

*ALWIL Software*

# *avast32*

*Firewall Edition - MS Proxy/ISA modul*



# Obsah

1	Úvod	5
2	Instalace	7
2.1	Požadavky na vybavení počítače	7
2.2	Instalujeme	7
3	První kroky	9
4	Konfigurace rezidentní úlohy	11
4.1	Stránka „Úloha“	11
4.2	Stránka „Typ“	12
4.3	Stránka „Rezidentní“	12
4.4	Stránka „MS Proxy/ISA“	13
4.5	Stránka „Testování“	13
4.6	Stránka „HTTP“	14
4.7	Stránka „FTP“	15
4.8	Stránka „Výjimky“	15
4.9	Stránka „Logování“	16
4.10	Stránka „Plánování“	17
5	Použití Avastu MS Proxy/ISA Server	19
5.1	Důsledky používání antivirové ochrany na proxy	19
5.2	Testování velkých souborů	19
5.3	Virové reporty	21
5.4	Složka s odvírovanými objekty	23
5.5	Zasílání poplašných zpráv a další nastavení	23

# Seznam obrázků

4.1	Stránka „Úloha“	11
4.2	Stránka „Typ“	12
4.3	Stránka „Rezidentní“	12
4.4	Stránka „MS Proxy/ISA“	13
4.5	Stránka „Testování“	13
4.6	Stránka „HTTP“	14
4.7	Stránka „FTP“	15
4.8	Stránka „Výjimky“	16
4.9	Stránka „Logování“	16
4.10	Stránka „Plánování“	17
5.1	Report, který Avast zasílá klientovi v případě nalezení viru	22

# 1 Úvod

Vážený zákazníku, blahopřejeme Vám k zakoupení antivirového prostředku AVAST32 3.0 Firewall Edition, jednoho z nejlepších programů ve své třídě. Doufáme, že budete s našim produktem spokojeni a že se Vám s ním bude příjemně pracovat.

AVAST32 3.0 Firewall Edition představuje úplnou antivirovou ochranu vybraných firewallů. Konkrétně jde o firewally podporující protokol CVP (např. CheckPoint Firewall 1), a firewally a proxy servery postavené na technologiích firmy Microsoft (MS Proxy Server 2 a MS ISA Server 2000). Tento dokument popisuje používání modulu pro ochranu firewallů od Microsoftu; popis modulu pro ochranu firewallů založených na CVP najdete v samostatném dokumentu.

V případě jakýchkoli problémů s programem či nejasností kontaktujte svého prodejce nebo firmu ALWIL Trade. Jejich pracovníci Vám rádi a ochotně poradí.

Příjemnou a viry nerušenou práci na Vašem počítači Vám přejí pracovníci firmy ALWIL Software.



## 2 Instalace

AVAST32 pro MS Proxy/ISA je nová verze antivirového systému AVAST vytvořeného speciálně k antivirové ochraně MS Proxy Serveru 2.x a MS ISA Serveru 2000. Je dodáván jako součást antivirové suity Avast32, Firewall Edition. Jádro programu je určeno pro počítač s Windows NT/2000/XP Serverem a MS Proxy/ISA Serverem. Konfiguraci ale můžete provádět z jakékoli síťové stanice s Windows 95/98 nebo Windows NT4/2000/XP. Program se skládá ze dvou částí:

- první je serverová, která provádí samotné testování a která je nainstalována přímo na počítač, na kterém běží Proxy/ISA Server,
- druhá je klientská, což je vlastně jenom přídatný modul do běžné instalace programu AVAST32 verze 3.0, který Vám umožní vzdálenou administraci serverové části.

AVAST32, Firewall Edition vyžaduje, abyste již měli nainstalován AVAST32 verze 3.0. Před započítím instalace se ujistěte, že je AVAST32 verze 3.0 instalován, a to jak na serveru, tak na klientské stanici, ze které budete provádět správu.

### 2.1 Požadavky na vybavení počítače

K tomu, aby mohl být AVAST32 úspěšně nainstalován na Váš počítač a poté i bezchybně pracovat, je nutné, aby Váš počítačový systém splňoval několik základních požadavků.

Pro instalaci na server:

- procesor Pentium nebo vyšší
- 64 MB paměti RAM
- Windows NT 4.0 Server nebo Windows 2000/XP Server
- MS Proxy Server 2 nebo MS ISA Server 2000 nebo vyšší
- Pokud používáte MS Proxy Server na IIS 4 (tzn. Windows NT), pak musí být instalován i hotfix opravující chybu v IIS (více informací viz <http://support.microsoft.com/support/kb/articles/q>

Pro instalaci jako klient

- počítač splňující požadavky na běh programu AVAST32 verze 3.0

### 2.2 Instalujeme

<To be supplied>



## 3 První kroky

Po úspěšně dokončené instalaci a restartu Windows můžete ihned nové funkce programu AVAST32 začít používat.

**Veškeré funkce AVAST32 3.0 Firewall Edition jsou ovládány prostřednictvím úlohy, vytvořené v rozšířeném ovládaní programu AVAST32 3.0.**

Pro spuštění programu AVAST32 klikněte na tlačítko „Start“, pak zvolte složku „Programy“, dále nalistujte složku „AVAST32 Antivirus“ a v této složce klikněte na ikonu „AVAST32“.

Po spuštění programu se ujistěte, zda pracujete v rozšířeném ovládaní. Pokud pracujete v jednoduchém ovládaní klikněte levým tlačítkem myši na ikonu v levém horním rohu programu a vyberte rozšířené ovládaní ze zobrazeného menu.

