Dépannage du chemin de données Firepower Phase 5 : Stratégie SSL

Contenu

Introduction

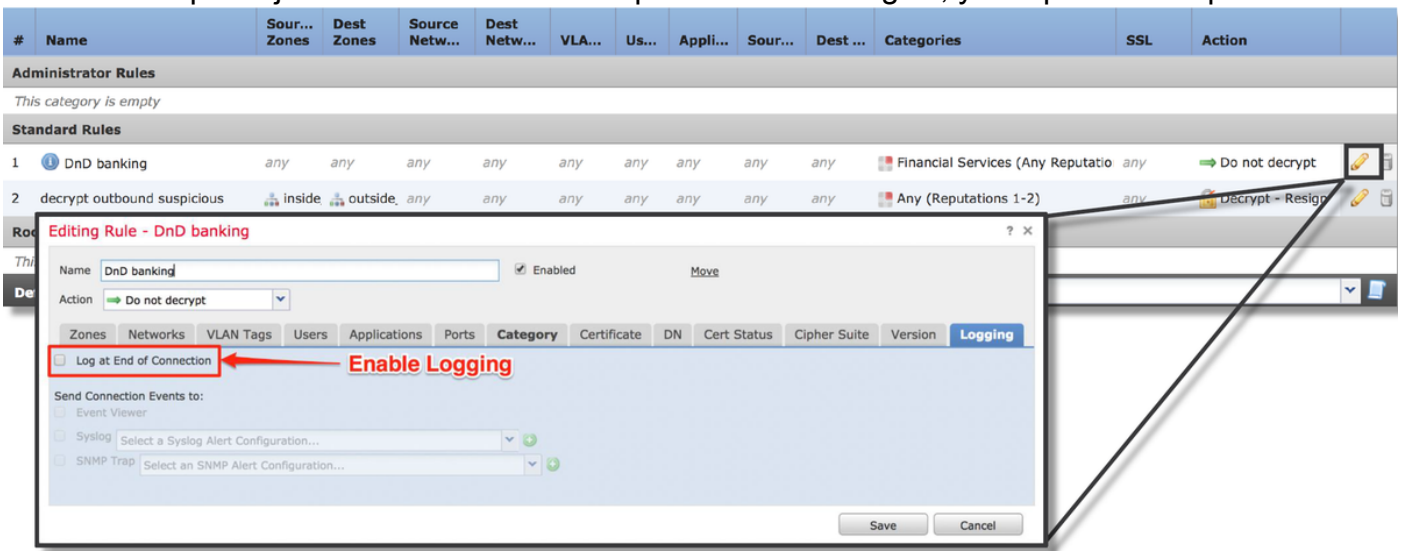
Cet article fait partie d'une série d'articles qui expliquent comment dépanner systématiquement le chemin de données sur les systèmes Firepower pour déterminer si les composants de Firepower peuvent affecter le trafic. Reportez-vous à l'article Présentation pour obtenir des informations sur l'architecture des plates-formes Firepower et des liens vers les autres articles de dépannage du chemin de données.

Cet article couvre la cinquième étape du dépannage du chemin de données Firepower, la fonction de stratégie SSL (Secure Sockets Layer).

