Industriële en biowetenschappen Geel

Master in de industriële wetenschappen: elektronica-ICT

ICT

Vergelijkende studie van enterprise firewalls

ISA Server 2006, Juniper SSG 20 en Check Point R70 onder de loep

CAMPUS

Geel

Dieter Van Den Bosch

Academiejaar 2008-2009

VOORWOORD

Graag had ik iedereen bedankt die op een of andere manier mee heeft geholpen aan de realisatie van mijn masterproef. Mede dankzij hen kan ik met een hele bagage aan competenties mijn leven als student Industrieel Ingenieur ICT afsluiten en een nieuw hoofdstuk openen als werknemer.

In de eerste plaats wil ik mijn externe begeleider Kris Joris bedanken om mij de kans te geven om mijn masterproef bij CIPAL te voltrekken en om mij min of meer vrij te laten in de keuze van dit project, in feite mijn 'droomproject'. Daarbij aansluitend zou ik iedereen bij CIPAL willen bedanken die mij heeft geholpen en gesteund.

Natuurlijk wil ik ook mijn interne begeleider Staf Vermeulen bedanken.

Tenslotte wil ik mijn familie bedanken voor de steun en het geduld tijdens het maken van mijn masterproef.

SAMENVATTING

Welke firewall is nu eigenlijk de beste? Welke firewall heeft zijn netwerkbeveiliging helemaal dichtgemetseld? Hoe werken de bekendste firewalls? Veel vragen, niet? Wel deze zullen allemaal beantwoord worden in deze masterproef dat over dat zeer boeiend onderwerp handelt!

Bovendien zal het je een breder beeld geven van de firewall-markt zodat je op de hoogte bent van de nieuwste en meest interessante ontwikkelingen. Concreet zal je een vergelijkend onderzoek aantreffen tussen drie verschillende enterprise firewalls. Dat zijn firewalls die in middelgrote en grote bedrijven worden gebruikt. Daar zitten volgende bekende namen bij: ISA Server, Juniper en Check Point.

Er wordt veel over gepraat, van sommige firewalls wordt gezegd dat ze rotslecht zijn, over anderen wordt dan weer gezegd dat ze de 'crème de la crème' zijn. Wat is daar nu eigenlijk waar van?!

INHOUDSOPGAVE

1 INLEIDING

Wil je nu wel eens weten hoe het zit met die firewalls? Wil je weten hoe de markt er ongeveer uit ziet en welke firewall de beste is? Dan moet je zeker dit werkstuk lezen!

Tijdens dit onderzoek dat op CIPAL te Geel liep zijn drie bekende firewalls geëvalueerd: ISA Server 2006, Juniper SSG 20, Check Point R70. Daarbij is onderzocht hoe het zit met de beveiliging, de werking en de voordelen & nadelen van de verschillende firewalls.

Het grootste deel bestaat uit een studie van de beveiliging van de firewalls. Dit gebeurde met penetration testing waarbij gekeken wordt of ze al dan niet aanvallen tegenhouden en/of in hun logs opnemen.

Tijdens deze vergelijkende studie staan volgende onderzoeksvragen centraal:

- Welke gaten treden op in de netwerkbeveiliging bij een implementatie van de firewall? En dit in de volgende configuraties:
    - De firewall met zo min mogelijk instellingen (de 'default' configuratie)
    - De firewall met een bepaalde vooraf bepaalde configuratie. Die configuratie stelt een realistische implementatie van de firewall voor.
- Gaat de firewall adequaat om met aanvallen?
- Houdt de firewall een aanval van Conficker, de revolutionaire nieuwe worm, tegen?

1.1 CIPAL

Het onderzoek vond plaats bij de 'Dienstverlenende Vereniging CIPAL', of kort CIPAL dv. Een korte geschiedenis [1]…

CIPAL (toen nog CIPA) werd bij KB van 2 april 1979 opgericht. CIPAL zou zich gaan bezighouden met de studie van informatica en software toepassingen die daar uitvloeiden. Bij de start van CIPAL waren er twee personeelsleden: Arthur Philips en zijn secretaresse. Op het einde van het eerste werkingsjaar telde CIPAL 9 personeelsleden.

Op 2 april 1984 werd een samenwerkingsakkoord gesloten tussen CIPA en de v.z.w. LIRIC, het Limburgs Reken- en Informatiecentrum. Door deze verruiming naar de provincie Limburg toe, kreeg de vereniging een nieuwe naam: CIPAL. Deze uitbreiding van het werkterrein had tot gevolg dat ook het personeelsbestand aanzienlijk uitgebreid werd. Ondertussen zijn ook de statutaire bepalingen van CIPAL dermate aangepast dat het werkingsgebied van CIPAL wordt verruimd naar gans Vlaanderen.

De software toepassingen, waar CIPAL voor zorgde, werden steeds verder uitgebouwd. De daarbij horende groei van de relaties met de traditionele klanten, zoals gemeenten, OCMW's, de provincies en diverse plaatselijke en regionale overheden resulteerden in de verdere groei van de omzetcijfers en in het aantrekken van steeds meer gespecialiseerde medewerkers.

Al meer dan een kwarteeuw zet CIPAL zich dagelijks in om de informatica bij de openbare besturen op een hoger niveau te tillen.

CIPAL (toen nog CIPA) is in 1979 gestart met een minimum aan huisvesting: één lokaal van ongeveer 6 meter op 8 meter in het gebouw van PIPDA te Antwerpen. In juli 1981 werd de hoofdzetel gevestigd in Geel, aangezien er een grote know-how op het gebied van informatieverwerking aanwezig was, meer bepaald in het Hoger Instituut der Kempen. De gehuurde kantoren van CIPAL werden dan ook ingericht op de eerste verdieping van de gebouwen van het H.I.K., gelegen aan de Technische-Schoolstraat te Geel.

De penibele huisvesting in de school in Geel, waar intussen drie verdiepingen werden ingenomen, en de wens van de toenmalige Raad van Bestuur om het eigen imago beter te profileren, heeft CIPAL aangezet om een eigen exploitatiecentrum te realiseren. Het nieuwe hoofdgebouw van CIPAL werd in januari 1994 officieel geopend. De nieuwe CIPAL-hoofdzetel situeert zich niet toevallig in het Wetenschapspark te Geel.

Tot zover de korte geschiedenis van CIPAL. Als laatste moet er nog worden opgemerkt dat om de beveiliging van al de gemeentes, OCMW's, bibliotheken e.d. te garanderen er niets wordt vermeld over de configuratie van de firewalls geïnstalleerd door CIPAL.

1.2 Algemene security informatie

1.2.1 De verschillende fasen van hacking

Hoe gaan hackers te werk? Wel je kan het best in verschillende fases los van elkaar zien. Over de juiste fases en de bijhorende begrippen is er echter veel onenigheid, bijna alle bronnen gebruiken andere termen.

De volgende opsomming is een beetje een gulden middenweg tussen alle verschillende benamingen die verkondigd worden [5]:

1. Reconnaissance: Wat 'rondkijken' voor het verzamelen van informatie over het netwerk als voorbereiding op een aanval. In deze stap wordt op Google en via DNS bruikbare gegevens gezocht. Je kan het zien als een eerste kennismaking met de organisatie die je voor ogen houdt. Deze stap wordt ook wel eens 'footprinting' genoemd [2].
2. Enumeration: Het netwerk scannen en controleren op het draaien van services. Scannen op vulnerabilities die horen bij die services zit ook in deze stap.
3. Gaining access: Eenmaal een vulnerability is gevonden kan men overgaan tot het gebruiken van een exploit (een 'uitbuiting' van een beveiligingslek) die van die vulnerability gebruik maakt.
4. Securing access: Een manier vinden om later nog toegang te krijgen tot het gehackte systeem.
5. Covering tracks: Alle sporen van de inbraak wissen.

Het boek 'Inside Network Perimeter Security' [3] vervangt de fase enumeration door de twee fasen 'Network service discovery' en 'Vulnerability discovery'. Om de verwarring compleet te maken gebruiken ze de term 'enumeration' wel als deel van de Network service discovery.

Het boek 'Configuring Juniper Networks Netscreen & Ssg Firewalls' [4] heeft het ook over dezelfde zaken maar neemt stap 1 & 2 en stap 4 & 5 samen.

Cisco Press combineert stap 1 en stap 2 en noemt het samen reconnaissance.

Als stap 2, de enumeration, geen vulnerabilities oplevert kan men niet verder gaan met de volgende stappen. Men kan vervolgens wel een DoS (Denial of Service) attack, als derde en laatste stap uitvoeren.

In dit onderzoek zullen enkel de eerste drie stappen behandeld worden.

1.2.2 Penetration testing

Het belangrijkste deel van het onderzoek zal bestaan uit penetration testing. Dat bestaat uit het evalueren van een (computer)systeem om zo gaten in de beveiliging te vinden die een hacker kan gebruiken.

De penetration test tijdens dit onderzoek is bewust kort gehouden om het zo overzichtelijk en beknopt mogelijk te houden. Een echte penetration test zou nog een stuk uitgebreider zijn waarin alle mogelijke aanvallen zouden uitgeprobeerd en gedocumenteerd worden.

Als je aan penetration testing wil doen dan moet je de weg volgen die een hacker ook zou bewandelen. Zoals reeds vermeld heet de tweede stap van de hacker 'Enumeration'. Twee tools die voor enumeration gemaakt zijn en enorm vaak gebruikt worden zijn Nmap en Nessus. Nessus heeft zelf ook een (TCP) port scanner aan boord, maar voor de volledigheid is in dit onderzoek ook de port scanner Nmap gebruikt. Dit omdat het een gevestigde waarde is. Nessus heeft geen UDP port scanner aan boord omdat het efficiënter is om direct te kijken naar de applicaties die op die poorten moeten zitten in plaats van de poorten zelf scannen [6].

1.2.3 Nmap

Nmap is een open source port scanner. Zijn naam komt van Network Mapper. Een port scanner onderzoekt of een systeem open poorten heeft. Een open poort geeft altijd een

open service of dienst aan. Een dienst dus die het systeem aanbiedt voor andere gebruikers op het netwerk. Sommige diensten kunnen door een hacker gebruikt worden om in te breken. In principe geldt altijd de regel 'hoe minder open poorten, hoe veiliger'.

Nmap wordt vaak gezien als de beste port scanner op de markt [7]. Een van de sterkten van Nmap is dat het zeer veel opties heeft die je kan meegeven in het commando dat je Nmap geeft.

Er zijn maar weinig port scanners die aan Nmap kunnen tippen. Zo is er Superscan die zeer vergelijkbare functies heeft. Er is echter toch voor Nmap gekozen omdat het zo'n vaste waarde is in het security wereldje.

1.2.4 Nessus

Figuur 1.1

Nessus is een vulnerability scanner. Merk het verschil op met Nmap, de *port* scanner. Een vulnerability scanner is een veel uitgebreidere versie van een port scanner. Nessus is software die systemen test op mogelijke beveiligingslekken. Nessus is de nummer 1 in de Top 100 Network Security Tools op http://sectools.org/. Dit komt ondermeer omdat het programma gratis is voor niet-commercieel gebruik en omdat er regelmatig updates verschijnen. Nessus is met andere woorden dé tool waaraan je het eerst moet denken als je een systeem wil testen op vulnerabilities.

Onderzoek naar alternatieven voor Nessus heeft de vulnerabilty scanners GFI Languard, CORE IMPACT en SAINT opgebracht. Zij zijn allemaal zeer uitgebreid en minstens even goed als Nessus. Je moet er echter veel geld voor neertellen. Dat heeft tot gevolg dat Nessus een stuk bekender is dan alle andere vulnerability scanners. Daarom is dan ook voor Nessus gekozen.

Nessus is een typische *white hat* vulnerability scanner [5]. White hat duidt op het feit dat het goede bedoelingen heeft. Het controleert alle mogelijke vulnerabilities in een keer en genereert zo een hele hoop detecteerbaar netwerktrafiek. Black Hat tools zullen er alles aan doen om op geen enkele manier op te vallen. Met enkele juiste instellingen kan Nessus dit min of meer ook maar het is er alleszins niet voor gemaakt. Je ziet ook dat Nessus een white hat tool is aan de oplossingen die je telkens krijgt om de vulnerabilities op te lossen. Nessus dient dus om te zien waar de security op je systeem lek is en hoe je dat kan dichten.

1.2.5 Metasploit

Tot nu toe zijn er enkel tools bekeken die het systeem scannen. Hackers stoppen hier natuurlijk niet want ze willen iets doen met de gebreken die ze ontdekt hebben op het systeem. We hebben dus een derde programma nodig dat de vulnerabilities kan uitbuiten (to exploit, in het Engels). Als 'vulnerability exploitation tool' is gekozen voor Metasploit. Dit omdat Metasploit, net zoals Nessus en Nmap, een standaard tool is geworden in de security wereld. Daarom staat het ook op nummer 5 in de top 100 van de security tools op http://sectools.org/.

Sinds de lancering in 2006 brak Metasploit volledig door in de security wereld, vooral omdat het een open-source en gratis programma is. Er bestaan ook alternatieve tools zoals SAINTexploit en CORE IMPACT maar die zijn zeer prijzig.

1.2.6 Conficker en andere bekende worms

Een worm is software die zichzelf dupliceert en verspreidt om zo zonder directe tussenkomst van een gebruiker zo veel mogelijk systemen te besmetten met zichzelf. Verwar een worm dus niet met een virus dat een tussenkomst van een gebruiker nodig heeft.

In het verleden zijn er heel wat bekende worms opgedoken [8]. Zo had je in 2001 Code Red die een vulnerability misbruikte in de web server Microsoft IIS (Internet Information Services). In 2003 was er Slammer die een vulnerability in MS SQL Server gebruikt om zich te verspreiden. Later dat jaar verscheen Blaster die een vulnerability misbruikt op poorten 135, 139, 445 en 593. De eigenlijke vulnerability zat in de Distributed Component Object Model (DCOM) interface binnen het RPC proces [2].

Verder had je in 2004 de Sasser-worm die zich verspreidde [9][10]. Dat deed het via de TCP poorten 139 en 445. De bekendste karakteristiek van Sasser was de shutdown timer die het geïnfecteerd systeem uitzette na 60 seconden, na een crash van LSASS.exe.

1.2.6.1 Conficker

Na een relatieve stilte op vlak van worms brengt Microsoft op 23 oktober 2008 een patch onder de naam MS08-067 uit voor een beveiligingslek van de RPC service [11]. Zowat alle huidige besturingssystemen van Microsoft hebben deze patch nodig. In november wordt Conficker voor het eerst gesignaleerd. Deze worm, die soms ook wel eens Downadup wordt genoemd, is groot nieuws in de security-wereld. Het blijkt een absoluut revolutionaire worm en de gevaarlijkste worm van de laatste jaren [12]!

Figuur 1.2

Hoogstwaarschijnlijk is het gemaakt door professionals die wisten wat ze deden. Bij het verschijnen van dit werkstuk zijn er al 5 varianten ontdekt van de worm. Ze worden telkens aangeduid met een letter zoals bijvoorbeeld Conficker.A. De code van Conficker.A was zo gesofisticeerd [13] dat het aannemelijk is dat het niet 'vanaf nul' is geschreven in de tijd tussen het uitkomen van de patch en het verschijnen van de worm. Iemand had vermoedelijk zijn worm al tot in de puntjes geprogrammeerd, en wachtte enkel nog op een exploit waardoor de worm zich kon verspreiden [14].

Net zoals Blaster en Sasser verspreidt Conficker zich via de Microsoft-DS (Microsoft Directory Services) poort 445 die voor SMB en bijgevolg ook Windows file sharing wordt gebruikt [15][16]. Gelukkig wordt poort 445 geblokkeerd door de meeste ISP's omwille van de slechte reputatie van die poort. De poort wordt echter wel niet altijd geblokkeerd binnen het netwerk van de ISP. Het kan bijvoorbeeld zijn dat je niet beschermd bent voor infecties vanuit pc's in het kabelnetwerk van je straat. Sinds service pack 2 van Windows XP wordt deze poort standaard dichtgezet in de Windows

Firewall [17]. Vaak wordt echter door de gebruiker zelf, al dan niet bewust, deze poort terug opengezet omdat hij bestanden wil delen over het netwerk.

Wat zeer opmerkelijk is, is dat Conficker.A naar de website maxmind.com gaat om daar de geografische locatie van het geïnfecteerde systeem te achterhalen gebruikmakende van het publieke IP-adres. Als het IP-adres uit Oekraïne komt dan laat Conficker dat systeem met rust! Er is dus een grote kans dat de makers uit Oekraïne komen.

In contrast met de andere worms besproken in deze paragraaf is Conficker heel geduldig en zorgt het niet voor een grote netwerkactiviteit. Een mogelijke verklaring daarvoor kan zijn dat Conficker op die manier niet wil ontdekt worden.

Nog een volledig revolutionaire techniek die Conficker gebruikt is digitale handtekening-technologie om alle binnenkomende bestanden naar Conficker gericht (om Conficker bijvoorbeeld te updaten) te controleren of het wel van de maker van Conficker komt.

1.2.6.2 Enkele verschillen tussen de varianten van Conficker

Conficker.A kijkt na of het keyboard de keyboard layout van Oekraïne heeft, als dat zo is dan zal Conficker deze pc met rust laten. Vanaf Conficker.B zit deze functie er niet meer ingebakken.

Conficker probeert zich ook steeds te updaten. Daarvoor kijken Conficker.A en Conficker.B elke dag naar 250 verschillende websites of er daar geen update op staat. Die URL's van die 250 websites worden dynamisch gegenereerd aan de hand van de datum. Om Conficker tegen te gaan is er een groep, de Conficker Cabal groep met bedrijven zoals Microsoft, die de 250 URL's zelf registreert zodat ze geen update kunnen bevatten. Bij Conficker.C worden er zo geen 250 URL's gegenereerd, doch maar liefst 50 000!

Conficker.B probeert te verhinderen dat je het kan verwijderen door anti-virus software uit te zetten en bepaalde websites te blokkeren waar je updates kan halen.

Sinds Conficker.E wordt er ook commerciële malware mee geïnstalleerd in de vorm van ondermeer nep anti-virus software [18].

1.2.6.3 Conficker & Metasploit

Waarom is Conficker nu belangrijk in dit onderzoek? Wel als laatste stap van de penetration test wordt er getest hoe het systeem reageert op een aanval gericht naar de vulnerabilty die gedicht wordt door de MS08-067 patch. Dit wordt gedaan met een exploit die in Metasploit zit. Met die exploit wordt dus een aanval van Conficker nagebootst omdat die dezelfde vulnerabilty uitbuit.

De kwaadaardige payload van Conficker zit natuurlijk niet bij de exploitmodule van Metasploit. De payload is de code die uitgevoerd wordt op het besmette systeem na het inbreken. De manier waarop ze inbreken in een systeem is bij Conficker en Metasploit wel gelijkaardig. Er is zelfs code gevonden in Conficker die afgekeken is van de exploitmodule van Metasploit [19]!

1.3 Opbouw tekst

Je vernam reeds dat er in dit werkstuk firewalls gaan bestudeerd en vergeleken worden. Elke firewall zal om de beurt onderworpen worden aan een reeks testen. Hoe die testen zijn aangepakt lees je in de volgende paragraaf '1.4 Plan van aanpak'.

Allereerst wordt er in hoofdstuk 2 ISA Server 2006 behandeld.

Vervolgens zal in hoofdstuk 3 Juniper SSG 20 besproken worden.

En als laatste zal in hoofdstuk 4 Check Point R70 aan bod komen.

Vergeet ook zeker dit eerste hoofdstuk niet te lezen want het vormt de basis van het verdere onderzoek.

Dit werkstuk is in de eerste plaats geschreven als een onderbouwd onderzoek, maar het zit tevens boordevol praktische tips die zijn voortgevloeid uit het onderzoek. Deze praktische tips zal je niet snel in andere werken over security kunnen vinden.

Ben je een netwerkbeheerder? Lees dan zeker de besluiten en de teksten met de muisaanwijzer-icoon. Vooral de paragrafen 'Voorbeeldpolicy toepassen' zal interessant zijn voor jou.

Ben je enkel geïnteresseerd in dit onderzoek in het algemeen en ben je niet van plan om het met dit werkstuk in de praktijk aan de slag te gaan? Dan kan je de teksten met het muisaanwijzer-icoon en de paragrafen 'Voorbeeldpolicy toepassen' links laten liggen.

Je zal merken dat Engelse vakterminologie vaak bewust niet worden vertaald. Deze woorden zijn nu eenmaal gangbaar binnen het vakgebied van netwerkbeveiliging. Moesten deze woorden toch vertaald worden zou dit de duidelijkheid van dit werkstuk niet ten goede komen.

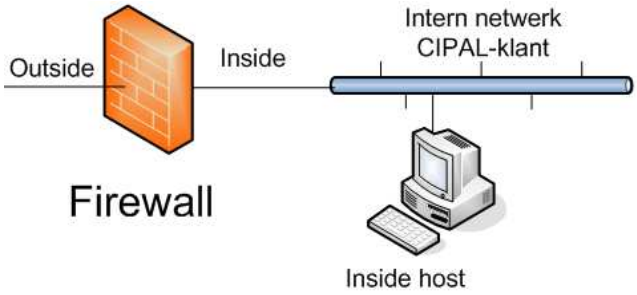
Als er wordt gesproken over 'een systeem', dan wordt daar een pc of een server mee bedoeld.

Vaak wordt er gesproken over een 'hacker'. Daarmee wordt dan een 'Black Hat' hacker bedoeld. Dat is een hacker met slechte bedoelingen. Dit wordt ook wel eens, vooral vroeger, een 'cracker' genoemd. Dat woord is echter minder en minder gangbaar en wordt daarom niet gebruikt.

1.4 Plan van aanpak

Om het onderzoek eenvormig, reproduceerbaar en duidelijk te houden wordt er nu een stappenplan opgesteld dat bij elke firewall wordt gevolgd. Eerst wordt de 'prijs' van de firewall behandeld, die altijd in bedragen zonder BTW wordt uitgedrukt. Indien nodig wordt de prijs omgerekend van Amerikaanse dollar naar euro. Daarna volgt de 'eerste kennismaking' waarin je ondermeer kan kennis maken met de interface van de firewall. Bij die kennismaking kan je ook steeds lezen hoe de firewall policy er default uit ziet.

Om de firewalls te evalueren zal er daarna telkens aan penetration testing gedaan worden. Dit zal gebeuren vanaf een systeem aan de outside interface van de firewall. Dit systeem moet een hacker vanaf het internet simuleren. Hieronder zie je een schema van de labopstelling.



Figuur 1.3

Stap 1: Penetration test met default configuratie

Het is moeilijk om firewalls objectief te beoordelen. Alle firewalls verschillen namelijk in de manier waarop ze een security policy (beveiligingsbeleid) toepassen. Hoe kan je dan een firewall beter testen wanneer ze nog helemaal geen policy toepassen. Dat is reden één waarom deze stap er in zit. Reden twee is om een inzicht te geven over wat de standaard instellingen zijn van een firewall. Dit is namelijk bij alle firewall anders. De ene zet bijvoorbeeld alles open, de andere alles toe. Dit inzicht moet diegene die de firewall configureert (hierna 'netwerkbeheerder' genoemd) hier zeker en vast hebben zodat die daar rekening mee kan houden. Bij elke deelstap hoort de output oftewel het resultaat van een van de geselecteerde netwerktools.

Stap 1a: Scan met Nmap

Er wordt gestart met het scannen met Nmap. Er zijn diverse scan profielen gedefinieerd in Nmap. Er is gekozen om te scannen met het 'intense scan, no ping' profiel omdat dit zowat de meest geavanceerde voorgedefinieerde scan is en omdat die doorheen het onderzoek de beste resultaten kon voorleggen. Met een packet sniffer zoals Wireshark is bevonden dat Nmap tijdens die scan maar liefst 2051 paketten verstuurt. Het aantal pakketten dat terugkomt van het gescande systeem is meestal een maat voor het aantal poorten die open staan want voor elke poort die open staat moet het systeem een pakket sturen om dit te laten weten.

Het commando dat bij het 'intense scan, no ping' profiel aan Nmap wordt gegeven is nmap -A -v -PN -T4 en daarna het IP-adres van het te scannen systeem. Hieronder vind je de uitleg van de verschillende opties [7][23]:

- -A: Zorgt voor OS en versie detectie, script scanning en traceroute.
- -v: 'Verbosity level' verhogen.
- -PN: Pingt de host niet om te zien of het opstaat. Het scant het systeem alsof het zeker opstaat.
- -T4: Agressieve timing, voor een snelle scan.

De output van dat commando zal telkens gegeven worden. In die output zal je steeds een regel vinden die zegt dat het systeem op staat ('… is up'). Dit wil echter niets zeggen [24] want Nmap doet alsof het systeem opstaat zoals je hierboven kan lezen met de optie –PN. Interessante regels van de output zullen iedere keer in het vet gezet worden.

Oorspronkelijk zaten de scans met het profiel 'regular scan' ook in dit onderzoek. Dit scanprofiel geeft geen opties mee aan Nmap. Deze regular scans zijn echter weggelaten wegens niet relevant. De regular scan gebruikt pingen (ICMP Echo Request) om te zien of het systeem op staat en maakt dan meestal de verkeerde conclusie dat het systeem niet opstaat. De keren dat pingen lukte (als er dus een ICMP echo reply kwam) gaf de regular scan dezelfde informatie als de 'intense scan, no ping'.

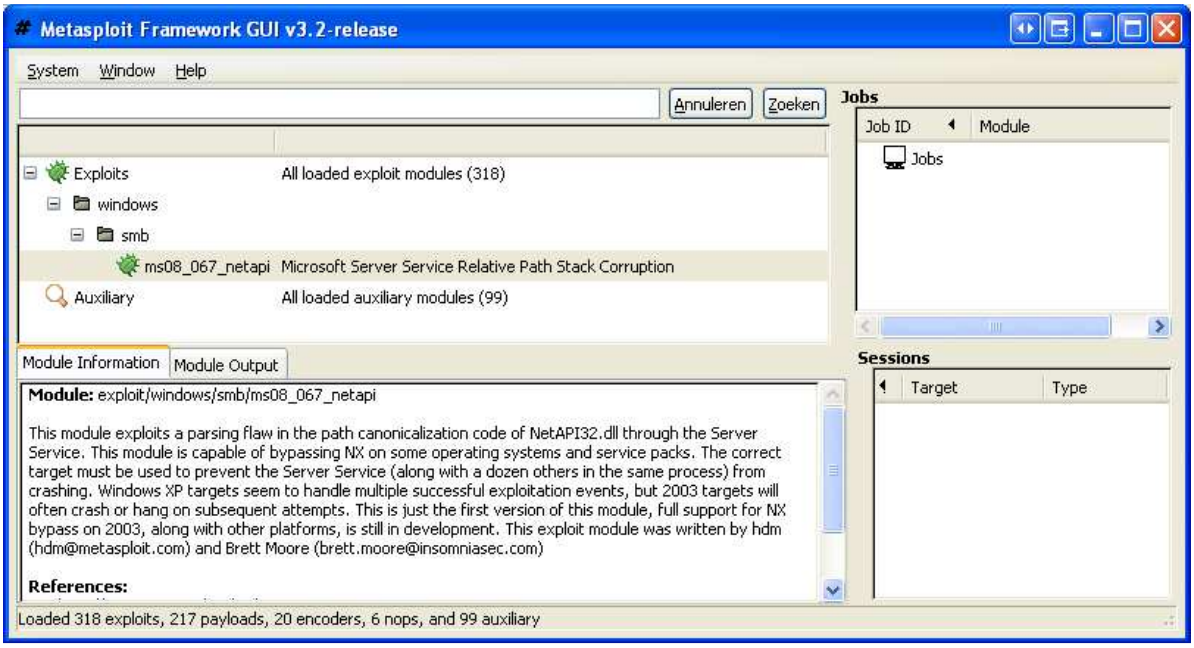
Stap 1b: Scan met Nessus

Nessus wordt gebruikt om de vulnerabilities bloot te leggen. Hierbij worden alle beschikbare plug-ins van Nessus geselecteerd zodat er op alle vulnerabilities gescand wordt.

Initieel stuurt Nessus steeds een 'TCP ping' en controleert het een aantal bekende poorten. Als hier geen reactie op komt, staakt Nessus zijn scan omdat het denkt dat het systeem niet op staat. Af en toe zal er daarom geen output verschijnen bij het scannen door Nessus. In die gevallen zal dat steeds vermeld worden.

Stap 1c: Aanval met Metasploit

Hier wordt er gezien of de firewall de Conficker-worm tegenhoudt of niet. Hiervoor wordt de MS08-067 exploit van Metasploit losgelaten. Metasploit heeft een exploitmodule die 'ms08_067_netapi: Microsoft Server Service Patch Stack Corruption' heet.



Figuur 1.4

Met die module kan een hacker de bijhorende vulnerability misbruiken zodat het zijn payload kan laten uitvoeren op het systeem. Meestal kiest de hacker dan een payload waardoor hij volledige controle heeft over het gekraakte systeem. Tijdens de penetration testen wordt er gevarieerd tussen de verschillende mogelijke payloads van Metasploit.

De module is geschreven in de programmeertaal Ruby (lijkt fel op C-code). Hier is er een klein stukje uit:

```
…
if(target['auto'])

      mytarget = nil

      print_status("Automatically detecting the target...")
      fprint = smb_fingerprint()

      print_status("Fingerprint: #{fprint['os']} #{fprint['sp']} -
```

```
lang:#{fprint['lang']}")
…
```

Dit stukje code geeft deze Module Output:

```
09:45:47 - ms08_067_netapi [*] Automatically detecting the
target...
09:45:50 - ms08_067_netapi [*] Fingerprint: Windows XP Service Pack
2 - lang:Dutch
```

Besluit

Na de penetration test komt er telkens een besluit waarin conclusies worden getrokken over de output van de drie programma's.

Stap 2: Penetration test met voorbeeldpolicy

Stap 2a, 2b en 2c zijn vergelijkbaar met stap 1a, 1b en 1c waarbij achtereenvolgens Nmap, Nessus en Metasploit wordt gebruikt om het systeem te testen. Het 'besluit' wordt hier ook analoog aan toegevoegd. Het verschil is nu dat de firewall een bepaalde voorbeeldpolicy heeft toegepast. Zie 1.5 voor de voorbeeldpolicy en zie de laatste paragraaf voor de werkwijze van het toepassen van die voorbeeldpolicy op de firewall.

Stap 3: Penetration test van inside host

Tot nu toe werd er altijd getest wat een hacker naar de externe interface van de firewall toe kan aanrichten. Maar de primaire taak van een firewall is nog altijd om zijn interne systemen te beschermen. Dan is het ook logisch dat dit geëvalueerd wordt, en dit met stap 3. Hierin wordt er een penetration test uitgevoerd van een outside systeem naar de inside host.

Weer is er een stap 3a voor Nmap, stap 3b voor Nessus, stap 3c voor Metasploit en een besluit waarin voorlopige conclusies worden getrokken.

Stap 4: Penetration test vanuit inside LAN

Hoe moet verkeer van het private LAN en terug naar het private LAN behandeld worden? Goede vraag, zullen de firewallproducenten denken want hier bestaan nog geen algemene normen voor. Deze test is dan ook interessant om te zien hoe de bewuste firewall dat verkeer hanteert. Dit is des te meer interessant met betrekking tot worms, virussen en interne hackers die een bedreiging vormen komende van het interne netwerk want deze reële bedreiging werd vroeger wel eens vergeten.
Intern op het netwerk kan er bijvoorbeeld een boze werknemer zijn die zo veel mogelijk schade wil aanrichten tijdens zijn ontslagtermijn. Worms en virussen die via mail op de pc van onwetende werknemers belanden vormen ook een reëel gevaar vanuit het interne netwerk.

Stap 5: IPS

IPS (Intrusion Prevention System) wordt meestal in een adem genoemd met IDS (Intrusion Detection System). IDS is een systeem om aanvallen te detecteren en IPS is een systeem om ze tegen te houden. Vaak lopen deze functies bij een firewall in elkaar over. Daarom wordt vanaf nu in dit werkstuk enkel gesproken van IPS als overkoepelende term voor IDS en IPS samen. In bepaalde literatuur wordt er ook wel eens gesproken van IDPS [25] of IDP [26].

Een belangrijk aspect van het onderzoek in dit werkstuk is het onderzoeken van de IPS-capaciteiten van de firewalls m.a.w. de capaciteiten van het detecteren, loggen en tegenhouden van aanvallen en portscans van Nmap, Nessus en Metasploit.

Na deze 5 stappen volgt telkens het onderdeel 'voorbeeldpolicy toepassen'.

Voorbeeldpolicy toepassen

In stap 2 wordt er een penetration test uitgevoerd op de firewall waar de voorbeeldpolicy op is toegepast. In deze paragraaf lees je hoe die voorbeeldpolicy is geconfigureerd op die firewall.

Een firewall rule toevoegen

Als je weet hoe je één firewall rule moet toevoegen dan kan je de rest van de voorbeeldpolicy ook toepassen. Dat toevoegen van een rule aan de firewall policy wordt hier dan ook gedocumenteerd. Een firewall rule is een regel die je toevoegt aan de firewall waarin je duidelijk specifieert wat er door mag of net niet.

URL filtering

Een belangrijke functie die alle firewalls geleidelijk aan aan het toevoegen zijn is URL filtering waarbij de firewall kan beslissen of een bepaalde website mag bekeken worden of niet.

Deep inspection

Deep inspection (oftewel deep packet inspection) is de volgende stap in de evolutie van de firewalls. Het houdt in dat er wordt gekeken tot op de hoogste laag, de applicatielaag. Meestal wordt deze functie geïmplementeerd in de firewall met behulp van een signature-database. Dat is een database met gekende patronen van een aanval, programma … waarop moet gezocht worden in een pakket. Als die signature gevonden wordt in een pakket kan dat pakket gedropt worden.

Zoals je in de voorbeeldpolicy (zie 1.5) kan lezen is er gekozen om Windows (Live) Messenger te blokkeren, via een signature. Hierbij wordt de deep inspection capaciteiten van de firewalls duchtig getest.

Deep inspection loopt een beetje over in IPS want ze worden allebei gebruikt om aanvallen tegen te houden. Om onderscheid te maken wordt in dit werkstuk deep inspection gezien als de *techniek* om tot in de applicatielaag te gaan inspecteren. En IPS wordt gezien als de verzamelnaam voor alle technieken om aanvallen tegen te houden.

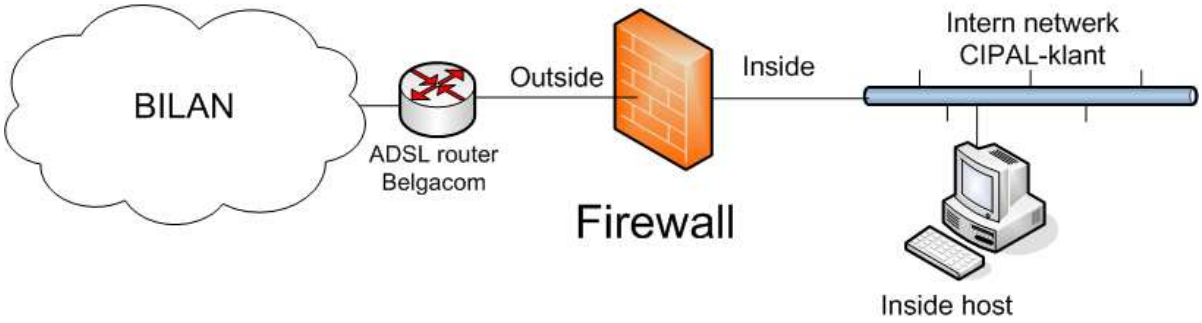
De uiteindelijke firewall policy

Hier vind je telkens een screenshot van de firewall policy nadat de voorbeeldpolicy is toegepast.

1.5 De voorbeeldpolicy

Een security policy is een document dat de beveiliging voor een organisatie op vlak van informatica beschrijft. Dit document mag je heel ruim zien en zal vaak vele pagina's omvatten. De security policy bepaalt ook altijd de instellingen van de firewall. De concrete instellingen van de firewall wordt in dit werkstuk de 'firewall policy' genoemd. In de security literatuur bestaat er echter geen algemeen woord voor.

Om de lezer heel wat werk te besparen wordt in dit werkstuk de security policy herleid tot de essentiële criteria die de instellingen van de firewall bepalen. Deze criteria worden vanaf nu de voorbeeldpolicy genoemd. Het zijn namelijk criteria of richtlijnen die zo zijn gekozen dat ze voor een algemeen doorsnee netwerk kunnen dienen. In praktijk is het gebaseerd op de netwerken van CIPAL-klanten. Zie volgende figuur voor een gemiddelde topologie van de CIPAL-klanten.



Figuur 1.5

Links in de topologie zie je een wolkje met daarin 'BILAN' geschreven. BILAN is een MPLS VPN van de CIPAL-klant naar het CIPAL-netwerk (dat CIPORT heet) over de infrastructuur van Belgacom. Aangezien het niet is geweten hoe de infrastructuur van Belgacom er uit ziet wordt dat stuk voorgesteld als een wolk.

