مرکز تخصصی آپا دانشگاه رازی

نحوه‌ی پیکربندی قابلیت

Dynamic IP Restrictions

بهار ۱۳۹۶

مقدمه

ماژول Dynamic IP Restrictions (DIPR) در IIS 7.0 و بالاتر امکان محافظت در برابر حملات انکار سرویس (DDoS) و brute force بر روی وب‌سرورها و وب‌سایت‌ها را فراهم می‌آورد. به منظور ایجاد این حفاظت، ماژول نامبرده موقتاً آدرس‌های IP از کلاینت‌های HTTP را که منجر به ایجاد تعداد بسیار زیادی درخواستِ همزمان می‌گردند یا که تعداد زیادی درخواست را در مدت زمان کوتاهی ایجاد می‌کنند مسدود (block) می‌نماید.

ویژگی‌ها

- **مسدود نمودن آدرس‌های IP بر اساس تعداد درخواست‌های همزمان**_ اگر تعداد درخواست‌های همزمان یک کلاینتِ HTTP از حد مجاز بیشتر شود، آدرس IP آن کلاینت به طور موقت مسدود می‌گردد.
- **مسدود نمودن آدرس‌های IP بر اساس تعداد درخواست‌ها در طول یک دوره‌ی زمانی**_ اگر تعداد درخواست‌های یک کلاینتِ HTTP در یک بازه‌ی زمانیِ مشخص بیش از حد مجاز باشد، آدرس IP آن کلاینت به طور موقت مسدود می‌گردد.
- **امکان لیست نمودن آدرس‌های IP که نمی‌خواهید مسدود شوند**_ شما می‌توانید لیستی از آدرس IP کلاینت‌هایی که می‌خواهید از قاعده‌ی مسدود شدن توسط ماژول نامبرده (صرف‌نظر از پیکربندی‌های دیگر) مستثنی باشند ایجاد نمایید.
- **اقدامات رد درخواست مختلف**_ شما می‌توانید[1] مشخص کنید که برای یک کلاینت HTTP که آدرس IP آن مسدود شده است چه پاسخی بازگردانده شود. ماژول می‌تواند کد وضعیت 403، 404 یا فقط خاتمه‌ی اتصال HTTP را بازگرداند یا اینکه هیچ پاسخی بازنگرداند.

[1] Deny

- **امکان پشتیبانی برای وب‌سرورها از پشت پراکسی**_ اگر وب‌سرور شما پشت یک پراکسی باشد، شما می‌توانید ماژول را جهت استفاده از آدرس IP کلاینت از یک هدر X-Forwarded-For پیکربندی نمایید.
- **IPV6**_ این ماژول به طور کامل آدرس‌های IPV6 را پشتیبانی می‌کند.

نصب ماژول DIPR (Dynamic IP Restrictions)

شما می‌توانید این ماژول را از لینک زیر دانلود نمایید:

https://www.iis.net/downloads/microsoft/dynamic-ip-restrictions

پیش‌نیازها:

شما باید یکی از سیستم‌عامل‌های زیر را داشته باشید.

- Windows Server 2008
- Windows Vista SP1
- Windows Server 2008 R2
- Windows 7

نسخه‌ی Betaی ماژول DIPR را حذف نمایید

اگر شما از نسخه‌ی first Beta ماژول DIPR استفاده می‌کنید باید قبل از نصب نسخه‌ی جدید آن را حذف نمایید، در غیراینصورت نصب با خطا مواجه خواهد شد.

توجه:

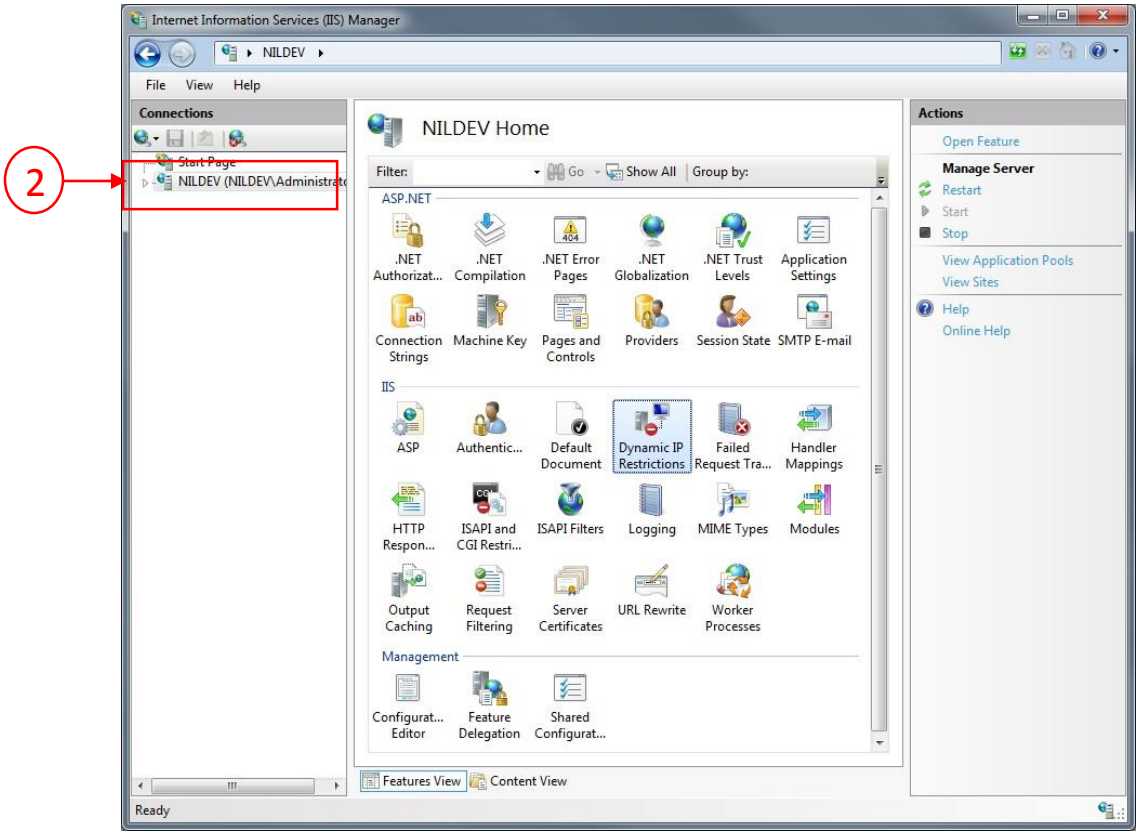
قبل از حذف نسخه‌ی Beta حتما از تنظیمات خود بک آپ تهیه نمایید.

در صورت استفاده از نسخه‌ی Beta2 ماژول DIPR، شما می‌توانید مستقیما آن را به نسخه‌ی نهایی ارتقاء دهید. با این کار تنظیمات شما حفظ خواهد شد.

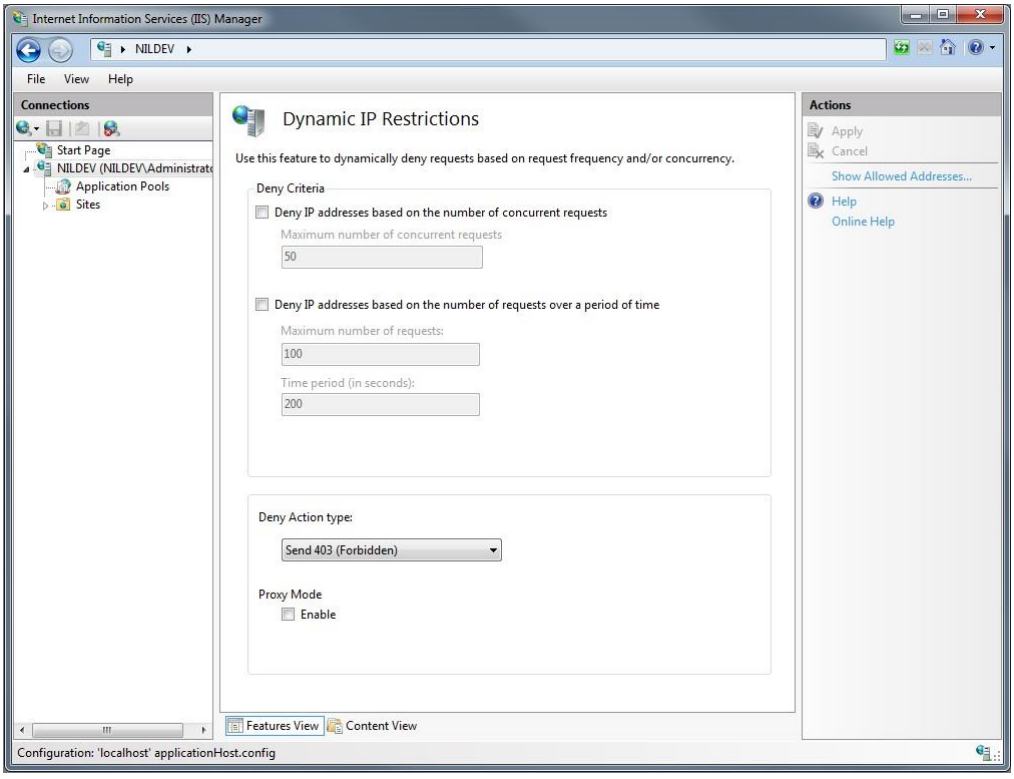
قابلیت Dynamic IP Restrictions را می‌توان با استفاده از **IIS Manager**، **IIS configuration API** یا از طریق ابزار خط فرمان **appcmd** پیکربندی نمود.

