SquiVi2 Readme

Steffen Schoch

1 Inhalt

1 Inhalt....2
2 Für Ungeduldige....3
3 Die Idee hinter SquiVi2....3
4 Was ist SquiVi2?....3
5 Was ist SquiVi2 nicht?....4
6 Vorraussetzungen....4
7 Funktionsweise....4
7.1 Aller Anfang....5
7.2 Firewall mit Proxy....5
7.3 Integration von SquiVi2 in Squid....5
8 Installation....7
8.1 Vorraussetzungen....7
8.2 squid.conf....7
8.2.1 confpath....7
8.2.2 squiviscan....7
8.2.3 squiduser....7
8.2.4 squidgroup....7
8.2.5 wgetbin....7
8.2.6 wgetusedata....7
8.2.7 waitforauthdata....8
8.2.8 wgetcookie....8
8.2.9 wgetuseragent....8
8.2.10 wgetreferer....8
8.2.11 wgetauthpass....8
8.2.12 wgetargs....8
8.2.13 downloaddir....8
8.2.14 showoutput....8
8.2.15 longoutput....8
8.2.16 redirectftp....9
8.2.17 usenewwin....9
8.2.18 backnewwin....9
8.2.19 refreshtime....9
8.2.20 authlifetime....9
8.2.21 lang....9
8.2.22 squivicss....9
8.2.23 logfaility....9
8.2.24 loglevel....9
8.2.25 limitlevel....9
8.2.26 limitarchiv....10
8.2.27 limitsize....10
8.2.28 limitfiles....10
8.2.29 packer....10
8.2.30 defaultaction....10
8.2.31 squivicgi....10
8.2.32 noscan Abschnitte....10
8.2.33 scan Abschnitte....11
8.2.34 scanner Abschnitte....11

8.3 squivi.cgi/squiviauth.cgi....11
8.4 squid....11
9 Die einzelnen Komponenten....11
9.1 squivi.pl....11
9.2 squivicleanup.pl....12
9.3 squivihead.pl....12
9.4 squivihead2.pl....12
9.5 squivilistdb.pl....12
9.6 squiviplex.pl....12
9.7 squiviscan.pl....13
9.8 squivi.cgi....13
9.9 squiviauth.cgi....13
9.10 squivi.css....13
10 Statistik....13
11 Bekannte Fehler....13
11.1 Fehler....13
11.2 Workarounds und behobene Fehler....13
12 Kontakt....14
13 Anhang....14
13.1 Abbildungsverzeichnis....14
13.2 GPL....14

2 Für Ungeduldige...

... empfehle ich einen kurzen Blick in das Kapitel 'Funktionsweise' zu werfen und Anschließend in 'Installation'. Falls es Probleme gibt kann hier immer noch nachgelesen werden ☺.

3 Die Idee hinter SquiVi2

Die Idee zu SquiVi kam mir damals als ich auf der Suche nach einer Virenscanner-Schnittstelle für Squid war. Das was es damals gab hat mich nicht wirklich überzeugt da zum Teil Fehler aufgetreten sind die man einem Kunden nicht zumuten kann.

Aus diesen zum Teil unschönen Erfahrungen und eigenen Wünschen und Ideen ist SquiVi 1 entstanden. An und für sich ein schönes Produkt – jedoch zeigte hier der Praxiseinsatz einige Grenzen auf. Z.B. gibt es da draußen Webserver die in der URL ungültige Zeichen benutzen und die konnten SquiVi außer Tritt bringen. Ebenfalls gab es sehr selten Probleme nach Abschluss des Downloads an die übertragene Datei zu gelangen.

Diese Probleme und der Wunsch nach noch besseren Konfigurationsmöglichkeiten hat mich dazu bewegt eine zweite Version von SquiVi zu erstellen: SquiVi2.

Für alle die es interessiert: SquiVi steht übrigens für 'Squid-Virus'.

4 Was ist SquiVi2?

- SquiVi2 ist zunächst ein leistungsstarker Redirector der in Squid integriert werden kann. Hierbei kann nach allen übergebenen Daten gefiltert werden und zusätzlich noch der Mime-Type angefordert werden.
- Als spezielle Erweiterung kann eine Datei über ein weiteres Tool auf dem Server gespeichert werden. Anschließend wird der Inhalt von Archiven ausgepackt und nach Viren durchsucht.
- Neue Archiv-Formate können über die Konfigurationsdatei eingebunden werden.
- Es kann jeder gängige Virenscanner eingebunden werden der über die Befehlszeile bedient werden kann.

