Netfilter & IPtables

محدوده:

بررسی ساختار پردازش بسته های شبکه در لینوکس

تاریخچه:

ردیف	نویسنده	تاریخ	شماره ویرایش	توضیحات
۱				
۲	تحقیق و توسعه فنی و مهندسی	۱۳۸۹	۲.۰.۰	
۳	تحقیق و توسعه فنی و مهندسی	۱۳۹۳	۲.۱.۰	

فهرست مندرجات

فهرست تصاویر

فهرست جداول

فهرست ضمائم

دفتر مرکزی: یزد -خیابان مطهری-مرکز فناوری اقبال - واحد C۲۵ کدپستی: ۸۹۱۷۶۹۷۹۹۸ تلفن (۳ خط): ۷۲۶۵۳۴۳ - ۰۳۵۱ فکس: ۷۲۴۵۰۸۷ - ۰۳۵۱
www.pdnsoft.com Email: info@pdnsoft.com

چکیده

ساختار *Netfilter* جهت پردازش پویای بسته های شبکه در سیستم عامل لینوکس طراحی و پیاده‌سازی شده است. این مستند ضمن معرفی معماری *Netfilter*، معماری *Iptables* به عنوان ابزاری پیاده‌سازی شده بر مبنای *Netfilter* برای پالایش(*Filtering*) بسته های شبکه، را مورد بررسی قرار میدهد.

کلید واژه ها

Linux, Netfilter, IPtables

۱ *Netfilter* یا ساختار پردازش بسته های شبکه

انجام پردازش دلخواه بر روي بسته‌هاي شبکه (بسته‌هاي متعلق به پروتکلهاي لاية شبکه) مستلزم شناخت مناسب *Protocol Stack* مربوط به پروتکل مربوطه مي‌باشد. *Protocol Stack* نمايشگر پردازشهاي انجام گرفته بر روي بستة شبکه و همچنين ترتيب آنها در امتداد مسيرهاي پردازشي مي‌باشد.

مسيرهاي پردازشي بيان منطقي سير حرکت بستة شبکه در درون سيستم مي‌باشند. مسير عبوري شامل بسته‌هايي مي‌باشد که خواستار عبور از سيستم ما هستند. اين مسير در هنگامي که سيستم به عنوان يک مسيرياب يا دروازه مورد استفاده قرار مي‌گيرد ايجاد مي‌شود. مسير ورودي شامل بسته‌هايي مي‌باشد که از سيستم‌هاي ديگر به هدف سيستم ما گسيل داده شده‌اند و مسير خروجي نيز بسته‌هايي را شامل مي‌شود که از سيستم ما به سمت سيستم‌هاي ديگر فرستاده شده‌اند.

تصميم بر انجام تغيير دلخواه بر روي بستة شبکه مستلزم شناختِ مکان مناسب در مسيرهاي پردازشي، در درون لايه شبکه، و سپس انجام تغيير در پردازش صورت گرفته در آن مکان مي‌باشد. اين موضوع تا اندازه‌اي سلامت ساختار *Protocol Stack* را به خطر مي‌اندازد.

دفتر مرکزی: یزد - خیابان مطهری - مرکز فناوری اقبال - واحد C۲۵ کدپستی: ۸۹۱۷۶۹۷۹۹۸ تلفن (۳ خط): ۷۲۶۵۳۴۳ - ۰۳۵۱ فکس: ۷۲۴۵۰۸۷ - ۰۳۵۱
www.pdnsoft.com Email: info@pdnsoft.com

ساختار پردازش، تلاشي براي ايجادِ امكانِ دستكاريِ دلخواهِ بسته‌هاي شبكه بدون ايجادِ تغيير در ساختار *Protocol Stack* سيستم، مي‌باشد.

در اين شيوه براي هر پروتكل، مكانهايي خاص به منظور انجام پردازشهاي دلخواه، در مسيرهاي پردازشي پروتكل مربوطه، تعريف مي‌شوند. خاصيت اصلي اين مكانها توانايي ثبت فانكشنهايِ خواهانِ پردازشِ بسته‌هاي شبكه و نگهداري ترتيبي آنها، بر اساس اولويت، مي‌باشد. هنگامي كه يک بستة شبكه در مسير پردازشي خود خواهان عبور از اين نقاط باشد، اين مكانها، بر اساس ترتيب ثبت فانكشنها، بسته را به ترتيب در اختيار تک‌تکِ آنها قرار مي‌دهند. هر فانكشن موظف مي‌باشد تا بعد از انجام پردازش دلخواه، اجازة عبور و يا فرمان حذف بسته را از گردونه صادر كند.

اين ساختار در سيستم عامل لينوكس با نام *netfilter* شناخته مي‌شود.

۱.۱ NetFilter

netfilter چهارچوبي است براي مديريت و پردازش بسته‌هاي شبكه، مستقل از پروتكل مربوطه. از ديدگاه پياده‌سازي، *netfilter* جايگاهي براي نگهداري ماژولهاي خواهانِ پردازشِ بسته‌هاي شبكه، در قالب مجموعه‌هايي با نام *hook* كه توسط پروتكل‌هاي مختلف در *netfilter* تعريف شده‌اند، مي‌باشد. *hook*ها همان مكانهاي ثبت فانكشنها در تعريف ساختار پردازش مي‌باشند.

