

Table of Contents

Table of Contents	1
Безопасность сети и защита от сетевых угроз	2
Межсетевое экранирование	3
Обнаружение и предотвращение вторжений	4
Защита от DOS-атак и сетевого флуда	5
Антивирусная проверка трафика	6
Проверка почтового трафика	7
Работа с внешними системами безопасности	8
Управление АСУ ТП	9
Настройка политик безопасности при помощи сценариев	10

Межсетевое экранирование

Documentation: 

Version: 5.x, 6.1.9, 7.x, 7.0.1

Product: NGFW

Межсетевой экран нового поколения UserGate NGFW фильтрует трафик, проходящий через определенные протоколы (например, TCP, UDP, IP), тем самым обеспечивая защиту сети от хакерских атак и разнообразных типов вторжений, основанных на использовании данных протоколов.

Обнаружение и предотвращение вторжений

Version: 7.0.1, 6.1.9, 5.x

Documentation: 

Система обнаружения и предотвращения вторжений (СОВ) позволяет распознавать вредоносную активность внутри сети. Основной задачей системы является обнаружение, протоколирование и предотвращение угроз в режиме реального времени, а также предоставление отчетов.

Администратор может создавать различные СОВ-профили (наборы сигнатур, релевантных для защиты определенных сервисов) и задавать правила СОВ, определяющие действия для выбранного типа трафика, который будет проверяться модулем СОВ в соответствии с назначенными профилями.

Защита от DOS-атак и сетевого флуда

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: 

NGFW позволяет задать параметры защиты каждой зоны сети от сетевого флуда (для протоколов TCP (SYN-flood), UDP, ICMP), указав порог уведомления - количество запросов с одного IP-адреса, после которого происходит запись в журнал - и порог отбрасывания пакетов - количество запросов, после которого пакеты отбрасываются с соответствующей записью в журнале.

Возможно настроить исключения, например, для зон, использующих IP-телефонию и поэтому отправляющих большое количество UDP-пакетов.

Антивирусная проверка трафика

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: 

Потоковый антивирус UserGate позволяет обеспечить антивирусную проверку трафика без ущерба для производительности и быстродействия сети. Модуль использует обширную базу сигнатур.

Проверка почтового трафика

Documentation: 

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

NGFW способен обрабатывать транзитный почтовый трафик (SMTP(S), POP3(S)), анализируя его источник, а также содержание письма и вложений, что гарантирует надежную защиту от спама, pharming- и phishing- атак. NGFW также предоставляет возможность гибкой настройки фильтрации почтового трафика по группам пользователей.

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: ☒

Имеется возможность передавать HTTP/HTTPS и почтовый трафик (SMTP, POP3) на внешние серверы ICAP, например, для антивирусной проверки или для проверки передаваемых пользователями данных DLP-системами. Администратор может указать, какой трафик требуется передавать на ICAP, а также настроить работу с фермами серверов.

Version: 5.x, 6.1.9, 7.0.1

Product: NGFW

Documentation: 

В новой версии платформы появилась возможность настройки автоматизированной системы управления технологическим производством (АСУ ТП) и управления ей. Администратор может контролировать трафик, настроив правила обнаружения, блокировки и журналирования событий. Это позволяет автоматизировать основные операции технологического процесса, сохраняя при этом возможность контроля и вмешательства человека при необходимости.

Настройка политик безопасности при помощи сценариев

Version: 5.x, 6.1.9, 7.0.1, 7.1.0

Product: NGFW

Documentation: 

NGFW позволяет существенно сократить время между обнаружением атаки и реакцией на нее благодаря автоматизации безопасности при помощи механизма сценариев (SOAR — Security Orchestration, Automation and Response).

Эта концепция находится на пике популярности и позволяет администратору создавать сценарии (запускаемые по плану или при обнаружении атаки), где прописываются автоматические действия в ответ на те или иные события. Такой подход обеспечивает гибкую настройку политик безопасности, сокращает участие человека благодаря автоматизации повторяющихся задач, а также дает возможность приоритезировать сценарии для скорейшей реакции на критичные угрозы.

