SEGURANÇA & Software Livre

na Rede do Governo do Estado do Paraná

Hermano Pereira

hermanopereira@celepar.pr.gov.br

outubro de 2009

LATINOWARE 2009

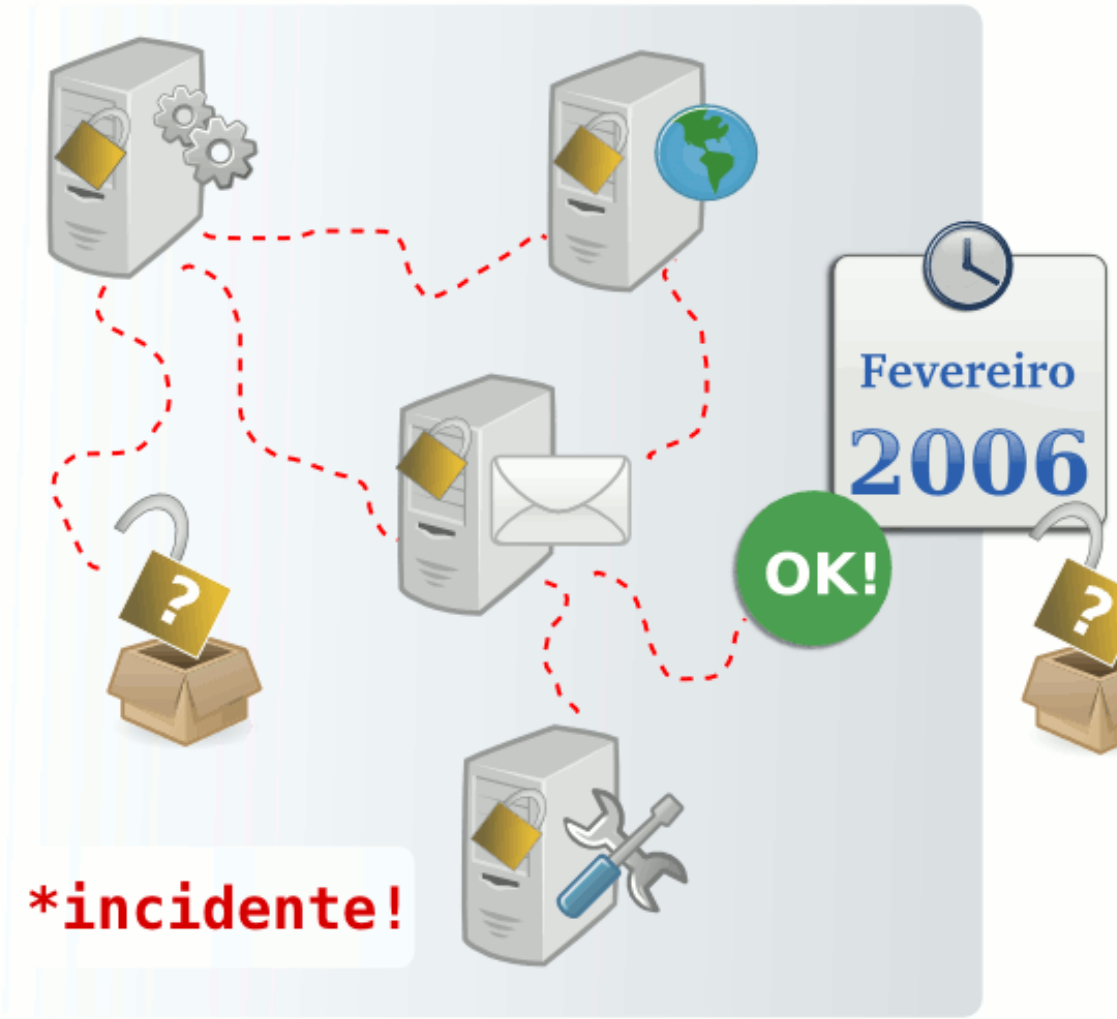
CELEPAR INFORMÁTICA do PARANÁ

Agenda

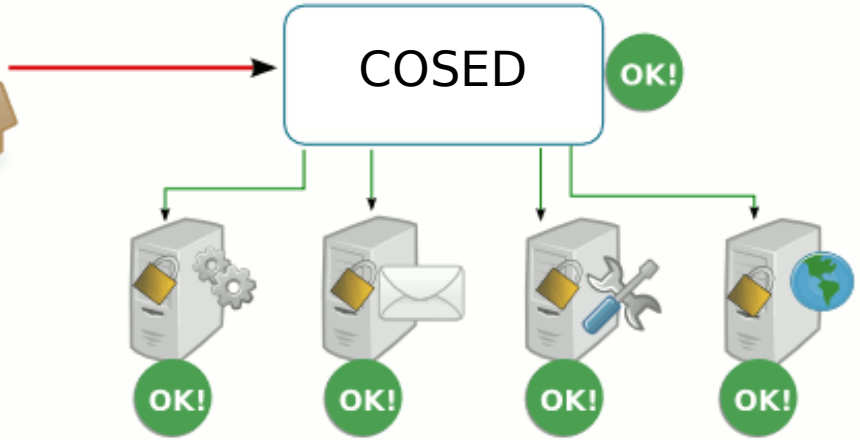
- COSED
- Conceitos de Segurança em TI
- Software Livre
- Implementações da COSED

COSED

Coordenação de Segurança Digital



- Gestão da Segurança
- Políticas
- Resposta a incidentes



Incidente de Segurança

“ Atividade suspeita que tenha sido ou não concretizada, violando uma política de segurança explícita ou implícita da empresa ”

“Taxonomia”


