NĚKTERÉ ZKUŠENOSTI S INSTALOVÁNÍM A SPRÁVOU FIREWALLU VE SPOLEČNOSTI ORKLA FOODS INTERNATIONAL

Martin Kořínek

Guseppe a.s., ČSA 449, 500 03 Hradec Králové, ČR
martin.korinek@guseppe.cz

Abstrakt

Tento příspěvek by chtěl seznámit čtenáře s některými zkušenostmi při instalování, konfigurování a správě firewallů CheckPoint VPN-1 ve společnosti Orkla Foods International.

1. Ofint

OFInt. (Orkla Foods International), jako jedna z divizí Norské společnosti ORKLA, se v současné době skládá z těchto firem:

- Felix (Rakousko, sídlo Mattersburg)
- Felix HU (Maďarsko, sídlo Budapešť)
- Guseppe (Česká republika, sídlo Hradec Králové, výrobní závod Rokytnice v Orlických horách)
- Kotlin (Polsko, sídlo Kotlin, pobočka Varšava)

Sídlo OFInt. je umístěno ve Vídni, ale v průběhu roku 2002 bude přesunuto (zpět) do Osla.

IT oddělení společnosti Guseppe bylo vybráno jako středisko „Firrewall Competence Center“, což znamená, že je zodpovědné za všechny aktivity spojené s firewally v rámci OFInt. Jeho úkolem bylo (a stále je) vybudovat systém ochrany a zabezpečení dat před průnikem z Internetu.

Po praktické stránce to znamená zvolit, nainstalovat a nakonfigurovat odpovídající firewall a antivirový program. Na řešení jsou kladeny následující nároky:

- platforma pouze Wintel,
- jednotlivé společnosti budou standardně chráněny (viz požadavky na firewall a antivirový program),
- mezi společnostmi (a jejich pobočkami) bude vytvořeno bezpečné propojení – VPN,
- firewally se budou spravovat z jednoho místa, bude určen jeden administrátor,
- tento administrátor bude moci konfigurovat firewally i po Internetu,
- firewall musí umožňovat snadné kryptované propojení mobilním uživatelům pomocí VPN,
- navržený systém firewall bude možno rychle aplikovat na případné další nové společnosti divize OFInt.

2. Minulost

Na začátku roku 1999 byla provedena instalace firewallu AltaVista ve všech společnostech OFInt. Tento systém se stal nevyhovujícím a to hned z několika důvodů:

- software (firewall) AltaVista byl prodán a jeho vývoj dočasně ukončen (posléze se objevil jako firewall Raptor)
- skončila licenční smlouva na software AltaVista,nešlo prodloužit tuto smlouvu
- skončila podpora od společnosti Compaq
- již v době instalování nebylo možno v ČR objednat školení na odpovídající verzi
- instalovaná a „licencovaná“ AltaVista byla určena jen pod Windows NT, nebyla testována pod Windows 2000 Server

Z těchto důvodů bylo rozhodnuto, že IT oddělení společnosti Guseppe navrhne firewall, který se nasadí v OFInt.

Poznámka: Jak už to bývá, Guseppe dostalo tento úkol zřejmě proto, že od začátku poukazovalo na zastaralou verzi instalovaného firewallu, nemožnost zaškolení a obtížné podpory.

V prosinci roku 2000 byl podán návrh na výběr nového firewallu pro OFInt. V polovině roku 2001 bylo založeno Firewall Competence Center, v říjnu roku 2001 se začalo s instalováním firewallu CheckPoint VPN-1 a to postupně v jednotlivých lokalitách

3. Současný stav

Jaký je stav firewallů v rámci OFInt. je patrné z následující části referátu, který byl přednesen na ITSC meetingu general managerů, finance managerů a IT managerů OFInt.

FIREWALL COMPETENCE CENTER

Start of Firewall Competence Center - After 2nd OFInt. ITSC meeting (14. August, Mattersburg)

Start cooperation with:
Lars Jorgen Granheim (ORKLA Brands IT Center – responsible for joint firewall solution and Internet services for the brands business area, the ODIN and ORKLA HQ)
Werner Neunteufl (IT Design Austria – expert for Firewalls)
Hans Kasbauer (IT Design Austria – expert for Firewalls)

What we have done
Prepared project of Firewall-1 CheckPoint installation
Prepared project for change IP addresses

Present situation

Felix Austria
Change IP addresses
Firewall NG (Compaq, Windows 2000 server)

Felix HU

Change IP addresses
Firewall 4.1 (Nokia)
Create VPN connection for Domino

Guseppe

Change IP addresses
Firewall NG, Feature Pack 1 (Compaq with RIB, Windows 2000 Server)
Management Console NG, Feature Pack 1
Create VPN connection between Hradec Kralove and Rokytnice
Create VPN connection for Domino
Remove Notes user from HKRMG001 to VIEMG001
(Done by Lotus Notes Competence Center)

