POSITIVE TECHNOLOGIES

ЗАО «ПОЗИТИВ ТЕКНОЛОДЖИЗ»
107061, МОСКВА, ПРЕОБРАЖЕНСКАЯ ПЛ., Д. 8
ТЕЛ. +7 495 744-01-44, ФАКС +7 495 744-01-87, PT@PTSECURITY.COM
PTSECURITY.RU, MAXPATROL.RU, SECURITYLAB.RU

# MAXPATROL SIEM

## РУКОВОДСТВО АДМИНИСТРАТОРА

11.0

# ОГЛАВЛЕНИЕ

# 1. Установка и развертывание

## 1.1. Архитектура и состав системы

Система MaxPatrol SIEM состоит из нескольких компонентов, что позволяет обеспечить масштабирование и внедрять систему в компаниях любого размера. Эти компоненты можно разместить как на одном сервере, так и на нескольких. Для продуктивных систем рекомендуется распределенная установка.

Основным компонентом системы является управляющий сервер MPX Core. Он устанавливается в центральном офисе компании или в крупных территориальных и функциональных подразделениях. MPX Core выполняет функции:

- централизованного хранения конфигурации активов;
- централизованного управления всеми компонентами системы;
- оперативного реагирования на инциденты информационной безопасности (ИБ) и обеспечения взаимодействия подразделений организации при расследовании этих инцидентов;
- автоматизации процесса управления уязвимостями.

MPX Core осуществляет обработку данных. На нем установлен веб-интерфейс системы. К одному такому компоненту можно подключать произвольное количество модулей, включая другие управляющие серверы. Это позволяет увеличивать производительность, учитывать при сканировании топологию сети и типы каналов связи (например, наличие межсетевых экранов или других средств защиты).

Компонент MPX SIEM осуществляет основные функции по обработке и хранению событий:

- централизованное хранение информации о событиях и сетевом трафике;
- агрегацию, фильтрацию, нормализацию и корреляцию событий,
- автоматическое создание инцидентов,
- привязку событий к активам.

Модульная платформа (компонент MPX Agent) предназначена для сканирования активов системы в режиме черного и белого ящиков. Этот модуль позволяет быстро обнаружить узлы и их открытые сетевые сервисы и провести специализированные проверки в режиме теста на проникновение. MPX Agent в режиме активного и пассивного сканирования собирает информацию об активах: название, версию и производителя операционной системы (ОС), установленные обновления ОС, список установленного программного обеспечения (ПО), настройки ОС и ПО, учетные записи пользователей и их привилегии, данные об аппаратном обеспечении, запущенных сетевых сервисах и службах ОС, настройках сети и средств защиты.

MPX Agent предназначен для сбора событий от различных источников и имеет модульную структуру, что позволяет осуществлять активный и пассивный сбор событий, а также подключать дополнительные модули, в том числе разработанные заказчиком. Реализованы следующие модули для сбора событий[1]:

1. Набор модулей постоянно пополняется. Обратитесь в службу технической поддержки Positive Technologies, чтобы получить полный актуальный список.

- модуль Syslog — сбор событий по протоколу Syslog;
- модуль Windows Event Log — активный сбор событий Windows Event log;
- модуль Windows File log — активный сбор событий из файлов Microsoft Windows;
- модуль Windows WMI log — пассивный сбор событий Microsoft Windows;
- модуль NetFlow — сбор событий по протоколу NetFlow;
- модуль ODBC Log — сбор событий из таблиц СУБД;
- модуль Checkpoint LEA;
- модуль SNMP Traps;
- модуль SSH File Log — сбор событий из файлов по протоколу SSH.

Компонент MPX Agent управляет указанными модулями, обеспечивает мониторинг их состояния и передачу данных между модулями и сервером.

Кроме указанных функций, компонент MPX Agent осуществляет сбор данных, которые используются модулем MPX Core для расчета уязвимостей активов.

Модульная платформа MPX Agent может выполнять транспортную функцию, играя роль шлюза — MPX Gate, который отвечает за передачу информации между компонентами системы по защищенному каналу связи. Кроме данных, шлюз передает команды от сервера остальным модулям и сообщения о состоянии того или иного процесса в обратную сторону.

Для централизованного обновления всех компонентов MPX Agent используется выделенный сервис компонента MPX Core. Обновления можно загружать на сервер как из сети Интернет, так и с помощью внешних накопителей. Такая схема позволяет обновлять компоненты, расположенные в изолированных сегментах сети или в сетях с ограниченным доступом к интернету, а также снижает объем сетевого трафика при масштабном обновлении.

## 1.2. Логическая схема взаимодействия компонентов

Рассмотрим примерную схему взаимодействия компонентов системы.

Модульная платформа MPX Agent собирает данные от источников событий и сканирует сети. Данные передаются на сервер MPX Server для хранения и обработки. События, полученные через MPX Agent, передаются компоненту MPX SIEM для нормализации и корреляции. Кроме того, используя полученные данные компонент MPX Core рассчитывает уязвимости активов системы. Пользователь подключается к серверу через веб-интерфейс, чтобы управлять системой, просматривать данные, строить отчеты и выполнять мониторинг системы MaxPatrol SIEM.

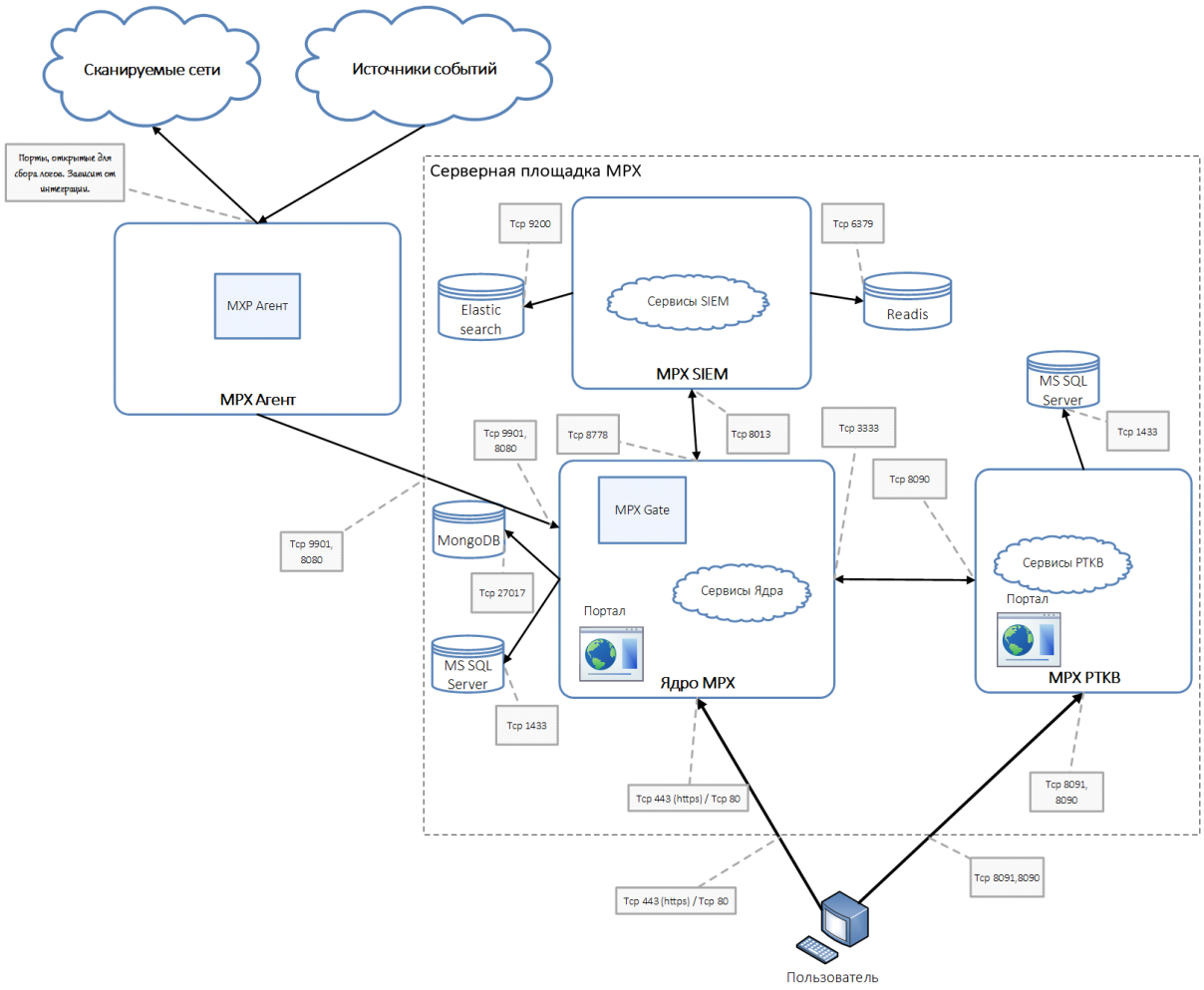
Компонент MPX PTKB управляет базой знаний, которая хранится в Microsoft SQL Server и включает в себя данные, необходимые системе MaxPatrol SIEM для структурирования сведений, собранных от источников событий и объектов инфраструктуры (например, для определения версий ОС, ПО, служб, типа аппаратного обеспечения), а также для обнаружения уязвимостей.

Компонент MPX SIEM обрабатывает входящий поток событий, которые приводятся к единому формату (нормализуются). Затем выполняется корреляция этих событий по

заданным правилам. В результате этого процесса поток событий может обогатиться новыми событиями (полученными в результате действия правил корреляции). Поступающие события хранятся в исходном и в нормализованным виде в базе данных (БД) Elasticsearch.

Серверный компонент MPX Core собирает, обрабатывает и хранит результаты сканирования объектов инфраструктуры с подробной информацией об обнаруженных ОС, ПО, службах, портах и пр., обнаруженные между ними связи. Кроме того, этот компонент сохраняет настройки заданий сбора данных, пользовательские учетные записи, профили сканирования, справочники и пр. Компонент MPX Core осуществляет контроль доступа к данным, связываясь с прочими компонентами системы для выполнения пользовательских запросов. Использует БД MongoDB и Microsoft SQL Server.

