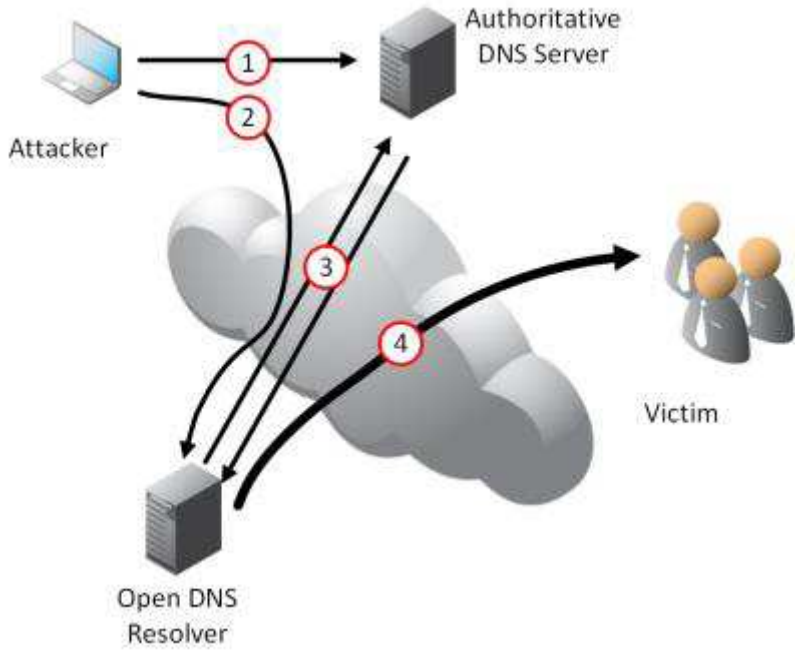
مشکلات امنیتی موجود بر روی سرویس Open DNS –



مشکلات امنیتی موجود بر روی سرویس Open DNS –

تاریخ تنظیم : بهمن ۱۳۹۵

گروه شرکت‌های شاتل

فهرست مطالب

Open DNS چیست؟

شرکت شاتل همواره در کنار اینکه خود را متعهد به ارایه سرویس مطلوب به کاربران میدانسته در زمینه امنیت سایبری نیز مسئول و همراه کاربران خود بوده است.متاسفانه با بررسی های انجام شده مشاهده می شود که در شبکه اینترنت حفره های امنیتی بسیاری موجود است که باعث ایجاد مشکلات متعددی برای کاربران خواهد شد.

در این فایل قصد داریم در مورد حفره امنیتی Open Resolver یا Open DNS و مشکلاتی که می تواند برای کاربران ایجاد کند صحبت کنیم.

به صورت روزانه هکرهایی در شبکه جهانی اینترنت مشغول جست و جو و یافتن پورت هایی هستند که می توانند از آن ها سوء استفاده کرده و با آن به مقاصد نادرست خود برسند.

یکی از این پورت ها که می تواند احتمال سوء استفاده را برای این هکر ها ایجاد کند پورت ۵۳ و به همراه آن فعال بودن قابلیت Open Relay است.

در این حالت با توجه به باز بودن پورت ۵۳ UDP روی سرویس شما و پاسخگو بودن سرویس DNS به تمام کویری‌ها، هکرهای فعال در شبکه اینترنت از سرویس شما برای حمله به سمت سرورهای اینترنتی استفاده کنند و این موضوع ممکن است بدون اینکه شما در جریان باشید مشکلاتی را برای شما به عنوان مسئول و مالک سرویس ایجاد کند که از آن جمله می‌توان به موارد زیر اشاره کرد:

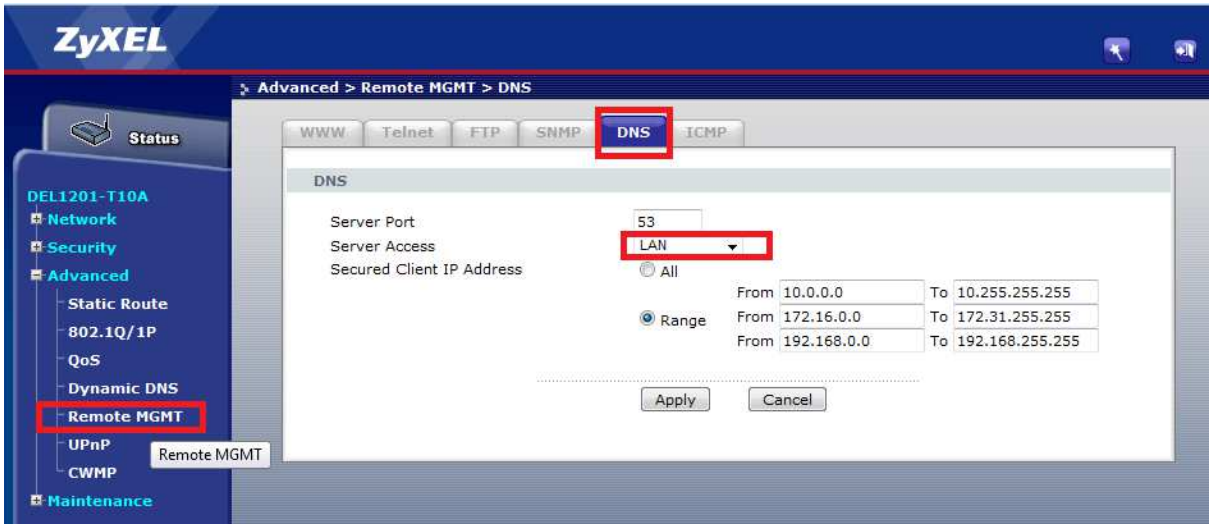
۱- مصرف ترافیک ناخواسته سرویس بدون اطلاع شما
۲- اشغال پهنای باند سرویس ADSL بدون اطلاع شما و به سبب آن کاهش سرعت سرویس اینترنت شما
۳- ایجاد مشکلات امنیتی و قانونی به دلیل Attack به سرورهای موجود در شبکه اینترنت توسط IP شما
۴- عدم باز شدن بعضی از سایت ها و یا عدم ارسال ایمیل به دلیل آلوده شناخته شدن IP سرویس شما
۵- امکان استعلام مشخصات شما از طرف نهادهای حاکمتی در صورت استفاده شدن از سرویس شما برای حمله و علی الخصوص حمله به زیرساخت‌های کشور
۶- امکان پیگیری قضایی علیه شما از طرف نهادهایی که از طریق سرویس شما مورد حمله قرار گرفته‌اند.

از آنجایی که در اغلب موارد مشاهده شده، علت Open DNS شدن مشترکین، تنظیم‌های اشتباه بر روی مودم/روتر سرویس ایشان و فعال بودن Open DNS Relay روی درگاه اینترنت ایشان بوده است، برای حل این مشکل بر روی مودم ADSL ، سرویس PTP و ... ما در این جا روش غیرفعال کردن این قابلیت را در چند نمونه روتر درج کرده ایم که می توانید با استفاده از راهنمایی های انجام شده این مورد را بررسی بفرمایید.

در صورتی که دستگاه شما در بین این لیست نیست می توانید با جست و جو در کنسول روتر این گزینه را بیابید و قابلیت مورد نظر را غیرفعال بفرمایید.

DEL 1201

برای انجام این کار کافیست از سربرگ Advance وارد قسمت Remote MGMT شده و گزینه DNS را انتخاب کنید.
در سربرگ DNS می بایست Service Access را بر روی LAN قرار دهید. با انجام این کار دسترسی به سرویس DNS مودم فقط از طریق شبکه داخلی شما فراهم خواهد بود.