De voorbeeldpolicy:

- HTTP:
  - Van inside naar outside moet HTTP en HTTPS doorgelaten worden.
  - Van inside naar outside moet aan URL filtering worden gedaan zodat websites als facebook.com kunnen geblokkeerd worden.
  - Windows Live Messenger en Windows Messenger moet worden geblokkeerd.

- FTP:
  - Van inside naar outside moet FTP doorgelaten worden, omdat bijvoorbeeld sommige software-sites hun software ter beschikking stellen via FTP.
- DNS:
  - Van inside naar outside moet DNS doorgelaten worden.

- Logging:
  - Er moet zo veel mogelijk aan logging worden gedaan.
  - Als de firewall niet genoeg vast geheugen heeft dan moet voor een alternatieve manier worden gezorgd, bij voorkeur een syslog-server waar de logs naar gestuurd moeten worden.

- Remote Desktop Protocol:
  - RDP moet toegelaten worden vanuit de pc van de netwerkbeheerder naar het interne netwerk toe.

- NAT:
  - De firewall moet niet aan NAT doen want het interne netwerk is rechtstreeks verbonden met het CIPORT netwerk via een MPLS VPN.

- ICMP:
  - Pingen moet overal mogelijk zijn

- Deny all:
  - Alle andere protocollen moeten tegengehouden worden.

Er wordt bij voorkeur geen NAT gebruikt. Er kan opgemerkt worden dat deze situatie zonder NAT, vergelijkbaar is met een situatie waarin er static NAT gebruikt wordt. Static NAT wordt zeer vaak gebruikt voor systemen zoals interne webservers die toegankelijk moeten zijn voor het internet. In beide gevallen kan een internet-gebruiker dus aan het interne systeem.

Je kan ook bedenkingen maken bij de beperktheid van deze voorbeeldpolicy. In een gemiddeld netwerk zullen er meestal meer richtlijnen zijn voor zaken zoals interne webservers. Wel, de voorbeeldpolicy is bewust beknopt gehouden. Dit omdat dit werkstuk niet gaat over 'hoe stel je de verschillende functies van een firewall in'. De voorbeeldpolicy is dus kort en bondig om niet te ver af te wijken van de essentie van dit werkstuk.

1.6 Inside host

Achter onze firewall komt een onveilige inside host die als een soort honeypot (systeem met beveiligingsgaten om hackers aan te trekken) gaat gebruikt worden voor hackers van buiten. 'Buiten' is in dit geval niet het internet maar een gecontroleerde testomgeving.
De onveilige pc heeft Microsoft Windows XP Professional Service Pack 2 als besturingssysteem, zonder Windows updates. Dit laatste gegeven zorgt ervoor dat die pc een goudmijn is voor mogelijke hackers. Zo zal later te zien zijn dat die pc ook niet bestand is tegen de exploit die de Conficker-worm gebruikt. Windows Firewall staat ook uit, dit om duidelijk te zien wat de geteste firewalls doen en niet wat Windows Firewall doet.

Net zoals later met de drie verschillende firewalls gaat gebeuren, gaat er nu een penetration test toegepast worden op de inside host. Dit om te bewijzen hoeveel beveiligingsgaten dit systeem heeft, zodat die later gedicht kunnen worden door de firewalls.

1.6.1 Stap a: Scan met Nmap

De eerste stap van de penetration test is de scan met Nmap. Hieronder vind je de output oftewel de informatie die Nmap geeft over het systeem dat gescand is.

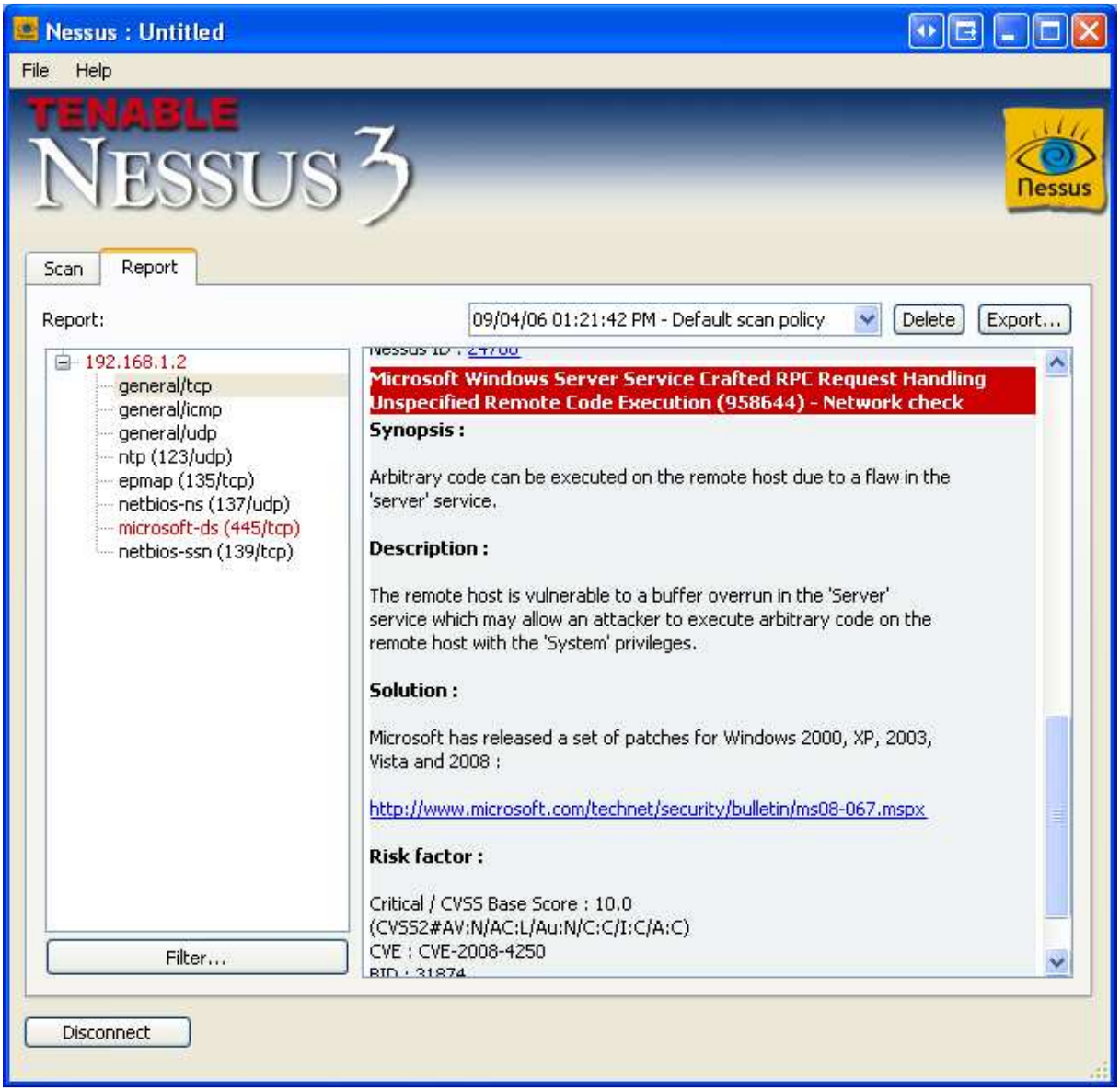
Intense scan, no ping (Nmap commando: nmap -A -v -PN -T4 10.130.223.11):

```
Starting Nmap 4.85BETA7 ( http://nmap.org ) at 2009-04-07 11:31 Romance
(zomertijd)

Initiating Parallel DNS resolution of 1 host. at 11:31
Completed Parallel DNS resolution of 1 host. at 11:31, 6.51s elapsed

Initiating SYN Stealth Scan at 11:31
Scanning wxpxx (10.130.223.11) [1000 ports]
Discovered open port 445/tcp on 10.130.223.11
Discovered open port 139/tcp on 10.130.223.11
Discovered open port 135/tcp on 10.130.223.11
Completed SYN Stealth Scan at 11:31, 0.38s elapsed (1000 total ports)

Initiating Service scan at 11:31
Scanning 3 services on wxpxx (10.130.223.11)
Completed Service scan at 11:31, 6.02s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against wxpxx (10.130.223.11)
10.130.223.11: guessing hop distance at 1
Initiating Traceroute at 11:31
```

```
Completed Traceroute at 11:31, 0.02s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 11:31
Completed Parallel DNS resolution of 2 hosts. at 11:31, 0.01s elapsed
NSE: Initiating script scanning.
Initiating NSE at 11:31
Completed NSE at 11:31, 0.39s elapsed

Host wxpxx (10.130.223.11) is up (0.000017s latency).
Interesting ports on wxpxx (10.130.223.11):
Not shown: 997 closed ports

PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Device type: general purpose

Running: Microsoft Windows XP
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003

Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=254 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows
Host script results:
|  nbstat: NetBIOS name: WXPXX, NetBIOS user: <unknown>, NetBIOS MAC:
00:e0:00:9b:1d:71
|  Name: WXPXX<00>            Flags: <unique><active>
|  Name: WXPXX<20>            Flags: <unique><active>
|  Name: WERKGROEP<00>        Flags: <group><active>
|  Name: WERKGROEP<1e>        Flags: <group><active>
|  Name: WERKGROEP<1d>        Flags: <unique><active>
|_ Name: \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|  smb-os-discovery: Windows XP
|  LAN Manager: Windows 2000 LAN Manager
|  Name: WERKGROEP\WXPXX
|_ System time: 2009-04-07 11:31:23 UTC+2

TRACEROUTE (using port 199/tcp)
HOP RTT   ADDRESS
1   10.00 10.130.209.1
2   0.00  wxpxx (10.130.223.11)

Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 17.40 seconds           Raw
packets sent: 1018 (45.506KB) | Rcvd: 1020 (41.390KB)
```

1.6.2 Stap b: Scan met Nessus

Nessus geeft deze output:



Figuur 1.6

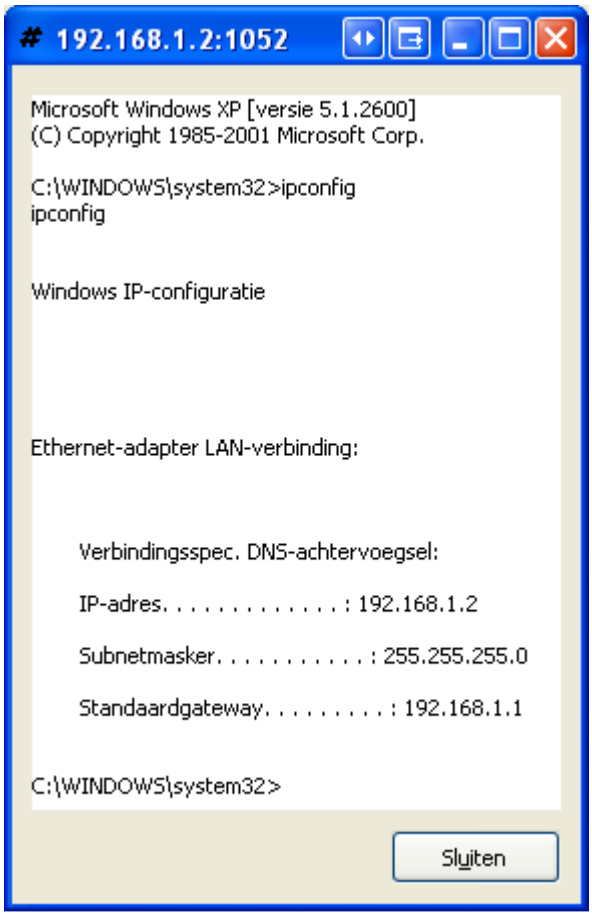
Nessus vindt in totaal maar liefst 6 kritische risico's. Zoals je in de screenshot kan zien ziet Nessus dat het systeem vatbaar is voor de Conficker worm. Nessus geeft bij de vulnerabilities waar mogelijk een manier waarop je het lek kan dichten, in dit geval geeft hij als 'Solution' aan dat je de MS08-067 patch moet installeren.

1.6.3 Stap c: Aanval met Metasploit

Bij het gebruiken van deze exploit-module krijg je volgende Module Ouput:

```
09:45:44 - ms08_067_netapi [*] Launching exploit
windows/smb/ms08_067_netapi...
09:45:47 - ms08_067_netapi [*] Started reverse handler
09:45:47 - ms08_067_netapi [*] Automatically detecting the target...
09:45:50 - ms08_067_netapi [*] Fingerprint: Windows XP Service Pack 2 -
lang:Dutch
09:45:50 - ms08_067_netapi [*] Selected Target: Windows XP SP2 Dutch (NX)
09:45:50 - ms08_067_netapi [*] Triggering the vulnerability...
09:45:50 - [*] Session 1 created for 192.168.1.2:1052
```

Als payload is gekozen voor een command-shell op te vragen. Zoals je hieronder kan zien is de aanval gelukt en is er met een heuse command-shell toegang tot onze pc!



Figuur 1.7

Nu kan je, als hacker, bijna alles op de nietsvermoedende pc doen wat je maar wil, mits een beetje kennis van MS-DOS commando's. Zo kan je bijvoorbeeld een FTP server op de pc downloaden en die openzetten zodat je aan alle bestanden die je wil kan.

In totaal duurt de attack 6 seconden (kan je nakijken in de Module Output) en is hij 96 pakketten groot (te zien met wireshark).

Je kan ook andere payloads uitproberen. Zo is het gelukt om in plaats van een shell op te vragen, een user met administratieve rechten aan te maken op de inside host alsook om een VNC-server DLL te injecteren en die te draaien vanuit het geheugen van de inside host. Dan is het hek natuurlijk helemaal van de dam voor de hacker! Het uittesten van deze exploit liep niet altijd van een leien dakje. Zo crasht de te exploiten service, het 'Generic Host Process for Win32 Services', ook vaak zodat je er niets meer mee kan doen. Metasploit crasht ook wel eens.

Figuur 1.8

1.6.4 Besluit

De inside host is in deze penetration test zeer onveilig bevonden. Nmap geeft aan dat de gevaarlijke poorten voor worms (zie 1.2.6 Conficker en andere bekende worms) open staan. Die poorten zorgen dus voor best wat zware beveiligingslekken, 6 volgens Nessus. Dit wordt dan ook bewezen met Metasploit waarmee simpelweg volledige controle over de inside host verkregen is.

1.7 Windows Server 2003 zonder patches

Met deze test wordt er gezien hoe het zit met de beveiliging van de server die het besturingssysteem Windows Server 2003 R2 Standard Edition met Service Pack 2 draait. Op deze server gaat namelijk de software van ISA Server 2006 en achteraf Check Point R70 geïnstalleerd worden. Er draait geen enkele vorm van firewall tijdens deze test.

1.7.1 Stap a: Scan met Nmap

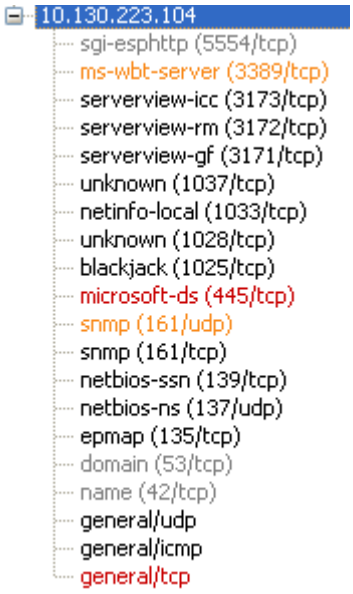
Intense scan, no ping:

```
Starting Nmap 4.76 ( http://nmap.org ) at 2009-03-30 12:39 Romance
(zomertijd)

Initiating Parallel DNS resolution of 1 host. at 12:39
Completed Parallel DNS resolution of 1 host. at 12:39, 0.00s elapsed

Initiating SYN Stealth Scan at 12:39
Scanning 10.130.223.104 [1000 ports]
Discovered open port 53/tcp on 10.130.223.104
Discovered open port 3389/tcp on 10.130.223.104
Discovered open port 1028/tcp on 10.130.223.104
Discovered open port 1033/tcp on 10.130.223.104
Discovered open port 445/tcp on 10.130.223.104
Discovered open port 1025/tcp on 10.130.223.104
Discovered open port 1037/tcp on 10.130.223.104
Discovered open port 42/tcp on 10.130.223.104
Discovered open port 139/tcp on 10.130.223.104
Discovered open port 135/tcp on 10.130.223.104
Completed SYN Stealth Scan at 12:39, 1.34s elapsed (1000 total ports)


Initiating Service scan at 12:39
```

```
Scanning 10 services on 10.130.223.104
Completed Service scan at 12:40, 48.69s elapsed (10 services on 1 host)
Initiating OS detection (try #1) against 10.130.223.104
10.130.223.104: guessing hop distance at 1
Initiating Traceroute at 12:40
Completed Traceroute at 12:40, 0.03s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 12:40
Completed Parallel DNS resolution of 2 hosts. at 12:40, 0.00s elapsed
SCRIPT ENGINE: Initiating script scanning.
Initiating SCRIPT ENGINE at 12:40
Completed SCRIPT ENGINE at 12:40, 0.00s elapsed

Host 10.130.223.104 appears to be up ... good.
Interesting ports on 10.130.223.104:
Not shown: 990 closed ports

PORT     STATE SERVICE       VERSION
42/tcp   open  wins          Microsoft Windows Wins
53/tcp   open  domain        Microsoft DNS
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
445/tcp  open  tcpwrapped
1025/tcp open  msrpc         Microsoft Windows RPC
1028/tcp open  msrpc         Microsoft Windows RPC
1033/tcp open  msrpc         Microsoft Windows RPC
1037/tcp open  msrpc         Microsoft Windows RPC
3389/tcp open  microsoft-rdp Microsoft Terminal Service

Device type: general purpose

Running: Microsoft Windows 2003
OS details: Microsoft Windows Server 2003 SP1 or SP2
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows

TRACEROUTE (using port 80/tcp)
HOP RTT   ADDRESS
1   16.00 10.130.209.1
2   0.00  10.130.223.104

Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 53.61 seconds
           Raw packets sent: 1072 (47.882KB) | Rcvd: 1021 (41.564KB)
```

1.7.2 Stap b: Scan met Nessus

Nessus vindt twee kritische risico's (in het rood), waaronder de MS08-067 vulnerability, en twee medium risico's (in het oranje).



Figuur 1.9

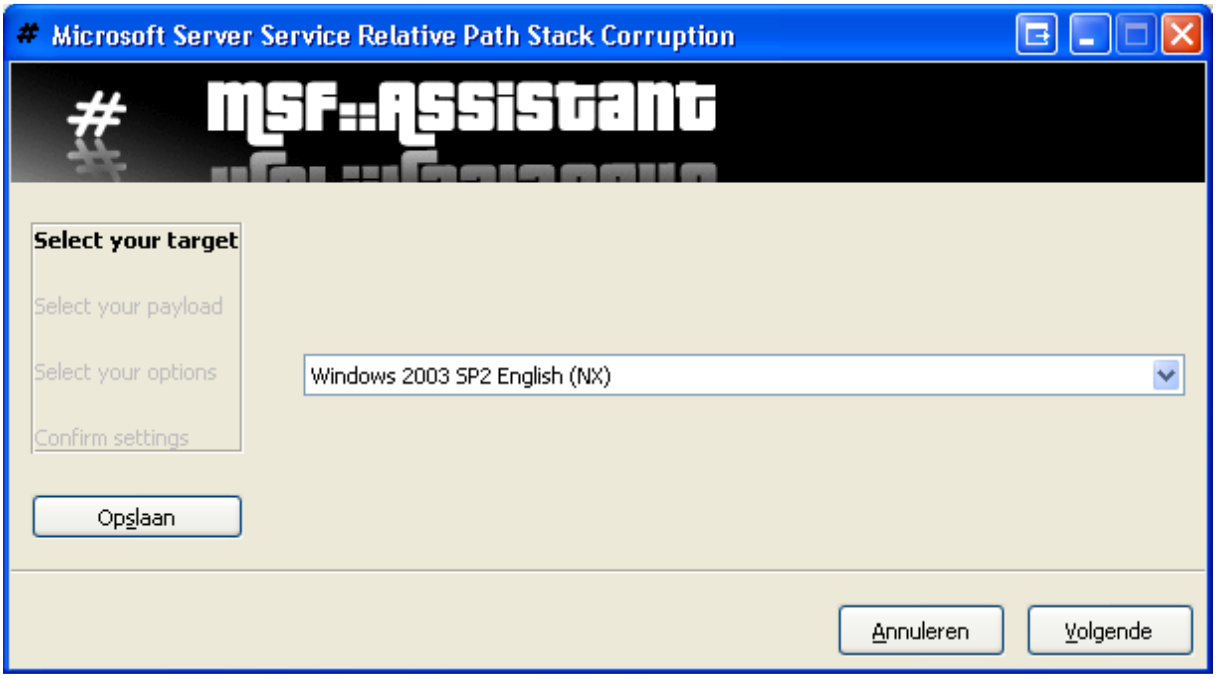
Bij wijze van voorbeeld van een medium risico hier een stukje uit de uitleg die Nessus geeft over de open poort, ms-wbt-server (3389/tcp).

Figuur 1.10

Nessus zegt dat een man-in-the-middle attack mogelijk is. Het valt te begrijpen dat dit maar een medium risico factor inhoudt want dergelijke aanval is heel geavanceerd en kan enkel in perfecte omstandigheden uitgevoerd worden.

1.7.3 Stap c: Aanval met Metasploit

Bij de opties van de exploit moet je nog wel even meegeven dat het target systeem ‘Windows 2003 SP2 English (NX)’ is. Daarbij ‘auto’ kiezen zoals je bij een Windows XP systeem kon, werkt hier niet.



Figuur 1.11

Als payload wordt er nu gekozen voor een VNC-server DLL te injecteren en die te draaien vanuit het geheugen van de inside host. Bijgevolg kan de pc leukweg overgenomen worden.

Figuur 1.12

1.7.4 Besluit

Net zoals bij de inside host heeft deze Windows Server 2003 enorme beveiligingsgaten die gemakkelijk uit te buiten zijn. Nmap geeft om te beginnen al veel open poorten aan. Nessus geeft twee gevaarlijke risico's aan. En met Metasploit kan het systeem van

op afstand overgenomen worden. Het is dus aan de software-firewalls ISA Server 2006 en Check Point R70 om hier iets aan te doen.

1.8 Server voor ISA Server en Check Point

ISA Server 2006 en Check Point R70 zijn softwarepakketten. Software moet geïnstalleerd worden op hardware, een server in dit geval. Om de prijzen later te vergelijken is er een server samengesteld op dell.com die een doorsnee server voor een middelgrote organisatie moet voorstellen. Er is gekozen voor een DELL PowerEdge R200.

De specificaties:

- Dual Core Intel® Xeon® E3120, 3.16GHz, 6MB Cache, 1333MHz FSB
- 4GB Memory, DDR2, 800MHz
- Één jaar basisgarantie Next Business Day (NBD)
- RAID 1 (mirroring) opstelling met 2 identieke harde schijven van 250 GB
- Intel® PRO 1000VT Quad Port Gigabit Network Card

De totaalprijs: € 1 104,30

2 ISA SERVER 2006

Dit hoofdstuk handelt over de evaluatie van Microsoft ISA Server 2006 (hierna regelmatig verkort tot ISA Server of ISA). ISA Server zal ingezet worden aan de rand van het netwerk tussen het interne en het externe netwerk (m.a.w. als een internet edge firewall). Wie aan ISA Server denkt, denkt aan Microsoft. Wie aan Microsoft denkt, denkt aan de vele ontdekte vulnerabilities van zijn besturingssystemen (zie ondermeer 1.2.6 Conficker en andere bekende worms). Er zijn dus vaak sterke vooroordelen rond de beveiliging van Microsoft producten. Of deze terecht zijn of niet met betrekking tot ISA Server, dat kom je hier te weten.

2.1 Prijs

Als er producten worden getest moeten de prijzen natuurlijk ook vergeleken worden. We moeten daarvoor dus de prijs weten van ISA Server 2006.

Voor deze test is de Enterprise Edition van ISA Server 2006 geïnstalleerd. Die versie is enkel voor grotere bedrijven die extra functionaliteit nodig hebben indien er met meerdere ISA Servers in array gewerkt wordt. [ISA UNLEASHED P19] Onze resultaten van het onderzoek voor de Enterprise Edition zouden echter niet verschillen van die van een Standard Edition omdat die array-functionaliteit niet gebruikt wordt in dit onderzoek.

De kosten van de hardware en het gastbesturingssysteem moeten ook in rekening gebracht worden. Als besturingssysteem is er gekozen voor Windows Server 2003 Standard Edition.

Hier zijn de officiële bedragen van Microsoft [27]:

- Enterprise Edition
  - € 4 250,99 per processor
- Standard Edition
  - € 1 062,22 per processor
- Microsoft Windows Server 2003, Standard Edition
  - € 707,91 per server

De bedragen zijn omgerekend van Amerikaanse dollar naar euro.

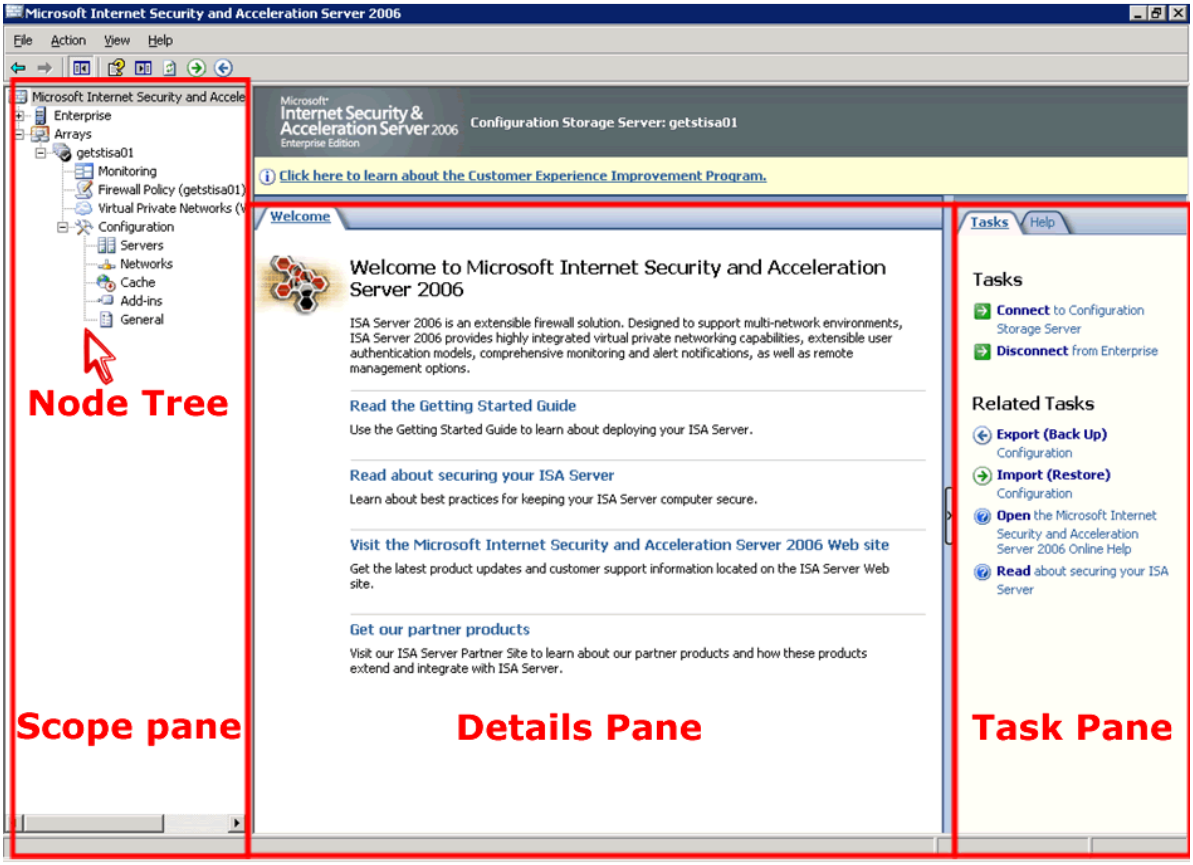
Vergeet niet de kosten van de server die in 1.8 berekend is op € 1 104,30.

Het totale kostenplaatje met de Standard Edition zou € 2 874,43 zijn.

2.2 Eerste kennismaking

2.2.1 Interface

ISA Server is te bedienen met een Graphical User Interface (GUI). Bij wijze van eerste kennismaking met ISA Server zie je die hieronder.



Figuur 2.1

Op de screenshot zie je de ISA Server 'Management Console', dat verder ISA management console zal worden genoemd. In deze ISA management console zijn er verschillende 'areas' of 'panes'. Zo heb je de Scope Pane aan de linker kant waarin de verzameling van alle nodes, de Node Tree, staat. Nodes zijn de verschillende vensters waarin je de aparte functies van ISA Server kan bekijken en instellen.

Verder heb je de Details Pane dat het hoofdscherm is van de gekozen node.

Ten laatste heb je het deel waarin vaak gebruikte taken van de gekozen node staan, de Task Pane. Ook is daar telkens een help tab waarin je meer informatie kan vinden over de huidige node.

De Task Pane en de Details Pane verandert van inhoud telkens je een andere node kiest.

De eerste hoofdnode die je tegenkomt is 'Enterprise', die staat er enkel in de Enterprise Edition van ISA Server 2006. Dit is een node die enkel nodig is als je een heleboel ISA Servers in je netwerk hebt staan.

2.2.2 Windows Server 2003 downtime

Er wordt wel eens gezegd dat de betrouwbaarheid van Microsoft besturingssystemen een stuk slechter uitvalt dan de UNIX & Linux tegenhangers. Alsook dat die besturingssystemen een grote downtime hebben. Downtime is de tijd waarin de server niet in werking is omdat het bijvoorbeeld aan het heropstarten is. Duidelijke onderzoeken omtrent deze veronderstelde onbetrouwbaarheid zijn echter moeilijk te vinden en bovendien spreken ze elkaar vaak tegen [28][29][30].

Wat wel een zeker feit is, is dat Microsoft besturingssystemen regelmatig updates nodig hebben waarbij het systeem moet heropgestart worden. Het valt echter aan te raden

om op de server zeker niet te kiezen voor automatische updates zodat je controle hebt over welke updates worden geïnstalleerd. Als er updates zijn waarvoor de server moet heropgestart worden en dit hinderlijk is voor de gebruiker, dan kan je die best enkel installeren als het echt niet anders kan.

2.2.3 Microsoft Forefront Threat Management Gateway

De volgende versie van ISA Server zal Microsoft Forefront Threat Management Gateway heten, oftewel Forefront TMG. Het past binnen Microsofts nieuwe security productlijn, dat Forefront heet.

Wat is er veranderd aan Forefront TMG ten opzichte van ISA Server 2006? Er zijn vele belangrijke functies bijgekomen zoals IPS, e-mail protection (tegen virussen en spam) en malware protection via HTTP [31].

ISA Server 2006 werkt niet op Windows Server 2008. Forefront TMG zal er wel op werken maar dan enkel de 64bit versie ervan. Het systeem waar het op draait moet dus ook een 64-bit processor bevatten.

2.2.4 Wat zet de firewall default open?

Wat zet ISA Server allemaal open voor alle hosts op het interne netwerk en op het externe netwerk (het internet)? Het antwoord is *niets*! Daarvoor zorgt de laatste regel in de Firewall Policy (zie onderstaande figuur). ISA Server laat het dus aan jou, de netwerkbeheerder, om de protocollen open te zetten die specifiek nodig zijn voor je netwerk.

Figuur 2.2

Naar de Local Host (de server zelf) toe zet ISA Server wel bepaalde protocollen open. Daarvoor moet je kijken bij de System Policy Rules, in de Firewall Policy Node. In totaal zijn er zo'n 32 standaard ingestelde System Policy Rules, waarvan er 12 nog disabled staan. Aangezien de regels zo goed als geen beveiligingsrisico met zich meebrengen worden er hier maar een paar besproken. Zo zie je een paar van die regels in volgende figuur.

Figuur 2.3

De eerste regel laat DNS verkeer dat gestart wordt vanuit de server naar eender waar toe. De tweede regel doet hetzelfde voor DHCP aanvragen. De derde regel laat toe dat de DHCP server op het interne netwerk DHCP replies mogen sturen. Door de laatste regel mag er vanuit bepaalde systemen gepingd worden naar de ISA Server. Andere systemen mogen dit standaard echter niet.

2.3 Stap 1: Penetration test met default configuratie

Eerder is al aangetoond dat de server waar ISA Server op geïnstalleerd wordt grote beveiligingsgaten vertoont. Nu gaat de beveiliging van de server na installatie van ISA

Server 2006 onderzocht worden. Hierbij is belangrijk te weten dat alles volledig 'out-of-the-box' is. Dat wil zeggen dat alles ingesteld staat zoals het default staat en dat er geen vorm van updates geïnstalleerd zijn, voor Windows Server 2003 noch ISA Server 2006. Op ISA Server 2006 is tevens Service Pack 1 nog niet geïnstalleerd.

2.3.1 Stap 1a: Scan met Nmap

Intense scan, no ping:

```
Starting Nmap 4.76 ( http://nmap.org ) at 2009-03-09 15:18 Romance
(standaardtijd)

Initiating Parallel DNS resolution of 1 host. at 15:18
Completed Parallel DNS resolution of 1 host. at 15:18, 0.00s elapsed

Initiating SYN Stealth Scan at 15:18
Scanning 10.130.223.104 [1000 ports]
SYN Stealth Scan Timing: About 28.05% done; ETC: 15:20 (0:01:17 remaining)
Discovered open port 8080/tcp on 10.130.223.104
Completed SYN Stealth Scan at 15:19, 39.08s elapsed (1000 total ports)

Initiating Service scan at 15:19
Scanning 1 service on 10.130.223.104
Completed Service scan at 15:19, 6.20s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 10.130.223.104
Retrying OS detection (try #2) against 10.130.223.104
Initiating Traceroute at 15:19
10.130.223.104: guessing hop distance at 1
Completed Traceroute at 15:19, 0.03s elapsed
Initiating Parallel DNS resolution of 3 hosts. at 15:19
Completed Parallel DNS resolution of 3 hosts. at 15:19, 0.00s elapsed
SCRIPT ENGINE: Initiating script scanning.
Initiating SCRIPT ENGINE at 15:19
Completed SCRIPT ENGINE at 15:19, 0.02s elapsed

Host 10.130.223.104 appears to be up ... good.
Interesting ports on 10.130.223.104:
Not shown: 999 filtered ports

PORT     STATE SERVICE    VERSION
8080/tcp open  http-proxy Microsoft ISA Server http proxy
Warning: OSScan results may be unreliable because we could not find at
least 1 open and 1 closed port
Device type: general purpose

Running (JUST GUESSING) : Microsoft Windows 2003 (98%)
Aggressive OS guesses: Microsoft Windows Server 2003 Enterprise Edition
SP2 (98%), Microsoft Windows Server 2003 SP2 (98%), Microsoft Windows
Server 2003 SP1 or SP2 (93%)
No exact OS matches for host (test conditions non-ideal).
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows

TRACEROUTE (using port 8080/tcp)
HOP RTT   ADDRESS
1   31.00 10.130.209.1
2   0.00  10.130.223.104
Read data files from: C:\Program Files\Nmap
```

```
OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/.

Nmap done: 1 IP address (1 host up) scanned in 54.92 seconds
           Raw packets sent: 2085 (96.780KB) | Rcvd: 119 (12.097KB)
```

De belangrijkste regel is de regel hieronder, waarin je ziet dat je te maken hebt met een Microsoft ISA Server. Dit is zeer belangrijke informatie voor de hacker.

```
8080/tcp open  http-proxy Microsoft ISA Server http proxy
```

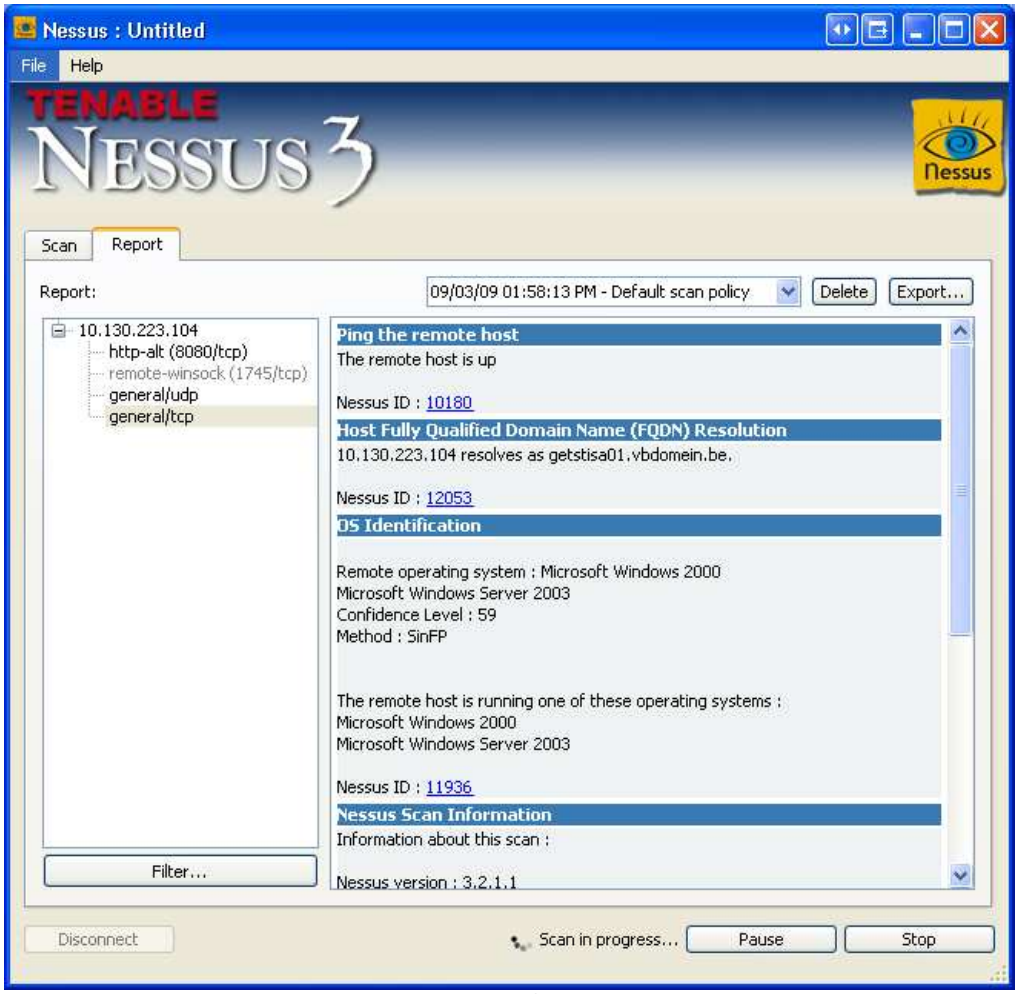
Het is opmerkelijk dat het lijkt alsof er gebruik kan gemaakt worden van de proxy functionaliteit van ISA Server vanaf de externe interface. De proxy staat echter default enkel open voor systemen op het interne netwerk. Na een tweede test met een volledig nieuwe installatie van Windows Server en ISA Server 2006 is deze 'merkwaardigheid' ook opgedoken. Na een derde test was dit dan weer niet meer het geval.