Kotlin

Change IP addresses
Firewall NG, Feature Pack 1 (Compaq with RIB, Windows 2000 Server)
Create VPN connection between Kotlin and Warsaw
Create VPN connection for Domino

Near future

Upgrade Firewall (install Feature Pack 1) at Mattersburg
Create object and rule for Domino VPN connection for Poland
Upgrade Firewall (on Nokia HW) at Budapest
Upgrade Cisco routers at Rokytnice (Guseppe)

Create pcAnywhere connection to all necessary DNS servers (all companies)

Finalization of documentation (describe objects, rules and all settings)

Vysvětlující poznámky:

- V Guseppe (resp. v Hradci Králové) je instalován modul Management Console, s jehož pomocí lze z jednoho místa monitorovat a konfigurovat všechny firewally.
- Až na Felix HU jsou všude instalovány firewally na HW Compaq s RIB (Remote Insight Board) a Windows 2000. Z důvodu bezpečnosti byl pro Felix HU zvolen HW Nokia.
- Na přelomu roku 2001/2002 bylo nutno změnit interní IP adresy tak, aby splňovaly kritéria pro zařazení OFInt. do WAN sítě ORKLA.
- Ve stejné době se provedly dvě zásadní změny na mailových systémech (Lotus Notes/Domino). Prvním krokem bylo převedení ISDN propojení mezi DOMINO servery (Level3) v jednotlivých společnostech s „hlavním“ serverem (Level2) v Mattersburgu na propojení po Internetu (VPN). Dalším krokem bylo zredukování počtu Level3 serverů OFInt ze 4 na 1. Znamená to, že uživatelé v jednotlivých společnostech OFInt. přistupují ke svým mailovým databázím výhradně vzdáleně a to po VPN. Všechny (nejen) mailové databáze jsou umístěny na jediném serveru, který je fyzicky umístěn v Mattersburgu. Pro všechna VPN propojení jsme museli pochopitelně definovat pravidla na firewallech.

4. Některé problémy

Při instalování a konfigurování jsme se setkali s mnohými problémy. Některé jsou v následujícím odstavci popsány.

4.1 Remote Insight Board

RIB je deska, která se instaluje do serveru a která umožňuje vzdálený přístup a ovládání počítače a to ihned po jeho zapnutí (dokážeme vzdáleně nastavit Setup).

Přestože jsme si pořádně pročetli dokumentaci, nepodařilo se korektně RIB nainstalovat. Teprve po ověření na www stránkách Compaq jsme se dozvěděli, že informace uvedené v manuálu jsou chybné.

Nicméně korektně se podařilo RIB nainstalovat pouze čistý server – jen se systémem Windows 2000 a nikoli již s instalovaným Firewallem. Jak v Česku tak i v Polsku jsme museli kompletně reinstalovat celý server.

4.2 Školení

V polovině roku 2001 se započalo s instalováním firewallu CheckPoint NG v OFInt. (první instalace byla uskutečněna v Mattersburgu). Od té doby jsme poptávali školení na nejnovější verzi – NG. Koncem roku 2001 bylo dostupné školení v Bratislavě (4 dny za 3 500 EUR) a ve Vídni (3 dny za 3 700 EUR). V Česku (firma Prago Data) teprve uvažovala o školení na verzi NG. Koncem měsíce března 2002 však ještě nebylo zřejmé, zdali firma PragoData bude poskytovat standardní školení či jenom „rozdílové“ školení (vzhledem k verzi 4.1.

Vzhledem k tomu, že IT oddělení Guseppe již má určité zkušenosti s instalováním a správou firewallu CheckPoint verze NG, rozhodlo se, že zjistíme možnost školení pouze vybraných okruhů v Bratislavě (jen dva dny) a u lokálního ISP (Contactel) – jeden den věnovaný tématům jako „Správa routerů“, „DNS, WINS“, „telnet“ a podobně.

4.3 IT Design - support

Pro prvotní fázi instalování FW v Mattersburgu jsme použili služeb rakouské společnosti IT design. S touto firmou, především s panem Wernerem Neuteufelem, máme delší dobré zkušenosti. I na základě jejich doporučení jsme vybrali CheckPoint jako standardní firewall pro OFInt.

Posléze se ukázalo, že tato firma má sice velké zkušenosti s firewally, ale přesto náš projekt je poněkud rozsáhlý a že jsme pro IT design prvním zkušebním „pilotem“. Nicméně, zjistili jsme, že i v ostatních zemích OFInt nemá žádná firma zkušenosti s tak rozsáhlou správou firewallů.

