

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

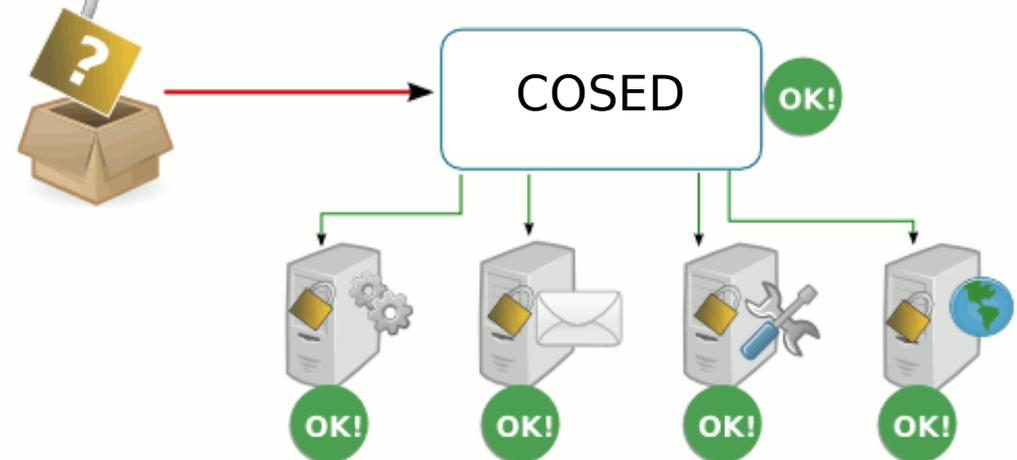
- COSED
- Conceitos de Segurança em TI
- Software Livre
- Implementações da COSED

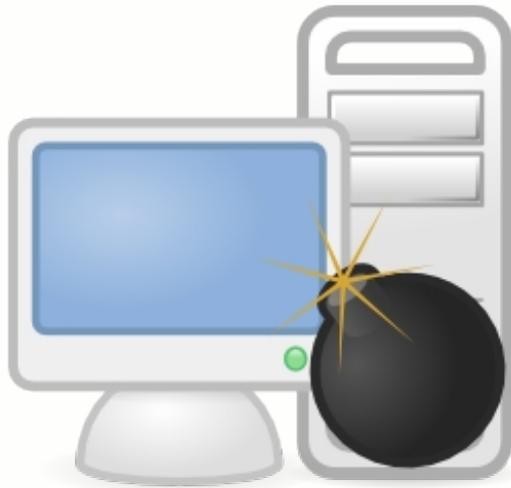
COSED

Coordenação de Segurança Digital



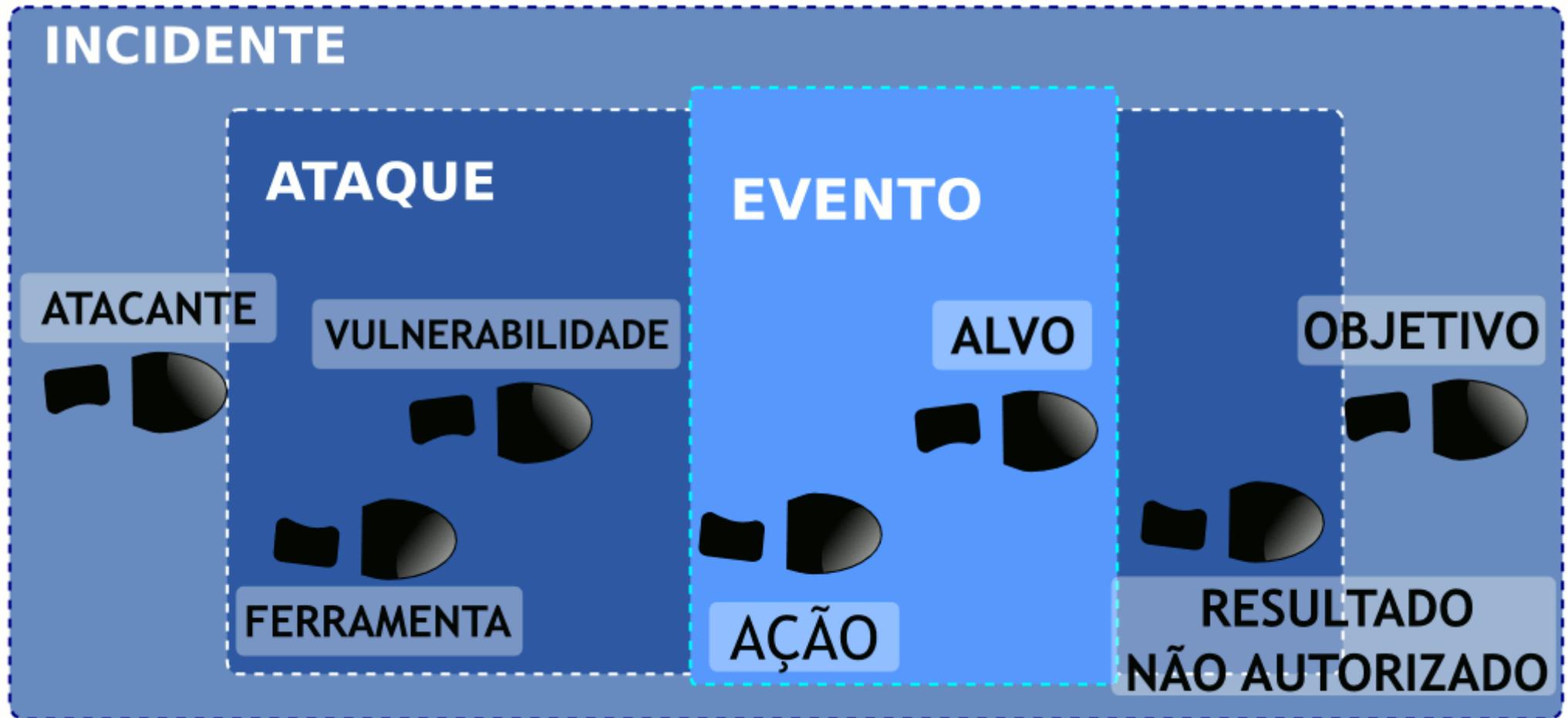
- Gestão da Segurança
- Políticas
- Resposta a incidentes





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

Conceitos de Segurança em TI “Taxonomia”



