
DMZ—Doesn't Mean Zebras (It's an important security component of your home/home-business network)

Almost every broadband router on the market today has the ability to help you create a DMZ (Demilitarized Zone - yup, the name comes from the area between the two Koreas). But what is a DMZ and why is it important in your efforts to protect your network and valuable business data?

The DMZ—What is it?

A DMZ is a “neutral zone” between your home network and the public Internet. It isn't part of your home network nor is it part of the Internet—it's a “virtual area” on the broadband router—and/or specified “host” computers that receives requests from users on the home network for access to companies or web sites on the Internet. It then sends these requests out to the destination hosts. The DMZ cannot, however, initiate sessions back into the home network.

The DMZ also receives all requests for access from users “outside” the home network. This means that no requests for access go directly to a host or computer on your home network, they're blocked right at the broadband router. If however, you have a web server on your home network and want to allow public access to it, the DMZ will allow access to that host—and no others, protecting other computers—and your data from attack.

Why You Need It

TCP/IP (the protocol used on the Internet) defines “ports” for different applications through a protocol identifier that indicates what should be done with incoming data. Every application—your children's online game, Voice over IP, web traffic, file transfers, etc. all use a specific TCP/IP port (0-1023 defined by the Internet Assigned Number authority—IANA). Using your DMZ capability, you can block—or allow—applications/users access to services at the TCP/IP port level. So, should a “hacker” attempt a Denial of Service attack, and you have blocked all access, except to your web server—the only place the hacker could attack on your network would be the web specific (HTTP) host/applications on your network.

It Sounds So Complex....

It may sound complex, but the broadband router companies have simplified setting up your DMZ and made it less “technical” and more “user friendly”. Instead of having to know what a TCP port is and what applications use which port numbers, most broadband routers simply identify a number of common Internet applications and allow you to block them all, some or just one or two of them. Usually, you'll get ‘drop down’ list of applications—and you can choose which ones to allow—or block.

We've included a link (below) to show how to setup (as an example) a PlayStation behind a Linksys router using DMZ functionality.

So there's no longer an excuse! Make sure you configure your broadband router today—and implement a DMZ

http://linksys.custhelp.com/cgi-bin/linksys.cfg/php/enduser/std_adp.php?p_faqid=728&p_created=1084220269&p_sid=vVrPr_rh&p_lva=&p_sp=cF9zcmNoPTEmcF9zb3J0X2J5PSZwX2dyaWRzb3J0PSZwX3Jvd19jbnQ9NDMwJnBfc2VhcmNoX3R5cGU9c2VhcmNoX25sJnBfcHJvZF9sdmwxPSZwX3Byb2RfbHZsMj0mcF9zY2ZfbGFuZz0xJnBfcGFnZT0xJnBfc2VhcmNoX3RleHQ9ZG16IHNIIdHVw&p_li=

December, 2004