Антивирус Касперского

для Juniper SSG, SRX и J-Series

JUNIPER NETWORKS

Высокая скорость работы, сверхбыстрая реакция на новые угрозы и высочайший уровень их обнаружения

Проблемы

информационной безопасности

Современные интернет-угрозы с каждым днём становятся всё более изощрёнными и опасными. Сегодня вредоносные программы – вирусы и черви, троянцы, шпионские модули и спам-боты – преследуют одну цель: захват контроля над компьютерами пользователей. Вредоносное ПО не только приносит финансовые убытки, но также способно вызвать утечку конфиденциальной информации и снижение производительности труда, а кроме того, часто наносит ущерб деловой репутации предприятия.

Решение

защита с помощью устройств Juniper и Антивируса Касперского

Обеспечение антивирусной безопасности на уровне интернет-шлюза является необходимым первым эшелоном защиты современной корпоративной сети (второй эшелон – это защита на уровне сервера, а третий – на уровне рабочих станций). Защита на уровне интернет-шлюза имеет следующие преимущества:

- **Значительное повышение общего уровня защиты** – большая часть быстро распространяющихся угроз перехватывается до их попадания в сеть.
- **Повышение производительности работы и масштабируемости сети** – несколько сетевых шлюзов могут работать в одной сети в параллельном режиме.
- **Оптимальное использование ресурсов** – электронное письмо, отправленное злоумышленником на множество адресов, достаточно просканировать и заблокировать всего один раз.

J-2320

SRX100

SSG140

SSG550

J-6350

SRX650

KASPERSKY lab

Антивирус Касперского для Juniper SSG, SRX и J-Series

Оптимальная защита сети

Благодаря интеграции с сетевым антивирусным решением мирового класса от «Лаборатории Касперского», устройства Juniper Networks обеспечивают надежную защиту сетевого трафика и электронной почты от вирусов, червей, шпионских программ, троянцев и других типов вредоносного ПО. Устройства сканируют весь входящий и исходящий трафик в соответствии с настройками политики безопасности, обеспечивая защиту как от внешних, так и от внутренних угроз. В отличие от прочих интегрированных антивирусных решений, основанных на простой проверке пакетов или поиске известных сигнатур, совместное решение Juniper и «Лаборатории Касперского» способно выполнять поиск вредоносного кода в файлах и архивах тысяч форматов.

Подавляющее большинство вредоносных программ проникают в корпоративные сети внутри заархивированных, сжатых или упакованных файлов. Решение «Лаборатории Касперского» поддерживает максимальное количество архиваторов и упаковщиков. Данное преимущество позволяет значительно повысить уровень безопасности в сети: входящие угрозы перехватываются шлюзом, даже если они скрыты в сжатом файле – например, в архиве, вложенном в электронное письмо.

Совместное решение Juniper Networks и «Лаборатории Касперского» обнаруживает и блокирует все известные типы вирусов, червей, похитителей паролей, троянов и прочих вредоносных программ. Предлагаемое решение также детектирует потенциально опасные программы, в том числе шпионское и рекламное ПО. Оптимальное сочетание сигнатурного и проактивного методов гарантирует практически 100% уровень обнаружения самых опасных, распространенных и последних зловредов с нулевой вероятностью ложных срабатываний.

В отличие от ряда решений, использующих отдельные сканеры для поиска отдельных типов вредоносного ПО, решение Juniper Networks и «Лаборатории Касперского» включает в себя единый универсальный сканер, базу сигнатур и модуль обновлений, обеспечивающие защиту сети от всех вредоносных программ.

Особенности и преимущества

Антивируса Касперского для Juniper SSG, SRX и J-series

Антивирус Касперского (Full AV)

Антивирусное ядро «Лаборатории Касперского» используется системой JUNOS для сканирования файлов. Когда сканирование включено, шлюз SSG/SRX Series или маршрутизатор J Series анализируют потоки данных, проверяя сообщения электронной почты, файлы, передаваемые по протоколу FTP, а также скрипты и файлы, загружаемые при просмотре страниц в интернете.

После того как шлюз направляет файл на сканирование, этот файл или скрипт сохраняется в кэше, а ядро антивируса сканирует его на все виды известного вредоносного кода. При обнаружении вируса файл удаляется, а пользователю направляется соответствующее уведомление.

При использовании традиционного антивирусного решения необходимо учитывать следующие факторы:

- Full AV обеспечивает высокий уровень обнаружения вредоносного ПО, так как использует большую базу антивирусных сигнатур и сканирует файлы целиком из кэша.
- Full AV позволяет сканировать сжатые файлы, поскольку файл в кэше можно разархивировать до начала сканирования.
- Размер сканируемых файлов ограничен только объёмом доступной памяти.
- Full AV замедляет работу шлюза, поскольку пересылаемые файлы сохраняются локально.
- Количество файлов, сканируемых параллельно, ограничивается только объёмом доступной памяти и вычислительной мощностью процессора.

