

Table of Contents

Table of Contents	1
Часто задаваемые вопросы	4
Как разрешить работу клиента Yandex.Disk	5
Как разрешить обновления Microsoft Edge (на базе Chromium) через UserGate	7
Исправление авторизации на сайте Авито (разблокировка гугл-капча)	8
Недоступны SNMP устройства за UserGate	10
Ошибка при настройке интерфейса	11
Yandex Browser vs SSL inspection	12
Записи о блокировке широковеб-пакетов заполняют журнал трафика	13
Постоянное переключение шлюзов	14
Не работают правила, содержащие ограничения по внешним пользователям	15
Блокировка доступа через VPN	16
Ошибки TLS в журнале веб-доступа	17
Выбор протокола PAP на MacOS	18
Избыточные записи о срабатываниях правил контентной фильтрации в журнале веб-доступа	19
Как проверить работу антиспам модуля	20
Сертификация ФСТЭК России	21
ОС Windows разрывает VPN-соединение	22
Отсутствует доступ из локальной сети к ресурсам, опубликованным с помощью reverse-прокси, по внешнему URL	23
Низкая скорость передачи при Site-to-Site VPN	24
VPN за UserGate	25
Ошибка: Мало места на разделе для журналов	26
Работа агента терминального сервера	27
Ошибка: Попытка L2TP-подключения не удалась из-за ошибки, произошедшей на уровне безопасности, во время согласований с удаленным компьютером	28
Использование пула IP-адресов для NAT трансляции	29
Запись трафика на NGFW	30
Можно ли удалить записи журналов (событий, веб-доступа и т.д.)	31
Чем отличаются варианты резервных копий в Support Menu	32
Некорректное отображение имен пользователей в журнале Web-доступа	33
Можно ли отключить список DNSBL не удаляя его?	34
Где хранятся журналы после подключения LogAn	35
Не открываются сайты при включенном SSL-инспектировании	36
Использование нескольких идентичных контроллеров домена	37
Как разрешить работу офисной SIP АТС через UserGate?	38
Ошибка: System is booting... LOM card present	39
Настройка работы AnyDesk	40
Расписание типа Повторяющиеся события	41
Как добавить сетевые адаптеры к UserGate (Virtual Appliance)?	42
Экспорт и импорт политик UserGate через CLI	43
Сотрудничество с ФинЦЕРТ	45
Поддерживается ли технология VxLAN в UserGate NGFW	46
Использование групп и пользователей LDAP в политиках безопасности, настраиваемых на Management Center	47
Ошибка подключения: не удалось найти имя хоста или домена	48
Настройка сервисов на UserGate 6.x.x	49
Как расширить системный раздел устройства UserGate 7.x.x	50
Низкая скорость передачи данных в туннеле Site-to-Site VPN между двумя устройствами	

UserGate	52
Как настроить правила аналитики SIEM	53
Настройка сервиса XML-RPC	57
Настройка защиты от DoS для трафика reverse-прокси	58
Подключение агентов аутентификации для Windows из разных подсетей	59
Периодические разрывы VPN соединений.	61
Долгая загрузка устройства	62
Почему UserGate посылает DNS-запросы для разрешения URL-адреса из списка угроз	63
Некорректная работа виртуальной машины с ПО UserGate при использовании динамических MAC-адресов	64
Какие версии UserGate сертифицированы ФСТЭК?	65
Правила фильтрации	66
Как ограничить полосу пропускания группе пользователей для доступа к видео из сети Интернет	67
Как запретить трафик для определенных приложений	68
Как разрешить работу клиента Dropbox	69
Не удастся настроить исключение блокировки рекламы	71
Не работают правила, содержащие ограничения по внешним пользователям	72
Разделение трафика для применения разных алгоритмов обработки	73
При включении DNS-фильтрации начинают блокироваться разрешенные ресурсы	74
Исключение трафика конкретных приложений из проксирования и инспектирования	75
Взаимодействие правил reverse-прокси, DNAT и межсетевого экрана	76
Запретить NAT "серых" IP адресов	77
Некорректная работа Яндекс Браузера с сервисами Google	78
Кластеризация	79
Отсутствует лицензия на одном из узлов кластера	80
Активация лицензии на кластере UserGate	81
Построение отказоустойчивого решения для кластера с 2 провайдерами и одним внешним IP-адресом на узле	82
2 ПАК с разной версией ПО. Как настроить кластер?	83
Рассинхронизация кластера Active - Passive	84
Меняются ли MAC-адреса VIP адреса, в кластере	85
Разрыв VPN соединения при переключении активного узла кластера	86
Как увидеть состояние VRRP	87
Как перезагрузить сервис VRRP?	88
Сбой экземпляра отказоустойчивости кластера при добавлении интерфейса	89
Авторизация и аутентификация	90
Определение пользователей при авторизации с помощью NTLM	91
Разрешения доступа администраторов	92
Настройка браузера Chrome на Linux для авторизации Kerberos/Captive portal	93
Некорректная работа правил UserGate NGFW при работе с доменными пользователями	95
Периодические разрывы связи при работе с потоковыми сервисами	94
Проблемы с авторизацией при использовании нескольких методов аутентификации	96
Загрузка сертификатов на клиентское устройство с ОС Windows 11	97
Как настроить прозрачную аутентификацию Kerberos в нескольких доменах?	98
Лицензирование	99
Лицензирование	100
Учёт лицензируемых устройств	101
Отсутствует лицензия на одном из узлов кластера	102
Активация лицензии на кластере UserGate	103
Ошибка при активации лицензии	104
Не удастся активировать лицензию	105

Получение лицензии для выполнения учебного проекта	106
Офлайн-активация лицензий	107
Маршрутизация	111
Не создается виртуальный маршрутизатор	112
Маршрутизация при использовании явного прокси	113
Не удаётся создать 2 моста L2 и L3 на одном устройстве	114
Кластер Актив-Пассив не использует виртуальный адрес для отправки трафика	115
Объединение нескольких сетей с помощью VPN site-to-site	116
Недоступны сервисы при использовании VRF	117
Пользовательский интерфейс	118
Персонализация страницы Captive-портала	119
Особенность отображения пользователей на графике	120
Одновременная авторизация с двух устройств	121
Не открывается JAVA консоль в IPMI	122
Журналы событий	123
Как настроить выгрузку журналов на FTP сервер	124
С какой периодичностью отсылаются уведомления о переполнении памяти?	126
Безопасность	127
Интерпретация результатов сканирования	128
53(UDP)-DNS Отказ в обслуживании.	129
DNS-сервер поддерживает рекурсию запросов.	130
443(TCP) - HTTP SSL	131
Слабый криптографический ключ	132
623(UDP) - IPMI	133
Обнаружение уязвимости типа CVE-2002-20001 при сканировании NGFW UserGate сторонними сканерами.	134
Статус портов при сканировании Nmap	135
Сканирование сети обнаруживает порты даже на тех адресах, где нет соответствующих сервисов	136
Ложные срабатывания сигнатур IDS	137

Product: UserGate NGFW

Задача

Необходимо разрешить работу клиента Yandex.Disk

Решение

Для организации работы клиента Яндекс.Диск необходимо создать новое правило дешифрования. Для этого перейдите в раздел **Политики безопасности → Инспектирование SSL**. Создайте правило инспектирования SSL и задайте параметры.

Во вкладке **Общие** укажите:

- **Название** правила инспектирования.
- **Действие** - **Не расшифровывать**.

The screenshot shows the 'Свойства правила инспектирования SSL' (SSL inspection rule properties) dialog box with the 'Общие' (General) tab selected. The 'Включено' (Enabled) checkbox is checked. The 'Название' (Name) field contains 'Don't decrypt Yandex.disk'. The 'Действие' (Action) dropdown is set to 'Не расшифровывать' (Do not decrypt). The 'Профиль SSL' (SSL profile) is 'Default SSL profile'. The 'Записывать в журнал правил' (Log rules) checkbox is checked. Under 'Атрибуты' (Attributes), there are four unchecked checkboxes: 'Блокировать сайты с некорректными сертификатами' (Block sites with incorrect certificates), 'Проверять по списку отозванных сертификатов' (Check against the list of revoked certificates), 'Блокировать сертификаты с истекающим сроком действия' (Block certificates with expiring date), and 'Блокировать самоподписанные сертификаты' (Block self-signed certificates). The 'Вставить' (Insert) dropdown is set to 'Наверх списка правил' (To the top of the rules list). At the bottom are 'Сохранить' (Save) and 'Отмена' (Cancel) buttons.

В разделе **Библиотеки → Списки URL** создайте новый список и добавьте следующие сайты:

- click.yandex.ru
- *.disk.yandex.net
- push.yandex.ru
- report.appmetrica.yandex.net
- *.storage.yandex.net
- webdav.yandex.
- passport.yandex.com
- downloader.disk.yandex.
- mds.yandex.net
- cloud-api.yandex.
- oauth.yandex.
- yastatic.net.

Список URL также можно создать при настройке правила во вкладке **Домены** (кнопка **Создать и добавить новый объект**).

The screenshot shows the 'Создать новый список URL' (Create new URL list) dialog box. The 'Название списка' (List name) field contains 'for yandex.disk'. The 'URL обновления' (URL update) field is empty. Below is a table of URLs with columns for 'Добавить' (Add), 'Редактировать' (Edit), and 'Удалить' (Delete). The table contains the following URLs: click.yandex.ru, *.disk.yandex.net, push.yandex.ru, report.appmetrica.yandex.net, *.storage.yandex.net, webdav.yandex., passport.yandex.com, downloader.disk.yandex., mds.yandex.net, cloud-api.yandex., and oauth.yandex. At the bottom are 'Сохранить' (Save) and 'Отмена' (Cancel) buttons.

Далее во вкладке **Домены** свойств правил инспектирования укажите созданный ранее список URL.

Свойства правила инспектирования SSL

ОбщиеПользователиИсточникАдрес назначенияСервисыКатегорииДоменыВремя

Добавить

Редактировать

Удалить

URL

Владелец

for yandex.disk

Вы

Создать и добавить новый объект

☐ Инвертировать

Сохранить

Отмена

Примечание Данное правило необходимо расположить в начале списка правил инспектирования SSL.

KnowledgeBase: 
Product: UserGate NGFW

Задача

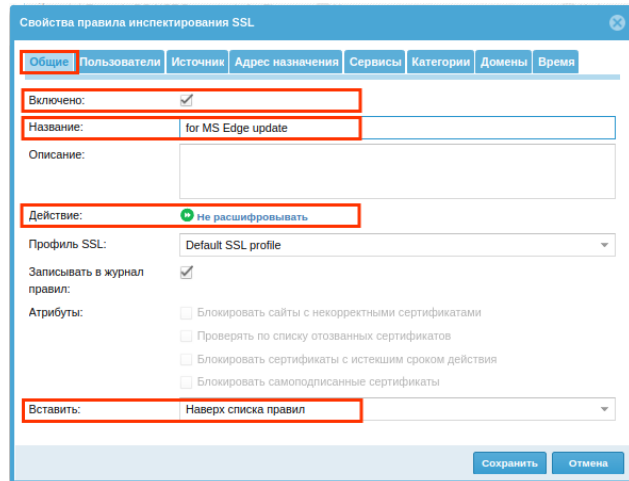
Необходимо разрешить получение обновления для Microsoft Edge (на базе Chromium)

Решение

Для того, чтобы браузер Microsoft Edge (версия на базе Chromium) мог получать обновления при доступе в Интернет через UserGate, необходимо создать дополнительное правило дешифрования. Для этого перейдите в раздел **Политики безопасности** → **Инспектирование SSL** и добавьте правило инспектирования. Укажите необходимые данные.

Во вкладке **Общие** укажите:

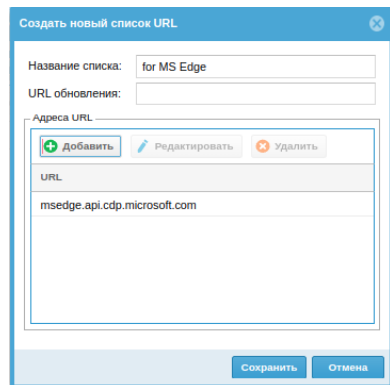
- **Название** правила инспектирования.
- **Действие**: **Не расшифровывать**.



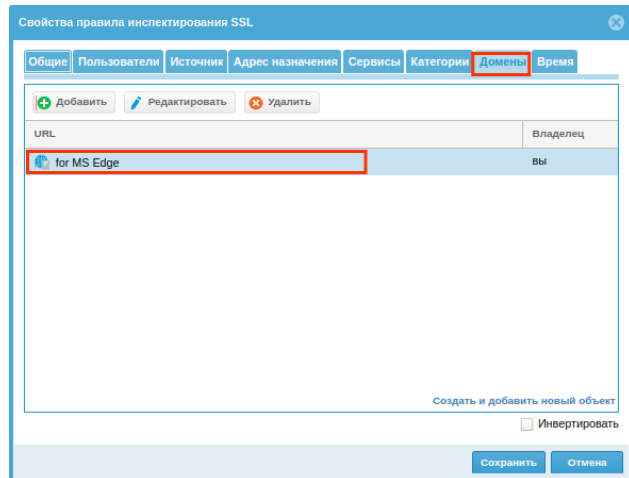
В разделе **Библиотеки** → **Списки URL** создайте новый список и укажите сайт:

- msedge.api.cdp.microsoft.com

Список URL также можно создать при настройке правила во вкладке **Домены** (кнопка **Создать и добавить новый объект**).



Далее во вкладке **Домены** свойств правила инспектирования укажите созданный ранее список URL.



Примечание Правило следует поместить в начало списка правил

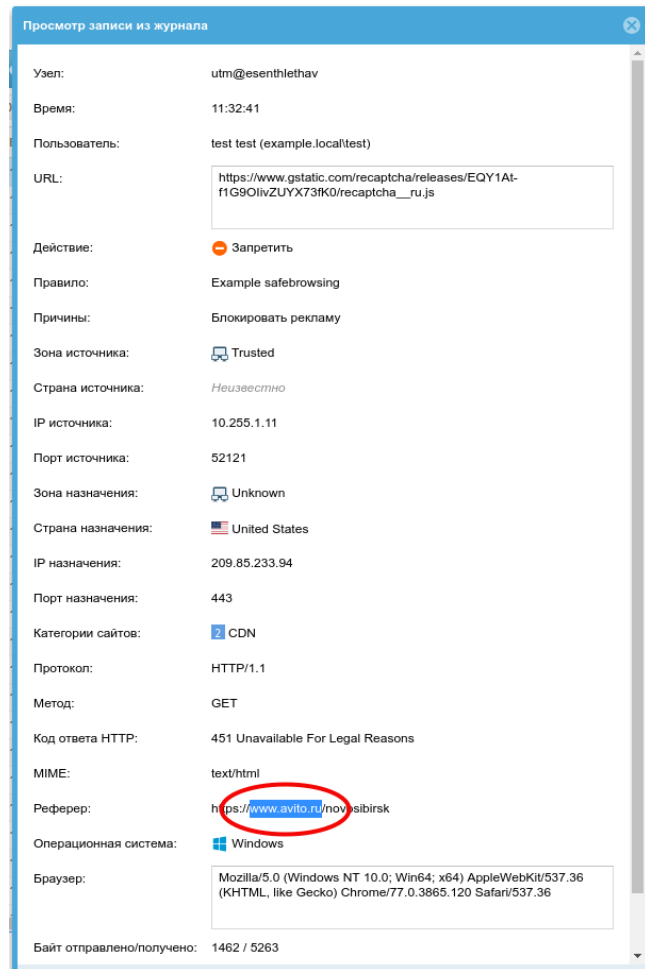
Product: UserGate NGFW

Задача

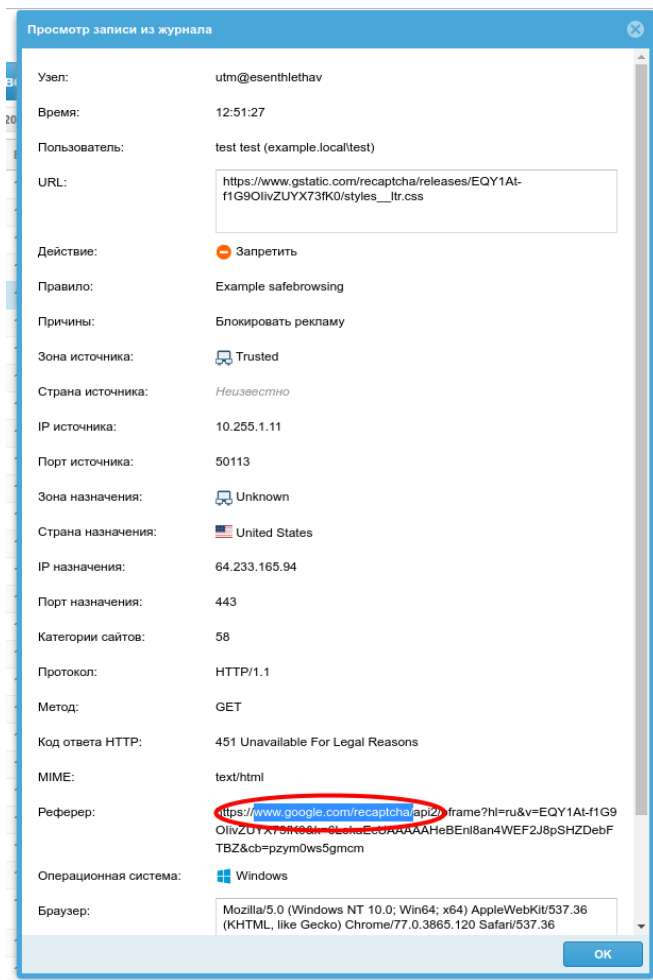
Ошибка при входе на сайт avito.ru

Решение

1. Для обнаружения правила веб-доступа, блокирующего авторизацию на сайте, нужно открыть сайт в браузере, кликнуть на "Вход и регистрация", во всплывающем окне нужно ввести имя и пароль и кликнуть на кнопку "Войти".
2. В журнале веб-доступа обнаружится сработавшее правило Веб-безопасности, следует внести в исключения URL www.avito.ru из поля Реферер (отмечен на скриншоте):

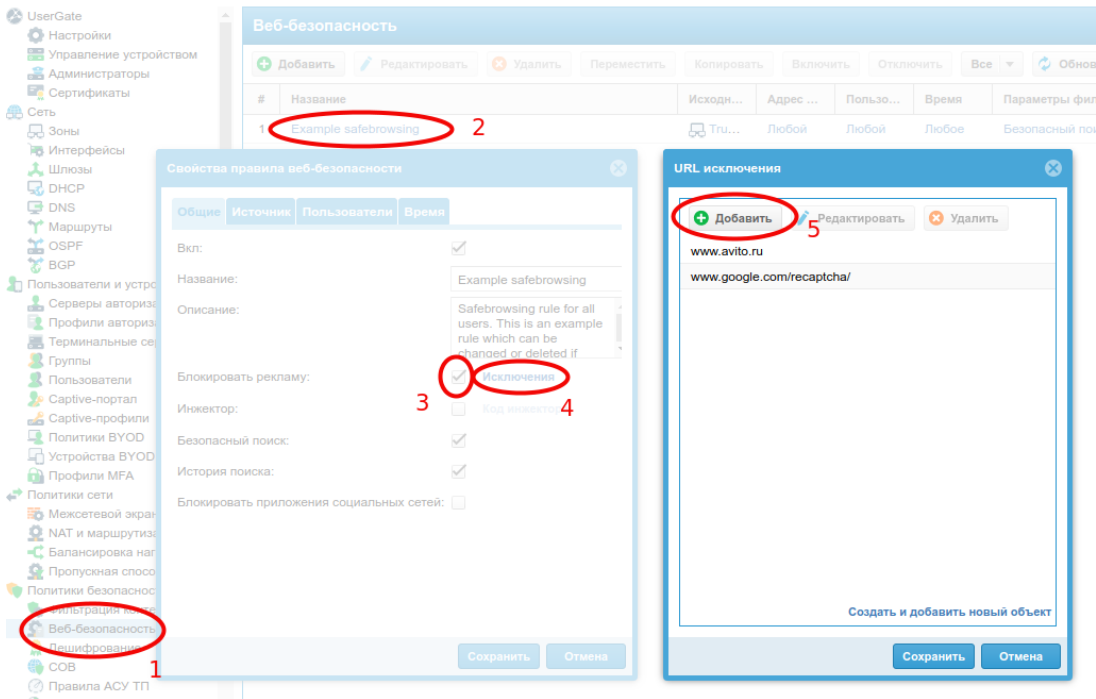


3. Еще раз повторить действия из п.1.
4. В журнале веб-доступа обнаружится еще одно сработавшее правило Веб-безопасности, в исключения которого следует внести URL www.google.com/recaptcha/ из поля Реферер:



После добавления этих исключений в правила, проблема исчезает.

Исключение из правила блокировки рекламы делается в самом правиле, пример на присоединённом скриншоте, названия листов соответствуют содержанию:



KnowledgeBase: 

Product: UserGate NGFW

Задача

Недоступен мониторинг устройств, находящихся за UserGate, по SNMP.

Решение

Возможно, в свойствах зоны, на которую приходят пакеты, был включен SNMP-прокси. При разрешении данного сервиса опрос устройств, находящихся за UserGate, будет происходить с использованием адреса самого UserGate. Таким образом, нужно либо выключить SNMP-прокси, либо разрешить опрос устройств с адреса UserGate.

Примечание Опрос по SNMP самого UserGate должен производиться с использованием адреса интерфейса, на который поступает пакет, в противном случае (пакет поступил на один интерфейс, а затем, в результате внутренней маршрутизации, был перенаправлен на IP-адрес другого интерфейса UserGate) сервис SNMP доступен не будет. Это сделано для корректной отработки сервисов при наличии VRF (подробнее читайте [Особенности реализации доступа к сервисам зон](#)).

