Firepower Data Path: probleemoplossing: Overzicht

Inhoud

Inleiding

Deze handleiding is bedoeld om snel te bepalen of een FirePOWER-apparaat (Firepower Threat Defense, FTD) of Adaptieve security applicatie (ASA) met FirePOWER Services een probleem veroorzaakt met netwerkverkeer. Tevens helpt het bedrijf bij het beperken van de vraag welke FirePOWER-component(s) moet(en) worden onderzocht en welke gegevens moeten worden verzameld voordat u het Cisco Technical Assistance Center (TAC) inschakelen.

Lijst met alle artikelen van de reeks van de het Problemen opsporen en verhelpen van het pad van Firepower.

Firepower Data Path Problemen opsporen en verhelpen fase 1: PacketIngress

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214574-firepower-data-path-troubleshooting-phas.html

Firepower Data Path Problemen opsporen en verhelpen fase 2: DAQ-laag
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214575-firepower-data-path-troubleshooting-phas.html

Firepower Data Path Problemen opsporen en verhelpen fase 3: Security Intelligentie
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214576-firepower-data-path-troubleshooting-phas.html

Firepower Data Path Problemen opsporen en verhelpen fase 4: Toegangsbeheerbeleid
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214577-firepower-data-path-troubleshooting-phas.html

Firepower Data Path Problemen opsporen en verhelpen fase 5: SSL-beleid
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214581-firepower-data-path-troubleshooting-phas.html

Firepower Data Path Problemen opsporen en verhelpen fase 6: Actieve verificatie
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/214608-firepower-data-path-troubleshooting-phas.html

Firepower Data Path Problemen opsporen en verhelpen fase 7: Inbraakbeleid
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214609-firepower-data-path-troubleshooting-phas.html

Firepower Data Path Problemen opsporen en verhelpen fase 8: Beleid voor netwerkanalyse

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214610-firepower-data-path-troubleshooting-phas.html

Voorwaarden

- Dit artikel gaat ervan uit dat er een basisbegrip is van de FTD- en ASA-platforms.
- Kennis van opensource wordt aanbevolen, maar niet vereist.

Bezoek de pagina met de routekaart voor de documentatie voor een compleet overzicht van de documentatie van de documentatie.

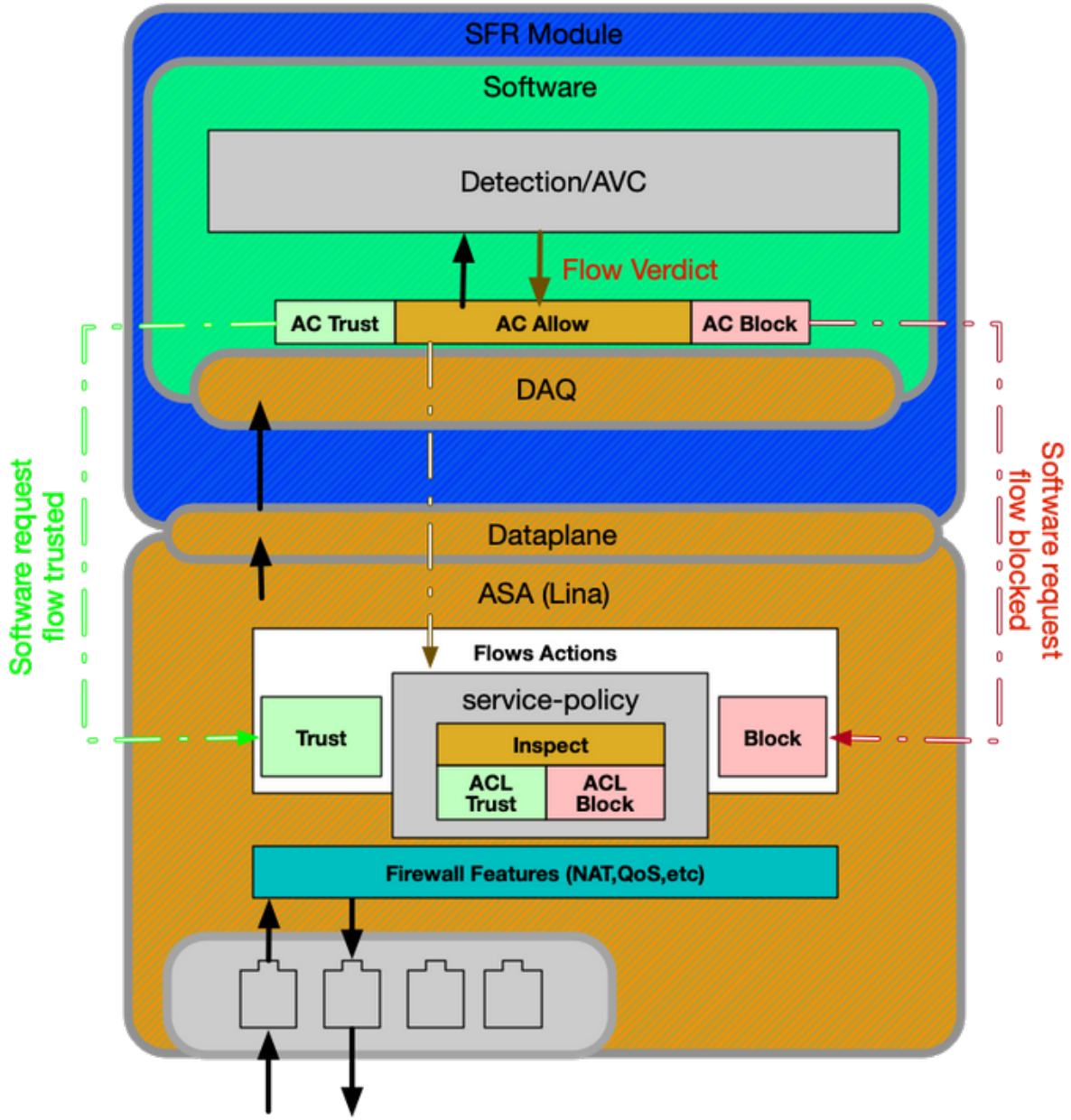
Architecturaal Overzicht van het pad

In het volgende gedeelte wordt gekeken naar het architectonische gegevenspad voor verschillende FirePOWER-platforms. Met de architectuur in gedachten, zullen we dan overgaan op hoe snel te bepalen of het Firepower apparaat de verkeersstroom blokkeert.

> Opmerking: Dit artikel heeft geen betrekking op de bestaande Firepower 7000- en 8000-series-apparaten, noch op het NGIPS (niet-FTD) virtuele platform. Kijk op onze TechNotes-pagina voor informatie over het oplossen van die platforms.

ASA met FirePOWER Services (SFR) platform

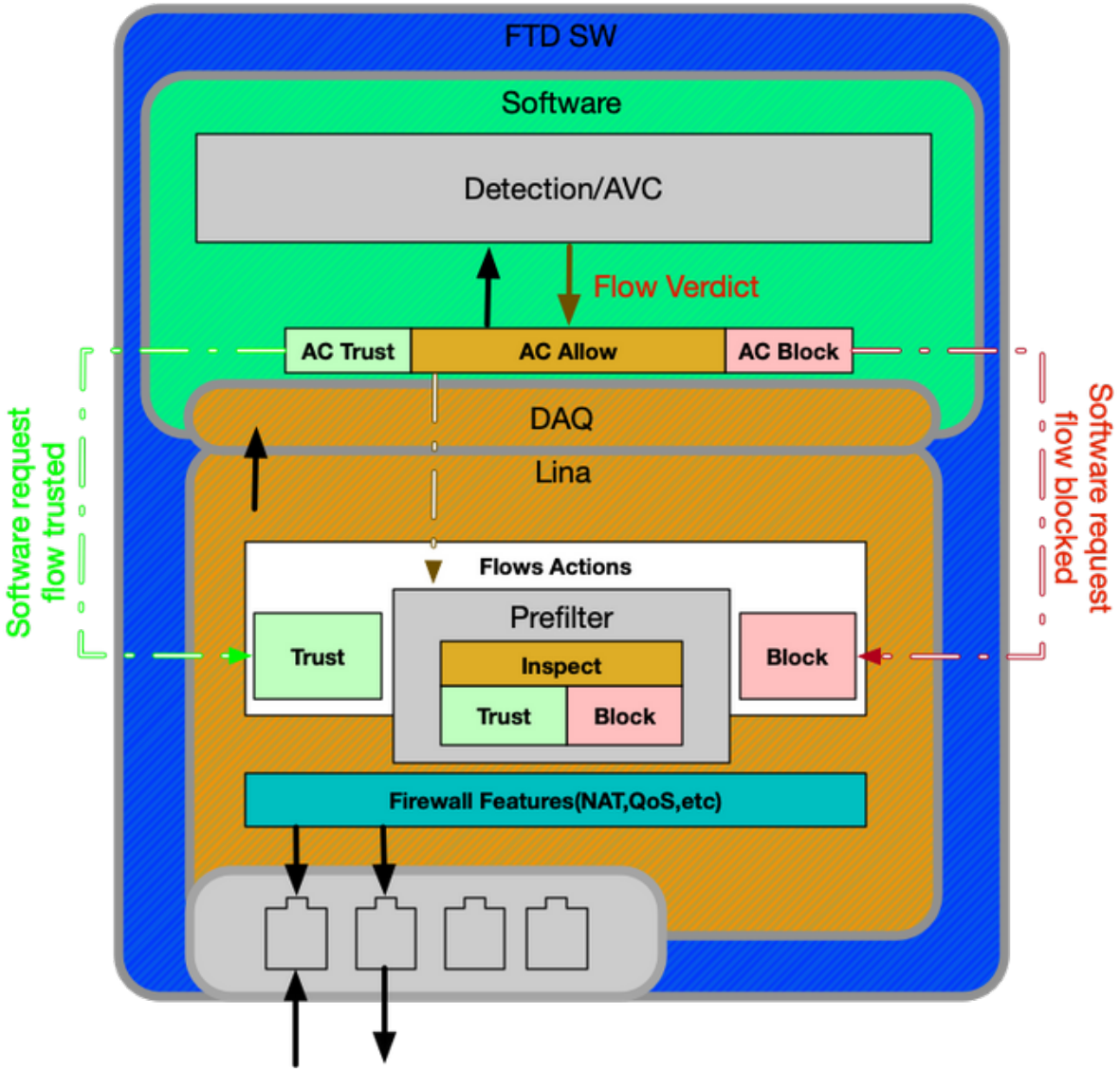
Het FirePOWER Services platform wordt ook SFR-module genoemd. Dit is eigenlijk een virtuele machine die werkt op 5500-X ASA-platforms.



