.
Ping request timed out.
```

Però riusciamo a raggiungerlo via www



Per consentire la risposta ai ping aggiungiamo la seguente ACL

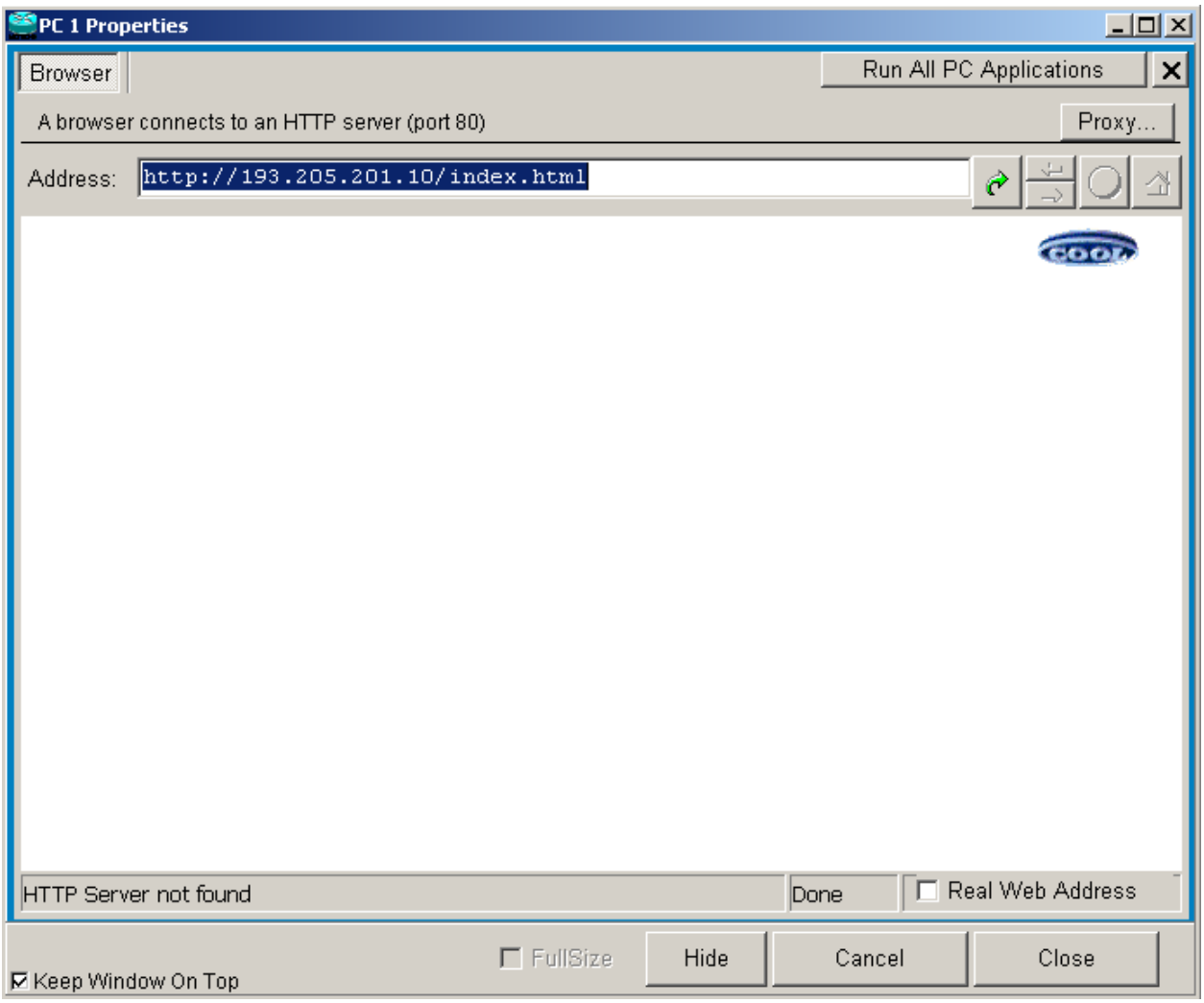
```
R2(config)#access-list 110 permit icmp any any echo
```

Nota: le regole sopra descritte, essendo di tipo extended, devono essere numerate con un valore compreso fra 100 e 199
A questo punto i requisiti sembrerebbero soddisfatti; si potrebbero applicare quindi le ACL all'interfaccia f0/0.

Notiamo però che, essendo bloccato tutto il traffico TCP in ingresso sull'interfaccia f0/0, ad eccezione di quello diretto alla porta 80 del web server in DMZ, l'host in Intranet non riceverebbe risposta qualora si collegasse al server web in Internet.

Infatti quando un client della Intranet si collega al server web in Internet riceve i pacchetti di risposta su porte efemerali (porta >= 1024) e questo tipo di traffico viene bloccato con le regole finora impostate.

Proviamo a connetterci al server esterno dal PC 1:



Lo stesso accade per la DMZ.

Occorre quindi fare in modo che i pacchetti diretti alle porte efemerali del server web in Intranet, in risposta a pacchetti inviati precedentemente, possano passare attraverso il firewall.

L'attuale versione di Netsimk non prevede l'utilizzo del parametro established (es. access-list 110 tcp any <Intranet network address> established) che consentirebbe il transito del traffico di risposta (ossia ai pacchetti con flag ACK/RST on).

Decidiamo quindi di lasciar passare, fra i pacchetti destinati alla Intranet, solo quelli destinati alle porte efemerali, assumendo, per questo solo fatto, che si tratti di pacchetti di risposta a richieste provenienti dalla Intranet.

