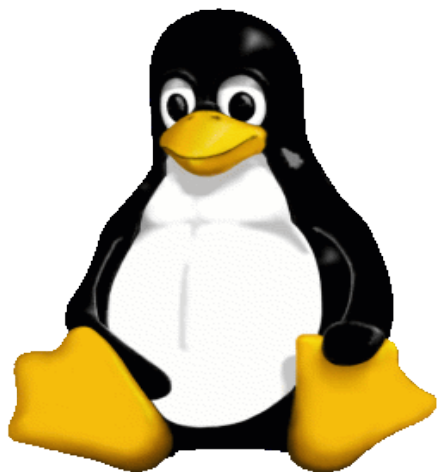


FOSS

Free Open Source Security



Bezpečnostní infrastruktura
s použitím Linuxu



Bezpečnost je služba

- nelze dosáhnout 100% zabezpečení
 - nové chyby v používaném software
 - nové techniky pro zneužívání chyb
 - social hacking
- práce na zabezpečování je kontinuální
 - stálé sledování informací o bezpečnosti (bugtraq, incidents)
 - sledování a analýza logů systémů přístupných z Internetu
 - NIDS & HIDS



Bezpečnostní řešení na Linuxu

- Open Source SW
 - firewally, šifrovací systémy, autentizace, IDS, log analysis
 - content filters, bandwidth management,
 - nadstavby pro usnadnění správy (filtergen, fwbuilder, guarddog, ipcop, webmin)
- Proprietární SW
 - firewally, šifrování, autentizace, IDS, antiviry
 - Check Point, Stonesoft, Intrusion.com, Trend Micro, Cryptocard



Proč použít Linux

- Jednoduchá a rychlá instalace, není nutné se starat o licence
- Vysoká konfigurovatelnost, většinou výborná dokumentace, rychlost
- Velký výběr komerčních i nekomerčních bezpečnostních produktů
- Bezpečná a rychlá vzdálená správa (ssh=cli + forwardování tcp portů, popř. https)
- Snadná automatizace běžných úkonů (cron, skripty)