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

Evolução das Técnicas

1988

- Senhas
- Vulnerabilidades conhecidas

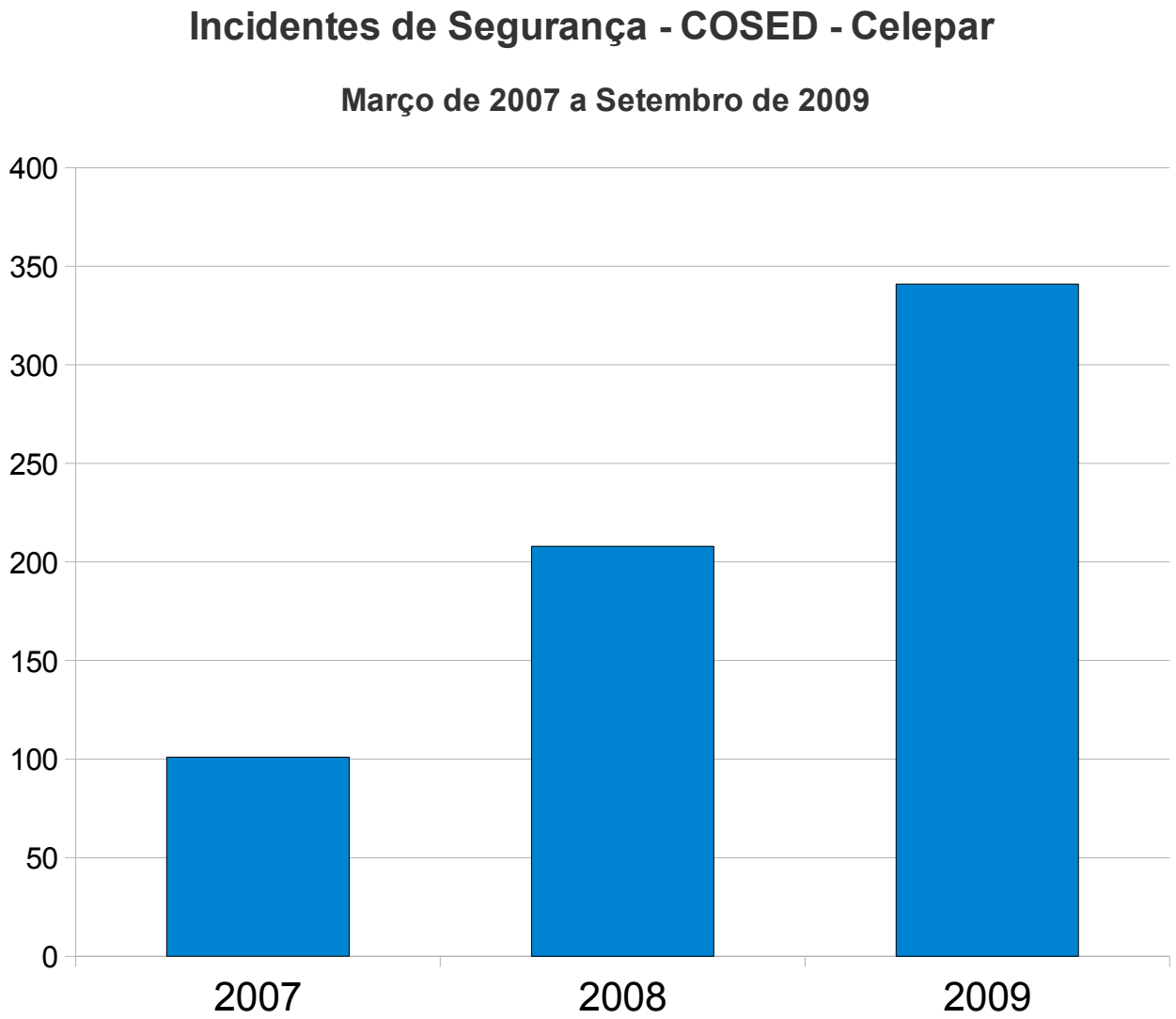
Hoje

- Senhas
- Vulnerabilidades conhecidas
- Falhas de protocolos e falhas no código fonte
- Abuso em servidores web e email
- Instalação de sniffers
- Spoofing no IP de origem
- DDoS
- Scanning automatizado
- Phishing Scam

Estatística: Incidentes Brasil

Incidentes reportados ao cert.br

Estatística: Incidentes COSED



Estatística: Incidentes COSED

Principais incidentes (2007 → 2008)

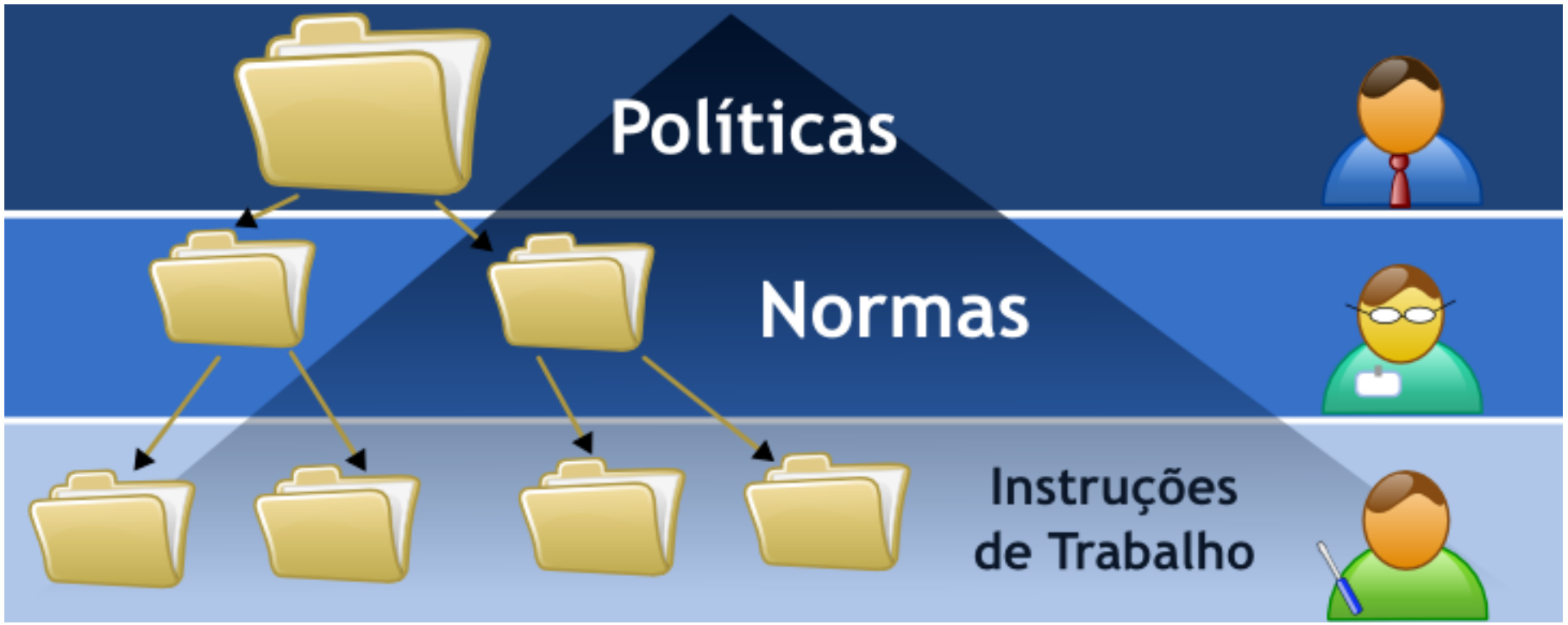
- Malware
- Mau uso de recursos
- Erros de configuração

