

Dealing With Network Security in Academic Institutions – a Case Study

Ivan Doležal¹, Jiří Grygárek¹, Ondřej Jakl² and Karel Krečmer²

¹VŠB – Technical University Ostrava, IT Services
17. listopadu 15, 708 33 Ostrava – Poruba, Czech Republic
{ivan.dolezal,jiri.grygarek}@vsb.cz

²Institute of Geonics of the Czech Academy of Sci.
Studentská 1758, 708 00 Ostrava – Poruba, Czech Republic
{jakl,krecmer}@ugn.cas.cz

Abstract: The paper presents a real-life experience of the authors with their efforts at a radical security improvement of the academic computer networks that they administer at a large university and a medium-sized research institute. The solution, which started in 2004 and is still going on, has been based on hardware multi-threat security appliances with high throughput. The requirements on them included a combination of general purpose Intrusion Prevention System, HTTP/FTP antivirus capabilities and firewall functions. In particular, experience with appliances of the FortiGate series, which have been deployed as the best solution available, is described.

Keywords: network security, firewall, IDS, IPS, FortiGate, academia.

1 Introduction

VŠB – Technical University (VSB) and Institute of Geonics of the Czech Academy of Sciences (IG) are adjoining, but independent academic institutions located in Ostrava, Czech Republic. Although incomparable in size (VSB is a large university having about 25 thousand students, whereas IG is a medium-sized research institute, the staff of which is about 100), they are capable to cooperate and in 2004 responded to a call for projects declared by the Czech Ministry of Education and proposed a joint infrastructural project concerning network security in the environment of research and development (R&D) organizations. The proposal has been accepted for funding. This contribution presents some intermediate experience obtained by the authors during the more than three years of the work on the project, namely with managing security in academic environment with help of specialized network protection systems.

1.1 Computer and Network Users in Academia

In general, when dealing with security in academic organizations, we have to consider their specific characteristics. Most of them can be derived from the diversity of users, who can be roughly split into three categories, each of which deserves quite different approach:

- By *standard users* we mean typically management and technical staff ensuring the everyday operation of the institution as such. For their routine work, most of them need regular computing environment, i.e. an office computer and corresponding software (usually text processor, spreadsheet,

mail/groupware client, (restricted) Internet access and interface to some local economic information system), which are now highly standardized. The administration of this environment can be extensively automated. While this type of users is prevalent in most non-academic organizations, they are in minority in academia.

- *Research workers* are typical computer and network users in R&D institutions, but represent the most diversified group. Depending on their field of study, they may need completely different computing environments, individual approach and specific services, e.g. software development, handling of large data sets or computer support for special laboratory equipment. Those users appreciate full freedom for their research and may be annoyed by security measurements posed by network administrators. As a rule, they are involved in inter-institutional collaboration and take advantage of remote access, data transfers, recently also Grid computing and other forms of network services. It may be difficult to enforce some regulations on them. On the other hand, the researchers are generally very competent and disciplined computer users.

- In this respect, the *students*, the third category of academic computer and network users, are the very opposite. They are probably the most problematic group to handle. From nature, they like to experiment and explore. Malicious activities must be anticipated, since some of them, such as the students of computer science, may have good background for efficient hacking. But also “normal” students can disable networks through legal or illegal activities generating large traffic. The great number and permanently changing classes make the handling extraordinary difficult.

It is the two latter categories of users that pose the greatest demands on network administration. VSB is an institution where all three categories of users meet in a heterogeneous collection, i.e. the network and security administration is particularly challenging, whereas at IG the missing students make the situation considerably easier.

1.2 Local Situation

In general, the starting point of our security-improving efforts was quite similar on VSB’s and IG’s networks, since their state was result of the former rather spontaneous and chaotic development, when the security was not adequately considered.

At VSB, the local network was protected by a set of stateless filters on the border router. Antivirus and/or firewall was installed on some of the employees’ computers. Student machines were entirely out of our control.

