Практические аспекты создания центра мониторинга безопасности

Михаил Кадер

Инженер

Содержание

1. Краткий обзор **MARS** и **Cisco Security Manager**
2. Настройка интеграции
3. Расследование инцидентов ИБ и корректировка политик ИБ
4. Что нового
5. Сценарии совместного использования CSM & MARS

Проблематика управления безопасностью

Управление
Как быстро внедрять новые политики

Мониторинг
Как наблюдать много-вендорные сети

Центры обработки данных

Надомные работники

Контроль доступа
Как контролировать доступ к ресурсам

Аналитика
Слишком много избы-точных данных

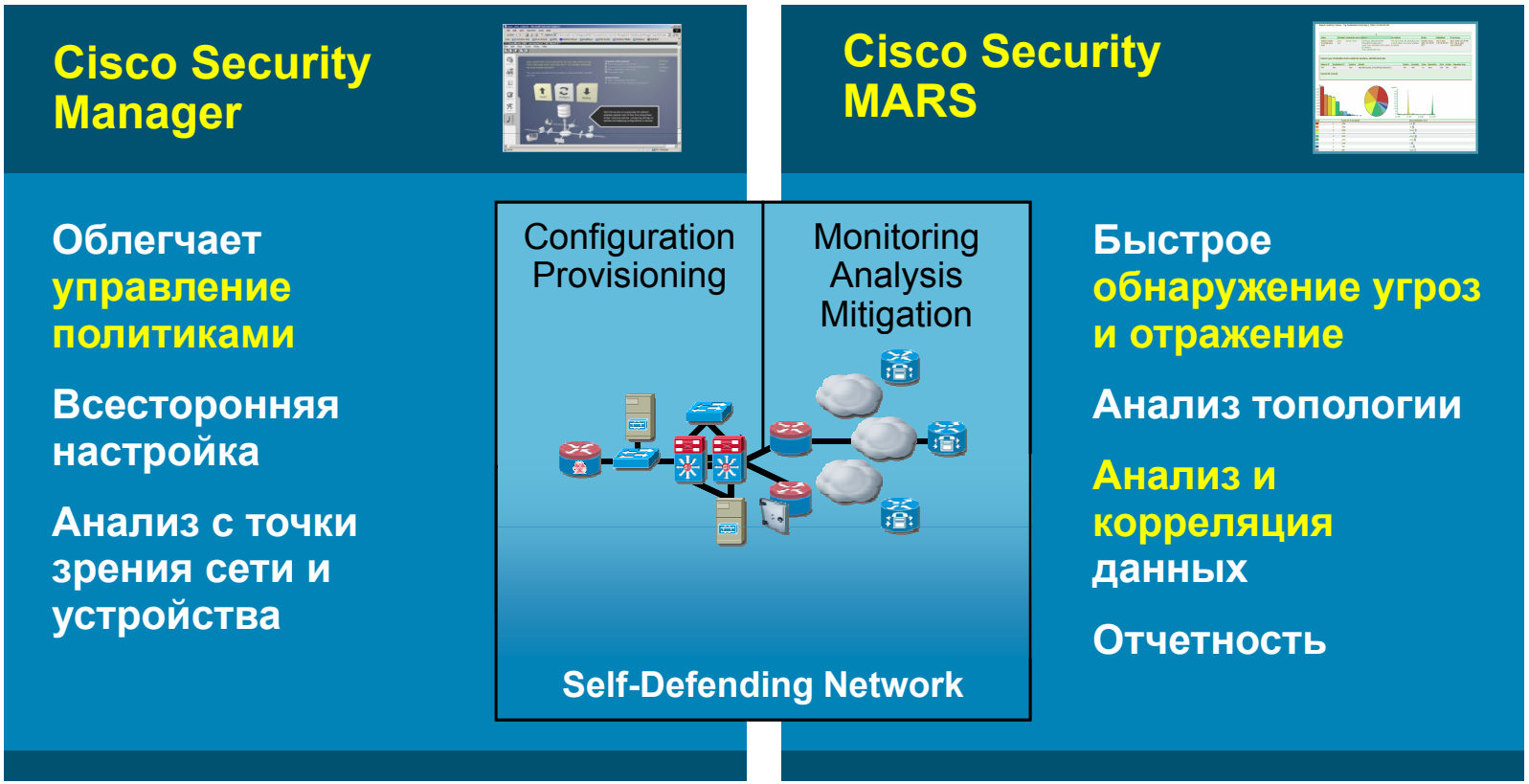
Мобильные пользователи

Удаленные офисы

Управление ПО
Образы, инвентаризация, патчи…

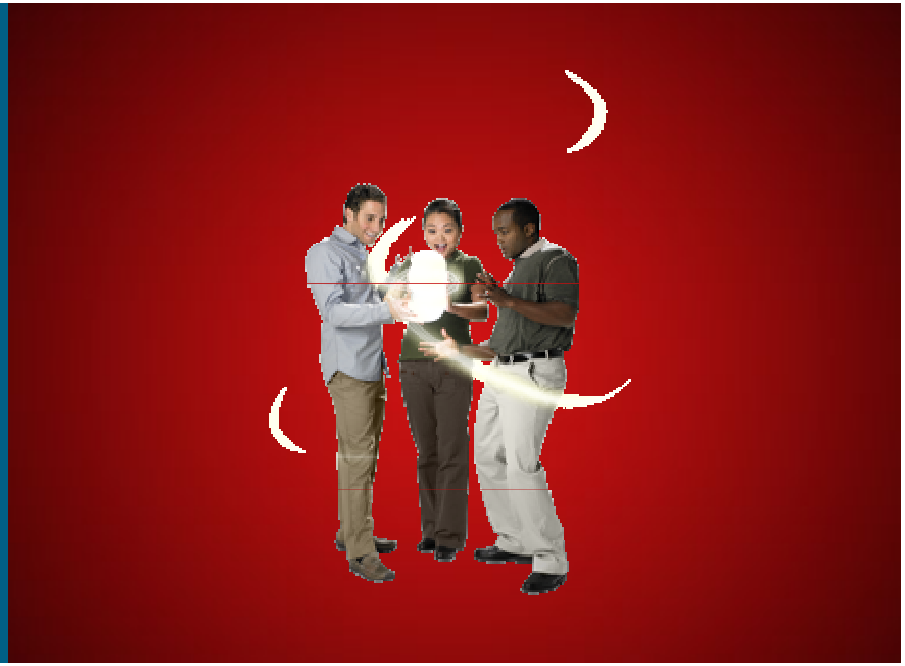
Противодействие
Как противодействовать угрозам с помощью сети

Cisco Security Management Suite



- Интеграция с Cisco Secure Access Control Server
  - Ролевой контроль доступа
  - Регистрация действий

Обзор MARS



Задача управления безопасностью

Характеристики современных сред:

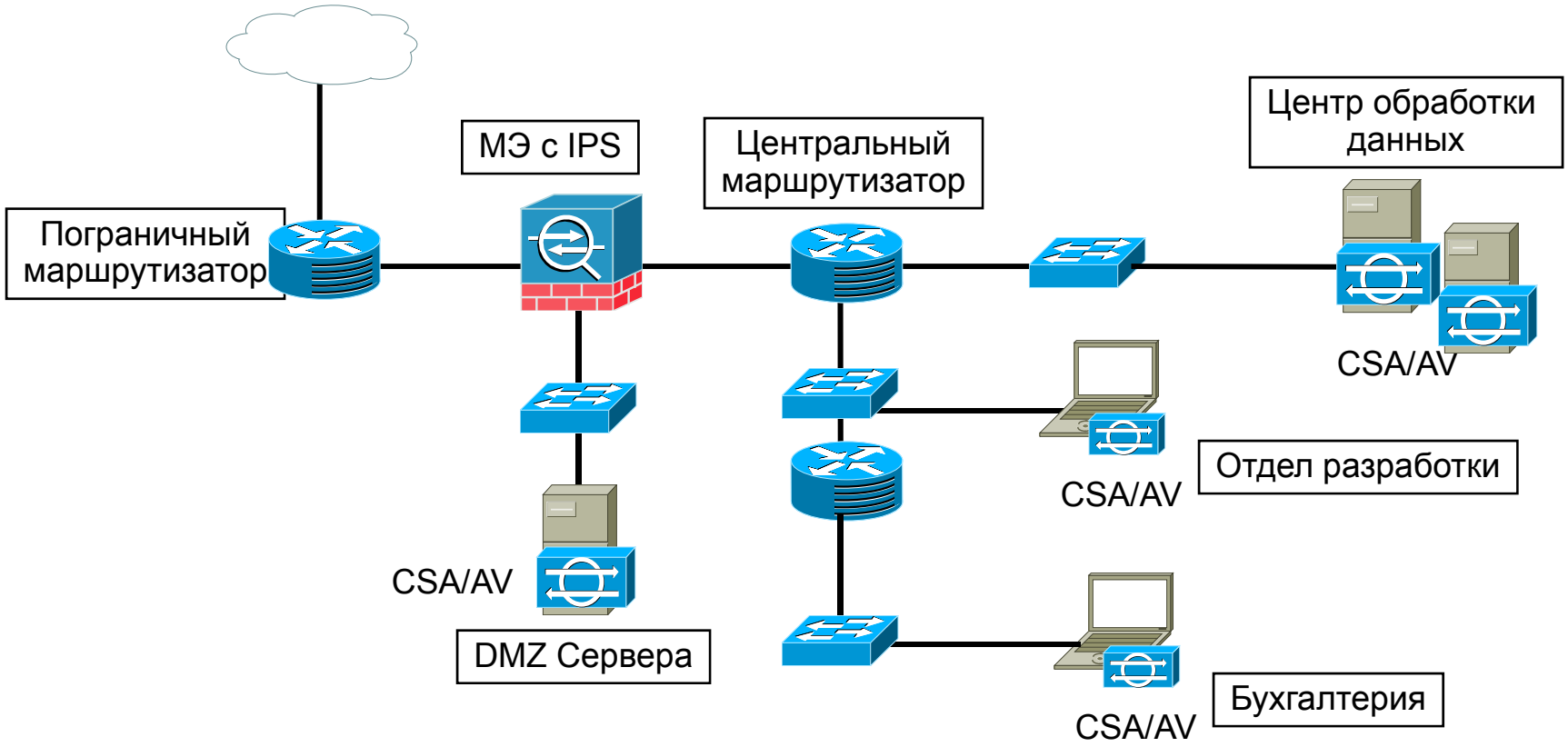
- Множество продуктов с различными интерфейсами настройки
- Большой объем данных журналов сетевых устройств
- События и тревоги безопасности от различных сетевых элементов
- Сложные архитектуры
- Отдельные средства управления политикой безопасности и информационными системами
- Отсутствие интегрированных средств формирования отчетности

Почему мы должны заниматься мониторингом инцидентов ИБ

- Требования стандартов и РД
  - ГОСТ Р ИСО/МЭК 17799:2005
  - ГОСТ Р ИСО/МЭК 18044
  - СТР-К
  - и др.
- Рекомендации (Cisco SAFE и т.п.)
- Политики ИБ

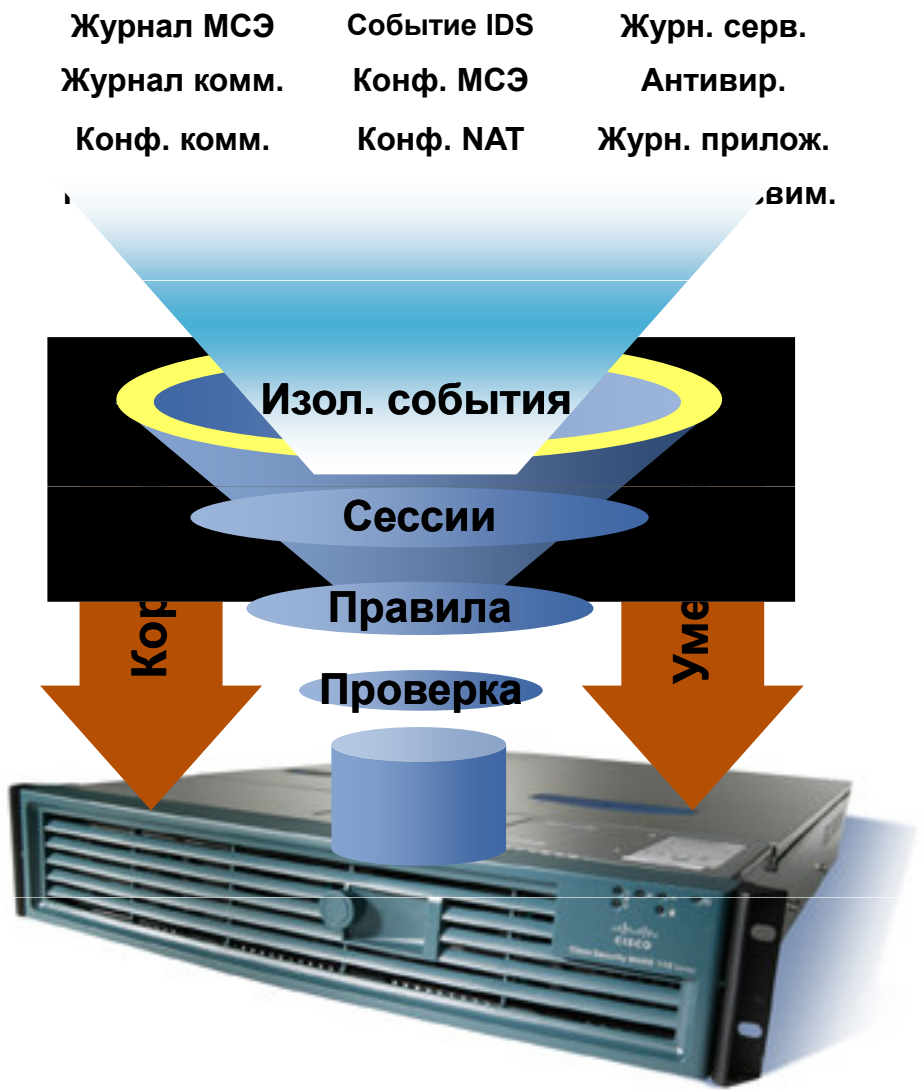
Обыкновенная сеть

- Большое кол-во событий, разрозненные консоли разных производителей



Cisco Security MARS
Monitoring, Analysis, Response System

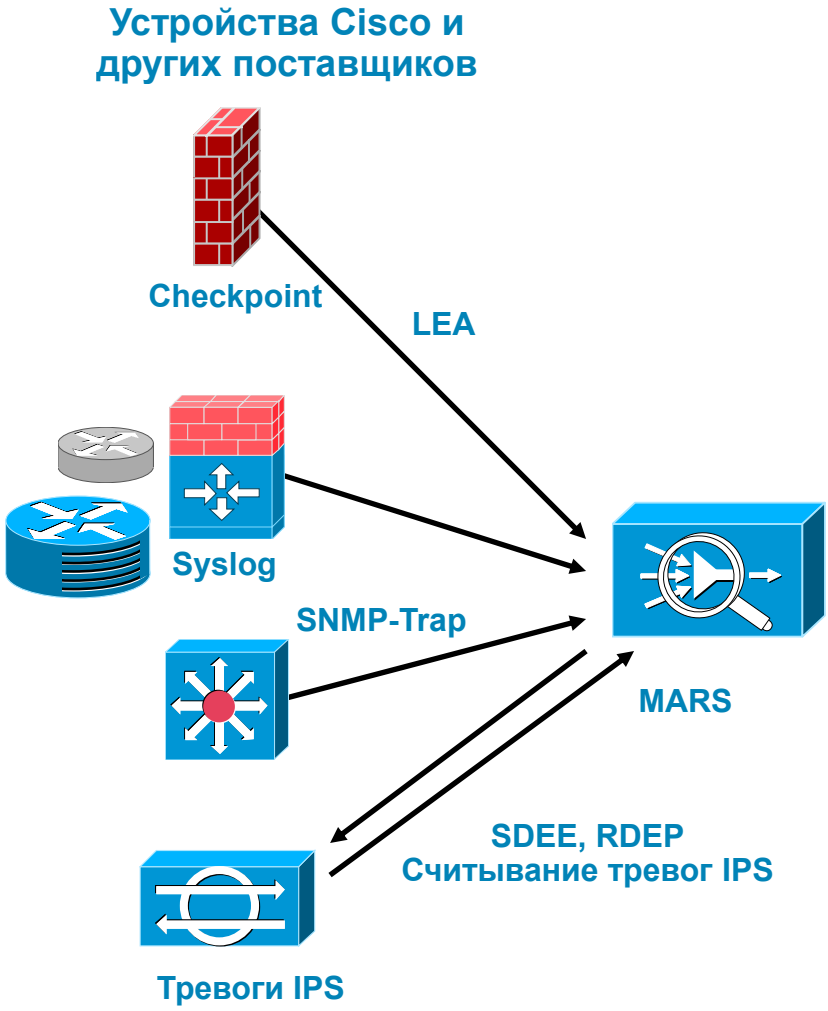
- Корреляционный анализ данных
- Поддержка различных устройств и систем ИБ разных поставщиков
- **Быстрое обнаружение инцидентов , их изоляция и противодействие**
- Привязка к топологии
- Анализ профилей сетевого трафика



Основные понятия — события

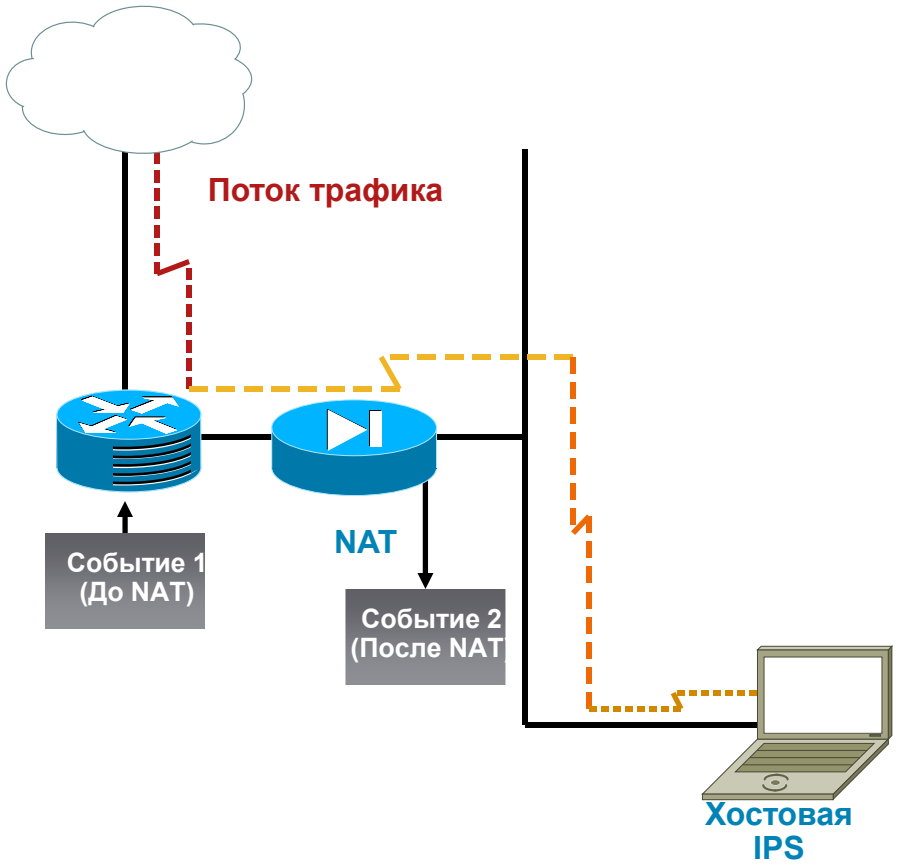
События от устройств

- Событие = сообщение, созданное устройством, которое контролируется MARS
- **Передача** (“Push”) сообщений в MARS устройствами мониторинга (syslog, SNMP-trap и т. п.)
- <ИЛИ>
- **Считывание** (“Pull”) сообщений устройством MARS (сообщения IPS, журналы Windows и т. п.)



