

## Sonderdruck für OSYON

### Ascenlink Load-Balancing-Router im Test

# Bandbreiten gebündelt und gesichert

Ascenvision liefert mit Ascenlink eine Appliance, die als Load Balancer für Netzwerkstrecken fungiert und alle verfügbaren WAN-Leitungen zu einem gemeinsamen Verbund koppelt. Die notwendigen Leitungskapazitäten für Verbindungen teilt das Gerät dann jeweils dynamisch zu.

Der Load-Balancing-Router Ascenlink von Ascenvision arbeitet mit einem Pool an verfügbaren WAN-Verbindungen, den der integrierte Load Balancer steuert und aus dem die aktiven Datenverbindungen wie beispielsweise VPN-Tunnels mit der notwendigen Leitungskapazität versorgt werden. Die Übertragung der Daten erfolgt dabei immer unter Ausnutzung aller Verbindungen in Abhängigkeit ihrer relativen Last. Das Gerät realisiert die Hochverfügbarkeit dieser Strecken über die Lastverteilung mit Failover-Funktionen. Um welche Art von WAN es sich dabei handelt, spielt für das Gerät keine Rolle. Unterstützt werden die DSL-Varianten ADSL, SDSL so-

wie unter Einbezug einer Zusatzhardware ISDN und UMTS.

Der Hersteller liefert die Appliance in sechs Ausbaustufen bis hin zur AL3820 mit 50 WAN-Anschlüssen. Für den LANline-Test stand die AL430 mit fünf frei belegbaren Netzwerkschnittstellen zur Verfügung. Diese Box kostet beim Distributor Osyon rund 3500 Euro. Zum Lieferumfang gehören neben dem Gerät im 1-HE-19-Zoll-Einschub alle notwendigen Anschlusskabel, Befestigungsmaterial und das Handbuch auf CD. An der Frontseite des Geräts befindet sich eine PowerLED, die fünf Netzwerkanschlüsse sowie zwei serielle Ports, die mit HA (High

Availability) und Console bezeichnet sind. Über den HA-Anschluss sind zwei Boxen im Failover-Active-/Passive-Verfahren zu verbinden. Die Verwaltung der Appliance erfolgt über eine https-Verbindung. Dabei hat der Administrator alle Berechtigungen, zudem können bis zu fünf Monitorbenutzer die Aktivitäten zumindest überwachen. Die Verwaltungsoberfläche verzichtet auf jeglichen grafischen Aufwand und arbeitet mit einfachen Menüs und Tabellen. Unterteilt ist die Verwaltung in die Bereiche System, Services, Statistics, Log und Language, wobei Englisch die derzeit einzig mögliche Auswahl darstellt. Auch das sehr detaillierte PDF-Handbuch ist ebenso wie alle Dialoge und Menüs in Englisch gehalten.

Unter „System“ finden sich allgemeine Systemeinstellungen zum Netzwerk, den Routen, Datum/Zeit oder Diagnose, ferner Funktionen zum Sichern der Konfiguration, dem Ändern von Kennwörtern oder für ein Reboot der Appliance. Einen Shutdown jedoch kennt sie nicht. Darüber hinaus finden sich hier Funktionen zur Bildung von IP- oder Servicegruppen. Eine IP-Gruppe stellt dabei eine frei zu definierende Menge an IP-Adressen dar. Dieser können eigene Berechtigungen oder auch Leitungen zugewiesen werden. Analog verhält es sich mit den Servicegruppen, wobei unter „Service“ die Protokolle und ihre Ports verstanden

werden. Eine Servicegruppe kann beispielsweise für den Dienst FTP-Upload oder für den SAP-Zugang eingerichtet werden. Eine dritte Basiseinstellung betrifft die Zeiten. Aus der Kombination der IP-Gruppe, Servicegruppen, Zeiten und Leitungen kann der Administrator festlegen, dass in den Geschäftszeiten SAP-Anwender mit bestimmten IP-Bereich Vorrang gegenüber der Servicegruppe Internetzugang erhalten. Nachts kann dann ein notwendiger FTP-Upload Vorrang erhalten.