Het dienstverleningsbeleid van de ASA bepaalt welk verkeer naar de SFR-module wordt gestuurd. Er is een dataplane-laag die wordt gebruikt om te communiceren met de DAQ-motor (Firepower Data Acquisition), die wordt gebruikt om pakketten te vertalen op een manier die snort kan begrijpen.

Firepower Threat Defense op ASA500-X en Virtual FTD-platform

Het FTD-platform bestaat uit één enkel beeld dat zowel de Lina (ASA) als de Firepower code bevat. Een belangrijk verschil tussen dit en de ASA met het SFR modulair platform is dat er efficiëntere communicatie tussen Lina en snort is.

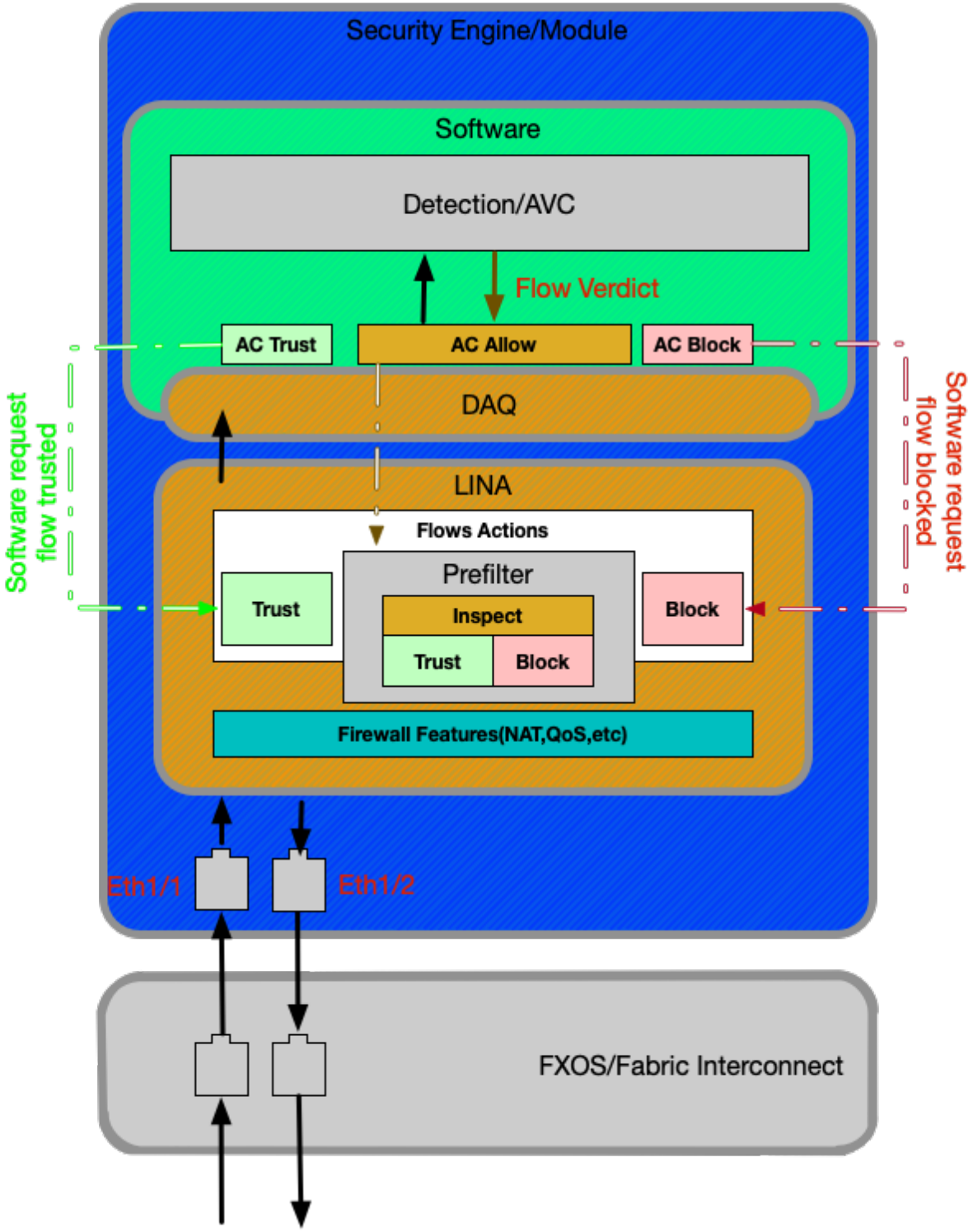


FTD op SSP-platforms

Op de SSP-modellen (Security Service Platforms) draait de FTD-software boven op het FXOS-platform (Firepower eXtensible Operative System), dat een onderliggend besturingssysteem is dat wordt gebruikt om de hardware van het chassis te beheren en verschillende toepassingen te host die bekend staan als logische apparaten.

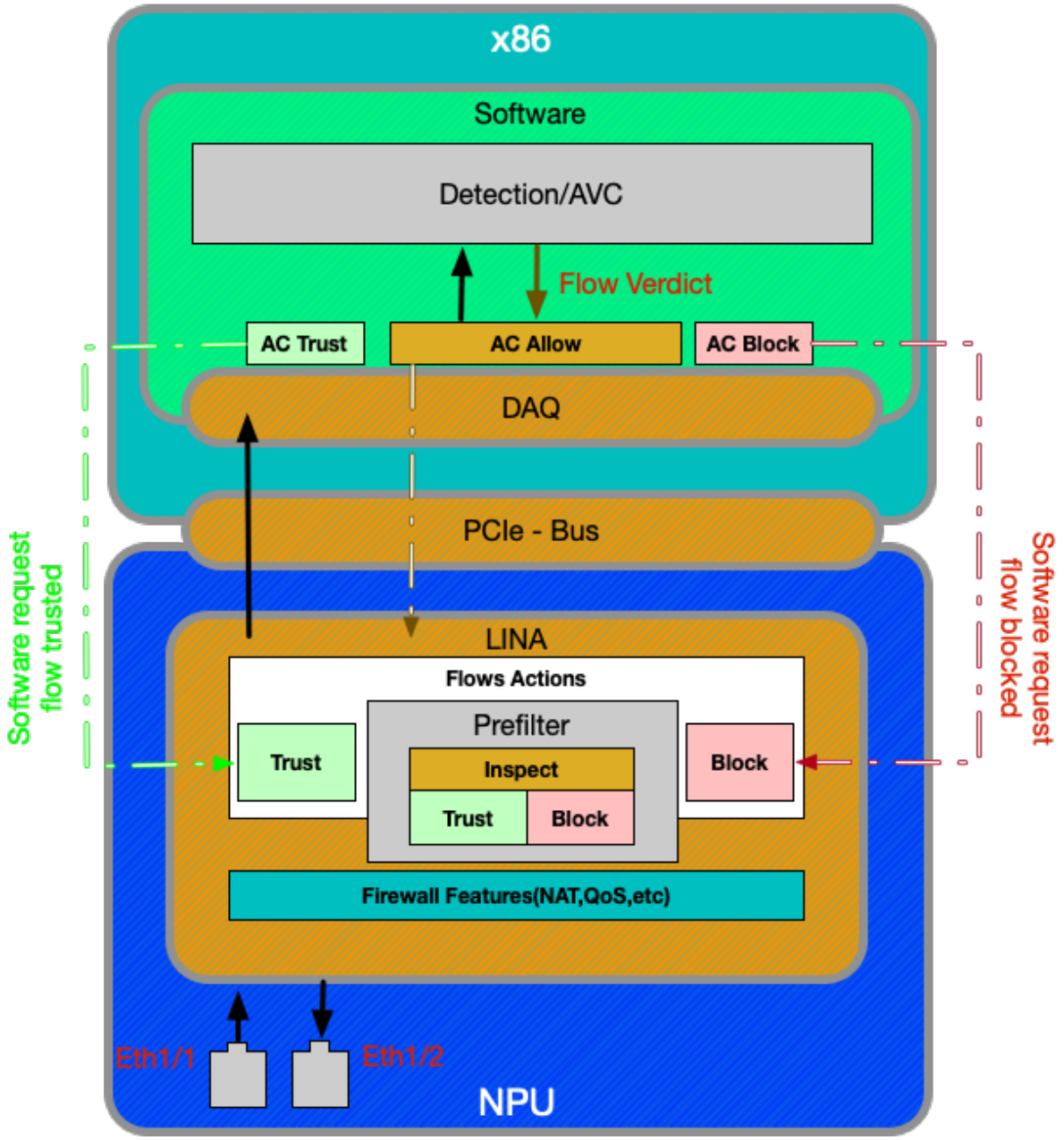
Binnen het SSP - platform zijn er enkele verschillen tussen modellen, zoals te zien is in de onderstaande diagrammen en beschrijvingen.

