بسم الله الرحمن الرحیم

آموزش کاربردی

Kerio Control

تهیه و تنظیم : وحید معصومی اصل

تیرماه ۹۳

مقدمه :

امروزه اینترنت یکی از پر کاربردترین سرویس ها در سازمانها ، اداره جات ، شرکتها و ... می باشد، در این حالت باید یک نظارت و مدیریت کلی ای نسبت به این موضوع داشته باشیم بدین صورت که آیا کارمندان و کاربران اینترنت در این سازمانها استفاده بهینه در جهت وظیفه محولشان انجام می دهند یا استفاده از نوع تفریحی از این سرویس می کنند و وظیفه محولشان را فراموش می کنند.

نظارت و مدیریت اینترنت سازمانها و اداره جات باعث بالا رفتن راندمان 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 اصطلاحاً به آنها firewall های سخت افزاری و نرم افزاری گفته می شود.

نرم افزارها و سخت افزارهای فایروالی متنوعی جهت نظارت و مدیریت اینترنت سازمانها واداره جات وجود دارد که از آن جمله می توان به نرم افزارهای ISA Server و Kerio Control اشاره کرد و از سخت افزارها نیز می توان Cisco ASA را نام برد. به فایروالهای سخت افزاری UTM گفته میشود.

در این مقاله قصد داریم که یک آموزش کاربردی ای نسبت به فایروال نرم افزاری Kerio Control داشته باشیم امید هست که مورد قبول دوستان قرار گیرد.

وحید معصومی اصل-

Vahidmasume64@gmail.com

Kerio Control **چیست؟**

Network Security for Your Business

Kerio Control is an award-winning UTM firewall designed to protect businesses from a comprehensive range of invasive and crippling corporate network threats. Kerio Control's auto-updating security layer detects and prevents emerging threats automatically while providing network administrators with flexible user policy tools, complete bandwidth management and QoS control, detailed network monitoring, and IPsec VPN connectivity for desktops, mobile devices and multiple sites. Kerio Control provides superior network protection and intelligence that is stable, secure, and above all, simple to manage.

ترجمه متن بالا: Kerio Control با دارا بودن بهترین طراحی شبکه، سازمان یا شرکت و یا اداره شما را از هجوم تهدیدات فلج کننده حفاظت می کند. Kerio Control بصورت اتوماتیک لایه های امنیتی را می یابد و مانع از این می شود که تهدیدات شبکه اعمال شوندتا زمانی که مدیر شبکه انعطاف پذیری های مورد نظرش را نسبت به کاربران اعمال کند با استفاده از Ploicy Tools ها، کنترل مدیریت پهنای باند، مونیتورینگ دقیق شبکه و اتصالات IPSec VPN برای دسکتاپ ها، دستگاههای موبایل و سایتهای مختلف. Kerio Control یک امنیت شبکه قوی وهوش پایدار با امنیت بهتر و بالاتر از همه یک مدیریت ساده فرآهم می کند.

نرم افزار Kerio Controlیک راه حل کامل برا ی تامین امنیت و مدیریت دسترسی به اینترنت برای تمامی شبکه ها به هر اندازه است. برای سازمانهای بزرگ طراحی شده است، در مقابل حملات بیرونی و ویروسها یک دفاع مستحکم و کم نظیر دارد، میتواند دسترسی به محتوای مطالب سایتهای اینترنتی را محدود و یا مانع شود. برقراری ارتباط VPNرا با هر نقطه فراهم میکند .

قابلیتهای و ویژگی های نرم افزار Kerio Control

مدیریت کاربر

- قابلیت یکپارچه شدن با Active Directory.
- اعتبار سنجی کاربران برای دسترسی به شبکه
- توانایی سریع به اشتراک گذاشتن اینترنت در شبکه از طریق Proxy و NAT.
- افزایش کارایی اینترنت با استفاده از Web Caching.

- قابلیت اختصاص IP به طور خودکار(DHCP) .
- تسریع کننده درخواست ارسالی DNS .
- پشتیبانی از منطقه DMZ .
- امکان تعریف قواعد دسترسی به شبکه و اینترنت برای هر کاربر
- نظارت بر فعالیت کاربران در وب

امنیت یکپارچه

- دارای Firewall جهت کنترل دسترسی ، جلو گیری از نفوذ و خرابکاری در شبکه.
- دارای سیستم شناسایی و ممانعت از نفوذ (IPS)
- قابلیت استفاده از انواع ضدویروسهای قدرتمند برای ترافیک HTTP, FTP, SMTP , POP3
- ساز و کار سر خود برای پالایش محتوای صفحات وب
- استفاده اختیاری از پالاینده های پیشرفته.
- توانایی جلوگیری از ورود آگهی های تبلیغاتی اینترنتی .
- بازرسی و کنترل کلیه پرتکلهای غیر استاندارد.

شبکه های خصوصی مجازی (VPN)

- پشتیبانی از VPNجهت برقراری ارتباط رمزگذاری شده.
- قابلیت برقراری ارتباط سایت به سایت ، کاربر به سایت.
- مدیریت پهنای باند
- قابلیت سهمیه بندی پهنای باند برای برنامه های مختلف.
- پشتیبانی از انواع ارتباطات اینترنتی (ماهواره ، DSL، ISDN، شماره گیری از طریق مودم و غیره).
- پشتیبانی از UPnP، فناوری ارتباط نرم افزارها بدون پیکره بندی خاص . (مانند MSN Messanger)
- پشتیبانی از VoIPپروتکل ارسال صوت از طریق اینترنت.

- ثبت وقایع مربوط به ترافیک اینترنت .
- نمایش فعالیتها بصورت گراف.
- مدیریت از راه دور با برخورداری از امنیت کامل.

امنیت در اینترنت

- *Firewall برای شبکه*

اصلی ترین وظیفه یک Firewall مستقر در محیط، نظارت بر ترافیک ورودی و خروجی شبکه بر مبنای سیاست امنیتی سازمان است. Kerio Control 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.

سیستم 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 Firewall سرویس دهنده های داخل شبکه را از هرگونه نفوذ و ارتباط غیر مجاز در امان دارد.

محافظت در برابر ویروسها

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, POP3 فراهم نموده است.

پشتیبانی از VPN

هنگامیکه لازم است بین دو شبکه و یا سرویس دهنده و ایستگاههای کاری، شبکه خصوصی مجازی برقرار گردد، Kerio Control اجازه میدهد با استفاده از پرتکلهای IPSec NAT و PPTP VPN این ارتباط ایمن به سادگی برقرار گردد.

پشتیبانی از VoIP

برقراری ارتباط تلفنی از میان شبکه ای که تحت محافظت Firewall قرار داشته باشد کار مشکلی است زیرا اساسا پرتکلهای VoIP مانند H.323 جهت گذر آسان از میان دیواره آتش طراحی نشده اند Kerio Control اجازه میدهد، VoIPدر کنار آن به اجرا در آید تا از رها ساختن عمومی زیر ساختهای VoIPدر اینترنت بدون امنیت لازم بی نیاز شوید.

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 و بطور افزودنی Kerio Control با نرم افزار پالایشی Cobion Orang Filter تجهیز شده است. در این نرم افزار محتوای صفحات وب، به 58 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.

Kerio Control دارای ورژنهای متفاوتی می باشد که در این مقاله سعی کرده ایم آموزش Kerio Control 8.3.1 Build 2108 را خدمتتان ارائه بدهیم.

Kerio Control 8.3.1 Build 2108یک دیوار آتشین (firewall) که به منظور استفاده سازمانهایی با اندازه کوچک و متوسط طراحی شده است و از طرف انجمن بین المللی امنیت کامپیوتری International Computer Security Association تضمین شده است. این نرم افزار به یک نظام امنیتی یکنواخت, قابلیت سانسور و فیلتر مضامین اینترنتی بر روی سیستمهای تجارتی بین المللی International Business Machine (IBM) امکان نظارت بر کارکرد کارمندان, تنظیمات کنترلی پهنای باند و سرورهای VPN مجهز میباشد و این دیوار آتشین یک دسترسی وسیع برای کاربران اینترنتی پدید آورده و به همراه تنظیمات و ابزار امنیتی, کنترل آنها را توسط کارفرما ممکن و آسان میسازد. نسخه 7.1 این برنامه تنظیمات بارگذاری لینک و ۱۱ زبان زنده دنیا را پشتیبانی میکند.

ویژگی های Kerio Control 8.3.1 **از وب سایت رسمی خود شرکت به شرح زیر هست:**

+ Added Reverse Pr0xy feature
+ Traffic rules: added search text, test rules and hide/collapse rule features
+ MAC address can now be used for automatic user login
+ Added support for FTP in automatic configuration backup
+ New log Host introduced
+ Added possibility to create service groups
+ Manually assigned IP addresses within DHCP scope can now be blocked
* Traffic rules: added last used column, added more colors
* Traffic rules are now added by wizard
* Active hosts now shows MAC address
* MAC Filter now can automatically permit MAC addresses used in DHCP reservations and automatic user login
* Bandwidth management rules can be now applied to V*P-N tunnel traffic before encryption
* Dynamic DNS client now can detect public IP address
* Automatic login now doesn’t work for users disabled in directory service
* DHCP reservation and automatic user login can be created from context menu on Active Hosts screen
* Linux kernel upgraded to version 3.12
- Fixed: DNS forwarder now forwards DKIM queries
- Fixed: OpenSSL vulnerability CVE-2014-0160

شروع کار:

برای پیاده سازی یک Kerio Server علاوه بر اینکه یک سرور را بعنوان Kerio در نظر می گیریم دو سرور دیگر بعنوان Certificate Authority (CA) و Primary Domain Controller (PDC) در نظر می گیریم، این سرورها الزاماً لازم نیست که در داخل شبکه مان باشند، ولی برای اینکه یک شبکه Stable داشته باشیم بهتر هست که در سناریومان این دو سرور را داشته باشیم. در داخل سرور PDC همانا Damin Controller (DC) راه اندازی می کنیم.

نحوه راه اندازی سرورهای CA و PDC چونکه خارج از موضوع مقاله می باشد به همین دلیل سناریوی مورد بحث را با این فرض پیش می بریم که این دو سرور راه اندازی شده اند، ان شاالله در سری مقالات بعدی آموزش این دو موضوع را نیز ارائه خواهیم داد. با توجه به این توضیحات سرور CA را بعد از راه اندازی Join to Domain می کنیم و بعد Certificate های مربوطه را ایجاد و به سرورهای CA و PDC ارائه می دهیم.

مشخصات سرورهای مورد استفاده در این سناریو :

Server Name: PDC

IP Address: 192.168.100.2

Domain Name: Cyber.local

OS: Win Server 2012

Computer Name: PDC

User Name: Administartor

Defult Getway: 192.168.100.1

Server Name: CA

IP Address: 192.168.100.3

Computer Name: CA

DNS Server: 192.168.100.2

User Name: Administartor

Log on Domain: Cyber.local

Defult Getway: 192.168.100.1

Server Name: Kerio Control

Public Interface:192.168.1.101

Private Interface: 192.168.100.1

و دو سیستم بعنوان Client در نظر می گیریم، یعنی Client 1 و Client 2 با مشخصات زیر:

Computer Name: Client1

IP Address:192.168.100.11

Computer Name: Client 2

IP Address: 192.168.100.12

Kerio Control 8.3.1 Build 2108 به دلیل اینکه هسته اصلی اش Linux Base هست به همین دلیل اصولاً درست نیست که بر روی ویندوز نصب شود.

توضیح نصب Kerio Control 8.3.1 Build 2108 *بدین شرح می باشد:*

زمانی که شما یک کامپیوتر تازه خریداری می کنید، فقط از لحاظ سخت افزاری تامین شده است و یک کامپیوتر خام می باشد، در این حالت در اولین مرحله شروع به نصب ویندوز و پارتیشن بندی می کنید. در حالت کلی نصب Kerio Control 8.3.1 Build 2108 نیز بدین صورت می باشد یعنی نرم افزار Kerio Control 8.3.1 Build 2108 را در یک سرور خام که دارای چیز دیگری نمی باشد نصب می کنیم، یعنی شبیه نصب یک ویندوز در یک کامپیوتر خام.

