Лекция. Как защитить сеть компании с филиалами

Головная боль ИБ-департамента компаний с региональными подразделениями — обеспечение всесторонней защиты сетевой инфраструктуры филиалов от различных рисков. Нужно не только разработать политики информационной безопасности, но и внедрить их в регионах, обеспечить постоянный мониторинг защиты, контроль за действиями пользователей и работой местных администраторов. А ещё приходится оперативно вносить изменения в конфигурацию, устанавливать исправления для уязвимостей и делать массу вещей, которые далеко не всегда можно найти в должностной инструкции.

Не меньшее беспокойство вызывает безопасность работы филиалов у руководства компании. Это только кажется, что утечки данных, действия инсайдеров и кибератаки — проблема ИТ- и ИБ-служб. На самом деле такие инциденты наносят бизнесу репутационный и вполне материальный ущерб в виде простоев, штрафов и потери клиентов.

Получается, что комплексная защита сетей компании и филиалов — не прихоть руководителя департамента безопасности, а серьёзная проблема, требующая безотлагательного решения.

Реализовать защиту сети компаний с филиалами можно различными способами. Наиболее распространёнными являются два подхода:

1. **Независимый**, при котором на уровне организации принимается набор стандартов, а их реализацией занимаются сотрудники региональных подразделений исходя из имеющихся бюджетов и оборудования.
2. **Централизованный**, когда для филиалов закупается и внедряется типовое защитное решение, а его настройкой и управлением занимаются сотрудники центрального офиса.

Независимый подход

В этом случае региональные ИТ- и ИБ-службы самостоятельно обеспечивают внедрение и реализацию принятых в компании стандартов безопасности.

Когда сетевая инфраструктура филиалов разнородна, например, если она досталась в наследство от вошедшей в состав холдинга компании, унификация оборудования может занять не один год в зависимости от бюджета. Но даже в переходный период сеть компании нужно защищать, настроив имеющееся оборудование в соответствии с действующей политикой безопасности.

Кажется целесообразным привлечь к реализации этой задачи региональных сотрудников. Они хорошо знакомы с сетью и сами настраивали своё оборудование, поэтому всё должно получиться легко и просто. Однако здесь следует учитывать две потенциальные проблемы:

- **Злоупотребления.** Сотрудники филиалов подчиняются местному руководству, поэтому могут по его указанию открыть удалённый доступ к сети с личных ноутбуков или разрешить сотрудникам офиса посещать небезопасные интернет-ресурсы «для решения задач бизнеса».
- **Низкая квалификация.** Если в крупных городах дефицит квалифицированных специалистов — редкое явление, в небольших городских поселениях это вполне обычная картина. Настройка защитного решения, произведённая сотрудником, не обладающим необходимыми знаниями, может привести к тому, что сеть окажется уязвимой для всех видов атак.

Централизованный подход

Этот вариант взаимодействия предполагает, что всё управление инфраструктурой и защитой производятся из единого центра. Обычно такую работу выполняет выделенная группа администраторов в составе ИТ-службы головного офиса. При этом региональные подразделения оснащены стандартным оборудованием, конфигурация сети и настройки защиты унифицированы, а необходимые изменения можно быстро развернуть во всех регионах разом.

В случае с разнородной сетевой инфраструктурой филиалов централизованный подход может потребовать затрат на приобретение унифицированного оборудования, однако в долгосрочной перспективе эти расходы достаточно быстро окупятся благодаря снижению стоимости сопровождения и повышению управляемости.

Таким образом, для защиты сетей компаний с филиалами наиболее эффективным вариантом является централизованный подход, в основе которого лежит решение, обладающее богатым набором функций, достаточной гибкостью настроек и возможностью централизованного управления. Для государственных компаний и организаций, работающих с персональными данными важно, чтобы решение было сертифицировано ФСТЭК.

Что выбрать?

В качестве решения, которое позволяет централизованно управлять безопасностью всех территориально удалённых структурных подразделений, рассмотрим универсальный шлюз безопасности (UTM) Traffic Inspector Next Generation версии Enterprise.