- Über diesen Vorgang wird der User über eine Statusseite auf dem laufenden gehalten und hat jederzeit genaue Informationen über den Fortschritt.
- Eine Vielzahl von Einstellungen können in der Konfiguration vorgenommen werden.
- Schon einmal angeforderte Dateien werden von der lokalen Platte gezogen und nicht noch einmal aus dem Internet.
- SquiVi2 ist unter der GPL veröffentlicht und somit fallen keine Lizenzkosten an (je nachdem welcher Virenscanner eingesetzt werden soll fallen für diesen durch dessen Lizenz zusätzliche Kosten an).
- SquiVi2 ist eine perfekte Ergänzung für die bereits vorhandne Virenschutz-Strategie!

5 Was ist SquiVi2 nicht?

- Die Lösung alle Deiner Probleme (zumindest was Viren betrifft). Dies ist garantiert nicht der Fall. Bis die Viren durch einen Scanner gefunden werden haben diese bereits eine gewisse Verbreitung. Ebenfalls gibt es mehrere Wege um einen Virus zu übertragen, z.B. Disketten, CDs usw. Man sollte dieses Tool also wirklich nur als (sinnvolle?) Ergänzung zur bereits vorhanden Virenschutz-Strategie sehen.

6 Vorraussetzungen

Folgende Vorraussetzungen für den Einsatz von SquiVi2 müssen gegeben sein:

- Perl (entwickelt unter Perl 5.8) und folgende Perl-Module (einige davon sind bereits bei Perl enthalten, andere können von der Adresse cpan.perl.org im Internet geholt werden):
  - Config::General
  - Data::Dumper
  - Fcntl
  - File::Basename
  - File::Copy
  - File::Path
  - Getopt::Std
  - IO::Handle
  - IPC::Open2
  - LWP
    - LWP::MediaTypes
    - LWP::Simple
    - LWP::UserAgent
  - Storable
  - URI::Escape
  - Unix::Syslog
- Squid (Proxyserver)
- Webserver mit CGI-Schnittstelle (getestet unter Apache)
- wget (zu finden unter http://www.gnu.org/software/wget/wget.html)
- Virenscanner. Davon wird die Befehlszeilenversion benötigt (z.B. www.clamav.net).
- Optional:
  - Diverse Dekomprimierungsprogramme wie z.B. tar, gunzip, bunzip, unzip, ...

7 Funktionsweise

In diesem Abschnitt will ich anhand von Skizzen die Funktionsweise von SquiVi2 zeigen und das Zusammenspiel der einzelnen Module erklären.

7.1 Aller Anfang...

Wie sooft beginnt alles damit, dass ein Benutzer eine Datei oder ein Programm aus dem Internet laden will.

Hierzu wird er seinen Browser nehmen und die entsprechende Datei aus dem Internet anfordern wie in Abbildung 1 gezeigt.

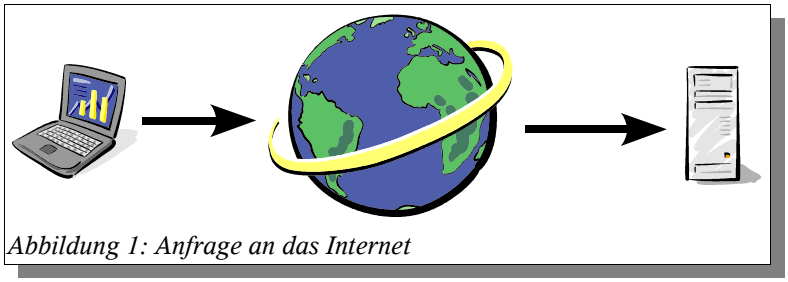


Abbildung 1: Anfrage an das Internet

Die gewünschte Datei wird direkt auf den lokalen Arbeitsplatz kopiert – ohne dass der User weiß, ob nun ein Virus in der Datei enthalten ist oder nicht...

7.2 Firewall mit Proxy

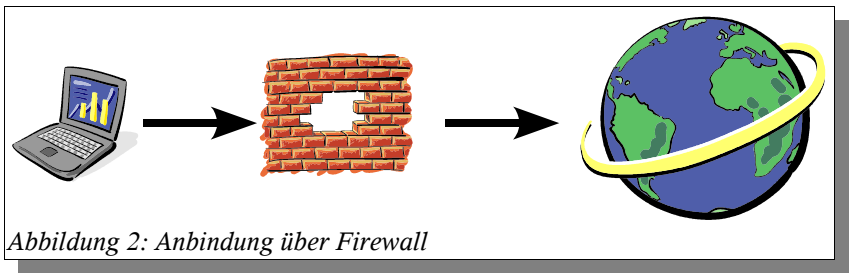


Abbildung 2: Anbindung über Firewall

Unternehmen, aber auch immer Privatanwender setzen zwischen dem Arbeitsplatz und dem Internet eine Firewall (Abbildung 2). Diese soll ungebetene Gäste aus dem Internet vor einem möglichen Eindringen abhalten.