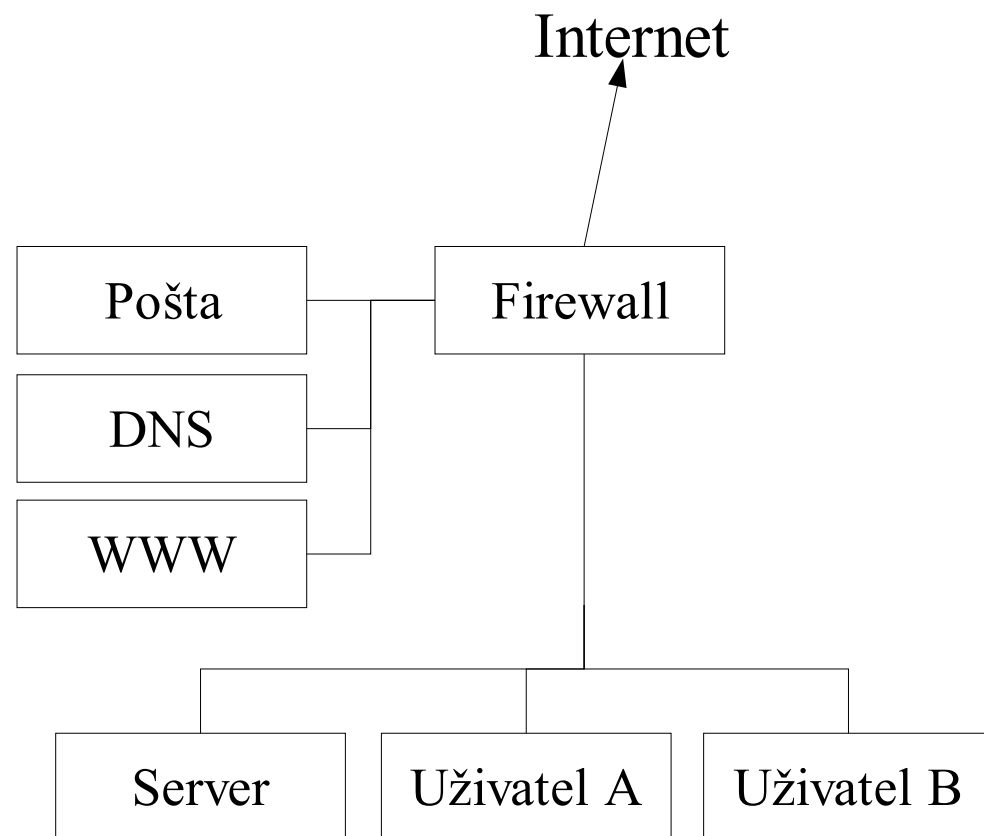


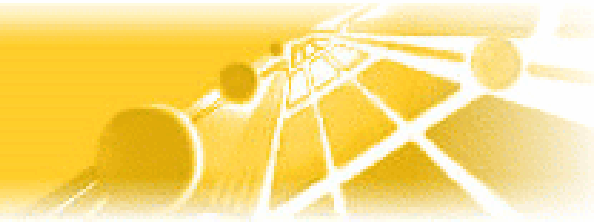
Nevýhody použití Linuxu

- Nutnost naučit se ho nastavit a používat (?)
- Velké rozdíly v distribucích, většina komerčních produktů podporuje jen RedHat, někdy dokonce jen určitou verzi jádra od RH
- Často nejsou k dispozici ovladače na nejnovější produkty nebo nejsou podporovány všechny funkce těchto produktů (mnohdy však bývá „Černý Petr“ na straně výrobce produktu)

Připojení k Internetu

- Firewall
- IDS
- Demilitarizovaná zóna
 - DNS server
 - Poštovní server
 - Antivirová brána
 - Proxy Cache
 - WWW server, FTP server a pod.





Firewalling

Kontrola spojení, navazovaných mezi sítěmi
s různou úrovní důvěryhodnosti

iptables

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
iptables -A OUTPUT -o eth+ -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -I INPUT -i eth+ -p tcp ! --syn -m state --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth+ -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -I INPUT -i eth+ -p udp -m state --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth+ -p icmp -j ACCEPT
iptables -A OUTPUT -o eth+ -j LOG
iptables -A OUTPUT -o eth+ -j DROP
iptables -A OUTPUT -o ppp+ -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -I INPUT -i ppp+ -p tcp ! --syn -m state --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o ppp+ -p udp -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -I INPUT -i ppp+ -p udp -m state --state ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o ppp+ -p icmp -j ACCEPT
iptables -A OUTPUT -o ppp+ -j LOG
iptables -A OUTPUT -o ppp+ -j DROP
iptables -A INPUT -i eth+ -p icmp -j ACCEPT
iptables -A INPUT -i eth+ -p tcp -m state --state NEW,ESTABLISHED --dport 137:139 -j DROP
iptables -A INPUT -i eth+ -p udp -m state --state NEW,ESTABLISHED --dport 137:139 -j DROP
iptables -A INPUT -i eth+ -p tcp -m state --state NEW,ESTABLISHED --dport 80 -j ACCEPT
iptables -I OUTPUT -o eth+ -p tcp ! --syn -m state --state ESTABLISHED --sport 80 -j ACCEPT
[... dalších 160+ pravidel se nevešlo ...]
```

filtergen

```
local {input lo; output lo} accept;
```

```
local output { eth+ ppp+ } {  
    proto { tcp udp icmp } accept;  
    log drop;  
};
```

