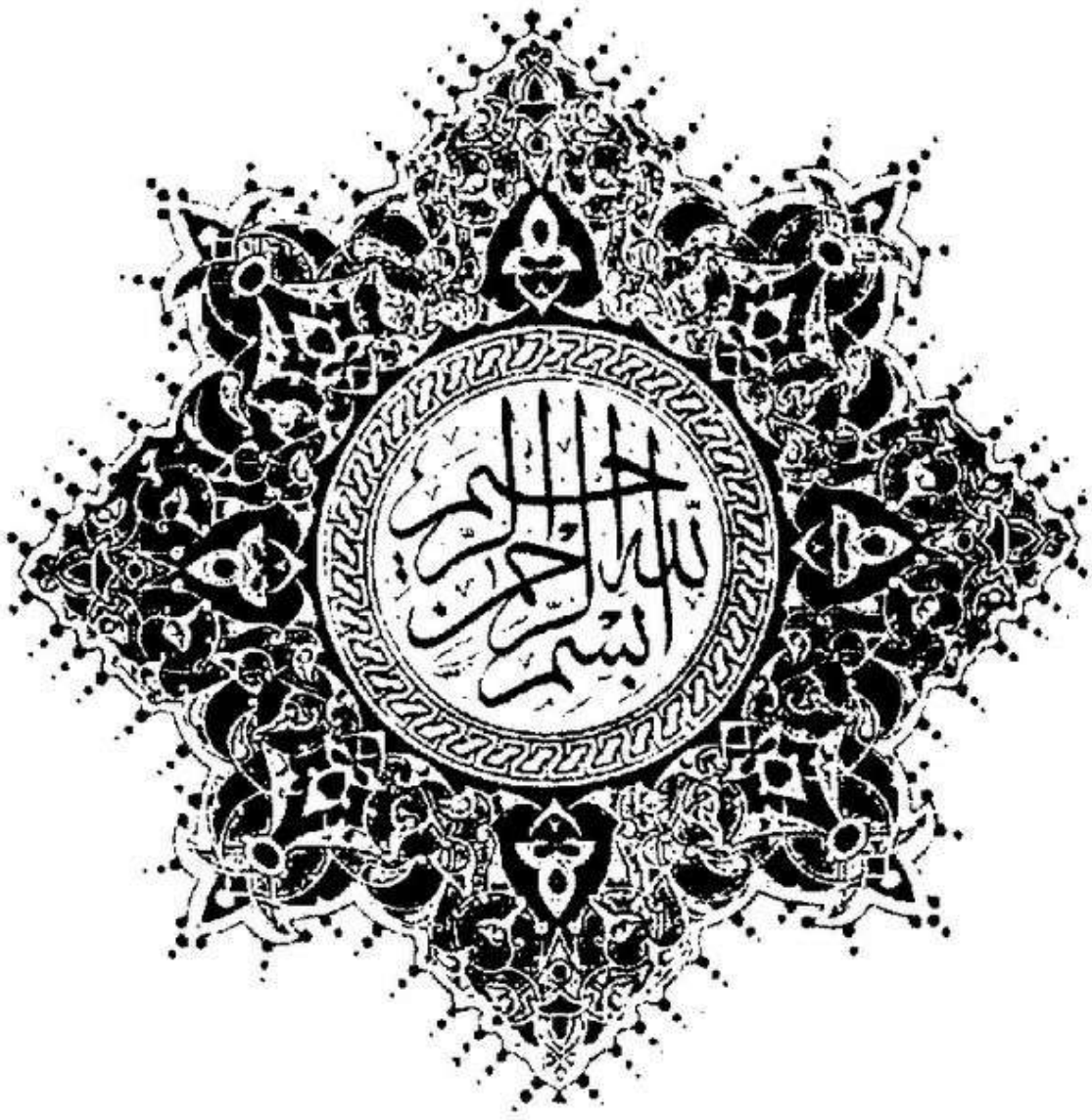
شامل :