Protože verze NG byla skutečně velmi nová, nebylo snadné rychle zprovoznit některé aplikace (moduly). Navíc pan Werner Neuteufel začal být zaneprázdněn jiným projektem a tak jsme obdrželi jiného zástupce firmy IT design – Hanse Kasbauera. Musíme zdůraznit, že tato změna byla velice pozitivní. Po seznámení se s naší problematikou je Hans Kasbauer důležitým poradcem našeho systému firewallů a sám navrhl důležité a zásadní změny (HW

doporučení, instalování RIB, změna IP struktury a konfigurování DNS, poznámky k registrací domén a MX záznamů a podobně). Na druhou stranu je vidět, že i on se „učí“ a že některá nastavení na firewallech později „vylepšuje“.

4.4 Winroute

OFInt jako součást ORKLA má jako mailový standard systém Lotus Notes/Domino. Ovšem vzhledem k výši ročních poplatků za jednoho uživatele rozhodlo Guseppe instalovat pro střední management svůj vlastní dodatečný mailový server – Winroute. S integrací firewallů a nastavováním práv však vyvstaly, jak jednoduše nastavit pravidla pro nestandardní mailový server.

V současné době je Guseppe nuceno ukončit provoz mailového serveru a všechny účty převést na „standard“ – Lotus Notes/Domino mail systém.

4.5 Definování pravidel (rule)

Definování pravidel pro (omezení přístupu z venku a i zevnitř podnikové sítě) je na firewallu CheckPoint poměrně snadné. Po krátkém seznámení se s podstatou není problémem učinit některé, byť dočasné, změny.

Při změnách pravidel jsme se však několikráte potýkali s problémem chyby uživatele – administrátora. Jelikož pro celou OFInt jsme nuceni definovat v podstatě značné množství síťových objektů (firewally, servery, částí sítí a podobně), pravidel a definování překladů adres (NAT), používáme pro zobrazení na 17“ monitoru větší rozlišení. Na druhou stranu se pak snadno stává, že přehlédneme chybějící písmenko či naopak jeden znak navíc.

Zcela konkrétně se toto stalo při definování pravidel pro VPN propojení mezi Domino servery v Rakousku a Polsku (v definici mail domén u domény @kotlin.com.pl „vypadlo poslední písmenko „l“), při instalování pravidel jsme si spletli firewall „Felixat“ a „Felixhu“.

Podobným problém nastal při pozastavení pravidla (disable rule) pro VPN propojení mezi Domino servery „kotlin/mattersburgu“, když jsme přehlédli v názvu podsítě příponu „notes“.

Všechny tyto problémy jdou jen na vrub zvolenému příliš malému fontu a nevhodně zvolenému pojmenování objektů. Oba stavy bylo možno snadno změnit.

4.6 Upgrade – FP1

Další problém se ukázal při instalování FP-1 („service pack“) na firewally. Jak v Hradci Králové tak v Kotlinu jsme museli posléze celý systém instalovat nanovo (top znamená na „čistý“ server instalovat Windows 2000, SP2, CheckPoint a poté FP-1). Otázkou zůstává, zdali problém nebyl zapříčiněn kolizí s instalováním RIB (HW).

Nicméně, při posledním upgrade firewallu v Mattersburgu , se poté objevovalo „zamrznutí“ systému. Nutno podotknout, že v Mattersburgu není prozatím na serveru instalována RIB. Problém se opět vyřešil úplným přeinstalováním firewallu (serveru).

4.7 Odlišný HW

Zprvu se zdálo rozumné, aby ve Felixu HU byl instalován CheckPoint na jiném HW – Nokia. Důvodem bylo nepříliš kompetentní oddělení IT. S integrací všech firewallů v rámci OFInt. se však ukázalo, že s jinou HW platformou nastávají menší potíže – nemožnost upgradovat firewall ve Felix HU na stejnou verzi (prozatím je instalována předchozí verze 4.1), problémy s verifikací správy firewallu ve Felixu HU pomocí Management Console v Guseppe HK a podobně.

V blízké době bude proto instalován ve Felixu HU shodný firewall jako v celé OFInt (Compaq server s Windows 2000 - a pochopitelně RIB).

4.8 Obnovování starých pravidel

Při upgradování Management Console v Guseppe jsme narazili na velmi zajímavý problém – při ukládání definice pravidel se ukládala rovněž i všechna stará nastavení. Jediným řešením bylo postupné a ruční mazání nepotřebných (starých) pravidel. Toto mazání, protože jsme jej prováděli vzdáleně z Kotlinu (Polsko), nám zabralo celé jedno dopoledne. Po odmazání všech starých nastavení byl systém již funkční a podstatně se urychlilo ukládání (záloha) nových pravidel.