Основные понятия — сессии

Сессия — множество сообщений (событий), которые коррелируют в ходе анализа MARS с учетом NAT-преобразования

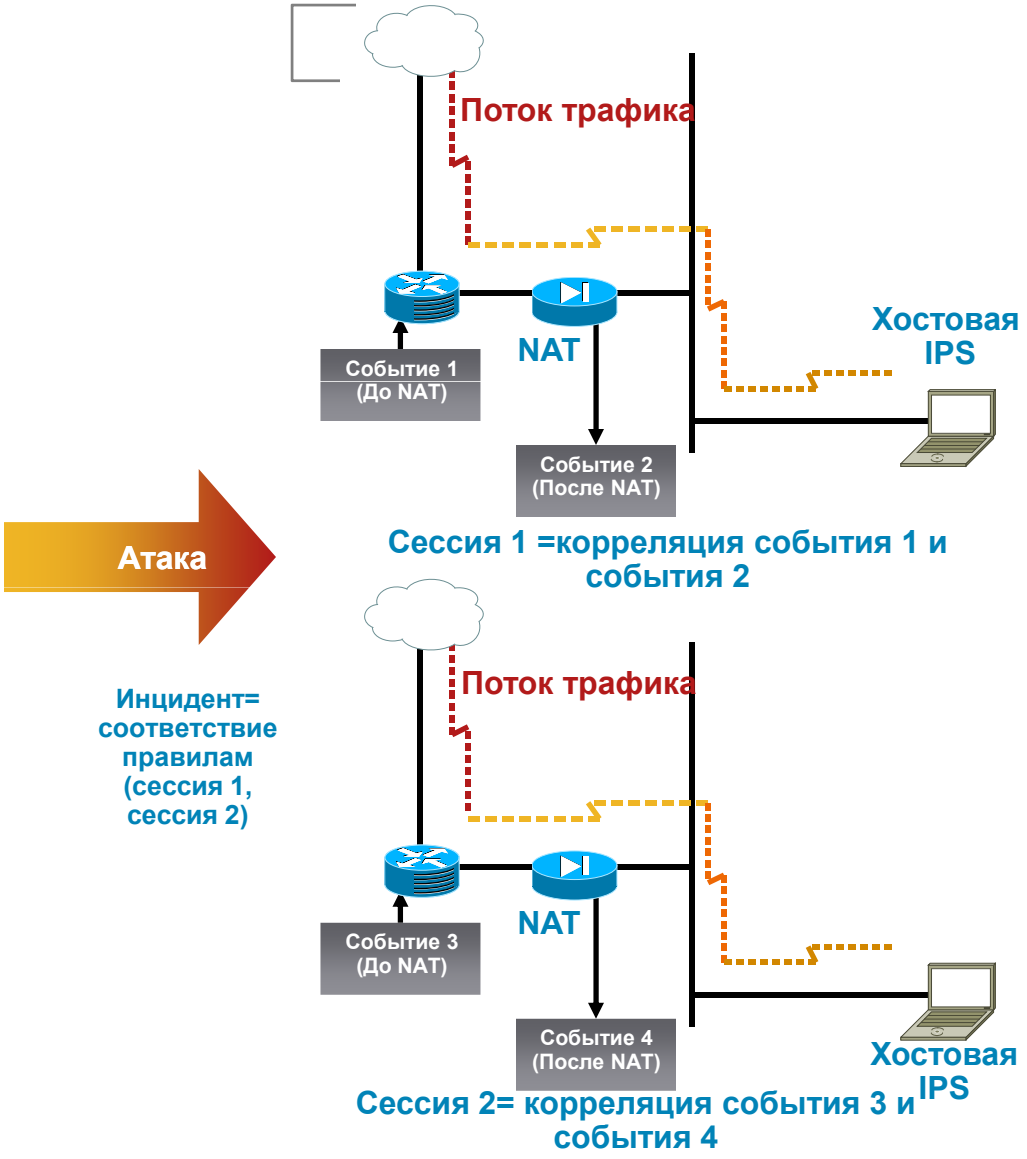


Сессия = корреляция события 1 и события 2 с учетом NAT-преобразования

Основные понятия — инциденты

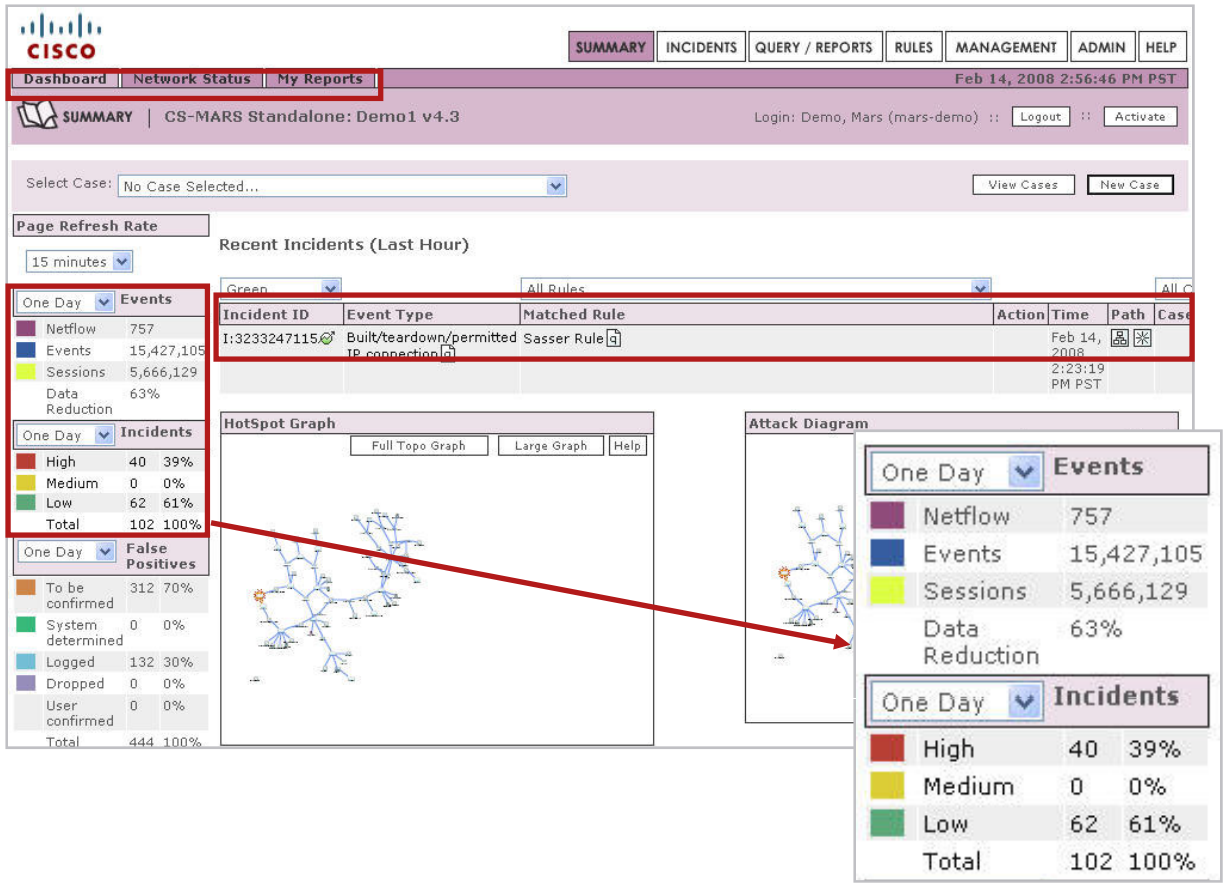
Инцидент — множество сессий, соответствующее определенным правилам обнаружения угроз

- **В качестве правил могут использоваться правила, заложенные в систему MARS компанией Cisco, или правила, определенные администратором для своей системы**



Обнаружение угроз и отражение атак

«Единая панель» обнаружения угроз – уменьшение объема данных



Панель инцидентов

- **Агрегация**
- **Корреляция**
- **Выделение важной информации**

15 427 105 событий

5 666 129 сессий

102 инцидента

40 инцидентов с высоким уровнем опасности

- **Объединение данных Netflow, Syslog и информации о топологии сети позволяет создать центр управления безопасностью на базе MARS**
- **Оперативное обнаружение угроз за счет снижения объема данных в режиме реального времени позволяет администраторам сконцентрироваться на решении высокоприоритетных задач**

Обнаружение угроз и отражение атак
Путь распространения атаки и учет топологии сети

Жертва/зараженный хост

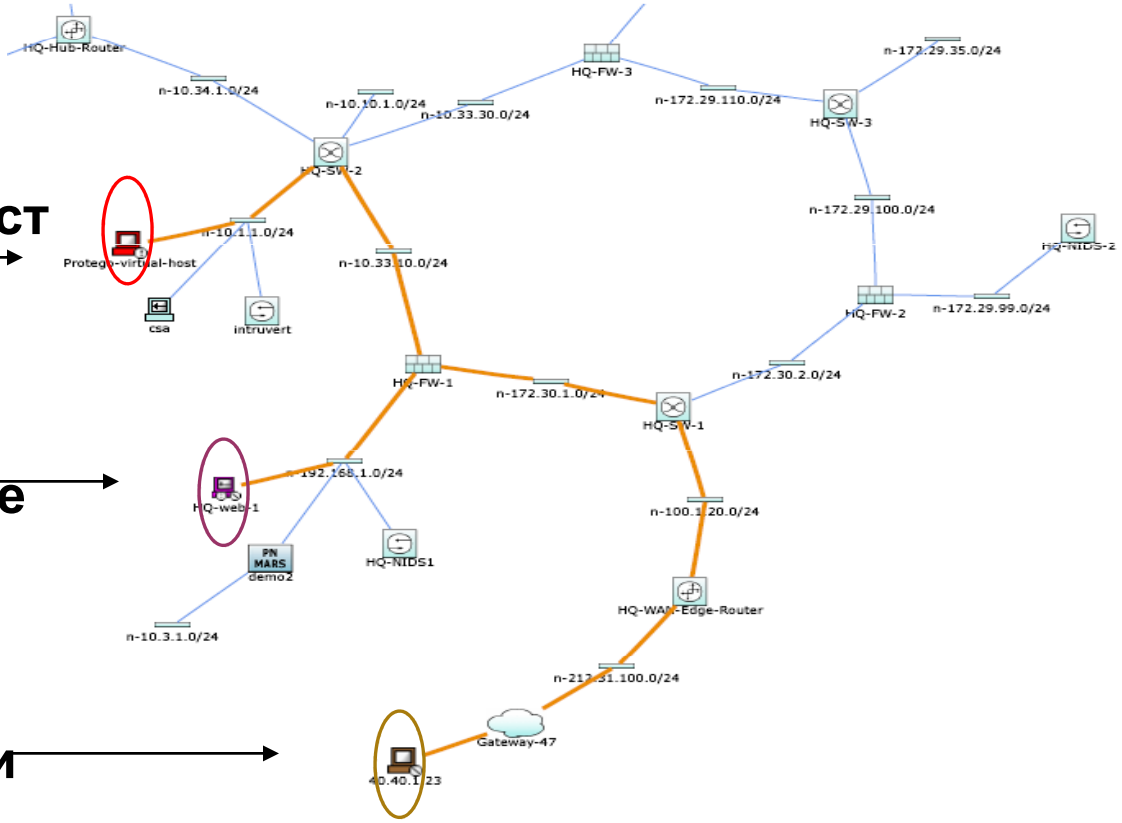
(красный)

Взломанный хост, участвующий в атаке

(сиреневый)

Источник атаки

(коричневый)



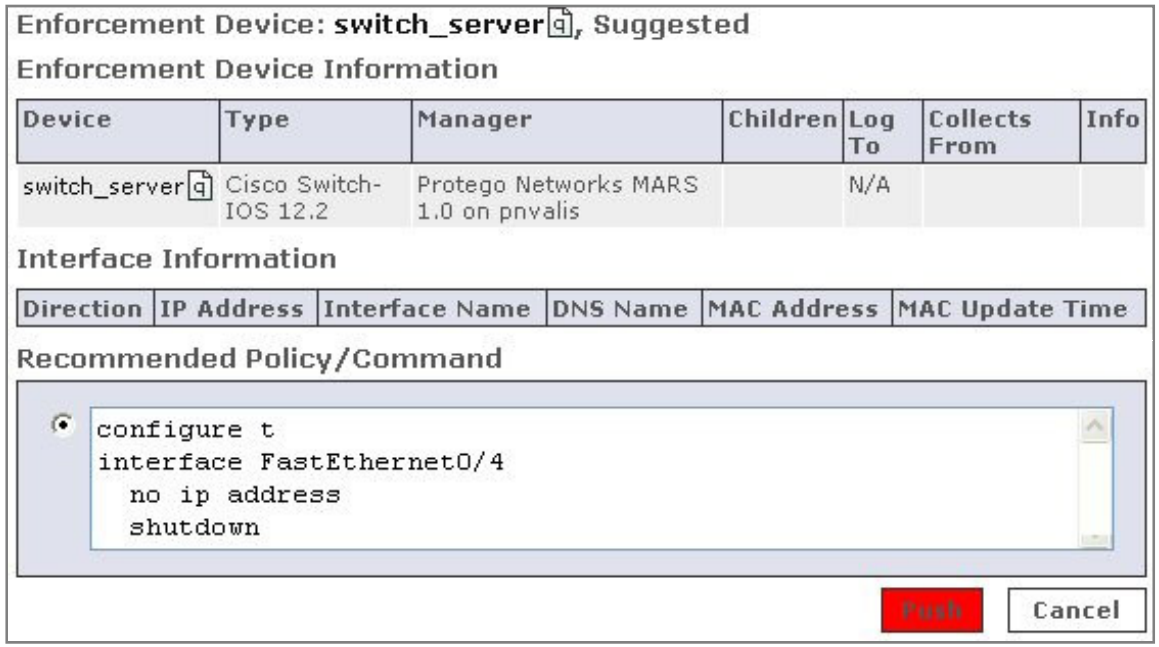
Обнаружение угроз и отражение атак

Отражение атак

- **Использование функций управления, уже существующих в рамках ИТ-инфраструктуры**

  Четкое представление пути атаки на уровнях 2 и 3

  Обнаружение устройств для отражения атак



Системные/настраиваемые отчеты

Пример. Отчет по 10 наиболее популярным портам, соединения на которые были запрещены МСЭ

Отчет создается каждый час

Отчет за 24 часа

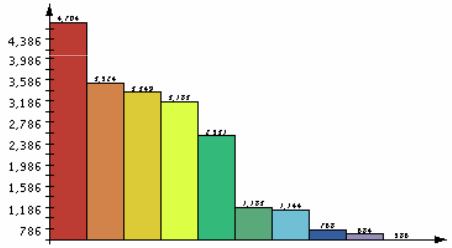
Report: Activity: Denies - Top Destination Ports Sep 8, 2004 1:07:45 PM PDT

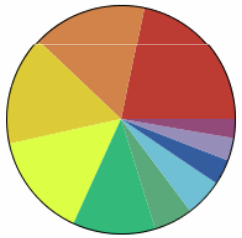
Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
Activity: Denies - Top Destination Ports	*Every hour*	*Normal*	None	*Event type: AttacksProtected, FirewallPolicyViolation/ACL, Query Type: Destination Ports ranked by Sessions Time: 1dd:0hh:0mm:0ss*	This report ranks the destination ports to which attacks have been targetted but denied.	Finished: Sep 8, 2004 1:07:43 PM PDT	Sep 8, 2004 1:07:39 PM PDT	Sep 7, 2004 1:07:39 PM PDT - Sep 8, 2004 1:07:39 PM PDT

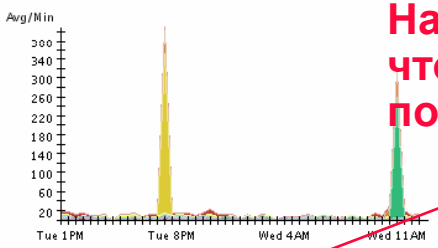
Report type: Destination Ports ranked by Sessions, 1dd:0hh:0mm:0ss

Source IP	Destination IP	Service	Events	Device	Severity	Zone	Operation	Rule	Action	Reported User
ANY	ANY	ANY	AttacksProtected, FirewallPolicyViolation/ACL	ANY	ANY	CA	None	ANY	ANY	ANY

Keywords: [None]



