Fehlerbehebung für FirePOWER-Datenpfade: Übersicht

Inhalt

Einführung

Dieser Leitfaden soll dabei helfen, schnell festzustellen, ob ein FirePOWER Threat Defense (FTD)-Gerät oder eine Adaptive Security Appliance (ASA) mit FirePOWER Services ein Problem mit dem Netzwerkverkehr verursacht. Darüber hinaus hilft es bei der Festlegung, welche FirePOWER-Komponenten untersucht werden sollten und welche Daten vor der Einbindung des Cisco Technical Assistance Center (TAC) gesammelt werden sollten.

Liste aller Artikel der FirePOWER Data Path Troubleshooting Series.

Fehlerbehebung für FirePOWER-Datenpfade Phase 1: Paketeingang

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

Fehlerbehebung für FirePOWER Data Path 2: DAQ-Schicht
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214575-firepower-data-path-troubleshooting-phas.html

Fehlerbehebung für FirePOWER Data Path 3: Sicherheitsinformationen

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214576-firepower-data-path-troubleshooting-phas.html

Fehlerbehebung für FirePOWER Data Path 4: Zugriffskontrollrichtlinie
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214577-firepower-data-path-troubleshooting-phas.html

Fehlerbehebung für FirePOWER-Datenpfad Phase 5: SSL-Richtlinie
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214581-firepower-data-path-troubleshooting-phas.html

Fehlerbehebung für FirePOWER-Datenpfad Phase 6: Aktive Authentifizierung
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/214608-firepower-data-path-troubleshooting-phas.html

Fehlerbehebung für FirePOWER Data Path 7: Richtlinie für Sicherheitsrisiken
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214609-firepower-data-path-troubleshooting-phas.html

Fehlerbehebung für FirePOWER-Datenpfade Phase 8: Richtlinie für Netzwerkanalysen

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

Voraussetzungen

- In diesem Artikel wird davon ausgegangen, dass der Benutzer grundlegende Kenntnisse der FTD- und ASA-Plattformen besitzt.
- Es wird empfohlen, Kenntnisse über Open-Source-Snacks zu erwerben, dies ist jedoch nicht erforderlich.

Eine vollständige Liste der Firepower-Dokumentation, einschließlich der Installations- und Konfigurationsanleitungen, finden Sie auf der Dokumentations-Roadmap-Seite.

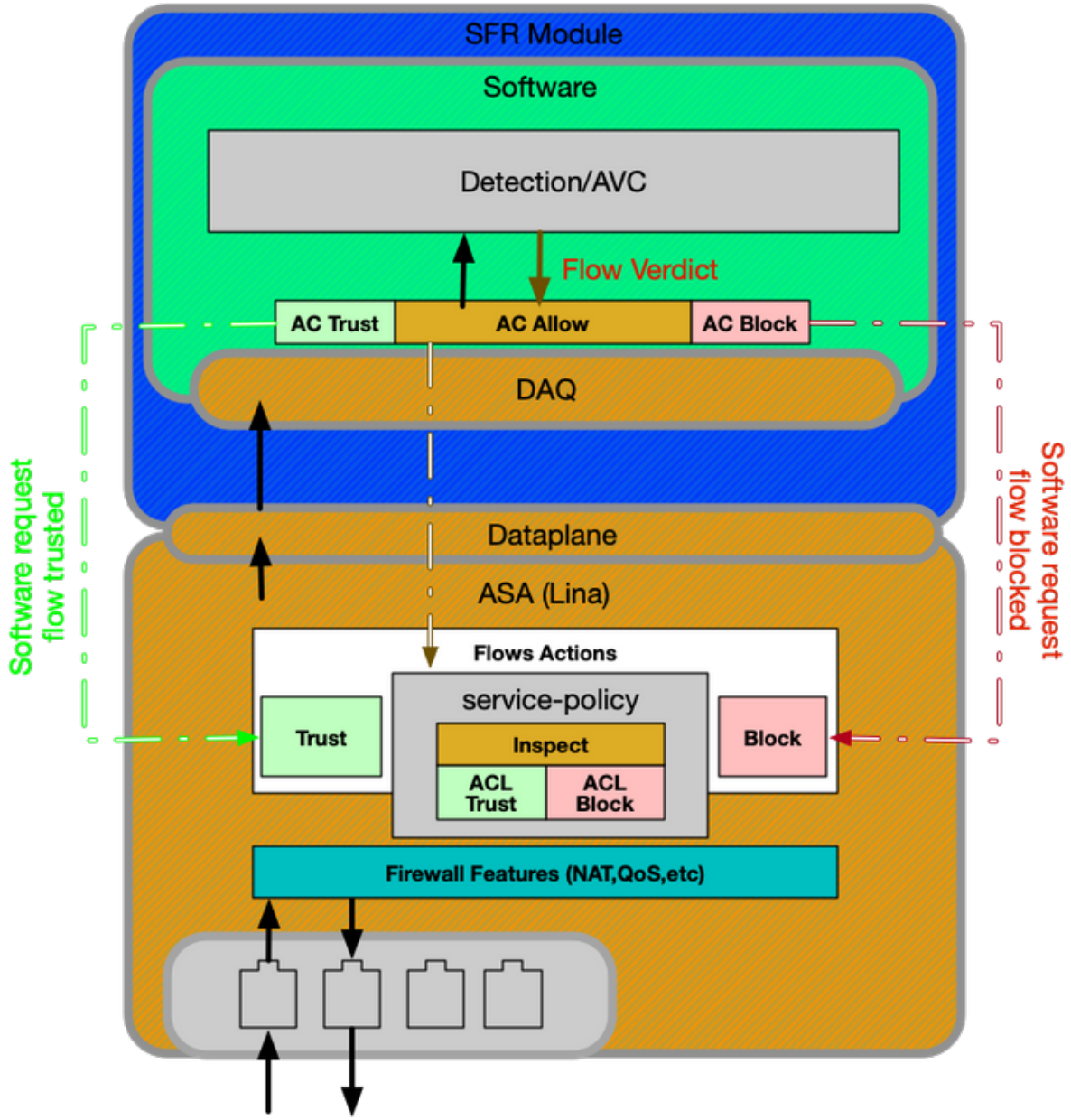
Architekturübersicht über den Datenpfad

Im folgenden Abschnitt wird der Datenpfad der Architektur für verschiedene FirePOWER-Plattformen beschrieben. Im Hinblick auf die Architektur werden wir nun prüfen, wie schnell festgestellt werden kann, ob das FirePOWER-Gerät den Datenverkehrsfluss blockiert.

> **Hinweis**: Dieser Artikel behandelt weder die älteren Geräte der Firepower 7000- und 8000-Serie noch die virtuelle NGIPS-Plattform (nicht FTD-basiert). Informationen zur Fehlerbehebung für diese Plattformen finden Sie auf unserer TechNotes-Seite.

ASA mit FirePOWER Services (SFR-Modul)-Plattform

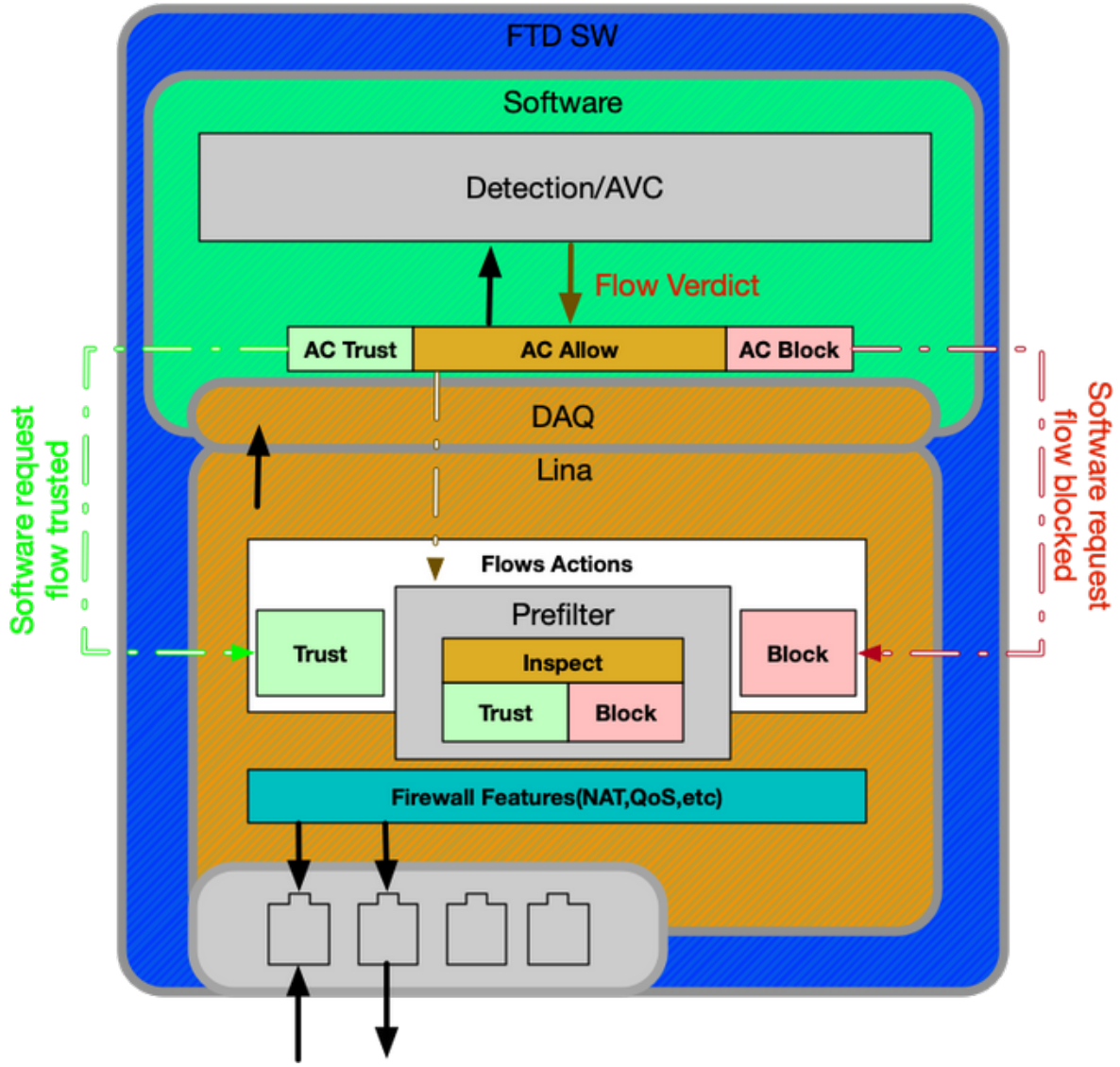
Die FirePOWER Services-Plattform wird auch als SFR-Modul bezeichnet. Dies ist im Grunde ein virtuelles System, das auf ASA-Plattformen der Serie 5500-X ausgeführt wird.