At IG, all networked personal computers were protected by antivirus software and the e-mail traffic was checked on the mail server for viruses and spams. The network as a whole was protected by a Linux machine instrumented as firewall (*iptables* with *fwbuilder*, later *shorewall* user interface), which we found rather awkward for occasional administration. More importantly, Fast Ethernet network interfaces of the firewall machine limited the traffic throughput to 100 Mbit/s, wasting the capacity of the institute’s Gigabit uplink to the Internet.

In both environments, the network operation had to count on conscientiousness of users who were urged to protect their workstation themselves by local antivirus and firewall software. Especially at VSB this was very difficult to enforce since its organizational units (faculties, departments, etc.) are quite independent.

1.3 Objectives

Our general aim was to improve the security of the local network environment of VSB and IG without seriously affecting the users, especially in the R&D sphere.

In particular, we intended to solve the long-standing issues of the network perimeter, i.e. at the boundary of the local and public network (Internet). The idea was to implement some security apparatus that would

- be aware of as many application layer protocols as possible (e.g. H.323, SIP)
- block viruses, worms and spyware from HTTP, FTP and mail traffic,
- implement IPS – not only to protect the local network from Internet attacks, but possibly also to quickly identify potentially harmful computers inside LAN.

The great difference between the VSB’s and IG’s requirements on the solution was related to the throughput: Based on long-term observations and knowledge of the traffic characteristics, for VSB we had to find an appliance that would be able to handle simultaneously about 400 000 connections, 800 Mbits/s firewall throughput and 70 Mbits/s antivirus throughput, i.e. performance, that was on the cutting edge of the actual offerings. For IG, firewall’s speed in network traffic control was not an urgent point. Here, the network administration would appreciate the ease of use and as far as possible maintenance-free operation. Nevertheless, both organizations preferred to build their solutions on similar and compatible devices of the same vendor.

2 Towards Efficient Network Security

The realization of our plans was not straightforward. Especially at VSB, we considered simultaneously several possible conceptions of the solution and tried to match them with products available on the market.

2.1 A Kick-off Solution

We addressed the vendors of security systems to offer an appropriate appliance that would be positioned on the border between the Internet and the local area network and that would fulfil our requirements specified in section 1.3 at a very high speed. At the end of 2004, we could find just some three vendors in the Czech Republic who claimed to meet the requirements. In the testing phase, it was difficult to verify and compare the capabilities since those complex devices

need some study to be set up. Already in this point we appreciated the FortiGate specimen which surpassed the other products in the ease of deployment. More importantly, the family of Fortinet appliances fitted best our functional needs at an acceptable price. In fact, we could not find any serious competitor at that time. *FortiGate* (1) is the brand name of the multi-threat security appliances for real-time network protection made by Fortinet Inc. (2). These are ASIC accelerated network devices, the capabilities of which include statefull firewalling, shaping, Intrusion Detection/Prevention System (IDS/IPS), antivirus (AV) and antispam functionality. FortiGate units can work on L2 (link layer) of OSI model and allow both command line and web-based management. Some more characteristics can be found in Table 1.

The estimated life expectancy of the deployment was five years – that’s why we inclined to buy the most powerful models affordable. Especially at VSB, to get the best performance and reliability, we decided to build a cluster of two FortiGate FG3600 (cf. Table 1) and configured them to run in the *active – active* high availability mode. This mode truly load balances the TCP sessions (antivirus, IPS) between the units in the cluster – other kinds of the IP traffic flow over the primary unit only. So far, we have verified that this configuration can handle throughputs of more than 500 Mbit/s. To prevent changes in network addressing, we decided to explore a unique L2 transparent mode feature, where the device acts as a network bridge.

Model	Interfaces [#]	Firewall [Mbits/s]	AV [Mbits/s]	Sessions [#]
FG60	4 FE	70	15	50k
FG200A	8 FE	150	30	400k
FG400A	2 GE, 4 FE	500	100	400k
FG800	4 GE, 4 FE	1000	150	400k
FG1000	2 GE, 4 FE	1000	~200	600k
FG3600	6 GE, 1 FE	4000	~400	1000k

Table 1. Number of Ethernet (Fast, Gigabit) interfaces and performance of selected FortiGate products (data of 2004).

