

Администрирование межсетевых экранов UserGate 7

Программа курса

О курсе

Код курса	UG.NGFW7 (UGOS7)
Версия курса	3.0
Длительность курса	5 дней / 40 академических часов
Описание	В данном курсе рассматривается установка и конфигурирование межсетевых экранов UserGate, работающих под управлением операционной системы UGOS 7.X. Вы научитесь выполнять установку и первоначальную настройку, создавать кластеры конфигурации и отказоустойчивости, формировать политику безопасности, включающую в себя инспектирование SSL, контроль доступа пользователей, настройку системы предотвращения вторжений, VPN-туннели и многие другие функции. В курсе также рассматривается журналирование с использованием UserGate Log Analyzer и централизованное управление устройствами с использованием UserGate Management Center.
Аудитория	Курс предназначен для системных инженеров и специалистов в области информационной безопасности, которым необходимо получить знания и навыки по работе с межсетевыми экранами UserGate.
Предварительные требования	Для успешного прохождения курса вам необходимо обладать следующими знаниями и навыками: ■ знания сетевых моделей ISO/OSI и TCP/IP; ■ знания основных сетевых протоколов IP, TCP, UDP, DNS, DHCP, HTTP, HTTPS, FTP, SSH и других; ■ знания принципов работы протокола IP и IP-маршрутизации (статическая и динамическая маршрутизация, шлюз по умолчанию, IP-адресация, маска подсети); ■ базовые знания процессов аутентификации и авторизации и соответствующих протоколов; ■ понимание концепций межсетевого экранирования; ■ опыт работы с операционными системами на базе Windows и/или Linux; ■ желательно обладать опытом работы в командной строке.

Настоящим уведомляем, что исключительное право на все материалы данного Учебного курса, включая программу курса, опубликованную на сайте <https://usergate.com>, принадлежат ООО «Юзергейт». Любое копирование, распространение, использование любым другим способом данных материалов без разрешения правообладателя запрещено.

* с подробными изменениями в различных версиях курса можно ознакомиться в конце данной программы

Программа курса

1

Обзор продуктов UserGate

- межсетевые экраны UserGate;
- экосистема UserGate SUMMA.

Установка и базовая настройка

- установка;
- первоначальная настройка.

Интерфейсы администратора

- обзор административных интерфейсов;
- графический интерфейс;
- интерфейс командной строки.

Лицензирование

- общие сведения о лицензировании;
- процесс активации лицензии.

Ролевая модель доступа

- обзор ролевой модели;
- настройка ролевой модели.

Лабораторная работа 1.1. «Установка и базовая настройка»

- знакомство со стендом;
- базовая конфигурация;
- настройка ролевой модели;
- экспорт/импорт конфигурации;
- настройка NGFW в филиале.

2

Кластер конфигурации

- обзор кластеров UserGate;
- настройка кластера конфигурации.

Отказоустойчивый кластер

- протоколы отказоустойчивости первого хопа (FHRP);
- концепции кластера отказоустойчивости;
- настройка кластера отказоустойчивости.

Лабораторная работа 2.1. «Кластеры»

- настройка кластера конфигурации;
- настройка отказоустойчивого кластера.

3

Зоны и сетевые интерфейсы

- зоны;
- сетевые интерфейсы.

Маршрутизация

- шлюзы;
- виртуальные маршрутизаторы;
- статическая и динамическая маршрутизация.

Сетевые сервисы

- DNS;
- DHCP.

Сетевая диагностика

- мониторинг сети;
- протокол LLDP.

Лабораторная работа 3.1. «Сетевая конфигурация»

- маршрутизация;
- настройка DNS и DHCP;
- сетевая диагностика;
- компоненты UserGate SUMMA.

4

Обзор политик сети

- алгоритм обработки трафика;
- библиотеки элементов;
- сценарии.

Политика межсетевого экрана

- правила политики межсетевого экрана;
- идентификация приложений;
- работа с правилами политики межсетевого экрана.

NAT и PBR

- правила NAT;
- маршрутизация с использованием политик (PBR).

Балансировка и управление пропускной способностью

- балансировка нагрузки;
- управление пропускной способностью.

Лабораторная работа 4.1. «Политики сети»

- работа с библиотеками;
- правила межсетевого экрана;
- трансляция адресов;
- балансировка, правила пропускной способности и сценарии.

5

Применение сертификатов в NGFW

- цифровые сертификаты;
- настройки сертификатов на NGFW.