Die Service-Richtlinie auf der ASA bestimmt, welcher Datenverkehr an das SFR-Modul gesendet wird. Es gibt eine Datenebenenschicht, die für die Kommunikation mit der FirePOWER Data Acquisition (DAQ)-Engine verwendet wird, die verwendet wird, um Pakete so zu übersetzen, dass sie leicht verständlich sind.

FirePOWER Threat Defense auf ASA500-X und Virtual FTD-Plattform

Die FTD-Plattform besteht aus einem einzigen Image, das sowohl den Lina- (ASA) als auch den FirePOWER-Code enthält. Ein großer Unterschied zwischen dieser und der ASA mit SFR-Modulplattform besteht darin, dass die Kommunikation zwischen Lina und Snort effizienter ist.

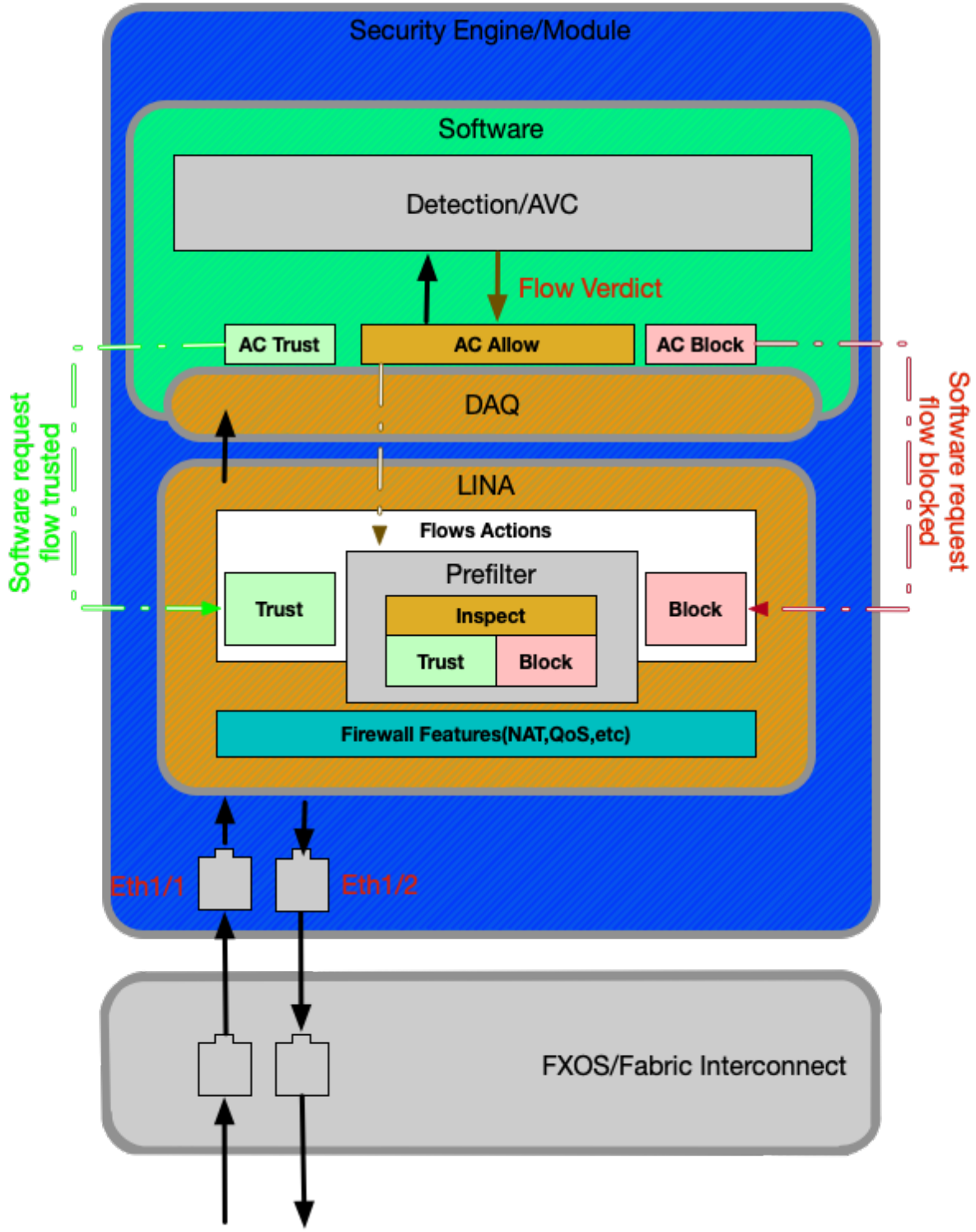


FTD auf SSP-Plattformen

Auf den SSP-Modellen (Security Service Platforms) wird die FTD-Software auf der FirePOWER eXtensible Operative System (FXOS)-Plattform ausgeführt. Dabei handelt es sich um ein zugrunde liegendes Betriebssystem, das zum Verwalten der Chassis-Hardware und zum Hosten verschiedener Anwendungen, die als logische Geräte bezeichnet werden, verwendet wird.

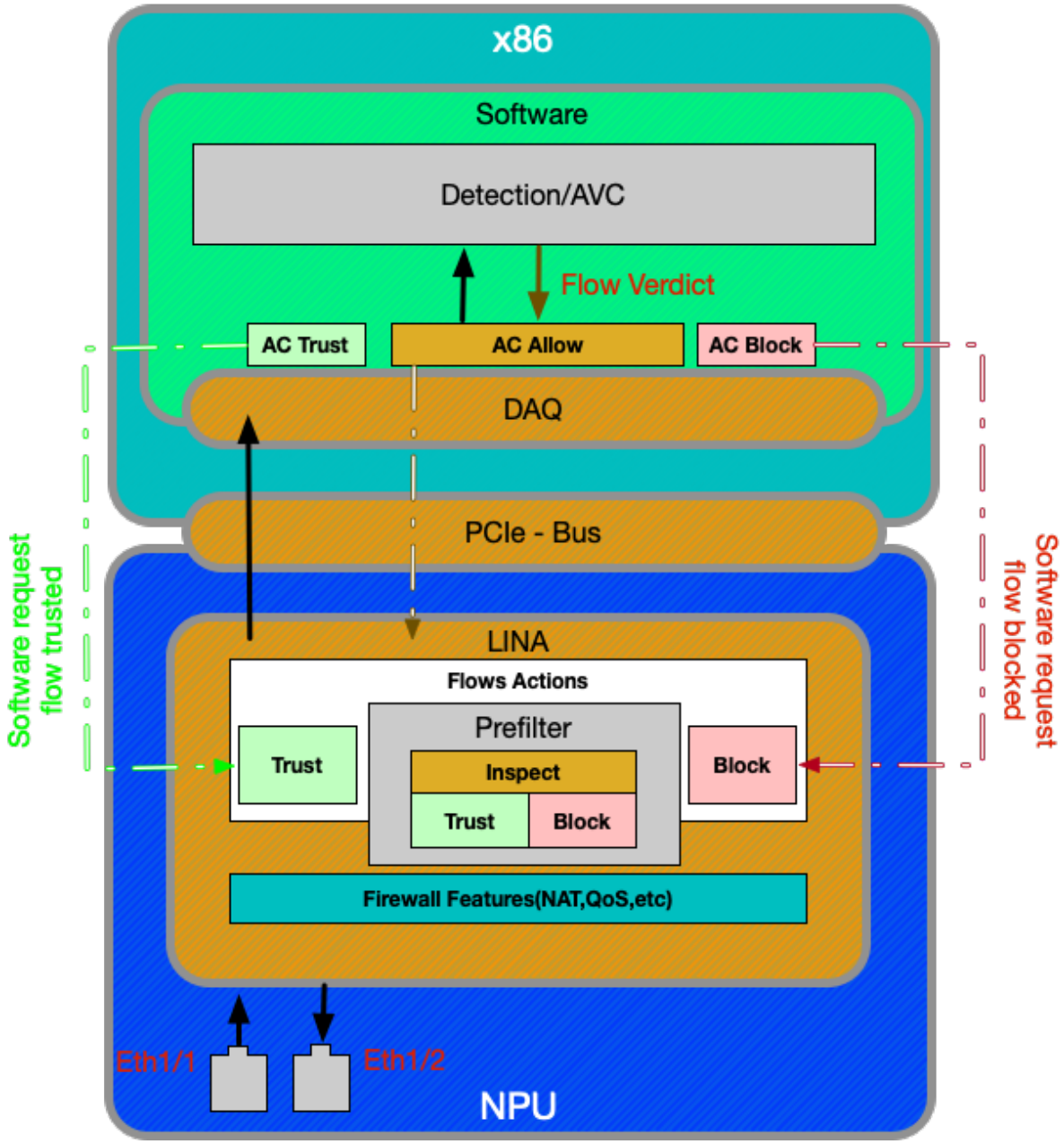
Innerhalb der SSP-Plattform gibt es einige Unterschiede zwischen den Modellen, wie in den nachfolgenden Diagrammen und Beschreibungen dargestellt.

FirePOWER-Appliances der Serien 9300 und 4100



Auf den Firepower 9300- und 4100-Plattformen werden eingehende und ausgehende Pakete von einem Switch verarbeitet, der mit der FXOS-Firmware (Fabric Interconnect) betrieben wird. Die Pakete werden dann an die Schnittstellen gesendet, die dem logischen Gerät zugewiesen sind (in diesem Fall FTD). Danach erfolgt die Paketverarbeitung wie auf den FTD-Plattformen ohne SSP.