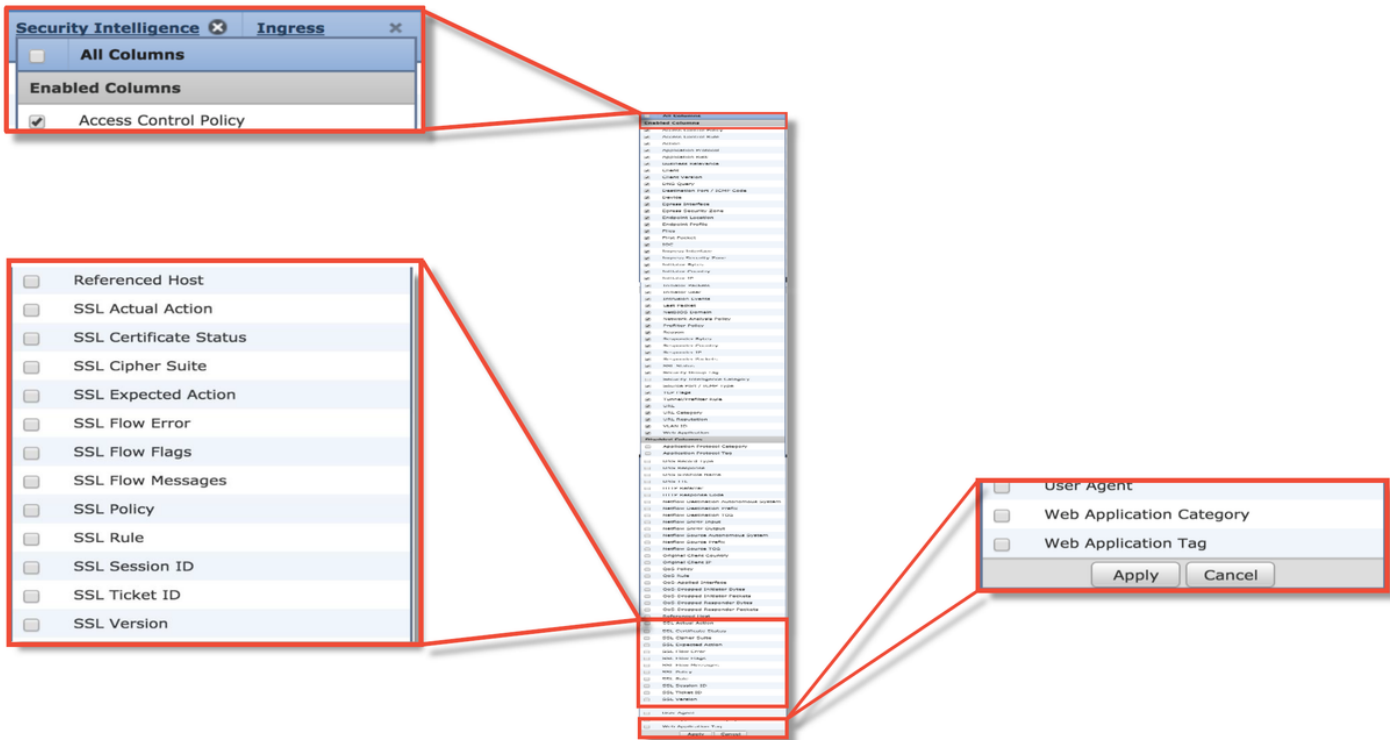
Conditions préalables

- Les informations de cet article s'appliquent à toute plate-forme Firepower Décryptage SSL pour ASA (Adaptive Security Appliance) avec les services FirePOWER (module SFR) uniquement disponible dans la version 6.0+La fonction de modification Hello du client n'est disponible que dans la version 6.1+
- Confirmer que la stratégie SSL est utilisée dans la stratégie de contrôle d'accès

- Vérifiez que la journalisation est activée pour toutes les règles, y compris 'Action par défaut'



- Cochez l'onglet Actions non décryptables pour voir si une option est définie pour bloquer le trafic
- Dans les événements Connection, lorsque vous êtes dans la table des événements de connexion, activez tous les champs avec 'SSL' dans le nom
  La plupart sont désactivées par défaut et doivent être activées dans la visionneuse Événements de connexion



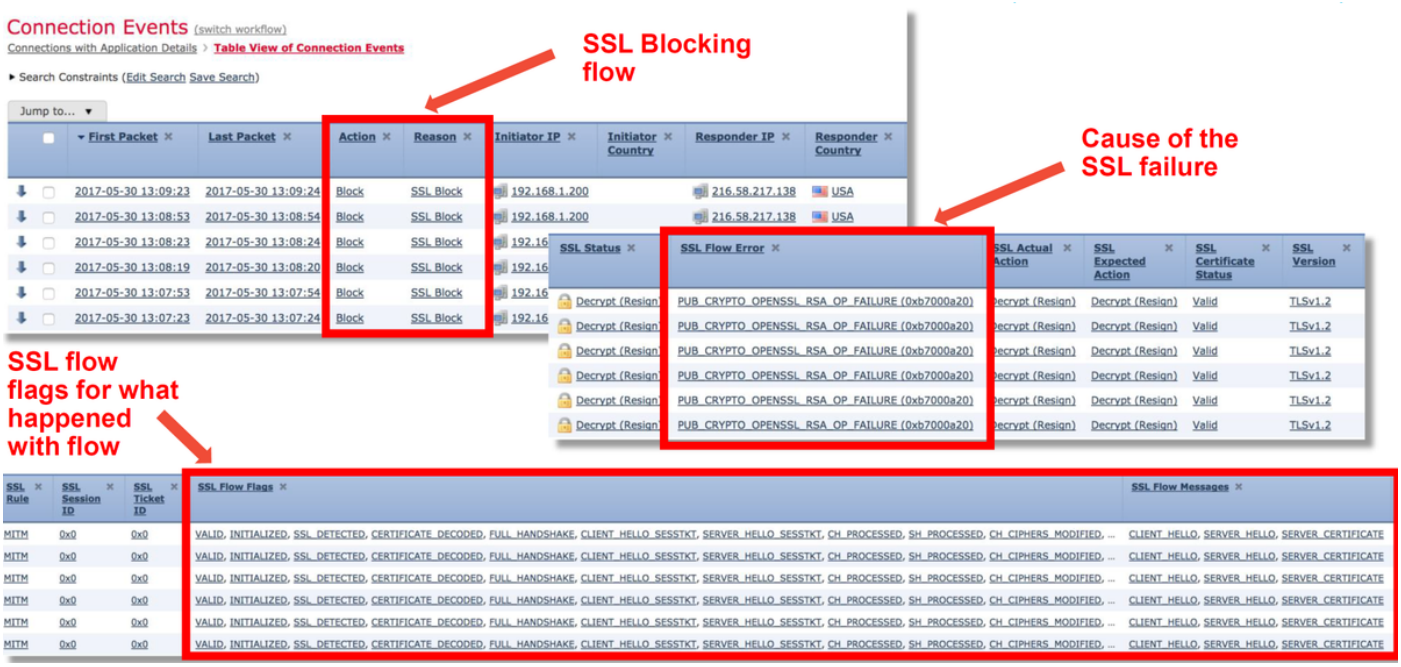
Dépannage de la phase de stratégie SSL

Des étapes spécifiques peuvent être suivies pour aider à comprendre pourquoi la stratégie SSL peut abandonner le trafic qui est censé être autorisé.

Vérifier les champs SSL dans les événements de connexion

Si la stratégie SSL est suspectée de provoquer des problèmes de trafic, la première place à vérifier est la section Événements de connexion (sous **Analyse > Connexions > Événements**) après avoir activé tous les champs SSL, comme indiqué ci-dessus.

