

ESET Tech Center

Knowledgebase > Best Practices > Best practice policies voor nieuwe installaties - Mail Security for Microsoft Exchange Server

Best practice policies voor nieuwe installaties - Mail Security for Microsoft Exchange Server

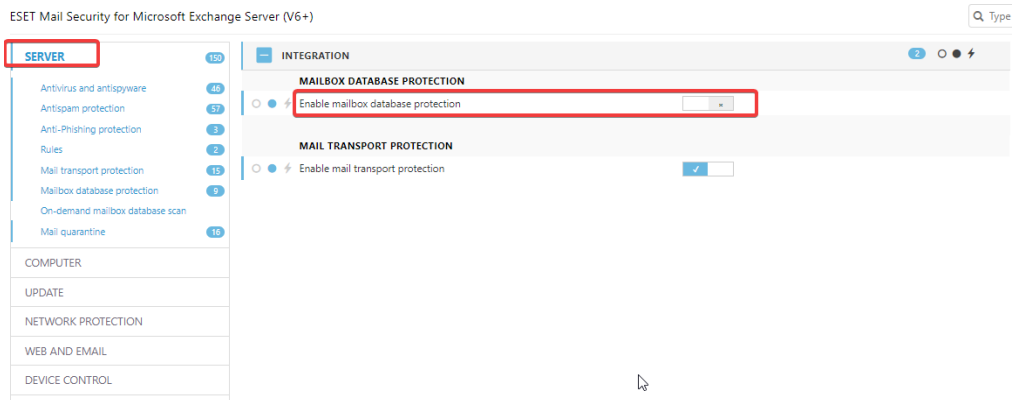
Danny | ESET Nederland - 2023-04-03 - Comments (0) - Best Practices

In dit artikel bespreken we de best practices voor Mail Security for Microsoft Exchange Server.

Veel instellingen komen overeen met die van het Endpoint Security en/of Server Security product en we benoemen daarom enkel de aanpassingen en/of bijzonderheden ten opzichte van deze producten.

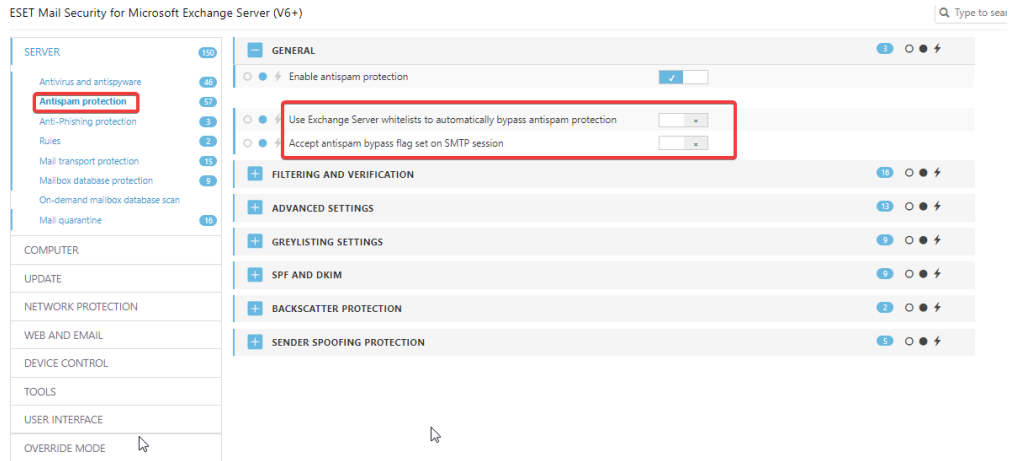
SERVER:

- Schakel Mailbox Database Protection uit. Deze functie is enkel beschikbaar op EOL versies van Microsoft Exchange (https://help.eset.com/emsx/10.0/en-US/features_roles.html). Het scannen van mailboxen op nieuwere versies kan middels een On-Demand database scan.

