Aktivieren des Inline-Normalisierungspräprozessors und Verstehen der Pre-ACK- und Post-ACK-Inspektion

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie der Inline-Normalisierungspräprozessor aktiviert wird. Außerdem werden die Unterschiede und Auswirkungen zweier erweiterter Optionen für die Inline-Normalisierung erläutert.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse des Cisco FirePOWER-Systems und von Snort verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco FireSIGHT Management Center und den FirePOWER-Appliances.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

Ein Inline-Normalisierungspräprozessor normalisiert den Datenverkehr, um die Wahrscheinlichkeit zu minimieren, dass ein Angreifer die Erkennung durch Inline-Bereitstellungen umgehen kann. Die Normalisierung erfolgt unmittelbar nach der Paketdekodierung und vor allen anderen Präprozessoren und verläuft von den inneren Schichten des Pakets nach außen. Bei der Inline-Normalisierung werden keine Ereignisse generiert, aber Pakete werden für die Verwendung durch andere Präprozessoren vorbereitet.

Wenn Sie eine Angriffsrichtlinie mit aktiviertem Inline-Normalisierungspräprozessor anwenden, testet das FirePOWER-Gerät diese beiden Bedingungen, um sicherzustellen, dass Sie eine Inline-Bereitstellung verwenden:

- Bei den Versionen 5.4 und höher ist der *Inline-Modus* in der Network Analysis Policy (NAP) aktiviert, und *Drop when Inline* ist ebenfalls in der Intrusion Policy konfiguriert, wenn die Intrusion Policy so eingestellt ist, dass Datenverkehr verworfen wird. Bei Version 5.3 und früheren Versionen ist die Option *Bei Inline*-Zugriff *löschen* in der Richtlinie für Sicherheitsrisiken aktiviert.

- Die Richtlinie wird auf eine Inline-Schnittstellengruppe (oder eine Inline-Schnittstellengruppe mit Failopen) angewendet.

Daher müssen Sie zusätzlich zur Aktivierung und Konfiguration des Inline-Normalisierungspräprozessors sicherstellen, dass diese Anforderungen erfüllt werden, da der Präprozessor den Datenverkehr nicht normalisiert:

- Ihre Richtlinie muss so festgelegt sein, dass Datenverkehr in Inline-Bereitstellungen verworfen wird.

- Sie müssen Ihre Richtlinie auf einen Inline-Satz anwenden.

Inline-Normalisierung aktivieren

In diesem Abschnitt wird beschrieben, wie Sie die Inline-Normalisierung für Version 5.4 und höher sowie für Version 5.3 und höher aktivieren.

Inline-Normalisierung in Version 5.4 und höher aktivieren

Die meisten Präprozessoreinstellungen werden im NAP für Version 5.4 und höher konfiguriert. Führen Sie die folgenden Schritte aus, um die Inline-Normalisierung im NAP zu aktivieren:

1. Melden Sie sich bei der Webbenutzeroberfläche Ihres FireSIGHT Management Center an.

2. Navigieren Sie zu **Richtlinien > Zugriffskontrolle**.

3. Klicken Sie oben rechts auf der Seite auf **Network Analysis Policy** (**Netzwerkanalyserichtlinie**).

4. Wählen Sie eine *Netzwerkanalyserichtlinie aus*, die auf das verwaltete Gerät angewendet werden soll.

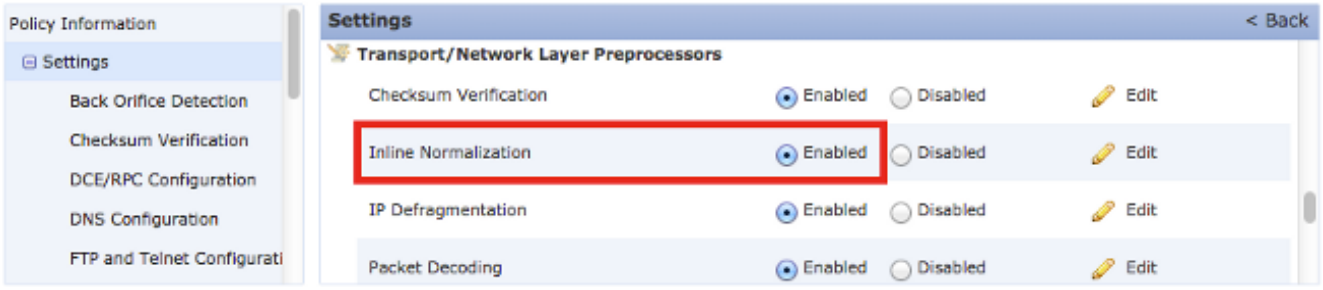
5. Klicken Sie auf das *Bleistiftsymbol*, um mit der Bearbeitung zu beginnen, und die Seite