Lo stesso andrebbe fatto per la DMZ ma, ai fini dell'esercizio, effettuiamo le modifiche solo per la Intranet.

Ovviamente l'apertura delle porte efemerali costituirebbe un problema di sicurezza nel caso fosse presente un trojan sul web server della Intranet in ascolto su una di queste porte. Questa è una delle ragioni che hanno portato nel tempo all'introduzione di regole stateful inspection, che però esulano dal contesto di questo esercizio. Definiamo quindi la regola che consente il passaggio del traffico di risposta sull'interfaccia f0/0 ed inseriamo le regole per bloccare tutto il traffico rimanente.

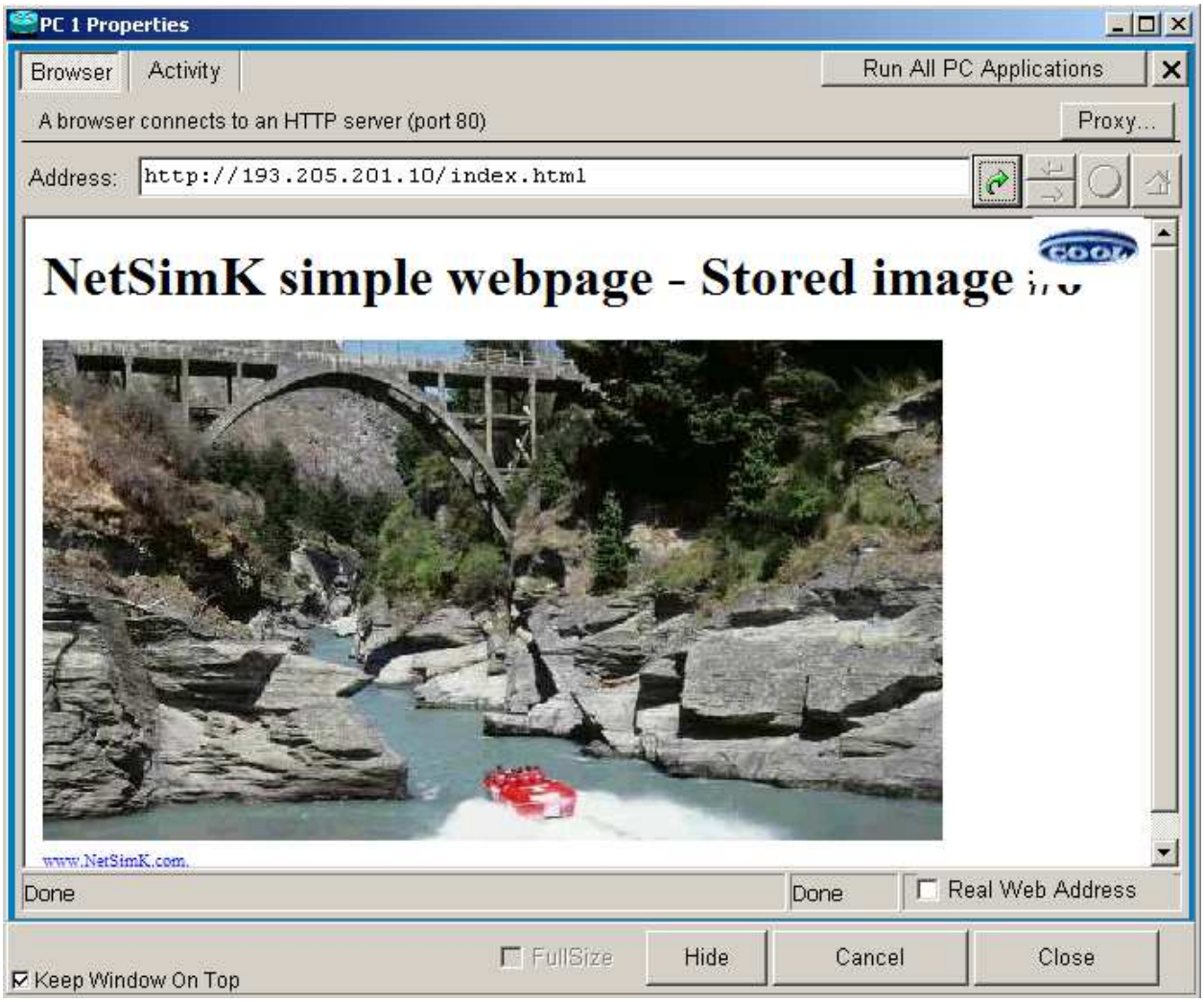
permettiamo tutto il traffico di ritorno diretto al server web Intranet;
per ora non abilitiamo il traffico in risposta alla DMZ

```
R2(config)#access-list 110 permit tcp any 192.168.1.10 0.0.0.0 gt 1024
```

Per controllare che tutto sia a posto eseguiamo il comando show access -list.

```
R2#sh access-lists
access-list 110 permit tcp any host 193.205.101.10 eq www
access-list 110 permit icmp any any echo
access-list 110 permit tcp any host 192.168.1.10 gt 1024
```

Proviamo ora a fare un refresh sul browser del PC 1:



Verifichiamo quindi che:

- da Internet sia raggiungibile il server web in DMZ ma non quello Intranet
- da Intranet siano raggiungibili i server web Internet e DMZ
- non sia possibile il ping dall'esterno né della DMZ né di Intranet

Potremo anche notare che da DMZ non si riesce a raggiungere Internet. Questo dipende dal fatto che non è stata configurata la regola per lasciare passare i pacchetti di risposta all'host in DMZ.

Aggiungiamo la seguente regola per ottenere il risultato voluto:

```
access-list 110 permit tcp any host 193.205.101.10 gt 1024
```