Особенности:

- Эффективное сочетание технологий обнаружения на основе сигнатурных и проактивных методов
- Поддержка всех известных форматов файлов (более 4000 форматов)
- Регулярные обновления антивирусных баз
- Внеочередные обновления в случае эпидемии
- Уникальная технология фильтрации и оптимизация производительности антивируса для защиты корпоративных сетей

Преимущества:

- Высокий уровень обнаружения всех самых опасных, распространенных и новейших вредоносных и потенциально опасных программ с практически нулевым уровнем ложных срабатываний
- Быстрое обнаружение новых и наиболее опасных вредоносных программ
- Минимизация ущерба в случае заражения одного из компьютеров в сети

KASPERSKY lab

Juniper ExpressAV

Компания Juniper добавила в свои продукты SRX и J-series модуль сканирования ExpressAV на потоках данных, который обнаруживает вирусы с помощью сигнатурного метода. При этом достигается увеличение производительности сканирования. Несколько сниженный уровень обнаружения вирусов компенсируется возможностью защиты от самых последних и опасных, а также наиболее распространённых вредоносных программ. Модуль ExpressAV использует модифицированные базы сигнатур «Лаборатории Касперского».

У такого подхода к сканированию есть ряд особенностей, таких как:

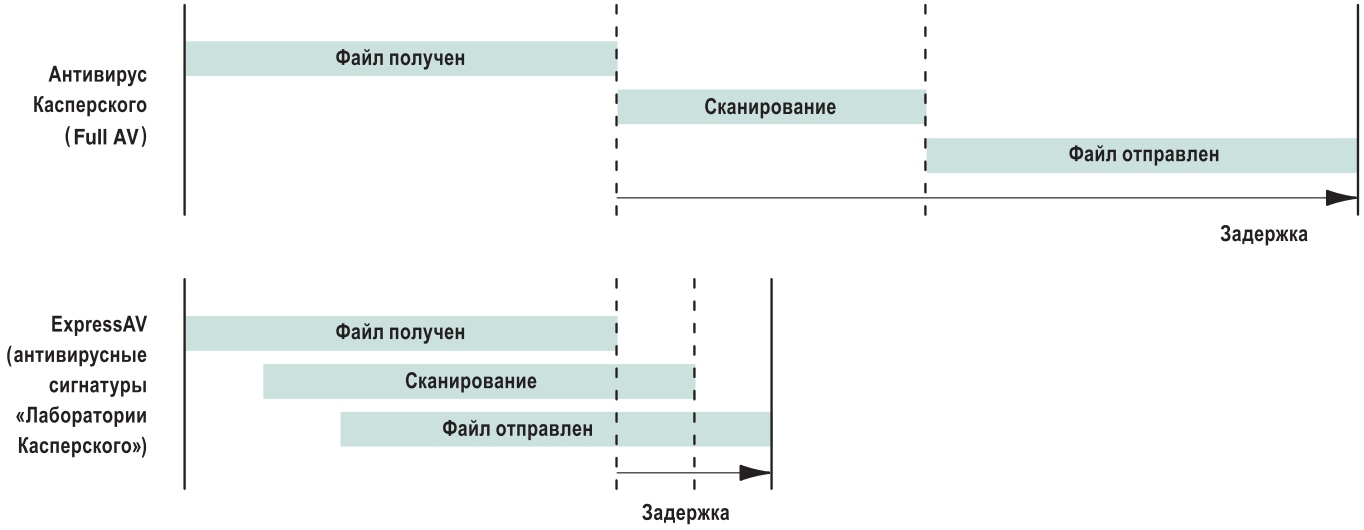
- Уровень обнаружения ExpressAV ниже, чем у полного антивируса, однако ExpressAV успешно обнаруживает наиболее распространённые вирусы.
- ExpressAV не обнаруживает полиморфные и метаморфные вирусы, которые могут изменять своё тело, поскольку в модуле ExpressAV нет необходимых для этого эвристических алгоритмов.
- Сканирование сжатых файлов поддерживается для потоковых алгоритмов архивирования (например, ZIP, GZIP, TAR), а сканирование многократно сжатых файлов не поддерживается.

При этом Juniper ExpressAV обладает следующими преимуществами:

- ExpressAV поддерживает аппаратное ускорение, обеспечивая за счёт этого более высокую пропускную способность шлюза.
- В ряде случаев кэширование файлов не производится, что увеличивает производительность всего решения.
- При использовании ExpressAV задержки передачи данных минимальны, поскольку пакеты могут пересылаться параллельно со сканированием, как это показано на схеме.

