5 советов по выбору межсетевого экрана нового поколения

Сделайте выбор в пользу межсетевого экрана нового поколения (NGFW). Уточните, обеспечивает ли выбранное вами решение следующие возможности.

1 Предотвращение нарушений и расширенные функции безопасности

Предотвращайте атаки и быстро обнаруживайте вредоносное ПО, если оно проникнет внутрь сети.

Межсетевой экран предназначен в первую очередь для того, чтобы предотвращать нарушения и защищать вашу организацию от угроз. Но поскольку никакие профилактические меры не могут гарантировать абсолютную безопасность, в вашем межсетевом экране должны быть также расширенные функции для быстрого обнаружения сложного вредоносного ПО на тот случай, если оно обойдет первую линию защиты. Сделайте выбор в пользу межсетевого экрана со следующими возможностями и преимуществами.

- Система предотвращения вторжений для остановки атак прежде, чем будет нарушен периметр безопасности.
- Лучшая в своем классе встроенная система предотвращения вторжений нового поколения, позволяющая находить скрытые угрозы и быстро блокировать их.
- Фильтрация URL-адресов для применения заданных политик к сотням миллионов страниц.
- Встроенная «песочница» и инструменты защиты от сложного вредоносного ПО, непрерывно анализирующие поведение файлов, что позволяет оперативно выявлять и устранять угрозы.
- Возможность блокировки новых угроз благодаря последним аналитическим данным для брандмауэра, поступающим из международной организации по исследованию угроз.

2 Комплексный мониторинг сети

Чем шире обзор, тем больше угроз можно остановить.

Обеспечить защиту, действуя вслепую, невозможно. Вы должны знать, что происходит в вашей сети в любой момент времени, чтобы вовремя замечать подозрительное поведение и быстро принимать меры. Ваш межсетевой экран – это решение, призванное обеспечить вам целостную картину происходящего в сети и полную контекстуальную информацию для мониторинга следующих объектов и операций.

- Признаки вредоносной активности среди пользователей, на хостах, в сетях и на устройствах.
- Место и время возникновения угрозы, траектория ее распространения в вашей распределенной сети и ее статус в настоящий момент.
- Активные приложения и веб-сайты.
- Обмен данными между виртуальными машинами, передача файлов и т. д.

Дополнительные ресурсы

Ваш межсетевой экран способен на большее. Узнайте все о межсетевом экране нового поколения (NGFW) Cisco Firepower.

Обзор межсетевого экрана Cisco нового поколения

Демонстрация межсетевого экрана Cisco нового поколения

Отзыв заказчика: Downer Group

Посетите страницу https://www.cisco.com/c/ru_ru/products/security/firewalls/index.html

3 Многообразие вариантов управления и развертывания

Индивидуальная настройка с учетом уникальных потребностей организации.

Межсетевой экран любой организации – малой, средней или крупной – должен удовлетворять ее уникальным требованиям.

- Определите подходящий вариант управления для вашего сценария: встроенный диспетчер или централизованная система администрирования, охватывающая все устройства.
- Разверните решение в локальной среде или облаке с помощью виртуального межсетевого экрана.
- Индивидуализируйте продукт с учетом ваших потребностей – для доступа к расширенным функциям нужно просто активировать подписку на них.
- Выберите необходимую пропускную способность из широкого диапазона доступных значений.

4 Минимальное время обнаружения

Своевременно обнаруживайте вредоносное ПО и устраняйте риски безопасности.

Среднее время обнаружения угроз в отрасли сегодня составляет от 100 до 200 дней. Многовато, не правда ли?! От межсетевых экранов нового поколения требуется следующее.

- Обнаруживать угрозы за считаные секунды.
- Обнаруживать нарушение периметра безопасности за несколько часов или минут.
- Приоритизировать оповещения, чтобы оператор мог быстро принять необходимые меры для устранения угроз.
- Упростить жизнь заказчика за счет развертывания простой в обслуживании и согласованной политики, которая будет автоматически применяться на всех уровнях вашей организации.

5 Не отдельное решение, а часть экосистемы

Интегрированная архитектура безопасности обеспечивает возможность автоматизации и упрощает среду.

Межсетевой экран нового поколения не должен быть изолированным инструментом. Ему необходимо обмениваться данными и взаимодействовать с другими компонентами вашей архитектуры безопасности. При выборе обратите внимание, реализованы ли следующие функции.

- Простая интеграция с другими инструментами того же поставщика.
- Автоматический обмен информацией об угрозах, данными о событиях, а также сведениями о политиках и контексте с системами защиты электронной почты, веб-трафика, оконечных устройств и сети.
- Автоматизация таких задач, как оценка последствий, настройка политик и идентификация пользователей.