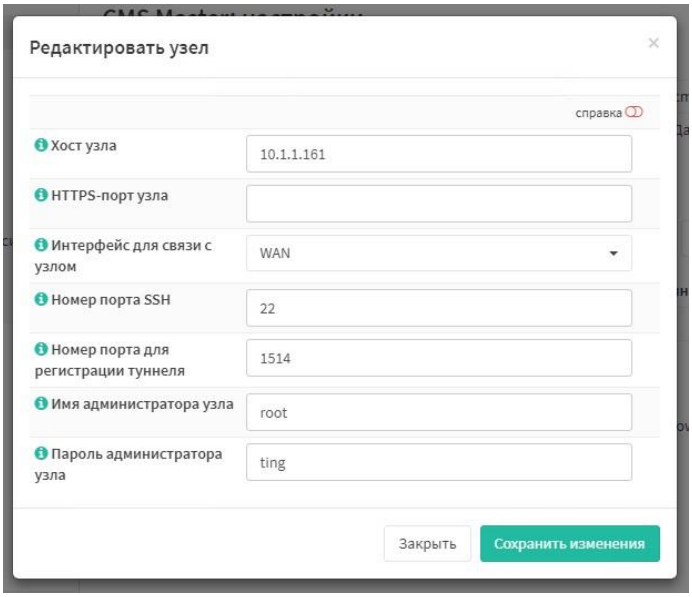
Traffic Inspector Next Generation Enterprise имеет в составе систему централизованного управления распределённой инфраструктурой сетевых шлюзов - Central Management System.

Для организации управления «из центра» одному из шлюзов Traffic Inspector Next Generation назначают роль *мастер-узла (master node)*. Обычно в этом качестве используют шлюз центрального офиса организации. Из интерфейса мастер-узла выполняется централизованное администрирование, диагностика и сбор данных с сетевых шлюзов, расположенных в удалённых офисах.

Шлюзы Traffic Inspector Next Generation в каждом из удалённых офисов учреждения устанавливаются в режиме *подчинённого узла (slave node)*. Подчинённый узел получает свои настройки от мастер-узла и в соответствии с ними контролирует и защищает сетевое взаимодействие между компьютерами удалённого офиса и интернетом.

Система централизованного управления распределённой инфраструктурой сетевых шлюзов Traffic Inspector Next Generation Enterprise

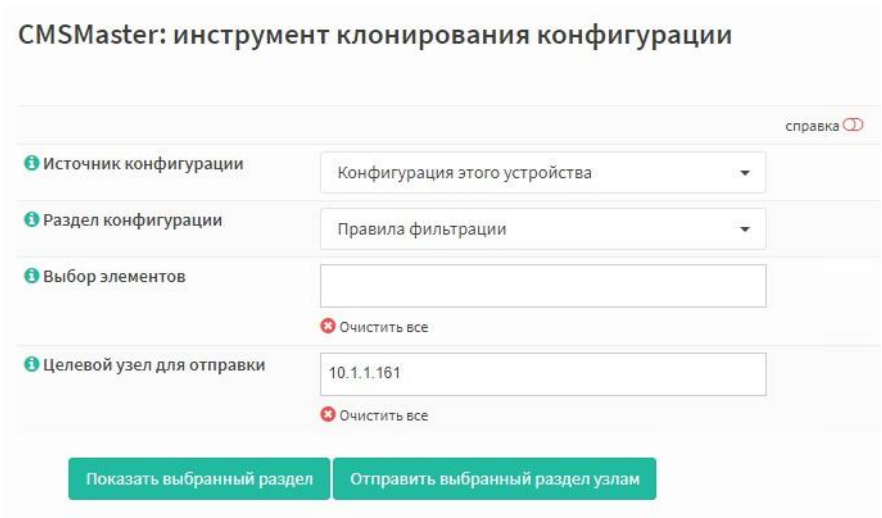
В процессе развёртывания решения администратор настраивает каждый из узлов будущей инфраструктуры для взаимодействия с мастер-узлом, а на мастер-узле производится регистрация подчинённых шлюзов.



Окно добавления подчиненного узла в Traffic Inspector Next Generation Enterprise

Сетевое взаимодействие между главным и подчинёнными шлюзами производится по защищённым соединениям SSH и HTTPS. Завершив базовую настройку инфраструктуры, администратор может передать на подчинённые узлы настройки и получить от них диагностические сообщения, просмотреть syslog-журналы и установить обновления.

Если потребуется добавить в сеть организации новое подразделение, с помощью Central Management System легко клонировать конфигурацию имеющегося узла и отправить её на новый шлюз.



Настройки для передачи правил фильтрации Traffic Inspector Next Generation Enterprise

Заключение

Централизованный подход к защите сетевой инфраструктуры филиалов компании обеспечивает лучшую эффективность и более высокий уровень безопасности. При этом первоначальные инвестиции на унификацию оборудования и приобретение комплексного защитного решения быстро окупятся за счёт устранения рисков информационной безопасности и снижения трудозатрат ИТ-персонала.

TRAFFIC INSPECTOR NEXT GENERATION

Протестировать Traffic Inspector Next Generation в своей сети.

Попробовать бесплатно