Title:
Define Port Forwarding

Word Count:
714

Summary:
Port forwarding, often referred to as .tunnelling. is the forwarding of network ports from one network device to another. This is commonly done using a NAT (network address translation) enabled router or server and another computer within the local network.

Keywords:
Define Port Forwarding

Article Body:
Port forwarding, often referred to as .tunnelling. is the forwarding of network ports from one network device to another. This is commonly done using a NAT (network address translation) enabled router or server and another computer within the local network. The main purpose of using port forwarding is to allow hosts outside your local network who doesn.t have their own public IP address access to some services running on machines within your LAN.
Port forwarding is easy to set up on a router since the management interface allows for easy configuration. In some cases this easy configuration feature might be a problem since most routers cannot provide complex customization for port forwarding and other services. In such case a Linux box can do the job. With Linux, port forwarding is configured by adding iptable rules with a DNAT target to the PREROUTING chain and a SNAT target to the POSTROUTING chain. After doing so iptables will use the existent masquerade table to rewrite packages so they will reach the desired host in concordance with the port forwarding rules you provided. This is similar to OSX and BSD, however ipfw is used. In most cases ipfw is already compiled with kernel.
With port forwarding you can use a router to connect to the Internet and also run a web-server or a FTP server on a computer with your LAN. By using port forwarding you can instruct the router to forward all information that comes on a specific net port (such as 80 for the web-server or 21 for the FTP server) to a host within the local network. This means that if an outside host try to make a HTTP request towards the public IP the router has, it will be sent to the machine known to handle such request within the LAN. This is done in a transparent manner, meaning that the network client is not aware of the fact that he is accessing a machine found somewhere in the LAN. Applications of such

methods are widely used both in business environments and in small home networks.

With more and more devices in the home needing to be connected to the internet or to each other, the router has become a very popular device worldwide. In such situations port forwarding is used to allow access within the network for applications that require access on a specific port, such as games or multimedia streaming software.eaming softwaR.th port forwarding you can use a router to connect to the Internet and also run a web-server or a FTP server on a computer with your LAN. By using port forwarding you can instruct the router to forward all information that comes on a specific net port (such as 80 for the web-server or 21 for the FTP server) to a host within the local network. This means that if an outside host try to make a HTTP request towards the public IP the router has, it will be sent to the machine known to handle such request within the LAN. This is done in a transparent manner, meaning that the network client is not aware of the fact that he is accessing a machine found somewhere in the LAN. Applications of such methods are widely used both in business environments and in small home networks. With more and more devices in the home needing to be connected to the internet or to each other, the router has become a very popular device worldwide. In such situations port forwarding is used to allow access within the network for applications that require access on a specific port, such as games or multimedia streaming software.

Forwards are possible with larger networks. This is done when one router or server forward packets to another router or server that delivers it to the host that should handle it. Such methods are rarely used in small home networks, but can become useful in larger networks whether or not they are connected to the Internet.

Port forwarding can be more secure than using other methods such as a DMZ (demilitarized zone). When using a DMZ all the ports of your machine are forwarded, thus you are no longer truly behind the firewall. Port forwarding provides you security by only allowing access to ports you specifically select.