



iTables

Een handleiding voor gebruikers.

iTables: gebruikershandleiding

Inhoudsopgave

1	Blok 1: Algemene informatie	1
1.1	Inleiding	1
1.2	Wat is iTables?	3
1.3	Ondersteunde browsers	3
2	Blok 2: Basiskennis.....	3
2.1	Wat is een firewall configuratie?	3
2.2	Wat zijn tables en chains?	5
2.3	Starten met een configuratie.....	6
3	Blok 3: De analyse	7
3.1	Vinden van policy conflicten	7
3.2	Oplossen van policy conflicten.....	10
3.3	Wijzigen van firewall regels	11
3.4	Zoeken naar redundante (overbodige) regels	12
3.5	Opsomming van een segment opvragen	14
4	Blok 4: De pagina met firewall regels.....	15
4.1	Toevoegen van een regel	15
4.2	Bepaal matchende regel.....	16
5	Blok 5: Overige	17
5.1	Logboek bekijken	17
5.2	Downloaden en laden van een (evt. gewijzigde) iptables configuratie..	17
5.3	Exporteren van de resultaten van de sessie	18
5.4	Beëindigen van een sessie (bv. als men met een andere firewall configuratie wil werken).....	19
5.5	Hoe maak ik een configuratie in iptables	19

1 Blok 1: Algemene informatie

1.1 Inleiding

iTables is een tool om firewall-configuraties te analyseren (althans een aantal aspecten daarvan) en deze aan te passen.

iTables is ontwikkeld als bachelor afstudeeropdracht van de Open Universiteit. De ontwikkelaars zijn Thomas Van Poucke, Ron Melger en Joël Craenhals.

Dit document is een handleiding voor iTables.

Dezelfde handleiding is ook te vinden op de iTables website zelf. Op de website staan de paragrafen als uitklapbare secties. Doorheen de website staan links naar specifieke gedeelten van deze handleiding.

Bij het klikken op zo'n link krijgt de gebruiker enkel de relevante sectie te zien.

Daarom is elke paragraaf in dit document zoveel mogelijk geschreven als een losstaand geheel. De paragrafen zijn verdeeld over 5 blokken.

Paragraaf 1.2 legt kort uit wat iTables is.

De iTables website is op verschillende browsers getest. Paragraaf 1.3 beschrijft welke browsers ondersteund worden.

Blok 2 bevat de basiskennis die nodig is om te kunnen werken met iTables. In paragraaf 2.1 staat de noodzakelijke kennis over firewall-configuraties. iTables werkt met iptables configuraties. iptables kent verschillende tables en chains, en ook om te kunnen werken met iTables is deze kennis nodig. In paragraaf 2.2 staat hier informatie over.

In paragraaf 2.3 wordt tenslotte beschreven wat een gebruiker moet doen om een configuratie te starten. Daarbij kan een gebruiker kiezen om met een lege configuratie te starten, zelf een iptables configuratie te uploaden, of één van de voorbeeldconfiguraties te kiezen.

Blok 3 gaat over de analyse.

Paragraaf 3.1 is daarbij belangrijk om de overige paragrafen van deze blok te begrijpen. Deze paragraaf bevat een beschrijving van de nodige begrippen (segment, correlatiegroepen en policy conflicten) en hoe deze gepresenteerd worden in iTables.

Paragraaf 3.2 beschrijft daarna hoe deze policy conflicten in iTables opgelost kunnen worden naargelang bepaalde voorkeursacties.

Paragraaf 3.3 is een korte beschrijving hoe men ook op de pagina met de analyse de firewall regels kan wijzigen. Dit heeft niets te maken met de analyse zelf maar is in deze blok gezet omdat in deze blok de gebruiker rondgeleid wordt in de pagina met de analyse.

In paragraaf 3.4 staat hoe redundante (=overbodige) regels gevonden kunnen worden en in paragraaf 3.5 staat hoe men de inhoud van een segment kan opsommen.

Blok 4 gaat over de pagina met firewall regels. Paragraaf 4.1 beschrijft hoe regels toegevoegd moeten worden aan de configuratie – dit gebeurt zoals men zou verwachten door een knop om een regel toe te voegen.

Op de pagina met firewall regels staat ook een formulier waarin men de waarden van een virtueel netwerkpakket kan invoeren. De gebruiker krijgt dan terug bij welke regel het virtueel netwerkpakketje zou matchen. Dit staat uitgelegd in paragraaf 4.2.

In blok 5 staan de zaken die niet aan bod zijn gekomen in de overige blokken.

Paragraaf 5.1 legt uit hoe men het logboek moet bekijken.

Men kan op elk gewenst moment de configuratie terug inladen in een iptables firewall. Paragraaf 5.2 legt uit hoe.

In paragraaf 5.3 staat kort hoe een rapport kan gedownload worden van de sessie. Paragraaf 5.4 beschrijft hoe een sessie beëindigd kan worden.

Paragraaf 5.5 gaat niet over iTables zelf maar over de firewall iptables. Er wordt beschreven hoe men een configuratie aanmaakt in iptables, en welke functies van iptables ondersteund worden.

1.2 Wat is iTables?

Iptables is een firewall in Linux. Iptables is beschikbaar op Linux vanaf kernel versie 2.2 .

iTables is een tool om firewall configuraties te analyseren. Daarbij is het mogelijk zelf iptables configuratie te uploaden.

Achteraf kan de evt. gewijzigde configuratie terug geladen worden in iptables.

1.3 Ondersteunde browsers

Ondersteunde browsers:

Browser	Vanaf versie
Internet Explorer	9
Firefox	4
Chrome	14

Voor een optimale gebruikerservaring raden wij de laatste versie van Internet Explorer, Firefox of Chrome aan. Bij gebruik van Firefox is de weergave iets minder netjes als de bladwijzers open blijven staan, maar het werkt wel gewoon.

