Защита виртуального частного и гибридного облака

Харламов Павел

ИТ менеджер

www.activecloud.ru

pavel.kharlamov@activecloud.ru

Active CLOUD
a Softline Company

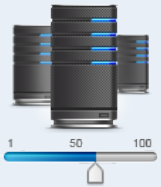
О компании

Компания ActiveCloud работает с 2003 года, с 2010 года входит в группу Softline. Имеет представительства в 6 странах СНГ: Россия, Белоруссия, Азербайджан, Армения, Грузия, Узбекистан, а также представительство в Арабских Эмиратах.

ActiveCloud обслуживает более 50 000 клиентов и предоставляет полный комплект «облачных» решений, от хостинга сайтов, до построения частных облаков. Обеспечивается полная автоматизация услуг на базе платформы Parallels Automation и собственных разработок. Компания входит в ТОП-3 поставщиков услуг IaaS в России.

ActiveCloud предоставляет публичный SLA с финансовыми гарантиями: SLA доступности 99.95%, SLA сроков реакции техподдержки (24/7) – 30 минут. Площадки присутствия компании расположены в Москве, Минске, Ташкенте, а также в Европе и Арабских Эмиратах






Статистика и разновидности угроз

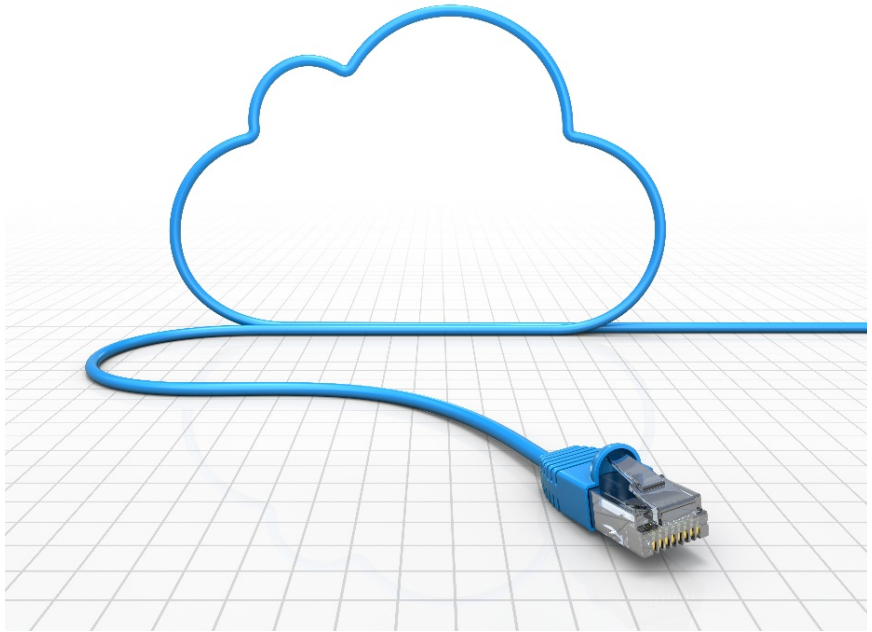
09.06.2014 - HTTP DDoS
16.06.2014 - SSDP Amplification RDDoS
27.07.2014 - DNS Amplification RDDoS
05.09.2014 - Исходящий TCP SYN DoS от нашего клиента1 (4ый инцидент участия в массовых атаках за последний год от этого клиента)
24.09.2014 - исходящий TCP SYN DoS клиента 2
20.10.2014 - UDP Flood на клиента3
22.10.2014 - исходящий TCP SYN DoS клиента 2
27.11.2014 - входящий TCP SYN DoS
07.12.2014 - по 21.12.2014 - 4 атаки на клиента4, две из которых 20+Gbps NTP Amplification RDDoS