Principais incidentes (2008 → 2009)

- Malware
- Tentativas de invasão
- Detecção de vulnerabilidades

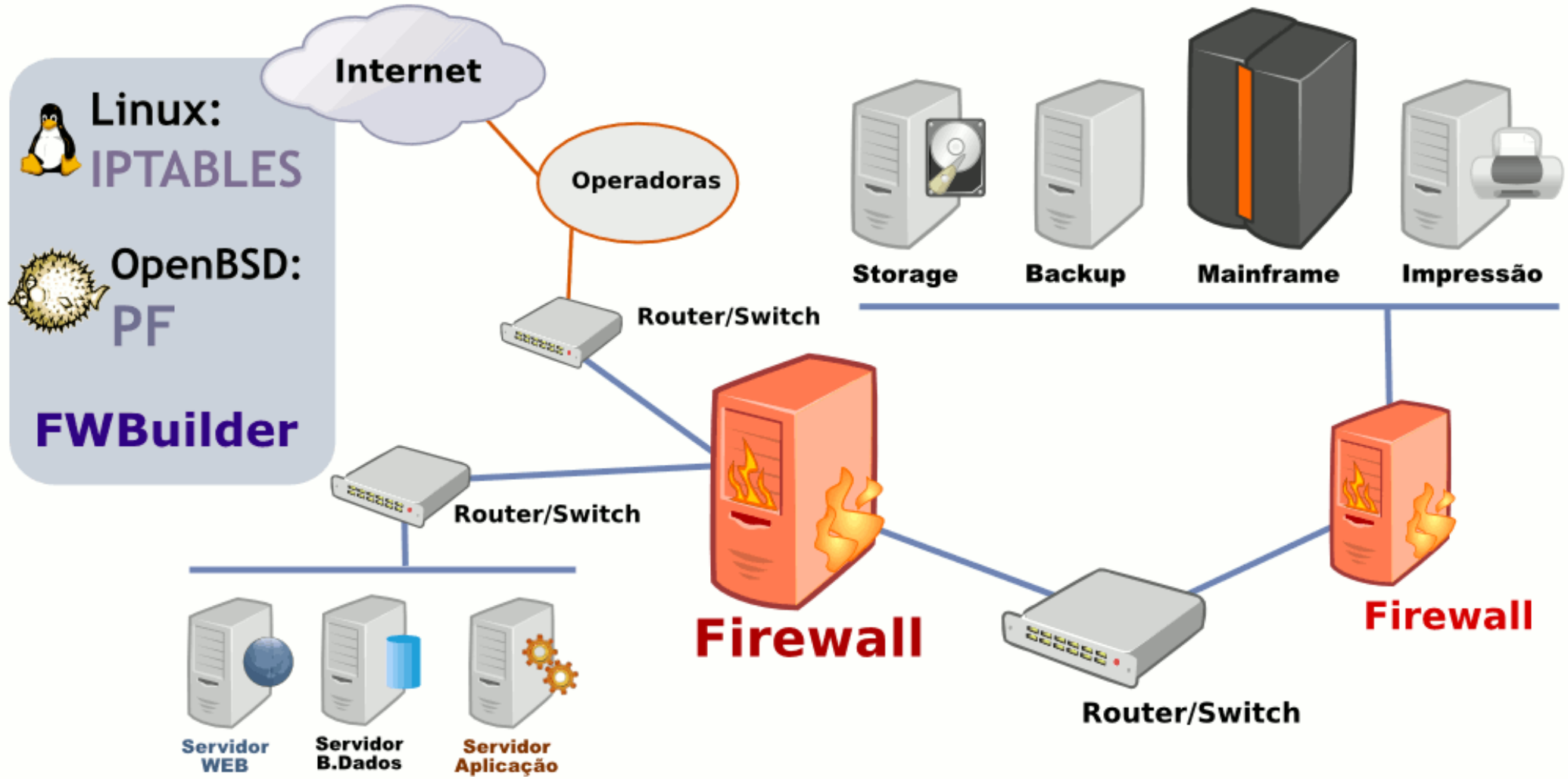
Políticas de Segurança

“ Conjunto de documentos descrevendo os objetivos que as atividades ligadas a Sistemas de Informações na organização devem trabalhar para atingir ”

