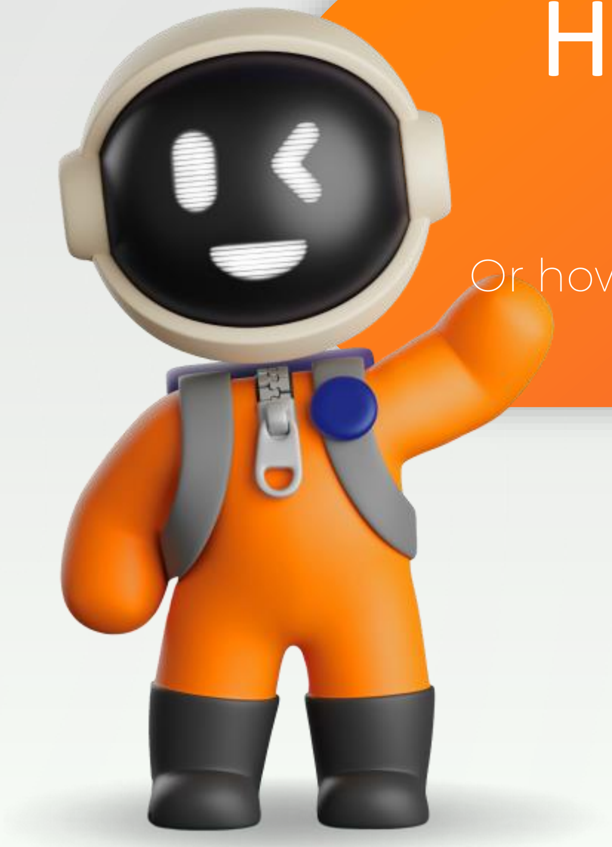
openntf

How to use Domino as a Mail Server in a Modern World

Or how to get your mails in your customer's mailboxes and spam out of yours



Martijn de Jong (e-office)

Daniel Nashed (Nash!Com)

Nash!Com Communication Systems

e-office

engage

Martijn de Jong

- Senior HCL Consultant @ e-office
- Studied electrical engineering, psychology and music
- Working with “Lotus” portfolio since 2000
- https://blog.martdj.nl

@martdj

HCL Ambassador 2020
HCL Ambassador 2021
HCL Ambassador 2022
HCLSoftware HCL Ambassador 2023
HCLSoftware HCL Ambassador 2024

Agenda

- SMTP Basics
- Outbound SMTP configuration in Domino
- Inbound SMTP configuration in Domino

SMTP Basics

- SMTP History
- SMTP Protocol
- PTR Record
- Sender Policy Framework (SPF)
- Domain Keys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting & Conformance (DMARC)
- SMTP submission vs SMTP relaying
- SMTP: Accept vs Reject vs Greylisting
- Secure transmission

SMTP History

- 1981: Simple Mail Transfer Protocol (SMTP) – RFC 788 - Jonathan B. (Jon) Postel
- “by design, every SMTP server was an open mail relay”
- 1995: Extended Simple Mail Transfer Protocol (ESMTP) – RFC 1869
- 1998: Message submission – RFC 2476
- 1999: SMTP Service Extension for Authentication – RFC 2554
- 2001: Simple Mail Transfer Protocol – RFC 2821
- 2008: Simple Mail Transfer Protocol – RFC 5321
- 2011: DomainKeys Identified Mail (DKIM) Signatures – RFC 6376
- 2014: Sender Policy Framework (SPF) – RFC 7208
- 2015: Domain-based Message Authentication, Reporting, and Conformance (DMARC) – RFC 7489
- 2015: SMTP 521 and 556 Reply Codes – RFC 7504
- 2018: Cryptographic Algorithm and Key Usage Update to DomainKeys Identified Mail (DKIM) – RFC 8301
- 2018: Use of Transport Layer Security (TLS) for Email Submission and Access – RFC 8314
- 2018: A New Cryptographic Signature Method for DomainKeys Identified Mail (DKIM) – RFC 8463
- 2019: Email Authentication for Internationalized Mail – RFC8616
- 2021: Deprecation of TLS 1.1 for Email Submission and Access – RFC 8997

SMTP Protocol example

```
S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.org
S: 250 Hello relay.example.org, I am glad to meet you
C: MAIL FROM:<bob@example.org>
S: 250 Ok
C: RCPT TO:<alice@example.com>
S: 250 Ok
C: RCPT TO:<theboss@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: "Bob Example" bob@example.org
C: To: "Alice Example" <alice@example.com>
C: Cc: theboss@example.com
C: Date: Tue, 15 Jan 2008 16:02:43 -0500
C: Subject: Test message
C:
C: Hello Alice.
C: This is a test message with 5 header fields and 4 lines in the message body.
C: Your friend,
C: Bob
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
{The server closes the connection}
```

PTR record

- Every mail starts with a connection:
  ```
  SMTP Server: notes.nashcom.de (157.90.30.24) connected
  ```
- Reverse DNS lookup – Does 157.90.30.24 belong to notes.nashcom.de?
- Looks for a PTR record

PTR record lookup

```
dig 24.30.90.157.in-addr.arpa PTR

; <<>> DiG 9.16.23-RH <<>> 24.30.90.157.in-addr.arpa PTR
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32637
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d39bb4213a56db7901000000668e58c4cde082e76f760d4c (good)
;; QUESTION SECTION:
;24.30.90.157.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
24.30.90.157.in-addr.arpa. 81732 IN     PTR     notes.nashcom.de.
```

PTR Record

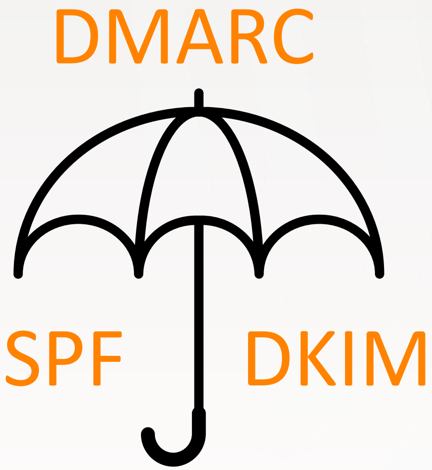
- PTR records can only be set by the owner of your IP address(es)
- That’s usually your internet or hosting provider
- Some provide an admin interface to set your PTR record
- Some provide no PTR records
- No PTR record or non-matching PTR record => huge hit on your reputational score!

Reputational Score

- Anti-spam measures work with a reputational score
- The score is calculated based on:
  - The sending server (PTR record, blacklists, SPF)
  - The domain of the sender (SPF, DKIM, DMARC)
  - The mail content
- The higher the score, the better your chance your mail is delivered in the inbox of the intended recipient

SPF, DKIM & DMARC

- SPF: Is the sending server allowed to send mail for this domain?
- DKIM: Is this mail from this domain really sent from this domain?
- DMARC: What to do with the result of the previous checks?



e-office

Sender Policy Framework

- Server tries to drop a mail at the server:
  C: EHLO notes.nashcom.de
  S: 250-poseidon.martdj.nl Hello notes.nashcom.de ([157.90.30.24]), pleased to meet you
  C: MAIL FROM:nsh@nashcom.de

- Check in DNS if 157.90.30.24 is allowed to send mail from nashcom.de

SPF – DNS TXT Record

- RFC 7208 - Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1
  - https://datatracker.ietf.org/doc/html/rfc7208
- Defines which host are **allowed to send mails for a domain**
- **DNS TXT record** for a domain or sub-domain with flexible rule set
- Example:

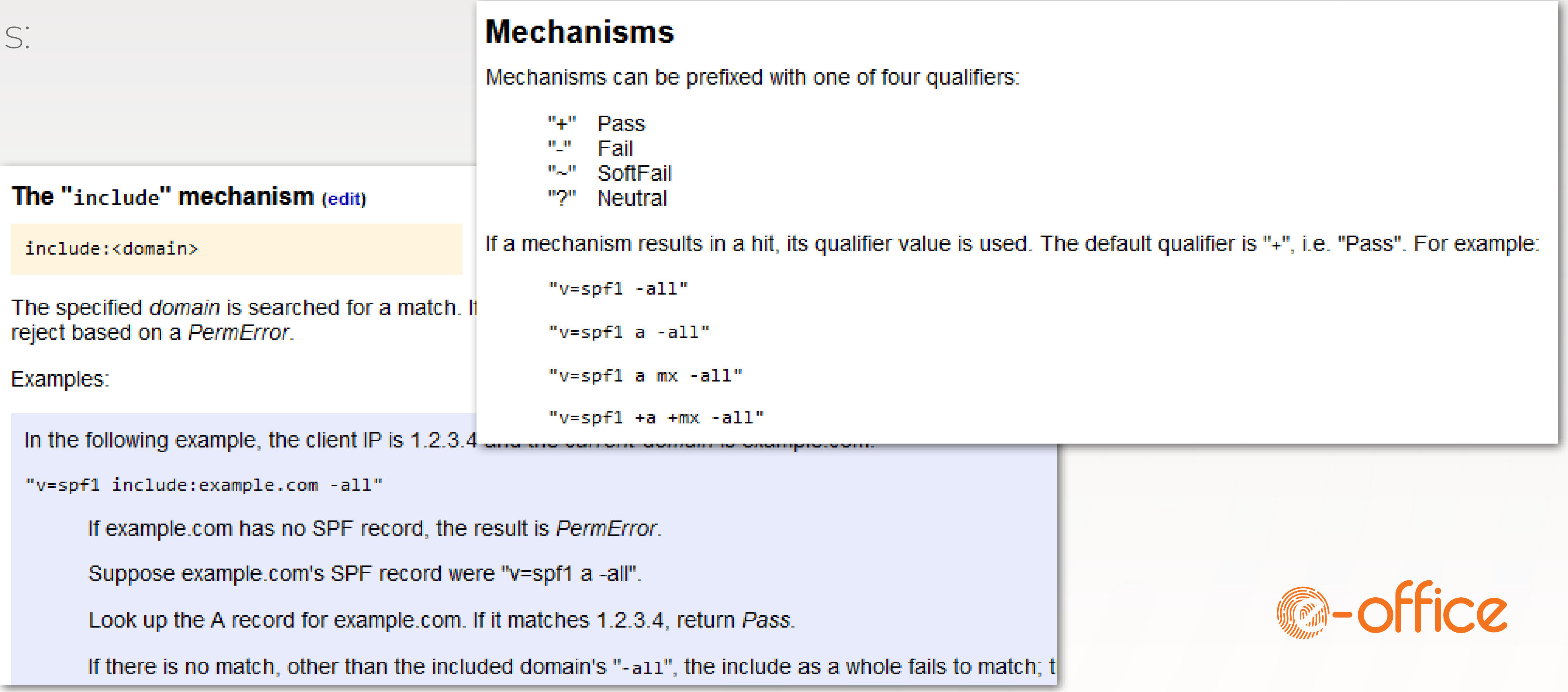
```
host -t txt nashcom.de -> nashcom.de descriptive text "v=spf1 mx
~all"
```

  - Only allows domain's defined MX record hosts to send mail
- More complex example **dnug.de**

```
v=spf1 mx
 a:domino.dnug.de ip4:87.230.23.16
 include:spf.nl2go.com include:mail.zendesk.com include:spf.ce.cloud-y.com
 -all
```

SPF Syntax

- http://www.open-spf.org/SPF_Record_Syntax
- Mechanisms:
  - all
  - ip4
  - ip6
  - a
  - mx
  - ptr
  - exists
  - include



Mechanisms

Mechanisms can be prefixed with one of four qualifiers:

"+"	Pass
"-"	Fail
"~"	SoftFail
"?"	Neutral

If a mechanism results in a hit, its qualifier value is used. The default qualifier is "+", i.e. "Pass". For example:

```
"v=spf1 -all"
"v=spf1 a -all"
"v=spf1 a mx -all"
"v=spf1 +a +mx -all"
```

The "include" mechanism (edit)

```
include:<domain>
```

The specified *domain* is searched for a match. I
reject based on a *PermError*.

Examples:

In the following example, the client IP is 1.2.3.4 and the current domain is example.com.

```
"v=spf1 include:example.com -all"
```

If example.com has no SPF record, the result is *PermError*.

Suppose example.com's SPF record were "v=spf1 a -all".

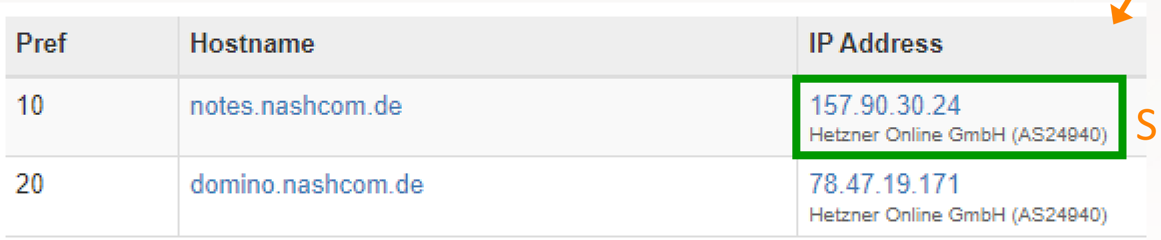
Look up the A record for example.com. If it matches 1.2.3.4, return *Pass*.