Инспектирование SSL

- обзор SSL/TLS;
- настройка инспектирования SSL;
- отправка дешифрованного трафика на внешние системы.

Инспектирование SSH

- обзор SSH;
- настройка инспектирования SSH.

Лабораторная работа 5.1. «Сертификаты и инспектирование SSL»

- цифровые сертификаты;
- инспектирование SSL и SSH.

6

Компоненты идентификации пользователей

- способы идентификации;
- серверы аутентификации;
- профили аутентификации.

Технология UserID

- обзор UserID;
- настройка UserID.

Captive-портал, агенты авторизации, идентификация по атрибутам

- captive-портал;
- локальные пользователи и агенты авторизации.

Лабораторная работа 6.1. «Идентификация пользователей»

- технология UserID;
- captive-портал;
- локальные пользователи и агент аутентификации.

7

Обзор политики безопасности

- компоненты политики безопасности;

Настройка политик безопасности

- настройка фильтрации контента и веб-безопасности;
- система обнаружения вторжений.

Лабораторная работа 7.1. «Политика безопасности»

- фильтрация контента;
- система обнаружения вторжений.

8

Обзор технологий удаленного доступа

- VPN-туннели;
- способы публикации ресурсов.

Настройка VPN сайт-сайт и VPN удаленного доступа

- настройка VPN-туннеля сайт-сайт;
- настройка VPN-туннелей удаленного доступа.

Лабораторная работа 8.1. «Технологии предоставления удаленного доступа»

- настройка IKEv2 VPN-туннеля сайт-сайт;
- настройка IKEv2 VPN-туннеля удаленного доступа;
- настройка L2TP/ipsec VPN-туннеля сайт-сайт;
- настройка L2TP/ipsec VPN-туннеля удаленного доступа.

9

Веб-портал

- настройка веб-портала.

Reverse-прокси

- настройка reverse-прокси.

Лабораторная работа 8.1. «Технологии предоставления удаленного доступа»

- веб-портал;
- Reverse-прокси.

10

Средства диагностики и мониторинга

- мониторинг и диагностика;
- оповещения и SNMP.

Журналы и отчеты

- работа с журналами;
- отчеты.

Техническая поддержка и устранение неисправностей

- работа со службой технической поддержки UserGate;
- решение типовых проблем.

Лабораторная работа 9.1. «Мониторинг, журналы, отчетность»

- средства диагностики и мониторинга;
- журналы и отчеты.

Изменения в курсе UGOS 7

Версия 2.0

New! В лабораторном стенде используется версия UGOS 7.1.1. Обновлено команды, скриншоты и т.д. в соответствии с данной версией.

Установка и базовая настройка / Ролевая модель доступа / Настройка ролевой модели / Подключение LDAP-коннектора

- Добавлена информация об отказоустойчивости LDAP;

Мониторинг, поиск и устранение неисправностей / Журналы и отчеты / Работа с журналами / Ротация журналов при экспорте

- Исправлен текст и слайд;

New! Мониторинг, поиск и устранение неисправностей / Журналы и отчеты / Работа с журналами / Системная ротация журналов

- Новый слайд и текст, описывающий системный процесс ротации журналов;

Политики сети / Политика межсетевого экрана / Правила политики межсетевого экрана / Обработка правил

- Изменен скриншот на слайде в соответствии с интерфейсом версии 7.1.1;

New! Сетевая конфигурация / Зоны и сетевые интерфейсы / Зоны

- Добавлена глава «Защита от DoS-атак на уровне зоны».

Политики сети / Политика межсетевого экрана / Правила политики межсетевого экрана / Идентификация приложений

- Дополнены разделы «Сигнатуры приложений» и «Профиль приложений». В частности, в главу о профиле добавлена информация о зависимостях между сигнатурами и ссылка на соответствующий раздел документации;
- Добавлена информация о зависимостях на слайд.

Политики сети / Обзор политик сети / Сценарии

- Тема по сценариям перенесена из главы «Политики безопасности» в главу «Политики сети». Добавлена опциональная лабораторная работа Политики сети / Балансировка, правила пропускной способности и сценарии/ Правила пропускной способности и сценарии.

New! Сертификаты, инспектирование SSL и SSH / Применение сертификатов в NGFW / Настройка сертификатов на NGFW

- Добавлена глава «Обзор PKI-аутентификации»;
- Добавлена глава «Профиль клиентского сертификата»;
- Добавлена глава «Аутентификация по сертификатам».