KnowledgeBase: 

Product: UserGate NGFW

Задача

При настройке интерфейса возникает ошибка: Адрес из этого диапазона уже используется на другом интерфейсе.

Решение

Два разных интерфейса в UserGate не могут иметь адреса из одной подсети. Если бы это было возможно, маршрутизация была бы непредсказуемой.

KnowledgeBase: 📖

Product: UserGate NGFW

Задача

Yandex Browser не использует импортированный сертификат UserGate (проблема характерна, в основном, для Linux систем).

Решение

Для доверия сертификату UserGate со стороны Yandex Browser необходимо сделать следующее:

1. В Яндекс-браузере зайдите в **Настройки → Системные → Управление сертификатами**.
2. Импортируйте сертификат UserGate: нажмите **Импорт** и выберите скачанный сертификат UserGate.
3. Отметьте чекбоксы **Доверять этому сертификату...**

Примечание Если сертификат уже импортирован, то настройка доверия сертификату производится во вкладке Центры сертификации: найдите в списке сертификат UserGate и нажмите Изменить.

KnowledgeBase: 
Product: UserGate NGFW

Задача

Записи о блокировке широковещательных UDP-пакетов заполняют журнал трафика, что затрудняет его чтение.

Решение

Создать правило DNAT для перенаправления таких пакетов на широковещательный адрес несуществующей сети. Это предотвратит срабатывание блокирующего правила, созданного по умолчанию, и заполнение журналов лишними записями. Пример правила DNAT представлен на рисунке ниже:

NAT и маршрутизация												
Добавить Редактировать Удалить Переместить Копировать Включить Отключить Принудительно применить Показать Все												
#	Тип	Название	Зона источника	Адрес источника	Пользователи	Зона назначения	Адрес назначения	Сервис	DNAT	Шлюз	Сценарий	Network mapping
1	DNAT	DNAT Broadcast	Любая	Любой	—		10.255.1.255 255.255.255.255	Любой	1.255.255.255	—	—	

KnowledgeBase: 

Product: UserGate NGFW

Задача

Постоянное переключение шлюзов.

Решение

Это поведение является результатом работы проверки сети - указанный в настройках адрес периодически не проходит проверку.

Проверка сети настраивается в разделе **Сеть→ Шлюзы** вкладки **Настройки** веб-интерфейса управления (подробнее читайте в соответствующей [главе](#) руководства администратора).

Product: UserGate NGFW

Задача

Не работают правила, содержащие ограничения по пользователям, полученным с внешних серверов (например, LDAP-коннектора).

Решение

Возможны несколько причин возникновения данной проблемы.

Возможная причина №1

Для того чтобы пользователей можно было использовать в правилах любого модуля, пользователи должны пройти аутентификацию одним из поддерживаемых методов (подробнее читайте в соответствующем [разделе](#) руководства администратора).

Примечание Для использования пользователей в правилах межсетевого экрана в соответствующем captive-профиле, если используется не агент аутентификации, в качестве метода идентификации необходимо указать *Запоминать IP-адрес*.

Возможная причина №2

Случай асимметричного трафика: пакет от клиента к серверу передаётся через UserGate, а обратный - напрямую к клиенту (без обработки на UserGate). В этом случае межсетевой экран с контролем состояния обратный пакет не привязывает к пользователю. В такой ситуации необходимо правильно настроить маршрутизацию трафика, чтобы все пакеты шли через UserGate либо настроить правило SNAT для отправки такого трафика от имени UserGate.

KnowledgeBase: 

Product: UserGate NGFW

Задача

Необходимо оперативно заблокировать пользователю доступ через VPN.

Решение

Необходимо создать для пользователя запрещающее правило межсетевого экрана.

В результате создания правила, пользователь будет подключаться по VPN, но не будет иметь доступа к ресурсам.

Примечание Если сбросить сессию пользователя, то клиент автоматически переподключится, поэтому данный вариант не работает.

KnowledgeBase: 

Product: UserGate NGFW

Задача

При использовании инспектирования SSL в журнале веб-доступа появляются ошибки **TLS Server Alert: Fatal - Bad Record Mac**, **TLS Server Alert: Fatal - Protocol Version**, **TLS Client Alert: Fatal - Unknown Ca** и т.п.

Решение

Ошибки **TLS Server Alert: Fatal - Bad Record Mac** и **TLS Server Alert: Fatal - Protocol Version** возвращают браузеры пользователей вследствие наличия ошибок конфигурации. Для обеспечения максимальной совместимости UserGate поставляется с созданными по умолчанию профилями SSL (подробнее читайте в главе [Профили SSL](#)).

Ошибка **TLS Client Alert: Fatal - Unknown Ca** возникает, если в браузеры пользователей не установлен сертификат для дешифрования SSL-трафика. Подробнее об установке сертификата читайте соответствующей [главе](#) руководства администратора.

KnowledgeBase: 

Product: UserGate NGFW

Задача

При настройке VPN на клиентском компьютере необходимо указать протокол PAP для авторизации пользователя.

Решение

На устройствах с операционной системой MacOS запретите использование протоколов авторизации, отличных от PAP. Для этого выполните в терминале следующие команды:

```
echo refuse-chap > ~/.ppprc  
echo refuse-mschap >> ~/.ppprc  
echo refuse-mschap-v2 >> ~/.ppprc>
```

Результатом выполнения команд является создание файла ~/.ppprc со следующим содержимым:

```
refuse-chap  
refuse-mschap  
refuse-mschap-v2
```

KnowledgeBase: 

Product: UserGate NGFW

Задача

В журнале веб-доступа присутствуют избыточные записи о срабатываниях правил контентной фильтрации (переход по ссылке может сформировать 20-30 записей).

Решение

Такое поведение обусловлено особенностями работы веб-сервиса - невозможно отличить, когда переход совершен браузером, а когда пользователем.

Для изучения рекомендуется:

- создать дубликат общего для всех пользователей правила, указав одного пользователя, который будет использоваться для тестирования правил;
- отключить журналирование общего правила.

Таким образом будет легче разобраться в механизме веб-фильтров и изучить работу созданных правил.

Примечание Представленные выше действия не уменьшат количество срабатываний, приходящееся на одного пользователя, а лишь упростят процесс изучения работы веб-фильтра, т.к. будут журналироваться действия только одного пользователя.

KnowledgeBase: 

Product: UserGate NGFW

Задача

Необходимо проверить что правила антиспам модуля находятся в рабочем состоянии и выполняют свою задачу.

Решение

Проверить работу антиспам фильтра можно с помощью шаблона GTUBE (Generic Test for Unsolicited Bulk Email). Для этого нужно создать почтовое сообщение, содержащее следующую строку(без пробелов и переносов) и отправить его на Ваш почтовый адрес:

XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X

Работу антиспам фильтра можно посмотреть с помощью виджетов [Графики защиты почты](#) и [Сводные показатели защиты почты](#) в разделе [Дашборд](#).

Примечание Данные виджеты можно добавить с помощью кнопки [Добавить виджет](#).

Также возможно отслеживать результаты работы антиспам фильтров UserGate по логам самих почтовых серверов, которые находятся за периметром UserGate, если в вашем правиле стоит функция [Маркировать](#) - тогда письма будут приходить с дополнительным тегом [SPAM].

Примечание Нужно учитывать, что блокировка писем будет срабатывать только при выбранном действии [Блокировать](#) в правиле фильтрации SMTP и POP3 трафика. **Примечание** При выбранном действии [Блокировать с ошибкой](#) UserGate будет отсылать ошибку о недоступности сервера отправителю.

Product: UserGate NGFW

Сертификат ФСТЭК относится к решению в целом, а не к его конкретной версии. UserGate в должном порядке вносит изменения в свое сертифицированное средство защиты информации, как это предусмотрено [Приказом ФСТЭК №55](#) от 03 апреля 2018 года (см. п. 71, 73, 74).

Исходя из этого, в любой период времени правильным является использование последней версии решения UserGate со всеми новейшими обновлениями. О выходе версии сообщено во ФСТЭК, и она передана в испытательную лабораторию для проведения испытаний. Обновления сертификатов, технических условий и формуляра происходит в установленном ФСТЭК порядке после окончания испытаний, информация об этом доводится до пользователей сертифицированного решения. С более детальной информацией можно ознакомиться [на сайте UserGate](#).

KnowledgeBase: 
 Product: UserGate NGFW
 Version: 6.x, 7.x
 Technology: VPN

Задача

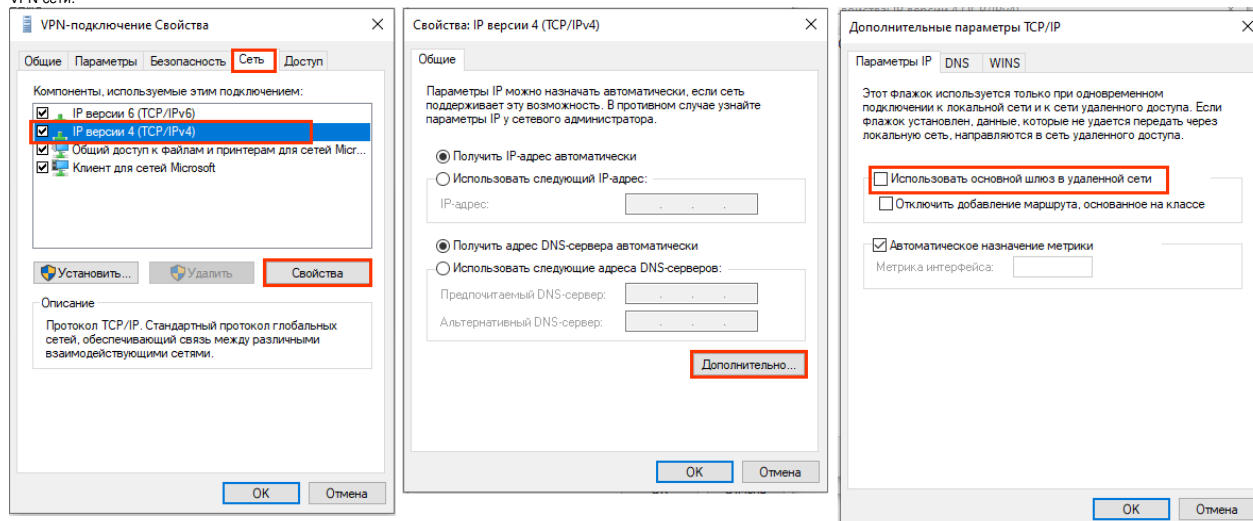
При подключении по VPN устройства с ОС Windows разрывают соединение.

Решение

Разрыв соединения происходит после получения системой отрицательного результата проверки доступности сети Интернет (для проверки доступности выполняется запрос на ресурс www.msftconnecttest.com).

Для решения проблемы добавьте разрешающее правило контентной фильтрации, указав зону источника, с которой происходит подключение пользователей по VPN.

Также можно на компьютере в свойствах VPN-подключения отключить использование основного шлюза в удалённой сети, тогда ОС Windows не будет выполнять разрыв соединения при отсутствии на NGFW разрешающего правила контентной фильтрации. В этом случае при VPN-подключении шлюз по умолчанию не изменится, а нужные маршруты будут получены компьютером от NGFW в соответствии с настройками VPN-сети.



KnowledgeBase: 

Version: 7.0.0, 6.x

Задача

Из локальной сети нет доступа к ресурсам, опубликованным с использованием правил reverse-прокси, по внешнему URL.

Решение

Для обеспечения доступа пользователей локальной сети к ресурсам, опубликованным с помощью reverse-прокси, через адрес внешнего интерфейса необходимо:

1. Создать правило межсетевого экрана, разрешающее соединение из зоны интерфейса UserGate, за которым находится локальная сеть, в зону интерфейса, к которому подключён сервер.
2. Разрешить сервис **Reverse-прокси** на зоне интерфейса, к которому подключена локальная сеть.
3. В настройках правила reverse-прокси добавить зону, которой принадлежит локальная сеть, в качестве зоны источника.
4. Если локальная сеть и сервер находятся за одним интерфейсом, то не отмечайте чекбокс **Сохранять адрес источника** в настройках сервера reverse-прокси, в противном случае - настройте правило NAT для соединений из локальной сети.

ПримечаниеВ связи с изменениями данная инструкция неактуальна для версии 6.1.9.

Для обеспечения доступа к опубликованным ресурсам из локальной сети по внешнему URL для версии 6.1.9 необходимо на внутреннем DNS-сервере создать запись типа A, которая будет разрешать FQDN ресурса во внутренний IP-адрес сервера.

KnowledgeBase: 

Product: UserGate NGFW

Version: 5.x, 6.x, 7.x

Technology: VPN

Задача

Настроен Site-to-Site VPN между двумя UserGate, маршруты до внутренних сетей прописаны. После подключения наблюдается низкая скорость передачи.

Решение

Необходимо сделать исключения защиты от DoS для адресов интерфейсов, которые используются для построения VPN-туннеля. Исключения добавляются в свойствах зоны, которой принадлежит интерфейс, в разделе **Сеть → Зоны**.

KnowledgeBase: 

Product: UserGate NGFW

Version: 5.x, 6.x, 7.x

Technology: VPN

Вопрос

Можно ли развернуть VPN за UserGate, если на нём уже настроен VPN?

Ответ

Да, можно, если сервер за UserGate использует UDP-порты отличные от 500 и 4500 или на внешнем интерфейсе UserGate есть второй адрес.

На UserGate произведите следующие настройки:

1. Создайте сервис, указав протоколы и порты, используемые разворачиваемым за UserGate сервером.
2. Создайте правило DNAT и укажите созданный сервис.

Product: UserGate NGFW, UserGate LogAn
Version: 6.x, 7.x

Задача

Возникает ошибка **Мало места на разделе для журналов**.

Решение

Данное сообщение информирует о превышении 95% занимаемого места от размера диска. Ротация журналов происходит автоматически при заполнении раздела на 99%, т.е. старые данные удаляются, освобождая место для записи новых. Место на диске освобождается небольшими блоками, поэтому данное сообщение будет периодически появляться.

Записи о ротации базы данных будут отображены в журнале событий. В случае, если подключен LogAn, то запись будет отображена в журнале событий Log Analyzer.

Примечание Записи журнала событий никогда не ротируются.

Если требуется хранить журналы за больший период времени, то можно добавить дополнительный диск или увеличить размер существующего диска на виртуальной машине. Далее необходимо выполнить перезагрузку UserGate; при загрузке в **Support Menu** необходимо выполнить увеличение раздела для журналов на весь выделенный диск (**Expand log partition**); данный метод доступен в ПО версий 6.1.x.

В ПО версий 7.x возможно увеличить размер системного раздела. Подробнее читайте в статье: [Расширение системного раздела](#).

Примечание Если NGFW подключён к Log Analyzer, то добавление дополнительного диска или увеличение размера существующего диска производится на LogAn.

Product: UserGate NGFW
Version: 5.x, 6.x, 7.x

Задача

У пользователя на терминальном сервере в браузере периодически появляется ошибка "**Нет подключения к прокси серверу**". С чем это может быть связано?

Решение

Терминальный сервер перехватывает запросы от каждого пользователя и назначает свой диапазон портов. По диапазону портов NGFW идентифицирует пользователей терминального сервера.

Терминальный сервер использует следующий диапазон портов: 5000 - 49000 (всего 44000 портов). Агент, по умолчанию, настроен на работу 50 пользователей, на каждого из которых выделяется 880 портов; если портов не хватает, то соединения не будут установлены.

Проверьте журнал работы агента (файл **entsagent** в папке %ALLUSERSPROFILE%\Entensys\Terminal Server Agent\). Если есть сообщение **not enough ports**, то подключение не устанавливается из-за нехватки портов.

В настройках агента терминального сервера можно изменить количество пользователей, которые будут использовать агент терминального сервера. Если уменьшить количество пользователей, то на каждого пользователя будет выделено больше портов, и наоборот. Диапазон портов назначается пользователю после его регистрации на терминальном сервере, данная информация передаётся на NGFW. Освобождение диапазона происходит после прекращения сеанса работы в качестве зарегистрированного пользователя терминального сервера.

ПримечаниеВесь доступный диапазон портов делится на указанное число пользователей и, соответственно, каждому пользователю выделяется ограниченное количество портов.

Файл конфигурации **tsagent.cfg** находится в той же папке, что и журнал работы агента. Для указания количества пользователей измените параметр **Maximum user count**.

ПримечаниеЕсли выделяются порты для системной учетной записи, то в журнале формируется запись вида: *user 'NT AUTHORITY\SYSTEM' port range 5000-5879*.

ПримечаниеПосмотреть порты, используемые пользователем, можно в журнале веб-доступа, сделав соответствующую выборку.

Если терминальных подключений много, то можно добавить на интерфейс сервера еще адрес (или несколько); при добавлении адреса количество доступных портов увеличивается в 2 раза.

Ошибка: Попытка L2TP-подключения не удалась из-за ошибки, произошедшей на уровне безопасности, во время согласований с удаленным компьютером

Product: UserGate NGFW
Version: 5.x, 6.x, 7.x
Technology: VPN

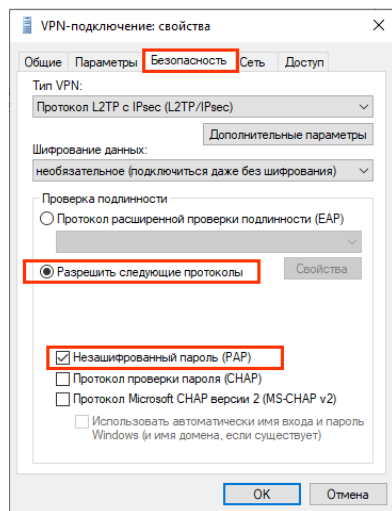
Задача

При попытке подключения к VPN отображается ошибка: **Попытка L2TP-подключения не удалась из-за ошибки, произошедшей на уровне безопасности, во время согласований с удаленным компьютером**.

Решение

На клиентском ПК проверьте:

- параметр **AssumeUDPEncapsulationContextOnSendRule** в реестре должен принимать значение **2** (т.е. Windows может установить связи безопасности, когда сервер и клиентский компьютер находятся за устройствами NAT);
- значение параметра **HKLM\SYSTEM\CurrentControlSet\Services\RasMan\Parameters\ProhibitIpSec** должно принимать значение **0**;
- настройки безопасности адаптера:



Примечание В случае внесения изменений в реестр, компьютер необходимо перезагрузить.

Product: UserGate NGFW

Version: 5.x, 6.x, 7.x

Technology: Networking

Вопрос

Как правильно использовать пул IP-адресов для NAT трансляции?

Ответ

В настройках правила типа **NAT** укажите пул IP-адресов в виде диапазона адресов, которые будут использоваться для замены адреса источника при подмене адресов пакетов (поле **SNAT IP**). Например, 10.10.0.2-10.10.0.10.

KnowledgeBase: 
Product: UserGate NGFW
Version: 6.x, 7.x

Вопрос

Как настроить запись трафика на NGFW?

Ответ

Запись трафика осуществляется на вкладке **Диагностика и мониторинг** в разделе **Сеть → Захват пакетов**.

Например, для записи трафика TCP с адреса 10.0.0.1, подключённого к port1, произведите следующие действия:

1. На панели **Фильтры** произведите настройку фильтров:
 - **Источник**: 10.0.0.1 (IP-адрес источника, трафик с которого необходимо записать);
 - **IPv4 протокол**: 6 (в соответствии с <http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml>).

При настройке фильтра также можно указать порт источника/назначения.

2. На панели **Правила** создайте правило захвата пакетов. При настройке укажите интерфейс NGFW, который используется для маршрутизации трафика (port1), и добавьте ранее созданный фильтр. Для начала/остановки записи трафика используйте соответствующие кнопки **Начать запись/Остановить запись**.
3. Файл PCAP доступен для скачивания на панели **Файл** (по умолчанию панель скрыта; для отображения нажмите стрелочку в правом верхнем углу).

ПримечаниеЕсли в настройках фильтра указан только адрес источника или только назначения, то будет записываться трафик в одну сторону.

KnowledgeBase: 

Product: UserGate NGFW

Version: 5.x, 6.x, 7.x

Вопрос

Как выполнить очистку журналов (событий, веб-доступа и т.д.)?

Ответ

Журналы удалить невозможно, так как это требования информационной безопасности.

Возможность удаления журналов с устройства за определенный промежуток времени (или все сразу) позволяет скрыть нарушения безопасности. Управление журналами автоматизировано и не требует участия администратора, журналы циклически перезаписываются, обеспечивая необходимое для работы свободное дисковое пространство.

Примечание Записи журнала событий никогда не ротируются.

Ротация записей журналов (всех, кроме журнала событий) происходит автоматически по критерию свободного пространства на данном разделе. При работе с большими дисками (более 100GB) критерий очистки установлен в **99%** занятого места: удаляется раздел журналов с самыми старыми данными, освобождая место для записи новых. Записи о ротации базы данных будут отображены в журнале событий. В случае, если подключен LogAp, то запись будет отображена в журнале событий Log Analyzer.

Product: UserGate NGFW, UserGate MC, UserGate LogAn
Version: 6.x, 7.x

Вопрос

Что предполагают **Backup full** и **Backup system only** в **Support Menu**?

Ответ

Backup full предполагает создание полной копии диска UserGate. Для определения размера съёмного носителя можно посмотреть информацию в Дашборд, виджет **Диски** (сложить значения колонки **"Занято"**). Для сжатия данных используется **gzip**.

Backup system only создаёт полную копию только системного раздела UserGate с абсолютно всеми настройками, состоянием кластера и лицензией; раздел журналов не копируется.

ПримечаниеС версии 7.x.x доступно создание только полной копии диска UserGate: *Create backup*.

KnowledgeBase: 

Product: UserGate NGFW

Version: 5.x, 6.1.8, 6.1.9, 7.0.0, 7.0.2, 7.1.0, 7.2.0, 6.x, 7.x

Technology: LDAP

Задача

Некорректно отображаются пользователи в журнале веб доступа.

