IV JAI
UNICENTRO
15 de agosto de 2011

HoneyNet PR.GOV.BR

Hermano Pereira
Oeslei Taborda Ribas

Agenda

- Rede PR.GOV.BR
- Conceito:
  - HoneyPot, DNS SinkHole, HoneyNet
- Aplicação:
  - HoneyPot Corporativo, HoneyPot Alliance
- Tratamento de Incidentes

96 slides em ~40 minutos

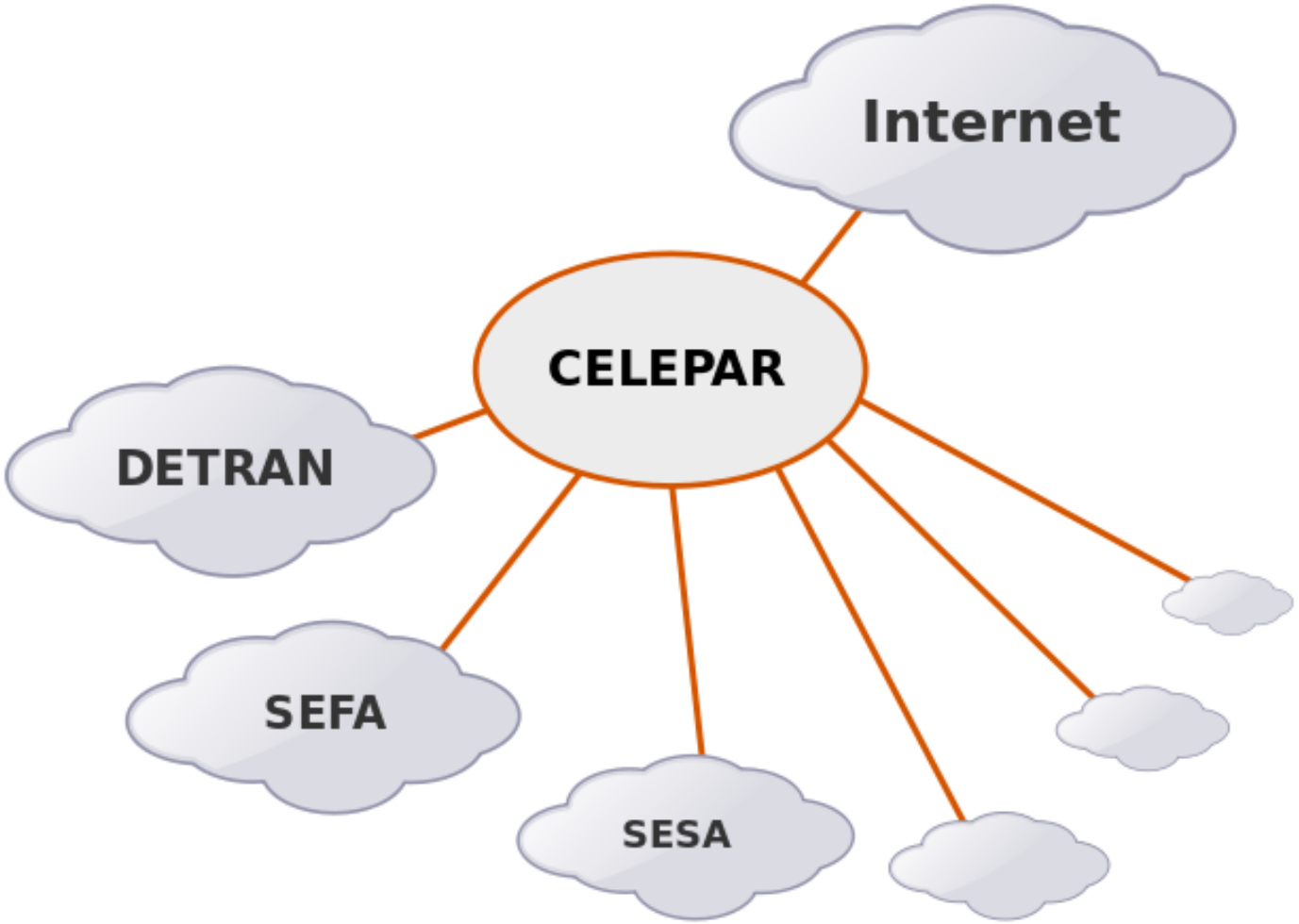
Rede PR.GOV.BR

- CELEPAR
  - Companhia de Informática do Paraná
  - Economia Mista (Governo do Paraná)
  - Clientes:

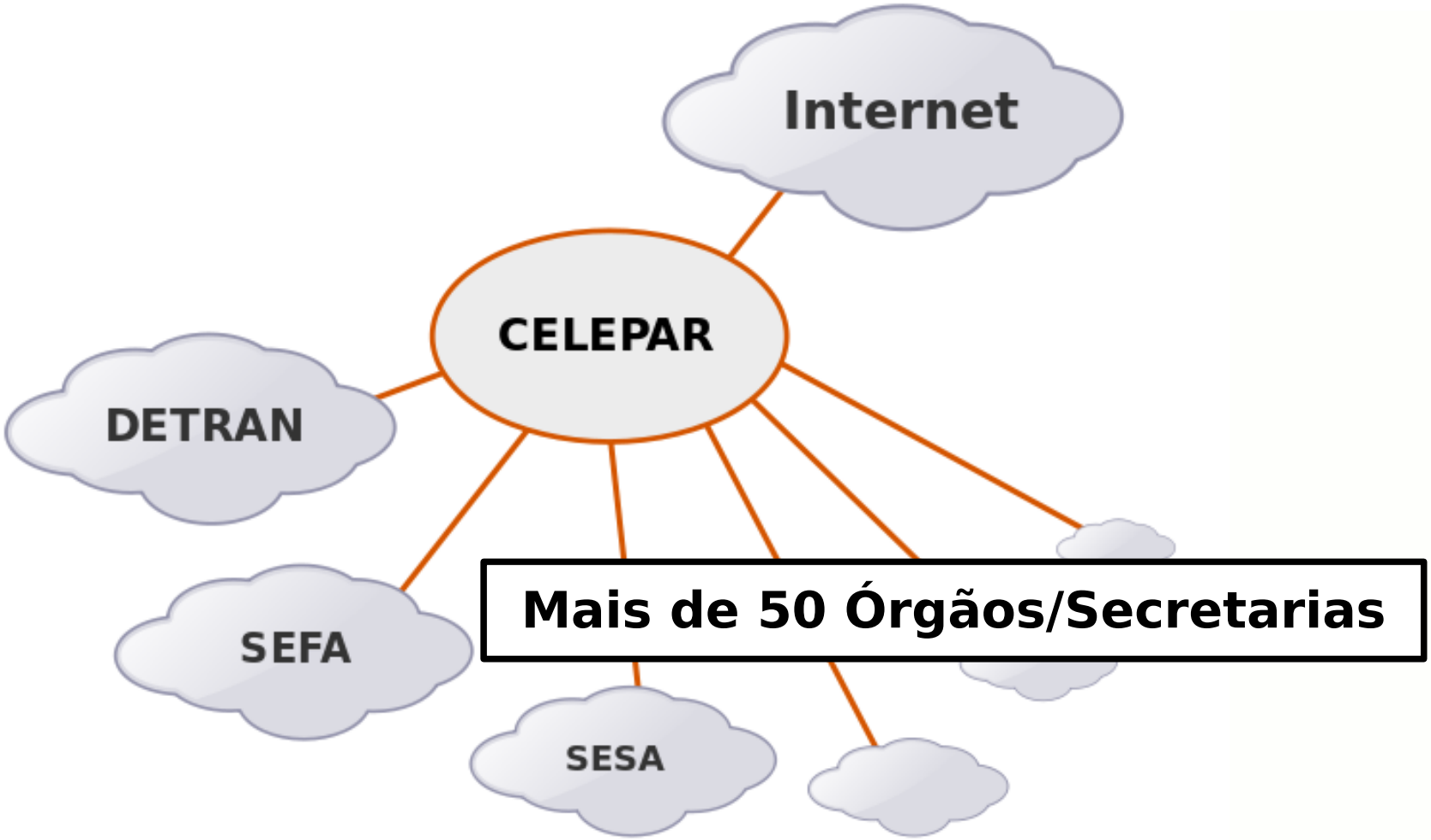
    DETRAN, SEFA, SESA, SEED, SESP...