FirePOWER 2100-Appliances



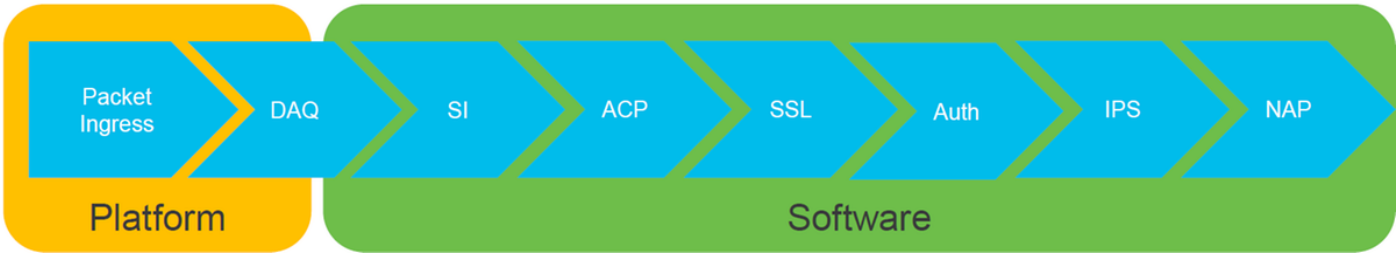
Das FirePOWER 2100-Gerät funktioniert ähnlich wie die Nicht-SSP-FTD-Plattformen. Sie enthält keine Fabric Interconnect-Layer, die auf den Modellen 9300 und 4100 vorhanden ist. Die Geräte der Serie 2100 unterscheiden sich jedoch erheblich von den anderen Geräten, und zwar durch den anwendungsspezifischen integrierten Schaltkreis (Application-Specific Integrated Circuit, ASIC). Alle traditionellen ASA-Funktionen (Lina) werden auf der ASIC ausgeführt, und alle NGFW-Funktionen (Snort, URL-Filterung usw.) der nächsten Generation werden auf der herkömmlichen x86-Architektur ausgeführt. Die Kommunikation von Lina und Snort auf dieser Plattform erfolgt über PCIe (Peripheral Component Interconnect Express) über eine Paketwarteschlange, im Gegensatz zu anderen Plattformen, die Direct Memory Access (DMA) für die Warteschlange von Paketen verwenden, um sie zu synchronisieren.

> **Hinweis**: Auf der FPR-2100-Plattform werden die gleichen Methoden zur Fehlerbehebung für FTD-Plattformen, die nicht SSP-Plattformen sind, angewendet.

Empfohlener Prozess zur Fehlerbehebung für FirePOWER Data Path

Nachdem wir nun besprochen haben, wie eindeutiger Datenverkehr sowie die grundlegende Datenpfad-Architektur in Firepower-Plattformen identifiziert werden können, sehen wir uns nun die spezifischen Orte an, an denen Pakete verworfen werden können. Es gibt acht grundlegende Komponenten, die in den Data Path-Artikeln behandelt werden. Diese können systematisch Fehler beheben, um mögliche Paketverluste zu ermitteln. Dazu gehören:

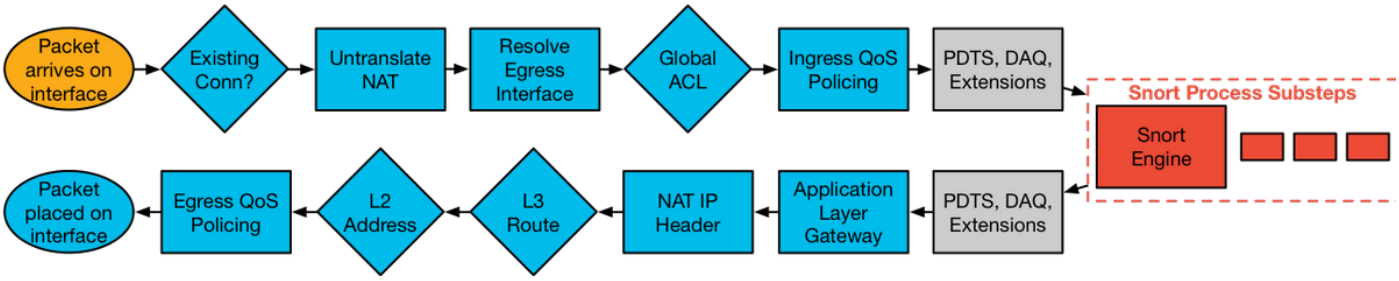
1. Paketeingang
2. FirePOWER-DAQ
3. Sicherheitsinformationen
4. Zugriffskontrollrichtlinie
5. SSL-Richtlinie
6. Aktive Authentifizierungsfunktionen
7. Intrusion Policy (IPS-Regeln)
8. Richtlinien für die Netzwerkanalyse (Snort-Vorprozessoreinstellungen)



Hinweis: Diese Komponenten sind nicht in der genauen Reihenfolge der Vorgänge in der FirePOWER-Verarbeitung aufgeführt, sondern werden gemäß unserem empfohlenen Workflow zur Fehlerbehebung bestellt. In der Abbildung unten wird der tatsächliche Pfad des Paketdiagramms dargestellt.

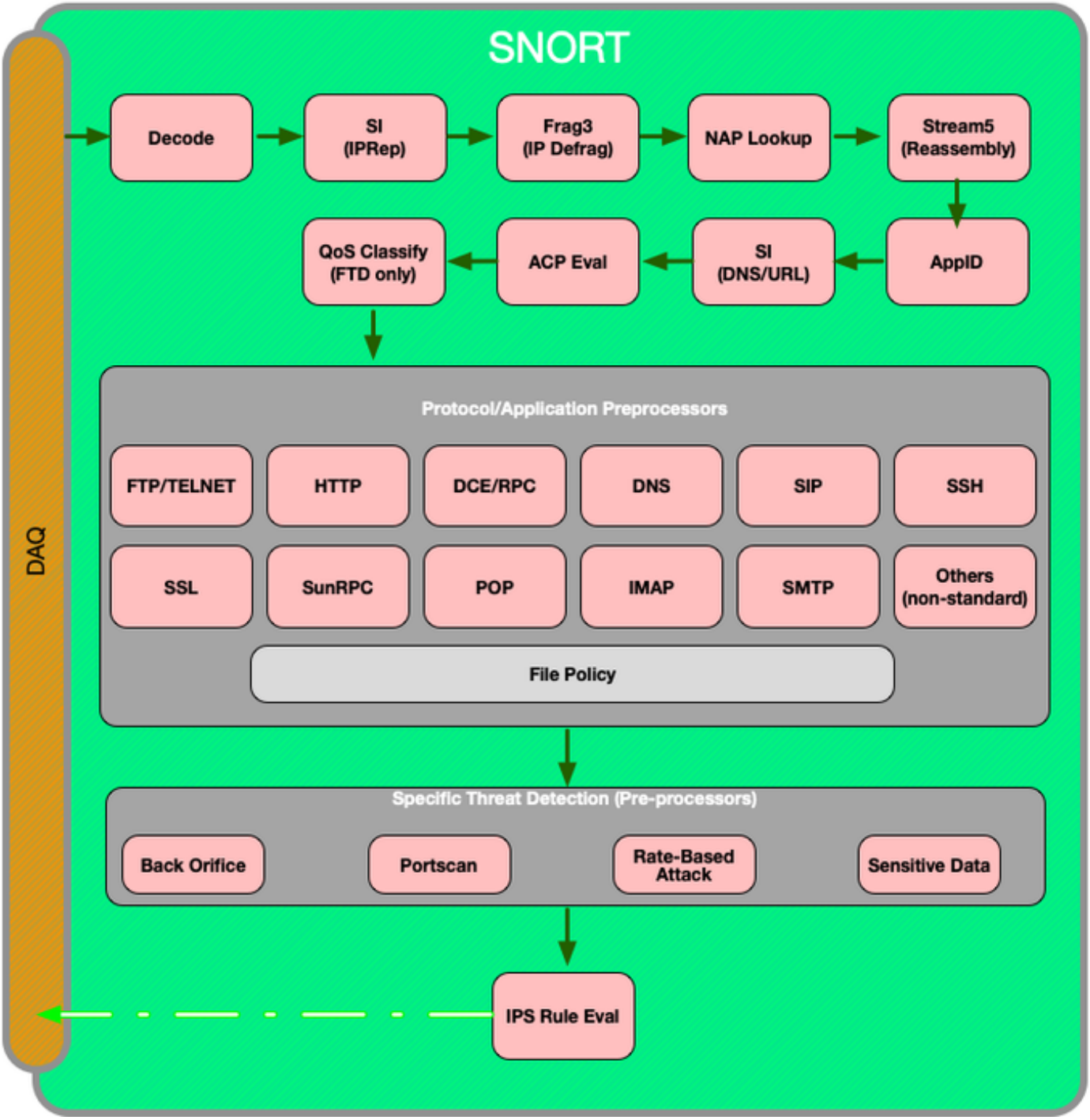
Tatsächlicher Pfad des Pakets durch FTD

Die folgende Abbildung zeigt den tatsächlichen Pfad des Pakets, während es durch FTD verläuft.



Snort-Paketpfad

Die folgende Abbildung zeigt den Pfad des Pakets durch die Snort-Engine.



Paketeingang und -ausgang

Der erste Schritt zur Fehlerbehebung bei Datenpfaden besteht darin, sicherzustellen, dass es bei der Ein- oder Ausgangs-Paketverarbeitung keine Paketverluste gibt. Wenn ein Paket eingeht, aber nicht absteigt, können Sie sicher sein, dass das Paket vom Gerät an einer Stelle im Datenpfad verworfen wird.

Dieser Artikel erläutert die Fehlerbehebung bei ein- und ausgehenden Paketen in FirePOWER-Systemen.