جهت دسترسی به تنظیمات *Dynamic IP Restrictions* در *IIS Manager* به صورت زیر عمل نمایید:

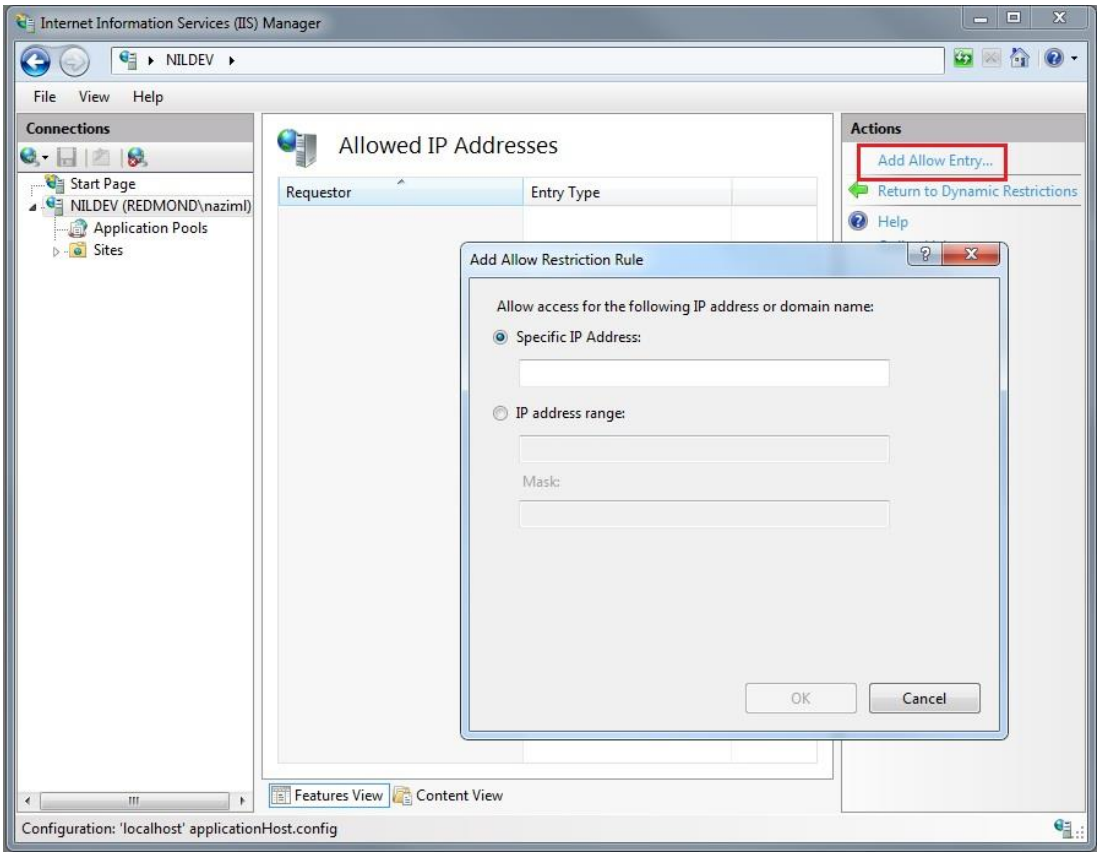
1. IIS Manager را باز کنید.
2. در نمای درختی سمت چپ:
   - اگر می‌خواهید تنظیمات سمت سرور را پیکربندی کنید قسمت Server را انتخاب نمایید.
   - اگر می‌خواهید تنظیمات سایت خاصی را پیکربندی کنید قسمت Site را انتخاب نمایید.
3. در پنجره‌ی باز شده (پنجره‌ی Features view) بر روی "Dynamic IP Restrictions" کلیک کنید.