جزوه آموزشی

فیلم آموزشی

مرجع کاربردی میکروتیک - فصل چهارم

www.bazyar.ir


بسم الله الرحمن الرحیم

ای دو جهان از قلمت یک رقم بی رقمت لوح دو عالم عدم

در کف من مشعل توفیق نه ره به نهان خانه تحقیق ده

شمع زبانم سخن افروز ساز شام من از صبح سخن روز ساز

آنچه در این فصل می خوانید:

Filtering

یکی دیگر از قابلیت های فایروال ، ایجاد فیلترینگ است . در فیلترینگ پکت هایی که از مسیر یاب عبور می کنند تحت کنترل قرار می گیرند و بر اساس قوانینی که به آنها RULE گفته می شود فیلتر می شوند.

هر rule شامل دو قسمت کلی می باشد :

قسمت اول ، ترافیک بسته ها را مشخص می کند (ترافیک ورودی یا خروجی از میکروتیک)

قسمت دوم ، عملیاتی است که بر روی بسته ها انجام می شود.

تنظیم filtering در مسیریاب :

[admin@mikrotik] > ip firewall filter add chain=[input | output | forward] action=[drop | accept | reject] src-address=[source ip address] dst-port=[destination port] protocol=[protocol]

پارامترهای مورد استفاده در rule های فیلترینگ :

۱) **Chain :** در این پارامتر ، مسیر ترافیک بسته های مورد نظر را مشخص می کنیم. این پارامتر می تواند سه حالت را در بر بگیرد ، که به این شرحند :

- **Input : این حالت مربوط به پکت هایی است که مقصدشان خود دستگاه میکروتیک است.**

به طور مثال : ارسال بسته های icmp برای Ping کردن مسیریاب میکروتیک و یا زمانی که شما با استفاده از WinBox یا دیگر روش های ممکن به میکروتیک متصل می شوید ، بنابراین از chain=input استفاده می کنید.

- **Output : این حالت مربوط به بسته هایی است که از مسیریاب میکروتیک خارج می شوند.**

به طور مثال : بسته هایی که از داخل مسیریاب سعی در telnet کردن به سیستم یا دستگاهی را داشته باشند و یا مسیریاب سعی در اتصال به سرویس دهنده های DNS یا NTP و ... را داشته باشد .

- **Forward : این حالت مربوط به ترافیکی است که از مسیریاب شما عبور می کند .**

فرایند ارسال بسته از یک کارت شبکه مسیریاب به کارت شبکه دیگر آن را forward می گویند.

به طور مثال : یک سیستم داخلی درخواست سایتی را از اینترنت داشته باشد و چنانچه مسیریاب شما نقش gateway را در شبکه داشته باشد، مسیریاب بسته درخواست را از کارت شبکه ای که به شبکه داخلی مرتبط می باشد ، دریافت می کند و به کارت شبکه ای که به wan مرتبط است ارسال می کند.)

۲) **Action :** در این پارامتر ، عملیاتی که بر روی پکت ها اعمال می شود را تعیین می کنیم. . این پارامتر می تواند سه حالت را در بر بگیرد ، که به این شرحند :

- **Accept** : در این حالت به بسته ها اجازه عبور داده می شود.
- **Drop** : در این حالت به بسته ها اجازه عبور داده نمی شود. به عبارتی بسته ها متوقف می شوند.وهیچ جوابی به فرستنده بسته ها داده نمی شود.
- **Reject** : در این حالت همانند عملیات Drop است با این تفاوت که پیغامی با استفاده از بسته icmp نیز به کاربر نشان می دهد.

۳) **Src-address :** برای مشخص کردن آدرس فرستنده یک بسته از این پارامتر استفاده می کنیم.