FirePOWER-DAQ

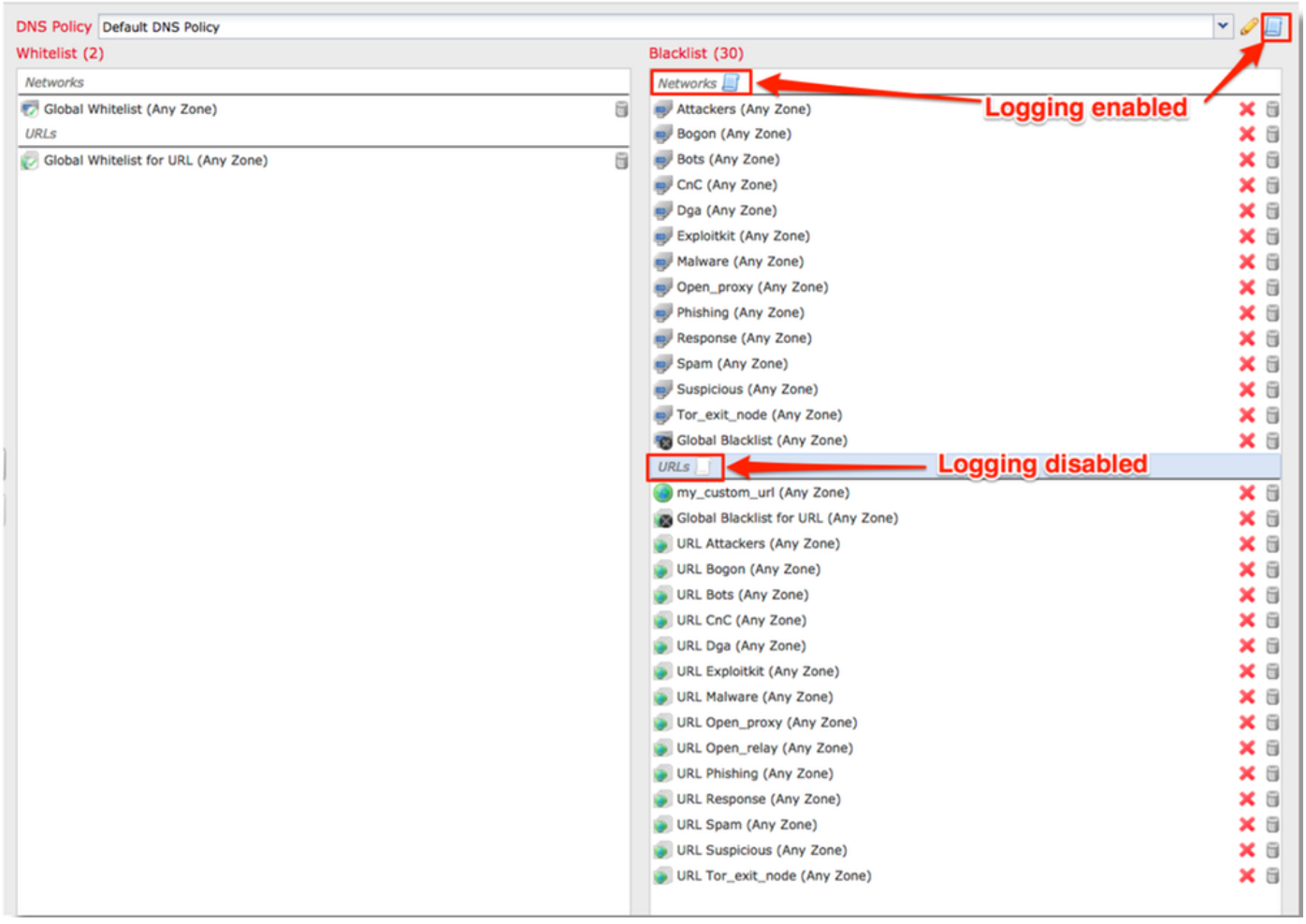
Wenn festgestellt wurde, dass das Paket eingeht, aber nicht absteigt, sollte der nächste Schritt bei der Fehlerbehebung für den Datenpfad auf der Ebene der Firepower-Datenerfassung erfolgen, um sicherzustellen, dass der betreffende Datenverkehr zur Überprüfung an FirePOWER gesendet wird. Wenn dies der Fall ist, sollte er verworfen oder geändert werden.

In diesem Artikel wird die Fehlerbehebung bei der erstmaligen Verarbeitung des Datenverkehrs durch Firepower und der Pfad beschrieben, den diese Lösung in der gesamten Appliance einnimmt.

Darüber hinaus wird erläutert, wie das FirePOWER-Gerät vollständig umgangen werden kann, um festzustellen, ob eine FirePOWER-Komponente für das Datenverkehrsproblem verantwortlich ist.

Sicherheitsinformationen

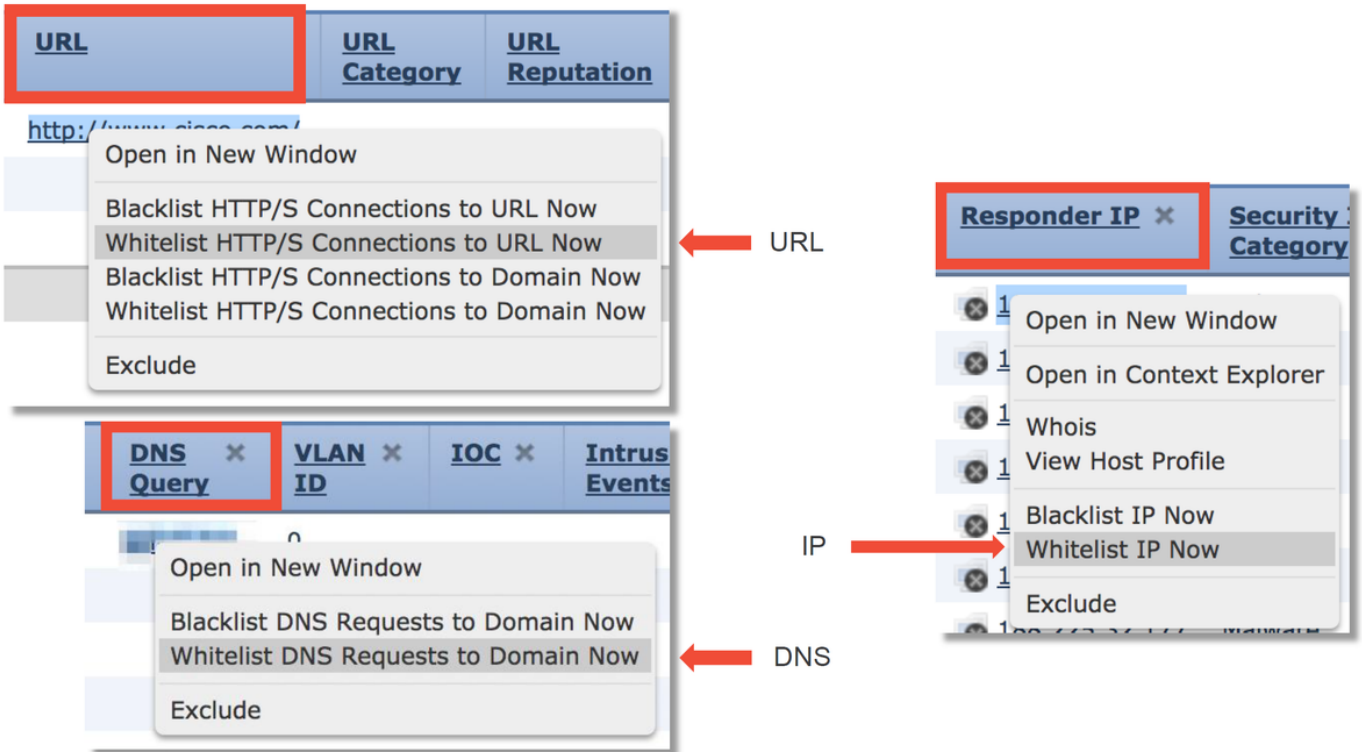
Security Intelligence ist die erste Komponente in Firepower, die den Datenverkehr überprüft. Die Blockierung auf dieser Ebene ist sehr einfach zu bestimmen, solange die Protokollierung aktiviert ist. Dies kann über die FMC-GUI bestimmt werden, indem Sie zu **Richtlinien > Zugriffskontrolle > Zugriffskontrollrichtlinie** navigieren. Navigieren Sie nach dem Klicken auf das Bearbeitungssymbol neben der betreffenden Richtlinie zur Registerkarte **Sicherheitsinformationen**.



Sobald die Protokollierung aktiviert ist, können Sie unter **Analysis > Connections > Security Intelligence Events (Analyse > Verbindungen > Sicherheitsinformationsereignisse)** die Security Intelligence Events (Sicherheitsinformationsereignisse) **anzeigen**. Es sollte klar sein, warum der Datenverkehr blockiert wird.

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 einen schnellen Eindämmungsschritt können Sie mit der rechten Maustaste auf die IP-, URL- oder DNS-Abfrage klicken, die durch die Funktion "Sicherheitsintelgence" blockiert wird, und eine Whitelist-Option auswählen.



Wenn Sie den Verdacht haben, dass etwas falsch auf die Blacklist gesetzt wurde, oder Sie eine Reputation beantragen möchten, können Sie ein Ticket direkt bei Cisco Talos unter dem folgenden Link öffnen:

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

Sie können die Daten auch an das TAC senden, um zu berichten, was blockiert wird, und möglicherweise einen Eintrag aus einer Blacklist entfernen lassen.

Detaillierte Fehlerbehebung für die Security Intelligence-Komponente finden Sie im entsprechenden Artikel zur Fehlerbehebung für Datenpfade.

