Test av Brandväggar för hemmabruk

Version 0.9
Datum: 2004-10-30

Sammanfattning

SNUS har utfört en serie tester av brandväggar riktade mot småföretags- och hemmarknaden.

Logghantering i dessa brandväggar lämnar en del att önska - såväl funktionsmässigt som innehållsmässigt.

Den brandvägg jag rekommenderar med pris och lättanvänlighet i åtanke är Intertex SurfinBird Gate FW.

Innehållsförteckning

Lista över figurer

Lista över tabeller

Upphovsrättslig status

Kontaktinformation

Föreningen Swedish Network Users' Society är en ideell förening för alla som är intresserade av datorkommunikation, nätverksteknologi och Internet. Medlemsavgiften är 250 kr/år.

Adress:

Swedish Network Users' Society
Box 3051
169 03 SOLNA

Webbsida: http://www.snus.se
E-post: info@snus.se

Dokumentets utformning

Rapporten är primärt en sammanställning av de testprotokoll som skapats under testerna av brandväggarna. Inledningsvis ges en överblick av testerna samt allmänna omdömen.

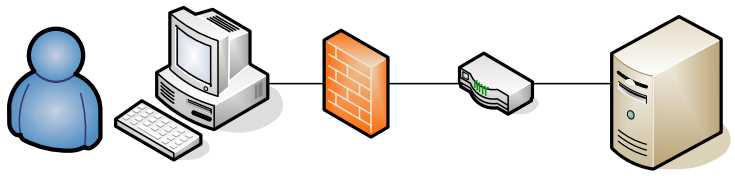
Bakgrund

Som en aktivitet inom IP-country och Internetdagarna 2004 anordnade Swedish Network Users' Society, SNUS, en test av hårdvarubaserade småbrandväggar. Brandväggar har ställts till förfogande av leverantörer och privatpersoner. Små brandväggar för hemanvändare och småföretag kan uppvisa ett förvånande bra pris och många funktioner – den stora frågan man ställer sig är ifall de håller måttet. Denna test har givit svar på några av de vanligaste frågorna rörande funktionalitet, säkerhet och prestanda.

Arbetet har varit relaterat till den samtidigt pågående aktiviteten med distansarbete som SNUS anordnat. Distansarbetsaktiviteten finns redovisad i en separat rapport ifrån SNUS, rapport 2004-01.

Arbetets utformning

Allt testarbete har utförts av Andreas Jonsson andreas@romab.com under loppet av ca två veckors tid. Testerna har genomförts med hjälp av ett laborationsnätverk som delvis varit anslutet till Internet. Labbnätets utformning kan ses i figur 1.



Figur 1 Översiktsbild av testmiljö

Vid testerna har följande applikationer använts:

- Punk
- tcpdump
- Ethereal
- nmap
- ping
- TPTEST
- Diverse standardiserade UNIX-program i FreeBSD.

Utformning- och skrivande av rapport, textbearbetning samt tekniskt stöd utfört av Robert Malmgren, rom@romab.com. Tryck, distribution och textbearbetning utfört av Joakim Fallsjö, fallsjo@sanchin.se

Introduktion

Detta test av brandväggar för hemmabruk och för små och medelstora företag har haft fokus på funktionalitet och användarvänlighet. Vi har dock även tittat på andra aspekter såsom kostnad, avancerade funktioner, prestanda, etc.

En anledning till att många skaffar sig en hårdvarubaserad brandvägg är att man behöver mer IP-adresser än vad bredbandsleverantören tillhandahåller. En annan anledning är att man kanske inte riktigt litar på mjukvarubaserade brandväggar. En tredje anledning brukar vara att man vill ha en trådlös anslutningspunkt – en s.k. accesspunkt, och att man då väljer en integrerad lösning som tillhanda håller alla tjänsterna. Ofta pratar man om utrustningen som ”SOHO-utrustning”, dvs ”Small Office/Home Office”.

Priset på små brandväggar startar på några hundralappar och går upp till tusenlappar och upp till ca 15000. SNUS har valt att titta på något dyrare brandväggar, ofta i klassen runt 2000 kr, men några billigare och några dyrare brandväggar är med i testen.

Tabellen nedan sammanställer de produkter som omfattades av testen. Marknaden för SOHO-utrustning är omfattande, varför ett urval har fått göras. Vi har valt att testa utrustning som har lite mer funktioner än de allra enklaste och billigaste utrustningen – man kan säga att vi valt att testa snäppet dyrare SOHO-utrustning än den som i princip enbart attraherar hemanvändarna. Anledningen är att vi velat testa utrustning som även kan användas av små- och mellanstora organisationer och företag.

Namn	*Lan-portar*	*WAN-portar*	*Pris*
Monowall / Soekris Net 4501	2	1	1600*
Symantec Gateway Security 360	8	2	8000
Intertex SurfinBird Gate FW	2	1	1800
Linksys rv082 VPN Router	8	2	7000
Billion Broadband router	4	1	495
Cyberguard SG300	4	1	2150
Sonicwall tz170sp	6	1	6-12000

* Enbart hårdvarukostnad, fri mjukvara

Tabell 1 Produkternas portar och pris

I nedanstående tabell sammanställs några av de mer avancerade funktionerna som de olika produkterna erbjuder. Kan produkten skapa och terminera VPN-anslutningar via IPSec? Eller har den möjlighet att detektera, eller till och med avvärja, attackförsök? Finns det kopplingar direkt från brandväggen till antivirusprogrammen så man kan filtrera nätinnehåll efter virus och maskar?

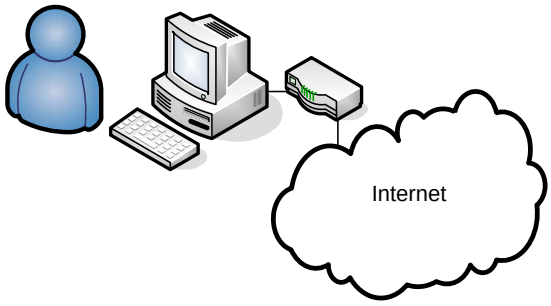
Namn	***VPN terminering***	***IPS/IDS***	***Antiviruskoppling***
Monowall / Soekris Net 4501	Ja	Nej	Nej
Symantec Gateway Security 360	Ja	IPS	Ja
Intertex SurfinBird Gate FW	Nej	Nej	Nej
Linksys rv082 VPN Router	Ja	Nej	Nej
Billion Broadband router	Ja	Nej	Nej
Cyberguard SG300	Ja	IDS	Nej
Sonicwall tz170sp *	Ja	IPS*	Ja*

* Kräver uppgradering.

