

Gebruiksvriendelijke open source oplossingen voor netwerkbeveiliging

Gerben Dierick & Pieter Geens
Katholieke Hogeschool Leuven

`gerben.dierick@khleuven.be`

`pieter.geens@khleuven.be`

REN - Thema Beveiliging

1 Inleiding

In deze vergelijking beschouwen we 3 verschillende Linux-distributies die kunnen helpen bij het afschermen van je netwerk: IPCop, CensorNet en eBox. Ze kunnen alledrie dienst doen als firewall, maar de overige beschikbare functies zijn niet dezelfde. De verschillen zijn een gevolg van een andere doelstelling van het project.

Deze tekst heeft niet tot doel om de distributies kwalitatief te beoordelen. De drie producten doen wat ze beloven en zijn voldoende configureerbaar en gebruiksvriendelijk. Ook hun installatie- en gebruikershandleidingen zijn voldoende duidelijk. Deze tekst is bedoeld om te helpen bij het kiezen van het meest geschikte product door de verschillen in aanpak tussen de distributies aan te geven.

Voor deze platformen zijn nog distributies zijn nog talrijke alternatieven, zoals vaak bij vrije software. We vonden de gekozen platformen geschikt wat betreft gebruiksvriendelijkheid en functionaliteit, maar dat wil niet zeggen dat dit niet geldt voor andere distributies.

IPCop en eBox laten toe dat vrijwilligers extra modules ontwikkelen. In deze vergelijking beschouwen we alleen functionaliteit in het standaard-pakket, maar als je vindt dat een bepaalde functie ontbreekt kan je best nagaan of er geen externe module beschikbaar is voor het platform van je keuze.

Als de handleidingen van deze producten niet voldoende blijken of als er andere vragen zijn kan je altijd contact opgenomen via `gerben.dierick@khleuven.be`.

1.1 CensorNet

Volgens hun website is CensorNet “the world’s favourite open source Internet Web Filtering & Management solution for Enterprise, Education and Personal use”. De nadruk bij de ontwikkeling van CensorNet ligt duidelijk op het afschermen van gebruikers van ongeoorloofd geacht materiaal op het internet.

CensorNet wordt ontwikkeld door Adelix, een Engels software-bedrijf. Een basisversie is beschikbaar onder de GPL, maar enkele extra modules en diensten zijn betalend. De functionaliteit in de basisversie is echter voldoende uitgebreid voor de meeste toepassingen.

<http://www.censornet.com>



1.2 eBox Platform



Het eBox-platform wil een alles-in-één oplossing zijn voor een klein netwerk. Naast een firewall en proxy bevat het o.a. ook een mail en file server. Als deze diensten al aanwezig zijn in een organisatie is eBox waarschijnlijk niet de beste keuze. Als men ook interesse heeft in deze extra diensten kan het een voordeel zijn dat ze in één systeem op te zetten zijn.

eBox wordt ontwikkeld door het Spaanse Warp Networks. Het is een volledig vrij beschikbaar, maar Warp Networks biedt gegarandeerde ondersteuning tegen betaling.

<http://www.ebox-platform.org>

1.3 IPCop

De IPCop slogan “The bad packets stop here!” toont aan dat deze distributie in de eerste plaats een netwerk wil beschermen. Het is een firewall met enkele extra functies.

IPCop wordt ontwikkeld door een ploeg van vrijwilligers. Ze weigeren zelfs financiële bijdragen als ondersteuning.



Individuele leden van het team mogen eventueel wel betaald worden voor ontwikkelingswerk.

<http://www.ipcop.org>

2 Opstelling

Een firewall zal het netwerk in minstens 2 delen verdelen: een intern en een extern netwerk. Daarom worden 2 netwerkkaarten voorzien.