Zugriffskontrollrichtlinie

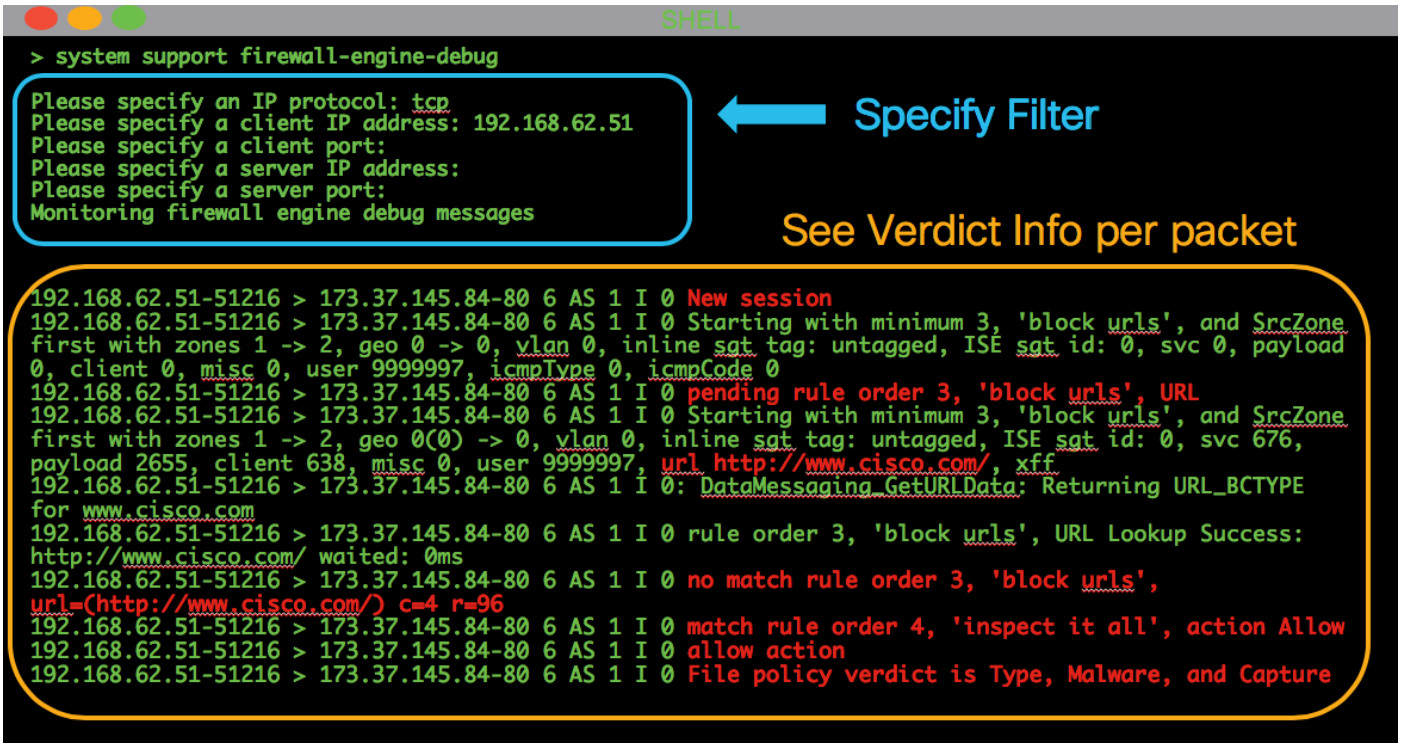
Wenn festgestellt wurde, dass die Funktion Sicherheitsinformationsfunktion den Datenverkehr nicht blockiert, wird als nächster Schritt empfohlen, die Zugriffskontrollrichtlinien zu überprüfen, um

festzustellen, ob eine Regel mit einer Blockierungsaktion den Datenverkehr verwirft.

Es wird empfohlen, den Befehl "firewall-engine-debug" oder die Erfassung mit trace zu verwenden. In der Regel können Sie mit diesen Tools sofort eine Antwort erhalten und Ihnen mitteilen, welche Regel der Datenverkehr trifft und aus welchen Gründen.

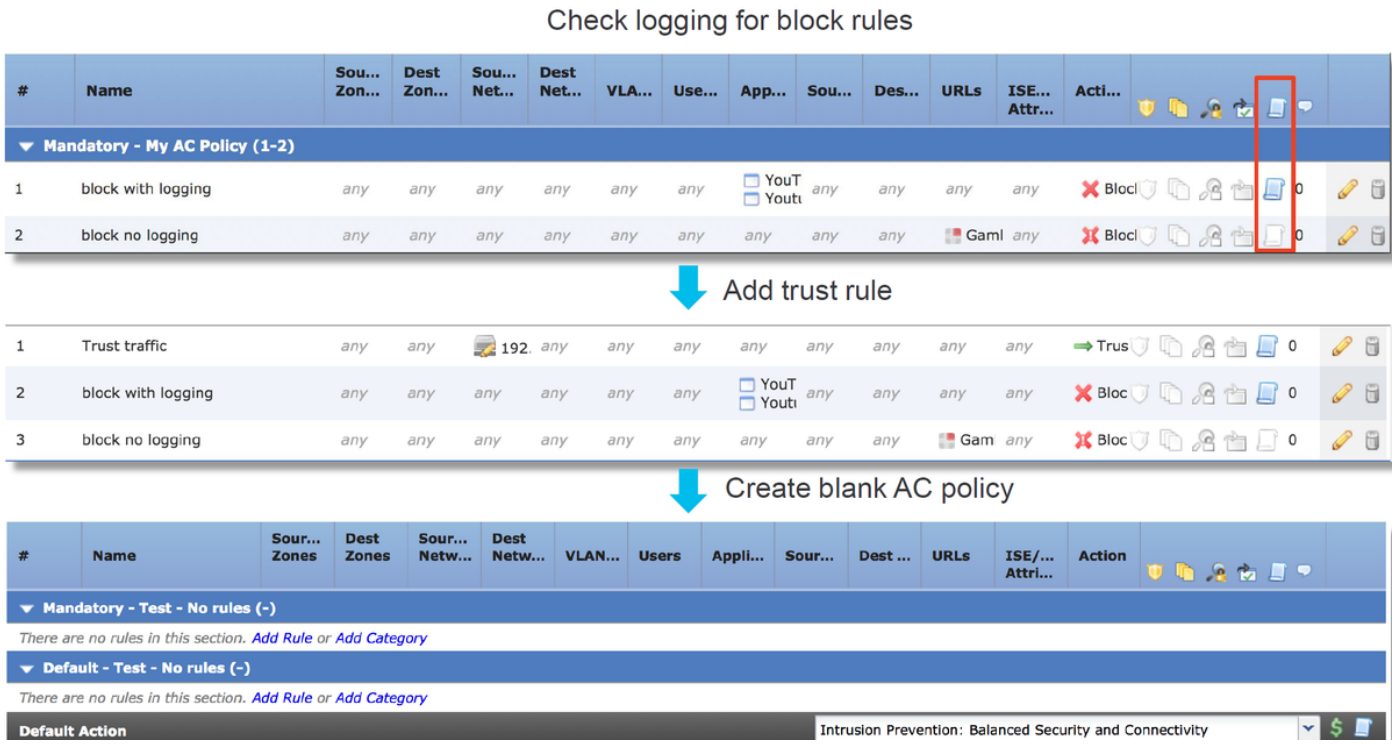
- Führen Sie das Debuggen auf der FirePOWER-CLI aus, um zu sehen, welche Regel den Datenverkehr blockiert (geben Sie möglichst viele Parameter ein), indem Sie den folgenden Befehl verwenden: **> Systemunterstützung Firewall-Engine-Debugging**
- Die Debug-Ausgabe kann dem TAC zur Analyse bereitgestellt werden.

Im Folgenden finden Sie einige Beispielausgabe, in der die Regelauswertung für Datenverkehr dargestellt wird, der einer Zugriffskontrollregel mit der Aktion 'Zulassen' entspricht:



Wenn Sie nicht feststellen können, welche Zugriffskontrollregel zugeordnet wird, oder Sie mithilfe der oben genannten Tools nicht feststellen können, ob die AC-Richtlinie das Problem darstellt, sind im Folgenden einige grundlegende Schritte zur Fehlerbehebung für die Zugriffskontrollrichtlinie aufgeführt (beachten Sie, dass diese Optionen nicht die erste Option sind, da sie Richtlinienänderungen/Bereitstellung erfordern):

- Aktivieren der Protokollierung für alle Regeln mit einer Blockierungsaktion
- Wenn Sie immer noch keine Verbindungsereignisse für den Datenverkehr sehen und er blockiert wird, erstellen Sie als Eindämmungsschritt eine Vertrauensregel für den betreffenden Datenverkehr.
- Wenn die Vertrauensregel für den Datenverkehr das Problem immer noch nicht behebt, Sie aber dennoch vermuten, dass die AC-Richtlinie fehlerhaft ist, erstellen Sie als Nächstes möglichst eine neue leere Zugriffskontrollrichtlinie. Verwenden Sie dabei eine andere Standardaktion als "Gesamten Datenverkehr blockieren".

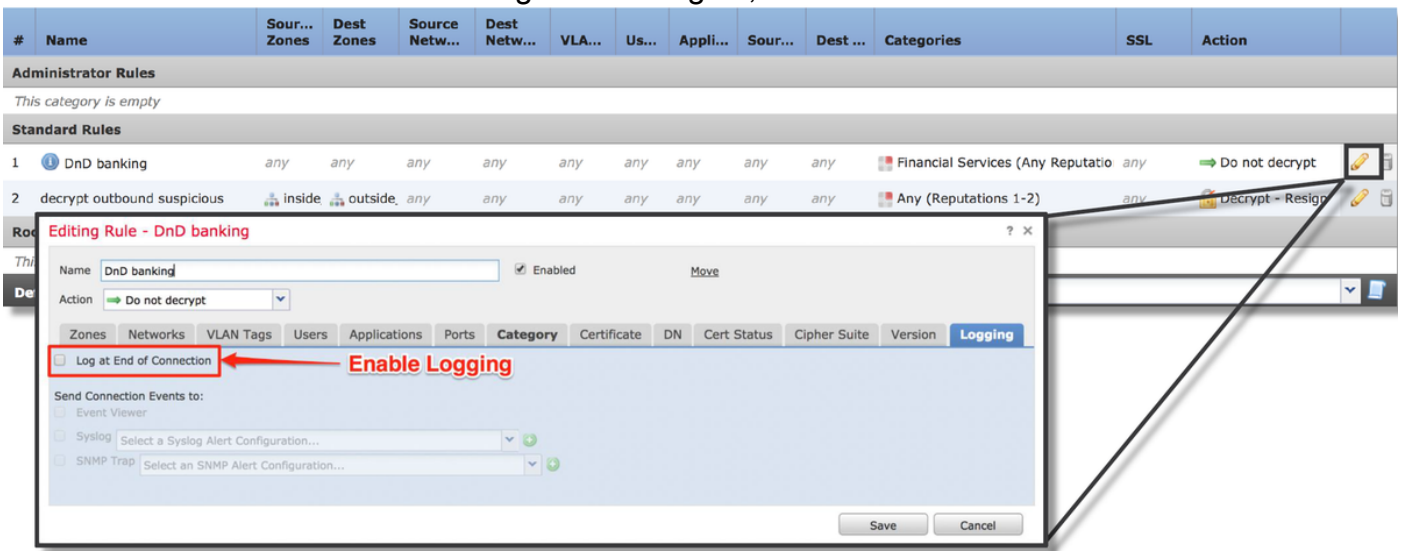


Detaillierte Fehlerbehebung für die Zugriffskontrollrichtlinie finden Sie im entsprechenden Artikel zur Fehlerbehebung für Datenpfade.

