TECH BRIEF

# MALWARE CONTAINMENT SETUP

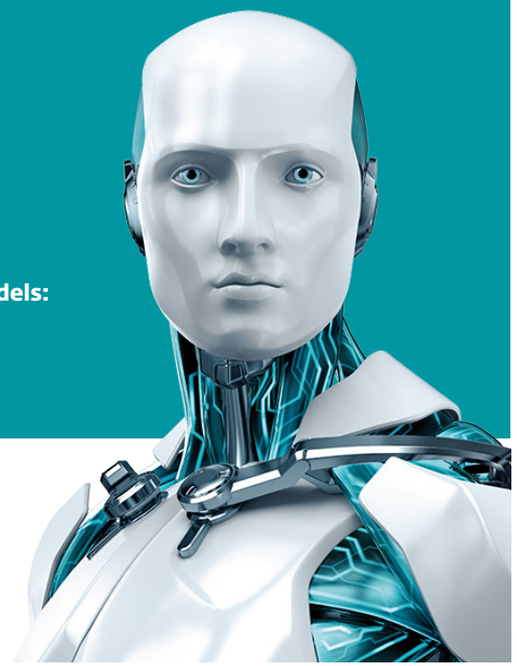
## AUTOMATISCHE SECURITY RESPONSE OP MALWARE OF RANSOMWARE UITBRAKEN

**Vereisten:**

*ESET Endpoint Security 6.x (EES)*
*ERA Agent voor (offline) Incident Response*
*ESET Remote Administrator 6.x*

**Endpoint Security en ESET Remote Administrator zijn onderdeel van de volgende bundels:**

*ESET Endpoint Protection Advanced*
*ESET Secure Business*
*ESET Secure Enterprise*



**Versie:** *1.0*
**Auteurs:** *Michael van der Vaart, Mitchell Wesdijk*

ENJOY SAFER TECHNOLOGY™

# Inhoud

## INTRODUCTIE

De malware containment setup bestaat uit meerlaagse beveiliging en geautomatiseerde incident response om de impact van een malware uitbraak tot een minimum te beperken.

## MALWARE CONTAINMENT BINNEN EN BUITEN HET BEDRIJF

Moderne malware, waaronder ransomware, probeert continu in een organisatie binnen te dringen. Een meerlaagse aanpak tegen deze cyberaanvallen is noodzakelijk en biedt meer weerstand aan cybercriminelen. Lukt het de malware toch om binnen te dringen op een endpoint, dan is het van belang de schade tot een minimum te beperken.

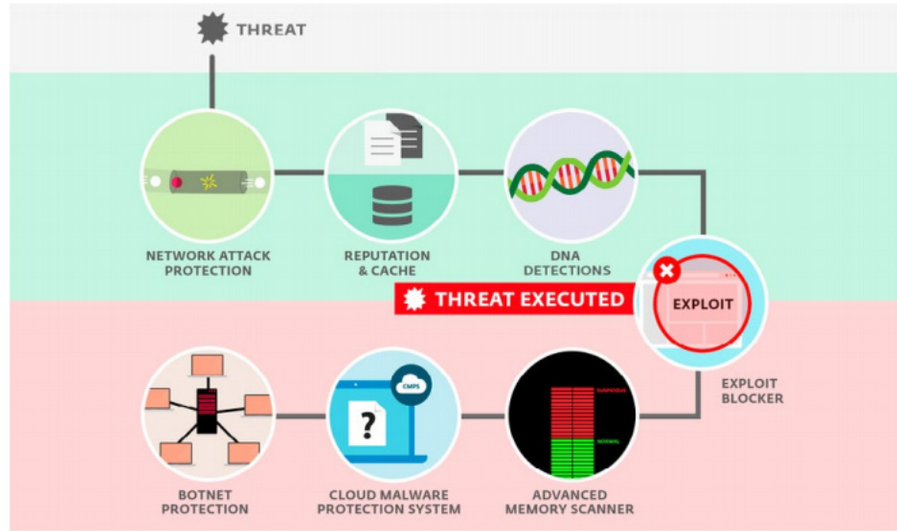
De ESET Malware Containment Setup maakt gebruik van de geavanceerde detectie- en preventiemogelijkheden van Network Attack Protection (NAP) in Endpoint Security om een endpoint in quarantaine te plaatsen en verspreiding of versleuteling van data te beperken op het actieve (WiFi) netwerk binnen of buiten kantoor.

