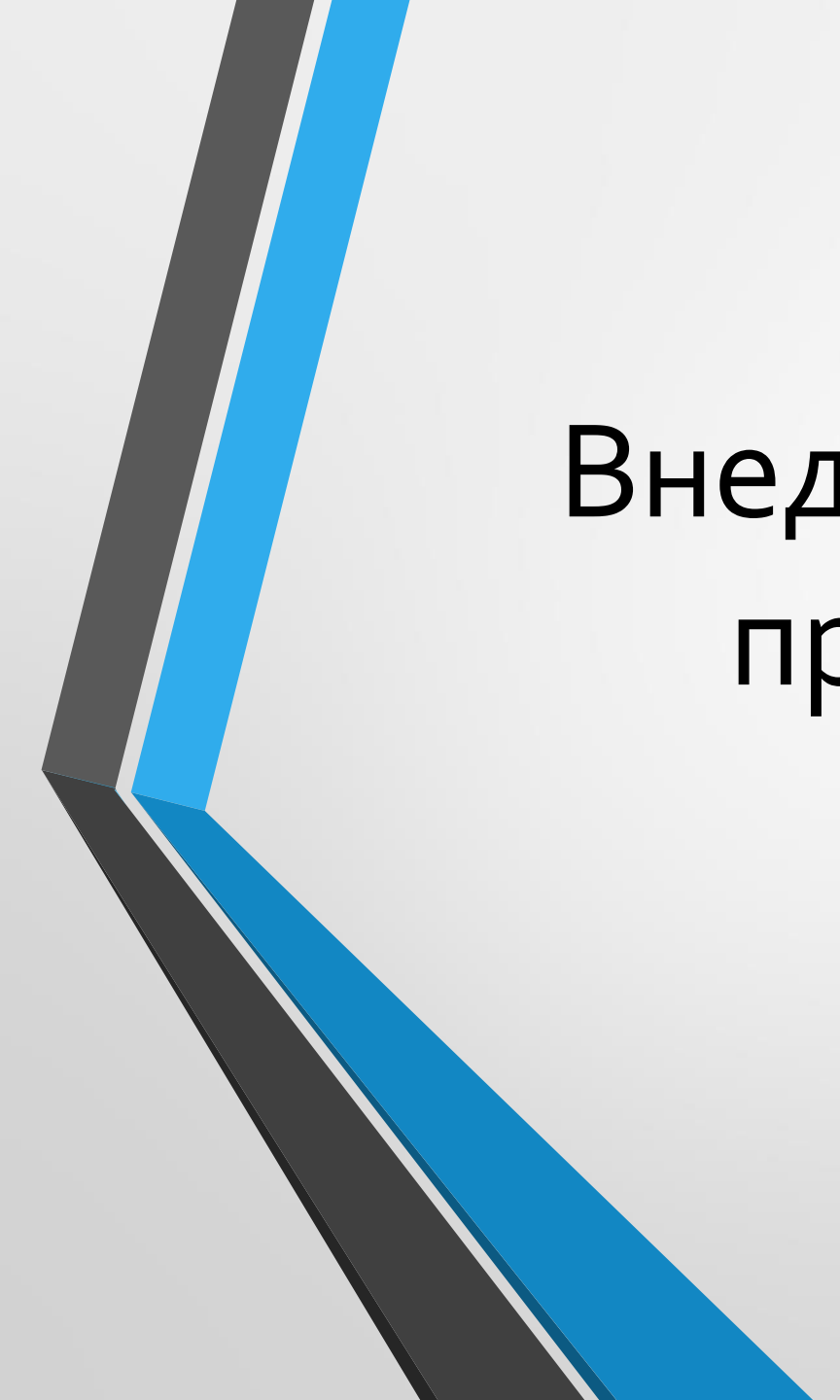




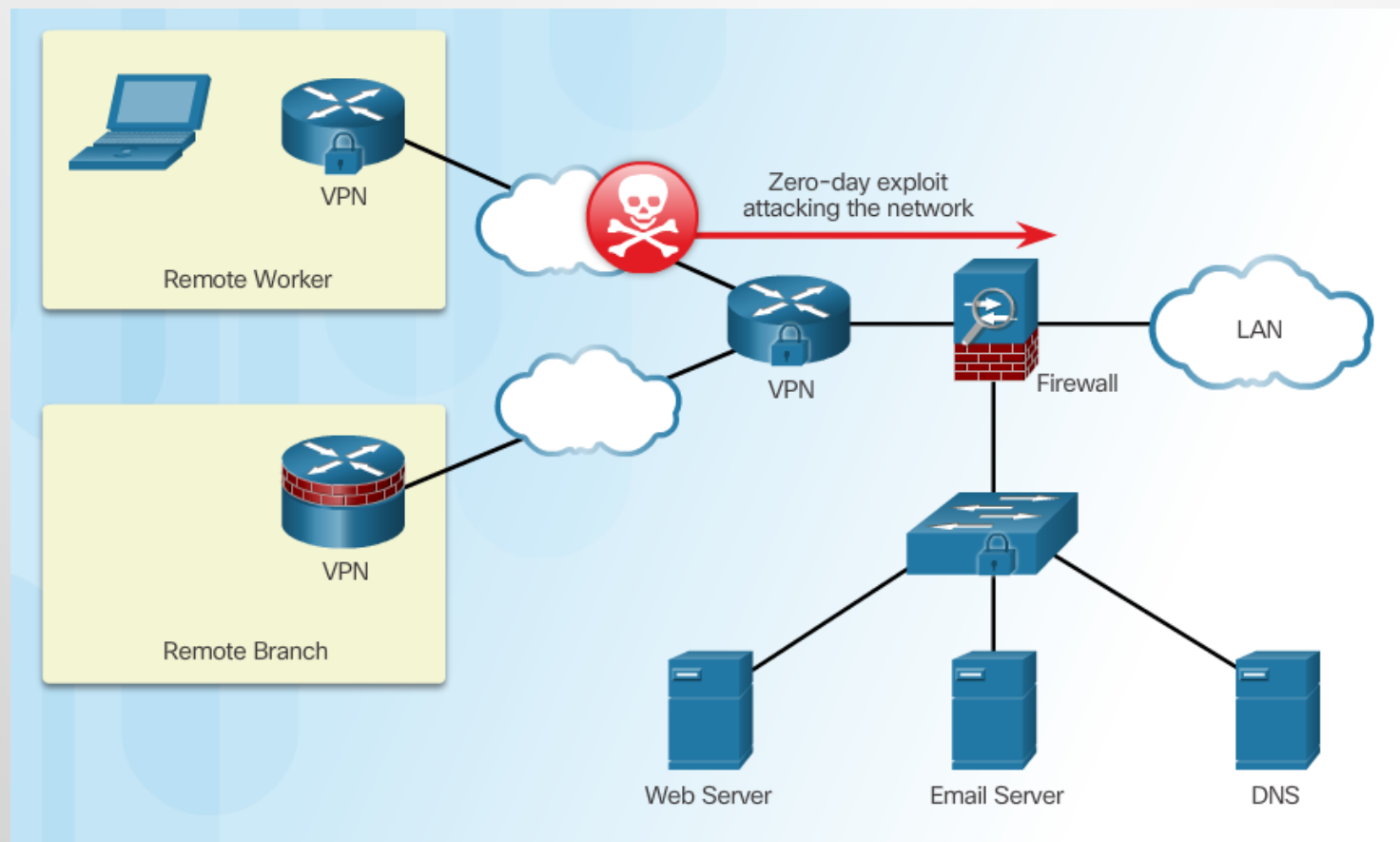
# Лекция 7

## Внедрение системы предотвращения вторжений



# Тема Характеристики систем IDS и IPS

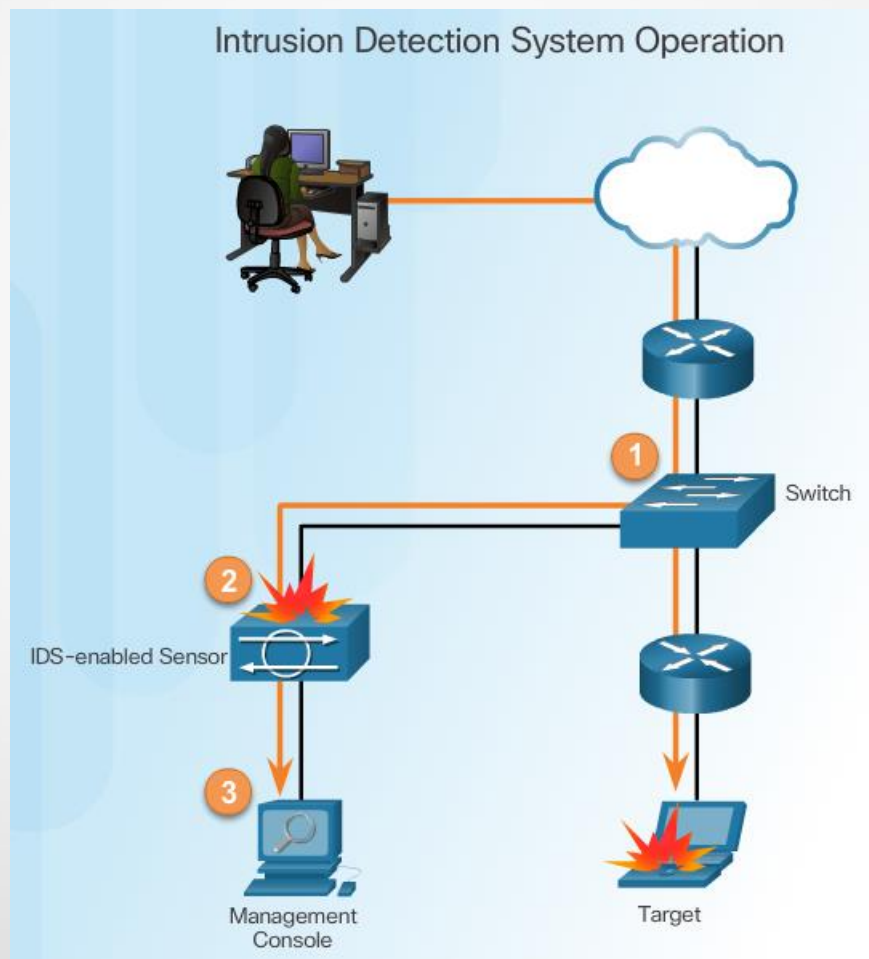
# Атаки нулевого дня



# Мониторинг атак

## Преимущества системы IDS:

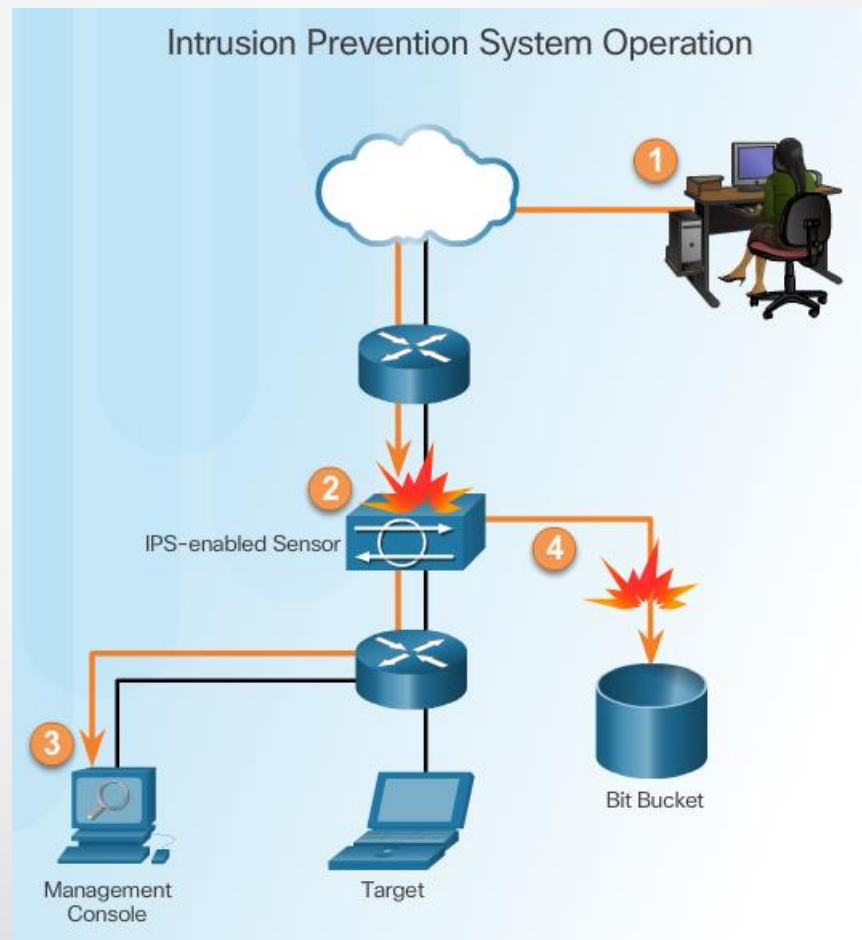
- Пассивная работа
- Необходимо зеркалирование трафика, чтобы его достичь
- Сетевой трафик не проходит через IDS, если он не зеркалируется



# Обнаружение и остановка атак

## IPS:

- Внедрение в inline-режиме
- Контроль трафика на уровне 3 и 4
- Может останавливать однопакетные атаки на пути к цели
- Реагирует немедленно, не пропуская никакого вредоносного трафика

