Esposizione su Internet dei Servizi di una Rete Locale

Esporre su Internet una **porzione** di rete locale significa avere un Server Web o un Server di Posta in Azienda e, al contempo, accessibili da Internet. Il fatto di avere i dati "fisicamente" posizionati all'interno della propria rete, ne semplifica notevolmente gestione e manutenzione. Per contro si può delegare ad un Maintainer esterno la gestione del servizio DNS che è l'operazione più complessa (nonostante i pochi aggiornamenti necessari).

I passi da seguire per **esporre** su Internet una **porzione** di **rete locale** sono i seguenti:

1) Acquistare un indirizzo IP pubblico. Si può acquistare :

- **Un singolo indirizzo IP** da un ISP, nel qual caso si continua ad utilizzare un collegamento **Punto Punto** verso un **Server PPP** dell'ISP.
- **Una intera rete di indirizzi IP** più o meno grande a seconda delle esigenze.

2) Acquistare e Registrare un **dominio** presso www.nic.it/domini. Es. **isisfermi.edu**

- L'acquisto di indirizzi IP può essere effettuato soltanto a potenze di due **a partire da 4**, cioè 4, 8, 16, etc. Nel caso di acquisto di una intera rete di indirizzi IP l'indirizzo "**esterno**" del router di uscita verso internet sarà comunque deciso dall'ISP, che dovrà anche provvedere a programmare la **tabella di routing del router stesso**. Gli indirizzi acquistati potranno essere utilizzati **a valle** del router per l'indirizzamento della "**parte pubblica**" della rete interna.

- In caso di acquisto di soli 4 indirizzi IP:
  - ✓ un indirizzo dovrà essere utilizzato come indirizzo di rete,
  - ✓ un indirizzo dovrà essere utilizzato come broadcast,
  - ✓ un indirizzo dovrà essere utilizzato per la porta interna del router
  - ✓ un solo indirizzo potrà essere utilizzato per il reale indirizzamento.

  In questo caso l'unico indirizzo disponibile potrà essere utilizzato per **indirizzare un singolo PC** oppure per indirizzare un **secondo router** a valle del router dell'ISP (esattamente come se si disponesse di un unico indirizzo IP). Peraltro la necessità di utilizzare un secondo router a valle del router dell'ISP spesso deriva dal fatto di non poter pienamente configurare a proprio piacimento il router dell'ISP, per cui si collega in modalità punto-punto un secondo router in grado di risolvere tutte le specifiche esigenze. Per il collegamento punto-punto fra i due router si possono però tranquillamente utilizzare indirizzi privati.

Per cui, per quanto concerne gli indirizzi pubblici,

- o si acquista un unico indirizzo IP pubblico
- o si acquistano direttamene otto/sedici indirizzi.

1° Soluzione : Rete Interna Unica

Una prima semplice soluzione potrebbe essere quella di acquistare un **unico indirizzo IP pubblico (ex: 1.2.3.4) da assegnare alla porta pubblica del router** ed esporre su Internet alcuni server della rete locale. Ad esempio:

Web Server 10.0.0.11
In ascolto sulla porta 80.
Esempio: IIS (Microsoft Internet Information Services), Apache, Tomcat.

Mail Server 10.0.0.12
In ascolto sulla porta **25** (messaggi in arrivo tramite SMTP), **110** e **143** (download tramite Client di Posta tramite POP3 e IMAP), **80** web Mail.
Esempio: Microsoft Exchange Server, Squirrell Mail, SME Server.

DNS Server 10.0.0.13
Il **DNS Server Autoritativo (Autorevole)** per il dominio **isisfermi.edu** deve contenere un file che associ ciascuna URL pubblica (es. www.isisfermi.edu) con il corrispondente indirizzo IP pubblico. Poiché si dispone di un **unico indirizzo pubblico 1.2.3.4**, tutte le varie URL dovranno far riferimento a quest'unico indirizzo che in realtà è **l'indirizzo del firewall**.
Il **DNS Server** dovrà contenere almeno i seguenti record:

record **A**	www.isisfermi.edu	1.2.3.4
record **A**	posta.isisfermi.edu	1.2.3.4
record **MX**	Mail Server	1.2.3.4

di solito non servono record NS (Name Server)

PROXY Server 10.0.0.14
Per la gestione del traffico in uscita (navigazione Internet), è possibile utilizzare un **Proxy Server** (es **SQUID**), che consente di installare vari **filtri di protezione** della navigazione. Il proxy tiene traccia sull'identità del richiedente e, in corrispondenza della risposta, provvede a convogliarla correttamente verso il client richiedente.

