КОД безопасности

Secret Net LSP\For Linux

Сертифицированное средство защиты от несанкционированного доступа для ОС семейства GNU/Linux

Secret Net LSP позволяет построить систему защиты от внутренних угроз и защитить конфиденциальную информацию и персональные данные на рабочих станциях и серверах под управлением ОС Linux.

Сертификаты

ФСТЭК России

5-й класс защищенности СВТ
4-й класс защиты МЭ типа «В»
4-й уровень доверия
4-й класс защиты СКН

Сравнение SNS для Windows и SNS для Linux

		Secret Net Studio для Windows	Secret Net Studio для Linux
Механизмы защиты	Дискреционное управление доступом	✓	✓
	Мандатное управление доступом	✓	—
	Контроль входа пользователей	✓	✓
	Контроль устройств	✓	✓
	Контроль печати	✓	—
	Замкнутая программная среда	✓	✓
	Контроль целостности	✓	✓
	Затирание остаточной информации	✓	✓
	Теневое копирование данных	✓	—
	Межсетевой экран уровня узла	✓	✓
	Полнодисковое шифрование	✓	—
	Шифрование контейнеров	✓	—
	Средство обнаружения вторжений	✓	*
	Антивирус	✓	*
Управление и мониторинг	Регистрация событий безопасности	✓	✓
	Аудит действий пользователей	✓	✓
	Централизованное управление	Через СБ SNS (Windows)/ Security Code Orchestrator (с 8.11)	Через Security Code Orchestrator/СБ SNS (Windows)
	Интеграция с МДЗ «Соболь»	✓	✓

* - будет доступно в следующей версии

Лицензирование

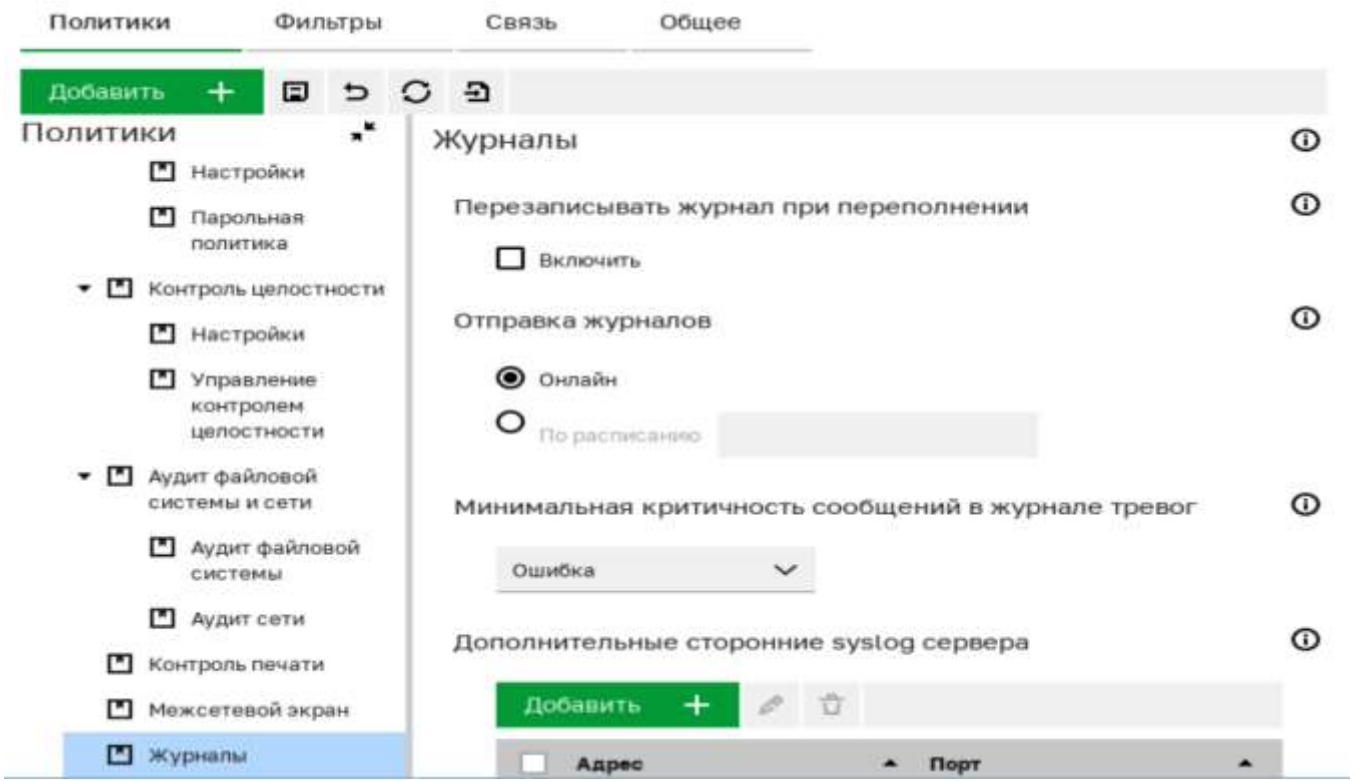
- Лицензируются только защитные компоненты по количеству компьютеров.
- Срочные и бессрочные лицензии
- Нет дополнительных лицензий на сервер безопасности, терминальные подключения, централизованное управление и управление лицензиями.

