در این مقاله آموزشی قصد داریم با نحوه مدیریت ترافیک شبکه با استفاده از میکروتیک در کنار فایروال Kerio Control آشنا شویم.

نظارت و مدیریت اینترنت سازمان ها باعث بالا رفتن بازدهی کاری کاربران و نیز ایجاد امنیت در شبکه مورد استفاده در آن اداره و یا سازمان می باشد. این نوع نظارت و مدیریت هم بصورت نرم افزاری می تواند باشد و هم بصورت سخت افزاری که اصطلاحا به آنها فایروال Firewall های سخت افزاری و نرم افزاری گفته می شود . نرم افزارها و سخت افزارهای فایروالی متنوعی جهت نظارت و مدیریت اینترنت سازمان وجود دارد که از آن جمله می توان به نرم افزارهای افزاری UTM گفته میشود. توان MikroTik را نام برد. به فایروالهای سخت افزاری UTM گفته میشود.

# قابلیتهای کلیدی نرم افزار: Kerio Control

اصلی ترین وظیفه یک دیواره آتش مستقر در محیط، نظارت بر ترافیک ورودی و خروجی شبکه بر مبنای سیاست امنیتی سازمان است کریو قادر است برای نظارت بر ترافیک اینترنت قواعد قابل درک و ساده ای را مبتنی بر رویه های امنیتی شبکه پیشنهاد دهد. دستیار نصب خودکار فراهم شده در نرم افزار میتواند خیلی به سرعت این کار را به انجام برساند.

## سيستم ضد نفوذ: (IPS)

سیستم ضد نفوذ Kerio Control می تواند بطور غیر محسوس تمامی ترافیک ورودی و خروجی شبکه را تحت نظارت قرار دهد و در کنار دیواره آتش سرویس دهنده های داخل شبکه را از هرگونه نفوذ و ارتباط غیر مجاز در امان دارد.

## محافظت در مقابل ويروسها:

داشتن ضدویروس در محیط شبکه، خطر انتشار سریع ویروس را کاهش میدهد Kerio Control به طور اختیاری یک پویشگر قوی، مختص ویروس را برا ی ترافیک ورودی و خروجی HTTP, FTP, SMTP, فراهم نموده است.

## نظارت بر محتوای: Web

Kerio Control بطور سر خود دارای ویژگی اعمال محدودیت بر روی محتوای صفحات وب است که بر مبنای کلید واژه، دسترسی به یک سایت را میتواند مسدود نماید در این نرم افزار محتوای صفحات وب، به چندین مقوله مختلف نظیر اخبار، بازی، خرید، ورزش، مسافرت و غیره تقسیم شده است و میتواند دسترسی کاربران مختلف، به مقوله های گوناگون را کنترل و یا مسدود نماید.

با توجه به ویژگی ها و قابلیت هایی که این سیستم برای مدیران شبکه فراهم می کند می توانیم از آن برای تکمیل قابلیت های بی شمار میکروتیک به عنوان یک روتر قدرتمند استفاده نماییم.

در این سناریو از یک سرور ویندوز به عنوان Active Directory برای مدیریت یکپارچه کاربران در شبکه استفاده می کنیم. نحوه راه اندازی سرویس های Active Directory بر روی ویندوز سرور در این مقاله قرار داده نمی شود و فرض را بر این میگذاریم که این سرویس از قبل راه اندازی شده است.

در ابتدا باید ویندوز سرور خود را به یک RADIUS Server برای احراز هویت کاربران تبدیل کنیم که این کار با استفاده از سرویس Network Policy Server ایجاد می شود.

 در این سناریو برای حفظ امنیت کاربران دسترسی کاربران شبکه به اینترنت فقط با اتصال VPN برقرار می شود.

ابتدا با استفاده از بخش Server Manager نقش Network Policy Server را نصب و راه اندازی می نماییم.

بعد از نصب وارد تنظیمات Network Policy Server می شویم و طبق عکس زیر مراحل راه اندازی RADIUS Server را پیگیری می نماییم.