Технологии предоставления удаленного доступа

- Модуль разбит на 2 части: VPN – часть 1, Web Portal & Reverse Proxy – часть 2.

Технологии предоставления удаленного доступа – часть 1

- Изменена графика на слайде Настройка VPN сайт-сайт и VPN удаленного доступа / Настройка VPN-туннеля сайт-сайт / Алгоритм настройки сервера с учетом IKEv2 и аутентификации по сертификатам;
- Несколько изменен и дополнен текст главы Настройка VPN сайт-сайт и VPN удаленного доступа / Настройка VPN-туннеля сайт-сайт / Алгоритм настройки сервера;
- Изменена графика на слайде Настройка VPN сайт-сайт и VPN удаленного доступа / Настройка VPN-туннеля сайт-сайт / Алгоритм настройки клиента с учетом IKEv2 и аутентификации по сертификатам;
- Несколько изменен и дополнен текст главы Настройка VPN сайт-сайт и VPN удаленного доступа / Настройка VPN-туннеля сайт-сайт / Алгоритм настройки клиента;

Removed! UserGate Management Center и управление NGFW

- Модуль убран вместе с лабораторными работами. Будет перенесен в том или ином виде в курс по UserGate SUMMA.

Изменения Lab Guide версия 2.0

New! В лабораторном стенде используется версия UGOS 7.1.1. Обновлено команды, скриншоты и т.д. в соответствии с данной версией.

Политики сети / Правила межсетевого экрана / Идентификация приложений / Проверка / Модификация конфигурации для последующих лабораторных работ

- В шаге 8 изменено название профиля на Default Application Profile;
- Добавлен блок «Примечание» с рекомендациями перейти в Дашборд и просмотреть данные виджета «Топ 10 приложений»;

Политики сети / Трансляция адресов / Настройка NAT / Настройка DNAT

Лабораторная работа по настройке DNAT теперь более соответствует реальным внедрениям. Получаемая конфигурация является более безопасной.

- В лабораторной работе Политики сети / Работа с библиотеками / Создание объектов в CLI / Создание списков IP-адресов дополнительно создаются объекты для публикации A-WWW1 и A-WWW2 в DNAT. Объекты A-WWW1-Ext и A-WWW2-Ext с соответствующими внешними адресами.
- В лабораторной работе Политики сети / Трансляция адресов и балансировка / Настройка NAT / Настройка DNAT добавлены шаги по добавлению A-WWW1-Ext в поле «Адрес назначения» и соответствующий скриншот.

New Lab! Политики сети / Балансировка, правила пропускной способности и сценарии/ Правила пропускной способности и сценарии.

- Добавлена опциональная лабораторная работа по ограничению полосы пропускания со связанным сценарием. Аналогичная лабораторная работа была в курсе NGFW6.

Изменения в генерации сертификатов

Практически по всех заданиях в CSR-запросы добавляются атрибуты SAN, включающие соответствующие доменные имена и IP-адреса. Необходимо для корректной работы SSL-инспектирования, Captive-портала и страниц блокировки, в особенности при подключении с доменных машин.

New Lab! Сертификаты, инспектирование SSL и SSH / Цифровые сертификаты

- Добавлена обязательная лабораторная работа «Настройка Active Directory Certification Authority и профиля клиентских сертификатов». В лабораторной работе создается и публикуется шаблон сертификата, который в дальнейшем будет использоваться для генерации

* с подробными изменениями в различных версиях курса можно ознакомиться в конце данной программы

сертификатов клиентов (Web Console, VPN RA). В этой же лабораторной работе создается профиль клиентского сертификата, который также используется в последующих заданиях;

- Добавлена опциональная лабораторная работа по аутентификации в веб-консоли с использованием сертификатов. Openssl + Firefox.

Изменения в настройке DNS в виртуальных машинах ISP1 и ISP2

Внесены изменения в конфигурацию DNS на ISP1 и ISP2. Это необходимо для распознавания имени vpn.usergate.ext, которое используется при создании VPN-туннеля S2S.