www.celepar.pr.gov.br

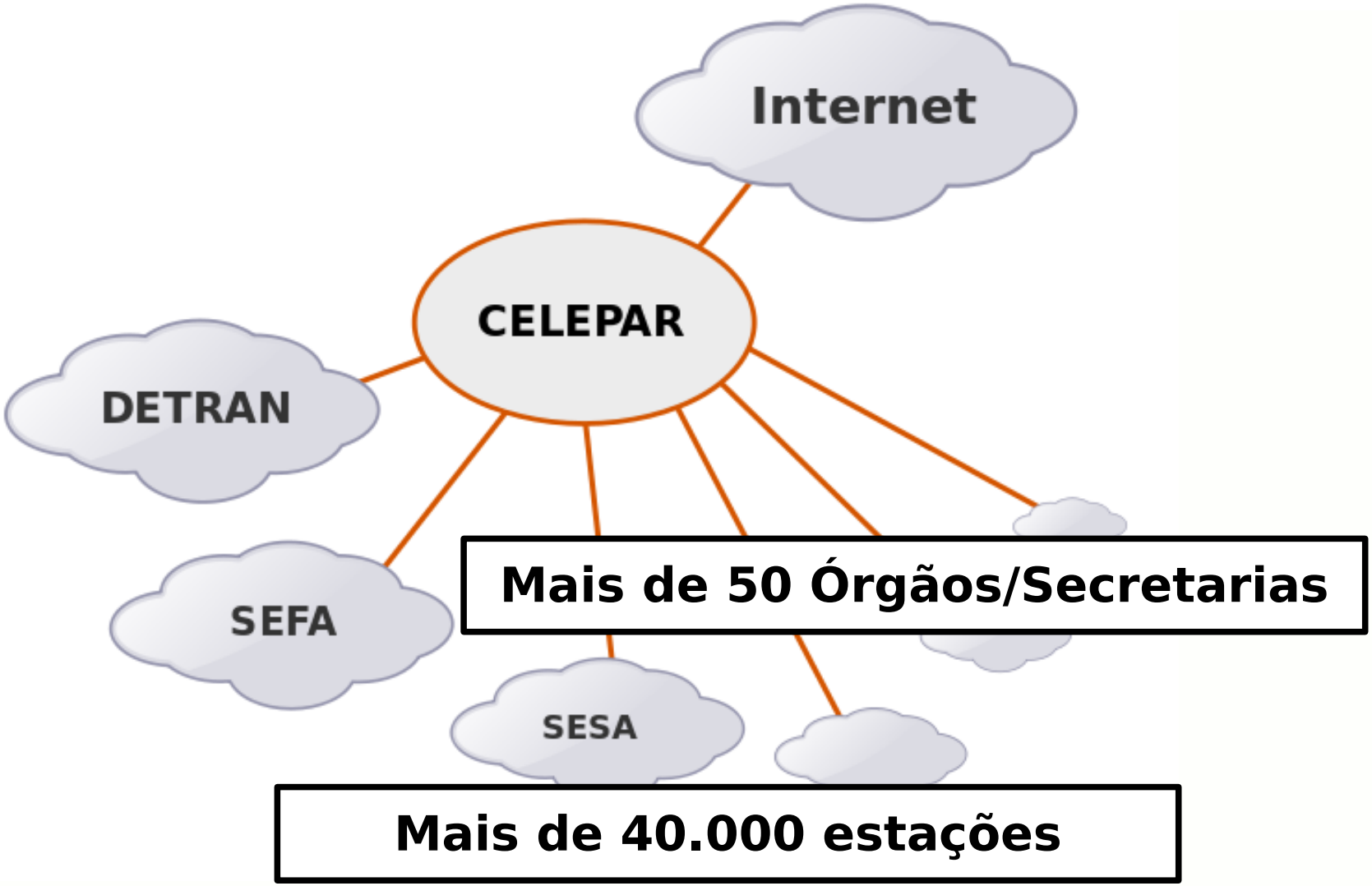
Rede PR.GOV.BR



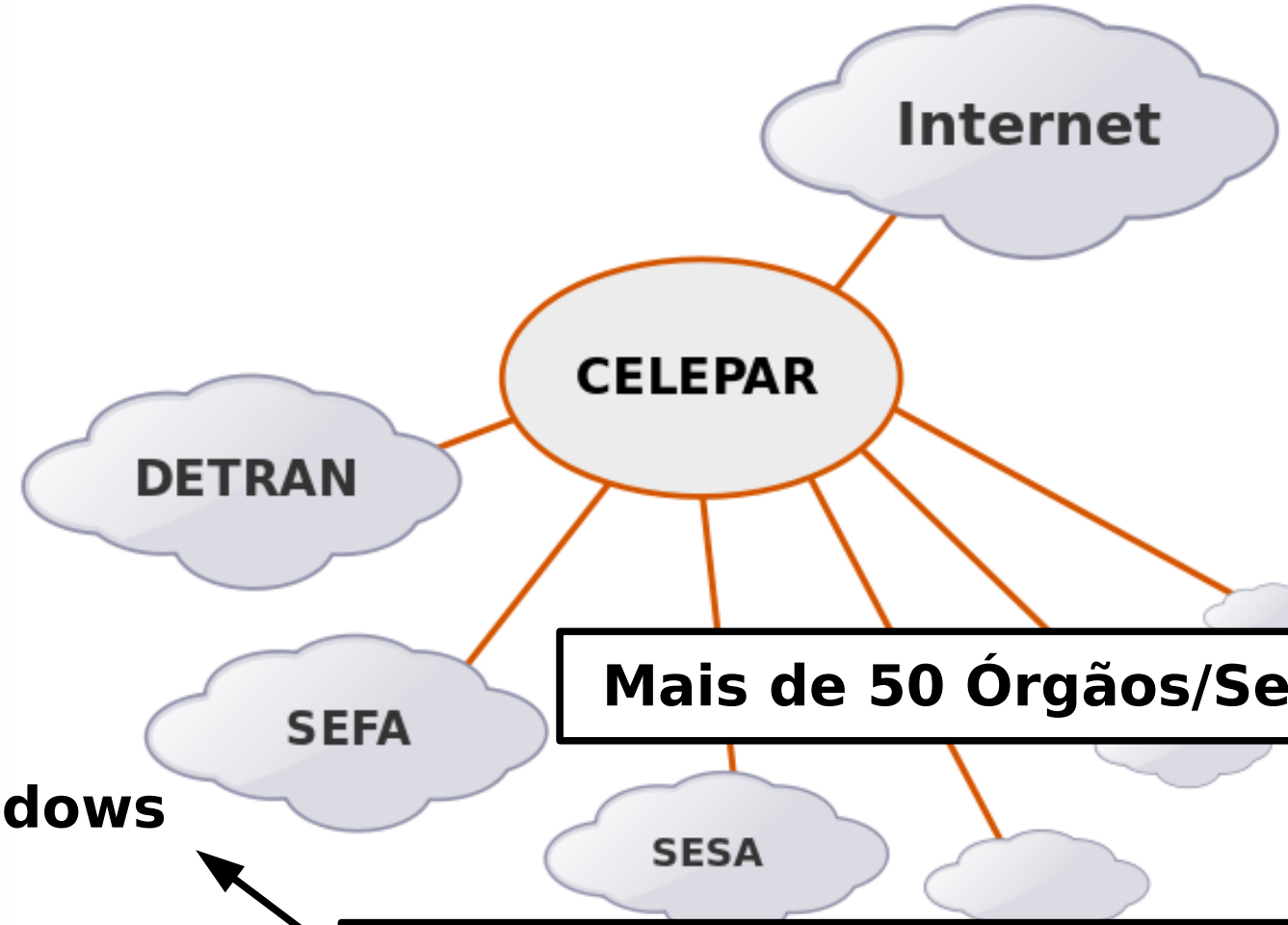
Rede PR.GOV.BR



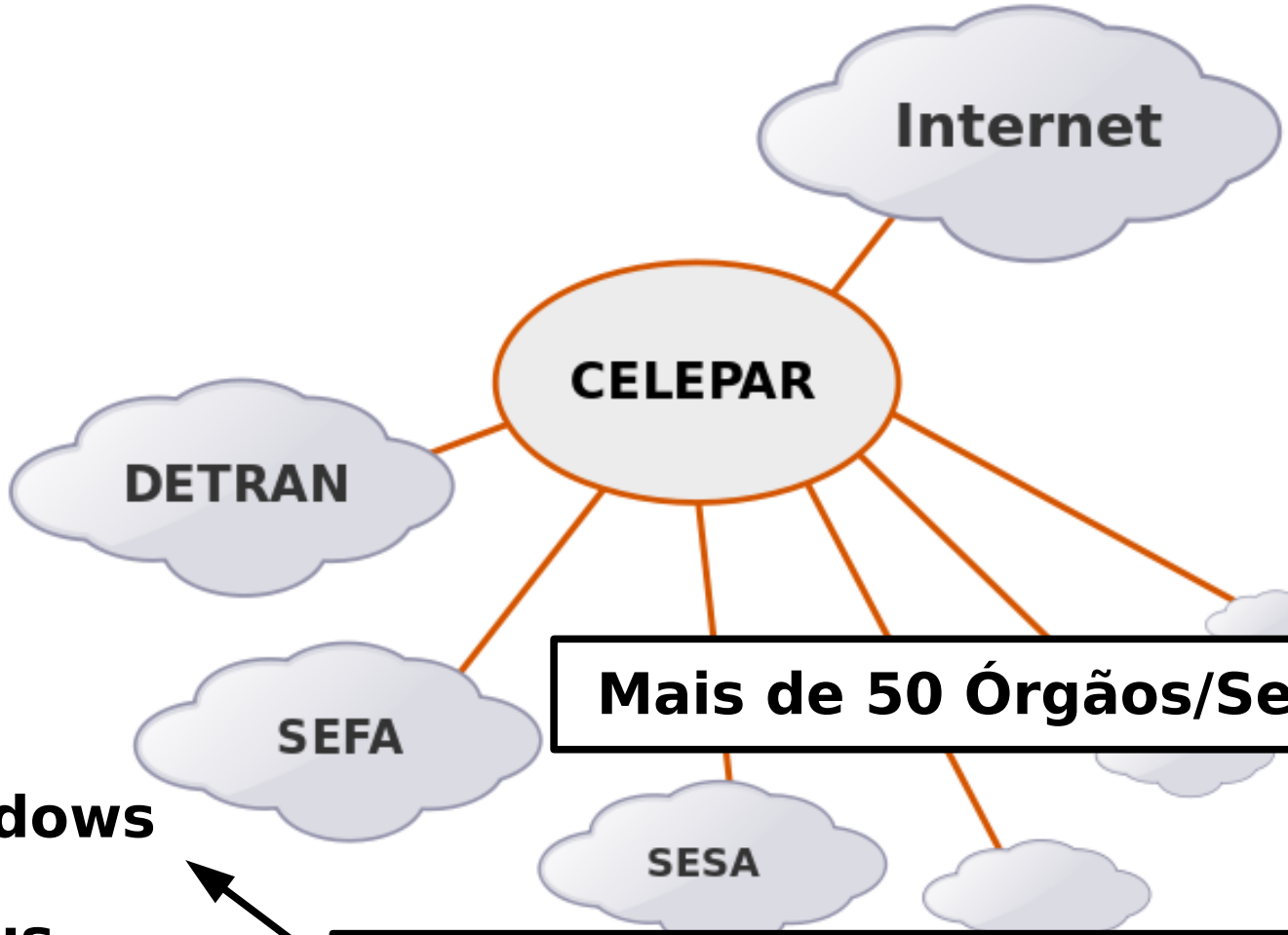
Rede PR.GOV.BR



Rede PR.GOV.BR



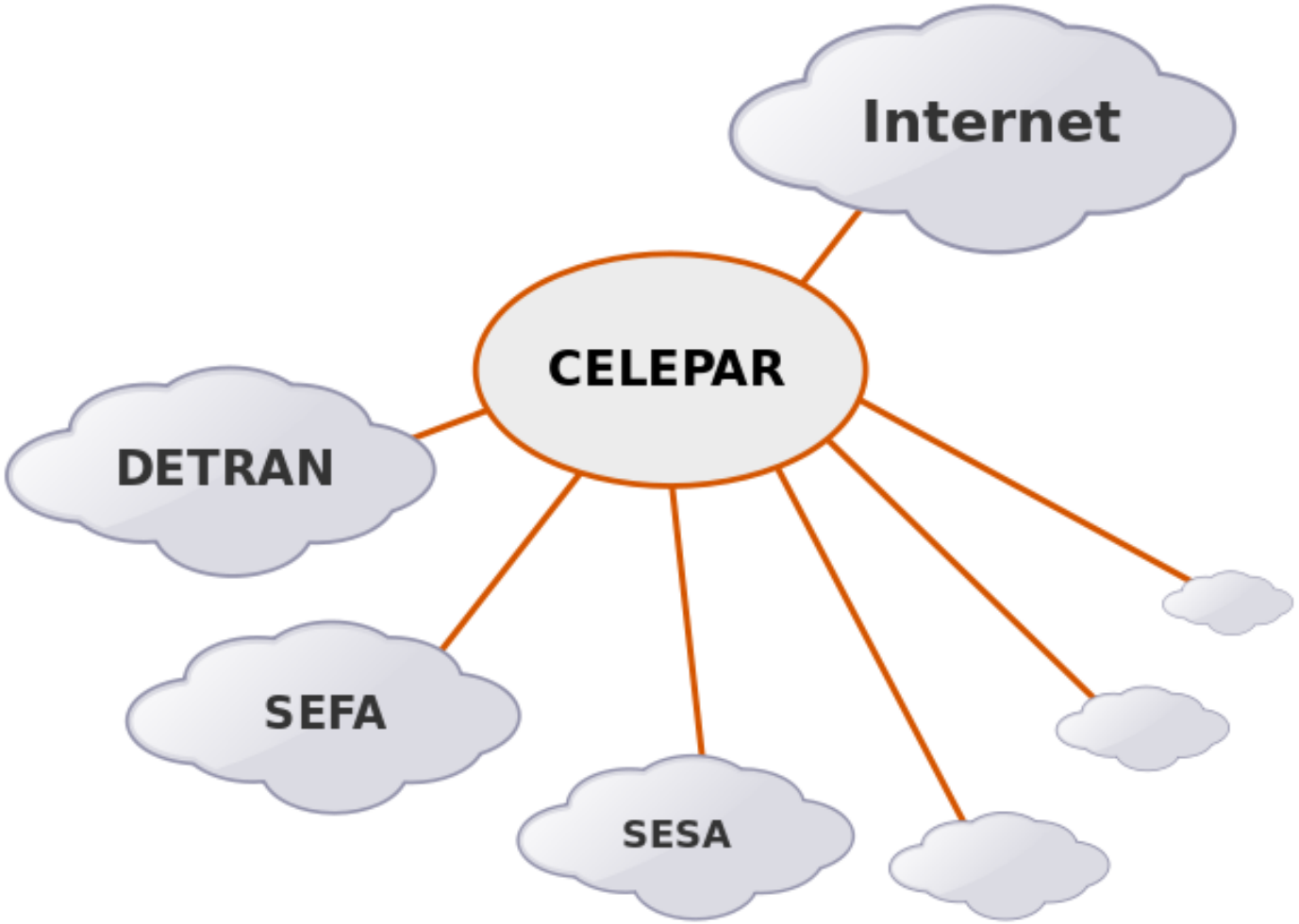
Rede PR.GOV.BR



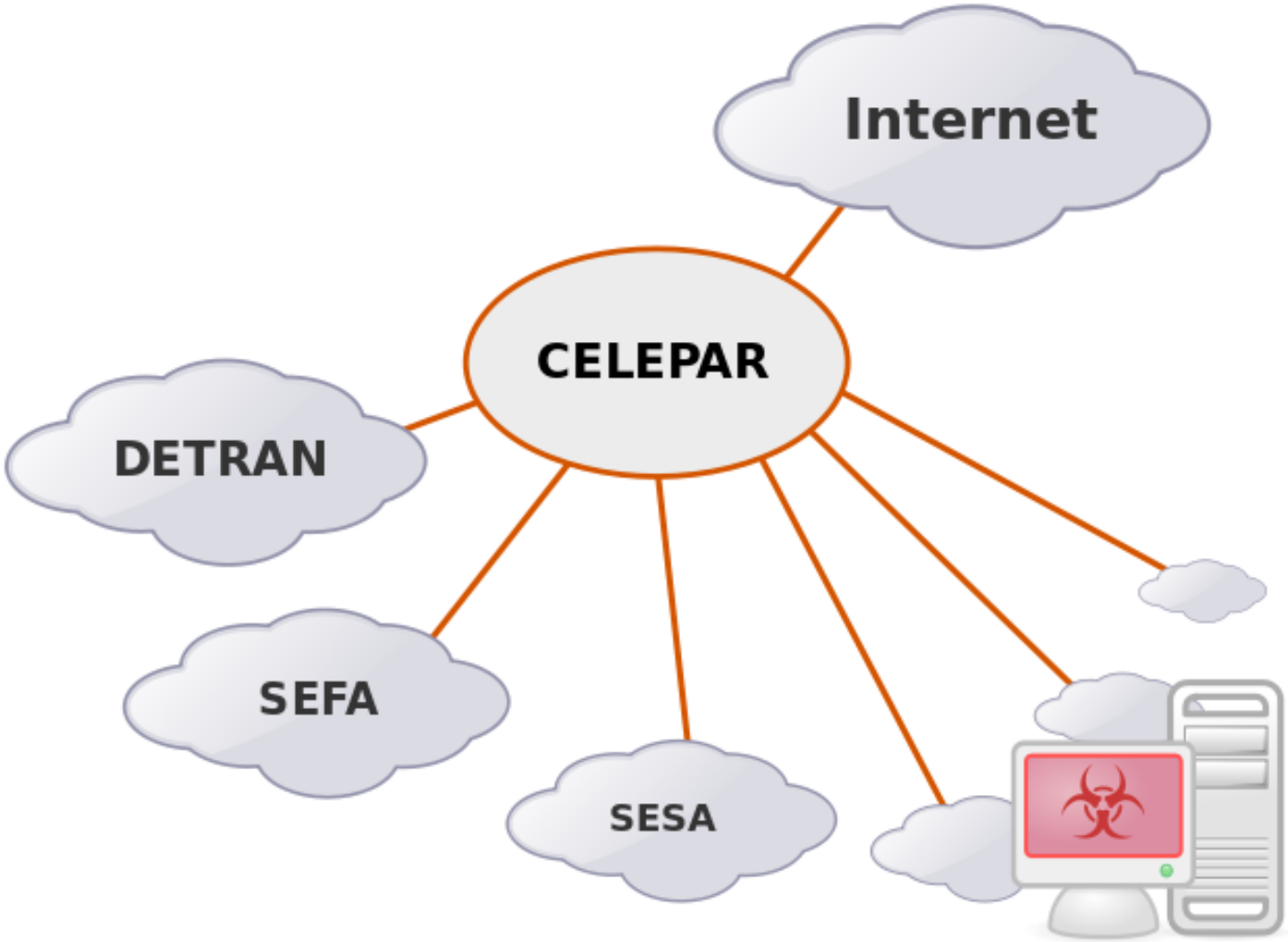
~45% Windows

Antivírus Corporativo

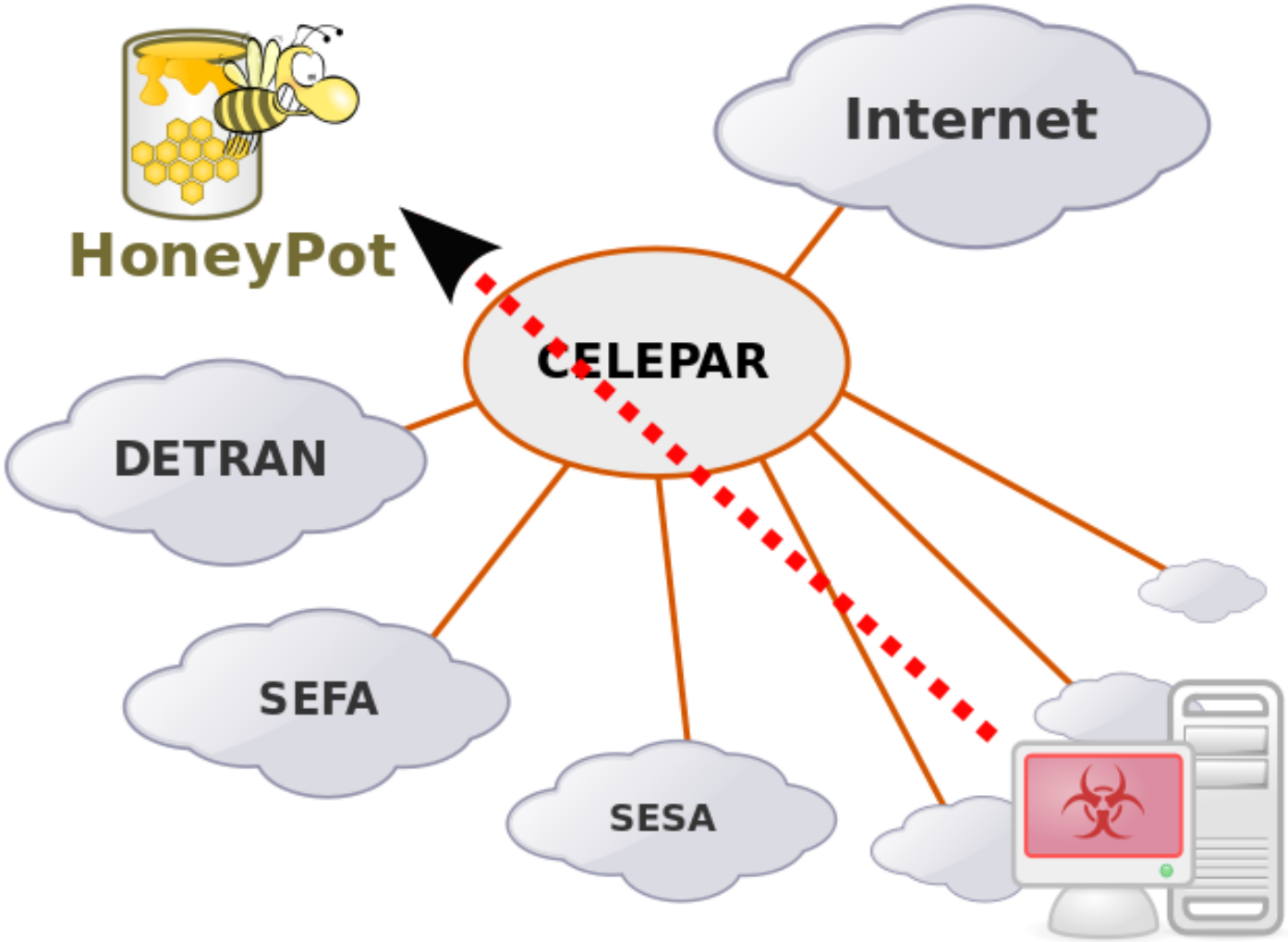
Rede PR.GOV.BR



Rede PR.GOV.BR



Rede PR.GOV.BR



Conceitos

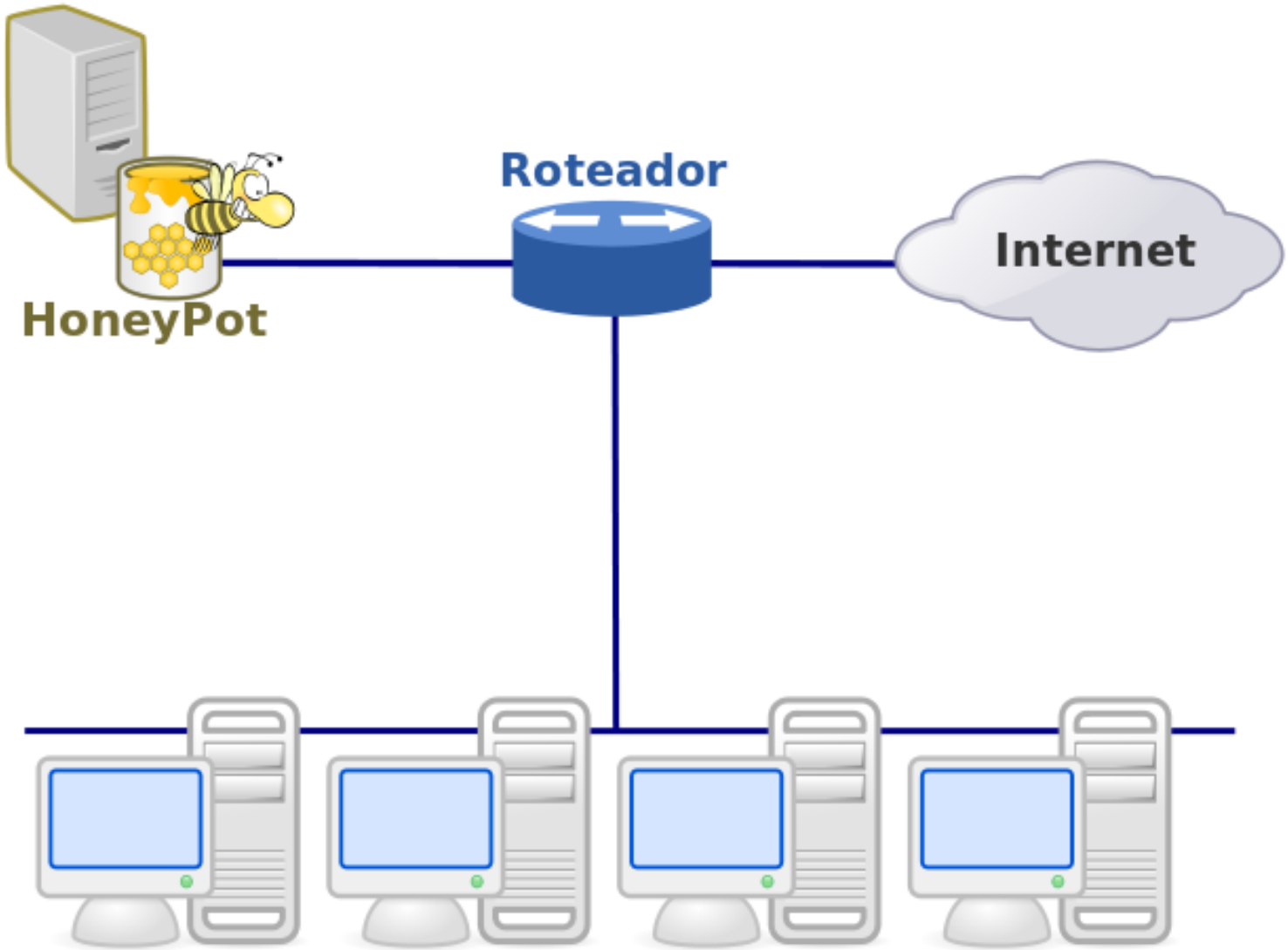
HoneyPot
DNS SinkHole
HoneyNet

CELEPAR
INFORMÁTICA
do PARANÁ

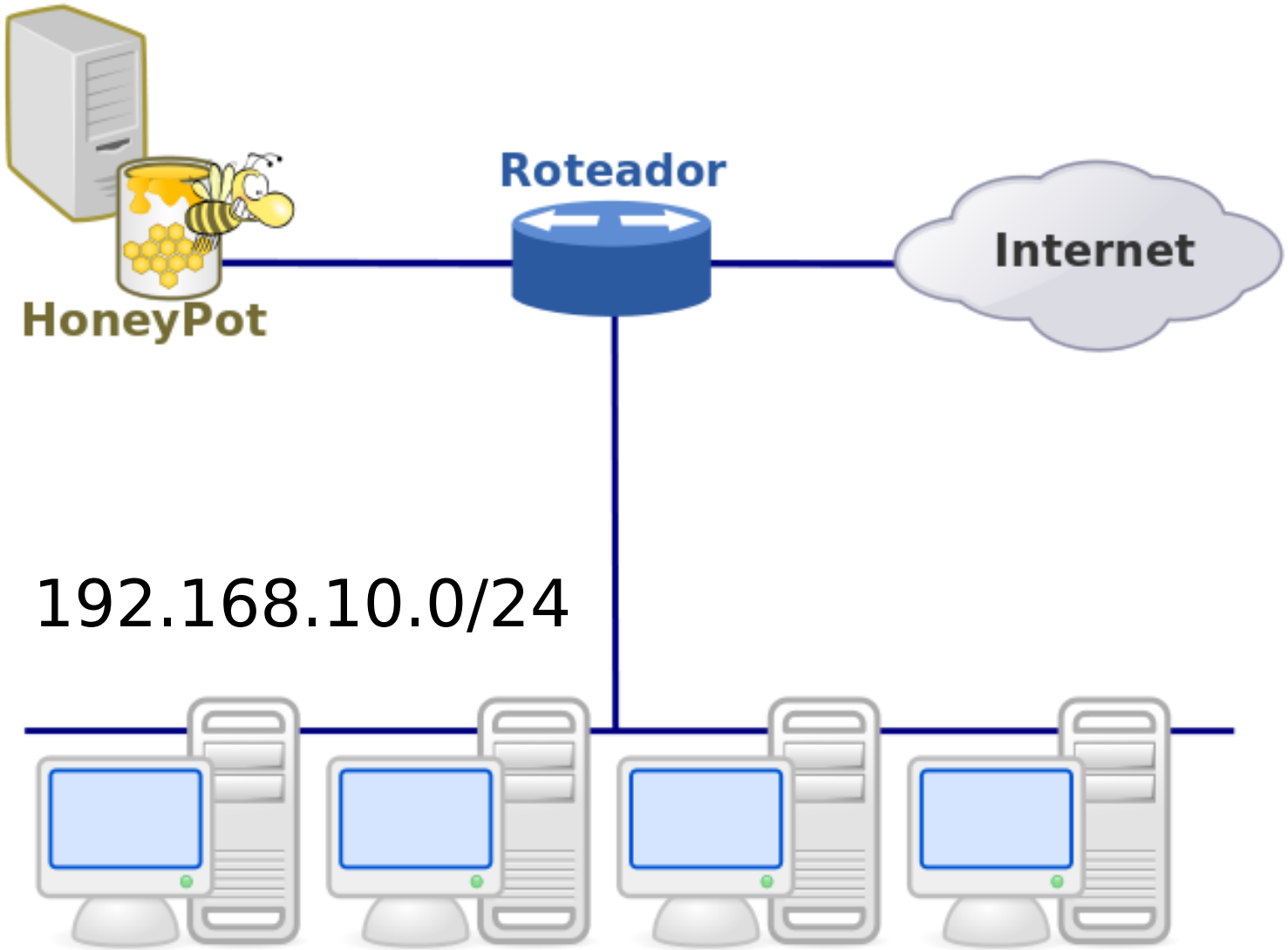
- **HoneyPot**

  Um honeypot é um recurso computacional de segurança dedicado a ser sondado, atacado ou comprometido.

HoneyPot



HoneyPot



HoneyPot

Roteador

Internet

Rotas para o HoneyPot:

HoneyPot

Roteador

Internet

Rotas para o HoneyPot:

RFC 1918
- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

HoneyPot

Roteador

Internet

Rotas para o HoneyPot:

RFC 3927
- 169.254.0.0/16

RFC 1112
- 0.0.0.0/8
- 127.0.0.0/8

HoneyPot

Roteador

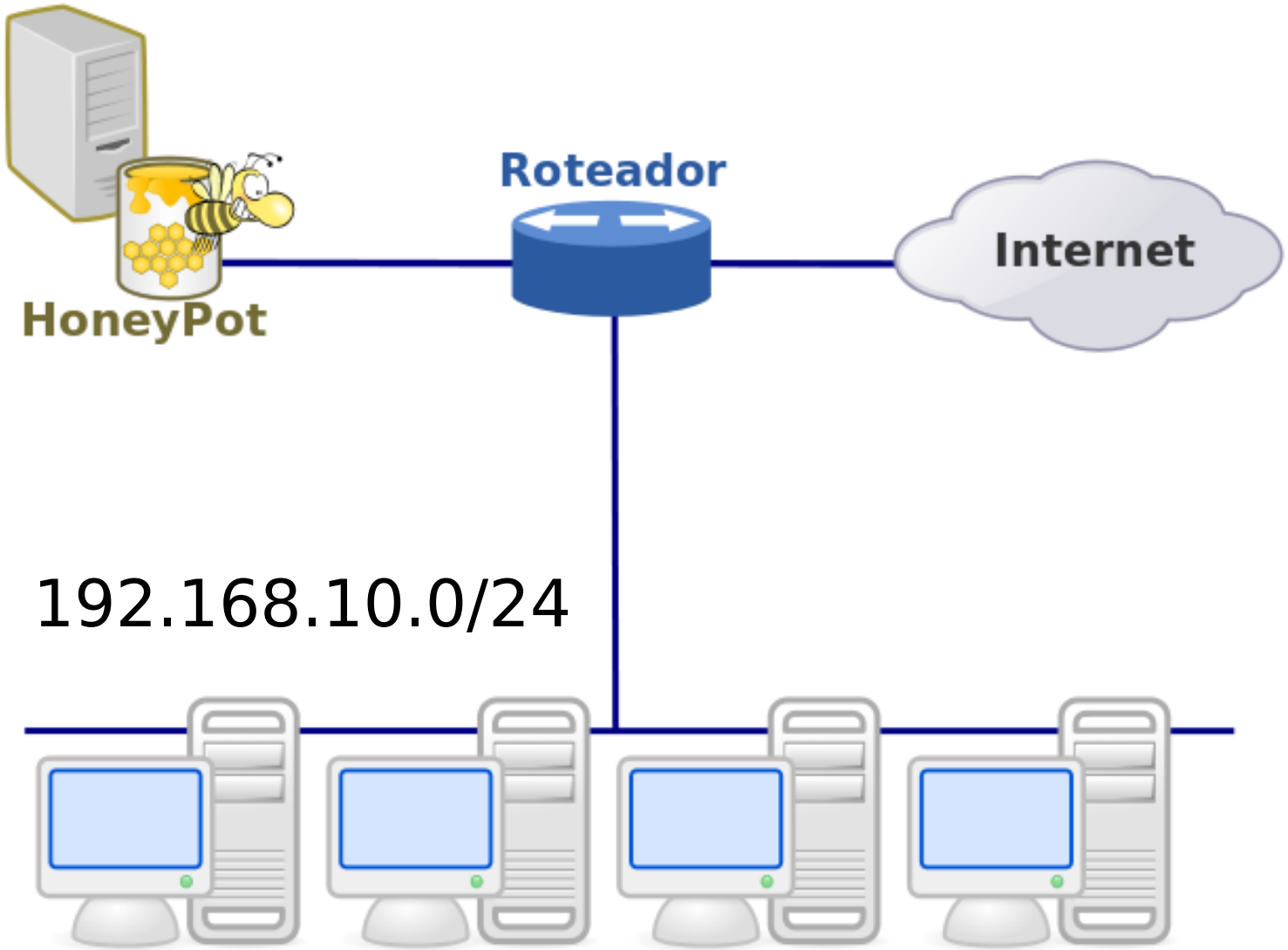
Internet

Rotas para o HoneyPot:

RFC 5737
- 192.0.2.0/24
- 198.51.100.0/24
- 203.0.113.0/24

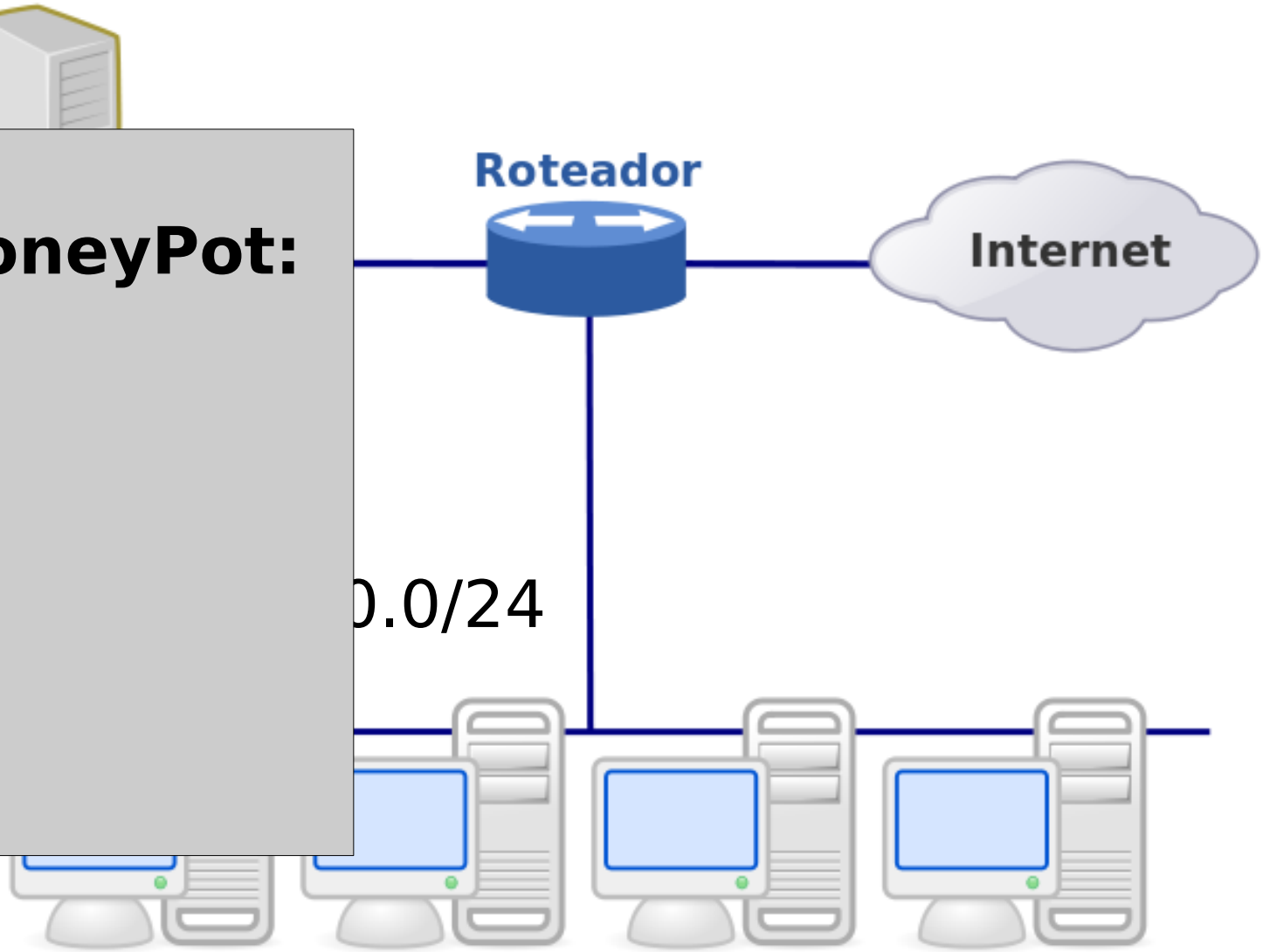
RFC 2544
- 198.18.0.0/15

HoneyPot

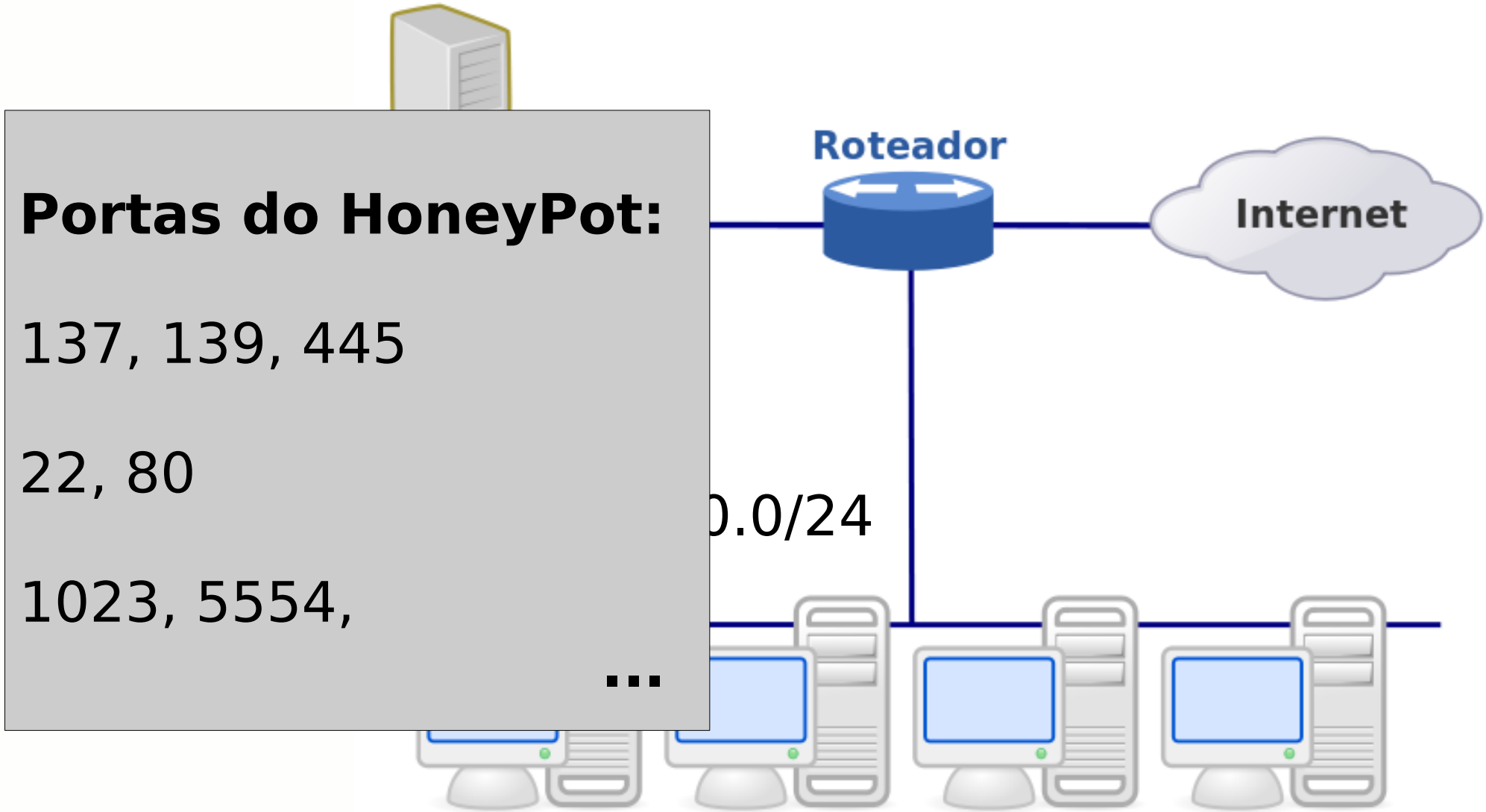


HoneyPot

Portas do HoneyPot:



HoneyPot



Portas do HoneyPot:

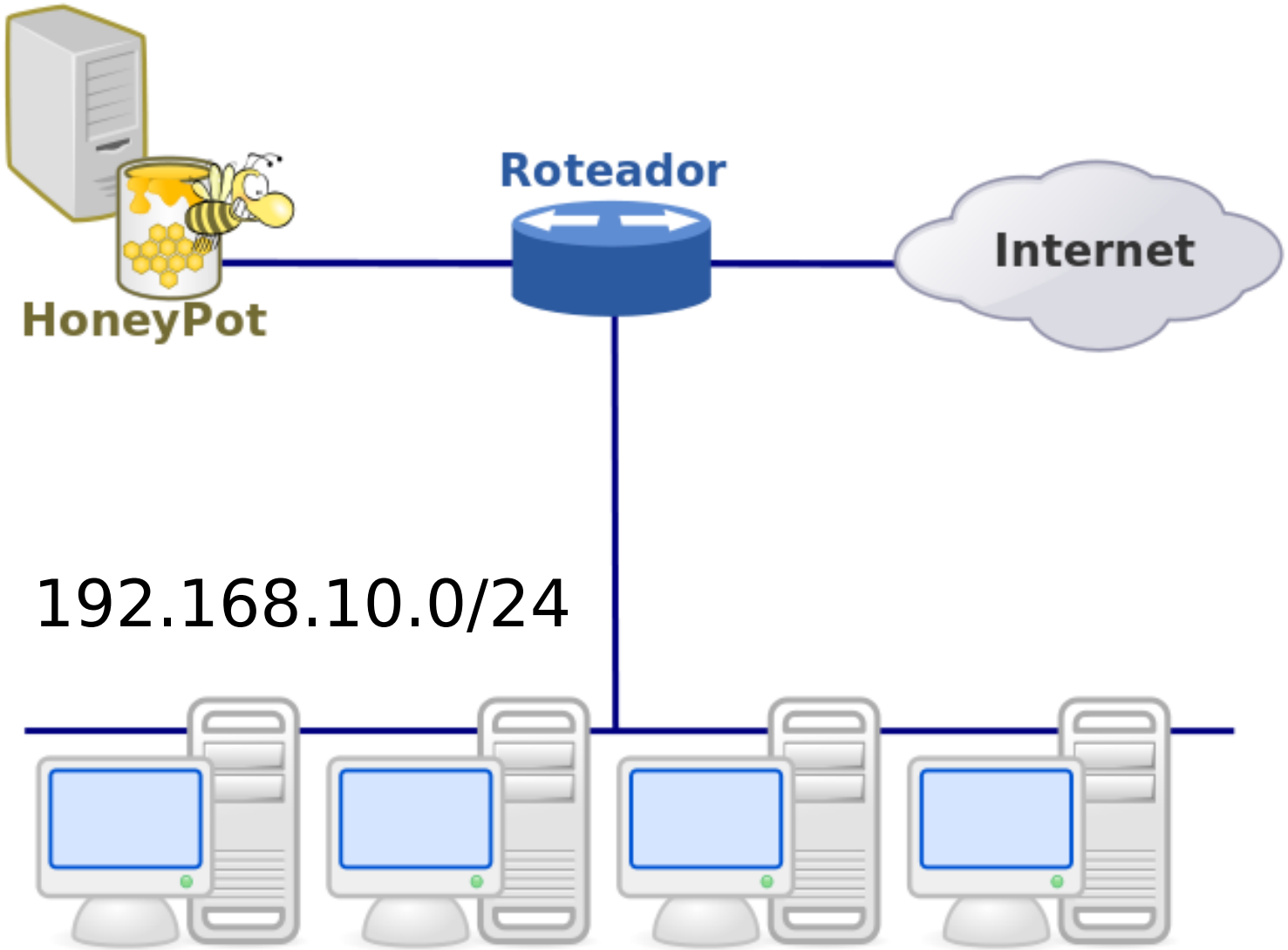
137, 139, 445

22, 80

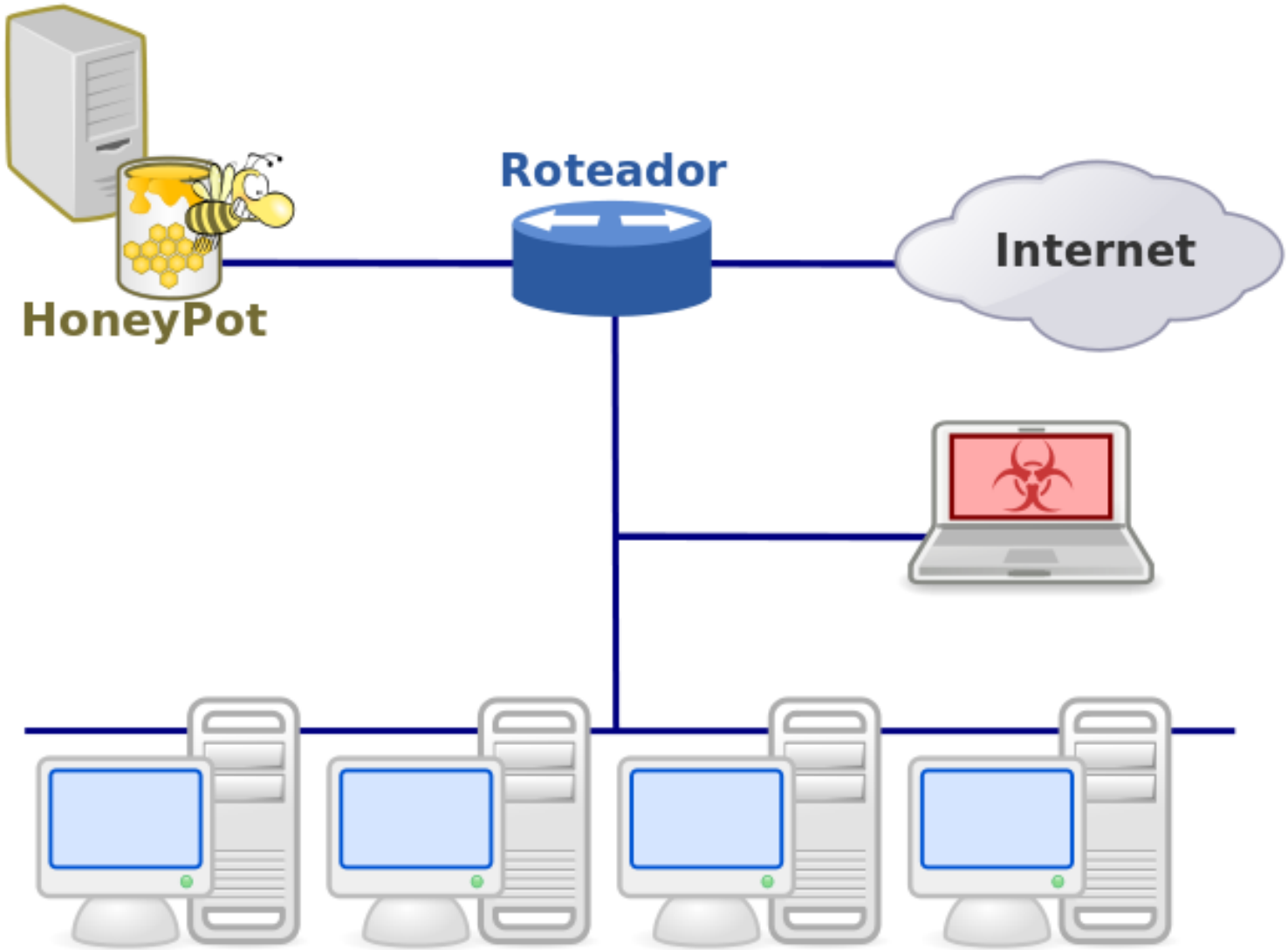
1023, 5554,

...

