HOB GmbH & Co. KG
Schwadermühlstr. 3
90556 Cadolzburg

Tel: 09103 / 715-0
Fax: 09103 / 715-271
E-Mail: support@hob.de

WhitePaper

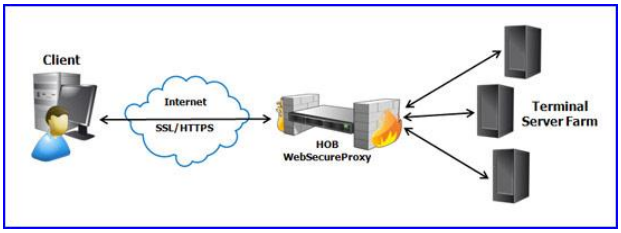
HOB WTS Computing

Sicherer Zugriff auf eine Windows Terminal Server Farm – auch über das Internet

Dezember 2010

HOB WTS Computing:
Sicherer Zugriff auf eine Windows Terminal Server Farm – auch über das Internet

Ein wichtiger Bestandteil des HOB RD VPN Konzeptes betrifft das Arbeiten mit Applikationen über das Microsoft RDP Protokoll. Dieses gilt in der aktuellen Version des MS Windows Server 2008 R2 als äußerst leistungsfähig. Die für die Nutzung über Internet unabdingbar wichtige Security wertet HOB mit erweiterter SSL Funktionalität auf. Eine Abschottung der bereitgestellten Windows Terminal Server geschieht über den HOB WebSecureProxy. Die Terminal Server sind dadurch nicht direkt aus dem Internet erreichbar.



Prinzipielle Funktionsweise des HOB WTS Computing

Die Abbildung zeigt die prinzipielle Anbindung von Anwendern über das Internet. Hierbei baut der Anwender mit einem beliebigen Web-Browser eine sichere Verbindung zum HOB WebSecureProxy über HTTPS auf. Dort muss er sich mit Benutzername und Passwort, optional auch mittels Tokens wie beispielsweise RSA SecurID, authentifizieren. Der HOB WebSecureProxy bietet entsprechende Schnittstellen via RADIUS Protokoll zu beliebigen Authentifizierungsservern an. Eine Zertifikats-basierte Authentifizierung mit SmartCard oder USB-Token ist ebenso möglich. Nach erfolgreicher Authentifizierung beginnt der Download des HOB Terminal Server Clients HOBLink JWT, welcher sogleich SSL geschützt die Verbindung zum HOB WebSecureProxy aufbaut. Dieser wählt gemäß des HOB Load Balancing den am besten geeigneten Terminal Server aus. Wichtiger Hinweis für Firewall-Administratoren: Die gesamte Kommunikation zwischen dem Client und der Firewall geschieht über einen einzigen Port, vorzugsweise Port 443.

Die Verwendung einer Serverfarm mit Windows Remote Desktop Services zur Bereitstellung von Applikationen bedingt einen leistungsfähigen Load Balancing Mechanismus. Die von Microsoft angebotene Variante beschränkt sich hierbei entweder auf ein nacheinander Auswählen der einzelnen Server (Round Robin) oder einer Verteilung über die Netzwerklast.

Für die optimale Nutzung einer Windows Terminal Serverfarm ist jedoch die Auswertung der CPU-Nutzung oder weiterer Parameter auf dem jeweiligen Server notwendig.

Der von HOB entwickelte Load Balancing Mechanismus misst hierfür bis zu 13 verschiedene Kenngrößen, die der Administrator unterschiedlich gewichten kann.

Die folgende Auswahl steht hierfür zur Verfügung:

- CPU-Auslastung
- Pagefile-Nutzung
- Swap activity (gesamt, lesen, schreiben)
- Speichernutzung
- aktive Sitzungen
- getrennte Sitzungen
- Netzwerkauslastung
- Anzahl Prozesse
- Anzahl Threads
- Festplattenauslastung
- Ein-/Ausgabeaktivität

Funktionsprinzip des HOB Load Balancing:

Vor dem Verbindungsaufbau sendet der HOB Client eine Anfrage an die verfügbaren Windows Terminal Server. Dies kann wahlweise über Broadcast oder eine definierte Liste geschehen. Jeder angesprochene Server gibt daraufhin seine momentane Auslastung zurück. Der anfragende Client kann so den am wenigsten ausgelasteten Server ansteuern. Dieser Mechanismus unterstützt ebenso „disconnected sessions“. Hierbei wird der Benutzer wieder mit dem selben Terminal Server, den er vor dem Verbindungsabbruch hatte, verbunden.

Im Falle des Zugriffs über das Internet – HOB WTS Computing – geschieht die Abfrage der Auslastung über den HOB WebSecureProxy. Dieser steuert als zentrale Instanz die gesamte Kommunikation zwischen den Anwender-Clients und der Windows Terminal Serverfarm. Vorzugsweise in der DMZ, zwischen den beiden Firewalls platziert, werden die firmeninternen Server wirkungsvoll vor dem direkten Zugriff aus dem Internet abgeschottet.

Das dargestellte Szenario bildet die Basisfunktionalität des HOB WTS Computing ab. Selbstverständlich lässt es sich um eine leistungsfähige Benutzerverwaltung mit LDAP bzw. MS

Active Directory erweitern. Auf der Clientseite sind keine besonderen Vorbereitungen nötig. Die Lösung funktioniert quasi „clientless“. Trotzdem bietet die HOB Lösung zahlreiche wichtige Zusatzfunktionalitäten wie z.B.:

- HOB True Windows – lässt Remote-Applikationen so aussehen als würden sie lokal ausgeführt werden
- Audio
- Virtual Channel Support
- SmartCard Redirection für SmartCard basierte Anmeldung am Windows Terminal Server
- Drucken unabhängig von der Drucker-Hardware (HOB EasyPrint)
- optionales Virenscannen der über Local Drive Mapping ausgetauschten Daten

Lesen Sie mehr zu den bereitgestellten Funktionalitäten in den Produktbeschreibungen zu HOBLink JWT und HOBLink JWT Enterprise Access (inkl. Benutzerverwaltung). Weitere Informationen über Funktionalitäten des HOB WebSecureProxy entnehmen Sie bitte den entsprechenden HOB Whitepapern.

01.03.07 SB
akt. 19.12.10