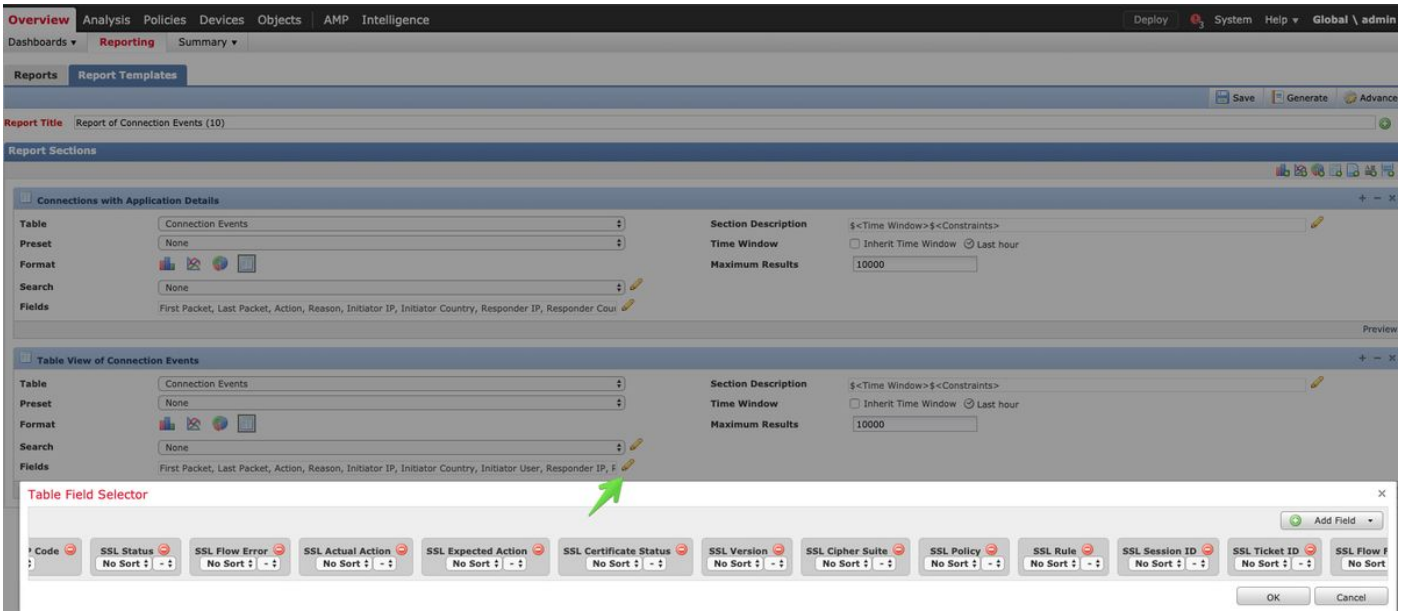
Si la stratégie SSL bloque le trafic, le champ **Motif** affiche « Bloquer SSL ». La colonne **Erreur de flux SSL** contient des informations utiles sur la raison pour laquelle le blocage s'est produit. Les autres champs SSL contiennent des informations sur les données SSL détectées par Firepower dans le flux.



Ces données peuvent être fournies au centre d'assistance technique Cisco (TAC) lors de l'ouverture d'un dossier pour la politique SSL. Pour exporter facilement ces informations, vous pouvez utiliser le bouton **Concepteur de rapports** situé dans le coin supérieur droit.

Si vous cliquez sur ce bouton dans la section Événements de connexion, les filtres et les options de fenêtre de temps sont copiés automatiquement dans le modèle de rapport.

Assurez-vous que tous les champs SSL mentionnés sont ajoutés à la section 'Champ'.



Cliquez sur **Generate** pour créer un rapport au format PDF ou CSV.

Déboguer la stratégie SSL

Si les événements de connexion ne contiennent pas suffisamment d'informations sur le flux, le débogage SSL peut être exécuté sur l'interface de ligne de commande (CLI) de Firepower.

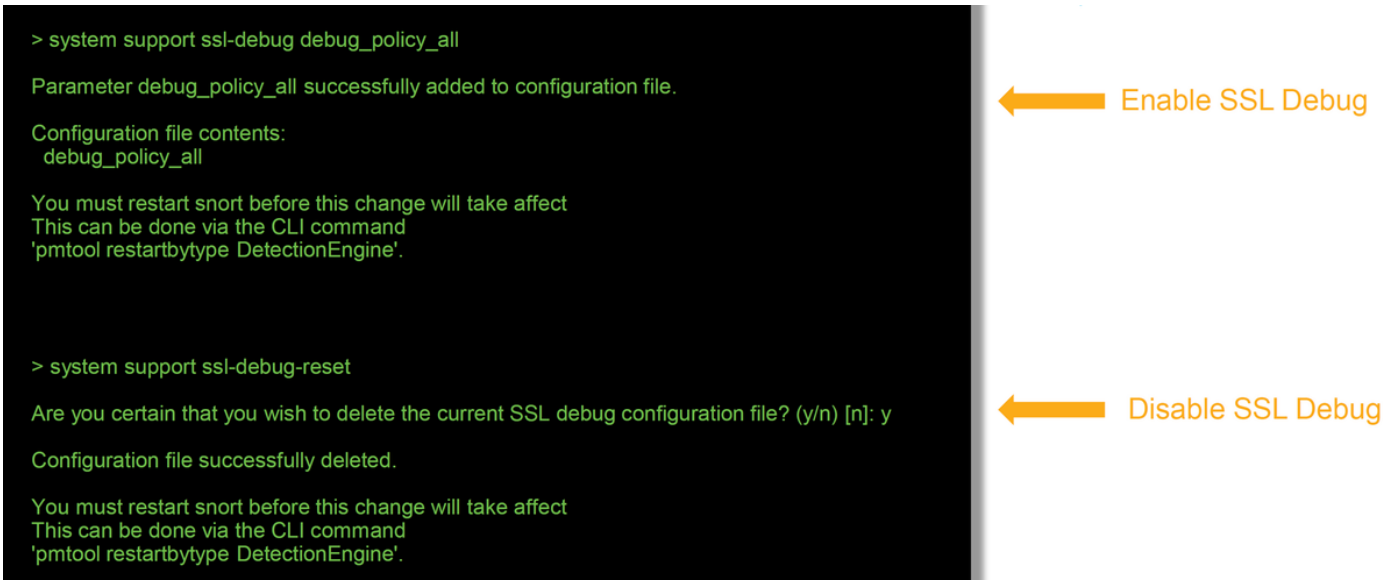
> **Note**: Tout le contenu de débogage ci-dessous est basé sur le déchiffrement SSL qui se produit dans le logiciel sur l'architecture x86. Ce contenu n'inclut pas les débogages des fonctionnalités de déchargement matériel SSL qui ont été ajoutées dans la version 6.2.3 et ultérieures, qui sont différentes.

