РУКОВОДСТВО ДЛЯ ПОКУПАТЕЛЕЙ МЕЖСЕТЕВЫХ ЭКРАНОВ

Подробное руководство для оценки межсетевых экранов для корпоративных сетей.

paloalto NETWORKS®

the network security company™

Изменения порождают инновации

Даже при более усовершенствованных функциях и высокой пропускной способности, чем это было раньше, межсетевые экраны недостаточно эффективно справляются с задачами идентификации. Характер угроз стремительно меняется, и традиционная фильтрация по портам и IP-адресам больше не позволяет их остановить.

Введение

Вне сомнения, ваша сеть стала намного сложнее, чем раньше. Ваши сотрудники запускают необходимые приложения, используя как рабочие, так и собственные устройства. Эти приложения могут использоваться как для работы, так и в личных целях, однако бизнес-риски и риски информационной безопасности часто игнорируются. Новые сотрудники интересуются о действующих политиках в отношении использования приложений еще до того, как они дают свое согласие на трудоустройство. Дальнейшее усложнение всей инфраструктуры грозит тем, что система безопасности станет неэффективной. Подвергается ли ваша компания опасности? Вне сомнений, да, вопрос лишь, когда именно? Готовы ли вы к этому? Сложность сети и инфраструктуры безопасности может ограничивать или замедлять вашу способность реагирования на эти и другие угрозы для кибербезопасности.

Когда усложнение инфраструктуры ограничивает или замедляет процесс принятия решений, практически всегда помогает подход, при котором внимание уделяется фундаментальным вещам, что позволяет найти более эффективный выход из сложившейся ситуации. Учитывая все это, мы обратились к трем фундаментальным функциям, которые изначально должен выполнять межсетевой экран:

1. являться центральным компонентом инфраструктуры безопасности сети;

2. выполнять функцию управления доступом для всего трафика — разрешать или запрещать передачу данных в сеть в зависимости от установленной политики;

3. исключать риск, связанный со всем «неизвестным», благодаря использованию «позитивной» модели управления, при которой разрешается передача того, что явно указано, а все остальное — запрещается.

Со временем эти фундаментальные функции, которые выполняли межсетевые экраны, были аннулированы из-за очень большого трафика, который они должны были контролировать. Приложения переместились в ту область, где межсетевой экран, составляющий основу инфраструктуры безопасности, не может обеспечить необходимый контроль для защиты цифровых ресурсов.

Переключение портов, использование нестандартных портов и шифрование — это лишь несколько примеров возможных вариантов доступа к приложениям. Те же самые приемы также используются и злоумышленниками как напрямую в создаваемых ими атаках, так и косвенным образом, когда угрозы скрыты внутри трафика самого приложения. Дополнительный фактор, который усложняет проблему, создаваемую современными приложениями, состоит в том, что ваши сотрудники, вероятно, используют эти приложения для выполнения своих должностных обязанностей. Приведем примеры приложений и угроз, обнаруживаемых в сети.

- **Распространенные приложения для конечных пользователей.** К таким приложениям относятся социальные сети, файлообменники, передача видео и мгновенных сообщений, а также электронная почта. Это примерно 25% от всех приложений, используемых в сети, и 20% от общего сетевого трафика[1]. Некоторые из них сотрудники могут использовать для работы, другие же исключительно в личных целях. Очень часто эти приложения являются очень сложными по структуре и часто содержат функции, создающие нежелательный риск. Подобные приложения создают риски как для предприятий, так и для системы безопасности, и ваша задача состоит в том, чтобы понять, как можно добиться оптимального баланса, при котором некоторые приложения блокируются, а другие разрешаются с поддержанием необходимого уровня безопасности.
- **Основные бизнес-приложения.** Это приложения, от которых зависит работа компании; они составляют наиболее ценные ресурсы (например, базы данных, файловые службы и службы печати, каталоги). Данная группа приложений постоянно является целью разнообразных кибератак, и ваша задача состоит в том, чтобы определить, как лучше всего изолировать и защитить эти ресурсы от скрытых атак, которые легко обходят межсетевой экран и систему предотвращения вторжений с помощью часто используемых тактик обхода.
- **Инфраструктура и нестандартные приложения.** К данной группе относятся основные инфраструктурные приложения, например SSL, SSH и DNS, а также приложения собственной разработки и неизвестные приложения. Такие приложения часто используются для маскировки команд и управляющего трафика, который создается ботами и другими вредоносными программами. Что интересно, многие их этих приложений используют самые различные нестандартные порты. Восемьдесят пять из 356 приложений, использующих SSL, никогда не используют порт 443, равно как и не используют порты, определенные в SSL (37 выполняют подмену портов, 28 используют порт TCP/80, 20 используют порты, отличные от TCP/443).

[1] Palo Alto Networks. Отчет по использованию приложений и угрозам, январь 2013 г.

Чтобы попробовать решить эти проблемы, разработчики постарались пересмотреть фундаментальные принципы работы межсетевых экранов, чтобы они могли идентифицировать и контролировать трафик в зависимости от самого приложения, а не просто по порту и протоколу. Межсетевые экраны, которые способны реализовать подход к управлению трафиком в зависимости от приложений, теперь обобщенно называются межсетевыми экранами «нового поколения», и каждый производитель межсетевых экранов подтверждает, что контроль приложений становится все более важной частью системы безопасности сети.

Подобное внимание фундаментальным основам объясняется двумя очевидными причинами. Прежде всего, приложения и связанные угрозы могут легко преодолевать межсетевые экраны, работающие по принципу блокировки портов, а также дополнительные элементы, используемые для предотвращения угроз. Во-вторых, межсетевой экран — это единственное место, где виден весь трафик, проходящий через сеть, поэтому было бы логично внедрять политики контроля доступа именно в этом месте. Ценность подобного пересмотра фундаментальных принципов очевидна: общий уровень безопасности должен повыситься, при этом трудозатраты, связанные с управлением межсетевыми экраном и реакцией на инциденты, должны сократиться или, как минимум, остаться на прежнем уровне.

Революция, а не эволюция

В силу очень большого объема трафика, значительного количества приложений и недопустимости снижения производительности добавление устройств и новых программных «модулей», предназначенных для анализа трафика, не представляется возможным.

Межсетевые экраны нового поколения

Межсетевой экран нового поколения был определен компанией Gartner как нечто новое, ориентированное для использования на крупных предприятиях, «включающее в себя полный набор средств для проверки и предотвращения проникновения, проверки на уровне приложений и точное управление на основе политики». В настоящее время большинство производителей систем сетевой безопасности предлагают решения, в которых визуализация и контроль приложений обеспечиваются либо с помощью добавления сигнатур приложений в систему предотвращения вторжений, либо в виде лицензии на дополнительный модуль управления приложениями. В любом случае эти компоненты являются дополнениями для межсетевого экрана, контролирующего порты, они мало помогают в выполнении фундаментальных задач, для которых создавался межсетевой экран.

Эффективность работы предприятия сильно зависит от приложений, которые используют ваши сотрудники, а также содержимого, с которым работают сами приложения. Если просто разрешить некоторые из них и заблокировать другие, то это может помешать работе предприятия. Если ваши сотрудники системы безопасности хотят использовать компоненты и возможности межсетевого экрана нового поколения, то самое главное определить, обеспечит ли межсетевой экран нового поколения возможность безопасного внедрения приложений во благо организации. Необходимо учитывать следующее:

- Позволит ли межсетевой экран нового поколения повысить прозрачность и понимание трафика приложений в сети?
- Можно ли сделать политику управления трафиком более гибкой, добавив дополнительные варианты действий, кроме разрешения и запрета?
- Будет ли ваша сеть защищена от угроз и кибератак, как известных, так и неизвестных?
- Сможете ли вы систематически идентифицировать и управлять неизвестным трафиком?
- Можете ли вы внедрять необходимые политики безопасности без ущерба производительности?
- Будут ли сокращены трудозатраты вашей команды по управлению межсетевым экраном?
- Позволит ли это упросить управление рисками и сделать данный процесс более эффективным?
- Позволят ли внедряемые политики повысить рентабельность работы предприятия?

В случае положительного ответа на вышеприведенные вопросы обосновать ваше решение на переход со старых межсетевых экранов на межсетевые экраны нового поколения будет легко. На следующем этапе следует изучить альтернативные решения, которые предоставляют производители межсетевых экранов. При оценке имеющихся альтернатив очень важно изучить архитектурные различия между предлагаемыми межсетевыми экранами нового поколения и соответствующими результатами их использования с точки зрения функций/компонентов, работающих в реальном времени, а также управления и производительности.