錄 Network Policy Server	
File Action View Help	
🗇 🔿  🖬 🚺	
NPS (Local)     ADIUS Clients and Servers     Policies     Network Access Protection     Accounting     Templates Management	NPS (Local)           Getting Started           Image: Started in the start of the sta
	Standard Configuration         Select a configuration scenario from the list and then click the link below to open the scenario wizard.         RADIUS server for Dial-Up or VPN Connections         Network Access Protection (NAP)         RADIUS server for Dial-Up or VPN Connections         RADIUS server for Bial-Up or VPN Connections         RADIUS server for 800.1X Wireless or Wired Connections         allow NPS to authenticate and authorize connections from Dial-Up or VPN network access servers (also called RADIUS clients). @DorsaWr1
	Configure VPN or Dial-Up         Advanced Configuration         Templates Configuration

Configure VPN	or Dial-Up				X
	Select Dial-up Type	or Virtual P	rivate Ne	twork Co	nnections
Type of conr C Dial-up Con When you c	nections: nections Jeploy Dial-up servers on yo	urnetwork, NPS ca	n authenticate a	and authorize cor	nnection requests
<ul> <li>Virtual Priva</li> <li>When you of made by VP</li> </ul>	te Network (VPN) Connecti leploy VPN servers on your N clients connecting throug	ions network, NPS can gh the servers.	authenticate an	d authorize conn	ection requests
Name: This default text default text or m	t is used as part of the name nodify it @DorsaWrl	e for each of the pol	icies created wit	th this wizard. Yo	u can use the
Virtual Private	Network (VPN) Connection:	8			
		Previous	Next	Finish	Cancel

# در این بخش باید روتر میکروتیک را به عنوان یک RADIUS Client به ویندوز سرور معرفی کنیم:

rk Policy S Configure VPN or Dial-Up	×
tion View Cocal) ADIUS Client	
etwork Acces and Remote Access as a VPN servers as RADIUS clients click Add amplates Mar If you want to add remote V/PN servers as RADIUS clients, click Add	computer is running Routing ADIUS clients below.
New RADIOS Client       Settings       Select an existing template:       Image:       Name and Address       Friendly name:       Image:	Add Edit Remove
Address (IP or DNS):       1       192.168.5.1       Verify   Shared Secret Select an existing Shared Secrets template:	
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.	Finish Cancel
Manual     O Generate       Shared secret:     ••••••       Confirm shared secret:     2	
OK Cancel	

در این بخش آدرس IP میکروتیک و یک نام دلخواه در نظر می گیریم

# ۲. در این بخش باید یک رمز به عنوان Secret برای برقراری ارتباط بین RADIUS Server & در این بخش باید یک در هر دو سمت باید یکسان باشد.

## در این بخش متد های احراز هویت را فعال می کنیم

Configure VPN or Dial-Up	×
Configure Authentication Methods	
The following protocols are supported by servers running Microsoft Routing and Remote Access. If you use a different remote access server, make sure the protocols you select are supported by that software.	
Type (based on method of access and network configuration):         Microsoft: Smart Card or other certificate         Configure	
<ul> <li>Microsoft Encyrpted Authentication version 2 (MS-CHAPv2) Select this option to allow your users to specify a password for authentication.</li> <li>Microsoft Encyrpted Authentication (MS-CHAP) Select this option only if your network runs operating systems that do not support MS-CHAPv2.</li> </ul>	
Previous Next Finish Cancel	

در این مرحله باید گروهی از کاربران AD که این Policy روی آن ها اعمال می شود را انتخاب کنیم که در این سناریو ما Domain Users را انتخاب می کنیم.

C	Configure VPN or Dial-Up						
		Specify User Groups					
	Users that are members of the selected group or groups will be allowed or denied access based on the network policy Access Permission setting.						
	To select User Groups, click Add. If no groups are selected, this policy applies to all users.						
	Groups Add						
	RAHMANI\Do	omain Users	Remove	i			
				1			

مابقی موارد را بدون نیاز به تغییر تا انتهای پروسه راه اندازی Next می زنیم و در نهایت Finish می کنیم. در حال حاضر ویندوز سرور Active Directory ما به عنوان یک RADIUS Server فعال می باشد. در ادامه به انجام تنظیمات میکروتیک می پردازیم.