> **Note**: Sur les plates-formes Firepower 9300 et 4100, le shell en question est accessible via les commandes suivantes :
>
> **# connexion du module 1 console**
> Firepower-module1> **connect ftd**
> **>**
>
> Pour les instances multiples, l'interface de ligne de commande du périphérique logique est accessible à l'aide des commandes suivantes.
> **# connect module 1 telnet**
> Firepower-module1> **connect ftd ftd1**
> Connexion à la console du conteneur ftd(ftd1)... Entrez « exit » pour revenir à l'interface de ligne de commande de démarrage.
> **>**

La commande **system support ssl-debug debug_policy_all** peut être exécutée pour générer des informations de débogage pour chaque flux traité par la stratégie SSL.

> **Attention** : Le processus Snort doit être redémarré avant et après l'exécution du débogage SSL, ce qui peut entraîner l'abandon de quelques paquets en fonction des stratégies Snort down et du déploiement utilisé. Le trafic TCP sera retransmis, mais le trafic UDP peut être affecté de manière négative si les applications passant par le pare-feu ne tolèrent pas une

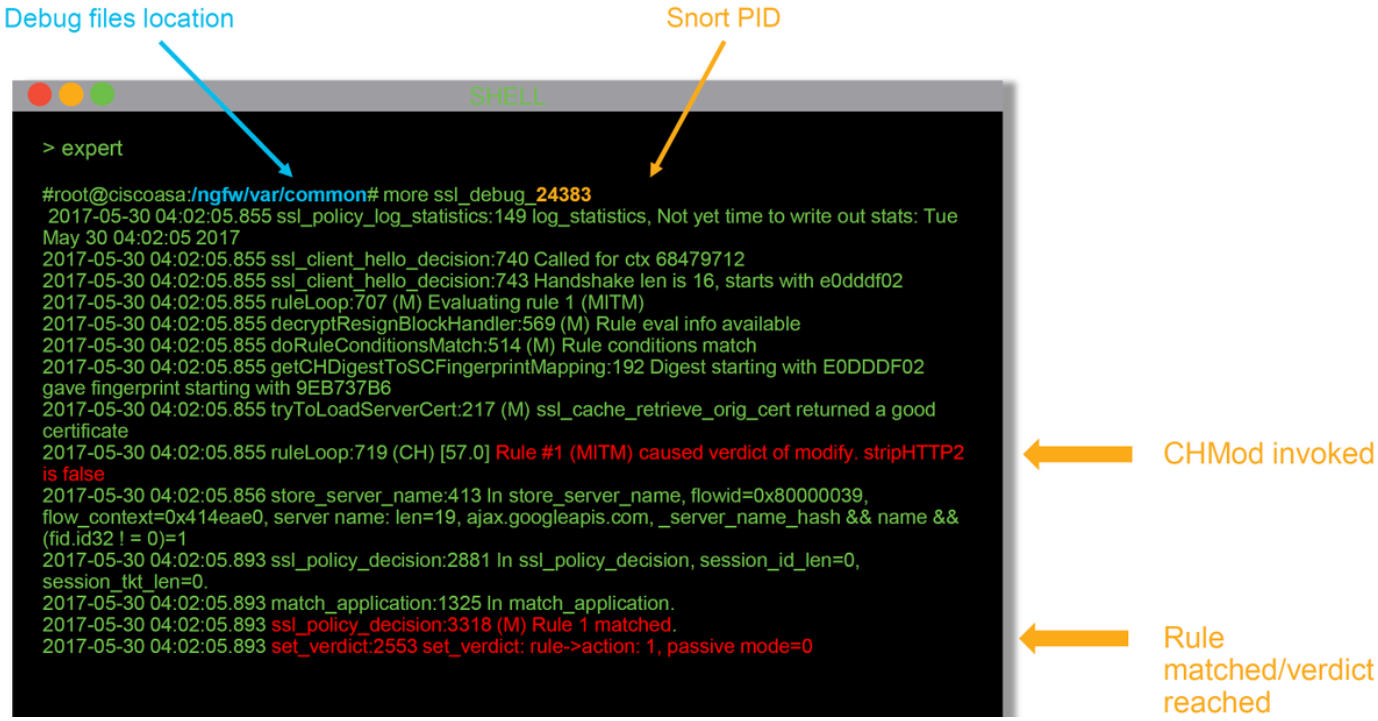
perte minimale de paquets.



Avertissement : N'oubliez pas de désactiver le débogage après la collecte des données nécessaires à l'aide de la commande **system support ssl-debug-reset**.