Javascript moet ingeschakeld zijn.

2 Blok 2: Basiskennis

2.1 Wat is een firewall configuratie?

Een firewall configuratie bepaalt of een pakket doorgelaten moet worden of niet. Dit gebeurt op basis van een aantal firewall regels.

Een firewall configuratie ziet er als volgt uit:

#▲	Protocol ↕	Bron IP ↕	Bronpoort ↕	Doel IP ↕	Doelpoort ↕	Actie ↕	
1	TCP	10.1.2.0/24	*	192.168.0.0/16	25	drop	🗑️
2	TCP	192.168.0.0/16	16015	173.252.110.27/32	80	accept	🗑️
3	*	10.2.0.0/16		192.168.0.0/16		drop	🗑️
4	TCP	10.2.54.0/24	1543	192.168.5.0/24	80	accept	🗑️
5	UDP	10.1.2.88/32	*	192.168.0.0/16	*	drop	🗑️

Elk netwerk pakket dat arriveert op de firewall heeft volgende informatie:

- Het IP adres van de zender

- Het IP adres van de bestemming
- Het protocol
- De poort van de zender (indien protocol TCP of UDP)
- De poort van de bestemming (indien protocol TCP of UDP)

Een firewall regel bevat volgende informatie:

- Een IP patroon voor de verzender. Deze is van de vorm a.b.c.d/e. Een IP adres bestaat eigenlijk uit $32=8*4$ bits. Dus 8 bits per getal. Het getal e geeft aan hoeveel van de eerste bits overeen moeten komen met het netwerk pakket. Bijvoorbeeld als het IP patroon 54.0.0.0/8 is zal elk IP adres dat begint met het getal 54 overeenkomen.
- Een IP patroon voor de bestemming. Deze is van de zelfde vorm als het IP patroon voor de verzender.
- Een protocol. Elk getal tussen 0 en 255 correspondeert met een protocol. Op <http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml> is een lijst te vinden met alle protocollen. Merk op dat de wildcard '*' betrekking heeft op alle 256 protocollen. In iTables kan men via een drop-down list ook snel kiezen voor TCP (6), UDP (17) of ICMP (1).
- Een poort patroon voor de verzender. Als het protocol TCP of UDP is kunnen poorten opgegeven worden. Als dit een getal is moet het netwerk pakket deze poort als verzender hebben. Als deze van de vorm a:b is moet a<b zijn. Dan moet de poort van de verzender in het interval [a,b] liggen. '*' betekent elke poort.
- Een poort patroon voor de bestemming. Als het protocol TCP of UDP is kunnen poorten opgegeven worden. Analoog aan het poort patroon voor de verzender.

Men zegt dat een netwerk pakket *matcht* aan een firewall regel als de waarden voor de 5 velden (protocol, bron IP,...) overeenkomen met de patronen van die regel.

Dan wordt de actie van die regel uitgevoerd.

Een firewall configuratie bestaat uit een aantal regels in een bepaalde volgorde. Als een netwerk pakket binnenkomt worden de regels in die volgorde doorlopen. Als er een *match* is met een regel wordt de actie van die regel gedaan.

Als blijkt dat geen enkele regel *matcht* wordt de default policy van de chain uitgevoerd. Deze kan ingesteld zijn op toelaten (ACCEPT) of weigeren (DROP). Op de firewall regel pagina kan men de default policy instellen.

Een firewall heeft meestal meerdere netwerkinterfaces. Minimaal een netwerkinterface voor het eigen netwerk en een netwerkinterface voor het WAN.

Naast de 5 velden die hier genoemd zijn zal een firewall regel vaak ook 2 velden hebben voor de netwerkinterfaces.

Deze 2 velden geven aan van welke netwerkinterface een matchend netwerkpakket moet komen en naar welke netwerkinterface een matchend netwerkpakket moet gaan.

Zo kan men bv. voorkomen dat door IP spoofing een netwerkpakket doet alsof het van het eigen veilige netwerk komt.

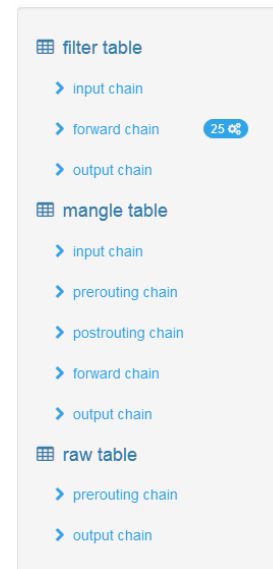
iTables ondersteunt de netwerkkinterface velden niet.

2.2 Wat zijn tables en chains?

iTables werkt enkel met de iptables firewall. Tables en chains zijn begrippen die specifiek zijn voor iptables firewalls.

In iptables zijn er verschillende tables. Er zijn in iptables standaard 4 tables aanwezig. Daarvan worden er 3 door iTables ondersteund.

- FILTER table: Deze table dient om te bepalen of een pakket toegelaten moet worden of geweigerd. In deze table zullen firewall regels in de meeste gevallen komen.
- MANGLE table: Dient voor het bewerken van netwerk pakketten. Bewerken van netwerk pakketten wordt niet ondersteund door iTables.
- RAW table: Wordt gebruikt in firewalls die bijhouden welke verbindingen opgebouwd zijn. Firewall regels met die functionaliteit worden niet ondersteund, maar andere regels wel.
- NAT table: Deze table dient voor Network Address Translation oftewel NAT. Omdat het weigeren van pakketten niet toegelaten is in deze table is een firewall functionaliteit niet mogelijk. Daarom wordt de NAT table niet mee ingelezen door iTables.



iTables ondersteunt enkel zogenaamde *packet filtering firewalls* (zie [Wikipedia](#)). Firewall regels van zo'n firewall zullen in de meeste gevallen in de FILTER table zitten.

