ARP-, ICMP- of DNS-Cache vergiftigingsaanval in ESET Home Producten voor Windows.

Tom | ESET Nederland - 2020-06-09 - ESET Internet Security

Probleem

- "ICMP-aanval" of "DNS-cache-vergiftigingsaanval" wordt gedetecteerd door de ESET-firewall
- "Detected ARP cache poisoning attack" wordt gedetecteerd door de ESET-firewall
- Maak een uitzondering voor intern IP-verkeer
- ESET technische ondersteuning heeft u naar dit artikel geleid om uw DNS-cache leeg te maken en het MS Hosts-bestand te herstellen
- Voer de DNS Flush-tool uit (alleen DNS-vergiftiging)

Oplossing

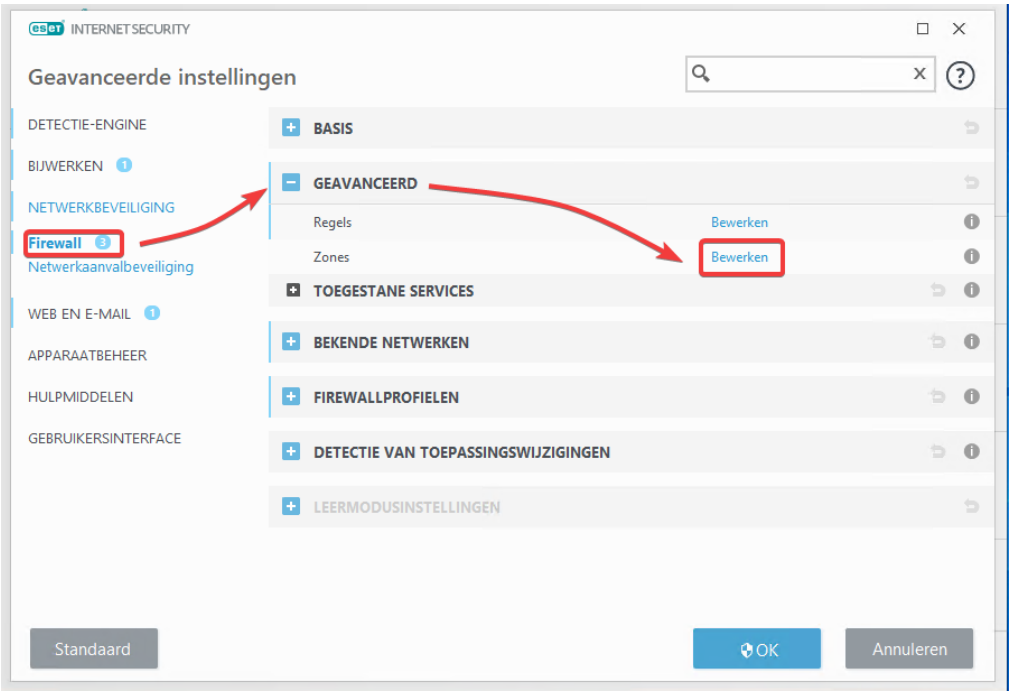
Als de ESET-firewall een bedreiging voor uw systeem detecteert, maak dan een uitzondering voor intern IP-verkeer. Volg onderstande stappen om te controleren of het uitzonderen verstandig is
Voer de DNS flush tool uit als het probleem niet is opgelost.

1. Bepaal of het IP-adres dat in de melding wordt gedetecteerd een nummer is dat binnen het volgende bereik valt (waarbij "x" 0-255 is):
   172.16.x.x - 172.31.x.x
   192.168.x.x
   10.x.x.x
2. Als het gedetecteerde IP-adres binnen het hierboven vermelde veilige bereik valt, opent u het hoofdprogrammavenster van uw ESET Windows-product. De uit te voeren stappen ziet u hieronder bij: Maak een uitzondering voor intern IP-verkeer .
3. Als het IP-adres, dat wordt gedetecteerd als een bedreiging, niet binnen het hierboven vermelde veilige bereik valt, of als er momenteel geen netwerkrandapparatuur in gebruik is op uw netwerk, bevindt het apparaat dat door de firewall wordt gedetecteerd zich op een openbaar netwerk en kan het een bedreiging voor uw systeem. We adviseren u om contact op te nemen met ESET Klantenservice voor eventueel meer uitleg over de bedreiging.