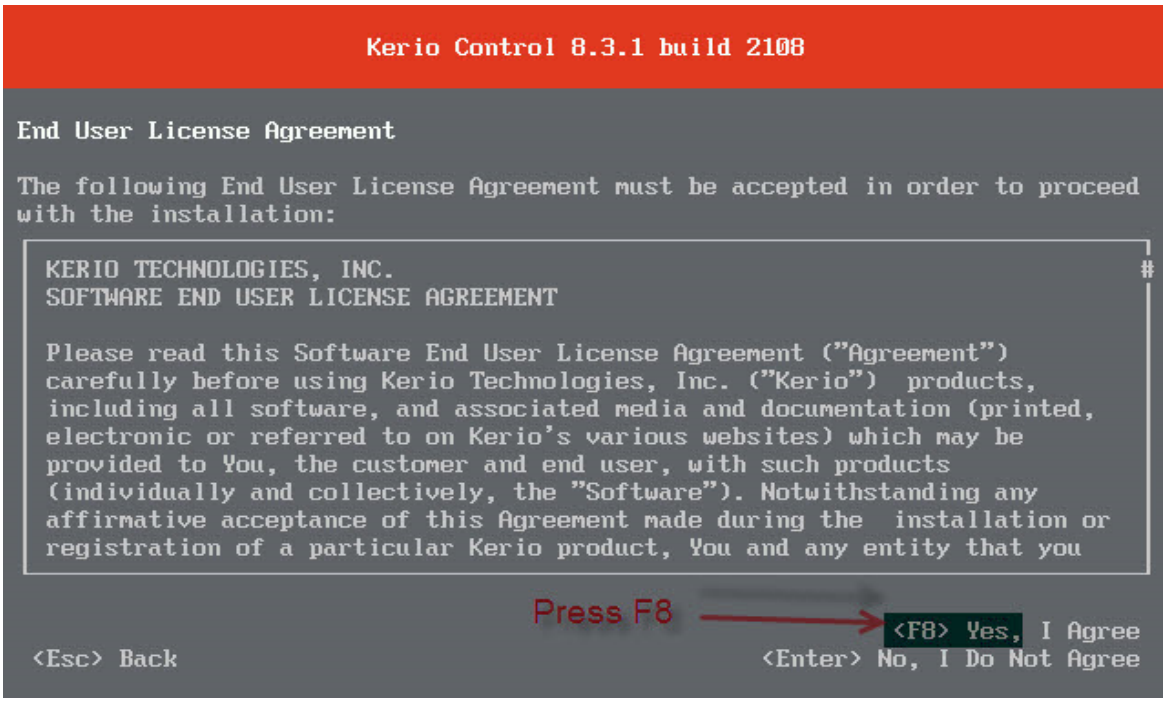
البته قابل ذکر هست دستگاهی که بعنوان Kerio Control در نظرگرفته شده باید دارای دو Network Interface باشد یعنی Public Interface و Private Interface که از Public Interface برای ارتباط با اینترنت استفاده می شود و از Private Interface برای ارتباط با شبکه داخلی یا همان LAN استفاده می شود

برای دریافت نرم افزار Kerio Control 8.3.1 Build 2108 به وب سایت رسمی شرکت Kerio به نشانی زیر مراجعه کنید:

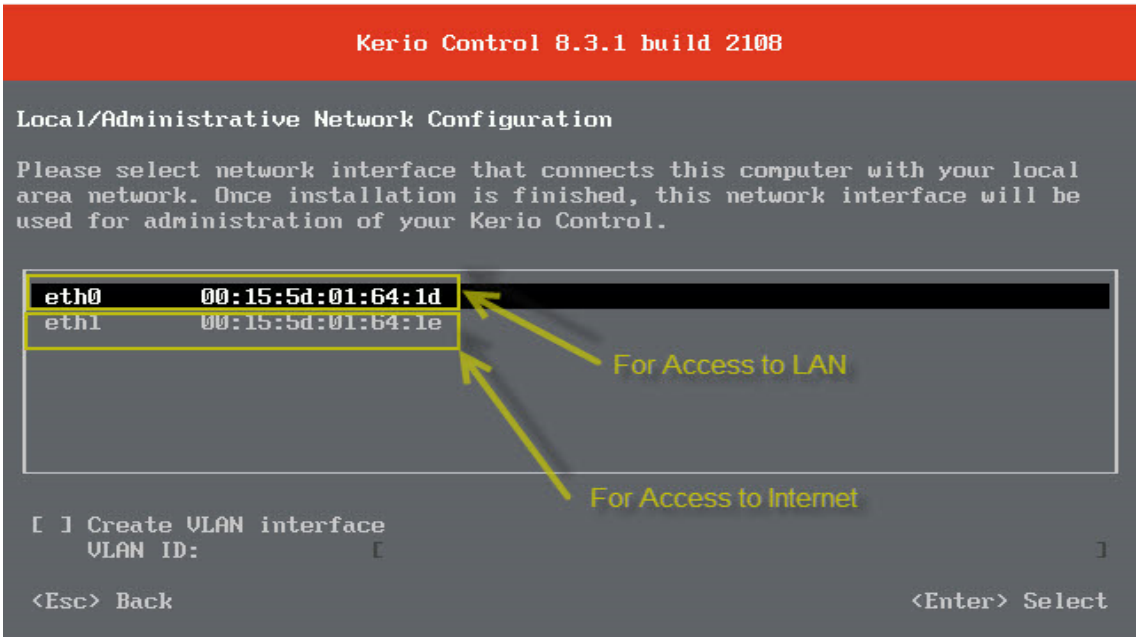
www.Kerio.com/support/kerio-control

در هنگام نصب Kerio Control در مرحله اول با صفحه زیر روبرو می شویم که همان انتخاب زبان مورد نظر می باشد، که بعد از انتخاب کردن زبان English دکمه اینتر را می زنیم.

بعد از زدن دکمه اینترصفحه Agreement ظاهر می شود که بعد از خواندن متن مربوطه دکمه F8 را برای ادامه کار می زنیم



در صفحه بعدی بر اساس توضیحاتی که قبلاً ارائه کردیم دو کارت شبکه ای که ایجاد کردیم نمایش داده می شوند یعنی eth0 و eth1 که از eth0 برای ارتباط با شبکه داخلی یا همان LAN و از eth1 برای ارتباط با اینترنت استفاده می کنیم. از IP که برای eth0 در نظر می گیریم برای دسترسی به پنل مدیریتی Kerio Control نیز استفاده می کنیم.

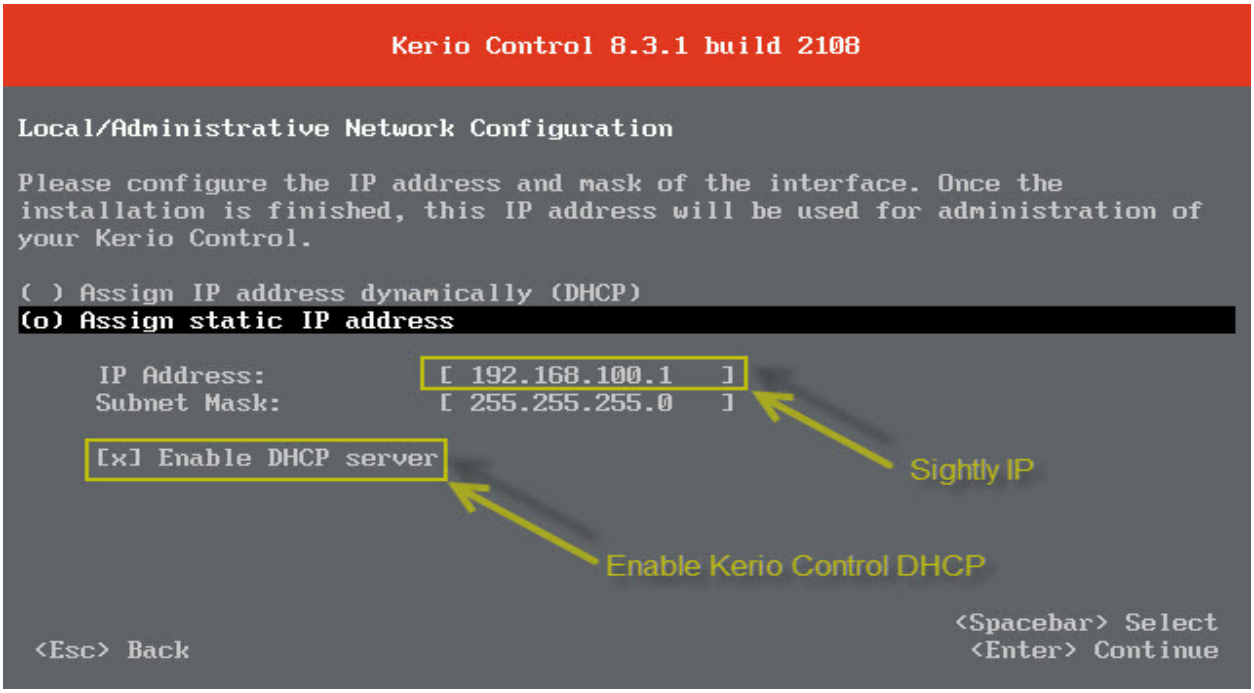


برای ادامه کار دکمه اینتر را می زنیم که در اینصورت صفحه Initial Configuration Completed ظاهر می شود یعنی اتمام تنظیمات اولیه، که این صفحه را نیز با زدن دکمه Enter رد می کنیم.

عکس صفحه بعد تنظیمات مربوط به کارت شبکه Private یا همان کارت شبکه ای که بوسیله آن می خواهیم با LAN در ارتباط باشیم هست، دو حالت برای دادن IP آدرس برای این NIC هست بدین صورت که اگر در شبکه مان DHCP داشته باشیم با انتخاب گزینه Assign IP Address Dynamically(DHCP) کارت شبکه IP خود را از DHCP Server می گیرد، ولی اگر گزینه Assign Static IP Address را انتخاب کنیم باید IP را بصورت دستی وارد کنیم، حال چونکه در این سناریو ما IP آدرس برای این NIC در نظرگرفتیم گزینه دومی را انتخاب و IP مورد نظر را وارد می کنیم.

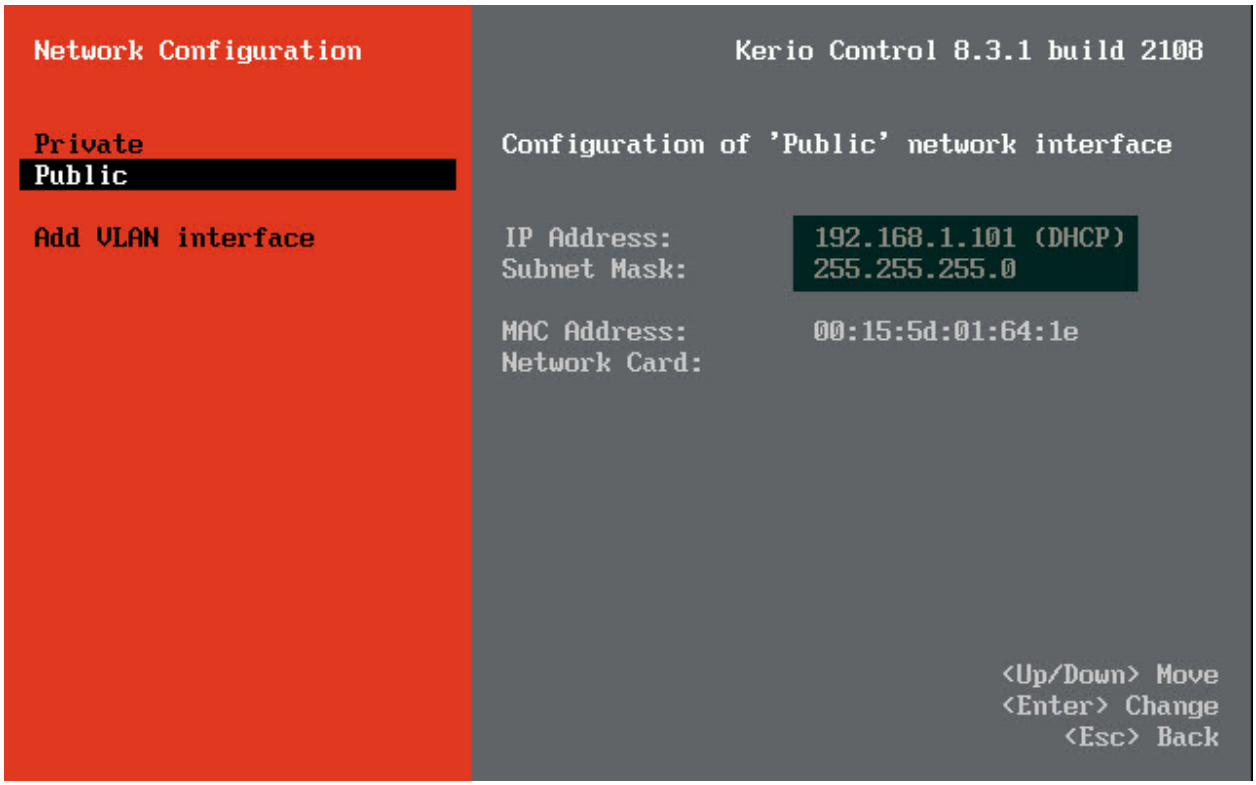
با انتخاب گزینه Enable DHCP Server همانا DHCP Server خود Kerio Control فعال و آماده ارائه خدمات می شود. توصیه می شود اگر در شبکه مورد نظرتان DHCP Server مایکروسافتی دارید این گزینه را انتخاب نکنید.

