DOKUMENTATION

Netfilter 2009

Autor: Christoph Schneeberger

Datum: 5. Juni 2009

Inhalt

Einführung

Ausgangslage

Der bestehende Netfilter auf Basis eines Soekris 4801 mit AMD Elan 486 CPU soll durch 2 SUN Fire V120 Server als Cold Standby Cluster ausgefuehrt werden. Zusätzlich soll für den Mitarbeiter vor Ort einfacher ersichtlich sein ob ein Netzwerk-Problem besteht oder die Maschine noch nicht in Netfilter authorisiert/freigeschaltet wurde. Dazu werden alle Webzugriffe auf die tcp-Ports 80, 81, 3128 und 8080 auf einen lokalen Webserver umgeleitet und der Anwender darüber informiert, dass er sein Gerät mit dem falschen Netzwerk verbunden hat. Mitarbeiter der Messe können das Gerät dann nach erfolgreicher HTTP-Authentisierung direkt und unittelbar freischalten.
Die Appliance wird aus Redundanzgründen doppelt ausgeführt, kann aber nur über manuelle Intervention (Master ausschalten, Slave einschalten) zum Failover gebracht werden! Durch einen eingebauten Update Mechanismus sind die Daten auf beiden Appliances jeweils identisch und aktuell.

Hardware

- 2 SUN Fire V120 mit:
  - 1024MB RAM
  - 2 * 70GB SCSI Harddisks (ST373307LSUN72G)
  - 2 * BCM5221 100baseTX NICs

Aufgabe

Die Netfilter Appliance wird als Layer2 Element (Bridge) zwischen das unkontrollierte Netz und das interne Netz angeschlossen und leitet Pakete vom internen Netz ohne Einschränkungen an das unkontrollierte Netz (Hallennetz) weiter, während vom unkontrollierten Netz nur Pakete von als erlaubt konfigurierten MAC-Adressen weitergeleitet werden.

Funktionsweise

Gesehene und erlaubte MAC-Adressen werden weiterhin zentral in einer MySQL DB geführt. Die Struktur der Datenbank ist dabei wie folgt:

DB-Struktur

Tabellen	Felder	Zweck
config	do_update1, do_update2, do_update3, do_update4, do_update5, do_update6	Beinhaltet den timestamp wann eine Aktualisierung der Bridge nötig wurde, oder 0 wenn die Bridge Aktualisierungen erfolgreich abgeholt hat.
mac_addr_allow	mac, tstamp	Beinhaltet erlaubte MAC-Adressen mit dem first-seen timestamp, wobei mac den primären Key darstellt.
mac_addr_seen	mac, tstamp	Beinhaltet gesehene MAC-Adressen mit dem first-seen timestamp, wobei mac den primären Key darstellt.
maclookup	mac_prefix_num, mac_prefix_str, mac_vendor	Beinhaltet bekannte MAC-Adressen Prefix mit Zuordnung zum entsprechenden Hersteller.

allg. Web-GUI

Im Web-GUI können die erlaubten und gesehenen Adressen gesichtet und bearbeitet werden (hinzufügen und löschen). Das Web-GUI ist unverändert gegenüber der bestehenden Netfilter Version

Netfilter-Komponenten

Auf der Netfilter Appliance wird das Programm macblock.pl in Abständen von 6 Minuten ausgeführt. macblock.pl trägt neu gesehene MAC-Adressen in der Datenbank ein und führt falls nötig Aktualisierungen der erlaubten Adressen durch (wenn das do_updateX Feld in der Tabelle config einen timestamp enthält, wobei X der ID der Bridge entspricht die in /etc/macblock.ini konfiguriert wird).

Netfilter Web-GUI

Nicht authorisierte Maschinen aus dem unkontrollierten Netz können über ein CGI Webinterface die MAC-Adresse von der der Zugriff erfolgt verzögerungslos freischalten.

Installation / Vorbereitung der Hardware

Installation Betriebssystem (OpenBSD)

Die Installation des Betriebssystems ist ausserhalb des Fokus dieser Dokumentation, es werden hier nur die vom in [1] beschriebenen Standardvorgaben dokumentiert.