13.02.2015 - SSDP Amplification RDDoS
20.02.2015 - NTP Amplification RDDoS
26.02.2015 - UDP length 1 150kpps DDoS
05.03.2015 - HTTP DDoS
14.04.2015 - NTP Amplification RDDoS
19.04.2015 - NTP Amplification RDDoS
20.04.2015 - NTP Amplification RDDoS
09.05.2015 - SSDP Amplification RDDoS
11.05.2015 - SSDP Amplification RDDoS на клиента4
20.05.2015 - UDP Flood
21.05.2015 - NTP Amplification RDDoS, SSDP Amplification RDDoS, TCP SYN DDoS
20.06.2015 - DNS RDDoS
21.06.2015 - SSDP Amplification RDDoS
15.07.2015 - HTTP DDoS 180kpps
30.08.2015 - NTP Amplification RDDoS
09.09.2015 - SSDP Amplification RDDoS
16.09.2015 - UDP Flood
02.10.2015 - HTTP DDoS
05.10.2015 - UDP Flood
20.10.2015 - NTP Amplification RDDoS
19.11.2015 - SSDP Amplification RDDoS на клиента5
20.11.2015 - NTP Amplification RDDoS на клиента5

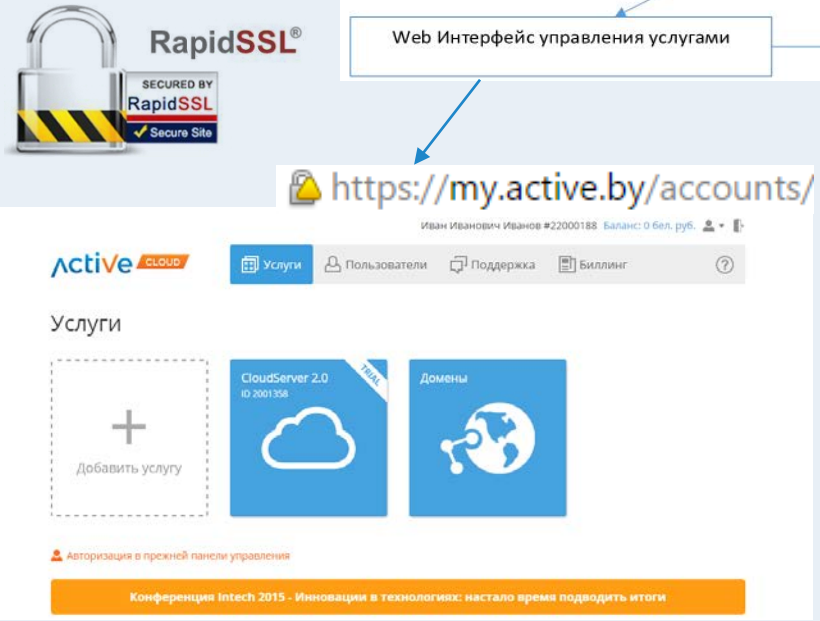
Сетевая инфраструктура

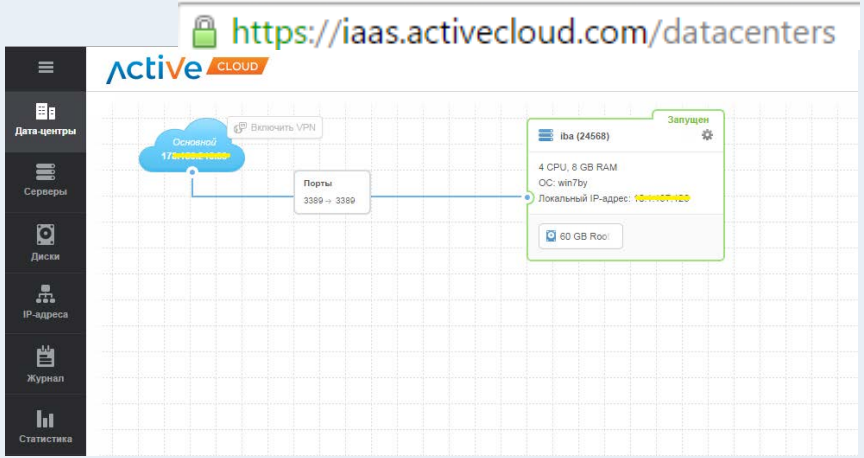
Для обеспечения отказоустойчивости сетевая инфраструктура ActiveCloud построена по принципам резервирования оборудования и каналов связи