4. در صفحه‌ی اصلیِ "Dynamic IP Restrictions" شما می‌توانید هر ویژگی دلخواه را فعال یا پیکربندی نمایید. جهت افزودن یک آدرس IP به لیست مجاز (Allow) می‌توانید بر روی لینک "Show Allowed Addresses" در سمت راست کلیک نمایید:



5. پس از انتخاب "Show Allowed Addresses" پنجره‌ای به شکل زیر نشان داده می‌شود که شما می‌توانید در آن لیست تمام آدرس‌های IPای که می‌توانند صحت اعتبار Dynamic IP Restriction را دور بزنند ببینید. شما می‌توانید با انتخاب "Add Allow Entry.." در قسمت بالای سمت راست آدرس‌های IP بیشتری به لیست اضافه نمایید.



مسدود کردن آدرس‌های IP بر اساس تعداد درخواست‌های همزمان

هنگام استفاده از این گزینه، سرور به هر آدرس IP کلاینت اجازه خواهد داد که تنها تعداد قابل تنظیمی درخواستِ همزمان ارسال نماید. هرگونه درخواستی که از این حد تعیین شده تجاوز نماید رد خواهد شد.

یک راه ساده جهت آزمودن این ویژگی این است که حداکثر تعداد درخواست‌های همزمان را مقدار۲ تنظیم نمایید، این کار را می‌توانید با استفاده از UI یا اجرای خط فرمان appcmd انجام دهید.

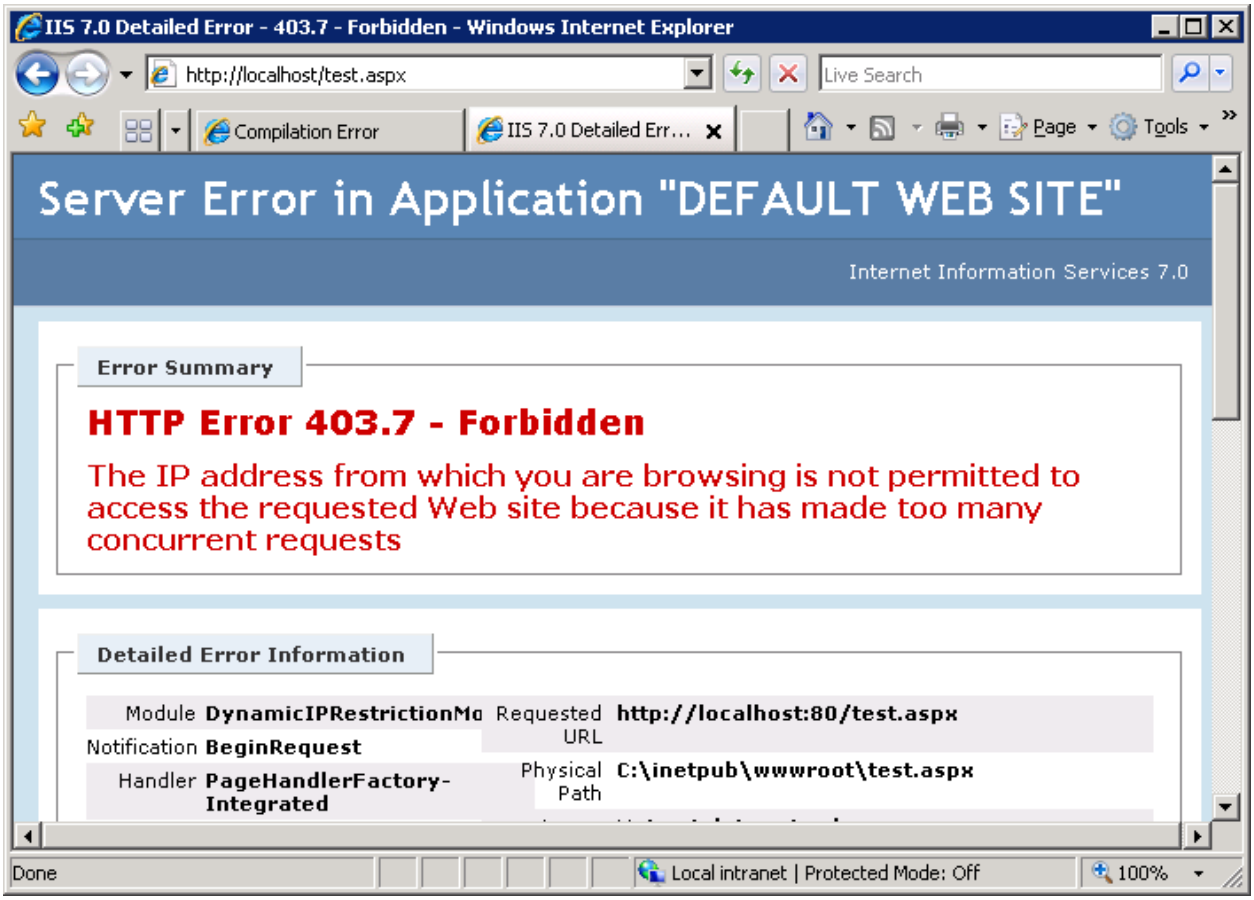
```
%WINDIR%\system32\inetsrv\appcmd.exe set config  -
setion:system.webServer/security/dynamicIpSecurity
/denyByConcurrentRequests.enabled:"True "
/denyByConcurrentRequests.maxConcurrentRequests:"2 "
/commit:apphost
```

