Предотвращение угроз

Комплексное управление защитой вашей сети от вредоносного кода и программного обеспечения

Организации постоянно подвергаются шквалу атак со стороны злоумышленников, ищущих легкой наживы. Современные злоумышленники сильно отличаются от тех, которые существовали 15 лет назад. Они используют хитроумную тактику для проникновения в вашу сеть незаметно для традиционных средств сетевой защиты: от подмены пакетов и шифрования до многофазной полезной нагрузки и быстрого потока DNS.

Сервисы предотвращения угроз, специально встроенные в платформу безопасности следующего поколения, защищают сети от широкого спектра угроз.

- **Проверка всего трафика в контексте приложений и пользователей**
- **Предотвращение угроз на всех этапах жизненного цикла кибератаки**
- **Архитектура однопроходной проверки для высокой производительности даже при включении всех функций предотвращения угроз**
- **Единая таблица политик для упрощения управления**
- **Ежедневные автоматические обновления для защиты от нового вредоносного ПО и опасных DNS**

Ситуация значительно усложняется тем, что в средствах обеспечения сетевой безопасности до сих пор используются те же стратегии защиты, что и раньше, до расширения существующих угроз. Трафик проверяется только на определенных портах, а добавление однофункциональных устройств в систему защиты, конечно, устраняет проблемы, но снижает наглядность и производительность. Все это создает опасную уязвимость сетевой защиты, поскольку средства обеспечения безопасности разрознены и трудно управляемы, а злоумышленники все ловчее проникают через них.

Palo Alto Networks® полностью переосмысливает подход к сетевой безопасности со своей платформой для предотвращения угроз на основе принципа нулевого доверия. Мы обеспечиваем безопасный доступ к приложениям с помощью защиты от усовершенствованных угроз на всех этапах жизненного цикла кибератаки, для чего используется многофункциональная платформа, анализирующая трафик на всех портах и протоколах за один проход.

Доступ к приложениям, предотвращение угроз

Приложения являются неотъемлемой частью ведения бизнеса, и поэтому пользователи все чаще обращаются к ним по зашифрованным сетевым каналам, через нестандартные номера портов и путем перехода между открытыми портами для обеспечения постоянного доступа.

К сожалению, усовершенствованные угрозы также используют эти новые способы предоставления приложений пользователям и дают злоумышленникам незаметно проникать в сеть. Они применяют туннелирование, скрываются в трафике с шифрованием SSL и входят в доверие ничего не подозревающих пользователей для захвата сети и выполнения злонамеренных действий.

Palo Alto Networks защищает вашу сеть от таких угроз с помощью многоуровневого предотвращения на всех этапах атаки. Подписка на программу Threat Prevention включает Intrusion Prevention, защиту сети от вредоносного и шпионского ПО и предотвращает усовершенствованные угрозы в сети путем определения и проверки всего трафика (приложений, пользователей и данных) вне зависимости от шифрования, для всех портов и протоколов.

Предотвращение угроз любой ценой

Практически во всех случаях нарушения безопасности у подвергавшейся атаке организации было однофункциональное средство защиты, которое обошли злоумышленники. Palo Alto Networks использует собственные встроенные защитные технологии, которые позволяют предотвратить угрозу, даже если одна из технологий ее пропустила. Ключом к успешной защите являются защитные функции специального назначения, обеспечивающие обмен информацией и предоставляющие контекст для проверяемого трафика и выявляемых и предотвращаемых угроз.

Рекомендованная безопасность

Palo Alto Networks — единственный поставщик со 100 % блокированием всех теневых вредоносных кодов по результатам теста IPS-систем следующего поколения NSS Labs 2015.

Intrusion Prevention

Механизм защиты от угроз обнаруживает и блокирует попытки внедрения вредоносного кода и злонамеренных технологий на уровне сети и приложений, включая сканирование портов, переполнение буфера, выполнение удаленного кода, фрагментацию протоколов и подмену пакетов. Защита основана на сопоставлении подписей и выявлении аномалий, которые включают дешифрование и анализ протоколов и использование полученной информации для оповещения об опасном трафике и его блокирования. Сопоставление шаблонов с отслеживанием состояния обнаруживает атаки по нескольким пакетам, учитывая порядок получения и последовательность и проверяя безопасность всего разрешенного трафика и отсутствие вредоносных программ.

