Firepower Data Path Problemen opsporen en verhelpen fase 4: Toegangsbeheerbeleid

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 heeft betrekking op de vierde fase van de oplossing voor het FirePOWER-gegevenspad, het Access Control Policy (ACS). Deze informatie is van toepassing op alle momenteel ondersteunde FirePOWER-platforms en -versies.

Probleemoplossing voor de fase van het toegangscontrolebeleid (ACS)

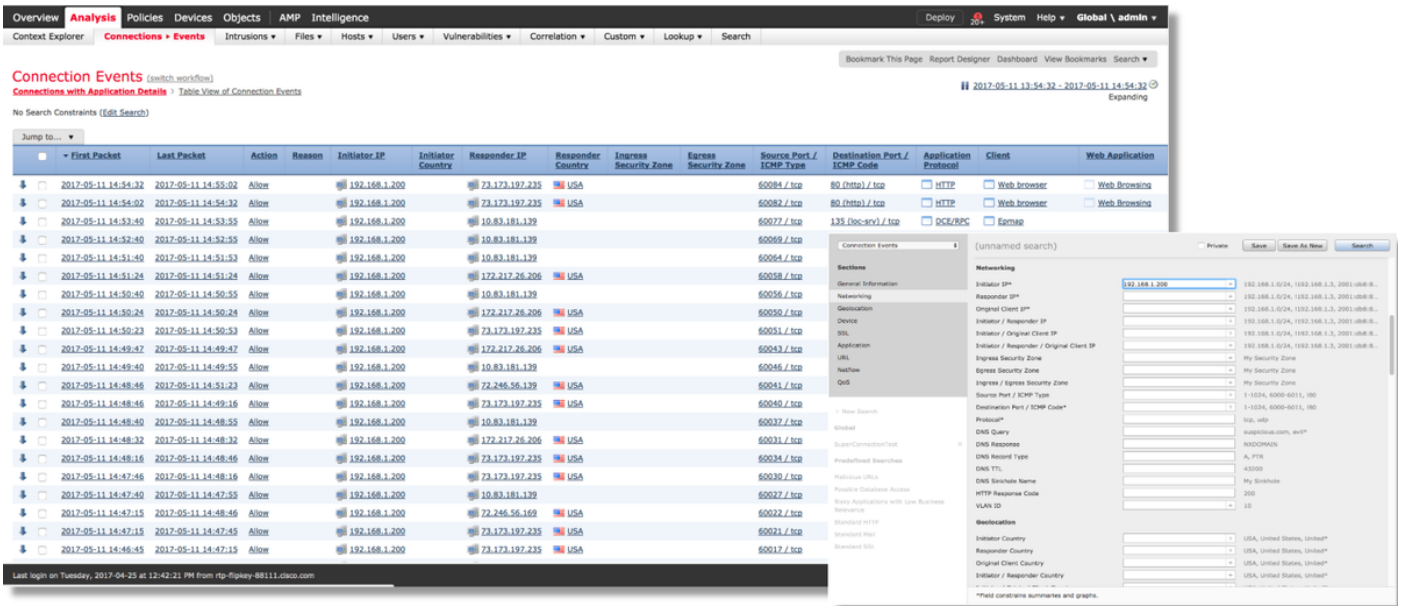
In het algemeen moet het vaststellen van welke ACS-regel een stroming op elkaar afgestemd wordt, vrij rechtuit zijn. De verbindingsgebeurtenissen kunnen worden herzien om te zien welke regel/actie wordt afgedwongen. Als dat niet duidelijk aantoont wat de ACS met het verkeer doet, kan het debuggen worden uitgevoerd op de Firepower Opdracht Line Interface (CLI).

Op aansluitingen controleren

Na het krijgen van een idee van de ingang en de spanning interface zou het verkeer zowel als de stroominformatie bij elkaar moeten passen, zou de eerste stap om te identificeren of Firepower de stroom blokkeert zijn om de verbindingsgebeurtenissen voor het betrokken verkeer te controleren.

U kunt deze informatie in het FireSIGHT Management Center bekijken onder **Analyse > Connecties > Evenementen.**

> Opmerking: Voordat u de verbindingsgebeurtenissen controleert, moet u ervoor zorgen dat houtkap is ingeschakeld in uw ACS-regels. Vastlegging is ingesteld in het tabblad "Vastlegging" binnen elke regel van het toegangsbeleid en in het tabblad Security Intelligence. Zorg ervoor dat de verdachte regels zijn ingesteld om de logbestanden naar het "Event Viewer" te sturen. Dit is ook van toepassing op de standaardinstelling.