Podrobný popis vytváření úloh pro ochranu MS Proxy/ISA Serveru se nachází v následujících kapitolách.



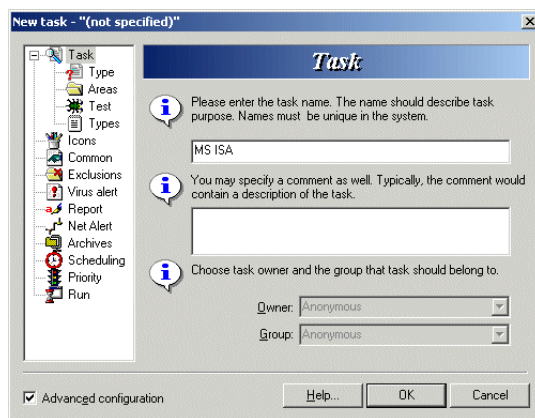
## 4 Konfigurace rezidentní úlohy

V následujícím textu budou popsány jednotlivé stránky s ovládacími prvky, které se týkají nastavení úlohy na rezidentní ochranu MS Proxy/ISA serveru. Obrázky zobrazené u jednotlivých stránek ukazují stránky při použití stromu při konfiguraci úlohy. Při použití průvodce nebo záložkového seznamu je podoba okna jiná, ale ovládací prvky a jejich význam jsou však tytéž.

Pro rezidentní ochranu můžete použít jak standardní úlohu „Rezidentní ochrana“ (po příslušné modifikaci, popsané níže - konkrétně zahrnutí poskytovatele MS Proxy/ISA), tak i zcela novou, vámi definovanou úlohu. Tu vytvoříte následujícím postupem: na stránce „Úlohy“ rozšířeného ovládacího panelu klikněte pravým tlačítkem myši na seznamu úloh nebo klikněte na nabídku „Úloha“ v hlavním menu programu, a ze zobrazeného menu vyberte položku „Vytvořit novou ...“. Zobrazí se dialog pro vytvoření nové úlohy.

### 4.1 Stránka „Úloha“

Na stránce „Úloha“ (obr. 4.1) je programem požadováno vložení jména vytvářené úlohy. To by mělo být co možná nejvýstižnější a nemělo by být kvůli přehlednosti shodné s některým jménem již existující úlohy. Jestliže nezadáte žádné jméno, nebude nová úloha vytvořena. Implicitně textové pole obsahuje „(nespecifikováno)“.



4.1 Stránka „Úloha“

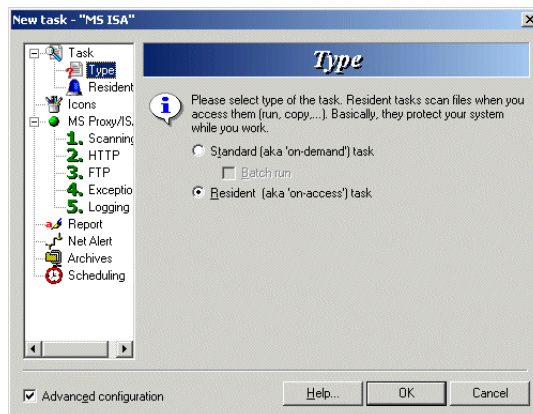
Do dalšího textového pole je možné napsat komentář úlohy stručně popisující činnost úlohy. Tato položka může zůstat prázdná.

Pomocí kombinovaného pole „Skupina“ nastavte skupinu, do které úloha patří.

Pomocí kombinovaného pole „Vlastník“ nastavte vlastníka, kterému úloha patří.

## 4.2 Stránka „Typ“

Na stránce „Typ“ (obr. 4.2) zvolte pomocí přepínače „Rezidentní“ vytváření rezidentní úlohy

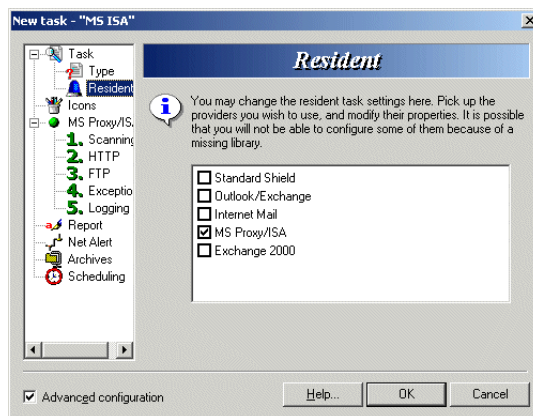


4.2 Stránka „Typ“

Po zvolení přepínače se automaticky změní možnosti dalšího nastavení úlohy.

## 4.3 Stránka „Rezidentní“

Stránka „Rezidentní“ (obr. 4.3) obsahuje seznam dostupných poskytovatelů rezidentní ochrany.



