آموزش نحوه باز کردن پورت در خانواده های ویندوز

۱۳۹۷/۰۲/۳

فایروال (Firewall) یا دیوار آتش نام برنامه‌هایی است که از دسترسی سایر افراد و ابزارهای غیرمجاز به کامپیوتر شما جلوگیری می‌کنند. این برنامه‌ها می‌توانند مستقل بوده یا از پیش تعبیه شده (مثل فایروال ویندوز) باشند. درواقع فایروال‌ها یک لایه امنیتی ایجاد کرده و داده‌های ورودی یا خروجی را کنترل و فیلتر می‌کنند. به این ترتیب کسی در یک شبکه یا اینترنت، بدون داشتن مجوزهای لازم نمی‌تواند از سیستم شما استفاده کند. دیوارهای آتش را می‌توان در ابزارهای شبکه مثل روترها (Routers) نیز یافت. این آموزش با هدف معرفی و پیکربندی فایروال پیش فرض سیستم عامل‌های ویندوز شرکت مایکروسافت تدوین شده است. از آنجا که پیکربندی فایروال ویندوز با روش های مختلفی قابل انجام است، پیکربندی از طریق واسط گرافیکی (GUI) و همچنین با ابزار NETSH و از طریق خط فرمان (CMD) تشریح شده است.

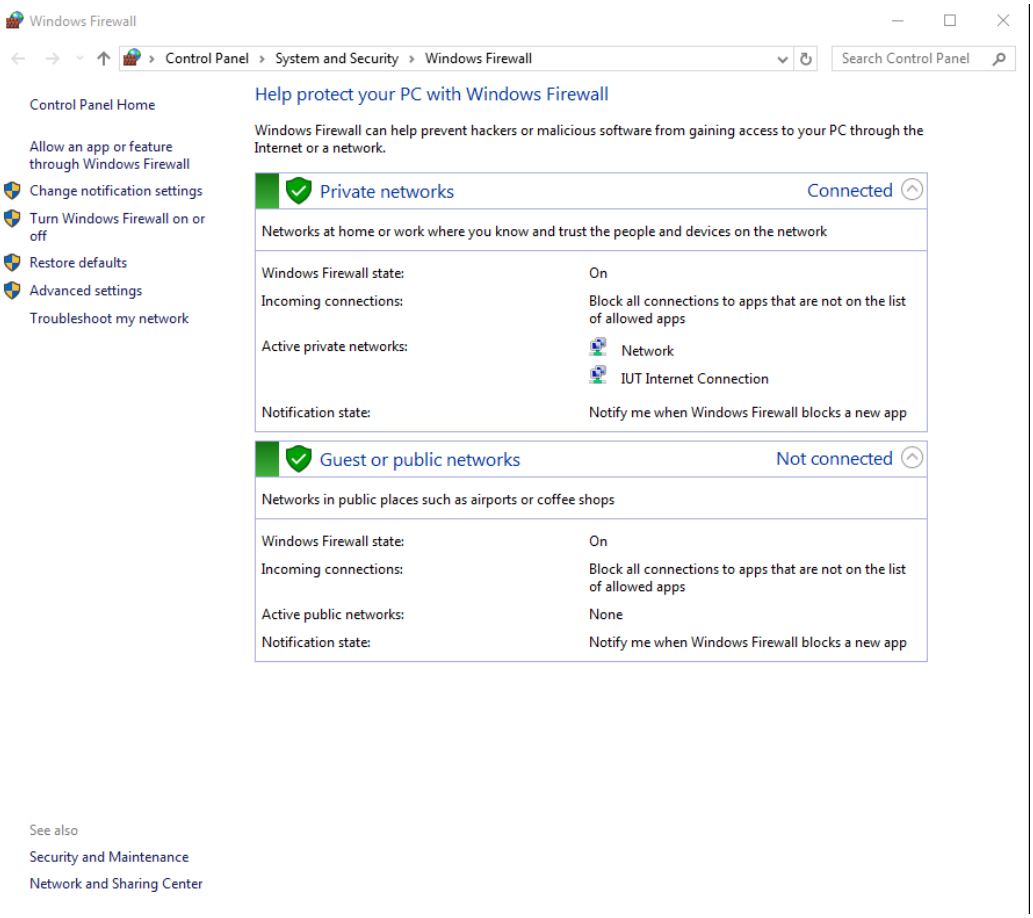
توجه: برای امنیت سیستم عامل، تنها پورت‌های لازم را باز کرده و از خاموش کردن فایروال و یا باز کردن تمامی پورت‌ها پرهیز نمایید.