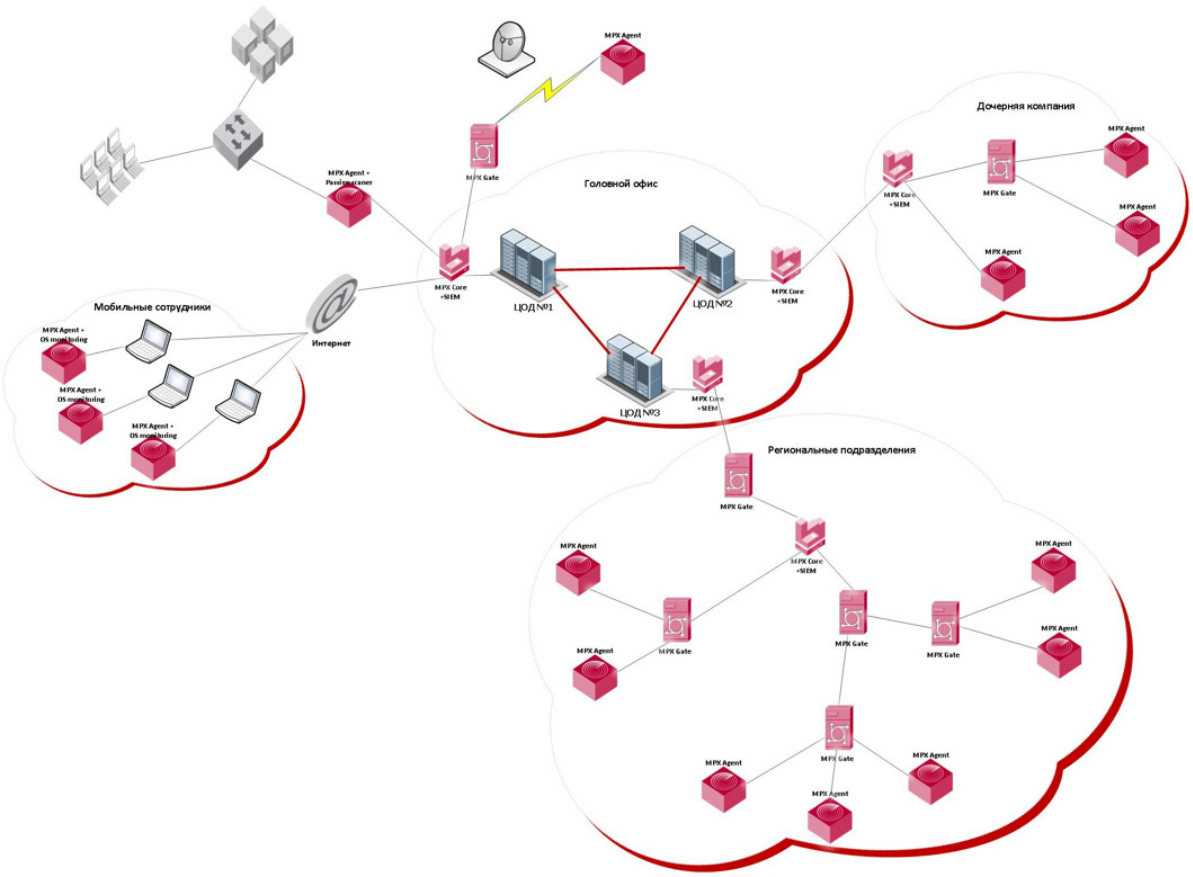
Компоненты MPX Core и MPX SIEM являются серверными и совместно образуются логическую единицу MPX Server — сервер системы.




# 1.3. Пример развертывания MaxPatrol SIEM

Рассмотрим пример внедрения MaxPatrol SIEM в распределенной сети со сложной структурой управления. В крупной компании с множеством региональных подразделений или дочерних организаций сотрудники на местах используют для обеспечения безопасности результаты сканирования и обработки событий в локальных компонентах MPX SIEM и MPX Server. Головной компонент PT SIEM ведет общий учет и обеспечивает централизованную отчетность. Для этого модульные платформы MPX Agent в подразделениях передают данные в головной офис на консолидацию.

Пример подобной конфигурации приведен ниже.ц



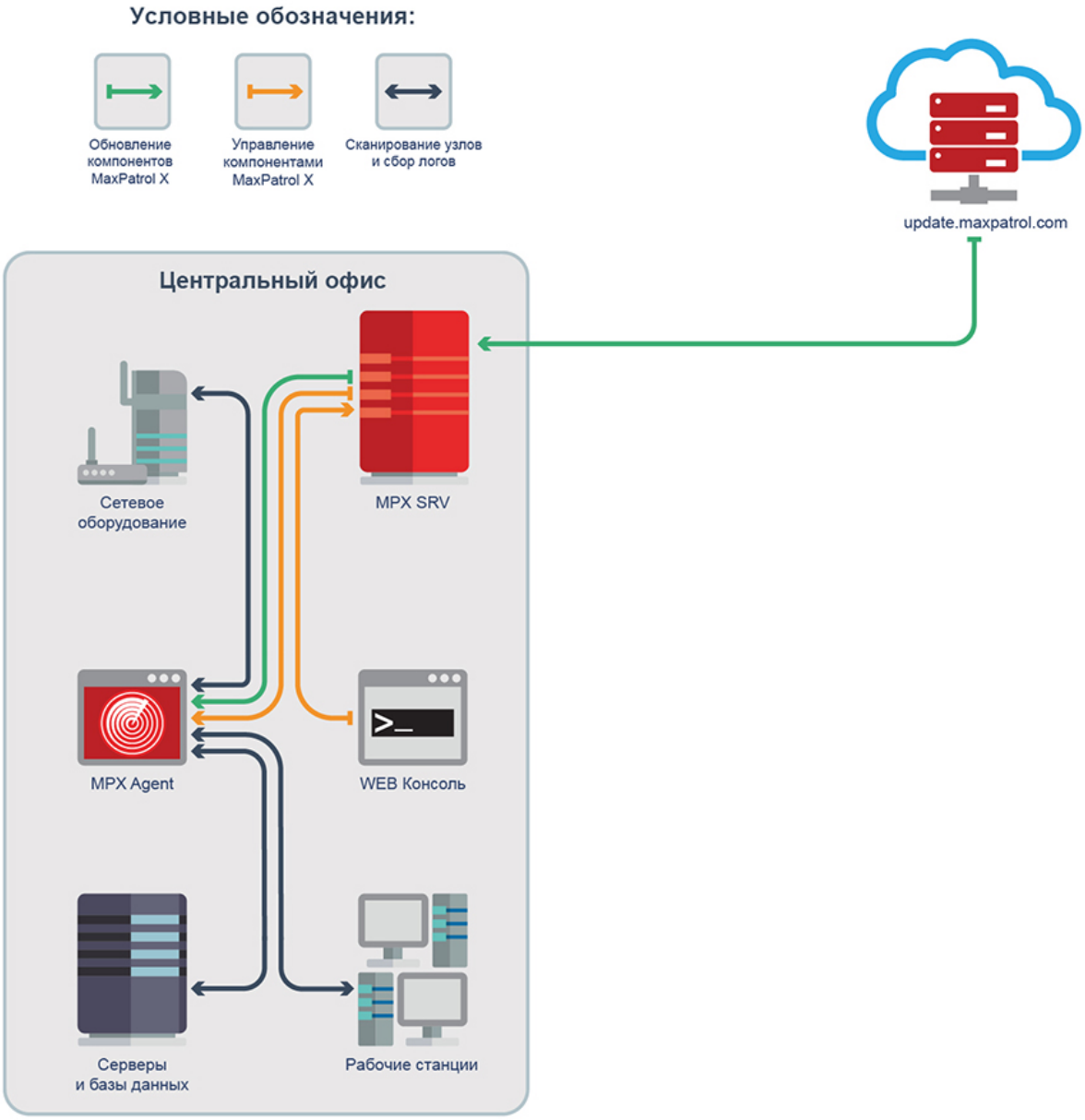

Далее рассмотрим варианты развертывания системы MaxPatrol SIEM и основные подходы к проектированию.

### 1.3.1. Минимальная конфигурация (единственный офис)

Минимальный вариант развертывания системы предполагает установку одного сервера MPX Server (состоящего из MPX Core и MPX SIEM), агентов активного и пассивного сбора событий и консоли управления. Эти компоненты размещаются в центральном офисе.

Сценарий актуален, если:

- обеспечена производительность для сборщика записей журналов событий ИБ,
- в организации не более 3000 сетевых узлов,
- сканирование производится не чаще 1 раза в месяц,
- узлы расположены на одной площадке,
- все узлы доступны по локальной сети.




При таком варианте планирование и предварительное проектирование с точки зрения размещения компонентов MaxPatrol SIEM практически не требуется. Аппаратные требования совпадают с рекомендуемыми.

Необходимый размер хранилища рассчитывается с учетом:

- срока хранения данных в системе;
- количества и типа источников событий;
- количества объектов и частоты сканирования с использованием network scanner.

Поскольку все компоненты MaxPatrol SIEM размещаются в пределах центрального офиса с наличием локальной сети, то ширина полосы пропускания каналов связи не имеет значения.

Для обеспечения сетевого взаимодействия компонентов MaxPatrol SIEM должны быть доступны следующие порты.

Таблица 1.

| Компоненты взаимодействия | Номера портов |
|---|---|
| MPX Agent – MPX Core | TCP 9901, 8080 |
| MPX SIEM – Elasticsearch | |
| MPX Core – Microsoft SQL Server | TCP 1433 |
| MPX Core – MongoDB | TCP 27017 |
| MPX Core – MPX SIEM | TCP 8013, 8778 |
| Console – MPX Core | TCP 80, 443 |

### 1.3.2. Конфигурация с несколькими агентами (несколько офисов)

Конфигурация с несколькими агентами сбора событий может использоваться при развертывании MaxPatrol SIEM в сетях среднего размера, когда требуется обеспечить сбор событий ИБ от источников в удаленных сегментах сети. Как правило, это территориально обособленный филиал, отделенный межсетевым экраном.