Tabell 2 Produkternas avancerade funktioner

Olika brandväggscenarios

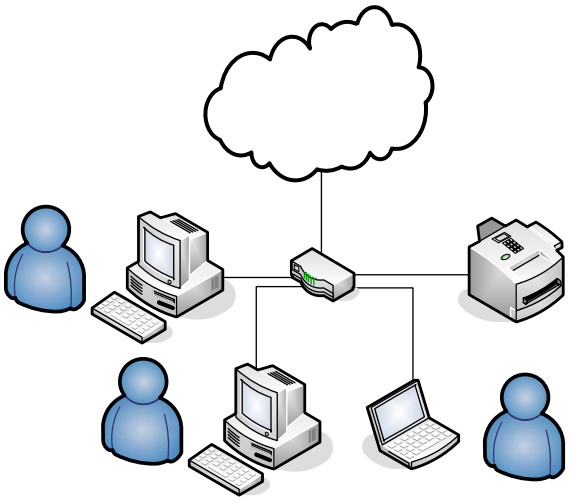
Det mest grundläggande scenariot är en PC-dator som är anslutet till Internet via en router med enkel filtrering eller adressöversättning. Anslutningsutrustningen erbjuder en port för att ansluta egen utrustning.



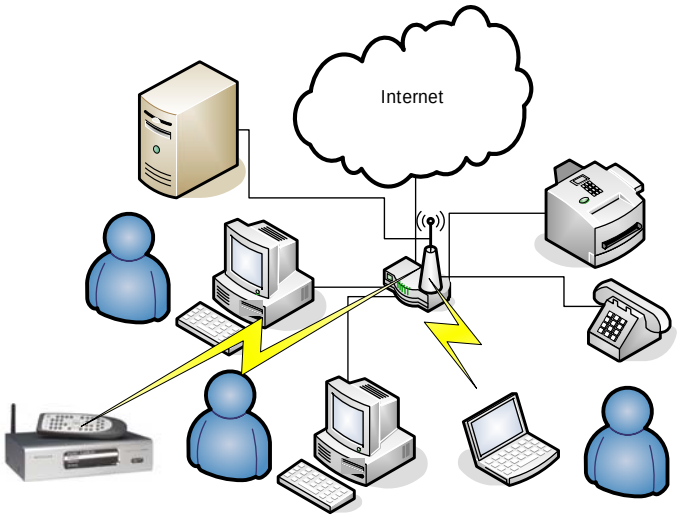
Figur 2 PC med enkel bredbandsrouter

Ett mer sannolikt scenario är att fler och fler hemanvändare bygger lokala nätverk, s.k. hemmanät, dit fler datorer och annan nätverkskapabel utrustning, såsom kombinations-maskiner (skrivare/fax/kopiatorer), ansluts, se figur 3. För detta behövs en brandvägg som klarar mer portar, alternativt att brandväggen kombineras med egen switch

Ett exempel på en annan trend är att hemutrustning har fått nätverksmöjligheter. TV-spelskonsoler såsom Xbox, stereoutrustning såsom NetGear:s spelare, etc. Man kan också ha egna serverdatorer hemma, både för eget bruk och för att erbjuda tjänster ut mot Internet, tex webb. Se figur 4.



Figur 3 Hemnät med arbets-PC, Hem-PC, bärbar dator samt skrivar/fax/scannerkombination



Figur 4 Mer avancerat hemnät med server, ljudanäggning och telefon ansluten till nätet

Uppgradering

Som regel kan man säga att all utrustning mjuvarumässigt måste uppgraderas från tid till annan. Det kan bero på att viss funktionalitet inte är brukbar eller fungerar felaktigt. Det kan bero på att någon hittar ett nytt säkerhetsproblem i produkten. Det kan också bero på att någon hittar ett nytt attacksätt eller en variant på ett äldre attacksätt som brandväggen, eller någon av de inbyggda funktionerna såsom IDS/IPS, måste utökas att hantera. En annan regel är att det i princip alltid finns en mer aktuell programversion att ladda ner ifrån leverantören än den som levereras med utrustningen som standard.

En till regel med uppgradering är att vi fann att de flesta produkterna fick bättre prestanda i samband med att man uppgraderade produkterna. Se kapitel ”Prestanda”, sid 15.

Det finns alltid problem med uppgradering av utrustning. Ett problem är att installationen kan misslyckas och leda till att utrustningen blir oanvändbar. Ett annat problem är att viss funktion kan ändras, i negativ bemärkelse, eller försvinna när man går från en version till en annan. Ett exempel vi fann vid testerna är att loggningen slutade fungera i samband med uppgraderingen på en av produkterna.

Loggning

Loggning är ett en viktig funktion hos alla säkerhetssystem, inte minst brandväggar. Tyvärr förefaller de flesta ”småbrandväggar” lida av olika problem i logghanteringen. Antingen innehåller loggarna alltför lite information och detta beror i stor del på det mycket begränsade minnesutrymmet i utrustningen. Ett annat problem är att många produkter innehåller buggar och felaktigheter i logghanteringen.

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			

Figur 5 Exempel på felaktiga loggar - adresserna har fallit bort

Då nästan alla brandväggarna har stöd för att logga mot en s.k. syslogserver är det inget större problem att lösa detta på ett mindre kontor. Tyvärr så kommer en hemanvändare förmodligen inte spendera särskilt mycket tid på att läsa loggar, eller ens förstå dem.

Prestanda

En viktig egenskap hos all nätverksansluten utrustning är att förstå vilken nätverksprestanda de har.

Vi använde programmet TPTEST för att utföra testerna. En klientdel och en serverdel installerades. På serversidan använde vi version 3.1.7 för UNIX.

Man kan konstatera att flera av utrustningarna inte har den prestanda som många bredbandsleverantörer idag tillhandahåller. Det kan vara ett problem då många klagar hos sin leverantör, men att flaskhalsen i själva verket sitter i utrustningen.

Namn	***Mottagning TCP. Mbit/s***	***Sändning TCP. Mbit/s***
Monowall / Soekris Net 4501	18.17	18.15
Billion Broadband router	8.09	4.17
Cyberguard SG 300	18.15	18.34
Sonicwall tz170sp	7.24	0.60599
Symantec Gateway Security 360	45.75	45.49
Linksys rv082 VPN Router	45.01	49.93
Intertex SurfinBird Gate FW AirSIP plus	11.00	10.87
FreeBSD 5.1-release-p17	73.4	93.4

Tabell 3 Produkternas prestanda

Notera att FreeBSD-5.1 användes som klient och serverdel, och att vi därför redogör separat för prestandan I den utrustningen så att det framgår att operativsystemet inte varit den begränsande faktorn i testutrustningen.

Vi fann att prestandan ökade i samband med att vi uppgraderade vissa av produkterna till att använda en modernare version av styrprogramvaran.

Monowall / Soekris Net4501

Monowall är en fritt tillgänglig brandväggslösning baserad på paketfiltreringsmotorn *ipfilter*. Monowall bygger på en specialanpassad, främst utrymmesmässigt nerbantad, version av det Berkeley-unixbaserade operativsystemet *FreeBSD*, version 4.9.

Figur 6 Soekris PC avsedd för lösningar baserade på fria operativsystem, exempelvis Monowall

Brandväggen har ett enkelt och lättarbetat webbaserat användargränssnitt. Monowall har inte särskilt mycket funktioner i förhållande till de andra brandväggarna som testats, men de grundläggande funktionerna och många avancerade finns i systemet. Att Monowall inte har alla upptänkliga funktioner blir en styrka såväl som en nackdel.

