II LUBUSKI KONWENT INFORMATYKÓW

ZASTOSOWANIE OPEN SOURCE W GMINIE GOLENIÓW

Dariusz Przybylski

Urząd Gminy i Miasta w Goleniowie

http://www.goleniow.pl

Łagów, 9-10.VI.2011r.

GOLENIÓW MIASTO HANZEATYCKIE
PRAWA MIEJSKIE OD 1268 r.

AGENDA

1. **Wprowadzenie** – rys historyczny (motywacje, wcześniejsze doświadczenia, kalendarium, infrastruktura)
2. **Przykład konkretnego rozwiązania** działającego w urzędzie w Goleniowie (szczegóły techniczne projektu)
3. **Podsumowanie**, wnioski (wady i zalety zaprezentowanego rozwiązania)
4. **Część praktyczna** – prezentacja wybranej funkcjonalności (jeśli czas pozwoli)

KALENDARIUM:

od 1993 do 2003

serwery system Novell Netware (3.11 -> 4.2)

stacje Microsoft DOS/Windows (DOS 6.22, Windows for Worgroups 3.11, 95, 98, Me, 2000)

aplikacje (bazy DBF, TAG, MS Works, MS Office, StarOffice)

łącza internetowe: ISDN, SDI (HIS)

od 2003 do 2011

serwery system GNU Linux (rpm, deb), Microsoft Windows Server 2003

stacje Microsoft Windows (XP, Vista, 7)

aplikacje (bazy SQL, StarOffice->OpenOffice)

łącza internetowe: xDSL

od 2012 do .....

główny kierunek -> wirtualizacja

pełne wdrożenie AD DS , GPO (LIKEWISE OPEN, SAMBA 4, a może MS Windows Server 2008 R2 ...?)

OpenOffice.org -> LibreOffice.org

INFRASTRUKTURA:

SPIS FIZYCZNYCH SERWERÓW - stan na maj 2011

lp	Nazwa / System operacyjny	Numer inwentarzowy	Specyfikacja techniczna	Rok (wdrożenie)	Przeznaczenie (Rola)
1	SERVER (LINUX DEBIAN)	UGM/04/KOMP109088	INTEL PENTIUM 2.8GHz, Seagate 2x120GB HDD SATA, ASUS P4P800-VM, LG DVDRW, Kingston 2x512MB RAM,Chieftec BH-01B-B-B - 400W	2003	File server (systemy F-K, ewidencja, windykacja), wewnętrzna poczta elektroniczna EXIM, Archiwizacja (replikacja scp/rsync), serwer WINS, kontroler domeny na poziomie Windows NT
2	SERVER (LINUX MANDRAKE)	UGM/04/KOMP109123	FUJITSU-SIEMENS ECONEL 200, Intel XeonT 3,2 GHz FSB 800, 2 MB cache Chipset IntelR E7320 RAM 1 GB ECC DDR2 SCSI Adaptec 29320 Dual-Channel Ultra320 RAID 1, 146,8GB Ultra320 SCSI X2, ATI Rage XL 8MB (D-SUB) Karta IntelR PRO/1000 Server Network FDD DVD-RW 16x	2006	File server (pozostałe ewidencje, rejestry), archiwalny system obiegu ISONET (MySQL), archiwizacje (replikacja), Baza SQL Firebird2
3	SERVER (LINUX DEBIAN)	UGM/04/KOMP109182	INTEL Core2 Duo E8500 3,16GHz, GIGABYTE GA-EP35-DS3,RAM Kingston 2x2048MB HYPERX 800MHz DDR2, Grafika GIGABYTE GeForce 7200GS 128MB PCI-E, INTEL FastEthernet Pro/100 x2, HDD WD 320GB SATA, CHIEFTEC LBX-02B-B-B 400W, FDD i LG-DVDRW IDE, +3wentylatory	2004 (modernizacja 2008)	Systemy bezpieczeństwa (proxy, firewall, ids/ips, vpn itp.) UTM
4	SERVER (LINUX DEBIAN)	UGM/04/KOMP109185	HP PROLIANT ML150G6 E5504 Intel Xeon (HP 5U LFF SATAx2, HP Smart Array P410/256MB, HP750W CS HE Powerx2, HP RPS 5U G6 2x250GB 3G 7.2K MDL HP, 2x1TB 3G 7.2K MDL HP ,2GB 2Rx8 PC3-10600R-9 Kit ECC, HP DVDRW SATA, 3Y gwarancja, Streamer HP StorageWorks DAT72 USB Int Drive, HP StorageWorks Data Protector Express Single Server Edition	2009	System obiegu dokumentów eOBIEG (PostgreSQL, PHP), baza dokumentów - skany pdf
5	SERVER (MS WINDOWS SERVER 2003 SBS OEM)	UGM/04/KOMP109126	Intel XeonT 3,2 GHz FSB 800, 2 MB cache Chipset IntelR E7320 RAM 1 GB ECC DDR2 SCSI Adaptec 29320 Dual-Channel Ultra320 RAID 1, 146,8GB Ultra320 SCSI X2, ATI Rage XL 8MB (D-SUB) Karta sieciowa: IntelR PRO/1000 Server Network FDD DVD-RW16x	2007	Systemy informacji prawnej LEX, monitorowanie centralnego zasilania LANSAFE, audyt infrastruktury informatycznej eAUDYTOR, Bazy ewidencyjne MS SQL 2005 Express, oraz bazy SQL Firebird2, system bilingowy centrali telefonicznej, print audyty, serwer update WSUS, bazy SQL BESTI@, Centralne repozytorium bazy programu antywirusowego ESET

STACJE KLIENCKIE (XP,Vista,7): aktualnie pracuje w naszej sieci LAN 105 aktywnych jednostek roboczych (z tego 90% to MS Windows XP Prof.)

INFRASTRUKTURA:

APLIKACJE OPENSOURCE używane obecnie w UGIM Goleniów	
Strony internetowe CMS	Joomla, PHP, MySQL, phpBB, phpMyAdmin, WordPress
Klient FTP	FileZilla
Edycja stron internetowych HTML	Nvu
Edycja grafiki	Gimp
Pakiet biurowy	openOffice.org, (odt)
Przeglądarka internetowa	Mozilla Firefox
Klient poczty	Mozilla Thunderbird
Kompresja danych, archiwizacja	CloneZilla.org, 7-Zip
Bezpieczeństwo, szyfrowanie	ClamWin, TrueCrypt
Zarządzanie zdalne	PuTTY, OpenVPN, WinSCP
Informacje personalne (PIM)	Mozilla Sunbird
Skrypty, programowanie	Notepad++
Diagnostyka	Memtest86+, BackTrack
Wirtualizacja	VirtalBox
Systemy operacyjne z GUI	Debian, Ubuntu, Knopix

MOTYWACJE I TRUDNOŚCI:

✓ Decydujący czynnik finansowy

✓ Zagmatwany sposób licencjonowania - polityka Microsoft, poirytowanie sposobem licencjonowania (Publisher zamiast PowerPoint, niespójność wersji, OEM, SB, brak dostępnych osobno produktów np. EXCEL), brak jedności w formacie zapisu danych tekstowych i kompatybilności w interfejsie użytkownika (np. doc, 97/2000 – 2007/2010)

✓ Realizowanie polityki legalności oprogramowania

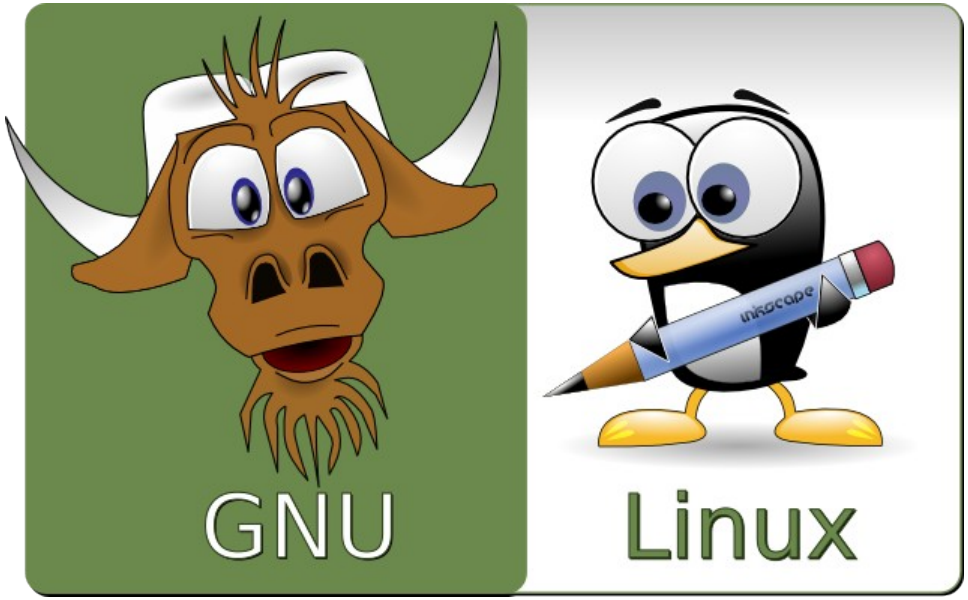
✓ Wolność (swoboda przenoszenia produktów miedzy komputerami, prawo swobodnego wyboru)

✓ Główne trudności: przełamanie przyzwyczajeń, wolniejsze uruchamianie aplikacji, nauczyć „SAVE AS”, skuteczne przekonanie pionu zarządzającego

Licencje Microsoft					
Part Number	Produkt	Ilość	Cena netto (PLN)	Wartość netto (PLN)	Wartość brutto (PLN)
P72-04229	Windows Server Enterprise 2008R2 MOLP Gov, 20 TCAL	1	6 640,00 zł	6 640,00 zł	
R18-02784	Windows Server CAL 2008 MOLP Gov User CAL	100	87,00 zł	8 700,00 zł	
6VC-01222	WinRmtDsktpSrvcsCAL 2008 OLP NL Gov UsrCAL	20	245,00 zł	4 900,00 zł	
				20 240,00 zł	24 895,20 zł

Produkt	ilość	Cena netto	Wartość netto	Wartość brutto
Microsoft Office 2010 PL BOX dla Użytkowników Domowych i Małych Firm	105	1 015,44 zł	106 621,20 zł	131 145 zł

PREZENTACJA WYBRANEGO PROJEKTU DZIAŁAJĄCEGO W GMINIE GOLENIÓW W OPARCIU O SYSTEM GNU DEBIAN LINUX

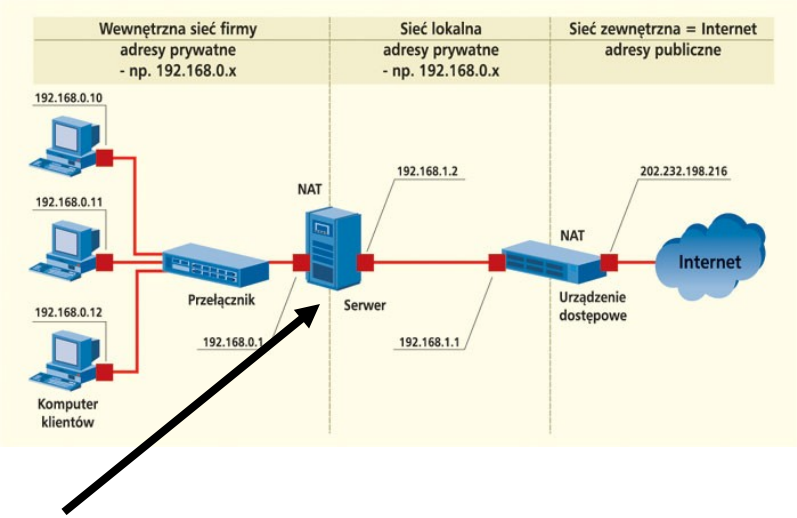


Kompleksowe zabezpieczenie sieci firmowej

pn. „DEBIAN **U**nified **T**hreat **M**anagement”

SCHEMAT IDEOWY LOKALIZACJI SERWERA DEBIAN-UTM

Rozwiązanie w oparciu o system Linux dystrybucja Debin 5.0.1 Lenny kernel 2.6



ZAKRES PROJEKTU:

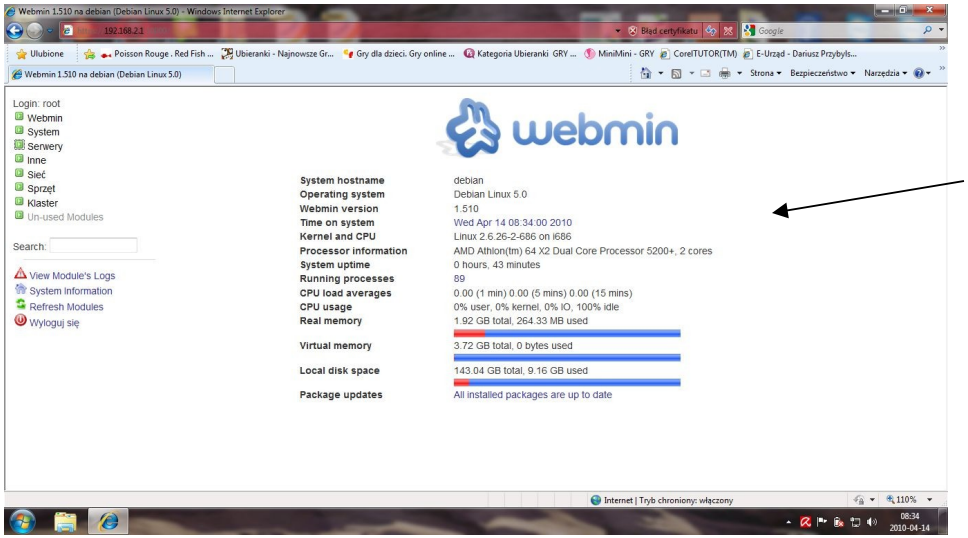
- Dwustrefowy **FIREWALL** (strona LAN i WAN)
- System detekcji i wykrywania włamań **IDS/IPS** (auto-blokada, powiadamianie e-Mail)
- Systemy **PROXY** filtrowanie treści na poziomie usług WWW i EMAIL (tzn: kontrola antywirusowa, kontrola załączników, kontrola słownikowa, kontrola na podstawie czarnych i białych list), buforowanie zapytań DNS
- **MONITORING** rejestracja zdarzeń, analiza logów, synchronizacja czasu NTP, kontrola temperatury w serwerowni (powiadamianie SMS)
- **BEZPIECZEŃSTWO** kontrola integralności rozwiązania, VPN, DHCP (jednoznaczna identyfikacja stacji), statyczna tablica ARP, dzielenie pasma
- **ZARZĄDZANIE** w miarę przyjazny sposób poprzez przeglądarkę internetową (skrypty)

