

# MICHELANGELO Office CX MICHELANGELO LAN CX

ADSL ROUTER



Manuale Operativo  
rev. 1.0 del 11/2004



**INDICE**

---

<b>PREMESSA</b>	<b>II</b>
CONDIZIONI AMBIENTALI	II
AVVERTENZE GENERALI	II
PULIZIA DELL'APPARATO	II
VIBRAZIONI O URTI	II
<b>DICHIARAZIONE CE DI CONFORMITA'</b>	<b>II</b>
<b>1. INTRODUZIONE</b>	<b>1.1</b>
1.1. CARATTERISTICHE	1.2
1.2. DESCRIZIONE PORTE E LED	1.3
<b>2. CONFIGURAZIONE ACCESSO INTERNET</b>	<b>2.1</b>
2.1. CONFIGURAZIONE LAN	2.1
2.2. CONFIGURAZIONE WAN	2.2
2.2.1. ABBONAMENTI ADSL CON AUTENTICAZIONE	2.2
2.2.2. ABBONAMENTI ADSL CON INDIRIZZO IP FISSO	2.3
<b>3. FUNZIONALITA' AVANZATE</b>	<b>3.1</b>
3.1. ESPORTAZIONE DI SERVIZI (VIRTUAL SERVER)	3.1
3.1.1. ESEMPIO CONFIGURAZIONE SERVER WEB	3.1
3.2. ESPORTAZIONE DEI SERVIZI (DMZ)	3.2
3.3. GENERALITÀ FIREWALL	3.3
<b>A. APPENDICE</b>	<b>A.1</b>
A.1. ELENCO PORTE TCP/UDP	A.1
A.2. ELENCO SERVER DNS	A.2

Per la versione completa di questo manuale,  
fate riferimento al formato PDF presente nel CD-ROM

For english language,  
please refer to the electronic version (PDF format)  
of this user guide on the supplied CDROM.

## PREMESSA

---

*E' vietata la riproduzione di qualsiasi parte di questo manuale, in qualsiasi forma, senza esplicito permesso scritto della Digicom S.p.A. Il contenuto di questo manuale può essere modificato senza preavviso.*

*Ogni cura è stata posta nella raccolta e nella verifica della documentazione contenuta in questo manuale, tuttavia la Digicom non può assumersi alcuna responsabilità derivante dall'utilizzo della stessa.*

Al fine di salvaguardare la sicurezza, l'incolumità dell'operatore ed il funzionamento dell'apparato, devono essere rispettate le seguenti norme installative:

## CONDIZIONI AMBIENTALI

---

Temperatura ambiente da -5 a +45°C

Umidità relativa dal 20 a 80% n.c.

Si dovrà evitare ogni cambiamento rapido di temperatura e umidità

- Polvere, umidità, calore elevato ed esposizione diretta alla luce del sole.
- Oggetti che irradiano calore. Questi potrebbero causare danni al contenitore o altri problemi.
- Oggetti che producono un forte campo elettromagnetico (altoparlanti Hi-Fi, ecc.)
- Liquidi o sostanze chimiche corrosive.

## AVVERTENZE GENERALI

---

Per tutti gli apparati alimentati direttamente da rete:

Classe di isolamento: solo quella indicata sull'etichetta dell'apparato

Correnti nominali: solo quelle indicate sull'etichetta dell'apparato

Per evitare scosse elettriche, non aprite l'apparecchio o il trasformatore. Rivolgetevi solo a personale qualificato.

Scollegate il cavo di alimentazione dalla presa a muro quando non intendete usare l'apparecchio per un lungo periodo di tempo.

Per scollegare il cavo tiratelo afferrandolo per la spina. Non tirate mai il cavo stesso.

In caso di penetrazione di oggetti o liquidi all'interno dell'apparecchio, scollegate il cavo di alimentazione e fate controllare da personale qualificato prima di utilizzarlo nuovamente.

## PULIZIA DELL'APPARATO

---

Usare un panno soffice asciutto senza l'ausilio di solventi.

## VIBRAZIONI O URTI

---

Attenzione a non causare vibrazioni o urti.