КОД безопасности

Оркестратор

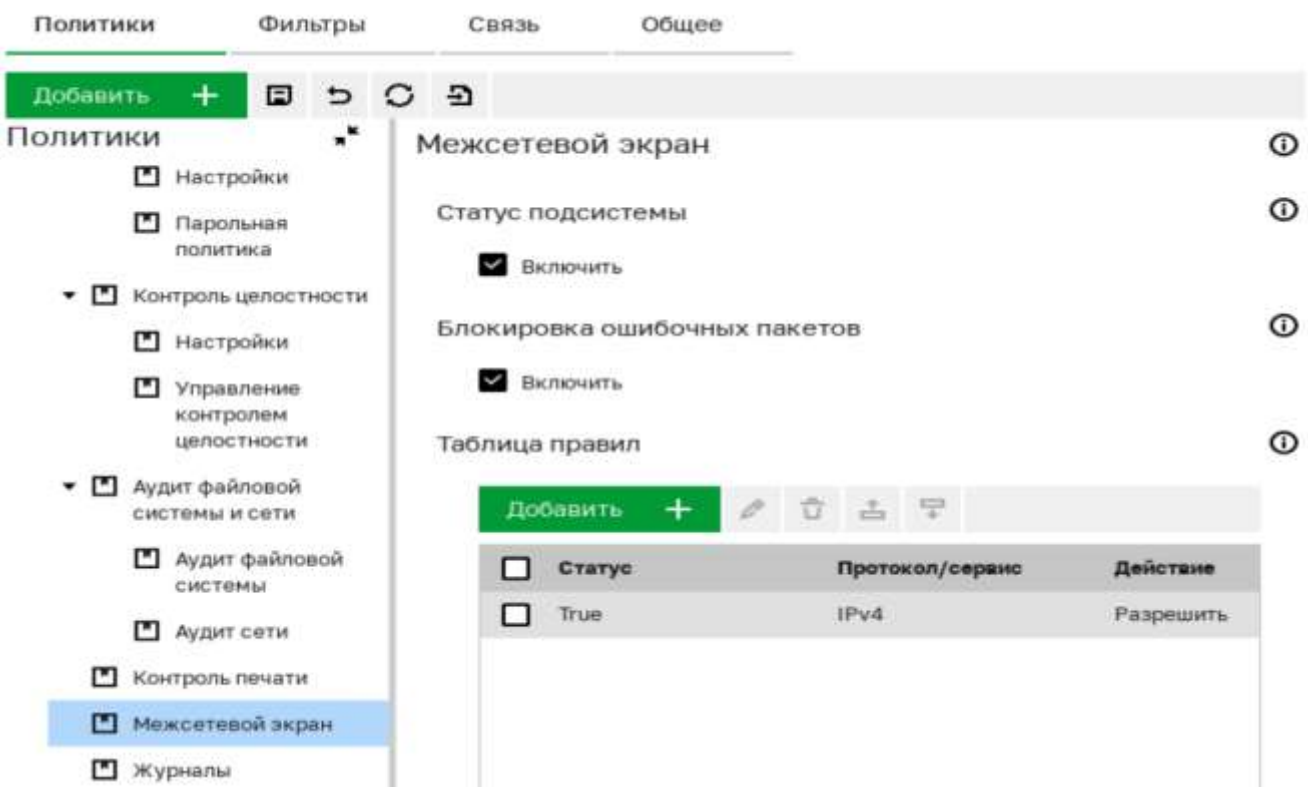
КОД безопасности

Политики ИБ



КОД безопасности

Политики ИБ



КОД безопасности

«Соболь»

Сертифицированный аппаратно-программный модуль доверенной загрузки (АПМДЗ)

Сертификаты

ФСТЭК России
УД 2, СДЗ.ПР2, АС до 1Б включительно (гостайна с грифом «совершенно секретно»), ИСПДн до УЗ1, ГИС до К1 и АСУ ТП до К1 включительно.

ФСБ России
АПМДЗ класса 3Б, АПМДЗ класса 1Б, может использоваться для защиты информации, содержащей сведения, составляющие государственную тайну.