Partitionierung Disk

Die folgenden Angaben stellen Minimal-Anforderungen an die Disk-Partionierung dar und dürfen ohne weiteres überschritten werden:

Partition	Mindestgrösse / max. sinnvolle Grösse	Mount Point
a	128M / 2G	/
b	2*Hauptspeicher, z.B. 2GB bei 1GB RAM	swap
d	256M / 2G	/tmp
e	1G / 12G	/var
g	4G / 20G	/usr
h	10M / unbegrenzt	/home

Zu installierende Basis-Pakete

Folgende Basis-Pakete müssen installiert/während der Installation ausgeählt werden:

- baseXY.tgz
- etcXY.tgz
- compXY.tgz (empfohlen, aber nicht kritisch)
- manXY.tgz (empfohlen, aber nicht kritisch)
- miscXY.tgz

Wobei XY jeweils die aktuelle Version, z.B. 45 bezeichnet.

Nach der Installation

Nach der Basis Installation sollten folgende sogenannte Ports resp. Packages eingespielt werden:

1 OpenBSD Installationsanleitung: http://www.openbsd.org/faq/faq4.html

Zu installierende Ports / Packages

bzip2-1.0.5	block-sorting file compressor, unencumbered
fping-2.4b2p4	quickly ping N hosts w/o flooding the network
mysql-client-5.0.77	multithreaded SQL database (client)
net-snmp-5.4.2.1p1	extendable SNMP implementation
p5-Config-IniFiles-2.47	module for reading .ini-style configuration files
p5-Crypt-DES-2.05p1	interface to the DES encryption algorithm
p5-DBD-mysql-4.010	MySQL drivers for the Perl DBI
p5-DBI-1.607	unified perl interface for database access
p5-Digest-HMAC-1.01p0	interface to HMAC Message-Digest Algorithms
p5-Digest-SHA1-2.11p1	module to calculate SHA1 digests
p5-IO-Socket-INET6-2.56p0	object interface for AF_INET and AF_INET6 domain sockets
p5-Net-Daemon-0.43	extension for portable daemons
p5-Net-SNMP-5.2.0	Perl modules to access SNMP
p5-PlRPC-0.2018p0	module for writing rpc servers and clients
p5-SNMP_Session-1.12	provides rudimentary access to remote SNMP agents
p5-Socket6-0.22	Perl defines relating to AF_INET6 sockets
py-mysql-1.2.2p2	Python interface to MySQL
py-setuptools-0.6c9	simplified packaging system for Python modules
python-2.5.4	interpreted object-oriented programming language
sqlite3-3.6.10	embedded SQL implementation

Die Version entspricht jeweils der in OpenBSD 4.5 enthaltenen Port Version, bei Verwendung einer neueren OpenBSD Version kann die entsprechend aktuellere Version eines Ports problemlos verwendet werden.

Installation Netfilter Software

Um die Netfilter Software zu installieren muss nur ein aktuelles Update-Paket über dem Dateisystem-Root ausgepackt werden, z.B. mit:

tar -C / -xzvf /home/macblock15.tgz

Nach einem Neustart ist die Netfilter Appliance betriebsbereit.

Konfiguration der Appliances

Konfiguration Datenbank

Die Konfiguration der Appliance findet ausschliesslich über die Datei /etc/macblock.ini statt. In erster Linie müssen nur die Angaben zur Datenbank (Sektion DB) und die Interface Konfiguration (Sektion Main, hot_if und cool_if) angepasst werden:

Konfigurationsdatei /etc/macblock.ini

```
[Main]
; Bridge Device name
bridgename=bridge0
; external Interface name
hot_if=gem1
; internal Interface name
cool_if=gem0
; type of bridge (1=master, 2=slave)
btype=1
; id of bridge for DB updates (reset flag)
bid=1
[DB]
driver=mysql
host=10.11.12.13
user=netfiler_db-user
pass=netfilter_db-pass
database=macblock
allow_tbl=mac_addr_allow
seen_tbl=mac_addr_seen
[Bridge]
maxage=8
fwddelay=5
timeout=20
maxaddr=1024
mpriority=32768
spriority=32770
```

Diese Konfigurationsdaten werden von macblock.pl wie auch von maccgi (dem Webinterface für die direkte Freischaltung aus dem unkontrollierten Netz) ausgelesen.

Update Funktion

Funktionsweise

Nach jedem Systemstart prüft die Netfilter Appliance anhand der in /etc/rc.conf.local konfigurierten Version/Releasenummer ob ein Update an der ebenfalls in /etc/rc.conf.local konfigurierten URL vorhanden ist. Ist ein solches vorhanden wird es heruntergeladen, installiert und die Appliance automatisch neu gestartet.
Es kann also durchaus sein, dass die Appliance mehrmals nacheinander neu startet um sich mittels mehrerer Updates auf den letzten Stand zu bringen. Dies ist vor allem zu beachten, wenn der Backup Node nach längerer Zeit erstmals in Betrieb genommen wird.