## DICHIARAZIONE DI CONFORMITA'

---

Noi, **Digicom S.p.A. via Volta 39 - 21010 Cardano al Campo (Varese - Italy)**

dichiariamo sotto la nostra esclusiva responsabilità, che i prodotti, Nome: **MICHELANGELO Office CX - MICHELANGELO LAN CX**

al quale questa dichiarazione si riferisce, soddisfano i requisiti essenziali della sotto indicata Direttiva:  
● **1999/5/CE** del 9 marzo 1999, R&TTE, (riguardante le apparecchiature radio e le apparecchiature terminali di telecomunicazione e il reciproco riconoscimento della loro conformità).

Come designato in conformità alle richieste dei seguenti Standard di Riferimento o ad altri documenti normativi:

- EN 55022
- EN 300 386
- EN 61000-3-2
- EN 61000-3-3
- EN 60950

## 1. INTRODUZIONE

### Gentile Cliente,

la ringraziamo per la fiducia accordataci nell'acquistare un prodotto Digicom.

**Michelangelo OFFICE CX o Michelangelo LAN CX** le permetterà di collegare il suo ufficio o dipartimento aziendale ad Internet in modo semplice ed efficiente.

Le stazioni della sua rete locale LAN avranno la possibilità di accedere ad Internet per la navigazione (WWW, HTTP) o l'accesso alla posta elettronica (e-mail) utilizzando la linea ADSL ed un abbonamento per singolo utente o multi-utente (con indirizzi IP globali). Tutte le operazioni di instaurazione del link saranno gestite in modo completamente automatico e trasparente da Michelangelo OFFICE CX, senza intervento alcuno da parte degli utilizzatori della rete.

Potrà inoltre sfruttare le funzionalità avanzate del Router per gestire in modo efficiente l'accesso ad Internet dei suoi computer, realizzando se necessario, l'esportazioni di servizi interni.

Tutta la vostra rete LAN sarà inoltre protetta da tutti i più comuni attacchi di hacker grazie alle funzionalità di firewall integrate.

In questo manuale troverà tutte le informazioni necessarie per collegare Michelangelo OFFICE CX alla rete di computer e configurare opportunamente l'insieme in pochi minuti.

Per una configurazione più estesa e completa del prodotto viene fornito un manuale in versione elettronica disponibile sul CDROM o sul sito [www.digicom.it](http://www.digicom.it)

### Prerequisiti

- Computer con schede di rete Ethernet 10/100 Megabit/s, connettori UTP
- Driver software per le schede di rete installati su ogni computer
- Protocollo TCP/IP installato su ogni computer
- Cavi di rete dritti, connettori RJ45 su entrambe le estremità
- Linea ADSL su linea telefonica analogica, connettore RJ11
- Abbonamento Internet ADSL per singolo utente o multiutente-stipulato con un ISP (Internet Service Provider)
- Dati relativi all'abbonamento ADSL

### Contenuto della confezione

- 1 Michelangelo OFFICE CX o Michelangelo LAN CX
- 1 Alimentatore
- 1 CD-ROM completo di manuali
- 1 Manuale di configurazione rapida
- 1 cavo RJ45-RJ45 dritto
- 1 cavo di linea RJ11-RJ11
- 1 cavo USB

## 1.1. CARATTERISTICHE

---

- Velocità dati asimmetrica
- Velocità massima Ricezione (downstream) : 8Mbit/s (dmt)
- Velocità massima Trasmissione (upstream) : 1Mbit/s (dmt)
  
- Standard ADSL:  
ANSI T1.413 Issue 2  
ITU G.992.1 (G.dmt)  
ITU G.992.2 (G.Lite)
  
- Protocolli Supportati:  
RFC2364 (PPP over ATM)  
RFC2516 (PPP over Ethernet)  
RFC1483 (Bridged e Routed Ethernet over ATM)
  
- Supporto ATM UNI3.1/4.0 PVC, ATMSAR, ATM AAL5 e OAM F5
  
- Interfaccia WAN ADSL: Connettore RJ11
- Porta LAN 10/100 Mbit/s
- Switch 4 porte 10/100 Mbit/s integrato (solo Michelangelo OFFICE CX)
- Porta USB
  
- Supporto NAT e NAT Export
- DHCP server e client
- Routing statico e RIPv2
- Firewall SPI Stateful Packet Inspection
- Supporto DMZ
- Autenticazione PAP e CHAP
  
- Configurazione Web based
- Configurazione da remoto
- Funzioni di autodiagnostica LAN, ADSL e ATM
- Aggiornabile via FTP TFTP

## 1.2. DESCRIZIONE PORTE E LED



Fig. 1.1. Vista frontale Michelangelo OFFICE CX e Michelangelo LAN CX

### Frontale

<b>PWR</b>	Accesso indica che il router è collegato all'alimentazione ed acceso.
<b>USB</b>	Accesso indica che è collegata e attiva la porta USB
<b>LAN</b>	Accesso indica che la connessione Ethernet è corretta, lampeggiante indica attività sulla porta Ethernet.
<b>ADSL</b>	Accesso indica che la linea Adsl è collegata correttamente, Lampeggiante indica che il router non è sincronizzato con la linea Adsl.
<b>DATA</b>	(solo Michelangelo LAN Cx) Lampeggia per indicare attività dati sulla linea Adsl.

