



Купол

Купол.Управление

Единый мультивендорный центр аналитики
и управления сетевыми устройствами, имеющий
функции создания и применения политик
безопасности

И С Т С | +IT



Основные проблемы систем централизованного управления



Оптимизация политик

Как эффективно анализировать и оптимизировать политики безопасности?



Управление политиками

Как централизованно управлять правилами на МЭ разных вендоров?



Мониторинг

Как контролировать состояние подключенных устройств?



Контроль

Как контролировать изменения конфигураций устройств?



Мультивендорная реализация

Как интегрировать решения разных вендоров МЭ в систему управления?



Безопасность

Как обеспечить необходимый уровень Идоступов и сетевой безопасности компании?



Совместимость

Как интегрировать продукт в существующую инфраструктуру?



Ограничение прав

Как ограничить права доступа пользователей к устройствам?

Купол.Управление

Единый мультивендорный центр контроля, управления и оптимизации работы межсетевых экранов, UTM, NGFW

Ценность для клиента

- + Ускорение и унификация настройки из единого интерфейса политик МЭ всех вендоров устройств, установленных в инфраструктуре компании
- + Видимость всех устройств МЭ в сети компании и своевременное нахождение неисправных
- + Быстрый ввод в эксплуатацию новых сегментов сети с помощью клонирования конфигураций на одно или несколько устройств
- + Полная видимость изменений политик на устройствах и возможность быстро найти устройство, политики которого нарушили какие-либо бизнес-процессы компании
- + Оптимально настроенные политики безопасности во всей инфраструктуре компании и отсутствие политик, снижающих пропускную способность сети компании и ее защищенность

Функции

Мониторинг состояния всех установленных МЭ

Подключение и мониторинг состояния доступности подключенных устройств МЭ: UserGate, CheckPoint, Cisco ASA, Fortigate и др.



Управление конфигурациями

Автобэкапирование конфигураций подключенных устройств, их клонирование на другие устройства, сравнение версий между собой и анализ



Интеграция с SIEM / SOAR

Отправка журналов событий продукта Купол.Управление в сторонние системы по протоколу Syslog



Управление политиками безопасности

Централизованный контроль и управление политиками / правилами МЭ вендоров: UserGate, CheckPoint, Cisco ASA и др.



Оптимизация правил на всех устройствах

Выявление аномалий в правилах МЭ: избыточных, дублирующихся, теневых и других. Рекомендации по их оптимизации



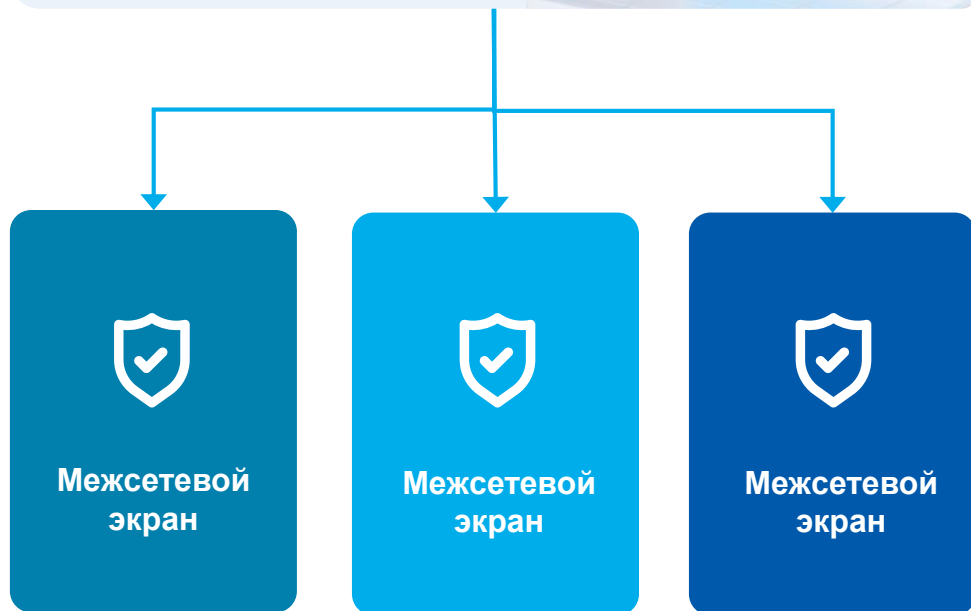
Администрирование

Предоставление прав доступа в систему локальным пользователям и из Active Directory / Astra Linux Directory. Управление парольной политикой. Журнал событий



Интеграция средства защиты информации

Купол.Управление



Единая система для контроля, анализа и управления

 UserGate

 CISCO

 КОД
безопасности

 ELTEX

 ideco

 FORTINET

 infotecs

 CHECK POINT

 ФАКТОР.ТС

Другие вендора МЭ, УТМ,
NGFW и сетевых устройств

Интеграция межсетевых экранов различных вендоров

КУПОЛ

Управление

Рабочий стол

Список устройств

Конфигурации

Анализ политик

Администратор

Главная > Список устройств

Подключение и мониторинг доступности МЭ

Святослав

Список устройств

Подключены 6

Отключены 4

Перезагрузка 0

Список устройств

Управление ответственными за устройства

+ Добавить

...