Update URL

Es wird empfohlen die Update URL auf einen internen Server zeigen zu lassen, da die enthaltene macblock.ini Zugangsdaten für den Datenbankserver enthält.

Erstellung von Updates

Um ein neues Update für die Netfilter Appliances zu erstellen muss wie folgt vorgegangen werden:

1. Herunterladen des letzten Updates
2. Entpacken des Updates in ein temporäres Verzeichnis
3. Merken und erhöhen der Releasenummer (MACBLOCK_VER) in etc/rc.conf.local
4. Durchführen der Änderungen an ausgepacktem Update
5. Packen des Updates mit:
   cd TMPDIR; tar -cvzf ../macblockXYZ.tgz etc/ usr/ var/
   (Setzen Sie für XYZ die oben gemerkte, vorherige Releasenummer ein [z.B. 015]!)
6. Kopieren Sie das Archiv in das Update Verzeichnis auf dem Webserver (konfiguriert durch die Variable MACBLOCK_URL in etc/rc.conf.local)
7. Starten Sie entweder die Netfilter Appliance neu oder rufen Sie den Befehl **macup** auf der zu aktualisierenden Netfilter Appliance auf.

Cold Failover

Die Appliances sind ausschliesslich auf manuelles Cold Failover eingestellt. D.h. ist ein failover gewünscht muss der Master Node ausgeschaltet (LOM-Befehl power-off) oder vollkommen vom Netz getrennt werden bevor der Slave Node in Betrieb genommen wird.

Gleichzeitiger Betrieb

WICHTIG: Sind beide Geräte gleichzeit hochgefahren und an eines der beiden Netzwerk-Segmente angeschlossen ist die Funktion der Appliance nicht mehr gewährleistet!

Wichtige/nützliche Kommandos

Wartung / Diagnose

uptime	Uptime und Last des Geräts
df -h	Freier Plattenplatz
halt	Herunterfahren des Systems
reboot	Neustarten des Systems
brconfig bridge0	Anzeigen der Bridge Diagnose Informationen
ifconfig -a	Anzeigen der Interface Konfiguration aller Netzwerkkarten

Netfilter Kommandos

macup	auf neue Updates prüfen, installieren und neu starten
macblock.pl	auf neue Datenbank Updates prüfen und installieren. Mit -v o. -vv mehr diagnostische Informationen.

DPKG

dpkg -l [*Paket-Namen*]	Listet Pakete auf.
dpkg -I *Paket*.deb	Zeigt Paket-Informationen.
dpkg -c *Paket*.deb	Listet den Inhalt einer Paket-Datei.
dpkg -S *Dateiname*	Zeigt, zu welchem Paket eine Datei gehört.
dpkg -i *Paket*.deb	Installiert Paket-Dateien.
deborphan	Zeigt, Pakete, von denen kein anderes Paket abhängt, benötigt **deborphan**.
debsums	Prüft die Check-Summen installierter Pakete, benötigt **debsums**.
kpkg-divert [Optionen] *Datei*	Aufheben der Version einer Datei eines Paketes.
dpkg-query -W `--showformat=`*format*	Abfrage über installierte Pakete, Format-Bsp.: '${Package} ${Version} ${Installed-Size}\n'.
Dpkg `--get-selections` > *Datei*	Schreibe Paket-Auswahl in Datei.
Dpkg `--set-selections` < *Datei*	Setze Paket-Auswahl aus Datei.

DAS NETZWERK

`/sbin/ifconfig`	Konfigurieren von Netzwerk-Schnittstellen.
`/etc/network/`	Netzwerk-Konfiguration, siehe vorallem interfaces und options.
ifup, ifdown	Starten, stoppen von Schnittstellen entsprechend obiger Dateien.
ssh -X *user@host*	Login auf einen anderen Rechner.
scp *Dateien* *user@host*:*Pfad*	Dateien zwischen Rechnern kopieren.

WEB SERVER (APACHE2)

`/etc/apache2/`	Konfigurations-Dateien.
`/etc/apache2/sites-enabled/default`	Definiert den virtuellen Standard-Host.
`/etc/apache2/mods-available/`	Enthält verfügbare Modul-Dateien. Um ein Modul zu aktivieren, erzeugen Sie einen symbolischen Link in `/etc/apache2/mods-enabled/`.

