

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

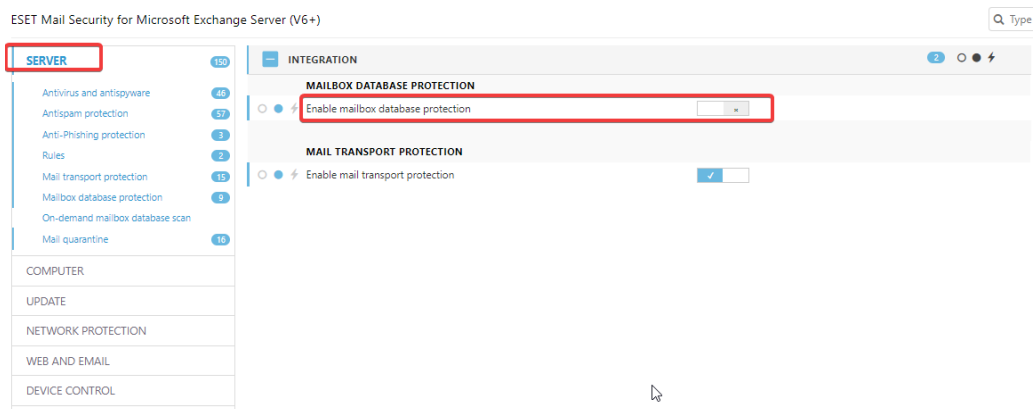
Danny | ESET Nederland - 2023-04-03 - [Reacties \(0\)](#) - [Best Practices](#)

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.

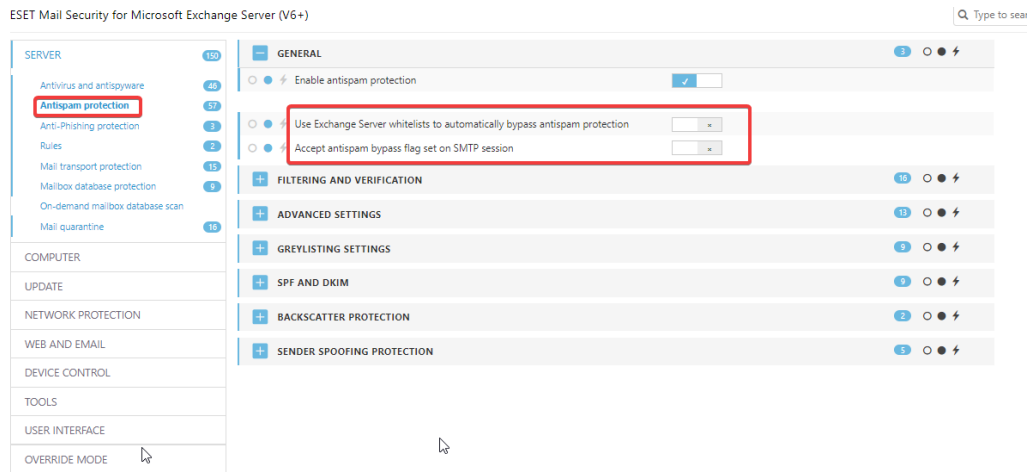
SERVER:

- 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.