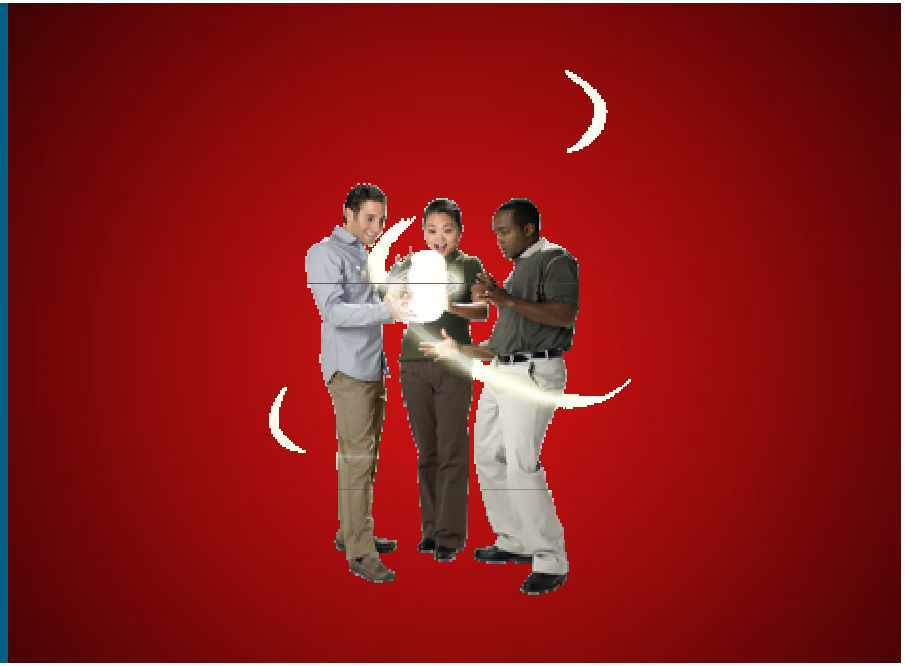




Нажмите на значок “q”, чтобы получить справку по порту 445

Rank		Count (# of sessions)	Raw Destination Port
	1	4704	445
	2	3524	80
	3	3349	26686
	4	3183	135
	5	2531	47683
	6	1183	1026
	7	1144	0
	8	768	139
	9	684	9898

Обзор CSM



Требования к системе управления политиками ИБ

- Масштабируемость от десятков до тысяч устройств
- Единая политика на всех устройствах
- Ролевой доступ
- Документооборот
- Контролирование, кто, и что можно делать на устройствах
- Абстрагировать политики от способов реализации правил на различных платформах

Cisco Security Manager

Управление политикой

Централизованное **управление политиками** для МСЭ, VPN и IPS

Хорошо **масштабируем**

Наследование политик позволяет эффективно распределять их по сети

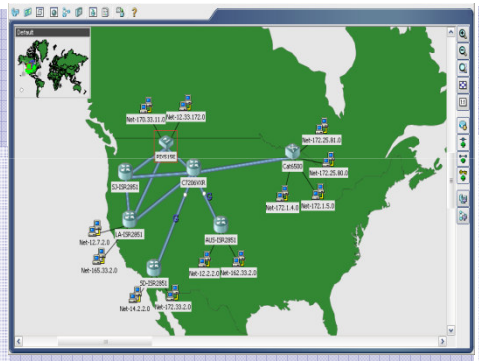
Мощное **группирование устройств**

Удобство использования

Визуальное управление политиками через таблицы или **карту сети**

Функция **Jumpstart:** удобный инструмент обучения

Эффективная **визуализация:**
- Policy-based
- Device-based
- Map-based
- VPN based



Управление МСЭ

Настройка политик для ASA, PIX, FW SM и IOS Firewall

Единая таблица правил для всех платформ

Анализ политик

«Умное» редактирование правил в таблице

Устранение избыточности и противоречивости

Управление VPN

VPN Wizard настраивает Site-to-Site, hub-spoke и full mesh VPN за несколько кликов мыши

Настройка VPN для удаленного доступа, DMVPN и устройств с Easy VPN

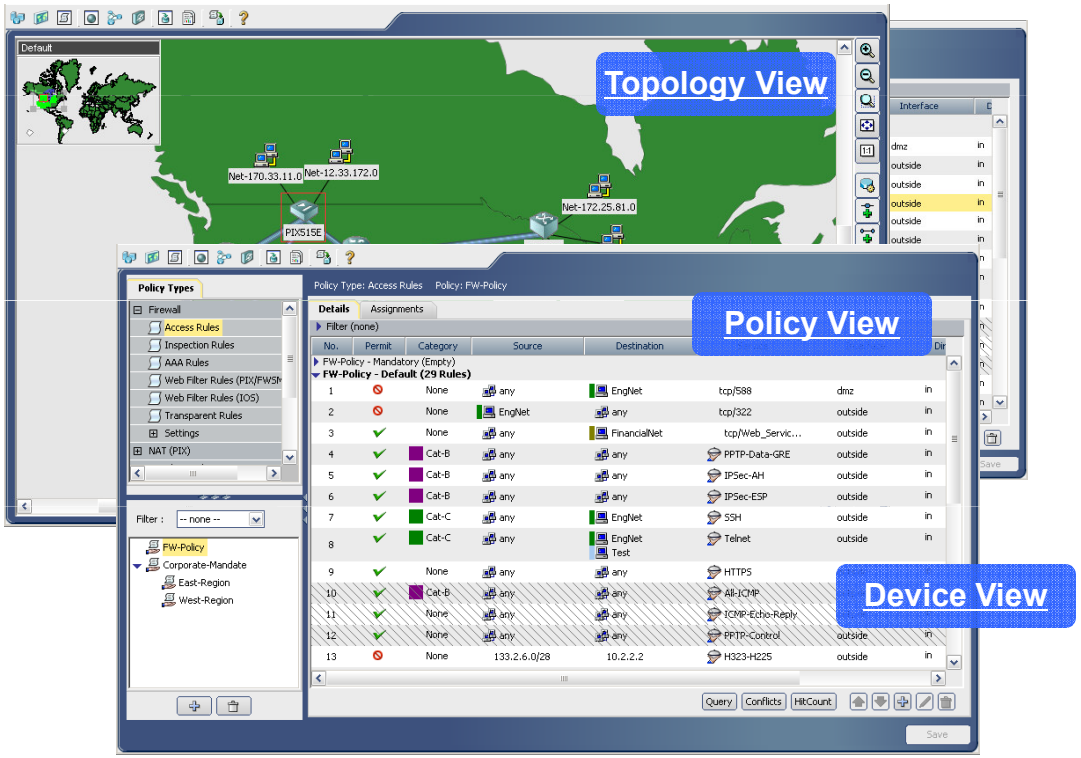
Управление IPS

Автоматическое обновление сенсоров IPS

Поддержка **Outbreak Prevention Services**

Простота использования

- Удобный и гибкий в настройке интерфейс управления
- Различные отображения для решения различных целей
  - Device View
  - Topology View
  - Policy View
- Создание VPN за несколько кликов мыши
- Унифицированное управление всеми средствами защиты , как абстрактным устройством
  - Firewall, VPN, IPS…
- Поддержка ASA, PIX, IPS Sensors, ISR, C6k и Catalyst Service modules



Лучшие методики

Совместное использование общих политик

Требования

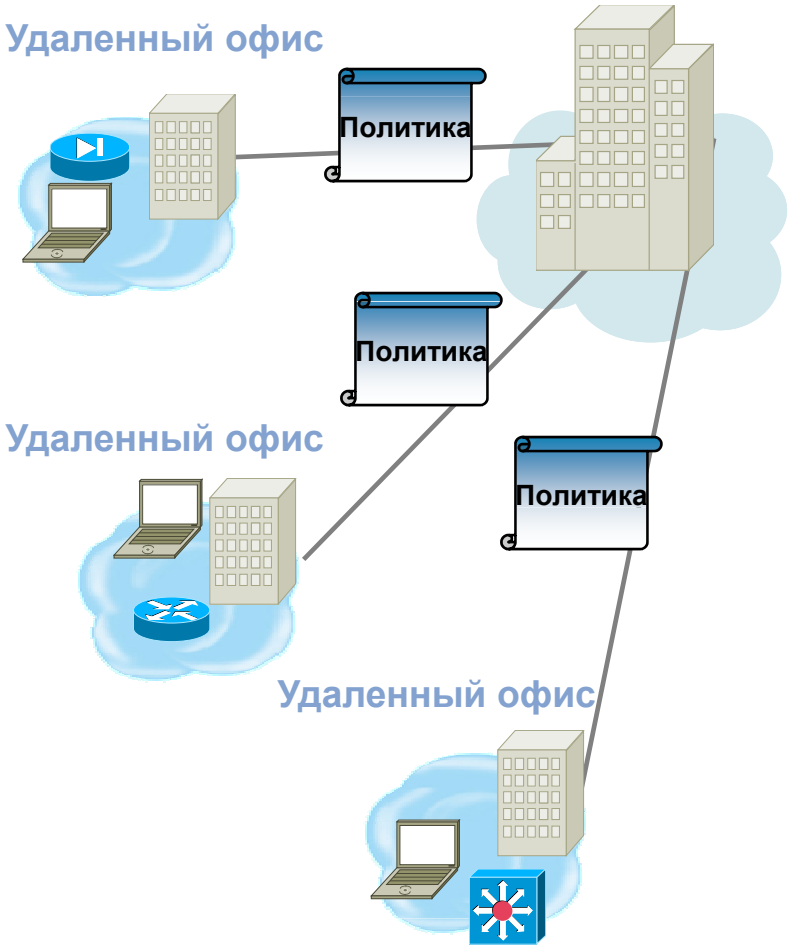
- Совместное использование политик на разных платформах
- Уточнение на уровне удаленных офисов

Примеры

- Для удаленных офисов 90% правил идентичны
- Различия минимальны
- Унификация правил
- Возможность переопределить правила на уровне удаленного офиса

Преимущества

- Поддержка одной последовательной политики провидит у упрощению
- Упрощение и ускорение внесений изменений



Лучшие методики
Иерархичные политики и наследование

Требования

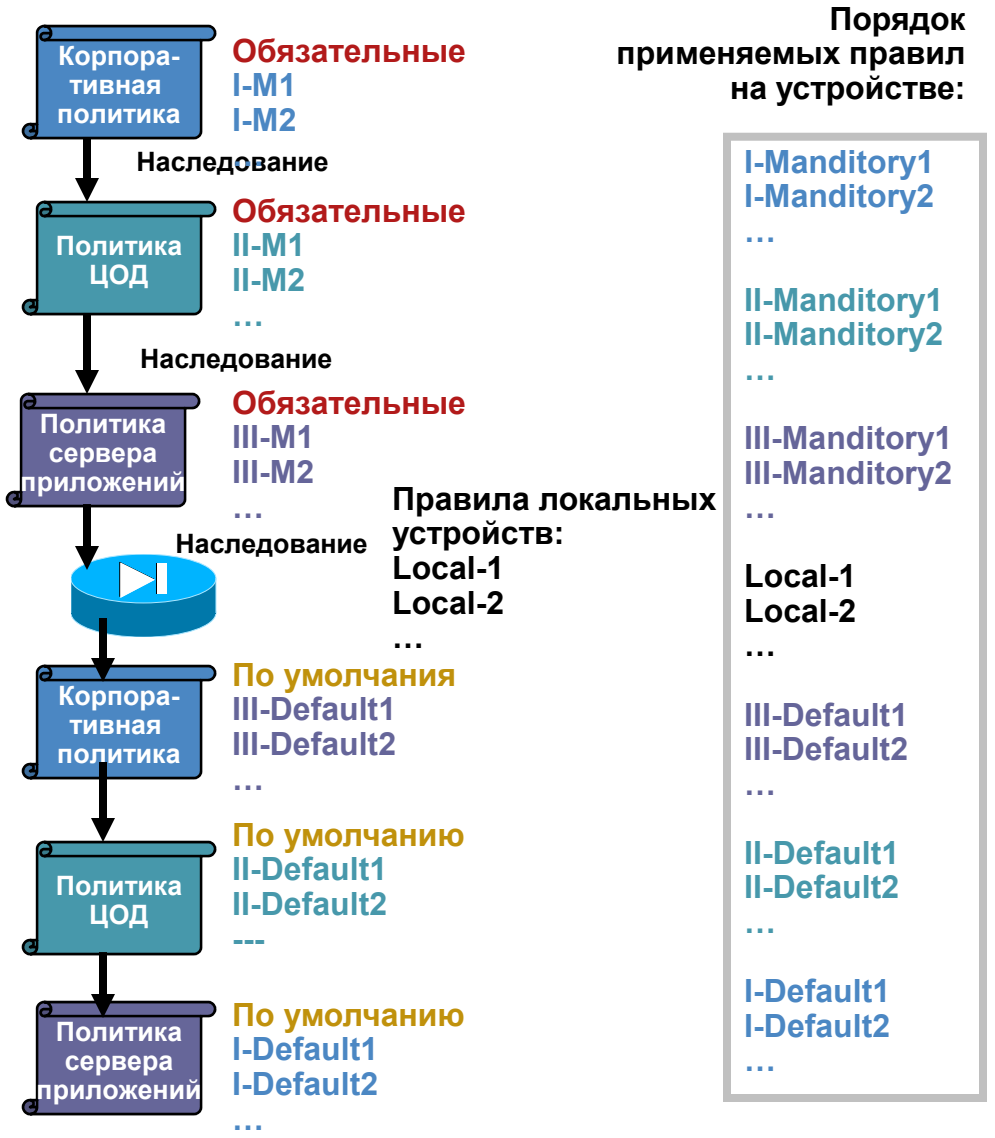
- Возможность создание обязательных и наследуемых политик
- Возможность по внесению исключений

Примеры

- Запретить IM file transfer
- Разрешить SSH, SSL

Преимущества

- Контроль организационного уровня
- Интеграция разрозненных политик
- Уменьшения вероятности ошибок



Применение политик на основе доменов

Требования

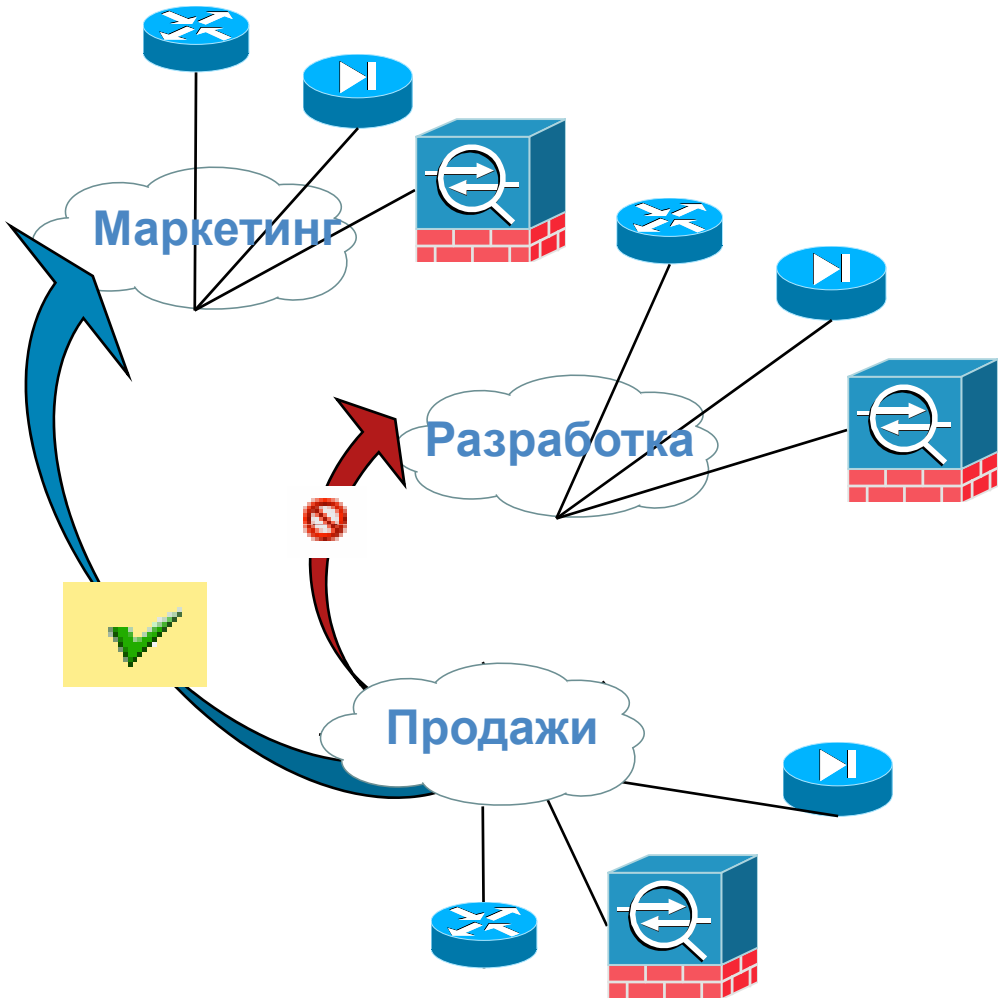
- Упрощение применения политик используя домены и роли
- Возможность исключений

Пример

- Запрет FTP для отделов разработки

Преимущества

- Рост гибкости
- Учет организационной структуры, а не физического размещения устройств
- Снижение времени на создание политик



Документооборот
“Хочу контролировать и ставить свою подпись”

Что это такое?

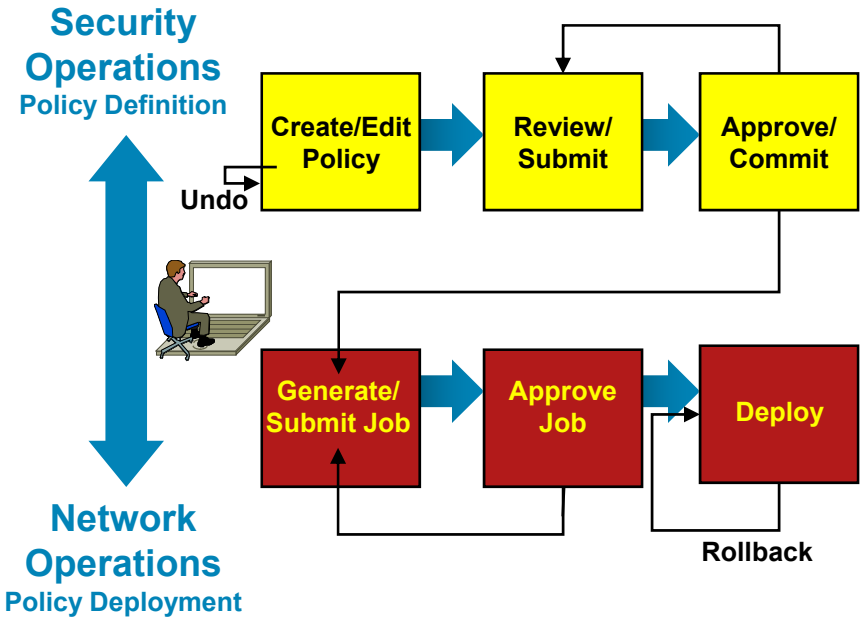
- Структурированный процесс контроля и утверждения изменений политики

Пример

- Кто создает политику?
- Кто утверждает политику?
- Кто применяет политику и когда?