```
local input { eth+ ppp+ } {  
    proto icmp accept;  
    proto {tcp udp} dport 137:139 drop;  
    proto tcp {  
        dport http accept;  
        source { 192.168.168.0/24 10.0.0.0/16 }  
            dport { ftp saft ssh cfengine }  
            accept;  
        source 194.228.107.242 dport cfengine accept;  
        source { medusa } dport { ftp 258 18190 } accept;  
        log drop;  
    };  
};
```

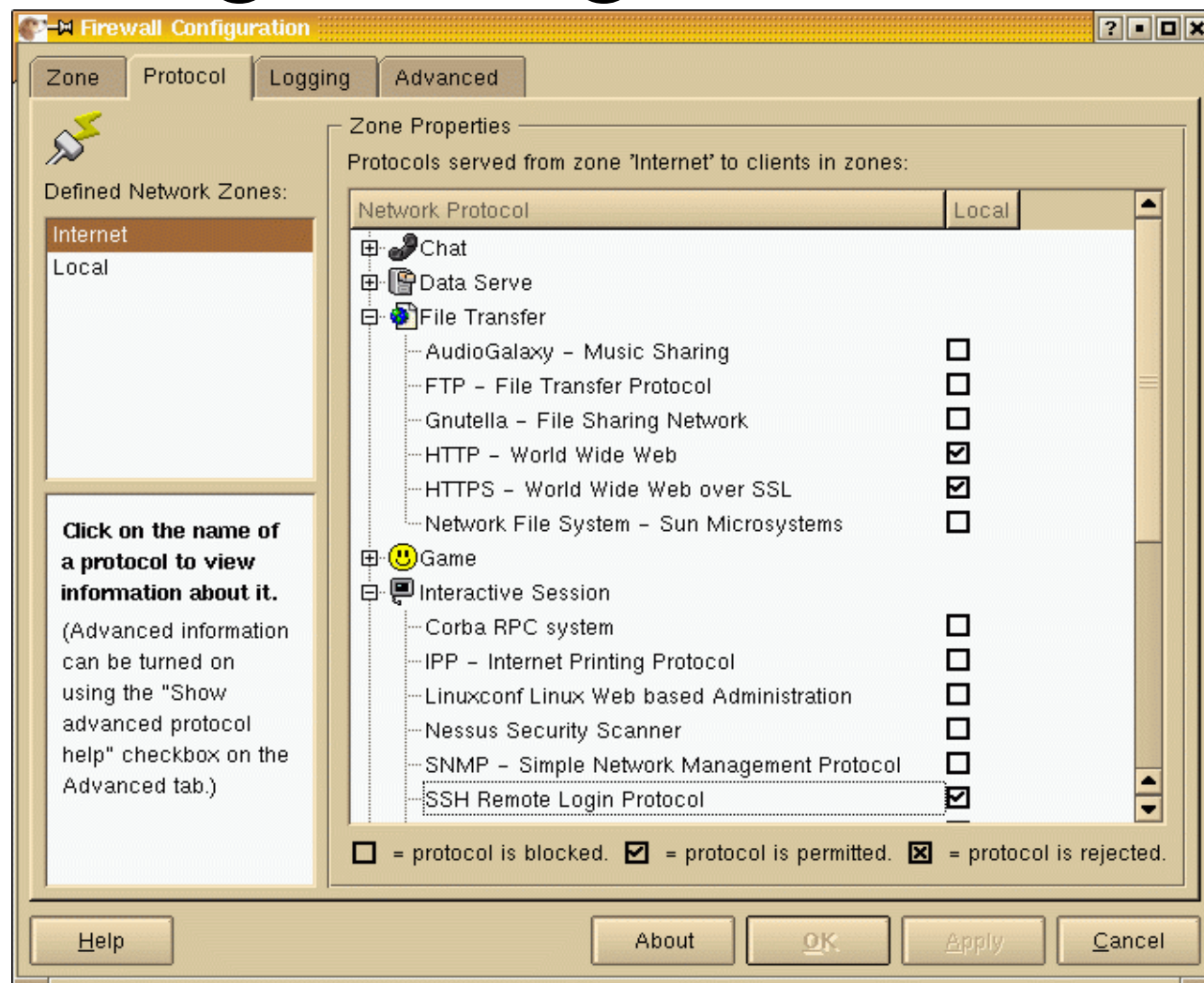
```
forward output { eth+ ppp+ } proto { tcp udp icmp } source 192.168.0.0/16 masq;
```

Targets:

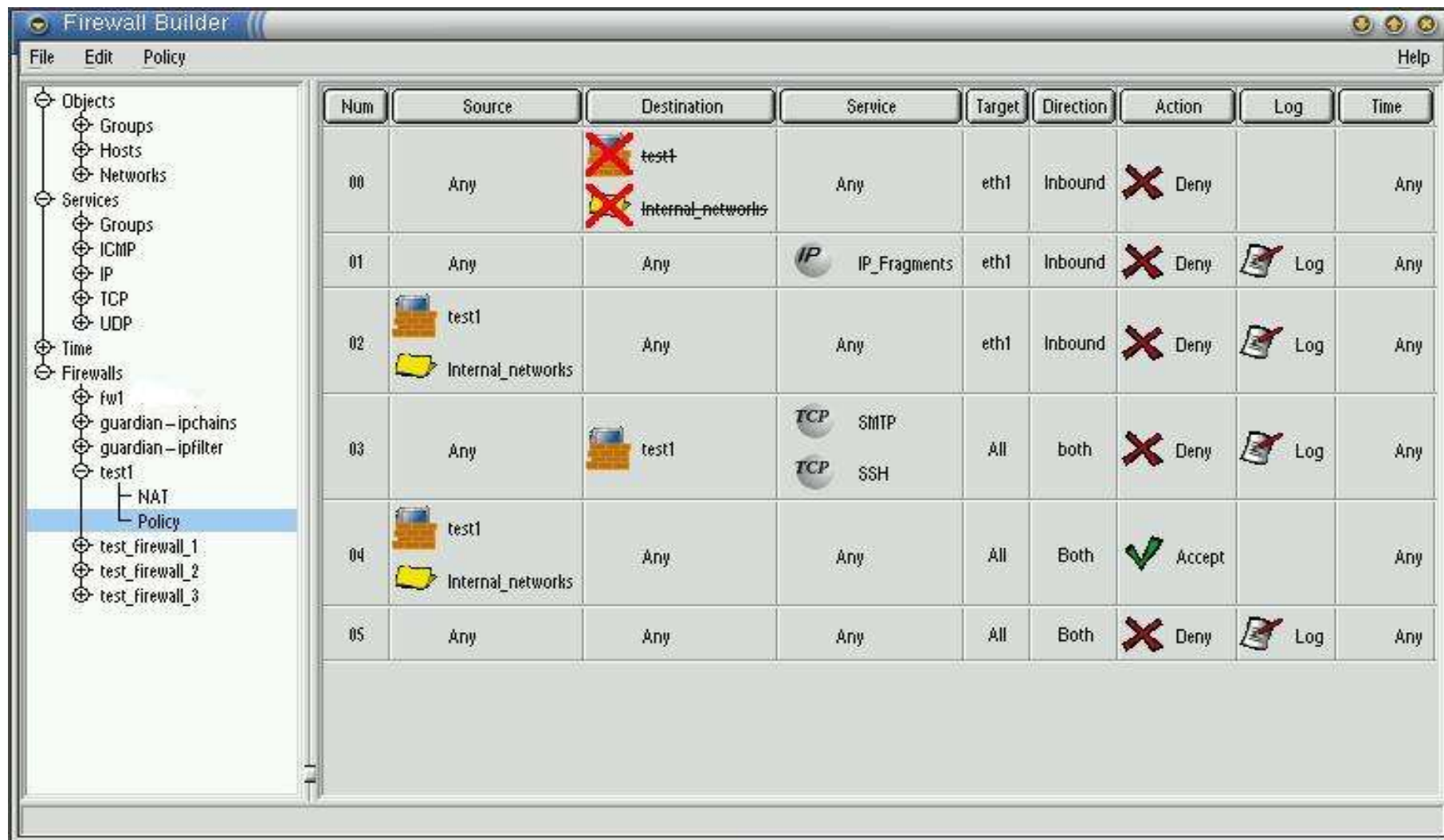
- iptables
- ipchains
- ipfilter
- cisco (acl)

guarddog

- IPTables
- Definice síťových zón
- Nastavení provozu mezi zónami
- Vhodné jako personal fw



fwbuilder



The screenshot shows the Firewall Builder application window. The interface includes a menu bar (File, Edit, Policy, Help), a left-hand tree view for 'Objects' and 'Firewalls', and a main table of firewall rules. The table has columns for Num, Source, Destination, Service, Target, Direction, Action, Log, and Time. Rule 04 is highlighted in blue, indicating it is the selected rule.

Num	Source	Destination	Service	Target	Direction	Action	Log	Time
00	Any	test1	Any	eth1	Inbound	Deny		Any
		Internal_networks						
01	Any	Any	IP_Fragments	eth1	Inbound	Deny		Any
02	test1	Any	Any	eth1	Inbound	Deny		Any
	Internal_networks							