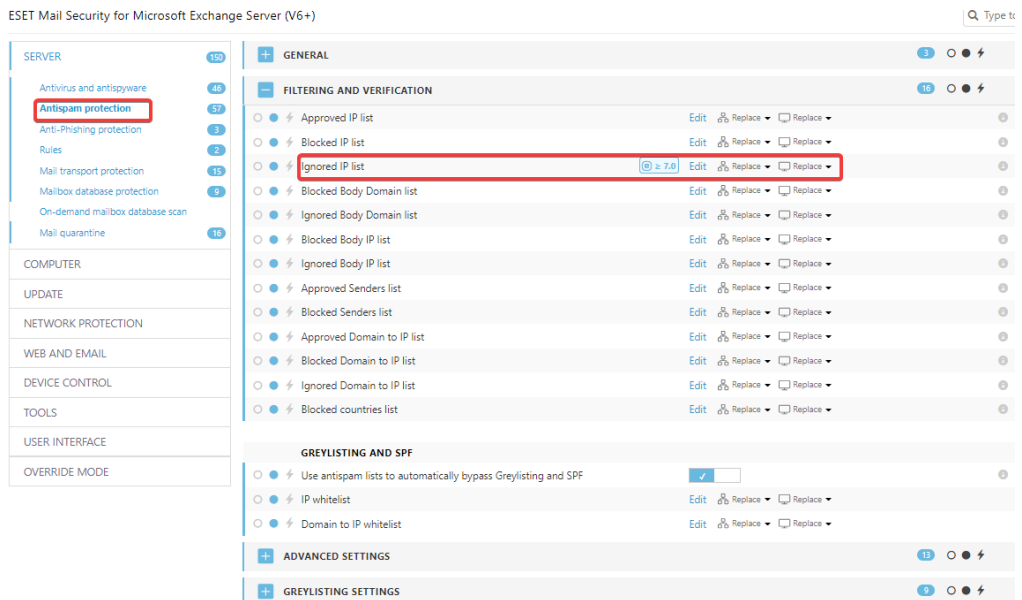


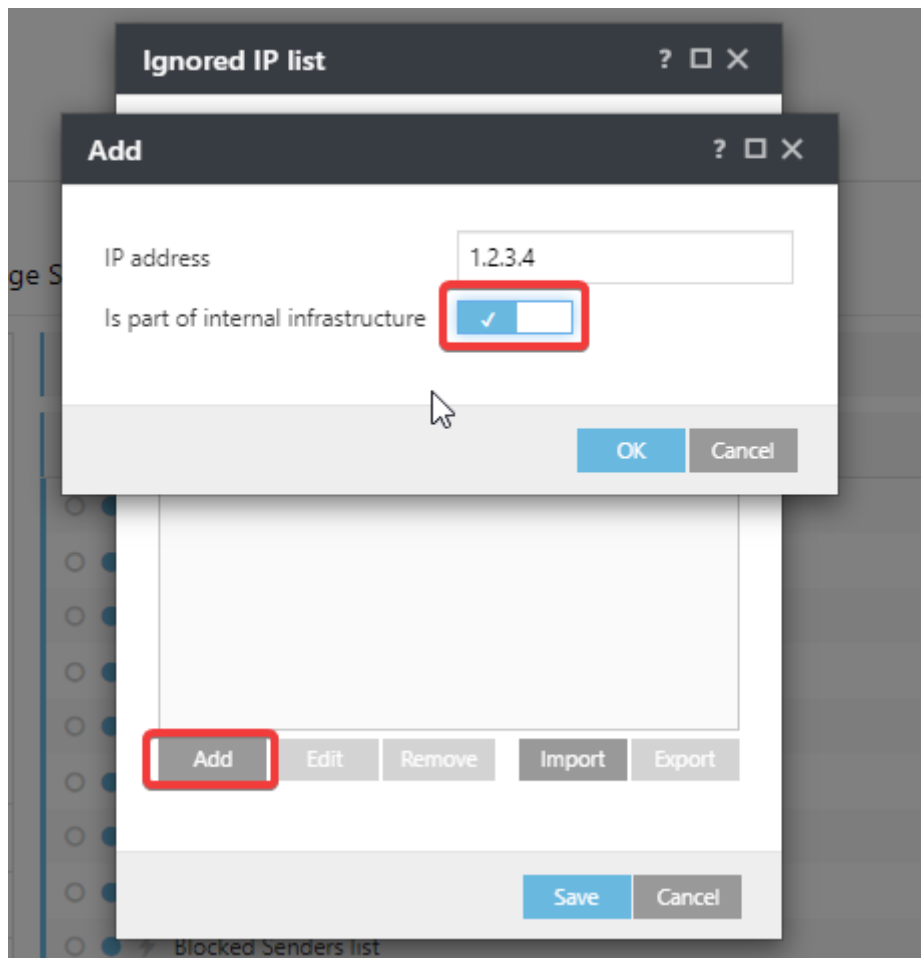
ANTISPAM PROTECTION:

- Schakel onderstaande functionaliteiten uit om ongewenste whitelisting vanuit Exchange whitelists en Bypass flags te voorkomen.