Door op "Zoeken bewerken" te klikken en door een unieke bron (Initiator) IP te filteren, ziet u de stromen die door Firepower werden gedetecteerd. De kolom Actie toont "toestaan" voor het verkeer van deze gastheer.

Als Firepower bedoeld verkeer blokkeert, zal de Action het woord "Block" bevatten. Wanneer u op "Tabelweergave van verbindingsgebeurtenissen" klikt, worden er meer gegevens gegenereerd. De volgende velden in de verbindingsgebeurtenissen kunnen worden bekeken als de actie "Blok" is:

- Reden

- Toegangscontroleregels

Snelle beperking

Om snel een probleem op te lossen dat vermoedelijk het gevolg is van de ACS-regels, kunnen de volgende maatregelen worden genomen:

- Schep een regel met "vertrouwen" of "toestaan" voor het betreffende verkeer en plaats deze bovenaan de ACS-regels, of bovenal de algemene regels.
- schakelt tijdelijk alle regels uit met een actie die het woord "Blok" bevat
- Als de standaardoptie is ingesteld op "Alle verkeer blokkeren", moet u deze tijdelijk overzetten op "Alleen netwerkontdekking"

> Opmerking: Deze snelle verzachting vereist beleidswijzigingen die mogelijk niet in alle

omgevingen mogelijk zijn. Aanbevolen wordt om eerst te proberen om sporen van systeemondersteuning te gebruiken om te bepalen welke regel het verkeer bij elkaar past voordat u het beleid wijzigt.

Ontduiking van de ACS-landen

Verdere problemen oplossen bij de ACS-operaties kan worden uitgevoerd via het CLI-hulpprogramma **voor systeemondersteuning**.

Opmerking: Op de platforms Firepower 9300 en 4100 kan de shell in kwestie worden benaderd via de volgende opdrachten:

 # sluit module 1 console aan
Firepower-module1> **verbinding-ftd**
>

Voor meerdere instellingen kan het logische apparaat CLI worden benaderd met de volgende opdrachten.
 # connect module 1 telnet
Firepower-module1> **verbinding ftd1**
Vet "exit" in om terug te keren naar CLI voor Opstarten
>

Het **systeem-ondersteuning** van **firewalls-machine-debug**-gebruik heeft een ingang voor elk pakket dat door de ACS-landen wordt geëvalueerd. Het laat zien dat het proces van evaluatie van de regels plaatsvindt, en waarom een regel wordt gematcht of niet wordt gematcht.

Opmerking: In versie 6.2 en hoger kan het **systeemondersteunende** traceringstool worden uitgevoerd. Het gebruikt dezelfde parameters maar bevat meer details. Vergeet niet 'y' in te voeren als dit wordt gevraagd met **ook "Schakel** de **firewall-motor uit?"**.

Voorbeeld 1: Verkeer komt overeen met een vertrouwensregel

In het onderstaande voorbeeld wordt het opzetten van een SSH-sessie geëvalueerd met behulp van **systeemondersteuning firewall-engine-debug**.

Dit is de ACS die op het FirePOWER-apparaat draait.

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN ...	Users	Applic...	Sourc...	Dest P...	URLs	ISE/S... Attrib...	Acti...
Mandatory - JG AC (all) (1-6)													
1	Trust ssh for host	Any	Any	192.168.0.7	Any	Any	Any	Any	Any	SSH	Any	Any	Trust
2	inspect	Any	Any	10.0.0.0/8	Any	Any	Any	Any	Any	Any	Any	Any	Allow
3	trust server backup	Any	Any	192.168.62.3	10.123.175.22	Any	Any	Any	Any	Any	Any	Any	Trust

De ACS-landen hebben drie regels.

1. De eerste regel is het vertrouwen van elk verkeer vanaf 192.168.0.7 met de bestemmingspoorten die door SSH worden gebruikt.

2. De tweede regel inspecteert al verkeer dat afkomstig is van 10.0.0.0/8 waarin de netwerkcriteria overeenkomen op basis van de XFF header gegevens (zoals aangegeven door het pictogram naast het netwerkobject)
3. De derde regel vertrouwt al het verkeer van 192.168.62.3 tot 10.123.175.22

In het scenario voor het oplossen van problemen wordt een SSH-verbinding van 192.168.62.3 tot 10.123.175.22 geanalyseerd.