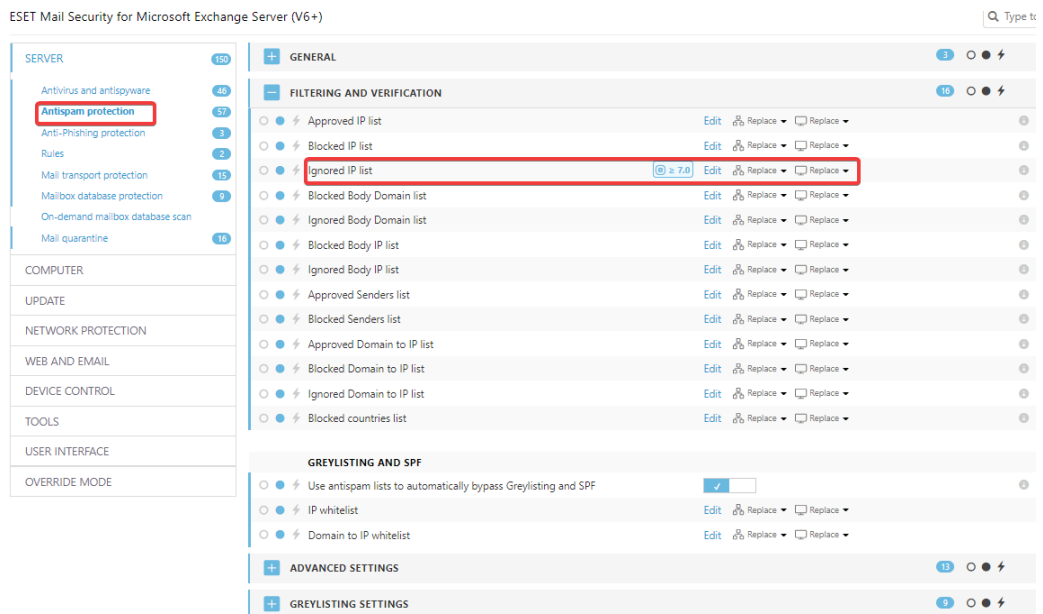


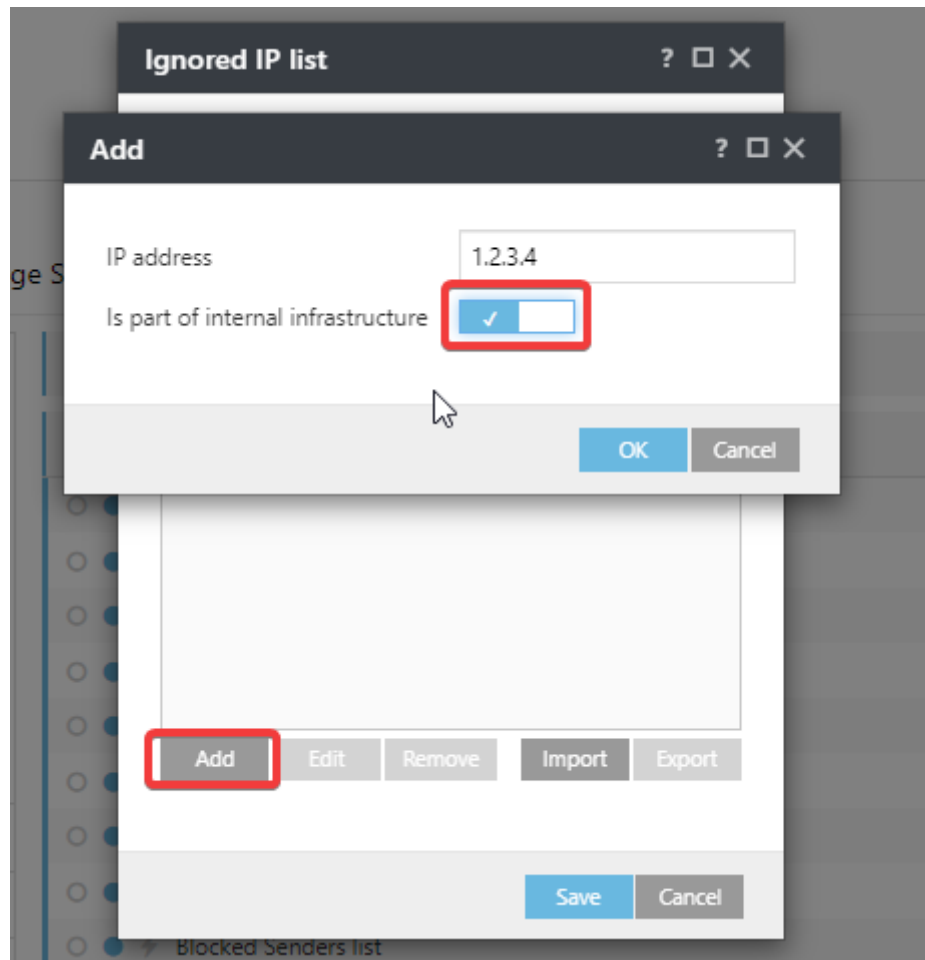
ANTISPAM PROTECTION:

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

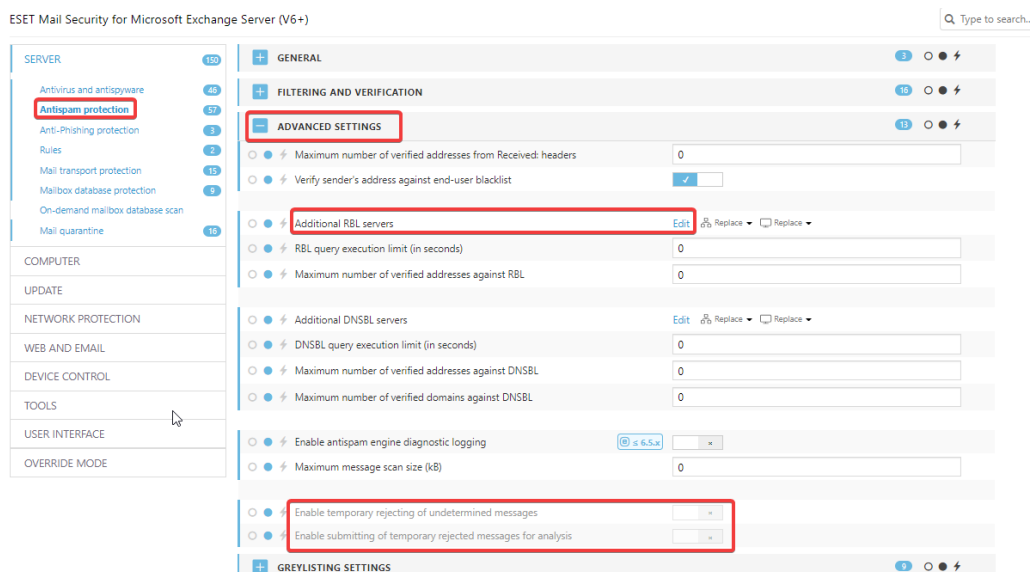


- Maak gebruik van de Ignore IP list om eigen infrastructuur en andere antispam oplossingen in de mailflow uit te zonderen. Vergeet ook niet om een vinkje te zetten wanneer het interne infrastructuur betreft.





- 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

ESET Mail Security for Microsoft Exchange Server (V6+)

The screenshot displays the configuration page for ESET Mail Security for Microsoft Exchange Server (V6+). The left sidebar lists various protection categories, with 'Antispam protection' highlighted in red. The main content area shows the 'GREYLISTING SETTINGS' section, also highlighted in red, with three checked checkboxes: 'Enable Greylisting', 'Use only domain part of sender address', and 'Synchronize greylisting databases across the ESET cluster'. Below this, the 'SMTP RESPONSE' section is visible, showing settings for response code (451), status code (4.7.1), and response message (Please try again later). Other protection modules like 'SPF AND DKIM', 'BACKSCATTER PROTECTION', and 'SENDER SPOOFING PROTECTION' are also listed at the bottom.