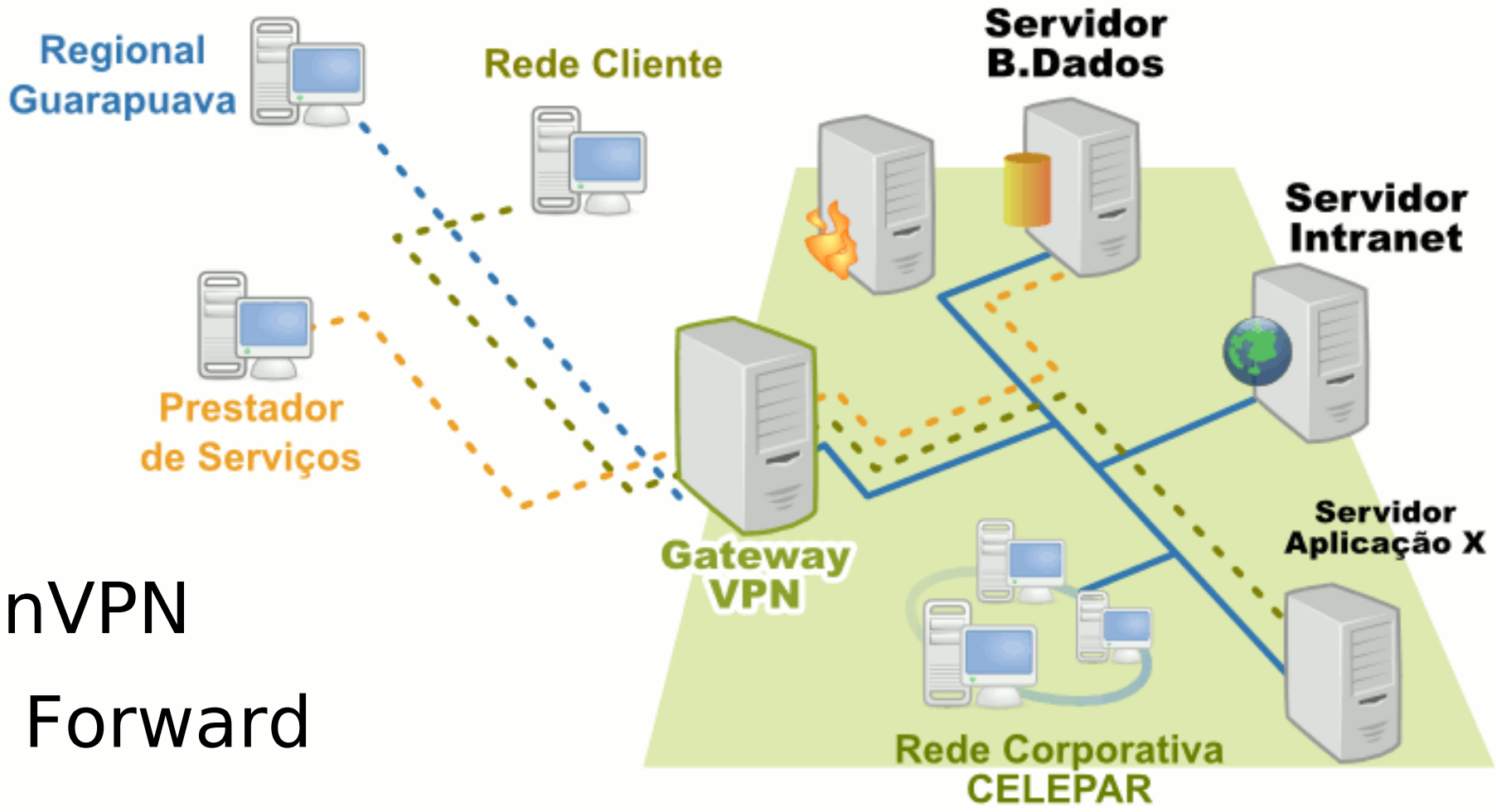


Soluções em Software Livre

Firewall

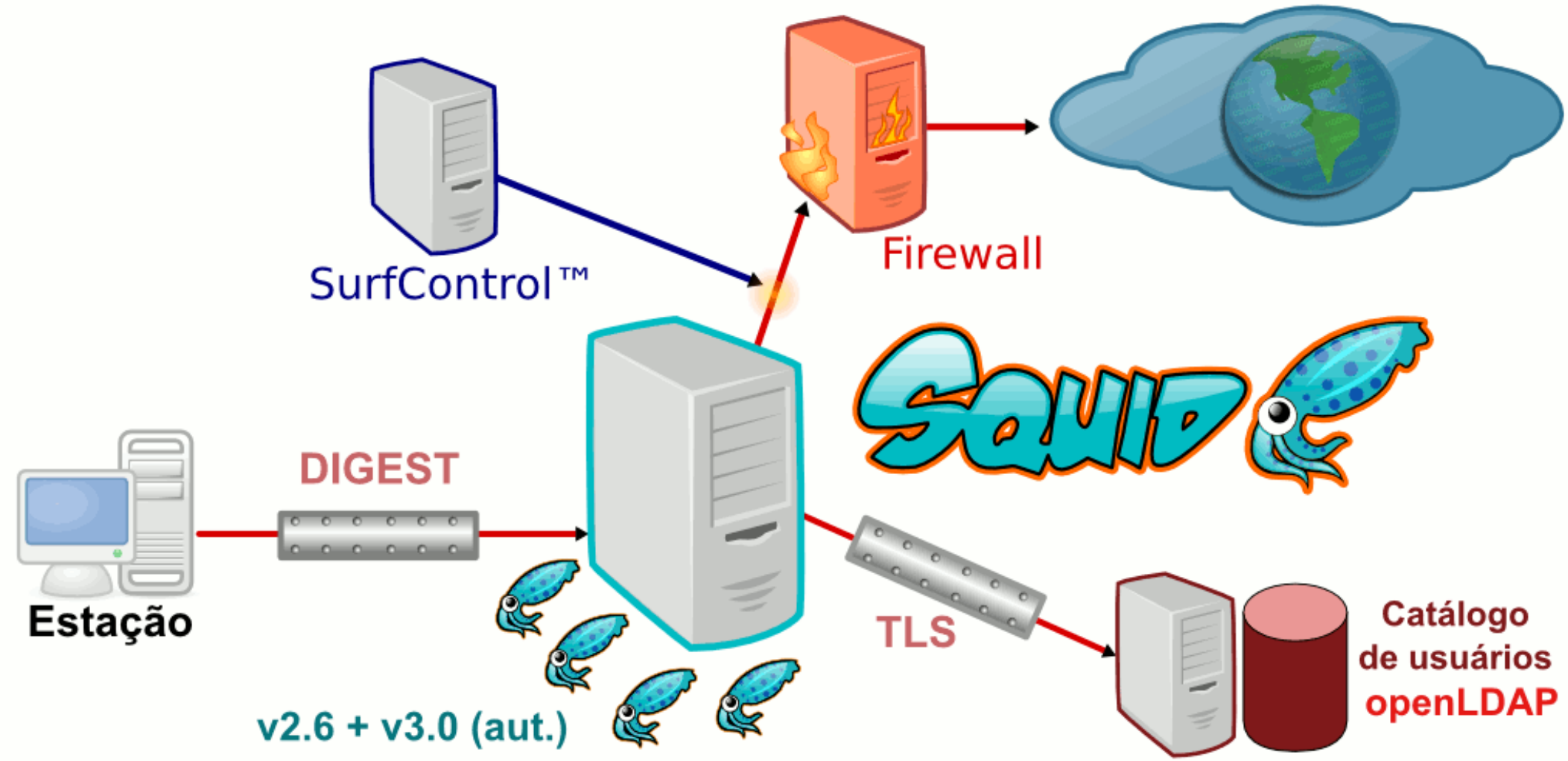

Linux:
IPTABLES
OpenBSD:
PF
FWBuilder
Internet
Operadoras
Router/Switch
Storage
Backup
Mainframe
Impressão
Router/Switch
Firewall
Firewall
Router/Switch
Servidor WEB
Servidor B.Dados
Servidor Aplicação

Virtual Private Network (VPN)