Преимущества

- Эффективное взаимодействие между ролями/отделами



МСЭ, VPN и IPS

- Кто может изменять политики?
- Кто может просматривать изменения?
- Кто может их утверждать?
- Кто отвечает за применение новых политик?

Что бы хотелось дополнительно…

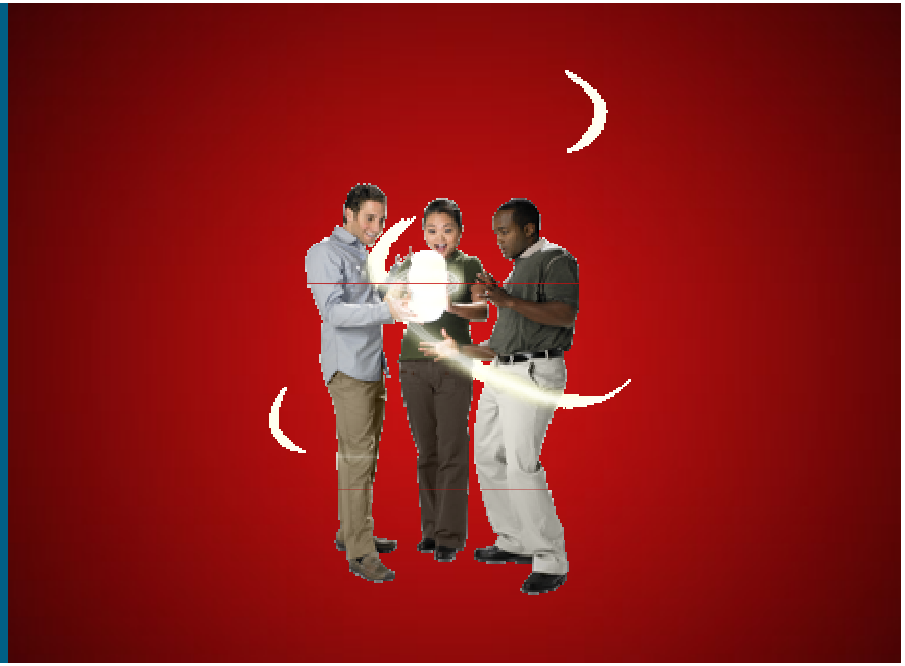
CSM

- Возможность получения исторической справки
- Возможность получения информации в режиме реального времени (отладка)

MARS

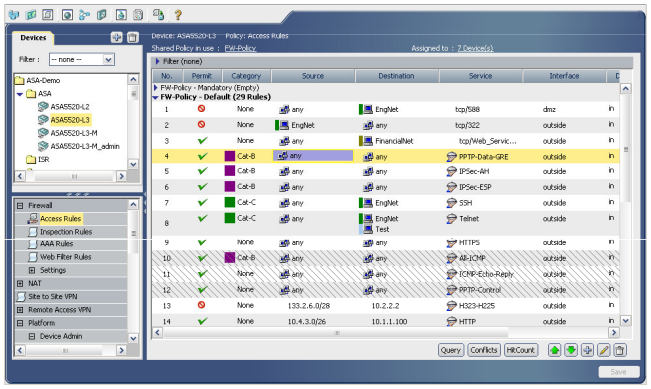
- Нет связи событий/инцидентов с политикой ИБ - «Зачем нужно это правило»
- «Какие настройки IPS сигнатур»

Интеграции между MARS и CSM

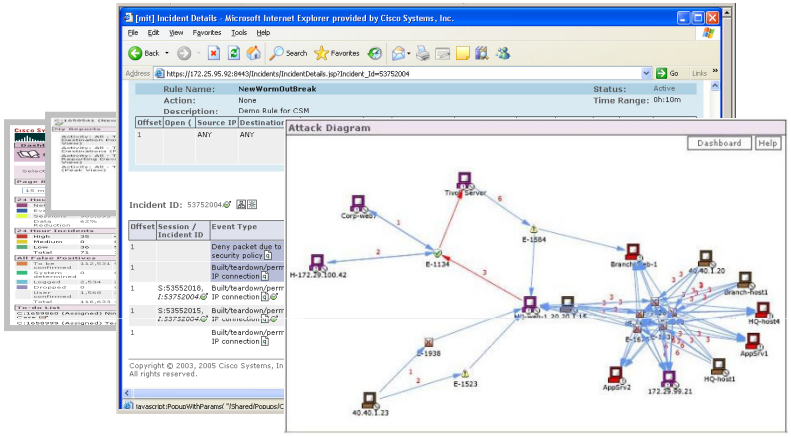


Управление эксплуатацией и политикой ИБ

Cisco® Security Manager



Cisco Security MARS



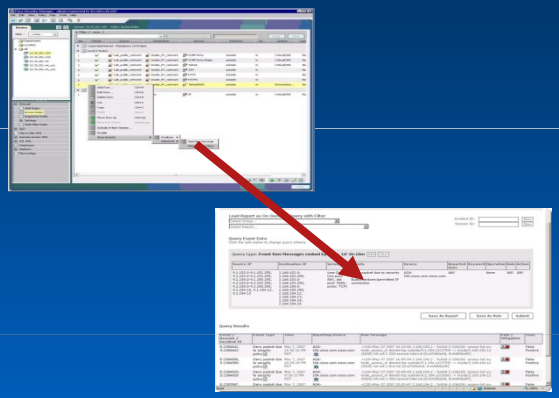
Преимущества интеграции

- **Упрощение работы** системы ИБ путем централизованной настройки политики и мониторинга угроз в режиме реального времени
- **Повышение эффективности** путем создания единого процесса управления работой сети и управления безопасностью
- **Интегрированные средства управления** изменениями и анализа инцидентов упрощают проведение аудита системы

Новые возможности CS-M 3.2 и MARS 6.0

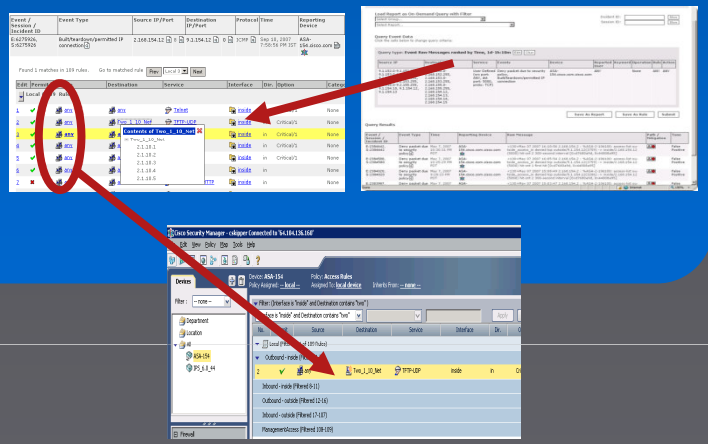
Упрощение управления за счет совместной работы

Связи событий МСЭ: «правила-события» и «события-правила»



«События-правила»

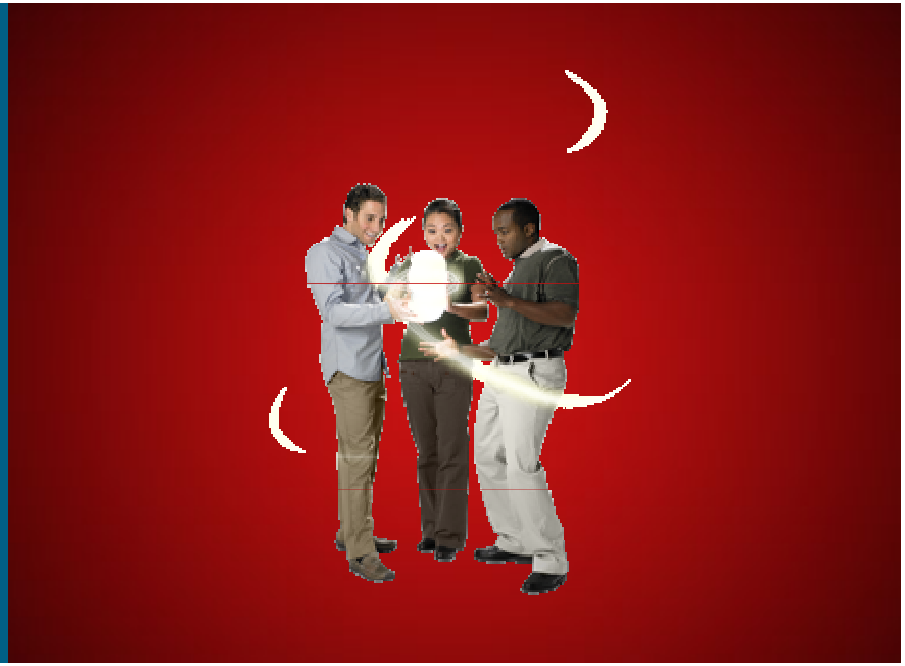
- Отслеживание событий до уровня правил создания, возможность внесения изменений
- Лучшее понимание исходных данных журнала



«Правила-события»

- Уменьшение времени поиска неполадок соединения
- Моментальная проверка новых развернутых политик

Расследование инцидентов ИБ и корректировка политик ИБ

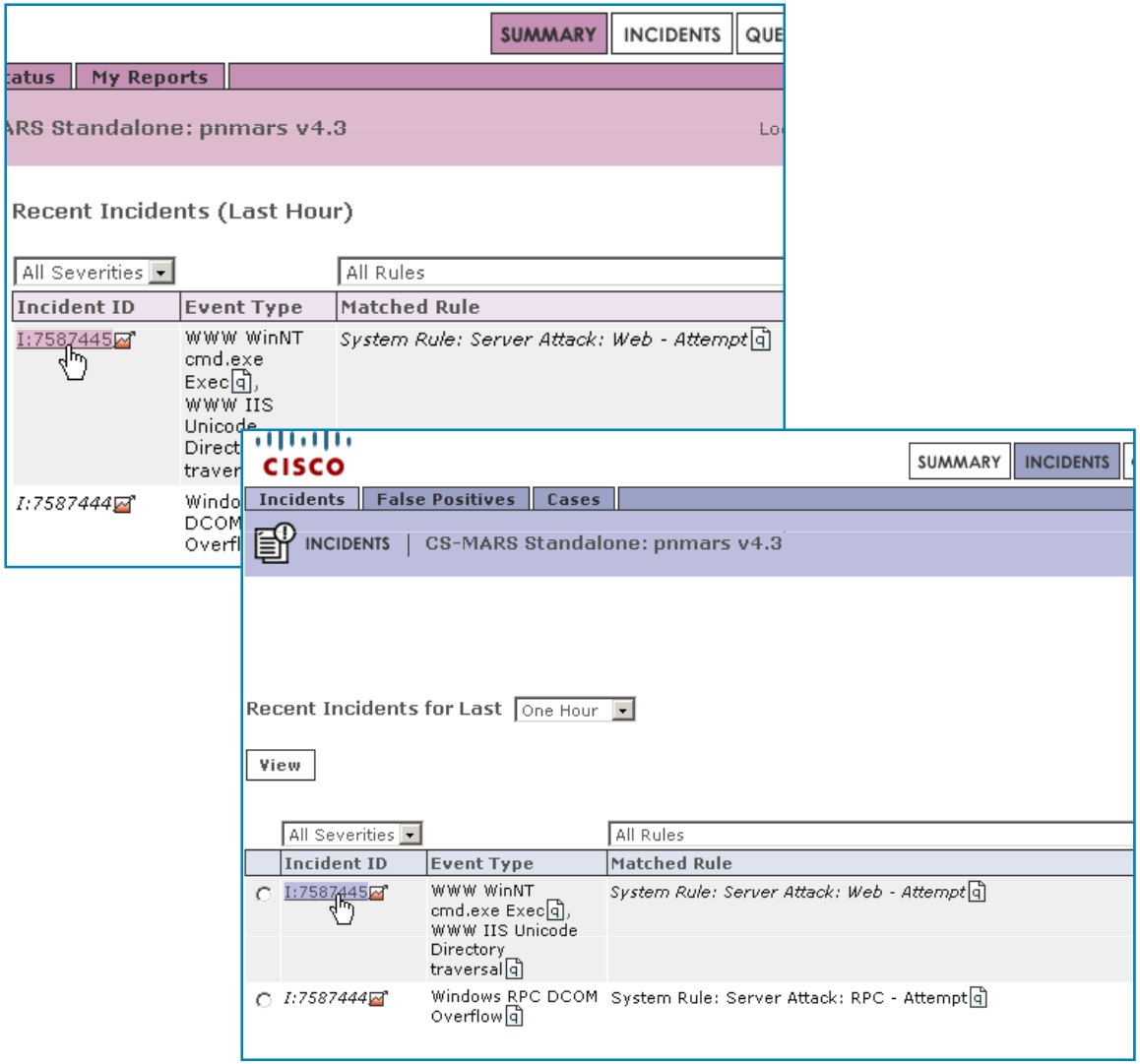


Примеры

- IPS событие → Политика
- Событие с МЭ → Политика
- Политика МЭ ASA → Событие

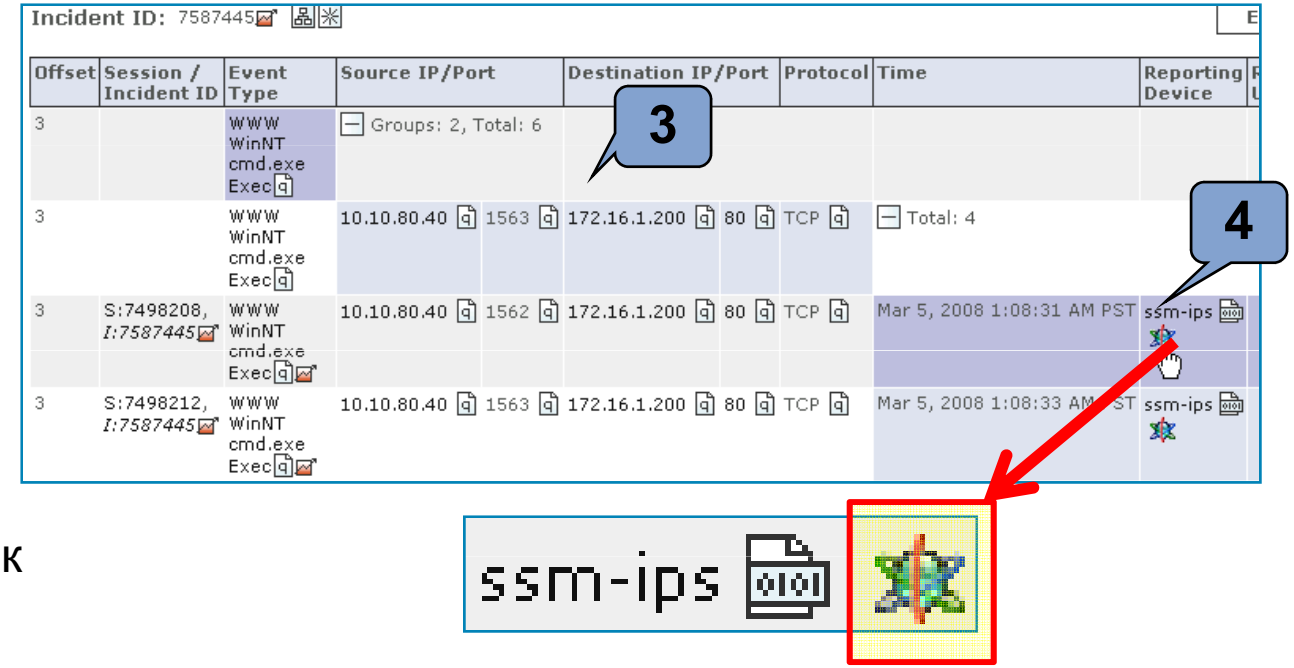
IPS событие → Политика

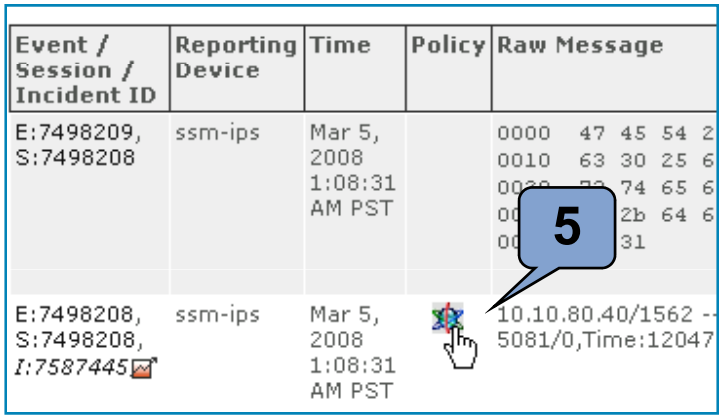
1. Откройте на MARS закладку – ***Summary*** *или* ***Incidents***
2. Выберите инцидент



IPS событие → Политика (прод.)

3. Раскройте сессии и обратите внимание на устройство, в этом случае ***ssm-ips***
4. Нажмите на иконку запроса к CSM.
5. Другая страница может показывать несколько строк, выберите одну и нажмите иконку CSM.

