Các khái niệm liên quan khác

Proxy là gì ?  
Có một số khái niệm về proxy như sau:  
• Proxy là một thiết bị cho phép kết nối vào Internet, nó đứng giữa các workstation trong một mạng và internet, cho phép bảo mật kết nối, chỉ cho phép một số cổng và protocol nào đó, ví dụ: TCP, HTTP, Telnet trên các cổng 80, 23 …. Khi một client yêu cầu một trang nào đó, yêu cầu này sẽ được chuyển đến proxy server, proxy server sẽ chuyển tiếp yêu cầu đến site đó. Khi yêu cầu được đáp trả, proxy sẽ trả kết quả này lại cho client tương ứng. Proxy server có thể được dùng để ghi nhận việc sử dụng internet và ngăn chặn những trang bị cấm.  
• Proxy server là một server đứng giữa một ứng dụng của client, như web browser, và một server ở xa. Proxy server xem xét các request xem nó có thể xử lý bằng cache của nó không, nếu không thể, nó sẽ chuyển yêu cầu này đến remote server.  
• Proxy server là một server đứng giữa một ứng dụng client, như một web browser, và một server thực. Nó chặn tất cả các yêu cầu đến các server thực để xem xem nó có khả năng đáp ứng được không, nếu không thể, nó sẽ chuyển yêu cầu này đến các server thực.  
• Proxy server là một loại buffer giữa máy tính của chúng ta và tài nguyên trên mạng internet mà chúng ta đang truy cập, dữ liệu bạn yêu cầu sẽ đến proxy trước, sau đó mới được chuyển đến máy của bạn.

Mục đích của proxy  
• Tăng tốc kết nối: các proxy có một cơ chế gọi là cache, có chế cache cho phép lưu trữ lại những trang được truy cập nhiều nhất, điều này làm cho việc truy cập của bạn sẽ nhanh hơn, vì bạn được đáp ứng yêu cầu một cách nội bộ mà không phải lấy tin trực tiếp từ internet.  
• Mọi truy cập đều phải thông qua proxy nên việc bảo mật được thực hiện tốt hơn. Thêm danh sách điều khiển truy cập vào các giao thức, yêu cầu các user hoặc các hệ thống cung cấp vài cấp độ xác thực trước khi gán quyền truy cập. Các proxy servser thông minh hơn, thỉnh thoảng được gọi là gateway mức ứng dụng (Application Layer Gateway - ALGs), có thể được hiểu được các giao thức đặc biệt và có thể được cấu hình để đóng khối chỉ các tiểu khu của giao thức. Ví dụ, một ALG cho FTP có thể phân biệt sự khác nhau giữa lệnh “put” và lệnh “get”; một tổ chức có thể cho phép các user “get” các file từ Internet, nhưng không thể “put” các file bên trong trên một server từ xa.  
• Lọc và ngăn cản các truy cập không được cho phép như các trang đồi trụy, các trang phản động …  
• Proxy servers cũng có thể được cấu hình để mã hóa luồng dữ liệu dựa vào các tham số khác nhau. Một tổ chức có thể sử dụng tính năng này để cho phép các kết nối được mã hóa giữa hai địa điểm mà các điểm truy cập của chúng đều trên Internet.

Các bất lợi và những phát sinh từ việc sử dụng proxy server  
• Các client trên mạng được bảo vệ phải được modify một cách đặc biệt. Điều này làm phức tạp việc cấu hình và thêm vào việc quản trị mạng to tát.  
• Proxy server hoạt động như một hệ điều hành đa năng (general-purpose OS), chúng bị tấn công vào các lỗ hỏng bảo mật mà hệ điều hành có thể có.  
• Performance (throughput) của hệ thống xuống cấp khi số lượng các kết nối proxy tăng lên bởi vì gia tăng các tiến trình có liên quan mà hệ điều hành cần điều khiển.  
• Proxy server có nhiều latency (độ trễ) bởi vì hai kết nối TCP riêng lẻ phải được thiết lập trước khi bất kỳ dữ liệu nào có thể được truyền. Các kết nối mới phải mất thời gian thiết lập kết nối cao do phụ thuộc vào “process” của một proxy. Mỗi kết nối yêu cầu một tiến trình riêng.  
• Rất nhiều địa chỉ trên mạng do một lý do nào đó mà bị cấm truy cập đối với người dùng như là các trang web đồi trụy, các trang phản động, có nội dung không lành mạnh… nhưng bằng việc sử dụng proxy thì các client có thể truy cập tới các site này.  
• Các truy cập vượt qua hệ thống phòng thủ qua HTTP proxy và web-based proxy. Chúng ta sẽ thảo luận thêm về vấn đề này khi tìm hiểu sâu vào các kỹ thuật vượt firewall trong các phần sau.

