Firepower Data Path Problemen opsporen en verhelpen fase 3: Security Intelligentie

Inhoud

Inleiding

Dit artikel maakt deel uit van een reeks artikelen waarin wordt uitgelegd hoe u het gegevenspad op FirePOWER-systemen systematisch moet oplossen om te bepalen of onderdelen van Firepower invloed kunnen hebben op het verkeer. Raadpleeg het gedeelte Overzicht voor informatie over de architectuur van FirePOWER-platforms en de koppelingen naar de andere artikelen voor probleemoplossing in datacenters.

Dit artikel bestrijkt de derde fase van de probleemoplossing bij het FirePOWER-gegevenspad, de beveiligingsfunctie.

Voorwaarden

- Dit artikel heeft betrekking op alle momenteel ondersteunde FirePOWER-platforms
- Security Intelligentie voor URL's en DNS is geïntroduceerd in versie 6.0.0

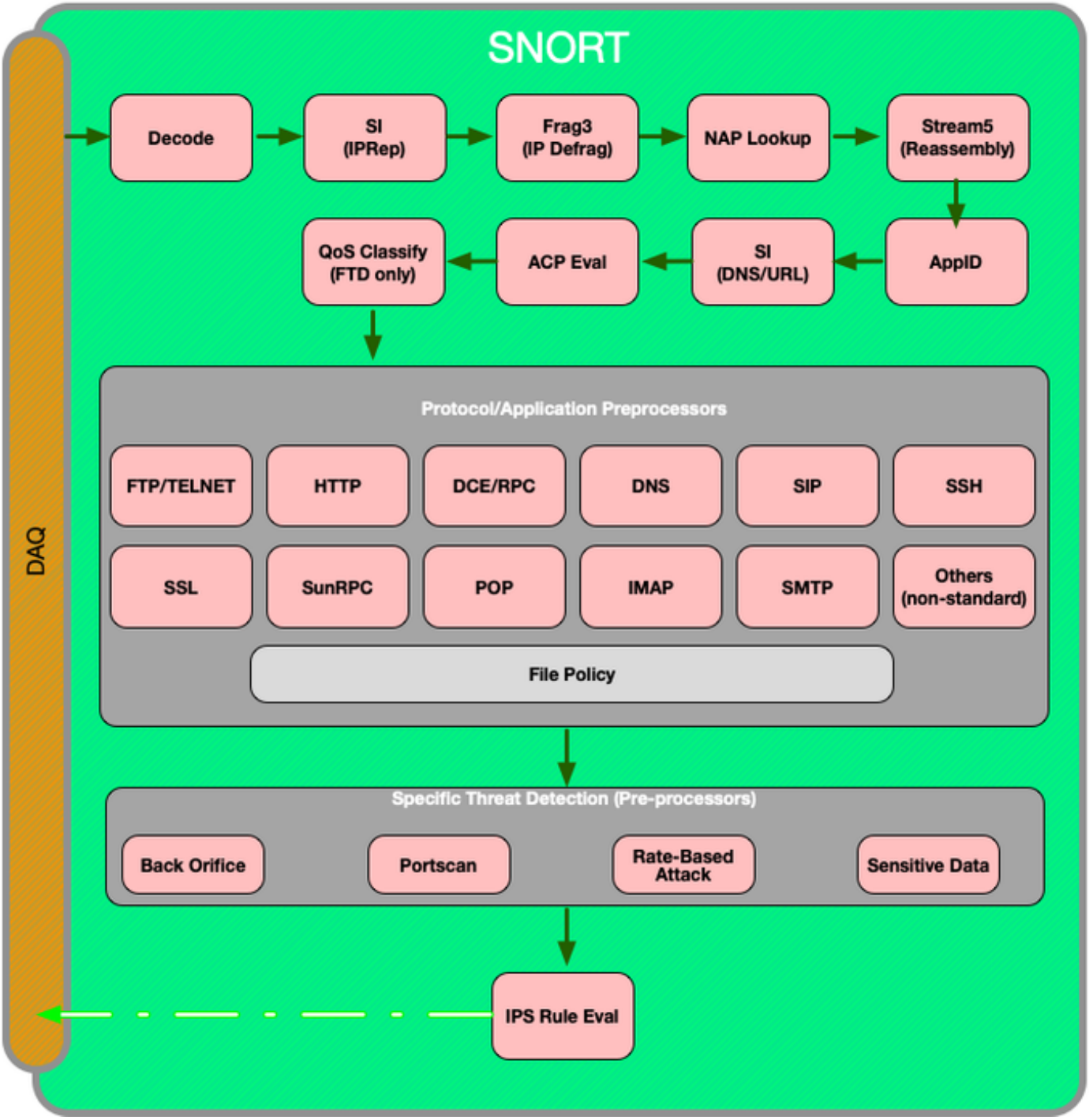
Probleemoplossing voor de fase van de Firepower Security Intelligence