Firepower 9300 en 4100 applicaties



Op de FirePOWER 9300 en 4100 platforms, worden het inladen en het repareren van pakketten behandeld door een schakelaar die door de FXOS firmware wordt aangedreven (Fabric Interconnect). De pakketten worden dan verzonden naar de interfaces die aan het logische apparaat (in dit geval, FTD) worden toegewezen. Daarna is pakketverwerking hetzelfde als bij de niet-SSP FTD-platforms.

Firepower 2100 applicaties



Firepower 2100 apparaat werkt net als de niet-SSP FTD platforms. Het bevat niet de fabric interconnect-laag die aanwezig is op de 9300- en 4100-modellen. Er is echter een groot verschil in de 2100-series-apparaten ten opzichte van de andere apparaten, namelijk de aanwezigheid van de specifieke schakelingen (ASIC). Alle traditionele ASA-functies (LAN) worden uitgevoerd op de ASIC en alle Next-generation firewallfuncties (NGFW) (snort, URL-filtering, enzovoort) worden uitgevoerd op de traditionele x86-architectuur. De manier waarop Lina en Snort op dit platform communiceren is via een Perifere Component Interconnect Express (PCIe) via een pakketwachtrij, in tegenstelling tot de andere platforms die Direct Memory Access (DMA) gebruiken om pakketten in de rij te zetten om te sorteren.

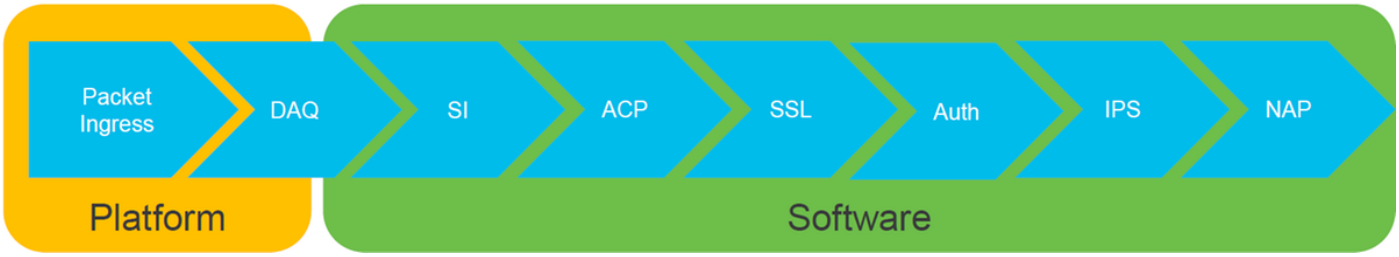
> Opmerking: Dezelfde methoden voor het oplossen van problemen met de FTD niet-SSP-platforms worden gevolgd op het FPR-2100 platform.

Aanbevolen proces voor probleemoplossing in FirePOWER Data-Path

Nu we hebben besproken hoe we uniek verkeer kunnen identificeren zowel als de

basisgegevenspadarchitectuur in Firepower platforms, kijken we nu naar de specifieke plaatsen waar pakketten kunnen worden ingetrokken. Er zijn acht basiscomponenten die in de artikelen van het Pad van Gegevens worden behandeld, die systematisch problemen kunnen oplossen om mogelijke pakketdalingen te bepalen. Deze omvatten:

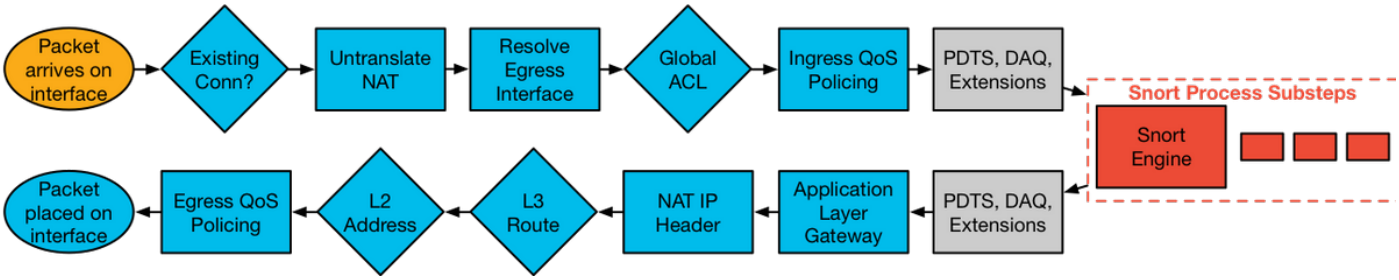
1. PacketIngress
2. Firepower DAQ-laag
3. Security Intelligentie
4. Toegangsbeheerbeleid
5. SSL-beleid
6. Functies voor actieve verificatie
7. Inbraakbeleid (IPS-regels)
8. Network Analysis Policy (gesorteerde voorprocessorinstellingen)



> Opmerking: Deze componenten zijn niet in de exacte volgorde van bewerkingen op FirePOWER-verwerking vermeld, maar worden geordend volgens onze aanbevolen werkstroomoplossing. Zie afbeelding hieronder voor het feitelijke pad van het pakketschema.

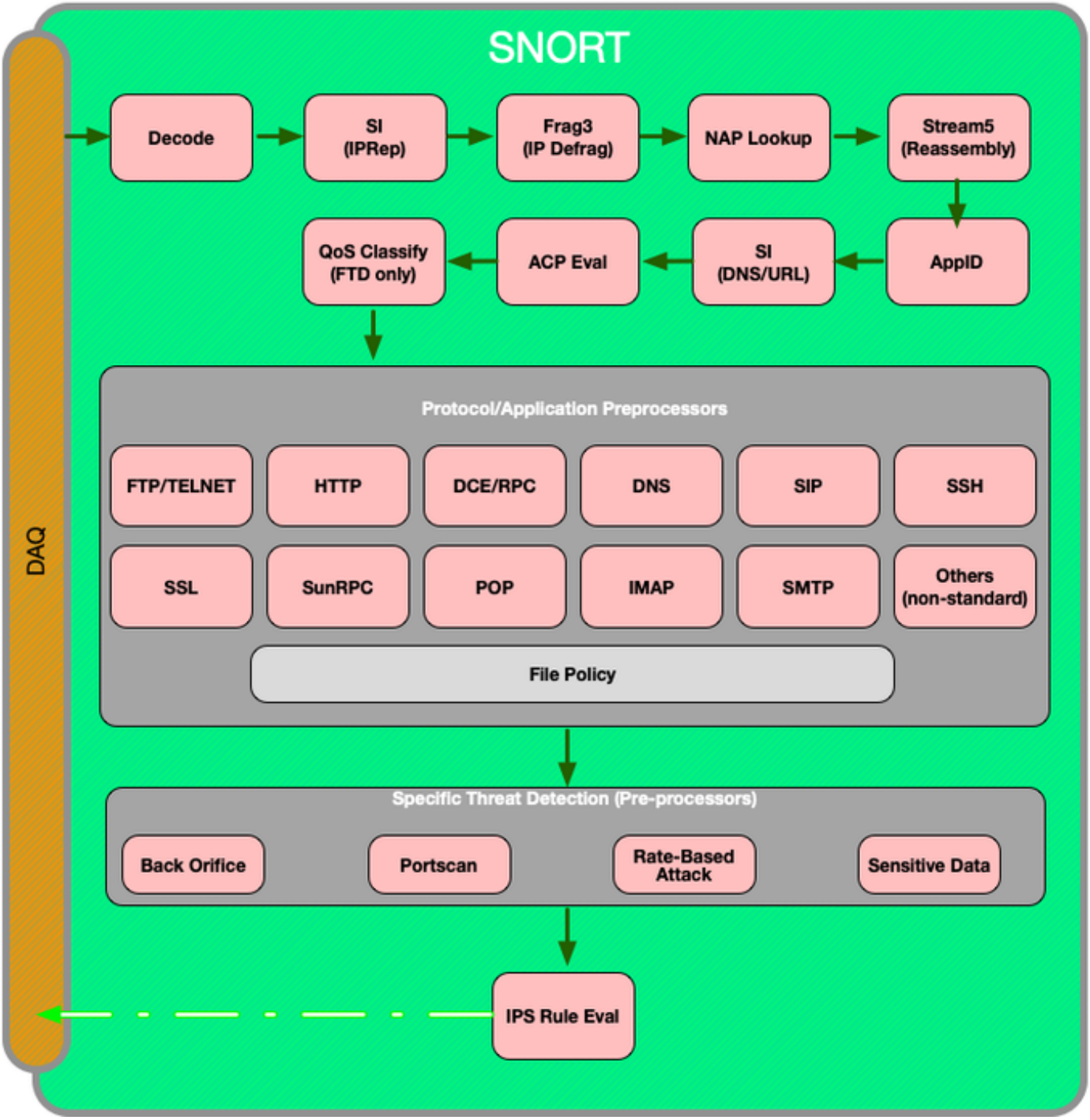
Feitelijk pad van het pakket door middel van FTD

De onderstaande illustratie toont het werkelijke pad van het pakket terwijl het door FTD loopt.



Snort pakketpad

De onderstaande illustratie toont het pad van het pakje door de Snort-machine.



PacketIngress en eieren

De eerste stap voor het opsporen van problemen bij het gegevenspad is om ervoor te zorgen dat er geen druppels voorkomen in het inloop- of voortgangsstadium van de pakketverwerking. Als een pakje probeert te knipperen maar niet, dan kunt u er zeker van zijn dat het pakje op een bepaalde plaats in het datapad door het apparaat is gevallen.