Межсетевые экраны нового поколения

1. **Идентификация приложений независимо от используемого порта, протокола, шифрования или тактики обхода средства защиты.**
2. **Идентификация пользователей независимо от устройства или IP-адреса.**
3. **Защита в реальном времени от известных и неизвестных угроз, встроенных в приложения.**
4. **Обеспечение максимальной прозрачности приложений и управления приложениями, пользователями и содержимым на основе политик.**
5. **Обеспечение межсетевого экранирования на многогигабитных скоростях.**

Учет особенностей архитектуры для классификации трафика в межсетевом экране

При создании межсетевых экранов нового поколения производители решений сетевой безопасности использовали один из двух подходов к архитектуре:

1. Встраивание системы идентификации приложений в межсетевой экран в качестве основного механизма классификации.
2. Добавление системы сопоставления сигнатуры приложений в межсетевой экран, основанный на контроле портов.

Оба подхода позволяют распознавать приложения, но только с разной степенью успеха, удобства использования и точности. Самое важное, эти архитектурные подходы определяют конкретную модель безопасности для политик в отношении приложений — либо позитивную (определение всего разрешенного и запрет всего остального), либо негативную (определение всего блокируемого и разрешение всего остального).

- Позитивная модель безопасности (межсетевой экран или иное решение) позволяет создавать политики, которые разрешают определенные приложения или функции (например, WebEx, SharePoint, Gmail), после чего все остальное явным образом запрещается. Чтобы добиться подобного уровня контроля, весь трафик необходимо заранее классифицировать на межсетевом экране (а не по факту), чтобы разрешить соответствующий трафик и запретить остальной. Благодаря обеспечению полной визуализации всего трафика предприятия смогут сократить трудозатраты на администрирование, связанные отслеживанием операций в сети, управлением политиками и исследованием инцидентов. По соображениям безопасности можно добавить более эффективную защиту от известных и неизвестных кибератак, несмотря на то, что вы можете при этом разрешить более широкий спектр приложений в сети и усилить контроль над неизвестными приложениями с помощью функции запрета всего остального по умолчанию на межсетевом экране
- Негативная модель безопасности (система предотвращения вторжений, антивирус и т. д.) обеспечивает возможность находить и блокировать угрозы или нежелательные приложения и разрешать все остальное. Это означает, что необязательно будет классифицировать весь трафик — только в том объеме, насколько это необходимо для реализации необходимого списка блокировки. Подобный метод является достаточным для селективного поиска и блокирования угроз или нежелательных приложений, однако негативная модель безопасности не подходит в качестве основного средства контроля всего трафика в сети. Скорее, ее следует использовать в качестве дополнения к межсетевому экрану, контролирующему порты. В результате использования негативной модели безопасности у организации увеличиваются трудозатраты на администрирование, поскольку возникает необходимость настройки нескольких политик и дублирования баз данных журналов.

Остальная часть данного руководства для покупателей делится на три отдельных раздела. В первом разделе описаны *10 обязательных функций межсетевого экрана нового поколения*. Его можно использовать в качестве доказательств того, что описанные архитектура и модель управления являются критически важными для идентификации и безопасной работы приложений на уровне межсетевого экрана. В остальных разделах подробно описано, как следует использовать эти 10 функций для выбора поставщика в рамках процесса заявки, а также как на практике можно оценить решение межсетевого экрана.

10 обязательных функций межсетевого экрана нового поколения

Критерии выбора межсетевого экрана обычно делятся на три основные области: функции безопасности, выполняемые операции и производительность. Функциональные элементы системы безопасности обеспечивают эффективность управления безопасностью и способность вашей команды управлять рисками, связанными с работой приложений в сети. С точки зрения выполняемых операций самый большой вопрос состоит в том, «где должна располагаться политика управления приложениями, насколько сложной она является, и насколько трудно ею управлять вашим специалистам?» В отношении производительности все просто: способен ли межсетевой экран выполнить возложенные на него функции, обеспечив нужную для предприятия пропускную способность? Несмотря на то, что каждая организация будет выдвигать свои требования и приоритеты среди трех критериев выбора, можно четко сформулировать 10 обязательных функций межсетевого экрана нового поколения:

1. **Идентификация и контроль приложений на всех портах**
2. **Идентификация и контроль приложений для обхода средств защиты**
3. **Дешифрация исходящего SSL- и управляющего SSH-трафика**
4. **Контроль функций приложений**
5. **Систематическое управление неизвестным трафиком**
6. **Сканирование с целью выявления вирусов и вредоносных программ во всех приложениях, по всем портам**
7. **Обеспечение одинакового уровня визуализации и контроля приложений для всех пользователей и устройств**
8. **Упрощение, а не усложнение системы безопасности сети благодаря добавлению функции контроля приложений**
9. **Обеспечение той же пропускной способности и производительности при полностью включенной системе контроля приложений**
10. **Поддержка абсолютно одинаковых функций межсетевого экрана как в аппаратном, так и виртуальном форм-факторе**

1.

Ваш новый межсетевой экран должен обеспечивать постоянную идентификацию и управление приложениями на всех портах.

Реальный пример. Разработчики приложений больше не следуют методологии разработки приложений, основанных на использовании стандартных портов и протоколов. Все большее число приложений может работать через нестандартные порты или переключаться между портами (например, приложения мгновенного обмена сообщениями, равноправного обмена файлами или VoIP). Кроме того, все большее число пользователей умеет направлять работу приложений через нестандартные порты (например, RDP, SSH). Чтобы внедрить политики межсетевого экрана для конкретных приложений, которые все чаще работают без привязки к портам, ваш новый межсетевой экран должен быть готов к тому, что каждое приложение может работать с любым портом. Концепция поддержки любого приложения, работающего на любом порте, является одним из фундаментальных изменений в работе приложений, которое заставляет переходить от межсетевых экранов, контролирующих трафик через определенные порты, к межсетевым экранам нового поколения. Принцип поддержки любого приложения, работающего по любому порту, еще раз показывает, что негативная модель управления не позволяет решить проблему. Если приложение может переключаться на любой порт, то в случае использования продукта, основанного на негативном управлении, он должен либо заблаговременно получить необходимую информацию, либо постоянно отслеживать все сигнатуры по всем портам.

Требования. Требование простое — необходимо исходить из того, что каждое приложение может работать по любому порту, поэтому ваш новый межсетевой экран по умолчанию должен постоянно классифицировать трафик по приложению по всем портам. Проблема классификации трафика по всем портам будет снова возникать при обсуждении всех оставшихся требований. В противном случае мы по-прежнему будем наблюдать обход средств контроля на основе портов с помощью все тех же приемов, которые существуют много лет.

2.

Ваш межсетевой экран нового поколения должен идентифицировать и контролировать инструменты, позволяющие обходить средства обеспечения безопасности.

Реальный пример. Только небольшое число приложений вашей сети можно использовать для целенаправленного обхода всех политик безопасности, защищающих цифровые ресурсы вашей организации. К инструментам обхода средств безопасности относятся приложения двух классов — приложения, изначально разрабатываемые для обхода средств защиты (например, внешние прокси, приложения, позволяющие туннелировать трафик (не VPN)), и приложения, которые можно адаптировать для выполнения этой задачи (например, инструменты управления удаленным сервером/рабочим столом).

- Внешние прокси и зашифрованные туннельные приложения (не VPN), оснащенные рядом методик маскировки, специально используются для обхода средств защиты. Поскольку эти приложения изначально создаются для обхода средств безопасности и поэтому способствуют рискам для бизнеса и защиты, они не имеют для вашей сети никакой бизнес-ценности.

- Инструменты управления удаленным сервером/рабочим столом, такие как RDP и Teamviewer, обычно используются работниками служб поддержки и ИТ-специалистами в целях повышения эффективности работы. Они также часто используются сотрудниками организаций для подключения к домашним и другим компьютерам за пределами корпоративной сети в обход межсетевого экрана. Злоумышленники прекрасно знают об использовании таких приложений, и в официально публикуемых отчетах Verizon Data Breach Report (DBIR) и Mandiant сообщалось о том, что эти инструменты удаленного доступа использовались на одном или нескольких этапах сетевых атак.

Если быть точными, не все из этих приложений несут в себе одинаковую степень риска. У приложений удаленного доступа, как и у многих зашифрованных туннельных приложений, имеется свое законное применение. Однако эти же инструменты все чаще используются злоумышленниками на разных этапах в их сложных атаках. Если организации не смогут контролировать использование этих инструментов обхода средств безопасности, они не смогут успешно выполнять политики безопасности и подвергнут себя всем рискам, для защиты от которых эти средства безопасности предназначены.

Требования. Существуют различные типы приложений обхода, и методики, которыми оснащаются приложения каждого из этих типов, слегка различаются. Существуют публичные и частные внешние прокси (крупная база данных публичных прокси представлена на сайте proxy.org), которые могут использовать и HTTP, и HTTPS. Частные прокси часто настраиваются на базе не классифицируемых IP-адресов (например, домашних компьютеров) с такими приложениями, как PHProxy или CGIProxy. Такие приложения удаленного доступа, как RDP, Teamviewer или GoToMyPC, имеют законное применение, однако из-за связанного риска должны строго контролироваться. Большинство других приложений для обхода защиты (например, Ultrasurf, Tor, Hamachi) не имеют никакого бизнес-значения для вашей сети. Независимо от состояния вашей политики безопасности, ваш межсетевой экран нового поколения должен быть оснащен специальными методиками, позволяющими идентифицировать и контролировать все перечисленные приложения, не привязываясь к конкретному порту, протоколу, методу шифрования или другой тактике обхода. И еще один важный момент: приложения, обеспечивающие обход средств защиты, регулярно обновляются, что еще больше затрудняет их выявление и контроль. Поэтому так важно понять не только то, что ваш межсетевой экран нового поколения должен идентифицировать эти приложения обхода. Важно также знать, как часто выполняется обновление и обслуживание функций контроля приложений, которыми оснащен ваш межсетевой экран.