Вместо корректного отображения имени пользователя, оно появляется в формате логина или имени APM, на котором пользователь работает.

Решение

Данный эффект может наблюдаться в случае если доменный адрес в настройках сервера авторизации прописан некорректно. В этом случае ответ от LDAP-сервера содержит недопустимый по настройкам домен, что и приводит к описанному эффекту. Для устранения проблемы необходимо в настройках серверов авторизации на вкладке **домены-LDAP** добавить все допустимые в вашем контексте домены.

KnowledgeBase: 
Product: UserGate NGFW
Version: 5.x, 6.x, 7.x
Technology: Content Filtering

Вопрос

Можно ли отключить список DNSBL не удаляя его?

Ответ

Можно убрать галочку **DNSBL проверка** это не повлияет на список адресов в DNSBL, в дальнейшем ее можно включить обратно.

Свойства

Общие

Источник

Пользователи

Назначение

Сервис

Envelope from

Envelope to

Включено:

☐

Название:

DNSBL spam drop rule

Описание:

Quick spam drop rule. Must be first in the list and should not have exclusions Envelop from and Envelop to. Action should be set to Drop.

Действие:

Блокировать без ошибки

☐ Проверка антиспама UserGate

☒ DNSBL проверка (только SMTP)

Заголовок:

Subject

Маркировка:

Сохранить

Отмена

Также можно создать отдельное правило, с этой установленной галочкой. Правила можно отключать не удаляя их, через правую кнопку мыши

#	Название	Сервис	Действие		Зона источника
1	DNSBL spam drop rule	SMTP	Блокировать без ошибки		Untrusted
2	SMTP & POP3 filtering	SMTP POP3 SMTPS POP3S	Маркировать		Untrusted

Добавить

Редактировать

Удалить

Переместить

Копировать

Включить

Отключить

Обновить

Product: LogAn
Version: 6.x, 7.x

Вопрос

Где хранятся системные журналы после подключения NGFW к LogAn?

Ответ

После подключения LogAn, все сообщения отправляются на него. На NGFW в этом случае ничего не хранится. При просмотре журналов на NGFW, они берутся с LogAn.

Version: 5.x, 6.x, 7.x
Technology: SSL Inspection

Задача

Не открываются сайты во всех браузерах кроме Yandex browser при включенном SSL-инспектировании. Необходимо сделать сайты доступными со всех браузеров.

Решение

Это ошибка, возможно, связана с применением браузерами механизма HSTS (в Yandex browser этот механизм по умолчанию отключен). Для решения проблемы необходимо почистить кэш браузера, в случае переносного оборудования. Либо, как вариант, заблокировать применение протокола QUIC браузерами.

Для Mozilla Firefox:

1. Откройте страницу расширенных настроек браузера, написав в адресной строке *about:config* и нажав **Enter**.
2. Скопируйте в строку поиска **network.http.http3.enabled**.
3. измените значение опции на **FALSE** (означает, что поддержка HTTP/3 включена).

Для Google Chrome/Opera:

1. Введите в адресную строку **chrome://flags/** и перейдите по этому адресу (для Opera — *opera://flags/*).
2. В поисковой строке открывшегося меню разработчиков введите **Quic**.
3. Отключите пункт Experimental QUIC protocol, установив значение **Disabled**.

Задача

Как сконфигурировать UserGate NGFW для использования нескольких контроллеров домена?

Решение

Создайте один коннектор контроллера домена и укажите в нем вместо FQDN контроллера домена сам домен. В этом случае обращение будет происходить по очереди к каждому контроллеру, указанному в зоне DNS, т.е. при недоступности первого контроллера произойдет обращение к следующему, пока не будет установлено соединение.

В случае недоступности части контроллеров домена с площадки, где работает NGFW, следует добавить статическую запись в настройки DNS, где были бы указаны адреса доступных контроллеров, и использовать имя этой записи в коннекторе.

Как разрешить работу офисной SIP ATC через UserGate?

Product: UserGate NGFW

Version: 6.x

Задача

Необходимо разрешить работу офисной SIP ATC через VPN UserGate.

Решение

Для решения нужно разрешить загрузку модуля SIP в командной строке UserGate NGFW при помощи следующей команды:

```
UTM> device config -set module_sip_enabled true
```

Ошибка: System is booting... LOM card present

Product: UserGate NGFW, UserGate MC, UserGate LogAn, UserGate C100, UserGate D200/D500, UserGate E1000/E3000, UserGate F8000, UserGate X1, UserGate Log Analyzer E6/E14, UserGate Log Analyzer F25, UserGate Management Center C, UserGate Management Center E, KinderGate Родительский контроль, UserGate C150
Version: 6.x, 7.x

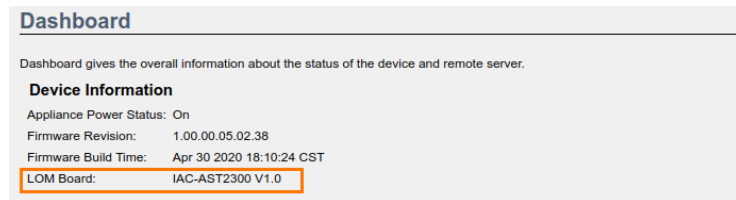
Задача

На программно-аппаратных комплексах (ПАК) UserGate возникает ошибка **System is booting... LOM card present**; устройство зависает на этапе загрузки.

Решение

В случае возникновения ошибки выполните следующие действия:

1. Отключите питание на 5-10 минут. После включения ПАК должен загрузиться в штатном режиме, в противном случае, обратитесь в службу технической поддержки UserGate.
2. После загрузки ПАК, можно проверить версию IPMI, подключившись к DashBoard



Если версия отличается от представленной на рисунке, необходимо [обновить](#) версию IPMI.

Product: UserGate NGFW

Version: 5.x, 6.x, 7.x

Задача

Необходимо настроить работу AnyDesk, используется инспектирование SSL.

Решение

Создайте список URL, содержащий запись (дословно, без кавычек): **"AnyNetRelay"**, и добавьте этот список в исключения инспектирования SSL.

Примечание AnyDesk при запросе не отправляет SNI, а при TLS-соединении отправляет CN=AnyNetRelay.

Product: UserGate NGFW

Version: 5.x, 6.x, 7.x

Задача

Перестало работать правило с расписанием типа **Повторяющиеся события**; отмечен чекбокс **Весь день**.

Решение

Для расписаний с типом повторения **Повторяющиеся события** присутствует ошибка в веб-интерфейсе управления UserGate. В настройках данного типа повторения наличие чекбокса **Весь день** является ошибочным, т.к. при его активации событие закончится в 00:00 и больше не повториться.

Для данного типа повторения пользователю необходимо указать интервал времени, в которое правило будет активно, и диапазон дат, т.е., чтобы правило работало весь день, можно указать период с 00:00 по 23:59, тогда правило не будет работать только 1 минуту в день. Чтобы правило работало весь день рекомендуется использовать интервал типа **Диапазон времени**.

Как добавить сетевые адаптеры к UserGate (Virtual Appliance)?

Product: UserGate NGFW, UserGate MC, UserGate LogAn

Version: 5.x, 6.x

Technology: Networking

Задача

Необходимо добавить сетевые интерфейсы в виртуальную машину.

Решение

После добавления сетевых интерфейсов на виртуальной машине необходимо перезагрузиться и при загрузке в **Boot Menu** выбрать пункт **Support menu → Refresh NIC names**, подробнее об этой и других служебных утилитах читайте в соответствующем [разделе](#) руководства администратора.

Внимание!VMware присваивает MAC-адреса в определенном порядке, а в устройствах UserGate (Virtual Appliance) сортировка интерфейсов производится по возрастанию MAC-адресов. Поэтому после выполнения Refresh NIC names необходимо проверить соответствие MAC-адресов в настройках VMWare и на устройстве UserGate. В случае необходимости, измените в настройках виртуальной машины подключение сетевых адаптеров к виртуальным сетям.

Экспорт и импорт политик UserGate через CLI

Product: NGFW
Version: 7.x
ПримечаниеЭкспорт и импорт правил с использованием CLI доступен с версии 7.0.0.

Импорт доступен в следующих разделах:

- Сеть: правила DNS;
- Пользователи и устройства: правила captive-портала;
- Политики сети: правила межсетевого экрана, NAT и маршрутизации, пропускной способности;
- Политики безопасности: правила фильтрации контента, веб-безопасности, инспектирования туннелей, инспектирования SSL, инспектирования SSH, защиты почтового трафика, ICAP, защиты DoS, системы обнаружения и предотвращения вторжений, сценарии;
- Глобальный портал: правила веб-портала и reverse-прокси;
- VPN: серверные и клиентские правила.

Указанные выше правила настраиваются с использованием UserGate Policy Language (UPL), подробную информацию о котором вы можете найти в соответствующем [разделе](#) руководства администратора.

Рассмотрим экспорт и импорт правил на примере правил межсетевого экрана. На NGFW созданы следующие правила:

Межсетевой экран														
Добавить Редактировать Удалить Переместить Копировать Включить Отключить Скопировать ID правила Открыть логи Сбросить счётчики Все Принуд														
#	C...	Название	Действие	Зона источ...	Адрес ...	Зона назначения	Адрес н...	Пользовате...	Сервис	Приложения	Время	Сценарий	Кол-во с...	Исто...
1	(...)	web1	Запретить	Trusted	Любой	Любая	Любой	Любой	Любой	Любое	Любое	—	0	Среа...
2	(...)	web2	Запретить	DMZ	Любой	Untrusted	Любой	Любой	Любой	Любое	Любое	—	0	Среа...
3	(...)	web3	Разрешить	Любая	Любой	Любая	Любой	Любой	Любой	Любое	Любое	—	0	Среа...
4	(...)	Default block	Запретить	Любая	Любой	Любая	Любой	Любой	Любой	Любое	Любое	—	—	—

ПримечаниеПравила созданы для демонстрации примера.
ПримечаниеПосле выполнения импорта все существующие правила раздела будут заменены на импортированные.

1. Для редактирования правила могут быть сохранены в файл конфигурации или скопированы из интерфейса командной строки. В обоих вариантах используется подключение к интерфейсу командной строки по SSH.

Для сохранения правил в файл, например, **fw_config.cfg**, выполните следующую команду:

```
ssh Admin@IP_ADDRESS -p 2200 show network-policy firewall >fw_config.cfg
```

где Admin - имя администратора;

IP_ADDRESS - адрес интерфейса UserGate.

Введите пароль учетной записи администратора, файл со списком правил будет сохранён на вашем устройстве.

Для копирования правил из интерфейса командной строки подключитесь к CLI по SSH:

```
ssh Admin@IP_ADDRESS -p 2200
```

где Admin - имя администратора;

IP_ADDRESS - адрес интерфейса UserGate.

Подключение по SSH необходимо для возможности копирования правил.

ПримечаниеКоманды выполняются в режиме конфигурации.

Для перехода в режим конфигурации используйте следующую команду:

```
Admin@UGOS> configure
```

Отобразите в CLI правила раздела, которые необходимо выгрузить:

```
Admin@UGOS# show network-policy firewall
```

ПримечаниеИспользуйте *Tab* или *?* для просмотра текущих возможных значений или автодополнения.

Также действия над правилами могут быть выполнены после перехода на уровень раздела, в таком случае не нужно указывать уровень для каждой команды:

```
Admin@UGOS# edit network-policy firewall
```

```
[ network-policy firewall ]  
Admin@UGOS# show
```

Результат выполнения команды:

```
[ network-policy firewall ]  
Admin@UGOS# show  
% ----- 1 -----  
DENY \  
src.zone = Trusted \  
enabled(true) \  
id(ba1abe50-f492-4e12-8a12-86df83b40a81) \  
name(web1)  
% ----- 2 -----  
DENY \  
src.zone = DMZ \  
dst.zone = Untrusted \  
enabled(true) \  
id(dd3b23e2-261d-48a5-8e63-3967ceb840b6) \  
name(web2)  
% ----- 3 -----  
PASS \  
enabled(true) \  
id("4e537010-322e-45e8-a1e1-7390f2300bce") \  
name(web3)
```

2. Скопируйте правила для редактирования; используйте, например, текстовый редактор.

ПримечаниеНе копируйте строку с позицией первого правила.

Отредактируйте необходимые параметры правила. Для примера изменим названия правил на **cli1**, **cli2** и **cli3**, соответственно:

```
DENY \  
src.zone = Trusted \  
enabled(true) \  
id(ba1abe50-f492-4e12-8a12-86df83b40a81) \  
name(cli1)  
% ----- 2 -----  
DENY \  
src.zone = DMZ \  
dst.zone = Untrusted \  
enabled(true) \  
id(dd3b23e2-261d-48a5-8e63-3967ceb840b6) \  
name(cli2)  
% ----- 3 -----  
PASS \  
enabled(true) \  
id("4e537010-322e-45e8-a1e1-7390f2300bce") \  
name(cli3)
```

name(cli3)

3. Импортируйте правила. Выделите и скопируйте правила в редакторе. Перейдите в CLI, введите команду **import upl-rule** и вставьте скопированные правила:

```
[ network-policy firewall ]
Admin@UGOS# import upl-rule DENY \
...   src.zone = Trusted \
...   enabled(true) \
...   id(ba1abe50-f492-4e12-8a12-86df83b40a81) \
...   name(cli1)
... % ----- 2 -----
... DENY \
...   src.zone = DMZ \
...   dst.zone = Untrusted \
...   enabled(true) \
...   id(dd3b23e2-261d-48a5-8e63-3967ceb840b6) \
...   name(cli2)
... % ----- 3 -----
... PASS \
...   enabled(true) \
...   id("4e537010-322e-45e8-a1e1-7390f2300bce") \
...   name(cli3)
...
[ network-policy firewall ]
Admin@UGOS#
```

4. Проверьте изменения в CLI:

```
[ network-policy firewall ]
Admin@UGOS# show

% ----- 1 -----
DENY \
  src.zone = Trusted \
  enabled(true) \
  id("082ed6ed-20b6-4c93-921a-047eb9ff40a4") \
  name(cli1)
% ----- 2 -----
DENY \
  src.zone = DMZ \
  dst.zone = Untrusted \
  enabled(true) \
  id(f5f08dbd-019f-490a-8cfa-342c34a348fa) \
  name(cli2)
% ----- 3 -----
PASS \
  enabled(true) \
  id(b5ad3589-98d4-4911-8cf2-9590d0f3f4ea) \
  name(cli3)
```

или веб-интерфейсе:

Межсетевой экран

Добавить

Редактировать

Удалить

Переместить

Копировать

Включить

Отключить

Скопировать ID правила

Открыть логи

Сбросить счётчики

Все

Принуд

✓

🔍

#	С...	Название	Действие	Зона источ...	Адрес ...	Зона назначения	Адрес н...	Пользовате...	Сервис	Приложения	Время	Сценарий	Кол-во с...	Исто...
1	(...)	cli1	🚫 Запретить	🖥️ Trusted	Любой	Любая	Любой	Любой	Любой	Любое	Любое	—	0	Среа...
2	(...)	cli2	🚫 Запретить	🖥️ DMZ	Любой	🖥️ Untrusted	Любой	Любой	Любой	Любое	Любое	—	0	Среа...
3	(...)	cli3	✅ Разрешить	Любая	Любой	Любая	Любой	Любой	Любой	Любое	Любое	—	0	Среа...
4	(...)	Default block	🚫 Запретить	Любая	Любой	Любая	Любой	Любой	Любой	Любое	Любое	—	—	—

Product: UserGate NGFW, UserGate MC, UserGate LogAn
Version: 5.x, 6.x, 7.x

Задача

Интеграция с центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ).

Решение

Компания UserGate сотрудничает с ФинЦЕРТ: информация синхронизируется со списком IP-адресов бот-сетей и списком URL фишинговых сайтов.

Product: UserGate NGFW

Version: 6.x, 7.x

Technology: VPN

Вопрос

Поддерживается ли технология VxLAN в UserGate NGFW?

Ответ

Да, UserGate NGFW может обрабатывать трафик, получаемый из удаленной сети и упакованный посредством технологии VxLAN.

Product: UserGate MC
Version: 7.x

Задача

Добавление групп/пользователей LDAP в настройках правил в шаблонах управляемых устройств.

Решение

Начиная с версии Management Center 7.x.x для возможности использования групп и пользователей LDAP в политиках безопасности UserGate, настраиваемых в шаблонах управляемых устройств (шаблоны NGFW и конечных устройств), необходимо корректно настроить LDAP-коннектор в разделе **Центр управления → Каталоги пользователей** консоли управления областью. Подробнее о настройке каталогов пользователей читайте в разделе [Каталоги пользователей](#).

ПримечаниеДля NGFW: серверы аутентификации, настраиваемые в шаблонах, не будут отображены в свойствах правил в списке LDAP-серверов и, следовательно, не могут быть использованы для указания пользователей.

Product: UserGate NGFW
Version: 6.x, 7.x
Technology: Routing

Задача

Часто возникают проблемы с открытием сайтов - **Ошибка подключения: не удалось найти имя хоста или домен**.

Решение

Ошибка такого типа может возникать в случае, когда UserGate не может разрешить доменное имя, на которое происходит обращение при явно указанном прокси. Это означает, что какие-то из DNS-серверов, указанных в настройках, работают неустойчиво.

Серверы некоторых интернет-провайдеров могут отвечать ошибкой на запросы, поступающие с адресов другого провайдера. Проверку можно произвести в разделе **Сеть → Запрос DNS** вкладки **Диагностика и мониторинг** (подробнее читайте в разделе [Запрос DNS](#)).

Для использования таких серверов необходимо настроить правила типа Policy-based routing (PBR), которые будут перенаправлять трафик на эти серверы через шлюзы соответствующего провайдера. Чтобы эти правила были применены к запросам, генерируемым UserGate, не указывайте зону источника трафика, т.е. не должно быть отмечено ни одной зоны - зона **Любая**. Подробнее о настройке правил PBR читайте в разделе [Policy-based routing](#).

Также возможен вариант использования публичных DNS-серверов, отвечающих на запросы вне зависимости от используемого провайдера.

Product: UserGate NGFW
Version: 6.x

Задача

Необходимо создать сервис без указания порта назначения.

Решение

При создании сервиса на UserGate 6.x.x указание порта назначения является обязательным. Указание всего диапазона портов (0-65535) никак не скажется на работе правил.

Примечание При настройке сервисов на UserGate 7.x.x указание портов назначения не является обязательным.

Product: UserGate NGFW, UserGate MC, UserGate LogAn
Version: 7.x

Задача

Необходимо расширить системный раздел узла UseGate v7.x.

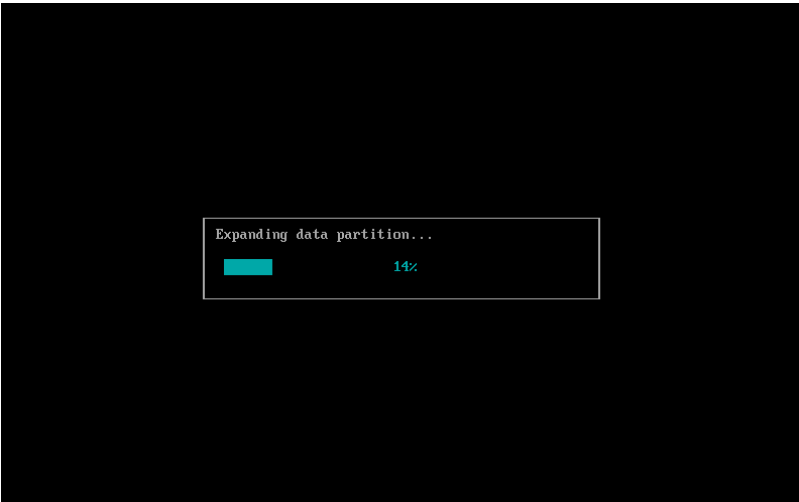
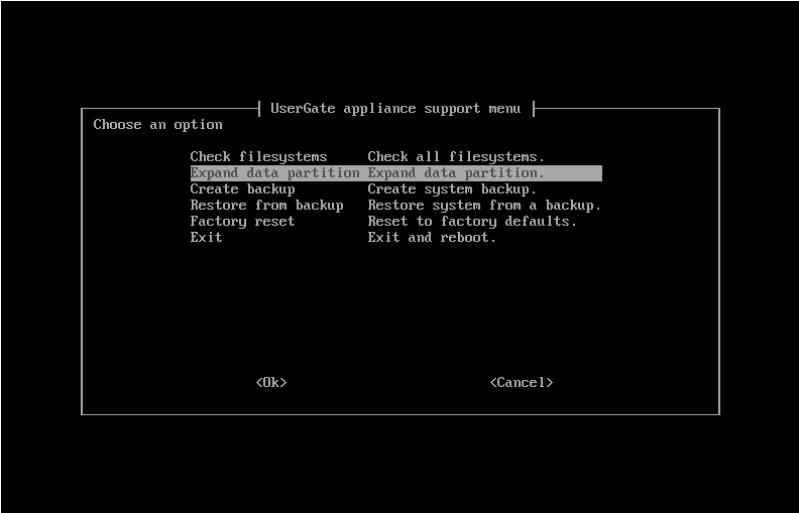
Решение

Для расширения системного раздела с сохранением конфигурации и данных узла UserGate необходимо выполнить следующие шаги:

- 1. Средствами гипервизора добавить **новый** диск необходимого размера в свойствах виртуальной машины UserGate.
- 2. В меню загрузки узла UserGate войти в раздел **Support menu**:



- 3. В открывшемся разделе выбрать **Expand data partition** и запустить процесс расширения системного раздела:



- 4. После завершения процесса расширения загрузить узел и в разделе **Дашборд → Диски** проверить размер системного раздела:

Disks			 
	In use	Total	
System partition (Clean)	165.82 MB	144 GB	

Product: UserGate NGFW
Version: 5.x, 6.x, 7.x
Technology: VPN

Задача

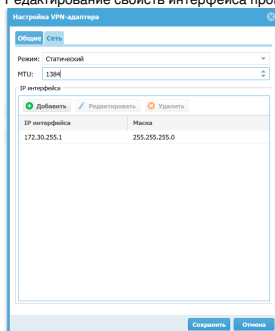
Настроен Site-to-Site VPN между двумя устройствами UserGate. При установке соединения в направлении КЛИЕНТ - СЕРВЕР наблюдается низкая скорость и нестабильная работа туннеля; при соединениях СЕРВЕР - КЛИЕНТ проблем не наблюдается.

