

Table of Contents

Table of Contents	1
Библиотеки элементов	2
Общие сведения	3
Сервисы	4
Группы сервисов	5
IP-адреса	6
Списки URL	8
Календари	10
Полосы пропускания	11
Шаблоны страниц	12
Приложения	14
Профили приложений	18
Группы приложений	24
Почтовые адреса	25
Номера телефонов	26
Сигнатуры COB	27
Профили COB	31
Профили оповещений	34
Профили NetFlow	35
Профили LLDP	36
Профили SSL	37
Профили BFD	40
Syslog-фильтры UserID агента	42

Общие сведения

Version: 8.x

Product: DCFW

Данный большой раздел содержит в себе все записи, адреса-сайтов, IP-адреса, шаблоны и прочие элементы, которые используются при настройке правил UserGate DCFW.

Первоначальные данные библиотек поставляются вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Некоторые элементы библиотек являются нередактируемыми, потому что поставляются и поддерживаются разработчиками UserGate. Библиотеки элементов, поставляемые UserGate, имеют механизм автоматического обновления. Автоматическое обновление элементов требует наличия специальной лицензии. Более подробно о лицензии на продукт вы можете прочитать в главе [Лицензирование](#).

Сервисы

Product: DCFW
Version: 8.x

Раздел сервисы содержит список общеизвестных сервисов, основанных на протоколе TCP/IP, например, таких, как HTTP, HTTPS, FTP и другие. Данные сервисы могут быть использованы при построении правил DCFW. Первоначальный список сервисов поставляются вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового сервиса необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать сервис.	Нажать на кнопку Добавить , дать сервису название, ввести комментарий.
Шаг 2. Указать протокол и порт.	Нажать на кнопку Добавить , выбрать из списка необходимый протокол, указать порты назначения и, опционально, порты источника. Для указания диапазона портов можно использовать — (тире), например, 33333—33355.

Группы сервисов

Product: DCFW

Version: 8.x

В этом разделе вы можете управлять (создавать, обновлять, удалять) группами объектов сервисов. Группы сервисов могут быть использованы при настройке политик безопасности DCFW.

Для создания группы сервисов:

1. В разделе **Настройки → Библиотеки → Группы сервисов** в блоке **Группы сервисов** нажмите **Добавить** и укажите название и произвольное описание создаваемой группы.
2. В блоке **Элементы** нажмите **Добавить** и выберите сервисы для добавления в группу. Для добавления всех сервисов нажмите **Добавить все**.

IP-адреса

Product: DCFW
Version: 8.x

Раздел IP-адреса содержит список диапазонов IP-адресов, которые могут быть использованы при построении правил DCFW. Первоначальный список адресов поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового списка адресов необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать список.	На панели Группы нажать на кнопку Добавить , дать название списку IP-адресов.
Шаг 2. Указать адрес обновления списка (не обязательно).	Указать адрес сервера, где находится обновляемый список. Более подробно об обновляемых списках смотрите далее в этой главе.
Шаг 3. Добавить IP-адреса.	На панели Адреса из выбранной группы нажать на кнопку Добавить и ввести адреса. IP-адреса вводятся в виде IP-адрес, IP-адрес/маска сети или диапазон IP-адресов, например: 192.168.1.5, 192.168.1.0/24 или 192.168.1.5-192.168.2.100.

Администратор имеет возможность создавать свои списки IP-адресов и централизованно распространять их на все межсетевые экраны UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми IP-адресами.	Создать файл list.txt со списком адресов. Список адресов записывается в обычный текстовый файл, где адреса прописываются в столбик без знаков препинания. Например: x.x.x.x y.y.y.y z.z.z.z
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.

Наименование	Описание
Шаг 5. Создать список IP-адресов и указать URL для обновления.	На каждом DCFW создать список IP-адресов. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. DCFW будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Примечание URL списка задается в формате: http://x.x.x.x/ или ftp://x.x.x.x/. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "**/2" в поле "часы" будет означать "каждые два часа".

Списки URL

Product: DCFW
Version: 8.x

Страница предназначена для задания списков указателей URL, которые могут быть использованы в правилах контентной фильтрации в качестве черных и белых списков.

Компания UserGate предоставляет собственные обновляемые списки. Для использования этих списков необходима соответствующая лицензия. Более подробно о лицензии на продукт вы можете прочитать в главе [Лицензирование](#).

Наименование	Описание
Список поисковых систем без безопасного поиска	Список известных поисковых систем, на которых отсутствует возможность блокировки поисковых запросов взрослого содержания. Рекомендуется блокировать такие поисковики для целей родительского контроля.
Соответствие списку запрещенных URL Министерства Юстиции РФ	Данный список содержит URL, запрещенные Министерством Юстиции Российской Федерации.
Соответствие списку запрещенных URL Республики Казахстан	Единый реестр доменных имен, указателей страниц сайтов в сети интернет и сетевых адресов, содержащих информацию, распространение которой запрещено в Республике Казахстан.
Список образовательных учреждений	Список доменных имен образовательных учреждений РФ.
Список фишинговых сайтов	Данный список содержит URL фишинговых сайтов.
Соответствие реестру запрещенных сайтов Роскомнадзора (URL)	Единый реестр указателей страниц сайтов в сети интернет, содержащих информацию, распространение которой в Российской Федерации запрещено. Данный список доступен на сайте http://eais.rkn.gov.ru .
Соответствие реестру запрещенных сайтов Роскомнадзора (домены)	Единый реестр доменных имен, содержащих информацию, распространение которой в Российской Федерации запрещено. Данный список доступен на сайте http://eais.rkn.gov.ru .

Администратор имеет возможность создавать собственные списки и централизованно распространять их на все межсетевые экраны UserGate. Для создания таких списков необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимым списком URL.	Создать текстовый файл list.txt со списком URL в следующем формате: www.site1.com/url1 www.site2.com/url2 ... www.siteend.com/urlN
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.

Наименование	Описание
Шаг 5. Создать список и указать URL для обновления.	На каждом DCFW создать список URL. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. DCFW будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Примечание URL списка задается в формате: <code>http://x.x.x.x/</code> или <code>ftp://x.x.x.x/</code>. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*" / 2 в поле "часы" будет означать "каждые два часа".

Календари

Product: DCFW
Version: 8.x

Календари позволяют создать временные интервалы, которые затем можно использовать в различных правилах DCFW. Первоначальный список поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления нового календаря необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать календарь.	В панели Группы нажать на кнопку Добавить , указать название календаря и его описание.
Шаг 2. Добавить временные интервалы в календарь.	В панели Элементы нажать на кнопку Добавить и добавить интервал. Дать название интервалу и указать время.

Полосы пропускания

Product: DCFW
Version: 8.x

Элемент библиотеки **Полоса пропускания** определяет скорость передачи данных, которую возможно в дальнейшем использовать в правилах управления полосой пропускания. Более подробно о правилах управления полосой пропускания смотрите в главе [Пропускная способность](#).

Первоначальный список поставляется вместе с продуктом. Администратор может добавлять необходимые ему элементы в процессе работы. Для добавления новой полосы пропускания необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать полосу пропускания.	Нажать на кнопку Добавить , дать название, описание.
Шаг 2. Указать скорость.	Указать скорость в Кбит/сек.
Шаг 3. Указать значение DSCP для QoS.	Необязательный параметр. Если установлен, то будет прописываться в каждый IP пакет. Диапазон от 0 до 63.

Шаблоны страниц

Product: DCFW

Version: 8.x

С помощью шаблонов страниц вы можете настраивать отображение страниц блокировки, авторизации, предупреждений и сетевых ошибок. Список шаблонов страниц, которые поставляются с UserGate DCFW, — см. в таблице ниже.