- На ISP1 дополнительно разрешены DNS-запросы от 172.30.30.1 (CLI-B);
- DNS на ISP1 дополнительно принимает запросы из сети 172.30.30.0/24 (port2 CLI-B);
- На ISP1 настроена статическая запись vpn.usergate.ext = 203.0.113.1;
- На ISP2 настроен DNS-сервер и разрешены DNS-запросы от 172.31.31.1 (CLI-B);
- DNS на ISP2 принимает запросы из сети 172.31.31.0/24 (port2 CLI-B);
- На ISP2 настроена статическая запись vpn.usergate.ext = 198.51.100.1;

Изменения в виртуальной машине DC-A

- Добавлен пользователь vpnuser в OU UserGate с паролем Pa\$\$w0rd. У пользователя заполнен атрибут email = vpnuser@usergate.test. Данный пользователь используется при создании VPN S2S IKEv2 с аутентификацией по сертификатам.
- Добавлены группа VPN Users, добавлены пользователи ann и bob с паролями Pa\$\$w0rd, являющиеся членами данной группы. Группа и пользователи используются в лабораторной работе VPN Remote Access IKEv2 с сертификатами;
- Создан каталог c:\UserGate. В каталоге находится файл request.inf, необходимый для генерации запроса на получение сертификата для аутентификации клиентов VPN Remote Access IKEv2.

Изменения в виртуальной машине WWW1-A

- В каталоге /usr/share/nginx/html создан файл warning.html. В файле содержится предупреждение пользователям, проходящим авторизацию через Captive Portal.

New Lab! Изменения в лабораторных работах модуля «Идентификация пользователей»

- Модифицирована лабораторная работа по настройке Captive-портала. Теперь после аутентификации на портале пользователь перенаправляется на URL <http://10.2.2.51/warning.html>;
- В Captive-портал добавлена опциональная лабораторная работа «Аутентификация с использованием сертификатов»;
- Изменен таймер интервала опроса мониторинга AD = 30 сек.

New Lab! Изменения в лабораторных работах модуля «Технологии предоставления удаленного доступа»

- Лабораторные работы разбиты на два блока, в соответствии с изменениями в учебнике (VPN – часть 1, Web Portal & Reverse Proxy – часть 2);
- Добавлена лабораторная работа «Настройка IKEv2 VPN-туннеля сайт-сайт»;
- Добавлена лабораторная работа «Настройка IKEv2 VPN-туннеля удаленного доступа»;
- Лабораторные работы с настройкой L2TP IPsec переведены в разряд опциональных. Лабораторные работы модифицированы с учетом ранее сделанной конфигурации для туннелей IKEv2. Как отдельные независимые лабораторные работы их использовать нельзя.

Removed! UserGate Management Center и управление NGFW

- Модуль убран вместе с лабораторными работами. Будет перенесен в том или ином виде в курс по UserGate SUMMA.

Версия 2.1

Общие изменения

- Изменен шрифт, используемый для выделения элементов интерфейса, на шрифт с более жирным начертанием в учебнике, Lab Guide и слайдах;
- Наименование набора протоколов IPsec скорректировано в соответствии со стандартом (sec – со строчной буквы);
- Версия программного обеспечения, используемого в курсе, обновлена до 7.1.2;
- Исправлен ряд опечаток;
- Заменены изображения топологии на актуальную на слайде в приветственной главе и в Lab Guide (незначительные корректировки, убран UGMC);
- **Important!** В дальнейшем минорные изменения в курсе, такие как исправление незначительных ошибок, опечаток и т.д. будут приводить к изменению номера младшей версии, например, 2.1.1, 2.1.2 и т.д. Рекомендуется перед курсом проверить наличие изменений.

Изменения в учебнике версия 2.1

Установка и базовая настройка / Установка и базовая настройка / Первоначальная настройка / Интерфейс Port0

- Скорректирована информация о принадлежности данного интерфейса к зоне __Default__ до инициализации устройства.

Установка и базовая настройка / Установка и базовая настройка / Первоначальная настройка / Настройка интерфейса port0;

- Добавлена информация о необязательности шага с включением интерфейса и изменением на нем способа назначения адреса;

Установка и базовая настройка / Интерфейсы администратора / Интерфейс командной строки / Режимы ...

- Добавлены блоки «Ссылка» со ссылкой на документацию и информацией о том, что там содержится полный и актуальный список команд;
- Для команд export/import указано, что они используются для экспорта/импорта части конфигурации.

Установка и базовая настройка / Интерфейсы администратора / Интерфейс командной строки / Вложенность уровней и выполнение команд

- Добавлено замечание в конце об отсутствии обязательности использовать пробелы при указании элементов в квадратных скобках. Подсвечены оба варианта на слайде.

