Piccola guida alla configurazione di un Mail Server con Synology

V.1.2

Di Alessandro Bonelli di Salci - alessandro@bonellidisalci.eu

Introduzione

Questa breve e sintetica guida vuole essere di supporto a chi intende gestire in autonomo il proprio server di posta elettronica con il Synology, non ha pretesa di spiegare i concetti di rete e delle applicazioni di posta elettronica che debbono essere conosciuti da chi si appresta a questa attività.

Il server Mail del Synology è minimale ma efficace e consente a chiunque con un minimo sforzo, sia in termini di setup che di day-by-day di gestire autonomamente la propria posta elettronica, con indubbi benefici in termini di privacy per la stessa.

Attività una volta esclusiva delle grandi aziende oggi è alla portata anche delle piccole o di singoli professionisti. I benefici di questa autonoma gestione sono considerevoli, i provider "infedeli" e/o i loro dipendenti "infedeli" o comunque le autorità non saranno nella condizione di poter vedere la nostra posta elettronica archiviata ne quella in ingresso / uscita dal server se non con un dispendio notevole di risorse ovvero duplicando ed analizzando a livello network la nostra connessione. Rammento che il modo più semplice e a costo zero per ottenere la posta elettronica di una persona è quello di chiedere al gestore del server di posta elettronica di fornire copia degli archivi di posta (memorizzati per anni e anni, alcune volte per sempre) e di duplicare ogni messaggio in ingresso / uscita dal server di posta verso un determinato indirizzo di posta elettronica.

Pre-requisiti:

1) Si deve possedere un dominio registrato su un provider che consente la gestione DNS
2) Si deve possedere un certificato digitale SSL WildCard per il proprio dominio
3) Si deve possedere almeno un IP pubblico statico
4) Il router deve consentire almeno il PAT (Port Address Translation)
5) La configurazione di rete che ospiterà il server Synology deve essere perfetta, pena la perdita dei messaggi (i server di posta tipicamente mantengono le code dei messaggi non ancora consegnati per 3 giorni)
6) OS Synology dal 5.2

Configurazione del DNS:

1) Si deve creare un record A contenente in nome host del server (FQDN) es smtpsrv.DOMINIO.XXX
2) Si deve creare un record MX che punta al record A al punto 1
3) Si deve creare un record PTR che punta al proprio indirizzo IP pubblico statico

Nota: I punti 1 e 2 sono gestiti dal maintainer di dominio mentre il punto 3 è gestito dal provider di telecomunicazioni.

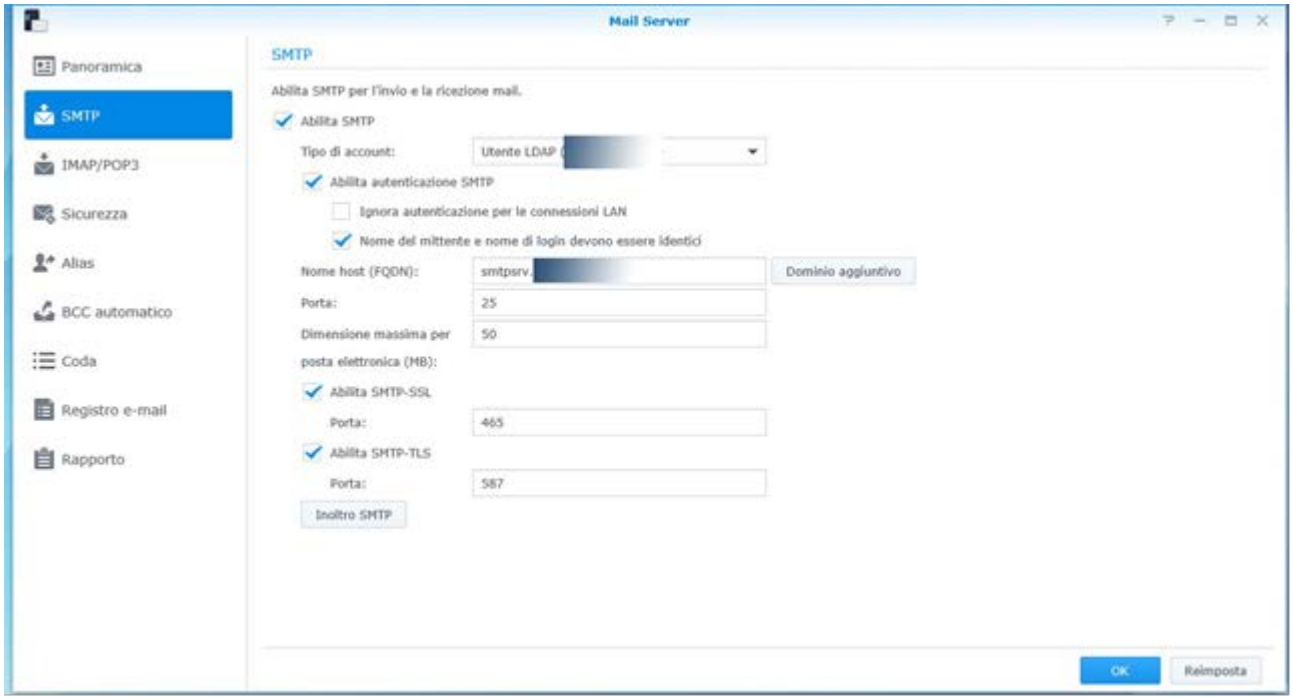
Nota: Maintainer testati www.gidinet.com e www.aruba.it . Gidinet perfettamente compatibile, Aruba parzialmente compatibile con configurazione custom fatte dall'help desk. Si consiglia Gidnet.

