# Fehlerbehebung für FirePOWER Data Path 3: Sicherheitsinformationen

## Inhalt



## Einführung

Dieser Artikel ist Teil einer Reihe von Artikeln, in denen erläutert wird, wie der Datenpfad auf FirePOWER-Systemen systematisch behoben wird, um festzustellen, ob Komponenten von FirePOWER den Datenverkehr beeinträchtigen können. Weitere Informationen zur Architektur von FirePOWER-Plattformen und Links zu anderen Artikeln zur Fehlerbehebung für Datenpfade finden Sie im Übersichtsartikel.

In diesem Artikel wird die dritte Phase der Fehlerbehebung für den FirePOWER-Datenpfad beschrieben, die Funktion "Security Intelligence".


## Voraussetzungen

- Dieser Artikel bezieht sich auf alle derzeit unterstützten Firepower-Plattformen
- Security Intelligence für URLs und DNS wurde in Version 6.0.0 eingeführt.

## Fehlerbehebung in der FirePOWER Security Intelligence-Phase

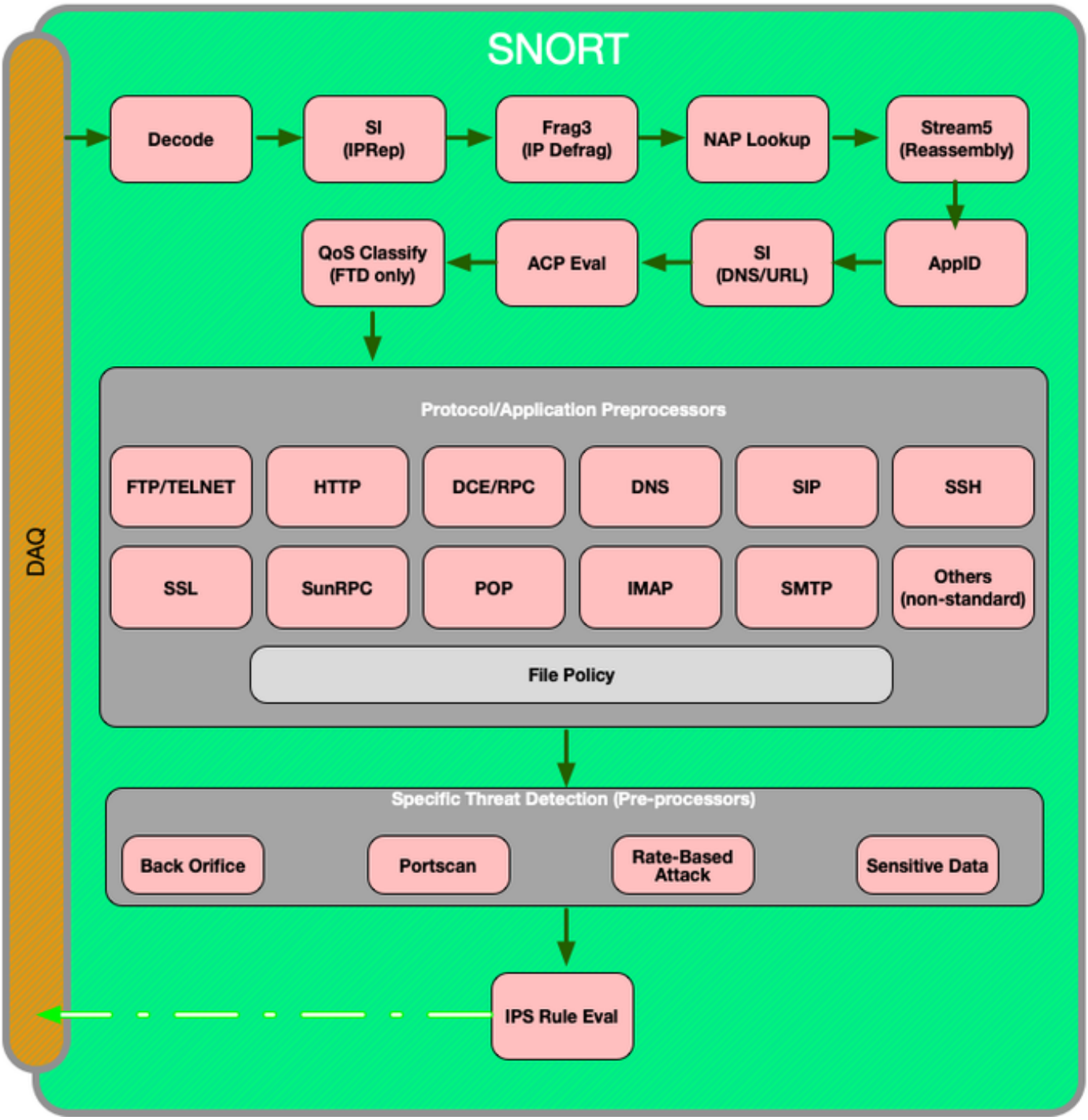
Sicherheitsintelligenz ist eine Funktion, die sowohl Blacklists als auch Whitelists prüft, um Folgendes zu erreichen:

- IP-Adressen (in bestimmten Bereichen der Benutzeroberfläche auch als "Netzwerke" bezeichnet)
- Uniform Resource Locators (URLs)
- DNS-Abfragen (Domain Name System)

Die Listen in Security Intelligence können durch von Cisco bereitgestellte Feeds und/oder

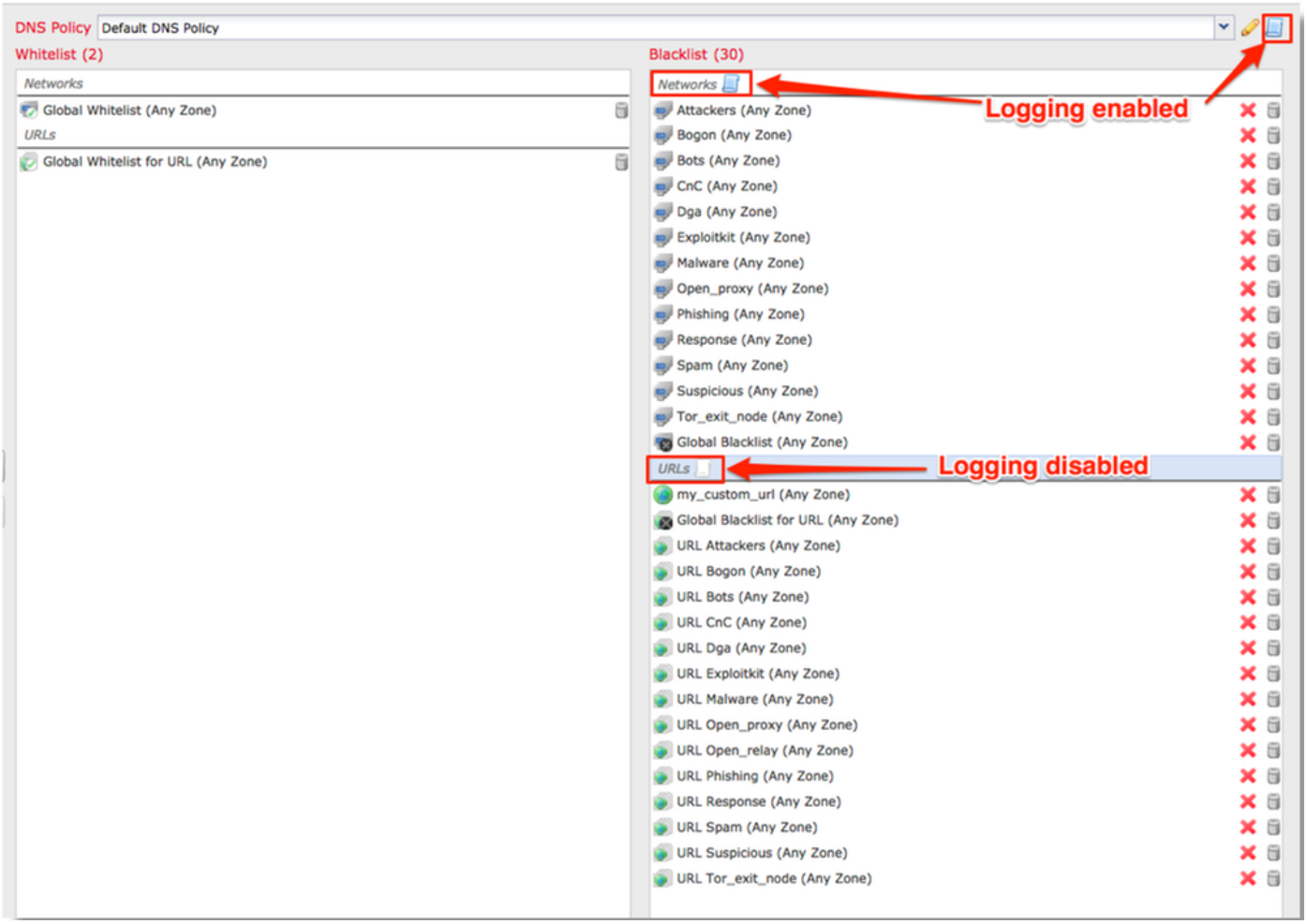
benutzerdefinierte Listen und Feeds ergänzt werden.