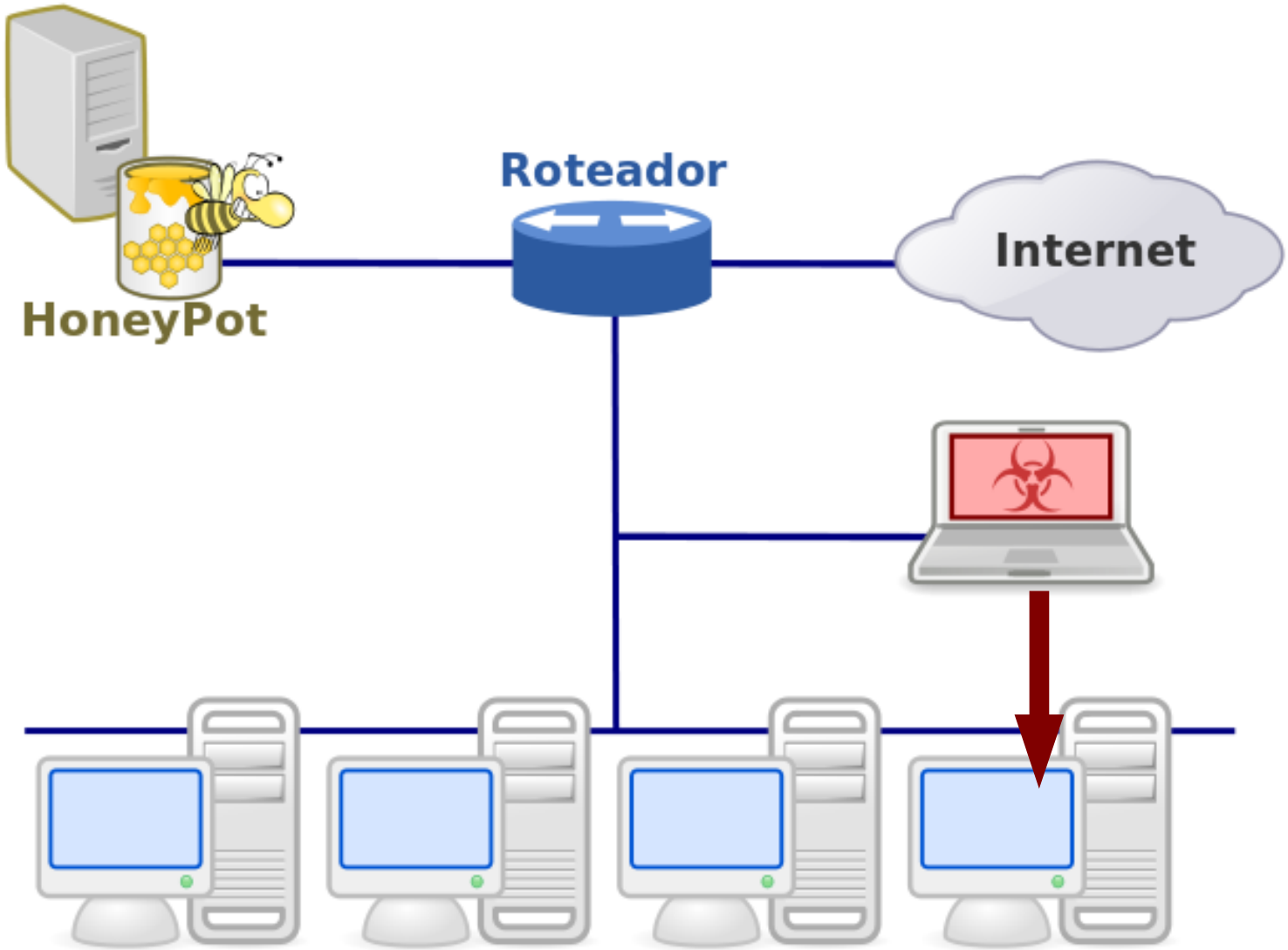
HoneyPot



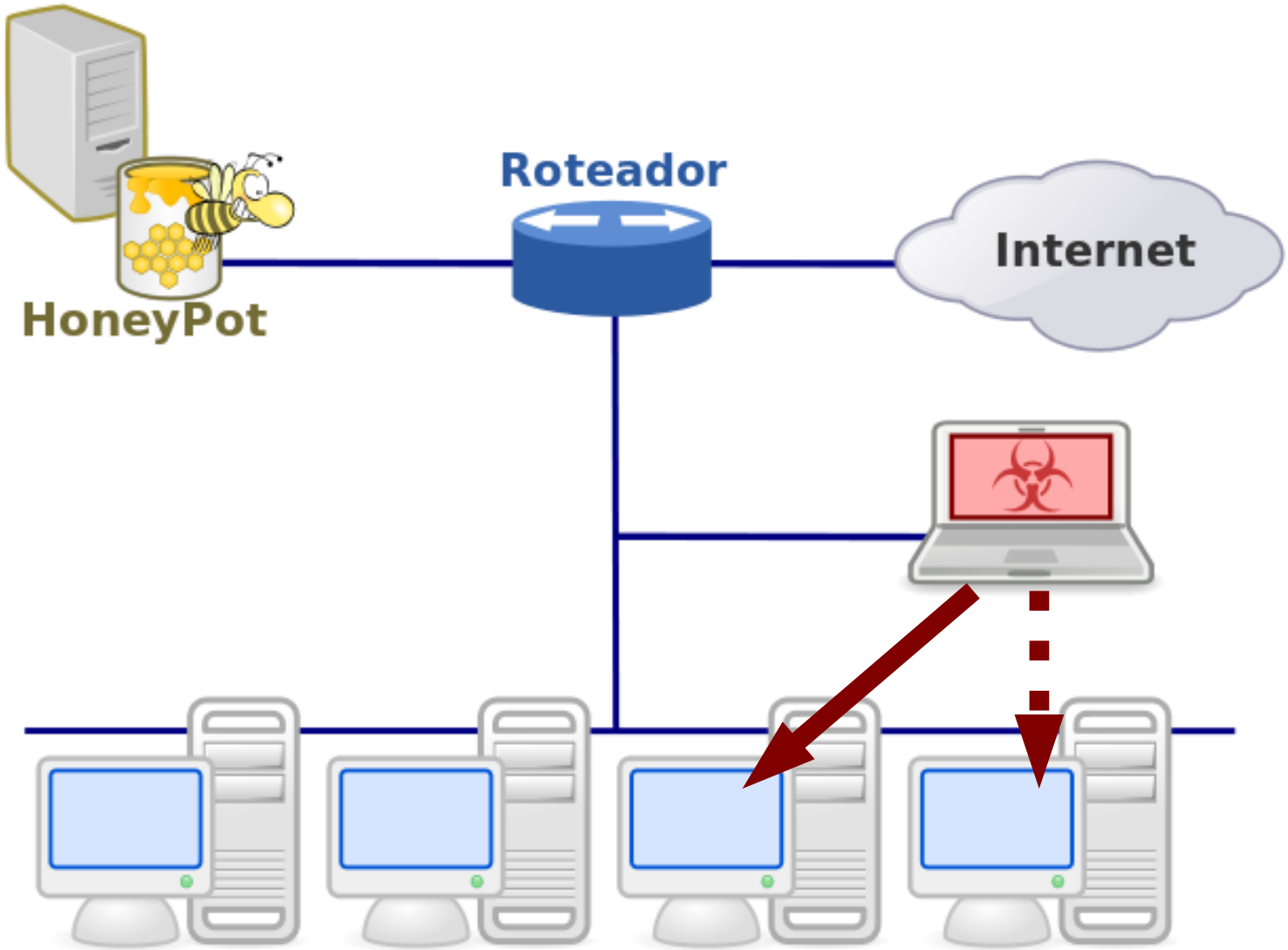
HoneyPot



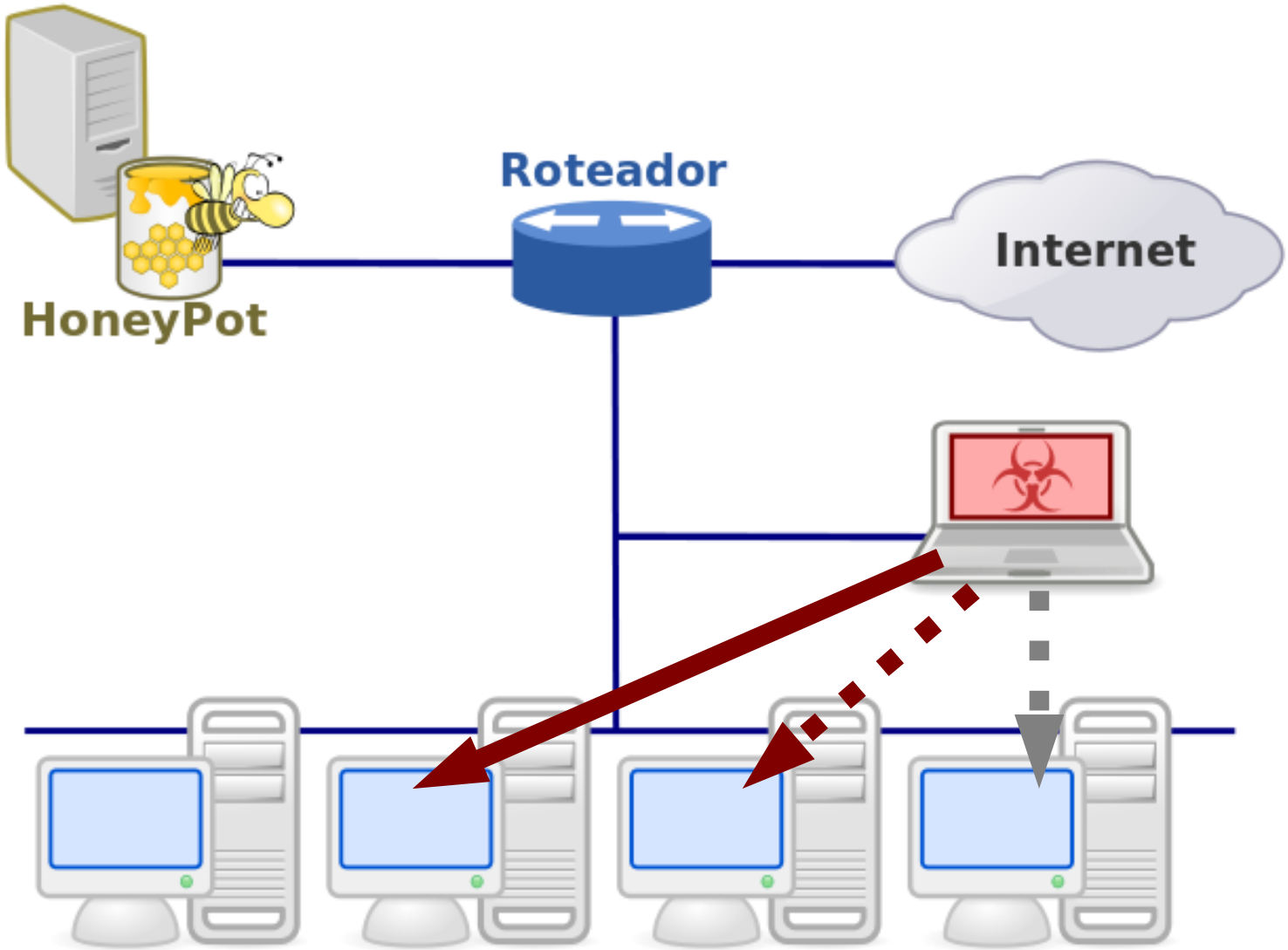
HoneyPot



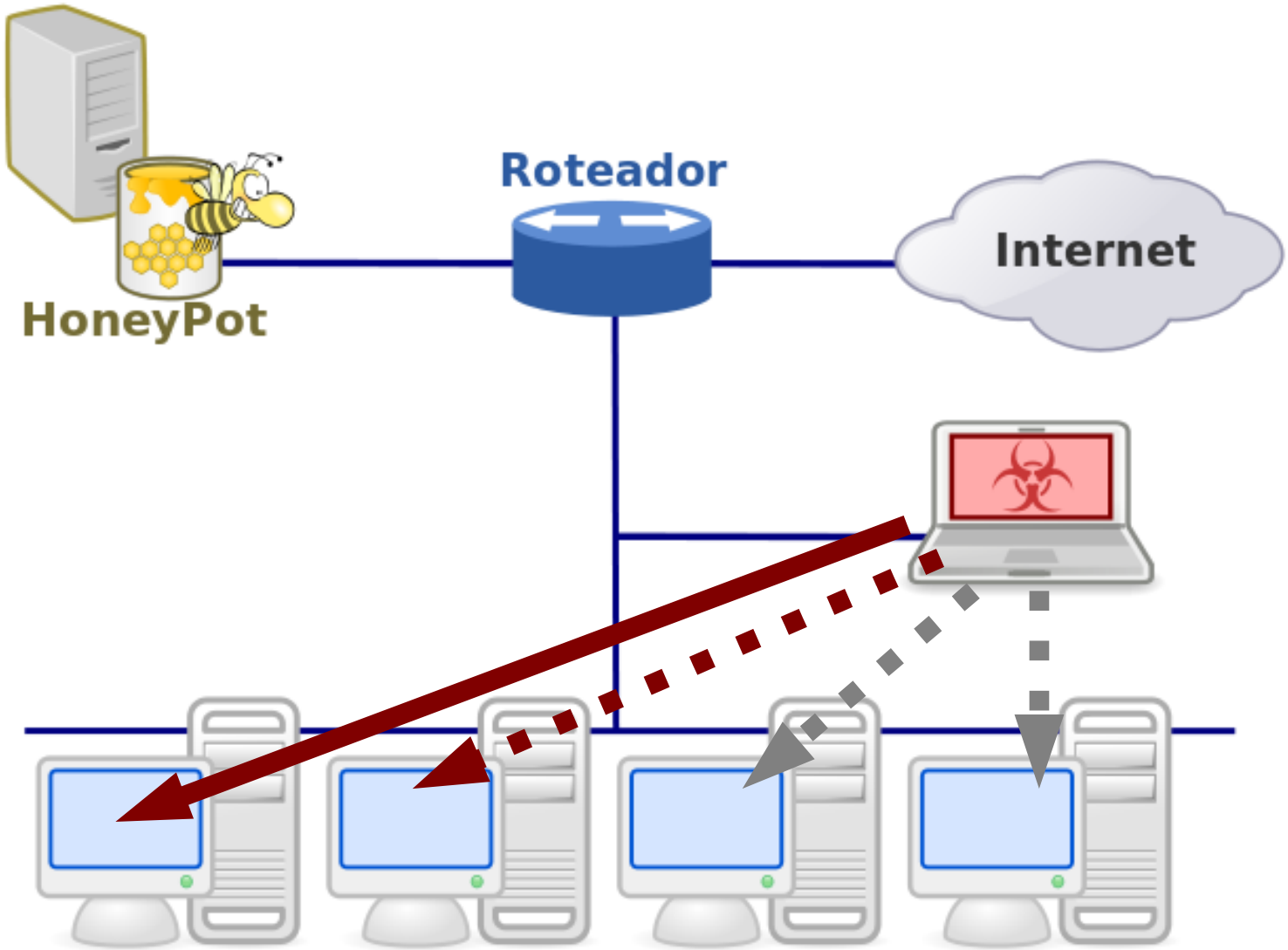
HoneyPot



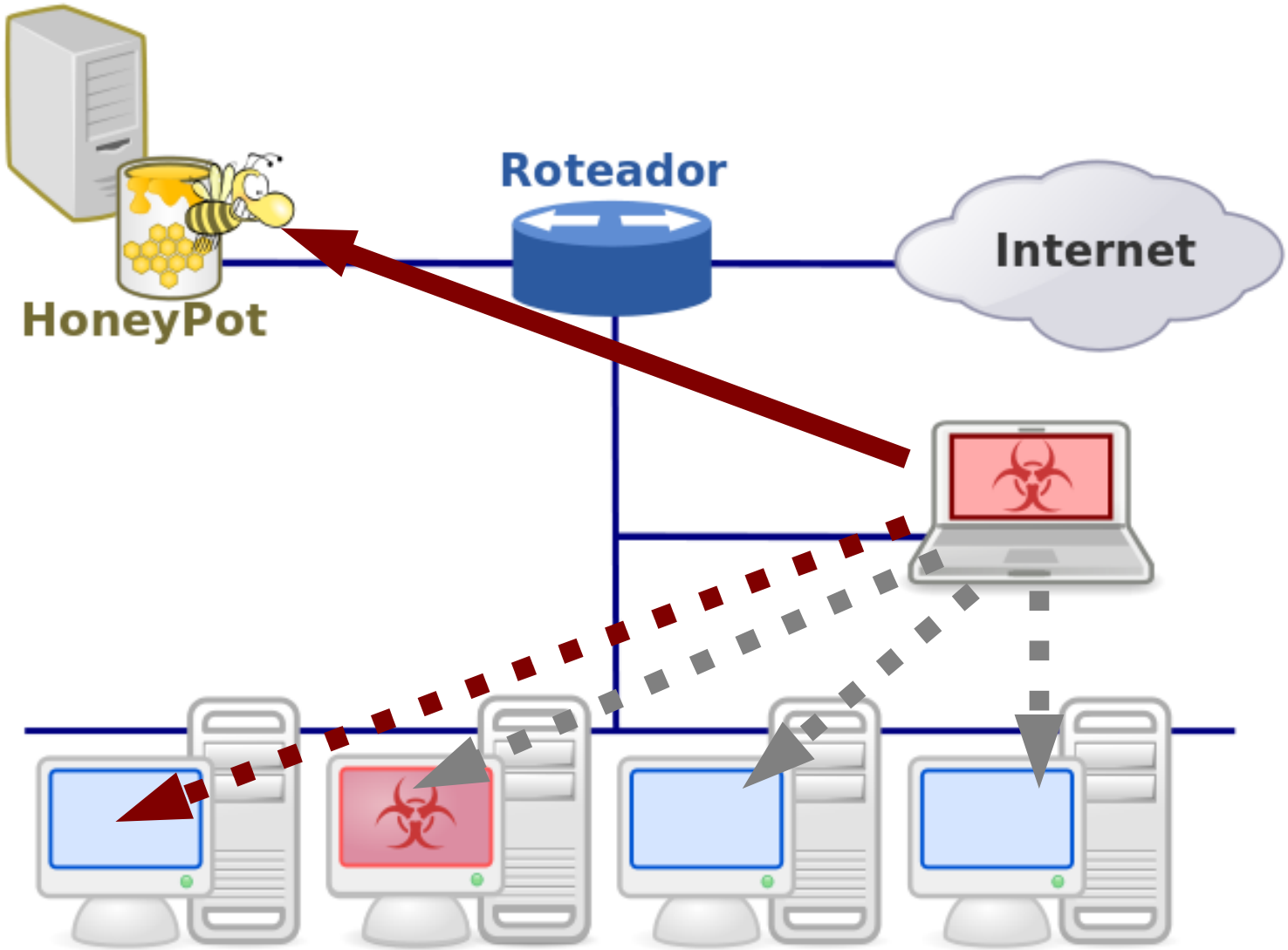
HoneyPot



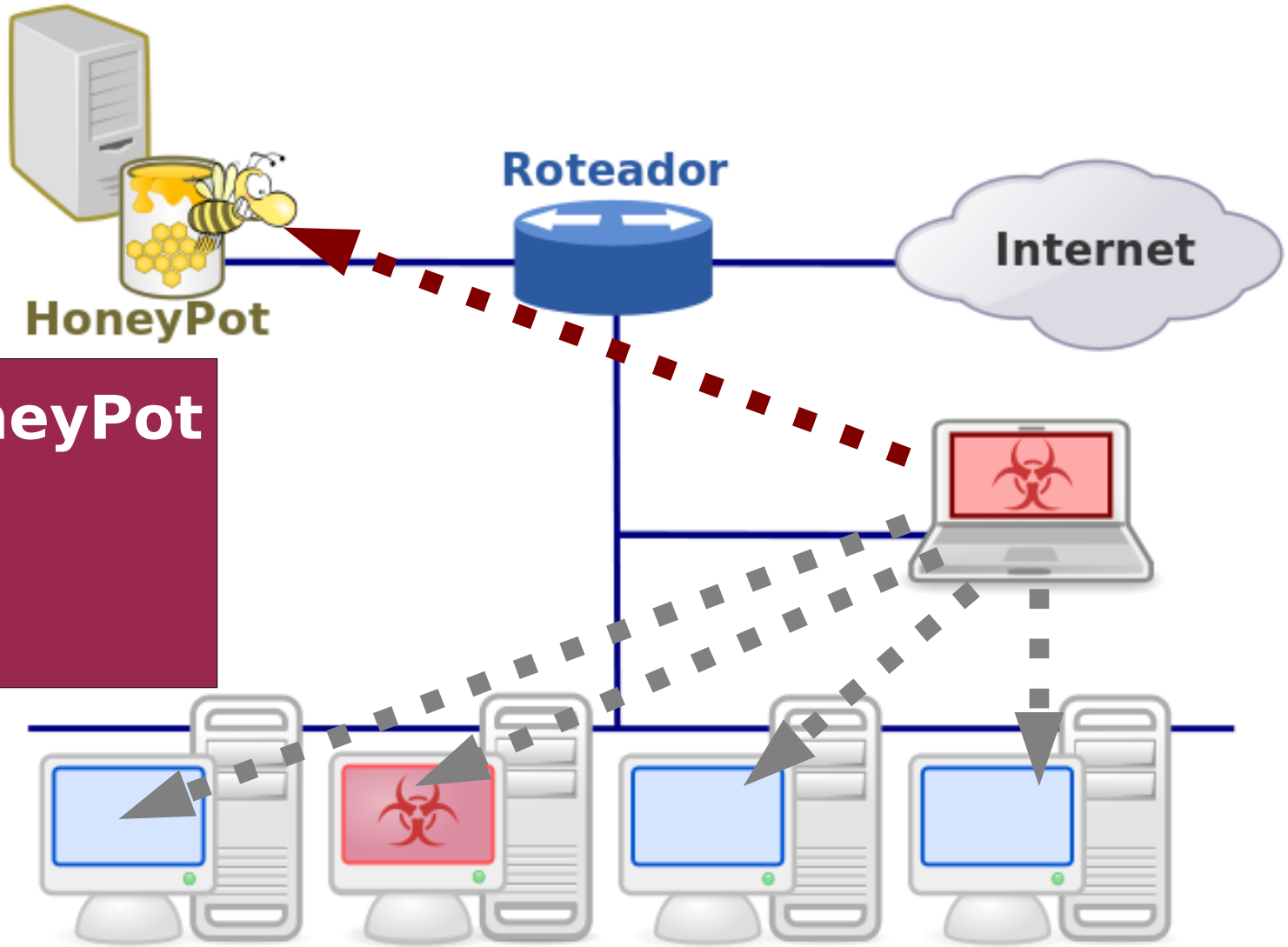
HoneyPot



HoneyPot

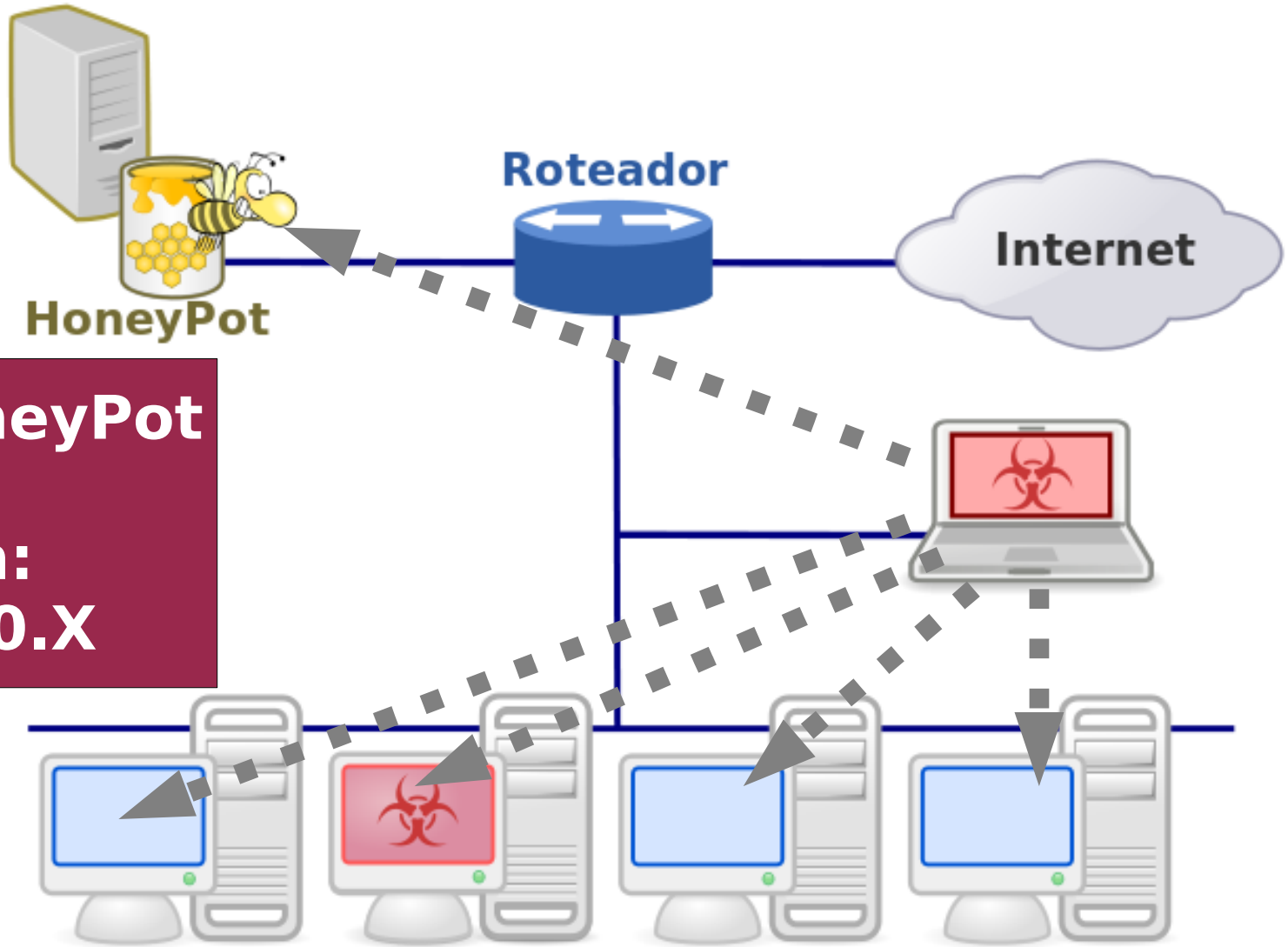


HoneyPot



Alerta do HoneyPot

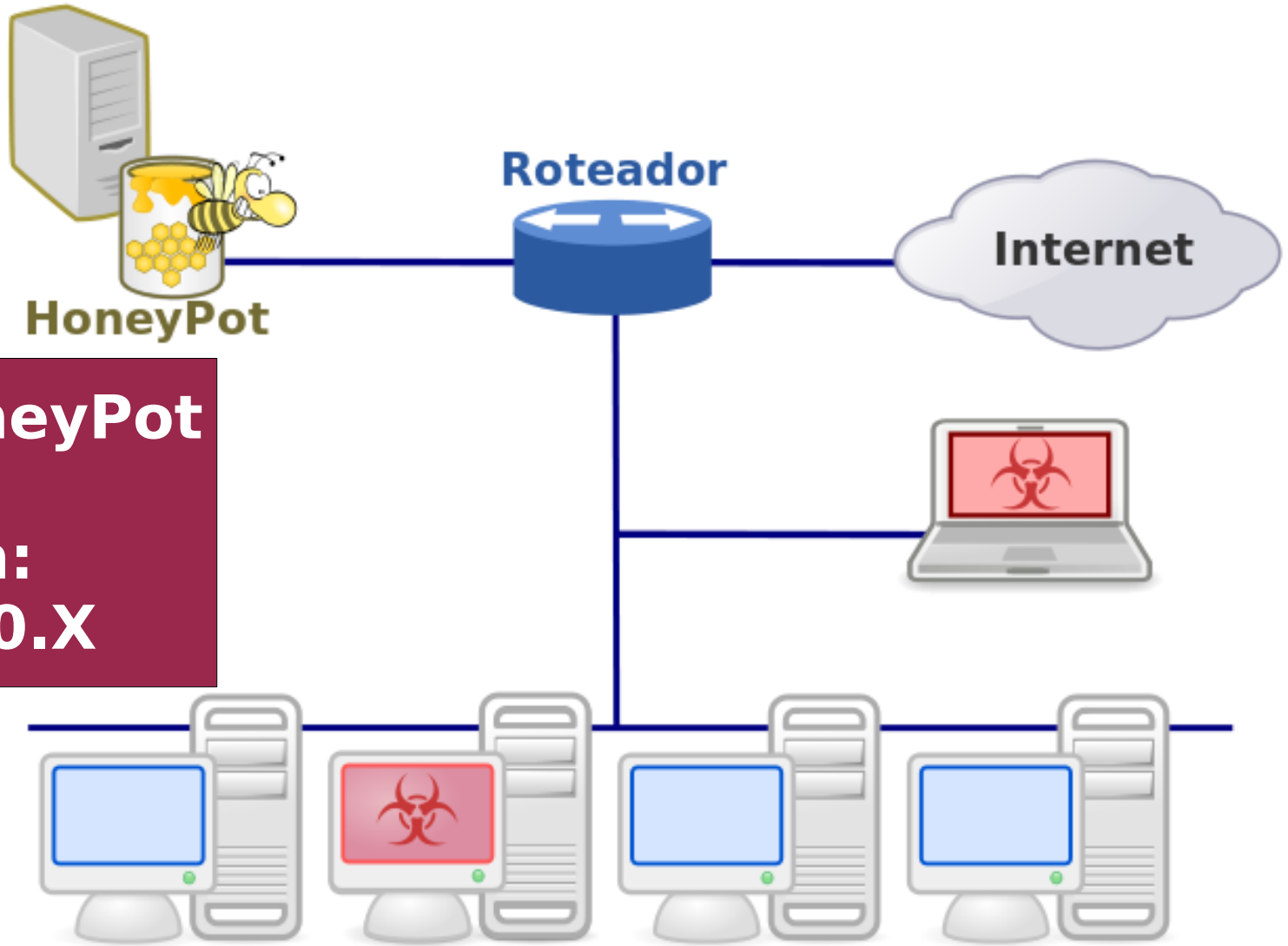
HoneyPot



Alerta do HoneyPot

Vírus em:
192.168.10.X

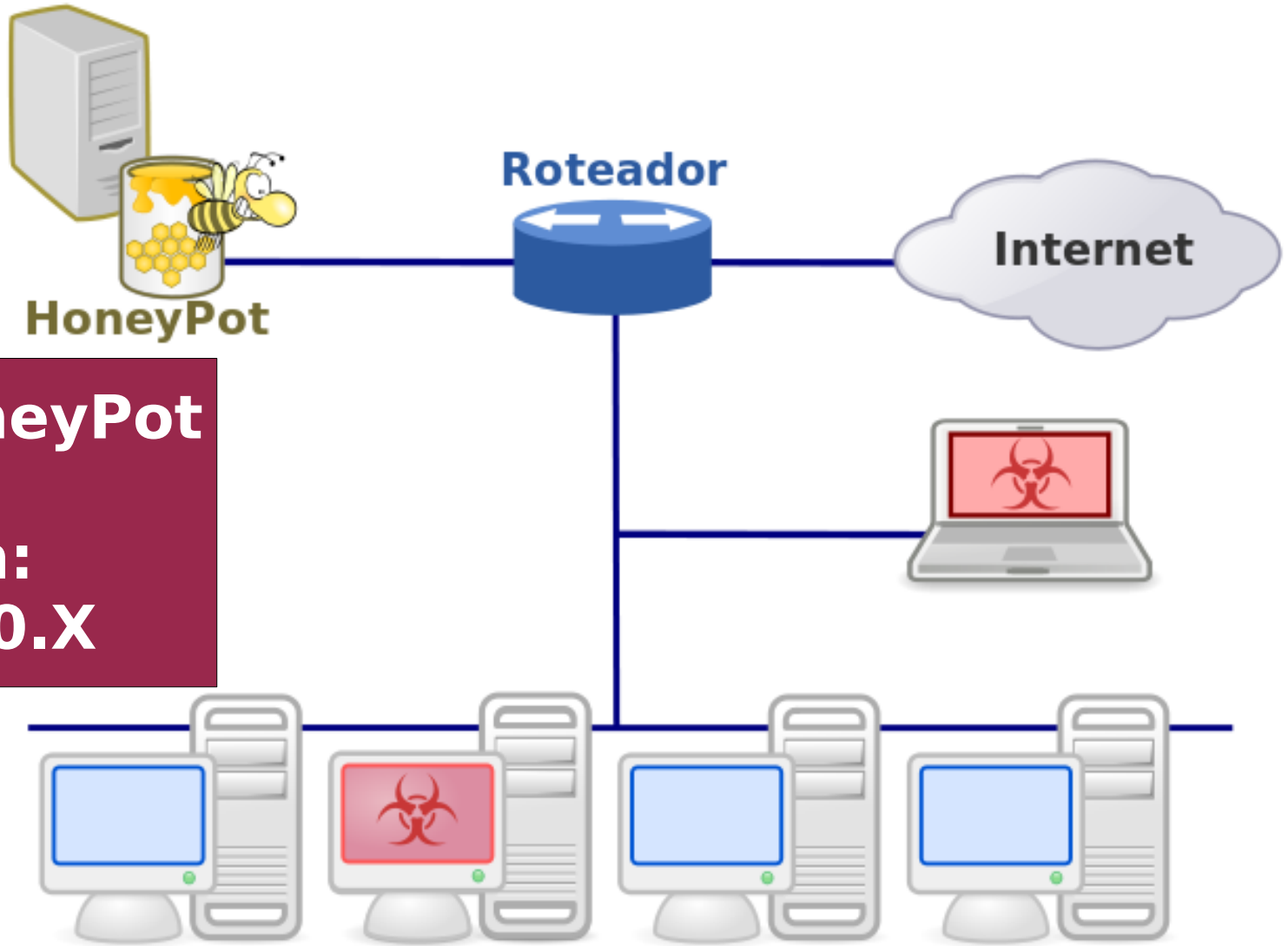
HoneyPot



Alerta do HoneyPot

Vírus em:
192.168.10.X

HoneyPot



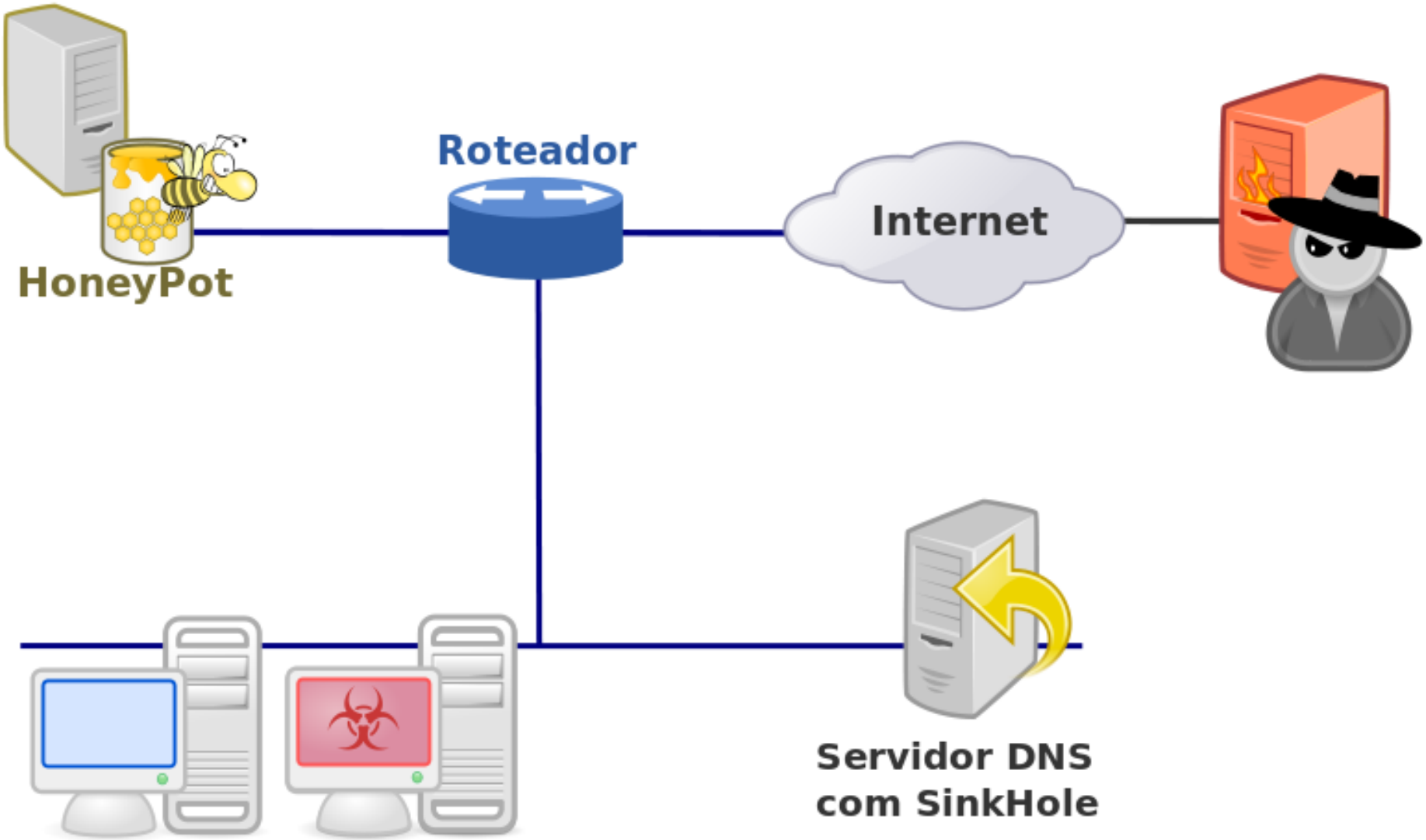
Alerta do HoneyPot

Vírus em:
192.168.10.X

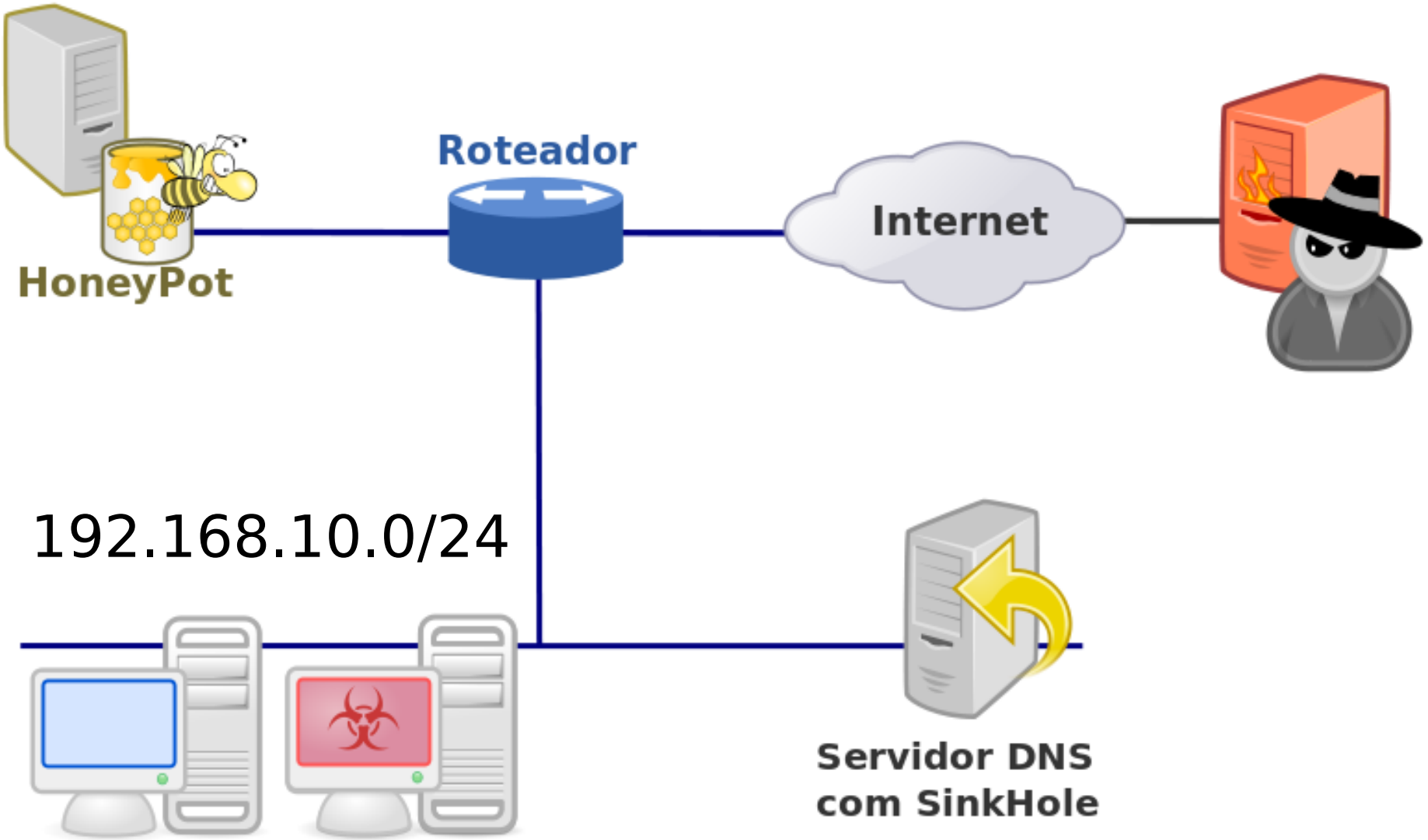
- **DNS SinkHole**

O DNS SinkHole é um recurso adicionado ao servidor de DNS para resolver domínios que são utilizados para fins maliciosos (vírus). Assim o domínio malicioso poderá ser resolvido para um endereço IP de um HoneyPot.

