FAE

São José dos Pinhais

Detecção de Intrusos PR.GOV.BR

Hermano Pereira

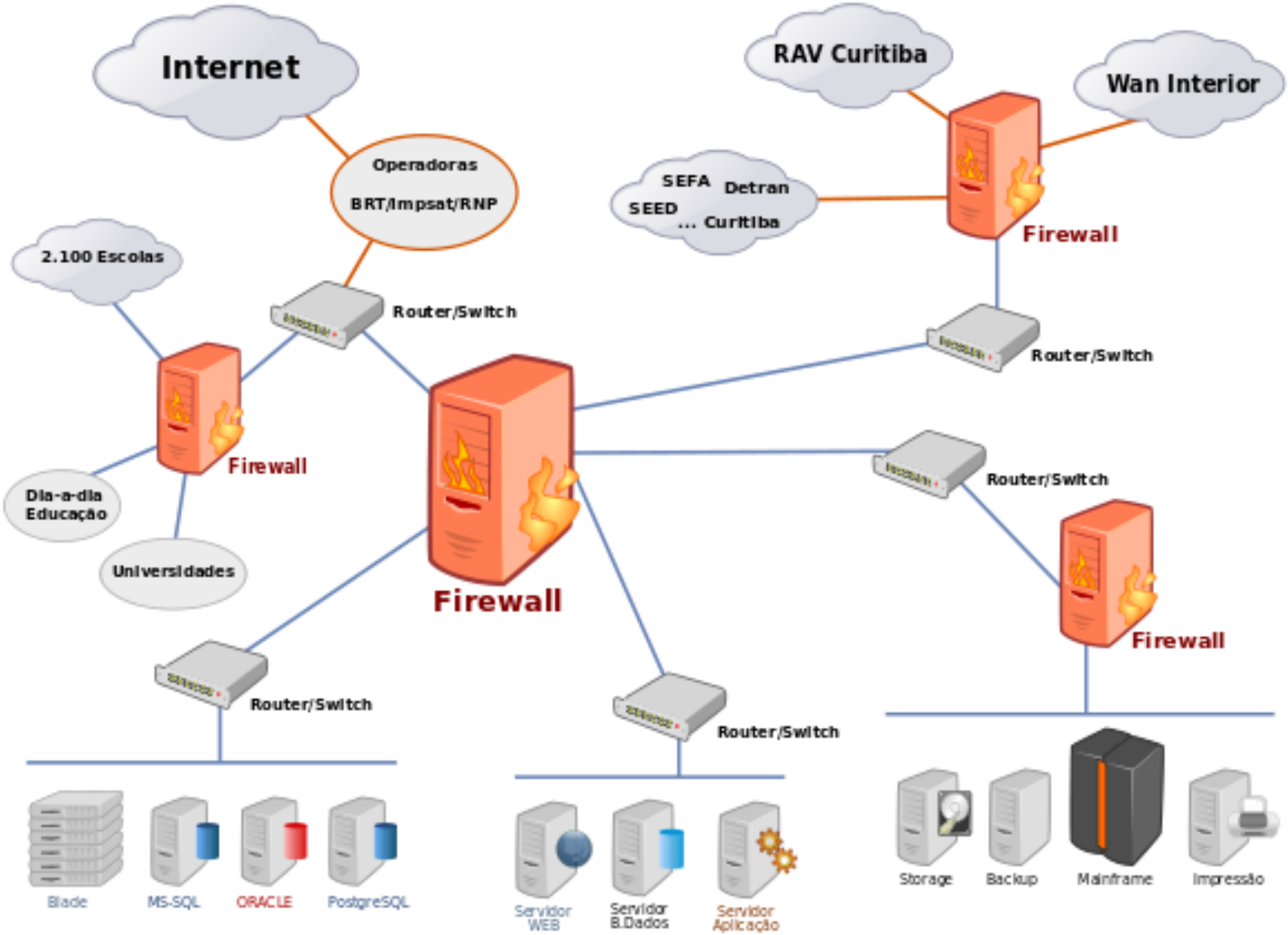
Agenda

- Segurança na Rede PR.GOV.BR
- Sistemas de Detecção de Intrusão
- Segurança da Informação e Gerência de Eventos
- Soluções da Equipe de Segurança
- Algumas Estatísticas
- Projetos em Andamento
- Considerações Finais

Segurança na Rede PR.GOV.BR

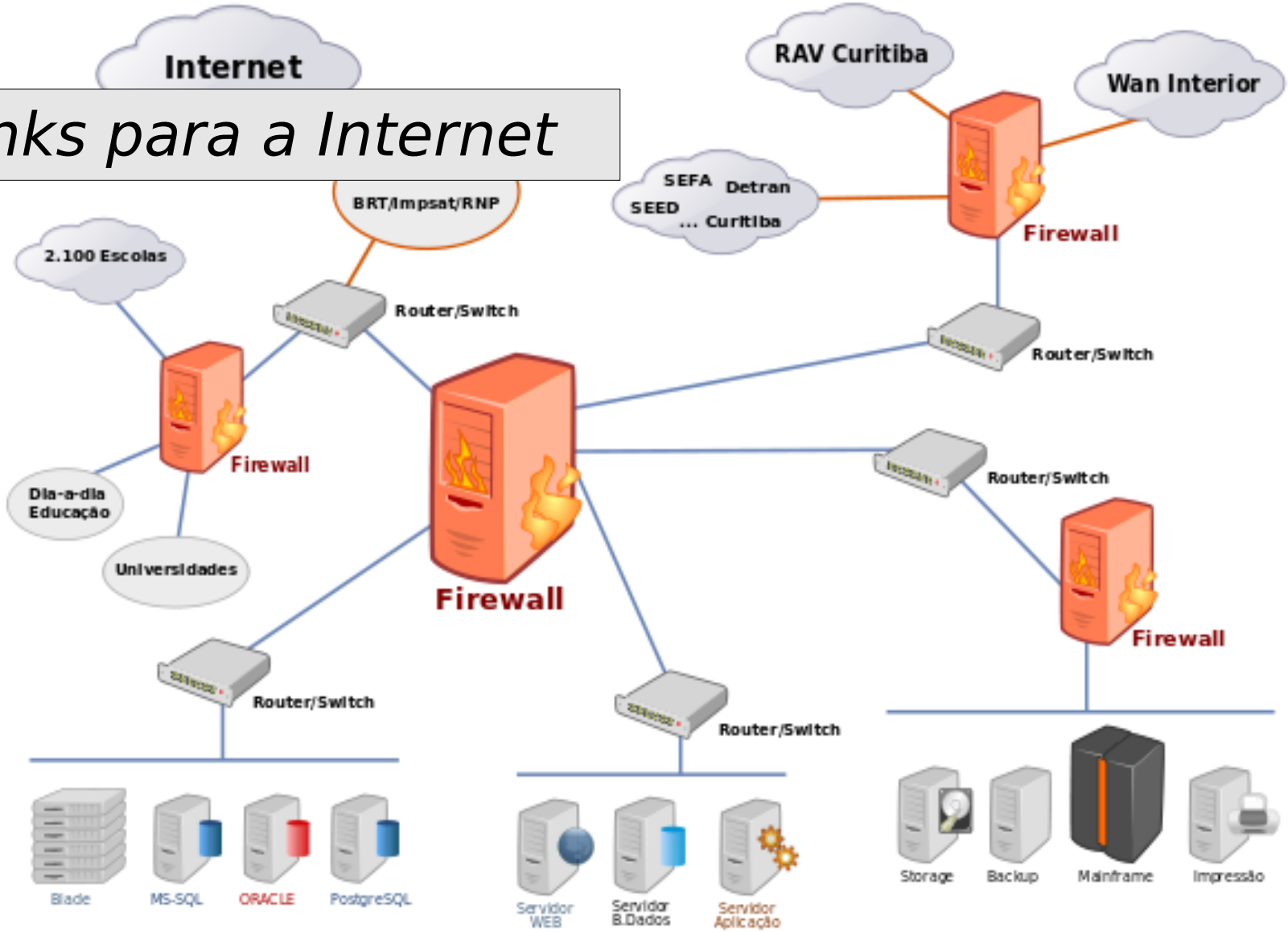
- CELEPAR
  - Companhia de Informática do Paraná
  - Economia Mista (Governo do Paraná)
  - Clientes: DETRAN, SEFA, SESA, SEED ...

Segurança na Rede PR.GOV.BR



Segurança na Rede PR.GOV.BR

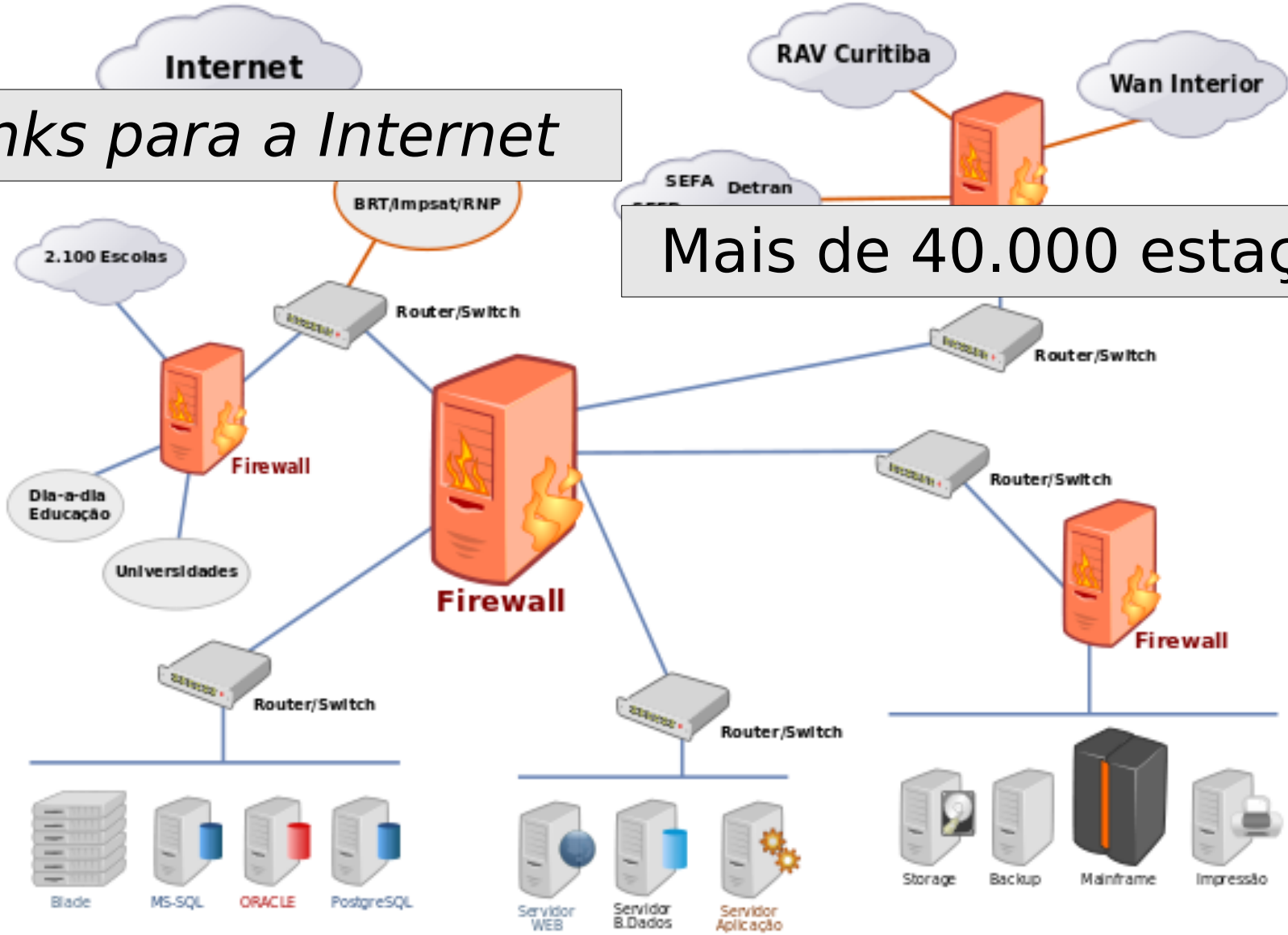
3 *links para a Internet*



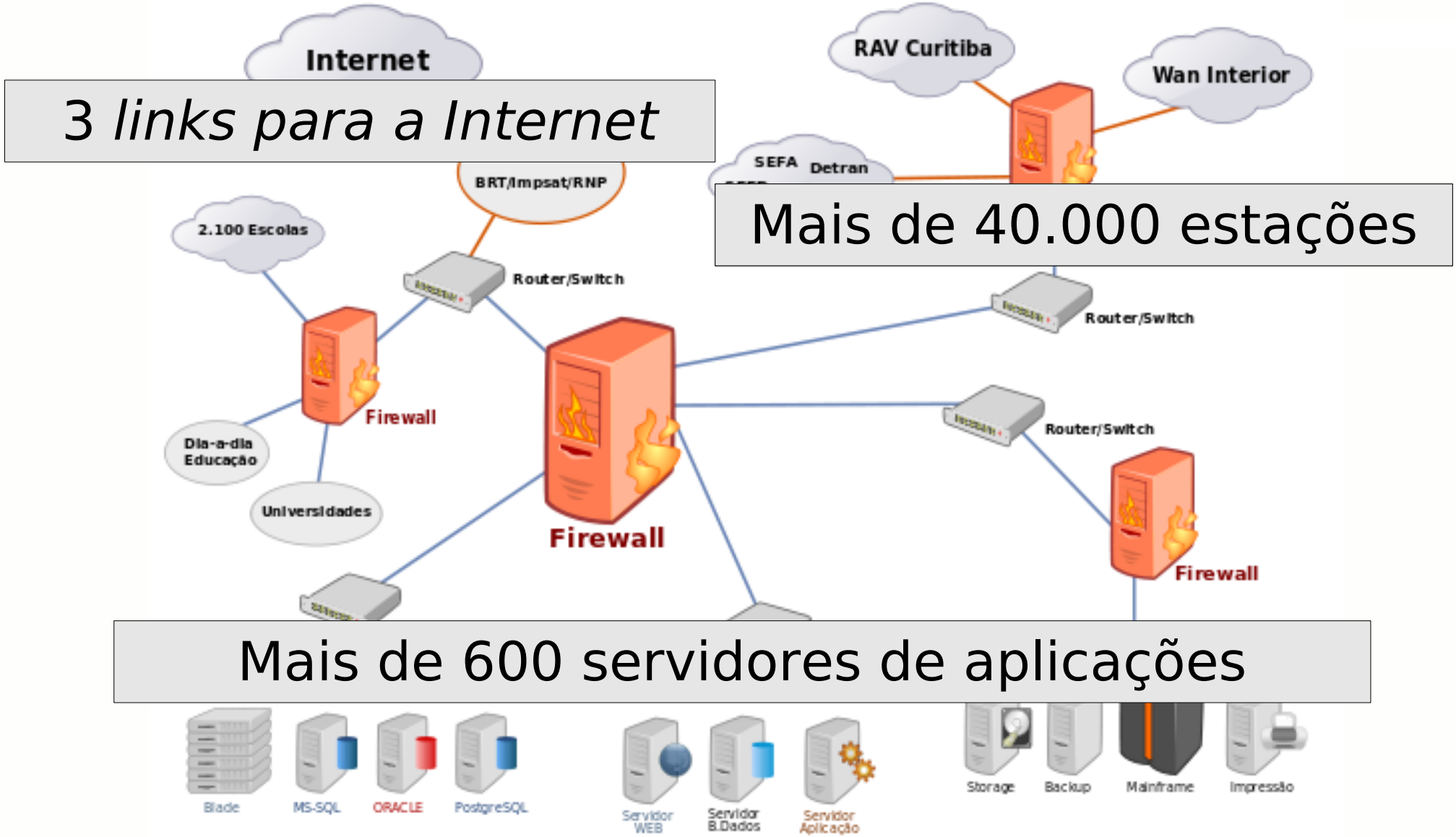
Segurança na Rede PR.GOV.BR

3 *links para a Internet*

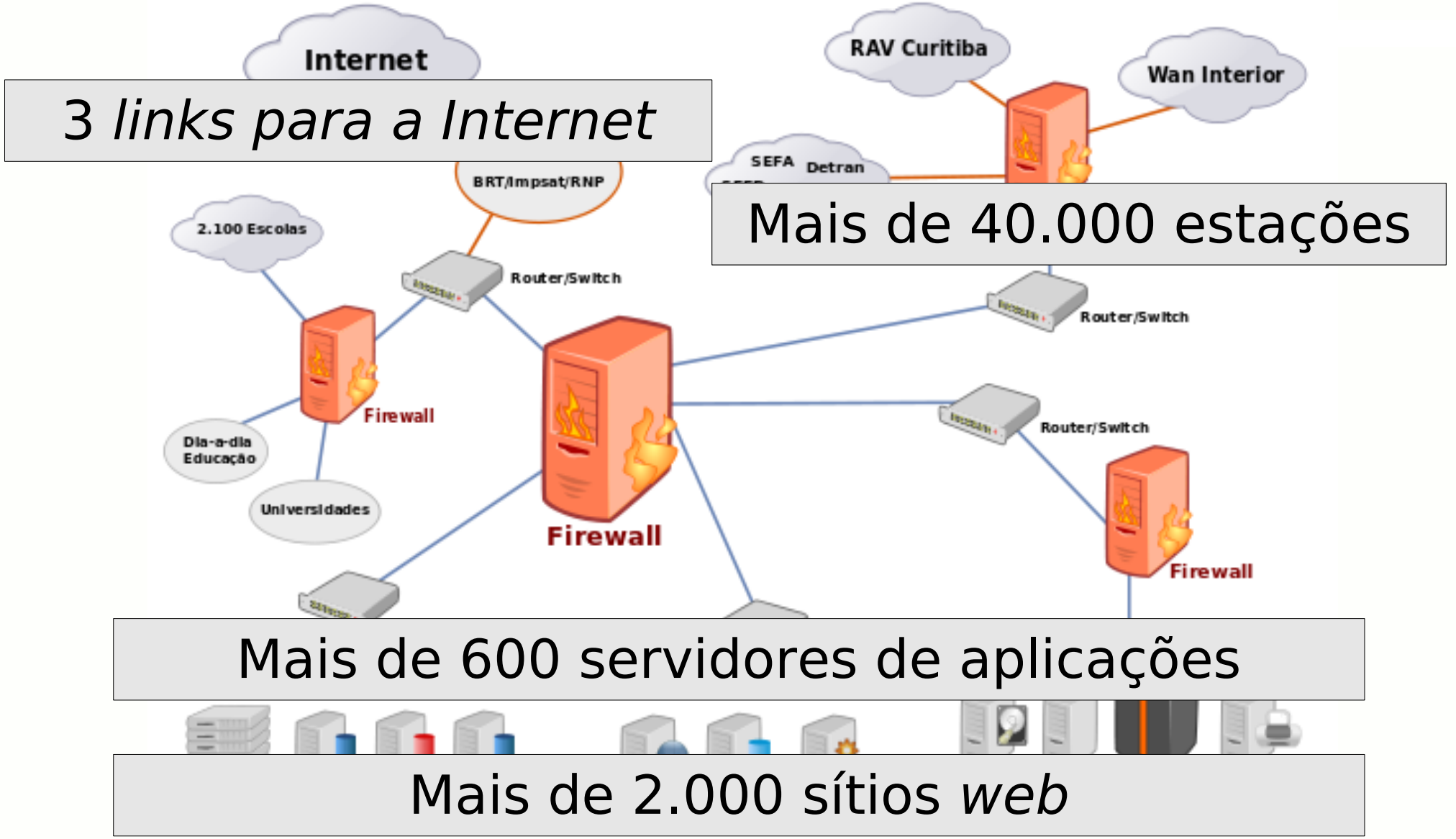
Mais de 40.000 estações



Segurança na Rede PR.GOV.BR

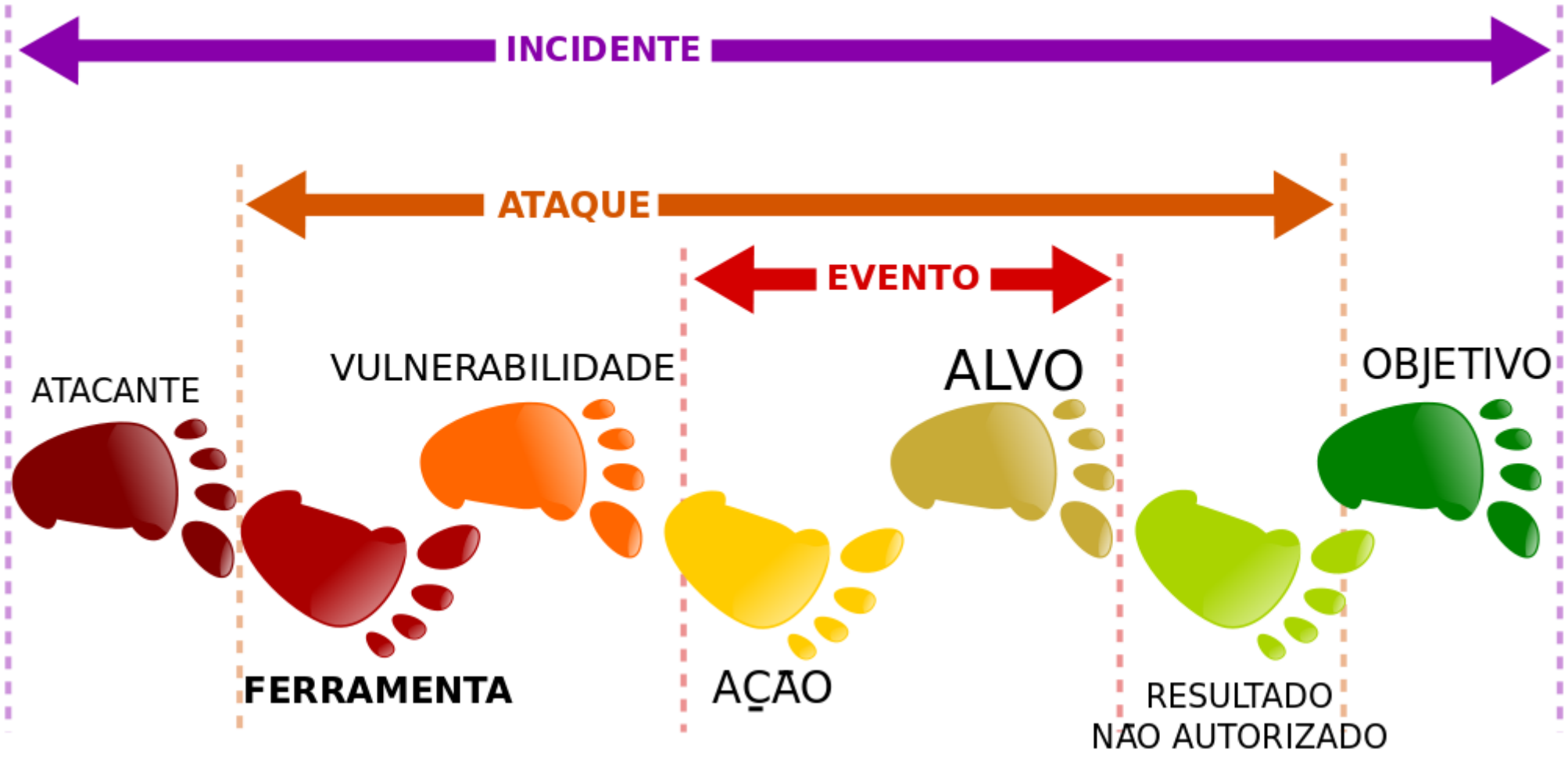


Segurança na Rede PR.GOV.BR

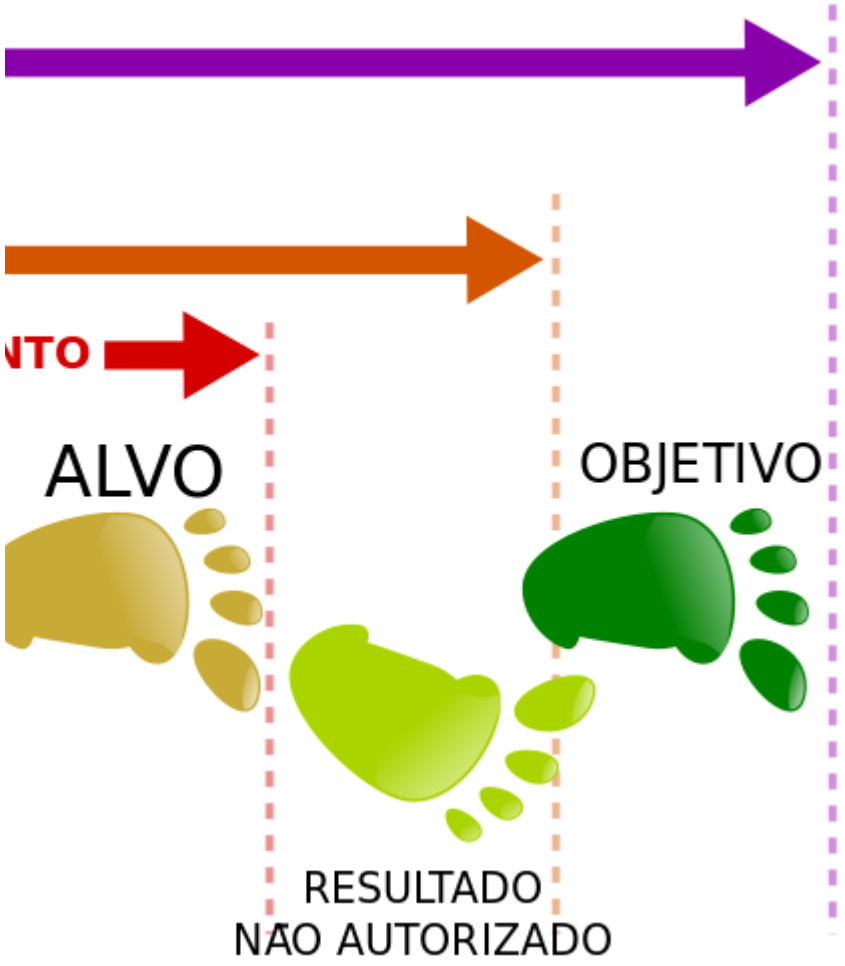


- Necessidade de Detecção de Intrusão:

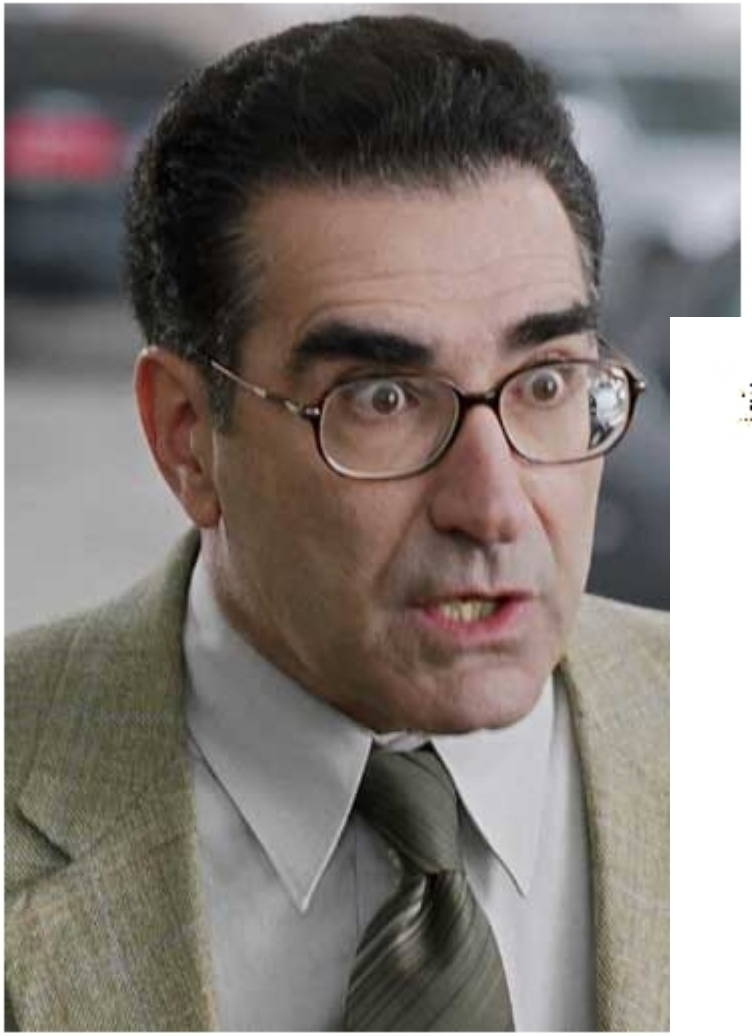
Intrusão


INCIDENTE
ATAQUE
EVENTO
ATACANTE
VULNERABILIDADE
ALVO
OBJETIVO
FERRAMENTA
AÇÃO
RESULTADO
NÃO AUTORIZADO

OWNED BY [redacted]

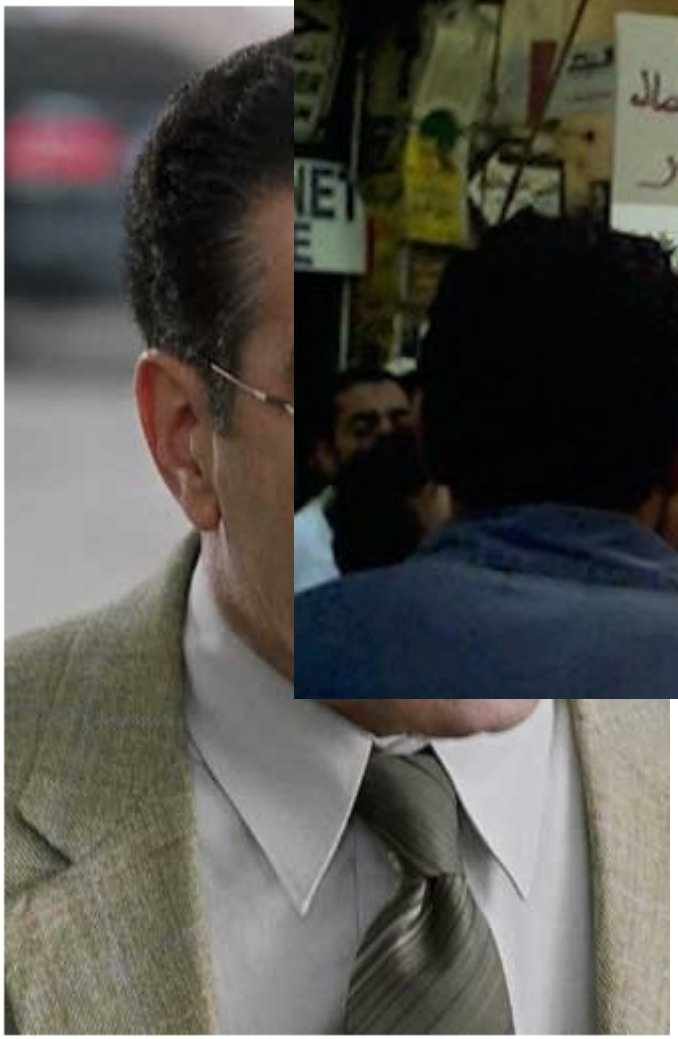


OWNED BY [redacted]o



Admin...."Não contavam com minha astúcia!"

OWNED BY [redacted]



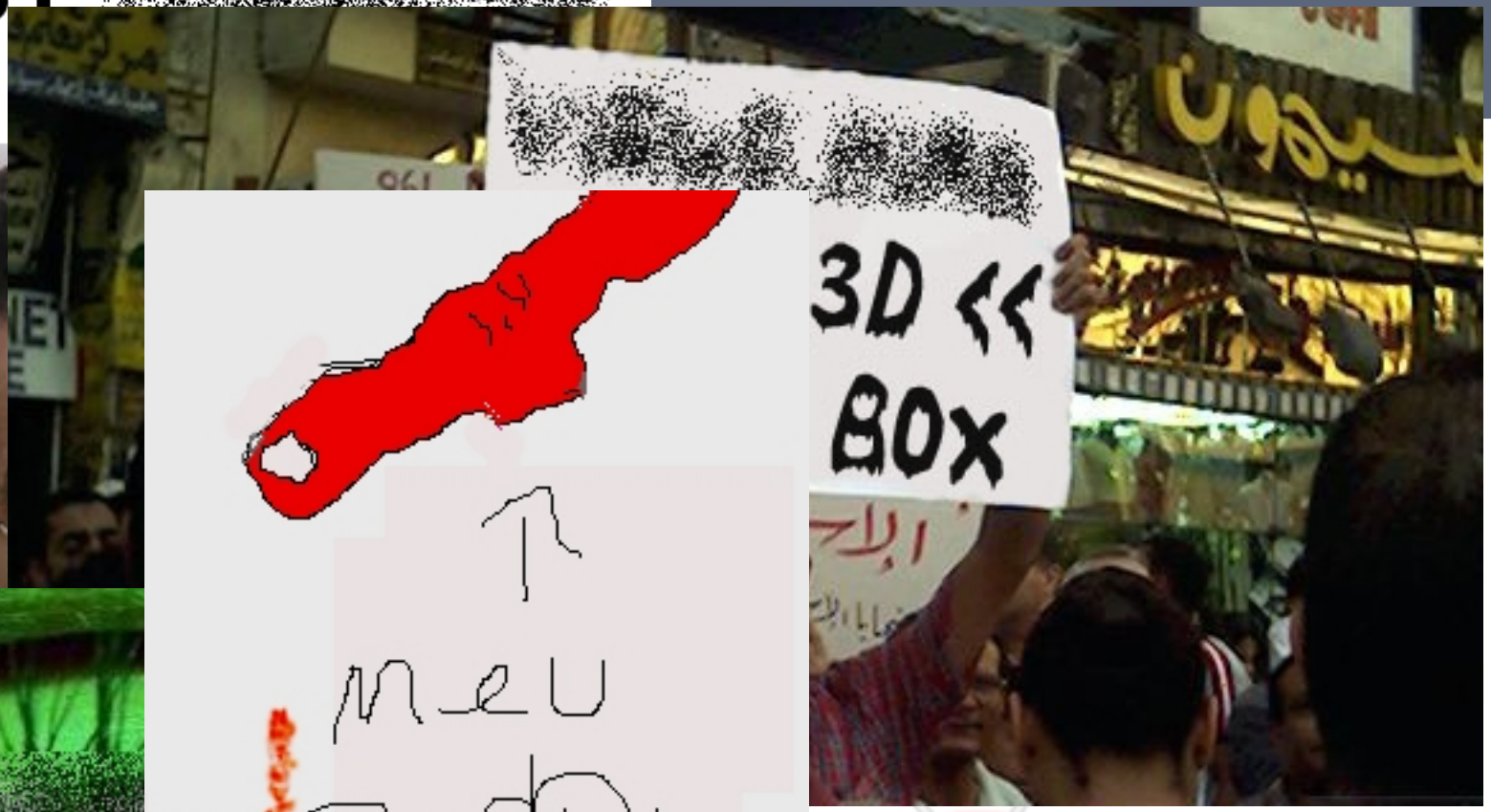
DETECÇ[redacted]

Admin...."Não contavam com minha astúcia!"

OWNED BY [redacted]

...atavam com minha astúcia!"

OWNED BY



ntavam com minha astúcia!"

OWNED BY

Software: Apache/2.2.9 (Debian) with Suhosin-Patch mod_perl/2.0.4 Perl/v5.10.0
System: Linux ecelepar14618 2.6.26-2-686 #1 SMP Mon Jun 21 05:58:44 UTC 2010 i686
User/Group: root/www-data
Php version: 5.2.6-1+lenny8
Php modules: ftp, sockets
Install program: gcc, cc, ld, php, perl, python, ruby, make, tar, nc, wget, links, curl, lwp-mirror, lwp-download
Allow_url_fopen: ON
Allow_url_include: OFF
Safe-mode: OFF (not secure)
/var/www/phpshell/ drwxr-xr-x
Free 8.14 GB of 18.62 GB (43.7%)

Search PHP-code Self remove

Listing folder (2 files and 0 folders):

Name	Size	Modify	Owner/Group	Perms	Action
.	LINK	10.08.2010 14:49:55	root/root	drwxr-xr-x	
..	LINK	10.08.2010 14:47:29	root/root	drwxr-xr-x	
0h94k.php	40.19 KB	10.08.2010 14:47:32	root/root	-rwxr-xr-x	E D X
decoded1.php	103.4 KB	10.08.2010 14:49:55	root/root	-rw-r--r--	E D X

Select all | Unselect all | With selected: | Confirm

:: Command execute ::

:: Enter :: cat /etc/passwd Execute

:: Select :: find .bash_history files in current dir Execute

:: Working with Archives ::

:: Option ::
Use system unpack:
Acceptable formats archives: zip, tgz, tar.gz, tar.gzip, tar.bz2, tbz2, tb2, tbz, tar
Number of archives in this folder: (0)

:: Select :: /var/www/phpshell/ Unarchive

tavam com minha astúcia!"

New to Online

SECURITY GUARANTEE

Complete our easy registration process.
Click on the relevant button below:

Stage 1: Register my details — Start registration

Stage 2: I've received my temporary password — Complete registration

Employee Share Scheme Customers
Register for Employee Share Schemes

Sign In

Username

Password

The name of your first school?

Sign in

Remember my username*

*Do not select if this computer is used by anyone else. More information about storing usernames

Useful info

Find out how Online works using our demo
Why use Online Banking?
Apply for a new account

Problem signing in?

Forgotten sign in details / access suspended?
Service availability
Are your phone details up to date?

Softwar
System
User/G
Php ver
Php mo
Install
Allow_u
Allow_u
Safe-m
/var/w
Free 8.

Search

Name					Action
.	LINK	10.08.2010 14:49:55	root/root	drwxr-xr-x	
..	LINK	10.08.2010 14:47:29	root/root	drwxr-xr-x	
0h94k.php	40.19 KB	10.08.2010 14:47:32	root/root	-rwxr-xr-x	E D X
decoded1.php	103.4 KB	10.08.2010 14:49:55	root/root	-rw-r--r--	E D X

Select all | Unselect all | With selected: | Confirm

:: Command execute ::

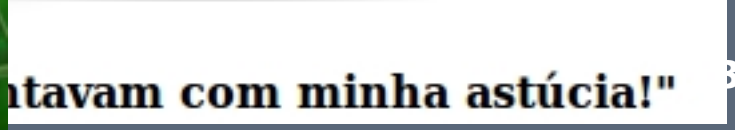
:: Enter ::
cat /etc/passwd — Execute

:: Select ::
find .bash_history files in current dir — Execute

:: Working with Archives ::

:: Option ::
Use system unpack:
Acceptable formats archives: zip, tgz, tar.gz, tar.gzip, tar.bz2, tbz2, tb2, tbz, tar
Number of archives in this folder: (0)

:: Select ::
/var/www/phpshell/
Unarchive



New to Online

SECURITY GUARANTEE

Complete our easy registration process.
Click on the relevant button below:

Stage 1: Register my details — Start registration

Stage 2: I've received my temporary password — Complete registration

Employee Share Scheme Customers
Register for Employee Share Schemes

Useful info

Find out how Online works using our demo
Why use Online Banking?
Apply for a new account

Sign In

Username

Password

The name of your first school?

Sign in

Remember my username*

Welcome to Internet Banking

To update your profile please enter your 6-digit sortcode
8-digit account number 16-digit Visa card number and your Security Code.

Sort code

Account number

Visa credit card number

Please enter your 4-digit security code and click OK.

