

Table of Contents

Table of Contents	1
Настройка сети	2
Настройка сетевых зон	3
Настройка интерфейсов	5
Маршруты	8
Настройка шлюзов	9

Настройка сетевых зон

Documentation: ☒
Product: LogAn
Version: 7.x

Под сетевой зоной в UserGate LogAn понимается логическое объединение сетевых интерфейсов. Рекомендуется объединять интерфейсы в зоне на основе их функционального назначения, например можно создать зону для локальной сети (LAN) или зону интерфейсов управления (Management).

По умолчанию в UserGate LogAn предусмотрены следующие сетевые зоны:

- **Management** — для доверенных сетей, из которых разрешено администрирование устройства.
- **Trusted** — для внутренних доверенных сегментов сети (например, LAN). Вы можете использовать эту зону для подключения к устройству сенсоров UserGate, а также для доступа в интернет.

Вы можете изменять параметры этих сетевых зон, а также [добавлять новые зоны](#) (не больше 255 зон). Кроме того, вы можете управлять доступом к сервисам устройства для подключенных к зоне клиентов.

В свойствах зоны можно управлять доступом к следующим сервисам UserGate LogAn.

Сервис	Назначение
Ping	Проверка доступности UserGate LogAn с помощью утилиты ping
SNMP	Доступ к UserGate LogAn по SNMP-протоколу (порт UDP 161)
Консоль администрирования	Доступ к веб-консоли UserGate LogAn (порт TCP 8010)
API XML RPC поверх HTTP	Доступ к API UserGate LogAn по протоколу HTTP (порт TCP 4041)
API XML RPC поверх HTTPS (доступен начиная с версии 7.3.3)	Доступ к API UserGate LogAn по протоколу HTTPS (порт TCP 4443)
Кластер	Объединение нескольких узлов UserGate LogAn в кластер конфигурации
VRRP	Объединение нескольких узлов UserGate LogAn в кластер отказоустойчивости
CLI по SSH	Доступ к интерфейсу командной строки UserGate LogAn (порт TCP 2200)
Агент аутентификации	Получение сообщений RADIUS Accounting от серверов сетевого доступа (по умолчанию — порт UDP 1813)
База данных журналов (для версии 7.2.0 и ниже — сервис Log Analyzer)	Интеграция UserGate LogAn с сенсорами UserGate . Исходящие подключения — порты TCP 9713 и TCP 2023. Входящие подключения — порт TCP 22711 либо порт 22699 (для сенсоров UserGate с ПО версии 6.1.9 и ниже)
Сборщик логов	Получение событий от syslog-источников (по умолчанию — порт TCP 514)

Для работы сервисов необходимо разрешить соответствующие порты и протоколы в сетевой инфраструктуре организации. Подробнее — в разделе «[Требования к сетевому окружению](#)».

Вы также можете включать защиту от DoS-атак и защиту от IP-спуфинга для каждой зоны. Кроме того, в свойствах зоны вы можете ограничить количество активных сессий для одного IP-адреса. Это позволит снизить нагрузку на инфраструктуру организации при DDoS-атаках, предотвратить злоупотребление ресурсами и обеспечить их доступность для всех пользователей.

Чтобы добавить сетевую зону:

1. В разделе **Настройки → Сеть → Зоны** нажмите **Добавить**.
2. На вкладке **Общие** выполните следующие действия:
 - Укажите название и при необходимости описание зоны.
 - При необходимости укажите параметры защиты сетевой зоны от DoS-атак для протоколов TCP (SYN-флуд), UDP, ICMP соответственно:
 - Установите флажок **Включено** для включения защиты.

- При необходимости установите флажок **Агрегировать** для суммарного подсчета всех входящих пакетов. Если флажок не установлен, пакеты учитываются отдельно для каждого IP-адреса.
- В поле **Порог уведомления** укажите количество запросов с одного IP-адреса, при превышении которого в системном журнале будет сгенерирована запись о событии.

Рекомендованное значение — 3000 пакетов/сек.

- В поле **Порог отбрасывания пакетов** укажите количество запросов с одного IP-адреса, при превышении которого будут отброшены пакеты, поступившие с этого IP-адреса, с регистрацией события в системном журнале.

Рекомендованное значение — 6000 пакетов/сек. Для протокола UDP необходимо увеличить это значение, если через интерфейсы зоны проходит трафик таких сервисов, как IP-телефония или L2TP VPN.

- При необходимости в блоке параметров **Исключения защиты от DoS** добавьте IP-адреса узлов, к которым не следует применять ограничения. Это может понадобиться, например, для серверов IP-телефонии, генерирующих интенсивный поток UDP-пакетов.

ПримечаниеРекомендуется включать защиту от DoS-атак для каждой сетевой зоны.