De verwachting is dat de sessie overeenkomt met AC regel 3 "back-up van vertrouwensserver". De vraag is hoeveel pakketten het voor deze sessie zou moeten nemen om deze regel aan te passen. Is alle informatie nodig in het eerste pakket om de AC-regel te bepalen of zijn er meerdere pakketten nodig, en als dat zo is, hoeveel?

Op de FirePOWER CLI wordt het volgende ingevoerd om te zien hoe de ACS-regel wordt geëvalueerd.

```
>system support firewall-engine-debug

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.62.3
Please specify a client port:
Please specify a server IP address: 10.123.175.22
Please specify a server port: 22
Monitoring firewall engine debug messages
```

> **Tip**: Het is best om zoveel mogelijk parameters in te vullen wanneer **firewall-engine-debug wordt** uitgevoerd, zodat alleen de interessante debug-berichten naar het scherm worden afgedrukt.

In de debug uitvoer hieronder ziet u de eerste vier pakketten van de sessie die worden geëvalueerd.

SYN

SYN,ACK

KRIJGEN

Eerste SSH-pakket (client naar server)

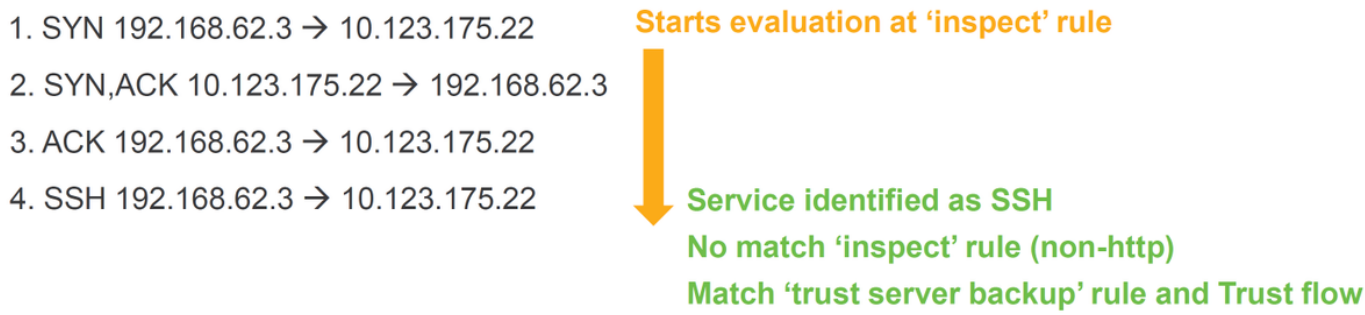
```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 846, payload -1, client 2000000846, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
```

Dit is een grafiek die verder de Debug-logica illustreert.



Voor deze stroom duurt het 4 pakketten zodat het apparaat aan de regel voldoet.

Dit is een gedetailleerde verklaring van de debug uitvoer.

- Het ACS-evaluatieproces begint met de "inspect"-regel, omdat de "trust ssh for host"-regel niet werd afgestemd, aangezien het IP-adres niet aan de eis voldeed. Dit is een snelle overeenkomst vanwege alle informatie die nodig is om te bepalen of deze regel moet worden aangepast is aanwezig in het eerste pakket (IP's en poorten)
- Het kan niet worden bepaald of het verkeer overeenkomt met de "inspectie"-regel totdat de toepassing is geïdentificeerd, aangezien de X-Forwarded-For (XFF) informatie wordt gevonden in het HTTP-toepassingsverkeer, is de toepassing nog niet bekend, dus dit zet de sessie in een hangende status voor regel 2, in afwachting van toepassingsgegevens.
- Zodra de toepassing in het vierde pakket is geïdentificeerd, resulteert de "inspect"-regel in een niet-overeenkomend product, omdat de toepassing SSH in plaats van HTTP is
- De regel "backup server-back-up" van de trust is dan aangepast, op basis van de IP-adressen.

Samengevat duurt de verbinding 4 pakketten om de sessie aan te passen omdat het op de firewall moet wachten om de toepassing te identificeren aangezien regel 2 een toepassingsbeperking heeft.

Als regel 2 alleen bronnetwerken had en het geen XFF was, dan had dit 1 pakje nodig om de sessie aan te passen.