OPMERKING: Bij firewall regels met niet-ondersteunde opties worden slechts de ondersteunde opties ingelezen. Er verschijnt dan wel een waarschuwing.

Bij elke table horen chains. iTables leest alle chains in. Sommige chains worden door de firewall automatisch op bepaalde momenten aangeroepen. Dit zijn volgende chains:

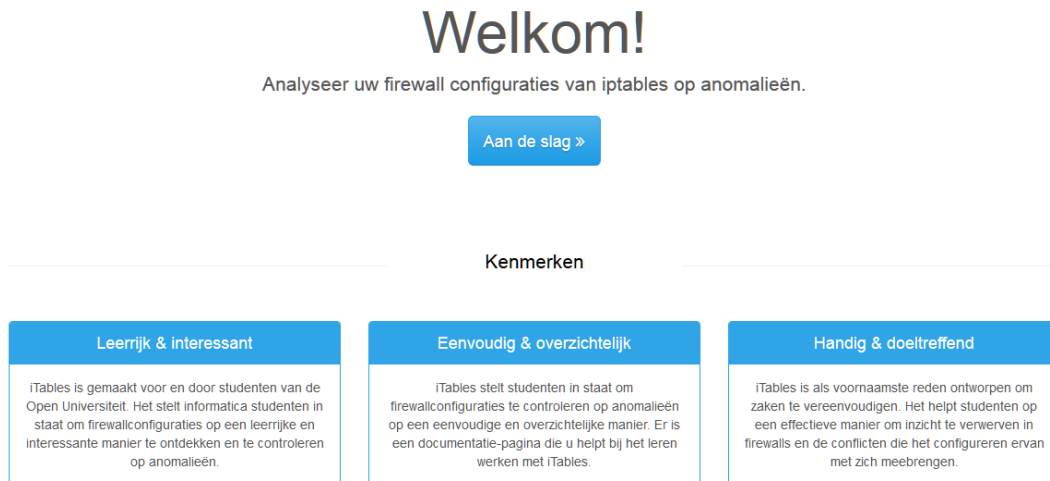
- INPUT chain: Om binnenkomende pakketten te filteren.
- FORWARD chain: Verwerkt alle pakketjes die door de firewall gerouteerd worden.
- OUTPUT chain: Verwerkt pakketjes die komen vanuit de computer waarop de firewall is geïnstalleerd.
- PREROUTING chain: Wordt gebruikt om pakketjes te behandelen zodra ze binnenkomen – nog voor het routingproces er mee aan de slag kan.
- POSTROUTING chain: Behandelt pakketjes voordat ze het systeem verlaten, maar nadat het routingproces er mee aan de slag is geweest.

Elke chain kan firewall regels bevatten. In iTables beschouwt men elke chain als een aparte firewall configuratie. Werken in de ene chain heeft geen invloed op een andere chain. De analyse gebeurt per chain.

Bron: http://nl.wikibooks.org/wiki/Linux_Systeembeheer/Firewalls

2.3 Starten met een configuratie

Bij het opstarten van de website ziet men volgend scherm:



Druk op 'Aan de slag' om te starten.

Dan krijgt men 3 opties:

- Ofwel start men een lege configuratie. Dan wordt een lege configuratie gestart waaraan men zelf nog firewall regels moet toevoegen.
- Ofwel neemt men 1 van de voorbeeldconfiguraties
- Ofwel uploadt men zelf een iptables configuratie bestand. In de paragraaf "Hoe maak ik een configuratie in iptables" wordt uitgelegd hoe men een configuratie aanmaakt in iptables.

Na het starten van een configuratie zijn er 3 modules:

- Men kan men de firewall regels bekijken.
- Men kan de anomalieën zoeken in de configuratie.
- Men kan het logbestand bekijken. Daarin staan alle acties die gedaan zijn op de configuratie.



Stel men heeft er voor gekozen om te starten met een lege configuratie. Het toevoegen van regels aan deze lege configuratie moet als volgt gebeuren. Kies voor de optie om de firewall regels te bekijken. Klik dan op de chain waaraan men de regels wil toevoegen. Meestal zal men de regels willen toevoegen in de FORWARD chain van de FILTER table. Zie de paragraaf “Wat zijn tables en chains?” voor uitleg. Men krijgt volgend scherm te zien:

Firewallrules
filter table → forward chain

Home / Mijn configuratie / Firewallrules

Toon 10 firewallregels per pagina

#	Protocol	Bron IP	Bronpoort	Doel IP	Doelpoort	Actie
Geen firewallregels aanwezig in de chain						

0 tot 0 van 0 firewallregels

Default Policy: ACCEPT

+ Firewallregel toevoegen

Bepaal matchende regel

Een educatief speeltje. U kunt in de volgende tabel een willekeurig aantal velden invullen. Nu zal getest worden met welke regel dit 'pakketje' het eerst zal matchen. Zie [Bepaal matchende regel](#) voor uitleg.

Protocol	Bron IP	Bronpoort	Doel IP	Doelpoort
--				

Q match wis invoer

Met de knop “Firewall regel toevoegen” kan men dan zelf firewallregels toevoegen. Zie de paragraaf “Toevoegen van een regel”.

3 Blok 3: De analyse

3.1 Vinden van policy conflicten

Start de voorbeeldconfiguratie ‘*Configuration with shadowing*’ zoals beschreven in paragraaf 3.