این آموزش در نسخه های زیر قابل استفاده می‌باشد:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2008 R2
- Windows Server 2008
- Windows 10
- Windows 8.1
- Windows 7

مراحل باز کردن پورت در ویندوز

۱- برای شروع وارد Control Panel شده System & Security را بیابید. سپس Windows Firewall را باز کنید. در منوی سمت چپ روی Advanced setting کلیک کنید.



2- زمانی که وارد گزینه Advanced Security شدید در پنل سمت چپ دو نوع Rules مشاهده میکنید:

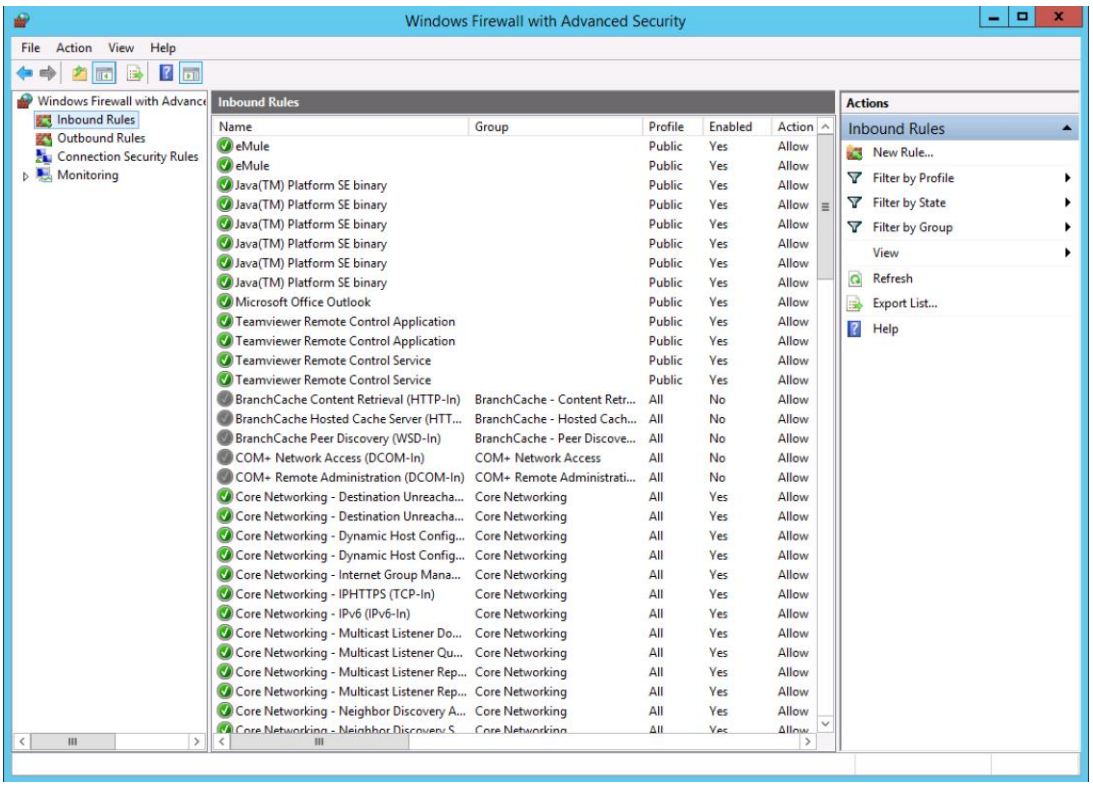
- Inbound Rules : Inbound Rulesبه کنترل ترافیکی که از بیرون سرور به سمت سرور میاید گفته میشود.

