UserGate

Администрирование межсетевых экранов UserGate 7

Программа курса

О курсе

Код курса
UG.NGFW7 (UGOS7)

Версия курса
2.2

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.

* с изменения в курсе UGOS 7 можете ознакомится в конце данной программы

Программа курса

1

Установка и базовая настройка

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.

* с изменения в курсе UGOS 7 можете ознакомится в конце данной программы

2

Кластеры

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.

* с изменения в курсе UGOS 7 можете ознакомится в конце данной программы

3

Сетевая конфигурация

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.

* с изменения в курсе UGOS 7 можете ознакомится в конце данной программы

4

Политики сети

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.

* с изменения в курсе UGOS 7 можете ознакомится в конце данной программы

5

Сертификаты и инспектирование SSL

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.

* с изменения в курсе UGOS 7 можете ознакомится в конце данной программы

6

Идентификация пользователей

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.

* с изменения в курсе UGOS 7 можете ознакомится в конце данной программы

7

Политика безопасности

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.

* с изменения в курсе UGOS 7 можете ознакомится в конце данной программы

8

Технологии предоставления удаленного доступа - I

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.

* с изменения в курсе UGOS 7 можете ознакомится в конце данной программы

9

Технологии предоставления удаленного доступа - II

Веб-портал

- настройка веб-портала.

Reverse-прокси

- настройка reverse-прокси.

Лабораторная работа 8.1. «Технологии предоставления удаленного доступа»

- веб-портал;
- Reverse-прокси.

* с изменения в курсе UGOS 7 можете ознакомится в конце данной программы

10

Мониторинг, поиск и устранение неисправностей

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.

* с изменения в курсе UGOS 7 можете ознакомится в конце данной программы

Изменения в курсе UGOS 7

Версия 2.0

New! В лабораторном стенде используется версия UGOS 7.1.1. Обновлены 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 слад;

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»;

* с изменения в курсе UGOS 7 можете ознакомится в конце данной программы

- 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. Обновлены 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.

* с изменения в курсе UGOS 7 можете ознакомится в конце данной программы

- 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 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.

* с изменения в курсе UGOS 7 можете ознакомится в конце данной программы

- 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.

* с изменения в курсе UGOS 7 можете ознакомится в конце данной программы

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.

* с изменения в курсе UGOS 7 можете ознакомится в конце данной программы

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;

* с изменения в курсе UGOS 7 можете ознакомится в конце данной программы

- 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 СОВ 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

* с изменения в курсе UGOS 7 можете ознакомится в конце данной программы

- 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 изменения в курсе UGOS 7 можете ознакомится в конце данной программы

Версия 2.2

Общие изменения

- Версия программного обеспечения, используемого в курсе, обновлена до 7.2;

* с изменения в курсе UGOS 7 можете ознакомится в конце данной программы

UserGate

www.usergate.ru | academy@usergate.ru