Il y aura un fichier écrit pour chaque processus Snort exécuté sur le périphérique Firepower. L'emplacement des fichiers sera le suivant :

- **/var/common** pour les plates-formes non FTD
- **/ngfw/var/common** pour plates-formes FTD



Voici quelques-uns des champs utiles dans les journaux de débogage.

```
...
2017-05-30 04:02:05.893  Verdict callback.
 Logstr: ssl_policy_decision: Found matching rule.
   Process ID: 24383
   Flow context: 0x414eae0
   Flow info: 0x7ffea4b8ccf0
     flowid: 0x80000039
     error: 0x00000000
     cipher_suite: 49199 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
     ssl_version: TLS1.2
     server_cert_h: 89
         cert summary: CN=*.googleapis.com;O=Google Inc;
     flags: 0x40820004048181c3/0x00000088c0000000
  Connection Event: 0x7ffea4b8c9e8 messages: 0x00000038
  Policy ID: 93a182e8-1d00-11e6-9e03-b6d00120637b
     Rule ID: 1
     Logging is on: 1
     Cipher Suite: 49199 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
     SSL Version: 16 - TLS1.2
     Server Cert Status: 2 - valid ca chain,
     URL Category Matched: 0
     App ID Matched: 0
     Client Hello Server Name: (null)
     Actual Action: 6 - Decrypt and resign.
     Expected Action: 6 - Decrypt and resign.
     SSL Flow Status: 2 - success - SSL Rule successfully applied.
     SSL Flow Error: 0x00000000 - NSLIB:Logging [0x00000000;code:0;sub:0] Success;
     SSL Flow Messages: 0x00000038 - CLIENT_HELLO,SERVER_HELLO,SERVER_CERTIFICATE
```

Certificate summary can help identify the flow

Validate that Expected and Actual actions are the same

```
...
    SSL Flow Flags: 0x00000088c48181c3 -
VALID,INITIALIZED,SSL_DETECTED,CERTIFICATE_DECODED,FULL_HANDSHAKE,CLIENT_HELL
O_SESSTKT,SERVER_HELLO_SESSTKT,CH_PROCESSED,SH_PROCESSED,CH_CIPHERS_MO
DIFIED,CH_CURVES_MODIFIED,CH_EXTENSION_REMOVED,CH_ALPN_HAS_H2
    SSL Session ID:
    SSL Session Ticket:

  Network parameters:
     src_addr: 192.168.1.200
     src_port: 55113
     src_intf: 3
     src_zone: -1
     dst_addr: 216.58.218.234
     dst_port: 443
     dst_intf: 2
     dst_zone: -1
     vlan: 0
  Matching Rule:
     ordinal rule id: 1
     rule id: 1
     rule name: MITM
  Verdict:
      Flow action: 6 - Decrypt and resign.
      Error action: 2 - Block.
```

Verdict the flow reached

```
...
2017-05-30 04:02:05.894  Error callback.
 Logstr: ssl_policy_error_callback
   Process ID: 24383
   Flow context: 0x414eae0
   Flow info: 0x7ffea4b8d3a0
       flowid: 0x80000039
       error: 0xb7000a20
       FLOW ERROR FOUND:
           - NSE:PubCrypto [0xb7000a20;code:32;sub:10] OpenSSL RSA operation failure;
       cipher_suite: 65535 - Unknown
       ssl_version: UNKNOWN
       server_cert_h: -1
       flags: 0xca4a0407068181c5/0x00000088c0000000
      messages: 0x00000078
  Connection Event: 0x7ffea4b8d290
      Policy ID: 93a182e8-1d00-11e6-9e03-b6d00120637b
     [ ...Omitting for brevity ]
     SSL Flow Status: 10 - decryption_error - Error found during SSL flow after server certificate.
     SSL Flow Error: 0xb7000a20 - NSE:PubCrypto [0xb7000a20;code:32;sub:10] OpenSSL RSA
operation failure;
...
```

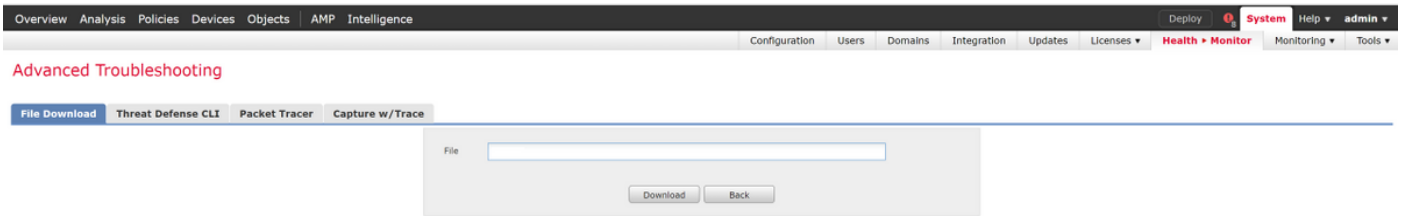
SSL Errors potentially causing drop

Note: Si une erreur de déchiffrement survient après le déchiffrement de Firepower, le trafic doit être abandonné car le pare-feu a déjà modifié/mis en place la session, de sorte qu'il

n'est pas possible pour le client et le serveur de reprendre la communication car ils ont différentes piles TCP ainsi que différentes clés de chiffrement utilisées dans le flux.

Les fichiers de débogage peuvent être copiés hors du périphérique Firepower à partir de l'invite > à l'aide des instructions de cet article.

Vous pouvez également utiliser une option sur le FMC dans Firepower version 6.2.0 et ultérieure. Pour accéder à cet utilitaire d'interface utilisateur sur le FMC, accédez à **Périphériques > Gestion des périphériques**. Cliquez ensuite sur le bouton en regard du périphérique en question, puis **Dépannage avancé > Téléchargement de fichier**. Vous pouvez ensuite entrer le nom d'un fichier en question et cliquer sur Télécharger.