03	Any	test1	SMTP SSH	All	both	Deny		Any
04	test1	Any	Any	All	Both	Accept		Any
	Internal_networks							
05	Any	Any	Any	All	Both	Deny		Any

IPCop

- Samostatná linuxová distribuce
- Správa přes www rozhraní
- IPTables firewa
- IDS snort
- Proxy server
- IPSEC VPN

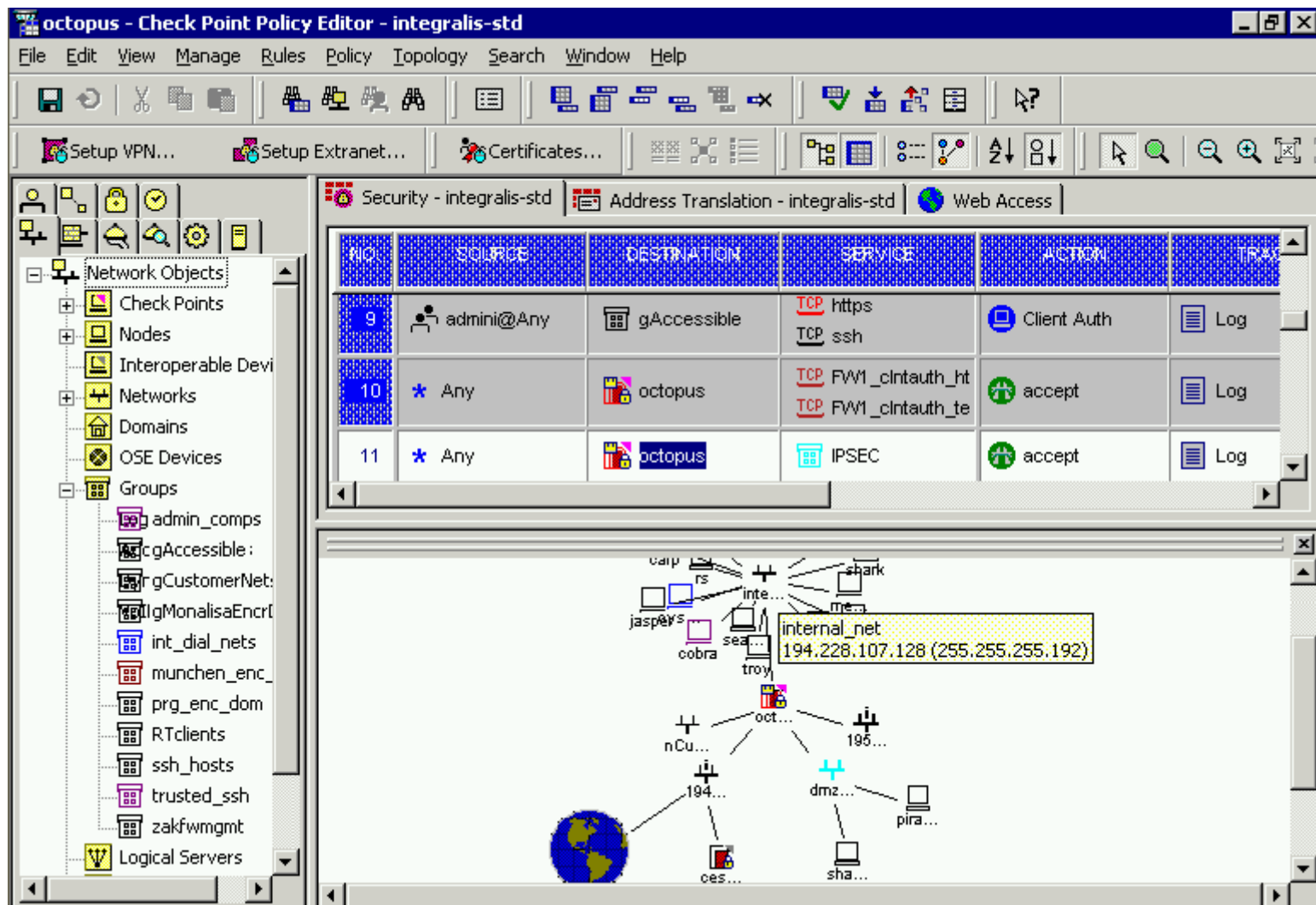


The screenshot shows the IPCop web interface. At the top, it features the IPCop logo with the slogan "The Bad Packets Stop Here" and a penguin mascot. Below this is a navigation menu with options like Home, Information, Dialup, Services, VPNs, Logs, and System. The main content area is titled "Web proxy configuration" and includes a sidebar with a SourceForge logo. The central panel displays the "Web proxy" settings, which are currently disabled. The settings include checkboxes for "Enabled" (unchecked) and "Transparent" (checked), and input fields for "Remote proxy", "Upstream username", "Upstream password", "Cache size (MB)", "Min object size (KB)", "Max object size (KB)", "Max incoming size (KB)", and "Max outgoing size (KB)".

Web proxy configuration		System: 9.1.15-000000.cz	IPCOP v1.3.0
the bad packets stop here			
web proxy dhcp port forwarding external aliases external service access dmz pinholes dynamic dns			
Web proxy:			
Enabled:	<input type="checkbox"/>	Remote proxy:	<input type="text"/>
Transparent:	<input checked="" type="checkbox"/>	Upstream username:	<input type="text"/>
