Purpose

The current CES demo allows you to connect one or several of your machines to a network served by a Customer Edge Switch (CES). This allows communication between

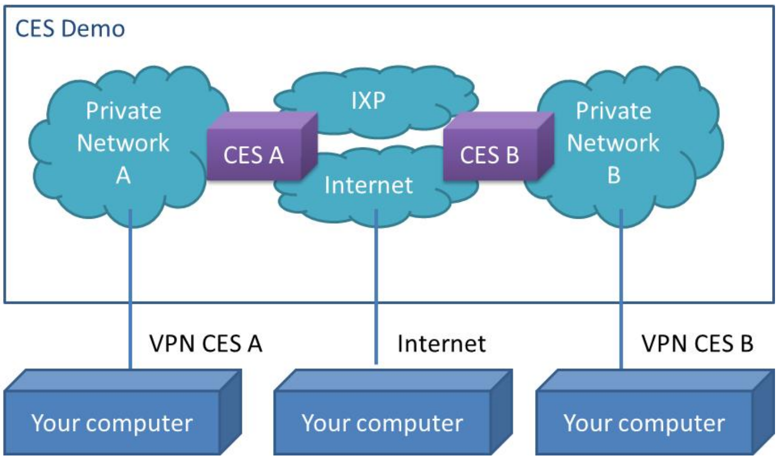
1. two devices in different CES enabled networks
2. two devices in the same CES enabled network (traffic routed through the CES)
3. a device in a CES enabled network and a device in the current public Internet ("legacy network")

The demo, in addition to illustrating the concept, allows you to test the compatibility of various protocols and applications with the CES. Of particular interest is the case where a server is in a CES enabled network, as CES provides inbound connectivity to private addresses by addressing the private host by their domain name.

If you are new to the CES concept, please study the publications available on the www.re2ee.org site.

Current setup

The demo network consists of two CES devices, a DNS server, and DHCP servers. A CES device serves a private network and provides connectivity to the hosts in this private network. Both the CES devices are connected to the public Internet. The CES devices are connected to each other directly via a separate network, modelling an Internet Exchange Point (IXP). The demo allows you to connect your machine to one of the private networks served by a CES device. You can then create connections from and to another machine that is located behind the other CES device or in the Internet.



The version of CES installed in the demo includes:

1. A Private Realm Gateway (PRGW) allowing access from and to hosts on the legacy Internet
2. Tunneling of packets between CES devices with the CETP protocol
3. An IPv6/IPv4 Gateway offering connectivity between the two versions of the IP protocol

Requirements

In order to be able to use the CES demo, you need to obtain a user account on the CES demo and the scripts for connecting to it by contacting us (see contact information below). To execute the commands illustrated here, you need a Linux computer with sudo rights. You can also perform similar steps to connect a Windows computer.

Connecting your machine to our CES demo

In order to connect your machine to our demo, you first need to establish a VPN connection so that all the traffic generated by your computer is routed through our CES. The steps required for the connection setup in a Linux environment are explained as follow.

1. Installation of OpenVPN: We have already created the configuration scripts for the client and the server side of OpenVPN. You can install OpenVPN with the following command.

```
apt-get install openvpn
```

2. Network configuration: In the current operation mode, our VPN server has been configured in a "bridged" mode, thus, forwarding all layer-2 traffic to and from the network. This means that the VPN client will be "plugged" to the network as if it were connected with a physical cable to the network. Auto-configuration for the host is provided by a DHCP server. Because all the traffic of the host is to be forwarded through the CES, first we have to perform slight modifications in the host's network configuration.
    a. Add a specific route to the VPN Server so that it is preferred over the default gateway. Use the parameters VPNSERVER_IP=**195.148.124.190** for the IP address of the VPN server, and GW_IP for the IP address of the gateway configured for your host. You can see your current gateway by performing a "route –n".

```
route add –host $VPNSERVER_IP gw $GW_IP
```

    b. Remove the exiting default gateway so that when the host gets the DHCP configuration it learns the new default gateway via the CES device.

```
route del -net 0.0.0.0
```

3. Creating the VPN connection: We have provided you with four different scripts for connecting to our demo. You can choose whether to connect to the *"CES-A"* or the *"CES-B"* network with the VPN established by either a TCP or a UDP connection. Open a terminal and locate the folder with the VPN scripts; then issue the following command with the appropriate script in that folder. The scripts use a TAP interface "tap1" for creating the VPN connection.

```
openvpn vpncesa_client_UDP.conf
```

4. Enable DHCP in the virtual TAP interface for host auto-configuration. Open a terminal and type the following:

```
dhclient tap1
```

5. After executing the previous command you should see that the host was successfully configured. The DHCP server offers the host an IP address in the private network, a default gateway and a DNS server for domain resolutions. In addition, when the host performs the DHCP request, it offers its hostname. This hostname is used by the CES to register the user enabling the outbound connections to other networks and the reception of inbound connections via its Fully Qualified Domain Name (FQDN) e.g. ***hostname.cesdemo.re2ee.org or hostname.ces2.research.netlab.hut.fi. NB: the shorter name may not work yet.***

Now you should be successfully connected to the CES demo. You can also check your public FQDN for receiving inbound connections on your machine by performing a reverse lookup of your IP address. Note that 10.10.0.151 is the IP address assigned by the DHCP server.

```
tester@test:~$ dig -x 10.10.0.151

; <<>> DiG 9.7.0-P1 <<>> -x 10.10.0.151
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27572
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;151.0.10.10.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
151.0.10.10.in-addr.arpa. 10    IN      PTR     test.cesdemo.re2ee.org.

;; Query time: 49 msec
;; SERVER: 10.10.0.2#53(10.10.0.2)
;; WHEN: Wed Mar 27 11:24:16 2013
;; MSG SIZE  rcvd: 79
```

Connecting to the CES Interactive Console

We have added an interactive console to our CES demo providing you with information of what is happening inside the CES. The main menu is represented below.

Once you have connected you own machine to CES, it is possible to reach the console via terminal on the IP address **10.10.0.1** and port **12345**.

```
tester@test:~$ telnet 10.10.0.1 12345
Trying 10.10.0.1...
Connected to 10.10.0.1.
Escape character is '^]'.
Welcome to CES prototype!
Choose one of the following options:
0. Display log
1. Display current NAT Table
2. Display firewall rules
```

```
3. Display registered hosts
4. Display interfaces
5. Update forwarding table
6. Update host connections
7. Delete a host connection
8. Initiate host mobility
9. Show CETP policies
10. Show DNS Cache
11. Sync a connection
12. Stop prototype
13. Exit
Option:
```

Disconnecting from the demo

When you are done, you only need to close the terminal with the OpenVPN and restore the network configuration. The network configuration can be automatically restored by restarting the networking Linux daemon or manually undoing the previous modifications of the routing table.

1. Restarting the networking daemon restores the routing table and DNS server settings.

```
/etc/init.d/networking restart
```

2. Manually revert the routing table to its previous state and modification of the DNS settings.

```
dhclient –r tap1
route del -net 0.0.0.0
route del –host $VPNSERVER_IP
route add –net 0.0.0.0 gw $GW_IP
#Remove CES related information from the /etc/resolv.conf file.
#Add a line for configuring the DNS server in use
#nameserver $USER_DNS_SERVER
nameserver 8.8.8.8
```

Contact information

In order to obtain access to the demo or to get more information about CES, please contact us on the following addresses:

raimo.kantola (at) aalto.fi

nicklas.beijar (at) aalto.fi

jesus.llorente.santos (at) aalto.fi