Бизнес и госсектор в безопасности: релиз Ideco NGFW 17

Максим Панин

Presale-инженер Ideco

О компании

ideco

Ideco – российский разработчик решений для ИБ.

+ Оптимизируем время настройки
+ Защищаем от кибератак
+ Экспертная ТП

2005 год

3 мажорных релиза в год

200 человек

5500 компаний

А что случилось?

- После того, как зарубежные производители ИТ/ИБ-решений покинули российский рынок, большая часть компаний была вынуждена переходить на аналогичные отечественные системы. Особенно остро встал вопрос замены NGFW-решений, процесс продолжается.

- В связи с этим заказчики столкнулись с большим количеством проблем, т.к. рынок российских решений, по их мнению, оказался не готов заменить зарубежные функционально, а также оказался и под давлением государственных регуляторов.

ideco

Свежие уязвимости в западных решениях или почему в современных реалиях импортозамещение – это важно

Критическая уязвимость в Juniper Networks

CVE-2024-21591

Об уязвимости:

- Уязвимость систем Juniper Networks Junos OS на устройствах серий SRX и EX позволяет злоумышленнику, не прошедшему проверку подлинности, вызывать отказ
  в обслуживании или совершать удаленное выполнение кода с root-привилегиями.

Исправление:

- Рекомендуется скорейшее обновление.

Оценка уязвимости по шкале CVSS 3.1 – 9.8 баллов.

Уязвимости в продуктах Cisco

CVE-2024-20253

Об уязвимости:

- Уязвимость в продуктах Cisco Unified Communications Manager и Contact Center Solutions позволяет злоумышленнику, не прошедшему проверку подлинности, выполнять произвольный код на устройстве, а также получить root-доступ.

Исправление:

- Рекомендуется скорейшее обновление.

Оценка уязвимости по шкале CVSS 3.1 – 9.9 балла.

Уязвимости в продуктах Cisco

CVE-2024-20272

Об уязвимости:

- Уязвимость в веб-интерфейсе управления Cisco Unity Connection, которая позволяет злоумышленнику, не прошедшему проверку подлинности, загружать произвольные файлы и выполнять команды в базовой операционной системе, а также повысить привилегии до root-пользователя.

Исправление:

- Рекомендуется скорейшее обновление.

Оценка уязвимости по шкале CVSS 3.1 – 7.3 балла.

Уязвимости в продуктах Cisco

CVE-2024-20320

Об уязвимости:

- В Cisco IOS XR Software обнаружена уязвимость, связанная с повышением привилегий в системе, возникающая при отправке специально созданных команд SSH в CLI. Затронуты маршрутизаторы серии 8000 и система NCS серий 540 и 5700.

Исправление:

- Рекомендуется скорейшее обновление.

Оценка уязвимости по шкале CVSS 3.1 – 7.8 балла.

Уязвимости в продуктах Cisco

CVE-2024-20327

Об уязвимости:

- В Cisco IOS XR Software обнаружена уязвимость, связанная с воздействием на функцию завершения PPP через Ethernet (PPPoE). Затронуты маршрутизаторы серии ASR 9000. Приводит к отказу в обслуживании.

Исправление:

- Рекомендуется скорейшее обновление.

Оценка уязвимости по шкале CVSS 3.1 – 7.4 балла.

Уязвимости в продуктах Cisco

CVE-2024-20318

Об уязвимости:

- В Cisco IOS XR Software обнаружена уязвимость, связанная с некорректной обработкой определенных кадров Ethernet, принимаемых на линейных картах. Приводит к отказу в обслуживании.

Исправление:

- Рекомендуется скорейшее обновление.

Оценка уязвимости по шкале CVSS 3.1 – 7.4 балла.

Уязвимость в Palo Alto

CVE-2024-3400

Об уязвимости:

- Уязвимость затрагивает функцию GlobalProtect в нескольких последних версиях PAN-OS и позволяет злоумышленнику, не прошедшему проверку подлинности, выполнить произвольный код с правами root на брандмауэре.

Исправление:

- Рекомендуется скорейшее обновление.

Оценка уязвимости по шкале CVSS 3.1 – 10.0 баллов.

Уязвимость в Fortinet FortiClient EMS

CVE-2023-48788

Об уязвимости:

- Некорректная нейтрализация специальных элементов, используемых в команде sql («sql-инъекция») в Fortinet FortiClientEMS, которая позволяет злоумышленнику выполнять несанкционированный код или команды через специально созданные пакеты.