If there is no match, other than the included domain's "-all", the include as a whole fails to match; t

Sender Policy Framework

- Server tries to drop a mail at the server:
  C: EHLO notes.nashcom.de
  S: 250-poseidon.martdj.nl Hello notes.nashcom.de ([157.90.30.24]), pleased to meet you
  C: MAIL FROM:nsh@nashcom.de

- Check in DNS if 157.90.30.24 is allowed to send mail from nashcom.de
- SPF DNX TXT Record nashcom.de: v=spf1 mx ~all
- MX Lookup:



Pref	Hostname	IP Address
10	notes.nashcom.de	157.90.30.24 Hetzner Online GmbH (AS24940)
20	domino.nashcom.de	78.47.19.171 Hetzner Online GmbH (AS24940)

SPF Pass

e-office

https://www.youtube.com/watch?v=jy6YMzQZTz8&t=11s

DKIM Explained

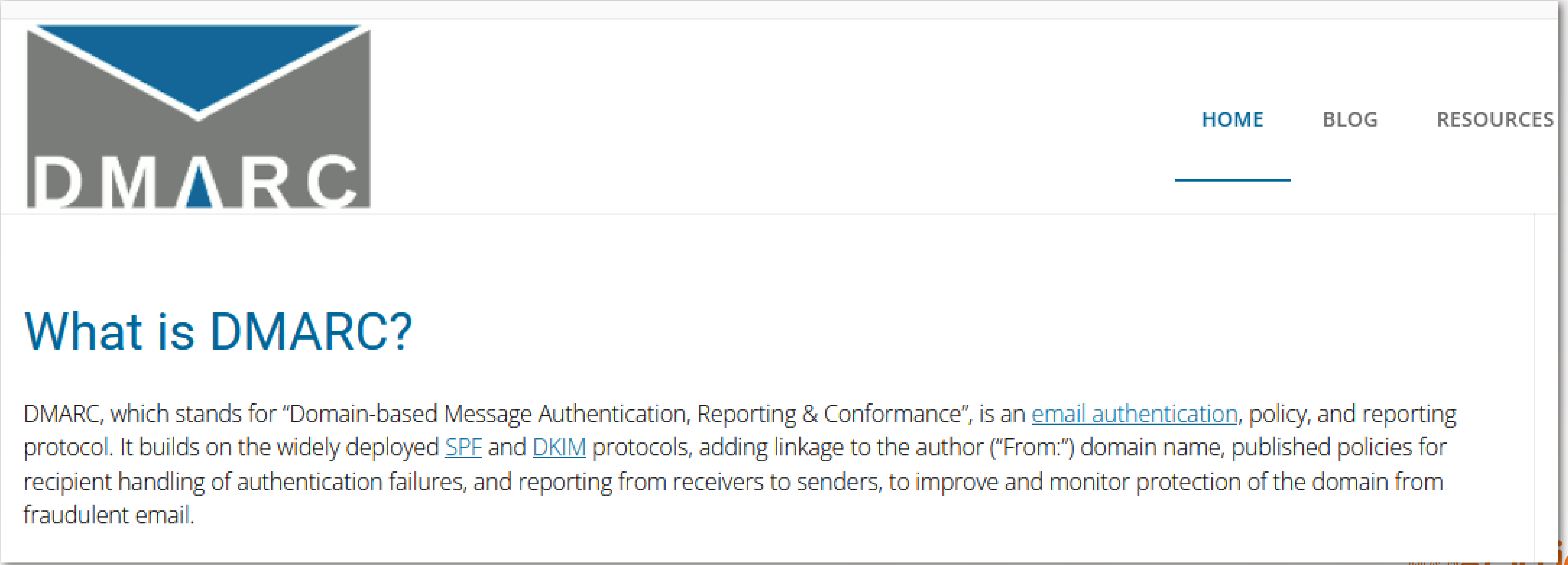
mailtrap

DomainKeys Identified Mail (DKIM)

- Verifies that the content of a mail was not altered after it was sent
- Used for reputation checking and spam prevention
- Non-repudiability – when a mail is sent with a DKIM hash, an organization can't deny that it was sent by them
- Depends on both a DNS TXT record and the sending mail server
- Multiple DKIM DNS TXT records allowed. Selector should be unique
- CNAME forwarding is allowed

DMARC

- Domain-based Message Authentication, Reporting and Conformance



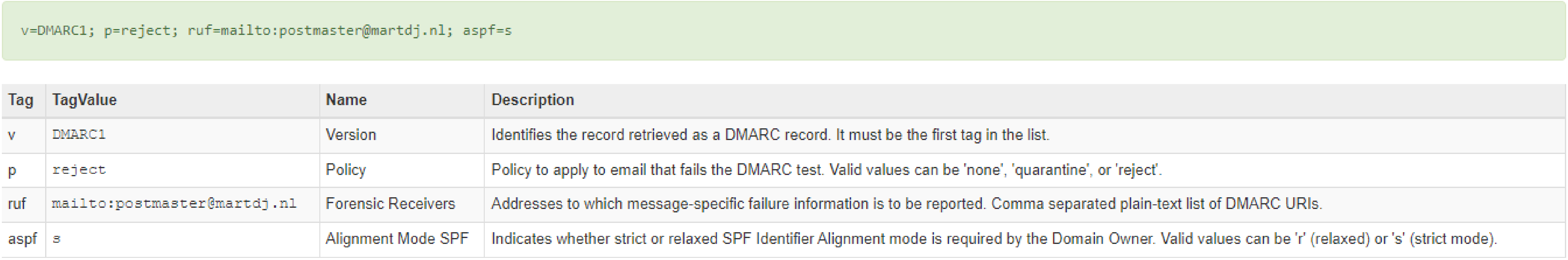
What is DMARC?

DMARC, which stands for "Domain-based Message Authentication, Reporting & Conformance", is an email authentication, policy, and reporting protocol. It builds on the widely deployed SPF and DKIM protocols, adding linkage to the author ("From:") domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email.

https://dmarc.org

DMARC

- Combines **SPF** and **DKIM** and allows to define policies for your domain
- **RFC 7489** - Domain-based Message Authentication, Reporting, and Conformance (DMARC)
  - https://datatracker.ietf.org/doc/html/rfc7489
- Another DNS TXT record
- example



```
v=DMARC1; p=reject; ruf=mailto:postmaster@martdj.nl; aspf=s
```

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	reject	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
ruf	mailto:postmaster@martdj.nl	Forensic Receivers	Addresses to which message-specific failure information is to be reported. Comma separated plain-text list of DMARC URIs.
aspf	s	Alignment Mode SPF	Indicates whether strict or relaxed SPF Identifier Alignment mode is required by the Domain Owner. Valid values can be 'r' (relaxed) or 's' (strict mode).

DMARC – Online Resource

- What is DMARC?
  - https://www.mailjet.com/blog/news/some-words-about-dmarc
- Google - Help prevent spoofing and spam with DMARC
  - https://support.google.com/a/answer/2466580
- Build your DMARC Record
  - https://dmarcguide.globalcyberalliance.org
- OpenSource DMARC Analyzer
  - https://domainaware.github.io/parsedmarc
- DMARC Organization
  - https://dmarc.org

SMTP: Accept vs Reject vs Greylisting

- Accept: Mail is accepted by server and will be delivered to recipient, moved to quarantine or moved to the trash
- Reject: Mail won't be accepted by the receiving mail server
- Greylisted: Mail is temporarily not accepted (see next slide)
- It's better to reject mail than to accept mail and throw it in the trash bin
    - Uses no resources in your domain
    - As long you don't accept a message you are not responsible for the message
    - Sending host must deal with it
    - Should give sender a Non Delivery Report
    - In case of a legitimate sender, they'll know that they should contact you in another way
- Same for badly monitored quarantine

Greylisting

- Greylisting is based on:
  "the SMTP client retains responsibility for delivery of that message" (section 4.2.5) and "mail that cannot be transmitted immediately MUST be queued and periodically retried by the sender.“ – RFC 5321
- Proper mail servers will retry sending a mail. Spammers usually won’t
- Disadvantages:
  - Mail is delayed (by at least 30 minutes)
  - Retries might come from a different IP address
  - Uses more resources on sending servers
- As a result, greylisting is controversial

Submission vs Relaying

- Mail client -> mail server: submission
  - Port 587, 465 or port 25

- Mail server -> mail server: relaying
  - Port 25

Secure transmission

- Not to be confused with Secure mail (S/MIME)
- Two methods:
  - STARTTLS (port 25 or 587)
  - Implicit TLS (port 465)

STARTTLS should be configured on every server

- Session is established on port 25 or port 587 unencrypted
- Server signals it supports TLS via STARTTLS extension
- Client issues "STARTTLS" command
- A new "EHLO" is used to restart the communication
- Standard TLS handshake is used to negotiate the connection
- Most servers don't verify certificates used for SMTP
  - Many servers still have default self signed certs → Lots of messages would be blocked
- Most environments use "opportunistic" STARTTLS and not enforce it
  - Client and server can decide if they want to enforce it

Implicit TLS

- SMTP over SSL on port 465 was established in 1997
- Deprecated in 1998
- Made a comeback in 2018 (RFC 8314)
- Now the preferred method for email submission
- TLS 1.2 and TLS 1.3 only (RFC 8997)

Domino Outbound SMTP Configuration

- DKIM
- StartTLS
- Implicit TLS
- Relay host
- Real-life examples
- Test your configuration

Outbound implementation for your domain

Method	DNS of your domain	Outbound mail server configuration
PTR Record	✓	-
SPF	✓	-
DKIM	✓	✓
DMARC	✓	-
StartTLS	-	✓
Implicit TLS	-	✓

DKIM – Initial setup

- HCL could have made this easy…
- … but they didn’t. So here we go:
- DKIM uses the OAuth Token Store
- Also known as the Credential Store
- The credential store is encrypted with a Notes Encryption Key
- Which is stored in de server’s id-file
- It must be shared among all servers that work with the credential store
- The credential store can replicate inside a cluster
- It can’t replicate outside a cluster

DKIM – Creating the credential store

- Check if you have a credential store
  - Might have been created for “more secure internet passwords”
  - Should be in IBM_CredStore directory on the server
- If no file is found:
  - From the Domino Console: (!)
  - `Keymgmt create nek credstorekey`
    Creates a Notes Encryption Key called “credstorekey”
  - `Keymgmt create credstore credstorekey`
    Creates the credential store / OAuth Token Store

DKIM – Creating DKIM Keys

- 2 Possible encryption types:
  - RSA
    Possible key length: 1024, 2048 or 4096 bits. 1024 bits currently recommended for DKIM
  - Ed25519
    Newer & more efficient. Added in 2018. Not supported by all receiving mail servers. Key length is 256 bits and is implicit (not added in commands)
- `keymgmt create DKIM <domain> <selector> <encryption type & strength>`
  domain: your domain (e.g. martdj.nl)
  selector: alphanumeric string (e.g. rsa202407)
  encryption type & strength: See above
- Examples:
  RSA: `keymgmt create DKIM martdj.nl rsa202407 rsa 1024`
  ED25519: `keymgmt create DKIM martdj.nl ed20240705 Ed25519`
  server response: Created DKIM key Ed20240705._domainkey.martdj.nl

DKIM – Export DNS TXT Value

- **keymgmt export DKIM DNS martdj.nl ed20240705 martdj_nl_ed20240705.txt**

  ```
  Parse domain martdj.nl
  Parse selector ed20240705
  Parse filename martdj_nl_ed20240705.txt
  Get DKIM key  d=martdj.nl, s=ed20240705, No error
  Get Key as PEM No error
  Get Key as DNSKey v=DKIM1; k=ed25519;
  p=jUMDZCZSx8CaGYVlUbwNaGF5LXgEFwRhpXqSx4O8GvI=;, 68, No error
  Exported DKIM key to DNS file /local/notesdata/martdj_nl_ed20240705.txt, No error
  ```

- Contents of martdj_nl_ed20240705.txt

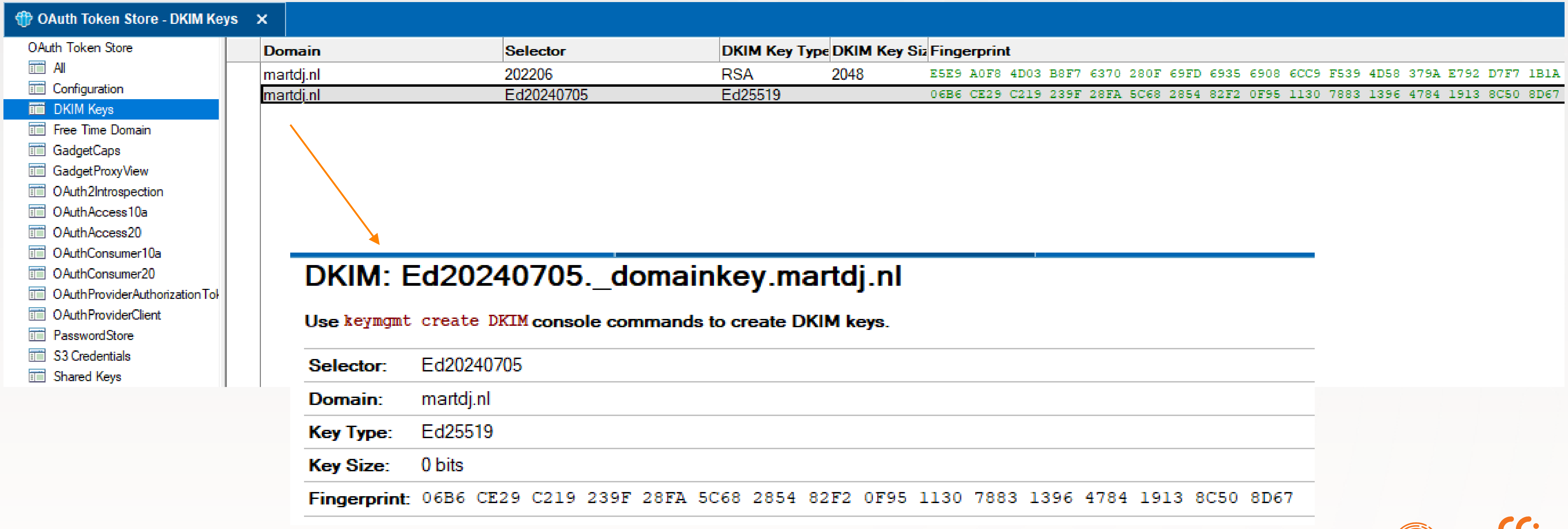
  ```
  v=DKIM1; k=ed25519; p=jUMDZCZSx8CaGYVlUbwNaGF5LXgEFwRhpXqSx4O8GvI=;
  ```

- Do the same for the RSA key

e-office

DKIM keys in OAuth Token Store

- OAuth Token Store



Domain	Selector	DKIM Key Type	DKIM Key Siz	Fingerprint
martdj.nl	202206	RSA	2048	E5E9 A0F8 4D03 B8F7 6370 280F 69FD 6935 6908 6CC9 F539 4D58 379A E792 D7F7 1B1A
martdj.nl	Ed20240705	Ed25519		06B6 CE29 C219 239F 28FA 5C68 2854 82F2 0F95 1130 7883 1396 4784 1913 8C50 8D67

DKIM: Ed20240705._domainkey.martdj.nl

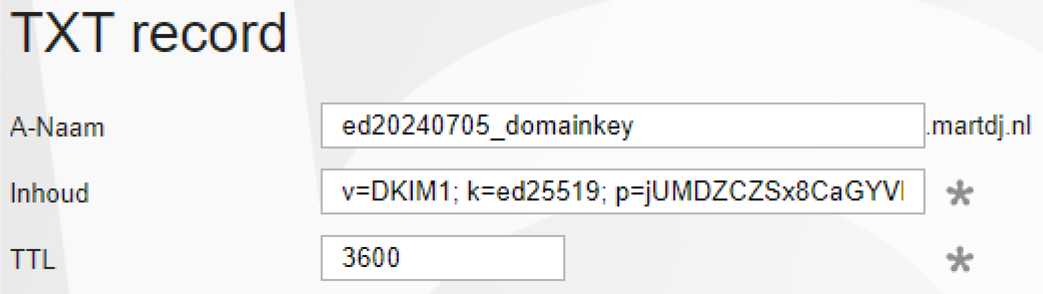
Use `keymgmt create DKIM` console commands to create DKIM keys.