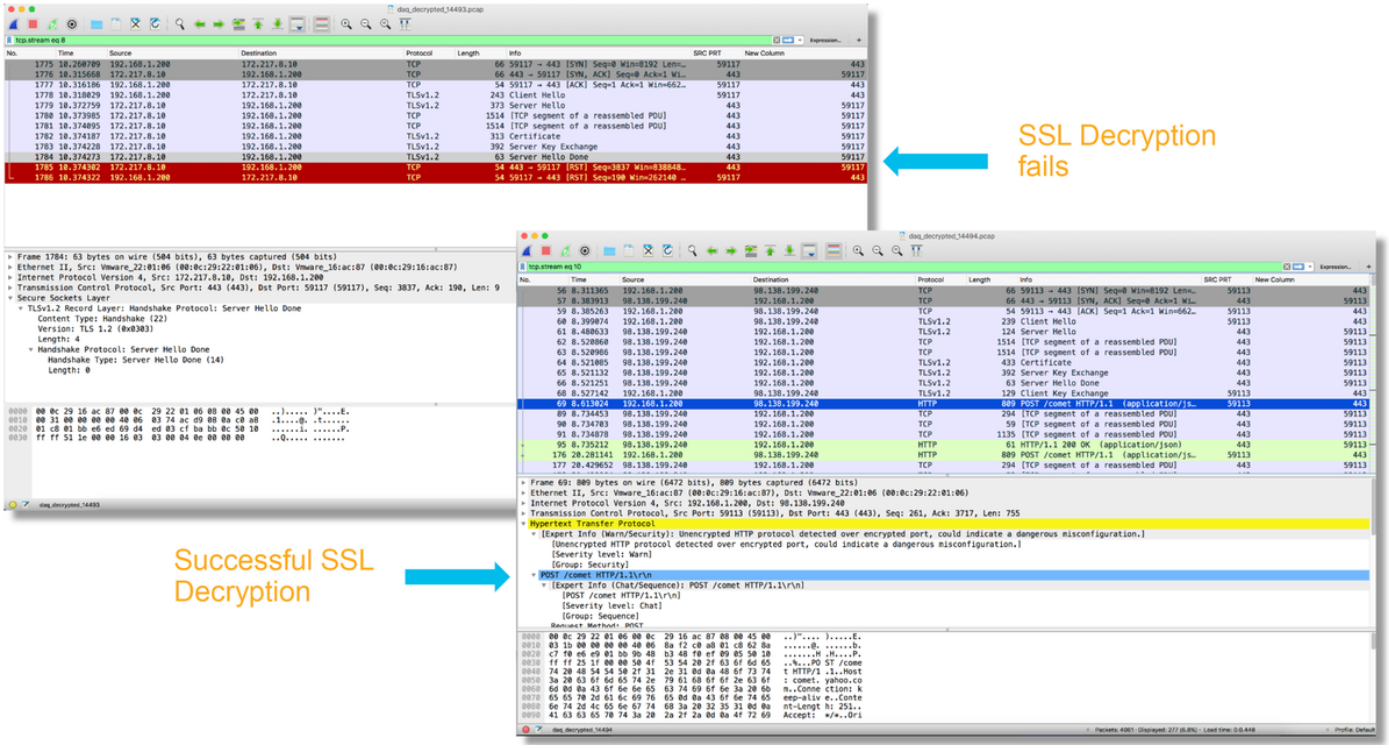


Générer une capture de paquets déchiffrée

Il est possible de collecter une capture de paquets non chiffrée pour les sessions qui sont déchiffrées par Firepower. La commande est **system support debug-DAQ debug_daq_write_pcap**

> **Attention** : Le processus Snort doit être redémarré avant de générer la capture de paquets décryptée, ce qui peut entraîner l'abandon de quelques paquets. Les protocoles avec état tels que le trafic TCP sont retransmis, mais d'autres trafics, tels que le protocole UDP, peuvent être affectés de manière négative.

```
> system support debug-DAQ debug_daq_write_pcap

Parameter debug_daq_write_pcap successfully added to configuration file.

Configuration file contents:
  debug_daq_write_pcap

You must restart snort before this change will take affect
This can be done via the CLI command
'system support pmtool restartbytype DetectionEngine'.

> system support pmtool restartbytype DetectionEngine

> expert
admin@firepower:~$ cd /var/common/
admin@firepower:/var/common$ ls
daq_decrypted_15903.pcap  daq_decrypted_15909.pcap

admin@firepower:/var/common$ tar pczf daq_pcaps.tgz daq_decrypted_*
```