Det finns inga ”wizards” som hjälpmedel för installation eller konfiguration i Monowall, så redan där ställs krav på användaren, men har användaren har en grundläggande förståelse av nätverk så är Monowall:s administration väldigt enkelt.

1. Grundläggande brandväggsfunktionalitet

Vilka protokoll klaras av?

1.1.1 TCP

Ja.

1.1.2 UDP

Ja.

1.1.3 ICMP

Ja.

1.1.4 RTP

Nej.

1.2.1 Vilka metoder används för att blockera trafik?

1.2.2 Block

Ja.

1.2.3 Reject

Ja.

1.2.4 Pass

Ja.

1.2.5 ICMP-TYPES

Nej, stöd finns i Ipfilter men inte i monowall-guiet.

1.2.6 Specifiering av port

Ja.

1.2.7 Är den statefull?

Ja.

1.2.8 Klarar den routing?

Ja
Vilka routing protokoll stödjs?

Static routes

1.2.9 Klarar den bryggning?

Ja. Dock problem med bryggning och NAT, vilket tros bero på implimentationen av ipfilter under FreeBSD.
Kan den att vara helt transparent?

Nej.

1.2.10 Klarar den olika regelverk på olika interface

Ja.

1.3.1 Loggning

1.3.2 Hur hanteras loggning?

Du ställer in under en viss regel att det ska loggas. Default så loggas ”default block”-regeln. Lite diskspace under de flesta omständigheter, så användade av loggserver rekommenderas eller att man väljer att bara logga vissa regler.

1.3.3 Hur ser loggarna ut?

Vanliga ASCII ipfilter-loggar.

1.3.4 Kan man få dem binärt i tcpdump format?

Nej.

1.3.5 Är det lätt att ta ut / exportera loggar?

Ja.

1.3.6 Klarar den fjärrloggning till loggserver?

Ja.

1.3.7 Kan den adressöversätta ipadresser i loggar?

Nej.

2. Avancead brandväggsfunktionalitet

2.1.1 Koppling till antivirusprogram för viruskontroll av överförd data

Nej.

2.2.1 IDS och /eller IPS-funktionalitet

Nej.

2.3.1 Vpn-funktionalitet

Ja.

2.3.2 IPSEC

Ja.

2.3.3 SSLVPN

Nej.

2.3.4 UDP-Inkapsling

Nej.

2.3.5 Prestandatester för VPN-funktionalitet

3. Säkerhetstester, postivita och negativa tester samt fel

3.1.1 Hur hanteras enkla portscans?

Precis som ipfilter så blockar den varje paket som matchar reglen, vilket ger så många entries i loggen som portar som scannats. Ingen ”portscan-detection” med andra ord.

3.1.2 Fin-scan?

Blockar, loggar som finscan.

3.1.3 Klarar den att blocka x-masscan i olika varrianter?

Samma beteende som med FIN-scann.

3.1.4 Släpper den igenom trafik om man kör precis när den bootar?

Nej.

3.1.5 Utgående trafik?

Nej.

3.1.6 Kan man nå administrationsinterfacet från WAN-porten?

Nej.

4. Administration och användargränssnitt

4.1.1 Är andvändargränssnitet intiutivt och lättarbetat?

Ja.

4.1.2 Fungerar det med mozilla/opera?

Ja.

4.1.3 Fungerar det att administrera med annat än windows, tex med FreeBSD eller Linux

Ja, det använder inget microsoft specifikt.

4.1.4 Finns CLI?

Nej. Det finns ett meny-system man kan nå från konsoll-porten.

4.1.5 Finns SSH-igång eller motsvarande?

Nej.

4.1.6 Finns scriptspråk?

Nej.

4.2.1 Finns åtkomst av användargränssnittet (TLS/SSL eller motsvarande)

Ja, om man skapar certifikat.

4.2.2 Hur hanteras / genereras / importeras certifikat?

Certifikaten får skapas på en annan maskin med tex OpenSSL, och sedan klistras in via admin-gränssnittet.

4.3 Koppling till förstärkt Autenticering

4.3.1 Klientcertifikat

Nej.

4.3.2 Dosor el motsvarande?

Nej.

4.4 Finns SNMP och annan fjärråtkomst / fjärrstyrning?

SNMP finns.

4.5 Kan man säkerhetskopiera regelverket?

Ja.

4.6 Kan man skriva ut regler?

Nej.

4.7 Finns det sårbarheter hos webservern eller ssl-implimentationen?

Nej.

5. Tillgänglighets och överlastningsattacker

5.1 Hur reagerar den mot en dos-attack?

Loggar.

5.2 Hur reagerar den mot en dos-attack mot admin-guiet?

Loggar, efter ett tag slutar den svara.

6. Funktionalitet

6.1 DynDNS eller motsvarande?

Ja.

7. Övriga Tester

7.1 Uppdatering av programvara / firmware / bios / signaturer eller motsvarande?

Ja.

7.2 Applikationsproxyfunktioner för något eller flera protokoll?

Nej.

7.3 Klarar den IP-telefoni?

Nej.

7.3.1 SIP?

Nej.

7.4 Stöd för Ipv6?

Nej.

7.5 Klarar den inloggning hos bredbandsoperatörer?

Nej.

7.6 Finns det stöd för NTP?

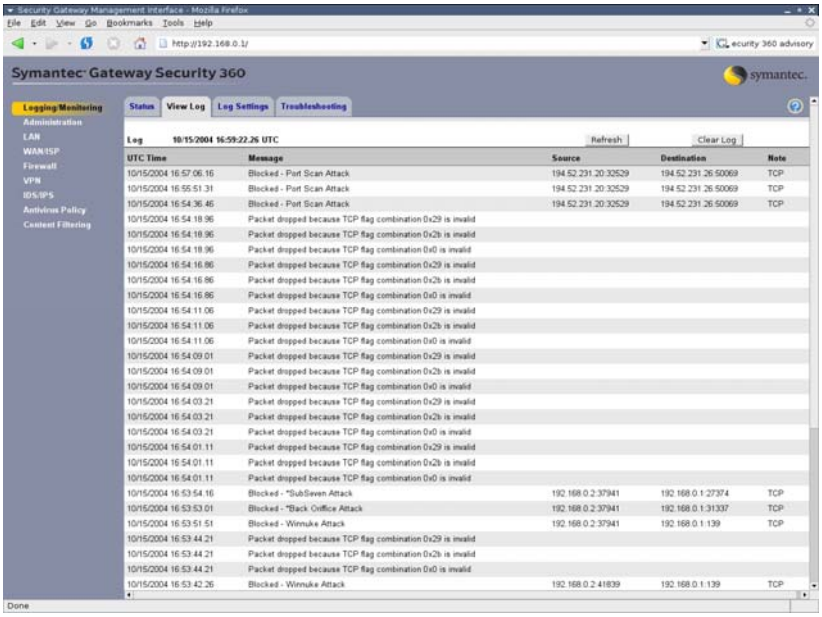
Nej.

