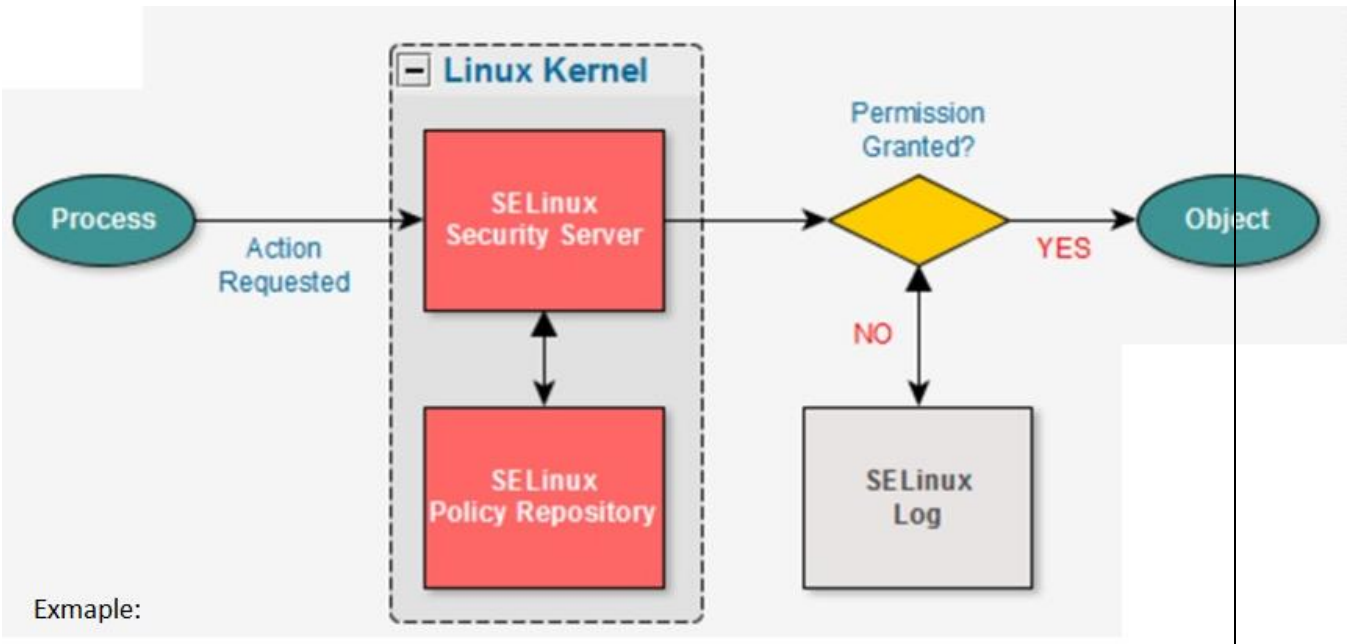
02-06-2021
https://youtu.be/-HK1KLbisNY

SELinux

Directory: /etc/sysconfig/selinux;
Config file: vi /etc/sysconfig/selinux;
Port #: 22; 2222
Package: policycoreutils-python;
Services: sshd
Protocol: tcp
Command: semanage, getenforce, setenforce, sestatus
URL:



ssh uses port 22	SELinux quietly check this	if this is normal, then access is allowed
ssh uses port 2222	SELinus quietly check this	this is not normal, access denied

Unusual activity is blocked by **SELinux**

What exactly **SELinux** does? – it protects the system from *unusual activity*.

For example, SSH works on port 22, but is SSH tries to use any other port it will be blocked, even after allowing through firewall.

If a person has access to building going through front door using the badge – this is normal activity for this person.

If the same person tries enter building from the side door using same badge, he will be denied access.