بعنوان مثال: چنانچه کاربری قصد اتصال به سیستم شما از طریق ریموت دسکتاپ را داشته باشد، آنگاه یک Rule از نوع Inbound باید تعریف نمایید.

- Outbound Rules : به ترافیکی که از داخل شبکه سرور قصد خارج شدن را دارد گفته میشود.

آموزش نحوه باز کردن پورت در خانواده های ویندوز

۱۳۹۷/۰۲/۳



زمانی که وارد گزینه Advanced Security شدید در پنل سمت چپ دو نوع Rules مشاهده میکنید:

- Inbound Rules : به کنترل ترافیکی که از بیرون سرور به سمت سرور میاید Inbound Rulesگفته میشود.

بعنوان مثال: چنانچه کاربری قصد اتصال به سیستم شما از طریق ریموت دسکتاپ را داشته باشد، آنگاه یک Rule از نوع Inbound باید تعریف نمایید.

- Outbound Rules : به ترافیکی که از داخل شبکه سرور قصد خارج شدن را دارد گفته میشود.

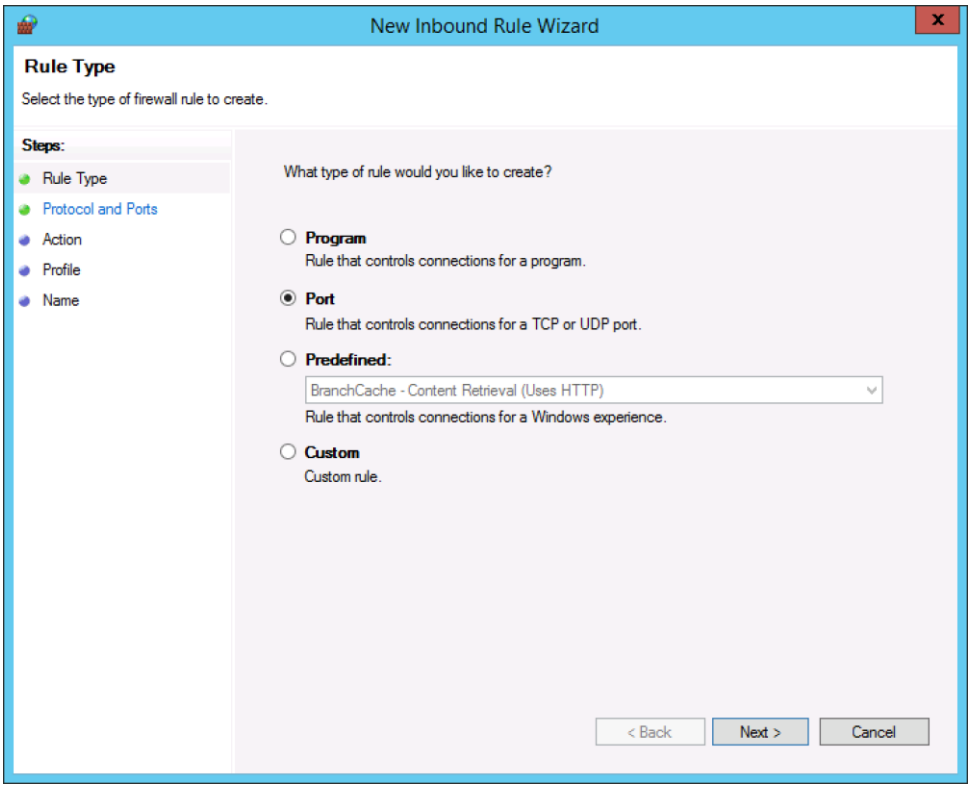
بر روی گزینه Inbound Rules راست کلیک کرده و گزینه "New Rules" را انتخاب نمایید.