Open de Firewallrules module. U ziet rechts een lijst met alle tables en chains van de iptables configuratie. Voor een uitleg over wat tables en chains zijn verwijzen we naar de paragraaf “Wat zijn tables en chains?”.

U ziet ook een getal naast de forward chain. Dit getal geeft aan hoeveel regels in die chain zitten. Klik op de forward chain om de regels te bekijken.

Firewallrules
filter table → forward chain

Home / Mijn configuratie / Firewallrules

Toon 10 firewallrules per pagina

#	Protocol	Bron IP	Bronpoort	Doel IP	Doelpoort	Actie
1	TCP	10.1.2.0/24	*	192.168.0.0/16	25	drop
2	TCP	192.168.0.0/16	16015	173.252.110.27/32	80	accept
3	*	10.2.0.0/16		192.168.0.0/16		drop
4	TCP	10.2.54.0/24	1543	192.168.5.0/24	80	accept
5	UDP	10.1.2.88/32	*	192.168.0.0/16	*	drop

1 tot 5 van 5 firewallrules

Default Policy: ACCEPT

+ Firewallregel toevoegen

filter table
 > input chain
 > forward chain **500**
 > output chain

mangle table
 > input chain
 > prerouting chain
 > postrouting chain
 > forward chain
 > output chain

raw table
 > prerouting chain
 > output chain

Bekijk regel 3 en regel 4:

3	*	10.2.0.0/16		192.168.0.0/16		drop	
4	TCP	10.2.54.0/24	1543	192.168.5.0/24	80	accept	

Hier is een policy conflict. Een policy conflict is een anomalie.

Een policy conflict komt voor als er netwerk pakketten zijn waarvoor meerdere regels een verschillende actie hebben.

Deze anomalie moeten we terug vinden op de anomalieën module. Open de anomalieën module door rechtsboven op 'Mijn configuratie' te klikken en dan op 'Anomalieën'.

Mijn configuratie ▾

- Anomalieën
- Firewallrules
- Logbestand
- Configuratie exporteren
- Sessie exporteren
- Sessie beëindigen

Men kan op elk gewenst moment van module wisselen door dit menu op te roepen.

U krijgt volgend scherm te zien:

Correlatiegroep 1		
	segment 1 ▾	
firewallregel 1	drop	

Correlatiegroep 2		
	segment 2 ▾	
firewallregel 2	accept	

Correlatiegroep 3		
	segment 3 ▾	segment 4 ▾
Voorkeursactie wijzigen	accept ▾	
firewallregel 3	drop	drop
firewallregel 4	accept	

Correlatiegroep 4		
	segment 5 ▾	
firewallregel 5	drop	

De firewall regels worden in groepen opgedeeld.

Bij het zoeken naar anomalieën kan men die groepen afzonderlijk beschouwen.

In de groen gemarkeerde groepen zijn geen policy conflicten.

Groep 3 is rood dus daar is ergens een policy conflict.

Elk netwerk pakket heeft 5 waarden:

- Een protocol
- Een bronpoort
- Een bronadres. Dit is het IP-adres van de afzender.
- Een doelpoort
- Een doeladres. Dit is het IP-adres van de bestemming.

Een firewall configuratie bepaalt aan de hand van die 5 waarden of het pakket doorgelaten wordt of geweigerd.

Op deze anomalieën pagina wordt die configuratie opgedeeld in segmenten. Zo een segment is dus een gedeelte van de configuratie.

In de tabel is te zien welke regels effect hebben op pakketten die vallen binnen een segment.

Naast segment 3 staat een uitroepteken. Dit wil zeggen dat hier een policy conflict is.

Regel 3 en regel 4 zitten beide in segment 3 maar geven een andere actie aan voor pakketten die vallen binnen dat segment.

Zoals verwacht is er dus een policy conflict tussen regel 3 en regel 4.


Nu men weet dat hier een policy conflict is kan men actie ondernemen om deze op te lossen.

3.2 Oplossen van policy conflicten

Start de voorbeeld configuratie 'Configuration with shadowing'. Bekijk de anomalieën pagina.

Correlatiegroep 1		
	segment 1 ▾	
firewallregel 1	drop	

Correlatiegroep 2		
	segment 2 ▾	
firewallregel 2	accept	

Correlatiegroep 3		
	segment 3 ▾	segment 4 ▾
 Voorkeursactie wijzigen	accept ▾	
firewallregel 3	drop	drop
firewallregel 4	accept	

Correlatiegroep 4		
	segment 5 ▾	
firewallregel 5	drop	


In segment 3 is er een policy conflict.

Men kan op de drop-down list onderaan de tabel van groep 3 kiezen wat de voorkeursactie is binnen elk segment waar een conflict is.

iTables zal dan proberen de regels te herordenen zodat aan de gekozen voorkeuren wordt voldaan.