به طور مثال چنانچه بخواهیم بسته هایی که فقط از سمت یک سیستم خاص به مسیریاب می رسند را فیلتر کنیم آدرس IP سیستم فرستنده را در این پارامتر مشخص می کنیم .

نکته : چنانچه بخواهیم بسته های مربوط به تمام کلاینت های موجود در شبکه مبدا را فیلتر کنیم پارامتر src-address را استفاده نمی کنیم .

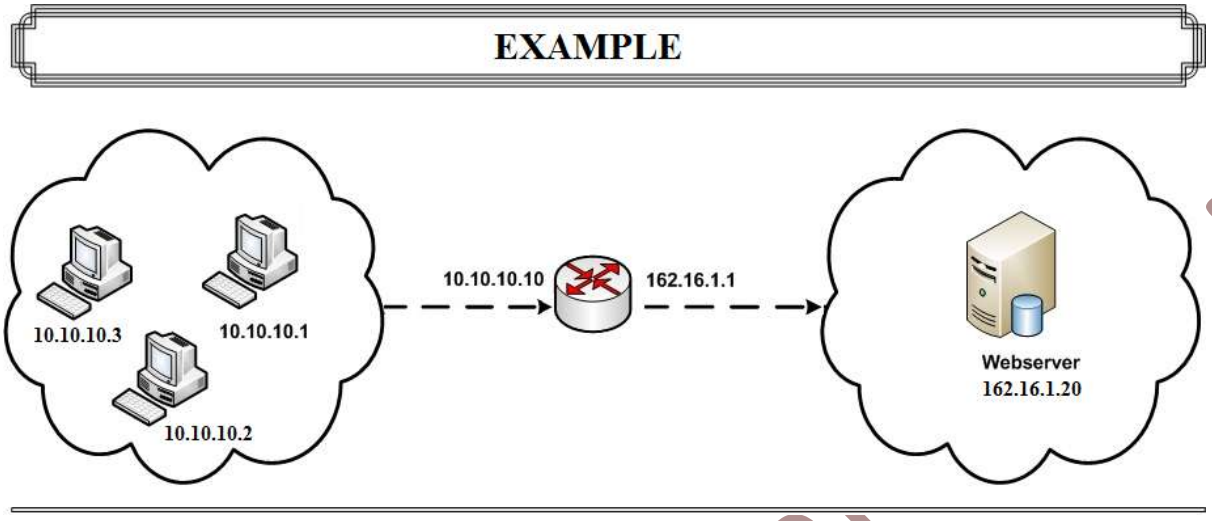
نکته : چنان چه در دستور فیلترینگ این پارامتر را ذکر نکنیم کل بسته ها در نظر گرفته می شود .

۴) **Dst-port :** برای اعمال فیلترینگ بر روی بسته هایی که مقصد آنها پورت خاصی باشد از این پارامتر استفاده می شود

نکته : قابل ذکر است که چنان چه در دستور فیلترینگ این پارامتر را ذکر نکنیم کل پورت ها را در نظر می گیرد.

۵) **Protocol :** برای اعمال فیلترینگ بر روی بسته هایی که مقصد آنها پروتوکل خاصی باشد از این پارامتر استفاده می شود . به طور مثال بسته های مربوط به پروتوکل icmp ، برای عملیات ping کردن.

کاربرد این موارد را در مثال هایی به تفصیل نشان خواهیم داد :



مثال شماره ۱ :

در این rule تمام بسته های پروتوکل icmp که به سمت میکروتیک می آید را drop می کند.

با اعمال این rule هیچ سیستمی نمی تواند مسیریاب میکروتیک را ping کند . چرا که از فیلد src-address استفاده نکرده ایم.

[admin@mikrotik] > ip firewall filter add chain=input action=drop protocol=icmp

مثال شماره ۲ :

در این rule تمام بسته های پروتوکل icmp که از سمت ip = 10.10.10.2 به سمت میکروتیک می آید را drop می کند.

