

Защита IP-адреса

Автори: С.М. Божаткин; В.А. Гусева-Божаткина, Национальный университет кораблестроения имени адмирала Макарова, г. Николаев

При хорошо развитой и отлаженной структуры телекоммуникаций меняется понятие рабочего места. В настоящее время это не привязка к определённом месту, а, скорее, комплекс средств для выполнения производственной задачи. Универсальным инструментом на сегодняшний день является компьютер, подключённый к интернет. Большое количество онлайн-сервисов привело к тому, что мощность компьютера уже не имеет значение, наличие на сервере службы терминалов даёт возможность перемещаться со своим рабочим местом. При удалённом подключении к серверу канал проходит через несколько коммутационных узлов, что накладывает определённые требования на защиту информации: достоверность, целостность и санкционированный доступ. Все эти задачи довольно хорошо решаются организацией VPN-канала. Но в этом случае возникает проблема – это на каком промежуточном узле оставить IP-адрес своего сервера и не вызвать атаку.

Рассмотрим возможность скрытия своего IP-адреса путём использования анонимных прокси-серверов для маскировки личного IP-адреса пользователя.

Главное преимущество работы прокси-серверов в том, что они расположены по всему миру, что позволяет работать через прокси-сервер в любой стране, и IP-адрес будет замаскирован под человека, проживающего в этой местности.

С помощью прокси-сервера можно скрыть свой реальный IP-адрес, а значит обходить любые запреты для использования IP-адресов, блокировки стран, городов и даже собственных провайдеров. При этом безопасность и анонимность существенно возрастают.

Все прокси-серверы делятся на две большие группы: transparent (прозрачные) и non-transparent (непрозрачные). Если использовать прозрачный- сервер, то надеяться на то, что реальный IP-адрес никто не раскроет, не приходится. При запросе такой прокси-сервер выдаст всю необходимую информацию. А вот при использовании непрозрачного прокси-сервера реальный IP-адрес узнать не удастся. То есть, можно увидеть лишь физическое положение самого прокси-сервера.

Если нет уверенности в том, что достаточно использовать только один анонимным прокси-сервер, то целесообразно использовать последовательность таких серверов, например:

`http://www.pentagon.gov/" target="_top">http://proxy2:port/http://www.pentagon.gov/"
target="_top">http:// proxy1:port/http://www.pentagon.gov/" target="_top">http://proxy2:port/http://
www.pentagon.gov/`

Следует учесть, что не все прокси-сервера могут работать таким образом. В этом случае устанавливается связь с нужным хостом, проходя через целую цепочку прокси-серверов. Если все они непрозрачные, то отследить подключение будет практически невозможно.

Существует, как минимум, два способа использования прокси-серверов:

- вручную (поиск прокси-сервера, проверка на работоспособность, установка и настройка);
- с помощью специальных, как правило, платных программ, которые обеспечивают анонимность интернета.

При ручной настройке прокси-сервера надо выполнить такие действия:

1. Поиск в интернете прокси-листов (списки прокси-серверов).
2. Проверка на работоспособность (методом перебора или другим аналогичным, для исключения «мертвых» прокси-серверов).

3. Собственно выбор прокси-сервера (с учетом его загруженности, местоположения и т.п.).

Порядок настройки браузеров примерно следующий:

- Opera 12.14 и выше : Инструменты → Настройки → Дополнительно → Безопасность → Сеть → Прокси → Серверы;
- Mozilla FireFox 24.0b5 и выше : Инструменты → Настройки → Сеть → Настроить;
- Internet Explorer 8 и выше : Сервис → Свойства обозревателя → Подключения → Настройка сети.

Кроме использования прокси-серверов существуют специальные программы для анонимного серфинга в интернете. Рассмотрим некоторые из них.

Mask Surf – одна из самых удобных программ для анонимного серфинга в интернете. Полностью автоматизирована: сама интегрируется в Internet Explorer и Mozilla FireFox, берет из своих баз анонимные прокси-серверы и тут же импортирует их в браузер. Все настройки интуитивно понятны, очень простая и эффективная в использовании программа. Поддерживает русский язык.

Proxy Switcher Pro – просканирует доступные прокси-сервера, проверит и найдет высокоскоростные. Для каждого прокси-сервера будет указана страна в виде пиктограммы. Достаточно удобная, интуитивно понятная программа, которая работает с высокой скоростью.

Proxyassistant – сразу после старта программа проверяет по своей базе списки прокси-серверов, фильтрует рабочие, и представляет их перечень пользователю. Одним из

достоинств программы является большой выбор прокси-серверов, полностью русский интерфейс и подробная статистика.

Все вышеперечисленные способы лишь повышают безопасность работы в сети, но не исключают возможность атак злоумышленников. Поэтому могут быть рассмотрены как дополнения к существующей защите сервера.

Список литературы:

1. Домарев В. В. Безопасность информационных технологий. Системный подход. - К. : Диасофт, 2004. – 992 с.
2. Стюарт Мак-Клар, Джоэл Скембрей, Джордж Курц. Секреты хакеров. Безопасность сетей - готовые решения.; 4- изд – М.:Вильямс, 2004. – 656 с.
3. Шаньгин В. Ф. Защита компьютерной безопасности. Эффективные методы и средства – М:-ДМК Пресс, 2008. – 349 с.
4. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях – М:-ДМК Пресс, 2012. – 592 с.
5. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты.- М: Книжный мир, 2009. – 352 с.