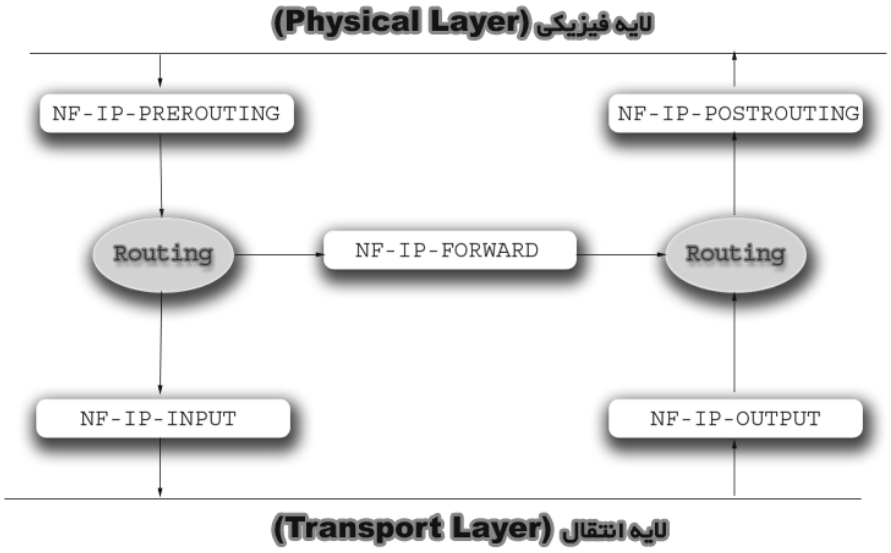
در صورتي كه بسته‌اي خواستار عبور از درون مجموعه‌اي مشخص (*hook*) باشد، اين بسته توسط *netfilter* در اختيار تك‌تك ماژولها قرار مي‌گيرد، ماژولها مشخص‌كنندة وضعيت بستة عبوري خواهند بود، يعني مي‌توانند بنا به تصميمات خود به آن اجازه عبور بدهند (*NF-ACCEPT*) ، آن را از گردونه حذف كنند (*NF-DROP*) و يا آن را براي انجام پردازش در سطح كاربر در صف قرار دهند (*NF-QUEUE*) و ....

پروتكل *IP*، به منظور مديريت آسان بسته‌هاي *IP*، پنج مجموعه را در اين چهار چوب تعريف مي‌كند. مي‌توانيد نحوة نامگذاري اين مكانها و نحوة عبور بسته‌هاي *IP* از درون آنها، را در شكل ۱ مشاهده كنيد. هر ماژولي كه خواستار بررسي و تعيين وضعيت بسته‌هاي *IP* باشد مي‌تواند خود را در يكي از اين مجموعه‌ها ثبت كند.

اين گونه رفتار با بسته‌هاي *IP* اين امكان را به ما مي‌دهد تا بدون دستكاري در ساختار *Protocol stack* بتوانيم

دفتر مرکزی: یزد - خیابان مطهری - مرکز فناوری اقبال - واحد C۲۵ کدپستی: ۸۹۱۷۶۹۷۹۹۸ تلفن (۳ خط): ۷۲۶۵۳۴۳ - ۰۳۵۱ فکس: ۷۲۴۵۰۸۷ - ۰۳۵۱
www.pdnsoft.com Email: info@pdnsoft.com

به اهداف خود، نظير پياده‌سازي ديواره‌هاي آتش و انجام اعمال *NAT* [1] ، دست يابيم.



تصویر ۱: شمای *hook*ها در *Netfilter*

اين ارتباط راهگشاي ما در يافتن مكان مناسب براي مديريت بسته‌ها خواهد بود. به عنوان مثال براي انجام عمل *filtering* مجموعه‌هاي *NF-IP-FORWARD*، *NF-IP-OUTPUT*، *NF-IP-INPUT* انتخاب شده‌اند. بدين صورت، تمام بسته‌هاي عبوري از سيستم تنها در يک مكان بررسي خواهند شد.

مثالي ديگر: براي انجام عمل *NAT*، مجموعه‌هاي *NF-IP-OUTPUT*، *NF-IP-PREROUTING* براي انجامِ عملِ انتقال آدرس مبداء [2] و *NF-IP-POSTROUTING* براي انتقال آدرس مقصد [3] ، انتخاب شده‌اند. به هر صورت اين چهارچوب امكان بسيار خوب و ساده‌اي را در اختيار پياده سازان ديواره‌هاي آتش قرار داده است.