### Posteriore

<b>Line</b>	Ingresso per la linea ADSL
<b>LAN 1x-4x (Michelangelo Office CX)</b>	Ingressi per la connessione di stazioni o dispositivi di rete a Michelangelo Office (Porte MDI-X). Utilizzare cavi RJ45-RJ45 diritti.
<b>LAN (Michelangelo LAN CX)</b>	Ingresso per la connessione alla rete LAN o PC.
<b>USB</b>	Porta per la connessione di un PC Windows via USB. (Necessita dell'installazione dei driver appositi).
<b>PWR</b>	Ingresso per il cavo proveniente dall'alimentatore. Utilizzare unicamente l'alimentatore fornito nella confezione. L'utilizzo di alimentatori diversi può comportare il danneggiamento del dispositivo conconseguente invalidazione delle condizioni di garanzia.
<b>Default (Reset)</b>	Pulsante per il ripristino della configurazione di fabbrica. Accendere il dispositivo tenendo premuto il pulsante Reset per 10 secondi. Dopo il reset al default di fabbrica il dispositivo si presenta con i seguenti parametri: Indirizzo IP <b>10.0.0.2</b> , id <b>admin</b> , pw <b>epicrouter</b> .

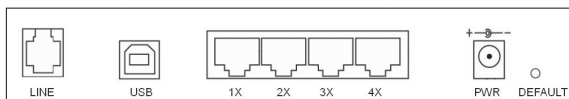


Fig. 1.2. Vista posteriore Michelangelo OFFICE CX



Fig. 1.3. Vista posteriore Michelangelo LAN CX

## **ASSISTENZA TECNICA**

---

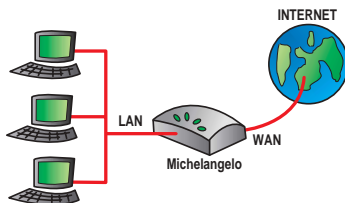
L'assistenza Tecnica Digicom risponderà ad ogni vostra richiesta all'indirizzo [support@digicom.it](mailto:support@digicom.it)

Prima di contattare il Supporto Tecnico verificate se la soluzione alla vostra problematica è disponibile alla pagina:  
<http://www.digicom.it/digisit/faqlink.nsf/perprodo?OpenForm>

oppure la disponibilità di Aggiornamenti alla pagina:  
<http://www.digicom.it/italiano/supporto/upgradeRouterWireless2.html>

## 2. CONFIGURAZIONE ACCESSO INTERNET

Michelangelo è un router Adsl, è un dispositivo in grado di fornire un accesso Internet a tutta la vostra rete di PC, utilizzando un unico abbonamento Internet.



### Il Router dispone di due Interfacce:

LAN (Local Area Network) è la rete interna, ove sono collegati tutti i pc. La porta USB fa parte della LAN. WAN (Wide Area Network) è la rete esterna, il collegamento del vostro router ad Internet.

Per configurare il dispositivo dobbiamo inizialmente configurare la LAN, che ci permette la comunicazione tra PC e Router e successivamente la WAN che permette al Router di comunicare con Internet.

### 2.1. CONFIGURAZIONE LAN

#### Il Router è configurato al default (impostazione di fabbrica):

Indirizzo IP: 10.0.0.2  
Subnet Mask: 255.0.0.0

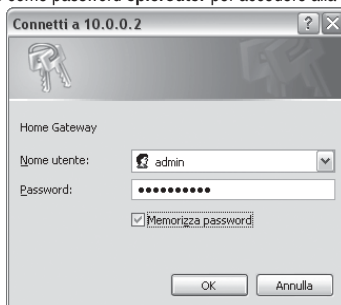
Per mettere in comunicazione i PC con il router è necessario che i PC abbiano degli indirizzi appartenenti alla stessa rete, come ad esempio tutti gli indirizzi compresi tra 10.0.0.3 e 10.0.0.254.