Dit artikel loopt door hoe te om pakketingang en stress op de systemen van de Vuurkracht te regelen.

Firepower DAQ-laag

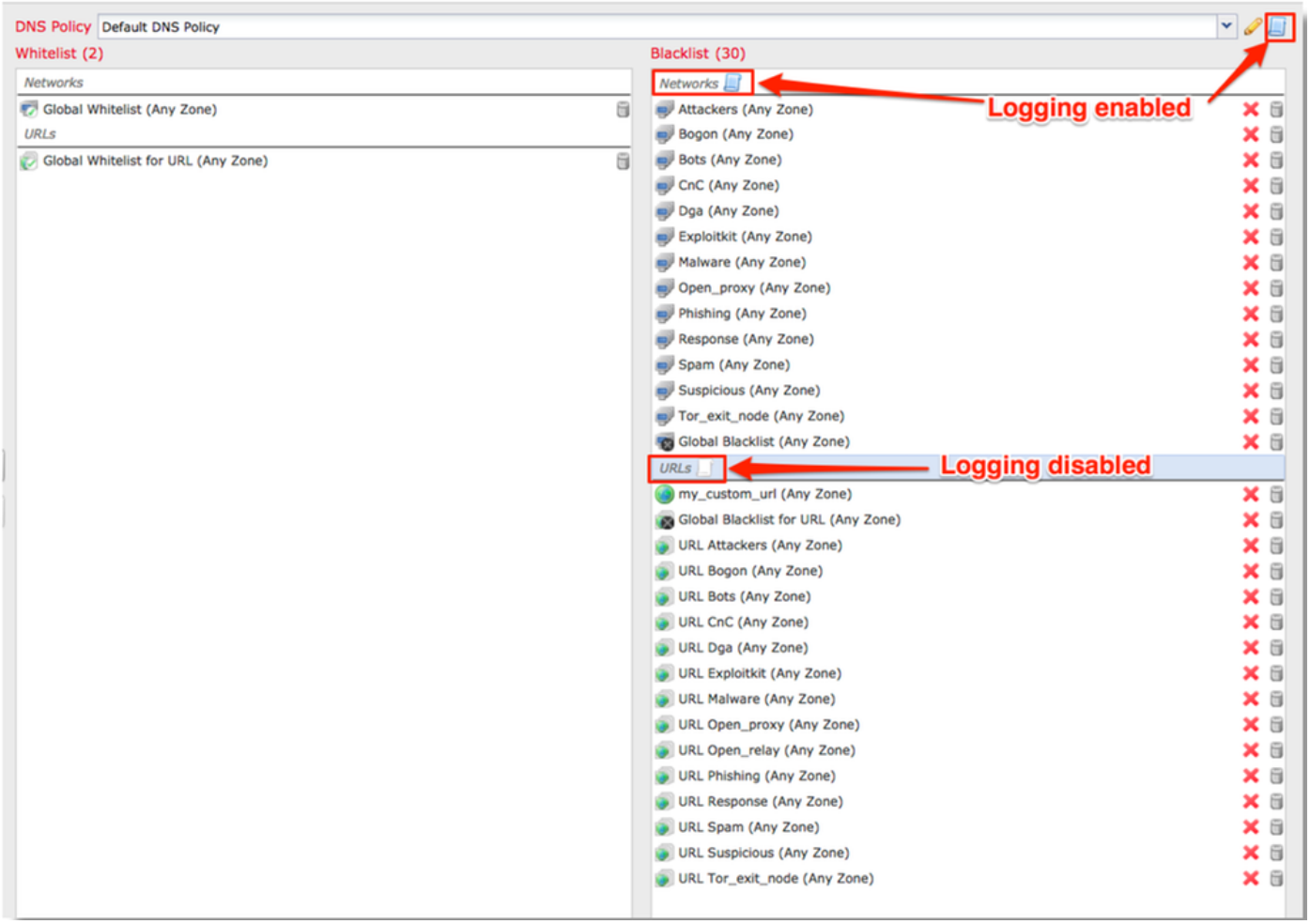
Als is vastgesteld dat het pakket zich kleedt maar niet kapselt, moet de volgende stap in het oplossen van het gegevenspad zich op de Firepower DAQ (Data Acquisition) laag bevinden om ervoor te zorgen dat het verkeer in kwestie naar Firepower wordt verzonden voor inspectie en als dit zo is, als het wordt ingetrokken of gewijzigd.

Dit artikel bekijkt hoe u problemen kunt oplossen bij de eerste bediening van verkeer door Firepower en het pad dat u door het apparaat loopt.

Het omvat ook hoe het Vuurenergieapparaat volledig kan worden omzeild om te bepalen of een component van de vuurkracht verantwoordelijk is voor het verkeersprobleem.

Security Intelligentie

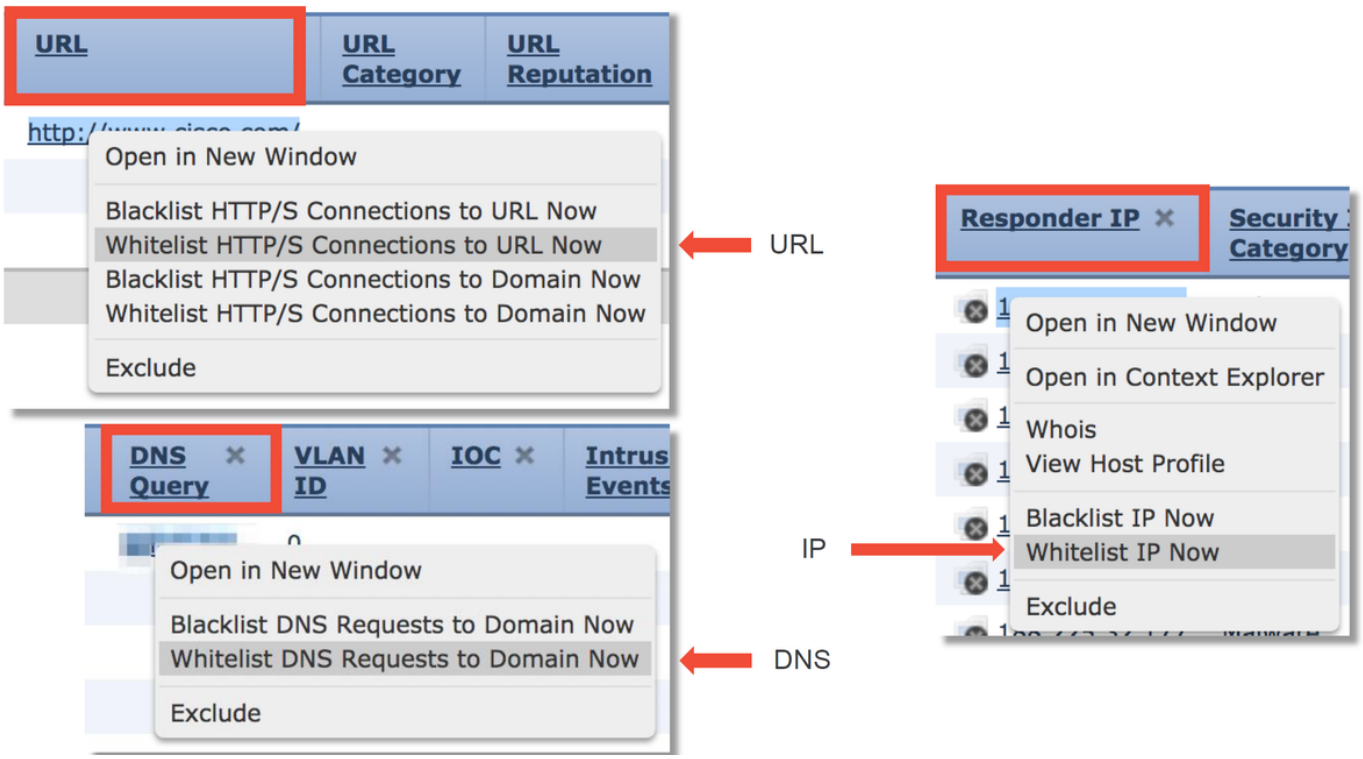
Security Intelligence is het eerste onderdeel van Firepower om het verkeer te inspecteren. Blokken op dit niveau zijn zeer gemakkelijk te bepalen zolang houtkap is ingeschakeld. Dit kan op de FMC GUI worden bepaald door te navigeren naar **beleid > Toegangsbeheer > Toegangsbeleid**. Nadat u op het pictogram Bewerken naast het beleid in kwestie hebt geklikt, navigeer dan naar het tabblad **Security Intelligence**.



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 aan TAC doorgeven om te rapporteren over wat wordt geblokkeerd en u kunt mogelijk een melding uit een zwarte lijst laten verwijderen.

Voor uitgebreide problemen oplossen bij de component Security Intelligence kunt u het relevante artikel over probleemoplossing in het gegevenspad bekijken.