Решение

Одной из возможных причин такого поведения может быть фрагментация пакетов. Если пакеты, передаваемые через VPN-туннель, превышают максимальный размер MTU на любом из промежуточных устройств, они могут быть разделены на фрагменты. Это может привести к увеличению задержки и потере производительности. Путем установки оптимального значения MTU на туннельном интерфейсе можно избежать фрагментации и снизить задержку.

Значение MTU на туннельных интерфейсах, созданных по умолчанию и предназначенных для соединения Site-to-Site VPN, по умолчанию установлено 1420 байт. Требуется уменьшить значение MTU до 1384.

Редактирование свойств интерфейса производится в разделе: **Сеть → Интерфейсы**.



Примечание Важно отметить, что при изменении MTU на туннельных интерфейсах необходимо убедиться, что все устройства на пути передачи данных поддерживают выбранное значение MTU.

Product: SIEM
Version: 7.x

Задача

Используя UserGate SIEM, настроить правило аналитики для поиска срабатываний правил защиты от DoS-атак и автоматического добавления адреса источника атаки в список блокируемых адресов на группу NGFW.

Решение

В данном примере будет рассмотрена настройка правила аналитики для группы NGFW, которое срабатывает при получении события о срабатывании правила защиты DoS на одном NGFW и отправляет команду на добавление IP-адреса источника в предварительно созданный на всех NGFW список адресов, который уже используется в правилах межсетевого экрана (МЭ) для блокировки нежелательных соединений. Данная конфигурация работает в режиме превентивной защиты.

Примечание Правило аналитики работает после того, как условие, в нашем случае это нахождение в журнале срабатывания правила защиты от DoS, выполнится указанное количество раз. Опционально можно ограничить время выполнения условия, тогда правило аналитики сработает только в случае, если условие выполнится заданное количество раз за указанный отрезок времени.

1. Создать список IP-адресов на NGFW.

В разделе **Библиотеки** → **IP-адреса** на панели **Группы** нажать на кнопку **Добавить**, дать название списку IP-адресов, например, **Blocked_addresses**. Выполнить аналогичную настройку на каждом из NGFW в группе.

Свойства

Общие

Настройка расписания скачивания обновлений

Название списка:

Blocked_addresses

Описание:

Уровень угрозы:

средний

Тип:

Локальный

URL обновления:

Сохранить

Отмена

2. Создать правила МЭ на NGFW.

В разделе **Политики сети** → **Межсетевой экран** создать запрещающие правила, используя созданный ранее список **Blocked_addresses** в качестве адреса источника. Выполнить аналогичную настройку на каждом из NGFW в группе.

Межсетевой экран													
Добавить Редактировать Удалить Переместить Копировать Включить Отключить Скопировать ID правила Открыть логи Сбросить счётчики Все Принудительно применить													
#	Статус журнал...	Название	Действие	Зона источника	Адрес источника	Зона назначения	Адрес назначе...	Пользователи	Сервис	Приложения	Время	Сценарий	Кол-во срабат...
1		DoS_defny_test	Запретить	Любая	Blocked_add...	Любая	Любой	Любой	Любой	Любое	Любое	—	0

Подробнее о настройке правил читайте в разделе [Межсетевой экран](#) руководства администратора NGFW.

3. Создать правило защиты DoS на NGFW.

В разделе **Политики безопасности** → **Правила защиты DoS** нажать на кнопку **Добавить**, создать правило с действием **Защитить** и включить журналирование. Выполнить аналогичную настройку на каждом из NGFW в группе.

Правила защиты DoS												
Добавить Редактировать Удалить Переместить Копировать Включить Отключить Скопировать ID правила Открыть логи Все												
#	Статус журнали...	Название	Профиль DoS	Действие	Зона источника	Адрес источника	Зона назначения	Адрес назначения	Пользователи	Сервис	Время	Сценарий
1		DoS_1	DoS_profile_1	Защитить	Любая	Любой	Любая	Любой	Любой	Любой	Любое	—

Подробнее о настройке правил защиты DOS читайте в разделе [Защита от DoS атак](#) руководства администратора NGFW.

4. Подключить NGFW к SIEM.

В разделе **Сенсоры** → **Сенсоры UserGate** нажать на кнопку **Добавить**, указать параметры NGFW. Выполнить аналогичную настройку на каждом из NGFW в группе.

Сенсоры UserGate							
Добавить Редактировать Копировать Удалить Включить Отключить Показать детальную информацию Показать все 10 секунд							
Имя ↑	Адрес	Модель PAM	Версия	Лицензия	Время непрерывной работы	Мониторинг устройства	
UTM_7	172.25.84.51	VMware Virtual Platform	UserGate 7.0.1.905R	Зарегистрированная версия	6 д, 20 ч, 49 мин.	RAM: 10 % свободно Swap: 99% свободно CPU: 3% Сессии: 0 of 100	
UTM_7_1	172.25.84.155	VMware Virtual Platform	UserGate 7.0.1.905R	Зарегистрированная версия	34 мин.	RAM: 31 % свободно Swap: 100% свободно CPU: 4% Сессии: 0 of 100	

Подробнее о подключении NGFW к SIEM читайте в разделе [Сенсоры](#).

5. Создать список команд на SIEM.

На SIEM перейти в раздел **Библиотеки** → **Команды** и создать группу команд (на панели **Группы команд** нажать **Добавить** и указать название). На панели **Команды** нажать **Добавить** и указать название и следующий текст команды (синтаксис команды аналогичен синтаксису команд CLI NGFW. Подробнее о командах CLI читайте в разделе [Интерфейс командной строки](#) руководства администратора NGFW):

set libraries ip-list Blocked_addresses ips + [{SRC_IP}]

Свойства

Название:

SRC_IP

Текст команды:

set libraries ip-list Blocked_addresses ips + [{SRC_IP}]

Используйте фигурные скобки {} для определения переменных. Они будут трансформированы в тестовые поля для подстановки актуальных значений либо переменных второго уровня

Сохранить

Отмена

Данная команда будет отправлена на NGFW в качестве действия реагирования на срабатывание правила аналитики. При написании команды использована переменная **SRC_IP** — адрес источника, который при отправке команды добавляет IP-адрес источника в список IP-адресов **Blocked_addresses**, созданный ранее на NGFW.

6. Создать коннектор на SIEM.

На SIEM в разделе **Сенсоры** → **Коннекторы** нажать **Добавить** и указать свойства коннектора:

- Имя: название коннектора;
- Тип сервера: SSH;
- Адрес сервера: IP;
- IP-адрес: IP-адрес NGFW;
- Порт: порт сервера;

- **Логин:** логин пользователя для авторизации на коннекторе;
- **Пароль:** пароль учётной записи пользователя, необходимый для авторизации на коннекторе;
- **Группа команд:** группа команд, созданная на п.5.

Выполнить аналогичную настройку на каждом из NGFW в группе.

Коннекторы		
Добавить Редактировать Удалить ↺ ↻		
Имя	Описание	Группа команд
conn_UTM_7_1		command
conn_UTM_7		command

7. Создать действие реагирования на SIEM.
 Действие реагирования также может быть создано при настройке правила аналитики во вкладке **Действия реагирования** (нажать **Создать и добавить новый объект**).

Перейти во вкладку **Аналитика** веб-интерфейса SIEM. Во вкладке **Действия реагирования** нажать **Добавить** и указать свойства действия реагирования:

- Во вкладке **Общие** указать параметры:
 - поставить флажок **Включено**;
 - **Название** правила реагирования;
 - **Действие:** **Послать команду на коннектор** — отправка команды на выбранный коннектор.

- Во вкладке **Действие** добавить коннектор, созданный на шаге 6, и выбрать команду на добавления нового адреса в список **Blocked_addresses**. В появившемся поле **Параметры** указать **{SOURCE_IP}** в качестве значения переменной **SRC_IP**, использующейся в команде. Полный список переменных, относящихся к срабатываниям, смотрите в разделе [Переменные для уведомлений и команд](#).

8. Настроить правило аналитики.

Перейти во вкладку **Аналитика** веб-интерфейса SIEM. В разделе **Правила аналитики** нажать **Добавить** и указать следующие параметры:

- Во вкладке **Общие**:
 - Поставить флажок **Включено**;
 - **Название** правила аналитики;
 - **Уровень угрозы**, который будет отображаться при срабатывании правила;
 - **Приоритет**, установленный для срабатывания правила аналитики;
 - **Категория срабатывания**, к которой относится срабатывание.

- Во вкладке **Условия**:
 - **Название** условия правила аналитики;
 - **Запрос фильтра**: указать **rule = "DoS_rule_1" and action = deny** (где **DoS_rule_1** — название правила защиты DoS, созданного в п.3);
 - **Группировать по** отображает список параметров, по которым могут быть сгруппированы **правила** и **события** в результате срабатывания; указать **IP источника** (указание параметра группировки обязательно);
 - **Повторений шаблона**: количество выполнений условия, необходимое для срабатывания правила. Данный параметр может быть использован совместно с параметром **Ограничить время выполнения условия** или без него.

- Во вкладке **Действия реагирования** выбрать созданное в п.7 действие реагирования.

За более детальной информацией по настройкам раздела [Аналитика](#) можно обратиться в руководство администратора SIEM.

Product: UserGate NGFW, UserGate MC, UserGate LogAn
Version: 6.x, 7.x

Задача

Разрешить сервис XML-RPC только с определенных IP-адресов, выполняющих запросы по API.

Решение

Доступ к API разрешается в профиле администратора и может быть ограничен по адресу источника. Для обеспечения доступа с определенных IP-адресов в свойствах сетевой зоны необходимо настроить сервис XML-RPC.

Примечание На MC и LogAn сервис XML-RPC по умолчанию отображается в свойствах сетевой зоны.

Для того, чтобы отображался сервис на зоне NGFW, необходимо:

- 1. Открыть NGFW веб-консоль администратора таким образом: https://<usergate_ip>:8001/?features=zone-xml-rpc .
- 2. В настройках нужной зоны активировать сервис **"XML-RPC для управления"**.

Свойства сетевой зоны

Общие

Контроль доступа

Защита от IP-спуфинга

Ограничение сессий

Разрешённые сервисы	Разрешённые адреса
☒ Ping	Любой
☐ SNMP	Любой
☒ Captive-портал и страница блокировки	Любой
☒ XML-RPC для управления	Любой
☐ Кластер	Любой
☐ VRRP	Любой
☒ Консоль администрирования	Любой
☒ DNS	Любой
☒ HTTP(S)-прокси	Любой
☒ Агент аутентификации	Любой
☒ SMTP(S)-прокси	Любой
☒ POP3(S)-прокси	Любой
☐ CLI по SSH	Любой
☒ VPN	Любой
☒ SCADA	Любой
☐ Reverse-прокси	Любой
☒ Веб-портал	Любой

Сохранить

Отмена

- 3. В параметре **Разрешенные адреса** нажать **Любой** и добавить требуемый **IP-адрес** .

Выберите IP-адрес/подсеть

Добавить

Редактировать

Удалить

Название списка ↑	Владелец
-------------------	----------

Создать и добавить новый объект

Сохранить

Отмена

Product: UserGate NGFW
Version: 6.1.8, 6.1.9, 7.0.1

Задача

Необходимо настроить защиту от DoS-атак для веб-сервера, опубликованного через reverse-прокси.

Решение

ПримечаниеВ версиях 6.1.8, 6.1.9, 7.0.1 присутствуют проблемы в работе правил защиты DoS для трафика reverse-прокси.

ПримечаниеПравилами межсетевого экрана нельзя ограничить доступ к ресурсам, опубликованным через reverse-прокси.

Для версий NGFW, в которых есть проблемы с работой правил защиты от DoS, для защиты ресурсов, опубликованных через reverse-прокси, можно использовать следующий вариант: перенаправить нежелательный трафик на несуществующий адрес. Для этого необходимо произвести следующие настройки:

1. Создать два правила DNAT для нежелательного трафика (трафик от бот-сетей и адресов, не принадлежащих российскому пространству):

- в первом правиле в качестве адреса источника выбрать GeoIP Russian Federation и отметить чекбокс Инвертировать, в условии Адрес назначения DNAT (вкладка DNAT) указать любой адрес, который у вас не используется, например, 1.2.3.4;
- во втором правиле в качестве адреса источника выбрать список IP-адресов Список бот-сетей, в условии Адрес назначения DNAT (вкладка DNAT) указать любой адрес, который у вас не используется, например, 1.2.3.4.

ПримечаниеВажно создавать 2 правила, т.к. при указании в одном условии списков IP-адресов и GeoIP применяется логика "И" - для срабатывания правила адрес источника должен находится в обоих списках.

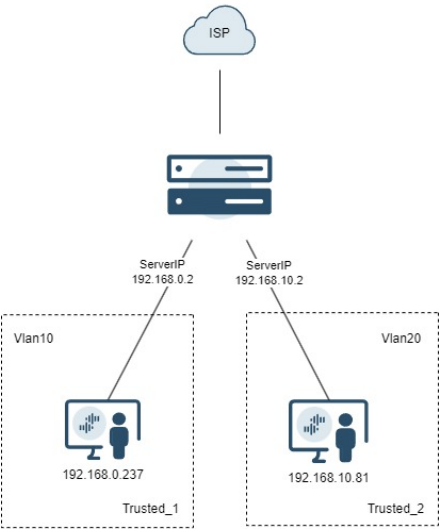
2. Создать статический маршрут типа blackhole, в качестве адреса назначения указать 1.2.3.4/32.

В соответствии с Packet Flow (подробнее читайте в [UserGate NGFW 6 Packet Flow](#)) правила DNAT сработают раньше правил reverse-прокси и перенаправят нежелательный трафик blackhole.

Product: NGFW
Version: 6.1.9

Задача

Организовать соединение между агентами аутентификации, установленными в разных сегментах сети, и сервером UserGate в кластере отказоустойчивости **Актив-Пассив**, используя один адрес назначения.



Решение

Для указания адреса интерфейса UserGate, на который приходят запросы агента аутентификации для Windows, используется параметр "ServerIP". NGFW принимает пакет только в том случае, если указанный в настройках агента адрес назначения ("ServerIP") совпадает с адресом интерфейса, куда пакет пришел; если IP-адрес принадлежит другому интерфейсу NGFW, то пакет будет отброшен.

Для отправки пакетов со всех интерфейсов в один адрес назначения, принадлежащий одному интерфейсу NGFW, необходимо настроить правила DNAT.

Адрес назначения меняется правилом DNAT по адресу источника (для каждой локальной подсети в адрес своего интерфейса). "ServerIP" должен быть виртуальным, поэтому интерфейсы узлов должны быть в разных зонах (узлы разные, на одном сегменте сети одна зона). Необходимо настроить по 2 правила DNAT для каждой сети, соответственно во всех других правилах нужно будет указать по две зоны.

Для того чтобы использовать один адрес назначения для разных подсетей, необходимо произвести следующие настройки:

- 1. Перейдите в раздел **Сеть** → **Зоны** и создайте разные зоны для подсетей с пользователями.

UserGate

Настройки

Управление устройством

Администраторы

Сертификаты

Сеть

Зоны

Интерфейсы

Шлюзы

DHCP

DNS

Виртуальные маршрутизаторы

WCCP

Пользователи и устройства

Группы

Пользователи

Серверы аутентификации

Профили аутентификации

Сaptive-портал

Зоны

Добавить

Редактировать

Удалить

Копировать

Зона	Защита от DoS включена для	Защита от спуфинга	Контроль доступа
Cluster	Нинеро	Отключено	Ping, Кластер, VRRP, Консоль администрирования, DNS
DMZ	SYN, UDP, ICMP	Отключено	Ping, DNS, SMTP(S)-прокси, POP3(S)-прокси
Management	SYN, UDP, ICMP	Отключено	Ping, SNMP, Captive-портал и страница блокировки, Консоль администрирования, CLI по SSH
TEST_Manag...	SYN, UDP, ICMP	Отключено	Консоль администрирования, CLI по SSH
Trusted_1	SYN, UDP, ICMP	Отключено	Ping, Captive-портал и страница блокировки, VRRP, DNS, HTTP(S)-прокси, Агент аутентификации, SMTP(S)-прокси, POP3(S)-прокси, SCADA
Trusted_2	SYN, UDP, ICMP	Отключено	Ping, Captive-портал и страница блокировки, VRRP, DNS, HTTP(S)-прокси, Агент аутентификации, SMTP(S)-прокси, POP3(S)-прокси, SCADA
Untrusted	SYN, UDP, ICMP	Отключено	Ping, SMTP(S)-прокси, POP3(S)-прокси
VPN for rem...	SYN, UDP, ICMP	Отключено	Ping, Captive-портал и страница блокировки, DNS, HTTP(S)-прокси
VPN for Site...	SYN, UDP, ICMP	Отключено	Ping, Captive-портал и страница блокировки, DNS, HTTP(S)-прокси

- 2. Перейдите в раздел **Сеть** → **Интерфейсы**, установите корректные IP-адреса, соответствующие вашим сетям, и назначьте зоны интерфейсам.

UserGate

Настройки

Управление устройством

Администраторы

Сертификаты

Сеть

Зоны

Интерфейсы

Шлюзы

DHCP

DNS

Виртуальные маршрутизаторы

WCCP

Пользователи и устройства

Группы

Пользователи

Серверы аутентификации

Профили аутентификации

Сaptive-портал

Терминальные серверы

Профили MFA

Политики BYOD

Устройства BYOD

Политики сети

Межсетевой экран

NAT и маршрутизация

Балансировка нагрузки

Пропускная способность

Политики безопасности

Фильтрация контента

Веб-безопасность

Инспектирование SSL

Инспектирование SSH

CSOV

Правила АСУ ТП

Сценарии

Защита почтового трафика

ICAP-правила

ICAP-серверы

Правила защиты DoS

Профили DoS

Интерфейсы

Добавить

Редактировать

Удалить

Включить

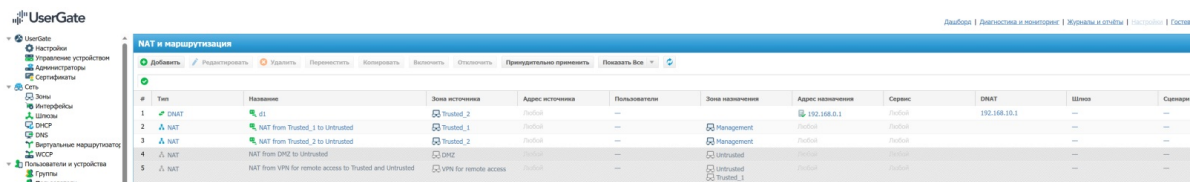
Отключить

Показать Все

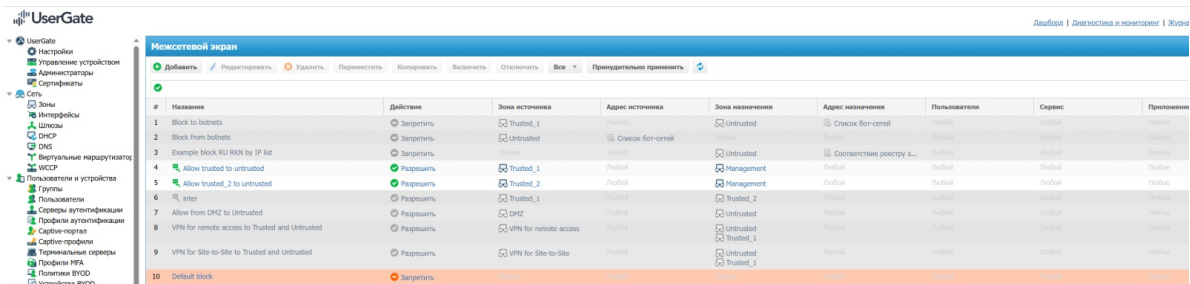
Тип	Название	Режим	IP интерфейс	MAC-адрес	Зона	MTU	DHCP-релей	Интерфейсы	Скорость	Тип интерфейса
Узел кластера: cluster										
VPN	tunnel1	Статичес...	172.30.250.1/255.255.255.0		VPN for r...	1420			0 Mb/s	Layer 3
VPN	tunnel2	Статичес...	172.30.255.1/255.255.255.0		VPN for S...	1420			0 Mb/s	Layer 3
VPN	tunnel3	Динамич...	Нет		VPN for S...	1420			0 Mb/s	Layer 3
Узел кластера: utmcore@1 (текущий узел)										
Cetevo...	port0	Статичес...	10.10.10.170/255.255.255.0	50:00:00:14:00:00	Manage...	1500			0 Mb/s	Layer 3
Cetevo...	port1	Без адре...	Нет	50:00:00:14:00:01	Зона не уста...	1500			0 Mb/s	Layer 3
Cetevo...	port2	Статичес...	10.1.1.1/255.255.255.0	50:00:00:14:00:02	Cluster	1500			0 Mb/s	Layer 3
Cetevo...	port3	Без адре...	Нет	50:00:00:14:00:03	Зона не уста...	1500			0 Mb/s	Layer 3
VLAN	port1.10(por...	Статичес...	192.168.0.2/255.255.255.0	50:00:00:14:00:01	Trusted_1	1500			0 Mb/s	Layer 3
VLAN	port1.20(por...	Статичес...	192.168.10.2/255.255.255.0	50:00:00:14:00:01	Trusted_2	1500			0 Mb/s	Layer 3
VPN	tunnel1	Статичес...	172.30.250.1/255.255.255.0		VPN for r...	1420			0 Mb/s	Layer 3
VPN	tunnel2	Статичес...	172.30.255.1/255.255.255.0		VPN for S...	1420			0 Mb/s	Layer 3
VPN	tunnel3	Динамич...	Нет		VPN for S...	1420			0 Mb/s	Layer 3
Узел кластера: utmcore@2										
Cetevo...	port0	DHCP	10.10.10.179/255.255.255.0	50:00:00:02:00:00	Manage...	1500			0 Mb/s	Layer 3
Cetevo...	port1	Без адре...	Нет	50:00:00:02:00:01	Зона не уста...	1500			0 Mb/s	Layer 3
Cetevo...	port2	Статичес...	10.1.1.2/255.255.255.0	50:00:00:02:00:02	Cluster	1500			0 Mb/s	Layer 3
Cetevo...	port3	Без адре...	Нет	50:00:00:02:00:03	Зона не уста...	1500			0 Mb/s	Layer 3
VLAN	port1.10(por...	Статичес...	192.168.0.3/255.255.255.0	50:00:00:02:00:01	Trusted_1	1500			0 Mb/s	Layer 3
VLAN	port1.20(por...	Статичес...	192.168.10.3/255.255.255.0	50:00:00:02:00:01	Trusted_2	1500			0 Mb/s	Layer 3
VPN	tunnel1	Статичес...	172.30.250.1/255.255.255.0		VPN for r...	1420			0 Mb/s	Layer 3
VPN	tunnel2	Статичес...	172.30.255.1/255.255.255.0		VPN for S...	1420			0 Mb/s	Layer 3
VPN	tunnel3	Динамич...	Нет		VPN for S...	1420			0 Mb/s	Layer 3

- 3. Перейдите в раздел **Политики сети** → **NAT и маршрутизация**. Поменяйте адрес назначения правилом DNAT по адресу источника (для каждой локальной подсети в адрес своего интерфейса). Адрес должен быть не виртуальным, поэтому интерфейсы узлов должны быть в разных зонах.