Die auf IP-Adressen basierende Reputation der Sicherheitsintelligenz ist die erste Komponente in FirePOWER, die den Datenverkehr überprüft. URL- und DNS-Sicherheitsinformationen werden ausgeführt, sobald das entsprechende Anwendungsprotokoll erkannt wird. Im folgenden Diagramm wird der FirePOWER-Softwareprüfungsworkflow dargestellt.




## Stellen Sie fest, ob die Protokollierung für Sicherheitsinformationsereignisse aktiviert ist.

Blöcke auf der Sicherheitsinformationsebene lassen sich sehr einfach festlegen, solange die Protokollierung aktiviert ist. Dies kann über die FMC-Benutzeroberfläche (FirePOWER Management Center) festgestellt werden, indem Sie zu **Richtlinien > Zugriffskontrolle > Zugriffskontrollrichtlinie** navigieren. Navigieren Sie nach dem Klicken auf das Bearbeitungssymbol neben der betreffenden Richtlinie zur Registerkarte **Sicherheitsinformationen**.

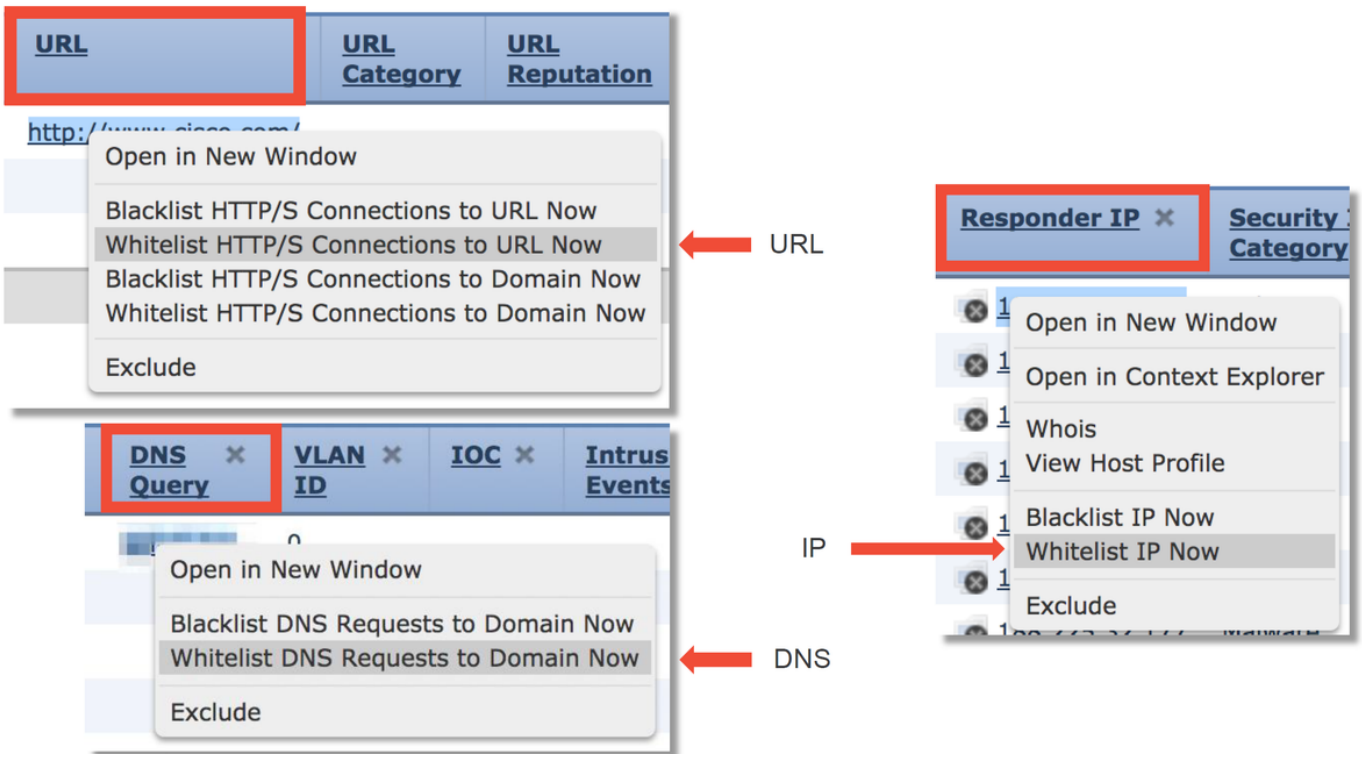




# Überprüfen Sie die Sicherheitsinformationsereignisse.

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

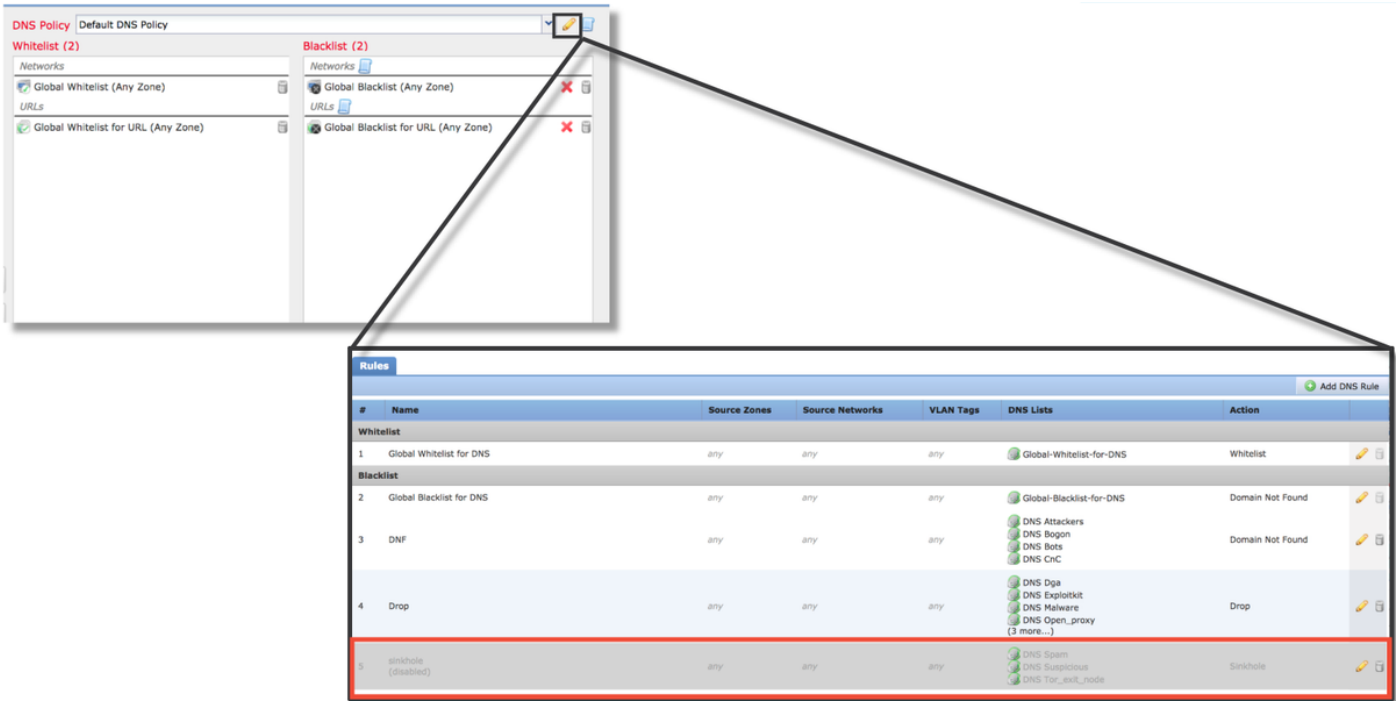
Sie können die Daten auch dem Cisco Technical Assistance Center (TAC) übermitteln, um zu ermitteln, ob ein Artikel aus der Blacklist entfernt werden sollte.