3. При необходимости на вкладке **Контроль доступа** укажите сервисы, которые будут доступны подключенным к зоне клиентам.

Важно! Не рекомендуется разрешать доступ к сервисам для зон, подключенных к недоверенным сетям (например, к интернету).

Примечание Вы можете дополнительно ограничить доступ к каждому сервису, указав разрешенные диапазоны IP-адресов или географические регионы (GeoIP).

4. При необходимости на вкладке **Защита от IP-спуфинга** включите защиту и укажите для зоны разрешенные диапазоны IP-адресов или географические регионы (GeoIP). Сетевые пакеты, поступающие с IP-адресов, не входящих в разрешенный список, будут отброшены.

При включении инвертирования (соответствует логическому отрицанию) указанные диапазоны IP-адресов будут запрещены для сетевой зоны.

Примечание Например, можно указать диапазоны «серых» IP-адресов (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) и установить флажок «Инвертировать».

5. При необходимости на вкладке **Ограничение сессий** включите ограничение и укажите максимальное количество активных сессий для одного IP-адреса.

Примечание В блоке параметров «Исключения» вы можете добавить список IP-адресов, для которых ограничение не будет действовать.

6. Нажмите **Сохранить**.

Documentation: ☒
Product: LogAn
Version: 7.x

Раздел **Интерфейсы** отображает все физические и виртуальные интерфейсы, имеющиеся в системе, позволяет менять их настройки и добавлять VLAN и бонд-интерфейсы.

ПримечаниеДля работы LogAn достаточно одного настроенного интерфейса. Разделение функций управления устройством и сбора данных на разные сетевые интерфейсы рекомендовано для обеспечения безопасности, но не является жестким требованием.

Кнопка **Редактировать** позволяет изменять параметры сетевого интерфейса:

- Включить или отключить интерфейс.
- Указать тип интерфейса — Layer 3.
- Назначить зону интерфейсу.
- Изменить физические параметры интерфейса — MAC-адрес, размер MTU, размер MSS.
- Выбрать тип присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.

Кнопка **Добавить** позволяет добавить следующие типы логических интерфейсов:

- VLAN.
- Бонд.

Создание интерфейса VLAN

С помощью кнопки **Добавить VLAN** администратор может создавать сабинтерфейсы. При создании VLAN необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает VLAN.
Название	Название VLAN. Название присваивается автоматически на основе имени физического порта и тега VLAN.
Описание	Опциональное описание интерфейса.
Тип интерфейса	Указать тип интерфейса — Layer 3 или Mirror.
Тег VLAN	Номер сабинтерфейса. Допускается создание до 4094 интерфейсов.
Имя узла	Имя узла в кластере, на котором создается данный VLAN.
Интерфейс	Физический интерфейс, на котором создается VLAN.
Зона	Зона, которой принадлежит VLAN.
Алиас/Псевдоним	Альтернативное имя интерфейса, заданное администратором. Параметр является опциональным и используется для работы с SNMP. Значение параметра — строка длиной не более 64-х символов. Важно! Значение параметра не может содержать символы кириллицы.
Сеть	Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Возможность изменить MAC-адрес, размер MTU, размер MSS (доступно начиная с релиза ПО 7.3.x).

Объединение интерфейсов в бонд

С помощью кнопки **Добавить бонд-интерфейс** администратор может объединить несколько физических интерфейсов в один логический агрегированный интерфейс для повышения пропускной способности или для отказоустойчивости канала. При создании бонда необходимо указать следующие параметры:

Наименование	Описание
Вкл	Включает бонд.
Название	Название бонда.
Зона	Зона, к которой принадлежит бонд.
Интерфейсы	Один или более интерфейсов, которые будут использованы для построения бонда.
Режим	Режим работы бонда должен совпадать с режимом работы на том устройстве, куда подключается бонд. Может быть: • Round robin. Пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости. • Active backup. Только один сетевой интерфейс из объединенных будет активным. Другой интерфейс может стать активным только в том случае, когда упадет текущий активный интерфейс. При такой политике MAC-адрес бонд-интерфейса виден снаружи только через один сетевой порт, во избежание появления проблем с коммутатором. Эта политика применяется для отказоустойчивости. • XOR. Передача распределяется между сетевыми картами используя формулу: [(«MAC-адрес источника» XOR «MAC-адрес назначения») по модулю «число интерфейсов»]. Получается, одна и та же сетевая карта передает пакеты одним и тем же получателям. Опционально распределение передачи может быть основано и на политике «xmit_hash». Политика XOR применяется для балансировки нагрузки и отказоустойчивости. • Broadcast. Передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости. • IEEE 802.3ad — режим работы, установленный по умолчанию, поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Выбор, через какой интерфейс отправлять пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать «xmit_hash» политику. • Adaptive transmit load balancing . Исходящий трафик распределяется в зависимости от загруженности каждой сетевой карты (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущую сетевую карту. Если она выходит из строя, то другая сетевая карта берет себе MAC-адрес вышедшей из строя карты. • Adaptive load balancing . Включает в себя предыдущую политику плюс осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт наружу, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом, различные пиры используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами.
MII monitoring period (мсек)	Устанавливает периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. Значение по умолчанию — 0 — отключает MII-мониторинг.
Down delay (мсек)	Определяет время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0.
Up delay (мсек)	Задаёт время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0.
LACP rate	Определяет, с каким интервалом будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения: • Slow — запрос партнера на передачу LACPDU-пакетов каждые 30 секунд. • Fast — запрос партнера на передачу LACPDU-пакетов каждую 1 секунду.