Toegangsbeheerbeleid

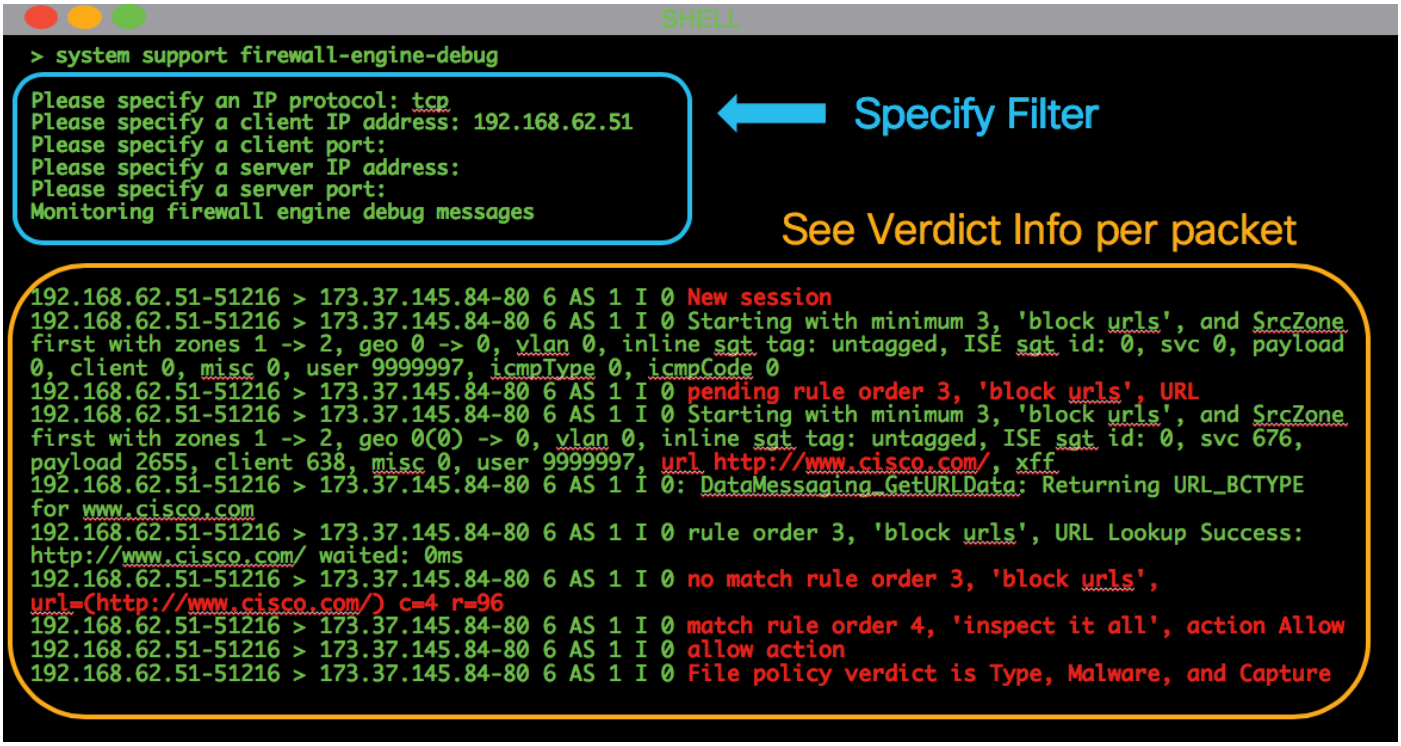
Als is vastgesteld dat de Security Intelligence-functie geen verkeer blokkeert, is de volgende aanbevolen stap om problemen op te lossen met de regels van het toegangsbeleid om te zien of een regel met een 'Blok'-actie het verkeer laat vallen.

Aanbevolen wordt om de opdracht "firewall-motor-debug" te gebruiken of met sporen op te

nemen. Deze hulpmiddelen kunnen je meestal meteen het antwoord geven en je vertellen welke regel het verkeer slaat en om welke redenen.

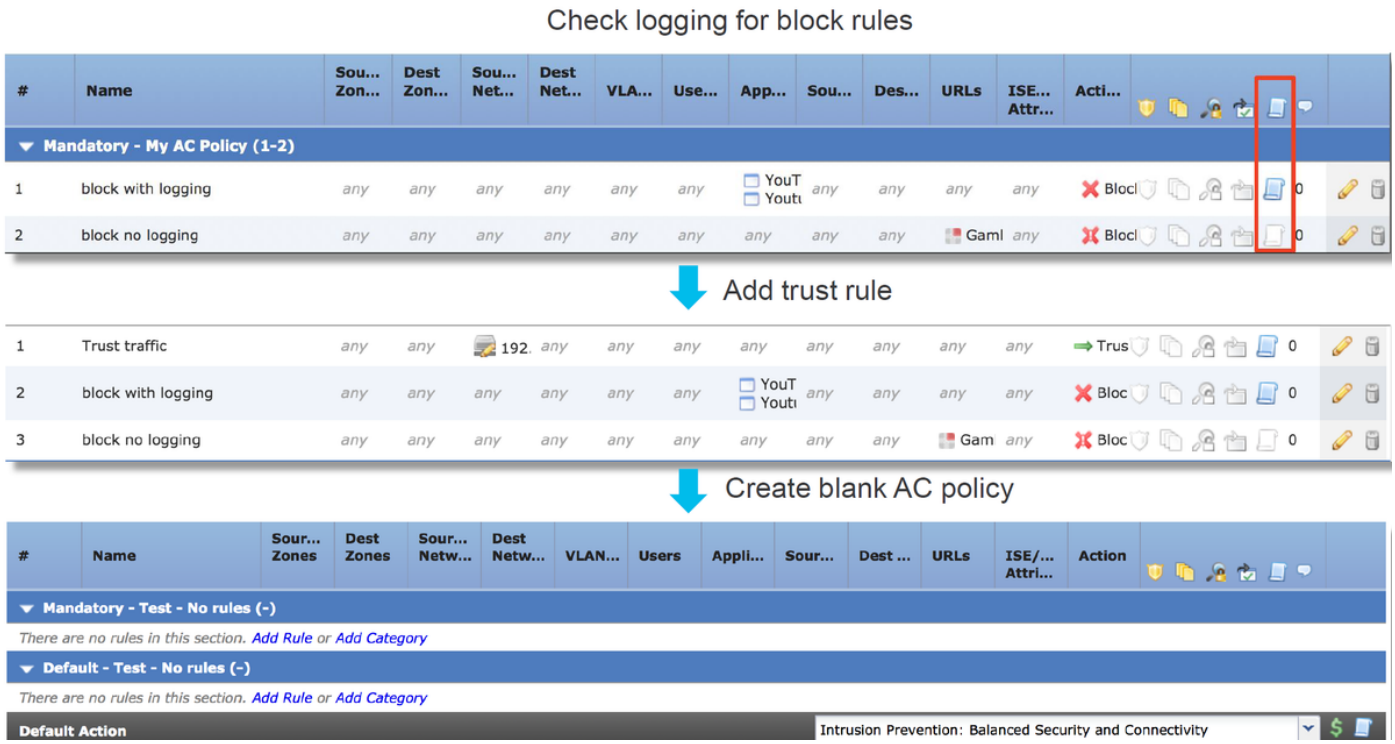
- Start debugging op Firepower CLI om te zien welke regel het blokkeren van verkeer is (zorg ervoor dat je zoveel mogelijk parameters invoert) via de volgende opdracht: **> systeemondersteuning voor firewall-motoren**
- De debug-uitvoer kan aan TAC worden geleverd voor analyse

Hieronder staat een aantal voorbeeldoutput, die een regelevaluatie weergeeft voor verkeer dat voldoet aan een toegangscontroleregel met de actie 'Toestaan':



Als u niet kunt bepalen welke toegangscontrole (AC)-regel is aangepast, of u niet kunt bepalen of het AC-beleid het probleem is met de bovenstaande tools, dan zijn hieronder een aantal basisstappen voor het oplossen van het Access Control Policy (let wel deze opties zijn niet de eerste optie omdat ze beleidswijzigingen/implementaties vereisen):

- houtkap voor alle regels inschakelen met een "Blok"-actie
- Als u nog steeds geen verbindingsgebeurtenissen voor het verkeer ziet en dit wordt geblokkeerd, moet u vervolgens een vertrouwensregel voor het betreffende verkeer definiëren als een mitigatiemaatregel
- Als de vertrouwensregel voor het verkeer nog steeds niet de kwestie oplost maar u nog steeds vermoedt dat het AC-beleid fout is, moet u vervolgens een nieuw leeg Access Control Policy maken als dat mogelijk is, door gebruik te maken van een andere standaardoptie dan "Alle verkeer blokkeren"

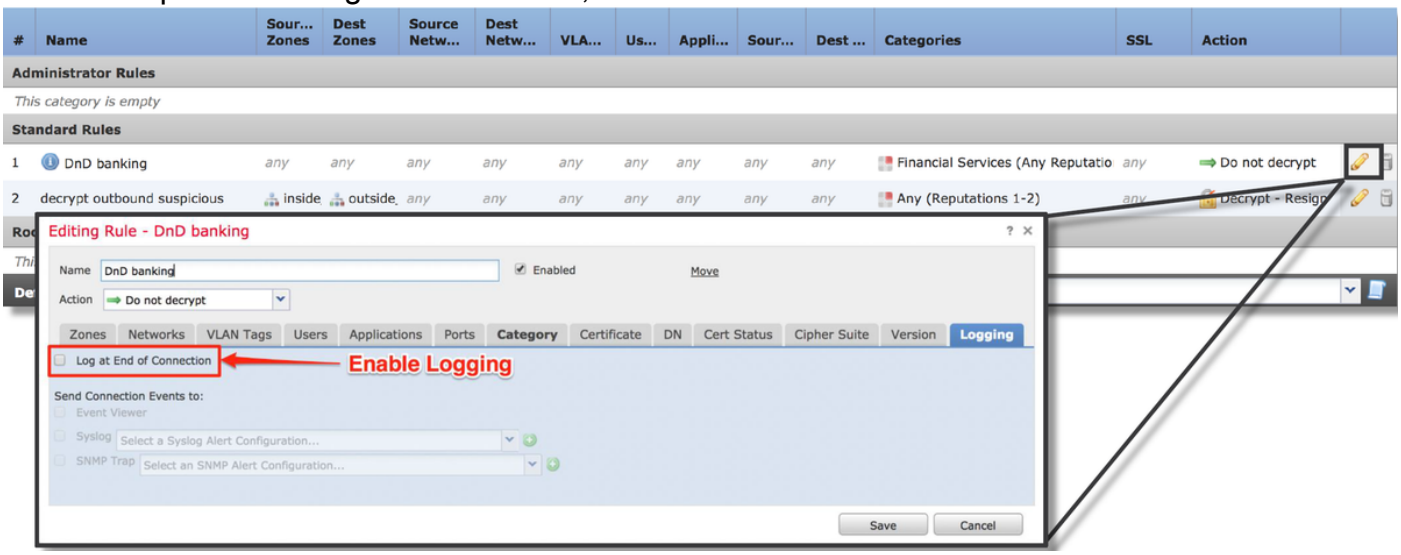


Voor een diepgaande oplossing voor het probleem van het toegangsbeleid, raadpleeg dan het artikel over het oplossen van het pad.