با وارد کردن IP مورد نظر و زدن دکمه Enter کار را ادامه می دهیم.



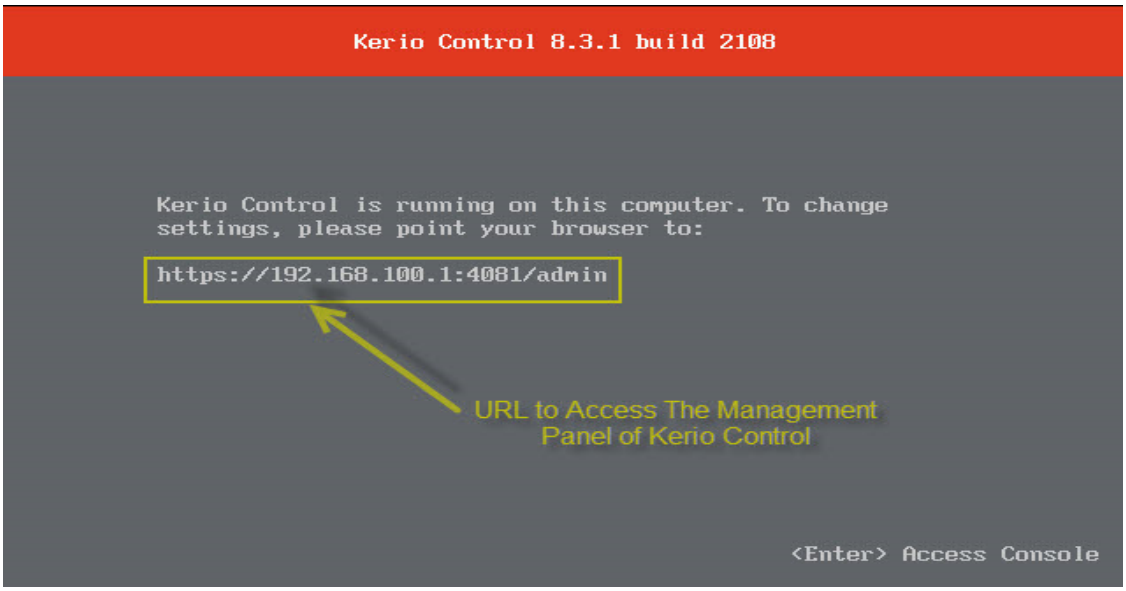
در این صفحه Kerio Control شروع به Start شدن می شود.

تنظیمات Public NIC نیز بدین صورت می باشد که چون قرار هست که این NIC با اینترنت در ارتباط باشد و به مودم ADSL متصل هست به همین دلیل IP خود را از مودم می گیرد، اگر به بخش مربوطه اش یعنی eth1 وارد بشویم IP اختصاص داده شده از طرف مودم ADSL به Public NIC را مشاهده خواهیم کرد که شکل زیر مشاهده می کنید.



در شکل بالا Public همان eth1 می باشد که اسمش از طریق پنل مدیریتی Kerio Control تغییر داده شده هست،و همانطور که مشاهده می کنید IP: 192.168.1.101 Subnet Mask: 255.255.255.0 را از طریق DHCP مودم گرفته است.

در آخر نصب Kerio Control بصورت کامل به اتمام می رسد، حال برای اینکه بتوانیم به پنل مدیریتی Kerio Control دسترسی داشته باشیم از آدرسی که در مرحله آخر نصب ایجاد شد استفاده می کنیم.

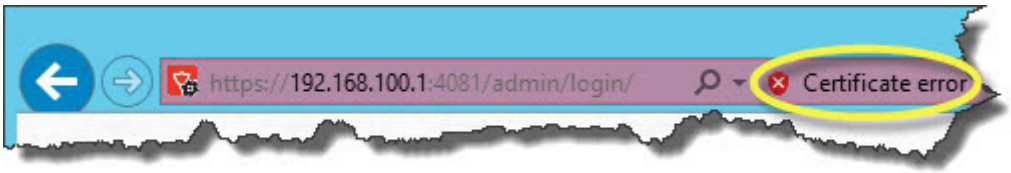


قبل از اینکه وارد پنل مدیریتی Kerio Control بشویم یک تنظیماتی مانده که با توجه به شکل زیر انجامش می دهیم.

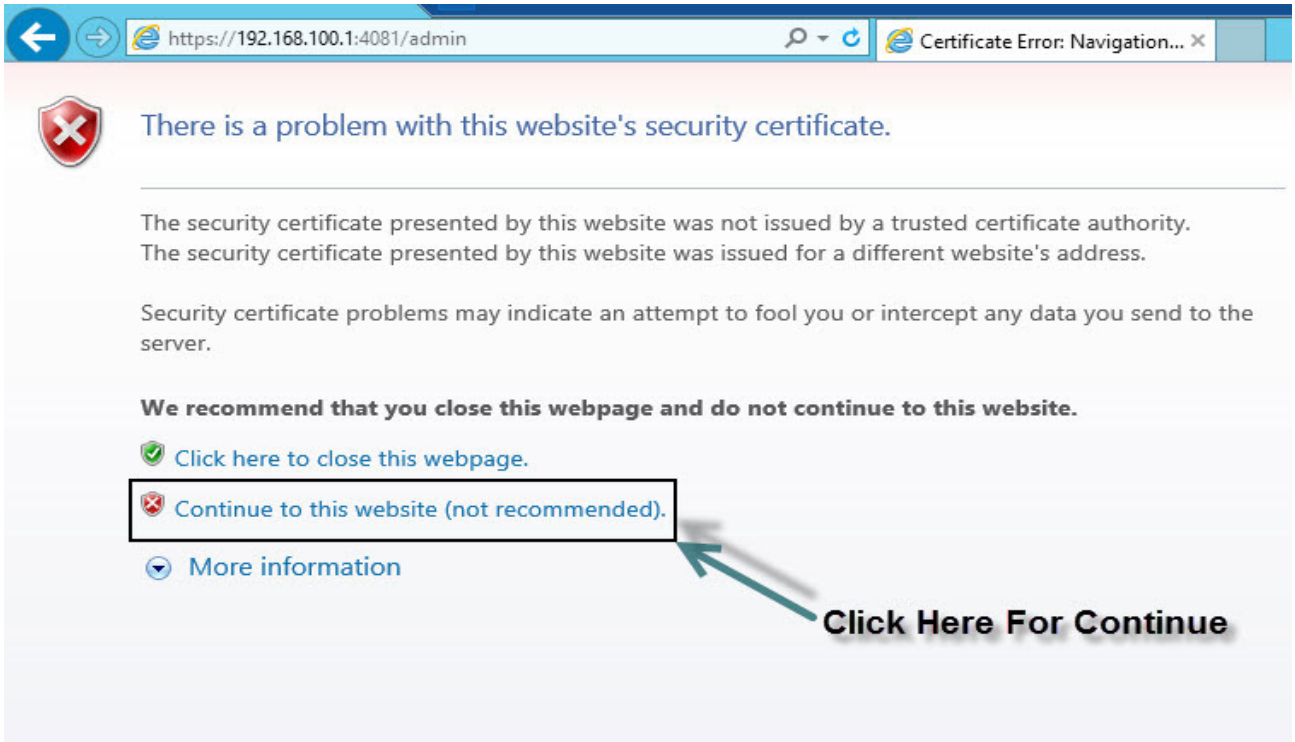
با توجه به شکل صفحه قبل در Kerio Control وارد قسمت Remote Administration می شویم و با زدن دکمه F8 این حالت را فعال می کنیم، چون می خواهیم در سناریوی مورد نظرمان از امکانات Remote نیز استفاده کنیم.

برای دسترسی به پنل مدیریتی Kerio Control آدرس https://192.168.100.1:4081/admin را در Internet Explorer یکی از سیستم هایمان که در اینجا مثلا سرور PDC را انتخاب کرده ایم وارد می کنیم.

بعد از چند ثانیه با صفحه تصویر زیر مواجه می شویم که در این صفحه با Certificate Error ای مواجه خواهیم شد.



این Error در حالت کلی یک چیزه عادی می باشد به این دلیل که هنوز Certificate ای برای Kerio Control نگرفتیم و تا اینجا خود Kerio Control برای خود یک Certificate ای صادر کرده است که در اصطلاح به آن Self Assign Certificate گویند. بعد از گرفتن Certificate از سایت خود CA ونصب در Kerio Control این Error برطرف خواهد شد و دیگر Certificate Error ای دریافت نخواهیم کرد.



نکته: اگر می خواهید که Kerio Control را برای یادگیری نصب کنید می توانید از نسخه های سری ۳۰ روزه یا همان Trial Version استفاده کنید ولی اگر می خواهید در داخل سازمان، اداره و یا شرکت Kerio Control را راه اندازی کنید بهتر هست که از نسخه های License دارش استفاده کنید (تا حد ممکن از قوانین کپی رایت حمایت کنیم).

بعد از تایپ IP مورد نظر در قسمت آدرس Internet Explorer با یک سری تنظیماتی جهت وارد شدن به پنل مدیریتی Kerio Control مواجه می شویم که این تنظیمات بصورت تصویری همراه با توضیحات در زیر آورده شده است.

Picture1 مربوط به انتخاب زبان مورد نظر می باشد.

Picture 2 مربوط به تنظیمات مکانی زمان و تاریخ و زمان می باشد، یعنی اینکه مثلا تنظیمات Time Zone باید بر روی تهران تنظیم شود.

Picture 3 مربوط به تنظیمات لایسنس Kerio Control می باشد، بدین صورت که اگر قصد دارید که Kerio Control را در یک سازمان ، شرکت و یا ... راه اندازی کنید باید از قسمت I Will Use a Commercial or NFR License اقدام به تهیه لایسنس کنید که همان خریداری لایسنس می باشد، ولی اگر می خواهید Kerio Control را بصورت دوره ای نصب و راه اندازی کنید مثلاً برای امور آموزش بهتر هست که از قسمت I Want to Try It Free For 30 Days دکمه Trial را انتخاب کنید که در این حالت Kerio Control ای که راه اندازی کرده ایم به مدت 30 روزه با ارزش خواهد بود یعنی به عبارتی به مدت 30 روزه فعال خواهد بود.

چونکه در این مقاله قصد ما فقط آموزش هست به همین دلیل نسخه Trial Version را نصب می کنیم.