- I **vari browser della LAN devono essere configurati per inviare le richieste al Proxy**, il quale, se i criteri di filtro sono soddisfatti, provvederà a girare la richiesta al Router impostando se stesso come richiedente.

- **Il Firewall del router dovrà accettare come richieste HTTP soltanto quelle provenienti dal Proxy**. Doppio passaggio ma maggior controllo sulla navigazione.

Configurazione del servizio NAT sul Router

- Occorre definire sul router di uscita la **porta WAN** (**1.2.3.4**) come porta **NAT OUTSIDE**.
- Attivare un **servizio NAT in uscita**, tale da consentire l'uscita verso Internet degli utenti interni.

- Attivare un **servizio NAT in ingresso**, tale da consentire l'accesso da Internet verso i server interni.

NAT Dinamico in uscita

Per le richieste provenienti dall'interno verso l'esterno, il **Dynamic PAT** sostituisce

- l'**indirizzo privato** del mittente con l'**indirizzo pubblico** della porta **NAT OUTSIDE**
- la **porta** del mittente con una **porta effimera (maggiori di 1023)** generata dinamicamente.

NAT Statico in ingresso

Per le richieste provenienti dall'esterno verso l'interno, il servizio **NAT** provvede a sostituire l'**indirizzo pubblico di destinazione** (e relativa porta) con gli indirizzi **privati impostati** staticamente all'interno delle **ATT** (**Address Translation Table**).

Apertura delle porte in Uscita

Si possono chiudere tutte le porte, **aprendo in uscita** soltanto le seguenti:
Porta 80 per consentire agli utenti interni di accedere ai web server esterni.
Porta 443 (HTTPs) per consentire agli utenti interni di accedere alle pagine protette
Porta 25 per consentire agli utenti interni di inviare posta elettronica all'esterno.
Porta 53 per consentire al DNS interno di **risolvere** gli **Internet DNS Name** tramite l'accesso ad altri **DNS server esterni**.
Porte 110 143 per consentire agli utenti interni di **scaricare posta** dai Mail Server esterni mediante **Client di Posta.**

Apertura delle porte in Ingresso

Porta 80 per consentire agli utenti esterni l'accesso al web server locale (www.isisfermi.edu)
Porta 443 (HTTPS) se il sito gestisce dati sensibili accessibili soltanto attraverso HTTPS. In tal caso occorre installare sul web server un **certificato digitale ufficiale (150** €) o generato localmente.
Porta 25 per consentire agli utenti esterni di inviare posta elettronica al mail server locale.
Porta 53 per consentire ai DNS Server esterni di inviare richieste al DNS Server interno
Porte 110 e 143 per consentire agli utenti interni di scaricare la posta dall'esterno mediante **Client di Posta**.

Graficamente l'apertura delle porte in ingresso può essere rappresentata nel seguente modo:

	Public IP DEST	Public Port	Private IP	Private Port
WEB	1.2.3.4	80	10.0.0.11	80
MAIL	1.2.3.4	25	10.0.0.12	25
MAIL	1.2.3.4	110,143	10.0.0.12	110,143
DNS	1.2.3.4	53	10.0.0.13	53

La colonna **Public IP DEST** normalmente è sottintesa, riferendosi ovviamente alla porta **WAN** del router.
Avendo a disposizione **un unico indirizzo pubblico**, **ogni "Servizio" accettato in ingresso deve essere riferito ad una porta differente**. Sulla base della porta e della ATT, il Firewall deciderà su quale server instradare i messaggi.