3.

Ваш межсетевой экран нового поколения должен обеспечивать расшифровку и проверку SSL, а также управление SSH.

Реальный пример. В настоящее время 26% приложений в современных корпоративных сетях тем или иным образом, в той или иной форме, используют протокол SSL[2]. Принимая во внимание тот факт, что конечные пользователи все чаще применяют HTTPS для многих востребованных приложений с высокой степенью риска (таких как Gmail, Facebook), а также могут применять SSL на многих веб-сайтах, ваши специалисты службы безопасности сталкиваются с тем, что им становится неподвластна все большая часть сетевого трафика, и они теряют возможность дешифрации, классификации, контроля и сканирования трафика, зашифрованного с помощью SSL. Естественно, межсетевой экран нового поколения должен быть достаточно гибким, чтобы оставлять как есть трафик определенных типов, зашифрованный с помощью SSL (например, веб-трафик от финансовых служб или организаций здравоохранения), и расшифровывать трафик других типов (например, SSL на нестандартных портах, HTTPS с не классифицируемых веб-сайтов Восточной Европы), согласно установленной политике. Использование SSH носит практически универсальный характер, и конечные пользователи могут легко настраивать этот протокол для своих личных целей, как и любой другой инструмент для управления удаленным рабочим столом. Тот факт, что данные, передаваемые по SSH, зашифрованы, делает этот протокол эффективным средством для скрытия действий нерабочего характера.

Требования. Возможность дешифрации SSL — это основополагающий фактор. И не только из-за того, что речь идет о значительной части корпоративного трафика, но и из-за того, что эта возможность повышает эффективность других ключевых функций, которые без дешифрации SSL будут неполными или неполноценными. К другим ключевым факторам можно отнести выявление и дешифрацию SSL на любом порте, как входа, так и выхода; управление на основе политики с применением дешифрации, а также набор аппаратных и программных средств, необходимых для дешифрации SSL в рамках десятков тысяч одновременных подключений SSL с предсказуемой производительностью. Еще одним важным требованием является возможность идентификации и контроля за использованием SSH. Если говорить конкретно, то контроль за SSH подразумевает возможность определения целей использования протокола — туннелирование трафика (локальная, удаленная, X11) или использование по назначению (SCP, SFTP и доступ к shell). Сведения о целях и характере использования SSH можно затем преобразовать в соответствующие политики безопасности.

[2] Palo Alto Networks. Отчет по использованию приложений и угрозам, январь 2013 г.

4.

Ваш межсетевой экран должен осуществлять контроль за работой приложений.

Реальный пример. Разработчики платформ приложений, таких как Google, Facebook, Salesforce.com или Microsoft, предлагают пользователям богатейший набор компонентов и функций, которые повышают лояльность пользователей, но при этом представляют сложнейшие профили риска. Возьмем, к примеру, приложение Webex, которое является эффективнейшим бизнес-инструментом. Однако функция совместного доступа к рабочему столу (Webex Desktop Sharing), позволяющая осуществлять доступ к рабочим столам ваших сотрудников с внешнего источника, способствует нарушению внутренних политик или нормативных требований. Другим примером могут служить приложения Google Mail (Gmail) и Google Talk (Gtalk). Как только пользователь входит в систему Gmail, что может быть разрешено политикой, он может легко переключить контекст на Gtalk, что может быть запрещено той же политикой. Ваш межсетевой экран нового поколения должен уметь распознавать и разграничивать отдельные компоненты и функции — только в этом случае можно будет внедрить соответствующие политики.

Требования. Ваш межсетевой экран нового поколения должен постоянно осуществлять классификацию каждого приложения, отслеживая все изменения, которые могут указывать на использование той или иной функции этого приложения. Концепция «однократной» классификации трафика не является выходом из положения, поскольку при этом игнорируется тот факт, что различные широко распространенные приложения могут использовать одни и те же сетевые сессии или выполнять осуществляют доступ к разным сеансам и выполняют сразу несколько функций. Если в данной сессии будет идентифицирована другая функция или приложение, межсетевой экран должен зафиксировать этот факт в таблицах состояния сессий и выполнить проверку на основе политики. Непрерывный мониторинг состояния с целью выявления различных функций, которые может поддерживать каждое приложение, а также связанных с ними рисков, — это важнейшее требование к вашему межсетевому экрану нового поколения.

Безопасное разрешение приложений
Для безопасной работы приложений и технологий, а также для обеспечения основанных на них бизнес-процессов, специалистам по сетевой безопасности требуется внедрить не только соответствующие политики, но и средства, контролирующие их соблюдение.

5.

Ваш межсетевой экран нового поколения должен осуществлять систематическое управление неизвестным трафиком.

Реальный пример. В небольших количествах неизвестный трафик присутствует в каждой сети, однако даже незначительный неизвестный трафик представляет существенный риск для вас и вашей организации. Существует целый ряд важных факторов, имеющих отношение к неизвестному трафику, которые следует учитывать: распределен ли он по категориям, можно ли сократить его до минимума, используя управление на основе политики, может ли ваш межсетевой экран легко характеризовать пользовательские приложения так, чтобы они переходили в категорию «известных» приложений в вашей политике безопасности, и способен ли ваш межсетевой экран определить, представляет ли неизвестный трафик угрозу?

Неизвестный трафик также тесно связан с сетевыми угрозами. Злоумышленники часто модифицируют протокол, чтобы поразить нужное приложение. Например, для атаки на веб-сервер злоумышленнику может потребоваться изменение заголовка HTTP, в результате которого трафик больше не будет идентифицироваться как веб-трафик. Подобная аномалия может служить ранним свидетельством атаки. Вредоносное ПО также часто использует модифицированные протоколы для связи с командным центром, что позволяет специалистам по безопасности ликвидировать любые проникновения неизвестного вредоносного ПО.

Требования. Ваш межсетевой экран нового поколения по умолчанию должен классифицировать весь трафик на всех портах — это тот аспект, который должен обязательно учитываться на ранних этапах разработки архитектуры и модели управления средствами безопасности. Позитивная модель (блокирование по умолчанию) подразумевают классификацию всего трафика, тогда как негативная модель (разрешение по умолчанию) подразумевают классификацию только определенного трафика. Классификация всего трафика — это только малая часть проблемы, которую приносит неизвестный трафик. Ваш межсетевой экран нового поколения должен обеспечить видимость всего неизвестного трафика, на всех портах. Он должен быстро выполнять анализ этого трафика и определять его природу — (1) внутреннее или кастомизированное приложение, (2) коммерческое приложение без сигнатуры или (3) угроза. Кроме того, межсетевой экран должен быть оснащен всеми необходимыми инструментами, которые обеспечат не только видимость неизвестного трафика, но и систематический его контроль в соответствии с политикой: создание пользовательской сигнатуры, отправка PCAP трафика коммерческого приложения для проведения дальнейшего анализа или проведение аналитического исследования, которое позволит определить, не является ли трафик угрозой.

6.

Ваш межсетевой экран нового поколения должен сканировать приложения на всех портах, проверяя наличие угроз.

Реальный пример. Организации постоянно внедряют все новые и новые приложения, повышающие эффективность бизнеса, размещенные как внутри локальной сети, так и за ее пределами. Будь это SharePoint, Box.com, Google Docs, Microsoft Office365 или иное приложение, ваша организация может использовать приложение, способное работать через нестандартные порты, использовать SSL или предоставлять совместный доступ к файлам. Другими словами, эти приложения могут повышать эффективность бизнеса, но при этом служить вектором развития киберугроз. Более того, некоторые из этих приложений (например, SharePoint) зависят от поддержки технологий, которые являются регулярной мишенью для компьютерных атак (например, IIS, SQL Server). В этом случае блокировка приложения не решит проблему. Не решит также проблему слепое разрешение всех приложений, несущих с собой соответствующие риски для бизнеса и кибербезопасности.

В борьбе с вредоносным ПО тенденция использования нестандартных портов представляет острую проблему. Поскольку вредоносное ПО базируется в сети и при большинстве соединений вредоносный клиент (вредоносное ПО) связывается с вредоносным сервером (командным центром), то злоумышленник может использовать любую комбинацию портов и протоколов. Как показал анализ за последние три месяца, в 97% всего неизвестного вредоносного ПО, проникающего через FTP, использовались только нестандартные порты.