Al de andere 999 poorten die Nmap heeft getest zijn dichtgetimmerd door ISA Server.

Je kan ook zien dat Nmap zegt dat het besturingssysteem 'Microsoft Windows Server 2003 Enterprise Edition SP2' is. Dit klopt, buiten dat het geen Enterprise Edition is maar een Standard Edition.

2.3.2 Stap 1b: Scan met Nessus

Nessus geeft volgend figuur als resultaat.



Figuur 2.4

Je ziet hierbij dat er geen enkele kritische vulnerability is gevonden. De poort 8080 wordt natuurlijk wel weer aangegeven als open, maar zonder dat daar een zware vulnerability voor is gevonden.

2.3.3 Stap 1c: Aanval met Metasploit

Misschien klopt de output van Nessus niet en wordt Conficker wel doorgelaten? Om dat te testen kan je de exploit van MS08-067 loslaten. Dit geeft volgende Module Output:

```
16:47:30 - Initialized the Metasploit Framework GUI.
16:49:25 - ms08_067_netapi [*] Launching exploit
windows/smb/ms08_067_netapi...
16:49:29 - ms08_067_netapi [*] Started reverse handler
16:49:39 - ms08_067_netapi [-] Exploit failed: The connection timed out
(10.130.223.104:445).
```

Dit werkt niet meer, Nessus had dus gelijk.

2.3.4 Besluit

Dat ISA Server geen enkel zwaar risico nog open laat is toch wel uiterst verrassend! Als je ISA Server, zonder enige updates, installeert op een Windows Server 2003 waarvan de beveiliging een zeef is (omdat er ook geen updates op geïnstalleerd zijn) is plots de beveiliging toch adequaat! Voor ISA Server en voor Windows Server 2003 lijkt de Conficker-exploit als het ware een zero-day attack. Dat is een attack waar nog geen patch voor bestaat. Toegegeven, er bestaat wel een patch voor maar ISA Server en Windows Server hebben deze niet en ze hebben nog geen mogelijkheid om die te downloaden.

Al dan niet het belangrijkste argument om ISA Server als onveilig te bestempelen, is dat het moet draaien op een Windows systeem. En Windows systemen zijn, zonder de juiste updates, volgens eerder onderzoek heel onveilig. Dit argument valt nu volledig weg omdat de ISA Server het Windows systeem waterdicht maakt, zelfs voor zero-day attacks! Er is wel een puntje van kritiek dat je daarop dan weer kan hebben. Namelijk dat het Windows systeem mogelijk niet meer waterdicht zal zijn als er eigen firewall policy rules worden gemaakt die bepaalde services naar de ISA Server toch toelaten. De boodschap is dus: zet geen extra services open naar de ISA Server zelf en gebruik hem dus enkel als firewall!

2.4 Stap 2: Penetration test met voorbeeldpolicy

In deze stap 2 wordt er een penetration test uitgevoerd op de server met Windows Server 2003 als besturingssysteem en met ISA Server 2006 erop geïnstalleerd. Beiden hebben al de laatste nieuwe updates geïnstalleerd om zo veel mogelijk een werkelijke implementatie in een organisatie na te bootsen. Om diezelfde reden is natuurlijk ook de voorbeeldpolicy ingesteld.

2.4.1 Stap 2a: Scan met Nmap

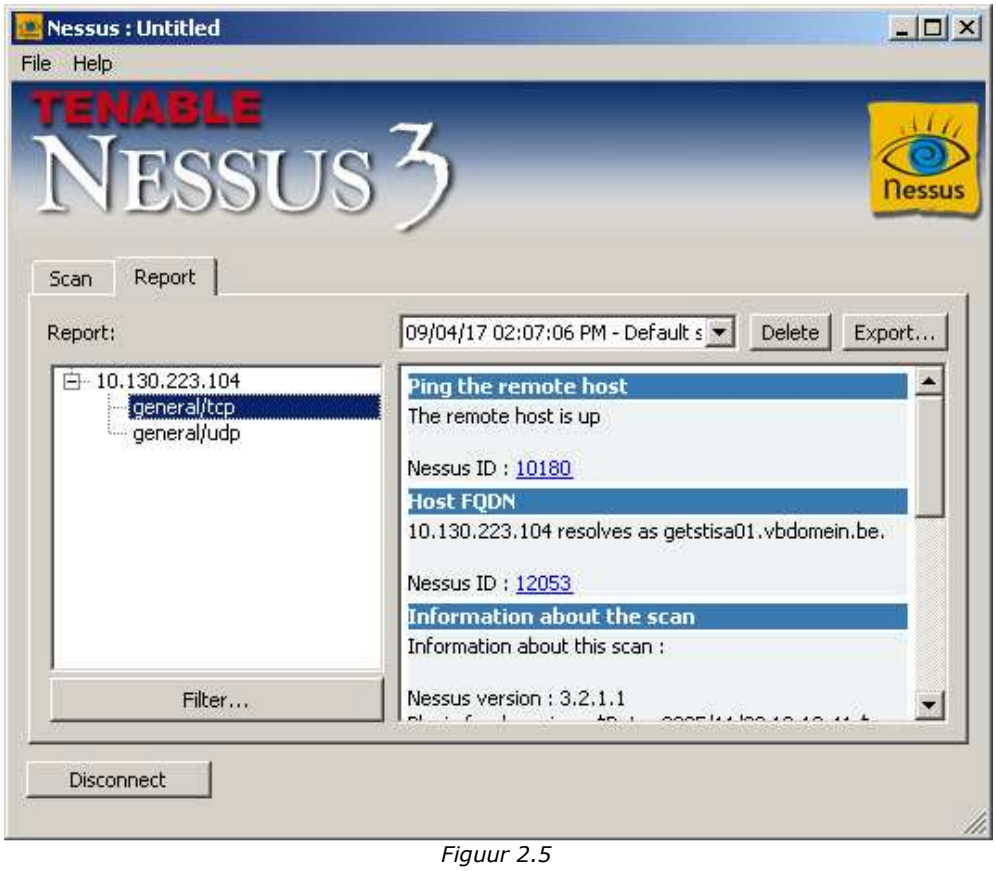
Intense scan, no ping:

```
Starting Nmap 4.85BETA7 ( http://nmap.org ) at 2009-04-17 15:12 Romance
(standaardtijd)
Initiating Parallel DNS resolution of 1 host. at 15:12
Completed Parallel DNS resolution of 1 host. at 15:12, 6.50s elapsed
```

```
Initiating SYN Stealth Scan at 15:12
Scanning getstisa01.vbdomein.be (10.130.223.104) [1000 ports]
SYN Stealth Scan Timing: About 29.50% done; ETC: 15:14 (0:01:14 remaining)
SYN Stealth Scan Timing: About 58.50% done; ETC: 15:14 (0:00:43 remaining)
Completed SYN Stealth Scan at 15:14, 104.22s elapsed (1000 total ports)

Initiating Service scan at 15:14
Initiating OS detection (try #1) against getstisa01.vbdomein.be
(10.130.223.104)
Retrying OS detection (try #2) against getstisa01.vbdomein.be
(10.130.223.104)
NSE: Initiating script scanning.

Host getstisa01.vbdomein.be (10.130.223.104) is up (0.00s latency).

All 1000 scanned ports on getstisa01.vbdomein.be (10.130.223.104) are
filtered

Too many fingerprints match this host to give specific OS details
Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 113.80 seconds
           Raw packets sent: 2042 (93.604KB) | Rcvd: 83 (27.522KB)
```

Nmap geeft aan dat er helemaal geen open poorten zijn.

2.4.2 Stap 2b: Scan met Nessus



Figuur 2.5

Met Nessus krijg je net zoals met Nmap bijna geen enkele informatie.

2.4.3 Stap 2c: Aanval met Metasploit

Zoals je dan ook kan verwachten maakt Conficker hier geen kans:

Een deel van de Module Output van de MS08-067-module van Metasploit:

```
15:30:18 - ms08_067_netapi [-] Exploit failed: The connection timed out
(10.130.223.104:445).
```

2.4.4 Besluit

De tools zijn geen vulnerabilities tegen gekomen. De beveiliging zit dus snor! Een beter resultaat kan je niet verwachten.

2.5 Stap 3: Penetration test van inside host

Bij stap 3 wordt een penetration test uitgevoerd op de inside host dat Windows XP draait en dat wordt beschermd door de ISA firewall. De voorbeeldpolicy is ondertussen erop geconfigureerd. Even een herinnering dat de beveiliging van de inside host bewust waardeloos is gehouden. Zoals aangetoond, heeft de inside host dus meerdere vulnerabilities zoals de vulnerability van Conficker.

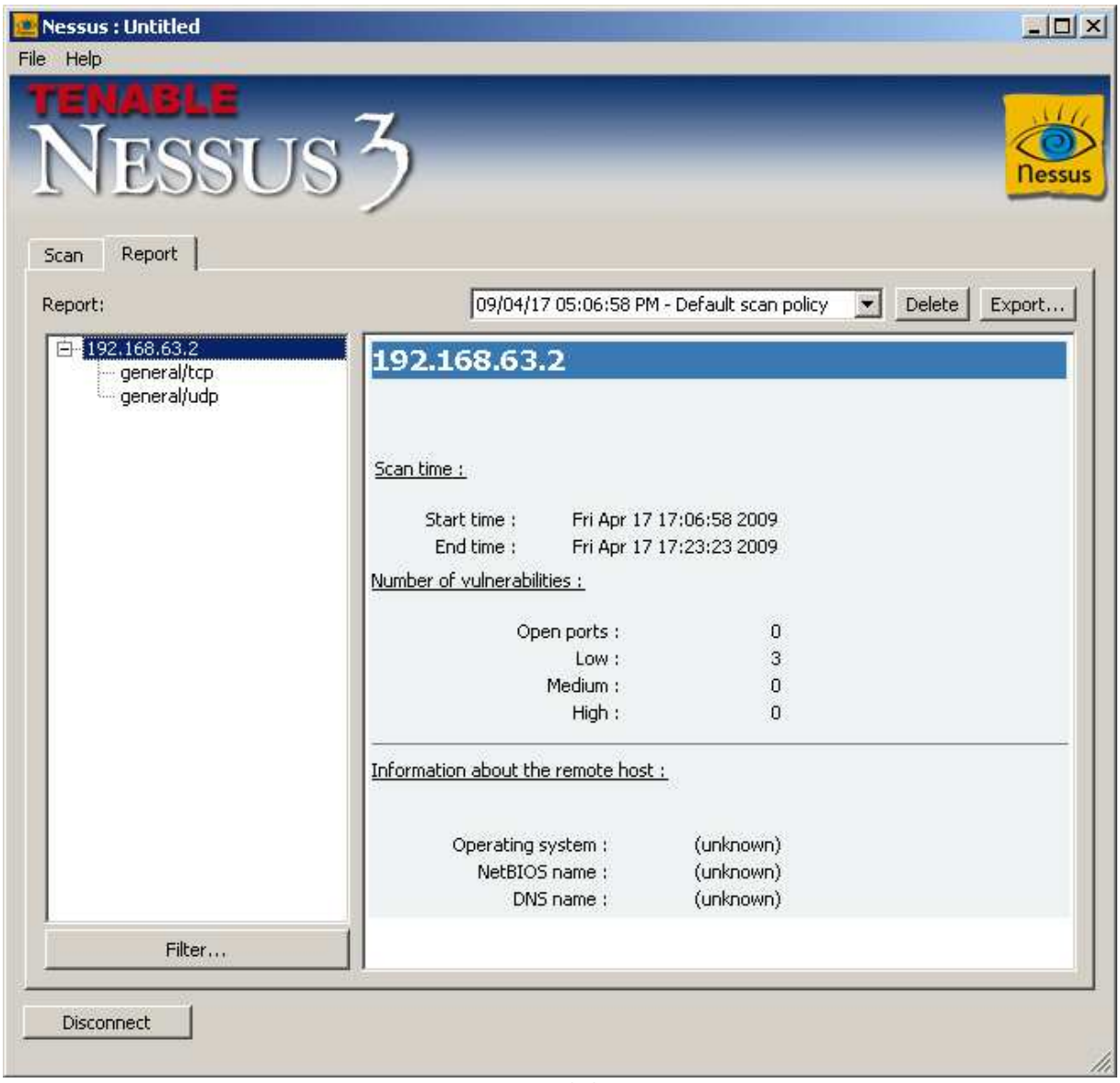
2.5.1 Stap 3a: Scan met Nmap

Intense scan, no ping:

```
Starting Nmap 4.85BETA7 ( http://nmap.org ) at 2009-04-17 15:40 Romance
(standaardtijd)
Initiating Parallel DNS resolution of 1 host. at 15:40
Completed Parallel DNS resolution of 1 host. at 15:40, 0.00s elapsed

Initiating SYN Stealth Scan at 15:40
Scanning 192.168.63.2 [1000 ports]
SYN Stealth Scan Timing: About 29.00% done; ETC: 15:42 (0:01:16 remaining)
SYN Stealth Scan Timing: About 58.00% done; ETC: 15:42 (0:00:44 remaining)
Completed SYN Stealth Scan at 15:42, 104.22s elapsed (1000 total ports)

Initiating Service scan at 15:42
Initiating OS detection (try #1) against 192.168.63.2
Retrying OS detection (try #2) against 192.168.63.2
NSE: Initiating script scanning.
Host 192.168.63.2 is up (0.00s latency).

All 1000 scanned ports on 192.168.63.2 are filtered

Too many fingerprints match this host to give specific OS details
Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 107.42 seconds
           Raw packets sent: 2042 (93.604KB) | Rcvd: 2 (356B)
```

Nmap vindt geen enkele open poort.

2.5.2 Stap 3b: Scan met Nessus



Figuur 2.6

Net zoals bij Nmap geeft Nessus zo goed als geen informatie over de inside host met slechte beveiliging.

2.5.3 Stap 3c: Aanval met Metasploit

```
16:53:26 - ms08_067_netapi [*] Launching exploit
windows/smb/ms08_067_netapi...
16:53:28 - ms08_067_netapi [*] Started reverse handler
16:53:39 - ms08_067_netapi [-] Exploit failed: The connection timed out
(192.168.63.2:445).
```

Dit is niet gelukt dus, maar dat kon je al verwachten vanuit de output van Nmap en Nessus.

Besluit

Dit is een uiterst verrassend resultaat want je krijgt geen enkele informatie over de inside host waarvan de beveiliging volledig lek is. ISA Server beschermt onze inside host dus vrijwel perfect! Er heersen zo'n grote vooroordelen rond ISA Server omdat die

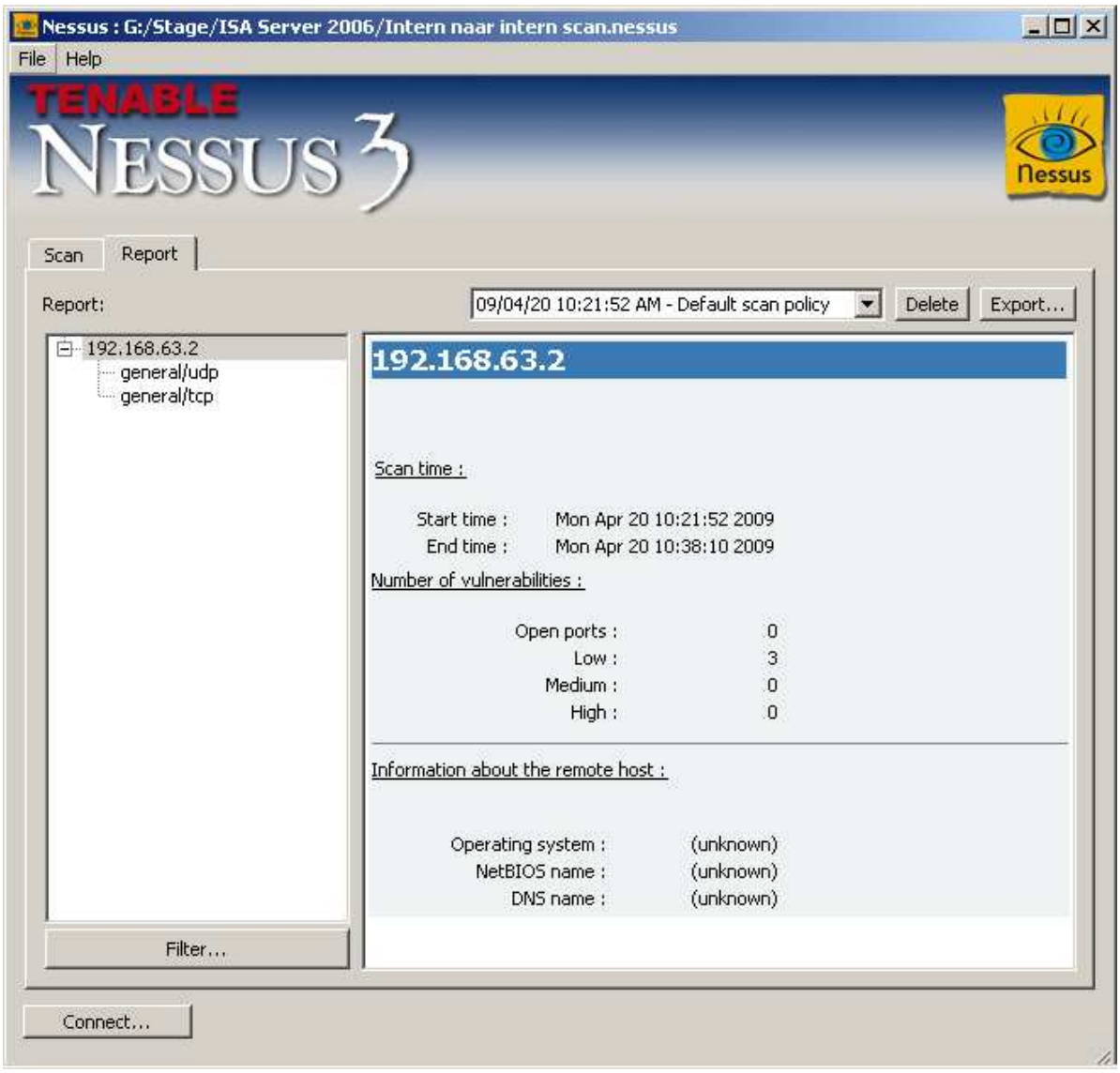
op een Microsoft besturingssysteem werkt. Die vooroordelen klinken logisch en zal je daarom gemakkelijk geloven. Nu weet je echter hoe het werkelijk zit.

2.6 Stap 4: Penetration test vanuit inside LAN

In de volgende stap gaat er gekeken worden wat een worm of hacker kan aanrichten als die zich al in het interne netwerk bevindt.

2.6.1 Vanuit inside naar inside

De scan van Nmap is hier weggelaten omdat het dezelfde informatie geeft als Nessus.

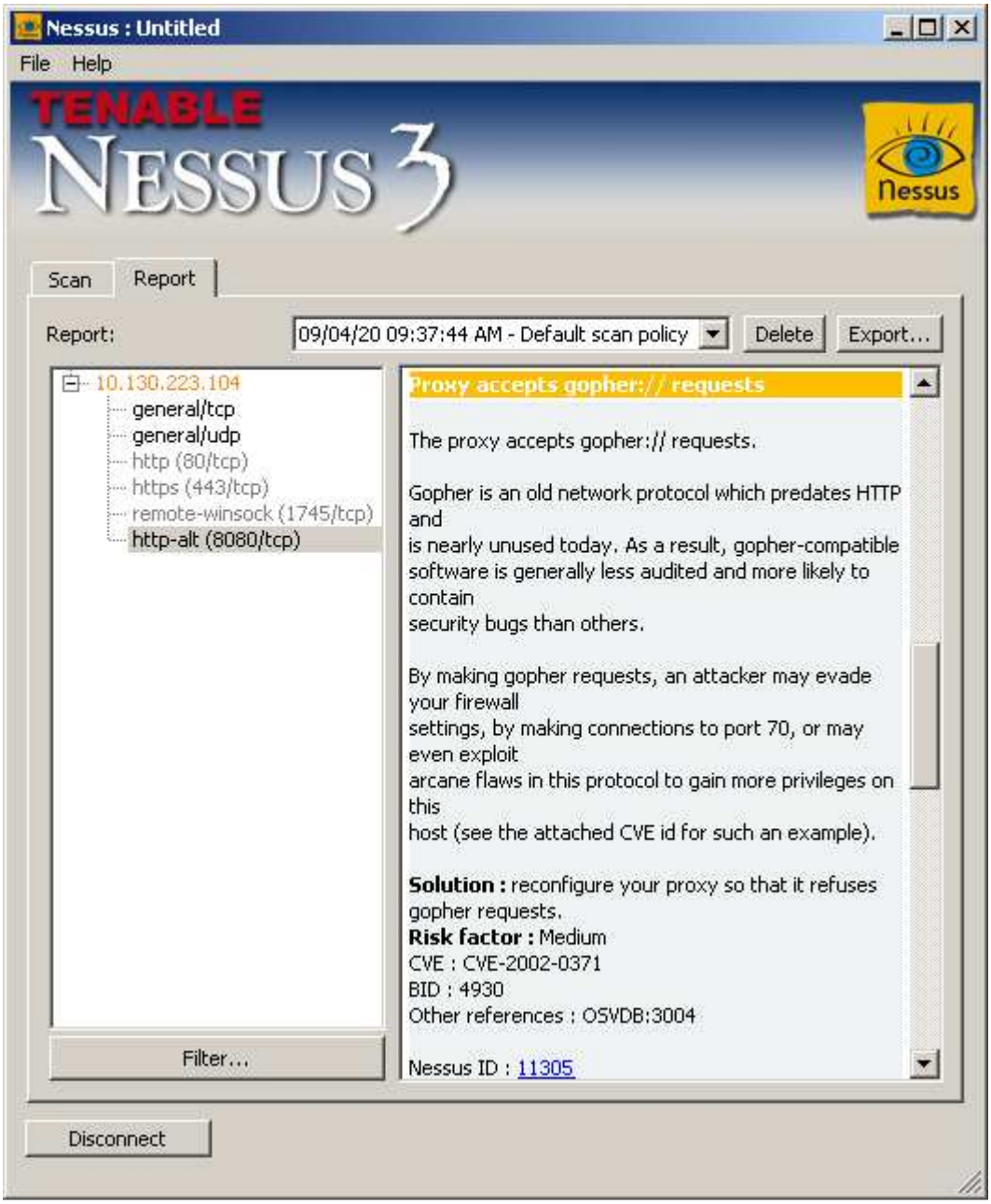


Figuur 2.7

Nessus geeft zo te zien geen informatie over een ander systeem op het interne netwerk, buiten dat het aan staat. De verklaring hiervoor is dat er in de Firewall Policy geen regels staan die verkeer van het intern netwerk naar het intern netwerk toelaten. Enkel pingen (ICMP Echo Request paketten) wordt toegelaten.

2.6.2 Van inside naar ISA Server 2006

De scan van Nmap is ook hier niet getoond omdat het dezelfde informatie presenteert als Nessus.



Figuur 2.8

Je ziet vier protocollen die de ISA Server heeft open staan voor het interne netwerk. Dit zijn gelukkig protocollen die geen grote vulnerabilities hebben, dat ze open staan geeft dus geen zware risico's. Er is wel (maar) een medium risico, zoals je boven in de screenshot ziet. De open poort 80 (HTTP), 443 (HTTPS) en HTTP-alt (8080) hebben te maken met de proxy-functie van ISA. De remote-winsock poort (1745) dient voor het doorlaten van het controle kanaal tussen ISA en zijn firewall clients [32]. Firewall clients zijn pc's in het interne LAN die extra beschermd worden door de Firewall Client software. Die Firewall Client software is speciaal gemaakt om in combinatie met ISA Server gebruikt te worden.

Nessus wist ook uit te vissen dat het besturingssysteem Windows 2000 of Windows Server 2003 is.

2.6.3 Besluit

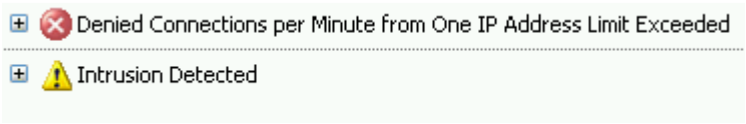
ISA Server 2006 laat standaard geen verkeer van en naar het inside netwerk toe, net zoals al het andere verkeer die het tegenhoudt met de laatste 'deny all'-regel in de policy. Je moet dus zelf bepalen wat er wel mag doorgelaten worden. Deze aanpak van ISA Server zorgt ervoor dat hackers en worms vanuit het interne netwerk geen schijn van kans maken.

2.7 Stap 5: IPS

Er wordt nu onderzocht wat er in de logs verschijnt van onze penetration tests en in hoeverre ISA de tools in hun werk kan hinderen.

2.7.1 Na scan met Nmap

Na de Nmap-scan zie je dit in de Monitoring Node van ISA Server:



Figuur 2.9

Bij de beschrijving van de 'Intrusion Detected'-event staat dit: 'ISA Server detected a possible Internet Protocol (IP) half-scan attack from IP address 10.130.209.95.'

2.7.1.1 Een half-scan attack

Even uitleggen wat een half-scan attack is.

Een normale TCP connectie wordt als volgt opgebouwd:

1) Client: SYN
2) Server: SYN/ACK
3) Client: ACK

Dit is wat men noemt een 'three way handshake'. Een half-scan attack wijkt daarvan af.

Een half-scan attack wordt als volgt opgebouwd:

1) Client: SYN
2) Server: SYN/ACK

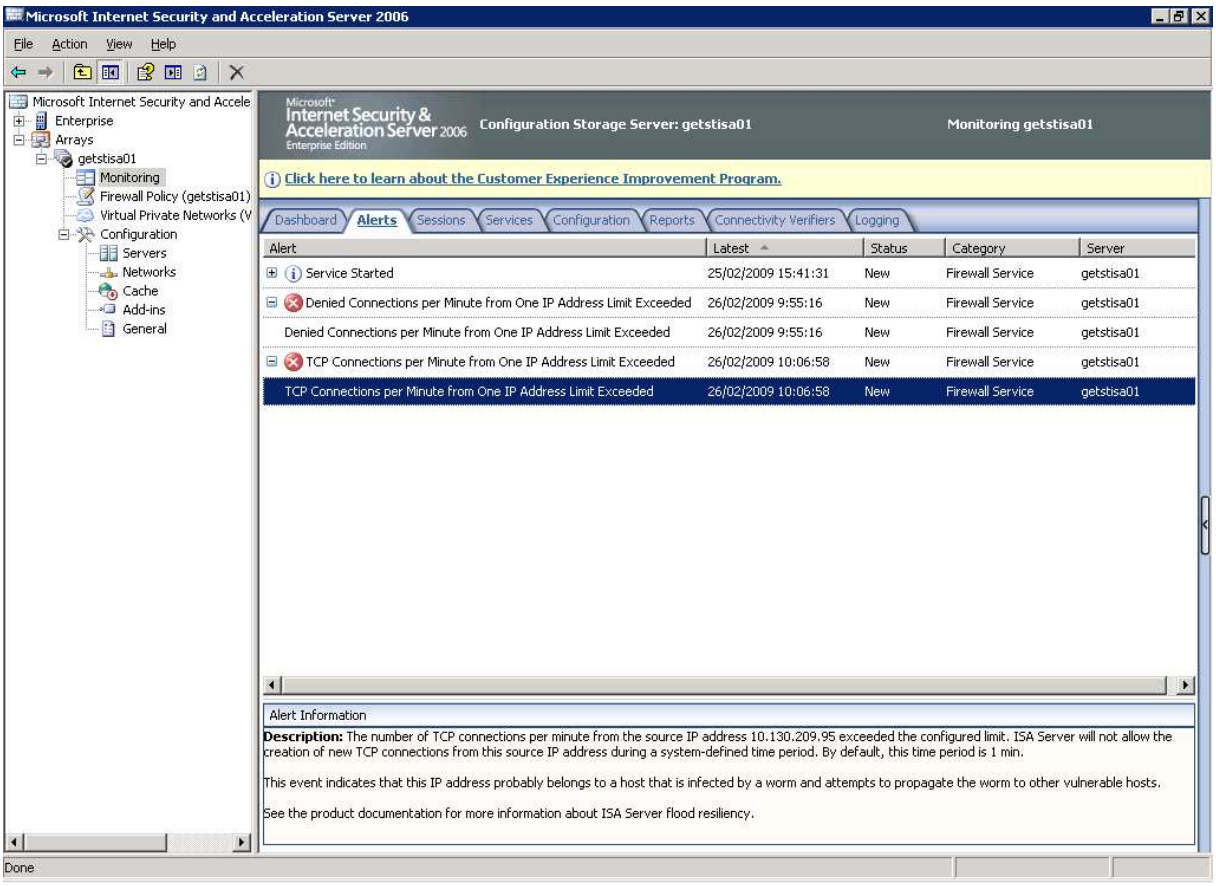
Het belangrijkste is dat er geen derde stap is. Er wordt geen laatste ACK (acknowledge) gestuurd door de client, in dit geval de hacker. Deze methode wordt gebruikt om snelheid te verhogen [2] en security apparaten te misleiden omdat er geen volledige connectie gemaakt wordt, geen volledige connectie is dan gelijk aan geen connectie. Dit misleiden is in dit geval dus niet volledig gelukt.

In de vierde regel van de output van Nmap zie je dat Nmap een SYN Stealth Scan toepast. Dit is een van de andere namen voor een half-scan. Nog andere namen ervoor zijn half-open scan [33], SYN scanning [2] en Finish Packet (FIN) scan [26].

Zo zie je dat er veel onenigheid is rond begrippen in de network security literatuur.

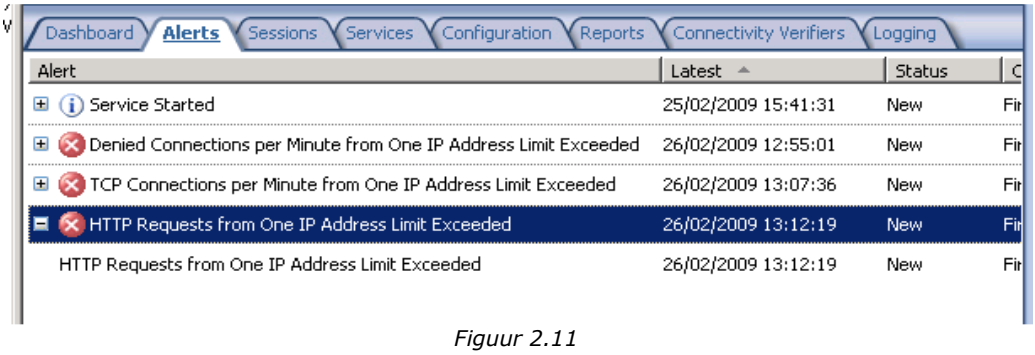
2.7.2 Na scan met Nessus

Na de vulnerability scan met Nessus vind je in het Alerts tab de informatie van volgende figuur terug.



Figuur 2.10

Je ziet in de Alert Information, onderaan, dat ISA Server 2006 zegt dat de pc 10.130.209.95 een host met een worm is die te veel TCP connecties aan het maken is. De uitleg dat het een worm moet zijn geweest klopt dus niet, maar het is geen belangrijke fout.



Figuur 2.11

Telkens je Nessus inzet om de server te testen geeft ISA andere alerts. Soms geeft ISA aan dat er teveel HTTP connecties zijn en soms dat er teveel TCP connecties zijn, maar dit is niet altijd het geval. Waarschijnlijk ligt dit aan een variabele troughput (dat vulnerability scans de ene keer sneller gebeuren dan de andere keer).

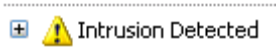
Je kan Nessus instellen zodat hij geen TCP port scanner gebruikt, dan geeft ISA geen alerts. Zoals verwacht geeft Nessus dan wel minder informatie over het te scannen

systeem. Maar in dit concreet geval valt de verminderde hoeveelheid informatie zeer goed mee.

Een doorwinterde hacker, die tevens weet dat hij te maken heeft met een ISA Server, zal zijn TCP port scanner initieel afzetten. In dat geval kan je zeggen dat de Alerts in ISA niet effectief zijn.

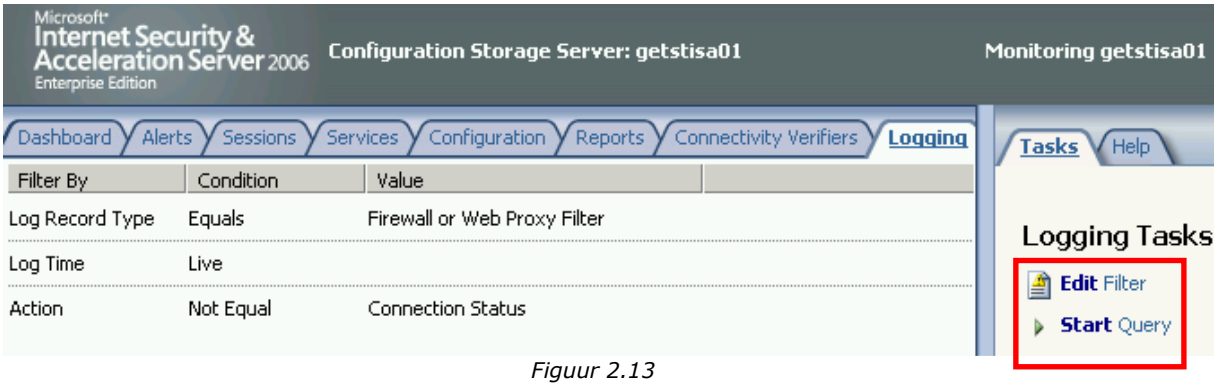
2.7.3 Na aanval met Metasploit

De aanval wordt niet tegengehouden maar wordt wel gedetecteerd. Er wordt namelijk melding gegeven van volgende alert.



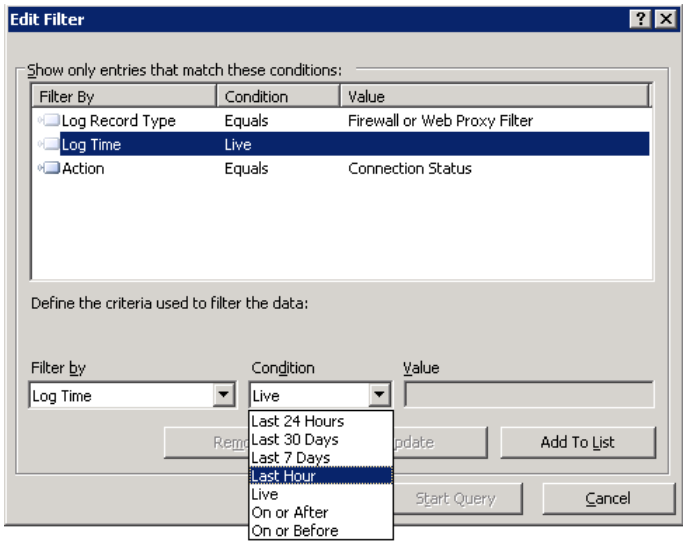
Figuur 2.12

ISA Server heeft ook een log-file waarin het intensief alle connecties gaat loggen. Standaard zie je deze log-file niet in de log viewer (die je vind in het tabblad Logging). Als je die toch wil zien moet je de query starten, door op Start Query te klikken.



