

Настройте IPS для предотвращения ошибочного допуска Использование фильтра действия события

Содержание

[Введение](#)

[Перед началом работы](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Понимание EAFs](#)

[!--- конфигурацию](#)

[Дополнительные сведения](#)

[Введение](#)

Этот документ предоставляет шаги, требуемые для настройки Системы предотвращения вторжений (IPS) для Предотвращения Ошибочного допуска с помощью диспетчера устройств IPS (IDM) или IPS Manager Express (IME). Ошибочный допуск, настраиваемый на IPS, достигнут функцией, названной Фильтром действия события (EAF).

[Перед началом работы](#)

[Требования](#)

Читатели данной документации должны ознакомиться с Cisco IPS.

[Используемые компоненты](#)

Сведения в этом документе не на основе определенных версий программного и аппаратного обеспечения.

[Условные обозначения](#)

[Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.](#)

[Понимание EAFs](#)

EAFs настроены прежде всего для настройки ошибочного допуска. EAF предоставляет способность иметь особую подпись **не**, берут необходимые действия для подмножества трафика.

EAFs полезны в ситуациях, где это требуется, чтобы удовлетворять множественные условия, такие как:

- Подпись **х не** принимает меры у для желаемой подсети трафика.
- Подпись **х** принимает меры у для всего другого трафика.

EAFs полезны имея дело с мягким иницированием подписи.

!--- конфигурацию

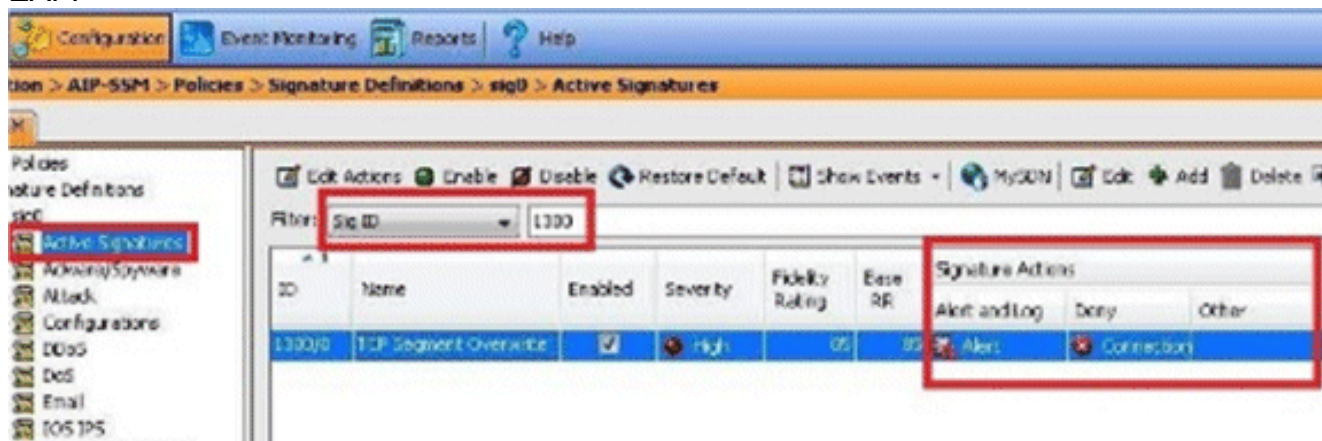
Пример: Событие Ошибочного допуска: Подпись 1300 иницирует для трафика, прибывающего от и до известных надежных хостов.

Примечание: Это - просто демонстрационный пример цели только. Если вы не уверены, мягко ли определенное событие из-за триггера подписи или нет, обратитесь в техническую поддержку Cisco для дальнейшего анализа.

Примечание: См. [Подписи системы предотвращения вторжений Cisco \(IPS\)](#) для дополнительных сведений относительно подписей IPS.

Выполните следующие действия:

1. Проверьте действия по умолчанию для подписи (1300, в данном примере), для которого должен быть настроен EAF.



Действия по умолчанию подписи 1300 включают, **Производят Предупреждение и Запрещают Встроенное Соединение.**

2. Определите хосты, для которых не должна срабатывать эта подпись. Например, вы **не** хотите, чтобы подпись сработала для трафика, прибывающего из доверяемой подсети, такой как 10.1.1.1-10.1.1.254.
3. Создайте EAF для критериев, описанных в Шаг 2: От IDM/IME перейдите к **Конфигурации> Политика> Политика IPS**. Нажмите вкладку **Event Action Filters**. Под этой вкладкой **нажмите Add**.

