NETLOG

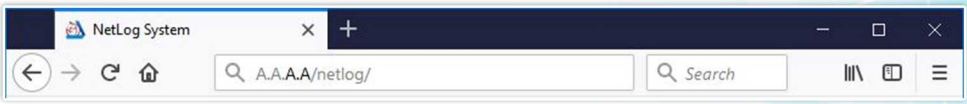
Network Surveillance

راهنمای پنل مدیریت

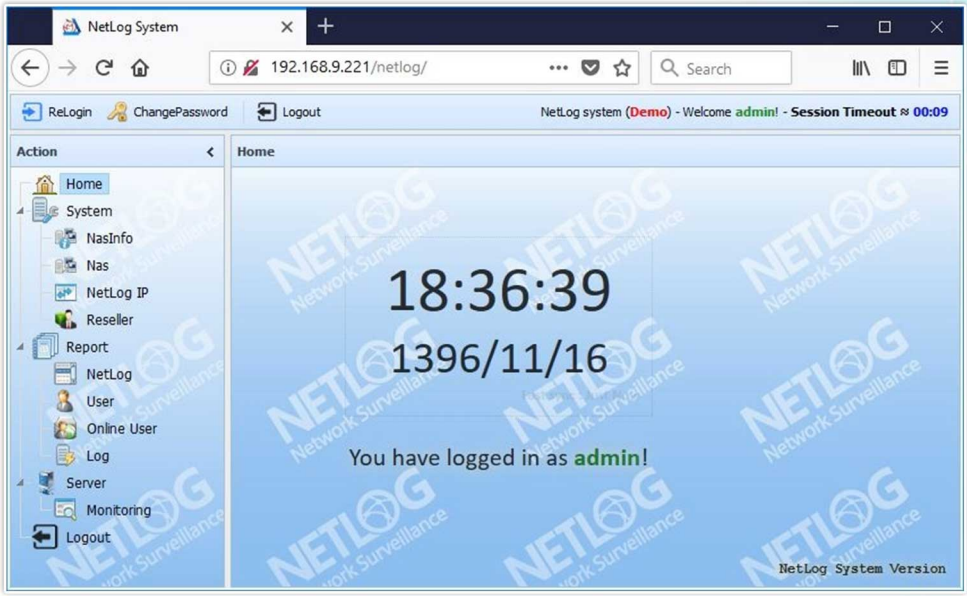
NETLOG
Network Surveillance

راهنمای پنل مدیریت Netlog

همـان طـور کـه قبلا گفتـه شـد از مزایای نـرم افـزار Netlog کارکـرد تحت وب این برنامه می باشد.
برای ورود به پنل کاربری در مرورگر خود آدرس A.A.A.A/netlog را وارد نماییـد. بـه جای مقادیر A.A.A.A آی پی مربـوط به Netlog که در هنگام نصب تعیین نمودید را وارد نمایید.



بـا ورود بـه پنـل کاربـری محیطـی ماننـد تصویـر زیـر را مشـاهده خواهیـد کرد.



در بخش Action (سمت چپ محیط کاربری) سه منوی کلی ، System Report و Server را مشاهده می کنید که هر کدام شامل چند زیرمنو می باشد که به توضیح هر یک خواهیم پرداخت.

منوی System

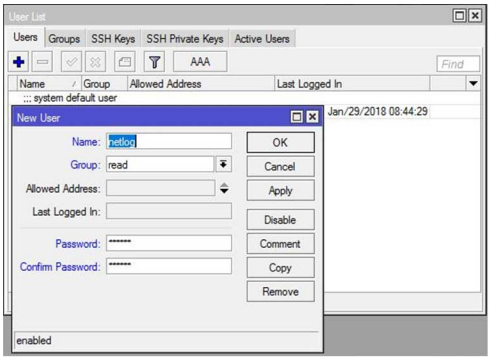
در این منو تنظیمات لازم برای برقراری ارتباط سرور Netlog با Router و خواندن کاربران متصل به شبکه و همچنین تنظیمات آی پی هایی که باید لاگ برای آن ها تهیه گردد، مشخص می شود.