• راه اندازی سرور VPN میکروتیک:

برای اجرای این سناریو به ترتیب موارد زیر را اجرا می کنیم: ایجاد یک Pool آدرس IP مختص کاربران اینترنت

/ip pool

add name=VPN ranges=192.168.70.0/24

سپس برای فعال سازی سرویس VPN Server روی روتر باید یک Profile برای مشخصات و تنظیمات سرور خود در میکروتیک ایجاد کنیم:

/ppp profile

add dns-server=8.8.8.8,4.2.2.4 idle-timeout=59m local-address=10.50.50.1 \

name="Local VPN" remote-address=VPN

سپس سرویس VPN سرور را فعال می کنیم:

/interface pptp-server server

set authentication=pap,chap,mschap1,mschap2 default-profile="Local VPN" \

max-mru=1460 max-mtu=1460

در این سناریو من از سرویس PPTP استفاده می کنم.

در ادامه مشخصات Active Directory را به عنوان Radius به میکروتیک معرفی می کنیم.

برای تعریف Active Directory به عنوان RADIUS Server در میکروتیک به قسمت Radius رفته و به شکل زیر تنظیمات و مشخصات Active Directory را وارد می کنیم:

General       Status       OK         Service:       ✓ ppp       login       Cancel         hotspot       wireless       Apply         dhcp       ipsec       Disable         Called ID:       ✓       Disable         Domain:       ✓       Comment         Address:       192.168.5.10       Copy         Secret:       Copy       Remove         Authentication Port:       1812       Reset Status         Accounting Port:       1813       ms	Radius Server <192	.168.5.10>	
Service: ✓ ppp login   hotspot wireless   dhcp ipsec     Called ID: ✓   Domain: ✓   Domain: ✓   Address: 192.168.5.10   Secret: Copy   Remove Remove   Reset Status     Authentication Port: 1812   Accounting Port: 1813   Timeout: 300   Mathematical point: Mathematical point:	General Status		ОК
hotspot wireless   dhcp ipsec     Called ID: ✓   Domain: ✓   Domain: ✓   Address: 192.168.5.10   Secret: Copy   Remove Remove   Reset Status     Authentication Port: 1812   Accounting Port: 1813   Timeout: 300   Mathematical point 1813	Service	e: 🔽 ppp 📃 login	Cancel
Called ID: Disable Comment Domain: Comment Address: 192.168.5.10 Copy Secret: ****** Authentication Port: 1812 Accounting Port: 1813 Timeout: 300 ms Accounting Backup		hotspot wireless	Apply
Domain: Comment   Address: 192.168.5.10   Secret: Copy   Remove Remove   Authentication Port: 1812   Accounting Port: 1813   Timeout: 300   Maccounting Backup	Called ID	·	Disable
Address:       192.168.5.10       Copy         Secret:       Remove         Authentication Port:       1812         Accounting Port:       1813         Timeout:       300       ms         Accounting Backup       Accounting Backup	Domain	н <b>— — — —</b>	Comment
Secret:     Remove       Authentication Port:     1812       Accounting Port:     1813       Timeout:     300       Maccounting Backup	Address	: 192.168.5.10	Сору
Authentication Port: 1812 Accounting Port: 1813 Timeout: 300 ms Accounting Backup	Secret		Remove
Accounting Port: 1813 Timeout: 300 ms Accounting Backup	Authentication Port	:: 1812	Reset Status
Timeout: 300 ms	Accounting Port	:: 1813	
Accounting Backup	Timeout	:: 300 ms	
		Accounting Backup	

سپس در قسمت PPP بخش Secrets احراز هویت از طریق Radius را فعال می کنیم:

PPP					
Interface	PPPoE Servers	Secrets Profi	les Active	Connections L	2TP Secrets
+ -		PPP /	Authenticati	on&Accounting	
Name	∠ Password	Service C	aller ID	Profile	Local Address
	PPP Auth	entication&Acc	counting e Radius		OK
			e Circuit ID i	n NAS Port ID	Cancel Apply
	Interim U	lpdate:		▼	

تا این مرحله امکان اتصال کاربران Active Directory به میکروتیک که بصورت VPN Server راه اندازی شده است فراهم شده است.

