



## [ case study: isa 2004 ]

### Migration Firewall auf ISA 2004 bei der VETSUISSE- Fakultät der Universität Bern

#### Ausgangslage

Die Veterinärmedizin (Tierheilkunde) befasst sich mit der Erforschung, Diagnostik, Verhütung und Behandlung von Krankheiten der Tiere. Zu ihrem Gebiet gehören aber auch der Schutz des Menschen vor Krankheiten, die von Tieren übertragbar sind, die Kontrolle der vom Tier stammenden Lebensmittel sowie Probleme des Tierschutzes.

Die wichtigste Aufgabe der VETSUISSE-Fakultät der Universität Bern ist die Ausbildung von Studierenden zu Tierärztinnen und Tierärzten. Dabei steht die klinische Ausbildung am kranken Tier im Zentrum, was ohne gut funktionierende moderne Kliniken nicht denkbar ist. Somit erfüllen die Klinik für Nutztiere und Pferde und die Klinik für kleine Haustiere mit ihren diversen spezialisierten Abteilungen eine dreifache Aufgabe: Die Patientenbetreuung, die Ausbildung von Studierenden und Spezialisten sowie die Forschung auf dem Gebiet der Tierkrankheiten.

So vielfältig wie die Arbeitsgebiete der Fakultät sind, ist auch die IT-Infrastruktur der VETSUISSE-Fakultät. Für die jeweiligen Laborversuche, Unterrichtsräume und Büroarbeitsplätze sind die entsprechenden Rechner vorhanden. Rund 500 Arbeitsplätze sowie 10 Server inklusive SAN, unterstützen die Studenten, Fachmediziner und Mitarbeiter in ihrer anspruchsvollen Aufgabe. Unix-, Windows- und Macintosh-Server, Macintosh- und Windows-Clients sowie IBM Systeme von Partnerfirmen zeigen in etwa den Rahmen, in welchem sich in der VETSUISSE-Fakultät die IT-Projekte bewegen.

Die VETSUISSE-Fakultät ist bezüglich Vernetzung ein Teil der Universität Bern. E-Mail-Gateways, Internetverbindungen, Router, IP Adressen, Switches, Verkabelung etc. werden von den Informatikdiensten der Universität Bern, für die VETSUISSE-Fakultät auf Anforderung bereitgestellt und konfiguriert.

Die beschriebene IT-Umgebung der VETSUISSE-Fakultät benötigt angemessenen Schutz, wenn es um die Vernetzung geht. Aus diesem Grund ist das gesamte Netz mittels einer internen Firewall vom Netz der Universität Bern getrennt. Nur über dieses Gerät ist eine Verbindung aus der Veterinärmedizinischen Fakultät heraus grundsätzlich möglich. Über diverse Regeln wird daraufhin genau bestimmt, wie die Datenübertragung geschehen darf.

Zusätzlich sind weitere Firewalls am „Ausgang“ des Uni Netzes angeordnet, welche den gesamten Campus mit dem Internet verbinden und über die schliesslich auch der Zugriff aus der VETSUISSE-Fakultät auf das Web erfolgt.



## Lösung

### Projektauftrag für die FITIT Informatik GmbH

Der Auftrag für den „Neubau“ der VETSUISSE-Fakultät Firewall war integriert in ein grösseres Gesamtprojekt, worin die FITIT Informatik GmbH ein Upgrade der ganzen Infrastruktur auf Windows Server 2003 sowie die Migration von Exchange 5.5 auf Exchange 2003 durchführen konnte. Auch die Bereitstellung eines SAN (Storage Area Network) wurde durch die FITIT Informatik GmbH vorgenommen.

Weil die IT-Gruppe der VETSUISSE-Fakultät die Verantwortung über ihre Firewall neu selber übernehmen durfte, musste ein Produkt mit übersichtlicher Menüführung und klaren Strukturen gefunden werden. Geringere Lizenzkosten sowie ersatzbedürftige Hardware waren weitere Gründe für einen Wechsel auf eine andere Firewall.

Im Anforderungsprofil für die neue VETSUISSE-Fakultät Firewall sind die wesentlichen Punkte ihrer Aufgabe aufgelistet:

- Sicherer Anschluss von rund 500 Clients ans Netz und Internet der Universität Bern.
- Sicherer Zugriff auf Outlook Web Access (OWA) und Exchange E-Mail Server.
- Zahlreiche Punkt zu Punkt Verbindungen für spezielle Unix Services.
- Einbindung in die Netzwerküberwachung der Universität Bern mittels SNMP (Simple Network Management Protocol).
- Bereitstellen einer DMZ (Demilitarized Zone) für einen Unix Web Server sowie für einen Cisco VPN Concentrator (Virtual Private Network).
- VPN Verbindungen über die neue Firewall zu einem VPN Concentrator in der DMZ für Remote-Support und Partnerbetriebe.