به عبارتی فقط سیستم 10.10.10.2 نمی تواند به میکروتیک ping کند. بقیه سیستم ها می توانند ping کنند .

[admin@mikrotik] > ip firewall filter add chain=input action=drop protocol=icmp

Src-address = 10.10.10.2

مثال شماره ۳ :

[admin@mikrotik] >ip firewall filter add chain=forward action=drop protocol=icmp

Src-address = 10.10.10.2

در این rule تمام بسته های پروتوکل icmp که از سمت ip=10.10.10.2 به سمت مسیریاب می آیند ،چنان چه خود میکروتیک را ping کرده باشند، بسته جواب برگشت داده می شود و پیغام زیر نشان داده میشود :

Reply from 10.10.10.10 : bytes=32 time=0ms TTL=64

اما اگر شبکه ای که بعد از مسیریاب وجود دارد را ping کرده باشند بسته ها drop میشوند، به عبارتی بسته جواب برگشت داده نمیشود و پیغام .Request timed out نشان داده می شود .

به طور مثال : چنانچه سرور 162.16.1.20 را Ping کند ، بسته ها Drop میشوند،اما اگر خود مسیریاب یعنی 162.16.1.1 را ping کند ، بسته های جواب به فرستنده برگشت داده می شود.

مثال شماره ۴ :

در این rule مشخص کرده ایم که هیچ سیستمی اجازه ارتباط از طریق telnet به هیچ مقصدی را نداشته باشد.

(پورت 23 مربوط به پروتوکل telnet است)

[admin@mikrotik] > ip firewall filter add chain=forward action=drop protocol=icmp protocol=tcp Dst-port = 23

نکته : چنان چه سیستمی بخواهد به خود مسیریاب telnet بزند ، مشکلی وجود ندارد . اما چنانچه بخواهید این rule را به صورتی تنظیم کنید که کلاینت ها نتوانند به میکروتیک telnet بزنند باید chain = inpute را انتخاب کنید.

مثال شماره ۵ :

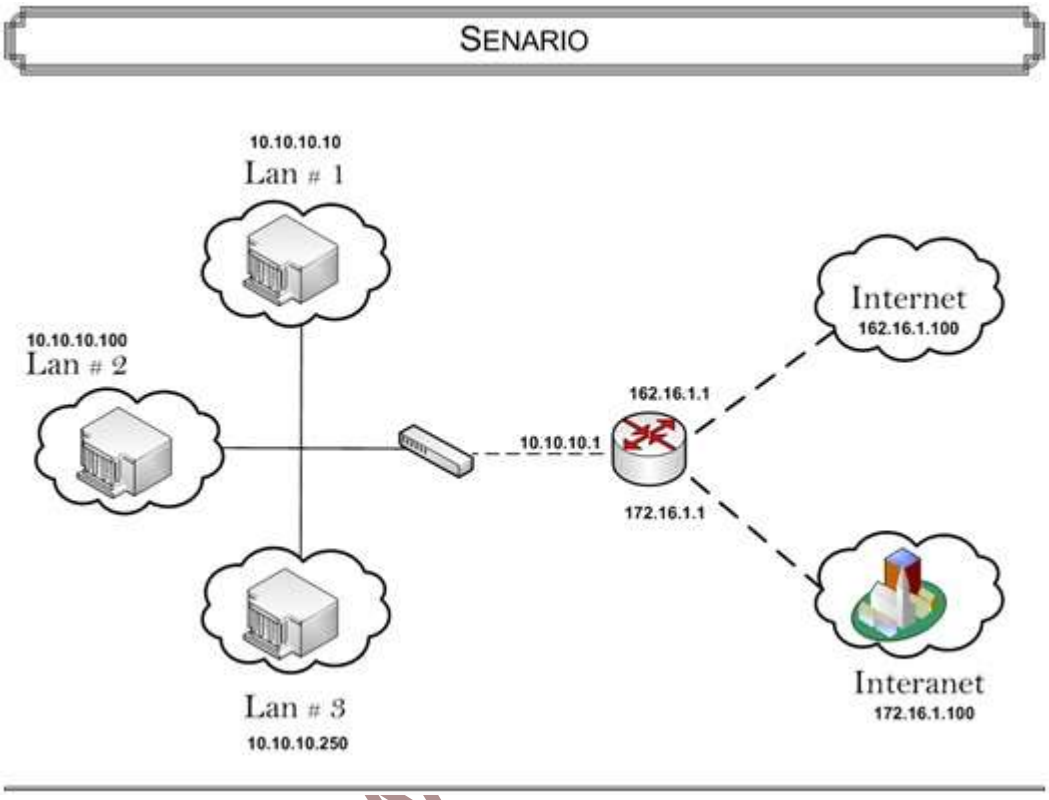
در این rule مشخص کرده ایم که هیچ سیستمی اجازه فرستادن بسته icmp به سمت میکروتیک را نداشته باشد و این پیغام برای فرستنده نشان داده شود.