		Upstream password:	<input type="text"/>
Cache size (MB):	<input type="text" value="50"/>	Max object size (KB):	<input type="text" value="4096"/>
Min object size (KB):	<input type="text" value="0"/>	Max incoming size (KB):	<input type="text" value="0"/>
		Max outgoing size (KB):	<input type="text" value="0"/>
● This field may be blank.			

Check Point

- Nejrozšířenější firewall na světě
- Vynikající centrální správa
- Linux (Red Hat / SecurePlatform), Solaris, IPSO, Windows, HP-UX, AIX
- Nemá GUI pro Linux
- Vyžaduje konkrétní verzi Red Hat kernelu



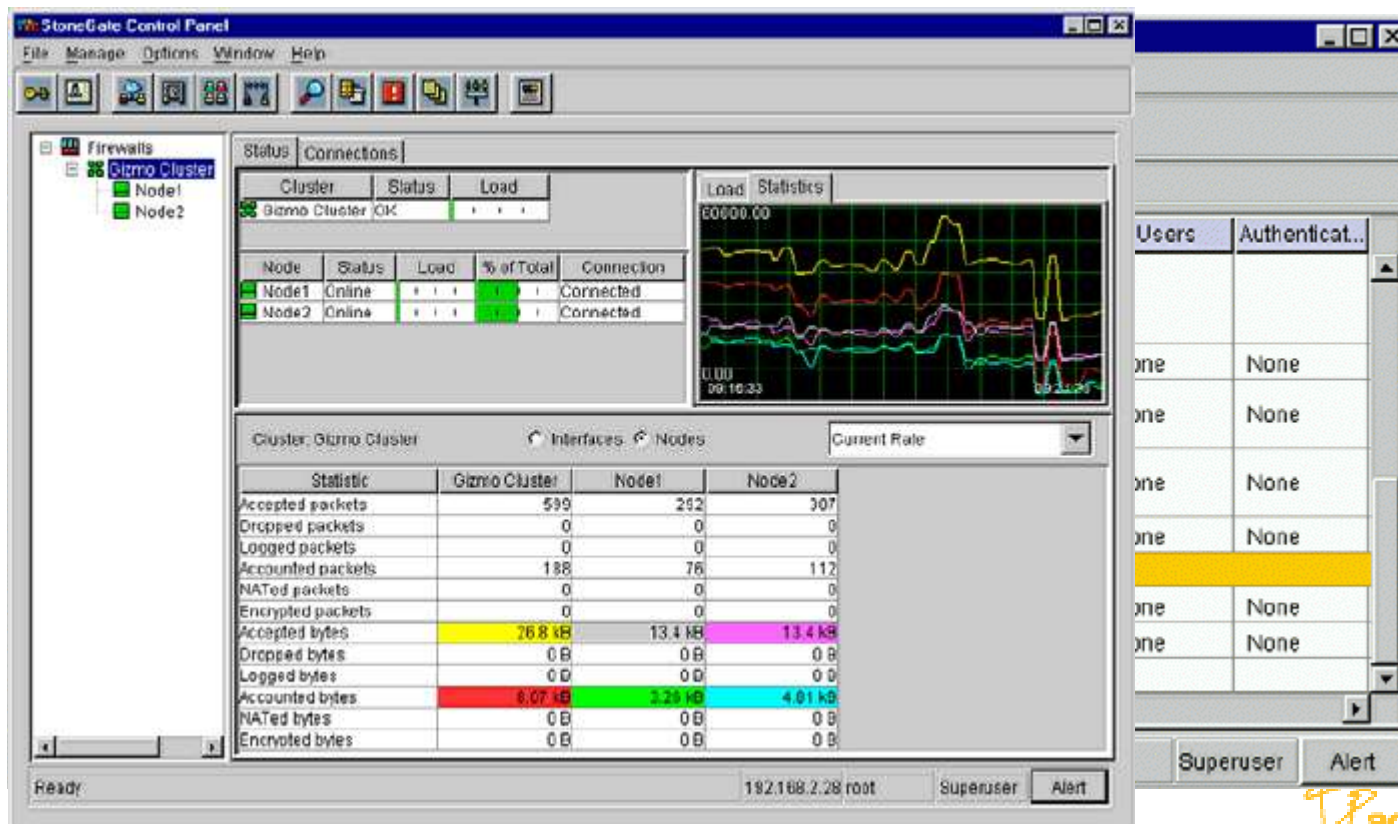
The screenshot shows the Check Point Policy Editor interface. The main window displays a table of rules with the following data:

ID	SOURCE	DESTINATION	SERVICE	ACTION	TRACK
9	admini@Any	gAccessible	TCP https TCP ssh	Client Auth	Log
10	* Any	octopus	TCP FW1_clntauth_ht TCP FW1_clntauth_te	accept	Log
11	* Any	octopus	IPSEC	accept	Log

Below the table is a network topology diagram showing various nodes and connections. A specific node labeled 'internal_net' is highlighted with a yellow box, showing its IP address range: 194.228.107.128 (255.255.255.192).

StoneGate

- Vlastní upravený linuxový operační systém na platformě Intel nebo Sparc
- Zabudovaná podpora High Availability (load balancing, podpora pro několik různých providerů, HA pro VPN přes různé providery)