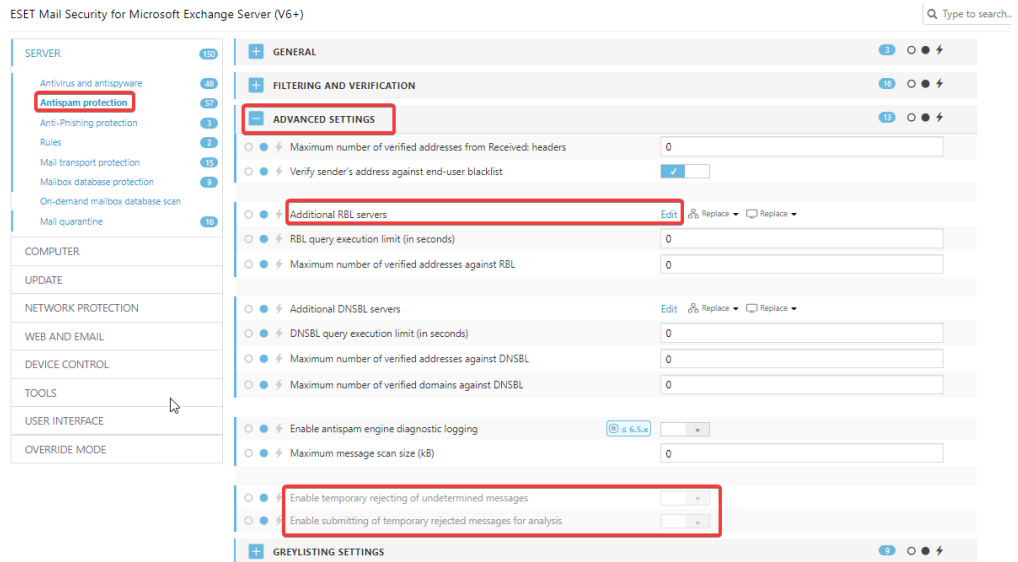


- Maak gebruik van de Ignore IP list om eigen infrastructuur en andere antispam oplossingen in de mailflow uit te zonderen. Vergeet ook niet om een vinkje te zetten wanneer het interne infrastructuur betreft.

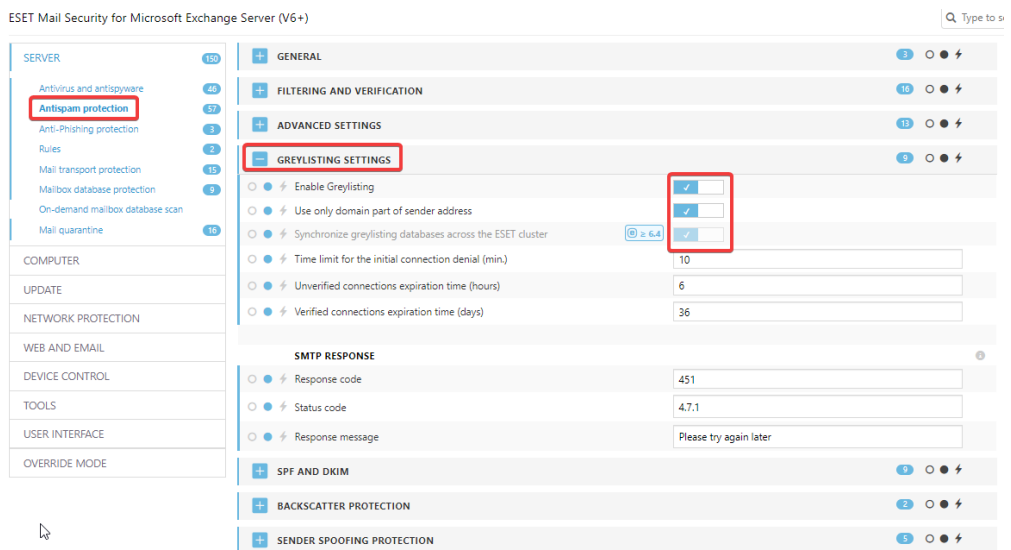




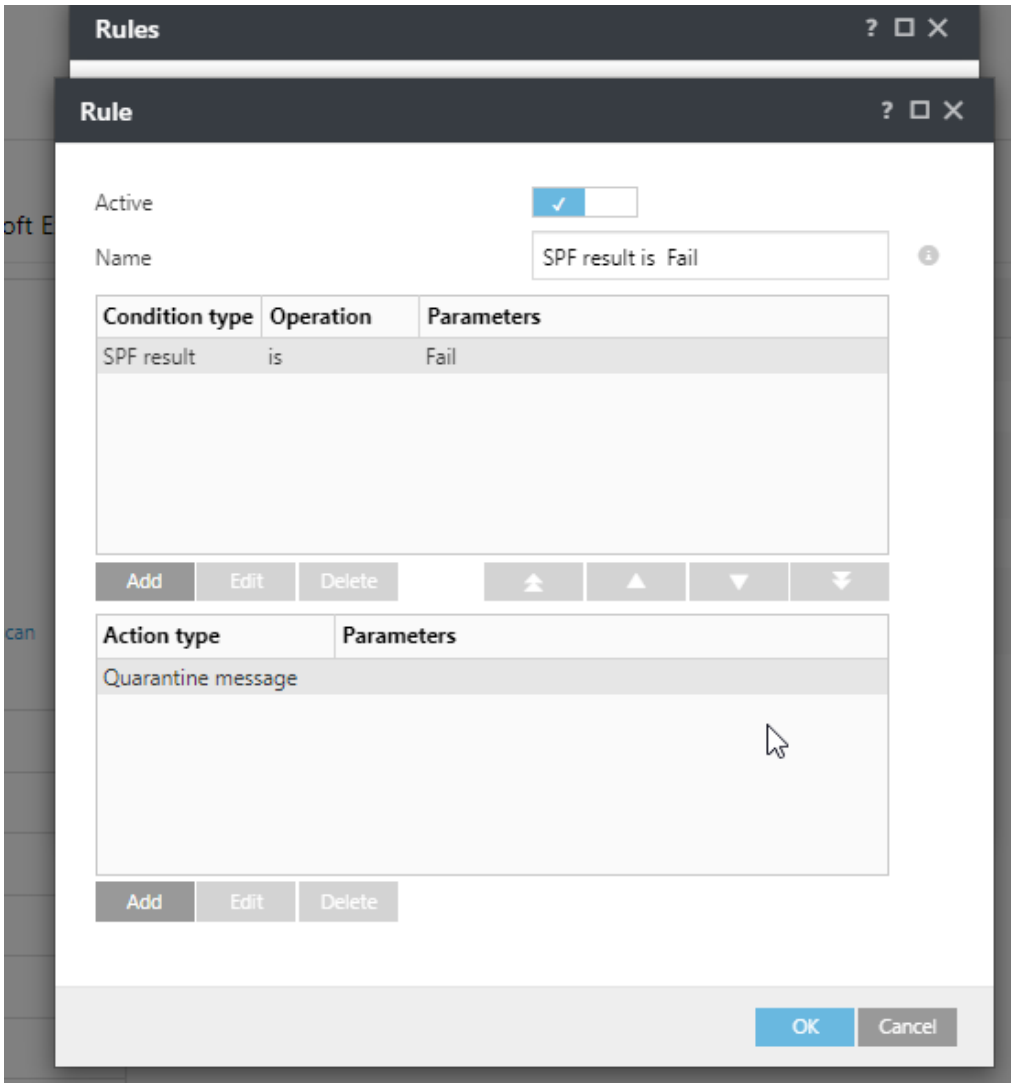
- Het is mogelijk om additionele RBL servers toe te voegen welke kunnen worden gebruikt voor het classificeren van mails.
- Wanneer het op inhoud en reputatie niet direct mogelijk is een waardeoordeel over een e-mail te geven of deze spam is of niet, kan het product worden ingesteld om dit soort berichten tijdelijk te blokkeren.