[admin@mikrotik] > ip firewall filter add chain=input action=reject protocol=icmp protocol=tcp

قابل ذکر است که در مواردی ممکن است ،سیستم عامل Windows 7 بعضی از این پیغام ها را تشخیص ندهد و به جای آن عبارت Request Time Out را نشان دهد.

لابراتوار ۱ :

هدف از بررسی این لابراتوار بررسی عملیات فیلترینگ به همراه پیاده سازی در نرم افزار WinBox می باشد .



در این سناریو مسیریاب را به گونه ای تنظیم می کنیم که Lan#1 تنها به سرور اتوماسیون اداری موجود در اینترانت Lan#2 تنها به اینترنت و Lan#3 هم به اینترنت و هم به اینترانت دسترسی داشته باشند.

برای پیاده سازی این سناریو :

- سه سیستم Windows 7 جهت شبیه سازی کلاینت های موجود در هر Lan
- یک مسیریاب میکروتیک به عنوان Firewall
- دو سیستم Windows Server 2008 برای شبیه سازی اینترنت و اینترانت راه اندازی می کنیم.

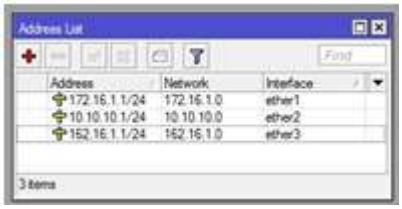
تنظیمات در مسیریاب :

۱. انتساب آدرس Ip به کارت های شبکه مسیریاب :

```
[admin@mikrotik] > ip address add address=10.10.10.1/24 interface=ether1
[admin@mikrotik] > ip address add address=172.16.1.1/24 interface=ether2
[admin@mikrotik] > ip address add address=162.16.1.1/24 interface=ether3
```

انتساب آدرس Ip به کارت های شبکه مسیریاب از طریق نرم افزار winbox :

در نرم افزار WinBox از منوی اصلی گزینه IP و از زیر منوی باز شده Addresses را انتخاب می کنیم . در صفحه address List بر روی علامت ADD برای اضافه کردن مشخصات IP مربوط به کارت شبکه های مسیریاب کلیک می کنیم.



نکته :جهت تنظیم قوانین فایروال میکروتیک ، از آنجا که به صورت پیش فرض تمام ترافیک بسته ها اجازه عبور از فایروال را دارند بنابراین تنها مواردی که اجازه عبور از فایروال را ندارند به مسیریاب میکروتیک اضافه می کنیم .

