

# Protocolo CIE - ADETTI: *Tecnologia ProGuard* Paulo Trezentos



Dia do Centro de Informática do Exército

7 . Outubro . 2003



## Agenda

- Apresentação da ADETTI / Linux Caixa Mágica
- Tecnologia ProGuard
- Âmbito do Protocolo CIE – ADETTI
- Conclusões



## Apresentação ADETTI

- Instituição de Investigação sem fins lucrativos fundada em 1989
- Centro associado do ISCTE na área de Telecomunicações e Tecnologias de Informação
- Recursos humanos
  - 13 PhD, 11 MSc, 6 MBAs, 11 elementos administrativos / gestão projecto
  - Vários investigadores convidados e alunos de licenciatura



## Apresentação Linux Caixa Mágica

- Distribuição de Linux portuguesa desenvolvida de raíz
- Projecto da ADETTI iniciado em Outubro de 2000
- Equipa de 10/ 15 pessoas
- Desenvolvimento de soluções baseadas em software livre



Caixa Mágica



## Software

## Formação

## Appliances

CM

Desktop

8.01  
CM

Servidor

Linux @PME

Linha  
Técnica

Linha  
Profissional  
I



**Suporte**

**Parcerias**

**Integradores**

**Documentação**

**Divulgação**

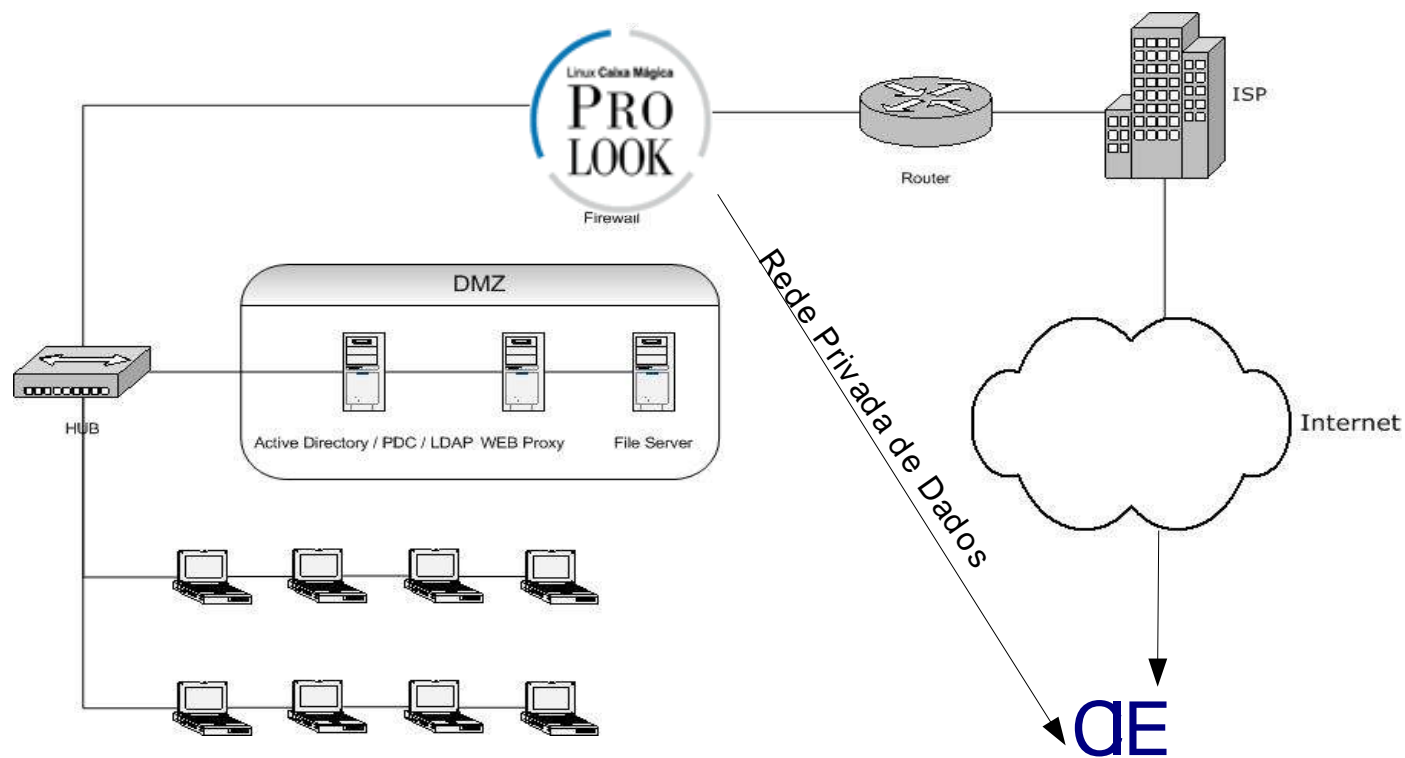


## Tecnologia ProGuard

- Solução de Firewall altamente flexível
- Disponibilizada sob a forma de *Appliance*
  - Solução chave-na-mão de Software + Hardware
- Categorias de funcionalidades
  - Monitorização do sistema / tráfego (gráficos MRTG, ligações activas,...)
  - Firewall (Políticas, Regras, QoS, DNAT, SNAT, Ligações backup, Li)
  - VPN (host-to-net, net-to-net,...)
  - Outros serviços (DHCP, DNS dinâmico, forwarding SQUID,...)