- Возможность проброса только необходимых для работы внешних портов
- Возможность ограничения доступа к BM подключениями только из указанной подсети
- Возможность использования виртуального маршрутизатора и балансировщика нагрузки
- Защита от DDoS общего и выделенных каналов
- Возможность использования программных и аппаратных VPN туннелей (OpenVPN, IPSEC, L2TP, S-To-S, P-To-P, и т. д.)

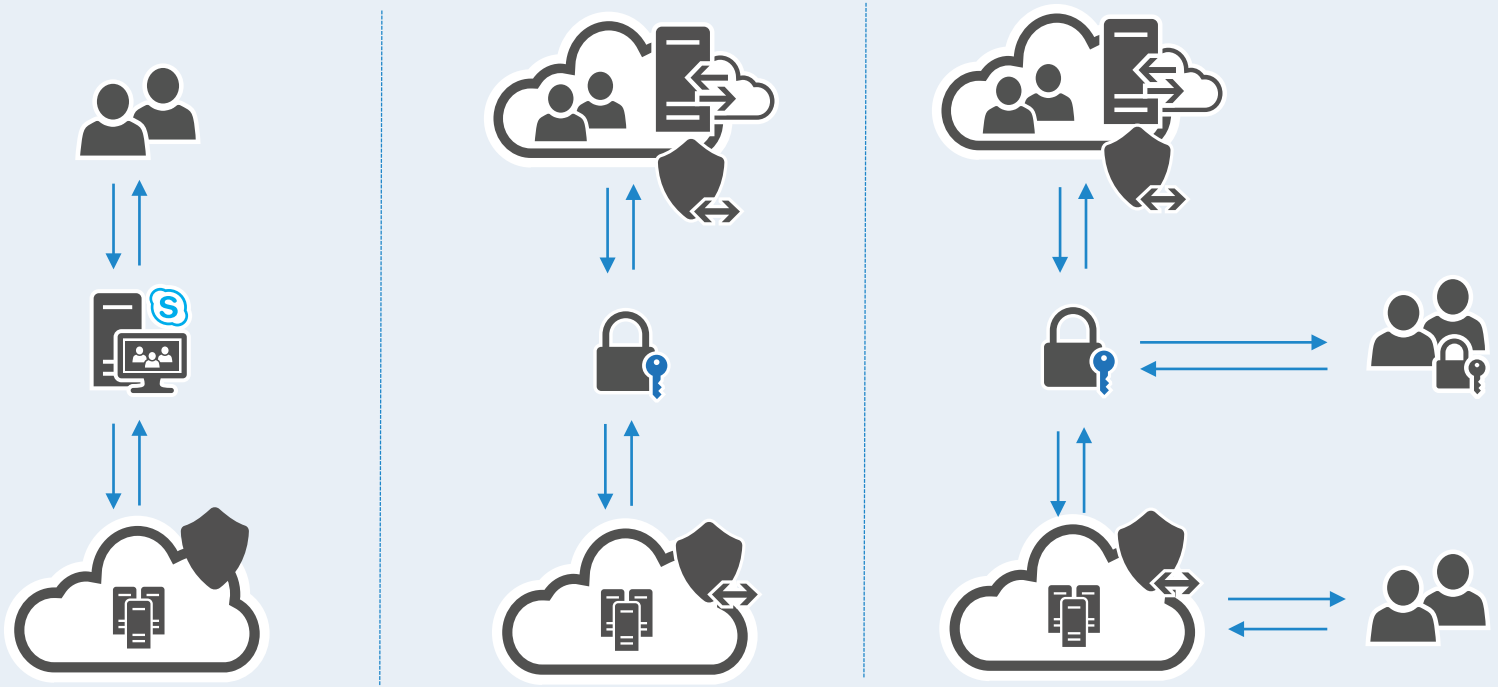


Защита на уровне панели управления





Безопасность виртуального частного и гибридного облака



Защита данных в облаке

Active CLOUD
a Softline Company

Аппаратные
IDS/IPS
Firewall
VPN

Программные средства

- PPTP / L2TP OpenVPN
- IPSEC
- Firewall OS
- Антивирус

Защита от DDOS

- Защита от вредоносного трафика всех клиентов
- Защита клиентов с выделенным каналом доступа
- WAF

Основные принципы нашего облака

Конфиденциальность

Информация может быть прочитана и интерпретирована только теми пользователями, которые авторизованы это делать. Обеспечение конфиденциальности включает процедуры и меры, предотвращающие раскрытие информации неавторизованными пользователями.

Целостность

Информация остается неизменной, корректной и аутентичной.
Обеспечивается:

- Проверка вводимых пользователем данных,
- Идентификация по e-mail,
- Аутентификация – по паролю (учитывается сложность пароля).

Доступность

Только авторизованные пользователи получают доступ и работают с информационными активами, ресурсами и системами, при этом обеспечивается:

- Требуемая производитель-ность
- Проверка прав и уровня доступа

3 типа учетных записей:

- Владелец
- Администратор
- Пользователь

Безопасность в облаке ActiveCloud

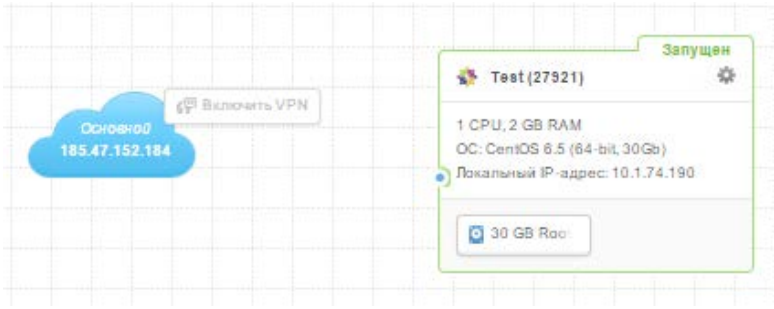
- Защита каналов передачи данных в «облачной» инфраструктуре;
- Защита каналов связи между сетью клиента и облачной инфраструктурой;
- Отслеживание уязвимостей, резервирование и защита от потери данных;
- Использование идентификации/аутентификации;
- Соглашение о конфиденциальности NDA;
- Обеспечение доступности ресурса: 99.95%.

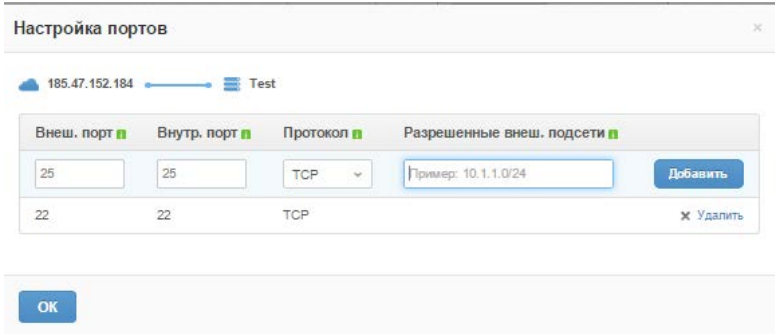




Защита виртуальных машин от несанкционированного доступа

- После создания ВМ – закрыта для доступа из вне
- Проброс только необходимых для работы портов Возможность ограничения доступа, из указанной подсети
- Подключение через защищенный канал к виртуальной инфраструктуре
- Роутинг и автоматическое выделение инфраструктуры клиента в независимую подсеть