System>NasInfo

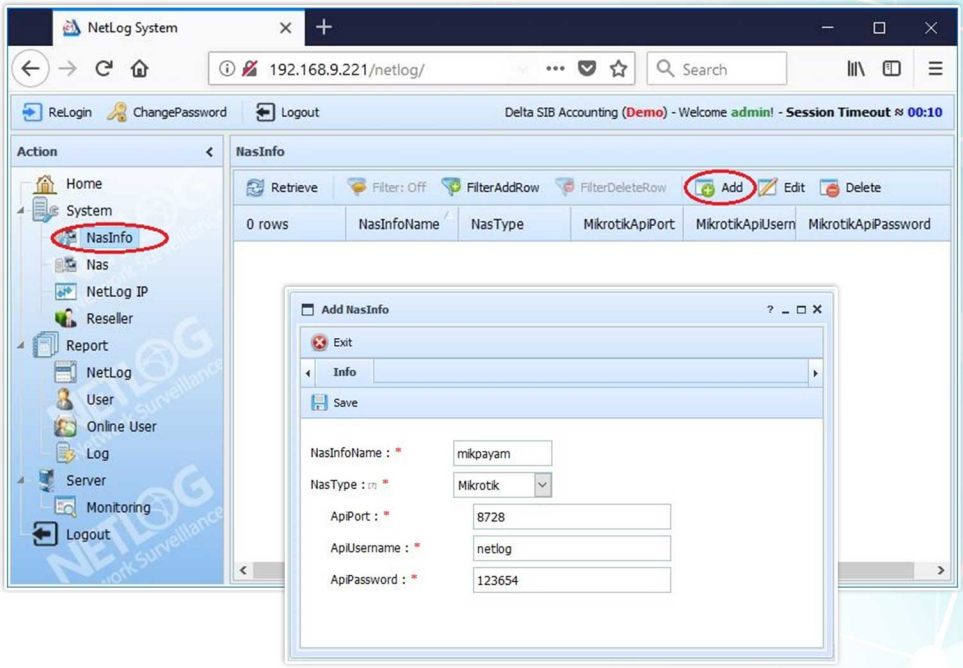
با انتخاب گزینه NasInfo در پخش راست صفحه تنظیمات مربوط به آن را مشاهده خواهید کرد.

توجه داشته باشید که در این راهنما تنظیمات لازم برای اتصال Netlog به روتر MikroTik توضیح داده شده است.

برای اتصال Netlog به میکروتیک نیاز است تا ابتدا یک یوزر در میکروتیک تعریف شود. برای این کار در میکروتیک وارد منوی System>Users می شویم و روی کلید + کلیک می کنیم. در قسمت Name یک نام دلخواه و درقسمت Password نیز رمز مورد نظر خود را وارد می نماییم. دقت کنید که این نام و رمز در تنظیمات پنل Netlog استفاده خواهد شد. دسترسی قسمت Group را نیز در حالت read قرار میدهیم و کلید OK را می فشاریم.

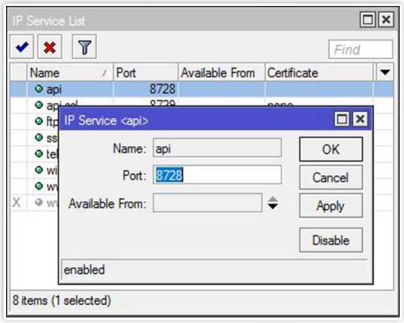


سپس به پنل Netlog بر می گردیم. در بخش تنظیمات مربوط به NasInfo روی گزینه Add کلیک می کنیم.



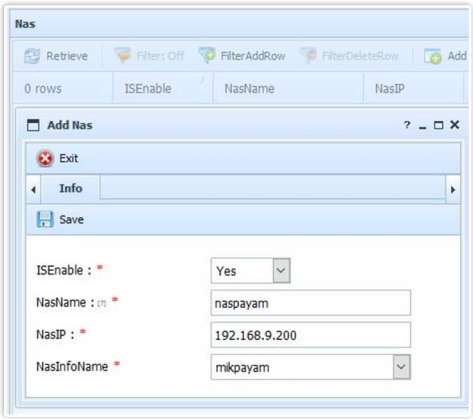
در پنجره ی باز شده در قسمت NasInfoName یک نام دلخواه تعیین میکنیم. گزینه NasType را Mikrotik انتخاب می کنیم. پورت پیش فرض ApiPort روی ۸۷۲۸ می باشد که در صورت نیاز تغییر می دهیم.