Socks  
SOCKS là chuẩn IEEE, là giao thức proxy điều khiển luồng lưu thông giữa các hệ thống TCP/IP. SOCKS về cơ bản xác định cách cài đặt và cung cấp các dịch vụ firewall, cũng như các dịch vụ kiểm toán, quản lý. Máy chủ SOCKS được cài đặt giữa mạng nội và Internet. Nó cho phép người dùng nội bộ truy cập Internet nhưng ngăn cản người dùng ngoại tìm cách truy cập mạng nội bộ. Bằng cách này, nó cung cấp dịch vụ firewall một chiều. Một thành phần quan trọng của SOCKS là khả năng “ngu hóa” người dùng nội và máy chủ ngoại bằng cách cho chúng tin rằng họ đang nói chuyện trực tiếp với nhau. Thật tế, người dùng nói chuyện với máy chủ SOCKS và máy chủ SOCKS nói chuyện với máy chủ khác ở mạng bên ngoài.  
Ba thao tác quan trọng của SOCKS là:  
• Cung cấp cách để người dùng yêu cầu kết nối ngoài từ proxy server. Yêu cầu này chứa địa chỉ của máy chủ (đích) và các thông tin thích hợp khác.  
• Thiết đặt mạch giữa khách và proxy server. Một khi mạch được thiết lập, người dùng nghĩ rằng họ đang truy cập trực tiếp Internet.  
• Chuyển tiếp dữ liệu giữa mạng bên ngoài và mạng bên trong.

Bức tường lửa High-end  
Một kết nối internet dựa trên bộ định tuyến cho phép kết nối điểm-điểm giữa khách trên mạng nội bộ và máy chủ internet. Vì các kết nối như thế nói chung không an toàn, người điều hành mạng phải chuyển sang sử dụng các firewall đầu cuối trên (high-end).  
Gateway mức ứng dụng cung cấp các proxy điều khiển truy cập qua firewall theo một cách duy nhất. Chúng hiểu rõ các giao thức của ứng dụng được phép vận hành qua lại thông qua gateway, và quản lý toàn bộ luồng lưu thông vào ra, trong trường hợp không thể dùng bộ định tuyến kiểm tra.  
Dịch vụ FTP là ví dụ tốt minh họa về cách proxy server mức ứng dụng cung cấp kỹ thuật lọc cao cấp. Nó cho phép người dùng từ ngoài truy cập máy chủ FTP, nhưng vẫn nhìn trong mỗi gói và ngăn chặn những gói chứa lệnh PUT đối với một số người dùng. Điều này giúp tránh việc ghi các tập tin vào máy chủ.  
Một đặc điểm quan trọng của các máy chủ mức ứng dụng là kiểm tra tính hợp lệ. Bạn có thể cho phép chỉ những người dùng nhất định qua được firewall trên cơ sở những đặc quyền của họ. Điều này rất hữu ích đối với những người dùng di động hoặc những người thuộc chi nhánh cần truy cập đến một số hệ thống trên mạng của bạn.  
Firewall cũng có thể che dấu địa chỉ mạng nội bộ từ internet. Điều này cho phép bạn cài đặt bất cứ sơ đồ địa chỉ IP mà không cần đăng ký với các tổ chức internet. Đặc điểm này ngày càng hữu ích vì các địa chỉ IP đang trở nên hiếm hoi.

So sánh các tính năng của Firewall

Host-based firewall so với network firewall  
Host-based firewalls (còn được gọi là các firewall cá nhân) là đơn giản, các chương trình hoặc các thiết bị chi phí thấp, được dùng để bảo vệ một máy đơn lẻ. Ví dụ: ZoneAlarm, Norton Personal Firewall, và Internet Connection Firewall (ICF) được xây dựng cho Windows XP.  
Network firewall có thể bảo vệ nhiều máy. Tuy nhiên, không phải tất cả các network firewall đều như nhau. Có vài thiết bị hoặc chương trình mà giá của nó chỉ đắt hơn một chút so với firewall cá nhân.  
Các enterprise firewall dùng cho mục đích kinh doanh, chúng được thiết kế cho các mạng rộng lớn và phức tạp. Chúng điều khiển nhiều user, có thông lượng cao, và có nhiều tính năng tiên tiến, như là:  
• Hợp nhất với các VPN gateway  
• Khả năng quản lý nhiều firewall trung tâm  
• Cơ chế giám sát và báo cáo tinh vi  
• Có thể được mở rộng thông qua các add-on module hoặc plug-in  
• Khả năng điều khiển truy cập thông qua các chính sách và áp dụng các chính sách khác nhau cho các user khác nhau  
• Có nhiều cơ chế xác thực tinh vi  
• Rất tốt trong việc cân bằng tải và khả năng chịu lỗi cao  
Chi phí cho host-based firewall thường là $100 hoặc thấp hơn. Enterprise firewall có thể trên $25,000. Các firewall dùng cho mục đích kinh doanh mức trung bình chi phí khoảng từ $1500 tới $5000.