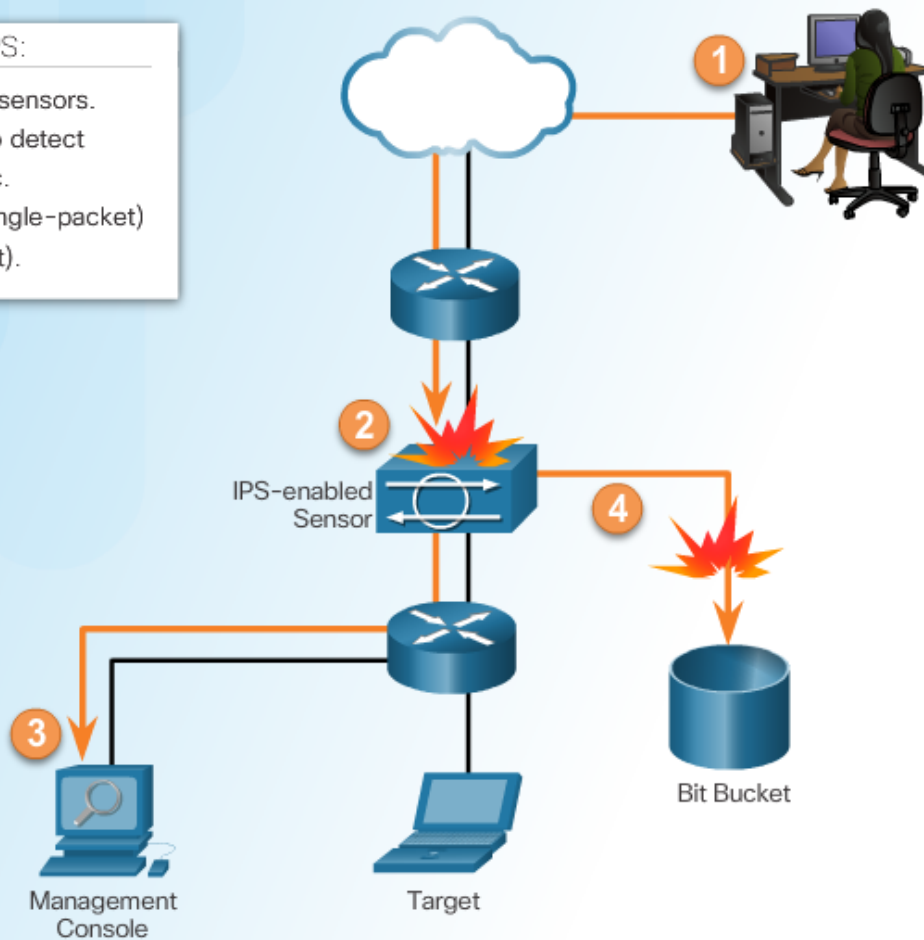


# Сходство IDS и IPS

## IDS and IPS Characteristics

Common characteristics of IDS and IPS:

- Both technologies are deployed as sensors.
- Both technologies use signatures to detect patterns of misuse in network traffic.
- Both can detect atomic patterns (single-packet) or composite patterns (multi-packet).



# Преимущества и недостатки систем IDS и IPS

## Преимущества IDS:

- Не влияет на сеть.
- Нет влияния на сеть в случае выхода сенсора из строя.
- Нет влияния на сеть в случае перегрузки сенсора.

## Недостатки IDS:

- Ответные действия не могут остановить вредоносный пакет.
- Для ответных действий нужна корректная настройка.
- Более уязвима перед техниками нарушения безопасности сети.

## Преимущества IPS:

- Останавливает вредоносные пакеты.
- Может использовать техники потоковой нормализации.

## Недостатки IPS:

- Проблемы с сенсором могут сказываться на сетевом трафике.
- Перегрузка сенсора влияет на сеть.
- Небольшое негативное влияние на производительность сети.

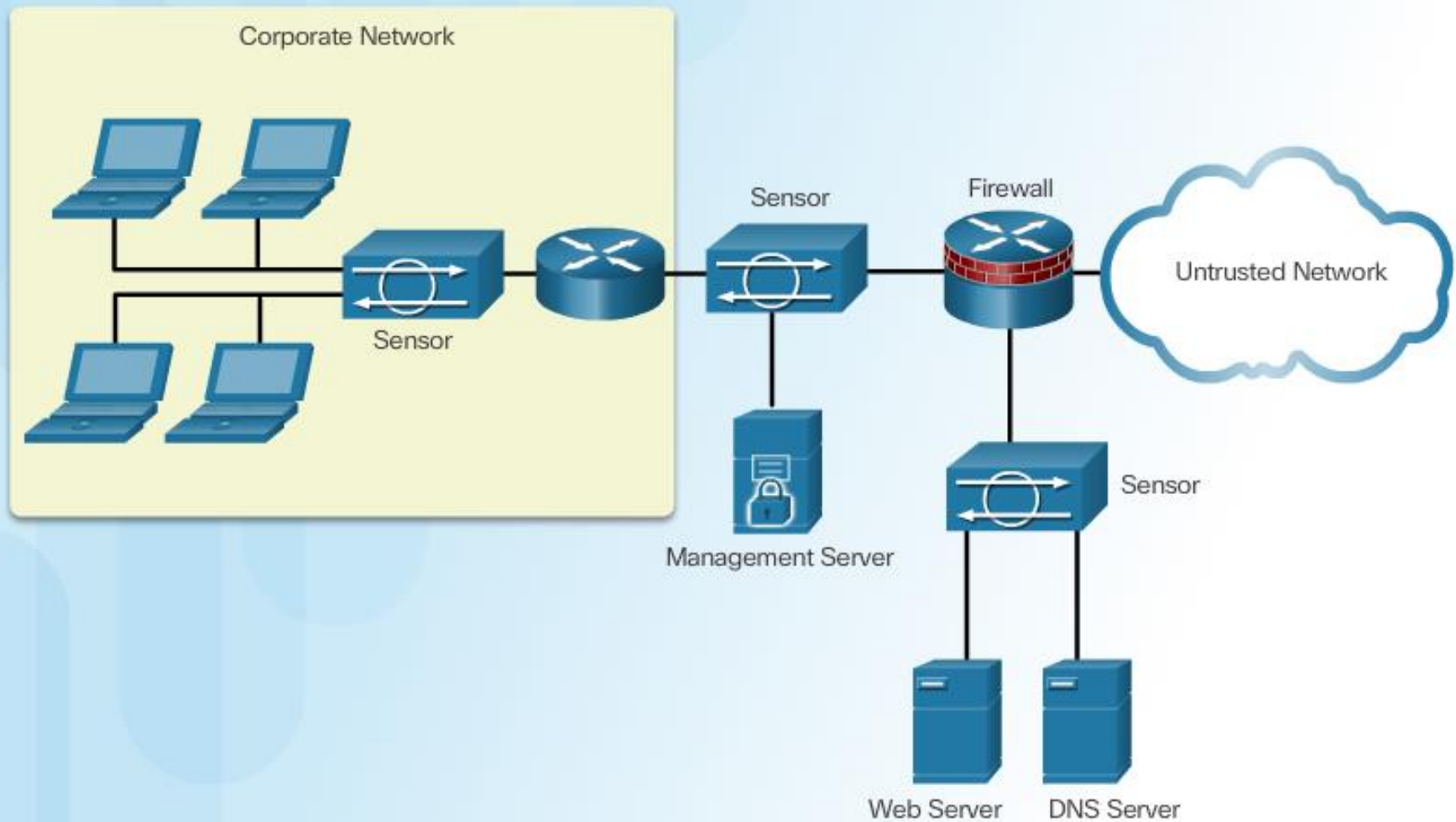


# Тема Сетевые реализации IPS

# Хостовые и сетевые реализации IPS

| Advantages        |                                                                                                                                                                                                                                           | Disadvantages                                                                                                                                      |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Host-Based IPS    | <ul style="list-style-type: none"><li>• Provides protection specific to a host operating system</li><li>• Provides operating system and application level protection</li><li>• Protects the host after the message is decrypted</li></ul> | <ul style="list-style-type: none"><li>• Operating system dependent</li><li>• Must be installed on all hosts</li></ul>                              |
| Network-Based IPS | <ul style="list-style-type: none"><li>• Cost effective</li><li>• Operating system independent</li></ul>                                                                                                                                   | <ul style="list-style-type: none"><li>• Cannot examine encrypted traffic</li><li>• Must stop malicious traffic prior to arriving at host</li></ul> |

# Сетевые IPS-сенсоры



# Модульные и аппаратные решения Cisco IPS



Cisco IPS AIM и Network Module Enhanced (IPS NME)



Cisco ASA AIP-SSM



Сенсоры Cisco IPS серии 4300



Cisco Catalyst серии 6500 IDS-M-2

# Выбор решения IPS

Факторы, влияющие на выбор и развертывание IPS-сенсора:

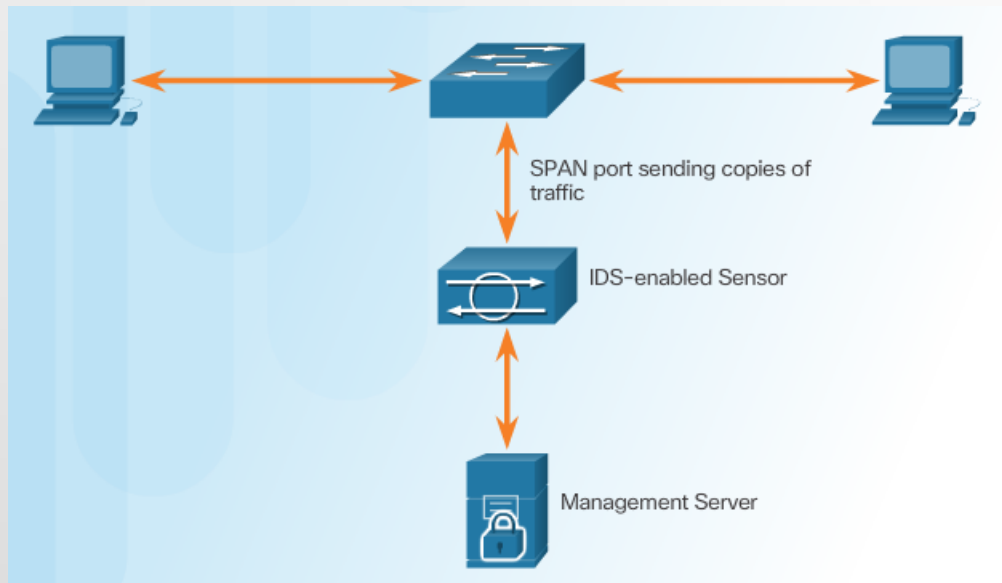
- Объем сетевого трафика
- Топология сетей
- Бюджет на ИБ
- Наличие специалистов по безопасности, способных работать с IPS

# Преимущества и недостатки IPS

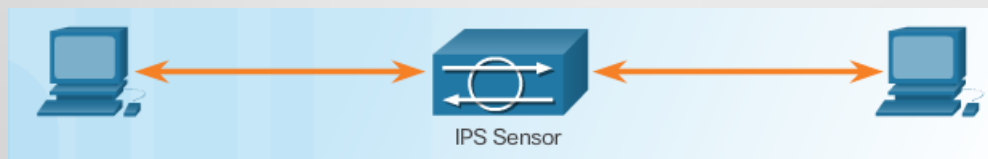
| Advantages  |                                                                                                                                                                                           | Disadvantages                                                                                                                                  |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Network IPS | <ul style="list-style-type: none"><li>• Is cost-effective</li><li>• Not visible on the network</li><li>• Operating system independent</li><li>• Lower level network events seen</li></ul> | <ul style="list-style-type: none"><li>• Cannot examine encrypted traffic</li><li>• Cannot determine whether an attack was successful</li></ul> |