- Možnost řetězení pravidel podobně jako ipchains / iptables
- GUI v Javě funguje i na Linuxu



The screenshot displays the StoneGate Control Panel interface. The main window shows the 'Status' and 'Connections' tabs. The 'Status' tab displays the following information:

Cluster	Status	Load
Gizmo Cluster	OK	...

The 'Connections' tab shows a table of active connections:

Node	Status	Load	% of Total	Connection
Node1	Online	Connected
Node2	Online	Connected

Below the connection table, there is a 'Load Statistics' graph showing network activity over time. At the bottom, a detailed statistics table is provided:

Statistic	Gizmo Cluster	Node1	Node2
Accepted packets	599	292	307
Dropped packets	0	0	0
Logged packets	0	0	0
Accounted packets	188	76	112
NATed packets	0	0	0
Encrypted packets	0	0	0
Accepted bytes	76.8 kB	13.4 kB	13.4 kB
Dropped bytes	0 B	0 B	0 B
Logged bytes	0 B	0 B	0 B
Accounted bytes	6.07 kB	3.29 kB	4.01 kB
NATed bytes	0 B	0 B	0 B
Encrypted bytes	0 B	0 B	0 B

The interface also includes a 'Users' table on the right side, showing authentication status for various users, and a status bar at the bottom indicating the system is 'Ready' and the user is 'Superuser'.

Šifrování

Virtual Private Networks

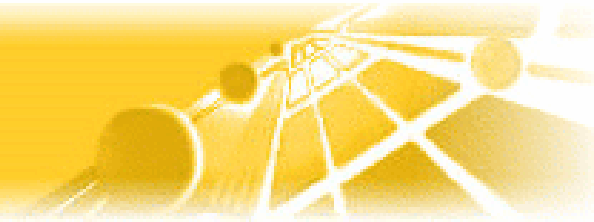
Souborové šifrovací systémy

Subsystemy, rozhraní API



Šifrovací programy

- OSS
 - FreeS/WAN, CIPE, VTun, Secure Shell
 - GnuPG
 - cfs, tcfs, cryptoapi (kerneli), bcrypt