Configurazione del Mail Server Synology (OS 5.2)

1) Configurare un server LDAP, quello del Synology o altro
2) Installare il software MAIL SERVER

Pannello SMTP

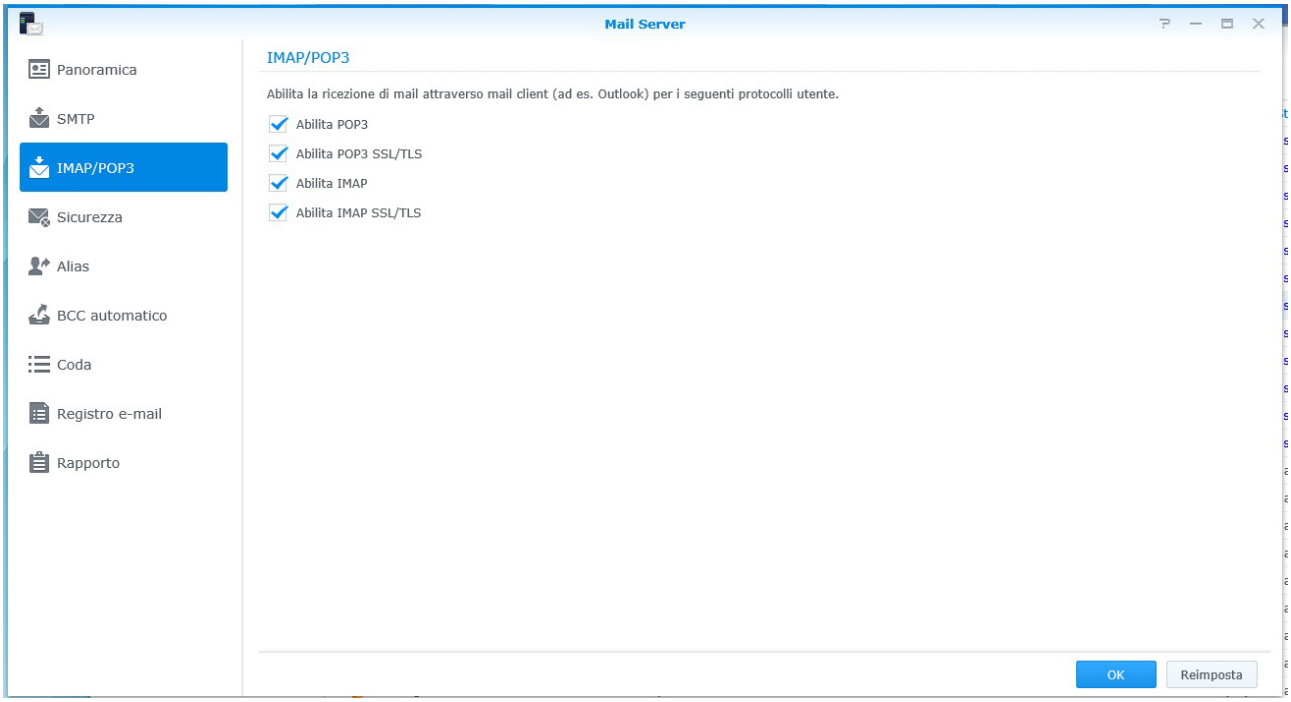
1) Abilitare SMTP con tipo account il proprio LDAP server
2) Abilitare autenticazione SMTP
3) Abilitare “Nome del mittente e nome login devono essere identici
4) Configurare il nome host del server a smtpsrv.DOMINIO.XXX
5) Nel menù dominio aggiuntivo aggiungere tutti i domini che si possiedono, se uno solo aggiungere comunque DOMINIO.XXX (questo è fatto per configurare correttamente l’SMTP banner check)
6) Abilitare SMTP-SSL
7) Abilitare SMTP-TLS