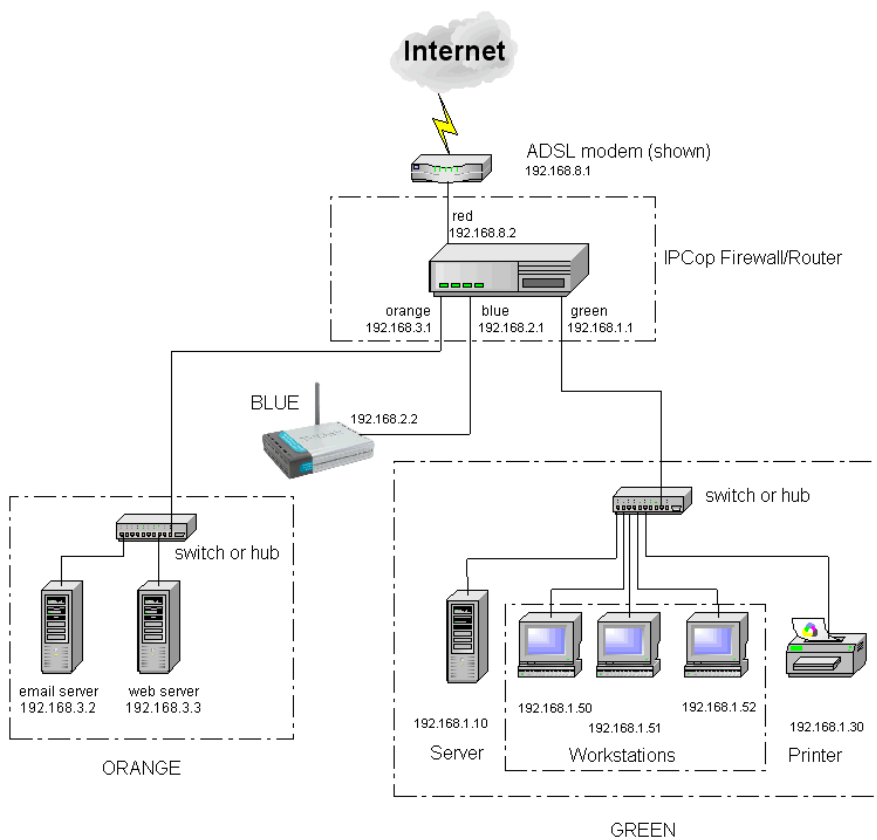
Het extern netwerk komt overeen met het internet, en het intern netwerk omvat alle computers die door de firewall van het internet afgeschermd worden. IPCop gebruikt kleuren om de netwerken aan te duiden. Het rode netwerk (RED) is het externe netwerk of het internet en het groene netwerk (GREEN) is het interne netwerk. CensorNet, IPCop en eBox kunnen deze onderverdeling in 2 maken.

Het doel van een firewall is in de eerste plaats om het groene netwerk te beschermen tegen aanvallen uit het rode netwerk. Daarnaast kan ook verhinderd worden dat gebruikers in het groene netwerk bepaalde acties ondernemen op het rode netwerk, m.a.w. hun mogelijkheden op het internet kunnen ingeperkt worden.