Для сбора событий ИБ из удаленных сегментов можно использовать компоненты MPX Agent, установленные в центральном офисе и или на удаленной площадке.

Рекомендуется устанавливать MPX Agent в центральном офисе, если:

- количество событий от удаленных источников незначительно,
- канал между центральным офисом и удаленной площадкой имеет большую пропускную способность (не менее 3 Мбит/с),
- есть возможность обеспечить сетевое взаимодействие MPX Agent со всеми источниками событий.

В остальных случаях рекомендуется устанавливать компонент MPX Agent на удаленной площадке.

Таким образом необходимость использования нескольких компонентов MPX Agent определяется следующими условиями:

- необходимо проводить сбор событий ИБ и сканирование большого количества узлов (масштабирование),
- сеть, в которой находятся сканируемые узлы, соединена с MPX Agent каналами связи с низкой пропускной способностью (требования пропускной способности),
- особенности физической или логической топологии требуют размещать компоненты MPX Agent в определенных сетевых сегментах; типичные причины: вынос управляющих интерфейсов в отдельную виртуальную сеть (VLAN) или использование средств защиты информации (требования топологии).

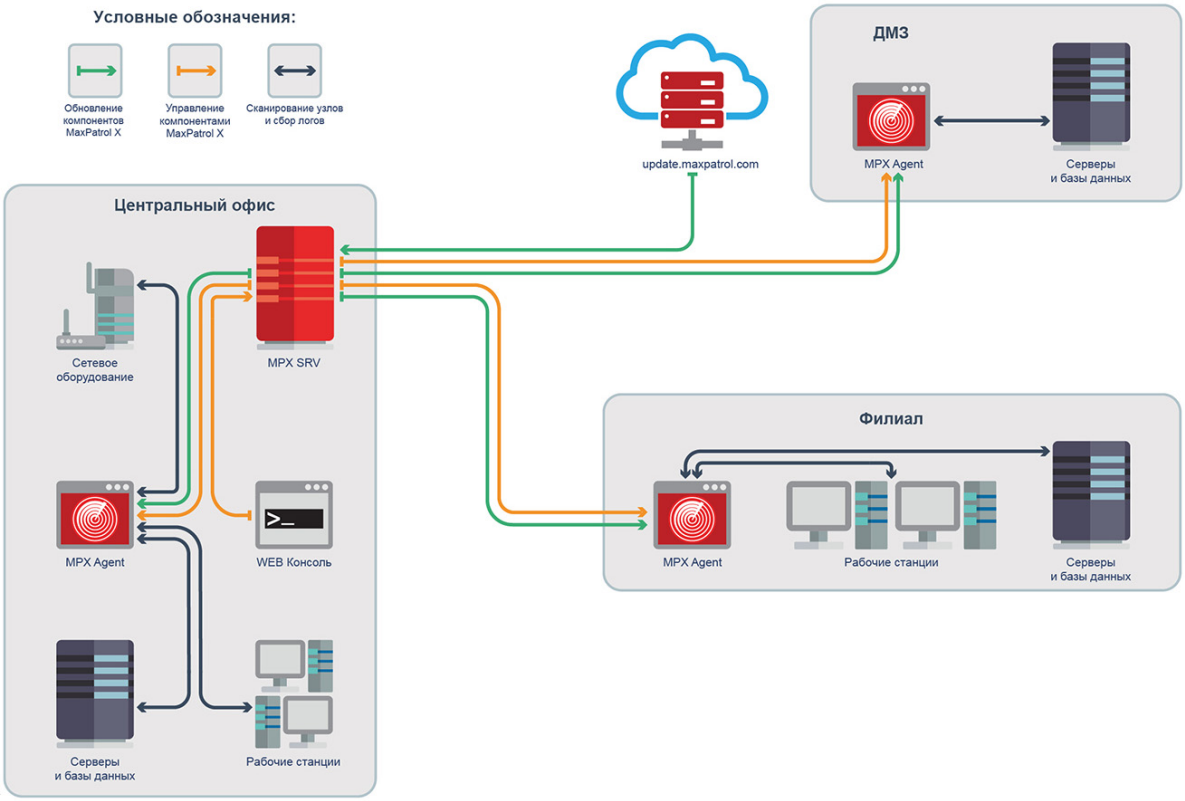
Типовым случаем является такая конфигурация: в филиале, который связан с центральным офисом каналом связи с низкой пропускной способностью или каналом, который уже загружен трафиком других приложений, устанавливается MPX Agent, который подключается к серверу в головном офисе. Кроме того, дополнительные

компоненты MPX Agent устанавливаются в ДМЗ, если невозможно обеспечить взаимодействие сервера в центральном офисе и узлами в ДМЗ напрямую.

Такой сценарий развертывания MaxPatrol SIEM актуален в случае, если:

- для обработки количества событий, поступающих на сервер MaxPatrol SRV достаточно одного компонента MPX Server,
- требования безопасности и показатели пропускной способности каналов связи не позволяют размещать компоненты MaxPatrol SIEM локально,
- производительность, обеспечиваемая одним компонентом MPX Agent, недостаточна для сбора событий ИБ и сканирования,
- общее количество сетевых узлов не более 3000 в случае использования Microsoft SQL Server Express,
- сканирование производится чаще одного раза в месяц,
- узлы, с которых производится сбор событий ИБ и сканирование, расположены на разных площадках,
- все узлы доступны по локальной сети.

Пример такой конфигурации приведен ниже.



### 1.3.3. Конфигурация с несколькими серверами и агентами (центральный офис и дополнительные офисы разных размеров)

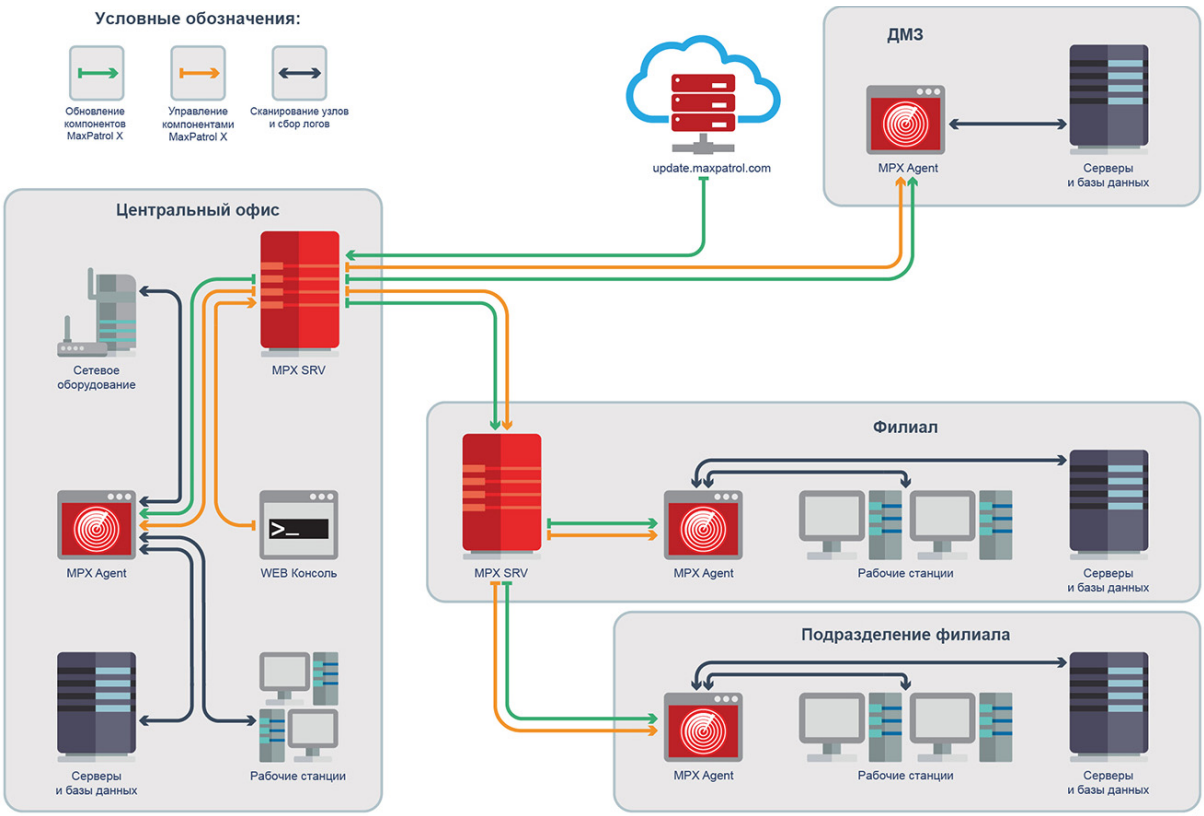
В случае масштабных внедрений существует возможность выстраивать цепочку серверов MPX Server. Использование такой архитектуры может понадобиться для распределенных сетей, имеющих сложную структуру управления. Например, если используется трехуровневая структура Головной офис – Филиал – Подразделение, и в рамках каждого подразделения функционирует собственная служба ИБ.

Сотрудникам филиала нужно иметь централизованный доступ к результатам работы MaxPatrol SIEM во всех подразделениях филиала, поэтому в филиале устанавливается собственный сервер MPX Server. Этот сервер передает результаты работы вышестоящему серверу в иерархической цепочке, что обеспечивает консолидацию данных, централизованную отчетность и мониторинг ИБ в рамках всей компании. Такой вариант обладает максимальной гибкостью с точки зрения масштабирования, управления и разграничения доступа.

Например, этот вариант развертывания применяется, если региональные подразделения ИБ полностью самостоятельны, и в задачи центра входит только функция контроля результатов сканирования. В этом случае все функции по управлению сбором событий и сканированием реализуются на базе компонентов MPX Server, расположенных в филиалах. При этом строится иерархия компонентов MPX Server, в которой все данные консолидируются на одном выделенном MPX Server (обычно такой выделенный сервер располагаются в центральном офисе).

Обратной стороной гибкости в данном случае является необходимость учета дополнительных переменных при планировании развертывания — так, например, требуется предусмотреть требования к хранилищам для всех компонентов MPX Server, расположенных в центральном офисе и на удаленных площадках

Пример подобной конфигурации приведен ниже.