Các firewall phần cứng so với các firewall phần mềm  
Firewall phần cứng có thể được phân chia thành những thứ chuyên dùng cho các PC với các đĩa cứng và những thiết bị bán dẫn xây dựng trên kiến trúc ASIC (Application Specific Integrated Circuit).  
Firewall phần mềm bao gồm Microsoft ISA Server, CheckPoint FW-1 và Symantec Enterprise Firewall dùng cho cả cấp độ xí nghiệp lẫn các firewall cá nhân. ISA Server chạy trên Windows 2000/2003, và FW-1 chạy trên Windows NT/2000, Solaris, Linux, và AIX. Symantec EF chạy trên Windows và Solaris.  
Firewall phần cứng bao gồm Cisco PIX, Nokia, SonicWall, NetScreen, Watchguard,…

**Sự khác nhau giữa Firewall và Proxy**

[Leave a comment](https://systemvn.wordpress.com/2014/11/24/su%cc%a3-khac-nhau-giu%cc%83a-firewall-va-proxy/#respond)Posted by [sse7en](https://systemvn.wordpress.com/author/sse7en/) on November 24, 2014

Proxy và Firewall là thành phần quan trọng và luôn có trong những hệ thống mạng. Điểm khác nhau giữa Proxy và FW luôn là điều tranh cãi giữa các System Admin. Mặc dù cả 2 đều là những điều căn bản nhất. Tùy theo định nghĩa của mỗi người, nên mỗi người sẽ có một cách define khác nhau. Để các bạn hiểu rõ hơn về 2 thứ này. Trường đã sưu tầm 1 bài viết mà mình thấy khá hay. Mạn phép giữ nguyên bản English không dịch ra nhé. ( Mà Trường có dịch ra cũng không chính xác lắm đâu  ).

**Difference Between a Firewall and a Proxy Server**

A firewall and a proxy server are both components of network security. To some extent, they are similar in that they limit or block connections to and from your network, but they accomplish this in different ways. Firewalls can block ports and programs that try to gain unauthorized access to your computer, while proxy servers basically hide your internal network from the Internet. It works as a firewall in the sense that it blocks your network from being exposed to the Internet by redirecting Web requests when necessary.

**Blocking Malware** Firewalls and proxy servers both can help you block viruses and other forms of malware from infecting your computers. A firewall can block ports commonly used by malicious viruses and worms. You can also use the firewall to specify which ports can be open. Common ports that are usually open are HTTP (port 80), SMTP (port 25) and POP3 (port 110). You may wish to leave certain other ports open as well, while closing other ports. Proxy servers, on the other hand, create a barrier by being the “middleman” that sits between your network and the Internet. Users outside your network can see only your proxy server, while those inside the network can access the Internet only by passing through the proxy. This limits the window of opportunity through which viruses and worms can enter.

**Blocking Programs** A firewall can prevent programs from running on your computer. A proxy server cannot do this. Specific programs such as games and instant messaging applications can be blocked by the firewall. You can also block services and create exceptions for programs that you wish to allow.

**Blocking Websites** You can block websites through a firewall, but you may bring your Internet access down. A firewall can block port 80, which the HTTP protocol uses to serve Web pages, but if you do this, you won’t be able to access any websites at all. A proxy server is better suited to this task in that it is more discriminating in filtering websites. For example, you can choose to block all social networking sites during office hours but allow access to them during lunch breaks and after hours. Some proxy servers have the option to categorize websites, making it easier for you to block all entertainment websites or all adult websites without having to type Web addresses one by one. Functional Differences A firewall essentially blocks communication, while a proxy server simply redirects it. When you cannot access a website because a proxy is blocking it, it is not exactly blocking the communication. When a user tries to access a disallowed website, the proxy server has an internal mechanism that redirects those requests to a Web page in your network. It appears to the user that the website is blocked, but the request was simply redirected to point to something else. Other Proxy Server Functions A proxy server is not only capable of redirecting websites, but it can also cache them. If users access a particular website every day, instead of fetching pages from the site again and again, the proxy server simply sends cached information to the users. This considerably reduces network traffic because your request won’t have to go out to the Internet every time.