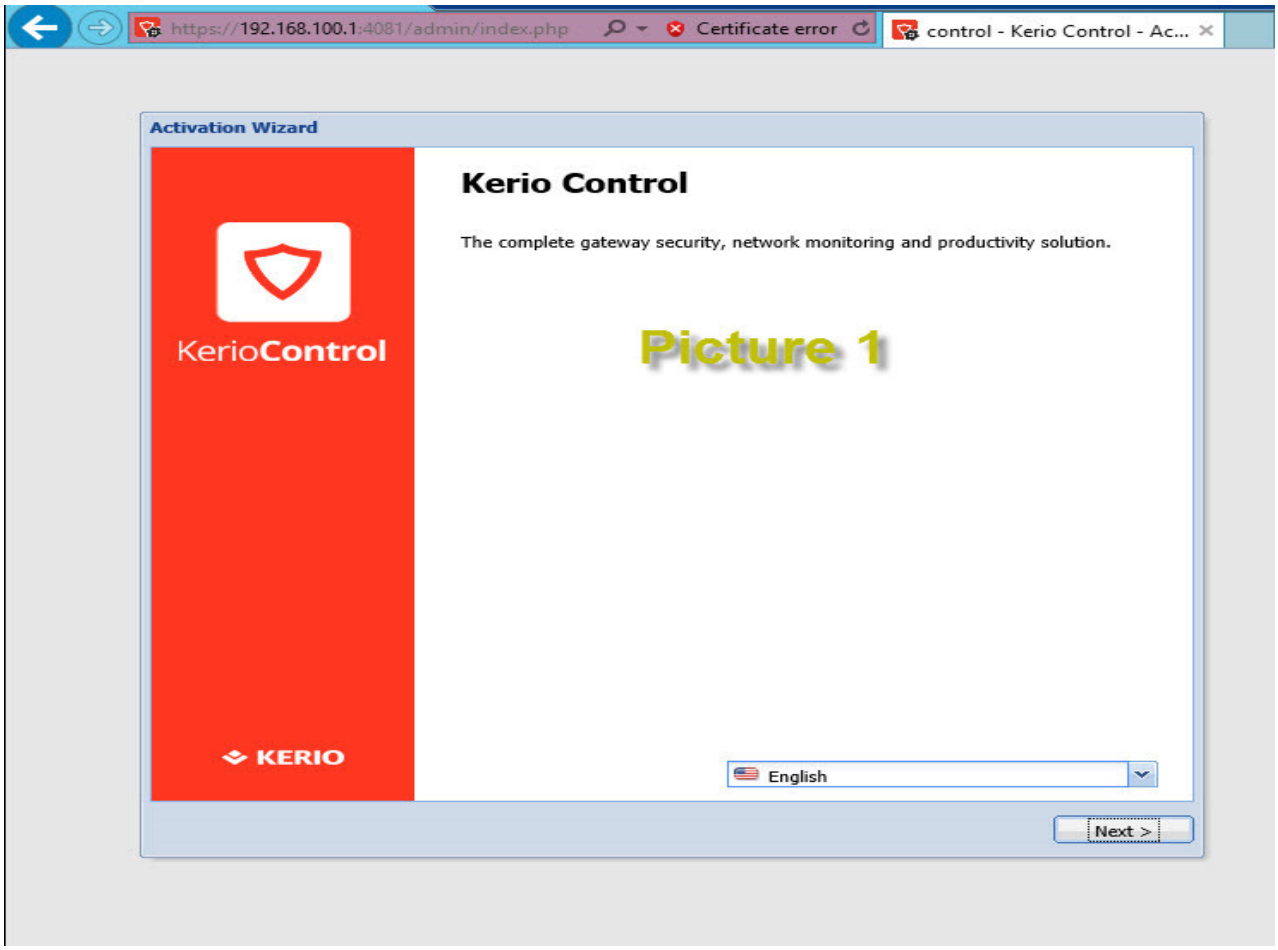
Picture 4 در این قسمت دو گزینه داریم یعنی:

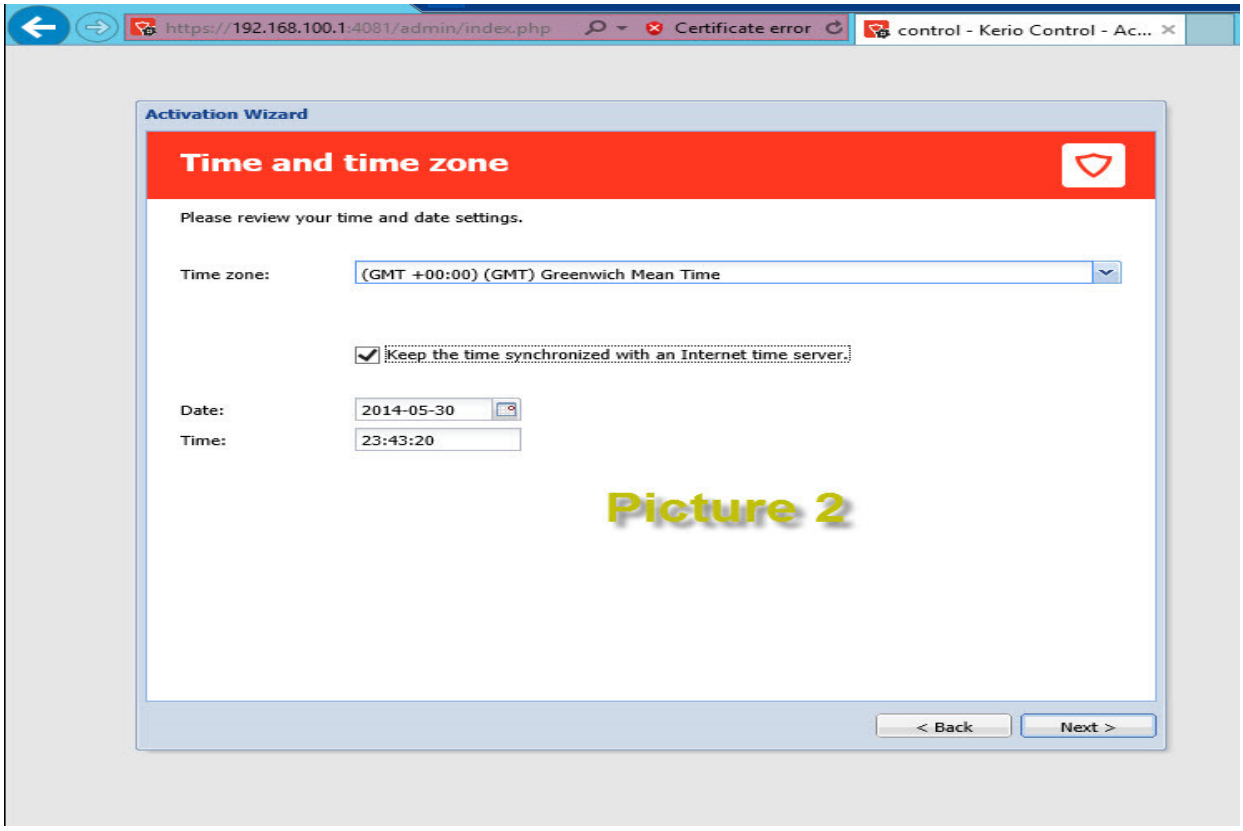
1) Get a Trial License Number
2) Activate in Unregistered Mode

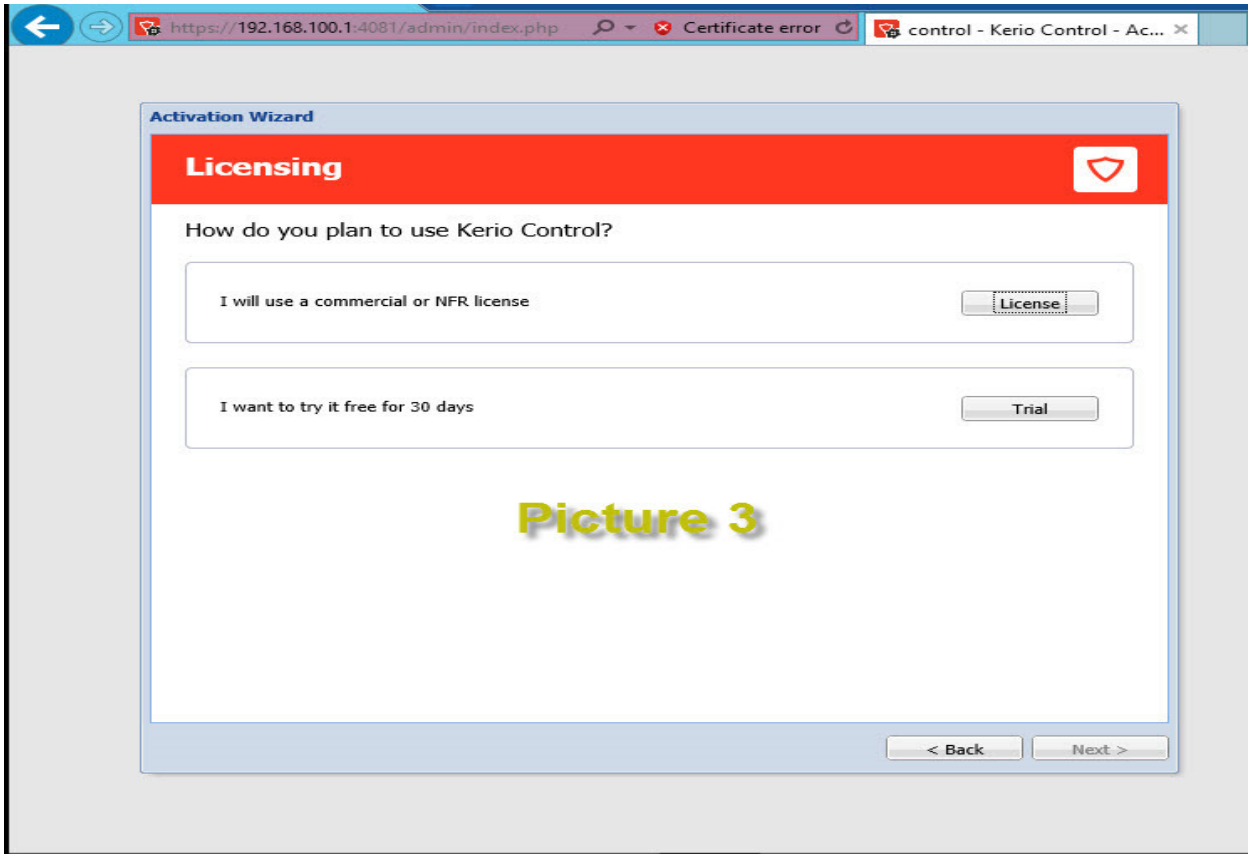
با انتخاب گزینه اولی یک Temporary License جهت راه اندازی Kerio Control ایجاد می شود که در اصل بصورت موقت Register می شود، ولی اگر گزینه دومی انتخاب شود حالت Trial بصورت Unregistered فعال می شود.

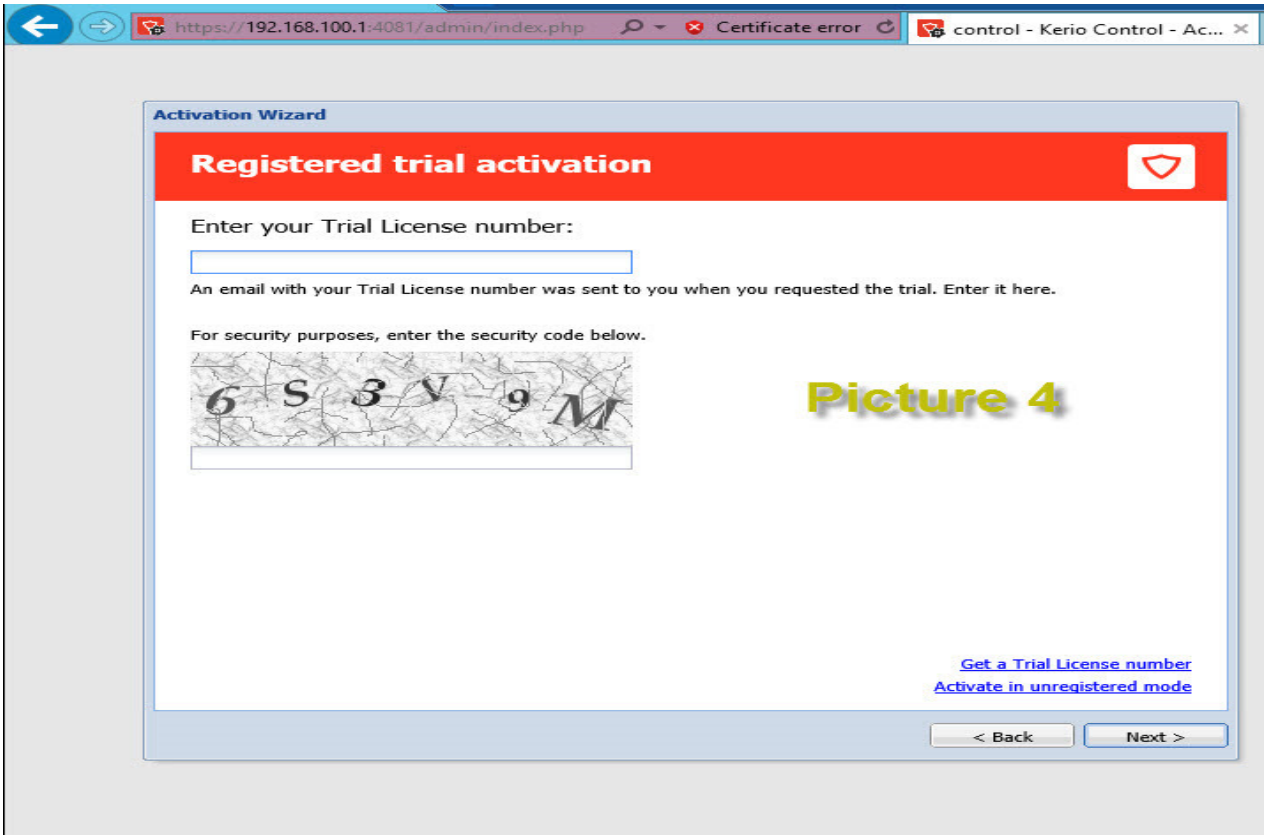
Picture 5 در این قسمت یک Password برای ورود به پنل مدیریتی Kerio Control ثبت می کنیم که در حالت کلی باید یک پسورد پیچیده باشد.