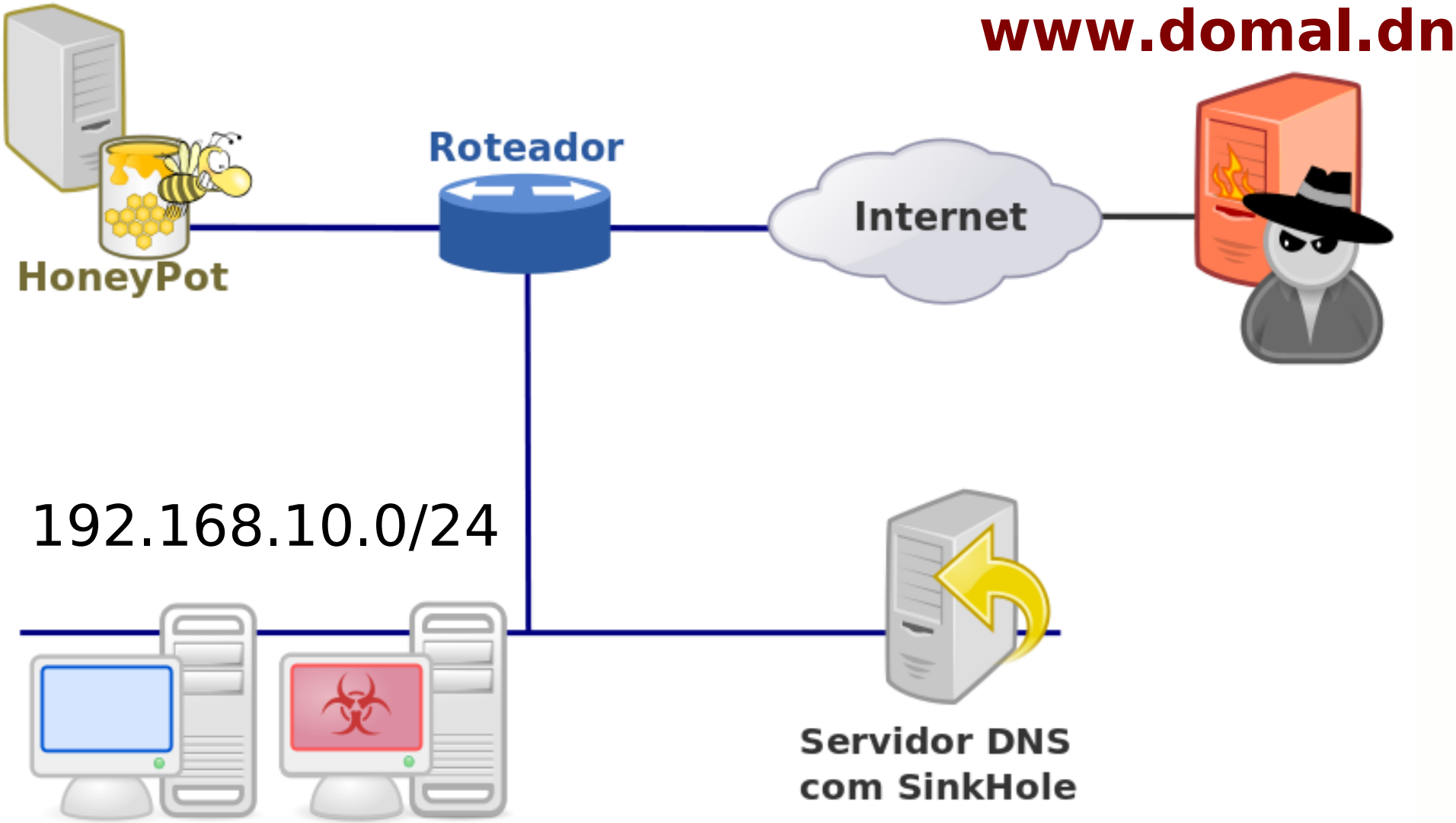
DNS SinkHole



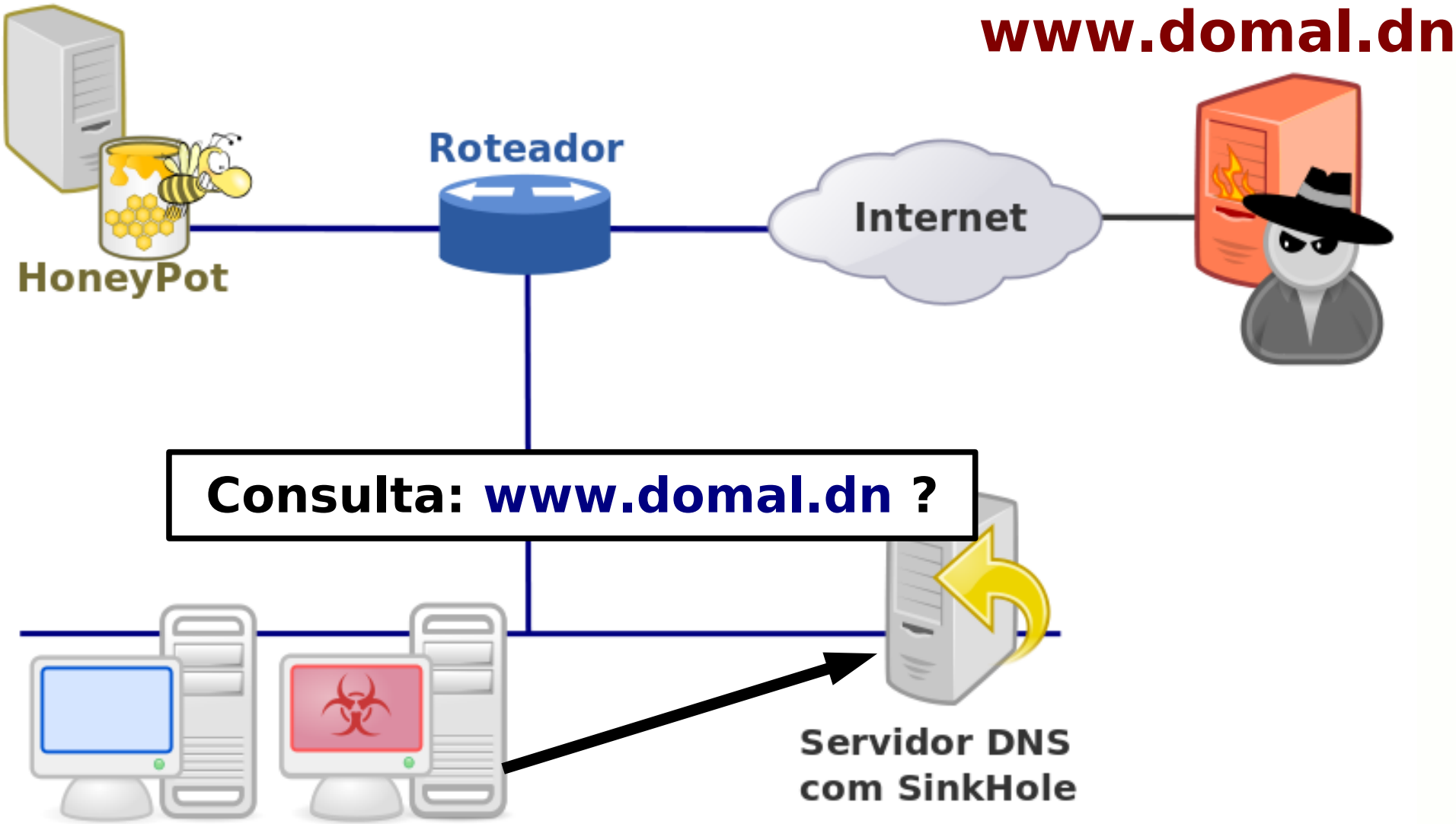
DNS SinkHole



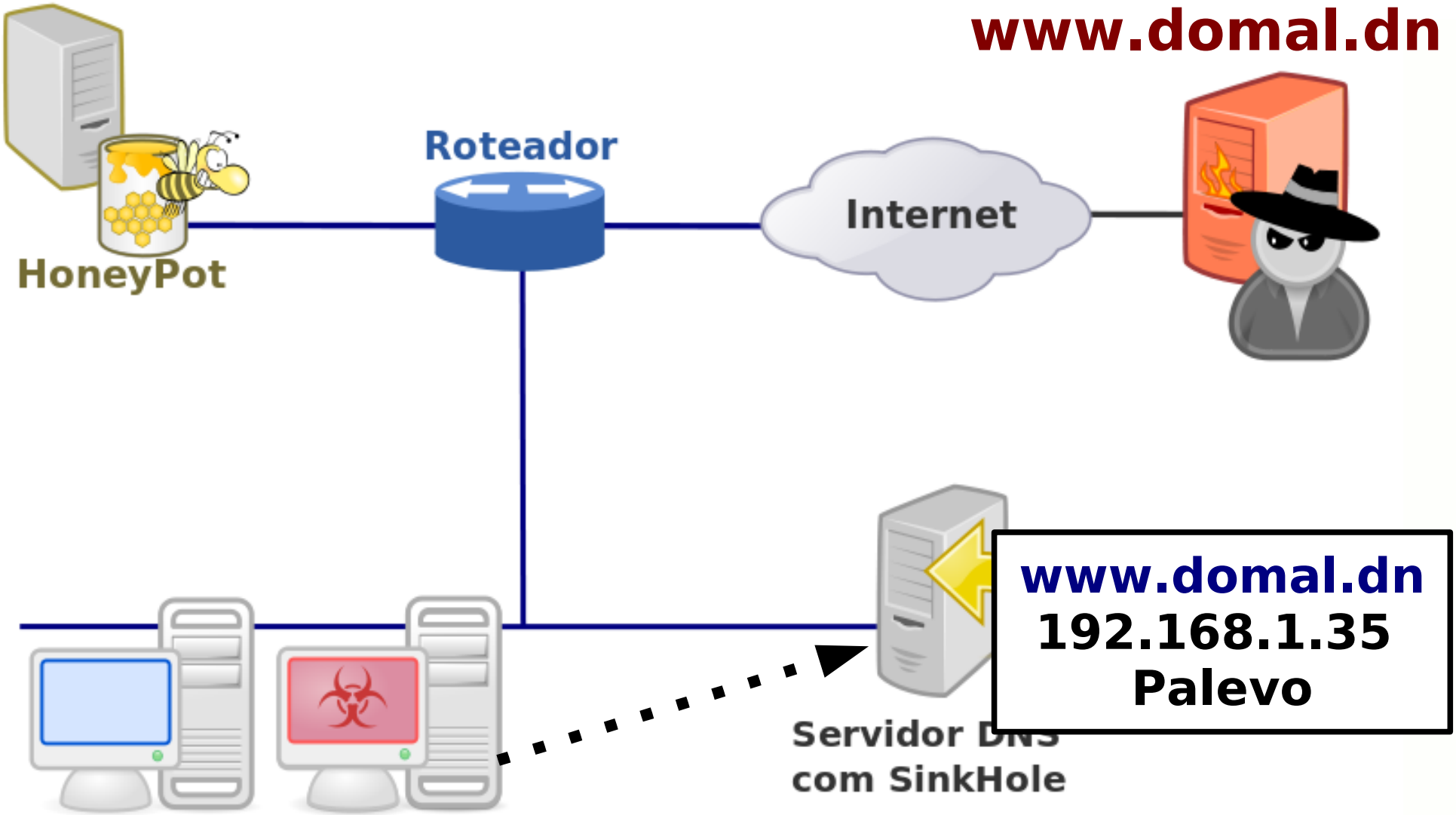
DNS SinkHole



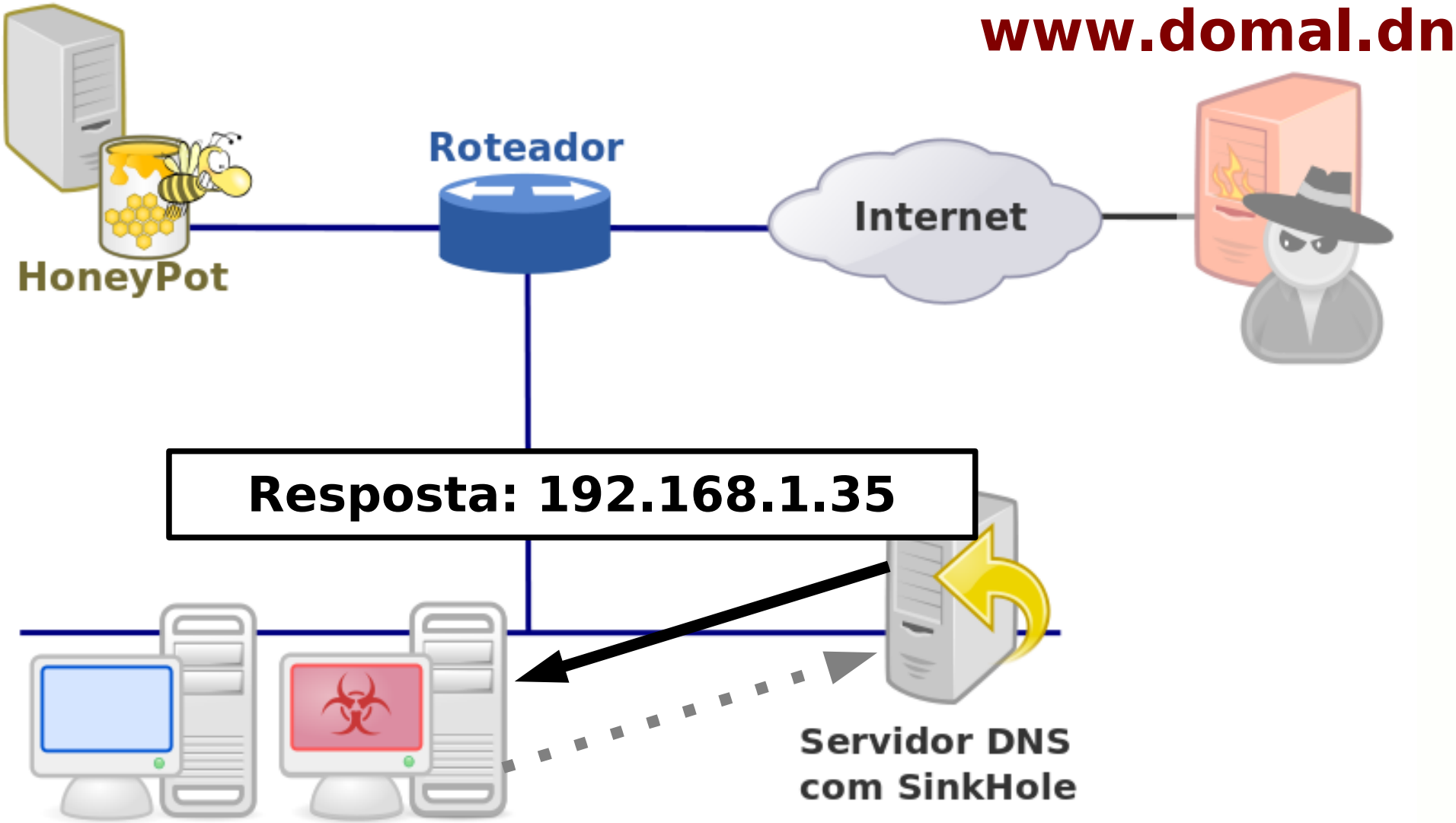
DNS SinkHole



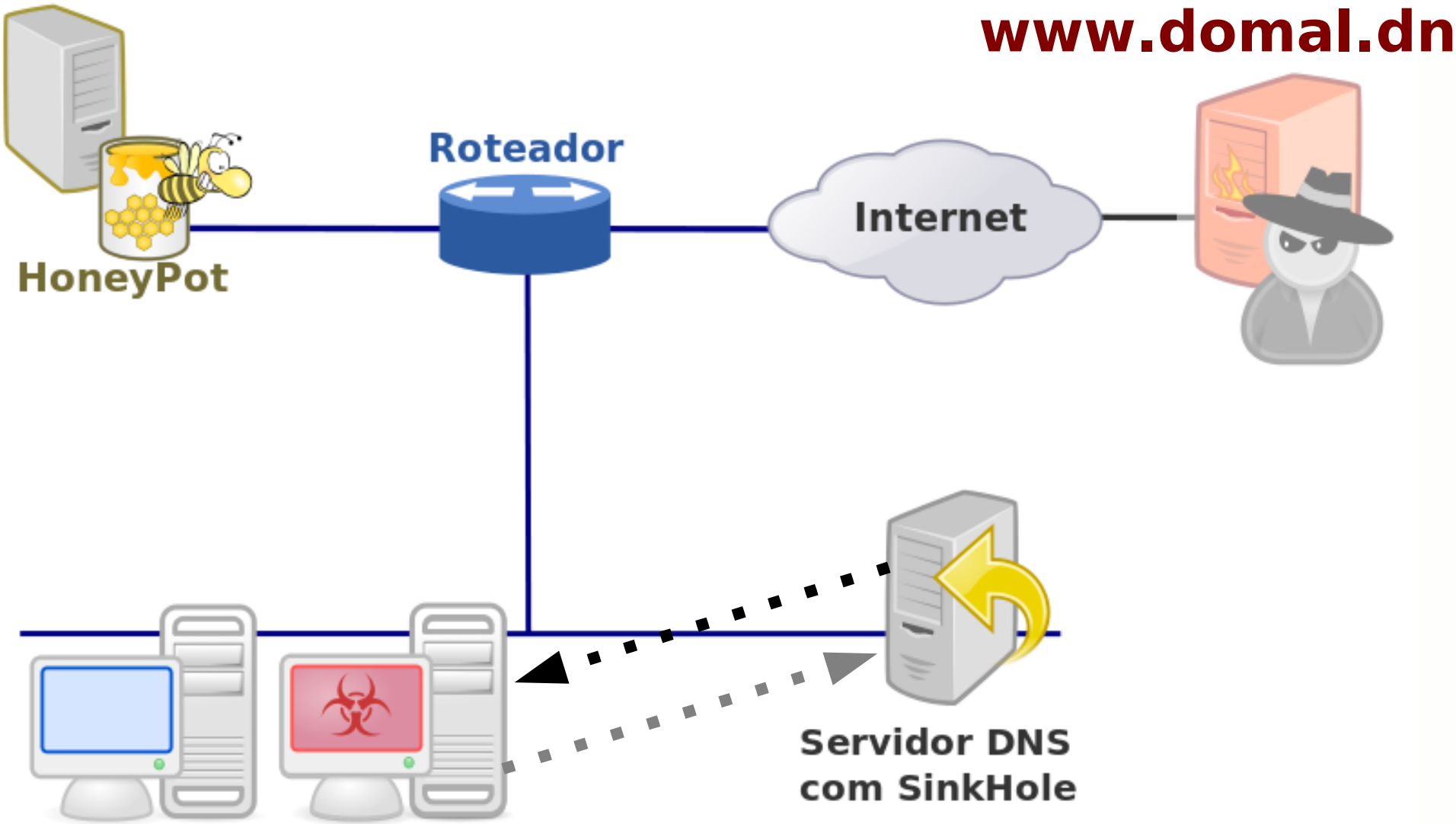
DNS SinkHole



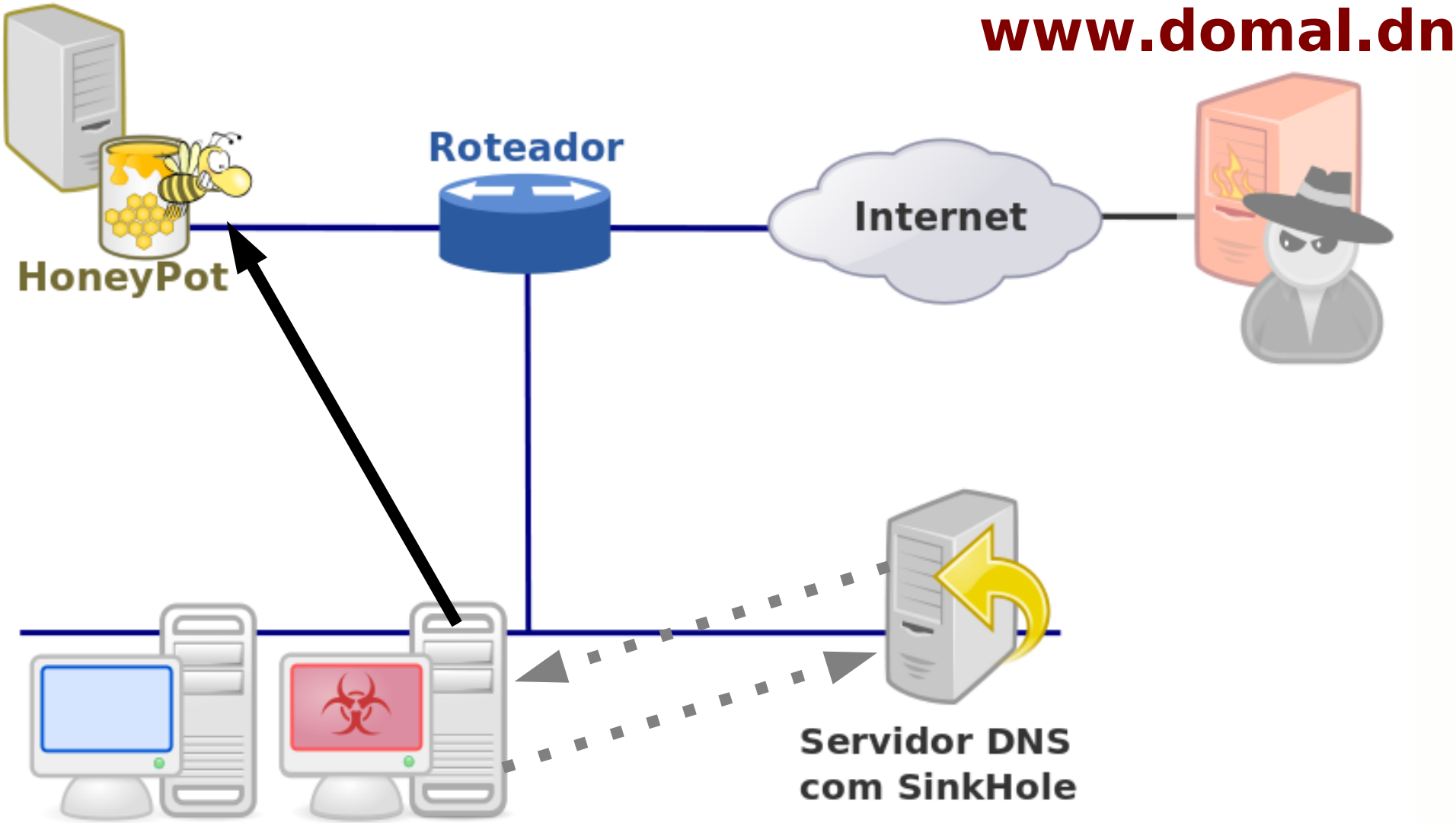
DNS SinkHole



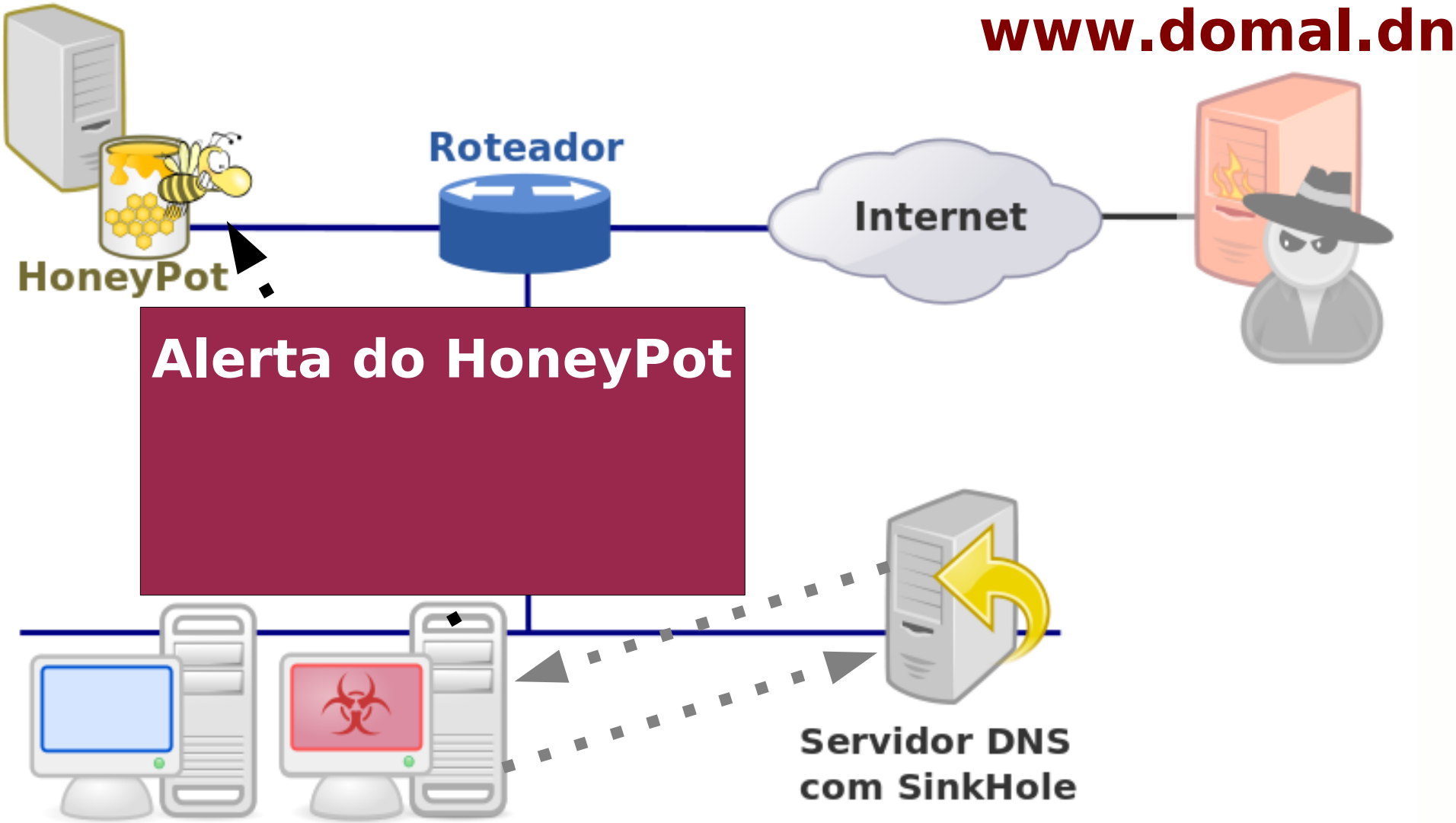
DNS SinkHole



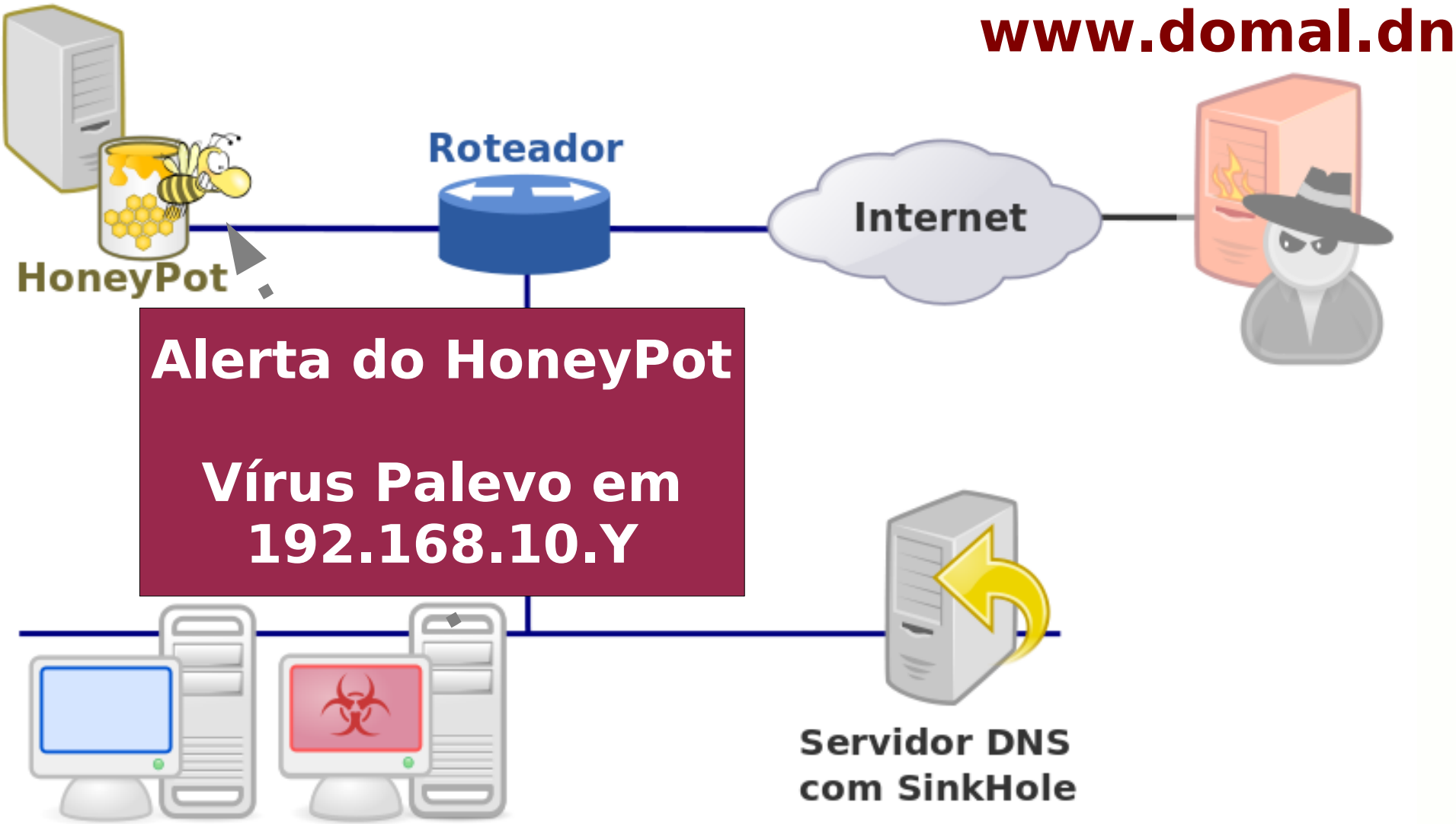
DNS SinkHole



DNS SinkHole



DNS SinkHole

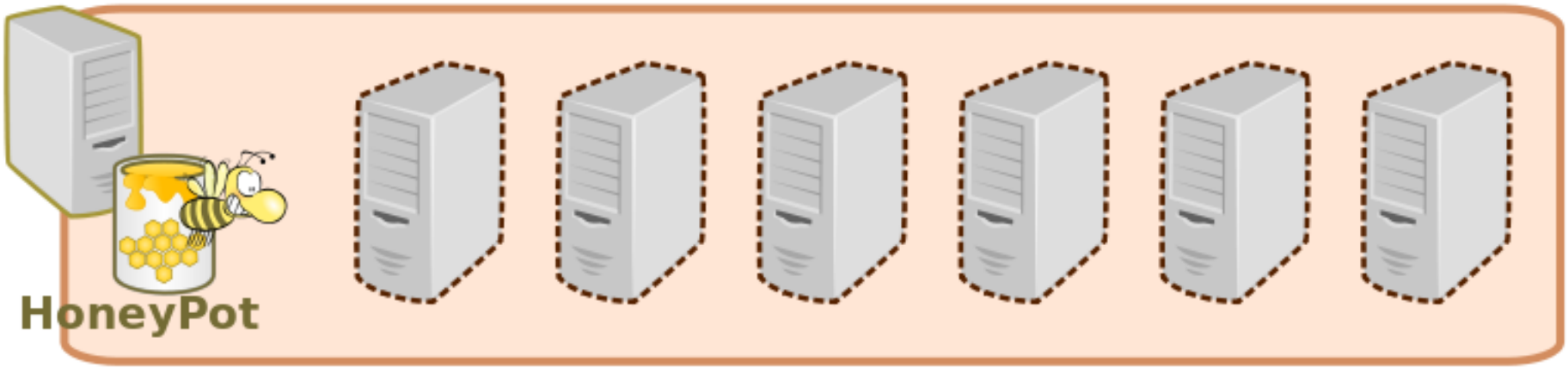


- **HoneyNet**

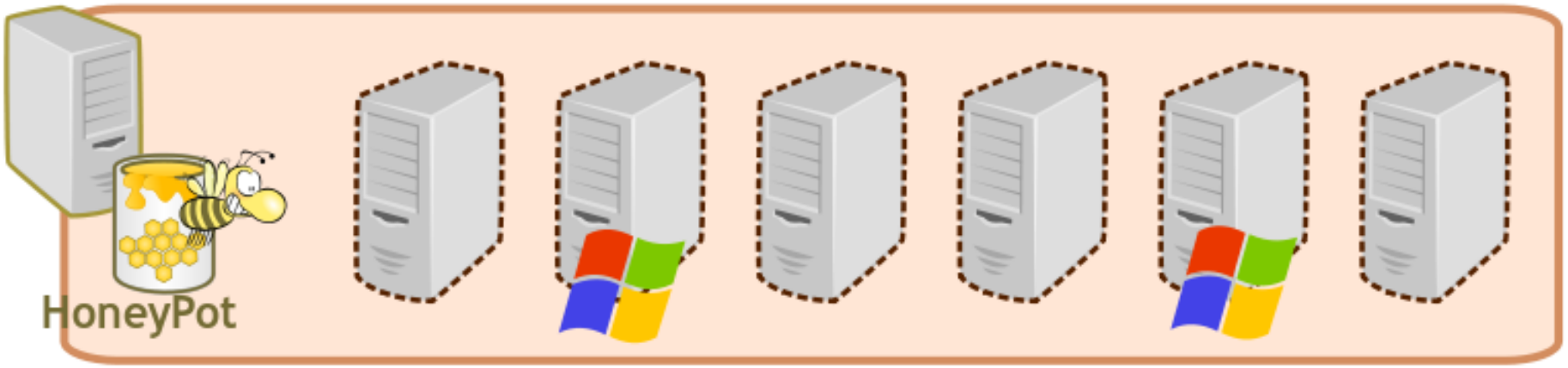
  Uma HoneyNet é uma ferramenta de pesquisa, que consiste de uma rede projetada especificamente para ser comprometida, e que contém mecanismos de controle para previnir que seja utilizada como base de ataques contra outras redes.