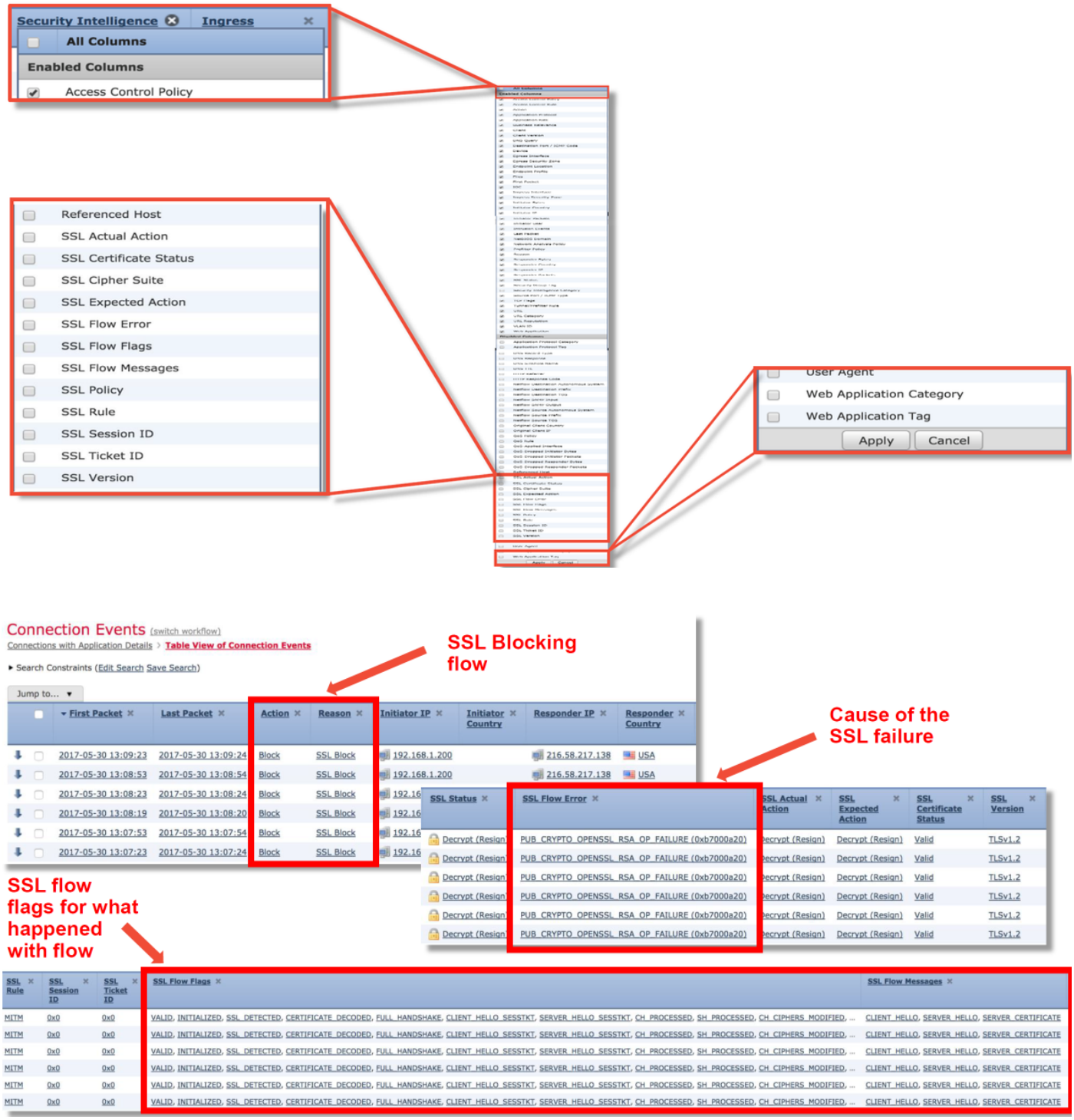
SSL-Richtlinie

Wenn SSL Policy verwendet wird, kann es sein, dass diese den Datenverkehr blockiert. Im Folgenden finden Sie einige grundlegende Schritte zur Fehlerbehebung für die SSL-Richtlinie:

- Aktivieren Sie die Protokollierung für alle Regeln, einschließlich der 'Standardaktion'.



- Überprüfen Sie die Registerkarte Unentschlüsselte Aktionen, um festzustellen, ob eine Option zum Blockieren des Datenverkehrs festgelegt ist.
- Aktivieren Sie im Abschnitt Connection events (Verbindungsereignisse) alle Felder mit dem Namen 'SSL'.
  Die meisten sind standardmäßig deaktiviert und müssen im Connection Events Viewer aktiviert werden, indem Sie auf das Kreuz neben einem Spaltennamen klicken.



- Erstellen Sie eine leere SSL-Richtlinie, wobei Do not Decrypt als Standardaktion als Eindämmungsschritt verwendet wird.
- Entfernen Sie die SSL-Richtlinie als Eindämmungsschritt aus der Zugriffskontrollrichtlinie. Dies wird auf der Registerkarte Erweitert festgelegt.

Es wird vermutet, dass die SSL-Richtlinie den Datenverkehr verwirft. Die Verbindungsereignisse zusammen mit der Richtlinienkonfiguration können an das TAC gesendet werden.

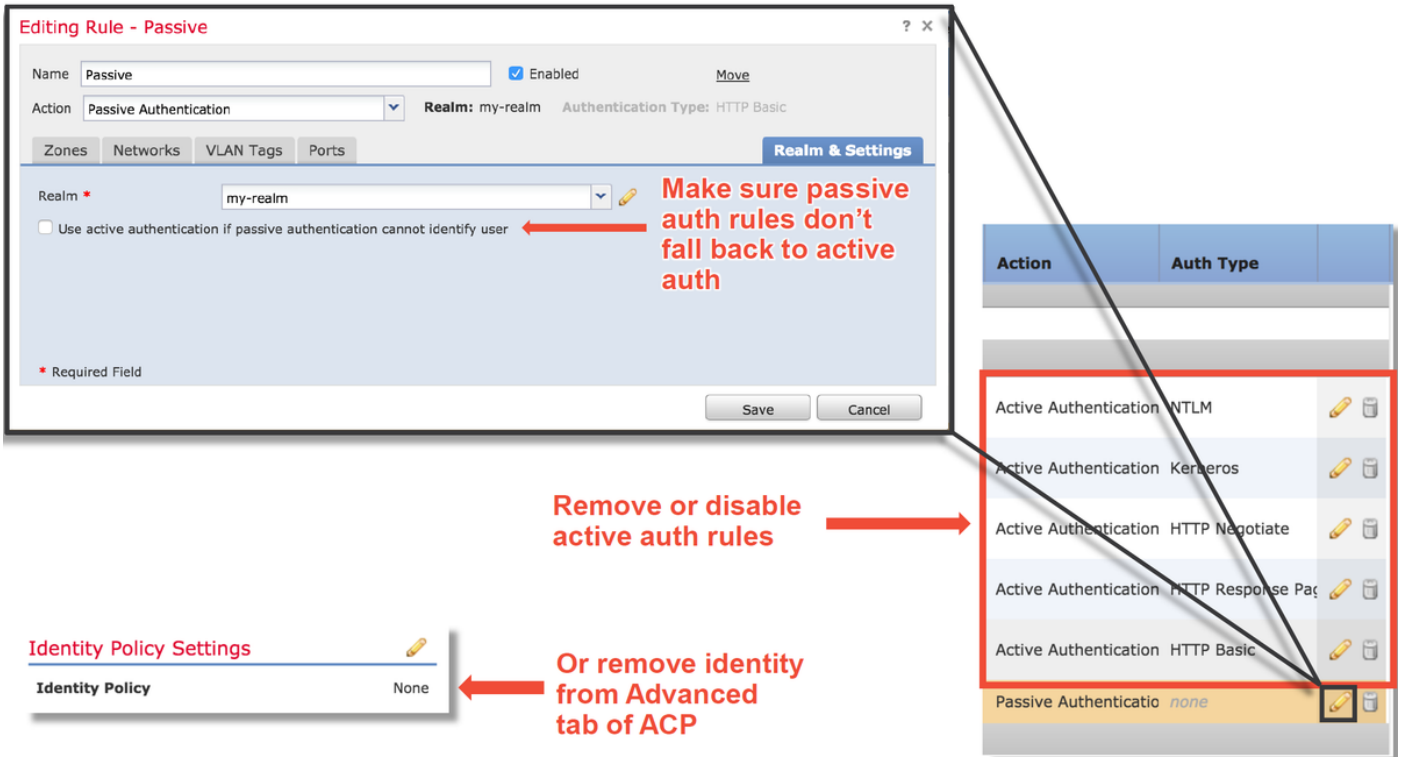
Weitere Informationen zur Fehlerbehebung der SSL-Richtlinie finden Sie im entsprechenden Artikel zur Fehlerbehebung für den Datenpfad.