IG similarly needed a scalable and robust multi-threat firewall solution (i.e. a Gigabit router-firewall) to protect its LAN against attacks, which would be dimensioned at least for a five-year service. Respecting the compatibility with VSB, we chose two FG800 units from the FortiGate product family (Table 1). Its characteristics perfectly suited our demands on capabilities and performance and we quickly got accustomed to its friendly user interface. Whereas for VSB, the pair of FG3600 units above was just the starting point for further development to meet its needs (cf. next section), IG’s network, from the performance point of view, can be served just by one unit until now. That is why the two-box cluster runs in the *active – passive* high availability mode (the primary unit handles the traffic and the secondary unit is in the hot-standby state).

2.2 Response to Network Pervasiveness

Since 2005, wireless networking (WiFi) has been deployed at VSB, especially for student needs. Unfortunately, private notebooks, although becoming part of the campus network, are out of our control. Their users are just required to prove

the identity either with IEEE 802.1x EAP-TLS (“with a user certificate”) or by connecting through VPN. Students’ notebooks can also get connected through Ethernet with 802.1x authentication, but this technology has never reached the expected popularity. The number of VPN connections is growing fast. To protect these new network entry points in a topologically clean way, we purchased and deployed two pieces of Fortinet’s FG400A and FG1000 units.

The number of mobile devices, however, has been continually growing among regular staff, too. Many such devices are not being connected only through the well-defined set of network sockets and/or WiFi – the same entry points are often shared by “safe” desktops and “promiscuous” notebooks. Consequently, the whole concept of the fortified perimeter is deprecated. We considered the following advancements:

- 802.1x authentication of all connected devices – not only this is not a security solution per se, furthermore this feature would have to be supported by all of the network switches which in turn would require massive upgrade.
- Cisco NAC (Network Admission Control) – high TCO plus overcomplicated manageability would be the indisputable cons of this option.
- Leaving the end-user devices without special supervision and minimizing the impact of potential incidents by a strict network segmentation.

We decided for radical changes in the spirit of the last alternative: We sliced the network and created “internal perimeters” that correspond to more than 120 smaller subnets. Many of those VLANs are already connected to the network backbone through a FortiGate security appliance, each of them representing one security domain; yet more are to be connected.

This slicing approach was applied at every site, where VSB (its branch) is situated. These sites are interconnected by redundant L3 links,¹ that’s why every locality was equipped with its own FortiGate unit, operating in L2, as depicted in Fig. 1. At present, VSB employs 13 FortiGate units in total, what might make it the greatest Fortinet customer in the Czech Republic.