# 1.4. Установка компонентов в ОС Windows

До начала установки убедитесь, что ваша система соответствует требованиям, предъявляемым к программному и аппаратному обеспечению, указанным в главе *Системные требования*.

Комплект для установки системы MaxPatrol SIEM состоит из трех дистрибутивов:

- MPX Core (включает в себя компонент MPX Core и базу знаний),
- MPX SIEM (модуль нормализации, консолидации и корреляции данных),
- модульная платформа MPX Agent (активный и пассивный сбор данных от источников).

Названия дистрибутивов имеют следующий вид:

```
MPX<Название компонента>Setup_<номер версии>_<локаль>.
```

Например, MPXAgentSetup_7.0.0_ru-RU.

Для установки компонентов MaxPatrol SIEM рекомендуется использовать отдельные экземпляры операционных систем. В процессе установки может потребоваться перезагрузка операционной системы.

Все компоненты MaxPatrol SIEM можно устанавливать, настраивать и запускать в произвольном порядке.

Компоненты MPX Core и MPX SIEM в качестве шины для передачи данных используют платформу RabbitMQ (rabbitmq.com), которая устанавливается автоматически с каждым из них.

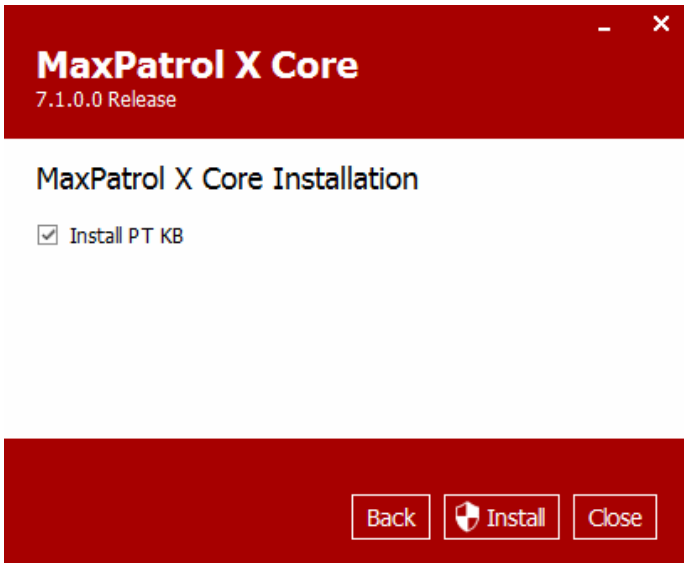
### 1.4.1. Установка компонента MPX Core

Для установки компонента MPX Core используется дистрибутив

```
MPXCoreSetup_<номер версии>.exe
```

После запуска дистрибутива пользователь видит окно со ссылкой на текст лицензионного соглашения, с которым следует внимательно ознакомиться. Чтобы продолжить установку, необходимо принять лицензионное соглашение.


Далее пользователь выбирает, следует ли вместе с компонентом MPX Core установить базу знаний. Для этого требуется выбрать или отключить соответствующую опцию.



Далее запускается процесс установки с выбранными опциями. Если в процессе установки требуется перезагрузить операционную систему, то пользователь получит соответствующее уведомление.

Если пользователь отказывается от перезагрузки, то для продолжения установки перезагрузку следует выполнить позже, а затем заново запустить программу-установщик.

Если перезагрузка выполняется сразу, то установка будет продолжена автоматически после перезагрузки.

После установки компонента MPX Core следует задать имя или IP-адрес узла, по которому к нему смогут обращаться другие компоненты. Для этого выполните команду

```
mpxcore set -p HostAddress mpxcore.domain.ru
```

Кроме того, компонент MPX Core нужно связать с соответствующим компонентом MPX SIEM. Для этого выполните команду

```
mpxcore set -p SiemAddress mpxsiem.domain.ru
```

Аргументом может являться как имя узла (в нашем примере mpxsiem.domain.ru), так и его IP-адрес.

Чтобы настроить шлюз, который является транспортом между компонентами, нужно:

1. включить режим шлюза:

```
mpxagent set -p GateRoleEnabled true AgentRoleEnabled false
```

2. настроить на шлюзе адрес MPX SIEM:

```
mpxagent set -p SiemAddress mpxsiem.domain.ru
```

При установке компонента MPX Core для его веб-сайта автоматически устанавливается самоподписанный сертификат, поставляемый в составе дистрибутива. Поэтому при попытке подключения пользователь получит предупреждение о том, что создаваемое подключение не защищено. Вы можете установить собственный доверенный сертификат, который отвечает следующим требованиям:

- используется алгоритм подписи SHA-256,
- длина закрытого ключа не менее 2048 бит,
- область применения сертификата: Digital Signature или Key Encipherment,
- значения SAN: DNS:localhost, IP:127.0.0.1, DNS:<GQDN или IP-адрес в ЛВС>, IP:<IP-адрес в ЛВС>.

Чтобы установить новый сертификат, выполните следующие действия.

1. Установите сертификат в хранилище Local Computer\Personal.

2. При помощи команды mpxcore задайте для сертификата thumbprint:

```
mpxcore set -p SSLCertificateThumb
FB27CD4F310F37814304535D1E7C51F2890BDB4E
```

Вместе с компонентом MPX Core автоматически устанавливаются системы управления базами данных (СУБД), необходимые для его работы (Microsoft SQL Server 2012, MongoDB).

### 1.4.2. Установка MPX SIEM

Для установки MPX SIEM используется дистрибутив

```
MPXSiemSetup_<номер версии>.exe
```

После запуска дистрибутива пользователь видит окно со ссылкой на текст лицензионного соглашения, с которым следует внимательно ознакомиться. Чтобы продолжить установку, необходимо принять лицензионное соглашение.


Далее запускается процесс установки. Если в процессе установки требуется перезагрузить операционную систему, то пользователь получит соответствующее уведомление.

После установки компонента MPX SIEM следует настроить адрес соответствующего MPX Core. Для этого выполните команду

```
mpxsiem set -p AssetResolverHost mpxcore.domain.ru
```

Аргументом может являться как имя узла (в нашем примере mpxcore.domain.ru), так и его IP-адрес.

Вместе с компонентом MPX SIEM автоматически устанавливается СУБД Elasticsearch, которая используется для хранения событий. Директории для хранения файлов с индексами и лог-файлов указываются в файле конфигурации Elasticsearch при помощи следующих параметров:

```
path.data: директория
path.logs: директория
```

Примечание: по умолчанию файл конфигурации *elasticsearch.yml* расположен в директории *c:\ProgramData\Elasticsearch\config\elasticsearch.yml*

### 1.4.3. Установка модульной платформы MPX Agent

Дистрибутив модульной платформы включает в себя установщик собственно модульной платформы (MPXAgentSetup_<номер версии>.exe), а также дистрибутив InstallAgentAsGateOnly.exe. Оба дистрибутива необходимо разметить в одном каталоге.

После запуска дистрибутива MPX Agent пользователь видит окно со ссылкой на текст лицензионного соглашения, с которым следует внимательно ознакомиться. Чтобы продолжить установку, необходимо принять лицензионное соглашение.


Далее запускается процесс установки.

Комплект поставки включает в себя утилиту mpxagent.exe, которая позволяет настраивать модульную платформу. После установки компонента MPX Agent следует настроить адрес шлюза, расположенного на сервере соответствующего MPX Core. Для этого выполните команду

```
mpxagent set -p GateAddress mpxcore.domain.ru
```

## 1.5. Установка компонента MPX-SRV-S (SIEM) в операционной системе Debian

Данный раздел описывает установку компонента MPX-SRV-S MaxPatrol SIEM в операционной системе Debian версий 8.0 и выше. Для установки требуется наличие дополнительных компонентов, таких как сервер RabbitMQ, сервер Redis и сервис Elasticsearch. Команды инсталляции и запуска сервисов должны выполняться от имени суперпользователя (с правами root).

### 1.5.1. Системные требования

1. Наличие прав суперпользователя (root) в операционной системе Debian;
2. Соединение с интернетом для доступа к репозиториям Debian;
3. Доступ к интернет-ресурсам:

   http://www.rabbitmq.com/releases/rabbitmq-server/v3.5.4/

   hkp://keyserver.ubuntu.com:80

http://ppa.launchpad.net/webupd8team/java/ubuntu

### 1.5.2. Сервер RabbitMQ

#### 1.5.2.1. Установка

1. Сервер RabbitMQ можно установить из подключенного репозитория Debian. В этом случае установка осуществляется командой:

```
apt-get install rabbitmq-server
```

2. При необходимости установки последней версии сервера RabbitMQ, ее следует скачать со страницы http://www.rabbitmq.com/install-debian.html. При установке используется следующий набор команд (в примере использована версия 3.5.4):

```
wget http://www.rabbitmq.com/releases/rabbitmq-server/v3.5.4/
rabbitmq-server_3.5.4-1_all.deb
dpkg -i rabbitmq-server_3.5.4-1_all.deb
apt-get -f install
```

Примечание: команда apt-get -f install устанавливает необходимые зависимости между компонентами.

3. После установки рекомендуется увеличить минимальный объем свободного места на диске. Для этого файл */etc/rabbitmq/rabbitmq.config* должен содержать строку:

```
[{rabbit, [{disk_free_limit, 1000000000}]}]
```

Примечание: при отсутствии файла *rabbitmq.config* его можно создать вручную и поместить в директорию */etc/rabbitmq*.

#### 1.5.2.2. Настройка

Сервер RabbitMQ поддерживает возможность удаленного управления при помощи веб-интерфейса. Для этого необходимо установить плагин:

4. Добавить пользователя *mpxsiem* :

```
rabbitmqctl add_user mpxsiem mpxsiem
rabbitmqctl set_user_tags mpxsiem administrator
rabbitmqctl set_permissions -p / mpxsiem '.*' '.*' '.*'
```

5. Установить плагин для удаленного управления:

```
rabbitmq-plugins enable rabbitmq_management
```

6. Перезапустить сервер RabbitMQ:

```
systemctl restart rabbitmq-server.service
```

После выполнения этих команд сервером можно управлять через веб-интерфейс.