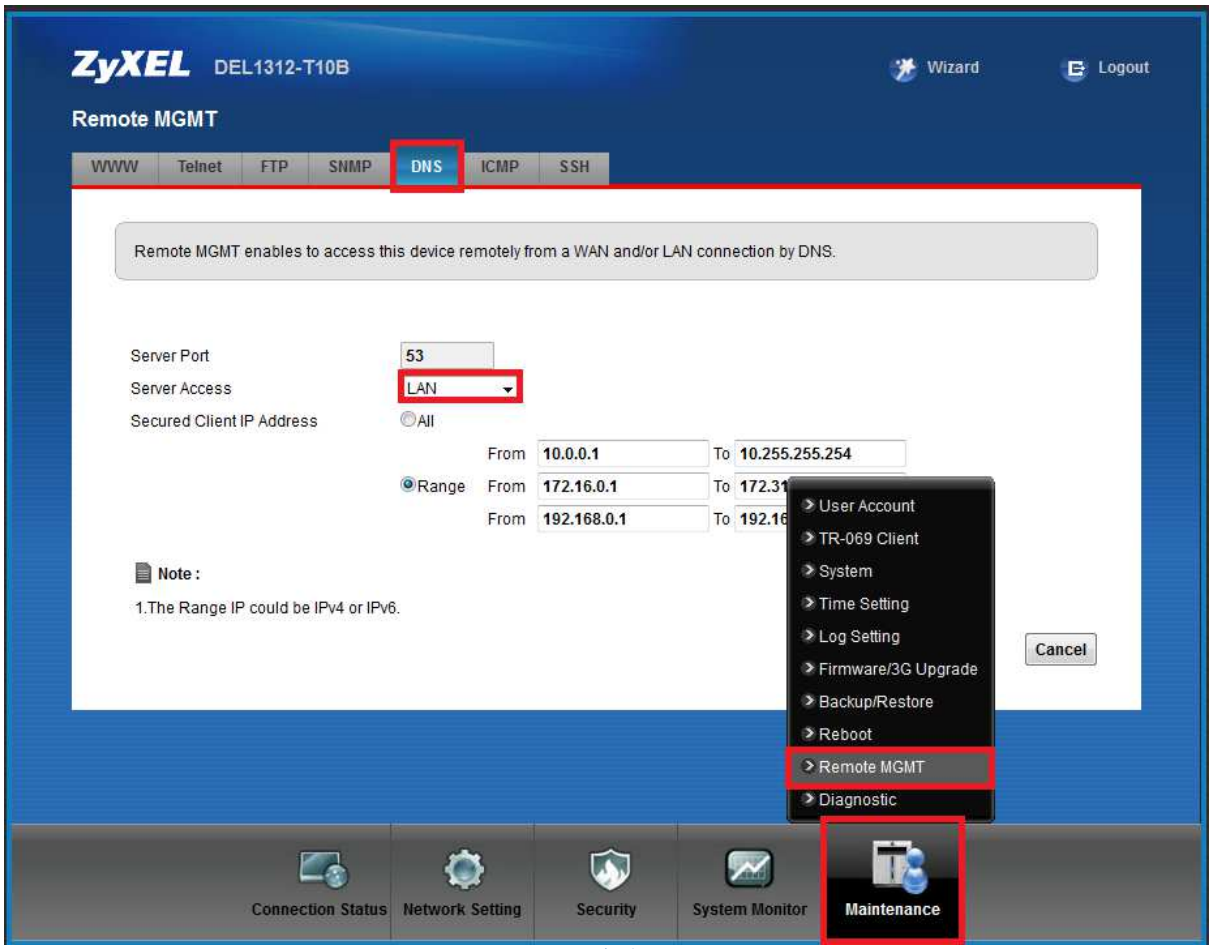


شکل ۱

DEL 1312 – 1202

برای انجام این کار کافیست از سربرگ Maintenance وارد قسمت Remote MGMT شده و گزینه DNS را انتخاب کنید.

در سربرگ DNS می بایست Service Access را بر روی LAN قرار دهید. با انجام این کار دسترسی به سرویس DNS مودم فقط از طریق شبکه داخلی شما فراهم خواهد بود.