Die Funktionalität der Firewall wird oftmals durch den zusätzlichen Einsatz von Proxys erhöht. Ein Proxy kann z.B. die angeforderten Daten auf der Festplatte zwischen speichern, damit diese zu einem späteren Zeitpunkt nicht noch einmal angefordert werden müssen. Eine Ergänzung zu Proxys sind Content-Filter. Diese Filter können z.B. den Zugriff auf bestimmte Webseiten wie z.B. Pornographie, Werbung und weitere verbieten.

Genau an dieser Stelle setzt SquiVi2 an: bei Viren in Downloads handelt es sich ja genau genommen ebenfalls um 'Content'; und genau dieser 'Content' wird gefiltert. In diesem Fall von einem Virenscanner...



SquiVi2 braucht als Proxy-Server squid (www.squid-cache.org) und kann über dessen Redirector-Schnittstelle integriert werden. Auf die Installation von squid wird in dieser Dokumentation nicht eingegangen. Hierzu gibt es genügend andere hervorragende Quellen im Internet.

7.3 Integration von SquiVi2 in Squid

SquiVi2 wird in Squid über dessen Redirector-Schnittstelle integriert. Da Bilder mehr sagen als tausend Worte erkläre ich den genauen Ablauf einer anhand der folgenden Abbildung 3.