Inizialmente sarà sufficiente configurare un solo PC per accedere alla configurazione del router, pertanto impostate sul PC:

Indirizzo IP: 10.0.0.3  
Subnet Mask: 255.0.0.0  
Gateway: 10.0.0.2 (infatti è il router il nostro "cancello" per raggiungere Internet)  
DNS: Inserite gli indirizzi che trovate sul vostro abbonamento Internet oppure utilizzate uno degli indirizzi che trovate nell'apposita sezione del manuale.

Verificate che il vostro Pc sia collegato al Router ed aprite il Browser (Internet Explorer, Mozilla... etc); collegatevi all'indirizzo <http://10.0.0.2>

Inserite come nome utente **admin** e come password **epicrouter** per accedere alla configurazione.



## 2.2. CONFIGURAZIONE WAN

La sezione di WAN deve essere necessariamente configurata come indicato dal vostro provider nel contratto Adsl. Esistono diversi tipi di abbonamento Adsl che necessitano di configurazione differenti, principalmente esistono due tipi di abbonamento:

- **Abbonamenti con autenticazione (PPPoA, PPPoE)**  
Sono abbonamenti che necessitano di un **Username** e di una **Password** per la connessione, sono abbonamenti principalmente per utenza domestica, che vengono solitamente associati a dei modem usb adsl.
- **Abbonamenti con Indirizzo IP fisso (RFC1483 – Router IP LLC)**  
Sono abbonamenti che hanno un indirizzo IP fisso sul lato WAN, sono abbonamenti per utenze aziendali. Anche questi abbonamenti hanno una username ed una password ma solo per l'accesso alla/e caselle di posta.

### 2.2.1. ABBONAMENTI ADSL CON AUTENTICAZIONE

Per configurare il router con questo tipo di abbonamenti Adsl è necessario disporre delle seguenti informazioni:

- **Nome Utente e Password**, queste informazioni sono indispensabili per effettuare correttamente la connessione Internet.
- **VPI e VCI**, questi parametri devono essere forniti dal provider, sono Vpi=8 e Vci=35 se non specificato.
- **Protocollo**, solitamente queste linee utilizzano **PPPoA** con **Vc Mux**, inoltre le nuove linee Adsl sono multi protocollo, in caso di problemi l'unica alternativa è **PPPoE** con **LLC**.

Selezionate **WAN** dal menù **Configuration** per accedere alla configurazione.

Configuration  
WAN

#### Select Adapter:

Adapter: Pvc 0

Verificate che sia selezionato **Pvc 0** e premete il tasto **Submit**

Submit

Impostate **Enable** per attivare questo profilo di configurazione

Virtual Circuit Enabled

**PPPoA VC-Mux** è il protocollo più diffuso; se non siete sicuri del protocollo da utilizzare impostate questo.

Encapsulation PPPoA VC-Mux

#### ATM

Generalmente in Italia la maggioranza delle linee Adsl utilizza:

VPI 8

VCI 35

VPI = 8

VCI = 35

Se è necessario impostare valori differenti verranno sicuramente specificati nel contratto.

Service Name è solamente il nome della connessione, potete anche lasciarlo vuoto.

**Username:** inserite il vostro Nome Utente per la connessione.

**Password:** inserite la vostra password.

<b>PPP</b>	<a href="#">Advanced PPP configuration</a>
Service Name	<input type="text"/>
Username	<input type="text"/>
Password	<input type="text"/>

Per salvare le impostazioni effettuate è necessario confermare i parametri immessi premendo il tasto **Submit (1)** e successivamente **Save Configuration (2)** e **Save & Reboot (3)**.



Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.



Save settings and reboot.



Reboot modem without saving settings.



### 2.2.2. ABBONAMENTI ADSL CON INDIRIZZO IP FISSO

Per configurare il router con questo tipo di abbonamenti Adsl è necessario disporre delle seguenti informazioni:

- **Indirizzo/i IP pubblico/i (o globale/i)** da assegnare staticamente al router.
- **Indirizzo di Punto-Punto Nazionale** nel caso di abbonamenti con un pool di indirizzi IP assegnati.
- **VPI e VCI**, questi parametri devono essere forniti dal provider, sono Vpi=8 e Vci=35 se non specificato.
- **Protocollo**, queste linee utilizzano il protocollo **1483 Routed IP LLC**.