Symantec Gateway Security 360

Symantec:s Gateway Security 360 är en lite större SoHo brandvägg med åtta lanportar och två wanportar för redundans eller failover. Ett visst IPS-stöd finns och även möjlighet att begränsa vilka siter som får besökas. Den har även en console-port och en pccardslot för wireless ethernet. Användargränssnittet är lättnavigerat och tillåter definition av services och datorer vilket gör administration av större nät betydligt enklare. Dessvärre lämnar den en del att önska.

Figur 7 Symantec Gateway Security 360

Problematiken ligger i att loggningen inte loggar allt, bla inte ICMP eller vissa typer av TCP-paket. Detta gör att det blir väldigt svårt att se vad som försigår på utsidan av brandväggen. Även IPS-funktionaliteten lämnar en hel del att önska, då den inte tycks använda sig av signaturer på innehållet i paketet öht vilket resulterar i att det blir en s.k. false-positives om man försöker nå valfri port som Gateway Security anser vara en trojanport. Eftersom i stort sätt alla trojaner tillåter enkelt byte av port så är denna typ av IPS inte tillräcklig.



Figur 8 Utdrag ifrån loggfönstret på SGS 300

1. Grundläggande brandväggsfunktionalitet

Vilka protokoll klaras av?

1.1.1 TCP

Ja

1.1.2 UDP

Ja

1.1.3 ICMP

Det går att ställa in att brandväggen svarar på icmp echo.

1.1.4 RTP

Nej

1.2.1 Vilka metoder används för att blockera trafik?

1.2.2 Block

Ja

1.2.3 Reject

Nej.

1.2.4 Pass

Ja.

1.2.5 ICMP-TYPES

Nej

1.2.6 Specifiering av port

Ja.

1.2.7 Är den statefull?

Ja.

1.2.8 Klarar den routing?

Ja

Vilka routing protokoll stödjs?

Rip2, Static route.

1.2.9 Klarar den bryggning?

Ja

Kan den vara helt transparent?

Nej

1.2.10 Klarar den olika regelverk på olika interface

Ja.

1.3.1 Loggning

1.3.2 Hur hanteras loggning?

Loggning ställs in på regelbasis.

1.3.3 Hur ser loggarna ut?

Loggarna visas i ett table med utc time, source:port, destination:port och message, där detta kan vara mer eller mindre beskrivande. Det står alltid om det är outbound eller inbound rules som triggas.

1.3.4 Kan man få dem binärt i tcpdump format?

Nej

1.3.5 Är det lätt att ta ut / exportera loggar?

Nej

1.3.6 Klarar den fjärrloggning till loggserver?

Ja.

1.3.7 Adressöversättning?

Nej.

2. Avancead brandväggsfunktionalitet

2.1.1 Koppling till antivirusprogram för viruskontroll av överförd data

Nej, dock kan man använda den för att tvinga fram uppdateringar av virusdefinitioner.

2.2.1 IDS och /eller IPS-funktionalitet

Ja, en viss IPS-funktinoalitet finns, men för att trigga false positives räcker det med att göra en enkel portscan, eller tex att telnetta till port 31337 (back oriffice). Detections av mycket gamla sårbarheter gör IPS-funkiotnaliteten till ett skämt. För att lura den (i trojan-fallet) är allt som krävs att man byter port i klienten, något som de allra flesta trojaner stödjer.

2.3.1 Vpn-funktionalitet

2.3.2 IPSEC

Ja

2.3.3 SSLVPN

Nej

2.3.4 UDP-Inkapsling

2.3.5 Prestandatester för VPN-funktionalitet

3. Säkerhetstester, postivita och negativa tester samt fel

3.1.1 Hur hanteras enkla portscans?

Symtantecs ”IPS” märker att det är en portscan, skriver en rad i loggen, och skiver sedan resterande portar som scannas.

3.1.2 Fin-scan?

Paketen droppas. Ingen rad om src och destination skrivs.

3.1.3 Klarar den att blocka x-masscan i olika varianter?

Ja. Paketen droppas. Ingen rad om src och destination skrivs.

3.1.4 Släpper den igenom trafik om man kör precis när den bootar?

Nej.

3.1.5 Kan man nå administrationsinterfacet från WAN-porten?

Nej.

4. Administration och användargränssnitt

4.1.1 Är andvändargränssnittet intuitivt och lättarbetat?

Ja.

4.1.2 Fungerar det med mozilla/opera?

Ja.

4.1.3 Fungerar det att administrera med annat än windows, tex med FreeBSD eller Linux

Ja.

4.1.4 Finns CLI?

Nej

4.1.5 Finns SSH-igång eller motsvarande?

Nej

4.1.6 Finns scriptspråk?

Nej

4.2.1 Finns uppsäkrad åtkomst av användargränssnittet (TLS/SSL eller motsvarande)

Nej

4.2.2 Hur hanteras / genereras / importeras certifikat?

-

4.3 Koppling till förstärkt Autenticering

4.3.1 Klientcertifikat

Nej.

4.3.2 Dosor el motsvarande?

Nej.

4.4 Finns SNMP och annan fjärråtkomst / fjärrstyrning?

Ja.

4.5 Kan man säkerhetskopiera regelverket?

Nej.

4.6 Kan man skriva ut regler?

Nej.

4.7 Finns det sårbarheter hos webservern eller ssl-implimentationen?

Nej.

5. Tillgänglighets och överlastningsattacker

5.1 Hur reagerar den mot en dos-attack?

Den slutar svara och routa trafik. Efter att attacken är över blir brandväggen funktionell igen.

5.2 Hur reagerar den mot en dos-attack mot admin-guiet?

Den skriver konstiga rader i loggen, och slutar sedan svara och routa trafik. Efter att attacken är över blir brandväggen funktionell igen.

6. Funktionalitet

6.1 DynDNS eller motsvarande?

Ja.

7. Övriga Tester

7.1 Uppdatering av programvara / firmware / bios / signaturer eller motsvarande?

Ja.

7.2 Applikationsproxyfunktioner för något eller flera protokoll?

Nej.

7.3 Klarar den IP-telefoni?

Nej.

7.3.1 SIP?

-

7.4 Stöd för Ipv6?

Nej.

7.5 Klarar den inloggning hos bredbandsoperatörer?

Nej.

7.6 Finns det stöd för NTP?

Ja, ntp stöd finns men tycks inte fungera.

SurfinBird Gate FW AirSIP Plus

SurfinBird GateFW AirSIP Plus är en liten brandvägg baserad på operativsystemet VXWorks. Den är utrustad med två ethernet interface, en usb-port och ett rj11-jack för telefoni. En bug i mjukvaran resulterade i att brandväggen låste sig av fragmenterade paket, och ingen uppdatering finns på hemsidan. Intertex har dock en uppdatering som löser problemet.