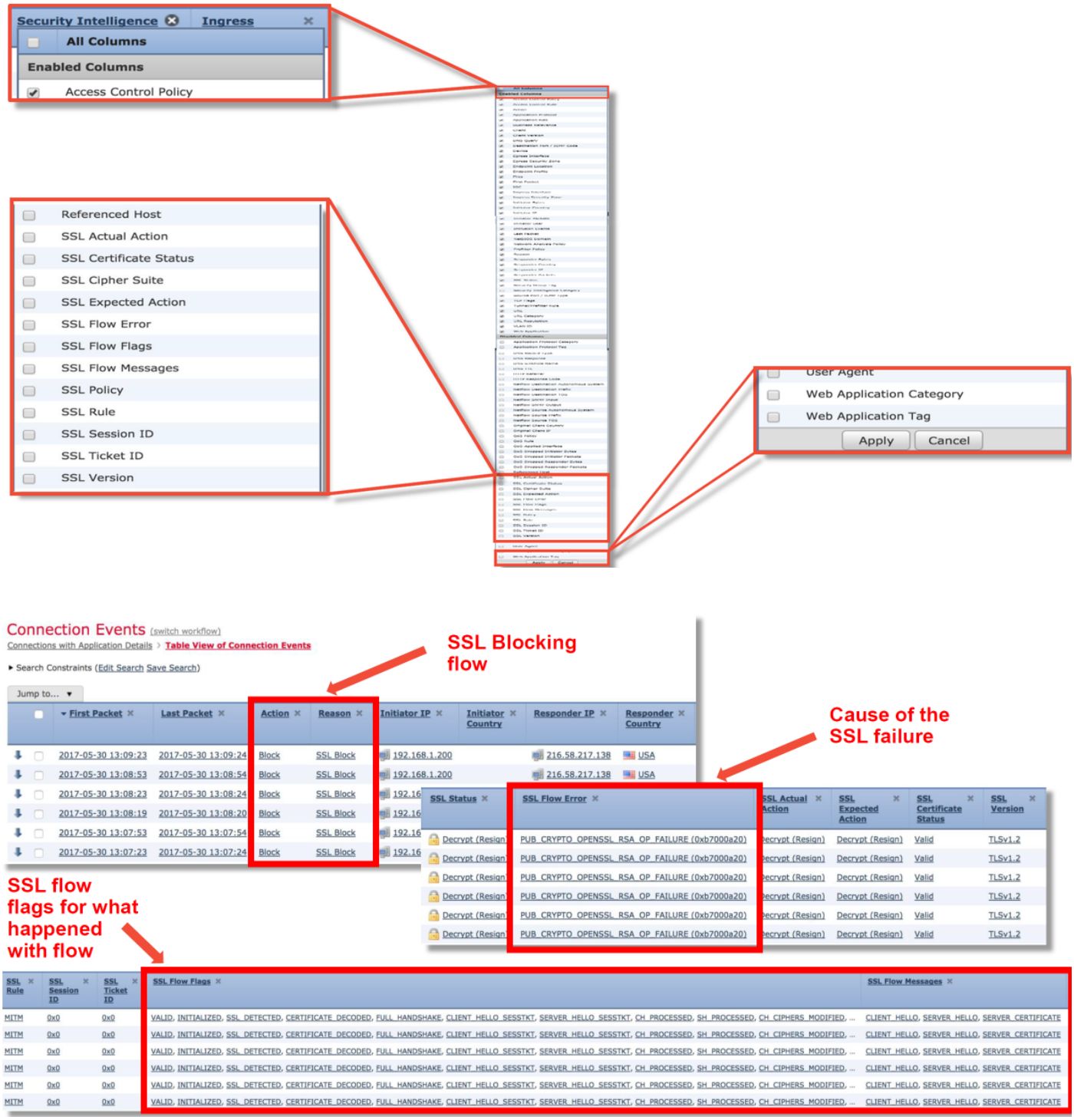
SSL-beleid

Als SSL Policy wordt gebruikt, is het mogelijk dat dit verkeer blokkeert. Hieronder staan enkele basisstappen voor het oplossen van het SSL-beleid:

- houtkap voor alle regels inschakelen, inclusief de 'actie standaard'



- Controleer het tabblad Undecrypable Actions om te zien of een optie is ingesteld om verkeer te blokkeren
- Controleer in het gedeelte Connection-gebeurtenissen alle velden met 'SSL' in de naam De meeste zijn standaard uitgeschakeld en moeten worden ingeschakeld in de kijker Connection Events door op het kruisbeeld naast elke kolom naam te klikken



- Een leeg SSL-beleid maken met Niet decrypteren als de Standaardactie als een limiteringsstap
- Verwijder het SSL-beleid van het toegangscontrolbeleid als een limiteringsstap
  Dit wordt ingesteld in het tabblad Geavanceerd

Het SSL Policy wordt verdacht van het laten vallen van verkeer, de verbindingsgebeurtenissen samen met de beleidsconfiguratie kunnen naar TAC worden verzonden.

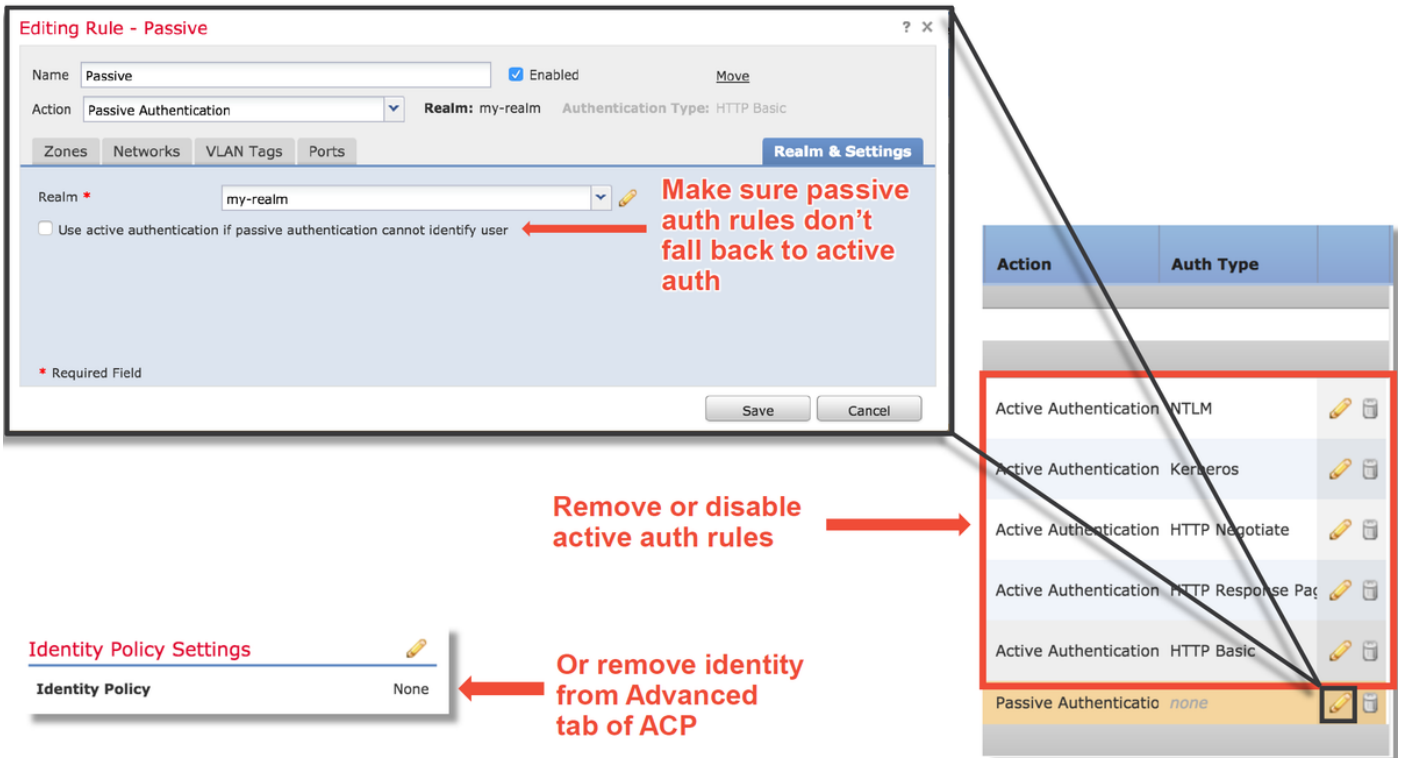
Voor een grondiger probleemoplossing bij het SSL-beleid raadpleegt u het artikel over het oplossen van het gegevenspad.