Selezionate **WAN** dal menù **Configuration** per accedere alla configurazione.

**Configuration**  
WAN

Select Adapter:

Adapter:

Verificate che sia selezionato **Pvc 0** e premete il tasto **Submit**



Impostate **Enable** per attivare questo profilo di configurazione

Virtual Circuit

Impostate **1483 Routed IP LLC**

Encapsulation

ATM

Generalmente in Italia la maggioranza delle linee Adsl utilizza:

VPI	<input type="text" value="8"/>
VCI	<input type="text" value="35"/>

VPI = 8

VCI = 35

Se è necessario impostare valori differenti verranno sicuramente specificati nel contratto.

**IP Address:**

inserie l'indirizzo IP che vi è stato assegnato (unico IP oppure il Punto-Punto Nazionale)

**Subnet Mask:**

inserie 255.255.255.0

**Gateway:**

Inserie il Gateway che trovate sul contratto, i primi tre campi sono uguali a quelli dell'indirizzo IP e generalmente l'ultimo è 254

**Static IP Settings**

IP Address	<input type="text" value="195.103.9.66"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="195.103.9.254"/>

Per salvare le impostazioni effettuate è necessario confermare i parametri immessi premendi il tasto **Submit (1)** e successivamente **Save Configuration (2)** e **Save & Reboot (3)**.



Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.



Save settings and reboot.



Reboot modem without saving settings.



### 3. FUNZIONALITA' AVANZATE

Terminata la configurazione descritta nel capitolo 2, il router è già in grado di fornire accesso Internet a tutta la rete. Questa sezione del manuale descrive la configurazione di funzionalità avanzate, non effettuate le configurazioni descritte in questa sezione se non necessarie.

#### 3.1. ESPORTAZIONE DI SERVIZI (VIRTUAL SERVER)

Utilizzando un Router Adsl con NAT abilitato non è possibile utilizzare delle funzioni Server all'interno della nostra rete, in quanto il NAT blocca tutte le connessioni in Ingresso. E' pertanto necessario "istruire" il router per permettere una gestione corretta delle sessioni in ingresso qualora fosse necessario.

Per configurare correttamente un'esportazione (Virtual Server) è necessario disporre delle seguenti informazioni:

- N° porta legato al servizio.
- Protocollo
- Indirizzo IP del PC che dovrà utilizzare il servizio.

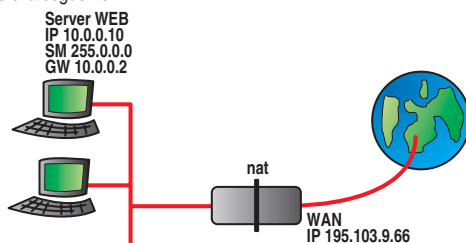
Tipicamente la funzione Virtual Server viene utilizzata per:

- Server Web: Protocollo TCP e UDP, porta 80 (443 per Secure Http)
- Server di posta POP3: Protocollo TCP, porta 110
- Server di posta SMTP: Protocollo TCP, porta 25
- Server FTP: Protocollo TCP, porta 21
- Desktop Remoto (WinXP): Protocollo TCP, porta 3389

Gli esempi sopra riportati utilizzano tipicamente delle impostazioni fisse, per altre applicazioni (Gaming On-Line, Peer-to-Peer) fate riferimento al sito di supporto del software che volete utilizzare oppure (come per Emule) il numero della porta è personalizzabile nella configurazione stessa del programma.

##### 3.1.1. ESEMPIO CONFIGURAZIONE SERVER WEB

La configurazione della rete è la seguente:



Accedete alla pagina di configurazione **Virtual Server**, la regola per l'esportazione è riportata nell'immagine seguente:

Virtual Server Configuration

ID	Public Port - Start	Public Port - End	Private Port	Port Type	Host IP Address
<input type="text" value="1"/>	<input type="text" value="80"/>	<input type="text" value="80"/>	<input type="text" value="80"/>	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text" value="10.0.0.10"/>

Settings need to be saved to Flash and the system needs to be rebooted for changes to take effect.  
 The maximum number of entries above is 20. The maximum number of mapped ports is 20

**ID = 1**

Numero progressivo della regola, è possibile inserire un massimo di 20 regole.