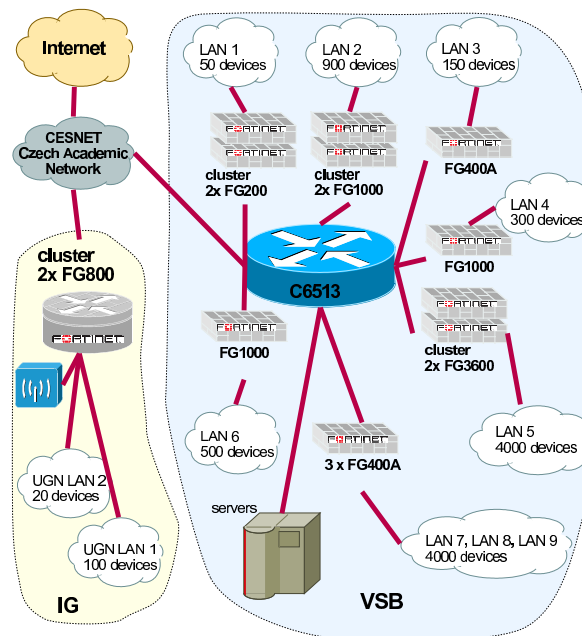


Figure. 1. IG and VSB network topology

The size of IG is comparable to the size of a smaller branch of VSB, so the issues discussed above could be handled in analogy with any VSB branch here. In fact, the IG network is divided into two subnets considered as separate security domains. We try to minimize the risk involved in accessing IG’s network from machines out of our control in various ways. For example, the most urgent service, remote mail access, has been satisfactorily solved through the IMAP server and users’ needs to remotely access IG’s servers or their local machines is possible through the SSH protocol and tunnelling. In general, we still refuse to connect foreign machines directly to our network. However, moderate and stable number of users makes it possible to have even their notebooks under reasonable control, i.e. at least to ensure that they are protected by local antivirus and firewall software. Similarly, computers making use of the IG’s wireless connect, which has been designed primarily for visitors and conference participants, are kept separated and the firewall handles them in the same way as ordinary machines on the Internet. Nevertheless, VPN, Eduroam and other modern services that could be beneficial for R&D are certainly under consideration. Our experience shows that FortiGate appliances are very valuable for the development of our LAN.

3 Real Life Experience

In this section, we present some concrete experience with the FortiGate deployment.

3.1 Is Less More?

Before the decision was made to acquire FortiGate multi-treat security appliances in 2004, Snort (4) among other alternatives was also evaluated. Its pro was the public availability of open source signatures. Its con was lack of them. Commercial solutions are the true opposite: plenty of them, but no one (including Fortinet support) knows what they exactly do. If an event is triggered, it is often very difficult to investigate if it is true positive or false positive. We decided to use about

¹Not shown in Fig. 1.

three quarters of the signatures only for detection (the actual ratio changes over time).

3.2 Tuning Up IDS/IPS

The Fortinet company sells a rather expensive auxiliary appliance called *FortiAnalyzer* for logging, analyzing and reporting information from FortiGate devices. However we learned to get raw information from the devices through Unix legacy syslog. Here is an example of a logged attack:

```
Jun  6 09:17:52 pixl1a1 date=2007-06-06 time=09:17:52
devname=Pixl1a1 device_id=FG36002805033272
log_id=0419070000
type=ips subtype=signature pri=alert vd=zamestnanci
serial=1237491673 attack_id=107610115 severity=high
src=158.196.154.46 dst=83.10.110.7 src_port=4163
dst_port=111
src_int=v1-206 dst_int=v1-2206 status=detected
proto=6
service=111/tcp user=N/A group=N/A
ref="http://www.fortinet.com/ids/ID107610115"
msg="rpc_decoder: RPC.Fragment.Overflow"
```

In the VSB environment, we log over 300 000 lines a day on a regular Linux PC. Since it would be hardly possible to analyze all this information manually,² the authors wrote a simple Perl analyzer *CORELLA* (“correlation”). This tool allows us to

- aggregate records with the same source IP address,
 - match information on leased addresses from other systems involved (RADIUS server, DHCP server, Active Directory in the future),
- all that in the heterogeneous university network infrastructure consisting of Cisco devices, Fortigate appliances and various open source software.

An example of information processed by *CORELLA* follows. In this example we can see an IPS aggregation that clearly points out a computer infected by a virus:

```
158.196.49.27 kolc408c.vsb.cz 55 x netbios:
MS.Windows.ASN.1.Bitstring.Overflow drop_session
prnk222a.vsb.cz gps.vsb.cz pcj331n.vsb.cz
pcj331d.vsb.cz
... (~20 more destinations follow)
```

It is not only the signature itself that is significant, but also the number of computers attacked from the source IP as well as the fact that some of them cannot be resolved by reverse DNS. A very useful strategy is that (a) whenever possible, the computer should have a static IP address that can be resolved and that (b) unused IP addresses cannot be resolved. The `drop_session` string indicates that suspicious packets were dropped and the connection was violently terminated.