Selector:	Ed20240705
Domain:	martdj.nl
Key Type:	Ed25519
Key Size:	0 bits
Fingerprint:	06B6 CE29 C219 239F 28FA 5C68 2854 82F2 0F95 1130 7883 1396 4784 1913 8C50 8D67

DKIM – Add records to DNS

- Add the DKIM key to DNS as a TXT record

- A-Name = selector + "._domainkey"



TXT record

A-Naam	ed20240705_domainkey	.martdj.nl
Inhoud	v=DKIM1; k=ed25519; p=jUMDZCZSx8CaGYVI	*
TTL	3600	*

- Add both Ed25519 record and RSA record

DKIM – Add key to notes.ini

- Enable DKIM on your server:

```
set config DKIM_KEY_martdj.nl=ed20240705,202206

set config RouterDKIMSigning=1

restart task router
```

Ed25519

RSA

DKIM

That didn’t seem too hard!

That was just the beginning...

DKIM in a cluster

- If you didn't have a credential store yet:
- keymgmt export nek <nekname> <nekname>.key <password>

  ```
  example: keymgmt export nek credstorekey credstorekey.key passw0rd
  NEK > NEK credstorekey - Fingerprint A8C5 9018 C714 3F05 E574 93D9
  5E70 005A 5371 4A71
  NEK credstorekey exported successfully
  ```

- Copy file <nekname>.key to cluster server(s)
- keymgmt import nek overwrite <nekname>.key <password>

  ```
  example: keymgmt import nek overwrite credstorekey.key passw0rd
  NEK > NEK credstorekey - Fingerprint A8C5 9018 C714 3F05 E574 93D9
  5E70 005A 5371 4A71
  NEK credstorekey imported successfully
  ```

- Create replicas of IBM_CredStore\<credstorename>.nsf on the original server to the other servers in the cluster

DKIM in a cluster – notes.ini

- Enable DKIM on every server
  set config DKIM_KEY_<domain>=<selector1>,<selector2>
  example: **`set config DKIM_KEY_martdj.nl=ed20240705,202206`**

```
set config RouterDKIMSigning=1

restart task router
```

- Or add to the notes.ini section in the configuration document for a group of servers

DKIM outside a cluster

- If you didn't have a credential store yet:
  - See previous section to export and import the Notes Encryption Key

- Create a credstore (as documents in the credential store can only be decrypted inside a cluster)

  ```
  Keymgmt create credstore credstorekey
  ```

DKIM outside a cluster – export DKIM keys

- Export the DKIM keys to a temporary database
  keymgmt export DKIM <dkimdb>.nsf <destination server>
  example:

```
keymgmt export DKIM dkimdb-pegasus.nsf Pegasus/SRV/Martinus
Credential Store Name : IBM_CredStore\credstore.nsf
Recovery Manager: Assigning new DBIID for
/local/notesdata/IBM_CredStore/dkimdb-pegasus.nsf (need new backup
for media recovery).
05-07-2024 11:46:12   Recovery Manager: Assigning new DBIID for
/local/nif/IBM_CredStore/dkimdb-pegasus_nsf.ndx (need new backup
for media recovery).
Exported DKIM keys No error
```

- Copy or replicate temporary database to destination server

DKIM outside a cluster – Import DKIM keys

- Import DKIM keys in Credential Store
  keymgmt import <name of credential store> <name of temporary db.nsf>
  example: `keymgmt import credstore dkimdb-pegasus.nsf`

  ```
  Credential Store Name : IBM_CredStore\credstore.nsf
  Credential Store imported successfully
  ```

- Do this for every cluster or server

- Add notes.ini parameter to each server that sends SMTP mail

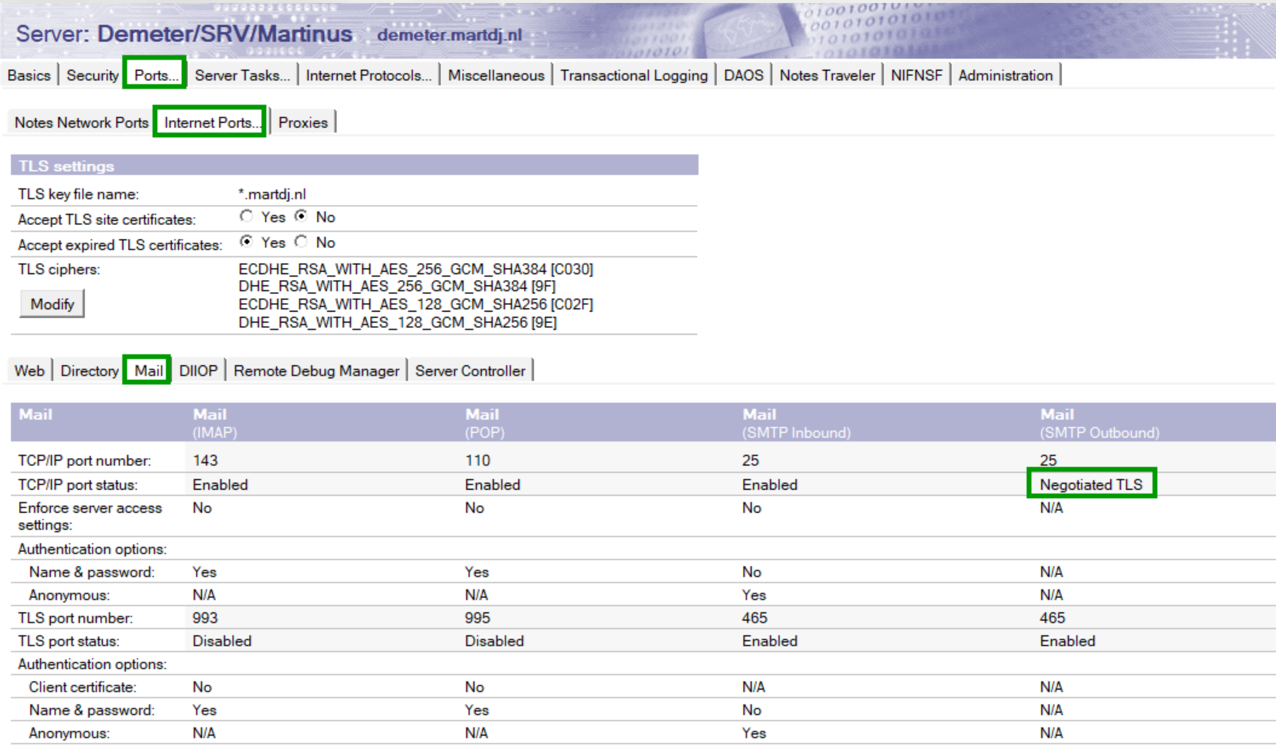
  ```
  set config DKIM_KEY_martdj.nl=ed20240705,202206
  set config RouterDKIMSigning=1
  restart task router
  ```

- You can export / import multiple DKIM keys in one go

Enable Outbound STARTTLS

- Set “Negotiated TLS” on SMTP Outbound

- For servers that don’t support StartTLS there’s a Notes.ini setting to fall back to an unencrypted connection
  - Notes.ini ROUTERFALLBACKNONTLS=1



Server: Demeter/SRV/Martinus demeter.martdj.nl

Basics | Security | Ports... | Server Tasks... | Internet Protocols... | Miscellaneous | Transactional Logging | DAOS | Notes Traveler | NIFNSF | Administration
Notes Network Ports | Internet Ports... | Proxies

TLS settings

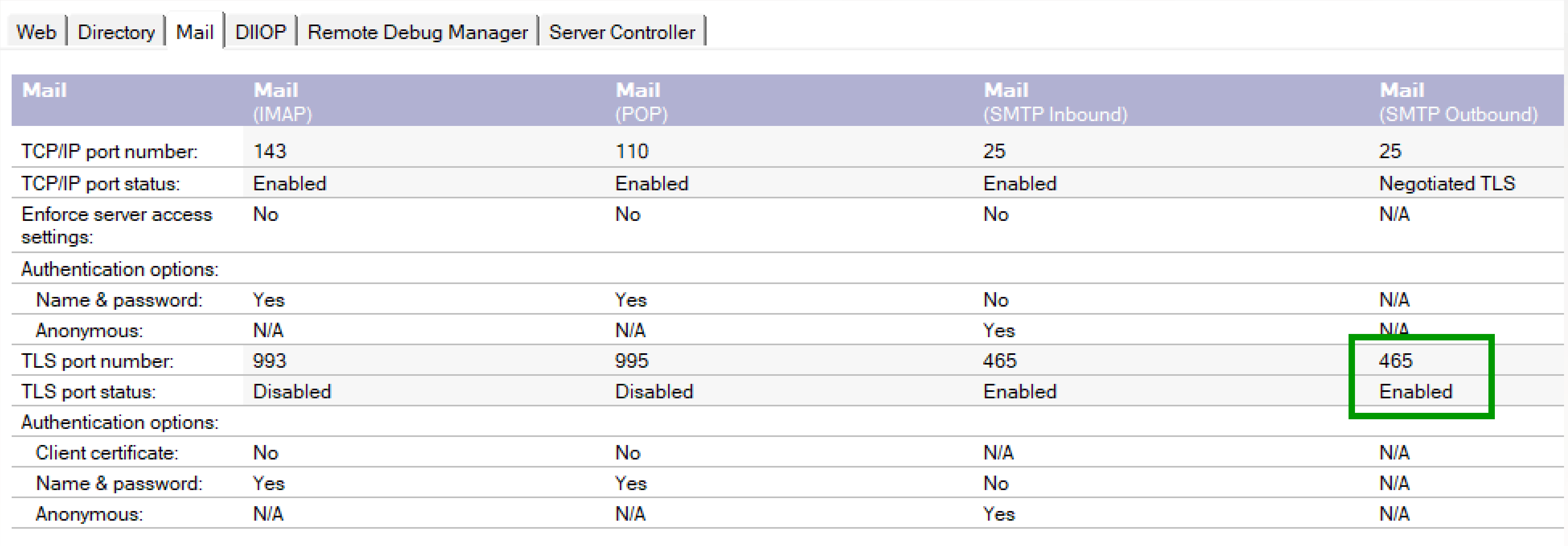
TLS key file name:	*.martdj.nl
Accept TLS site certificates:	○ Yes ● No
Accept expired TLS certificates:	● Yes ○ No
TLS ciphers: Modify	ECDHE_RSA_WITH_AES_256_GCM_SHA384 [C030] DHE_RSA_WITH_AES_256_GCM_SHA384 [9F] ECDHE_RSA_WITH_AES_128_GCM_SHA256 [C02F] DHE_RSA_WITH_AES_128_GCM_SHA256 [9E]

Web | Directory | Mail | DIIOP | Remote Debug Manager | Server Controller

Mail	Mail (IMAP)	Mail (POP)	Mail (SMTP Inbound)	Mail (SMTP Outbound)
TCP/IP port number:	143	110	25	25
TCP/IP port status:	Enabled	Enabled	Enabled	Negotiated TLS
Enforce server access settings:	No	No	No	N/A
Authentication options:				
Name & password:	Yes	Yes	No	N/A
Anonymous:	N/A	N/A	Yes	N/A
TLS port number:	993	995	465	465
TLS port status:	Disabled	Disabled	Enabled	Enabled
Authentication options:				
Client certificate:	No	No	N/A	N/A
Name & password:	Yes	Yes	No	N/A
Anonymous:	N/A	N/A	Yes	N/A

SMTP over TLS

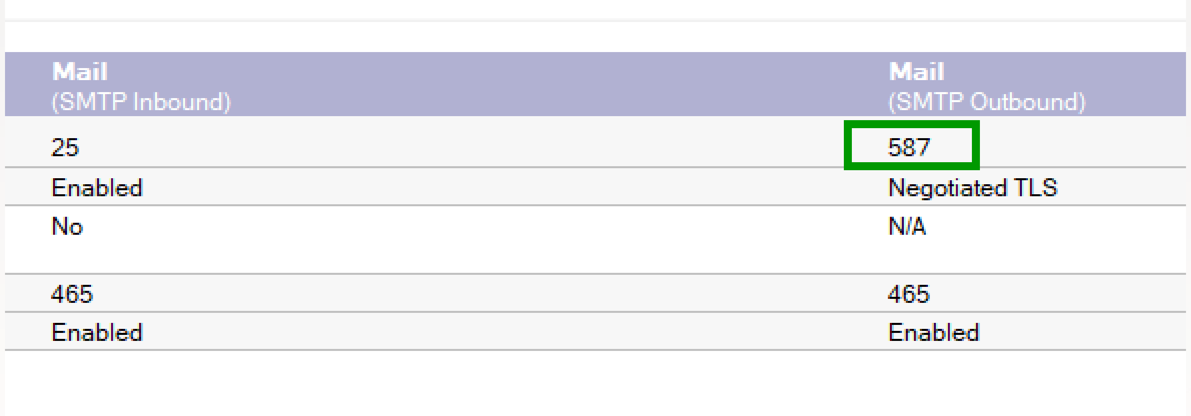
- Implicit TLS
- Uses port 465



Mail	Mail (IMAP)	Mail (POP)	Mail (SMTP Inbound)	Mail (SMTP Outbound)
TCP/IP port number:	143	110	25	25
TCP/IP port status:	Enabled	Enabled	Enabled	Negotiated TLS
Enforce server access settings:	No	No	No	N/A
Authentication options:				
Name & password:	Yes	Yes	No	N/A
Anonymous:	N/A	N/A	Yes	N/A
TLS port number:	993	995	465	465
TLS port status:	Disabled	Disabled	Enabled	Enabled
Authentication options:				
Client certificate:	No	No	N/A	N/A
Name & password:	Yes	Yes	No	N/A
Anonymous:	N/A	N/A	Yes	N/A