Шаблон	Описание
Blockpage (EN) и Blockpage (RU)	Стандартные шаблоны блокировки на английском и русском языках
Captive portal user auth (EN) и Captive portal user auth (RU)	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках. Шаблон выводит форму авторизации пользователя (имя и пароль). При успешной авторизации пользователь получает доступ в Интернет
Captive portal user auth + policy (EN) и Captive portal user auth + policy (RU)	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках. Шаблон выводит форму авторизации пользователя (имя и пароль), правила пользования сетью (соглашение об использовании), а также требует принятия пользователем правил политики доступа. При успешной авторизации пользователь получает доступ в Интернет
Captive portal: email auth (EN) и Captive portal: email auth (RU)	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках, позволяющие пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя письмом по email. Для корректной работы данных шаблонов необходимо настроить раздел Оповещения в Captive-профиле
Captive portal: SMS auth (EN) и Captive portal: SMS auth (RU)	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках, позволяющие пользователю самостоятельно зарегистрироваться в системе с подтверждением пользователя с помощью SMS. Для корректной работы данных шаблонов необходимо настроить раздел Оповещения в Captive-профиле
Captive portal policy (EN) и Captive portal policy (RU)	Шаблоны для авторизации пользователя с помощью Captive-портала на английском и русском языках. Шаблон не требует ввода имени и пароля пользователя, а выводит правила пользования сетью (соглашение об использовании) и требует принятия пользователем правил политики доступа. При согласии с политикой доступа пользователь получает доступ в интернет. Для работы данного шаблона требуется установить метод Принять политику в качестве метода аутентификации в Captive-профиле
Captive portal user session (EN) и Captive portal user session (RU)	Шаблоны на английском и русском языках, с помощью которых пользователь может завершить свою авторизованную сессию, перейдя на страницу http://logout.captive или http://USERGATE_IP/cps
FTP client (EN) и FTP client (RU)	Шаблоны на английском и русском языках для отображения контента FTP-серверов поверх HTTP
SSL VPN RDP (EN) и (RU)	Шаблоны на английском и русском языках для отображения страницы аутентификации при подключении к ресурсам RDP через веб-портал
SSL VPN SSH (EN) и (RU)	Шаблоны на английском и русском языках для отображения страницы аутентификации при подключении к ресурсам SSH через веб-портал
TOTP INIT PAGE (EN) и TOTP INIT PAGE (RU)	Шаблоны на английском и русском языках для отображения страницы инициализации устройства TOTP для VPN-пользователей

Настройка шаблона страницы блокировки

По умолчанию шаблон страницы блокировки настроен на отображение следующей информации:

- Сведения о блокирующем правиле;
- Сведения об угрозе;
- Категория URL;
- Морфологические категории;

- Кнопка запроса добавления URL в белый список.

Но в HTML-коде шаблона страницы блокировки содержатся дополнительные блоки информации или интерактивных элементов, которые по умолчанию закомментированы. В режиме редактирования HTML-кода в шаблон блокировки можно добавить следующие сведения и формы:

- Поле для указания причины добавления URL в белый список.
- Дата блокировки.
- IP-адрес пользователя, отправившего запрос, который был заблокирован.
- Имя узла UserGate DCFW, заблокировавшего запрос.
- Названия групп, в которых состоит пользователь.
- Форма ввода логина и пароля администратора для снятия блокировки

Чтобы создать пользовательский шаблон страницы блокировки:

1. В разделе **Настройки → Библиотеки → Шаблоны страниц** нажмите **Добавить** и выберите **Страница блокировки**.
2. Выберите из списка созданный шаблон и нажмите **Экспорт**. На ПК загрузится шаблон в формате HTML-страницы.
3. Используя текстовый редактор, откройте страницу, найдите закомментированные блоки для отображения дополнительных сведений и раскомментируйте нужные.

Примечание Не рекомендуется использовать специальные редакторы, предназначенные для редактирования HTML-файлов, поскольку они могут изменить внутреннюю структуру шаблона.

4. Импортируйте измененную страницу в созданный шаблон.

Настройка пользовательского оформления страниц

По умолчанию шаблоны страниц настроены на отображение сведений в стандартном оформлении. Вы можете использовать шаблоны в качестве основы для создания пользовательских шаблонов в собственном стиле, например в стиле вашей организации.

Чтобы настроить оформление страницы:

1. В разделе **Настройки → Библиотеки → Шаблоны страниц** нажмите **Добавить** и создайте шаблон страницы нужного типа.
2. Выберите из списка созданный шаблон и нажмите **Экспорт**. На ПК загрузится шаблон в формате HTML-страницы.
3. Используя текстовый редактор, откройте страницу и отредактируйте HTML-код для настройки собственного оформления.

Примечание Не рекомендуется использовать специальные редакторы, предназначенные для редактирования HTML-файлов, поскольку они могут изменить внутреннюю структуру шаблона.

4. Импортируйте измененную страницу в созданный шаблон.

Product: DCFW
Version: 8.x
Technology: L7

Сигнатуры приложений представляют собой совокупность семантических выражений, с помощью которых описываются характерные признаки определенных сетевых приложений. Они используются в межсетевом экране для анализа трафика на 7 уровне модели OSI для контроля сетевого трафика.

Типы сигнатур приложений

В UserGate могут использоваться два типа сигнатур приложений:

- Проприетарные сигнатуры приложений.
- Кастомизированные сигнатуры приложений.

Проприетарные сигнатуры приложений создаются разработчиками UserGate и автоматически добавляются в библиотеку системы при наличии соответствующей лицензии. В списке сигнатур в библиотеке такие сигнатуры помечаются в колонке **Владелец** как: @UserGate.

Кастомизированные сигнатуры приложений создаются самим пользователем. Для создания пользовательской сигнатуры приложений в веб-консоли администратора необходимо перейти в раздел **Библиотеки → Приложения** и нажать на кнопку **Добавить**. Далее заполняются поля с параметрами сигнатуры, описываются признаки сигнатуры с помощью [синтаксиса UASL](#).

Необходимо заполнить следующие поля:

Наименование	Описание
Тип	Тип сигнатуры; • Приложение. • Протокол. • Поддержка — вспомогательная сигнатура.
Id	ИИдентификатор сигнатуры. Если поле оставить пустым, то будет выдан свободный id из пользовательского пула.
Название	Название сигнатуры.
Описание	Описание сигнатуры.
Уровень угрозы	Уровень угрозы, определяемый сигнатурой. Определены следующие значения: • 1 — очень низкий. • 2 — низкий. • 3 — средний. • 4 — высокий. • 5 — очень высокий.
Технология	Технология приложения: • browser-based — браузерное веб-приложение. • client-server — клиент-серверное приложение. • network-protocol — сетевой протокол. • peer-to-peer — приложение точка-точка.

Наименование	Описание
Категория	Категория сигнатуры приложений — группа сигнатур, объединенных общими параметрами. Список категорий приложений может быть пополнен. • Media streaming • Email • Coin Miners • Tunneling • Games • Remote access • Conferencing • Trojan Horses • Business • Mobile • Proxies and anonymizers • Standard networks • VOIP • Web posting • Software update • File storage and backup • Web browsing • File sharing P2P • Instant messaging • Social networking
UASL	Описание признаков сигнатуры с помощью синтаксиса UASL .

Сигнатуры приложений, зависимые от типа протокола

Некоторые сигнатуры приложений для своей работы в профилях приложений требуют наличия сигнатур определенного протокола.