1 Network Address Translation
2 Source NAT
3 Destination NAT

دفتر مرکزی: یزد - خیابان مطهری - مرکز فناوری اقبال - واحد C۲۵ کدپستی: ۸۹۱۷۶۹۷۹۹۸ تلفن (۳ خط): ۷۲۶۵۳۴۳ - ۰۳۵۱ فکس: ۷۲۴۵۰۸۷ - ۰۳۵۱
www.pdnsoft.com Email: info@pdnsoft.com

۲ IPtables : ساختار پالايش بسته‌هاي IP

پالايش بسته‌هاي شبكه به معني تقسيم جريان واحد بسته‌ها در قالب جريانهاي مختلف براي انجام پردازش‌هـاي متنوع بر روي هر جريان مي‌باشد. هر جريان توسط يک قانون كه شرايطي را بر فيلدهاي سرآيند بستة شبكه اعمـال مي‌كند، مشخص مي‌شود.

ساختار پالايش بسته‌هاي IP (iptables) به دنبال ايجاد چهارچوبي جهت ذخيره‌سازي و مديريتِ مناسب قانونها مي‌باشد. اين ساختار سعي خواهد كرد تا با توجه به استراتژي و سياسـت خـود در مـديريت قانونهـا، امكـان تعييـن تكليف بسته را با توجه به قانونهاي موجود فراهم آورد.

ملزومات هر ساختار پالايش عبارتند از:

۱-ساختمان دادة انباره

۲-ساختمان دادة قانون

۳-رابط مديريت قانونها

۴-رابط ايجاد انباره

۵-رابط مديريت انباره

۶-الگوريتم جستجو

۷-رابط تعيين تكليف بسته

بدين صورت در پياده‌سازي يک فرآيندِ دسته‌بندي نيازي به پياده‌سازي يک انباره و الگوريتم جسـتجوي مسـتقل نخواهد بود، بلكه مي‌توان از ويرايش موجود در ساختار پالايش استفاده كرد. در اين ساختار هـر فرآينـد مي‌بايسـت پردازشهاي و تطابقهاي مناسب براي قوانين متعلق به خود را تعريف و همچنين ملزومات لازم براي انجـام مناسـب آنها را فراهم آورد (با توجه به اينكه هر قانون شامل چند تطابق و يک پردازش مي‌باشد).

ساختار پالايش بسته‌هاي IP، از تقسيم موضوعي فرآيند دسته‌بندي بسته‌هاي شـبكه بـه منظـور ايجـاد چنـدين فرآينـد دسـته‌بندي، مربـوط بـه موضـوعات كـاري مختلـف (*filter, NAT, mangle* ...)، اسـتفاده مي‌كند. طرح اين عمل بدان دليل مي‌باشد كه محقق شدن هر موضوع كاري در مكانهاي خاصي از سـاختار پـالايش

دفتر مرکزی: یزد - خیابان مطهری - مرکز فناوری اقبال - واحد C۲۵ کدپستی: ۸۹۱۷۶۹۷۹۹۸ تلفن (۳ خط): ۷۲۶۵۳۴۳ - ۰۳۵۱ فکس: ۷۲۴۵۰۸۷ - ۰۳۵۱
www.pdnsoft.com Email: info@pdnsoft.com

بسته *IP* امکانپذیر مي‌باشد، چنانکه عمل *NAT* هرگز نمي‌تواند در مکان *FORWARD* انجام شود، چرا که تنها مکانهاي مناسب براي آن قبل و بعد از انجام عمل مسيريابي مي‌باشند، و به همين صورت نمي‌توان عمل *filtering* را در مکان *PREROUTING* انجام داد چرا که اين موضوع ناقض قانون تست بسته تنها در يک مکان (فقط يک مرتبه) در موضوع کاري *filter* مي‌باشد. در نتيجه به جاي ساخت يک موضوع کاري گنده و وزين با تقسيم آن به موضوعات کاري مختلف که نيازهاي متفاوتي را مي‌طلبند، پياده‌سازي‌هاي جداگانه‌اي را براي هر يک انجام داده است.

هر موضوع کاري در ابتداي شروع به کار خود، انباره‌اي را در *IPtables* با نام خودش ايجاد مي‌کند، و سپس به منظور اعمال قوانين دسته‌بندي، خود را در مکان‌هاي مناسبِ ساختار پردازش بسته‌هاي *IP* ثبت مي‌کند. ثبت در مکانها با توجه به هدفِ موردِ نظرِ موضوع‌کاري انجام مي‌شود.

IPtables به منظور مديريت بهتر بسته‌هاي شبکه فضاي انباره‌هاي خود را به واحدهايي با نام زنجيره[4] تقسيم کرده است. هر موضوع کاري در هنگام ايجاد انبارة خود، زنجيره‌هايي[5] را متناظر با مکانهاي ثبت در ساختار پردازش بسته‌هاي *IP*، ايجاد مي‌کند تا بدين طريق مديريت بسته‌هاي عبوري از هر مکان با استفاده از قانونهاي موجود در زنجيرة متعلق بدان مکان انجام شود.

وجود زنجيره‌ها در هر انباره، با خصوصيات ذکر شده در بالا، امکان انجام پردازشهاي جداگانه در امتداد مسيرهاي پردازشي مختلف، بر روي بسته‌هاي شبکه، را فراهم مي‌کند.