Минобороны России
НДВ 2, СДЗ.ПР2, АС до 1Б включительно (гостайна с грифом «совершенно секретно»).

КОД безопасности

Модельный ряд

Платы на старых чипах (2014 год):

PCI Express

Mini PCI-E Half

M.2 A-E

Платы на новых чипах (2022 год):

PCI Express

M.2 A-E

КОД безопасности

Континент 4

Многофункциональный межсетевой экран (NGFW/UTM) с поддержкой алгоритмов ГОСТ

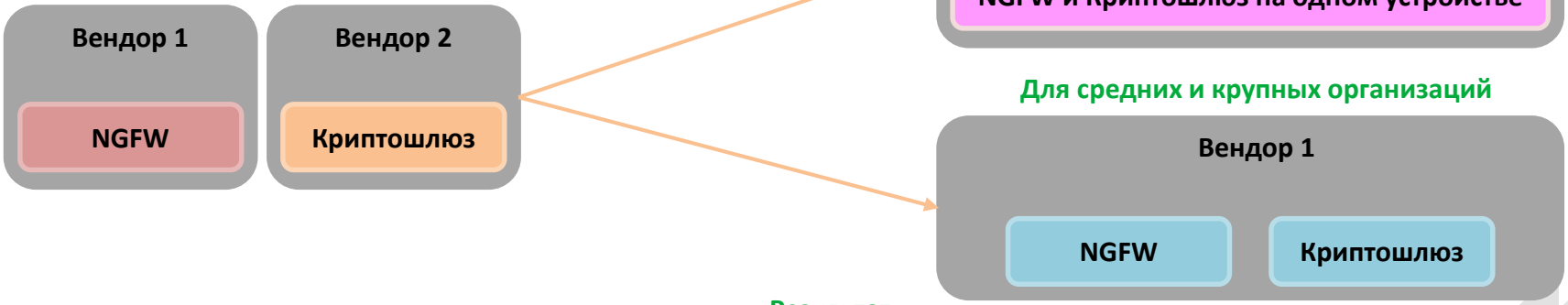
Сертификаты

ФСТЭК:
4-й класс защиты МЭ типа «А»
4-й класс защиты МЭ типа «Б»
4-й класс защиты СОВ уровня сети
4-й уровень доверия