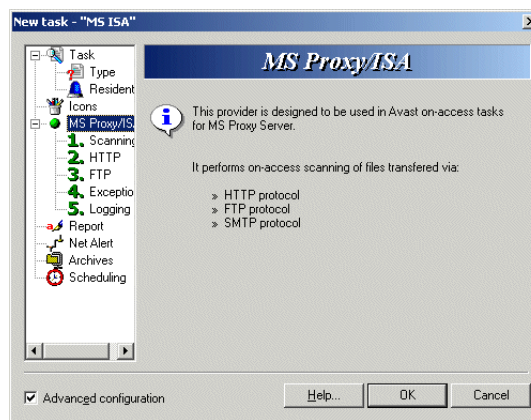
4.3 Stránka „Rezidentní“

Počet položek uvedených v seznamu je závislý na verzi programu, kterou používáte, a též na počtu instalovaných komponent. Na této stránce zaškrtněte zaškrťávací pole „MS Proxy/ISA“. U ostatních položek seznamu můžete (ovšem nemusíte) zaškrtnutí zrušit, pokud nechcete dané poskytovatele používat. Například plně podporovaná konfigurace je i ta, kde na stejném počítači používáte jak poskytovatele pro MS Proxy/ISA, tak i Standardní štít.

Jedinou výjimkou z tohoto pravidla je poskytovatel Internet Mail - jeho používání na serverech není doporučeno. Důvodem je skutečnost, že tento poskytovatel pro svou činnost používá jednoduchý SMTP/POP3 server. Protože pro tyto služby jsou přiděleny pevná čísla TCP portů (u SMTP jde o 25, v případě POP3 je to 110), je možné na jednom počítači provozovat nejvýše jeden takový server. Na serveru však většinou běží „opravdový“ SMTP server, takže by při použití poskytovatele Internet Mail docházelo ke kolizím při společném používání TCP portu.

#### 4.4 Stránka „MS Proxy/ISA“

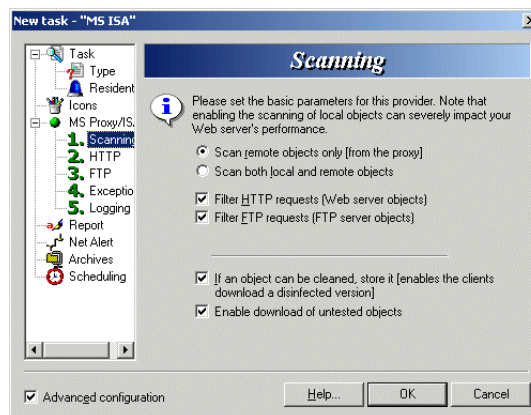
Tato stránka zobrazuje pouze informace o zvoleném poskytovateli rezidentní ochrany.



4.4 Stránka „MS Proxy/ISA“

#### 4.5 Stránka „Testování“

Stránka „Testování“ (obr. 4.5) umožňuje uživateli nastavit základní parametry poskytovatele.



4.5 Stránka „Testování“

Pomocí zaškrťovacího pole „Testovat pouze vzdálené objekty (z proxy)“ určíte, že poskytovatel bude testovat pouze objekty přicházejících ze vzdálených serverů (tzn. neumístěných na lokálním IIS serveru, je-li nainstalován). Toto pole je standardně zaškrtnuto. Chcete-li testovat jak vzdálené, tak i lokální objekty, zaškrtněte „Testovat jak lokální, tak i vzdálené objekty“.

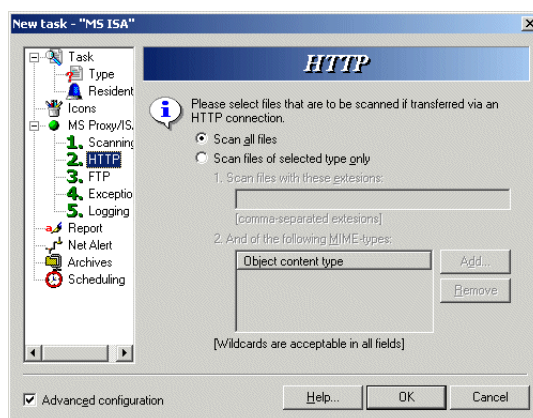
Zaškrtnutím zaškrťovacího pole „Filtrovat HTTP spojení (objekty z Web serverů)“ zajistíte testování objektů uložených na HTTP serverech. Analogicky, zvolení parametru „Filtrovat FTP spojení (objekty z FTP serverů)“ způsobí, že Avast bude testovat objekty přicházející ze serverů FTP. Implicitně jsou obě tato pole zaškrtnuta.

Přepínačem „Lze-li objekt odvirovat, uložit jej (umožňuje klientům stáhnout vyčištěnou verzi)“ se zapíná možnost čištění infikovaných objektů (je-li to možné, tzn. např. v případě makrovirů). Je-li toto pole zaškrtnuto (standardně je) a lze-li zavirovaný objekt vyčistit, uživatel, který se pokoušel objekt stáhnout, dostane možnost si stáhnout vyčištěnou verzi.

Konečně volba „Umožnit stažení netestovaných objektů“ určuje, zda má Avast umožňovat projití přes proxy i těm objektům, které nelze z nějakých důvodů otestovat (např. archívy komprimované s heslem).

## 4.6 Stránka „HTTP“

Stránka „HTTP“ (obr. 4.6) umožňuje uživateli nastavit parametry testování souborů stahovaných pomocí HTTP protokolu. Tato nastavení budou efektivní pouze v případě, že je na stánce Testování zapnuta volba „Filtrovat HTTP spojení (objekty z Web serverů)“.



4.6 Stránka „HTTP“

Zaškrtnutím pole „Testovat všechny soubory“ zvolíte, že testování se bude provádět pro soubory všech typů (mimo těch, jež jsou uvedeny na stránce Výjimky, viz dále). Chcete-li testovat pouze některé typy souborů, zaškrtněte pole „Testovat pouze soubory zvoleného typu“ a v některém z následujících polí přesně specifikujte typy, které se mají do testování zařadit.

