

Informazioni sulla sicurezza per accesso al servizio FIOL

0 Modifiche rispetto alle versioni precedenti

Differenze fra versione 2009-09-10 (attuale) e 2009-07-01

- Punto 1 specificato ambito applicazione nota.
- Punto 3 cambiato nome a dominio server HTTP/HTTPS.

Differenze fra versione 2009-07-01 e 2004-12-01

- Punto 2 rimossa opzione porta alternativa RDP 443
- Punto 3 cambiato indirizzo server connessione RDP e nota uso porta 443.
- Punto 4.1 cambiato indirizzo server connessione RDP, eliminata nota uso porta 443.
- Punto 4.2 cambiato indirizzo server connessione RDP, eliminata nota uso porta 443.
- Punto 4.3 aggiunta indicazione uso RDP su porta 443.
- Punto 4.4 rimosso rafforzamento sicurezza porta 3389, ora usata solo porta 443.

1 Introduzione

Questa nota è ad uso di chi gestisce la sicurezza della rete e del computer dal quale si accede al servizio IL FORO ITALIANO online, in seguito citato come FIOL.

Contiene informazioni generali sul servizio e istruzioni relative alle possibili configurazioni di sicurezza.

La nota si applica alla consultazione del servizio con la modalità tramite Connessione Desktop Remoto.

2 Architettura generale del sistema FIOL

L'accesso al servizio FIOL avviene in prima istanza verso un server HTTPS che gestisce i diritti di consultazione degli abbonati.

Al primo accesso su tale sito viene richiesta l'introduzione di un codice di abbonamento fornito dal servizio abbonamenti. Tale codice identifica il cliente al fine di riconoscerne i diritti di consultazione (periodo di tempo, sessioni, eventuali vincoli del sito di consultazione).

Nella pagina *Attivazione abbonamento* è inoltre possibile specificare alcune preferenze:

- la dimensione della finestra di consultazione;
- il non utilizzo dei cookie (anche se disponibili) per la memorizzazione preferenze.

Completata l'attivazione dell'abbonamento, la consultazione della banca dati avviene a partire dalla pagina *Accesso al servizio* con tecnologia thin client.

Viene utilizzata una sessione Desktop remoto (protocollo RDP) verso un Microsoft Terminal Server.

Questa tecnica consente, con modesta banda passante, prestazioni paragonabili o superiori alla consultazione locale da media ottico (CD-ROM/DVD-ROM).

Eventuali stampe (in formato PDF) ed esportazioni (in formato testo) generate durante la consultazione vengono distribuite agli utenti attraverso il sito web di accesso, nella pagina *Accesso al servizio*.

La sessione di consultazione Terminal Server avviene utilizzando il programma Connessione Desktop Remoto, che si trova preinstallato su Windows XP e Vista e che può essere installato su altri sistemi operativi dove non sia presente.

Nel caso in cui non sia agevole scaricare e installare il programma Connessione Desktop Remoto si può utilizzare la modalità di consultazione standard che prevede il download di un eseguibile per la consultazione denominato “Il Foro Italiano – banche dati online.exe” o “Il Foro Italiano - rivista online.exe”.

3 Considerazione generali sulla sicurezza del sito FIOL

Dal punto di vista generale della sicurezza vanno evidenziati i seguenti fatti.

- La connessione con il sito WEB di supporto usa il protocollo HTTPS per garantire la sicurezza dei dati trasmessi e la certezza della fonte. In tal modo si limita la possibilità di attacchi del tipo "Man In The Middle" e l'intercettazione della comunicazione. Il protocollo HTTP è usato solo per redirigere gli accessi errati al sito.
- Il server HTTPS di supporto distribuisce solo file con contenuto passivo, PDF 1.3 e testo puro. Unica eccezione è il modulo Microsoft *Client ActiveX di Servizi terminal* (MSRDP.CAB) distribuito, se necessario, per il collegamento desktop remoto direttamente dal browser. Il modulo è firmato digitalmente dal produttore in modo che l'installazione ne possa riconoscere l'autenticità.
- La sessione desktop remoto avviene su porte che sono vincolate all'uso di un utente anonimo di sistema con poteri estremamente limitati, in grado di eseguire la sola applicazione di consultazione della banca dati. Non avviene nessun colloquio di logon via rete.