هر موضوع‌کاري با دريافت يک بسته، رابطِ تعيين تکليف بسته (اين رابط يک فانکشن با نام *ipt_do_table* مي‌باشد) را فراخواني مي‌کند و *IPtables* نيز با توجه به موضوع‌کاري فراخواننده، انبارة مناسب را، و با توجه به مکان دريافت بسته در ساختار پردازش *IP*، زنجيرة مربوطه را مشخص و به جستجو در بين قوانين موجود در آن زنجيره به منظور تعيين تکليف بسته مي‌پردازد.

انباره‌هاي ايجاد شده در *IPtables* با نام جدول[6] شناخته مي‌شوند، که دليل نامگذاري آن به صورت *IPtables* وجود جداول مختلف، مربوط به موضوعات کاري گوناگون، مي‌باشد.

4 Chain
5 Builtin Chains
6 Table

دفتر مرکزی: یزد - خیابان مطهری - مرکز فناوری اقبال - واحد C۲۵ کدپستی: ۸۹۱۷۶۹۷۹۹۸ تلفن (۳ خط): ۷۲۶۵۳۴۳ - ۰۳۵۱ فکس: ۷۲۴۵۰۸۷ - ۰۳۵۱
www.pdnsoft.com Email: info@pdnsoft.com

۱.۲ قانونها در *IPtables*

هر قانون در *IPtables* از سه قسمت تشکيل مي‌شود:

۱-**شناسه**: شامل آدرس مبدا، آدرس مقصد، درگاه ورودي، درگاه خروجي و پروتكل بستة شبكه مي‌باشد. اين اطلاعات، بسته‌هاي شبكة متعلق به جرياني را كه اين قانون نمايندة آن مي‌باشد، به صورت ايستا متمايز مي‌كنند.

۲-**تطابق‌ها**[7]: فانكشنهايي مي‌باشند كه بسته‌هاي شبكه را به طرز دلخواه پردازش مي‌كنند. هر قانون مي‌تواند صفر يا چند تطابق داشته باشد. شرط تطابق بسته با يک قانون در مرحلة اول تطابق با شناسة قانون و در مرحلة دوم پذيرفته شدن توسط تک‌تکِ تطابقها مي‌باشد.

۳-**پردازش**[8]: (مشخص‌كنندة تكليف بسته) يک فانكشن يا نام يک زنجيره و يا يک مورد استاندارد مي‌باشد. پردازش براي يک بسته در صورتي فراخواني خواهد شد كه بسته با قانون تطابق داشته باشد.

- ✗ در حالت استاندارد به صورت مستقيم تكليف بسته را مشخص مي‌كند (براي آگاهي از مقادير استاندارد نگاه كنيد به قسمت جستجو در *IPtables* – فرمانهاي صادره).
- ✗ در صورت بيان پردازش به صورت يک فانكشن، بسته به منظور انجام پردازش در اختيار فانكشن قرار مي‌گيرد و تكليف بسته توسط فانكشن مشخص خواهد شد.
- ✗ فقط زنجيره‌هاي كاربر[9] مي‌توانند به عنوان پردازش مورد استفاده قرار گيرند. اين زنجيره‌ها توسط كاربران *IPtables* تعريف مي‌شوند و متفاوت از زنجيره‌هايي هستند كه توسط موضوعات كاري ايجاد مي‌شوند، چرا كه اين زنجيره‌ها قابل حذف شدن هستند درست بر خلاف زنجيره‌هاي متعلق به موضوعات‌كاري. وجود اين زنجيره‌ها به منظور ايجاد فضاي پردازش انعطاف‌پذير و پويا مي‌باشد. در اين حالت تمام بسته‌هاي مطابق با اين قانون به درون زنجيرة ذكر شده گسيل داده خواهند شد و بدين صورت قانونهاي موجود در آن زنجيره مشخص كنندة تكليف بسته خواهند بود.

تطابقها و پردازشها(به صورت فانكشن) جزو ابزار توسعة *IPtables* به حساب مي‌آيند. اين موضوع بدان معني

7 Maches
8 Target
9 User Chains

دفتر مرکزی: یزد – خیابان مطهری – مرکز فناوری اقبال – واحد C۲۵ کدپستی: ۸۹۱۷۶۹۷۹۹۸ تلفن (۳ خط): ۷۲۶۵۳۴۳ – ۰۳۵۱ فکس: ۷۲۴۵۰۸۷ – ۰۳۵۱
www.pdnsoft.com Email: info@pdnsoft.com

است که ساخت و گسترش آنها نيازي به ايجاد تغيير در *IPtables* ندارد بلکه با استفاده از رابطي که به همين منظور در نظر گرفته شده است اين ابزارها امکان ثبت و استفاده شدن دارند.

قدرت *IPtables* در حد زيادي وابسته به پردازشها و تطابقهاي مناسب و مفيدي مي‌باشد که براي آن ساخته شده‌اند. هر موضوع‌کاري برحسب نياز خود پردازشهاي خاص خود را تعريف مي‌کند، به عنوان مثال *NAT* پردازشهاي *DNAT* و *SNAT* را که فقط در جدول *nat* مجاز مي‌باشند، تعريف مي‌کند. اصولا ساخت تطابقها و پردازشها بر اساس اهداف مورد نظر سازندگان صورت مي‌گيرد که مانعِ استفاده از آنها را در تمام جداول و زنجيره‌ها مي‌گردد.