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

Rules



Rule



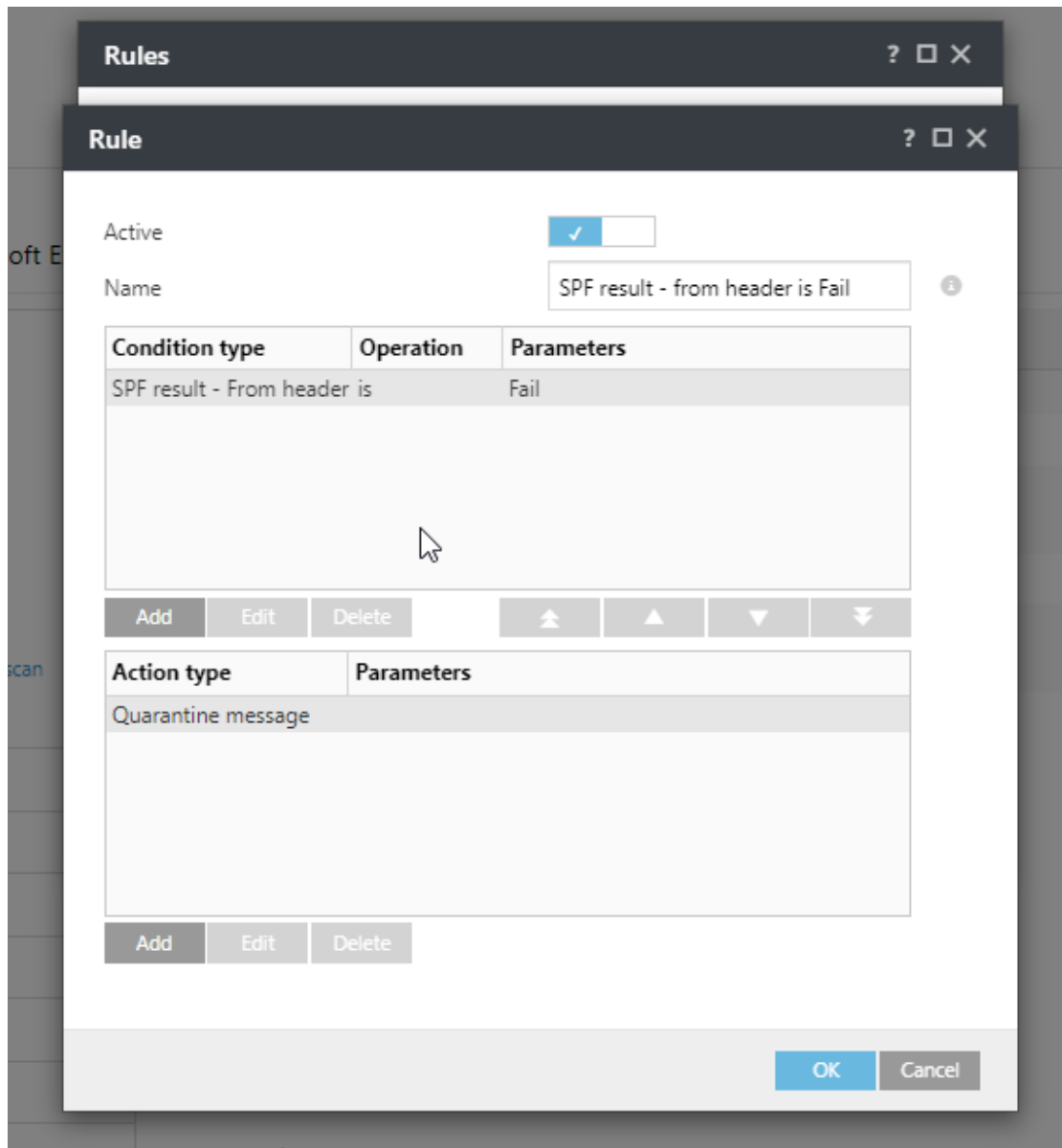
Active

Name



Condition type	Operation	Parameters
SPF result	is	Fail

Action type	Parameters
Quarantine message	



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

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

GENERAL 3

FILTERING AND VERIFICATION 16

ADVANCED SETTINGS 13

GREYLISTING SETTINGS 9

SPF AND DKIM 9

- Auto-detect DNS servers ⓘ ≥ 6.4
- DNS server IP address ⓘ ≥ 6.4
- DNS query timeout (seconds) ⓘ ≥ 6.4
- Automatically reject messages if SPF check fails ⓘ ≥ 6.4
- Use From: header if MAIL FROM is empty ⓘ ≥ 6.4**
- Automatically bypass Greylisting if SPF check passes ⓘ ≥ 6.4

SMTP REJECT RESPONSE

- Response code ⓘ ≥ 6.4
- Status code ⓘ ≥ 6.4
- Response message ⓘ ≥ 6.4

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 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

GENERAL 3

FILTERING AND VERIFICATION 16

ADVANCED SETTINGS 13

GREYLISTING SETTINGS 9

SPF AND DKIM 9

BACKSCATTER PROTECTION 2

- Enable NDR check ⓘ ≥ 7.0
- Automatically drop NDR messages if check fails ⓘ ≥ 7.0
- Signature seed ⓘ ≥ 7.0

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 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

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 ⓘ ≥ 8.0
- Enable incoming emails with my own domain in the sender's address ⓘ ≥ 8.0 **Only when they pass the SPF check**
- Automatically load my own domains from the Accepted domains list ⓘ ≥ 8.0
- List of my own domains ⓘ ≥ 8.0 Edit
- List of my own IP addresses ⓘ ≥ 8.0 Edit

ANTI-PHISHING PROTECTION:

The screenshot displays the ESET Mail Security for Microsoft Exchange Server (V6+) interface. On the left, a navigation menu lists various protection categories: SERVER (150), Antivirus and antispamware (48), Antispam protection (57), Anti-Phishing protection (3), Rules (2), Mail transport protection (15), Mailbox database protection (9), On-demand mailbox database scan, and Mail quarantine (16). The 'Anti-Phishing protection' category is highlighted with a red box. The main content area shows the 'ANTI-PHISHING PROTECTION' settings. Under 'MAILBOX DATABASE PROTECTION', there is an option to 'Enable anti-phishing mailbox database protection' with a version requirement of '≥ 7.0'. Under 'MAIL TRANSPORT PROTECTION', there is an option to 'Enable anti-phishing mail transport protection' with a version requirement of '≥ 7.0' and a checked checkbox. Under 'ON-DEMAND MAILBOX DATABASE SCAN', there is an option to 'Enable anti-phishing on-demand protection' with a version requirement of '≥ 7.0' and a checked checkbox. The 'MAIL TRANSPORT PROTECTION' section is highlighted with a red box.

RULES:

- Een krachtig onderdeel binnen Mail Security zijn rules.

The screenshot displays the ESET Mail Security for Microsoft Exchange Server (V6+) interface. On the left, a navigation menu lists various protection categories: SERVER (150), Antivirus and antispamware (48), Antispam protection (57), Anti-Phishing protection (3), Rules (2), Mail transport protection (15), Mailbox database protection (9), On-demand mailbox database scan, and Mail quarantine (16). The 'Rules' category is highlighted with a red box. The main content area shows the 'RULES' settings. Under 'MAILBOX DATABASE PROTECTION', there is a 'Rules' entry with an 'Edit' button. Under 'MAIL TRANSPORT PROTECTION', there is a 'Rules' entry with an 'Edit' button and a 'Replace' dropdown menu. Under 'ON-DEMAND MAILBOX DATABASE SCAN', there is a 'Rules' entry with an 'Edit' button and a 'Replace' dropdown menu. The 'MAIL TRANSPORT PROTECTION' section is highlighted with a red box.

- 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

SPF result - from header is Fail

Condition type	Operation	Parameters
SPF result - From header is		Fail

Add Edit Delete [Up Arrow] [Down Arrow]

Action type	Parameters
Quarantine message	

Add Edit Delete

OK Cancel

Rule ? □ ×

Active

Name ⓘ

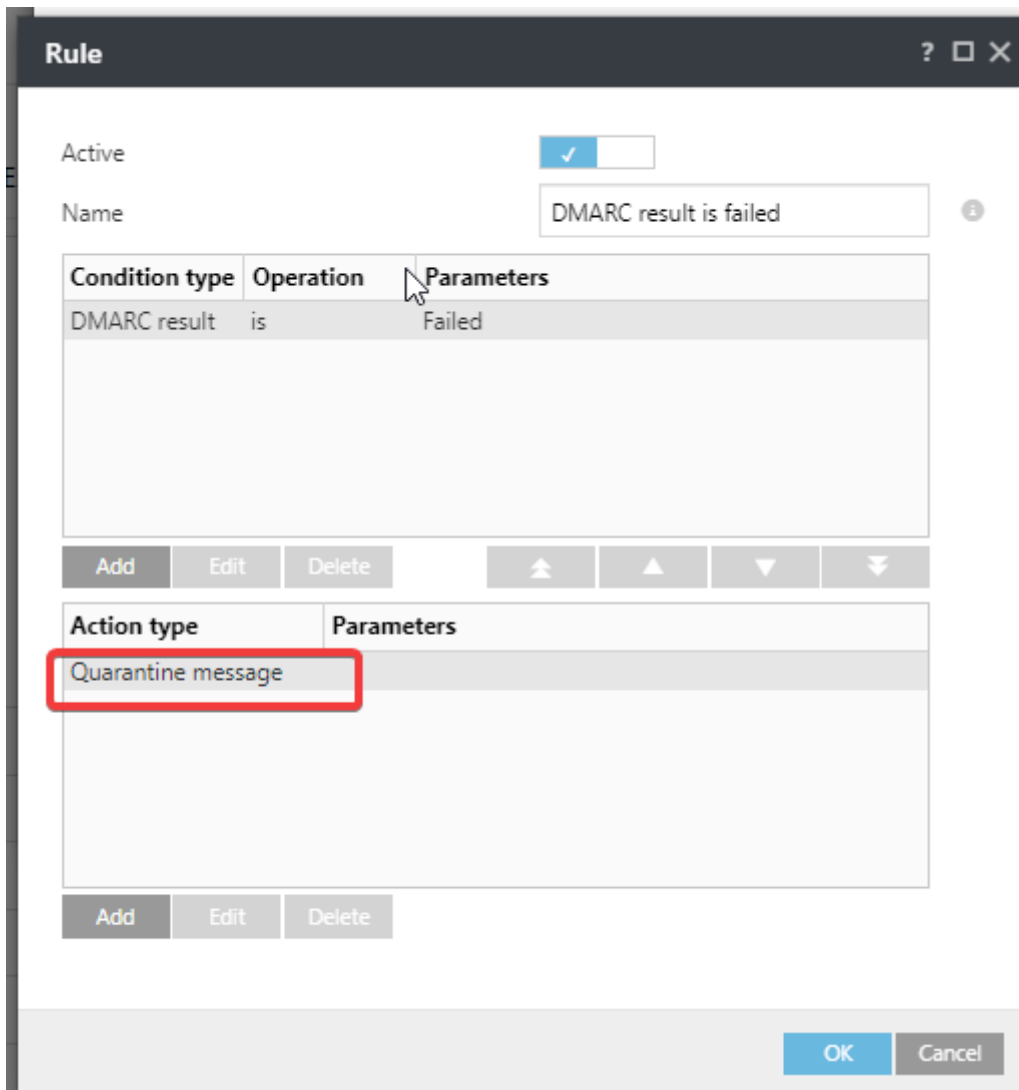
Condition type	Operation	Parameters
DKIM result	is	Failed

