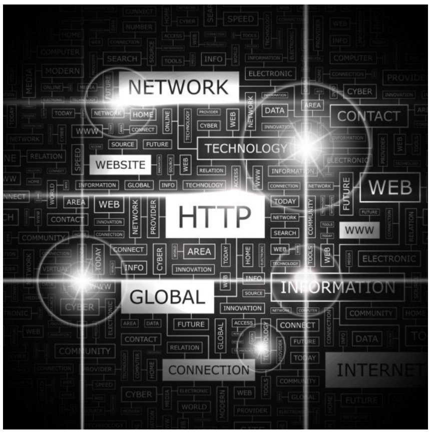
HTTP Tunneling – Connections Through Restrictions

Udemy Editor

Share this article



You want to allow internet access to a certain group of people in your company without compromising the entire network security. You need to use your Internet applications safely from behind a restrictive firewall, or you don't want your work to be monitored in your office. How do you achieve each of the above jobs? HTTP tunneling is the simple solution to resolve the above problems. It is used to bypass firewalls and other network restrictions and an HTTP tunnel is used to create a direct network link between two locations.

But before proceeding further, let us look into the meaning of some of the terms we will use in this context.

Commonly Used Terms

HTTP

HTTP or Hyper Text Transfer Protocol is the network protocol or language used by web browsers to communicate with web servers. HTTP defines how messages should be formatted and transmitted, what actions web servers and browsers should take in response to various commands. For example, when you enter a URL as the web address, an HTTP command is sent to the web server directing it to fetch and transmit the requested web page. HTTP is called a stateless protocol because each command is executed independently, without any knowledge of the preceding commands.

Tunneling

Tunneling, also known as "port forwarding," is the method of transmitting private network data and protocol information through public network by encapsulating the data. Tunneling is when instead of sending a packet directly through the network, the data is sent inside another encrypted connection. Tunneling can be achieved by nearly all protocols. A tunnel is used to ship a foreign protocol across a network that normally wouldn't support it. You can take protocol A and wrap it or put it in a tunnel with protocol B. If you want to refresh your knowledge on TCP/IP models, Network Protocols, Network security, VPNs then CompTIA Network+ N10-005 is an excellent course to browse through.

Tunneling provides the basic underlying structure for setting up a VPN or Virtual Private Network. VPN is a network that is constructed by using public connections, usually the internet to connect to a private network, such as a company's internal network. The process involves use of encryption and transmission protocols to create secure virtual tunnels for data transmission. This ensures that only authorized users can access the network and that the data cannot be intercepted. Data is transmitted in the form of packets over the Internet. The information contained in a data packet is called the payload and contains the routing information required to transmit the packet to a remote destination.

In VPN connection, a tunnel provides a secure medium for data exchanged between the corporate intranet, remote users, and networks of branch offices, suppliers, and business partners. The creation of a tunnel requires the following:

- Carrier protocol: This is the network transport protocol to be used as the carrier protocol, for example PPP.
- Encapsulation protocol: This protocol will encapsulate the payload of a data packet.
- Passenger protocol: Refers to the protocol used by the by the data packets that are being transmitted through the tunnel. NetBEUI is an example of passenger protocol.

What is HTTP Tunneling?

HTTP tunneling is the process in which communications are encapsulated by using HTTP protocol. An HTTP tunnel is often used for network locations which have restricted connectivity or are behind firewalls or proxy servers. A firewall is typically a computer and software that sits between a group of client users and the wider outside Internet or intranet. The firewall is used to protect the internal client network from unauthorized access from outside the firewall.

Certain networks may have restricted connectivity in the form of blocked TCP/IP ports. Traffic is restricted from outside the network to secure it from internal and external threats and most network protocols are restricted except a few which are used for secured communication. If a user, for example, in a corporate environment has no permission to open TCP connections the user cannot use certain services or connect to the internet. In such a case, HTTP tunneling is a possible solution, when the protocol is encapsulated inside HTTP requests that can pass through the firewall or HTTP proxy. In HTTP tunneling, HTTP protocol acts as a wrapper for a channel that the network protocol being tunneled uses to communicate. HTTP tunnel software is used for this purpose which consists of client-server HTTP tunneling applications that integrate with existing application software, and allow them to communicate in restricted network connectivity. The application plays the role of a tunneling client. HTTP tunnel clients are used to access applications from behind restrictive firewalls or proxy servers, to access blocked sites, or to share confidential resource over HTTP securely.

How to Implement HTTP Tunneling?

When a HTTP connection is made through a proxy server, the client, which is usually the browser, sends the request to the proxy. The proxy opens the connection to the destination, sends the request, receives the response and sends it back to the client. The HTTP protocol specifies a request method called CONNECT. The CONNECT method can be used by the client to inform the proxy server that a connection to some host on some port is required. The proxy server tries to connect to the destination address specified in the requested header. If the operation fails, it sends a negative HTTP response back to the client and closes the connection. If the operation succeeds, it sends back an HTTP positive response and the connection is established. After that, the proxy server transmits and forwards all data in both directions between the client requesting the connection and the destination. It acts as the tunnel for this communication.

In some networks, the use of CONNECT method is restricted to some trusted sites. In such cases, an HTTP tunnel can still be implemented using only the usual HTTP methods as POST, GET, PUT and DELETE. In this case, the server runs outside the protected network and acts as a special HTTP server. The client program is run on a computer inside the protected network. Whenever any network traffic is passed to the client, it repackages it as an HTTP request and relays it to the outside server, which extracts and executes the original network request for the client. The response to the request, which was sent to the server is repackaged as an HTTP response and relayed back to the client. Since all traffic is encapsulated inside normal GET and POST requests and responses, this approach works through most proxies and firewalls.

Conclusion

Next time if you want to use your Internet applications safely despite restrictive firewalls and want an extra layer of protection against hackers, spyware, ID theft, then using HTTP tunnel may be the right option for you. IT Security Beginner: Certified Hacking Training course unfolds exciting facts on cyber threats and security.

Page Last Updated: May 2014