۲ . تنظیمات جهت عدم دسترسی کلاینت های موجود در Lan#1 به اینترنت :

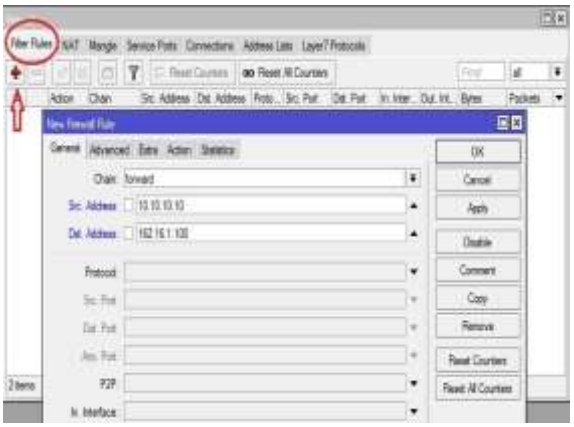
[admin@mikrotik] > ip firewall filter add chain=forward action=drop

Src-address=10.10.10.10/24 dst-address=162.16.1.100

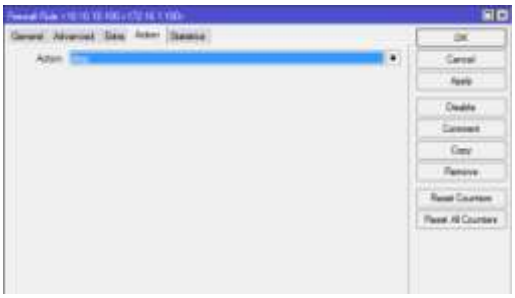
از آنجا که به صورت پیش فرض تمام بسته ها ی سیستم موجود در Lan 1 اجازه عبور از فایروال میکروتیک را دارند بنابراین تنها بسته هایی که مقصد آنها اینترنت می باشد را فیلتر می کنیم.

تنظیمات جهت عدم دسترسی کلاینت های موجود در Lan#1 به اینترنت از طریق نرم افزار winbox :

برای اعمال قوانین فایروال بر روی مسیریاب میکروتیک از طریق نرم افزار WinBox ، از منوی اصلی گزینه Ip و از زیر منوی باز شده گزینه Firewall را انتخاب می کنیم. در پنجره Firewall از سربرگ Filter Rules بر روی علامت ADD برای اضافه کردن قانون جدید کلیک می کنیم. در پنجره New Firewall Rule در سربرگ General قسمت های مورد نظر را وارد می کنیم



در پنجره New Firewall Rule در سربرگ Action نوع عملیاتی که بر روی بسته های که از سمت Lan1 می آید را مشخص می کنیم . که در این مثال action = drop وارد می کنیم .



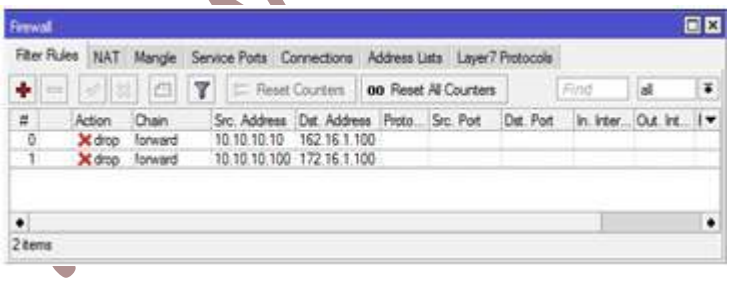
۳ . تنظیمات جهت عدم دسترسی کلاینت های موجود در Lan#2 به اینترانت :

[admin@mikrotik] > ip firewall filter add chain=forward action=drop

Src-address=10.10.10.100/24 dst-address=172.16.1.100

از آنجا که به صورت پیش فرض تمام بسته ها ی سیستم موجود در Lan 1 اجازه عبور از فایروال میکروتیک را دارند بنابراین تنها بسته هایی که مقصد آنها اینترنت می باشد را فیلتر می کنیم.

تنظیمات برای ترافیک بسته های Lan2 را نیز مانند تنظیمات Lan1 انجام می دهیم و در نهایت تنظیمات Firewall در میکروتیک به این صورت خواهد بود .