Add Edit Delete ↑ ▲ ▼ ↓

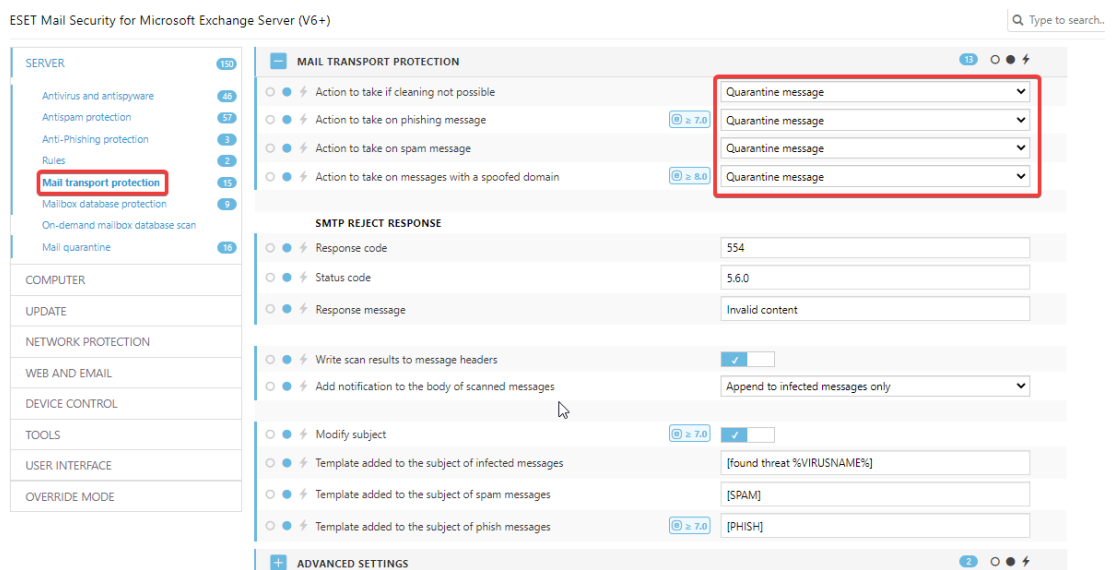
Action type	Parameters
Quarantine message	