Кластеры / Отказоустойчивый кластер / Настройка кластера отказоустойчивости / Проверка кластера отказоустойчивости

- Добавлены команды диагностики и мониторинга «show ha-cluster...»;

Сетевая конфигурация / Зоны / Контроль доступа зоны

- Скорректирован список сервисов. Добавлен блок «Ссылка» со ссылкой на документацию и информацией о том, что там содержится полный и актуальный список сервисов;
- Добавлена информация о том, что разрешенные адреса в контроле доступа добавляются либо из списков IP-адресов библиотек, либо из GeoIP.

Мониторинг, поиск и устранение неисправностей / Техническая поддержка и устранение неисправностей / Работа со службой технической поддержки

- Глава «Уровни ТП» переименована в «Планы ТП». Добавлено описание нового плана Platinum;
- Глава «Приоритеты и уровни обслуживания» переименована в «Приоритеты проблем и время решения». Изменены значения SLA для различных приоритетов проблем и планов поддержки;
- **New!** Добавлена глава «Профессиональные сервисы».

Политики сети / Обзор политик сети / Алгоритм обработки трафика

- Изменен дизайн слайда «Компоненты инспектирования трафика»;
- **New!** Добавлена глава «Стадии обработки трафика», кратко описывающая стадии обработки;
- В главе «Packet Flow» добавлена корректная и актуальная схема обработки трафика. Аналогичные схемы добавлены в соответствующие главы, рассматривающие конкретные функции (DNAT, Web Portal, Reverse Proxy и т.д.);
- **Removed!** Главы про обработку трафика DNAT и Proxy из этого раздела удалены. Данные главы скорректированы, актуализированы и перенесены в соответствующие разделы;
- **New!** Добавлена глава «Fast Path».

Политики сети / Обзор политик сети / Библиотеки элементов / Обзор раздела «Библиотек»

- Убраны «Профили АСУ ТП».

Политики сети / Обзор политик сети / Библиотеки элементов / Создание объектов библиотек в CLI

- Глава переименована в «Работа с библиотеками в CLI»;
- Исправлены команды по добавлению элементов в список на слайде и в учебнике. Использование символа «+» при добавлении более не является обязательным;
- Добавлен блок «Обратите внимание» с информацией о том, как использовался «+» в старых версиях;
- Добавлены команды по удалению отдельных элементов списка и просмотру элементов на слайд и в учебник.

Политики сети / Обзор политик сети / Библиотеки элементов / Динамические списки

- Добавлена информация в учебник и на слайд о том, что теперь кроме веб-сервера можно также использовать и FTP;
- В учебнике добавлен последний абзац, описывающий, как проверить наличие обновлений (системных и пользовательских списков) и инициировать их загрузку.

Политики сети / Политика межсетевого экрана / Работа с правилами политики МЭ / Импорт правил UPL

- Добавлена информация о том, что после импорта создаются правила с новыми ID и о связанных с этих последствий. Предпоследний абзац.

New! Политики сети / Политика межсетевого экрана / Работа с правилами политики МЭ / Рекомендации для оптимизации производительности

- Новая глава. Даны общие рекомендации по работе с правилами для оптимизации производительности МЭ.

Политики сети / NAT и PBR / Правила NAT

- **New!** Добавлена глава «Packet flow для DNAT и port forwarding» с описанием обработки пакета при использовании DNAT. Обратите внимание на то, что трафик DNAT теперь проверяется соответствующими правилами межсетевого экрана с включенными профилями COV и L7.

Политики сети / Балансировка нагрузки и управление пропускной способностью / Управление пропускной способностью / Настройка правил пропускной способности

- Исправлены опечатки;
- Удалена информация о возможности выбрать тип правила (шейпинг или полисинг) и заменен скриншот на слайде.

Политики безопасности / Обзор политик безопасности

- **New!** Добавлен новый подраздел «Обработка трафика при включенных функциях политики безопасности», в котором рассматриваются работа в режиме явного и прозрачного прокси и соответствующие packet flow.

Изменения в Lab Guide версия 2.1

Установка и базовая настройка / Описание стенда

- Заменена топология на актуальную;
- Незначительно отредактирован текст в описании головного офиса, убрано упоминание MC-A.

Установка и базовая настройка / Конфигурация и коммутация виртуальных машин

- Удален MC-A во всех таблицах;
- В таблице «Коммутация виртуальных машин» добавлены интерфейсы dumX на ISP1 и ISP2.

Цифровые сертификаты / Установка корневого сертификата корпоративного УЦ / Установка корневого сертификата в MGT-A

- Добавлены шаги с описанием процедуры очистки кэша Firefox.

