



HOB Networking informiert:

Modul: "ASA Adaptive Security Appliance"

- Durchgehende Netzwerk-Sicherheit
Abwehr von Softwareangriffen
- E-Mail- und Web-Sicherheit
Spam und Virenschutz
- Sicherheitsmanagement
Vereinfachtes Konfigurationsmanagement
- Sichere Zugriffskontrolle
Authentisierung & Autorisierung
- Sichere Zugriffskontrolle (NAC)
- Sichere Mobilität

Kurzbeschreibung / Einsatzbereiche:

Ein Unternehmen sichert seine gesamte IT-Infrastruktur und Kommunikation mit einem eigenen „Sicherheits Regelwerk“ (Security Policy) ab. Alle Anwender können das Firmennetz (z.B. Intranet) erst nach umfangreichen Authentisierungsmechanismen nutzen. Kommunikation via Internet/Intranet sollte Medium unabhängig verschlüsselt erfolgen. Dies gilt sowohl für Daten als auch für Sprache mit allen anhängenden Anwendungen.

Stetig neue Gefahren (Malware) aus dem Internet bedrohen ganze Netze und richten bei Unternehmen einen enormen Schaden an. Hinzu kommt, dass „Unified Communication“ offene Netze nutzen und entsprechend gegen Angriffe geschützt werden müssen. Einzelne Schutzmaßnahmen parallel aufzubauen ist



aufwändig, ineffektiv und zu teuer.

Zeit, neue Strukturen mit „Selbsteilungsmechanismen“ aufzubauen und unter ein gemeinsames „Sicherheitsdach“ zu bringen.

Partnerprodukte / Vorgehensweise

Mit Ciscos „ASA Adaptive Security Appliance“ geht HOB den Weg die immer mehr in sich verzahnten Prozesse und Applikationen abzusichern. Das beginnt mit der Infrastruktur und setzt sich fort mit verschlüsselten Verbindungen einzelner Filialen / Mitarbeiter, Unified Communication, wie z.B. Sprache, ERP Anwendungen bis hin zu Wide Area File Services. Mit Ciscos breiter Produktpalette ist ein intelligenter Aufbau von „Selbst

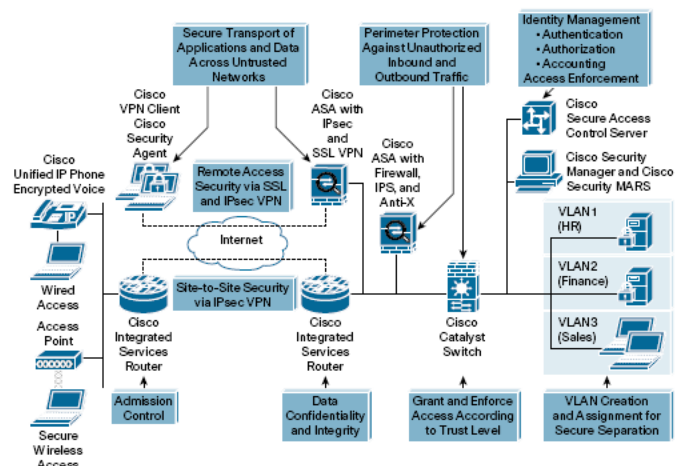
heilenden Netzen“ möglich. Eine Integration von neuen Technologien ist stets gegeben.

Know-how

HOB Networking plant und realisiert Projekte bei Kunden aus Industrie und Einzelhandel mit zahlreichen Filialen - mit Switching, Routing, VPN-Anbindungen und der Erstellung von ganzheitlichen Security Lösungen. Verbunden mit einem 24x7x365 Monitoring der gesamten Infrastruktur.

Szenarien / Projekte

Der Aufbau erfordert umfangreiche Planung. Erst ein vollständig erschlossenes Szenario schafft eine größtmögliche Sicherheit. Es lohnt sich eine partielle Migration,



die mit jedem Projektabschnitt die eingeleiteten Security-Maßnahmen weiter umsetzt und die Kommunikation sicherer macht.

Lösungsnaher Module

- ✓ Branch Office
- ✓ Wireless
- ✓ Switching
- ✓ WAN / Routing
- ✓ Unified Communications
- ✓ Management
- ✓ Firewalls / Security Appliances