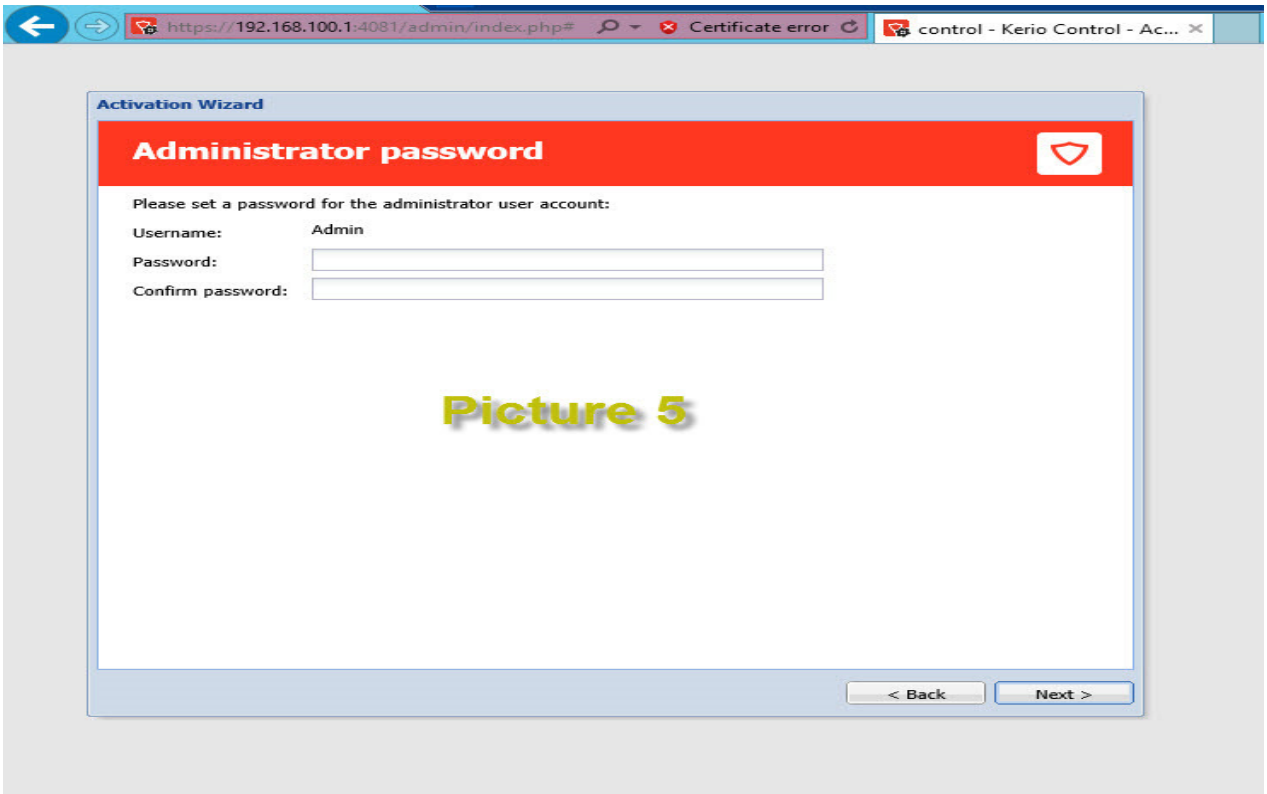
Picture 6 این تصویر آخر از مراحل نصب و راه اندازی Kerio Control می باشد، در این مرحله کادری باز می شودکه با وارد کردن Username & Password توسط Admin می توانیم وارد پنل مدیریتی Kerio Control بشویم.

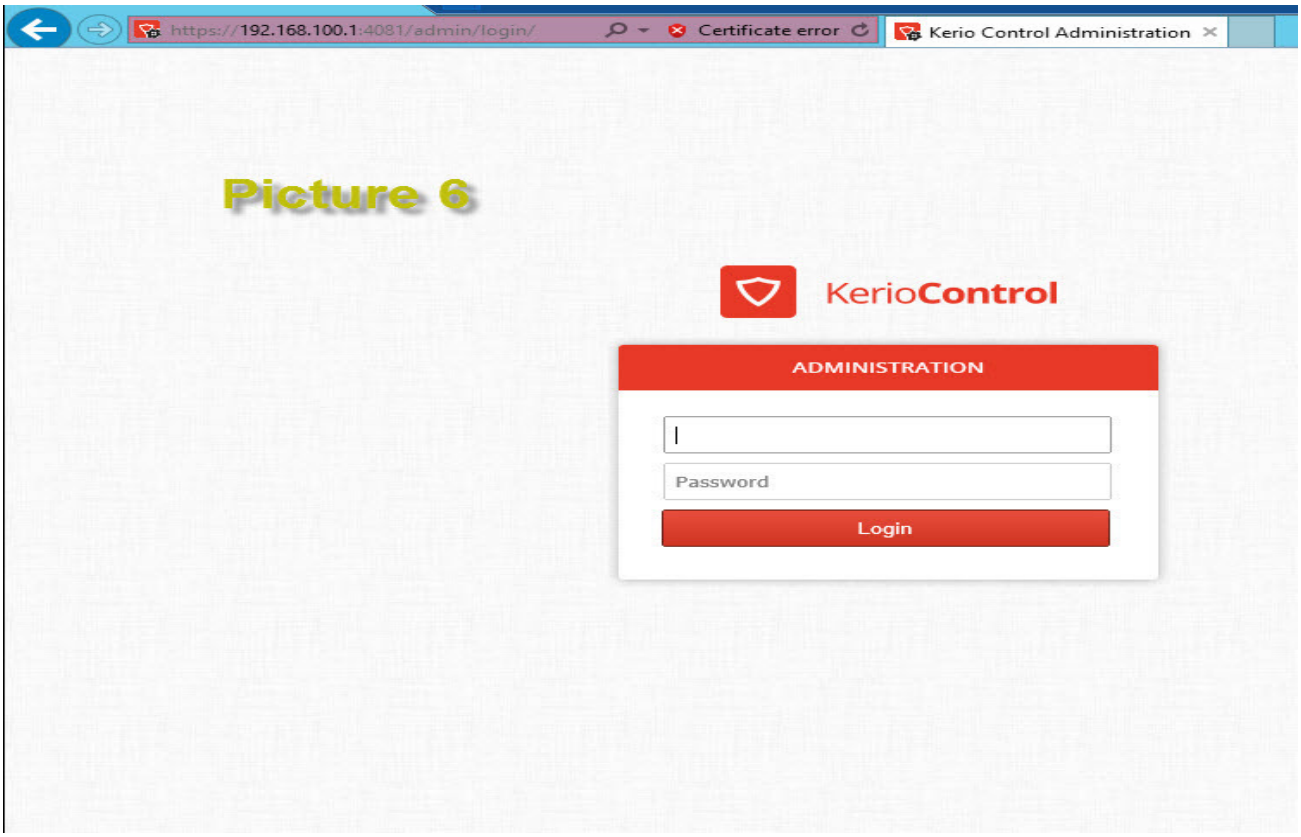



https://192.168.100.1:4081/admin/index.php
Certificate error
control - Kerio Control - Ac...
Activation Wizard
Time and time zone
Please review your time and date settings.
Time zone:
(GMT +00:00) (GMT) Greenwich Mean Time
Keep the time synchronized with an Internet time server.
Date:
2014-05-30
Time:
23:43:20
Picture 2
< Back
Next >

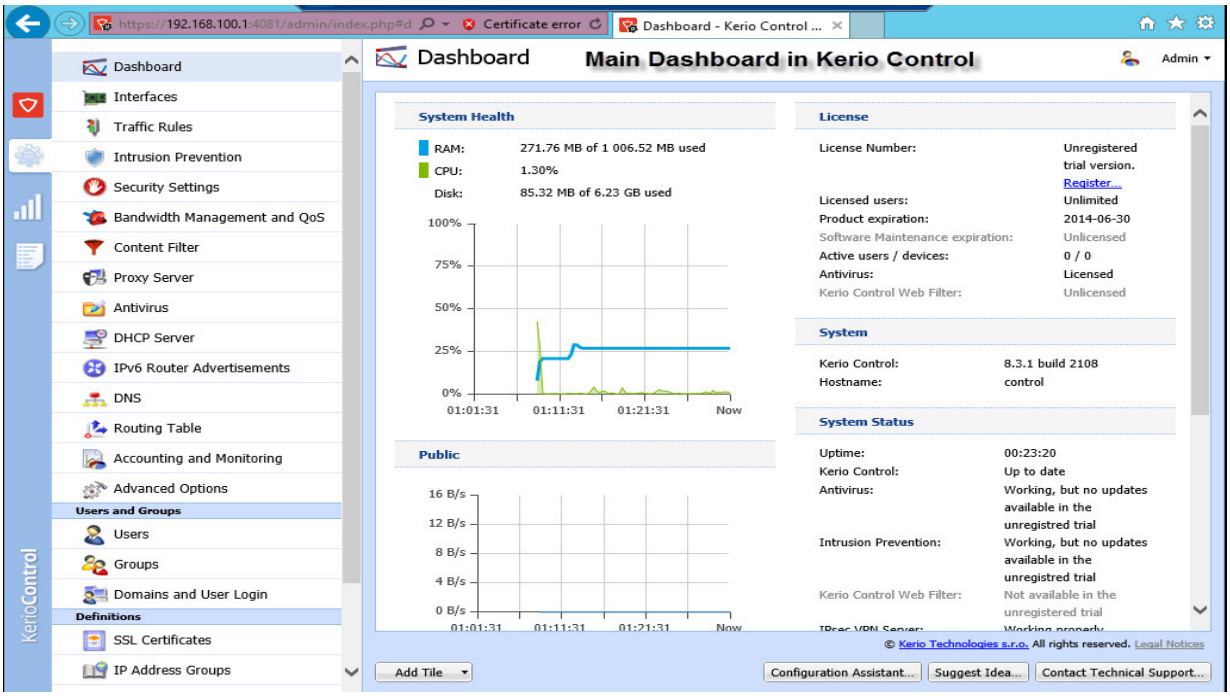

https://192.168.100.1:4081/admin/index.php
Certificate error
control - Kerio Control - Ac...
Activation Wizard
Licensing
How do you plan to use Kerio Control?
I will use a commercial or NFR license
License
I want to try it free for 30 days
Trial
Picture 3
< Back
Next >


https://192.168.100.1:4081/admin/index.php
Certificate error
control - Kerio Control - Ac...
Activation Wizard
Registered trial activation
Enter your Trial License number:
An email with your Trial License number was sent to you when you requested the trial. Enter it here.
For security purposes, enter the security code below.
6 S 3 V 9 M
Picture 4
Get a Trial License number
Activate in unregistered mode
< Back
Next >


https://192.168.100.1:4081/admin/index.php#
Certificate error
control - Kerio Control - Ac...
Activation Wizard
Administrator password
Please set a password for the administrator user account:
Username:
Admin
Password:
Confirm password:
Picture 5
< Back
Next >