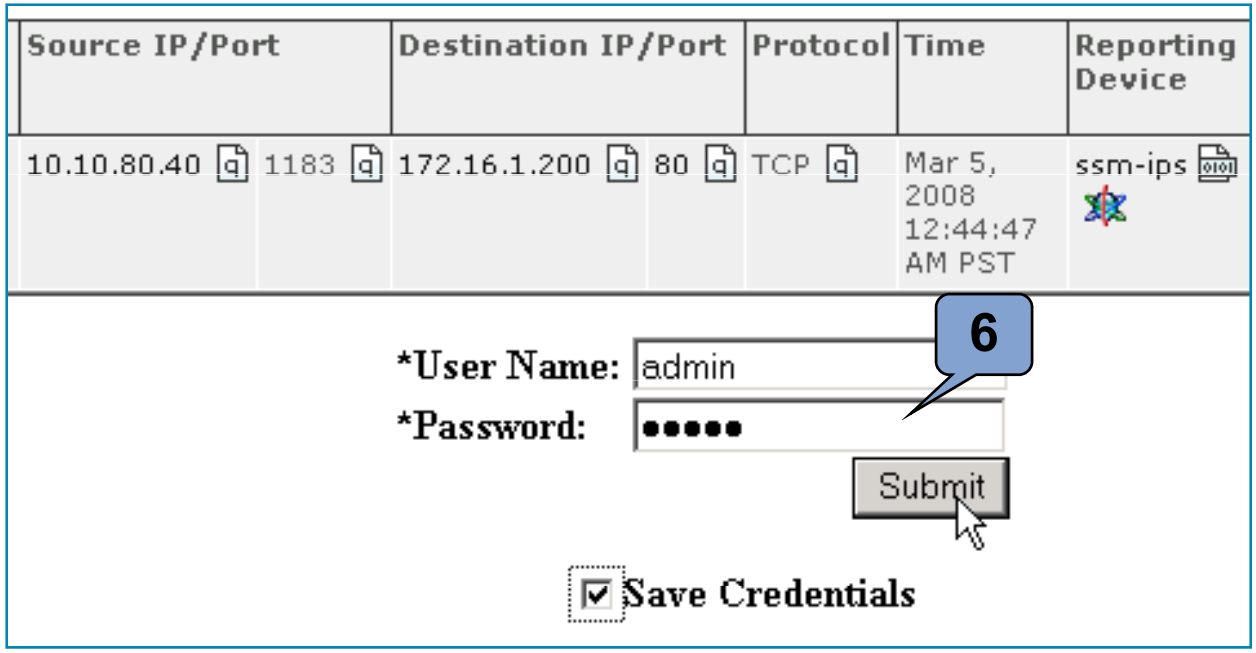




IPS событие → Политика (прод.)

6. MARS может запросить логин для CSM.

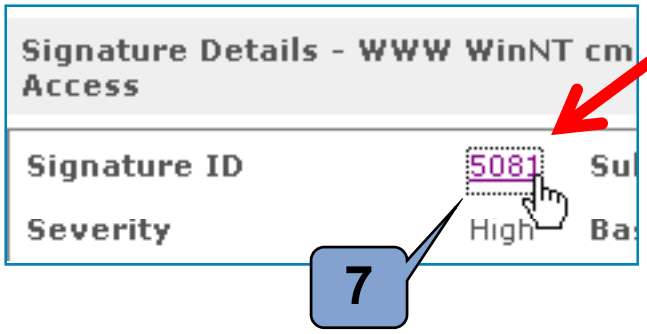
Логин будет закэширован только в рамках этой сессии.

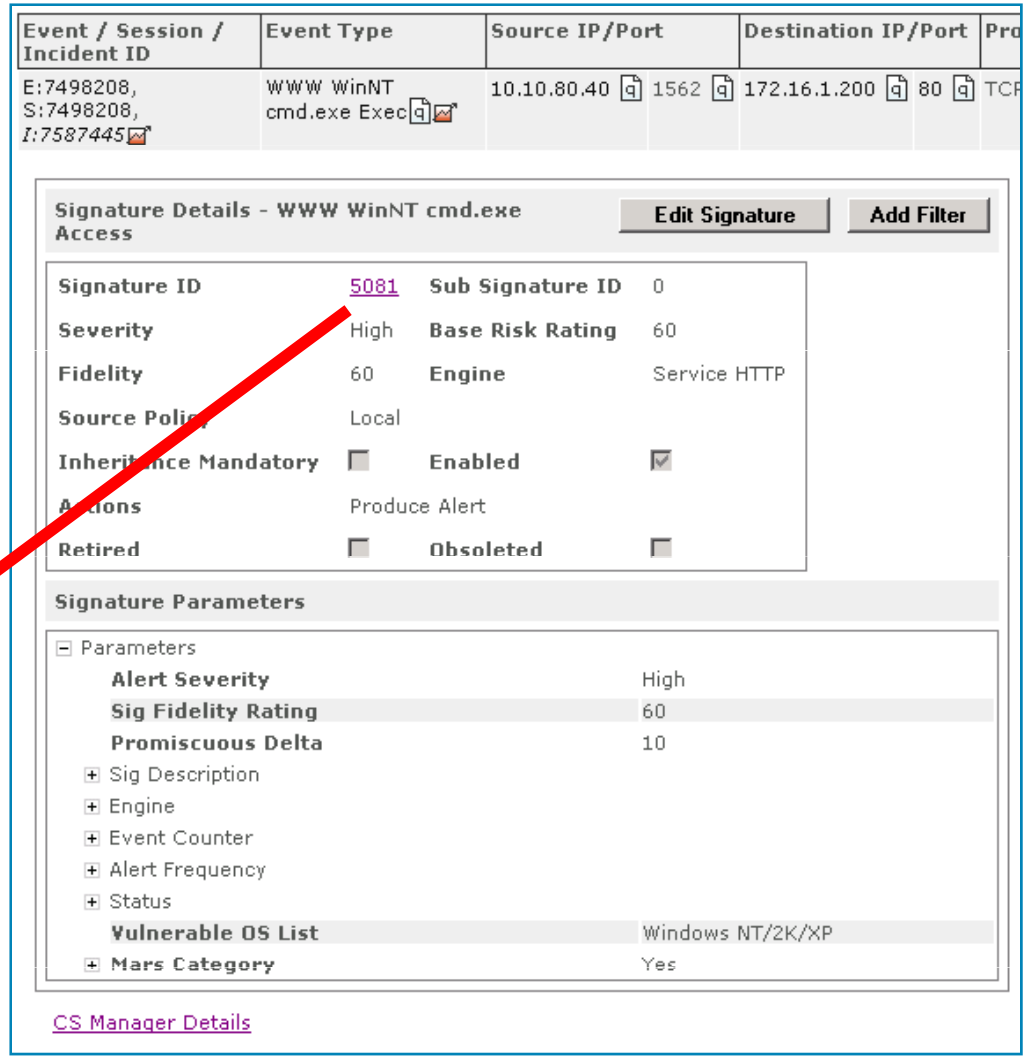


IPS событие → Политика (прод.)

MARS покажет страницу запроса с настройками сработавшей в этом инциденте сигнатуре.

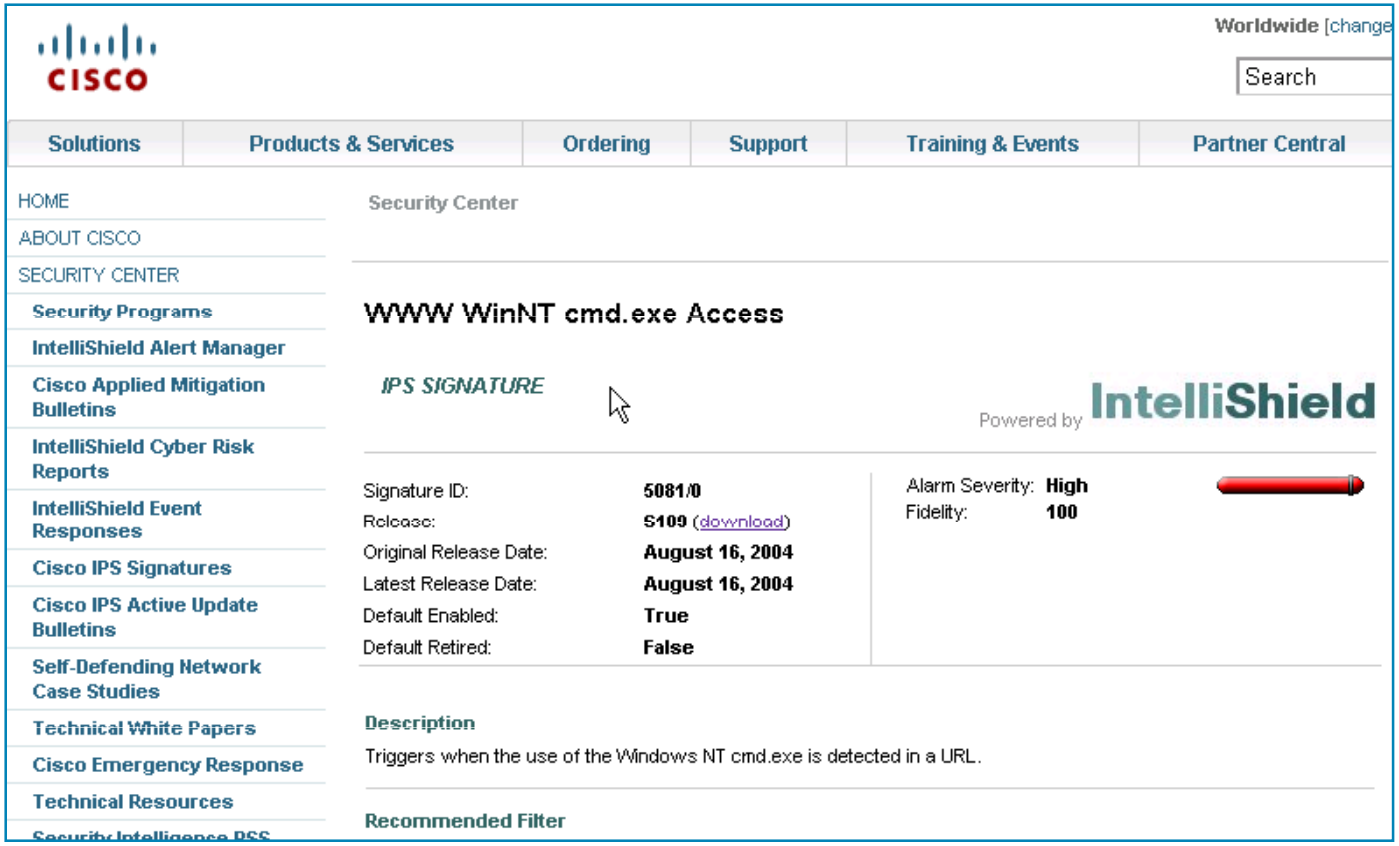
7. Нажмите на ***Signature ID***





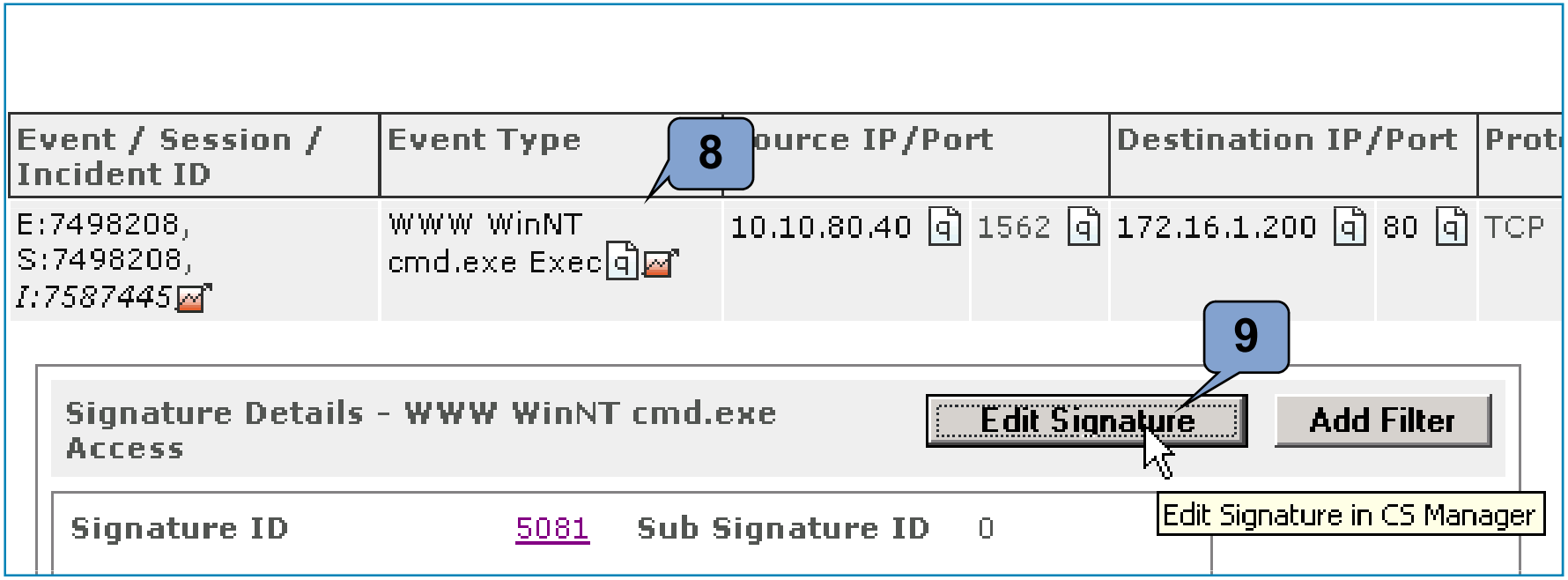
IPS событие → Политика (прод.)

MARS откроет страницу из базы **IntelliShield** посвященную этой сигнатуре.



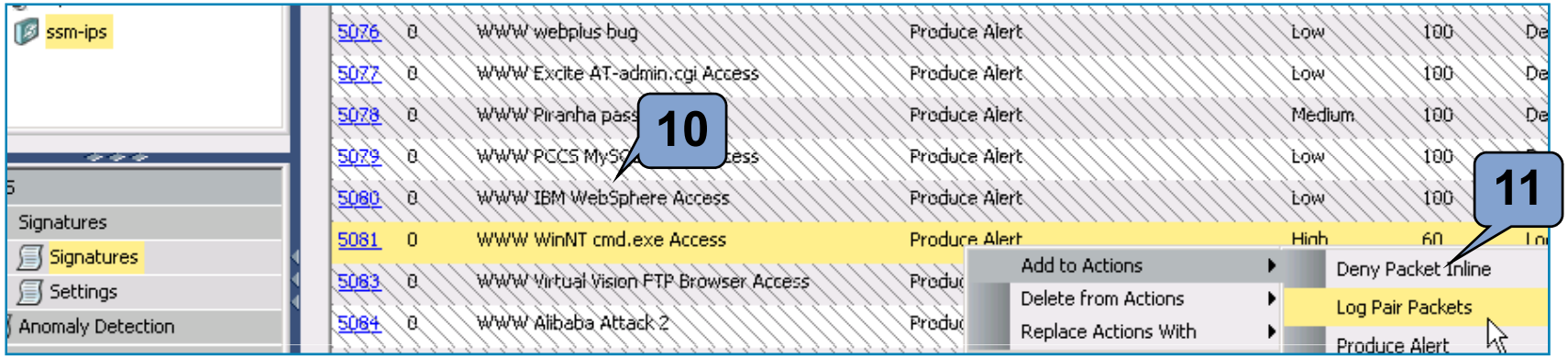
IPS событие → Политика (прод.)

8. Вернитесь на страницу создания запроса MARS
9. Нажмите ***Edit Signature***



IPS событие → Политика (прод.)

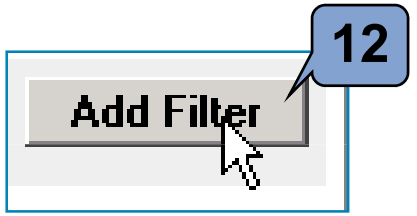
10. MARS запустит CSM → откроя страницу устройства, в этом случае ***ssm-ips*** → автоматически выделив сигнатуру (***5081***).
11. Здесь пользователь может настроить политику, в соответствии с своими полномочиями на CSM, например добавив какое-либо действие.

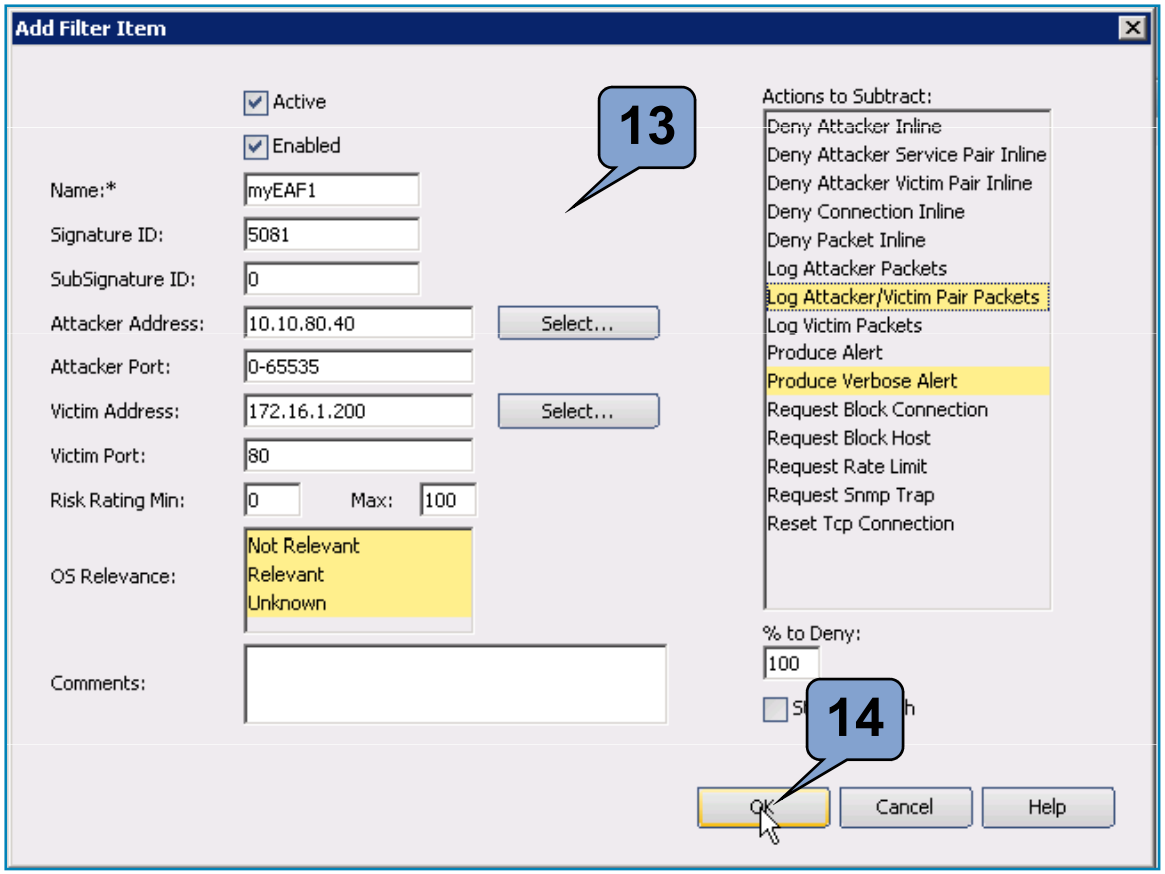


IPS событие → Политика (прод.)