Dodatkowo dwie dokumentacje: **użytkowa**-administratora oraz **techniczna**-projektowa

ZASTOSOWANE PAKIETY PRZY BUDOWIE SERWERA DEBIAN-UTM

- integralność systemu: TRIPWIRE
- synchronizacja czasu: RDATE
- kontrola antywirusowa: CLAMAV
- anty malware (rootkity itp): RKHUNTER, CHKROOTKIT, UNHIDE
- bezpieczeństwo serwera OPENSSH: DENYHOSTS (klient Windows PuTTY: www.putty.org)
- proxy EMAIL: P3SCAN + RENATTACH
- proxy WWW: SQUID + DANSGUARDIAN + DGLOG + SARG + CALAMARIS
- proxy DNS (cache only): BIND9
- firewall IPTABLES: skrypt IPTABLES (polityka wszystkich łańcuchów INPUT, OUTPUT i FORWARD domyślnie ustawiona na DROP, przepuszczam tylko jawnie zadeklarowany ruch, reszta do LOGów, dobre wzorce: www.cipherdyne.org)
- zarządzanie przydziału pasma QoS: skrypt HTB oparty na TC (alternatywa: niceshaper.jedwabny.net)
- system IDS/IPS: PSAD (monitorowanie wszelkich anomalii sieciowych również z poziomu LANu , warstwa sieciowa i transportowa)
- dodatkowa ochrona w oparciu o sygnatury - konwersja reguł SNORT na iptables: FWSNORT (warstwa aplikacji)
- serwer DHCP: DHCP3-SERVER (skrypt LISTA, stałe powiązanie MAC z IP)
- powiadamianie e-mail: EXIM4
- kontrola sprzętu (temperatura, prędkość obrotowa coolera, napięcia CPU itp): LM-SENSOR, I2C-TOOLS
- zarządzanie: WEBMIN (zwłaszcza w zakresie dansguardian i dglog ułatwienie zarządzania i monitorowania przez przeglądarkę IE)
- wizualizacja logów: LSTAT, RRDTOOL, APACHE2 (alternatywa: www.cacti.net)
- powiadamianie SMS: skrypt python (rodion.grolsh.pl) wykorzystujący konto mBox operatora orange.pl
- dostęp VPN w oparciu o certyfikaty, Client-to-Site : OPENSSL, OPENVPN (klient Windows: www.openvpn.net)
- testowanie: NMAP, IPTRAF, JOHN, DNSUTILS, NETCAT

WYBRANE ASPEKTY ZARZĄDZANIA SYSTEMEM



Time on system (aktualny czas na serwerze)

System uptime (czas pracy serwera od ostatniego startu)

CPU load averages (średnie obciążenie procesora)

Real memory (rzeczywiste użycie pamięci operacyjnej RAM)

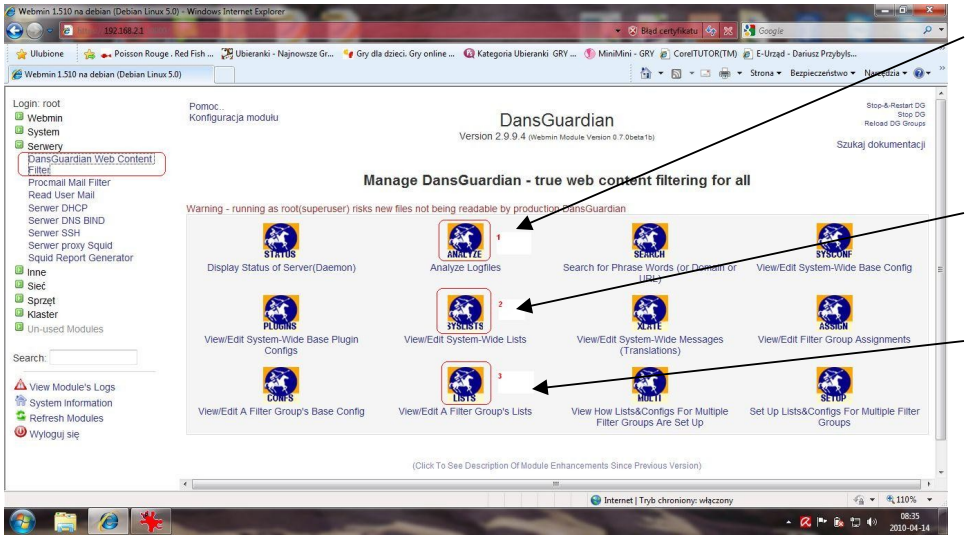
Local disk space (realna zajetość dysków)

Operating system, Processor information (wersja systemu operacyjnego, typ procesora)

Running processes (liczba uruchomionych zadań na serwerze)

Kernel and cpu (wersja kompilacji jądra systemu linux)

Virtual memory (rzeczywiste wykorzystanie pamięci buforowej Swap)



1) **Analyze Logfiles** (przegląd zdarzeń zarejestrowanych w ruchu WWW)

- można oglądać LOGI według zadanego zakresu dat zdarzenia (Enter Date Range)

-adresu IP danego użytkownika (Enter Client IP Adrdess)

-adresu domenowego URL (Enter a Site Name)

-różnych zarejestrowanych zdarzeń blokad i kryteriów (Choose a Reason Action)

2) **View/Edit Systems-Wide Lists** (możliwość wprowadzenia czarnej i białej listy na konkretne IP)

- podział na Banned IP list (lista adresów zablokowanych dla usługi WWW)

- Exeption IP list (lista adresów IP wyłączonych spod sprawdzania filtrów słownikowych)

3) **View/Edit A Filter Group's Lists** (lista 25 filtrów kontekstowych WWW)

- tu między innymi odgórnie ustawiamy strony zablokowane BANNED lub odblokowane EXCEPTION

