

Een passeerregel instellen op een Cisco-voedingssysteem

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Een voorbeeldregel maken](#)

[Een passeringsregel inschakelen](#)

[Verifiëren](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft een pass-regel, hoe deze gecreëerd wordt en hoe deze in een indringingsbeleid kan worden toegepast.

U kunt slagen regels creëren om te voorkomen dat pakketten die aan criteria voldoen die in de passeerregel worden gedefinieerd de alarmregel in specifieke situaties in werking stellen, in plaats van de alarmregel uit te schakelen. Standaard passeren regels de alarmregels. Een Firepower System vergelijkt pakketten met de voorwaarden die in elke regel zijn gespecificeerd en, als de pakketgegevens voldoen aan alle voorwaarden die in een regel zijn gespecificeerd, leidt de regel tot triggers. Als een regel een alarmregel is, genereert deze een inbraakgebeurtenis. Als het om een pass-regel gaat, negeert hij het verkeer.

Bijvoorbeeld, zou u een regel kunnen willen die pogingen zoekt om in een FTP server als "anoniem" te registreren om actief te blijven. Als uw netwerk echter een of meer legitieme anonieme FTP-servers heeft, kunt u een passeerregel schrijven en activeren die aangeeft dat, voor die specifieke servers, anonieme gebruikers niet de oorspronkelijke regel activeren.

Voorzichtig: Wanneer een oorspronkelijke regel dat de pass-regel gebaseerd is op een herziening, wordt de pass-regel niet automatisch bijgewerkt. Het kan dan ook moeilijk zijn om regels goed te keuren.

Opmerking: Als u de Suppression voor een regel toelaat, onderdrukt het de gebeurtenis berichten voor die regel. De regel wordt echter nog geëvalueerd. Als u bijvoorbeeld op een uitrolregel drukt, worden pakketten die overeenkomen met de regel, in de stilte ingetrokken.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

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.

Configureren

Een voorbeeldregel maken

1. Navigeer naar **objecten > Inbraakregels**. De lijst van regelcategorieën verschijnt.
2. Vind de regelcategorie die aan de regel is gekoppeld die u wilt filteren. Klik op het pijlpictogram om de categorie uit te vouwen in de categorie en vind de regel waarvoor u een slagen-regel wilt maken. In plaats hiervan kunt u ook het regel zoekveld gebruiken.
3. Nadat u de gewenste regel hebt gevonden, klikt u op het pictogram naast de regel om de regel te bewerken.
4. Wanneer u een regel bewerkt, voert u deze stappen uit: Klik op de knop **Bewerken** die aan de regel voldoet. Kies in de vervolgkeuzelijst Actie **doorgeven**. Verander het veld Bron IPs en het veld Bestemming naar de hosts of netwerken waarop u de regel niet wilt waarschuwen. Klik op **Opslaan als nieuw**.

Edit Rule 3:13921:5


[\(View Documentation, Rule Comment\)](#)

Message	IMAP Altrium Software MERCUR IMAPD NTLMSSP command handling me		
Classification	Attempted Administrator Privilege Gain ▼ Edit Classifications		
Action	pass ▼		
Protocol	tcp ▼		
Direction	Directional ▼		
Source IPs	any	Source Port	any
Destination IPs	\$HOME_NET	Destination Port	143

Detection Options

reference		
<input type="text" value="url,secunia.com/advisories/24596"/>		
reference		
<input type="text" value="bugtraq,23058"/>		
reference		
<input type="text" value="cve,2007-1578"/>		
metadata		
<input type="text" value="engine shared, soid 3 13921, service imap"/>		
ack ▼	<input type="button" value="Add Option"/>	<input type="button" value="Save As New"/>

5. Let op het ID-nummer van de nieuwe regel. Bijvoorbeeld 1000000.

 **Success** ✕
Successfully created new rule "IMAP Altrium Software MERCUR IMAPD NTLMSSP command handling memory corruption attempt"

Edit Rule 3:1000000:1 [\(View Documentation, Rule Comment\)](#)

Message:

Classification: ▼
[Edit Classifications](#)

Action: ▼

Protocol: ▼

Direction: ▼

Source IPs: Source Port:

Destination IPs: Destination Port:

Detection Options

reference

reference

reference

metadata

▼

Een passeringsregel inschakelen

U moet uw nieuwe regel in het juiste inbraakbeleid toestaan om verkeer op de bron of de bestemmingsadressen door te geven die u hebt opgegeven. Volg deze stappen om een passeerregel mogelijk te maken:

1. Het actieve inbraakbeleid wijzigen: Navigeren in op **beleid > Toegangsbeheer > Inbraakcontrole**. Klik op **Bewerken** naast het actieve inbraakbeleid.
2. Voeg de nieuwe regel aan de regellijst toe: Klik op **Regels** in het linker deelvenster. Voer de regel-ID in die u eerder in het filtervak hebt opgemerkt. Controleer het aanvinkvakje Regels

- en verander de status van de Regel om **gebeurtenissen** te **genereren**. Klik op **Policy Information** in het linker deelvenster. Klik op **Aanmelden wijzigingen**.
3. Klik op **Uitvoeren** om de wijzigingen op het apparaat in te voeren.

Verifiëren

U dient de nieuwe gebeurtenissen enige tijd te controleren om er zeker van te zijn dat er geen gebeurtenissen gegenereerd worden voor deze specifieke regel voor de bepaalde bron of het bestemming IP-adres.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.