Минпромторг
Статус телекоммуникационного оборудования российского производства

Проблемы и решение

Континент 4.2 – NGFW и Криптошлюз на одном устройстве



Проблемы:

1. Устройства со своей спецификой
2. Дополнительные точки отказа (технические и административные)

Результат:

1. Единая программа управления
2. Единая экспертиза
3. Гибкость замещения устройств

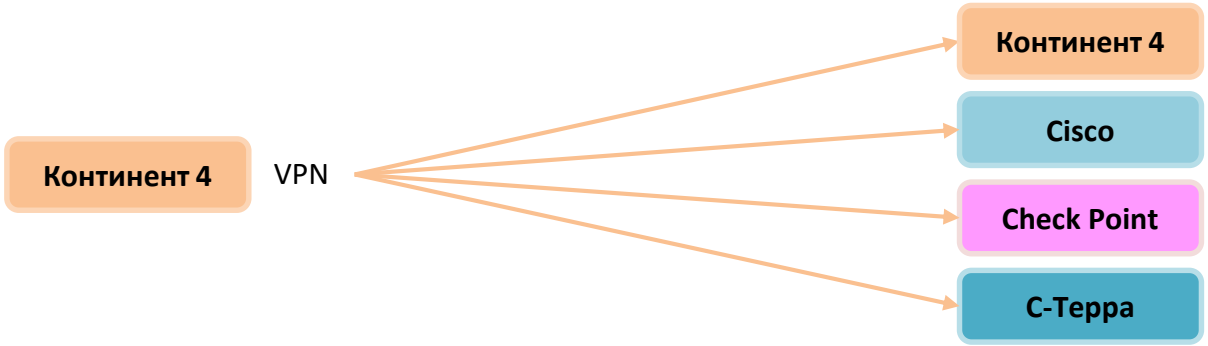
VPN в Континент 4.2

Что было ДО:

- Проприетарный протокол для организации Site-to-Site VPN
  (ограничения на построение VPN с другими сетевыми устройствами, кроме Континент 4)

Что стало ПОСЛЕ:

- Проприетарный протокол
- IPSec ГОСТ
- IPSec AES
- Сертификация по требованиям ФСБ России



Основа КиберАльянса - API

Экспорт конфигурации всех или выбранных Континент 4 под управлением отдельного ЦУС через API	▪ Политика безопасности и журналирование ▪ Настройки времени ▪ Сетевые функции
Миграции со сторонних NGFW (UserGate, FortiGate, Check Point, Palo Alto, Cisco)	▪ Правила фильтрации и трансляции ▪ Связанные с правилами сетевые объекты и группы ▪ Связанные с правилами сервисы и группы
Импорт индикаторов компрометации (IoC) в Континент 4	▪ IP-адреса вредоносных ресурсов ▪ FQDN вредоносных ресурсов ▪ URL-адреса вредоносных сайтов ▪ Hash ВПО
Создание политик безопасности	▪ Из SOAR-систем ▪ Из систем управления политиками безопасности

КОД безопасности

Мы рассказываем о наших проектах

«Код Безопасности» и «ТС Солюшен» осуществили миграцию с Check Point на Континент 4 на предприятии в отрасли машиностроения

24 января 2024

Перед специалистами «ТС Солюшен» стояла задача импортозамещения межсетевого экрана (МСЭ) на периметре организации. Ранее Заказчик использовал МСЭ Check Point.

Читать полностью

«Код Безопасности» и «Астрал. Безопасность» осуществили миграцию с Cisco на Континент 4 на предприятии в отрасли строительства.

22 декабря 2023

Команда «Код Безопасности» и «Астрал.Безопасность» провели модернизацию сетевой инфраструктуры предприятия в отрасли строительства.

Читать полностью

«Код Безопасности» и «Кросс технолоджис» осуществили миграцию с Palo Alto на Континент 4 на предприятии в отрасли энергетики

16 ноября 2023

Наши коллеги из «Кросс технолоджис» провели модернизацию сетевой инфраструктуры предприятия в отрасли энергетики.