Примечание: HTTP-сервер веб-интерфейса использует порт 15672 (например, http://10.0.180.222:15672).

### 1.5.3. Сервер Redis

#### 1.5.3.1. Установка

Сервер Redis устанавливается из подключенного репозитория Debian командой:

```
apt-get install redis-server
```

#### 1.5.3.2. Настройка

По умолчанию сервер принимает только локальные соединения. Изменения не требуются, если компоненты MaxPatrol SIEM и Redis установлены на одном сервере.

В случае раздельной установки:

1. Необходимо изменить значение для параметра *bind* в файле */etc/redis/redis.conf* (например: *bind 10.0.180.222*).
2. Перезапустить сервер Redis:

```
systemctl restart redis-server.service
```

### 1.5.4. Сервис Elasticsearch

#### 1.5.4.1. Установка

1. Установить Sun Java 8:

```
apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys
EEA14886
echo "deb http://ppa.launchpad.net/webupd8team/java/ubuntu precise
main" > /etc/apt/sources.list.d/java.list
apt-get update
apt-get install oracle-java8-installer
```

2. Скачать с официального сайта версию Elasticsearch для Debian www.elasticsearch.org/download/ и выполнить команду:

```
dpkg -i elasticsearch-1.7.x.deb
```

Примечание: 1.7.x – версия Elasticsearch

#### 1.5.4.2. Настройка

3. Выполнить команду для отключения функции SWAP:

```
sudo swapoff –a
```

4. Внести изменения в файл */etc/default/elasticsearch*.
   4.1. Отключение функции SWAP:

```
MAX_LOCKED_MEMORY=unlimited
```

   4.2. Количество открытых файлов может достигать больших значений из-за нехватки ресурсов жесткого диска. Необходимо установить ограничение:

```
MAX_OPEN_FILES=655350
```

   4.3. Рекомендуемый объем оперативной памяти для работы Elasticsearch составляет 64 ГБ. При наличии меньшего объема, рекомендуется установить следующий параметр, равный 50% от объема ОЗУ, но не более 30 ГБ:

```
ES_HEAP_SIZE=30g
```

5. Для систем, основанных на systemd, необходимо выполнить команду:

```
systemctl enable elasticsearch
```

6. Внести изменения в файл /etc/systemd/system/multi-user.target.wants/elasticsearch.service.

6.4. Установить максимально количество дескрипторов файлов, которые поддерживаются процессом:

```
LimitNOFILE=655350
```

6.5. Установить максимальное количество байтов памяти, которые могут быть заняты ОЗУ:

```
LimitMEMLOCK=infinity
```

Примечание: параметру *LimitMEMLOCK* присваивается значение *infinity* при наличии настроек *'bootstrap.mlockall: true'* в файле *elasticsearch.yml* и *'MAX_LOCKED_MEMORY=unlimited'* в */etc/default/elasticsearch*.

7. Выполнить команду:

```
systemctl daemon-reload
```

8. Внести изменения в файл *etc/elasticsearch/elasticsearch.yml*:

```
cluster.name: ptsiem


# Ограничение до одного пишущего потока команд.
index.merge.scheduler.max_thread_count: 1
# Параметр для возможности индексирования данных пакетами, объемом до 15 МБ.
threadpool.bulk.queue_size: 50000
# Параметры для настройки 32 элементов с возможностью их хранения в течении 100 дней и поддержкой 10 одновременных запросов.
threadpool.index.queue_size: 32000
threadpool.search.queue_size: 32000
threadpool.get.queue_size: 32000
# При условии установки storage и frontend (компоненты MaxPatrol SIEM) на одном хосте, следует указать локальный IP-адрес. В противном случае требуется настройка межсетевого экрана с целью контроля доступа к порту 9200.
network.bind_host: 127.0.0.1
# Минимальный объем памяти жесткого диска, при достижении которого прекращается индексация данных.
cluster.routing.allocation.disk.watermark.low: 500mb


Объем ОЗУ, затрачиваемый на кэширование значений полей.
indices.fielddata.cache.size: 40%


# Объем ОЗУ, затрачиваемый на кэширование значений полей с учетом временных структур запросов.
indices.breaker.total.limit: 70%


# По умолчанию инстанс Elasticsearch участвует в кластере, что может усложнить процесс тестирования. Чтобы исключить инстанс из кластера, необходимо внести следующие изменения:
node.local: true
```

```
discovery.zen.ping.multicast.enabled: false
```

9. Для систем, основанных на systemd, дополнительно требуется выполнить:

```
/bin/systemctl daemon-reload
/bin/systemctl enable elasticsearch.service
```

10. Запустить сервис Elasticsearch:

```
service elasticsearch start
```

Для возможности просмотра данных о производительности системы и использования ресурсов рекомендуется установить плагин Marvel:

```
/usr/share/elasticsearch/bin/plugin -install elasticsearch/marvel/
latest
```

Примечание: в некоторых ситуациях стандартная установка плагина Marvel недоступна. В таком случае следует скачать архив http://download.elasticsearch.org/elasticsearch/marvel/marvel-latest.zip и распаковать его содержимое (файл .jar) в директорию */usr/share/elasticsearch/plugins*.

### 1.5.5. Установка MaxPatrol SIEM

Для установки компонента MaxPatrol SIEM необходимо выполнить команду:

```
dpkg -i mpxsiem_9.x-xxxx.deb
```

Примечание: 9.x-xxxx – версия MaxPatrol SIEM.

Файлы MaxPatrol SIEM будут расположены в подкаталоге /opt/mpxsiem/ в следующей структуре:

| | |
|---|---|
| `<root>/bin/` | исполняемые модули программ |
| `<root>/etc/` | конфигурационные данные |
| `<root>/log/` | лог-файлы и файлы статистики |
| `<root>/var/lib/` | правила агрегации, нормализации и корреляции |
| `<root>/tmp/` | временные данные программ |

Владельцами подкаталога */opt/mpxsiem/* будут пользователь *mpxsiem* и группа *mpxsiem*. Группа и пользователь создаются автоматически, при установке компонента MaxPatrol SIEM. Кроме того, регистрируются сервисы:

```
mpxsiem-aggregator
mpxsiem-commander
mpxsiem-correlator
mpxsiem-frontend
```

```
mpxsiem-normalizer
mpxsiem-rester
mpxsiem-router
mpxsiem-storage
```

Перед запуском сервисов необходимо осуществить настройку параметров (например, ввести IP-адрес сервера, на котором расположен Elasticsearch). Настройка параметров осуществляется в файле */opt/mpxsiem/etc/ptsiem.conf*.

Сервисы MaxPatrol SIEM не запускаются автоматически. Для их запуска необходимо выполнить команду:

```
systemctl start mpxsiem-*.service
```

## 1.6. Настройка соединений между компонентами

Для настройки опций установленных компонентов применяются утилиты, которые устанавливаются вместе с соответствующими компонентами. Путь к этим утилитами заносится в системную переменную окружения PATH в процессе установки.

Утилиты имеют следующие имена:

Таблица 2.

| Имя | Компонент |
|---|---|
| mpxcore.exe | для модуля MPX Core |
| mpxsiem.exe | для компонента MPX SIEM |
| mpxagent.exe | для модульной платформы |
| mpxptkb.exe | для базы знаний. |

Эти утилиты следует выполнять в консоли, которая запущена с правами администратора.

Утилиты mpxcore.exe и mpxsiem.exe поддерживают следующие команды:

Таблица 3.

| Команда | Действие |
|---|---|
| list | перечислить доступные параметры |
| get | получить текущие значения параметров (значения выдаются в одинарных кавычках) |
| set | установить значения параметров (соответствующие службы перезапускаются автоматически). |

Рассмотрим параметры утилиты mpxcore.exe.

Таблица 4. Общие настройки

| Настройка | Примечание |
|---|---|
| InstallDir | каталог установки компонента MPX Core (стандартное значение: C:\Program Files\Positive Technologies\MaxPatrol X Core) |
| ProgramDataDir | каталог для хранения файлов данных (стандартное значение: C:\ProgramData\Positive Technologies\MaxPatrol X Core) |
| HostAddress | IP-адрес или FQDN узла, на котором установлен MPX Core |
| SiemAddress | адрес связанного компонента MPX SIEM |
| CoreSiteId | идентификатор сайта, на котором установлен веб-интерфейс системы (стандартное значение: 4D617850-6174-726F-6C39-536974654964) |
| GateUrl | URL шлюза, который использует компонент MPX Core (стандартное значение: https://127.0.0.1:3030/) |
| DataVersion | версия базы знаний |
| MongoDbUrl | URL используемой БД MongoDB (без заключительного слэша; стандартное значение: mongodb://localhost) |
| флаг CleanServiceData: True/ False | включена/отключена очистка баз данных во время установки и удаления компонента MPX Core (стандартное значение: False). |

Таблица 5. Настройки экземпляра Microsoft SQL Server, используемого компонентом MPX Core

| Настройка | Примечание |
|---|---|
| SqlServerName | имя экземпляра Microsoft SQL Server (стандартное значение: localhost\MaxPatrolXCore) |
| SqlServerUserName | имя пользователя экземпляра Microsoft SQL Server (стандартное значение: sa) |
| SqlServerPassword | пароль пользователя экземпляра Microsoft SQL Server (стандартное значение: P@ssw0rd). |

Таблица 6. Настройки базы знаний

| Настройка | Примечание |
|---|---|
| флаг LoadPtkbData: True/False | включено/отключено копирование данных из MPX PT KB (стандартное значение: True) |
| PtkbDbName | имя базы знаний, из который импортируются данные об уязвимостях. |

Таблица 7. Настройки сертификата

| Настройка | Примечание |
|---|---|
| SSLCertificateThumb | отпечаток (thumb) используемого сертификата (опция используется для замены стандартного сертификата из поставки MaxPatrol X; стандартное значение: FB27CD4F310F37814304535D1E7C51F2890BDB4E). |

Таблица 8. Настройки SMTP-сервера

| Настройка | Примечание |
|---|---|
| SmtpSender | значение поля Отправитель (sender) в электронном уведомлении (стандартное значение: MaxPatrol Notification System <NoReply@MaxPatrol.com>) |
| SmtpHost | адрес SMTP-сервера (стандартное значение: localhost) |
| SmtpPort | порт, который использует SMTP-сервер (стандартное значение: 25) |
| SmtpUseDefaultCredentials | определяет режим аутентификации SMTP-сервера; true — используется учетная запись Windows (стандартное значение: True). |

Если для параметра SmtpUseDefaultCredentials задано значение False, то для подключения к SMTP-серверу используются следующие параметры:

- SmtpUser: имя пользователя,
- SmtpPassword: пароль пользователя.