Conceitos de Segurança em TI

Evolução das Técnicas

1988

- Senhas
- Vulnerabilidades conhecidas

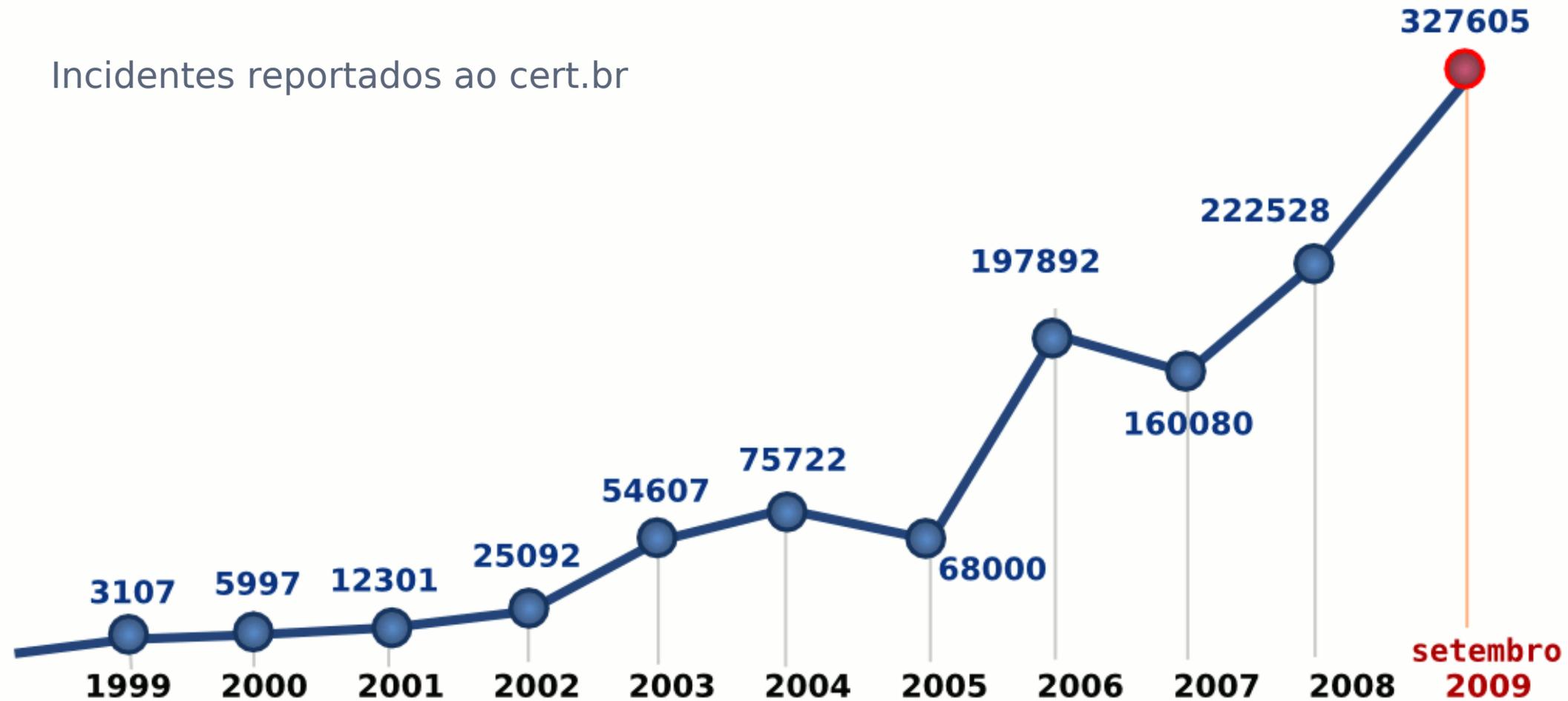
Hoje

- 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

Conceitos de Segurança em TI

Estatística: Incidentes Brasil

Incidentes reportados ao cert.br

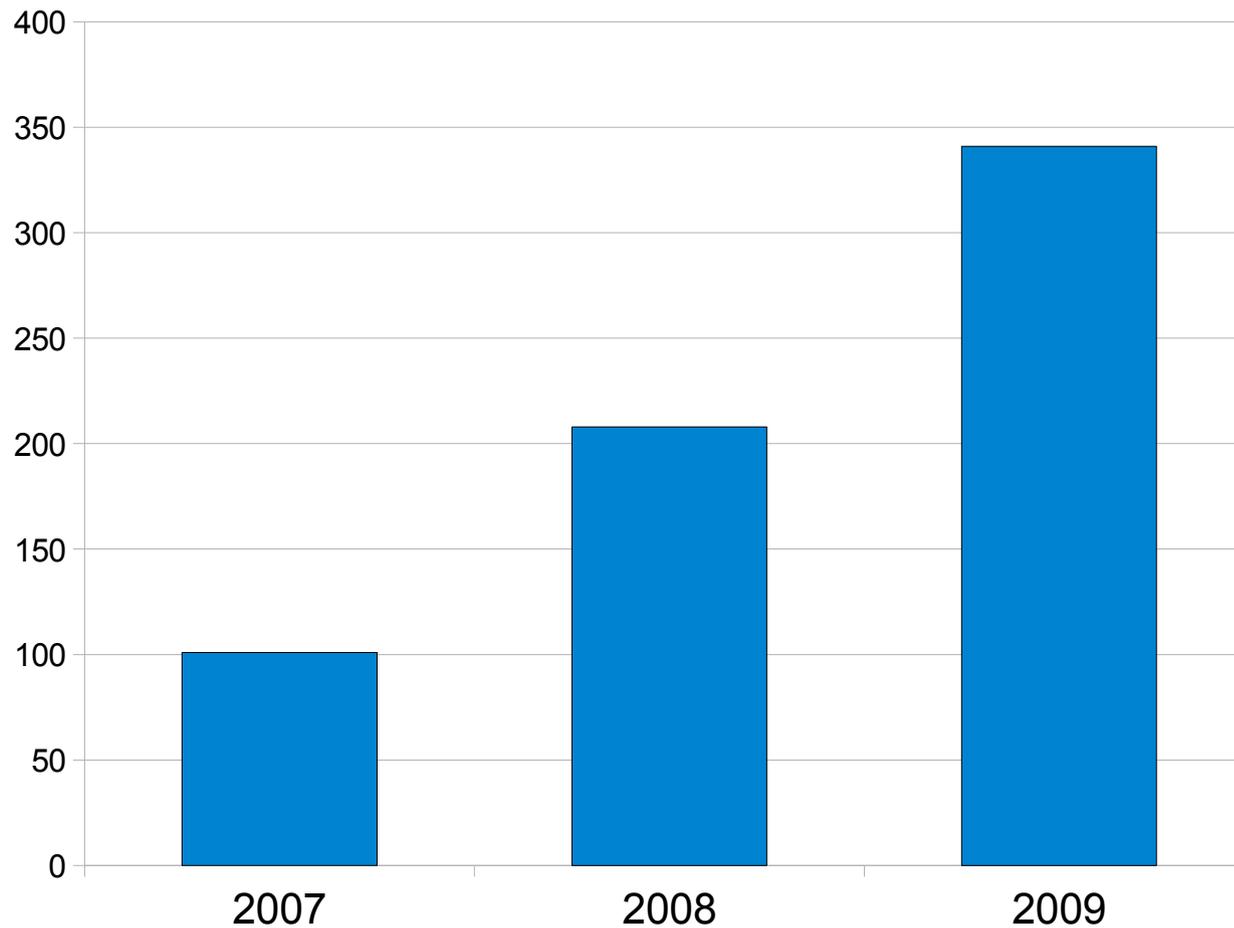


Conceitos de Segurança em TI

Estatística: Incidentes COSED

Incidentes de Segurança - COSED - Celepar

Março de 2007 a Setembro de 2009



Principais incidentes (2007 → 2008)