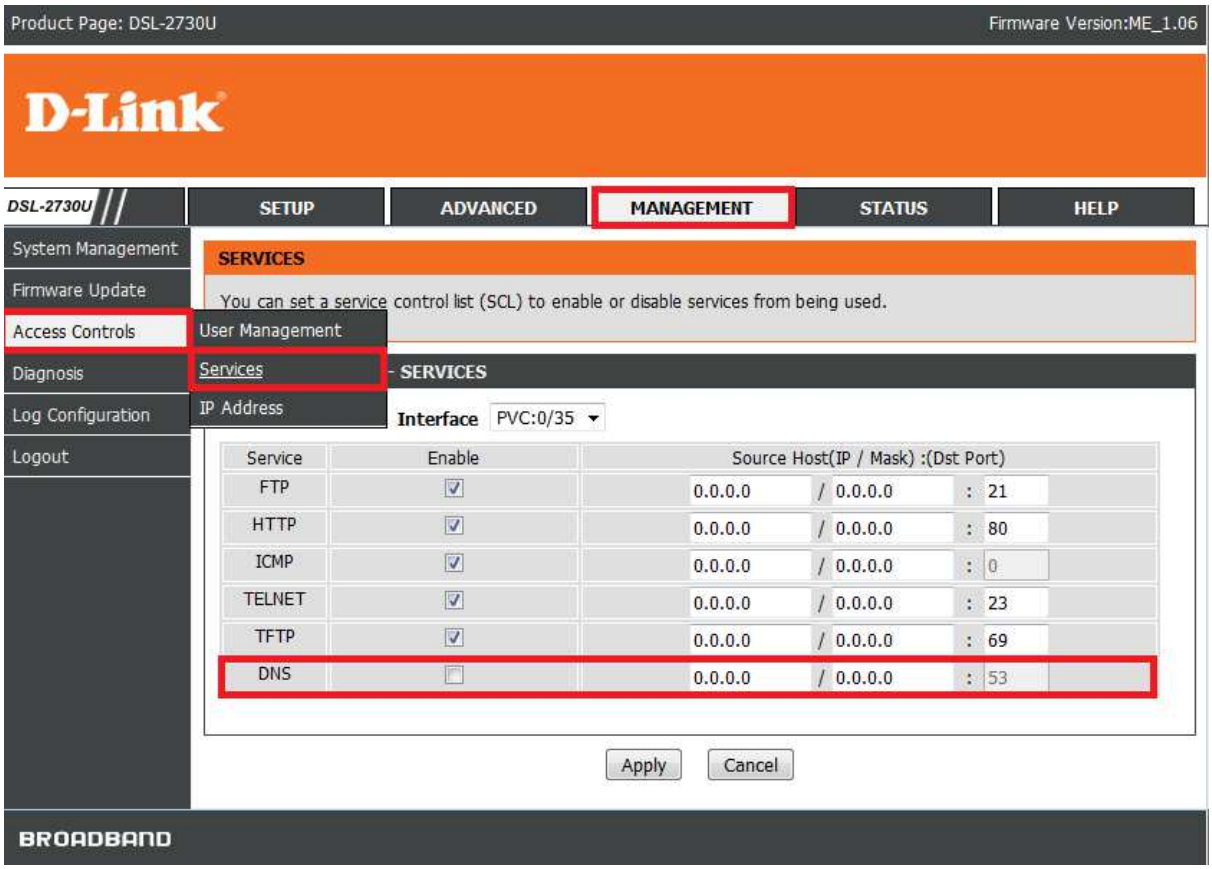


شکل ۲

Dlink

برای انجام این کار کافیست از سربرگ Management وارد قسمت Access Control شده و گزینه Services را انتخاب کنید.

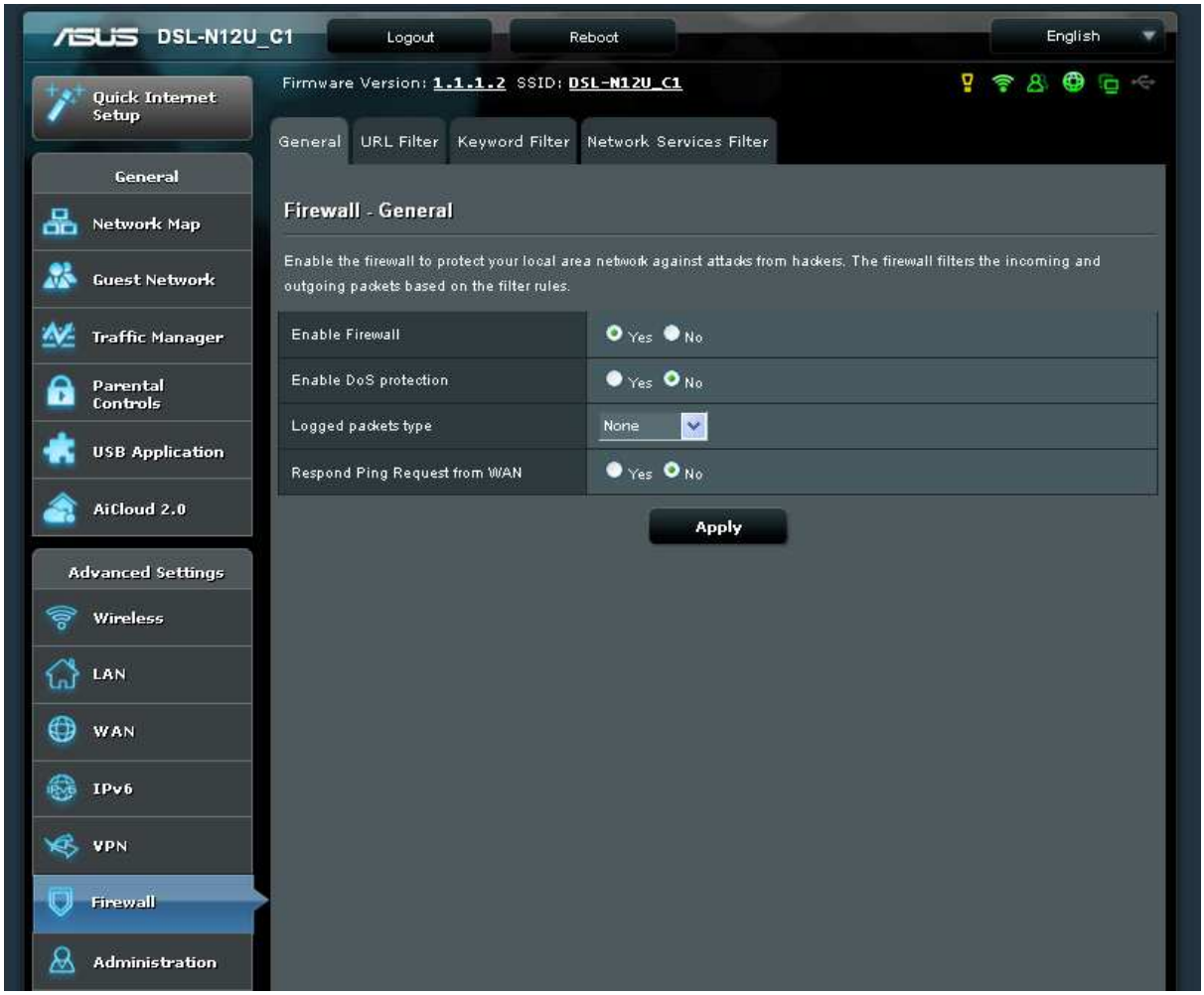
در سربرگ Services می بایست Interface را بر روی 0/35 قرار داده و بعد از آن با برداشتن تیک گزینه DNS بر روی Apply کلیک کنید.