Требования. В процесс безопасного разрешения приложения входит разрешение самого приложения и его сканирование на наличие угроз. Эти приложения могут осуществлять связь, используя различную комбинацию протоколов (например, приложение SharePoint использует протоколы CIFS, HTTP и HTTPS и требует применения более сложной политики межсетевого экрана, чем просто «блокировка приложений»). Первым шагом является идентификация приложения (независимо от порта или типа шифрования), определение функций, которые будут разрешаться или отклоняться, и последующее сканирование разрешенных компонентов на наличие угроз — проникновений, вирусов/вредоносного ПО или шпионского ПО... или даже конфиденциальной, подотчетной или секретной информации.

7.

Ваш межсетевой экран нового поколения должен обеспечивать непрерывный контроль над всеми пользователями, независимо от местоположения или типа устройства.

Реальный пример. Ваши пользователи все чаще работают за стенами организации, осуществляя доступ к корпоративной сети со своих смартфонов или планшетов. В настоящее время значительная часть ваших сотрудников имеет возможность работать удаленно. Работая в любом месте — за столиком в кафе, у себя дома или в организации клиента — ваши сотрудники считают само собой разумеющимся, что они могут подключаться к своим рабочим приложениям через WiFi, беспроводную широкополосную сеть или другой вид связи. Независимо от местоположения пользователя или даже самого приложения, межсетевой экран должен применять один и тот же стандарт контроля доступа. Если ваш межсетевой экран нового поколения обеспечивает визуализацию и контроль приложений только в пределах стен организации, но не за ними, он в любой момент может упустить трафик, представляющий огромный риск.

Требования. В принципе, требования просты — ваш межсетевой экран нового поколения должен обеспечивать постоянную видимость и контроль трафика любому авторизованному пользователю, независимо от его местоположения. Это не означает, что в вашей организации будет применяться одна и та же политика для трафика в пределах и за пределами территории. Например, некоторые организации допускают использование сотрудниками программы Skype, но не разрешают ее использовать на рабочем месте. Согласно политике других организаций, вне офиса сотрудники не могут загружать вложения Salesforce.com, если только у них не активировано шифрование жесткого диска. Все это должен обеспечить ваш межсетевой экран нового поколения, причем при этом он должен исключить существенные задержки для конечных пользователей, чрезмерные трудности для сетевых администраторов или значительные затраты для организации в целом.

8.

Ваш межсетевой экран нового поколения должен обладать расширенными функциями управления приложениями, что позволит упростить задачи сетевой безопасности.

Реальный пример. Многие организации постоянно стремятся внедрять дополнительные информационные потоки, политики и средства управления, в то время как их специалисты в области информационной безопасности уже сильно перегружены, управляя множеством процессов защиты. Другими словами, если ваши сотрудники не справляются со своими текущими задачами, то добавление устройств и управление интерфейсами, а также соответствующими политиками и информацией, не позволит разгрузить ваших специалистов, равно как и не ускорит процесс обработки инцидентов. Чем сложнее политика (например, межсетевой экран на базе портов разрешает трафик через порт 80, система предотвращения вторжений выявляет/блокирует угрозы и приложения, шлюз для веб-защиты выполняет контроль URL-запросов), тем тяжелее этой политикой управлять. А какую политику в отношении WebEx используют ваши специалисты по безопасности? Как они определяют и решают конфликты политики на различных устройствах? Если предположить, что для типичных межсетевых экранов на основе портов определены базы правил, включающие тысячи всевозможных правил, то при добавлении тысяч сигнатур приложений в рамках десятков тысяч портов сложность будет возрастать в десятки раз.

Требования. Работа вашей организации основана на приложениях, пользователях и содержимом, поэтому ваш межсетевой экран нового поколения должен позволять использовать политики, напрямую поддерживающие все ваши бизнес-инициативы. Обмен информацией, охватывающий приложения, пользователей и содержимое во всех их аспектах (видимость, управление на базе политики, ведение журналов и формирование отчетов), поможет значительно упростить вашу инфраструктуру безопасности. Политика межсетевого экрана, основанная на портах и IP-адресах и используемая совместно с отдельными политиками для управления приложениями, системами обнаружения вторжений и защиты от вредоносного ПО, только усложнит процесс управления на базе политик и, в конечном счете станет препятствием развитию бизнеса.

9.

При полной активации функций управления приложениями ваш межсетевой экран нового поколения должен обеспечивать такую же пропускную способность и производительность, как прежде.

Реальный пример. Многие организации ведут постоянную напряженную работу, пытаясь добиться оптимального баланса между производительностью и безопасностью. Нередко активация функций безопасности на вашем межсетевом экране означает заведомое принятие того факта, что пропускная способность и производительность будут существенно снижены. Если ваш межсетевой экран нового поколения разработан правильно, вам не потребуется сражаться за этот баланс.

Требования. При рассмотрении этого требования также становится очевидным значение архитектуры, только в несколько ином ключе. Поспешный подбор межсетевого экрана на основе портов и других функций безопасности от разных поставщиков технологий обычно выливается в чрезмерное количество сетевых уровней, механизмов сканирования и политик, что приводит к снижению производительности. Межсетевой экран должен быть нацелен на эти задачи еще при разработке архитектуры ПО. Более того, если считать, что вам требуется выполнять ресурсоемкие вычислительные задачи (такие как идентификация приложений, предотвращение угроз на всех портах и т. д.) в среде высокоинтенсивного трафика, не допускающей малейшие задержки в работе критически важной инфраструктуры, ваш межсетевой экран нового поколения должен быть оснащен и всеми аппаратными средствами, необходимыми для сканирования сетей, систем безопасности и содержимого.

10.

Ваш межсетевой экран нового поколения должен быть оснащен одинаковыми наборами функций для аппаратного и виртуального форм-фактора.

Реальный пример. Стремительное распространение виртуализации и облачных вычислений приводит к появлению новых проблем в области безопасности, и с помощью межсетевых экранов прежних версий, для которых характерна несогласованная работа функций, разрозненность управления и нехватка точек интеграции с виртуализированной средой, решить эти проблемы сложно или вообще невозможно. Чтобы защитить как входящий и выходящий трафик центра обработки данных, так и трафик внутри виртуализированных сред вашей организации, ваш межсетевой экран нового поколения должен предлагать абсолютно одинаковый функционал как в аппаратных, так и виртуальных форм-факторах.

Требования. Динамическая настройка и отмена приложений в среде виртуализированного центра обработки данных еще больше усложняет задачи идентификации и контроля приложений, выполняемые на основе портов и IP-адресов. Кроме тех функций, которые уже описаны в разделе 10 обязательных функций межсетевого экрана нового поколения и имеют отношение как к аппаратным, так и к виртуальным форм-факторам, важно, чтобы ваш межсетевой экран нового поколения поддерживал всестороннюю интеграцию со средой виртуализации. Благодаря этому при добавлении и удалении новых виртуальных машин и приложений можно будет создавать соответствующие политики, нацеленные именно на приложения. Это единственный способ, который гарантирует поддержку развития архитектур современных центров обработки данных, обеспечивает операционную гибкость и защиту от рисков и позволяет соблюдать стандарты и нормативы.

Межсетевые экраны должны обеспечивать безопасную работу приложений — и всецело поддерживать ваш бизнес

Ваши пользователи постоянно внедряют новые приложения и технологии. Большей частью они делают это для выполнения своей работы, однако все эти новшества мало связаны с работой всей организации и несут с собой угрозу безопасности. Иногда блокировка таких приложений силами вашей службы безопасности может препятствовать нормальной работе вашей организации.

От выбора приложений зависит, насколько эффективно ваши сотрудники будут выполнять свою работу и насколько успешно они будут конкурировать с остальными в личном и профессиональном плане. Именно поэтому безопасное разрешение приложений становится все более важным атрибутом любой политики безопасности. Чтобы добиться безопасной работы приложений и технологий, используемых в вашей сети и связанных бизнес-процессах, ваши специалисты по сетевой безопасности должны осуществлять постоянный контроль на базе соответствующих политик, а также активно применять средства, контролирующие их соблюдение.

В разделе *10 обязательных функций межсетевого экрана нового поколения* описаны критически важные возможности, позволяющие организациям безопасно использовать приложения и в конечном итоге — успешно осуществлять работу. Следующий шаг — преобразование этих требований в соответствующие действия, выбор поставщика посредством составления заявки, а также оценка предлагаемых решений. Только после всех этих действий настает время приобретения и внедрения выбранного межсетевого экрана нового поколения.

Поддержка вашего бизнеса
В современном мире управление приложениями — это не просто их разрешение или запрет; это обеспечение безопасной работы приложений, способствующее успешному продвижению бизнеса.

