Опыт использования PAM в крупном ритейле

Дмитрий Безбородов
Начальник отдела кибербезопасности

О компании Магнит

«Магнит» является одной из ведущих розничных сетей в России по торговле продуктами питания, лидером по количеству магазинов и географии их расположения.

- Входит в список крупнейших публичных компаний мира рейтинга Global 2000 Forbes
- Крупнейший частный работодатель России. Количество сотрудников превышает 300 тысяч человек
- Работает более чем в 3800 населенных пунктах
- Ежедневно магазины компании посещают 13 миллионов человек
- Более 50 миллионов покупателей являются участниками кросс-форматной программы лояльности
- Компания имеет 22 344 магазина в 66 регионах России
- Компания имеет более 6 тысяч магазинов парфюмерии и косметики
- В сеть магазинов входит более 1 тысячи аптек
- Автопарк компании составляет более 4 тысяч автомобилей
- Обладает 17 собственными пищевыми и агропромышленными комплексам

Данные за 30 июня 2021 года

Об ИТ инфраструктуре компании Магнит

«Магнит» обладает масштабной, географически распределенной инфраструктурой.

- Головной офис компании и основные ИТ-мощности находятся в Краснодаре
- Несколько тысяч серверов
- Несколько сотен тысяч единиц сетевого оборудования
- Три собственных дата-центра
- Обслуживают инфраструктуру более 3000 специалистов
- Порядка 1500 человек обслуживают инфраструктуру магазинов
- В штате более 1000 разработчиков
- Имеет 39 распределительных центра
- Инфраструктура располагается в 66 регионах

Задачи PAM

1. Контроль доступа подрядчиков
2. Обеспечение безопасности особо критичных сервисов
3. Помощь в разборе инцидентов
4. Предоставление удаленного доступа для сотрудников компании к целевым ИС компании через контролируемый шлюз
5. Real-time контроль действий внешних аудиторов и партнеров, работающих с наиболее критичной информацией

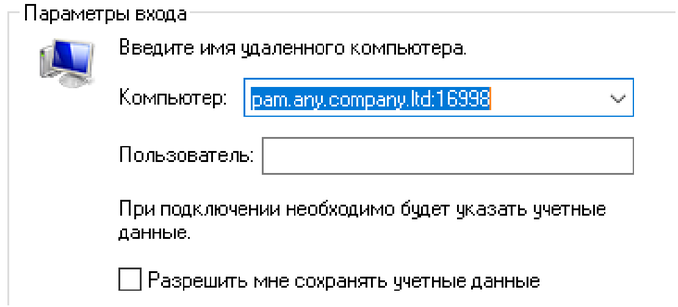
Как было (jump-сервер)

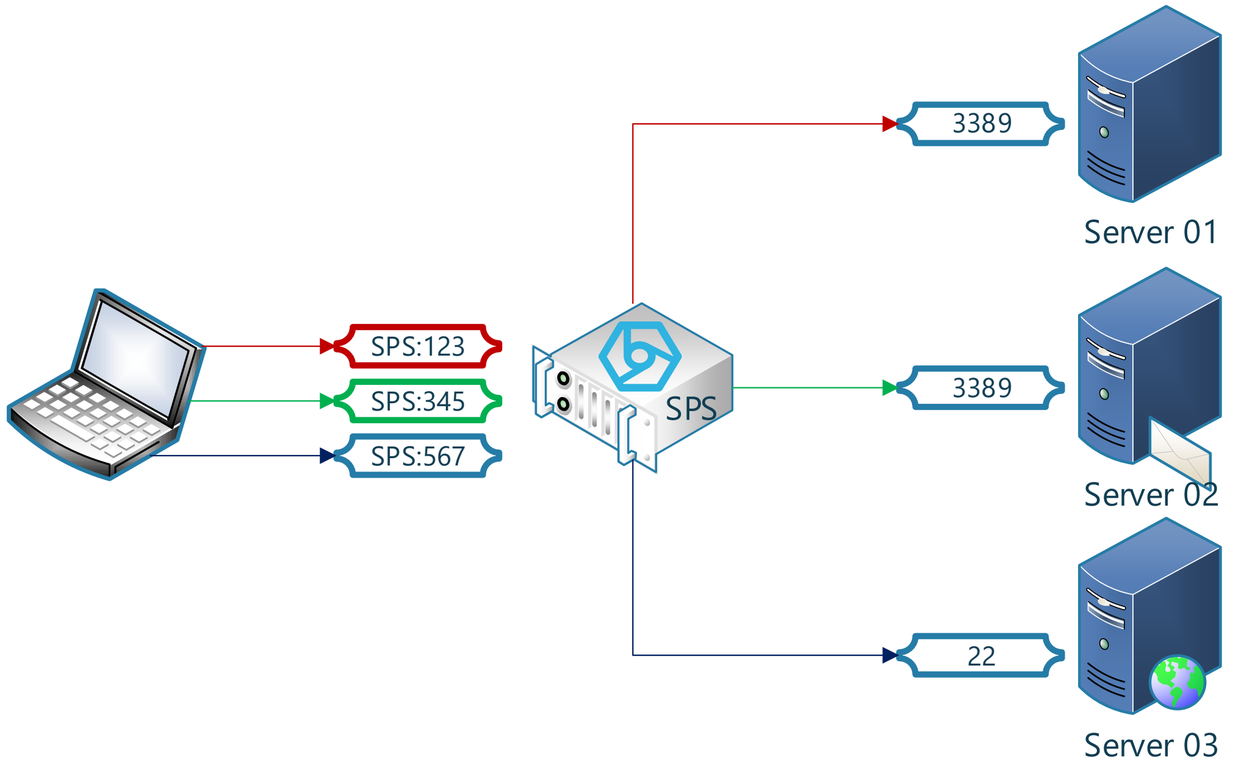
Схема подключения:

- В строке подключения пользователь указывает PAM + порт PAM

Сложности:

- Необходимость указывать не те адреса и порты, которые знают пользователи





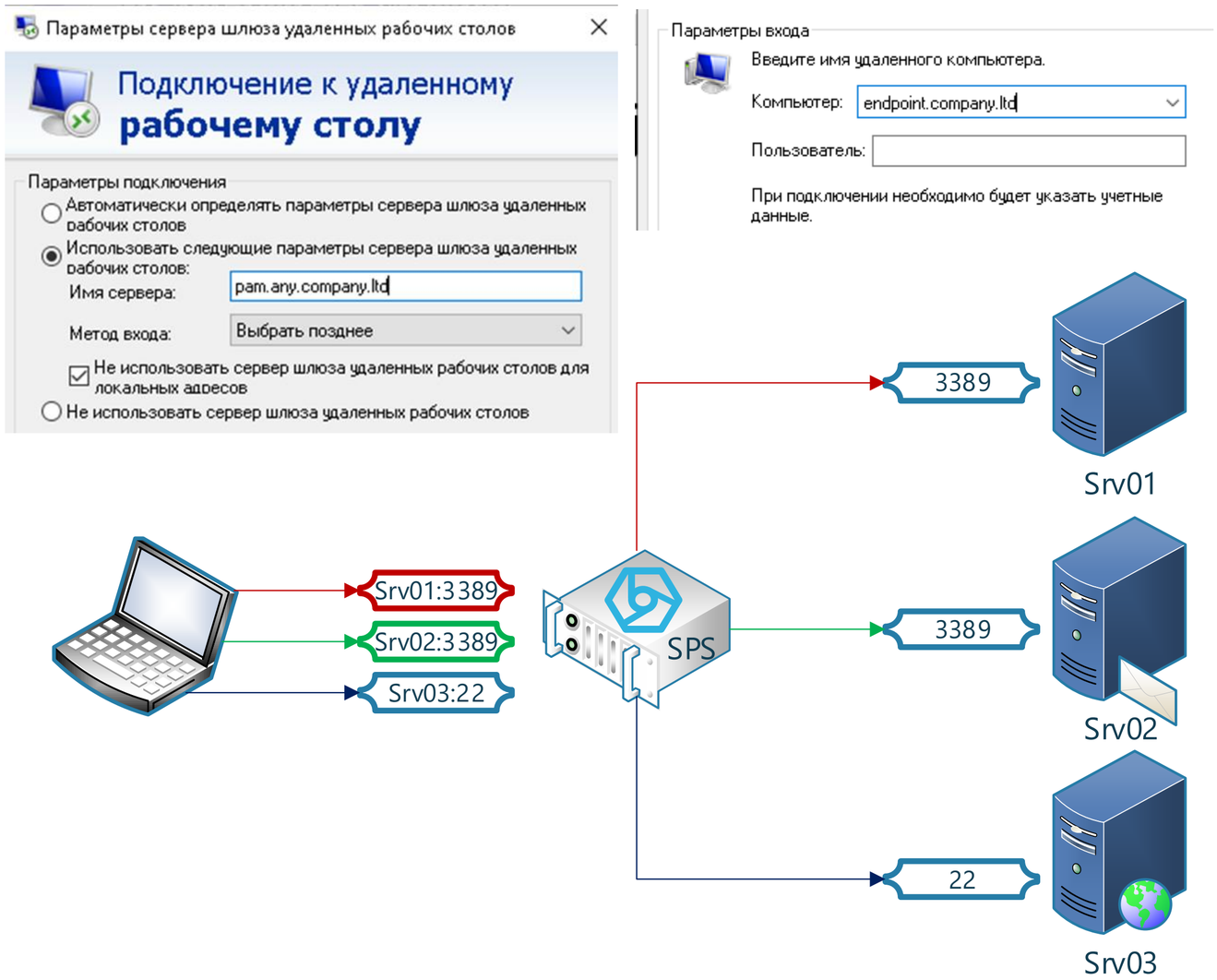
Как стало (в режиме шлюза)