در پوشه‌ی ریشه (Root) وب سایت یک فایل test.aspx ایجاد کنید و محتوای زیر را در آن کپی نمایید.

aspx Copy

```aspx
<%@ Page Language="C#" %>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org
<script runat="server">
protected void Page_Load(object sender, EventArgs e)
{
 System.Threading.Thread.Sleep(3000);
}
</script>
<html xmlns="http://www.w3.org/1999/xhtml">
 <head runat="server">
 <title>Dynamic IP Restrictions Test</title>
 </head>
 <body>
 <form id="form1" runat="server">
 <div>
 <h1>Hello World!</h1>
 </div>
 </form>
 </body>
</html>
```

این صفحه‌ی ASP.NET قبل از بازگرداندن هر گونه پاسخی به مدت ۳ ثانیه نشان داده خواهد شد. این فایل را ذخیره نموده و سپس مرورگر خود را باز کنید، آدرس http://localhost/test.aspx را در آن وارد نمایید، در ادامه کلید F5 را جهت رفرش نمودن صفحه بفشارید. این در مرورگر منجر به ایجاد بیش از ۲ درخواست همزمان خواهد شد و همانطور که می‌بینید خطای ۴۰۳ مشاهده می‌شود_ خطای Forbidden از جانب سرور:



مسدود کردن آدرس‌های IP بر اساس تعداد درخواست‌ها در طول زمان

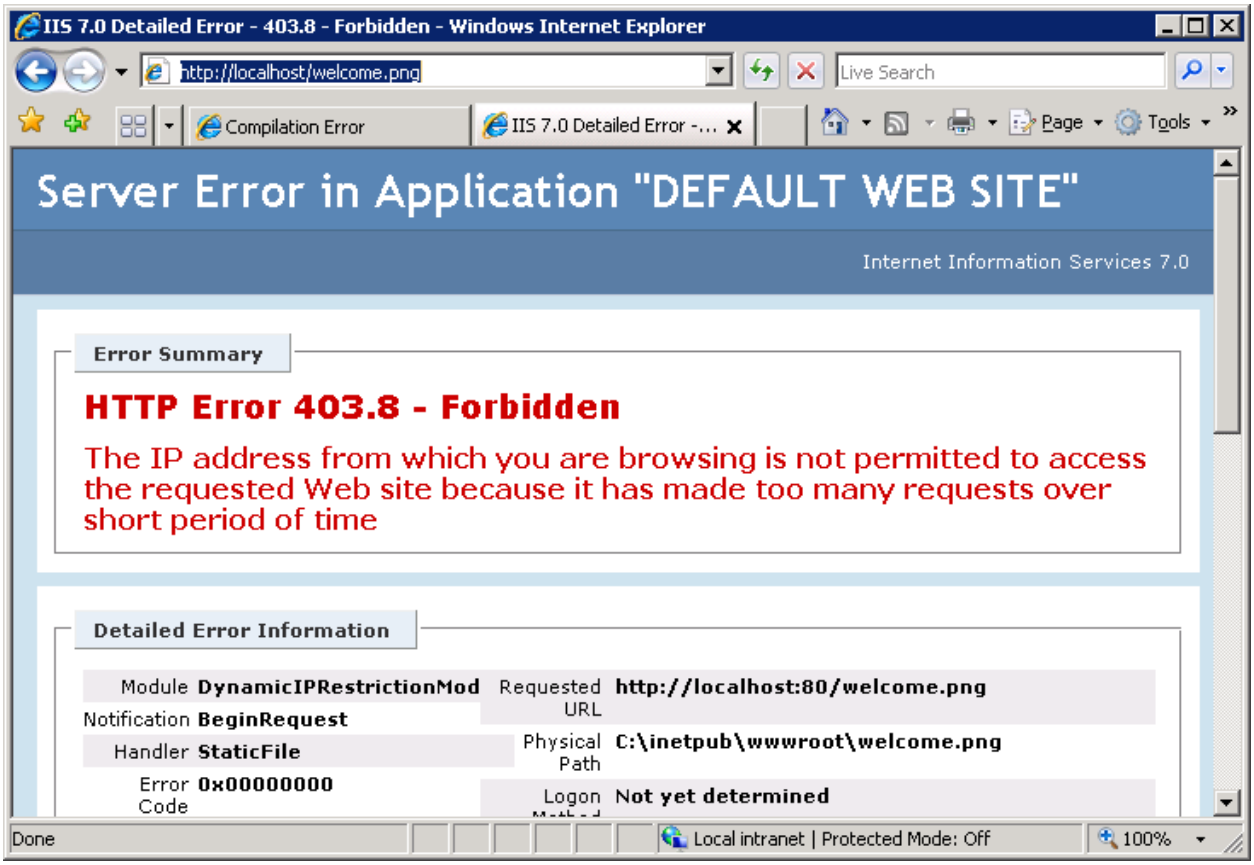
هنگام استفاده از این گزینه، سرور، درخواستِ هر آدرس IP کلاینتِ HTTP را که تعداد درخواست آن بیش از تعداد تنظیم شده در طول یک دوره‌ی زمانی باشد رد خواهد نمود. این آدرس IP در حالت مسدود باقی خواهد ماند تا زمانی که تعداد درخواست‌های آن در یک دوره‌ی زمانی کمتر از مقدار تنظیم شده باشد.