U dient altijd de regels van lagen 1-4 boven alle andere regels in het beleid te plaatsen wanneer mogelijk, aangezien deze regels doorgaans 1 pakje vereisen om een beslissing te nemen. U kunt echter ook opmerken dat zelfs met slechts lagen 1-4 regels het meer dan slechts 1 pakket kan zijn om een AC-regel aan te passen en dat de reden hiervoor URL/DNS-security intelligentie is. Als u één van deze machtigt, moet de firewall de toepassing voor alle sessies bepalen die door het AC beleid worden geëvalueerd omdat het moet bepalen of zij HTTP of DNS zijn. Dan moet zij bepalen of zij de sessie op basis van de zwarte lijsten moet toestaan.

Hieronder staat een ingekapselde uitvoer van de opdracht **firewall-motor-debug**, die de relevante velden in rood heeft gemarkeerd. Let op de opdracht die wordt gebruikt om de naam van de applicatie te verkrijgen die geïdentificeerd is.

```
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId

[…omitted for brevity]

192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 846, payload -1, client 2000000846, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-46594 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust


[! How to map service/application ID to name]
> expert
$ grep "^846[^0-9]" /var/sf/appid/odp/appMapping.data
846 SSH 32 0 0 ssh
```

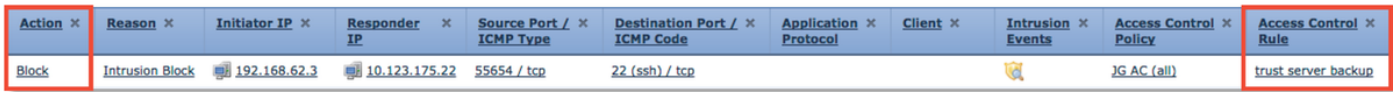
Voorbeeld 2: Verkeersovereenstemming met een vertrouwensregel is geblokkeerd

In sommige scenario's kan het verkeer worden geblokkeerd, ondanks de overeenstemming van een vertrouwensregel in de ACS-landen. Het onderstaande voorbeeld evalueert verkeer met het zelfde toegangscontrolebeleid en hosts.

```
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 New session
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 4, 'inspect', and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0,
inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 pending rule order 4, 'inspect', XFF wait for AppId
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Deleting session

[!Session was deleted because we hit a drop IPS rule and blacklisted the flow.
This happened before AC rule was matched (Intrusion policy before AC rule match dropped).
Firewall engine will re-evaluate from top of AC policy to find a rule for logging decision]

192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 Starting with minimum 0, id 0 and IPProto first with zones 1 -> 2, geo 0 -> 0, vlan 0, inline
sgt tag: 0, ISE sgt id: 0, svc -1, payload -1, client -1, misc -1, user 9999997, icmpType 102, icmpCode 22
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 3, 'Trust ssh for host', src network and GEO
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 no match rule order 4, 'inspect', XFF non-http
192.168.62.3-54650 > 10.123.175.22-22 6 AS 1 I 0 match rule order 5, 'trust server backup', action Trust
```



Zoals hierboven te zien is, toont de **firewall-motor-debug** uitvoer aan dat het verkeer overeenkomt met een "vertrouwen", terwijl de verbindingsgebeurtenissen actie van **Blok** laten zien door een regel van het inbraakbeleid (bepaald omdat de kolom van de Reason **Inbraakblok** toont).

Dit kan gebeuren omdat het **inbraakbeleid** is **gebruikt voordat de toegangscontroleregel wordt bepaald** Instellen in het **tabblad Geavanceerd** op de ACS-landen. Voordat het verkeer op basis van de regel kan worden aangestuurd, identificeert het betrokken Inbraakbeleid een patroonmatch en laat het verkeer vallen. De evaluatie van de ACS-regel resulteert echter in een overeenstemming met de vertrouwensregel, aangezien de IP-adressen voldeden aan de criteria van de "trust server back-up"-regel.