• نکته قابل توجه این است که در Active Directory کاربری که ایجاد می کنیم دسترسی VPN را داشته باشد:

Active Directory Users and Com	puters		Behdad Rahman	i Properties		1-1-1-1	? ×
File Action View Help							
		🏡 🖗 🤝 👼	Remote Deskto	op Services Profile	Personal Virtu	ual Desktop	COM+
		<u>~ i v 4</u>	General Addres	ss Account Profile	Telephones	Organization	Member Of
Active Directory Users and Comput Saved Queries Rahmani.com Computers Computers Computers ForeignSecurityPrincipals Managed Service Accounts Users	Name Allowed RODC Passw Cert Publishers Denied RODC Passwo DnsAdmins RAS and IAS Servers DnsUpdateProxy Domain Admins Domain Computers Domain Computers Domain Controllers Domain Guests Domain Guests Domain Users Read-only Domain Co Read-only Domain Co Enterprise Read-only Schema Admins Administrator Behdad Rahmani Coust	Type A Security Group . Security Group .	Dial-in Network Acce Allow acce Deny acce Control acc Verify Calle Callback Optic No Callback Set by Call Always Ca Always Ca Define IP add Dial-in connee Define routes connection.	Environment Environment Ess Permission Ess Ess Ess Eccess through NPS Net er-ID: Dons Er-ID: Dons Ek ler (Routing and Remo Ilback to: tic IP Addresses tic IP Addresses tic IP Addresses Esses to enable for this Dial	in	ce only)	
	J			ОК	Cancel	Apply	Help

در ادامه به اتصال Kerio Control به AD می پردازیم.

روش نصب و راه اندازی Kerio Control در این مقاله مورد بررسی قرار نمی گیرد و فرض بر این است که راه اندازی و نصب اولیه از قبل انجام شده است.

برای این سرور می توان ۲ کارت شبکه در نظر گرفت که یکی به اینترنت و دیگری به شبکه داخلی متصل گردد. محمد Interfaces

	📉 Dashboard	Incentaces							
$\Diamond$	Interfaces	- Internet connectivity	Internet connectivity						
	🖡 Traffic Rules	Select an option of how the f	Select an option of how the firewall is connected to the Internet:						
*	Intrusion Prevention	A Single Internet Link	A Single Internet Link						
	🕐 Security Settings								
Ш	Bandwidth Management and QoS	Name 🔺	Status	IPv4	IPv6	_			
E	Y Content Filter	🖃 📥 Internet Interfaces		100 100 0 010	TO C PULL	<u> </u>			
-	Proxy Server	Trusted/Local Inter	Up	192.168.3.216	IPv6 disabled				
	🖉 Antivirus	Ethernet	Up	192.168.5.2	IPv6 disabled				
	PHCP Server	IPsec and Kerio VPN	l Interfaces			I			

بصورت پیش فرض Kerio Control بصورت Nat دسترسی کاربران به اینترنت را فراهم می کند و نیاز به اعمال تغییرات خاصی نیست.

در ابتدا باید Kerio Control را هم به Active Directory متصل کنیم که برای احرازهویت کاربران از آن استفاده نماید. برای این کار از بخش Domains and Users تب Directory Services مشخصات اتصال به سرور Active Directory را طبق تصویر زیر وارد می کنیم:

ــــــــــــــــــــــــــــــــــــــ	ی در قبلی مصویر ریز ورو کمی د						
DHCP Server	🛛 🛃 Domains and User Log	in					
😢 IPv6 Router Advertisements	Authentication Options Security Options	Directory Services Guest Interfaces					
🕂 DNS	Member of domain rahmani.com.						
💺 Routing Table	Map user accounts and groups from a dire	ctory service					
Accounting and Monitoring	Domain						
🙈 Remote Services	Directory service type:	Microsoft® Active Directory®					
🚁 Advanced Options	Domain name: rahmani.com						
Users and Groups	- Account with read access to the direct	ctory service					
🧟 Users	Username:	administrator@rahmani.com					
🙀 Groups	Password:	*****					
졅 Domains and User Login							
Definitions	Connection						
SSL Certificates	Automatically connect to the first directory server available						
📑 IP Address Groups	Primary server: 192.168.5.2						
🗐 URL Groups	Secondary server:						

در صورتی که اتصال با موفقیت برقرار شود در قسمت Users می توانید لیست کاربران Active Directory را مشاهده نمایید:

$\mathbf{\overline{\mathbf{A}}}$	Users
----------------------------------	-------

Domain: rahmani.com	Hide disabled user accou	nts	Filter:
Username 🔺	Full Name	Description	Groups
administrator	Administrator	Built-in account for administering	Domain Users, Group Policy Creator Owners, Domain Admin
🚨 behdad	Behdad Rahmani		Domain Users
a Guest	Guest	Built-in account for guest access	Domain Guests, Guests
🧟 krbtgt	krbtgt	Key Distribution Center Service A	Domain Users, Denied RODC Password Replication Group

هم اکنون هم تنظیمات اتصال میکروتیک و هم تنظیمات اتصال Kerio Control به سرور Active Directore به سرور Directory به عنوان مرجع احراز هویت کاربران برقرار شده است.