Политики сети / Трансляция адресов / Настройка DNAT

- **Important!** В задании «Предварительная настройка интерфейсов» теперь адреса, под которыми публикуются ресурсы, назначаются в качестве виртуальных IP в кластер отказоустойчивости. Ранее адреса 203.0.113.51 и 198.51.100.51 назначались на физические интерфейсы port2 и port5 узлов кластера, что не является корректным.

Технологии предоставления удаленного доступа / Настройка IKEv2 VPN-туннеля сайт-сайт / Настройка VPN-сервера / Настройка публикации удостоверяющего центра для получения сертификатов клиентами / Настройка адресов на интерфейсах

- **Important!** Адреса для публикации по DNAT назначаются в виде виртуальных IP в кластер отказоустойчивости.

* с подробными изменениями в различных версиях курса можно ознакомиться в конце данной программы

Версия 2.2

Общие изменения

- Во вводную презентацию About добавлен слайд «Информационные ресурсы». Просьба обращать внимание слушателей на портал документации docs.usergate.com;
- Версия программного обеспечения, используемого в курсе, обновлена до 7.2;

Изменения в учебнике версия 2.2

Установка и базовая настройка / Обзор продуктов UserGate / Межсетевые экраны UserGate

- Добавлен слайд «Межсетевые экраны UserGate», описывающий классы межсетевых экранов. Это принятая стратегия компании по развитию направления «Межсетевые экраны»;
- В главу «Программно-аппаратные комплексы» добавлена информация о новых устройствах B50, D250, FG и ссылка на сайт с описанием моделей;

Изменения в Lab Guide версия 2.2

- **New!** В лабораторные работы добавлены блоки «Информация о задании», описывающие, что и для чего необходимо сделать.

Версия 2.3

Общие изменения

- Версия программного обеспечения, используемого в курсе, обновлена до 7.3;
- В курсе рассматривается не только NGFW, но и DCFW;
- Названия некоторых модулей и глав изменены, чтобы исключить термин NGFW, если рассматриваемый функционал общий для обоих классов МЭ (пример, глава по применению сертификатов), или, наоборот, включить, чтобы показать, что функционал реализован только на NGFW (пример, главы по SSL и SSH);
- В лабораторном стенде на UTM-B установлено ПО DCFW версии 8;
- Скриншоты в учебнике и лаб-гайде актуализированы.

Изменения в учебнике версия 2.3

Установка и базовая настройка / Обзор продуктов / Межсетевые экраны

- Незначительные правки заголовков и текста, в связи с тем, что в курсе рассматриваются NGFW и DCFW;
- Изменена графика на слайде «Межсетевые экраны». Выделены NGFW и DCFW, как продукты, рассматриваемые в курсе;
- Глава «Программно-аппаратные комплексы» актуализирована. Поправлены данные производительности для версии UGOS 7.X. Добавлена информация о новых ПАК;
- **New!** Добавлена глава «Соответствие требованиям регуляторов».

Установка и базовая настройка / Обзор продуктов / Экосистема UserGate SUMMA

- **New!** Добавлена глава по SIEM. Начиная с версии 7.3 является отдельным продуктом;
- **New!** Добавлена глава по WAF. Начиная с версии 7.3 является отдельным продуктом;
- Добавлены блоки «Ссылка» на документацию к продуктам;
- Изменена графика на слайде «Экосистема UserGate SUMMA».

Установка и базовая настройка / Интерфейсы администратора / Интерфейс командной строки / Конфигурационный режим

- Добавлено, что команда execute предназначена не только для выполнения команд режима диагностики, но и для выполнения ряда служебных команд.

Установка и базовая настройка / Лицензирование и обновления

- Раздел переименован в «Лицензирование и обновления»;
- **New!** Добавлена глава про базовую лицензию;
- **New!** Добавлена тема по работе с обновлениями (общее описание обновлений, обновление библиотек, обновление системы);

Установка и базовая настройка / Лицензирование и обновления / Процесс активации лицензии / Онлайн активация

- Добавлена информация на слайд и в учебник об активации в CLI.
- **New!** Добавлена информация об автоматической проверке лицензии;

* с подробными изменениями в различных версиях курса можно ознакомиться в конце данной программы

Установка и базовая настройка / Лицензирование / Процесс активации лицензии / Офлайн активация

- **New!** Добавлена информация о самостоятельной активации на специальном портале (портал работает в тестовом режиме);
- Изменена графика на слайде.