**Public Port –Start / End = 80**

Numero della porta del servizio da esportare, nel nostro caso è sufficiente l'esportazione della porta 80, pertanto Public Port-Start è uguale a Public Port-End

**Private Port = 80**

Numero della porta del servizio attivo sulla macchina in LAN; se in Public Port è stato definito un range, Private Port indica la prima porta del range interno.

**Port Type = TCP**

Indica il tipo di protocollo, TCP oppure UDP

**Host IP Address = 10.0.0.10**

Indica l'indirizzo IP del PC connesso in LAN che gestirà la connessione in Ingresso.

E' necessario salvare le impostazioni e riavviare il router con l'apposita funzione per attivare le impostazioni

### 3.2. ESPORTAZIONE DEI SERVIZI (DMZ)

---

Alcune applicazioni richiedono, per poter funzionare, un numero elevato di porte oppure un range di porte dinamico, pertanto NON è possibile utilizzare dei semplici Virtual Server.

La funzione DMZ permette di esportare **tutte** le porte su un determinato indirizzo IP.

Accedete alla pagina di configurazione **Misc Configuration**, selezionate l'opzione **DMZ Enable** ed inserite nel campo **DMZ HOST IP** l'indirizzo IP del PC che utilizzerà questa funzione.

DMZ	<input type="text" value="Enabled"/>
DMZ HOST IP	<input type="text" value="10.0.0.10"/>

Applicate l'impostazione premendo il tasto **Submit** a fondo pagina.

*E' necessario salvare le impostazioni e riavviare il router con l'apposita funzione per attivare le impostazioni.*

### 3.3. GENERALITÀ FIREWALL

---

L'interconnessione di una rete LAN ad Internet offre molteplici vantaggi, ma nasconde anche alcune insidie che possono rivelarsi alquanto spiacevoli. Al fine di proteggere la riservatezza, integrità e sicurezza dei propri dati è sempre consigliabile la messa in opera di alcune contromisure atte a proteggersi dal "mondo esterno" rappresentato da Internet e dai pericoli che da lì possono sorgere.

Spesso un hacker tenta di penetrare una rete al solo scopo di scoprire cosa sia in essa contenuta, altre volte per carpire o modificare dei dati, altre ancora per piazzare dei "cavalli di troia" che gli permettano in un secondo tempo di prendere possesso delle macchine ed utilizzarle per i propri scopi. Molte volte le macchine attaccate vengono a loro volta utilizzate per attaccare altre reti, per salvare dati, file o contenuti illegali nascondendo la vera identità dell'attaccante.

E' quindi di notevole importanza l'inserimento di un **Firewall** in grado di proteggere la rete dagli attacchi più comuni, chiudendo tutti i punti di accesso dall'esterno e bloccare qualsiasi tentativo di intrusione. Il firewall implementato in questo router è di tipo **SPI - Statefull Packet Inspection**, permette di proteggere la propria rete e di poter definire delle regole per il passaggio dei dati, inoltre include degli algoritmi per controllare lo stato di tutte le connessioni che lo attraversano, cercando i segni rilevatori di tentativi di intrusione.

#### Configurazione

Il menù per la configurazione del firewall è strutturato in questo modo:

##### **Advanced Options:**

- **Protection Policy** Abilitazione per la protezione dagli attacchi più comuni.
- **Hacker Log** Gestione degli eventi da visualizzare nel Log
- **Service Filtering** Abilitazione del filtro per le richieste da reti esterne di alcuni protocolli comuni.

##### **Firewall Databases:**

- **IP Group** Permette la creazione di gruppi contigui di indirizzi IP per semplificare l'utilizzo di regole
- **Service Group** Permette l'associazione di un nome ad una porta Tcp o Udp
- **Time Window** Permette la creazione di fasce orarie in cui applicare le regole.

##### **Inbound / Outbound Policies:**

- **Inbound Policies** Elenco regole per la gestione dei pacchetti in ingresso
- **Outbound Policies** Elenco regole per la gestione dei pacchetti in uscita

**Configurazione – Esempio di creazione regole**

**1. Proteggere la rete**

Abilitate tutte le protezioni da attacchi esterni in **Protection Policy**.  
 Abilitate tutte i filtri in **Service Filtering**.

