Impostazioni firewall / antivirus per Dylog linea UP

Appunti sulla corretta configurazione di installazioni client-server dei prodotti Dylog della “Linea UP” (Expert Up, Manager Up/OpenManager, Telematico Up), a integrazione di quanto descritto nella documentazione originale.

Data la progressiva integrazione dei servizi, queste informazioni possono risultare utili anche per i prodotti della linea “SEAsoft” (Fascicolo di bilancio, ecc…)

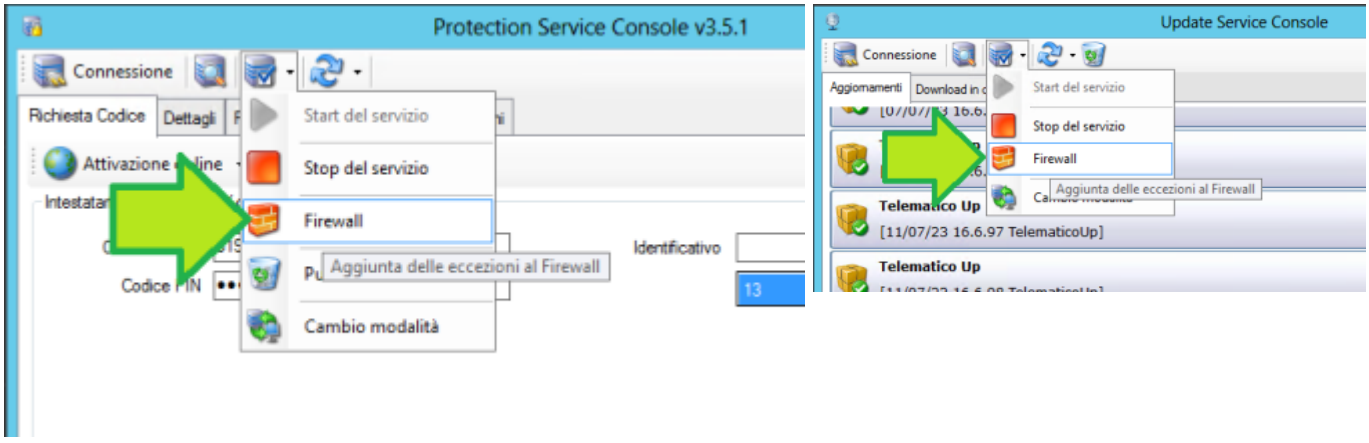
I SERVIZI APPLICATIVI

Configurando il server, vengono installati anche i servizi applicativi necessari per la gestione delle licenze (*Dylog Protection Server*, o “DPS”) e degli aggiornamenti (*Dylog Update Service*, o “DUS”).

I client di rete devono poter comunicare con questi servizi per poter funzionare correttamente. Data la specificità di questi servizi, è necessario informare il sistema operativo del server che i tentativi di connessione a questi servizi devono essere consentiti.

Se il server è protetto solo dal firewall integrato di Windows, il programma di setup è in grado di modificarne la configurazione.

È eventualmente possibile, dalle rispettive *console*, reimpostare le eccezioni nel firewall in un secondo momento (à necessario essere amministratori):



SOFTWARE DI SICUREZZA INTEGRATA

Può capitare che il server sia protetto da un pacchetto di sicurezza integrata che include sia diverse forme di antivirus e di controllo di comportamenti anomali delle applicazioni, sia un proprio firewall – in modo da tenere sotto controllo le connessioni di rete sia in entrata che in uscita.

In questi casi il firewall di sistema viene disattivato, in quanto la sua funzione viene svolta dal software di sicurezza. Se si è fortunati, questo eredita le impostazioni dal firewall di sistema, ma se i

servizi applicativi Dylog sono stati installati successivamente, è un'eventualità più difficile.

Si rende perciò necessario configurare le eccezioni nei parametri del software di sicurezza.

ECCEZIONI PER I SERVIZI

Per le connessioni in ingresso

L'impostazione del firewall di sistema fatta dal setup Dylog è basato sul *nome del programma*: si dichiara, in pratica, di lasciar fare al programma (DUS e/o DPS) quello che richiede, in quanto degno di fiducia.

Questo approccio non sempre è possibile; per alcuni software di sicurezza le impostazioni sono gestite da un'altra macchina o da un portale centralizzato, e questi *non* può sapere con sicurezza dove i programmi da autorizzare sono installati. In qualche caso, inoltre, le eccezioni da impostare devono risultare valide per qualsiasi server, ed essere di conseguenza più generiche possibili.

Questo è anche il caso di firewall esterni basati su sistemi operativi diversi da Windows.

Si deve pertanto scegliere la modalità "porta".

Queste sono le porte utilizzate per i servizi applicativi Dylog. Il firewall (o chi ne fa le veci) deve essere configurato per **permettere** le connessioni in entrata sul server per:

Servizio	Protocollo	Numero porta
Dylog Protection Service, DPS, `DPService.exe`	TCP	3500
	UDP	3600
Dylog Update Service, DUS, `DUService.exe`	TCP	11600
	UDP	11700

Se il firewall lo consente, limitare l'accesso solo all'interno di rete di dominio o rete privata.

Per le connessioni in uscita

Se la protezione della rete locale comprende anche limitazioni alle connessioni in uscita, è necessario consentire l'accesso ai server Dylog responsabili della distribuzione degli aggiornamenti:

Nome del server	Indirizzo IP (a luglio 2023)	Note
`sd.dyog.it`	45.89.181.183	
`update.dnn.it`	82.112.195.133	*(non più utilizzato, ma deve essere accessibile)*
`dwnl.dylog.it`	45.89.181.236	

Per poter utilizzare il software di teleassistenza impiegato dal personale Dylog (ISL, scaricabile all'indirizzo http://isl.dylog.it/isl.exe), si deve consentire l'accesso anche a:

Nome del server	Porte TCP	Note
`*.islonline.net`	8080, 7615, 80, 443	*Le porte 80 e 443 sono normalmente già aperte per le normali connessioni web.*

Microsoft SQL Server

I prodotti delle linea “UP” utilizzano come archiviazione il database MS SQL Server: anch'esso colloquia tramite rete su specifiche porte.

Essendo un prodotto commerciale molto diffuso, è probabile che i software di sicurezza integrata e i firewall esterni prevedono già delle apposite regole per consentire la connessione al database, che sono, magari, semplicemente da attivare.

In caso contrario, la tipica configurazione richiesta dai prodotti Dylog prevede:

Servizio	Protocollo	Numero porta
MS SQL Server	TCP	1433
MS SQL Server Browser	UDP	1434

(documento terminato)