# Режимы развертывания

## Promiscuous-режим



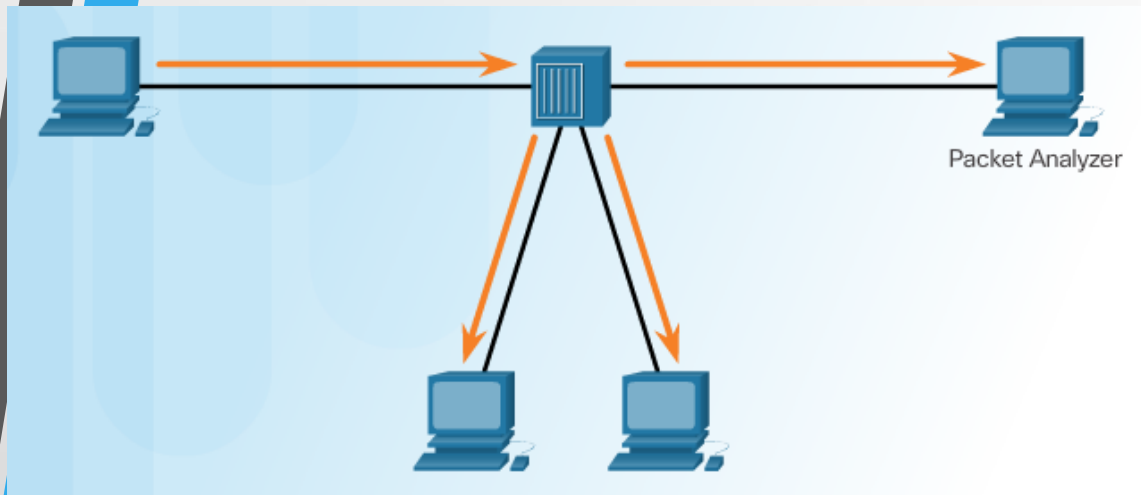
## Inline-режим





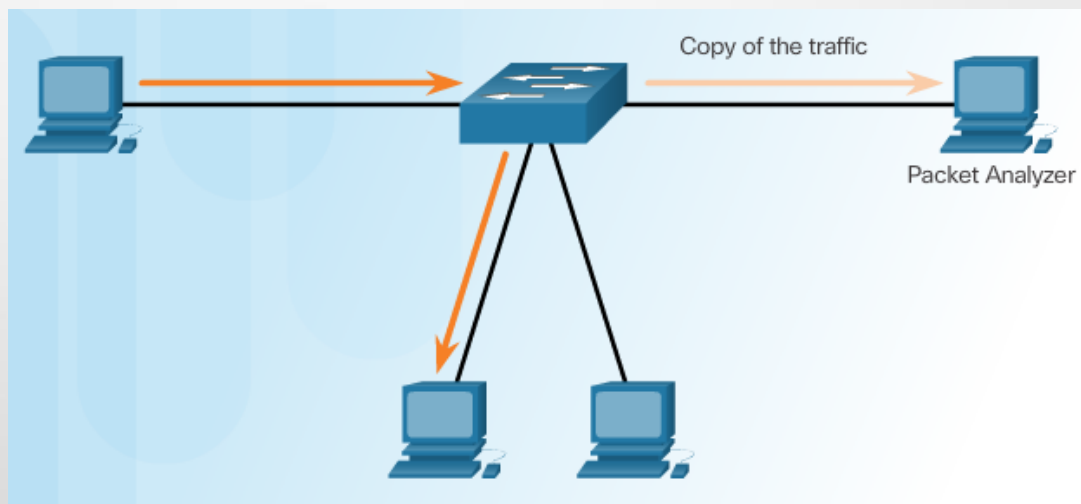
# Tema Cisco Switched Port Analyzer

# Зеркалирование портов

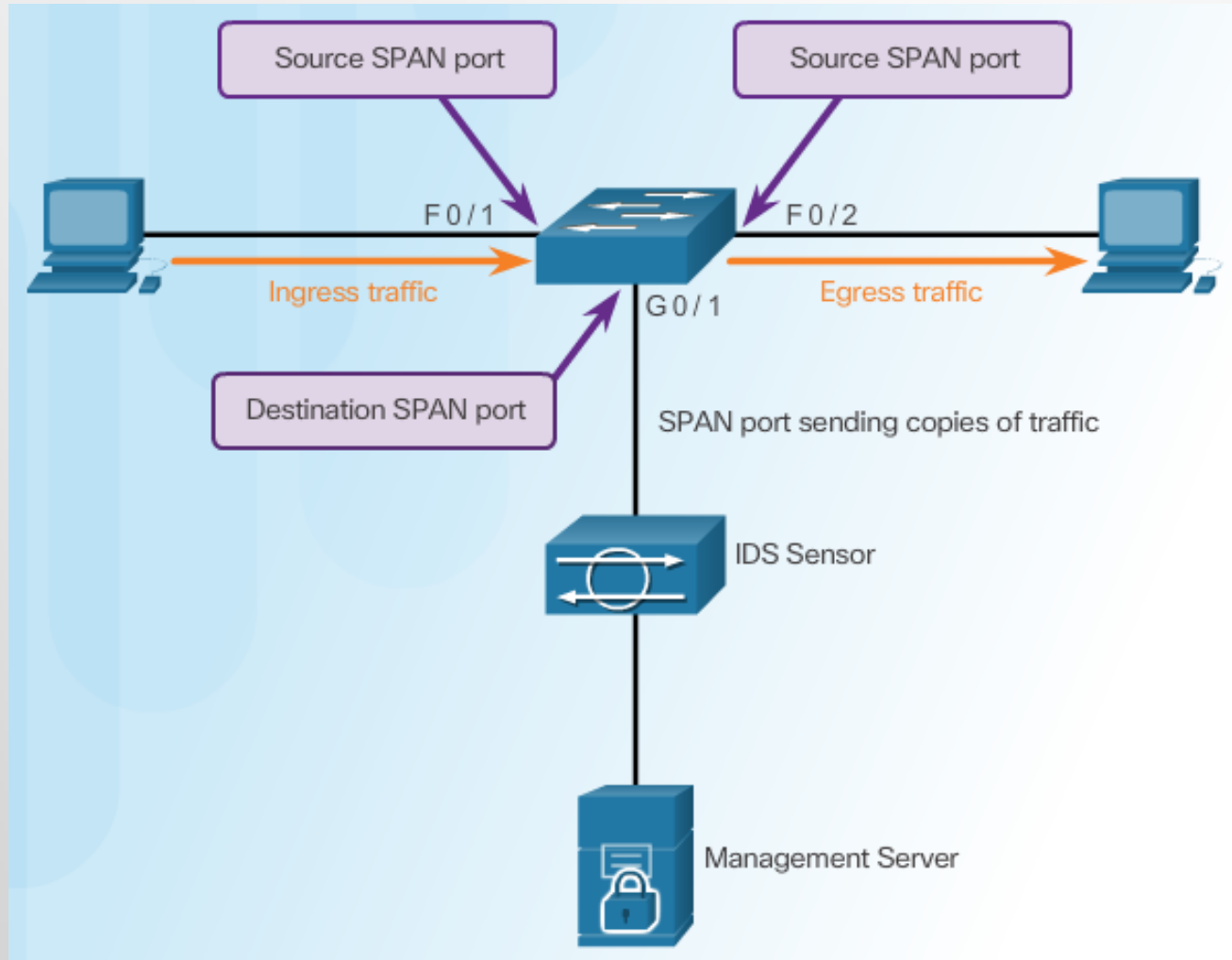


Прослушивание  
трафика с помощью  
концентратора

Прослушивание  
трафика с помощью  
коммутатора



# Cisco SPAN



# Конфигурирование Cisco SPAN с использованием системы обнаружения вторжений

## Команды Cisco SPAN:

- Команда `monitor session` используется для ассоциации порта источника и порта назначения с сеансом SPAN.

### Associate a SPAN session with a source port

```
Switch(config)# monitor session number source [ interface interface | vlan vlan ]
```

### Associate a SPAN session with a destination port

```
Switch(config)# monitor session number destination [ interface interface | vlan vlan ]
```

- Команда `show monitor` используется для проверки работы сеанса SPAN.



# Тема Характеристики сигнатур IPS

# Атрибуты сигнатур

Сигнатура – это набор правил, которые используют системы IDS и IPS для обнаружения типичной вредоносной активности.

У сигнатур есть три четких атрибута:

- Тип
- Триггер (сигнал тревоги)
- Действие

# Типы сигнатур

Сигнатуры категоризируются следующим образом:

- Атомарная – простейший тип сигнатуры, заключающейся в проверке одиночного пакета, действия или события на предмет его соответствия сконфигурированной сигнатуре. Если соответствие установлено, подается сигнал тревоги и предпринимается определенное сигнатурой действие.
- Составная (композиционная) сигнатура – этот тип сигнатуры обнаруживает последовательность операций, распределенных по разным хостам в течение произвольного периода времени.

# Файл сигнатур

- При обнаружении новых угроз должны создаваться новые сигнатуры, которые должны загружаться в систему IPS.
- Файл сигнатур содержит набор определений сетевых угроз.

The screenshot shows the Cisco Software Download Center interface. The top navigation bar includes the Cisco logo, links for Products & Services, Support, How to Buy, Training & Events, and Partners. A search bar is located on the right. Below the navigation bar, the page title is "Download Software". A breadcrumb trail indicates the path: Downloads Home > Products > Security > Network Security > Integrated Threat Control > IOS Intrusion Prevention System Feature Software > IOS IPS Signature Data File-S855. The main content area is titled "IOS Intrusion Prevention System Feature Software". On the left, there is a sidebar with a search bar and a list of releases, with "S855" selected under the "Latest" section. The main content area displays "Release S855" with a "Signature Update S855 Readme" link. A warning message states: "Attention: Cisco has discovered a defect in some versions of IOS that can unexpectedly halt all processes when signature updates are applied. To avoid further instances of this problem, IOS IPS Signature updates will not be available for automatic downloading from Software Download Center. http://tools.cisco.com/security/center/php/home.x?m=62". Below this, a table lists the file information:

| File Information                                                                 | Release Date | Size     |                                                         |
|----------------------------------------------------------------------------------|--------------|----------|---------------------------------------------------------|
| IOS IPS Signature Update Package in 5.x format for CLI users<br>IOS-S855-CLI.pkg | 03-MAR-2015  | 21.52 MB | <a href="#">Download</a><br><a href="#">Add to cart</a> |

# Микромодули сигнатур

Cisco IOS определяет пять микромодулей:

- Atomic – сигнатуры, проверяющие простые пакеты.
- Service – сигнатуры, проверяющие трафик сервисов, подверженных атакам.
- String – сигнатуры, использующие шаблоны на регулярных выражениях для определения вторжений.
- Multi-string – поддерживают гибкое сопоставление образцов и сигнатур Trend Labs.
- Other – внутренний модуль, работающий с прочими сигнатурами.

# Загрузка файла сигнатур

The screenshot shows the Cisco Software Download Center interface. The top navigation bar includes the Cisco logo, links for Products & Services, Support, How to Buy, Training & Events, and Partners. User account information for Rick Graziani is visible. The main heading is "Download Software". A breadcrumb trail leads to "IOS IPS Signature Data File-S855". The page title is "IOS Intrusion Prevention System Feature Software". A search bar and "Expand All | Collapse All" link are present. The "Release S855" section contains an attention warning about a defect in some IOS versions. Below this is a table with file information, release date, and size, along with download and add-to-cart buttons.

Worldwide [change] | Welcome, Rick Graziani | Account | Log Out | My Cisco

**CISCO** Products & Services Support How to Buy Training & Events Partners

Download Software [Download Cart \(0 items\)](#) [Feedback](#) [Help](#)

[Downloads Home](#) > [Products](#) > [Security](#) > [Network Security](#) > [Integrated Threat Control](#) > [IOS Intrusion Prevention System Feature Software](#) > [IOS IPS Signature Data File-S855](#)

### IOS Intrusion Prevention System Feature Software

Search...