# Arquitetura potencial






## Tecnologia ProGuard II

- Software Livre
  - Kernel Linux + iptables, Free S/Wan, Calamaris, mrtg, Webalizer, snort, ...
- Desenvolvimento
  - Distribuição de Linux especial
  - Interface Web
  - Motor de configuração
  - Alterações e otimização de software base






Estabob Sistema

File Edit View Go Bookmarks Tools Window Help



Linux Caixa Mágica

# PRO GUARD

**Serviços:**

CRON server	A CORRER
VPN	PARADO
Sistema de detecção de intrusão	A CORRER
Web server	A CORRER
Servidor DHCP	PARADO
Logging server	A CORRER
DNS proxy server	A CORRER
Interligacao com CM Prolook	PARADO
Kernel logging server	A CORRER

**Memoria:**

	total	used	free	shared	buffers	cached
Mem:	61896	60144	1752	0	26892	11328
-/+ buffers/cache:		21924	39972			
Swap:	96380	7440	88940			

**Disco utilizado:**

Filesystem	Size	Used	Avail	Use%	Mounted on
/dev/hda4	7.3G	1.4G	5.5G	20%	/
/dev/hda1	30M	4.9M	24M	17%	/boot
/dev/hda3	6.5G	211M	5.9G	3%	/var/log

**Uptime e utilizadores:**

6:26pm up 4 days, 21:52, 1 user, load average: 0.00, 0.00, 0.00

USER	TTY	FROM	LOGING	IDLE	JCPU	PCPU	WHAT

javascript:displaySubs('div2')



File Edit View Go Bookmarks Tools Window Help

Linux Caixa Mágica **PRO GUARD** inicio ajuda logout

Principal Estado Serviços Firewalling VPN Logs Logs

**Gráficos tráfego de rede:**  
Host: inetgate  
Time created: 2003/10/06 01:00:00 WES  
Data Start time: 2003/10/05 17:00:00 WES  
Data End time: 2003/10/06 01:00:00 WES  
Resolution (time/pixel): 1 min 4 sec

**Incoming GREEN Direct**  
Incoming GREEN Direct Start: Sun 2003/10/05 17:00:00 max: 1 avg: 0

**Outgoing GREEN Direct**  
Outgoing GREEN Direct Start: Sun 2003/10/05 17:00:00 max: 17 avg: 8



Regras de Firewall

File Edit View Go Bookmarks Tools Window Help

Linux Caixa Mágica

# PRO GUARD

Principal

Estado

Serviços

Firewalling

VPN

Logs

Logs

### Definicao de politica da Firewall

INPUT

ACCEPT

OUTPUT

ACCEPT

FORWARD

ACCEPT

### Adicionar Regra de Firewall

! IP origem

! Porta de origem:

! IP de Destino

! Porta de destino:

Protocolo

ALL

Estado

ANY

Accao

ACCEPT

Ligado:

\* Marcar caixas com (!) permite criar excepcoes (i.e. corresponder a tudo menos o 'match' inserido)

### Regras actuais:


ID	Fonte	Porta de origem	Destino	Porta de destino:	Protocolo	Estado	Accao	Ligado:	Seleccao	Mover
0	anywhere	all	172.16.0.4	all	all	ANY	ACCEPT	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="↑"/> <input type="button" value="↓"/>



Ligação Adetti




File Edit View Go Bookmarks Tools Window Help

Pragma: no-cache Cache-control: no-cache Connection: close Content-type: text/html



Linux Caixa Mágica

# PRO GUARD

**Ligacoes Activas**

Origem LAN (VERDE) / Destino Internet (VERMELHO)