Схема сравнения

скорости сканирования



Как приобрести

Лицензия на Антивирус Касперского продается вместе с оборудованием SSG, SRX и J-series через партнеров компании Juniper Networks.

Технологии «Лаборатории Касперского» доступны в двух вариантах – как часть системы унифицированной защиты от угроз (Unified Threat Management, UTM) и отдельно. Доступны версии на 30 дней для тестирования.

Подробности о распространении лицензий на Антивирус Касперского уточняйте, пожалуйста, у партнеров компании Juniper Networks.

Антивирус Касперского для Juniper SSG, SRX и J-Series

Спецификация

Антивируса Касперского для устройств Juniper

Сканирование протоколов	SMTP, POP3, FTP, IMAP, HTTP
Сканирование входящего / исходящего трафика	Да/Да
Время реагирования на появление новых вирусов	~ 30 минут
Количество вирусных сигнатур	> 480 000
Поддерживаемые форматы архиваторов и упаковщиков	ACE, ARJ, Alloy, Astrum, BZIP2, BestCrypt, CAB, CABSFX, CHM, Catapult, CaveSFX, CaveSetup, ClickTeam, ClickTeamPro, Commodore, CompiledHLP, CreateInstall, DiskDupe, DiskImage, EGDial, Effect Office, Embedded, Embedded Class, Embedded EXE, Embedded MS Expand, Embedded PowerPoint, Embedded RTF, FlyStudio, GEA, GKWare Setup, GZIP, Gentee, Glue, HA, HXS, HotSoup, Inno, InstFact, Instyler, IntroAdder, LHA, MS Expand, MSO, Momma, MultiBinder, NSIS, NeoBook, OLE files, PCAcme, PCCrypt, PCInstall, PIMP, PLCreator, PaquetBuilder, Perl2Exe, PerlApp, Presto, ProCarry, RARv 1.4 and above, SEA, SbookBuilder, SetupFactory, SetupSpecialist, SilverKey, SmartGlue, StarDust Installer, Stream 1C, StubbieMan, Sydex, TSE, Tar, Thinstall, ViseMan, WinBackup, WiseSFX, ZIP, 7-Zip
Поддерживаемые форматы веб-контента	pif, lnk, reg, ini (Script.Ini, etc), cla (Java Class), vbs (Visual Basic Script), vbe (Visual Basic Script Encrypted), js (Java Script), jse (Java Script Encrypted), htm, html, htt (HTTP pages), hta - HTA (HTML applications), asp (Active Server Pages), chm – CHM (compressed HTML), pht – PHTML, php – PHP, wsh, wsf, the (.theme)
Поддерживаемые форматы файлов MS Office	doc, dot, fpm, rtf, xl*, pp*, md*, shs, dwg (Acad2000), msi (MS Installer), otm (Outlook macro), pdf (AcrobatReader), swf (ShockwaveFlash), prj (MapInfo project), jpg, jpeg, emf (Enhanced Windows Metafile), elf
Поддерживаемые форматы исполняемых файлов DOS	com, exe, sys, prg, bin, bat, cmd, dpl (Borland's Delphi files), ov*
Поддерживаемые форматы исполняемых файлов WIN	dll, scr, cpl, ocx, tsp, drv, vxd, fon 386
Поддерживаемые форматы e-mail	eml, nws, msg, plg, mbx (Eudora database)
Поддерживаемые форматы файлов справки	hlp
Прочие поддерживаемые форматы файлов	sh, pl, xml, itsf, reg, wsf, mime, rar, pk, lha, arj, ace, wmf, wma, wmv, ico, efi

О компании Juniper Networks

Juniper Networks является лидером в области современных сетевых технологий. Компания производит высокопроизводительное сетевое оборудование, позволяющее обеспечить ускоренное внедрение новых услуг и приложений, необходимых современным высокорентабельным предприятиям. Дополнительная информация на сайте: www.juniper.net.

О «Лаборатории Касперского»

«Лаборатория Касперского» – самый популярный в России и крупнейший в Европе производитель систем защиты от вредоносного и нежелательного ПО, хакерских атак и спама, входит в четверку ведущих мировых производителей программных решений для обеспечения информационной безопасности. Продукты компании надежно защищают компьютеры и мобильные устройства более 250 млн пользователей во всем мире, технологии используются в продуктах крупнейших мировых поставщиков программных и аппаратных решений. «Лаборатория Касперского» представляет собой группу компаний с центральным офисом в Москве, пятью региональными дивизионами и десятками локальных представительств. Подробнее на www.kaspersky.ru

KASPERSKY lab