برای این که Kerio Control دسترسی کاربران به اینترنت را با احراز هویت انجام دهد در قسمت Domains and Users قسمت Authentication Options بخش Web Authentication موارد را طبق تصویر زیر فعال می کنیم:

🛜 Domains and User Login						
	Authentication Options Security Options Directory Services Guest Interfaces					
	Web authentication					
	Always require users to be authenticated when accessing web pages					
	Force non-transparent proxy server authentication					
	Each browser session will require user authentication. This is useful in Citrix or Terminal Service environments,					
	Apply only to these IP addresses:					
	Enable automatic authentication using NTLM					
	Automatic logout          Image: Automatically logout users if they are inactive         Timeout:       120         minute(s)					

با فعال کردن این گزینه ها در زمان اتصال کاربر به اینترنت صفحه لاگین Kerio Control نمایش داده می شود و از کاربر درخواست شناسه کاربری و رمز عبور می کند ( همانند هات اسپات میکروتیک ) در صورتی که

کاربر Join به Domain شده باشد با فعال کردن گزینه Join منه است الما می است الما می شود و نیازی به سیستم خود لاگین کرده است احراز هویت انجام می شود و نیازی به وارد کردن دستی اطلاعات کاربری نمی باشد.

ارسال ترافیک کاربران میکروتیک به کریو:

این بخش اصلی مقاله می باشد که با تنظیمات زیر ترافیک کاربران شبکه که با VPN متصل شده اند را به سمت Kerio Control هدایت می کنیم تا بعد از احراز هویت امکان دسترسی به اینترنت را داشته باشند و تمام فعالیت های اینترنتی کاربران تحت نظارت Kerio Control انجام شود.

Mark برای این منظور از ابزار VPN در میکروتیک استفاده می کنیم تا ترافیک کاربران VPN را با ابزار Routing علامت گذاری کرده و به سمت Kerio Control ارسال نماییم. همانطور که در بالا توضیح داده شد کاربر با شناسه و رمز دامنه خود لاگین می کند و وقتی در کریو گزینه Table automatic فعال باشد بدون نیاز به وارد کردن اطلاعات کاربری دسترسی به اینترنت فراهم می شود ولی اگر این گزینه فعال نباشد یک صفحه لاگین به کاربر نمایش داده می شود.

© admin@192.168.5.1 (Behdad) - WinBox v6.41.4 on x86 (x86)						
Session Settings Dashb	Session Settings Dashboard					
Safe Mode	Session: 192.168.5.1		<b>—</b> 🙃			
🔏 Quick Set	Mangle Rule <>	New Mangle Rule				
I CAPSMAN	General Advanced Extra Action Statistics	General Advanced Extra Action Statistics	ОК			
Interfaces	Chain: prerouting	Action: mark routing	Cancel			
2 Wireless	Src. Address: VPN IP Range		Apply			
Bridge	Dst. Address:					
E PPP		Log Heix.	Disable			
°t% Mesh	Protocol:	New Routing Mark: to_Kerio 🗧	Comment			
	Src. Port:	Passthrough	Сору			
Reuting	Dst. Port:		Remove			
Svstem	Any. Port:		Reset Counters			
Queues	In. Interface: I ether2-to-Lan		Reset All Counters			
Files	Out, Interface:					
E Log						
🧟 Radius	In. Interface List:					
ŏ <mark>⊁ Tools ▷</mark>	Out. Interface List:					

: Mangle تنظيمات

توجه داشته باشید در قسمت In . Interface ترافیک ورودی کارت شبکه Lan را در میکروتیک از این رول مستثنی می کنیم که ترافیک ورودی به روتر مجدد در این flow قرار نگیرد.

