Чек-лист

На что обратить внимание при выборе межсетевых экранов?

Сформируйте план

Данный чек-лист поможет при реализации сетевой защиты в компании. Пройдя по всем пунктам документа, вы сформируете план, в котором будут учтены основные вопросы, связанные с выбором и эксплуатацией межсетевого экрана.

01 Цель и задачи

02 Персонал

03 Выбор подрядчика

04 Оценка и тестирование

05 Эксплуатация

06 Стоимость

Ростелеком Солар

Цель и задачи

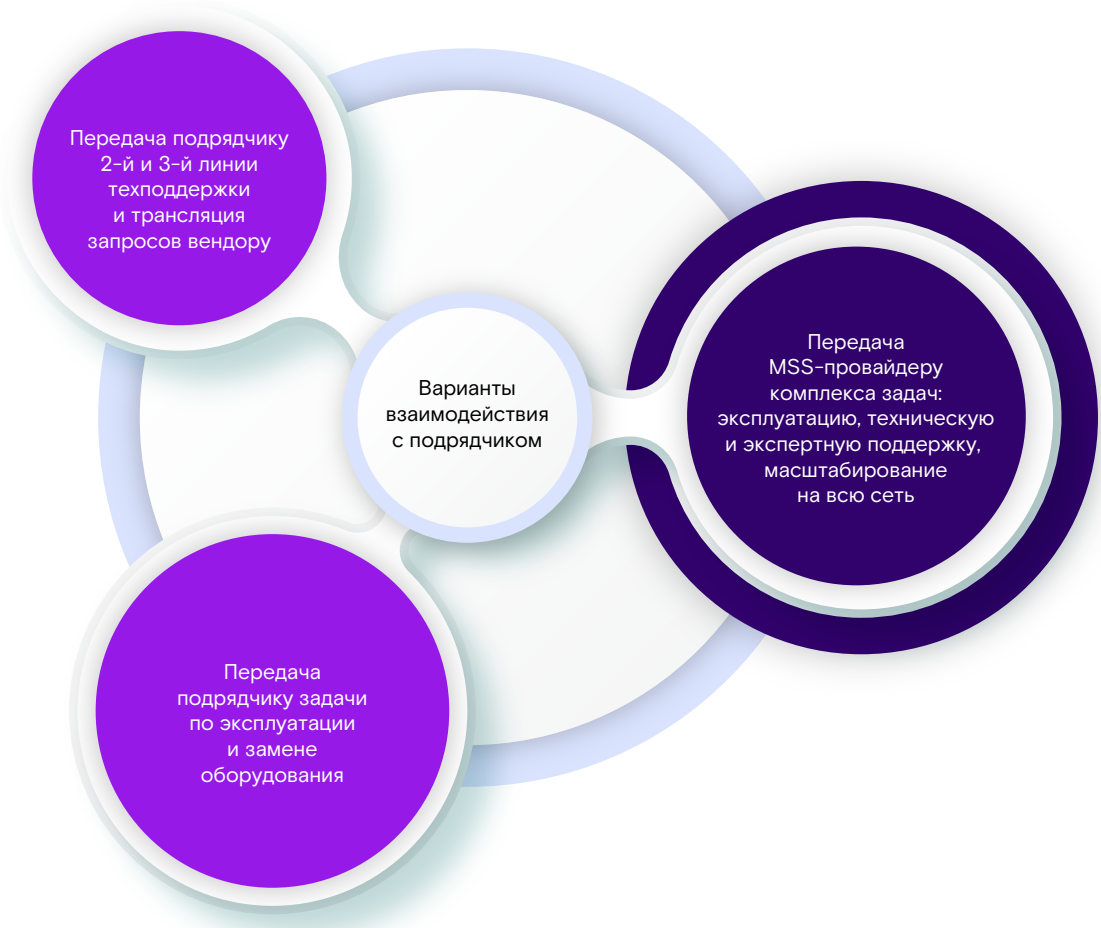
- [ ] Определите задачи, которые планируете решить с помощью подключения межсетевого экрана:
  - [ ] Обеспечить периметровую защиту сети.
  - [ ] Управлять доступом пользователей в интернет со всех площадок.
  - [ ] Контролировать трафик внутри сети (использование внутри ЦОД, как ядро сети).
  - [ ] Заменить существующие решения сетевой безопасности (прокси-сервер, межсетевые экраны L4, другие решения).

- [ ] Зафиксируйте, какие функции межсетевого экрана будете использовать. Наиболее часто используемые:
  - [ ] Маршрутизация (статическая, динамическая).
  - [ ] Система обнаружения вторжений (IPS).
  - [ ] Потоковый антивирус.
  - [ ] Блокировка подключений к серверам ботнетов (C&C).
  - [ ] URL-фильтрация и категоризация
    Распознавание и контроль трафика приложений на всех портах.
  - [ ] Удаленный доступ к ресурсам компании.
  - [ ] Идентификация стран и внутренних пользователей.
  - [ ] Расшифровка и инспекция SSL/TLS-трафика.
  - [ ] Идентификация файлов и возможность отправки во внешние системы.