- Анализ протокола на основе дешифратора выполняет дешифровку протокола с отслеживанием состояния и интеллектуальное добавление подписей для обнаружения вредоносного кода в сети и приложениях.
- Поскольку одну уязвимость можно использовать несколькими способами, наши подписи Intrusion Prevention создаются на основе самой уязвимости, что обеспечивает более высокую степень защиты от различного вредоносного кода. Одна подпись может предотвратить несколько попыток внедрения вредоносного кода через известную уязвимость сети или приложения.
- Защита протоколов на основе выявления аномалий обнаруживает не соответствующее RFC использование протокола, такое как слишком длинный URI или вход на FTP.
- Эвристический анализ определяет аномальные пакеты и шаблоны трафика, такие как сканирование портов, развертка узлов и атаки DoS.
- Другие функции защиты от атак, такие как блокирование некорректных или неправильно сформированных пакетов, дефрагментация IP и переборка TCP, применяются для защиты от методов внедрения вредоносного кода и подмены пакетов, используемых злоумышленниками.
- Легко настраиваемые пользовательские подписи уязвимости позволяют адаптировать функции Intrusion Prevention к требованиям сети.

Помимо этих традиционных функций Intrusion Prevention, Palo Alto Networks предоставляет уникальную функцию обнаружения и блокирования угроз на всех портах, вместо применения подписей для ограниченного набора встроенных портов. Используя App-ID™ в нашем брандмауэре следующего поколения, который проверяет весь трафик на всех портах, механизм предотвращения угроз не пропускает ни одной угрозы, независимо от порта.

Защита от вредоносного ПО

Встроенная защита от вредоносного ПО блокирует такие программы до их проникновения в целевой узел с помощью подписей, основанных на полезной нагрузке, а не хэше. Защита от вредоносного ПО компании Palo Alto Networks блокирует известные вредоносные программы и все их варианты, включая те, которые ранее не встречались. Механизм потокового сканирования защищает сеть без снижения скорости передачи данных, что обычно свойственно сетевым антивирусам, в которых используются механизмы сканирования на базе прокси-сервера. Потоковое сканирование вредоносного ПО от компании Palo Alto Networks проверяет трафик сразу же после получения первых пакетов файла и предотвращает угрозы, а также позволяет решить проблемы производительности, присущие традиционным автономным решениям. Основные функции защиты от вредоносного ПО:

- встроенное потоковое обнаружение и устранение вредоносного ПО, спрятанного в сжатых файлах и веб-содержимом;
- защита от полезной нагрузки, скрытой в общих типах файлов, таких как документы Microsoft® Office® и PDF;
- обновления из WildFire, обеспечивающие защиту от нового вредоносного ПО, которое использовалось в последних известных атаках.

Подписи для всех типов вредоносного ПО создаются напрямую из миллионов реальных образцов, собранных Palo Alto Networks, включая ранее неизвестные образцы, отправленные в WildFire, глобальную сеть ловушек для злоумышленников и другие ведущие исследовательские организации мира.

Защита от командного (шпионского) ПО

Нам хорошо известно, что универсальной защиты от всех возможных сетевых угроз не существует. После первого заражения злоумышленники взаимодействуют с хост-компьютером по каналу управления и контроля (CnC), передавая дополнительное вредоносное ПО и другие инструкции и воруя данные. Наши средства защиты от такого вторжения проникают в канал несанкционированной связи и отрезают

ПОДПИСИ НА БАЗЕ СОДЕРЖИМОГО/ХЭША

Подписи на базе содержимого, то есть полезной нагрузки, позволяют обнаруживать модели в тексте файла, которые указывают, что файл должен сделать.