Figuur 2.13

Je kan de log-files van het verleden ook bekijken als je Edit Filter kiest en daarna het tijdstip bepaalt waarvan je de log-gegevens wil zien.



Figuur 2.14

Volgende figuur geeft (een stuk uit) het resultaat van het loggen tijdens de vulnerability scan van Nessus.

IP	Destination IP	Destination Port	Protocol	Action
.209.95	10.130.223.104	2002	Unidentified IP Traffic	Denied Connection
.209.95	10.130.223.104	2002	Unidentified IP Traffic	Denied Connection
.209.95	10.130.223.104	9200	Unidentified IP Traffic	Denied Connection
.209.95	10.130.223.104	9200	Unidentified IP Traffic	Denied Connection
.209.95	10.130.223.104	79	Finger	Denied Connection
.209.95	10.130.223.104	79	Finger	Denied Connection
.209.95	10.130.223.104	80	HTTP	Denied Connection
.209.95	10.130.223.104	80	HTTP	Denied Connection
.209.95	10.130.223.104	280	Unidentified IP Traffic	Denied Connection
.209.95	10.130.223.104	280	Unidentified IP Traffic	Denied Connection
.209.95	10.130.223.104	631	Unidentified IP Traffic	Denied Connection

Figuur 2.15

Je ziet bij de kolom Action, dat er geen connecties toegelaten worden door ISA Server.

2.7.4 Besluit

Nmap en Metasploit worden default gedetecteerd en Nessus in de meeste gevallen ook. Dat dit default al gebeurd is zeer goed. De IPS functie in het algemeen kan nog wel een heel pak kan verbeteren. Voornamelijk op vlak van signatures herkenen van worms en andere malafide software hinkt ISA Server 2006 volledig achterop. Hopelijk gaat dit recht gezet worden bij de nieuwe versie van ISA Server 2006, Forefront TMG genaamd. Er bestaat wel extra software die je samen met ISA Server 2006 kan installeren om wel een adequate virusbescherming e.d. te hebben. Een voorbeeld van zo'n extern programma is GFI WebMonitor. Dit programma is een zeer goede partner voor ISA, zo bleek na onderzoek.

2.8 Voorbeeldpolicy toepassen

In stap 2 en stap 3 zijn respectievelijk de firewall en de inside host onderworpen aan een penetration test nadat de voorbeeldpolicy was toegepast. In 1.5 kan je de voorbeeldpolicy lezen en hier kan je lezen hoe die wordt ingesteld op de ISA Server.

2.8.1 Een firewall rule toevoegen

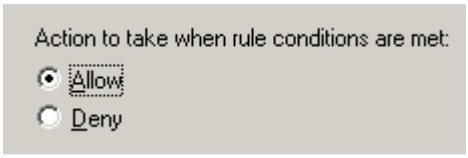
Bij wijze van voorbeeld volgt hierna de methode waarop 1 firewall rule is toegevoegd. De anderen rules toevoegen werkt op een vergelijkbare manier. De regel die hier gaat gedemonstreerd worden is de regel die HTTP- en HTTPS-verkeer moet doorlaten.

Standaard laat ISA Server niets door vanuit het interne netwerk dus moet je een Access Rule maken die HTTP & HTTPS doorlaat.

Ga daarvoor naar de Firewall Policy Node en in het Task Pane klik je op 'Create Access Rule'.

Figuur 2.16

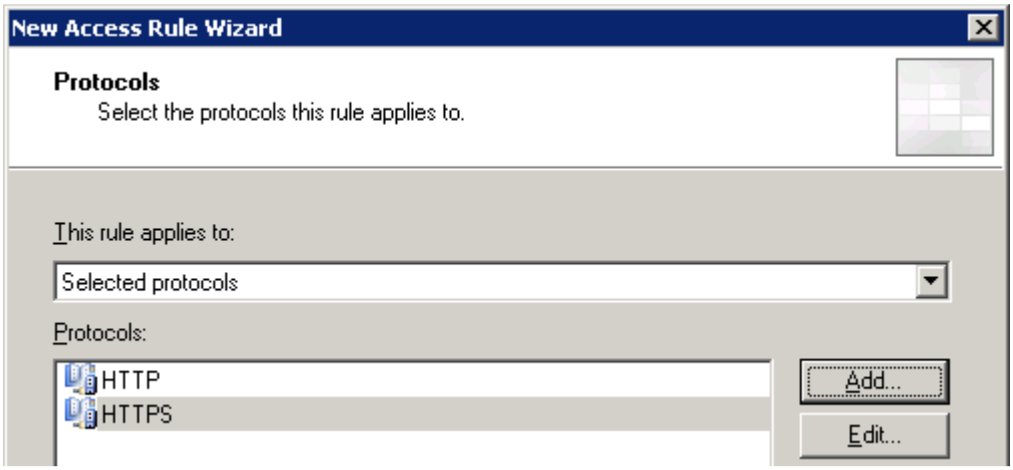
Daar vul je 'HTTP(S) van Intern naar Extern' in.



Figuur 2.17

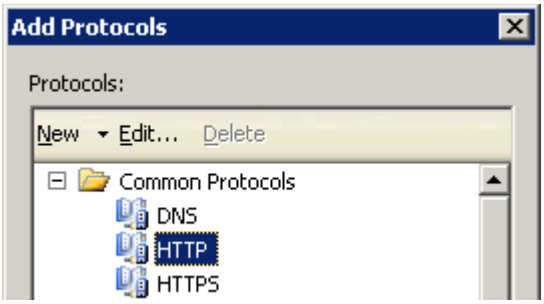
Daarna kies je voor 'Allow'

Op het volgende scherm klik je op 'Add...'



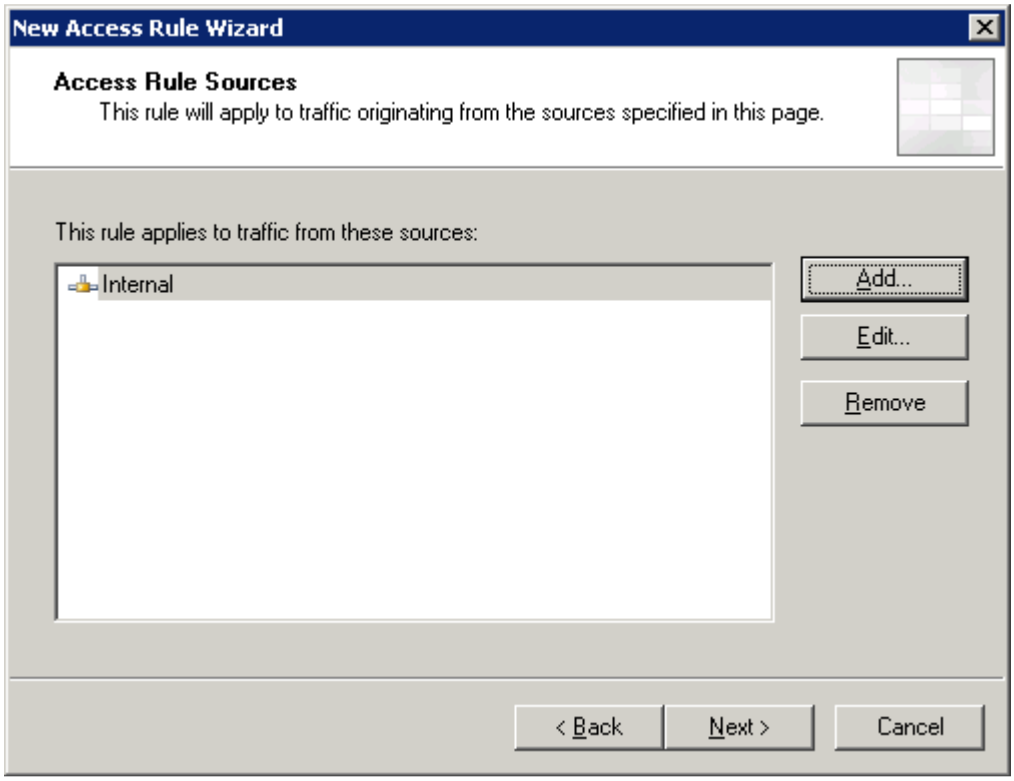
Figuur 2.18

En in het Add Protocols menu 'Add' je HTTP & HTTPS door er dubbel op te klikken.



Figuur 2.19

Klik daarna op Close en vervolgens op Next

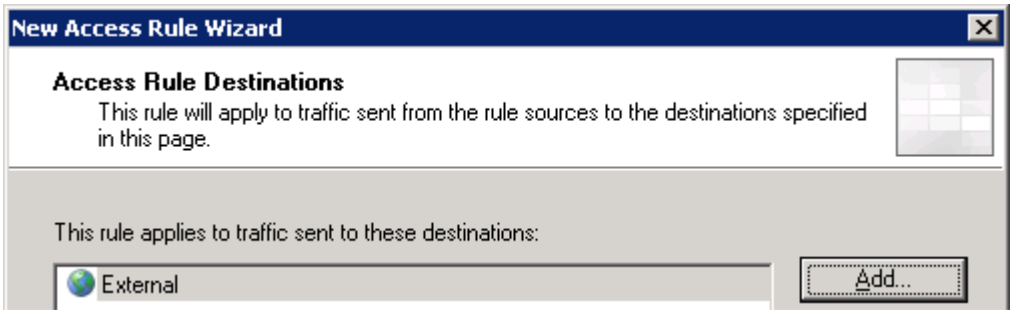


Figuur 2.20

Bepaal van waar je HTTP(S) verkeer wil toelaten in het volgende venster door op Add... te klikken en Internal toe te voegen.

Daarna op Next klikken.

Vervolgens geef je aan naar waar HTTP(S) moet toegelaten worden.



Figuur 2.21

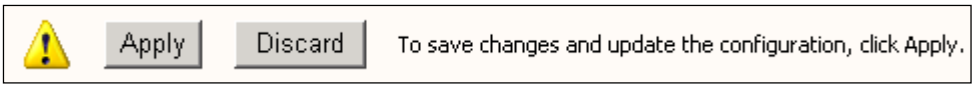
En klik je op Next.

In het volgende venster dat bepaalt voor welke gebruikers de rule geldt, klik op Next. Daardoor is de rule van toepassing op alle gebruikers.

Als je nu op Finish klikt zal je de 'HTTP(S) van Intern naar Extern' vinden onder Firewall Policy Rules.

Figuur 2.22

Om die rule nu toe te passen moet je nog wel op Apply klikken.

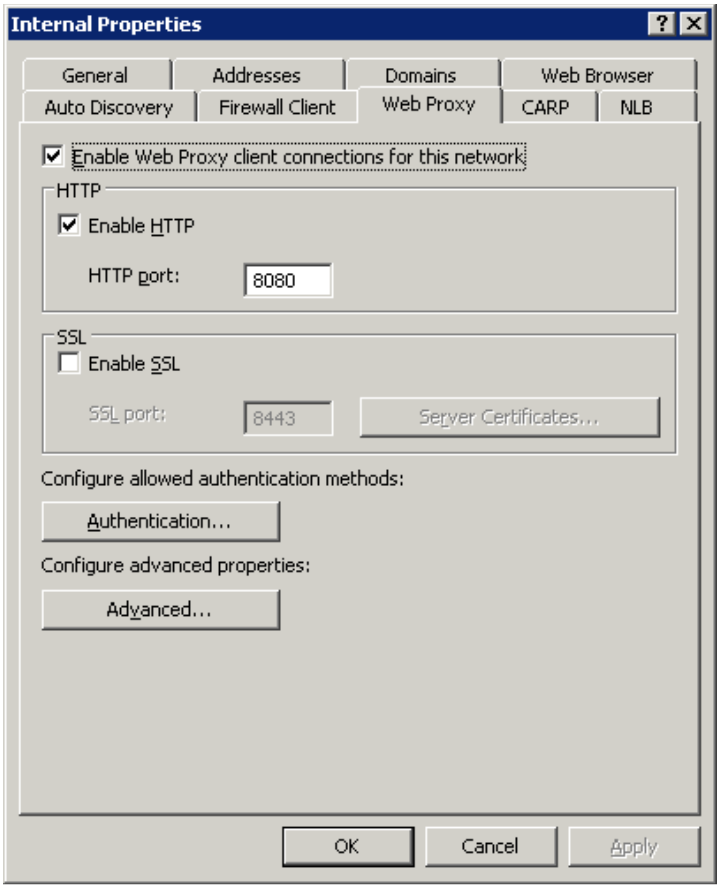


Figuur 2.23

Nu kan je nog kiezen of je ISA Server als een proxy wil gebruiken of als transparante proxy. De transparante proxy zorgt ervoor dat ISA als een gewone firewall werkt waarbij de systemen op het interne netwerk niets merken van ISA. ISA gebruiken als een echte proxy heeft als voordeel dat ISA Server minder belast wordt (ongeveer de helft minder) en dat je op die manier al het internetverkeer zeker via de ISA Server laat gaan ook al staat die niet op een centrale plaats in het netwerk. De mindere belasting van de ISA Server zal je wel pas voelen als het aantal gebruikers tegen de 1000 aangaat [34].

De ISA Server staat echter centraal tussen het internet en het externe netwerk (als internet edge firewall dus) dus wordt het hier geconfigureerd als transparant proxy.

Standaard staat ISA echter als proxy ingesteld. Dat zie je bij het vinkje bij de Properties van het Internal network, zie onderstaand figuur.



Figuur 2.24

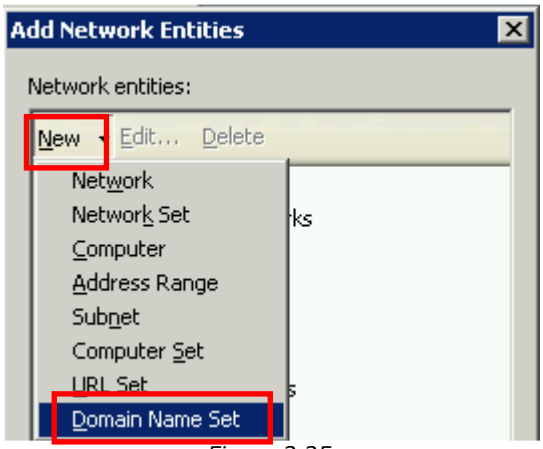
Doe het vinkje weg om ISA als transparant proxy in te stellen.

Om webverkeer ook daadwerkelijk door te laten is het nog niet gedaan. Nu moet je wel een Access Rule toevoegen in ISA Server die DNS toelaat. Dit volgt dezelfde werkwijze als HTTP(S) toelaten, alleen moet je nu voor DNS kiezen i.p.v. HTTP & HTTPS. Dan bekom je de firewall Access Rule zoals op volgende figuur.

2.8.2 URL filtering

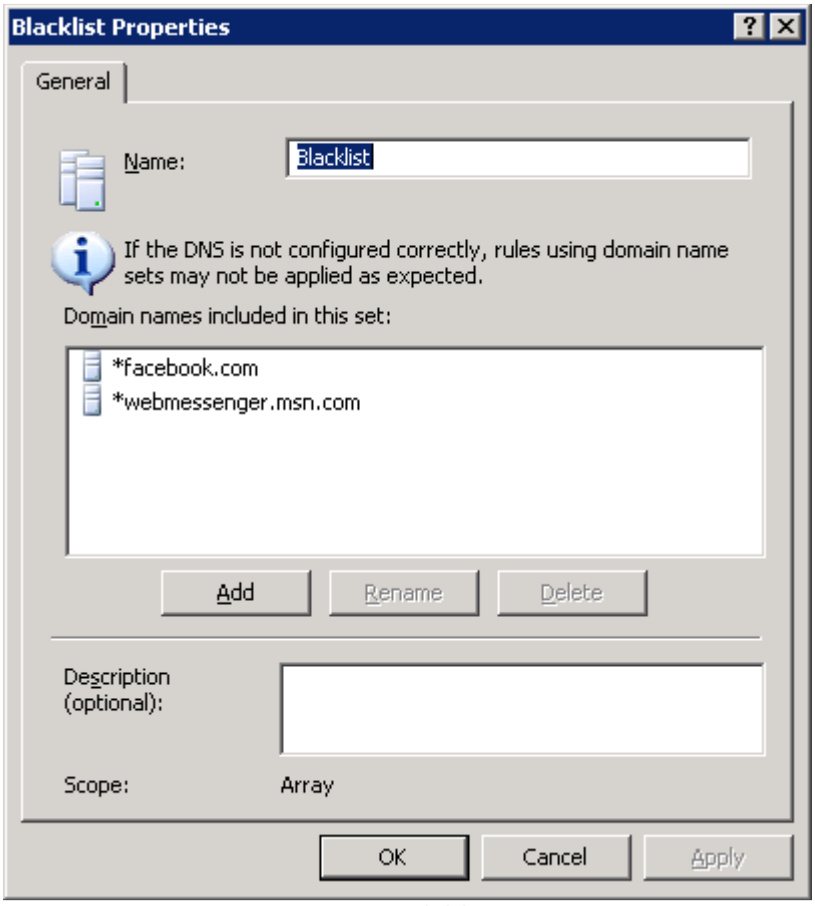
Facebook.com is tegenwoordig de aartsvijand van menig werkgever. Velen willen deze website dan ook blokkeren. Hiervoor maak je een Access Rule aan, net zoals je HTTP moet toelaten (zie eerder). Er zijn echter twee verschillen. Het eerste verschil is dat je Deny moet kiezen ipv. Allow want je wil toegang tot die website weigeren. Het tweede verschil zit hem in de Acces Rule Destination. Hier moet je een Domain Name Set opgeven ipv. HTTP(S). Die Domain Name Set moet je nog wel eerst maken, dat doe je op volgende wijze.

Klik op New > Domain Name Set



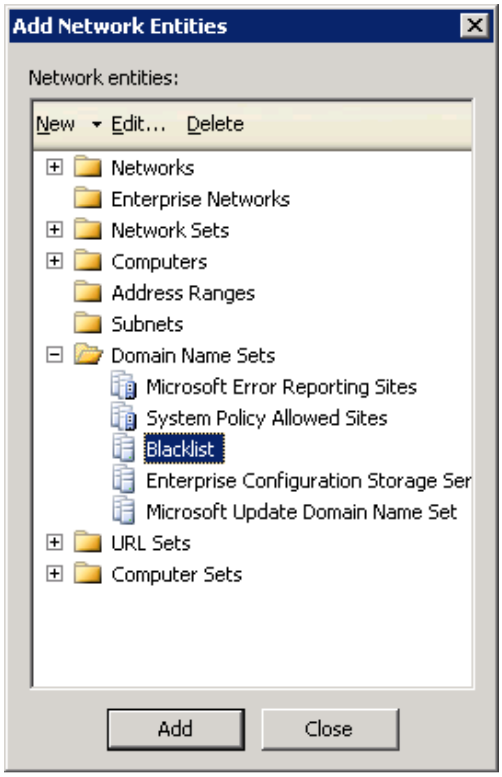
Figuur 2.25

Je geeft je Domain Name Set een naam en klikt op 'Add' en voegt zo de websites toe die je wil blokkeren. Zet er een sterretje voor als je wil dat alle deelwebsites van die domeinnaam ook geblokkeerd worden. Zet het gebruikelijke punt (zie afbeelding) niet voor de domeinnaam als je wil dat www.domeinnaam.be en domeinnaam.be (zonder www) beiden geblokkeerd worden.



Figuur 2.26

Nadat je deze Domain Name Set hebt aangemaakt moet je hem nog wel toevoegen aan de Acces Rule Destination, door het te selecteren en op 'Add' te klikken.



Figuur 2.27

Druk nog 2 maal Next en daarna Finish en je zal zien dat de websites niet meer toegankelijk zijn. De veranderingen niet vergeten toe te passen door op Apply te drukken natuurlijk.

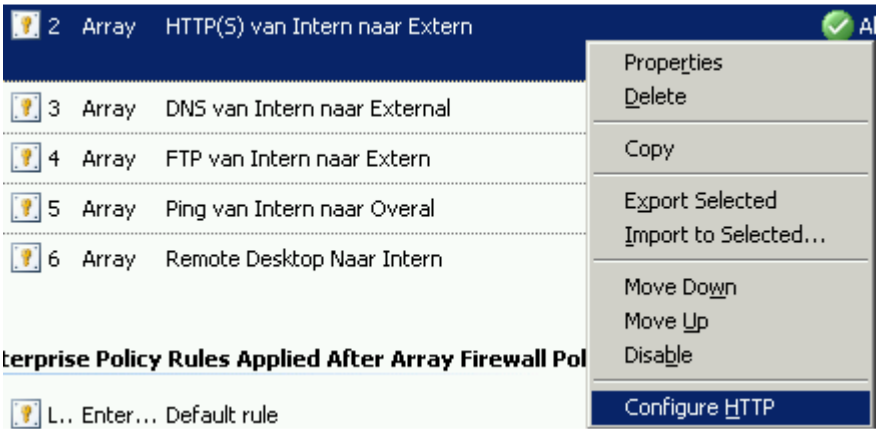
Waar je zeker nog op moet letten is dat de nieuwe regel boven de regel komt die HTTP toelaat. Bij het al dan niet toelaten van verkeer zoekt ISA Server (net zoals alle gebruikelijke firewalls) naar de eerste regel die van toepassing is op dat verkeer. Naar de rest van de regels wordt dan niet meer gekeken.

2.8.3 Deep inspection

ISA Server is ontworpen om te dienen als proxy server. Vandaar ook de naam Microsoft Proxy Server die de software initieel had. Een proxy server kan tegenwoordig doorgaans tot op de applicatielaag kijken. Daar zou dus de kracht van ISA Server in liggen. ISA Server is daarom ook goed voorzien om signatures van bepaalde programma's te blokkeren, zoals die van Windows (Live) Messenger.

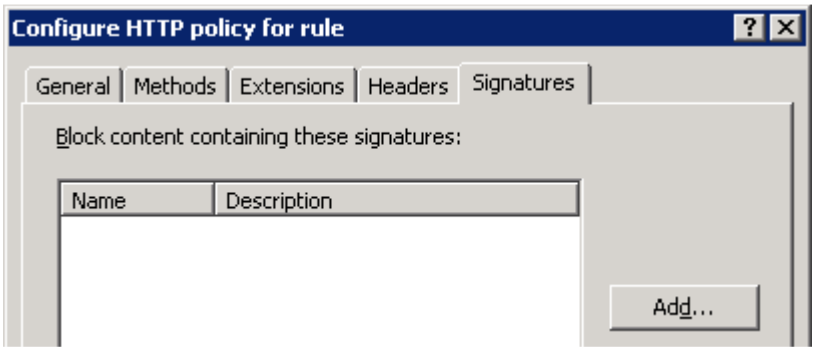
Microsoft heeft in het verleden drie verschillende versies van zijn messenger uitgebracht. Eerst was er MSN Messenger, maar die wordt niet meer ondersteund. Windows Messenger en Windows Live Messenger worden nog wel gebruikt en moeten dus kunnen geblokkeerd worden in onze ISA Server.

De eerste stap hiervoor is rechts klikken op de regel die HTTP verkeer doorlaat. In het menu dat verschijnt selecteer je 'Configure HTTP'.



Figuur 2.28

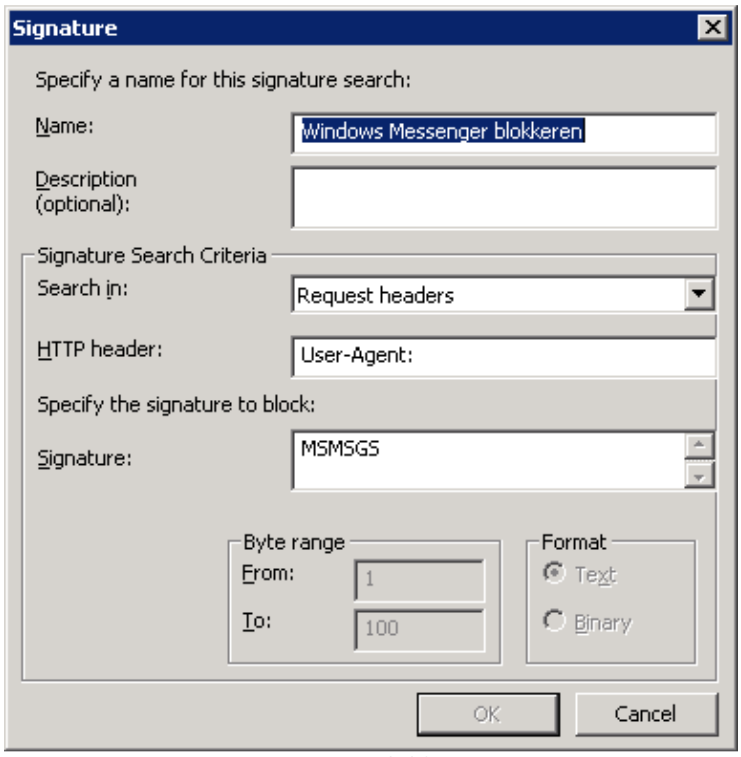
Je gaat naar het tabblad 'Signatures'.



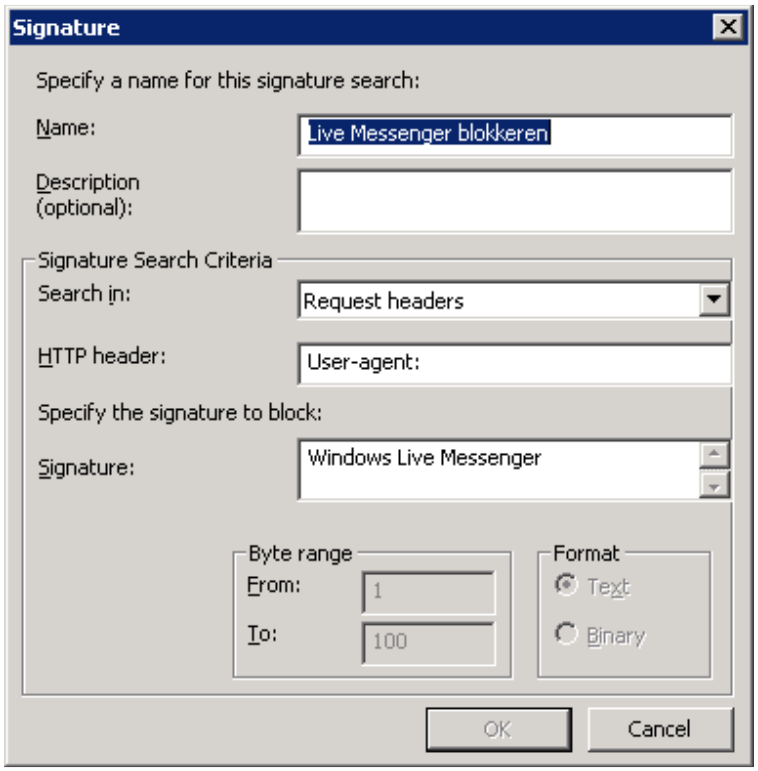
Figuur 2.29

En daar klik je op 'Add'.

Zoals eerder al vermeld kan ISA alle binnenstromende data controleren op patronen om zo pakketten met een bepaald patroon erin te blokkeren. In dit voorbeeld gaat er in de header van HTTP-paketten gezocht moeten worden in het veld 'User-agent' op de tekst 'MSMSGS' (voor Windows Messenger) en 'Windows Live Messenger', zo is gebleken na onderzoek. In de volgende figuren zie je wat je moet intikken.



Figuur 2.30



Figuur 2.31

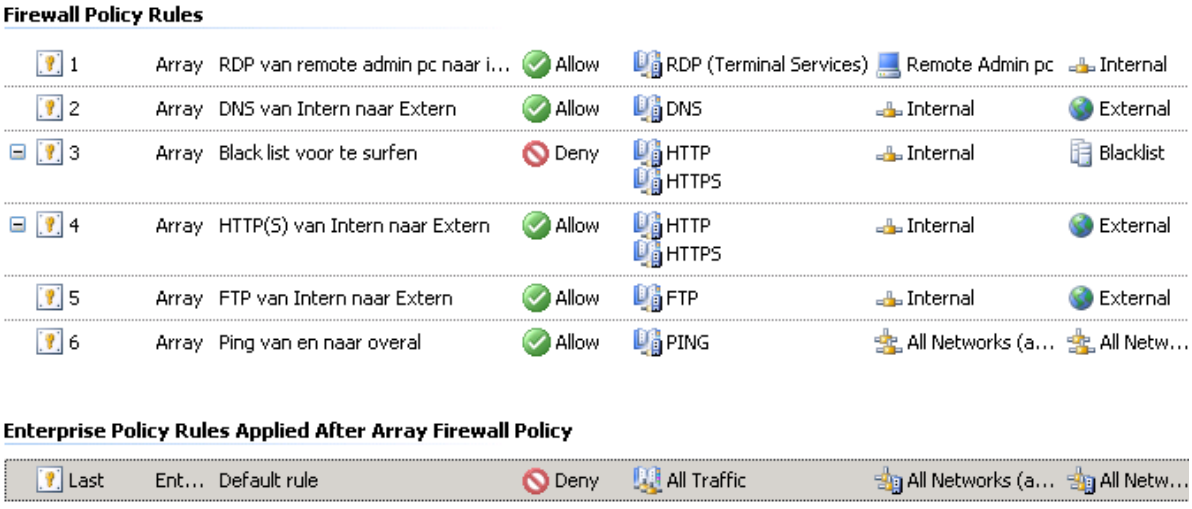
Bij de Common Protocols van ISA zal je ook het 'MSN Messenger' protocol vinden dat je zou kunnen gebruiken in een Deny-rule. Echter Windows Messenger noch Windows Live Messenger krijg je hiermee geblokkeerd, werd duidelijk na onderzoek.

Om P2P programma's te blokkeren zijn er ook zo'n signatures die je moet opgeven. Hier is een greep uit de signatures die je kan gebruiken.

Toepassing die je wil blokkeren	Search in	HTTP-header	Signature
KaZaA	Request headers	P2P-Agent:	Kazaa & Kazaaclient
	Request headers	User-Agent:	KazaaClient
	Request headers	X-Kazaa-Network:	KaZaA
Gnutella	Request headers	User-Agent:	Gnutella & Gnucleus
Edonkey	Request headers	User-Agent:	e2dk
Bearshare	Response header	Server:	Bearshare
BitTorrent	Request headers	User-Agent:	BitTorrent

2.8.4 De uiteindelijke firewall policy

Hoe de voorbeeldpolicy er uitziet nadat ze is toegepast op de ISA Server zie je in volgend figuur.



Figuur 2.32

3 JUNIPER SSG 20

De volgende firewall in rij die bestudeerd gaat worden is de Juniper SSG 20.

3.1 Prijs

Het officiële bedrag voor een SSG 20 met 256 MB is 814,81 EUR.

De verschillende licenties (per jaar):
- Deep inspection: 100 EUR
- Kapersky: 160,0 EUR
- Anti-spam: 222,2 EUR
- Web-filtering: 141,34 EUR
- Alle licenties samen: 513,33 EUR

De bedragen voor de licenties en ondersteuning zijn de bedragen bij aankoop via de leveranciers van CIPAL.

Het totale kostenplaatje met al de licenties samen zou € 1 328,14 zijn.

3.2 Eerste kennismaking

Figuur 3.1

De SSG productlijn van Juniper draait op het besturingssysteem ScreenOS. Op de Juniper SSG 20 in dit onderzoek draait de laatste nieuwe versie van ScreenOS dat op het moment van de test beschikbaar was voor het platform, namelijk ScreenOS 6.2.0r1.0 [35].

Juniper heeft in 2004 het bedrijf NetScreen overgenomen voor 4 miljard dollar [26]. Dat bedrijf had degelijke firewalls die snel aan populariteit wonnen en die draaiden op ScreenOS. Na de overname heeft Juniper de Netscreen firewalls verder ontwikkeld onder eigen naam.

Figuur 3.2

Je zou kunnen zeggen dat de basis van een Juniper SSG 20 een router is waarop firewall functionaliteit is gebouwd. In theorie kan je zo een firewall ook als router gebruiken die geen restricties legt op je verkeer. In praktijk koop je geen firewall als je eigenlijk een router nodig hebt natuurlijk.

De Juniper firewalls werken met zones, dat zijn volledig afgescheiden netwerksegmenten. De zones worden toegekend aan fysieke interfaces. Bij de SSG 20 worden standaard de untrust zone aan ethernet 0/0 interface toegekend, de DMZ zone aan ethernet 0/1 en de trust zone aan ethernet 0/2, 0/3 en 0/4. De trust zone is het inside netwerk en de untrust zone is het outside netwerk.

3.2.1 Interface

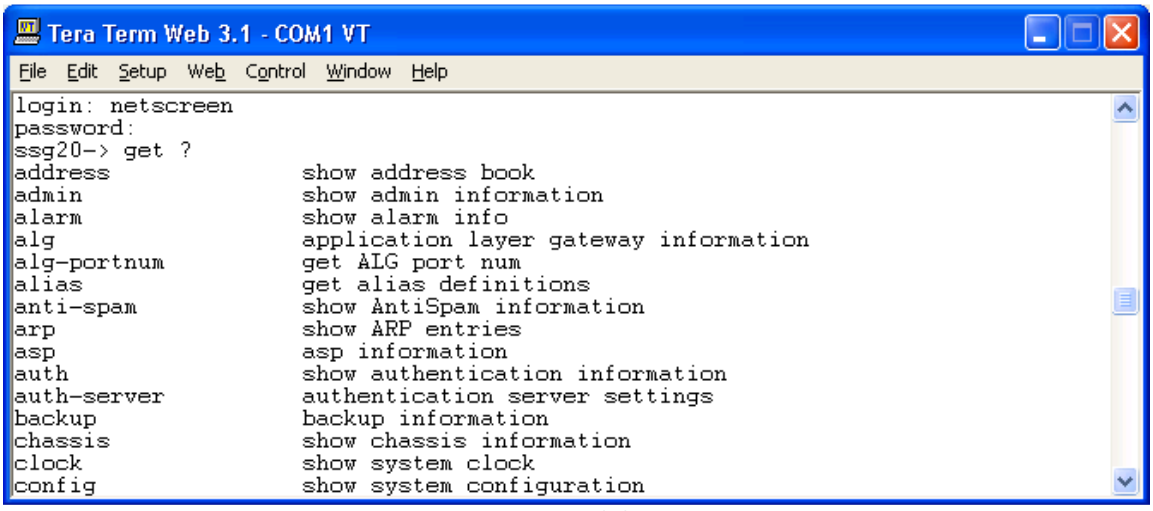
De Juniper firewall kan je bedienen met een Graphical User Interface (GUI) of via commando's. Zij worden behandeld in respectievelijk a en b.

a) Commando's

Je kan een pc met zijn seriële aansluiting direct aan de consolepoort van de firewall aansluiten. Dan heb je de CLI (Command Line Interface) van het besturingssysteem ScreenOS ter beschikking, tenminste als je eerst het standaardwachtwoord en login 'netscreen' ingeeft. Via de CLI heb je met commando's toegang tot alle functies.

Als je de commando's van het Cisco besturingssysteem IOS kent dan komen volgende vergelijkingen van pas:

- 'show' commando's van Cisco zijn doorgaans 'get' commando's.
  - Bijvoorbeeld 'show config' wordt nu 'get config' (zie laatste regel onderstaande figuur).
- Cisco commando's in global config mode (te bereiken via het Cisco commando 'config terminal') beginnen doorgaans met 'set'. De CLI van ScreenOS heeft geen modes zoals Cisco.



Figuur 3.3

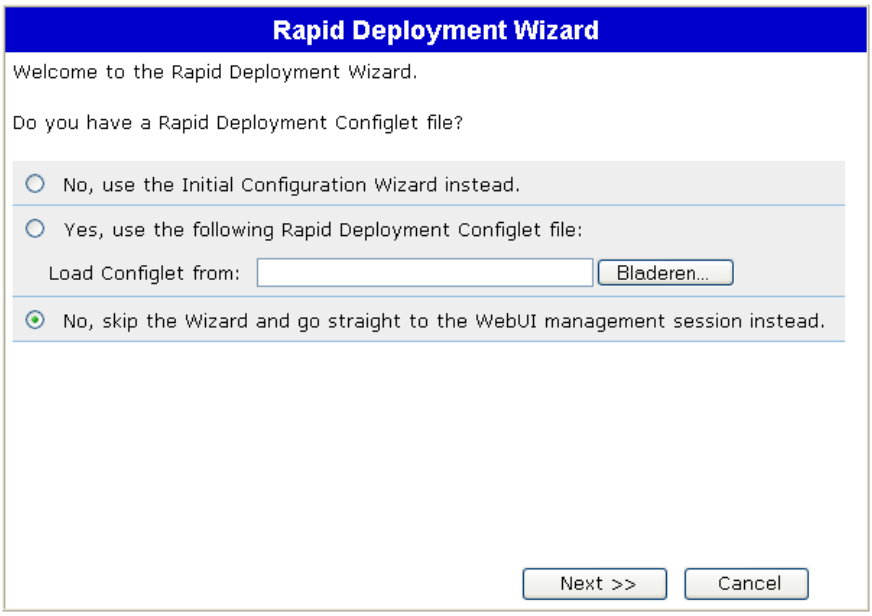
b) GUI

In de GUI vind je veruit de meeste functies van de CLI terug, spijtig genoeg wel niet alles.