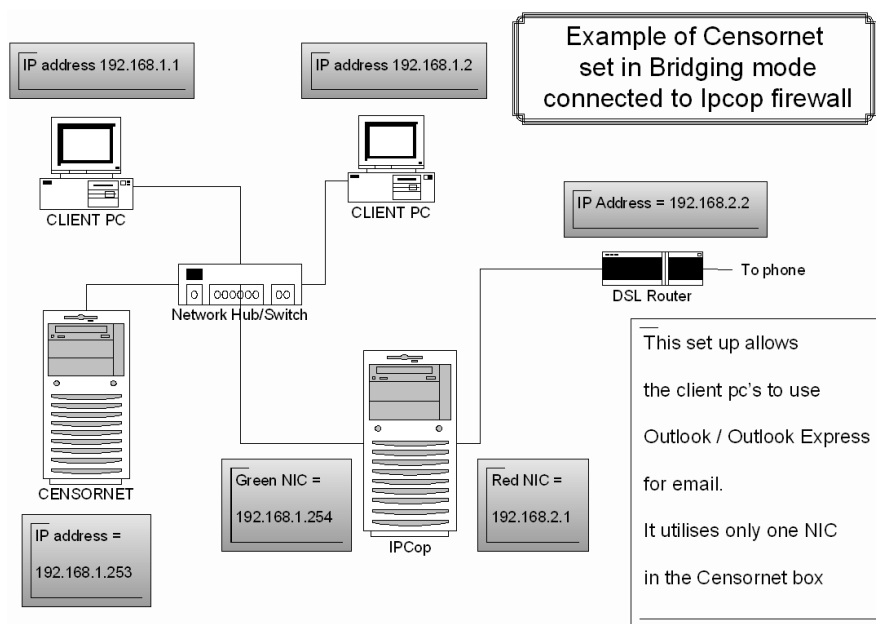
In figuur 1 zien we dat het bij IPCop mogelijk is om twee extra netwerken te voorzien. Het oranje netwerk (ORANGE) is een zogenaamde De-Militarize Zone (DMZ). Dit betekent dat de regels voor dit netwerk minder streng zijn dan voor het groene. Computers in het rode netwerk kunnen toegang krijgen tot bepaalde diensten in het oranje netwerk. Servers die vanop het internet toegankelijk moeten zijn worden in de DMZ geplaatst. De DMZ dient dan om te verhinderen dat een aanvaller die toegang verkrijgt op een server volledige toegang heeft tot het interne netwerk.

Het blauwe netwerk (BLUE) is een netwerk dat gebruikt kan worden als er voor een deel van het netwerk andere regels moeten bestaan. In het figuur 1 wordt het blauwe netwerk gebruikt voor een draadloos netwerk.

Figuur 2 laat zien dat de voorgestelde producten eventueel samen gebruikt kunnen worden. Hier wordt IPCop als firewall gebruikt, en CensorNet wordt geconfigureerd in zogenaamde "bridge mode". Je kan dan CensorNet b.v. als web proxy verplichten, om zo de CensorNet-filters te gebruiken.



Figuur 1: IPCop Voorbeeldnetwerk (van www.ipcop.org)



Figuur 2: IPCop Firewall met CensorNet filter (van www.censornet.com)

3 Kenmerken

3.1 Installatie

Censornet en IPCop worden verdeeld als CD images. Na het downloaden kan een opstart-CD gebrand worden waarmee het systeem geïnstalleerd kan worden op een leeg computersysteem. Ook eBox is op deze manier beschikbaar, maar er is een andere mogelijkheid. EBox kan via apt-get geïnstalleerd worden op een eerder opgezet Debian GNU/Linux-systeem.

De installatie van de systemen is relatief eenvoudig. Voor de drie systemen is een installatiehandleiding voorzien. De handleiding van IPCop is het meest uitgebreid. Men moet wel voorzichtig zijn met erg recente hardware die nog niet ondersteund wordt door de gebruikte Linux-kernels.

De installatie-procedure gebeurt in een ouderwets aandoende text-interface met enkele menu's. Laat je hierdoor niet afschrikken. Dit gebeurt om zo weinig mogelijk vereisten te stellen aan de hardware waarop het systeem geïnstalleerd wordt. Na de installatie gebeurt het beheer d.m.v. een web-interface vanop een andere PC. Het zou jammer zijn als je firewall over een zwaardere grafische kaart of meer geheugen moet beschikken, enkel voor de installatie-procedure.

Voor meer info over de vereiste hardware, zie verder.

3.2 Gebruikersinterface

De pakketten maken alledrie gebruik van een web-interface voor een eenvoudige bediening. De CensorNet interface is (nog?) niet in het Nederlands beschikbaar.

	CensorNet	eBox	IPCop
Web-interface	x	x	x
Nederlandstalig		x	x

3.3 Firewall

Uiteraard beschikken alle systemen over een firewall om het interne netwerk af te schermen van het internet. IPCop ondersteunt daarnaast nog een derde en vierde netwerkkaart. Hierdoor is het mogelijk een DMZ te voorzien voor servers die vanop het internet bereikbaar moeten zijn, en een extra netwerk om bv. draadloze apparaten in een afzonderlijk netwerk onder te brengen.