☐	Название	Статус	IP-адрес	Вендор	Ответственный
☐	Fortigate_test	Подключен	fortigate.fortidemo.com	Fortigate	test@test.ru
☐	CheckPoint1	Подключен	172.31.142.120	CheckPoint	Иванов Дмитрий Кузьмин Владимир
☐	Cisco ASA	Подключен	172.31.142.14	Cisco	Иванов Дмитрий Кузьмин Владимир
☒	UG2602	Подключен	10.229.0.74	UserGate	Андрей test@test.ru Святослав
☐	UserGate	Подключен	172.31.142.126	UserGate	

Настройки устройства

Перезагрузить

Клонировать конфигурацию

Удалить

Настройка столбцов

ФИЛЬТРЫ

Без фильтра

Сохранить фильтр

Клонирование и перенос конфигураций

Анализ политик безопасности

КУПОЛ

Управление

Рабочий стол

Список устройств

Конфигурации

Анализ политик

Администратор

Главная > Анализ политик > Сводка

Святослав

Анализ политик

СводкаОптимизацияОчистка

Выбор устройстваUG2602 10.229.0.74#Всего правил12

Получите наглядное представление обо всех правилах, прописанных в брандмауэре

Запрещающие правила4

Разрешающие правила8

Входящие правила брандмауэра0

Исходящие правила брандмауэра0

Отключенные правила8

Правила с отключённым логированием7

Разрешенные ANY-ANY правила7

Правила, разрешающие трафик любого сервиса без ограничений6

Двухнаправленные правила0

Категорирование результатов анализа

ПолитикиОтключенные правила x

№	Название	Действие	Зона источника	Включено	Адрес источника	Зона назначения
2	Block from botnets	Запретить			Iran, Islamic Republ... Iceland Latvia Holy See (Vatican C... Slovakia Georgia Kazakhstan Estonia Croatia Moldova, Republic of Mexico Saudi Arabia Malta Hungary Bermuda	
3	Allow trusted to untrusted	Разрешить	Trusted			Untrusted
4	Block to botnets	Запретить	Trusted		BAD_SEARCH_BLA... ENTENSYS_KAZ_B...	Untrusted
5	Allow from DMZ to Untrusted	Разрешить	DMZ			Untrusted
6	VPN for Site-to-Site to Trusted and Untrusted	Разрешить	VPN for Site-to-Site			Untrusted Trusted

Рекомендации по оптимизации



 Управление

Рабочий стол

Список устройств

Анализ политик

Сканирование уязвимостей

Администратор

Анализ политик > Переупорядочивание

Анализ политик

Обзор Оптимизация Очистка Сравнение **Переупорядочивание** Временные правила

Выбор устройства: Firewall 1 192.168.1.1 Период: 08.03.2024 00:00 — 15.03.2024 00:00 Анализ политик от 27.03.2024 09:26:00 Обновить

В результате анализа частоты срабатывания правил за определенный период система предлагает вам изменить порядок правил для повышения производительности брандмауэра

Правила

Список устройств > Firewall 1 > Межсетевой экран

Firewall 1 Статус: Подключен IP-адрес: 192.168.1.1

Рекомендуется перенести на + 5 позицию
 В результате анализа частоты срабатывания правил система предлагает вам переместить выбранное правило на 5 позицию

Политики

Межсетевой экран

№	Название	Действие	Зона источника	Адрес источника	Зона назначения	Адрес назначения	Включено	Пользователи
1	Блокировать доступ network1	Запретить	Network6	WTC dms server	Network6	WTC dms server	Включено	
2	Блокировать доступ network1	Разрешить	Network6	Network6	Network6	Network6	Включено	Альянс Банк
3	Блокировать доступ network1	Разрешить	Network6	Network6	Network6	Network6	Включено	
4	Блокировать доступ network1	Разрешить	Network6	Network6	Network6	WTC dms server	Включено	