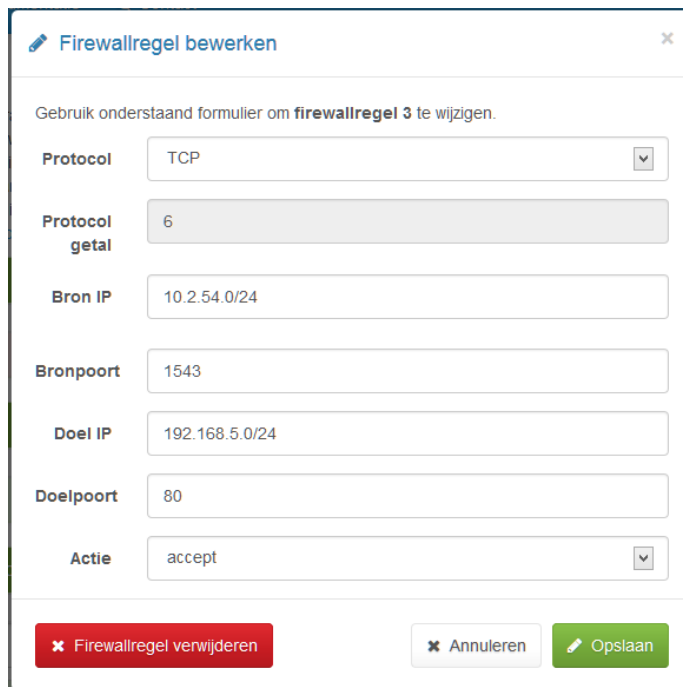
Het kan zijn dat het niet mogelijk is om de regels te herordenen zodat aan alle voorkeuren voldaan wordt. Men krijgt daar dan een melding van.

Neem hier als voorkeursactie in segment 3 'accept'. Het resultaat is dan volgend:

Correlatiegroep 3 - Conflicten opgelost		
	segment 3 ▾	segment 4 ▾
 Voorkeursactie wijzigen	accept ▾	
firewallregel 3	accept	
firewallregel 4	drop	drop

Men kan policy conflicten ook oplossen door de firewall regels aan te passen. Dit kan zowel op de firewallregels pagina als rechtstreeks op de anomalieën pagina.

Regels wijzigen op de anomalieën pagina is eenvoudig. Klik op een regel en er verschijnt een pop-up. Daar kan men nieuwe waarden voor de regel invullen of de regel verwijderen.



Firewallregel bewerken

Gebruik onderstaand formulier om firewallregel 3 te wijzigen.

Protocol: TCP

Protocol getal: 6

Bron IP: 10.2.54.0/24

Bronpoort: 1543

Doel IP: 192.168.5.0/24

Doelpoort: 80

Actie: accept

Buttons: ✖ Firewallregel verwijderen ✖ Annuleren ✎ Opslaan

Na elke wijziging aan de configuratie worden de segmenten opnieuw bepaald. Wel houdt de applicatie bij welke policy conflicten reeds opgelost zijn. Groepen met alleen opgeloste policy conflicten worden steeds als opgelost gemarkeerd.

Let op! Bij het oplossen van een policy conflict kan het soms zijn alsof niet aan de ingegeven voorkeursacties voldaan werd. Dit lijkt dan slechts zo omdat de segment nummering en de positie van de kolommen van de segmenten anders zijn. Als men kijkt naar de inhoud van de segmenten dan ziet men dat het policy conflict wel is opgelost volgens de voorkeursacties.

3.3 Wijzigen van firewall regels

We werken verder met de configuratie uit de vorige sectie. Dit is de voorbeeldconfiguratie *'Configuration with shadowing'*, waarin de voorkeursactie voor segment 3 gewijzigd is in 'accept'. Ga naar de firewallregels pagina.

Firewallrules

filter table → forward chain

Home / Mijn configuratie / Firewallrules

Toon 10 firewallrules per pagina

#	Protocol	Bron IP	Bronpoort	Doel IP	Doelpoort	Actie
1	TCP	10.1.2.0/24	*	192.168.0.0/16	25	drop
2	TCP	192.168.0.0/16	16015	173.252.110.27/32	80	accept
3	TCP	10.2.54.0/24	1543	192.168.5.0/24	80	accept
4	*	10.2.0.0/16		192.168.0.0/16		drop
5	UDP	10.1.2.88/32	*	192.168.0.0/16	*	drop

1 tot 5 van 5 firewallrules

Default Policy: ACCEPT

+ Firewallregel toevoegen

filter table

- input chain
- forward chain** (5 rules)
- output chain

mangle table

- input chain
- prerouting chain
- postrouting chain
- forward chain
- output chain

raw table

- prerouting chain
- output chain

Klik op een veld van een firewall regel om deze te wijzigen.

Klik op het vuilbakje om een regel te verwijderen.

Klikken op de knop 'Firewallregel toevoegen' zorgt dat een regel toegevoegd wordt achteraan.

Versleep een regel om zijn positie te wijzigen.

Men kan het aantal regels dat in 1 keer getoond wordt wijzigen. Standaard staat deze op 10.

Verander de actie van firewall regel 4 in accept.

Gebruik deze configuratie voor de volgende paragraaf 'Zoeken naar redundante (overbodige) regels'.

3.4 Zoeken naar redundante (overbodige) regels

We werken in deze paragraaf verder met de firewall configuratie uit de vorige sectie 'Wijzigen van firewall regels'.

Dit is de voorbeeld configuratie 'Configuration with shadowing'. Daarin is de voorkeursactie in segment 3 gewijzigd in 'accept'. Daarna is de actie van regel 4 gewijzigd in 'accept'.

Redundante regels zijn regels die overbodig zijn in de configuratie. Redundante regels kan men zonder problemen verwijderen.

Redundantie is naast policy conflicten ook een soort anomalie.

Kijk naar regel 3 en regel 4 op de firewallrules pagina:

3	TCP	10.2.54.0/24	1543	192.168.5.0/24	80	accept	
4	*	10.2.0.0/16		192.168.0.0/16		accept	

Regel 4 is algemener dan regel 3.

De actie van regel 3 is dezelfde als regel 4.

Daarom is regel 3 redundant.

Dit moeten we terugvinden op de anomalieën pagina.

Ga naar de anomalieën pagina door rechtsboven op 'Mijn configuratie' te klikken.

Kies voor 'Anomalieën'.

In groep 3 is zichtbaar dat regel 3 redundant is.