فایروال ویندوز چهار نوع از قانون ها (Rule)را پیشنهاد می کند :

- Program:بلوکه کردن یا اجازه دادن به یک برنامه

- Port: بلوکه کردن یا اجازه دادن به یک پورت، رنج پورت یا پروتکل
- Predefined: استفاده از یک قانون فایروال از پیش تعیین شده درون ویندوز
- Custom: ترکیبی از برنامه، پورت و IP address را برای بلوکه کردن یا اجازه دادن مشخص می کند.

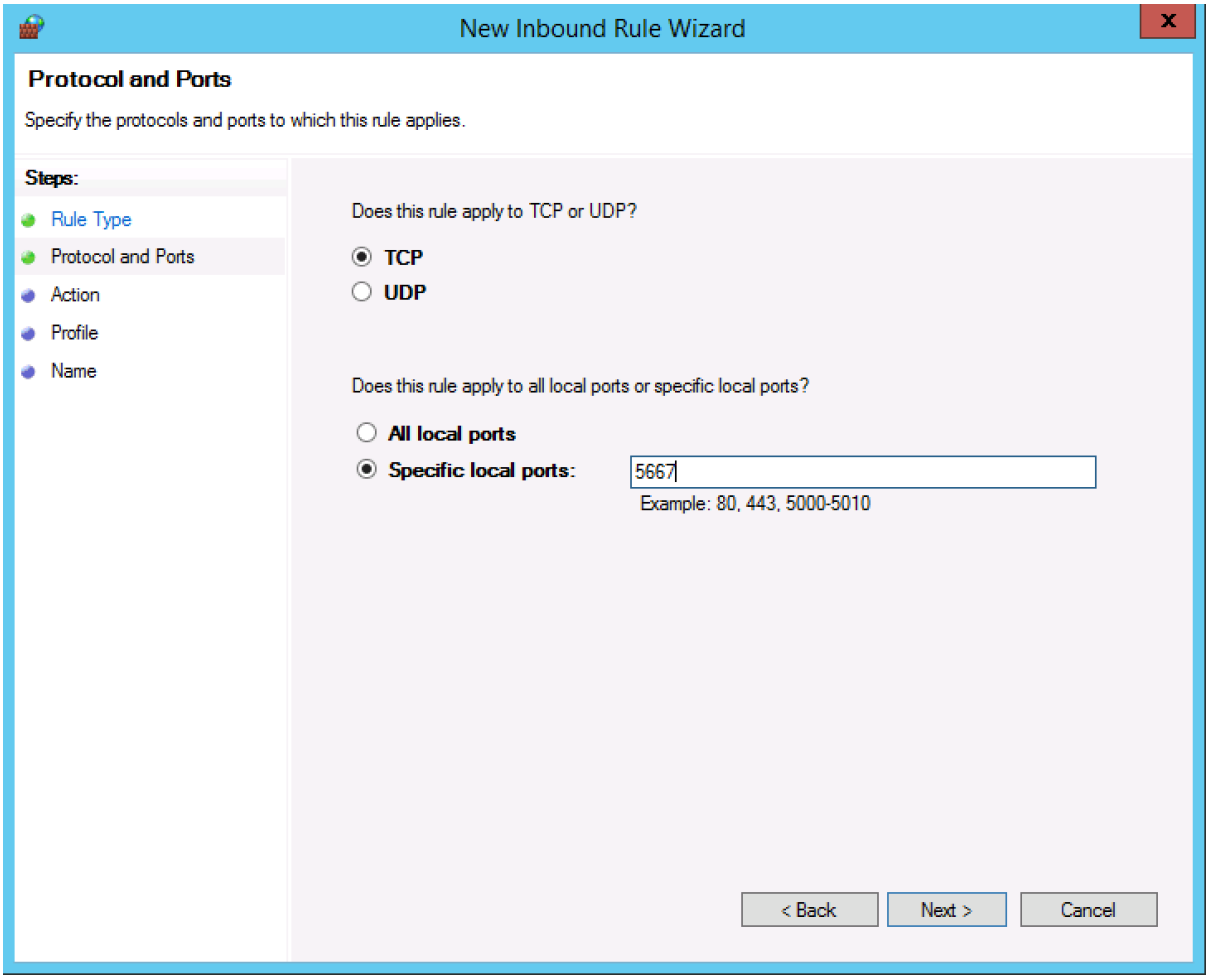
در این قسمت rule مورد نظر خود را انتخاب نمایید. هدف ما باز کردن پورت است پس گزینه Port را انتخاب نمایید.



