

Re: VPN-Zugriff auf SQL-Server

Source:

<http://www.tech-archive.net/Archive/German/Server/microsoft.public.de.german.windows.server.networking/2007-05>

- *From:* Horst Lange <ng005_nospam@xxxxxxx>
 - *Date:* Sat, 12 May 2007 16:10:51 +0200
-

PlankTom schrieb:

Hi an alle,
herzlichen Dank für eure Stellungnahmen. Vielleicht noch ein paar Erklärungen:

Hi Tom,

Du musst den SQL-Server nicht extra nach außen hin absichern – besser gar nicht nach aussen erreichbar sein!

Ich hab' doch aber Clients, die von anderen Standorten aus auf die Datenbank zugreifen müssen.

Ich denke, die kommen per VPN in das Netz?! Damit ist der Zugang zum SQL-Server wie auch die Sicherheit (durch VPN) vorhanden.

Zudem ist standardmäßig der parallele Zugang eines VPN-Clients ins Internet unterbunden. Der User müßte sich vom Netz trennen, um den SQL-Server zu erreichen.

Andernfalls könnte ein Angreifer vom Internet über den Client ins Hauptnetz gelangen. Dann könnte man sich den VPN-Tunnel gleich sparen.

Der SQL-Server horcht am Port 1433 auf Anfragen. Jeder mit diesem Netz verbundene Computer kann auf diese Verbindung zugreifen, also auch Deine über VPN angebotenen Clients. So läuft es bei uns in der Firma.

Das Netz wäre in diesem Fall der Rechner mit dem SQL-Server, der nur über VPN angesprochen werden kann. Wobei ich dann hier keinen Unterschied zwischen internen und externen Clients mache – der Rechner ist kein Mitglied der Domäne.

Bei uns am Standort läuft (noch) keine Domäne. Allerdings sind der Windows-Server (mit SQL) sowie einige Clients in eine Linux-Domäne eingebunden. Neben diesen verbinden sich Benutzer mit Notebook sowie unsere Bauleitungsbüros per VPN (Sonicwall-Gateway) in unser Netz. Alle können auf SQL zugreifen. Also sehe ich kein Problem. Nimm Dein Frontend, erstelle Deine ODBC und teste z.B. mit einem Notebook den Zugriff innerhalb des Netzes sowie über VPN. Ggf. wirst Du jedoch Deine Firewall (Gateway) anpassen müssen. Route eben alle 1433-Anfragen auf deinen SQL-Server.

Re: VPN-Zugriff auf SQL-Server

Interessant wird die Frage jedoch nach der Performance. Access einfach per ODBC an MS-SQL anbinden genügt selten, zumal wenn die Anwendung zunächst unter Access entwickelt wurde...

Die Anwendung wurde als Access-Projekt entwickelt, soviel wie möglich ist als Views oder Stored Procedures auf dem SQL-Server abgelegt.

Dann ist hier ja alles gemacht :-)

Das Ganze sollte zudem mit sDSL > 2000 (besser mehr) und an den Clients mit 16000/580 Kbit/s (wegen Upload) ausgestattet sein, damit in beide Richtungen genügend Daten gesendet werden können.

Zwischen den Standorten können wir auf einen sym. Backbone zurückgreifen (DFN), wobei die Anwendung auch von zu Hause aus (DSL-384, ja gibt's wirklich) reibungsfrei lief.

Ist die sDSL-384 nicht sehr Teuer? sDSL sind ja immer eine recht teure angelegenheit, weshalb wir bei den Außenstellen darauf verzichten. Immerhin kann dort i.d.R. mit ADSL 16.000 auf 580 kbit/s zugegriffen werden. Pro Standort also Summa Sumarum 50€ (T-Net + 1&1 3DSL) Selbst an dem schlechtesten Standort sind derzeit ca. 11.000 / 400.

Aber nochmals mein Hauptproblem. Bald ich diesen Server "Stand-alone" betreibe. Sollte ich dennoch, zur Authentifizierung der Clients, ein AD installieren oder genügt die lokale Benutzerverwaltung.

Wie Walter Steinsdorfer schrieb, kannst Du die SQL-Authentifizierung verwenden, damit bist Du von der restlichen Domäne/AD-/Userberechtigung unabhängig. Ich habe es so der Einfachheit halber gemacht. So ist im Access Frontend eine automatische DSN-Installation integriert, die den Zugang zum SQL-Server definiert. Der Server selbst könnte sich nun auch gegen alle andere Zugriffe verwehren und nur 1433-Zugriffe zulassen. Da die Datenbank weniger Kritisch ist als der Server selbst ist dies meiner Meinung nach sogar die bessere Sicherheit.

Als Stand-alone DB-Server muß der zugreifende Client lediglich die IP kennen und Zugriff auf das "Netz" (Adressraum) des SQL-Servers haben. Dennoch würde ich den SQL-Server im Netz lassen, weil dies die einfachste Methode ist, auf diesen zuzugreifen. Oder gibt es Benutzer im Internet, die ebenfalls darauf zugreifen sollen (Web-Shop)?

HTH

Horst

.