В системе MaxPatrol SIEM используются два способа задания новых значений параметров для компонентов с помощью команды set.

- ключ -p: перечисление в командной строке,
- ключ -f: считывание параметров из файла.

При использовании ключа -p параметры и их новые значения задаются парами строк, разделенными пробелами.

```
mpxcore set -p HostAddress “10.0.76.13”
```

При использовании ключа -f необходимо указать полный путь к XML-файлу с новыми значениями параметров. Этот файл должен иметь следующий вид.

```
<?xml version="1.0" encoding="utf-8"?>
<params>
```

```
    <param id="MongoHost" value="localhost" />
    <param id="ForwardEnabled" value="false" />
  </params>
```

При внесении изменений все необходимые сервисы будут перезапущены автоматически.

Рассмотрим параметры утилиты mpxsiem.exe.

Таблица 9. Параметры утилиты mpxsiem.exe

| Настройка | Примечание |
|---|---|
| InstallDir | каталог установки компонента MPX SIEM (стандартное значение: C:\Program Files (x86)\Positive Technologies\MaxPatrol X SIEM) |
| ProgramDataDir | каталог для хранения файлов данных (стандартное значение: C:\ProgramData\Positive Technologies\MaxPatrol X SIEM) |
| CoreSiteId | идентификатор сайта, на котором установлен веб-интерфейс системы (стандартное значение: 4D617850-6174-726F-6C39-536974654964) |
| AssetResolverHost | адрес компонента MPX Core который отвечает за привязку событий к существующим активам системы (стандартное значение: Localhost) |
| Флаг ForwardEnabled: True/ False | включена/отключена пересылка сообщений (стандартное значение: False) |
| ForwardAgentHost | адрес шлюза, через который компонент MPX SIEM пересылает сообщения (стандартное значение: Localhost) |
| DataVersion | версия базы знаний |
| ElasticsearchHost | адрес узла, на котором установлена Elasticsearch (стандартное значение: Localhost) |

Рассмотрим параметры утилиты mpxagent.exe.

Таблица 10. Параметры утилиты mpxagent.exe

| Настройка | Примечание |
|---|---|
| InstallDir | каталог установки компонента MPX Agent (стандартное значение: C:\Program Files (x86)\Positive Technologies\MaxPatrol X Agent) |
| ProgramDataDir | каталог для хранения файлов данных (стандартное значение: C:\ProgramData\Positive Technologies\MaxPatrol X Agent) |
| AgentID | идентификатор компонента MPX Agent, который выдается при установке системы |
| AgentName | название компонента MPX Agent |
| GateAddress | адрес связанного шлюза (стандартное значение: localhost) |
| Флаг AgentRoleEnabled: True/ False | включена/выключена роль агента (стандартное значение: True) |
| Флаг GateRoleEnabled: True/ False | включена/выключена роль шлюза (стандартное значение: False) |
| SiemAddress | адрес SIEM-сервера, параметр компонента MPX Agent в роли шлюза (стандартное значение: localhost) |

Таблица 10. Параметры утилиты mpxagent.exe

| Настройка | Примечание |
|---|---|
| CoreUrl | стандартное значение: https://localhost:8779/api/v1/ |
| Флаг ConsolidatorEnabled: True/False | консолидация включена/отключена (стандартное значение: False) |
| ConsolidatorAddress | адрес компонента MPX Agent, который консолидирует данные |
| SslCert | путь к сертификату SSL |
| SslKey | путь к ключу SSL |
| DataVersion | версия базы знаний. |

Рассмотрим параметры утилиты mpxptkb.exe.

Таблица 11. Параметры утилиты mpxptkb.exe

| Настройка | Примечание |
|---|---|
| InstallDir | каталог установки компонента MPX PT KB (стандартное значение: C:\Program Files\Positive Technologies\PT KB) |
| ProgramDataDir | каталог для хранения файлов данных (стандартное значение: C:\ProgramData\Positive Technologies\PT KB) |
| HostAddress | IP-адрес или FQDN компонента MPX Core |
| SSLCertificateThumb | отпечаток (thumb) используемого сертификата (опция используется для замены стандартного сертификата из поставки MaxPatrol SIEM; стандартное значение: DDAA6A521205B95F55D11D850F7CB1E9FA9BFB52) |
| SqlServerName | имя экземпляра Microsoft SQL Server (стандартное значение: localhost\MaxPatrolXCore) |
| SqlServerUserName | имя пользователя экземпляра Microsoft SQL Server (стандартное значение: sa) |
| SqlServerPassword | пароль пользователя экземпляра Microsoft SQL Server (стандартное значение: P@ssw0rd) |

## 1.7. Развертывание системы в конфигурации

# Virtual Appliance

Система MaxPatrol SIEM может поставляться в виде OVA-образов виртуальных машин, которые содержат операционную систему с установленными компонентами системы. В комплект поставки входят четыре образа:

Таблица 12. Образы ОС с компонентами MaxPatrol SIEM

| Название образа | Компоненты | Учетная запись |
|---|---|---|
| MPXCORE | MPX Core, MPX Gate | Administrator/P@ssw0rd |
| MPXSIEM | MPX SIEM | |
| MPXAGENT | MPX Agent | |
| MPXHOST | Комбинированная установка | Administrator/P@ssw0rd |

Для всех образов используется одинаковая конфигурация ОС Windows Server 2008 R2 и аппаратного обеспечения:

- 4 процессора,
- RAM: 8 ГБ,
- HDD: 400 ГБ,
- Учетная запись: Administrator/P@ssw0rd.

Полученные от производителя образы следует импортировать, а затем с помощью штатных средств настроить виртуальные сетевые карты в соответствии с требованиями к сети компании. Обратите внимание, что все узлы должны иметь статическое имя (IP-адрес, FQDN, сетевое имя), по которому другие узлы и компоненты смогут к ним обращаться. Кроме того, следует выполнить действия по первоначальной настройке, описанные в разделе установки соответствующих компонентов (глава *Системные требования*).

# 2. Системные требования

В данном разделе представлены требования, предъявляемые к аппаратному и программному обеспечению при развертывании компонентов MaxPatrol X.

## 2.1. Аппаратное обеспечение

Для установки компонентов MaxPatrol X можно использовать как физическое, так и виртуальное оборудование. Ниже указаны типовые аппаратные требования к системе, на которую устанавливаются компоненты MaxPatrol X.

Таблица 13. Рекомендуемые требования к серверной инфраструктуре

| Компонент | Параметр | до 6000 EPS | до 10000 EPS | до 15000 EPS |
|---|---|---|---|---|
| MPX SIEM | Процессор | 12 ядер, 2,4 ГГц | 14 ядер, 2,6 ГГц | 16 ядер, 3,0 ГГц |
| | Оперативная память | 48 ГБ | 64 ГБ | 64 ГБ |
| | Жесткий диск (ОС, SIEM) | 2x600 ГБ, SAS, 10000 об/мин, RAID 1 | 2x600 ГБ, SAS, 10000 об/мин, RAID 1 | 2x900 ГБ, SAS, 10000 об/мин, RAID 1 |
| | Жесткий диск (База данных) | 2x600 ГБ, SAS, 10000 об/мин, RAID 1 | 2x600 ГБ, SAS, 10000 об/мин, RAID 1 | 2x900 ГБ, SAS, 10000 об/мин, RAID 10 |
| | Внешнее хранилище событий | SAS, 10000 об/мин, RAID 10 (объем рассчитывается отдельно) | SAS, 10000 об/мин, RAID 10 (объем рассчитывается отдельно) | SAS, 10000 об/мин, RAID 10 (объем рассчитывается отдельно) |
| | Сеть | 1000 Мбит/с | 1000 Мбит/с | 1000 Мбит/с |
| MPX Core | Процессор | 6 ядер, 2,0 ГГц | 6 ядер, 2,5 ГГц | 8 ядер, 3,0 ГГц |
| | Оперативная память | 32 ГБ | 48 ГБ | 64 ГБ |
| | Жесткий диск (ОС, компоненты) | 2x600 ГБ, SAS, 10000 об/мин, RAID 1 | 2x600 ГБ, SAS, 10000 об/мин, RAID 1 | 2x600 ГБ, SAS, 10000 об/мин, RAID 1 |
| | Жесткий диск (Локальная база данных) | 2x600 ГБ, SAS, 10000 об/мин, RAID 1 | 2x600 ГБ, SAS, 10000 об/мин, RAID 1 | 2x600 ГБ, SAS, 10000 об/мин, RAID 1 |
| | Сеть | 1000 Мбит/с | 1000 Мбит/с | 1000 Мбит/с |
| MPX Agent | Процессор | 4 ядра, 2,5 ГГц | | |
| | Оперативная память | 8 ГБ | | |
| | Жесткий диск | 1 ТБ, SATA, 7200 об/мин | | |
| | Сеть | 1000 Мбит/с | | |

Система MaxPatrol X способна обрабатывать до 30000 событий в секунду. Для расчета необходимой конфигурации аппаратного обеспечения обратитесь в службу технической поддержки.

Ниже представлены аппаратные требования к модулям, подключаемым к платформе MPX Agent.