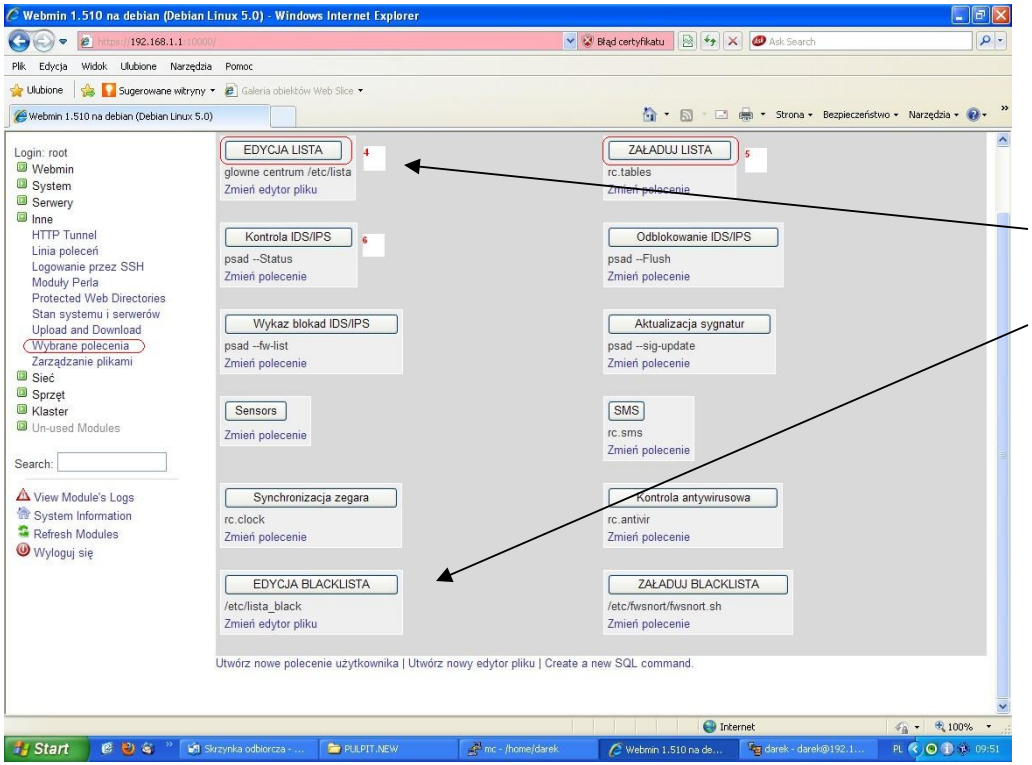
- Banned site list (lista stron www uznanych przez kierownictwo za zablokowane)

- Exception site list (strony odblokowane ze sprawdzania filtra słownikowego)

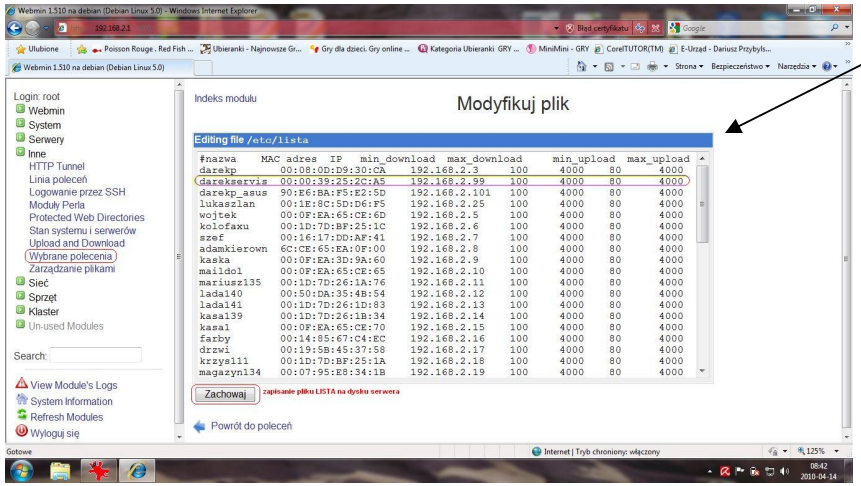
- Banned extension list (lista zablokowanych rozszerzeń np.: .exe, .com .pif, .vbs)

-Exception extension list (lista rozszerzeń plików dopuszczonych do pobrania np.: .xls, .doc, .zip itp. według aktualnej polityki firmy)

WYBRANE ASPEKTY ZARZĄDZANIA SYSTEMEM



ilość i rodzaj przycisków w grupie menu INNE -> WYBRANE POLECENIA można dowolnie modelować według indywidualnych potrzeb administratora lub kierownictwa firmy. Na szczególną uwagę zasługuje możliwość edycji BLACKLISTY (czyli wykaz stacji-IP dla których ruch przez UTM jest całkowicie zablokowany)



Edycja WHITE LISTA załatwia kilka tematów (zasila 4 pliki konfiguracyjne):

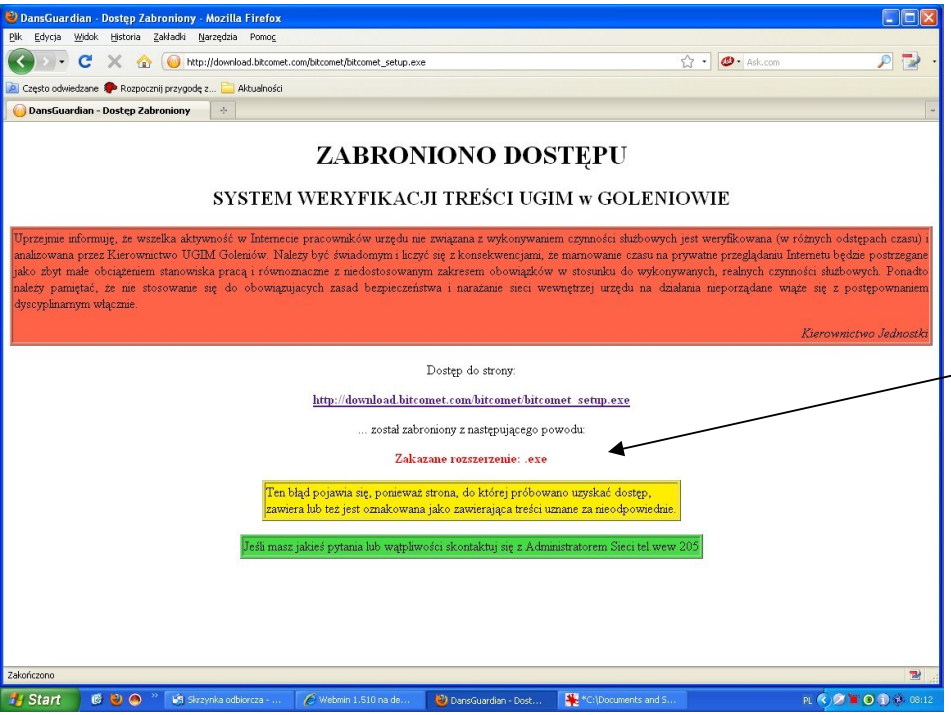
- możliwość sterowania przepustowością poszczególnych stacji (regulacja pasma upload i download)