Figur 9 Surfinbird brandvägg

Brandväggen är extremt lättanvänd och en ovanlig men bra funktion är möjligheten att cykla säkerhetsprofiler (eller regelverk) genom att trycka på en knapp på brandväggen. Detta gör att det är väldigt enkelt att låsa ned nätaktiviteten om misstanke om intrång uppstår. En mycket bra funktion för en hembrandvägg.

1. Grundläggande brandväggsfunktionalitet

Vilka protokoll klaras av?

1.1.1 TCP

Ja

1.1.2 UDP

Ja.

1.1.3 ICMP

Ja.

1.1.4 RTP

Nej.

1.2.1 Vilka metoder används för att blockera trafik?

1.2.2 Block

Ja.

1.2.3 Reject

Nej.

1.2.4 Pass

Ja.

1.2.5 ICMP-TYPES

Ja.

1.2.6 Specifiering av port

Ja.

1.2.7 Är den statefull?

Ja.

1.2.8 Klarar den routing?

Ja.

Vilka routing protokoll stödjs?

Static routes.

1.2.9 Klarar den bryggning?

Ja.
Kan den vara helt transparent?

Nej.

1.2.10 Klarar den olika regelverk på olika interface

Ja

1.3.1 Loggning

1.3.2 Hur hanteras loggning?

Loggning ställs in på reglebasis med olika informationsnivåer, beroende på hur mycket information man vill ha loggat.

1.3.3 Hur ser loggarna ut?

Loggarna är i ascii format men man kan även spara loggar i hex-format och bestämma hur mycket av paketet som ska loggas.

1.3.4 Kan man få dem binärt i tcpdump format?

Nej

1.3.5 Är det lätt att ta ut / exportera loggar?

Nej.

1.3.6 Klarar den fjärrloggning till loggserver?

Ja.

1.3.7 Adressöversättning?

Nej.

2. Avancead brandväggsfunktionalitet

2.1.1 Koppling till antivirusprogram för viruskontroll av överförd data

Nej

2.2.1 IDS och /eller IPS-funktionalitet

Nej

2.3.1 Vpn-funktionalitet

Ja och Nej. Brandväggen stödjer både PPTP och IPSEC, dock så stödjer inte firmwaren vpn-terminering. I manualen står det att version 3.0 stödjer vpnterminering, men när man ska uppdatera firmwaren så står det att 2.07 är den senaste versionen.

2.3.2 IPSEC

Ja.

2.3.3 SSLVPN

Nej.

2.3.4 UDP-Inkapsling

Ja.

2.3.5 Prestandatester för VPN-funktionalitet

-

3. Säkerhetstester, postivita och negativa tester

3.1.1 Hur hanteras enkla portscans?

Blockar, skriver rader i loggen. Ingen kommentar om att en portscan skulle inträffa.

3.1.2 Fin-scan?

Blockar, skriver rader i loggen, noterar fin-paket. Ingen kommentar om portscan eller dylikt.

3.1.3 Klarar den att blocka x-masscan i olika varianter?

Ja.

3.1.4 Släpper den igenom trafik om man kör precis när den bootar?

Nej.

3.1.5 Utgående trafik?

Nej.

3.1.6 Kan man nå administrationsinterfacet från WAN-porten?

Nej.

4. Administration och användargränssnitt

4.1.1 Är andvändargränssnittet intuitivt och lättarbetat?

Mycket enkelt fram tills det är dags att skriva egna regler, då man måste skriva reglerna manuellt vilket inte har en särskilt enkel syntax.

4.1.2 Fungerar det med mozilla/opera?

Ja, det fungerar med både mozilla och opera, men Internet Explorer eller Opera rekommenderas då SurfinBird använder digest authentication för att lösenordet inte ska skickas i klartext. Det går dock att använda mozilla ändå, men då blir lösenordet som sagt i klartext.

4.1.3 Fungerar det att administrera med annat än windows, tex med FreeBSD eller Linux

Ja.

4.1.4 Finns CLI?

Ja.

4.1.5 Finns SSH-igång eller motsvarande?

Telnet.

4.1.6 Finns scriptspråk?

Nej.

4.2.1 Finns åtkomst av användargränssnittet (TLS/SSL eller motsvarande)

Nej, Digest Authentication vid auktorisering.

4.2.2 Hur hanteras / genereras / importeras certifikat?

-

4.3 Koppling till förstärkt Autenticering

4.3.1 Klientcertifikat

Nej.

4.3.2 Dosor el motsvarande?

Nej.

4.4 Finns SNMP och annan fjärråtkomst / fjärrstyrning?

Nej.

4.5 Kan man säkerhetskopiera regelverket?

Ja.

4.6 Kan man skriva ut regler?

Ja.

4.7 Finns det sårbarheter hos webservern eller ssl-implimentationen?

Nej.

5. Tillgänglighets och överlastningsattacker

5.1 Hur reagerar den mot en dos-attack?

SurfinBird klarade en denial of service utan problem. Givetvis gick det långsammare att nå nätet, men detta beror mer på att bandbredden fylls än något annat.

5.2 Hur reagerar den mot en dos-attack mot admin-guiet?

När en dos-attack sker mot insidan så kan brandväggens administrationsgränssnitt sluta svara under persioden. Detta resulterar även i att det inte går att byta regleverk manuellt.

6. Funktionalitet

6.1 DynDNS eller motsvarande?

Ja stöd för DynDNS finns

7. Övriga Tester

7.1 Uppdatering av programvara / firmware / bios / signaturer eller motsvarande?

Ja, via webgränsnittet.

7.2 Applikationsproxyfunktioner för något eller flera protokoll?

En transparent proxy för ftp finns i brandväggen, men den är inte igång default

7.3 Klarar den IP-telefoni?

Ja.

7.3.1 SIP?

Ja.

7.4 Stöd för Ipv6?

Nej.

7.5 Klarar den inloggning hos bredbandsoperatörer?

Ja, stöd för flera leverantörer finns.

7.6 Finns det stöd för NTP?

Ja stöd för SNTP finns.

Linksys rv082 VPN Router

Linksys VPN Router kommer utrustad med 8 portar, en wan-port samt en DMZ/internet för redundans eller dmz. I övrigt är den mycket lik symantecs brandvägg i det att man definerar datorer och services i en meny för att sedan kunna manipulera dem i de övriga.

Figur 10 Linksys rv082 VPN Router

En firmware-uppgradering till rv082 medför möjligheten att blockera nedladding av activex, javakomponenter och cookies, dessvärre resulterar detta i att logg-funktionen slutar fungera. Den har dock en rollback-funktion vid mjukvaruupgradering. Snyggt.

1. Grundläggande brandväggsfunktionalitet

Vilka protokoll klaras av?

1.1.1 TCP

Ja

1.1.2 UDP

Ja

1.1.3 ICMP

Bara ping.

1.1.4 RTP

Nej

1.2.1 Vilka metoder används för att blockera trafik?

1.2.2 Block

Ja.

1.2.3 Reject

Nej.

1.2.4 Pass

Ja.

1.2.5 ICMP-TYPES

Nej.

1.2.6 Specifiering av port

Ja.

1.2.7 Är den statefull?

Ja.