**2. Bloccare l'uscita dei pacchetti non consentiti**

Nel menu **Outbound Policies** inserite una nuova regola come mostra l'immagine seguente:

*... Adding New Policy ...*

Src IP: <input type="text"/> ~ <input type="text"/> Any IP ▾	DB: None ▾
Dest IP: <input type="text"/> ~ <input type="text"/> Any IP ▾	DB: None ▾
Src Port: <input type="text"/> ~ <input type="text"/> Any Port ▾	
Dest Port: <input type="text"/> ~ <input type="text"/> Any Port ▾	DB: None ▾
Transport Protocol: All Protocol ▾	
Filtering Action: Deny ▾	
Time Window Filtering: None ▾	

Il risultato sarà il seguente:

	IP Address	Port #	Prot.	Act.	Opt. Filtering	
1	SrcIP: Any IP DesIP: Any IP	SrcPort: Any Port DesPort: Any Port	All	Deny		<input type="button" value="Up"/> <input type="button" value="Dn"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

In questo modo tutti i pacchetti in uscita vengono bloccati; il passo successivo è quello di creare delle regole per abilitare SOLO il passaggio delle applicazioni necessarie.

I servizi più comunemente utilizzati sono la navigazione web e la posta, pertanto è necessario aprire le seguenti porte:

per la navigazione:

- porta 80 TCP – protocollo http
- porta 445 TCP – protocollo https
- porta 53 UDP – protocollo DNS

per scaricare file da alcuni siti:

- porta 20-21 TCP – protocollo FTP

per inviare / ricevere posta:

- porta 110 TCP – protocollo POP3
- porta 25 TCP – protocollo SMTP

### 3. Abilitare l'uscita di una singola porta

Nel menù **Outbound Policies** inserite una nuova regola come mostra l'immagine seguente:

... Adding New Policy ...

Src IP: <input type="text" value="10.0.0.1"/> ~ <input type="text" value="255.0.0.0"/> Mask Range ▾	DB: None ▾
Dest IP: <input type="text"/> ~ <input type="text"/> Any IP ▾	DB: None ▾
Src Port: <input type="text"/> ~ <input type="text"/> Any Port ▾	
Dest Port: 80 ~ <input type="text"/> Single Port ▾	DB: None ▾
Transport Protocol: TCP Protocol ▾	
Filtering Action: Allow ▾	
Time Window Filtering: None ▾	

**Src IP: Source IP** indica il gruppo di indirizzi IP considerati in questa regola, pertanto rappresenta la nostra rete LAN, è possibile rendere più selettiva la regola utilizzando il range (ex. 10.0.0.3 – 10.0.0.12 per una rete di 12 Pc)

**Dest IP: Destination IP** indica la destinazione dei pacchetti filtrati da questa regola, pertanto è corretto indicare **Any IP**, infatti questa regola deve permettere la navigazione internet, verso tutti i siti raggiungibili (ANY, qualsiasi).

**Src Port: Source Port** indica la porta sorgente, pertanto la porta sorgente nel nostro tipo di applicazione è una porta qualsiasi, infatti la porta che identifica il tipo di protocollo / applicazione è la porta di destinazione.

**Dest Port: Destination Port** indica la porta di destinazione, nel nostro caso 80 perché questa regola permette il passaggio del protocollo http.

**Transport Protocol:** questo parametro viene sempre definito nella descrizione di un applicazione, la maggior parte delle applicazioni utilizza TCP o UDP.

**Filtering Action:** Selezionate **Allow** per permettere il passaggio dei pacchetti identificati dalla regola appena descritta.

### 4. Gestire correttamente l'ordine delle regole

Tutte le regole vengono processate in ordine, pertanto è importante l'ordine in cui le regole sono disposte.

La regola per il blocco di tutto il traffico deve essere sempre posta per ultima, in questo modo, se il pacchetto in uscita NON corrisponde ad alcuna regola precedente viene bloccato.

	IP Address	Port #	Prot.	Act.	Opt. Filtering	
1	SrcIP: 10.0.0.1 ~ 255.0.0.0 DesIP: Any IP	SrcPort: Any Port DesPort: 80	TCP	Allow		<input type="button" value="Up"/> <input type="button" value="Dn"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
2	SrcIP: Any IP DesIP: Any IP	SrcPort: Any Port DesPort: Any Port	All	Deny		<input type="button" value="Up"/> <input type="button" value="Dn"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Per spostare le regole, utilizzate i tasti **Up** e **Dn**.