В следующей таблице представлены такие зависимости:

Сигнатура протокола	ID зависимых сигнатур

Сигнатура протокола	ID зависимых сигнатур
SSL/TLS (id=19)	185, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 198, 199, 200, 201, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 267, 268, 269, 270, 271, 272, 273, 275, 276, 277, 278, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 437, 439, 440, 441, 443, 444, 445, 446, 449, 450, 451, 458, 459, 465, 466, 470, 471, 472, 474, 475, 477, 481, 482, 485, 486, 487, 490, 492, 494, 495, 496, 501, 502, 504, 505, 511, 512, 513, 515, 516, 517, 518, 521, 524, 525, 526, 527, 528, 531, 532, 535, 536, 537, 538, 539, 544, 549, 550, 552, 554, 556, 557, 560, 563, 564, 566, 567, 568, 576, 577, 579, 581, 585, 589, 590, 592, 595, 596, 597, 600, 601, 603, 604, 606, 607, 610, 612, 613, 617, 621, 622, 623, 625, 627, 632, 635, 636, 638, 710, 730, 731, 734, 738, 739, 744, 746, 748, 752, 753, 754, 755, 756, 759, 760, 761, 762, 763, 766, 769, 770, 771, 772, 773, 774, 775, 776, 781, 783, 785, 788, 790, 795, 797, 800, 801, 807, 808, 810, 811, 813, 815, 817, 818, 820, 822, 825, 826, 831, 832, 833, 835, 836, 837, 841, 842, 846, 847, 848, 850, 851, 852, 853, 854, 858, 859, 860, 863, 864, 867, 869, 872, 874, 875, 877, 878, 879, 880, 883, 885, 887, 888, 891, 893, 894, 895, 897, 898, 899, 902, 903, 904, 905, 908, 909, 1967, 2027, 4062, 4082, 4437, 4459, 5294, 5301, 5317, 5321, 5323, 5324, 5385, 5395, 5407, 5431, 5506, 5637, 5641, 5644, 5645, 5649, 5650, 5652, 5654, 5656, 5658, 5668, 5671, 5673, 5674, 5675, 5676, 5678, 5679, 5680, 5681, 5688, 5692, 5693, 5695, 5699, 5710, 5711, 5715, 5719, 5730, 5736, 5739, 5740, 5742, 5744, 5750, 5762, 5765, 5769, 5770, 5773, 5776, 5777, 5778, 5786, 5791, 5792, 5794, 5795, 5800, 5804, 5809, 5810, 5812, 5813, 5815, 5816, 5820, 5822, 5823, 5825, 5826, 5827, 5828, 7688, 7689, 7690, 7691, 7692, 7694, 7695, 7698, 7699, 7704, 7705, 7707, 7708, 7740, 7843, 7864, 7865, 7867, 7868, 8000, 8001, 8002, 8003, 8004, 8005, 8006, 8007, 8009, 8010, 8011, 8012, 8014, 8015, 8016, 8017, 8018, 8019, 8022, 8024, 8026, 8027, 8028, 8031, 8032, 8033, 8034, 8035, 8036, 8037, 8038, 8039, 8040, 8041, 8043, 8044, 8045, 8048, 8049, 8053, 8054, 8055, 8056, 8057, 8058, 8059, 8060, 8063, 8064, 8066, 8067, 8069, 8070, 8071, 8075, 8077, 8078, 8079, 8080, 8081, 8082, 8083, 8084, 8086, 8087, 8088, 8089, 8090, 8091, 8092, 8094, 8095, 8096, 8098, 8099, 8101, 8102, 8103, 8104, 8105, 8106, 8107, 9003, 9007, 9008, 9016, 9019, 9030, 9042, 9044, 9048, 9050, 9051, 9052, 9053, 9054, 9055, 9056, 9057, 9058, 9059, 9060, 9061, 9062, 9063, 9064, 9065, 9066, 9067, 9068, 9069, 9071, 9072, 9074, 9075, 9076, 9077, 9078, 9079, 9080, 9081, 9083, 9084, 9085, 9086, 9087, 9088, 9089, 9090, 9091, 9092, 9094, 9096, 9097, 9098, 9099, 9100, 9101, 9102, 9103, 9104, 9105, 9114, 9128, 9141, 9147, 9148, 9150, 9529, 9543, 9544, 9553, 9563, 9566, 9572, 9573, 9575, 9579, 9580, 9622, 9625, 9627, 9628, 9641, 9650, 9655, 9657, 9714, 9733, 10514, 11011, 11024, 11025, 11044, 11504, 12001, 12002, 12003, 12006, 12007, 12008, 12009, 12010, 12011, 12012, 12013, 12014, 12015, 12016, 12017, 12018, 12019, 12020, 12021, 12022, 12023, 12024, 12025, 12026, 12027, 12028, 12033, 12034, 12035, 12036, 12044, 12045, 12501, 14002, 14003
HTTP (id=3)	196, 239, 261, 475, 532, 535, 610, 612, 627, 710, 1967, 4133, 4340, 4441, 5323, 5395, 5506, 5655, 5672, 5674, 5676, 5693, 5728, 5730, 5750, 5754, 5763, 5769, 5770, 5773, 5778, 5788, 5792, 5823, 5830, 7867, 8002, 8013, 8048, 9777, 9823, 9824, 9845, 11027, 12032, 12033
DNS (id=5)	1967, 5395, 5672, 5815
IKE (id=11041)	11056

Связанные сигнатуры

Некоторые сигнатуры зависят не только от сигнатуры протокола, но и от связанных сигнатур.

Список связанных сигнатур приложений приведен в следующей таблице:

ID сигнатуры	Название сигнатуры	Зависит от протокола	Связана с сигнатурой	Примечание
218	Yandex.Disk	SSL/TLS (id=19)	—	Для работы данной сигнатуры в профиль необходимо добавить только сигнатуру протокола (id=19).
7707	Yandex.Disk download	SSL/TLS (id=19)	Yandex.Disk (id=218), Yandex Services (id=12044)	Для работы данной сигнатуры в профиль необходимо добавить сигнатуру протокола (id=19), а также связанные сигнатуры (id=218 и id=12044).
7708	Yandex.Disk upload	SSL/TLS (id=19)	Yandex.Disk (id=218), Yandex Services (id=12044)	Для работы данной сигнатуры в профиль необходимо добавить сигнатуру протокола (id=19), а также связанные сигнатуры (id=218 и id=12044).
12044	Yandex Services	SSL/TLS (id=19)	—	Для работы данной сигнатуры в профиль необходимо добавить только сигнатуру протокола (id=19).
16020	Yandex Tracker	SSL/TLS (id=19)	Yandex Services (id=12044)	Для работы данной сигнатуры в профиль необходимо добавить сигнатуру протокола (id=19), а также связанную сигнатуру (id=12044).
12045	Yandex Cloud	SSL/TLS (id=19)	Yandex Services (id=12044)	Для работы данной сигнатуры в профиль необходимо добавить сигнатуру протокола (id=19), а также связанную сигнатуру (id=12044).

Product: DCFW

Version: 8.x

Technology: L7

Назначение профиля приложений

Профиль приложений позволяет создавать динамический набор [сигнатур приложений](#), предназначенный для анализа трафика на 7 уровне модели OSI. Динамичность профиля достигается за счет того, что профиль явно не содержит в себе никаких сигнатур, а содержит фильтры, с помощью которых собирается набор сигнатур. При изменении библиотеки сигнатур приложений профили динамически наберут новые наборы сигнатур, удовлетворяющих фильтрам профилей.

Помимо создания необходимого набора сигнатур в профиле могут определяться действия, которые необходимо выполнить над приложениями, отфильтрованными сигнатурами и действия, которые должны быть применены к трафику, который не удалось идентифицировать.

Создание профиля приложений в веб-консоли администратора

В веб-консоли администратора профили приложений создаются в разделе **Библиотеки → Профили приложений**.

Необходимо нажать **Добавить** и заполнить соответствующие поля в свойствах профиля приложений:

1. В поле **Название** указать название создаваемого профиля.
2. В поле **Описание** опционально указать назначение профиля.
3. В области **Фильтры** добавляются фильтры для выбора необходимых сигнатур из библиотеки и настраиваются действия, которые необходимо выполнить над приложениями, отфильтрованными сигнатурами.
4. В области **Настройки сигнатуры неопределенных приложений** определяются действия с трафиком, который не был определен сигнатурами данного профиля.
5. На вкладке **Совпавшие сигнатуры** отображается превью сигнатур приложений, отобранных всеми фильтрами профиля, и настроенные действия, которые необходимо выполнить над приложениями, отфильтрованными этими сигнатурами.

Настройка фильтров сигнатур в профиле приложений

Для создания фильтра сигнатур приложений необходимо в области **Фильтры** нажать кнопку **Добавить**. Откроется окно свойств фильтра.