سپس نام کاربری و رمز مربوط به یوزر ایجاد شده در میکروتیک را در قسمت های ApiUsername و ApiPassword وارد می کنیم و در نهایت روی کلید Save کلیک می کنیم.



لازم به توضیح است که برای تغییر ApiPort ابتدا در تنظیمات میکروتیک وارد منوی IP>Services شده و api را ویرایش کنید.
در تنظیمات api همچنین می توانید برای امنیت بیشتر در قسمت Available from تنها برای آی پی های خاصی دسترسی ایجاد کنید.

System>Nas



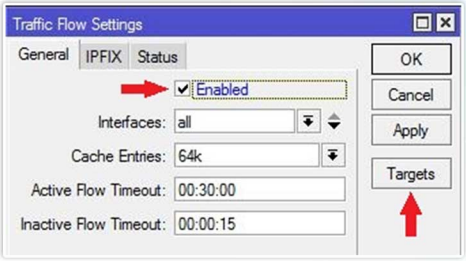
روی Add کلیک می کنیم.

- در قسمت ISEnable می توانیم Nas تعریف شده را فعال یا غیر فعال کنیم.
- در قسمت NasName یک نام دلخواه وارد می کنیم.
- در قسمت NasIP آی پی مربوط به پورتی از روتر که به اینترنت متصل است را وارد می کنیم.
- در قسمت NasInfoName نام تعریف شده در منوی قبل را انتخاب می کنیم. با انتخاب کلید Save پیغام زیر نمایش داده می شود.

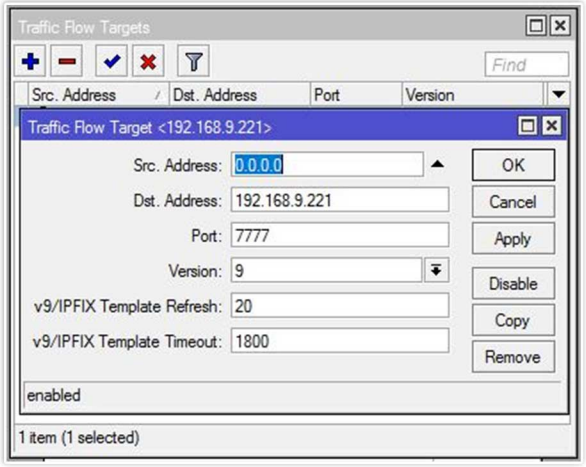
همان طورکه در تصویر مشاهده می کنید از شما خواسته شده است که در محیط لینوکس CentOS دستور pak.netcollector.restart را اجرا کنید.
در حال حاضر اگر یوزری در میکروتیک آنلاین باشد باید در منوی Report>Online User مشاهده کنید.

System>NetLog IP

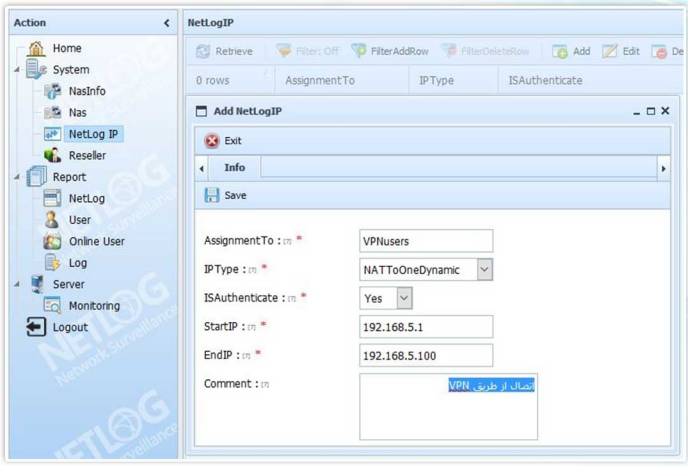
برای اینکه Log مربوط به هر یوزر را داشته باشید نیاز به انجام تنظیمات در این منو و همچنین تنظیمات لازم در میکروتیک دارید.
ابتدا در میکروتیک وارد منوی IP>TrafficFlow می شویم.