Сравнение конфигураций

КУПОЛ
Управление

Рабочий стол

Список устройств

Конфигурации

Анализ политик

Сканер уязвимостей

Администратор

Устройства

Конфигурации

Резервные копииИзбранноеСравнениеОтслеживание изменений

Выбрать сохраненные конфигурации

Загрузить файлы

Конфигурация и файл

Устройство 1
Firewall 1 192.168.1.1

Конфигурация 1
Текущая конфигурация

Устройство 2
Firewall 1 192.168.1.1

Конфигурация 2
config2 25.10.2021, 12:48

Сравнить

Сравнение правил

2167

Показывать только отличия

Экспорт

Конфигурация 2

Конфигурация 1

№	ID	Правило	Сравнение	ID	Правило
1			Добавлено	722	Блокировать доступ network1
2			Добавлено	161	Блокировать доступ network1
3	46	Блокировать доступ network1		46	Блокировать доступ network1
4	725	Блокировать доступ network1	Изменено	725	Блокировать доступ network1
	126	Блокировать доступ network1	Удалено		
5	51	Блокировать доступ network1		51	Блокировать доступ network1
	414	Блокировать доступ network1	Удалено		
	61	Блокировать доступ network1	Удалено		
6	53	Блокировать доступ network1		53	Блокировать доступ network1
7	423	Блокировать доступ network1		423	Блокировать доступ network1

Проверка уязвимостей МЭ

КУПОЛ
Управление

Рабочий стол

Список устройств

Анализ политик

Уязвимости

Администратор

Список устройств

Уязвимости Купол.Сети 7 351 +124 18 База уязвимостей от 25 мар 2023г

Список уязвимостей Все 25 68 125 6 616 Показать только изменения

Название	Уровень ↑	Источник	Дата обновления	Устройства
Переход в режим CVT	10	CVE	15 мар 2023, 15:43	24
Выход за пределы контура	10	CERT	15 мар 2023, 15:43	156
Прекращение или нарушение функционирования...	10	CERT	15 мар 2023, 15:43	12
Переход в режим CVT	9,5	CERT	15 мар 2023, 15:43	22
Множественная уязвимость доступа	8	JSA	15 мар 2023, 15:43	70
Переход в режим CVT	7,7	CVE	15 мар 2023, 15:43	46
Множественная уязвимость доступа	6	BID	15 мар 2023, 15:43	11
Ошибка протокола авторизации	5,1	INTEL	15 мар 2023, 15:43	515
Выход за пределы контура	4	JSA	15 мар 2023, 15:43	44
Переход в режим CVT	4	JSA	15 мар 2023, 15:43	1 254

Найдено записей: 47 1 из 5 10

Пример решения проблем

Предприятие с ~110 межсетевыми экранами 4 различных производителей

Проблема клиента до внедрения продукта



Обслуживание межсетевых экранов

Обслуживание межсетевых экранов осуществлялось 2 специалистами (блок ИТ), тем не менее, ввиду импортозамещения и наличие у каждого производителя своего центра управления- время на контроль и настройку значительно увеличивалось



Отсутствуют решения, которые работают с российскими межсетевыми экранами

Рынок российских решений, которые будут поддерживать российские МЭ очень скудный. А также требуется поддержка специфичных межсетевых экранов



Сложность в анализе правил МЭ

Наличие на каждом из МЭ по 50–100 тысяч правил, что значительно снижает производительность сетевых средств защиты, на анализ которых у персонала просто нет времени

Результат внедрения продукта



Единый центр управления

У заказчика появилась возможность не только управлять всеми межсетевыми экранами, но и проводить перенос настройки из одной группы МЭ в другую



Поддержка любого производителя

Решение из коробки поддерживала 3 производителя заказчика, в течении пилотного проекта был освоен и подключен 4, финальный производитель, который использовался у заказчика. В дорожную карту также были заложены 2 производителя, которые в перспективе заменят оставшихся западных производителя



Оптимизация политик МЭ

Были выявлены аномалии в настройках политик подключенных МЭ, что позволило снизить количество правил до 30 000 правил и увеличить производительность сетевых средств защиты



Конкурентные преимущества Купол.Управление



Централизованное мультивендорное управление правилами МЭ, подключенных устройств



Более 15 категорий анализа правил МЭ устройств различных вендоров и формирование рекомендаций по их оптимизации



Автобэкапирование конфигураций подключенных устройств с возможностью их клонирования на другие устройства вендора и сравнения между собой



Предоставление доступа в систему пользователям каталога Astra Linux Directory



Возможность назначения пользователей системы ответственными за одно или несколько подключенных устройств



Интеграция средства защиты информации

Доступные вендора в Купол.Управление



Межсетевые экраны UserGate



Межсетевые экраны Cisco



Межсетевые экраны
Код безопасности



Межсетевой экраны Eltex



Межсетевые экраны Ideco



Межсетевые экраны Fortinet



Межсетевые экраны Infotecs



Межсетевые экраны
Check Point



Межсетевые экраны Фактор-ТС



Другие вендора МЭ, UTM,
NGFW и сетевых устройств



Купол

**Спасибо
за внимание**

И С Т С | +IT

