

Re: Problem with IPSEC

internal subnets is allowed, and outside those subnets is completely blocked. But if I do the same thing, allow all traffic from a first internal subnet to an external IP address (even allowing all ports from that address) IPSEC doesn't allow it. I'm only using RRAS for a firewall and if I turn off the IPSEC blocking of all TCP the internet all works.

Steven L Umbach wrote:

No it is not a bug in ipsec. Many websites, especially the larger volume websites use multiple websites links/IP addresses. What you want to do may work if you are trying to allow a simple website that uses a single or a couple IP address. You can see what I mean if you use something like Ethereal while connecting connect to a website. Also when you enter a DNS name it will resolve to the IP addresses it currently finds to create the filter. However I have seen many large websites then seem to use dozens of IP addresses for their main website that seem to change frequently time you access them. You can sometimes see this when use nslookup to resolve a domain name and try it a couple of times. A better solution would be to use something like ISA 2004 to restrict access though that is not a trivial investment in software/licenses and configuration time. Otherwise try using a packet sniffer like Ethereal to see if you can track down all necessary IPs needed to allow the website to work though again that will not work if the website starts resolving to different IPs not included in the filter list. TDImon fee from SysInternals can also give you an idea of IPs and ports/protocols the operating system accesses when connecting to a website and it does not need to be installed as an application.

Steve

"Greg O" <gregorme@xxxxxxxx> wrote in message
news:1153148032.486898.123020@xx

Hi,
I use IPSEC to control internet access on a domain. I block port 80 for browsers and ports 8080 and 3128 for most internet proxies. I also block all UDP since most internet games will run on UDP even with all

Re: Problem with IPSEC

TCP blocked. I want to allow individual web sites into the domain though. In IPSEC there is a setting for a particular domain, if you try it with say nytimes.com it looks up DNS and makes filters with each of the IP addresses listed there. IPSEC I think is supposed to work so that more specific filters (like allowing a web site) override more general filters (like blocking port 80. So allowing the IP addresses of nytimes.com should make it work, but it is still filtered by IPSEC. I know that's the problem because if I list the port 80 block the nytimes.com site starts working. Is this a bug in IPSEC? Also is there another way to do this without IPSEC, I see that network adaptor filters and RRAS filters don't seem to have the settings for this.