ИССЛЕДОВАНИЕ

Обеспечение безопасности проводных и беспроводных сетей

Основные проблемы и решения

Аннотация

Наиболее обширным направлением возможных атак на корпоративную сеть является уровень доступа. Он обеспечивает все подключения к сети (при помощи как проводных коммутаторов Ethernet, так и беспроводных точек доступа) для сотрудников, подрядчиков и посетителей, а также устройств Интернета вещей (IoT). Количество подключающихся к сети устройств непрерывно растет, в связи с чем возрастает и потребность в эффективных средствах защиты уровня доступа. Во время пандемии COVID-19 удаленная работа вошла в норму, и в ближайшее время эта тенденция сохранится. Таким образом, задача предотвращения атак на уровне доступа стала как никогда актуальной[1].

Модернизация сети LAN кампуса не только обеспечивает безопасность части корпоративной сети, которой до этого пренебрегали, но и может стать предпосылкой к внедрению комплексных функций управления и отслеживания[3].

Проблемы существующей инфраструктуры доступа

Периферия LAN — это масштабная и потенциально уязвимая для киберпреступников область сети, особенно в наше время: ведь от наличия и производительности сетевых подключений зависит выживание организаций во всех отраслях. При этом количество атак растет. К примеру, в первом квартале 2020 г. количество атак типа «отказ в обслуживании» (DDoS), ориентированных на перегрузку сетевых подключений, на 542% превысило аналогичный показатель за предыдущий период (4 квартал 2019 г.).[2]

Перечислим некоторые проблемы, с которыми сталкиваются ИТ-организации в процессе управления уровнями доступа:

- Синхронизация разных конфигураций
- Отслеживание всех компонентов сети
- Управление разными уровнями доступа
- Высокая совокупная стоимость владения (TCO)

В целях повышения эффективности управления компонентами сетевой безопасности организации принимают на вооружение концепцию интегрированной платформы. Стремясь снизить операционные расходы, ИТ-специалисты все чаще внедряют решения, включающие функции управления как проводными и беспроводными сетями, так и компонентами безопасности. Однако не все из этих решений отличаются достаточной простотой, функциональностью и производительностью.

Сложность структуры снижает производительность локальных сетей (LAN)

По мере развития бизнеса, сопровождающегося появлением новых пользователей и устройств, традиционные сети LAN физически расширяются и усложняются. В связи с этим ИТ-администраторам приходится уделять больше времени отслеживанию различных событий в сети. Такие тенденции, как развертывание сетей филиалов и дополнительных офисов, а также рост количества сотрудников, работающих из дома, усугубляют сложившуюся ситуацию с сетями LAN и требуют повышения расходов на операционном уровне.

Управление конфигурацией

- В больших филиалах одно незначительное изменение способно нарушить работу огромных областей сети. Организации должны позаботиться о том, чтобы отслеживание и управление дополнениями, изменениями и обновлениями осуществлялось без ущерба для синхронизации и работоспособности всех компонентов сети.
- Проблемы конфигурации также могут возникнуть во время развертывания сетей в удаленных офисах. Процессы внедрения и поддержки единых стандартов в большом количестве удаленных расположений с разной топологией нередко приводят к быстрому истощению ресурсов ИТ-отдела.

Отслеживание сетей

- Сотрудники, подрядчики и сторонние посетители постоянно подключаются к сетям филиалов со своих устройств. С помощью стандартного средства отслеживания периметра LAN можно получить информацию о подключении устройства, однако не всегда удается отследить контекст более высокого уровня, к примеру, уровня проверки подлинности пользователей, включая все связанные с ним ограничения доступа к ресурсам.
- Сложнее всего отслеживать устройства IoT. При появлении такого устройства в сети ИТ-специалист должен предоставить ему доступ таким образом, чтобы устранить риски для безопасности сети в целом. Задача становится еще сложнее, если в удаленных офисах нет собственных ИТ-специалистов. Это обусловлено тем, что сведения об устройстве ограничиваются данными интерфейса уровня доступа.

Безопасности сетей LAN уделяется недостаточно внимания: они лишены таких ключевых функций, как шифрование, управление доступом и детализированное отслеживание. Уязвимость сетей LAN достаточно быстро стала очевидна злоумышленникам[4].