Der im August 2004 von Microsoft freigegebene ISA Server 2004, erfüllt diese Anforderungen und wurde deshalb von der FITIT Informatik GmbH für das Projekt in der VETSUISSE-Fakultät vorgeschlagen.

#### 1. Flexibilität von ISA 2004

Die beschriebene vielfältige Umgebung der VETSUISSE-Fakultät erfordert ein Firewall Produkt, welches diesen verschiedenen Anforderungen genügen kann. Ursprünglich war vorgesehen, mit ISA Server 2000 (Internet Security and Acceleration Server) die Aufgabe zu lösen. Obwohl auch diese Firewall bereits umfangreiche Möglichkeiten bereitstellt, konnte damit in einzelnen Bereichen nicht die gewünschte Flexibilität erreicht werden. Erst das Nachfolgeprodukt ISA Server 2004 weist alle für die VETSUISSE-Fakultät nötigen Features auf. Die wesentlichen Punkte, welche in der VETSUISSE-Fakultät massgebend waren, sind in der folgenden Liste zusammengestellt:



## NAT und Routing

Mit ISA 2004 lässt sich zwischen den direkt angeschlossenen Netzen frei entscheiden, ob die Beziehung „normal geroutet“ oder per NAT (Network Address Translation) vorhanden sein soll. In der VETSUISSE-Fakultät muss beides gleichzeitig möglich sein, damit die nötigen Verbindungen zustande kommen können.

## OWA (Outlook Web Access)

ISA 2004 kann Outlook Web Access, das als Erweiterung auf dem Exchange Server der VETSUISSE-Fakultät installiert ist, gegen aussen „komplett abschirmen“. Die Web Verbindungen von Clients aus dem Internet werden dabei auf ISA terminiert. Der ISA Server holt sich dann gemäss den Eingaben des Clients die entsprechenden Daten aus Exchange heraus und leitet sie für die Anzeige im Web-Browser weiter (Reverse Proxy).

## Übersichtliche Bedienung

ISA 2004 weist ein Administrator Interface auf, womit eine funktionierende Grundkonfiguration mit wenigen Schritten erreichbar ist. Mittels Templates lässt sich eine „Three-Leg“ Firewall, samt DMZ, relativ einfach durch Auswählen der entsprechenden Grafik einrichten. Vorteil davon ist, dass sich die Konfiguration von ISA für die VETSUISSE-Fakultät in relativ kurzer Zeit erstellen liess.

## Application Layer Firewall

Die von der VETSUISSE-Fakultät gestellten Sicherheitsanforderungen erfüllt ISA 2004 indem zusätzlich zu den Filtern auf Niveau IP, zusätzliche „Application Filters“ vorhanden sind. Der Datenstrom wird also für die gängigen Protokolle bis und mit OSI-Layer 7 durch die ISA Firewall kontrolliert und entsprechend abgesichert.

## Integration in Windows Active Directory

Die Integration mit den weiteren Windows Servern in der VETSUISSE-Fakultät sowie mit Active Directory, ist bei ISA 2004 von Haus her gegeben. Auch das Zusammenspiel mit Exchange 2003 liess sich sauber realisieren. Für die VETSUISSE-Fakultät resultiert daraus der Vorteil, dass die Integration der Umgebung mit einheitlichen Interfaces, integriert in die vorhandene IT-Umgebung, erfolgen kann.

## Funktionalität in heterogenem Umfeld

Im ISA Server 2004 ist eine grosse Zahl von Protokollen bereits vordefiniert, so dass auch aussergewöhnliche Verbindungen zwischen einzelnen Unix Maschinen aufgesetzt werden können. Einzelne noch nicht vorhandene Protokolle liessen sich „von Hand“ einrichten, so dass nun alle Verbindungsanforderungen der VETSUISSE-Fakultät erfüllbar sind.

## 2. Realisierung

Die Ablösung der bestehenden VETSUISSE-Fakultät Firewall stellte besondere Anforderungen an das Projektteam, da die Umstellung den laufenden Betrieb nicht stören durfte. Die Ablösung der bestehenden Firewall wurde deshalb in zwei Schritten vorgenommen:



Zuerst galt es, nach der Migration von Exchange 5.5 auf 2003 das OWA- und SMTP Publishing über die neue ISA Firewall zu führen. Der gesamte E-Mail-Verkehr der VETSU-ISSE-Fakultät war also davon betroffen. Ebenfalls in dieser ersten Phase wurde eine DMZ auf ISA 2004 eingerichtet und ein VPN Concentrator darin platziert. In diesem Zwischenstadium funktionierten also die alte und neue Firewall parallel zueinander mit entsprechender Konfiguration der umgebenden Router.

Im zweiten Schritt wurde dann der gesamte „restliche“ Datenverkehr sowie die Web-Server in der DMZ zur neuen ISA Firewall migriert. Besonderes Augenmerk erforderten dabei die speziellen Protokolle zwischen einzelnen Unix-Servern, die über nicht standardmässig vergebene Ports zu führen waren.