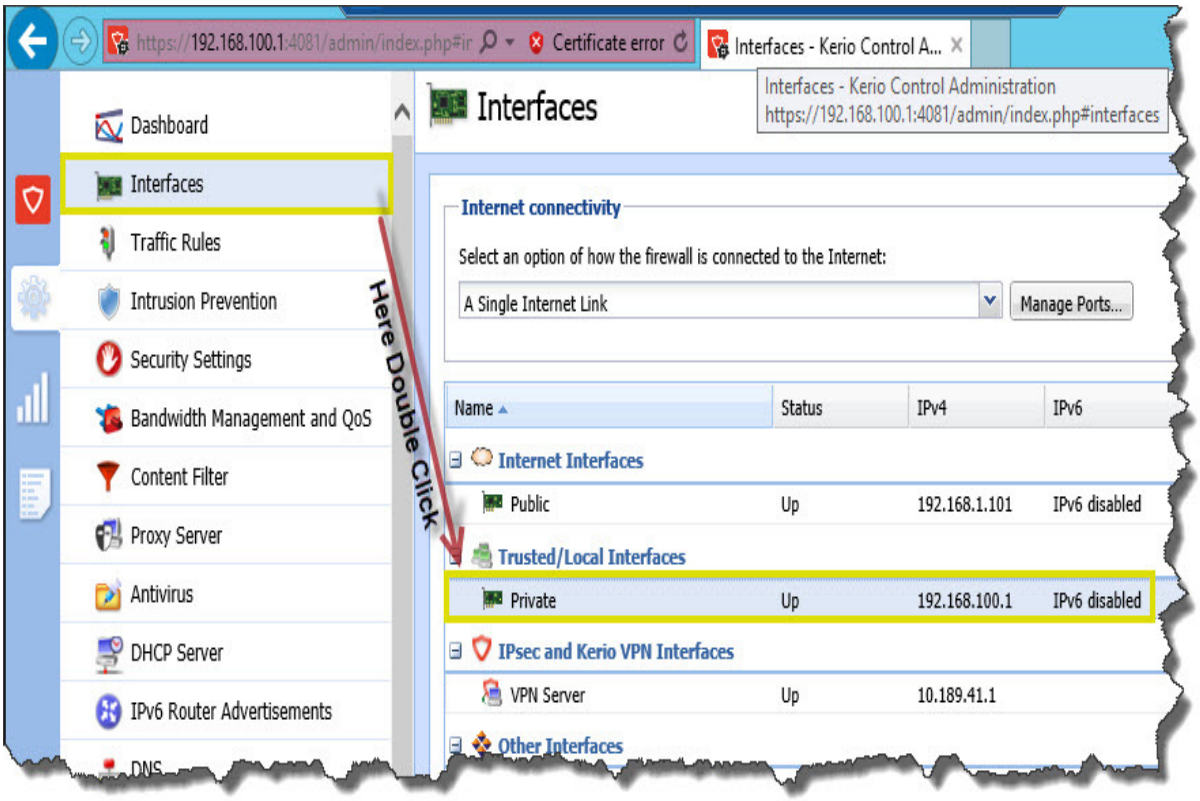


با توجه به تصویر شماره 6 یوزرنیم و پسورد مربوط به Kerio Control را وارد می کنیم تا به پنل مدیریتی اش دسترسی داشته باشیم. تصویر زیر پنل اصلی مدیریتی Kerio Control را نمایش می دهد.

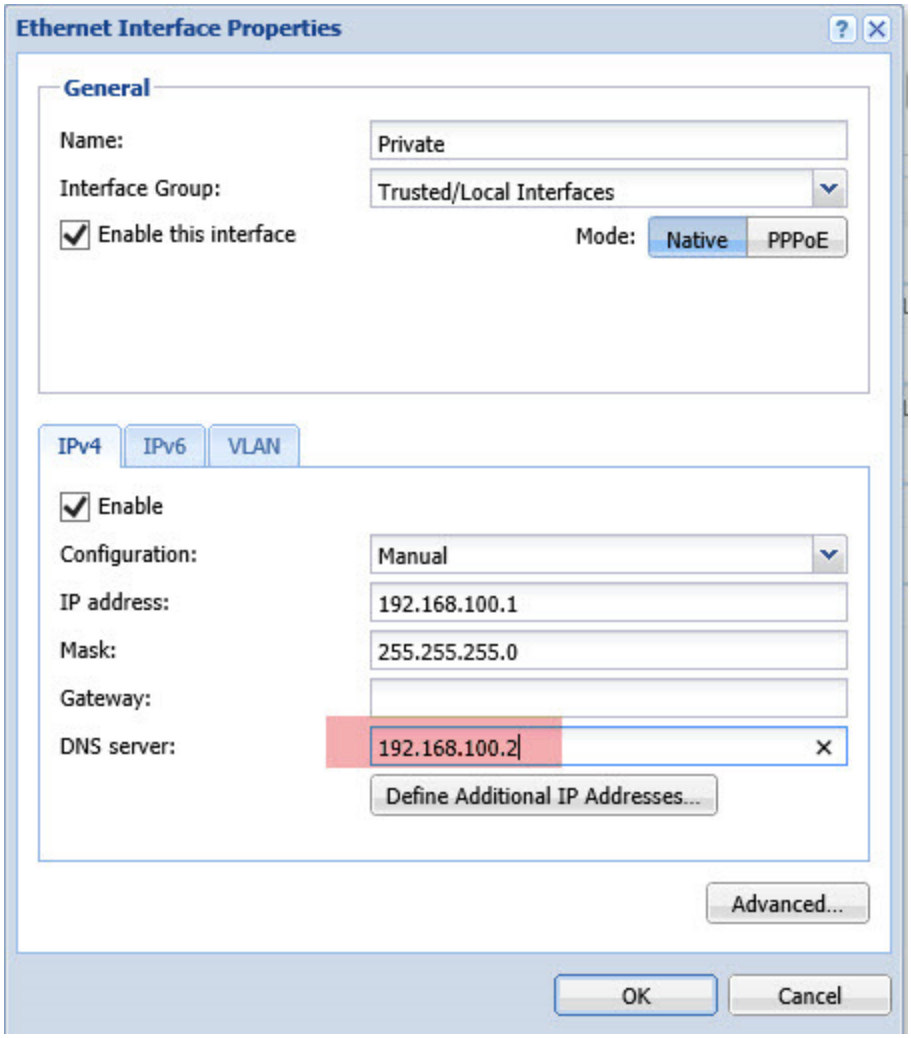


در این قسمت گزینه های متفاوتی برای مدیریت اینترنت داخل شبکه مان هست مثلا در قسمت Interfaces دو کارت شبکه یعنی Private و Public را خواهیم دید که بوسیله یکی با شبکه داخلی یا همان LAN و با دیگری با شبکه اینترنت در ارتباط خواهیم بود. در قسمت Traffic Rules نیز Rule های مورد نیاز برای ایجاد یک بستر مناسب اینترنت در داخل شبکه مان ایجاد خواهیم کرد. توضیحات قسمتهای دیگر این پنل را نیز با توجه به ایجاد سناریوهای مختلف در داخل این مقاله توضیح خواهیم داد.

قبل از ایجاد سیاستهای مورد نظر از حیث مدیریت اینترنت در داخل شبکه مان چند کار مقدماتی هست که باید انجام دهیم، یکی از این کارها Join کردن خود Kerio Control به Domain می باشد، از کارهای اولیه Join کردن یک سیستم به Domain تنظیم کردن IP آدرس سیستم Domain بعنوان DNS بر روی سیستم که می خواهد Join شود می باشد که همین کار را بوسیله پنل مدیریتی Kerio Control انجام می دهیم یعنی DNS Server دستگاه Kerio Control همانا 192.168.100.2 می شودکه برای انجام دادن این تنظیمات از قسمت Interfaces وارد تنظیمات کارت شبکه Private می شویم و بعد تنظیمات مورد نظر را اعمال می کنیم.

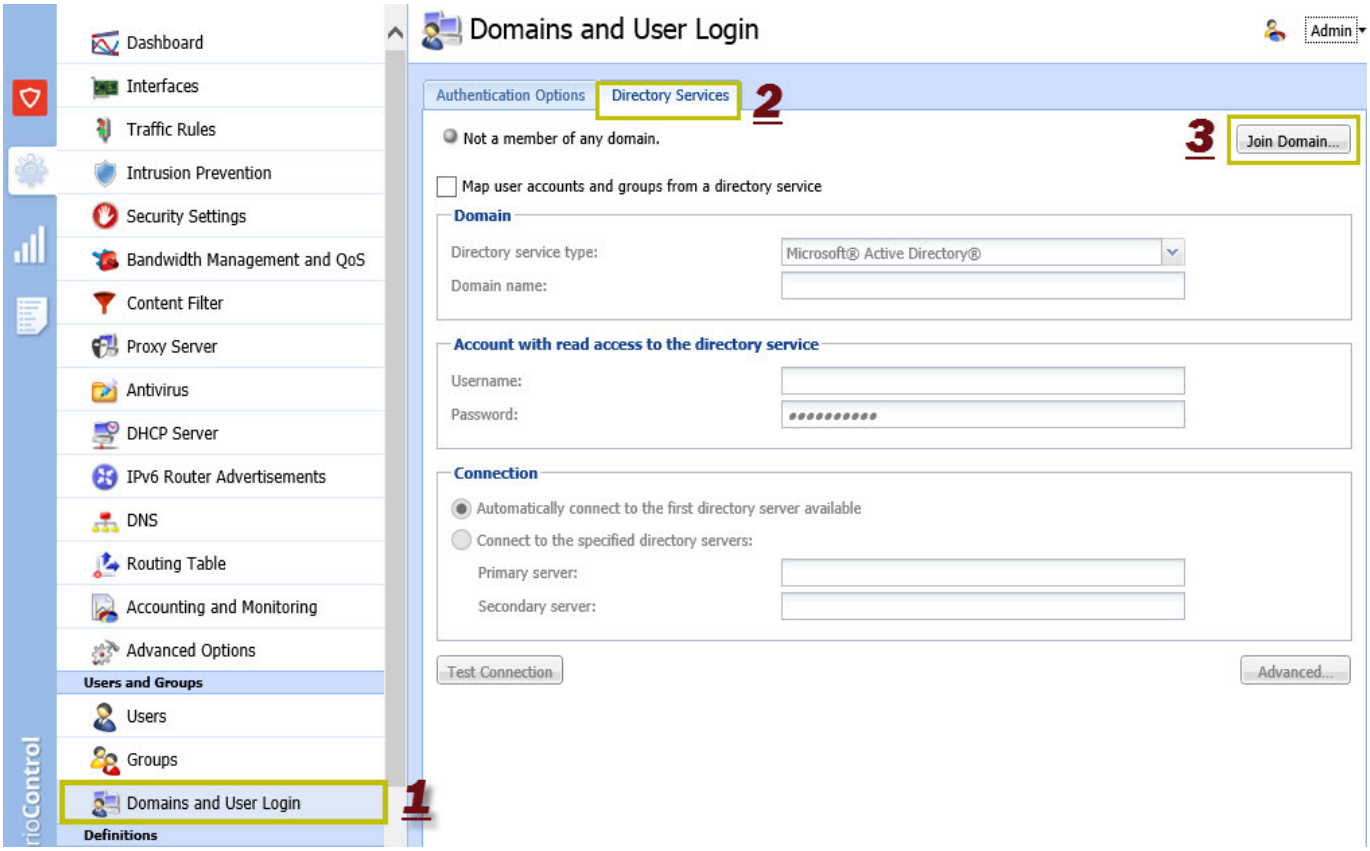


وارد کردن IP آدرس دستگاه PDC بعنوان آدرس DNS برای دستگاه Kerio Control بصورت شکل زیر انجام می گیرد.