V poli „1. Testovat soubory s těmito příponami“ můžete zapsat seznam přípon souborů, které se mají testovat. Přípony odděluje čárkou. Pro specifikaci lze použít i zástupné znaky ? a \*. Příkladem může být zapsání hodnoty

EXE,COM,HT\*,DO?,VBS,JS

která určuje, že testovat se budou soubory s příponami EXE, COM, VBS, a JS, dále pak soubory, jejichž přípona začíná znaky HT (tzn. např. HTM, HTML apod.) a též soubory, které začínají znaky DO a jejichž délka je tři znaky (např. DOC, DOT apod.)

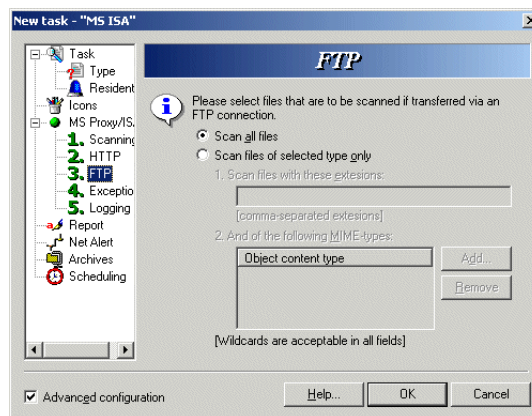
Typy souborů, které se mají testovat, lze určit i jinak, a to pomocí jejich MIME typu (content-type). K tomu slouží pole „2. A těchto MIME-typů“, do kterého můžete vložit všechny MIME typy, které mají být testovány. Použití zástupných znaků je opět přípustné. Příklad:

```
application/*
text/html
```

tzn. testování HTML souborů a všech „aplikačních“ souborů, např. obecných binárních (application/octet-stream).

## 4.7 Stránka „FTP“

Stránka „FTP“ (obr. 4.7) umožňuje uživateli nastavit parametry testování souborů stahovaných pomocí protokolu FTP. Tato nastavení budou efektivní pouze v případě, že je na stránce Testování zapnuta volba „Filtrovat FTP spojení (objekty z FTP serverů)“.

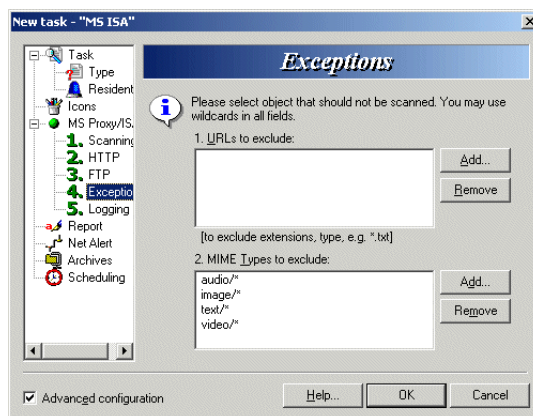


4.7 Stránka „FTP“

Nastavení parametrů pro FTP je zcela stejné jako nastavení parametrů pro HTTP. Více informací viz stránka HTTP.

## 4.8 Stránka „Výjimky“

Na stránce „Výjimky“ (obr. 4.8) můžete nastavit typy souborů, které mají být z testování vyloučeny. To je užitečné zejména pro zvýšení rychlosti, neboť testování všech souborů může mít neblahý vliv na celkovou odezvu serveru.



#### 4.8 Stránka „Výjimky“

Výjimky se opět definují pomocí typů souborů, a to podobně jako v případě HTTP a FTP pomocí URL a MIME-typu souborů. Podrobnější popis, stejně jako příklady MIME-typů lze nalézt v popisu stránky HTTP.

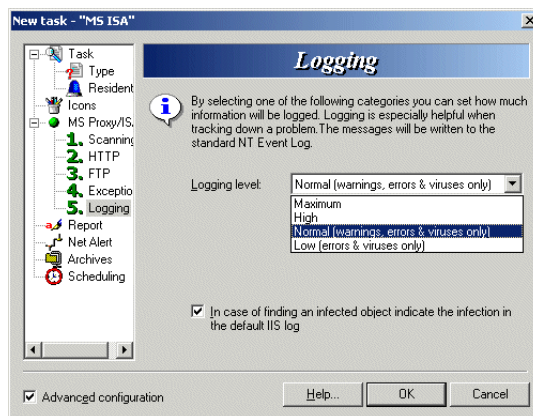
Pole „1. Z testování vyřadit následující URL:“ je implicitně prázdné; pole „2. Z testování vyřadit následující MIME typy:“ standardně obsahuje hodnoty

audio/\*  
 image/\*  
 text/\*  
 video/\*

tzn. z testování jsou implicitně vyřazeny obrázky, textové soubory a též zvukové a video soubory.

#### 4.9 Stránka „Logování“

Na stránce „Logování“ (obr. 4.9) je možné nastavit úroveň, s jakou bude poskytovatel MS Proxy/ISA zapisovat logovací zprávy. Logování je užitečné zejména při řešení nejrůznějších problémů.