Security Intelligence is een functie die inspectie uitvoert tegen zowel zwarte lijsten als blanken voor:

- IP-adressen (ook bekend als "netwerken" in bepaalde delen van de UI)
- Unified Resource Locators (URL's)
- Domain Name System (DNS)-reeks

De lijsten binnen Security Intelligence kunnen worden bevolkt door Cisco-geleverde feeds en/of door gebruiker ingestelde lijsten en voedingen.

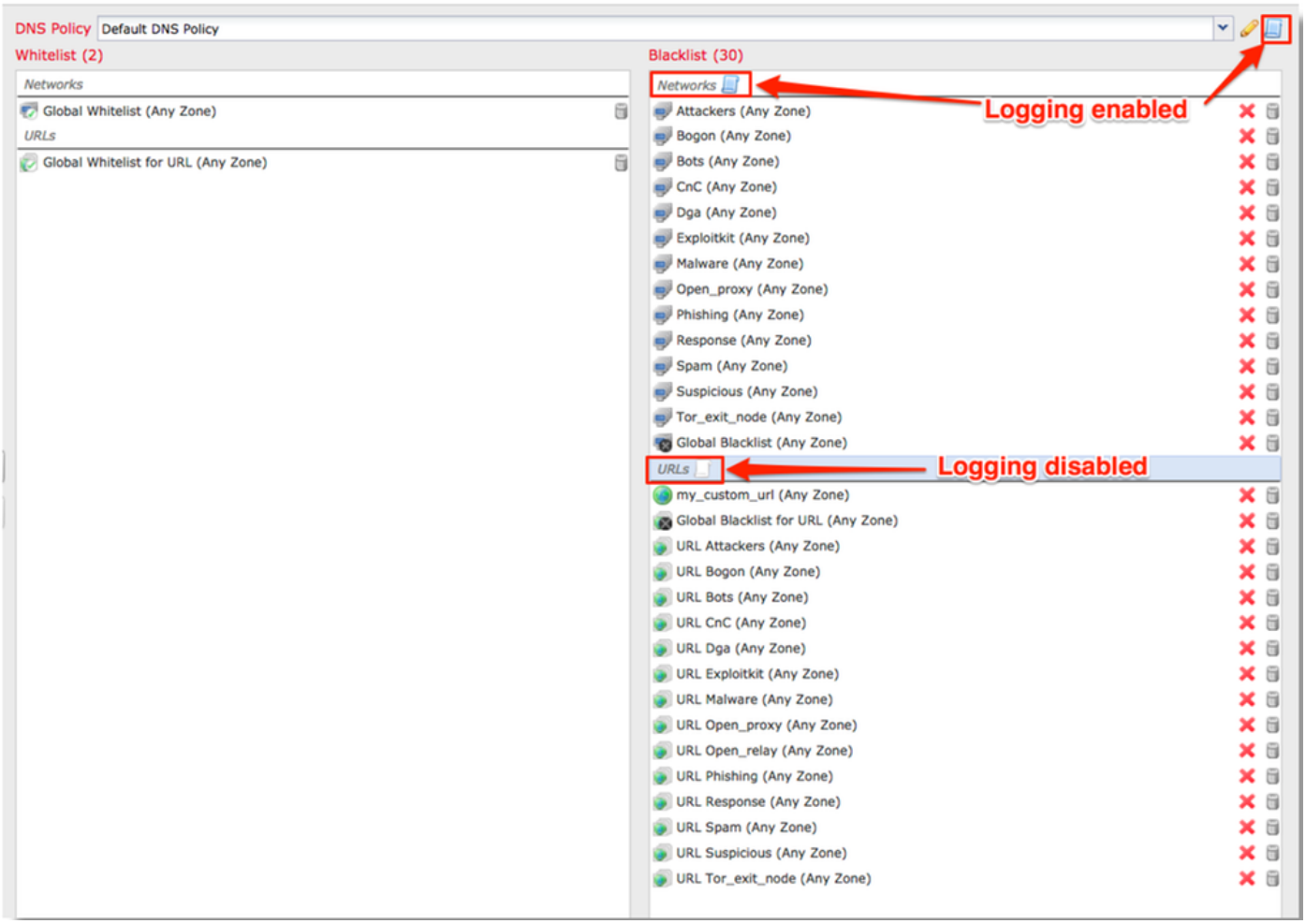
De reputatie van de veiligheidscontrole op basis van IP adressen is de eerste component binnen Firepower om het verkeer te inspecteren. URL- en DNS-beveiligingsinformatie wordt uitgevoerd zodra het betreffende toepassingsprotocol wordt ontdekt. Hieronder staat een schema met een overzicht van de computeruitslagen van de softwareinspectie van Firepower.



Bepaal dat vastlegging ingeschakeld is voor security intelligentie

gebeurtenissen

Blokken op het niveau van de veiligheidscontrole zijn heel makkelijk te bepalen zolang houtkap is ingeschakeld. Dit kan worden bepaald op de Firepower Management Center (FMC) gebruikersinterface (UI) door te navigeren naar **beleid > Toegangsbeheer > Toegangsbeheer > Toegangsbeheer**. Nadat u op het pictogram Bewerken naast het beleid in kwestie hebt geklikt, navigeer dan naar het tabblad **Security Intelligence**.



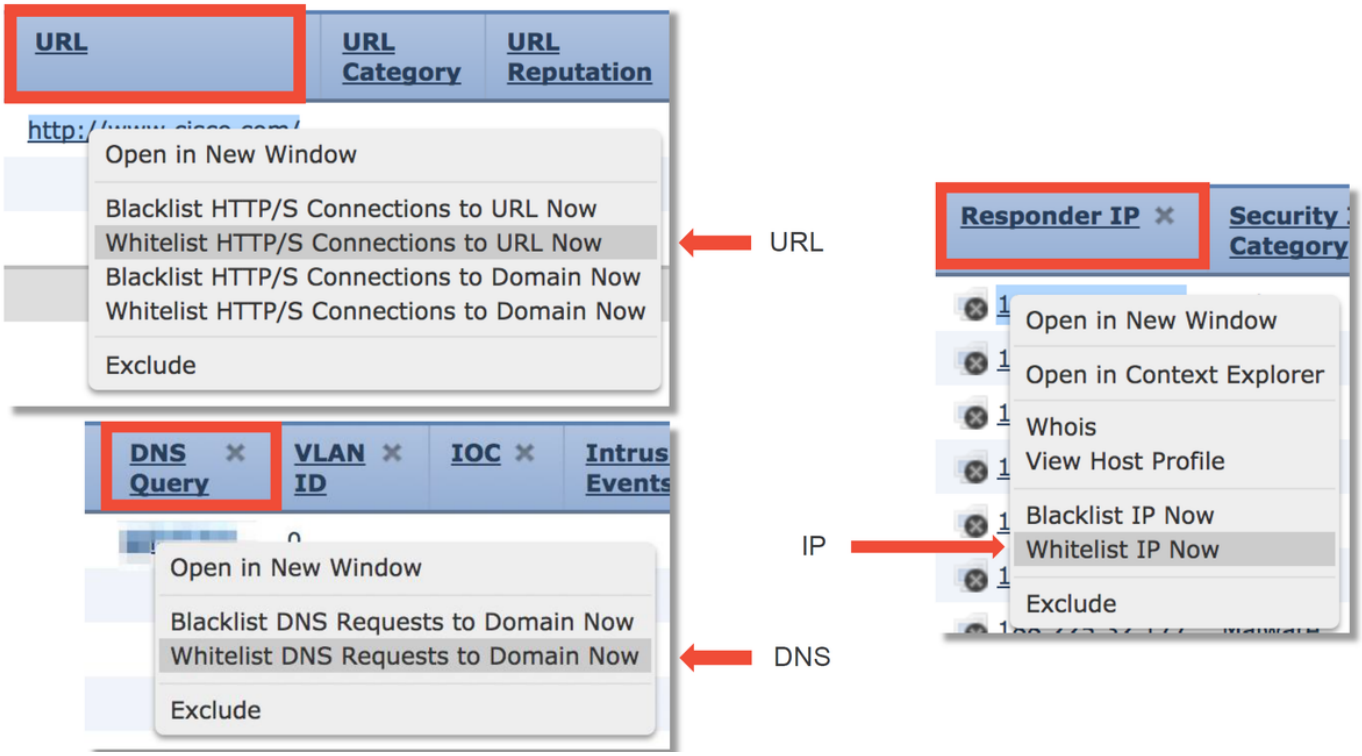
Bekijk de security Intelligence-gebeurtenissen

Als logging mogelijk is, kunt u de security intelligentie gebeurtenissen bekijken onder **Analyse > Connections > Security Intelligence events**. Het moet duidelijk zijn waarom het verkeer wordt geblokkeerd.

First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Security Intelligence Category
2017-05-16 17:00:16		Domain Not Found	DNS Block	192.168.1.95		DNS Response
2017-05-16 16:57:50	2017-05-16 16:57:50	Block	URL Block	192.168.1.95	10.83.48.40	my_custom_url
2017-05-16 16:50:05		Block	IP Block	192.168.1.95		Malware

Als een snelle mitigatiestap kunt u met de rechtermuisknop op de IP, URL of DNS Query die

geblokkeerd worden door de Security Intelligence-functie en een whitelist-optie kiezen.



Als u vermoedt dat iets niet correct op de zwarte lijst is geplaatst, of u wilt vragen om de reputatie te veranderen kunt u een ticket rechtstreeks met Cisco Talos openen op de volgende link:

https://www.talosintelligence.com/reputation_center/support

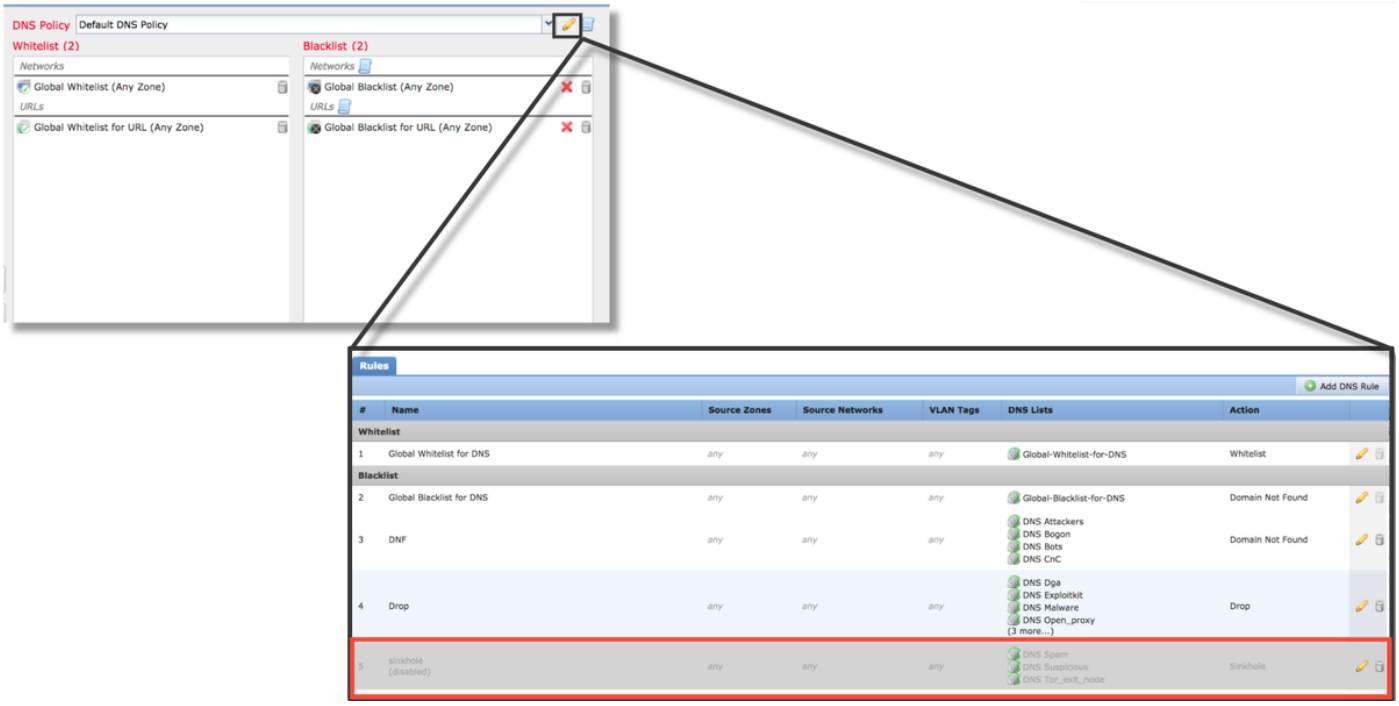
U kunt de gegevens ook leveren aan het Cisco Technical Assistance Center (TAC) om te onderzoeken of een item moet worden verwijderd van de zwarte lijst.

> Opmerking: Wanneer je aan de informant toevoegt, voeg je alleen een vermelding toe aan de whitelist van de veiligheidsinlichtingendienst, wat betekent dat het object de veiligheidscontrole mag doorgeven. Alle andere onderdelen van de vuurkracht kunnen echter nog steeds het verkeer inspecteren.

Configuraties van beveiligingsinlichtingen verwijderen

Om de veiligheidsinlichtingenconfiguraties te verwijderen, navigeer dan naar het tabblad **Security Intelligence**, zoals hierboven vermeld. Er zijn drie afdelingen. één voor netwerken, URL evenals een beleid voor DNS.

Van daaruit kunnen de lijsten en diervoeders worden verwijderd door op het trashcan-symbool te klikken.



Merk op dat in het bovenstaande screenshot alle IP- en URL-beveiligingslijsten zijn verwijderd, behalve de wereldwijde zwarte lijst en de witte lijst.

Binnen het DNS-beleid, dat is waar de DNS-beveiligingsconfiguratie is opgeslagen, is een van de regels uitgeschakeld.