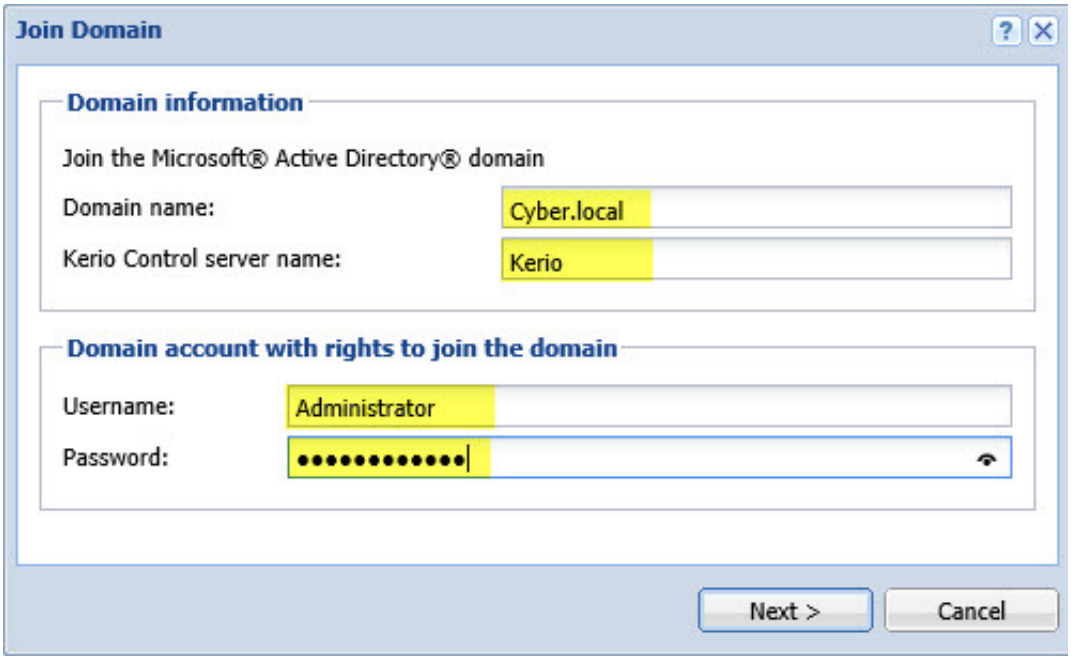


برای Join کردن دستگاه Kerio Control به Domain در صفحه مدیریتی Kerio Control از سمت چپ وارد قسمت Domain and User Login می شویم در صفحه مربوطه وارد تب Directory Services می

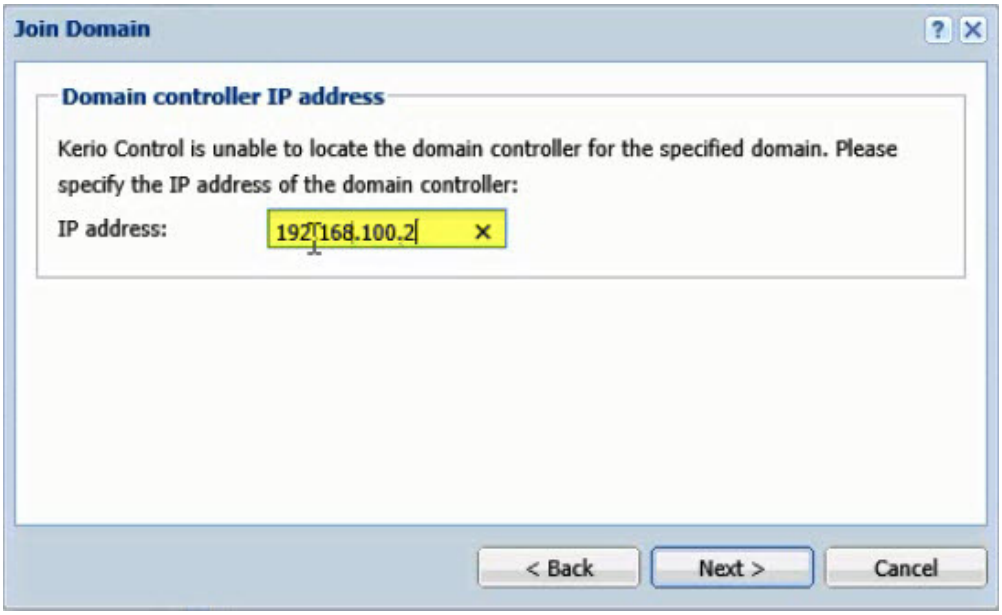
شویم که توسط تنظیمات این صفحه می توانیم دستگاه Kerio Control را Join to Domain کنیم روی دکمه Join Domain کلیک می کنیم تا صفحه Join Domain باز شود.



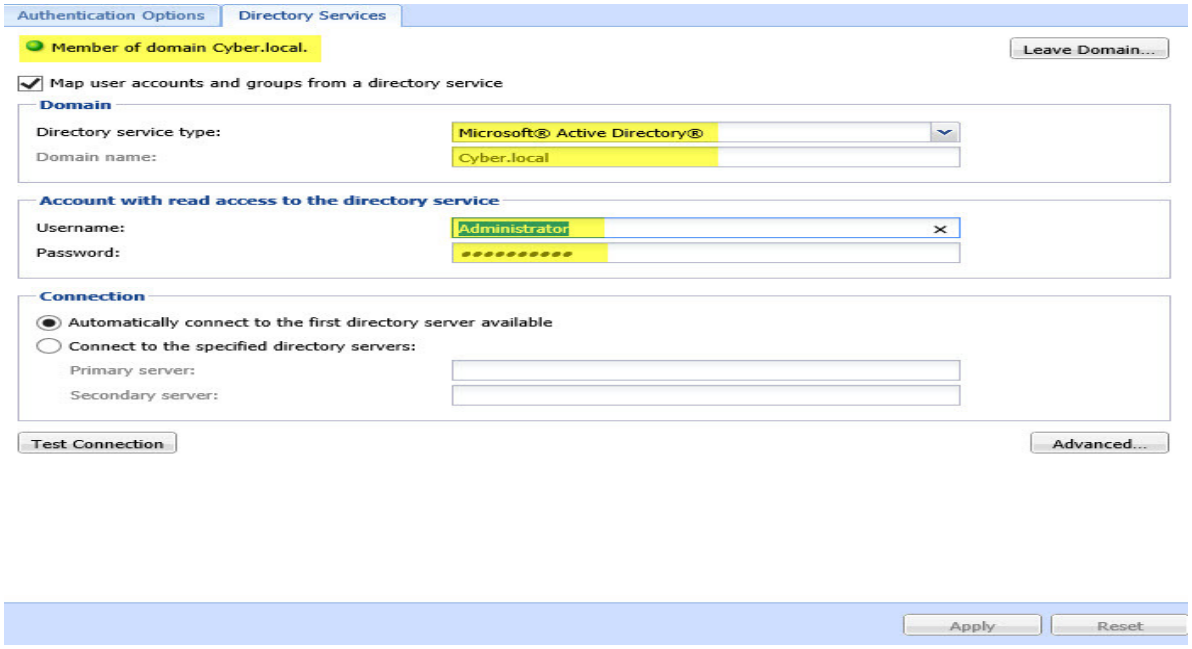
در قسمت Domain Name اسم Domain ای که می خواهیم دستگاه Kerio Control به آن Join شود را وارد می کنیم، با توجه به اینکه در سناریوی این مقاله دستگاهی که بعنوان PDC در نظر گرفتیم اسم Domain مربوطه اش Cyber.local می باشد به همین دلیل در قسمت Domain Name مربوط به تنظیمات Joinکردن دستگاه Kerio Control به دامین Cyber.local را وارد می کنیم و در قسمت Kerio Control Server Name یک اسمی بعنوان اسم دستگاه Kerio Control در نظر می گیریم که برای مثال اسم Kerio را وارد می کنیم. در قسمت Username/Password اطلاعات مربوط به یوزرنیم پسورد Admin را وارد می کنیم.



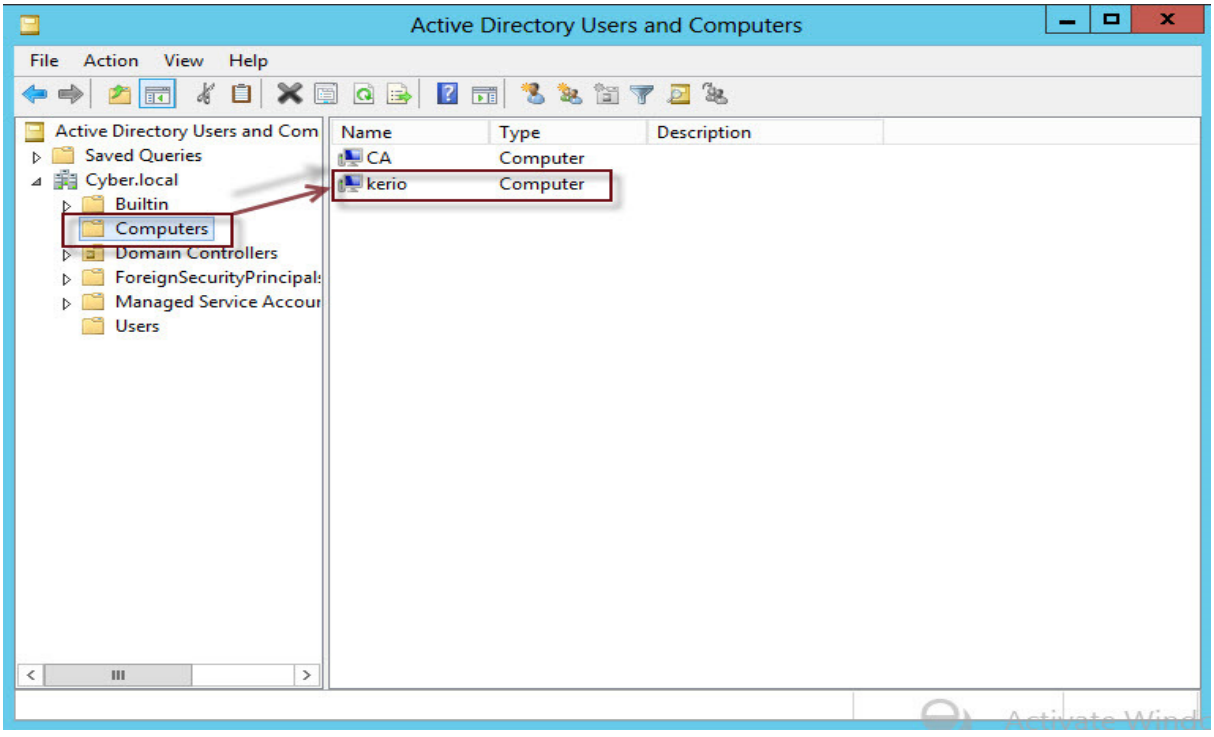
ممکن هست که بر اثر ترافیک ناشی از تبادل اطلاعات Kerio Control نتواند سرور PDC را پیدا کند تا عملیات Join را انجام دهد، به همین دلیل برای اینکه احتمال این خطا کاهش یابد در صفحه بعد از صفحه ای که مشخصات Domain را وارد کردیم Text Box ای ظاهر میشود که باید در داخل آن IP آدرس سرور Domain را وارد کنیم، بعد از وارد کردن IP آدرس Domain روی Next کلیک می کنیم تا عملیات Join با موفقیت به اتمام برسد.



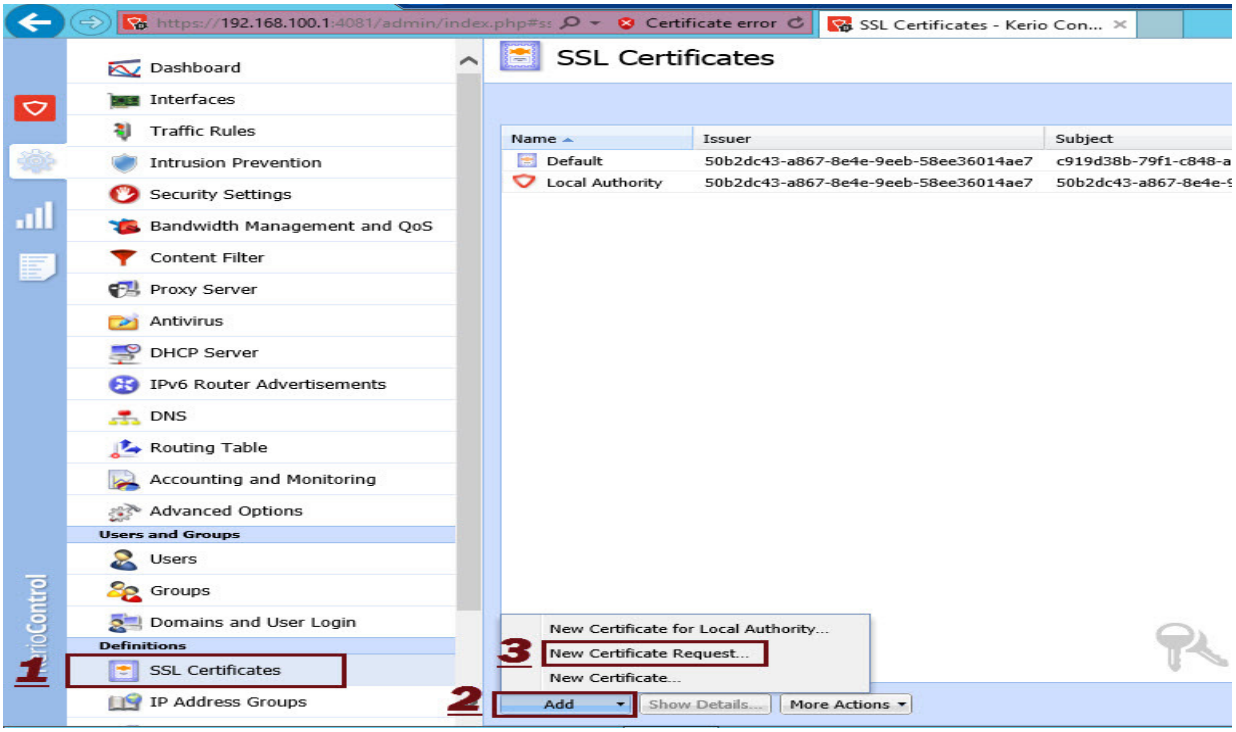
بعد از اینکه عملیات Join به اتمام رسید باید صفحه مربوط به Directory Services بصورت زیر باشد.