#### 4.9 Stránka „Logování“

Volba se provádí pomocí pole „Úroveň logování:“. K dispozici jsou čtyři úrovně:

- Maximální
- Vysoká
- Normální (pouze varování, chyby a viry)
- Nízká (pouze varování a chyby)

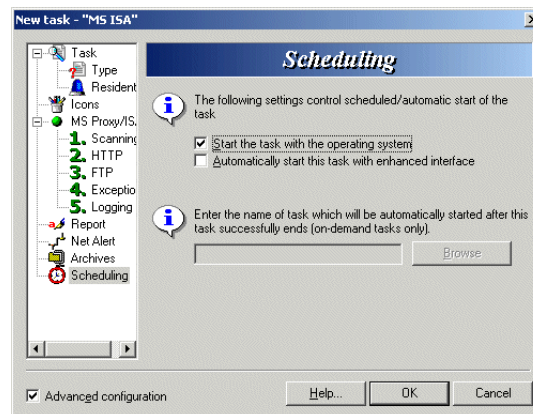
Maximální úroveň zapíná velmi důkladné logování. Doporučeno pouze při hledání příčin problémů, neboť může rychle vést k zaplnění logu. Vysoká úroveň vypouští některé ze zpráv, zapisovaných na maximální úrovni, stejně však ponechává i množství zpráv, které mají spíše informativní charakter. Úroveň Normální (standardně nastavena) způsobuje, že logovat se budou pouze varování, chyby a zprávy o nalezení virů. Konečně úroveň Nízká se od Normální liší tím, že hlášení o nalezení viru nejsou do logu zaznamenávány.

Všechny zprávy se zapisují do aplikačního NT Event Logu.

V dolní části okna se nachází ještě volba „V případě nalezení infikovaného objektu indikovat virus i prostřednictvím implicitního IIS logu“, jejíž zapnutí má za následek, že do IIS logu bude v případě pokusu o download infikovaného souboru jako status operace zapsána speciální hodnota 88448844 hex.

## 4.10 Stránka „Plánování“

Stránka „Plánování“ (obr. 4.10) obsahuje nastavení automatického spouštění a ukončování úloh.



4.10 Stránka „Plánování“

Zaškrtnutím pole „Spustit úlohu s operačním systémem“ uživatel sdělí programu, že vytvářená úloha má být spuštěna ihned po přihlášení uživatele. Implicitně není pole zaškrtnuto.

Zaškrťovací pole „Spustit úlohu při startu programu AVAST32“ zapíná spouštění úlohy automaticky po startu programu AVAST32. Spouštění úlohy zároveň s programem AVAST32 je implicitně vypnuto.



## 5 Použití Avastu MS Proxy/ISA Server

Tato kapitola podrobně popisuje praktické aspekty používání Avastu na MS Proxy a ISA serverech.

### 5.1 Důsledky používání antivirové ochrany na proxy

### 5.2 Testování velkých souborů

Jak již bylo řečeno, pro každý antivir na proxy serveru je důležité se co nejlépe vypořádat s velkými soubory. Důvodem je skutečnost, že aby mohl být nějaký soubor řádně otestován, musí ho mít antivir celý. Nejbezpečnější by bylo, že by antivir ze žádného objektu, který ještě nebyl otestován, neposlal klientovi ani bajt. Tím by se dokonale předešlo nákaze ve všech případech. Problém ale spočívá v tom, že doba, za kterou může být v některých případech testování provedeno, může být velmi dlouhá: antivir na proxy serveru musí k sobě soubor nejprve stáhnout, a je-li velký, nebo je-li spojení pomalé, může taková operace trvat třeba celé hodiny. Protože však ke klientovi žádná data nepřicházejí, může dojít k nejrůznějším timeoutům, nebo prostě dojde trpělivost uživateli a download sám přeruší.

Proto má většina kvalitních antivirových programů mechanismy, jak těmto situacím předcházet. Avast obsahuje takové mechanismy hned dva:

- Předcházení timeoutů na straně klienta
- Speciální zpracování dlouhých souborů.

#### Předcházení timeoutů na straně klienta

K timeoutům (= vypršení časového limitu) dochází zpravidla v případě, že klientská aplikace nedostane ze strany serveru za nějakou určitou časovou periodu žádnou zprávu. Klient potom neví, zda server ještě vůbec odpovídá, resp. zda jeho konkrétní TCP spojení se serverem je stále platné. A protože většina protokolů postavených na TCP (HTTP nevyjímaje) není tzv. full-duplex, tzn. neumožňuje současnou komunikaci v obou směrech, klient v podstatě nemá k dispozici jiné prostředky, než jednoduše čekat (samozřejmě, může se serverem navázat nové TCP spojení, ale pomocí něj nemůže nijak ovlivnit spojení původní).

Je třeba si uvědomit, že v případě, že by Avast na proxy serveru neobsahoval žádné speciální mechanismy, by k timeoutům docházelo potenciálně velmi často, neboť doba, za kterou může Avast otestovaný soubor klientovi odeslat, v podstatě odpovídá době jeho stahování ze vzdáleného zdroje, a může být tudíž velmi dlouhá.

Řešení tohoto problému však není příliš složité: protokol HTTP našťastí nabízí jistou metodu, jak klientovi posílat data, aniž by tato data byla pro něj příliš relevantní (alespoň v jistém stadiu HTTP požadavku). Konkrétně jde o tzv. HTTP headery (záhlaví).

Podávejme se trochu blížeji na typický HTTP požadavek na stažení souboru. V nejjednodušším případě to vypadá takto (S: značí komunikaci ze strany serveru, C: komunikaci ze strany klienta)

```
C: GET http://www.alwil.com/index.html
S: 200 HTTP/1.1 OK
Content-type: text/html
Content-Length: 13492
<zde jsou další HTTP headery>
```

<Zde následuje obsah stánky index.html>

Klient tedy požádá proxy server o stažení stánky <http://www.alwil.com/index.html>. Server pak vrátí klientovi určitý blok informací tvořený HTTP headery, prázdným řádkem a dále samotným obsahem požadovaného objektu.