A few signatures can themselves reliably indicate an infected machine:

```
158.196.158.46 kocour.vsb.cz 25 x netbios:
LSASS.445
[Reference: http://www.fortinet.com/ids/ID102039611]
drop_session ts1-106.vsb.cz ts1-112.vsb.cz
ts1-116.vsb.cz
```

²In small organizations like IG there will be no problem with manual analysis of logs through the standard FortiGate web interface.

```
vpns157.vsb.cz ts1-103.vsb.cz vpns252.vsb.cz
vpns248.vsb.cz
```

Traffic anomaly detector logs can show us suspicious behaviour of a PC. However, to determine the difference between zero-day attacks and a curious student playing with *nmap*, personal investigation is needed:

```
158.196.229.36 kolc411c.vsb.cz 7249 x anomaly:
portscan, 1001 1000 > threshold 1000 [Reference:
http://www.fortinet.com/ids/ID1006633981000]
clear_session
vpns241.vsb.cz vpns368.vsb.cz 158.196.198.1
158.196.198.157
158.196.198.164
... (~30 more destinations follow)
```

Peer-to-peer (P2P) networks are “special case”. Although Fortinet did produce some signatures to positively identify and possibly block this traffic, it is hide-and-seek game. The P2P clients try to mask the traffic. A totally obscure way to identify P2P network activity is by finding a different-than-expected signature. In our opinion it is quite unlikely that all of the downloaded files in the following example contained the BMP attack – we guess the traffic originated from P2P.³

```
158.196.xxx.xxx xxx.vsb.cz 525 x misc:
MS.Windows.Media.Player.BMP.Buffer.Overflow
[Reference:
http://www.fortinet.com/ids/ID101974234] dropped
1olo-172.dialup.vol.cz ap-veseli-hutnik.netopen.cz
gw-contactel.teltech.cz ppp141.brno.tiscali.cz
ovj-84-242-94-58.nat.karneval.cz
ip-85-160-88-194.eurotel.cz
wov-1-46.802.cz 85.132.180.86
... (~20 more destinations follow)
```

In the following log fragment, *CORRELA* identified users of systems that were assigned dynamic IP addresses (although we aim at avoiding dynamic address assignment, we were forced to use it in favour of WiFi and VPN):

```
158.196.68.42 vpn042.vsb.cz 1 x misc:
IRC.clientToServer.communication.JOIN detected
ost069.kolb410b.vsb.cz-09:13
```

False positive alarm that we cannot really handle: A typical example caused by a network printer:

```
158.196.154.191 prnj303a.vsb.cz 1 x snmp_decoder:
SNMP.Restricted.OID detected pcn304d.vsb.cz
```

3.3 FUD⁴ Unconfirmed (Not Really)

There was a nightmare for the project team that some IPS rule would totally paralyze traffic from some key application. Fortunately we encountered this only in a few cases of minor importance - Debian update or IBM Software Update. Both cases were promptly identified and resolved by an IP address exception.

Low latency multicast support was one of our important requirements. During the selection four years ago we could not find any other vendor than Fortinet that would meet our

³Btw: This signature was later disabled by the manufacturer himself.

⁴Fear, Uncertainty and Doubt

demands in this respect. Most appliances did not let the multicast pass through at all, whereas FortiGate units operated smoothly with latency under 1 ms.

3.4 Latest Update

In spring 2006 new FortiGate firmware version 3 with major improvements was released. One of them was the P2P filtering capability. After applying the new filter set we could recognize some 80% decrease of the P2P traffic, but we cannot exterminate it completely (yet). Instant messaging antivirus is another highly remarkable feature and URL blocking is a “cherry on the pie”: It is suitable for preventing users from accessing phishing web pages.

With the new firmware, the licensing policy was also modularized. Now, different features and various kinds of support must be purchased separately. Devices offer many more features (antispam, web pages classification, etc.), but in this paper we referred only to the features we have personal experience with.

4 Conclusion

When we look back after nearly four years, we can find that the FortiGate suite employed in our networks did improve manageability of security incidents both by reducing their number with AV/IPS and improving their detection with traffic analysis. This has been achieved without negative impact on the diversity of academic users in our institutions. Here are some additional comments.

The fear of the “bottleneck effect” was not confirmed.

