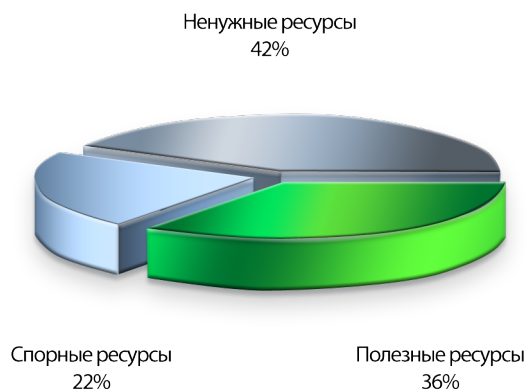


Фильтрация трафика как первый шаг к безопасности сети



Большинство компаний, активно использующих в своей работе ресурсы сети Интернет, сегодня сталкиваются с вопросами, связанными с защитой корпоративной сети, рисками занесения вирусов при посещении сомнительных ресурсов, перегрузки интернет-каналов трафиком, используемом сотрудниками в личных целях, а также вопросами оптимизации затрат компании на Интернет-доступ. Поддерживать столь мощный инструмент, как доступ в Сеть, в рабочем состоянии и обеспечивать целостность и непрерывность бизнес процессов поможет комплексный контроль доступа к Интернет-ресурсам.

Проблема нецелевого доступа в Сеть

По данным статистики, при отсутствии гибкой фильтрации доступа к сети Интернет на долю ненужных и опасных ресурсов, ежедневно посещаемых сотрудниками, приходится порядка 42% от общего трафика, еще 22% занимают ресурсы спорные, и только 36% ресурсов могут быть расценены как полезные и имеющие отношение к работе¹.

Лидерами в списке нежелательных ресурсов являются социальные сети, порталы, выкладывающие контент непристойного содержания, сервера онлайн-игр, а также сайты, генерирующие так называемый «тяжелый» трафик, предлагающие посетителям загружать и просматривать видеоролики и flash-баннеры.

Потенциальные угрозы, возникающие в результате посещения сотрудниками различных категорий не относящихся к работе сайтов, помимо нецелевого использования рабочего времени, могут выглядеть как:

- чрезмерная нагрузка на сеть, вызванная неконтролируемой загрузкой сотрудниками объемных файлов из Интернет. В случае, когда речь идет о постоянном или выделенном подключении с фиксированной скоростью канала от провайдера, просмотр или загрузка пользователями видеочайлов, например, с YouTube или файлообменных сетей негативно скажется на распределении ресурсов сети и загрузке интернет-канала в целом, а также на стоимости нецелевого трафика;
- нерациональное использование ресурсов сети и рабочего времени в результате деятельности офисных любителей онлайн-игр с видео- или голосовыми чатами;
- неконтролируемые удаленные соединения сотрудников с рабочими серверами корпоративных сетей посредством VPN-соединений или утилит, аналогичных Hamachi, несущие риски заражения локальной сети вирусами, потенциально находящимися на удаленном компьютере;
- снижение уровня безопасности корпоративной сети – именно внутренние ресурсы и данные компании часто становятся объектом угроз и рисков при отсутствии полноценного контроля посещаемых сотрудниками сайтов той или иной тематики. По данным Computer Economics, размеры мирового экономического ущерба от различных вирусов могут исчисляться десятками миллиардов долларов в год. Так, например, годовой ущерб, нанесенный вирусом с названием Melissa, оценен в \$1.10 млрд.²

¹ BrightCloud, 2008, <http://www.brightcloud.com/longtail.asp>.

² Computer Economics, 2000.

Зоны рисков

Потенциальными зонами риска распространения вредоносных кодов, фишинговых атак, причинами утечки информации, кражи паролей и других шпионских ухищрений были и остаются порносайты, всем известные социальные сети и блоги, развлекательные порталы и иные сайты взрослого содержания, где ежедневно инфицируются тысячи новых страниц, появляются новые модификации хорошо известных угроз.

Так, например, в 2008 году пользователи социальной сети «В Контакте» стали жертвами сетевого вирусного «червя», который рассылал с инфицированных машин ссылку на зараженный ресурс другим пользователям сети.

Кроме того, по мнению специалистов WatchGuard Technologies³, «атаки на пользователей будут направлены с привычных и не вызывающих подозрений сайтов, которые незаметно заражаются SQL-инъекциями».

Зараженные сайты могут охватывать широкий спектр интересов, а, следовательно, и категорий интернет-ресурсов: от автомобилей, туризма, знакомств, фильмов и музыки до сайтов по трудоустройству, недвижимости и других, на первый взгляд, совершенно безобидных сервисов, предлагаемых сегодня глобальной Сетью. Находящийся на зараженных сайтах вредоносный код, попадая на один компьютер легкомысленного сотрудника, мгновенно распространяется по локальной сети, нанося компании порой неопределимый ущерб.

По статистике большая доля утечек информации приходится именно на действия сотрудников по неосторожности и только малая часть – на целенаправленно подготовленные злоумышленниками атаки.