۲.۲ جستجو در *IPtables*

در پي فراخواني رابط تعيين تکليف بسته توسط يک موضوع‌کاري و مشخص شدن جدول و زنجيرة متناظر، عمل جستجو در بين قانونهاي آن زنجيره آغاز مي‌شود.

جستجو در بين قانونهاي زنجيره به صورت ترتيبي انجام مي‌شود و تا مشخص شدن تکليف بسته ادامه پيدا مي‌کند. هر قانون مي‌تواند چهار گونه فرمان را صادر کند:

۱-**فرمان پذيرش** (*ACCEPT*): در اين صورت عمل جستجو متوقف و به بسته اجازة عبور داده خواهد شد.

۲-**فرمان حذف** (*DROP*): در اين حالت نيز همچون حالت قبل عمل جستجو متوقف مي‌شود ولي بسته از گردونه حذف مي‌شود.

۳- **فرمان ادامة جستجو** (*CONTINUE*): در اين مورد جستجو از قانون بعدي ادامه پيدا مي‌کند.

۴-**فرمان بازگشت** (*RETURN*): به معني بازگشت به زنجيرة فراخواننده و ادامة جستجو از قانون بعد از قانون فراخواننده مي‌باشد. اين مورد هنگامي مورد استفاده قرار مي‌گيرد که ما در يک زنجيرة فراخوانده شده باشيم (زنجيره‌هاي کاربر) و بخواهيم به زنجيرة قبلي بازگرديم.

۵-**فرمان صف‌بندي** (*QUEUE*): در اين حالت بسته براي پردازش در سطح کاربر، به درون صف رانده مي‌شود و عمل جستجو متوقف مي‌شود.

دفتر مرکزی: یزد - خیابان مطهری - مرکز فناوری اقبال - واحد C۲۵ کدپستی: ۸۹۱۷۶۹۷۹۹۸ تلفن (۳ خط): ۷۲۶۵۳۴۳ - ۰۳۵۱ فکس: ۷۲۴۵۰۸۷ - ۰۳۵۱
www.pdnsoft.com Email: info@pdnsoft.com

پردازش هر قانون وظيفة صدور فرمان را بر عهده دارد. درهنگام جستجو، بر اساس شروط اعمال شده توسط هر قانون (شناسه و تطابقها)، تطابق بسته تصميم‌گيري مي‌شود. در صورت بروز تطابق پردازش قانون فراخواني و فرمان توسط آن صادر مي‌شود.

در اين جستجو، حصول به تطابق عامل توقف جستجو نيست بلكه فرمان صادره از سوي پردازشِ قانونِ تطابق يافته مبناي تصمصم‌گيري مي‌باشد. به عبارتي جستجو در صورت مشخص شدن تكليف بسته، متوقف خواهد شد.

۳.۲ سطوح مختلف *IPtables*

ساختار پالايش، مجموعه‌اي از دو ويرايش در دو سطح هسته و كابر مي‌باشد. سطح هسته[10] وظيفة مديريت بسته هاي شبكه و انجام عمل جستجو، و سطح كاربر[11] وظيفة مديريت انباره‌ها را برعهده دارند.

در سطح هسته قانونها توسط ماژول *ip_tables* نگهداري و بسته ها توسط آن مديريت مي‌شوند. در سطح كاربر دستور *iptables* در پوستة[12] لينوكس، رابط كاربران در سطح كاربر با ماژول *ip_tables* در سطح هسته، وظيفة مديريت اطلاعات موجود در انباره‌ها را بر عهده دارد.

۴.۲ فعاليتهاي مديريتي كاربر

تمامي فعاليتها مديريتي توسط كاربران سيستم و به وسيلة دستور *iptables* در پوستة لينوكس انجام مي‌شود. عمدة اين فعاليتها عبارتند از:

۱-**اضافه، حذف و جايگزيني قانون**: از مهمترين و پركاربردترين فعاليتهاي مديريتي مي‌باشند. در تعريف هر قانون، كاربر بعد از مشخص كردن جدول و زنجيره‌اي كه خواستار مديريت قانون در آن مي‌باشد، اقدام به تعريف شناسه، بيان تطابقها و در پايان، بيان پردازش مربوطه مي‌كند. با توجه به ذخيرة ترتيبي قانونها از شمارة قانون براي انجام اعمال حذف و جايگزيني مي‌توان استفاده كرد. مثال:

iptables -t filter -A FORWARD -s 1.1.1.1 -d 2.2.2.2 -m state --state NEW -j DROP

10 Kernel Space
11 User Space
12 Shell

دفتر مرکزی: یزد - خیابان مطهری - مرکز فناوری اقبال - واحد C۲۵ کدپستی: ۸۹۱۷۶۹۷۹۹۸ تلفن (۳ خط): ۷۲۶۵۳۴۳ - ۰۳۵۱ فکس: ۷۲۴۵۰۸۷ - ۰۳۵۱
www.pdnsoft.com Email: info@pdnsoft.com