- stałe powiązanie MAC i IP w DHCP (daje praktycznie 100% identyfikacji użytkownika - co, kto i kiedy)

- zpobiega podłączaniu "obcych" komputerów (np. przyniesiony przez pracownika notebook z domu nie połączy się z internetem i nic nie wyśle i nie odbierze)

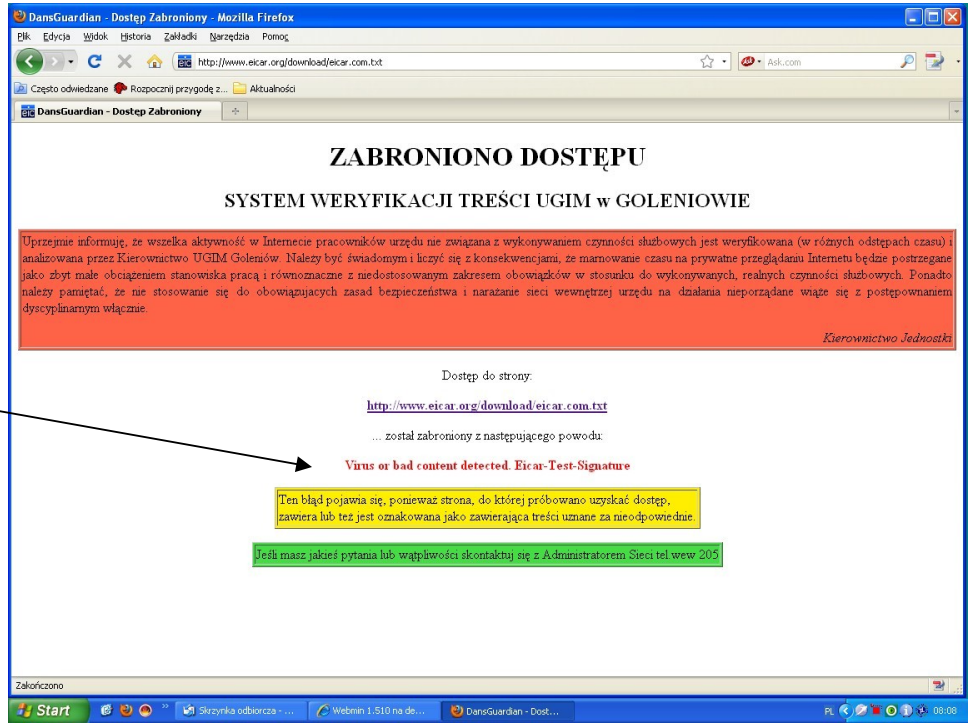
- zapobiega atakowi "man in the middle" (polega na modyfikacji tablicy Address Resolution Protocol (ARP), opisywany w literaturze jako zatrucie ARP , ARP spoofing lub ARP Poison Routing)

WYBRANE ASPEKTY KONTROLI WWW



Blokada plików mogącymi być potencjalnymi nośnikami wirusów, trojanów itp. oraz niektórych plików multimedialnych
– sprawdzanie i blokowanie rozszerzeń plików np: com, exe, pif, scr, .bat, .dll , .scr, vbs, vbe, vb, mp3, mpeg itp

Filtr antywirusowy – sprawdzanie pobieranych treści skanerem CLAMAV, kolejna weryfikacja na stanowisku rezydentnym skanerem NOD32 (podwójna ochrona antywirusowa od strony Internetu)



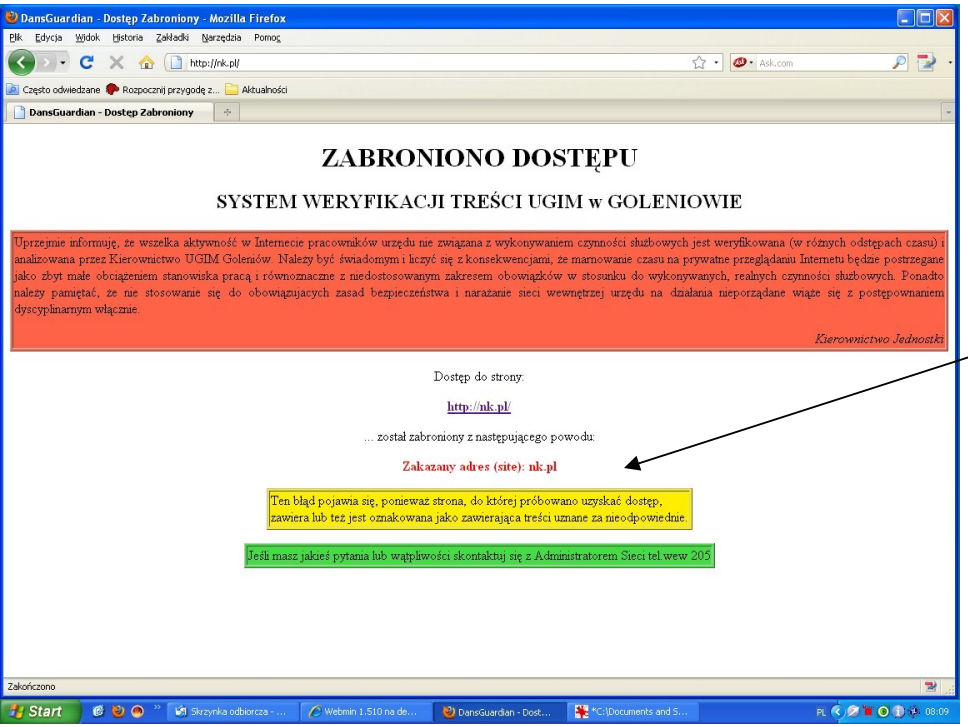
WYKAZ BLOKOWANYCH TYPÓW PLIKÓW

.ade # Microsoft Access project extension
.adp # Microsoft Access project
.bas # Microsoft Visual Basic class module
.bat # Batch file
.cab # Windows setup file
.chm # Compiled HTML Help file
.cmd # Microsoft Windows NT Command script
.com # Microsoft MS-DOS program
.cpl # Control Panel extension
.crt # Security certificate
.dll # Windows system file
.exe # Program
.hlp # Help file
.ini # Windows system file
.hta # HTML program
.inf # Setup Information
.ins # Internet Naming Service
.isp # Internet Communication settings
.lnk # Windows Shortcut
.mda # Microsoft Access add-in program
.mdb # Microsoft Access program
.mde # Microsoft Access MDE database
.mdt # Microsoft Access workgroup information
.mdw # Microsoft Access workgroup information
.mdz # Microsoft Access wizard program
.msc # Microsoft Common Console document
.msi # Microsoft Windows Installer package
.msp # Microsoft Windows Installer patch
.mst # Microsoft Visual Test source files
.pcd # Photo CD image, Microsoft Visual compiled script
.pif # Shortcut to MS-DOS program
.prf # Microsoft Outlook profile settings
.