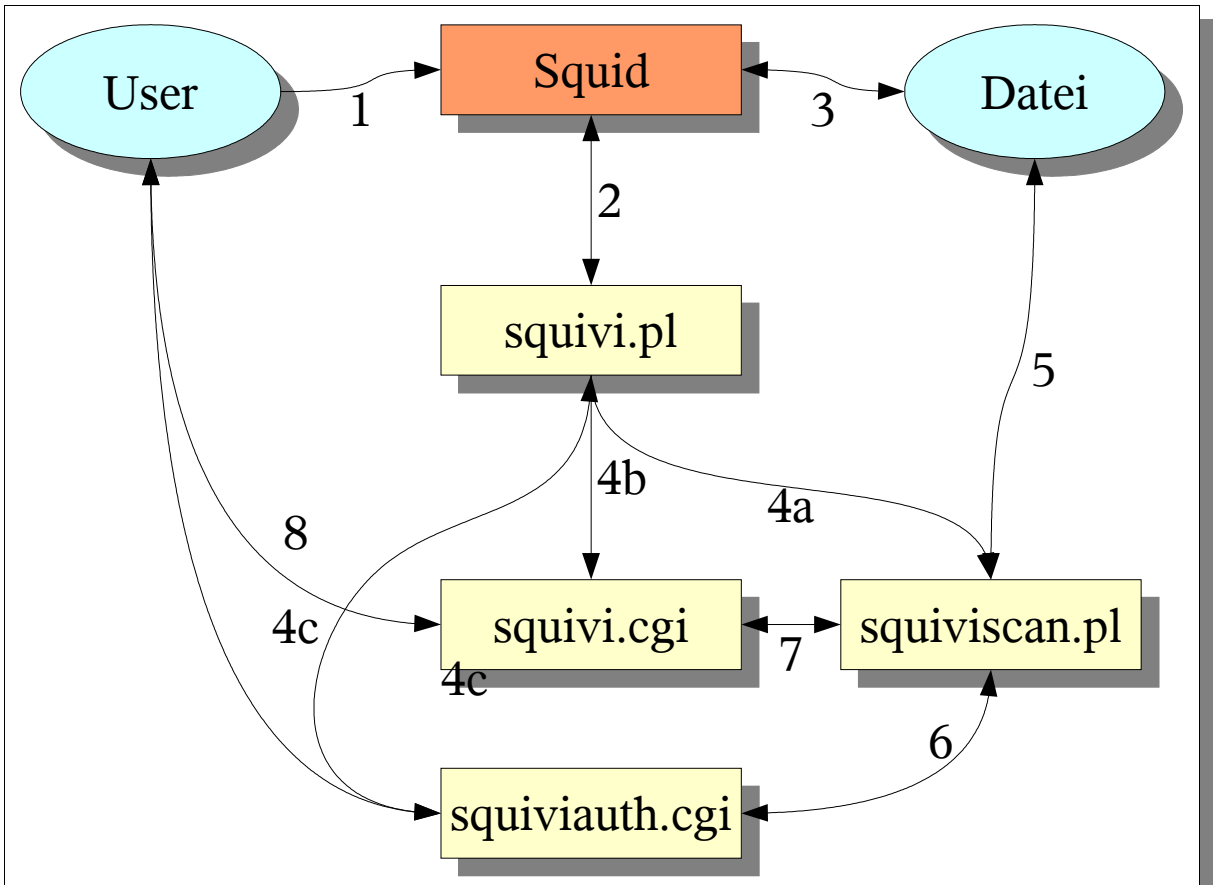


Abbildung 3: Integration in squid

1	Als erstes ist wieder unser User von vorhin da. Auch dieses mal will er wieder eine Datei aus dem Internet haben und richtet die entsprechende Anfrage an squid.
2	Über die Redirector-Schnittstelle wird squivi.pl aufgerufen. Anhand seiner Regeln entscheidet squivi.pl ob die Datei nach Viren durchsucht werden muss oder nicht. Falls nicht wird ist kein Eingriff nötig, es folgt im Anschluss Schritt 3. Für den Fall, dass nach Viren gesucht werden soll folgen die Schritte 4a und 4b.
3	Squid holt die Datei aus dem Internet und liefert Sie an den User aus. Mit der Auslieferung der Datei ist der Vorgang beendet.
4a	squiviscan.pl wird im Hintergrund von squivi.pl gestartet.
4b	Anstelle der eigentlichen Datei erhält der User zunächst die Ansicht auf squivi.cgi. Hier wird er über den Fortschritt des Downloads informiert. Die Umleitung auf squivi.cgi geschieht über die Redirector-Schnittstelle.
4c (2x)	Sollte Authentifizierung (HTTP) erforderlich sein wird jedoch zuerst squiviauth.cgi gestartet und Benutzername und Passwort durch Eingabe vom User ermittelt.
5	squiviscan.pl holt die Datei über wget aus dem Internet, dekomprimiert ggf. Archive und sucht nach Viren.
6	Falls Authentifizierung erforderlich ist werden die Daten von squiviauth.cgi an squiviscan.pl übermittelt.

7	squivi.cgi informiert sich permanent über den Fortschritt von squiviscan.pl und stellt diese Informationen für den User entsprechend zusammen.
8	Falls kein Virus gefunden wurde bietet squivi.cgi die Datei zum Download an.



Damit squivi.cgi funktioniert wird ein Webserver mit CGI-Schnittstelle (z.B. Apache; www.apache.org) benötigt. Auf dessen Konfiguration wird hier ebenfalls nicht weiter eingegangen.

8 Installation

In diesem Abschnitt wird die Konfiguration von SquiVi2 gezeigt.

8.1 Vorraussetzungen

Für die Installation von SquiVi2 muss Squid, ein Webserver z.B. Apache, mindestens ein Virenscanner und die Internetanbindung bereits eingerichtet sein. Auf deren Konfiguration wird hier, wie bereits erwähnt, nicht eingegangen.

8.2 squid.conf

Über die Datei squivi.conf werden die Einstellungen für SquiVi2 vorgenommen. Diese Datei ist ausführlich kommentiert. Jetzt ist wahrscheinlich ein guter Zeitpunkt um den Inhalt dieser Datei einmal durchzulesen.

In den nächsten Abschnitten werden alle Einstellungen kurz erklärt. Die Reihenfolge orientiert sich an der Ordnung in der Beispielkonfiguration.

8.2.1 confpath

Der Pfad zu eben dieser Konfigurationsdatei.

8.2.2 squiviscan

Der Pfad zu squiviscan.pl.

8.2.3 squiduser

Der User mit dem Squid gestartet wird.

8.2.4 squidgroup

Die Gruppe mit der Squid gestartet wird.

8.2.5 wgetbin

Der Pfad zu wget.

8.2.6 wgetusedata

Ist diese Option auf 1 gesetzt speichert squivi.cgi beim ersten Aufruf Informationen wie den Referer, den UserAgent und Cookies. Diese Daten werden dann von squiviscan.pl über wget an den jeweiligen Webserver eins zu eins weitergeleitet.

Für alle wo das unklar war: diese Header-Informationen gibt's natürlich nur bei HTTP Übertragungen.

8.2.7 waitforauthdata

Dies ist die Anzahl der Sekunden die squiviscan.pl wartet um die Authentifizierungsinformationen zu erhalten. Sollte der User innerhalb dieser Zeit keine gültigen Daten eingeben wird der Vorgang abgebrochen.

Um die geforderte Datei dennoch zu erhalten ist ein Neustart des Downloads nötig.

8.2.8 wgetcookie

Dies ist die Option mit der bei wget ein Cookie gesetzt werden kann.

8.2.9 wgetuseragent

Analog für den UserAgent.

8.2.10 wgetreferer

Und natürlich noch für den Referer.

8.2.11 wgetauthpass

Mit diesen Optionen werden Benutzername und Passwort für die Authentifizierung (HTTP) übertragen.

8.2.12 wgetargs

Optionale weitere Argumente für wget. Mehrere Zeilen dieses Schlüsselwortes werden zu einer Zeile zusammengesetzt. Ich empfehle mindestens folgende Argumente: `-N -S -t 1 --passive-ftp --retr-symlinks.`

Für alle Optionen lese bitte die Dokumentation von wget.



