Managing Security

- Configure firewall settings using firewall-cmd/firewalld
- Restrict network access using firewall-cmd/firewalld
- Manage default file permissions
- Configure key-based authentication for SSH
- Set enforcing and permissive modes for SELinux
- List and identify SELinux file and process context
- Restore default file contexts
- Manage SELinux port labels
- Use boolean settings to modify system SELinux settings
- Diagnose and address routine SELinux policy violations

Introducing firewalld and firewalld zones

Firewalls are used to protect systems from unwanted traffic from outside world. **firewalld** is a **dynamic firewall service daemon** that allows to add ,delete and modify firewall rules without restarting firewalld daemon each time a change is made.

firewalld uses concept of services and zones to simplify traffic management.

firewalld services have predefined configs that allow incoming traffic for specific service, and they are scoped to zone they are defined in.

firewalld zones are predefined set of firewall rules and they allow traffic depending on the level of trust on the network.

There are few predefined zones and **public zone** is the default zone. **Public zone** is used for **untrusted networks** and traffic is allowed as per firewall rules configured by you, as System Admin.

To list zones : `firewall-cmd --get-zones`
To list services: `firewall-cmd --get-services`

➢ Configure the firewall on system.example.com to allow inbound http traffic (default zone- public) .
- Changes done should be persistent.

Command	**Action/Description**
systemctl status firewalld	To check status of **firewalld** service
firewall-cmd --get-services	To get list of **firewalld** services
firewall-cmd --add-service=http	Adding http service on firewall in runtime
firewall-cmd --add-service=http --permanent	Adding http service on firewall persistently
firewall-cmd --reload	Reload firewall

- Configure the firewall to accept inbound traffic on 443/tcp port.
  - Changes done should be persistent.
  - Use firewall-config for this task.

Command	Action/Description
dnf install firewall-config	Install package firewall-config
firewall-config	Launching firewall-config
firewall-cmd --list-all	Checking firewall configs

❑ Configure system.example.com machine to restrict ssh access to 192.168.99.0/24

Command	Action/Description
firewall-cmd --list-all	Displaying firewall configurations
firewall-cmd --add-rich-rule 'rule family="ipv4" source address="192.168.99.0/24" service name="ssh" accept' --permanent	Adding firewalld rich rule to accept traffic form **192.168.99.0/24** network
firewall-cmd --remove-service=ssh --permanent	Removing **ssh** service from services list
firewall-cmd --reload	Reloading firewall to make changes effective
firewall-cmd --list-all	To verify firewall configs after making changes

Note :

Remove **ssh service** from services list ,if you don't remove **ssh service** ,then ssh traffic will be allowed irrespective of the source network.

To Test This : .

We have only one network, so it is not possible to test this. To test this working of rich rule , you just add rule to allow access from network other than **192.168.99.0/24** network and then test ssh connection from **ipaserver.example.com**, it must be denied.

Managing default file permissions

Default permissions on file (or directory) are set as per default umask (user file-creation mode mask) set in shell profile file /etc/bashrc (non-login shell) and /etc/login.defs (login shell).

Default Permissions = Base Permissions – Umask
Base Permissions on directory = 0777
Base Permissions on file = 0666
umask (Default) = 0022

Default Permissions on directory = 0777-0022 = 0755
Default Permissions on file = 0666-0022 = 0644

Below listed shell profile files set shell environment for users :

- /etc/profile - Global settings (for all users)
- /etc/bashrc - Global settings (for all users)
- ~/.bash_profile - User specific
- ~/.bashrc - User specific

We are concerned about umask (user file-creation mode mask) which determines the default permissions to be set on file and directory .

➢ Configure default umask for user rhcsa as 0066, so default file permissions are 0600 (files) and 0711(directories).

Command	Action/Description
echo ‘umask 0066’ >> /home/rhcsa/.bashrc	Add umask value in user specific profile file
touch test-file & ls -l test-file	Create test file and verify permissions (0666-0066=0600)
mkdir test-dir & ls -ld test-dir	Create directory and verify permissions(0777-0066=0711)

➢ Configure password-less ssh login (for root user) on system.example.com to establish connection to ipaserver.example.com.
- Use passphrase access to protect the private key.

Command	Action/Description
ssh ipaserver.example.com	Testing SSH connection
ssh-keygen -t rsa	Generating SSH key-pair
ssh-copy-id ipaserver.example.com	To copy public key to SSH Server
ssh ipaserver.example.com	Testing password less connection
cd /root/.ssh	Path where private/public key-pair is stored on client
more /root/.ssh/authorized_keys	File where public key is stored on server side

- Web server (httpd) needs to access the files in /web directory. Set the correct SELinux context type on /web directory to make this possible.
  - Changes done should be persistent.
  - Restore the SELinux Context.

Command	Action/Description
chcon -R -t httpd_sys_content_t /web	Configuring SELinux context type recursively in run time
semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?”	Setting SELinux context type recursively and persistently
restorecon -R -v /web	Restoring SELinux context recursively
ls -ldZ /web	Displaying SELinux contexta
man semanage fcontext	To display man page for **semanage fcontext**
man restorecon	To display man page for **restorecon**

- Configure correct Selinux context type for ssh service to listen on non-default TCP port 555.
  - Changes done should be persistent.

Command	Action/Description
semanage port -l	To list all SELinux context types set on default ports
semanage port -a -t ssh_port_t -p tcp 555	To set the correct selinux context type on non-default port

- List all SELinux booleans and set the SELinux boolean samba_export_all_rw to 1 to allow Samba server to share exports with r/w permissions.
  - Changes done should be persistent.

Command	Action/Description
getsebool -a	To list all SELinux Booleans
setsebool -P samba_export_all_rw 1	To set the Boolean persistently