Packet Data (PCAP-bestand) downloaden met WebUser Interface

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Stappen om PCAP-bestand te downloaden](#)

Inleiding

Met behulp van de webgebruikersinterface kunt u het pakje(en) downloaden dat de getriggerde SNELregel heeft (geactiveerd). Het artikel bevat de stappen om pakketvastlegging gegevens (PCAP-bestand) te downloaden via de webgebruikersinterface van een Sourcefire FireSIGHT Management System.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben over Sourcefire FirePOWER-apparaat en de virtuele apparaatmodellen.

Gebruikte componenten

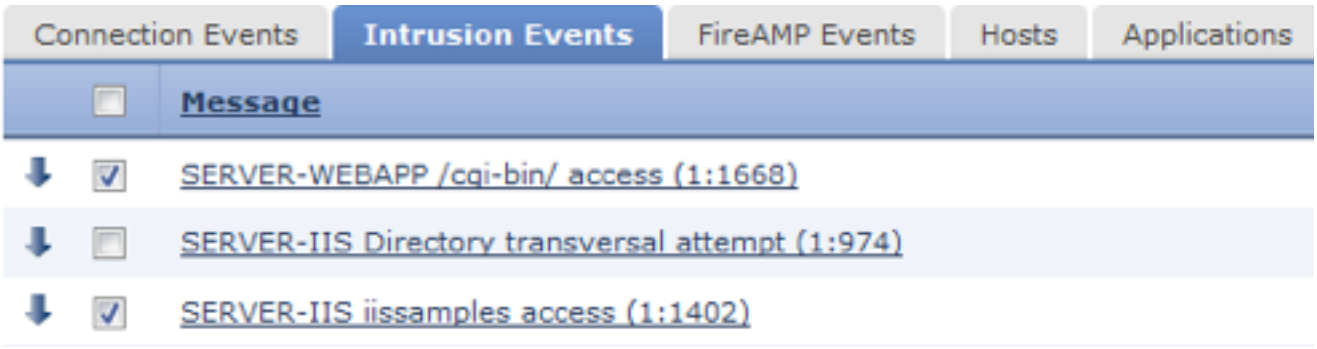
De informatie op dit document is gebaseerd op Sourcefire FireSIGHT Management Center, ook bekend als Defense Center, met softwareversie 5.2 of hoger.

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.

Stappen om PCAP-bestand te downloaden

Stap 1: Meld u aan bij een Sourcefire Defense Center of Management Center en navigeer naar de pagina Inbraakgebeurtenissen zoals hieronder:

Stap 2: Selecteer de gebeurtenis(en) die u wilt downloaden (PCAP-bestand) in het aankruisvakje.



Stap 3: Scrolt naar de onderkant van de pagina en of:

- Klik op Packet downloaden van de pakketten die de geselecteerde inbraakgebeurtenis(n) hebben geactiveerd
- Klik op Alle pakketten downloaden om alle pakketten te downloaden die de inbraakgebeurtenissen in de huidige beperkte weergave hebben geactiveerd

  Opmerking: De gedownload pakketten worden als een PCAP opgeslagen. Als u de pakketvastlegging wilt analyseren, moet u software downloaden en installeren die een PCAP-bestand kan lezen.

Stap 4: Sla het PCAP-bestand op de harde schijf wanneer dit wordt gevraagd.