- Malware
- Mau uso de recursos
- Erros de configuração

Principais incidentes (2008 → 2009)

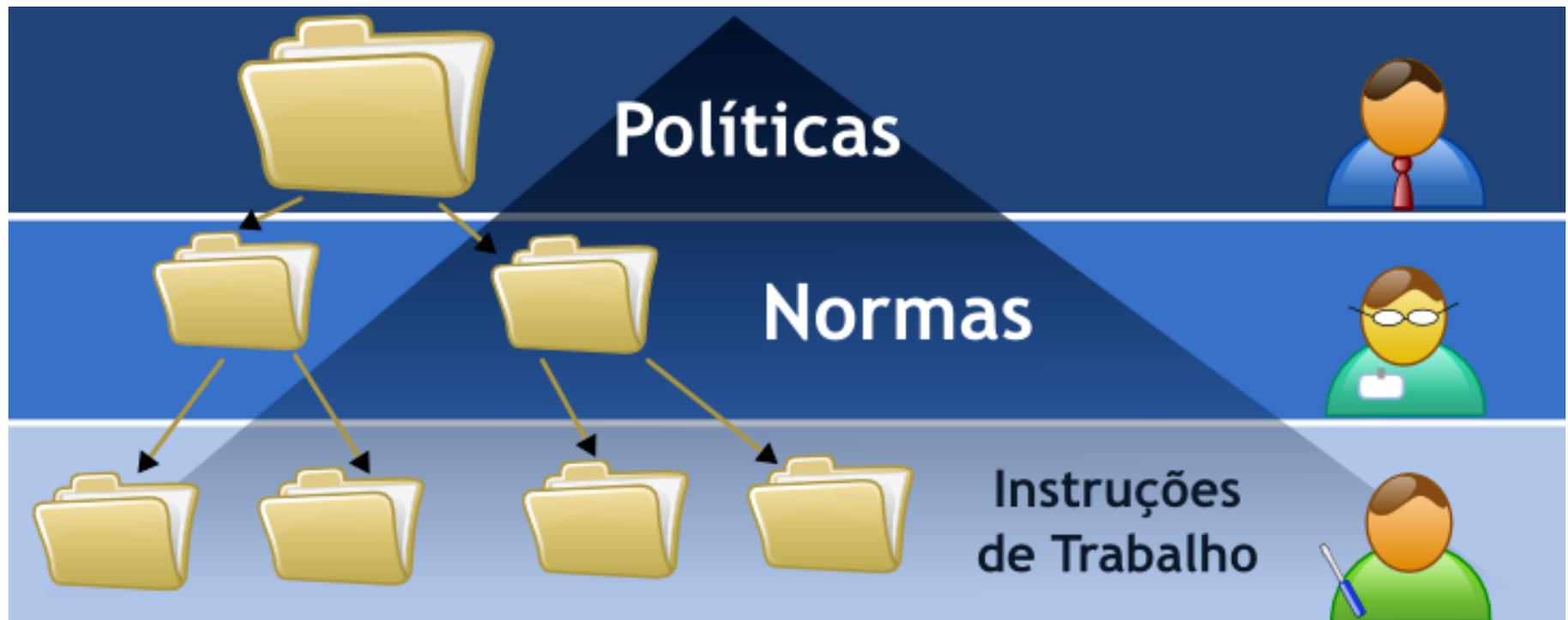
- Malware
- Tentativas de invasão
- Detecção de vulnerabilidades