reg # Windows registry entries
.scf # Windows Explorer command
.scr # Screen saver
.sct # Windows Script Component
.sh # Shell script
.shs # Shell Scrap object
.shb # Shell Scrap object
.sys # Windows system file
.url # Internet shortcut
.vb # VBScript file
.vbe # VBScript Encoded script file
.vbs # VBScript file
.vxd # Windows system file
.wsc # Windows Script Component
.wsf # Windows Script file
.wsh # Windows Script Host Settings file
.otf # Font file - can be used to instant reboot 2k and xp
.ops # Office XP settings
.dmg # Mac disk image
.smi # Mac self mounting disk image
.sit # Mac compressed file
.sea # Mac compressed file, self extracting
.bin # Mac binary compressed file
.hqx # Mac binhex encoded file
.mp3 # Music file
.mpeg # Movie file
.mpg # Movie file
.avi # Movie file
.iso # CD ISO image
.ogg # Music file
.wmf # Movie file
.bin # CD ISO image
.cue # CD ISO image

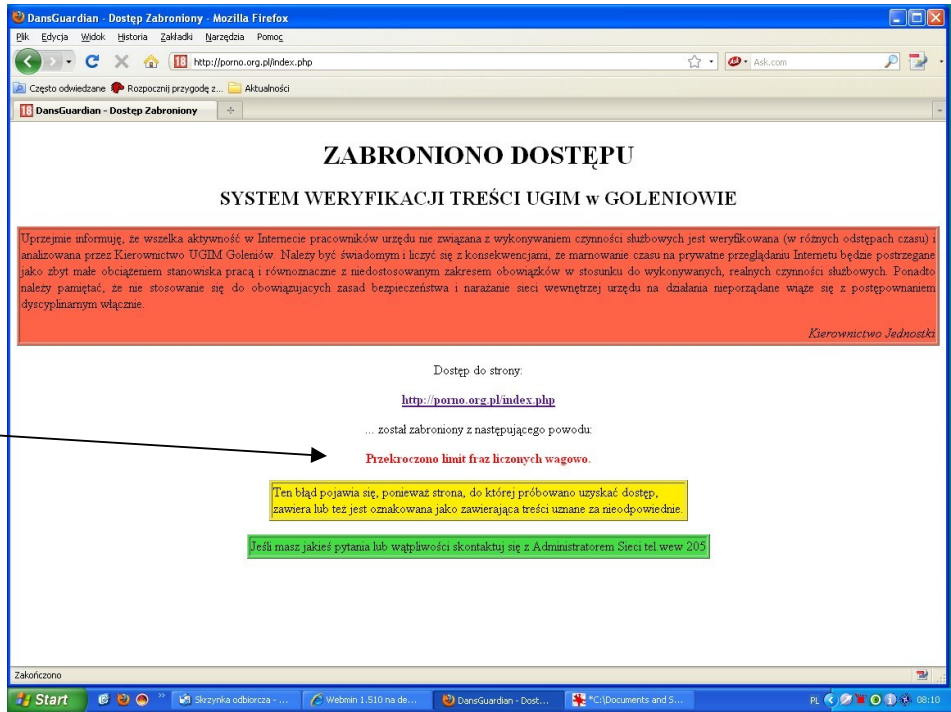
RENATTACH zależnie od konfiguracji wycina lub zmienia nazwy rozszerzeń załączników podlegające filtrowaniu i uznane za potencjalnych nosicieli wirusów: ADE, ADP, BAS, BAT, CHM, CMD, COM, CPL, CRT, EML, EXE, HLP, HTA, HTM, HTML, INF, INS, ISP, JS, JSE, LNK, MDB, MDE, MSC, MSH, MSI, MSP, MST, NWS, OCX, PCD, PIF, REG, SCR, SCT, SHB, SHS, URL, VB, VBE, VBS, WSC, WSF, WSH

WYBRANE ASPEKTY KONTROLI WWW

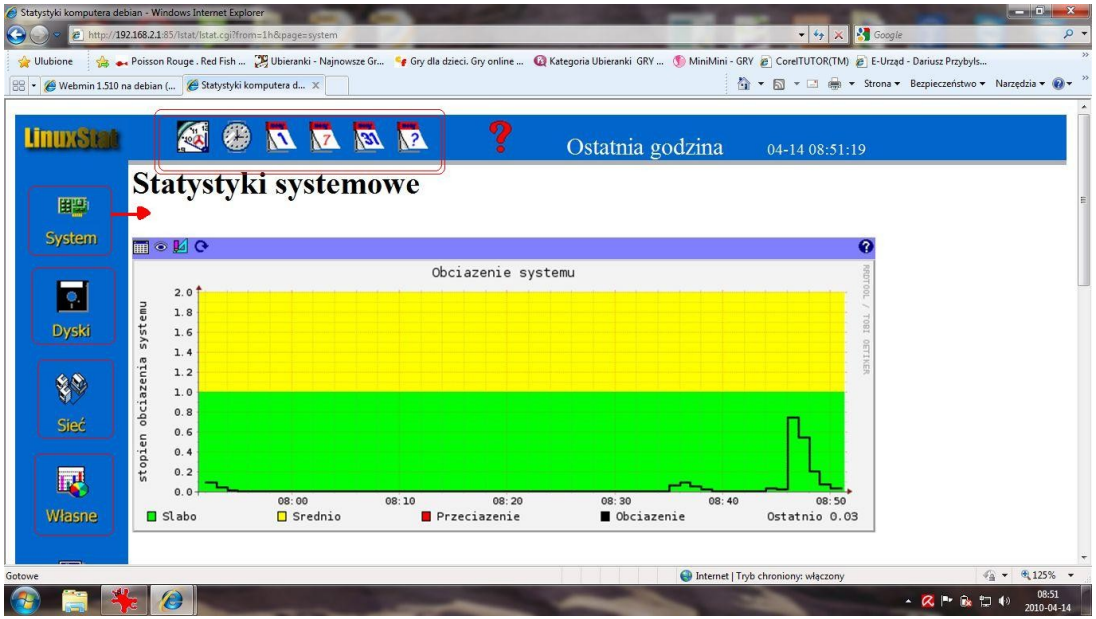


Blokada stron na podstawie tzw czarnych i białych list (na czarnej liście znajdują się strony np.: nasza-klasa.pl facebook.com itp., na białej np. gov.pl)