Speifikace HTTP přímo určuje, že všechny HTTP headery, kterým klient nerozumí, má ignorovat (tz. nijak dále nezpracovávat). A to je vlastně vše, co Avast potřebuje k tomu, aby mohl účinně implementovat mechanismus předcházení timeoutů. Konkrétně jde o to, že Avast čas od času (typicky jednou za 20 vteřin, což je čas, za který rozhodně žádný klientský program netimeoutuje) klientovi zašle jeden HTTP header, konkrétně

```
X-Antivirus-Status: Scanning
```

Klient s největší pravděpodobností tomuto headeru nebude rozumět, a proto jej bude ignorovat. Bude však vědět, že komunikace se serverem je stále „živá“ a spojení nadále funguje (narozdíl od implicitní situace, kdy by se server vůbec neozval až do okamžiku, kdy by měl celý objekt k sobě stažený a oskenovaný).

### Speciální zpracování dlouhých souborů

Zatímco posílání redundantních HTTP headerů ve většině případů zamezí timeoutům ze strany klienta, rozhodně nezamezí frustraci ze strany stahujícího uživatele, který ani po půl hodině od započetí downloadu nevidí ze souboru stažený ani bajt.

Proto byla do Avastu implementována jistá vlastnost, jejímž cílem je takovým situacím předcházet. Vychází z heuristického (ovšem ne nutně vždy platného) poznatku, že viry jsou zpravidla obsaženy pouze v menších souborech (řádově do 100KB). Avast pro MS Proxy/ISA Server proto nyní rozlišuje soubory podle jejich velikosti na dva typy:

- *Malé* - tyto soubory jsou nejčastějšími zdroji nákazy a proto se z nich nikdy klientovi neodešle ani bajt, dokud není celý soubor řádně otestován. Jelikož jde ale o soubory malé, klient zpravidla nezaznamená významnější časové prodlevy ve stahování.
- *Velké* - tyto soubory obsahují viry (hypoteticky) méně často, a proto s nimi lze pracovat trochu jinak. Konkrétně tak, že Avast začne obsah souboru normálně posílat klientovi, takže ten jakoby vesele downloaduje, jako kdyby na proxy žádný antivir nebyl. Před odesláním posledních paketu (v době, kdy Avast má k dispozici soubor již celý) je ale soubor otestován, a pokud je zjištěno, že obsahuje virus, je TCP spojení s klientem okamžitě ukončeno. Klient tedy dostane soubor nekompletní, zpravidla tedy „poškozený“ a nepoužitelný (v ideálním případě by Avast klientovi dal vědět, že soubor je špatný a že jej má zahodit. Něco takového ale bohužel HTTP protokol nepodporuje, jediné, co může Avast udělat, je prostě spojení s klientem ihned ukončit).

Jde pochopitelně o částečné riziko, ale necháme na Vás, abyste se rozhodli, zda chcete tuto vlastnost používat (příjemnější stahování za cenu jistého bezpečnostního rizika), a též jaká by měla být hranice mezi „malými“ a „velkými“ soubory. Instalace Avastu je implicitně nastavena tak, že malý soubor je ten, jehož velikost je menší než 200KB. Toto nastavení lze změnit prostřednictvím souboru Avast32.ini umístěného v adresáři <Avast32>\Data. V sekci „MS Proxy/ISA“ (bez uvozovek, jméno sekce v hranatých

závorkách; tato sekce pravděpodobně nebude v souboru zatím vůbec uvedena, proto ji tam budete muset sami vepsat) stačí nastavit hodnotu

MinKBLargeObject=Xxx

kde Xxx určuje minimální počet KB pro to, aby soubor s touto velikostí byl již považován za velký a byl pro něj tedy použit zmíněný mechanismus (implicitně je tedy MinKBLargeObject=200, a tato hodnota platí i v případě, že klíč MinKBLargeObject není v INI souboru vůbec uveden). Nastavíte-li tuto hodnotu na -1, nebude technika rozlišování malých-velkých souboru používána a všechny soubory se budou zpracovávat jako malé (tzn. méně příjemně pro stahovatele, ale bezpečně).

### 5.3 Virové reporty

V případě, že Avast pro MS Proxy/ISA server nalezne v nějakém souboru virus, a není-li tento soubor zpracováván jako „velký“ (tzn. jeho obsah není průběžně klientovi zasílán, viz sekce Testování velkých souborů), dostane klient místo požadovaného souboru od Avastu úhledný report o tom, že soubor je zavirován a že viry škodí zdraví.