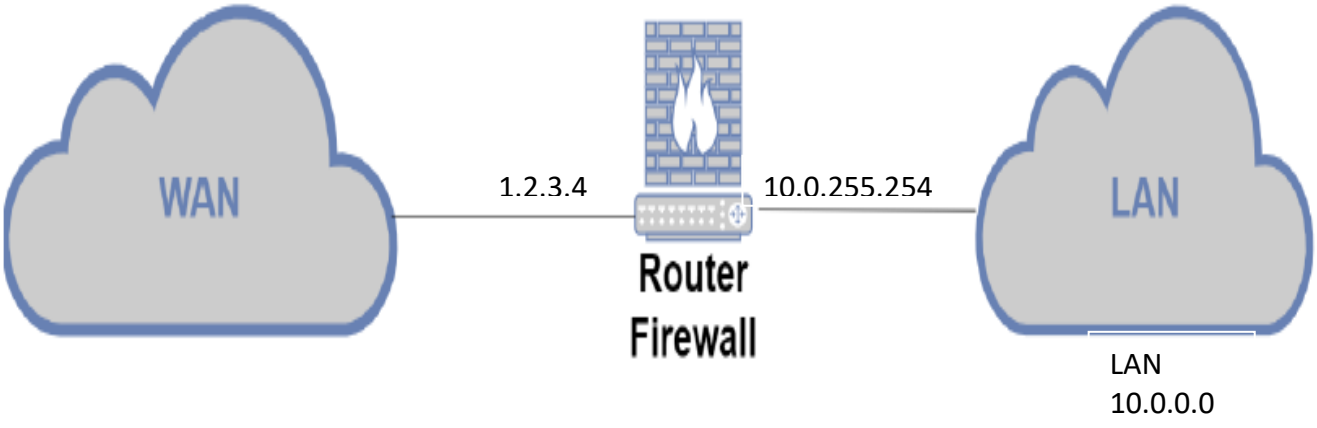
Gestione del servizio web mail

Rimane il problema di come consentire l'accesso web mail al Server di Posta. Se gli utenti devono consultare le proprie mail da casa via web, devono potersi connettere al server di posta locale sulla porta 80.
Poiché tutte le richieste arrivano al Firewall, e la porta 80 del Firewall è già utilizzata per reindirizzare le richieste verso il web server, non può essere utilizzata anche per reindirizzare le richieste relative al mail server. Tre soluzioni:

- Acquistare **più indirizzi IP pubblici** (eventualmente tutti concentrati sul Firewall), assegnando indirizzi IP differenti al Web Server (www.isisfermi.edu) rispetto al Mail Server (posta.isisfermi.Edu). Soluzione **pulita** ma più onerosa

- Una soluzione più semplice consiste nell'**aprire un'altra porta** sul Firewall (ad esempio 8080 o 2525) e costringere gli utenti della web mail ad utilizzare tale porta non standard da scrivere ogni volta sulla barra di navigazione: ***http://posta.isisfermi.edu:8080***

- Una terza e più brillante soluzione, supponendo di disporre di un **Firewall HTTP di livello 7**, è quella individuare il servizio richiesto non soltanto sulla base della porta di richiesta, ma sulla base del **DNS Name richiesto** e contenuto all'interno **dell'intestazione HTTP** (in pratica lo stesso principio dello **smart hosting**). In questo modo, a parità di indirizzo IP, se la richiesta riguarda **www.isisfermi.edu:80** viene inoltrata su **una certa macchina** (10.0.0.11), mentre se riguarda **posta.isisfermi.edu:80** viene inoltrata su **una macchina differente** (10.0.0.12).
  Funzionalità disponibile soltanto con **HTTP 1.1**



2° Soluzione : DMZ (Demilitarized Zone)

Aprire una o più porte di una LAN ad Internet, dal punto di vista della sicurezza, è estremamente pericoloso.

- **Il Firewall perimetrale esegue sì dei controlli sui pacchetti, ma non garantisce da virus e intrusioni.**
- **Inoltre sulle porte aperte deve necessariamente consentire l'accesso a chiunque ne faccia richiesta.** Se qualcuno riesce a prendere possesso di un PC della rete locale, questi avrà libero accesso all'intera rete.

Il passo successivo per avere maggiore protezione, è quello di inserire una **doppia barriera tra Rete Esterna e Rete Locale**, **separando fisicamente** i Server Pubblici dalla Rete Locale con un secondo Firewall a protezione della rete locale più **fine** del primo (soluzione **cuscinetto**). Le due porzioni di rete in cui viene suddivisa la rete locale sono dette rispettivamente

- **MZ** (**Militarized Zone**) cioè la **rete Locale** vera e propria, protetta dal 2° firewall con regole molto stringenti riguardo agli accessi (in pratica **blindata** rispetto ad Internet), avente ad es. l'indirizzo privato di **classe A 10.0.0.0.**
- **DMZ** (**Demilitarized Zone**) contenente tutti i server visibili su Internet (ad es. Mail Server, Web Server, DNS Server). Anche l'indirizzo della DMZ è un indirizzo privato, ad esempio **192.168.0.0**