Conceitos de Segurança em TI

Políticas de Segurança



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

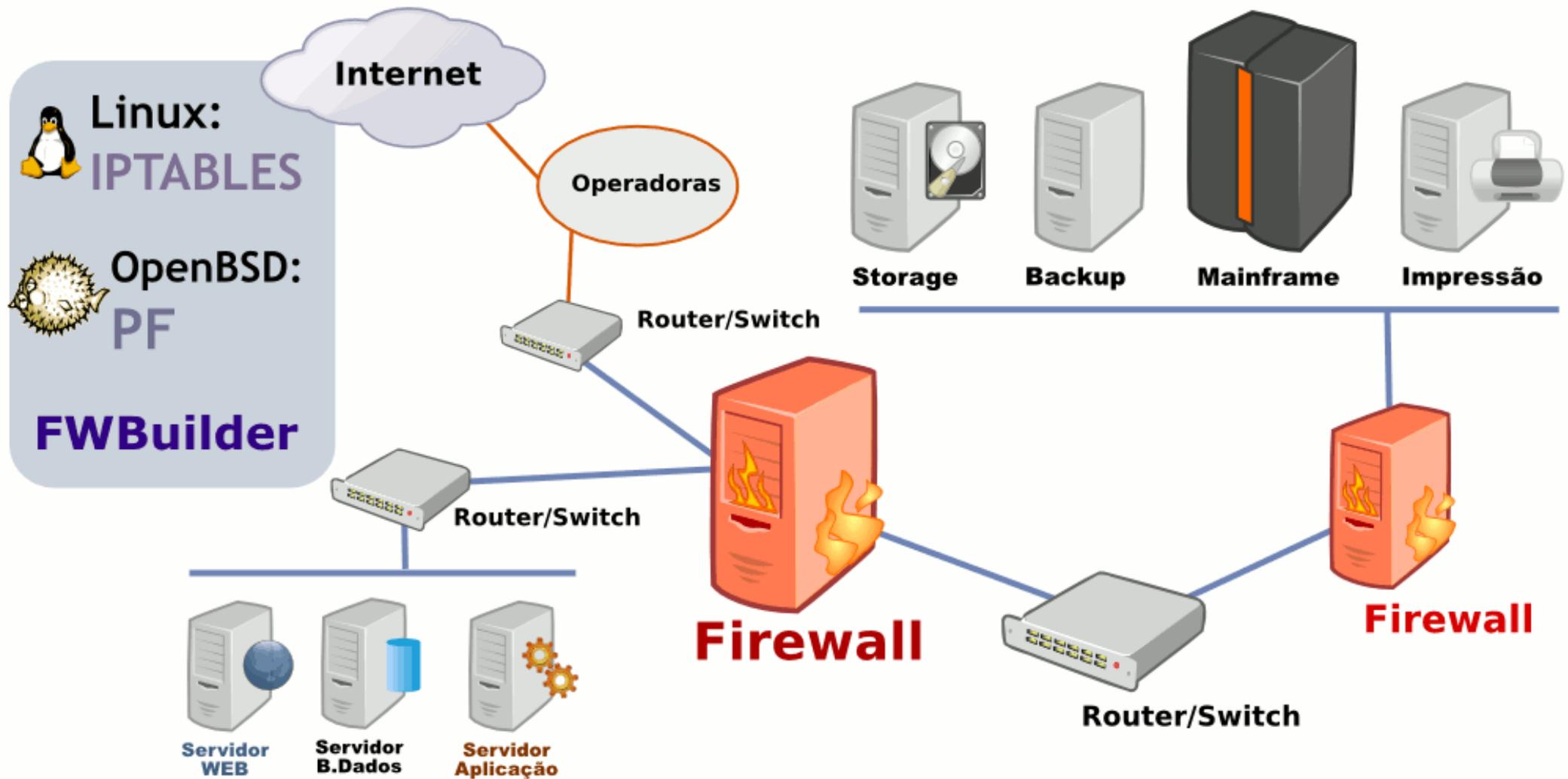


Soluções em Software Livre



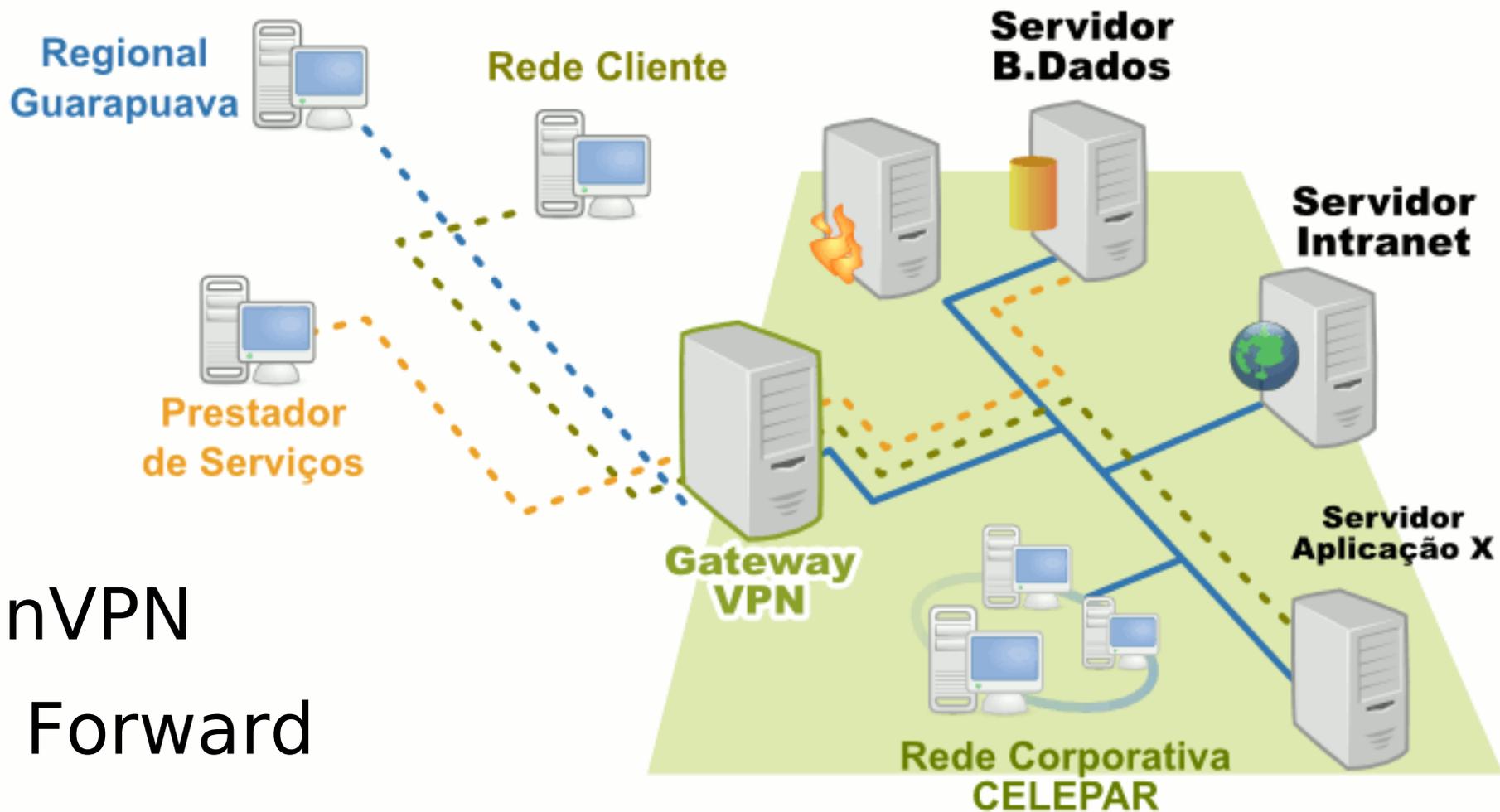
Soluções em Software Livre

Firewall



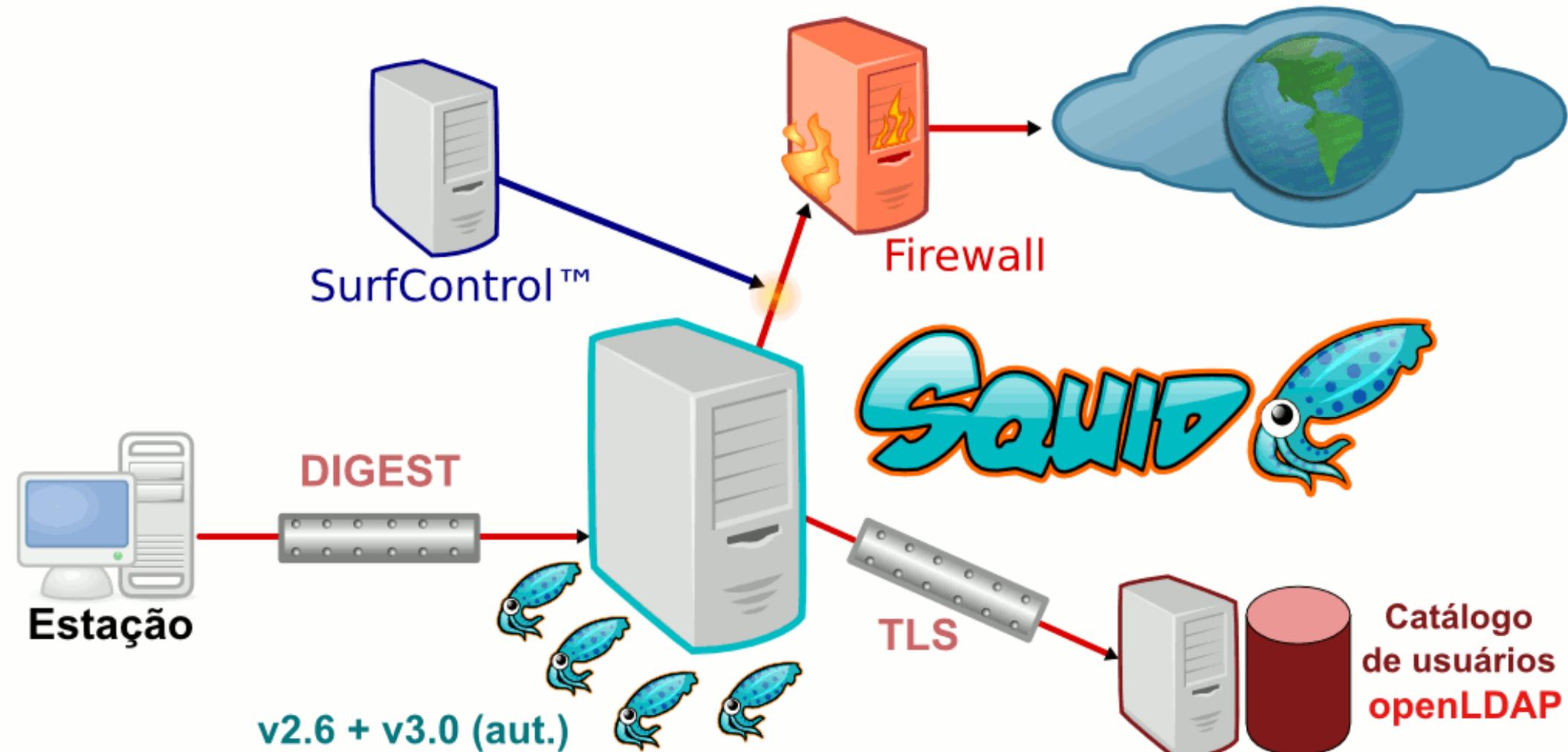
Soluções em Software Livre

Virtual Private Network (VPN)