Security code

Name		
.	LINK	10.08.201
..	LINK	10.08.201
0h94k.php	40.19 KB	10.08.201
decoded1.php	103.4 KB	10.08.201

:: Command execute ::

:: Enter ::
cat /etc/passwd Execute

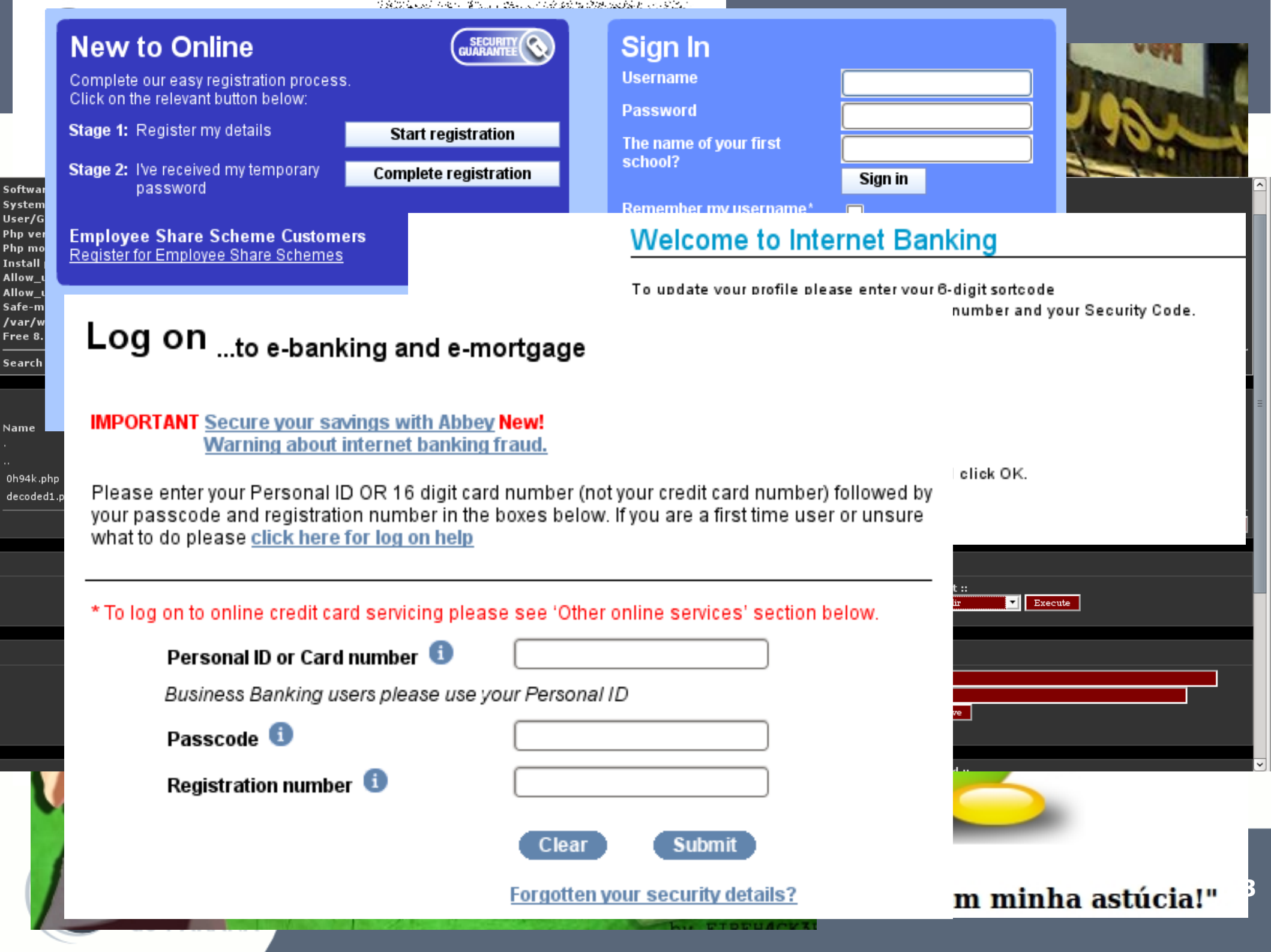
:: Select ::
find .bash_history files in current dir Execute

:: Working with Archives ::

:: Option ::
Use system unpack:
Acceptable formats archives: zip, tgz, tar.gz, tar.gzip, tar.bz2, tbz2, tb2, tbz, tar
Number of archives in this folder: (0)

:: Select ::
/var/www/phpshell/
Unarchive

tavam com minha astúcia!"


New to Online
SECURITY GUARANTEE
Complete our easy registration process.
Click on the relevant button below:
Stage 1: Register my details
Start registration
Stage 2: I've received my temporary password
Complete registration
Employee Share Scheme Customers
Register for Employee Share Schemes
Sign In
Username
Password
The name of your first school?
Sign in
Remember my username*
Welcome to Internet Banking
To update your profile please enter your 6-digit sortcode
number and your Security Code.
click OK.
Log on ...to e-banking and e-mortgage
IMPORTANT Secure your savings with Abbey New!
Warning about internet banking fraud.
Please enter your Personal ID OR 16 digit card number (not your credit card number) followed by your passcode and registration number in the boxes below. If you are a first time user or unsure what to do please click here for log on help
* To log on to online credit card servicing please see 'Other online services' section below.
Personal ID or Card number
Business Banking users please use your Personal ID
Passcode
Registration number
Clear
Submit
Forgotten your security details?
Execute
m minha astúcia!"

New to Online

Complete our easy registration process.
Click on the relevant button below:

Stage 1: Register my details — **Start registration**

Stage 2: I've received my temporary — **Complete registration**

Sign In

Username

Password

The name of your first school?

Sign in

403 Forbidden - Iceweasel

Arquivo Editar Exibir Histórico Favoritos Ferramentas Ajuda

http://www.google.com.br/sorry/?continue=http://www.google.com.br/search%3Fhl%3Dpt-BR%26q%3D

Google

Gestão Operacional | Registration Service... | Inspect an IP | Proje... | User Agent and IP A... | Welcome to RIPE.NET | Lucas 21:14-15 - Je...

Google **Erro**

Desculpe...

... mas não é possível executar essa ação no momento. Estamos recebendo pedidos automatizados de conexão gerados por um vírus ou spyware, e aparentemente seu computador ou rede foram infectados.

Tente acessar essa página novamente dentro de alguns instantes. Ela voltará ao normal assim que possível. Neste ínterim, sugerimos que você use um aplicativo antivírus ou de detecção de spyware para checar se seu computador está livre de vírus e outros softwares predatórios.

Lamentamos o inconveniente. Esperamos sua que você volte ao Google em breve!

Para continuar pesquisando, digite os caracteres abaixo:

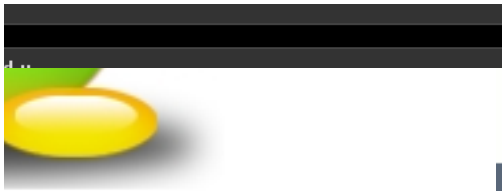
dersesse

Passcode

Registration number

Clear Submit

Forgotten your security details?

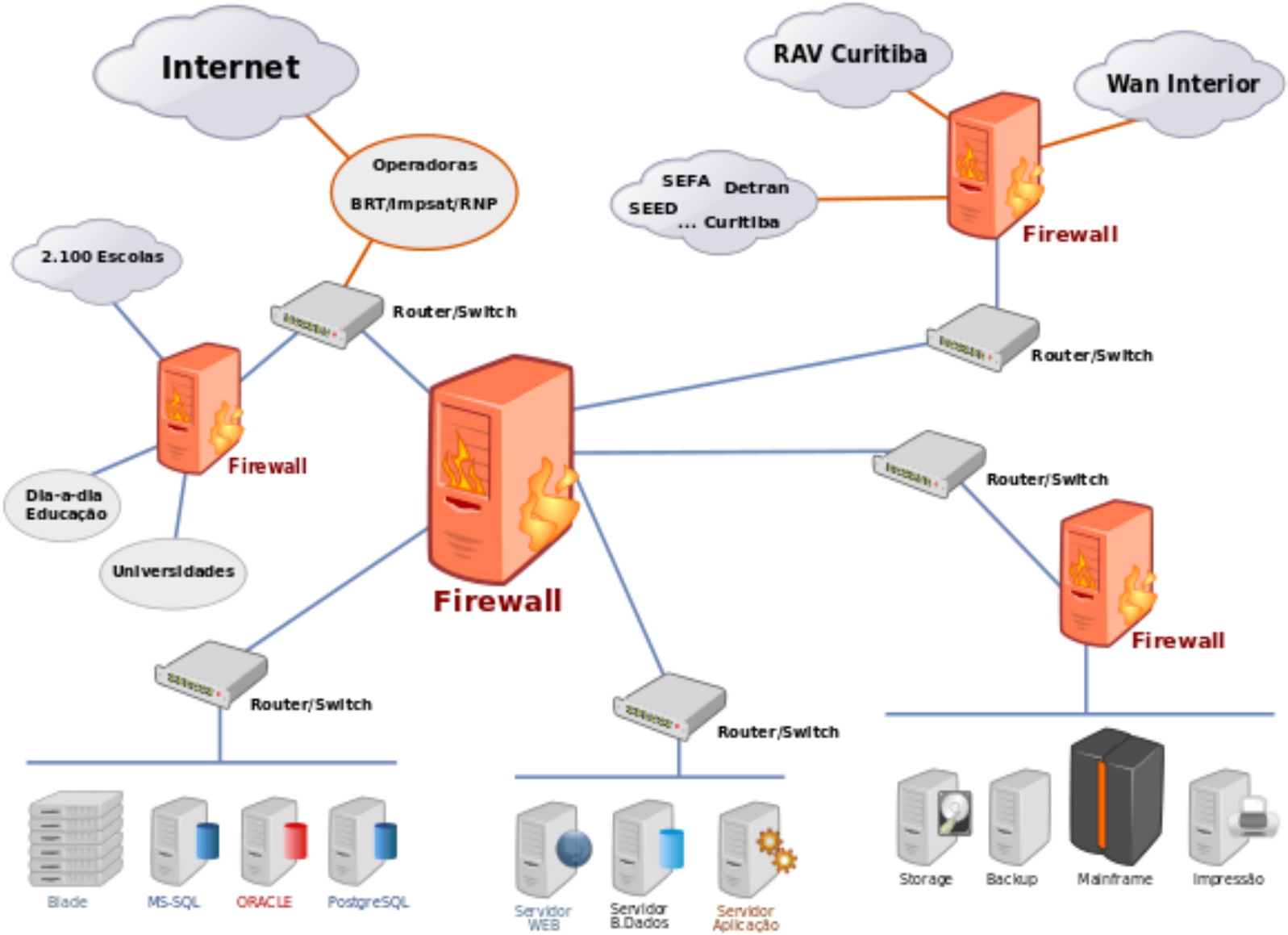


m minha astúcia!"

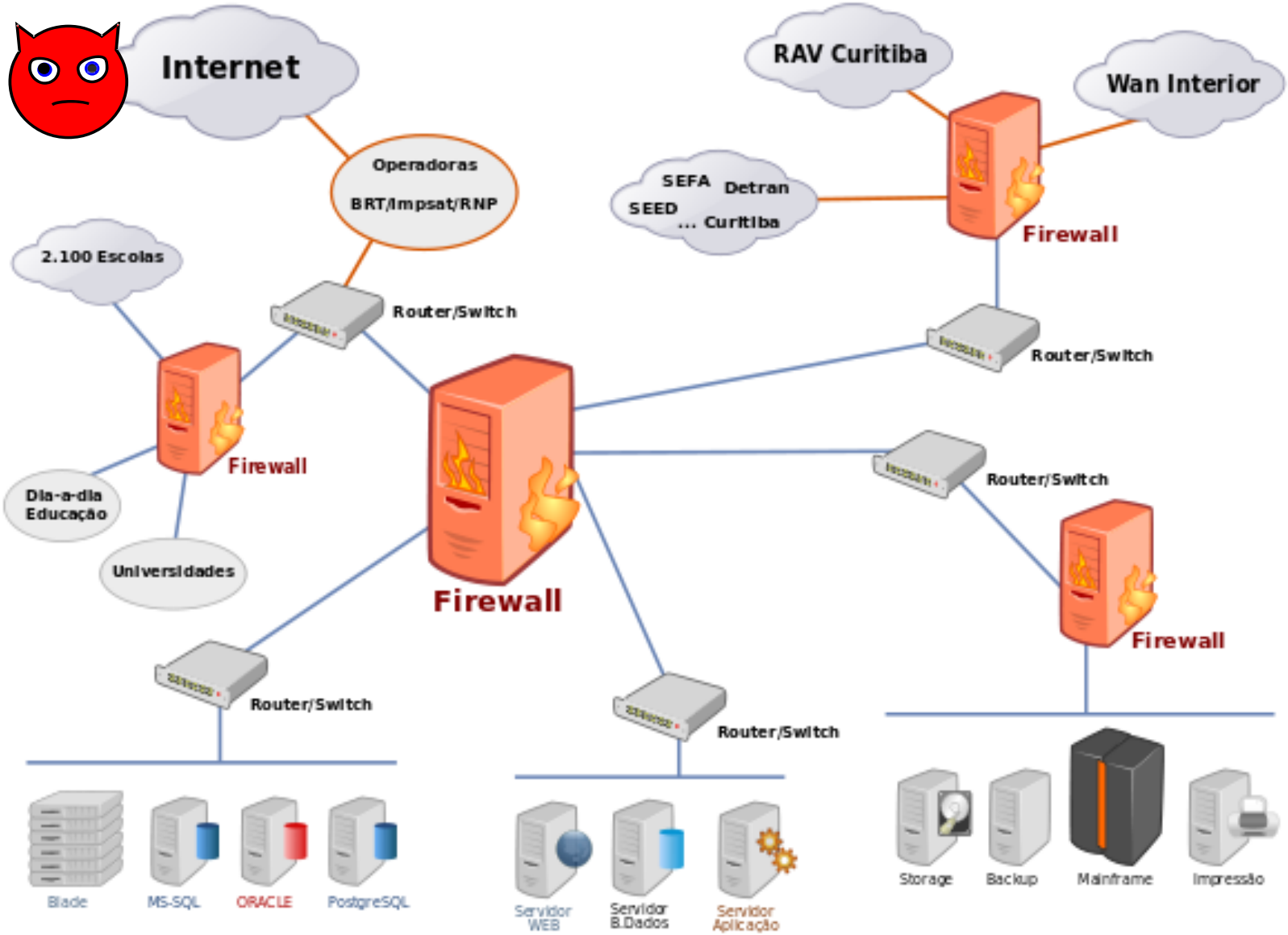
Segurança na Rede PR.GOV.BR

- Necessidade de Detecção de Intrusão:
  - Ativos da empresa
  - Imagem e Reputação
  - Dados dos clientes
  - Dados do cidadão
  - Vírus / SPAM
  - ...

