

# Check Point connector

## *Configuration manual & Test Plan*

## TABLE OF CONTENT

<b><u>1</u></b>	<b><u>CONTENTS OF THE PACKAGE .....</u></b>	<b><u>4</u></b>
<b><u>2</u></b>	<b><u>REQUIREMENT .....</u></b>	<b><u>4</u></b>
<b><u>3</u></b>	<b><u>DEPLOYMENT .....</u></b>	<b><u>5</u></b>
3.1	SCHEMA OF THE TEST ENVIRONMENT	5
3.2	DESCRIPTION	6
3.2.1	OVERVIEW	6
3.2.2	OUTSIDE NETWORK	6
3.2.3	INSIDE NETWORK	6
3.2.4	SIP PHONES CONFIGURATION	7
3.2.5	CHECKPOINT FIREWALL-1 CONFIGURATION	7
<b><u>4</u></b>	<b><u>RUNNING.....</u></b>	<b><u>7</u></b>
4.1	TEST PROCEDURE OVERVIEW	7
4.2	TEST PROCEDURE DETAILS	7
<b><u>5</u></b>	<b><u>APPENDIX A .....</u></b>	<b><u>8</u></b>

## Document revision control

DOCUMENT REVISION		
Date	Author	Description
08/15/06	H. Lee	Initial release
12/05/06	E. Craeymeersch	Ethernet interface change
01/16/07	M. Beretti	Installation procedure update
02/08/07	M. Beretti	Procedures minor updates

---

## 1 Contents of the package

---

- ❖ asterpoint RHE3 server with :
  - asterisk
  - ETSS security Check Point connector
  - ETSS security supervisor
  