Подписи на базе хэша анализируют фиксированную кодировку файла. Поскольку хэш файла легко изменить, подписи на базе хэша неэффективны для обнаружения полиморфного вредоносного ПО или вариантов одного файла.

Использование подписей на базе хэша похоже на определение свежести содержимого ящика только по оформлению ящика, не заглядывая внутрь.

злоумышленников, блокируя исходящие запросы на опасные домены и из известных инструментов CnC, установленных на зараженных устройствах.

DNS Sinkhole

Наша защита CnC также предоставляет функции Sinkhole для исходящих запросов к опасным DNS, предотвращая проникновение и точно определяя цель злоумышленников. Настройте Sinkhole так, чтобы все исходящие запросы к опасным доменам и IP-адресам перенаправлялись на один из внутренних IP-адресов сети.
В результате коммуникация CnC будет блокирована, и такие запросы не смогут покинуть сеть вне зависимости от их частоты и времени, а также будет составлен отчет по узлам сети, отправляющим эти запросы.
Специалисты по обработке инцидентов получат ежедневные списки зараженных машин для принятия мер без какой-либо спешки, поскольку каналы воздействия злоумышленников уже отрезаны.

WildFire

Информация о защите от нового обнаруженного вредоносного ПО и доменов CnC ежедневно передается в библиотеки защиты Threat Prevention через WildFire™, нашу виртуальную среду для анализа вредоносного ПО, что обеспечивает актуальность защиты и предотвращение всех новейших усовершенствованных угроз на всех этапах жизненного цикла атаки.

Автоматические объекты корреляции

Palo Alto Networks поддерживает выявление усовершенствованных угроз через мониторинг и корреляцию сетевого трафика и журналов угроз, что позволяет быстро обнаруживать зараженных пользователей и анализировать странные модели поведения. Объекты корреляции используют данные исследований угроз подразделением Unit 42, результаты анализа незнакомых угроз из WildFire, а также User-ID™ для сопоставления аномалий трафика и индикаторов заражения и быстрого и точного определения зараженных сетевых устройств. Неизвестные или аномальные TCP и UDP и различные подозрительные модели поведения, такие как повторяющаяся загрузка, использование динамического DNS, попытки внедрения вредоносного кода и другие события отслеживаются и объединяются в оповещения со списком зараженных пользователей и соответствующими индикаторами заражения.

Комплексный мониторинг и снижение риска

Дешифрование SSL

Практически 40 % корпоративного сетевого трафика шифруется с помощью SSL, что создает уязвимость сетевой защиты, если не выполняются дешифрование и проверка на угрозы. Наша платформа имеет встроенное дешифрование SSL, которое можно использовать для выборочного дешифрования входящего и исходящего трафика SSL. После дешифрования трафика и подтверждения его безопасности он снова шифруется и отправляется по адресу назначения.

Блокирование файлов

Около 90 % вредоносных файлов, используемых в атаках целевого фишинг-мошенничества, является выполняемыми. Это, а также 59 % инцидентов в системе безопасности, связаны с недосмотром сотрудников, то есть пользователи не знают, что опасно. Для снижения риска заражения вредоносным ПО можно запретить передавать в сеть опасные типы файлов, в которых часто скрываются вредоносные программы, например, выполняемые файлы. Функции блокирования файлов можно комбинировать с User-ID для блокирования лишних файлов на основе должностных функций пользователей, чтобы все пользователи имели доступ только к нужным файлам и риск заражения снижался точечно с учетом различных требований организации. Для дальнейшего снижения вероятности атак можно отправлять все разрешенные файлы на анализ в WildFire для проверки на наличие нового вредоносного ПО.

Защита от теневой загрузки

Не подозревающие об опасности пользователи могут случайно загрузить вредоносное ПО, просто посетив интересную веб-страницу. Зачастую пользователь и даже владелец веб-сайта не знает, что страница заражена. Palo Alto Networks определяет потенциально опасные загрузки и выводит пользователю предупреждение, чтобы исключить случайные и неразрешенные загрузки. Для предотвращения атак из новых и быстро изменяющихся доменов эту функцию можно связать с фильтрацией URL и политиками блокирования файлов.