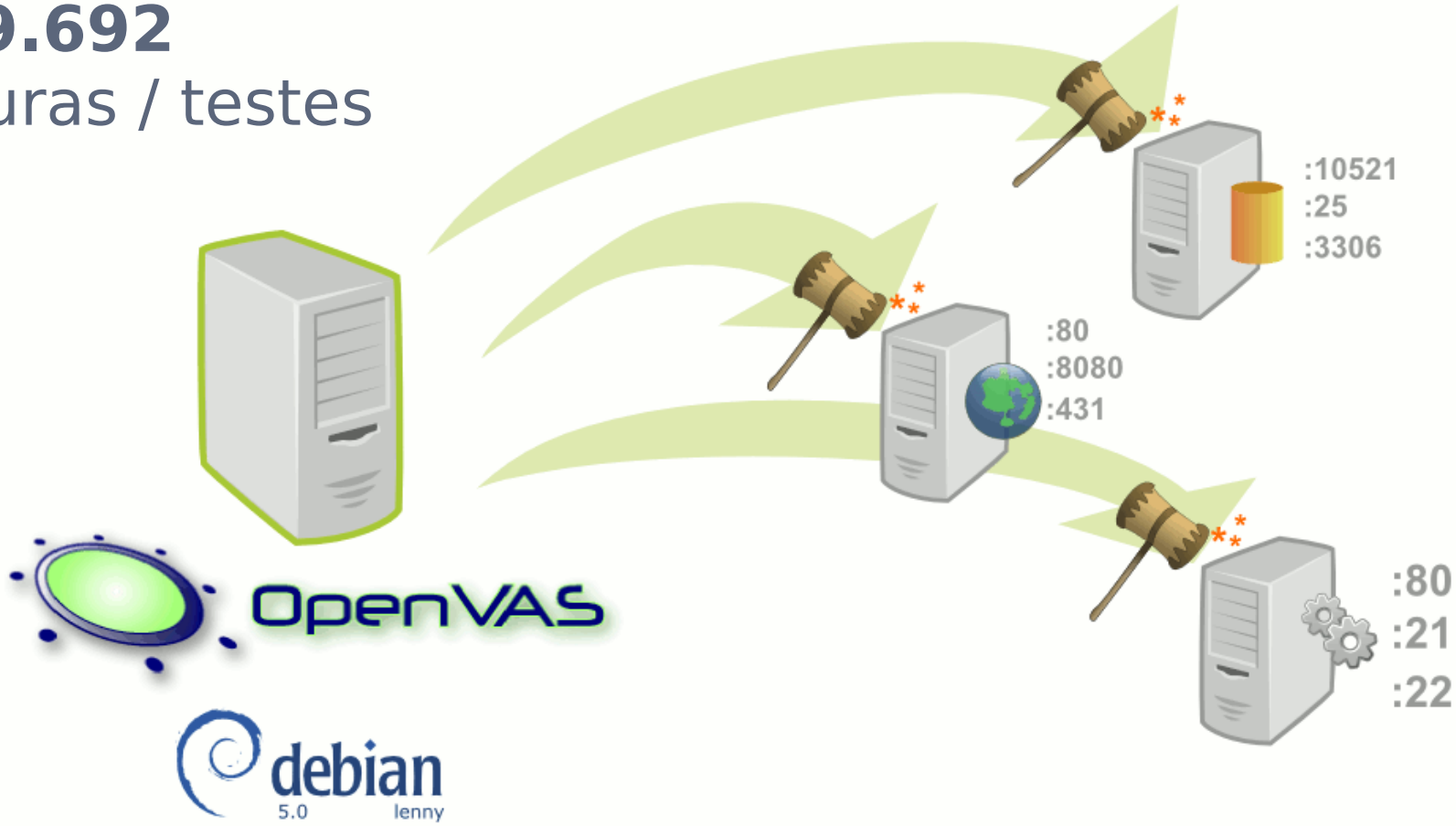
- OpenVPN
- SSH Forward

Web Proxy

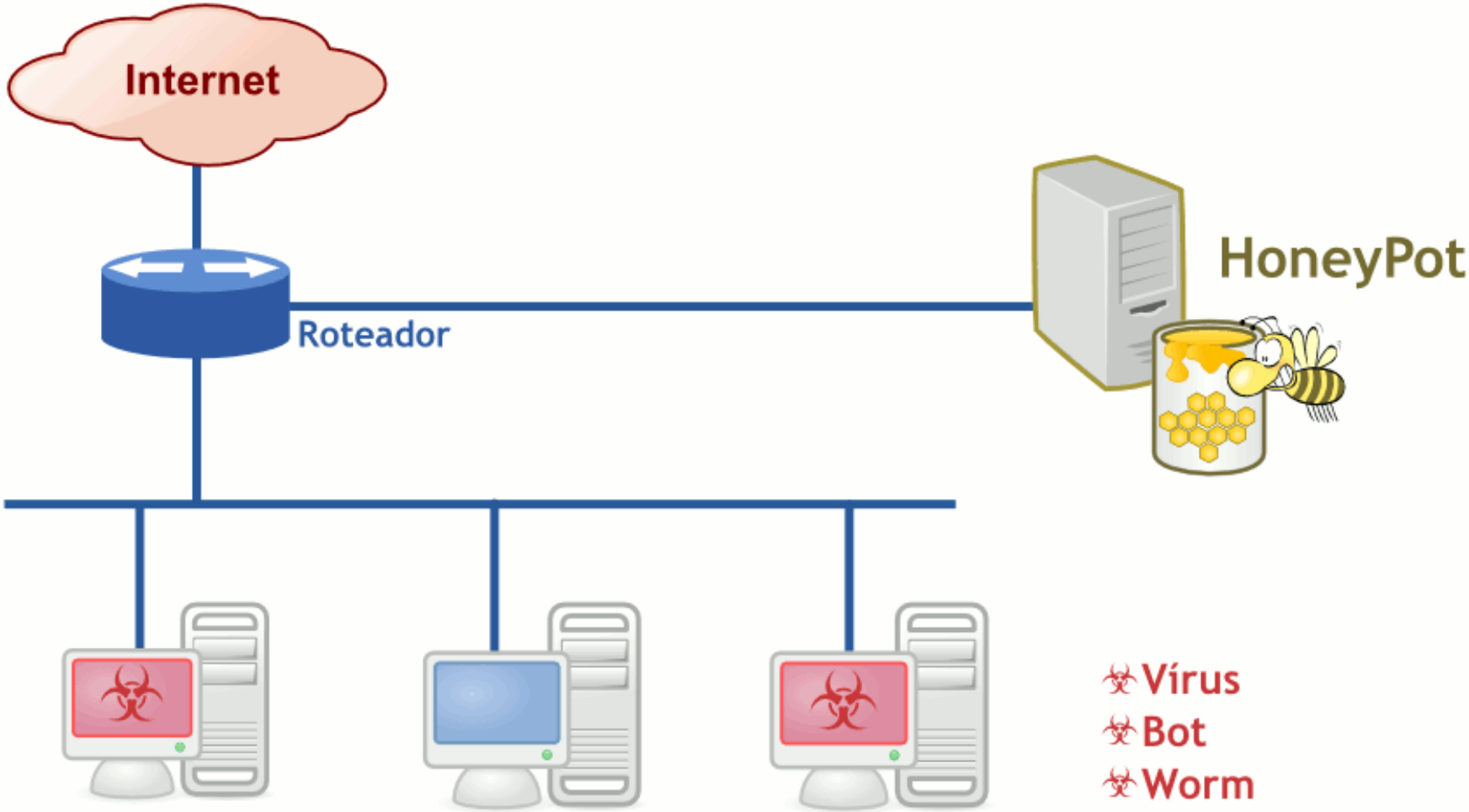

SurfControl™
Firewall
DIGEST
Estação
TLS
Catálogo
de usuários
openLDAP
v2.6 + v3.0 (aut.)