Als je de firewall voor het eerst opzet en wil bereiken via de GUI moet je een pc aansluiten op de meest rechtse 3 interfaces (ethernet 0/2, 0/3 en 0/4) zodat de pc automatisch een IP-adres verkrijgt via de ingebouwde DHCP-server van de firewall.

Nu kan je via de pc surfen naar de GUI (Graphical User Interface) van de firewall via http://192.168.1.1

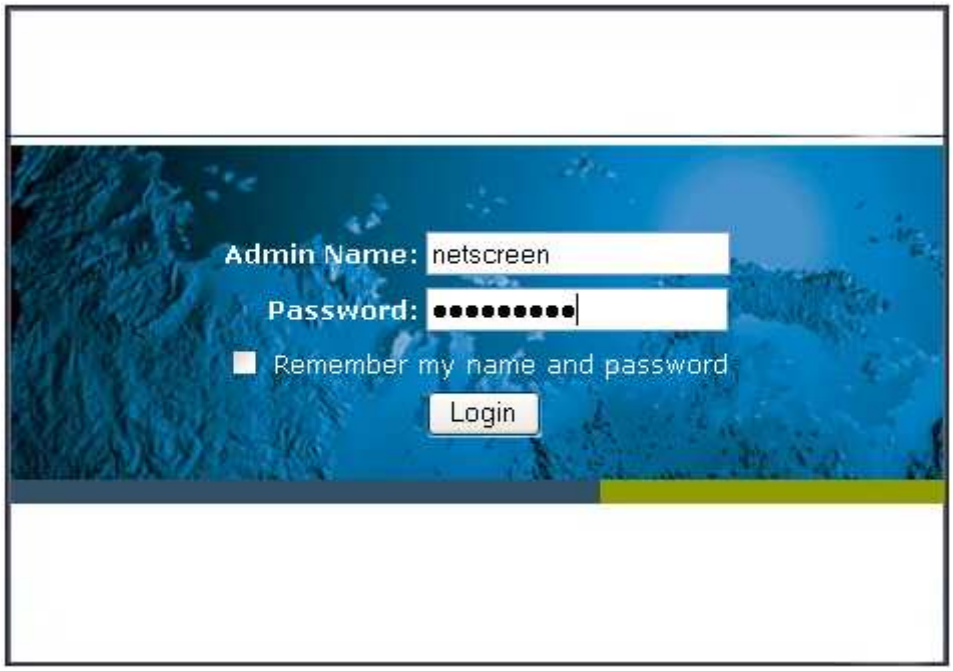
Dan krijg je het scherm in volgend figuur.



Figuur 3.4

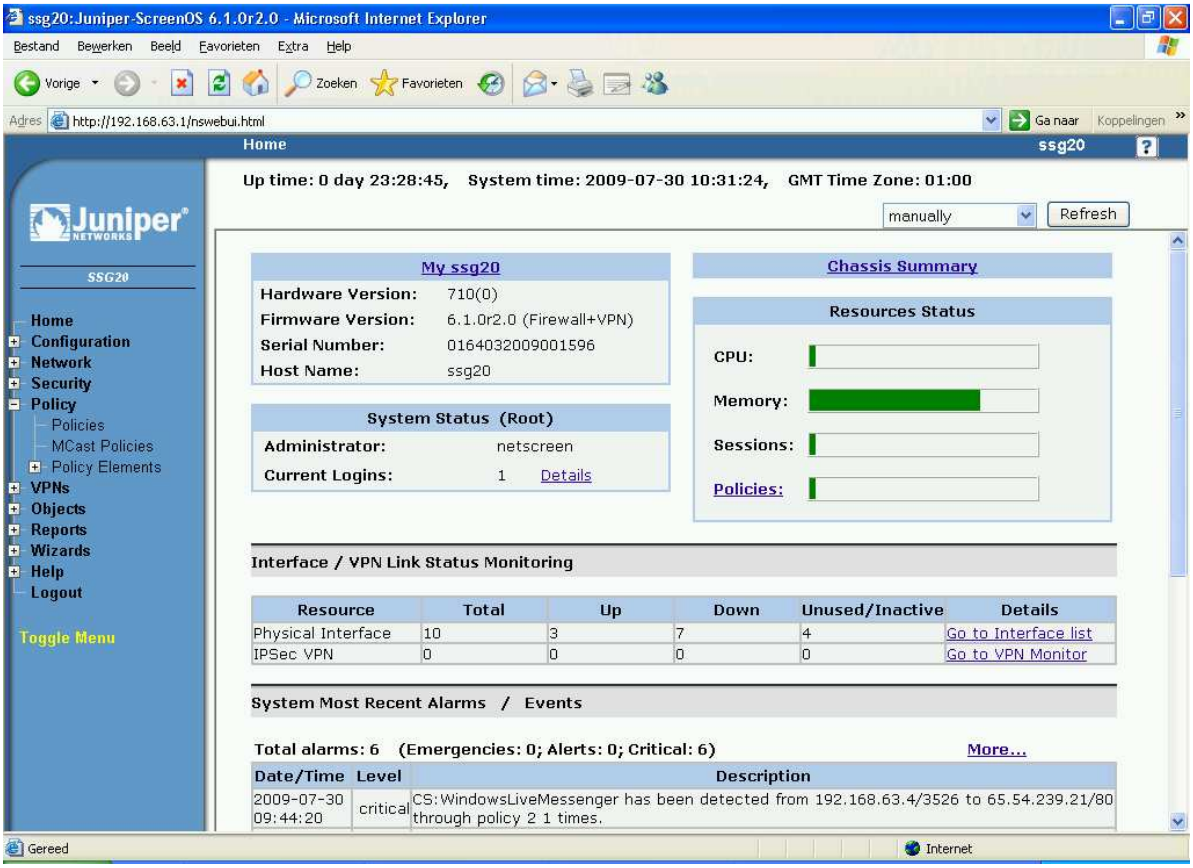
De bovenstaande vraag of je een wizard wil voor de initiële instellingen wijs je best af.

Vervolgens krijg je dan volgend aanmeldscherm waar je als standaard login en wachtwoord beide 'netscreen' opgeeft.



Figuur 3.5

Vervolgens krijg je een scherm vergelijkbaar met volgende figuur. Daarin zie je links het menu en rechts de 'homepagina'.



Figuur 3.6

3.2.2 Aan te raden aanpassingen

Het is aan te raden voor de veiligheid om het volgende in te stellen op een firewall met default instellingen [4]:

1) Verander het standaard login (netscreen) en wachtwoord (netscreen).
2) Bepaal wie toegang heeft tot de webinterface want standaard kan elke interne pc aan de webinterface.

Dit kan je veranderen via Configuration > Admin > Permitted IPs. Daar voeg je de IP-adressen toe van de systemen die de firewall moeten kunnen configureren. Als eerste Permitted IP kies je best het IP-adres van het systeem waar je op dat moment mee werkt, anders bestaat het gevaar dat je jezelf uitsluit.

3) Zet de Management Services uit naar de interne interface toe die je niet gebruikt. De Management Services zijn de manieren om de firewall te configureren, zoals bijvoorbeeld telnet, ssh.

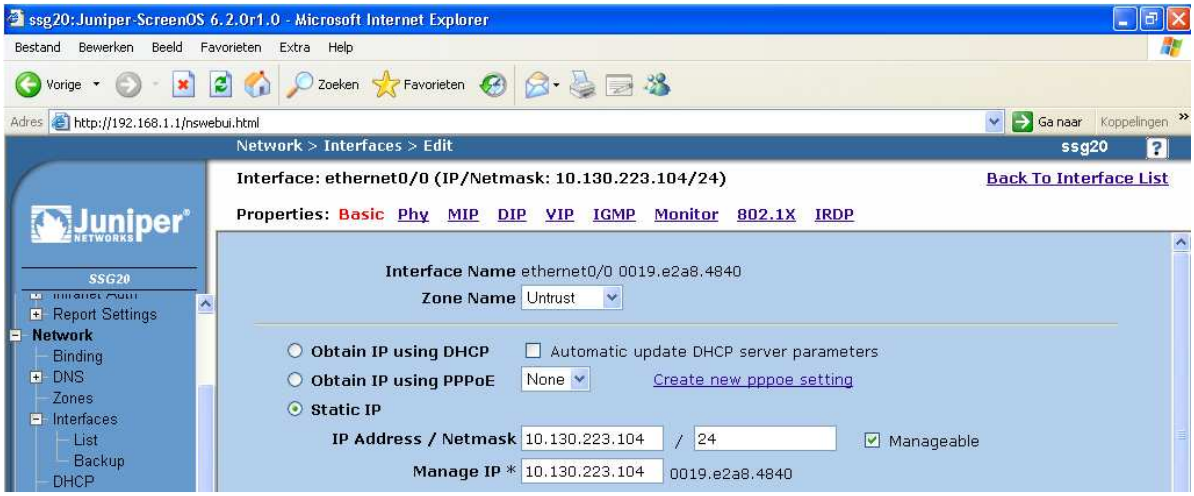
Pingen en alle andere services worden default niet toegelaten naar de externe interface toe, dus daar moet je niets voor veranderen.

3.2.3 Voorbereiding penetration test met default configuratie

Initieel is het de bedoeling om zo weinig mogelijk aan te passen van de default configuratie van de Juniper firewall. Maar om de firewall te bereiken om het te kunnen

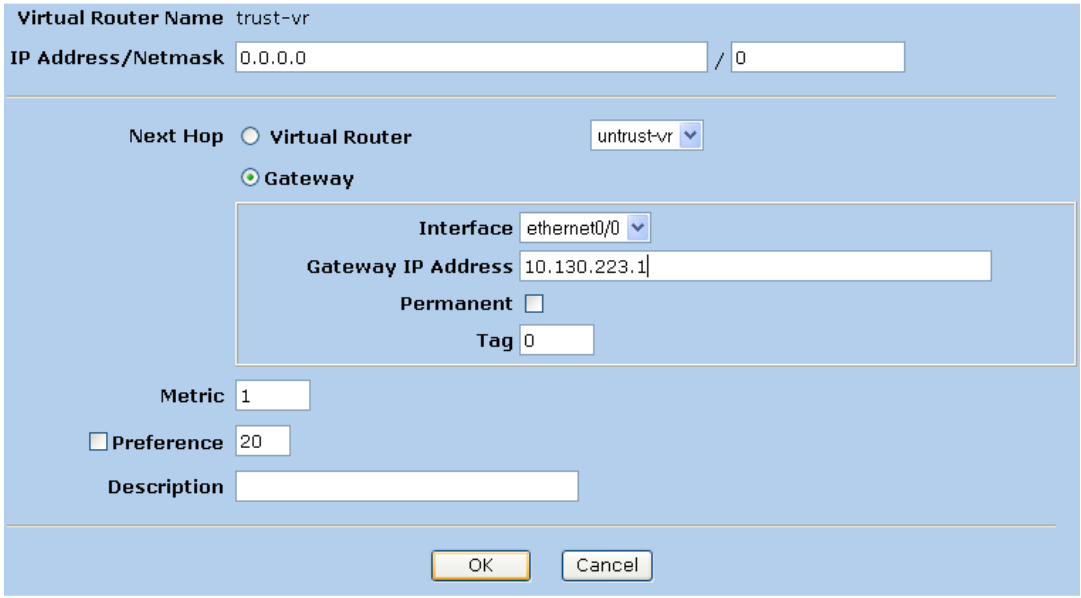
scannen moet je wel een default route ingeven en een IP-adres instellen voor de outside interface.

Dat laatste doe je bij Network > Interfaces waar je op Edit klikt op de regel van de untrust interface.



Figuur 3.7

Daarna moet je een default route instellen zodat er een route is voor het interne verkeer dat naar het internet moet. Dat doe je bij Network > Routing > Routing Entries waar je op New klikt zodat er een scherm opent met de routes voor de 'trust-vr'. In dat scherm vul je de gegevens van volgende figuur in.

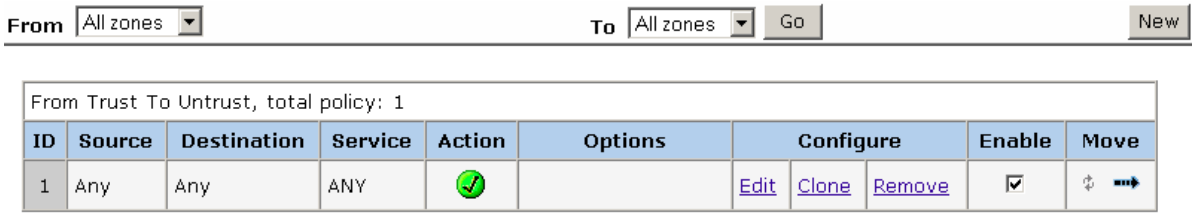


Figuur 3.8

Als laatste aanpassing zijn de adressen die de ingebouwde DHCP-server uitdeelt veranderd. Dit is omdat het interne netwerk adressen in het 192.168.63.0/24 subnet moeten hebben voor onze test en niet de 192.168.1.0/24 adressen die normaal worden uitgedeeld.

3.2.4 Wat zet de firewall default open?

Om de firewall policy te bekijken selecteer je Policy > Policies.



Figuur 3.9

Daarbij zie je dat al het verkeer van de Trust-zone naar de Unstrust-zone toegelaten wordt. Al de rest van het verkeer tussen de verschillende zones wordt tegengehouden. Het verkeer binnen een zone wordt default doorgelaten [36].

Door de default regel die alles openzet van trust naar untrust kan een worm die zich op het interne netwerk bevindt, zich ongehinderd verspreiden naar het internet.

Zoals eerder al aangehaald worden ping en alle andere services default niet toegelaten naar de externe interface toe.

3.3 Stap 1: Penetration test met default configuratie

3.3.1 Stap 1a: Scan met Nmap

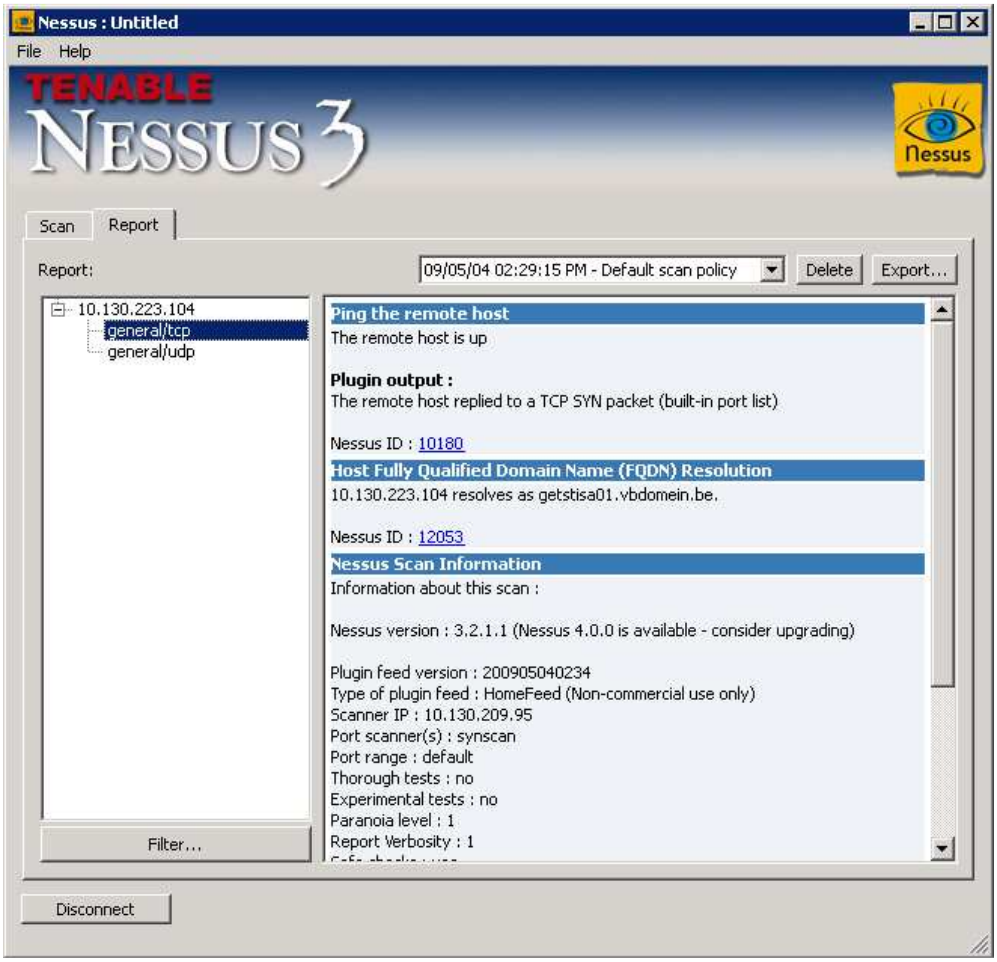
Intense scan, no ping:

```
Starting Nmap 4.85BETA7 ( http://nmap.org ) at 2009-05-04 14:19 Romance
(standaardtijd)
Initiating Parallel DNS resolution of 1 host. at 14:19
Completed Parallel DNS resolution of 1 host. at 14:19, 6.50s elapsed

Initiating SYN Stealth Scan at 14:19
Scanning getstisa01.vbdomein.be (10.130.223.104) [1000 ports]
SYN Stealth Scan Timing: About 29.00% done; ETC: 14:21 (0:01:16 remaining)
SYN Stealth Scan Timing: About 58.00% done; ETC: 14:21 (0:00:44 remaining)
Completed SYN Stealth Scan at 14:21, 104.22s elapsed (1000 total ports)

Initiating Service scan at 14:21
Initiating OS detection (try #1) against getstisa01.vbdomein.be
(10.130.223.104)
Retrying OS detection (try #2) against getstisa01.vbdomein.be
(10.130.223.104)
NSE: Initiating script scanning.

Host getstisa01.vbdomein.be (10.130.223.104) is up.

All 1000 scanned ports on getstisa01.vbdomein.be (10.130.223.104) are
filtered

Too many fingerprints match this host to give specific OS details
Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 117.36 seconds
           Raw packets sent: 2048 (94.672KB) | Rcvd: 129 (8786B)
```

De interessante (en enige) informatie die je krijgt is hetgeen dat, zoals gewoonlijk, in het vet staat. In dit geval is dat maar één regel en dan nog één die zegt dat er geen open poorten gevonden zijn.

Zoals je ziet wordt het IP-adres 10.130.223.104 nog altijd vertaald naar getstisa01.vbdomein.be. Dit komt omdat dit adres zo geregistreerd staat bij de interne DNS server van CIPAL.

3.3.2 Stap 1b: Scan met Nessus



Figuur 3.10

Deze scan gaf niet altijd dezelfde output. Er was even het probleem dat Nessus geen enkele output gaf. Dit valt te verklaren door het feit dat Nessus initieel altijd kijkt of het systeem aan staat. Als Nessus geen teken van leven krijgt van het systeem, stopt het met scannen. Na het opnieuw resetten van de firewall naar zijn default configuratie was dit euvel echter opgelost.

3.3.3 Stap 1c: Aanval met Metasploit

Module Output:

```
ms08_067_netapi [-] Exploit failed: The connection timed out
(10.130.223.104:445).
```

Zoals Nessus al aangaf is poort 445 niet toegankelijk naar de server toe. Conficker zou dus geen kans maken.

3.3.4 Besluit

De firewall blijkt helemaal dichtgemetseld, geen beveiligingsgaatje te bespeuren. Achteraf gezien was dat resultaat een beetje te verwachten omdat je in de firewall policy ziet dat er niets wordt toegelaten. Bovendien mag je verwachten van de firewall en zijn besturingssysteem ScreenOS dat zij geen beveiligingslekken hebben. Zij zijn dan ook speciaal ontworpen voor de beveiliging van je netwerk, wat bijvoorbeeld niet zo is bij ISA Server en bij Check Point. Zij draaien op een besturingssysteem dat niet gemaakt is voor netwerkbeveiliging.

Wat je wel zou moeten kunnen zien in de output van Nmap en Nessus, zijn de Management Services. Dit zijn de protocollen die je kan gebruiken om van buitenaf (untrust) de firewall te configureren. Uit de output kan je dus leren dat er standaard geen Management Services open staan voor de untrust interface.

3.4 Stap 2: Penetration test met voorbeeldpolicy

De Juniper firewall gaat weer uitgetest worden, maar nu niet meer met de default configuratie maar met een voorbeeldpolicy geïmplementeerd.

3.4.1 Stap 2a: Scan met Nmap

Intense scan, no ping:

```
Starting Nmap 4.85BETA7 ( http://nmap.org ) at 2009-07-30 11:28 Romance
(standaardtijd)
Initiating Parallel DNS resolution of 1 host. at 11:28
Completed Parallel DNS resolution of 1 host. at 11:28, 6.50s elapsed

Initiating SYN Stealth Scan at 11:28
Scanning getstisa01.vbdomein.be (10.130.223.104) [1000 ports]
SYN Stealth Scan Timing: About 29.00% done; ETC: 11:30 (0:01:16 remaining)
SYN Stealth Scan Timing: About 58.00% done; ETC: 11:30 (0:00:44 remaining)
Completed SYN Stealth Scan at 11:30, 104.21s elapsed (1000 total ports)

Initiating Service scan at 11:30
Initiating OS detection (try #1) against getstisa01.vbdomein.be
(10.130.223.104)
Retrying OS detection (try #2) against getstisa01.vbdomein.be
(10.130.223.104)
NSE: Initiating script scanning.

Host getstisa01.vbdomein.be (10.130.223.104) is up.

All 1000 scanned ports on getstisa01.vbdomein.be (10.130.223.104) are
filtered

Too many fingerprints match this host to give specific OS details
Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 117.52 seconds
           Raw packets sent: 2048 (94.672KB) | Rcvd: 0 (0B)
```

Nmap geeft aan dat er geen open poorten zijn.

3.4.2 Stap 2b: Scan met Nessus

Nessus geeft de open Management Services als output. Als je er geen open hebt gezet, geeft het dus geen enkele output zoals bij deze test het geval was.

3.4.3 Stap 2c: Aanval met Metasploit

Het lukt Metasploit niet om zijn aanval uit te voeren.

3.4.4 Besluit

Het is eerder al kort aangehaald, maar het scannen van de Juniper firewall zal normaal gezien geen verrassingen opleveren. Of de voorbeeldpolicy nu geconfigureerd is of niet. Je mag namelijk van een OS dat speciaal ontwikkeld is om een firewall te draaien, verwachten dat het goed afgedicht is. Zo dus ook bij deze Juniper firewall. Er kunnen poorten open staan, zoals bijvoorbeeld ssh, maar dat dan enkel als jij die bewuste poort hebt opengezet naar de Juniper zelf. De poorten die je kan open zetten stellen dan de protocollen voor waarmee je de firewall kan configureren, vandaar de naam Management Services.

3.5 Stap 3: Penetration test van inside host

3.5.1 Stap 3a: Scan met Nmap

Intense scan, no ping:

```
Starting Nmap 4.85BETA7 ( http://nmap.org ) at 2009-07-30 18:27 Romance
(standaardtijd)
Initiating Parallel DNS resolution of 1 host. at 18:27
Completed Parallel DNS resolution of 1 host. at 18:27, 0.00s elapsed

Initiating SYN Stealth Scan at 18:27
Scanning 192.168.63.4 [1000 ports]
SYN Stealth Scan Timing: About 29.50% done; ETC: 18:29 (0:01:14 remaining)
SYN Stealth Scan Timing: About 59.00% done; ETC: 18:29 (0:00:42 remaining)
Completed SYN Stealth Scan at 18:29, 104.22s elapsed (1000 total ports)

Initiating Service scan at 18:29
Initiating OS detection (try #1) against 192.168.63.4
Retrying OS detection (try #2) against 192.168.63.4
NSE: Initiating script scanning.

Host 192.168.63.4 is up (0.00s latency).

All 1000 scanned ports on 192.168.63.4 are filtered

Too many fingerprints match this host to give specific OS details
Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 107.81 seconds
           Raw packets sent: 2042 (93.604KB) | Rcvd: 2 (356B)
```

Nmap stelt dat de firewall geen open poorten heeft naar de inside host.

3.5.2 Stap 3b: Scan met Nessus

Voor Nessus leek het alsof het systeem niet aan stond dus geeft Nessus geen output.

3.5.3 Stap 3c: Aanval met Metasploit

```
18:34:30 - ms08_067_netapi [*] Launching exploit
windows/smb/ms08_067_netapi...

18:34:32 - ms08_067_netapi [*] Started reverse handler

18:34:42 - ms08_067_netapi [-] Exploit failed: The connection timed
out (192.168.63.4:445).
```

De aanval met Metasploit is niet gelukt.

3.5.4 Besluit

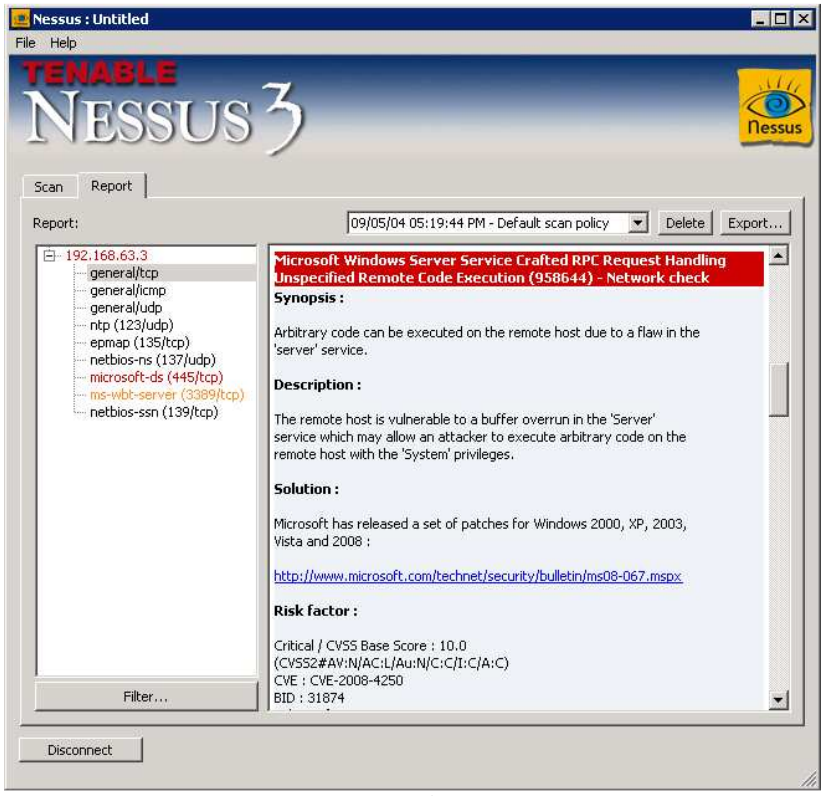
Ook naar de inside host toe laat de Juniper firewall niets toe. Het rapport van deze firewall is tot nu feilloos.

3.6 Stap 4: Penetration test vanuit inside LAN

Wat laat de Juniper firewall allemaal toe vanuit het intern netwerk naar het intern netwerk? Dit is vooral belangrijk bij worms, virussen en interne hackers die een bedreiging vormen komende van het interne netwerk. Bij deze test is de default instelling, die het intra-zone trafiek doorlaat, blijven staan, in tegenstelling tot wat de voorbeeldpolicy eigenlijk voorschrijft.

3.6.1 Stap 4b: Scan met Nessus

Nmap wordt gelaten voor wat het is, het zou in dit geval toch geen extra informatie opleveren.

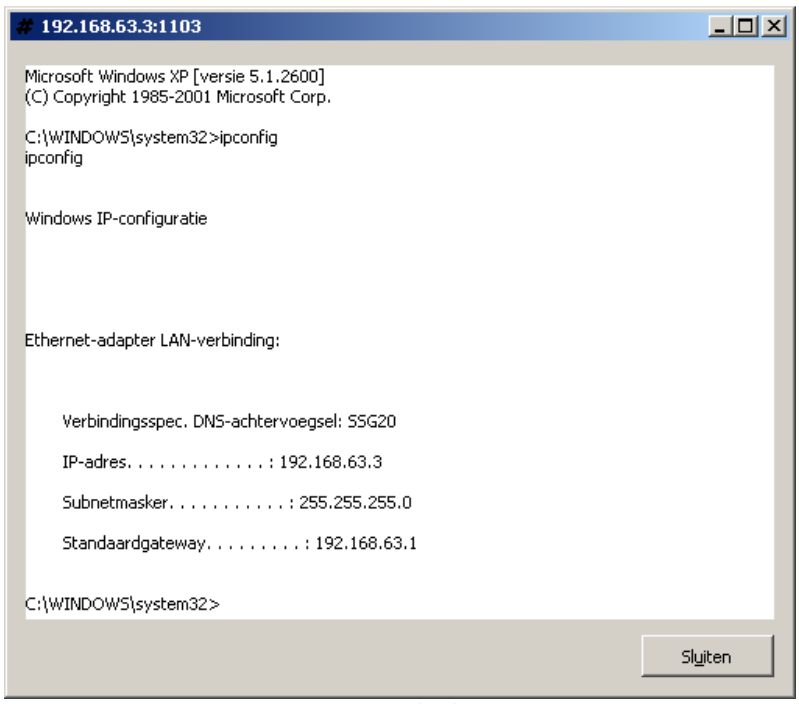


Figuur 3.11

Zoals je ziet wordt al het verkeer gewoon doorgelaten!

3.6.2 Stap 4c: Aanval met Metasploit

Aangezien alles doorgelaten wordt kan de Conficker-code losgelaten worden op het interne netwerk. Dit zie je hieronder aan de shell die geopend is met Metasploit. Met die shell kan je weer alles doen wat je wil, bijvoorbeeld het 'format c:' commando.



Figuur 3.12

3.6.3 Besluit

Deze test is waarschijnlijk de belangrijkste voor de Juniper firewall. Je ziet dat alles tussen twee dezelfde zones default doorgelaten wordt. Het verkeer van het intern netwerk naar het intern netwerk wordt dus gewoon doorgelaten alsof er geen firewall zou staan!

Dit vereist toch een hoge waakzaamheid van de netwerkadministrator. Een hacker kan bijvoorbeeld een pc op het interne netwerk besmetten door een virus of trojan te sturen via E-mail. Een werknemer die niet zo handig is met pc's kan die malafide software dan loslaten op zijn pc zonder dat hij het weet. Op die manier heeft de hacker toegang tot werkelijk alles op het interne netwerk want er worden hem default geen beperkingen opgelegd door de firewall! Daar komt nog eens bij dat default al het verkeer van untrust naar trust wordt doorgelaten (zie 3.2.4 Wat zet de firewall default open?) zodat het geïnfecteerde systeem VISA-gegevens e.d. naar de virusmaker kan sturen.

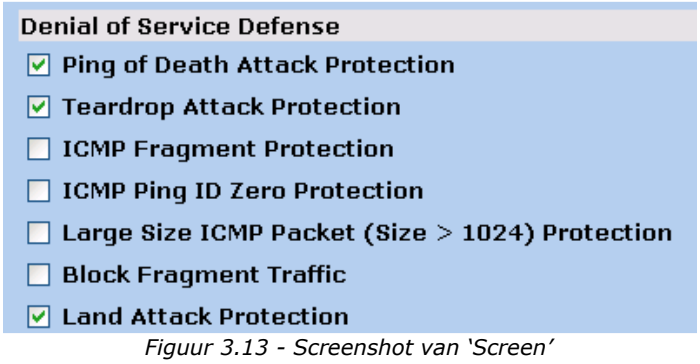
Deze manier van omgaan met intern verkeer is geen groot mankement maar vooral een keuze van implementatie door de makers. Een keuze die ISA Server en Check Point bijvoorbeeld anders hebben beslist. Wat wel zeker is, is dat de netwerkbeheerder ervan bewust moet zijn dat de Juniper firewall zo werkt.

3.7 Stap 5: IPS

Er zijn twee plaatsen in de GUI waar je IPS voor het loggen en tegenhouden van aanvallen kan instellen. Als je vooral op de netwerklaag en de transportlaag van het OSI-model wil controleren moet je zijn bij Security > Screening > Screen. Die opties zullen behandeld worden in het puntje 'Screening'. Juniper heeft voor IPS & IDS ook nog deep inspection voorzien dat je bij Security > Deep Inspection vindt. Die opties zullen behandeld worden in het puntje 'Deep inspection'.

3.7.1 Screening

Na onderzoek bleek dat standaard geen enkele vorm van aanval tegengehouden noch gelogd wordt. Toegegeven, enkele stokoude aanvallen (zie vinkjes in onderstaande figuur) worden wel herkend zoals de 'Ping of Death', dat vooral een probleem was bij Windows 95 systemen. En dit dan enkel voor aanvallen gericht naar de untrust-interface. Voor de trust-interfaces wordt alles, ook deze oude aanvallen, gewoon doorgelaten.



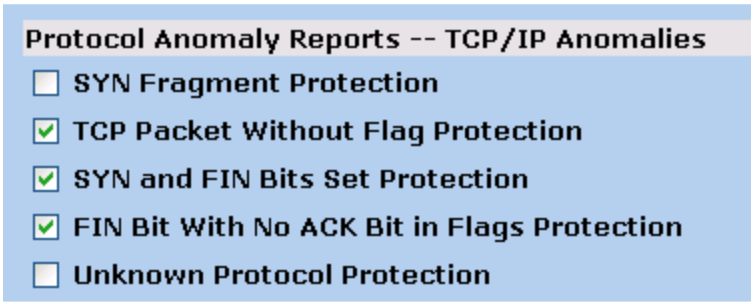
Figuur 3.13 - Screenshot van 'Screen'

3.7.1.1 Stap 5a: Na scan met Nmap

De Juniper firewall heeft helemaal niets van deze scan in zijn logs staan, zo blijkt. Dit is wel zeer opmerkelijk.

Je kan er wel zelf voor zorgen dat Nmap gedetecteerd wordt.

Daarvoor moeten volgende opties aangevinkt worden: SYN Flood Protection, Port Scan Protection en de opties in onderstaand figuur.



Figuur 3.14

Bij elke optie die je aanvinkt gaat de firewall op bepaalde zaken letten. Bij wijze van voorbeeld, het vinkje 'SYN and FIN Bits Set Protection' [37]:

Dit vinkje controleert of de SYN en de FIN bit tegelijk op 1 gezet zijn. De SYN en FIN bits zijn namelijk bij normale pakketten nooit tegelijk op 1 gezet. Hackers zullen ze soms wel beide op 1 zetten omdat ze informatie willen halen uit de manier van reageren op dat pakket. Aan de hand daarvan zouden ze bijvoorbeeld kunnen zien welk besturingsysteem gereageerd heeft. De hacker kan dan bepaalde vulnerabilities gebruiken die eigen zijn aan dat bewuste besturingssysteem.

Wanneer je deze optie aanvinkt zullen alle pakketten met beide bits op 1 gezet, worden gedropt.

Hoe dan ook geeft Nmap dezelfde informatie als output of je vorige zaken nu aanvinkt of niet.

3.7.1.2 Stap 5b: Na scan met Nessus

Hierbij valt op te merken dat de firewall weer standaard niets over een scan of aanval heeft gelogd!

Na onderzoek is duidelijk geworden dat om Nessus te loggen de opties 'Source IP Based Session Limit' en 'Port Scan Protection' aangevinkt moeten worden.

Bijgevolg komen er 'Src IP session limit!' en 'Port scan!" regels in het log te staan. Ook al je de TCP scanner van Nessus afzet worden die regels gelogd.

Net zoals bij Nmap geeft Nessus wel dezelfde informatie, eender hoe je de logging instelt.

3.7.1.3 Stap 5c: Na aanval met Metasploit

Er wordt niets van Metasploit gelogd noch tegengehouden. Het hangt dan van de policy af (of die poort 445 open zet) of er kan ingebroken worden op het systeem.

3.7.2 Deep inspection

Zoals al aangehaald is er ook een tweede manier om aan IPS te doen, namelijk met deep inspection. Als je die gebruikt wordt er wel een stuk meer geheugen verbruikt. Of je nu op veel signatures tegelijk controleert of maar eentje, dat maakt geen verschil in geheugenverbruik.
De signatures worden door de firewall 'attacks' genoemd. Om te controleren op die attacks moeten ze gegroepeerd worden in een 'attack group'. In deze test wordt er gecontroleerd op alle relevante attack groups.

3.7.2.1 Stap 5a: Na scan met Nmap

De regular scan van Nmap kan op geen enkele manier worden gelogd met deep inspection, zo bleek proefondervindelijk.

Met de intense scan, no ping krijg je 2 meldingen in de logs:

Date / Time	Level	Description
2009-07-30 17:14:00	notif	SMB:NETBIOS:UNK-SHDR-FLAGS has been detected from 10.130.209.95/3667 to 192.168.63.4/139 through policy 5 1 times.
2009-07-30 17:14:00	error	MS-RPC:ERR:FRAG-LEN-TOO-SMALL has been detected from 10.130.209.95/3666 to 192.168.63.4/135 through policy 5 1 times.