شکل ۳

Asus DSL-N12U-C1

برای انجام این کار می بایست از قسمت Advance setup وارد قسمت Firewall شده و Firewall مودم خود را Enable کنید.



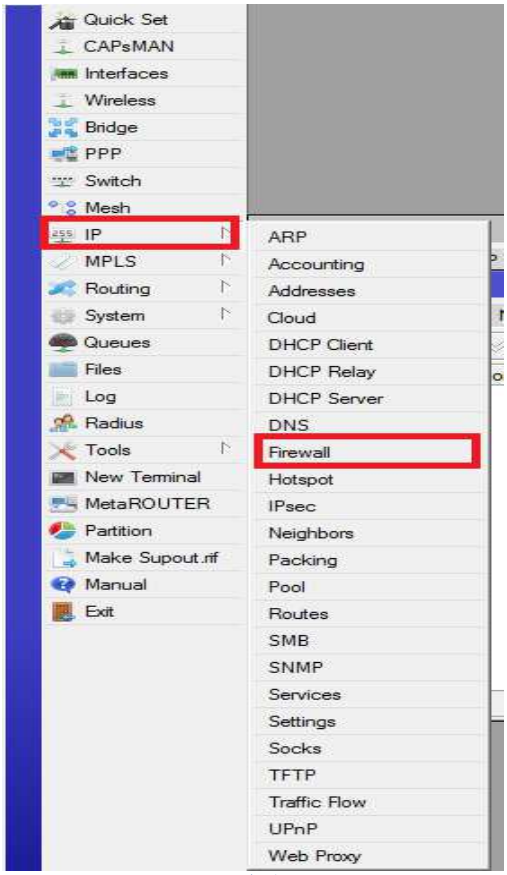
شکل ٤

Mikrotik

جهت بررسی پس از لاگین در نرم افزار Winbox با توجه به تصویر طبق آدرس مسیر را دنبال کنید