در پنجره ی باز شده تیک گزینه Enable را فعال می کنیم. کلید Apply را می فشاریم. سپس کلید Targets را انتخاب می کنیم.
در پنجره ی باز شده تنظیمات زیر را انجام می دهیم.
در قسمت Dst. Address آی پی Netlog را وارد میکنیم. Port را با ۷۷۷۷ مقدار دهی می کنیم و Version را به ۹ تغییر می دهیم. سپس OK را انتخاب می کنیم.



به پنل NetLog بر می گردیم.در منوی NetLog IP و از نوار فوقانی کلید Add را انتخاب می کنیم. در پنجره ی باز شده تنظیمات زیر را انجام می دهیم.



AssignmentTo را با یک نام دلخواه پر می کنیم.

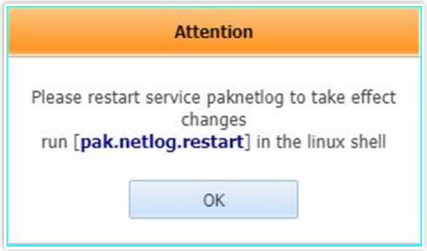
IPType شامل چهار گزینه می باشد:

- Route: این گزینه برای حالتی استفاده می شود که packet ها با همان Src IP خودشان از میکروتیک خارج می شوند و عمل NAT روی آنها انجام نمی شود. مانند IP Valid
- NATToMany: در صورت که آی پی های شبکه شما به سمت کلاس یا کلاس های آی پی دیگر NAT می شوند.
- NATToOneStatic: در صورتی که تمام آی پی های شبکه شما به سمت یک آی پی Static(Valid) ترجمه یا NAT می شوند.
- NATToOneDynamic: این گزینه مانند حالت قبل است با این تفاوت که آی پی NAT شده ثابت نیست. مانند حالت masquerade در میکروتیک.

گزینه ی مورد نظر را انتخاب کنید.

گزینه ISAuthenticate را در صورتی که کاربران شما در شبکه اعتبار سنجی می شوند Yes بگذارید.

(منظور از اعتبار سنجی کاربرانی است که از طریق VPN یا Hotspot و یا PPP وصل می شوند و در واقع به عنوان کاربر آنلاین در بخش Online user قابل مشاهده هستند.)
در صورتی که کاربران شما بدون نیاز به نام کاربری و رمز از طریق NAT به طور مستقیم به میکروتیک وصل شده و میخواهید Log آنها را دریافت کنید گزینه ISAuthenticate را در وضعت NO قرار دهید.
در قسمت StartIP مشخص کنید که آی پی هایی که می خواهید لاگ آن ها را دریافت کنید از چه آی پی شروع می شوند.
در قسمت EndIP مشخص کنید که که آی پی هایی که می خواهید لاگ آن ها را دریافت کنید به چه آی پی ختم می شوند.



در کادر Commnet هم می توانید در صورت نیاز توضیحاتی را وارد نمایید.
در پایان Save را می فشاریم.

مشاهده می کنید که پیغام ظاهر شده از شما می خواهد که دستور pak.netlog.restart را در محیط لینوکس اجرا کنید.
با انجام این تنظیمات Log مربوط به اتصالات هر یوزر ذخیره شده و می توانید از منوی Report>NetLog آن را مشاهده کنید.
توجه داشته باشید که NetLog برای تشخیص رکوردهای اضافی، اطلاعات را با یک تا دو دقیقه تاخیر ثبت می کند.

System>Reseller

در این قسمت شما می توانید دسترسی لازم برای افرادی که قرار است ورود و مدیریت پنل NetLog را انجام دهند ایجاد کنید. به طور پیش فرض فقط ریسلر admin وجود دارد که می توانید با انتخاب گزینه ی Edit این Reseller را ویرایش نموده و یا با انتخاب گزینه Add یک Reseller جدید ایجاد کنید. همچنین با انتخاب کلید Delete می توانید ریسلرهای ایجاد شده را حذف کنید.