Richtlinie bearbeiten wird angezeigt.

6. Klicken Sie links im Bildschirm auf **Einstellungen**, und die Seite *Einstellungen* wird angezeigt.

7. Suchen Sie die Option **Inline Normalization** (**Inline-Normalisierung**) im Bereich *Transport/Netzwerkschicht-Präprozessor*.

8. Wählen Sie das Optionsfeld **Aktiviert**, um diese Funktion zu aktivieren:



Der NAP mit der Inline-Normalisierung muss der Zugriffskontrollrichtlinie hinzugefügt werden, damit eine Inline-Normalisierung erfolgen kann. Der NAP kann über die Registerkarte "*Advanced*" (*Erweiterte* Zugriffskontrollrichtlinie) hinzugefügt werden:

Die Zugriffskontrollrichtlinie muss dann auf das inspizierende Gerät angewendet werden.

> **Hinweis**: Bei Version 5.4 oder höher können Sie die Inline-Normalisierung für bestimmten Datenverkehr aktivieren und für anderen Datenverkehr deaktivieren. Wenn Sie die Inline-Normalisierung für bestimmten Datenverkehr aktivieren möchten, fügen Sie eine *Netzwerkanalyseregel* hinzu, und legen Sie die Kriterien und die Richtlinie für den Datenverkehr auf die entsprechende Regel fest. Wenn Sie sie global aktivieren möchten, legen Sie die *Standardrichtlinie für die Netzwerkanalyse* auf die Richtlinie fest, für die die Inline-Normalisierung aktiviert ist.

Inline-Normalisierung in Version 5.3 und früheren Versionen aktivieren

Führen Sie die folgenden Schritte aus, um die Inline-Normalisierung in einer Richtlinie für Sicherheitsrisiken zu aktivieren:

1. Melden Sie sich bei der Webbenutzeroberfläche Ihres FireSIGHT Management Center an.

2. Navigieren Sie zu **Policies > Intrusion > Intrusion Policies**.

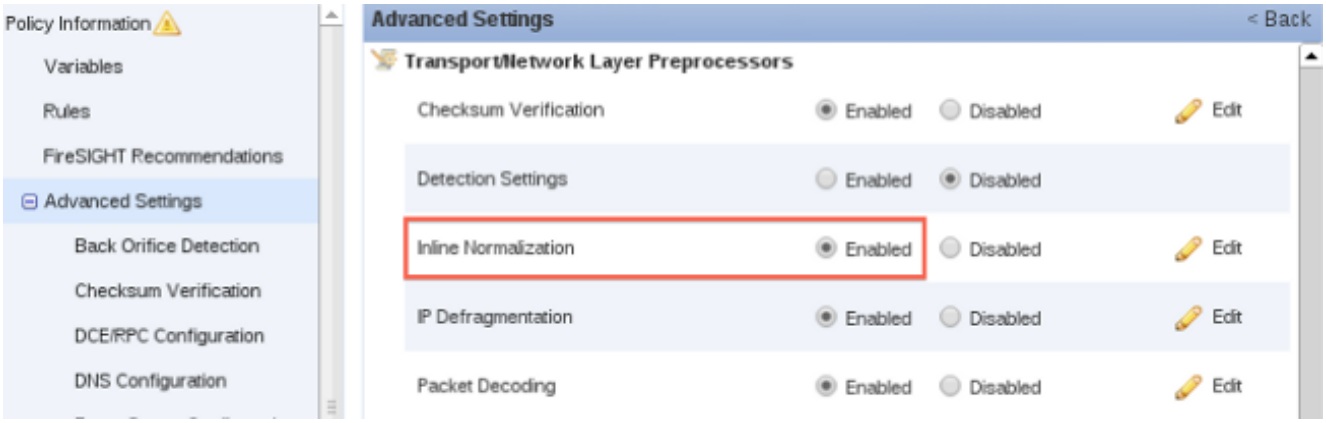
3. Wählen Sie eine *Richtlinie für Sicherheitsrisiken aus*, die auf das verwaltete Gerät angewendet werden soll.