1.2.8 Klarar den routing?

Ja.
Vilka routing protokoll stödjs?

Rip, RIP2

1.2.9 Klarar den bryggning?

Nej.
Kan den vara helt transparent?

Nej.

1.2.10 Klarar den olika regelverk på olika interface

Den klarar olika regler på lan, dmz och wan. Det går även att specifiea any.

1.3.1 Loggning

1.3.2 Hur hanteras loggning?

Loggarna delas upp i outgoing, incomming och system.

1.3.3 Hur ser loggarna ut?

Loggarna är i html-table med tre kolummer, TIME, Event type och message.

Time är tiden, Event type är tex ”policy violation, connection refused”, ”connection accepted” osv. Message innehåller source och destination, interface och protokoll.

1.3.4 Kan man få dem binärt i tcpdump format?

Nej.

1.3.5 Är det lätt att ta ut / exportera loggar?

Nej.

1.3.6 Klarar den fjärrloggning till loggserver?

Ja.

1.3.7 Adressöversättning?

Ja.

2. Avancead brandväggsfunktionalitet

2.1.1 Koppling till antivirusprogram för viruskontroll av överförd data

Nej

2.2.1 IDS och /eller IPS-funktionalitet

Nej

2.3.1 Vpn-funktionalitet

Ja.

2.3.2 IPSEC

Ja.

2.3.3 SSLVPN

Nej.

2.3.4 UDP-Inkapsling

Nej.

2.3.5 Prestandatester för VPN-funktionalitet

-

3. Säkerhetstester, postivita och negativa tester samt fel

3.1.1 Hur hanteras enkla portscans?

Blocked, Synflood

3.1.2 Fin-scan?

Blockar, loggar.

3.1.3 Klarar den att blocka x-masscan i olika varrianter?

Blockar, loggar.

3.1.4 Släpper den igenom trafik om man kör precis när den bootar?

Nej.

3.1.5 Utgående trafik?

Nej.

3.1.6 Kan man nå administrationsinterfacet från WAN-porten?

Nej, om man inte specifikt skriver regler för detta.

4. Administration och användargränssnitt

4.1.1 Är andvändargränssnitet intiutivt och lättarbetat?

Ja.

4.1.2 Fungerar det med mozilla/opera?

Ja.

4.1.3 Fungerar det att administrera med annat än windows, tex med FreeBSD eller Linux

Ja.

4.1.4 Finns CLI?

Nej.

4.1.5 Finns SSH-igång eller motsvarande?

Nej.

4.1.6 Finns scriptspråk?

Nej.

4.2.1 Finns åtkomst av användargränssnittet (TLS/SSL eller motsvarande)

Nej.

4.2.2 Hur hanteras / genereras / importeras certifikat?

-

4.3 Koppling till förstärkt Autenticering

4.3.1 Klientcertifikat

Nej.

4.3.2 Dosor el motsvarande?

Nej.

4.4 Finns SNMP och annan fjärråtkomst / fjärrstyrning?

Ja.

4.5 Kan man säkerhetskopiera regelverket?

Nej.

4.6 Kan man skriva ut regler?

Nej.

4.7 Finns det sårbarheter hos webservern eller ssl-implimentationen?

Nej.

5. Tillgänglighets och överlastningsattacker

5.1 Hur reagerar den mot en dos-attack?

En icmp ping flood klaras utan problem, dock skrivs inget om den i loggen. Om punk används istället så blir brandväggen inte nåbar från insidan, samt att den inte loggar. Kör man i kortare perioder så skriver den rader i loggen utan att skriva vare sig source eller destination.

5.2 Hur reagerar den mot en dos-attack mot admin-guiet?

Den blir långsam men fortsätter att fungera. Den skriver inte source och destination i loggen.

6. Funktionalitet

6.1 DynDNS eller motsvarande?

Ja.

7. Övriga Tester

7.1 Uppdatering av programvara / firmware / bios / signaturer eller motsvarande?

Ja, även rollback funktionalitet.

7.2 Applikationsproxyfunktioner för något eller flera protokoll?

Nej.

7.3 Klarar den IP-telefoni?

Nej.

7.3.1 SIP?

Nej.

7.4 Stöd för Ipv6?

Nej.

7.5 Klarar den inloggning hos bredbandsoperatörer?

Nej.

7.6 Finns det stöd för NTP?

Ja.

Billion Broadband Router

Billions brandvägg är en mycket enkel brandvägg att använda och med den funktionalitet man kan förvänta sig för det mycket låga priset. Administrationsgränssnittet är väldigt lättnavigerat då det finns få funktioner att välja mellan. Den kommer utrustad med fyra lan-portar och en wanport. Även här är loggning den svagaste punkten då den dels skiljer sig mellan de två olika logglägena.

Figur 11 Billion Broadband Router

Billion Broadband Router har en del onödig funktionalitet som kan ifrågasättas. Ett exempel är funktionen för att kontrollera oläst e-post vilket resulterar i att en lampa blinkar på apparatlådan.

1. Grundläggande brandväggsfunktionalitet

Vilka protokoll klaras av?

1.1.1 TCP

Ja.

1.1.2 UDP

Ja.

1.1.3 ICMP

Ja.

1.1.4 RTP

Nej.

1.2.1 Vilka metoder används för att blockera trafik?

1.2.2 Block

Ja.

1.2.3 Reject

Nej.

1.2.4 Pass

Ja.

1.2.5 ICMP-TYPES

Nej.

1.2.6 Specifiering av port

Ja.

1.2.7 Är den statefull?

Ja.

1.2.8 Klarar den routing?

Ja.
Vilka routing protokoll stödjs?

Rip 1, 2 och static routes.

1.2.9 Klarar den bryggning?

Nej.
Kan den vara helt transparent?

Nej.

1.2.10 Klarar den olika regelverk på olika interface

Nej.

1.3.1 Loggning

1.3.2 Hur hanteras loggning?

Loggning specifieras på regelbasis.

1.3.3 Hur ser loggarna ut?

Ascii-loggar en form, det går dock att se dem i rå text

1.3.4 Kan man få dem binärt i tcpdump format?

Nej.

1.3.5 Är det lätt att ta ut / exportera loggar?

Nej, och logfönstret och råloggen differensierar i innehåll.

1.3.6 Klarar den fjärrloggning till loggserver?

Nej.

1.3.7 Adressöversättning?

Nej.

2. Avancead brandväggsfunktionalitet

2.1.1 Koppling till antivirusprogram för viruskontroll av överförd data

Nej.

2.2.1 IDS och /eller IPS-funktionalitet

En viss IPS-funktionalitet finns, ”block hacker attacks” vilket innebär att ping of death, winnuke, zero lenght ip-packet, null scan, synflood, smurf & snork.

2.3.1 Vpn-funktionalitet

Ja.

2.3.2 IPSEC

Ja.

2.3.3 SSLVPN

Nej.

2.3.4 UDP-Inkapsling

Nej.

2.3.5 Prestandatester för VPN-funktionalitet

-

3. Säkerhetstester, postivita och negativa tester samt fel

3.1.1 Hur hanteras enkla portscans?

Beroende på vad brandväggen tycker är normalt på porten så skriver den antingen Synflood eller trojan scan.