Использование процесса составления заявок при выборе межсетевого экрана нового поколения

Обычно при выборе межсетевых экранов, систем предотвращения вторжений (IPS) или других критически важных компонентов, обеспечивающих безопасность инфраструктуры, организации прибегают к процессу формирования заявок, который гарантирует удовлетворение любых специфических потребностей. Согласно аналитикам, составившим Магический квадрант Gartner для корпоративных межсетевых экранов, « ...изменение характеристик угроз, а также изменение процессов в сфере бизнеса и ИТ потребует обновления инфраструктуры межсетевых экранов/IPS и заставит менеджеров по сетевой безопасности искать межсетевые экраны нового поколения, отвечающие конкретным требованиям их организаций». С появлением новых возможностей внедрения организациям следует расширить критерии выбора при составлении заявок, включив в них такой критерий, как «визуализация и контроль приложений». Эту возможность как раз и предлагают межсетевые экраны нового поколения. В предыдущем разделе были перечислены 10 основных требований к межсетевому экрану нового поколения. В этом разделе, взяв за основу представленные требования, мы расскажем о подходе, который позволит грамотно определить и выбрать межсетевой экран нового поколения.

Архитектура межсетевого экрана и модель управления — на что обращать внимание

При попытке оценить, насколько эффективно межсетевой экран, предлагаемый каким-либо поставщиком, способен обеспечить визуализацию и контроль приложений, следует учитывать множество разнообразных факторов. Архитектура межсетевого экрана, точнее говоря, присущий ей механизм классификации трафика как раз и определяет, насколько эффективно будет выполняться идентификация и контроль самих приложений, а не только портов и протоколов. Как уже говорилось ранее, основной функциональной возможностью любого нового межсетевого экрана должна быть возможность точной классификации трафика, которая затем будет использоваться как основа политики безопасности.

Такая модель политики межсетевого экрана носит «позитивный» характер (блокировка всего трафика приложений, за исключением явно разрешенного трафика). Позитивная модель подразумевает возможность управления приложениями и их разрешение — критически важное требование в современном деловом мире, нуждающемся в постоянной и повсеместной связи. Если организация для идентификации и контроля за приложениями полностью полагается на компоненты, основанные на системах обнаружения вторжений, это значит, что она использует «негативную» модель управления (разрешен весь трафик приложений, за исключением трафика, явно отклоняемого системой обнаружения вторжений). При использовании негативной модели приложения можно только блокировать. Разница становится очевидной на простом примере — можно включить свет в комнате, чтобы видеть и контролировать все (позитивная модель), а можно включить только фонарик, чтобы видеть и контролировать только то, что вас интересует (негативная модель). Этот дополнительный компонент, выявляющий и блокирующий «плохие» события, является только заплатой, а не полным решением, поскольку отслеживает только часть трафика, таким образом пытаясь бороться со снижением производительности, и не способен справиться со всем многообразием кибератак и приложений.

Визуализация и контроль приложений

В процессе создания заявки необходимо определить, как архитектура межсетевого экрана будет способствовать идентификации и контролю за всем спектром приложений, включая бизнес-приложения, персональные приложения и другие, а также контролю за протоколами, независимо от порта, шифрованием SSL и другими используемыми техниками маскировки. Разрабатывая техническое задание на межсетевые экраны нового поколения, обязательно используйте следующие вопросы и утверждения.

- Многие приложения могут уклоняться от обнаружения за счет использования нестандартных портов, путем изменения портов или быстрого переключения на другой порт.
  - Включены ли механизмы идентификации приложений в основной механизм классификации трафика межсетевого экрана (то есть, разрешены ли по умолчанию)?
  - Зависят ли механизмы идентификации приложений от выбора стандартного порта?
  - Могут ли сигнатуры применяться ко всем портам, и как конфигурируется данный процесс — автоматически или вручную?
- Когда трафик впервые поступает на устройство, каким образом осуществляется его классификация — путем определения порта (это порт 80, следовательно, HTTP) или приложения (это приложение Gmail)?
- Опишите подробно, каким образом межсетевой экран точно идентифицирует приложения.
  - Какие механизмы, кроме сигнатур, используются для классификации трафика?
  - Опишите, какие используются механизмы расшифровки приложений и протоколов.
  - Как происходит внедрение расшифровки SSL и SSH и средств управления?
  - Применяются ли механизмы идентификации приложений одинаково на всех портах?
- Какие механизмы используются для выявления намеренно маскируемых приложений, таких как UltraSurf или зашифрованный одноранговый трафик?
- Выполняется ли идентификация приложений непосредственно на межсетевом экране, или это процесс второстепенный, выполняемый после идентификации порта?
  - Каковы основные преимущества поддерживаемой архитектурной концепции?
- Отслеживается ли состояние приложений? Если да, то каким образом этот процесс обеспечивает постоянный контроль за приложениями и связанными второстепенными функциями?
  - Приведите три примера того, как состояние приложения используется в управлении на основе политики.
- Является ли идентификационная информация о приложении основой политики безопасности межсетевого экрана, или же управление приложениями рассматривается как второстепенный элемент политики?
- Как часто обновляется база данных приложений, и какой характер носит это обновление — динамический или на основе перезагрузки системы?
- Опишите, как в виртуализированных средах осуществляется классификация трафика, проходящего через виртуальные машины (восток/запад, север/юг).
  - Опишите точки интеграции в рамках виртуализированной среды.
  - Опишите процесс построения политики безопасности для вновь создаваемых виртуальных машин.
  - Опишите функции, позволяющие отслеживать перемещения, добавления и изменения виртуальных машин.
  - Опишите функции, обеспечивающие интеграцию в системы автоматизации и оркестровки.

Управление маскируемыми приложениями, SSL и SSH

Существует множество приложений, которые можно использовать для обхода систем защиты. Некоторые из них, такие как внешние прокси и зашифрованные туннельные приложения (не VPN), изначально разрабатываются в целях обхода средств безопасности. Другие, такие как инструменты управления удаленным сервером/рабочим столом, могут использоваться в целях обхода механизмов контроля сотрудниками организаций, не принадлежащими к ИТ-специалистам или специалистам по поддержке. Протокол SSL, используемый как средство обеспечения безопасности, становится стандартной конфигурацией для многих приложений конечного пользователя, однако применение SSL может способствовать маскировке входящих угроз или исходящей передачи данных, что является существенной проблемой. В настоящее время приблизительно 26% всех приложений, обнаруживаемых в вашей сети, могут использовать SSL[3] (тем или иным образом). Поэтому так важно найти надежных производителей, предлагающих межсетевые экраны нового поколения, которые учитывают особенности приложений этой категории. Разрабатывая техническое задание на межсетевые экраны нового поколения, обязательно используйте следующие вопросы и утверждения.

- Опишите процесс, с помощью которого выполняется идентификация приложений, зашифрованных с помощью SSL, на всех портах, включая нестандартные.
- Какие средства управления политики позволяют выполнять избирательную расшифровку, проверку и управление приложениями, использующими SSL?
- Поддерживаются ли процессы идентификации, расшифровки и проверки SSL, протекающие в обоих направлениях?
- Является ли расшифровка SSL стандартной функцией, или она предлагается за дополнительную плату? И требуется ли выделенное устройство?
- Протокол SSH широко используется ИТ-специалистами, специалистами служб поддержки и технически подкованными сотрудниками как средство доступа к удаленным устройствам.
  - Поддерживается ли управления SSH? Если да, то определите степень контроля.
- Какие механизмы используются для идентификации целенаправленно маскируемых приложений, таких как UltraSurf или Tor?
- Опишите, каким образом продукт может автоматически идентифицировать приложения для обхода системы защиты, использующие нестандартный порт.

[3] Palo Alto Networks. Отчет по использованию приложений и угрозам, январь 2013 г.

Разрешение приложений на базе политик

В современном мире постоянной связи управление приложениями — это не просто их разрешение или отклонение; это обеспечение их безопасной работы, способствующее успешному продвижению бизнеса. Многие платформы (Google, Facebook, Microsoft) предоставляют пользователям, осуществившим начальный вход в систему, доступ к разным приложениям. Требуется обязательно определить, как производитель межсетевого экрана осуществляет мониторинг состояния приложений, как он выявляет изменения в приложениях и как классифицирует изменения состояния. Разрабатывая техническое задание на межсетевые экраны нового поколения, обязательно используйте следующие вопросы и утверждения.

- Выполняется ли классификация трафика и проверка с отслеживанием состояния отдельно, до идентификации приложений? Если да, то каким образом после идентификации приложений отслеживаются изменения в их состоянии, и как эти изменения используются в рамках политики?
- Опишите, как иерархическая структура базы данных приложений (один уровень, несколько уровней и другое) влияет на работу функций в родительском приложении, обеспечивающих более детальные политики разрешений.
- Опишите уровни контроля, которые могут действовать в отношении отдельных приложений, а также их соответствующие функции:
  - разрешение;
  - разрешение на основе приложения, функций приложения, категории, подкатегории, технологии или фактора риска;
  - разрешение на основе расписания, пользователя, группы, порта;
  - разрешение и сканирование на вирусы, уязвимости приложений, шпионское ПО, скачивание вредоносного ПО;
  - разрешение и формирование/применение средств контроля за качеством обслуживания;
  - отклонение.