Фильтр можно создать, выбирая опции отбора в панели инструментов. Ниже в окне будут отображаться сигнатуры из библиотеки, попадающие под действие этого фильтра:

Также фильтр можно создать, описав его с помощью sql-подобного синтаксиса. Для этого необходимо нажать кнопку **Расширенный** в панели инструментов и в открывшейся строке описать свойства выбора фильтра:

--

В каждом фильтре могут настраиваться состояния сигнатур и действия, которые применяются ко всем сигнатурам, попадающим под него:

- Включение/отключение сигнатуры.
- Включение/отключение журналирования сигнатуры.
- Запись в рсар-файл, если сигнатура сработала.
- Предпринимаемое действие над трафиком, если сигнатура сработала, т.е. приложение было найдена в трафике. Действия могут быть следующие: пропустить, отбросить, отбросить с разрывом TCP соединения, заблокировать IP-адрес источника и/или назначения.

Для сохранения созданного фильтра необходимо нажать кнопку **Сохранить**.

В одном профиле может быть создано сразу несколько фильтров.

Фильтры в профиле работают по правилу логического ИЛИ.

Порядок фильтров сигнатур в профиле важен - настройки верхнего фильтра имеют высший приоритет. Например, если в библиотеку сигнатур приложений будут добавлены новые сигнатуры и они попадут под действие сразу нескольких фильтров одного профиля, им будет присвоено настроенное действие первого фильтра, под который они попадают.

Настройка действий для трафика, который не удалось идентифицировать

В профиле приложений может быть настроено действие, которое применяется к трафику, который не удалось идентифицировать с помощью набора сигнатур профиля.

В области **Настройки сигнатуры неопределенных приложений** настраивается действие, включается/отключается журналирование и запись в файл рсар.

Действия могут быть следующие: пропустить, отбросить, отбросить с разрывом TCP соединения.

Примеры настроек профилей приложений

Пример 1. Профиль приложения с сигнатурой, зависимой от сигнатуры протокола

Списки сигнатур, зависящих от сигнатур протоколов, приведены в разделе [Приложения](#).

Создадим профиль для приложения Kontur Talk, которое определяется соответствующей сигнатурой (id=14002). Чтобы запретить весь трафик, кроме трафика приложения Kontur Talk, профиль приложений должен выглядеть следующим образом:



Сигнатура SSL/TLS (id=19) необходима для работы сигнатуры Kontur Talk, поэтому она добавляется в профиль, но для нее выставляется действие **Отбросить**, чтобы не пропускать посторонний трафик по протоколам SSL/TLS. Для неидентифицированного трафика также устанавливается действие **Отбросить**.

Пример 2. Профиль для белого списка со связанными сигнатурами

Списки связанных сигнатур приведены в разделе [Приложения](#).

Создадим профиль для случая, когда необходимо разрешить загрузку файлов на Yandex Disk. Для того, чтобы сигнатура Yandex.Disk upload работала, необходимо учесть её зависимость от сигнатуры протокола SSL/TLS (id=19) и связанность с сигнатурами Yandex.Disk (id=218) и Yandex Services (id=12044). В данном примере профиль приложений будет выглядеть следующим образом:



Таким образом разрешается доступ и загрузка файлов на Yandex Disk, а весь остальной трафик помечается как неидентифицированный и отбрасываться либо действием сигнатуры SSL/TLS, либо действием для сигнатур неопределенных приложений.

Пример 3. Профиль для черного списка со связанными сигнатурами

В данном примере разрешается весь трафик, кроме попадающего под сигнатуру Yandex.Disk upload (id=7708). Для этого случая необходимо учесть зависимость сигнатуры Yandex. Disk upload от сигнатуры протокола SSL/TLS (id=19). Связанность с сигнатурами Yandex.Disk и Yandex Services **в случае блокировки не учитывается**. Профиль приложений в данном примере будет выглядеть следующим образом:



Таким образом запрещается загрузка файлов на Yandex Disk, а весь остальной трафик разрешается либо действием сигнатуры SSL/TLS, либо действием для сигнатур неопределенных приложений.

Применение профилей приложений

Администратор может создать необходимое количество профилей. Рекомендуется ограничивать количество сигнатур в профиле только теми, которые необходимы для защиты определенного сервиса. Большое количество сигнатур требует большего времени обработки трафика и загрузки процессора.

Профиль приложения применяется в разрешающем правиле [межсетевого экрана](#).

Правила межсетевого экрана обрабатываются сверху вниз и сессия попадает в первое правило, которое удовлетворяет всем условиям в нем (адреса/зоны источника/назначения, пользователи итд.). После попадания под разрешающее правило с профилем приложений, трафик начинает анализироваться с помощью сигнатур профиля. При этом анализируются как прямые, так и обратные пакеты согласно условий в фильтре, независимо от того, откуда устанавливается соединение. При срабатывании сигнатур профиля будет выполнено действие, настроенное в фильтрах профиля и произведена соответствующая запись в [Журнале трафика](#), если была включена опция журналирования. Если ни одна из сигнатур не была найдена, то к трафику будет применено действие, настроенное в профиле для неидентифицированного трафика.

Если срабатывает сигнатура с действием Блокировать IP, то тогда блокируется IP-адрес источника или назначения (в зависимости от настройки) на определенное в настройках время. Заблокированные сигнатурами IP-адреса отображаются на странице **Диагностика и мониторинг** в разделе **Заблокированные СОВ/L7 IP-адреса** (подробнее читайте в разделе [Заблокированные СОВ/L7 IP-адреса](#)).

Группы приложений

Version: 8.x
Product: DCFW

В данном разделе пользователь может управлять (создавать/обновлять/удалять) группами приложений. Группы приложений могут быть использованы при настройке правил управления пропускной способности.

Для создания группы приложений:

Наименование	Описание
Шаг 1. Создать группу.	В разделе Библиотеки → Группы приложений нажать на кнопку Добавить , указать название и, опционально, описание группы приложений.
Шаг 2. Добавить сигнатуры приложений в группу.	На панели Приложения нажать Добавить и выбрать сигнатуры приложений для добавления в группу. Для добавления всех сигнатур приложений использовать кнопку Добавить все .

Почтовые адреса

Product: DCFW
Version: 8.x

Элемент библиотеки **Почтовые адреса** позволяет создать группы почтовых адресов, которые впоследствии можно использовать в правилах фильтрации почтового трафика и для использования в оповещениях.

Для добавления новой группы почтовых адресов необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать группу почтовых адресов.	В панели Группы почтовых адресов нажать на кнопку Добавить , дать название группе.
Шаг 2. Добавить почтовые адреса в группу.	Выделить созданную группу, в панели Почтовые адреса нажать на кнопку Добавить и добавить необходимые почтовые адреса.

Администратор имеет возможность создавать списки почтовых адресов и централизованно распространять их на все межсетевые экраны UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком почтовых адресов.	Создать файл list.txt со списком почтовых адресов.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии базы, например, 3. Необходимо инкрементировать данное значение при каждом обновлении морфологического словаря.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.
Шаг 5. Создать список почтовых адресов и указать URL для обновления.	На каждом DCFW создать список адресов. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. DCFW будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: - Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. - Ежедневно. - Еженедельно. - Ежемесячно. - Каждые ... часов. - Каждые ... минут. - Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Номера телефонов

Product: DCFW
Version: 8.x

Элемент библиотеки **Номера телефонов** позволяет создать группы номеров, которые впоследствии можно использовать в правилах оповещения SMPP.

Для добавления новой группы телефонных номеров необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать группу телефонных номеров.	В панели Группы телефонных номеров нажать на кнопку Добавить , дать название группе.
Шаг 2. Добавить номера телефонов в группу.	Выделить созданную группу, в панели Группа телефонных номеров нажать на кнопку Добавить и добавить необходимые номера.

Администратор имеет возможность создавать списки телефонных номеров и централизованно распространять их на все межсетевые экраны UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком номеров.	Создать файл list.txt со списком номеров.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии базы, например, 3. Необходимо инкрементировать данное значение при каждом обновлении морфологического словаря.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.
Шаг 5. Создать список телефонных номеров и указать URL для обновления.	На каждом DCFW создать список адресов. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. DCFW будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*" / 2 в поле "часы" будет означать "каждые два часа".