Actieve verificatie

Indien gebruikt in een identiteitsbeleid, heeft actieve verificatie de mogelijkheid om verkeer te laten vallen wat zou moeten worden toegestaan als er iets verkeerd gaat. De actieve authenticatie optie zelf kan direct invloed hebben op al HTTP/HTTPS-verkeer omdat als bepaald wordt dat we een gebruiker moeten authenticeren, dit alles alleen via het HTTP-protocol gebeurt. Dit betekent dat actieve authenticatie geen invloed zou moeten hebben op andere netwerkdiensten (zoals DNS, ICMP, etc.) tenzij u specifieke toegangscontroleregels hebt die op gebruiker gebaseerd blokkeren, en gebruikers niet in staat zijn om authenticatie door de actieve authenticatiediensten op de FTD te controleren. Dit zou echter geen direct probleem zijn van de actieve authenticatiefunctie, maar het gevolg van het feit dat gebruikers niet in staat zijn om authenticatie te verkrijgen en een beleid hebben dat ongeauthenticeerde gebruikers blokkeert.

Een snelle mitigatiemaatregel zou zijn om regels binnen het identiteitsbeleid uit te schakelen met de actie 'Actieve Verificatie'.

Zorg er ook voor dat alle regels met "passieve verificatie"-actie niet de optie "actieve authenticatie gebruiken indien passieve verificatie niet kan identificeren" hebben ingeschakeld.



Meer gedetailleerde problemen oplossen bij de actieve verificatie kunt u het artikel over probleemoplossing bij het datapad bekijken.

Inbraakbeleid

Een inbraakbeleid kan verkeer laten vallen of netwerkvertraging veroorzaken. Een inbraakbeleid kan op één van de volgende drie plaatsen binnen het toegangscontrolebeleid worden gebruikt:

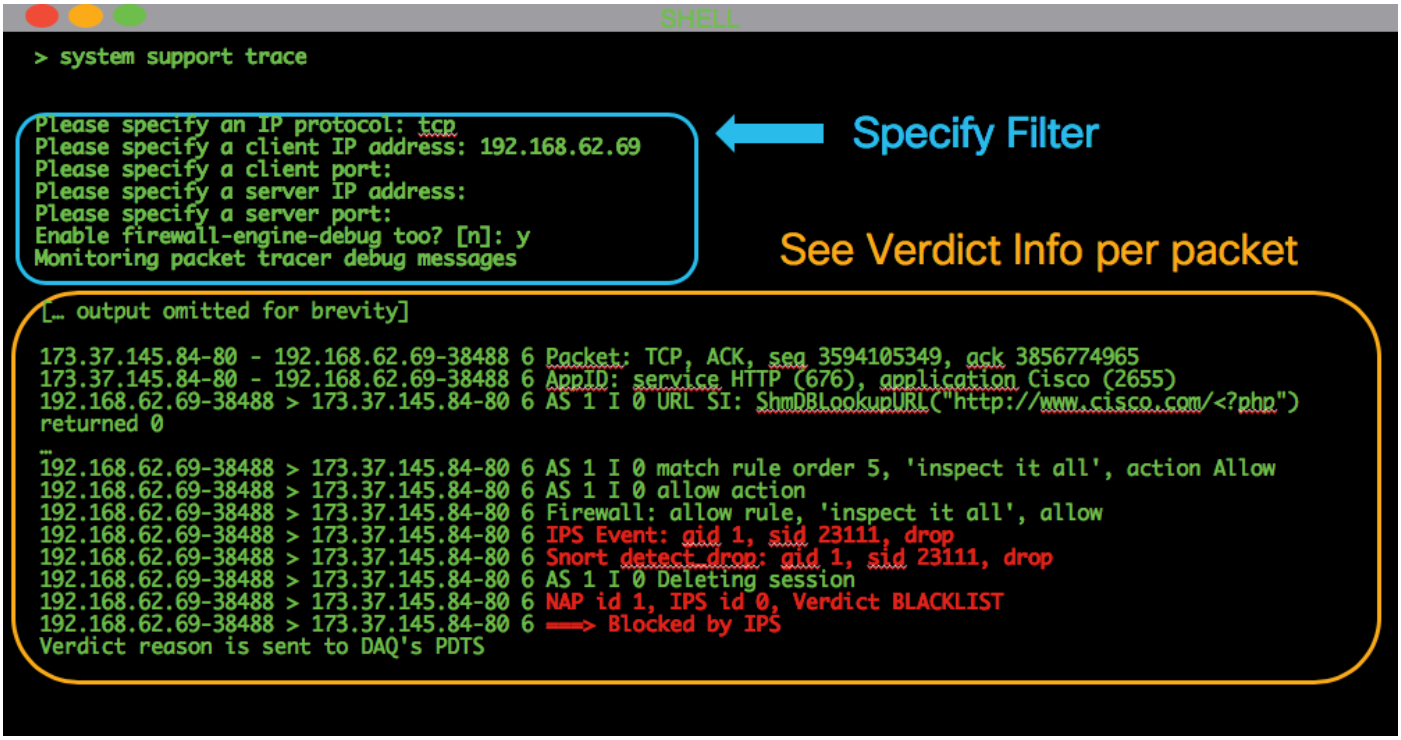
- In een toegangscontroleregel kunt u binnen het tabblad "Inspectie"
- In de standaardinstelling
- In het tabblad Geavanceerd **is** in het gedeelte Netwerkanalyse **en inbraakbeleid > Inbraakbeleid dat is gebruikt voordat de toegangscontroleregel is ingesteld, ingesteld**

Om te zien of een Inbraakbeleid regel het verkeer blokkeert, kunt u navigeren naar de pagina **Analyse > Inbraakingen > Gebeurtenissen** in het FMC. De **weergave van de**

Inbraakgebeurtenissen in de tabel geeft informatie over de hosts die bij de gebeurtenissen betrokken zijn. Raadpleeg het betreffende artikel over probleemoplossing in het gegevenspad op informatie met betrekking tot de analyse van gebeurtenissen.

De eerste aanbevolen stap om te bepalen of een IPS (Inbraakbeleid Signature) het verkeer blokkeert, is om de optie van de**>-systeemondersteuning** van de CLI van de FTD te gebruiken. Dit debug-opdracht werkt op dezelfde manier als firewall-motor-debug, en het geeft u ook de optie om firewall-motor-debug naast het spoor mogelijk te maken.

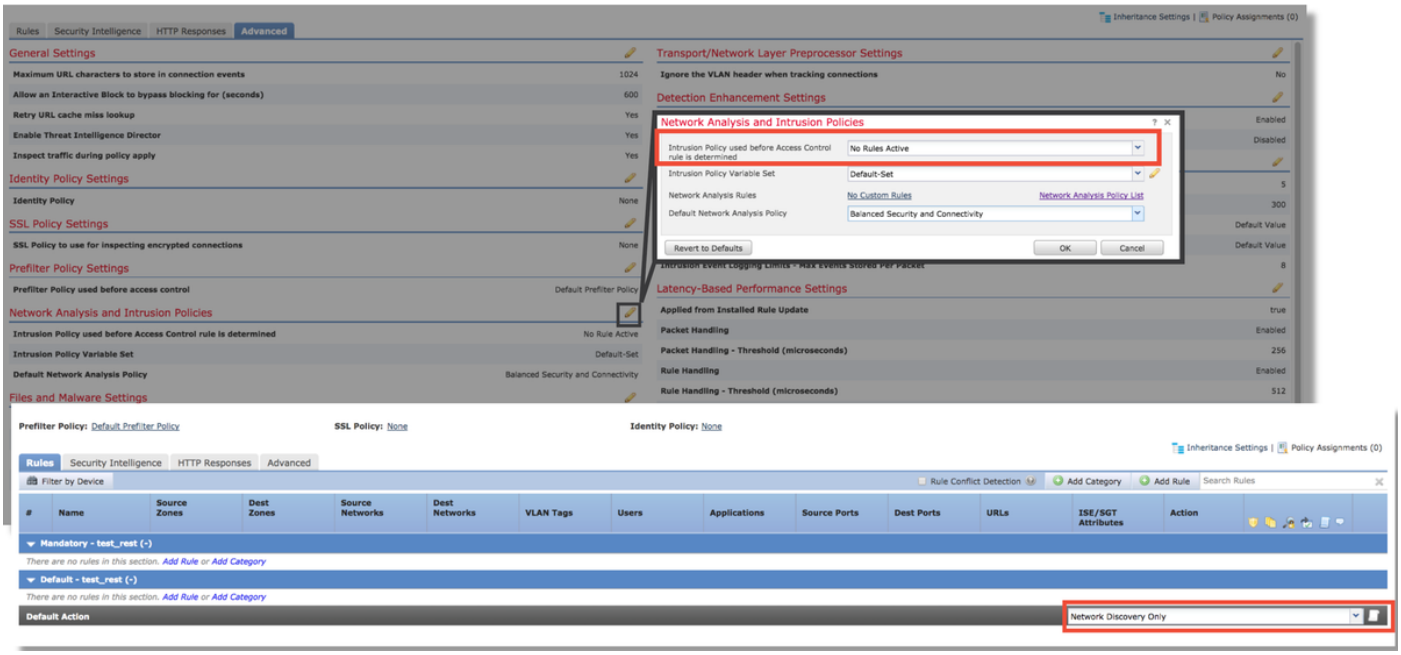
De onderstaande illustratie toont een voorbeeld van het gebruik van het traceringstool voor systeemondersteuning wanneer het resultaat aangeeft dat een pakje is geblokkeerd vanwege een inbraakregel. Dit geeft u alle details zoals de GID (Group Identifier), SID (Signature Identifier), NAP (Network Analysis Policy) ID en IPS ID zodat u precies kunt zien welk beleid/regel dit verkeer blokkeert.



