ROMAB
ROBERT MALMGREN AB

Brandväggar för hemmabruk och småkontor

Andreas Jonsson
andreas@romab.com

ROMAB
ROBERT MALMGREN AB

Brandväggar som testats

Namn	Lan-Portar	WAN-portar	VPN-terminering	IPS/IDS	Antivirus-koppling	Pris
Monowall / Soekris Net 4501	2	1	Ja	Nej	Nej	1600
Symantec Gateway Security 360	8	2	Ja	IPS	Ja	8000
SurfinBird GateFW	2	1	Nej	Nej	Nej	1800
Linksys RV082 VPN Router	8	2	Ja	Nej	Nej	7000
Billion Broadband router	4	1	Ja	Nej	Nej	495
Cyberguard SG300	4	1	Ja	IDS	Nej	2150
Sonicwall tz170sp	6	1	Ja	IPS*	Ja*	6-12000

ROMAB
ROBERT MALMGREN AB

Utrustningen

ROMAB
ROBERT MALMGREN AB

Problem

- Loggning
  - Ofta för lite, ibland inte alls
- Regelhantering
  - Finkontroll av regler
- Buggar
  - Många buggar I de olika produkterna: funktioner trillar bort, prestandaproblem

ROMAB
ROBERT MALMGREN AB

Problem

- Prestanda
  - Ibland sämre än DSL-leverantörens bandbredd…
- Lätt att tro att de är säkrare än de är
- För många finesser…
  - Varför bry sig om ”IDS/IPS” när funktionen är medlagd bara för att bli en till i faktabladet?

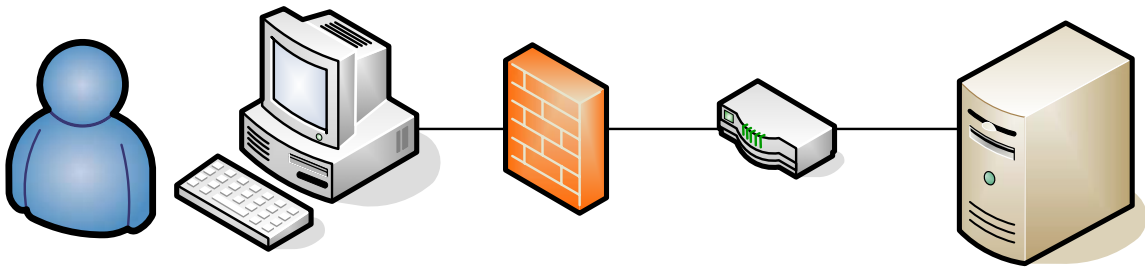
ROMAB
ROBERT MALMGREN AB

Loggning

UTC Time	Message	Source	Destination	Note
10/15/2004 16:57:06.16	Blocked - Port Scan Attack	194.52.231.20:32529	194.52.231.26:50069	TCP
10/15/2004 16:55:51.31	Blocked - Port Scan Attack	194.52.231.20:32529	194.52.231.26:50069	TCP
10/15/2004 16:54:36.46	Blocked - Port Scan Attack	194.52.231.20:32529	194.52.231.26:50069	TCP
10/15/2004 16:54:18.96	Packet dropped because TCP flag combination 0x29 is invalid			
10/15/2004 16:54:18.96	Packet dropped because TCP flag combination 0x2b is invalid			
10/15/2004 16:54:18.96	Packet dropped because TCP flag combination 0x0 is invalid			
10/15/2004 16:54:16.86	Packet dropped because TCP flag combination 0x29 is invalid			
10/15/2004 16:54:16.86	Packet dropped because TCP flag combination 0x2b is invalid			
10/15/2004 16:54:16.86	Packet dropped because TCP flag combination 0x0 is invalid			
10/15/2004 16:54:11.06	Packet dropped because TCP flag combination 0x29 is invalid			
10/15/2004 16:54:11.06	Packet dropped because TCP flag combination 0x2b is invalid			
10/15/2004 16:54:11.06	Packet dropped because TCP flag combination 0x0 is invalid			
10/15/2004 16:54:09.01	Packet dropped because TCP flag combination 0x29 is invalid			
10/15/2004 16:54:09.01	Packet dropped because TCP flag combination 0x2b is invalid			
10/15/2004 16:54:09.01	Packet dropped because TCP flag combination 0x0 is invalid			
10/15/2004 16:54:03.21	Packet dropped because TCP flag combination 0x29 is invalid			
10/15/2004 16:54:03.21	Packet dropped because TCP flag combination 0x2b is invalid			
10/15/2004 16:54:03.21	Packet dropped because TCP flag combination 0x0 is invalid			
10/15/2004 16:54:01.11	Packet dropped because TCP flag combination 0x29 is invalid			