- Могут ли средства контроля на базе портов быть внедрены для всех приложений, включенных в базу данных приложений, так, чтобы администратор мог регулировать взаимосвязи между приложениями и портами на основе политики? Например:
  - так, чтобы разработчики базы данных Oracle использовали определенный порт или диапазон портов?
  - Убедитесь в том, что использовать SSH и RDP могут только ИТ-специалисты.
  - Проверьте возможность обнаружения и блокировки вредоносного ПО в приложении, даже если оно использует нестандартный порт.
- Составьте список всех репозиториев с идентификационными данными, используемых для управления, зависящего от пользователя.
- Предоставляется ли API-интерфейс для интеграции компонентов инфраструктуры на основе пользовательской или нестандартной идентификации?
- Опишите, как пользователи и группы могут осуществлять внедрение средств управления на базе политик в средах терминальных сервисов.
- Перечислите различия между механизмами разрешения приложений, предназначенными для аппаратных и виртуализированных экземпляров.

Управление неизвестными приложениями

В каждой сети присутствует трафик неизвестных приложений. Типичным его источником являются внутренние или пользовательские приложения, однако в его роли могут выступать не идентифицированные коммерческие приложения или, что самое худшее, какая-либо вредоносная программа. При составлении заявки или оценке решений особое внимание следует обращать на то, каким образом поставщик обеспечивает систематическое управление неизвестным трафиком, представляющим огромный риск для организации и ее безопасности. Разрабатывая техническое задание на межсетевые экраны нового поколения, обязательно используйте следующие вопросы и утверждения.

- Опишите подробно, как выполняется идентификация неизвестного трафика для последующего анализа.
- Являются ли средства выполнения анализа частью стандартного набора функциональных возможностей, или они входят в состав второстепенных, дополнительных продуктов?
- Какие действия, если они вообще предусмотрены, могут предприниматься в отношении неизвестного трафика (разрешение, отклонение, проверка, формирование и т. д.)?
- Опишите рекомендуемые лучшие практики, используемые при управлении трафиком неизвестных приложений.
  - Доступно ли управление на базе политик, используемое в отношении официально разрешенных приложений (например, разрешение, отклонение, проверка, формирование, контроль на основе пользователей, зоны действия и т. д.)?
  - Возможно ли «переименование» внутреннего трафика?
  - Возможно ли создание пользовательских сигнатур приложений?
- Что представляет собой процесс отправки запросов на новые или обновленные сигнатуры приложений?
- Какое время занимает выполнение условий SLA с момента отправки заявки?
- Какие механизмы позволяют определить, является ли неизвестный трафик вредоносной программой?

Предотвращение угроз

Угрозы все в большей степени связаны с различными приложениями, которые могут служить либо векторами для проникновений и заражения, либо средством отправки команд и управления зараженными устройствами. По этой причине аналитики единогласно рекомендуют организациям объединять традиционные системы предотвращения вторжений и технологии предотвращения угроз, делая их неотъемлемым компонентом межсетевых экранов нового поколения. Разрабатывая техническое задание на межсетевые экраны нового поколения, обязательно используйте следующие вопросы и утверждения.

- Опишите все используемые механизмы предотвращения угроз (системы обнаружения вторжений, антивирусные программы, антишпионское ПО, контроль URL-адресов, контроль передаваемых данных и т. д.).
- Каким образом лицензированы эти механизмы предотвращения угроз?
- Какие механизмы предотвращения угроз разработаны самой организацией, а какие приобретены у сторонней организации или в рамках услуг?
- Каким образом предотвращаются угрозы, которые встроены в приложения, использующие нестандартные порты?
- Являются ли данные для идентификации приложений интегрированным компонентом, или они включены в технологии предотвращения угроз? Если да, то определите уровень интеграции.
- Опишите, какие механизмы по предотвращению угроз (системы обнаружения вторжений, антивирус и т. д.) работают на базе портов, а какие — на базе приложений.
- Способен ли механизм предотвращения угроз выполнять сканирование внутри сжатого содержимого, например ZIP или GZIP?
- Способен ли механизм предотвращения угроз выполнять сканирование содержимого, зашифрованного с помощью SSL?
- Опишите, каким образом межсетевой экран может выявлять пользовательское или полиморфное вредоносное ПО и защищать от него.
  - Какие механизмы используются для блокировки вредоносного ПО?
- Опишите ваш процесс исследований и разработок в области предотвращения угроз.

Защита удаленных пользователей

Пользователи современных сетей считают само собой разумеющимся, что они всегда могут подключиться к сети и работать в ней, находясь в любом месте за пределами традиционного сетевого периметра. Эти пользователи, которые могут работать на любом устройстве, таком как персональный компьютер, смартфон или планшет, должны быть всегда защищены, даже если находятся за пределами периметра. Цель данного раздела – определить, какие механизмы защиты доступны для таких удаленных пользователей, и в чем состоят различия в уровне защиты, когда пользователь находится в пределах или за пределами сетевого периметра. Разрабатывая заявку на межсетевые экраны нового поколения, обязательно используйте следующие вопросы и утверждения

- Опишите подробно, включив в описание все необходимые компоненты, все доступные средства для защиты удаленных пользователей.
- Если включен клиентский компонент, то как выполняется его распределение?
- Опишите требования к установке масштаба. Сколько пользователей одновременно может поддерживаться?
- Прозрачен ли набор функций безопасности, предназначенных для удаленного пользователя, для клиента?
- Опишите процесс внедрения средств управления удаленными пользователями, работающих на основе политик (например, политики межсетевого экрана, отдельной политики/устройства и т. д.).
- Перечислите все функции и механизмы защиты, включенные в инструменты удаленной работы (SSL, управление приложениями, система обнаружения вторжений и т. д.)
- Способен ли ваш межсетевой экран, твердо следуя правилам политики, сохранять активными подключения пользователей, независимо от их местоположения?
- Как осуществляется поддержка пользователей мобильных устройств? Сможете ли вы обеспечить строгое соблюдение правил политики в отношении пользователей, когда они работают во внешних сетях или внутренних беспроводных сетях?
- Позволяет ли межсетевой экран решать проблемы, связанные с внедрением BYOD, например, обеспечивать одинаково безопасную работу на ноутбуках, телефонах и планшетах, находящихся во владении компании и в личном пользовании сотрудников?

Управление

Управление — это важнейшая составляющая процесса внедрения эффективной сетевой безопасности. Основной целью при переходе на межсетевой экран нового поколения должно стать максимальное упрощение процесса управления безопасностью за счет более эффективной визуализации и контроля приложений. Разрабатывая техническое задание на межсетевые экраны нового поколения, обязательно используйте следующие вопросы и утверждения.

- Требуется ли для управления устройствами отдельный сервер или устройство?
- Опишите все поддерживаемые средства управления: интерфейс командной строки; браузер; клиентское ПО; централизованный сервер.
  - При описании каждого из поддерживаемых средств управления определите, насколько легко или сложно переключаться с одного средства на другое.
- Дайте описание архитектуры централизованного управления и вариантов внедрения.
- Какие инструменты визуализации, кроме средств просмотра журналов и составления отчетов, обеспечивают четкую картину работы приложений и пользователей, а также перемещения данных в сети?
  - Включены ли инструменты визуализации в базовый набор функций, или же они предлагаются за дополнительную плату/по дополнительной лицензии?
  - Предлагаются ли инструменты визуализации уже готовыми для использования, или они развертываются на базе отдельного устройства?
- Опишите подробно все действия, необходимые для получения полной и детальной картины трафика всех приложений в сети.
- Возможна ли активация средств управления, включенных в политику приложений и политику межсетевого экрана, а также средств предотвращения угроз, в рамках одного правила в редакторе политик межсетевого экрана?
- Опишите функции ведения журналов и формирования отчетов: предлагаются ли они готовыми для использования? Если да, то насколько снижается производительность при активации процесса ведения журналов?
  - Является ли система полного анализа журналов готовой для использования, или она предлагается за дополнительную плату/по дополнительной лицензии или развертывается на отдельном устройстве?
- Предлагаются ли полностью настраиваемые инструменты формирования отчетов, позволяющие понять, как используется сеть, а также отследить изменения в характере ее использования?
  - Верно ли, что они предлагаются за дополнительную плату/по дополнительной лицензии или развертываются на отдельном устройстве?
- Опишите, каким образом обеспечивается доступ к средствам управления, когда устройство перегружено трафиком.
- Опишите характер взаимосвязи средств управления отдельными устройствами и средств централизованного управления несколькими устройствами.
- Опишите различия в управлении аппаратными и виртуализированными экземплярами.

Производительность

Реальная производительность — это важнейший фактор, который следует учитывать при внедрении систем безопасности. Для успешного управления приложениями требуется более глубокий анализ трафика, чем при использовании межсетевых экранов, работающих на основе портов и в силу этого требующих большего количества вычислительных ресурсов. Добавление проверки на наличие угроз и управление на базе политик в отношении такого трафика только увеличит нагрузку на межсетевой экран, связанную с обработкой данных. Важно определить реальную производительность, когда включены все функции безопасности и выполняется анализ реального сетевого трафика. Разрабатывая техническое задание на межсетевые экраны нового поколения, обязательно используйте следующие вопросы и утверждения.

