CAcert infra01 setup notes

Author: Jan Dittberner <jandd@cacert.org>
Version: 0.3
Date: 2011-04-27

Contents

initial setup

- update packages using aptitude
- setup apticron to get informed about available updates
- install etckeeper, bash-completion, vim, lxc, bridge-utils, debootstrap, ntp, screen, pwgen, ferm, python-apt, python-ipcalc

virtual machine setup

- create script lxc-setup for lxc container creation (know how from http://wiki.debian.org/LXC and /usr/share/doc/lxc)
- initialization file

```
[network]
subnet=24
gateway=10.0.0.1
device=br0
domain=cacert.org
smtprelay=emailout.cacert.org

[host]
volumegroup=vg0

[debian]
mirror=http://ftp.nl.debian.org/debian/
release=squeeze
packages=ifupdown, libui-dialog-perl, dialog, netbase, net-tools,
  exim4-daemon-light, iproute, openssh-server, etckeeper, python,
  locales, vim, iputils-ping, screen, sudo

[lxc]
cachedir=/var/cache/lxc/debian
```

- example for svn VM

```
sudo ./lxc-setup -n svn -l 8G -i 10.0.0.20 -r `pwgen -s 32 -n 1` \
  -a svn-admin@cacert.org
```

```
sudo lxc-start -n svn -f /etc/lxc/svn.conf -d
```

- enable forwarding

```
echo "net.ipv4.ip_forward = 1" > /etc/sysctl.d/local.conf
sysctl net.ipv4.ip_forward=1
```

- setup of firewall rules in `/etc/ferm/ferm.conf`
  - use aliases for internal and external addresses in header
  - use subchains for hosts
  - host specific rules are put in separate files in `/etc/ferm/ferm.d/`

```
# -*- shell-script -*-
#
#  Configuration file for ferm(1).
#

@def $INFRA01 = 172.16.2.9;

@def $HOST_DEBMIRROR = @resolve((ftp.nluug.nl ftp.nl.debian.org security.debian.org));
@def $HOST_DNS = 172.16.2.1;
@def $HOST_SMTP = @resolve(emailout.intra.cacert.org);

@def &CONTAINER($name, $host, $host_ext) = {
    table filter {
        chain FORWARD {
            daddr $host @subchain "$name-fwd-in" {
                jump global-in;
            }
            saddr $host @subchain "$name-fwd-out" {
                jump global-out;
            }
        }
    }
}

@def &CONTAINER_NAT($name, $host_ext, $host_int) = {
    &CONTAINER($name, $host_int, $host_ext);

    table nat {
        chain PREROUTING {
            daddr $host_ext DNAT to $host_int;
        }
        chain POSTROUTING {
            saddr $host_int SNAT to $host_ext;
        }
    }
}

@def &CONTAINER_IN($name, $proto, $port) = {
    table filter {
        chain "$name-fwd-in" {
            proto $proto dport $port ACCEPT;
```

```
        }
    }
}

@def &CONTAINER_OUT($name, $host, $proto, $port) = {
    table filter {
        chain "$name-fwd-out" {
            proto $proto daddr $host dport $port ACCEPT;
        }
    }
}

table filter {
    chain INPUT {
        policy DROP;

        # connection tracking
        mod state state INVALID DROP;

        # allow local packet
        interface lo ACCEPT;

        # respond to ping
        proto icmp ACCEPT;

        jump global-in;

        mod state state (ESTABLISHED RELATED) ACCEPT;
    }

    chain OUTPUT {
        policy DROP;
        mod state state INVALID DROP;
        jump global-out;
        # connection tracking
        mod state state (ESTABLISHED RELATED) ACCEPT;
    }

    chain FORWARD {
        policy DROP;

        # connection tracking
        mod state state INVALID DROP;
    }

    chain global-out {
        proto udp daddr $HOST_DNS dport domain ACCEPT;
        proto tcp daddr $HOST_SMTP dport smtp ACCEPT;
        proto tcp daddr $HOST_DEBMIRROR dport http ACCEPT;
    }

    chain global-in {
        proto tcp dport ssh ACCEPT;
    }
```

```
}

@include 'ferm.d/';

table filter chain FORWARD mod state state (ESTABLISHED RELATED) ACCEPT;

# IPv6:
domain ip6 {
    table filter {
        chain INPUT {
            policy DROP;
        }
        chain FORWARD {
            policy DROP;
        }
        chain OUTPUT {
            policy DROP;
        }
    }
}
```

- add ip address of svn vhost to `/etc/network/interfaces` in `eth0` section:

```
iface eth0 inet static
  address 172.16.2.9
  netmask 255.255.255.0
  network 172.16.2.0
  broadcast 172.16.2.255
  gateway 172.16.2.1
  # dns-* options are implemented by the resolvconf package, if installed
  dns-nameservers 172.16.2.1
  dns-search infra.cacert.org
  post-up ip -4 addr add 172.16.2.15 dev eth0
  pre-down ip -4 addr del 172.16.2.15 dev eth0
```