- Komerční
 - VPN-1, StoneGate
 - PGP
 - BestCrypt



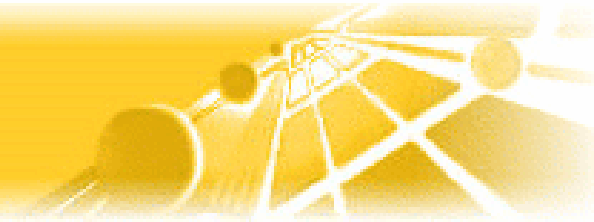
Autentizace

Ověření totožnosti



Druhy autentizace

- Tradiční, zcela nedostatečná
 - statické heslo + přenos jména a hesla po síti v cleartextu
- Silnější, přijatelná pro většinu použití za předpokladu dostatečné ukázněnosti uživatelů
 - statické heslo + challenge response
 - passphrase + RSA/DSA keys
- Silná (opět za předpokladu ukázněnosti uživatelů)
 - dvoufaktorová autentizace, jednorázová hesla, biometrika + veškerá komunikace šifrovaná



Produkty pro autentizaci

- Volně dostupné
 - s/key (palm - pilOTP, linux)
 - rsa/dsa keys (ssh)
- Komerční
 - RSA SecurID
 - Cryptocard
 - Čipové karty, USB tokens
 - Biometrika

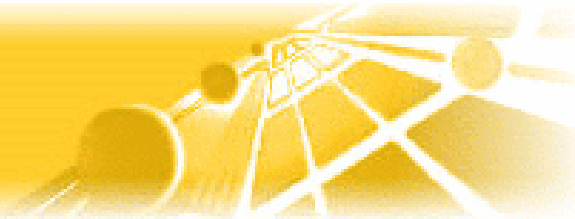
IDS

Intrusion Detection Systems
Systémy pro varování před útoky



Druhy IDS

- NIDS (Network IDS)
 - sledování a analýza provozu na síti
 - snort, firestorm, Prelude, ISS Realsecure, Cisco IDS
- HIDS (Host IDS)
 - sledování systémových logů, činnosti přihlášených uživatelů, změn na souborovém systému
 - host sentry, aide, tripwire, LIDS
- Ostatní
 - antiviry



Proxy, systémy správy obsahu

- Proxy servery

SQUID

- výkonný proxy server s možstvím voleb

- Systémy správy obsahu

squidGuard

- doplnění filtrovacích funkcí SQUIDu, blacklisty

Dans Guardian