Origem LAN (VERDE) / Destino Internet (VERMELHO)						
Protocolo	Fonte	Destino	Porta de origem:	Porta de destino:	Estado	
tcp	10.10.96.39	195.141.101.87	2051	4662	ESTABLISHED	
tcp	10.10.96.39	194.85.99.65	1655	4242	ESTABLISHED	
tcp	10.10.96.39	217.133.217.175	2638	4662	TIME_WAIT	
tcp	10.10.96.39	220.119.196.171	2576	4662	TIME_WAIT	
tcp	10.10.96.39	194.85.99.65	1399	4242	ESTABLISHED	
tcp	10.10.96.39	68.50.43.221	3358	4662	ESTABLISHED	
tcp	10.10.96.39	218.186.32.207	3701	43662	ESTABLISHED	
tcp	10.10.96.39	81.6.249.161	1351	4662	ESTABLISHED	
tcp	10.10.96.39	134.102.95.173	4707	4662	ESTABLISHED	
tcp	10.10.96.39	62.212.100.24	2910	4662	ESTABLISHED	
tcp	10.10.96.39	195.1.26.231	2141	80	ESTABLISHED	
tcp	10.10.96.39	217.232.244.99	1917	42662	ESTABLISHED	
tcp	10.10.96.39	194.85.99.65	3974	4242	ESTABLISHED	
tcp	10.10.96.39	217.133.213.246	1659	4662	ESTABLISHED	
tcp	10.10.96.250	195.23.126.144	2334	80	TIME_WAIT	
tcp	10.10.96.39	218.102.85.208	2883	4662	ESTABLISHED	
tcp	10.10.96.39	200.17.212.117	4633	8080	ESTABLISHED	
tcp	10.10.96.39	194.85.99.65	1362	4242	ESTABLISHED	





File Edit View Go Bookmarks Tools Window Help



Linux Caixa Mágica

# PRO GUARD





-  Principal
-  Estado
-  Serviços
-  Firewalling
-  VPN
-  Logs
-  Logs

### Definicao de SNAT (Source NAT):

IP interno

Destino \*

Porta de destino: \*

IP de saida

OU

Lista de IPs de saida (1 endereco por linha)

\* Branco para TODOS

Ligado:

---

**Regras actuais:**

ID	Protocolo	IP interno	Destino	Porta de destino:	IP de saida	Ligado	Selecione	Mover
0	ALL	172.16.0.4	all	all	193.136.190.97	✓	<input type="checkbox"/>	↑ ↓
1	ALL	10.10.96.0/24	all	all	193.136.190.65	✓	<input type="checkbox"/>	↑ ↓
2	ALL	172.16.0.3	193.136.188.4	all	193.136.190.65	✓	<input type="checkbox"/>	↑ ↓

SNAT



File Edit View Go Bookmarks Tools Window Help

---



Linux Caixa Mágica

# PRO GUARD





---

-  Principal
-  Estado
-  Serviços
-  Firewalling
-  VPN
-  Logs
-  Logs

### Definição de IPs virtuais:

Novo IP virtual

Máscara de Sub-Rede: \*

\* Se branco, uma escolha plausível de máscara de sub-rede será efectuada

---

### Tabela de Interfaces:

Interface	Endereco IP	Broadcast	Netmask	Remover
eth2	193.136.190.65	193.136.190.71	255.255.255.248	-
eth2:0	193.136.190.102	193.136.190.255	255.255.255.0	<input type="checkbox"/>
eth2:1	193.136.190.101	193.136.190.255	255.255.255.0	<input type="checkbox"/>
eth2:2	193.136.190.113	193.136.190.255	255.255.255.0	<input type="checkbox"/>
eth2:3	193.136.190.97	193.136.190.255	255.255.255.0	<input type="checkbox"/>

---

### Mensagens de erro:

---

[O CM PROGUARD](#) · [contactos](#) · [ADETTI](#)

IP Addressing





## Case de Utilização de Software Livre

- Los Alamos National Laboratory (25/10/2003)
  - Compra de um cluster Linux (1400x Opteron 64 bits) para modelação de armas nucleares
  - [http://www.gcn.com/22\\_24/inbrief/23252-1.html](http://www.gcn.com/22_24/inbrief/23252-1.html)
- NSA Security-Enhanced-Linux
  - Linux com características especiais de segurança
  - <http://www.nsa.gov/selinux/>



## Âmbito do protocolo ADETTI – CIE

- Disponibilização de tecnologia/ formação ProGuard
- Fornecimento do ambiente de desenvolvimento do ProGuard para o CIE poder utilizar na *IX box*
- Melhoramentos introduzidos pelo CIE serão incorporados em futuras versões
- Troca de experiências e conhecimentos na área da segurança informática



## Conclusões

- Protocolo reflecte várias oportunidades:
  - Software Livre como tendência emergente
  - Diminuição dependência de *vendors*, criação de tecnologia própria e reforçar a formação dos recursos humanos próprios
- Parceria Universidade/ Exército
  - Criar sinergias em áreas em que desenvolve trabalho comum
  - Melhora o produto, em ambos os sentidos



Obrigado.

Paulo.Trezentos@adetti.iscte.pt

- <http://www.caixamagica.pt>
- <http://www.adetti.pt>