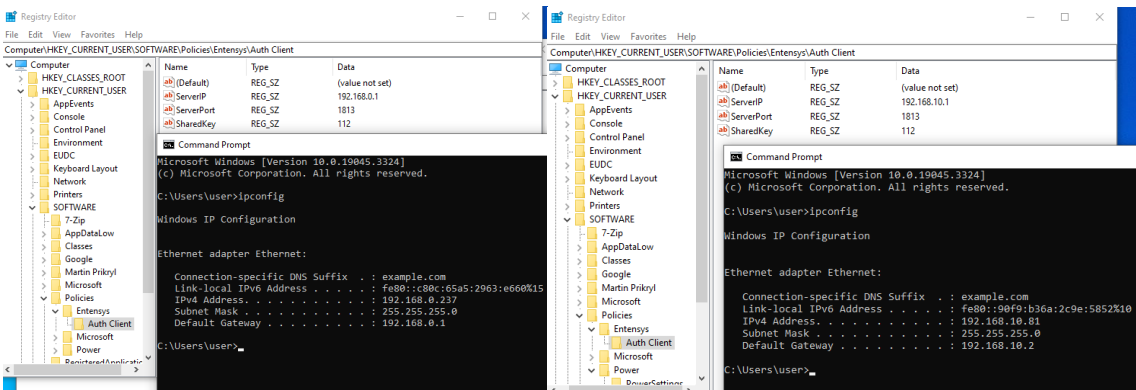
Создайте **правило DNAT** согласно инструкции, подробнее в разделе [Политики сети](#).



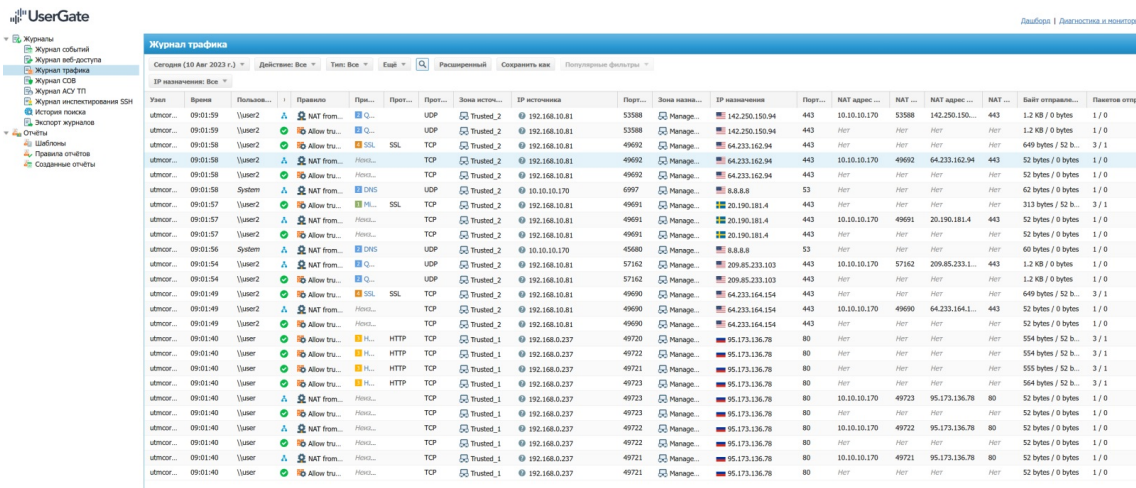
- Перейдите в раздел **Политики сети** → **Межсетевой экран**, в случае если пользователям локальных подсетей требуется в выход в интернет, создайте правило межсетевого экрана указав зоны, присвоенные подсетям.



- Установите агент аутентификации согласно инструкции [Агент аутентификации для Windows](#).



- Перейдите в раздел **Журналы и отчеты** → **Журнал трафика**. В окне журнала будут отражены активные соединения между ПК и NGFW и записи об аутентификации пользователей.



В случае использования кластера отказоустойчивости **Актив-Актив**: адрес назначения меняется правилом DNAT по адресу источника (для каждой локальной подсети в адрес своего интерфейса), но адрес должен быть **не виртуальный**, а физический, поэтому интерфейсы узлов должны быть в разных зонах (у каждого интерфейса своя зона). Должно быть создано по два правила DNAT для каждой сети, соответственно во всех других правилах нужно будет указать по две зоны.

Периодические разрывы VPN соединений.

Version: 6.1.8, 6.1.9, 7.0.1, 6.x, 7.x
Technology: VPN

Задача

Периодические разрывы VPN соединений.

Решение

Начиная с версии 6.1.9.12030R для устранения возможных разрывов подключения VPN клиента Windows к UserGate, необходимо в настройках профиля безопасности VPN на устройстве UserGate для первой фазы установить значение "Интервала проверки dead peer detection"(DPD) равным 0.
Если подключение успешно проходит, но в последствии соединение все равно разрывается, необходимо обратиться в отдел технической поддержки и подготовить записанный трафик с начала сессии и лог для анализа.

Долгая загрузка устройства

Product: UserGate NGFW, UserGate MC, UserGate LogAn, UserGate C100, UserGate D200/D500, UserGate E1000/E3000, UserGate F8000, UserGate X1, UserGate Log Analyzer E6/E14, UserGate Log Analyzer F25, UserGate Management Center C, UserGate Management Center E, KinderGate Родительский контроль, UserGate C150
Version: 5.x, 6.x, 7.x

Симптомы

Очень долго загружается устройство UserGate.

Решение

Долгая загрузка устройства может быть связана с тем что в настройках сервера авторизации (и не только) адрес сервера указан как FQDN. Если при этом присутствуют проблемы с доступом к DNS серверу, UserGate будет пытаться разрешить FQDN имя и ожидать пока закончится timeout обращения к DNS серверу. Следует проверить доступность сервера DNS и возможность разрешения FQDN имени(и его корректность), также сам сервер авторизации, на который ссылается FQDN имя должен быть доступен.

Product: UserGate NGFW

Version: 5.x, 6.1.8, 6.1.9, 7.0.0, 7.0.1, 7.0.2, 7.1.0, 7.2.0, 6.x, 7.x

Technology: Networking

Вопрос

Почему UserGate посылает DNS-запросы для разрешения URL-адреса из списка угроз?

Ответ

UserGate для обеспечения безопасности недостаточно знать URL-адреса потенциально опасных ресурсов, необходимо также знать актуальные IP-адреса этих ресурсов. Данные об актуальных адресах хранятся в DNS-кэше, и, когда истекает время жизни DNS-записи, UserGate делает запрос к системным DNS-серверам для обновления записи.

ПримечаниеВ кластере отказоустойчивости сервисы DNS автономны, т. е. работают независимо на каждом узле кластера, поэтому DNS-кэш они обновляют независимо. Но при добавлении нового адреса в список URL DNS-запись будет добавлена в кэш на каждом узле кластера.

Product: UserGate NGFW

Version: 5.x, 6.1.8, 6.1.9, 7.0.0, 7.0.1, 7.0.2, 7.1.0, 7.2.0, 6.x, 7.x

Technology: Networking

Проблема

В случае использования динамической выдачи MAC-адресов сетевым интерфейсам UserGate в системах виртуализации, при выдаче системой новых MAC-адресов нарушается сетевое взаимодействие с UserGate, т. к. адреса на устройстве не обновляются. При этом на UserGate сбрасываются сетевые адреса и маршрут по умолчанию.

Решение

В UserGate не реализован механизм автоматического получения динамических MAC-адресов. Во избежание подобных проблем рекомендуется закрепить за сетевыми адаптерами виртуальной машины UserGate статические MAC-адреса.

Какие версии UserGate сертифицированы ФСТЭК?

Product: UserGate NGFW, UserGate MC, UserGate LogAn, UserGate SIEM
Version: 7.0.1, 7.1.0

Вопрос

Какие версии UserGate сертифицированы ФСТЭК?

Ответ

Сертификат ФСТЭК относится к решению в целом, а не к его конкретной версии. UserGate в должном порядке вносит изменения в свое сертифицированное средство защиты информации, как это предусмотрено Приказом ФСТЭК №55 от 03 апреля 2018 года (см. п.п. 71, 73, 74 - <https://minjust.consultant.ru/files/39437>). Исходя из этого в любой период времени правильным является применение последней версии UserGate со всеми новейшими обновлениями. О выходе версии сообщено во ФСТЭК, и она передана в испытательную лабораторию для проведения испытаний. Обновления сертификатов, технических условий и формуляра происходит в установленном ФСТЭК порядке после окончания испытаний, информация об этом доводится до пользователей сертифицированного решения.

Как ограничить полосу пропускания группе пользователей для доступа к видео из сети Интернет

KnowledgeBase: 
Product: UserGate NGFW

Задача

Необходимо ограничить группе пользователей локальной сети полосу пропускания для доступа к видеоконтенту из сети Интернет и не ограничивать полосу пропускания для доступа к серверам компании, расположенным в зоне DMZ.

Решение

Правила пропускной способности работают только с исходящим от UserGate трафиком, на входящий трафик UserGate влиять не может, поэтому принимает весь трафик.

Особенность настройки заключается в том, что правило пропускной способности будет работать только для зоны назначения и будет не работать для зоны источника, поэтому в правилах указываются **Адрес источника** и **Зона назначения**.

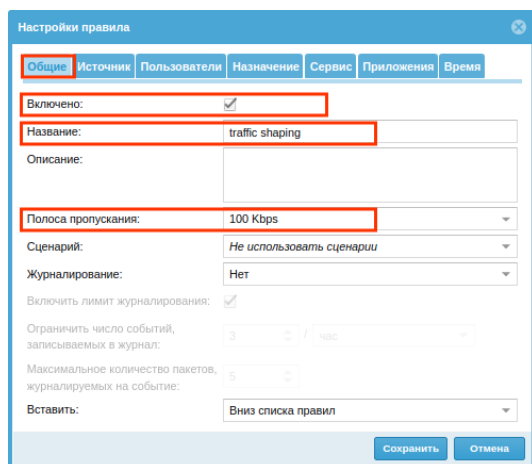
На UserGate настроена зона **Trusted**, назначенная для интерфейса, через который пользователи локальной сети получают доступ в Интернет. Также произведена настройка зоны **DMZ**, в которой расположены различные сервера компании, используемые для предоставления ресурсов пользователям локальной сети.

1. Создать правило для ограничения полосы пропускания.

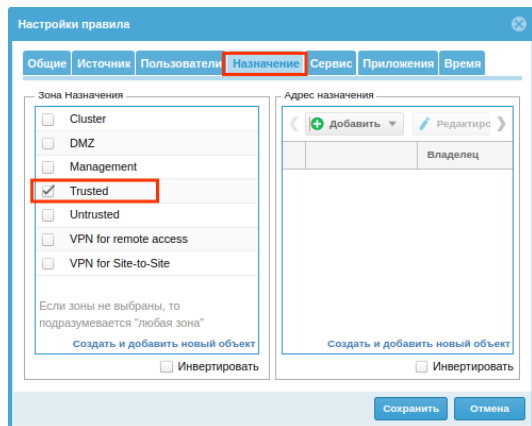
В разделе **Политики сети** → **Пропускная способность** нажмите кнопку **Добавить** и создайте правило. В свойствах укажите необходимые данные.

Во вкладке **Общие**:

- **Название правила.**
- **Полоса пропускания:** 100 Kbps.



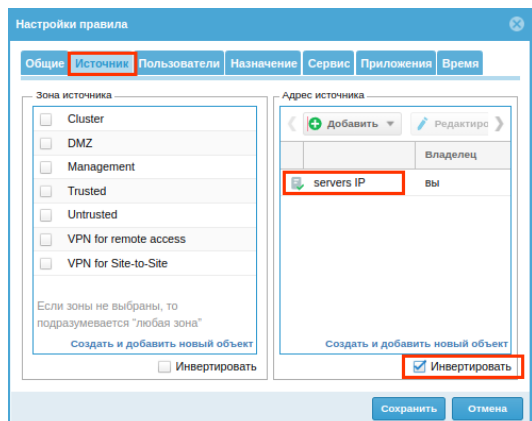
Во вкладке **Назначение** в разделе **Зона назначения** укажите **Trusted**.



Данное правило будет ограничивать весь трафик, как из зоны **Untrusted**, так и из зоны **DMZ** в зону **Trusted**.

2. Настроить правило так, чтобы не происходило ограничение полосы пропускания для доступа к серверам компании, расположенным в зоне DMZ.

Для того, чтобы трафик от серверов компании в зоне DMZ к данной группе пользователей не ограничивался, необходимо во вкладке **Источник** в разделе **Адрес источника** указать список IP-адресов серверов (**Добавить список IP-адресов**) и отметить чекбокс **Инвертировать**. Список IP-адресов может быть создан в разделе **Библиотеки** → **IP-адреса** или в настройках правила нажатием на **Создать и добавить новый объект**.



Как запретить трафик для определенных приложений

Product: UserGate NGFW

Задача

Необходимо запретить или разрешить трафик для определенных приложений

Решение

Перейдите в раздел **Политики сети → Межсетевой экран**. Создайте правило и укажите приложения, к которым оно должно применяться (в свойствах правила перейдите во вкладку **Приложения** и нажмите **Добавить → Добавить приложения**).

Помимо отдельных приложений можно указать:

- **Все группы приложений**.
- **Группы приложений**: выберите группы приложений, к которым необходимо применить правило межсетевого экрана (добавление групп описано далее).
- **Категории приложений**: выберите категории приложений, к которым необходимо применить правило межсетевого экрана (например, Games, Web browsing и т.п.).

Чтобы создать группы приложений для более удобного использования в правилах фильтрации сетевого трафика:

1. Перейдите в раздел **Библиотеки → Приложения**, на панели **Группы приложений** нажмите кнопку **Добавить**. Далее укажите название и описание группы приложений.
2. Добавьте приложения в созданную ранее группу, нажав на панели **Приложения** кнопку **Добавить** и выбрав нужные приложения.

Примечание Для идентификации приложения необходимо, чтобы соединение между клиентом и сервером было установлено и прошла какая-то часть трафика в обоих направлениях.

Объем такого трафика ограничен 1кб

Поэтому под правило, разрешающее приложение, может попасть любой трафик, удовлетворяющий остальным критериям в правиле, до того момента, когда приложение будет идентифицировано.

Аналогично, запрещающее правило по приложению сработает (разорвет сессию) только после завершения идентификации приложения.

Как разрешить работу клиента Dropbox

Product: UserGate NGFW

KnowledgeBase: 

Задача

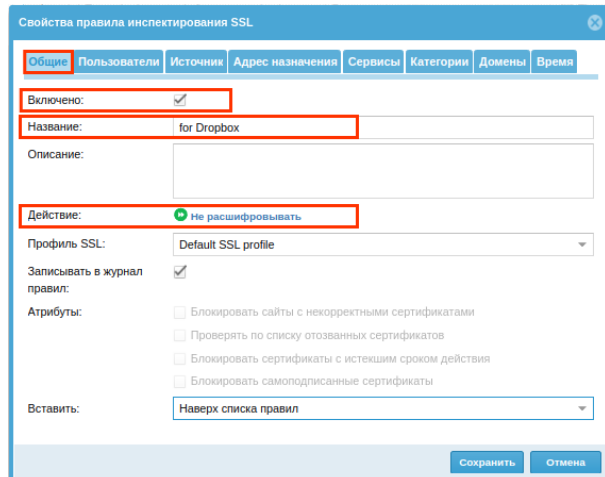
Необходимо разрешить работу клиента Dropbox

Решение

Для организации работы клиента Dropbox необходимо создать новое правило дешифрования в разделе **Политики безопасности → Инспектирование SSL**. Укажите необходимые данные.

Во вкладке **Общие** укажите:

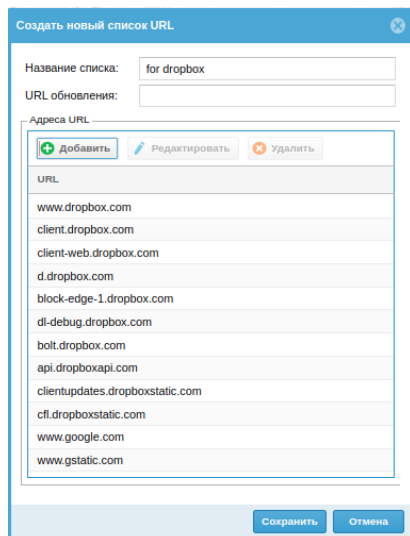
- **Название** правила инспектирования.
- **Действие** - **Не расшифровывать**.



В разделе **Библиотеки → Списки URL** создайте новый список и добавьте следующие сайты:

- www.dropbox.com
- client.dropbox.com
- client-web.dropbox.com
- d.dropbox.com
- block-edge-1.dropbox.com
- dl-debug.dropbox.com
- bolt.dropbox.com
- api.dropboxapi.com
- clientupdates.dropboxstatic.com
- cfl.dropboxstatic.com
- www.google.com
- www.gstatic.com

Список URL также можно создать при настройке правила во вкладке **Домены** (кнопка **Создать и добавить новый объект**).



Последние два URL требуются только для возможности первоначально авторизоваться в клиенте Dropbox с реквизитами учётной записи из Google. Если их не указывать, то первичная авторизация, независимо от типа учётной записи, будет произведена не в клиенте Dropbox, а в браузере по умолчанию. Для последующей работы клиента Dropbox эти URL не требуются.

Далее во вкладке **Домены** свойств правила инспектирования укажите созданный ранее список URL.

Свойства правила инспектирования SSL

ОбщиеПользователиИсточникиАдрес назначенияСервисыКатегорииДоменыВремя

ДобавитьРедактироватьУдалить

URL	Владелец
for dropbox	Вы

Создать и добавить новый объект

☐ Инvertировать

СохранитьОтмена

Примечание Данное правило необходимо расположить в начале списка правил инспектирования SSL.

Не удается настроить исключение блокировки рекламы

Technology: SSL Inspection

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW

Задача

При попытке зайти на необходимый сайт выдается страница блокировки. Попытка создать исключение для правил блокировки рекламы ни к чему не приводит, сайт по-прежнему блокируется.

Решение

Одной из возможных причин такого поведения является несоответствие алгоритмов шифрования, которые выбирает сервер алгоритмам, поддерживаемым браузером. Иными словами сервер может выбрать алгоритм шифрования, который не поддерживается браузером, но присутствует в профиле инспектирования SSL. Большинство сайтов прекрасно работают при использовании **SSL-профиля по умолчанию**, тем не менее, чтобы исключить конфликт, можно посмотреть какие алгоритмы шифрования выбирает сервер и поддерживает браузер. Для этого нужно записать трафик между браузером и сервером и внести в настройки профиля инспектирования SSL только те алгоритмы, которые поддерживает браузер на вкладке: **Свойства SSL-профиля → Общие**

Не работают правила, содержащие ограничения по внешним пользователям

Product: UserGate NGFW

Задача

Не работают правила, содержащие ограничения по пользователям, полученным с внешних серверов (например, LDAP-коннектора).

Решение

Возможны несколько причин возникновения данной проблемы.

Возможная причина №1

Для того чтобы пользователей можно было использовать в правилах любого модуля, пользователи должны пройти аутентификацию одним из поддерживаемых методов (подробнее читайте в соответствующем [разделе](#) руководства администратора).

Примечание Для использования пользователей в правилах межсетевого экрана в соответствующем captive-профиле, если используется не агент аутентификации, в качестве метода идентификации необходимо указать [Запоминать IP-адрес](#).

Возможная причина №2

Случай асимметричного трафика: пакет от клиента к серверу передаётся через UserGate, а обратный - напрямую к клиенту (без обработки на UserGate). В этом случае межсетевой экран с контролем состояния обратный пакет не привязывает к пользователю. В такой ситуации необходимо правильно настроить маршрутизацию трафика, чтобы все пакеты шли через UserGate либо настроить правило SNAT для отправки такого трафика от имени UserGate.

