

„Die Produkte von F5  
bedeuten für uns wenig  
Installationsaufwand und so gut  
wie keine Wartung“

Roger Heid, IT-Engineer  
der Business School

**KV ZÜRICH  
BUSINESS SCHOOL**

**KV Zürich Business School setzt auf die Technologie von F5**



## **Gemischte Clientlandschaft gab den Ausschlag**

Branche:  
Education

Herausforderungen:  
Gemischte Clientlandschaft

Lösung:  
FirePass

Vorteil:  
- Plattform-unabhängige Unterstützung  
- Nahtlose Integration in anwenderspezifische Lösungen durch API  
(Application Programming Interface)

Die Dozenten und Fachkräfte der KV Zürich Business School können ohne mulmiges Gefühl auf die Unternehmensdaten und zentralen Informationspools der KV Zürich Business School online zugreifen. Denn die Schweizer Schule hat sich bei der Planung ihres Virtual Private Networks (VPN) ganz auf F5 und seine Firepass-Technologie verlassen. Gekauft hat die Schule das System bei Matracom, einem Schweizer Distributor, die Implementierung haben Mitarbeiter der SITC AG übernommen, die auch eine Access-Lösung für Lehrkräfte und interne Mitarbeiter in die IT-Strukturen des Lehrinstituts integrierten.

Über 500 Dozenten und Verwaltungsmitarbeiter der KV Zürich Business School können so schnell auf Intranet und Internet zugreifen, ohne sich vor Hackern, Viren oder Würmern fürchten zu müssen. Die Lehrer haben auch von zu Hause aus Zugriff auf ihr persönliches Laufwerk auf dem Schulserver. Egal von welchem Ort, das interne Unternehmenslaufwerk kann immer erreicht werden. Außerdem auf zwei für die Dozenten wichtige Webdrehschreiben: zum einen das Intranet der KV Zürich Business School und zum anderen auf das schweizerische Bibliothekssystem.

„Wir haben uns für F5 deshalb entschieden, weil wir eine gemischte Client-Landschaft haben“, sagt Roger Heid, IT-Engineer der Business School. Denn F5 stellt mit dem FirePass Controller eine SSL VPN Lösung zur Verfügung, die eine vollständige plattform-unabhängige Unterstützung bietet. Mit der Erweiterung auf Macintosh- und Linux-Clients und den zusätzlichen Sicherheitsfunktionen für Clients beim Zugriff über das Internet auf das Firmennetz und Anwendungen, liefert der FirePass Controller die branchenweit stärkste Lösung.

Als einziger Hersteller bietet der Marktführer für Application Security und Traffic Management Technologien die offene Schnittstelle (API, Application Programming Interface) inklusive SDK (Software Developer's Kit). Dieses ermöglicht die nahtlose Integration in anwenderspezifische Lösungen wie z. B. Billing oder die Integration in fremde Security-Management-Systeme, wie es jetzt bei der KV Zürich Business School mit Erfolg praktiziert wurde.

Das offene iControl API und das SDK des FirePass Controllers ermöglichen durch die sichere Kommunikation zwischen zwei Systemen oder zwischen Anwendungen einen automatisierten, sicheren Zugang für Rich Windows Client Applications. Das API verbessert die Benutzerfreundlichkeit durch den automatischen Start eines sicheren Netzwerkzugangs aus der Anwendung selbst heraus. DevCentral von F5 (<http://devcentral.f5.com>) bietet den kostenfreien Support für Entwicklung, Sample Codes, Dokumentation und Zusammenarbeit. Dieser Support schont die Personal-Ressourcen der KV Zürich Business School, die denkbar knapp sind.

„Die Produkte von F5 bedeuten für uns wenig Installationsaufwand und so gut wie keine Wartung“, sagt Roger Heid. Damit fällt auch der externe Support weg. Das schont die schuleigenen Ressourcen, denn die Schule hat keine personellen Ressourcen frei, um solche Arbeiten abzuwickeln, bemerkt Heid weiter. Letztendlich konnten mit diesem Projekt auch die betriebsinternen Kosten gesenkt werden.

Integriert wurde die Firepass-Technologie auf dem Active Directory Windows Server 2003 der Business School. „Die Benutzer werden nur auf diesen Server geführt“, beschreibt Heid das Projekt. Eine Registrierung bei F5 fällt weg.