3.1.2 Fin-scan?

Blockar och skriver inga rader i loggen om det man scannar

inte råkar vara en port som billion fwn anser vara en trojan-port.

3.1.3 Klarar den att blocka x-masscan i olika varrianter?

Ja, men samma problem finns här. Loggar bara det som anses intressant.

3.1.4 Släpper den igenom trafik om man kör precis när den bootar?

Nej.

3.1.5 Utgående trafik?

Nej.

3.1.6 Kan man nå administrationsinterfacet från WAN-porten?

Nej, inte normalt. Det är möjligt att ställa in i administrationsgränsnittet, dock går det inte att göra någon form av säker anslutning, utan det är security by obscurity som gäller. Default är port 52520.

4. Administration och användargränssnitt

4.1.1 Är andvändargränssnitet intiutivt och lättarbetat?

Ja.

4.1.2 Fungerar det med mozilla/opera?

Ja.

4.1.3 Fungerar det att administrera med annat än windows, tex med FreeBSD eller Linux

Ja.

4.1.4 Finns CLI?

Nej.

4.1.5 Finns SSH-igång eller motsvarande?

Nej.

4.1.6 Finns scriptspråk?

Nej.

4.2.1 Finns åtkomst av användargränssnittet (TLS/SSL eller motsvarande)

Nej.

4.2.2 Hur hanteras / genereras / importeras certifikat?

-

4.3 Koppling till förstärkt Autenticering

4.3.1 Klientcertifikat

Nej.

4.3.2 Dosor el motsvarande?

Nej.

4.4 Finns SNMP och annan fjärråtkomst / fjärrstyrning?

Nej.

4.5 Kan man säkerhetskopiera regelverket?

Nej.

4.6 Kan man skriva ut regler?

Nej.

4.7 Finns det sårbarheter hos webservern eller ssl-implimentationen?

Nej.

5. Tillgänglighets och överlastningsattacker

5.1 Hur reagerar den mot en dos-attack?

Den blir obrukbar tills attacken är över, då den börjar fungera igen. Inget loggas dock.

5.2 Hur reagerar den mot en dos-attack mot admin-guiet?

Samma som ovan.

6. Funktionalitet

6.1 DynDNS eller motsvarande?

Ja.

7. Övriga Tester

7.1 Uppdatering av programvara / firmware / bios / signaturer eller motsvarande?

Möjlighet finns.

7.2 Applikationsproxyfunktioner för något eller flera protokoll?

Nej, UPnP dock.

7.3 Klarar den IP-telefoni?

Nej.

7.3.1 SIP?

Nej.

7.4 Stöd för Ipv6?

Nej.

7.5 Klarar den inloggning hos bredbandsoperatörer?

Nej.

7.6 Finns det stöd för NTP?

SNTP.

Cyberguard SG300

Cyberguard SG300 är en brandvägg baserad på Linux 2.4-kärnan och kommer med en wanport och fyra lanportar. Produkten kan anses vara lättanvänlig. Den har stöd för mer avancerade funktioner såsom VPN-terminering, en snort-baserad IDS samt centraliserad administration.

Figur 12 Cyberguard SG300

En intressant funktion som produkten har är möjligheten att tvinga klienter att köra brandväggsmjukvaran Zone Alarm Pro på PC-datorn som skyddas av Cyberguard. Användargränssnittet till SG300 lämnar en del övrigt att önska. Ett problem är att det ibland är oklart för en administratör hur menysystemet är strukturerat vilket gör att vissa funktioner är svåra att hitta.

1. Grundläggande brandväggsfunktionalitet

Vilka protokoll klaras av?

1.1.1 TCP

Ja.

1.1.2 UDP

Ja.

1.1.3 ICMP

Ja.

1.1.4 RTP

1.2.1 Vilka metoder används för att blockera trafik?

1.2.2 Block

Ja.

1.2.3 Reject

Ja.

1.2.4 Pass

Ja.

1.2.5 ICMP-TYPES

Om man skriver egna regler.

1.2.6 Specifiering av port

Ja.

1.2.7 Är den statefull?

Ja.

1.2.8 Klarar den routing?

Ja.
Vilka routing protokoll stödjs?

Static routes.

1.2.9 Klarar den bryggning?

Ja.
Kan den vara helt transparent?

Ja.

1.2.10 Klarar den olika regelverk på olika interface

Ja.

1.3.1 Loggning

1.3.2 Hur hanteras loggning?

För att logga måste detta specifieras per regelbasis och loggas sedan av klogd.

1.3.3 Hur ser loggarna ut?

Ascii.

1.3.4 Kan man få dem binärt i tcpdump format?

Nej.

1.3.5 Är det lätt att ta ut / exportera loggar?

Nej.

1.3.6 Klarar den fjärrloggning till loggserver?

Ja.

1.3.7 Adressöversättning?

Nej.

2. Avancead brandväggsfunktionalitet

2.1.1 Koppling till antivirusprogram för viruskontroll av överförd data

Nej.

2.2.1 IDS och /eller IPS-funktionalitet

Ja, snort 2 finns med.

2.3.1 Vpn-funktionalitet

Ja.

2.3.2 IPSEC

Ja.

2.3.3 SSLVPN

Nej.

2.3.4 UDP-Inkapsling

Nej.

2.3.5 Prestandatester för VPN-funktionalitet

3. Säkerhetstester, postivita och negativa tester samt fel

3.1.1 Hur hanteras enkla portscans?

Blockas, loggas.

3.1.2 Fin-scan?

Blockar.

3.1.3 Klarar den att blocka x-masscan i olika varrianter?

Ja.

3.1.4 Släpper den igenom trafik om man kör precis när den

bootar?

Nej.

3.1.5 Utgående trafik?

Nej.

3.1.6 Kan man nå administrationsinterfacet från WAN-porten?

Nej.

4. Administration och användargränssnitt

4.1.1 Är andvändargränssnitet intiutivt och lättarbetat?

Ja.

4.1.2 Fungerar det med mozilla/opera?

Ja.

4.1.3 Fungerar det att administrera med annat än windows, tex med FreeBSD eller Linux

Ja.

4.1.4 Finns CLI?

Ja.

4.1.5 Finns SSH-igång eller motsvarande?

Telnet.

4.1.6 Finns scriptspråk?

Nej.

4.2.1 Finns åtkomst av användargränssnittet (TLS/SSL eller motsvarande)

Nej.

4.2.2 Hur hanteras / genereras / importeras certifikat?

-

4.3 Koppling till förstärkt Autenticering

4.3.1 Klientcertifikat

Nej.

4.3.2 Dosor el motsvarande?

Nej.

4.4 Finns SNMP och annan fjärråtkomst / fjärrstyrning?

Nej.

4.5 Kan man säkerhetskopiera regelverket?

Nej.

4.6 Kan man skriva ut regler?

Nej.

4.7 Finns det sårbarheter hos webservern eller ssl-implimentationen?

Ja.

