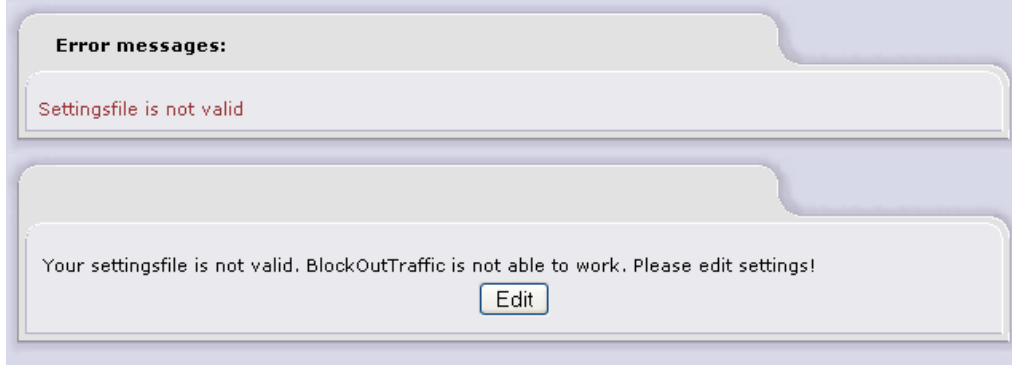


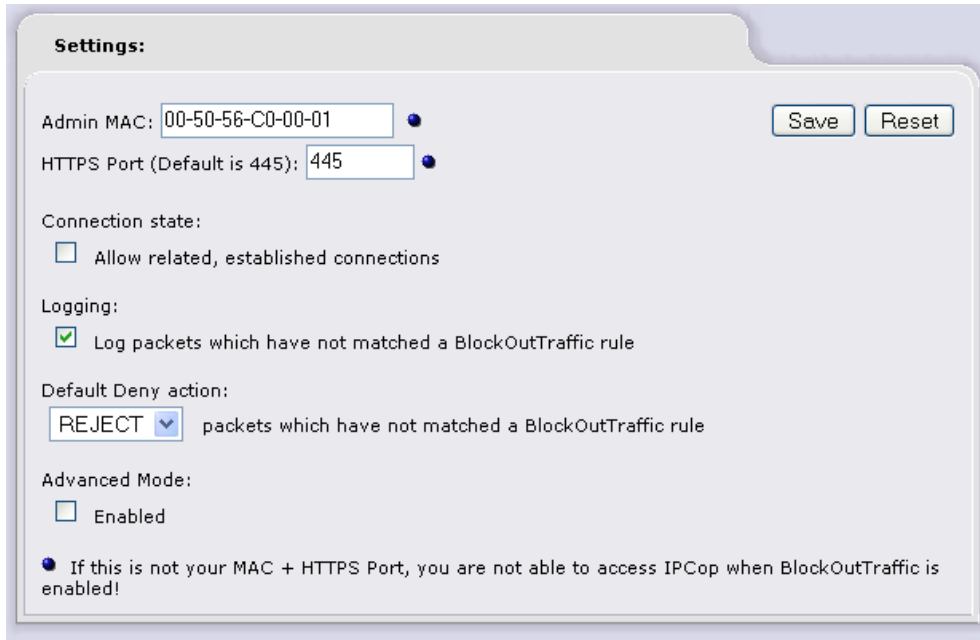
# BOT - Başlangıç

## Başlangıç Konfigrasyonu

BOT aktive edilmmeden önce BOT yöneticiliğini yapacak olan PC ayarları tanımlanmalıdır. Bunun için: IPCop WebGUI goto Firewall -> BlockOutTraffic seçilmeden sonra aşağıdaki menü açılır.



**BOT ayarlarını girmelisiniz:**



**Admin MAC:**

BOT'u yönetecek olan bilgisayarın MAC adresi.

**HTTPS Port:**

IPCop Web arayüzüne eriştiğiniz https portu.

