EDV Partner

Security Appliance Clusterlösung mit Clavister

AUF EINEN BLICK

Kunde
N-ERGIE Aktiengesellschaft

Standort
Nürnberg

Branche
Energieversorgung

Mitarbeiter
2.800

Internetadresse
www.n-ergie.de

HERRAUSFORDERUNG

Die Abteilung IT-Netzbetrieb hat die Verpflichtung den reibungslosen und ausfallsicheren IT-Netzwerkbetrieb zwischen den zentralen Rechenzentren und den verteilten Aussenstandorten sowie den verschiedenen Tochtergesellschaften des Konzerns sicherzustellen. Darüber hinaus muss der gesicherte Zugang ins Internet und auch der gesicherte Zugriff aus dem Internet auf Server im internen Netz gesichert bereitgestellt sein.

TECHNISCHE SITUATION

Die Außenstellen bzw. Standorte der Tochtergesellschaften sind zum Teil mit sehr hohen WAN-Bandbreiten(>100Mbit) verbunden. Dadurch muss bei der IP-Sicherheitslösung/Firewall-Lösung sehr hohen Wert auf Performance gelegt werden. Darüber hinaus darf bei zentralen ITLösungen kein "Single Point of failure" entstehen. Die Möglichkeit einer zentralen Administration und Monitoring müssen bei allen im Konzern eingesetzten Lösungen vorhanden sein.

LÖSUNG

Die EDV-Partner GmbH kann mit der Clavister Security Appliance Clusterlösung der Serie 4230 und 3110/50 ein ideales Produkt für die Aufgabenstellung bieten. Zunächst wurde der erste Cluster an einer nicht so kritischen WAN-Verbindung in Betrieb genommen um die ersten Erfahrungen mit dem Clavistersystem zu sammeln. Die Implementation wurden im Rahmen eines Workshop vorgenommen bei dem alle nachher im laufenden Betrieb für dieses System verantwortlichen Mitarbeiter beteiligt waren. Somit haben sich kostenintensive Schulungen weitgehenst erübrigt. Erste bestechende Erfahrungsergebnisse waren, dass im Fail-over Fall des Clavister-Clusters keinerlei Verzögerungen bzw. Ausfälle im IP-Datenverlust festzustellen waren. Nach mehreren Monaten des Betriebs des "Pilot-Clusters" wurden weitere Cluster in Betrieb genommen, dabei stellte sich zunächst ein Problem heraus: Es waren die jeweils angeschlossenen Netzwerkswitche nicht in der Lage auf Layer Ebene den Portwechsel im Fail-over Fall schnell genug zu registrieren. Als Lösung musste das Spanning-Tree-Protokoll auf den beteiligten Switch-Ports ausgeschaltet werden.

NUTZEN

Als äußerst positiv hat der Kunde herausgestrichen:

- zügige und einfache Konfiguration möglich
- auch bei insgesamt 8 Appliance Firewall (4 Cluster) eine einfach übersichtliche zentrale Administration möglich.
- Überwachungsmöglichkeit durch das unternehmensweite Netzwerküberwachungstool.
- Übersichtliches und effektives Fehleranalyse-Tool in der mitgelieferten Management-Software.
- Überaus gute Performance der Cluster-Appliances.
- Im Fail-Over Fall keine Einbußen im TCP/IP Datenfluss.