Читать полностью

КОД безопасности

Новые платформы Континент 4

Платформа	Производительность	Версия
	МЭ: 100 Гбит/сек Режим IPS: 15 Гбит/сек Режим NGFW: 15 Гбит/сек	Континент 4.2
	Real-world mix МЭ: 200 Гбит/сек Режим IPS: 40 Гбит/сек Режим NGFW: 25 Гбит/сек	Континент 4.3
	Real-world mix МЭ: 600 Гбит/сек Режим IPS: 200 Гбит/сек Режим NGFW: 100 Гбит/сек	Континент 4.3

КОД безопасности

Континент ZTN клиент

Клиентское приложение для защищенного доступа в корпоративную сеть с удаленных персональных компьютеров и смартфонов сотрудников

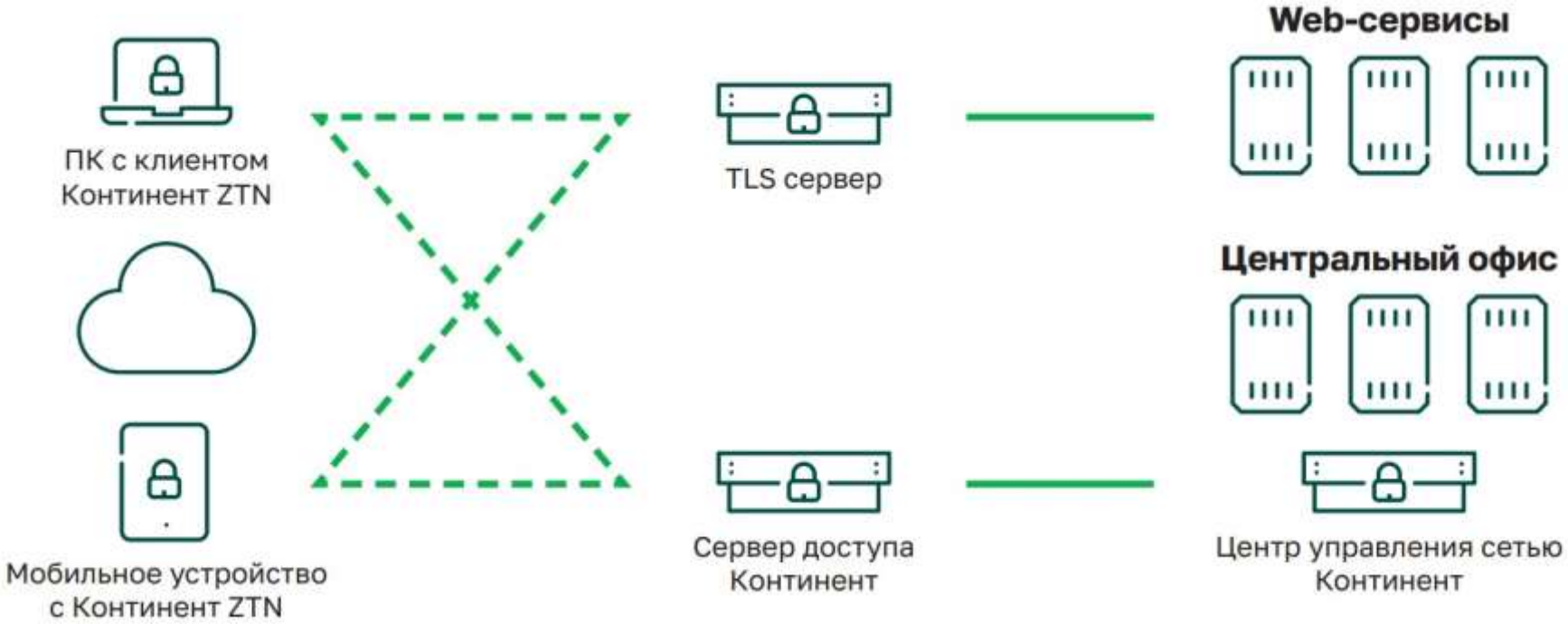
Планы по сертификации

ФСБ России
Континент ZTN Клиент для Windows – СКЗИ класса КС1/КС2/КС3
Континент ZTN Клиент для Linux – СКЗИ класса КС1/КС2/КС3
Континент ZTN Клиент для Аврора – СКЗИ класса КС1
Континент ZTN Клиент для Android – СКЗИ класса КС1