> Opmerking: Om de inhoud van de Global Blacklists en Whitelists te bekijken, navigeer naar **Objecten > Objectbeheer > Security Intelligence**. Klik vervolgens op het gedeelte van het belang (Netwerk, URL, DNS). Het bewerken van een lijst geeft de inhoud weer, hoewel de configuratie moet worden uitgevoerd in het kader van het toegangsbeleid.

Controleer de configuratie op de achterzijde

De configuratie van de veiligheidscontrole kan op CLI worden geverifieerd via het **>** bevel **om toegang-controle-**configuratie **te tonen**, dat de inhoud van het actieve beleid van de Toegangscontrole op het apparaat van de Firepower toont.

```
> show access-control-config

==================[ My AC Policy ]==================
Description              :
Default Action            : Allow
Default Policy            : SOC
Logging Configuration
   DC                   : Enabled
   Beginning             : Disabled
   End                  : Enabled
Rule Hits                 : 0
Variable Set              : Default-Set

===[ Security Intelligence - Network Whitelist ]====
   Name                 : Global-Whitelist (List)
   IP Count             : 0
   Zone                 : any

===[ Security Intelligence - Network Blacklist ]====
Logging Configuration     : Enabled
   DC                   : Enabled


--------------------[ Block ]---------------------
   Name                 : Attackers (Feed)
   Zone                 : any

   Name                 : Bogon (Feed)
   Zone                 : any
…[omitted for brevity]
```

In het bovenstaande voorbeeld is duidelijk dat houtkap is geconfigureerd voor de Blacklist van het netwerk en dat er ten minste twee voedingen zijn opgenomen in de zwarte lijst (Attachments en Bogon).

Of een individueel item in een Security Intelligence lijst staat, kan worden bepaald in de deskundigenmodus. Zie de onderstaande stappen:

```
> expert
$ grep <ip.addr> /var/sf/iprep_download/*
/var/sf/iprep_download/23f2a124-8278-4c03-8c9d-d28fe08b5e98.blf:<ip.addr>

$ head -1 /var/sf/iprep_download/23f2a124-8278-4c03-8c9d-d28fe08b5e98.blf
#Cisco intelligence feed: Malware
```

← IP SI lists are in /var/sf/iprep_download/

```
$ grep <url> /var/sf/siurl_download/*
/var/sf/siurl_download/00000000-0000-0ed3-0000-073014445223.lf:<url>

$ head -1 /var/sf/siurl_download/00000000-0000-0ed3-0000-073014445223.lf
#URL object: my_custom_url
```

← URL SI lists are in /var/sf/siurl_download/

```
$ grep <dns.hostname> /var/sf/sidns_download/*
/var/sf/sidns_download/032ba433-c295-11e4-a919-d4ae5275b77b.lf: <dns.hostname>

$ head -1 /var/sf/sidns_download/032ba433-c295-11e4-a919-d4ae5275b77b.lf
#Cisco DNS and URL intelligence feed: DNS Response
```

← DNS SI lists are in /var/sf/sidns_download/

Er is een bestand voor elke lijst met veiligheidsgegevens met een unieke UID. Het bovenstaande voorbeeld toont hoe de naam van de lijst te identificeren, met behulp van de opdracht **head-n1**.

Gegevens om te leveren aan TAC

Gegevens	Instructies
Probleemoplossing van bestanden van het FMC en FirePOWER-apparaat die het verkeer controleren	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/1176
Screenshots van gebeurtenissen (met tijdzegels inbegrepen)	Zie dit artikel voor instructies
Tekstuitvoer van CLI-sessies	Zie dit artikel voor instructies
Als u een valse positieve case indient, specificeert u het onderwerp (IP, URL, domein) dat u wilt aanvechten.	Vermeld de redenen en bewijzen waarom het geschil moet worden gevoerd.

Volgende stap

Als is vastgesteld dat de veiligheidscomponent niet de oorzaak van de kwestie is, zou de volgende stap het oplossen van de regels van het toegangscontrolebeleid zijn.

Klik hier om verder te gaan met het volgende artikel.