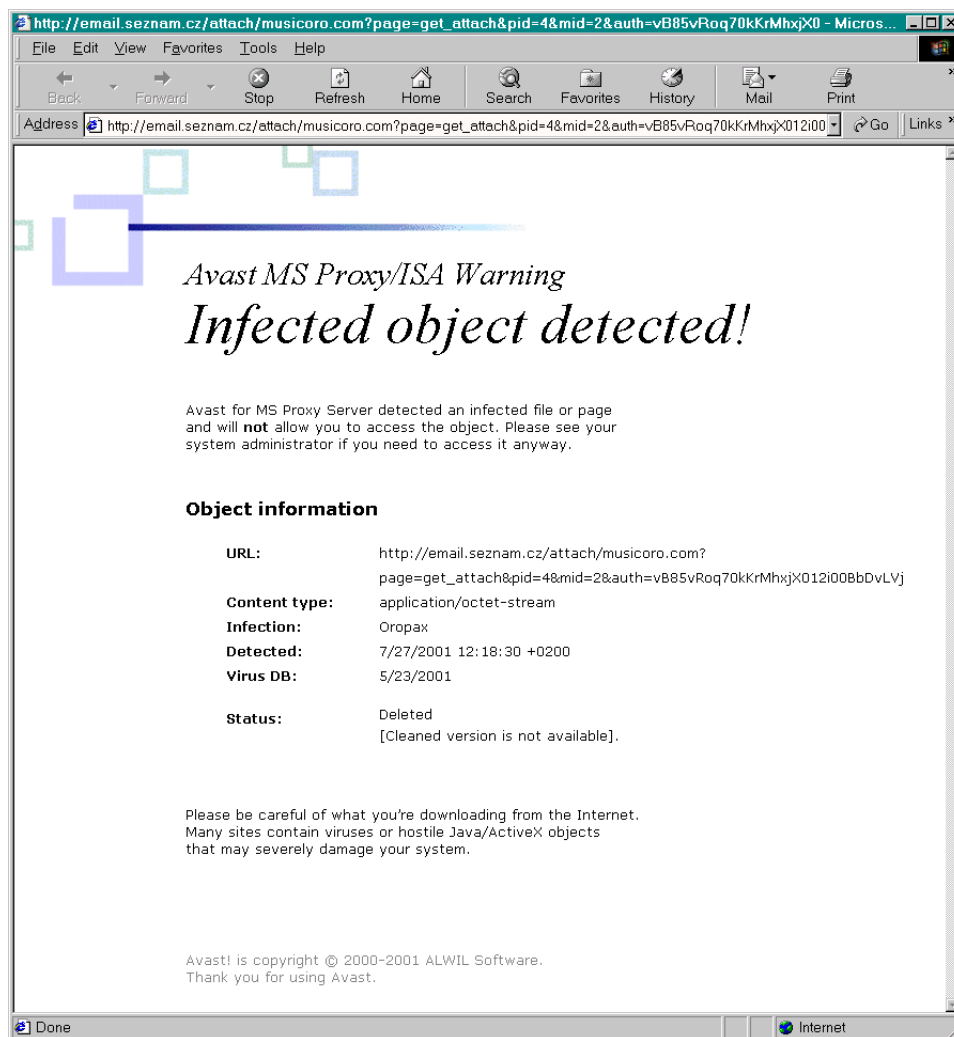
Tento report obsahuje dynamické informace, které jsou generovány v Avastem v závislosti na situaci. Standardně je report posílán v angličtině, protože ve většině případů Češi rozumí anglicky, ale bohužel ne naopak.

Report lze však plně přizpůsobit Vašim představám. Chcete-li report, který Avast posílá změnit, stačí zeditovat soubor AvPxyInf.htm, umístěný v adresáři <Avast32>\Data. Jde o zcela normální HTML soubor, takže pro jeho editaci lze použít libovolný nástroj k těmto účelům určený.

Dynamická data jsou v souboru samozřejmě nahrazována ad hoc při odesílání reportu Avastem. Pro jejich umístění se v souboru AvPxyInf.htm používají tzv. šablony, neboli klíčová slova, která jsou za běhu programu dynamicky nahrazována skutečnými údaji. Pro soubor AvPxyInf.htm Avast rozeznává následující šablony:

- %URL% - URL zavirovaného objektu.
- %TYPE% - MIME-typ (content-type) zavirovaného objektu.
- %TIMEDATE% - datum a čas nalezení viru.
- %VIRUS% - jméno viru.
- %CLEANFILE% - URL, z něhož lze v případě vyčištění viru stáhnout odvírovanou verzi souboru.
- %STATUS% - informace, zda byl soubor vyčištěn či nikoli. Používá hodnoty deklarativních šablon %CLEANED=Xxx% (vyčištěn) a %DELETED=Xxx% (nevyčištěn), viz dále.
- %MOREINFO% - další informace zobrazené v závislosti na tom, zda soubor byl vyčištěn či nikoliv. Používá hodnoty deklarativních šablon %CLEANINFO=Xxx% (vyčištěn) a %DELINFO=Xxx% (nevyčištěn), viz dále.
- %VPS% - datum a verze VPS souboru (virové databáze), který byl použit pro testování.

Kromě těchto jednoduchých šablon, jejichž výskyt v souboru je prostě nahrazen skutečnými daty, jsou ještě podporovány tzv. *deklarativní šablony*, které předdefinovávají určité hodnoty a jejichž výskyt je z konečného reportu zasílaného klientovi vždy odstraněn. Z tohoto důvodu mohou být v souboru umístěny na libovolném místě, třeba i za značkou </HTML>, určující konec HTML textu. Avast pro MS Proxy/ISA rozeznává následující deklarativní šablony:



### 5.1 Report, který Avast zasílá klientovi v případě nalezení viru

- **%DELETED=Hodnota%** - hodnota určuje textový řetězec, jímž bude nahrazena šablona **%STATUS%** v případě, že virus nemohl být ze souboru vyčištěn.
- **%CLEANED=Hodnota%** - hodnota určuje textový řetězec, jímž bude nahrazena šablona **%STATUS%** v případě, že virus byl ze souboru úspěšně vyčištěn.
- **%CLEANINFO=Hodnota%** - hodnota určuje textový řetězec, jímž bude nahrazena šablona **%MOREINFO%** v případě, že virus byl ze souboru úspěšně vyčištěn. Lze v ní s výhodou použít jednoduchou šablonu **%CLEANFILE%**.
- **%DELINFO=Hodnota%** - hodnota určuje textový řetězec, jímž bude nahrazena šablona **%MOREINFO%** v případě, že virus nemohl být ze souboru vyčištěn.

