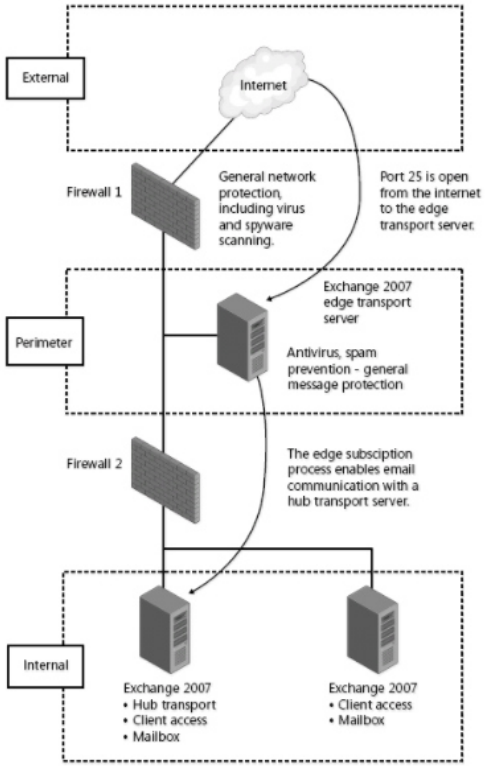
| | |
|---|---|
| **Oracle Database 12c** | Per informazioni aggiornate sulle impostazioni di protezione e privacy per Oracle Database 12c, scaricare il documento: http://www.oracle.com/us/products/database/securing-oracle-database-primer-2522965.pdf. |
| **Microsoft SQL Server 2012** | Per informazioni aggiornate sulle impostazioni di protezione e privacy per Microsoft SQL Server 2012, visitare il sito: https://docs.microsoft.com/en-us/sql/relational-databases/security/securing-sql-server. |

## 5.7 Sicurezza del Mail Server

### 5.7.1 Architettura

| **Isolamento dei sistemi critici** | |
|---|---|
| **Minaccia** | Accesso non autorizzato alle informazioni |
| **Contromisure** | I sistemi critici come il Mail Server devono avere un ambiente di elaborazione dedicato, strettamente controllato e monitorato.<br>Tipicamente è necessaria una protezione perimetrale fisica (CED) e logica (firewall).<br>Occorrono in linea di principio:<br>- un SMTP server hardenizzato collocato in DMZ che si limita ad accettare le connessioni in ingresso provenienti da Internet, con funzione di "relay";<br>- uno o più mail server interni anch'essi opportunamente messi in sicurezza (vedi best practices successive) a cui l'SMTP server in DMZ inoltra (relay) le mail ricevute dall'esterno e da cui riceve quelle provenienti dall'interno.<br>Inoltre si può considerare di installare un Application Layer inspection firewall a protezione del server SMTP in DMZ.<br>Si consideri, a titolo di esempio, il seguente schema (con 2 firewall) in ambiente Microsoft:<br>  <br><br>[Fonte: https://msdn.microsoft.com/en-us/library/cc505927.aspx] |