

Scenario 3: IPBrick.IC

30 de Maio de 2007

1 Presentation

This scenario includes 2 networks simulating an enterprise with two offices. On the first network, the domain is **ipbrick.pt** and we will call this network **network1**. We have two IPBrick servers on this network. One acting as communication server for vpn and mail functionality and another one acting as an intranet server. On the second network, the domain is **ipbrick.br** and we will call this network **network2**. We have a communication server on this network.

Material for this scenario:

- 2 IPBrick.C LDAP Master;
- 1 IPBrick.I LDAP Master;
- 2 Windows XP workstation;
- 1 switch;

2 Procedure

You must follow these steps in order to configure the scenario.

2.1 Mail

In this section, we will show on the communication server how we configure the mail service from relay email to an internal server and how we can access the email through a web interface from the internet.

2.1.1 Mail relay

- From the workstation at **network1**, open a web browser, on put **https://192.168.1.254**. Login: **admin** and password: **123456**
- Access the menu **IPBrick.C** – > **E-mail** – > **Configure**
- In the **Machine local domain** section remove the domain **ipbrick.pt**.
- In the **SMTP Routes** section **insert** a new smtp route. Fill the forms with the following information:

```
Domain:      ipbrick.pt
SMTP Route: 192.168.1.1
```

- In the menu, click in **Update Settings** and update settings.

2.1.2 Webmail

- From the workstation at **network1**, open a web browser, go to **https://192.168.1.254**.
Login: **admin** and password: **123456**
- In IPBrick Web interface, access the menu **IPBrick.C – > Webmail**
- Point webmail from IPBrick.C to imap server on IPBrick.I by clicking **modify**:

IMAP Server: 192.168.1.1
SMTP Server: gw.ipbrick.pt
- In the menu, click in **Update Settings** and update settings.

2.1.3 Testing email

- From the workstation **wkst1** on the **network2**, open Outlook express and write an email to **filipe@ipbrick.pt**.
- From the workstation **posto1** on the **network1**, open Outlook express and check if you received the email. View the email source code to see through which server this email has been relayed.
- From the workstation **wkst1** on the **network2**, open a web browser on put **http://webmail.ipbrick.pt**. Login: **filipe** and password: **123456**.
- Conclusion?

2.2 VPN SSL

In this section, we will show how we can access office information from internet through a secure tunnel. In other words, we will prove it's possible to work out of the office like as if there.

2.2.1 VPN SSL on the server

- From the workstation **posto1** on **network1**, open a web browser and go to **https://192.168.1.254**.
Login: **admin** and password: **123456**
- Access the menu **IPBrick.C – > VPN – > SSL**
- Click in **VPN SSL**
- In the **certificates** sections click in **insert** to create a certificate for the server. Fill the forms with the following information:

```
Country code: PT
Country:      portugal
City:         lisboa
Company:      ipbrick
Name:         server
Email:        admin@ipbrick.pt
```

- In the **certificates** sections click again in **insert** to create the first client certificate. Fill the forms with the following information:

Country code: PT
Country: portugal
City: lisboa
Company: ipbrick
Name: filipe
Email: filipe@ipbrick.pt
Password: ipbrick
Retype Password: ipbrick

- In the **definitions** sections click in **modify** to configure the vpn ssl service. Fill the forms with the following information:

Name / IP: 63.23.69.50
Port: 1194
Protocol: udp
VPN Network: 10.10.10.0 / 24
Domain: ipbrick.pt
DNS Servers: 192.168.1.1
Netbios Servers: 192.168.1.1
Routes for clients: 192.168.1.0 / 24

- Download the client certificate to the workstation.
- In the menu, click in **Update Settings** and update settings.
- In the menu, access **Advanced Settings** – > **System Vital** – > **Services**
- Select **VPN - SSL** service, enable it and put it as automatic start.
- Open Outlook express and write an email to **filipe@ipbrick.pt** with the vpn ssl config.

2.2.2 VPN SSL on the client

- From the workstation **wkst1** on **network2**. Access **http://webmail.ipbrick.pt** with a web browser. Login: **filipe** and password: **123456**
- Save the certificate to the workstation in C:\Program Files\OpenVPN\config.
- Uncompress the file to the same directory.
- Establish the vpn.

2.2.3 Testing VPN SSL

- ping remote communication server, intranet and workstation.
- Try access some application, ex: **https://192.168.1.254**, user account on intranet server.
- Conclusion?

2.3 Proxy

Finally, in this section, we will show how to control the web access. In this example, we will configure full access for the administration, restrict access for the technicians and block everything for the others.

2.3.1 Proxy configuration

- From the workstation **post01** on **network1**, open a web browser on **https://192.168.1.254**.
Login: **admin** and password: **123456**
- Access the menu **IPBrick.C** – > **Proxy** – > **settings**
- Select **transparent proxy** and click **modify**.
- Click **settings**
- In **Source groups list** section insert a new group.
Name: `administration`
- **modify IP Ranges** and insert:
Start of range: `192.168.1.10`
End of range: `192.168.1.19`
- In **Source groups list** section insert a new group.
Name: `technician`
- **modify IP Ranges** and insert:
Start of range: `192.168.1.20`
End of range: `192.168.1.49`
- In **Destination groups list** section insert a new group.
Name: `valid`
- **modify Domains** and insert:
`ipbrick.com`
`www.iportalmais.pt`
`kernel.org`
`linux.com`
- Now to config access list, in **Access lists** section insert a new acl:
Source: `administration`
Destination
Available Groups:
Blacklists:
Period: `not defined`
Policy: `accept`
- In **Access lists** section insert a new acl:
Source: `technician`
Destination
Available Groups: `only in valid`
Blacklists:
Period: `not defined`
Policy: `accept`
- In the menu, click in **Update Settings** and update settings.

2.3.2 Testing Proxy

- Configure the workstation **post01** on **network1** with the network data:

```
IP:          192.168.1.10
NETMASK:     255.255.255.0
GATEWAY:     192.168.1.254
DNS:         192.168.1.1
```

and try to access some sites. Ex: www.google.com, www.ipbrick.com

- Configure the workstation **post01** on **network1** with the network data:

```
IP:          192.168.1.20
NETMASK:     255.255.255.0
GATEWAY:     192.168.1.254
DNS:         192.168.1.1
```

and try to access some sites. Ex: www.google.com, www.ipbrick.com

- Configure the workstation **post01** on **network1** with the network data:

```
IP:          192.168.1.50
NETMASK:     255.255.255.0
GATEWAY:     192.168.1.254
DNS:         192.168.1.1
```

and try to access some sites. Ex: www.google.com, www.ipbrick.com

- Conclusion?