Mandatory Access Control

- An additional security layer over discretionary access control limiting who can do to what

Discretionary access control

- Traditional
  - File permissions
  - Access control List
  - setuid
  - setguid
  - su/sudo previlages
- if you own the file or folder – you get to determine who get the access to it.
- This is known a discretionary

Subject

- A user or process that accesses an object

Object

- A resource such as a file, directory, device, ports etc.,

Access

- An action performed by a subject on an object, example read write or create

Security policy

- System-wide policy of rules defining which subject can access which object
- Two policies in Enterprise Linux – Targeted and Strict – targeted is default

Security context

- Tag used by SELinux to store security attributes of subject and objects

SELinux modes

Enforcing mode

- Security policy is enforced
- That means SELinux security is active

```
[root@zmpt01 ~]# getenforce
Enforcing
```

Permissive mode

- Security policy is observed and warning will be displayed, but policy is not enforced

```
[root@zmpt01 ~]# setenforce 0
[root@zmpt01 ~]# getenforce
Permissive
```

If the system reboots the enforcing will turn on

```
[root@zmpt01 ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   permissive
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Max kernel policy version:      31
```

```
[root@zmpt01 sysconfig]# init 6
[root@zmpt01 sysconfig]# vi selinux
[root@zmpt01 sysconfig]# getenforce
Permissive
```

Disable SELinux

```
[root@zmpt01 ~]# vi /etc/sysconfig/selinux
```

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
#SELINUX=enforcing
SELINUX=disabled
# SELINUXTYPE= can take one of three values:
```

```
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted

[root@zmpt01 ~]# init 6

[root@zmpt01 ~]# getenforce
Disabled
```

Note: Never set SELinux disabled

Lest change the SSH Port to use port number 2222

Note: number of ports in OS – 2^16 = 2x2x…16 = 65,536

Ports are nothing but door of the operating system

Normal SSH port – 22

Change SSH port – 2222

Install semanage package

```
[root@zmpt01 ~]# yum install policycoreutils-python
```

Grep for port 22

```
[root@zmpt01 ~]# semanage port -l | grep 22

ssh_port_t                 tcp      22
```

Check the status of port 22

```
[root@zmpt01 ~]# grep SSH /etc/services

ssh             22/tcp                  # The Secure Shell (SSH) Protocol
ssh             22/udp                   # The Secure Shell (SSH) Protocol
ssh             22/sctp             # SSH
```

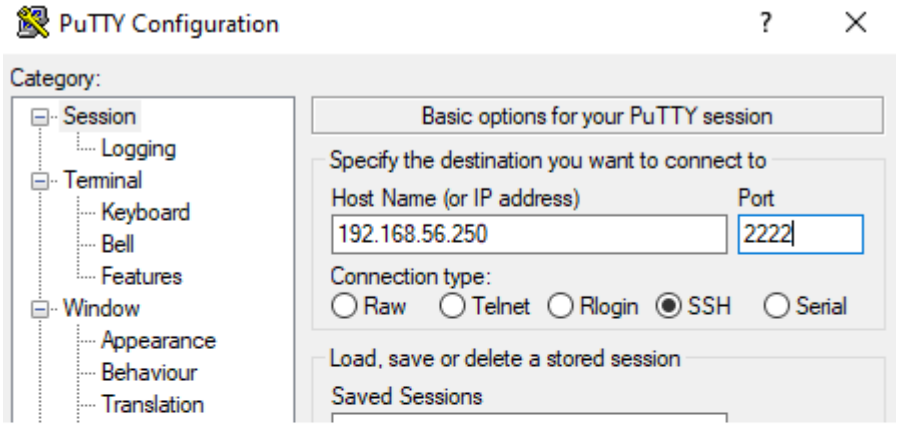
Change the port 2222

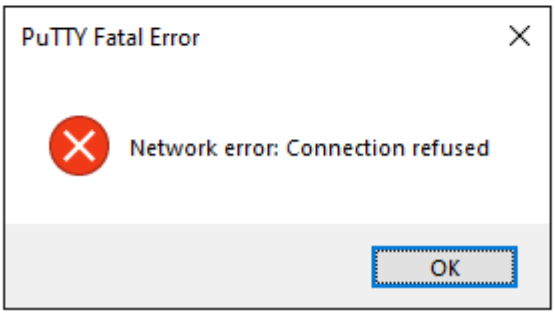
```
[root@zmpt01 ~]# vi /etc/ssh/sshd_config

Port=2222

[root@zmpt01 ~]# firewall-cmd --permanent --zone=public --add-port=2222/tcp
success
[root@zmpt01 ~]# firewall-cmd --reload
success
[root@zmpt01 ~]# firewall-cmd --list-port
2222/tcp
```