Несмотря на эти широко известные факты, по данным исследования Vault, порядка 87% служащих посещают социальные и развлекательные ресурсы на работе, выходя в Интернет с подключенных к корпоративной сети рабочих ПК. Причем более 50% делают это как минимум. Необходимо отметить аспект эффективности работы сотрудников: каждые потраченные на прочтение ненужных ресурсов, просмотр фотографий и чтение форумов 5-10 минут в час в конце месяца суммируются в десятки потерянных для компании и оплаченных впустую часов работы.

Механизмы фильтрации трафика

Чтобы обеспечить безопасность и целостность бизнеса, закрыть каналы возможной утечки информации и повысить производительность труда сотрудников на должном уровне, необходимо управлять потоком интернет-трафика, входящего в локальную сеть. Единственно правильным решением в борьбе со стихийным и неконтролируемым трафиком в любой организации должна стать фильтрация интернет-запросов. Запрещая при помощи настройки фильтров доступ к тем или иным ресурсам, можно не только оптимизировать рабочее время сотрудников, но и легко решить вопросы снижения затрат на нецелевые интернет-ресурсы, кроме того, значительно уменьшить риск инфицирования внутренних ресурсов корпоративной сети.

Большинство компаний давно озабочены поиском и внедрением решений надлежащего уровня, позволяющих минимизировать внешние угрозы и контролировать доступ в Интернет.

Компания Entensys с 2001 года активно разрабатывает направления интернет-безопасности и фильтрации интернет-ресурсов. Компания технологически сотрудничает с вендорами-разработчиками систем фильтрации и антивирусных решений, обеспечивая пользователей комплексным решением самого современного уровня. В результате, UserGate Proxy & Firewall⁴ успешно внедрен в тысячах компаний малого и среднего бизнеса, множестве организаций и филиалов государственных структур, а также некоммерческих и образовательных заведениях.

Гибкий инструментальный BrightCloud⁵, эксперта в области фильтрации наполнения сайтов по категориям, интегрирован в UserGate таким образом, что позволяет регламентировать доступ к различным категориям сайтов.

³ WatchGuard Technologies, 2009, <https://www.watchguard.com/latest/security-predictions.asp>

⁴ UserGate Proxy & Firewall – комплексное решение для организации доступа в Интернет и защите сети. Более полная информация на сайте производителя <http://www.entensys.com>

⁵ Американская компания BrightCloud Inc является ведущим разработчиком механизмов URL фильтрации по категориям. Подробная информация на <http://brightcloud.com>

Основная база данных BrightCloud содержит более 450 миллионов постоянно обновляемых интернет-страниц, сгруппированных в 70 основных категорий⁶ сайтов, такие, как «Знакомства», «Игры», «Социальные ресурсы», «Покупки», «Путешествия», «Обучение», «Бизнес и экономика», «Интернет» и многие другие, включающие рейтинги доверия по каждой категории, а также множество интернет-ресурсов на всех основных мировых языках. Особо стоит отметить расширенную поддержку русскоязычных сайтов.

Удобством использования системы фильтрации трафика от UserGate является именно тематическая категоризация нежелательных ресурсов, при внедрении которой нет необходимости перечислять и запрещать отдельно каждый определенный нежелательный сайт вручную, достаточно запретить категорию, и все попадающие под данную тематику ресурсы будут автоматически закрыты для посещения сотрудниками. Кроме того, данный подход позволяет отойти от неэффективного деления множества сайтов на так называемые «черные и белые» листы, делая политику безопасности более гибкой.

Используя различные правила фильтрации, предусмотренные в UserGate, и регулярно анализируя то, что же именно загружают из сети сотрудники, можно значительно сократить нецелевой расход трафика и сократить потери рабочего времени.

UserGate также позволяет настраивать ограничения на загрузку «тяжелых» файлов, например, видео или файлов, превышающих определенный размер. В совокупности с разграничением доступа по категориям сайтов это оптимизирует использование сетевых ресурсов и нагрузку на внешние каналы доступа к сети Интернет, избавляет от лишних затрат на трафик и обеспечивает дополнительную безопасность офисных ПК внутри периметра сети.

Интегрированные антивирусные модули, в свою очередь, обеспечивают фильтрацию входящего трафика на предмет наличия вирусов, пропуская только безопасный трафик и делая защиту локальной сети всесторонней и комплексной.

Заключение

Использование интернет-трафика с каждым днем становится все более масштабным, в связи с этим растет актуальность описанных задач по защите сетей от атак, контролю распространения вирусов и несанкционированной сетевой активности пользователей, снижению нерационального использования ресурсов. Потребность в анализе трафика возросла настолько, что решение, обладающее гибкими механизмами фильтрации, стало жизненно необходимым для множества компаний, использующих Интернет. Описанное решение от компании Entensys позволяет формировать надежную стратегию офисной безопасности, основываясь на гибкой политике фильтрации интернет-ресурсов, исключая потенциальные зоны рисков и предоставляя все возможности для управления целевым доступом в Сеть.

⁶ Полный перечень категорий сайтов представлен на <http://www.brightcloud.com/masterdburllist.asp>