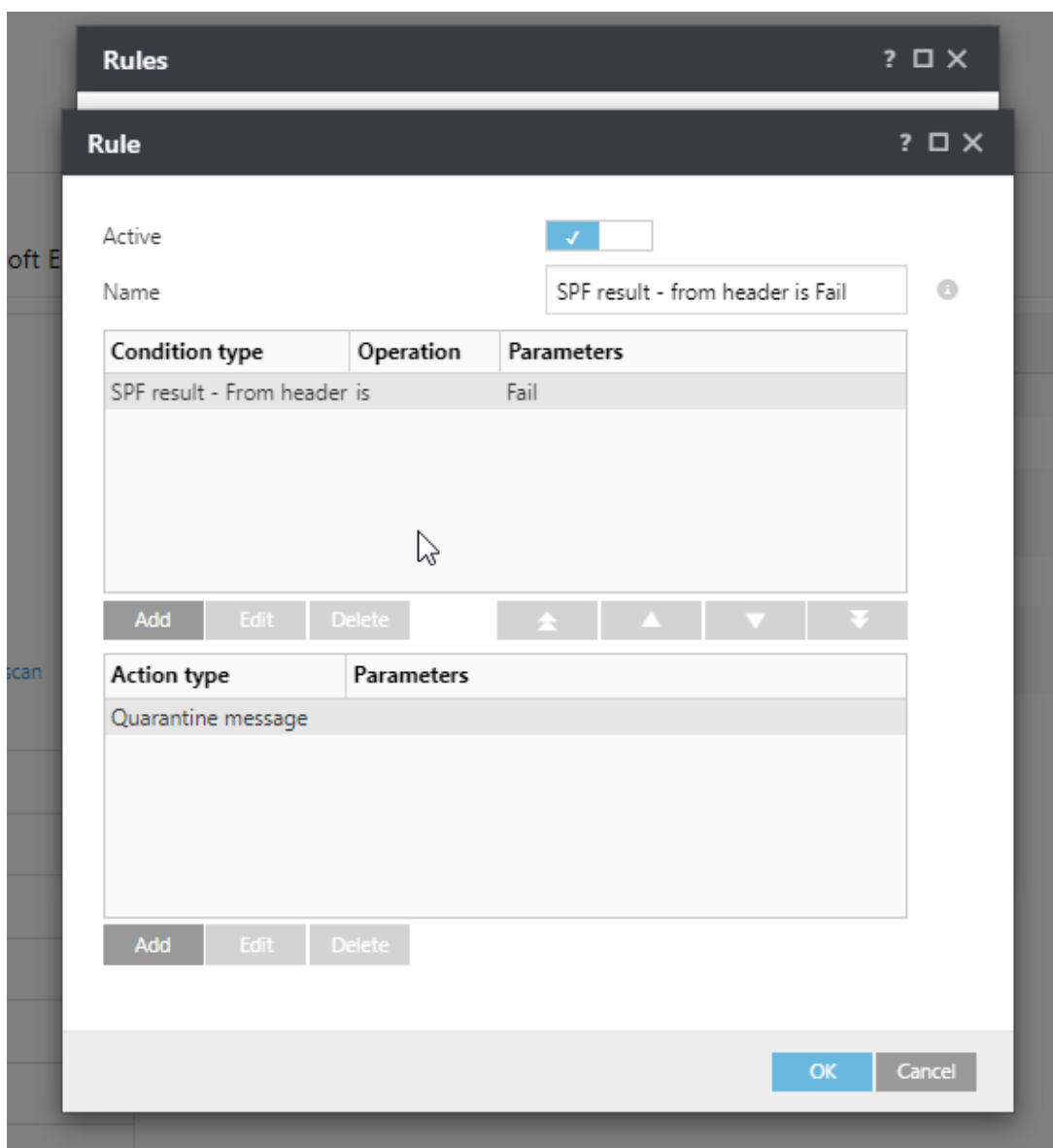


- Greylisting staat standaard uitgeschakeld, maar ons advies is om dit in te schakelen. Let op dat dit in eerste instantie een vertraging van e-mailbezorging kan zorgen. Meer informatie over Greylisting is te vinden op de volgende pagina: https://help.eset.com/emsx/10.0/en-US/idh_config_mailserver_greylisting.html