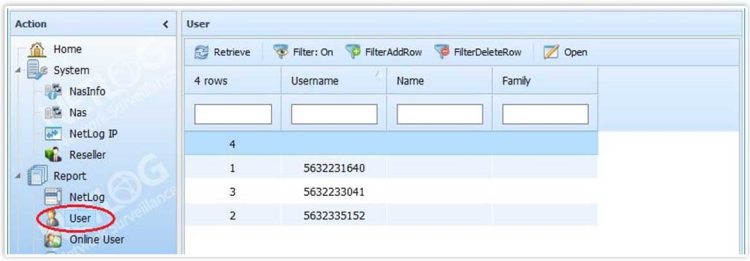
در تصویر زیر تنظیمات مربوط به افزودن ریسلر جدید را مشاهده می کنید.

منوی Report

در این منو می توانید کلیه ی یوزر های مجموعه و یوزرهای آنلاین و همچنین لاگ مربوط به هر یوزر را مشاهده کنید.

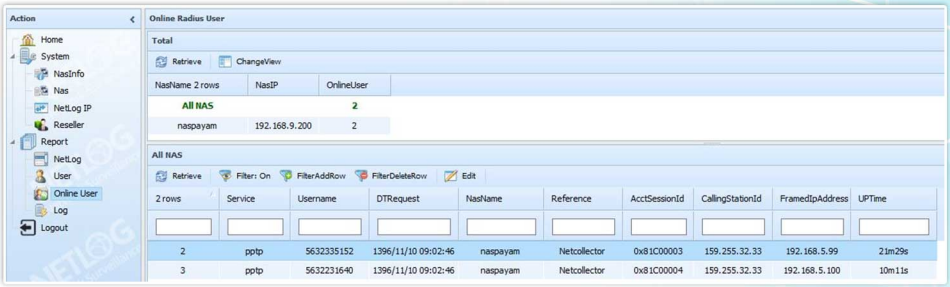
Report>User

در این منو شما می توانید کلیه ی یوزر هایی که تا به حال آنلاین شده اند را مشاهده کنید. در واقع یوزر هایی که قبلا آنلاین شده و در حال حاضر آفلاین هستند نیز نمایش داده می شوند.



Report>Online User

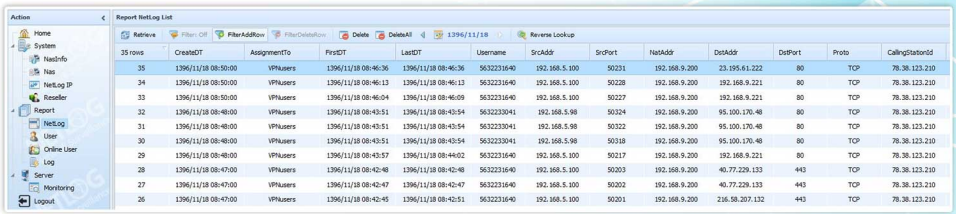
در این صفحه کاربرانی که در حال حاضر آنلاین می باشند نمایش داده می شود.



همان طور که مشاهده می کنید صفحه ی Online User شامل دو بخش می باشد. در بخش بالا (Total) می توانید انتخاب کنید که کاربران آنلاین مربوط به کدام یک از NAS های تعریف شده را می خواهید مشاهده کنید. در بخش پایین نیز می توانید کاربران آنلاین مربوط به آن NAS را مشاهده کنید.