Normalerweise sollten die wget Einstellungen aus der Beispielkonfiguration für die meisten Anwender völlig ausreichend sein.

8.2.13 downloaddir

In diesem Verzeichnis legt SquiVi2 die Downloads ab.

Der User der SquiVi2 startet, also der User unter dem Squid ausgeführt wird, benötigt Schreibrechte in diesem Verzeichnis. Leserechte werden vom Webserver benötigt, schreibrechte nur für die Datei .authdata (diese wird erst bei Bedarf erstellt).

Dieses Verzeichnis sollte regelmäßig aufgeräumt werden. Der Inhalt darf jedoch nicht einfach gelöscht werden um Inkonsistenzen zu vermeiden, sondern sollte über das Tool `squivicleanup.pl` entfernt werden. Siehe hierzu Kapitel 9.2.

8.2.14 showoutput

Falls 1 erzeugt squivi.cgi Ausgaben über den Fortschritt. Falls 0 werden keinerlei Ausgaben erzeugt.

8.2.15 longoutput

Auch bei dieser Option kann wieder 1 oder 0 gesetzt werden. Falls 1 wird anstelle der kurzen Zusammenfassung eine ausführlicher Bericht über die einzelnen Vorgänge erzeugt.

8.2.16 redirectftp

Einer der getesteten Browser (der von MS) hatte ein Problem bei der Darstellung von der Statusseite bei einer FTP-Verbindung. Dieses Problem kann durch diese Option umgangen werden. Sobald aktiviert werden alle Verbindungen erstmals auf http://<...> umgeleitet bevor die erste Statusausgabe beginnt.

8.2.17 usenewwin

Falls `redirectftp` gesetzt ist, kann mit dieser Option der Fortschrittsbericht in einem neuen Fenster geöffnet werden.

8.2.18 backnewwin

Falls `usenewwin` gesetzt ist kann mit `backnewwin` auf die vorherige Seite zurück gesprungen werden. 0 schaltet dieses Feature ab, alle anderen Werte werden als Wartezeit bis zum Aufruf interpretiert.



Achtung: Bei einigen „Browser-Webseiten-Kombinationen“ kann diese Funktion eine Endlosschleife verursachen. Dies passiert z.B. dann, wenn history.back() auf eine Weiterleitung verweist. Ich empfehle deshalb diesen Wert auf '0' zu setzen.

8.2.19 refreshtime

Nach dieser Anzahl von Sekunden lädt sich die Statusseite neu um den Fortschritt aufzuzeigen.

8.2.20 authlifetime

Nach dieser Anzahl von Sekunden ohne Zugriff auf die Authentifizierungsinformationen werden diese als ungültig angesehen und vom User nochmals abgefragt. Siehe hierzu auch 8.2.7 waitforauthdata.

8.2.21 lang

An dieser Stelle kann die Sprache des Frontends angegeben werden. Möglichkeiten sind im Verzeichnis `lang` enthalten.

Falls das Frontend in eine andere Sprache übersetzt werden soll kann eine Datei aus dem Ordner `lang` kopiert werden und der Inhalt übersetzt werden. Wer möchte kann mir diese Datei dann zukommen lassen, ich werde diese im Paket veröffentlichen.

8.2.22 squivicss

Die Adresse aus Sicht des Webservers zur Datei squivi.css.

8.2.23 logfaility

Die Syslog Facility unter der die Statusmeldungen eingetragen werden soll. Falls unsicher einfach so lassen.

8.2.24 loglevel

Gibt an wie viele Daten protokolliert werden sollen. 1 wenige Informationen, 9 einfach alles. Empfohlen ist der Wert 2.

8.2.25 limitlevel

Squiviscan.pl holt die gewünschte Datei aus dem Internet. Anschließend wird geprüft, ob ein Archiv enthalten ist. Falls dies der Fall ist wird der Inhalt ausgepackt und in diesem nach weiteren Archiven gesucht. Bei jedem dieser Durchläufe erhöht sich der Level um eins.

`limitlevel` gibt an wie oft nach Archiven gesucht werden soll. Falls die Anzahl der Suchdurchläufe diesen Wert überschreitet wird mit einem Fehler abgebrochen.

8.2.26 limitarchiv

Diese Anzahl legt fest wie viele Unterarchive maximal in dem Download enthalten sein dürfen.

8.2.27 limitsize

Hiermit wird die maximale Größe des Downloads angegeben (also Inhalt der Archive zzgl. der Archive selbst).

8.2.28 limitfiles

Analog zur Größe die Anzahl der Dateien.

8.2.29 packer

```
<packer tar>
  extension = tar
  bin = /bin/tar
  args = xvf
</packer>
```

Dieses Beispiel zeigt die Definition des Packers tar. Hinter Packer steht ein symbolischer Name der beliebig gewählt werden kann. Der Punkt extension gibt die Dateieindung an, bin den Pfad zum Programm und args die optionalen Argumente die zum auspacken benötigt werden.