- ❖ fraise OpenBSD 3.8 ethernet bridge with :
  - ETSS security Voice engine

---

## 2 Requirement

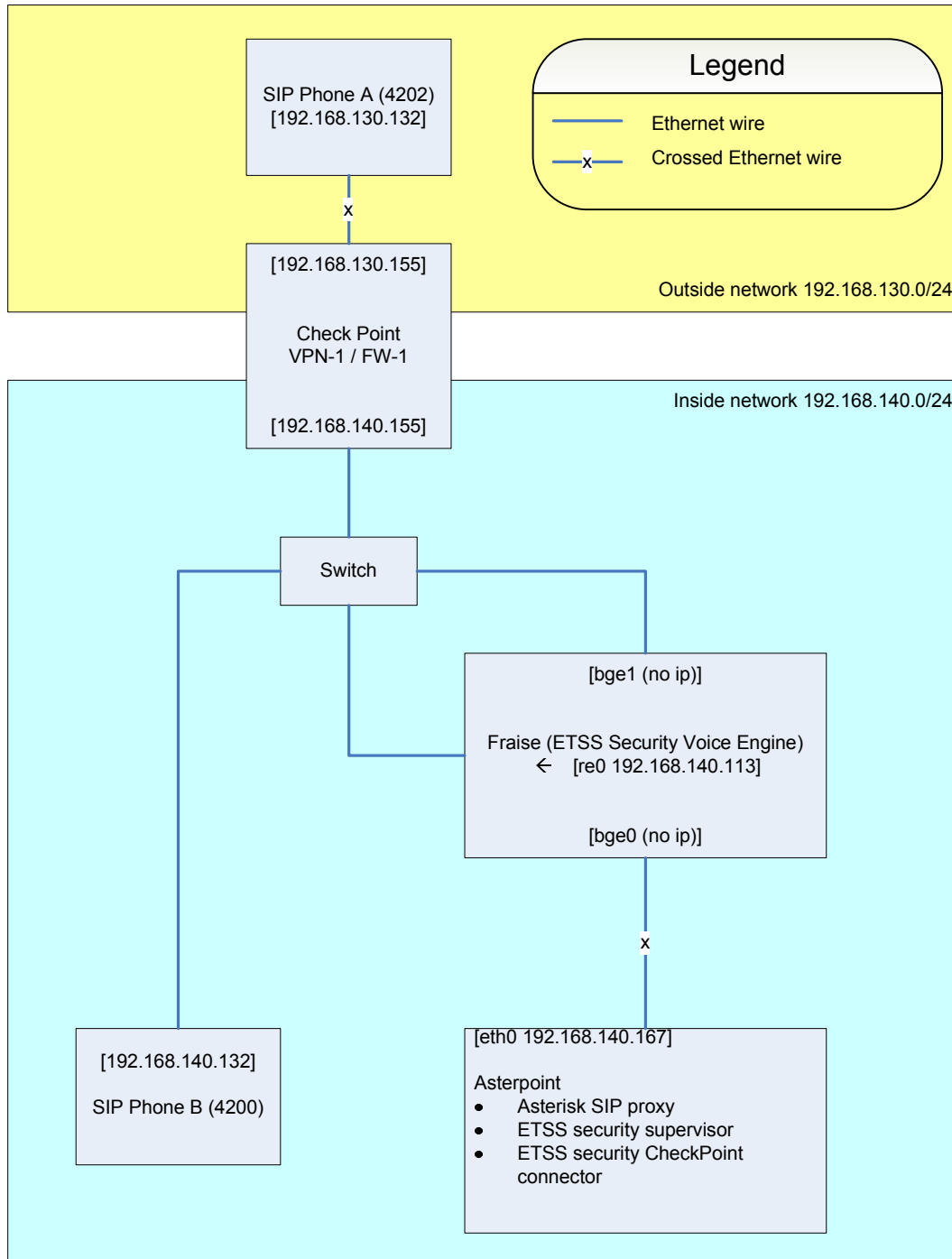
---

- 2 x SIP phones \*
- 1 x Check Point VPN-1/FireWall-1
- 2 crossover Ethernet cables
- 4 straight Ethernet cables
- 1 Ethernet switch
- 2 power cords
- Monitor and keyboard to plug on “asterpoint”.

\* SIP phones (hard phones or soft phones) compatible with UDP/SIP Registration process.  
(ex: SJPhone, Linphone, Cisco, Snom, Grandstream...)

## 3 Deployment

### 3.1 Schema of the test environment

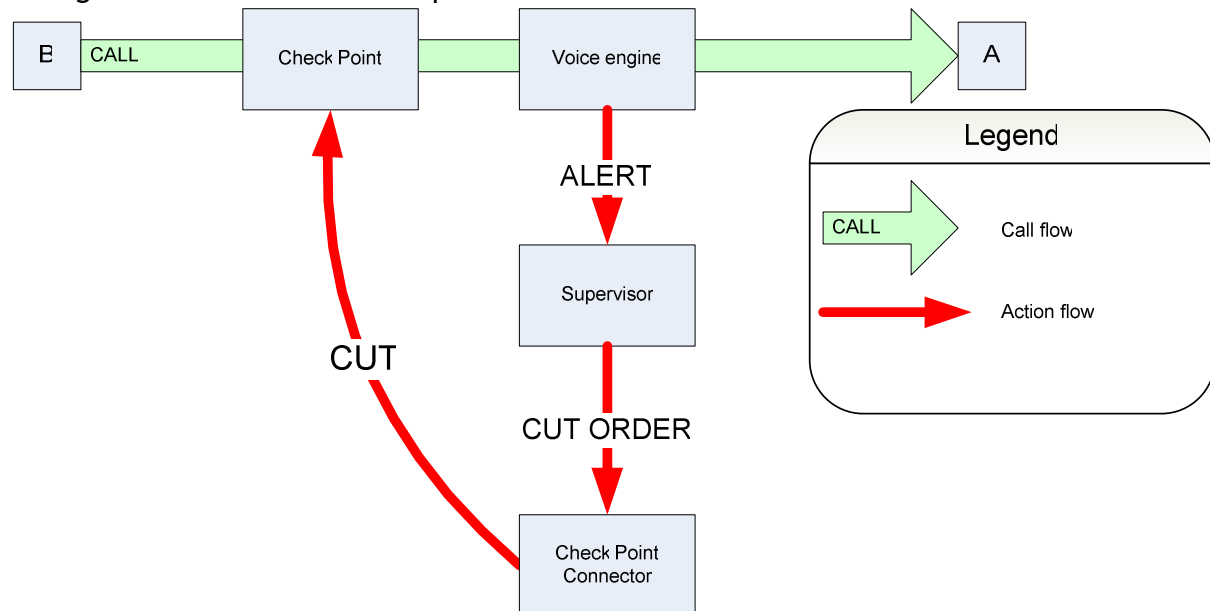


## 3.2 Description

### 3.2.1 Overview

The test environment is a network of two subnets. One is considered as outside and the other one as VoIP network. The "Check Point VPN-1/FW-1" route packets between these subnets. The outside subnet address is 192.168.130.0/24 and the inside subnet address is 192.168.140.0/24.

ETSS security works with a supervisor as well as all other ETSS security component like ETSS security Check Point connector. The supervisor acts as a message bus and configuration feeder for all components.



### 3.2.2 Outside network

The outside subnet contains just a single SIP phone called A, which has 4202 as phone number.

### 3.2.3 Inside network

The inside subnet is a VoIP subnet filtered by the transparent Ethernet bridge "fraise". "fraise" is an application layer filter that supports SIP/2.0 protocol. It applies filter rules received from the supervisor. When the filter match a rule that require cutting of an already established call, it send the cut order to the supervisor, the supervisor then forward that order to the Check Point firewall through it's connector.

The ETSS security supervisor, the Check Point connector and asterisk are running on the same box.