## NETWORK ATTACK PROTECTION IN ENDPOINT SECURITY VS. WANNACRY (OF ANDERE MODERNE MALWARE)

ESET detecteerde en blokkeerde WannaCryptor.D- en zijn varianten ruim een maand voor het in de media verscheen.  Network Attack Protection blokkeert daarnaast ook proactief de exploit; EternalBlue, die WannaCry gebruikt om zichzelf op netwerkniveau te verspreiden. Op de systemen die zijn beveiligd met ESET Endpoint Security worden alle pogingen om deze gelekte kwetsbaarheid uit te buiten gedetecteerd, gerapporteerd en geblokkeerd.

## NETWORK ATTACK PROTECTION


Network Attack Protection is een uitbreiding op de huidige firewall-technologie en verbetert de detectie van bekende kwetsbaarheden op netwerkniveau. Dit vormt een belangrijke beschermingslaag tegen de verspreiding van malware binnen uw netwerk, netwerk gerelateerde aanvallen en misbruik van kwetsbaarheden waarvoor een patch nog niet is vrijgegeven of uitgebracht.



# BEPERK DE IMPACT VAN EEN MALWARE OF RANSOMWARE UITBRAAK TOT SLECHTS/ MAXIMAAL 1 GECOMPROMITTEERD ENDPOINT

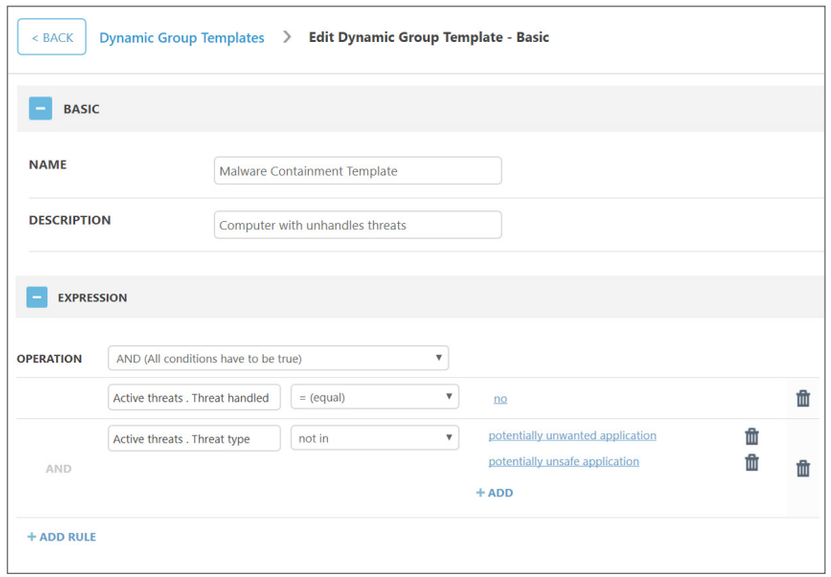
## Endpoint Security – Malware Containment Setup

## OPZETTEN MALWARE CONTAINMENT

1. Maak een nieuw DYNAMIC GROUP TEMPLATE (DGT).

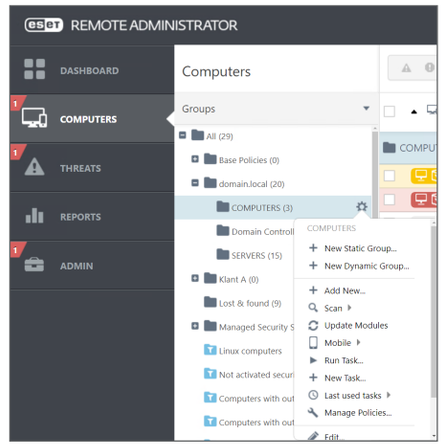
1.1. Navigeer naar: ADMIN > Dynamic Group Templates en klik op "New Template".