КОД безопасности

Континент ZTN-клиент

Архитектура



КОД безопасности

КиберАльянс

Многофакторная аутентификация

MULTIFACTOR Avanpost КОМПАНИЯ ИНДИД Аладдин

Удаленный доступ

iOS MacOS

Комплаенс-контроль

Континент ZTN клиент

Сакура

Микросегментация

vGate

Планируются в ближайшее время

Анализ правил

EFROS Нетхаб SPACE-BIT

Балансировка нагрузки

ЦИФРОВЫЕ РЕШЕНИЯ

Песочницы

positive technologies AVSOFT kaspersky

Индикаторы компрометации

kaspersky Security Vision CyberThreatTech R-Vision BI.ZONE

КОД безопасности

vGate

Средство защиты жизненного цикла
виртуальных машин и микросегментации сетей

Решение для контроля виртуальной инфраструктуры, действий администраторов и фильтрации сетевого трафика на уровне гипервизора.

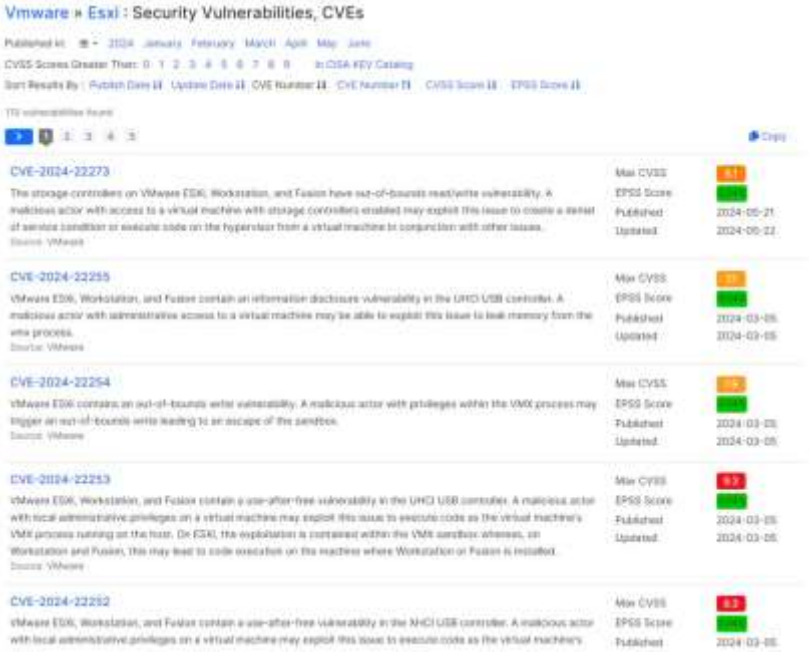
Сертификаты

ФСТЭК России
СВТ5/ УД4/ МЭ Б4

Может использоваться для защиты:
ГИС до К1 включительно
ИСПДн до УЗ1 включительно
АС до 1Г включительно
ЗОКИИ до К1 включительно
АСУ ТП до К1 включительно

КОД безопасности

Обзор уязвимостей VMware



vmware

Наименование	CVSS
CVE-2022-22972	9,8
CVE-2022-22973	7,8
CVE-2023-34048	9,8
CVE-2023-20867	3,9
CVE-2024-22252	9,3
CVE-2024-22253	9,3
CVE-2024-22255	7,1

