**Configure Host-based and User-based Security for the Service on RHEL 7**

Security for SSH, HTTP/S, DNS, NFS, SMB and SMTP.

**Host-based Security**

**SSH**

Allow firewall SSH access for all:

# firewall-cmd --permanent --add-service=ssh

Open /etc/hosts.deny and add the following:

sshd: my1337.hacker.local

Open /etc/hosts.allow and add the following:

sshd: \*.rhce.local

By default everything is allowed.

**# journalctl -xlf**

[...]

sshd[3069]: refused connect from my1337.hacker.local (10.8.9.99)

**HTTP/HTTPS (Apache)**

Allow firewall HTTP/S access for all:

# firewall-cmd --permanent --add-service={http,https}

Put the following into the httpd configuration file:

<RequireAll>

Require host rhce.local

Require not host my1337.hacker.local

</RequireAll>

**# journalctl -xlf**

[...]

[authz\_core:error] [pid 3057] [client 10.8.9.99:43378] AH01630: client denied by server configuration: /var/www/html/

**DNS (Unbound)**

Allow firewall DNS access for all:

# firewall-cmd --permanent --add-service=dns

Open /etc/unbound/unbound.conf and add the following line:

access-control: 10.8.8.0/24 allow

By default everything is refused.

**NFS**

Allow firewall NFS access for all:

# firewall-cmd --permanent --add-service=nfs

Open /etc/exports and configure access:

/nfs \*.rhce.local(ro)

Everything else is refused.

**SMB**

Allow firewall SMB access for all:

# firewall-cmd --permanent --add-service=samba

Open /etc/samba/smb.conf and configure hosts allow entries:

hosts allow = 10.8.8.

The hosts deny list can also be used, but note that where the lists conflict, the allow list takes precedence.

**SMTP (Postfix)**

Allow firewall SMTP access for all:

# firewall-cmd --permanent --add-service=smtp

Open /etc/postfix/access and add the following:

rhce.local OK

my1337.hacker.local REJECT

Run:

# postmap /etc/postfix/access

Add the following line to /etc/postfix/main.cf:

smtpd\_client\_restrictions = check\_client\_access hash:/etc/postfix/access

**# journalctl -xlf**

[...]

postfix/smtpd[3939]: connect from my1337.hacker.local[10.8.9.99]

postfix/smtpd[3939]: NOQUEUE: reject: RCPT from my1337.hacker.local[10.8.9.99]: 554 5.7.1 <my1337.hacker.local[10.8.9.99]>: Client host rejected: Access denied; from=<root@my1337.hacker.local> to=<root@rhce.local> proto=ESMTP helo=

postfix/smtpd[3939]: disconnect from my1337.hacker.local[10.8.9.99]

[...]

postfix/smtpd[3939]: connect from srv1.rhce.local[10.8.8.71]

postfix/smtpd[3939]: A075621186: client=srv1.rhce.local[10.8.8.71]

postfix/cleanup[3944]: A075621186: message-id=<20160801150634.86753207E9@srv1.rhce.local>

postfix/qmgr[3882]: A075621186: from=<root@rhce.local>, size=610, nrcpt=1 (queue active)

postfix/smtpd[3939]: disconnect from srv1.rhce.local[10.8.8.71]

postfix/local[3946]: A075621186: to=<root@rhce.local>, relay=local, delay=0.08, delays=0.06/0.01/0/0.01, dsn=2.0.0, status=sent (delivered to mailbox)

postfix/qmgr[3882]: A075621186: removed

**User-based Security**

**SSH**

Open /etc/ssh/sshd\_config and configure the following sections:

AllowUsers sandy

DenyUsers root

Don’t forget to restart the sshd service.

**HTTP/HTTPS (Apache)**

Open /etc/httpd/conf/httpd.conf and configure user authentication:

<Directory "/var/www/html">

AuthType Basic

AuthName "Login Required"

AuthUserFile "/etc/httpd/conf/htpasswd"

Require valid-user

</Directory>

You will need to create a password file with a valid user:

# htpasswd -c /etc/httpd/conf/htpasswd sandy

Don’t forget to restart the httpd service.

**NFS**

NFS server does not require authentication and only enforces access restrictions that are based on IP addresses or host names of a client. Using the default security method, which is sec=sys, the NFS server trusts any uid that is sent by the client.

Kerberos should be used to prove user identity.

**SMB**

Open /etc/samba/smb.conf and configure the following sections:

valid users = sandy, alice

write list = alice

read list = sandy

The valid users is a list of users that should be allowed to login to this service.

The write list is a list of users that are given read-write access to a service. If the connecting user is in this list then they will be given write access, no matter what the read only option is set to.

Don’t forget to restart the smb service.

**SMTP (Postfix)**

Postfix’s per-address access control /etc/postfix/access:

user@domain REJECT

This entry was posted in [Linux](https://www.lisenet.com/category/linux/), [Security](https://www.lisenet.com/category/security/) and tagged [CentOS](https://www.lisenet.com/tag/centos/), [EX300](https://www.lisenet.com/tag/ex300/), [RHCE](https://www.lisenet.com/tag/rhce/), [RHEL](https://www.lisenet.com/tag/rhel/). Bookmark the [permalink](https://www.lisenet.com/2016/configure-host-based-and-user-based-security-for-the-service-on-rhel-7/). If you notice any errors, please [contact us](https://www.lisenet.com/about/).