In de drie firewalls ondersteunen port forwarding. Verkeer dat aankomt op een poort op de internet-interface wordt doorgelaten naar een interne machine. Dit laat toe om een server op een interne machine vanop het internet bereikbaar te maken. Een dergelijke server loopt het risico om aangevallen te worden vanop het internet. Als iemand de controle over een dergelijke machine verwerft, heeft hij toegang tot het volledige interne netwerk.

De gevolgen van een dergelijke inbraak zijn minder groot als de server in een aparte netwerkzone staat. Zo'n DMZ verhindert dat de server toegang heeft tot computers in het interne netwerk. Zoals gezegd is dit enkel standaard ondersteund bij IPCop.

Hetzelfde geldt voor bv. een draadloos netwerk. Hier is het risico op indringers groter omdat het netwerk niet overal beperkt blijft tot het gebouw. Door dit af te zonderen op een aparte netwerkkaart van de firewall kunnen er regels opgelegd worden.

	CensorNet	eBox	IPCop
Packet filter	x	x	x
Port forwarding	x	x	x
DMZ interface			x
Extra netwerk-interface			x

3.4 Proxy server

Een caching proxy met de mogelijkheid om webverkeer te filteren is aanwezig in de drie producten. De performantiewinst door het cachen van webverkeer is niet meer zo groot door de opkomst van dynamische webpagina's. Filteren is echter zeer relevant voor deze producten.

Filteren op inhoud en op basis van een zwarte lijst van websites is in de drie gevallen mogelijk. CensorNet biedt echter duidelijk het meeste flexibiliteit bij het instellen van de filters. De filterinstellingen kunnen per computer of per gebruiker aangepast worden. Niet alle mogelijkheden zijn weergegeven in deze tabel.

	CensorNet	eBox	IPCop
HTTP Proxy	x	x	x
FTP Proxy		x	
Caching	x	x	x
Uitzonderingen	x		
Filter op inhoud	x	x	x
Filter op bestandstype		x	
Zwarte lijst	x	x	x
Witte lijst	x		

3.5 Netwerkbeheer

De drie producten bevatten een DHCP-server voor het toekennen van IP-adressen en instellen van de default gateway en DNS-servers in het intern netwerk. IPCop en eBox bieden nog meer hulpmiddelen bij het netwerkbeheer, die CensorNet niet biedt.

Als je internetverbinding gebruik maakt van een dynamisch IP-adres kan je dankzij Dynamic DNS zorgen dat je domeinnaam aan het juiste IP-adres gekoppeld blijft, ook als het adres verandert. eBox en IPCop bevatten een DynDNS client die de koppeling automatisch aanpast.

Het Network Time Protocol laat toe om de klok van een computer te synchroniseren met de tijd op een NTP-server.

VLANs of virtuele LANs laten toe om op één switch poorten toe te kennen aan verschillende virtuele LANs. Alleen poorten die in dezelfde VLAN zitten kunnen met mekaar communiceren. Het is alsof je je switch verdeelt in verschillende switches. Als je toch verkeer wil toelaten tussen de verschillende VLANs kan dat via de firewall/router, en kan je aan dit verkeer beperkingen opleggen. Op een switch zonder VLANs kunnen alle aangesloten apparaten zowiezo volledig

met mekaar communiceren. Jammer genoeg zijn VLANs enkel beschikbaar op duurdere switches.

eBox kan als enige geconfigureerd worden als Domain Name Server, zodat je domeinnamen kan gebruiken.

	CensorNet	eBox	IPCop
DHCP	x	x	x
DNS server		x	
Dynamic DNS client		x	x
NTP		x	x
VLANs		x	x
VPN		x	x
Autom. inventarisatie	x		

3.6 Bandbreedtecontrole

Als je organisatie over beperkte bandbreedte beschikt, of je vindt dat leerlingen de bandbreedte misbruiken, kan je deze beperken. CensorNet laat ook toe dit per gebruiker te doen, IPCop en eBox ondersteunen enkel algemene bandbreedtecontrole.