Als u niet kunt bepalen dat IPS blokkeert van sporenuitvoer maar u vermoedt dat het IPS daalt door een aangepast Inbraakbeleid, kunt u het Inbraakbeleid vervangen door een "gebalanceerd Beveiliging en Connectiviteit" beleid of een "Connectivity over Security" beleid. Dit zijn door Cisco opgegeven inbraakbeleid. Als u die verandering aanbrengt, lost u de kwestie op. Dan kan het aangepaste Inbraakbeleid dat eerder wordt gebruikt problematisch zijn door TAC. Als een standaard Cisco-beleid al gebruikt is, kunt u proberen het standaard in een minder beveiligde te wijzigen omdat deze minder regels hebben, zodat het bereik beperkt kan worden. Bijvoorbeeld, als het verkeer geblokkeerd is en je een evenwichtig beleid gebruikt, dan overstapt je op connectiviteit over het veiligheidsbeleid en het probleem verdwijnt, is het waarschijnlijk dat er een regel in het evenwichtige beleid was om het verkeer te laten vallen die niet is ingesteld om de connectiviteit over het veiligheidsbeleid te verminderen.

De volgende wijzigingen kunnen worden aangebracht in het toegangscontrolebeleid om alle mogelijkheden voor inbraakbeleidsinspecties uit te schakelen (aanbevolen wordt om zo min mogelijk wijzigingen door te voeren om uw veiligheidsefficiëntie niet te wijzigen, zodat doelgerichte AC-regels voor het betreffende verkeer worden aanbevolen in plaats van IPS in het gehele beleid uit te schakelen):

- In alle regels voor toegangscontrole (of alleen de regels die overeenkomen met het specifieke verkeer dat wordt beïnvloed), verwijdert u het inbraakbeleid uit het tabblad Inspectie
- In het tabblad Geavanceerd **kiest** u in het **gedeelte Network Analysis and Inbraakbeleid > Inbraakbeleid dat is gebruikt voordat Access Control-regel wordt ingesteld** het beleid "No Rules Active".



Als dat probleem nog steeds niet oplost, gaat u verder met het oplossen van de netwerkanalyse.

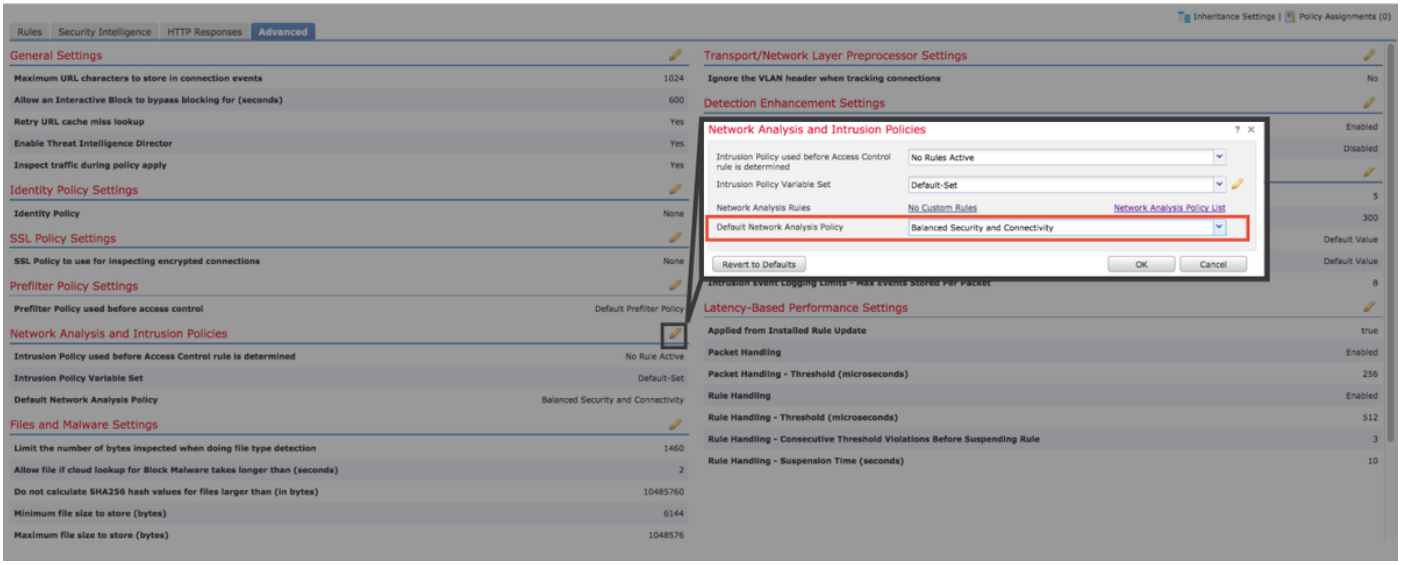
Meer gedetailleerde problemen oplossen bij de optie Inbraakbeleid, raadpleeg dan het artikel over het oplossen van het pad.

Beleid voor netwerkanalyse

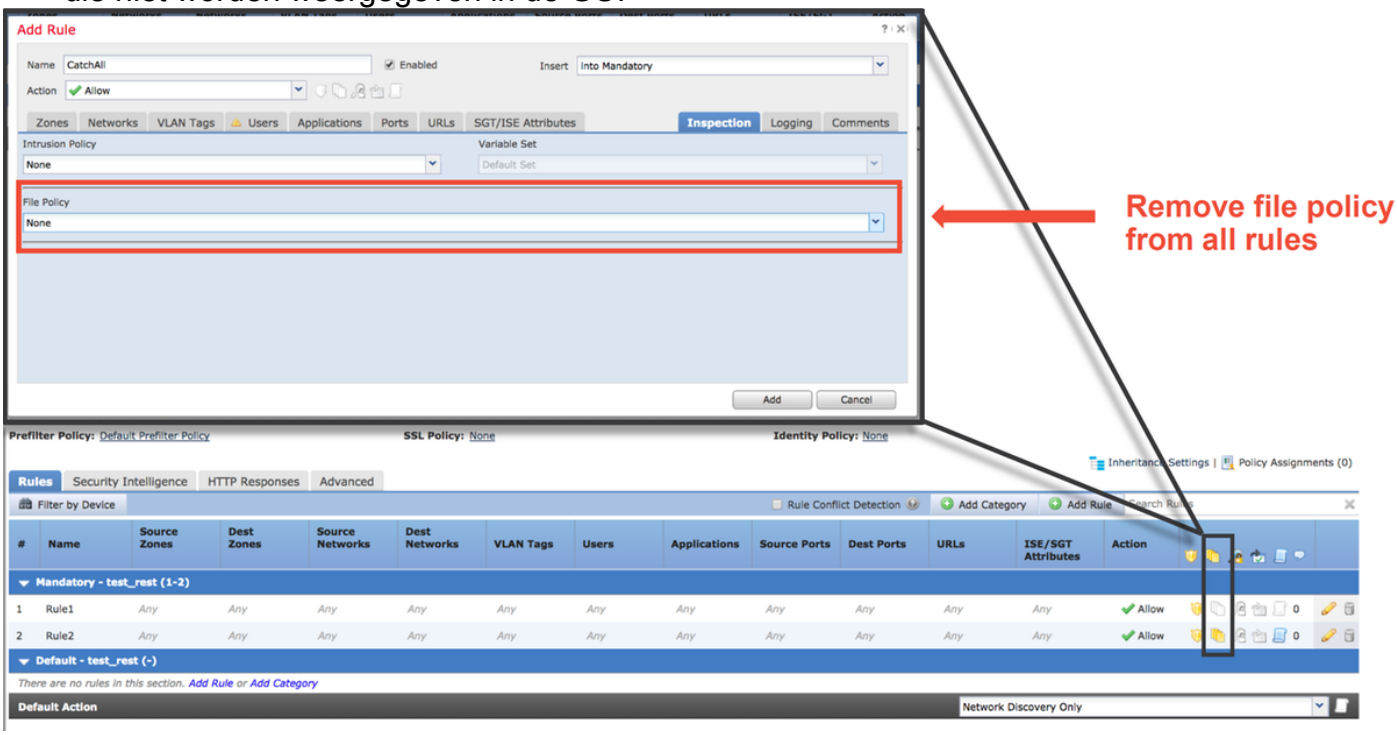
Het Network Analysis Policy (NAP) bevat FirePOWER-instellingen per processor, waarvan sommige het verkeer kunnen beperken. De eerste aanbevolen stap voor het oplossen van problemen is dezelfde als voor de IPS-oplossing, namelijk het trackgereedschap **> systeemondersteuning** te gebruiken om te proberen te vinden wat in het verleden het verkeer blokkeert. Zie het gedeelte "Inbraakbeleid" hierboven voor meer informatie over dit gereedschap en voorbeeldgebruik.

Om mogelijke problemen met de NAP snel te verhelpen, kunnen de volgende stappen worden uitgevoerd:

- Als een aangepaste NAP wordt gebruikt, vervang deze dan door een beleid dat is gericht op "gebalanceerde beveiliging en connectiviteit" of "Connectivity over Security"



- Als er "Aangepaste regels" worden gebruikt, zorg er dan voor dat u de NAP op een van de bovengenoemde standaardinstellingen instelt
- Als een toegangscontroleregeling een bestandsbeleid gebruikt, verwijdert u deze tijdelijk als een bestandsbeleid waarmee instellingen voor voorprocessors op de onderkant mogelijk zijn die niet worden weergegeven in de GUI



Er kan in dit artikel meer informatie worden opgenomen over de problemen bij de behandeling van de beleidsfunctie voor netwerkanalyse.

Gerelateerde informatie

Links naar documentatie bij vuurkracht

https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html