КОД безопасности

Основные направления развития средств защиты виртуализации

Контроль жизненного цикла ВМ

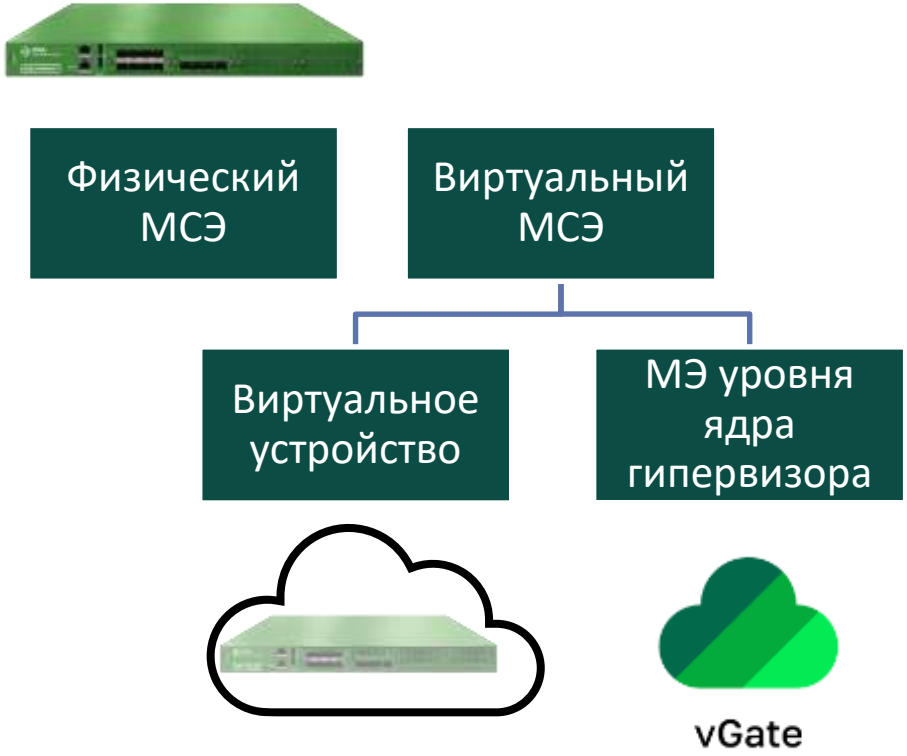
- Контроль потенциально фатальных действий админа
- Аудит
- Контроль целостности ВМ