	CensorNet	eBox	IPCop
Traffic shaping	x	x	x
Per gebruiker	x		

3.7 Bijkomende mogelijkheden

Voorals eBox biedt naast de firewall functionaliteiten een aantal extra diensten zoals een file en print server, LDAP server en e-mail en instant messaging. IPCop laat toe om het Snort Intrusion Detection System te gebruiken om het netwerk te bewaken.

	CensorNet	eBox	IPCop
File server		x	
LDAP		x	
Printserver		x	
E-mail		x	
Instant messaging		x	
Intrusion detecti			x

3.8 Systeemvereisten

IPCop vermeldt als enige expliciet minimale systeemvereisten, maar die zijn erg laag. Volgens de installatiehandleiding neemt IPCop genoegen met een 386 processor, 32 MB werkgeheugen en een harde schijf van 300MB. Je hebt minimaal 2 netwerkkaarten nodig, 3 als je een DMZ gaat gebruiken. Deze minimale vereisten voldoen voor een firewall, maar als je gebruik gaat maken van het Intrusion Detecion Systeem of de caching proxy heb je waarschijnlijk meer geheugen en rekenkracht nodig.

	CensorNet	eBox	IPCop
Processor	?	?	386
Geheugen	?	?	32MB
Harde schijf	?	?	300MB
Netwerkkaarten	?	?	2+

Voor beide andere systemen liggen de basisvereisten waarschijnlijk iets hoger dan bij IPCop, maar nog altijd erg laag. Ze laten zeker toe het systeem te installeren op oude hardware.

De manier van gebruik van het systeem beïnvloedt de minimale vereisten. Zoals gezegd komt de performantie van IPCop in het gedrang bij het gebruik van een functie als intrusion detection op de minimaal vereiste hardware. Hetzelfde geldt voor b.v. eBox. Je hebt niet veel schijfruimte nodig om het systeem te installeren, maar als je het als bestandserver wil gebruiken moet je natuurlijk een grotere harde schijf voorzien.

Een ander voorbeeld is de betalende Active Image Control module van CensorNet. Deze module controleert afbeeldingen op het moment dat ze gedownload worden. Dit vereist natuurlijk de nodige rekenkracht, in dit geval minstens een 1GHz processor.

De lage systeemvereisten van deze distributies laten toe om oude hardware te gebruiken. Dit kan, maar je mag niet vergeten dat al je netwerkverkeer door dit systeem loopt. Als het uitvalt, wordt je netwerk grotendeels onbruikbaar. Als je toch oude (elders afgedankte) hardware gebruikt, kan je eventueel een zogenaamde "cold spare" voorzien, een tweede systeem dat geïnstalleerd klaarstaat en enkel ingeschakeld moet worden om het andere te vervangen. Als je dan regelmatig de configuratie bewaart, is je netwerk binnen enkele minuten weer bruikbaar.

4 Conclusie

Uit de voorgaande vergelijking blijkt dat de 3 besproken producten ieder een eigen accent leggen. CensorNet is in de eerste plaats bedoeld om de internet-toegang te beperken op basis van de gebruiker, de computer, het tijdstip of de inhoud van de communicatie. EBox streeft ernaar een volledige oplossing te zijn voor het netwerk een relatief kleine organisatie, met alle benodigde diensten. En IPCop richt zich sterk op het firewall-aspect, met bv. extra netwerkzones.

Voor een school die al beschikt over een domeincontroller en fileserver is eBox waarschijnlijk minder interessant. Als je een firewall zoekt, maar niet veel belang hecht aan het beperken van de mogelijkheden van de gebruikers is IPCop een logischere keuze dan CensorNet, maar het omgekeerde is ook mogelijk. Zoals reeds aangehaald kan je de systemen ook combineren.