در قسمت بعد پروتکل مورد نیاز را انتخاب کرده و سپس پورت نظر را وارد نمایید. لیست کامل پورت ها در RFC6335 قابل دستیابی هست. برخی از سرویس های پر کاربرد به همراه پورت‌هایشان در جدول زیر آورده شده است.

نام سرویس	شماره پورت
FTP Service	۲۰ و ۲۱
RDP Service (Remote Desktop)	۳۳۸۹
SMTP Service	۲۵

۸۰	HTTP Service
۴۴۳	HTTPS Service
۵۳	DNS Service



-6 در قسمت بعدی با توجه به اعمال از میان ۳ گزینه نمایش داده شده گزینه Public را انتخاب نمایید .

فایروال ویندوز شامل سه پروفایل مختلف است که شما می توانید rule های (قوانین) مختلفی را برای شبکه های خصوصی و عمومی بکار ببرید :

Domain Profile: هنگامی که کامپیوتر شما به یک Domain متصل است از آن استفاده می شود .

Private Profile: هنگامی که کامپیوتر شما به یک شبکه خصوصی از قبیل یک شبکه خانگی یا کاری متصل است ازآن استفاده می شود .

Public Profile: هنگامی که به یک شبکه عمومی از قبیل یک public Wi-Fi access point یا اتصال مستقیم به اینترنت متصل هستید از آن استفاده می شود. ویندوز هنگامی که برای اولین بار به یک شبکه وصل می شود می پرسد که آیا شبکه عمومی است یا خصوصی .

یک کامپیوتر ممکن است از چندین پروفایل بسته به موقعیت استفاده کند. برای مثال یک لپ تاپ تجاری هنگامی که در سر کار به یک Domain وصل می شود ممکن است از domain profile استفاده کند و هنگامی که به شبکه خانگی وصل می شود از private profile استفاده کند

7- در اخرین مرحله اجازه connection ها را مشخص می کنید. برای این مرحله Allow The Connectionرا انتخاب نمایید. به محض پایان مراحل این تغییرات اعمال می شود .

چنانچه بخواهید برای ترافیک خروجی هم Rule تعریف نمایید، این مراحل را برای Outbound Rulesنیز تکرار نمایید تا Port برای Send باز باشد.

تنظیمات فایروال ویندوز باNETSH

netsh.exeابزاریست که از طریق Command-Line اجازه می دهد تا به صورت Local و یا Remoteتنظیمات شبکه ی کامپیوتری که Netsh.exe را اجرا می کند را تغییر و یا نمایش دهید. Netsh.exe همچنین از طریقScripting این اجازه را می دهد تا گروهی از دستورات را به حالت Batch برای کامپیوترهای مشخصی اجرا شوند. Netsh.exe همچنین این امکان را در اختیار قرار می دهد تا تنظیمات را در قالب یک فایل متنی به منظور پیکر بندی سیستم های دیگر ذخیره کنید.

Netsh.exe بر روی ویندوزهای ۲۰۰۰، XP، Vista، 7، Server 2003، Server 2008، Server 2012، Server 2016 میباشد.

باز کردن و بلاک پورت با دستورNETSH

ساختار کلی

```
netsh advfirewall firewall add rule name="Rule name" protocol=[TCP or UDP or ...] dir=[Outbound or Inbound] remoteport=[port number] action=[Allow or Block]
```

مثال

```
netsh advfirewall firewall add rule name="Block8080" protocol=TCP dir=out remoteport=8080 action=block
netsh advfirewall firewall add rule name="Allow8081" protocol=TCP dir=out remoteport=8081 action=Allow
```

در خط اول پورت ۸۰۸۰ بلاک شده و در خط دوم پورت ۸۰۸۱ باز برای خروجی (Outbound) باز شده است.