Correlatiegroep 3		
	segment 3 ▼	segment 4 ▼
firewallregel 3	accept	
firewallregel 4	accept	accept

Regel 4 heeft de actie 'accept' in zowel segment 3 als segment 4. Regel 3 heeft de actie 'accept' in enkel segment 3.

Als we dus regel 3 verwijderen blijft de configuratie dezelfde. De actie blijft 'accept' voor netwerk pakketten die vallen binnen segment 3 of segment 4.

iTables kan alle redundante regels zoeken. Klik daarvoor op de knop 'Chain onderzoeken op redundancies'.

Het resultaat is zoals verwacht:

Redundante firewallregels						
#	Protocol	Bron IP	Bronpoort	Doel IP	Doelpoort	Actie
3	6	10.2.54.0/24	1543	192.168.5.0/24	80	accept
1 tot 1 van 1 firewallregels						
<div>Verwijder deze regels</div> <div>Sluiten</div>						

Met de knop 'Verwijder deze regels' kunnen de redundante regels in 1 klik verwijderd worden.

Nog een voorbeeld om aan te tonen dat de volgorde van de regels een rol speelt bij het bepalen van de redundante regels.

Beschouw een configuratie met de volgende segmentering:

Correlatiegroep 1				
	segment 1 ▼	segment 3 ▼	segment 4 ▼	segment 5 ▼
<input checked="" type="checkbox"/> Voorkeursactie wijzigen	accept			
firewallregel 1	accept	accept		
firewallregel 3	drop		drop	
firewallregel 4	accept	accept		accept

Men zou de gedachte kunnen hebben dat firewallregel 1 redundant is t.o.v. firewallregel 4, echter in de huidige volgorde van de regels zijn geen regels redundant:

- Verwijderen van regel 1 zou bv. zorgen dat de actie in segment 1 wijzigt naar DROP.
- Verwijderen van regel 3 zou de configuratie wijzigen want dan is er geen actie meer voor pakketten in segment 4. Voor pakketten in dit segment wordt dan de default policy actie uitgevoerd. Deze default policy actie wordt bij het bepalen van de anomalieën buiten beschouwing gehouden.

- Verwijderen van regel 4 zou ervoor zorgen dat er geen actie meer is voor pakketten in segment 5.

Nu wisselen we de regels 1 en 4 van plaats. Resultaat:

Correlatiegroep 1				
	segment 1	segment 3	segment 4	segment 5
<input checked="" type="checkbox"/> Voorkeursactie wijzigen	accept			
firewallregel 1	accept	accept		accept
firewallregel 3	drop		drop	
firewallregel 4	accept	accept		

Nu is er wel een redundante regel.

Als men regel 4 verwijdert blijven immers de acties in elk segment dezelfde.

3.5 Opsomming van een segment opvragen

Zoals uitgelegd in de paragraaf 'Vinden van policy conflicten' deelt iTables de configuratie op in segmenten. Zo kunnen policy conflicten gevonden worden. Ga naar de anomalieën pagina.

Het is mogelijk om de inhoud van een segment op te vragen.

Klik daarvoor op een segment.

Correlatiegroep 3		
	segment 3	segment 4
<input checked="" type="checkbox"/> Voorkeursactie wijzigen	<input type="text" value="Compacte segmentinhoud tonen"/> <input type="text" value="Uitgebreide segmentinhoud tonen"/>	
firewallregel 3	drop	drop
firewallregel 4	accept	

Herinner dat een netwerk pakket bestaat uit 5 velden.

De optie om de segmentinhoud uitgebreid te tonen zal een opsomming geven van alle combinaties van die 5 waarden die horen bij dat segment.

Een netwerk pakket valt dus binnen een segment als het een van de opgesomde waarden heeft.

Meestal is de opsomming zo groot dat het niet zinnig is deze volledig weer te geven. Zo ook hier:

✕

De inhoud van het segment is te groot om weer te geven.

✕ Sluiten

iTables heeft echter de mogelijkheid om een compacte versie van de opsomming weer te geven.

Klik op een segment en kies nu voor 'Compacte segmentinhoud tonen'. Het resultaat is volgende:

Inhoud van segment 3 (compacte weergave)

Hier een opsomming van de inhoud van het segment.

Protocol	Bron IP	Bronpoort	Doel IP	Doelpoort	Info
TCP	10.2.54.0	1543	192.168.5.0	80	begin
TCP	10.2.54.255	1543	192.168.5.255	80	einde

1 tot 2 van 2 regels

In de compacte weergave staan regels met 'begin' en regels met 'einde'.
Zie [Opsomming van een segment opvragen](#) voor uitleg.

Sluiten

In de compacte weergave staan regels met 'begin' en regels met 'einde'.
De regels met 'begin' worden altijd opgevolgd door een regel met 'einde'.
Alle pakketten met waarden tussen de waarden in de 'begin' regel en de waarden in de 'einde' regel vallen binnen het segment.
Zo wordt de opsomming veel compacter.
Opmerking: Regels zonder 'begin' of 'einde' aanduiding hebben dezelfde betekenis als bij de uitgebreide opsomming.

In dit voorbeeld vallen volgende netwerk pakketten binnen het segment:
Alle netwerk pakketten met protocol TCP, een bron IP adres tussen 10.2.54.0 en 10.2.54.255, bronpoort 1543, een doel IP adres tussen 192.168.5.0 en 192.168.5.255 en doelpoort 80 vallen binnen segment 3.

Opmerking: Soms zijn in de protocol-kolom getallen te zien. Elk getal tussen 0 en 255 is een mogelijke protocol waarde. Op <http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml> staat een lijst met alle protocollen.