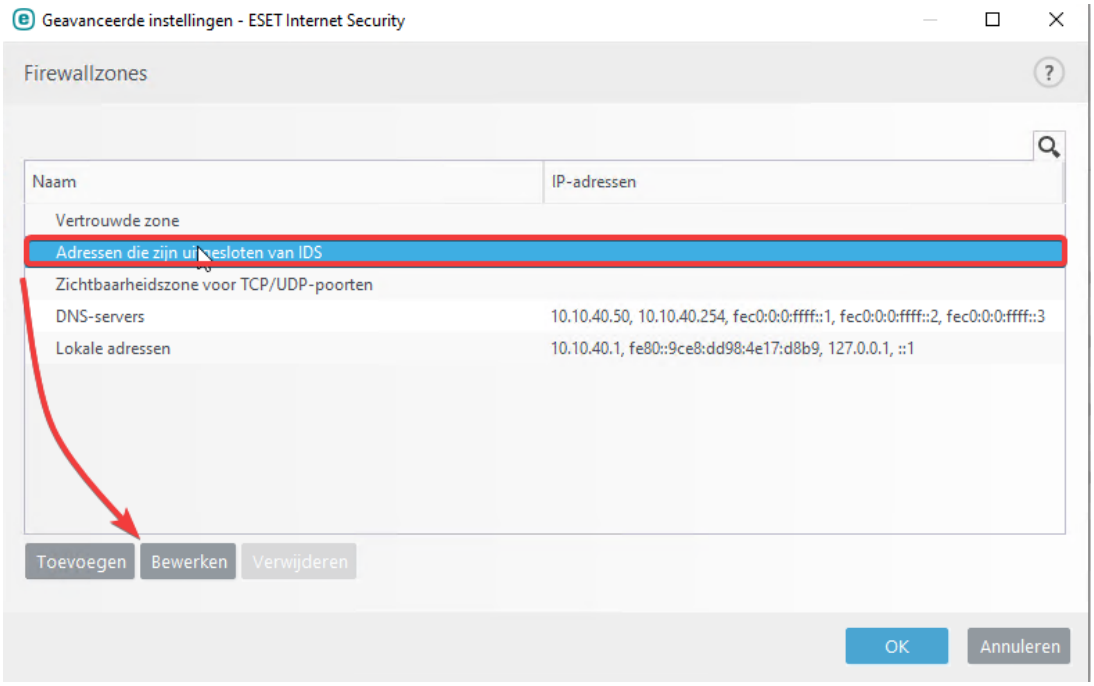
Maak een uitzondering voor intern IP-verkeer

1. Druk op de **F5**-toets op uw toetsenbord om toegang te krijgen tot Geavanceerde instellingen.

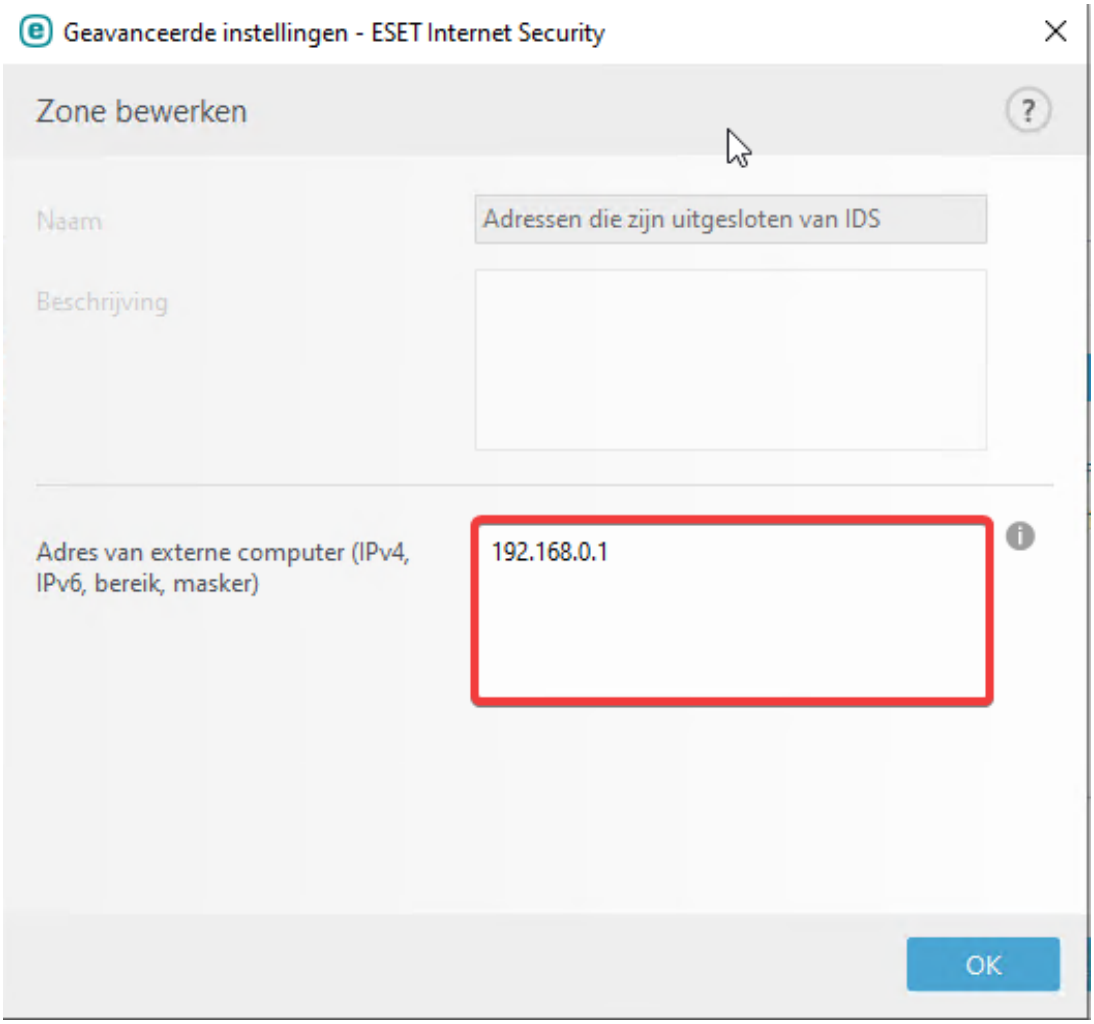
2. Vouw **Netwerkbeveiliging** uit, klik op **Firewall**, vouw **Geavanceerd** uit en klik vervolgens op **Bewerken** naast **Zones**.