Submitting vs Relaying

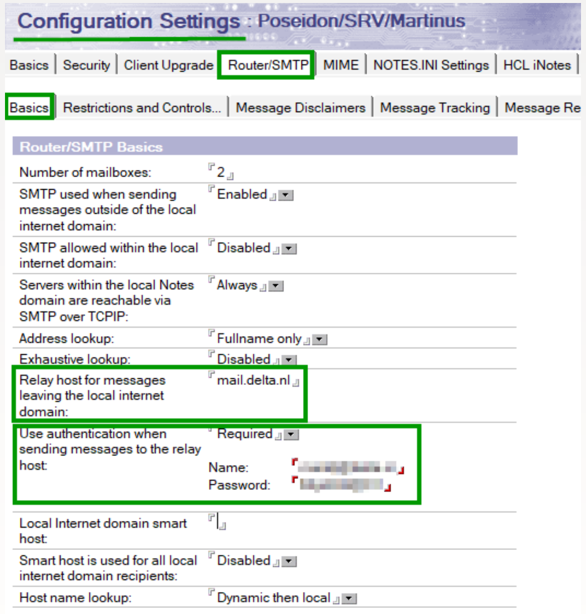
- Port 587 has become the default port for **submitting** SMTP mail to a mail server
- Port 25 is still the default port for **relaying** mail between mail servers
- How to configure your SMTP outbound port depends on whether you use a relay host (to which your server is **submitting** mail) or whether your server is relaying mail directly to the recipient's domain



Mail (SMTP Inbound)	Mail (SMTP Outbound)
25	587
Enabled	Negotiated TLS
No	N/A
465	465
Enabled	Enabled

Relay Host

- Some reasons to use a relay host
  - Your server can’t have a PTR record
  - Your server has no or limited access to internet
- Relay host is configured in Configuration document



Configuration Settings : Poseidon/SRV/Martinus
Basics | Security | Client Upgrade | Router/SMTP | MIME | NOTES.INI Settings | HCL iNotes |
Basics | Restrictions and Controls... | Message Disclaimers | Message Tracking | Message Re

Router/SMTP Basics

Number of mailboxes:	2
SMTP used when sending messages outside of the local internet domain:	Enabled
SMTP allowed within the local internet domain:	Disabled
Servers within the local Notes domain are reachable via SMTP over TCPIP:	Always
Address lookup:	Fullname only
Exhaustive lookup:	Disabled
Relay host for messages leaving the local internet domain:	mail.delta.nl
Use authentication when sending messages to the relay host:	Required Name: [redacted] Password: [redacted]
Local Internet domain smart host:	
Smart host is used for all local internet domain recipients:	Disabled
Host name lookup:	Dynamic then local

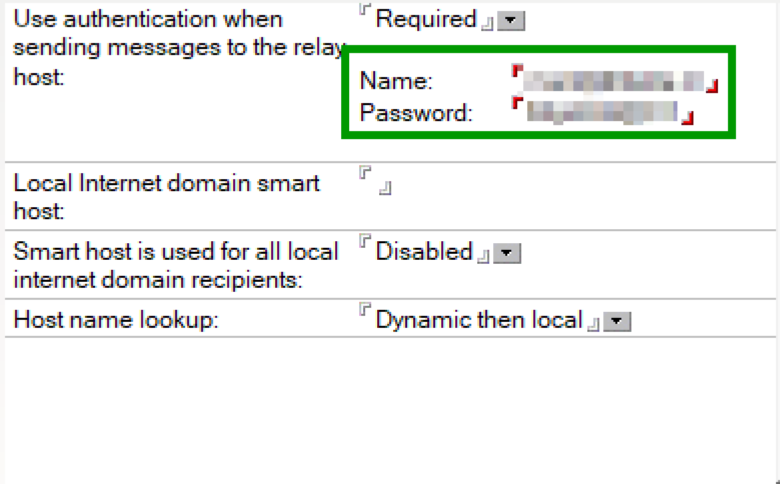
IP address or FQDN. Can be multi-value

Required – will only make connections if auth is supported

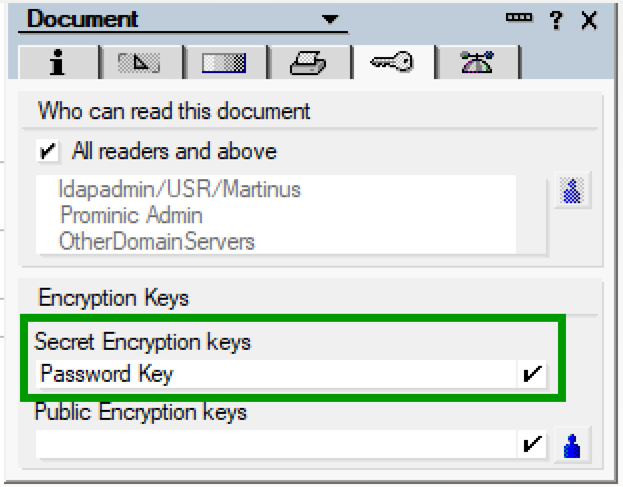
Enabled – will authenticate if supported, otherwise unauthenticated

Relay Host – Protect your password

- Name and password fields will be encrypted if the document is encrypted by a secret key
- Secret key has to be imported in IDs of all servers using this document and all administrators



Use authentication when sending messages to the relay host:	Required Name: [redacted] Password: [redacted]
Local Internet domain smart host:	
Smart host is used for all local internet domain recipients:	Disabled
Host name lookup:	Dynamic then local



Who can read this document

✓ All readers and above

ldapadmin/USR/Martinus
Prominic Admin
OtherDomainServers

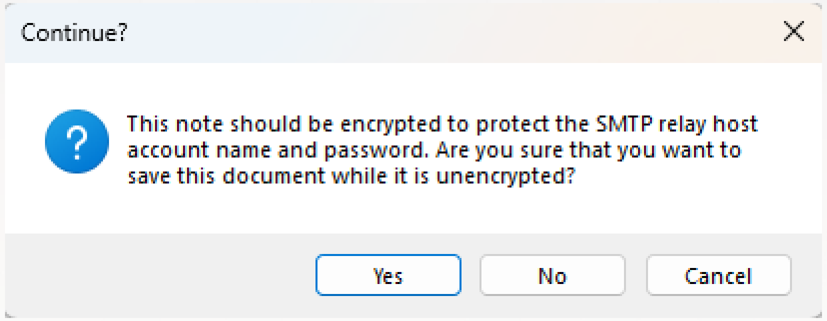
Encryption Keys

Secret Encryption keys

Password Key ✓

Public Encryption keys ✓

Otherwise:

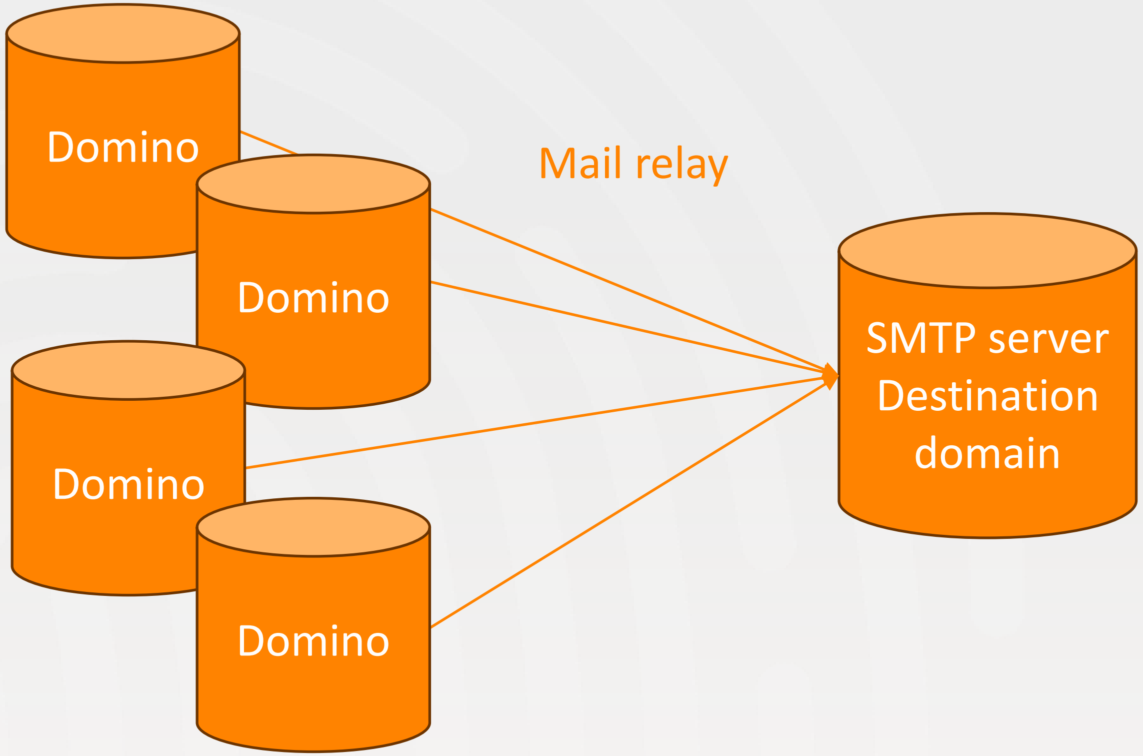


Continue?

This note should be encrypted to protect the SMTP relay host account name and password. Are you sure that you want to save this document while it is unencrypted?

Real life scenario’s

Sending Mail

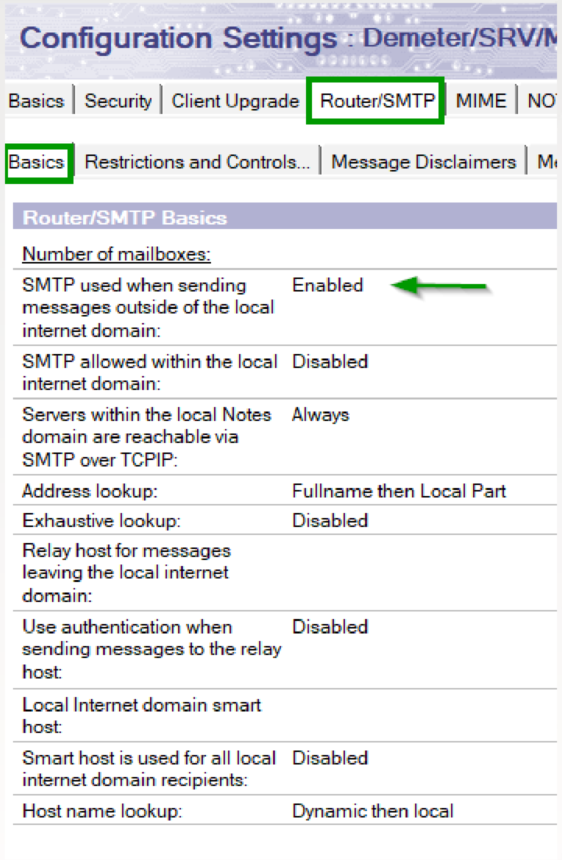


Scenario 1

Every server in the domain can send SMTP mail directly

Scenario 1

- Just make sure “SMTP used when sending messages outside of the local internet domain:” is enabled



Configuration Settings : Demeter/SRV/M

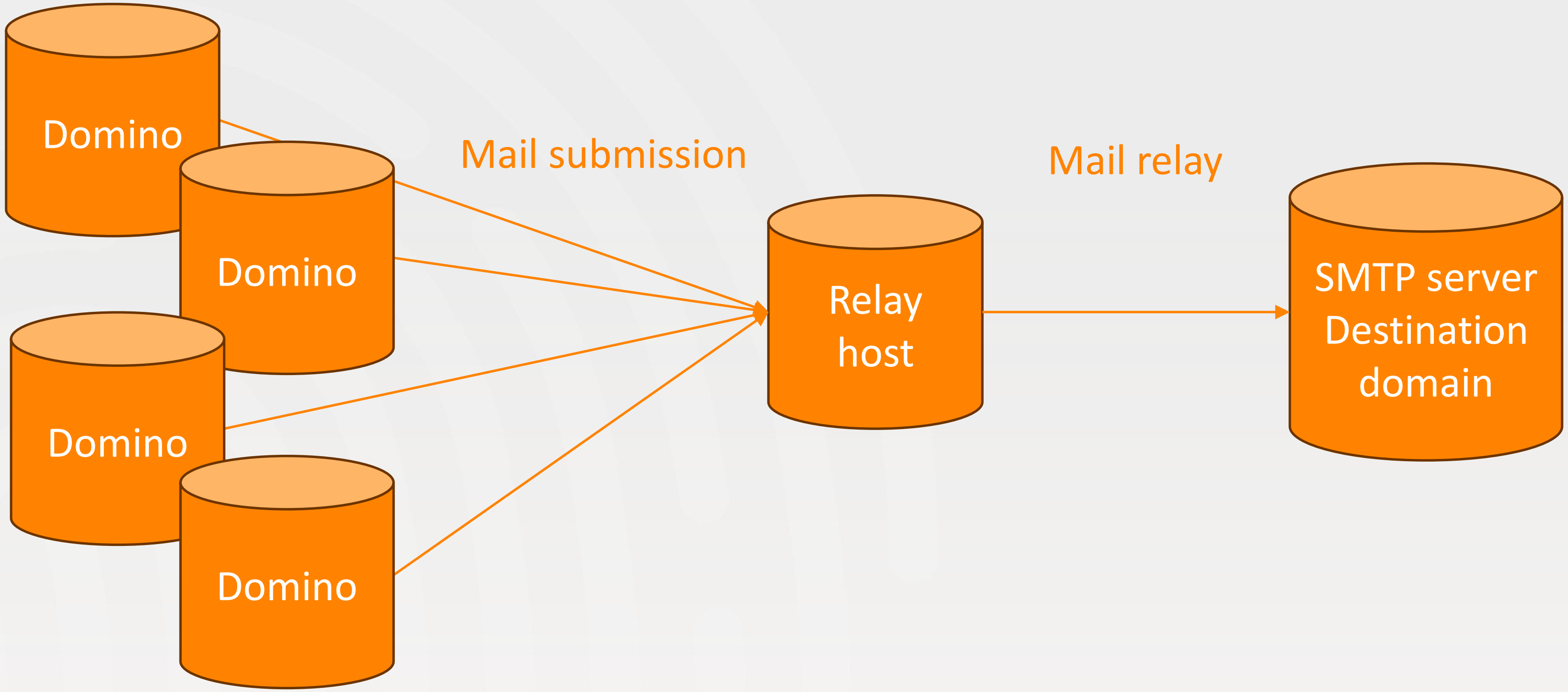
Basics | Security | Client Upgrade | Router/SMTP | MIME | NO