سپس از قسمت Route یک static route برای این mark routing به IP سرور Route منتقل کردیم. در صورت ایجاد می کنیم. در رول بالا ما تمام ترافیک کاربران را به سمت Kerio Control منتقل کردیم. در صورت نیاز می توانید ترافیک به مقاصد خاص را bypass کنید یا فقط برای پورت های 80,443 پروتکل TCP این رول را ایجاد نمایید.

Route List						
Routes	Nexthops Rules	VRF				
				Find		
	Det Address A	Gateway	Distance	Routing Mark	P	
AS	0.0.0/0	192.168.5.3 reachable ether2-to-Lan	1	to_Kerio		
AS DAS	0.0.0.0/0 0.0.0.0/0	192.168.5.3 reachable ether2to-Lan 192.168.13.1 reachable ether3to-Wan	1	to_Kerio		
AS DAS DAC	<ul> <li>0.0.0.0/0</li> <li>0.0.0.0/0</li> <li>192.168.5.0/24</li> </ul>	192.168.5.3 reachable ether2to-Lan 192.168.13.1 reachable ether3to-Wan ether2to-Lan reachable	1 1 0	to_Kerio	1	

بعد از ایجاد رول در قسمت route ترافیک کاربران به Kerio منتقل می شود و با توجه به اتصال کاربر با VPN می توانیم سرعت تبادل اطلاعات کاربر را در میکروتیک محدود کرده و مابقی موارد ( حجم مصرفی روزانه و هفتگی و ماهانه و... ) را به کریو منتقل کنیم.

بعد از اتصال کاربر با VPN به Mikrotik در قسمت Queue همانطور که مشاهده می کنید یک Simple بعد از اتصال کاربر با UPN به Limit در Queue ایجاد می شود:

Queue List									
Simple Queues	Interface Queues	Queue Tree	Queue Typ	es					
+ - 🖉	× 🖻 🍸	00 Reset C	ounters	o Reset	All Counters				Find
# Name	Tan	get	Upload Max	Limit	Download Max	k Limit	Packet	Marks	Total Ma 🔻
0 D 🚊 ⊲pp	tp-behdad> <pp< th=""><th>tp-behdad&gt;</th><td>1M</td><th></th><th>1M</th><td></td><td></td><td></td><td></td></pp<>	tp-behdad>	1M		1M				

در سمت کاربران فقط نیاز به ساخت یک اتصال VPN می باشد که من در این سناریو با توجه به اینکه روی میکروتیک PPTP Server را ه اندازی کردم همین اتصال را برای کاربر ایجاد می کنم.

VPN Connection Properties					
General Options Security Networking Sharing					
Type of VPN:					
Point to Point Tunneling Protocol (PPTP)					
Data encryption:					
Optional encryption (connect even if no encryption)					
Authentication C Use Extensible Authentication Protocol (EAP)					
Properties					
Allow these protocols					
Unencrypted password (PAP)					
Challenge Handshake Authentication Protocol (CHAP)					
Microsoft CHAP Version 2 (MS-CHAP v2)					
Automatically use my Windows logon name and password (and domain, if any)					
OK Cancel					

در صورتی که سیستم کاربر ما join به دامین شده باشد و کاربر با شناسه و رمز دامین خود لاگین کرده باشد با فعال کردن گزینه Automatically use my Windows logon name and password در زمان اتصال کاربر نیازی به وارد کردن شناسه و رمز دامنه نمی باشد و کانکشن کاربر بصورت خودکار متصل می شود.

در این زمان تمام فعالیت کاربر توسط Kerio مدیریت می شود و می توانید سایت های خاصی را فیلتر کنید یا دانلود فایل های خاصی را محدود نمایید و ...