Сигнатуры COB

Product: DCFW
Version: 8.x
Technology: IDPS

Сигнатуры COB представляют собой некоторую совокупность строк (паттернов) и семантических выражений (фильтров, модификаторов, иных конструкций), которые позволяют идентифицировать/пометить сетевую атаку и предпринять определенные действия. Сигнатуры добавляются в профили COB и используются в правилах межсетевого экрана для обнаружения вторжений и защиты сети.

В UserGate могут использоваться два типа сигнатур COB:

- Проприетарные сигнатуры.
- Кастомизированные пользовательские сигнатуры.

Проприетарные сигнатуры COB создаются разработчиками UserGate и автоматически добавляются в библиотеку системы при наличии соответствующей лицензии. В списке сигнатур в библиотеке такие сигнатуры помечаются в колонке **Владелец** как: @UserGate. В проприетарных сигнатурах пользователь может перенастроить следующие параметры:

- **Включение/отключение** сигнатуры.
- **Журналирование** сигнатуры.
- **Запись в рсар-файл**, если сигнатура сработала.
- Предпринимаемое **действие**, если сигнатура сработала, т.е. была найдена в трафике. Действия могут быть следующие: пропустить пакет, отбросить пакет, отбросить пакет с разрывом TCP соединения, заблокировать IP-адрес источника и/или назначения.

Дополнительные опциональные параметры проприетарных сигнатур:

- **Применить к** — настраивается, если параметр **Действие** выставлен в значения **Отбросить пакет с разрывом TCP соединения**, **Блокировать IP-адрес источника и/или назначения**. Параметр имеет следующие значения: **Источник**, **Назначение**, **Оба**.
- **Продолжительность** — возможно настроить, если параметр **Действие** имеет значение **Блокировать IP-адрес источника и/или назначения**. Число, указывающее время блокировки ip-адреса.

Некоторые сигнатуры также имеют настройку следующих дополнительных параметров:

- **Направление** — настройка агрегирования по IP-адресу источника или назначения.
- **Частота срабатывания** — количество срабатываний в единицу времени (секунды).

Примеры сигнатур с такими настройками:

1064, 1672, 1711, 1732, 1738, 1740, 1741, 5315, 5611, 5612, 5657, 5699, 5701, 5757,
13003, 17002, 17003, 17004, 45022, 3029251, 3031043, 3031817, 3032798, 3032823,
3033202, 3033935, 3034466, 3035136, 3037395, 3037608, 3037708, 3037771, 3039602,
3039703, 3039876, 3039883, 3040088, 3040443, 3042187, 3046218, 3046453, 3046609,
3049480, 3050453, 3050940, 3051410, 3051613, 3051634, 900000000, 900000001, 900000002,
900000003, 900000004, 900000005, 900000006, 900000007, 900000008, 900000009, 900000010

ПримечаниеВ данном списке приведены примеры сигнатур, которые имеют дополнительные параметры настройки Частота срабатывания и Направление. По мере развития продукта количество таких сигнатур будет увеличиваться.

После изменения настроек параметров по умолчанию у проприетарных сигнатур в колонке **Статус** будет указано: **Изменено**. Измененные пользователем настройки проприетарных сигнатур COB можно вернуть в первоначальное состояние, для этого в веб-консоли администратора в разделе **Библиотеки → Сигнатуры COB** нужно выделить сигнатуру в списке и нажать кнопку **Восстановить по умолчанию**.

Кастомизированные сигнатуры COB создаются самим пользователем.

Для создания кастомизированной сигнатуры COB в веб-консоли администратора необходимо перейти в раздел **Библиотеки → Сигнатуры COB** и нажать на кнопку **Добавить**. Далее заполняются поля с параметрами сигнатуры. Признаки сетевых уязвимостей описываются с помощью синтаксиса языка [UASL](#) (UserGate Application and Security Language).

При создании кастомизированной сигнатуры необходимо заполнить следующие поля:

Наименование	Описание
Включено	Индикатор включения/выключения сигнатуры.
Id	Идентификатор сигнатуры. Если поле оставить пустым, то будет выдан свободный id из пользовательского пула.
Название	Название сигнатуры.

Наименование	Описание
Описание	Описание сигнатуры.
Уровень угрозы	Уровень угрозы, определяемый сигнатурой. Определены следующие значения: • 1 - очень низкий. • 2 - низкий. • 3 - средний. • 4 - высокий. • 5 - очень высокий.
Класс	Класс сигнатуры определяет тип атаки, которая описывается данной сигнатурой. Определяются также общие события, которые не относятся к атаке, но могут быть интересны в определенных случаях, например, обнаружение установления сессии TCP. Список классов может быть пополнен. • arbitrary-code-execution - попытка запуска произвольного кода. • attempted-admin - попытка получения административных привилегий. • attempted-dos - попытка совершения атаки Denial of Service. • attempted-recon - попытка атаки, направленной на утечку данных. • attempted-user - попытка получения пользовательских привилегий. • bad-unknown - потенциально плохой трафик. • buffer overflow - попытка атаки, использующей принцип переполнения буфера. • command-and-control - попытка общения с C&C центром • default-login-attempt - попытка логина с именем/паролем по умолчанию. • denial-of-service - обнаружена атака Denial of Service. • exploit-kit - обнаружен exploit kit • information disclosure - утечка данных. • memory corruption - попытка атаки, использующей принцип повреждения памяти. • misc-activity - прочая активность. • misc-attack - обнаружена атака. • network-scan - сканирование сети. • path traversal - попытка атаки, использующей принцип обхода пути к файлам на сервере, на котором работает приложение. • policy-violation - нарушение сетевых политик. • protocol-command-decode - обнаружение необычной команды протокола. • shellcode-detect - обнаружен исполняемый код. • string-detect - обнаружена подозрительная строка. • successful-recon-limited - утечка информации • suspicious-login - попытка логина с использованием подозрительного имени пользователя. • system-call-detect - попытка использования системных вызовов. • targeted-activity - обнаружение направленной активности. • trojan-activity - обнаружен сетевой троян. • uncaught exception - необрабатываемое приложением исключение.

Наименование	Описание
Категория	Категория сигнатуры - группа сигнатур, объединенных общими параметрами. Список категорий может быть пополнен. • adware pup - нежелательное рекламное ПО. • attack_response - сигнатуры, определяющие ответы на известные сетевые атаки. • bruteforce - атака типа brutr force. • coinminer - скачивание, установка, деятельность известных майнеров. • dns - известные уязвимости DNS. • dos - сигнатуры известных Denial of services атак. • exploit - сигнатуры известных эксплоитов. • ftp - известные FTP-уязвимости. • icmp - известные уязвимости протокола icmp. • imap - известные IMAP-уязвимости. • info - потенциальная утечка информации. • ldap - известные LDAP-уязвимости. • malware - скачивание, установка, деятельность известных malware. • misc - другие известные сигнатуры. • netbios - известные уязвимости протокола NETBIOS. • p2p - идентификация трафика точка-точка (peer-to-peer). • phishing - сигнатуры известных phishing атак. • policy - нарушение информационной безопасности. • pop3 - известные уязвимости протокола POP3. • rpc - известные уязвимости протокола RPC. • scada - известные уязвимости протокола SCADA. • scan - сигнатуры, определяющие попытки сканирования сети на известные приложения. • shellcode - сигнатуры, определяющие известные попытки запуска программных оболочек. • sip - известные уязвимости протокола SIP. • smb - известные уязвимости протокола SMB. • smtp - известные уязвимости протокола SMTP. • snmp - известные уязвимости протокола SNMP. • sql - известные уязвимости SQL. • telnet - известные попытки взлома по протоколу telnet. • tftp - известные уязвимости протокола TFTP. • user_agents - сигнатуры подозрительных Useragent. • voip - известные уязвимости протокола VoIP. • web_client - сигнатуры, определяющие известные попытки взлома различных веб-клиентов, например, Adobe Flash Player. • web_server - сигнатуры, определяющие известные попытки взлома различных веб-серверов. • web_specific_apps - сигнатуры, определяющие известные попытки взлома различных веб приложений. • worm - сигнатуры, определяющие сетевую активность известных сетевых червей.