Per l'utente finale è impossibile accedere ad un desktop in grado di interagire con il server. Ciò per garantire la sicurezza del server stesso e dell'utente. Il blocco è al livello del file system, quindi praticamente impossibile da forzare.

- La sessione desktop remoto è avviata su un indirizzo IP fisso, non via DNS. Ciò per evitare possibili attacchi MITM tramite alterazione di DNS. Gli indirizzi usati dal servizio sono di seguito elencati.
- La potenziale mappatura di dischi locali del PC che consulta, consentita dalle più recenti versioni del programma Connessione Desktop Remoto, è inibita dalle politiche di sicurezza del server FIOL.

Ciò per evitare la possibilità di accesso a dati privati del client e per ragioni di sicurezza e prestazioni del server stesso.

I file RDP o HTML di connessione generati dal sito contengono la mappatura della sola clipboard e dei suoni locali.

Comunque il controllo finale di un eventuale tentativo di accesso ai dischi locali del client è subordinato all'accettazione da parte dell'utente finale di un avviso di sicurezza generato dal programma Connessione desktop remoto.

- Gli accessi di servizio al server FIOL avvengono solo da LAN privata protetta e isolata da internet con firewall. E' impedito l'accesso esterno al server per upload, le banche dati sono prodotte direttamente sulla LAN di servizio. La gestione degli abbonamenti è effettuata via HTTPS da indirizzi IP predeterminati.
- Il server che eroga il servizio FIOL è dedicato ai soli protocolli HTTP, HTTPS, RDP. Ha tutte le interfacce ethernet esterne protette da firewall integrato, con aperte le sole porte di ingresso HTTP, HTTPS, RDP.
- Il server del servizio FIOL è in ascolto sulle seguenti porte:

```
s1.zanichelli.it:443    server https;  
s1.zanichelli.it:80    server http (usato solo per redirezione https);  
77.89.1.58:443        porta RDP.
```

La connessione RDP non avviene sulla porta standard 3389 ma sulla 443, perché quest'ultima risulta normalmente già aperta in uscita. Ciò evita la necessità di configurazioni speciali degli apparati di sicurezza.

Tali informazioni sono utili se si desidera configurare le apparecchiature di controllo della sicurezza in uscita a livello indirizzo:porta.

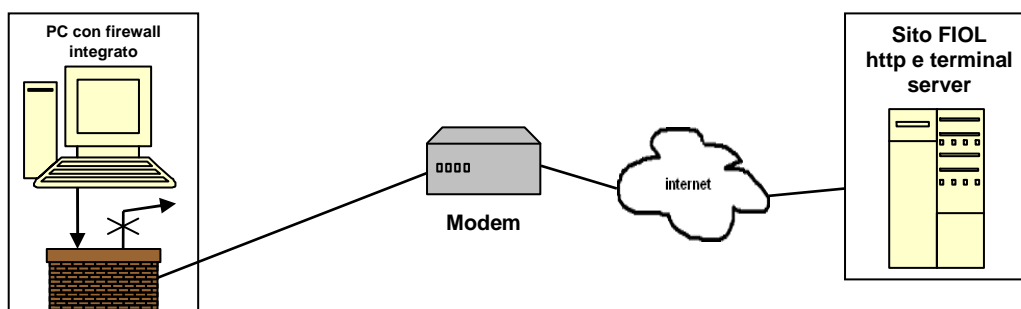
4 Analisi della sicurezza delle configurazioni tipiche di accesso

Il metodo di connessione e consultazione comporta alcune considerazioni sulla configurazione delle apparecchiature di sicurezza eventualmente presenti.

Segue una panoramica delle principali configurazioni di accesso internet.

Per ognuna di esse viene indicato il livello massimo di sicurezza configurabile sulle apparecchiature di comunicazione, compatibilmente con il funzionamento della consultazione del sito FIOL.