مثال ۲: باز کردن و بستن پورت مربوط بهSQL Server

```
netsh advfirewall firewall add rule name="Open SQL Server Port 1433" dir=in action=allow protocol=TCP localport=1433
netsh advfirewall firewall delete rule name="Open SQL Server Port 1433" protocol=tcp localport=1433
```

با توجه به اینکه NETSH.exe ابزار بسیار مفیدی برای مدیران شبکه می باشد، لذا پر کاربردترین دستورات آن در ادامه آورده شده است.

1- بررسی وضعیت فایروال ویندوز

- netsh advfirewall show allprofiles

2- خاموش و روشن کردن فایروال ویندوز توسط دستورNETSH

- netsh advfirewall set allprofiles state on
- netsh advfirewall set allprofiles state off

خط اول تمام پروفایل های فایروال را خاموش می کند و در خط دوم تمام پروفایل ها روشن می شود.

3- اگر می خواهید یک پروفایل خاص را خاموش یا روشن کنید از دستور زیر استفاده کنید.

```
netsh advfirewall set privateprofile state off
netsh advfirewall set privateprofile state on
```

4- بلاک کردن دسترسی به یک IP خاص

ساختار

```
netsh advfirewall firewall add rule name="Rule name" dir=[inbound or outbound] interface=[interface name] action=[allow or block] remoteip=[IP]
```

مثال

```
netsh advfirewall firewall add rule name="IP Block" dir=in interface=any action=block remoteip=5.5.5.5
```

5- بلاک کردن دسترسی یک برنامه به اینترنت

ساختار

```
netsh advfirewall firewall add rule name="Rule Name" dir=[inbound or outbound] action=[allow or block] program="Program address" enable=[yes or no]
```

مثال

```
netsh advfirewall firewall add rule name="photoshop block" dir=out action=block program="C:\Program Files\Adobe\Adobe Photoshop CC 2015\photoshop.exe" enable=yes
```

6- اجازه دسترسی به یک برنامه از اینترنت

- netsh advfirewall firewall add rule name="Allow Messenger" dir=in action=allow program="C:\programfiles\messenger\msnmsgr.exe"

8- باز کردن و بلاک یک سرویس در فایروال

ساختار کلی

netsh advfirewall firewall set rule group="profile Name" new enable=[yes or no]

مثال

netsh advfirewall firewall set rule group="remote desktop" new enable=yes

netsh advfirewall firewall set rule group="remote desktop" new enable=no

در خط اول سرویس Remote Desktop باز شده و در خط دوم بلاک شده است.

9- حذف کردن رول با دستورNETSH

ساختار

netsh advfirewall firewall delete rule name="Rule Name"

مثال

netsh advfirewall firewall delete rule name="IP Block"

10-ریست کردن تنظیمات فایروال به حالت پیش‌فرض

- netsh advfirewall reset

11-تغییر مسیر ذخیره سازیLOG های فایروال

- netsh advfirewall set currentprofile logging filename "C:\temp\pfirewall.log"

12-اجازه دادن و جلوگیری کردن ازPING

- netsh advfirewall firewall add rule name="All ICMP V4" dir=in action=block protocol=icmpv4
- netsh advfirewall firewall add rule name="All ICMP V4" dir=in action=allow protocol=icmpv4

13-تهیه خروجی از تنظیمات انجام شده جهت اعمال در سایر سیستم ها(EXPORT)

- netsh advfirewall export "C:\temp\WFconfiguration.wfw"

14- اعمال تنظیمات با استفاده از فایل WFW (IMPORT)

- "netsh advfirewall import "C:\temp\WFconfiguration.wfw

آموزش نحوه باز کردن پورت در خانواده های ویندوز

۱۳۹۷/۰۲/۳

جدول ۱: تاریخچه سند

نسخه	ویرایش	تاریخ	توضیحات
1.0	آقای محمدی	۹۷/۲/۴	