Наименование	Описание
Операционная система сигнатуры	Операционная система, для которой разработана данная сигнатура. • Windows • Linux • BSD • Mac OS • Solaris • Cisco • IOS • Android • Other
CVE	Идентификатор уязвимости по реестру CVE.
BDU	Идентификатор уязвимости по реестру BDU.
URL	Опциональная ссылка на ресурс с описанием уязвимости.
UASL	Описание признаков сигнатуры с помощью синтаксиса UASL .
Настройки	• Действие - реакция на срабатывание сигнатуры. Определены следующие значения:: ◦ Нет - действие не определено. ◦ Пропустить - пропустить пакет. ◦ Отбросить - отбросить пакет. ◦ Сбросить - отбросить пакет с разрывом TCP соединения (отправка TCP reset). ◦ Блокировать IP - блокировать IP-адрес источника и/или назначения. • Журналировать: ◦ Включить - включить запись событий в журнал. ◦ Отключить - отключить запись событий в журнал. • Файл рсар - трассировка срабатывания сигнатуры с записью в файл формата рсар. ◦ Включить - включить трассировку. ◦ Отключить - отключить трассировку. • Применить к - применимость действий типа Ресет или Блокировать IP на срабатывание сигнатуры: ◦ Источник - действия Ресет или Блокировать IP применяются к адресу источника отправления пакетов. ◦ Назначение - действия Ресет или Блокировать IP применяются к адресу назначения отправления пакетов. ◦ Оба - действия Ресет или Блокировать IP применяются и к источнику, и к назначению. • Продолжительность - длительность блокировки для действия Блокировать IP.

Product: DCFW
Version: 8.x
Technology: IDPS

Назначение профиля COB

Профиль COB позволяет создавать динамический набор [сигнатур COB](#), предназначенный для обнаружения вторжений и защиты определенных сервисов. Динамичность профиля достигается за счет того, что профиль явно не содержит в себе никаких сигнатур, а содержит фильтры, с помощью которых собирается набор сигнатур. Для фильтрации используются как описательные поля сигнатур, так и настройки. В итоге получается, что при изменении библиотеки сигнатур профили динамически наберут новые наборы сигнатур, удовлетворяющих фильтрам профилей.

Помимо создания необходимого набора сигнатур в профиле могут определяться действия, которые будут выполняться над трафиком, отфильтрованным сигнатурами.

Создание профиля COB в веб-консоли администратора

В веб-консоли администратора профили COB создаются в разделе **Библиотеки → Профили COB**.

Необходимо нажать **Добавить** и заполнить соответствующие поля в свойствах профиля:

1. В поле **Название** указать название создаваемого профиля.
2. В поле **Описание** опционально указать назначение профиля.
3. В области **Фильтры** добавляются фильтры для выбора необходимых сигнатур из библиотеки.
4. На вкладке **Совпавшие сигнатуры** отображается превью сигнатур COB, отобранных всеми фильтрами профиля, и настроенные действия, которые необходимо выполнить над трафиком, отфильтрованным этими сигнатурами.

Настройка фильтров сигнатур в профиле COB

Для создания фильтра сигнатур необходимо в области **Фильтры** нажать кнопку **Добавить**. Откроется окно свойств фильтра.

Фильтр можно создать, выбирая опции в панели инструментов. В окне под панелью инструментов будут отображаться сигнатуры, отбираемые этим фильтром:



Также фильтр можно создать, описав его с помощью sql-подобного синтаксиса. Для этого необходимо нажать кнопку **Расширенный** в панели инструментов и в открывшейся строке описать свойства выбора фильтра:



Для сохранения созданного фильтра необходимо нажать кнопку **Сохранить**.

В одном профиле можно использовать сразу несколько фильтров.

Фильтры в профиле работают по логическому ИЛИ. Например, если в профиле добавлено два фильтра ``category = injection`` и ``threat = low``, они эквивалентны одному фильтру ``category = injection OR threat = low``.

Настройка параметров сигнатур в профиле COB

В рамках профиля можно переопределить параметры сигнатур, такие как действие, журналирование, запись в файл pcap, включение/отключение сигнатуры. Для этого необходимо выбрать нужные сигнатуры в списке совпавших сигнатур и нажать кнопку **Переопределить** в панели инструментов.



Изменение настроек сигнатур в профиле COB имеет более высокий приоритет, чем настройки этих же сигнатур на странице сигнатур COB. Измененные настройки сигнатур COB можно вернуть в первоначальное состояние, для этого нужно выделить сигнатуру в списке сигнатур профиля и нажать кнопку **Восстановить по умолчанию** в панели инструментов профиля.

Применение профилей COB

Администратор может создать необходимое количество профилей. Рекомендуется ограничивать количество сигнатур в профиле только теми, которые необходимы для защиты определенного сервиса. Большое количество сигнатур требует большего времени обработки трафика и загрузки процессора.

Профиль COB применяется в разрешающем правиле [межсетевого экрана](#).

Правила межсетевого экрана обрабатываются сверху вниз и сессия попадает в первое правило, которое удовлетворяет всем условиям в нем. После попадания под правило с профилем COB, трафик начинает анализироваться с помощью определенного в профиле набора сигнатур. При этом анализируются как прямые, так и обратные пакеты согласно условий в фильтре, независимо от того, откуда устанавливается соединение. При срабатывании сигнатур профиля будет выполнено действие, настроенное в профиле и произведена соответствующая запись в [Журнале COB](#), если была включена опция журналирования. Если ни одна из сигнатур профиля не была найдена, то трафик пропускается дальше.

Если срабатывает сигнатура с действием Блокировать IP, то тогда блокируется IP-адрес источника или назначения (в зависимости от настройки) на определенное в настройках время. Заблокированные сигнатурами IP-адреса отображаются на странице **Диагностика и мониторинг** в разделе **Заблокированные COB/L7 IP-адреса** (подробнее читайте в разделе [Заблокированные COB/L7 IP-адреса](#)).

Профили оповещений

Version: 8.x
Product: DCFW

Профиль оповещения указывает транспорт, с помощью которого оповещения могут быть доставлены получателям. Поддерживается 2 типа транспорта:

- SMTP, доставка сообщений с помощью e-mail.
- SMPP, доставка сообщений с помощью SMS практически через любого оператора сотовой связи или через большое количество SMS-центров рассылки.

Для создания профиля сообщений SMTP необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMTP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Хост	IP-адрес или FQDN сервера SMTP, который будет использоваться для отсылки почтовых сообщений.
Порт	Порт TCP, используемый сервером SMTP. Обычно для протокола SMTP используется порт 25, для SMTP с использованием SSL - 465. Уточните данное значение у администратора почтового сервера.
Безопасность	Варианты безопасности отправки почты, возможны варианты: Нет, STARTTLS, SSL.
Авторизация	Включает авторизацию при подключении к SMTP-серверу.
Логин	Имя учетной записи для подключения к SMTP-серверу.
Пароль	Пароль учетной записи для подключения к SMTP-серверу.

Для создания профиля сообщений SMPP необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMPP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Хост	IP-адрес или FQDN сервера SMPP, который будет использоваться для отсылки SMS сообщений.
Порт	Порт TCP, используемый сервером SMPP. Обычно для протокола SMPP используется порт 2775, для SMPP с использованием SSL -- 3550.
SSL	Использовать или нет шифрацию с помощью SSL.
Логин	Имя учетной записи для подключения к SMPP-серверу.
Пароль	Пароль учетной записи для подключения к SMPP-серверу.
Правила трансляции номеров	В некоторых случаях SMPP-провайдер ожидает номер телефона в определенном формате, например, в виде 89123456789. Для соответствия требованиям провайдера можно указать замену первых символов номеров с одних на другие. Например, заменить все номера, начинающиеся на +7, на 8.

Профили NetFlow

Product: DCFW
Version: 8.x

NetFlow — сетевой протокол, предназначенный для учёта сетевого трафика, разработанный компанией Cisco Systems, поддерживаемый в настоящее время многими вендорами. Для сбора информации о трафике по протоколу NetFlow требуются следующие компоненты:

- Сенсор — собирает статистику по проходящему через него трафику и передает ее на коллектор.
- Коллектор — получает от сенсора данные и помещает их в хранилище.
- Анализатор — анализирует собранные коллектором данные и формирует пригодные для чтения человеком отчёты (часто в виде графиков).