در این مثال یک قانون به جدول *filter* زنجیرهٔ *FORWARD* اضافه خواهد شد. شناسهٔ این قانون دارای آدرس مبدا ۱.۱.۱.۱ و آدرس مقصد ۲.۲.۲.۲ می‌باشد. بیان نشدن درگاه‌های ورودی و خروجی و پروتکل مربوطه به معنای اجازهٔ پذیرش تمامی موارد می‌باشد. این قانون از تطابق *state* و پردازش استاندارد با مقدار *DROP* استفاده می‌کند. این قانون تمامی بسته‌های ارسالی از ۱.۱.۱.۱ به ۲.۲.۲.۲ را که در مرحلهٔ برقراری ارتباط باشند، حذف خواهد کرد.

۲-**تغییر سیاست زنجیره**: *IPtables* امکان تعریف سیاست‌زنجیره[۱۳] را برای زنجیره‌های *Built-in* فراهم می‌کند. در این صورت اگر قانونهای موجود در یک زنجیره نتوانستند تکلیف بسته را مشخص کنند از سیاست زنجیره برای تعیین تکلیف بسته استفاده می‌شود. سیاست زنجیره می‌تواند مقادیر *ACCEPT* و *DROP* را اختیار کند. مثال:

```
iptables -t filter -P INPUT DROP
```

چنانکه مشاهده می‌شود سیاست زنجیرهٔ *INPUT* در جدول *filter* ، *DROP* تعریف شده‌است. به عبارتی از ورود بسته‌هایی که قانونی برای آنها وجود ندارد به سیستم محلی، جلوگیری می‌شود.

۳-**ایجاد، حذف و تغییرِنام زنجیره‌های کاربر**: کاربران می‌توانند برای ایجاد محیط پردازش مناسب، زنجیره‌هایی را در جداول تعریف کنند. می‌توان از این زنجیره‌ها به عنوان پردازش در تعریف قانونهای آن جدول استفاده کرد. این زنجیره‌ها توانایی پذیرش سیاست زنجیره را ندارند. مثال:

```
iptables -t nat -N newCHIAN
```

این دستور زنجیرهٔ تازه‌ای را با نام *newCHAIN* در جدول *nat* ایجاد می‌کند.

۴-**پاک‌سازی جداول**[۱۴]: با استفاده از این دستور کاربر قادر خواهد بود تا تمام قانونهای موجود در یک جدول را حذف کنند.

13 Chain Policy
14 Flush

دفتر مرکزی: یزد - خیابان مطهری - مرکز فناوری اقبال - واحد C۲۵ کدپستی: ۸۹۱۷۶۹۷۹۹۸ تلفن (۳ خط): ۷۲۶۵۳۴۳ - ۰۳۵۱ فکس: ۷۲۴۵۰۸۷ - ۰۳۵۱
www.pdnsoft.com Email: info@pdnsoft.com

۵.۲ طریقه نگهداري اطلاعات جداول در سطح هسته

تفکر حاکم در پیاده‌سازي *IPtables* استفاده از حافظهٔ پیوسته و ذخیره‌سازي اطلاعات لازم به صورت متوالي در درون این حافظهٔ پیوسته مي‌باشد. عمده دلیل روي‌آوري پیاده‌سازان *IPtables* به این شیوه، فراهم کردن بهینه‌ترین محیط براي انجام جستجوي ترتیبي مي‌باشد، چرا که سیر کردن در یک فضاي حافظه‌اي پیوسته به مراتب ساده‌تر و سریعتر از حرکت در یک فضاي حافظه‌اي پراکنده مي‌باشد.

از سوي دیگر به دلیل تمرکز فعالیتهاي مدیریتي در سطح کاربر، انجام هر گونه تغییر در انباره مستلزم انتقال انبارهٔ مورد درخواست به سطح کاربر و، بعد از انجام به‌هنگام‌سازي انباره در سطح کاربر، انتقال انبارهٔ به‌هنگام‌شده از سطح کاربر به سطح هسته و جایگزیني با انبارهٔ قدیمي مي‌باشد. انجام این امور با حافظه‌هاي پیوسته، به مراتب، ساده‌تر خواهد بود چرا که هر انتقال را مي‌توان با کپي کردن حافظهٔ مربوط به انباره، از سطح کاربر به سطح هسته و بالعکس، انجام داد.

این تفکر باعث روي‌آوري پیاده‌سازان به استفاده از ابتکارت جالبي در تعریف ساختارها نیز شده‌است. به منظور دسترسي مناسب و ساده‌تر به فضاي انتهایي ساختارهایي که به صورت متوالي در یک فضاي پیوسته ذخیره مي‌شوند، *IPtables* از تعریف آرایه‌هایي با طول صفر در انتهاي این ساختارها استفاده مي‌کند. این آرایه‌ها به هیچ عنوان فضایي را اشغال نمي‌کنند، بلکه نام آنها اشاره‌گري به انتهاي ساختار مربوطه خواهد بود و در هنگام برنامه‌نویسي مي‌توان از نام آنها براي دسترسي به فضاي دنبالهٔ این ساختار استفاده کرد. استفاده از این تعاریف باعث جابجایي آسان در حافظه مي‌شود.