HoneyNet

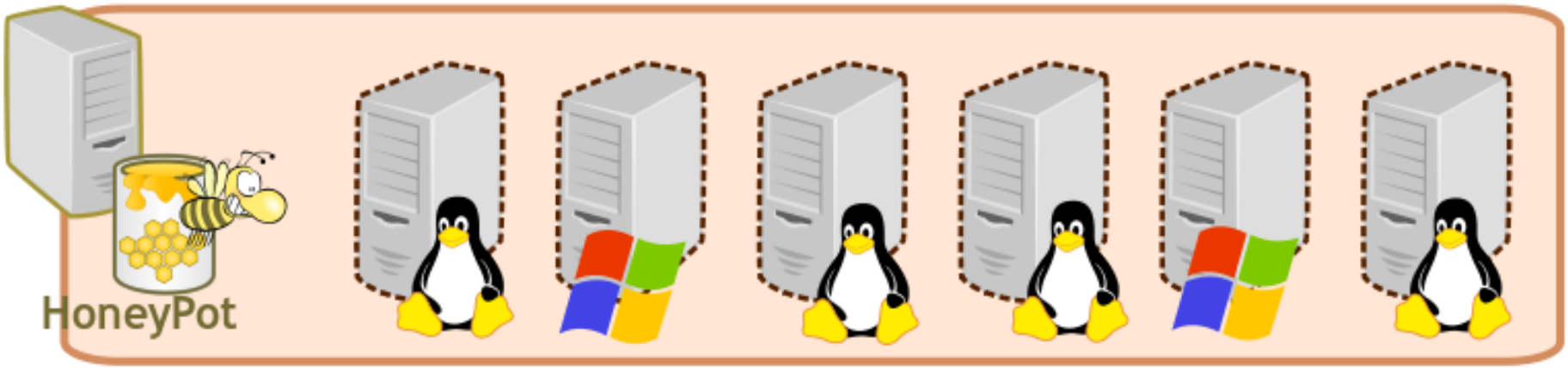
HoneyNet



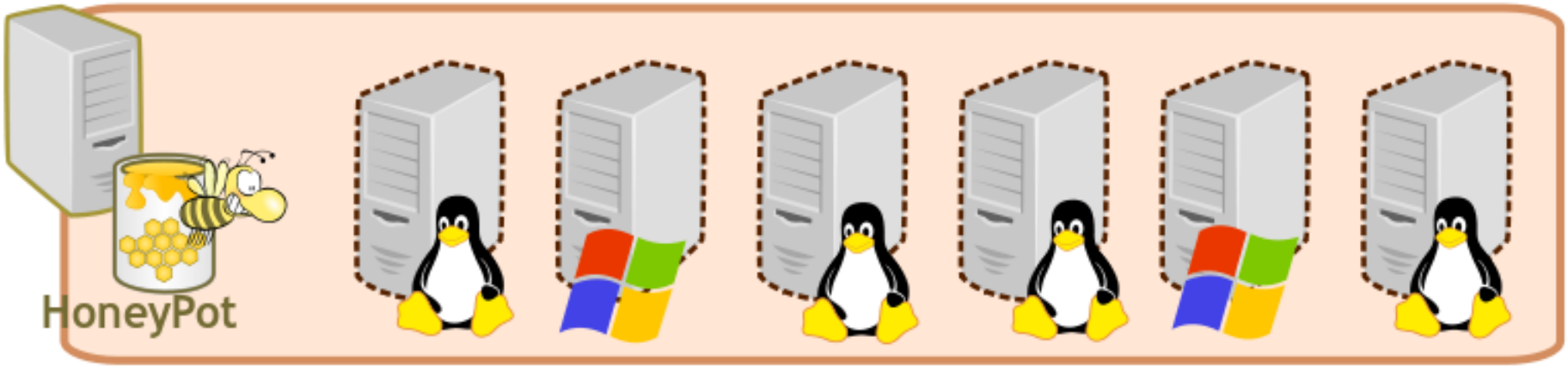
HoneyNet



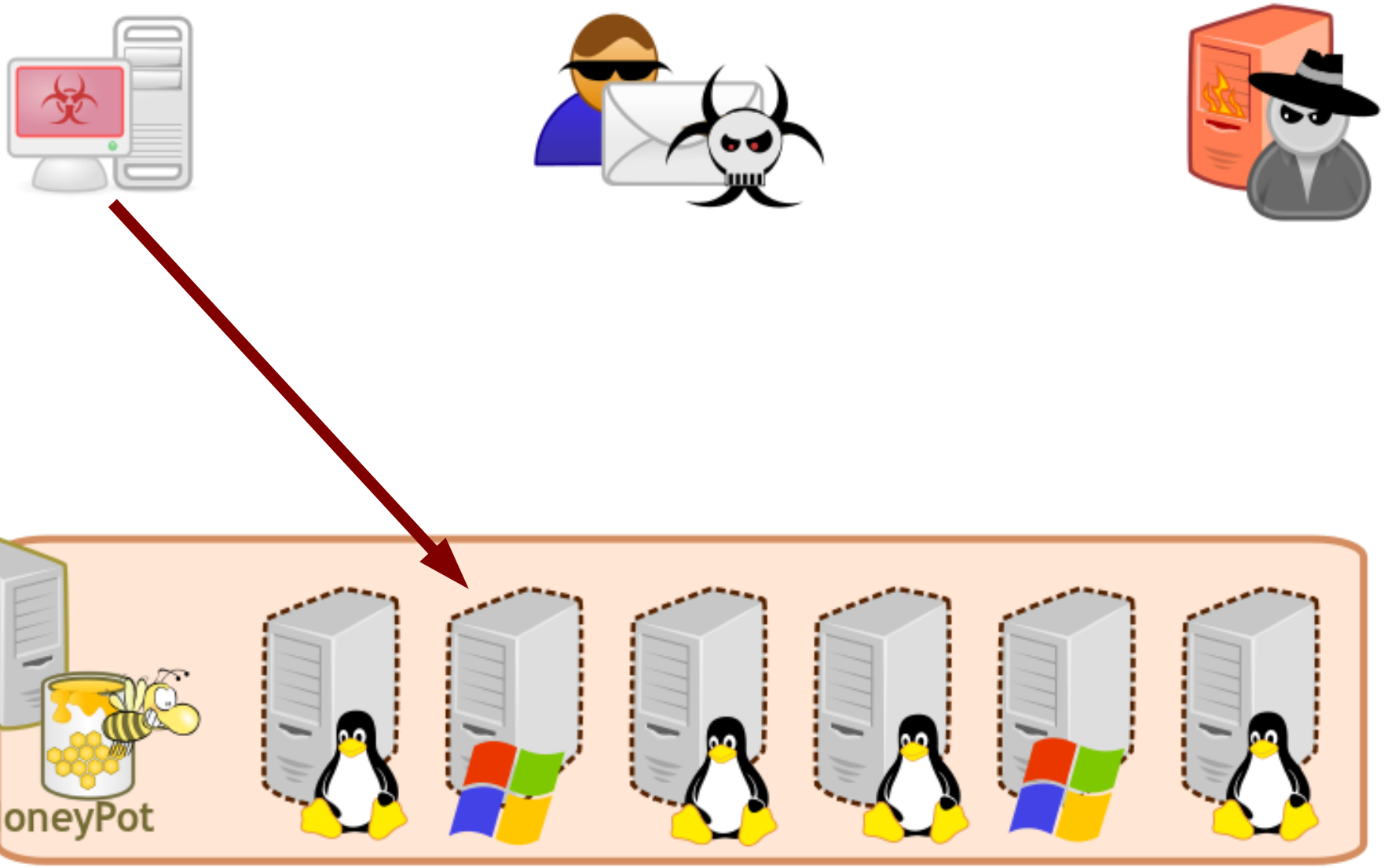
HoneyNet



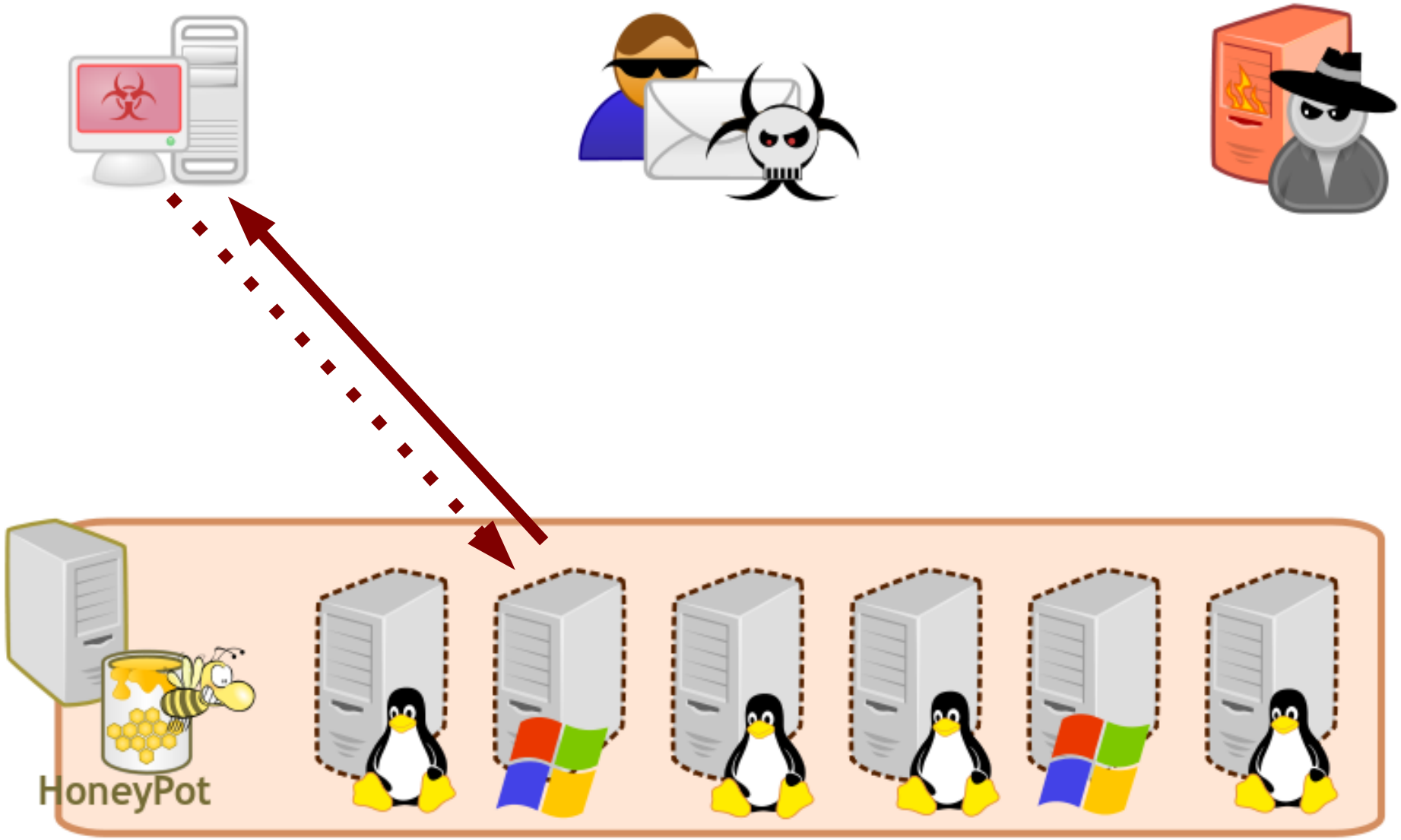
HoneyNet



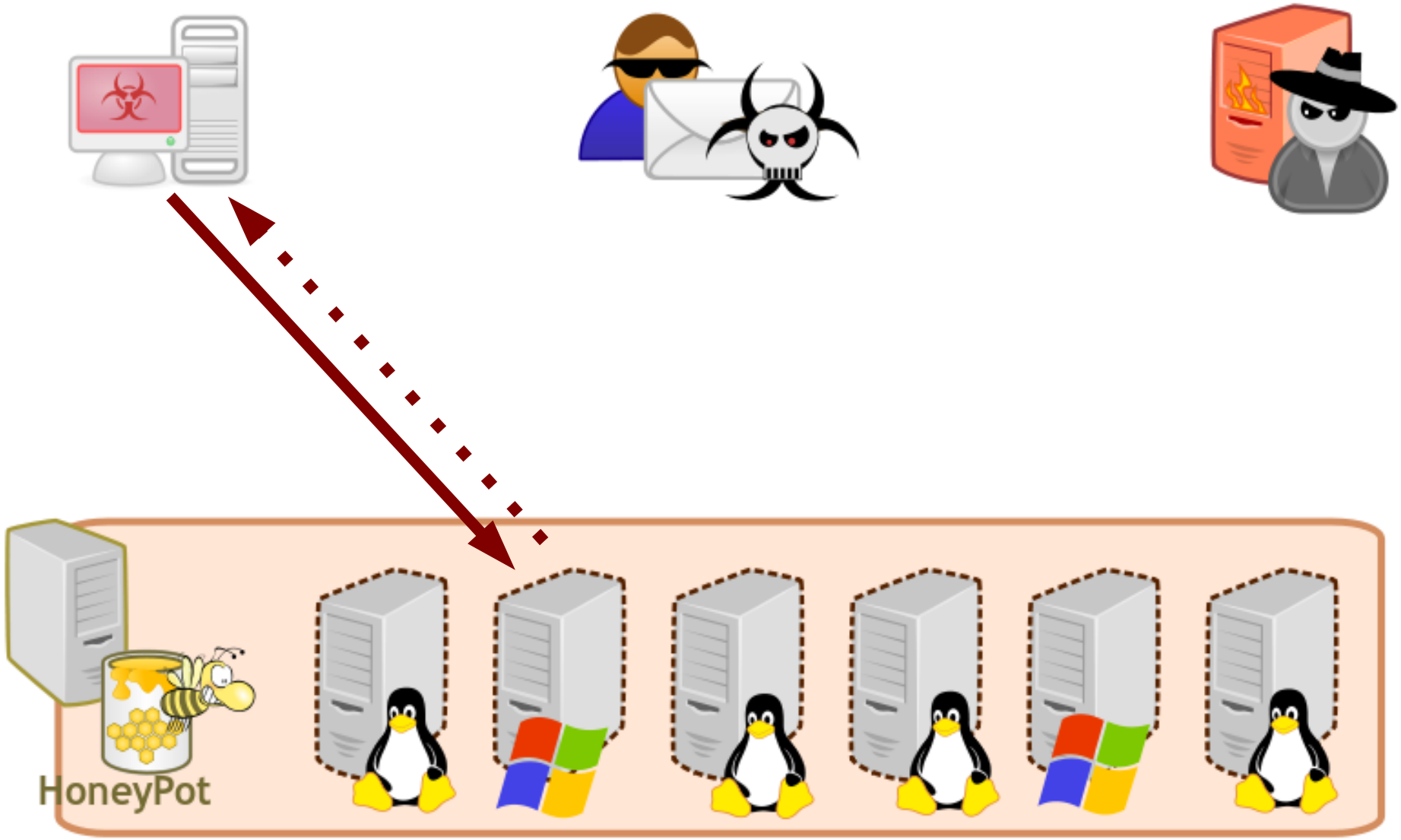
HoneyNet



HoneyNet



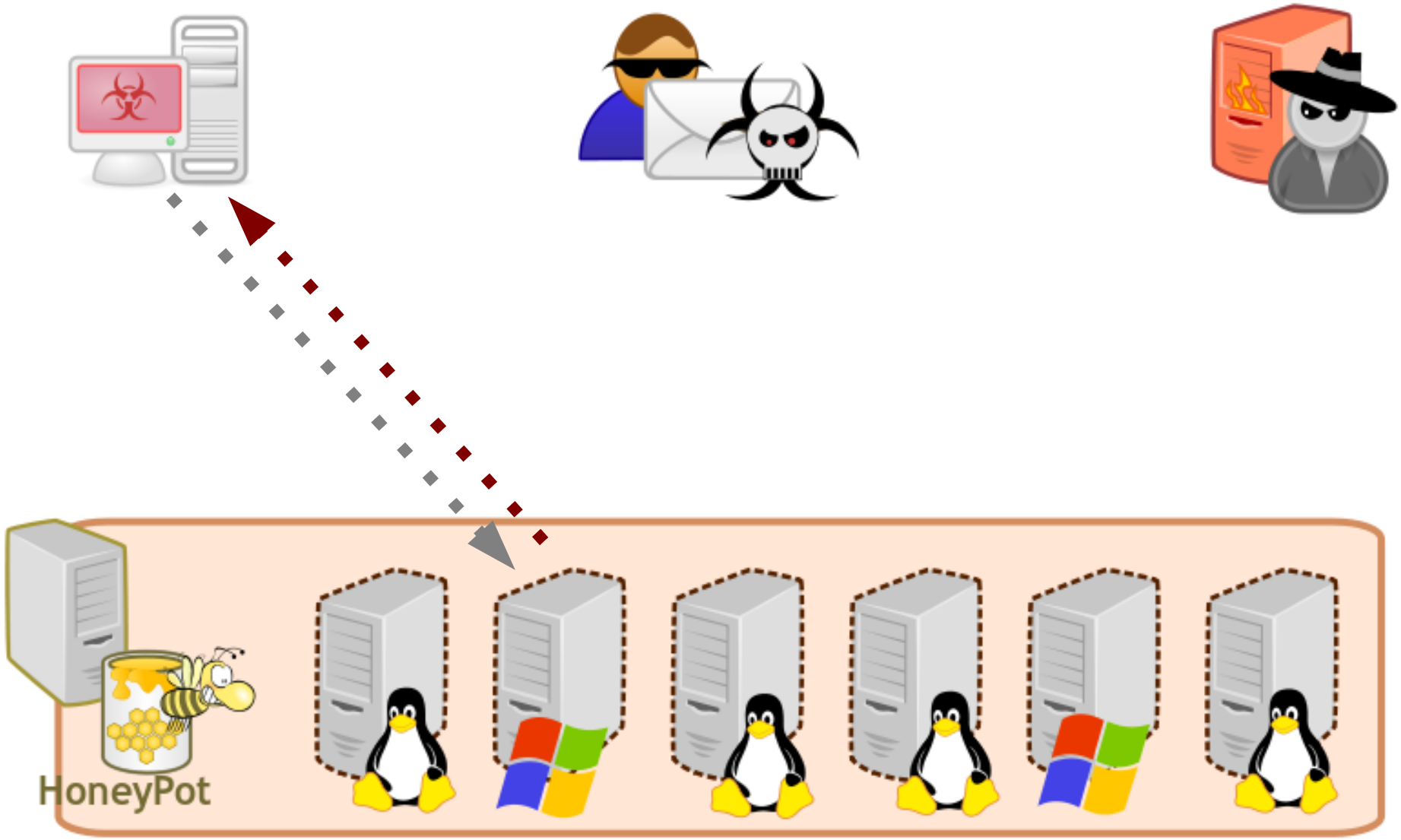
HoneyNet



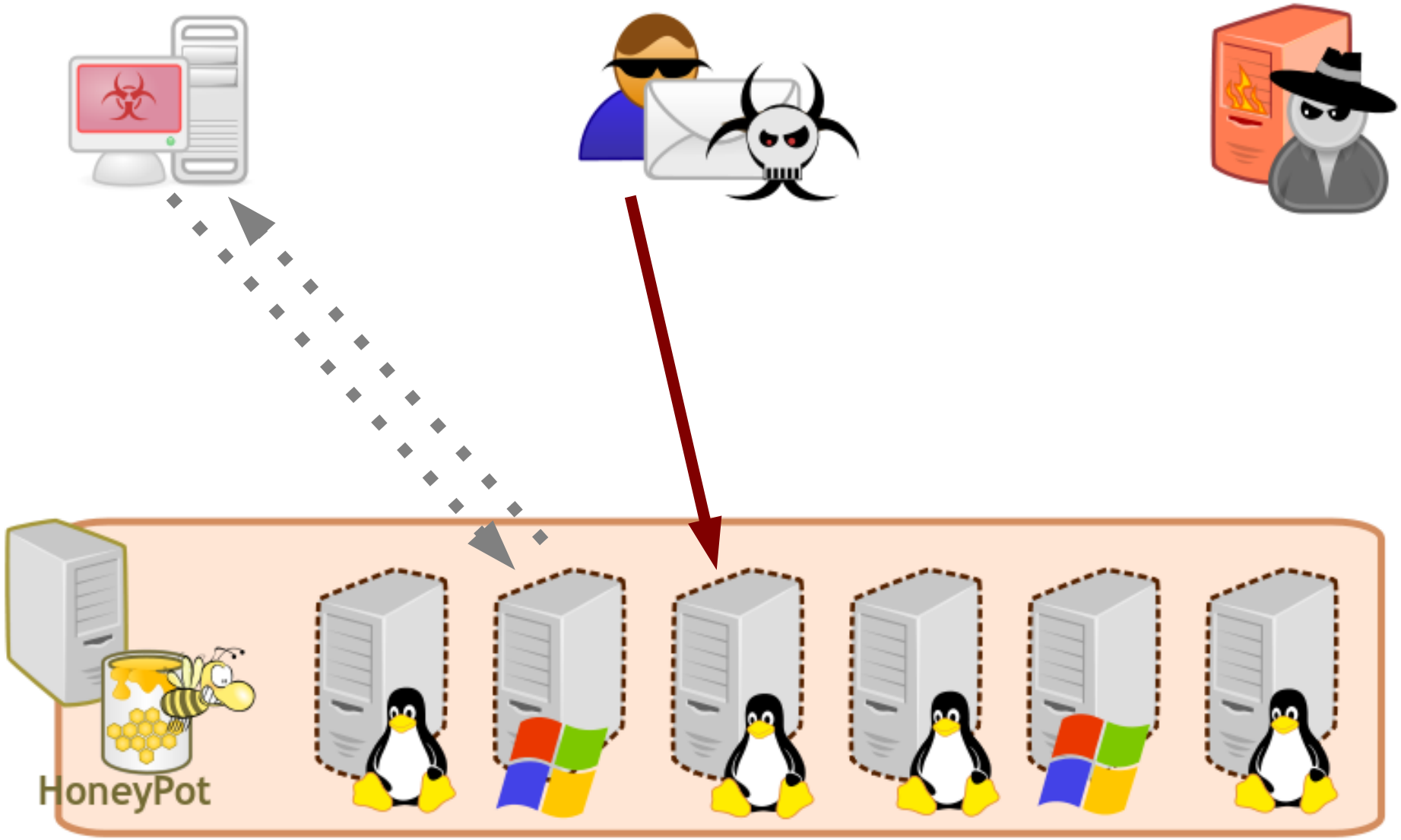
HoneyNet

HoneyNet

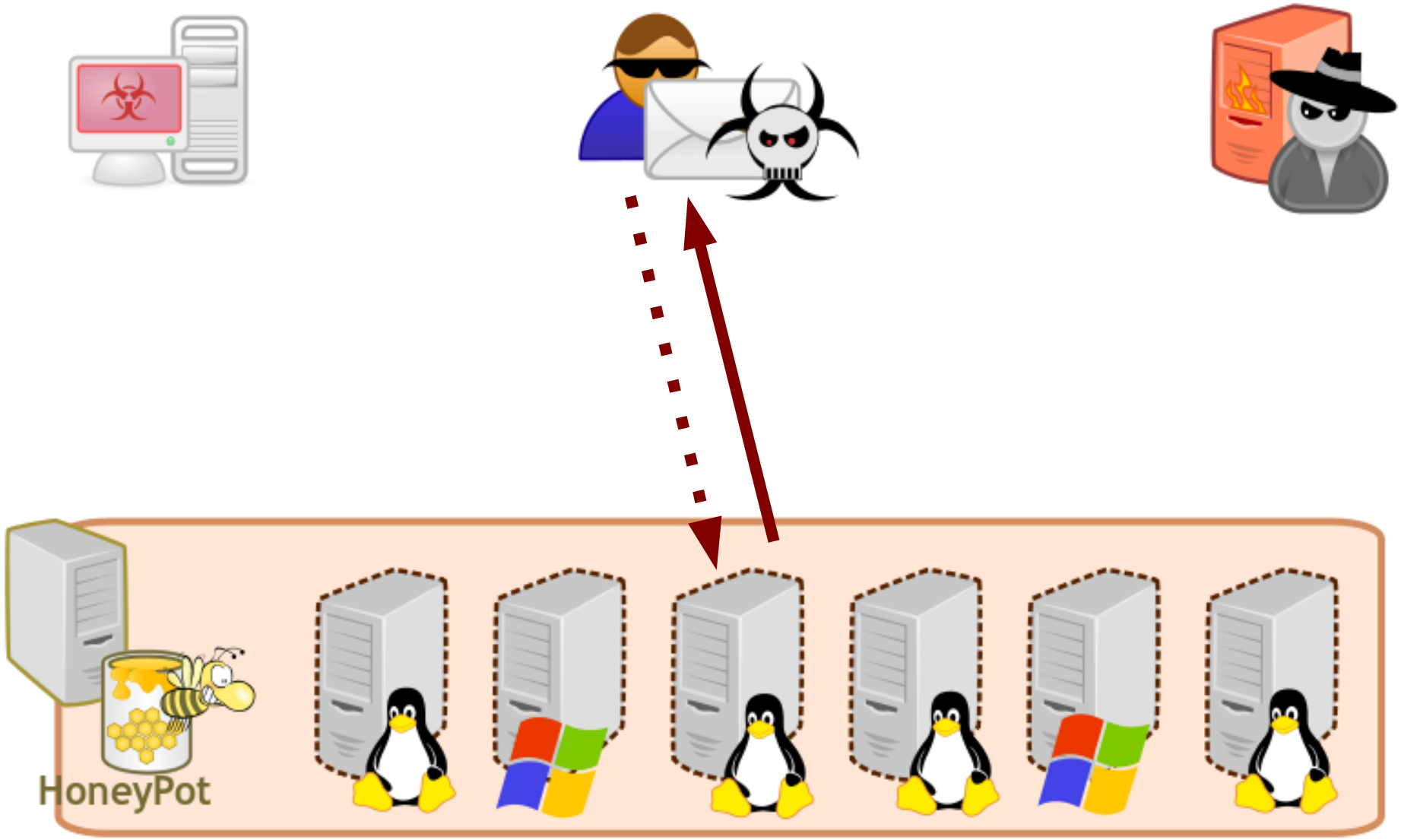
HoneyNet



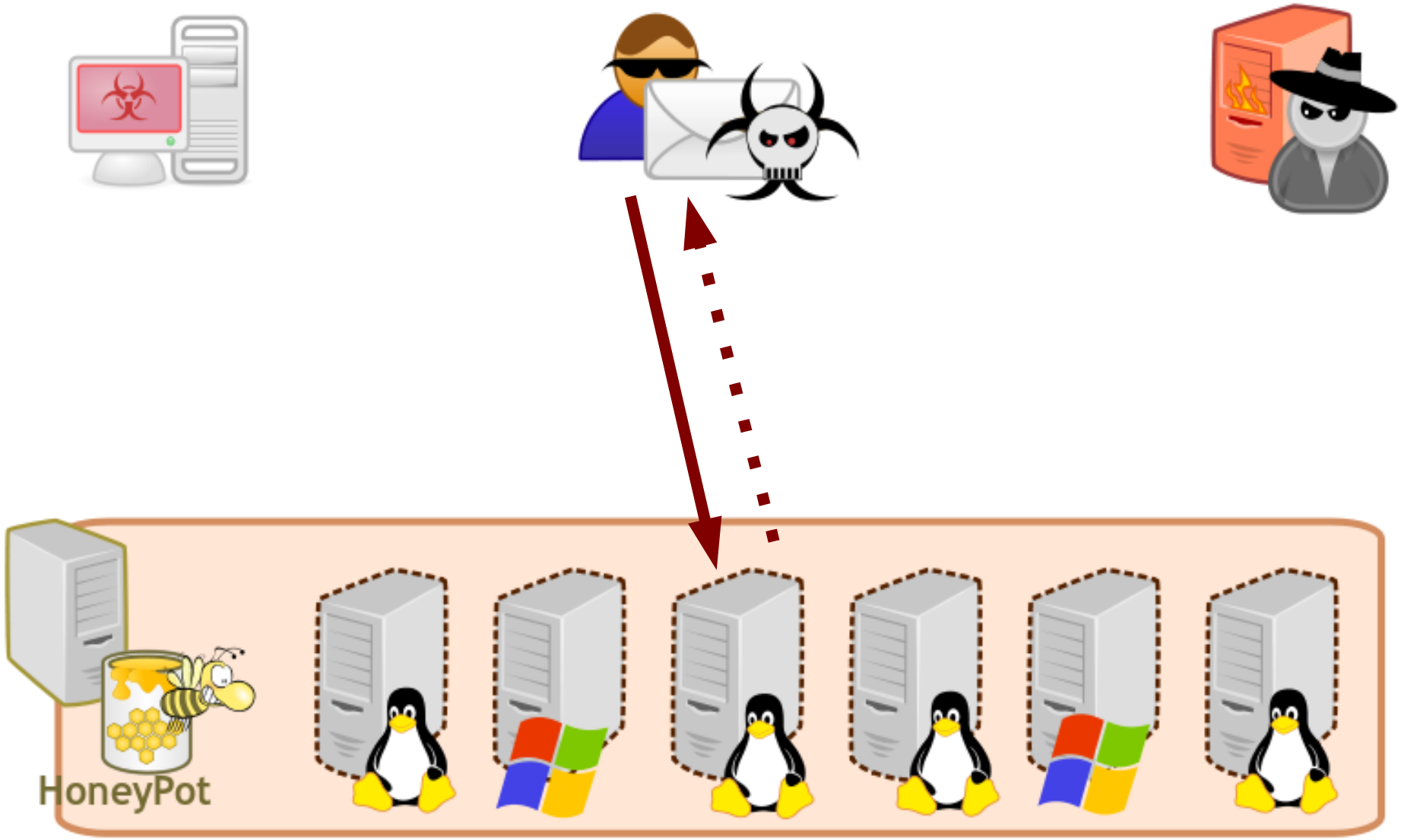
HoneyNet



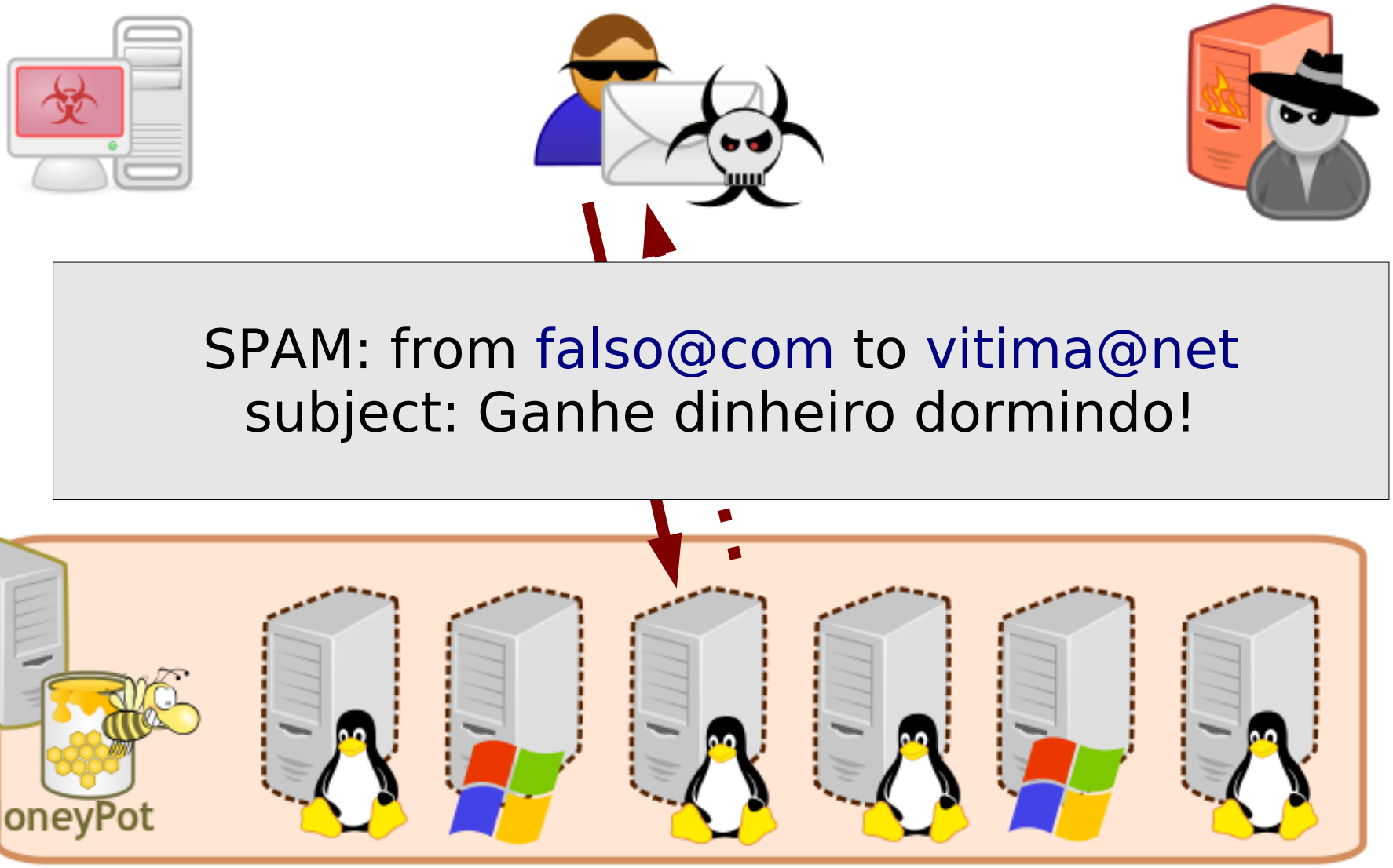
HoneyNet



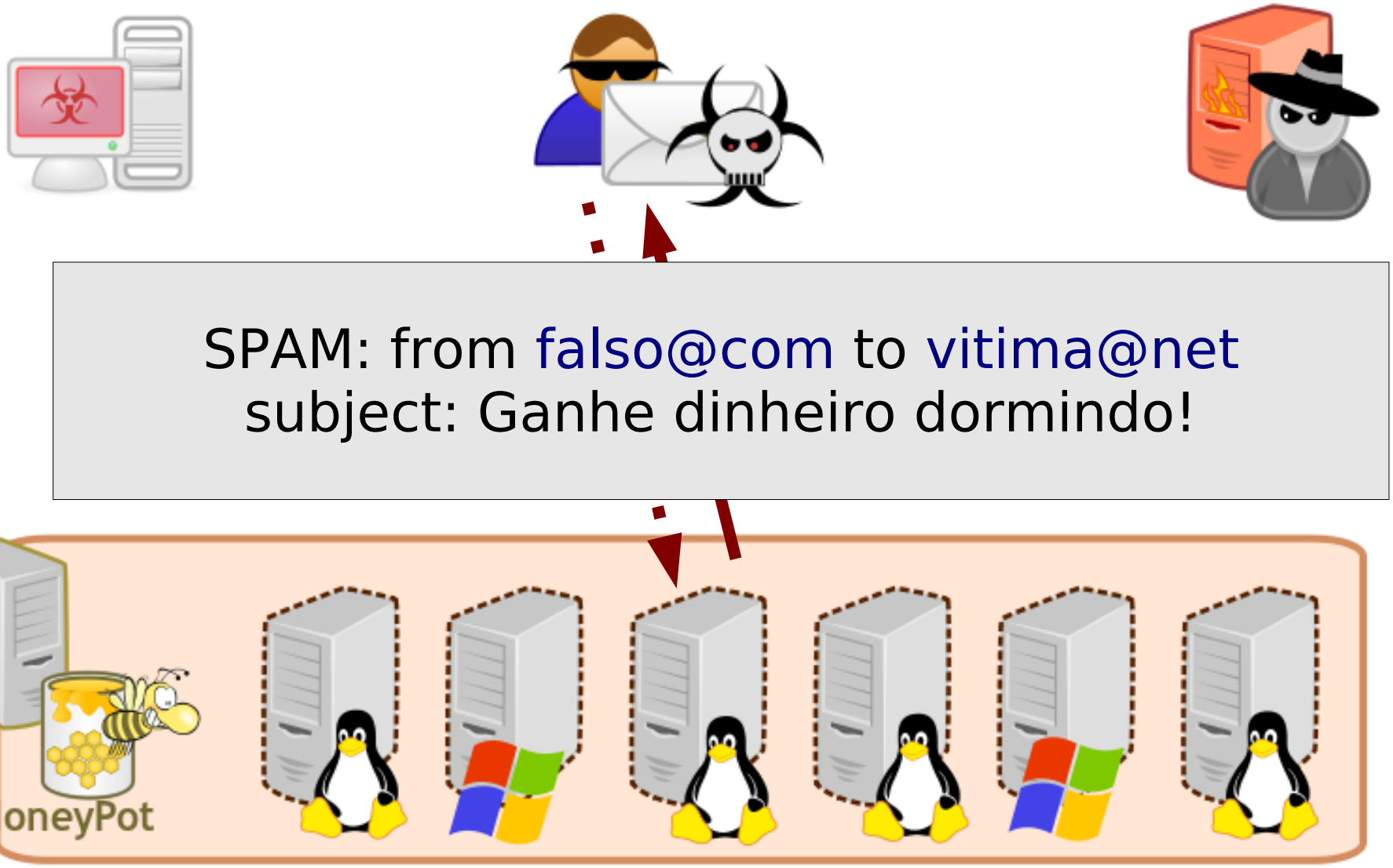
HoneyNet



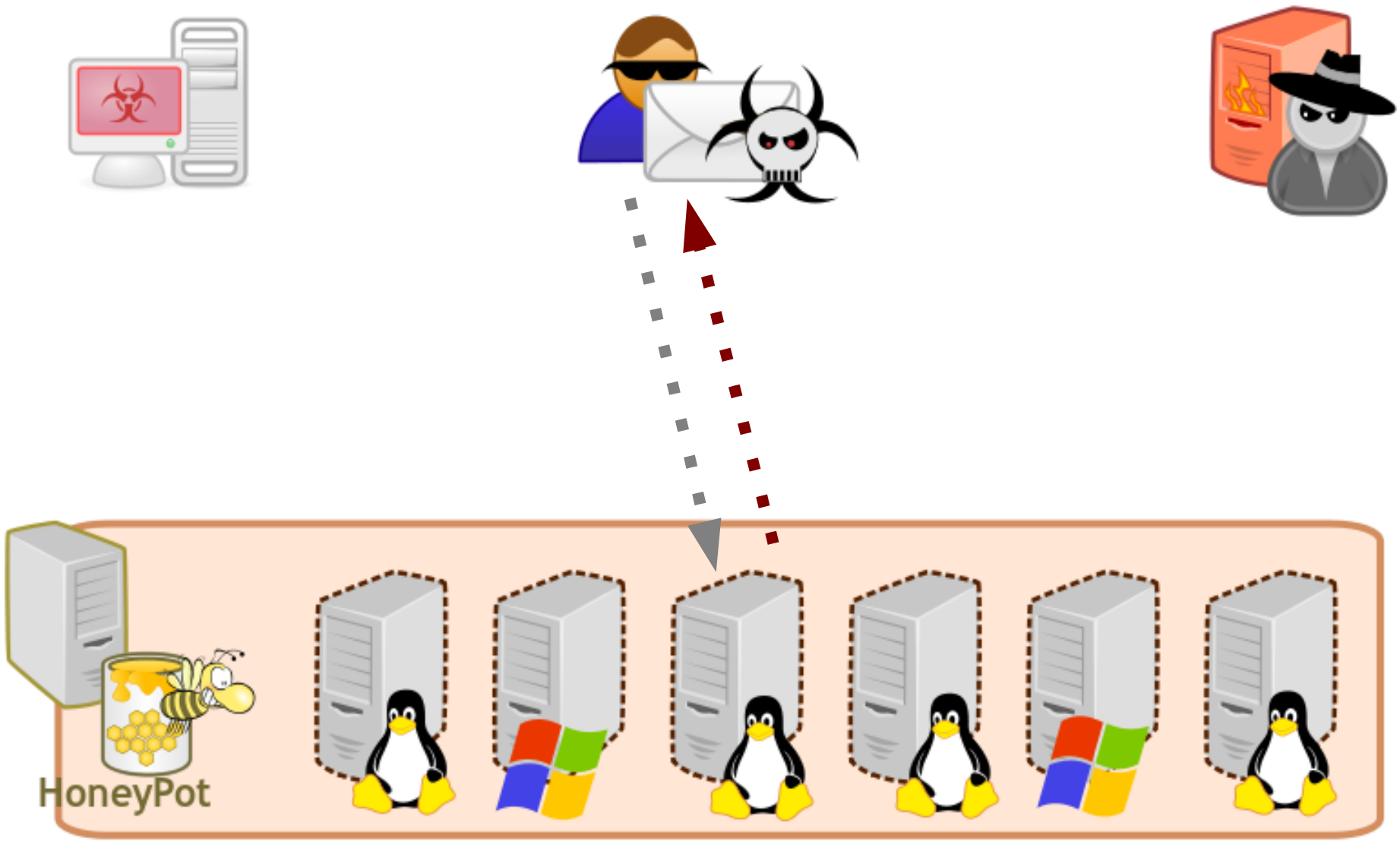
HoneyNet


SPAM: from falso@com to vitima@net
subject: Ganhe dinheiro dormindo!
HoneyPot

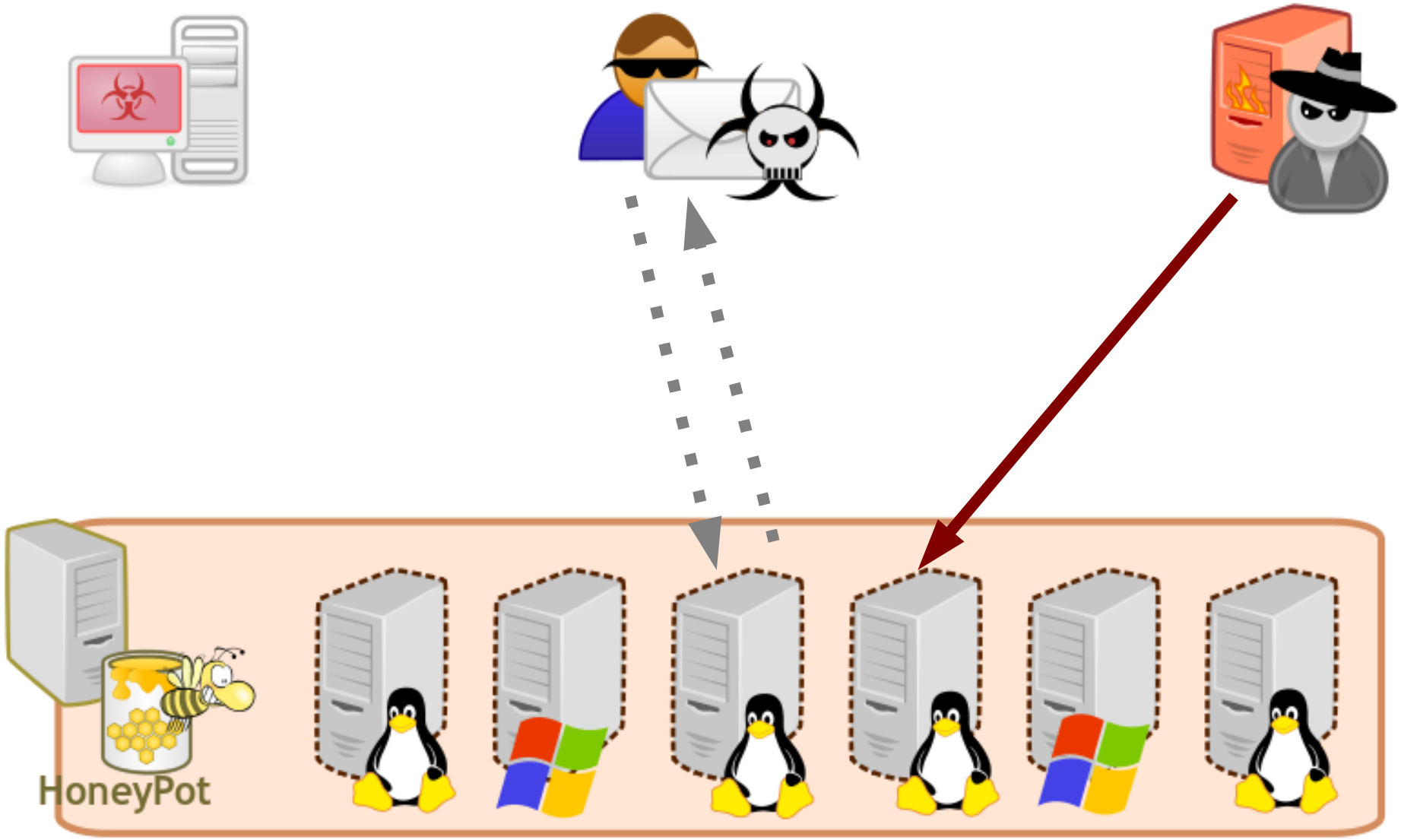
HoneyNet


SPAM: from falso@com to vitima@net
subject: Ganhe dinheiro dormindo!
HoneyPot

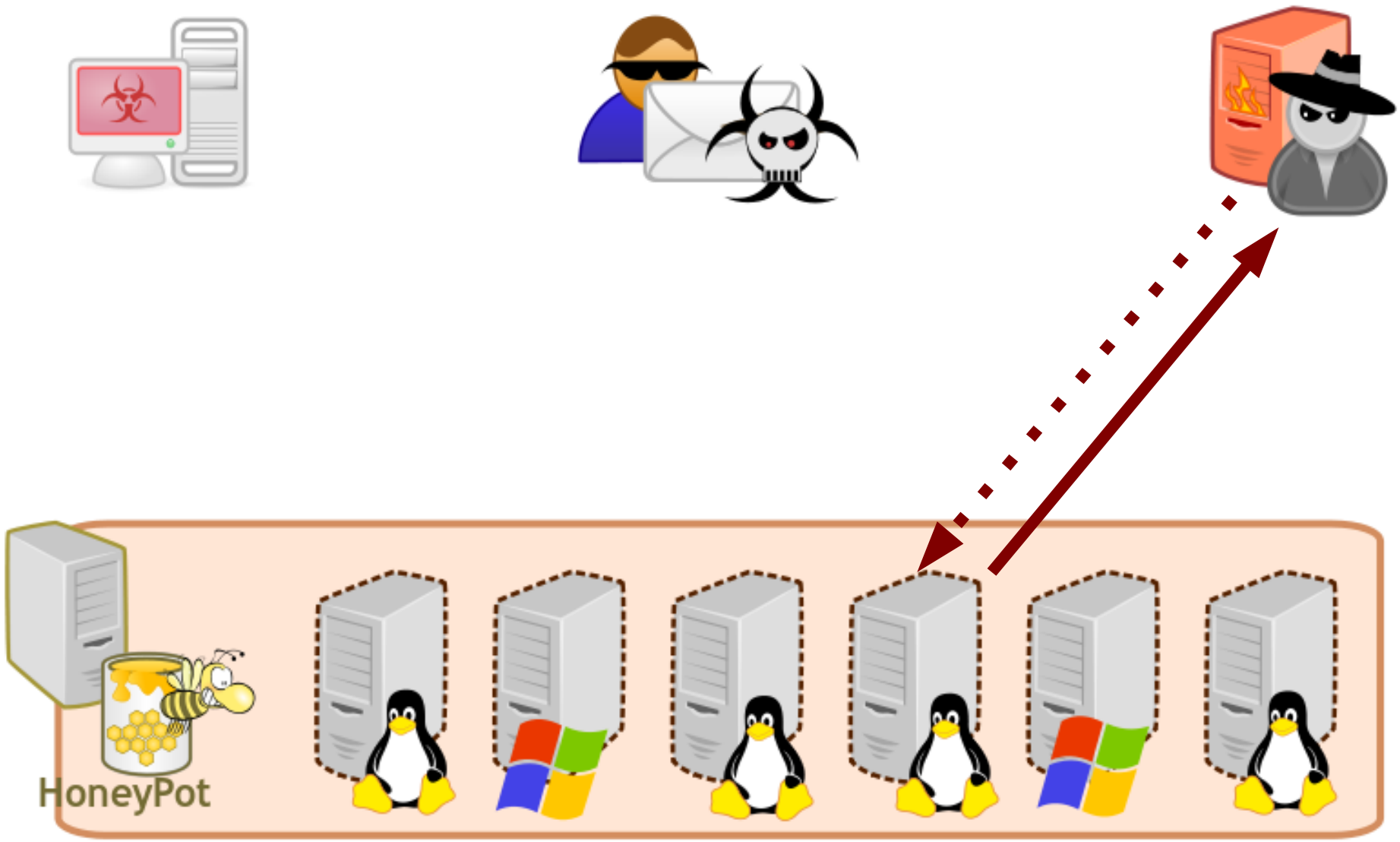
HoneyNet



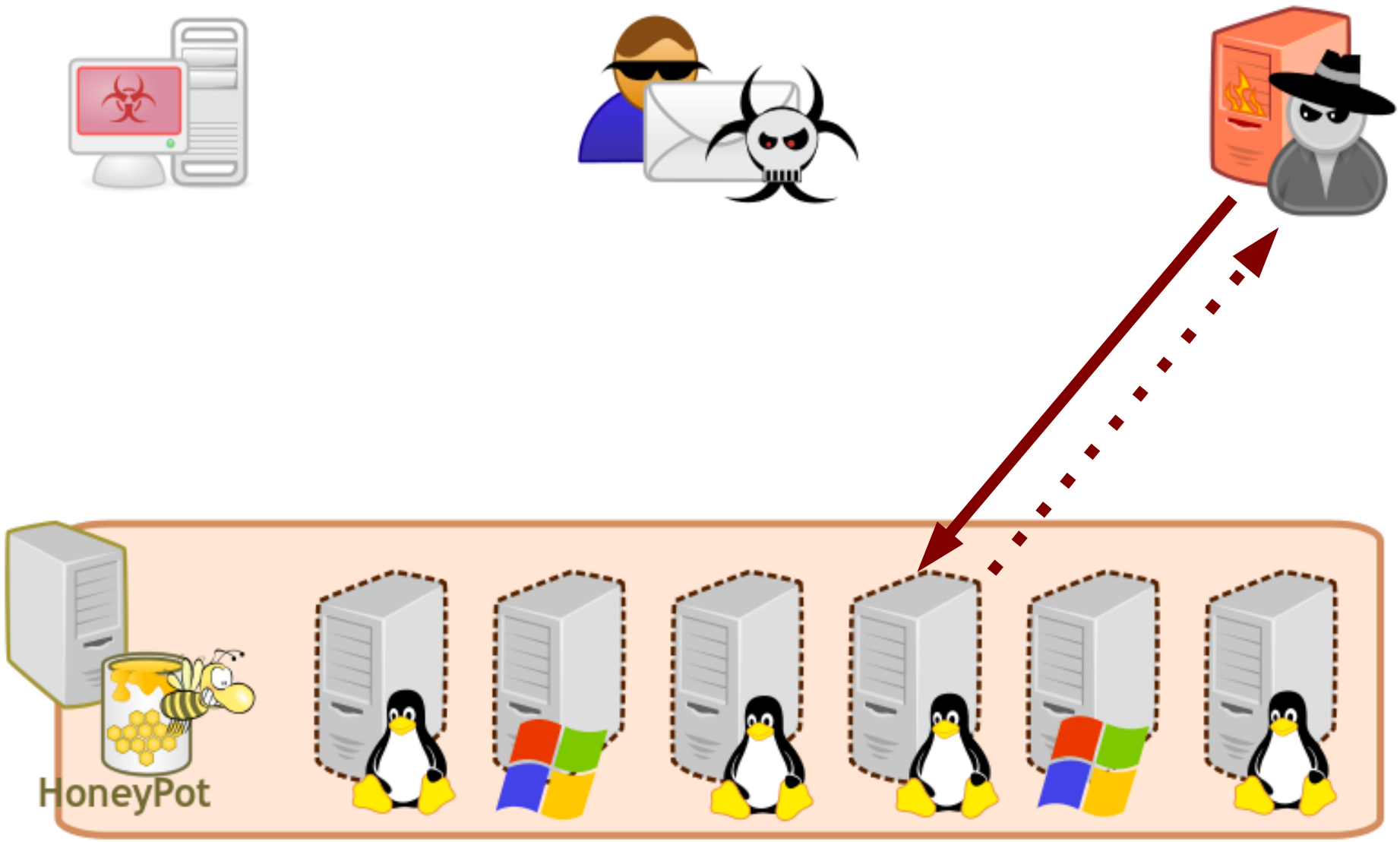
HoneyNet



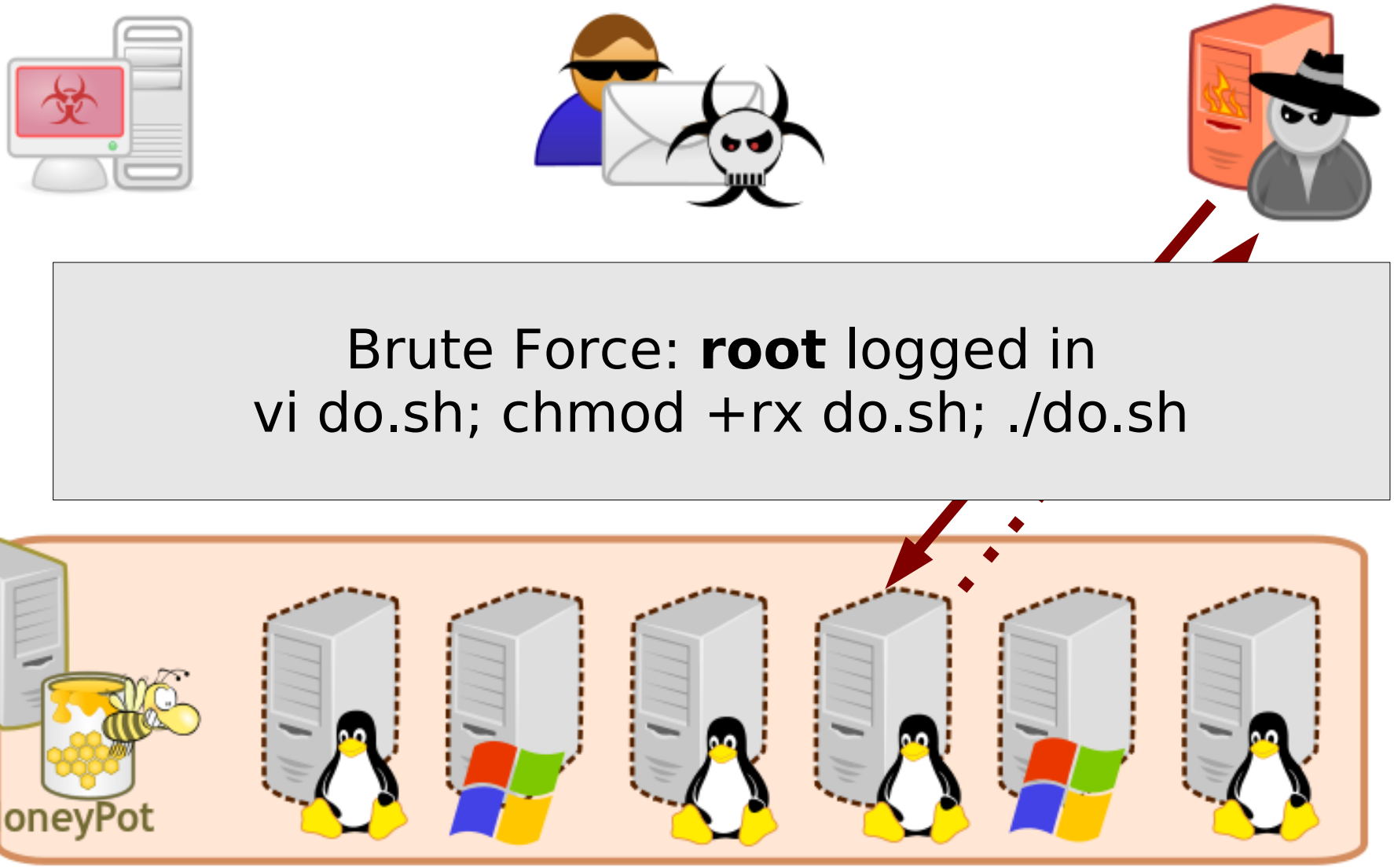
HoneyNet



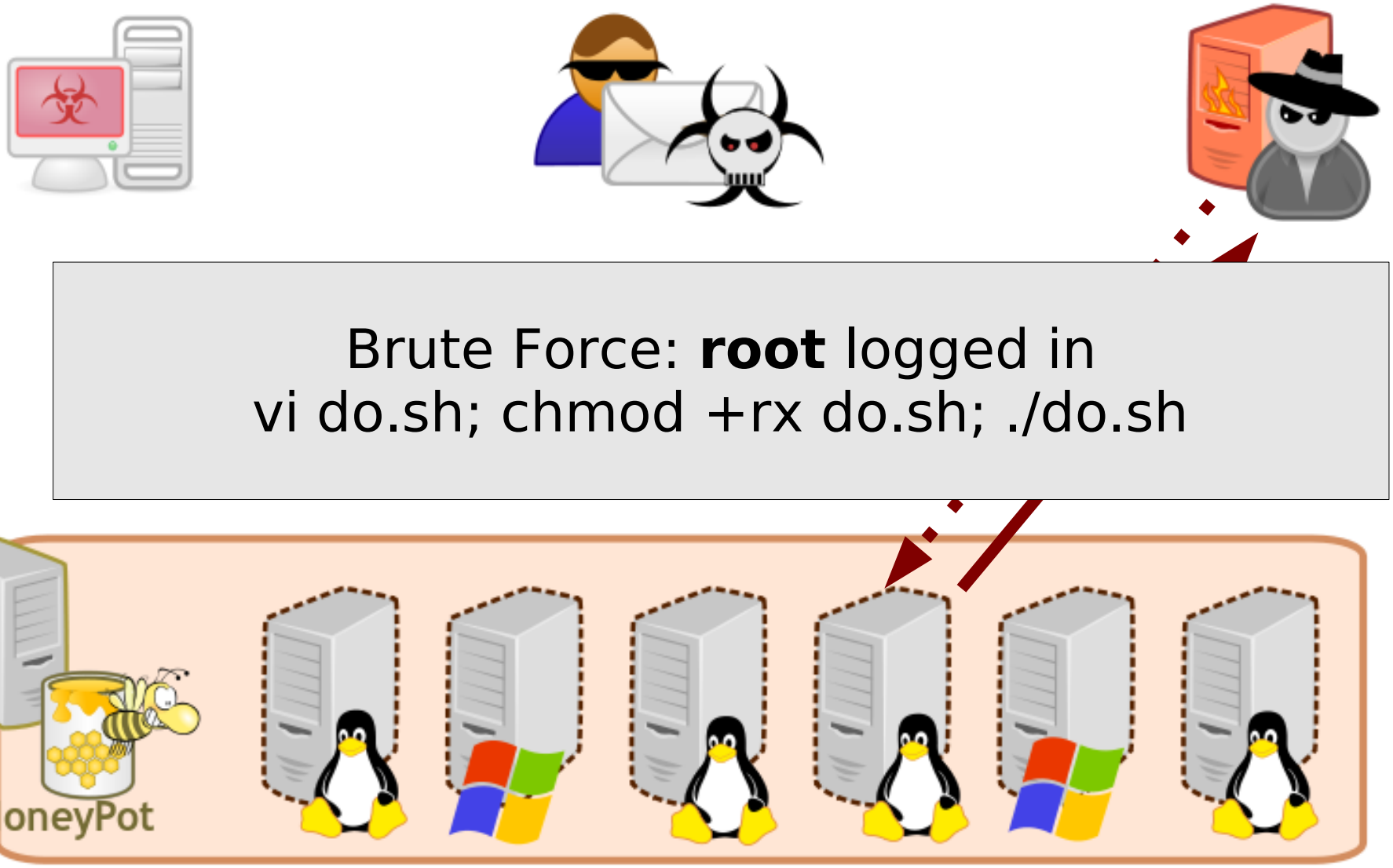
HoneyNet



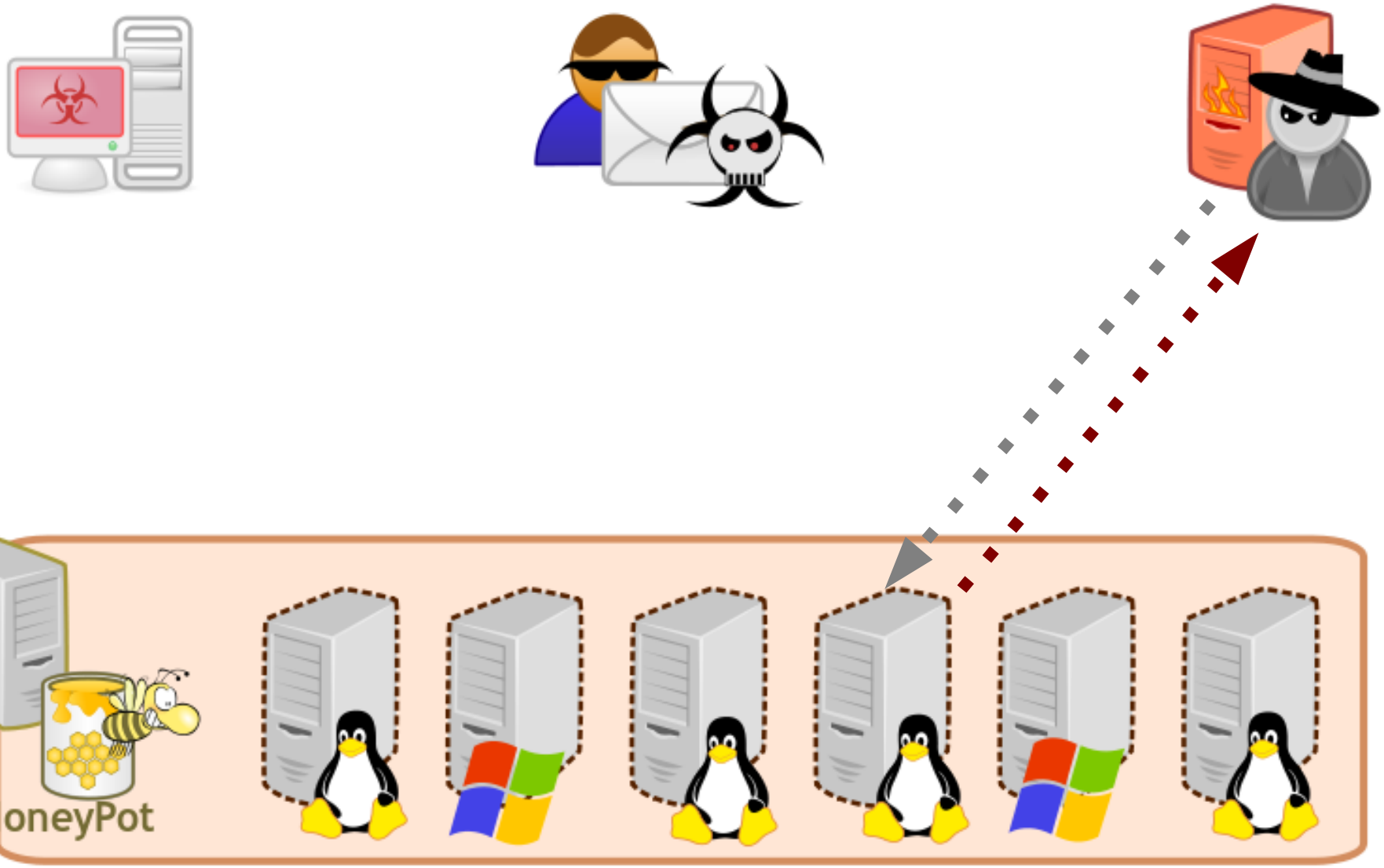
HoneyNet


Brute Force: **root** logged in
vi do.sh; chmod +rx do.sh; ./do.sh
HoneyPot

HoneyNet