Персонал

☐ Определите, кто в компании будет администрировать межсетевые экраны:

- собственные специалисты,
- подрядчик.



☐ Оцените, есть ли у вас обученные сотрудники, которые будут работать с выбранным вендором и определенным набором функциональных возможностей межсетевого экрана.

Если нет, то переходим к следующему пункту.

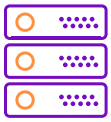
☐ Запланируйте обучение для работы с решением конкретного вендора.

Выбор подрядчика

- [ ] Проведите оценку подрядчика:
  - работали ли вы с ним ранее?
  - есть ли положительные отзывы от коллег или лидеров мнений?

- [ ] Уточните у подрядчика:

сроки поставки



наличие оборудования

возможность резервирования оборудования заранее

- [ ] Задайтесь вопросом: если вам понадобится срочная замена вышедшего из строя оборудования или изменение его производительности, какие необходимы действия от вас и партнера.

- [ ] Продумайте заранее план действий на случай, если вендор ограничит доступ к функциональности и обновлениям.

Оценка и тестирование

- [ ] Определите количество площадок, на которые необходимо установить межсетевые экраны. Выберите схемы подключения и набор функций, которые будут задействованы на каждой из площадок.

- [ ] Уточните, учтена ли отказоустойчивость в проекте и каким образом она реализована – например, на критичных площадках, в точке выхода в интернет и т. д.

- [ ] Учтите, что при тестировании функции межсетевого экрана должны работать только в режиме «блокирования/предотвращения», так как каждая дополнительно включенная опция уменьшает его производительность.

- [ ] Выясните, какие особенности имеют функциональные профили межсетевого экрана: IPS, потоковый антивирус, инспектирование шифрованного трафика. Запросите их состав у вендора, поскольку у каждого решения свои определенные шаблонные конфигурации.

- [ ] Проведите тестирование самостоятельно на своем профиле трафика, который формируется в организации. Тестировать следует сразу все планируемые к использованию функции межсетевого экрана одновременно, с включением правил фильтрации.

- [ ] Уточните возможность покупки и оперативного подключения дополнительных средств защиты, например защиты электронной почты или песочницы. Выясните, совместимо ли решение межсетевого экранирования вашего вендора с подключаемыми решениями других поставщиков услуг.

- [ ] Предусмотрите возможность быстрого развертывания устройства (Zero-Touch) без предварительной настройки конфигурации. Желательно сначала протестировать реализацию Zero-Touch на практике.

Эксплуатация

- [ ] Имейте ввиду, что архитектура сети может значительно измениться после внедрения межсетевого экрана.
- [ ] Запланируйте и используйте централизованное управление и сбор логов. Определите, где и как будете разворачивать это решение, каких специалистов следует привлечь.
- [ ] Проанализируйте, все ли планируемые к использованию функции межсетевого экрана задействованы и находятся в режиме «предотвращения/блокирования».
- [ ] Проработайте процесс подключения новых площадок, чтобы при необходимости это можно было осуществить оперативно.
- [ ] Добавьте и актуализируйте правила уровня приложений (L7), не создавая при этом большого списка исключений, которые потом остаются в конфигурациях.
- [ ] Реализуйте идентификацию пользователей, распределяя их по группам.
- [ ] Организуйте процесс патчинга и закрытия уязвимостей. Чем быстрее он будет проходить – тем эффективнее будет работать межсетевой экран.
- [ ] Производите настройку IPS, не оставляя конфигурацию «по умолчанию».
- [ ] Ведите учет конфигураций. Определите ответственного.
- [ ] Запланируйте обновление оборудования и зафиксируйте частоту его обновления. Цикл жизни оборудования (End-of-Life Policy) можно уточнить у вендора.
- [ ] Определите, где хранить запасное оборудование, как быстро сможете заменить вышедшее из строя и кто это будет реализовывать.

Стоимость

- [ ] Рассчитайте стоимость оборудования, планируемого к закупке, включая запасное (это в среднем 2–5% от общей стоимости оборудования).
- [ ] Уточните, каким образом происходит лицензирование функциональности. Запланируйте стоимость лицензирования на 4 года вперёд.
- [ ] Оцените стоимость оборудования за первый год использования, подписку на лицензии на последующие – минимально на ближайшие 4 года.
- [ ] Не забудьте учесть стоимость использования в течение 4х и более лет сервера хранения логов и сервера управления с подписками.
- [ ] Уточните, ко всем ли функциям, бесплатным в первый год использования, будет доступ в дальнейшем.
- [ ] Заложите расходы на команду, которая будет обслуживать межсетевые экраны. Это позволит сформировать итоговую оценку стоимости владения сетевой безопасностью.

Посчитать прямую выгоду довольно сложно, но обычно она заключается в снижении рисков инцидентов ИБ и возможных финансовых потерь.

Рекомендуем сравнить с другими решениями и сервисным подходом от поставщиков.