- OpenVPN
- SSH Forward

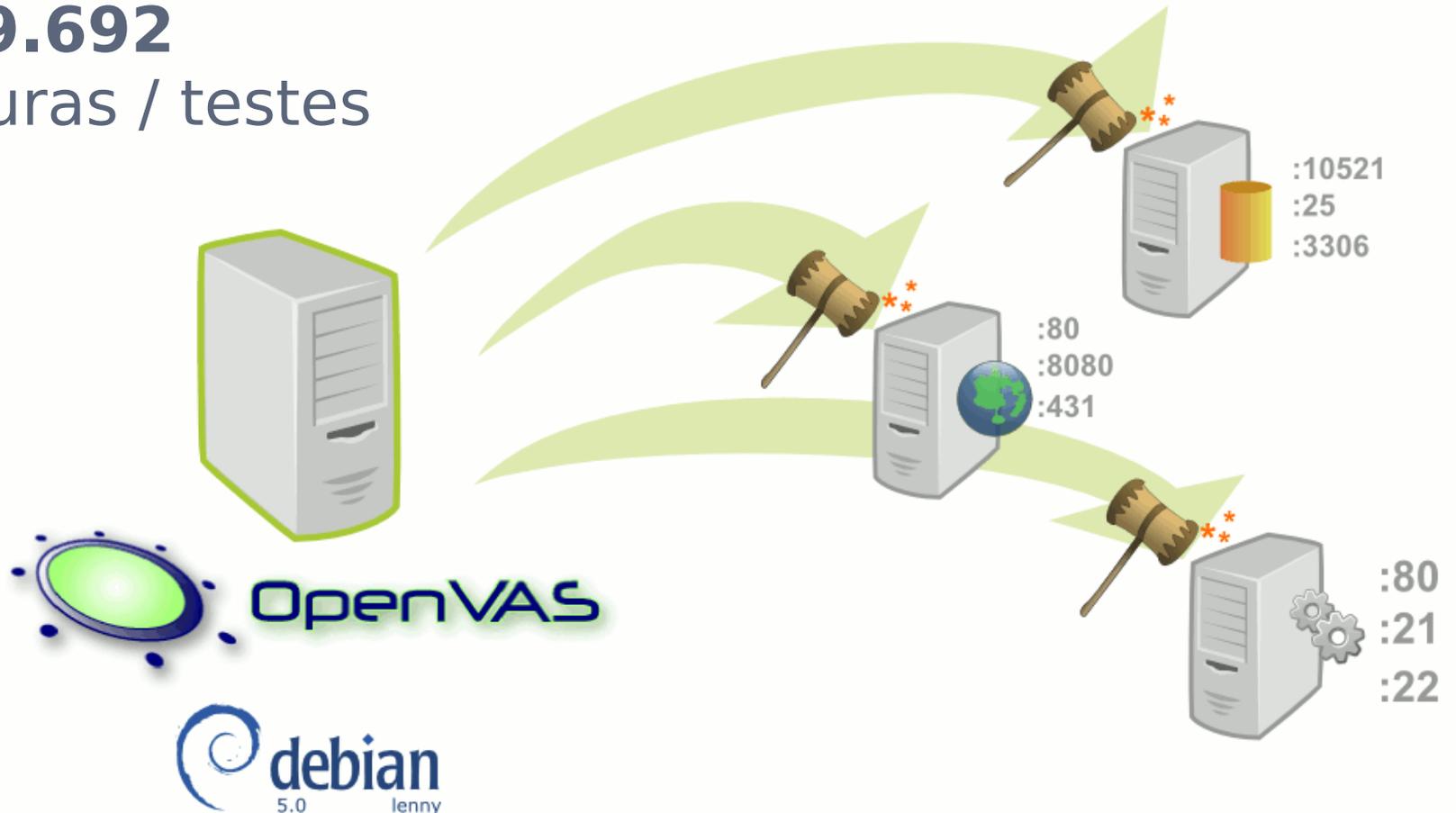
Soluções em Software Livre Web Proxy



Soluções em Software Livre

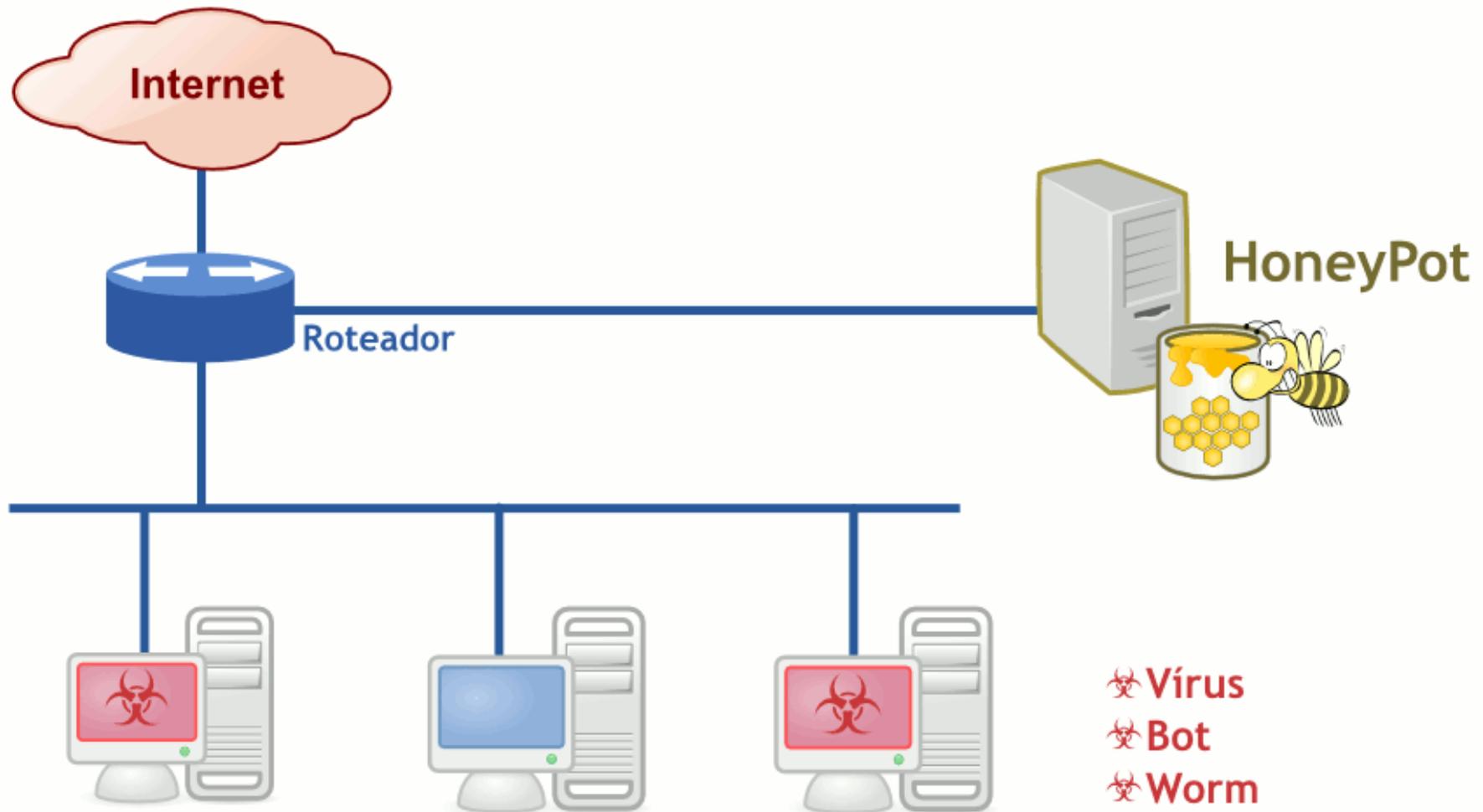
Verificação de Vulnerabilidades

29.692
assinaturas / testes



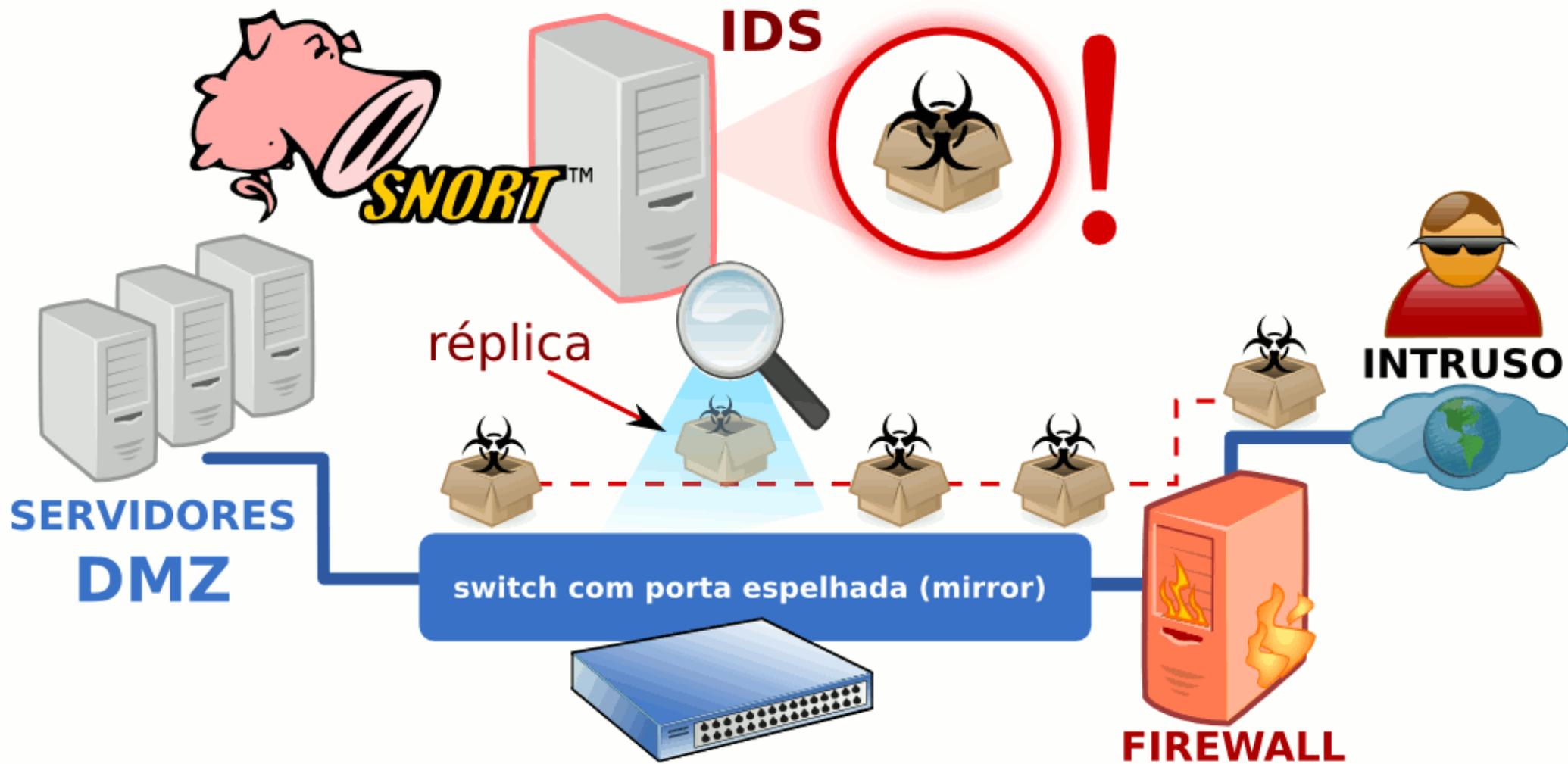
Soluções em Software Livre

HoneyPot - Nepenthes



Soluções em Software Livre

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



SABUJO



CORUJA



RAPOSA



ARAPONGAH



TAMANDUAH



PSQUILO



LAGARTOH

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

Implementações COSED

SABUJO: Identificação de usuários



SABUJO
Identificação de usuários Intranet

Início | Voltar | Telefones | | Enviar | Sair

Dados encontrados:



Nome: Jose Roberto Andrade Junior
Login: josejr
Setor: COOSEG
Telefone: [redacted]
E-mail: josejr@celepar.pr.gov.br

COOSEG

Coordenador/Superior: Tarso Dutra B de Queiroz*
Telefone: [redacted] | e-mail: tarso@celepar.pr.gov.br

DP

[redacted]



Raposa:

Sem resultados

Psquilo:

Consumo: 19,8193 KByt
Consultado em: 14/04/2009 20:

Squid:

Última requisição gerada: 14/0
URL: http://www.google.com/
IP's utilizados:

- [redacted]

DHCP:

Dados do DHCP

- Titular: JoseRoberto/COO
Host: [redacted]
MAC: [redacted]
IP: [redacted]

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



Implementações COSED

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%

Implementações COSED

CORUJA: Auditoria de Imagens



CORUJA

interface DriftNet - monitoração de imagens

Atual - Página 1

Captura de 68 arquivos | [Atualizar](#) | [Conteúdo Anterior](#)

Páginas: [1 2 3 4 5]

[Próximo](#)

<p>atual</p>  <p>Tamanho: 51,36 Kb ↓ Data: 11/07/2007 12:09 1280px_960px</p>	<p>atual</p>  <p>Tamanho: 118,91 Kb ↓ Data: 11/07/2007 12:09 1024px_768px</p>	<p>atual</p>  <p>Tamanho: 326,71 Kb ↓ Data: 11/07/2007 12:09 1024px_768px</p>	<p>atual</p>  <p>Tamanho: 313,61 Kb ↓ Data: 02/02/2007 15:27 1600px_1200px</p>
<p>atual</p>  <p>Tamanho: 747,61 Kb ↓ Data: 01/06/2007 14:39 1400px_1419px</p>	<p>atual</p>  <p>Tamanho: 382,47 Kb ↓ Data: 02/02/2007 15:27 1504px_1000px</p>	<p>atual</p>  <p>Tamanho: 160,20 Kb ↓ Data: 01/06/2007 14:47 650px_418px</p>	<p>atual</p>  <p>Tamanho: 412,01 Kb ↓ Data: 02/02/2007 15:27 937px_589px</p>
<p>atual</p>  <p>Tamanho: 384,44 Kb ↓ Data: 02/02/2007 15:27 937px_589px</p>	<p>atual</p>  <p>Tamanho: 170,36 Kb ↓ Data: 02/02/2007 15:27 1024px_768px</p>	<p>atual</p>  <p>Tamanho: 249,43 Kb ↓ Data: 01/06/2007 14:48 433px_312px</p>	<p>atual</p>  <p>Tamanho: 3,36 Mb ↓ Data: 01/06/2007 14:50 2126px_1367px</p>
<p>atual</p>  <p>Tamanho: 230,48 Kb ↓ Data: 11/05/2007 14:56 1676px_1114px</p>	<p>atual</p>  <p>Tamanho: 394,07 Kb ↓ Data: 07/08/2008 17:21 1600px_1200px</p>	<p>atual</p>  <p>Tamanho: 52,95 Kb ↓ Data: 01/06/2007 14:48 561px_421px</p>	<p>atual</p>  <p>Tamanho: 70,23 Kb ↓ Data: 26/06/2008 17:07 1500px_1000px</p>

Coruja - Interface DriftNet
CELEPAR - Informática do Paraná
Powered by PERL & PHP

Driftnet

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

Implementações COSED

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:

- 68.132.127.222

Domínios acessados

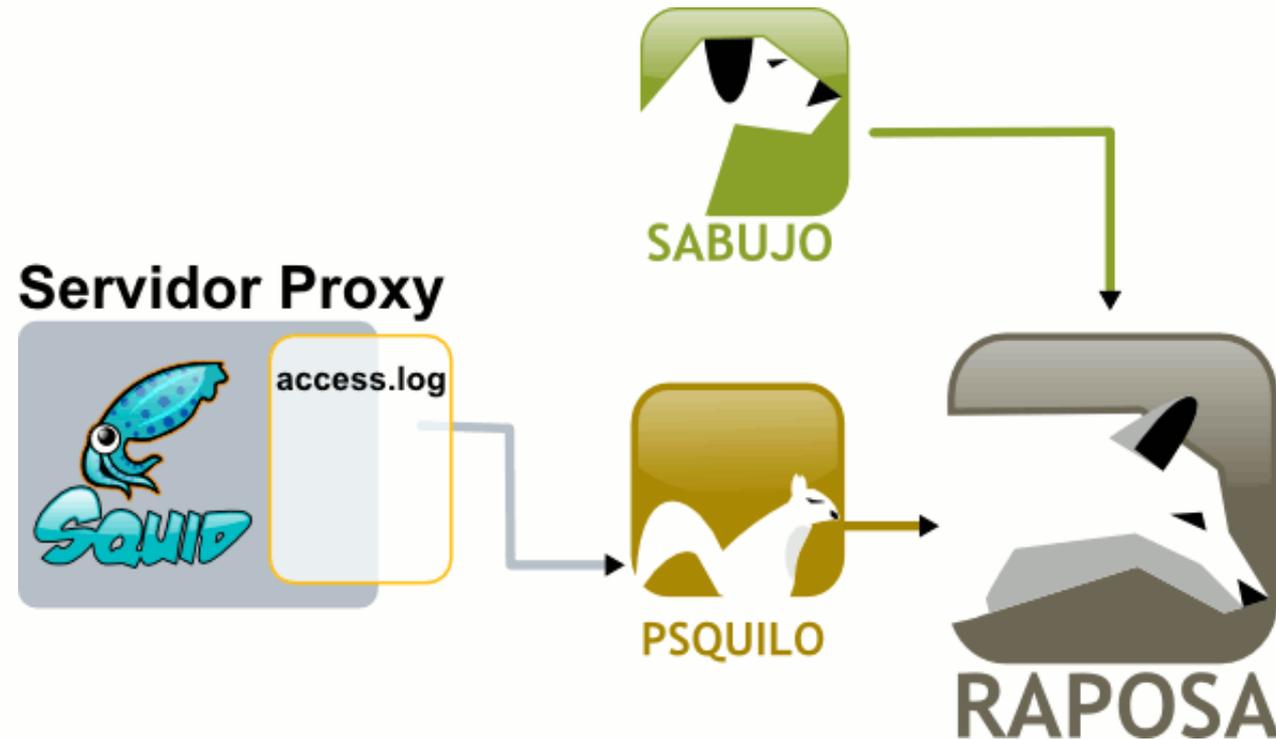
Legenda: * bloqueio parcial | ● liberados | ● negados | requisições