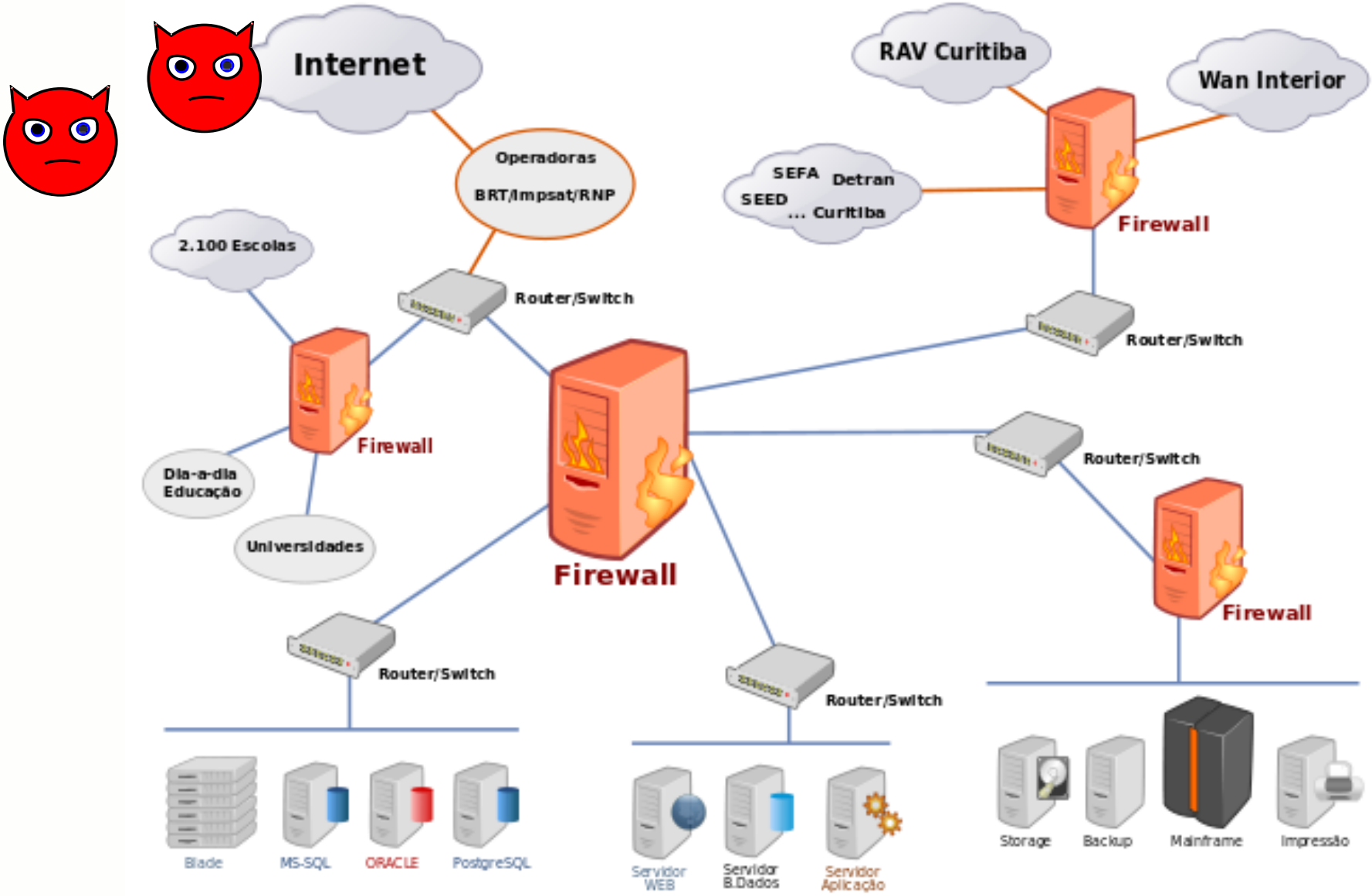
Segurança na Rede PR.GOV.BR



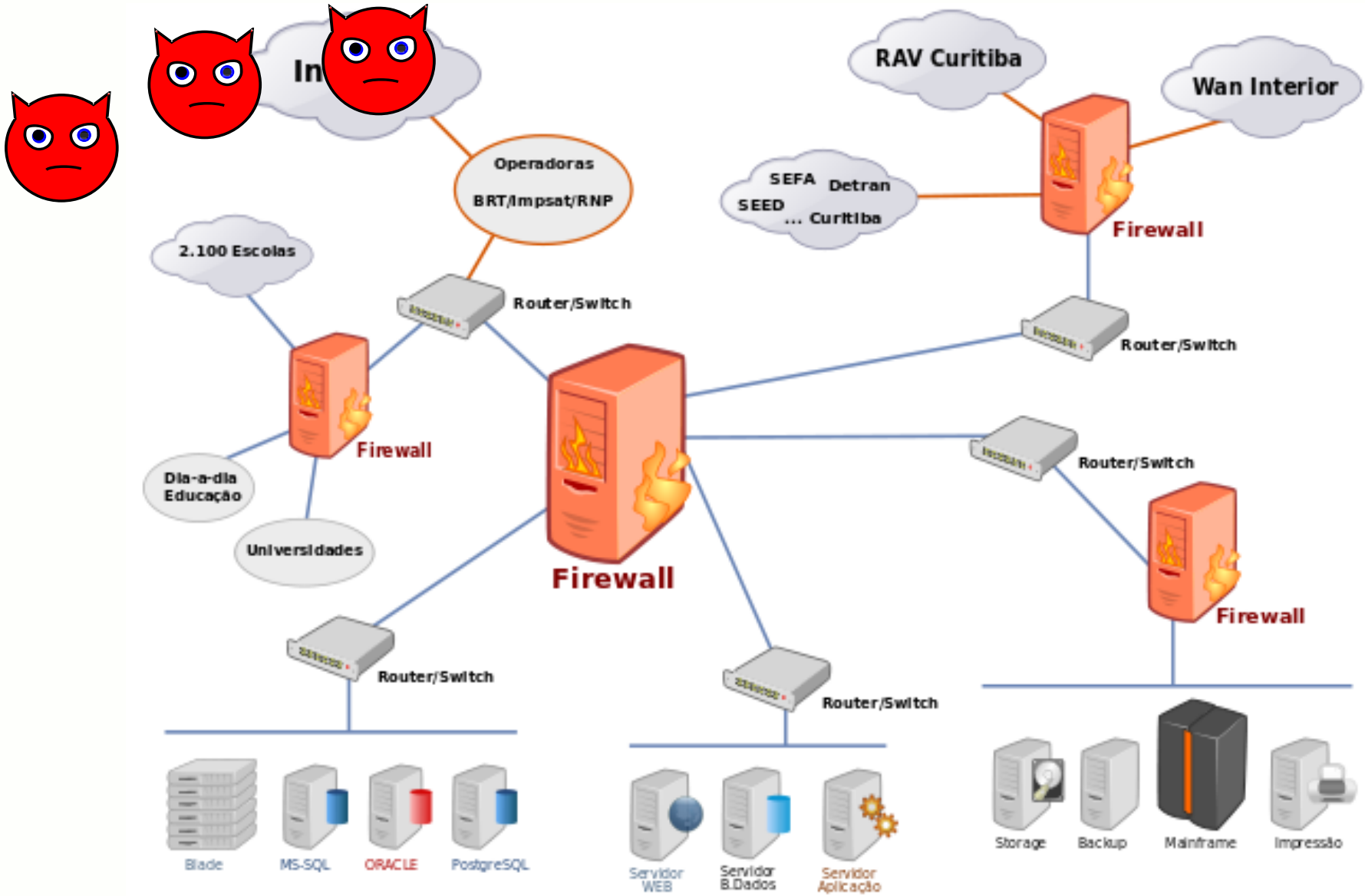
Segurança na Rede PR.GOV.BR



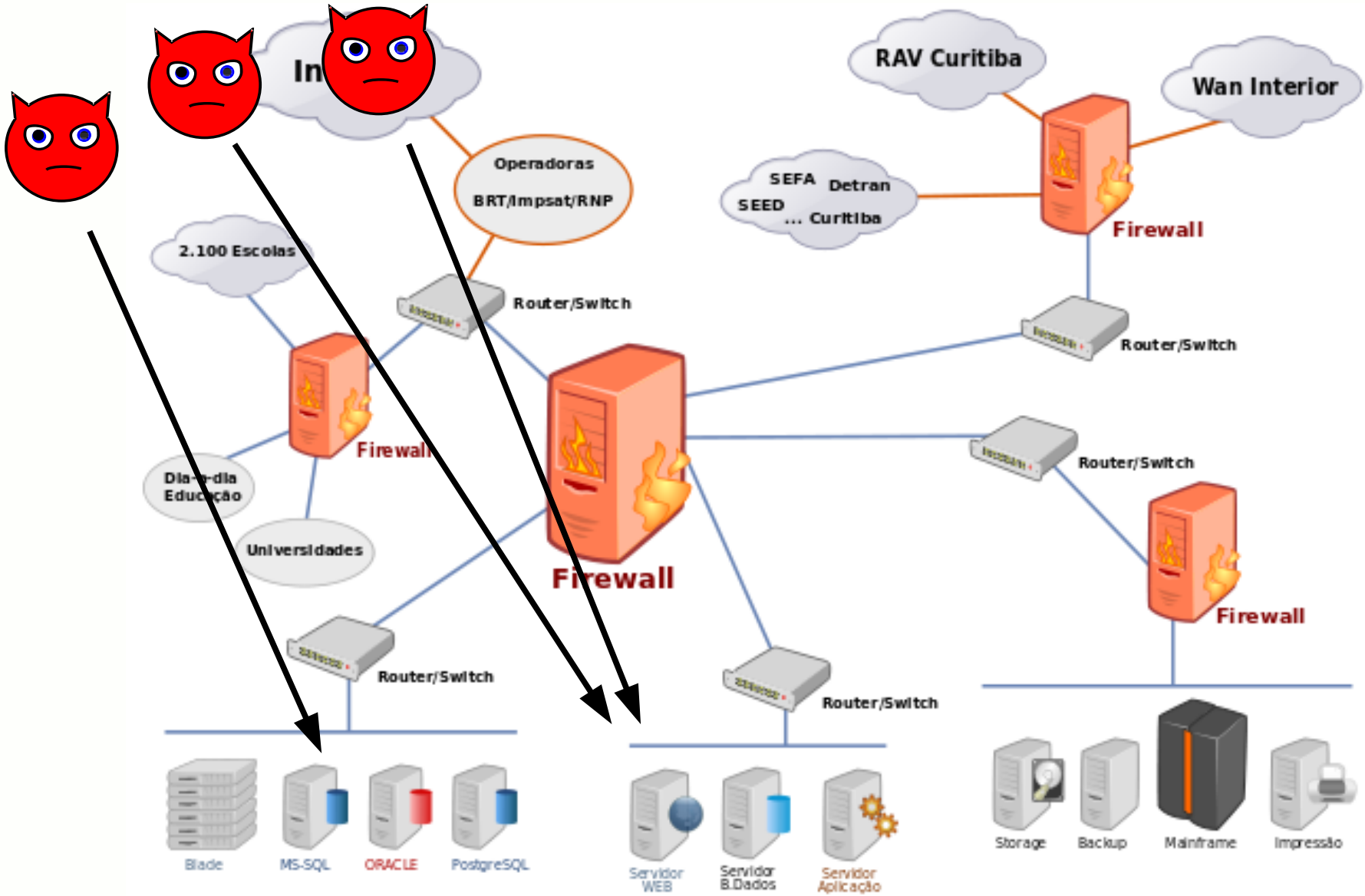
Segurança na Rede PR.GOV.BR



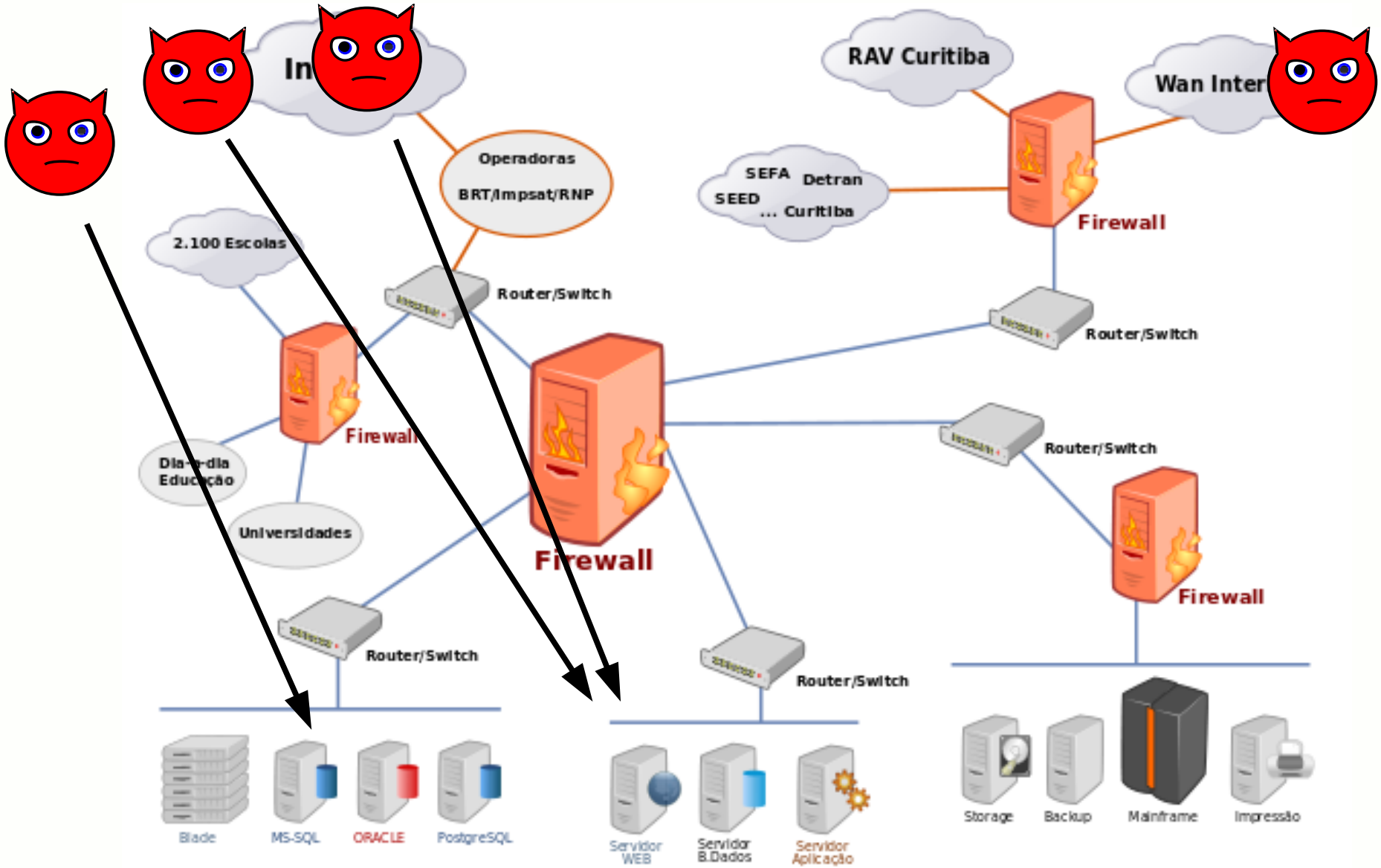
Segurança na Rede PR.GOV.BR



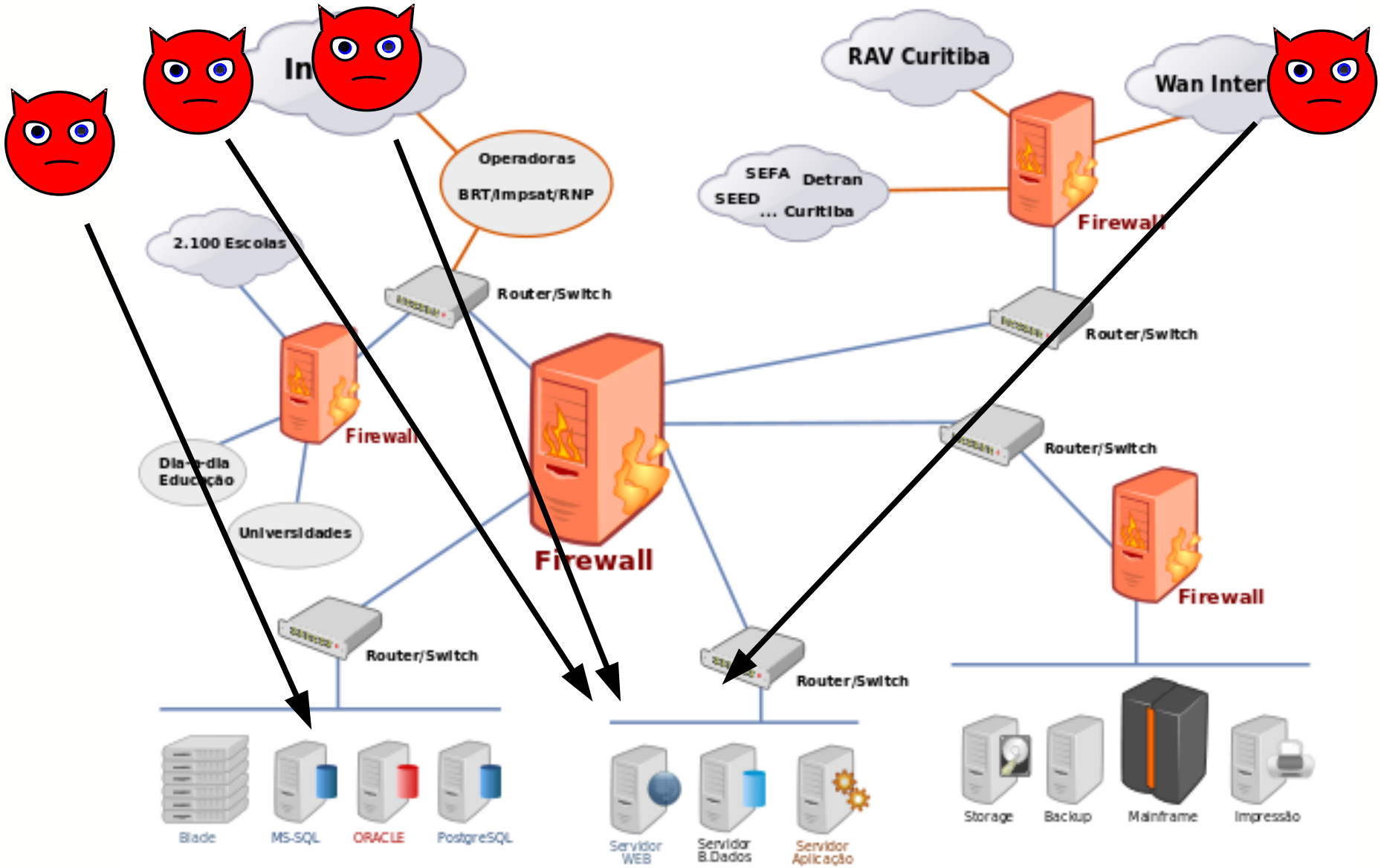
Segurança na Rede PR.GOV.BR



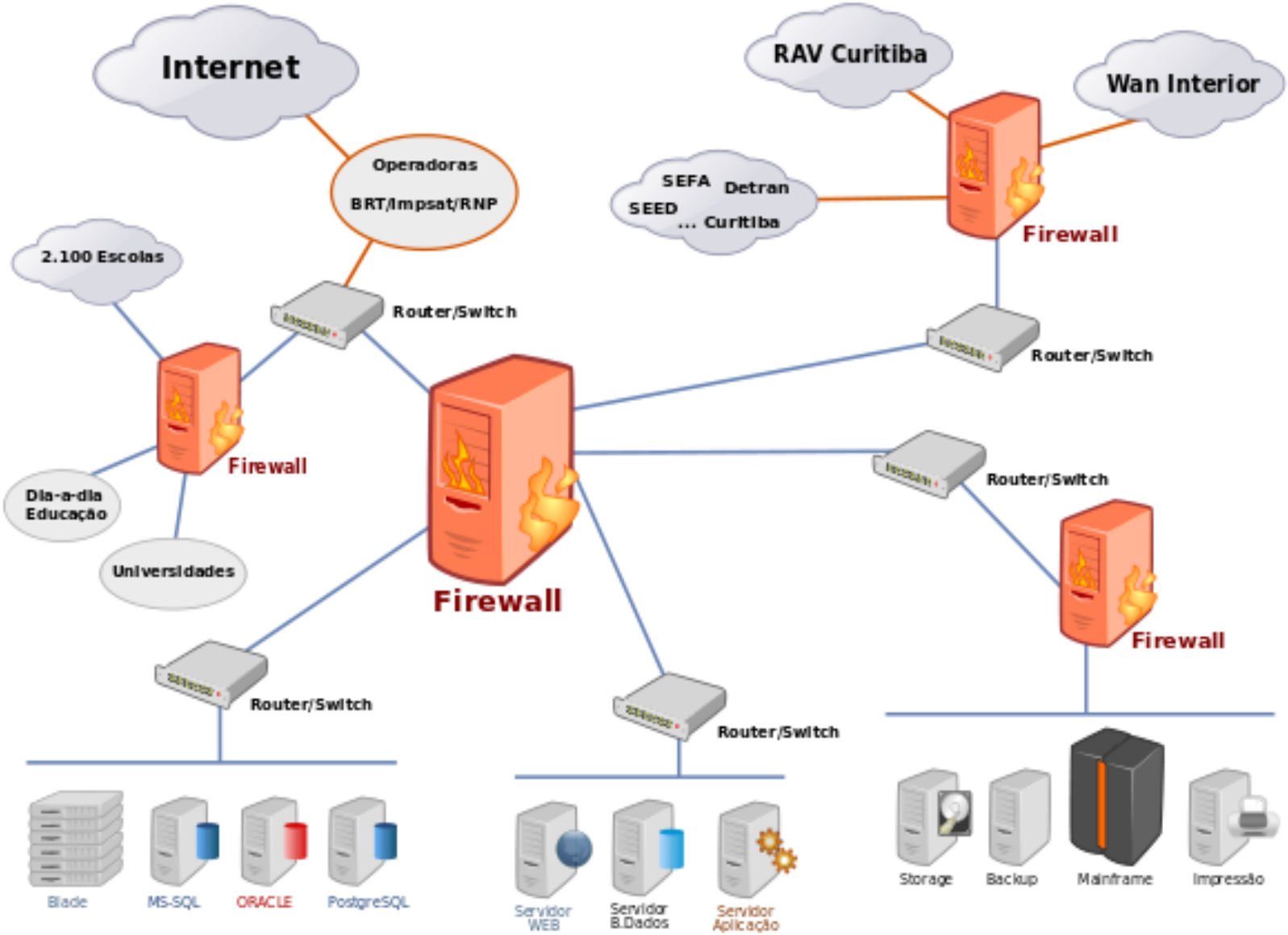
Segurança na Rede PR.GOV.BR



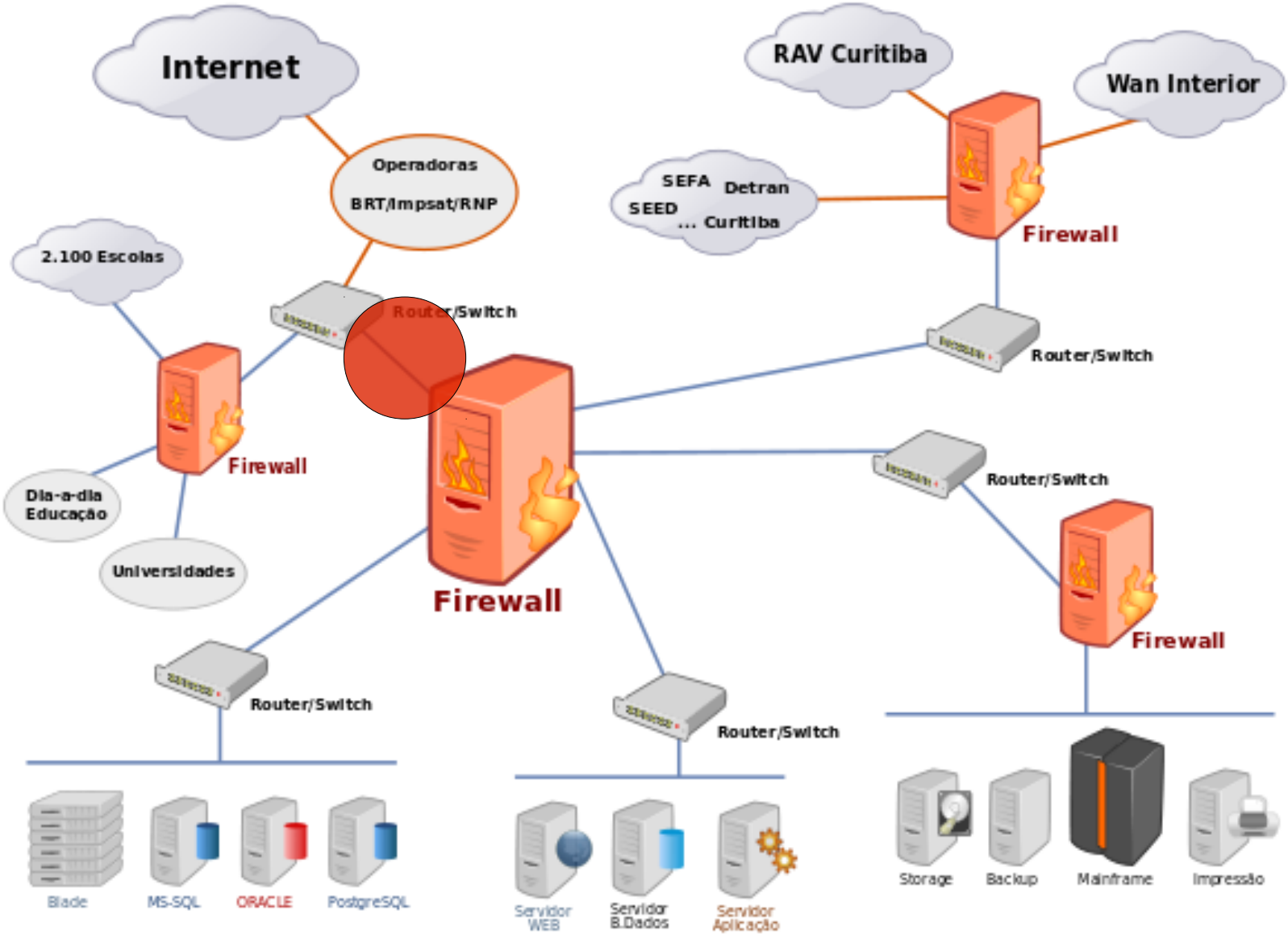
Segurança na Rede PR.GOV.BR



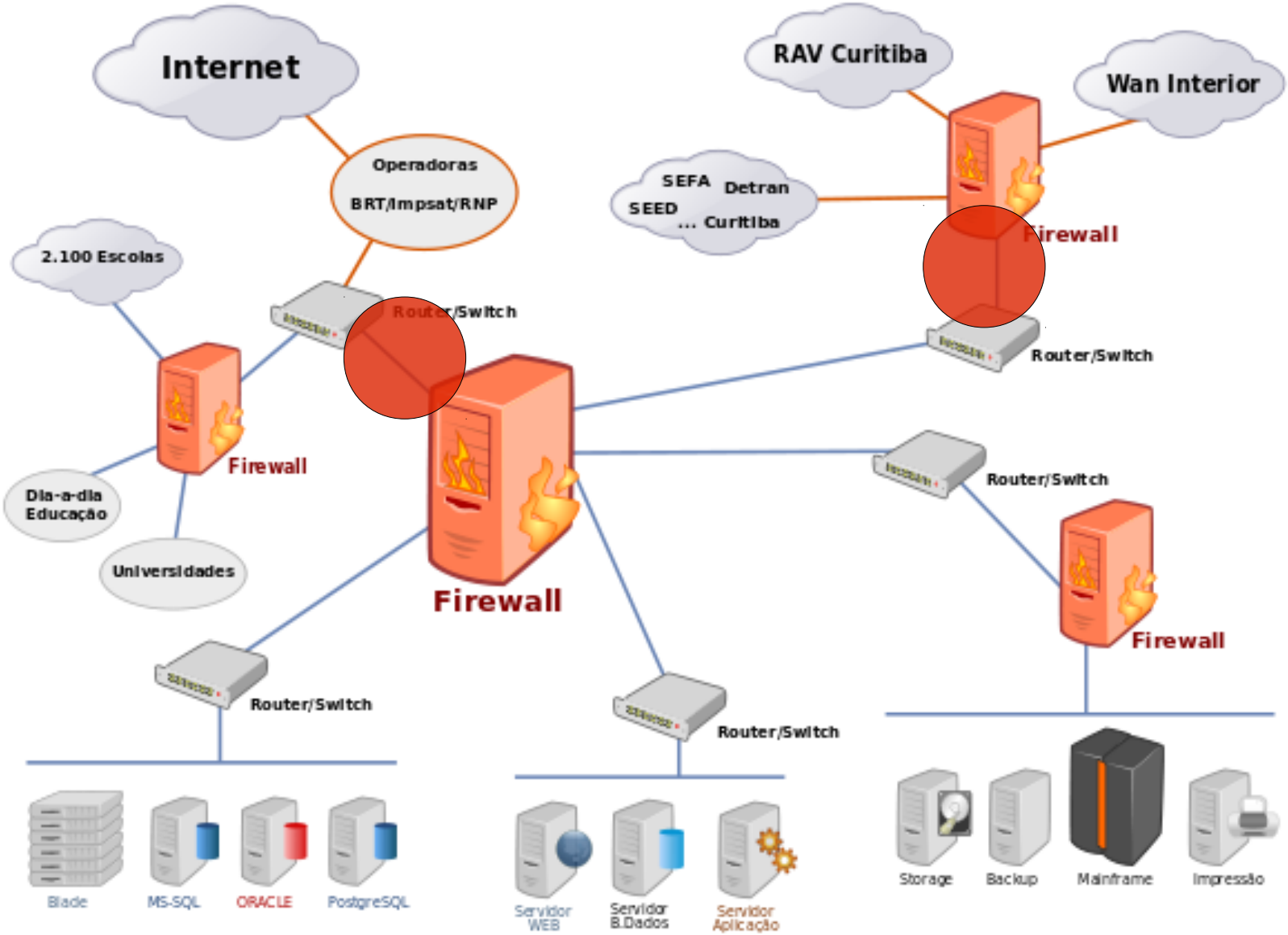
Segurança na Rede PR.GOV.BR



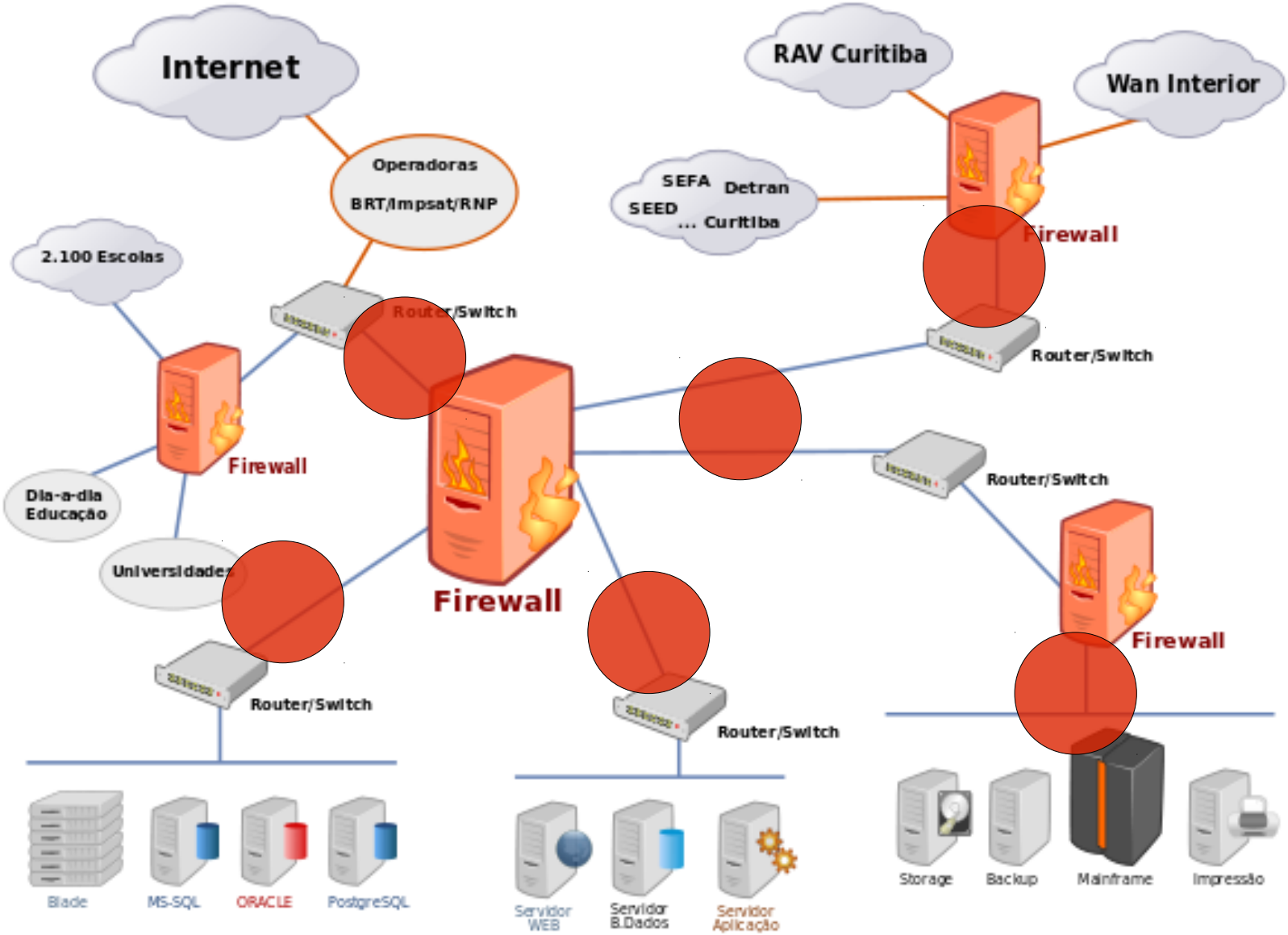
Segurança na Rede PR.GOV.BR



Segurança na Rede PR.GOV.BR



Segurança na Rede PR.GOV.BR



Sistemas de Detecção de Intrusão

CELEPAR
INFORMÁTICA
do PARANÁ

Sistemas de Detecção de Intrusão

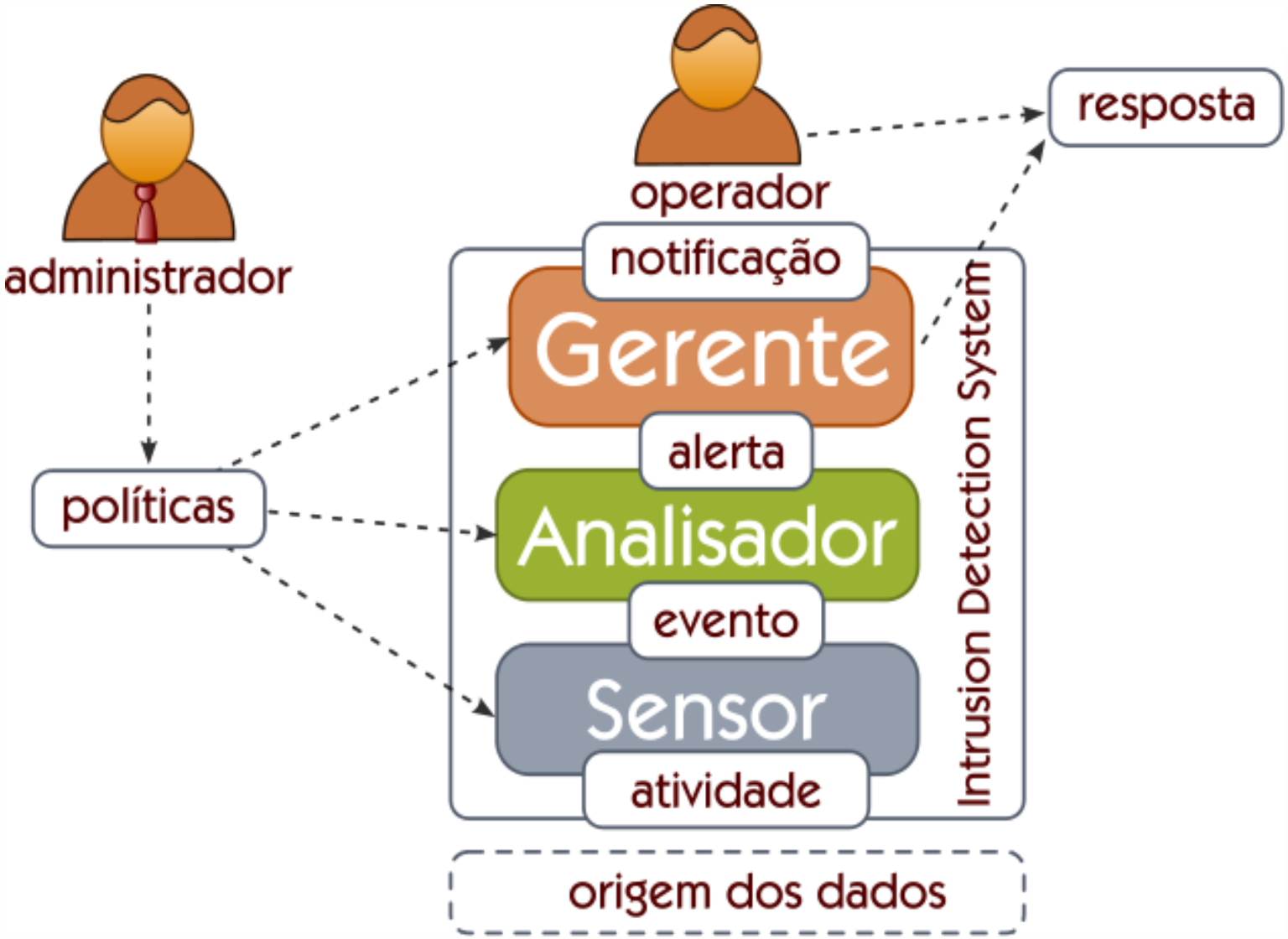
- Sistemas de Detecção de *Intrusão*

  (Intrusion Detection Systems)

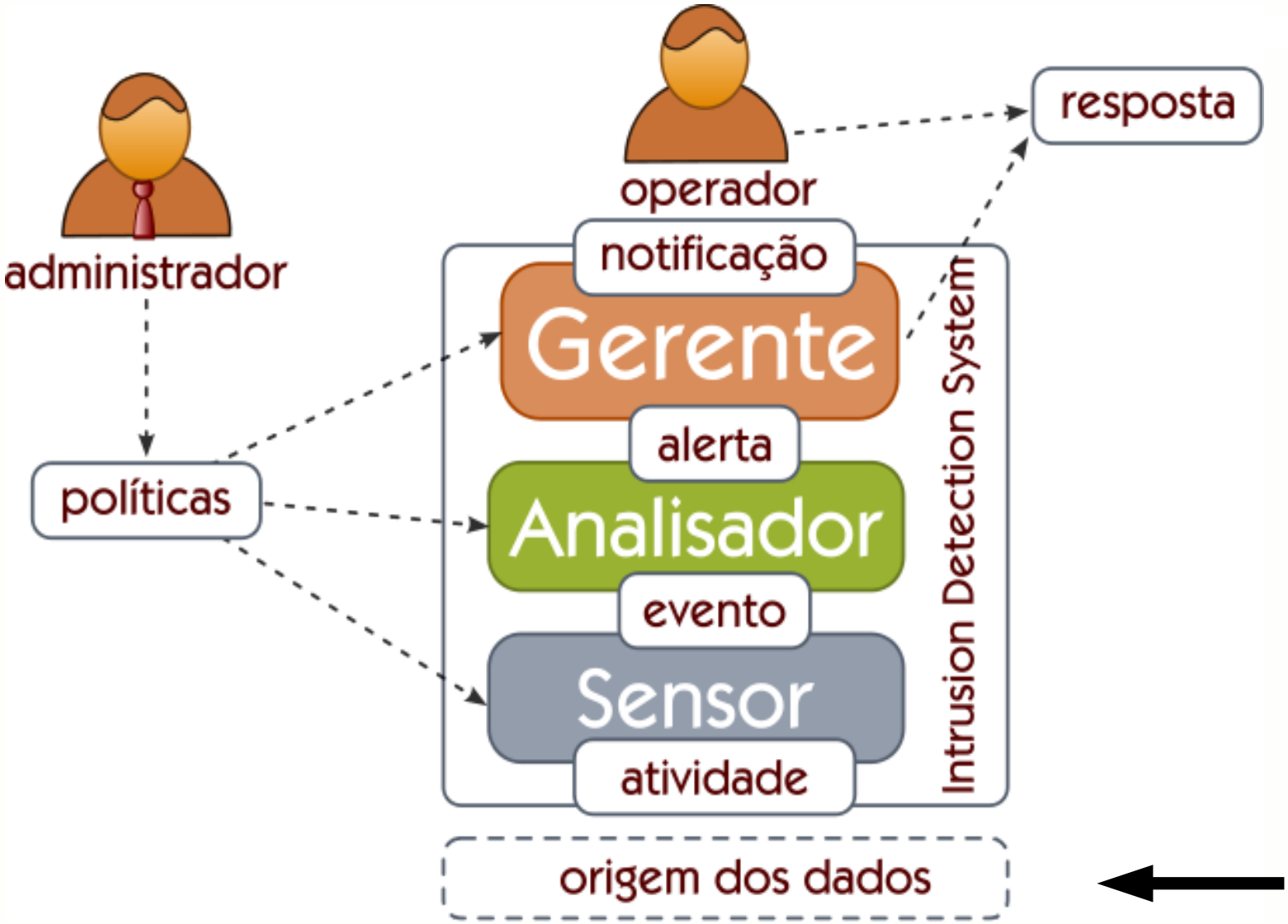
  IDS

  - IDS é como um alarme em uma empresa
  - IDS permite detectar intrusos em tempo real, e armazenar a ação do intruso.
  - IDS depende de inteligência humana.
  - IDS é uma ferramenta útil para segurança e administradores de redes.