In Abbildung 1 ist die prinzipielle Anordnung von ISA 2004, wie sie in der VETSUISSE-Fakultät in ähnlicher Weise vorhanden ist, dargestellt:

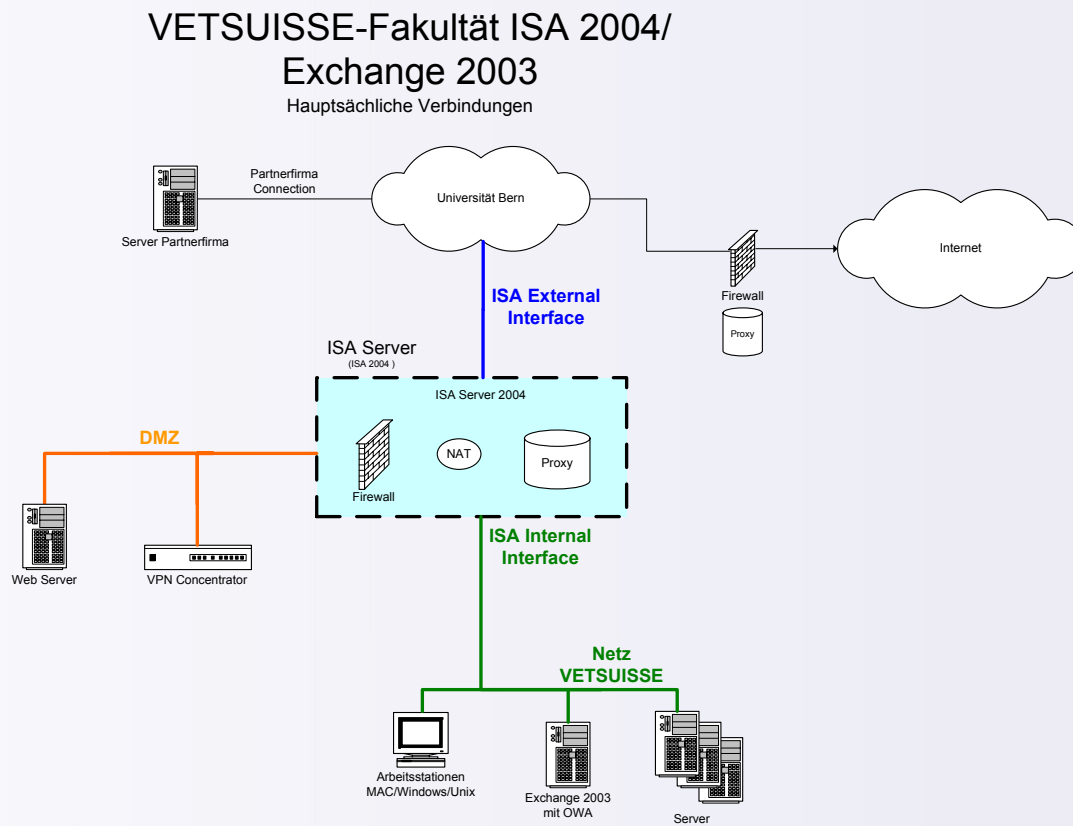


Abbildung 1: Prinzipielle Darstellung des ISA 2004 Umfelds in der VETSUISSE-Fakultät.



## Resultat

Das erste Projekt der FITIT Informatik GmbH mit dem ISA Server 2004 bei einem Kunden, konnte erfolgreich umgesetzt werden. Die Anlage in der VETSUISSE-Fakultät läuft stabil. Die Qualität des Produktes überzeugt, die Firewall kann ihre zentrale Rolle wahrnehmen.

Die Vorteile von ISA 2004 konnten im Projekt VETSUISSE-Fakultät zum Nutzen des Kunden weitgehend umgesetzt werden:

- Klare Menüstruktur, angelehnt an die bekannten Oberflächen anderer Microsoft Produkte
- Interessantes Preis-Leistungsverhältnis
- Geeignet auch für komplexe Anforderungen
- Stabiler Betrieb
- Weitgehende Integration mit Back Office Produkten wie Exchange 2003 und Outlook Web Access

Die grosse Menge an Protokollen und speziellen Konfigurationen, welche einzurichten waren, zeigen die herausragenden Möglichkeiten von ISA 2004 klar auf. Auch die Kompetenz der FITIT Informatik GmbH als Lösungsanbieter in diesem Bereich, konnten in dem Projekt eindrücklich unter Beweis gestellt werden.

## FITIT Informatik GmbH

Bernstrasse 67, Postfach  
3122 Kehrsatz  
Telefon: +41 (0)31 961 61 61  
Telefax: +41 (0)31 961 34 45

[www.fitit.ch](http://www.fitit.ch)  
[info@fitit.ch](mailto:info@fitit.ch)