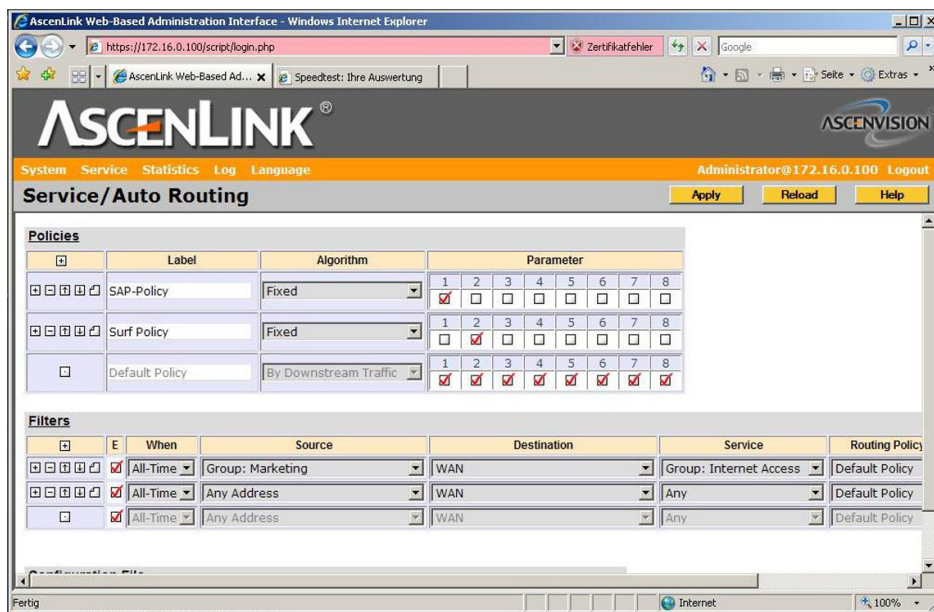
Für den Test wurden mehrere Service- und IP-Gruppen sowie unterschiedliche Zeiten definiert. Alle vorgenommenen Konfigurationsänderungen muss der Anwender durch den Apply-Knopf rechts oben im Menüfenster explizit bestätigen, andernfalls sind sie beim Wechsel der Maske verloren. Hier wäre ein entsprechender Hinweis angebracht. Damit sind die Änderungen allerdings noch nicht aktiv. Der Anwender muss hierzu die überarbeiteten Einstellungen durch eine Checkbox „Enabled“ explizit aktiv schalten. Andernfalls sind die Änderungen durch „Apply“ nur im Konfigurationssatz gesichert. Dies ermöglicht die temporäre Deaktivierung von Einstellungen, ohne sie gleich zu löschen. Bei umfangreichen Konfigurationen wird der Administrator dies zu schätzen wissen.

Die Appliance bietet eine Firewall, eine Adressumsetzung (NAT), einen Router und das Bandbreitenmanagement. Die integrierte Firewall erlaubt die Analyse des Datenverkehrs anhand einer vorbereiteten Sammlung unterschiedlicher Protokolle. Für das Routing kann der Anwender über Auto-Routing-Einstellungen festlegen, welche Verbindungen auf welcher Leitung geschaltet werden. In der Routing Policy bestimmt er, welche Dienste, welche Applikation, welche Service- oder Benutzergruppe zu welchen Zeiten über welche Leitungen kommunizieren dürfen. Da Kommunikationsstrecken ausfallen können, wird jeweils eine Failover-Bedin-

gung eingerichtet. Die Einstellungen für die Route lassen sich fest zuweisen, erlauben aber auch eine weitaus flexiblere Lastverteilung. So ist neben der festen Zuordnung nach Round-Robin unter anderem auch eine Zuordnung nach der Menge des Up- oder Downstream-Datenverkehrs oder nach dem Gesamtverkehr möglich. Um diese Zuordnung der Dienste zu den

weist keine Besonderheiten auf. Die Verbindung zur Konsole erfolgte im Test durch das Windows-Tool Hyperterminal.

Unter dem Punkt „Virtual Server“ werden die für das Inhouse Server Load Balancing notwendigen Server eingetragen. Die Einträge des Multi-Homing sind notwendig, wenn ein Server über mehrere redundante WAN-Leitungen verfügbar gemacht wer-



**Durch Routing Policies und Filter erfolgt die Zuweisung des Datenverkehrs oder der Internetverbindungen an die Netzwerkanäle**

Leitungen noch weiter zu spezifizieren, werden die Einstellungen zum Bandbreitenmanagement herangezogen. Das System unterscheidet dabei nach Inbound, also ankommendem, und Outbound Traffic, nach außen gerichtetem Datenverkehr. Durch das Bandbreitenmanagement erfolgt die Priorisierung verschiedener Traffic- und Nutzungsarten untereinander. Einzustellen ist ferner eine Begrenzung der Verbindungen (Connection Limit) für bestimmte Zielsever. Damit wird verhindert, dass einzelne Nutzer (etwa im Internet-Cafe) die zur Verfügung stehenden Anschlüsse übermäßig belasten und zum Beispiel für Spamming missbrauchen. Die im Test definierten Routen für die Service- und IP-Gruppen funktionierten einwandfrei. Die Ablauffolge ist schlüssig und

den soll. Fällt eine Leitung aus, lenkt Ascenlink den gesamten Verkehr auf die Failover-Leitung um. Ascenlink bündelt Leitungen zu ausfallsicheren WAN-Strecken. Die Arbeit mit der Appliance erwies sich als logisch, schlüssig und angenehm in der Bedienung.

Johann Baumeister/dp

**OSYON GmbH**  
 Peter Acker  
 Tel.: +49 (0) 30 310135 0  
 Fax: +49 (0) 30 310135 55  
 Leibnizstraße 33  
 10625 Berlin  
 www.osyon.com