Vor dem ersten Start von SquiVi sollten alle Packerangaben geprüft und angepasst werden. Ebenfalls sollten weitere Packer hinzugefügt werden falls diese benötigt werden sollten (z.B. jar, arc, compress usw.)

8.2.30 defaultaction

Falls SquiVi2 keine Aussage darüber macht ob gescannt werden soll oder nicht, wird diese Option gewählt. Sie sollte immer auf `noscan` gesetzt sein.

8.2.31 squivicgi

Der URL zu squivi.cgi.

8.2.32 noscan Abschnitte

Diese Abschnitte definieren die Regeln für Downloads die nicht gescannt werden sollen.

```
<noscan template>
  url = eine regex
  method = eine regex
  auth = eine regex
  host = eine regex
  action = noscan
  action = redirect  http://irgendwo.de/test.cgi?url=<url>&host=<host>&auth=<auth>&method=<method>
</noscan>
```

Wie bei dem Packer Abschnitt hat der Name hinter noscan nur symbolischen Charakter. Die Angabe der Werte url, method, auth und host sind optional, es sollte jedoch mindestens einer vorhanden sein. Hinter dem = muss ein regulärer Ausdruck stehen der gegen den von Squid übergebenen Wert geprüft wird. Mit einem ! hinter dem = wird geprüft, ob dieser Ausdruck nicht passt.

Sind alle Bedingungen erfüllt wird die Aktion bei action ausgeführt. Bei `noscan` wird der Download nicht gescannt, bei redirect wird die Anfrage auf die angebene URL umgeleitet. Die Werte <url> usw. werden durch die von Squid übergebenen Argumente bei Bedarf ausgetauscht.

Für weitere Infos sei auch auf die Dokumentation von Squid verwiesen.

8.2.33 scan Abschnitte

Dieser Abschnitt funktioniert analog zu den noscan-Abschnitten. Es gibt jedoch zwei Unterschiede:

- Als Aktion wird immer scan gewählt und somit der Download nach Viren durchsucht.
- Zusätzlich zu den Prüfungen kann hier noch der Mime-Type geprüft werden. Falls eine solche Prüfung vorkommt wird dieser vom Webserver über eine HEAD-Anfrage ermittelt (sofern noch nicht geschehen).



Achtung: ein FTP-Server kann keinen Mime-Type zurück liefern. Deswegen sollte für FTP über die Endung der Datei bestimmt werden ob gescannt werden soll oder nicht.



Bei Übertragungen mit SSL wird der Inhalt verschüsselt (Methode = CONNECT). Diese Daten können nicht nach Viren durchsucht werden! Dazu müsste ich die Daten entschlüsseln können (und damit hätte ich bewiesen, dass die Verschlüsselung zu knacken ist).

Aber auch für dieses Problem habe ich eine Lösung bereits in der Schublade liegen. Diese wird evtl. in SquiVi3 eingebaut. Bei dringendem Bedarf könnt Ihr Euch ja mal bei mir melden und den aktuellen Status abfragen.

8.2.34 scanner Abschnitte

```
<scanner clamscan>
        bin = /usr/local/bin/clamscan
        args = --verbose –recursive
        exitnovirus = 0
</scanner>
```

Mit diesem Abschnitt werden analog zu den Packer-Abschnitten die zu benutztenden Virenscanner definiert. `exitnovirus` gibt den Exitcode des Scanner an falls kein Virus gefunden wurde. Dies sollte idR. 0 sein.

Falls mehrere Scanner definiert sind werden diese alle durchlaufen – es ist also möglich den Download von mehreren Scanner durchsuchen zu lassen.

8.3 squivi.cgi/squiviauth.cgi

Der Inhalt des htdocs Verzeichnisses muss über den Webserver erreichbar sein. Ich empfehle hierzu die Einrichtung eines VirtualHost. Teste den Zugriff auf den Webserver über einen Browser (http://<Dein Server>/squivi.cgi). SquiVi2 sollte sich melden mit dem Hinweis auf fehlerhafte Benutzung.

8.4 squid

In der Konfiguration von Squid sollte folgende Zeile gesetzt werden:

```
redirect_program <Pfad zum Programm>/squivi.pl -c <Pfad zur Konfig>/squivi.conf
```

Falls an dieser Stelle schon auf ein anderes Programm verwiesen wird kann diese Zeile so nicht eingetragen werden. Siehe hierzu auch 9.6 squiviplex.pl, der SquiVi2 Multiplexer mit dem dieses Problem behoben werden kann.

Eventuell ist eine Anpassung der Option `redirect_children` nötig. Ein Wert von 8 hat bei mir sehr gute Ergebnisse geliefert.