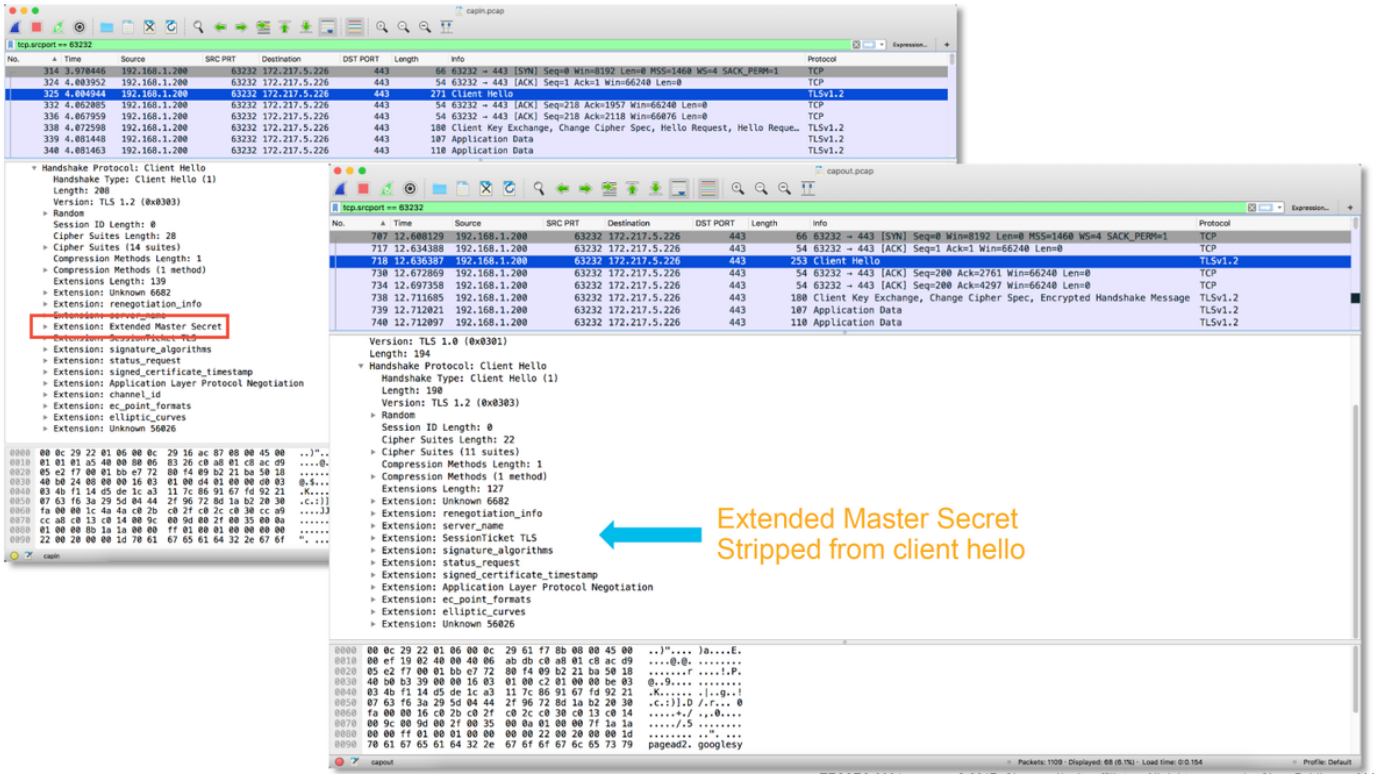


Attention : Avant d'envoyer une capture PCAP déchiffrée au TAC, il est recommandé de filtrer et de limiter le fichier de capture aux flux problématiques, afin d'éviter de révéler inutilement des données sensibles.

Rechercher les modifications Hello du client (CHMod)

La capture de paquets peut également être évaluée pour voir si une modification Hello du client est en cours.

La capture de paquets à gauche représente le Hello du client d'origine. Celui de droite montre les paquets côté serveur. Notez que le secret principal étendu a été supprimé via la fonction CHMod dans Firepower.



Assurez-vous que le client a confiance pour déconnecter l'autorité de certification pour déchiffrer/déconnecter

Pour les règles de stratégie SSL avec l'action « Décrypter - Désigner », assurez-vous que les hôtes clients font confiance à l'autorité de certification (AC) utilisée comme autorité de certification démissionnaire. Les utilisateurs finaux ne doivent pas avoir d'indication qu'ils sont pris en charge par le pare-feu. Ils devraient faire confiance à l'AC signataire. Ceci est le plus souvent appliqué via la stratégie de groupe Active Directory (AD), mais dépend de la stratégie de l'entreprise et de l'infrastructure AD.

Pour plus d'informations, vous pouvez consulter l'article suivant, qui décrit comment créer une stratégie SSL.

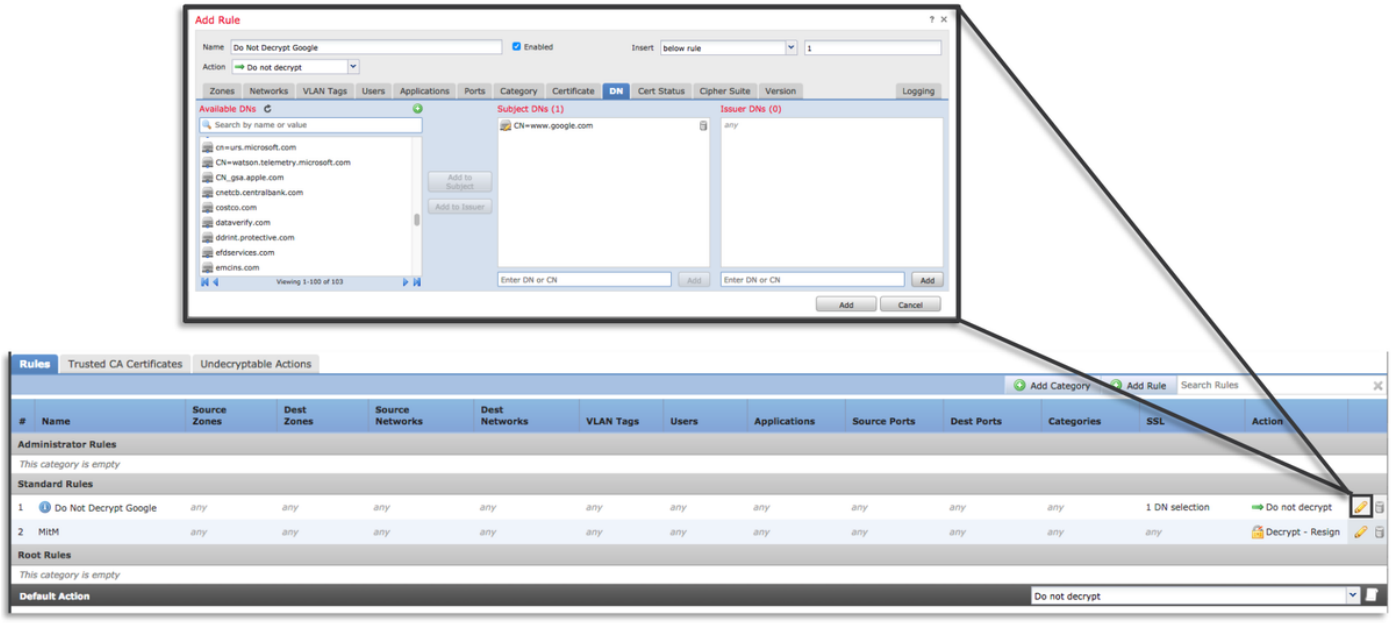
Étapes d'atténuation

Certaines mesures d'atténuation de base peuvent être suivies pour :