Установка и базовая настройка / Ролевая модель доступа / Настройка ролевой модели

- **New!** Добавлена глава по управлению сессиями администраторов (таймауты, просмотр и сброс сессий).

Кластеры / Кластер конфигурации / Свойства кластера конфигурации

- Добавлена информация о том, что UserID не является кластерной конфигурацией.

Сетевая конфигурация / Зоны и сетевые интерфейсы / Зоны / Защита от DoS-атак

- Добавлен блок «Обратите внимание», предупреждающий, что данный функционал реализован только на NGFW. Добавлено примечание на слайд.

Сетевая конфигурация / Маршрутизация / Статическая и динамическая маршрутизация

- Изменен слайд «Протокол OSPF», заменен скриншот в соответствии с интерфейсом 7.3, в тексте и на слайде упоминается редистрибуция с использованием routemaps;
- **New!** Добавлена глава «Редистрибуция маршрутов». Особое внимание обратите на возможности 7.3 по передаче маршрутов в OSPF с использованием routemaps.

Политики сети / Обзор политик сети / Библиотеки элементов / Обзор раздела библиотеки

- Описание разделов библиотек структурировано в соответствии с интерфейсом.
- **New!** Добавлена информация о новом разделе библиотек «Теги». Заменены графика и скриншот на слайде;
- **New!** Добавлена информация о новом разделе библиотек «Группы приложений». Используются только в правилах пропускной способности.

Политики сети / Обзор политик сети / Обработка трафика на NGFW

- Несколько изменены текст и графика на слайде. Цель – подсветить и постепенно подготовить слушателей, что компоненты политики безопасности это прокси, и затем показать отсутствие этих функций на DCFW.

Политики сети / Обзор политик сети / Обработка трафика на DCFW

- **New! Important!** Новый раздел. Дано описание преимуществ DCFW и процесса обработки трафика на устройствах класса UserGate DCFW.

Политики сети / NAT и PBR / Правила NAT / Packet Flow для DNAT и Port Forwarding

- Добавлен блок «Обратите внимание» об идентичности packet flow для DNAT на NGFW и DCFW за исключением определенных блоков.

* с подробными изменениями в различных версиях курса можно ознакомиться в конце данной программы

Политики сети / NAT и PBR / Правила NAT / Настройка правил SNAT

- **Important!** Добавлена информация о том, что в качестве условий правил SNAT могут выступать пользователи / группы (версия 7.3);
- Изменена графика на слайде.

Идентификация пользователей / Компоненты идентификации / Способы идентификации / Методы сброса идентификации

- Скорректирована команда на слайде и в учебнике "execute termination user-sessions";

Идентификация пользователей / Технология UserID / Настройка UserID

- Поправлена терминология «аутентификация/авторизация» во всем модуле;
- **New!** Глава «Алгоритм настройки UserID». Поменялся подход и интерфейс. Коннекторы UserID – набор параметров для коммуникации с источником данных, агент UserID – получатель и обработчик данных. В соответствии с этим изменен слайд и подредактирован текст;
- **Important!** Следующие главы соответствующим образом исправлены, заменены скриншоты на слайдах;
- Два слайда про журналы заменены одним, переработанным;
- **New!** Новая глава, описывающая работу UserID в кластере.

Технологии предоставления удаленного доступа – 1 / Обзор технологий / VPN-туннели / Типы VPN

- В описании SSL VPN или веб-портала добавлена ремарка о возможности настройки только на NGFW.

Технологии предоставления удаленного доступа – 1 / Способы публикации ресурсов / Reverse-прокси

- Добавлен блок «Обратите внимание» с информированием о том, что функционал поддерживается только на NGFW. Поправлен слайд.

Технологии предоставления удаленного доступа – 1 / Способы публикации ресурсов / Веб-портал

- Добавлен блок «Обратите внимание» с информированием о том, что функционал поддерживается только на NGFW. Поправлен слайд.

Технологии предоставления удаленного доступа – 1 / Способы публикации ресурсов / Сравнение способов публикации ресурсов

- В таблицу добавлен столбец с указанием, где (NGFW или DCFW) реализован указанный способ.

Технологии предоставления удаленного доступа – 2 / Веб-портал / Настройка веб-портала / Веб-портал

- Добавлен блок «Обратите внимание» с информированием о том, что функционал поддерживается только на NGFW.