9 Die einzelnen Komponenten

In diesem Abschnitt erkläre ich nun die Funktionsweise der einzelnen Komponenten.

9.1 squivi.pl

Dies ist der eigentliche Redirector – der Teil der in Squid integriert wird.

-c <conffile> Die Konfigurationsdatei
-d Debug-Modus – es werden zusätzliche Meldungen ausgegeben
-h Hilfemeldung

Der Debugmodus sollte nur genutzt werden um SquiVi2 zu testen, also beim direkten Start von der Konsole.

9.2 squivicleanup.pl

Dieses Tool räumt das Downloadverzeichnis auf und bereinigt auch die Katalogdatei.

-a <Tage> Es werden nur Dateien gelöscht, die älter als <Tage> Tage sind. Bei 0 wird alles gelöscht.
-i <id> Löscht nur eine einzelne ID (Achtung: funktioniert natürlich nur ohne -a)
-c <conffile> Die Konfigurationsdatei
-d Gibt Debuginformationen aus
-h Hilfemeldung



squivicleanup.pl sollte nur dann gestartet werden wenn kein squiviscan.pl Prozess mehr aktiv ist. Am Besten also in der Nacht zu Zeiten wo nur noch sehr wenige bis keine User mehr arbeiten.

9.3 squivihead.pl

Dies ist ein Tool von SquiVi1. squivihead.pl führt eine HEAD-Anfrage für die angegebene URL durch und zeigt das entsprechende Ergebnis an. Diese Funktion wird auch von squivi.pl genutzt um den Mime-Type des Downloads zu ermitteln.

9.4 squivihead2.pl

squivihead2.pl ist eine Alternative zu squivihead.pl. Bei dieser Variante kann zusätzlich zur URL noch der Benutzernamen und das Passwort für die basic-Authentifizierung als Argumente übergeben werden.

9.5 squivilistdb.pl

Mit diesem Befehl kann der Inhalt des Kataloges aufgelistet werden. Im Katalog sind Informationen enthalten, ob eine Datei bereits erfolgreich übertragen wurde. Falls dies der Fall ist, wird die Datei zu einem späteren Zeitpunkt nicht noch einmal übertragen.

-c <conffile> Die Konfigurationsdatei
-h Hilfemeldung

Ab Version 2.6 kann gewählt werden ob man den Cache-Katalog anzeigen will oder die Authentifizierungstabelle.

9.6 squiviplex.pl

Dies ist ein Tool von SquiVi1. Squid kann nur einen Redirector benutzen. Falls man aber zwei oder mehrere einsetzen will, z.B. SquidGuard und SquiVi2 kann dieses Tool genutzt werden.

Um dieses Tool zu nutzen sollte man zuerst den ersten Redirector in Squid einrichten und auf Funktion testen, dann den Zweiten. Sobald beide richtig funktionieren kann in Squid squidplex.pl als Redirector eingetragen werden.

In squidplex.pl müssen dann noch die beiden Programme definiert werden. Hierbei ist eigentlich nur zu überlegen, welches Programm als erstes genutzt werden soll. Bei SquidGuard und SquiVi2 sollte zuerst SquidGuard eingetragen werden. Wozu soll nach Viren gesucht werden wenn der Zugriff auf eine Seite sowieso abgelehnt wird?



squidplex.pl startet die Anfrage an den zweiten Redirector natürlich nur dann, falls der erste keinerlei Einwände gegen den Besuch der Adresse hatte.

9.7 squiviscan.pl

Dieses Programm lädt eine Datei aus dem Internet und schreibt gleichzeitig das Protokoll welches von squivi.cgi aufbereitet und dem User als Status angezeigt wird. Dabei werden auch Archive ausgepackt und nach Viren gescannt. Dieses Tool wird von squivi.pl automatisch gestartet – ein Aufruf von Hand lohnt sich nur zur Fehlersuche.

-c <conffile>	Die Konfigurationsdatei
-d	Debugmodus – sollte nur beim Start über die Konsole aktiviert werden
-h	Hilfemeldung
-i id	Die ID des Jobs der ausgeführt werden soll (wird von squivi.pl generiert und übergeben)

9.8 squivi.cgi

Dieses Skript hält den User über den Fortschritt des Downloads und der Suche nach Viren auf dem laufenden. Sollte kein Virus gefunden werden wird anschließend der Download angeboten.

9.9 squiviauth.cgi

Über dieses Skript ermittelt SquiVi2 die Authentifizierungsdaten für passwortgeschützte Bereiche. Siehe hierzu auch 8.2.7 waitforauthdata.

9.10 squivi.css

Dir gefällt die Optik der Ausgabe nicht? Na dann Volltreffer! Dies ist die CSS-Datei von squivi.cgi und kann den eigenen Bedürfnissen natürlich angepasst werden.

