Требования к стратегии обеспечения сетевой безопасности: от SD-WAN до SASE

Развитие цифровых технологий побуждает организации модернизировать корпоративные сети и принимать меры, направленные на повышение удобства использования приложений сотрудниками и клиентами. В прошлом периметр сети представлял собой узкую область доступа к сетевой периферии, однако сейчас он охватывает ИТ-инфраструктуру в целом. В связи с этим появляются новые требования к безопасности центров обработки данных, глобальных сетей (WAN), локальных сетей (LAN) и облачной периферии. В последнее время пандемия COVID-19 акцентировала важность планов обеспечения непрерывной деятельности, которые предусматривают внедрение масштабируемых технологий, поддерживающих гибкий и безопасный удаленный доступ в любое время и из любой точки.

В то же время угрозы безопасности становятся все более изощренными, активность злоумышленников растет. Более трети утечек данных в 2020 г. обусловлены применением технологий социальной инженерии[1]. Это лишь один из примеров, свидетельствующих о важности модернизации корпоративных сетей с внедрением более эффективных средств защиты.

Продуманная **стратегия обеспечения сетевой безопасности** ускоряет сближение компонентов сети и безопасности в подключенной среде — всех периферийных областей и пользователей, от ядра к филиалам и облаку. При помощи этой стратегии организации могут обеспечить эффективную защиту современных динамичных сред, не снижая качество доступа сотрудников и клиентов.

Сети, в основе которых лежат компоненты безопасности, легко развиваются, расширяются и адаптируются к инновациям в цифровой сфере. Это ключевое требование вычислительных технологий следующего поколения, таких как гипермасштабирование, многооблачные среды, 5G и другие новейшие решения. Объединение сети и безопасности обеспечивает гибкую, всеобъемлющую, постоянную защиту.

Продуманная стратегия обеспечения сетевой безопасности ускоряет сближение компонентов сети и безопасности в подключенной среде — всех периферийных областей и пользователей, от ядра к филиалам и облаку.

Ключевые элементы стратегии обеспечения сетевой безопасности

Стратегия обеспечения сетевой безопасности решает три задачи:

- **Управление внешними и внутренними рисками, угрожающими пользователям сети**
- **Обеспечение гибкой защиты облака для пользователей, находящихся вне сети**
- **Повышение удобства пользователей и снижение расходов на обслуживание сетей WAN**

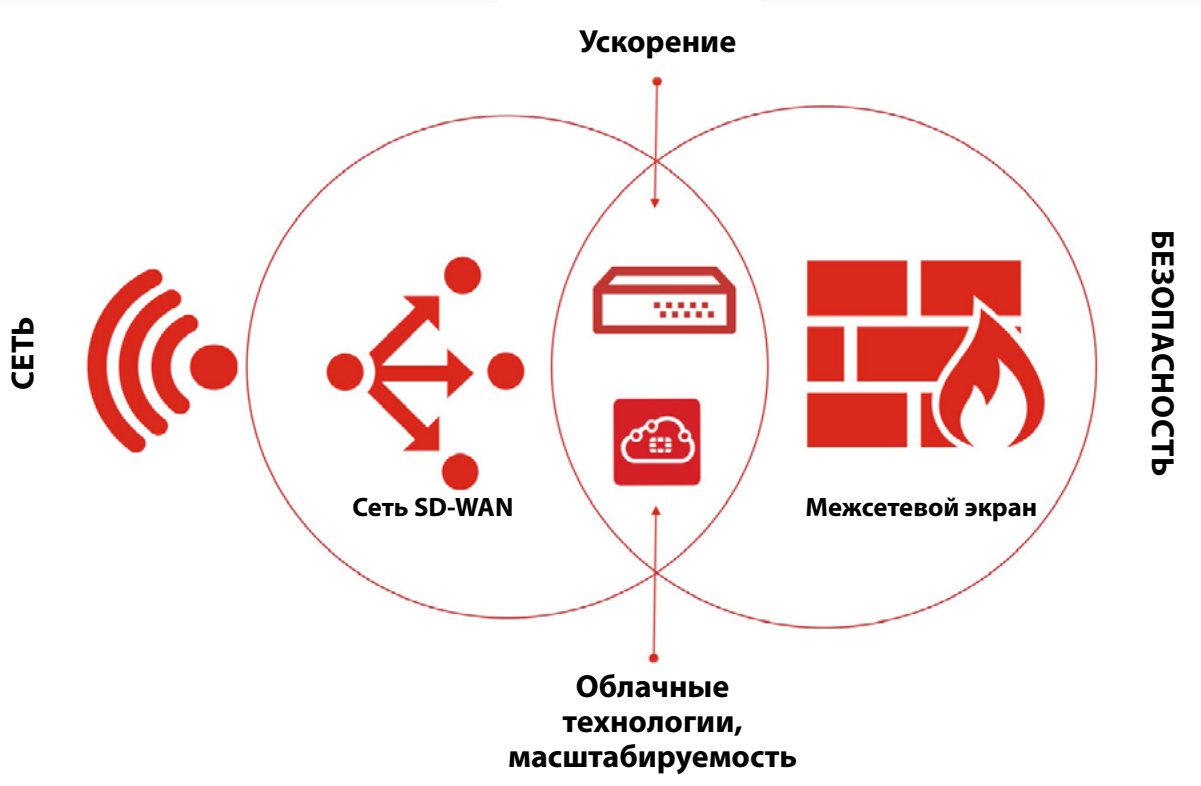
Первый этап обеспечения безопасности сети — это **развертывание настраиваемых процессоров безопасности**, или ASIC, с помощью которых сотрудники могут оперативно управлять сетями и безопасностью. Кроме того, они обеспечивают **консолидацию всех функций безопасности**, в том числе компонентов контроля приложений, межсетевых экранов и систем предотвращения вторжений (IPS) с формированием комплексных межсетевых экранов без ущерба для производительности и функциональности. Поддерживаются следующие варианты использования: безопасные программно-определяемые глобальные сети (SD-WAN), межсетевые экраны следующего поколения (NGFW), IPS, проверка на уровне защищенных сокетов (SSL), контроль приложений, веб-фильтрация, защита от вирусов и вредоносного ПО, «песочница» и ускоренная сегментация (последняя технология является одной из важнейших составляющих стратегии обеспечения сетевой безопасности, так как многие межсетевые экраны не справляются с обработкой дополнительных нагрузок, которые ложатся на них в процессе динамической внутренней сегментации).