4. Klicken Sie auf das *Bleistiftsymbol*, um mit der Bearbeitung zu beginnen, und die Seite *Richtlinie bearbeiten* wird angezeigt.

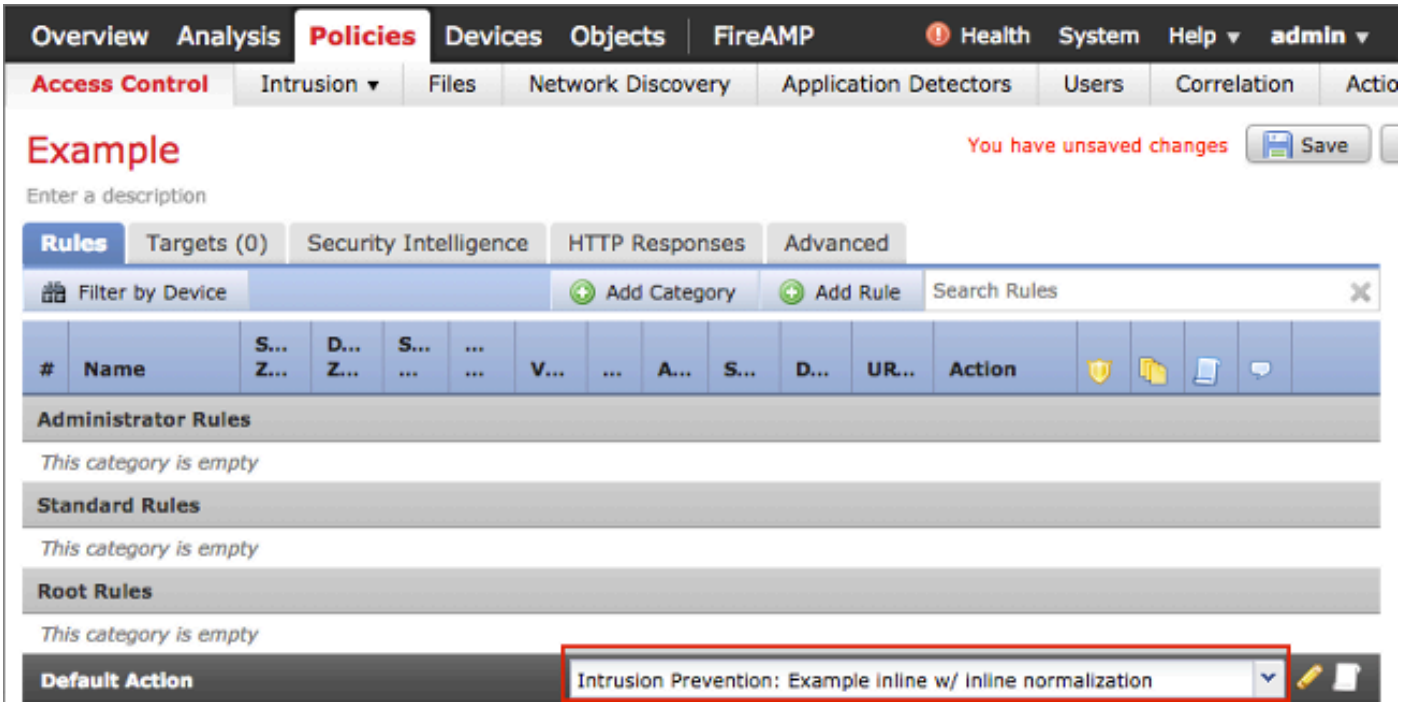
5. Klicken Sie auf **Erweiterte Einstellungen**, und die Seite ***Erweiterte Einstellungen*** wird angezeigt.