برای تست این ویژگی، با استفاده از IIS Manager و یا با اجرای خط فرمان appcmd، مقدار "Maximum number of requests" را 5 و "Time period" را 5000 تنظیم نمایید.

```
%WINDIR%\system32\inetsrv\appcmd.exe set config  -
section:system.webServer/security/dynamicIpSecurity
/denyByRequestRate.enabled:"True" /denyByRequestRate.maxRequests:"5"
/denyByRequestRate.requestIntervalInMilliseconds:"5000"

/commit:apphost
```

مرورگر را باز کرده و آدرس http://localhost/welcome.png را وارد نمایید، سپس کلید F5 را به طور مداوم جهت رفرش نمودن صفحه بفشارید. این در واقع بیش از ۵ بار درخواست در طول ۵ ثانیه است و همانطور که در تصویر زیر می‌بینید سرور کد خطای 403 را بازمی‌گرداند_ کد وضعیتِ Forbidden



اگر شما ۵ ثانیه دیگر صبر کنید که تمام درخواست‌های قبلی اجرا شوند و سپس درخواست ارسال نمایید، درخواست موفقیت‌آمیز خواهد بود.

اقدامات رد درخواست

این ماژول می‌تواند جهت انجام اقدامات زیر هنگام رد درخواستِ آدرس‌های IP پیکربندی گردد:

- ارسال پاسخ 403 برای کلاینت (Forbidden)

- ارسال پاسخ 404 برای کلاینت (File not found)
- نادیده گرفتن درخواست با قطع کردن اتصال HTTP، بدون ارسال هیچگونه پاسخی برای کلاینت

منبع:

https://docs.microsoft.com/en-us/iis/manage/configuring-security/using-dynamic-ip-restrictions