- samostatný proxy server, rozšířené možnosti filtrování, podpora PICS frází, blacklistů, URL regexp., MIME filtering, blokování uploadu, stealth mode



Správa bezpečnostních systémů

Linux je více než vhodná platforma pro správu a testování bezpečnostních systémů.

- Testování systémů – nmap, nessus, xprobe, nemesis
- Zpracování dat – cron, perl, calamaris, fwlogview
- Správa systémů – ssh, cfengine, screen, script, webmin
- Monitoring – nagios, mrtg/rrdtool, big brother



Zdroje

- Firewalling
 - filtergen: <http://hairy.beasts.org/filter/>
 - guarddog: <http://www.simonzone.com/software/guarddog/>
 - fwbuilder: <http://www.fwbuilder.org/>
 - Check Point FireWall-1 NG: <http://www.checkpoint.com/ng/>
 - Stonesoft StoneGate: <http://www.stonesoft.com/products/StoneGate/>
- Šifrování
 - <http://www.freeswan.org/>, <http://sites.inka.de/bigred/devel/cipe.html>
 - <http://vtun.sourceforge.net/>, <http://www.jetico.com/>, www.kerneli.org
 - <http://www.gnupg.org/>, <http://www.pgpi.com/>

Zdroje

- Autentizace
 - <http://www.palmgear.com/software/showsoftware.cfm?prodID=440>
 - <http://www.rsasecurity.com/>, <http://www.cryptocard.com/>
- IDS
 - <http://www.snort.org/>, <http://acidlab.sourceforge.net/>
 - <http://www.prelude-ids.org/>, <http://www.lids.org/>
 - <http://www.scaramanga.co.uk/firestorm/>
- Proxy, správa obsahu
 - <http://www.squid-cache.org/>
 - <http://dansguardian.org/>

Q & A

Děkuji za pozornost

Martin Slavík
msl@actinet.cz