6. Suchen Sie die Option **Inline Normalization** (**Inline-Normalisierung**) im Bereich *Transport/Netzwerkschicht-Präprozessor*.

7. Wählen Sie das Optionsfeld **Aktiviert**, um diese Funktion zu aktivieren:



Sobald die Richtlinie für Sicherheitsrisiken für die Inline-Normalisierung konfiguriert wurde, muss sie der Zugriffskontrollrichtlinie als Standardaktion hinzugefügt werden:



Die Zugriffskontrollrichtlinie muss dann auf das inspizierende Gerät angewendet werden.

Sie können den Inline-Normalisierungspräprozessor so konfigurieren, dass IPv4-, IPv6-, Internet Control Message Protocol Version 4 (ICMPv4)-, ICMPv6- und TCP-Datenverkehr in beliebiger Kombination normalisiert wird. Die Normalisierung der einzelnen Protokolle erfolgt automatisch, wenn die Protokollnormalisierung aktiviert ist.

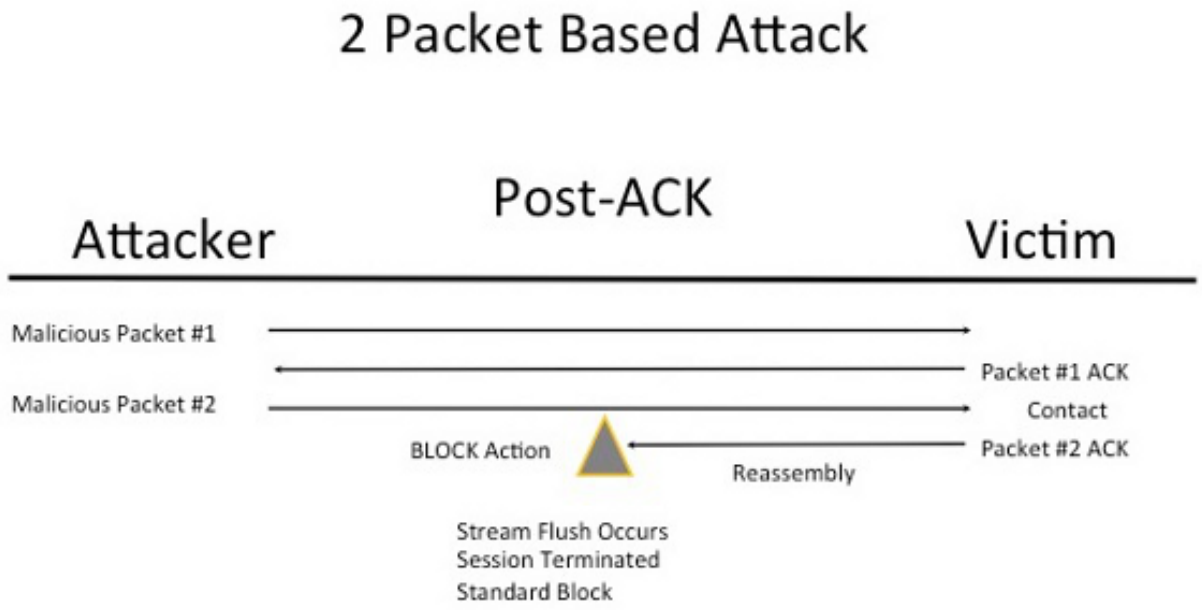
Aktivieren von Prüfungen nach der Aktivierung und vor der Aktivierung

Nachdem Sie den Inline-Normalisierungspräprozessor aktiviert haben, können Sie die Einstellungen bearbeiten, um die Option *TCP-Payload normalisieren* zu aktivieren. Diese Option im Inline-Normalisierungspräprozessor wechselt zwischen zwei verschiedenen Prüfmodi:

- Nach der Bestätigung (Nach der Bestätigung)
- Vor der Bestätigung (Pre-ACK)