SIP/2.0 signalisation flow must pass through the ETSS security VOICE ENGINE and the RTP voice flow must pass through the Check Point VPN-1/FW-1 for the reason that ETSS security VOICE ENGINE filters SIP/2.0 signalisation whereas Check Point VPN-1/FirWall-1 filters the RTP flow.

### 3.2.4 SIP phones configuration

SIP proxy : 192.168.140.167  
SIP proxy port : 5060  
SIP proxy gateway : 192.168.140.155

SIP phone A number : 4202  
SIP phone A IP : 192.168.130.132  
SIP phone A gateway : 192.168.130.155

SIP phone B number : 4200  
SIP phone B IP : 192.168.140.130  
SIP phone B gateway : 192.168.140.155

### 3.2.5 CheckPoint FireWall-1 configuration

- Configure the firewall network as described above with the two networks 192.168.130.0/24 and 192.168.140.0/24 and enable the routing between the two networks.
- Configure the firewall as described in the appendix A.

---

## 4 Running

---

### 4.1 Test procedure overview

#### Test 1: Call without filter

[ A ] -----< OK >-----> [ B ]

#### Test 2: Call with 5 seconds filtering

[ B ] -----< 5 sec OK / 10 sec mute / OK >-----> [ A ]

### 4.2 Test procedure details

1. Plug every device as described above, and switch them on. Note that the "Asterpoint" might beep at startup.
2. Both SIP phones must be registered on 192.168.140.167, check that both SIP phone are registered.
3. To monitor the Checkphone ETSS Check Point connector, log in "asterpoint" (login="root", password = "checkpoint") and type the following command:  
*tail -f /var/etss/var/log/cnCheckpoint.log*
4. From SIP phone A (4202) call B (4200). Result: Call must be established and nothing will be done to cut this call.
5. From Sip phone B call A. Result: This call must be established, RTP voice flow will pass during 5 seconds, then the Check Point VPN-1/FireWall-1 stop the voice flow during 10 seconds. RTP filter timeout after 10 seconds then both parties can talk again.

---

## 5 Appendix A : Check Point FireWall-1 Configuration

---

### On the Check Point FireWall side:

1. Open the Check Point Policy Editor.
2. Go to Manage > Servers and OPSEC Applications. The Servers and OPSEC Applications screen displays. Select the OPSEC (Open Platform for Security) application property that you want to edit. Click "Edit."
3. The Properties screen displays. On the General tab, click "Communication." The Communication page displays.
4. On the Communication page, type an activation key in the Activation Key field. Confirm your selection in the Confirmed Activation Key field. Click "Initialize," then click "Close" to close the Communication screen.
5. On the Servers and OPSEC Applications screen, with the SAM Option tab active, de-select Use early versions compatibility mode. Click "OK." Click "Close" to close the Servers and OPSEC Applications screen.
6. Reinstall the FireWall policy by going to the Check Point Policy Editor. Select Policy > Install and click "OK."
7. Execute the following command to put the connector auth key:  
fw putkey -p <your activation key> -opsec <connector IP address>

### On the CheckPhone SAM connector side:

1. Go to the "/etc/ssl/snkcrt/opsec " directory, and type the following command to get the certificate:

```
#opsec_pull_cert -h host -n object_name -p password
```

- "host" is the resolvable name or IP address (in dot format) of the Management Station running the Certificate Authority
- "object\_name" is the OPSEC application name
- "password" is the activation key you typed in step 4

2. Copy "opsec.p12" to the same directory as the SAM connector, in other words, the "/etc/ssl/snkcrt/opsec/" directory.
3. Execute the following command to put the firewall auth key:  
opsec\_putkey -p <your activation key> <firewall IP address>
4. Modify the "chksam.conf" file under the same directory to define the SAM server attributes. For example:

```
opsec_sic_name "CN=chk_sam_cn,O=localhost.localdomain..lcui4r"  
sam_server opsec_entity_sic_name "CN=cp_mgmt,O=localhost.localdomain..lcui4r"  
opsec_sslca_file "/etc/ssl/snkcrt/opsec/opsec.p12"  
sam_server ip 192.168.130.155  
sam_server auth_type auth_opsec # or "sslca" for communications encryption  
sam_server auth_port 18183  
sam_server port 0
```

The "opsec\_sic\_name" is the application full "DN" name, you can find it at the bottom of the Servers and OPSEC Applications page. Note: For more information about the "chksam.conf" file, please consult the Check Point OPSEC NGFP3 documentation.

CHECKPHONE	Réf :	Ed : 08/02/2007	Page : 8 / 9
------------	-------	-----------------	--------------

5. Restart the SAM server.

**To receive OPSEC debugging information:**

To receive OPSEC debugging information during runtime, set the environment variable OPSEC\_DEBUG\_LEVEL to a value between 0 (no debugging information) and 3 (all debugging information) before the application starts. The debugging information can be seen by starting the CVP server with command line parameter "-t."