[Expand All](#) | [Collapse All](#)

▼ Latest  
**S855**  
S351

▼ All Releases  
► 5.x  
► 4.x

#### Release S855

[Signature Update S855 Readme](#) [Add Devices](#) [Add Notification](#)

Attention: Cisco has discovered a defect in some versions of IOS that can unexpectedly halt all processes when signature updates are applied. To avoid further instances of this problem, IOS IPS Signature updates will not be available for automatic downloading from Software Download Center.  
<http://tools.cisco.com/security/center/phpframe.x?y=62>

| File Information                                                                 | Release Date ▼ | Size     |                                                         |
|----------------------------------------------------------------------------------|----------------|----------|---------------------------------------------------------|
| IOS IPS Signature Update Package in 5.x format for CLI users<br>IOS-S855-CLI.pkg | 03-MAR-2015    | 21.52 MB | <a href="#">Download</a><br><a href="#">Add to cart</a> |



# Тема Сигналы тревоги сигнатур IPS

# Сигнал тревоги сигнатуры

| Detection Type            | Advantages                                                                                                                                                                                         |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pattern-based Detection   | <ul style="list-style-type: none"><li>• Easy configuration</li><li>• Fewer false positives</li><li>• Good signature design</li></ul>                                                               |
| Anomaly-based Detection   | <ul style="list-style-type: none"><li>• Simple and reliable</li><li>• Customized policies</li></ul>                                                                                                |
| Policy-based Detection    | <ul style="list-style-type: none"><li>• Easy configuration</li><li>• Can detect unknown attacks</li></ul>                                                                                          |
| Honey pot-based Detection | <ul style="list-style-type: none"><li>• Window to view attacks</li><li>• Distract and confuse attackers</li><li>• Slow down and avert attacks</li><li>• Collect information about attack</li></ul> |

| Detection Type            | Disadvantages                                                                                                                                                                              |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pattern-based Detection   | <ul style="list-style-type: none"><li>• No detection of unknown signatures</li><li>• Initially a lot of false positives</li><li>• Signatures must be created, updated, and tuned</li></ul> |
| Anomaly-based Detection   | <ul style="list-style-type: none"><li>• Generic output</li><li>• Policy must be created</li></ul>                                                                                          |
| Policy-based Detection    | <ul style="list-style-type: none"><li>• Difficult to profile typical activity in large networks</li><li>• Traffic profile must be constant</li></ul>                                       |
| Honey pot-based Detection | <ul style="list-style-type: none"><li>• Dedicated honey pot server</li><li>• Hot pot server must not be trusted</li></ul>                                                                  |

# Обнаружение на основе шаблона

|                         | Signature Type                                                                                                  |                                                                                                  |
|-------------------------|-----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
|                         | Atomic Signature                                                                                                | Composite Signature                                                                              |
| Pattern-based Detection | No state required to examine pattern to determine if signature action should be applied.                        | Must contain state or examine multiple items to determine if signature action should be applied. |
| Example                 | Detecting an Address Resolution Protocol (ARP) request that has a source Ethernet address of FF:FF:FF:FF:FF:FF. | Searching for the string "confidential" across multiple packets in a TCP session.                |

# Обнаружение на основе аномалий

|                         | Signature Type                                                                           |                                                                        |
|-------------------------|------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
|                         | Atomic Signature                                                                         | Composite Signature                                                    |
| Anomaly-based Detection | No state required to identify activity that deviates from normal profile.                | State required to identify activity that deviates from normal profile. |
| Example                 | Detecting traffic that is going to a destination port that is not in the normal profile. | Verifying protocol compliance for HTTP traffic.                        |

# Обнаружение на основе политик и обнаружение с помощью Honey Pot

|                        | Signature Type                                                                     |                                                                                                               |
|------------------------|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
|                        | Atomic Signature                                                                   | Composite Signature                                                                                           |
| Policy-based Detection | No state required to identify undesirable behavior.                                | Previous activity (state) required to identify undesirable behavior.                                          |
| Example                | Detecting abnormally large fragmented packets by examining only the last fragment. | A Sun Unix host sending RPC requests to remote hosts without initially consulting the Sun PortMapper program. |

# Преимущества решения Cisco IOS IPS

## Преимущества:

- Использует базовую инфраструктуру маршрутизации для обеспечения дополнительного уровня безопасности.
- Выполняется в inline-режиме и поддерживается целым рядом платформ маршрутизации.
- Обеспечивает защиту от угроз на всех точках входа в сеть при использовании вместе с решениями Cisco IDS, Cisco IOS Firewall, VPN и NAC.
- Размер базы данных сигнатуры, используемый устройствами, может адаптироваться к объему доступной памяти на маршрутизаторе.



# Механизмы инициирования сигналов тревоги

Типы сигналов тревоги:

| Alarm Type     | Network Activity    | IPS Activity       | Outcome       |
|----------------|---------------------|--------------------|---------------|
| False positive | Normal user traffic | Alarm generated    | Tune alarm    |
| False negative | Attack traffic      | No alarm generated | Tune alarm    |
| True positive  | Attack traffic      | Alarm generated    | Ideal setting |
| True negative  | Normal user traffic | No alarm generated | Ideal setting |



# Тема Действия сигнатуры IPS

# Действия сигнатуры

Обзор категорий действий:

| Category                            | Specific Alert                                                                                                                                                               |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Generating an alert                 | Produce alert                                                                                                                                                                |
|                                     | Produce verbose alert                                                                                                                                                        |
| Logging the activity                | Log attacker packets                                                                                                                                                         |
|                                     | Log pair packets                                                                                                                                                             |
|                                     | Log victim packets                                                                                                                                                           |
| Dropping or preventing the activity | Deny attacker inline                                                                                                                                                         |
|                                     | Deny connection inline                                                                                                                                                       |
|                                     | Deny packet inline                                                                                                                                                           |
| Resetting a TCP connection          | Reset TCP connection                                                                                                                                                         |
| Blocking future activity            | Request block connection                                                                                                                                                     |
|                                     | Request block host                                                                                                                                                           |
|                                     | Request SNMP trap                                                                                                                                                            |
| Allow the activity                  | <p>This action will permit the traffic to appear as normal based on configured exceptions.</p> <p>An example would be allowing alerts from an approved IT scanning host.</p> |

# Управление сгенерированными сигналами тревоги

## Генерирование сигнала тревоги

| Specific Alert        | Description                                                                                                                                                                 |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Produce alert         | This action writes the event to the Event Store as an alert.                                                                                                                |
| Produce verbose alert | This action includes an encoded dump of the offending packet in the alert. An alert will be written to the Event Store, even if the Produce Alert action is not selected. * |

# Запись действий для последующего анализа

Запись действий в журнал:

| Specific Alert       | Description                                                                                                                                                                                   |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log attacker packets | This action starts IP logging on packets that contain the attacker address and sends an alert. An alert will be written to the Event Store, even if the Produce Alert action is not selected. |
| Log pair packets     | This action starts IP logging on packets that contain the attacker and victim address pair. An alert will be written to the Event Store, even if the Produce Alert action is not selected.    |
| Log victim packets   | This action starts IP logging on packets that contain the victim address and sends an alert. An alert will be written to the Event Store, even if the Produce Alert action is not selected.   |

# Запрещение действия

Сброс или предотвращение действия:

| Specific Alert         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Deny attacker inline   | <ul style="list-style-type: none"><li>• This action terminates the current packet and future packets from this attacker address for a specified period of time.</li><li>• The sensor maintains a list of the attackers currently being denied by the system.</li><li>• Entries may be removed from the list manually or automatically based on a timer.</li><li>• The timer is a sliding timer for each entry. Therefore, if attacker A is currently being denied, but issues another attack, the timer for attacker A is reset and attacker A remains on the denied attacker list until the timer expires.</li><li>• If the denied attacker list is at capacity and cannot add a new entry, the packet is still denied.</li></ul> |
| Deny connection inline | This action terminates the current packet and future packets on this TCP flow.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Deny packet inline     | This action terminates the packet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

# Сброс, блокировка и разрешение трафика

Сброс подключения и блокировка действия:

| Specific Alert           | Description                                                                                                                                                                                                                                           |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reset TCP connection     | This action sends TCP resets to hijack and terminate the TCP flow.                                                                                                                                                                                    |
| Request block connection | This action sends a request to a blocking device to block this connection.                                                                                                                                                                            |
| Request block host       | This action sends a request to a blocking device to block this attacker host.                                                                                                                                                                         |
| Request SNMP trap        | This action sends a request to the notification application component of the sensor to perform Simple Network Management Protocol (SNMP) notification. An alert will be written to the Event Store, even if the Produce Alert action is not selected. |



# Тема Управление и мониторинг IPS

# Мониторинг активности

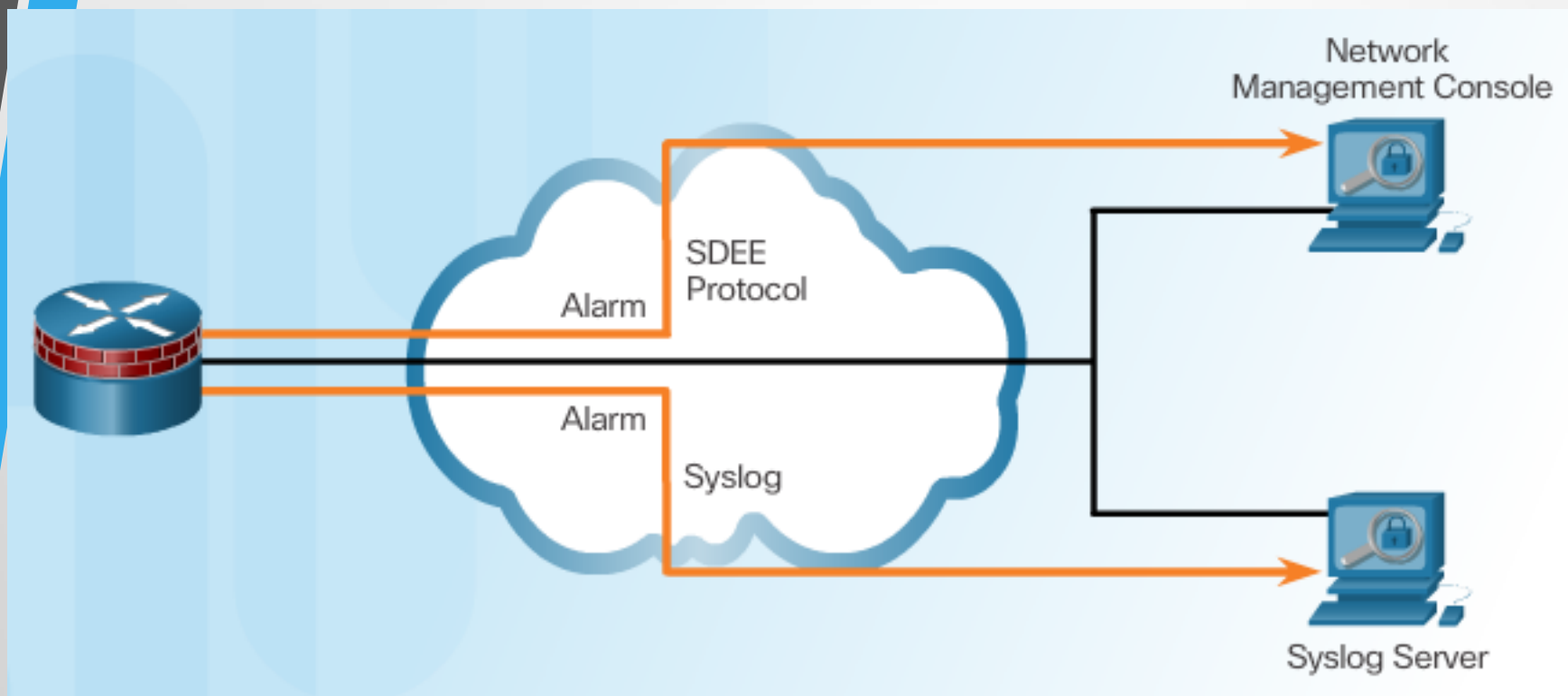
Факторы, которые необходимо учесть при планировании и мониторинге IPS:

- Способ управления
- Корреляция событий
- Специалисты по безопасности
- План реагирования на инциденты

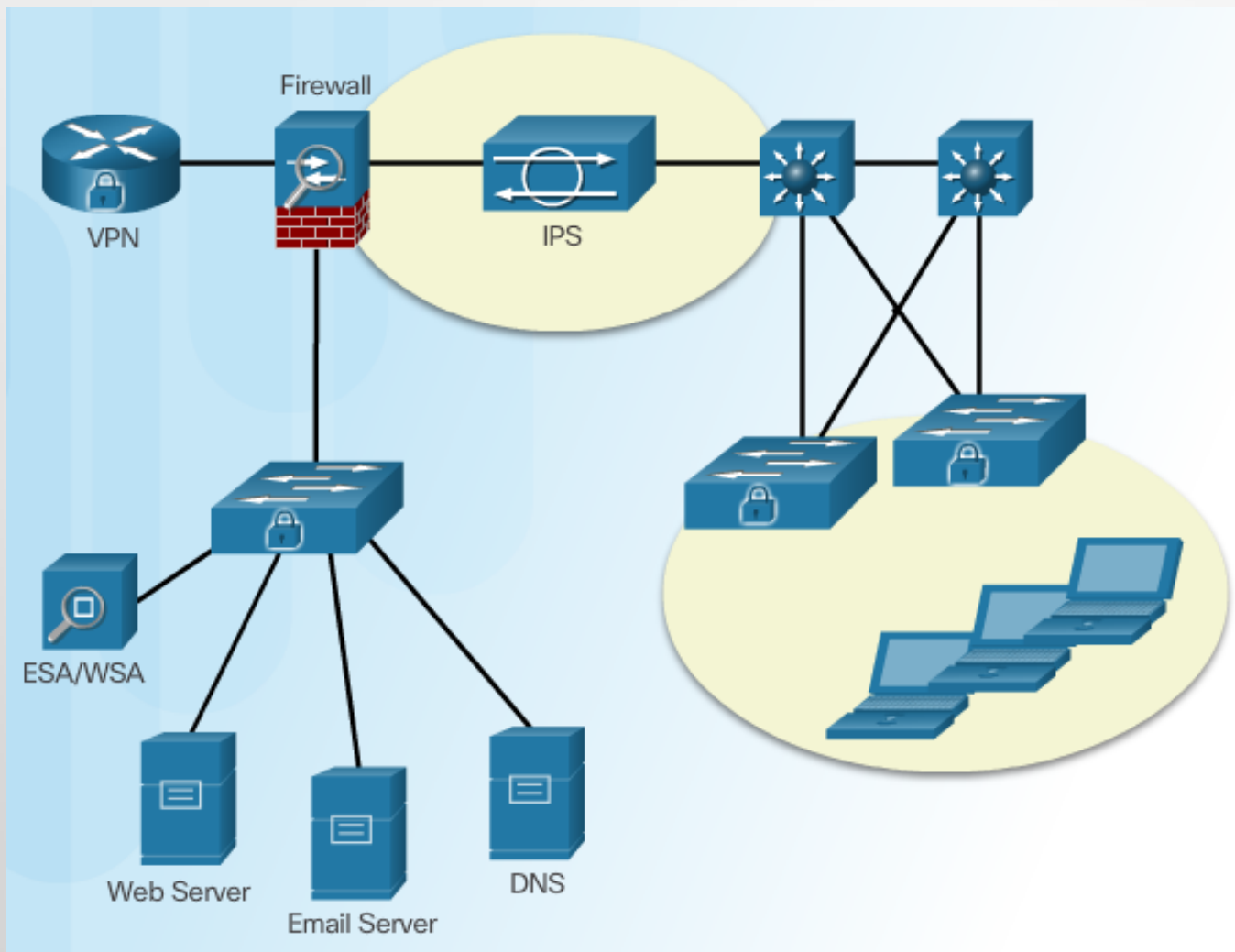
# Факторы, которые необходимо учесть при мониторинге