- SPF en DKIM kunnen worden gebruikt in rules om te reageren op resultaten van deze controles.





- Schakel "Use FROM: Header if MAIL FROM is empty" in en wanneer Greylisting is ingeschakeld ook de onderstaande settings.

ESET Mail Security for Microsoft Exchange Server (V6+)

SERVER 150

- Antivirus and antispamware 46
- Antispam protection 57**
- Anti-Phishing protection 3
- Rules 2
- Mail transport protection 15
- Mailbox database protection 9
- On-demand mailbox database scan
- Mail quarantine 16

COMPUTER

UPDATE

NETWORK PROTECTION

WEB AND EMAIL

DEVICE CONTROL

TOOLS

USER INTERFACE

OVERRIDE MODE

GENERAL 3

FILTERING AND VERIFICATION 16

ADVANCED SETTINGS 13

GREYLISTING SETTINGS 9

SPF AND DKIM 9

- Auto-detect DNS servers
- DNS server IP address
- DNS query timeout (seconds)
- Automatically reject messages if SPF check fails
- Use From: header if MAIL FROM is empty
- Automatically bypass Greylisting if SPF check passes

SMTP REJECT RESPONSE

- Response code 550
- Status code 5.7.1
- Response message SPF check failed

BACKSCATTER PROTECTION 2

SENDER SPOOFING PROTECTION 5

- Wanneer er sprake is van veel ongewenste/niet legitieme NDRs kan Backscatter protection worden ingeschakeld.

ESET Mail Security for Microsoft Exchange Server (V6+)

SERVER 150

- Antivirus and antispamware 46
- Antispam protection 57**
- Anti-Phishing protection 3
- Rules 2
- Mail transport protection 15
- Mailbox database protection 9
- On-demand mailbox database scan
- Mail quarantine 16

COMPUTER

UPDATE

NETWORK PROTECTION

WEB AND EMAIL

DEVICE CONTROL

TOOLS

USER INTERFACE

OVERRIDE MODE

GENERAL 3

FILTERING AND VERIFICATION 16

ADVANCED SETTINGS 13

GREYLISTING SETTINGS 9

SPF AND DKIM 9

BACKSCATTER PROTECTION 2

- Enable NDR check
- Automatically drop NDR messages if check fails
- Signature seed

SENDER SPOOFING PROTECTION 5

- Schakel Sender Proof Protection in en verander onderstaande settings.

ESET Mail Security for Microsoft Exchange Server (V6+)

SERVER 150

- Antivirus and antispamware 46
- Antispam protection 57**
- Anti-Phishing protection 3
- Rules 2
- Mail transport protection 15
- Mailbox database protection 9
- On-demand mailbox database scan
- Mail quarantine 16