> **Hinweis:** Durch Hinzufügen zur Whitelist wird der betreffenden Whitelist nur ein Eintrag hinzugefügt, d. h. das Objekt kann die Sicherheitsinformations-Prüfung übergeben. Alle anderen FirePOWER-Komponenten können den Datenverkehr jedoch weiterhin überprüfen.

## Entfernen der Sicherheitsinformations-Konfigurationen

Um die Security Intelligence-Konfigurationen zu entfernen, navigieren Sie zur Registerkarte **Security Intelligence** (Sicherheitsintelligenz), wie oben beschrieben. Es gibt drei Abschnitte: eine für Netzwerke, eine URL sowie eine Richtlinie für DNS.

Von dort aus können die Listen und Feeds entfernt werden, indem man auf das Papierkorbsymbol klickt.




Im obigen Screenshot wird darauf hingewiesen, dass alle IP- und URL-Sicherheitsinformationslisten außer der globalen Blacklist und Whitelist entfernt wurden.

In der DNS-Richtlinie, in der die DNS-Sicherheitsinformationskonfiguration gespeichert ist, wird eine der Regeln deaktiviert.

> **Hinweis**: Um den Inhalt der globalen Blacklists und Whitelists anzuzeigen, navigieren Sie zu **Objects > Object Management > Security Intelligence**. Klicken Sie dann auf den Bereich von Interesse (Netzwerk, URL, DNS). Beim Bearbeiten einer Liste wird dann der Inhalt angezeigt. Die Konfiguration muss jedoch innerhalb der Zugriffskontrollrichtlinie durchgeführt werden.

# Überprüfen der Konfiguration am Backend

Die Konfiguration der Sicherheitsinformationen kann über den Befehl **> show access-control-config in der CLI überprüft werden**, der den Inhalt der aktiven Zugriffskontrollrichtlinie anzeigt, die auf dem FirePOWER-Gerät ausgeführt wird.

```
> 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]
```

Im obigen Beispiel ist die Protokollierung für die Netzwerk-Blacklist konfiguriert, und mindestens zwei Feeds wurden in die Blacklist aufgenommen (Angreifer und Bogon).

Ob sich ein einzelnes Element in einer Sicherheitsinformationsliste befindet, kann im Expertenmodus bestimmt werden. Bitte beachten Sie die folgenden Schritte:

```
> 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



$ 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



$ 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
```

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

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

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

Es gibt eine Datei für jede Sicherheitsinformationsliste mit einer eindeutigen UID. Im obigen

Beispiel wird veranschaulicht, wie der Name der Liste mithilfe des Befehls **head -n1** identifiziert wird.

## Daten für TAC

| Daten | Anweisungen |
| --- | --- |
| Fehlerbehebung bei Dateien vom FMC und FirePOWER-Gerät, die den Datenverkehr überprüfen | http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/11766 |
| Screenshots der Ereignisse (mit Zeitstempeln) | Anweisungen hierzu finden Sie in diesem Artikel |
| Textausgabe aus CLI-Sitzungen | Anweisungen hierzu finden Sie in diesem Artikel |
| Wenn Sie einen falsch positiven Fall einsenden, geben Sie das anzufechtende Element (IP, URL, Domain) an. | Erläutern Sie, warum der Streit durchgeführt werden sollte. |

## Nächster Schritt

Wenn festgestellt wurde, dass die Security Intelligence-Komponente nicht die Ursache des Problems ist, besteht der nächste Schritt in der Fehlerbehebung für die Zugriffskontrollrichtlinien.

Klicken Sie hier, um mit dem nächsten Artikel fortzufahren.