The wise choice of an unknown appliance and ignoring Barnumesque advertisement has paid off. By the way, one of the most famous competitive products - Symantec SGS (6) - has been abruptly discontinued recently.

Even though prices for support represent significant annual expense (and are slightly growing), you can always give up buying the prefabricated signatures (support renewal) and add new signatures by hand using FortiGate’s simple configuration language. This is a tremendous difference from other vendors.

However, we also ran into a few problems:

- We experienced and reported three specific major bugs in the appliance (their explication is behind the scope of the paper). The time necessary for their resolution was in our opinion unacceptably long for a commercial customer. (The toughest issue has been solved by Fortinet for more than seven months.)
- Although Fortinet has been promising IPv6 support from the very beginning, neither IPS nor AV is functional for IPv6 traffic up to this day.
- Even though the appliance can provide its administrator with some log data, an advanced administrator will always want more data – be it more information on signatures or detailed statistics of accepted/rejected packets/sessions. Just by reading FortiAnalyzer Administration Guide we got an impression that purchasing this expensive device would not help either.
- If running more than two FortiGate appliances, you may want to buy *FortiManager* – another rather expensive appliance, which keeps the FortiGate configurations “in sync”. This is enormously important for setting up IPS

rules. Although we could work our some “do-it-yourself” tools for that purpose, too.⁵

Acknowledgment

This work was supported by the project No. 1N04035 of the Ministry of Education of the Czech Republic.

References

- [1] *FortiGate – Installation and Configuration Guide*, Fortinet Inc., 2004, 2007.
- [2] Fortinet. [Online] <http://www.fortinet.com/>
- [3] Juniper Networks IDP 50/200/600/1100 [Online] <http://www.juniper.net/>
- [4] Snort – the de facto standard for intrusion detection/prevention. [Online] <http://www.snort.org/>
- [5] M. Strebe, C. Perkins. *Firewalls and Proxy-Servers*, Computer Press, Brno, 2003. (In Czech)
- [6] Symantec SGS Security Appliance. [Online] <http://www.symantec.com/>
- [7] Wikipedia. [Online] <http://en.wikipedia.org/>

Author Biographies

Ivan Doležal was born in Ostrava, in former Czechoslovakia, now Czech Republic, in 1972. His graduations: B.A., FAMU in Prague, in 1993; MSc., electrical engineering and computer science, VŠB–Technical University Ostrava, in 1998. Currently he is an employee of the Centre for Information Technology of VŠB–Technical University Ostrava. He is the main coordinator of the grant 1N04035 of the Czech Ministry of Education which made this work possible.

Jiří Grygárek received his MSc. degree in electrical engineering in 1986 from VŠB–Technical University Ostrava. Initially he worked as a programmer. In the present time he works as a computer network technician at the university mentioned above. In 2006 he earned a CCNP certification (Cisco Certified Network Professional). His professional interests lie in the area of computer network security, routing and switching. He also works as an instructor of the Cisco Networking Academy.

Ondřej Jakl was born in Ostrava in 1959. He received his MSc degree in computer science from Charles University in Prague, Czech Republic, in 1984 and Ph.D. degree in extraction of deposits from the Academy of Sciences of the Czech Republic (ASCR) in 1994. Currently, he is the deputy head of the Department of Applied Mathematics and Computer Science at the Institute of Geonics ASCR, Ostrava and the head of its IT division. As senior scientist he deals with parallel processing in demanding finite-element simulations and their applications in geosciences. He is also an assistant professor at the Department of Computer Science of VŠB–Technical University Ostrava, giving lectures on parallel and distributed systems.

Karel Krečmer received his MSc. in 1999 in the field of software engineering and applied mathematics at VŠB–Technical University Ostrava. His Ph.D. studies are focused on efficient parallel implementation of FEM. Currently he is a researcher

⁵The boxes can be controlled over SSH.

at the Institute of Geonics ASCR, Ostrava and a project manager in the TietoEnator Czech company. His current interests include μ FEM, HPC and information security.