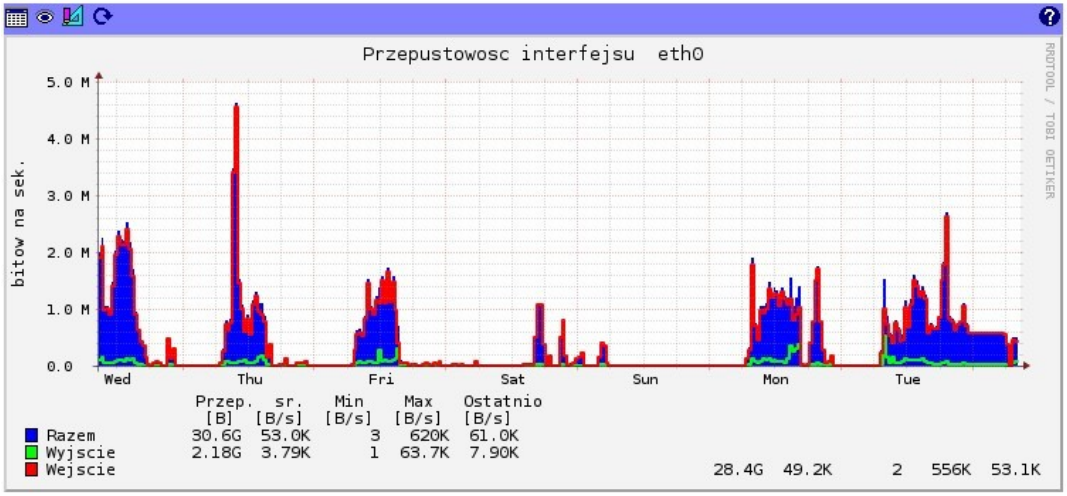
Kontrola zakazanych (np. pornograficznych) treści metodami słownikowymi
-słowniki polskie, angielskie, hiszpańskie, japońskie itp (zdarzają się fałszywe alarmy)
- > www.dansguardian.pl



WYBRANE ASPEKTY KONTROLI WYDAJNOŚCI



- Obciążenie systemu [%]
- Wykorzystanie procesora
- Wykorzystanie pamięci (100% na wykresie w podziale na RAM i SWAP)
- Użycie partycji dyskowych (stopień zajętości poszczególnych partycji)
- Użycie dysku (w podziale na zapis i odczyt)
- Przepustowość interfejsów sieciowych zarówno po stronie LAN i WAN (w układzie wyjście, wejście w dowolnych jednostkach: pakiet/s, bajt/s bit/s)



DOBRE PRAKTYKI

które warto uwzględnić przy projektowaniu prezentowanego rozwiązania

- wyłączenie zbędnych usług, rezygnacja z XWINDOWS (patrz: Windows Server 2008 Core)
- domyślna konfiguracja w jądrach pobranych z www.kernel.org powinna być jak najmniejsza, kompilacja jądra (usunięcie kompilatorów)
- wykonywać aktualizacje systemu apt-get update && apt-get upgrade
- podstawa to przemyślany, dobrze zbudowany NETFILTER (firewall z kontrolą stanu pakietu, poza dostępem do jawnie zadeklarowanych usług cały ruch powinien być logowany i zablokowany, domyślna polityka na wszystkich łańcuchach DROP)
- modyfikacja FSTAB (ustawienie flag nosuid, nodev, noexec i przemontowanie partycji)
- nie wystawiać usługi SSH na zewnątrz, a jeżeli już to poprzez np. technologię PORT KNOCKING, VPN (cert), zmodyfikować parametry sshd_config: PermitRootLogin, Protocol, Port, AllowUsers
- zastosować reguły SNORTa do ochrony warstwy aplikacji (np. wykorzystując mechanizm FWSNORT)
- testować rozwiązanie, stosować mocne hasła (nmap, tcpdump, John the Ripper, netstat itp)
- sprawdzać logi, okresowy audyt integralności (lastlog, tripwire –check, ps aux, faillog itp.)

ANALIZA PREZENTOWANEGO ROZWIZANIA:

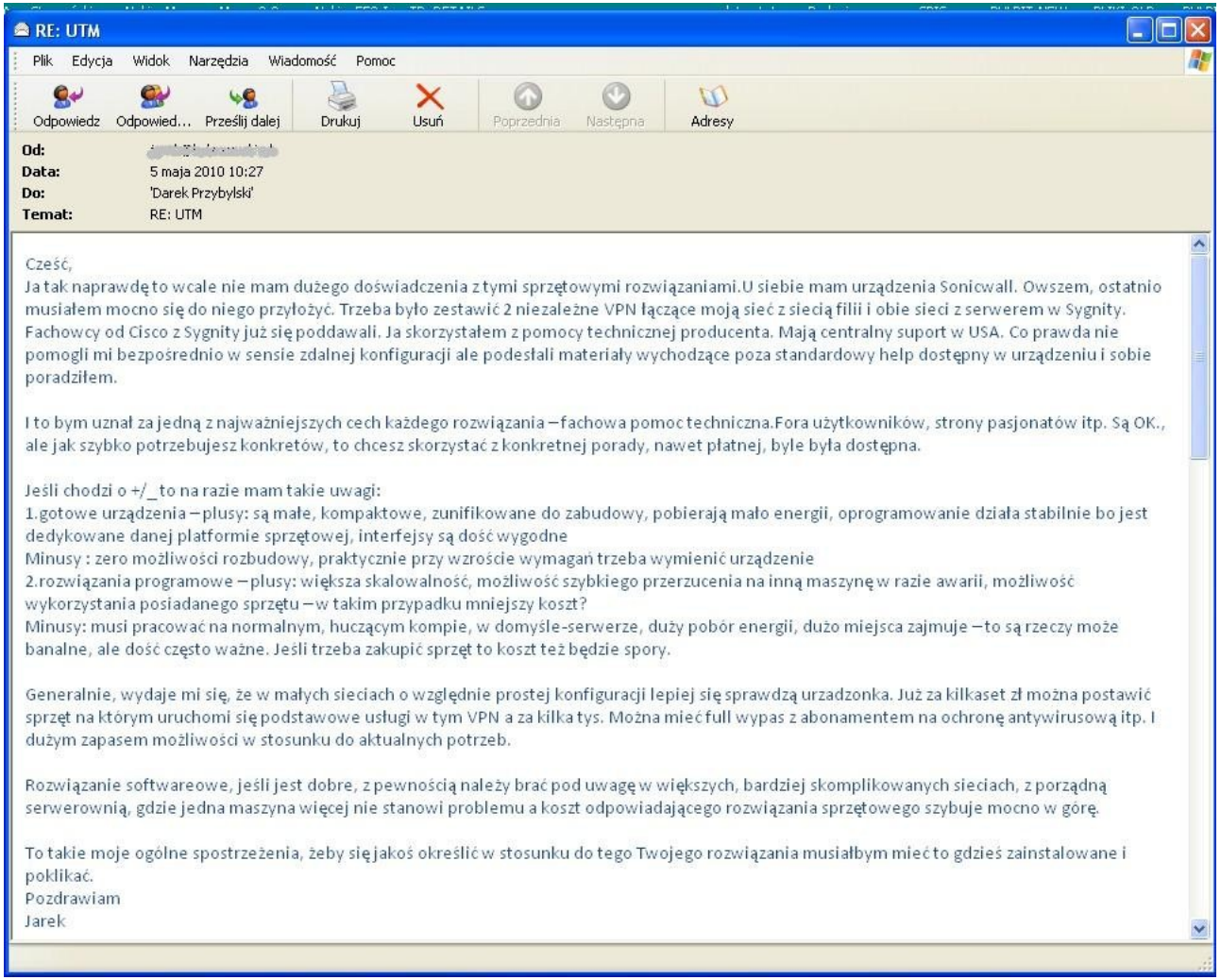
ZALETY:

- dobre rozwiązanie w odpowiednim czasie - byłem przed SOHO (Fortinet, Netasq)
- większa elastyczność i skalowalność rozwiązania (uszyte na miarę aktualnych potrzeb)
- większa kontrola i świadomość – jak to wszystko ma działać
- stabilność pracy software (ale też dużo zależy od sprzętu)
- szerokie wsparcie (google i wszystko jasne :-)
- cena (optymalizacja wydatków i potrzeb)
- edukacja (nauka, postawienie na rozwój)
- poczucie wolności (np. nie ma potrzeby pilnowania licencji – ilość, rodzaj itp)

WADY:

- wsparcie (czasami trudności, zużyty czas na poszukiwania może skutecznie zniechęcać)
- cena
- edukacja (dużo nauki kosztem np. braku czasu dla rodziny)
- stabilność pracy (większa podatność na spadki napięć niż wersje „box”)
- dobrej konfiguracji nie da się wyklikać (łatwość obsługi GUI)
- większe zużycie energii (zapewnienie skutecznego chłodzenia)

PRZYKŁAD NIEZALEŻNEJ OPINII:



RE: UTM

Plik Edycja Widok Narzędzia Wiadomość Pomoc

Odpowiedz Odpowied... Prześlij dalej Drukuj Usuń Poprzednia Następna Adresy

Od: [redacted]
Data: 5 maja 2010 10:27
Do: 'Darek Przybylski'
Temat: RE: UTM

Cześć,
Ja tak naprawdę to wcale nie mam dużego doświadczenia z tymi sprzętowymi rozwiązaniami.U siebie mam urządzenia Sonicwall. Owszem, ostatnio musiałem mocno się do niego przyłożyć. Trzeba było zestawić 2 niezależne VPN łączące moją sieć z siecią filii i obie sieci z serwerem w Sygnity. Fachowcy od Cisco z Sygnity już się poddawali. Ja skorzystałem z pomocy technicznej producenta. Mają centralny suport w USA. Co prawda nie pomogli mi bezpośrednio w sensie zdalnej konfiguracji ale podesłali materiały wychodzące poza standardowy help dostępny w urządzeniu i sobie poradziłem.

I to bym uznał za jedną z najważniejszych cech każdego rozwiązania – fachowa pomoc techniczna.Fora użytkowników, strony pasjonatów itp. Są OK., ale jak szybko potrzebujesz konkretów, to chcesz skorzystać z konkretnej porady, nawet płatnej, byle była dostępna.

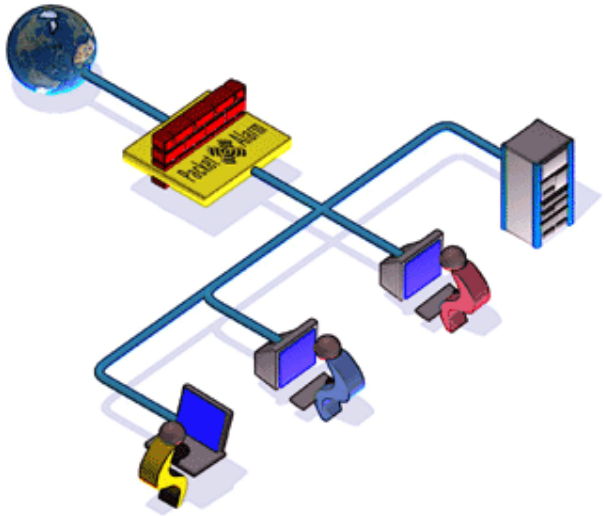
Jeśli chodzi o +/_ to na razie mam takie uwagi:
1.gotowe urządzenia – plusy: są małe, kompaktowe, zunifikowane do zabudowy, pobierają mało energii, oprogramowanie działa stabilnie bo jest dedykowane danej platformie sprzętowej, interfejsy są dość wygodne
Minusy : zero możliwości rozbudowy, praktycznie przy wzroście wymagań trzeba wymienić urządzenie
2.rozwiązania programowe – plusy: większa skalowalność, możliwość szybkiego przerzucenia na inną maszynę w razie awarii, możliwość wykorzystania posiadanego sprzętu – w takim przypadku mniejszy koszt?
Minusy: musi pracować na normalnym, huczącym kompie, w domyśle-serwerze, duży pobór energii, dużo miejsca zajmuje – to są rzeczy może banalne, ale dość często ważne. Jeśli trzeba zakupić sprzęt to koszt też będzie spory.

Generalnie, wydaje mi się, że w małych sieciach o względnie prostej konfiguracji lepiej się sprawdzą urzadzonka. Już za kilkaset zł można postawić sprzęt na którym uruchomi się podstawowe usługi w tym VPN a za kilka tys. Można mieć full wypas z abonamentem na ochronę antywirusową itp. I dużym zapasem możliwości w stosunku do aktualnych potrzeb.

Rozwiązanie softwareowe, jeśli jest dobre, z pewnością należy brać pod uwagę w większych, bardziej skomplikowanych sieciach, z porządną serwerownią, gdzie jedna maszyna więcej nie stanowi problemu a koszt odpowiadającego rozwiązania sprzętowego szybuje mocno w górę.

To takie moje ogólne spostrzeżenia, żeby się jakoś określić w stosunku do tego Twojego rozwiązania musiałbym mieć to gdzieś zainstalowane i poklikać.
Pozdrawiam
Jarek

ZAPRASZAM NA POKAZ WYBRANEGO ASPEKTU DZIAŁANIA SYSTEMU DEBIAN-UTM



DZIĘKUJĘ ZA UWAGĘ

Dariusz Przybylski

Kontakt: **darekp@goleniow.pl**

Portal: **http://www.goleniow.pl**

PrvWebSite: **http://debian.type.pl**

GOLENIÓW MIASTO HANZEATYCKIE
PRAWA MIEJSKIE OD 1268 r.

SZCZEGÓLNE PODZIĘKOWANIA DLA TYCH PANÓW:

Richard Stallman

Linus Torvalds

Ian Murdock

Eben Moglen

Grzegorz Fiuk

Michael Rash