Nmap lijkt echter geen hinder te ondervinden van de deep inspection.

3.7.2.2 Stap 5b: Na scan met Nessus

Er wordt geen melding gegeven en Nessus geeft zijn gewoonlijke resultaten.

3.7.2.3 Stap 5c: Na aanval met Metasploit

Je kan volgende melding vinden in de logs, na een Conficker-aanval.

Date / Time	Level	Description
2009-07-30 17:39:04	info	SMB:AUDIT:UNK-DIALECT has been detected from 10.130.209.95/3718 to 192.168.63.4/445 through policy 5 1 times.

Als je lang zoekt in de omslachtige Attack-tabellen vind je dat de regel in het log gegenereerd wordt door de Attack Group 'INFO:SMB:ANOM'. Die zorgt er niet alleen voor dat de Conficker-aanval gelogd maar ook tegengehouden wordt. Zo kon tijdens het onderzoek pas ingebroken worden in het systeem vanaf dat deze Attack Group terug verwijderd was.

3.7.3 Verschillend log-methodes

Waar de Juniper firewall in uitblinkt is het grote aantal manieren waarop je aan logging kan doen, meer bepaald de plaatsen waar de logging-gegevens naartoe gestuurd kunnen worden.

Bij Configuration > Report Settings > Log Settings staan de verschillende manieren om aan logging te doen. Zo zijn er: Console, Internal (het Event log), Email, SNMP, Syslog en USB. Voor elke manier kan je opgeven vanaf welk Security Level moet gelogd worden. Die Security Levels of niveaus gaan van debugging tot emergency. Dat laatste is het hoogste niveau en wordt gebruikt voor zaken zoals de zware aanvallen.

Voor de loginformatie kan het handig zijn dat de juiste datum en tijd bij de gegevens in de tabellen staan.

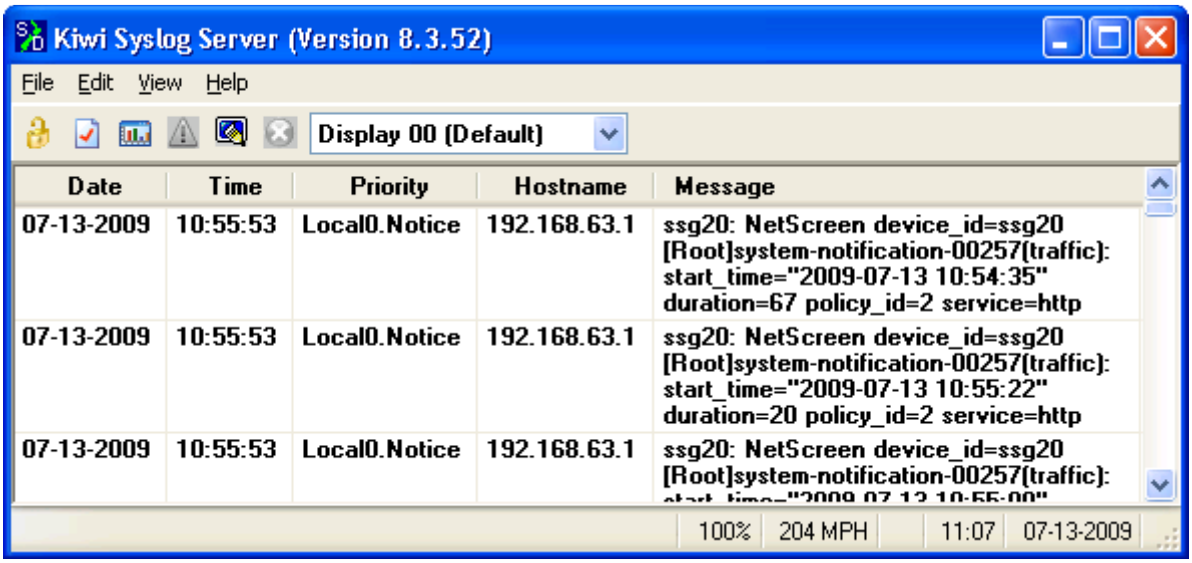
Dit doe je door naar Configuration > Date/Time te gaan en daar bovenaan 'Sync Clock With Client' aan te klikken.

De log-gegevens worden opgeslagen in het interne flash-geheugen. Dat flash-geheugen is beperkt, vooral als je veel gebruikers hebt en daar veel van wil loggen. Bij de SSG 20 zit er maar 64 MB flash in, zo bleek na onderzoek van de interne behuizing. Daarom zijn er andere manieren om meer log-gegevens te kunnen opslaan zoals syslog en USB, die nu gaan behandeld worden.

3.7.3.1 Syslog

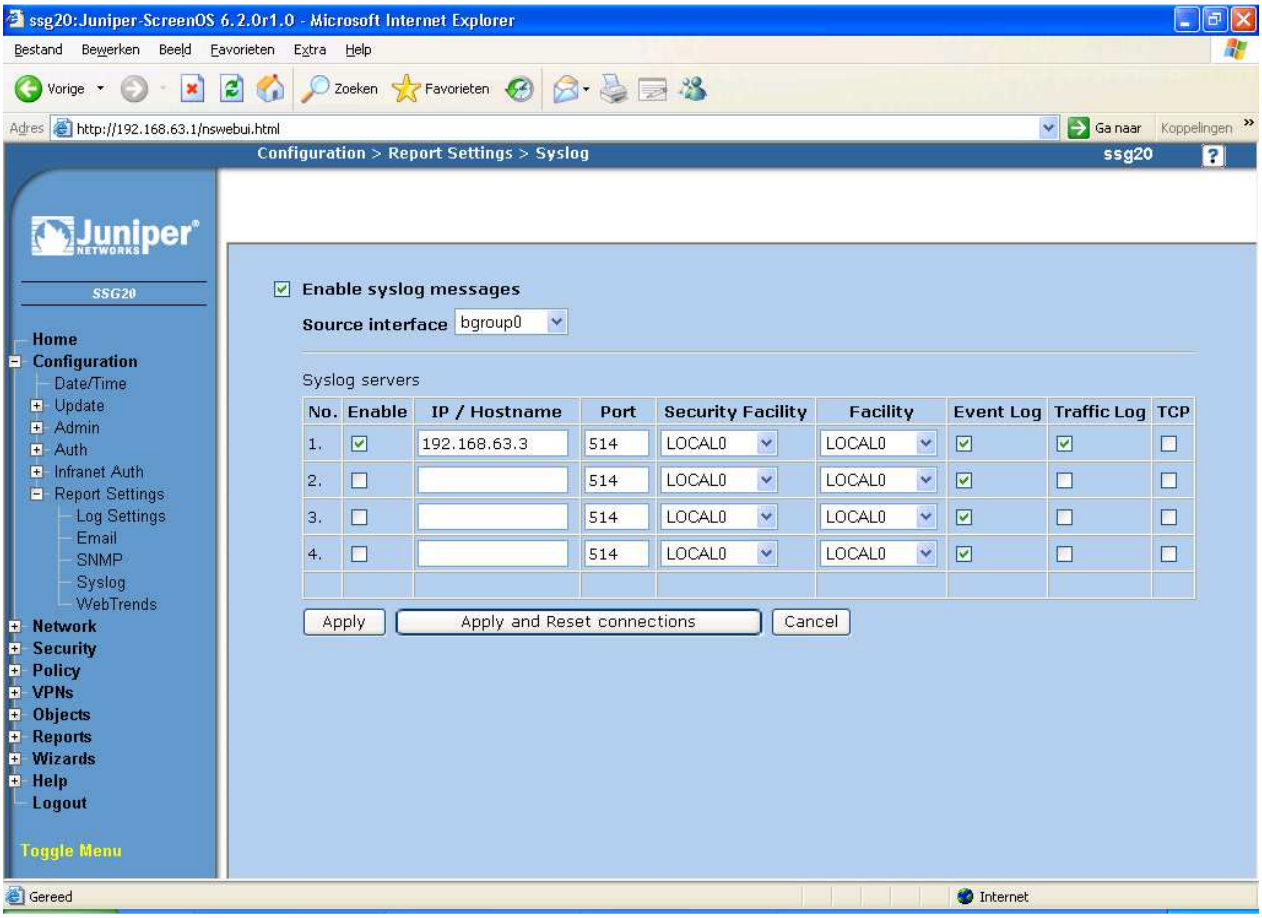
Syslog is een protocol om in de eerste plaats logging-gegevens over het netwerk te sturen. Een syslog-server is een systeem waar een syslog service op draait in de vorm van een programma. Die syslog service ontvangt en presenteert de gegevens die met het syslog-protocol toekomen op het systeem.

Als programma voor de syslog-service is er gekozen voor het gratis Kiwi Syslog Server. Dat programma is geïnstalleerd op de inside host. Er bestaan echter veel uitgebreidere software pakketten maar die vallen een stuk duurder uit.



Figuur 3.15 - Screenshot van Kiwi Syslog Server

Om syslog op de firewall in te stellen ga je naar Configuration > Report Settings > Syslog.



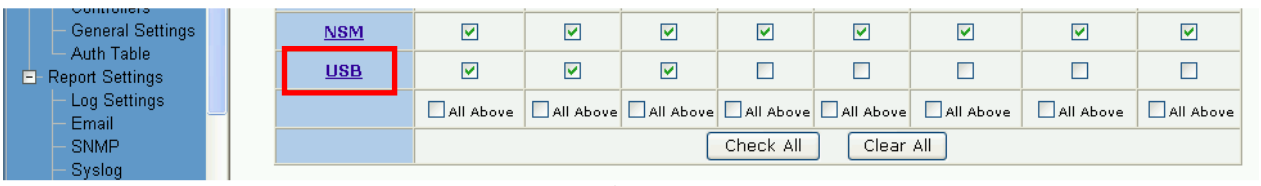
Figuur 3.16

Daar vink je 'Enable syslog messages' aan. Je vult op de eerste regel het IP-adres van je syslog server in en je vinkt 'Enable' aan.

Waar je op moet letten is het laatste vinkje om aan te geven of je via TCP of UDP je gegevens wil sturen naar je syslog server. Als je dit verschillend instelt aan beide kanten dan werkt het niet, zo bleek na het testen.

3.7.3.2 USB

Extern USB flash-geheugen oftewel een USB-stick wordt nog niet lang ondersteund. Dat zie je onder meer aan het feit dat de web interface er nog niet echt op voorzien is. Als je op de link USB klikt bij Configuration > Log Settings dan kom je bijvoorbeeld uit bij een pagina die NSM heet. Die link is dus nog niet de juiste.



Figuur 3.17

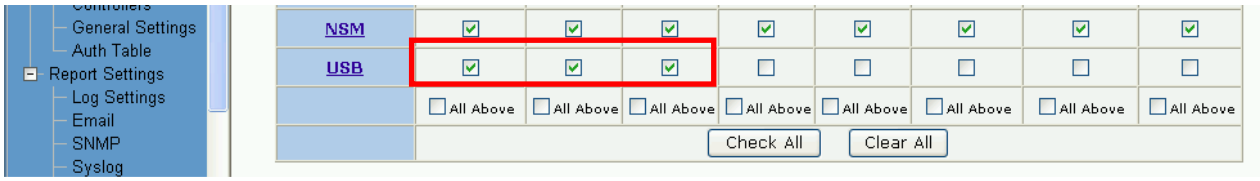
Tevens moet je het commando 'set log usb enable' gebruiken in de CLI voordat het werkt [37]. In de webinterface vind je die optie niet.

Verdere beperkingen zijn dat USB-sticks maar maximum 1 GB groot mogen zijn en dat er weinig documentatie voor handen is over de logging via USB. Verder kan je niet bepalen welke gegevens (welke kolommen) gelogd worden. Zo wordt van HTTP trafiek e.d., het interne IP-adres (van diegene die aan het surfen is) niet gelogd als je met NAT werkt. Het outside adres van de firewall, dat gebruikt wordt om de interne adressen naartoe te vertalen, staat er wel in. Die regels in de log zijn dan ook vrijwel waardeloos. Als je geen NAT gebruikt dan zijn ze niet waardeloos want dan zie je wel de interne adressen in de logs. NAT wordt echter in de meeste hedendaagse netwerken toegepast.

Hieronder volgt een voorbeeld van een regel in het log als je NAT gebruikt. Daarin zie je enkel het outside adres van de firewall (10.130.223.104).

```
2009-07-13 15:59:27   [Root]system-traffic-information:    0:00:14 src
10.130.223.104:1113   dst 213.199.164.111:80   HTTP     Close - TCP RST
```

Als je enkel de log-gegevens van aanvallen voor lange tijd wil loggen, ben je echter wel goed gesteld met de huidige functies van USB logging.



Figuur 3.18

Daarvoor moet je enkel de eerste drie vinkjes aanduiden bij Configuration > Report Settings > Log Settings.

Die zorgen ervoor dat je loggegevens van het niveau (van links naar rechts) emergency, alert en critical gaat loggen naar USB. Al de meldingen van scans door Nmap en Nessus (en van de meeste andere security tools) hebben namelijk die niveaus.

Een voorbeeld van een attack-regel in het log op de USB-stick:

```
2009-07-13 16:49:24  [Root]system-alert-00016: Port scan! From
10.130.209.95:59197 to 10.130.223.104:3370, proto TCP (zone Untrust int
ethernet0/0). Occurred 1 times.
```

Moest er een hacker fysiek aan de firewall kunnen via een consolekabel dan kan hij nog wel, als hij bedreven is met Juniper firewalls, het log wissen met '`delete file usb:ssg20_datumVanLog_log.txt`'. Hij moet natuurlijk dan wel de login gegevens kennen.

3.7.4 Besluit

Als besluit van de evaluatie van de IPS-mogelijkheden kunnen onderstaande zaken opgemerkt worden.

Standaard wordt er geen enkele aanval gelogd. Je moet zelf maar uitzoeken in verscheidene pagina's met tabellen welke opties je moet aanvinken. Vele netwerkbeheerders zullen deze moeite niet doen en bijgevolg blind zijn voor aanvallen.

Aangezien Nmap en Nessus dezelfde informatie geven, of je nu de screening of deep inspection opties opzet of niet, kan je zeggen dat het daadwerkelijk tegenhouden van aanvallen niet doeltreffend is. Bij de opties van screening komt het woord 'Protection' (bescherming) vaak voor, maar dat moet toch wel genuanceerd worden. Er wordt inderdaad wel wat beschermd, zij het niet dat de huidige netwerktools die bescherming te snel af zijn.

Vooral de Deep Inspection functie is zeer ongebruiksvriendelijk. Een paar voorbeelden:

- Je kan niet zoeken in de tabel met attacks naar een attack die jij zoekt.
- De informatie van de verschillende signatures is zonder meer cryptisch.
- Het toevoegen van meerdere attack groups in je policy is ontzettend omslachtig.

Het is ten sterkste aan te raden om de eerder aangegeven opties van screening, die Nmap en Nessus kunnen loggen, aan te vinken. Alsook op de attack group te controleren die de Metasploit-aanval kan loggen en tegenhouden.

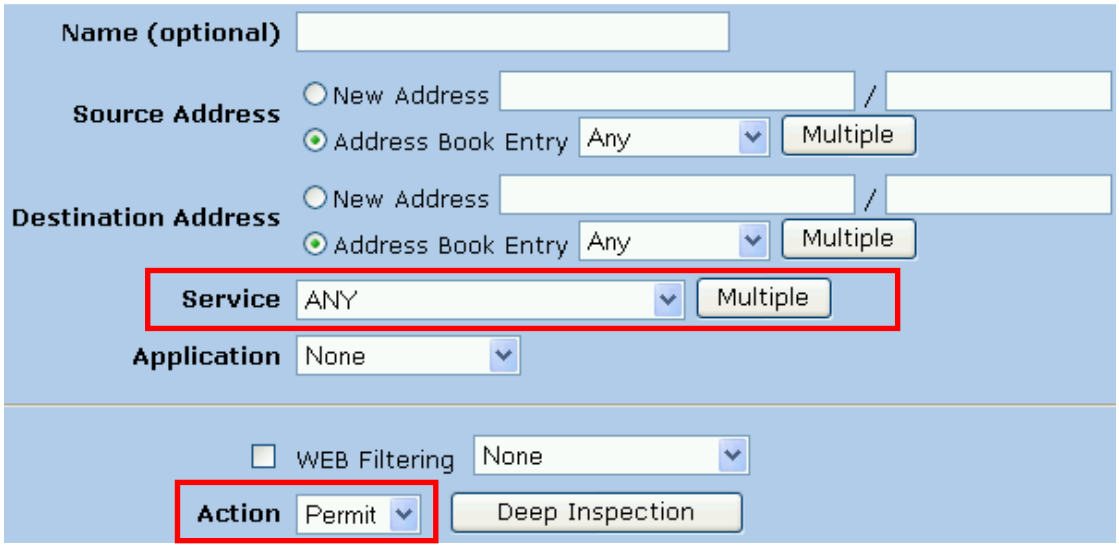
Het loggen heeft nog een beperking, namelijk dat de interne opslagruimte niet groot is. Als je veel gegevens wil loggen, bijvoorbeeld het HTTP-trafiek van een groot netwerk, dan zal het interne flash geheugen te beperkt zijn. Daarom kan je een USB-stick gebruiken of een syslog server die dit probleem gedeeltelijk of helemaal zal oplossen. De USB-stick is een sterke aanrader om aanvallen te loggen.

3.8 Voorbeeldpolicy toepassen

In stap 2 en stap 3 lees je over een penetration test nadat de voorbeeldpolicy is toegepast. Hier lees je hoe je die voorbeeldpolicy toepast.

3.8.1 Een firewall rule toevoegen

Telkens je een nieuwe regel in de firewall policy wil aanmaken moet je bij Policy > Policies vanboven kiezen tussen welke zones je het verkeer wil regelen (bij 'From' & 'To').
Daarna klik je op New. Dan kom je in onderstaand venster waar je zeker een of meerdere (Multiple) services moet selecteren . Bij Action geef je aan wat er moet gebeuren met dat verkeer (doorlaten of niet).



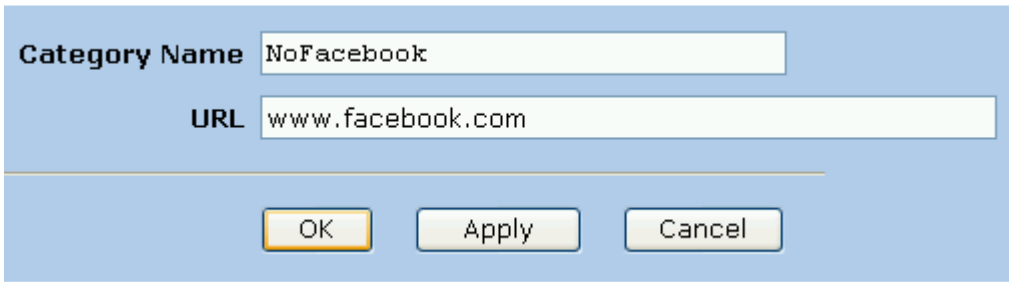
Figuur 3.19

3.8.2 URL filtering

URL filtering heet bij Juniper 'Web Filtering'. Je hebt daarbij drie verschillende mogelijkheden die je vindt bij Security > Web Filtering > Protocol.
Voor de tweede en derde optie heb je een eigen web filtering server nodig. Aangezien er onderzocht wordt wat de firewall kan, en niet wat extra servers kunnen is hier gekozen voor de eerste optie 'Integrated (SurfControl)' waarbij de web filtering server ingebouwd wordt in de firewall.

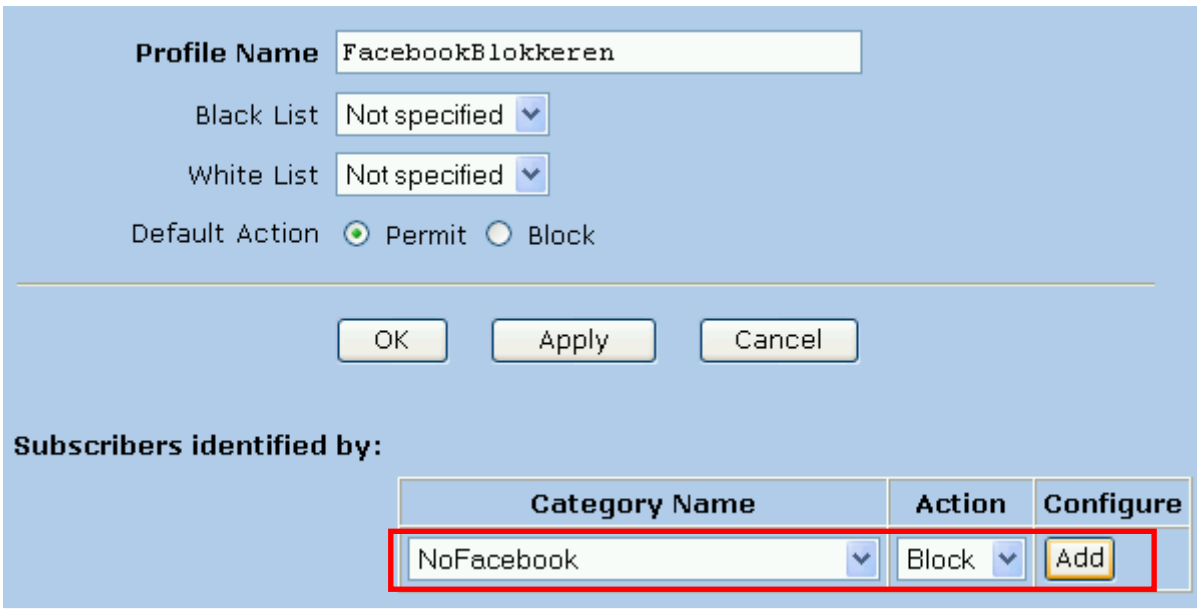
Bovenaan bij Web Filtering > Protocol kan je SC-CPA selecteren. Daar moet een vinkje zijn dat 'Enable Web Filtering via CPA Server' heet.

Om facebook.com te blokkeren ga je naar Security > Categories > Custom waar je op New klikt. Daar kan je je eigen profiel een naam geven met eigen URL's, in dit geval www.facebook.com.



Figuur 3.20

Bij Security > Profiles > Custom klik je tevens op New. Daar geef je je nieuw profiel een naam en zorg je ervoor dat je de categorie die je hebt aangemaakt, wordt geblokkeerd.



Figuur 3.21

Bij Policy > Policies klik je op Edit naast de policy-regel die je HTTP verkeer doorlaat. In het daaropvolgende venster, waar je je policy kan aanpassen, vink je WEB Filtering aan en selecteer je je webfiltering-profiel (zie onderstaande figuur). Je kan het ingebouwde profiel 'ns-profile' gebruiken maar je kan ook je eigen profiel maken met eventueel eigen categorieën.

Figuur 3.22

3.8.3 Deep inspection

De Juniper firewall heeft zelf de 'predefined services' die MSN en MS-Messenger heten, maar na onderzoek bleek dat zij Windows Live Messenger noch Windows Messenger tegenhouden.

Om Windows (Live) Messenger te blokkeren moet je een werkwijze volgen die sterk gelijkt op de manier waarop je facebook.com blokkeert. Bij web filtering had je voorgedefinieerde profielen, nu heb je voorgedefinieerde Attacks en Attack Groups. Om Windows (Live) Messenger te blokkeren wordt er een eigen Attack en Attack Group gemaakt.

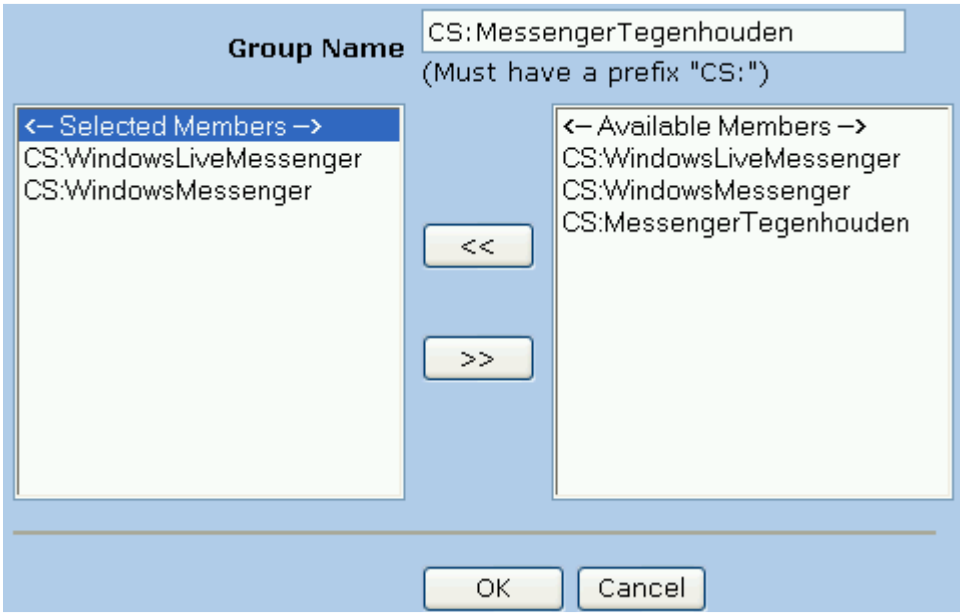
Dat eerste doe je bij Security > Deep Inspection > Attack > Custom waar je op New klikt. Je maakt op die manier twee Attacks aan zoals de Attacks op volgend screenshot.

Name	Type	Context	Severity	Pattern	Configure	
CS:WindowsLiveMessenger	signature	http-header-user-agent	info	.*Windows Live Messenger.*	Edit	Remove
CS:WindowsMessenger	signature	http-header-user-agent	info	MSMSGS	Edit	Remove

Figuur 3.23

Bij de Pattern-kolom zie je in de eerste regel de jokertekens '.*'. Dat dient om aan te geven dat er nog tekst voor en achter mag staan. Zonder dit werkt het niet, bleek na onderzoek.

Een eigen Attack Group maken doe je via Security > Deep Inpection > Attack Groups > Custom. Daar klik je weer op New. Om dan het volgend scherm in te vullen zoals in volgende screenshot.



Figuur 3.24

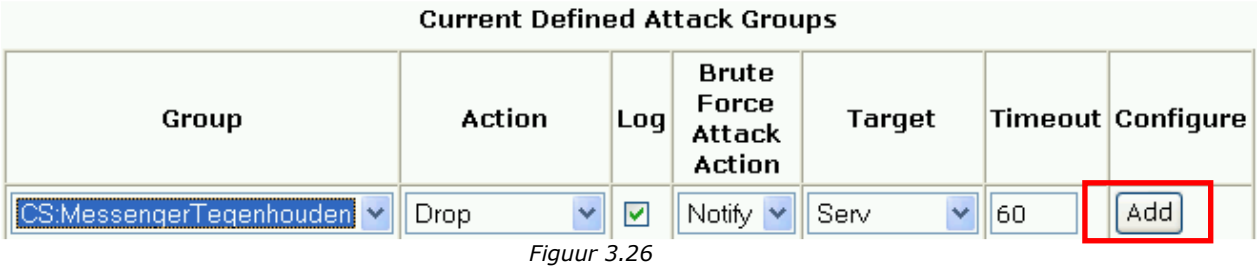
Onder de plaats in de interface waar je web filtering instelde per policy-regel kan je nu deep inspection instellen.

Je klikt daarvoor op de knop 'Deep Inspection' (zie figuur hieronder).

De Action drop down box naast die knop heeft niets te maken met webfiltering noch deep inspection. Het bepaalt gewoon de actie die ondernomen wordt als een connectie aan de firewall aankomt die aan die policy-regel voorwaarden voldoet. Je kan je dan ook afvragen waarom die knop op die plaats staat.

Figuur 3.25

Als je op de knop Deep Inspection hebt geklikt kom je in een venster waar je je Attack Group moet selecteren en dan op Add klikken, zoals in onderstaande screenshot.



Figuur 3.26

Er valt te noteren dat de lijst van Predefined Attacks die kunnen tegengehouden worden op geen enkele manier overzichtelijk is. Als je wil zien of er een bepaalde aanval tegen wordt gehouden moet je een tabel met ongeveer 800 regels zelf regel per regel controleren.

Verder valt het op dat er heel weinig instelbaar is voor Web Filtering en Deep Inspection.

3.8.4 De uiteindelijke firewall policy

From Trust To Untrust, total policy: 2

ID	Source	Destination	Service	Action	Options	Configure			Enable	Move
2	Any	Any	DNS FTP HTTP HTTPS PING			Edit	Clone	Remove	☑	
1	Any	Any	ANY			Edit	Clone	Remove	☑	

From Untrust To Trust, total policy: 3

ID	Source	Destination	Service	Action	Options	Configure			Enable	Move
3	10.130.209.95/24	Any	RDP- OpAfstandBeheren			Edit	Clone	Remove	☑	
4	Any	Any	PING			Edit	Clone	Remove	☑	
5	Any	Any	ANY			Edit	Clone	Remove	☑	

Figuur 3.27

Merk op dat het beter zou zijn moesten de IP-adressen bij Source of Destination meer gespecificeerd worden i.p.v. 'Any' te gebruiken.

Verder kan je ook opmerken dat de 'deny any' regels (regel 1 en 5) zijn toegevoegd aan de policy om de firewall policy duidelijker te maken. Er staat sowieso een impliciete regel op het einde die al het verkeer tegenhoudt, maar die zie je nooit.

4 CHECK POINT R70

De firewall van Check Point is als laatste aan de beurt. Vaak wordt Check Point bezien als een van de meest degelijke. Of dat terecht is of niet, lees je hier.

4.1 Prijs

Om de prijs te weten te komen van een Check Point softwarepakket moet er gekeken worden naar de prijs van de verschillende delen afzonderlijk [38].

Om te beginnen wordt er gekozen voor de 'SG201 Check Point Security Gateway Container'. Dat is een container die als basis dient voor de verschillende software blades. Elke software blade stelt een functie voor. De SG201 ondersteunt een processor met 2 kernen en tot 500 users. Prijs: € 4 606,01

De verschillende software blades:

- VPN: € 1 062,93
- IPS: € 2 125,85
- URL Filtering: € 1 062,93
- Alle software blades samen: € 3 543,08
    - De verschillende software blades: IPS, URL Filtering, Antivirus & Anti-Malware, Anti-Spam & Email Security

Het mag duidelijk zijn dat er gekozen wordt voor alle software blades samen wegens het schaalvoordeel.

De bedragen zijn omgerekend van Amerikaanse dollar naar euro.

Hierbij moet tevens de € 1 104,30 voor de server bijgerekend worden (zie 1.8 Server voor ISA Server en Check Point).

Zoals je in paragraaf 1.8 kan lezen is er gekozen voor een server met een processor met 2 kernen. Als er voor 1 kern wordt gekozen wordt de Check Point plots een stuk goedkoper. De SG201 wordt dan vervangen door de SG101 die maar € 1 417.23 kost. Het pakket met alle software blades in komt dan op € 1 771,54. In totaal een besparing van € 4 960.32, daarvoor kan je al eens nadenken of je wel 2 kernen nodig hebt.

Het totale kostenplaatje met de twee kernen zou € 9 253,39 zijn.

Het totale kostenplaatje met één kern zou € 4 293,07 zijn.

4.2 Eerste kennismaking

4.2.1 Naamgeving

Figuur 4.1

Check Point heeft voor al zijn producten een aparte naam en op de koop toe verandert Check Point vaak die naamgeving [39].

Zo heette het firewall product vroeger FireWall-1. Daarna had het de naam VPN-1 gekregen. Sinds de nieuwste versie (R70) is VPN-1 gedoopt onder de nieuwe naam Check Point Security Gateway.

Regelmatig kom je op de website, in de 'help' en in de installatieprocedure nog oude benamingen tegen die het er niet gemakkelijker op maken om alles te onderscheiden.

De versie van VPN-1/Check Point Security Gateway werd in het verleden ook vaak anders weergegeven. De versienummers werden eerst geschreven als gewone versienummers (bvb. 3.0), daarna werden de letters NG er aan toegevoegd. De vorige versie werd nog geschreven als NGX R64, maar ondertussen is de NGX achterwege gelaten bij R70 versie. Check Point verandert dus graag zijn naamgeving, dit zie je ook in onderstaande figuur van op de officiële website van Check Point. Volgens Check Point toont de figuur de verschillende 'vernieuwingen' over de jaren heen.

Figuur 4.2

Er is wel een positieve trend te merken in de naamgeving. Check Point lijkt bepaalde namen te vervangen door termen die meer gangbaar zijn in de security wereld. Zo is de term 'SmartDefense' vervangen door 'IPS' bijvoorbeeld.

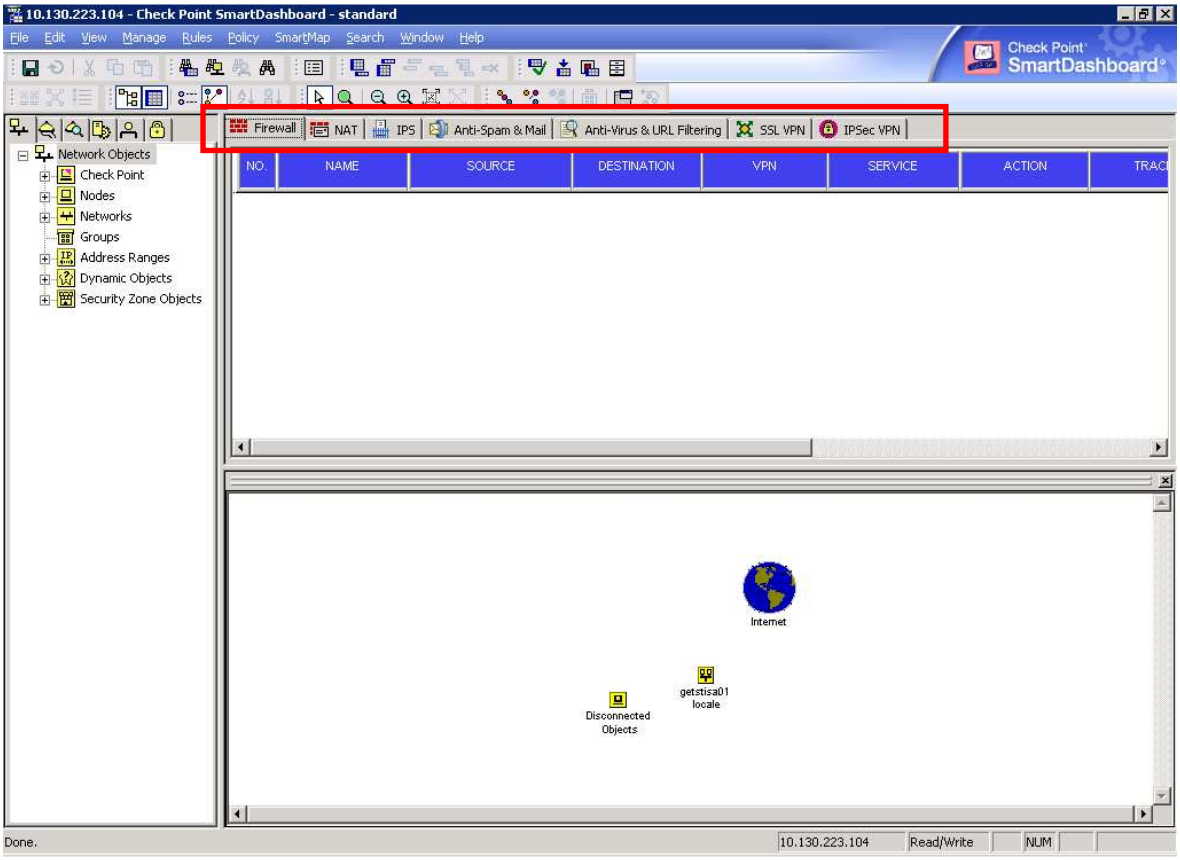
4.2.2 Interface

Als je het softwarepakket 'Check Point R70' installeert worden meerdere programma's geïnstalleerd, elk met zijn eigen interface.

De belangrijkste programma's:

- SmartDashboard: Dit is het belangrijkste onderdeel waarin je de gateway (de eigenlijke firewall) kan instellen. De verschillende functionaliteiten zoals de firewall policy (in de tab 'Firewall'), NAT, IPS, AntiSpam & Mail … vind je terug in verschillende tabs in de interface. Zie onderstaand screenshot.
- SmartView Tracker: Voor de logs te bekijken.
- SmartView Monitor: Voor de firewall(s) en het netwerk te monitoren.
- Check Point Configuration Tool: Voor instellingen voor bijvoorbeeld licenties.

In de screenshot hieronder wordt enkel de interface van SmartDashBoard bekeken. Je vindt de belangrijkste functies van de firewall in de verschillende tabs. Bij de tab Firewall kan je de firewall policy instellen. De rest van de namen voor de tabs spreken voor zich.