Pannello IMAP/POP3

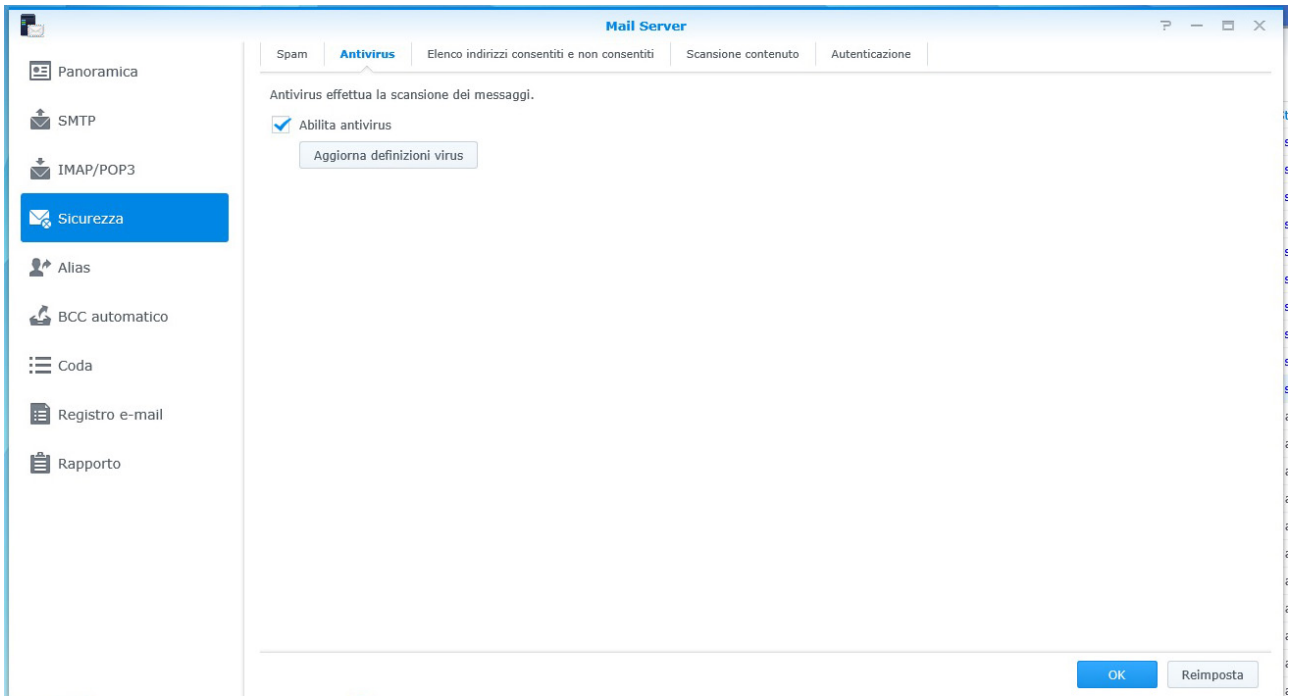
Abilitare tutte le opzioni per la ricezione della posta (tutte o quelle che si desiderano) si consiglia di usare esclusivamente le cifrate SSL/TLS e disabilitare a scelta le altre:

1) Abilita POP3, POP3 SSL/TLS, IMAP, IMAP SSL/TLS



Pannello Antivirus

Abilitare l’antivirus ed aggiornarlo



Pannello Sicurezza

Questo pannello è fondamentale ai fini del corretto funzionamento del server di posta elettronica, una non corretta configurazione mette a rischio la sicurezza del sistema di posta e successivo BAN del server da parte dei motori AntiSpam, pertanto consiglio di controllare bene le configurazioni prima di mettere online il sistema, pena l'essere posti in black list nel giro di alcuni giorni. Farsi rimuovere da queste liste può essere lungo e laborioso.

