Н.В. Гришина

Интернет-трафик: защита сетевых ресурсов организации

Если первоначально термин «статистика» употреблялся в значении «политическое состояние», то в настоящее время он отражает деятельность человека практически во всех областях. Специалисты отмечают, что благодаря результатам обработки статистической информации можно существенно повысить эффективность деятельности анализируемой системы, а порой предотвратить многие проблемы.

Постобработку статистики обращений к Интернету применяют многие корпорации, в основном для анализа и контроля использования ресурсов.

Задача эта важна с точки зрения как безопасности доступа к открытым сетям, так и более эффективной деятельности организации.

Средства постобработки статистической информации обычно нацелены на выполнение следующих задач:

1) защита внутренней сети от проникновения вредоносных программ за счет ограничения, запрета или организации специализированного доступа пользователей к потенциально опасным ресурсам сети;

2) обнаружение во внутренней сети вирусов и «троянских» программ, которые самостоятельно обращаются к внешним ресурсам;

3) фиксация использования ресурсов сети, не относящихся к работе, с целью блокирования доступа к ним, экономии рабочего времени и снижения трафика;

4) обеспечение возможности снижения внешнего трафика за счет выявления ресурсов и информации, к которым пользователи обращаются наиболее часто;

5) определение наиболее востребованных и часто используемых в работе категорий ресурсов и сайтов;

6) определение подразделений, наиболее активно работающих с ресурсами сети.

Анализ использования ресурсов сети Интернет осуществляется обычно путем обработки и исследования лог-файлов. Для этих целей создан достаточно широкий спектр программных продуктов — как бесплатных, так и коммерческих, как небольших скриптов, так и крупных программных комплексов, способных поддерживать и обрабатывать лог-файлы сразу с нескольких серверов. Одни программные продукты могут обрабатывать различные форматы лог-файлов, другие предназначены для конкретных прокси-серверов. С помощью одних можно получить очень специфическую информацию (например, среднее время обработки запросов различных типов), благодаря другим — детализированные общие отчеты. Отчеты, как правило, можно получить в текстовом или html-формате. Например, быстро получить детальные отчеты в формате html позволяет Webalizer — программа для анализа лог-файлов с открытым исходным кодом, написанная на языке C. Она поддерживает несколько форматов лог-файлов, выдает общую информацию по месяцам: число запросов, полученных файлов, страниц, переданных Кбайт, что позволяет оценить общую загрузку прокси-сервера и уровень активности пользователей. Детальный отчет содержит более подробную информацию: число уникальных пользователей и броузеров, максимальное и среднее за день количество запросов, файлов, страниц и переданных Кбайт, распределе-