Aktive Authentifizierung

Bei Verwendung in einer Identitätsrichtlinie kann mit Active Authentication Datenverkehr verworfen werden, der zugelassen werden sollte, wenn etwas schief läuft. Die aktive Authentifizierungsfunktion selbst kann sich direkt auf den gesamten HTTP-/HTTPS-Datenverkehr auswirken, denn wenn festgestellt wird, dass ein Benutzer authentifiziert werden muss, geschieht dies ausschließlich über das HTTP-Protokoll. Dies bedeutet, dass die aktive Authentifizierung keine Auswirkungen auf andere Netzwerkdienste (wie DNS, ICMP usw.) haben sollte, es sei denn, Sie verfügen über spezifische Zugriffskontrollregeln, die basierend auf dem Benutzer blockiert werden. Die Benutzer können sich nicht über die aktiven Authentifizierungsdienste auf der FTD authentifizieren. Dies wäre jedoch kein direktes Problem mit der aktiven Authentifizierungsfunktion, sondern das Ergebnis, dass Benutzer sich nicht authentifizieren können und eine Richtlinie vorhanden ist, die nicht authentifizierte Benutzer blockiert.

Ein schneller Schritt zur Risikominderung wäre die Deaktivierung einer Regel innerhalb der Identitätsrichtlinie mithilfe von "Active Authentication" (Aktive Authentifizierung).

Stellen Sie außerdem sicher, dass bei Regeln mit der Aktion 'Passive Authentication' die Option 'Use active authentication if passive authentication cannot identification user' nicht aktiviert ist.



Weitere Informationen zur Fehlerbehebung für die aktive Authentifizierung finden Sie im entsprechenden Artikel zur Fehlerbehebung für den Datenpfad.

Richtlinie für Sicherheitsrisiken

Eine Intrusion Policy kann Datenverkehr verwerfen oder Netzwerklatenz verursachen. Eine Intrusion Policy kann an einer der folgenden drei Stellen in der Zugriffskontrollrichtlinie verwendet werden:

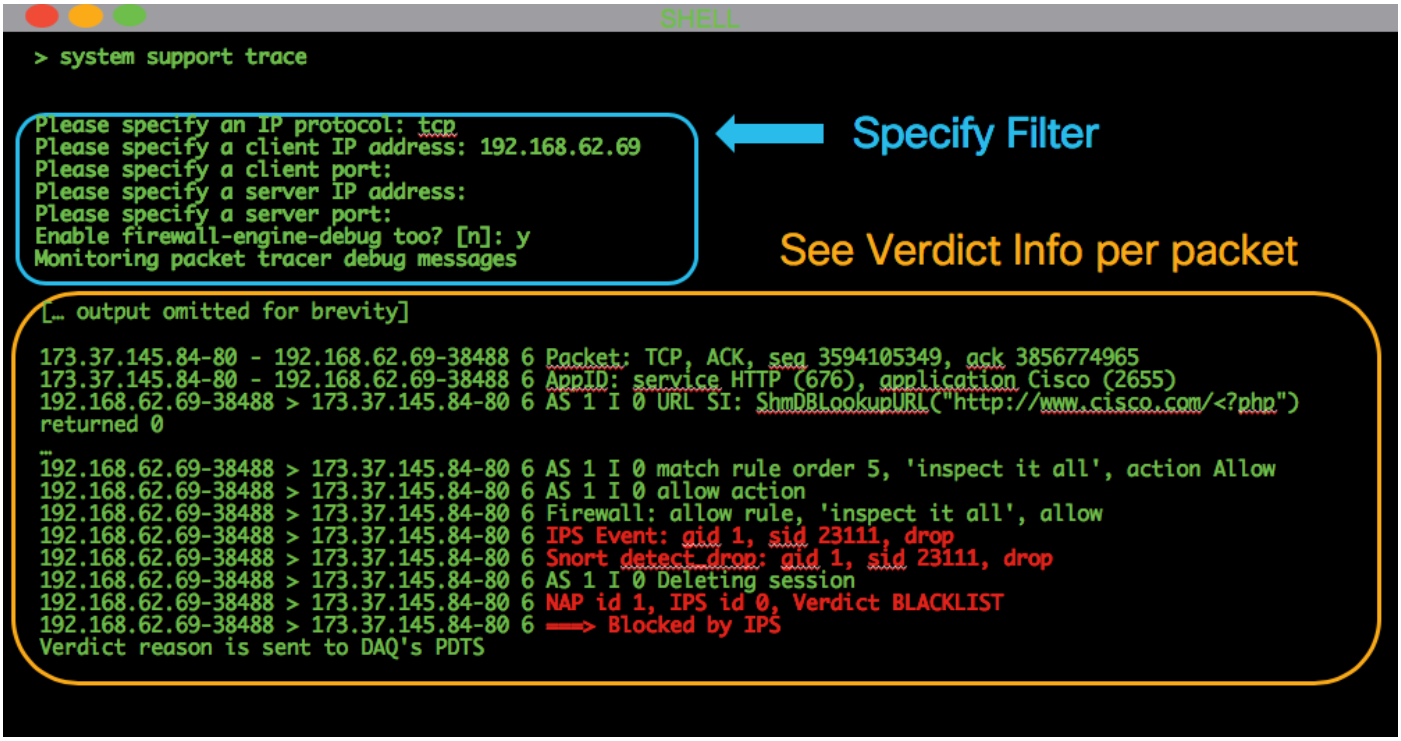
- In einer Zugriffskontrollregel auf der Registerkarte "Inspektion"
- In der Standardaktion
- Auf der Registerkarte Erweitert im Bereich **Netzwerkanalyse und Zugriffsrichtlinien > Zugriffsrichtlinie**, **die vor der Zugriffskontrollregel verwendet wird, wird der** Abschnitt

festgelegt.

Um festzustellen, ob eine Intrusion Policy-Regel Datenverkehr blockiert, navigieren Sie zur Seite **Analysis > Intrusions > Events** (Analyse > Intrusions > Ereignisse) im FMC. Die **Tabellenansicht von Angriffsereignissen** enthält Informationen über die an den Ereignissen beteiligten Hosts. Informationen zur Ereignisanalyse finden Sie im entsprechenden Artikel zur Fehlerbehebung für Datenpfade.

Der erste empfohlene Schritt zur Feststellung, ob eine Intrusion Policy Signature (IPS) den Datenverkehr blockiert, besteht darin, die **> System Support Trace-**Funktion aus der CLI der FTD zu verwenden. Dieser Debugbefehl funktioniert ähnlich wie das Debuggen von Firewall-Engines und bietet Ihnen außerdem die Möglichkeit, das Debuggen von Firewall-Engines neben der Ablaufverfolgung zu aktivieren.

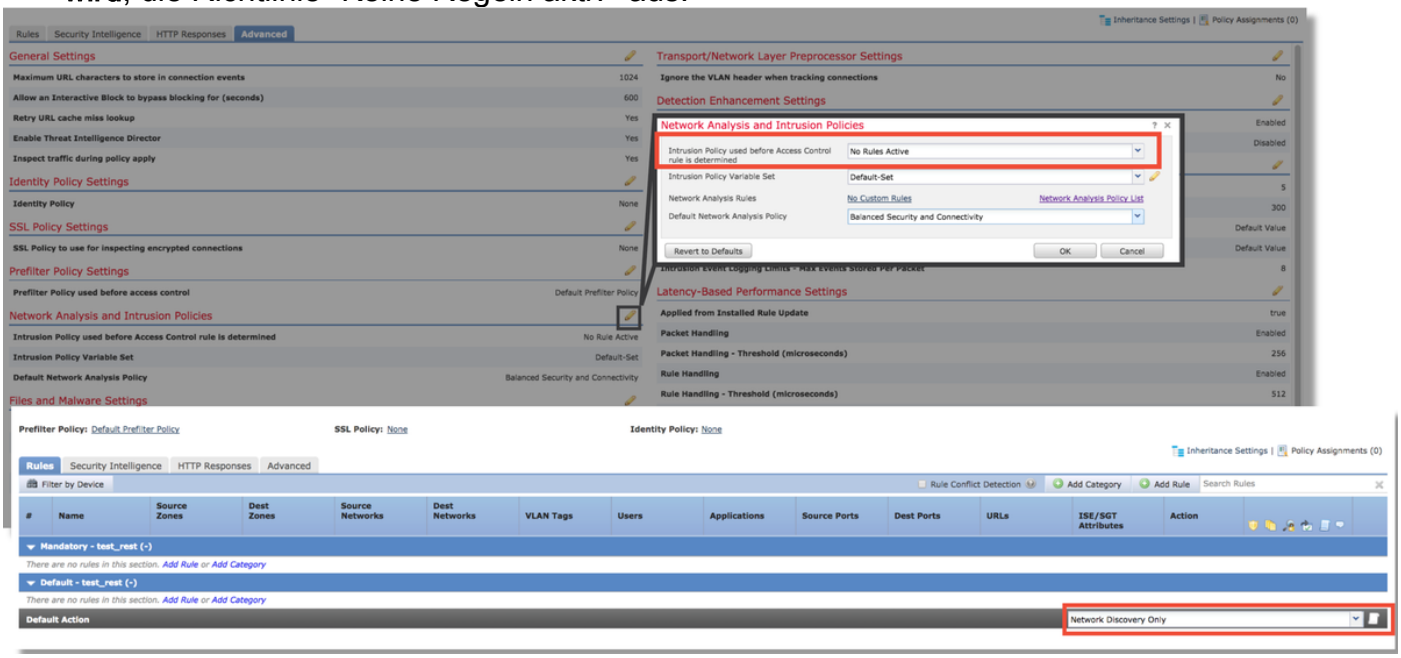
Die Abbildung unten zeigt ein Beispiel für die Verwendung des Trace-Tools zur Systemunterstützung, bei dem das Ergebnis zeigte, dass ein Paket aufgrund einer Intrusion-Regel blockiert wurde. Hier finden Sie alle Details wie die GID (Group Identifier), die SID (Signature Identifier), die NAP (Network Analysis Policy)-ID und die IPS-ID, sodass Sie genau sehen können, welche Richtlinie/Regel diesen Datenverkehr blockiert.