DCFW может выступать в качестве сенсора. Для сбора и отправки статистики о трафике, проходящем через определенный сетевой интерфейс DCFW, необходимо выполнить следующие действия:

1. Создать профиль NetFlow.
2. Назначить созданный профиль NetFlow сетевому интерфейсу, на котором необходимо собирать статистику.

Для создания профиля NetFlow необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили NetFlow** и указать необходимые параметры:

Наименование	Описание
Название	Название профиля NetFlow.
Описание	Описание профиля NetFlow.
IP-адрес NetFlow коллектора	IP-адрес сервера, куда сенсор будет отправлять статистику.
Порт NetFlow коллектора	UDP порт, на котором коллектор будет принимать статистику.
Версия протокола	Версия протокола NetFlow, которую следует использовать. Версия протокола должна совпадать на сенсоре и на коллекторе.
Таймаут активного потока (сек)	При длительных потоках, например, передача большого файла через сеть, время, через которое будет отправляться статистика на коллектор, не дожидаясь завершения потока. Значение по умолчанию — 1800 секунд.
Таймаут неактивного потока (сек.)	Время, резервируемое на завершение неактивного потока. Значение по умолчанию — 15 секунд.
Количество потоков	Максимальное количество учитываемых потоков, с которых собирается и отправляется статистика. Ограничение необходимо для защиты от DoS-атак. После достижения данного количества потоков, все последующие не будут учитываться. Значение по умолчанию — 2000000, установите 0 для снятия ограничения.
Отправлять информацию NAT	Отправлять информацию о NAT преобразованиях в статистику NetFlow.
Частота отправки шаблона (пакетов)	Количество пакетов, после которых шаблон отправляется на принимающий хост (только для NetFlow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 20 пакетов.
Период отправки старого шаблона (сек.)	Время, через которое старый шаблон отправляется на принимающий хост (только для NetFlow 9/10). Шаблон содержит информацию о настройке самого устройства и различную статистическую информацию. Значение по умолчанию — 1800 секунд.

Профили LLDP

Product: DCFW
Version: 8.x

Link Layer Discovery Protocol (LLDP) — протокол канального уровня, позволяющий сетевым устройствам, работающим в локальной сети, объявлять о своём существовании и передавать свои характеристики и получать аналогичные сведения. Информация, собранная при помощи операции LLDP, хранится в сетевом устройстве.

Для создания профиля безопасности необходимо нажать **Добавить** в разделе **Библиотеки → Профили LLDP** и указать следующие параметры:

Наименование	Описание
Название	Название профиля LLDP.
Описание	Описание профиля LLDP.
Статус порта	Режим: • Приём и передача данных LLDP — NGFW будет посылать информацию LLDP и будет анализировать информацию LLDP, полученную от соседей. • Только приём данных LLDP — NGFW не будет посылать информацию LLDP, но будет анализировать информацию LLDP от соседей. • Только передача данных LLDP — NGFW будет посылать информацию LLDP, но будет отбрасывать информацию LLDP, полученную от соседей.

Профили SSL

Product: DCFW
Version: 8.x

Профиль SSL позволяет указать протоколы SSL или отдельные алгоритмы шифрования и цифровой подписи, которые в дальнейшем могут быть использованы в настройках веб-консоли, страницы авторизации, страницы блокировки.

Для создания профиля SSL необходимо нажать на кнопку **Добавить** в разделе **Библиотеки → Профили SSL** и указать необходимые параметры:

Наименование	Описание
Название	Название профиля SSL.
Описание	Описание профиля SSL.
Протоколы SSL	Минимальная версия TLS — устанавливает минимальную версию TLS, которая может быть использована в данном профиле. Максимальная версия TLS — устанавливает максимальную версию TLS, которая может быть использована в данном профиле. Оба эти параметра определяют диапазон версий TLS, которые будут поддерживаться данным профилем.
Наборы алгоритмов	Данный раздел позволяет выбрать необходимые алгоритмы шифрования и цифровой подписи. Возможные значения указаны в виде строк, в которых перечислены алгоритм и подпись. Администратор может указать только те наборы алгоритмов и подписей, которые считает нужным для безопасной работы организации. Список поддерживаемых комбинаций следующий: • TLS AES 128 CCM SHA256 • TLS AES 128 GCM SHA256 • TLS AES 256 GCM SHA384 • TLS DHE DSS WITH 3DES EDE CBC SHA • TLS DHE DSS WITH AES 128 CBC SHA • TLS DHE DSS WITH AES 128 CBC SHA256 • TLS DHE DSS WITH AES 128 GCM SHA256 • TLS DHE DSS WITH AES 256 CBC SHA • TLS DHE DSS WITH AES 256 CBC SHA256 • TLS DHE DSS WITH AES 256 GCM SHA384 • TLS DHE RSA WITH 3DES EDE CBC SHA • TLS DHE RSA WITH AES 128 CBC SHA • TLS DHE RSA WITH AES 128 CBC SHA256 • TLS DHE RSA WITH AES 128 GCM SHA256 • TLS DHE RSA WITH AES 256 CBC SHA • TLS DHE RSA WITH AES 256 CBC SHA256 • TLS DHE RSA WITH AES 256 GCM SHA384 • TLS ECDH ECDSA WITH 3DES EDE CBC SHA • TLS ECDH ECDSA WITH AES 128 CBC SHA • TLS ECDH ECDSA WITH AES 128 CBC SHA256 • TLS ECDH ECDSA WITH AES 128 GCM SHA256 • TLS ECDH ECDSA WITH AES 256 CBC SHA • TLS ECDH ECDSA WITH AES 256 CBC SHA384 • TLS ECDH ECDSA WITH AES 256 GCM SHA384 • TLS ECDH RSA WITH 3DES EDE CBC SHA • TLS ECDH RSA WITH AES 128 CBC SHA

шифрования Наименование	Описание
	• TLS ECDH RSA WITH AES 128 CBC SHA256 • TLS ECDH RSA WITH AES 128 GCM SHA256 • TLS ECDH RSA WITH AES 256 CBC SHA • TLS ECDH RSA WITH AES 256 CBC SHA384 • TLS ECDH RSA WITH AES 256 GCM SHA384 • TLS ECDHE ECDSA WITH 3DES EDE CBC SHA • TLS ECDHE ECDSA WITH AES 128 CBC SHA • TLS ECDHE ECDSA WITH AES 128 CBC SHA256 • TLS ECDHE ECDSA WITH AES 128 GCM SHA256 • TLS ECDHE ECDSA WITH AES 256 CBC SHA • TLS ECDHE ECDSA WITH AES 256 CBC SHA384 • TLS ECDHE ECDSA WITH AES 256 GCM SHA384 • TLS ECDHE RSA WITH 3DES EDE CBC SHA • TLS ECDHE RSA WITH AES 128 CBC SHA • TLS ECDHE RSA WITH AES 128 CBC SHA256 • TLS ECDHE RSA WITH AES 128 GCM SHA256 • TLS ECDHE RSA WITH AES 256 CBC SHA • TLS ECDHE RSA WITH AES 256 CBC SHA384 • TLS ECDHE RSA WITH AES 256 GCM SHA384 • TLS GOST2012256 WITH 28147 CNT IMIT • TLS GOSTR341001 WITH 28147 CNT IMIT • TLS RSA WITH 3DES EDE CBC SHA • TLS RSA WITH AES 128 CBC SHA • TLS RSA WITH AES 128 CBC SHA256 • TLS RSA WITH AES 128 GCM SHA256 • TLS RSA WITH AES 256 CBC SHA • TLS RSA WITH AES 256 CBC SHA256 • TLS RSA WITH AES 256 GCM SHA384
Установка алгоритмов шифрования для стандартных протоколов	Данный раздел можно использовать для облегчения выбора необходимых алгоритмов шифрования и подписи для стандартных протоколов TLS. Администратор может указать в поле Выберите протокол для установки алгоритмов необходимые версии протоколов TLS, нажать на кнопку Применить, и алгоритмы, соответствующие выбранной версии протокола автоматически будут отмечены. Можно последовательно добавить несколько версий протокола TLS.