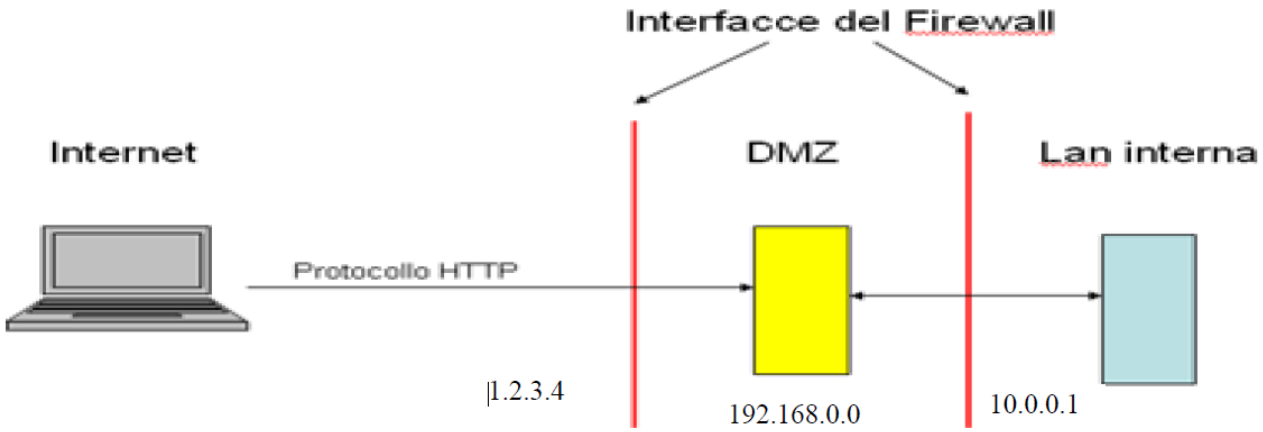
I server esposti su Internet rimangono così **separati** dalla LAN interna mediante un secondo Firewall. Le macchine inserite nel **DMZ** vengono solitamente indicate come **Server di Front End**, frontalmente esposti ad Internet, che **non contengono dati**, ma che fanno soltanto da **ponte** tra **Internet** e la **rete interna**.

Per contrapposizione i server interni alla rete locale, **contenenti i dati**, sono denominati **Server di Back End.**

Sul secondo firewall sono impostate delle regole molto stringenti che consistono nel bloccare tutte le richieste di accesso, tranne singole e specifiche eccezioni. In genere sono ammessi soltanto comunicazioni specifiche tra **un server di front-end con il suo rispettivo server di back-end**, e **solo** sulla singola porta necessaria. Ad esempio il **web server** del DMZ, (con indirizzo 192.168.0.3), può inviare richieste soltanto verso la macchina della LAN contenente il Database Server (es. SQL Server in ascolto sulla porta 1433 o 1521 nel caso di sql net).
In questo modo, anche supponendo che un hacker possa riuscire ad attaccare un server pubblico, da esso non riuscirà a fare partire un ulteriore attacco verso le macchine locali prima che i sistemi anti intrusione (funzione **IDS - Intrusion Detection System** degli antivirus) lo abbiano identificato ed abbiano intrapreso le adeguate contromisure difensive.