Version: 5.x, 6.x, 7.x
Product: UserGate NGFW

Задача

Необходимо разделить трафик пользователей: для одних пользователей UserGate должен работать в режиме явного прокси (Explicit Proxy Mode), для других - в режиме прозрачного прокси (Transparent Proxy Mode). Трафик от всех пользователей поступает на один интерфейс.

Решение

Поскольку весь трафик пользователей поступает на один интерфейс, UserGate автоматически применяет политики безопасности ко всему трафику с портами назначения 80 и 443.

Для разделения трафика выполните следующие действия:

1. Направьте трафик на разные интерфейсы (т.е. трафик, к которому должны быть применены политики UserGate направьте на один интерфейс, трафик, который должен пройти через UserGate без анализа - на другой); назначьте им разные зоны. Это позволит разделять трафик по признаку зоны источника.

Чтобы назначить двум интерфейсам адреса из одной сети (если нет другого маршрутизатора, на котором можно было бы выделить отдельную сеть), создайте для интерфейса, который будет указан как явный прокси, отдельный виртуальный маршрутизатор. В нём необходимо указать маршруты и шлюзы, аналогичные маршрутам и шлюзам маршрутизатора по умолчанию.

2. Для зоны источника интерфейса, указанного как шлюз по умолчанию, настройте разрешающие правила инспектирования SSL и фильтрации контента; расположите эти правила в начале списка.

Подробнее об алгоритме обработки трафика в UserGate версии 6.x.x читайте в статье [UserGate NGFW 6 Packet Flow](#).

При включении DNS-фильтрации начинают блокироваться разрешенные ресурсы

Product: UserGate NGFW
Technology: Content Filtering
Version: 5.x, 6.x, 7.x

Задача

При включении DNS-фильтрации начинают блокироваться разрешенные ресурсы.

Решение

Возможно в вашей сети используются интерфейсы типа L2 мост. К сожалению, в текущей версии UserGate NGFW функционалы DNS фильтрации и моста L2 несовместимы, в результате при включении DNS фильтрации, DNS запросы через L2 мост работать не могут.

Исключение трафика конкретных приложений из проксирования и инспектирования

Задача

Некоторые приложения некорректно работают при использовании устройств MITM. Требуется исключить их из проксирования и инспектирования.

Решение

Данная проблема решается путем исключения трафика проблемных приложений из проксирования и SSL инспектирования, для этого необходимо:

1. Создать список URL, содержащий доменные адреса, к которым подключаются проблемные сервисы.
2. Настроить правило captive-портала с действием "Не использовать аутентификацию" и указать созданный список URL. Правило необходимо поместить выше правила captive-портала, предназначенного для авторизации.
3. Настроить SSL-инспектирование с действием "Не расшифровывать" для созданного списка URL. Правило следует поместить выше правила расшифровки.
4. Настроить разрешающее правило контентной фильтрации для созданного списка URL и поместить его выше остальных правил.

Журналирование для всех перечисленных правил нужно выключить.

Technology: Content Filtering

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW

Вопрос

Интересует вопрос: как и на сколько корректно будут работать правила reverse-прокси, DNAT и Межсетевого Экрана, если везде в них будет фигурировать один и тот же IP адрес.

Ответ

Использование одного адреса для публикации разных сервисов - это общепринятая практика. Каждое правило публикации перенаправляет соединения в соответствии с указанными в его настройках протоколами и портами.

ПО UserGate позволяет использование правил reverse-проху для публикации одних портов и правил DNAT для других на одном общем адресе. В правилах reverse-прокси TCP-порт (или список портов) указывается в соответствующем поле на вкладке Общие, а в правиле DNAT протоколы и порты определяются сервисами выбранными на соответствующей вкладке. Если будет указан один и тот же порт для правил DNAT и reverse-прокси, то правила DNAT сработает первым и правило reverse-прокси не сработает.

Правила межсетевого экрана в данном случае могут выполнять роль дополнительного фильтра, т.е. запрещать часть соединений автоматически разрешаемых правилами reverse-прокси и DNAT.

Более подробно о правилах прохождения пакетов через ПО UserGate можно посмотреть [здесь](#).

Запретить NAT "серых" IP адресов

Technology: Firewall
Version: 7.0.0, 7.0.1, 7.0.2, 7.1.0, 6.x
Product: UserGate NGFW

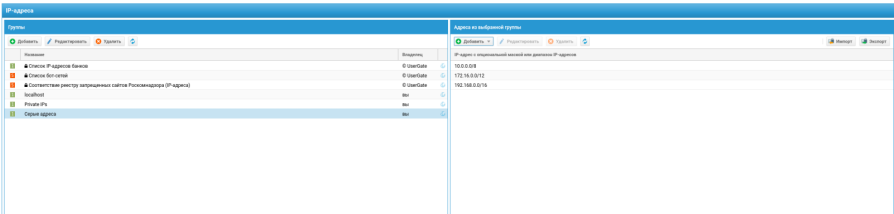
Задача

Необходимо запретить NAT трансляцию серых адресов.

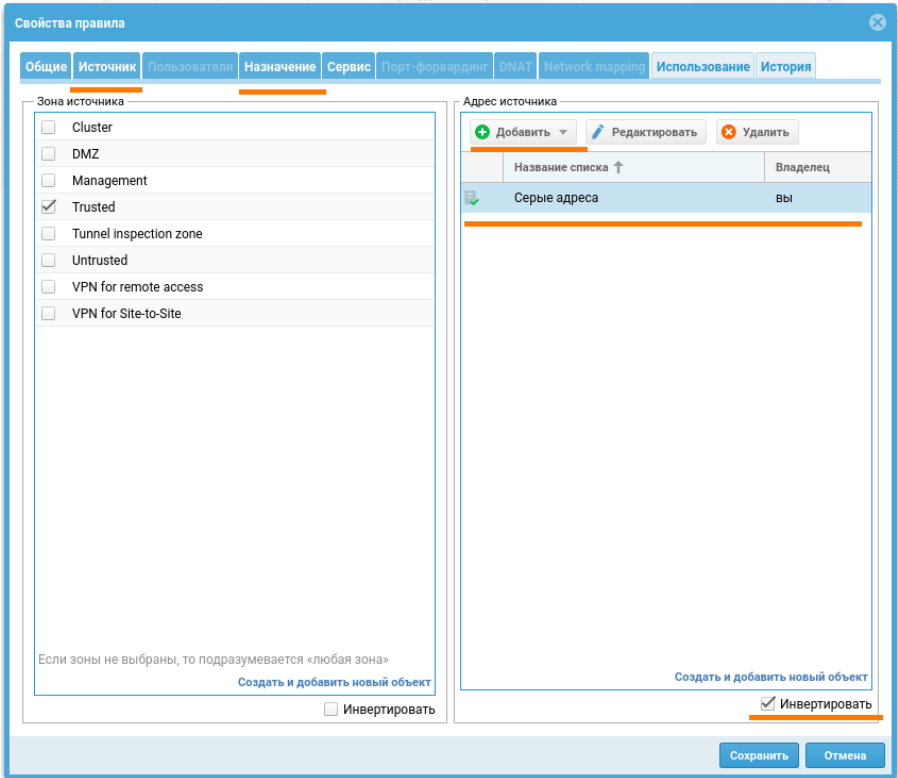
Решение

Для решения задачи необходимо выполнить следующие шаги:

1. Добавить список запрещенных для NAT IP-адресов. Для этого по пути: **Библиотеки → IP-адреса**, нужно добавить список запрещенных для NAT адресов.



2. В правилах NAT добавить данный список в качестве **Источника** или **Назначения** с установкой флага **Инвертировать**. Для этого: по пути: **Политики сети → NAT** и маршрутизация, добавить правило NAT или отредактировать существующее. Открыть настройки **Источника** и/или **Назначения**, и добавить запрещенные адреса с флагом **Инвертировать**.



Некорректная работа Яндекс Браузера с сервисами Google

Technology: Content Filtering

Version: 6.x, 7.x

Product: UserGate NGFW

Задача

Некорректная работа через Яндекс Браузер с сервисами Google, при этом на устройстве UserGate есть разрешающее правило для работы Яндекс Браузера.

Решение

Проблема скорее всего связана с этим:

«Разработчики Яндекса случайно обнаружили, что в драйверах AMD есть оптимизация под Chrome, но нет исправлений для других браузеров, основанных на Chromium. Компания уже направила запрос в AMD, но пока, чтобы не ждать, программисты просто встроили в Яндекс Браузер функцию мимикрии под Chrome — количество падений GPU-процесса снизилось в 5,5 раз, расход памяти уменьшился на 8%.»

Яндекс Браузер при работе с сервисами Google меняет свой User-Agent на Chrome, из-за чего могут происходить ложные срабатывания правил и другие артефакты обработки трафика. Это можно нивелировать с помощью средств разработчика, путем установки в браузере кастомизированного User-Agent на любую (даже не существующую) версию Яндекс Браузера. При этом отключается механизм подмены своего User-Agent в Яндекс Браузере.

Отсутствует лицензия на одном из узлов кластера

Technology: Clustering and HA
Version: 5.x, 6.x, 7.x
Product: UserGate NGFW

Вопрос

Один из узлов кластера в статусе "отсутствует лицензия".

Ответ

Скорее всего вам выдали лицензию без поддержки кластеризации. Как активировать лицензию в кластере смотрите [здесь](#).

Technology: Clustering and HA
Version: 5.x, 6.x, 7.x
Product: UserGate NGFW

Задача

Активировать лицензию в кластере.

Решение

Если на одном из узлов кластера отсутствует лицензия, выполните следующее:

1. Проверьте, что в вашу лицензию включен модуль Cluster, разрешающий работу устройств UserGate в режиме кластера конфигурации.
2. Убедитесь, что лицензия активирована на первом узле кластера (мастер-узле).

ПримечаниеДля всех узлов кластера конфигурации нужна только одна лицензия, которая сначала активируется на мастер-узле кластера в онлайн- или офлайн-режиме. Если на мастер-узле кластера лицензия была активирована онлайн, дополнительному узлу для активации лицензии также потребуется доступ в интернет. При офлайн-активации лицензии на первом узле подключение дополнительного узла к интернету не требуется.

3. Активируйте лицензию на дополнительном узле. Для этого в веб-интерфейсе дополнительного узла кластера конфигурации на странице **Дашборды** в виджете **Лицензия** нажмите **Проверить лицензию**.

Если для подключения к интернету на кластере настроен виртуальный IP-адрес, для активации лицензии выполните следующее:

1. Активируйте лицензию на мастер-узле кластера.
2. Назначьте дополнительный узел мастер-узлом, чтобы виртуальный IP-адрес был присвоен дополнительному узлу.
3. Активируйте лицензию на временном мастер-узле. Для этого в его веб-интерфейсе на странице **Дашборды** в виджете **Лицензия** нажмите **Проверить лицензию**.
4. Верните роль мастер-узла первому узлу.

Если к интернету посредством кабеля подключен только мастер-узел, для активации лицензии выполните следующее:

1. На мастер-узле и дополнительном узле настройте пару интерфейсов и соедините их кабелем.
2. На дополнительном узле укажите первый узел в качестве шлюза по умолчанию.
3. Создайте правила межсетевого экрана и трансляции адресов, разрешающие передачу трафика из интернета.
4. Активируйте лицензию на дополнительном узле. Для этого в веб-интерфейсе дополнительного узла кластера конфигурации на странице **Дашборды** в виджете **Лицензия** нажмите **Проверить лицензию**.

Построение отказоустойчивого решения для кластера с 2 провайдерами и одним внешним IP-адресом на узле

Product: UserGate NGFW
Technology: Clustering and HA
Version: 5.x, 6.x, 7.x

Задача

Настроен кластер отказоустойчивости Актив-Пассив, состоящий из 2-х узлов; используются 2 провайдера, каждый из которых выделил по одному белому адресу. Белые IP-адреса указаны в качестве виртуальных адресов (VIP). Проблема заключается в том, что при включенной проверке сети, если оба оператора ее не прошли, виртуальные IP-адреса пропадают и после восстановления соединения не могут появиться, т.к. проверка сети не может быть выполнена без VIP адресов.

Примечание VIP и адреса, назначенные на интерфейсы, могут быть в разных сетях. Данное решение применимо только для кластера Актив-Пассив.

Решение

Примечание Одним из условий того, чтобы узел стал Мастером и назначил на свои интерфейсы VIP адреса - это наличие в таблице маршрутизации маршрута по умолчанию.

В качестве решения предлагается использовать правила типа **Policy-based routing** со сценарием типа **Проверка состояния** вместо проверки сети.

1. Отключите проверку сети в разделе **Сеть → Шлюзы**.
2. На узлах создайте по одному сценарию типа **Проверка состояния**:

- **Результат:** отрицательный;
- **Применить для:** всех пользователей;
- **Шлюз:** шлюз основного провайдера каждого узла.

3. Создайте правило Policy-based Routing (PBR) для каждого шлюза. В настройках правил для резервного провайдера укажите созданные на шаге 2 сценарии и разместите их выше правил для основного провайдера.

Настройка правил производится в разделе **Политики сети → NAT и маршрутизация**. Правила PBR, предназначенные для основного провайдера, сценариев не используют. Правила, предназначенные для резервного провайдера, используют сценарии, созданные на шаге 2.

Переход на резервный провайдер происходит за счёт срабатывания негативного сценария в правиле Policy-based routing для резервного провайдера. Срабатывание сценария произойдет при отрицательном результате проверки состояния; в результате выполнения сценария, трафик будет перенаправлен через шлюз резервного провайдера.

После восстановления основного провайдера и по прошествии указанного количества времени (указывается в настройках сценария на вкладке **Общие**, параметр **Продолжительность**) сценарий отключается, и трафик маршрутизируется через шлюз основного провайдера.

2 ПАК с разной версией ПО. Как настроить кластер?

Technology: Clustering and HA

Version: 6.x

Product: UserGate C100, UserGate D200/D500, UserGate E1000/E3000, UserGate F8000, UserGate X1, UserGate Management Center C, UserGate Management Center E

Задача

2 программно-аппаратных комплекса с разной версией программного обеспечения: 1-й - с новой версией, 2-й - с прошивкой ранней версии.

Решение

Обновите 2-й ПАК до версии, установленной на 1-м устройстве:

1. Выполните **Factory reset**.
2. Не выполняя инициализации обновите устройство через USB.

Для этого подготовьте USB-носитель, диск должен иметь формат NTFS или FAT32 (рекомендуем FAT32). Из личного кабинета UserGate скачайте необходимый файл обновления и сохраните его в корень съёмного USB-носителя.

ПримечаниеНазвание файла обновления должно быть в следующем формате: update_xxxxx (где xxxxx - номер версии).

Вставьте USB-носитель в устройство и проверьте, что в BIOS в приоритете выставлена загрузка со встроенного в устройство HDD.

ПримечаниеПроверьте, что в BIOS в приоритете выставлена загрузка со встроенного в устройство HDD, а НЕ со съёмного USB-носителя (Boot Option Priorities → Hard Drive BBS Priorities).

3. Запустите устройство. При запуске в **Support Menu** выберите **Update from USB**.

В процессе обновления сервер перезагрузится дважды. В первый раз перезагрузится со старой версией, во второй раз - уже с новой.

Между первой и второй перезагрузкой управление устройством через веб-интерфейс и CLI недоступно.

После обновления произведите добавление узла в кластер. Подробнее читайте в разделе **Кластеризация и отказоустойчивость** руководств по [NGFW](#) и [MC](#).

Рассинхронизация кластера Active - Passive

Technology: Clustering and HA

Version: 6.1.8, 6.1.9, 6.x

Product: UserGate NGFW

Вопрос

Кластер исправен, но трафик идет через активный и пассивный узлы одновременно.

Ответ

Данный эффект может возникать, если на коммутаторах, использующихся сторонним оборудованием для подключения к UserGate, запрещено прохождение пакетов Gratuitous Arp. Таким образом, при смене режима работы узлов кластера (переключении), на ответном оборудовании в ARP-таблицах останется старый MAC-адрес узла кластера, и трафик будет переходить на новый узел по мере обновления ARP-таблиц оборудования. Для решения данной проблемы, следует проинспектировать магистральное оборудование на предмет фильтрации ARP пакетов.

Меняются ли MAC-адреса VIP адреса, в кластере

Technology: Clustering and HA

Version: 6.1.8, 6.1.9, 7.0.0, 7.0.1, 7.0.2, 7.1.0, 7.2.0, 6.x

Product: UserGate NGFW

Вопрос

Меняются ли MAC-адреса, во время смены активного узла кластера для VIP адресов?

Ответ

Да, при переходе виртуального адреса новый мастер отправляет gratuitous arp для изменения MAC-адреса виртуального IP в ARP-таблицах соседних маршрутизаторов.

Разрыв VPN соединения при переключении активного узла кластера

Technology: Clustering and HA

Version: 6.x, 7.x

Product: UserGate NGFW

Задача

Развернут кластер устройств Актив-Пассив. Между офисами настроены 2 VPN-туннеля L2TP IPSec на 2х разных провайдерах. При отключении одного VPN-туннеля трафик переключается на другой туннель. Проблема с переходом туннелей при отказе основного узла кластера, они не переходят на резервный, поэтому теряется VPN-соединение.

Решение

При работе с двумя провайдерами очень важно привязать обратный трафик VPN-соединений к тому провайдеру на адрес которого устанавливается соединение. Для привязки трафика нужно создать правила PBR с пустой зоной источника и адресом источника соответствующим виртуальному адресу на который соединяется клиент из облака и выбрать в нём шлюз соответствующего провайдера. Правил должно быть 4 - по два для каждого из узлов(1 правило на каждый шлюз провайдера, поскольку провайдеров два, правил - 2 на каждый узел).

Как увидеть состояние VRRP

Technology: Clustering and HA

Version: 6.x, 7.x

Product: UserGate NGFW, UserGate MC, UserGate LogAn

Вопрос

Как увидеть состояние VRRP?

Ответ

Состояние VRRP можно увидеть в меню Кластер отказоустойчивости, в случае каких либо проблем, там будет выведена надпись ошибка и значок предупреждения.

Как перезагрузить сервис VRRP?

Version: 6.x, 7.x

Product: UserGate NGFW, UserGate MC, UserGate LogAn

Вопрос

Как перезагрузить сервис VRRP?

Ответ

Перезагрузку VRRP вызовет любое изменение в кластере отказоустойчивости (включение\выключение, добавление удаления адреса или интерфейса в кластер).

Сбой экземпляра отказоустойчивости кластера при добавлении интерфейса

Technology: Clustering and HA

Version: 6.1.8, 6.1.9, 7.0.0, 7.0.1, 7.0.2, 7.1.0, 7.2.0, 6.x, 7.x

Product: UserGate NGFW, UserGate MC, UserGate LogAn

Задача

При добавлении еще одного VIP интерфейса в кластер отказоустойчивости, происходит сбой экземпляра отказоустойчивости кластера

Решение

Нарушение работоспособности кластера может происходить по нескольким причинам:

1. Не разрешен VRRP в настройках зон, участвующих в формировании кластера. В этом случае оба экземпляра кластера будут иметь роль **мастер** и фактически кластер не будет функционировать.
2. Добавляемый интерфейс не имеет IP адреса. Для интерфейсов, участвующих в создании кластера (VIP), необходимо наличие IP адреса, желательно из одного и того же диапазона для всех интерфейсов.

Product: UserGate NGFW

Задача

После авторизации на captive-портале с помощью NTLM для части запросов определяется только тип пользователей **Known/Unknown**.

Решение

При авторизации с использованием NTLM некоторые GET-запросы приходят от системы, а не от пользователя. В этом случае идентификация пользователя невозможна, поэтому такому пользователю присваивается тип **Known**. Для исправления данной ситуации необходимо в списке правил captive-портала включить и поставить первым правило **Skip auth for Microsoft Internet checker**, созданное по умолчанию для исключения подобных запросов из captive-портала.

Captive-портал

Добавить

Редактировать

Удалить

Включить

Отключить

Все

#	Название	Captive-профиль	Зона ...	Зона н...	Адрес ...	А...	Категор...	URL	Время
1	Skip auth for Microsoft Internet checker	Не использовать аутентификацию	Любая	Любая	Любой	Л...	Любая	Microsoft Windows Internet checker	Любое
2	Example Captive portal	Example Captive profile	Tr...	Любая	Любой	...	Любая	Любой	Любое

Примечание В список URL Microsoft Windows Internet checker, возможно, необходимо будет добавить домены ipv6.msftncsi.com и *.microsoft.com.
Важно! В качестве зоны источника следует указать зону, назначенную на интерфейсах, через которые доступны сети с пользовательским трафиком, например, Trusted.
Важно! После добавления правила пользователям необходимо повторно авторизоваться (можно сбросить авторизацию всех пользователей или подождать истечения срока жизни авторизованного пользователя).

Разрешения доступа администраторов

Version: 7.0.0, 6.x

Product: UserGate NGFW

Задача

Администратору даны права доступа **Чтение и запись** на раздел **Политики сети → Межсетевой экран**. При попытке редактирования правил данного раздела отображается ошибка: **У вас нет прав доступа**.

Решение

Необходимы дополнительные разрешения на объекты: сценарии, серверы ICAP, профили защиты DoS и т.п.

Для возможности внесения изменений в политику межсетевого экранирования, помимо прав **Чтение и запись** на раздел **Межсетевой экран**, администратору необходимы разрешения на просмотр раздела **Политики безопасности → Сценарии**.

Данное разрешение необходимо для работы с разделами **Межсетевой экран**, **NAT и маршрутизация**, **Пропускная способность**, **Фильтрация контента**, **Правила защиты DoS** (для раздела **Правила защиты DoS** также необходимы права на раздел **Политики безопасности → Профили DoS**).