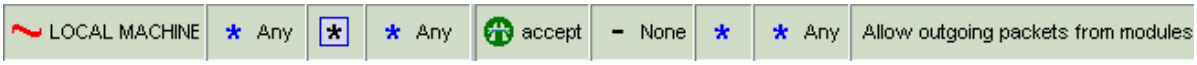


Figuur 4.3

4.2.3 Wat zet de firewall default open?

Standaard staat alles dicht, enkel een paar controle- en VPN-connecties worden doorgelaten. Die regels zijn 'impliciete regels' en worden standaard niet getoond in de firewall policy. Je kan ze zichtbaar maken via het menu bij View > Implied Rules.

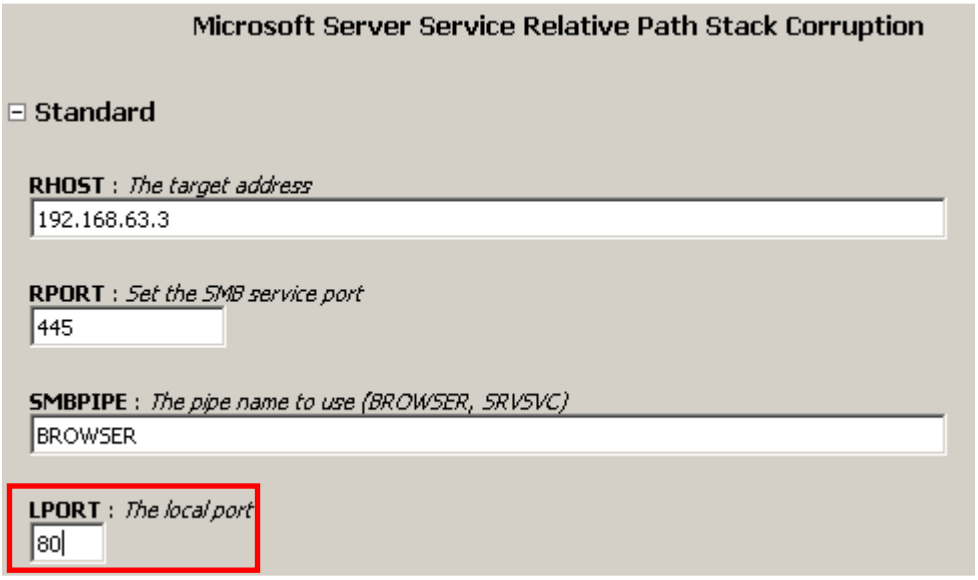
Een voorbeeld van zo'n impliciete regel is de volgende regel die al het verkeer toelaat dat vanaf de firewall zelf komt.



Figuur 4.4

4.2.4 Wat moet er open staan voor Metasploit?

Na onderzoek bleek dat de enige poorten die moeten open staan om een Conficker-aanval met Metasploit door te laten 445 (check point naam: microsoft-ds) van de hacker pc naar inside host en 4444 (check point naam: Napster_directory_4444) van inside host naar hacker pc zijn. Poort 4444 is de poort die standaard door Metasploit gebruikt wordt om van het geïnfecteerde systeem een connectie terug naar de aanvaller te maken.
Die poort kan je aanpassen in Metasploit. Het slimste voor de hacker is dan om poort 80 te kiezen omdat die toch meestal open staat vanuit de inside hosts naar het internet toe. De hacker kan ook kiezen voor een andere poort die vaak openstaat zoals 21 (FTP). Met andere woorden, het enige wat de hacker nodig heeft om in te breken op een systeem is dat de poort 445 open staat naar het onveilige systeem toe.



Figuur 4.5

4.3 Stap 1: Penetration test met default configuratie

4.3.1 Stap 1a: Scan met Nmap

Intense scan, no ping:

```
Starting Nmap 4.85BETA7 ( http://nmap.org ) at 2009-07-15 11:19 Romance
(standaardtijd)
Initiating Parallel DNS resolution of 1 host. at 11:19
Completed Parallel DNS resolution of 1 host. at 11:19, 6.50s elapsed
Initiating SYN Stealth Scan at 11:19
Scanning getstisa01.vbdomein.be (10.130.223.104) [1000 ports]
SYN Stealth Scan Timing: About 29.50% done; ETC: 11:20 (0:01:14 remaining)
Completed SYN Stealth Scan at 11:19, 34.45s elapsed (1000 total ports)
Initiating Service scan at 11:19
Initiating OS detection (try #1) against getstisa01.vbdomein.be
(10.130.223.104)
Initiating Traceroute at 11:19
10.130.223.104: guessing hop distance at 1
Completed Traceroute at 11:19, 0.02s elapsed
Initiating Parallel DNS resolution of 3 hosts. at 11:19
Completed Parallel DNS resolution of 3 hosts. at 11:19, 0.00s elapsed
NSE: Initiating script scanning.
```

```
Host getstisa01.vbdomein.be (10.130.223.104) is up (0.00s latency).
Interesting ports on getstisa01.vbdomein.be (10.130.223.104):
Not shown: 999 filtered ports

PORT    STATE  SERVICE VERSION
264/tcp closed bgmp

Device type: firewall|general purpose|media device|WAP

Running: ISS Linux 2.4.X, Linux 2.6.X, Microsoft Windows
2000|2003|98|Vista|XP, Motorola Windows PocketPC/CE, NetworksAOK embedded,
Planet embedded
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using port 264/tcp)
HOP RTT   ADDRESS
1   16.00 10.130.209.1
2   0.00  getstisa01.vbdomein.be (10.130.223.104)

Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 43.06 seconds
           Raw packets sent: 2025 (91.332KB) | Rcvd: 11 (472B)
```

Nmap krijgt informatie over één poort, namelijk die van BGMP. Omdat het systeem reageert weet je dat het systeem op staat. De bewuste poort is echter wel gesloten. De gesloten poort, BGMP (Border Gateway Multicast Protocol) is geen bekende poort waar gebruikers op zitten. Dat geeft dus aan dat het systeem normaal gezien een netwerkapparaat is en geen gewone pc.

4.3.2 Stap 1b: Scan met Nessus

Nessus geeft geen enkele output omdat het denkt dat het systeem uit staat.

4.3.3 Stap 1c: Aanval met Metasploit

De Conficker-aanval met Metasploit werkt niet.

4.3.4 Besluit

Standaard staat zowat alles toe naar de firewall en naar de andere interfaces (dus ook naar de inside host). Dan is het ook te begrijpen dat de scan van Nmap en de scan van Nessus helemaal niet veel te weten komen over het systeem. Dit is een goede default instelling voor een firewall.

4.4 Stap 2: Penetration test met voorbeeldpolicy

4.4.1 Stap 2a: Scan met Nmap

Intense scan, no ping:

```
Starting Nmap 4.85BETA7 ( http://nmap.org ) at 2009-07-20 11:31 Romance
(standaardtijd)
```

```
Initiating Parallel DNS resolution of 1 host. at 11:31
Completed Parallel DNS resolution of 1 host. at 11:31, 6.50s elapsed

Initiating SYN Stealth Scan at 11:31
Scanning getstisa01.vbdomein.be (10.130.223.104) [1000 ports]
Completed SYN Stealth Scan at 11:32, 12.42s elapsed (1000 total ports)

Initiating Service scan at 11:32
Initiating OS detection (try #1) against getstisa01.vbdomein.be
(10.130.223.104)
Initiating Traceroute at 11:32
10.130.223.104: guessing hop distance at 1
Completed Traceroute at 11:32, 0.03s elapsed
Initiating Parallel DNS resolution of 3 hosts. at 11:32
Completed Parallel DNS resolution of 3 hosts. at 11:32, 0.00s elapsed
NSE: Initiating script scanning.

Host getstisa01.vbdomein.be (10.130.223.104) is up (0.00s latency).
Interesting ports on getstisa01.vbdomein.be (10.130.223.104):
Not shown: 999 filtered ports

PORT    STATE  SERVICE VERSION
264/tcp closed bgmp

Device type: firewall|general purpose|media device|WAP
Running: ISS Linux 2.4.X, Linux 2.6.X, Microsoft Windows
2000|2003|98|Vista|XP, Motorola Windows PocketPC/CE, NetworksAOK embedded,
Planet embedded
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using port 264/tcp)
HOP RTT   ADDRESS
1   16.00 10.130.209.1
2   0.00  getstisa01.vbdomein.be (10.130.223.104)
Read data files from: C:\Program Files\Nmap

OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 20.42 seconds
           Raw packets sent: 2026 (91.376KB) | Rcvd: 12 (512B)
```

Weer geeft Nmap aan dat de BGMP-poort dicht staat, meer niet.

4.4.2 Stap 2b: Scan met Nessus

Voor Nessus lijkt het alsof het systeem uit staat. Het geeft daarom geen output.

4.4.3 Stap 2c: Aanval met Metasploit

Een aanval met Metasploit werkt niet omdat poort 445 niet open wordt gelaten door de firewall.

4.4.4 Besluit

Check Point geeft bijna niets prijs. De Check Point firewall is dus zeer goed afgedicht.

4.5 Stap 3: Penetration test van inside host

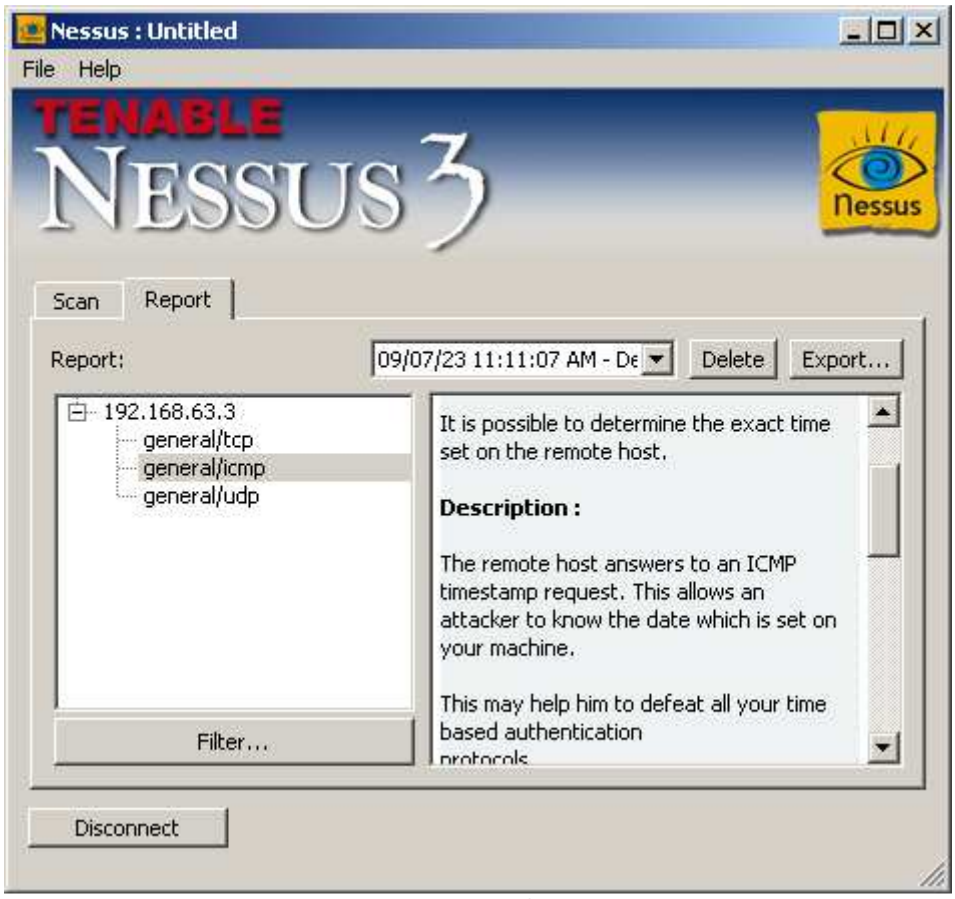
4.5.1 Stap 3a: Scan met Nmap

Intense scan, no ping:

```
Starting Nmap 4.85BETA7 ( http://nmap.org ) at 2009-07-23 11:01 Romance
(standaardtijd)
Initiating Parallel DNS resolution of 1 host. at 11:01
Completed Parallel DNS resolution of 1 host. at 11:01, 0.00s elapsed
Initiating SYN Stealth Scan at 11:01
Scanning 192.168.63.3 [1000 ports]
SYN Stealth Scan Timing: About 29.50% done; ETC: 11:03 (0:01:14 remaining)
SYN Stealth Scan Timing: About 58.50% done; ETC: 11:03 (0:00:43 remaining)
Completed SYN Stealth Scan at 11:03, 104.00s elapsed (1000 total ports)
Initiating Service scan at 11:03
Initiating OS detection (try #1) against 192.168.63.3
Retrying OS detection (try #2) against 192.168.63.3
NSE: Initiating script scanning.
Host 192.168.63.3 is up (0.00s latency).

All 1000 scanned ports on 192.168.63.3 are filtered
Too many fingerprints match this host to give specific OS details

Read data files from: C:\Program Files\Nmap

OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 107.01 seconds

Raw packets sent: 2036 (92.716KB) | Rcvd: 4 (652B)
```

Bij de vorige scans gaf Nmap nog aan dat de BGMP-poort toe stond. Nu geeft Nmap nog minder informatie. Er is geen enkele open poort gevonden, daarom is de output van Nmap ook korter dan gewoonlijk.

4.5.2 Stap 3b: Scan met Nessus



Figuur 4.6

Omdat Nessus anders geen output geeft is er hier gekozen voor een ICMP ping i.p.v. een TCP ping. Daarmee komt Nessus enkel te weten dat het systeem op staat.

4.5.3 Stap 3c: Aanval met Metasploit

Metasploit kon zijn aanval niet voltrekken omdat de poort 445 niet open staat.

4.5.4 Besluit

In de policy die gedefinieerd is (zie 4.9.4 De uiteindelijke firewall policy)Inleiding merk je al dat enkel ICMP wordt doorgelaten. Dat merk je ook bij de penetration test want geen enkele test weet informatie los te weken. En omdat ICMP door wordt gelaten zie je dat de inside host aan staat.

4.6 Stap 4: Penetration test vanuit inside LAN

4.6.1 Stap 4a: Scan met Nmap

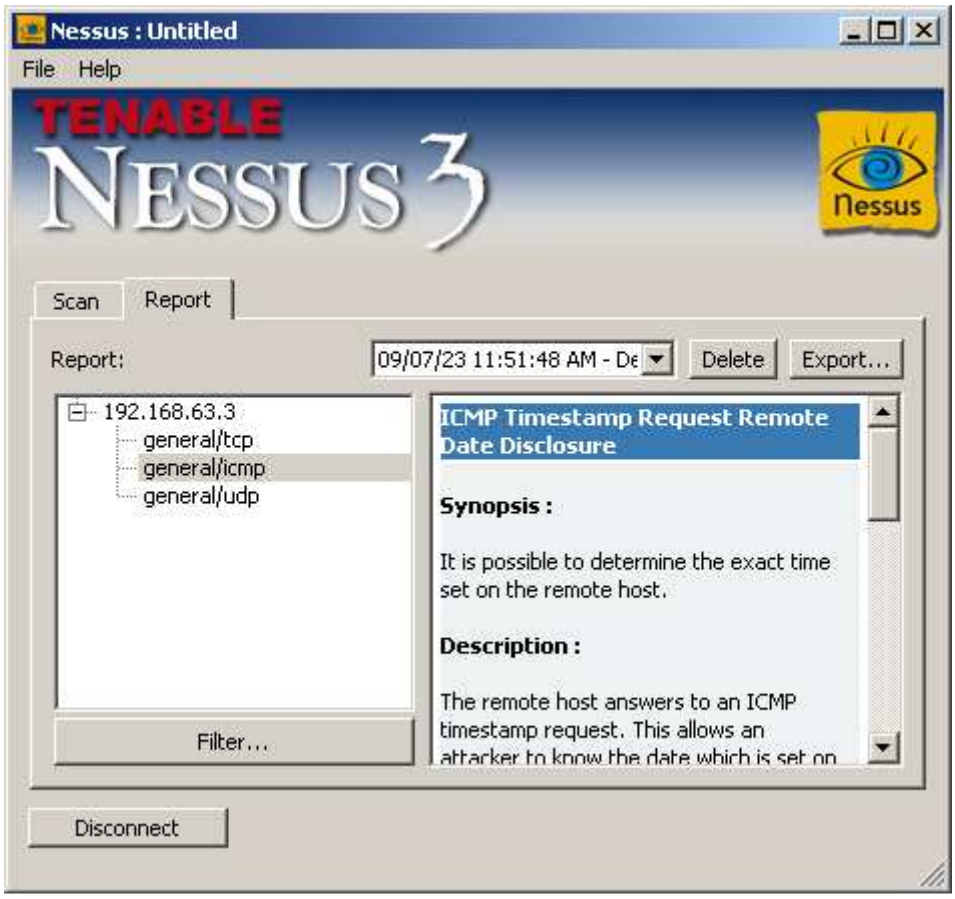
Intense scan, no ping:

```
Starting Nmap 4.85BETA7 ( http://nmap.org ) at 2009-07-23 11:51 Romance
(standaardtijd)
```

```
Initiating Parallel DNS resolution of 1 host. at 11:51
Completed Parallel DNS resolution of 1 host. at 11:51, 0.00s elapsed

Initiating SYN Stealth Scan at 11:51
Scanning 192.168.63.3 [1000 ports]
Completed SYN Stealth Scan at 11:51, 5.42s elapsed (1000 total ports)

Initiating Service scan at 11:51
Initiating OS detection (try #1) against 192.168.63.3
Initiating Traceroute at 11:51
192.168.63.3: guessing hop distance at 2
Completed Traceroute at 11:51, 0.02s elapsed
Initiating Parallel DNS resolution of 4 hosts. at 11:51
Completed Parallel DNS resolution of 4 hosts. at 11:51, 6.50s elapsed
NSE: Initiating script scanning.

Host 192.168.63.3 is up (0.00s latency).
Interesting ports on 192.168.63.3:
Not shown: 996 filtered ports

PORT    STATE  SERVICE VERSION
21/tcp  closed ftp
53/tcp  closed domain
80/tcp  closed http
443/tcp closed https
Warning: OSScan results may be unreliable because we could not find at
least 1 open and 1 closed port

Device type: general purpose|media device
Running: Microsoft Windows 2000|2003|XP, Motorola Windows PocketPC/CE
OS details: Microsoft Windows 2000 Server SP4 or XP Professional SP3,
Microsoft Windows Server 2003 SP0 or Windows XP SP2, Microsoft Windows
Server 2003 SP1 or SP2, Microsoft Windows Server 2003 SP2, Microsoft
Windows XP Professional SP2 (French), Microsoft Windows XP SP2, Microsoft
Windows XP SP3, Motorola VIP1216 digital set top box (Windows CE 5.0)

TRACEROUTE (using port 21/tcp)
HOP RTT   ADDRESS
1   16.00 10.130.209.1
2   0.00  getstisa01.vbdomein.be (10.130.223.104)
3   0.00  192.168.63.3
Read data files from: C:\Program Files\Nmap
OS and Service detection performed. Please report any incorrect results at
http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 13.30 seconds
           Raw packets sent: 2018 (90.310KB) | Rcvd: 19 (1058B)
```

Er worden geen open poorten gevonden.

4.6.2 Stap 4b: Scan met Nessus



Figuur 4.7

4.6.3 Stap 4c: Aanval met Metasploit

De aanval met Metasploit lukt niet.

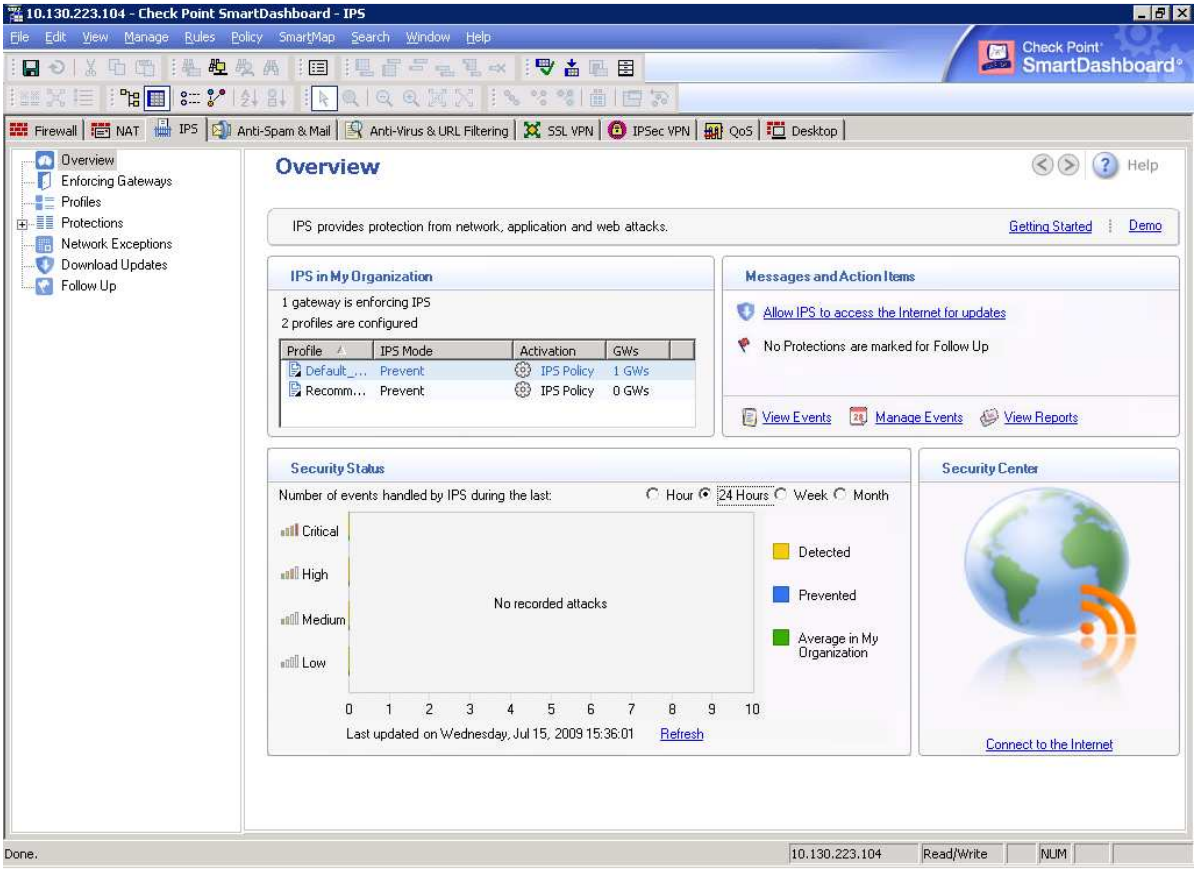
4.6.4 Besluit

Uit deze test is gebleken dat worms en hackers op het interne netwerk geen kans maken om in te breken op andere interne systemen.

4.7 Stap 5: IPS

De penetration tests hebben geen beveiligingslekken opgeleverd. Maar wat nog interessanter is, is kijken of de Check Point firewall even goed is in het detecteren en tegenhouden van de aanvallen en port scans van Nmap, Nessus en Metasploit?

De IPS functionaliteit is te vinden in de IPS-tab, zie figuur hieronder.



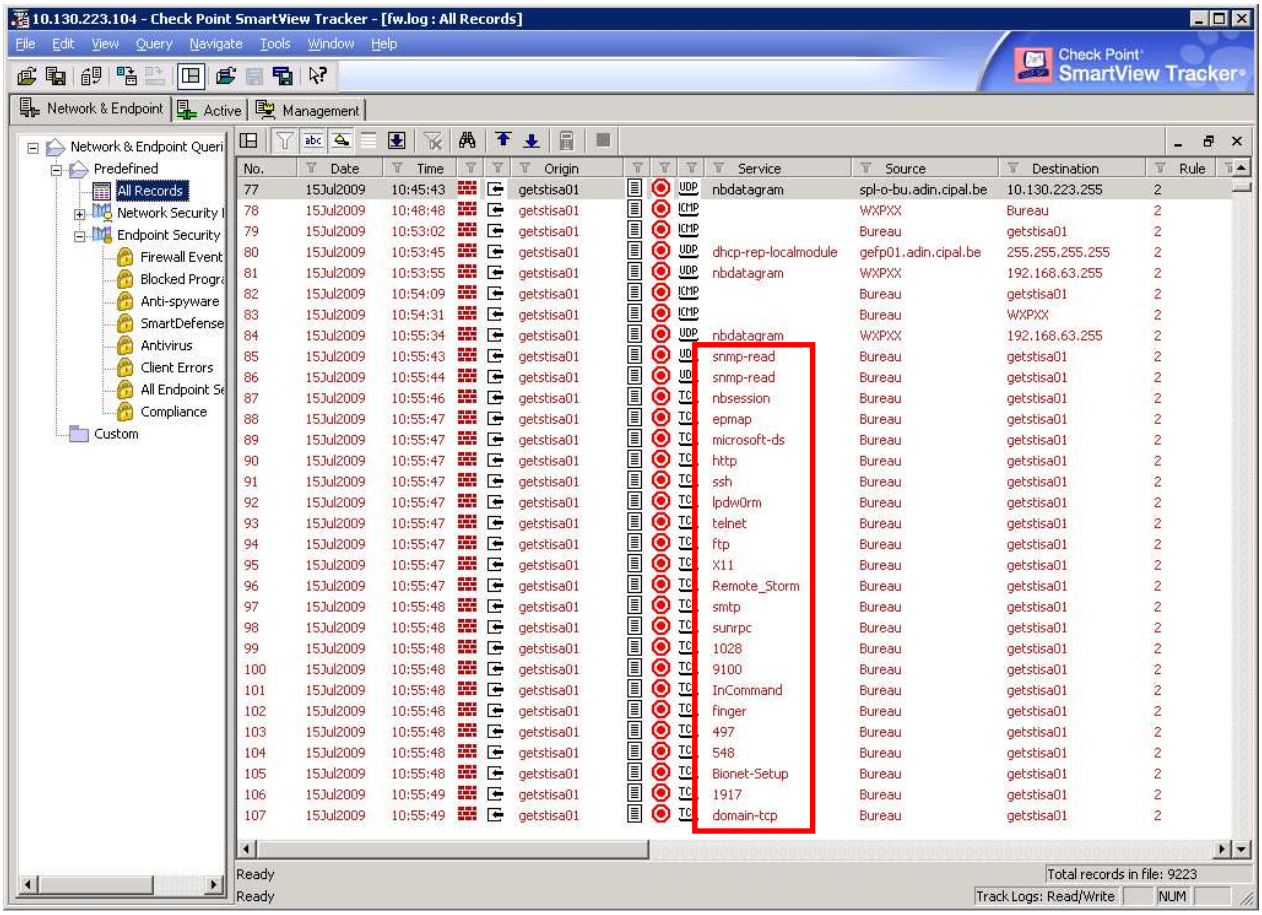
Figuur 4.8

Aangezien Check Point firewalls op servers draaien met harde schijven is er voldoende ruimte om log-gegevens op te slagen, alternatieve methodes zijn dan ook niet nodig. In het geval van een Alert, bij een aanval, kan er wel een mail of SNMP trap gestuurd worden.

Er kunnen verschillende IPS-profielen toegepast worden. Er zijn twee voorgedefinieerde profielen 'Default_Protection' en 'Recommended_Protection'. Nadat deze twee uitgetest zijn zal er een eigen aangepast profiel gemaakt en getest worden.

4.7.1 Default_Protection

Hoewel de IPS functie er op eerste zicht heel volledig uitziet en goed ingesteld staat, wordt er helemaal geen port scan of aanval gedetecteerd in het IPS-tabblad. De scans van Nmap en Nessus worden dus niet gelogd. Een Conficker-aanval wordt ook niet gesignaleerd in het IPS-tabblad. De scans en aanvallen worden echter wel gelogd samen met alle andere trafiek. Dus als je weet hebt van een aanval op een of andere manier kan je dit wel uitpluizen in de (vaak omvangrijke) log, zie onderstaand screenshot.



Figuur 4.9

In bovenstaande figuur zie je een screenshot van SmartView Tracker. Zoals eerder al vermeld dient dat programma om de logs te bekijken. Je kan in de log een port scan identificeren, maar enkel als je weet naar waar je moet zoeken. Je ziet namelijk dat verschillende willekeurige services, pakketjes aankrijgen.

Het niet detecteren van de tools kan je verklaren met het profiel dat default aanstaat. Dat profiel, 'Default_Protection', controleert op zo weinig mogelijk aanvallen om zo de firewall niet te veel te belasten. Zo staat de bescherming voor de Conficker-aanval default niet aan.

Figuur 4.10

Tijdens deze tests is de interface van de firewall, de SmartDashboard, een keer volledig gecrasht. De interface reageerde niet meer. En twee maal was de interface plots weg zonder dat de vensters door de gebruiker gesloten werden. Dit gegeven is toch wel verrassend.

4.7.2 Recommended_Protection

Nu wordt er getest wat er gebeurt als het profiel op 'Recommended_Protection' ingesteld staat. Dat profiel houdt de belangrijke zaken tegen zonder dat je daarvoor iets extra moet instellen.

4.7.2.1 Na scan met Nmap

De 'regular scan' lokt geen aanval-alarm uit. De 'intense scan, no ping' wel. Er is namelijk een melding dat een 'Malformed Packet' aangeeft. Nmap doet echter gewoon zijn ding, zonder daarbij echte hinder te ondervinden.

4.7.2.2 Na scan met Nessus

Er verschijnt dezelfde melding die 'Malformed Packet' aangeeft. Nessus lijkt er zich niets van aan te trekken.

4.7.2.3 Na aanval met Metasploit

Weer krijg je een melding 'Malformed Packet'. De aanval met Metasploit lukt niet.

4.7.3 Aangepast profiel

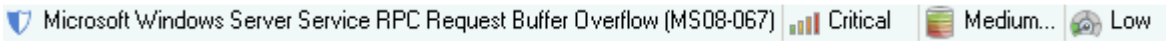
Je kan de Protection 'Host Port Scan' opzetten zodat de port scans van Nmap en Nessus wel worden gelogd.

Daarvoor zoek je bij Protections naar 'port scan'. Dan dubbelklik je op de 'Host Port Scan'. Je dubbelklikt in het venster dat verschijnt, op het profiel dat op dit moment van toepassing is. Je selecteert de optie 'Override IPS Policy with: Detect'.

Je krijgt dan volgende melding in de logs:

Figuur 4.11

Bij het profiel 'Recommended_Protection' staat volgende Protection voor MS08-067 automatisch op:



Figuur 4.12

Om te testen of de Conficker-aanval wordt tegengehouden, wordt even poort 445 open gezet. Anders kan de IPS-functie niet getest worden omdat alles sowieso tegenhouden zou worden.

Gelukkig wordt de Conficker-aanval tegengehouden door de IPS-functie. Tijdens het uittesten verschenen er echter meldingen van de Protection 'Microsoft Windows NT Null CIFS Sessions'. Als je die bescherming afzet dan wordt de Conficker aanval aangegeven door de protection 'MS-RPC over CIFS Inspection Properties'. Het wordt dus op verschillende manieren tegengehouden.

Dit tegenhouden gebeurde tijdens het onderzoek echter niet altijd rechtlijnig want als je vorige twee Protections afzet wordt hij soms tegengehouden door de Protection 'Microsoft Windows Server Service RPC Request Buffer Overrun (MS06-040)' en soms ook niet.

Het is echter heel verrassend dat de Protection, die 'Microsoft Windows Server Service RPC Request Buffer Overflow (MS08-067)' heet, helemaal niet de MS08-067 aanval

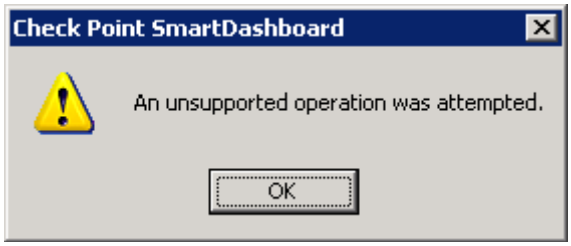
tegenhoudt! Ook niet als je de andere Protections afzet. Bij het testen is namelijk een remote shell kunnen geopend worden ook al stond de bewuste Protection op.

4.7.4 Besluit

Een goede netwerkbeheerder moet weten hoe hij zijn firewall moet instellen om zoveel mogelijk aanvallen te loggen en/of tegen te houden. Dat is eens te meer gebleken. De IPS-functie ziet er heel uitgebreid uit, maar is standaard niet ingesteld zodat het aanvallen kan ontdekken (default_protection). Dat dit de default configuratie is, valt wel te begrijpen omdat dit de firewall het minst belast. Maar er moet wel rekening mee gehouden worden door de netwerkbeheerder.

Na het onderzoek bleek dat de netwerkbeheerder ook zeker moet weten hoe hij port scan detectie moet opzetten. Bovendien moet hij zijn logs kunnen interpreteren zodat hij aanvallen tegen de MS08-067 vulnerability kan identificeren. Als hij denkt dat de Protection die speciaal gemaakt is voor MS08-067, ook beschermt tegen deze vulnerability komt hij er bedrogen uit!

Wat nog bijzonder is, is dat de GUI niet stabiel is bevonden tijdens deze test. Zo crashte de GUI soms. Bovendien verschenen er regelmatig rare foutmeldingen terwijl je gewone zaken instelt.



Figuur 4.13

4.8 Extra stap: Penetration test zonder de eerste firewall rule

De boosdoener, voor de hacker althans, is de eerste regel in de policy die alle connecties naar de firewall zelf blokkeert (zie 4.9.4 De uiteindelijke firewall policy). Als je die per ongeluk niet opzet of je zet toch een aantal management services open dan bekom je (met Nessus) een ander resultaat. Daarom wordt er nog eens een penetration test uitgevoerd op de firewall, waarbij de eerste regel uit de firewall policy werd gehaald.

4.8.1 Stap a: Scan met Nmap

Nmap geeft dezelfde output als bij het scannen van de firewall met de voorbeeldpolicy.

4.8.2 Stap b: Scan met Nessus

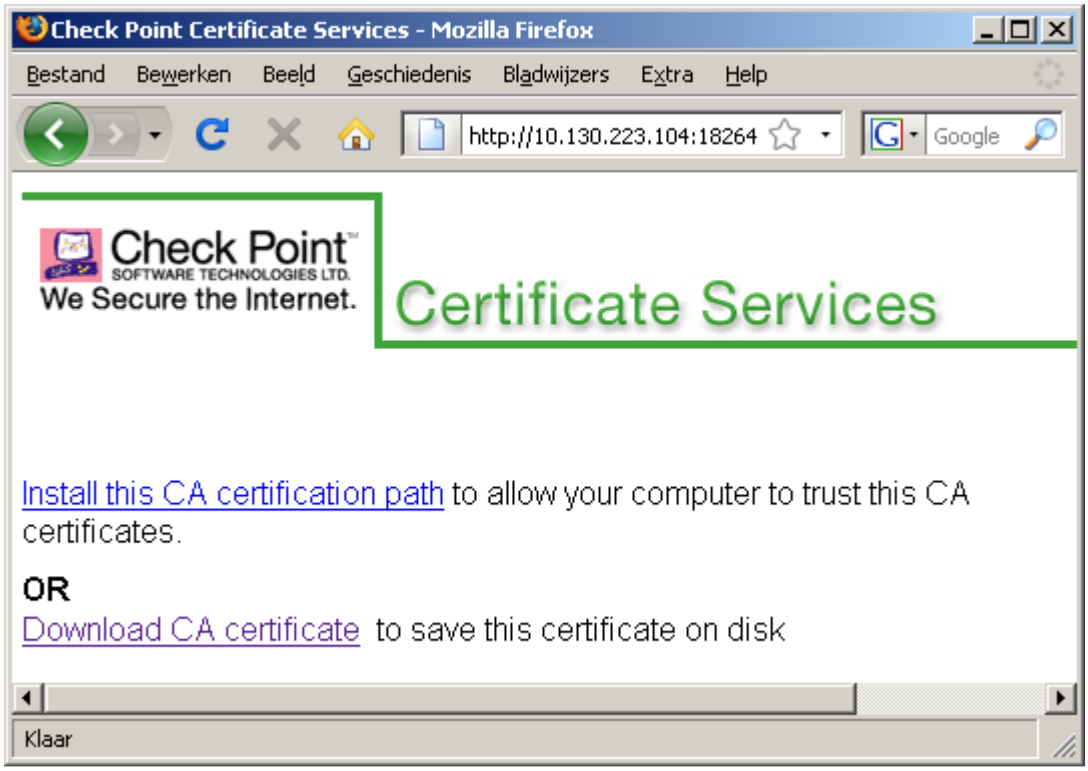
Nessus kan zo ingesteld worden (door met een IMCP ipv. een TCP scan te werken) dat het toch open poorten vindt.

Volgende open poorten worden ontdekt:

- checkpoint-ng-policy-editor (18190/tcp)
  - Uitleg Nessus: ‘There is an unknown service running on the remote host.’
- unknown (18264/tcp)
  - Uitleg Nessus: ‘The remote host is running Check Point FireWall-1 and is operating a web server on this port for its internal certificate authority

(ICA), which provides users with certificate revocation lists and registers users when using the Policy Server.
Note that it is not known whether it is possible to disable this service or limit its access to only certain interfaces or addresses.'