Наименование	Описание
Failover MAC	Определяет, как будут прописываться MAC-адреса на объединенных интерфейсах в режиме active-backup при переключении интерфейсов. Обычным поведением является одинаковый MAC-адрес на всех интерфейсах. Возможные значения: • Отключено — устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения. • Active — MAC-адрес на бонд-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на бонд-интерфейсе меняется во время обработки отказа. • Follow — MAC-адрес на бонд-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. На втором и последующем интерфейсе этот MAC не устанавливается, пока они в резервном режиме. MAC-адрес прописывается во время обработки отказа, когда резервный интерфейс становится активным, он принимает новый MAC (тот, что на бонд-интерфейсе), а старому активному интерфейсу прописывается MAC, который был на текущем активном.
Xmit hash policy	Определяет хэш-политику передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения: • Layer 2 — использует только MAC-адреса для генерации хэша. При этом алгоритме трафик для конкретного сетевого хоста будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad. • Layer 2+3 — использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad. • Layer 3+4 — используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хэша. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефрагментированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут прийти до получателя не в том порядке, так как отправляются через разные интерфейсы.
Сеть	Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP. Возможность изменить MAC-адрес, размер MTU, размер MSS (доступно начиная с релиза ПО 7.3.x).

Маршруты

Documentation: ☒
Product: LogAn
Version: 7.x

Данный раздел позволяет указать маршрут в сеть, доступную за определенным маршрутизатором. Например, в локальной сети может быть маршрутизатор, который объединяет несколько IP-подсетей.

Для добавления маршрута необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Задать название и описание данного маршрута	В разделе Сеть выберите в меню Маршруты , нажмите кнопку Добавить . Укажите имя для данного маршрута. Опционально можно задать описание маршрута.
Шаг 2. Указать адрес назначения	Задайте подсеть, куда будет указывать маршрут, например, 172.16.20.0/24 или 172.16.20.5/32.
Шаг 3. Указать шлюз	Задайте IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с сервера LogAn.
Шаг 4. Указать интерфейс	Выберите интерфейс, через который будет добавлен маршрут. Если оставить значение Автоматически , то LogAn сам определит интерфейс, исходя из настроек IP-адресации сетевых интерфейсов.
Шаг 5. Указать метрику	Задайте метрику маршрута. Чем меньше метрика, тем приоритетней маршрут в данную сеть, если маршрутов несколько.

Настройка шлюзов

Documentation: ☒
Product: LogAn
Version: 7.x

Для подключения LogAn к Интернету необходимо указать IP-адрес одного или нескольких шлюзов.

Можно указать несколько шлюзов, если для подключения к Интернету используется несколько провайдеров. Пример настройки сети с двумя провайдерами:

- Интерфейс port1 с IP-адресом 192.168.11.2 подключен к Интернет-провайдеру 1. Для выхода в Интернет с этого провайдера необходимо добавить шлюз с IP-адресом 192.168.11.1
- Интерфейс port2 с IP-адресом 192.168.12.2 подключен к Интернет-провайдеру 2. Для выхода в Интернет с этого провайдера необходимо добавить шлюз с IP-адресом 192.168.12.1

При наличии двух или более шлюзов возможны 2 варианта работы:

Наименование	Описание
Балансировка трафика между шлюзами	Установить флажок Балансировка и указать Вес каждого шлюза. В этом случае весь трафик в Интернет будет распределен между шлюзами в соответствии с указанными весами (чем больше вес, тем большая доля трафика идет через шлюз).
Основной шлюз с переключением на запасной	Выбрать один из шлюзов в качестве основного и настроить Проверку сети , нажав на одноименную кнопку в интерфейсе. Проверка сети проверяет доступность хоста в Интернет с указанной в настройках периодичностью, и в случае, если хост перестает быть доступен, переводит весь трафик на запасные шлюзы в порядке их расположения в консоли.

По умолчанию проверка доступности сети настроена на работу с публичным DNS-сервером Google (8.8.8.8), но может быть изменена на любой другой хост по желанию администратора.