4.1 Accesso da PC con modem (telefonico o ADSL)

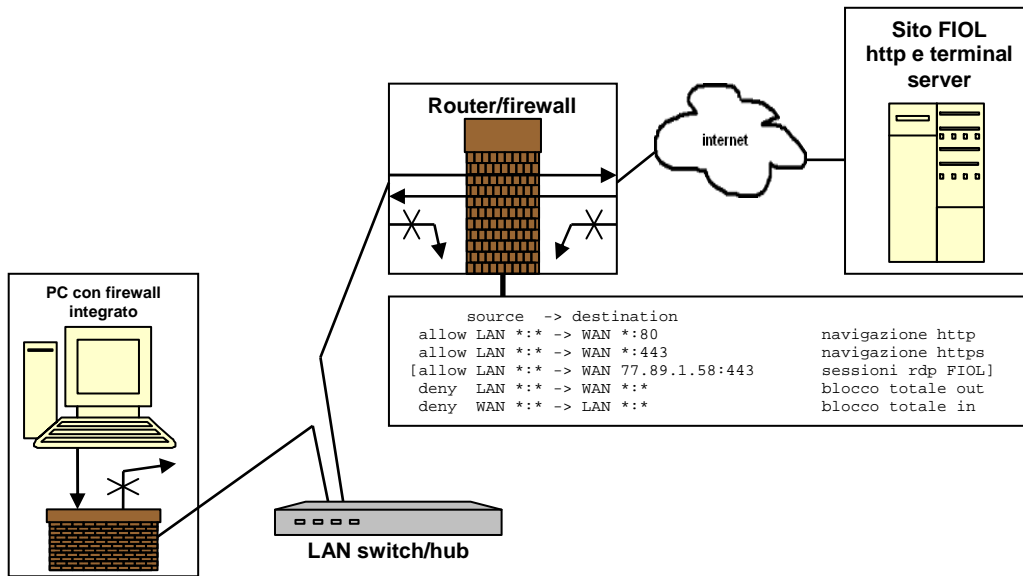


Normalmente la consultazione funziona senza problemi.

Per PC con sistema operativo Windows XP o Vista si consiglia di attivare il firewall integrato, che chiude tutte le porte in ingresso.

La consultazione del servizio FIOL funziona comunque, dato che le connessioni necessarie avvengono solo verso il server.

4.2 Accesso da LAN con gateway su router/firewall



E' il caso di piccole reti o di singolo PC connesso direttamente al router/firewall con cavo crossover ethernet.

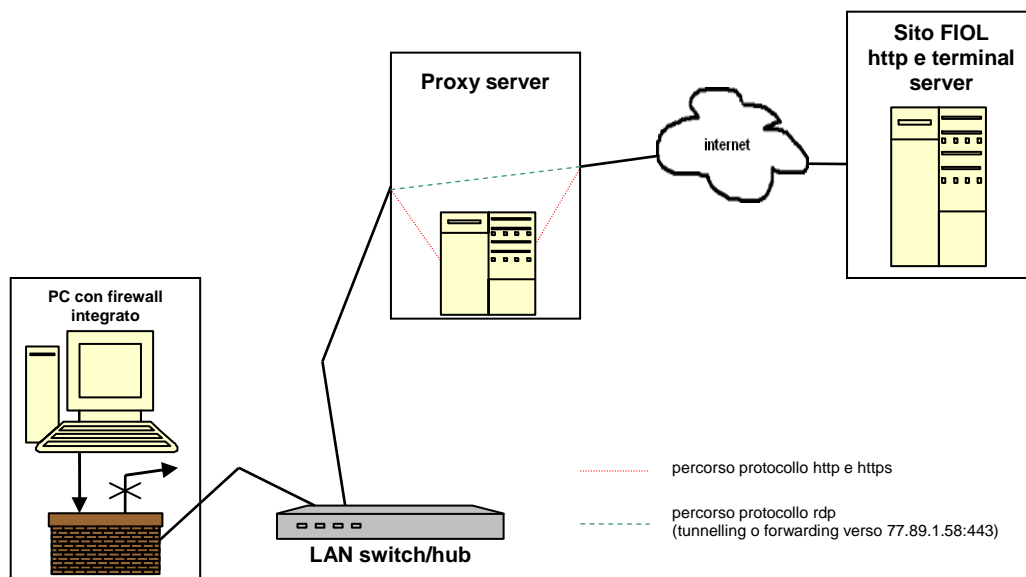
In questi casi il gateway assunto di ogni PC viene impostato (esplicitamente o tramite protocollo DHCP) sull' indirizzo LAN del router/firewall.

