# Configuratie van de variabele SNORT_BPF op een Defensiecentrum

## Inhoud


Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Configuratiestappen
Configuratievoorbeelden
Scenario 1: negeer al verkeer, AAN en VAN een kwetsbaarheidsscanner
Scenario 2: Alle verkeer, NAAR en VAN twee kwetsbaarheidsscanners negeren
Scenario 3: VLAN-gecodeerd verkeer, NAAR en VAN twee kwetsbaarheidscanners negeren
Scenario 4: Verkeer negeren vanaf een back-upserver
Scenario 5: Voor het gebruik van netwerkbereiken in plaats van afzonderlijke hosts


## Inleiding

U kunt Berkeley Packet Filter (BPF) gebruiken om te voorkomen dat een host of netwerk wordt geïnspecteerd door een Defense Center. Snort gebruikt de variabele **Snort_BPF** om verkeer uit te sluiten van een inbraakbeleid. Dit document bevat instructies voor het gebruik van de variabele **Snort_BPF** in verschillende scenario's.

> **Tip**: het is sterk aanbevolen om een vertrouwensregel in een toegangscontrolebeleid te gebruiken om te bepalen wat verkeer is en niet is geïnspecteerd, in plaats van een BPF in het inbraakbeleid. De variabele **`Snort_BPF`** is beschikbaar op softwareversie 5.2 en wordt afgekeurd op softwareversie 5.3 of hoger.

## Voorwaarden

### Vereisten

Cisco raadt u aan kennis te hebben over het Defense Center, Inbraakbeleid, Berkeley Packet Filter en Snelregels.

### Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwareversies:

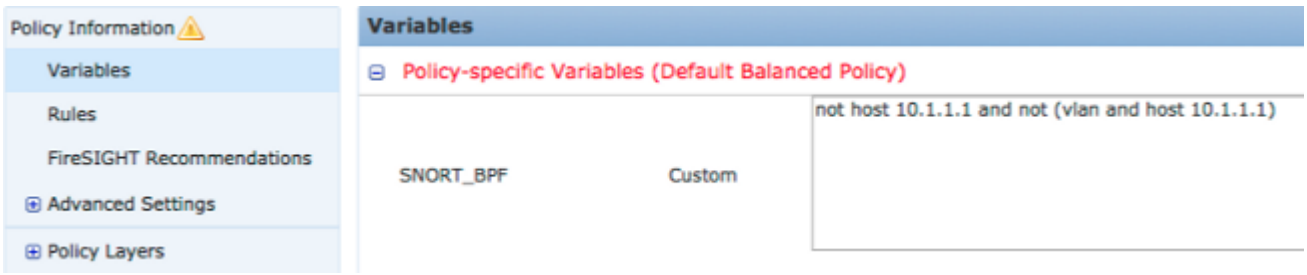
- Defensiecentrum
- Software versie 5.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

# Configuratiestappen

Om de variabele **Snort_BPF** te kunnen configureren volgt u de onderstaande stappen:

1. Toegang tot de web-gebruikersinterface van uw Defence Center.
2. Ga naar **Beleid > Inbraakbeleid > Inbraakbeleid**.
3. Klik op het *potloodpictogram* om uw inbraakbeleid te bewerken.
4. Klik op **Variabelen** van het menu aan de linkerkant.
5. Zodra de variabelen zijn geconfigureerd, moet u de wijzigingen opslaan en opnieuw uw inbraakbeleid toepassen zodat het van kracht wordt.




*Afbeelding: Screenshot van de pagina voor de configuratie van de variabele Snort_BPF*

# Configuratievoorbeelden

Hieronder volgen een aantal basisvoorbeelden ter referentie:

## Scenario 1: negeer al verkeer, AAN en VAN een kwetsbaarheidsscanner

1. We hebben een kwetsbaarheidsscanner op IP-adres 10.1.1.1
2. We willen alle verkeer van en naar de scanner negeren
3. Het verkeer kan al dan niet een 802.1q (vlan) tag hebben

De **SNORT_BPF** is:

```
not host 10.1.1.1 and not (vlan and host 10.1.1.1)
```

VERGELIJKING: verkeer *is niet* VLAN-getagd, maar de punten 1 en 2 blijven waar zijn:

```
not host 10.1.1.1
```

In gewoon Engels zou dit verkeer negeren waarbij een van de eindpunten 10.1.1.1 (de scanner) is.