COMPUTER

UPDATE

NETWORK PROTECTION

WEB AND EMAIL

DEVICE CONTROL

TOOLS

USER INTERFACE

OVERRIDE MODE

GENERAL 3

FILTERING AND VERIFICATION 16

ADVANCED SETTINGS 13

GREYLISTING SETTINGS 9

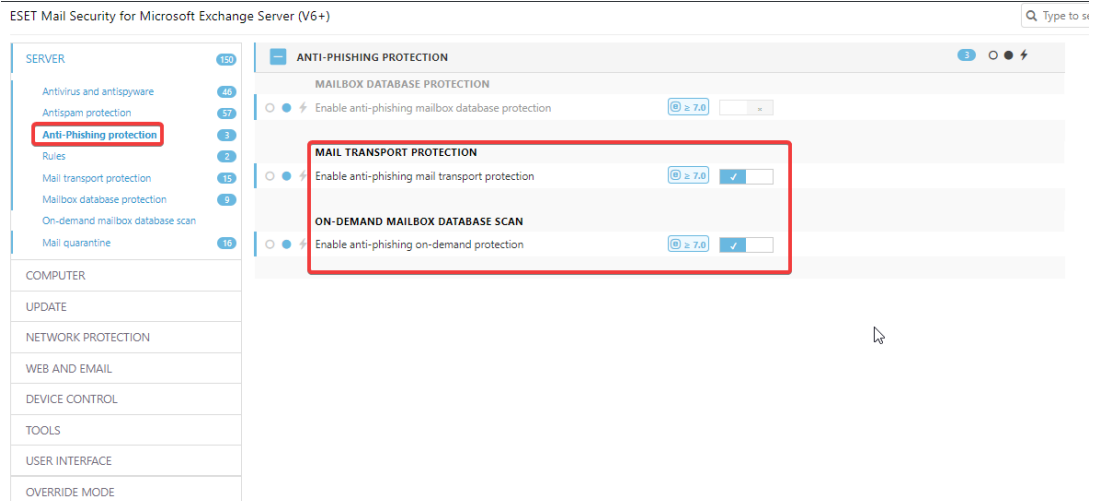
SPF AND DKIM 9

BACKSCATTER PROTECTION 2

SENDER SPOOFING PROTECTION 5

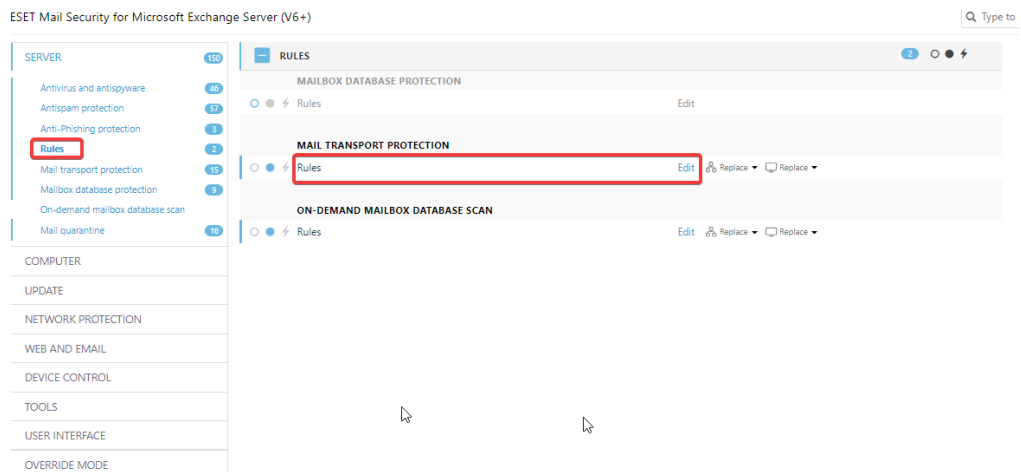
- Enable sender spoofing protection
- Enable incoming emails with my own domain in the sender's address Only when they pass the SPF check
- Automatically load my own domains from the Accepted domains list
- List of my own domains Edit Replace Replace
- List of my own IP addresses Edit Replace Replace

ANTI-PHISHING PROTECTION:



RULES:

- Een krachtig onderdeel binnen Mail Security zijn rules.



- Rules kunnen worden gebruikt voor een groot aantal functies, hieronder een voorbeeld hoe mails welke falen op SPF/DMARC/DKIM controles niet verloren gaan, maar juist in quarantaine worden geplaatst.

Rule ? □ ×

Active

Name ⓘ

Condition type	Operation	Parameters
SPF result	is	Fail

Add Edit Delete ↑ ▲ ▼ ↓

Action type	Parameters
Quarantine message	

Add Edit Delete

OK Cancel

Rule ? □ ×

Active

Name ⓘ

Condition type	Operation	Parameters
SPF result - From header is		Fail

Add Edit Delete ↑ ▲ ▼ ↓

Action type	Parameters
Quarantine message	

Add Edit Delete

OK Cancel

Rule



Active

Name ⓘ

Condition type	Operation	Parameters
DKIM result	is	Failed

Action type	Parameters
Quarantine message	

Rule ? □ ×

Active

Name DMARC result is failed ⓘ

Condition type	Operation	Parameters
DMARC result	is	Failed

Add Edit Delete ↑ ▲ ▼ ↓

Action type	Parameters
Quarantine message	

Add Edit Delete

OK Cancel

MAIL TRANSPORT PROTECTION:

ESET Mail Security for Microsoft Exchange Server (V6+) Type to search...

SERVER 150

- Antivirus and antispware 46
- Antispam protection 57
- Anti-Phishing protection 3
- Rules 2
- Mail transport protection 15**
- Mailbox database protection 9
- On-demand mailbox database scan
- Mail quarantine 16

COMPUTER

UPDATE

NETWORK PROTECTION

WEB AND EMAIL

DEVICE CONTROL

TOOLS

USER INTERFACE

OVERRIDE MODE

MAIL TRANSPORT PROTECTION 15

- Action to take if cleaning not possible Quarantine message
- Action to take on phishing message Quarantine message
- Action to take on spam message Quarantine message
- Action to take on messages with a spoofed domain Quarantine message