10 Statistik

squiviscan.pl schreibt sofern der Loglevel >= 1 ist Zeilen ins syslog die mit '(statistics)' beginnen. Diese Zeilen beinhalten die übergebene Daten von Squid an den Redirector, die Größe des Downloads (optional, nur falls Download erfolgreich) und eine Meldung welcher Scanner einen Virus gefunden hat.

Diese Zeilen kann man z.B. mit grep aus dem syslog filtern und dann entsprechend dem eigenen Bedarf weiter verarbeiten. Damit sollten sich Statistiken für den eigenen Bedarf erstellen lassen. Am Besten schaue Dir einfach mal an was squiviscan.pl aufschreibt.

11 Bekannte Fehler

So was wird sich leider auch nicht vermeiden lassen – deswegen hier eine Übersicht über bekannte Fehler und auch solche die zum Teil mit Workarounds gelöst worden sind.

11.1 Fehler

In dieser Liste stehen Fehler und Probleme die noch nicht behoben sind (z.B. weil die Ursache durch Dritte verursacht ist).

- Darstellungsfehler in Mozilla bei CSS und großen weißen Rahmen

11.2 Workarounds und behobene Fehler

Die Fehler bzw. Workarounds hier sind in der Reihenfolge des Auftretens gelistet.

- Konqueror: Bei Refresh wurde nicht auf den Anker am unteren Ende des Statusberichts gesprungen. Lösung durch Modifikation des Ankers.
- IE: Manche Versionen haben Probleme beim Refresh, dieser wurde nicht automatisch durchgeführt (bei anderen Browsern und auch anderen IE Versionen ging's aber). Lösung: komplette Umstellung der Argumente von der URL auf PATH_INFO.
- IE: Mei FTP Anfrage Problem mit Mime-Type text/html - keine Darstellung. Lösung durch Umleitung.
- IE: Bei Fertigstellung von Download und Gang über Argumente in URL wird Mime-Type abgeschnitten und immer auf text/file gesetzt, dabei wird die Endung abgeschnitten. Lösung durch Benutzung von PATH_INFO.

12 Kontakt

Am Besten über Mail: sschoch@users.sourceforge.net oder auf der Homepage: squivi2.sourceforge.net.

13 Anhang

13.1 Abbildungsverzeichnis

Abbildungsverzeichnis

Abbildung 1: Anfrage an das Internet 4
Abbildung 2: Anbindung über Firewall 4
Abbildung 3: Integration in squid 5

13.2 GPL

```
                    GNU GENERAL PUBLIC LICENSE
                       Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc.
                          59 Temple Place, Suite 330, Boston, MA  02111-1307  USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

                            Preamble

  The licenses for most software are designed to take away your
freedom to share and change it.  By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users.  This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it.  (Some other Free Software Foundation software is covered by
the GNU Library General Public License instead.)  You can apply it to
your programs, too.

  When we speak of free software, we are referring to freedom, not
price.  Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

  To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

  For example, if you distribute copies of such a program, whether
gratis or for a fee, you must give the recipients all the rights that
you have.  You must make sure that they, too, receive or can get the
```

source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS

```
TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU.  SHOULD THE
PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,
REPAIR OR CORRECTION.

  12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING
WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR
REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING
OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED
TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY
YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER
PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE
POSSIBILITY OF SUCH DAMAGES.

                     END OF TERMS AND CONDITIONS


            How to Apply These Terms to Your New Programs

  If you develop a new program, and you want it to be of the greatest
possible use to the public, the best way to achieve this is to make it
free software which everyone can redistribute and change under these terms.

  To do so, attach the following notices to the program.  It is safest
to attach them to the start of each source file to most effectively
convey the exclusion of warranty; and each file should have at least
the "copyright" line and a pointer to where the full notice is found.

    <one line to give the program's name and a brief idea of what it does.>
    Copyright (C) <year>  <name of author>

    This program is free software; you can redistribute it and/or modify
    it under the terms of the GNU General Public License as published by
    the Free Software Foundation; either version 2 of the License, or
    (at your option) any later version.

    This program is distributed in the hope that it will be useful,
    but WITHOUT ANY WARRANTY; without even the implied warranty of
    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
    GNU General Public License for more details.

    You should have received a copy of the GNU General Public License
    along with this program; if not, write to the Free Software
    Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA  02111-1307  USA


Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

    Gnomovision version 69, Copyright (C) year name of author
    Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
    This is free software, and you are welcome to redistribute it
    under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License.  Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary.  Here is a sample; alter the names:

  Yoyodyne, Inc., hereby disclaims all copyright interest in the program
  `Gnomovision' (which makes passes at compilers) written by James Hacker.

  <signature of Ty Coon>, 1 April 1989
  Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs.  If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library.  If this is what you want to do, use the GNU Library General
Public License instead of this License.
```