DATENBANKEN (POSTGRESQL)

createdb	Erzeugen einer neuen Datenbank.
dropdb	Entfernen einer Datenbank.
createuser	Erzeugen eines neuen Datenbank-Benutzers.
dropuser	Entfernen eines Datenbank-Benutzers.
`/etc/postgresqul/pg_hba.conf`	Klienten-Zugriffs-Konfiguration.
ALTER USER name WITH PASSWORD 'password';	Ändern des Passwortes in der SQL-Konsole **psql**.

DATEI- UND DRUCK-SERVER (SAMBA)

`/etc/samba/smb.conf`	Haupt-Konfigurations-Datei.
smbclient	SMB-Netzwerk Ressourcen durchstöbern, z.Bsp. Dateien hoch- oder runterladen.

Erstellt mit: `http://people.debian.org/~debacle/refcard/`

Debian GNU/Linux Referenz-Karte

Version 3.1-0.2, 2005-09-03
http://www.debian.org/

HILFE BEKOMMEN

man *Seite* oder man bash	Lesen der Handbuch-Seite für jedes Kommando und viele Konfigurations-Dateien.
Kommando `[--help oder -h]`	Die meisten Kommandos haben eine kurze Hilfe
`/usr/share/doc/[`*Paket-Name*`/]`	Hier finden Sie alle Dokumentationen. `README. Debian` enthält ggf. Spezifika.
Web-Dokumentation	Referenz, Handbücher, FAQs, HOWTOs, etc. unter `http://www.debian.org/doc/`
man *Seite* oder man bash	Lesen der Handbuch-Seite für jedes Kommando und viele Konfigurations-Dateien.
Mailing-Listen unter `http://lists.debian.org/`	Die Debian-Gemeinde ist immer hilfsbereit, suchen Sie nach `users`.

INSTALLATION

Installer	Alle Informationen dazu unter `http://www.debian.org/devel/debian-installer/`
`boot: expert`	z.Bsp. zum Konfigurieren des Netzwerkes ohne DHCP oder zum Nutzen von LILO statt GRUB.
`boot: linux26 o. boot: expert26`	Linux kernel 2.6 für die Installation verwenden.

BUGS

Fehlerdatenbank unter `http://bugs.debian.org/`	Alles über bekannte und gelöste Fehler
Bestimmtes Paket	Siehe `http://bugs.debian.org/`*Paket-Name*, benutze `wnpp` um neue Pakete anzufragen.
reportbug	Fehler per E-Mail berichten.
Berichten	Anweisungen zum Berichten von Fehlern unter `http://www.debian.org/Bugs/Reporting`

KONFIGURATION

`/etc/`	Alle Konfigurations-Dateien des Systems befinden sich im Verzeichnis `/etc./`
nano *Dateien*	Standard Text-Editor. Falls nicht vorhanden, probieren Sie **emacs, vi** oder **Joe**.
webmin unter `https://hostname:10000`	Browser-Oberfläche zur System-Konfiguration. Zugriffsrechte sind in `/etc/webmin/miniserv.conf` definiert
CUPS unter `http://hostname:631`	Browser-Oberfläche zur Drucker-Konfiguration.
dpkg-reconfigure *Paket-Name*	Rekonfigurieren eines Paketes, z.Bsp. Console-common (Tastatur), locales (Sprache).
update-alternatives *Optionen*	Konfiguration von Kommando-Alternativen.
update-grub	Nach Installation eines neuen Kernels.

`/etc/`	Alle Konfigurations-Dateien des Systems befinden sich im Verzeichnis `/etc./`
make-kpkg –initrd --revision=2.my.1.0 --rootcmad fakeroot --uc –us kernel_image	Ein Kernel-Paket aus den Quellen bauen, wenn ein angepasster Kernel wirklich gebraucht wird. Benötigt `kernel-package`.
m-a a-i module kernel_image	Erzeuge und installiere Fremd-Module (nvidia, ...), benötigt `module-assistant`.