Brute Force: **root** logged in
vi do.sh; chmod +rx do.sh; ./do.sh
HoneyPot

HoneyNet

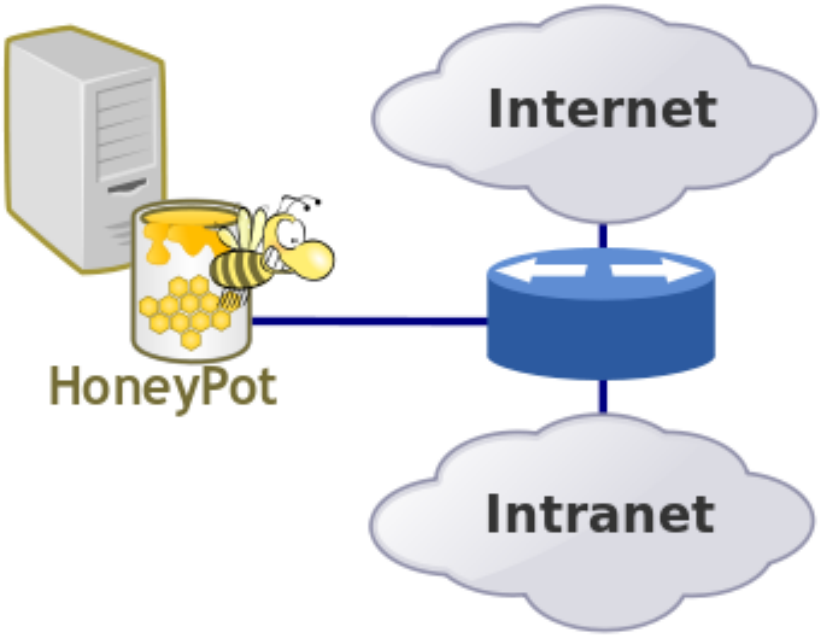


Aplicação

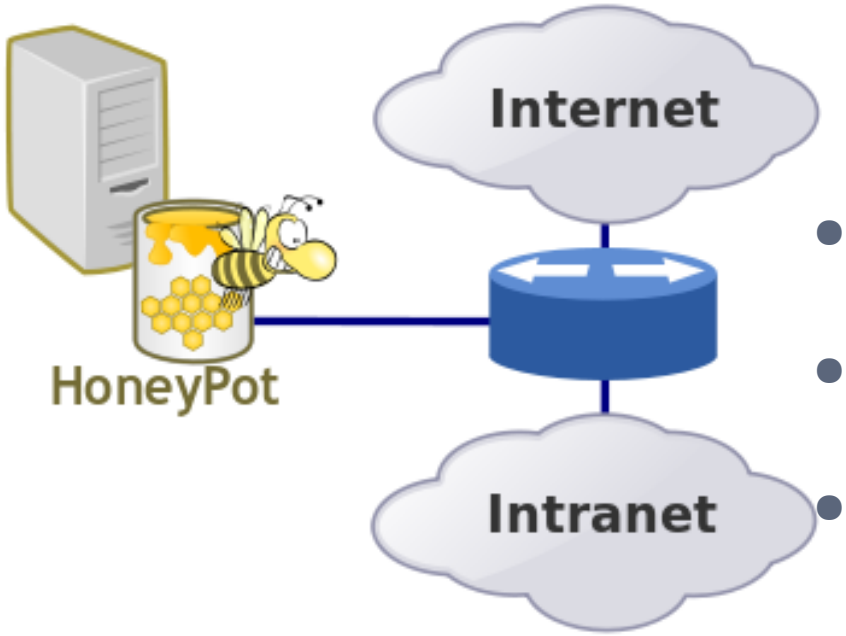
HoneyPot Corporativo
HoneyPot Alliance

CELEPAR
INFORMÁTICA
do PARANÁ

HoneyPot Corporativo



HoneyPot Corporativo



Hoje:

- 1 Servidor HoneyPot
- Roteamento Switch Core
- Nepenthes, Snort e IPTables

Próximo passo:

- Honeyd/Dionaea
- HoneyPot nos Clientes

HoneyPot Corporativo

Hoje:

- Servidor HoneyPot em 3 DMZs
- Sem roteamento

Próximo passo:

- Em todas as redes hospedadas

HoneyPot Corporativo

Hoje:

- 1 Servidor DNS em Teste

  (~2000 hosts)
- SinkHole → ISC Bind
- AMADA e Malware Domain List

Próximo passo:

- DNS Corporativo
- DNS Clientes

HoneyPot Corporativo

Alguns dados:

- ~ 35% dos alertas de segurança
- ~ 23% das estações infectadas
- Diversos ataques (Portscan)
- Erros de configuração
- Novos vírus/malwares
- Erros em WebSites

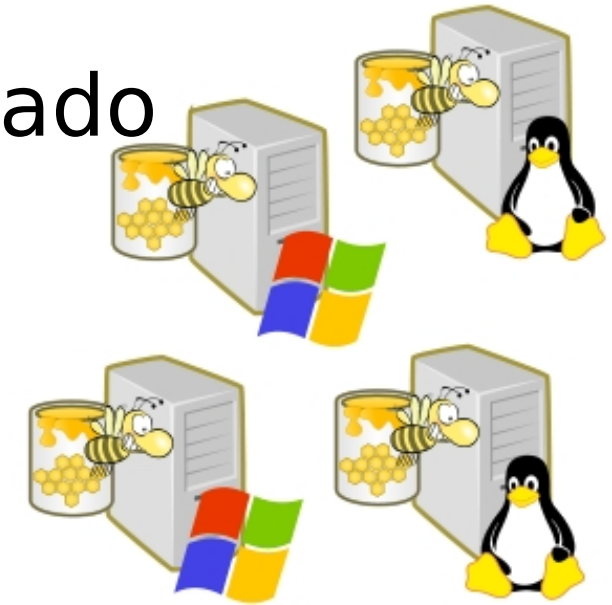
HoneyPot Alliance

Consórcio Brasileiro de HoneyPots

- Coordenado pelo CERT
- Termo de Confidencialidade

Servidor HoneyPot:

- Rede secreta – Servidor dedicado
- Honeyd → Criação de perfis
- Relatórios diários
  - E-mails criptografados