# Защищенный обмен событиями между устройствами



# Рекомендации по конфигурации IPS





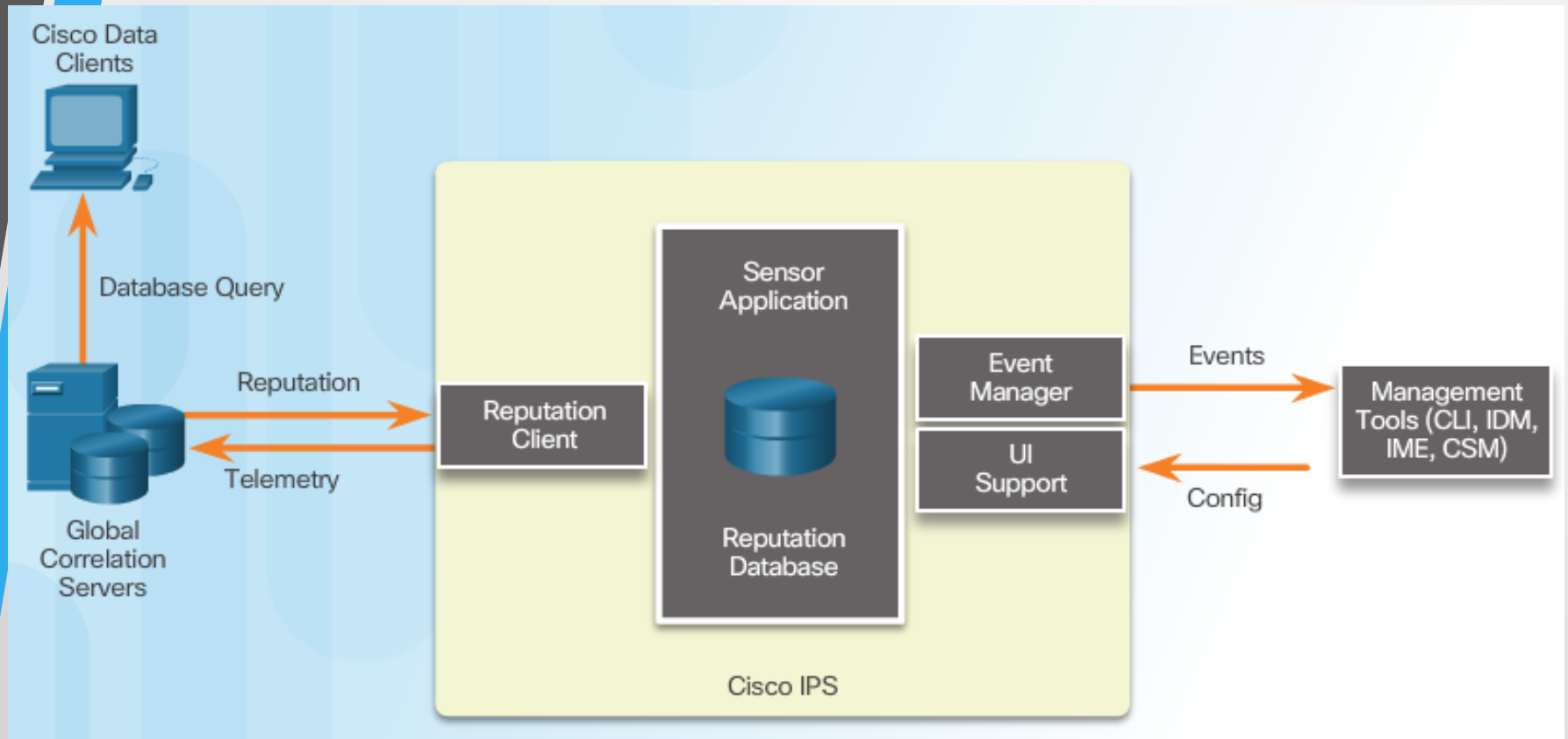
# Тема Глобальная корреляция IPS

# Глобальная корреляция Cisco

## Цели глобальной корреляции

- Интеллектуальная обработка сигналов тревоги с целью повышения эффективности
- Усовершенствованная защита против известных вредоносных сайтов
- Обмен данными телеметрии с сетью SensorBase Network для улучшения мониторинга сигналов тревог и действий сенсоров в глобальном масштабе
- Упрощение настроек конфигурации
- Автоматическое выполнение загрузки и выгрузки информации системы безопасности

# Cisco SensorBase Network



# Cisco Security Intelligence Operation

Сеть позволяет собрать следующие данные:

- ИД сигнатуры
- IP-адрес злоумышленника
- Порт злоумышленника
- Максимальный размер сегмента
- IP-адрес жертвы
- Порт жертвы
- Версия сигнатуры
- Строка опций TCP
- Оценка репутации
- Показатель риска

# Репутационные фильтры, черные списки и фильтры трафика

Home Spam Email Malware Support About

## SenderBase

The world's largest Email and Web traffic monitoring network.

☒ I have read and agree to SenderBase [Terms of Service](#)

### Email Overview



Map Satellite

Legitimate Spam Malware

Click on markers on the map to see details.

### Latest Security Report



[Read More](#)

### Email Types



| Email Type | Percentage |
|------------|------------|
| Legitimate | 14.14%     |
| Spam       | 85.86%     |
| Malware    | 0.0081%    |

[Read More](#)

### Cisco Security Blog

[What I Mean to be a Woman of Influence](#)  
4/16/2015

[Secure Access Control in the Internet of Everything](#)  
4/15/2015

[Three Key Considerations When Evaluating Threat Intelligence Solutions](#)  
4/15/2015

More about Cisco Security also on

 [Facebook](#) [Join Us >](#)

 [YouTube](#) [Watch More >](#)

### Tweets

 [Cisco Security](#) [@CiscoSecurity](#) [Follow](#)

Heading to #BSAC next week? Don't miss "Making Threat Intelligence Actionable: Recommending Responses with STIX" [pic.twitter.com/2BvX35e0SR](#)



# Репутационные фильтры, черные списки и фильтры трафика