Add Edit Delete

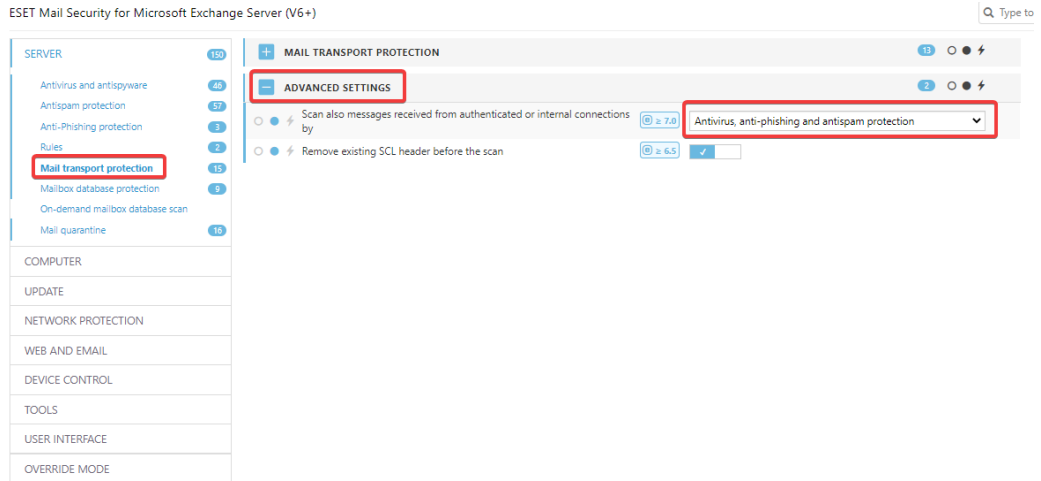
OK Cancel



MAIL TRANSPORT PROTECTION:



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

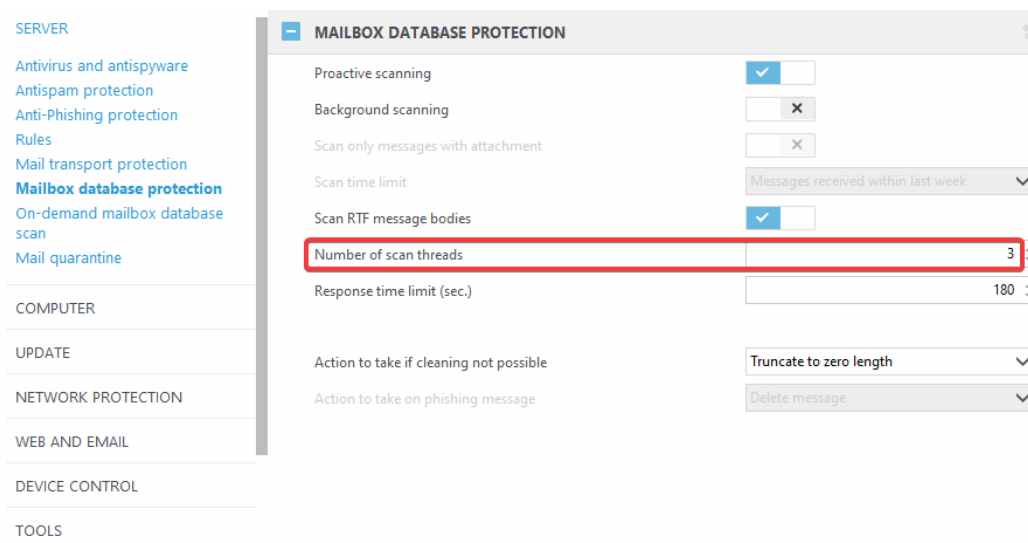


MAILBOX DATABASE PROTECTION:

- 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.

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

<p>SERVER 150</p> <ul style="list-style-type: none"> Antivirus and antispware 46 Antispam protection 57 Anti-Phishing protection 3 Rules 2 Mail transport protection 15 Mailbox database protection 5 On-demand mailbox database scan Mail quarantine 16 <p>COMPUTER</p> <p>UPDATE</p> <p>NETWORK PROTECTION</p> <p>WEB AND EMAIL</p> <p>DEVICE CONTROL</p> <p>TOOLS</p> <p>USER INTERFACE</p>	<p>MAIL QUARANTINE 16</p> <p>Quarantine type: Local quarantine</p> <ul style="list-style-type: none"> Store messages for non-existent recipients <input checked="" type="checkbox"/> Skip evaluation of rules when releasing emails <input checked="" type="checkbox"/> (≥ 6.4) Mail signature seed for multi-server environment <input checked="" type="checkbox"/> (≥ 7.0) VERZINEENSEED Format of attachment envelope <input checked="" type="checkbox"/> (≥ 7.0) Administrator %UserName% released the attachment %AttNan <p>FILE STORAGE 3</p> <p>WEB INTERFACE 3</p>
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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