- Reconfigurer la stratégie SSL pour ne pas déchiffrer certains trafics
- Éliminer certaines données d’un paquet Hello client pour que le déchiffrement réussisse

Ajouter des règles de déchiffrement (DnD)

Dans l'exemple suivant, il a été déterminé que le trafic vers google.com est interrompu lors de l'inspection de la stratégie SSL. Une règle est ajoutée, basée sur le nom commun (CN) dans le certificat du serveur afin que le trafic vers google.com ne soit pas déchiffré.



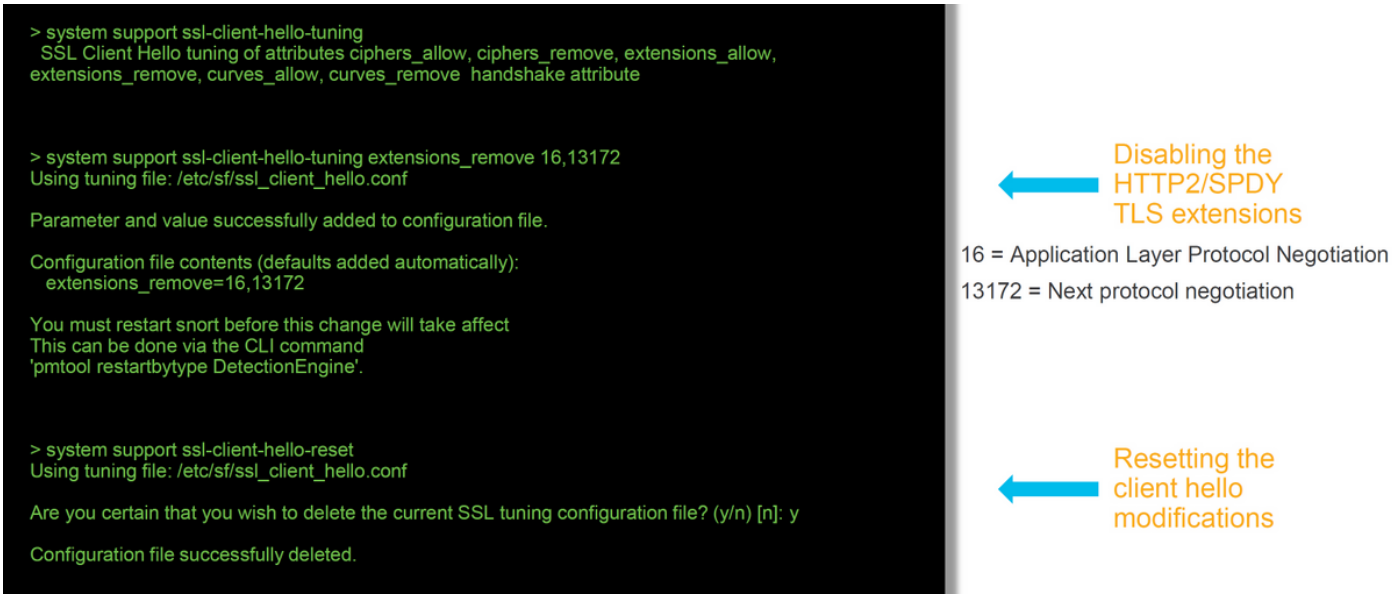
Après avoir enregistré et déployé la stratégie, les étapes de dépannage décrites ci-dessus peuvent être suivies à nouveau pour voir ce que Firepower fait avec le trafic.

Réglage de la modification Hello du client

Dans certains cas, le dépannage peut révéler que Firepower rencontre un problème de déchiffrement de certains trafics. L'utilitaire **de prise en charge du système ssl-client-hello-tuning** peut être exécuté sur l'interface de ligne de commande pour que Firepower supprime certaines données d'un paquet Hello client.

Dans l'exemple ci-dessous, une configuration est ajoutée afin que certaines extensions TLS soient supprimées. Les ID numériques sont trouvés en recherchant des informations sur les extensions TLS et les normes.

> **Attention** : Le processus Snort doit être redémarré avant que les modifications Hello du client ne prennent effet, ce qui peut entraîner l'abandon de quelques paquets. Les protocoles avec état tels que le trafic TCP sont retransmis, mais d'autres trafics, tels que le protocole UDP, peuvent être affectés de manière négative.



Afin de rétablir les modifications apportées aux paramètres de modification Hello du client, la commande **system support ssl-client-hello-reset** peut être implémentée.

Données à fournir au TAC

Données	Instructions
Dépannage des fichiers à partir de Firepower Management Center (FMC) et des périphériques Firepower	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-tech
Débogues SSL	Reportez-vous à cet article pour obtenir des instructions.
Captures de paquets de session complète (côté client, périphérique Firepower lui-même et côté serveur lorsque cela est possible)	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-8000-series-applia
Captures d'écran ou rapports d'événements de connexion	Reportez-vous à cet article pour obtenir des instructions.

Étape suivante

S'il a été déterminé que le composant Stratégie SSL n'est pas la cause du problème, l'étape suivante consiste à dépanner la fonctionnalité Authentification active.

Cliquez ici pour passer à l'article suivant.