

Re: Setting up 2 domains with one way trust to dmz

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2006-11/msg00128.html>

- *From:* "Roger Abell [MVP]" <mvpNoSpam@xxxxxxx>
 - *Date:* Wed, 15 Nov 2006 08:54:15 -0700
-

What you refer to as the client ports are probably due to the RPC usage of dynamic port allocation. While it is possible to restrict RPC to use of a predefined port range you still need a range of ports and you also need to coordinate this so that it works system-wide and is sufficient.

There is *_always_* a trade-off between safety and convenience.

What I hear you saying is that it would be more convenient to administer if what is in the DMZ could share the security control context that exists inside the protected network. Well, sure. But, why does the DMZ exist? Is it not to make sure that the security control context used on the protected network is not exposed outside of that network?

You need to decide what is more important; protect the internal or administer conveniently as a single whole. Also, if use of accounts (other than for management of the DMZ resources) on the DMZ machines is part of the issue, as part of what you said does seem to indicate, then perhaps there is room to rethink what is being made available from the DMZ to internal users/clients.

Consider. I somehow penetrate one of your DMZ machines. Now, not wanting to be noticed I just plant something that gets a chance to examine the context it is executing within every time someone logs in to the machine. When I find that I have an admin or better a Domain Admin account (especially of the internal domain) a batch process gets started that will survive the accounts logoff. Now, since you have torn down the walls of the DMZ, as soon as I penetrated the DMZ system I discovered that there was a larger internal world just by examining things like trusts, info picked out from DNS, DMZ domain's group memberships, etc.. So, the process waits, hiding quietly, until it manages to get a long-lived process running as internal domain's Domain Admin member. At that point your internal world is mine. Being in the DMZ I likely could have no problem communicating back to my mother ship fleet, if nothing else over tcp 80. Also, since you have opened up access to the internal DCs I long ago pretty much mapped out what you have

Re: Setting up 2 domains with one way trust to dmz

inside (probably with any, even non-admin, internal account) and so can act quickly once that Domain Admin access is snagged. Of course, since all that is being done is being done by accounts that are expected to be in use on/from the DMZ it would take some fairly detailed monitoring of the traffic/logs to notice something is up, but then the processes on the DMZ machine trickle those events out over time (remember, I have time) so it is even harder for you IDS/IPS to trigger. etc. etc. etc.

Again. Why is it that you have a DMZ? What accesses from/by internal accounts are necessary? What are convenience alone? Of the necessary, why are they necessary and are there alternatives?

MS people, and others in the field, have often pointed out that there is a triangle between security/reliability, functionality/convenience, and low-cost such that one can fairly easily get only any two of the three. With what you are wanting, apparently secure and convenient deployment, then you would have to throw money at it to make it so, such as by use of intermediate screened networks IPS monitored, etc.

—
Roger

<fliben@xxxxxxxx> wrote in message
news:1163545106.502853.79970@xx

What I have now is a domain on the inside interface of a firewall and workgroups on the dmz. I am thinking for easier administration that making a second domain on the dmz with a one way trust would help cut down the administration of accounts and such.

To me it looks fairly straight forward for the domain creation. I would create a new domain like dmz.xxxxx.com for the dmz with inside domain being xxxxx.com.

Now the big question what ports need to be open for all this to work correctly on the firewall?

I found ms artical 179442 which lists a ton of ports that need to be opened to make this work.

I have no problem with the server ports its the client ports that I don't like. maybe I am reading it wrong or something. any help would be most welcome.

list of server ports

135/tcp RPC
389/TCP/UDP LDAP
636/TCP LDAP SSL
3268/TCP LDAP GC

Re: Setting up 2 domains with one way trust to dmz

3269/TCP LDAP GC SSL

53/TCP/UDP DNS

88/TCP/UDP Kerberos

445/TCP SMB

Client ports

1024–65535/TCP/UDP

or is this the same as I have configured already on the firewall of any
on the inside has access to dmz?