12. Вернитесь на страницу запросов MARS, нажмите ***Add Filter***
13. MARS запустит CSM → открыв окно ***Add Filter Item***. Поля будут заполнены соответствующими данными.
14. Сделайте необходимые изменения, укажите имя фильтра → нажмите ***OK***.

    Изменения будут внесены в соответствии с расписанием.





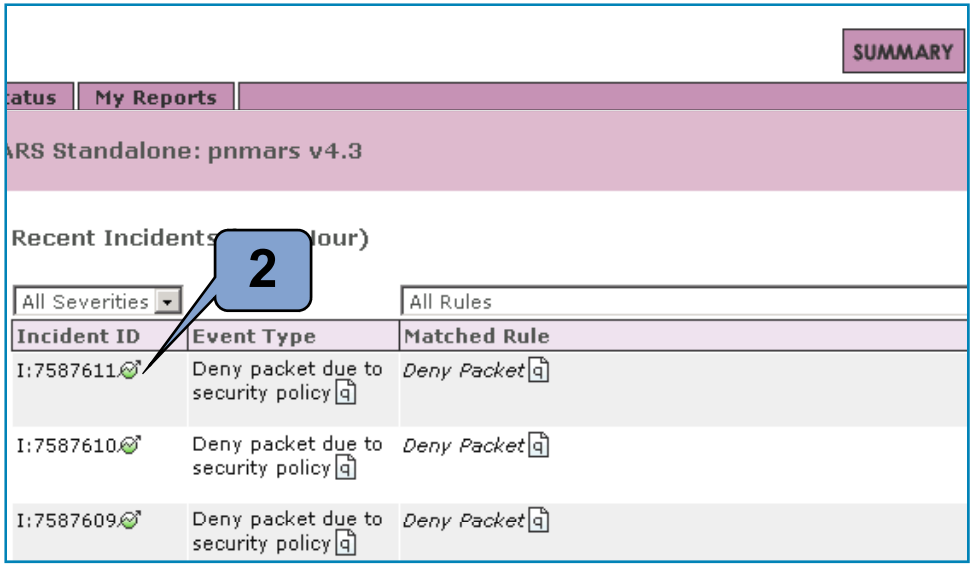
Примеры

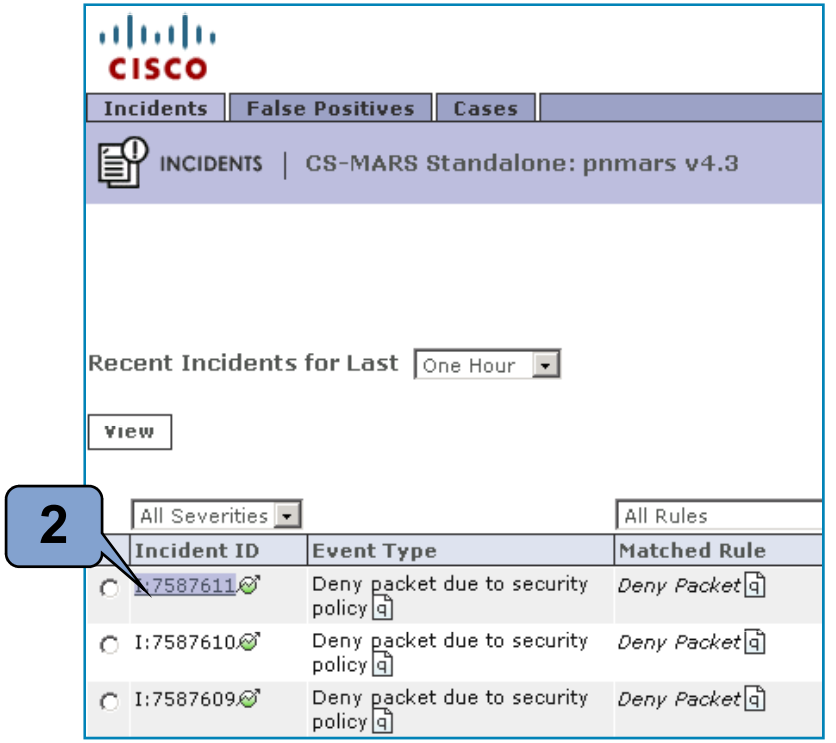
- IPS событие → Политика
- Событие с МЭ → Политика
- Политика МЭ ASA → Событие

Событие с МЭ → Политика

1. Откройте интерфейс MARS

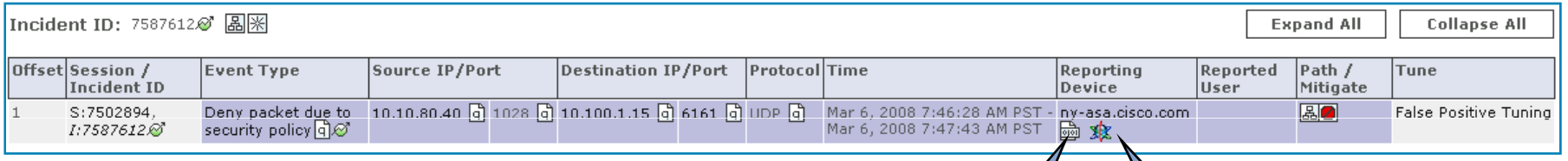
2. Из закладки Summary или Incidents tab выберите конкретный инцидент.



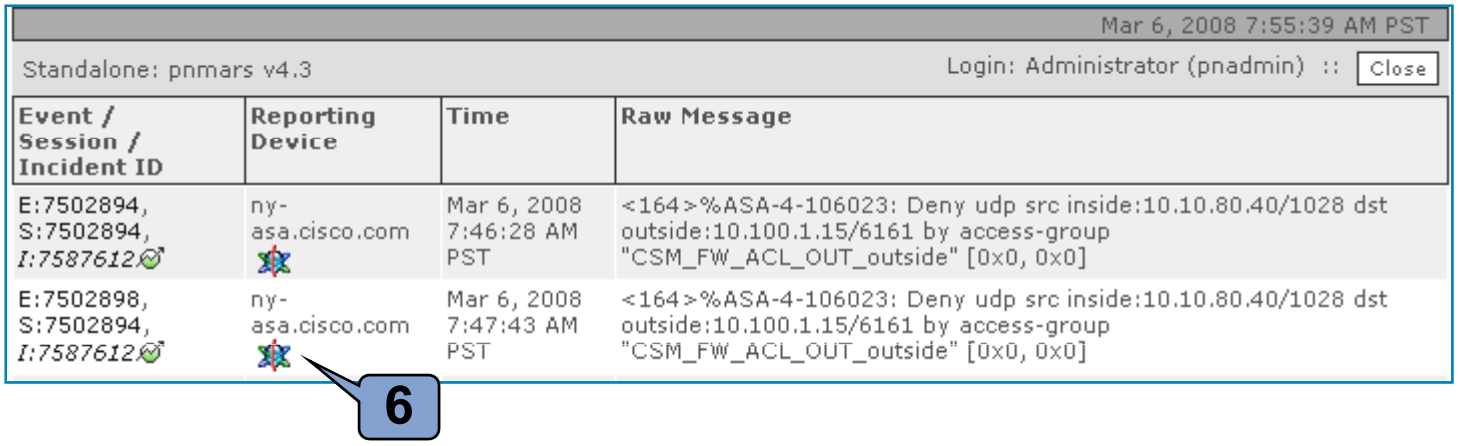


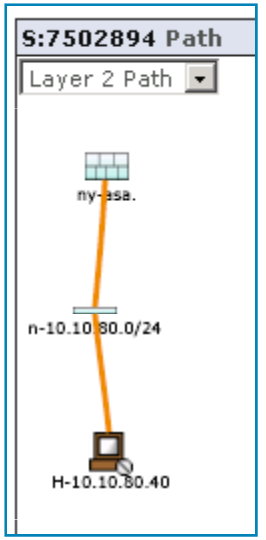
Событие с МЭ → Политика (прод.)

3. Откроется новое окно с деталями инцидента
4. Нажатие на иконку топологии покажет схему инцидента
5. Нажмите на иконку CSM для того что бы получить больше информации о устройстве и исходном сообщениимessage.



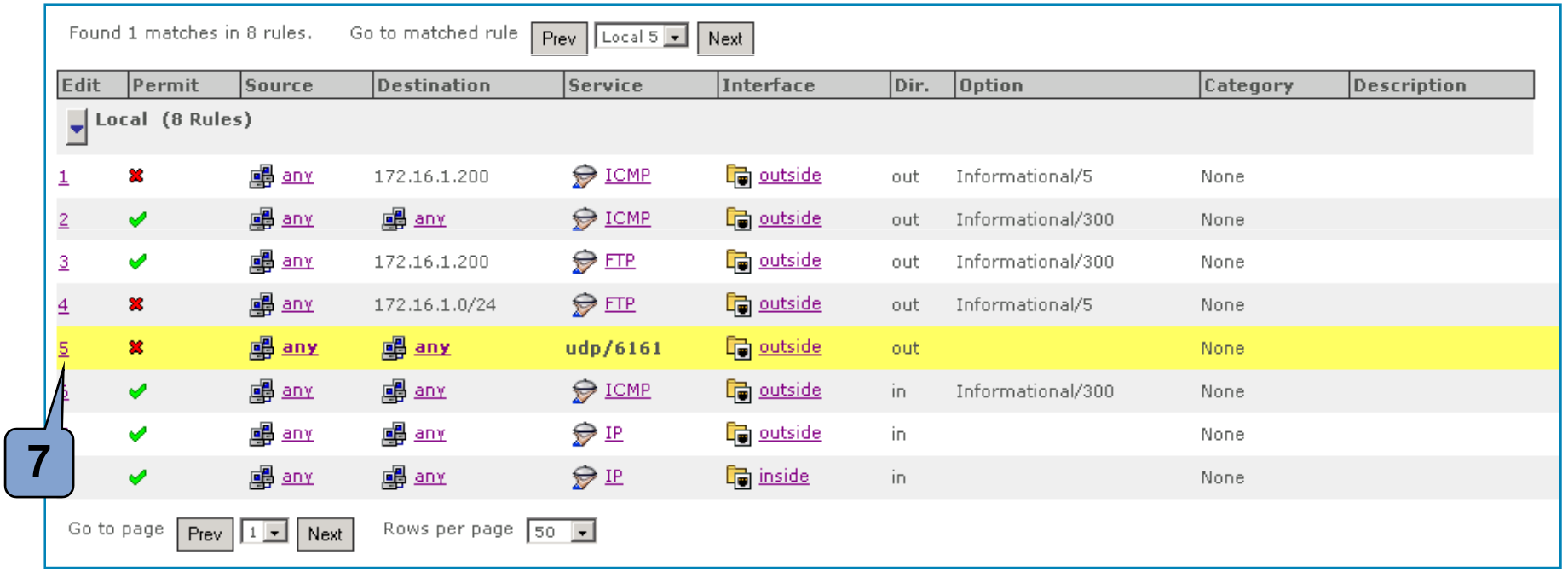
6. В окне “Raw message” нажмите иконку CSM. Это откроет таблицу правил CSM, с выделением конкретной строчкой.





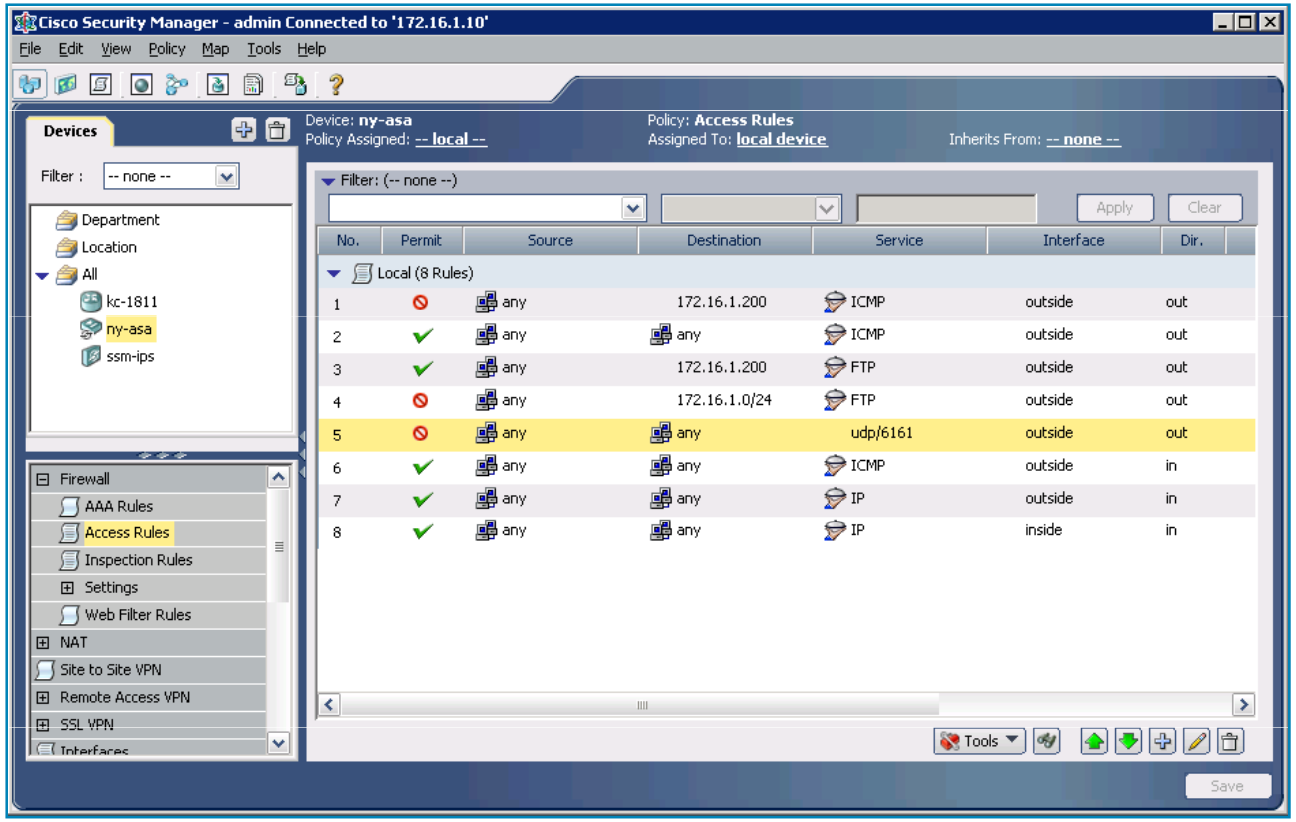
Событие с МЭ → Политика (прод.)

7. Нажатие на выделенное правило или на номер любого другого правила запустит CSM.



Событие с МЭ → Политика (прод.)

7. MARS откроет окно CSM. Пользователь будет иметь возможность редактировать политику, если имеет на это право.

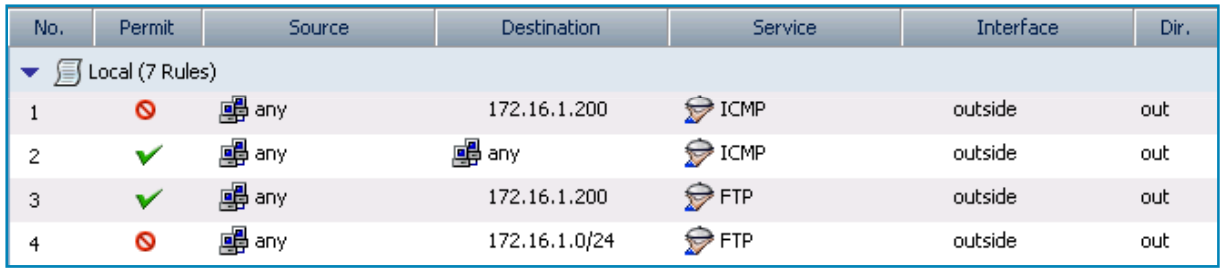


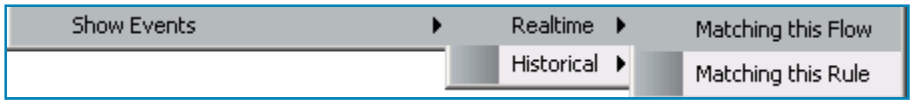
Примеры

- IPS событие → Политика
- Событие с МЭ → Политика
- Политика МЭ ASA → Событие

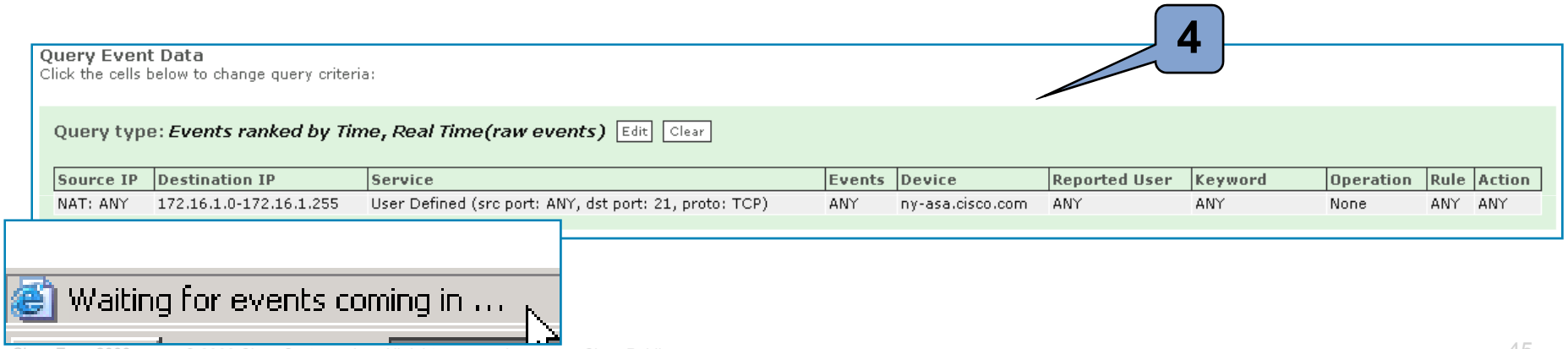
Политика МЭ ASA → Событие
В реальном времени – Match Flow