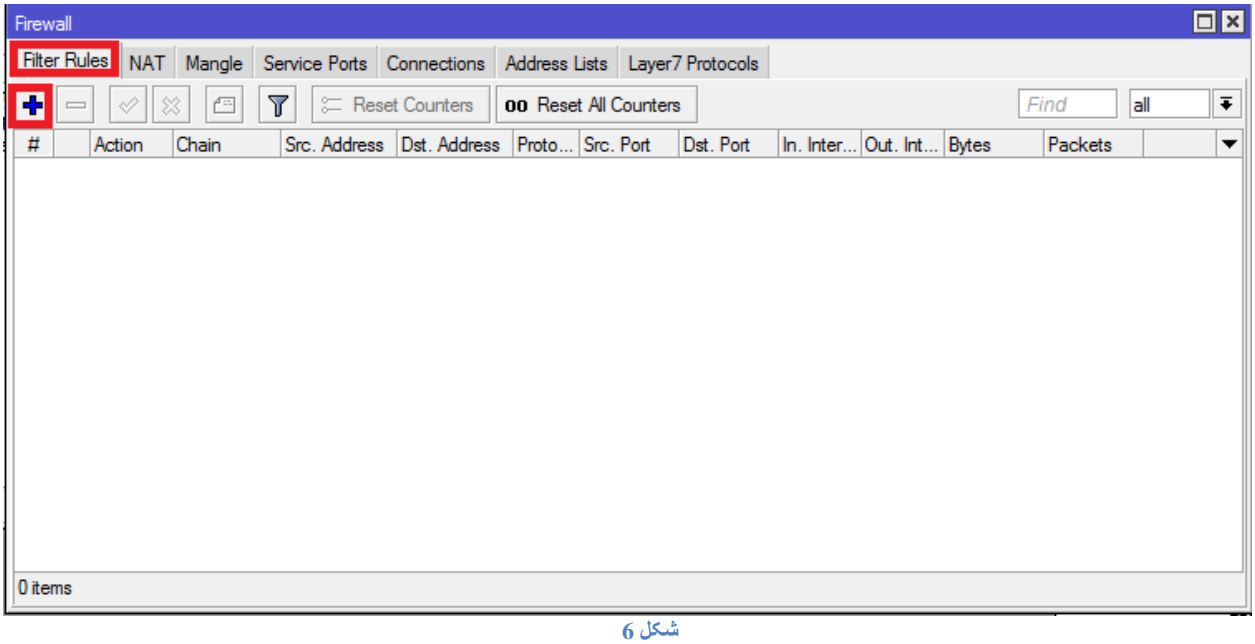
IP>Firewall>>Filter Rules

در این قسمت باید یک Rule برای فایروال تعریف کرد با توجه به تصویر از قسمت IP وارد قسمت Firewall می شویم



شکل 5

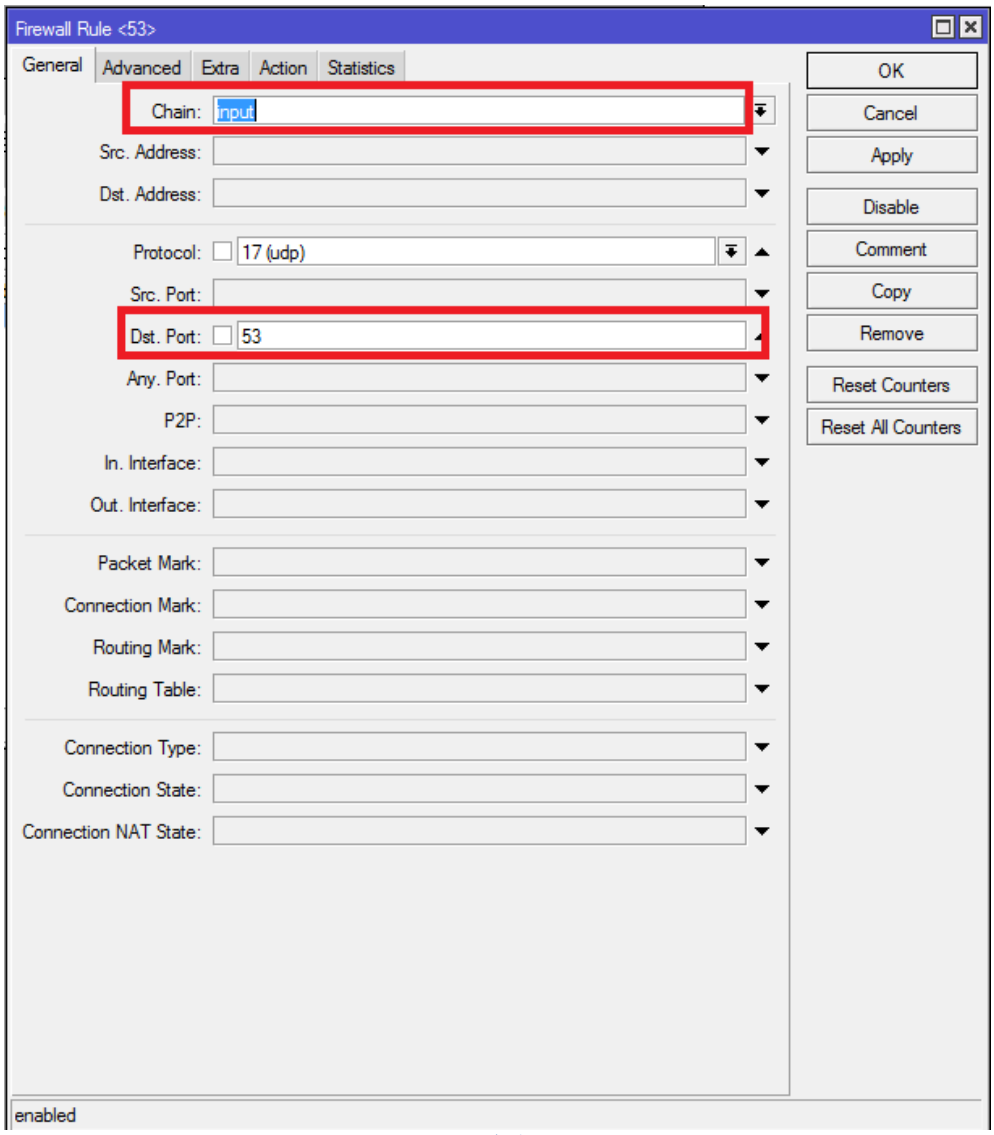
سپس در سربرگ Filter Rules ب گزینه ی + انتخاب می کنیم