1.2. Configureer het DYNAMIC GROUP TEMPLATE (DGT) met de volgende expressie:

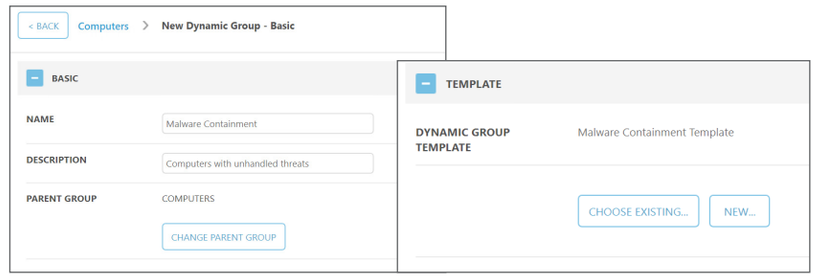



2. Maak een nieuw DYNAMIC GROUP (DG) aan en koppel deze aan de groep waar Malware Containment ingezet dient te worden.

2.1 Navigeer naar: COMPUTERS > static group > tandwiel > New Dynamic Group:

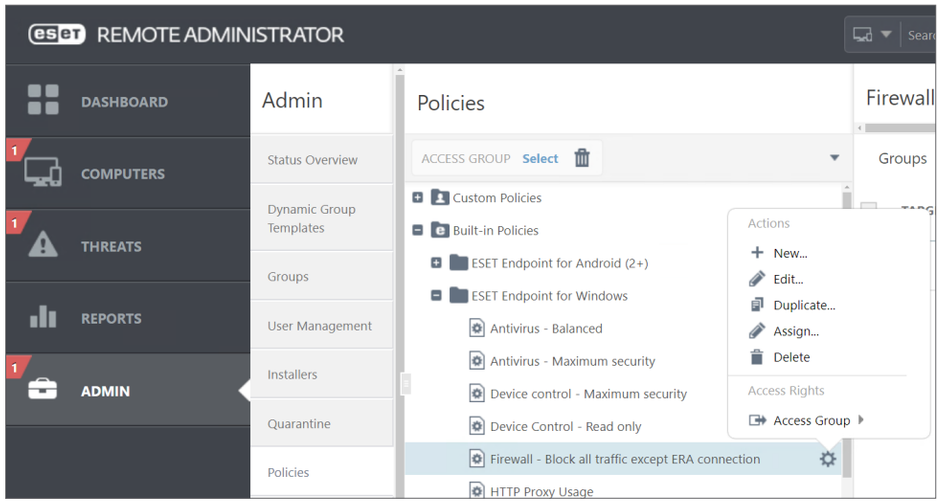



2.2 Configureer de volgende settings binnen de Dynamic Group:

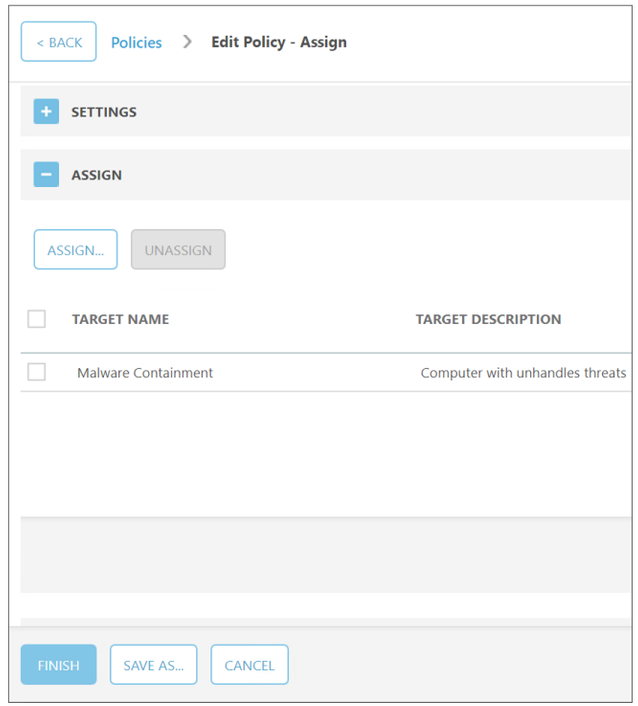


3. Koppel aan deze DG de standaard aanwezige policy: "Firewall - Block all traffic except ERA Connection"