Příklad: do souboru AvPxyInf.htm můžete např. zapsat řádek

**%CLEANINFO=**Click <a href=„%CLEANFILE%“>here</a> to download the cleaned version.%

který způsobí, že šablona **%MOREINFO%** bude v případě možnosti vyčištění souboru nahrazena textem, na který půjde poklepat a stáhnout odvírovanou verzi souboru.

### Použití odkazů v souboru AvPxyInf.htm

Chcete-li v souboru AvPxyInf.htm použít nějaké odkazy na lokální objekty, např. na HTML stránku zahrnout obrázky, postup není tak přípomačarý jako v případě normálního HTML dokumentu. Problém spočívá v tom, že odkazy na lokální objekty se na HTML stránku zapisují s lokální cestou (např. /images/banner.gif) relativní ke kořeni web serveru; na proxy však žádný web vůbec nemusí existovat (např. v případě ISA Serveru), resp. může existovat, ale nemusí být používán. Proto je potřeba při vkládání odkazů na lokální objekty do souboru AvPxyInf.htm postupovat podle následujících pravidel:

- Všechny objekty, na které se bude stránka AvPxyInf.htm odkazovat, zkopírovat do adresáře <Avast32>\Data\HtmlData. Tento adresář je určen výhradně k těmto účelům a je společně s <Avast32>\Data\PxyCache jediným adresářem, ke kterému budou mít HTTP klienti prostřednictvím Avastu přístup.
- Do AvPxyInf.htm uvést jako URL odkazu speciální hodnotu ve tvaru  
http://avast-data-files. /  
<jméno\_souboru>, tzn. např.  
<imgsrc = http : //avast - data - files./banner.gif>.

Tímto postupem zajistíte, že Avast správně na proxy serveru rozezná požadavek na stažení svého vlastního souboru a klienta korektně sám obslouží.

Jako příklad použití všech výše uvedených pravidel a šablon můžete použít implicitní verzi souboru AvPxyInf.htm, která je v adresáři <Avast32>\Data vytvořena instalačním programem.

## 5.4 Složka s odvírovanými objekty

V konfiguraci poskytovatele MS Proxy/ISA lze na stránce Testování nastavit, aby bylo možno stahovat odvírované verze infikovaných objektů (volba „*Lze-li objekt odvírovat, uložit jej (umožňuje klientům stáhnout vyčištěnou verzi)*“). Toto nastavení je dokonce implicitně zapnuté.

Za tímto účelem poskytovatel na disku používá speciální adresář, konkrétně <Avast32>\Data\PxyCache, do kterého jsou všechny odvírované objekty, které Avast během své práce nashromáždil, zapisovány. Kromě toho tento adresář ještě obsahuje speciální soubor *index.dat*, ve kterém jsou zapsány informace o jednotlivých objektech v adresáři uskladněných. Tento soubor má binární formát a je spravován výhradně Avastem.

Práce programu je optimalizována v tom smyslu, že zbytečně neukládá víc verzí stejného souboru, a tím šetří místo na disku.

## 5.5 Zasílání poplašných zpráv a další nastavení

Pro efektivní použití Avastu na proxy serveru se doporučuje provést některá další nastavení. Typicky jde o zasílání poplašných zpráv administrátorovi v případě nalezení viru (např. pomocí SMTP protokolu). Tím má administrátor dobrý přehled o tom, kolik virů je na úrovni proxy serveru zachyceno. Detailnější informace o tom, co je to za virus a kdo a kdy se jej pokoušel stáhnout nalezne pak v event logu.

Další užitečnou volbou je nastavení prohlížení pakovaných souborů (např. ZIP). Mnoho souboru je v dnešní době komprimováno a aby mohl Avast tyto archívy procházet, musí to mít zapnuto.

V neposlední řadě může být užitečné zapnout generování tzv. zprávy, tzn. souboru, do kterého se podrobně zapisují jména všech objektů, které Avast během své činnosti otestoval, a též výsledek testování (zavirován x nezavirován, a v případě infekce i jméno viru).

Všechny tyto volby, tzn. poplašné zprávy, testování pakovaných souborů a generování zprávy se zapíná editací rezidentní úlohy, obsahující poskytovatele MS Proxy/ISA (naprosto stejně, jako u kterékoli jiné úlohy Avastu). Podrobný popis lze nalézt v manuálu k programu Avast32.

Rovněž je velmi podstatné zajistit pravidelnou aktualizaci virové databáze. V Avastu existuje několik způsobů aktualizace, můžete použít např. systém inkrementální aktualizace *iAVS*, který typicky virovou databázi stahuje přímo z Internetu (pro pravidelné spouštění použijte příkaz „Naplánovaná *iAVS*“ ve vlastnostech počítače v rozšířeném ovládní Avastu), nebo systém podnikové aktualizace pomocí souborů *.VPU*. Podrobný popis lze opět nalézt v manuálu ke standardnímu Avastu.