Report>NetLog

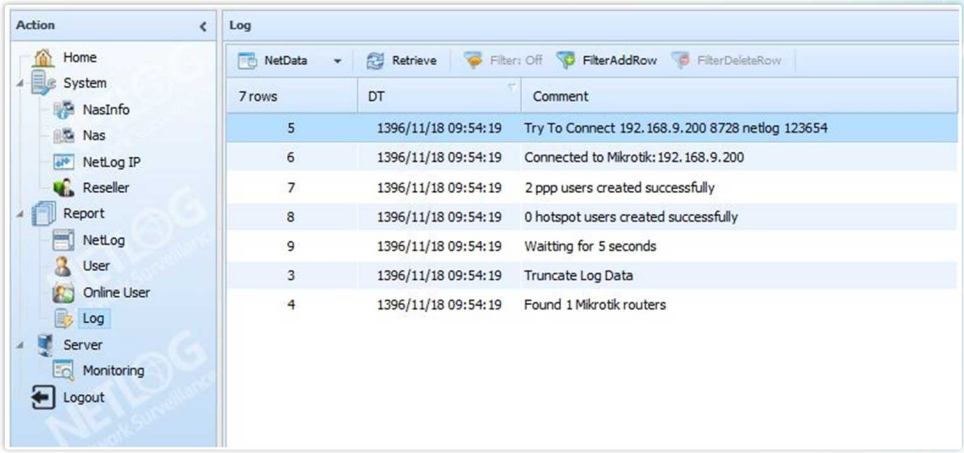
نرم افزار قدرتمند NetLog قادر است تا لاگ کاربران را به با جزئیات دقیق تاریخ، نام کاربری یوزر، آی پی یوزر، آی پی NAT شده، پورت و پروتکل و ... را به طور لحظه ای ثبت و ذخیره نماید.
در این بخش می توانید از فیلترهای متفاوت جهت جستجوی لاگ مربوط به یک تارخ خاص، یوزر خاص، پورت خاص، آی پی خاص و ... به طوردقیق تر و سریع تر به نتیجه ی لازم برسید. برای اضافه کردن فیلتر از کلید FilterAddRow استفاده کنید. برای این که فیلتر مورد نظر شما اعمال شود حتما باید کلید Filter در وضعیت On با شد.



در صفحه ی NetLog کلیدی با عنوان Reverse Lookup قرار داده شده است که می توانید با انتخاب هر سطر و زدن این کلید به اطلاعاتی در خصوص آی پی انتخاب شده دست یابید.

Report>Log

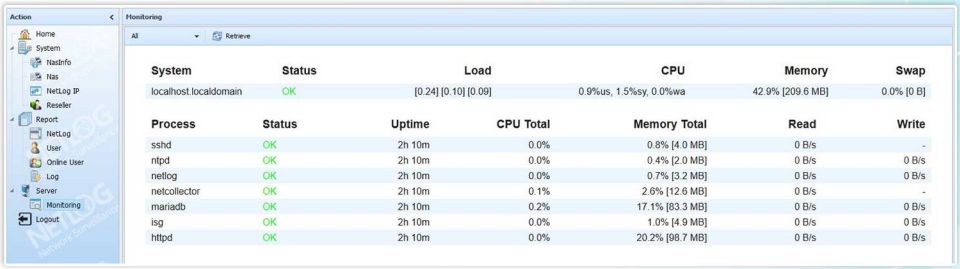
در این صفحه می توانید درخواست های لحظه ای سرویس Netcollector و NetLog به روتر را مشاهده کنید.



NETLOG
Network Surveillance

Server>Monitoring

وضعیت سرویس های نرم افزار را نشان می دهد.
به عنوان مثال در تصویر زیر مشاهده می کنید که هر هفت سرویس مورد نیاز NetLog در وضعیت OK قرار دارند.



System	Status	Load	CPU	Memory	Swap
localhost.localdomain	OK	[0.24] [0.10] [0.09]	0.9%us, 1.5%sy, 0.0%wa	42.9% [209.6 MB]	0.0% [0 B]

Process	Status	Uptime	CPU Total	Memory Total	Read	Write
sshd	OK	2h 10m	0.0%	0.8% [4.0 MB]	0 B/s	-
ntpd	OK	2h 10m	0.0%	0.4% [2.0 MB]	0 B/s	0 B/s
netlog	OK	2h 10m	0.0%	0.7% [3.2 MB]	0 B/s	0 B/s
netcollector	OK	2h 10m	0.1%	2.6% [12.6 MB]	0 B/s	-
mariadb	OK	2h 10m	0.2%	17.1% [83.3 MB]	0 B/s	0 B/s
isg	OK	2h 10m	0.0%	1.0% [4.9 MB]	0 B/s	0 B/s
httpd	OK	2h 10m	0.0%	20.2% [98.7 MB]	0 B/s	0 B/s