3.1 Navigeer naar: ADMIN > Policies > Built-in Policies > tandwiel > Assign.

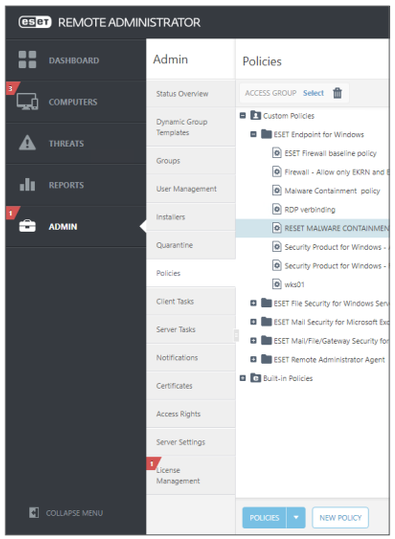



3.2 Klik op "ASSIGN" en selecteer hier de in stap 2 aangemaakte DG.

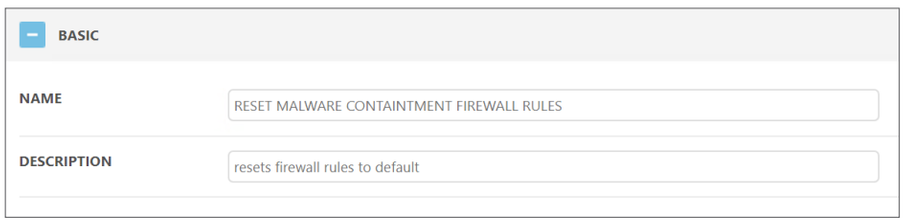


4. Pas een Policy toe om de firewall regels te resetten naar default (enkel nodig indien er geen andere firewall policies aanwezig zijn).

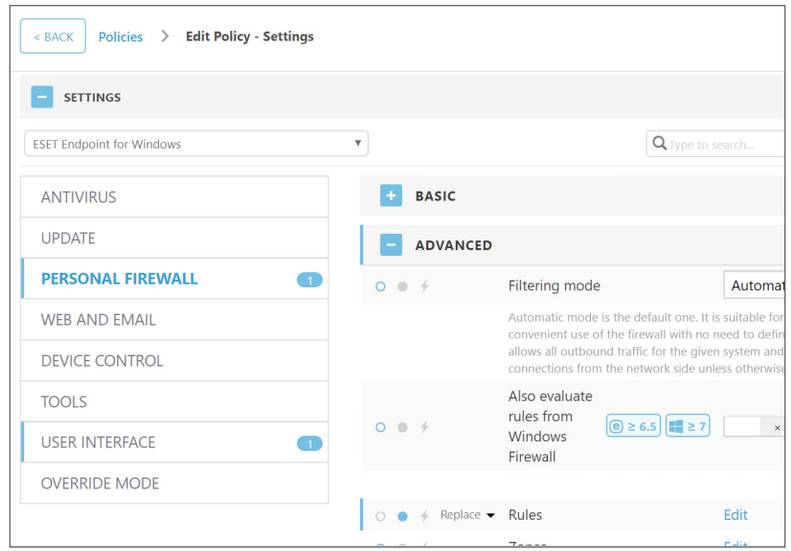
4.1 Maak een nieuwe policy aan (ADMIN > Policies > New Policy):