SMTP REJECT RESPONSE

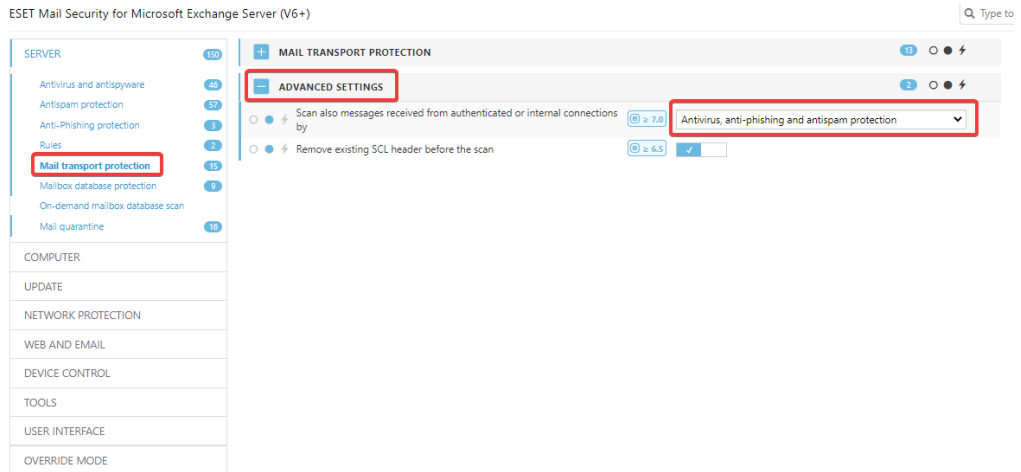
- Response code 554
- Status code 5.6.0
- Response message Invalid content

- Write scan results to message headers
- Add notification to the body of scanned messages Append to infected messages only

- Modify subject [found threat %VIRUSNAME%]
- Template added to the subject of infected messages [SPAM]
- Template added to the subject of spam messages [PHISH]

ADVANCED SETTINGS 2

- Schakel onder Advanced Settings ook het scannen van interne connecties in.

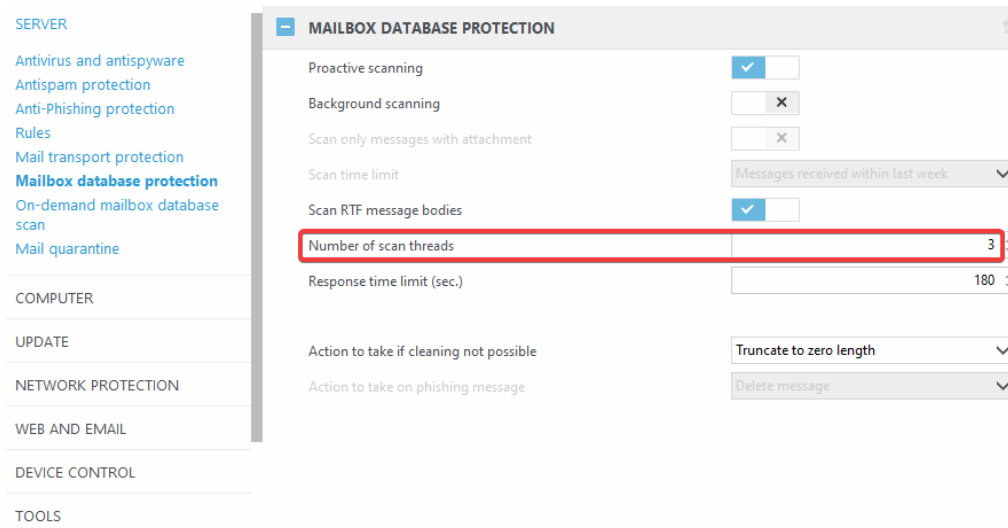


MAILBOX DATABASE PROTECTION:

- Deze functie is enkel beschikbaar in oude (EOL) versies van Exchange Server.

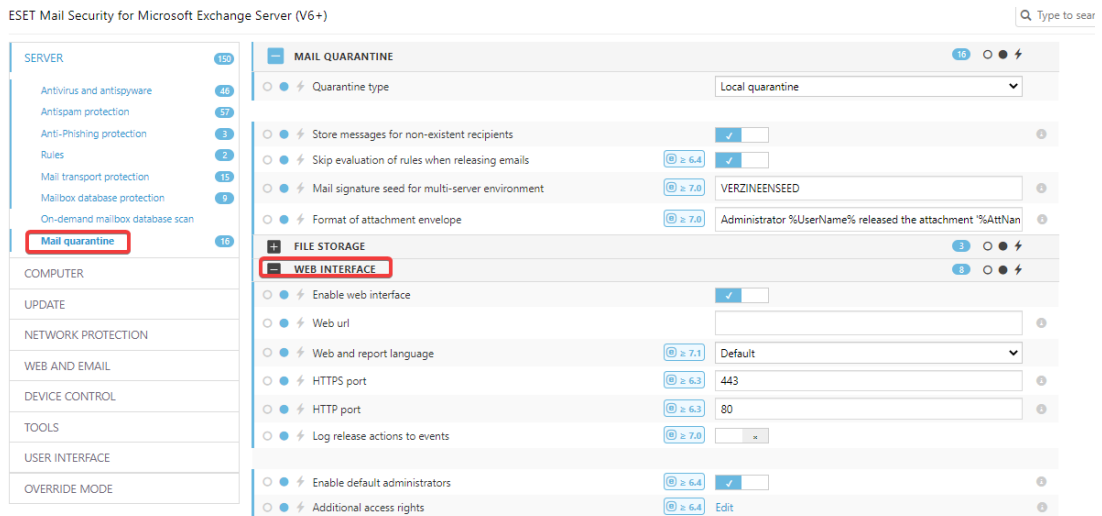
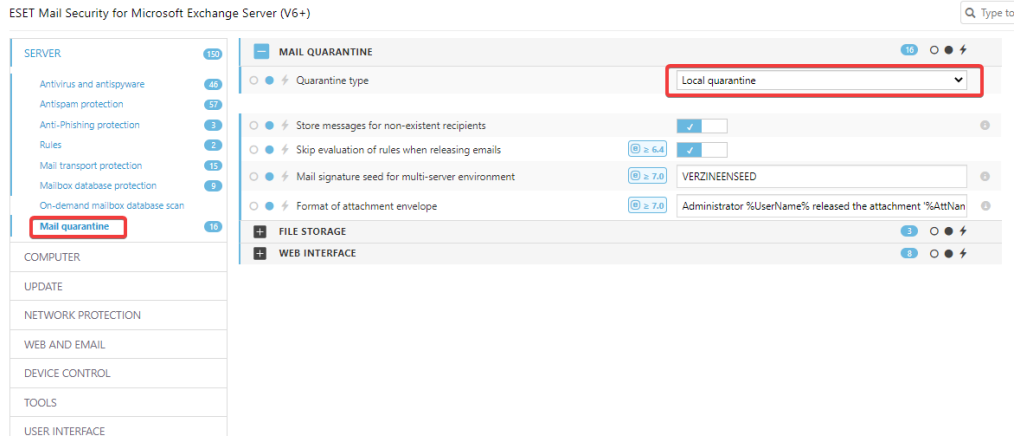
ON-DEMAND MAILBOX DATABASE SCAN:

- Controleer of het aantal Threads klopt met de hardware



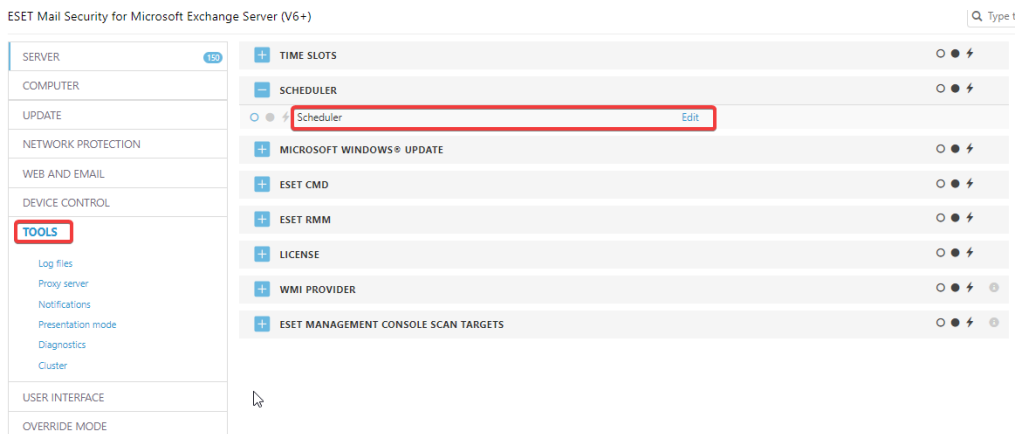
MAIL QUARANTINE:

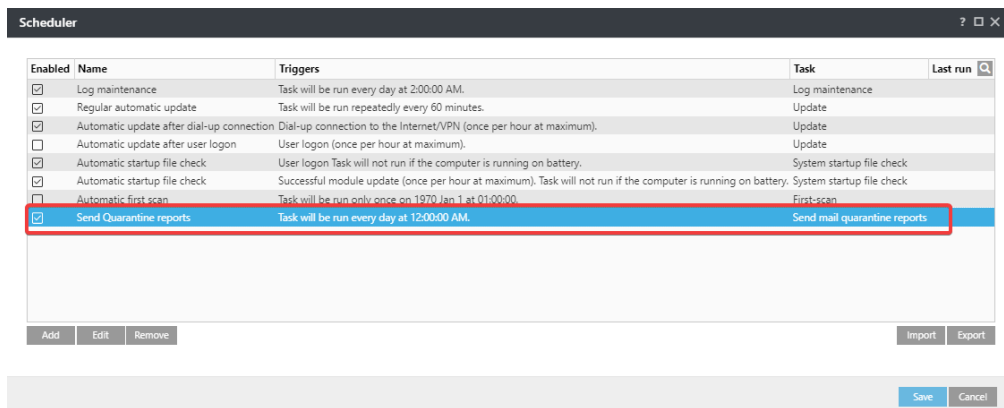
- Onderstaande instellingen zijn aan de hand van de wensen uit een organisatie verschillend. In dit voorbeeld maken we gebruik van de lokale quarantaine samen met de webinterface.



SCHEDULER:

- Om het versturen van quarantaine rapportages te automatiseren kan in de scheduler een taak worden aangemaakt om deze automatisch naar de eindgebruiker of beheerder te versturen.





Related Content

- [Best practice policies voor nieuwe installaties - Server Security for Windows](#)
- [Best practice policies voor nieuwe installaties - Endpoint Security](#)
- [Best practice policies voor nieuwe installaties - Intro](#)