Технологии предоставления удаленного доступа – 2 / Reverse-прокси / Настройка reverse-прокси / Обзор reverse-прокси

- Добавлен блок «Обратите внимание» с информированием о том, что функционал поддерживается только на NGFW.

Политики безопасности / Обзор политик безопасности / Компоненты политики безопасности / Обзор компонентов

- Измена графика на слайде и текст главы, чтобы показать какие компоненты политик безопасности реализованы на NGFW (все) и на DCFW (только COB).

Политики безопасности / Настройка политик безопасности / Система обнаружения вторжений / Алгоритм настройки COB

- Немного подредактирован текст и изменена графика на слайде в соответствии с новой логикой и интерфейсом.

Политики безопасности / Настройка политик безопасности / Система обнаружения вторжений / Профили COB

- Отредактирован тест – описана возможность изменения поведения сигнатур с помощью редактирования свойств фильтра и возможность редактировать отдельные сигнатуры внутри фильтра.

Политики безопасности / Настройка политик безопасности / Система обнаружения вторжений / Логика обработки сигнатур в профиле COB

- **New!** Дано описание логики работы фильтров (свойства сигнатур и свойства фильтров).

Мониторинг, поиск и устранение неисправностей / Средства диагностики и мониторинга / Мониторинг и диагностика / Диагностика и мониторинг

- Добавлена информация о новом разделе Диагностика Мониторинг – Мониторинг – Заблокированные COB/L7 IP-адреса. Заменен скриншот на слайде.

Мониторинг, поиск и устранение неисправностей / Тех. поддержка и устранение неисправностей / Работа со службой технической поддержки

- Немного отредактирован текст и изменена графика на слайде «Планы технической поддержки»;
- **New!** Добавлена глава «Разрешительная документация на деятельность», к которой описаны документы, лицензирующие деятельность сервисных подразделений UserGate.

Изменения в Lab Guide версия 2.3

Установка и базовая настройка / Знакомство со стендом / Описание стенда

- В топологии и далее в тексте филиал переименован в "Branch Datacenter", «дата-центр филиала» и т.д.

* с подробными изменениями в различных версиях курса можно ознакомиться в конце данной программы

Установка и базовая настройка / Базовая конфигурация / Настройка базовых параметров и активация лицензии / Активация лицензии и проверка / Активация и просмотр лицензии

- Добавлена сноска о появлении окна для просмотра обновлений библиотек.

Установка и базовая настройка / Настройка DCFW в филиале

- Вместо NGFW в филиале настраивается DCFW. Процедура идентична NGFW.

Сетевая конфигурация / Маршрутизация / Статическая и динамическая маршрутизация / Настройка протокола OSPF

- Отредактирован текст и заменены скриншоты по причине выноса редистрибуции на отдельную вкладку.

Политики сети / Работа с библиотеками / Создание объектов в GUI и CLI / Создание объектов в GUI

- **New!** Добавлено задание «Создание и применение тегов».
- **Important!** В последующих лабораторных работах созданные теги назначаются на правила межсетевого экрана, интерфейсы и т.д. Соответствующим образом отредактирован текст и скриншоты.

Политики сети / Работа с библиотеками / Вложенные и динамические списки / Динамические списки / Обновление списка

- **New!** Добавлено опциональное задание с ручным обновлением списка через «Центр обновлений». Позволяет слушателям в том числе ознакомиться с тем, как происходит обновление системных библиотек.

Политики сети / Работа с правилами межсетевого экрана / Работа с правилами в GUI / Редактирование правил

- **New!** Добавлены несколько пунктов и по групповому назначению тегов.

Политики сети / Работа с правилами межсетевого экрана / Язык UPL / Импорт правил UPL

- **New!** Добавлено задание по восстановлению тегов после импорта. Теги не передаются экспортом. Так как импорт перезаписывает текущую политику, то теги надо восстановить. Задание опциональное.

Идентификация пользователей / Технология UserID

- Текст лабораторной работы и скриншоты скорректированы в соответствии с интерфейсом 7.3.

Идентификация пользователей / Технология UserID / Настройка UserID / Настройка агента UserID / Создание коннектора

- Добавлен блок «Обратите внимание» о том, что агенты не являются кластерными и создаются на том узле, к которому подключен администратор.

Идентификация пользователей / Технология UserID / Проверка конфигурации и использование пользователей и групп в правилах

- **New!** Добавлено задание по проверке в CLI.

Политики безопасности / СО

New! Important! Переделана лабораторная работ

