1. Pre-Requisites for Infraon SecuRA

1. Time Sync: NTP must be installed and system time must be synced with NTP server prior to installation.

Note: Updating time post installation would lead to data mismatch and other issues and might lead to software re-installation.

2. Preferred OS version: CentOS Linux release 7.7.1908 (Core).
3. SNMP must be enabled in the target devices.
4. SSH details must be shared to Everest team.
5. Supported Browsers : Chrome ,Edge and Firefox

2. Information and Troubleshooting Points:

Service Status:

1. Apache

    Service httpd status

2. Postgresql

    Service postgresql-10 status

3. EverestCLI

    Service everestcli status

4. Daemon

    Service daemon status

5. FTP

    Service vsftpd status

6. TFTP

    Service xinetd status

    Service tftp status

7. SNMP

Service snmpd status

8. SecuRA Service

Service secura status (service name must be given)

9. Firewall

Service firewall status (if port is not added, it must be added to the firewall or firewall must be stopped)

Ports used in SecuRA:

1. SNMP - 161
2. Syslog -514
3. Postgres - 5432
4. FTP -21
5. SSH - 22
6. Telnet - 23
7. TFTP - 69
8. https - 443
9. NCCM Configured Port - default 9000 (could be configured in other ports too)
10. SSL - 465
11. TLS - 587
12. SMTP -25
13. EverestCLI - default 8020 (could be configured in other ports too)
14. Netconf - 830

Checklist for Onboarding devices onto SecuRA:

✓ Device is reachable through PING from NCCM server

✓ SNMP has been enabled in all the devices

- ✓ Time zone is synced with NTP Server
- ✓ Proxy is configured on the server
- ✓ Daemon is configured
- ✓ FTP and TFTP are functioning properly
- ✓ System Parameters are set
    - IP
    - Location of TFTP
    - Repo is local
    - Policy check enabled during review
    - Default Connection protocol is **SSH**.
- ✓ Global Parameters are configured as per the requirement
- ✓ Configuration Profile, Templates and Rules are imported as per the requirement
- ✓ Device Credentials are added as per the requirement
- ✓ SELINUX status is disabled
- ✓ Daemon is properly configured with the related Port. *For e.g. if SecuRA has been configured with "9000" port but has been mapped with "8000" on daemon the application keeps rebooting often.*

Things to check if TFTP is not working:

1. Check TFTP service using:

    Service tftp status

    Service xinetd status

2. TFTP Folder permission

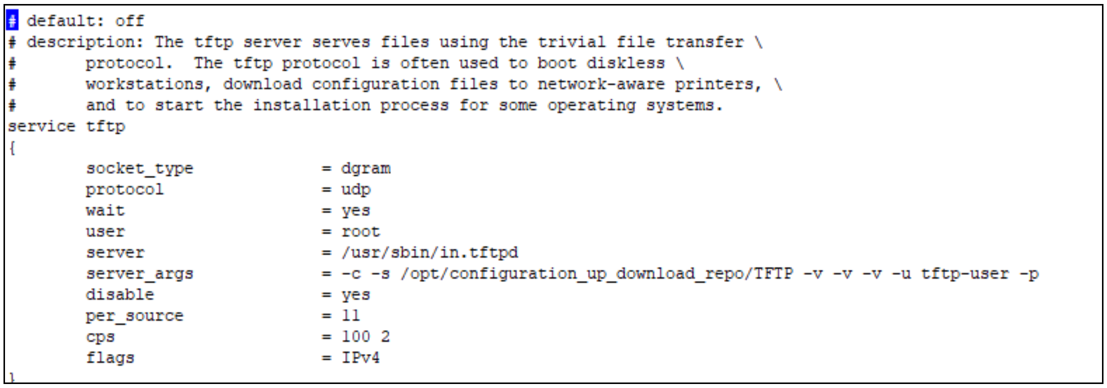
    Chmod 777 /TFTP_FolderPath

    For e,g   chmod 777 /opt/configuration_up_download_repo/TFTP

3. Check contents of the below file:

Vi /etc/xinetd.d/tftp

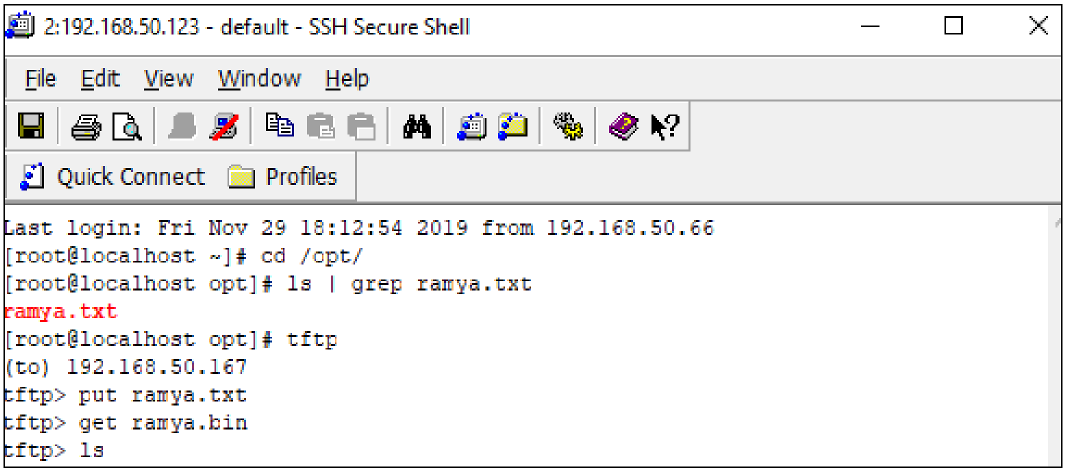
Content must match the example given in the below image:



```
# default: off
# description: The tftp server serves files using the trivial file transfer \
#       protocol.  The tftp protocol is often used to boot diskless \
#       workstations, download configuration files to network-aware printers, \
#       and to start the installation process for some operating systems.
service tftp
{
        socket_type             = dgram
        protocol                = udp
        wait                    = yes
        user                    = root
        server                  = /usr/sbin/in.tftpd
        server_args             = -c -s /opt/configuration_up_download_repo/TFTP -v -v -v -u tftp-user -p
        disable                 = yes
        per_source              = 11
        cps                     = 100 2
        flags                   = IPv4
}
```

4. File transfer using GET and PUT commands:

From SecuRA server, enter the below command:



```
Last login: Fri Nov 29 18:12:54 2019 from 192.168.50.66
[root@localhost ~]# cd /opt/
[root@localhost opt]# ls | grep ramya.txt
ramya.txt
[root@localhost opt]# tftp
(to) 192.168.50.167
tftp> put ramya.txt
tftp> get ramya.bin
tftp> ls
```

Apache Issue:

It might happen that the apache service may not be active. Ensure that IP v6 is disabled on the server's ethernet settings (refer Trouble shooting guide).

TCP Dump check:

Ensure that tcpdump package is installed (This will be within the installation folder)

To know the snmpwalk requests:

tcpdump and capture the snmp request and response with specified port 161

For e.g.

```
tcpdump -vv -i eth0 port 161
```

For syslog:

```
tcpdump -vv -i eth0 port 514
```

Firewall Check:

If any of the Port is not accessible, ask the user to check their IT policies on firewall.

Check the port reachability before accessing the URL or a specific port:

Telnet <Target IP Address> <Port Number>

For e.g.:

```
Telnet 192.168.50.123 80
```

Template making:

Before configuring the template, it is necessary to check commands on the device.

Template must be in Jinja format (simple command must be avoided, and it is highly recommended to use XML format).

SCP Connection Check:

When the SCP command is executed by SecuRA on a UAT device, the device will establish an SSH connection to copy the file. So, the direction of file copy over SCP will happen from device to SecuRA. Hence SSH from SecuRA to device is only open and not the other way.

If SCP is required to check, it is recommended to use putty and try copying the OS image to SecuRA server. Once that is successful, retry using SecuRA. It is possible that the issue is with the device (Cisco) or the user's network block in case of copy failure.

When the user downloads/uploads through SCP, and **"Administratively disabled"** is displayed on the device, the below command must be executed:

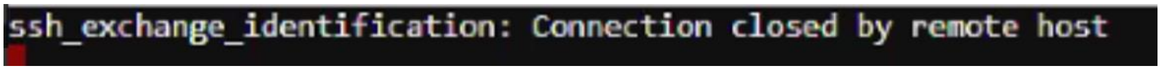
"***ip SCP server enable***"

"no ip ssh stricthostcheck"

When the user downloads/uploads through SCP, and **"Privilege denied"** is displayed on the device, note that the user must be created with the level 15 privileges.

Unable to establish CLI connection:

When the user is unable to establish a CLI connection and the following error message is displayed, the user needs to clear the contents from known_hosts file across all servers.



```
ssh_exchange_identification: Connection closed by remote host
```

Go to */root/.ssh/known_hosts* file and check if the RSA key for the selected IP is correct.

Save the changes to establish CLI connection.