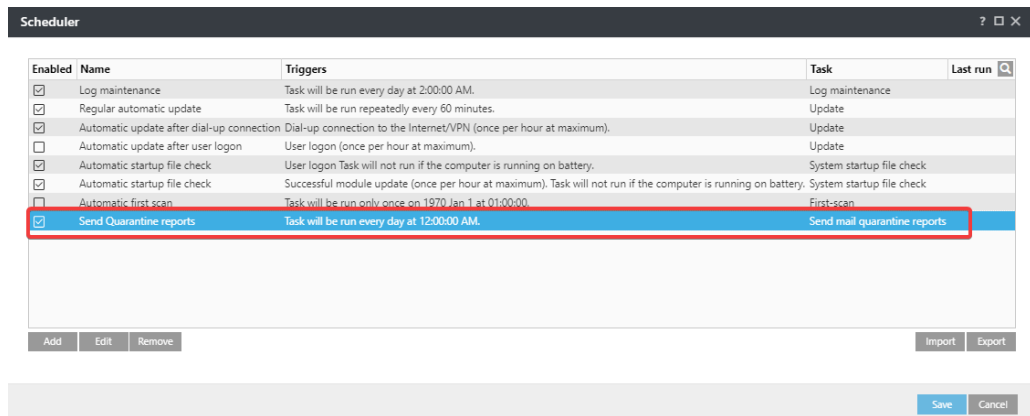
<p>SERVER 150</p> <ul style="list-style-type: none"> Antivirus and antispware 46 Antispam protection 57 Anti-Phishing protection 3 Rules 2 Mail transport protection 15 Mailbox database protection 5 On-demand mailbox database scan Mail quarantine 16 <p>COMPUTER</p> <p>UPDATE</p> <p>NETWORK PROTECTION</p> <p>WEB AND EMAIL</p> <p>DEVICE CONTROL</p> <p>TOOLS</p> <p>USER INTERFACE</p> <p>OVERWRITE MODE</p>	<p>MAIL QUARANTINE 16</p> <p>Quarantine type: Local quarantine</p> <ul style="list-style-type: none"> Store messages for non-existent recipients <input checked="" type="checkbox"/> Skip evaluation of rules when releasing emails <input checked="" type="checkbox"/> (≥ 6.4) Mail signature seed for multi-server environment <input checked="" type="checkbox"/> (≥ 7.0) VERZINEENSEED Format of attachment envelope <input checked="" type="checkbox"/> (≥ 7.0) Administrator %UserName% released the attachment %AttNan <p>FILE STORAGE 3</p> <p>WEB INTERFACE 3</p> <ul style="list-style-type: none"> Enable web interface <input checked="" type="checkbox"/> Web url Web and report language <input checked="" type="checkbox"/> (≥ 7.1) Default HTTPS port <input checked="" type="checkbox"/> (≥ 6.3) 443 HTTP port <input checked="" type="checkbox"/> (≥ 6.3) 80 Log release actions to events <input checked="" type="checkbox"/> (≥ 7.0) Enable default administrators <input checked="" type="checkbox"/> (≥ 6.4) Additional access rights <input checked="" type="checkbox"/> (≥ 6.4) Edit
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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.

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

<p>SERVER 150</p> <p>COMPUTER</p> <p>UPDATE</p> <p>NETWORK PROTECTION</p> <p>WEB AND EMAIL</p> <p>DEVICE CONTROL</p> <p>TOOLS</p> <ul style="list-style-type: none"> Log files Proxy server Notifications Presentation mode Diagnostics Cluster <p>USER INTERFACE</p> <p>OVERWRITE MODE</p>	<p>TIME SLOTS</p> <p>SCHEDULER</p> <ul style="list-style-type: none"> Scheduler Edit <p>MICROSOFT WINDOWS® UPDATE</p> <p>ESET CMD</p> <p>ESET RMM</p> <p>LICENSE</p> <p>WMI PROVIDER</p> <p>ESET MANAGEMENT CONSOLE SCAN TARGETS</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Gerelateerde inhoud

- [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](#)