```
[root@zmpt01 ~]# systemctl restart sshd
Job for sshd.service failed because the control process exited with error code. See "systemctl status sshd.service" and "journalctl -xe" for details.
```





Connection is still denied, even though the port 2222 is open through firewall

Also regular port 22 will not work either after we perform semanage update through SELinux

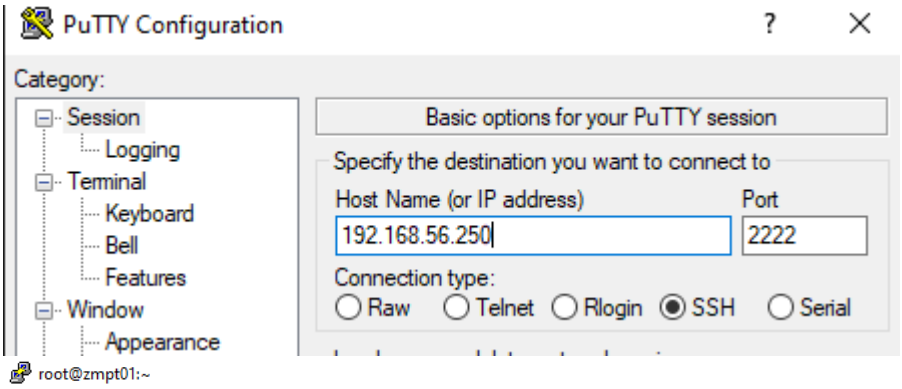
Now allow through the SELinux

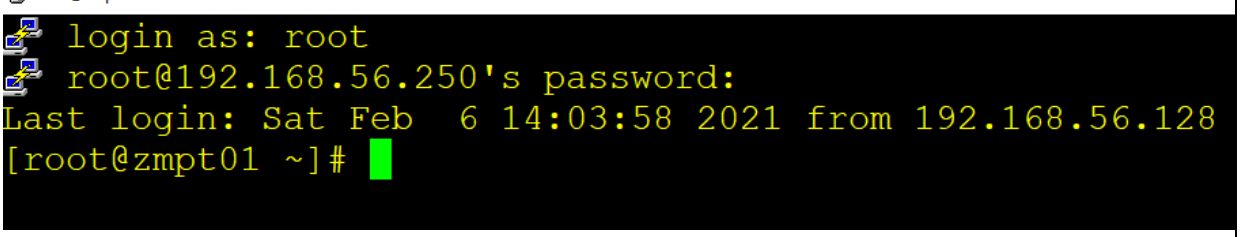
```
[root@zmpt01 ~]# semanage port -l | grep -i 22
```

ssh_port_t tcp 22

[root@zmpt01 ~]# semanage port -a -t ssh_port_t -p tcp 2222 #< --- adding port 2222 to SELinux

ssh_port_t tcp 2222, 22





Login successful

Note: port 22 is disabled, only port 2222 will work

To make port 22 work again, add to /etc/ssh/sshd_config

port=2222
port=22

Set it back to original setting

[root@zmpt01 ~]# semanage port -d -t ssh_port_t -p tcp 2222

Port 2222 is removed

[root@zmpt01 ~]# semanage port -l | grep 22

ssh_port_t tcp 22

```
[root@zmpt01 ~]# vi /etc/ssh/sshd_config

#Port 22
```

```
[root@zmpt01 ~]# systemctl restart sshd

No errors
```

```
[root@zmpt01 ~]# systemctl status sshd
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
   Active: active (running) since Sat 2021-02-06 15:26:01 EST; 36s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 2152 (sshd)
   CGroup: /system.slice/sshd.service
           └─2152 /usr/sbin/sshd -D

Feb 06 15:26:01 zmpt01.prod.zmprotech.com systemd[1]: Stopped OpenSSH server daemon.
Feb 06 15:26:01 zmpt01.prod.zmprotech.com systemd[1]: Starting OpenSSH server daemon...
Feb 06 15:26:01 zmpt01.prod.zmprotech.com sshd[2152]: Server listening on 0.0.0.0 port 22.
Feb 06 15:26:01 zmpt01.prod.zmprotech.com sshd[2152]: Server listening on :: port 22.
Feb 06 15:26:01 zmpt01.prod.zmprotech.com systemd[1]: Started OpenSSH server daemon.
```