Pannello SPAM

1) Abilitare SPAM assassin
2) Abilitare filtro elenco blackhole basato su DNS

Pannello Antivirus

1) Abilitare l'antivirus
2) Aggiornare l'antivirus

Pannello Elenco indirizzi consenti e non consentiti

1) Lasciare le impostazioni standard

Pannello Scansione del contenuto

1) Abilitare Abilita Scansione del contenuto pericoloso
2) Abilitare Respingi messaggi parziali
3) Abilitare Respingi corpi dei messaggi esterni
4) Evidenzia Frode Pishing

Il seguente pannello "Autenticazione" richiede un paragrafo a sé essendo fondamentale per evitare di essere catalogati come server inaffidabili o di SPAM.

Pannello Autenticazione:

Configurazione SPF (AntiSPAM)

1) Si deve creare un record DNS SPF nella forma “v=spf1 mx ptr ip4:*PROPRIO-IP-STATICO* mx:smtpsrv. DOMINIO.XXX –all”

Nota: per la creazione del record DNS SPF si può utilizzare il tool http://www.spfwizard.net/

Configurazione DKIM (AntiSPAM)

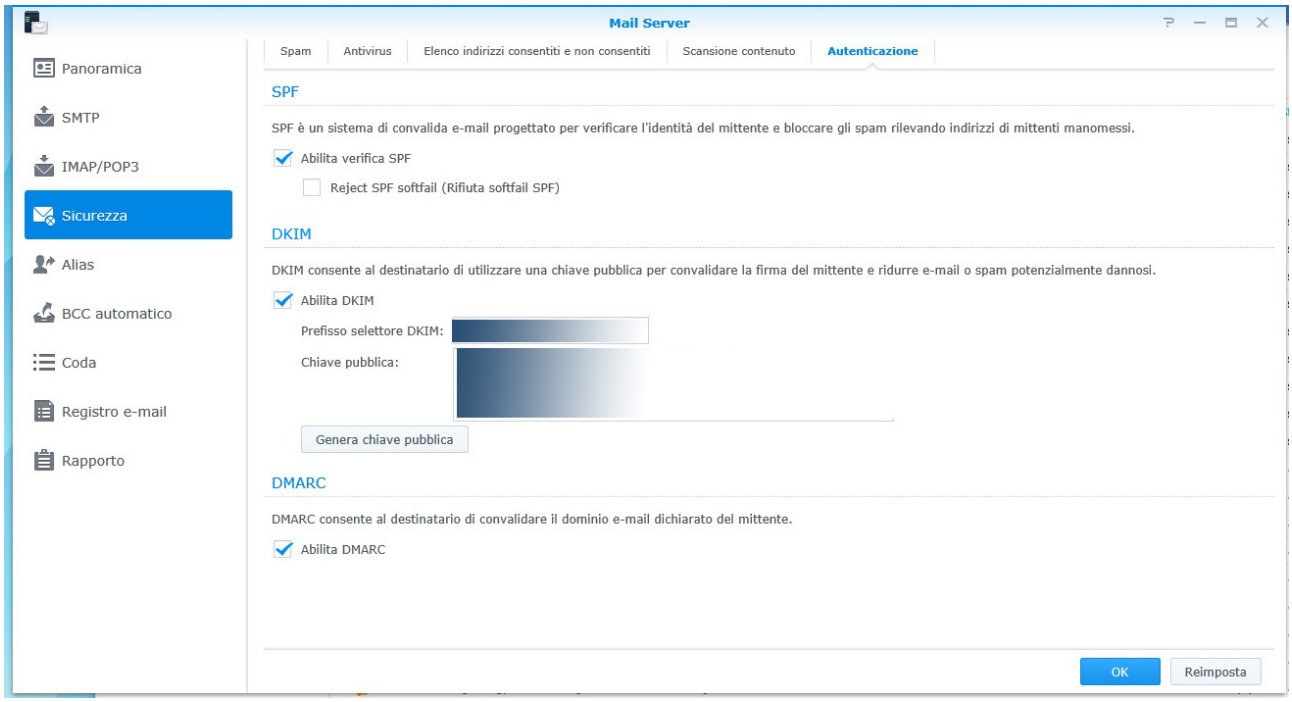
Per configurare il servizio DKIM si dovrà procedere alla creazione di un record DNS TXT nella seguente forma:

PrefissoSelettoreDKIM._domainkey. **DOMINIO.XXX**

"v=DKIM1; k=rsa; p=**ChiavePubblica** "

Alcuni importanti provider non supportano il record TXT DKIM ufficialmente, che come vedete è composto da un nome e da un valore, ad esempio ARUBA, ma tramite supporto tecnico si potrà comunque far creare il record DNS TXT necessario al DKIM sapendo che il provider ufficialmente non vi supporterà in caso di problemi. Alternativa alla vita incerta è di cercare un provider maintainer che ufficialmente supporti i record TXT DKIM oppure installare sul Synology il proprio server DNS e farsi delegare la gestione della propria zona, ovviamente è una cosa che richiede un ulteriore sforzo tecnico ed inoltre la sconsiglio a chi non può permettersi la ridondanza del server DNS, ma pur sempre è una strada percorribile.

1) Nel menù sicurezza abilitare Abilita verifica SPF
2) Abilitare DKIM impostando il nome es. MioServer01
3) Tramite il tasto genera chiave pubblica far generare la chiave
4) I punti 2 e 3 sono i dati con i quali si configurerà il DNS come sopra specificato.



Abilitare il DMARK (AntiSpam)

Per poter far funzionare il DMARK si deve creare uno specifico record DNS, valgono le stesse considerazione fatte sopra per il DKIM.

Il record ha la forma:

_dmarc. DOMINIO.XXX

"v=DMARC1; p=none; sp=none; rf=afrf; pct=100; ri=86400"

si può utilizzare il tool seguente per la creazione del record DMARK:

https://www.unlocktheinbox.com/dmarcwizard/

Abilitare la cifratura TLS/SSL

Per un corretto funzionamento della crittografia TLS/SSL sarà necessario installare un certificato digitale wildcard nel Synology. Tra le Certification Autority che conosco sicuramente tra le più economiche e compatibili con il Syno c'è SSL2BUY http://store.ssl2buy.com/ che vende un certificato wildcard attualmente a 42 USD/anno. Il certificato wildcard è un certificato digitale che permette di autenticare un dominio di secondo livello DOMINIO.XXX e tutti i suoi sottodomini *.DOMINIO.XXX. Questo è fondamentale perché nel server come minimo utilizzerete smtpsrv. DOMINIO.XXX e www. DOMINIO.XXX. e pertanto uno dei due domini di terzo livello risulterebbe non verificato con un normale certificato SSL.

Per installare il certificato wildcard dal panello sicurezza -> certificato si dovrà effettuare una richiesta di nuovo certificato "crea richiesta di firma del certificato (CSR)". Una volta generata la richiesta utilizzeremo i due file ricevuti dal Syno per completare la richiesta di wildcard e successivamente procederemo con l'importare il certificato generato dalla CA ed inoltrato per posta elettronica.

Test della configurazione DNS per SPF, DKIM e DMARK

Per verificare la corretta impostazione del DNS si può utilizzare il seguente tool:

https://www.mail-tester.com/spf-dkim-check

oppure utilizzare il seguente selezionando le opzioni di test per SPF, DKIM e DMARKLookUp

http://mxtoolbox.com/diagnostic.aspx

Test della configurazione del server SMTP e del DNS

Per verificare che il server SMTP ed il DNS sono correttamente configurati si può utilizzare il seguente tool opzioni MX test ed SMTP Server Test:

http://mxtoolbox.com/diagnostic.aspx

Test della configurazione TLS/SSL

Per verificare il corretto funzionamento della cifratura TLS/SSL si può utilizzare il seguente sito inserendo uno degli utenti di posta elettronica del server:

http://www.checktls.com/