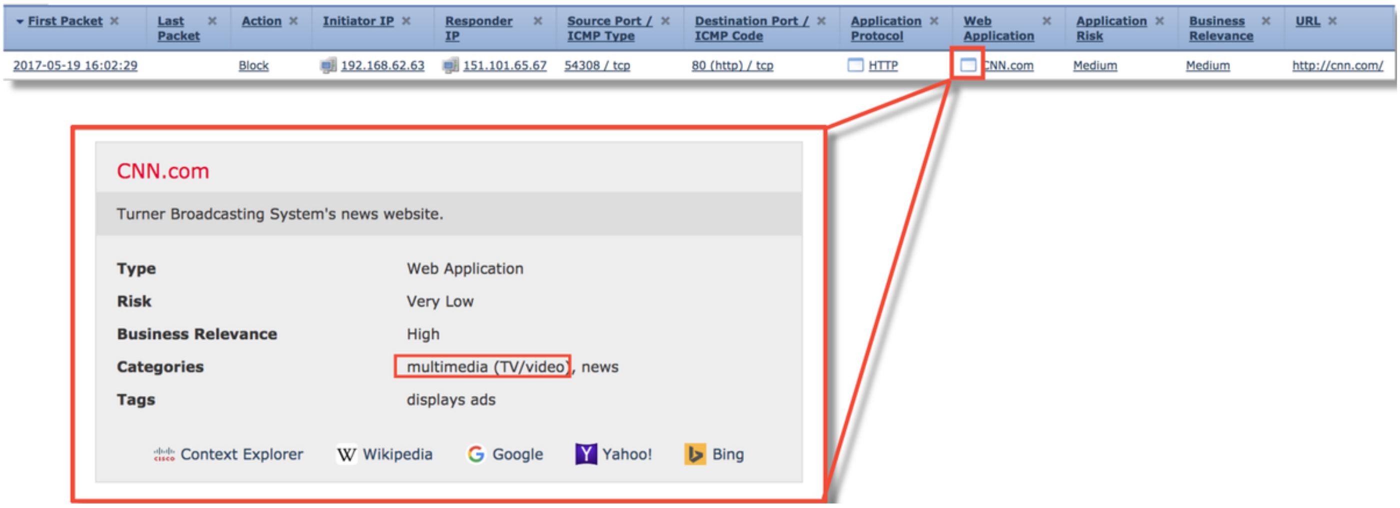
Om ervoor te zorgen dat het verkeer geen inbraakbeleid ondergaat, kan de vertrouwensregel boven de "inspectie"-regel worden geplaatst, wat in beide gevallen een goede praktijk zou zijn. Aangezien de identificatie van de toepassing noodzakelijk is voor een match of non-match van de "inspectie"-regel, **wordt** het **inbraakbeleid dat vóór de toegangscontroleregel wordt gebruikt** gebruikt voor verkeer dat door hetzelfde wordt beoordeeld. Het plaatsen van de "steun van de server van het vertrouwen" regel boven de "inspect" regel veroorzaakt het verkeer om de regel aan te passen wanneer het eerste pakket wordt gezien aangezien de regel op IP adres gebaseerd is, dat in het eerste pakket kan worden bepaald. Daarom **is** het **inbraakbeleid dat wordt gebruikt**

voor de toegangscontrole niet nodig.

Scenario 3: Verkeer geblokkeerd door toepassingslabel

In dit scenario melden gebruikers dat CNN.com wordt geblokkeerd. Er is echter geen specifieke regel die CNN blokkeert. De gebeurtenissen van de verbinding, in combinatie met **firewall-motor-debug** uitvoer, tonen de reden voor het blok.