Home Configuration Event Monitoring Reports Help

Configuration > AIP-SSM > Policies > IPS Policies

AIP-SSM

IPS Policies

Signature Definitions

- sig0
 - Active Signatures
 - Aware/Spyware
 - Attack
 - Configurations
 - DDoS
 - DoS
 - Email
 - IGMP IPS
 - Instant Messaging
 - L2/L3/L4 Protocol
 - Network Services
 - OS
 - Other Services
 - PGP
 - Reconnaissance
 - Releases
 - Specialty Licensed Signat...
 - TelePresence
 - UC Protection
 - Viruses/Worms/Trojans
 - Web Server
 - All Signatures
- Event Action Rules
- rules0
- Anomaly Detections
- ad0
- Global Correlation
- Inspection/Reputation
- Network Participation

Sensor Setup

Interfaces

Policies

Add Virtual Sensor Edit Delete

Name	Assigned Interfaces (or Pairs)	Signature Definition Policy	Event Action Override Policy			Anomaly Det Policy	
			Risk Rating	Actions to Add	Enabled		
vs0	GigabitEthernet0/1.0 (Backplane Interface)	sig0	rules0 (1 action overrides)	HIGH-RISK	Deny Packet Tr...	Yes	ad0

Event Action Rules "rules0" for virtual sensor "vs0"

Event Action Filters IPv4 Target Value Rating IPv6 Target Value Rating OS Identifications Event Variables Risk Category

Event Action Filters lets you **subtract** the actions associate with an event if the conditions for that event meet the criteria of the filter.

Add Edit Delete

Name	Enabled	Sig ID	SubSig ID	Attacker (IPv4 / IPv6) port
------	---------	--------	-----------	-----------------------------

Это окно
отображено:

Add Event Action Filter

Name:

Enabled: Yes No

Signature ID:

Subsignature ID:

Attacker IPv4 Address:

Attacker IPv6 Address:


Attacker Port:


Victim IPv4 Address:

Victim IPv6 Address:

Victim Port:

Risk Rating: to

Actions to Subtract: 

More Options 

OK Cancel Help

Настройте различные поля, такие как **Название**, **Идентификатор подписи**, **IP Атакующего**, и

Add Event Action Filter

Name:

Enabled: Yes No

Signature ID:

Subsignature ID:

Attacker IPv4 Address:

Attacker IPv6 Address:


Attacker Port:


Victim IPv4 Address:

Victim IPv6 Address:

Victim Port:

Risk Rating: to

Actions to Subtract: 

More Options 

OK Cancel Help

т.д.

Нажми

те значок направо от поля **Actions to Subtract** для открытия диалогового окна Edit

Add Event Action Filter

Name:

Enabled: Yes No

Signature ID:

Subsignature ID:

Attacker IPv4 Address:

Attacker IPv6 Address:


Attacker Port:


Victim IPv4 Address:

Victim IPv6 Address:

Victim Port:

Risk Rating: to

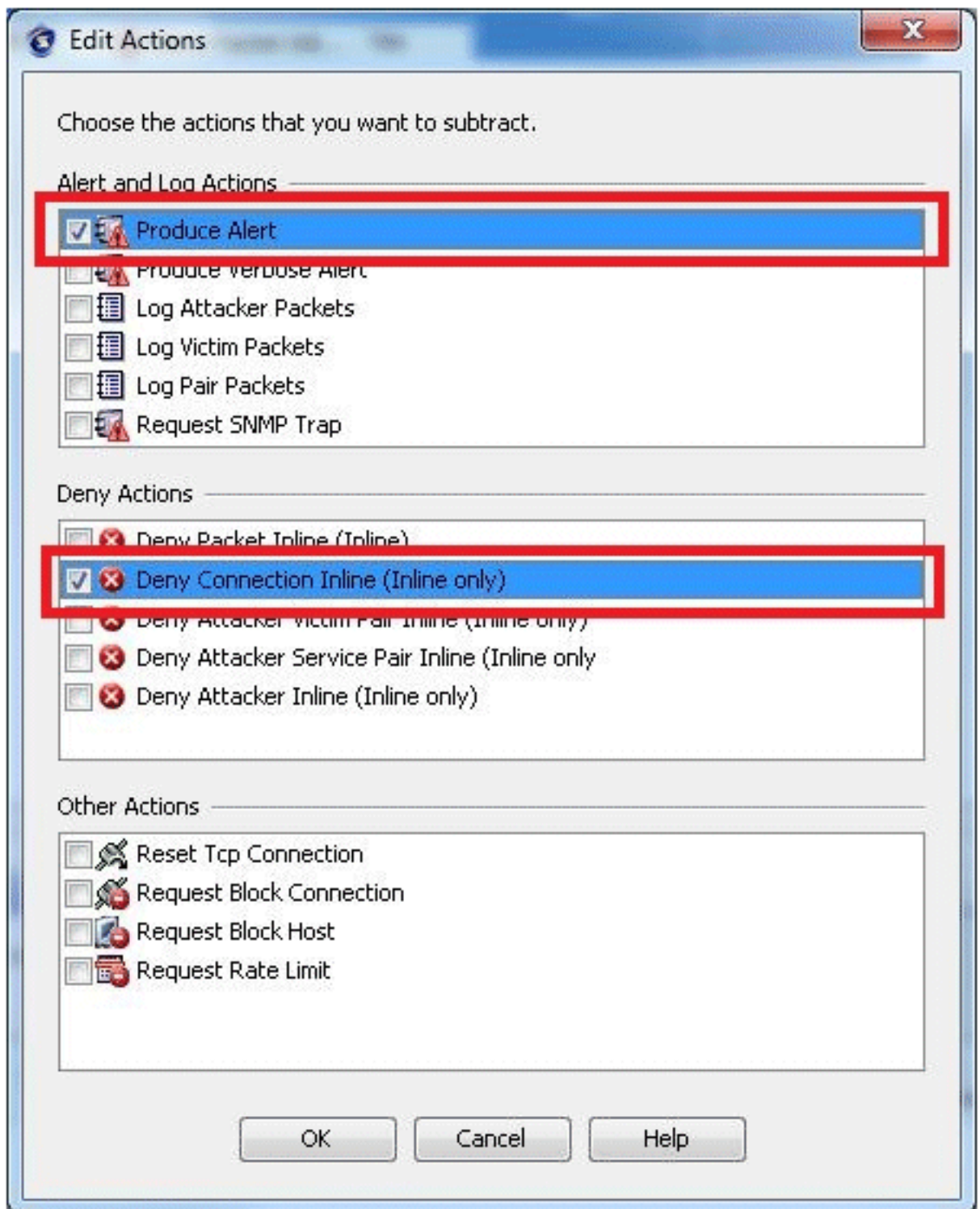
Actions to Subtract: 