Domínio	Volume	1 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

Implementações COSED

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: 10.152.227.55**

◆ **MAC: 00:22:15:0A:00:00**

◆ **MAC: 00:22:15:0A:00:00**

 **DHCP/IP NAO CADASTRADO - Alertas: 18**

Última coleta: 2009-10-20 15:10:24

🖨 **IP: 10.152.227.227**

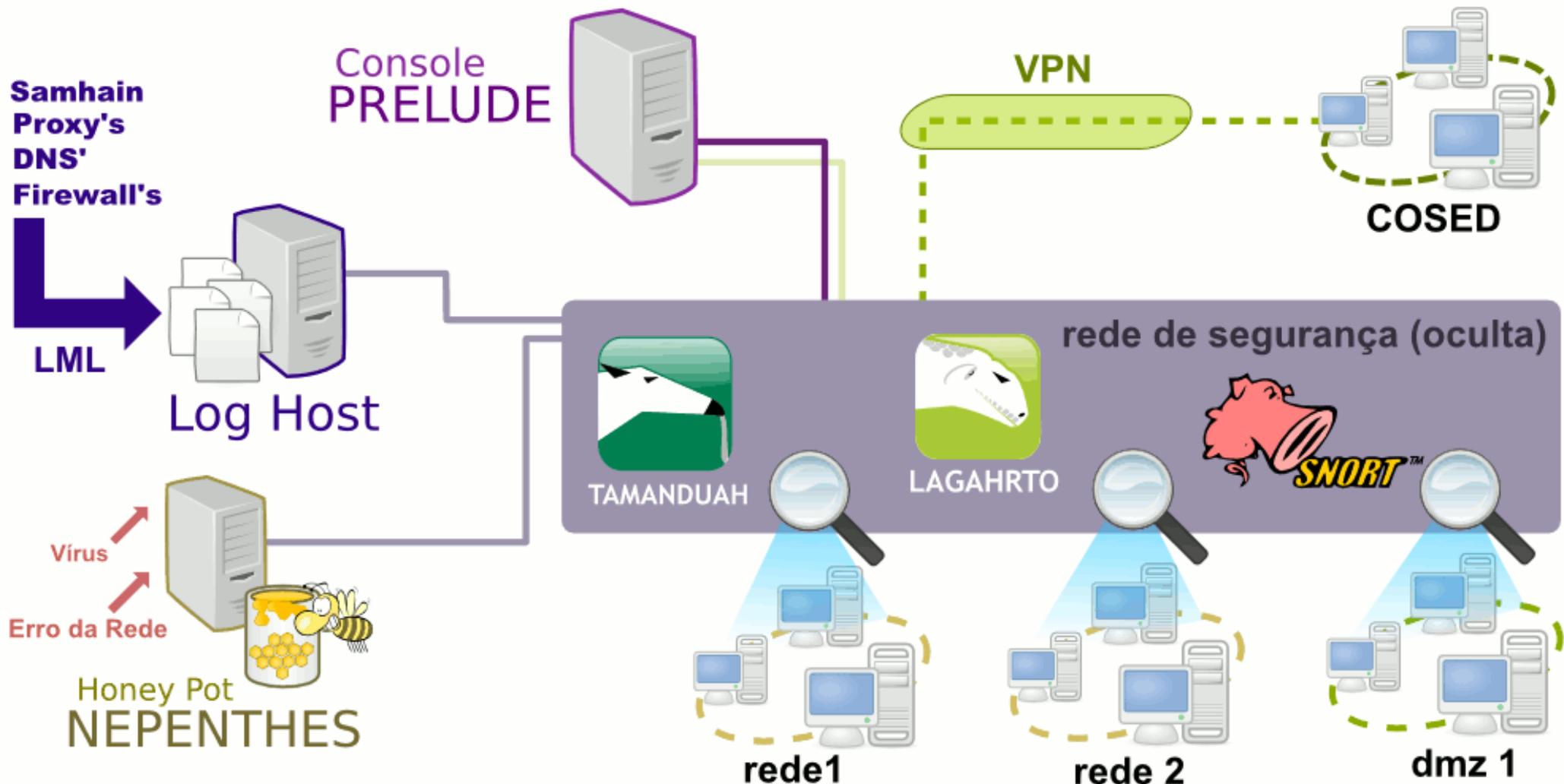
◆ **MAC: 00:22:15:0A:00:00**

 **DHCP/IP NAO CADASTRADO - Alertas: 18**

Última coleta: 2009-10-20 15:10:22

🖨 **IP: 10.152.227.151**

Implementações COSED Rede de Segurança



Implementações COSED

Monitor de Segurança - Prewikka/Prelude

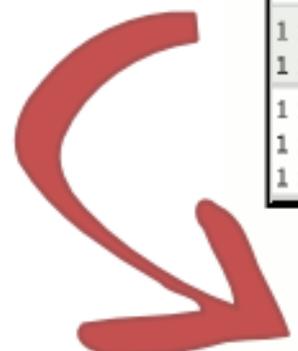



IDS




INTRUSO

1 x ET SCAN Potential SSH Scan	n/a	200.189.113.204	snr.dmzinter
1 x ET POLICY Inbound Frequent Emails - Possible Spambot Inbound	n/a	200.189.113.204	snr.dmzintera
8 x PSNG_TCP_PORTSWEEP	n/a	200.189.113.204	snr.dmzinter
1 x ICMP PING CyberKit 2.2 Windows	n/a	200.189.113.204	snr.dmzinter
1 x ICMP PING	n/a	200.189.113.204	snr.dmzinter
1 x [CSG-GOP] WEB-ATTACK - Tentativa SQL Injection (GET)	n/a	200.189.113.204	snr.dmzinter
1 x ET POLICY Proxy POST Request	n/a	200.189.113.204	snr.dmzinter
1 x ET DROP Spamhaus DROP Listed Traffic Inbound	n/a	200.189.113.204	snr.dmzinter



...: Console Corporativa ...

Localização Equipamento	Ocorrência	Mensagem
 Aplicativo: <u>CSG</u>	20/10/2009 17:51:23	 Verificar alertas! Ultimo foi 672537 (200.189.113.83) !
 Datacenter RACK001 <u>SNIC001-001</u>	20/10/2009 17:44:23	 - Resoluções atingiu o limite de conexões. Aguardar 20 minutos
 Datacenter RACK001 <u>SC001-010</u>	20/10/2009 17:49:20	Memoria livre (MB) (Valor=6.67, limite inferior=10.0) SNMP

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?

Material distribuído segundo a licença:



Atribuição-Usu Não-Comercial-Vedada a Criação
de Obras Derivadas 2.5 Brasil



<http://creativecommons.org/licenses/by-nc-nd/2.5/br/>

Produzido com:

