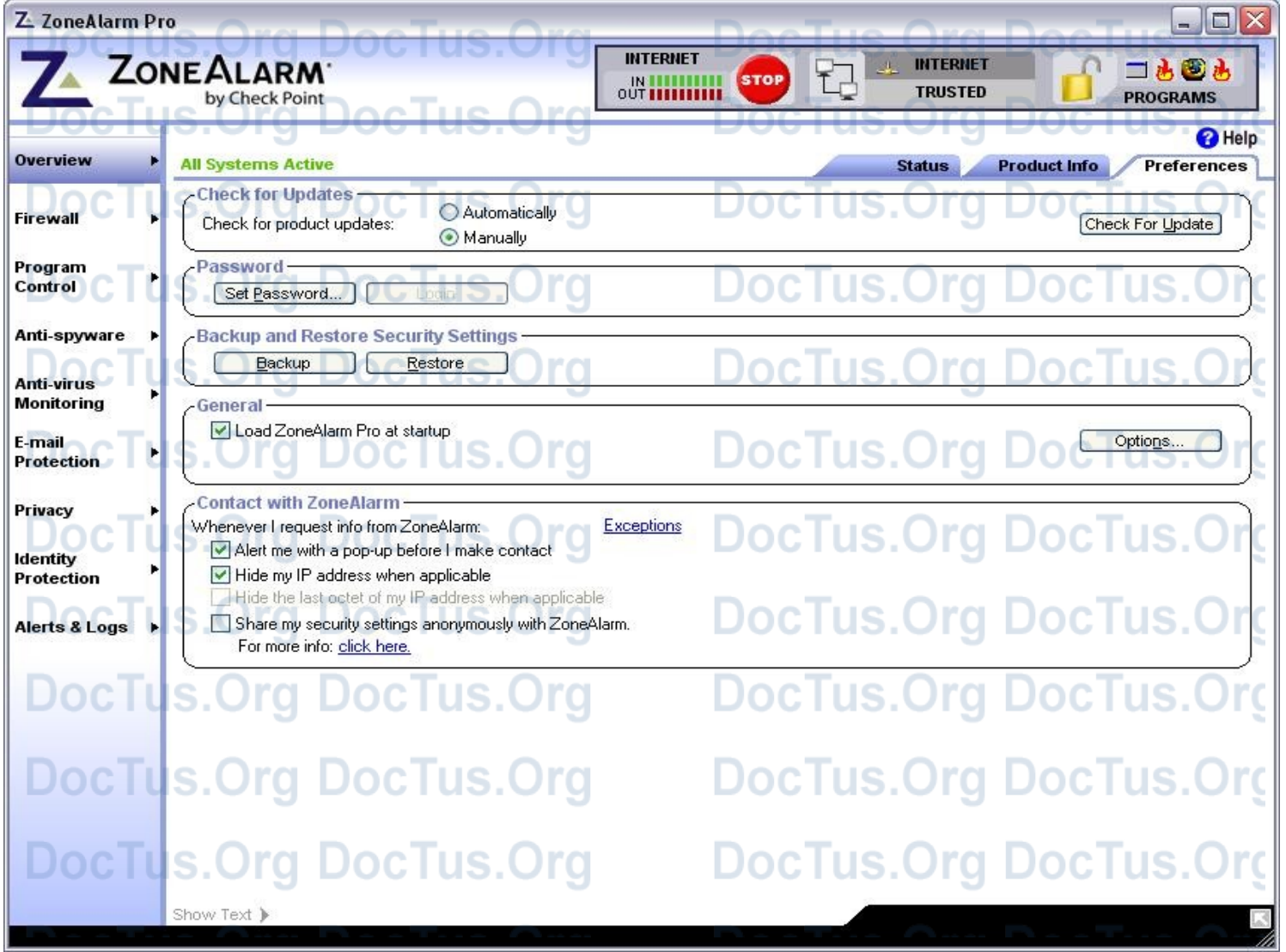


Gelişmiş Ayarlar

Sadece gelişmiş ileri seviye ayarlara değinilmiştir. **Stealth mode** (gizli mod) için kendi kullandığım ayarlar; **Overview** sekmesinde **Preferences** tabında ayarlar aşağıdaki gibi.



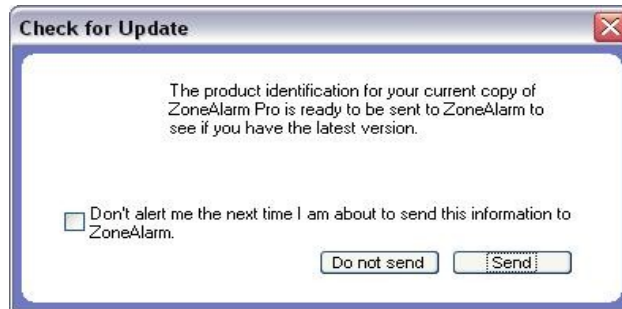
The screenshot shows the ZoneAlarm Pro Preferences window. The left sidebar lists various security features: Overview, Firewall, Program Control, Anti-spyware, Anti-virus Monitoring, E-mail Protection, Privacy, Identity Protection, and Alerts & Logs. The main area is divided into several sections:

- Check for Updates:** Includes a status bar for INTERNET (IN/OUT) and a STOP button. Below it, there are radio buttons for "Automatically" and "Manually", and a "Check For Update" button.
- Password:** Includes "Set Password..." and "Upgrade" buttons.
- Backup and Restore Security Settings:** Includes "Backup" and "Restore" buttons.
- General:** Includes a checked checkbox for "Load ZoneAlarm Pro at startup" and an "Options..." button.
- Contact with ZoneAlarm:** Includes a "Whenever I request info from ZoneAlarm:" section with a link to "Exceptions". Below it are three checkboxes: "Alert me with a pop-up before I make contact" (checked), "Hide my IP address when applicable" (checked), and "Hide the last octet of my IP address when applicable" (unchecked). There is also an unchecked checkbox for "Share my security settings anonymously with ZoneAlarm." and a link "For more info: click here."

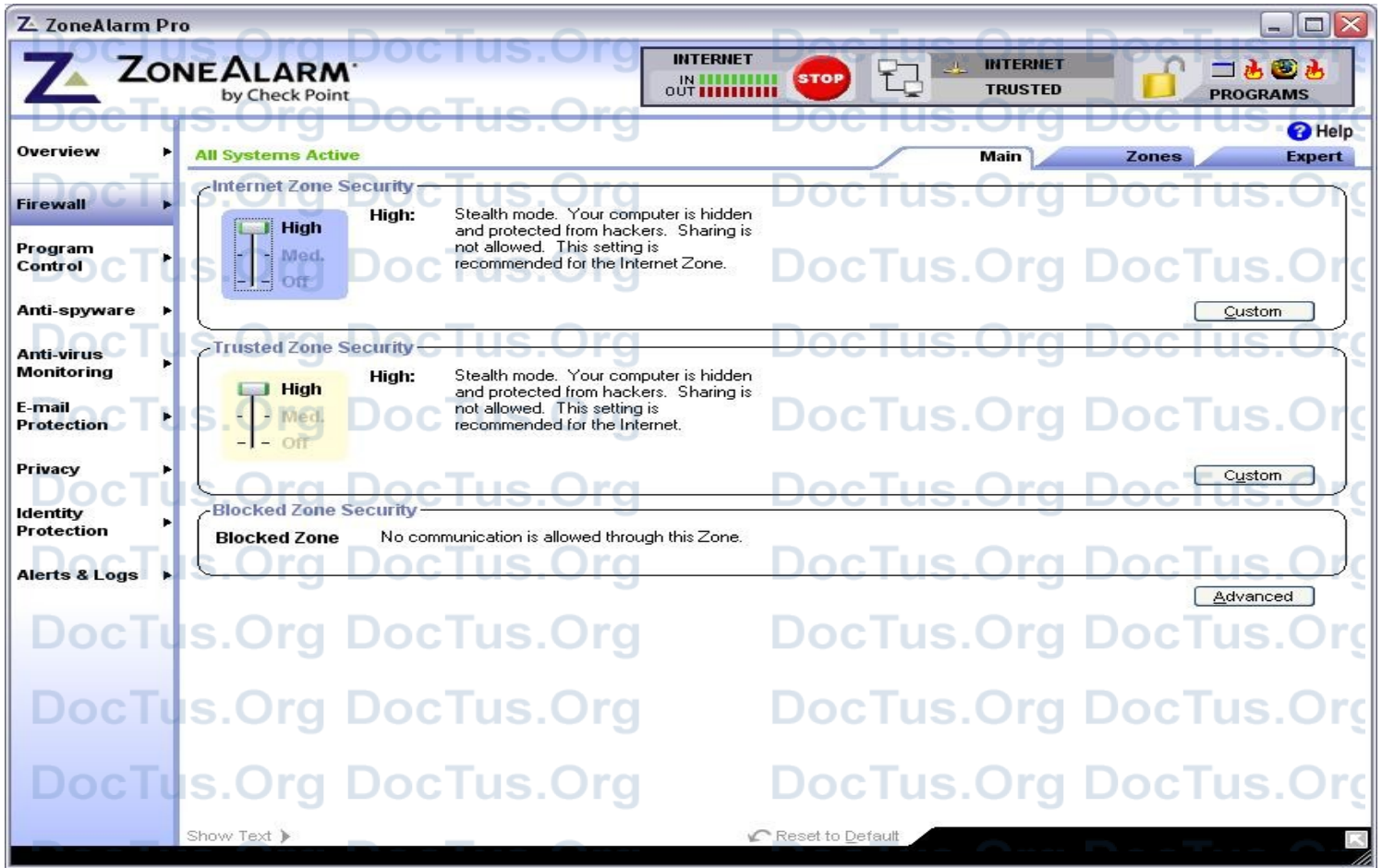
At the bottom left, there is a "Show Text" link.

Contact with ZoneAlarm bölümünde

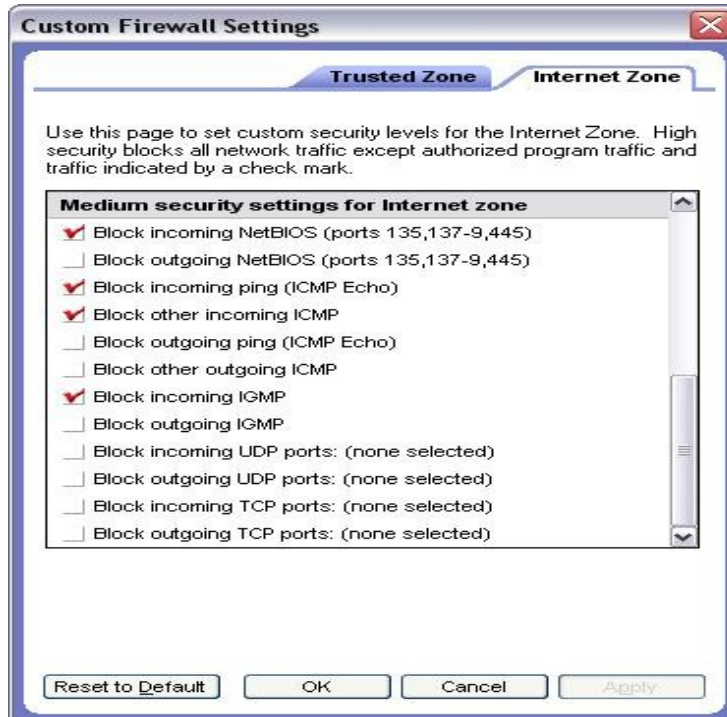
Alert me with a pop-up before I make contact kutusu işaretlenerek, program güncelleme için sunucuya bağlanmak istediğinde aşağıdaki gibi açılan bir pencere ile uyarılırsınız.



Firewall sekmesi **Main** tabında kendi kullandığım ayarlar aşağıdaki gibi. Port taramalarında sisteminizde açık görünmemesi için **High** olarak seçiyoruz.



Internet Zone Security bölümündeki **Custom** butonuna tıklayarak açılan penceredeki Firewall ayarlarını aşağıdaki gibi seçerek **Apply** butonuna tıklıyoruz ve gereksiz ping isteklerini de önleyip tamamen gizli moda geçiyoruz.



Advanced butonuna tıklayıp açılan pencerede firewallı aşağıdaki gibi ayarlıyoruz.

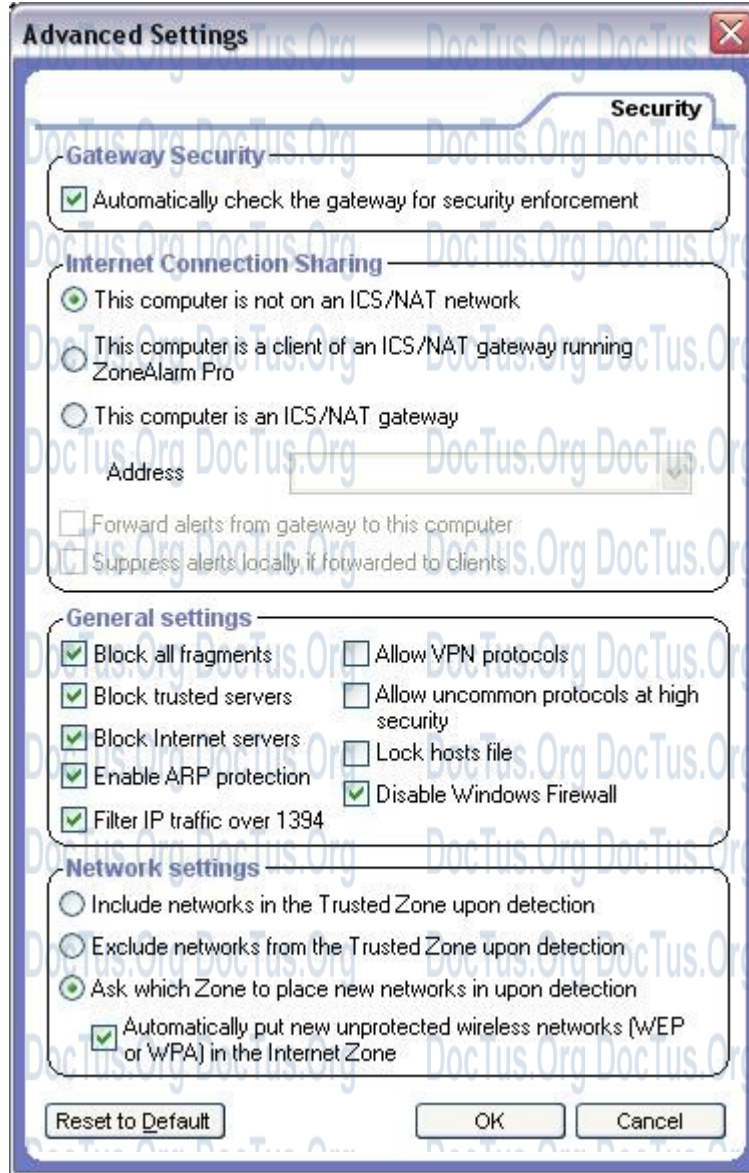
Tüm server çıkışlarını ve parçalanmış paketleri engelliyoruz.

ARP protection Firewall arkasında kalan donanımımıza ait kimlik bilgisini koruyor (MAC ID)

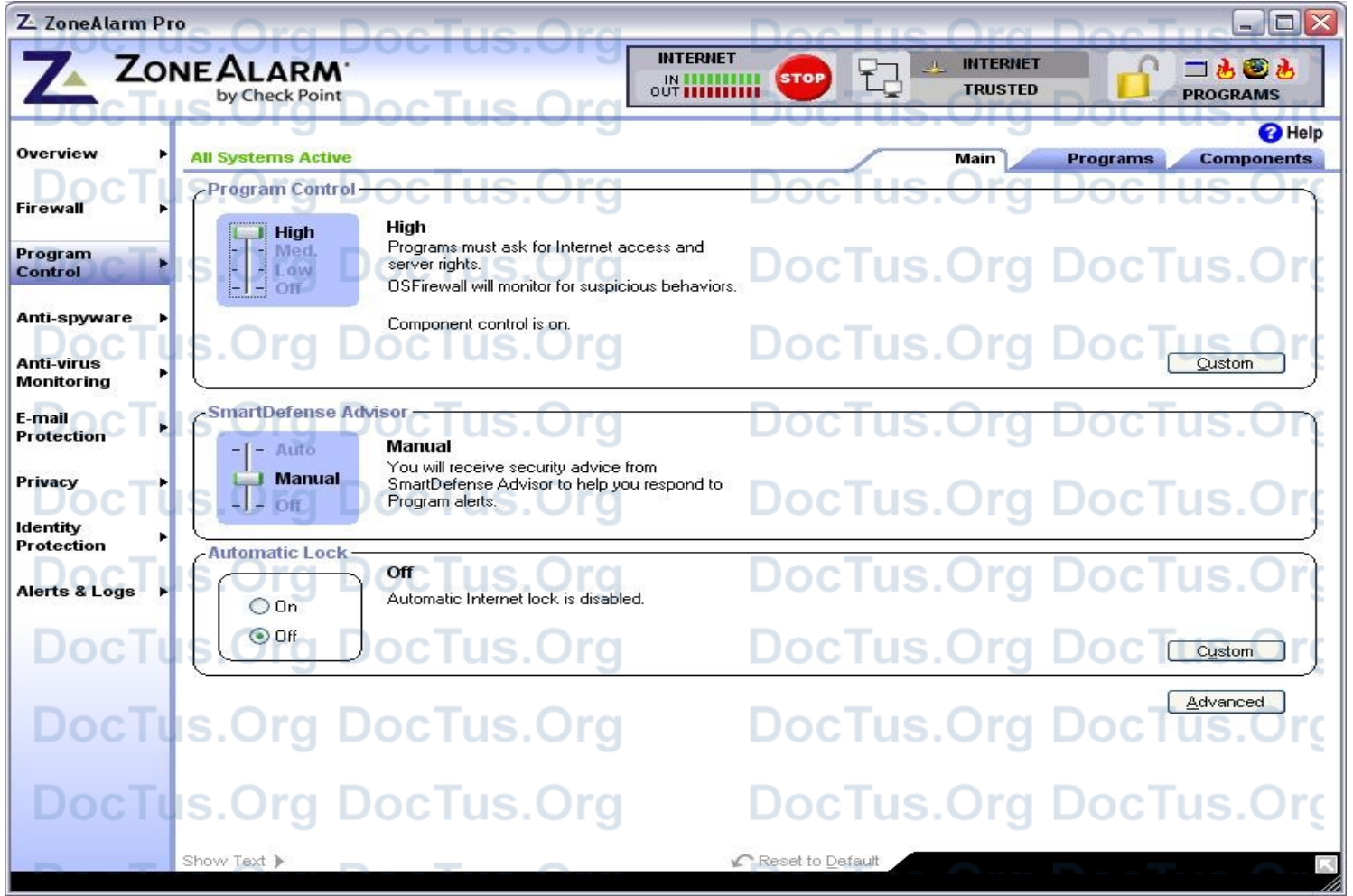
Uzak masaüstü bağlantı filtresinide aktif ederek istem dışı bağlantılar isteklerinden haberdar olabiliriz.

Herhangi bir ağa bağlı olmadığım ve USB modem kullandığım için "**Internet Connection Sharing**" herhangi bir bağlantı paylaşımı yapmıyoruz.

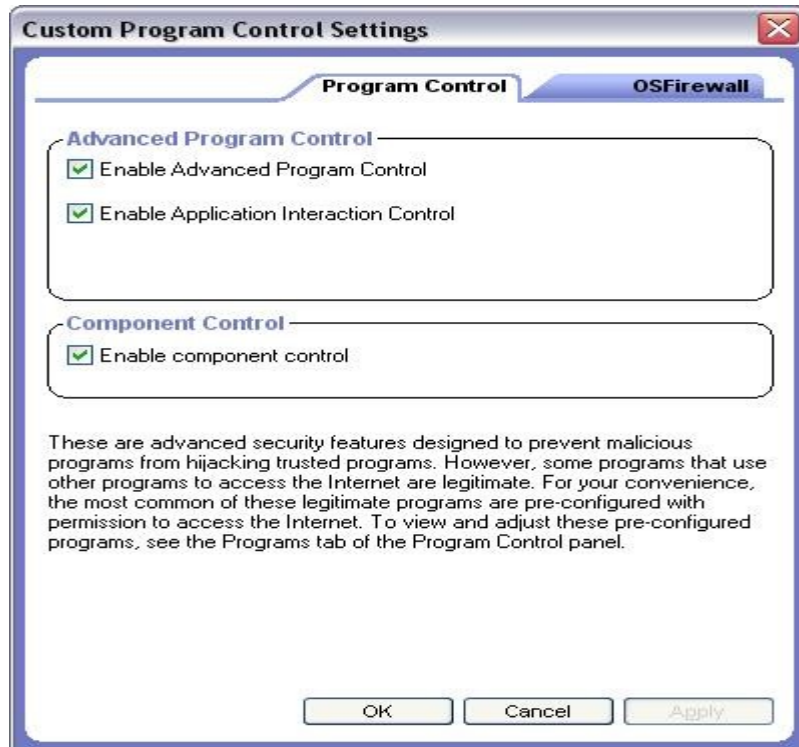
General settings bölümündeki ayarlar dışında kalan bölümler USB modem için varsayılan olarak şekildeki gibi.



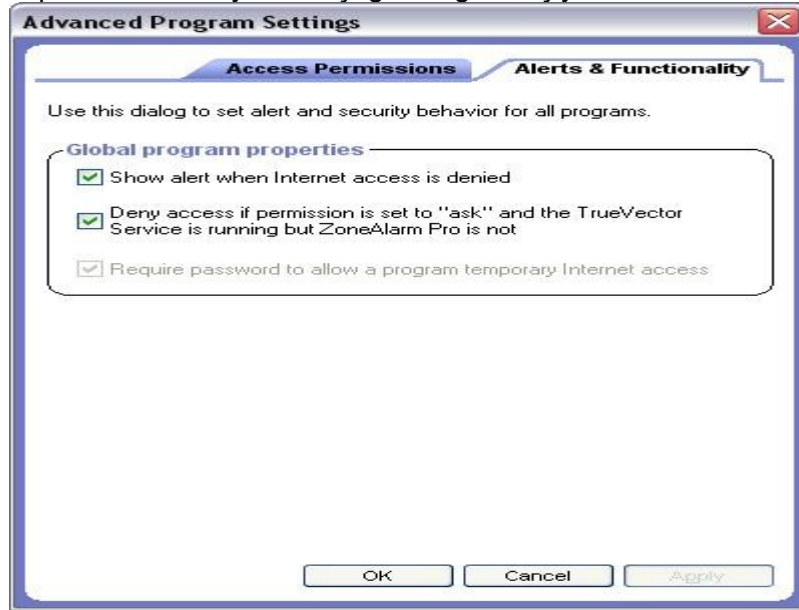
Program Control sekmesi **Main** tabında ayarlar aşağıda görüldüğü gibi.



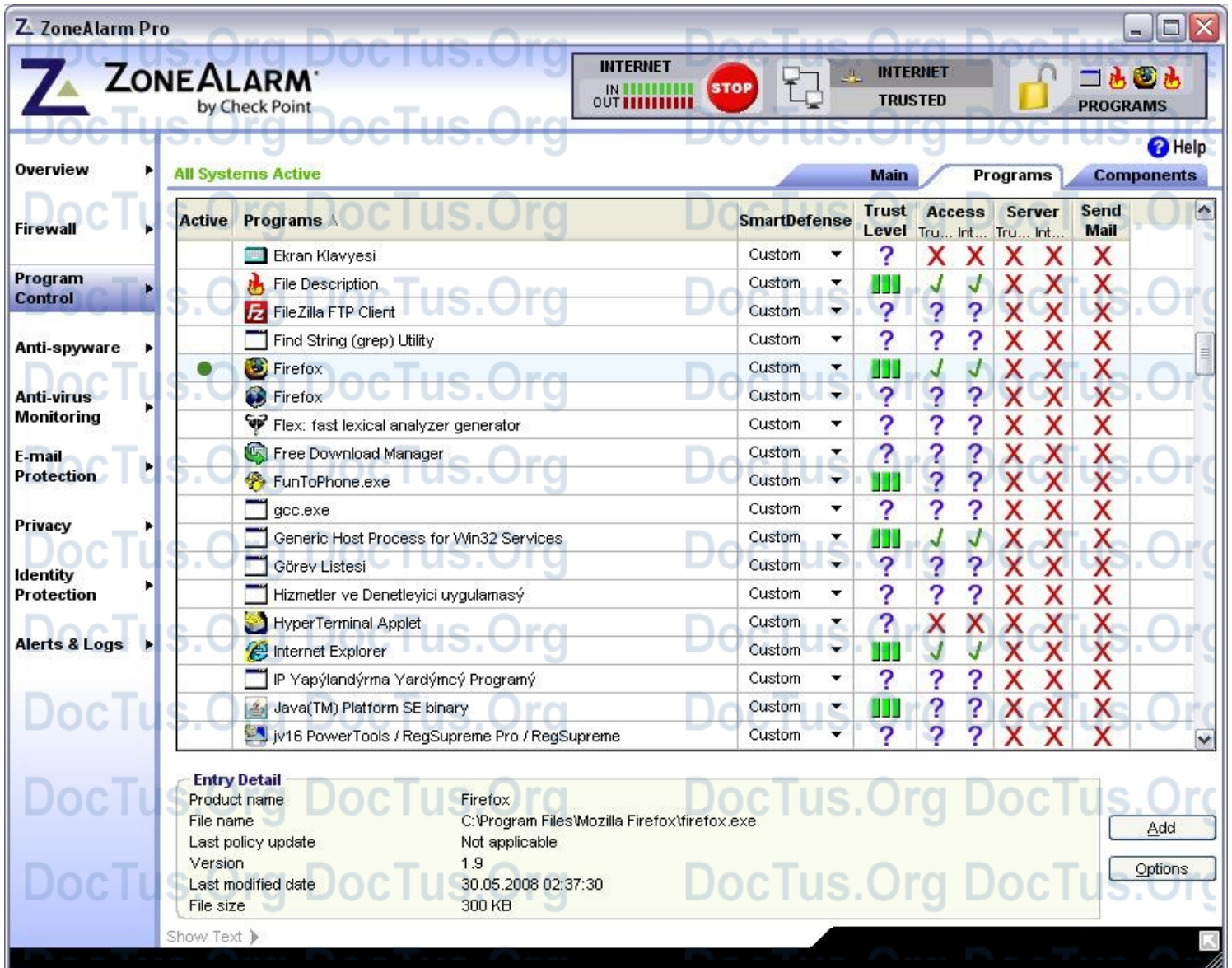
Program Control bölümündeki **Custom** butonu ile açılan pencereki ayarlar aşağıdaki gibi seçiyoruz.



Advanced butonu ile açılan pencerede ki ayarları aşağıdaki gibi seçiyoruz.



Program Control sekmesi **Programs** tabı için bazı programlara ait ayarlar aşağıdaki gibi.



Kurulumdan sonra programlar kullanıldıkça bu bölümde beliren her satır için **Server** ve **Send Mail** sütunu bloklanabilir. Tabi Eğer sisteminizde kurulu web server gibi bir programın server çıkışına izin vermez iseniz localden web host edemezsiniz. Online oynanan oyunlar içinde yine server çıkışları bloklanmamalıdır.

The screenshot shows the ZoneAlarm Pro interface with the 'Programs' tab selected. The main window displays a list of active programs with columns for SmartDefense, Trust Level, Access, Server, and Send Mail. A context menu is open over the Firefox entry, showing options like 'Options...', 'Properties...', 'Remove', and 'Add program...'. The 'Entry Detail' section at the bottom left shows information for Firefox, including its file name, version, and last modified date.

Active	Programs	SmartDefense	Trust Level	Access	Server	Send Mail
	Ekran Klavyesi	Custom	?	X X	X X	X
	File Description	Custom	?	X X	X X	X
	FileZilla FTP Client	Custom	?	X X	X X	X
	Find String (grep) Utility	Custom	?	X X	X X	X
	Firefox	Custom	?	X X	X X	X
	Firefox	Custom	?	X X	X X	X
	Flex: fast lexical analyzer generator	Custom	?	X X	X X	X
	Free Download Manager	Custom	?	X X	X X	X
	FunToPhone.exe	Custom	?	X X	X X	X
	gcc.exe	Custom	?	X X	X X	X
	Generic Host Process for Win32 Services	Custom	?	X X	X X	X
	Görev Listesi	Custom	?	X X	X X	X
	Hizmetler ve Denetleyici uygulaması	Custom	?	X X	X X	X
	HyperTerminal Applet	Custom	?	X X	X X	X
	Internet Explorer	Custom	?	X X	X X	X
	IP Yapılandırma Yardımcı Programı	Custom	?	X X	X X	X
	Java(TM) Platform SE binary	Custom	?	X X	X X	X
	jv16 PowerTools / RegSupreme Pro / RegSupreme	Custom	?	X X	X X	X

Her program için sağ tık menüsündeki **Options** tıklanarak özel güvenlik ayarları ve kural atamaları yapılabilir. Firefox için seçtiğimiz **Security** ayarları hemen hemen her programa uygulanabilir.

The screenshot shows the 'Program Options' dialog box for Firefox. The 'Security' tab is selected, and the 'Advanced Program Control' section is expanded. The 'This program may use other programs to access the Internet' checkbox is checked. Other sections include 'Filter Options', 'Authentication', and 'Passlock'.

Program Options

Customize the program security level for:

Firefox
Version: 1.9

Advanced Program Control

This program may use other programs to access the Internet
 Allow Application Interaction

Filter Options

Enable Privacy for this program

Authentication

Authenticate components
 Authenticate program by full path name only

Passlock

Enable Passlock

Reset to Default OK Cancel Apply

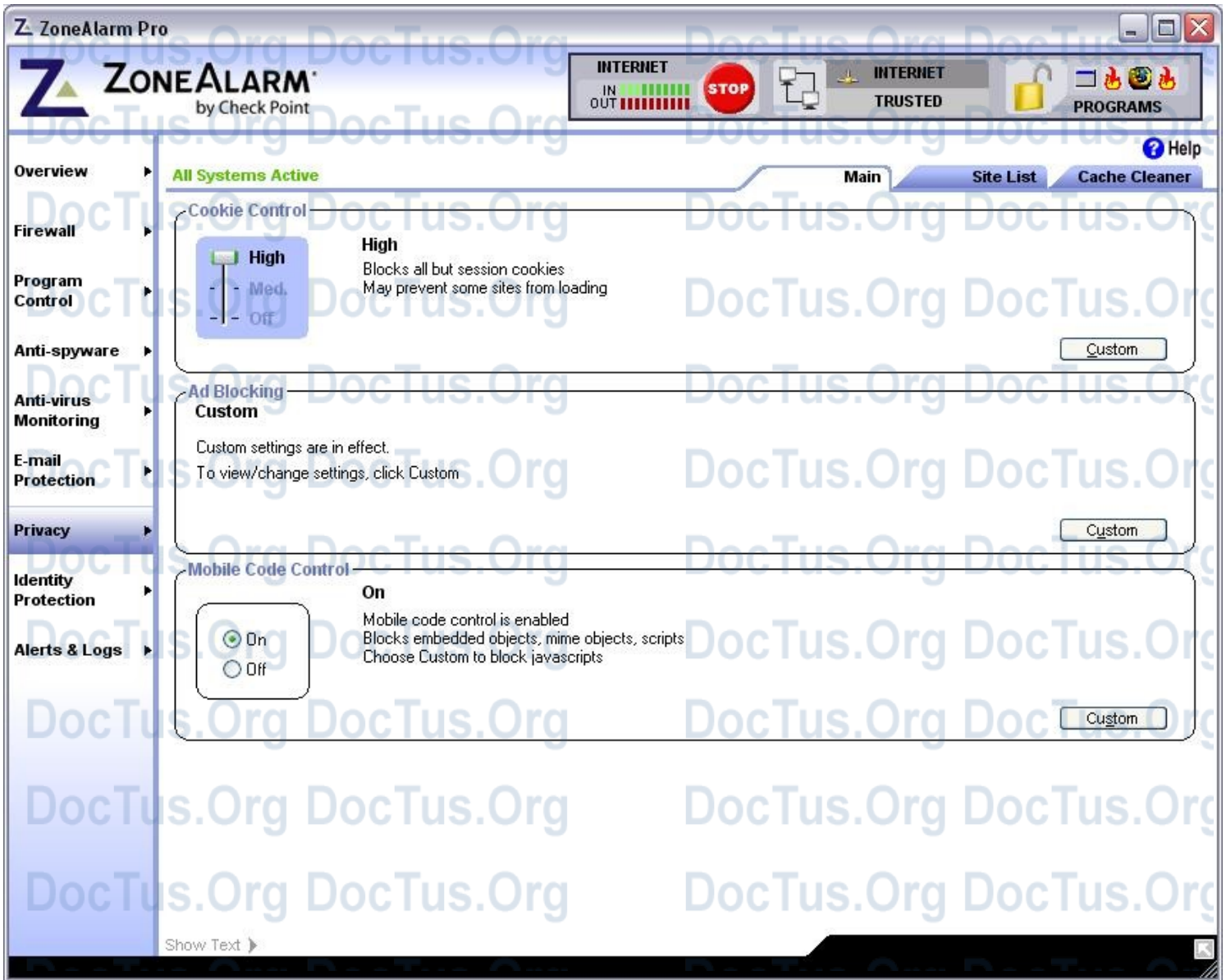
Yukarıdaki pencerede “**Enable Privacy for this program**” seçildiğinde ilgili program **Privacy** filtresine eklenir ve bu programın internete yaptığı istekler bu filtreden geçer.