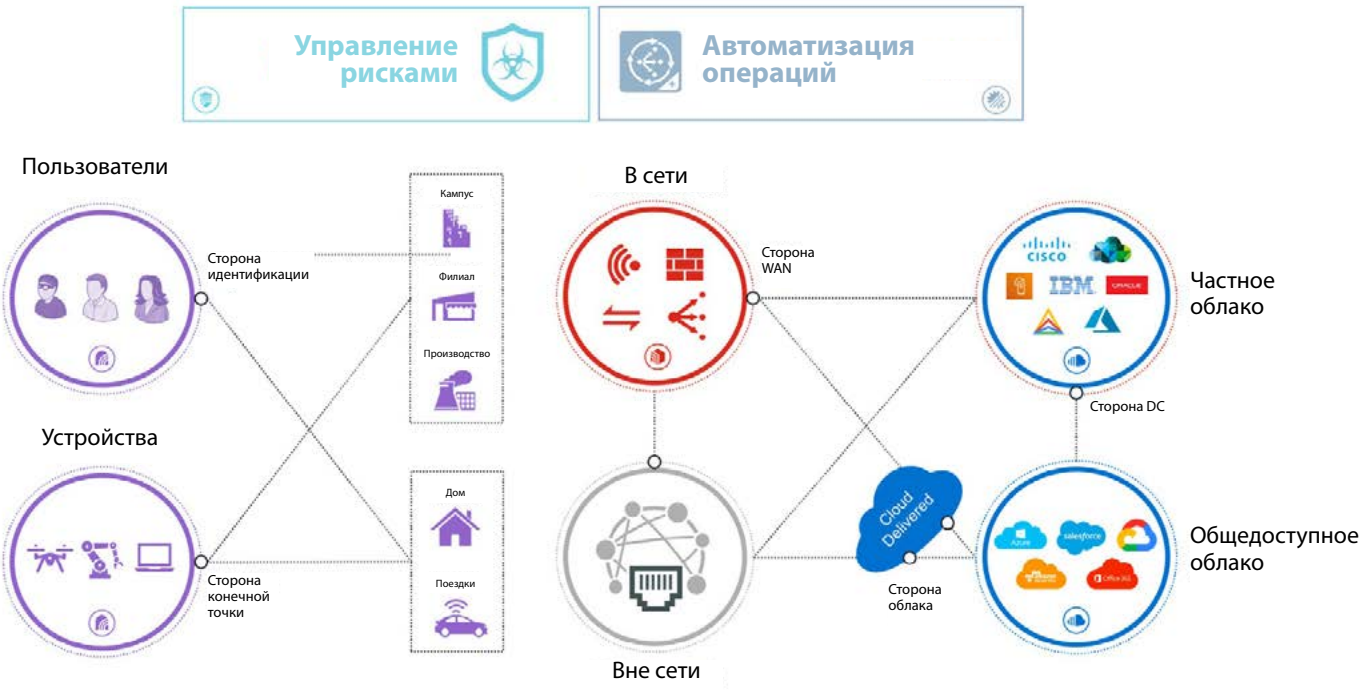
Специально разработанная облачная архитектура способствует сближению компонентов сети и безопасности в организациях, которые отдают приоритет облачным технологиям или находятся в поиске гибко развертываемых решений.