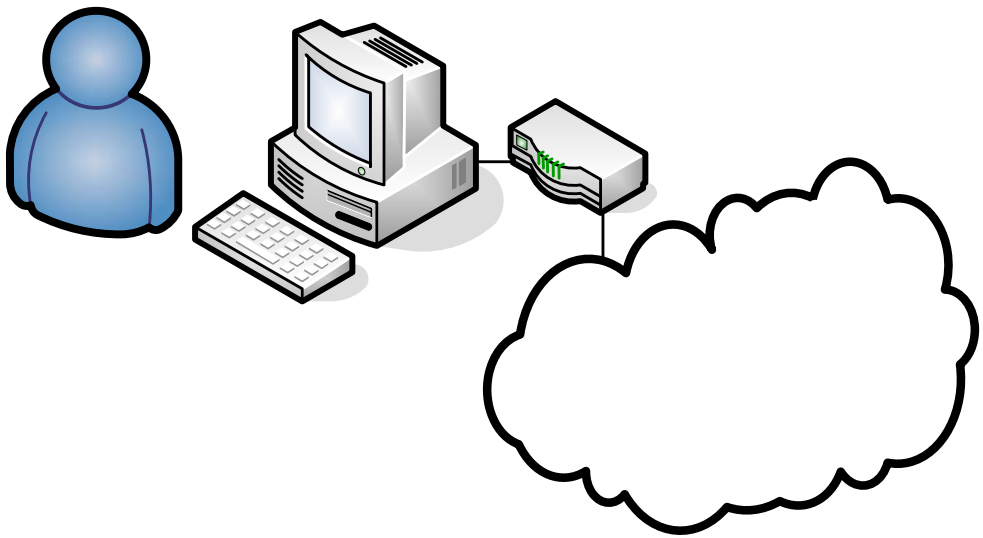
ROMAB
ROBERT MALMGREN AB

Prestandatest, nätskiss



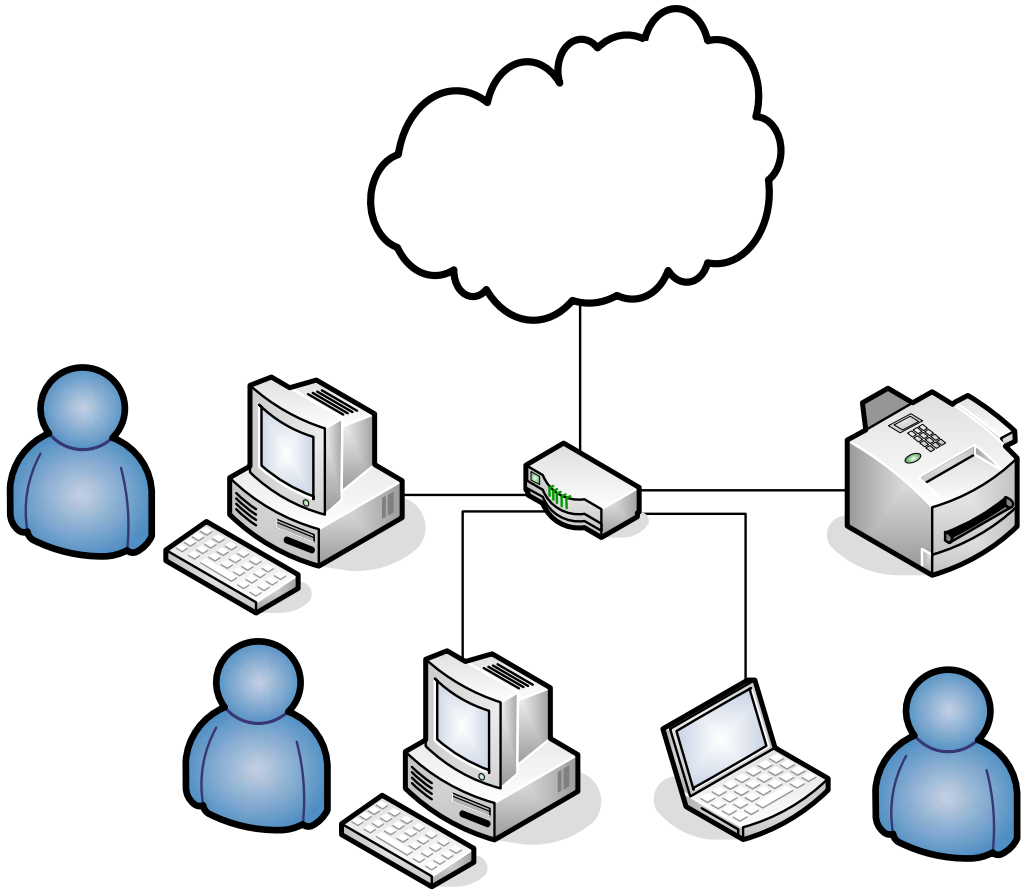
ROMAB
ROBERT MALMGREN AB

Enkel hemarbetsplats



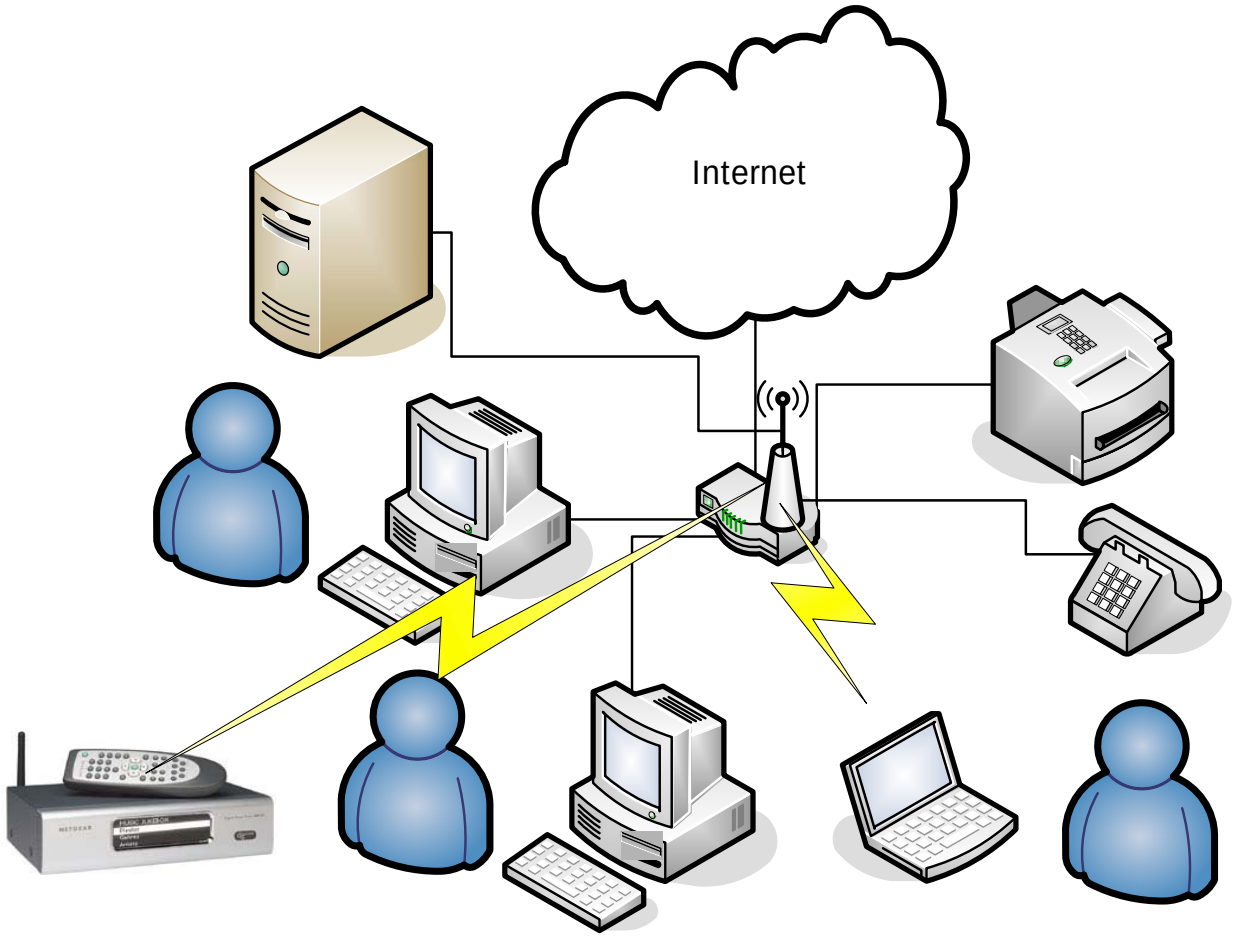
ROMAB
ROBERT MALMGREN AB

Vanligare scenario hemma…



ROMAB
ROBERT MALMGREN AB

(Snart) standardscenario hemma…



ROMAB
ROBERT MALMGREN AB

Prestanda

Namn	*Mottagning TCP*	*Sändning TCP*
Cyberguard SG 300	18.15 Mbit/s	18.34 Mbit/s
Monowall / Soekris net4501	18.17 Mbit/s	18.15 Mbit/s