“**Authenticate components**” seçilerek Programa ait bileşenler de control edilebilir. (import edilmiş dll' ler vs. gibi) Herhangi bir uygulamaya inject edilmiş dll' den bir fonksiyon çağırılmak istendiğinde uyarılırsınız.

“**This program may use other programs to access the internet**” seçilerek ilgili program üzerinden internete bağlanmaya çalışan farklı bir program olduğunda uyarı alırsınız. (mesela Messenger uygulamasındaki mail butonu tıklandığında IE, posta kutunuzu açmak için internete bağlanmak ister.)

“**Authenticate program by full path name only**” seçildiğinde ilgili program sadece kendi dizininden çalıştırıldığına bu ayarlar geçerli olur. Farklı bir dizinden çalıştırıldığında **Programs** tabında yeni bir satır oluşur.

Privacy sekmesinde **Main** tabında ki ayarları aşağıdaki gibi seçiyoruz.



Ad Blocking bölümünde **Custom** butonuna tıklayıp açılan pencerede ki ayarları aşağıdaki gibi değiştiriyoruz.

Aynı bilgisayarda 2 firewall kullanılmayacağı gibi aynı görevi üstlenmiş farklı bir yazılımın ilgili modülünde (Avira web guard, Kaspersky port monitoring vs. gibi.) işletim sistemi OSI katmanında aynı anda filtreleme yapacağı için sistem kararsızlığına neden olur.

ZoneAlarm ile beraber Avira Antivirüs kullanan bir kullanıcının, Avira web guard özelliğini deaktif etmesi gerekir. Aksi durumda ZoneAlarm firewallının çalıştığı halde filtreleme yapmadığını görebilirsiniz.

Avira web guard özelliği ZoneAlarmı bypass etmiştir.

Avira web guard, sadece imza veribani ile sınırlı bir tanımlama yetisine sahiptir. ZeroDay olarak bilinen 0 günü güvenlik açıkları AV imza veritabanlarında olmadığı için bu tür bir açıkla exploit edilmiş bir web sitesini ziyaretiniz sırasında web guard zararlıyı es geçecektir.

0 günü açıklarından firewallda sizi koruyamaz ama diğer güvenlik duvarlarında olmayan Privacy Control özelliği sayesinde, ZoneAlarm sizi bu açıkra karşıda korur. Fakat hiçbir yazılımda olmadığı gibi Zone alarmda %100 güvenlik sağlayamaz. Güvendiğiniz bir site için Privacy bölümünde gerekli tüm izinleri verdikten sonra kötü niyetli kişilerce güvendiğiniz bu sitedeki uygulama hatalarından dolayı içeriğe inject edilmiş zararlı kodlardan siteyi ziyaretiniz sırasında sizde etkilenirsiniz.

Bu ayarlar USB modem kurulu olan WinXP SP3 makinada, ZoneAlarm Pro v7.0.473 sürümü için yapılmıştır.

<http://7f6343.blogspot.com>

osC++CoDeR's BLOG

SECURITY service & research

Kaynak gösterilerek dağıtılabilir.