4 Blok 4: De pagina met firewall regels

4.1 Toevoegen van een regel

Het toevoegen van een regel kan enkel op de firewallregels pagina.

Toon firewallregels per pagina

#	Protocol	Bron IP	Bronpoort	Doel IP	Doelpoort	Actie	
1	TCP	10.1.2.0/24	*	192.168.0.0/16	25	drop	
2	TCP	192.168.0.0/16	16015	173.252.110.27/32	80	accept	
3	*	10.2.0.0/16		192.168.0.0/16		drop	
4	TCP	10.2.54.0/24	1543	192.168.5.0/24	80	accept	
5	UDP	10.1.2.88/32	*	192.168.0.0/16	*	drop	

1 tot 5 van 5 firewallregels

Default Policy:

[+ Firewallregel toevoegen](#)

Klik op de firewallregel toevoegen knop.

+ Firewallregel toevoegen

Gebruik dit formulier om een nieuwe firewall regel toe te voegen achteraan de regelset van de huidige chain. Voor tussenvoegen onderaan aanvinken s.v.p.

Protocol

Protocol getal

Bron IP

Bronpoort

Doel IP

Doelpoort

Actie

Voeg in op een positie zodat hij geen conflict oplevert met voorgaande regels. ☐

Voer de waarden van de nieuwe regel in.

Als laatste is er een checkbox. Als men deze checkbox niet aanvinkt wordt de regel achteraan de configuratie toegevoegd.

Als men deze checkbox aanvinkt gebeurt het volgende:

De regel wordt in de configuratie toegevoegd zodanig dat er geen policy conflicten ontstaan met voorgaande regels. Dat wil zeggen zodanig dat er geen overlappingen zijn met eerdere regels een andere actie hebben. Zo zal de regel gegarandeerd volledig effect hebben.

4.2 Bepaal matchende regel

Een educatief speeltje. De gebruiker kan van de 5 velden een willekeurig aantal invullen, bijv. het protocol en het bron IP adres. Nu kan getest worden met welke regel van de chain dit 'pakketje' het eerst zal matchen.

Q Bepaal matchende regel

Een educatief speeltje. U kunt in de volgende tabel een willekeurig aantal velden invullen. Nu zal getest worden met welke regel dit 'pakketje' het eerst zal matchen. Zie [Bepaal matchende regel](#) voor uitleg.

Protocol	Bron IP	Bronpoort	Doel IP	Doelpoort
---	.		.	

Voer daarvoor de gewenste waarden in en klik op de knop 'match'.

5 Blok 5: Overige

5.1 Logboek bekijken

Alle acties van de gebruiker op de firewall configuratie worden bijgehouden. Men kan deze bekijken op de Logbestand pagina. Op elk moment kan naar de Logbestand pagina gegaan worden door rechtsboven op 'Mijn configuratie' te klikken en dan op 'Logbestand'.

Mijn configuratie ▾

Anomalieën

Firewallregels

Logbestand

Configuratie exporteren

Sessie exporteren

Sessie beëindigen

Het Logbestand bevat alle acties met het tijdstip waarop de actie gedaan is.

Logbestand

[Home](#) / [Mijn configuratie](#) / [Logbestand](#)

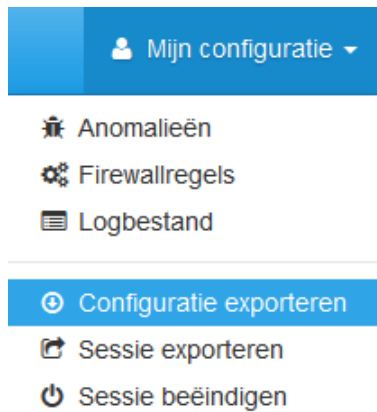
Toon 10 logs per pagina

#	Tijdstip	Gebeurtenis	Details
1	04/12/2013 - 17:15:51	Voorbeeldconfiguratie gestart	Configuration with shadowing
2	04/12/2013 - 17:35:54	Firewallregel bijgewerkt	Regel 1 van table filter van chain forward bijgewerkt van (TCP,10.1.2.0/24,*,192.168.0.0/16,25,deny) naar (TCP,10.1.2.0/24,*,192.168.0.0/15,25,deny)
3	04/12/2013 - 17:36:01	Firewallregel verwijderd	Firewallregel 5 (index: 5; protocol: UDP; bron IP: 10.1.2.88/32; bronpoort: *; doel IP: 192.168.0.0/16; doelpoort: *; actie: deny) verwijderd van filter table en forward chain

1 tot 3 van 3 logs

5.2 Downloaden en laden van een (evt. gewijzigde) iptables configuratie

Klik op 'Mijn configuratie' rechtsboven. Kies voor 'Configuratie exporteren'.

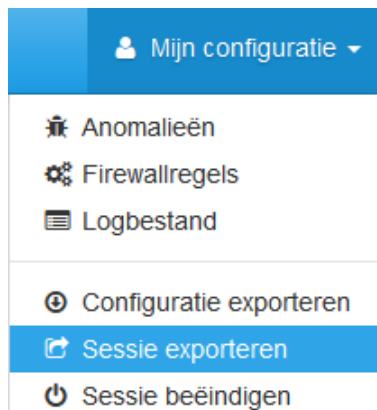


De configuratie kan terug ingelezen worden in iptables.
Gebruik daarvoor het *iptables-restore* commando in de Linux terminal.
Voor een bestand met de naam `iTables_export.iptables` ziet het commando er als volgt uit:

```
sudo iptables-restore < iTables_export.iptables
```

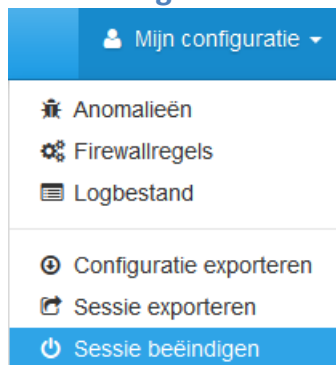
5.3 Exporteren van de resultaten van de sessie

iTables biedt de mogelijkheid aan om de sessie te exporteren.
Daarbij worden de resultaten van de analyse en het Logbestand in een Excel-bestand gezet.
Het exporteren van de sessie kan op elk moment door rechtsboven op 'Mijn configuratie' te klikken en voor 'Sessie exporteren' te kiezen.