4.2 Geef deze policy een logische naam & beschrijving:



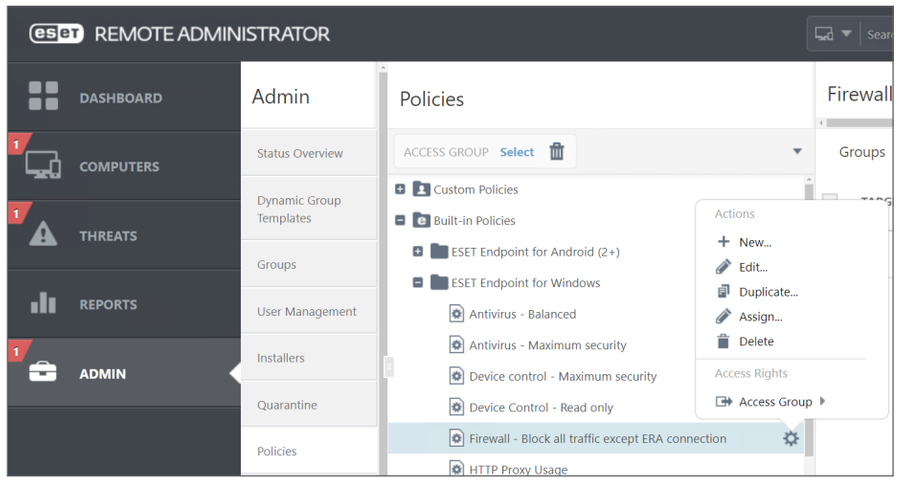

4.3 Zorg ervoor dat de firewall rules ingesteld staan op "replace" (ESET Endpoint for Windows > PERSONAL FIREWALL > ADVANCED):



## OPTIONELE INSTELLINGEN

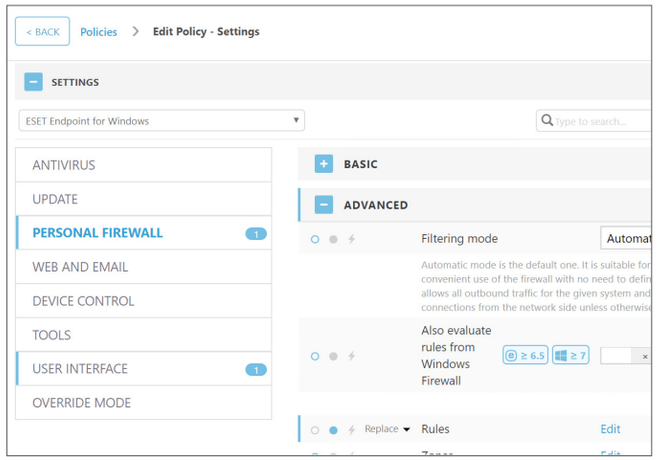
5. Voeg additionele firewall regels toe aan de policy voor eigen beheer en monitoring tooling, zoals RDP of Teamviewer.

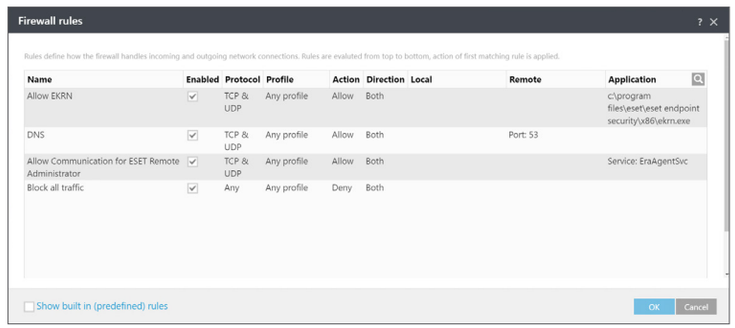
5.1 Bewerk de policy (ADMIN > Policies > Built-in Policies > "Firewall - Block all traffic except ERA Connection" > tandwiel > Edit).




5.2 Plaats hier de extra regels t.b.v. eigen beheer en monitoring tooling (PERSONAL FIREWALL > ADVANCED > Rules - Edit).

Zorg ervoor dat de aangemaakte regels boven de "Block all traffic" regel worden geplaatst.



## RESULTAAT

Alle endpoints met de actieve malware containment setup worden autonoom in quarantaine geplaatst, zolang een bedreiging nog niet opgeschoond kan worden. Zodra ESET een module update uitbrengt die de bedreiging kan opschonen, zullen de getroffen systemen automatisch uit de malware containment setup worden gehaald en terugkeren naar de standaard policy.