! Alert	🖻 Web
Config	
Connection	کچا و به صرفه بخر، استایل باکس، ست برند های معتبر پوشاک" 16/Apr/2018 16:21:21 [192.168.5.1 behdad@rahmani.com] [16/Apr/2018 16:21:21 192 168 5.1 behdad@rahmani.com][16/Apr/2018 16:21:21 192 168 5.1 behdad@rahmani.com]]
Debug	المورسية العراق براي تركين مرجع ليشريك المورسي المعالي المعالي المعالي المعالي المعالي المعالي المعالي المعالي [16/Apr/2018 16:21:21] 192:168.5.1 behdad@rahmani.com المدالي المدالي المعالي المعالي المعالي المعالي المعالي ا [16/Apr/2018 16:21:21] 192:168.5.1 behdad@rahmani.com المعالي المعالي المعالي المعالي المعالي المعالي المعالي ا
📞 Dial	المرابق المرابق [16/Apr/2018 16:21:21] 192.168.5.1 behdad@rahmani.com أومد المرابق المرابق المرابق المرابق المرابق المرابق المرا المرابق المرابق
Error	<u>الماري://beta.ka</u> المورشان طراحان و برنامه نويسان و الماري من <u>الماري الماري الماري</u>
Filter	http://bei/ اموزش های ویدتویی منابع کنکور کارشناسی ارشد" [16/Apr/2018 16:21:22] 192.168.5.1 behdad@rahmani.com ا [16/Apr/2018 16:21:23] افیلمهای آموزشی طراحی و برنامه نویسی وب" http://beta.k البله: البله: ا
💻 Host	ببود عملكرد حافظه رم و - Chris-PC RAM Booster v4.60 دانلود" Chris-PC RAM Booster v4.60 [16/Apr/2018 16:21:24] [16/Apr/2018 16:21:24] 192.168.5.1 behdad@rahmani.com "صدها ساعت فيلم آموزشنى رايگان در فرادرس" <u>http://beta.ka</u>
🚯 Http	h <u>ttp://beta.kapi "</u> فرادرس: بزرگترین مرجع فیلمهای اموزشی" [16/Apr/2018 16:21:24] [192.168.5.1 behdad@rahmani.com [16/Apr/2018 16:21:24] 192.168.5.1 behdad@rahmani.com "فیلمهای آموزشی" (16/Apr/2018 16:21:24] [192.168.5.1 behdad
O Security	موعه فیلرهای آموزشنی دروس کنکور مشترک رشته های فنی" [16/Apr/2018 16:21:24] 192.168.5.1 behdad@rahmani.com موعه فیلرهای آموزشنی دروس کنکور مشترک رشته های فنی" (16/Apr/2018 16:21:24] 192.168.5.1 behdad@rahmani.com در دیویی استایل Gucci 16/Apr/2018 16:21:24]
🛕 Warning	http://beta.ka "صدها ساعت فیلم آموزشی رایگان در فرادرس" http://beta.ka "صدها ساعت فیلم آموزشی رایگان در فرادرس" http://beta.ka "موزش های ویدئویی منابع کنکور کارشناسی ارشد" http://beta.ka [16/Apr/2018 16:21:25] 192.168.5.1 behdad@rahmani.com "آموزش های ویدئویی منابع کنکور کارشناسی ارشد" http://beta.ka
web 🔛	h <u>ttp://beta.ka</u> "صدها ساعت فیلم أموزشـی رایگان در فرادرس" http://beta.ka [16/Apr/2018 16:21:25] 192.168.5.1 behdad@rahmani.com "صدها ساعت فیلم أموزشـی (http://beta.kap "http://beta.kap "http://beta.kap "فرادرس: بزرگترین مرجع فیلمهای آموزشـی" http://beta.kap
	[16/Apr/2018 16:21:26] 192.168.5.1 behdad@rahmani.com "مجموعه فيلمهاى آموزشى برنامه نويسى اندرويد" (http://bet [16/Apr/2018 16:21:26] 192.168.5.1 behdad@rahmani.com "را در ديجى استايل ببينيد Skechers جديدترين مدلهاى" (http:// ما جلم الله الله المالي الم
	http://beta.ka صدها ساعت فیلم اموزشی رایگان در فرادرس "http://beta.ka صدها ساعت فیلم اموزشی رایگان در فرادرس "http://beta.ka [16/Apr/2018 16:21:27] 192.168.5.1 behdad@rahmani.com آموزش های ویدئویی منابع کنکور کارشناسی ارشد" http://beta
	[16/Apr/2018 16:22:36] 192.168.5.1 behdad@rahmani.com "faradars.org" <u>http://beta.kaprila.com/a/go.php?url=https/</u> [16/Apr/2018 16:22:38] 192.168.5.1 behdad@rahmani.com "iaqua solitic ingerity" (http://faradars.org/how-to- التركيم المراجع
	[1//Apr/2018 09:03:59] 192.168.5 L bendad@ranmani.com "تدبير انديشان درسا" <u>http://dorsaco.net/</u>

با سپاس بهداد رحمانی