Basics | Restrictions and Controls... | Message Disclaimers | M

Router/SMTP Basics

Number of mailboxes:

SMTP used when sending messages outside of the local internet domain:	Enabled
SMTP allowed within the local internet domain:	Disabled
Servers within the local Notes domain are reachable via SMTP over TCPIP:	Always
Address lookup:	Fullname then Local Part
Exhaustive lookup:	Disabled
Relay host for messages leaving the local internet domain:	
Use authentication when sending messages to the relay host:	Disabled
Local Internet domain smart host:	
Smart host is used for all local internet domain recipients:	Disabled
Host name lookup:	Dynamic then local

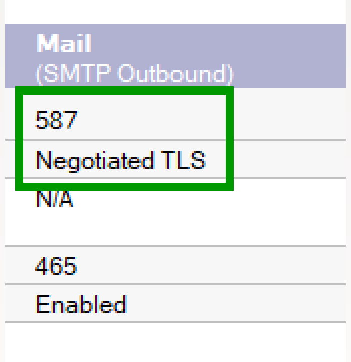


Scenario 2

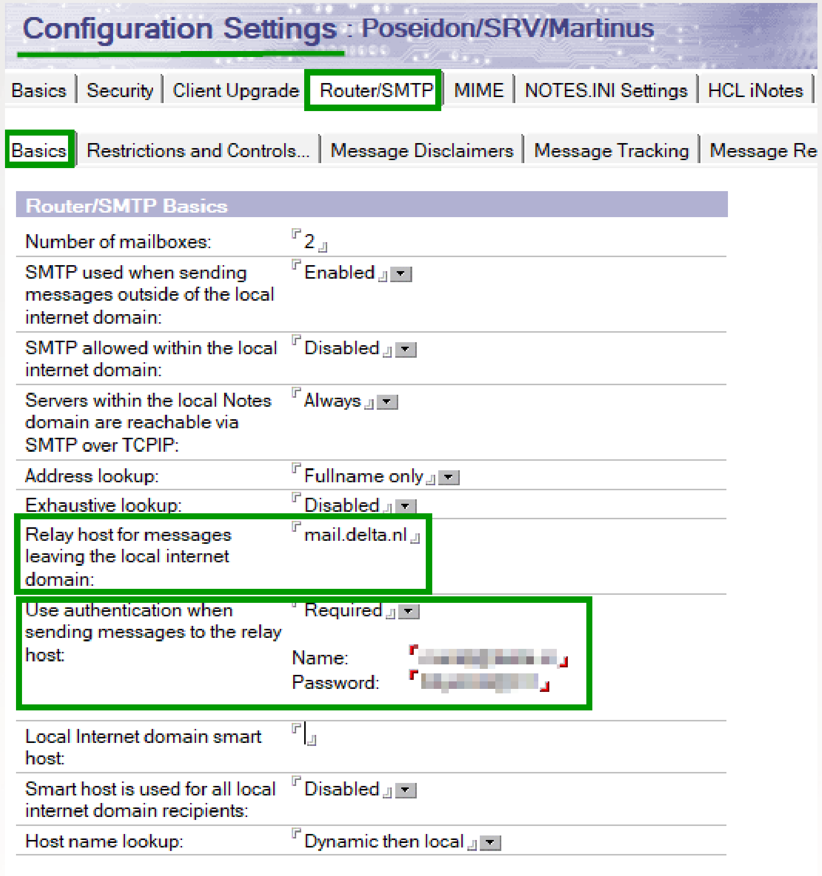
Servers are using a relay host to send mail to the internet

Scenario 2

- Set relay host in the configuration document
- Domino server now acts a mail client
- Depending on relay host, you might have to change the port to 587 in your server documents(s)



Mail (SMTP Outbound)
587
Negotiated TLS
N/A
465
Enabled

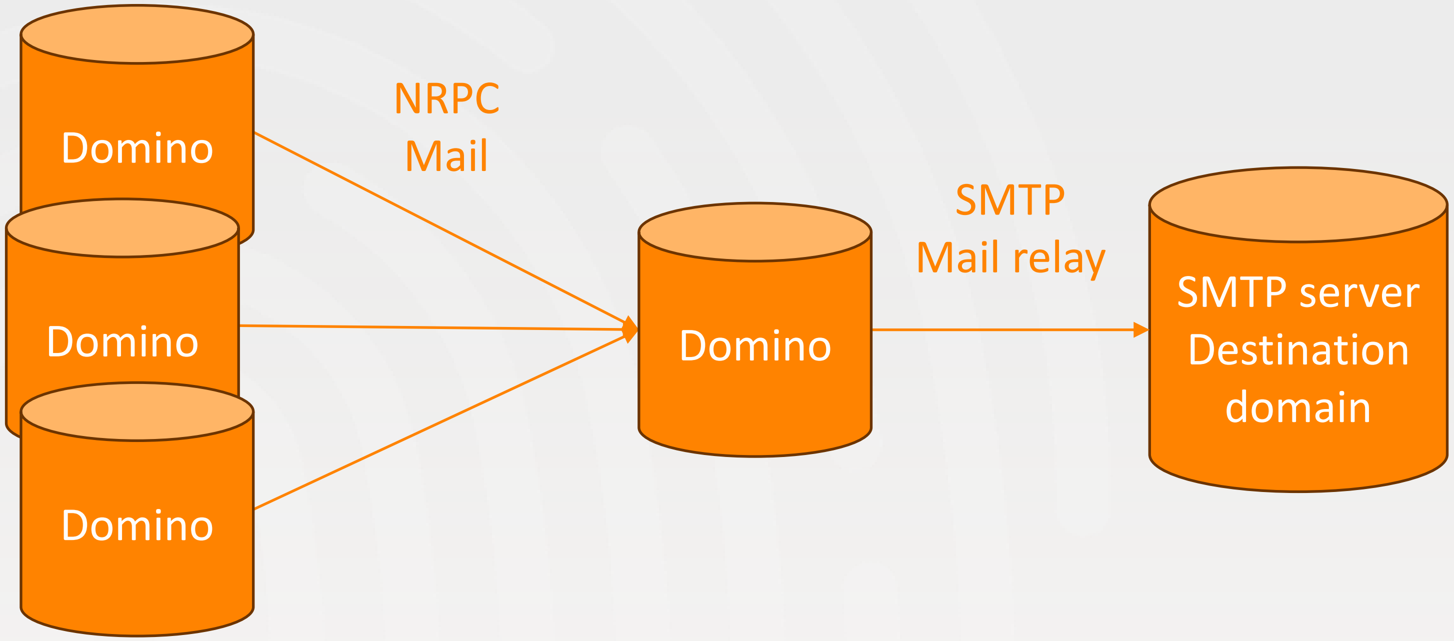


Configuration Settings : Poseidon/SRV/Martinus

Basics | Security | Client Upgrade | Router/SMTP | MIME | NOTES.INI Settings | HCL iNotes |
Basics | Restrictions and Controls... | Message Disclaimers | Message Tracking | Message Re

Router/SMTP Basics

Number of mailboxes:	2
SMTP used when sending messages outside of the local internet domain:	Enabled
SMTP allowed within the local internet domain:	Disabled
Servers within the local Notes domain are reachable via SMTP over TCPIP:	Always
Address lookup:	Fullname only
Exhaustive lookup:	Disabled
Relay host for messages leaving the local internet domain:	mail.delta.nl
Use authentication when sending messages to the relay host:	Required Name: [redacted] Password: [redacted]
Local Internet domain smart host:	
Smart host is used for all local internet domain recipients:	Disabled
Host name lookup:	Dynamic then local

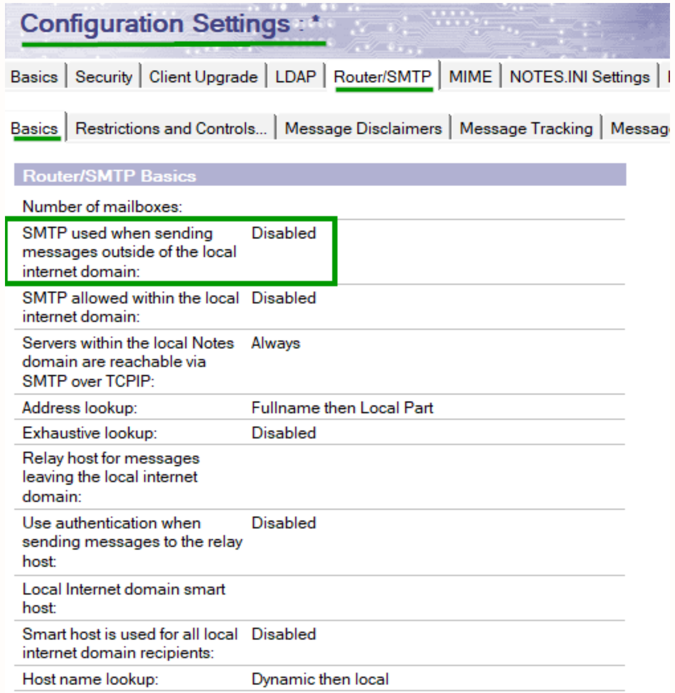


Scenario 3

Multiple servers, but only one can send mail to the internet

Scenario 3 – Configuration document

All servers

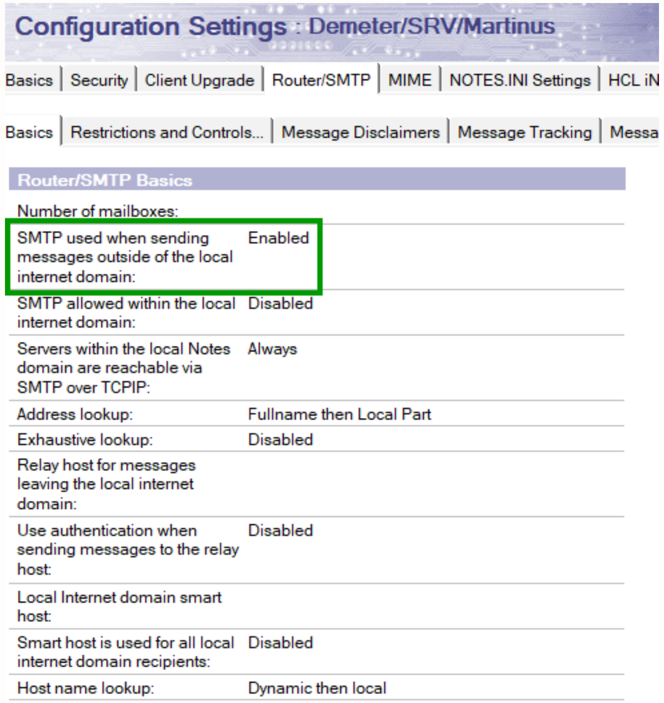

Basics | Security | Client Upgrade | LDAP | Router/SMTP | MIME | NOTES.INI Settings |
Basics | Restrictions and Controls... | Message Disclaimers | Message Tracking | Messag

Configuration Settings : *

Router/SMTP Basics

Number of mailboxes:	
SMTP used when sending messages outside of the local internet domain:	Disabled
SMTP allowed within the local internet domain:	Disabled
Servers within the local Notes domain are reachable via SMTP over TCPIP:	Always
Address lookup:	Fullname then Local Part
Exhaustive lookup:	Disabled
Relay host for messages leaving the local internet domain:	
Use authentication when sending messages to the relay host:	Disabled
Local Internet domain smart host:	
Smart host is used for all local internet domain recipients:	Disabled
Host name lookup:	Dynamic then local

Server sending mail to internet


Basics | Security | Client Upgrade | Router/SMTP | MIME | NOTES.INI Settings | HCL iN
Basics | Restrictions and Controls... | Message Disclaimers | Message Tracking | Messa

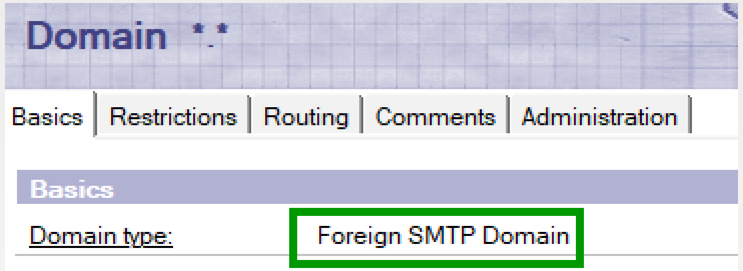
Configuration Settings : Demeter/SRV/Martinus

Router/SMTP Basics

Number of mailboxes:	
SMTP used when sending messages outside of the local internet domain:	Enabled
SMTP allowed within the local internet domain:	Disabled
Servers within the local Notes domain are reachable via SMTP over TCPIP:	Always
Address lookup:	Fullname then Local Part
Exhaustive lookup:	Disabled
Relay host for messages leaving the local internet domain:	
Use authentication when sending messages to the relay host:	Disabled
Local Internet domain smart host:	
Smart host is used for all local internet domain recipients:	Disabled
Host name lookup:	Dynamic then local