Высокая совокупная стоимость владения (TCO)

- Разработчики современных сетей LAN попытались решить проблему их чрезмерной сложности путем добавления дополнительных лицензий и/или подписок, призванных удовлетворить потребности ИТ-специалистов. В процессе добавления этих улучшений совокупная стоимость владения по сравнению со стоимостью сетевого оборудования возросла вдвое и даже втрое.
- Кроме того, развертывание новых систем и дополнительных уровней управления и защиты периферии сетей LAN вынуждает ИТ-специалистов тратить время и силы на изучение интерфейсов и администрирование этих разрозненных решений.

Безопасность

- По мере усложнения сетей LAN структуры защиты всех точек входа в сеть для всех категорий авторизованных пользователей также становятся все более разветвленными. В попытке устранить уязвимости многие организации последовательно внедряют специализированные средства защиты. Этот сложный и несогласованный подход к безопасности способен поставить под удар всю корпоративную сеть. Единственная ошибка конфигурации средства безопасности LAN может привести к утечке данных непосредственно из сети.

Критерии, которые следует учитывать при оценке решений

В процессе модернизации корпоративных проводных и беспроводных сетей LAN необходимо принять во внимание несколько факторов.

- ✓ **Топологическая структура.** Выбранное средство безопасности LAN должно соответствовать характеристикам местоположения, где планируется развернуть сеть. Это совокупность крупных офисов или нескольких маленьких филиалов? Будут ли удаленные работники подключаться к сети? Нередко решение представляет собой сочетание двух и более компонентов. Каждая топология отличается собственными особенностями и ограничениями, поэтому готовое решение должно легко поддаваться расширению и масштабированию. В этом случае его функциональность будет соответствовать условиям применения.
- ✓ **Подключенные устройства.** Какие устройства будут подключаться к сети? Кем они используются? Если гостям и подрядчикам со своими устройствами необходим доступ к сети LAN, об этом следует позаботиться в процессе выбора решения. Эффективное средство защиты периметра LAN включает функции, поддерживающие работу со всеми категориями подключаемых устройств и пользователей без вмешательства ИТ-специалистов. Технологии агрегирования каналов сравнительно легко обеспечивают растущую потребность конечных пользователей в пропускной способности, что упрощает задачи сетевых администраторов[6].
- ✓ **Низкая совокупная стоимость владения.** Даже если решение обладает всеми вышеперечисленными характеристиками, совокупная стоимость лицензирования, активации и подписки на отдельные службы может оказаться слишком высокой. Сетевые администраторы должны тщательно отбирать системы и решения, которые необходимо приобрести для обеспечения ожидаемого уровня защиты корпоративной сети, а также контролировать количество лицензий и наличие ключевых функций, требующих возобновления подписки.

  Более того, стоимость владения не сводится к первоначальному вложению средств и расходам на подписки. В зависимости от решения затраты времени на его развертывание и обслуживание могут быть разными. Руководители должны учитывать сложность управления решением. Готово ли оно к работе или требует внедрения различных «связующих» продуктов?

- ✓ **Интегрированная система безопасности.** Многие решения LAN лишены встроенных компонентов безопасности. В связи с этим специалистам приходится внедрять дополнительные элементы уже после развертывания решения, что усложняет структуру и влечет за собой новые расходы. Некоторые решения включают функции безопасности, однако они не интегрируются в периферию LAN. Это приводит к появлению уязвимостей сети — участков, где накапливаются несоответствия конфигураций, чем могут воспользоваться злоумышленники. Развертывание и обслуживание сетей должно происходить в контексте безопасности. Только так можно обеспечить максимально эффективную защиту без снижения управляемости инфраструктуры LAN в целом.

Для безопасного доступа необходимо комплексное решение

Проводные и беспроводные сети LAN не только лежат в основе корпоративной сети, но и требуют значительных затрат средств и ресурсов ИТ-отделов. Чтобы ИТ-специалисты и специалисты по безопасности могли в полной мере реализовать корпоративную стратегию, необходимо грамотно подбирать решения.

В настоящее время на рынке представлено множество поставщиков сетевого оборудования. Вице-президенты в сфере ИТ должны тщательно рассмотреть все доступные варианты и выбрать решение, которое обладает достаточной гибкостью развертывания на уровне доступа и включает интегрированные компоненты безопасности, обеспечивающие непрерывность работы.

[1] «In addition to traditional DDoS attacks, researchers see various abnormal traffic patterns», Help Net Security, 21 июля 2020 г.

[2] Там же.

[3] Эндрю Фрелих (Andrew Froehlich), «A Network's Weakest Link May be Different Than you Think», Network Computing, 26 ноября 2019 г.

[4] Там же.

[5] Там же.

FORTINET

www.fortinet.com/ru

февраля 9, 2021 11:23 AM

762006-0-1-RU