Виртуализация сети

- Микросегментация
- Обеспечение сетевой связности

Щелчок Таноса для оператора связи

Различные варианты межсетевых экранов для задачи



Выделяют три варианта использования МСЭ/NGFW в ЦОД

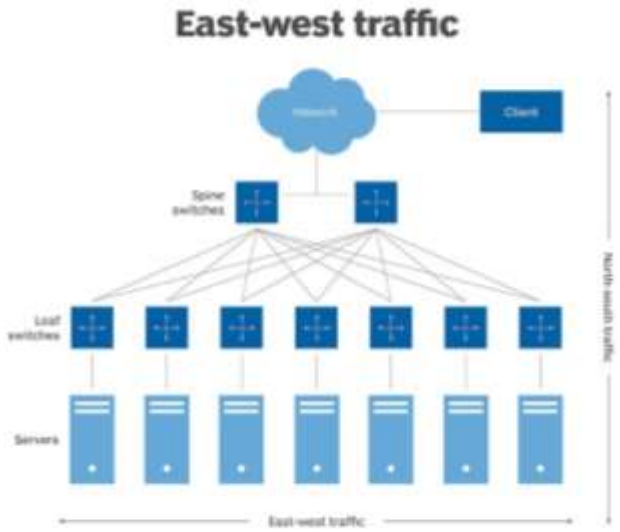
1.Физический межсетевой экран

2.Виртуальный межсетевой экран уровня сети

3.Виртуальный межсетевой экран уровня гипервизора

КОД безопасности

Контроль трафика

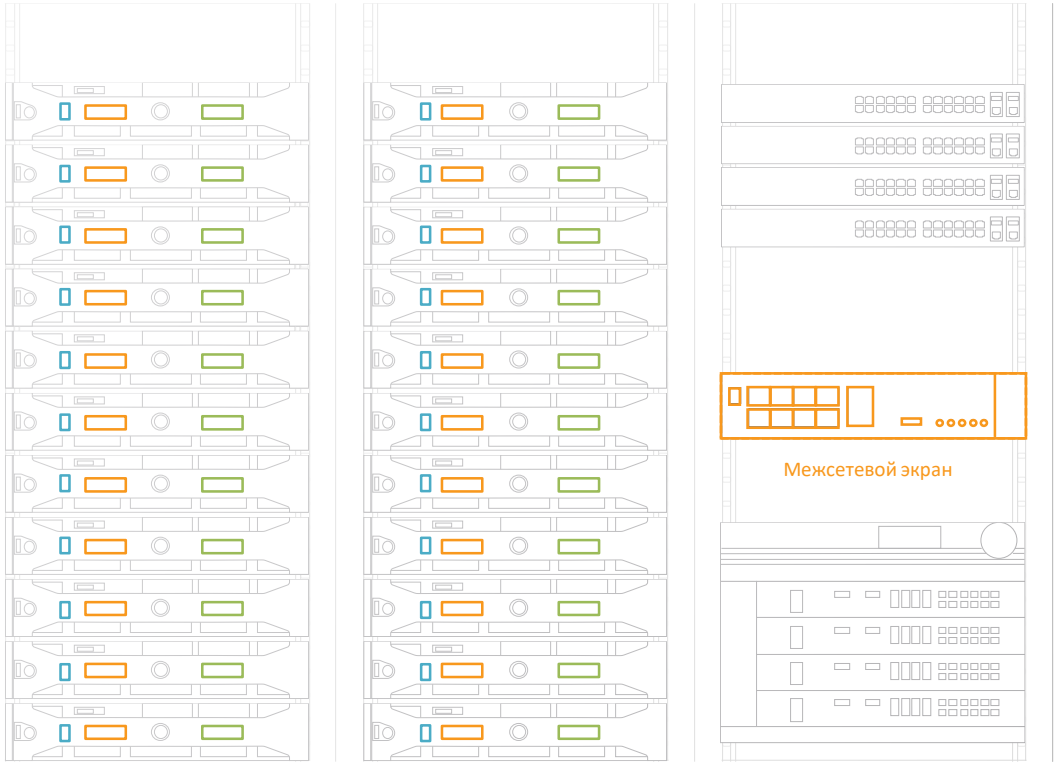


В ЦОД обрабатываются большие объемы трафика и нужна соответствующая пропускная способность МСЭ/NGFW.
К тому же необходимо фильтровать трафик как для выхода виртуальных машин в Интернет (паттерн север-юг), так и трафик между виртуальными машинами (паттерн запад-восток)

КОД безопасности

Сегментирование

Межсетевой экран в рамках vGate



Преимущества

- Встроен в гипервизор
- Распределенная scale-out архитектура без ограничений по производительности
- Гиперконвергентность
- Прозрачность всего трафика между виртуальными машинами
- Правила привязаны к виртуальной машине, т.е. они мобильны и всегда актуальны
- Виртуальная машина может быть добавлена в сегмент в момент создания

КОД безопасности

Эффект от внедрения

Снижение вероятности инцидентов ИБ

Выполнение требований регуляторов

Снижение нагрузки на администраторов сети/средств защиты

Решение проблемы недостаточной производительности межсетевых экранов уровня ЦОД

КОД безопасности

Спасибо за внимание!

Центральный офис: Москва, 1-й Нагатинский проезд, д. 10, стр. 1

Сервисный центр: Москва, Электролитный проезд, д. 9, корп. 1

Телефон: +7 (495) 982-30-20

E-mail: info@securitycode.ru

www.securitycode.ru