۶.۲ طریقه ذخیره‌سازي قانونها

یک قانون در *IPtables* به صورت یک حافظهٔ پیوسته مي‌باشد که اطلاعت یک قانون به ترتیبِ سرآیند، تطابقها و پردازش در آن قرار مي‌گیرند. ساختار سرآیند، در پیاده‌سازي انجام شده، علاوه بر شناسه، فیلدهاي گوناگوني را براي شناسایي طول قانون و مکان پردازش قانون، با خود یدک مي‌کشد.

تطابقها و پردازشها مي‌توانند اطلاعات مختلفي را از کاربر براي انجام پردازشهاي خود دریافت کنند. این

دفتر مرکزی: یزد - خیابان مطهری - مرکز فناوری اقبال - واحد C۲۵ کدپستی: ۸۹۱۷۶۹۷۹۹۸ تلفن (۳ خط): ۷۲۶۵۳۴۳ - ۰۳۵۱ فکس: ۷۲۴۵۰۸۷ - ۰۳۵۱
www.pdnsoft.com Email: info@pdnsoft.com

اطلاعات در حافظة قانون در ادامة حافظة متعلق به تطابق و يا پردازش مربوطه قرار مي‌گيرد(قسمتهاي تيره در شكل زير). اندازة حافظة اين اطلاعات بستگي به پردازش و يا تطابق مربوطه داشته و توسط آنها در هنگام ثبت مشخص مي‌شود. شمايل حافظه‌اي يک قانون در تصوير ۲ نمايش داده شده است.

تصوير ۲ : شمايل حافظه‌اي يک قانون

۳ پارامترهاي كارآيي

سرعت جستجو: پيچيدگي الگوريتم جستجوي خطي از مرتبة $O(n)$ مي‌باشد، به عبارتي با افزايش تعداد قانونهاي موجود در انباره، انتظار مي‌رود كه سرعت فرآيند جستجو كاهش يابد.

يكي از مزيتهاي نسبي *IPtables* براي انجام جستجوي خطي، ذخيره‌سازي قانونها به صورت متوالي در يک حافظة پيوسته مي‌باشد. در آزمايشهاي انجام شده مشخص شد كه اين گونه پياده‌سازي، با تعداد قوانين ۱۰۰۰-۱۲۰۰ ، هيچگونه بار اضافي بر سيستم تحميل نمي‌كند اما در ۲۰۰۰، كارآيي شبكه به نصف كاهش مي‌يابد.

به عبارتي پيوسته بودن حافظه به عنوان يک استراتژي مناسب در پياده‌سازي الگوريتم جستجوي خطي توانسته تا با بهره‌گيري مناسب از پردازندة سيستم، پيچيدگي الگوريتم جستجوي خطي را براي ۱۰۰۰ قانون به صورت $O(1)$ نگه دارد. دستيابي به اين موضوع بدون شک ارتباط مستقيم با معماري پردازنده و معماري سيستم عامل استفاده شده دارد.

اما عدد ۱۰۰۰ در دنياي كنوني ديگر عدد بزرگي به حساب نمي‌آيد. امروزه نياز به تعريف و مديريت بيش از ۳۰.۰۰۰ قانون در ديواره‌هاي آتش وجود دارد، كه تصور حمايت از اين تعداد قانون توسط *IPtables* كاملا دور از ذهن و غير عملي مي‌باشد. اين موضوع با انجام تست عملي نيز ثابت شد چنانكه در تعداد ۱۱۰۰۰ قانون، كارآيي يک شبكه با ظرفيت *100mbps* به عدد *4mps* كاهش يافت.

آنچه كه به عنوان ضعف اصلي *IPtables* به حساب مي‌آيد كاهش شديد كارآيي شبكه در تعداد بالاي قانونها

دفتر مرکزی: یزد - خیابان مطهری - مرکز فناوری اقبال - واحد C۲۵ کدپستی: ۸۹۱۷۶۹۷۹۹۸ تلفن (۳ خط): ۷۲۶۵۳۴۳ - ۰۳۵۱ فکس: ۷۲۴۵۰۸۷ - ۰۳۵۱
www.pdnsoft.com Email: info@pdnsoft.com

(نياز اصلي ديواره‌هاي آتش امروزي) مي‌باشد.

حافظة مصرفي: اصولا معضل اصلي در الگوريتمهاي دسته‌بندي، تقابل حافظه و زمان مي‌باشد. بدان معني كه توجه و حصول به كارآيي مناسب در يكي از اين دو، باعث قرباني شدن ديگري مي‌شود. الگوريتمهايي داراي مقدار حافظة معقول و در مقابل زمان پاسخگويي نامناسب و تعدادي نيز حافظة زيادي را براي رسيدن به زمان مناسب اشغال كرده‌اند. اندک الگوريتمهايي با كارآيي مناسب در هر دو حوزه نيز وجود دارند (*Hicuts*).