5. Tillgänglighets och överlastningsattacker

5.1 Hur reagerar den mot en dos-attack?

Administrationsgränssnittet blir långsamt. Inget loggas.

5.2 Hur reagerar den mot en dos-attack mot admin-guiet?

Adminguietgränssnittet blir väldigt långsamt.

6. Funktionalitet

6.1 DynDNS eller motsvarande?

Ja.

7. Övriga Tester

7.1 Uppdatering av programvara / firmware / bios / signaturer eller motsvarande?

Ja.

7.2 Applikationsproxyfunktioner för något eller flera protokoll?

ftp, irc, tftp, pptp..

7.3 Klarar den IP-telefoni?

Nej.

7.3.1 SIP?

Nej.

7.4 Stöd för Ipv6?

Ja. Dock inte via användargränssnittet.

7.5 Klarar den inloggning hos bredbandsoperatörer?

Nej.

7.6 Finns det stöd för NTP?

Ja.

Sonicwall tz170 sp

Sonicwall kommer utrustad med fem lanportar, en wanport, och en för anslutning till en accesspunkt. Även här används VXWorks som OS. Brandväggen fungerar bra, men loggning verkar bara ske då den triggar något som brandväggen anser vara ovanligt. Sonicwall har mängder med funktioner, men flera av dem krävs det att man köper till, så som antivirus och IPS-funktionalitet.

Figur 13 Sonicwall tz170 sp

1. Grundläggande brandväggsfunktionalitet

Vilka protokoll klaras av?

1.1.1 TCP

Ja.

1.1.2 UDP

Ja.

1.1.3 ICMP

Ja.

1.1.4 RTP

Nej.

1.2.1 Vilka metoder används för att blockera trafik?

1.2.2 Block

Ja.

1.2.3 Reject

Ja.

1.2.4 Pass

Ja.

1.2.5 ICMP-TYPES

Ja.

1.2.6 Specifiering av port

Ja.

1.2.7 Är den statefull?

Ja.

1.2.8 Klarar den routing?

Ja.
Vilka routing protokoll stödjs?

Static routes, rip1 och rip2.

1.2.9 Klarar den bryggning?

Nej.
Kan den vara helt transparent?

-

1.2.10 Klarar den olika regelverk på olika interface

Ja.

1.3.1 Loggning

1.3.2 Hur hanteras loggning?

Loggar sätts på regelbasis.

1.3.3 Hur ser loggarna ut?

Loggarna visas i ett html-table där kollummerna time, priority, category, message, source, och notes visas. Priority visar vilken nivå du definerat händelsen att logga som. Tex kan man tycka att alla ssh-försök är critical, vilket kommer resultera i att den skrivs med röd bakgrund i tabellen och på såvis sticker ut mer.

1.3.4 Kan man få dem binärt i tcpdump format?

Nej.

1.3.5 Är det lätt att ta ut / exportera loggar?

Ja.

1.3.6 Klarar den fjärrloggning till loggserver?

Ja.

1.3.7 Adressöversättning?

Ja.

2. Avancead brandväggsfunktionalitet

2.1.1 Koppling till antivirusprogram för viruskontroll av överförd data

Ja om uppgraderad.

2.2.1 IDS och /eller IPS-funktionalitet

Ja om uppgraderad.

2.3.1 Vpn-funktionalitet

Ja.

2.3.2 IPSEC

Ja.

2.3.3 SSLVPN

Nej.

2.3.4 UDP-Inkapsling

Nej.

2.3.5 Prestandatester för VPN-funktionalitet

3. Säkerhetstester, postivita och negativa tester samt fel

3.1.1 Hur hanteras enkla portscans?

Portscan detectas och skrivs i loggen. Den skriver även om trojanattacker och annat den känner igen.

3.1.2 Hur hanteras Fin-scan?

En rad i loggen angående terminal services. Inget om fin-scan.

3.1.3 Klarar den att blocka x-masscan i olika varrianter?

Ja, dock skrivs inget i loggen.

3.1.4 Släpper den igenom trafik om man kör precis när den

bootar?

Nej.

3.1.5 Utgående trafik?

Nej.

3.1.6 Kan man nå administrationsinterfacet från WAN-porten?'

Nej.

4. Administration och användargränssnitt

4.1.1 Är andvändargränssnitet intiutivt och lättarbetat?

Relativt. För mycket menyer och submenyer vilket gör att man lätt letar bland menyerna för att hitta det man söker.

4.1.2 Fungerar det med mozilla/opera?

Ja.

4.1.3 Fungerar det att administrera med annat än windows, tex med FreeBSD eller Linux

Ja.

4.1.4 Finns CLI?

Ja.

4.1.5 Finns SSH-igång eller motsvarande?

Nej.

4.1.6 Finns scriptspråk?

Ja.

4.2.1 Finns åtkomst av användargränssnittet (TLS/SSL eller motsvarande)

Ja.

4.2.2 Hur hanteras / genereras / importeras certifikat?

Ett självsignerat certifikat är med som default. Det finns funktionalitet för att importera ett eget.

4.3 Koppling till förstärkt Autenticering

4.3.1 Klientcertifikat

Nej.

4.3.2 Dosor el motsvarande?

Nej.

4.4 Finns SNMP och annan fjärråtkomst / fjärrstyrning?

Ja. Snmp.

4.5 Kan man säkerhetskopiera regelverket?

Ja.

4.6 Kan man skriva ut regler?

Nej.

4.7 Finns det sårbarheter hos webservern eller ssl-implimentationen?

Nej.

5. Tillgänglighets och överlastningsattacker

5.1 Hur reagerar den mot en dos-attack?

Ip protocoll 255 dropped skrivs i loggen. I övrigt fungerar den normalt.

5.2 Hur reagerar den mot en dos-attack mot admin-guiet?

Den blir långsam. När attacken upphör återgår den till det normala.

6. Funktionalitet

6.1 DynDNS eller motsvarande?

Nej.

7. Övriga Tester

7.1 Uppdatering av programvara / firmware / bios / signaturer eller motsvarande?

Ja.

7.2 Applikationsproxyfunktioner för något eller flera protokoll?

Nej.

7.3 Klarar den IP-telefoni?

Ett visst stöd finns.

7.3.1 SIP?

Ja, SIP-transformation.

7.4 Stöd för Ipv6?

Nej.

7.5 Klarar den inloggning hos bredbandsoperatörer?

Nej.

7.6 Finns det stöd för NTP?

Ja.

Produktinformation

Billion Broadband router

http://www.billion.com/product/broadband.htm

Linksys rv082 VPN Router

http://www.linksys.com/products/product.asp?grid=34&scid=29&prid=589

Monowall

http://m0n0.ch/wall/

Symantec Gateway Security 360

http://www.symantec.com/smallbiz/gtw/

Intertex SurfinBird Gate FW

http://www.intertex.se

Cyberguard SG300

http://www.cyberguard.com/snapgear/SG300.html

SonicWall tz170sp

http://www.sonicwall.com/products/tz170SP_wireless.html

Register