Billion VPN Firewall router	8.09 Mbit/s	4.17 Mbit/s
Sonicwall tz170sp	7.24 Mbit/s	605.99 Kbit/s
Symantec Gateway security 360	45.75 Mbit/s	45.49 Mbit/s
Linksys RV082	45.01 Mbit/s	49.93 Mbit/s
SurfinBird GateFW AirSIP plus	11.00 Mbit/s	10.87 Mbit/s
FreeBSD 5.1-release-p17	73.4 Mbit/s	93.4 Mbit/s

TPTest klient + egen server. Serverversion 3.7.1

ROMAB
ROBERT MALMGREN AB

Less is more

- En brandvägg är en brandvägg. Onödiga funktioner bör ej vara med av säkerhetsskäl.
  - Tex möjligheten att låta brandväggen kontrollera om det finns ny Epost.

ROMAB
ROBERT MALMGREN AB

Rekommendationer

- För hemanvändare anser jag att Surfinbird är den bäst lämpade.
- För den avancerade användaren skulle jag rekommendera Monowall eller SG300
- Det lilla företaget bör överväga Linksys , symantec eller SG300. Kanske även sonicwall om prestandan förbättras.

ROMAB
ROBERT MALMGREN AB

Slutsatser

- Generationsskifte av hembrandväggar då hemanslutningar blir allt snabbare
- Loggning är den svagaste punkten
- Ständig fråga – dags för uppgradering?
- Svår balansgång mellan enkelhet och finkontroll