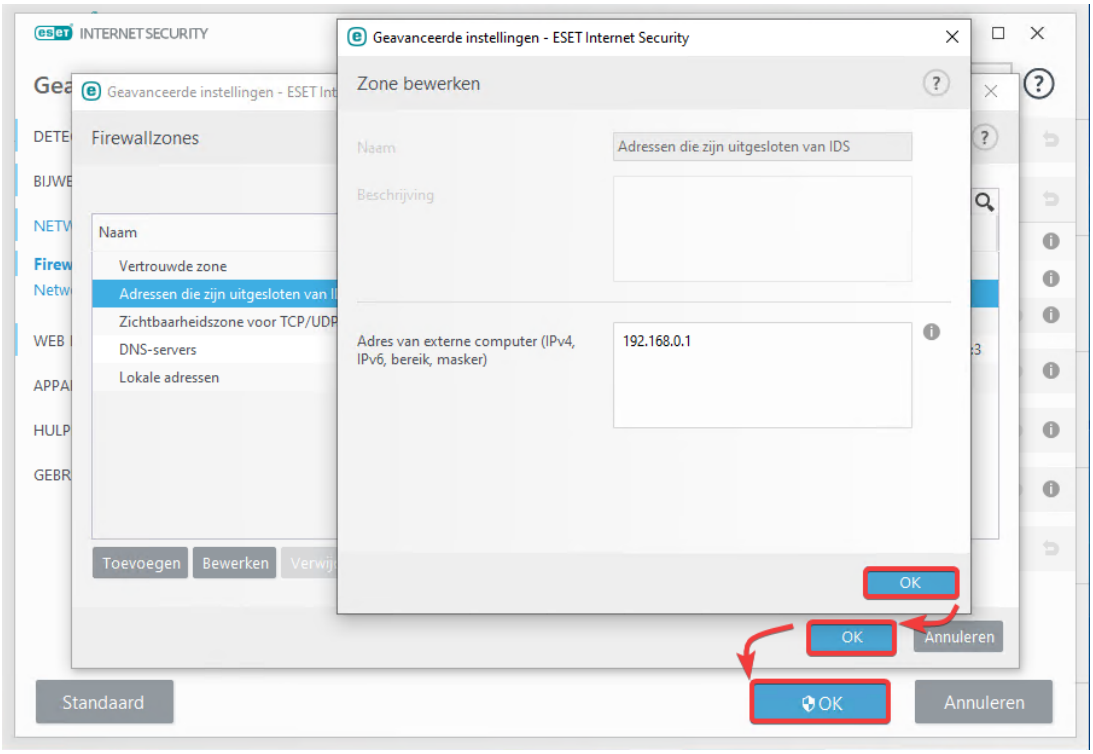
3. Selecteer in het venster Firewall-zones **Adressen uitgesloten van IDS** en klik op **Bewerken**.
4. Klink op "Adressen uitgesloten van IDS"
5. Klik op "Bewerken"



6. Voer het interne IP-Adres waar de melding betreffende 'aanval' vandaan komt.



7. Klik driemaal op **OK** om Geavanceerde instellingen af te sluiten en uw wijzigingen op te slaan.



8. U zou geen berichten meer moeten zien over aanvallen afkomstig van een intern IP-adres waarvan u weet dat het veilig is. Als u dit probleem blijft ondervinden kunt u het beste contact opnemen met de ESET klantenservice voor meer informatie.

Is uw vraag hiermee niet beantwoord of uw probleem niet verholpen? Klik dan hier om uw vraag te stellen aan de klantenservice van ESET Nederland.