Схема подключения:

- В строке подключения пользователь указывает адрес целевого сервера

Преимущества:

- Удобство использования
- Работа по готовой инструкции



Сложности с которыми столкнулись

При настройке работы SPS в режиме шлюза в техническом плане сложностей не возникло.

Большую часть времени заняло изменение процессов по предоставлению доступа через PAM по новой схеме:

- составление инструкций по подключению по новой схеме
- оповещение пользователей и контроль их перехода на новую схему
- оперативная правка и дополнение политик доступа
- решение проблем с подключением у пользователей (в основном при подключении с устаревших версий ОС)
- реализация нового шаблона на портале самообслуживания, который позволяет в режиме «одного окна» получить все необходимое для возможности подключения через PAM

Масштаб применения PAM-системы

Требования к системе:

- Визуальная запись сессий по основным протоколам (RDP, SSH, HTTPS)
- Возможность предоставление доступа только в режиме терминала
- Запрет на доступ к буферу обмена, пробросу дисков, SCP даже если это разрешено на конечном хосте
- Предоставление прав (доступ к той или иной системе, доступ к буферу обмена, пробросу дисков и др.) на основе членства в доменной группе
- Завершение сессии при выявлении попыток выполнения деструктивных действий на конечном хосте

Текущие объемы:

- Одновременных подключений – 200
- Итого подключений в день – 1500
- Подключений под уникальными УЗ в день – до 400

Интересные кейсы

- **Кейс 1:** Сотрудник подрядной организации выполнил деструктивные действия по уничтожению базы в продуктовой среде и удалил следы.
  - Установили время выхода из строя
  - Проверили сессии и выявили виновного
- Удалось быстро разобрать ситуацию, т.к. весь доступ к продуктовым системам был только через PAM
- **Кейс 2:** сотрудник подрядной организации выполнил установку ПО, запрещенного для использования в компании. Так как данный сотрудник имел административные права на ВМ, куда выполнял подключение, то был на особом контроле и при просмотре записей подключений был выявлен факт установки запрещенного ПО и оно было оперативно удалено.
- **Кейс 3:** при выполнении работ внешним подрядчиком сотрудники компании в нарушении требований ИБ создавали локальные УЗ с административными правами, которые использовал подрядчик. Также разглашались пароли от сервисных УЗ. С помощью PAM эти факты были выявлены и схема работы подрядчика была пересмотрена.

Планы по развитию системы

- Управление паролями
- Аналитика поведения
- Превентивное реагирование
- Удаленный доступ к порталам без VPN
- Гранулированный контроль доступа

Сопровождение PAM

Кол-во сотрудников: 2

Время на сопровождение:

- 10% - добавление новых контролируемых систем и отключение старых
- 15% - согласование доступов
- 20% - просмотр сессий доступа к наиболее критичным системам
- 30% - просмотр сессий при разборе инцидентов
- 15% - анализ отчетности для выявления
- 5% - настройка новых и тюнинг имеющихся правил
- 5% - тестирование новых версий и обновление системы

Процесс управления доступом

- Регламентированный процесс управления доступом
  - Запрос
  - Согласование
  - Предоставление
  - Анализ
- Особое внимание к особо критичным сервисам
  - Онлайн-мониторинг доступа
  - Обязательный просмотр сессии перед разрешением следующего сеанса
- Категорирование подрядчиков в зависимости от уровня доступа и истории взаимодействия

Дорожная карта

- 2020-2021:
  - Переход с режима работы через Jump-сервер на режим шлюза
  - Переход на отказоустойчивую конфигурацию
  - Протестировали модуль визуальной записи HTTPS-сессий, высказали пожелания к доработке.
  - Протестировали модуль управления паролями
  - Протестировать абсолютно прозрачный режим
- 2022:
  - Внедрить модуль управления паролями
  - Автоматизировать составление отчетов по подключениям
  - Продолжить масштабирование системы для реализации доступа к критичной инфраструктуре через SPS
  - Протестировать удаленный доступ к корпоративным порталам без VPN и гранулярное управление доступом

Спасибо за внимание!