1. Выберите МЭ
2. Кликните на правило 4
3. Выберите Show Event → Real time → Matching this Flow
4. CSM откроет окно MARS с подготовленным запросом



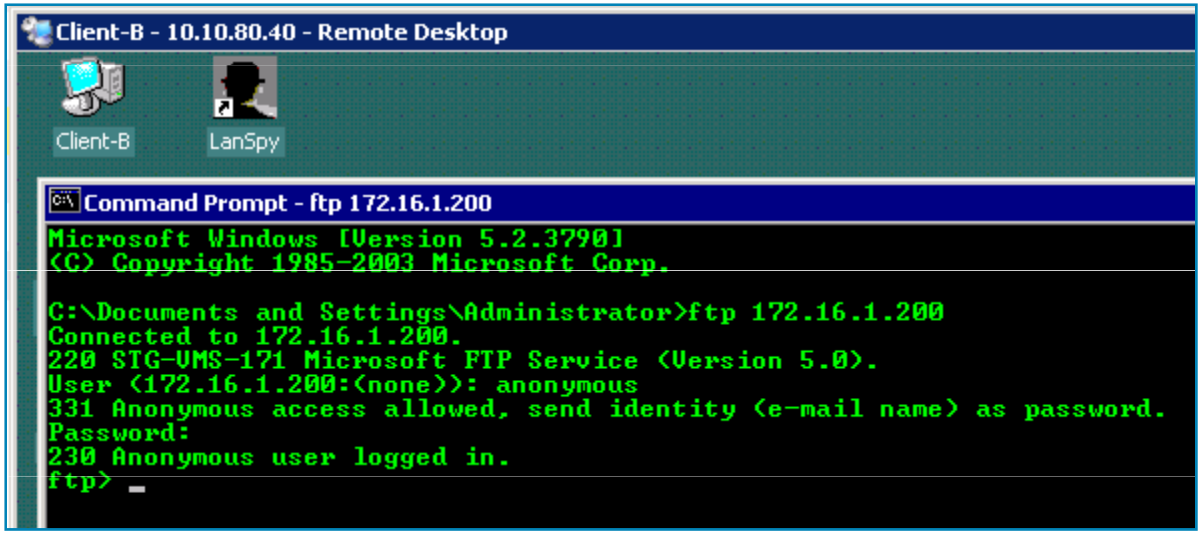


Внимание: Match Flow использует поиск по 5 параметрам (5 Tuple Match), ACE в этом случае может быть не уникальна в этом случае.



Политика МЭ ASA → Событие (прод.)
В реальном времени – Match Flow

5. Откройте консоль и запустите FTP соединения к PC (PC находится за ASA)
6. Переключитесь на MARS и просмотрите результаты



Внимание: Запрос ниже показывает результат который больше относится к правилу №3

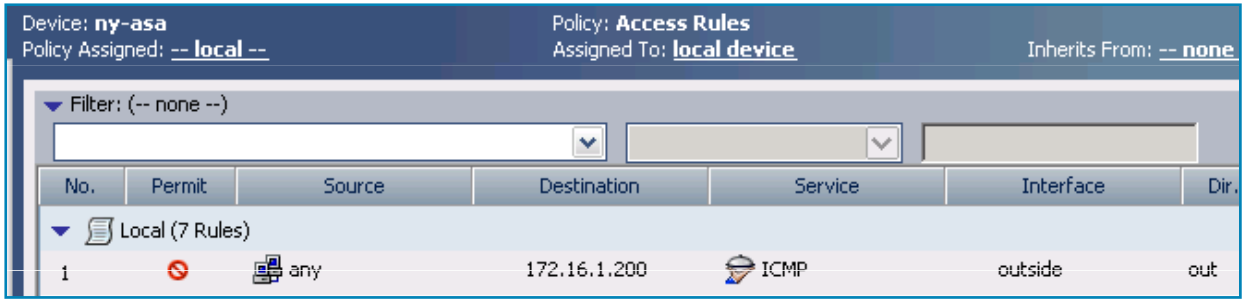
Query Results

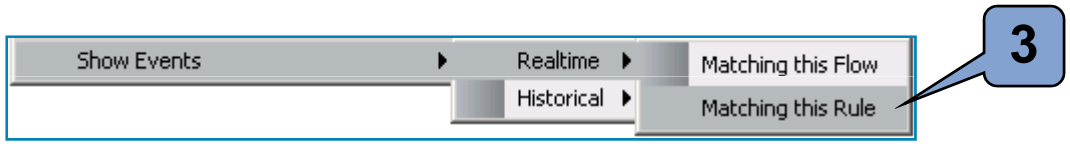
6

Event ID	Event Type	Source IP/Port		Destination IP/Port		Protocol	Time	Reporting Device
6946450	*Built/teardown/permitted IP connection*	172.16.1.80	1028	172.16.1.200	21	TCP	Mar 5, 2008 8:34:32 AM PST	*ny-asa.cisco.com*
6946451	*Built/teardown/permitted IP connection*	10.10.80.40	1490	172.16.1.200	21	TCP	Mar 5, 2008 8:34:32 AM PST	*ny-asa.cisco.com*

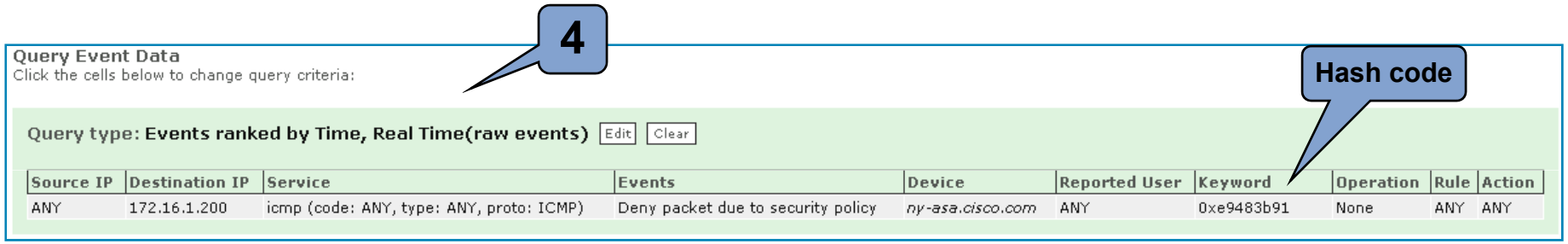
Политика МЭ ASA → Событие
В реальном времени – Match Rule

1. Выберите МЭ
2. Кликните на правиле №1
3. Выберите Show Event → Real time → Matching this Rule
4. CSM откроет окно Query на MARS



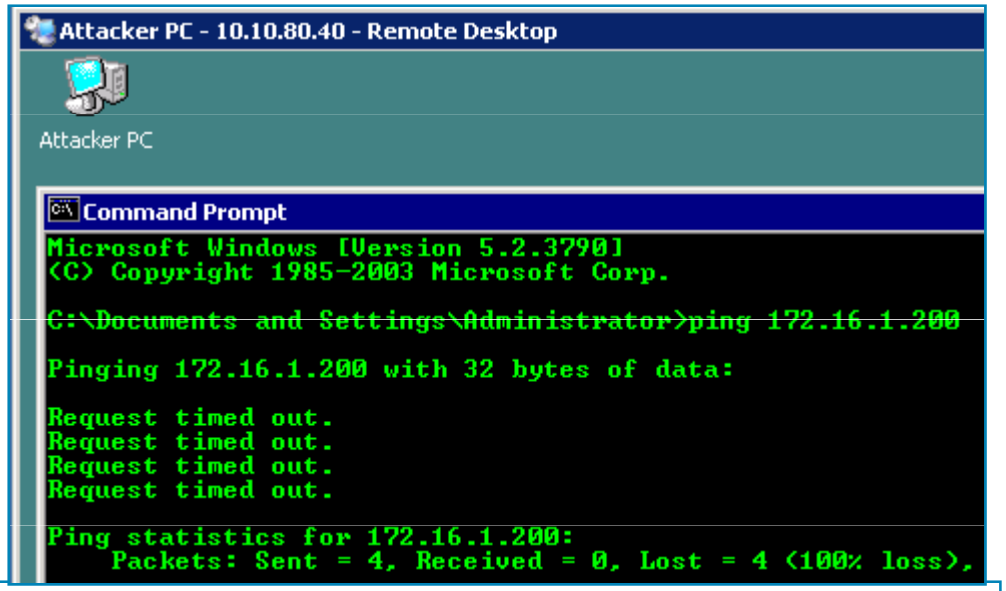


Внимание: Запрос ниже содержит Hash Code. Работает только в том случае если ACE применено на устройстве.



Политика МЭ ASA → Событие (прод.)
В реальном времени – Match Rule

5. Откройте консоль и запустите ping на PC
6. Вернитесь в окно MARS и вы должны увидеть запрос с событиями.
7. В исходном сообщении будет указан Hash code.



Query Results

7

Event ID	Event Type	Source IP/Port		Destination IP/Port		Protocol	Time	Reporting Device
7499884	*Deny packet due to security policy*	172.16.1.80	8	172.16.1.200	0	ICMP	Mar 5, 2008 2:19:52 PM PST	*ny-asa.cisco.com*

Mar 5, 2008 2:20:10 PM PST

Standalone: pnmars v4.3 — Login: Administrator (pnadmin) :: Close

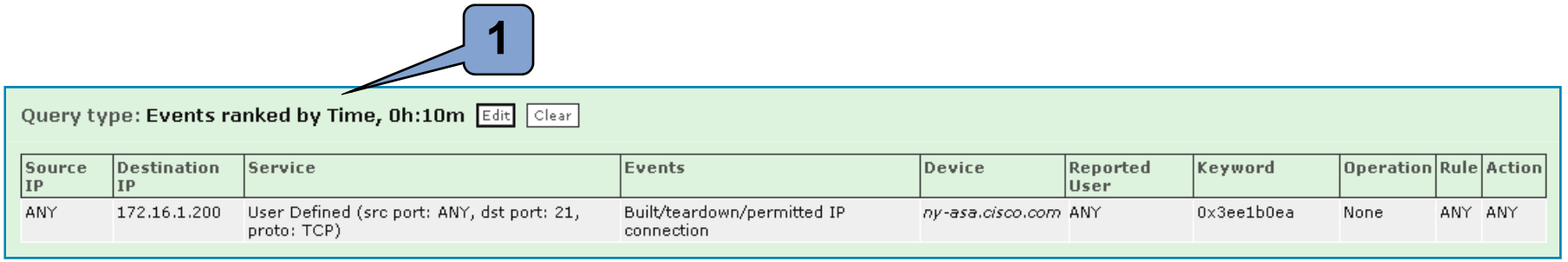
7

Event ID	Reporting Device	Time	Raw Message
7499884	ny-asa.cisco.com	Mar 5, 2008 2:19:52 PM PST	<166>%ASA-6-106100: access-list CSM_FW_ACL_OUT_outside denied icmp inside/172.16.1.80(8) -> outside/172.16.1.200(0) hit-cnt 1 first hit [0xe9483b91, 0x0]

Hash code

Политика МЭ ASA → Событие

За определенное время



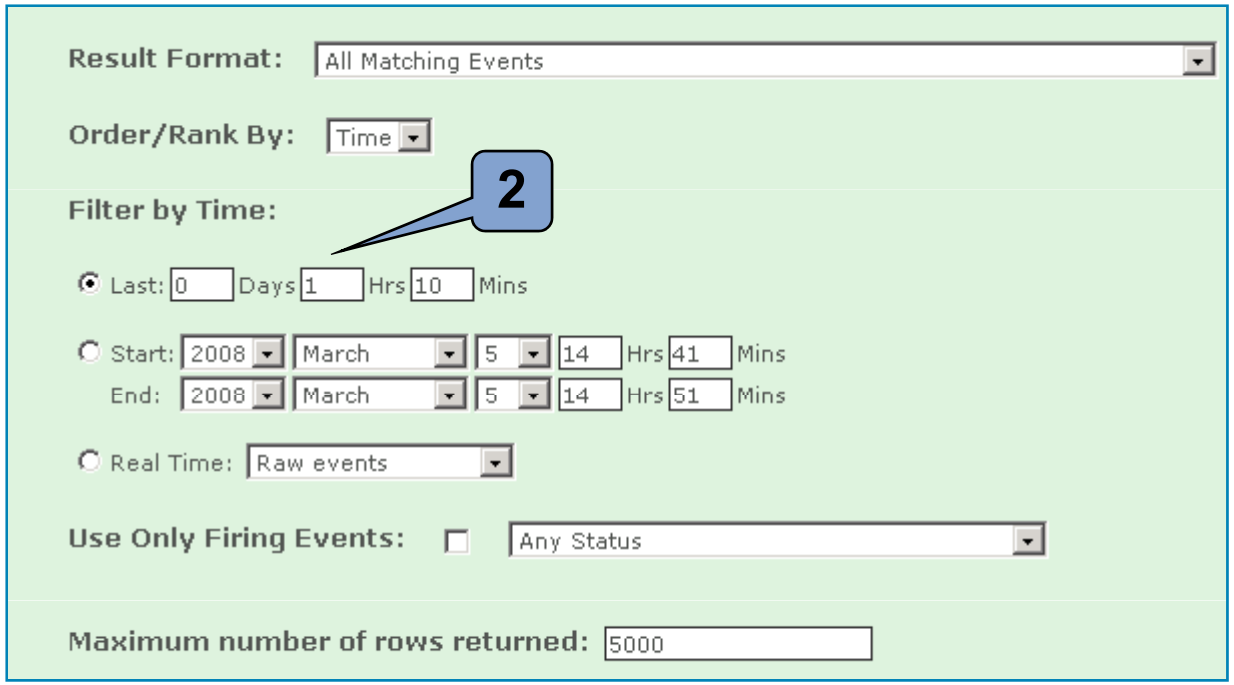
1. Выберите МЭ в CSM

   Кликните на любом правиле

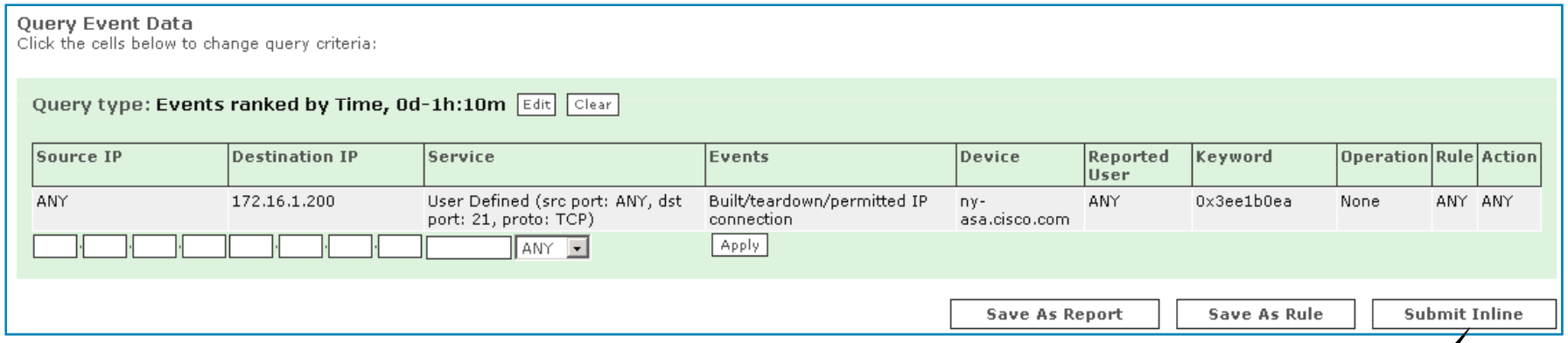
   Выберите Show Event → Historical → Matching this Rule

   CSM откроет окно MARS с типом запросом : Events ranked by time.

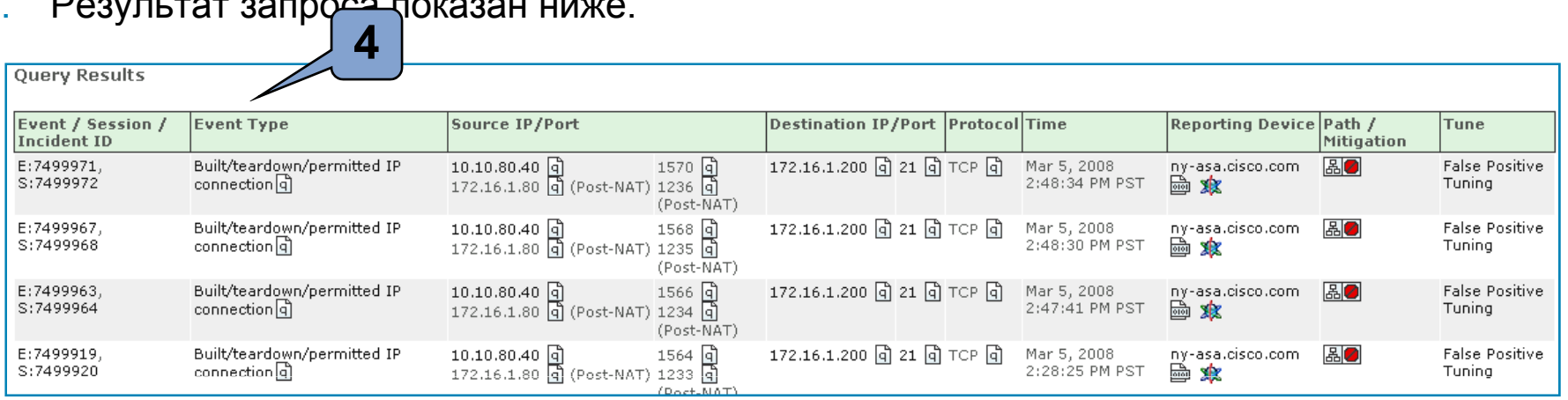
2. Укажите необходимое кол-во дней и нажмите кнопку Apply.