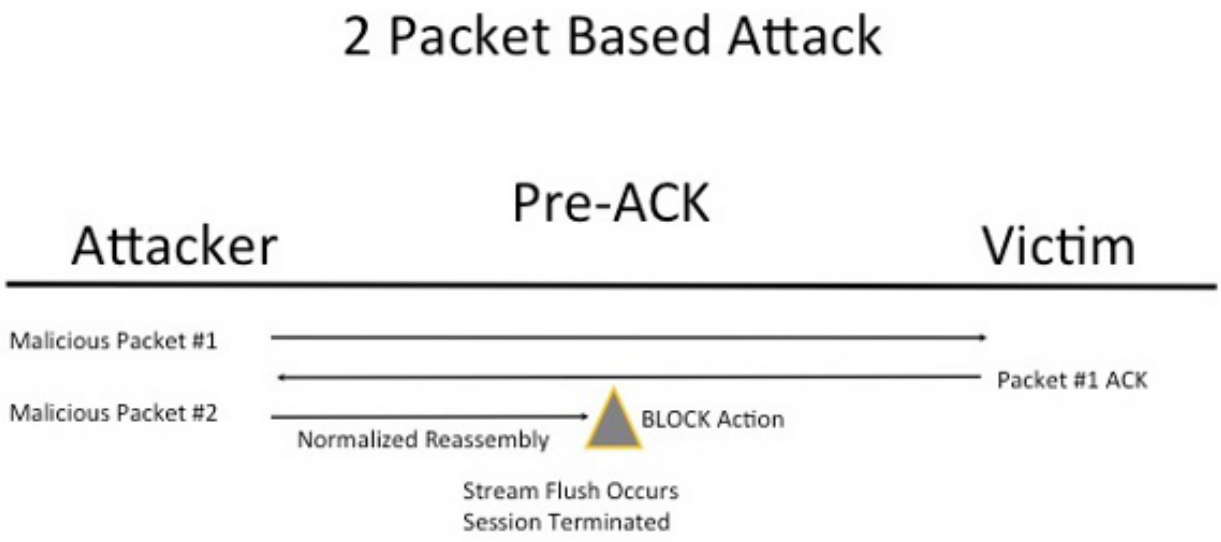
Analyse nach dem ACK verstehen (TCP normalisieren/TCP-Payload normalisieren deaktiviert)

Nach der ACK-Überprüfung erfolgt die Reassemblierung, Leerung (Weiterleitung an den Rest des Überprüfungsprozesses) und Erkennung in Snort nach der Bestätigung (ACK) des Opfers für das Paket, das den Angriff abschließt, durch das Intrusion Prevention System (IPS). Bevor die Flushübertragung stattfindet, hat das betroffene Paket bereits das Opfer erreicht. Daher erfolgt die Warnung/Löschung, nachdem das betroffene Paket das Opfer erreicht hat. Diese Aktion tritt auf, wenn die ACK des Opfers für das verletzende Paket das IPS erreicht.



Analyse vor dem Aktivieren des ACK (TCP normalisieren/TCP-Payload normalisieren aktiviert)

Diese Funktion normalisiert den Datenverkehr unmittelbar nach der Paketdekodierung und vor der Verarbeitung anderer Snort-Funktionen, um TCP-Umgehungsaktionen zu minimieren. Dadurch wird sichergestellt, dass die Pakete, die das IPS erreichen, dieselben sind wie die, die an das Opfer weitergeleitet werden. Snort verwirft den Datenverkehr auf dem Paket, das den Angriff abschließt, bevor der Angriff sein Opfer erreicht.



Wenn Sie *TCP normalisieren* aktivieren, wird der Datenverkehr, der diese Bedingungen erfüllt, ebenfalls verworfen:

- Kopien zuvor verworfener Pakete erneut übertragen
- Datenverkehr, der versucht, eine zuvor unterbrochene Sitzung fortzusetzen
- Datenverkehr, der mit einer der folgenden Präprozessorregeln des TCP-Streams übereinstimmt:

  129:1129:3129:4129:6129:8129:11129:14 bis 129:19

  Hinweis: Um die Warnungen für die Regeln des TCP-Streams zu aktivieren, die vom Normalisierungspräprozessor verworfen werden, müssen Sie die Funktion *Stateful Inspection Anomalies (Stateful Inspection Anomalien)* in der Konfiguration des TCP-Streams aktivieren.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.