# Datencenter Umzug

Veröffentlicht: Dienstag, 13. Nov 2012

Neuaufbau einer weltweiten Intranet Anbindung über Site2Site (L2L) und Remote Access VPN

Projektbeschreibung:

Ein weltweit agierendes Unternehmen verlagert sein Datencenter aus einer Geschäftsstelle in ein externes Datencenter. Zu den Aufgaben des Datencenters gehören z.B. eine Microsoft Window Server Domain, der Anti-Spam-Mailservice des Unternehmens und ein FTP Server. Dabei ist es notwendig, den laufenden Betrieb wenig zu stören.

Aufgabenstellung:

Umzug eines Intranet VPN Sternpunktes aus der Geschäftsstelle in ein Firmen externes Datencenter. Anbindung weiterer Standorte an das Intranet. Aufrechterhaltung des laufenden Betriebes während der Umstellung.

Verwendete Produkte:
Firewalls/VPN
Cisco 2811 Integrated Service Router
Cisco PIX 501
Cisco ASA 5505
Cisco ASA 5520
Cisco ASA AnyConnect Remote Access VPN

Switches
Cisco Switch Catalyst
Cisco SMB Switch

Netzsicherheit:

Die Netzwerksicherheit hat in der heutigen Zeit ein hohes Maß an Priorität. Es muss sichergestellt werden, dass die Daten die über das Internet versendet werden, nicht missbraucht werden können. Zu diesem Zweck werden die Daten im VPN-Tunnel mittels einer Kryptografie Einheit in Verbindung mit einem PSK (Presharedkey) gesichert. Da es sich um einem L2L VPN Tunnel handelt, müssen beide Endpunkte bekannt und genaustens identifiziert werden können. Dies unterbindet eine so genannte „man in the middle“ Attacke.
Bei der Einwahl von Mitarbeitern via Remote VPN wird die Zugriffsberechtigung mittels eines

Radiusservers geregelt. Des Weiteren handelt es sich bei der AnyConnect Clientsoftware um eine SSL verschlüsselte Verbindung mittels eines „Self Sigend Certificate“.
Um ein Angriff von außen ab zu wehren ist außerdem die Konfiguration der Firewalls (ASA 55XX) notwendig.

Konzeptionierung:

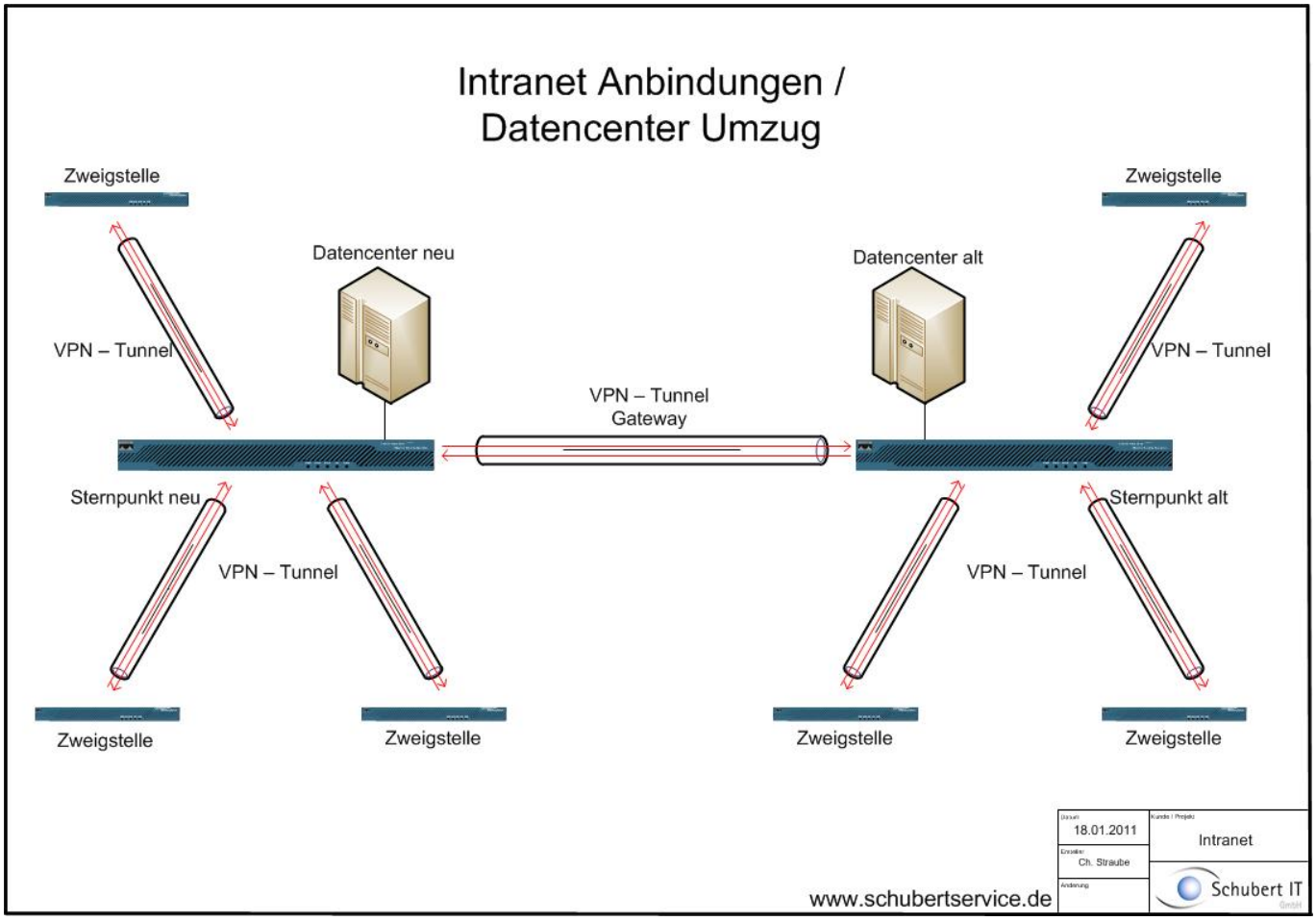
Um die Ausfallzeiten auf ein Minimum zu reduzieren, muss zu den bereits existierenden VPN Tunneln zum Sternpunkt ein weiterer Sternpunkt aufgebaut werden. Beide Sternpunkte agieren dann als Gateway der VPN-Tunnel auf dem neuen und/oder alten Sternpunkt.

Umsetzung:

Der Aufbau der Hardware wurde von dem Unternehmen selbst übernommen. Um die Konfiguration remote ausführen zu können, wurde die Hardware soweit vorkonfiguriert, das nur noch die Layer 1 Verbindung hergestellt werden musste (physikalischer Link). Alle weiteren Programmierungen wurden dann über eine SSH (Secure Shell) Verbindung ausgeführt.
In Schritt 1 wurde ein VPN-Tunnel zwischen dem alten und neuen Datencenter aufgebaut. Als dieser eingerichtet und getestet war, wurde die Weiterleitung der Sternpunkte programmiert.
In Schritt 2 wurden die VPN-Tunnel auf dem alten Sternpunkt erst abgebaut und dann zum neuen Sternpunkt wieder aufgebaut. Durch die Weiterleitung über die Sternpunkte ist eine Kommunikation der Standorte untereinander noch immer gegeben.
Bei diesem Schritt zeigten sich starke Probleme bei der zum Teil sehr alten Hardware. Diese wurden dann gegen nachfolge Produkte ausgetauscht.
In Schritt 3 wurde die Weiterleitung der Sternpunkte wieder abgebaut, so dass der alte Sternpunkt nur noch als normaler Standort fungiert.

Abschluss:

Nach ausführlichen Tests sowie der Behebung vereinzelter Fehler wurde dieses Projekt erfolgreich abgeschlossen.
Ich danke dem beteiligten Unternehmen für die sehr gute Zusammenarbeit.


Intranet Anbindungen /
Datencenter Umzug
Zweigstelle
Zweigstelle
Datencenter neu
Datencenter alt
VPN – Tunnel
VPN – Tunnel
VPN – Tunnel
Gateway
Sternpunkt neu
Sternpunkt alt
VPN – Tunnel
VPN – Tunnel
Zweigstelle
Zweigstelle
Zweigstelle
Zweigstelle
18.01.2011
Ch. Straube
Intranet
www.schubertservice.de
Schubert IT

[Zurück]