Таблица 14. Рекомендуемые требования к MaxPatrol X Scanner

| Компонент | Параметр | Значение |
|---|---|---|
| MPX-SCN-S | Процессор | 4 ядра, 2,5 ГГц |
| | Оперативная память | 8 ГБ |
| | Жесткий диск | 1 ТБ, SATA, 7200 об/мин |
| | Сеть | 1000 Мбит/с |

Таблица 15. Рекомендуемые требования к MaxPatrol X Log Collector

| Компонент | Параметр | Модель 1<br>до 2500 EPS | Модель 2<br>до 15000 EPS |
|---|---|---|---|
| MPX-LC-S | Процессор | 4 ядра, 2,5 ГГц | 4 ядра, 2,5 ГГц |
| | Оперативная память | 8 ГБ | 16 ГБ |
| | Жесткий диск | 1 ТБ, SATA, 7200 об/мин | 1 ТБ, SAS, 10000 об/мин |
| | Сеть | 1000 Мбит/с | 10/100/1000 Мбит/с |

Таблица 16. Рекомендуемые требования к MaxPatrol X Network Traffic

| Компонент | Параметр | Модель 1<br>до 200 Мбит/с | Модель 2<br>до 2 Гбит/с |
|---|---|---|---|
| MPX-NT-S | Процессор | 4 ядра, 2,4 ГГц | 4 ядра, 2,8 ГГц |
| | Оперативная память | 8 ГБ | 16 ГБ |
| | Жесткий диск | 2x1 ТБ, SATA, 7200 об/мин | 2x1 ТБ, SATA, 7200 об/мин |
| | Сеть управления | 10/100/1000 Мбит/с | 10/100/1000 Мбит/с |
| | Сеть мониторинга | 10/100/1000 Мбит/с | 1000 Мбит/с |

Если к одной модульной платформе подключено несколько модулей, то следует сложить соответствующие аппаратные требования.

Если используется виртуальное оборудование, и гипервизор позволяет зарезервировать ресурсы, выделяемые виртуальной машине, то рекомендуется установить резерв ресурсов со значениями не меньше указанных в таблице.

Требования указаны для оборудования, которое будет использоваться только для системы MaxPatrol X. В сложных нетиповых случаях требования к аппаратному обеспечению необходимо уточнять в службе технической поддержки.

Нагрузка на объект при сканировании зависит от типа узла и способа сбора информации, но редко бывает значительной. Не рекомендуется сканировать узлы, находящиеся на

пределе загрузки (процессор загружен более чем на 70%, свободной оперативной памяти менее 256 МБ, свободного места на системном диске менее 50 МБ).

Производитель рекомендует разворачивать систему на одном сервере только для демонстрационных целей. Продуктивные системы следует разворачивать на нескольких серверах.

## 2.2. Программное обеспечение

Система MaxPatrol X разработана для функционирования на базе следующих операционных систем:

- Microsoft Windows Server 2008 R2 SP1,
- Microsoft Windows Server 2012,
- Microsoft Windows Server 2012 R2,
- Linux Debian 8.0 и выше.

Для доступа к компонентам системы рекомендуется использовать браузеры Google Chrome 30 (и выше) или Mozilla Firefox 26 (и выше).

Для корректного функционирования компонентов требуется установить необходимое программное обеспечение. Пакеты программ включены в поставляемые дистрибутивы и разворачиваются автоматически при установке соответствующего компонента.

Для основного компонента системы MPX Core требуется следующее ПО:

- NET Framework 4.5,
- Visual C++ Redist 2012 Update 4x86/4x64,
- Microsoft SQL Server Express 2012 SP1 15.55.4500,
- WMF 4.0,
- Erlang Runtime R16,
- RabbitMQ 3.1.0,
- MongoDB 2.6.5.

Примечание: в случае наличия более 3000 сетевых узлов требуется установка Microsoft SQL Server Standard.

Для компонента MPX SIEM требуется следующее ПО:

- .NET Framework 4.5,
- Elasticsearch 1.7.1,
- Visual C++ Redist 2012 Update 4x86,
- Redis 2.8.17,
- Erlang Runtime R16,
- WMF 4.0,
- RabbitMQ 3.1.0,
- MongoDB 2.6.5.

Для модульной платформы требуется следующее ПО:

- Visual C++ Redist 2008 SP1xX86,
- Visual C++ Redist 2012 Update 4x86,
- Visual C++ Redist 2013 Update 4x86,
- .NET Framework 4.5,
- WinPcap 4.1.3,
- MPConnectors Oracle 1.13.0,
- WMF 4.0.

Для корректной установки и функционирования MPX Core в операционной системе сервера необходимо активировать определенные системные компоненты. Активация выполняется автоматически в процессе установки системы. Набор системных компонентов зависит от версии используемой ОС.

Таблица 17. Набор системных компонентов

| MS Windows Server 2008 R2 | MS Windows Server 2012 |
|---|---|
| IIS-WebServerRole | |
| IIS-ISAPIExtensions | |
| IIS-ISAPIFilter | |
| IIS-RequestFiltering | |
| IIS-NetFxExtensibility | IIS-NetFxExtensibility45 |
| IIS-DefaultDocument | |
| IIS-ASPNET | IIS-ASPNET45 |
| IIS-StaticContent | |
| IIS-DirectoryBrowsing | |
| IS-WindowsAuthentication | |
| IIS-HttpRedirect | |

Средства обеспечения безопасности могут оказывать негативное влияние на работу системы MaxPatrol X. Поэтому на этапе планирования и развертывания рекомендуется провести тестовые сканирования и при необходимости принять меры для снижения негативных последствий, например отключить средства межсетевого экранирования, антивирусную защиту или специализированные средства контроля аппаратного оборудования на серверах, где установлены компоненты MaxPatrol.

Большинство сетевых средств обеспечения безопасности содержат модули анализа прикладных протоколов (stateful inspection, application firewall), которые могут вмешиваться в процесс сканирования, снижая достоверность полученных результатов. Так, например, результат сканирования веб-приложения через межсетевой экран, поддерживающий функции защиты веб-приложений (web application firewall), не будет достоверным, поскольку МЭ заблокирует ряд потенциально опасных запросов, используемых сканером. В некоторых средствах защиты нельзя отключить фильтрацию

прикладных протоколов для отдельных узлов, и в таких случаях рекомендуется выносить агент за МЭ.

Системы обнаружения и предотвращения атак часто реагируют на процесс сканирования, как на потенциальную атаку. Получение списка открытых портов, проверка стойкости паролей, доступ к протоколам удаленного управления — все это может привести к срабатыванию средств защиты. В случае если механизм предотвращения атак не задействован, множественные срабатывания сигнатур приведут только к увеличению объема журналов системы обнаружения атак. Если механизм предотвращения атак включен, то система может вмешаться в процесс сканирования и исказить результаты работы. В связи с этим рекомендуется вносить узлы, на которых установлены компоненты MaxPatrol X, в список исключений системы обнаружения атак.

# 3. Обновление системы

MaxPatrol X позволяет выполнять обновление с помощью дистрибутива новой версии системы. Модульные платформы можно обновлять централизованно из интерфейса управления.

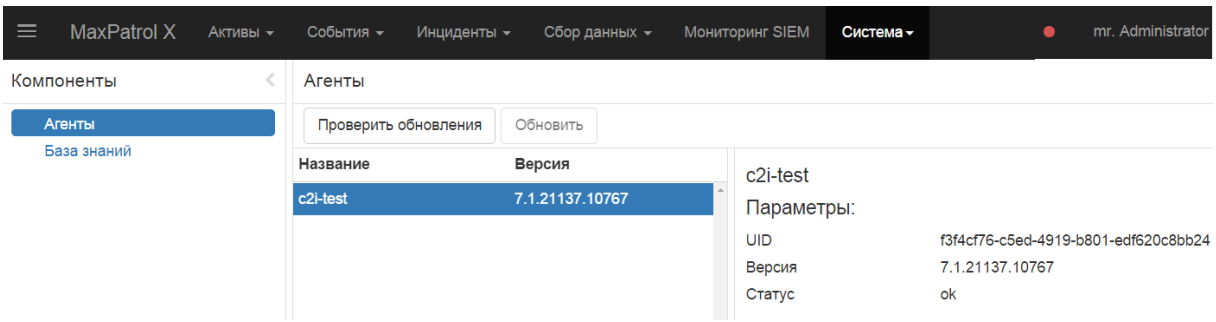
## 3.1. Обновление сервера

Для обновления серверных компонентов MPX Core и MPX SIEM следует обратиться к производителю системы и получить дистрибутив с новой версией.

## 3.2. Обновление модульной платформы

Компоненты MPX Agent можно обновлять централизованно из консоли управления сервера, к которому они подключены. По команде пользователя система проверит версии модульных платформ и при необходимости предложит запустить процесс обновления, который проходит в автоматическом режиме.

Перейдите в меню *Система – Обновление*. Слева на панели *Компоненты* выберите *Агенты*. В правой панели появится список всех доступных агентов. Убедитесь, что система работает без ошибок (зеленый индикатор справа в строке меню).




Нажмите кнопку *Проверить обновления*, и если обновления обнаружены — нажмите *Обновить*.

# 4. Удаление системы

Для удаления системы пользуйтесь стандартными средствами Windows. Мастер удаления работает в двух режимах — полное удаление системы и удаление приложения без удаления пользовательских данных.

Чтобы выбрать один из режимов, используйте опцию “Remove application data”. Если она включена, то производится полное удаление системы, иначе пользовательские данные сохраняются.

# 5. Работа с базами данных

Для хранения событий система MaxPatrol X использует нереляционную БД Elasticsearch версии 1.7.x. Для работы с этой БД используется инструмент Kibana 4, установка которого описана ниже.

## 5.1. Установка и настройка БД Elasticsearch

Для установки и настройки БД Elasticsearch на операционных системах CentOS и Debian следует выполнить следующие шаги.

- Установить Sun Java 8.
- Скачать с официального сайта дистрибутив www.elasticsearch.org/download/ .
- Выполнить команду *dpkg -i elasticsearch-1.7.1.deb*
- Подготовить БД Elasticsearch к установке командой *sudo swapoff -a*
- Отредактировать конфигурационный файл */etc/default/elasticsearch* (Debian) либо */etc/sysconfig/elasticsearch* (CentOS):

```
MAX_LOCKED_MEMORY=unlimited
MAX_OPEN_FILES=65535
ES_HEAP_SIZE=30g
```

Если в системе менее 64 Гб RAM, то для параметра ES_HEAP_SIZE следует задать значение, равное 50% имеющейся памяти, но не более 30 Гб.