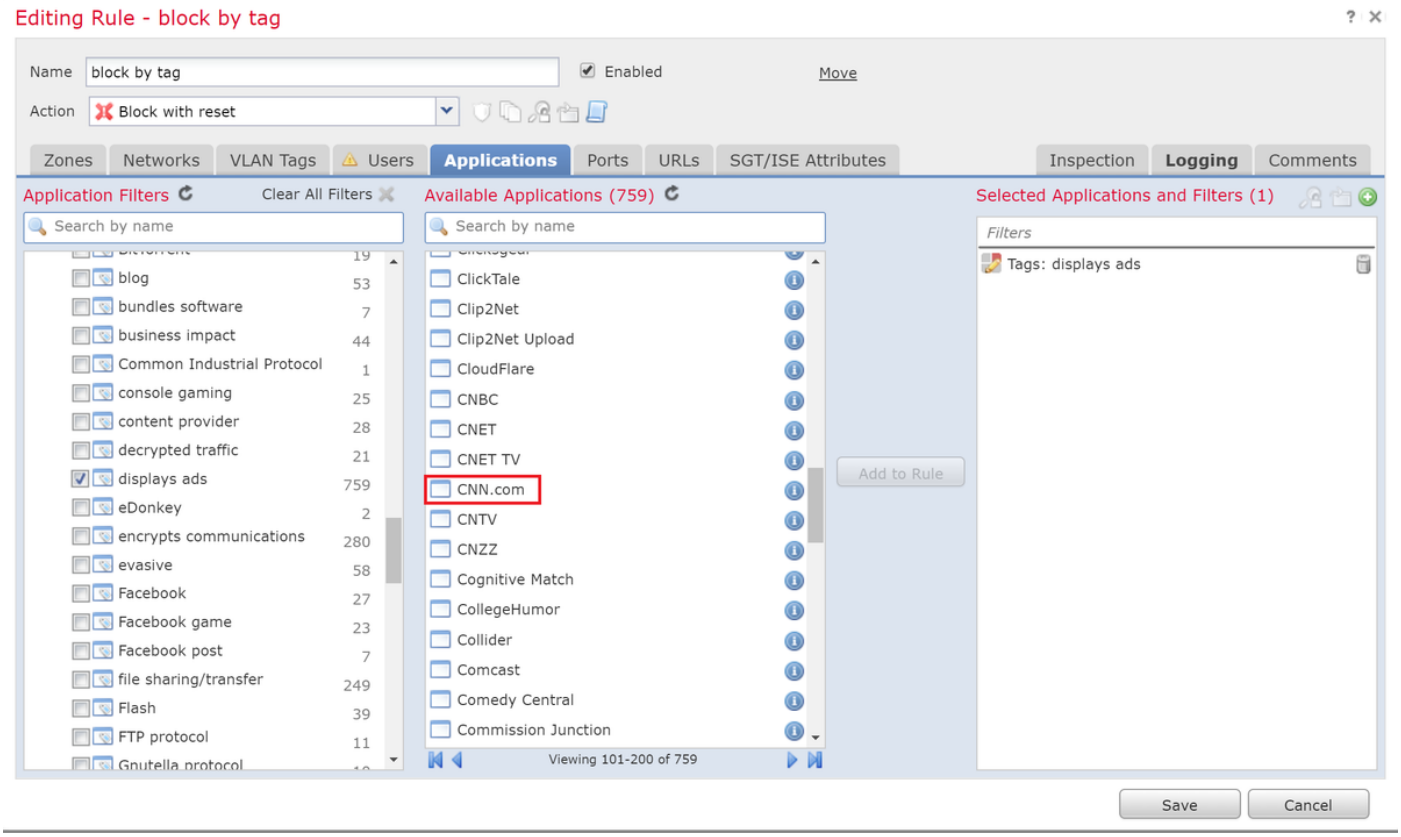
Eerst heeft de verbinding gebeurtenissen een informatievak naast de toepassingsvelden die informatie over de toepassing en hoe Firepower de genoemde toepassing categoriseert, bevat.



Met deze informatie in gedachten wordt **firewall-engine-debug** uitgevoerd. In de debug-uitvoer wordt het verkeer geblokkeerd op basis van de toepassingstag.

```
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 New session
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0 -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0, payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 pending rule order 4, 'block by tag', AppID
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 URL SI: ShmDBLookupURL("http://cnn.com/") returned 0
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Starting with minimum 4, 'block by tag', and SrcZone first with zones 1 -> 2, geo 0(0) -> 0,
vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 676, payload 1190, client 638, misc 0, user 9999997, url http://cnn.com/, xff
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 match rule order 4, 'block by tag', action Block
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 sending block response of 605 bytes
192.168.62.63-54308 > 151.101.65.67-80 6 AS 1 I 0 Deleting session
```

Ook al is er geen regel die expliciet http://cnn.com blokkeert, wordt de **gelabelde** advertenties geblokkeerd in het **tabblad Toepassingen** van een ACS-regel.



Gegevens om te leveren aan TAC

Gegevens	Instructies
Probleemoplossing bestand via het FirePOWER-apparaat dat het verkeer controleert	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/1
systeemondersteuning voor firewall-motor-debug en **systeemondersteunende** uitvoer	Zie dit artikel voor instructies
Uitvoer van toegangsbeheerbeleid	Navigeren in op **Systeem > Gereedschappen > Importeren / Exporteren**, selecte de knop **Exporteren**

> **Voorzichtig:** Indien de ACS een SSL-beleid bevat, verwijdert u het SSL-beleid van de ACS-landen alvorens te exporteren om gevoelige PKI-informatie te vermijden

Volgende stap: Probleemoplossing voor de SSL-beleidslaag

Als een SSL Policy in gebruik is en de probleemoplossing bij toegangsbeheer het probleem niet heeft blootgelegd, is de volgende stap de probleemoplossing in het SSL-beleid.

Klik hier om verder te gaan met het volgende artikel.