- Проверьте, является ли устройство программно-определяемым продуктом, сервером OEM или специализированным устройством.
- Проанализируйте аппаратную архитектуру, чтобы убедиться в наличии процессорной мощности, достаточной для выполнения постоянной классификации и проверки трафика на уровне приложений.
- Опишите комбинации трафика, используемые для выявления и публикации показателей производительности:
  - Межсетевой экран + ведение журналов
  - Межсетевой экран + управление приложениями
  - Межсетевой экран + управление приложениями + предотвращение угроз
- Какова номинальная пропускная способность при следующих комбинациях трафика:
  - Межсетевой экран + ведение журналов
  - Межсетевой экран + управление приложениями
  - Межсетевой экран + управление приложениями + предотвращение угроз

Дополнительные рекомендации при составлении технического задания

В каждой организации наверняка будут свои требования, выходящие за рамки тех, которые представлены в этом документе. Они могут касаться рентабельности компании, рекомендаций клиентов, простоты внедрения, а также поддержки сетевого оборудования и маршрутизации. Рекомендации в отношении составления технического задания должны быть четко структурированы. Только тогда производитель сможет убедительно доказать, что все заявленные возможности решения соответствуют истине.

Факторы, влияющие на производительность
Важно определить реальную производительность, когда включены все функции безопасности и выполняется анализ реального сетевого трафика.

Оценка межсетевых экранов нового поколения в процессе испытаний

После окончательного выбора поставщика или узкого круга поставщиков, выполненного с помощью заявки, наступает этап оценки физических функций межсетевого экрана, выполняемой с применением трафика различных типов и комбинаций, а также объектов и политик, которые точно передают особенности бизнес-процессов организации. В этом разделе представлен ряд рекомендаций, касающихся оценки физических аспектов межсетевого экрана нового поколения. Такая оценка позволит в реальной среде определить, насколько полно и эффективно межсетевой экран выполняет основные требования. Обращаем внимание на то, что испытания, представленные ниже, включают примерный перечень функций, которыми должен обладать межсетевой экран нового поколения. Эти примеры являются инструкциями, на базе которых затем разрабатывается более подробный, пошаговый план испытаний.

Визуализация и контроль приложений

В данном разделе мы преследуем три цели. Во-первых, донести до читателя тот факт, что основной задачей проверяемого устройства является классификация трафика на основе идентификации приложений, а не сетевых портов. Во-вторых, подчеркнуть, что проверяемое устройство классифицирует все без исключения приложения, независимо от тактик маскировки, которые они могут использовать (изменение портов, использование нестандартных портов или другие тактики обмана). В-третьих, доказать, что идентификация приложений является основой политики межсетевого экрана, а не одним из элементов второстепенной политики.

Идентификация приложений

- Убедитесь в том, что межсетевой экран может идентифицировать различные приложения. Идеальный способ проведения такого испытания — развернуть проверяемое устройство в режиме разветвителя или прозрачном режиме в целевой сети.
- Убедитесь в том, что проверяемое устройство правильно идентифицирует трафик приложений, используя графические инструменты, инструменты обобщенного уровня и инструменты для аналитических исследований.
  - Определите интенсивность административных процессов, связанных с выполнением этой задачи.
- Оцените шаги, необходимые для начальной идентификации приложений. Насколько быстро пользователь может задать политику и начать «просматривать» трафик приложений? Требуются ли дополнительные шаги, чтобы добиться визуализации приложений, меняющих порты или использующих нестандартные порты?

Идентификация приложений, меняющих порты или использующих нестандартные порты

- Убедитесь в том, что межсетевой экран может идентифицировать и контролировать приложения, использующие вместо порта по умолчанию другие порты. Например, SSH — порт 80 и Telnet — порт 25.
- Убедитесь в том, что межсетевой экран может идентифицировать приложения, меняющие порты, такие как Skype, AIM или одно из многих одноранговых приложений.

Идентификация приложений как основа политики безопасности межсетевого экрана

- Убедитесь в том, что при создании политики межсетевого экрана в качестве основного элемента политики определяется приложение, а не порт.
  - Требуется ли для политики контроля приложений сначала установить правило, связанное с идентификацией по портам?
  - Является ли элемент контроля приложений абсолютно отдельным редактором политики?
- Создайте политику, которая будет разрешать одни приложения и блокировать другие, а затем проверьте, контролируются ли приложения так, как планировалось.
- Поддерживает ли политика, основанная на идентификации приложений, стратегию «запрещать все остальные», на которой базируется работа межсетевого экрана?

Идентификация и контроль приложений для обхода защиты

- Убедитесь в том, что проверяемое устройство способно идентифицировать и контролировать приложения, используемые для обхода средств обеспечения безопасности. К приложениям этой группы относятся внешние прокси (PHproxy, Kproxy), средства доступа к удаленному рабочему столу (RDP, LogMeIn!, TeamViewer, GoToMyPC) и зашифрованные туннельные приложения, не относящиеся к VPN (Tor, Hamachi, UltraSurf).
- Убедитесь в том, что во время испытания точно идентифицируется каждое приложение для обхода средств защиты.
- Убедитесь в том, что можно заблокировать любое приложение для обхода средств защиты, даже если оно использует нестандартный порт.

Идентификация и контроль приложений, использующих SSL или SSH

В условиях все более широкого распространения приложений, использующих шифрование SSL, и приложений, использующих SSH не по назначению, требуется оценить возможность межсетевого экрана идентифицировать и контролировать приложения, использующие протоколы SSL и SSH.

- Убедитесь в том, что проверяемое устройство способно выполнять идентификацию и дешифрацию приложений, заведомо использующих шифрование SSL.
- Убедитесь в том, что проверяемое устройство способно выполнять идентификацию и дешифрацию приложений и применять политику к дешифрованному приложению.
- Убедитесь в том, что если приложение, прошедшее дешифрацию, «разрешается», оно снова зашифровывается и направляется к цели.
- Убедитесь в возможности выполнять дешифрацию и проверку SSL в отношении входящего и исходящего трафика.
- Проверьте точность идентификации SSH, независимо от порта.
- Убедитесь в том, что контроль за SSH позволяет определить цель использования этого протокола — переадресация портов (локальная, удаленная, X11) или предназначенное использование (SCP, SFTP и доступ к оболочке).

Идентификация и контроль приложений, использующих одно и то же соединение

Определите, выполняют ли механизмы классификации приложений непрерывный мониторинг состояния приложения, отслеживая изменения. Особое внимание обратите на то, правильно ли классифицируется изменение состояния. Многие платформы (Google, Facebook, Microsoft) предоставляют пользователям, осуществившим начальный вход в систему, доступ к разным приложениям. Способность отслеживать подобные изменения в состоянии приложений является важнейшей особенностью межсетевых экранов нового поколения.

- Используя такое приложение, как WebEx или SharePoint, убедитесь в том, что проверяемое устройство идентифицирует исходное приложение (как WebEx или SharePoint).
- Не выходя из системы приложения, перейдите к отдельной функции (WebEx Desktop Sharing, SharePoint Admin, SharePoint Docs) и убедитесь в том, что изменение в состоянии отслеживается и новое приложение/функция идентифицируется верно.
- Проверьте механизмы проверки и контроля на базе политики на примере определенной функции приложения.

Контроль функций приложения

Определите возможность проверяемого устройства идентифицировать и контролировать конкретные функции приложения. Контроль на уровне функций имеет огромное значение при разрешении использования приложения, поскольку усиливает контроль над бизнес-рисками и рисками безопасности. Наиболее распространенным примером может служить передача файлов, однако это касается и таких функций родительских приложений, как администрирование, VoIP, публикации в социальных сетях и чат.

- Убедитесь в том, что проверяемое устройство дает визуальное представление об иерархии приложения (основного приложения и совокупности функций).
- Проверьте, как осуществляется контроль функций передачи файлов, выполнив идентификацию и контроль приложения, поддерживающего передачу файлов.
- Убедитесь в возможности проверяемого устройства блокировать выгрузку/загрузку файлов, основываясь на типе приложения и файла. Например, убедитесь в возможности предотвратить передачу документа Word при использовании web почтового клиента.

Возможность контроля неизвестного трафика

В небольших количествах неизвестный трафик присутствует в каждой сети, и вам необходимо определить, насколько быстро вы можете выявлять такой неизвестный трафик и предпринимать соответствующие действия.