Schema Logico

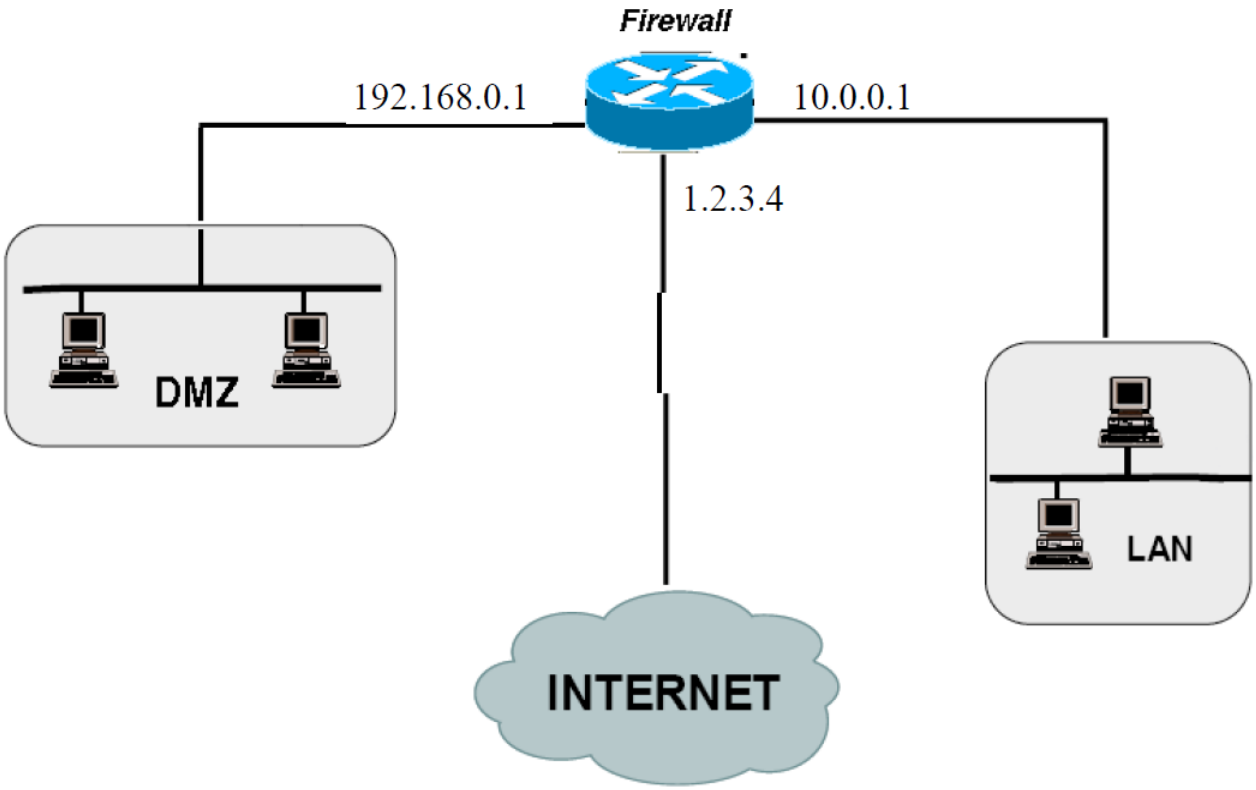
Da un punto di **vista logico**, la situazione precedente può essere illustrata nel modo seguente:



Le **richieste che arrivano da Internet** vengono filtrate dal **primo Firewall** che le **gira** al DMZ senza possibilità di accesso alla rete interna. Le richieste provenienti dalla LAN arrivano al Proxy Server della LAN che sostituisce l'indirizzo IP del richiedente con il proprio indirizzo IP (**10.0.0.2**) ed invia la richiesta al proprio Default Gateway (1° Firewall **10.0.0.1**). Il Firewall la gira al secondo Firewall (2° Firewall **192.168.0.1**) che, tramite NAT, sostituisce ancora una volta l'indirizzo del mittente (**10.0.0.1**) con il proprio indirizzo pubblico (**1.2.3.4**) e la invia all'esterno.

Schema Fisico

In genere, anziché utilizzare due macchine Firewall indipendenti, si utilizza una un **unico Router** dotato di una interfaccia **WAN** (1.2.3.4 collegata al **Router Pubblico**) e **due interfacce LAN** (10.0.0.1 e 192.168.0.1) collegate **rispettivamente** a LAN (rete 10.0.0.0) e **DMZ** (rete 192.168.0.0). (soluzione **vicolo cieco**).



Macchine da posizionare nel DMZ_(192.168.0.0)_____

Allo switch del DMZ vengono collocate tutte le macchine che devono essere accessibili dall'esterno; di solito :

1) DNS Server	porta 53
2) Web Server	porta 80
3) Mail Server	porta 25 + porta 80 per le web mail

Macchine posizionate all'interno del MZ_(10.0.0.0)_____

Primary Domain Controller (**PDC**), ad esempio **ADS** (Active Directory Server), **DHCP**, **Database Server**, **Proxy Server (se c'é). Ovviamente tutti gli host della rete.**

Programmazione del Firewall_____

Occorrerà programmare separatamente

- l'interfaccia WAN del Firewall, con attivazione del servizio NAT in ingresso (verso il DMZ) ed eventualmente in uscita (che potrebbe anche essere del tipo **CONSENTI TUTTO**)
- l'interfaccia LAN con possibilità agli utenti locali di uscire verso l'esterno **ma con regole molto stringenti per quanto riguarda le richieste verso l'interno**

In genere non vengono impostate regole sull'interfaccia relativa al DMZ.