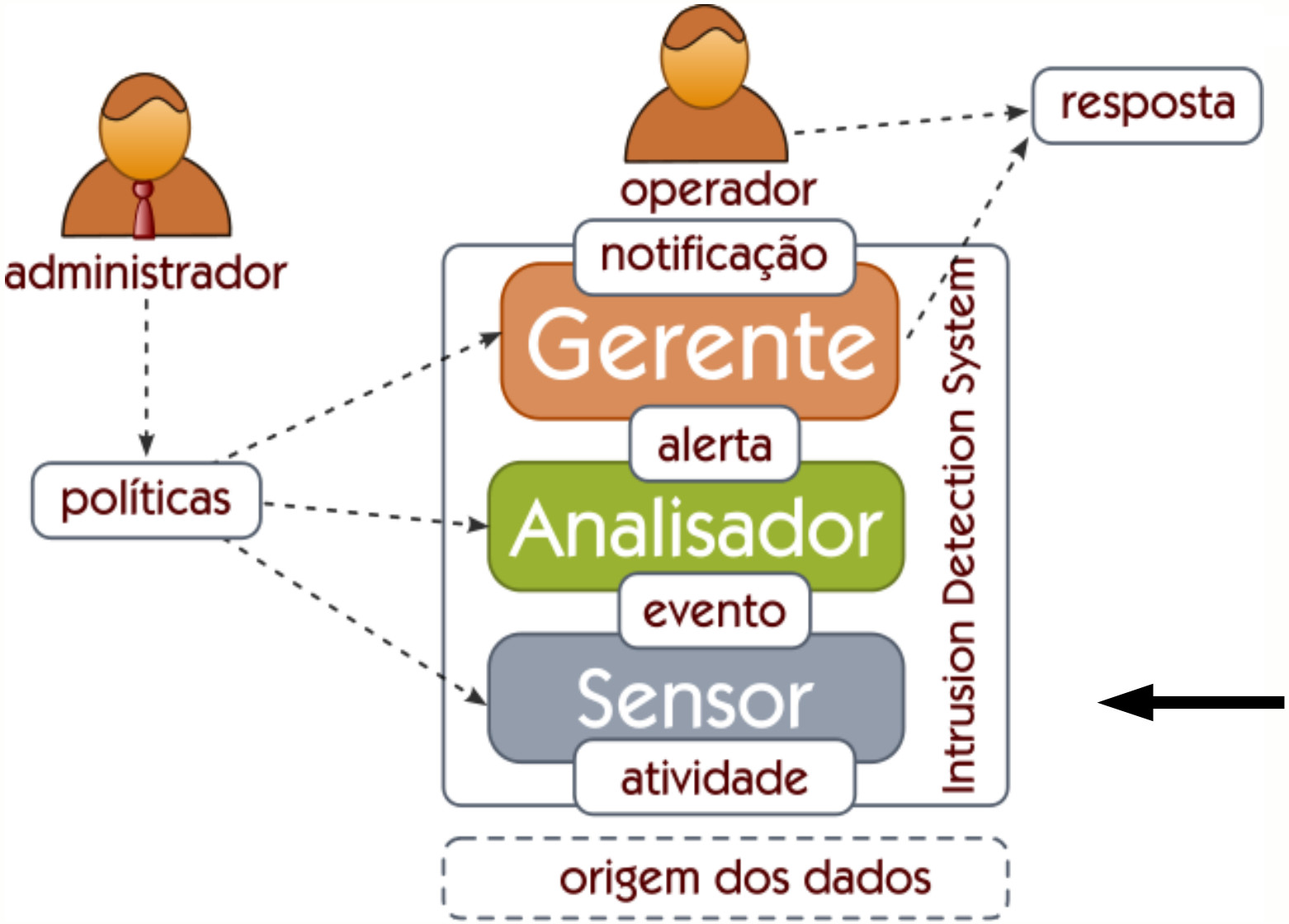
Sistemas de Detecção de Intrusão



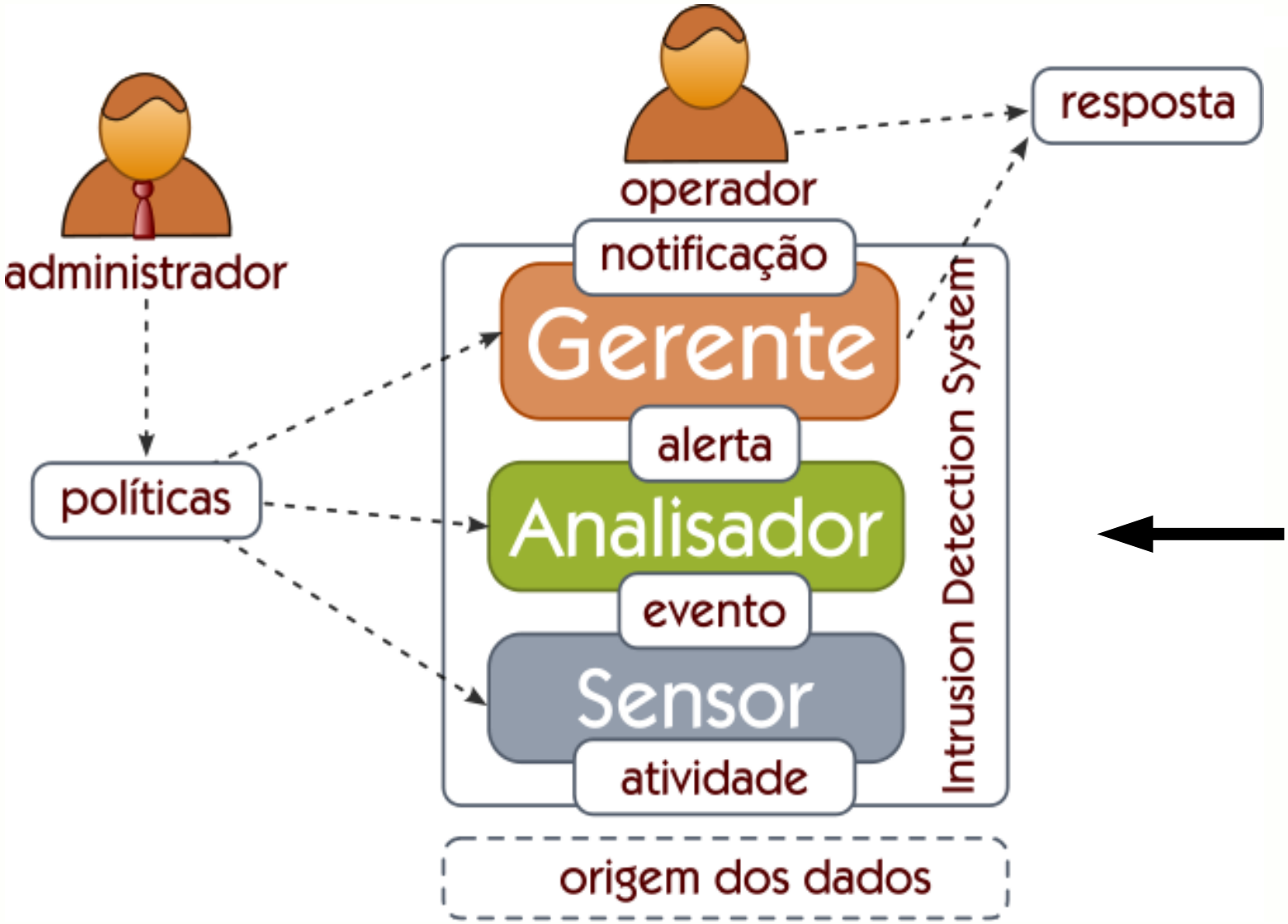
Sistemas de Detecção de Intrusão



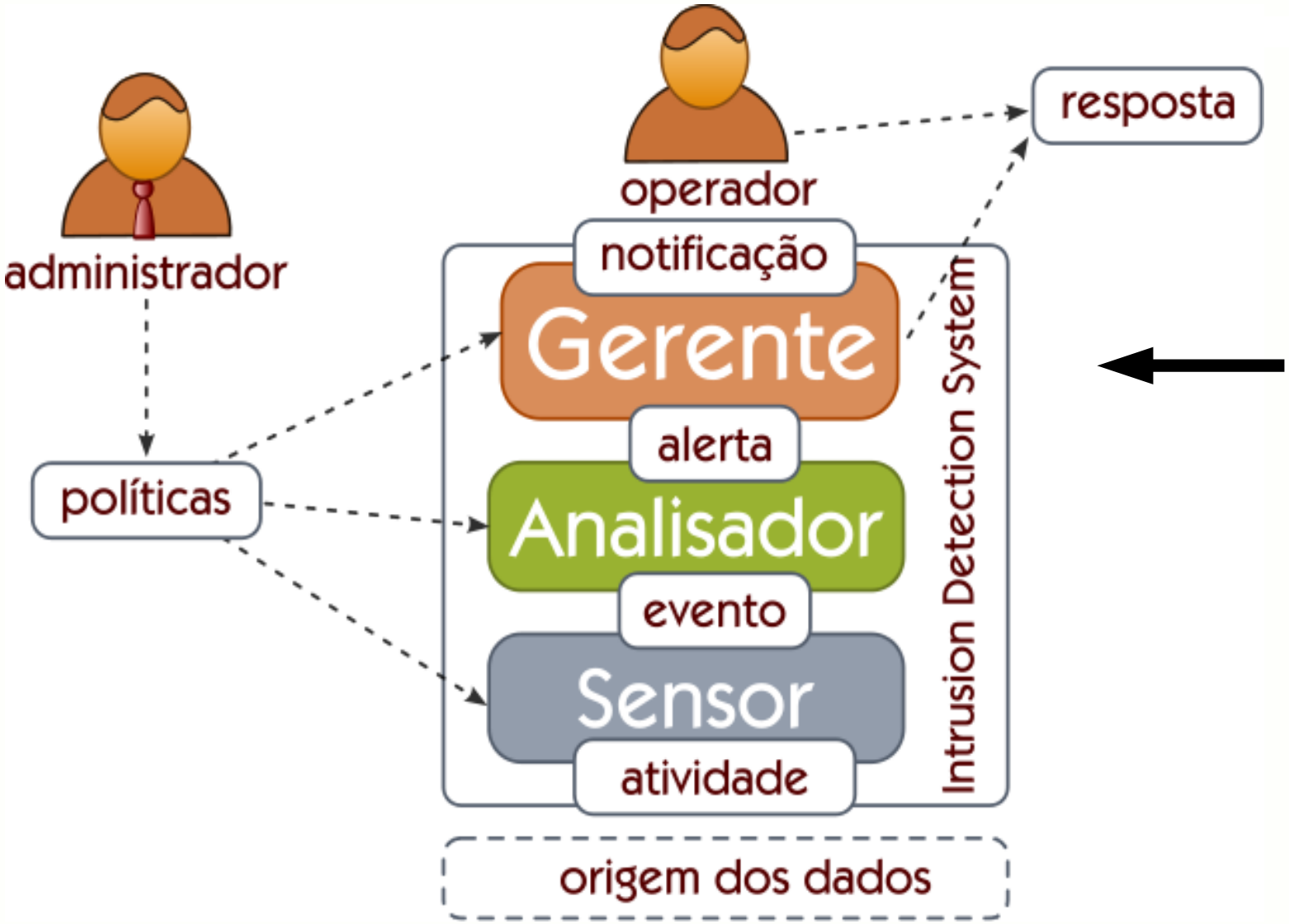
Sistemas de Detecção de Intrusão



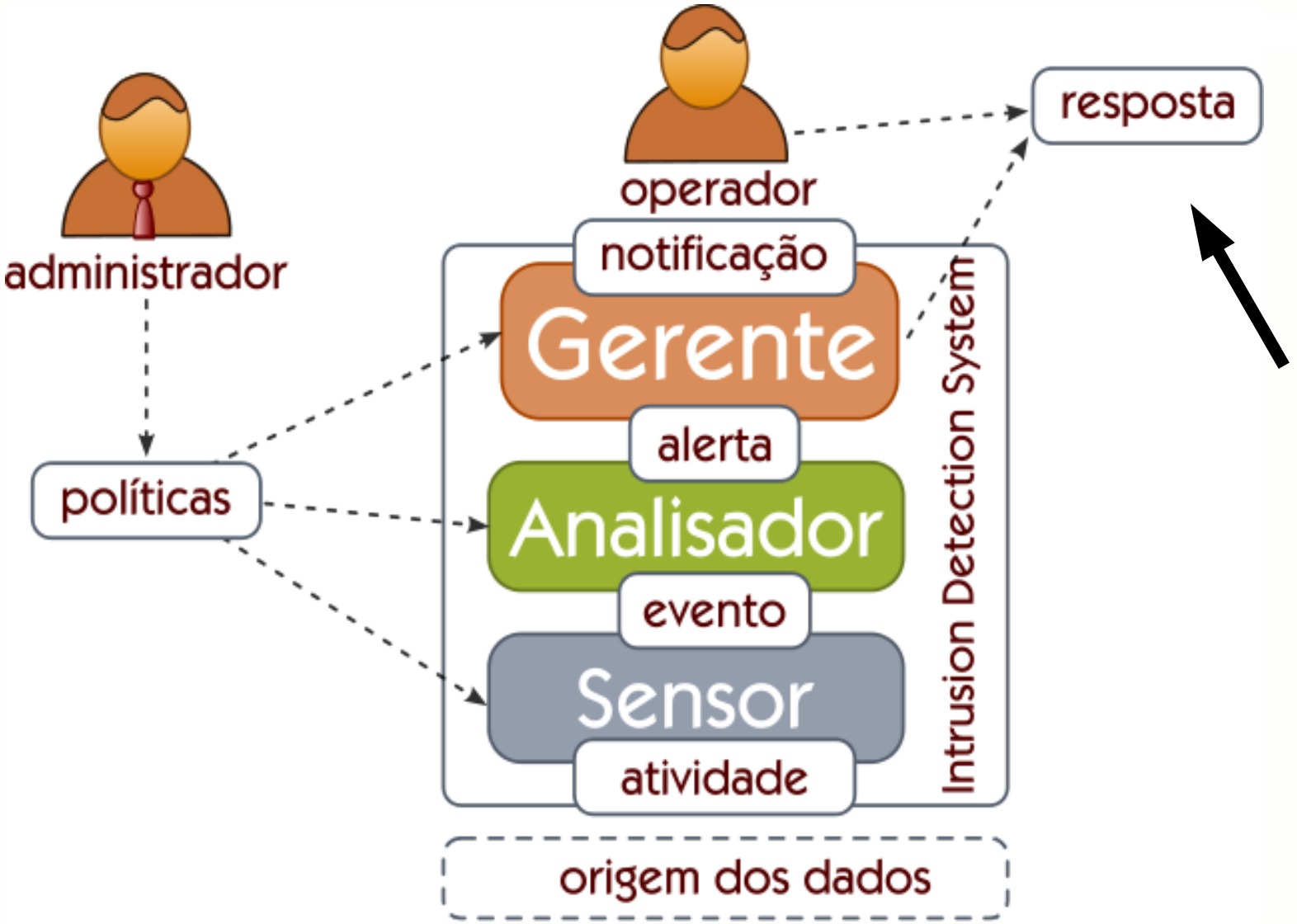
Sistemas de Detecção de Intrusão



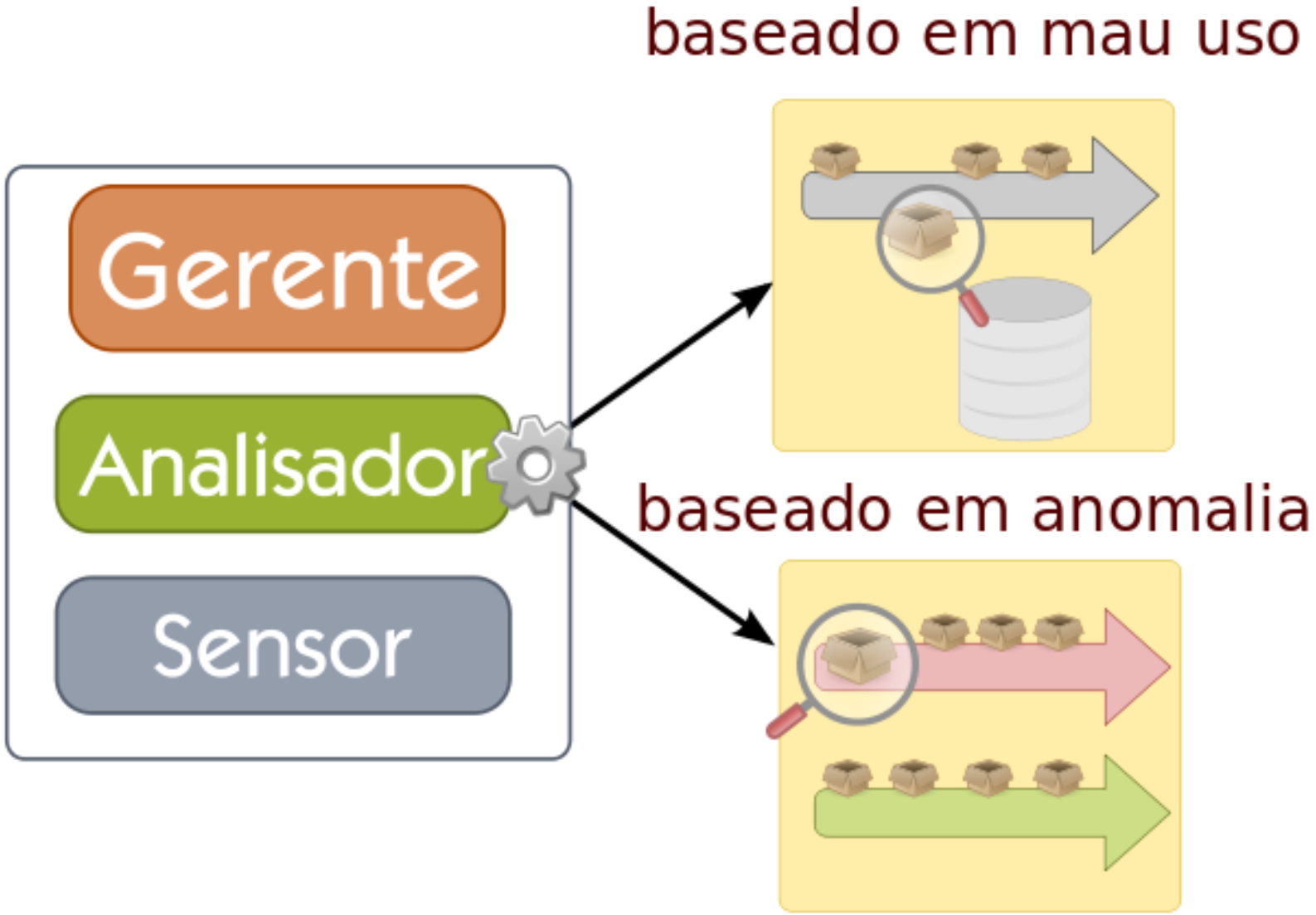
Sistemas de Detecção de Intrusão



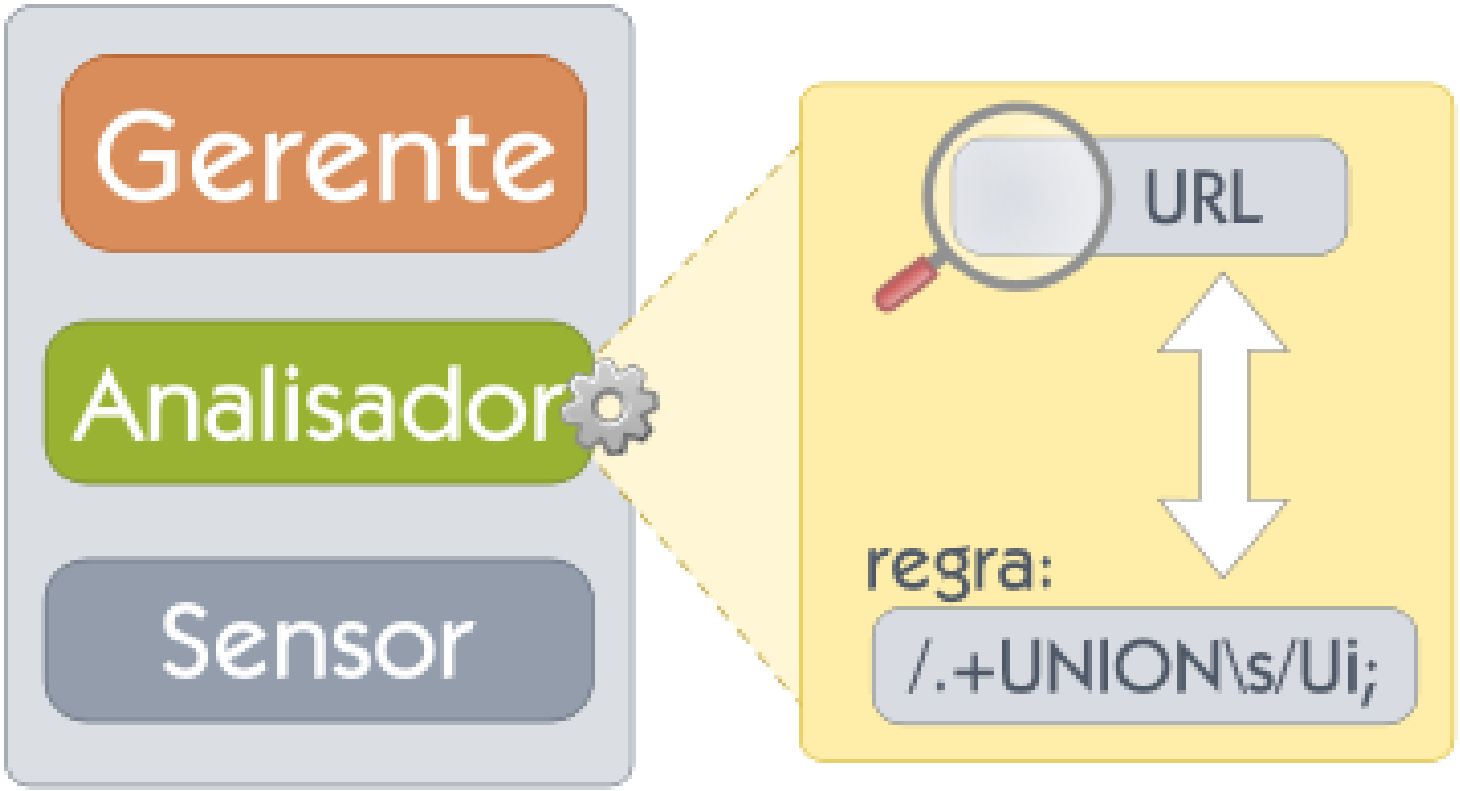
Sistemas de Detecção de Intrusão



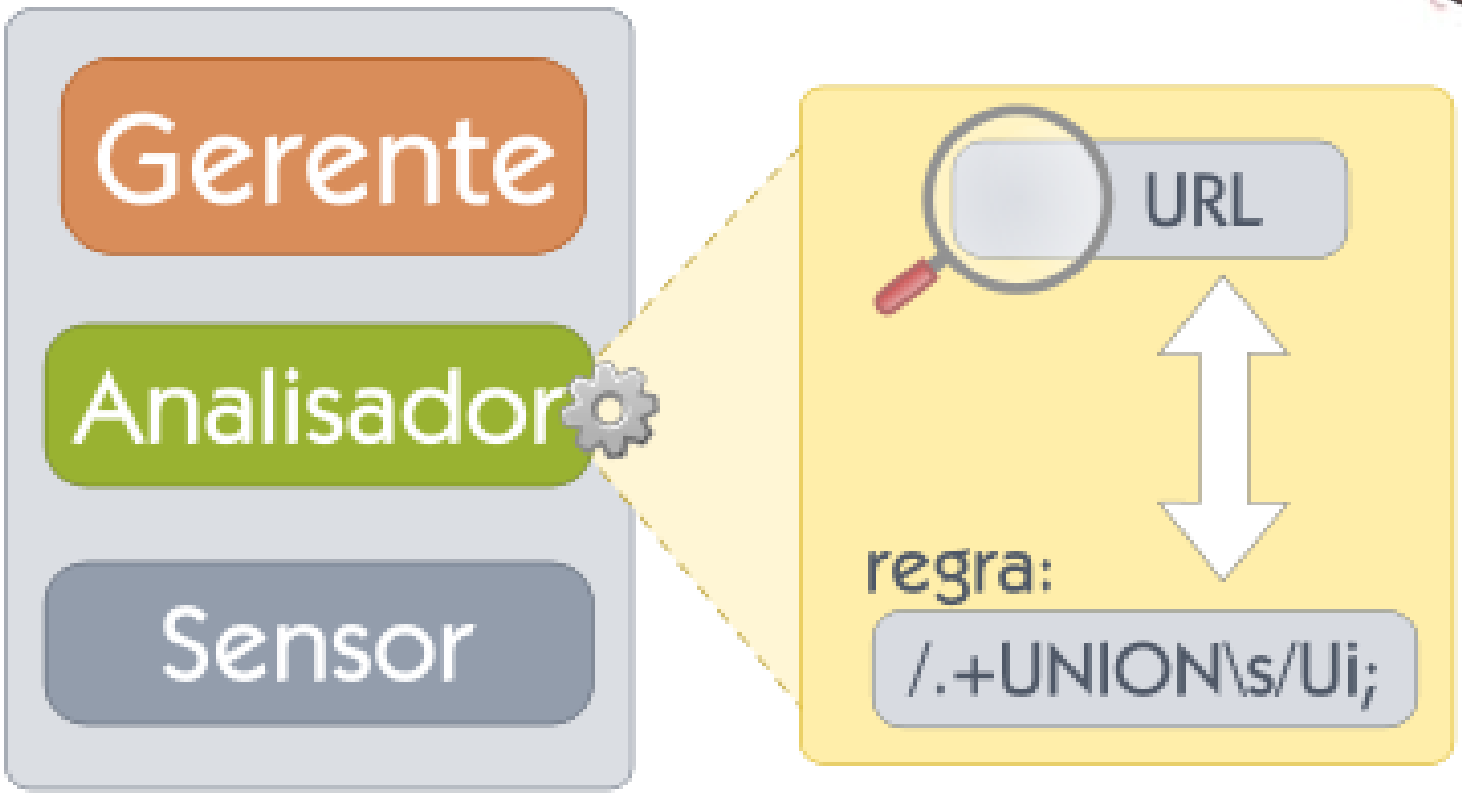
Sistemas de Detecção de Intrusão



IDS baseado em Regras



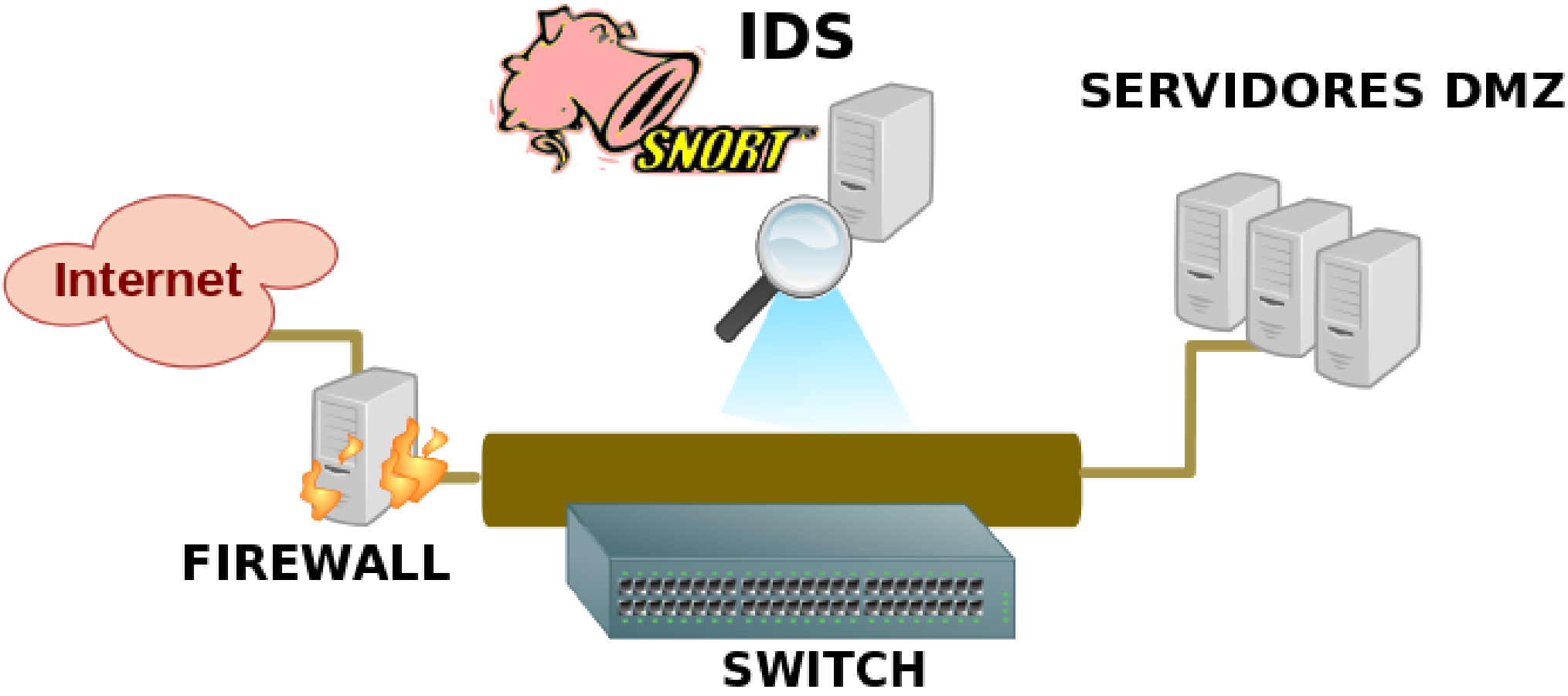
IDS baseado em Regras



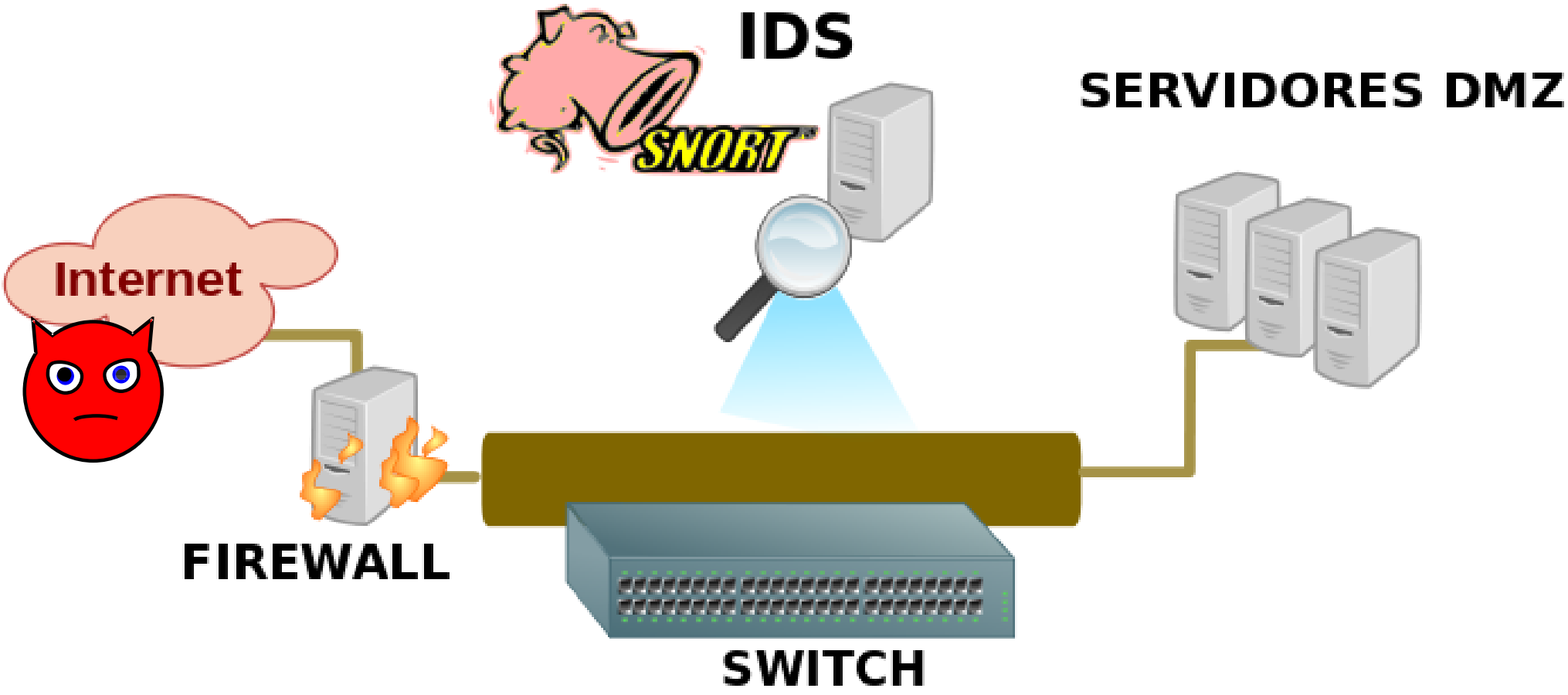
Sistemas de Detecção de Intrusão

- SNORT
  - Martin Roesch (1999)
  - Robusto
  - Estável
  - Software livre
  - Assinaturas GPL
  - Assinaturas EMERGING THREATS