Исправление:

- Рекомендуется скорейшее обновление.

Оценка уязвимости по шкале CVSS 3.1 – 9.8 баллов.

Сертификация.
Или почему этого не произойдет с вами

Соответствие требованиям регулятора

Сертификат ФСТЭК №4503 от 28.12.2021 г.

- Требования доверия (4)
- Требования к МЭ
- Требования к СОВ
- Профиль защиты МЭ

(А четвертого класса защиты. ИТ.МЭ.А4.ПЗ)

- Профиль защиты МЭ

(Б четвертого класса защиты. ИТ.МЭ.Б4.ПЗ)

- Профили защиты СОВ

(четвертого класса защиты. ИТ.СОВ.С4.ПЗ)

- Работаем над получением сертификата ФСБ
- ГОСТ VPN уже при помощи интеграции с модулей Dcrypt Smart SFP от ТСС
- Проходит сертификацию версия Ideco UTM 16
- Ведем работы по сертификации VPP и на требования для NGFW

Решение входит в реестр российского ПО Минцифры РФ

Переход с конкурентных решений

- Библиотека скриптов для переноса объектов и правил
- Под каждого клиента можем дорабатывать скрипты
- Бесплатный перенос в рамках пилотного проекта
- Удобен как для самостоятельного внедрения, так и при помощи партнёра

Функциональность.
Что важно для вас?

Результаты исследований

Необходимая функциональность

- Контроль приложений
- Контроль пользователей
- IPS
- NAT
- Зоны интерфейсов
- L3, статическая маршрутизация, динамическая маршрутизация
- Отказоустойчивый кластер
- URL-фильтрация
- Потоковый антивирус
- TLS-инспекция
- L2, поддержка VLAN, прозрачный режим
- VRF, виртуальные контексты
- VPN (в т.ч. ГОСТ)
- Контроль состояния оборудования (SNMP и пр.)
- Интеграция с SOC
- Балансировка нагрузки

Чем недовольны?

По результатам опросов заказчики, использующие отечественные NGFW-решения в большей степени:

- Отмечают низкую производительность
- Не удовлетворены качеством обнаружения сетевых угроз
- Недовольны количеством поддерживаемых режимов работы и протоколов маршрутизации
- Отмечают сложности при настройке

Какие задачи решает Ideco NGFW

- Фильтрация трафика
- Учёт и авторизация пользователей
- Организация удалённого доступа
- Отчётность и мониторинг
- Соблюдение требований регулятора
- Централизованное управление
- Отказоустойчивость
- Миграция с зарубежных решений

Презентация продукта

RoadMap 2024

- SSL VPN
- ГОСТ VPN
- Расширение настроек IDS/IPS
- Клиенты для всех операционных систем
- Синхронизация сессий в кластере, кластер Active-Active
- Расширенные возможности Центральной Консоли
- Группировка правил, улучшение взаимодействия администратора с интерфейсом создания политик
- Улучшение ролевых моделей администрирования, rollback
- L2 Bridge
- Расширение сетевой функциональности
  - Улучшение VCE
  - Улучшение динамической маршрутизации
  - SPAN
  - NetFlow

Ideco NGFW VPP

Ideco NGFW VPP — это высокоскоростной межсетевой экран следующего поколения на технологиях DPDK/VPP для защиты сетевого периметра, который позволяет построить современную систему защиты корпоративной сети и сделать доступ в интернет абсолютно управляемым.

Возможности:

- Межсетевой экран
- Система предотвращения вторжений
- Контроль приложений.

Какие задачи решает Ideco NGFW VPP:

- управление и фильтрация трафика (в т.ч. и контентной) на границе внешней и внутренней сетей
- контроль приложений
- защита корпоративной сети от несанкционированного доступа
- поиск и предотвращение вторжений и вредоносного трафика.

IDECO NGFW VPP имеет высокую производительность межсетевого экранирования и системы обнаружения вторжений.

Тестирование

1. Зарегистрироваться на my.ideco.ru
2. Скачать Ideco NGFW
3. Установить Ideco NGFW

- 40 дней тестовая лицензия
- помощь в тестировании
- обратная связь

ideco

СОЗДАЕМ ВМЕСТЕ

t.me/idecoutm - группа
t.me/ideco - канал
my.ideco.ru - скачать