В дальнейшем межсетевые экраны должны будут обладать достаточной производительностью для **поддержки гибридных и гипермасштабируемых центров обработки данных, а также требований технологии 5G**. С распространением новых высокопроизводительных технологий, таких как «слоновьи» потоки, периферийные вычисления, защита HDTV и другого мультимедийного трафика, сети 5G и динамическая сегментация ядра, от решений NGFW потребуется беспрецедентно высокий уровень производительности. Однако в процессе разработки некоторых межсетевых экранов эта перспектива не учитывалась, поэтому они изначально лишены возможности подстроиться под требования будущего. Во многих случаях ситуацию не исправят даже огромные расходы.

Стратегия обеспечения сетевой безопасности преобразует периферию сетей WAN при помощи корпоративной технологии SD-WAN, полностью интегрированной в устройство NGFW. Эта интеграция обеспечивает полную безопасность самой сети **SD-WAN**, в отличие от некоторых технологий SD-WAN, нуждающихся в дополнительном уровне безопасности. Кроме того, эффективная стратегия SD-WAN также включает технологии прогнозной аналитики на базе искусственного интеллекта (ИИ), интуитивной оркестрации и самовосстановления.

И наконец, организации должны позаботиться о безопасности периферии проводных и беспроводных сетей за счет глубокой интеграции, которая обеспечивает постоянную и всеобъемлющую защиту периферии LAN. Таковы **характеристики работоспособных, быстро реагирующих сетей**, обеспечивающих безопасность доступа на сетевой периферии.





Помимо этого, периферийные области также нуждаются в **централизованном управлении**, что упрощает структуру и обеспечивает автоматизацию в целях повышения гибкости сети.

Основа безопасности облачной периферии: SASE

В 2020 г. и в настоящее время все обсуждения сетевой безопасности неизбежно сводятся к периферийным сервисам безопасного доступа (SASE – Secure Access Service Edge). SASE — это новая корпоративная инфраструктура, сочетающая функции сетевой безопасности и WAN, что удовлетворяет потребность современных организаций в динамическом безопасном доступе. Такой подход в полной мере соответствует стратегии обеспечения сетевой безопасности. SASE является ключевым компонентом новой концепции, согласно которой безопасность должна быть всеобъемлющей, в особенности на облачной периферии, а также на устройствах удаленных и мобильных пользователей.

Как правило, решение SASE относят к технологиям облачных вычислений, однако во многих случаях эффективная интеграция SASE в сеть требует совместного использования физических и облачных решений. Речь может идти о сочетании подключений SASE, элементов управления доступом к сети и устройств безопасности периметра, обеспечивающих поддержку физического устройства SD-WAN, в особенности устройства, включающего полный набор компонентов безопасности. Также возможна интеграция перечисленных элементов с контроллерами корпоративных беспроводных сетей LAN и точками доступа Wi-Fi в филиалах. Важно упомянуть, что благодаря SASE организации получают возможность **обеспечить постоянную защиту удаленных пользователей** вне зависимости от их местоположения, что повышает удобство работы и производительность периферийных подключений к специально разработанным облакам за счет использования оптимизированных путей с низкой задержкой.

Не следует путать решение SASE с комплексной стратегией обеспечения сетевой безопасности. Помимо ключевых компонентов защиты облака, о которых говорится в широко известном определении технологии SASE[2], надежное решение SASE должно поддерживать сетевую сегментацию и соответствовать требованиям, невыполнимым для облачных компонентов безопасности без полной блокировки облачного трафика на время проверки.

Именно такое решение SASE способно стать фундаментом комплексной стратегии обеспечения сетевой безопасности, эффективность и производительность которой соответствует требованиям современных организаций.

[1] «2020 Data Breach Investigations Report», Verizon, май 2020 г.

[2] «The Future of Network Security Is in the Cloud», Gartner, 13 сентября 2019 г.

февраля 10, 2021 8:04 PM

745599-0-1-RU