شکل 6

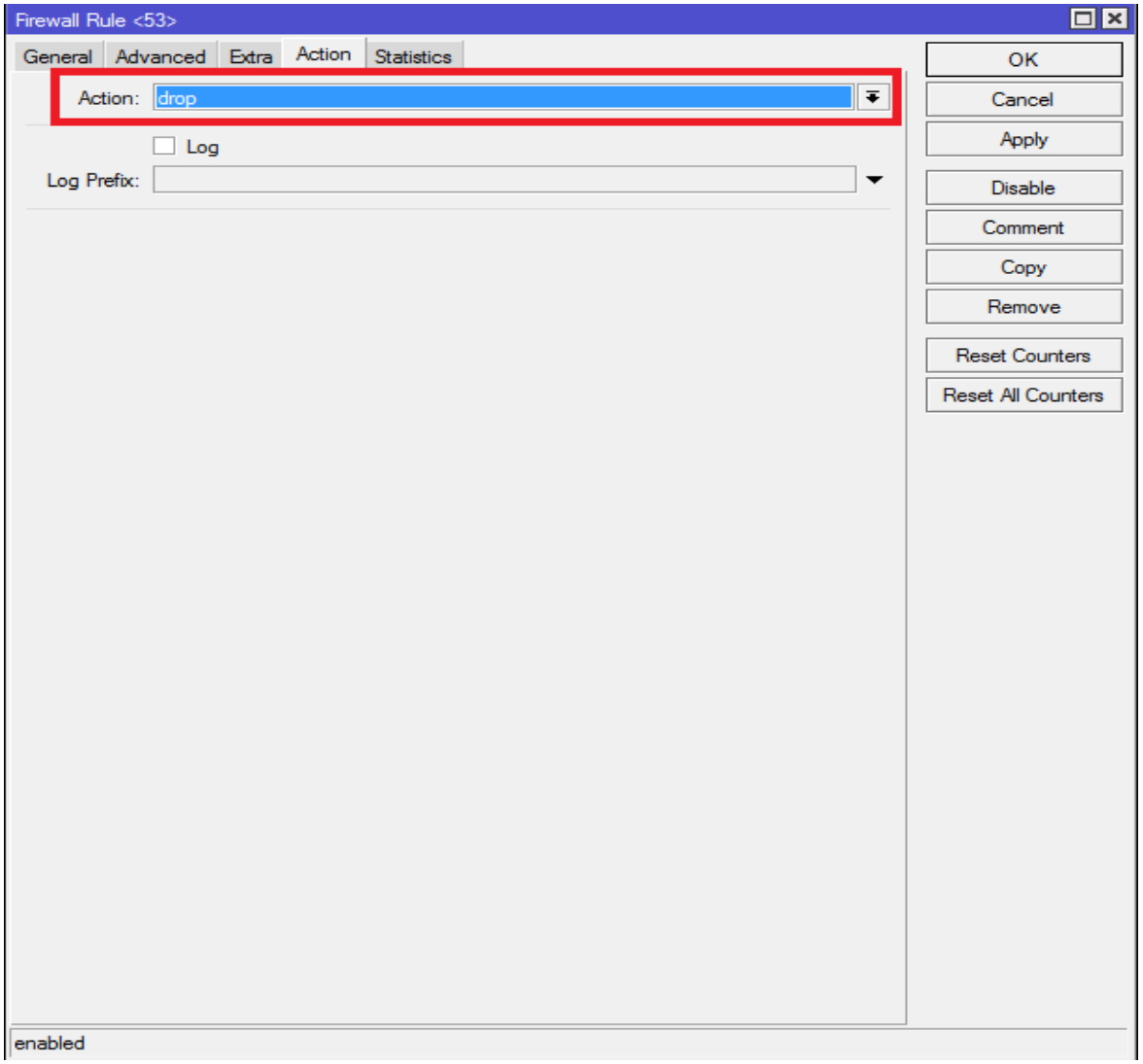
در صفحه ی باز شده Rule را بدین شرح تعریف می کنیم