Использование глобальной аналитики угроз для предотвращения атак

Подробные журналы всех угроз не просто находятся в одном интерфейсе управления, а совместно используются всеми механизмами предотвращения для предоставления контекста. Благодаря WildFire глобальная аналитика угроз применяется нами для автоматического обнаружения незнакомого вредоносного ПО и обеспечения постоянной защиты всей клиентской базы от новейших усовершенствованных угроз.

Пассивный мониторинг DNS

Для защиты организации от быстро изменяющихся вредоносных программ и веб-сайтов можно использовать анализ на основе DNS компании Palo Alto Networks. Пассивный мониторинг DNS позволяет использовать большие объемы аналитических данных, которые передаются в нашу базу опасных доменов и на основе которых в дальнейшем нами формируется защита для всей клиентской базы.

Исследования мирового уровня

Исследователи Palo Alto Networks — это специалисты мирового уровня, которые занимаются выявлением и анализом угроз, приложений и соответствующего сетевого поведения. Наши специалисты работают над защитой от обширного списка вредоносных кодов путем обратного инжиниринга уязвимостей. Каждый год исследователи Palo Alto Networks обнаруживают и публикуют больше уязвимостей продуктов Microsoft, чем другие поставщики систем защиты.

Palo Alto Networks также включает подразделение Unit 42, эксперты которого анализируют данные угроз, собранные мировым сообществом, для определения и расследования новых способов атаки, вредоносного ПО и текущих кампаний и выявления актуальных трендов хакерства.

Однопроходное сканирование всех угроз

Механизм Threat Prevenion компании Palo Alto Networks является лидером отрасли по проверке и классификации трафика, а также обнаружению и блокированию вредоносного ПО и кода, угрожающего уязвимостям, за один проход.

Традиционные технологии предотвращения угроз требуют двух и более механизмов сканирования, что значительно замедляет операции и снижает производительность. Palo Alto Networks использует единый формат подписи для всех угроз, что обеспечивает быструю обработку, так как все операции анализа выполняются в одном комплексном проходе и исключаются лишние процессы, присущие решениям с несколькими механизмами сканирования.

Наша технология предотвращения угроз проверяет каждый пакет, проходящий через платформу, и детально анализирует последовательности байтов в заголовке пакета и полезной нагрузке. На основе этого анализа определяются важные сведения о пакете, включая используемое приложение, источник и цель, совместимость протокола с RFC и наличие в полезной нагрузке вредоносного кода или ПО. Помимо отдельных пакетов, также анализируется контекст, формируемый порядком получения и последовательностью нескольких пакетов, для обнаружения и предотвращения проникновения. Все эти операции по анализу и сопоставлению подписей выполняются за один проход, поэтому скорость передачи данных не снижается

.

Пропускная способность при предотвращении угроз

Модель	Пропускная способность
PA-200	50 Мбит/с
PA-500	100 Мбит/с
PA-2020	200 Мбит/с
PA-2050	500 Мбит/с
PA-3020	1 Гбит/с
PA-3050	2 Гбит/с
PA-3060	2 Гбит/с
PA-5020	2 Гбит/с
PA-5050	5 Гбит/с
PA-5060	10 Гбит/с
PA-7050	100 Гбит/с*
PA-7080	160 Гбит/с*

*С поддержкой DSRI

4401 Great America Parkway
Santa Clara, CA 95054

Основной тел.: +1-408-753-4000
Отдел продаж: +1-866-320-4788
Служба поддержки: +1-866-898-9087

www.paloaltonetworks.com

© Palo Alto Networks, Inc, 2015. Название «Palo Alto Networks» является зарегистрированным торговым знаком компании Palo Alto Networks. Список наших торговых знаков можно просмотреть по адресу http://www.paloaltonetworks.com/company/trademarks.html. Все остальные товарные знаки, упоминаемые в данном документе, могут быть товарными знаками соответствующих компаний. **PAN_DS_USGSS_082115**