- Отредактировать файл */etc/elasticsearch/elasticsearch.yml*

```
cluster.name: ptsiem
index.merge.scheduler.max_thread_count: 1
threadpool.bulk.queue_size: 50000
# Because we have 32 shards per each of ~100 daily indices.
threadpool.index.queue_size: 32000
threadpool.search.queue_size: 32000
threadpool.get.queue_size: 32000
network.bind_host: 127.0.0.1
cluster.routing.allocation.disk.watermark.low: 500mb
node.local: true
discovery.zen.ping.multicast.enabled: false
```

Параметры node.local и discovery.zen.ping.multicast.enabled следует настраивать, если узел нужно исключить из кластера.

- Запустить БД Elasticsearch командой *service elasticsearch start*

## 5.2. Установка и использование Kibana 4

Чтобы установить Kibana 4, выполните следующие шаги:

- Запустить MaxPatrol X.

- Если в системе еще нет событий (например, она была установлена недавно), то сгенерировать несколько событий. Этот шаг необходим для создания хотя бы одного индекса нормализованных данных в БД.
- Скачать дистрибутив Kibana 4 с официального веб-сайта (https://www.elastic.co/thank-you?url=https://download.elastic.co/kibana/kibana/kibana-4.0.2-windows.zip) и распаковать его.
- В каталоге config задать адрес системы, на которой установлена БД Elasticsearch, в параметре elasticsearch_url.
- Запустить файл bin/kibana.bat
- Открыть http://localhost:5601/
- Перейти на страницу Settings и указать ptsiem_events в качестве индекса. Опция Use event times to create index names должны быть отключена.
- Выбрать time в качестве поля времени.
- На странице Settings добавить дополнительный индекс ptseim_raw.
- Выбрать recv_time в качестве поля времени.

Чтобы выполнять запросы для поиска данных, перейдите на вкладку Discover.

Поиск событий производится по соответствующему индексу. Чтобы задать временной диапазон для поиска, нажмите кнопку в правом верхнем углу окна. Запросы к БД составляются на языке Lucene, официальное описание которого приведено на веб-странице http://www.lucenetutorial.com/lucene-query-syntax.html.

Для поиска нормализованных событий используйте индекс ptsiem_events, а для событий в исходном виде — ptsiem_raw.

Ниже приведены примеры запросов.

- _id:00000005-45cf-0392-f000-45a37d36ac19 (поиск по идентификатору)
- status:error or status:failure (поиск по значению поля status, условия объединены по ИЛИ)
- rule.name:Lock_unlock_domain_account (поиск по значению поля rule.name)
- time:[2015-03-01T12:00:00Z TO 2015-03-01T13:00:00Z] (поиск по времени создания события)
- id:PT_SIEM_Vpn_session (поиск по идентификатору)
- user.name:* (события, у которых задано поле user.name, user.name != null)
- !user.name:* (события, у которых нет поля user.name, user.name == null)

# 6. Консолидация данных

Ценность и достоверность знаний зависит не только от эффективности используемых аналитических методов и алгоритмов, но и от того, насколько правильно подобраны и подготовлены исходные данные для анализа. Данные могут храниться в различных источниках, иметь разный тип и формат, являться недостаточными или избыточными. Поэтому консолидация данных необходима для принятия взвешенных решений.

В основе консолидации лежит процесс сбора и организации хранения данных в виде, оптимальном с точки зрения их обработки на конкретном уровне.

В MaxPatrol X консолидация данных решает несколько задач. Во-первых, она позволяет следить за состоянием ИБ любого филиала или подразделения. События ИБ выборочно передаются на центральный MPX Server, где включаются в общий процесс корреляции событий. Общую отчетность по всем филиалам или статистику по выбранному подразделению можно получить на любом уровне (в зависимости от настроенных прав доступа). Во-вторых, консолидация дает возможность выявлять атаки, направленные на несколько подразделений компании одновременно. Это позволяет быстро реагировать на подобные инциденты и эффективно противостоять им.

Критерии отбора событий записываются в специальном маршруте forward.xp правил корреляции. Например:

```
!COND = (criticality == "security" or
         criticality == "critical_security") and
        site_id == null
# Rule for regional SIEM to forward all correlated events to HeadQuaters
_correlation_id = []
_routing_key = "storage.pack"
_rule_name = "forward"
_event_name = "forward"
_action_name = "forward"
```

В указанном примере такие события, у которых параметр criticality имеет значение security или critical_security, а параметр side_id имеет значение NULL (такие события созданы на рассматриваемом сервере, а не переданы от других экземпляров), будут перенаправлены вышестоящему серверному компоненту.

Пример: массовая установка ПО

В данном примере рассматривается ситуация, когда на рабочие станции филиалов устанавливается ПО. Эта ситуация может интерпретироваться как атака, поскольку похожа на действия хакеров, которые создают бот-сети, следят за действиями пользователя и пр.

Рассмотрим инфраструктуру из одного головного офиса и двух филиалов, рабочие станции которых находятся в доменах domain1 и domain2 соответственно.

*Предварительная настройка инфраструктуры*

Перед началом работы следует:

- установить компоненты MaxPatrol X в головном офисе и на серверы с ролью доменного администратора в каждом из филиалов;
- на каждом компоненте MXP Agent включить роль Gate.

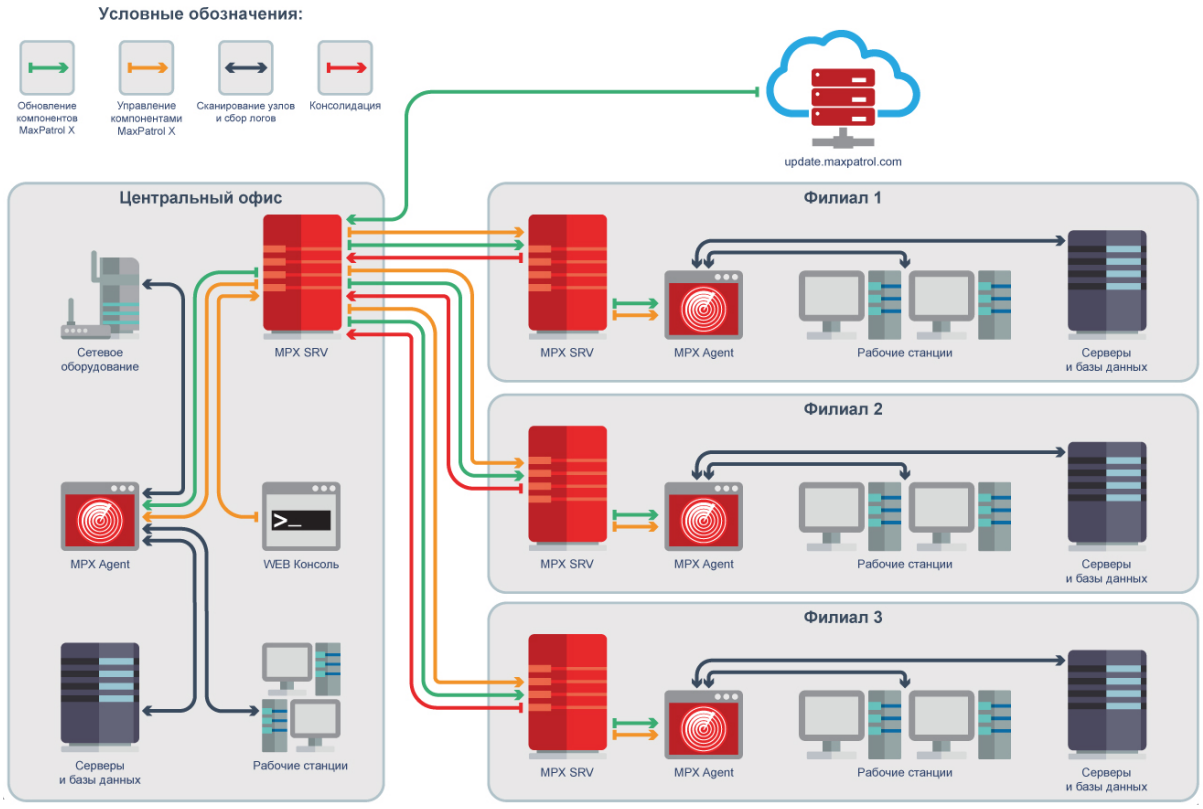
Для настройки связи MPX Agent между собой:

- На компонентах MPX SIEM, установленных в филиалах, включить роль Consolidator командой *ptsiem set -p ConsolidatorEnabled true*
- На компонентах MPX SIEM, установленных в филиалах, задать адрес головного сервера: *mpxsiem set -p ConsolidatorAddress <IP-адрес головного сервера>*

- Убедиться, что на компонентах MPX Agent заданы разные значения site_id в файле ptsiem.conf, расположенном в каталоге установки MPX Agent (подкаталог config). При необходимости измените значения этого параметра.
- На компонентах MPX SIEM, установленных в филиалах, в файле ptsiem.conf, расположенном в каталоге установки MPX Agent (подкаталог config), установить значение 1 параметров enabled и ssl в секции storage\forward.

Для рассматриваемого эксперимента изменим время срабатывания правил корреляции, чтобы они срабатывали быстрее (600 секунд вместо стандартного часа).

- На компонентах MPX Agent в файле ptsiem.conf, расположенном в каталоге установки MPX Agent (папка config), добавить параметр max_timeout со значением 600 в секции correlator. Перезагрузить службу MaxPatrol X SIEM data correlation service.




На рабочих станциях в филиалах создаем задачи по сбору событий WinEventLog.

Затем устанавливаем ПО на каждую из рабочих станций. Мы предлагаем использовать пакет установки 7-Zip, который распространяется как MSI-установщик и имеет небольшой размер.

Для просмотра собранных событий используются соответствующие фильтры.

После завершения эксперимента остановите сбор событий по задаче WinEventLog.

**Как связаться с производителем**

Адрес штаб-квартиры компании:
107061, Россия, Москва, Преображенская пл., д.8, бизнес-центр «ПРЕО 8»
Телефон: +7 495 744-01-44
Веб-сайт: support.ptsecurity.com