Scenario 3 – Foreign SMTP Domain document

- Create a Foreign SMTP Domain document

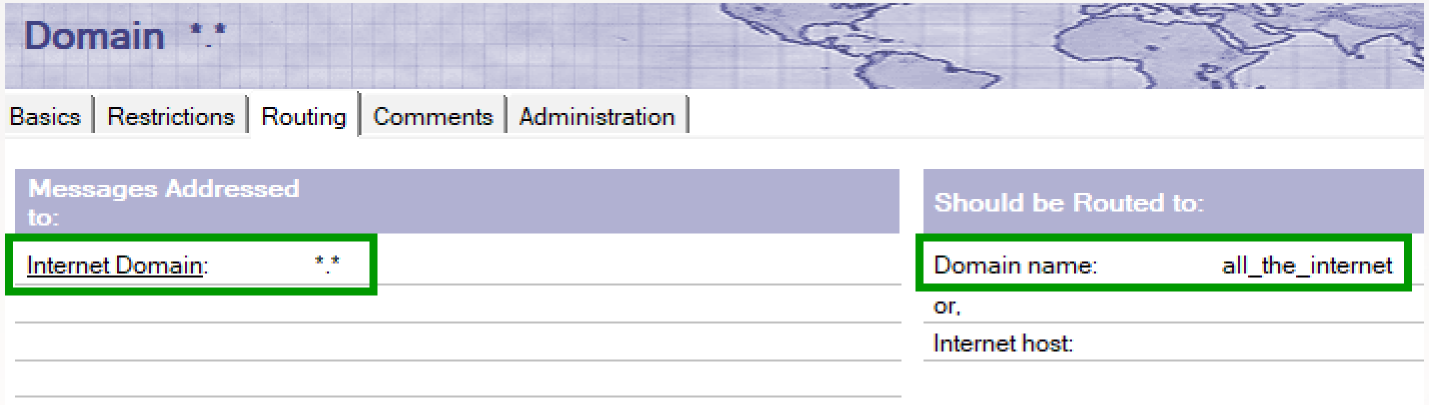


Domain *.*

Basics

Domain type: Foreign SMTP Domain

- All internet domains are routed to all_the_internet (custom label)



Domain *.*

Messages Addressed to:

Internet Domain: *.*

Should be Routed to:

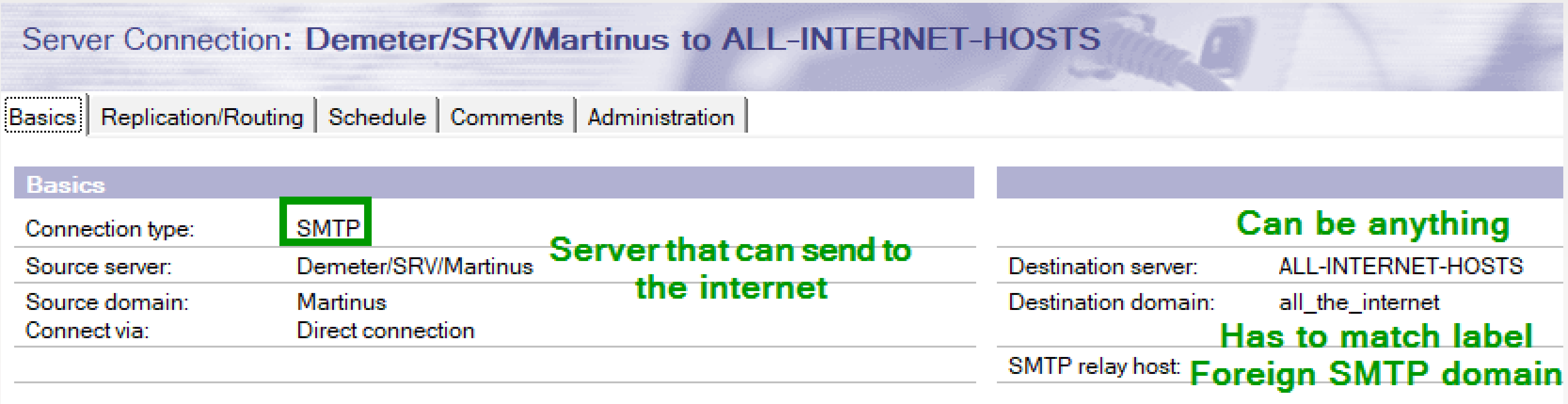
Domain name: all_the_internet

or,

Internet host:

Scenario 3 – SMTP Connection document

- Create an SMTP Connection document



Server Connection: Demeter/SRV/Martinus to ALL-INTERNET-HOSTS

Basics

Connection type:	SMTP		
Source server:	Demeter/SRV/Martinus	Destination server:	ALL-INTERNET-HOSTS
Source domain:	Martinus	Destination domain:	all_the_internet
Connect via:	Direct connection	SMTP relay host:	

Server that can send to the internet

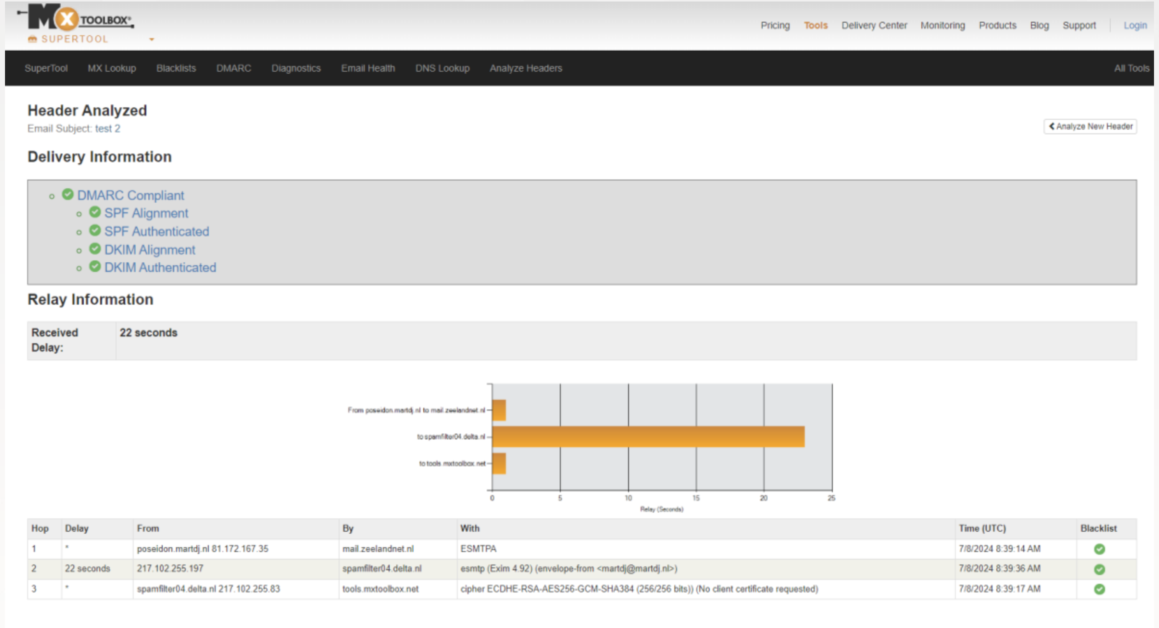
Can be anything

Has to match label

Foreign SMTP domain

Test your configuration

- Sent a mail to ping@tools.mxtoolbox.com
- Check your mail or go to https://mxtoolbox.com/deliverability/EmailHeaders.aspx and enter your email address



Header Analyzed

Email Subject: test 2

Delivery Information

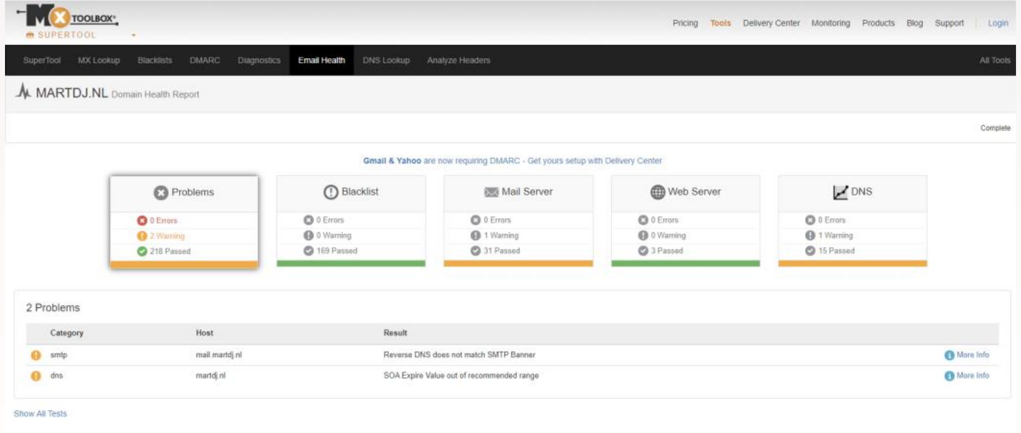
- ✓ DMARC Compliant
  - ✓ SPF Alignment
  - ✓ SPF Authenticated
  - ✓ DKIM Alignment
  - ✓ DKIM Authenticated

Relay Information

Received Delay:	**22 seconds**

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	poseidon.martdj.nl 81.172.167.35	mail.zeelandnet.nl	ESMTPA	7/8/2024 8:39:14 AM	✓
2	22 seconds	217.102.255.197	spamfilter04.delta.nl	esmtp (Exim 4.92) (envelope-from <martdj@martdj.nl>)	7/8/2024 8:39:36 AM	✓
3	*	spamfilter04.delta.nl 217.102.255.83	tools.mxtoolbox.net	cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits)) (No client certificate requested)	7/8/2024 8:39:17 AM	✓

- Check the Email health of your domain https://mxtoolbox.com/emailhealth



MARTDJ.NL Domain Health Report

Gmail & Yahoo are now requiring DMARC - Get yours setup with Delivery Center

Problems	Blacklist	Mail Server	Web Server	DNS
0 Errors	0 Errors	0 Errors	0 Errors	0 Errors
2 Warning	0 Warning	1 Warning	0 Warning	1 Warning
218 Passed	169 Passed	31 Passed	3 Passed	15 Passed

2 Problems

Category	Host	Result	
smtp	mail.martdj.nl	Reverse DNS does not match SMTP Banner	More Info
dns	martdj.nl	SOA Expire Value out of recommended range	More Info

Domino Inbound SMTP Configuration

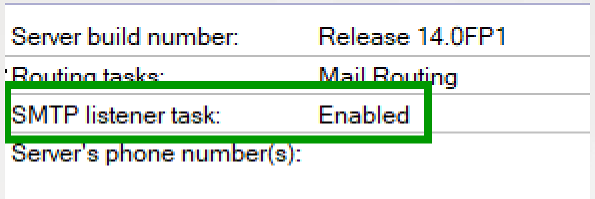
- Enable Inbound SMTP
- SMTP Inbound Site
- Inbound StartTLS
- Inbound Relay Control
- Inbound Recipient Check
- Sender’s domain
- Connecting Hostname
- Blacklists & Whitelists
- SPF & DKIM
- DMARC
- Spamgeek

Inbound SMTP implementation

Method	DNS of sender’s domain	Inbound mail server configuration
PTR Record	✓	✓
SPF	✓	✓
DKIM	✓	✓
DMARC	✓	✓
StartTLS	-	✓
Implicit TLS	-	✓

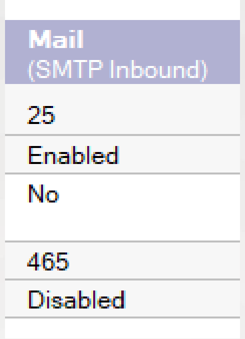
Enable Inbound SMTP

- Enable SMTP listener task server document – Basics

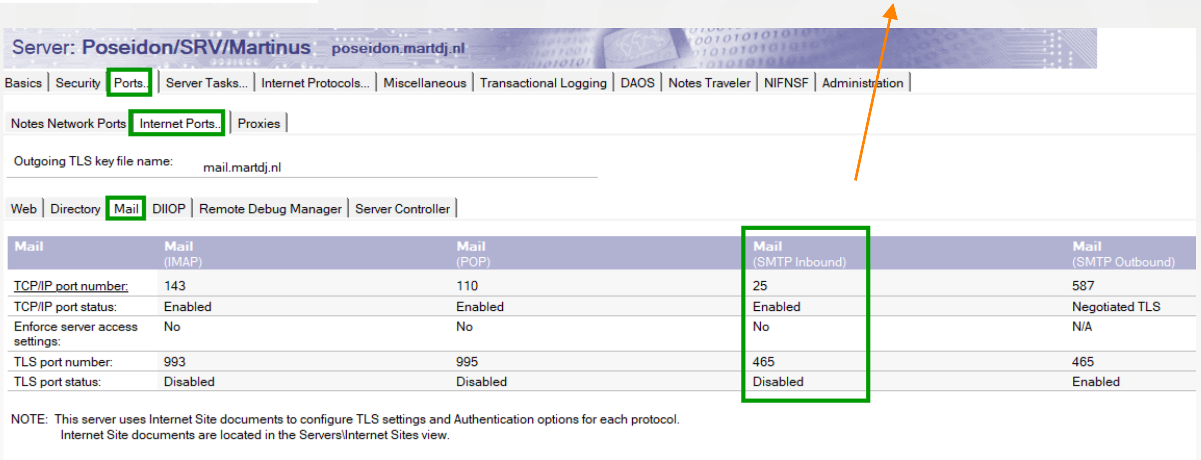


Server build number:	Release 14.0FP1
Routing tasks:	Mail Routing
SMTP listener task:	Enabled
Server's phone number(s):	

- SMTP Inbound port 25 enabled server documents – ports – mail (Port 465 only if Domino is accepting mail from other mail clients)



Mail (SMTP Inbound)
25
Enabled
No
465
Disabled



Server: Poseidon/SRV/Martinus poseidon.martdj.nl

Basics | Security | Ports.. | Server Tasks... | Internet Protocols... | Miscellaneous | Transactional Logging | DAOS | Notes Traveler | NIFNSF | Administration
Notes Network Ports | Internet Ports.. | Proxies
Web | Directory | Mail | DIIOP | Remote Debug Manager | Server Controller