جستجوي خطي از جنبة تئوريک جزو الگوريتمهايي به حساب مي‌آيد كه زمان را قرباني حافظة اشغالي كرده است، چرا كه براي ذخيره‌سازي قانونها از هيچگونه ساختار اضافي (در كنار ساختار قانونها) استفاده نمي‌كند و آنها را به صورت يک ليست نگهداري مي‌كند، در مقابل جستجوي خطي آن از مرتبة $O(n$) مي‌باشد.

IPtables به عنوان يک پياده‌سازي از الگوريتمهاي جستجوي خطي، جزو آن دسته از پياده‌سازيها به حساب مي‌آيد كه در هر دو زمينه ضعف دارد.

در پياده سازي *IPtables* براي حمايت از چندپردازندگي[15] و پرهيز از استفاده از *Lock*هاي سيستم به منظور مديريت نواحي بحراني ايجاد شده، حاصل از همروندي فعاليت پردازنده‌ها، و حصول به سرعت بيشتر و نفس منطق چندپردازندگي، به ازاي هر پردازنده يک كپي از انباره‌هاي موجود در *IPtables* تهيه مي‌شود. بدين صورت هر پردازنده بر روي كپي متناظر خود تمركز كرده و از ايجاد مزاحمت توسط پردازنده‌هاي ديگر نيز مصون مي‌باشد.

اين موضوع به طرز قابل توجهي حافظة مصرفي توسط *iptables* را افزايش داده است. با توجه به اينكه تنها عمل نوشتاري كه توسط پردازنده ها انجام مي‌شود به‌هنگام‌سازي شمارنده‌هاي قانونها مي‌باشد (شمارنده‌ها نمايشگر تعداد و طول بسته‌هاي تطابق يافته با قانون مربوطه مي‌باشند) و طريقة استفاده از ديگر فضاي اشغالي به صورت خواندني مي‌باشد، حجم زيادي از اين فضاي اشغال شده، كاملا، غير ضروري مي‌باشد.

سرعت به‌هنگام‌سازي: تمام فعاليتهاي به هنگام‌سازي در سطح كاربر انجام مي‌شود. صدور هر فرمان به‌هنگام‌سازي، از جانب كاربر، مستلزم انجام مراحل زير مي‌باشد:

۱-انتقال حافظة انبارة مورد نظر از سطح هسته به سطح كاربر

15 SMP: Symmetric MultiProcessor

دفتر مرکزی: یزد -خیابان مطهری-مرکز فناوری اقبال - واحد C۲۵ کدپستی: ۸۹۱۷۶۹۷۹۹۸ تلفن (۳ خط): ۷۲۶۵۳۴۳ - ۰۳۵۱ فکس: ۷۲۴۵۰۸۷ - ۰۳۵۱
www.pdnsoft.com Email: info@pdnsoft.com

۲-انجام تغییرات خواسته شده در انباره

۳-انتقال انبارة به هنگام شده به سطح هسته

۴-جاگزين كردن اطلاعات قديمي با اطلاعات جديد.

حجم زياد تبادل اطلاعات بين سطوح هسته و كاربر و انجام فعاليتهاي پيچيدة مديريت حافظه در هر مرتبه انجام تغييرات، سرعت به‌هنگام‌سازي را در حد قابل توجهي كاهش داده است.

با توجه به اين كاستي، استفاده از *IPtables* در يک محيط محاوره‌اي به هيچ عنوان مناسب نمي‌باشد.

مقياس‌پذيري در تعدادِ فيدهاي استفاده شده براي دسته‌بندي: هر قانون در *IPtables* از سه جزءِ شناسه، تطابقها و پردازش تشكيل مي‌شود. يک قانون مي‌تواند هر تعداد تطابق را اختيار كند كه اين موضوع همان مسئلة مقياس‌پذيري مي‌باشد.

از طرف ديگر تطابقها و پردازشها جزو ابزار توسعة *IPtables* شناخته مي‌شوند كه ساخت آنها نيازي به تغيير در *IPtables* ندارد. در نتيجه مي‌توان تطابقاي دلخواه را نيز پياده‌سازي كرد.

امكان استفاده از تطابقهاي گوناگون، بدون محدوديت در تعداد، در يک قانون، امكان دسته بندي بسته‌هاي شبكه بر اساس فيلدهاي مختلف را فراهم مي‌آورد.

اين موضوع يكي از پارامترهاي بسيار مثبت و زيباي *IPtables* مي‌باشد.

دفتر مرکزی: یزد -خیابان مطهری-مرکز فناوری اقبال - واحد C۲۵ کدپستی: ۸۹۱۷۶۹۷۹۹۸ تلفن (۳ خط): ۷۲۶۵۳۴۳ - ۰۳۵۱ فکس: ۷۲۴۵۰۸۷ - ۰۳۵۱
www.pdnsoft.com Email: info@pdnsoft.com