Jeder User logt sich extern ein, wie in der Schule – und das sicher. Denn mit den neuen Sicherheitsfunktionen werden die Unternehmensapplikationen und -daten noch besser geschützt. Die Sicherheitsfeatures von FirePass Controller für Internetanwendungen blockieren Angriffe über die Anwendungsebene, wie z.B. Cross-Site Scripting, Buffer Overflow und SQL Injection, durch die Überprüfung des gesamten Internetverkehrs über die FirePass.

FirePass Controller, den nun auch die eidgenössischen Pädagogen nutzen, ist auch in der Lage, Uploads aus dem Internet und aus Dateien zu scannen, indem es entweder einen integrierten oder einen externen Scanner via ICAP (Internet Content Adaptation Protocol) API benutzt. Infizierte Dateien werden am FirePass Gateway blockiert und können weder auf die Mailserver noch auf die Fileserver im Netzwerk gelangen. Für eine sorgfältige Überprüfung der Integrität der Clients kann der FirePass Controller überprüfen, ob ein aktuelles McAfee Antivirus-Programm oder andere nutzerdefinierte Sicherheitsfeatures installiert und aktuell sind, bevor ihm eine vollständige Netzwerkverbindung gewährt wird.

Kann ein Nutzer diese nicht vorweisen, kann eingeschränkter Zugriff auf ein besonderes Quarantäne-Netzwerksegment ermöglicht werden. Hier kann der Nutzer die Antivirus-Software oder Virendateien aktualisieren, um die Sicherheitsanforderungen des Unternehmens zu erfüllen.

Der FirePass Controller beinhaltet eine neue Sicherheitsoption „Protected Workspace“, mit deren Hilfe Nutzer auf geschützte Arbeitsbereiche im Client-System (Windows XP) wechseln können. Diese werden für jede Session neu angelegt. Befinden sie sich im gesicherten Arbeitsplatzmodus, können die Nutzer keine Dateien außerhalb des gesicherten

Arbeitsbereiches auf dem Client-PC speichern. Die Ordner mit den Temporary Files werden mitsamt ihrem Inhalt nach jeder Session automatisch gelöscht. Das „Secure Virtual Keyboard“ des FirePass Controllers bietet zudem weitere verbesserte Sicherheitsfeatures beim Eingeben von Passwörtern. So werden zur Eingabe der Passwörter Mausclicks auf eine virtuelle Tastatur verlangt, welche die Aufzeichnung und den Diebstahl der Passwörter über „Spyware“-Software wirksam verhindert.

Vier Monate hat die KV Zürich Business School von den ersten Planungen bis zur Inbetriebnahme gebraucht. „Wir hatten in dieser Zeit eine relativ lange Testphase“, blickt Heid zurück. Kleine Schwierigkeiten gab es, denn die F5-Technologie akzeptierte nicht ohne weiteres den schweizerischen Zeichensatz. Dieses Problem ist jedoch inzwischen behoben.

Die Lehrkräfte nutzen die virtuellen Möglichkeiten zunehmend. Waren es anfangs 15 bis 20 Benutzer, sind es jetzt bereits 80 bis 160 – Tendenz steigend. Als nächstes sollen die Lehrkräfte direkt auf den Host eingebunden werden. Denn das Schulsystem wird auf einem IBM AS/400 betrieben. Schließlich soll das Notenmanagement vereinfacht werden und den Lehrern über einen direkten Zugriff auf das Großsystem Mehrarbeit erspart werden. Erste Tests sind für das kommende Frühjahr geplant. Bleibt es bei der Planung, können die Fachlehrer F5 direkt und ohne Umwege die Note 1 geben.

---

**F5 Networks GmbH**

Einsteinring 35  
85609 München-Dornach  
Germany  
Tel: +49 (0) 89 94383 0  
Fax +49 (0) 89 94383 111  
www.f5networks.de

**F5 Networks, Inc.  
Corporate Headquarters**

401 Elliot Avenue West  
Seattle, WA 98119  
(206) 272-5555 Voice  
(888) 88BIGIP Toll-Free  
(206) 272-5556 Fax  
www.f5.com  
info@f5.com

**F5 Networks  
Asia-Pacific**

+65-6533-6103 Voice  
+65-6533-6103 Fax  
info.asia@f5.com

**F5 Networks, Ltd  
Europe/Middle-East/Africa**

+44 (0)1932 582 000 Voice  
+44 (0)1932 582 001 Fax  
emeainfo@f5.com

**F5 Networks  
Japan K.K.**

+81-3-51 14-3200 Voice  
+81-3-51 14-3201 Fax  
info@f5networks.co.jp