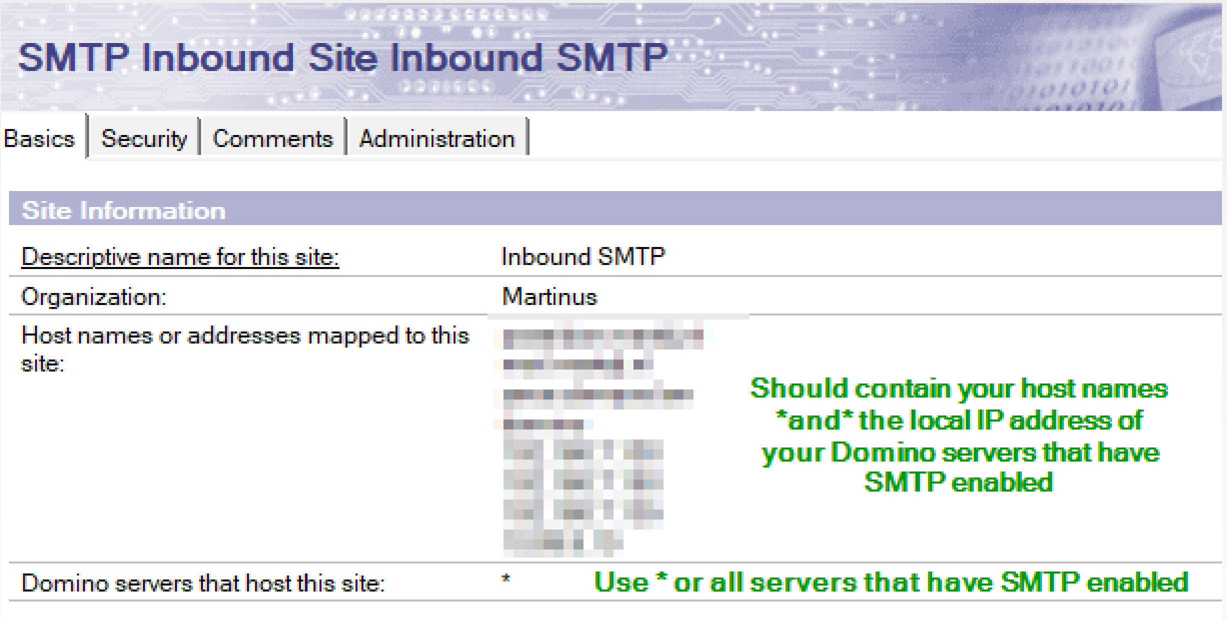
Outgoing TLS key file name: mail.martdj.nl

Mail	Mail (IMAP)	Mail (POP)	Mail (SMTP Inbound)	Mail (SMTP Outbound)
TCP/IP port number:	143	110	25	587
TCP/IP port status:	Enabled	Enabled	Enabled	Negotiated TLS
Enforce server access settings:	No	No	No	N/A
TLS port number:	993	995	465	465
TLS port status:	Disabled	Disabled	Disabled	Enabled

NOTE: This server uses Internet Site documents to configure TLS settings and Authentication options for each protocol.
Internet Site documents are located in the Servers\Internet Sites view.

SMTP Inbound Site

- If using Internet site documents, you must have an SMTP inbound internet site document



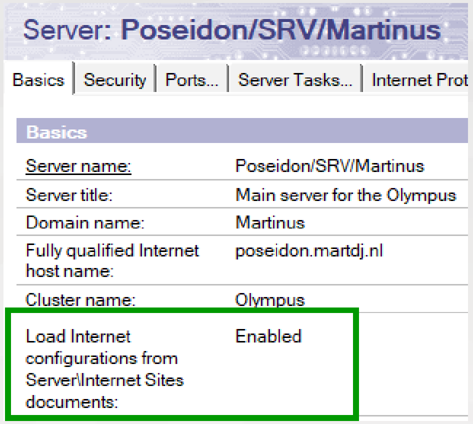
SMTP Inbound Site Inbound SMTP

Site Information

Descriptive name for this site:	Inbound SMTP
Organization:	Martinus
Host names or addresses mapped to this site:	[redacted]
Domino servers that host this site:	*

Should contain your host names *and* the local IP address of your Domino servers that have SMTP enabled

Use * or all servers that have SMTP enabled

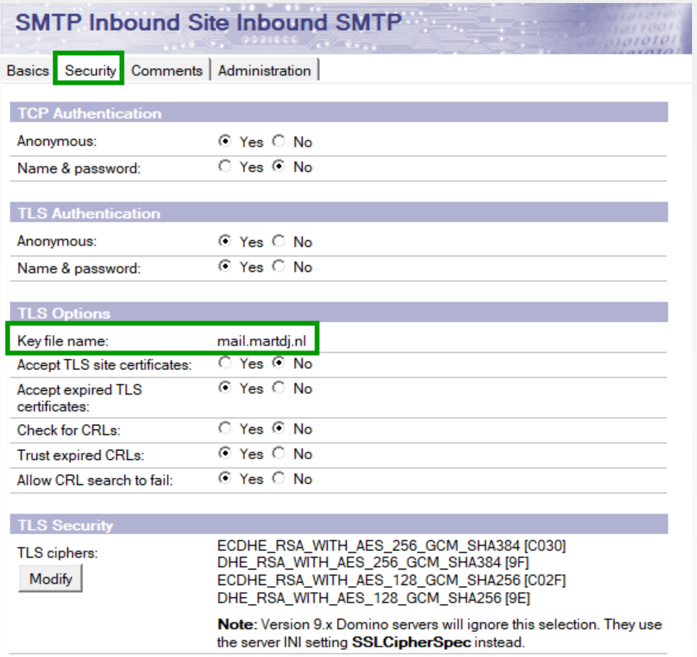


Server: Poseidon/SRV/Martinus

Basics | Security | Ports... | Server Tasks... | Internet Prot

Basics

Server name:	Poseidon/SRV/Martinus
Server title:	Main server for the Olympus
Domain name:	Martinus
Fully qualified Internet host name:	poseidon.martdj.nl
Cluster name:	Olympus
Load Internet configurations from Server\Internet Sites documents:	Enabled



SMTP Inbound Site Inbound SMTP

TCP Authentication

Anonymous:	● Yes ○ No
Name & password:	○ Yes ● No

TLS Authentication

Anonymous:	● Yes ○ No
Name & password:	● Yes ○ No

TLS Options

Key file name:	mail.martdj.nl
Accept TLS site certificates:	○ Yes ● No
Accept expired TLS certificates:	● Yes ○ No
Check for CRLs:	○ Yes ● No
Trust expired CRLs:	● Yes ○ No
Allow CRL search to fail:	● Yes ○ No

TLS Security

TLS ciphers: Modify	ECDHE_RSA_WITH_AES_256_GCM_SHA384 [C030] DHE_RSA_WITH_AES_256_GCM_SHA384 [9F] ECDHE_RSA_WITH_AES_128_GCM_SHA256 [C02F] DHE_RSA_WITH_AES_128_GCM_SHA256 [9E] **Note**: Version 9.x Domino servers will ignore this selection. They use the server INI setting **SSLCipherSpec** instead.

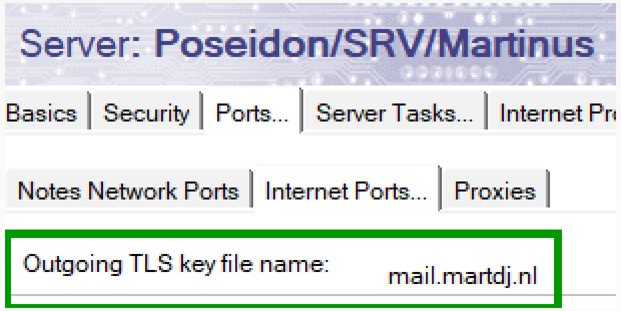
Enable inbound StartTLS

- Offers “negotiated TLS over port 25
- Needs a TLS certificate

▷ TLS Credentials used from CertStore based on keyfile tag in server document / internet site

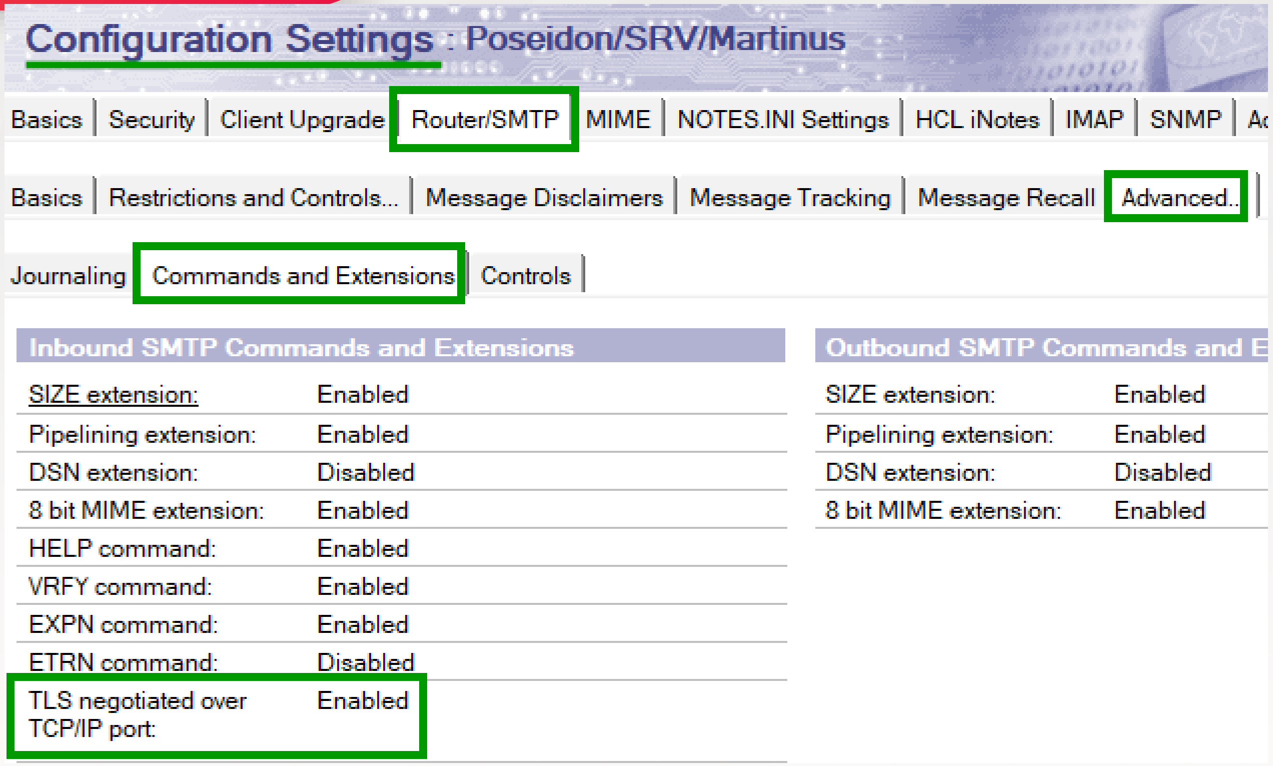
  ▷ Key file tag must match a keyfile name (e.g. keyfile.kyr) assigned to your server

  ▷ Key file tag can be also a FQDN



Server: Poseidon/SRV/Martinus

Outgoing TLS key file name:	mail.martdj.nl



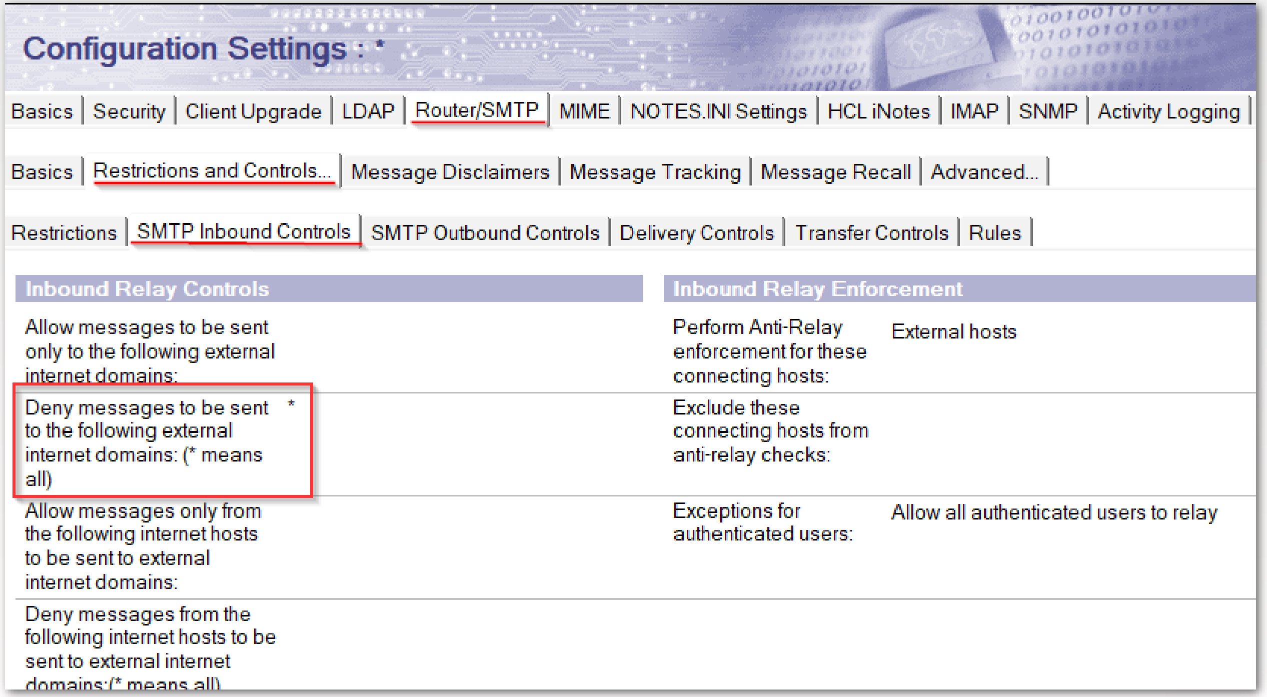
Configuration Settings : Poseidon/SRV/Martinus

Inbound SMTP Commands and Extensions	
SIZE extension:	Enabled
Pipelining extension:	Enabled
DSN extension:	Disabled
8 bit MIME extension:	Enabled
HELP command:	Enabled
VRFY command:	Enabled
EXPN command:	Enabled
ETRN command:	Disabled
TLS negotiated over TCP/IP port:	Enabled