## A. APPENDICE

---

### A.1. ELENCO PORTE TCP/UDP

---

Nome	Numero	Descrizione
ftp-data	20/tcp	File Transfer (Default Data)
ftp-data	20/udp	File Transfer (Default Data)
ftp	21/tcp	File Transfer (Control)
ftp	21/udp	File Transfer (Control)
ssh	22/tcp	SSH Remote Login Protocol
ssh	22/udp	SSH Remote Login Protocol
telnet	23/tcp	Telnet
telnet	23/udp	Telnet
smtp	25/tcp	Simple Mail Transfer
smtp	25/udp	Simple Mail Transfer
domain	53/tcp	Domain Name Server
domain	53/udp	Domain Name Server
http	80/tcp	World Wide Web HTTP
http	80/udp	World Wide Web HTTP
www	80/tcp	World Wide Web HTTP
www	80/udp	World Wide Web HTTP
www-http	80/tcp	World Wide Web HTTP
www-http	80/udp	World Wide Web HTTP
pop3	110/tcp	Post Office Protocol - Version 3
pop3	110/udp	Post Office Protocol - Version 3
nntp	119/tcp	Network News Transfer Protocol
nntp	119/udp	Network News Transfer Protocol
ntp	123/tcp	Network Time Protocol
ntp	123/udp	Network Time Protocol
netbios-ns	137/tcp	NETBIOS Name Service
netbios-ns	137/udp	NETBIOS Name Service
netbios-dgm	138/tcp	NETBIOS Datagram Service
netbios-dgm	138/udp	NETBIOS Datagram Service
netbios-ssn	139/tcp	NETBIOS Session Service
netbios-ssn	139/udp	NETBIOS Session Service
snmp	161/tcp	SNMP
snmp	161/udp	SNMP
snmptrap	162/tcp	SNMPTRAP
snmptrap	162/udp	SNMPTRAP
pptp	1723/tcp	pptp
pptp	1723/udp	pptp
ms-wbt-server	3389/tcp	
ms-wbt-server	3389/udp	MS WBTerminal Server

## A.2. ELENCO SERVER DNS

---

Gli indirizzi riportati in questa pagina hanno lo scopo di aiutare nella configurazione del router, qualora questi dati non siano stati specificati dal provider.

La gestione di questi indirizzi dipende solo dai rispettivi provider, pertanto non è possibile garantirne la funzionalità nel tempo.

### *TIN*

dns1.village.tin.it	195.14.96.135
dnscsca2.tin.it	212.216.172.222
dnscache2.tin.it	212.216.172.162
dns2.tin.it	194.243.154.51
dnscache1.tin.it	212.216.172.62
dns1.fullcompany.telecomitalia.it	212.131.30.42
dnscsca.tin.it	212.216.112.112
dnscsca.tin.it	195.31.190.31
dns.tin.it	194.243.154.62

### *Interbusiness*

r-dns.interbusiness.it	151.99.125.1
dns2.interbusiness.it	151.99.125.3
dns.interbusiness.it	151.99.125.2
server-b.cs.interbusiness.it	151.99.250.2

### *Infostrada*

ns2.libero.it	193.70.192.100
ns1.libero.it	195.210.91.100
cns-a.libero.it	193.70.192.25
cns-b.libero.it	193.70.152.25

### *Wind*

dns.wind.it	212.245.255.2
dns2.wind.it	212.245.158.66
dns.inwind.it	212.141.53.123
dns2.wind.it	212.245.158.66

*Atlant*

ns1.atlanet.it	213.234.128.211
ns2.atlanet.it	213.234.132.130
ns1.its.it	151.92.2.35
ns.telexis.it	213.199.1.132

*McLink*

dns.mclink.it	195.110.128.1
---------------	---------------

*Flashnet*

dns.flashnet.it	194.247.160.1
dns2.flashnet.it	194.247.160.8

*Albacom*

ns2.albacom.net	212.17.192.209
-----------------	----------------

*I.Net*

urano.inet.it	194.20.8.1
venere.inet.it	194.20.8.4

*Elitel*

elitel.it	212.34.224.193
ns.elitel.it	212.34.224.132
ns2.elitel.it	217.146.65.7
ns3.elitel.it	217.146.65.80

*Tiscali*

ns.tiscali.it	195.130.224.18
sns.tiscali.it	195.130.225.129

*Jumpy*

-	212.17.192.216
-	212.17.192.56

*Public DNS*

dns.nic.it	193.205.245.5
dns2.nic.it	193.205.245.8
nameserver.cnr.it	194.119.192.34

21010 Cardano al Campo VA  
via A. Volta 39