Nessus is dus te weten gekomen dat het een Check Point firewall is en dat die een webserver draait op poort 18264. Als je er naar surft bekom je volgende webpagina.



Figuur 4.14

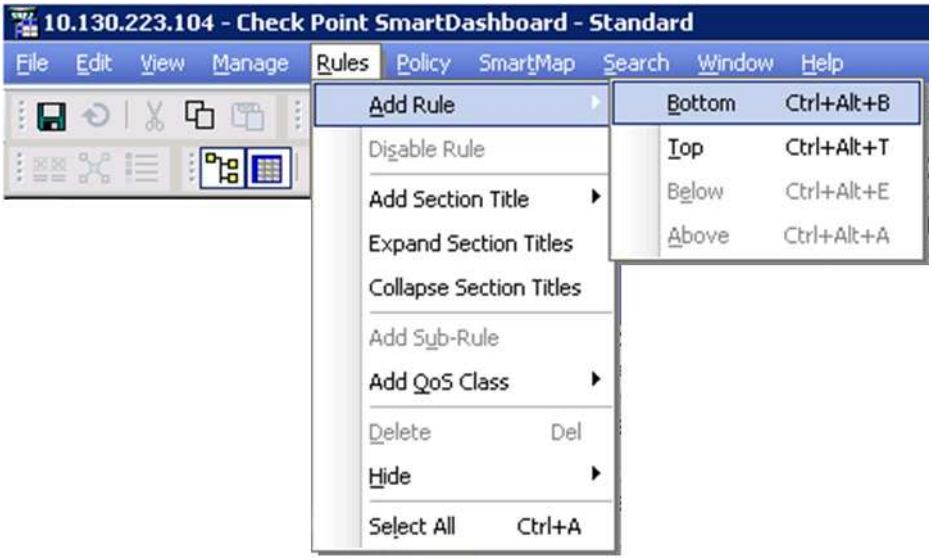
4.8.3 Besluit

Er zijn twee open poorten gevonden met Nessus, beide open poorten geven echter wel geen beveiligingsrisico. De hacker kan wel te weten komen dat hij te maken heeft met een Check Point firewall.

4.9 Voorbeeldpolicy toepassen

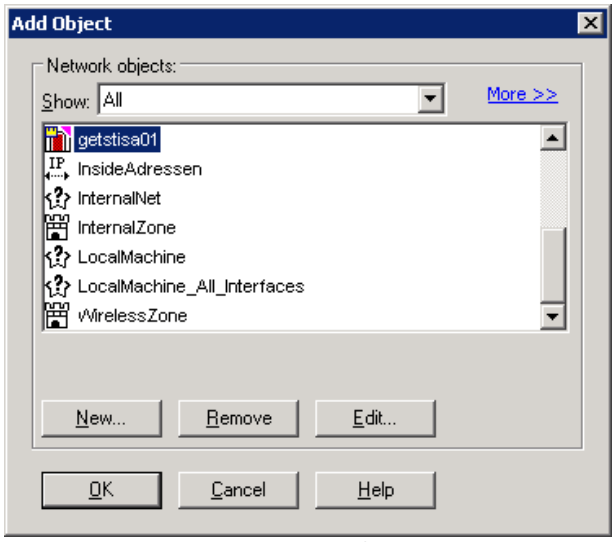
4.9.1 Een firewall rule toevoegen

Een regel toevoegen aan de policy doe je via Rules > Add Rule > Bottom of Top.



Figuur 4.15

Als je de source of destination wil veranderen dan klik je rechts in de juiste kolom van de nieuwe regel waarna je op Add klikt. Daar kan je een netwerk object kiezen (zie onderstaand figuur) om '* Any' te vervangen dat standaard in een nieuwe regel komt te staan.



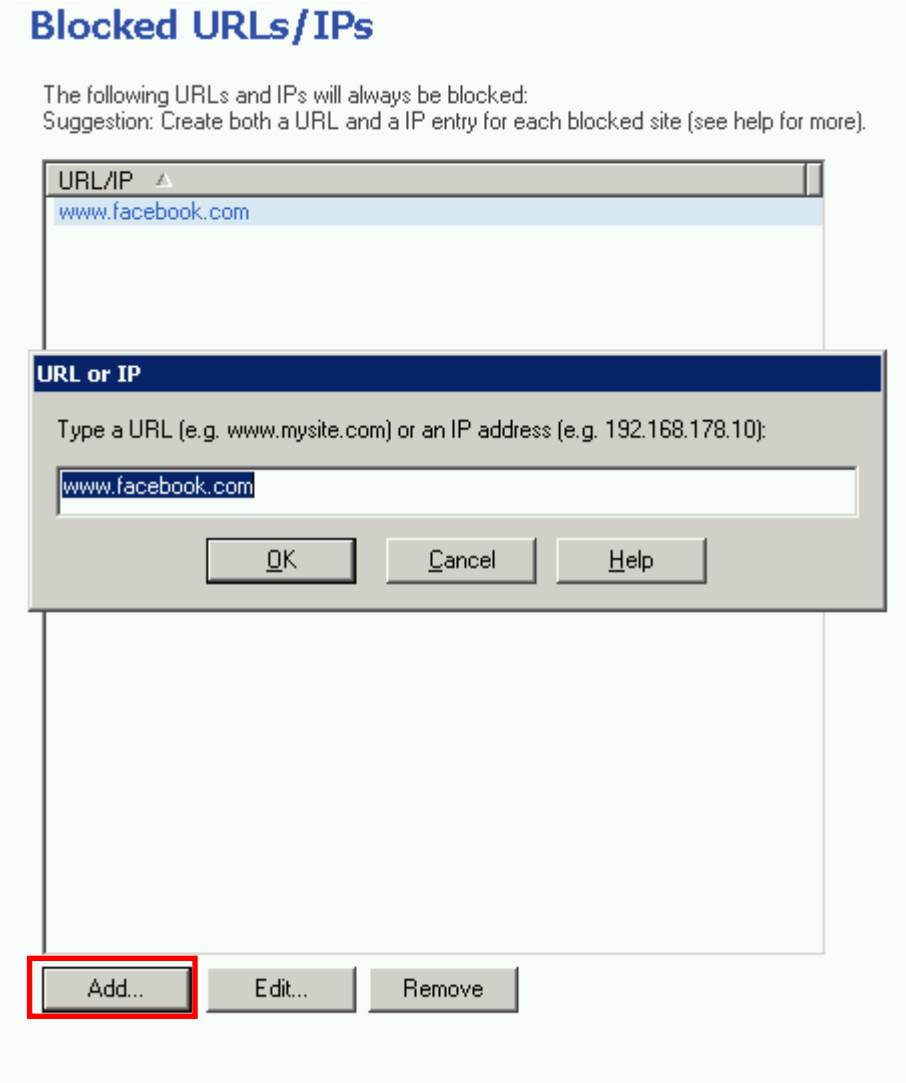
Figuur 4.16

Als je de aangemaakte rules ook daadwerkelijk wil toepassen op je firewall dan klik je op Policy > Install > OK > OK.

Dit toepassen of installeren van je aangepaste policy duurt spijtig genoeg wel lang. Je moet de policy ook installeren bij elke wijziging die je wil doorvoeren van NAT en IPS.

4.9.2 URL filtering

Daarvoor ga je naar het tablad 'Anti-Virus & URL Filtering'. Daar klik je verder op URL Filtering > URL Filtering Policy waar je moet zien dat de URL Filtering Policy aan staat en dat die toegepast (enforced) wordt op de gateway. Een gateway is de benaming van Check Point voor een firewall. Om nu een URL op te geven die geblokkeerd moet worden ga je naar Blocked URLs/IPs waar je op Add… klikt.



Figuur 4.17

4.9.3 Deep inspection

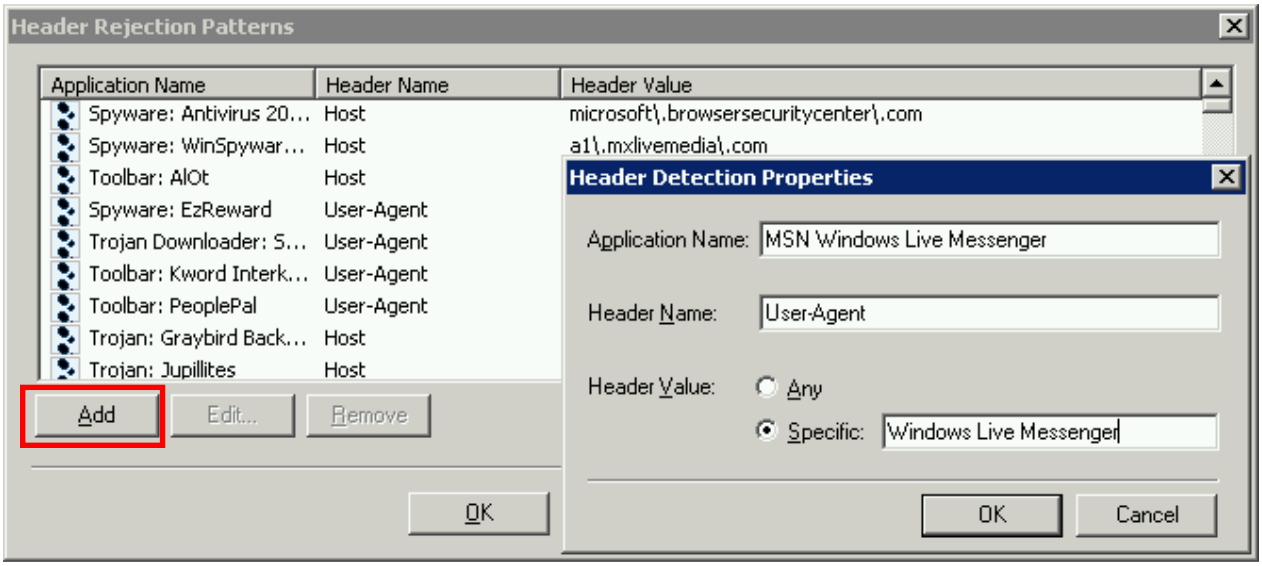
Na facebook.com te blokkeren komt zoals gewoonlijk het blokkeren van Windows (Live) Messenger.

In de Firewall-tab, waar je de policy kan aanpassen, kan je in een rule aangeven dat je MSN Messenger wil blokkeren. In de kolom waar je het protocol specificeert kan je een object toevoegen dat 'MSN_Messenger' heet. Zo'n regel toevoegen houdt Windows (Live) Messenger echter niet tegen dus ben je niets met die regel en moet er andere manier worden gezocht.

Die kan gezocht worden in het IPS-tabblad. Als je Protection kiest en dan zoekt op 'msn' dan kom je 8 regels tegen die elke een deel van MSN of een aanval tegen MSN tegenhouden. Na testen bleek dat geen enkele van die Protections Windows (Live) Messenger kon blokkeren. Zoals eerder al aangegeven werkt Windows Live Messenger anders dan zijn voorganger MSN Messenger waardoor waarschijnlijk het tegenhouden nog niet lukt.

Dan maar verder zoeken. Veel documentatie is er niet over te vinden maar er kan ook op eigen gedefinieerde signatures gefilterd worden. Dat wil zeggen dat alle HTTP-headers gaan gecontroleerd worden op bepaalde patronen.

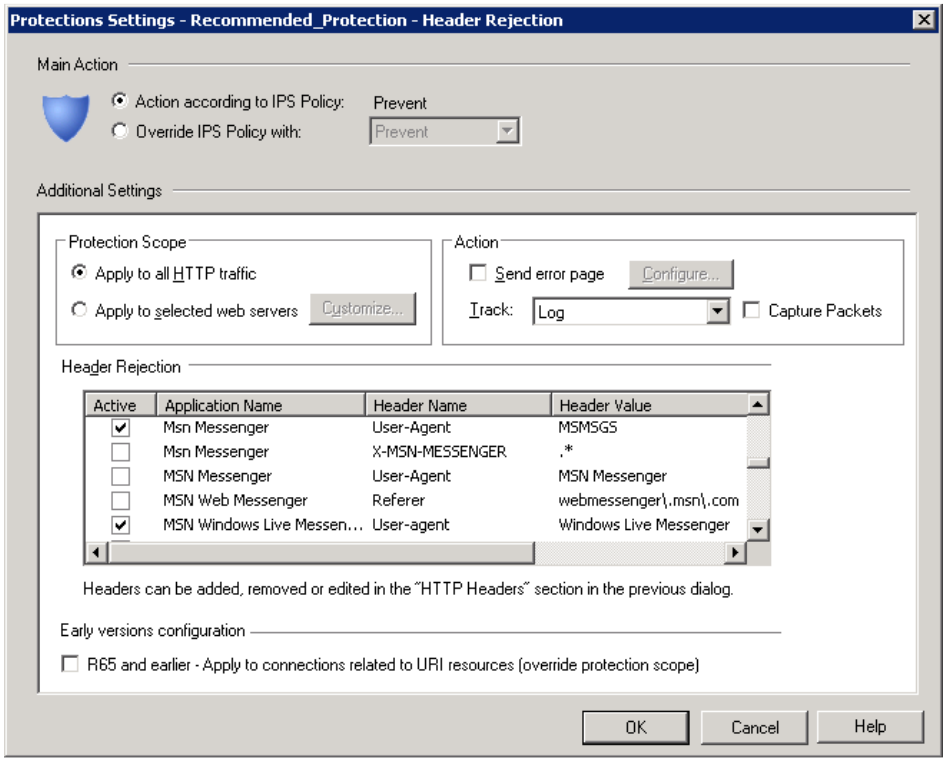
Daarvoor ga je in het tabblad IPS naar Protections. In het vakje om te zoeken typ je 'Header Rejection'. Op de enige 'Protection' die dan over blijft dubbelklik je zodat het 'Protection Details' venster opent. Daar klik je op 'Edit' en daarna op 'Add' zodat het 'Header Detection Properties' scherm te voorschijn komt. Daar vul je de gegevens in van onderstaande figuur. Klik daarna tweemaal op 'OK'.



Figuur 4.18

Je moet de nieuwe 'Header Rejection Patterns' oftwel signatures nog opzetten.

Daarvoor dubbelklik je in het 'Header Rejection' venster op het profiel dat op dit moment toegepast wordt.
In het groepsvak 'Protection Scope' kies je voor 'Apply to al HTTP traffic'. Vink daarna de signatures aan die je wil loggen of tegenhouden (zie onderstaand figuur). Vergeet achteraf ook niet de policy te installeren.



Figuur 4.19

4.9.4 De uiteindelijke firewall policy

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME
	Zelf aangemaakte regels (Rules 1-7)								
1	Alle connecties naar gateway	* Any	getstisa01	Any Traffic	* Any	drop	Log	Policy Targets	Any
2	RDP van admin pc naar intern	RemoteAdminPC	InsideAdressen	Any Traffic	Remote_Desktop	accept	Log	Policy Targets	Any
3	DNS van intern naar extern	InsideAdressen	* Any	Any Traffic	dns	accept	Log	Policy Targets	Any
4	HTTP(S) van intern naar extern	InsideAdressen	* Any	Any Traffic	http https	accept	Log	Policy Targets	Any
5	FTP van intern naar extern	InsideAdressen	* Any	Any Traffic	ftp	accept	Log	Policy Targets	Any
6	Ping van en naar overal	* Any	* Any	Any Traffic	icmp-proto	accept	Log	Policy Targets	Any
7	Standaard regel	* Any	* Any	Any Traffic	* Any	drop	Log	Policy Targets	Any

Figuur 4.20

Wat anders is bij Check Point dan bij ISA Server of Juniper firewalls is dat als je bij Check Point iets wil toelaten/tegenhouden van of naar het internet je '* Any' moet zetten in de policy. Alle mogelijke IP-adressen worden omvat door Any, bijvoorbeeld ook de interne adressen. Bij ISA en Juniper is dit bereik enger want het internet wordt daar omvat door de external (ISA) of untrust (Juniper) zone.
Wat heeft dit tot nu toe als gevolg voor deze standaard policy? Dat je een extra regel (de eerste regel) moet toevoegen die alle connecties naar de firewall zelf moet toe zetten (en loggen). Als die regel er niet bij zit dan kan er vanaf interne IP-adressen naar de firewall connecties gemaakt worden met DNS, HTTP(S), ICMP en FTP en dat is niet de bedoeling.

Er komen veel netbios-broadcasts toe op de firewall, vooral van de services nbdatagram en nbname, te zien in de log. Je kan facultatief nog een regel toevoegen die deze services toelaat maar niet logt. Dan blijft je log een beetje beknopter.

5 EINDVERGELIJKING

Een uitgebreid onderzoek zou niets zijn zonder samenvatting waarin alles nog eens op een rijtje wordt gezet. Hierin worden de meest opmerkelijke zaken herhaald samen met wat eigen mening van de auteur. Heb je geen zin om het hele werkstuk te lezen? Lees dan zeker deze eindvergelijking, en je bent helemaal mee…

5.1 ISA Server 2006

De eerste firewall in het lijstje is ISA Server 2006. Er bestaan veel vooroordelen over deze software die je op een Microsoft besturingssysteem moet installeren. De vooroordelen voor die besturingssystemen zijn gedeeltelijk correct. Dit is gebleken na onderzoek van een systeem met Windows XP en een met Windows Server 2003. Als er kennelijk geen beveiligingspatches worden geïnstalleerd zijn deze systemen zo lek als een zeef op vlak van beveiliging.

Na een uitgebreide evaluatie is gebleken dat de vooroordelen rond ISA Server volledig onterecht zijn omdat het een nagenoeg perfect rapport heeft op vlak van de beveiliging van de firewall zelf en van de interne systemen op het LAN. Een van de belangrijkste redenen hiervoor is dat ISA Server default het verkeer in alle richtingen potdicht zet. De netwerkbeheerder heeft dan zelf in de hand wat hij open zet en welke beveiligingsrisico's hij mogelijk daardoor in de hand werkt. Daarom is het ook sterk aan te raden om de ISA Server op een server te plaatsen die speciaal voorzien is om het te draaien zodat er geen onnodige poorten worden opengezet. Ga alstublieft dus geen ISA Server draaien op je domain controller!

De GUI van ISA Server 2006, die gebruik maakt van een soort tabs, is vergelijkbaar met die van Check Point, maar heeft een extra Microsoft-feel. De GUI van Check Point is echter nog een stuk overzichtelijker.

Op vlak van prijs is ISA Server 2006 klaarblijkelijk de gulden middenweg!

De IPS van ISA Server 2006 detecteert als enige firewall in de test de scans van Nmap, Nessus en Metasploit, zonder dat je daarvoor iets moet instellen. Dat is toch wel een groot pluspunt. Het kan echter nog een stuk beter als je het vergelijkt met Check Point die een heel uitgebreide IPS heeft. Wat Check Point en Juniper wel hebben en ISA niet is een manier om malafide software zoals worms en virussen tegen te houden. Er is geen anti-virus functionaliteit dus. Er bestaan extra software pakketten die deze leemte van ISA Server opvullen, zoals bijvoorbeeld GFI WebMonitor. Deze software is uitgetest en zeer gebruiksvriendelijk bevonden. Deze evaluatie is niet in het werkstuk opgenomen, om het beknopt en overzichtelijk te houden. Bij de nieuwe versie van ISA Server 2006, Forefront TMG genaamd, zal de IPS enorm uitgebreid zijn, naar het voorbeeld van Check Point. Van die nieuwe versie mag je dus zeker heel veel verwachten!

5.2 Juniper SSG 20

De Juniper firewalls staan in enorm veel netwerken verspreid over de wereld. Hun populariteit hebben ze voor een groot deel te danken aan hun prijs. Ze komen uit dit onderzoek als kampioenen op vlak van de prijs. Nog een voordeel is dat het heel gemakkelijk is om de configuratie (de 'config') op te slaan en later terug te laden op hetzelfde of een ander apparaat.

Ooit hadden ze een van de betere interfaces als je het vergeleek met de andere toenmalige firewalls die vooral met commando's werkten, zoals de Cisco PIX. De titel van 'beste interface' hebben ze tegenwoordig niet meer, verre van.

Het belangrijkste nadeel tegenwoordig van deze firewall is dan ook zijn gebruiksvriendelijkheid. De GUI is zonder meer onoverzichtelijk. Zo kan je bijvoorbeeld NAT op drie verschillende manieren en plaatsen instellen in de GUI, terwijl één plaats in de interface genoeg zou moeten zijn, kijk maar naar Check Point. De GUI is buitengewoon onoverzichtelijk op vlak van IPS (zie 3.7.4). Het feit dat de Juniper firewalls in het verleden in zo veel netwerken werden geïmplementeerd maakt dat er heel veel netwerkbeheerders zijn die deze GUI als het ware vanbuiten kennen. Voor hun is dit nadeel dan ook niet van toepassing.

Dit nadeel is ook niet van toepassing als de firewall bediend wordt met de CLI, omdat deze in vergelijking met andere CLI's op de markt, zoals die van Cisco, zeer goed in elkaar steekt.

Een ander nadeel is de default configuratie die een beetje gedateerd is. Doorheen de jaren heeft Juniper zijn default instellingen zo min mogelijk gewijzigd. Dit is handig voor de vele netwerkbeheerders die de firewalls kennen. Maar na verloop van tijd heeft het ook zijn nadelen.
Zo merk je dat default al het verkeer van het interne netwerk naar buiten mag. Vroeger werd zo'n configuratie vaak gebruikt waarbij de netwerkbeheerder moest opgeven welk verkeer *niet* naar buiten mocht. In huidige tijden van gesofisticeerde worms e.d. wordt vaak op een andere manier naar netwerkbeveiliging gekeken. Die manier houdt in dat alles default toe gezet wordt en dat de netwerkbeheerder dan de protocollen zelf moet open zetten die *wel* nodig zijn (HTTP, FTP …). Deze betere implementatie van de default configuratie vind je dan ook terug bij ISA Server en Check Point.

Door die instelling dat al het verkeer default naar buiten mag, hebben gebruikers geen restricties en kunnen worms gemakkelijk andere systemen op het internet besmetten. De meeste netwerkbeheerders weten echter ondertussen dat ze de regel die alles toelaat, moeten vervangen door een regel die alles dicht zet. Voor die netwerkbeheerders is dit nadeel dan ook niet van toepassing.

Nog een nadeel aan die default configuratie is dat van trust naar trust alles default wordt doorgelaten. Daardoor kan een worm die binnengeraakt alle systemen op het interne netwerk moeiteloos besmetten. De instelling om dit te wijzigen staat bovendien op een obscuur plekje in de GUI. Ervaren netwerkbeheerders weten deze instelling echter staan zodat ook dit nadeel niet van toepassing is op hen.

Nog een minpunt aan de GUI is dat niet alle functies erin terug te vinden zijn. De ervaren netwerkbeheerder weet echter blindelings hoe hij de CLI voor die functies moet bedienen.

Je leest het al, de grote conclusie is dat de Juniper firewall *de* perfecte (en veruit goedkoopste) oplossing is voor netwerkbeheerders die weten wat ze doen en die ervaring hebben met de firewall. Netwerkbeheerders zonder die ervaring kunnen gelukkig dit werkstuk lezen voor de juiste instellingen!

5.3 Check Point R70

De koning van alle firewalls is misschien wel de Check Point firewall. Het is echter ook de koning op vlak van prijs die torenhoog boven de rest uitsteekt.

Het belangrijkste voordeel is de interface. Zijn overzichtelijkheid is onovertroffen! Het duurde zeker de helft minder lang om de interface onder te knie te hebben, ten opzichte van de andere firewalls.

Wat zeer opmerkelijk is voor een 'koning der firewalls' is dat de GUI tijdens het onderzoek maar liefst 6 keer crashte! Rare foutmeldingen kwamen daar ook bij te pas.

Het valt echter moeilijk voor te stellen dat deze instabiliteit zich voordoet bij alle implementaties en alle versies van deze firewall.

Een nadeel is de naamgeving (zie 4.2.1). Marketing-gewijs zal het lanceren van weer een nieuwe flitsende naam zeer slim zijn, maar op vlak van duidelijkheid is dit niet slim. Als Check Point zich dan nog eens niet altijd aan de nieuwe namen houdt is de verwarring compleet. Een Check Point-kenner zal echter geen probleem hebben met deze naamgeving. Eens je de namen kent voor de verschillende functies (en de vroegere namen) is het dan ook niet meer moeilijk.

Een ander nadeel is dat elke verandering in de firewall policy e.d. moet toegepast worden. Dit toepassen of installeren van de policy op zich is niet het nadeel, maar wel het feit dat het tergend traag is. Als je veel verschillende instellingen wil testen (zoals in dit onderzoek gebeurd is) zal je die wachttijd snel beu zijn.

Opmerkelijk is dat Check Point evenals ISA Server en Juniper een voorgedefinieerd MSN-object heeft om de messenger van Microsoft tegen te houden. Geen enkele firewall kan daarmee echter Windows (Live) Messenger ook daadwerkelijk tegenhouden. Hiervoor moest telkens een nieuwe signature voor ingevoerd worden. Geen enkele firewall was op dat vlak goed gedocumenteerd.

De hardware firewalls hebben meestal als voordeel dat ze zelden stuk gaan. De hardware is dus meestal heel degelijk. Bij CIPAL is bijvoorbeeld, in de vele jaren dat ze Juniper al op grote schaal gebruiken, nog nooit een firewall stuk gegaan. Nog een voordeel is dat hardware firewall meestal op een besturingssysteem draait dat speciaal voor een firewall ontwikkeld is. Dat komt de veiligheid alleen maar ten goede.

Net zoals ISA Server is Check Point een software firewall. Dit heeft als grote voordeel dat de software regelmatig kan geüpdatet (in hoeverre dit wensbaar is voor het bedrijf natuurlijk) worden zonder dat de hardware moet vervangen worden. Bovendien zijn de GUI's van software firewalls vaak een stuk beter dan de hardware variant. Het is zeer aannemelijk dat software firewalls daarom in de toekomst alleen maar aan populariteit zullen winnen. Firewalls die echter de voordelen van de software en hardware firewalls combineren zijn het beste bewapend voor de toekomst. Voorbeelden hiervan zijn Check Point en Astaro Security Gateway. Het zijn software firewalls die je ook kan kopen met een eigen firewall-besturingssysteem en eigen hardware. De combinatie van een degelijke hardware firewall met een mooi ogende GUI vind je ook terug bij Juniper, tenminste als je gebruik maakt van NSM (Network and Security Manager). Dat is de software om een hele reeks van Juniper-firewalls te beheren in één interface. Die software voor firewalls centraal te beheren bevindt zich echter niet in de scope van dit onderzoek.

5.4 Samenvattingstabel

Opmerkingen bij de verschillende criteria:

- Prijs:
  - De eerste prijs van Check Point R70 is die van een systeem met een processor met één kern. De tweede prijs is die van één met twee kernen.
- Deep inspection, URL Filtering, Anti-virus en VPN:
  - Een kruisje of een vinkje geeft enkel aan of de firewall deze functionaliteit bezit. Er wordt geen rekening gehouden met de gebruiksvriendelijkheid van die functie.
- Anti-virus:
  - Bij ISA zie je dat die functionaliteit er niet in zit. Via externe software en met de volgende versie kan dit daarentegen wel bereikt worden.
- Interface:
  - Hierbij wordt in de eerste plaats gekeken naar de gebruiksvriendelijkheid.
- Algemene beveiliging:
  - Het is een criterium waarvan de uitslag bepaald wordt door de uitslag van de penetration tests. Daarin zit automatisch de hoeveelheid ontdekte vulnerabilities van de firewall in verwerkt omdat die effect hebben op de uitslag van de penetration tests.

Samenvattingstabel

	Prijs	Deep inspection	URL Filtering	VPN	Anti-virus	Interface	Default configuratie	IPS	Algemene beveiliging
ISA Server 2006	€ 2 874,43	✓	✓	✓	✗	✓ ✓	✓ ✓ ✓	✓ ✓	✓ ✓ ✓
Juniper SSG 20	€ 1 328,14	✓	✓	✓	✓	✓	✓	✓ ✓	✓ ✓ ✓
Check Point R70	€ 4 293,07/ € 9 253,39	✓	✓	✓	✓	✓ ✓ ✓	✓ ✓ ✓	✓ ✓ ✓	✓ ✓ ✓

BESLUIT

Bij de start van dit werkstuk werden volgende onderzoeksvragen gesteld:

1. Welke gaten treden op in de netwerkbeveiliging bij een implementatie van de firewall?
2. Gaat de firewall adequaat om met aanvallen?
3. Houdt de firewall een aanval van Conficker, de revolutionaire nieuwe worm, tegen?

Op de eerste vraag kan een, voor de firewalls, gunstig antwoord gegeven worden. De firewalls laten dus zo goed als geen gaten in de netwerkbeveiliging open! De uitgebreide penetration tests bij de verschillende configuraties bewijzen dat.

Het antwoord op de tweede vraag is wat minder gunstig voor de firewalls. Geen enkele firewall detecteerde aanvallen en scans, laat staan dat ze tegengehouden werden. ISA Server was hier echter een uitzondering op. De rest van de IPS-functionaliteit van ISA Server was echter wat pover (geen anti-virus of dergelijke).
De bescherming tegen aanvallen bij de Juniper SSG 20 was verre van adequaat. Dat kwam vooral omdat het niet gebruiksvriendelijk werkte zodat de juiste instellingen moeilijk te configureren zijn.

De laatste vraag heeft twee antwoorden. Het eerste antwoord is kort: ja! Alle firewalls hielden de worm tegen, zelfs bij de default configuratie. Dit kwam omdat ze de poort 445, die Conficker gebruikt, niet open zetten.
Maar er is een tweede antwoord, want de firewalls houden Conficker niet tegen als die poort wel open staat. Met een paar juiste instellingen, die je kan terugvinden in dit werkstuk, is dit vaak echter verholpen zodat Conficker wel tegen wordt gehouden.

Een rode draad door dit eindwerk was een wijsheid die zegt dat de firewalls zo goed zijn als hun netwerkbeheerder. Die moet namelijk weten wat hij doet. Bij het lezen van dit eindwerk weet hij dat hopelijk beter.

Ten slotte is mijn persoonlijk besluit dat ik ongelofelijk veel heb bijgeleerd bij de realisatie van mijn masterproef. Het heeft me bewapend met een arsenaal aan kennis rond netwerkbeveiliging waarvan ik ongetwijfeld de vruchten zal plukken tijdens mijn toekomstige carrière.

LITERATUURLIJST

[1] CIPAL . Wie is en wat doet CIPAL.

Gevonden op 19 augustus, 2009 op het internet: http://www.cipal.be/Default.aspx?tabid=316

[2] Scambray, J., McClure, S., .(2008). Hacking Exposed Windows: Windows Security Secrets & Solutions. McGraw-Hill.

[3] Northcutt, S., Zeltser, L., Winters, S., Kent, K., Ritchey, R., .(2005). Inside Network Perimeter Security. Sams Publishing.

[4] Cameron, R., .(2007). Configuring Juniper Networks Netscreen & Ssg Firewalls. Syngress.

[5] Gregg, M., .(2006). Certified Ethical Hacker Exam Prep. Pearson Certification

[6] Tenable Security . Limiting the Ports Probed by Nessus Scans.

Gevonden op 19 augustus, 2009 op het internet: http://blog.tenablesecurity.com/2006/09/limiting_the_po.html

[7] Howlett, T., .(2004). Open Source Security Tools - Practical Guide to Security Applications. Prentice Hall

[8] Wikipedia . Timeline of computer viruses and worms.

Gevonden op 19 augustus, 2009 op het internet: http://en.wikipedia.org/wiki/Timeline_of_notable_computer_viruses_and_worms

[9] Scambray, J., McClure, S., George, K., .(2008). Hacking Exposed: Network Security Secrets & Solutions. McGraw-Hill.

[10] Wikipedia . Sasser worm.

Gevonden op 19 augustus, 2009 op het internet: http://en.wikipedia.org/wiki/Sasser_worm

[11] Microsoft . Microsoft Security Bulletin MS08-067 – Critical.

Gevonden op 19 augustus, 2009 op het internet: http://www.microsoft.com/technet/security/bulletin/ms08-067.mspx

[12] Security.nl . Conficker gevaarlijkste worm afgelopen jaren.

Gevonden op 19 augustus, 2009 op het internet: http://www.security.nl/artikel/26877

[13] ZDNet . Kaspersky impressed by botnet slickness.

Gevonden op 19 augustus, 2009 op het internet: http://www.zdnet.com.au/news/security/soa/Kaspersky-impressed-by-botnet-slickness/0,130061744,339296562,00.htm

[14] Gibson Research Corporation . Security Now!.

Gevonden op 19 augustus, 2009 op het internet: http://www.grc.com/securitynow.htm

[15] Gibson Research Corporation . Port 445.

Gevonden op 19 augustus, 2009 op het internet: http://www.grc.com/port_445.htm

[16] NetSpert Security . microsoft-ds.

Gevonden op 19 augustus, 2009 op het internet: http://spert.net/security/port-details.php?port=445

[17] Windows IT Pro . How do I open port 445 for remote administration of Windows XP (SP2 or greater) with the Windows Firewall enabled?.

Gevonden op 19 augustus, 2009 op het internet: http://windowsitpro.com/article/articleid/80599/jsi-tip-7907-how-do-i-open-port-445-for-remote-administration-of-windows-xp-sp2-or-greater-with-the-windows-firewall-enabled.html

[18] Channel Web . Conficker E Variant Linked To Fake Antivirus Scams.

Gevonden op 19 augustus, 2009 op het internet: http://www.crn.com/security/216500299;jsessionid=VJGBDR5SNN2Y2QSNDLPCKH0CJUNN2JVN

[19] McAfee . Conficker Worm using Metasploit payload to spread.

Gevonden op 19 augustus, 2009 op het internet: http://www.avertlabs.com/research/blog/index.php/2009/01/15/conficker-worm-using-metasploit-payload-to-spread/

[20] SRI International . An Analysis of Conficker's Logic and Rendezvous Points.

Gevonden op 19 augustus, 2009 op het internet: http://mtc.sri.com/Conficker/

[21] The Honeynet Project . Conficker.A going down?.

Gevonden op 19 augustus, 2009 op het internet: https://honeynet.org/node/461

[22] Downadup Conficker Worm . Downadup Conficker Worm.

Gevonden op 19 augustus, 2009 op het internet: http://downadup-conficker.blogspot.com/

[23] Insecure.org . Options Summary.

Gevonden op 19 augustus, 2009 op het internet: http://nmap.org/book/man-briefoptions.html

[24] Insecure.org . Nmap Development: -PN reason, localhost isn't really responding.

Gevonden op 19 augustus, 2009 op het internet: http://seclists.org/nmap-dev/2008/q3/0188.html

[25] Wikipedia . Intrusion detection system.

Gevonden op 19 augustus, 2009 op het internet: http://en.wikipedia.org/wiki/Intrusion_detection_system

[26] Henmi, A., .(2006). Firewall Policies and VPN Configurations. Syngress.

[27] Microsoft . ISA Server 2006 Pricing and Licensing.

Gevonden op 19 augustus, 2009 op het internet:
http://www.microsoft.com/forefront/edgesecurity/isaserver/en/us/pricing-licensing.aspx

[28] Softpedia . Windows vs. Linux vs. Reliability.

Gevonden op 19 augustus, 2009 op het internet:
http://news.softpedia.com/news/Windows-vs-Linux-vs-reliability-25859.shtml

[29] IAPS . 2008 Server OS Reliability Survey.

Gevonden op 19 augustus, 2009 op het internet:
http://www.iaps.com/2008-server-reliability-survey.html

[30] I Get Off Microsoft . Research on Linux vs. Windows: For What It's Worth.

Gevonden op 19 augustus, 2009 op het internet:
http://www.tonybove.com/getoffmicrosoft/blog/?p=38

[31] ISAServer.org . What's new in Forefront TMG Beta 2 (Part 1).

Gevonden op 19 augustus, 2009 op het internet:
http://www.isaserver.org/tutorials/Whats-new-Forefront-TMG-Beta-2-Part1.html

[32] Microsoft TechNet . Troubleshooting Firewall Clients in ISA Server 2004.

Gevonden op 19 augustus, 2009 op het internet:
http://technet.microsoft.com/en-us/library/cc302546.aspx

[33] Wikipedia . Port scanner.

Gevonden op 19 augustus, 2009 op het internet:
http://en.wikipedia.org/wiki/Port_scanner

[34] Henmi, A., .(2008). Microsoft ISA Server 2006 Unleashed. Sams Publishing.

[35] Juniper . SSG20.

Gevonden op 19 augustus, 2009 op het internet:
http://www.juniper.net/us/en/products-services/security/ssg-series/ssg20/

[36] Behrens, T., .(2007). The Best Damn Firewall Book Period. Syngress.

[37] .(2008). ScreenOS Reference Guide. Juniper Networks.

[38] Check Point . Check Point Software Technologies Price List.

Gevonden op 19 augustus, 2009 op het internet:
https://pricelist.checkpoint.com/pricelist/US/PLUSswblades/SWBlist.jsp

[39] Wikipedia . Check Point VPN-1.

Gevonden op 19 augustus, 2009 op het internet:
http://en.wikipedia.org/wiki/Check_Point_VPN-1