- Проверьте, доступна ли вам визуализация неизвестного трафика, которая должна обеспечивать хотя бы следующие данные:
  - объем трафика;
  - пользователь и/или IP-адреса;
  - используемый порт;
  - связанное содержимое — файл, угроза и т. д.
- Насколько легко или тяжело выявить и проанализировать неизвестный трафик?
- Можно ли задать политику межсетевого экрана (разрешение, блокировка, проверка и т. д.) в отношении неизвестного трафика?
- Удостоверьтесь в наличии средств для более точной идентификации и контроля неизвестного трафика приложений.
  - Возможно ли «переименование» трафика?
  - Может ли пользователь создать свой механизм идентификации?
  - Предоставит ли поставщик собственный механизм идентификации? Если да, то как быстро?

Сокращение систем, подверженных атакам
Чтобы защитить свою сеть, необходимо строго контролировать угрозы и предотвращать их проникновение вместе с трафиком разрешенных приложений.

Предотвращение угроз

Чтобы защитить свою сеть, необходимо строго контролировать угрозы и предотвращать их проникновение вместе с трафиком разрешенных приложений. Вам необходимо проверить возможности проверяемого устройства соблюдать политику безопасности в реальной среде, включающей ранее неизвестные угрозы; угрозы, которые несут с собой приложения, использующие нестандартные порты; угрозы, завуалированные процессом сжатия; а также проверить, соблюдаются ли при этом требования организации в отношении производительности.

- Убедитесь в детализации профилей предотвращения угроз — носят ли они глобальный характер, или их можно задавать индивидуально, основываясь на трафике, характере угроз, пользователях и т. д.
- Убедитесь в том, что техники предотвращения угроз (системы обнаружения вторжений, блокировка вредоносного ПО, контроль передаваемого содержимого) одинаково применяются ко всем приложениям (и угрозам), которые могут использовать нестандартные порты. Это означает, что требуется не только контроль приложений на нестандартных портах силами проверяемого устройства. Необходимо, чтобы механизм предотвращения угроз остановил распространение угроз через эти нестандартные порты.
- Убедитесь в том, что проверяемое устройство выявляет вредоносное ПО и не утвержденные файлы даже после сжатия (ZIP или GZIP).
- Определите процесс идентификации и блокировки неизвестного вредоносного ПО.
- Установите производительность проверяемого устройства при активации всех средств предотвращения угроз, что позволит убедиться в их практической пригодности.

Защита удаленных пользователей

Сначала следует определить, обеспечивает ли проверяемое устройство защиту удаленных пользователей с помощью политики безопасности, используемой в периметре сети. Затем следует определить, насколько сложны процессы управления и внедрения.

- Определите, обеспечивает ли проверяемое устройство защиту удаленных пользователей, использующих несколько соединений SSL VPN или транзитных соединений.
- Проверьте простоту внедрения и управления, создав группу удаленных пользователей и развернув для них тестовую политику.
- Может ли проверяемое устройство предоставлять политики, основанные на типе устройств?
- Может ли проверяемое устройство защитить от мобильного вредоносного ПО и от уязвимостей мобильных ОС?
- Способно ли проверяемое устройство обеспечить контроль мобильных приложений?
- Завершите испытание, выполнив мониторинг удаленных пользователей с помощью средства просмотра журналов.

Управление

Необходимо оценить сложность управления проверяемым устройством в аспекте отдельных устройств, а также сложности (количество шагов, понятность интерфейса пользователя и т. д.) выполняемой задачи.

- Определите методику управления проверяемым устройством. Требуется ли отдельное устройство или сервер для индивидуального управления устройствами? Возможно ли управление проверяемым устройством с помощью браузера, или требуется «толстый» клиент?
- Проверьте наличие инструментов визуализации, которые обеспечивают «сетевой интеллект» путем предоставления сводок по приложениям, угрозам и URL-адресам, присутствующим в сети.
  - Хранятся ли журналы централизованно или в отдельных базах данных функционального уровня (межсетевой экран, контроль приложений, система предотвращения вторжений)?
  - Определите интенсивность административных процессов, связанных с анализом журналов с целью визуализации и изучения инцидентов.
- Убедитесь в том, что активацию средств управления, включенных в политику приложений и политику межсетевого экрана, а также средств предотвращения угроз, можно выполнить с помощью одного редактора политик.
  - Создается и применяется ли правило межсетевого экрана на основе портов до средства управления уровня приложений?
  - Используется ли несколько политик (например, межсетевого экрана, контроля приложений, системы предотвращения вторжений)? Имеются ли в наличии инструменты согласования политик, позволяющие выявлять потенциальные разногласия в политиках?

Производительность при активированных сервисах

Контроль приложений требует намного больше вычислительных ресурсов, чем при использовании традиционных межсетевых экранов, работающих на основе идентификации портов. Поэтому так важно проверить, способно ли проверяемое устройство функционировать с достаточной производительностью во время идентификации и контроля приложений.

- Проверьте, является ли проверяемое устройство программно-определяемым продуктом, сервером OEM или специализированным устройством.
- Если это специализированное устройство, проанализируйте его аппаратную архитектуру, чтобы убедиться в том, что его процессорная мощность во время активации всех сервисов отвечает требованиям к сетевой производительности.
- Обязательно выполните эту проверку! Оцените реальную производительность в среде испытаний, используя трафик различных типов и комбинаций, который будет наверняка иметь место в среде целевой сети.

Важные факты об аппаратных и виртуальных форм-факторах

Если планируемым местом внедрения является центр обработки данных, мы рекомендуем воспользоваться описанными выше сценариями испытаний, которые позволят убедиться в том, что эффективность работы межсетевого экрана будет такой же и в виртуальном форм-факторе. Кроме того, если речь идет о виртуализированных средах, обратите внимание на следующие моменты:

- Каков процесс управления политикой, имеющей отношение к взаимосвязи экземпляров виртуальных машин? Каково количество необходимых действий?
- Возможно ли создание политик одинакового типа для физических и виртуальных экземпляров?

- Одинаковый ли набор функций поддерживается в аппаратных и виртуальных экземплярах?
- Убедитесь в том, что проверяемое устройство способно защитить весь трафик между виртуальными машинами, принадлежащими одному виртуальному серверу.
- Убедитесь в том, что проверяемое устройство обеспечивает соблюдение политик в отношении приложений, пользователей и содержимого на одном и том же виртуальном экземпляре.
- Убедитесь в том, что проверяемое устройство обеспечивает соблюдение политик даже при миграции гостевых виртуальных машин.
- Проверьте взаимодействие с системой управления виртуализированной платформы.
- Проверьте взаимодействие с системами автоматизации и оркестровки.

Дополнительные рекомендации по оценке

Процесс оценки и испытаний продуктов сетевой безопасности в разных организациях будет разным и практически во всех случаях не будет совпадать с теми процедурами, которые описаны в данном документе. Это может быть как простота внедрения (режим зеркалирования трафика, прозрачный режим, другое), особенностей сетевой инфраструктуры (L2, L3, смешанный режим) и поддерживаемой маршрутизации (RIP, OSPF, BGP). Для проведения оценки межсетевого экрана следует определить набор конкретных критериев оценки, а затем пропустить каждое устройство через полный набор испытаний, подробно фиксируя все результаты. Только тогда выбор устройства будет носить последовательный характер.

Безопасное разрешение приложений с помощью межсетевых экранов нового поколения

Было время, когда поход, в рамках которого сотрудникам разрешалось использовать внешние или персональные приложения для выполнения своей работы, казался неслыханным. Сегодня сотрудники организаций имеют постоянный доступ к Интернету и часто используют самые современные приложения и для личных, и для рабочих целей. И блокирование этих приложений равнозначно блокированию рабочих процессов.

В разделе *10 обязательных функций межсетевого экрана нового поколения* мы попытались доказать, что самым удачным местом для безопасного разрешения приложений является межсетевой экран, выполняющий идентификацию приложений и использующий политики на базе позитивной модели контроля, которые позволяют администраторам определять, основываясь на требованиях бизнеса, какие приложения следует разрешить, а какие — запретить. Использование инструментов, представленных в этом документе, позволит доказать, что разрешение приложений с помощью негативной модели контроля, работающей по принципу системы обнаружения вторжений, нереально.

О компании Palo Alto Networks

Компания Palo Alto Networks® является лидером по производству систем сетевой безопасности нового поколения. Предлагаемая ею инновационная платформа позволяет предприятиям, поставщикам услуг и правительственным учреждениям защищать сети путем безопасного разрешения все более сложных и многочисленных сетевых приложений, а также путем надежного предотвращения кибератак. Ядром платформы Palo Alto Networks является межсетевой экран нового поколения, оснащенный функциями визуализации и контроля приложений, пользователей и содержимого, интегрированными в аппаратную и программную архитектуру, которая является собственной разработкой компании. Продукты и услуги Palo Alto Networks отвечают широкому ряду требований к сетевой безопасности, обеспечивая защиту самых разных объектов, от центра обработки данных до периметра сети, а также территориально рассредоточенных предприятий с филиалами и растущим числом мобильных устройств. Продукты Palo Alto Networks используются более чем 12 500 клиентами из более чем 100 стран.

Дополнительные сведения можно получить на сайте компании по адресу: www.paloaltonetworks.com.

the network security company™

www.paloaltonetworks.com