Outbound SMTP Commands and E	
SIZE extension:	Enabled
Pipelining extension:	Enabled
DSN extension:	Disabled
8 bit MIME extension:	Enabled

Inbound Relay Control

- For external server ALWAYS ensure nobody can use your server as a “Relay Host”
- The single “ * “ in the field means nobody can relay

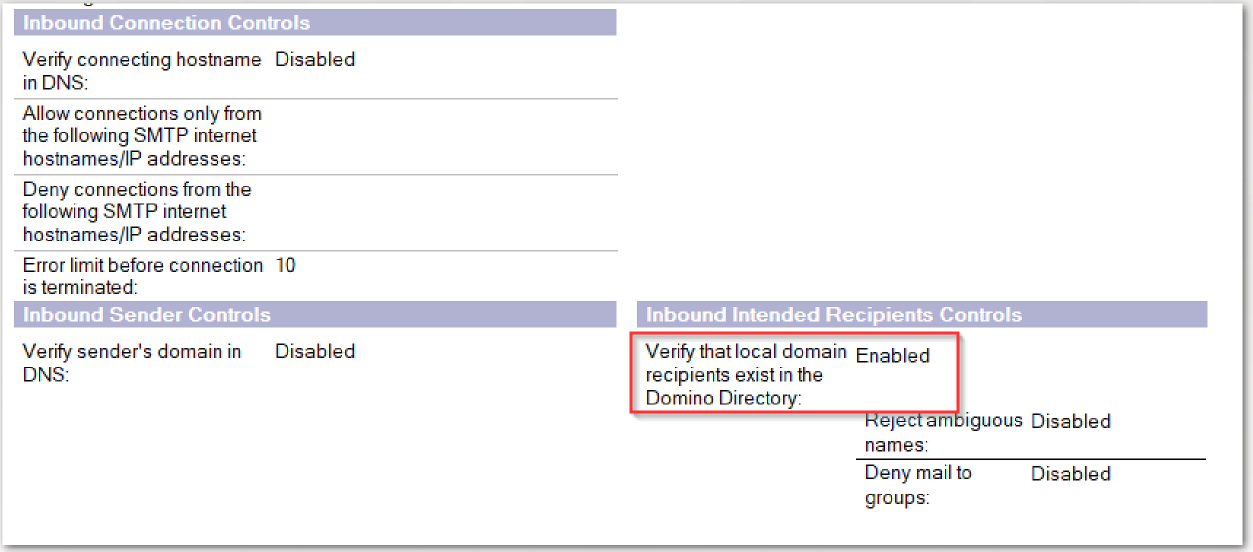

Basics | Security | Client Upgrade | LDAP | Router/SMTP | MIME | NOTES.INI Settings | HCL iNotes | IMAP | SNMP | Activity Logging |
Basics | Restrictions and Controls... | Message Disclaimers | Message Tracking | Message Recall | Advanced... |
Restrictions | SMTP Inbound Controls | SMTP Outbound Controls | Delivery Controls | Transfer Controls | Rules |

Configuration Settings : *

Inbound Relay Controls		Inbound Relay Enforcement	
Allow messages to be sent only to the following external internet domains:		Perform Anti-Relay enforcement for these connecting hosts:	External hosts
Deny messages to be sent to the following external internet domains: (* means all)	*	Exclude these connecting hosts from anti-relay checks:	
Allow messages only from the following internet hosts to be sent to external internet domains:		Exceptions for authenticated users:	Allow all authenticated users to relay
Deny messages from the following internet hosts to be sent to external internet domains:(* means all)			

Inbound Recipient Check

- Setting in same tab in config document further down in the form
- Denies all recipients not found in directory
- Recommendation: Enabled



Inbound Connection Controls

Verify connecting hostname in DNS:	Disabled
Allow connections only from the following SMTP internet hostnames/IP addresses:	
Deny connections from the following SMTP internet hostnames/IP addresses:	
Error limit before connection is terminated:	10

Inbound Sender Controls

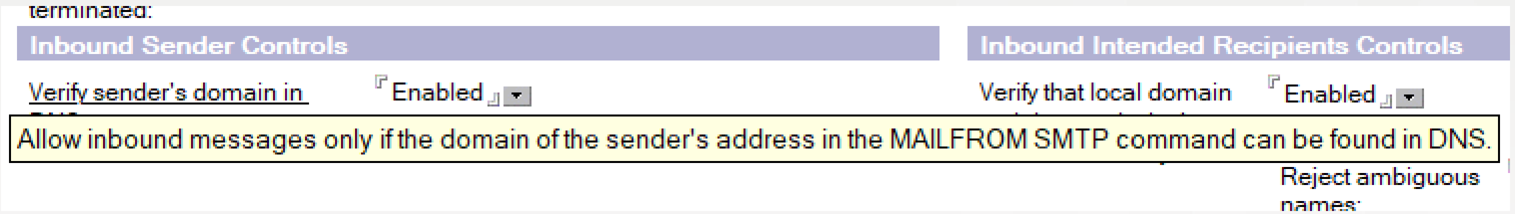
Verify sender's domain in DNS:	Disabled

Inbound Intended Recipients Controls

Verify that local domain recipients exist in the Domino Directory:	Enabled
Reject ambiguous names:	Disabled
Deny mail to groups:	Disabled

Sender’s domain

- Verify sender’s domain in DNS
  - Checks whether mail from domain exists in DNS
  - Recommendation: Martijn – Enabled, Daniel – Disabled



terminated:

Inbound Sender Controls

Verify sender's domain in — Enabled

Inbound Intended Recipients Controls

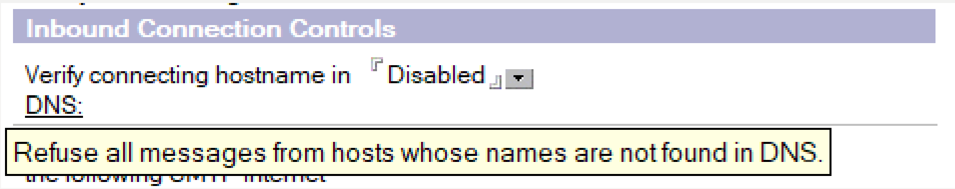
Verify that local domain — Enabled

Reject ambiguous names:

Allow inbound messages only if the domain of the sender's address in the MAILFROM SMTP command can be found in DNS.

Connecting hostname

- Verify connecting hostname in DNS
- Checks for a PTR record
- Strong recommendation: Disabled



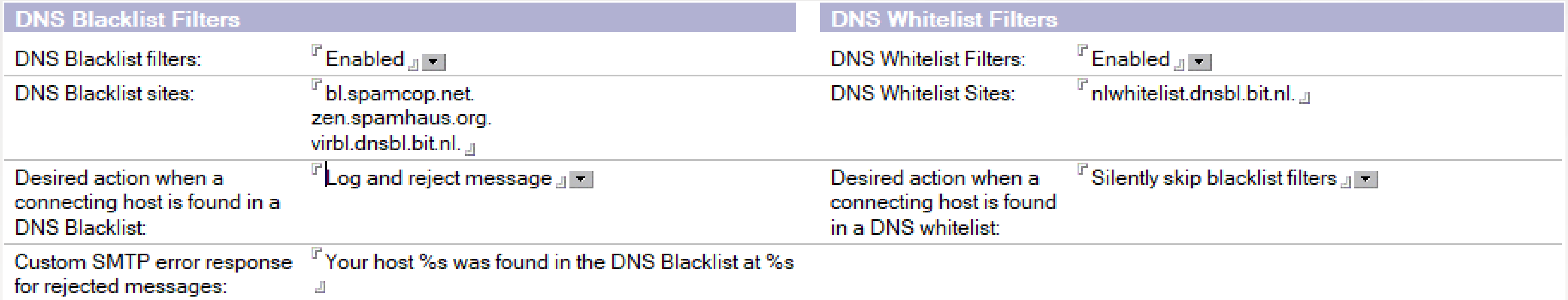
Inbound Connection Controls

Verify connecting hostname in DNS: Disabled

Refuse all messages from hosts whose names are not found in DNS.

Blacklists & Whitelists

- Blacklists / whitelists

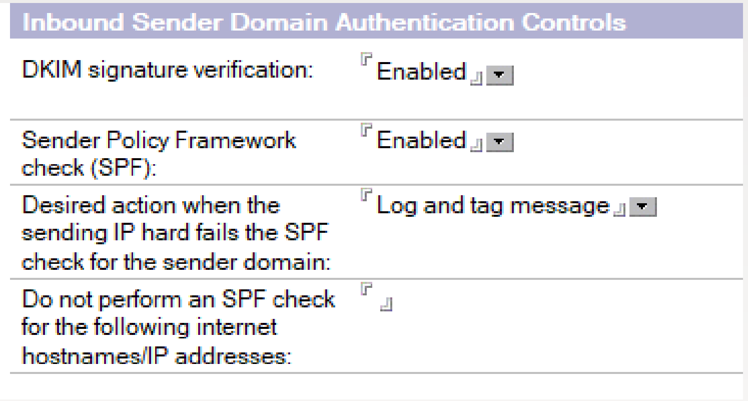


DNS Blacklist Filters		DNS Whitelist Filters	
DNS Blacklist filters:	Enabled	DNS Whitelist Filters:	Enabled
DNS Blacklist sites:	bl.spamcop.net. zen.spamhaus.org. virbl.dnsbl.bit.nl.	DNS Whitelist Sites:	nlwhitelist.dnsbl.bit.nl.
Desired action when a connecting host is found in a DNS Blacklist:	Log and reject message	Desired action when a connecting host is found in a DNS whitelist:	Silently skip blacklist filters
Custom SMTP error response for rejected messages:	Your host %s was found in the DNS Blacklist at %s		

  - Reasonably safe to log and reject
  - Log and tag, combined with a 3rd party tool / plugin would be better
  - But many 3rd party tools do the blacklist check themselves

SPF & DKIM

- Inbound Sender Domain Authentication Controls



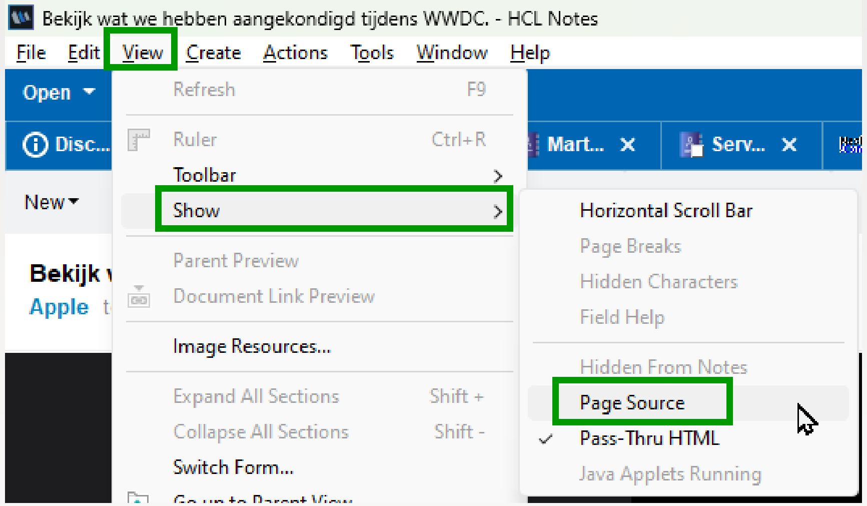
Inbound Sender Domain Authentication Controls

DKIM signature verification:	Enabled
Sender Policy Framework check (SPF):	Enabled
Desired action when the sending IP hard fails the SPF check for the sender domain:	Log and tag message
Do not perform an SPF check for the following internet hostnames/IP addresses:	

  - Too dangerous to Log and reject
  - “Log and tag message” adds 2 fields to an incoming mail
    - DKIM_Signature
    - Received_SPF
  - Can be used in mail rules
  - Or 3rd party plugins…

See SPF & DKIM results in header

- From an email: View – Show – Page Source



- Authentication-Results: martdj.nl 1; **spf=pass** smtp.mailfrom=n_i_bounces@insideapple.apple.com (sender IP 17.32.227.198); **dkim=pass** header.s=insideapple0517 header.d=insideapple.apple.com

DMARC

- We hope…
- You can still vote: https://domino-ideas.hcltechsw.com/ideas/IDEAMLCT-I-6

All Domino checks are binary…

- Modern anti-spam systems use a reputational score based on all these previous parameters
- We currently can’t do that in Domino

Introducing SpamGeek

- SMTP protocol Extension Manager created by Daniel Nashed
- Tool and basic support is free. Complex questions or scenarios are consulting
- Adds flexible anti-spam features to Domino
- Good for small environments and offers a lot of tracing

SMTP Debug parameters

- **SMTPDebug**

  This parameter can be set to capture inbound SMTP protocol conversations. This is for all messages received by the SMTP listener from all clients and servers via the SMTP protocol.
  1 - Enable minimal logging of the SMTP listener
  2 - Enable information logging of data sent and received along with some additional debugging information. This setting indicates commands and responses being received/sent along with the number of bytes being transmitted. However, it does not include the text that is transmitted.
  3 - Enable verbose logging of data sent and received. Along with the information recorded at setting 2, this level shows the actual text received/sent via SMTP. Note that this does not include the text body of messages.
  4 - This is the most verbose setting.

- **SMTPDebugIO Description**: Enables the logging of all data received by the SMTP listener task:

- 0 - No logging
  1 - Number of bytes sent and received during the SMTP conversation
  3 - Logs all data received by the SMTP task
  4 - RFC822 data (message data)

- **Syntax:** SMTPDebugIO=*value*
- **Caution:** Use SMTPDebugIO only when necessary and disable it again as soon as possible. It can cause the log file to grow very large, and logs the contents of received messages.
- **Applies to:** SMTP servers
- **Default:** 0
- **UI equivalent:** None

Useful Resources

- https://blog.martdj.nl
  Martijn's blog
- https://blog.nashcom.de
  Daniel's blog
- https://mxtoolbox.com
  Check your configuration and whether your server is listed on blacklists
- https://talosintelligence.com/
  Daniels tip to check your reputational score
- https://mailtrap.io/blog/smtp-commands-and-responses/
  Useful site to understand return codes in an SMTP communication

Questions?