Chain: Input
Protocol: UDP
Dst Port:53
Action : Drop



شکل 7

همچنین Action را بر روی حالت Drop قرار می دهیم

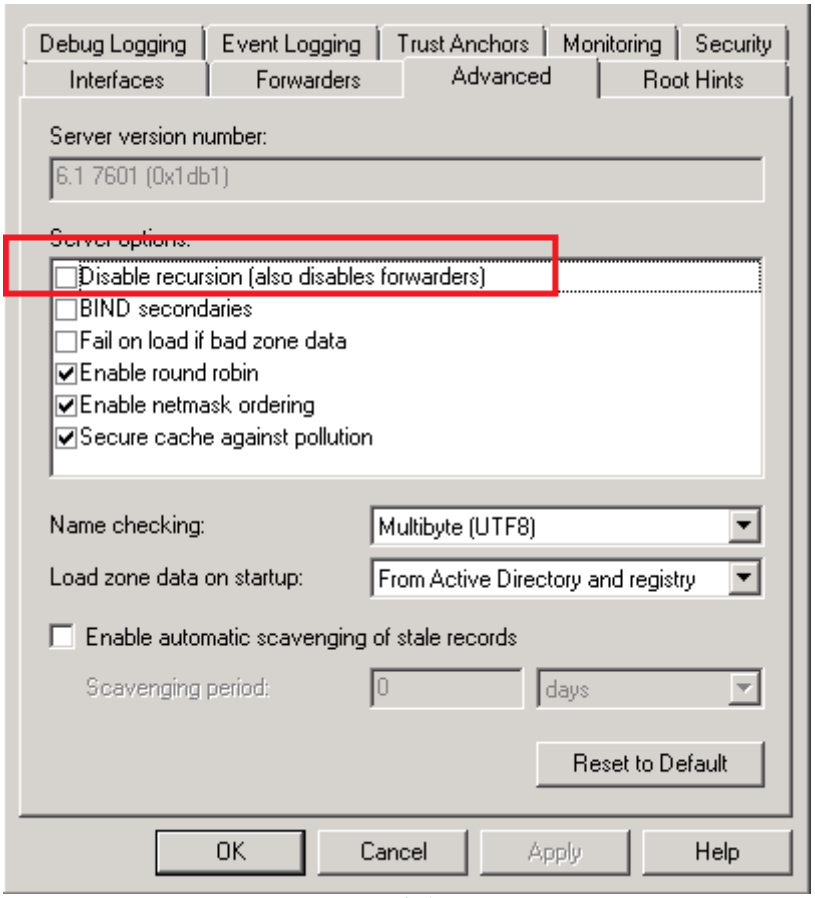


شکل 8

سپس تنظیمات را OK کنید .

غیر فعال سازی Recursive DNS بر روی سرورهای ویندوز

۱- به مسیر Start > Administrative Tools > DNS مراجعه فرمایید.
۲- بر روی نام سرور کلیک راست کنید و Properties را انتخاب نمایید.
۳- از تب Advanced گزینه Disable recursion (also disables forwarders) را انتخاب کنید.



شکل 9