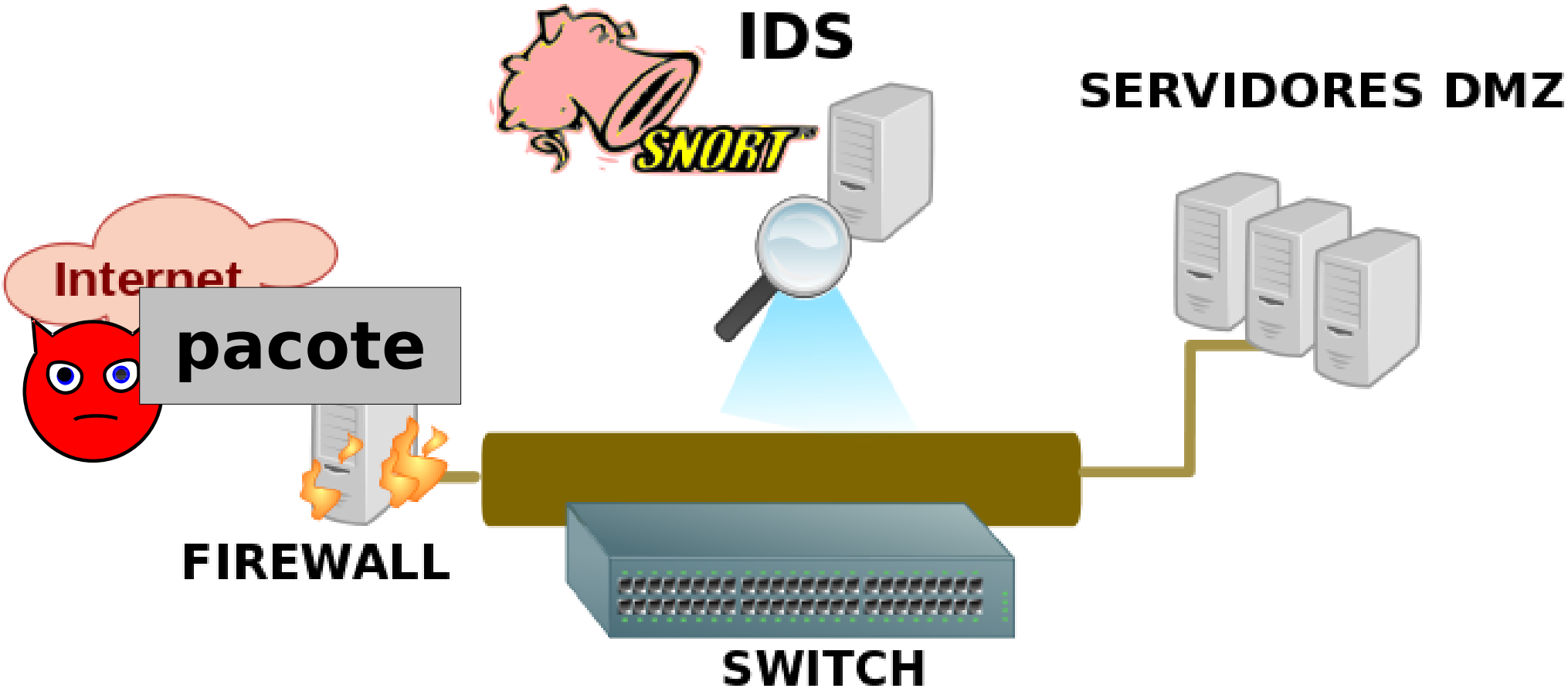
Sistemas de Detecção de Intrusão



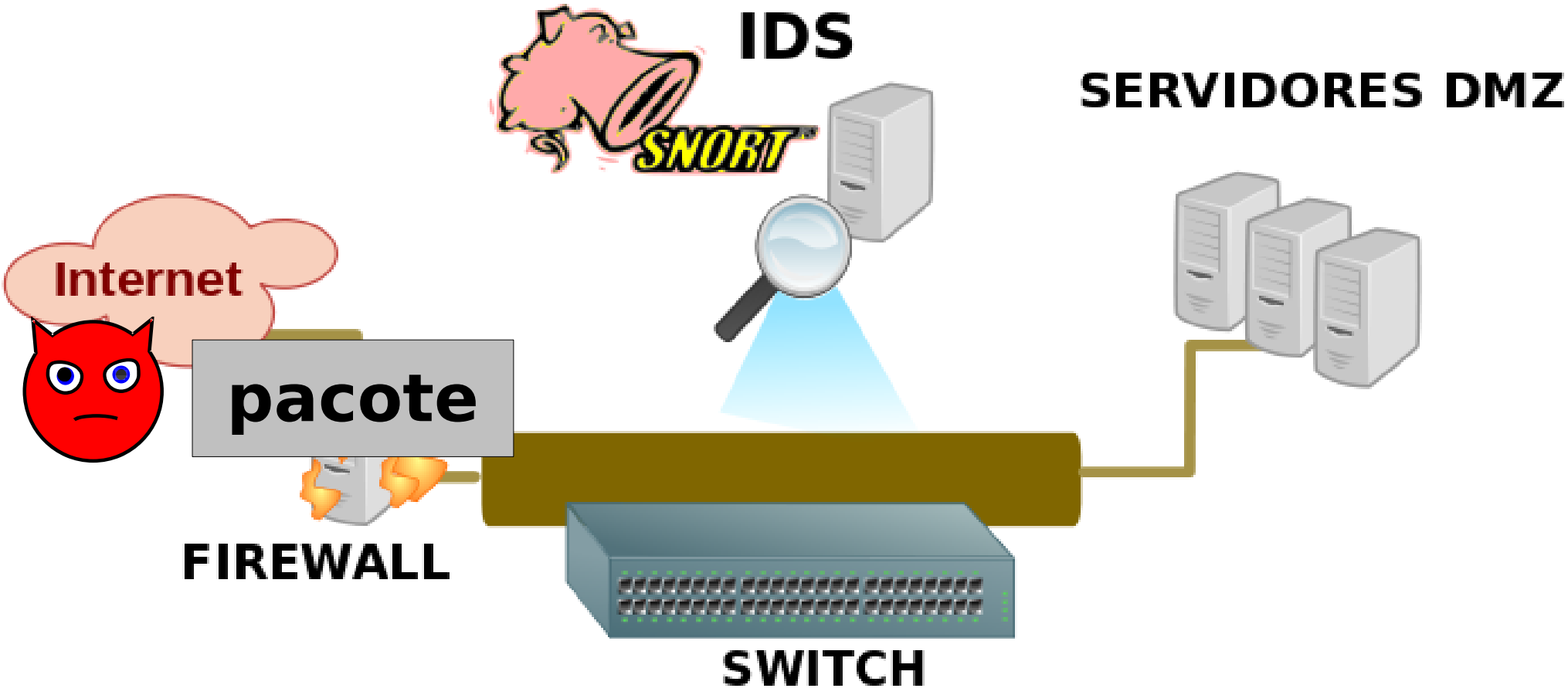
Sistemas de Detecção de Intrusão



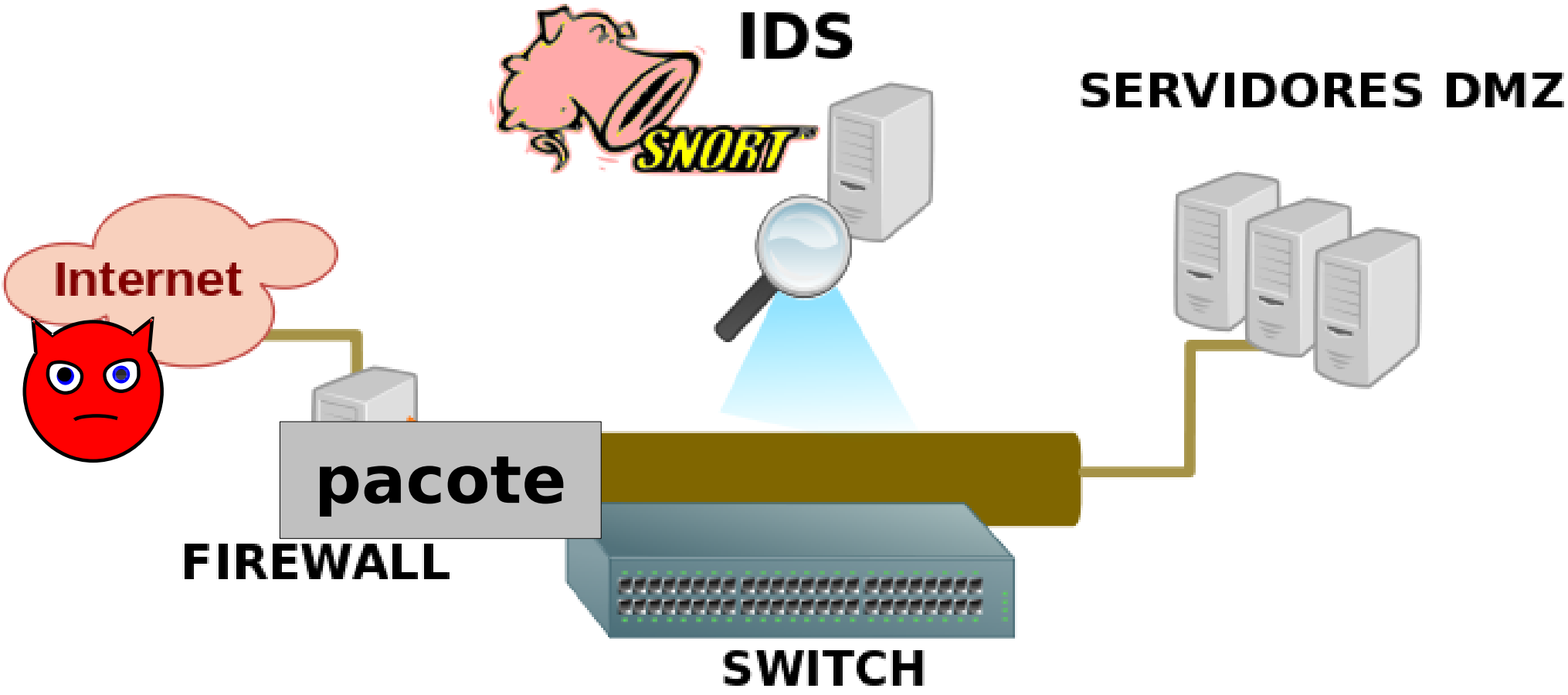
Sistemas de Detecção de Intrusão



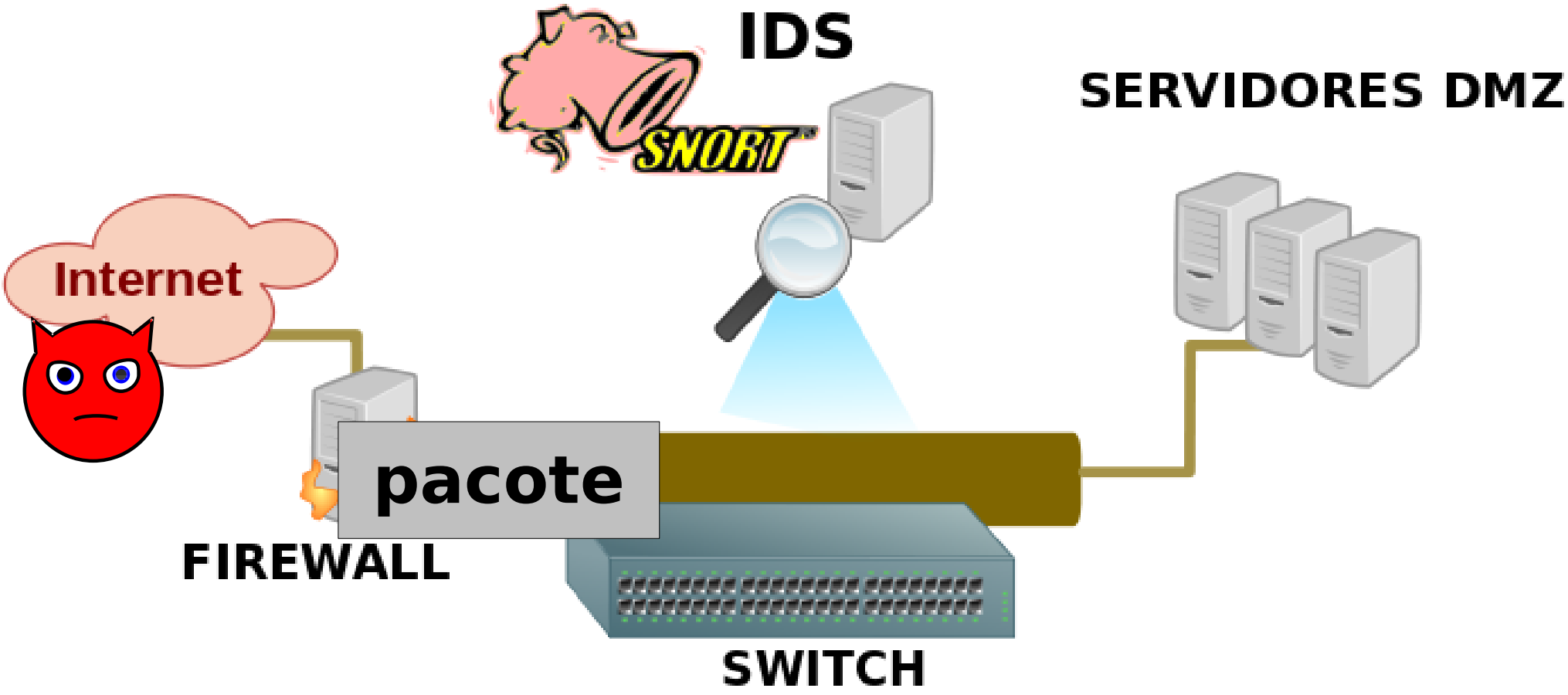
Sistemas de Detecção de Intrusão



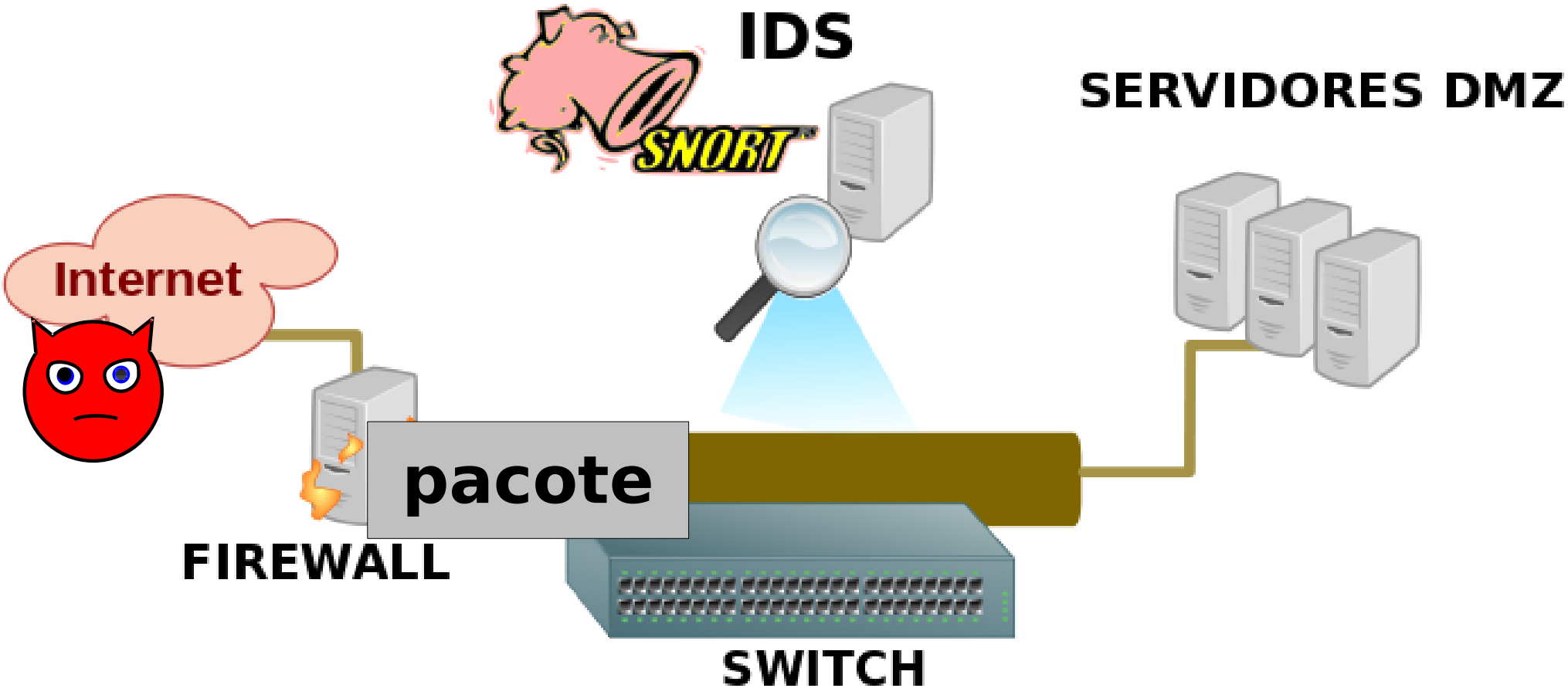
Sistemas de Detecção de Intrusão



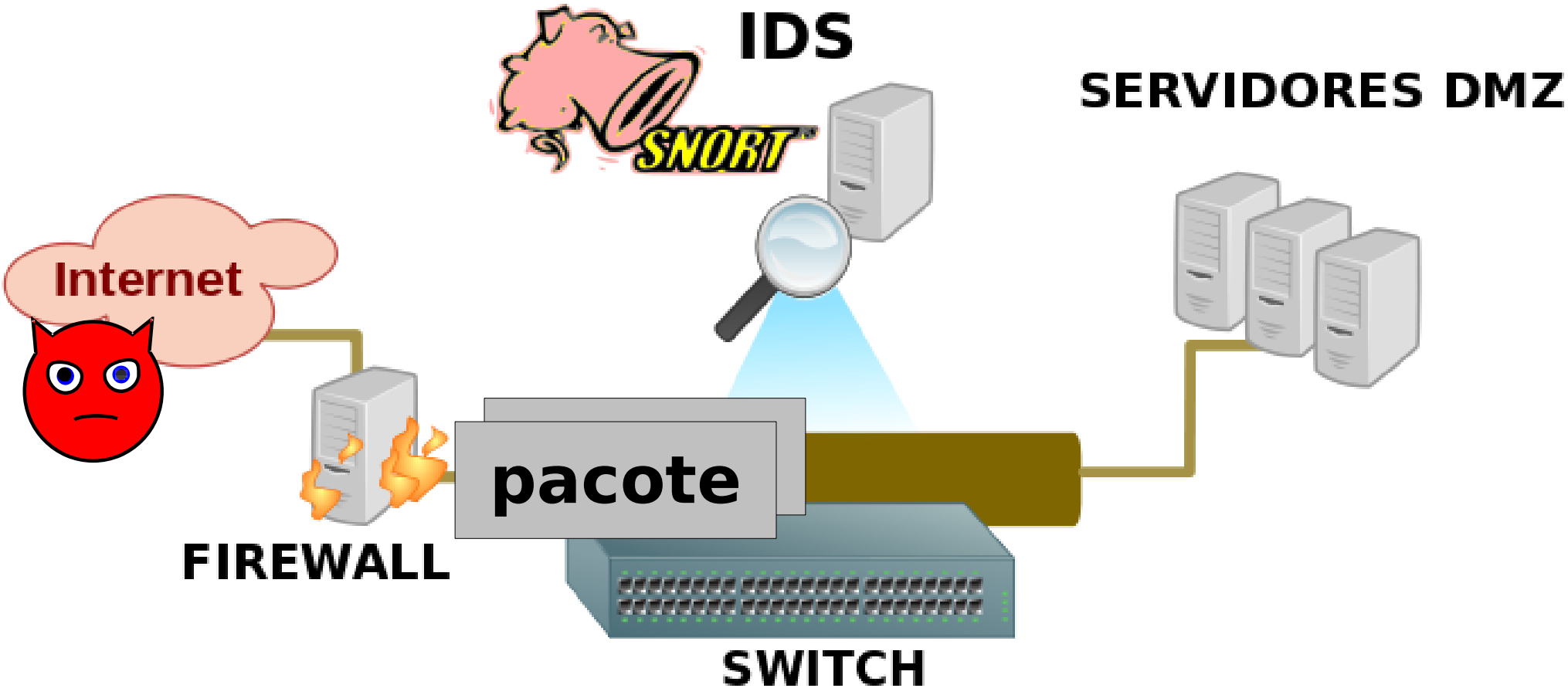
Sistemas de Detecção de Intrusão



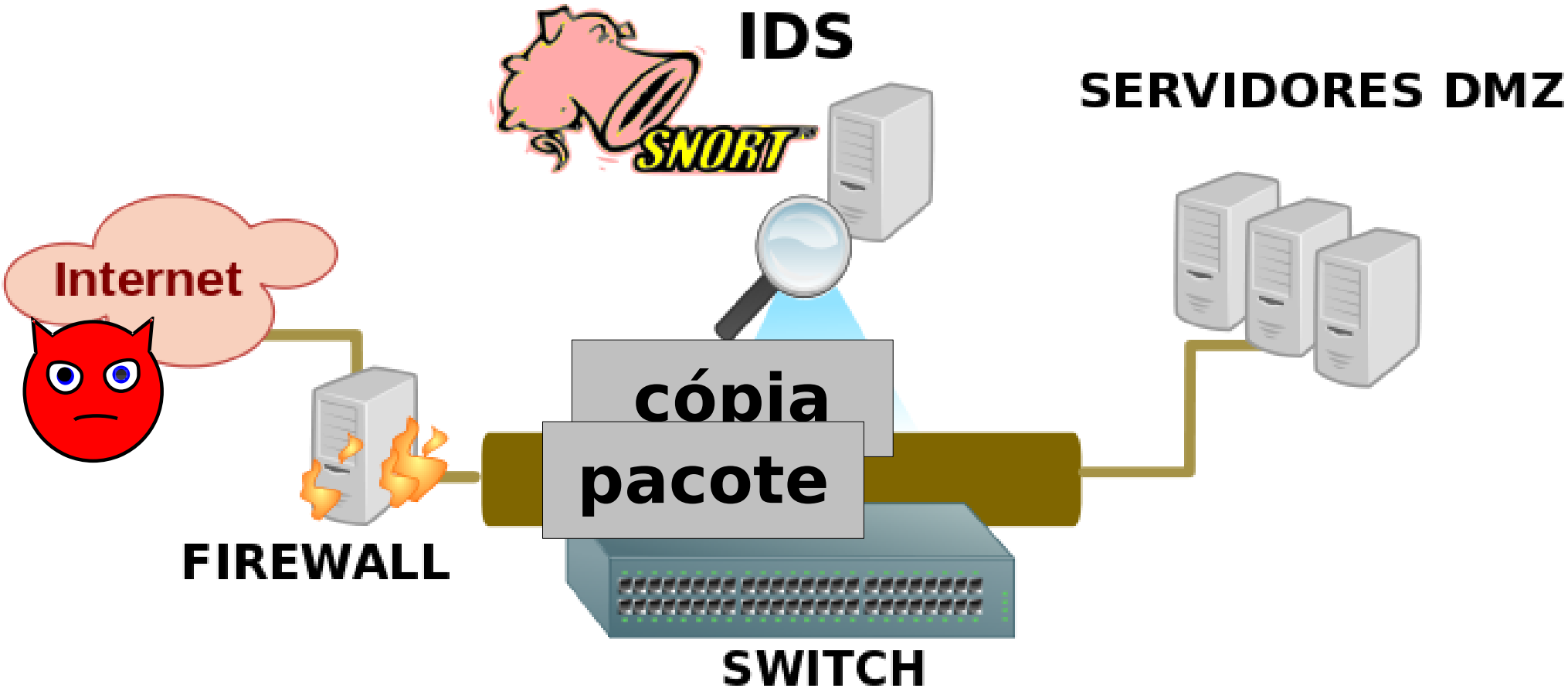
Sistemas de Detecção de Intrusão



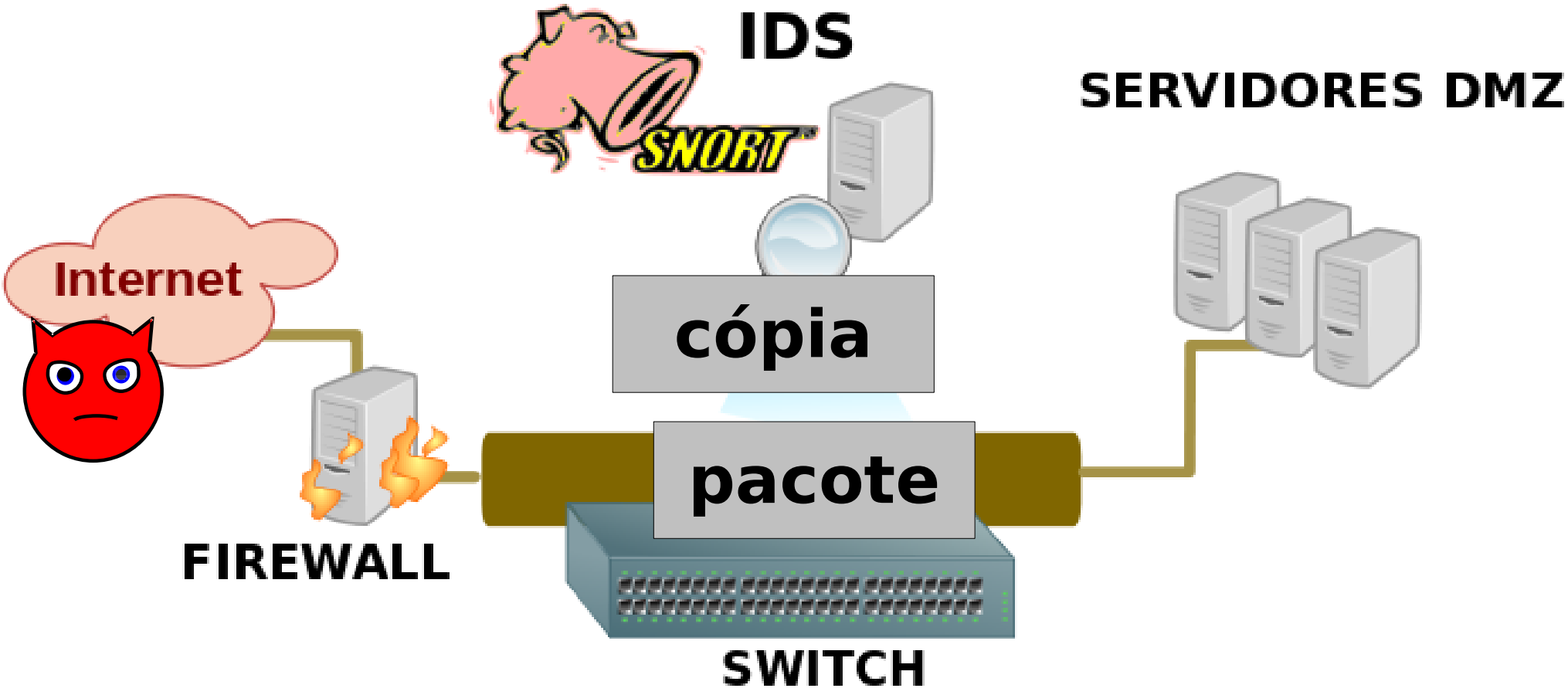
Sistemas de Detecção de Intrusão



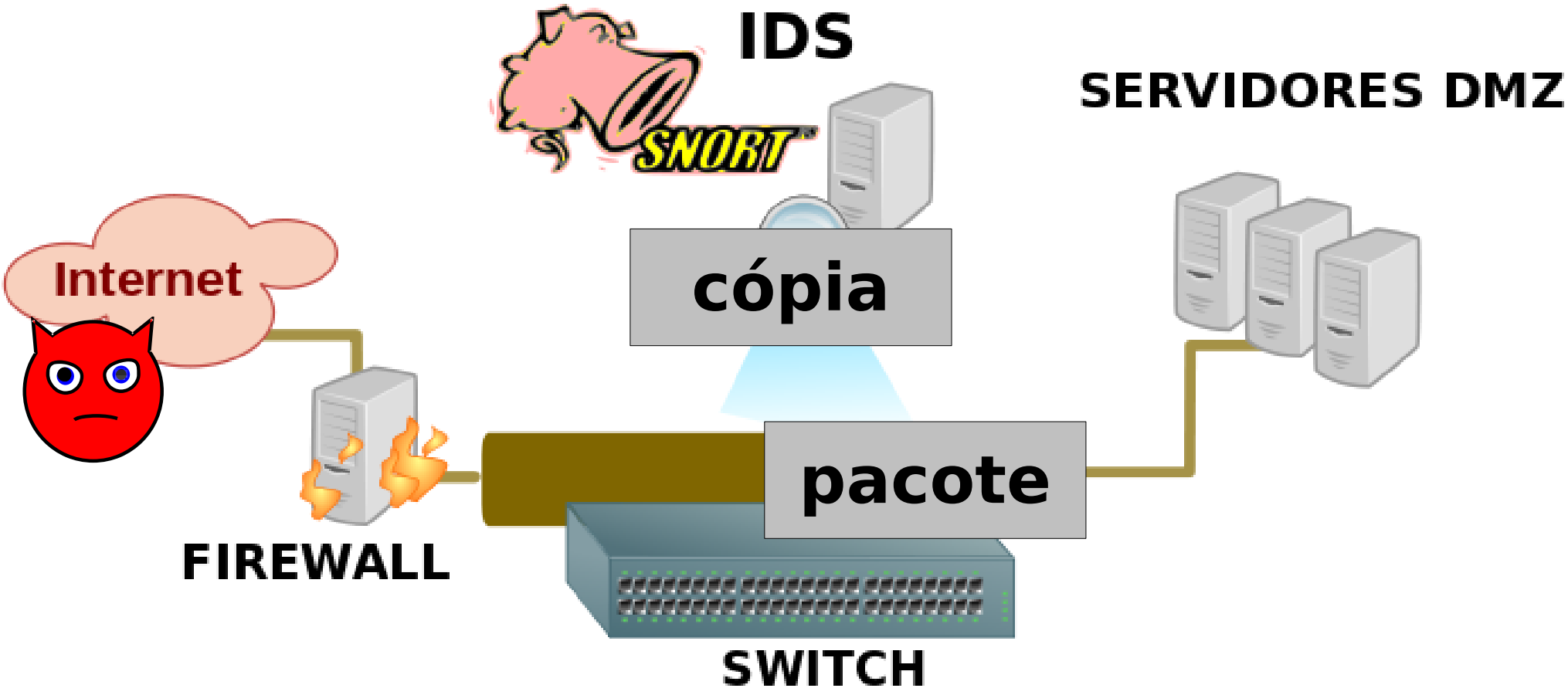
Sistemas de Detecção de Intrusão



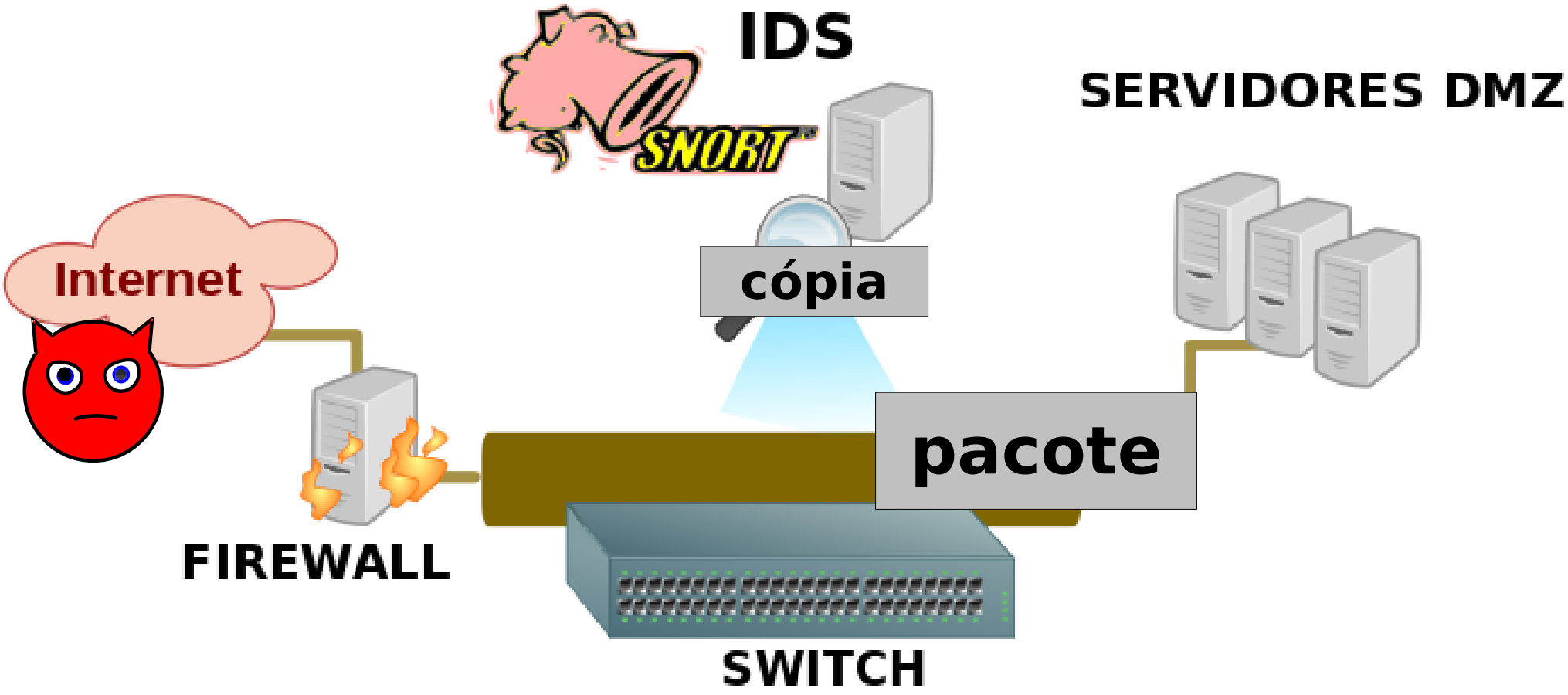
Sistemas de Detecção de Intrusão



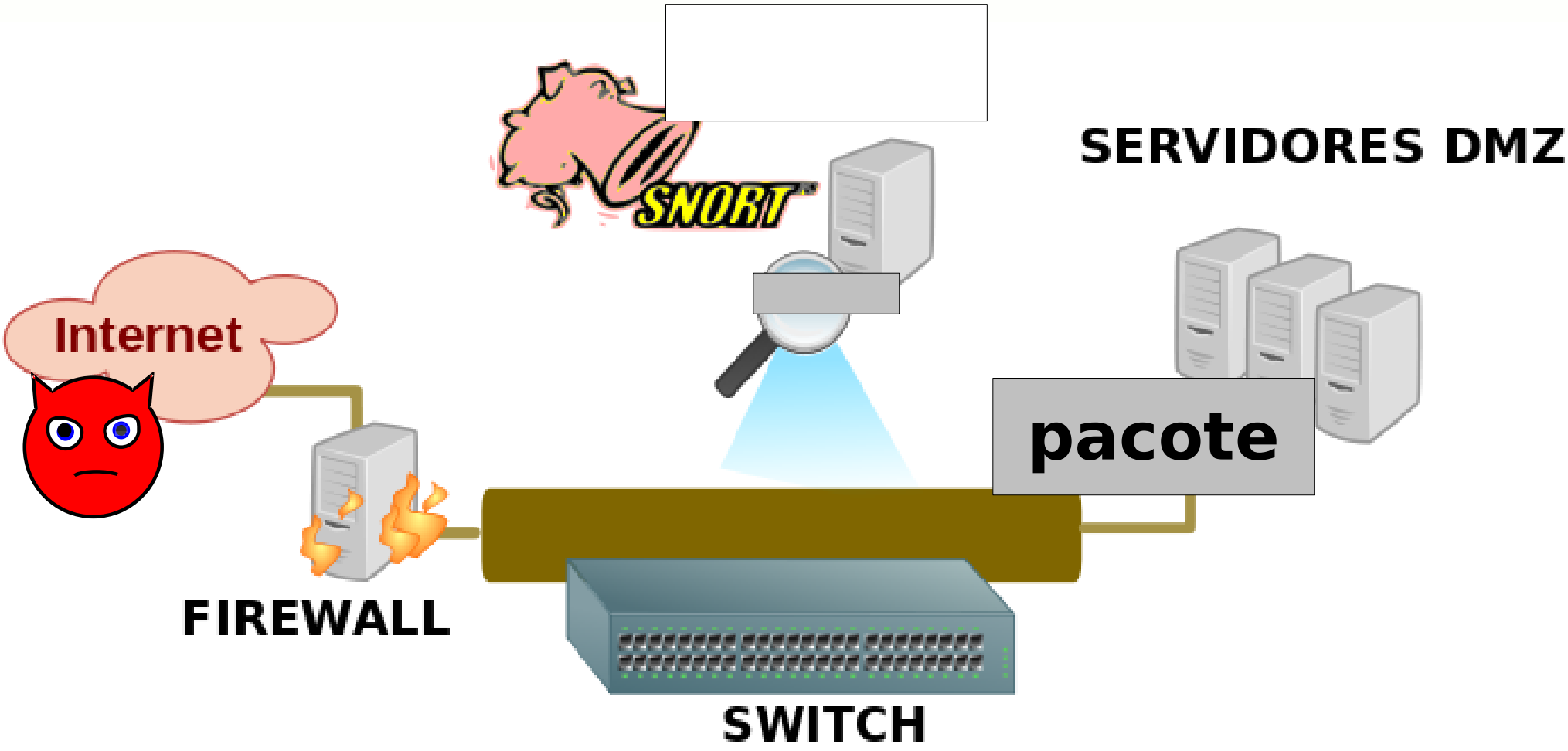
Sistemas de Detecção de Intrusão



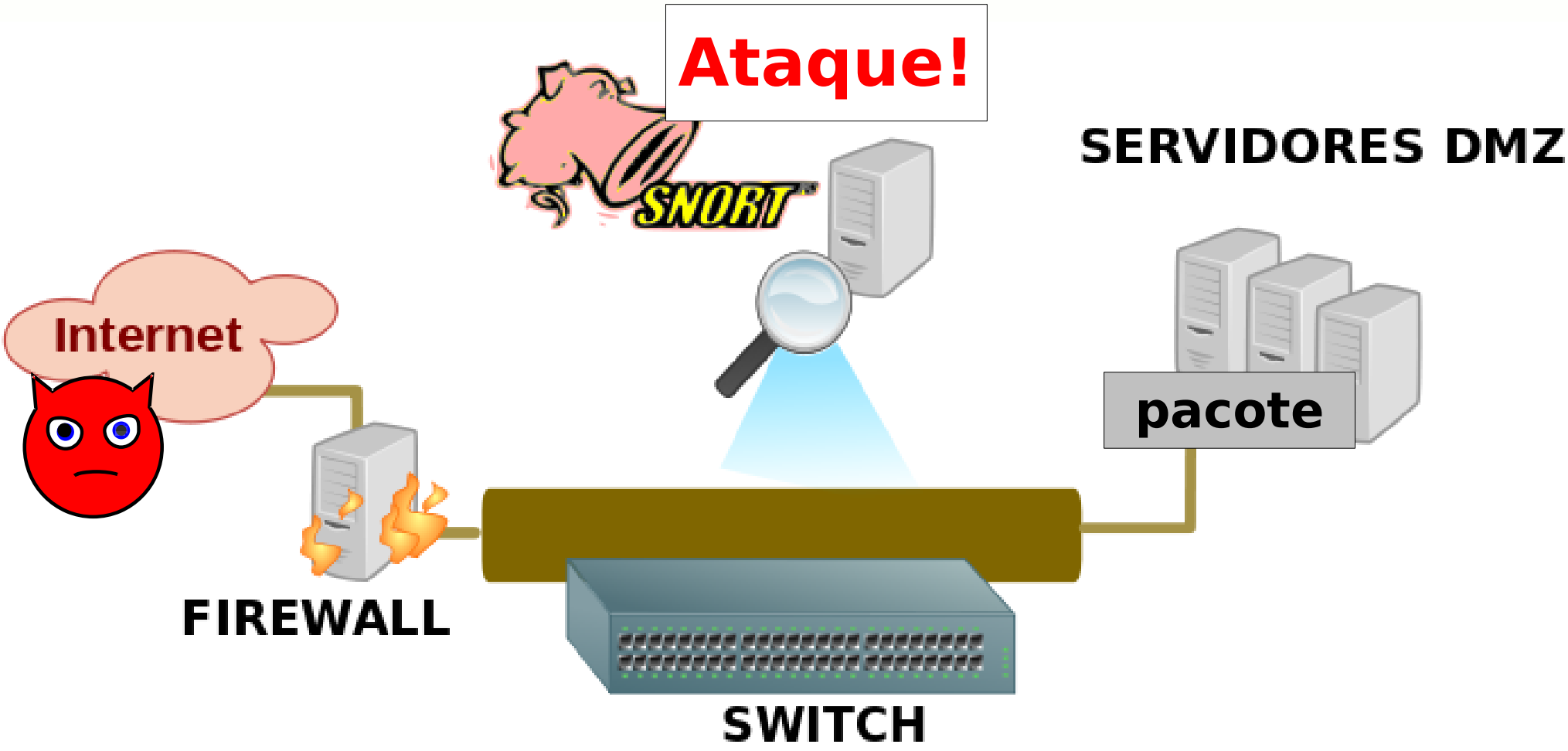
Sistemas de Detecção de Intrusão



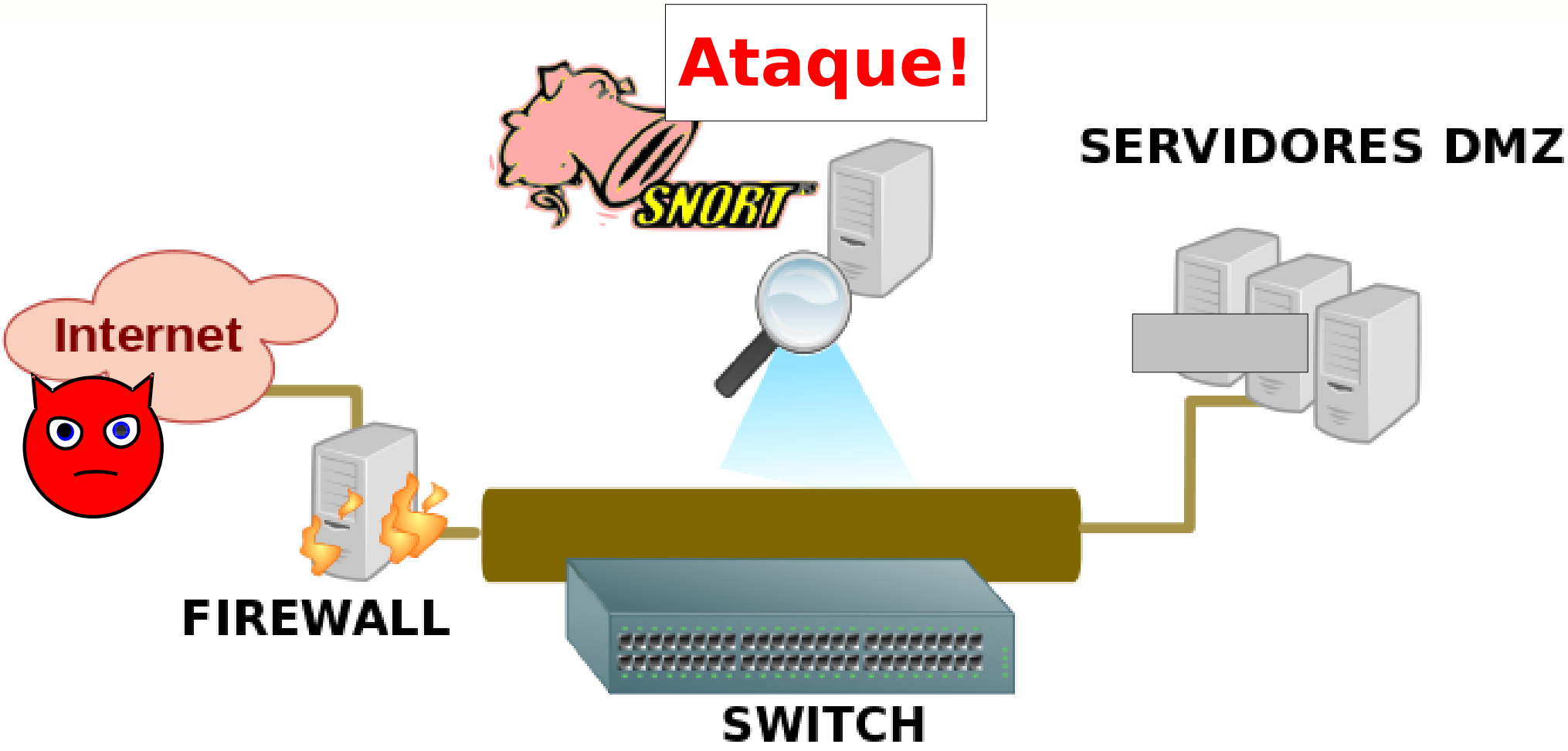
Sistemas de Detecção de Intrusão



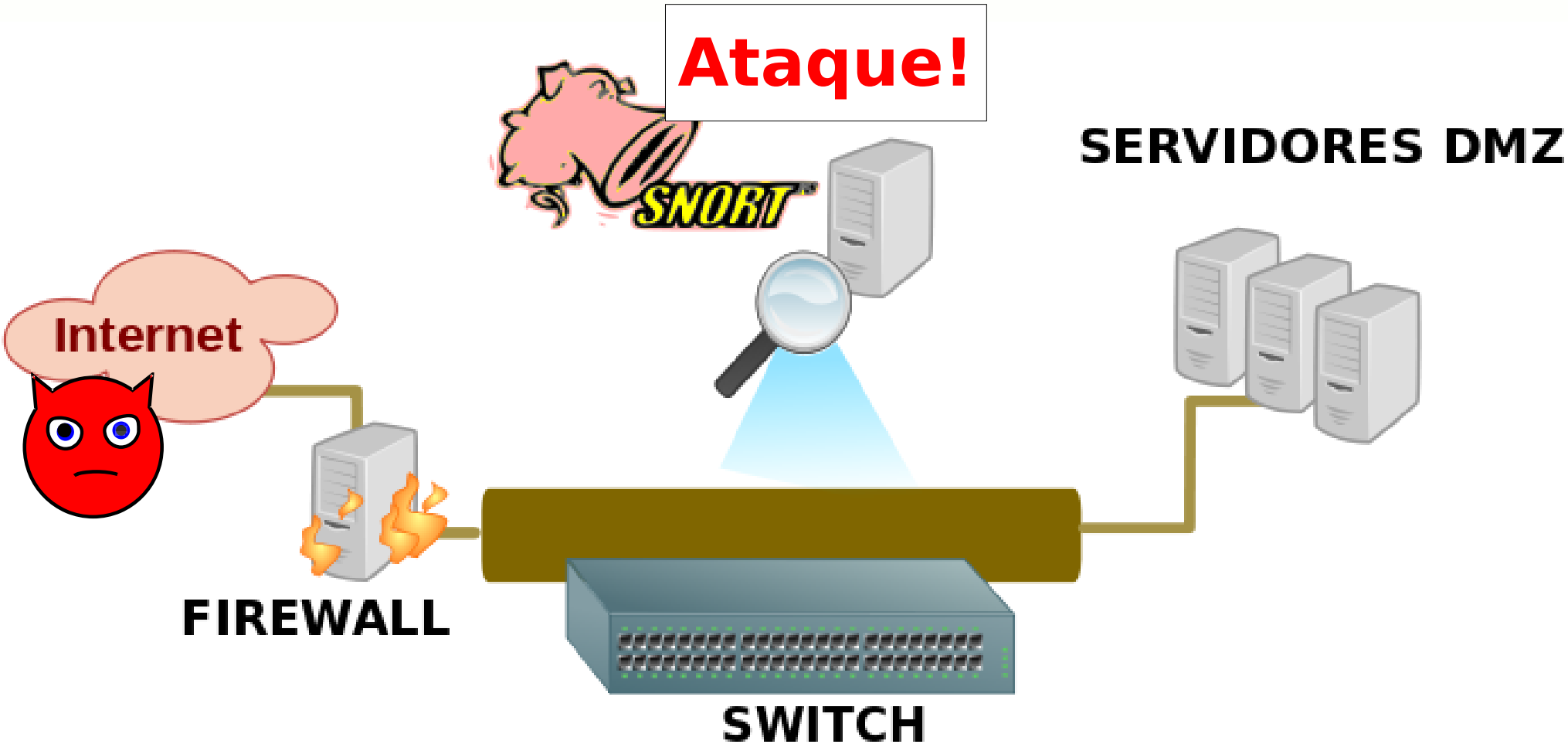
Sistemas de Detecção de Intrusão



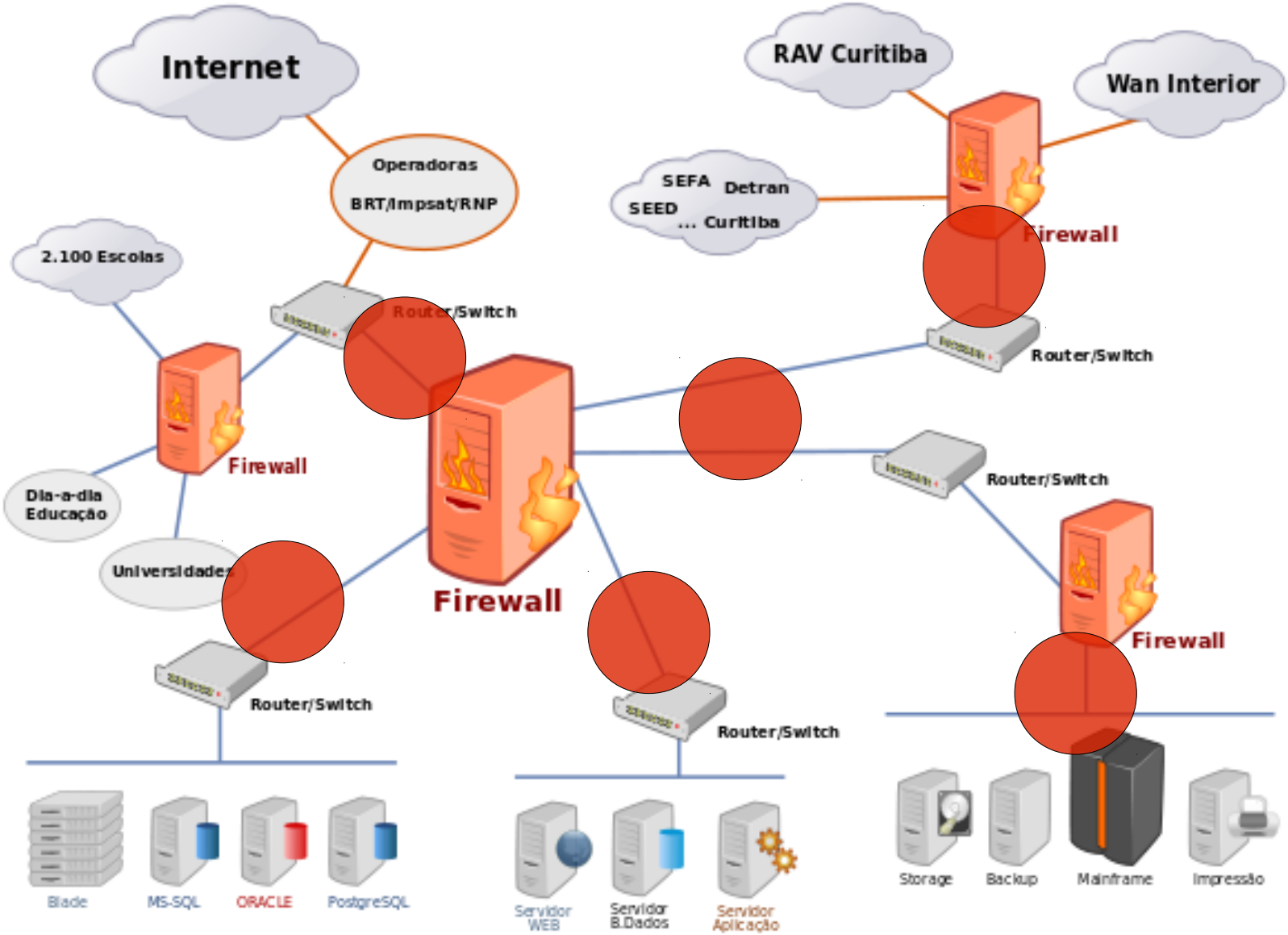
Sistemas de Detecção de Intrusão



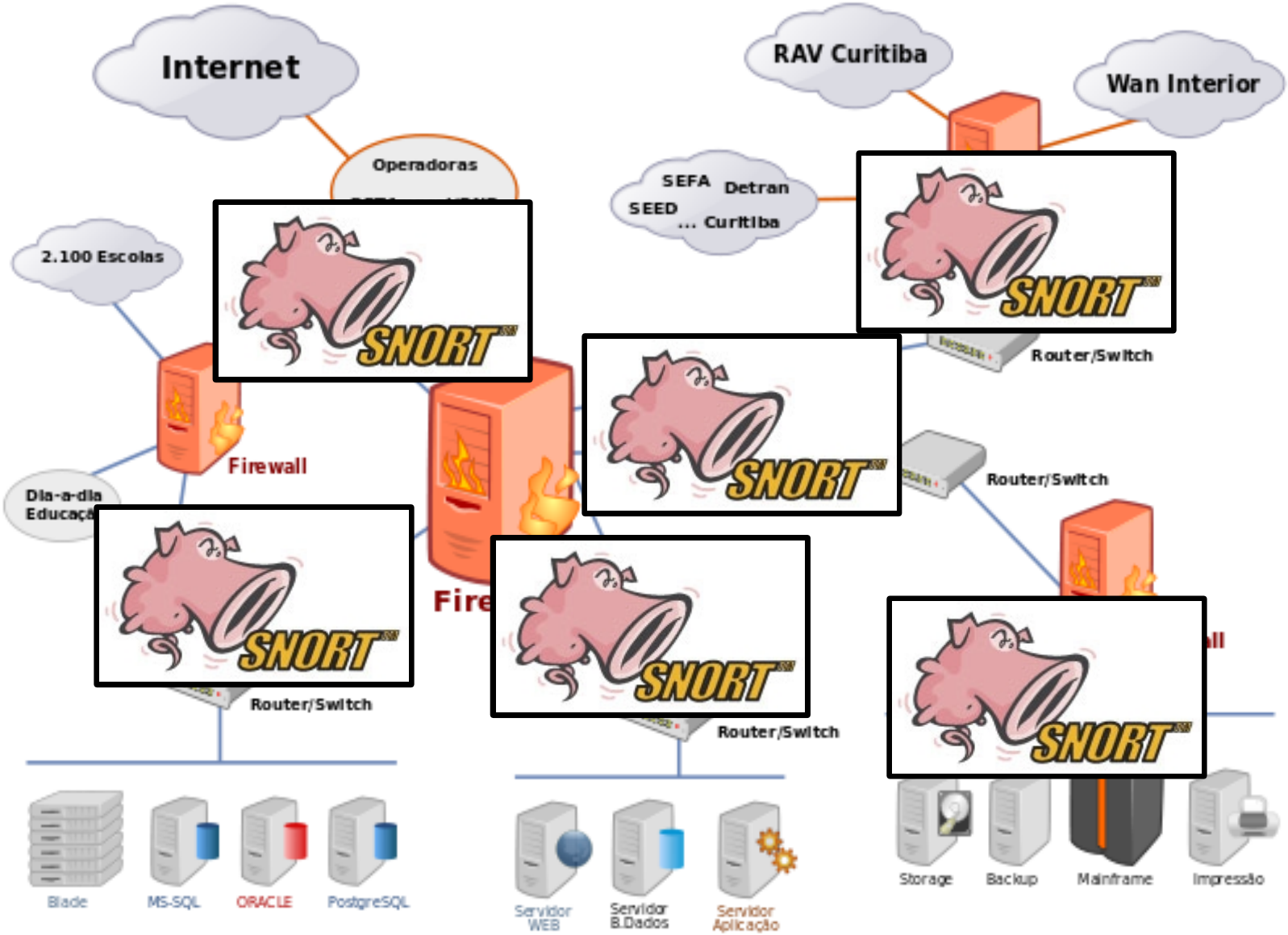
Sistemas de Detecção de Intrusão



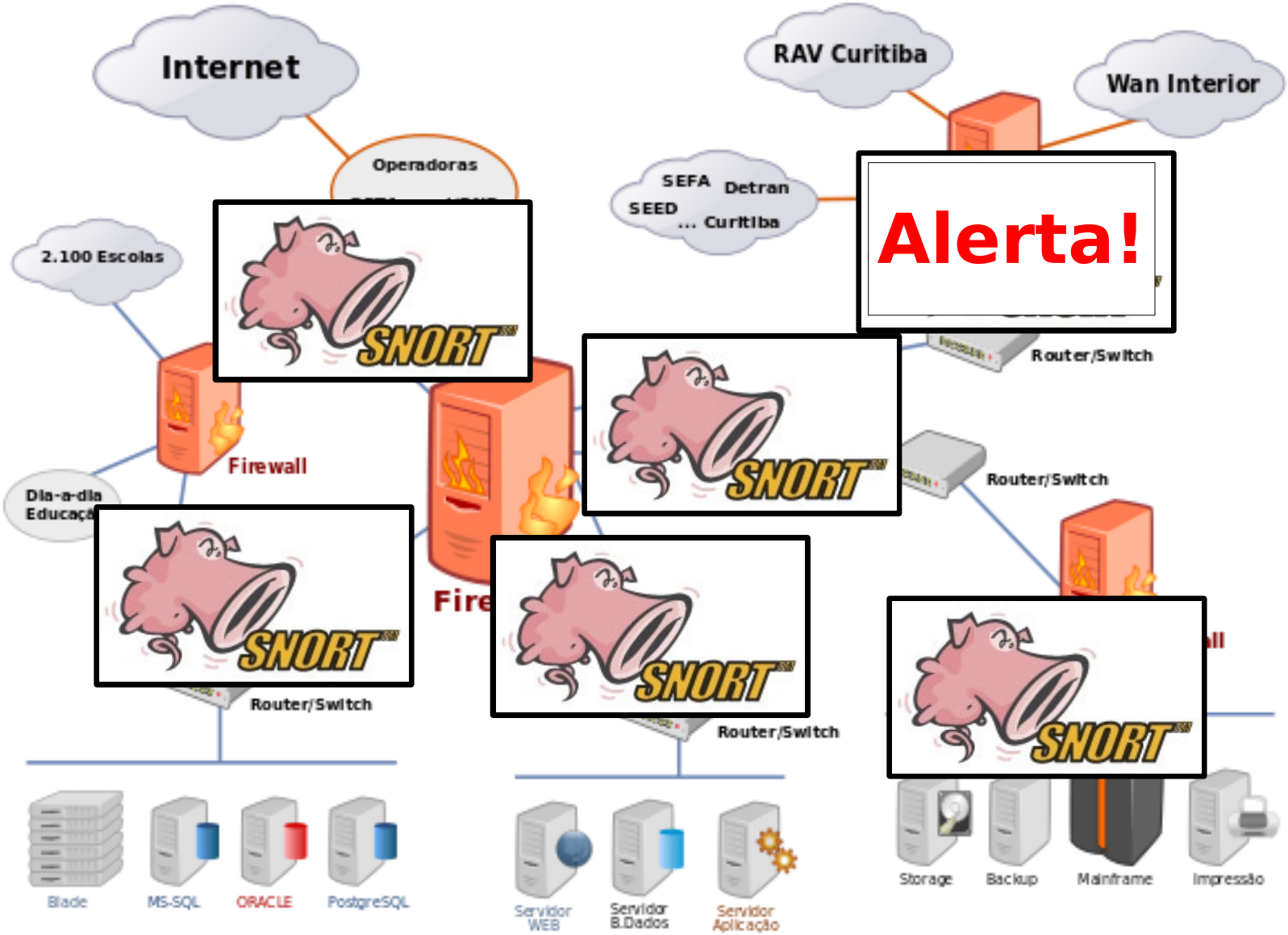
Sistemas de Detecção de Intrusão



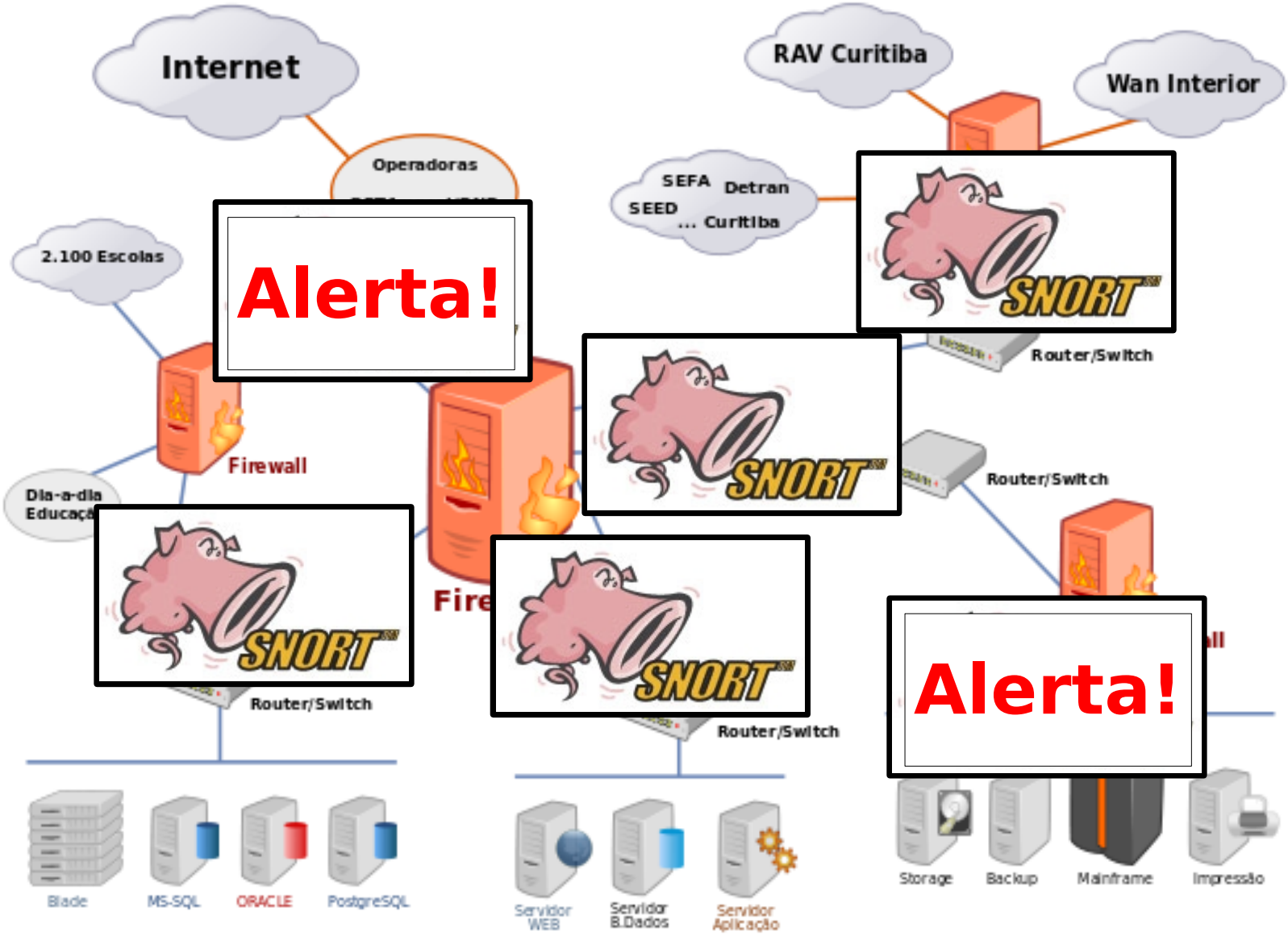
Sistemas de Detecção de Intrusão



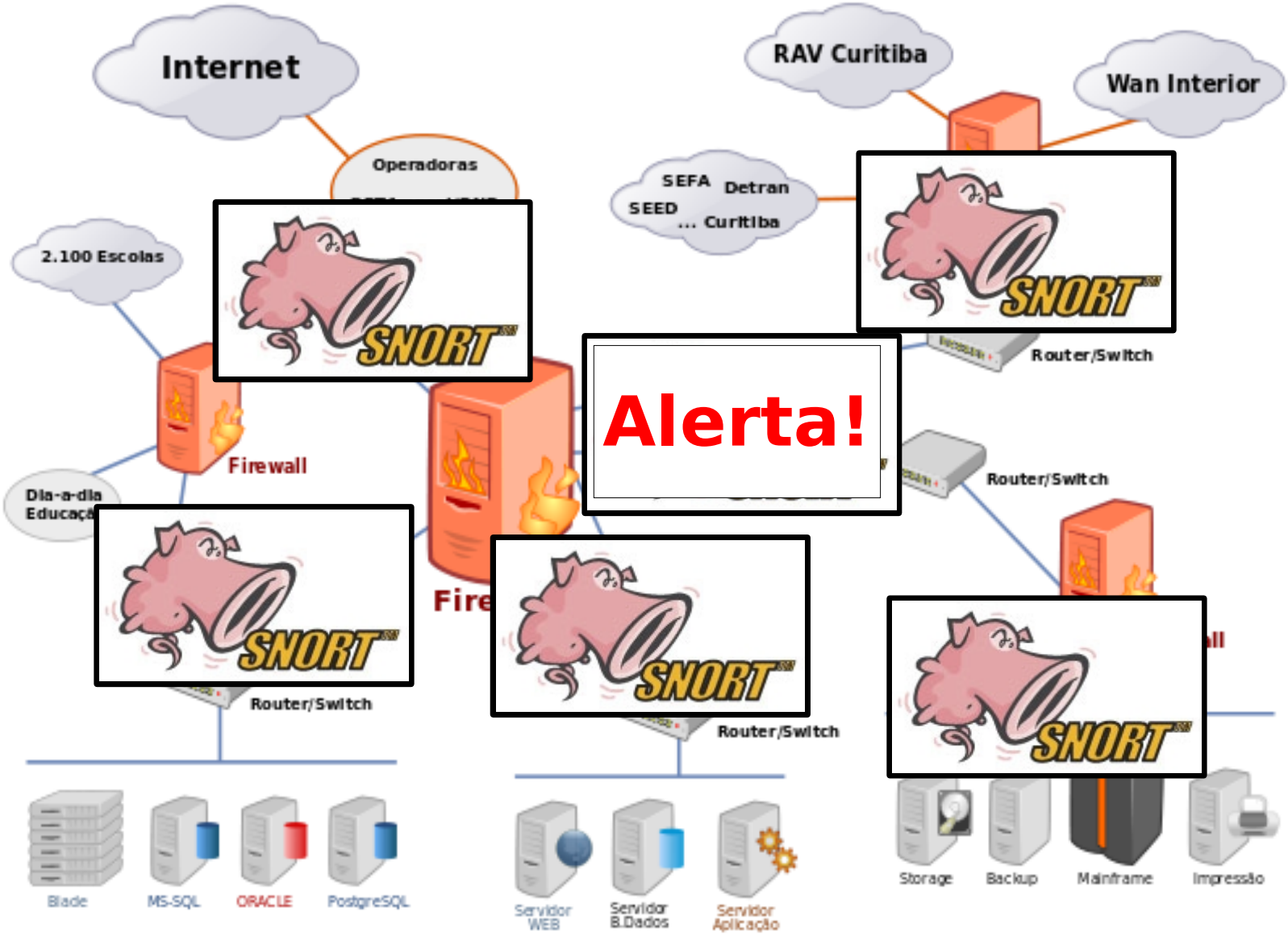
Sistemas de Detecção de Intrusão



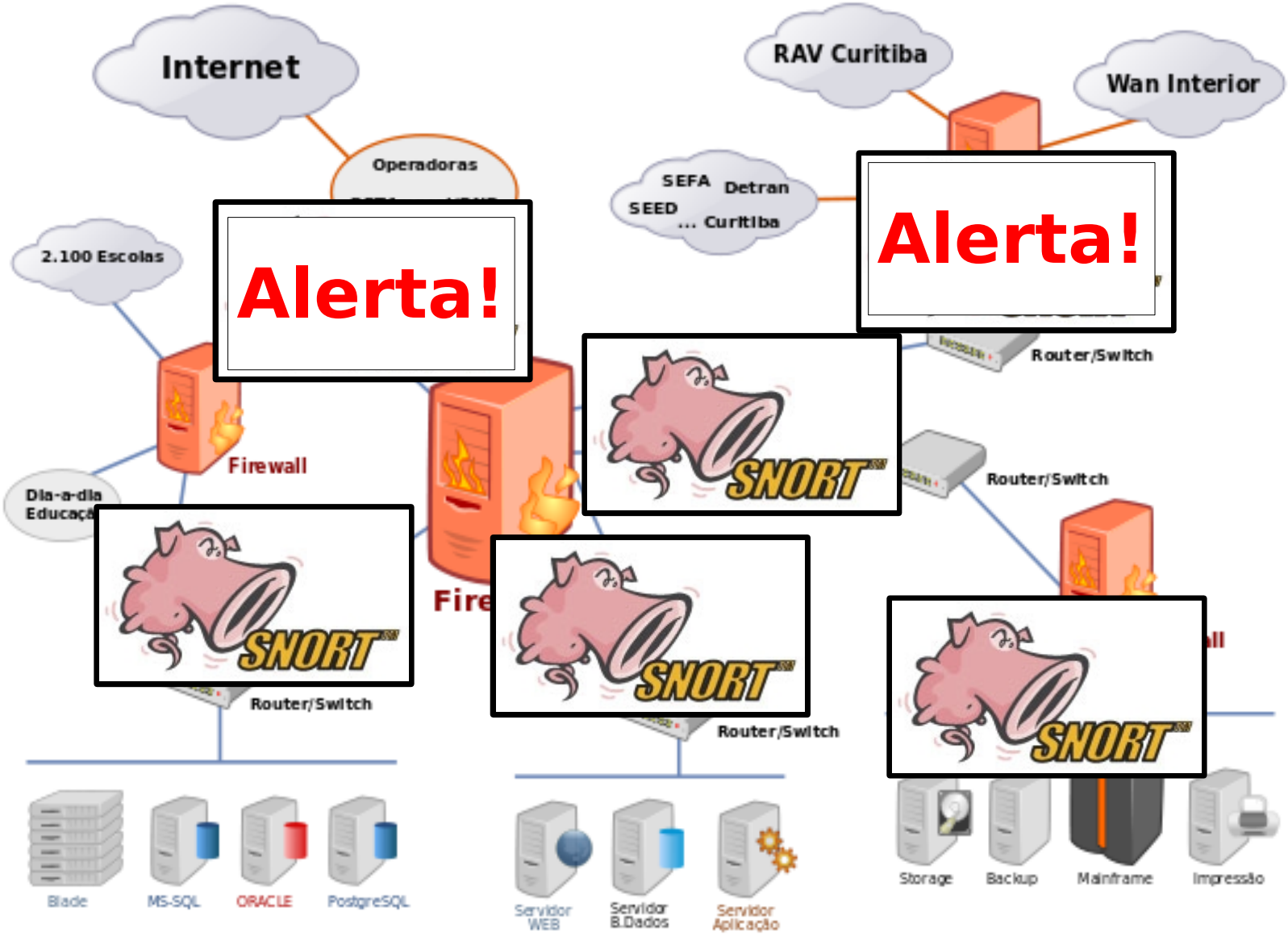
Sistemas de Detecção de Intrusão



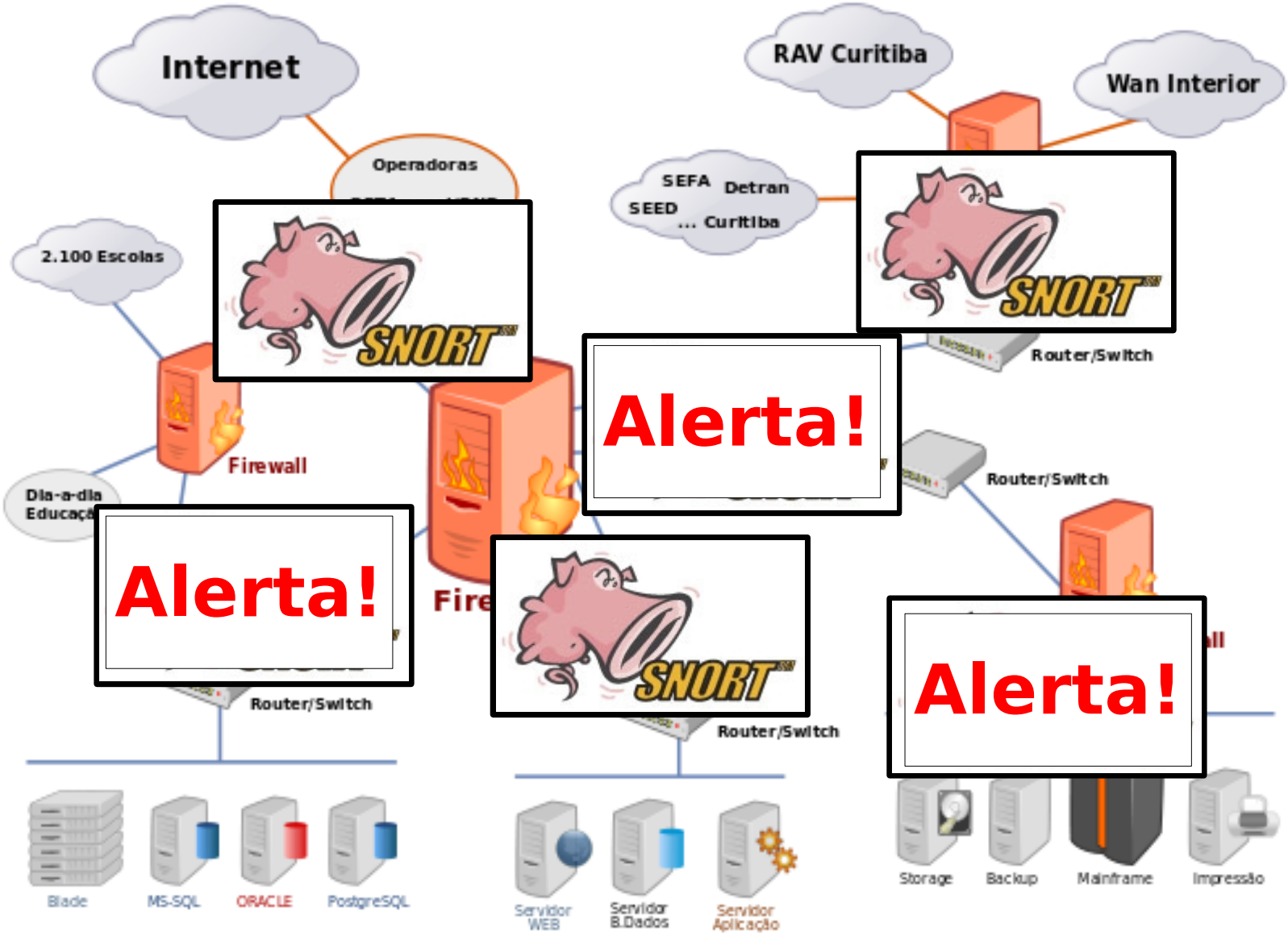