DÄMONEN UND SYSTEM

`/etc/init.d/Datei restart`	Neustarten eines Dienstes oder System-Dämons.
`/etc/init.d/Datei stop`	Stoppen eines Dienstes oder System-Dämons.
`/etc/init.d/Datei start`	Starten eines Dienstes oder System-Dämons
Halt, reboot, poweroff	Hält das System an, startet es neu oder schaltet es aus.
`/var/log/`	Hier finden Sie alle Protokoll-Dateien.
`/etc/default/`	Standard-Werte für viele Dämonen und Dienste.

WICHTIGE SHELL-KOMMANDOS

cat *Dateien*	Ausgeben der Dateien
cd *Verzeichnis*	Wechsle das Verzeichnis
cp *Dateien Ziel*	Kopiere Dateien und Verzeichnisse
echo *Text*	Echo des Textes.
gzip, bzip2 [-d]*Dateien*	Komprimiere, dekomprimiere Dateien.
less *Dateien*	Zeigt den Inhalt von Dateien.
ls [*Dateien*]	Listet Dateien auf
mkdir *Verzeichnis-Namen*	Erzeuge Verzeichnisse.
mv *Datei1 Datei2*	Verschiebe Dateien und/oder benenne sie um.
rm *Dateien*	Lösche Dateien.

cat *Dateien*	Ausgeben der Dateien
rmdir *Verzeichnisse*	Lösche leere Verzeichnisse.
tar [c][x][t][z][j]-*f Archiv-Datei* [*Dateien*]	Erzeuge (c), entpacke (x) oder liste den Inhalt (t) einer Archiv-Datei, z/j für .gz/.bz2.
find *Verzeichnisse Ausdruck*	Finde passende Dateien (z.Bsp.-name oder -size)
grep *Text Dateien*	Finde gesuchten Text in Dateien.
kill [*-9*]*Nummer*	Sende Signal an Prozess (z.Bsp. Zum Beenden).
ln -s *Datei Link*	Erzeuge einen symbolischen Link auf eine Datei.
ps [*Optionen*]	Zeige aktuelle Prozesse.
su – [*username*]	Zu einem anderen Benutzer werden, z.Bsp. Root.
sudo *Kommando*	Führe als normaler Benutzer ein Kommando als root aus, siehe `/etc/sudoers`
Kommando >Datei	Überschreibe Datei mit Ausgabe des Kommandos.
Kommando >>Datei	Füge Ausgabe des Kommandos an Datei an.
Kmd1 | Kmd2	Benutze Ausgabe von Kommando 1 als Eingabe von Kommando 2.
Kommando <Datei	Benutze Datei als Eingabe für Kommando.

APT

apt-get update	Aktualisieren der Datenbank der vorhandenen Pakete aus den Repositorien die in `/etc/apt/sources.list` aufgelistet sind. Aufzurufen, wenn der Inhalt der Repositories oder die Datei selbst verändert wurde und im Zweifelsfall.
apt-cache search *Text*	Durchsuche Paketnamen und ihre Beschreibungen nach dem *Text*.
apt-cache policy *Paket-Namen*	Zeige Versionen und Prioritäten verfügbarer Pakete.
apt-cache show *Paket-Namen*	Zeige Paket-Informationen einschliesslich Beschreibung.
apt-cache showpkg *Paket-Namen*	Zeieg Paket-Abhängigkeiten (benötigte Pakete).
apt-get install *Paket-Namen*	Installiere Pakete aus den Repositores mit all ihren Abhängigkeiten.

apt-get update	Aktualisieren der Datenbank der vorhandenen Pakete aus den Repositorien die in `/etc/apt/sources.list` aufgelistet sind. Aufzurufen, wenn der Inhalt der Repositories oder die Datei selbst verändert wurde und im Zweifelsfall.
apt-get upgrade	Installiere die neuesten Versionen aller derzeit installierten Pakete.
apt-get dist-upgrade	Wie **apt-get upgrade**, aber mit erweiterter Konflikt-Auflösung.
apt-get remove *Paket-Namen*	Entferne installiertes Paket und alle davon abhängenden Pakete.
apt-cache depends *Paket-Namen*	Listet alle Pakete auf, die von einem bestimmten Paket benötigt werden.
apt-cache rdepends *Paket-Namen*	Listet alle Pakete auf, die selbst ein bestimmtes Paket benötigen.
apt-file update	Aktualisieren der Inhalt-Datenbank der Paket-Repositores, siehe **apt-get update**.
apt-file search *Datei-Namen*	Suche, in welchem Paket eine Datei enthalten ist.
apt-file list *Paket-Name*	Listet den Inhalt eines Paketes.