Voor het openen van het bestand is *Microsoft Excel 2003* (of later) nodig.

5.4 Beëindigen van een sessie (bv. als men met een andere firewall configuratie wil werken)



OPGELET! Het beëindigen van een sessie wist alle gegevens.

De firewall configuratie waar men mee aan het werken is verdwijnt. Het Logboek wordt gewist.

Als men terug met een firewall configuratie wil werken moet men een nieuwe firewall configuratie starten. (zie paragraaf 3)

5.5 Hoe maak ik een configuratie in iptables

Voor een complete uiteenzetting hoe iptables gebruikt kan worden verwijzen we naar de *man*-pagina's in linux. Gebruik daarvoor volgend commando:

man iptables

Wis eerst de bestaande iptables configuratie op uw computer.

Gebruik daarvoor het commando

sudo iptables --flush

iTables beperkt zich tot configuraties waarvan firewall regels slechts 5 velden hebben. Deze regels zijn als volgt te maken in iptables.

De syntax is volgende:

sudo iptables [-t table] -A naam_chain [-s bron_IP_adres] [-d doel_IP_adres] [-p protocol] [--sport bron_poort] [--dport doel_poort] -j actie

met:

- *table*: Naam van de table waar de regel in moet komen. iTables ondersteunt enkel de waarden FILTER, NAT, MANGLE of RAW. Indien de *-t* optie niet wordt opgegeven zal iptables de FILTER table nemen.
- *naam_chain*: Naam van de chain van de table.
- *protocol*: Mogelijke waarden: tcp, udp, icmp of een getal tussen 0 en 255. Optie *-p* niet opgeven staat gelijk aan de wildcard (*). Let er op dat de opties *--sport* en *--dport* alleen mogen opgegeven worden als het protocol tcp of udp is.
- *bron_IP_adres*: Een IP patroon voor de verzender. Deze is van de vorm a.b.c.d/e. Een IP adres bestaat eigenlijk uit 32=8*4 bits. Dus 8 bits per getal. Het getal e geeft aan hoeveel van de eerste bits overeen moeten komen met het netwerk pakket. Bijvoorbeeld als het IP patroon 54.0.0.0/8 is zal elk IP adres dat begint met het getal 54 overeenkomen.
- *doel_IP_adres*: Een IP patroon voor de bestemming. Deze is van de zelfde vorm als het IP patroon voor de verzender.

- *bron_poort*: Een poort patroon voor de verzender. Kan enkel opgegeven worden als protocol TCP of UDP is. Als dit een getal is moet het netwerk pakket deze poort als verzender hebben. Als deze van de vorm a:b is moet a<b zijn. Dan moet de poort van de verzender in het interval [a,b] liggen.
- *doel_poort*: Een poort patroon voor de bestemming. Kan enkel opgegeven worden als protocol TCP of UDP is. Analooq aan het poort patroon voor de verzender.

Men kan de configuratie bewaren onder de naam *naam_bestand* met het commando

iptables-save > naam_bestand

Dat bestand kan geüpload worden in iTables.

iptables-save zet de firewall configuratie in een tekstbestand met UNIX indeling. Ook in een ander besturingssysteem zoals Windows is het mogelijk een tekstbestand aan te maken met UNIX indeling. Bijvoorbeeld met de tool Notepad++ kan men kiezen voor een UNIX indeling. Zo een tekstbestand volgt een bepaalde syntax:

```
# Regels die starten met # dienen voor commentaar. iptables en iTables negeren deze.
# Volgende regel geeft aan dat men vanaf hier in de FILTER tabel configureert.
*filter
# Volgende is een definitie van een chain. De ACCEPT in de volgende regel geeft de default policy in de INPUT chain aan.
:INPUT ACCEPT

:FORWARD DROP
# Regels na een definitie van een chain komen in die chain.
# Regel 1. Syntax voor een regel is idem aan de syntax die eerder uitgelegd is, maar het iptables commando woord kan weggelaten worden.
-A FORWARD -s 135.20.30.88/32 -d 10.65.46.0/24 -p 49 -j ACCEPT
# Regel 2
-A FORWARD -d 173.252.110.27/32 -p tcp --dport 80 -j DROP
# Regel 3
-A FORWARD -s 10.6.27.96/32 -d 173.252.111.56/32 -p udp --sport 1404 --dport 107 -j ACCEPT
# Regel 4
-A FORWARD -s 135.20.30.0/24 -d 10.65.46.0/24 -p tcp --dport 88 -j ACCEPT
# Regel 5
-A FORWARD -d 10.65.46.0/24 -j DROP

:OUTPUT ACCEPT
# De COMMIT opdracht commit al het voorgaande naar de firewall.
COMMIT
# Tabel mangle
*mangle
:INPUT ACCEPT

:PREROUTING ACCEPT

:POSTROUTING ACCEPT

:FORWARD ACCEPT

:OUTPUT ACCEPT

COMMIT
# Tabel raw
*raw
:PREROUTING ACCEPT

:OUTPUT ACCEPT

COMMIT
```