## Scenario 2: Alle verkeer, NAAR en VAN twee kwetsbaarheidsscanners negeren

1. We hebben een kwetsbaarheidsscanner op IP-adres 10.1.1.1
2. We hebben een tweede kwetsbaarheidsscanner op IP-adres 10.2.1.1
3. We willen alle verkeer van en naar de scanner negeren
4. Het verkeer kan al dan niet een 802.11 (vlan) tag hebben

De **SNORT_BPF** is:

```
not (host 10.1.1.1 or host 10.2.1.1) and not (vlan and (host 10.1.1.1 or host 10.2.1.1))
```

**Vergelijking: Traffic *is niet* VLAN-getagd, maar de punten 1 en 2 blijven waar:**

```
not (host 10.1.1.1 or host 10.2.1.1)
```

Samengevat, zou dit verkeer negeren waar één van de eindpunten 10.1.1.1 OF 10.2.1.1 is.

> **Opmerking**: het is belangrijk om op te merken dat de VLAN-tag in bijna alle gevallen slechts eenmaal mag voorkomen in een gegeven BPF. De enige keer dat u het meer dan eens moet zien, is als uw netwerk geneste VLAN-tagging gebruikt (soms 'QinQ' genoemd).

## Scenario 3: VLAN-gecodeerd verkeer, NAAR en VAN twee kwetsbaarheidscanners negeren

1. We hebben een kwetsbaarheidsscanner op IP-adres 10.1.1.1
2. We hebben een tweede kwetsbaarheidsscanner op IP-adres 10.2.1.1
3. We willen alle verkeer van en naar de scanner negeren
4. Traffic is 802.11 (vlan) getagd en u wilt een specifieke (vlan) tag gebruiken, zoals in vlan 101

De **SNORT_BPF** is:

```
not (host 10.1.1.1 or host 10.2.1.1) and not (vlan 101 and (10.1.1.1 or host 10.2.1.1))
```

## Scenario 4: Verkeer negeren vanaf een back-upserver

1. We hebben een netwerk back-upserver op IP-adres 10.1.1.1
2. Machines in het netwerk maken verbinding met deze server op poort 8080 om hun nachtelijke back-up uit te voeren
3. We willen dit back-upverkeer negeren, omdat het versleuteld is en grote hoeveelheden bevat

De **SNORT_BPF** is:

```
not (dst host 10.1.1.1 and dst port 8080) and not (vlan and (dst host 10.1.1.1
```

```
and dst port 8080))
```

Vergelijking: Traffic *is niet* VLAN-getagd, maar de punten 1 en 2 blijven waar:

```
not (dst host 10.1.1.1 and dst port 8080)
```

Vertaald betekent dit dat verkeer naar 10.1.1.1 (onze hypothetische back-upserver) op poort 8080 (luisterpoort) niet moet worden geïnspecteerd door de IPS-detectiemachine.

Het is ook mogelijk om net te gebruiken in de plaats van de host om een netwerkblok te specificeren in plaats van een enkele host. Voorbeeld:

```
not net 10.1.1.0/24
```

In het algemeen is het een goede praktijk om de BPF zo specifiek mogelijk te maken; het verkeer uit te sluiten van inspectie dat moet worden uitgesloten, zonder daarbij elk niet-gerelateerd verkeer uit te sluiten dat wellicht uitbuitingspogingen bevat.

## Scenario 5: Voor het gebruik van netwerkbereiken in plaats van afzonderlijke hosts

U kunt netwerkbereiken opgeven in de BPF-variabele in plaats van hosts om de lengte van de variabele te verkorten. Om dit te doen zult u het netto sleutelwoord in plaats van gastheer gebruiken en zult een bereik CIDR specificeren. Hieronder zie je een voorbeeld:

```
not (dst net 10.8.0.0/16 and dst port 8080) and not (vlan and (dst net 10.8.0.0/16
and dst port 8080))
```

> Opmerking: Zorg ervoor dat u het netwerkadres invoert met behulp van de CIDR-notatie en een bruikbaar adres in de CIDR-blokadresruimte. Gebruik bijvoorbeeld net 10.8.0.0/16 in plaats van net 10.8.2.16/16.

Het **SNORT_BPF** variabele wordt gebruikt om te voorkomen dat bepaald verkeer door een IPS-detectiemotor wordt geïnspecteerd, vaak om prestatieredenen. Deze variabele gebruikt het standaard Berkeley Pack Filters (BPF) formaat. Verkeer dat overeenkomt met de **SNORT_BPF** variabele wordt geïnspecteerd; terwijl het verkeer NIET overeenkomt met de **SNORT_BPF** Deze variabele wordt NIET geïnspecteerd door de IPS-detectiemotor.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.