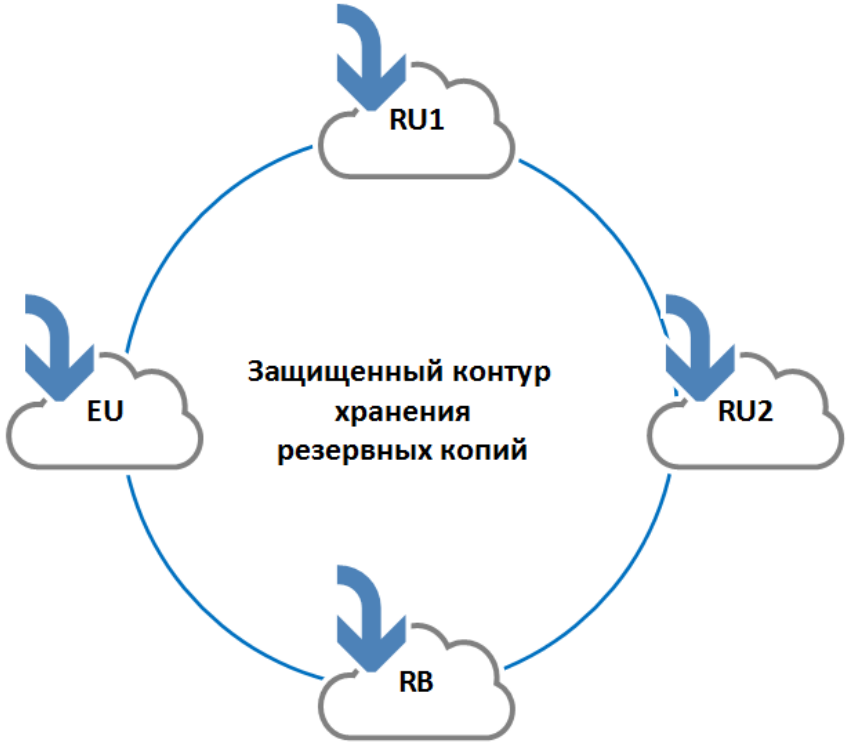




Заказчик может использовать различные программные средства, для защиты персональных данных:

- Модерация паролей/уровня доступа
- Шифрование ФС
- Настройка правил файерволов в ОС ВМ
- Использование Антивирусных средств и т.д.

Защищенное резервное копирование



- Объектное хранилище с доступом по интерфейсу REST
- GEO распределенная система хранения с уровнем надежности хранения девять девяток
- Выбор площадок размещения
- Выпор ПО для резервного копирования, совместим с API Amazon S3
- Синхронный алгоритм записи

Решение по защите авторизации

Сфера применения:

- Сервисы онлайн оплат
- Банковская сфера
- Интернет казино
- Онлайн сервисы с авторизацией пользователей

Преимущества над стандартными решениями:

- Сервис расположен в РФ
- Поддержка Windows, Linux, Mac, IOS, Android
- Самостоятельное решение или дополнение к существующим компонентам
- Привязка к устройству и геоположению
- Уровень безопасности 2FA

Решение для защиты документов

Незащищенные документы

Защита и учет документа

Уникальные защищенные копии

Расследование инцидентов

Сфера применения:

- Коммерческие организации
- Банковская сфера

Преимущества:

- Сервис расположен в РФ
- Поддержка защиты PDF документов
- Возможность самостоятельной проверки скомпрометированной копии документа через онлайн сервис
- Заказ расследования инцидента утечки информации через онлайн сервис
- Приобретается из расчета необходимого количества уникальных копий документа

Нам доверяют

СПАСИБО!

Харламов Павел

ИТ менеджер

pavel.kharlamov@activecloud.ru

www.activecloud.ru