По умолчанию в продукте создано несколько профилей SSL, которые могут быть использованы администратором как есть, либо изменены/удалены при необходимости. Созданы следующие профили SSL:

Наименование	Описание
Default SSL profile	Содержит алгоритмы и подписи, соответствующие версиям с TLS v.1.1 до TLS v.1.2. Это наиболее распространенные версии протоколов, используемые в сети интернет в данное время. Данный профиль используется по умолчанию в: • Для страницы авторизации Captive-портала. • Для страницы блокировки.
Default SSL profile (TLSv1.3)	Содержит алгоритмы и подписи, соответствующие версии TLS v.1.3. По умолчанию не используется.
Default SSL profile (GOST)	Содержит алгоритмы и подписи, соответствующие TLS с ГОСТ-алгоритмами (TLS GOST2012256 with 28147 CNT IMIT и TLS GOSTR341001 with 28147 CNT IMIT). Может быть использован в организациях, где требуется использование данных алгоритмов. Поддержка данных протоколов должна также быть обеспечена со стороны используемых браузеров. По умолчанию не используется.

Наименование	Описание
Default SSL profile (web console)	Содержит алгоритмы и подписи, соответствующие версиям с TLS v.1.0 до TLS v.1.2. Данный профиль используется по умолчанию для предоставления SSL-доступа в веб-консоль. Важно! Изменение данного профиля следует производить с осторожностью. Указание алгоритмов, не поддерживаемых вашим браузером, может привести к потере доступа в веб-консоль!

Профили BFD

Product: DCFW
Version: 8.x

BFD (Bidirectional Forwarding Detection) — протокол, работающий на уровне интерфейса и протокола маршрутизации и предназначенный для быстрого обнаружения сбоев между двумя соседними маршрутизаторами, включая интерфейсы, каналы передачи данных и механизмы пересылки. BFD работает поверх любого протокола передачи данных (сетевой уровень, канальный уровень, туннели и т.д.), передаваемого между двумя системами. Пакеты BFD передаются в качестве полезной нагрузки инкапсулирующего протокола, который подходит для данной среды и сети. BFD может работать на нескольких уровнях в системе.

Маршрутизаторы с BFD отправляют пакеты друг другу с согласованной скоростью. Если пакеты от маршрутизатора, поддерживающего BFD, не поступают, то этот маршрутизатор объявляется неработающим. BFD передает эту информацию соответствующим протоколам маршрутизации, и информация о маршрутизации обновляется. BFD помогает обнаружить односторонний отказ устройства и используется для быстрой конвергенции протоколов маршрутизации.

Профиль BFD — это конфигурация или набор параметров, используемых в протоколах динамической маршрутизации (BGP, OSPF), для определения работы функции обнаружения двунаправленной переадресации. Профиль обычно включает такие параметры, как желаемое время обнаружения, время удержания и другие параметры, определяющие скорость обнаружения и реагирования сетевых устройств на сбой в канале связи.

Настройка и использование профилей обеспечивают оперативное обнаружение сбоев в сети, что позволяет ускорить перенаправление трафика на интерфейсы и повысить надежность сети.

Настройка BFD для OSPF позволяет соответствующим событиям подключения сеанса BFD мгновенно обновлять статус интерфейса OSPF.

В случае протокола BGP, BFD также может быть использован для регулирования времени обнаружения сбоев. Настройка BFD на более быстрое обнаружение неисправностей соединений позволяет оперативней реагировать и улучшать конвергенцию маршрутизации BGP.

Чтобы создать профиль BFD, необходимо в разделе **Библиотеки → Bfd profiles** нажать на кнопку **Добавить** и указать необходимые параметры:

Наименование	Описание
Название	Задать имя профиля BFD.
Detect multiplier	Определить множитель времени обнаружения. Локальная система рассчитывает время обнаружения неисправностей соединения как произведение множителя времени обнаружения, полученного от удаленной системы, и согласованного интервала передачи удалённой системы. Если BFD не получит управляющий пакет до истечения времени обнаружения, то считается, что произошел сбой соединения. Например, если интервал передачи равен 300 мс, а множитель — 3, то локальная система будет обнаруживать сбой только через 900 мс отсутствия приема пакетов.
Receive interval	Настроить интервал приема управляющих пакетов BFD (минимальное время, которое требуется между пакетами). Интервал не согласовывается между узлами. Для определения интервала каждый из узлов сравнивает свой интервал передачи с интервалом приема соседа — большее из двух значений принимается в качестве интервала передачи для этого узла. Значение по умолчанию — 50 мс.
Transmit Interval	Указать интервал передачи управляющих пакетов BFD; интервал должен быть согласован между узлами. Значение по умолчанию — 50 мс.
Echo receive Interval	Настроить минимальный интервал, через который данная система способна принимать echo-пакеты. Значение по умолчанию — 50 мс.
Echo transmit interval	Настроить минимальный интервал передачи, через который эта система будет способна отправлять echo-пакетов BFD. Значение по умолчанию — 50 мс.
Echo mode	Включить или выключить режим передачи Echo mode . По умолчанию этот режим отключен. Когда функция Echo активна, поток пакетов BFD Echo передается на удалённую систему, которая возвращает их обратно по тому же маршруту пересылки. Если некоторое количество пакетов эхо-потока данных не получено, сессия объявляется нерабочей. Преимущество Echo mode состоит в том, что она тестирует только путь пересылки на удаленной системе. Это позволяет уменьшить задержку при прохождении маршрута и уменьшить время, затрачиваемое на обнаружения сбоев. Эхо-режим не поддерживается в многоуровневых сетях (см. RFC-5883).

Наименование	Описание
Passive mode	Включить или выключить режим Passive. При работе в режиме Passive система ждет управляющие пакеты от соседей и отвечает на них в случае их получения. Эта функция полезна, когда маршрутизатор выступает в роли центрального узла звездообразной сети, и вы хотите избежать отправки ненужных управляющих пакетов BFD. По умолчанию используется режим Active. В случае работы в режиме Active — узел отправляет управляющие пакеты соседнему узлу. Важно! Оба узла не могут работать в режиме Passive; хотя бы один из них (или оба) должен работать в режиме Active.
Minimum-ttl	Только для сеансов с несколькими переходами: настроить минимальное значение времени жизни (количество переходов), которое BFD будет принимать в управляющем пакете BFD. Может принимать значения от 1 до 254. Все пакеты с меньшим значением TTL будут отброшены. Установка данного значения необходима для ужесточения требований к проверке пакетов во избежание получения управляющих пакетов BFD от других сессий. Значение по умолчанию равно 254 (это означает, что мы ожидаем только один прыжок между этой системой и аналогом).

Syslog-фильтры UserID агента

Product: DCFW
Version: 8.x
Technology: Identification and Authentication

При использовании syslog в качестве источников событий UserGate производит фильтрацию событий в соответствии с указанными syslog-фильтрами UserID агента. Фильтры syslog представляют из себя стандартные Regexp-выражения, которые пользователь может писать и сам. В стандартной поставке представлены три вида фильтров:

Наименование	Описание
SSH Authentication	Фильтр, предназначенный для отслеживания событий входа\выхода пользователей по протоколу SSH в журналах syslog.
Unix PAM Authentication	Фильтр, предназначенный для отслеживания событий входа\выхода пользователей посредством технологии Pluggable Authentication Modules (PAM) в журналах syslog.
UserGate WEC Agent	Фильтр, предназначенный для отслеживания событий, переданных через syslog из UserID агента для AD/WEC-серверов. (Доступно начиная с релиза ПО 7.2.0).

ПримечаниеИспользуя правила Regexp, возможно написание дополнительных правил. Таким образом фильтры syslog представляют из себя универсальный инструмент, который можно использовать практически в любых случаях.

Найденные события отображаются во вкладке **Журналы и отчёты**, в разделе **Журналы —> Агент UserID —> Syslog**.