۴ . تنظیمات جهت دسترسی کلاینت های موجود در Lan#3 به اینترانت و اینترنت :

طبق قانون گفته شده از آنجا که محدودیتی برای ترافیک بسته های Lan 3 وجود ندارد ، هیچ فیلتری برای این نوع ترافیک ها در نظر گرفته نمی شود.

۵ . تنظیمات در کلاینت ها :

تنظیمات کلاینت موجود در Lan 1 :

IP=10.10.10.10

Subnet Mask=255.255.255.0

Default Gateway=10.10.10.1

تنظیمات کلاینت موجود در Lan 2 :

IP=10.10.10.100

Subnet Mask=255.255.255.0

Default Gateway=10.10.10.1

تنظیمات کلاینت موجود در Lan 3 :

IP=10.10.10.250

Subnet Mask=255.255.255.0

Default Gateway=10.10.10.1

۶ . تنظیمات در سرور ها :

تنظیمات سرور موجود در اینترانت :

IP=172.16.1.100

Subnet Mask=255.255.255.0

Default Gateway=172.16.1.1

تنظیمات سرور موجود در اینترنت :

IP=162.16.1.100

Subnet Mask=255.255.255.0

Default Gateway=162.16.1.1

۷ . تست ارتباط :

۷.۱) برای تست ارتباط از سیستم موجود در lan 1 با استفاده از دستور ping 172.16.1.100 بسته ای را به سمت سرور اتوماسیون اداری در اینترانت ارسال می کنیم .و در پاسخ این عبارت نشان داده می شود :

Reply from 172.16.1.100: bytes=32 time<1ms TTL=63

همان طور که در نتیجه دستور نشان داده شده است بسته به سرور در اینترانت رسیده است بنابراین ارتباط سیستم موجود در lan1 با این سرور بر قرار است .

۷.۲) برای تست ارتباط از سیستم موجود در lan 1 با استفاده از دستور ping 162.16.1.100 بسته ای را به سمت اینترنت ارسال می کنیم ، و در پاسخ این عبارت نشان داده می شود :

Request timed out

همان طور که در نتیجه دستور نشان داده شده است ارتباط سیستم موجود در lan1 با اینترنت برقرار نیست.

۷.۳) برای تست ارتباط از سیستم موجود در lan 2 با استفاده از دستور ping 172.16.1.100 بسته ای را به سمت سرور اتوماسیون اداری در اینترانت ارسال می کنیم :

Request timed out.

همان طور که در نتیجه دستور نشان داده شده است ارتباط سیستم موجود در lan2 با سرور اتوماسیون اداری در اینترانت برقرار نیست.

۷.۴) جهت تست ارتباط از سیستم موجود در lan 2 با استفاده از دستور ping 162.16.1.100 بسته ای را به سمت اینترنت ارسال می کنیم :

Reply from 162.16.1.100: bytes=32 time<1ms TTL=63

همان طور که در نتیجه دستور نشان داده شده است ارتباط سیستم موجود در lan2 با اینترنت برقرار است.

۷.۵) برای تست ارتباط از سیستم موجود در lan 3 با استفاده از دستور ping 172.16.1.100 بسته ای را به سمت سرور اتوماسیون اداری در اینترانت ارسال می کنیم :

Reply from 172.16.1.100: bytes=32 time<1ms TTL=63

همان طور که در نتیجه دستور نشان داده شده است ارتباط سیستم موجود در lan3 با این سرور بر قرار است

۷.۶) برای تست ارتباط از سیستم موجود در lan 3 با استفاده از دستور ping 162.16.1.100 بسته ای را به سمت اینترنت ارسال می کنیم :

Reply from 162.16.1.100: bytes=32 time<1ms TTL=63

همان طور که در نتیجه دستور نشان داده شده است ارتباط سیستم موجود در lan3 با اینترنت برقرار است.