Product: UserGate NGFW

Задача

В браузере Chrome (и его вариациях) не отображается портал авторизации. Пользователь видит пустое окно со следующим содержимым:

Заголовок:

HTTP/1.1 407 Authorization Required

Содержимое страницы

```
<html> <!-- please auth via kerberos/NTLM --> </html>
```

Решение

Для подробной информации по работе с политиками в браузере, обратитесь к документации по адресу: <https://www.chromium.org/administrators/linux-quick-start>

1. В соответствии с инструкцией, нужно создать json-файл в директории managed:

```
touch /etc/opt/chrome/policies/managed/test_policy.json
```

Содержимое файла должно быть следующего вида:

```
{
  "AuthServerWhitelist": "/*.usergate.demo",
  "AuthSchemes": "ntlm,negotiate"
}
```

"usergate.demo" необходимо заменить на доменное имя вашего домена.

2. В браузере Chrome открыть страницу политик [about:policy](#).

Вы должны увидеть настройки прописанные в файле на открытой странице:

Chrome Policies

Policy name	Policy value
AuthSchemes	ntlm,negotiate
AuthServerWhitelist	/*.usergate.demo

Если этих строк нет, значит браузеру не удалось загрузить политики из созданного файла. Проверьте права доступа, и другие возможные причины. Обратите внимание, различные браузеры имеют особенности в загрузке политик. Например браузер Chromium на Kali Linux автоматически не загружает описанные политики.

После проведенных манипуляций, браузер не способен произвести прозрачную Kerberos аутентификацию, будет перенаправлять пользователя на портал авторизации.

Некорректная работа правил UserGate NGFW при работе с доменными пользователями

Version: 5.x, 6.x, 7.x

Technology: Identification and Authentication

Product: UserGate NGFW

Задача

При изменении членства пользователя в доменных группах, UserGate NGFW не учитывает эти изменения.

Решение

Для того, чтобы UserGate NGFW обновил информацию о членстве в группах для пользователя, нужно:

1. В CLI выполнить команду: `cache ldap-clear`
2. Произвести переподключение пользователя на клиентской станции (Вход-Выход).
3. Произвести процедуру выхода пользователю на UserGate NGFW.

После этого работа с обновленным пользователем нормализуется.

Technology: Identification and Authentication

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW

Задача

При работе с потоковыми сервисами (например, видеоконференция) периодически происходит обрыв связи.

Решение

Это штатное поведение, описанное в [Руководстве Администратора](#). Параметр *Время жизни авторизованного пользователя* - это таймер, устанавливаемый при аутентификации пользователя. По его истечении сбрасываются все установленные с IP-адреса пользователя соединения.

Вы можете:

1. увеличить этот таймер до нужных значений;
2. создать для пользователя отдельное правило Captive-портала с дополнительным условием, например, IP-адрес источника, с указанием другого профиля авторизации;
3. установить на компьютер пользователя агент авторизации.

Проблемы с авторизацией при использовании нескольких методов аутентификации

Technology: Identification and Authentication

Version: 6.x, 7.x

Product: UserGate NGFW

Задача

Настроены несколько методов аутентификации (Kerberos, NTLM, локальный пользователь); используются несколько правил captive-портала без дополнительных условий (источник, назначение и т.п.), т.е. всегда срабатывает первое правило, для которого совпали все условия.

Решение

Добавьте в используемый профиль аутентификации сразу три метода аутентификации: **Kerberos**, **NTLM** и **локальный пользователь**. В соответствии с данным профилем:

- для доменных пользователей и компьютеров будет работать авторизация с использованием Kerberos;
- для доменных пользователей, но недоменных компьютеров можно будет вводить учетные данные домена;
- локальные пользователи смогут авторизоваться на Captive-портале с логином/паролем.

О применении политик UserGate к пользователям читайте в соответствующей статье: [Применение к пользователям политик UserGate](#).

Technology: Identification and Authentication

Задача

Как автоматизировать загрузку сертификатов на клиентское устройство с ОС Windows 11.

Решение

При тестировании технических решений бывает необходимо автоматизировать процесс загрузки пользовательских сертификатов на клиентское устройство с ОС Windows. Часто для этих целей в скриптах используется системная утилита certutil. Однако в Windows 11 утилита certutil загружает пользовательский сертификат некорректно. В качестве альтернативного метода загрузки сертификата на клиентском устройстве с ОС Windows 11 можно использовать следующую последовательность команд в PowerShell:

```
$pfx = new-object System.Security.Cryptography.X509Certificates.X509Certificate2
$pfx.import("C:\cert.pfx","1234","MachineKeySet, PersistKeySet")
$store = new-object System.Security.Cryptography.X509Certificates.X509Store("My","LocalMachine")
$store.open("MaxAllowed")
$store.add($pfx)
$store.close()
```

Подробнее об использованных атрибутах смотрите в статье: <https://learn.microsoft.com/en-us/dotnet/api/system.security.cryptography.x509certificates.x509keystorageflags?view=net-8.0>

Как настроить прозрачную аутентификацию Kerberos в нескольких доменах?

Technology: Identification and Authentication
Version: 6.x, 7.x
Product: NGFW

Задача

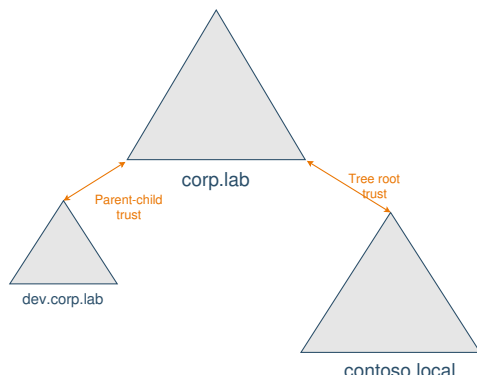
Как настроить прозрачную аутентификацию Kerberos в нескольких доменах?

Решение

На самом прокси-сервере никаких дополнительных настроек производить не требуется. Для корректной работы аутентификации Kerberos в нескольких доменах необходимо настроить некоторые параметры доменов. А именно, потребуется произвести следующие настройки:

- Убедиться, что между всеми деревьями и лесами доменов, а также между всеми доменами в дереве установлено транзитивное двунаправленное доверие.
- Во всех доменах синхронизировано время.
- Хосты во всех доменах доверяют прокси-серверу.

Возьмём для примера инфраструктуру Active Directory со следующей конфигурацией:



Хосты из всех доменов пользуются прокси-сервером с FQDN auth.corp.lab, который разрешается в IP-адрес интерфейса UserGate NGFW. Keytab-файл также создан в домене corp.local и привязан к принципу HTTP/auth.corp.local.

Хосты из леса corp.lab, по умолчанию будут доверять запросам аутентификации Kerberos от хоста auth.corp.lab, так как все они находятся в рамках единого домена. Чтобы хосты из домена contoso.local также начали предоставлять данные аутентификации хосту из другого домена, нужно добавить FQDN прокси-сервера в зону доверенных хостов. Сделать это удобно при помощи групповых политик:

- User Configuration → Policies → Administrative Templates → Windows Components → Internet Explorer → Internet Control Panel → Security Page \ Site to Zone Assignment List.

В данной конфигурации прописать FQDN прокси-сервера и задать значение 2:

- User Configuration → Policies → Administrative Templates → Windows Components → Internet Explorer → Internet Control Panel → Security Page \ Trusted Sites Zone \ Logon Options. Установить в значение "Automatic logon with current username and password".

Для браузера FireFox возможно потребуется дополнительная настройка доверенных FQDN хостов для аутентификации. Подробнее читайте в статье [Авторизация с помощью Kerberos](#).

Лицензирование

Version: 6.x, 7.x, 7.5.x
Product: NGFW, UGMC, LogAn, SIEM, DCFW, WAF, SWG

Модель лицензирования решений UserGate включает два основных компонента:

1. Базовая лицензия (обязательная) — обеспечивает основные функциональные возможности устройства.
2. Дополнительные модули (опциональные) — позволяют активировать расширенные функции.

Базовая лицензия определяется параметрами производительности:

- для физических устройств — зависит от типа аппаратной платформы;
- для виртуальных образов — определяется количеством поддерживаемых ядер виртуальной машины.

Базовая лицензия является бессрочной (без обновлений).

Дополнительные модули можно активировать выборочно.

Модули включают регулярные обновления:

- программного обеспечения;
- встроенных библиотек и баз данных;
- сигнатур и аналитических моделей;
- экспертных правил и сервисов.

Способы активации лицензий на устройстве:

- Онлайн-активация (требуется подключение к интернету).
- Офлайн-активация (через сервис офлайн-активации ПИН-кодов).

Подробнее об особенностях лицензирования решений:

Категория продукта	Версия ПО
NGFW (New Generation Firewall)	6.x
	7.x
DCFW (Datacenter Firewall)	8.x
WAF (Web Application Firewall)	7.x
SWG (Secure Web Gateway)	7.5.x
MC (Management Center)	6.x
	7.x
LogAn (Log Analyzer)	6.x
	7.x
SIEM (Security Information and Event Management)	7.2
	7.x

Product: UserGate NGFW

Version: 6.x, 7.x

Задача

Что отображает список, открывающийся нажатием кнопки **Показать в Дашборд**? Как узнать количество занятых/свободных лицензий?

Решение

Кнопка **Показать в Дашборд** отображает список IP-адресов, занимающих лицензию. В этом списке могут присутствовать внешние IP-адреса, если через UserGate NGFW проходит трафик с этих адресов, за исключением устройств, чей трафик проходит через UserGate с использованием правил публикации DNAT, Reverse-прокси, веб-портала, защиты почтового трафика.

UserGate считает уникальные IP-адреса, трафик с которых приходит на интерфейсы UserGate; освобождение лицензии происходит по факту прекращения трафика с IP-адреса, который уже был учтён как "получивший" или "израсходовавший" лицензию. Таймаут, в течение которого с уникального IP-адреса не должно приходить ни одного TCP/IP пакета, - 1 минута.

Лицензии расходуются не только на подключения к NGFW, но и на любые исходящие соединения (например, соединение почтовой программой к внешнему почтовому серверу) и подключения неинтерактивных пользователей (например антивируса, службы обновления ОС и т.д.).

Чтобы узнать количество свободных лицензий необходимо от общего количества лицензируемых устройств отнять количество устройств, уже занимающих лицензию.

Отсутствует лицензия на одном из узлов кластера

Version: 5.x, 6.x, 7.x
Technology: Clustering and HA
Product: UserGate NGFW

Вопрос

Один из узлов кластера в статусе "отсутствует лицензия".

Ответ

Скорее всего вам выдали лицензию без поддержки кластеризации. Как активировать лицензию в кластере смотрите [здесь](#).

Technology: Clustering and HA
Version: 5.x, 6.x, 7.x
Product: UserGate NGFW

Задача

Активировать лицензию в кластере.

Решение

Если на одном из узлов кластера отсутствует лицензия, выполните следующее:

1. Проверьте, что в вашу лицензию включен модуль Cluster, разрешающий работу устройств UserGate в режиме кластера конфигурации.
2. Убедитесь, что лицензия активирована на первом узле кластера (мастер-узле).

ПримечаниеДля всех узлов кластера конфигурации нужна только одна лицензия, которая сначала активируется на мастер-узле кластера в онлайн- или офлайн-режиме. Если на мастер-узле кластера лицензия была активирована онлайн, дополнительному узлу для активации лицензии также потребуется доступ в интернет. При офлайн-активации лицензии на первом узле подключение дополнительного узла к интернету не требуется.

3. Активируйте лицензию на дополнительном узле. Для этого в веб-интерфейсе дополнительного узла кластера конфигурации на странице **Дашборды** в виджете **Лицензия** нажмите **Проверить лицензию**.

Если для подключения к интернету на кластере настроен виртуальный IP-адрес, для активации лицензии выполните следующее:

1. Активируйте лицензию на мастер-узле кластера.
2. Назначьте дополнительный узел мастер-узлом, чтобы виртуальный IP-адрес был присвоен дополнительному узлу.
3. Активируйте лицензию на временном мастер-узле. Для этого в его веб-интерфейсе на странице **Дашборды** в виджете **Лицензия** нажмите **Проверить лицензию**.
4. Верните роль мастер-узла первому узлу.

Если к интернету посредством кабеля подключен только мастер-узел, для активации лицензии выполните следующее:

1. На мастер-узле и дополнительном узле настройте пару интерфейсов и соедините их кабелем.
2. На дополнительном узле укажите первый узел в качестве шлюза по умолчанию.
3. Создайте правила межсетевого экрана и трансляции адресов, разрешающие передачу трафика из интернета.
4. Активируйте лицензию на дополнительном узле. Для этого в веб-интерфейсе дополнительного узла кластера конфигурации на странице **Дашборды** в виджете **Лицензия** нажмите **Проверить лицензию**.

Ошибка при активации лицензии

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW, UserGate MC, UserGate LogAn

Задача

При попытке активации лицензии возникает ошибка: **Превышен таймаут (между фронтендом и xapi-гис). Проверьте сетевые настройки (IP, DNS, шлюз)** .

Решение

Данная ошибка обычно возникает при недоступности одного из необходимых для обновления и лицензирования серверов. Необходимо обеспечить доступ до следующих серверов:

reg2.entensys.com
static.entensys.com
direct.entensys.com
urif.entensys.com

Также необходимо проверить настройки DNS сервера на устройстве, устройство должно быть в состоянии разрешать вышеуказанные имена.

Не удается активировать лицензию

Technology: Networking

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW, UserGate MC, UserGate LogAn, UserGate C100, UserGate D200/D500, UserGate E1000/E3000, UserGate F8000, UserGate X1, UserGate Log Analyzer E6/E14, UserGate Log Analyzer F25, UserGate Management Center C, UserGate Management Center E, KinderGate Родительский контроль, UserGate C150

Задача

Не удается ввести лицензию. Выдает такую ошибку: "Невозможно подключиться к серверу лицензирования (Network error). Проверьте сетевые настройки (IP, DNS, шлюз)".

Решение

Необходимо убедиться, что настройки сети на устройстве верны, т.е. проверить верно ли указан ip - адрес устройства, маска подсети, шлюз по умолчанию и DNS - сервер. При ошибочных настройках в любом из этих компонентов будут неполадки при работе с сетью и невозможно будет активировать лицензию, то есть для активации лицензии необходим доступ до сервера лицензий UserGate - reg2.entransys.com.

Подробнее о настройке сети можно прочитать в документации: [UserGate NGFW](#), [UserGate MC](#), [UserGate LogAn](#)

Получение лицензии для выполнения учебного проекта

Version: 6.x, 7.x

Product: UserGate NGFW, UserGate MC, UserGate LogAn

Задача

Я пишу курсовую или дипломную работу по информационной безопасности. Как мне получить временную лицензию на ПО UserGate?

Решение

Обратитесь на кафедру информационной безопасности вашего учебного заведения за доступом к установленным виртуальным машинам с ПО UserGate.

Если ваш вуз еще не сотрудничает с нашей компанией, то вам нужно проделать следующие шаги:

1. Зарегистрируйтесь, указав актуальный адрес электронной почты в домене учебного заведения, на официальном сайте компании, заполнив [форму регистрации](#).
2. Подтвердите свой электронный адрес, пройдя по ссылке из электронного письма. Если письмо долго не приходит, проверьте папку с нежелательной почтой.
3. Напишите письмо на academy@usergate.com с описанием проекта и указанием адреса электронной почты, использованного при регистрации, чтобы завершить процесс активации пользователя, получить доступ к дистрибутивам и облегчить подбор параметров лицензии.

Офлайн-активация лицензий необходима для устройств UserGate, находящихся в изолированной сети без доступа к интернету.

Процесс лицензирования включает следующие этапы:

- 1. Генерация запроса — создание на лицензируемом устройстве файла запроса на офлайн-активацию.
- 2. Активация запроса — обработка сгенерированного файла запроса с помощью сервиса офлайн-активации ПИН-кодов.
- 3. Применение лицензии — загрузка активированного файла обратно на лицензируемое устройство.

Генерация запроса

Чтобы сгенерировать файл запроса на офлайн-активацию лицензии, зайдите с помощью веб-браузера на лицензируемое устройство по следующему адресу:

- <https://IP-address:8001?features=offline-reg> — для NGFW, WAF, DCFW;
- <https://IP-address:8010?features=offline-reg> — для MC, LogAn, SIEM.

Где IP-address — это IP-адрес лицензируемого устройства.

В веб-консоли устройства перейдите на вкладку **Дашборд**.

В виджете **Лицензия** нажмите на строку **Нет лицензии**.

В окне активации продукта нажмите на строку **Начать активацию в автономном режиме**:



Введите ПИН-код устройства а нажмите **Далее**:

Скачайте сгенерированный файл запроса на офлайн-активацию:

Активация запроса

С компьютера, имеющего доступ в интернет, обратитесь в [сервис офлайн-активации ПИН-кодов](#). Для входа в сервис потребуется авторизация в [Едином центре авторизации](#).

На странице сервиса офлайн-активации нажмите **Выбрать** и добавьте файл с запросом на офлайн-активацию, полученный с лицензируемого устройства:

Выберите версию ПО активируемого устройства и нажмите **Обработать**:

Подтвердите операцию активации:

В случае успешной активации файла отобразится статус: «Успешно активирован». Скачайте активированный файл, нажав на значок со стрелкой в столбце **Действия**:

Если активация не была успешной, отобразится статус: «Ошибка активации».

При нажатии на статус отобразится описание возможной причины ошибки.

Применение лицензии

Загрузите активированный файл на лицензируемое устройство. Для этого:

- 1. В виджете **Лицензия** на вкладке **Дашборд** лицензируемого устройства откройте окно офлайн-активации.
- 2. Выберите опцию **Завершить активацию в автономном режиме**:

3. В открывшемся окне укажите активированный файл, полученный в сервисе офлайн-активации, и нажмите **Далше**:

Процесс лицензирования завершен.

Не создается виртуальный маршрутизатор

Product: UserGate NGFW

Задача

Не создается виртуальный маршрутизатор

Решение

В названии VRF нельзя использовать русские буквы, заглавные буквы, а также оно не должно содержать имена интерфейсов, например port1 или tunnel1. [Подробнее...](#)

Маршрутизация при использовании явного прокси

Product: UserGate NGFW

Version: 5.x, 6.x, 7.x

Вопрос

При использования явного прокси будет ли явный прокси использовать для маршрутизации наружу только основной шлюз? Будут ли правила PBR учитываться в работе явного прокси?

Ответ

Правила PBR применяются к соединениям устанавливаемым через явный прокси, IP и зона источника в них также работают. Подробнее об алгоритме обработки трафика в UserGate читайте в статье [UserGate NGFW 6 packet flow](#).

Не удаётся создать 2 моста L2 и L3 на одном устройстве

Product: UserGate NGFW

Version: 5.x, 6.x, 7.x

Technology: Networking

Задача

Не удаётся создать 2 моста L2 и L3 на одном устройстве.

Решение

Это ограничения архитектуры. Мосты L2 и L3 отличаются возможностью использовать интерфейс моста L3 для исходящего трафика самого устройства и, как недостаток описанного выше, необходимостью иметь на устройстве полную таблицу маршрутизации для проходящего через мост L3 клиентского трафика; использование моста L2 требует также наличия интерфейсов L3 для связи устройства с внешними серверами.

Примечание Работа в режиме Мост ничем не отличается от работы в режиме маршрутизации трафика, но нужно учитывать, что в правилах межсетевого экрана необходимо указать одинаковые зону источника и зону назначения.

Для решения поставленной задачи, т.е. создания аналога конфигурации с мостами L2 и L3 одновременно, необходимо:

1. Создать все мосты как L3.
2. Для мостов, которые должны выполнять функции L2, создать отдельные виртуальные маршрутизаторы.
3. Каждому мосту, выполняющему функции L2, выделить по одному адресу из сетей, в разрыв которых он включен, и создать полную таблицу маршрутизации.

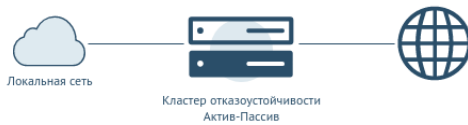
Примечание Схема организации связи не должна быть организована так, чтобы трафик мог проходить через устройство дважды без смены адресов/портов источника/назначения.

Кластер Актив-Пассив не использует виртуальный адрес для отправки трафика

Product: UserGate NGFW
Version: 5.x, 6.x, 7.x
Technology: Routing

Задача

Два устройства UserGate NGFW настроены на работу в кластере отказоустойчивости в режиме Актив-Пассив.



Адресация на интерфейсах, использующихся для выхода в Интернет:

- мастер-узел: IP_address1;
- резервный узел: IP_address2;
- виртуальный адрес кластерного интерфейса: IP_address3.

Необходимо произвести настройку, чтобы для отправки трафика в сеть Интернет UserGate использовал виртуальный адрес IP_address3.

Решение

Необходимо настроить правило типа NAT. Для этого перейдите в раздел **Политики сети → NAT и маршрутизация** веб-интерфейса управления, нажмите **Добавить** и укажите следующие условия:

- **Тип:** NAT;
- **SNAT IP:** виртуальный адрес IP_address3;
- **Источник:** зона локальной сети или адреса отдельных устройств, для отправки трафика которых необходимо использовать виртуальный адрес;
- **Назначение:** зона, которой принадлежат внешние интерфейсы.

Product: UserGate NGFW
Version: 5.x, 6.x, 7.x
Technology: VPN

Задача

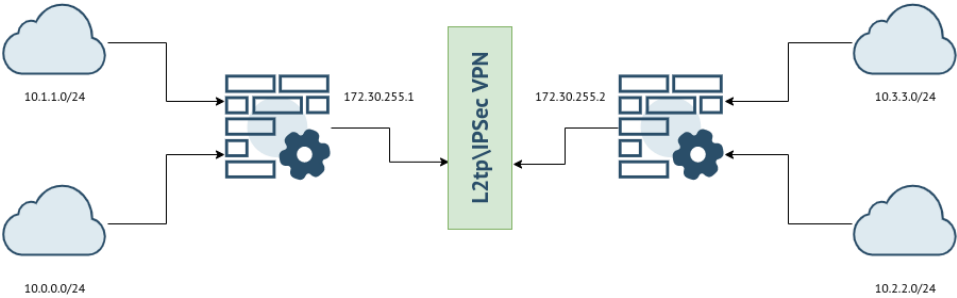
Объединить несколько сетей с помощью VPN site-to-site.