ACL

Le **Access Control List**, sono **Liste di REGOLE** mirate a controllare il traffico in transito su un router **statefull inspection**. Ogni entry dell'Access Control List **abilita** o **nega** il passaggio dei pacchetti. Le **ACL semplici-standard** (oggi poco significative) tengono conto **soltanto dell'indirizzo IP Source**, mentre le **ACL Extended** sono costituite dalle **seguenti 4 colonne**

Porta Destinazione	*Indirizzo Destinazione*	*Indirizzo Sorgente*	*Azione*

- La porta del Sorgente, trattandosi di una porta effimera, non ha importanza.
- Azione può essere **NEGA** (**Deny**) oppure **CONSENTI** (**Allow**).

Sulla base delle informazioni contenute nella **ACL**, il **Firewall** decide se **Consentire** la richiesta, oppure **Bloccare** la richiesta. **Le regole devono essere scritte in sequenza dalle più specifiche (in testa) alle più generali (al fondo).**

In corrispondenza di ogni pacchetto, tutte le regole vengono scandite dalla cima al fondo dell'elenco.

Nel momento in cui una regola risulta soddisfatta, questa viene eseguita e la scansione interrotta

Sono possibili due tipi di Access List, **a seconda** di come viene impostato **l'ultimo record** in fondo alla lista :

- **Nega tutto** tranne i pacchetti che trovano corrispondenza nelle entry precedenti (**entry di consenso**). Quello autorizzato è espressamente scritto.
- **Lascia passare tutto** tranne i pacchetti che trovano corrispondenza nelle entry precedenti (**entry di negazione**)

Naturalmente la prima soluzione fornisce maggiore sicurezza e dunque risulta preferibile.

Le **Access Control List** possono essere definite **su ogni singola interfaccia del router** e, su ogni interfaccia, possono essere definite come

- **INBOUND** (cioè riferite al traffico **entrante** nel router)
- **OUTBOUND** (cioè riferite al traffico **uscente** dal router).

Quando un pacchetto si **presenta all'interfaccia del router** (indipendentemente che provenga dall'esterno o dal router), il router verifica

(1) se su quella interfaccia è stata definita una ACL

(2) se la ACL è definita nella stessa direzione del pacchetto (cioè se la ACL è INBOUND ed il pacchetto è entrante nel router *oppure* se la ACL è OUTBOUND ed il pacchetto è uscente dal router)

(3) In caso affermativo verifica se il pacchetto soddisfa ai requisiti dell'ACL. Una ACL OUTBOUND non ha influenza sul traffico INBOUND e viceversa.

Sequenza delle operazioni eseguite da un router

Dato un certo pacchetto **in ingresso** su una qualsiasi porta del router, il router esegue sempre la seguente sequenza:

PRE ROUTING

1) Verifica della INBOUND ACL relativa alla porta di ingresso del pacchetto.
2) Applicazione dell'eventuali traslazioni NAT in ingresso (solo nel caso della porta WAN, con sostituzione dell'indirizzo pubblico di destinazione con quello privato effettivo).
3) Consultazione **tabella di routing** e **scelta** della porta di **uscita**.

POST ROUTING

4) Applicazione dell'eventuali traslazioni NAT in uscita (solo nel caso della porta WAN, con sostituzione dell'indirizzo privato del sorgente con quello del router).
5) verifica della OUTBOUND ACL relativa alla porta di uscita del pacchetto.

Esempio

Si consideri la 2° soluzione precedente con un **router** a **3 porte (vicolo cieco) collegate** rispettivamente a :

- **Rete Interna 10.0.0.0**
- **DMZ indirizzo di rete 192.168.0.0** (192.168.0.2 DNS server, 192.168.0.3 Web server, 192.168.0.4 Mail Server)
- **WAN 1.2.3.4**

Dopo aver impostato sul Router una apposita tabella di routing, si possono impostare:

- Una **ACL INBOUND** sulla porta WAN,
- Una **ACL OUTBOUND** molto selettiva **sull'interfaccia LAN** relativa alla rete interna.