Normalmente non vi sono particolari problemi, dato che la configurazione standard di un router/firewall chiude tutte le porte in ingresso e le lascia tutte aperte in uscita.

Se comunque fossero chiuse delle porte in uscita è necessario verificare che rimangano aperte le porte 80-HTTP, 443-HTTPS e RDP.

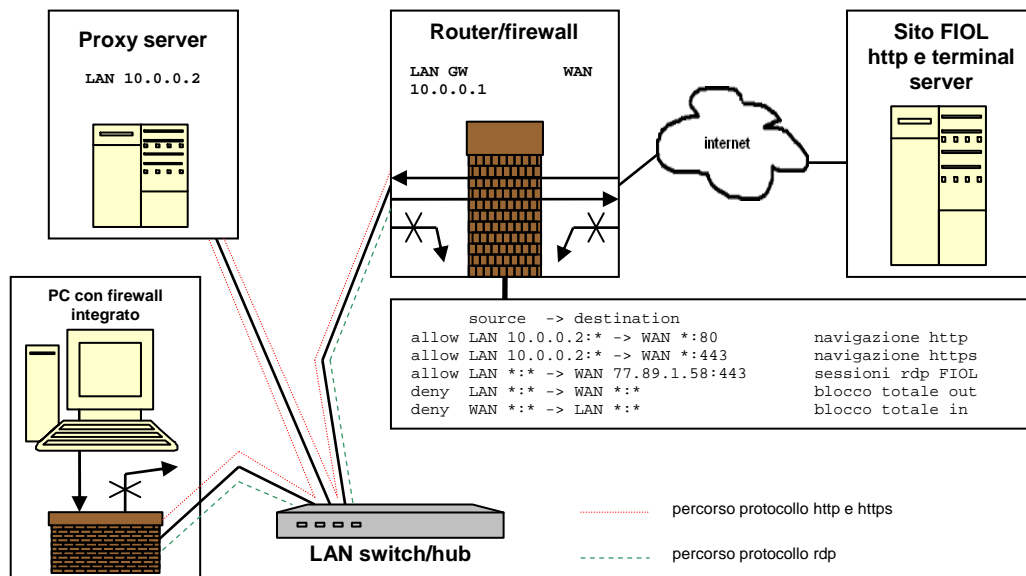
Anche in questo caso, per i PC con Windows XP o Vista, si consiglia l'attivazione del firewall integrato.

4.3 Accesso via proxy server interposto fra LAN e WAN



Nel caso in cui, invece, il proxy server sia interposto fra LAN e il router/firewall di accesso WAN la consultazione è possibile solo se il proxy server può essere configurato per far passare in modo trasparente il protocollo RDP su porta 443, con tunnelling o forwarding. Altrimenti la consultazione non è possibile.

4.4 Accesso via proxy server e firewall attestati su stessa LAN



Con la presenza di un server proxy le cose si complicano e la possibilità di accesso al servizio FIOL è vincolata ad alcune condizioni.

Un caso che funziona è quello in cui il proxy server è sulla LAN e comunica con l'esterno tramite un firewall anch'esso attestato direttamente sulla LAN.

In questo caso i PC che consultano vanno configurati in modo che il browser internet usi il proxy e che il gateway predefinito punti al firewall.

In tal modo il Programma Desktop Remoto può direttamente accedere all'esterno e il browser internet sfruttare le cache e le funzioni di filtro del server proxy.