Решение

Для решения этой задачи необходимо настроить VPN туннель между граничными устройствами. В качестве таких устройств могут выступать UserGate NGFW, маршрутизаторы типа MikroTik и др. Посмотреть настройки VPN site-to-site можно [здесь](#) или [здесь](#).

Внимание! Плохой идеей будет использование разных VPN подключений для каждой сети, при наличии единого маршрутизатора для этих сетей.

После настройки VPN туннеля необходимо будет прописать маршруты для объединяемых сетей. Например, для случая на следующей схеме:



маршруты будут выглядеть следующим образом:

На устройстве с адресом 172.30.255.1:

Название	Тип	Адрес назначения	Шлюз	Интерфейс	Метрика
for10.2.2.0	unicast	10.2.2.0/24	172.30.255.2	tunnel3	0
for10.3.3.0	unicast	10.3.3.0/24	172.30.255.2	tunnel3	0

На устройстве с адресом 172.30.255.2:

Название	Тип	Адрес назначения	Шлюз	Интерфейс	Метрика
for10.0.0.0	unicast	10.0.0.0/24	172.30.255.1	tunnel2	0
for10.1.1.0	unicast	10.1.1.0/24	172.30.255.1	tunnel2	0

Где: 172.30.255.1 и 172.30.255.2 - адреса VPN интерфейсов граничных устройств, имена интерфейсов взяты для примера и их нужно поменять соответственно вашей рабочей схеме сети. Метрика - отвечает за приоритет маршрута и может быть любой, в общем случае можно оставить значение 0. Номера сетей вида 10.x.x.x нужно заменить на соответствующие вашей рабочей схеме.

Недоступны сервисы при использовании VRF

Product: UserGate NGFW

Version: 6.x, 7.x

Technology: Routing

Задача

При использовании VRF некоторые сервисы становятся недоступными.

Решение

Чаще всего проблема заключается в маршрутах до искомым сервисов. Надо иметь в виду, что сервисы ПО HW UserGate запускаются в VRF "Маршрутизаторе по-умолчанию"(Default VRF), и необходимо внимательно следить за передачей маршрутов между виртуальными маршрутизаторами. Маршруты необходимо передавать в обе стороны(прямой и обратный).

Product: UserGate NGFW

Version: 5.x, 6.x, 7.x

Задача

Необходимо добавить на страницу авторизации Captive-портала логотип компании.

Решение

1. Скачайте шаблон страницы Captive-портала, это текстовый файл html.
2. Вставьте в нужное место страницы картинку в кодировке base64, например:

```
<div>
<p>Taken from wikipedia</p>

</div>
```

3. Сохраните файл.
4. Создайте новый шаблон страницы captive-портала и импортируйте в него сохранённый файл. Выберите созданный шаблон в используемом captive-профиле или назначьте его шаблоном по умолчанию.

Особенность отображения пользователей на графике

Product: UserGate NGFW

Version: 6.x, 7.x

Задача

В лицензии на продукт нет лимита пользователей, но на графике производительности отражается "Пользователи 24 из 25 (96%)"

Решение

График производительности отображает количество пользователей, подключенных в данный момент, и максимальное количество одновременно подключённых пользователей, зафиксированное до настоящего момента. Т.е., для данного примера:

- 24 - количество пользователей, подключенных в данный момент;
- 25 - максимальное количество одновременно подключённых пользователей, зафиксированное до настоящего момента.

Вычисление процента, соответственно, происходит относительно максимального количества одновременно подключённых пользователей, зафиксированного до настоящего момента.

Если бы системой было зарегистрировано пиковое значение в 100 человек, то процент высчитывался бы от 100. В случае лицензии без ограничения по пользователям статистика в таком виде выглядит более наглядно.

Одновременная авторизация с двух устройств

Product: UserGate NGFW

Version: 5.x, 6.x, 7.x

Technology: Identification and Authentication

Задача

При одновременной авторизации пользователя через captive-портал и агент терминального сервера NGFW сбрасывает авторизацию данного пользователя со всех устройств.

Решение

Проблема заключалась в том, что информация о группах пользователя, которую UserGate получал при авторизации на captive-портале и от агента аутентификации, не совпадала.

ПримечаниеРекомендуется установить терминальный агент последней версии (установочный файл доступен в личном кабинете My.UserGate)

1. Проверьте группы пользователя, полученные устройствами.

Например, для проверки на ПК с ОС Windows используйте **whoami-groups**.

2. Если группы не совпадают, перезагрузите устройства.
3. Повторно авторизуйтесь на UserGate.

Для сброса авторизации всех пользователей в веб-интерфейсе управления перейдите в раздел **Пользователи и устройства → Серверы аутентификации** и нажмите на кнопку **Сбросить аутентификацию всех пользователей**.

Можно выполнить сброс авторизации конкретного пользователя с помощью интерфейса командной строки (Command Line Interface, CLI); для выполнения команды необходимо знать IP-адрес пользователя (<IP_ADDRESS>):

- UserGate NGFW 6.x.x:
UTM> usersession terminate -ipv4 <IP_ADDRESS>
- UserGate NGFW 7.x.x:
Admin@UGOS# execute terminate usersession <IP_ADDRESS>

Также пользователь может самостоятельно завершить сессию, используя домен Logout captive-портала, указанный в настройках UserGate.

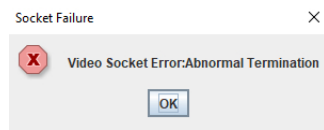
ПримечаниеUserGate в момент авторизации пользователя получает информацию только о группах LDAP, информация о которых есть на ПК пользователя. Информация о группах пользователя будет записана в базу данных, только в случае их использования в политиках UserGate.

Не открывается JAVA консоль в IPMI

Product: UserGate NGFW

Задача

Не открывается JAVA консоль при использовании IPMI. Возникающая ошибка: Video Socket Error: Abnormal Termination



Решение

Подобные ошибки практически всегда решаются выключением устройства штатными средствами с последующим отсоединением его от сети питания на 5 минут и последующим перезапуском.

Примечание Простая перезагрузка с использованием консоли к нужному результату скорее всего не приведет.

Как настроить выгрузку журналов на FTP сервер

Product: UserGate NGFW, UserGate LogAn
Version: 6.x, 7.x

Задача

Необходимо настроить выгрузку журналов за предыдущие сутки на FTP-сервер.

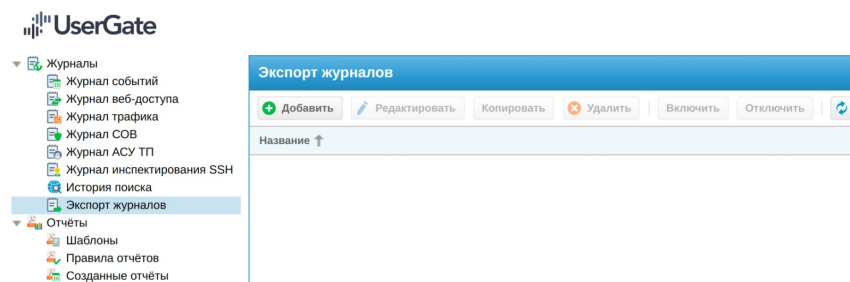
Решение

Функция экспорта журналов UserGate позволяет выгружать информацию на внешние серверы для последующего анализа или обработки. Подробную информацию о типах журналов и способах экспорта можно найти в разделе [Журналы](#) Руководства администратора.

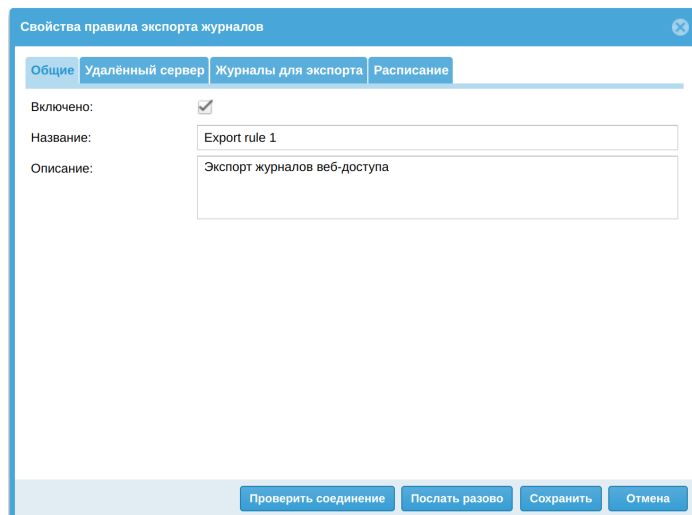
При отправке журналов на серверы ftp и ssh UserGate сохраняет данные для отправки во временных файлах в кодировке UTF-8. Журналы за предыдущие дни (по количеству дней ротации) хранятся в виде архивов, журнал за текущий день не архивирован. По указанному расписанию все созданные для отправки файлы копируются на удаленный сервер, при этом файлы не очищаются и не удаляются. Данная настройка позволяет указать период ротации временных файлов (в днях) или удалить любой из временных файлов вручную. Ротация файлов происходит один раз в сутки.

Для создания правила экспорта журналов необходимо выполнить следующие шаги:

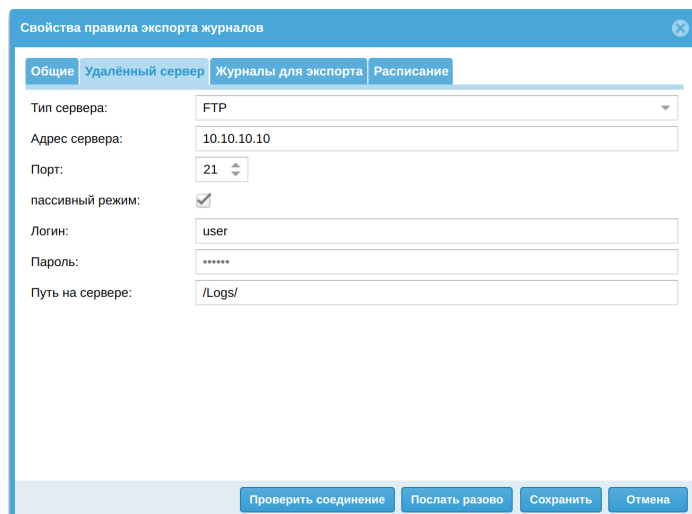
1. В разделе **Журналы** → **Экспорт журналов** добавить новое правило:



2. На вкладке **Общие** установить флажок **Включено**, указать название нового правила и его краткое описание:



3. На вкладке **Удаленный сервер** указать параметры сервера, на который будут экспортироваться журналы:



4. Нажать на кнопку **Проверить соединение** и убедиться в доступности сервера:

Свойства правила экспорта журналов

Общие Удалённый сервер Журналы для экспорта Расписание

Тип сервера: FTP

Адрес сервера:

Порт:

пассивный режим:

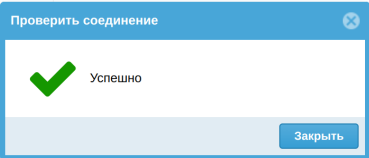
Логин:

Пароль:

Путь на сервере: Downloads/Logs

Проверить соединение

Послать разово Сохранить Отмена



4. На вкладке **Журналы для экспорта** установить период ротации журналов, выбрать тип экспортируемых журналов и их формат. Доступны следующие типы форматов:

- CEF;
- CEF Compact;
- JSON;
- @CEE: JSON;

Свойства правила экспорта журналов

Общие Удалённый сервер Журналы для экспорта Расписание

Период ротации журналов (дней): 7

Журналы	Формат	Размер журнала
☐ Журнал DNS	JSON	—
☐ Журнал событий	JSON	—
☐ Журнал COB	JSON	—
☐ Журнал АСУ ТП	JSON	—
☐ Журнал инспектирования SSH	JSON	—
☐ Журнал трафика	JSON	—
☒ Журнал веб-доступа	JSON	—

Проверить соединение Послать разово Сохранить Отмена

5. На вкладке **Расписание** указать периодичность и время выполнения данного правила. Если журнал необходимо экспортировать разово, нажать кнопку **Послать разово**:

Свойства правила экспорта журналов

Общие Удалённый сервер Журналы для экспорта Расписание

☒ Ежедневно Каждый день в 01:00
☐ Еженедельно
☐ Ежемесячно
☐ Каждые ... часов
☐ Каждые ... минут
☐ Задать вручную

Проверить соединение Послать разово Сохранить Отмена

6. Сохранить созданное правило экспорта журналов, нажав **Сохранить**.

Примечание Возможно сохранение журнала администратором вручную непосредственно из веб-консоли. При этом данные сохраняются только в формате CSV.

Примечание Если в настройках указан Log Analyzer, то обработка и экспорт журналов производится сервером LogAn.

С какой периодичностью отсыдаются уведомления о переполнении памяти?

Version: 6.1.8, 6.1.9, 7.0.0, 7.0.1, 6.x, 7.x

Вопрос

С какой периодичностью отсыдаются уведомления о переполнении памяти?

Ответ

Проверка на переполнение памяти происходит раз в 10 секунд, при этом берется моментальное значение памяти. И если есть переполнение отсылается уведомление.

Интерпретация результатов сканирования

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW, UserGate MC, UserGate LogAn, UserGate SIEM

Очень часто нам задают вопросы по уязвимостям обнаруженным сторонними сканнерами безопасности в наших продуктах. Ниже представлены ответы на подобные вопросы.

53(UDP)-DNS Отказ в обслуживании.

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW

Вопрос

Версия сервера: Usergate DNS v7.0.1.989R

Высокий уровень

Отказ в обслуживании

ID: 8352

CVE: CVE-2016-2776

Дата публикации: 27.09.2016

Краткое описание:

Уязвимость позволяет злоумышленнику вызвать отказ в обслуживании (ошибку утверждения и завершение работы демона).

Описание

Уязвимость в buffer.c в named в ISC BIND, связанная с некорректным построением ответов, позволяет злоумышленникам, действующим удаленно, вызвать отказ в обслуживании (ошибку утверждения и завершение работы демона) при помощи специально сформированного запроса.

Ответ

В продукте UserGate в качестве DNS сервера **не используются** версии компонента ISC BIND, подверженные данной уязвимости.

DNS-сервер поддерживает рекурсию запросов.

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW

Вопрос

Уязвимость: Рекурсия

ID: 1058

CVE: CVE-1999-0024

Дата публикации: 13.08.1997

Описание:

DNS-сервер поддерживает рекурсию запросов. При определенных обстоятельствах злоумышленник может вызвать на сервере отказ в обслуживании.

Ответ

В продукте UserGate ограничена глубина рекурсии DNS запросов, в связи с этим вызвать отказ в обслуживании данным способом не представляется возможным, данная уязвимость не применима к продукту UserGate.

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW

Вопрос

Уязвимость: Некорректная цепочка сертификатов

ID: 7034

Описание:

При проверке цепочки доверия сертификата данного сервиса были обнаружены следующие ошибки # Цепочка сертификатов не полная

Ответ

В продукте UserGate используются самоподписанные сертификаты. Поскольку сертификаты не подписаны каким-либо удостоверяющим центром, сканеры определяют цепочку с их участием неполной. Для устранения данной уязвимости необходимо заменить сертификат по умолчанию на подписанный удостоверяющим центром пользовательский сертификат.

Слабый криптографический ключ

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW

Вопрос

Уязвимость:

Слабый криптографический ключ

ID: 8309

Краткое описание:

Обнаружен слабый криптографический ключ. Длина ключа, используемая криптографическим алгоритмом, определяет уровень безопасности, который может быть достигнут.

Алгоритм (длина ключа): rsaEncryption(1024)

Ответ

В продукте UserGate используются сертификаты по умолчанию (default) с длиной ключа 1024. Для устранения данной уязвимости необходимо заменить сертификат по умолчанию (default) на пользовательский сертификат с требуемой длиной ключа.

Version: 5.x, 6.x, 7.x

Product: UserGate NGFW

Вопрос

Уязвимость:

Найден логин и хэш пароля пользователя IPMI

ID: 8312

CVE: CVE-2013-4786

Краткое описание:

Был подобран логин и получен SHA-1 хэш пароля учетной записи IPMI. Если пароль недостаточно сложный, его можно восстановить с помощью общедоступных утилит.

Ответ

Функционал модуля IPMI опционален, требуется только для подключения из локальной сети организации. Не рекомендуется публиковать доступ к данному интерфейсу во внешнюю сеть, где существуют риски эксплуатации данной уязвимости.

Обнаружение уязвимости типа CVE-2002-20001 при сканировании NGFW UserGate сторонними сканерами.

Version: 6.x, 7.x

Product: UserGate NGFW

Задача

Сканирование NGFW UserGate сторонними сканерами показывает открытую уязвимость типа CVE-2002-20001 Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater). Как устранить?

Решение

Уязвимость CVE-2002-20001 Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater) использует механизм реализации протокола обмена ключами Diffie-Hellman Key Exchange (DHE). Злоумышленник со стороны клиента может отправлять на сервер произвольную последовательность под видом открытого ключа, вызывая повышение загрузки CPU сервера вычислениями протокола DHE. Согласно методике оценки уязвимостей (CVSS) она имеет высокую, но не критичную оценку (7.5) и влияет на доступность ресурса, при этом конфиденциальность данных и целостность ресурса не находятся под угрозой. Эффективность потенциальной атаки с использованием этой уязвимости во многом зависит от типа используемого криптографического протокола, конкретной реализации системной библиотеки, а также размера ключа, используемого во время обмена ключами. В базовом сценарии атаки клиент запрашивает использование только протокола DHE и максимально возможную длину ключа.

В решениях UserGate используется протокол DHE. Анализ воздействия уязвимости на конкретную реализацию DHE в оборудовании UserGate не показал ее влияния на производительность. В качестве дополнительных мер безопасности можно сделать следующее:

- Отключить протокол DHE в настройках используемых [профилей SSL](#) для удаленного доступа к устройству. Вместо DHE могут использоваться протоколы RSA (для поддержки устаревших приложений) и/или ECDHE.
- Ограничить количество и тип DH групп в настройках [профилей безопасности VPN](#) только реально используемыми.

Статус портов при сканировании Nmap

Technology: Firewall
Version: 5.x, 6.x, 7.x
Product: UserGate NGFW

Вопрос

Что означают статусы портов при сканировании nmap или им подобным.

Ответ

Nmap и ему подобные сканеры портов определяют 6 состояний программногo порта:

Открыт (open)

Приложение принимает запросы на TCP соединение или UDP пакеты на этот порт.

Закрыт (closed)

Закрытый порт доступен (он принимает и отвечает на запросы Nmap), но не используется каким-либо приложением.

Фильтруется (filtered)

Администраторы могут заблокировать порты с помощью брандмауэров. в этом случае Nmap не может определить, открыт ли порт, т.к. фильтрация пакетов не позволяет достичь запросам Nmap этого порта.

Не фильтруется (unfiltered)

Это состояние означает, что порт доступен, но Nmap не может определить открыт он или закрыт.

Открыт|фильтруется (open|filtered)

Nmap характеризует порт таким состоянием, когда не может определить открыт порт или фильтруется. Это состояние возникает при таких типах сканирования, при которых открытые порты не отвечают. Отсутствие ответа также может означать, что пакетный фильтр пропустил запрос или ответ не был получен. Поэтому Nmap не может определить наверняка открыт порт или фильтруется. При сканировании UDP, по IP протоколу, FIN, NULL, а также Xmas порт может быть охарактеризован таким состоянием.

Закрыт|фильтруется (closed|filtered)

Это состояние используется, когда Nmap не может определить закрыт порт или фильтруется.

Сканирование сети обнаруживает порты даже на тех адресах, где нет соответствующих сервисов

Technology: Firewall
Version: 5.x, 6.x, 7.x
Product: UserGate NGFW

Задача

При сканировании IP адресов серверов, защищенных UserGate NGFW, порты, на которых нет соответствующих сервисов, показываются в статусе "закрытый".

Решение

Сканеры типа Nmap распознают [статус](#) порта по ответу от сканируемого ресурса. Статус "закрыт" означает, что на отправку сканером пакета SYN, цель ответила пакетом RST. Это означает, что данный порт доступен, но на нем не запущено никаких сетевых сервисов. Если этот порт разрешен на межсетевом экране UserGate NGFW, это нормальное поведение системы. В противном случае следует внимательно изучить настройки межсетевого экрана UserGate NGFW и устранить ошибки конфигурирования.

Если есть список устройств, для которых необходимо сделать порт недоступным, то можно создать правило DNAT в неиспользуемый адрес и заблокировать трафик на этот адрес правилом межсетевого экрана.

Ложные срабатывания сигнатур IDS

Product: UserGate NGFW

Version: 6.x, 7.x

Задача

Происходят ложные срабатывания сигнатур COB

Решение

Чтобы исключить ложные срабатывания:

1. Создать профиль COB.

Перейдите в раздел **Библиотеки → Профили COB**. На панели **Профили** нажмите **Добавить** и создайте профиль COB. Выбрав профиль нажмите **Добавить** на панели **Сигнатуры**. Далее укажите сигнатуры, ложные срабатывания которых нужно исключить.

2. Исключить срабатывание сигнатуры.

После создания профиля COB с необходимым набором сигнатур перейдите в раздел **Политики безопасности → COB**. Откройте настройки правила, действие которого выполнится в результате срабатывания сигнатуры (правила с действиями **Журналировать** или **Запретить**); во вкладке **Профили исключения** добавьте профиль COB с сигнатурами, создающими ложные срабатывания.

Подробнее о настройке системы обнаружения и предотвращения вторжений читайте в [UserGate 6. Руководство администратора](#).