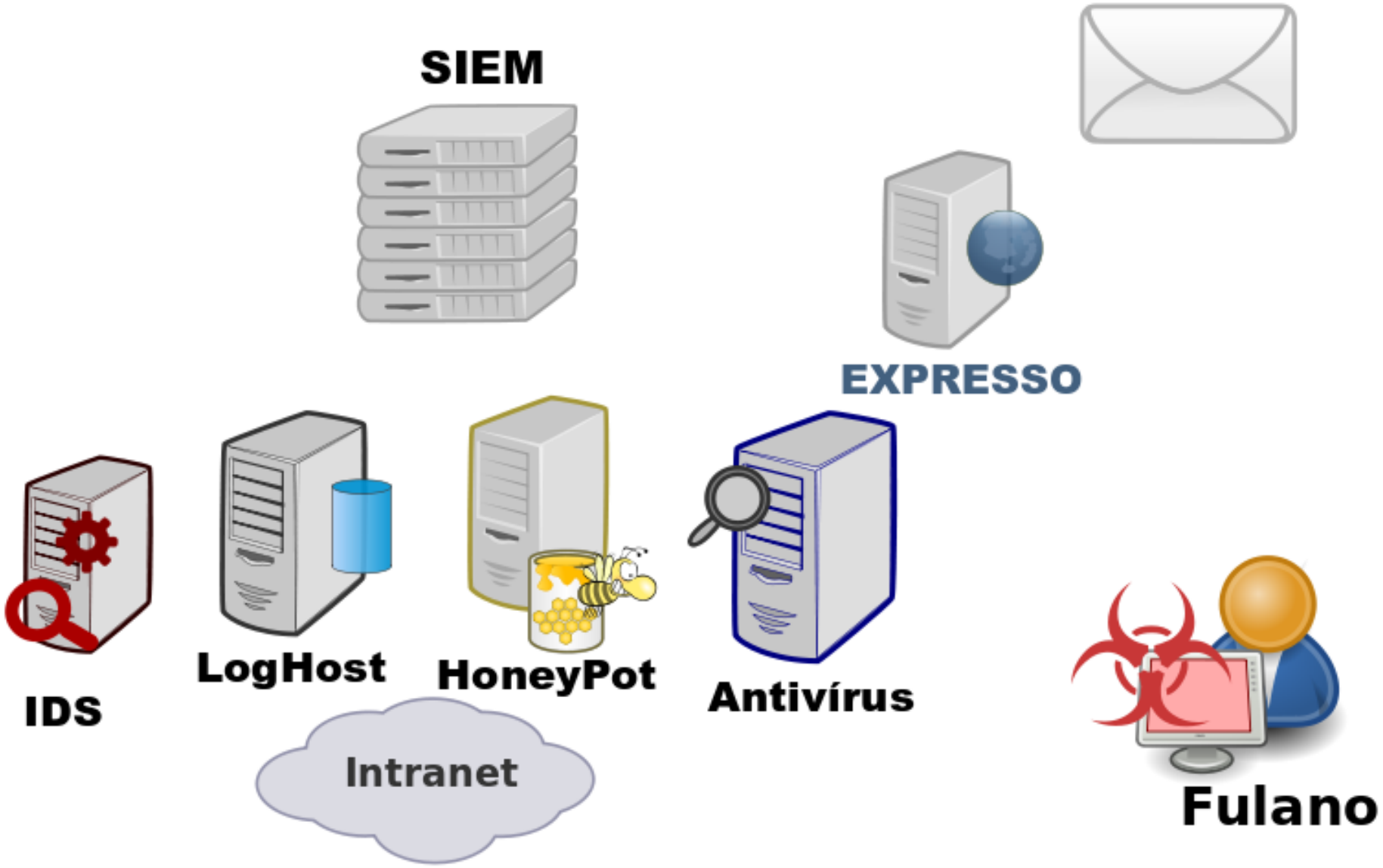


INCIDENTES

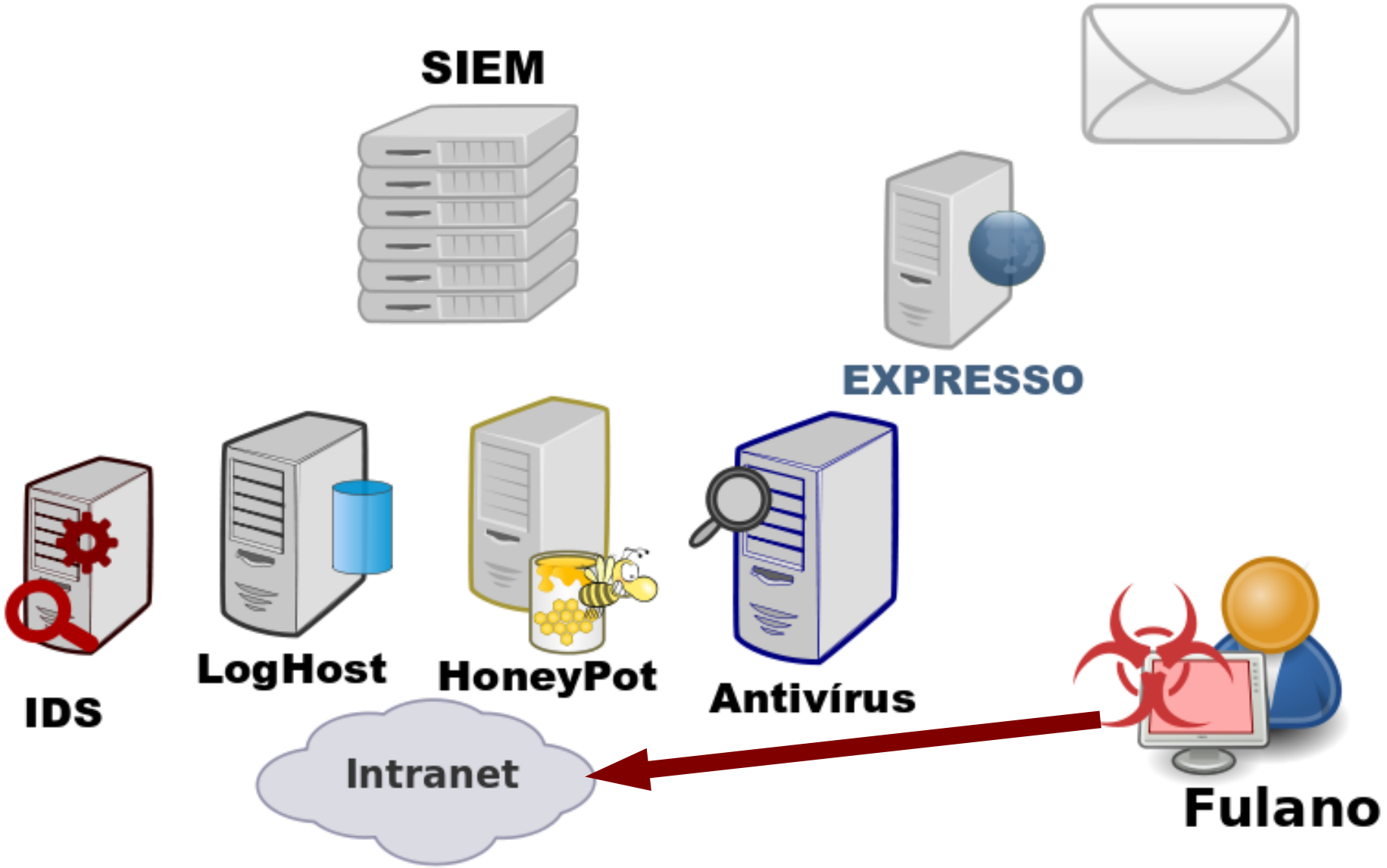
Tratamento de Incidentes e Notificações

CELEPAR
INFORMÁTICA
do PARANÁ

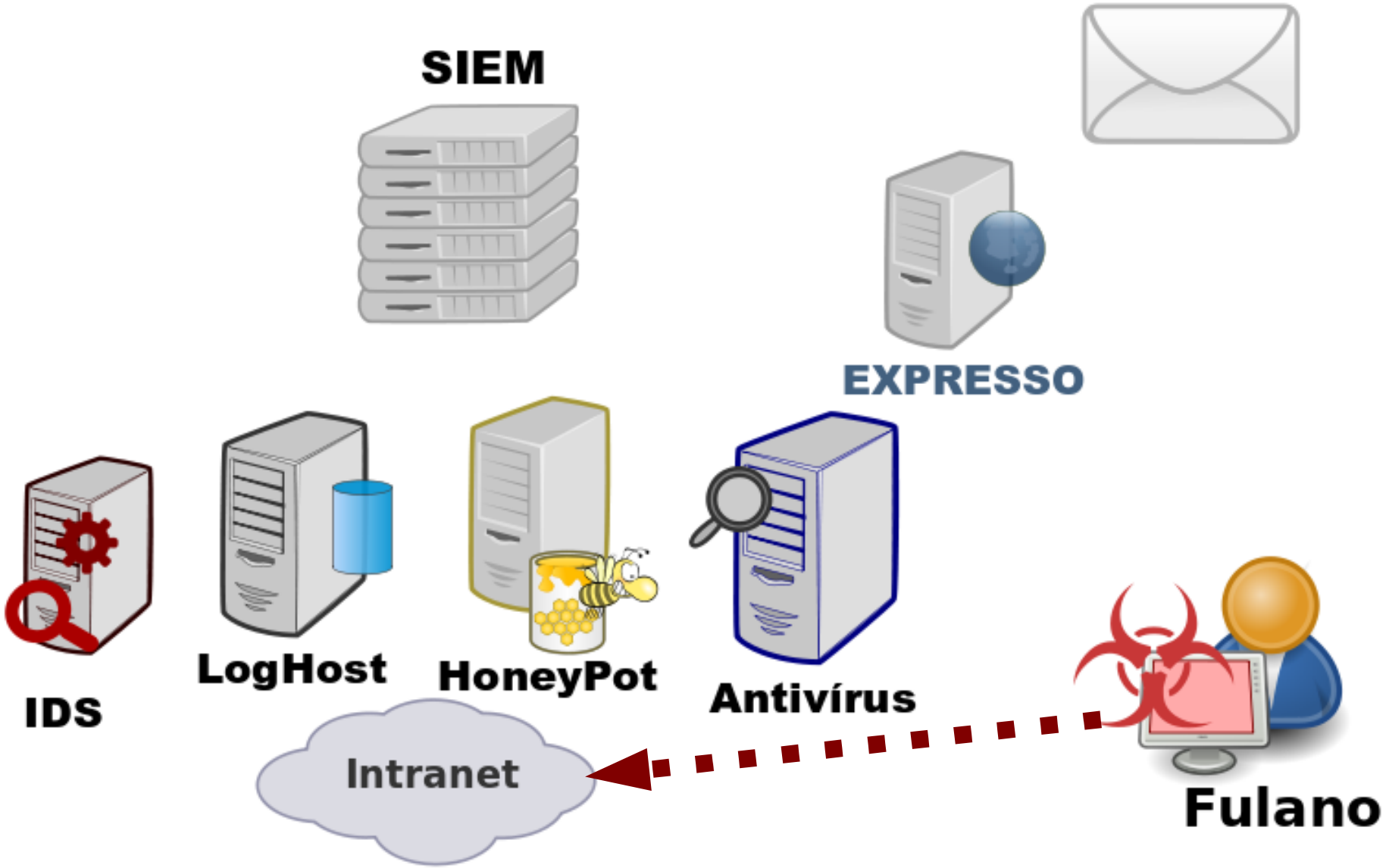
Tratamento de Incidentes



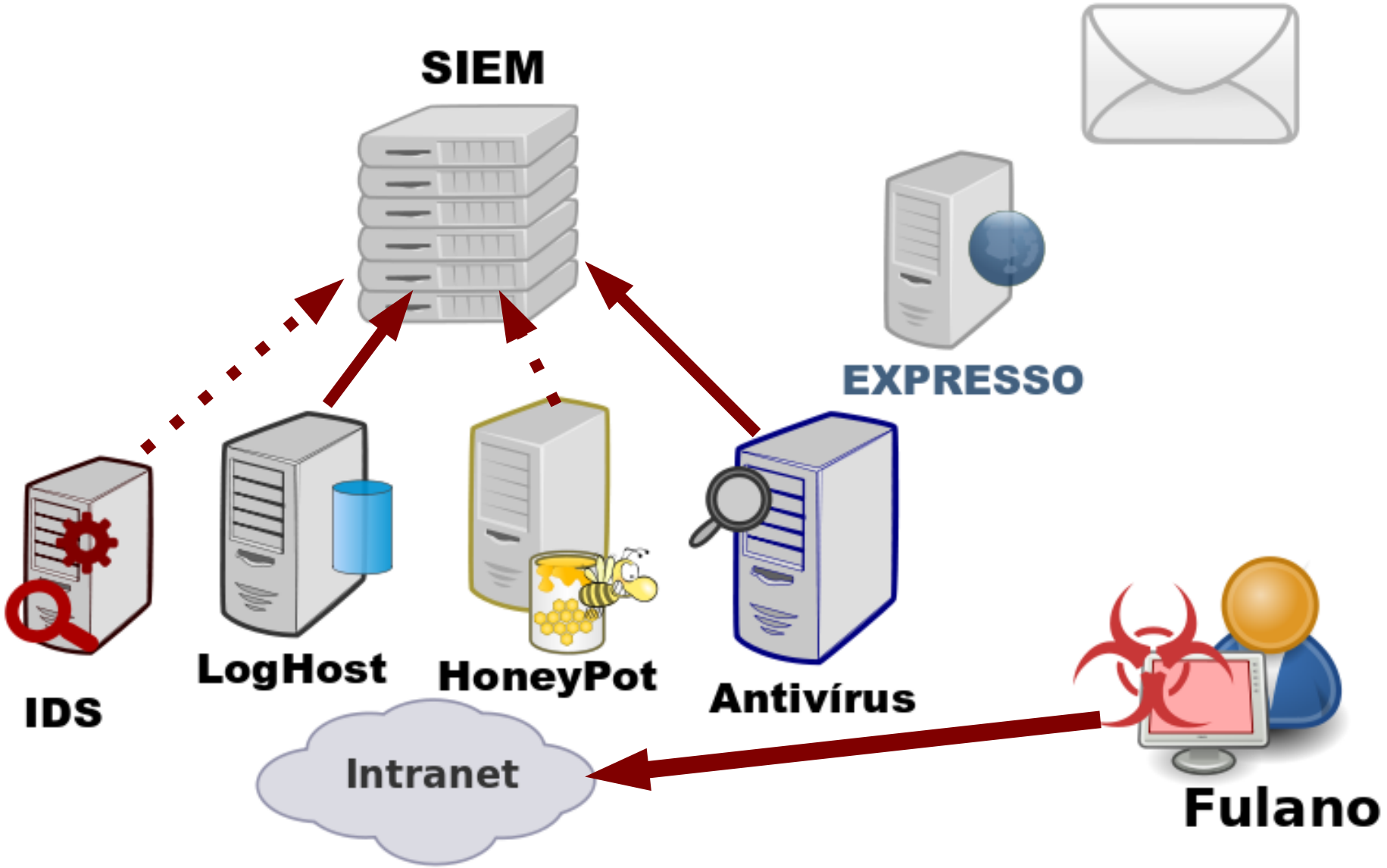
Tratamento de Incidentes



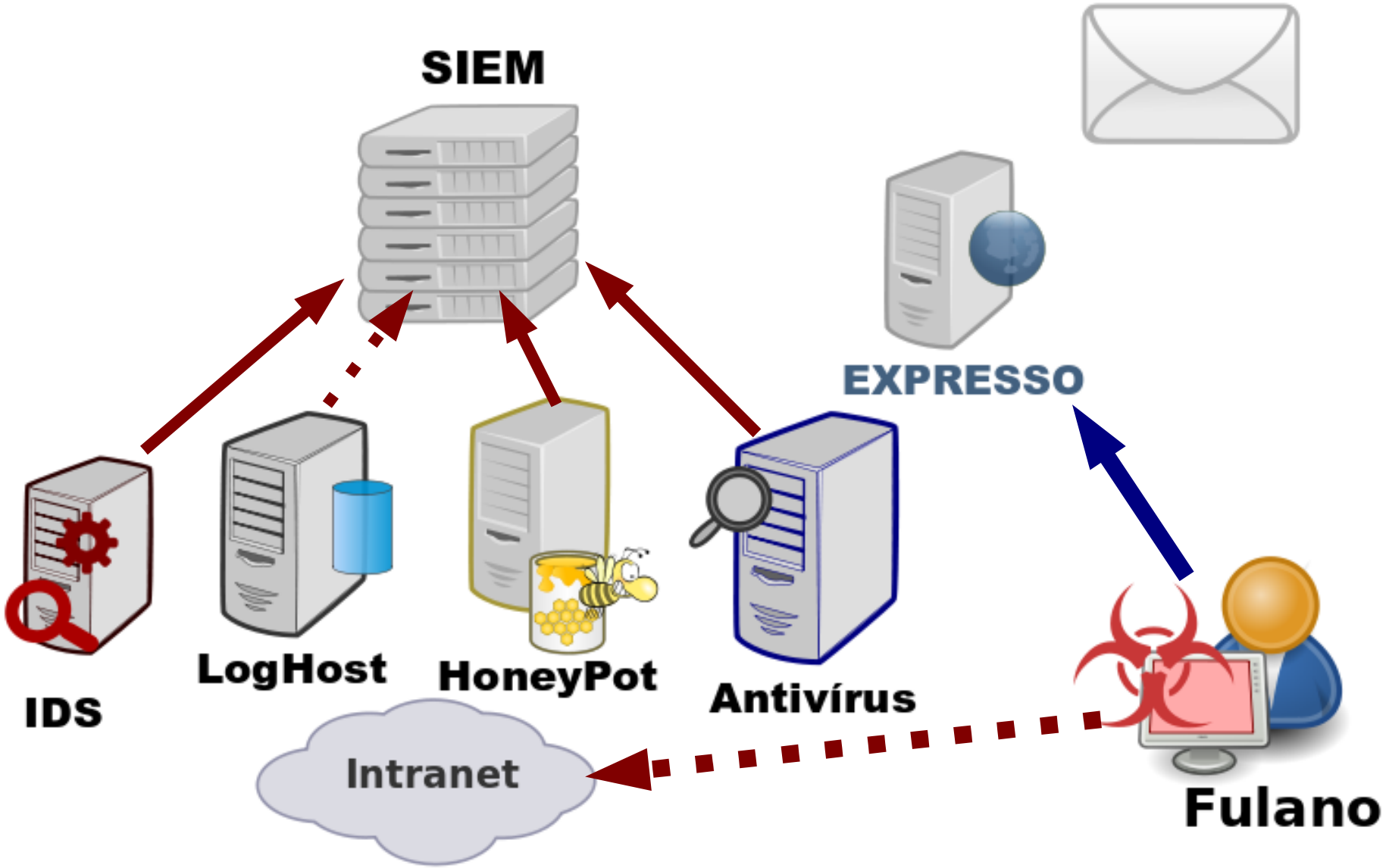
Tratamento de Incidentes



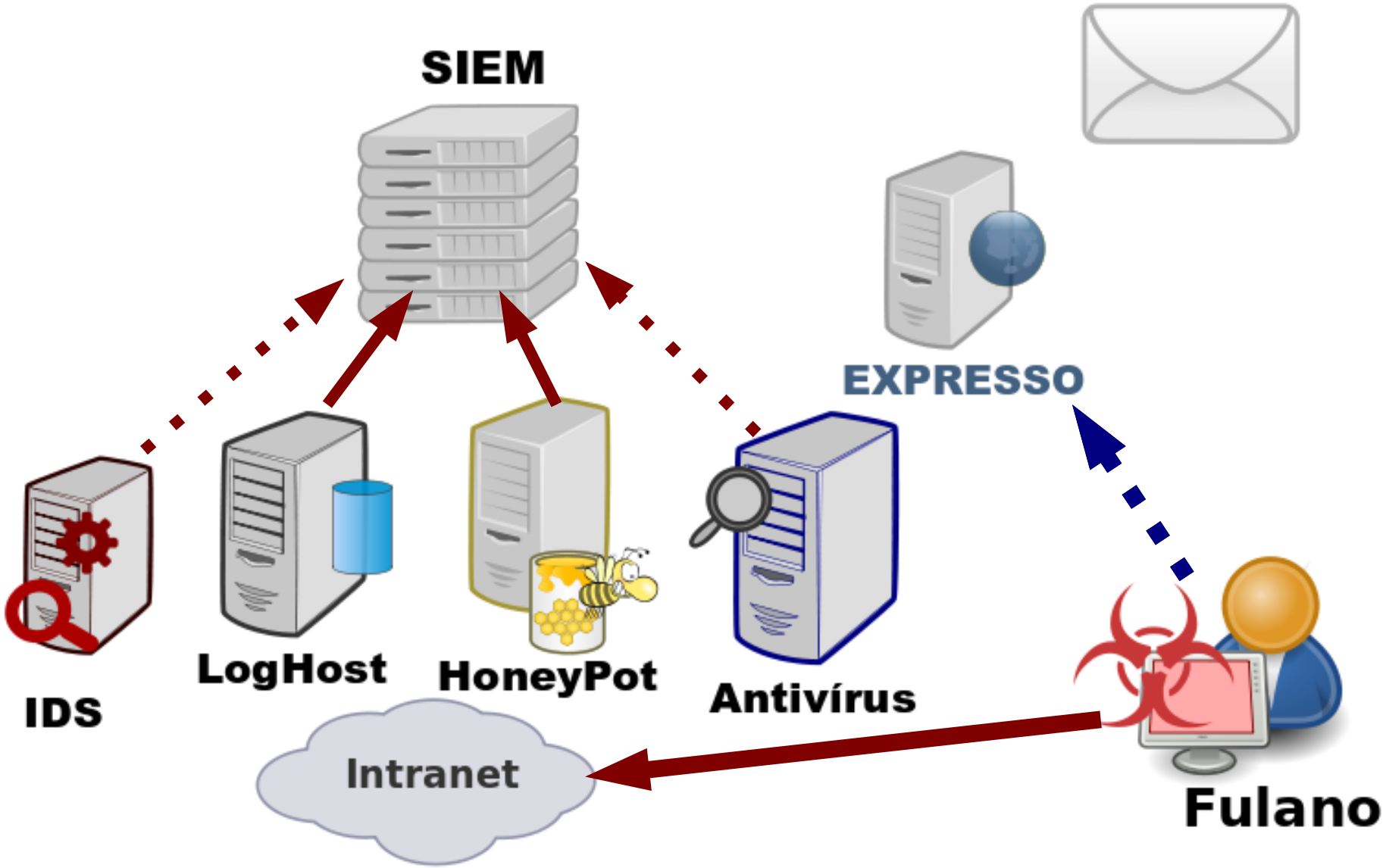
Tratamento de Incidentes



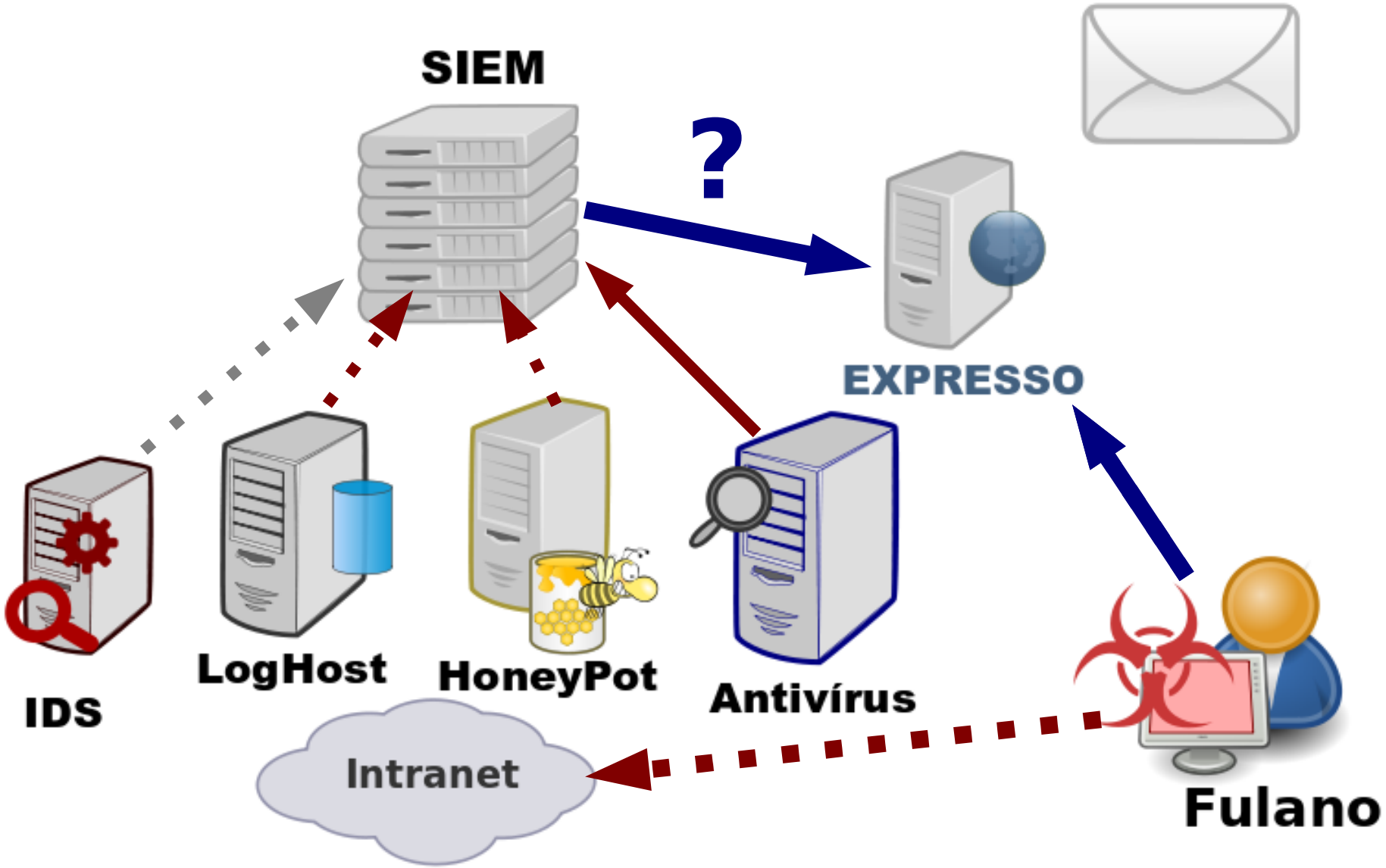
Tratamento de Incidentes



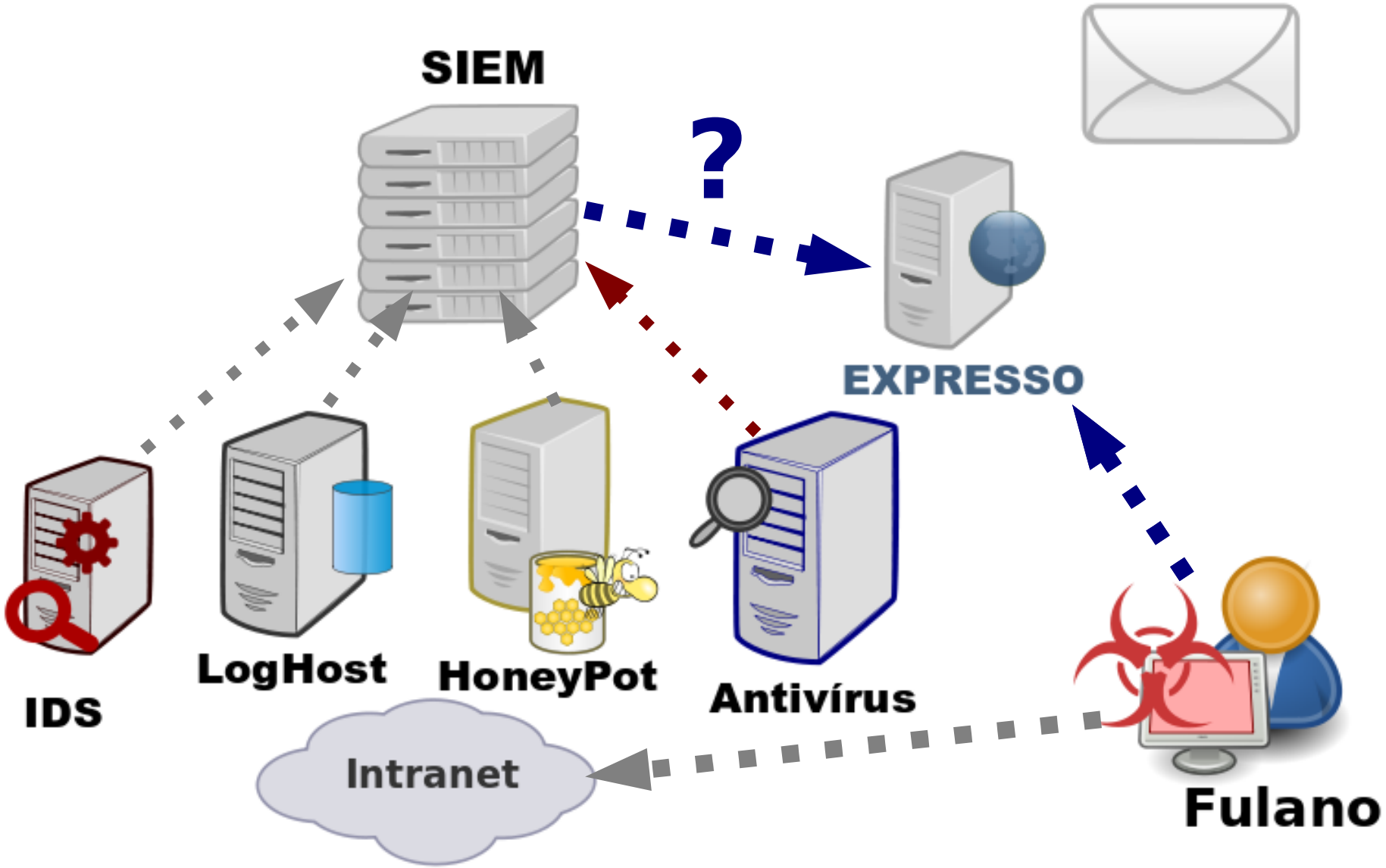
Tratamento de Incidentes



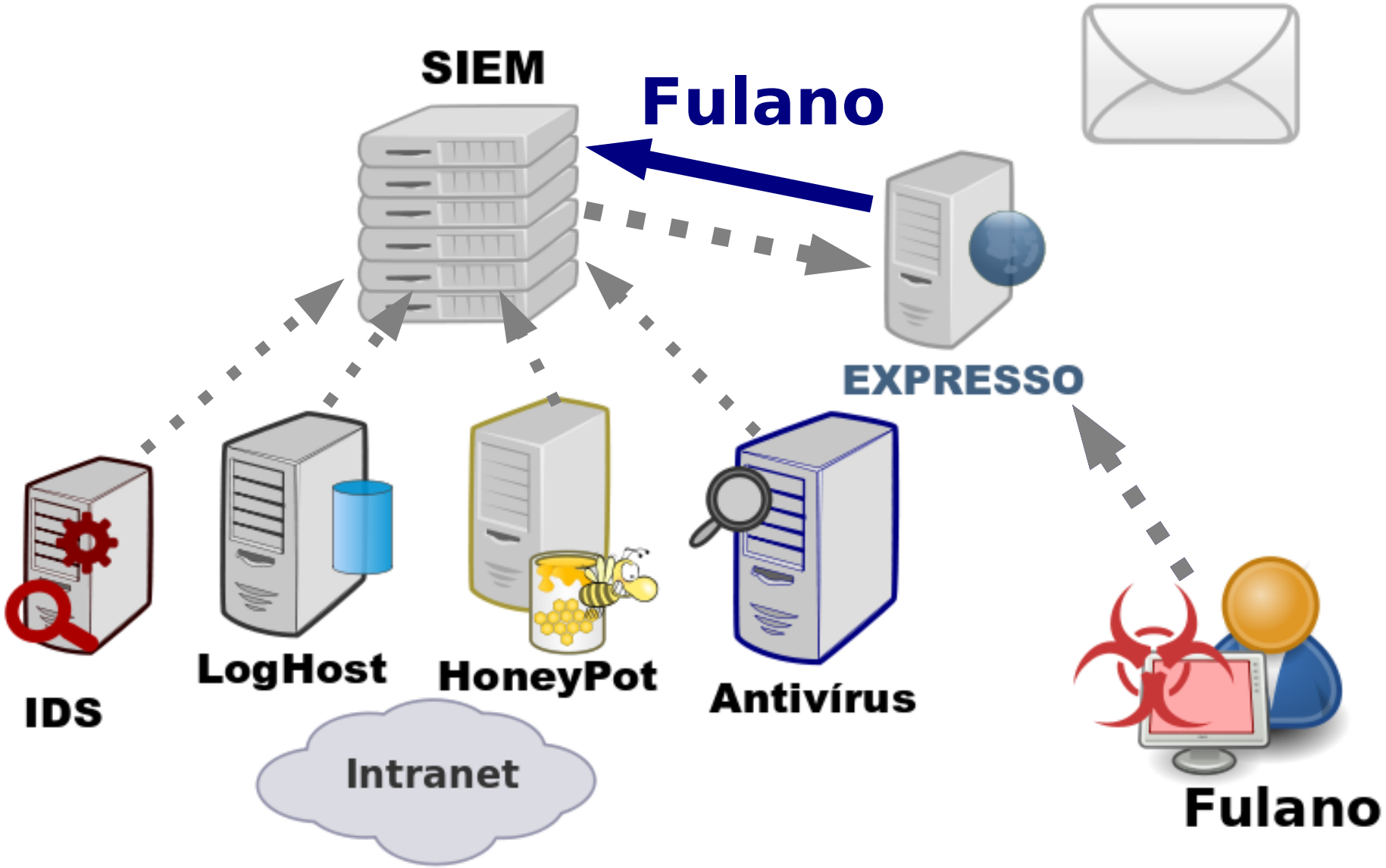
Tratamento de Incidentes



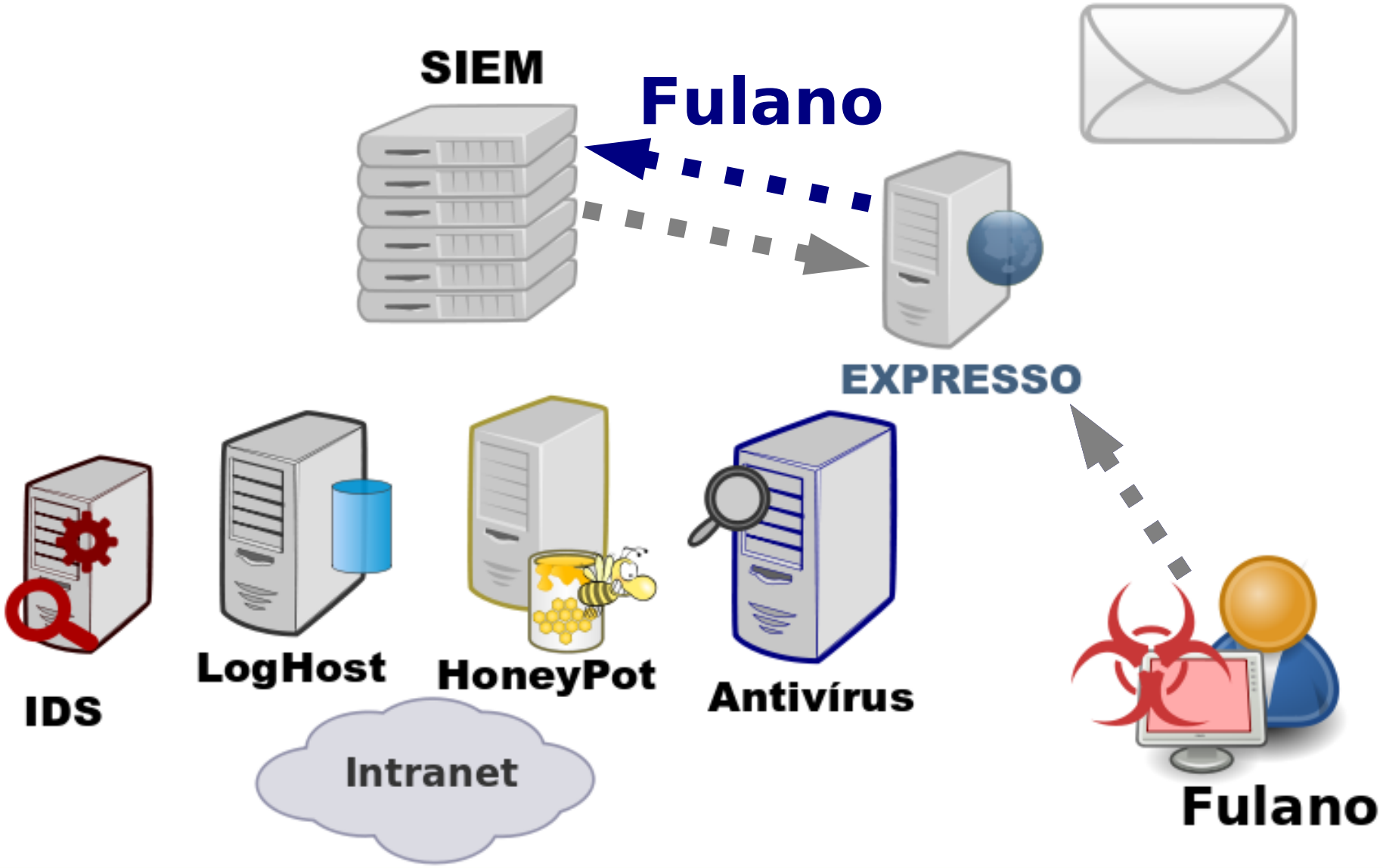
Tratamento de Incidentes



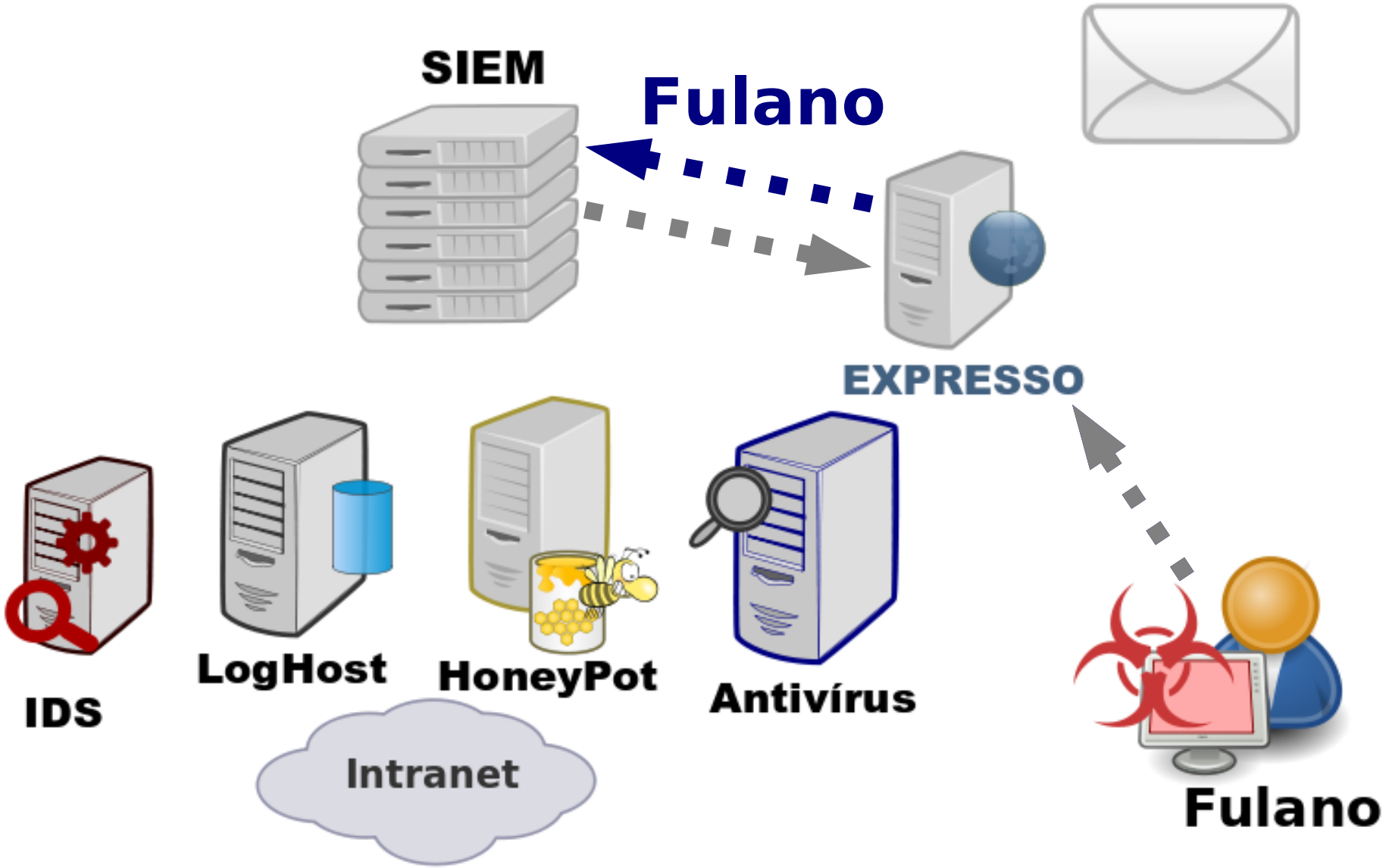
Tratamento de Incidentes



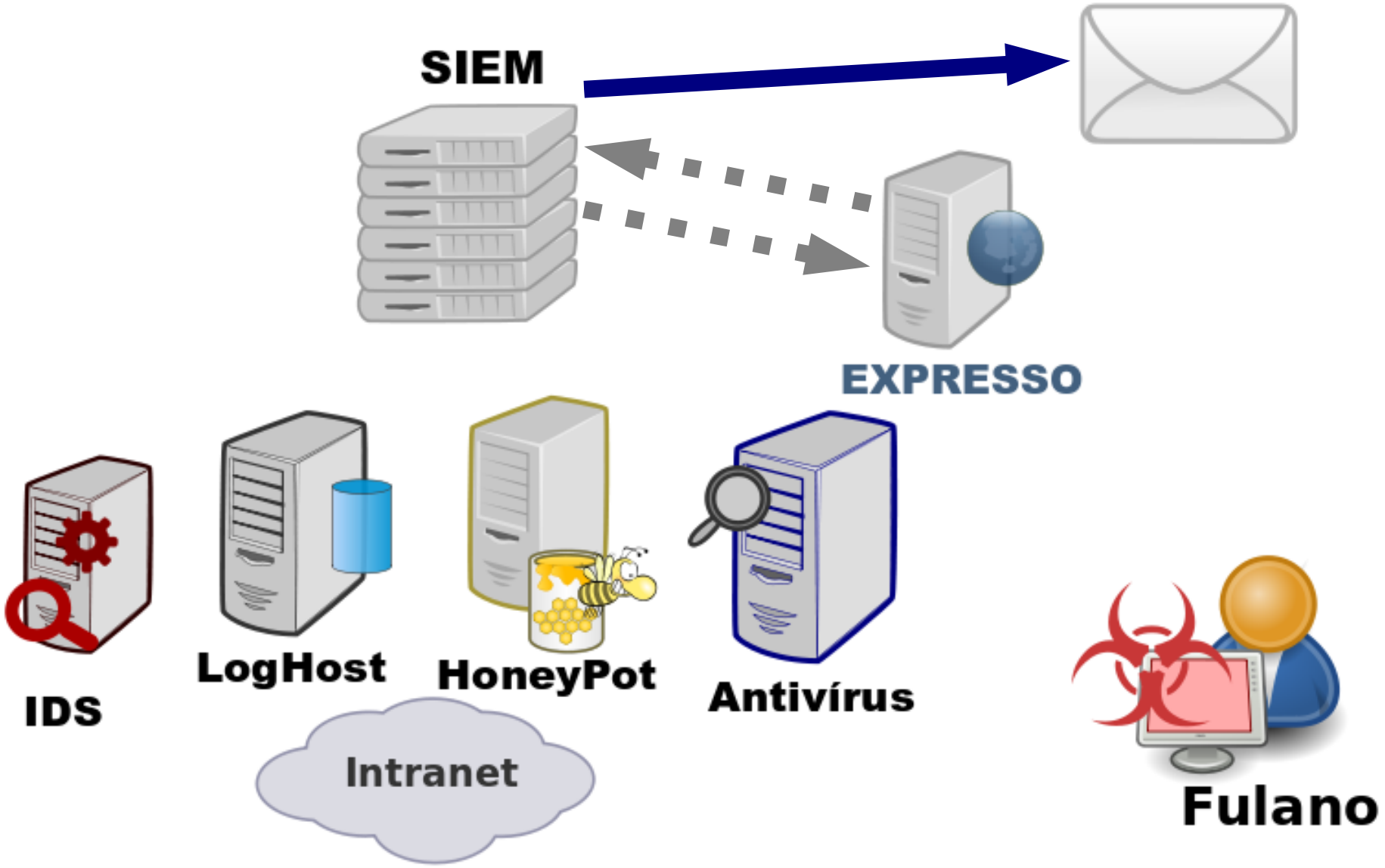
Tratamento de Incidentes



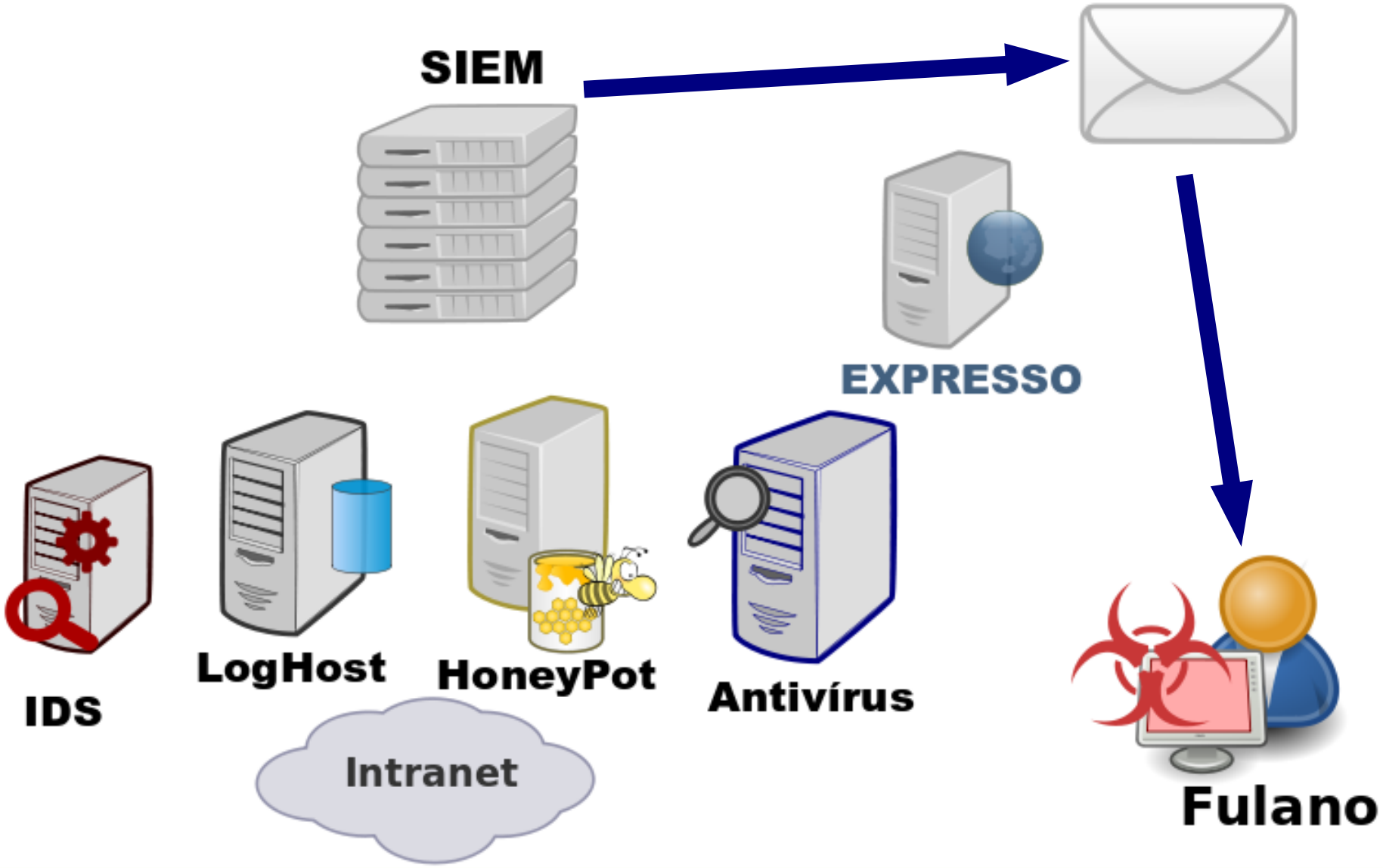
Tratamento de Incidentes



Tratamento de Incidentes



Tratamento de Incidentes



Tratamento de Incidentes

From: Equipe de Segurança