Verificação de Vulnerabilidades

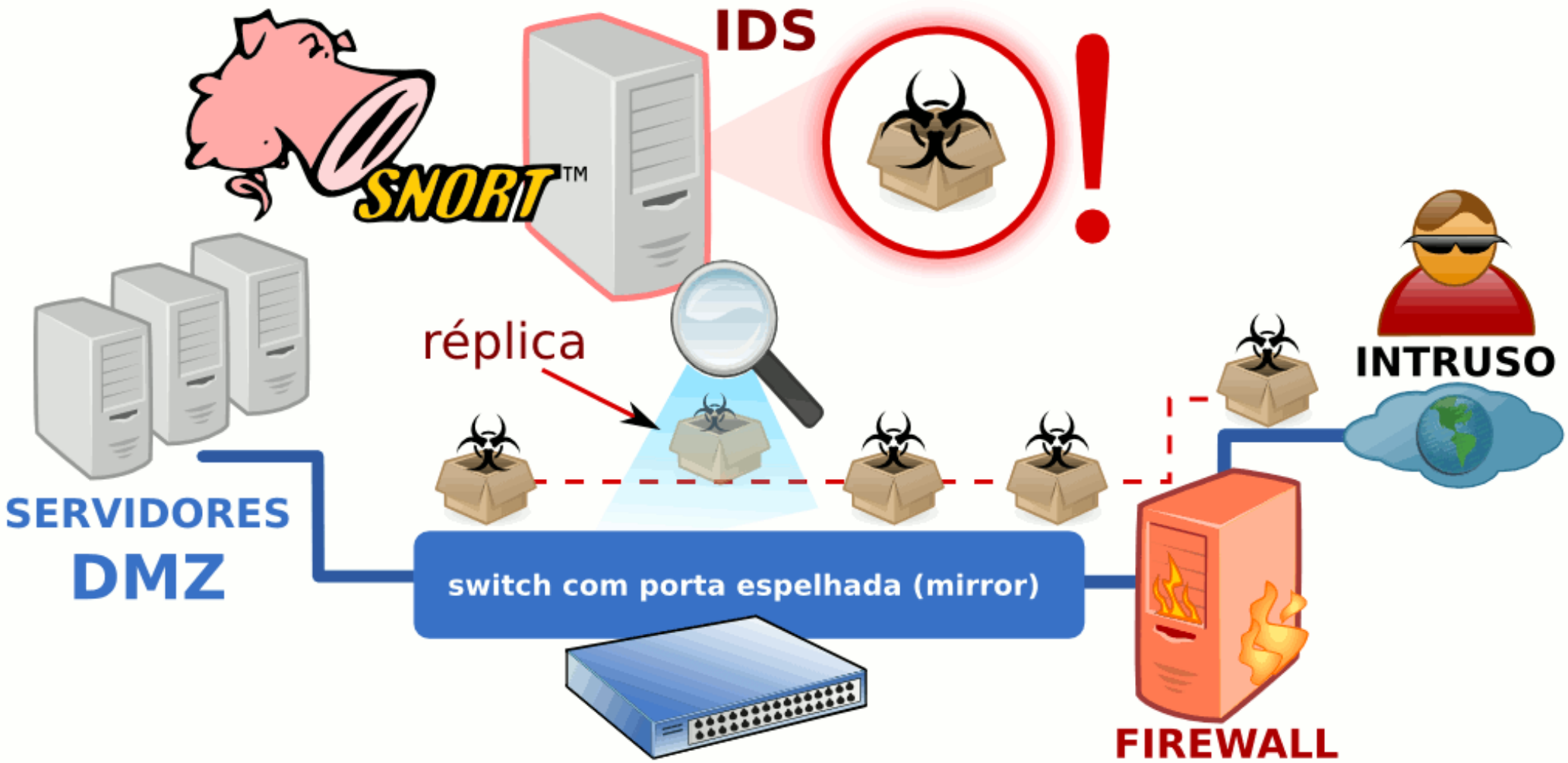
29.692
assinaturas / testes



HoneyPot - Nepenthes



Intrusion Detection System (IDS)



Soluções em Software Livre

Pen Test

- **Metasploit**
- **Scapy**

Autenticação

- **OpenLdap**
- **FreeRadius**

Coleta de Pacotes

- **Wireshark**

Sessão Segura

- **OpenSSH**
- **SCP**

Inventário de Hardware/Software

- **OCS Inventory**

Sistema Operacional

- **BackTrack**

Soluções implementadas pela COSED

Implementações COSED

- Apoio
- Monitoração
- Automatizar processos
- Software Livre
- Foco no ambiente interno

SABUJO: Identificação de usuários

- Organograma
- PHP
- Dados contato
- Últimos acessos
- Dados Estação
- Históricos
- Rastreamento

Tamanduah: Consumo de Banda

- 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%
```

CORUJA: Auditoria de Imagens

Driftnet

- Perl + PHP
- Na imagem:
  - IP
  - Upload/Download
  - Tamanho
  - Data/Hora acesso

PSQUILO: Relatórios de Acesso

PSQUILO

Gerador de Relatórios do Squid Proxy em PHP

Opções: Índice | relatório por usuário | relatório por domínio | relatório para múltiplos ips

Conta josejr em 17/04/2009

Usuário: josejr
Data: 17/04/2009
Consumo: 19,9168 MBytes
Tempo de conexão: 3018581 segundos
Endereço(s) IP:

- [redacted]

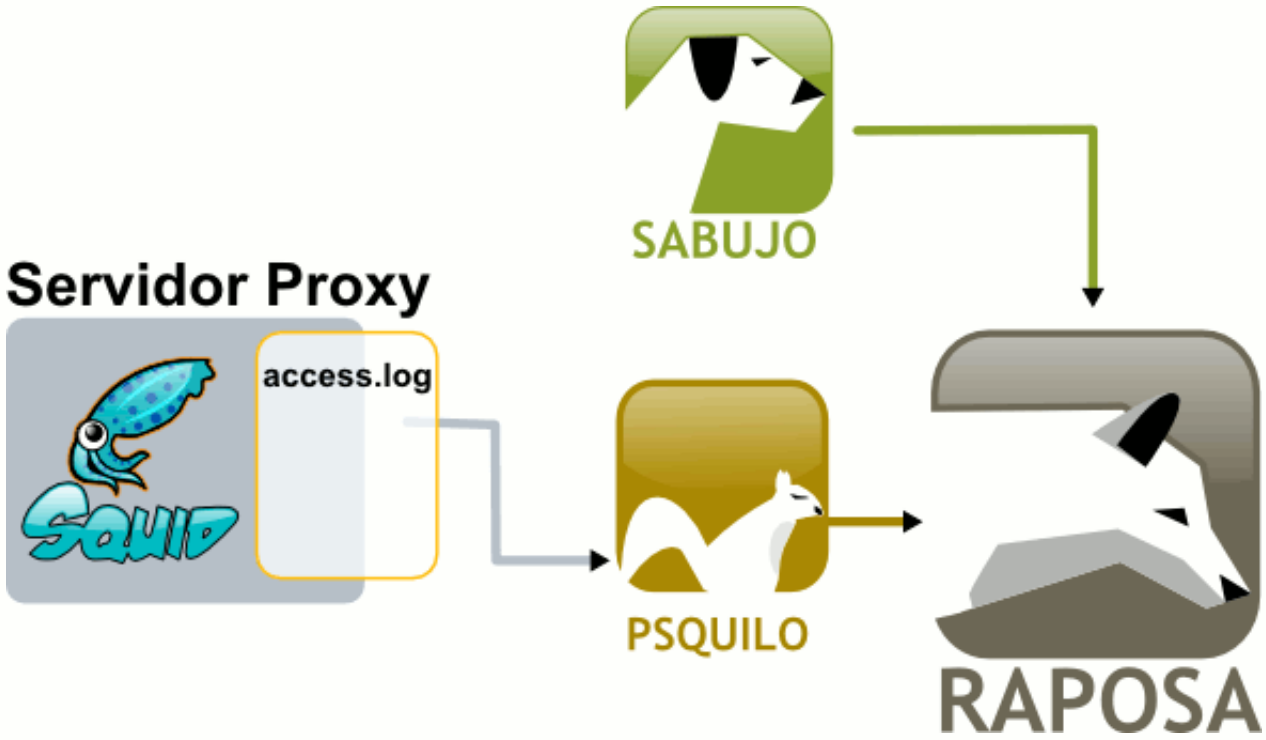
Domínios acessados

Legenda: bloqueio parcial | liberados | negados | requisições

Domínio	Volume	1ª req.	req. final			
extensions.services.openoffice.org	12,9771 MBytes	09:52:37	10:02:39	271	234	37
d.scribd.com	3,3209 MBytes	09:16:22	09:17:10	3	2	1
sun.com	1,0747 MBytes	09:34:57	09:50:45	173	119	54
search.sun.com	447,1895 KBytes	09:50:37	09:50:49	61	48	13
java.sun.com	440,8076 KBytes	09:31:11	09:45:07	65	57	8
ubuntuforums.org	266,4023 KBytes	09:31:54	09:31:58	53	38	15
s.scribd.com	227,7168 KBytes	09:16:15	09:16:23	39	32	7
static.sourceforge.net	186,8770 KBytes	09:56:25	09:56:41	35	29	6
www.paypalobjects.com:443	175,1133 KBytes	11:34:58	11:35:52	20	12	8
www-cdn.sun.com	140,5879 KBytes	09:31:20	10:02:39	32	31	1

- Squid access.log
- PHP
  - Dados em XML
  - Múltiplas Instâncias
  - Dados Relevantes
    - Plugins
    - Múltiplas datas

RAPOSA: Controle da Internet



- Reaproveitamento de informações
- Gestão de norma interna de segurança
  - Notificações
  - Bloqueios

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**

Filtro COSED: Known Bot		
Origem	Qtde.	Primeiro Alerta
10.[redacted].204.21	2	2009-10-15 22:30:50
10.[redacted].126.10	6	2009-10-15 22:31:03
10.[redacted].128.3	2	2009-10-15 22:30:37
10.[redacted].13.40	6	2009-10-15 22:31:02
10.[redacted].146.10	2	2009-10-15 22:30:37
10.[redacted].156.19	1	2009-10-15 22:05:30
10.[redacted].168.2	1	2009-10-15 22:31:59

Relatório de estações com Bot

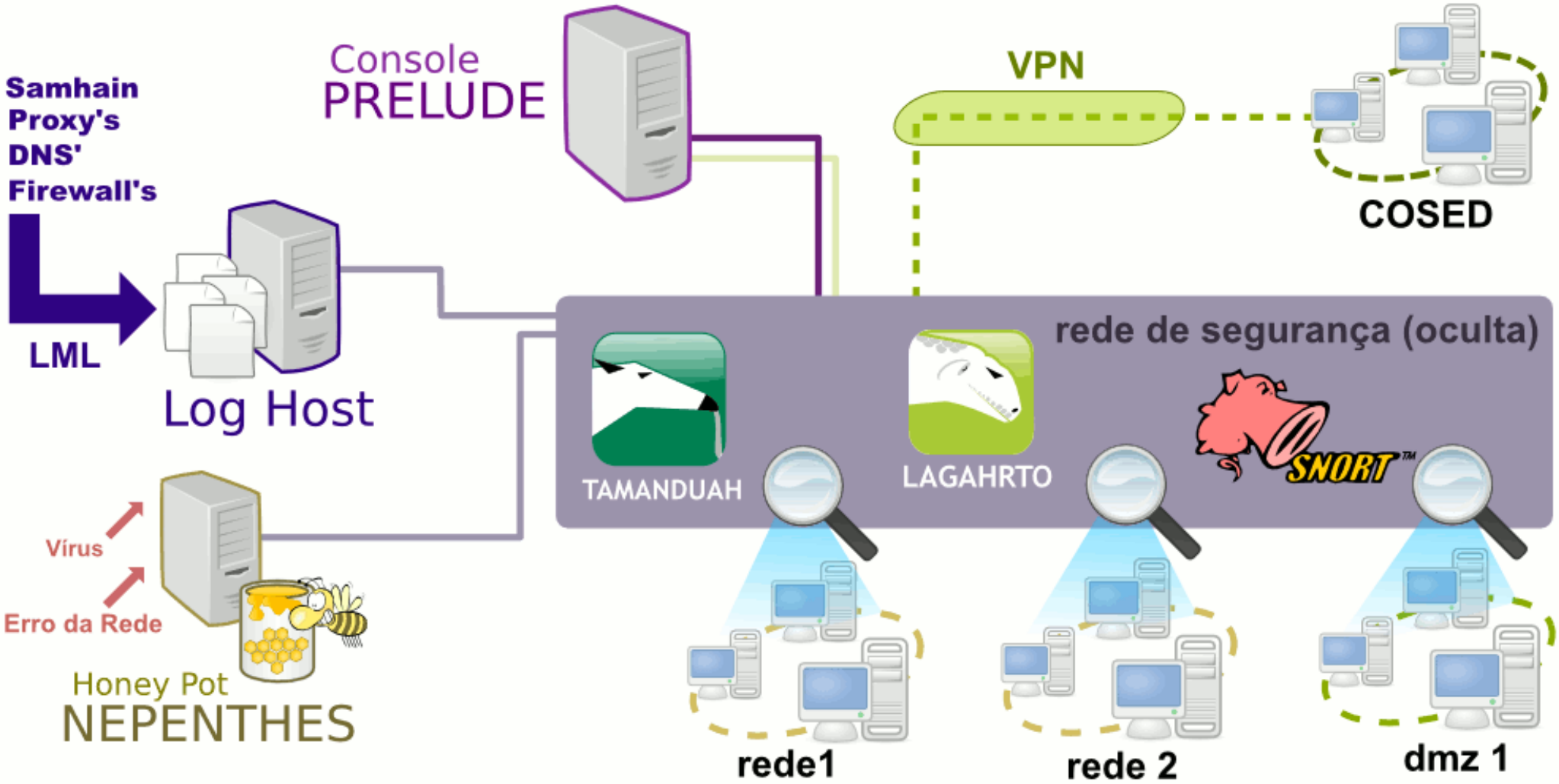
http://alertas.celepar.parana/bot

Médio risco

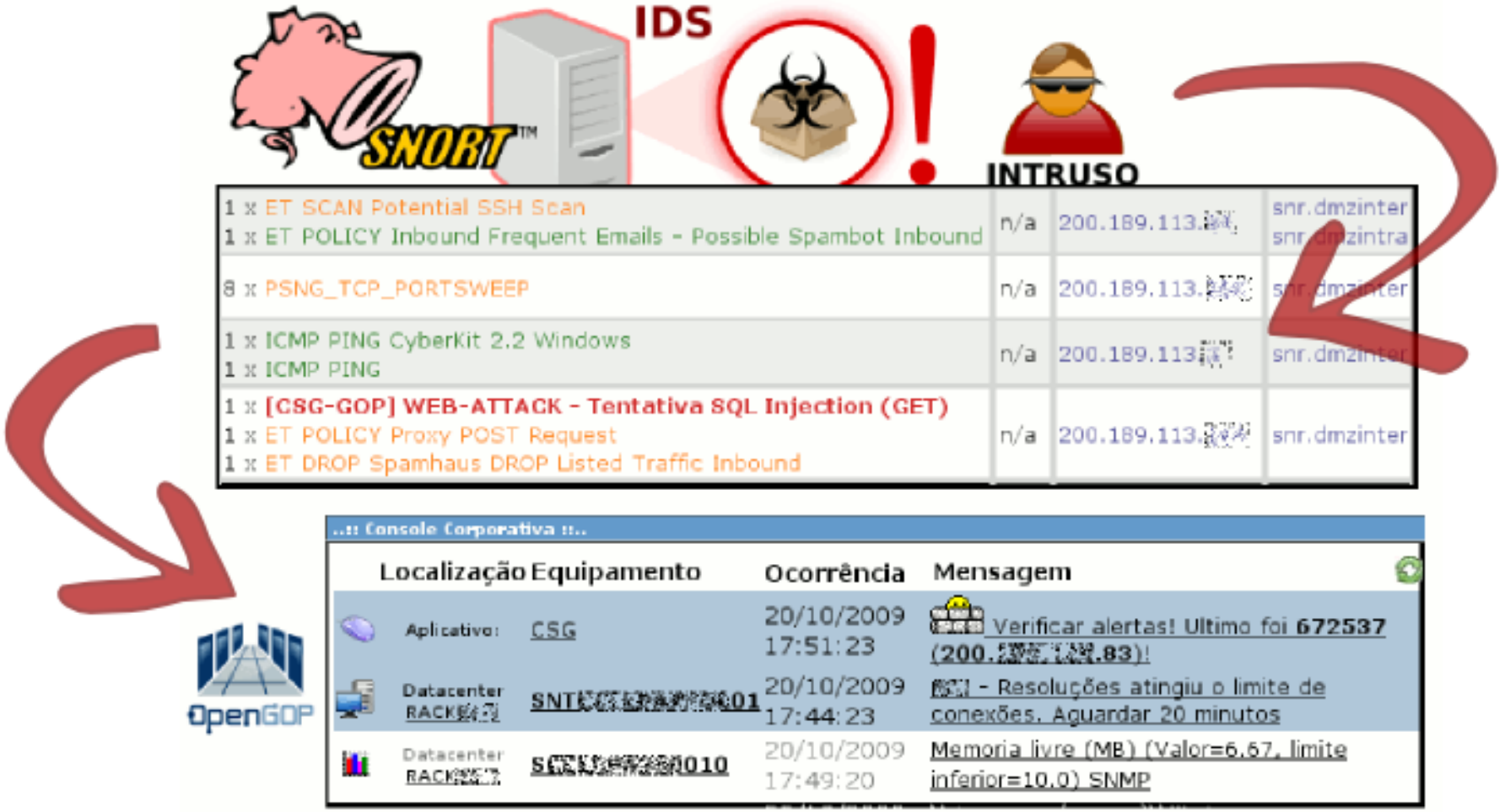
Atualizado a cada 15 minutos e zerado às 03, 07, 11, 15, 19 e 23 horas.

Descrição:
Este tipo de alerta ocorre quando uma estação infectada por algum tipo de bot tenta se comunicar com o seu invasor via Internet. A maior parte destas comunicações são barradas pelo firewall. Estações infectadas por bots podem atuar como qualquer tipo de malware (vírus, worm, trojan

Rede de Segurança



Monitor de Segurança - Prewikka/Prelude



Referências

- http://cert.br
- http://antispam.br
- www.snort.org
- www.openbsd.org
- http://www.ietf.org/rfc/rfc4766.txt

- www.iptables.org
- www.prelude-ids.org
- http://httpd.apache.org/docs/2.0/mod/mod_ssl.html
- www.squid-cache.org
- www.openvas.org
- www.openvpn.org

OBRIGADO!
Perguntas?

Produzido com:

debian

GNOME™

OpenOffice.org

INKSCAPE

GIMP