



# Межсетевой экран нового поколения Cisco Firepower NGFW

**Первый в отрасли полностью интегрированный межсетевой экран нового поколения с активной защитой от угроз до, во время и после сетевых атак**

Большинство межсетевых экранов нового поколения (NGFW) ориентированы преимущественно на контроль приложений, но не на собственные функции защиты от угроз. Чтобы компенсировать это, некоторые разработчики NGFW попытаются дополнить свою систему предотвращения вторжений первого поколения набором неинтегрированных вспомогательных функций и компонентов. Однако такой подход не способен защитить ваш бизнес от современных киберпреступников и сложного вредоносного ПО. Кроме того, при заражении вашей системы подобные устройства никак не смогут распознать его тип, предотвратить распространение и быстро устранить последствия.



С этими задачами справится лишь интегрированный, ориентированный на угрозы межсетевой экран нового поколения. Такая система гарантирует тщательный контроль за работой приложений и эффективную защиту от угроз со стороны сложных и трудно обнаруживаемых атак вредоносного ПО.

Межсетевой экран нового поколения Cisco Firepower™ — это первое в отрасли полностью интегрированное решение с активной защитой от угроз до, во время и после сетевой атаки. Оно обеспечивает комплексное, унифицированное управление политиками функций межсетевого экрана, контроль приложений, предотвращение угроз и защиту от сложного вредоносного ПО — начиная с сети и заканчивая устройствами, подключенными к ней.

Это решение можно развернуть на устройствах Cisco Firepower 4100 и 9300 и таким образом получить оптимизированную по производительности и плотности платформу (сетевой) безопасности на основе NGFW для интернет-периметра, а также высокопроизводительных сред.

## Защитите свою организацию до, во время и после сетевой атаки

Межсетевой экран нового поколения Cisco Firepower также включает в себя наиболее широко применяемый в отрасли межсетевой экран с контролем состояния соединений и обеспечивает детальный контроль более чем 4000 коммерческих приложений. Его единый интерфейс управления позволяет осуществлять унифицированный мониторинг как самой сети, так и конечных устройств. Firepower NGFW обеспечивает полное управление политиками, которое подразумевает контроль доступа, блокирование атак и защиту от вредоносного ПО, а также предоставляет интегрированные средства для отслеживания и сдерживания атак и восстановления после атак, которым все же удалось обойти уровни защиты.

## Преимущества

- **Блокируйте большее угроз** — как известных, так и неизвестных — с помощью самого эффективного в отрасли решения защиты от угроз.
- **Получите полную картину происходящего в сети** и возможность контроля над пользователями, приложениями, устройствами, угрозами и уязвимостями в вашей сетевой среде.
- **Обнаруживайте угрозы раньше и реагируйте на них быстрее:** сократите время на поиск вредоносного ПО с нескольких месяцев до нескольких часов и оперативно нейтрализуйте атаки.
- **Уменьшите сложность** и упростите себе задачу, собрав все функции информационной безопасности в единый интерфейс управления.
- **Сделайте вашу сеть эффективнее** за счет интеграции с другими сетевыми решениями и средствами безопасности Cisco.

Cisco Firepower NGFW – это единственный на сегодня межсетевой экран нового поколения, который:

- Предоставляет систему предотвращения вторжений нового поколения (NGIPS) для лучшей в отрасли защиты от угроз.
- Включает в себя полностью интегрированное решение защиты от сложного вредоносного ПО (AMP) для эффективной борьбы с известными угрозами и угрозами нулевого дня, а также технологию «песочницы».
- Дает возможность отслеживать и сдерживать заражения вредоносным ПО.
- Автоматически сопоставляет случаи возникновения угроз с уязвимостями в вашей сетевой среде, позволяя направить все силы на борьбу с наиболее критическими угрозами.
- Анализирует слабые места в вашей сети и рекомендует к применению оптимальные политики безопасности.
- Интегрируется со множеством продуктов Cisco® для сетевой безопасности, что дает возможность максимально эффективно использовать ранее внедренные решения и гарантировать более высокий уровень информационной безопасности.

### Дальнейшие шаги

Дополнительную информацию можно получить, посетив наш веб-сайт по адресу [www.cisco.com/go/NGFW](http://www.cisco.com/go/NGFW).