Wenn Sie nicht feststellen können, dass IPS die Ablaufverfolgungsausgabe blockiert, aber vermuten, dass IPS aufgrund einer benutzerdefinierten Intrusion Policy (Richtlinie für Sicherheitsrisiken) verworfen wird, können Sie die Intrusion Policy durch eine Richtlinie für "Balanced Security and Connectivity" (Ausgeglichene Sicherheit und Konnektivität) oder eine Richtlinie für "Connectivity over Security" ersetzen. Dies sind von Cisco bereitgestellte Intrusion Policies (Intrusion Policies). Wenn Sie diese Änderung vornehmen, wird das Problem behoben, und die zuvor verwendete benutzerdefinierte Richtlinie für Sicherheitsrisiken kann vom TAC überprüft werden. Wenn bereits eine Cisco Standardrichtlinie verwendet wird, können Sie versuchen, die Standardeinstellung auf eine weniger sichere Richtlinie zu ändern, da diese über weniger Regeln verfügt. Dies kann zur Eingrenzung des Bereichs beitragen. Wenn z. B. Datenverkehr blockiert wird und eine ausgeglichene Richtlinie verwendet wird, dann wird die Verbindung über Sicherheitsrichtlinien hergestellt, und das Problem verschwindet, ist es wahrscheinlich, dass es eine Regel in der Richtlinie für die ausgewogene Verteilung gibt, die den Datenverkehr verwirft, der bei der Anbindung über Sicherheitsrichtlinien nicht fallen soll.

Die folgenden Änderungen können in der Zugriffskontrollrichtlinie vorgenommen werden, um alle intrusion Policy Inspection-Blockierungsmöglichkeiten zu eliminieren (es wird empfohlen, so wenig Änderungen wie möglich vorzunehmen, um die Sicherheit nicht zu verändern. Daher wird empfohlen, für den betreffenden Datenverkehr zielgerichtete AC-Regeln einzuführen, anstatt IPS in der gesamten Richtlinie zu deaktivieren):

- Entfernen Sie in allen Zugriffskontrollregeln (oder nur bei der Regel(n), dass der jeweilige Datenverkehr mit dem betroffenen Datenverkehr übereinstimmt) die Intrusion Policy (Intrusionsrichtlinie) von der Registerkarte Inspection (Inspektion).
- Wählen Sie auf der Registerkarte Erweitert im Abschnitt **Netzwerkanalyse und Zugriffsrichtlinien > Zugriffsrichtlinie, die vor Festlegung der Zugriffskontrollregel verwendet wird**, die Richtlinie "Keine Regeln aktiv" aus.



Wenn das Problem dadurch immer noch nicht behoben wird, fahren Sie mit der Fehlerbehebung für die Network Analysis Policy fort.

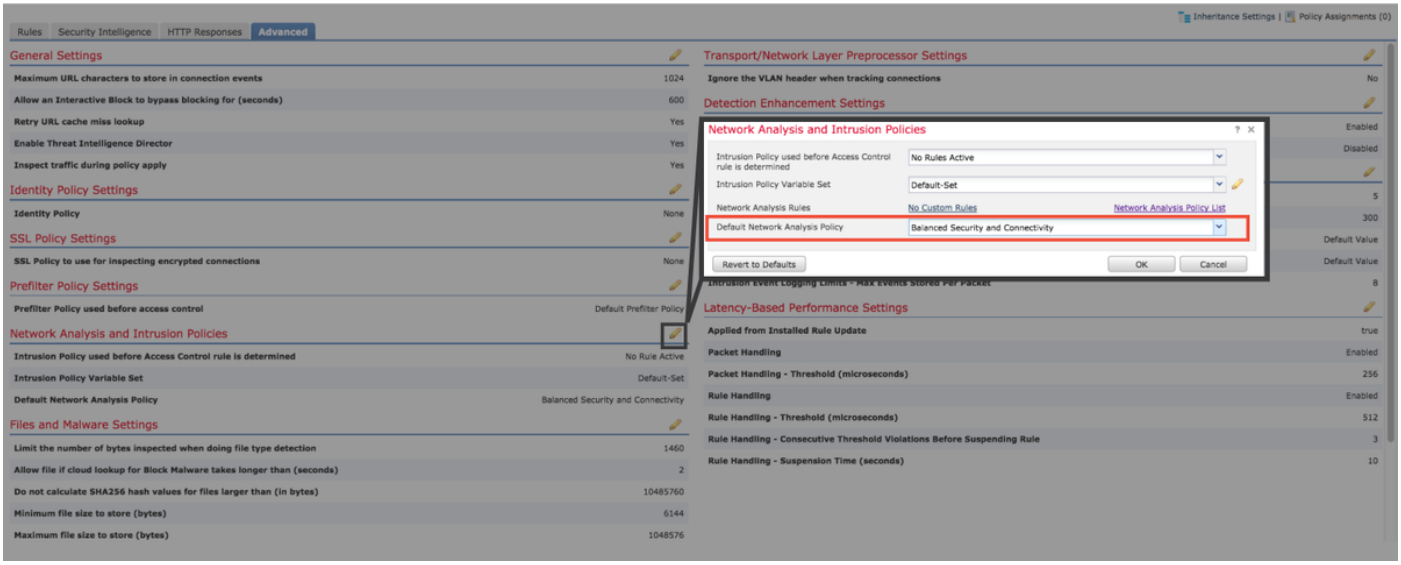
Weitere Informationen zur Fehlerbehebung im Zusammenhang mit der Intrusion Policy-Funktion finden Sie im entsprechenden Artikel zur Fehlerbehebung für Datenpfade.

Richtlinie für Netzwerkanalysen

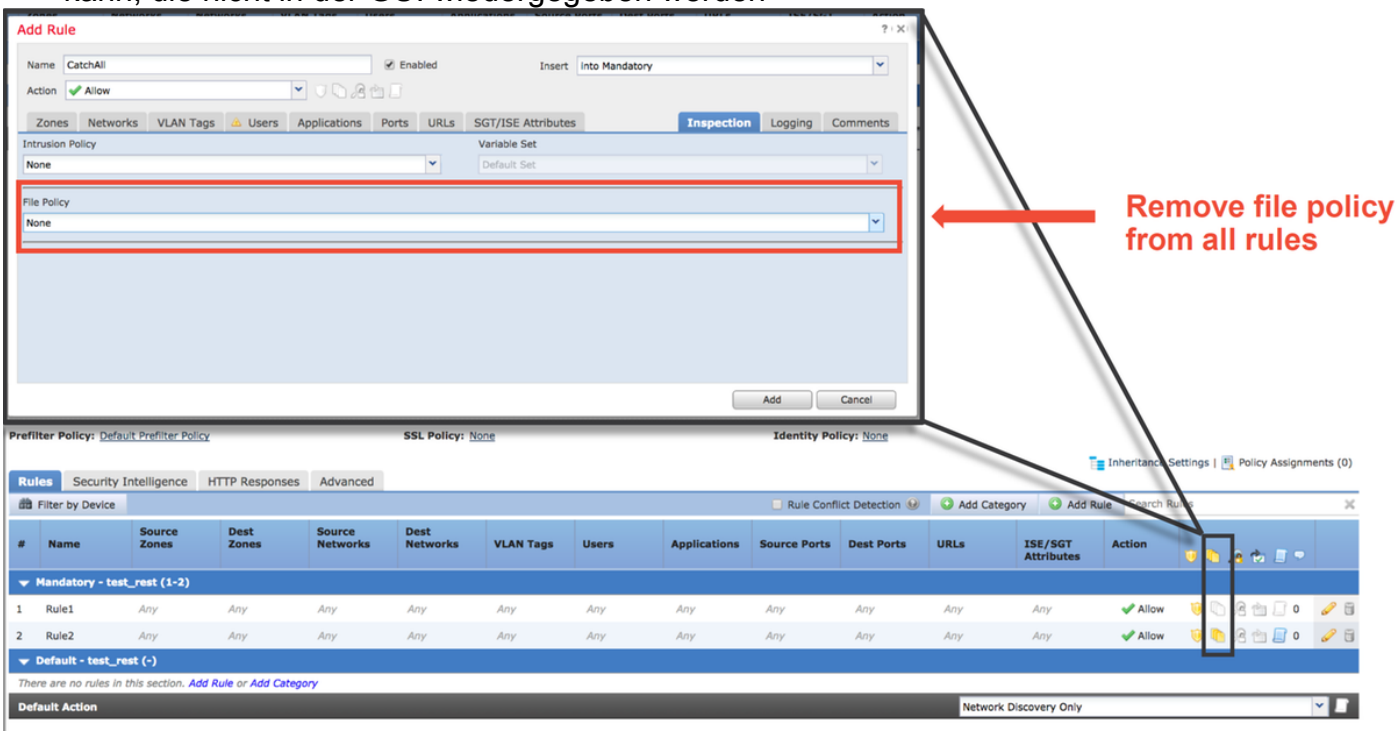
Die Network Analysis Policy (NAP) enthält die FirePOWER-Präprozessoreinstellungen, von denen einige den Datenverkehr verwerfen können. Der erste empfohlene Schritt zur Fehlerbehebung ist der gleiche wie bei der IPS-Fehlerbehebung, bei der das **> System Support Trace**-Tool verwendet wird, um herauszufinden, was in der Snort den Datenverkehr blockiert. Weitere Informationen zu diesem Tool und zur Verwendung von Beispielen finden Sie im Abschnitt "Intrusion Policy" weiter oben.

Um mögliche Probleme mit dem NAP schnell zu beheben, können folgende Schritte durchgeführt werden:

- Wenn ein benutzerdefiniertes NAP verwendet wird, ersetzen Sie es durch eine "Balanced Security and Connectivity"- oder "Connectivity over Security"-Richtlinie



- Wenn benutzerdefinierte Regeln verwendet werden, stellen Sie sicher, dass für das NAP eine der oben genannten Standardeinstellungen festgelegt wird.
- Wenn Zugriffskontrollregeln eine Dateirichtlinie verwenden, entfernen Sie diese vorübergehend, da eine Dateirichtlinie die Vorprozessoreinstellungen am Back-End aktivieren kann, die nicht in der GUI wiedergegeben werden



Detailliertere Fehlerbehebung für die Network Analysis Policy-Funktion kann in diesem Artikel überprüft werden.

Zugehörige Informationen

Links zur FirePOWER-Dokumentation

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