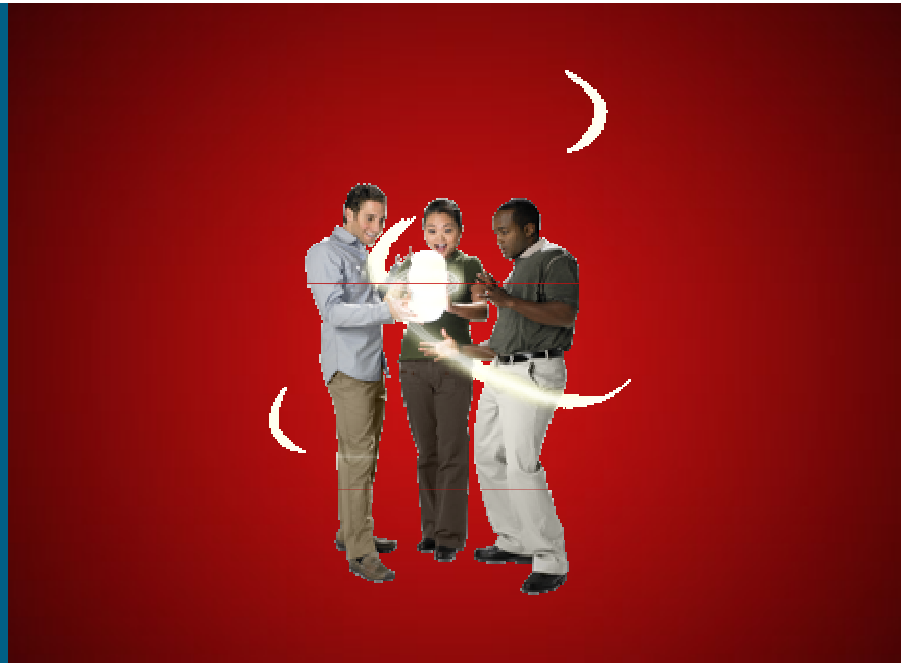
Политика МЭ ASA → Событие (прод.)
За определенное время



3. Нажмите **Submit Inline**.
4. Результат запроса показан ниже.



Cisco MARS 6.0



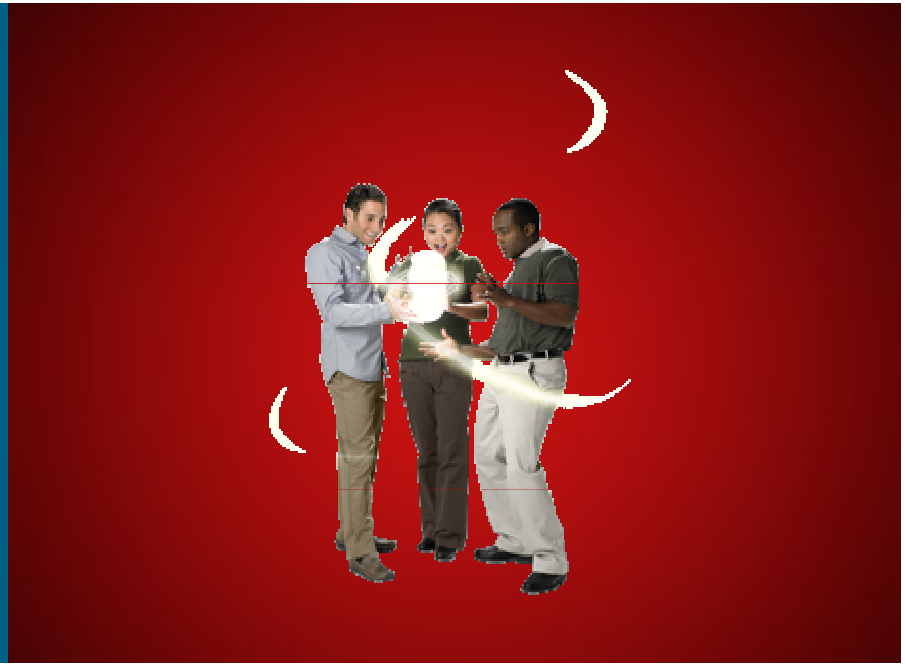
Device Support Framework (DSF)

- DSF реализует следующую функциональность:
  - **Добавляет** новые типы устройств и парсеры
  - **Предопределяет** системные парсеры
  - **Наследует** настройки существующих типов устройств
  - **Возможность импорта и экспорта**, всего выше перечисленного, включая измененные правила (rules), отчеты, и группы event type.

Другие улучшения

- Унифицированная версия ПО
- Улучшена интеграция CSM и GC MARS
- Улучшена поддержка виртуальных сенсоров Cisco IPS
- Поддержка IPS Threat Rating и Risk Rating
- Поддержка Netflow v9 (ASA 8.1)
- Поддержка новых версий устройств (ASA 8.1, CSA 6.0 и т.п.)
- Поддержку Wireless Controller

Сценарии совместного использования CSM & MARS



Терминология

- **Политика ИБ** – формализованный документ, описывающий правила доступа и контроля на сетевом уровне. Может иметь достаточно общие формулировки – например запрещать удаленный доступ.
- **Правила ИБ** – реализации **политики ИБ** в правилах CSM, которые в свою очередь транслируются в конкретные настройки для сетевых устройств и устройств ИБ. Как правило содержат более точные описания, чем **политика ИБ**, например настройка доступа к определенным сервисам для конкретного сервера.

Сценарий 1

- **Отдел ИБ**
  - **Разработка политики ИБ**
  - **Утверждение политики ИБ**
  - **Контроль выполнения политики ИБ**
  - **Расследование инцидентов ИБ**
  - **Внесение изменений в политику ИБ**
  - **Отсутствие прямого административного доступа к СЗИ**
- **Отдел ИТ**
  - **Управление сетевым оборудованием**
  - **Управление СЗИ**
  - **Применение политики ИБ в виде настроек устройств**
  - **Поддержка сетевых приложений**

Формирование новой политики ИБ

Отдел ИТ	Отдел ИБ
В данном сценарии отдел ИТ не разрабатывает политику ИБ.	**Задача:** Сформировать **политику ИБ**, учитывая уже существующие приложения, и профили трафика в сети
	Аналитики ИБ используют MARS для получения информации о протоколах, и хостах существующих и взаимодействующих в сети. Новая **политика ИБ** определяет должен ли этот сетевой обмен быть заблокирован или разрешен.
	Пример: В соответствии с best practices необходимо заблокировать протокол Telnet. Через MARS получаем список узлов использующих Telnet. Если блокирование этого трафика невозможно, то в **политике ИБ** должны быть сделаны исключения.

Реализация политики ИБ

Отдел ИТ	Отдел ИБ
Задача: Реализация **политики ИБ** на конкретных устройствах	В данном сценарии отдел ИБ не выполняет задачи по настройки устройств.
Использует CSM, что бы реализовать **политику ИБ** в виде **правил ИБ** в CSM. **Политики ИБ** могут быть также реализованы в настройках конкретных устройств СЗИ и инфраструктуры.	

Контроль реализации политики ИБ

Отдел ИТ	Отдел ИБ
Задача: Контроль настройки **политики ИБ**	**Задача:** Контроль трансляции **политики ИБ** в правила ИБ.
Использует запросы из CSM в MARS для того, что бы оценить то, как именно работает **правила ИБ**, в настоящий момент, или за определенный момент времени в прошлом.	Использует CSM для просмотра текущих **правил ИБ**. Использует доступ к GUI или CLI устройств, с разграничением доступа через ACS.
Пример: Мы изменили настройки МЭ и хотим увидеть, что трафик теперь блокируется (или разрешается). В CSM оператор выбирает новое правило, и получает выборку событий из MARS, вызванных этим правилом.	

Контроль политики ИБ в целом

Отдел ИТ	Отдел ИБ
Задача: Контроль **политики ИБ**	**Задача:** Контроль **политики ИБ**
Нарушение **политики ИБ** может быть вызвано ошибкой в ее реализации в **правилах ИБ**. На MARS могут быть настроены правила (rules) которые фактически отражают **политику ИБ**, и в случае обнаружение нарушения **политики ИБ** формируется инцидент.	Использует MARS, который контролирует, что все требования **политики ИБ** выполняются. Требуется дополнительная настройка правил, для генерации инцидентов нарушения **политики ИБ.**
Например: Необходимо обеспечить блокирование telnet. Правила в CSM (на устройстве) верны и соответствуют политике ИБ. Но была выбрана неверная точка применения – пограничный МЭ, т.к. это не блокирует протокол внутри сети. Поэтому такую ошибку можно отследить только используя MARS.	←

Поиск ошибок при реализация политики ИБ, поиск неисправностей

Отдел ИТ	Отдел ИБ
Задача: После внедрения той или иной **политики/правил ИБ** перестало работать приложение. Существует большое кол-во устройств (и их консолей), которые могли заблокировать прохождение трафика	В данном сценарии отдел ИБ не отвечает за поиск неисправностей, не связанных с инцидентами
MARS позволяет получать события о блокировании/прохождения трафика в реальном масштабе времени с различных средств СЗИ и сетевого оборудования.	
Пример: при поиске проблемы подключения АРМ к серверу БД, необходимо сделать запрос в MARS для поиска событий связанных с этой сессией, пришедших со всех устройств и приложений. Например трафик может быть блокироваться на уровне хоста (CSA), а не на уровне сети.	

Расследование инцидентов

Отдел ИТ	Отдел ИБ
Задача: Получение информации, необходимой для сопоставления проблем в ИТ с проблемами в ИБ. Например DoS атака на канал/устройство, вызывает ошибки, которые могут регистрироваться только устройствами (или на уровне) ИБ	**Задача:** Повседневный анализ текущих инцидентов, расследования, подавление угроз, устранение последствий атак.
Использует режим просмотра инцидентов, просмотра готовых отчетов, просмотра сетевой статистики, и консоли с выводом сообщений определенных типов.	Используют MARS, для аналитической работы над автоматическими отобранными инцидентами. Используют запросы к БД MARS.
Пример: При поиске неисправностей с IP телефонией, администратор проверят текущие инциденты ИБ, что бы найти факторы, которые могли оказать влияние на функционирование IPT (например DoS атаки на устройства IPT или каналы связи).	

Расследование инцидентов

Определение связи между инцидентами и конкретными политиками

Отдел ИТ	Отдел ИБ
В данном сценарии отдел ИТ не отвечает за расследование инцидентов	**Задача:** Определение связи между инцидентами и конкретными **политиками/правилами ИБ**.
	Используют MARS для связи событий, входящих в инциденты ,с текущими правилами/политикой ИБ через CSM.
	Пример: Есть возможность получения информации, какая именно строчка **правил ИБ** вызвала события повлекшие инцидент. В правилах CSM могут быть использованы комментарии для установки связи между **правилами ИБ** и **политиками ИБ**, например номер параграфа политики ИБ, где описаны требования по наличию подобного правила. Может использоваться ссылка на систему управления изменениями (change management).

Расследование инцидентов

Визуализация топологии

Отдел ИТ	Отдел ИБ
В данном сценарии отдел ИТ не отвечает за расследование инцидентов	**Задача:** Обеспечить построение актуальной сетевой топологии для визуализации векторов атаки
	В случае отсутствия специализированных утилит для построения топологий сети, MARS может визуализировать топологию сети, с показом устройств вовлеченных в конкретный инцидент.

Расследование инцидентов

Эскалация инцидентов

Отдел ИТ	Отдел ИБ
В данном сценарии отдел ИТ не отвечает за расследование и эскалацию инцидентов.	**Задача:** эскалировать инциденты, в случае необходимости взаимодействия с другими подразделениями.
	MARS с помощью XML может передавать информацию о инцидентах в такие системы как Remedy и HP Service Desk

Внесение изменений в политику ИБ и правила ИБ

Отдел ИТ	Отдел ИБ
В данном сценарии отдел ИТ не изменяет **политику ИБ**, и не инициирует изменения в **правила ИБ**.	**Задача:** В результатах расследования внести изменения в **политику ИБ** и/или **правила ИБ**.
Получив заявку от отдела ИБ, в CSM вносятся соответствующие изменения. Есть возможность контроля сделанных изменений, возможность отката. Дополнительно можно указать в дополнительных полях в правилах CSM причину, по которой были изменены или добавлены строки правил.	Формируется заявка, передаваемая на исполнение в Отдел ИТ.

Содействие проведению аудиту

Отдел ИТ	Отдел ИБ
Задача: Предоставить аудитору подтверждения выполнении тех или иных требований	**Задача:** Предоставить аудитору подтверждения выполнении тех или иных требований
Используют MARS для быстрой выборки из базы событий необходимой информации. Использование готовых отчетов.	Используют MARS для быстрой выборки из базы событий необходимой информации. Использование готовых отчетов.
Пример: При проведение аудитов по стандартам серии **ISO 9000** (управление качеством) требуется подтверждение наличия и работоспособности СЗИ для защиты данных клиентов. Помощь в проведение аудитов по стандарту **COBIT**.	**Пример:** Помощь в проведение аудитов по стандартам **ISO 27001**, **PCI DSS** и т.п.

Единая консоль сообщений

Отдел ИТ	Отдел ИБ
Задача: Обеспечить сбор сообщений с различных устройств по протоколу Syslog	
MARS является единой консолью, которая объединяет не только СЗИ но и сетевое оборудование. Используются различные протоколы для сбора информации, в том числе Syslog и SNMP. Возможно подключения принципиально новых устройств.	

Аналитика

Отдел ИТ	Отдел ИБ
Задача:	**Задача:** Прогнозирование изменений кол-ва угроз, кол-во инцидентов
	Используются отчеты и запросы в MARS за необходимый период времени

Анализ статистики Netflow

Отдел ИТ	Отдел ИБ
Задача: Обеспечить анализ статистики **Netflow**	**Задача:** Обеспечить анализ статистики **Netflow**
MARS обеспечивает сбор статистики **NetFlow**, которая может использоваться для формирования отчетов, и поиска аномалий.	Используют **NetFlow** для создания профиля нормального поведения сети. В случае детектирования аномалий, создается инцидент. В этот момент автоматически сохраняется информация о передаваемом трафике (можно включить постоянно).

Сценарий 2
Что меняется?

- **Отдел ИБ**
  - **Разработка политики ИБ**
  - **Утверждение политики ИБ**
  - **Контроль выполнения политики ИБ**
  - **Расследование инцидентов ИБ**
  - **Внесение изменений в политику ИБ**
  - ***Управление СЗИ***
  - ***Применение политики ИБ в виде настроек устройств***
  - ***Отсутствие прямого административного доступа к сетевому оборудованию***
- **Отдел ИТ**
  - ***Отсутствие прямого административного доступа к СЗИ***
  - **Управление сетевым оборудованием**
  - **Поддержка сетевых приложений**

Получение информации о событиях с устройств под чужим управлением

Отдел ИТ	Отдел ИБ
Задача: Представлять себе текущие инциденты, для уточнения влияния СЗИ на функционирование сети	**Задача:** Представлять общую картину развития инцидентов в сети, используя информацию с инфраструктурного оборудования
Используют MARS. Поддерживаются различные типы сообщений http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/user/guide/combo/appDsfEventTypeGroup.html Ошибки конфигурации, перегрузка устройств, ошибки на интерфейсах, атаки DoS, и DDoS, поиск ошибок при настройке политик доступа (блокирование СЗИ легитимного трафика)	Используют MARS. Поддерживаются различные типы сообщений http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/user/guide/combo/appDsfEventTypeGroup.html Ошибки аутентификации, изменение конфигураций, блокирование трафика и т.п.

Внесение изменений в политику ИБ и правила ИБ

Отдел ИТ	Отдел ИБ
Задача: Внесение настроек в сетевые устройства	**Задача:** В результатах расследования внести изменения в **политику ИБ** и/или **правила ИБ**.
Используют CSM для изменения настроек связанных с безопасность на инфраструктурном оборудовании. Доступ к оборудованию СЗИ блокируется ролевым доступом в CSM, с интеграцией с ACS.	Используют MARS для быстрого перехода в настройки **политики ИБ** в CSM. В случае наличия доступа можно вносить изменения. Если доступ в CSM ограниченный, то создается заявка в Отдел ИТ для внесения изменения в **правила ИБ**.

Дополнительная информация

- **Cisco Security Center**

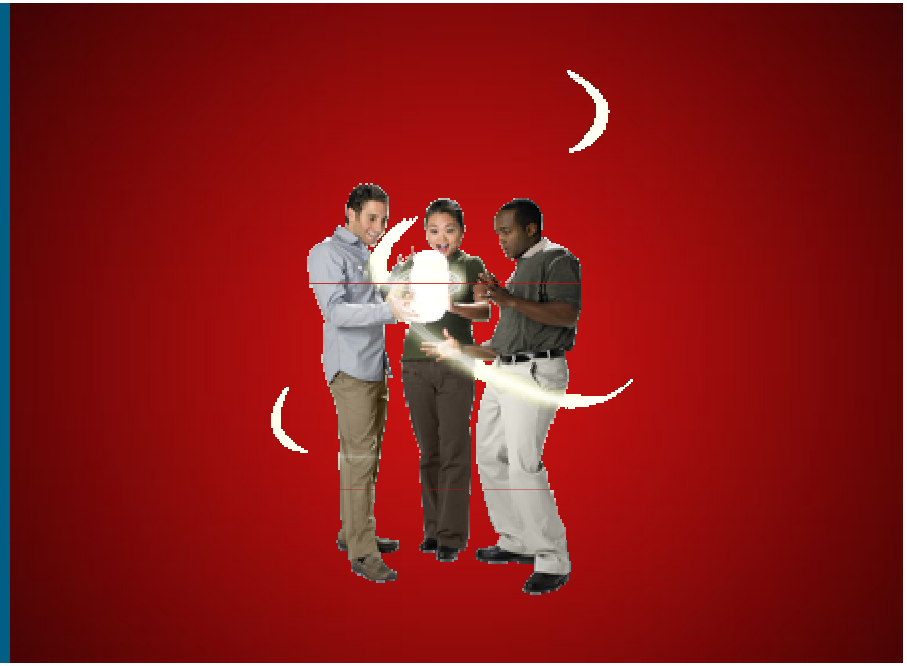
  www.cisco.com/security

- **Security Threat Mitigation (STM) Task Flow Overview**

  http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/user/guide/combo/taskFlow.html

- **NIST sp800-61, ISO/IEC 18044, и т.п.**

Вопросы?



Дополнительные вопросы Вы можете задать по электронной почте security-request@cisco.com