More Options 

OK Cancel Help

Actions.

В этом окне можно задать Действия подписи, которые вы **не** хотите, чтобы IPS выполнил. **Примечание:** Для корректного выбора действий подписи, которые вы хотите вычесть, необходимо понять действия подписей по умолчанию, как описано в Шаге 1. В данном примере мы выбрали **Produce Alert** и **Deny Connection**



Inline.

Если подпись 1300 года инициирует для трафика, прибывающего от 10.1.1.1-10.1.1.254, IPS не примет эти меры. Для всего другого трафика, действия подписи по умолчанию **Предупреждения Продукта** и **Запрещают Встроенное Соединение**, все еще применятся. После выбора Produce Alert и Deny Packet Inline вы будете видеть, что эти действия заполняют у основания экрана

Add Event Action Filter

Name:

Enabled: Yes No

Signature ID:

Subsignature ID:

Attacker IPv4 Address:

Attacker IPv6 Address:


Attacker Port:


Victim IPv4 Address:

Victim IPv6 Address:

Victim Port:

Risk Rating: to

Actions to Subtract: 

More Options 

EAF: **Нажмите** **OK**, и затем **Применить** для сохранения изменений.

Нажм

The screenshot displays the configuration interface for a virtual sensor named "vs0". At the top, there are buttons for "Add Virtual Sensor", "Edit", and "Delete". Below this is a table with the following data:

Name	Assigned Interfaces (or Pairs)	Signature Definition Policy	Event Action Override Policy			Anomaly Detection Policy	Description	
			Risk Rating	Actions to Add	Enabled			
vs0		sig0	rules0 (1 action override)	HIGH-RISK	Deny Packet 38...	Yes	add	default virtual se...

Below the table is a section titled "Event Action Rules 'rules0' for virtual sensor 'vs0'". It contains several tabs: "Event Action Filters", "IPv4 Target Value Rating", "IPv6 Target Value Rating", "OS Identifications", "Event Variables", "Risk Category", "Threat Category", and "General". The "Event Action Filters" tab is active, showing a description: "Event Action Filters lets you subtract the actions associate with an event if the conditions for that event meet the criteria of the filter." Below this are buttons for "Add", "Edit", and "Delete", along with up and down arrows. A table lists the filters:

Name	Enabled	Sig ID	SubSig ID	Attacker (IPv4 / IPv6 / port)
EAF_1000	Yes	1000	0	10.1.1.1-10.1.1.254 ip-only (attacker) (attacker ip only) (attacker ip-only)

At the bottom right, there are "Apply" and "Reset" buttons, with the "Apply" button highlighted by a red box.

Для конфигурации Фильтра Действия События с помощью CLI обратитесь к разделу Интерфейса командной строки IPS на [странице Configuration Guides](#). От соответствующего Руководства по конфигурации нажмите **Configuring Event Action Rules** и поиск "Фильтров Действия События Настройки".

[Дополнительные сведения](#)

- [Cisco Systems – техническая поддержка и документация](#)