Sistemas de Detecção de Intrusão



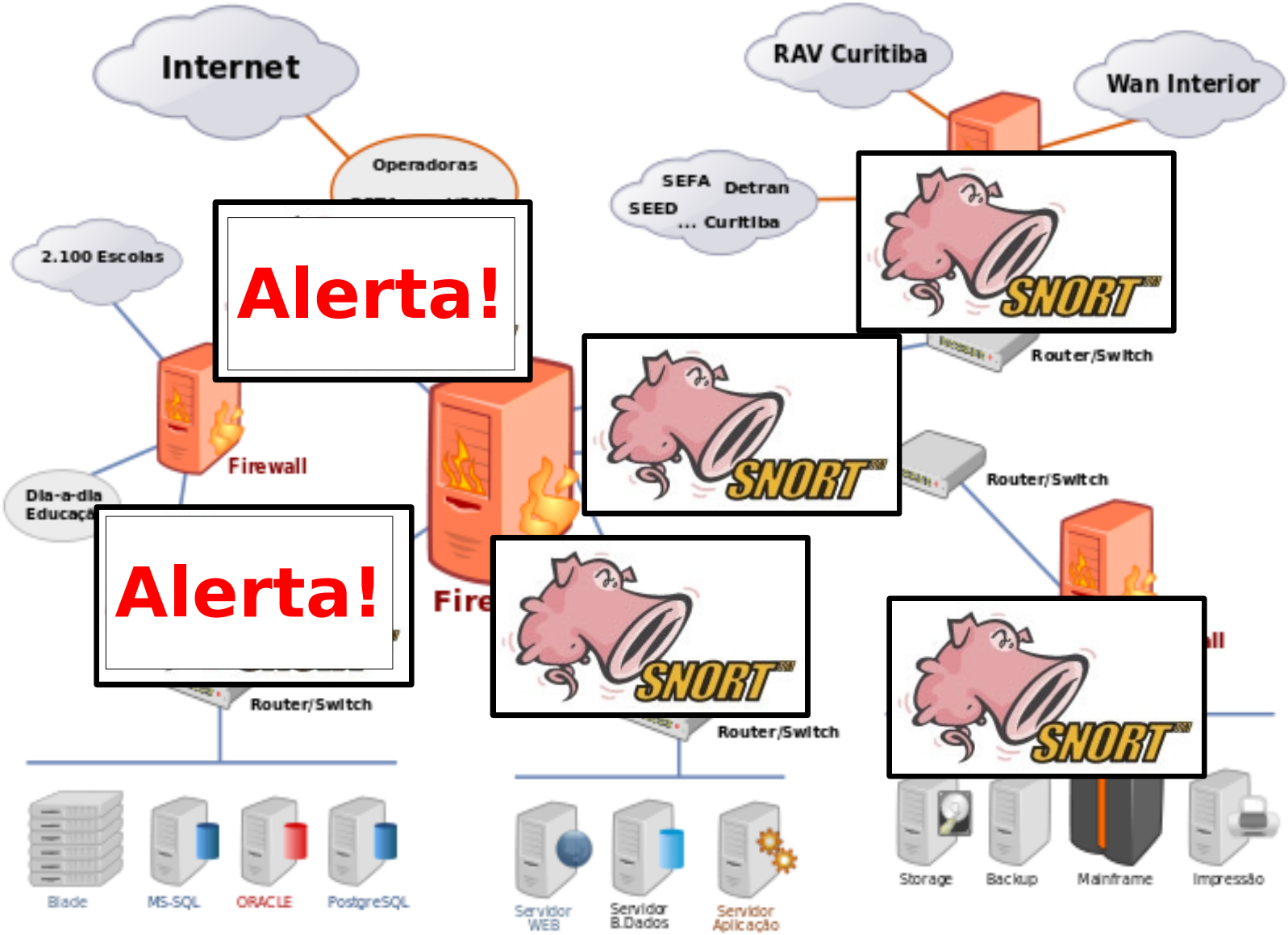
Sistemas de Detecção de Intrusão



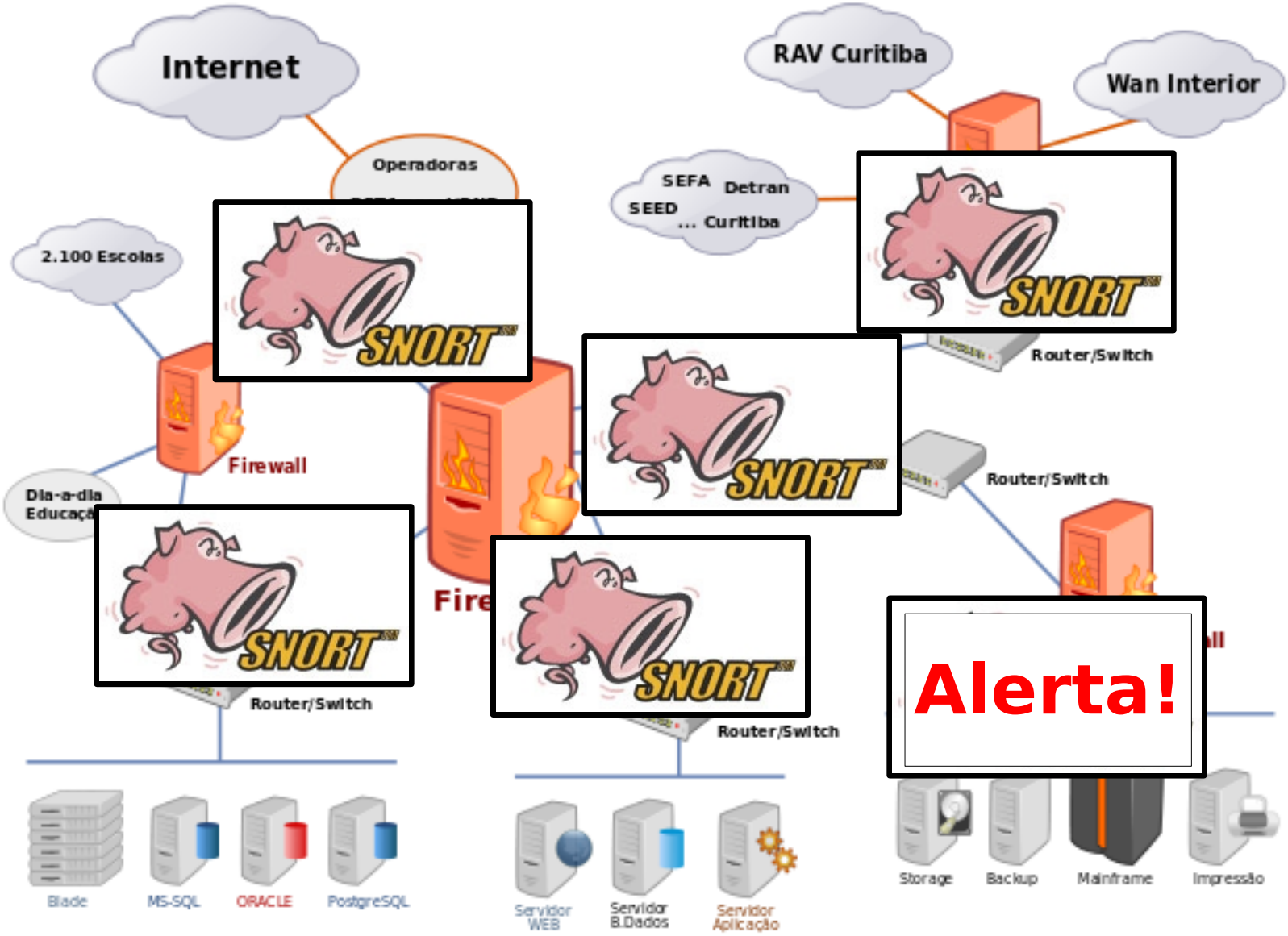
Sistemas de Detecção de Intrusão



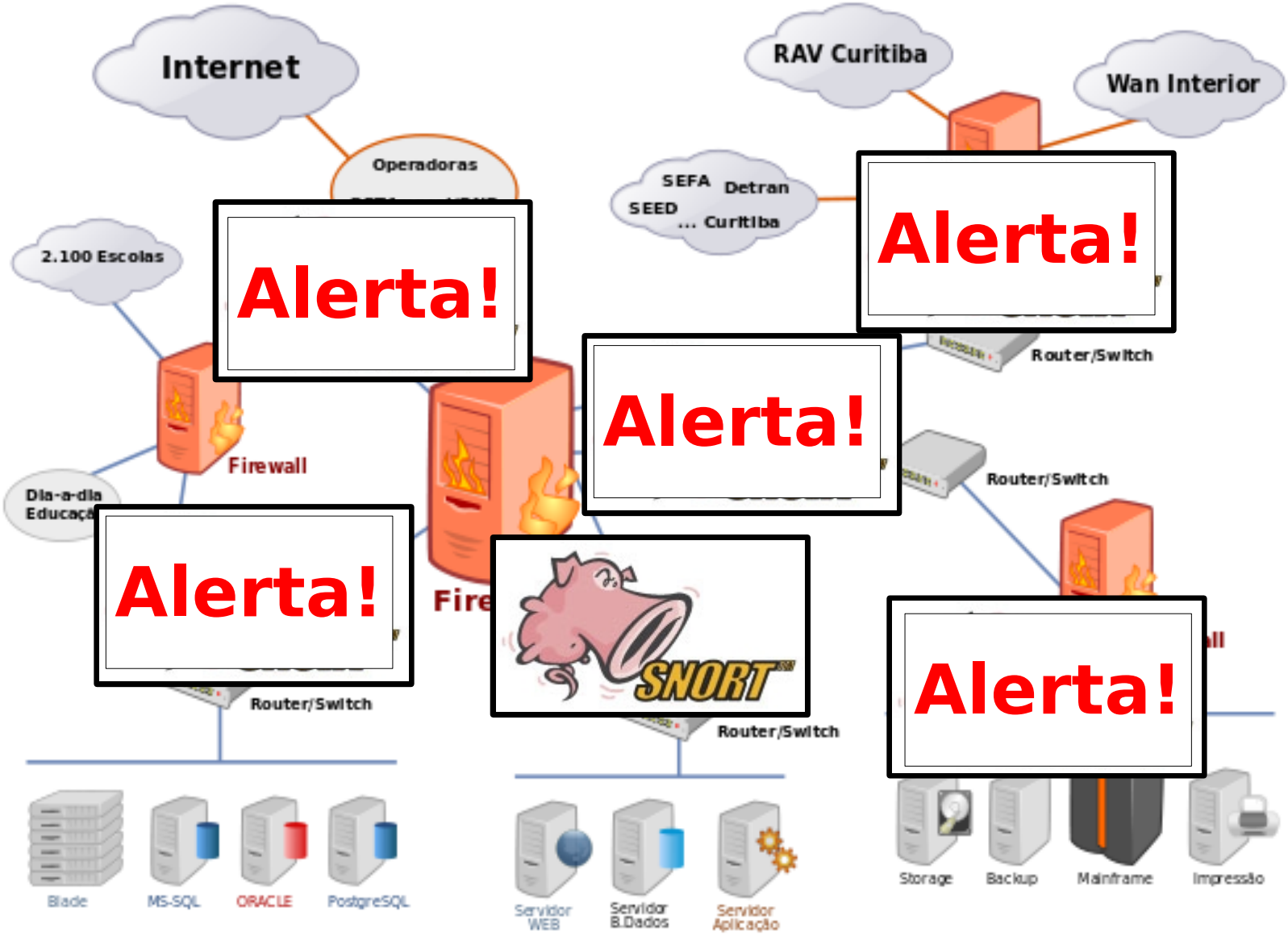
Sistemas de Detecção de Intrusão



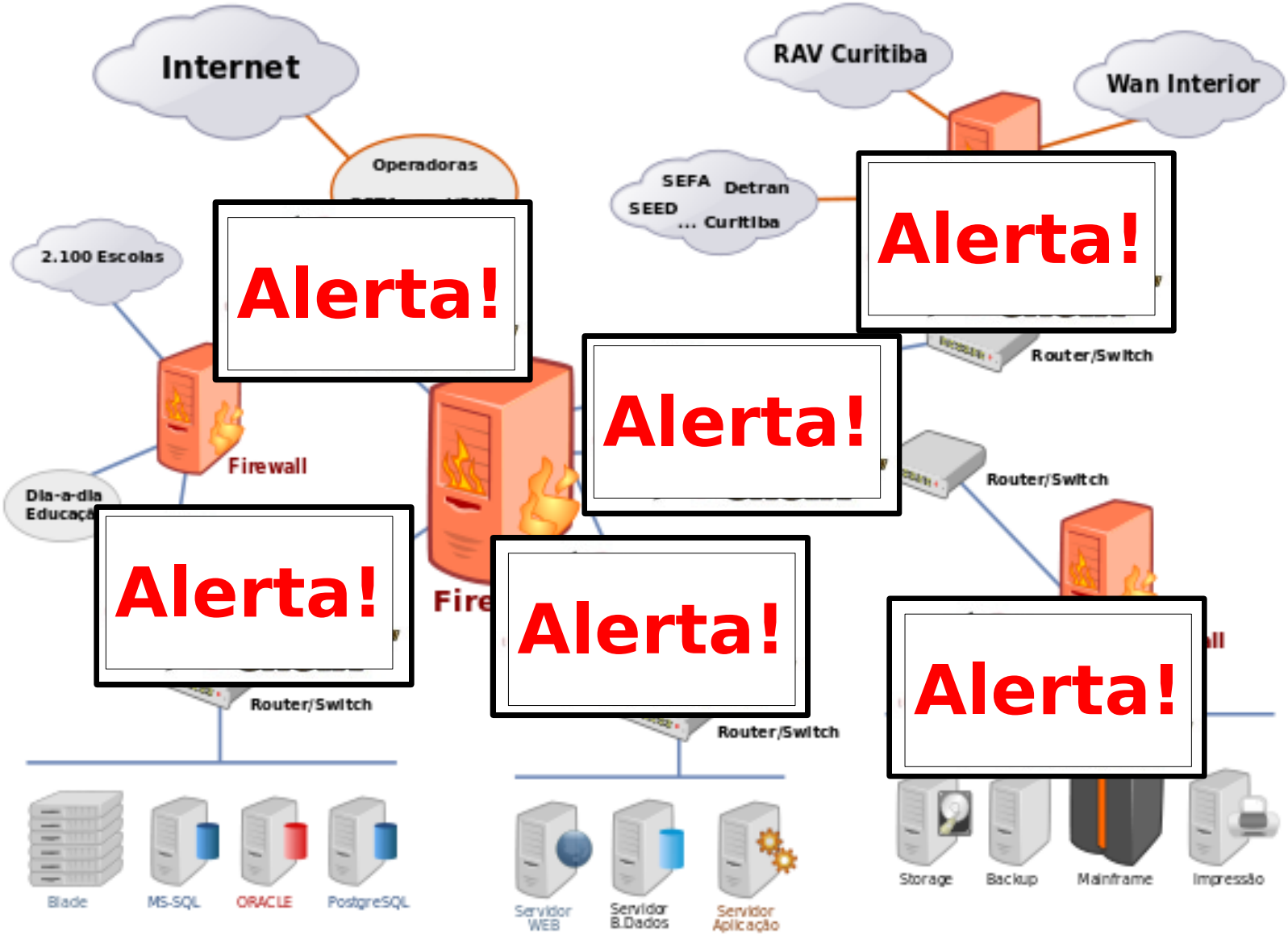
Sistemas de Detecção de Intrusão



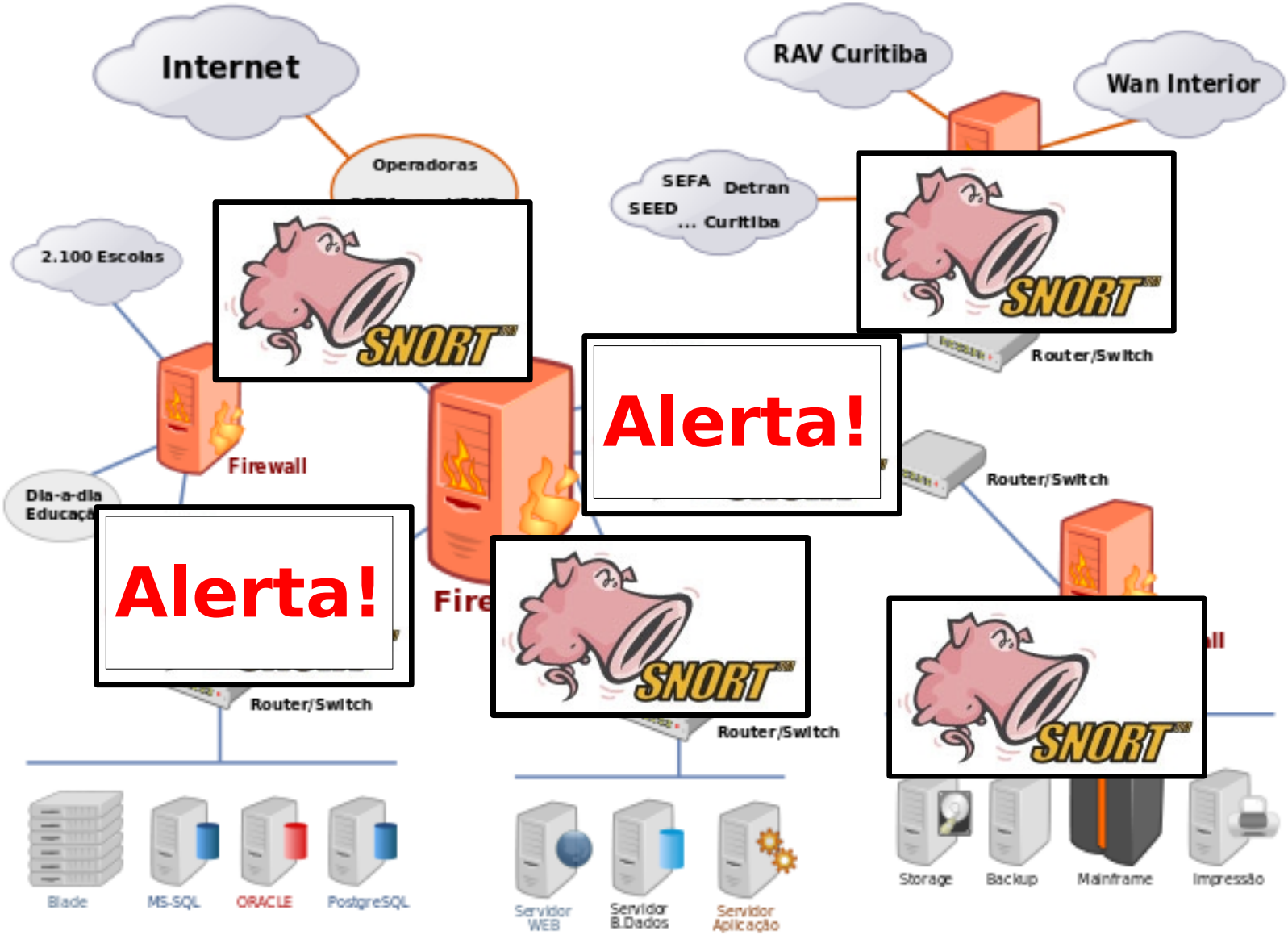
Sistemas de Detecção de Intrusão



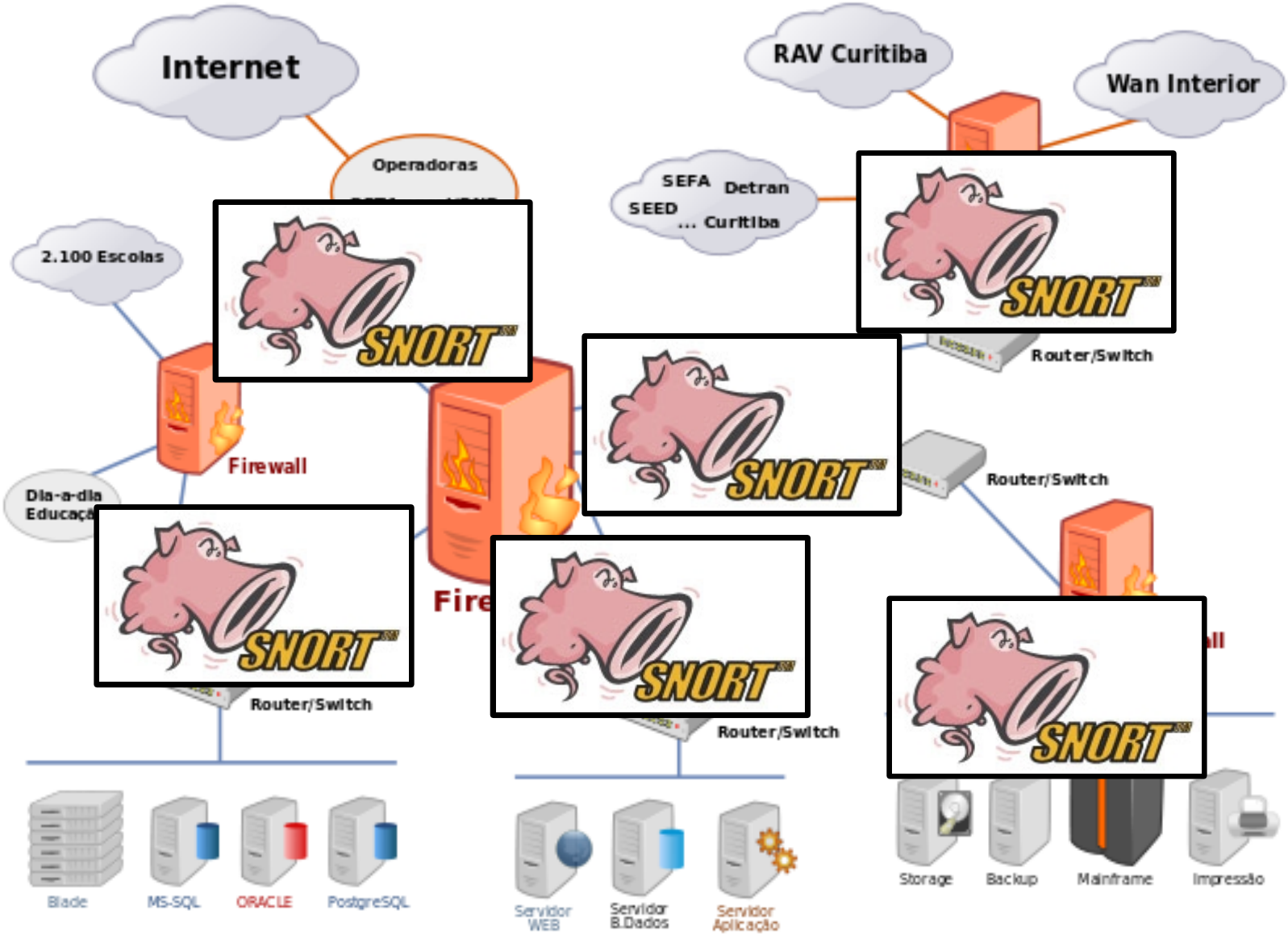
Sistemas de Detecção de Intrusão



Sistemas de Detecção de Intrusão



Sistemas de Detecção de Intrusão



Segurança da Informação e Gerência de Eventos

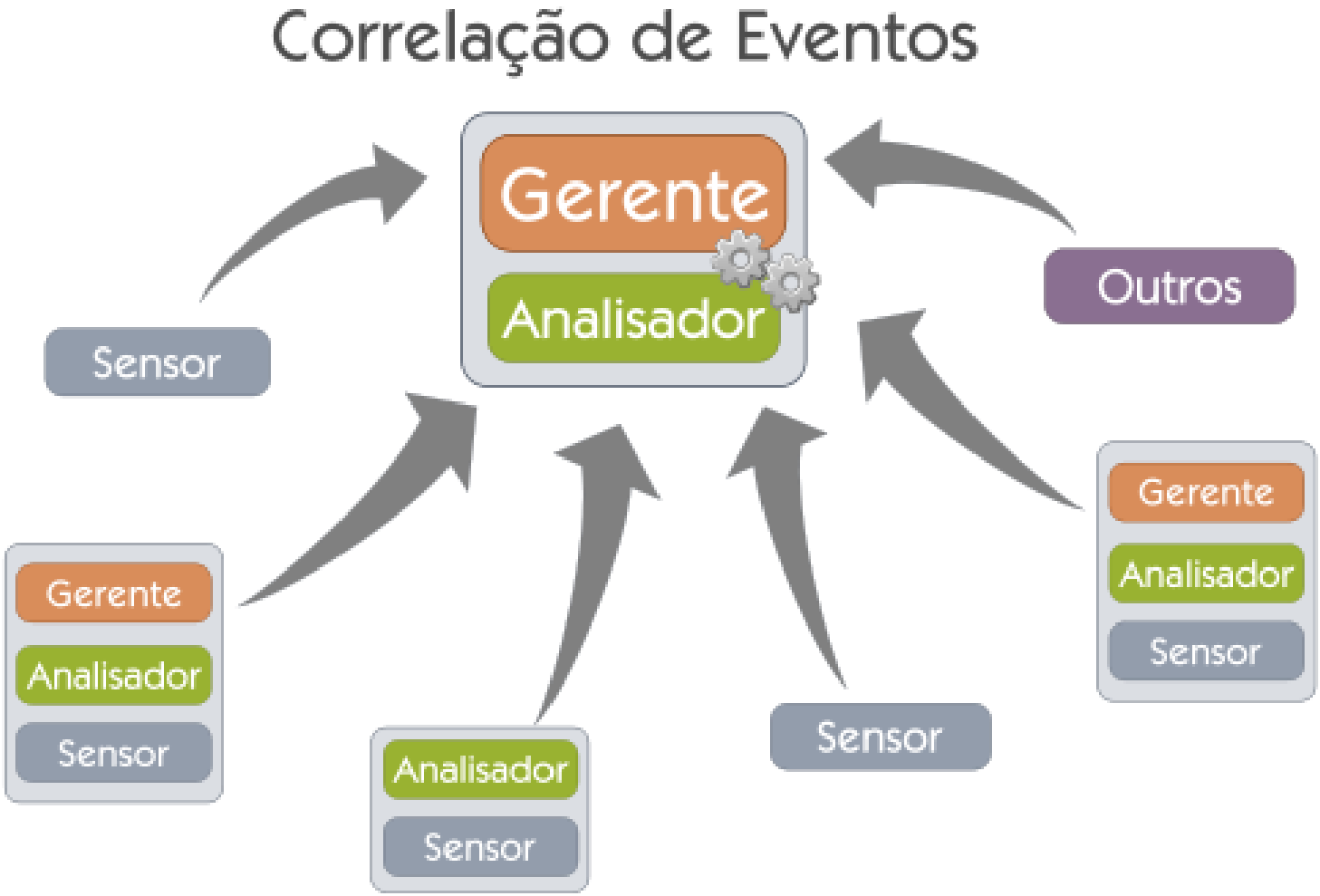
CELEPAR
INFORMÁTICA
do PARANÁ

Segurança e Gerência de Eventos

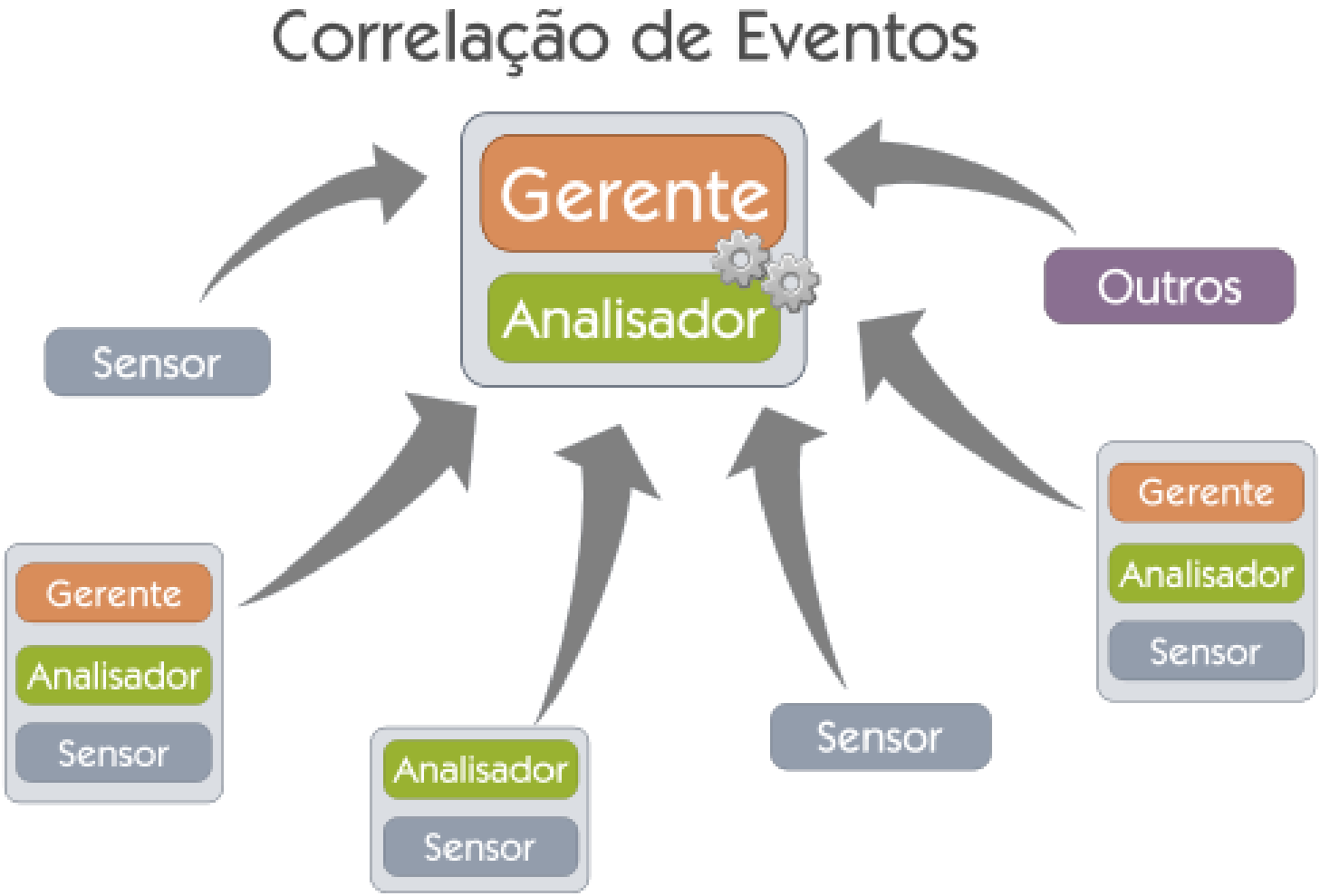
- Segurança da Informação e Gerência de Eventos *(Security Information and Event Management)*

  SIEM

  - SIEM centraliza os eventos
  - SIEM aceita eventos de diversas origens
  - SIEM correlaciona eventos para identificar ataques
  - SIEM implementa o protocolo IDMEF

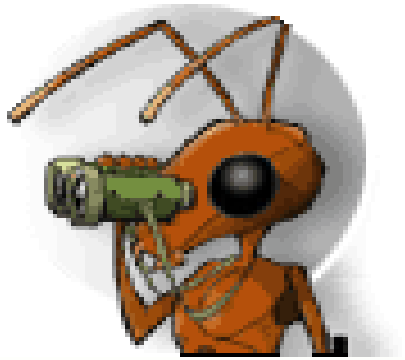

Correlação de Eventos
Gerente
Analisador
Sensor
Outros
Gerente
Analisador
Sensor
Analisador
Sensor
Sensor
Gerente
Analisador
Sensor

Segurança e Gerência de Eventos

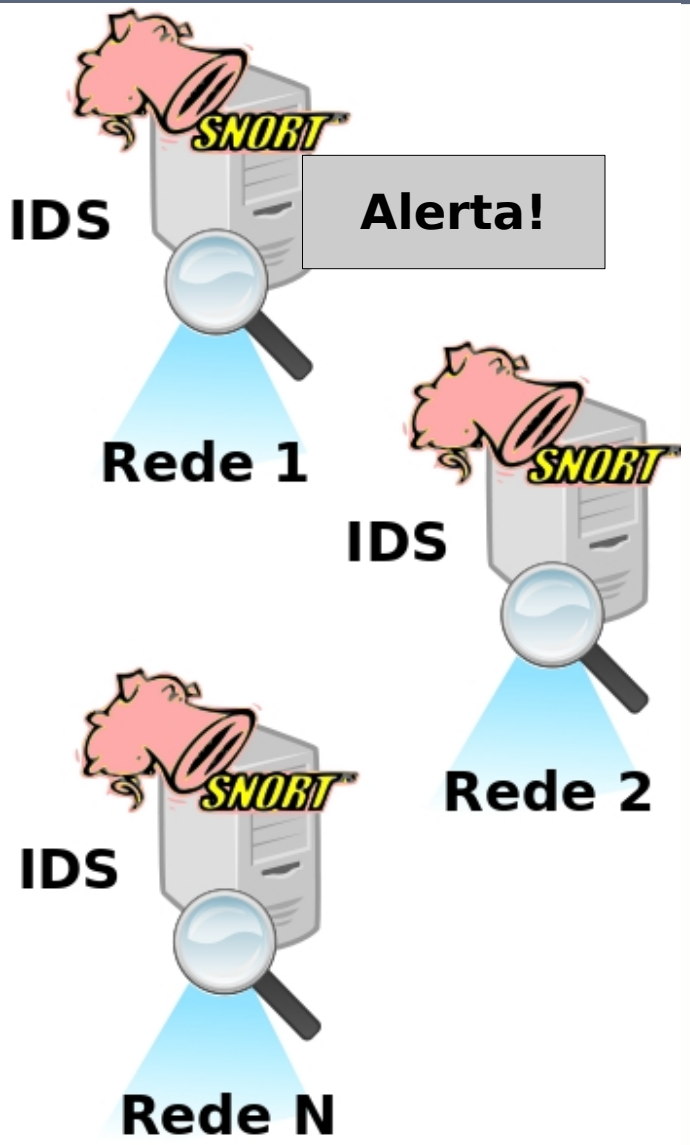


Segurança e Gerência de Eventos

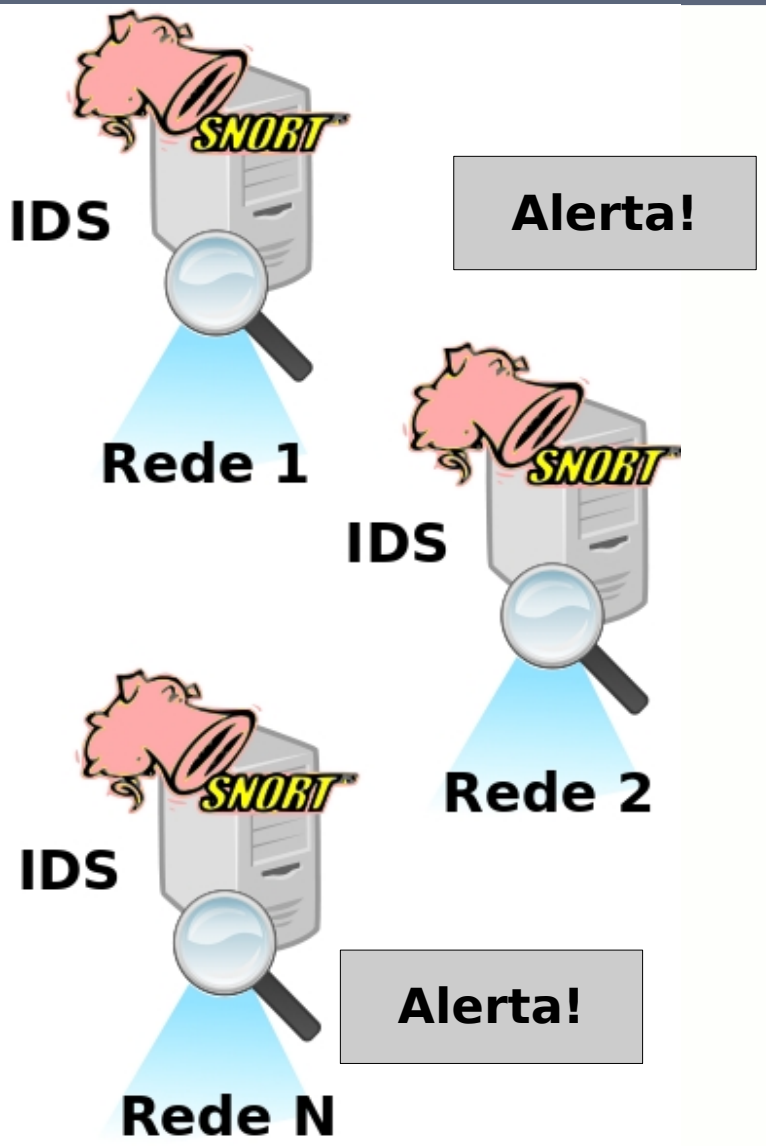
- PRELUDE SIEM
  - Desde 2005 (IDS->SIEM)
  - Software Livre
  - Gerenciador em ambiente Web
  - Correlacionador
  - Sensores: Snort, AuditD, Nepenthes, NuFW, OSSEC, PAM, Samhain, SanCP, etc...