BOT 'geçerli yönetici erişim kuralı' olarak bu MAC adresini kullanır. Böylece IPCop erişimlerinizde Web arayüzü erişiminizin kesilmemesi garantilenir. Bu yüzden bu ayarı yapmanız gerekir.

**Connection state (Bağlantı Durumu):**

BOT will allow traffic which belongs to a related or established connection if you enable this option. When you use Port-Forwardings (for example to an internal webserver) you should enable this option.

BOT erişilmiş yada ilişkilendirilmiş bağlantılara izin vermesi için bu seçeneği etkinleştirmelisiniz. Port yönlendirmeleri (örneğin iç web sunucusuna) kullandığınızda bu seçeneği etkinleştirmeniz gerekir.

**Logging (Kayıt):**

Bu seçeneği etkinleştirdiğiniz BOT trafik kuralları tarafından tanımlanmamış durumların kayıtlarını tutmasını sağlarsınız.

**Default Deny action (Geçerli REDDET hareketi):**

Tanımlanan trafik kuralları dışındaki hareketler için BOT'un yapacağı hareketi buradan tanımlayabilirsiniz. DROP: Bağlantıyı düşürmek için. REJECT: Bağlantıyı reddetmek için. ACCEPT: Bağlantıyı kabul etmek için.

#### Advanced Mode (Gelişmiş Mod):

Bu seçeneği seçtiğiniz zaman BOT'u ayarlamak için daha fazla seçeneğe sahip olacaksınız. Bu mod ancak ve ancak firewall konusunda derin bilgiye sahip kişiler tarafından kullanılacak üzere açılmalıdır.

'Save' butonuna tıkladığınız zaman bu ayarlar kaydedilir. BOT'u gelişmiş ayarlarla kaydettiğiniz zaman Firewall -> Advanced BOT Config seçeneği web arayüzünde gözükür:



Öncelikle çeşitli servisleri bilgisayardan tanımlamalısınız, bu tanımlamaları daha sonra BOT kurallarınızı tanımlarken kullanabilirsiniz:

**BlockOutTraffic:**

BlockOutTraffic is **Disabled** Services settings Show Firewall Config

**Add service:**

Service Name  Invert  Ports  Invert  Protocol  ICMP Type:

Add Reset

**Custom services:**

Service Name	Ports	Protocol	ICMP Type	Used
IPCop SSH	222	TCP	N/A	1x
IPCop https	445	TCP	N/A	1x
IPCop proxy	800	TCP	N/A	1x

**Default services:**

Service Name	Ports	Protocol
acap	674	TCP & UDP
afbackup	2988	TCP & UDP
afpovertcp	548	TCP & UDP
afs3-bos	7007	TCP & UDP
afs3-callback	7001	TCP & UDP
afs3-errors	7006	TCP & UDP
afs3-fileserver	7000	TCP & UDP
afs3-kaserver	7004	TCP & UDP
afs3-prserver	7002	TCP & UDP
afs3-rtmfs	7003	TCP & UDP

Burada ekran görüntülerinde de görebileceğini üç adet özelleştirebileceğiniz servis var:

- IPCop ssh, IPCop'u ssh üzerinden yönetebilmeniz için gereklidir.
- IPCop https, IPCop'u web arayüzünden kullanabilmeniz için gereklidir. 'Admin MAC' (Yönetici MAC) adresine sahip olan bilgisayar her zaman için ulaşabilir. Ancak bu bilgisayar dışındaki bilgisayarın da erişimine izin vermek isteyebilirsiniz.
- IPCop proxy (vekil), IPCop vekil sunucu üzerine erişip internet üzerinde sörf yapabilmek için kural oluşturmanızı sağlar.

Daha sonra servis gruplarını (Service Grouping), adres tanımlarını (Address settings), adres gruplamalarını (Address Grouping) veya arayüz ayarlarını (Interface Settings) yapabilirsiniz:

**BlockOutTraffic:**

BlockOutTraffic is **Disabled**

Services settings

Services settings  
Service Grouping  
Address settings  
Address Grouping  
Interfaces settings

**Add service:**

Service Name	Export	Ports	Event	Interface
--------------	--------	-------	-------	-----------

'Service Grouping' (Servis grupları) seçeneğini seçtiğinizde aşağıdaki ekranı görürsünüz:

**BlockOutTraffic:**

BlockOutTraffic is **Disabled**

Service Grouping

**Add service to Group:**

Service Group name:  Remark:

Service Group name:

Default services:

Custom services:

Enabled:

This field may be blank.

**Service Groups:**

**Default services - Some services for internet access - Used 1x :**

smtp	Default	<input checked="" type="checkbox"/>	<input type="checkbox"/>
smtps	Default	<input checked="" type="checkbox"/>	<input type="checkbox"/>
pop3	Default	<input checked="" type="checkbox"/>	<input type="checkbox"/>
pop3s	Default	<input checked="" type="checkbox"/>	<input type="checkbox"/>
imap	Default	<input checked="" type="checkbox"/>	<input type="checkbox"/>
imaps	Default	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**IPCop admin - Services to administrate IPCop - Used 1x :**

IPCop SSH	Custom	<input checked="" type="checkbox"/>	<input type="checkbox"/>
IPCop https	Custom	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**IPCop services - Some services on IPCop - Used 1x :**

domain	Default	<input checked="" type="checkbox"/>	<input type="checkbox"/>
IPCop proxy	Custom	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ntp	Default	<input checked="" type="checkbox"/>	<input type="checkbox"/>
bootpc	Default	<input checked="" type="checkbox"/>	<input type="checkbox"/>
bootps	Default	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Yukarıdaki ekran görüntüsünde şu gruplar tanımlanmaktadır:

- Geçerli olan servisler (e-posta ile ilgili olanlar) iç ağdaki bilgisayarların internet üzerinden erişmelerini istediğiniz servisleri tanımlayabilirsiniz.
- IPCop admin (IPCop yönetici), IPCop yönetimi için gerekli servisleri barındırır. Bu grup birden fazla bilgisayarın IPCop yönetimi erişimi için elverişlidir.
- IPCop servisleri DNS, Proxy, NTP ve DHCP gibi servisleri barındırır. Bu grup bilgisayarınızın bu IPCop servislerini kullanabilmelerini sağlar.

Bu servisleri ve servis gruplarını tanımladıktan sonra, BOT kuralları tanımlamalarında kullanabilirsiniz.

Yapılması gereken ne iş kaldı? İç bilgisayarlara izin verilmesi.

- e-posta alıp vermeleri için izinlerin tanımlanması,
- IPCop webproxy üzerinden sörf izni verilmesi,
- IPCop üzerinden DNS, DHCP ve NTP servislerini kullanma izni tanımlanması,
- sonra, IPCop yönetimi yapmak üzere gerekli olan bilgisayarlara web arayüzü ve ssh erişimi haklarını tanımlıyoruz.

Biz zaten servis gruplarımızı arşivlemiştik. Yani artık ilk BOT kuralımızı yazabiliriz, Yerel ağ üzerindeki bilgisayarlara IPCop servislerini kullanma izni veriyoruz.

BlockOutTraffic bölümüne dönün (Webgui -> Firewall -> BlockOutTraffic) ve 'Add a new rule' (Yeni kural ekleyin) seçeneğini seçin. Aşağıdaki arayüzü göreceksiniz. Firewall kuralları için çeşitli seçenekler göreceksiniz. Firewall seçenekleri şu kategorilere göre gruplanmıştır: source (kaynak), destination (hedef), additional settings (ek ayarlar) ve timeframe (zaman aralığı) (kural için çalışma zamanı belirlemek isterseniz kullanın).

Green (Yeşil) ağınızdaki bilgisayarlara IPCop servis erişimlerini vermek için kaynak seçimleriniz:

- Default interface (Geçerli arabirim): Green (Yeşil)
- Default networks (Geçerli ağlar): Green Network (Yeşil Ağ)

ve hedef olarak:

- IPCop erişimi
- 'Service' ve 'Service Group' "IPCop services" i kullanın (advanced BOT config içerisinde daha önce tanımladığınız)

Kural enabled (geçerli) olarak seçilmelidir. İsterseniz kurala açıklama da yazabilirsiniz.

Bu kuralı eklemenin iki yolu var. [Next] veya [Save] tuşuna tıklamak. [Save] tuşu ile kuralı kaydederseniz ve kuralı BOT kural listesinin en altına eklersiniz. [Next] tuşu ile kurala genel bir bakış görürsünüz ve BOT kurallarında hangi sıraya ekleneceğini seçebilirsiniz.

**ÖNEMLİ HATIRLATMA:** Kuralların birinciden sonuncuya doğru uygulanarak işletildiğini unutmayın. Bu durumda bir işlem için öncelikli olan kurallarda yasaklama varsa, alt kurallardaki izin geçersiz olur.

## Add a new rule: ACCEPT

### Source

Default interfaces: Green

Addressformat: MAC Source Address (MAC or IP or network):

Default networks: Green Network

Custom addresses: Admin 1

Address Groups: Admins

Invert

### Destination

IPCop access

Other Network/Outside:

Default networks: Any

Custom addresses: Admin 1

Address Groups: Admins

Destination IP, or network:

Invert

Use Service:

Service Groups: IPCop services

Custom services: IPCop proxy

Default services: -Default services-

### Additional

Rule enabled

Log rule

Rule Action: ACCEPT

Remark: Lan PCs are allowed to use some IPCop services

This field may be blank.

### Add Timeframe

Add Timeframe

Days:

1 to 31

Days of the week:

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Daytime:

00 : 00 to 00 : 00

Back

Next

Save

Reset

Cancel

[Next] tuşuna tıklarsanız, aşağıdaki ekranı göreceksiniz:

### Add a new rule: Overview

**Source:**  
Interface: **Green**  
Address: **Green Network**

**Destination: IPCop access**  
Service: **IPCop services**

Rule Action: **ACCEPT**

Rule enabled:

Log rule:

Remark: **Lan PCs are allowed to use some IPCop services**

Rule Position:

### Current rules:

**IPCop access:**

#	Net Iface	Source	Log	Destination	Remark
		Logging Enabled (click to disable)	Logging Disabled (click to enable)	Standard Accept Rule	Logging Rule, only Log
		Enabled (click to disable)	Disabled (click to enable)	Edit	Advanced Accept Rule, open Firewall
		<input checked="" type="checkbox"/>	<input type="checkbox"/>		

**Legend:**

- Logging Enabled (click to disable)
- Enabled (click to disable)
- Down
- Logging Disabled (click to enable)
- Disabled (click to enable)
- Edit
- Copy rule
- Remove
- Up
- Down
- Standard Accept Rule
- Deny Rule
- Logging Rule, only Log
- Advanced Accept Rule, open Firewall

İsterseniz [Back] tuşu ile geri dönebilir ve özizlemenizdeki kuralda değişiklik yapabilirsiniz veya [Save] ile belirlediğiniz sıraya kuralı kaydedebilirsiniz. İlk kural için fark etmese de sonraki kurallar için sıralamanın önemli olacağını unutmayın.

Kural kaydedildikten sonra geçerli kuralların genel görünümü şu şekilde görünecektir:

**BlockOutTraffic:**

BlockOutTraffic is **Disabled** [Settings](#)

**Add a new rule:**

Rule Action: **ACCEPT** [New Rule](#)

**Current rules:**

**Other Network/Outside:**

#	Net Iface	Source	Log	Destination	Remark	Action
1		Green Network		IPCop : IPCop services	Lan PCs are allowed to use some IPCop services	

**Legend:**

- Logging Enabled (click to disable)
- Logging Disabled (click to enable)
- Standard Accept Rule
- Deny Rule
- Logging Rule, only Log
- Advanced Accept Rule, open Firewall
- Enabled (click to disable)
- Disabled (click to enable)
- Edit
- Copy rule
- Remove
- Up
- Down

Böylece IPCop servisleri iç ağdan (Green Network - Yeşil Ağ) erişilebilir durumdadır. Sonra internet servislerine erişim için gerekli kuralları tanımlayın.

[New Rule] butonuna tıklayarak yeni kural ekleme seçeneğini seçin ve aşağıdaki ayarları girin:

**Kaynak olarak:**

- Default interface (Geçerli Arabirim): Green (Yeşil)
- Default networks (Geçerli Ağlar): Green Network (Yeşil Ağ)

**Hedef olarak:**

- Other Network/Outside (Diğer Ağlar/Dışarı)
- Default networks (Geçerli Ağlar): Any (Herhangi biri) (bilgisayarlar tüm internet adreslerine erişebilir)
- Services seçeneğine tıklayarak seçili konuma getirin.
- Service Groups (Servis Grupları): Default services (Geçerli Servisler) (BOT yapılandırmasında tanımladığınız ikinci grup)

Kural çalışır (rule enabled) seçeneği seçilmeli, isterseniz 'Remark' kısmına açıklamalar yazabilirsiniz. Şimdi [Save] veya [Next]+[Save] tuşları ile ikinci BOT kuralınızı kaydedin.

İçerideki bilgisayarlarınız internet üzerinden Posta hizmetlerine erişebilirler. (Siz "Default services" grubuna daha fazla servis ekleyebilirsiniz) Bununla beraber IPCop tarafından verilen DNS, DHCP, NTP ve webproxy hizmetlerine de erişebilirler.

Sizin 'Current rules' (geçerli kurallar) listeniz şu şekilde görünmeli:



**BlockOutTraffic:**  
BlockOutTraffic is **Disabled**

**Add a new rule:**  
Rule Action:

**Current rules:**  
**Other Network/Outside:**

# Net Iface	Source	Log	Destination	Remark	Action
1	Green Network		Any : Default services	Lan PCs are allowed to use some internet services	<input checked="" type="checkbox"/>

  
**IPCop access:**

# Net Iface	Source	Log	Destination	Remark	Action
1	Green Network		IPCop : IPCop services	Lan PCs are allowed to use some IPCop services	<input checked="" type="checkbox"/>

  
**Legend:**

Logging Enabled (click to disable)	Logging Disabled (click to enable)	Standard Accept Rule	Deny Rule	Logging Rule, only Log	Advanced Accept Rule, open Firewall
<input checked="" type="checkbox"/> Enabled (click to disable)	<input type="checkbox"/> Disabled (click to enable)	Edit	Copy rule	Remove	Up
Down					

Artık siz BOT u çalışır hale getirmeye hazırsınız. Geçerli kurallarınız dışındaki tüm trafik engellenecektir.

You may want to allow some PCs to administrate the IPCop box via Webgui or SSH. See next chapter "Further advanced config".

Bazı bilgisayarlar Web arayüzü ve ssh erişimi ile IPCop yönetimi izni vermek isteyebilirsiniz. Bunun için "Daha Fazla Gelişmiş Yapılandırma" başlığını okuyunuz.

## Daha Fazla Gelişmiş Yapılandırma

İlk BOT kurallarını tanımladık ve artık bir adım daha ilerleyebiliriz. İç ağ üzerinde istediğimiz bilgisayarlara yönetim iznini BOT kuralı olarak tanımayacağız.

İlk olarak 'advanced BOT' seçimindeki 'Address settings' kısmından Admin PC olarak özelleştirilmiş adres tanımlaması yapılmalı:



**BlockOutTraffic:**

BlockOutTraffic is **Enabled** Address settings Show Firewall Config

**Add address:**

Name	Addressformat	Address	Netmask		
<input type="text"/>	IP	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>	<input type="button" value="Reset"/>

**Note:**  
A MAC address can not be used as destination address!

**Custom addresses:**

Name	Address	Netmask	Used	
Admin 1	00:50:56:C0:00:01		1x	
Admin 2	00:10:DC:F2:75:B1		1x	

**Default networks:**

Name	IP Address	Netmask
Any	0.0.0.0	0.0.0.0
Green Address	192.168.2.200	255.255.255.255
Green Network	192.168.2.0	255.255.255.0
Private Network 10.0.0.0	10.0.0.0	255.0.0.0
Private Network 172.16.0.0	172.16.0.0	255.240.0.0
Private Network 192.168.0.0	192.168.0.0	255.255.0.0
Red Address	192.168.0.200	
localhost	127.0.0.1	255.255.255.255
localnet	127.0.0.0	255.0.0.0

Ekran görüntüsünde MAC adresine göre tanımlanmış iki tane admin PC göreceksiniz. custom services (özelleştirilmiş servisler) de olduğu gibi bunları bir adres grubunda birleştirebiliriz.

Sonraki advanced BOT config bölümünde 'Address Grouping' başlığında 'Admins' adı verilen ve tanımladığımız bu iki adresi içeren bir grup yaratıyoruz:

**BlockOutTraffic:**

BlockOutTraffic is **Enabled** Address Grouping Show Firewall Config

**Add address to Group:**

Address Group name:  Remark:

Address Group name: Admins

Default networks: - Default networks -

Custom addresses: Admin 1

Enabled:

This field may be blank.

**Note:**  
A MAC address can not be used as destination address!

Add Reset

**Address Groups:**

**Admins - Group of admins - Used 0x :**

Admin 1	Custom	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Admin 2	Custom	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Artık bir admin kuralı yaratabilecek bilgileri girdik. BlockOutTraffic sayfasına dönün ve [New Rule] butonuna tıklayın.

Gerekli olan kural seçeneklerini girin, kaynak olarak:

- Default interface (Geçerli Arabirim): Green (Yeşil)
- Address Group (Adres Grubu): Admins

Hedef olarak:

- IPCop access (IPCop erişimi)
- Services seçeneğini seçin
- Service Group(Servis Grubu) seçeneğini seçin: IPCop admin (BOT yapılandırmasında tanımladığınız üçüncü grup)

Hepsi bu kadar. Tanımlamalarımız bitti. 'Current rules' (geçerli kurallar) başlığı altındaki görünüm aşağıdaki gibi olmalı:



## BlockOutTraffic 2.3 - Build 1

## BlockOutTraffic:

BlockOutTraffic is **Enabled**[Settings](#)

## Add a new rule:

Rule Action:  [New Rule](#)

## Current rules:

## Other Network/Outside:

#	Net Iface	Source	Log	Destination	Remark	Action
1		Green Network		Any : Default services		<input checked="" type="checkbox"/>

## IPCop access:

#	Net Iface	Source	Log	Destination	Remark	Action
1		Admins		IPCop : IPCop admin		<input checked="" type="checkbox"/>
2		Green Network		IPCop : IPCop services		<input checked="" type="checkbox"/>

**Legend:** Logging Enabled (click to disable) Logging Disabled (click to enable) Standard Rule Deny Rule Logging Rule, only Log Advanced Accept Rule, open Firewall  
 Enabled (click to disable)  Disabled (click to enable) Edit Copy rule Remove Up  
 Down



Connected (0d 1h 20m 37s)

14:14:53 up 1:20, 1 user, load average: 0.11, 0.06, 0.01



Bundan sonra kendinize özgü kurallarınızı ekleyerek istediğiniz yapılandırmaları yapabilirsiniz.

Translated 2007 by Çağlar ÜLKÜDERNER (caglar@ulkuderner.net)