To: Fulano

Subject: [Mensagem Automática]

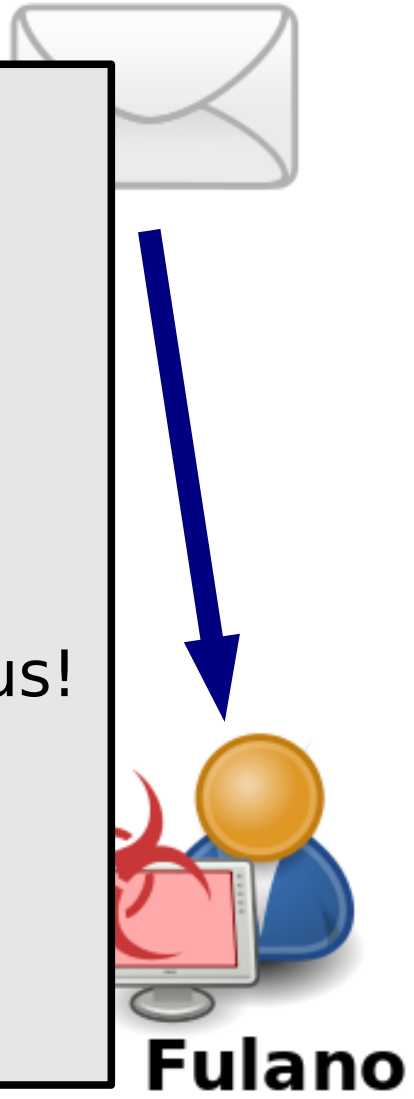
Caro(a) Fulano,

Identificamos que sua estação está com vírus!

Alertas: XYZ

Procedimentos: ABC

Gratos pela sua colaboração!



Notificações Externas

- CAIS
- Shadow Servers
- Google
- Outros...

Finalizando

Próximos Projetos
Conclusão

CELEPAR
INFORMÁTICA
do PARANÁ

Próximos Projetos

Em estudo:

- HoneyPot de alta interatividade:
  - SSH Kojoney, PHP, BotHunter

Futuramente:

- HoneyPot para VoIP
- HoneyPot em redes IPv6

Conclusão

HoneyPot/SinkHole/HoneyNet

- Monitorar estações que estão sem o antivírus corporativo
- Detecção de novos vírus e ameaças
- Baixo custo, efetivo, escalável e fácil de manter

Referências

- amada.abuse.ch
- [dionaea|nepenthes].carnivore.it
- www.honeyd.org
- www.honeypots-alliance.org.br
- http://isc.sans.edu/diary.html?storyid=7930
- www.malwaredomainlist.com
- www.rfc-editor.org
- www.shadowserver.org

OBRIGADO!

Perguntas?

seginfo@celepar.pr.gov.br

Produzido com:

debian GNOME

OpenOffice.org

INKSCAPE

GIMP