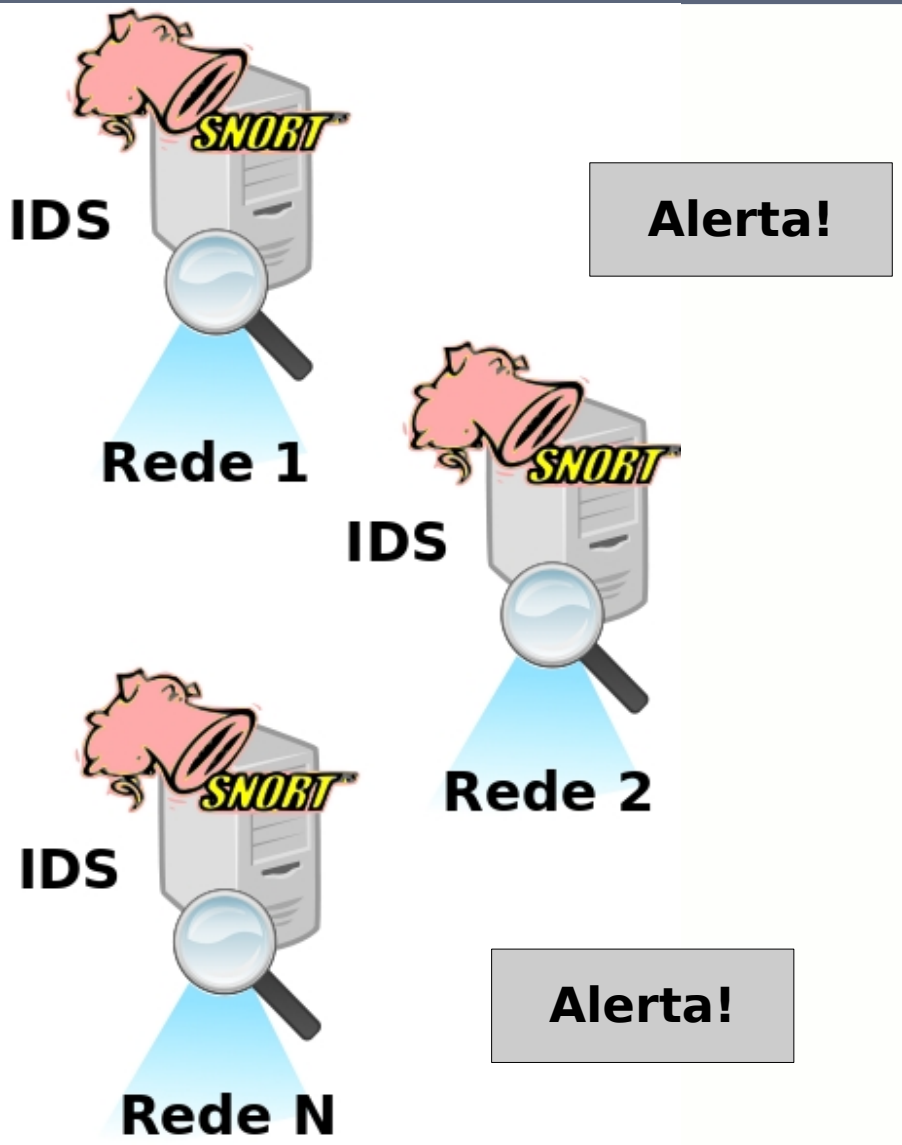
Prelude


SNORT
IDS
Alerta!
Rede 1
SNORT
IDS
Rede 2
SNORT
IDS
Rede N

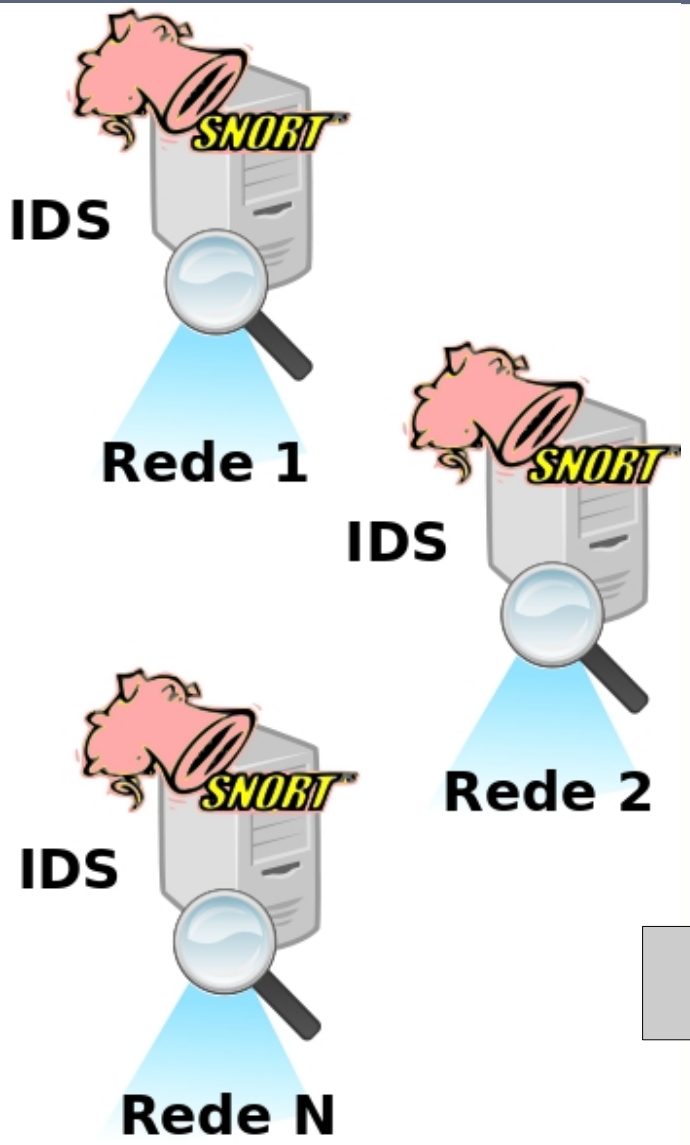
Segurança e Gerência de Eventos



Segurança e Gerência de Eventos



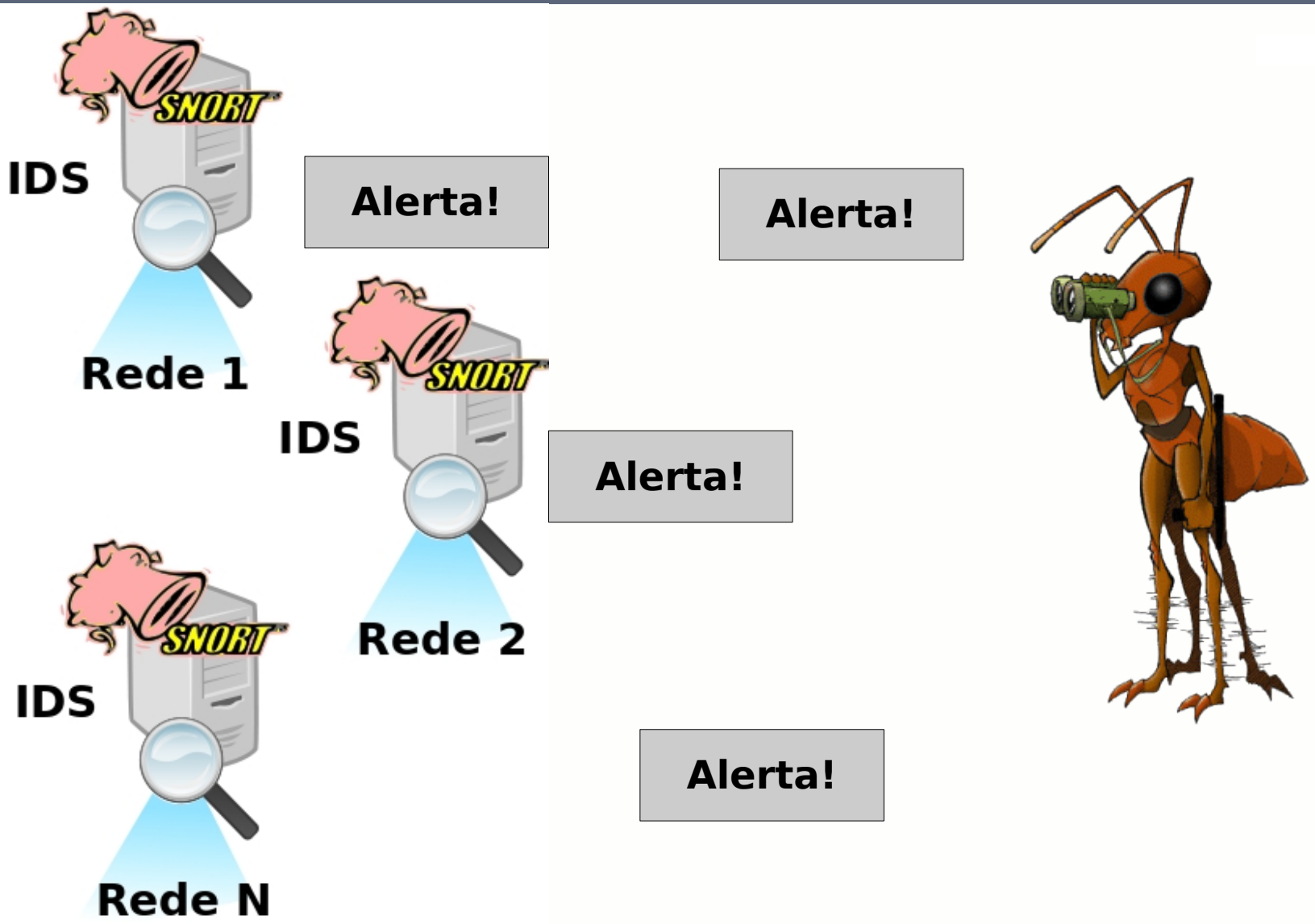
Segurança e Gerência de Eventos



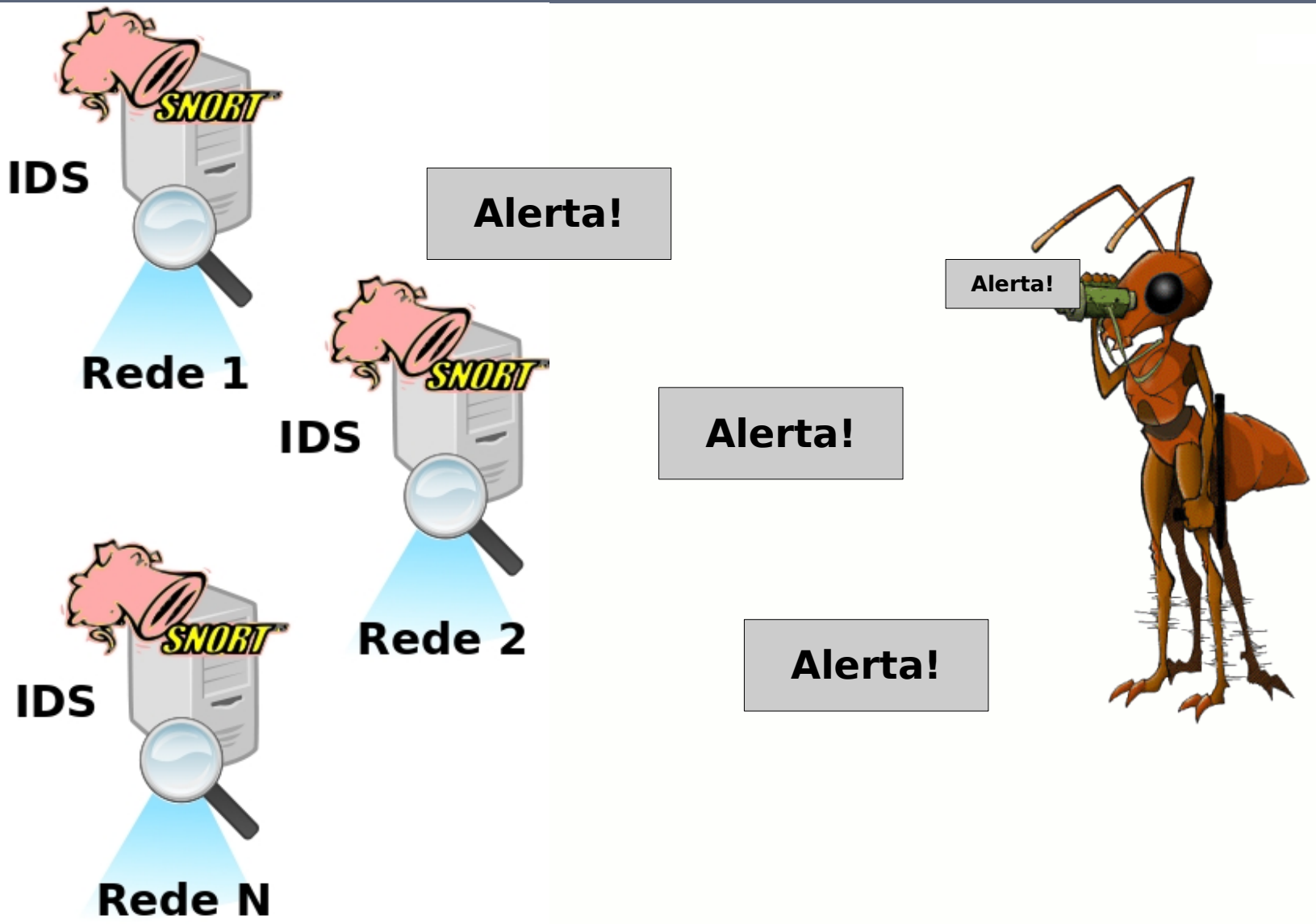
Alerta!

Alerta!

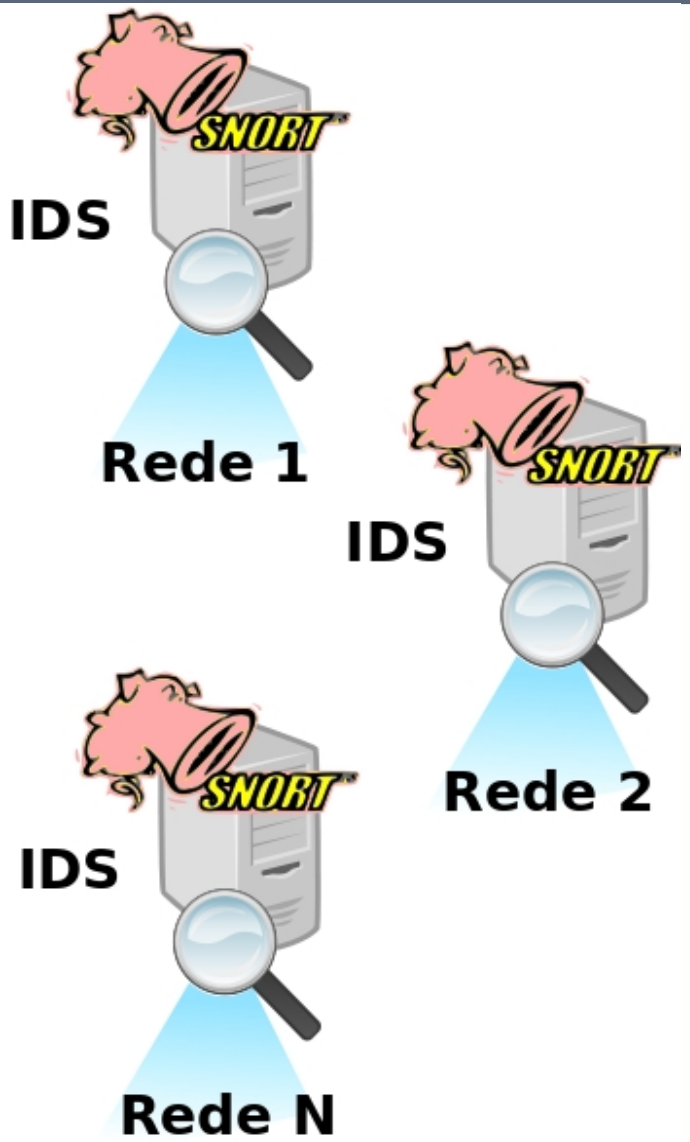
Segurança e Gerência de Eventos



Segurança e Gerência de Eventos



Segurança e Gerência de Eventos

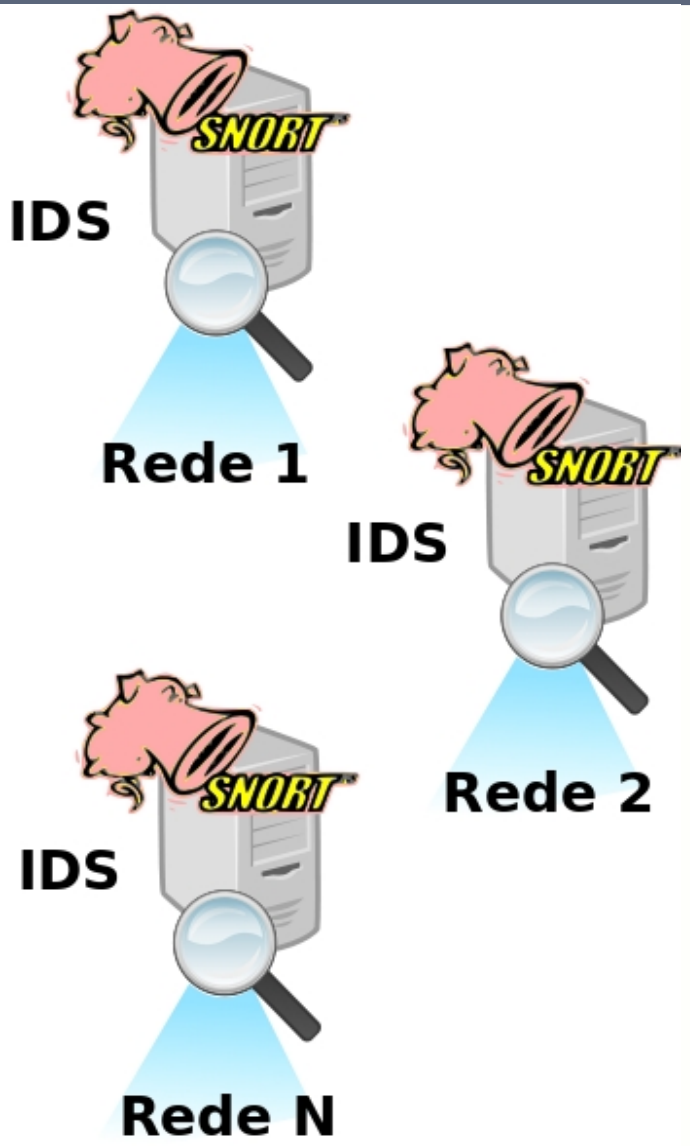


Alerta!

Alerta!

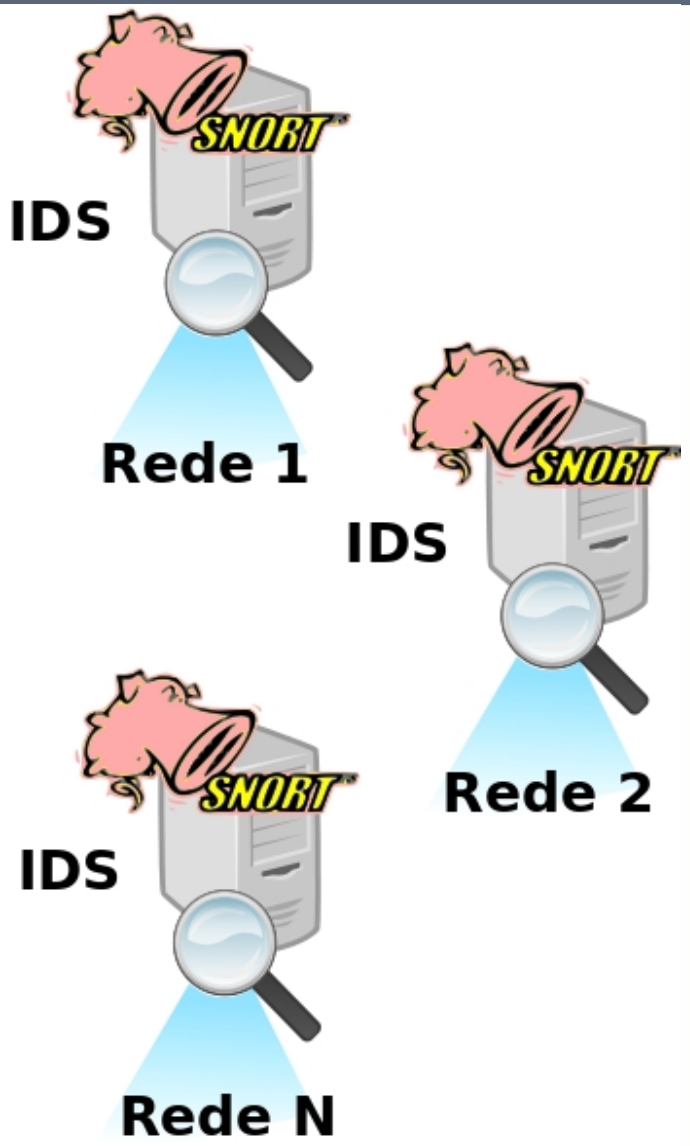
Alerta!

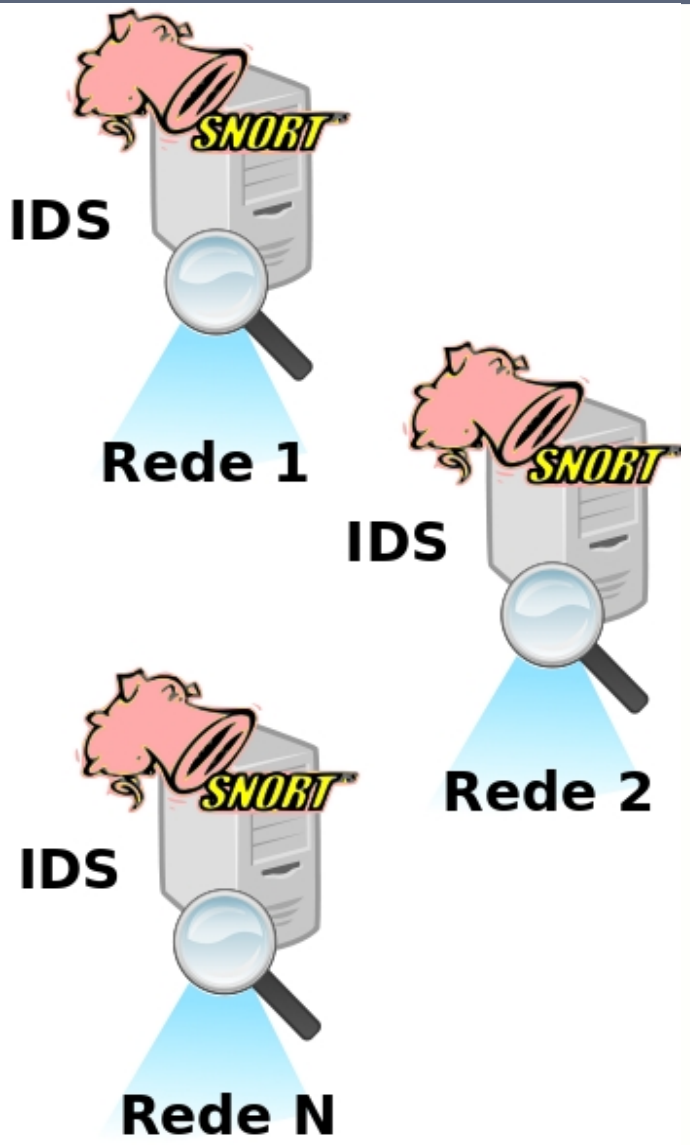
Segurança e Gerência de Eventos



Alerta!

Segurança e Gerência de Eventos

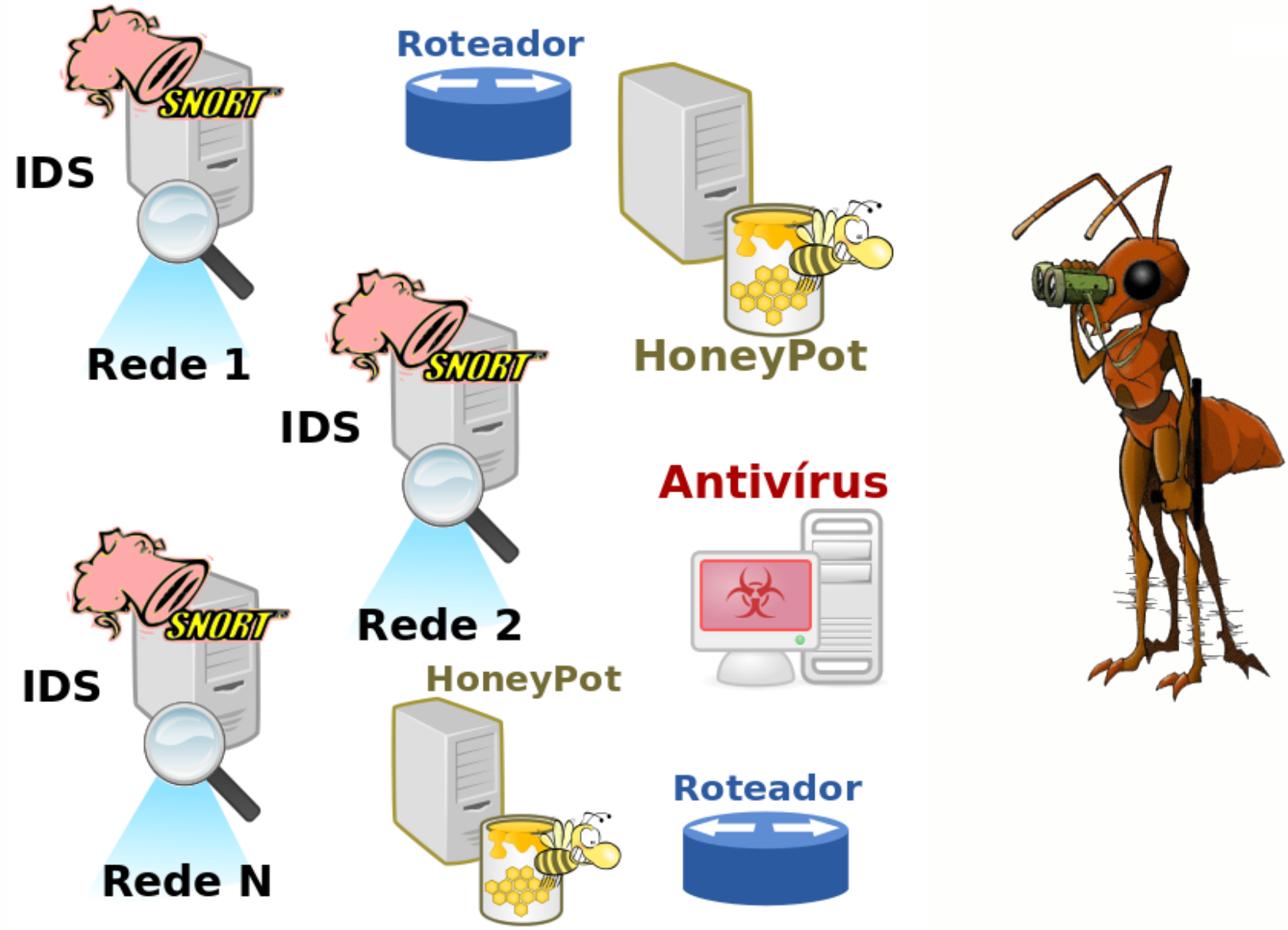




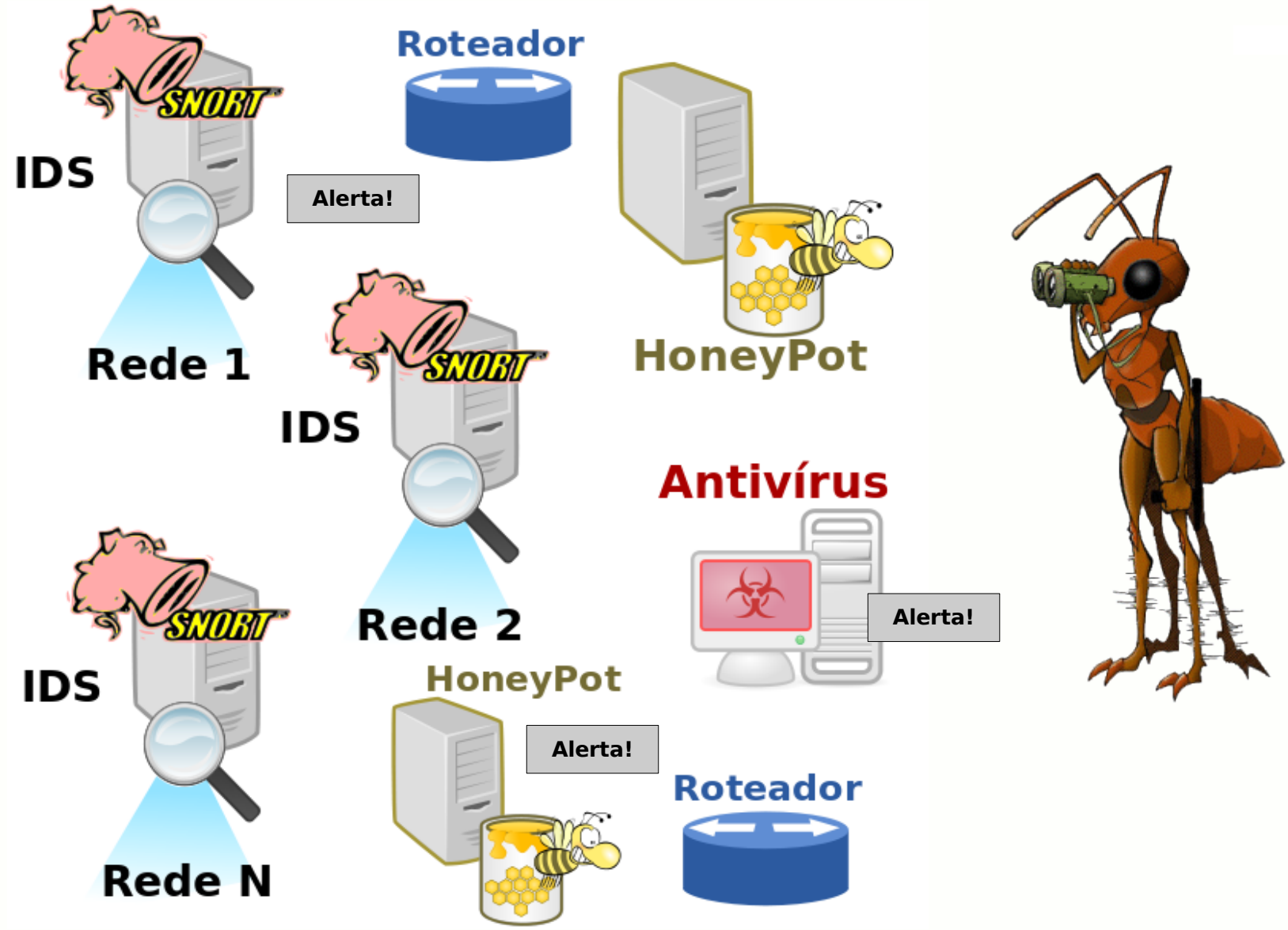
Ataque!

3x Alerta X
1x Alerta Y

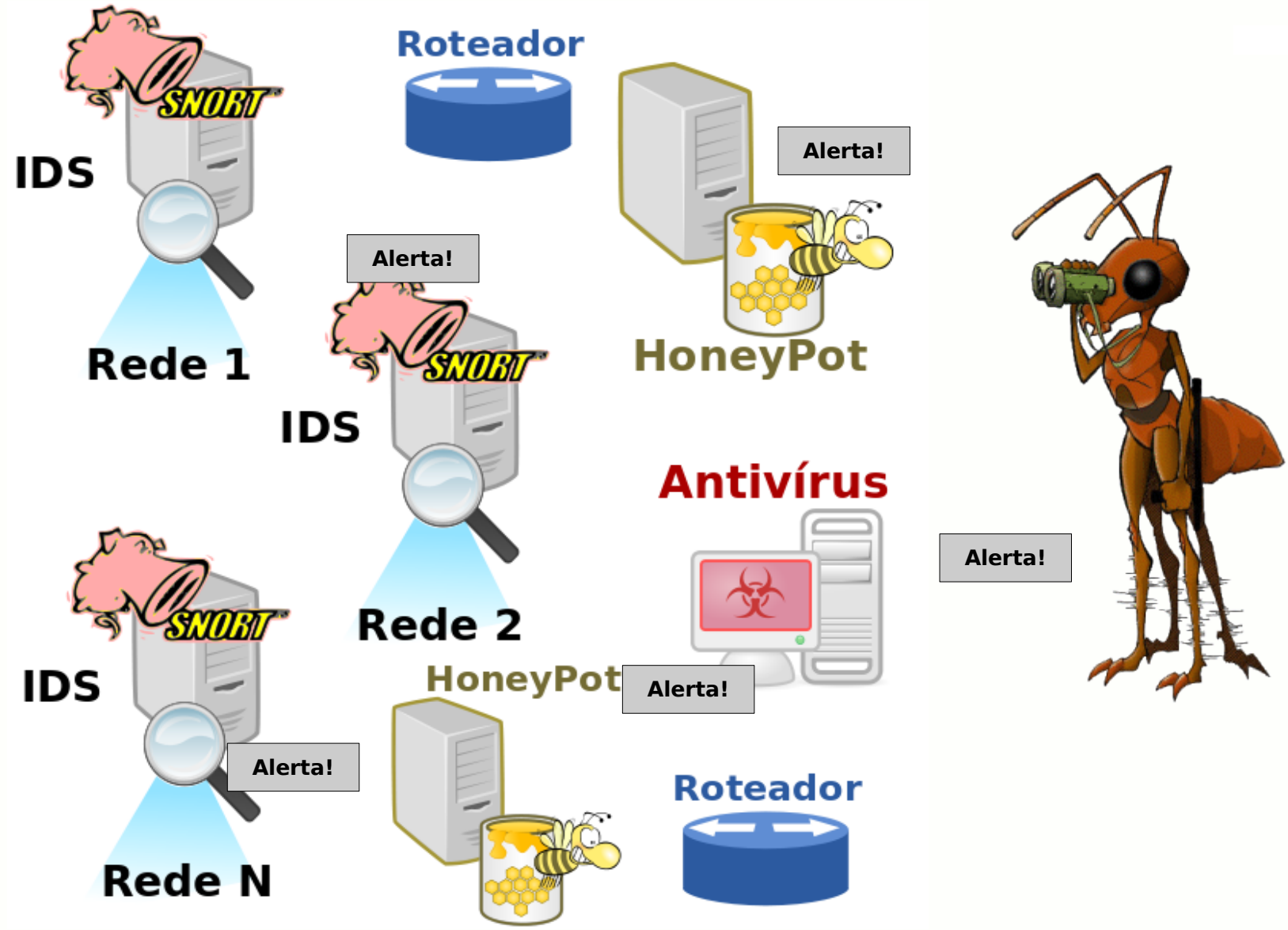
Segurança e Gerência de Eventos



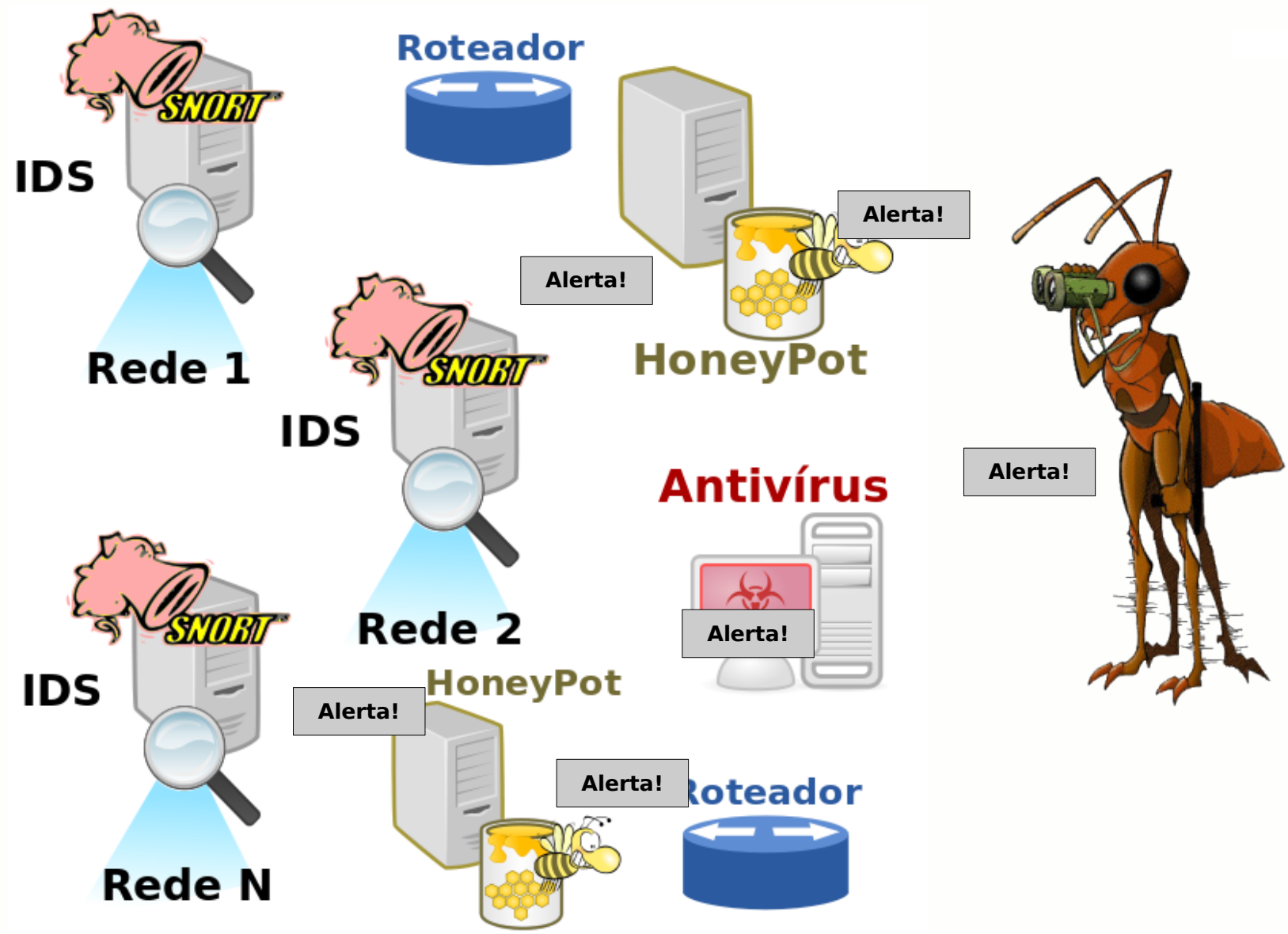
Segurança e Gerência de Eventos



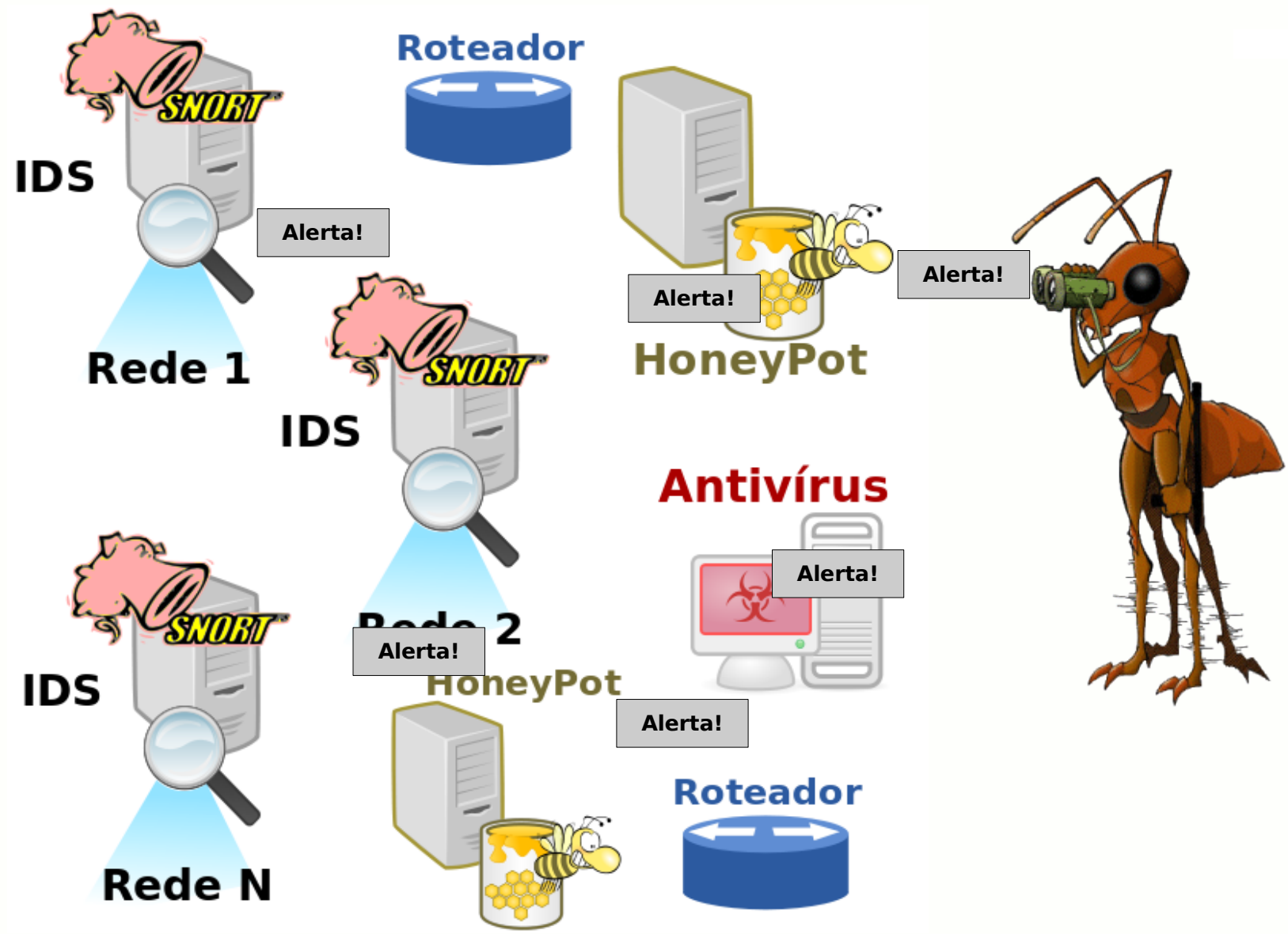
Segurança e Gerência de Eventos



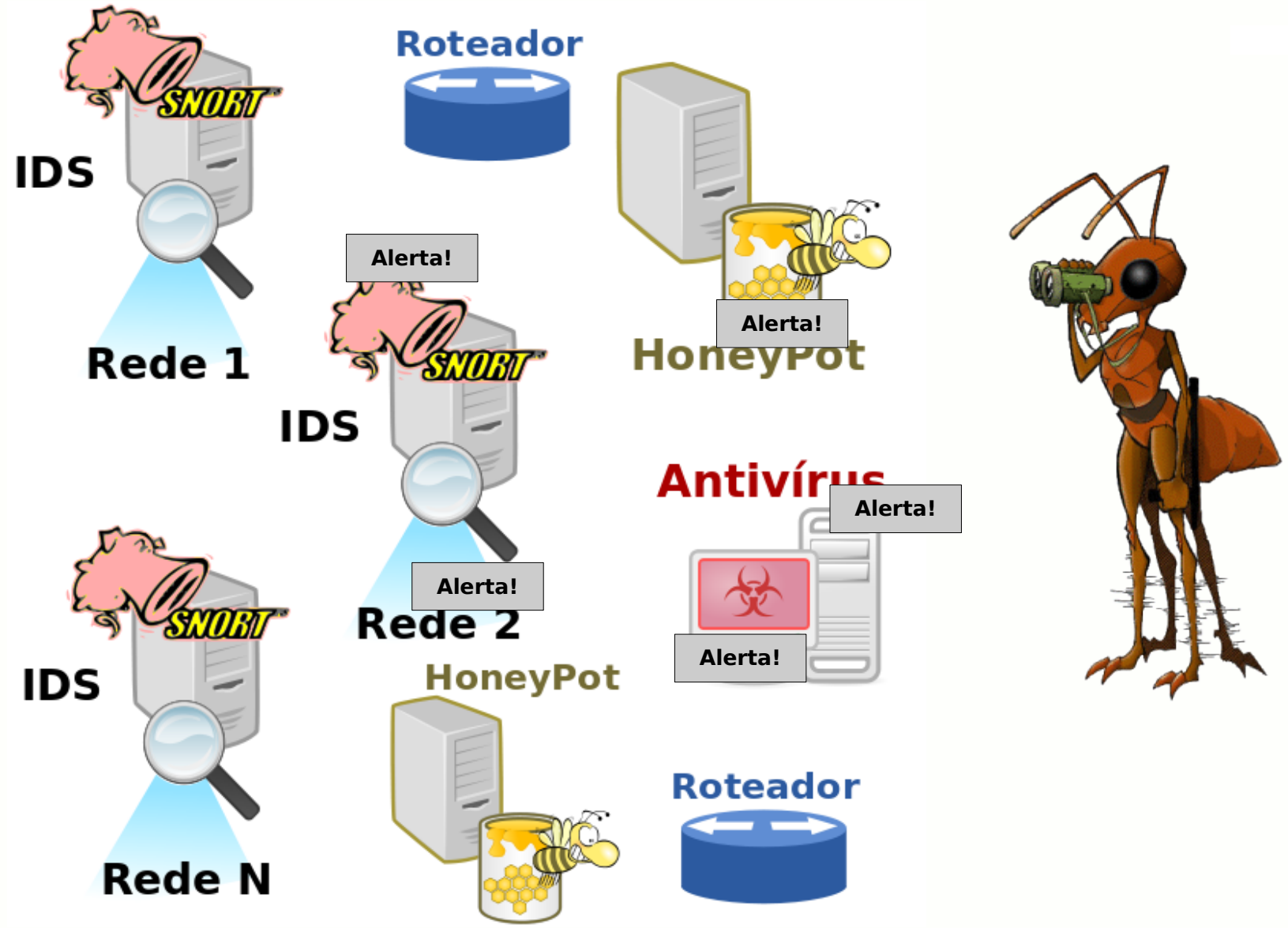
Segurança e Gerência de Eventos



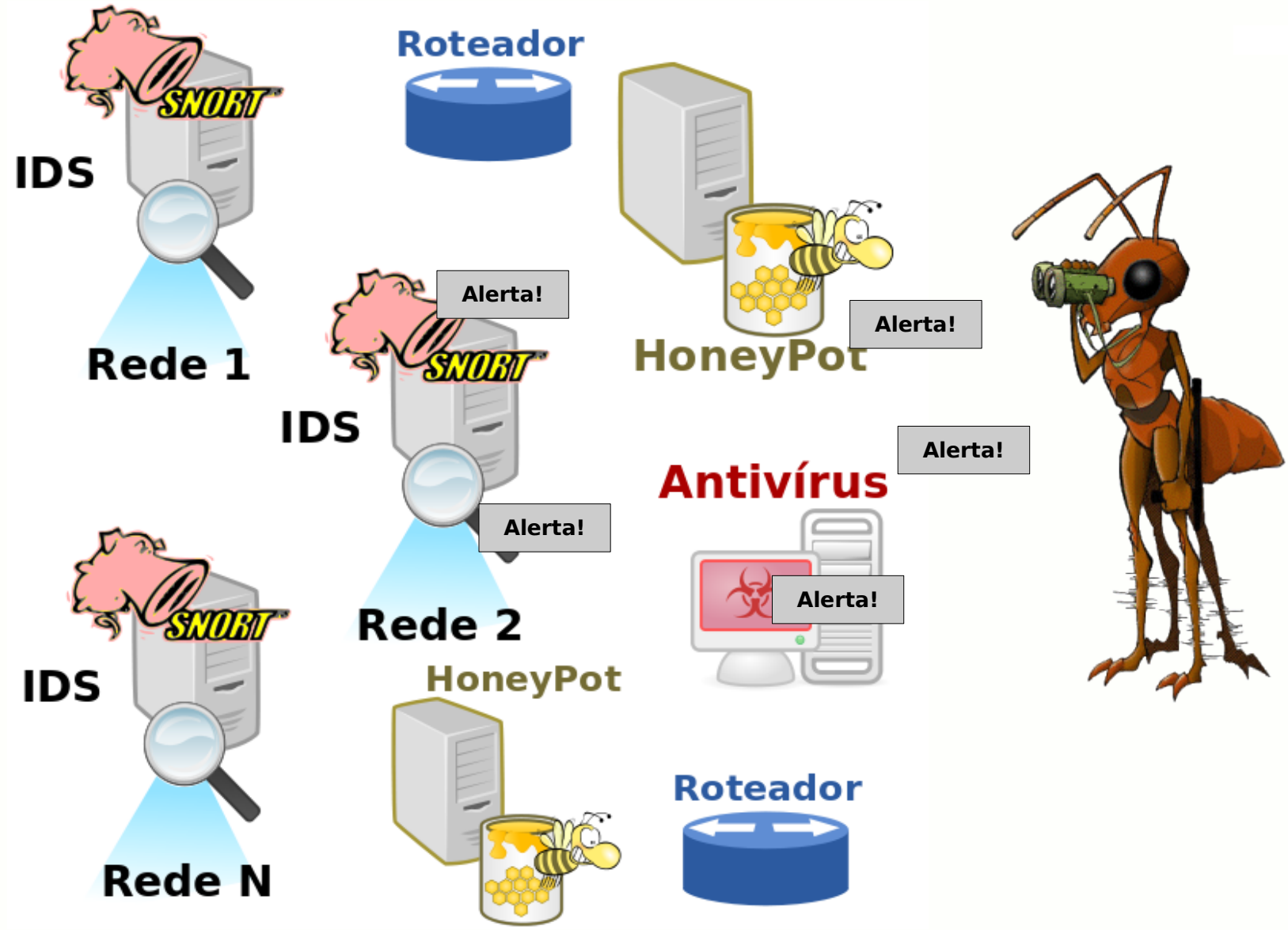
Segurança e Gerência de Eventos



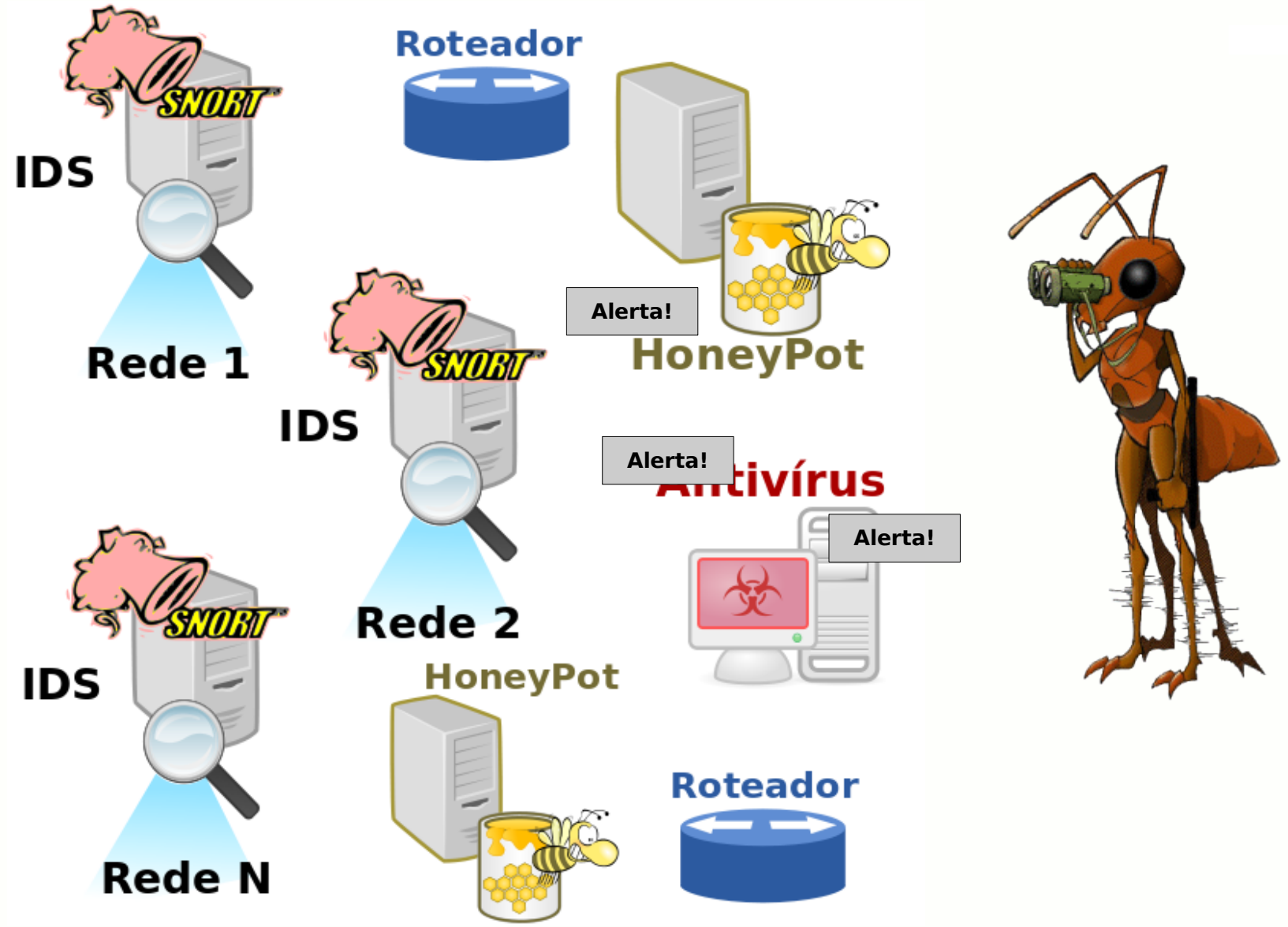
Segurança e Gerência de Eventos



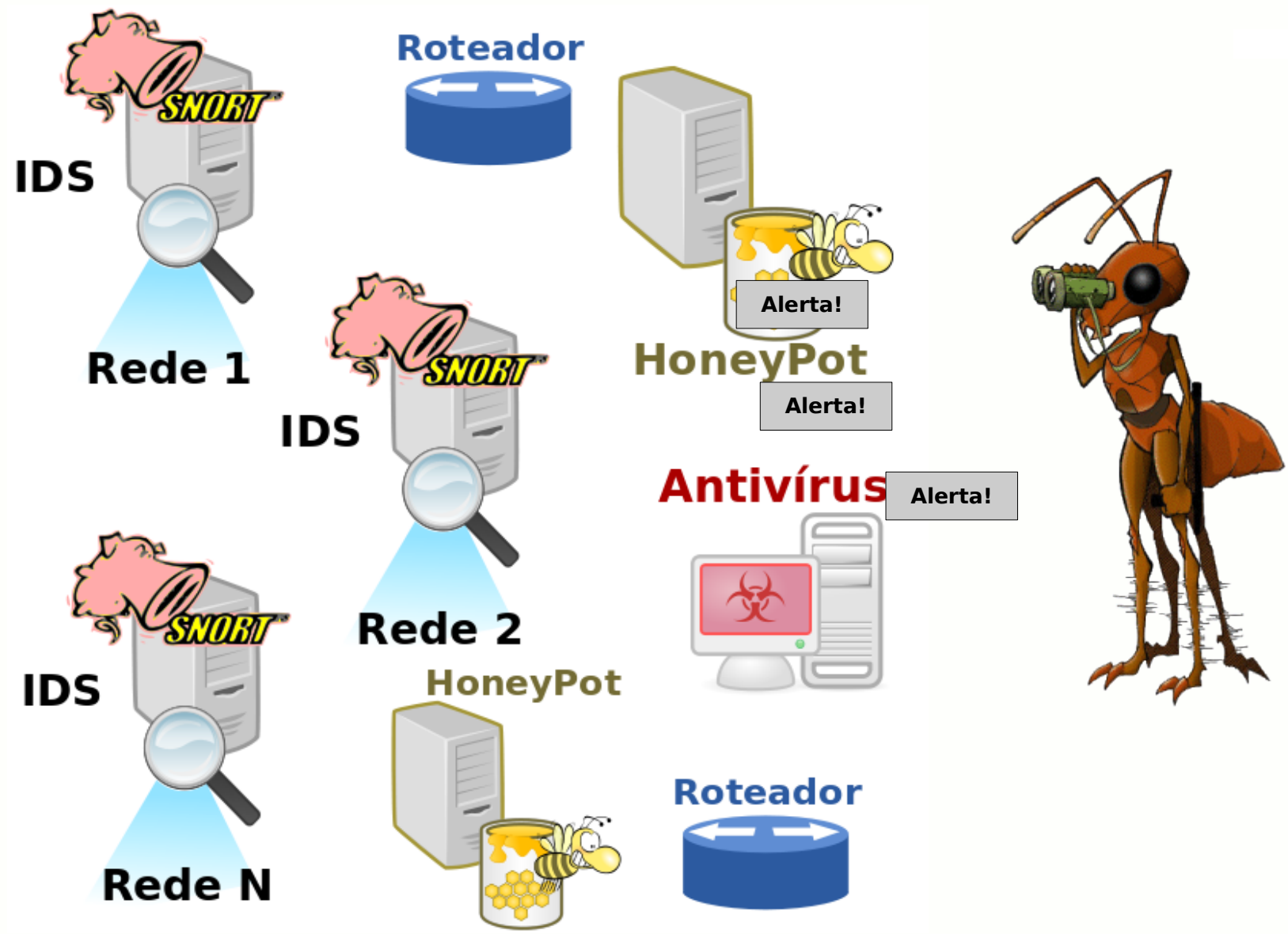
Segurança e Gerência de Eventos



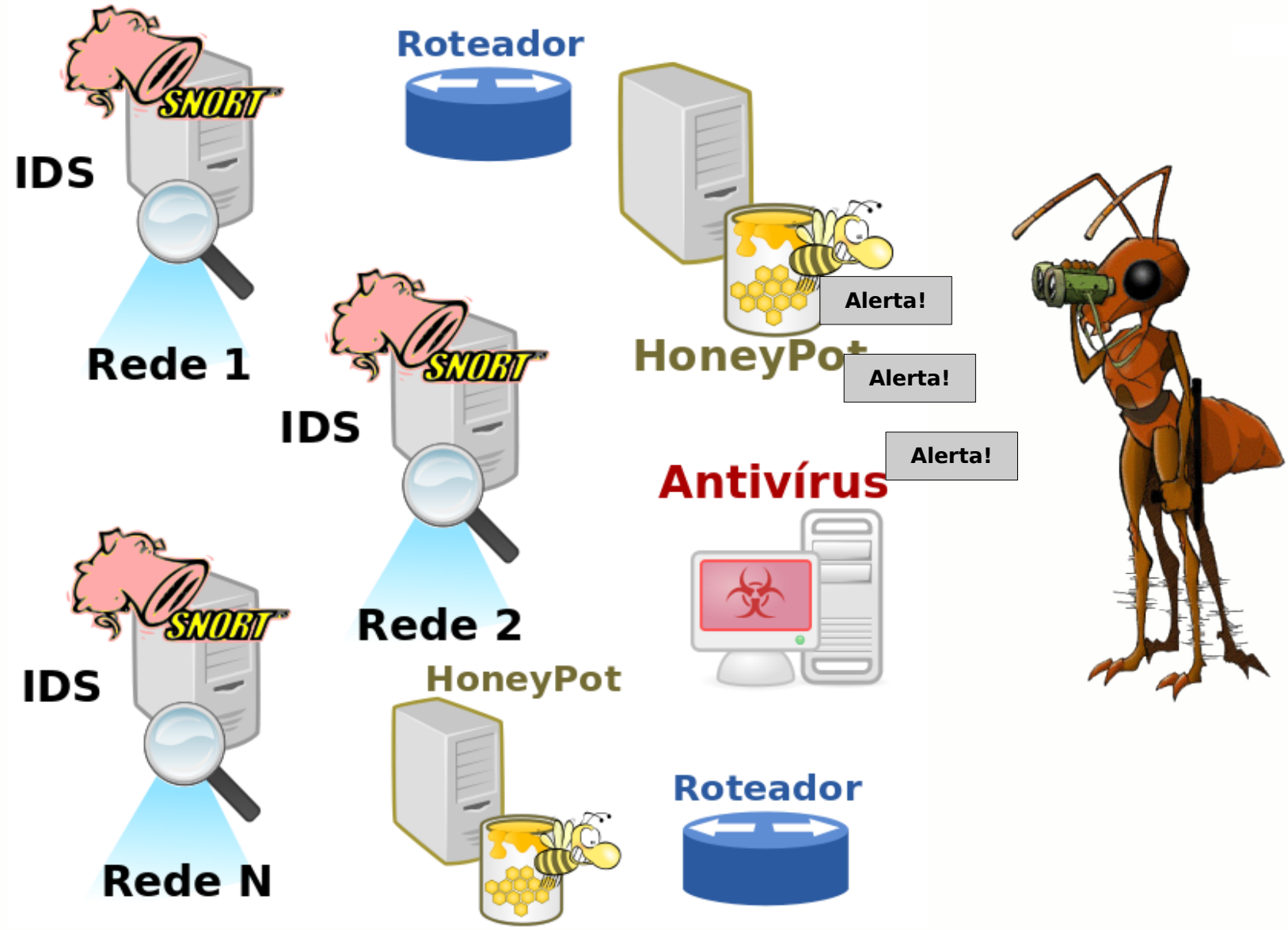
Segurança e Gerência de Eventos



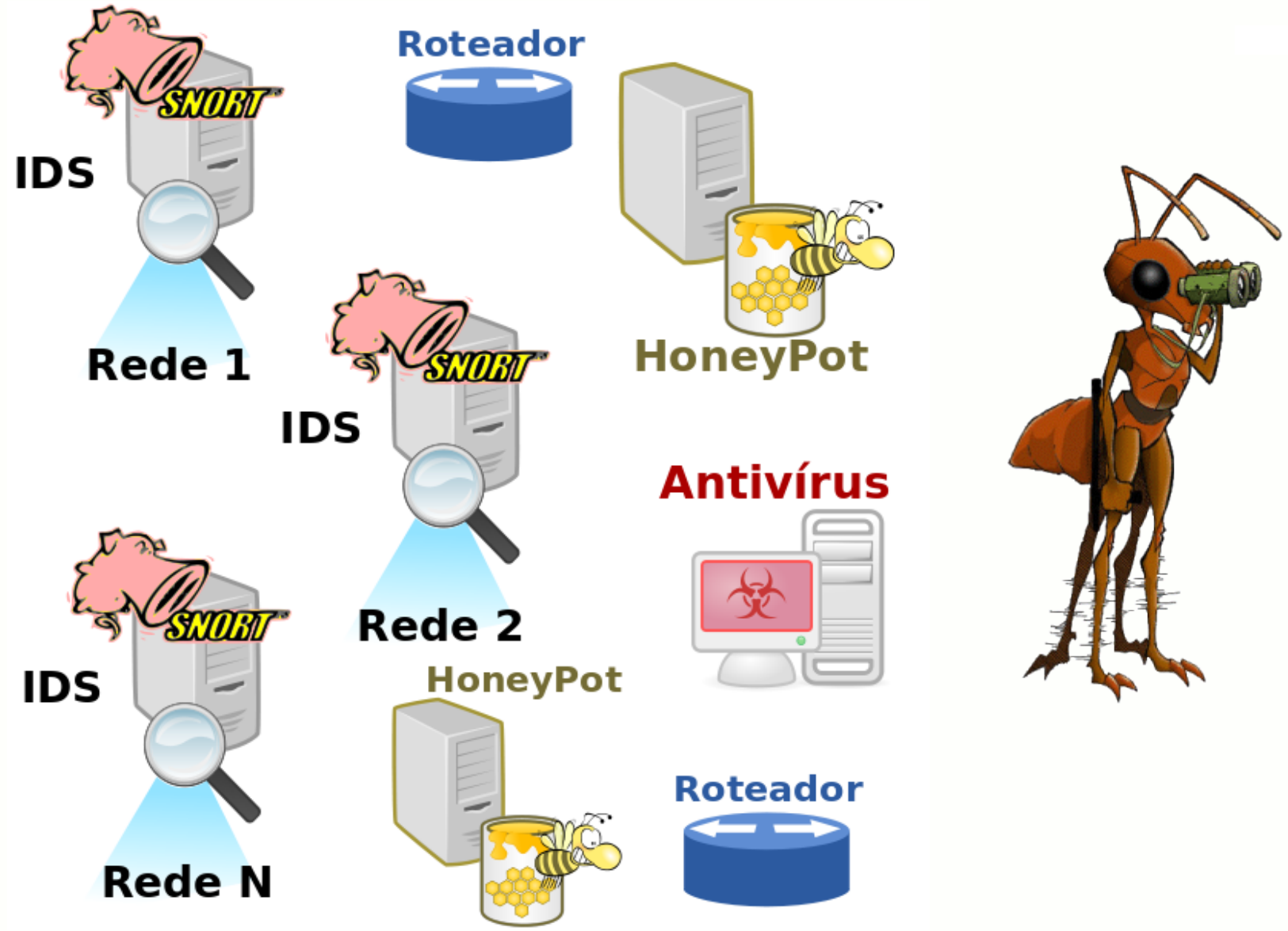
Segurança e Gerência de Eventos



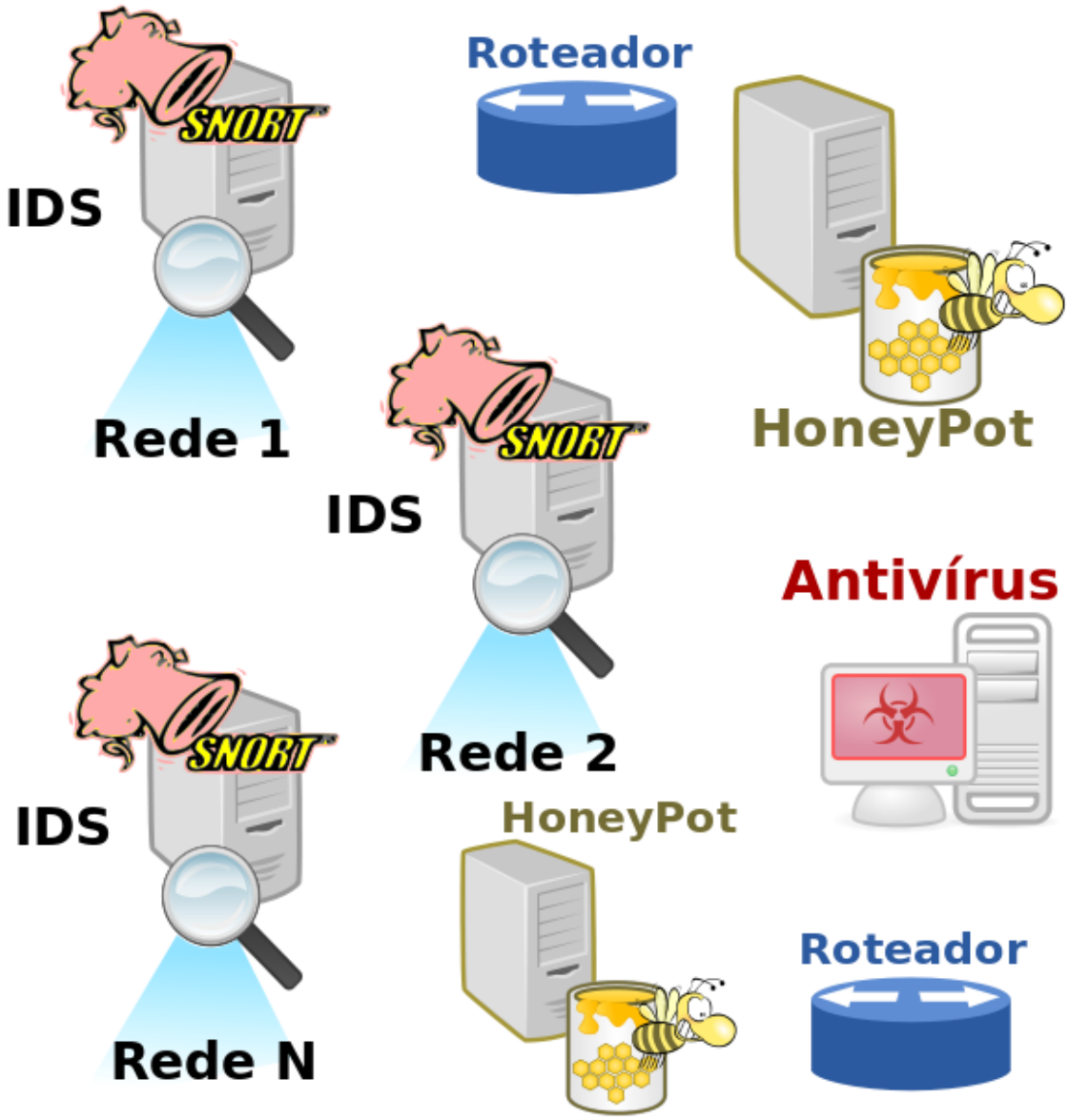
Segurança e Gerência de Eventos



Segurança e Gerência de Eventos



Segurança e Gerência de Eventos



Ataque!

2x Alerta X
1x Alerta Y

Vírus!

2x Alerta K
2x Alerta L

Soluções da Equipe de Segurança

CELEPAR
INFORMÁTICA
do PARANÁ

Atualizado constantemente.

Total de MACs:**0** - Total de IPs:**1** - Total de DHCPs: **5**

IP DUPLICADO - Alertas: 2

Última coleta: 2009-10-20 14:10:23

IP: 10.[illegible].55

MAC: [illegible]:9E:C2:40

MAC: 00:22:15:[illegible]

DHCP/IP NAO CADASTRADO - Alertas: 18

Última coleta: 2009-10-20 15:10:24

IP: 10.[illegible]227

MAC: [illegible]:9E:C2:40

DHCP/IP NAO CADASTRADO - Alertas: 18

Última coleta: 2009-10-20 15:10:22

IP: 10.[illegible]151

Soluções da Equipe de Segurança

- Pcap / TCPDump
- TCP / IP
- Espelhamento
  - Firewall, Proxy

```
perl tamanduah.pl -i eth0 -s 10.0.0.0/8 -d "^10.0.0.0/8,:53" -p udp -q 10

--Tamanduah--2.2-------------------------------------------------------------------------------
     Hosts              Bytes IN                    Bytes OUT                   Bytes Total
-------------------------------------------------------------------------------------------------
1    10.X.X.X           245934          44.54%      82497           41.26%      328431          43.67%
2    10.X.X.X           162296          29.39%      67269           33.64%      229565          30.52%
3    10.X.X.X           130920          23.71%      39905           19.96%      170825          22.71%
4    10.X.X.X           3663            0.66%       818             0.41%       4481            0.60%
5    10.X.X.X           3860            0.70%       518             0.26%       4378            0.58%
6    10.X.X.X           602             0.11%       887             0.44%       1489            0.20%
```

CELEPAR INFORMÁTICA do PARANÁ

ARAPONGAH
alertas de segurança

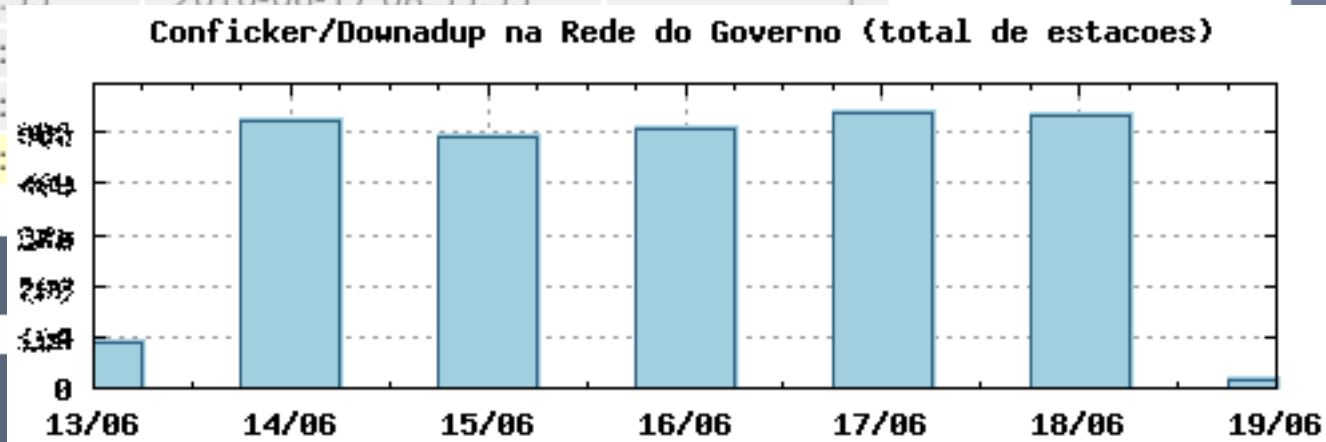
Relatório de estações infectadas pelo vírus Downadup/Conficker

Médio risco

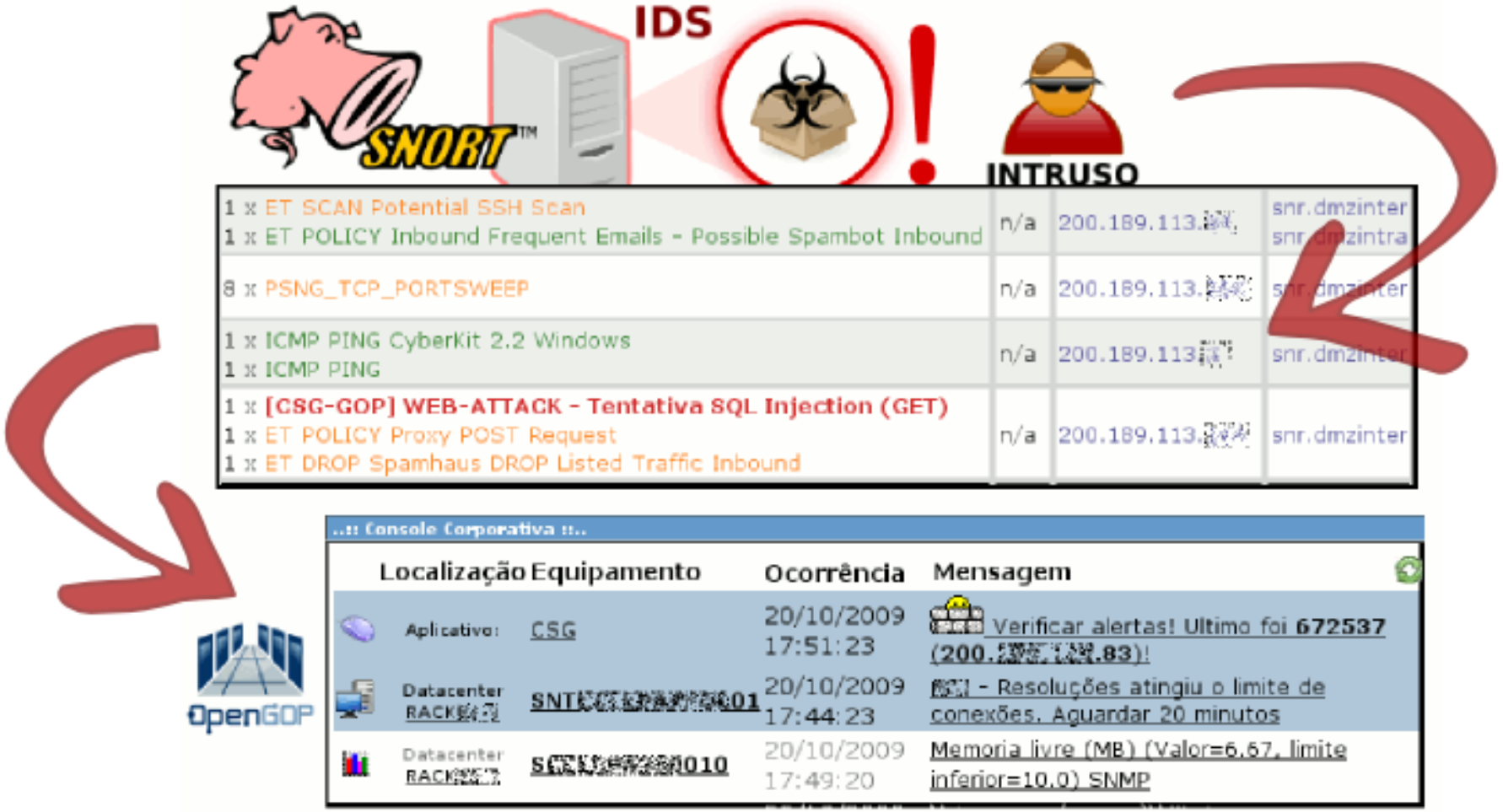
Descrição:	Este tipo de alerta ocorre quando uma estação infectada pelo vírus Conficker e tenta se comunicar com o seu invasor via Internet. A maior parte destas comunicações são barradas pelo firewall. Estações infectadas pelo Conficker são problemáticas pois estão vulneráveis à varredura de variantes e versões recentes do próprio Conficker.
Coleta:	Últimas 48 horas

Total de elementos: [illegible] - Total de alertas: [illegible] Última atualização: [illegible]

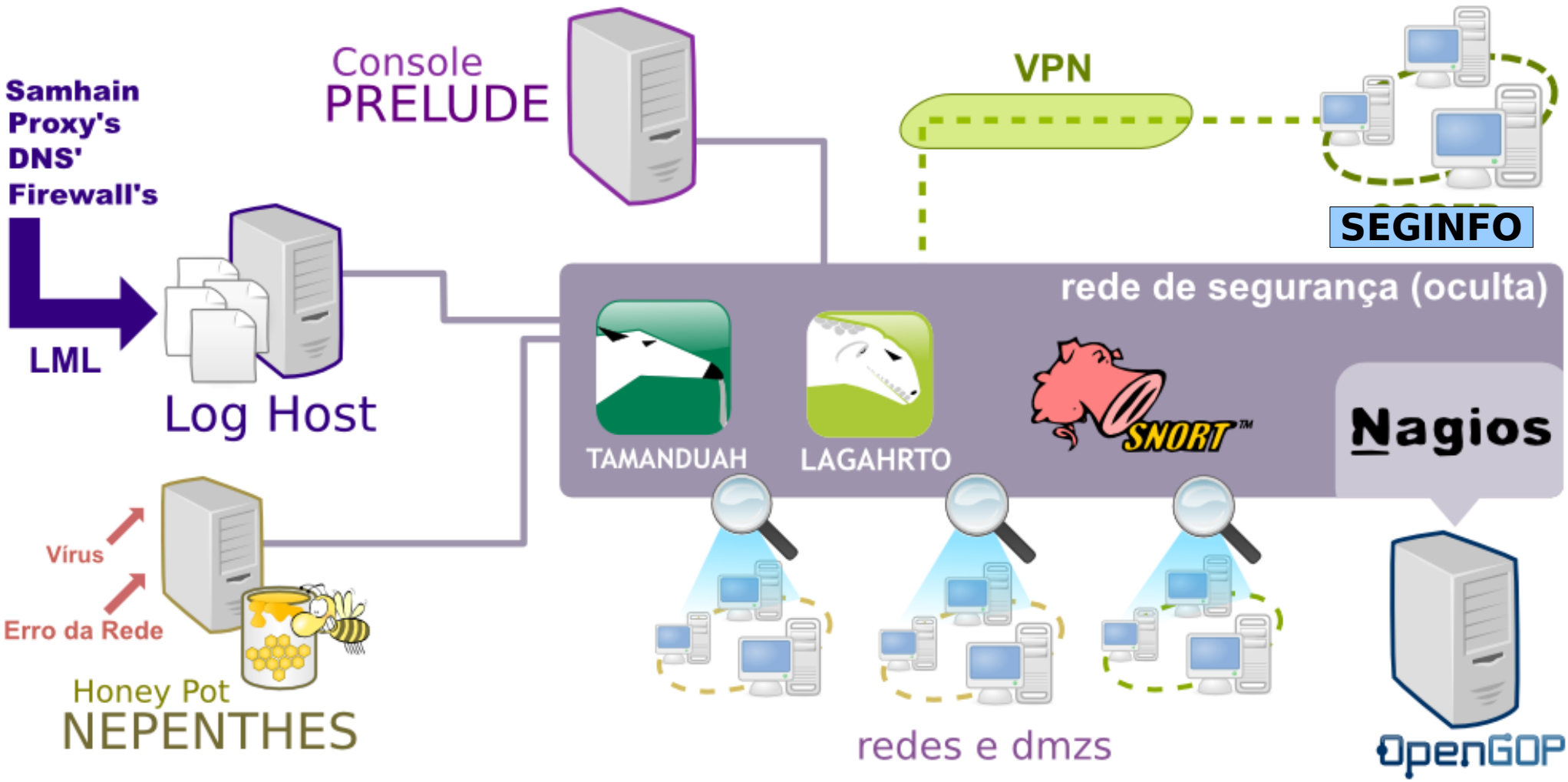
Estação	Primeiro alerta	Último alerta	Qtde
10.[illegible]	2010-06-17 09:36:59	2010-06-18 10:05:40	2
10.[illegible]	2010-06-17 10:24:14	2010-06-18 10:56:05	3
10.[illegible]	2010-06-17 14:34:43	2010-06-18 14:24:47	2
10.[illegible]	2010-06-17 15:00:37	2010-06-18 20:31:01	3
10.[illegible].155	2010-06-17 07:59:26	2010-06-18 06:32:38	8
10.[illegible].164	**2010-06-17 01:00:50**	**2010-06-18 22:47:03**	**16**
10.[illegible].218	2010-06-17 12:12:41	2010-06-17 12:12:41	1
10.[illegible].226	2010-06-17 08:33:33	2010-06-17 08:33:33	1
10.[illegible]16	2010-06-17 08:50:		
10.[illegible].17	2010-06-17 08:25:		
10.[illegible]27	2010-06-17 08:09:		



Soluções da Equipe de Segurança



Soluções da Equipe de Segurança



Algumas Estatísticas

CELEPAR
INFORMÁTICA
do PARANÁ

Algumas Estatísticas

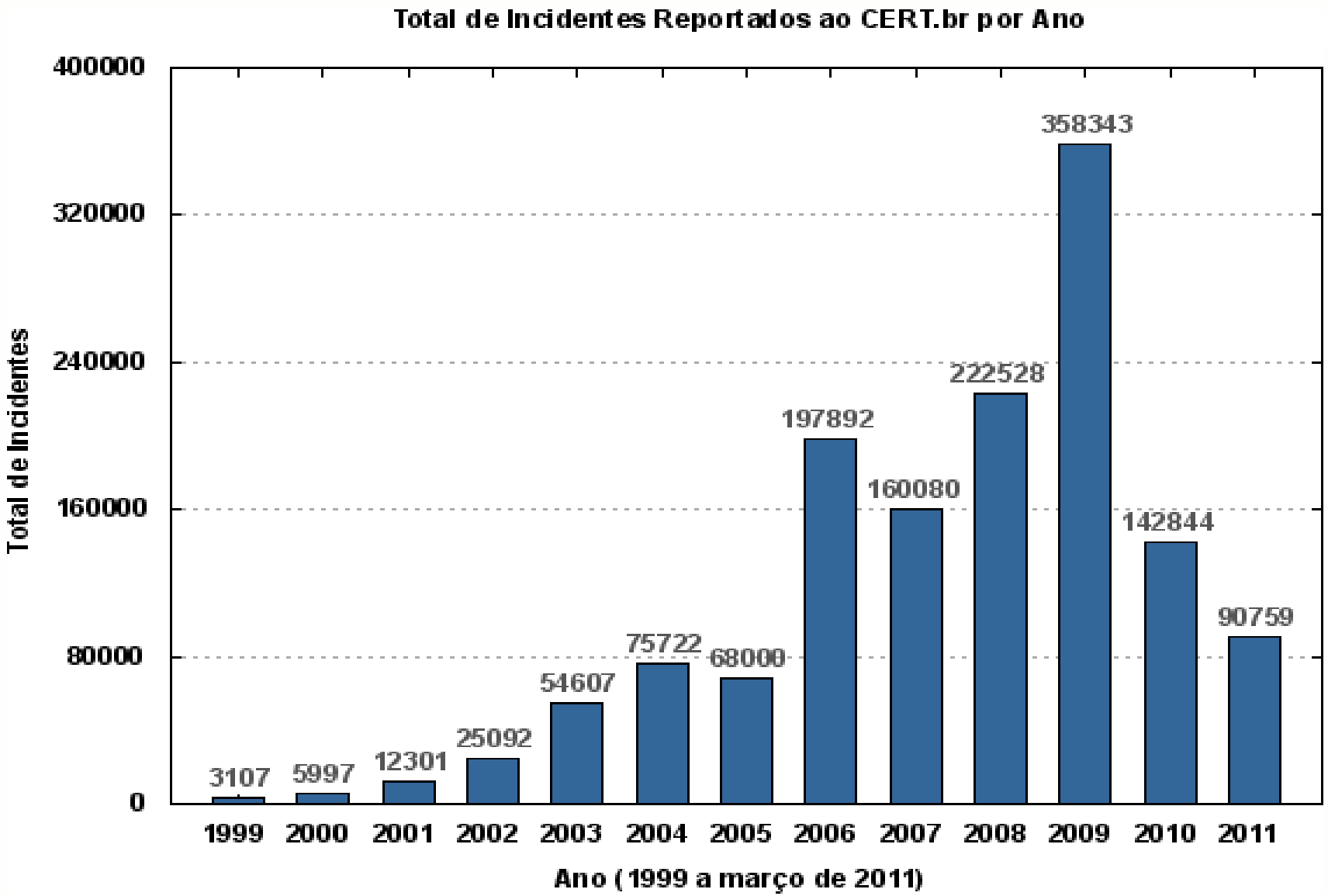
Principais incidentes (2007 → 2008)

- Malwares
- Mau uso de recursos
- Erros de configuração

Principais incidentes (2008 → 2011)

- Malwares
- Tentativas de invasão
- Identificação de vulnerabilidades

Algumas Estatísticas



Projetos em Andamento

Produto

- IPS (*Intrusion Prevention System)*
- SSL Appliance

Desenvolvimento

- IDS baseado em Anomalia (HTTP)

Considerações Finais

- Software Proprietário vs Software Livre

- Eventos correlacionados

- Relatórios personalizados e notificações

- Rápida resposta aos Incidentes

- Dificuldade na Inspeção de Dados Criptografados

- Dificuldade no tratamento de Falsos Positivos e Falsos Negativos

...

Referências

- www.cert.br
- www.emergingthreats.net
- www.ietf.org/rfc/rfc4766.txt
- www.prelude-ids.org
- www.snort.org

OBRIGADO!

Perguntas?

seginfo@celepar.pr.gov.br
hermanopereira@celepar.pr.gov.br

Produzido com:

debian GNOME OpenOffice.org INKSCAPE GIMP