Sull'interfaccia DMZ in genere non si impostano ACL. Sull'**interfaccia WAN** occorre **abilitare il servizio NAT** sia in uscita per consentire l'accesso ad Internet sia in ingresso in modo da consentire l'accesso ai server del **DMZ**.

ACL interfaccia WAN INBOUND

L'utente esterno per qualunque servizio farà riferimento all'unico indirizzo pubblico assegnato al router di ingresso sul quale il servizio NAT, sulla base del numero di porta, ridirigerà la richiesta verso il corrispondente server del DMZ, sostituendo **IP DEST pubblico** con **l'IP PRIVATO** del server. Si tratta di decidere quali servizi abilitare. La tabella seguente mostra l'abilitazione dei principali servizi Internet.
Con un **firewall di livello 7 in grado di distinguere le richieste sulla base del DNS Name** si può aprire **la porta 80** in ingresso sia verso **il web server sia verso il mail server.**

Porta destinazione	*Indirizzo Mittente*	*Indirizzo Destinazione*	*Azione*
ACL porta WAN in INGRESSO			
80 (HTTP)	Qualsiasi	1.2.3.4 NAT 192.168.0.3	Consenti
80 web mail	Qualsiasi	1.2.3.4 NAT 192.168.0.4	Consenti
443 (HTTPs)	Qualsiasi	1.2.3.4 NAT 192.168.0.3	Consenti
443 web mail	Qualsiasi	1.2.3.4 NAT 192.168.0.4	Consenti
53 (DNS)	Qualsiasi	1.2.3.4 NAT 192.168.0.2	Consenti
25 (SMTP)	Qualsiasi	1.2.3.4 NAT 192.168.0.4	Consenti
110 (POP3) - 143 (IMAP)	Qualsiasi	1.2.3.4 NAT 192.168.0.4	Consenti
Qualsiasi	**Qualsiasi**	**Qualsiasi**	**Blocca**

In uscita verso la WAN non vengono impostate ACL OUTBOUND, lasciando tutte le porte aperte ed inserendo eventuali filtri di navigazione come ACL INBOUND sulla interfaccia relativa alla LAN.

ACL interfaccia LAN OUTBOUND

Come **protezione della LAN**, si può impostare sulla porta LAN (in uscita dal router e quindi entrante verso gli host della LAN) una ACL **OUTBOUND molto selettiva** che chiude tutte le porte con una unica eccezione che consente al **web server del DMZ** di indirizzare delle richieste verso il Server di database interno (ad esempio host **10.0.0.99** porta 1433 nel caso di SQL Server)

ACL porta LAN in USCITA (in uscita dal router)			
1433 (SQL Server)	192.168.0.3 (web server)	10.0.0.99 (SQL Server)	Consenti
Qualsiasi	Qualsiasi	Qualsiasi	Blocca

ADS porta 398; MySQL porta 3306; SQLServer porta 1433

ACL interfaccia LAN INBOUND

Per quanto riguarda le richieste provenienti dalla LAN (dirette verso il DMZ oppure verso la porta WAN) si può impostare la ACL indicata dalla tabella, in cui si aprono le principali porte sia verso il DMZ sia verso l'esterno WAN.

- POP3 e IMAP sono aperte soltanto verso il DMZ per cui non è possibile scaricare posta da server esterni.
- Gli utenti 10.0.0.41 – 10.0.0.80 non hanno accesso alla navigazione HTTP.
- **(*)** Se nella LAN fosse presente un Server Proxy, soltanto lui sarebbe abilitato a far uscire le richieste HTTP.

ACL porta LAN in INGRESSO (verso il router)			
80 (HTTP)	10.0.0.41 – 10.0.0.80	Qualsiasi	Blocca
80 (HTTP)	Qualsiasi (*)	Qualsiasi	Consenti
443 (HTTPs)	Qualsiasi	Qualsiasi	Consenti
53 (DNS) e 25 (SMTP)	Qualsiasi	Qualsiasi	Consenti
110 (POP3)	Qualsiasi	192.168.0.4	Consenti
143 (IMAP)	Qualsiasi	192.168.0.4	Consenti
Qualsiasi	Qualsiasi	Qualsiasi	Blocca