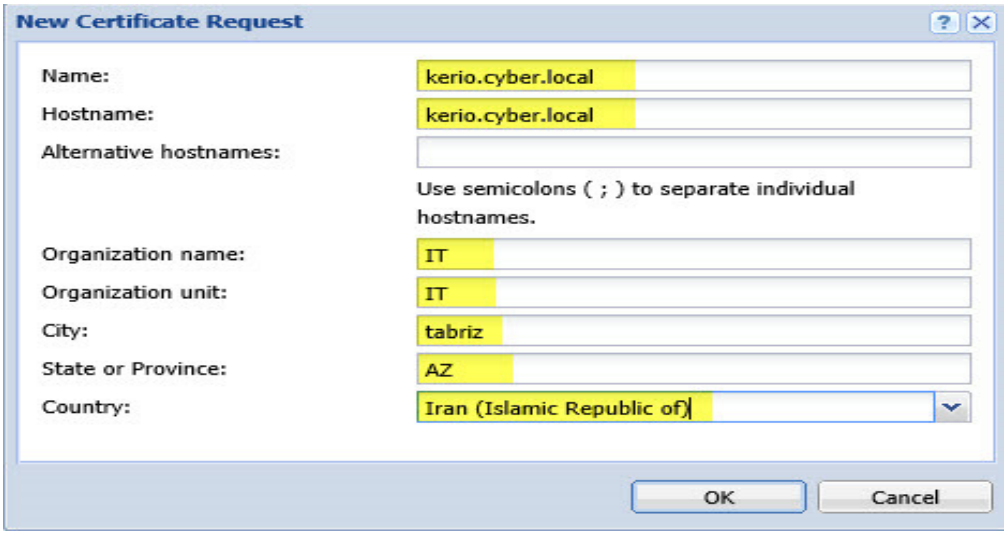
برای اینکه اطمینان پیدا کنیم Kerio Control به دامین Join شده در داخل سرور PDC وارد بخش Active Directory Users and Computers شده و از این بخش وارد قسمت Computers می شویم که اگر در آن قسمت computer Account ای با نام Kerio مشاهده کنیم می توانیم مطمئن شویم Kerio Control بصورت صحیح به دامین join شده است.



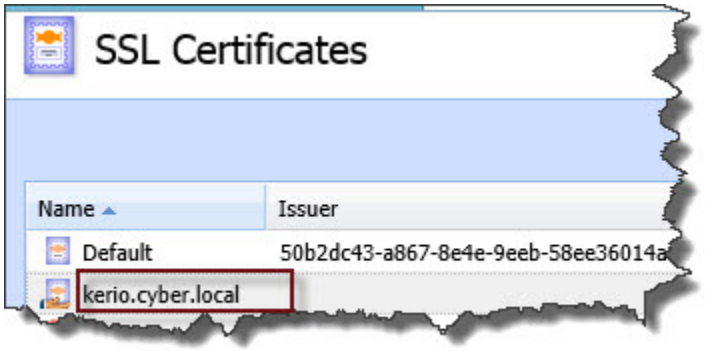
بعد از Join کردن Kerio Control به Domain نوبت به گرفتن Certificate از سایت CA برای Kerio Control می باشد، چونکه Certificate ای که در حال حاضر Kerio دارد بصورت Self Assign می باشد، یعنی خود Kerio به خودش Certificate داده است. برای این منظور از پنل مدیریتی Kerio Control وارد قسمت SSL Certificate می شویم، در پایین صفحه گزینه ای به نام Add وجود دارد که آن را کلیک می کنیم وبعد New Certificate Request را انتخاب می کنیم.



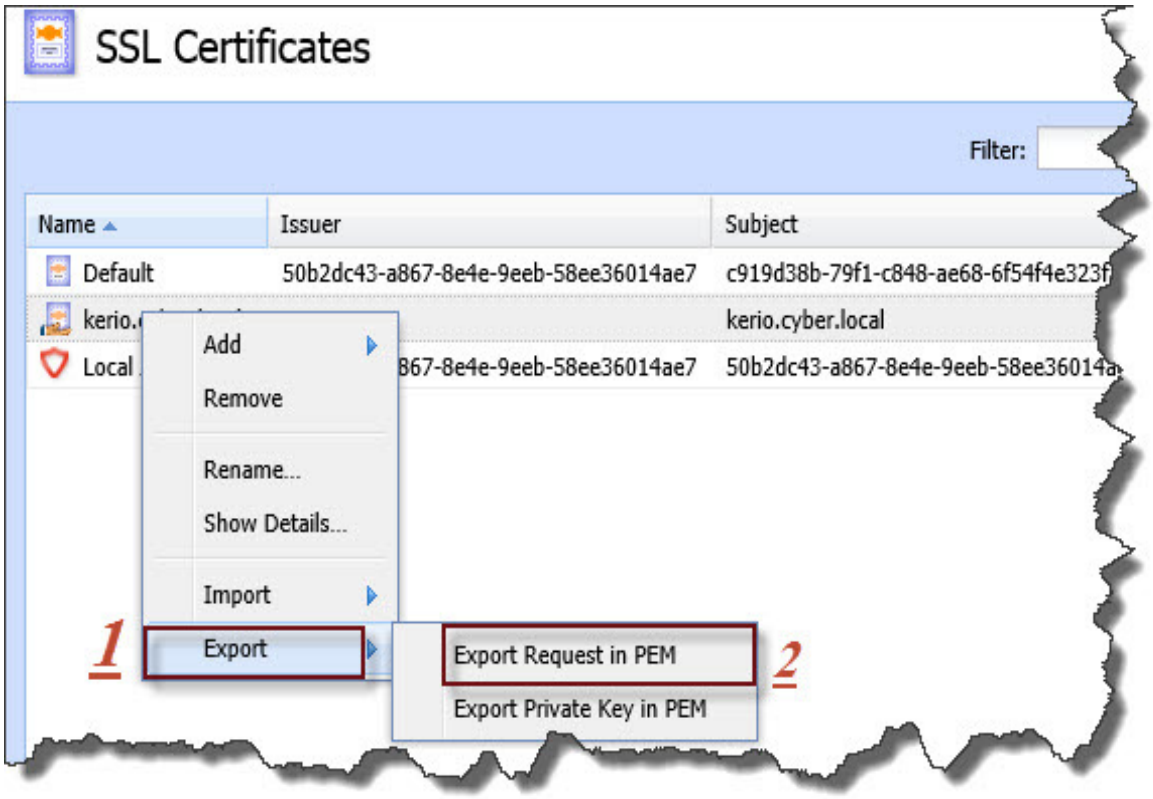
با انتخاب این گزینه صفحه ای باز می شود که با وارد کردن اطلاعات مورد نظر درخواست یک Certificate برای ارائه به سایت CA و دریافت یک Certificate آماده می شود.



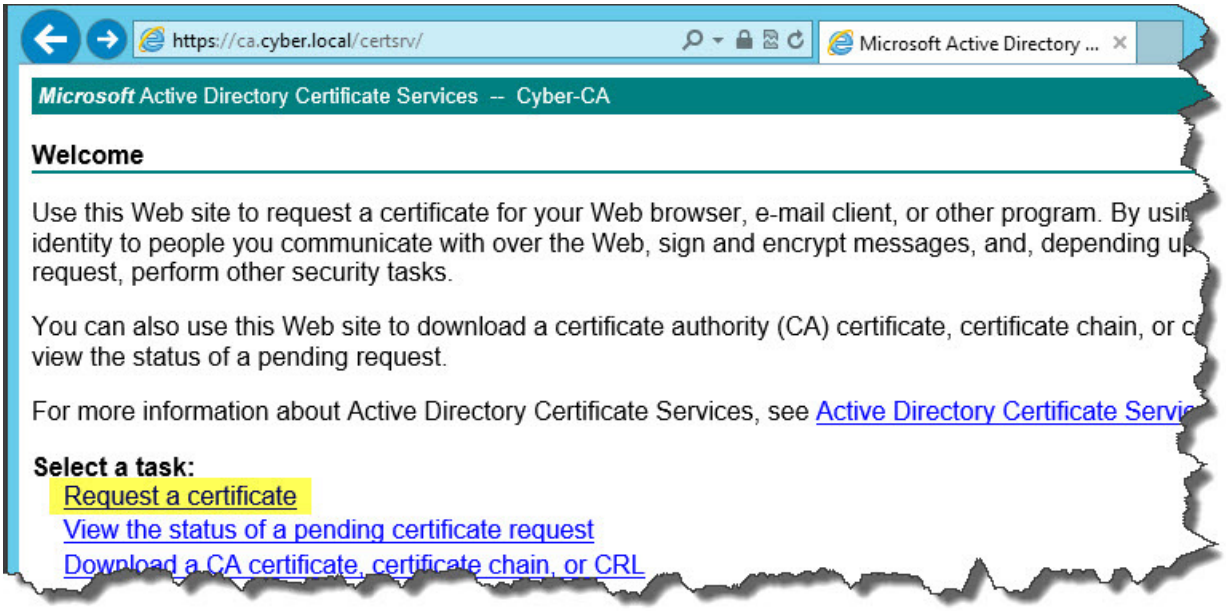
بعد از ثبت کردن درخواست مورد نظر بصورت شکل زیر در قسمت SSL Certificate نمایش داده می شود.



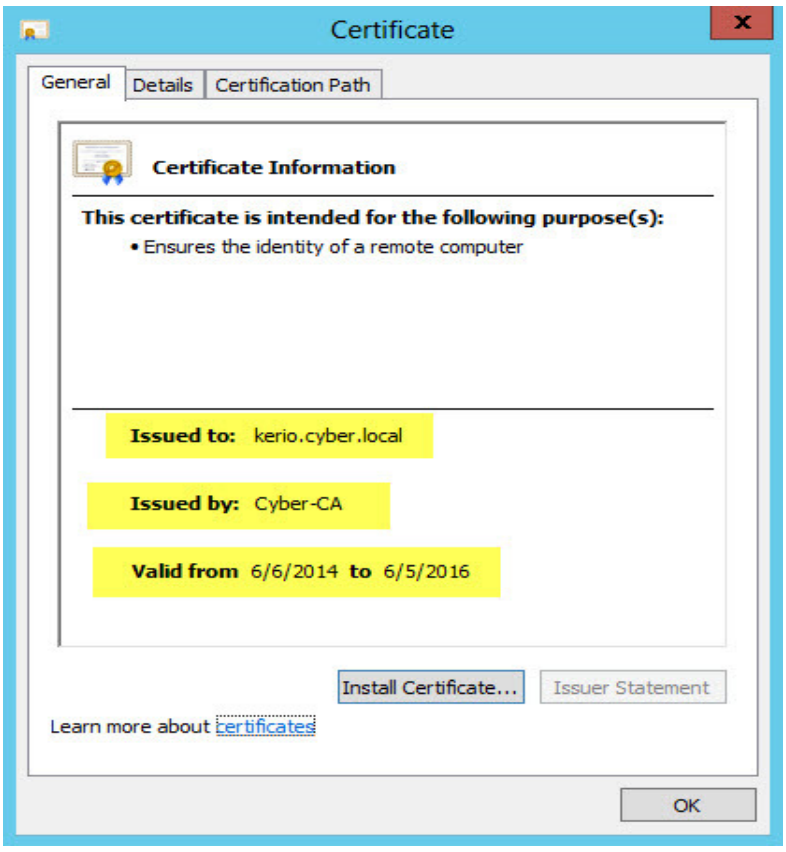
برای اینکه بتوانیم این درخواست را به سایت CA به جهت گرفتن یک Certificate برای Kerio Control ارجاع بدهیم باید از درخواست مورد نظر یک خروجی *cer*. بگیریم، به همین دلیل روی درخواست مورد نظر راست کلیک می کنیم و از گزینه Export گزینه Export Request in PEM را انتخاب می کنیم و درخواست مورد نظر را با پسوند *cer*. در هر مقصدی مثلاً در دسکتاپ سیستم ذخیره می کنیم.



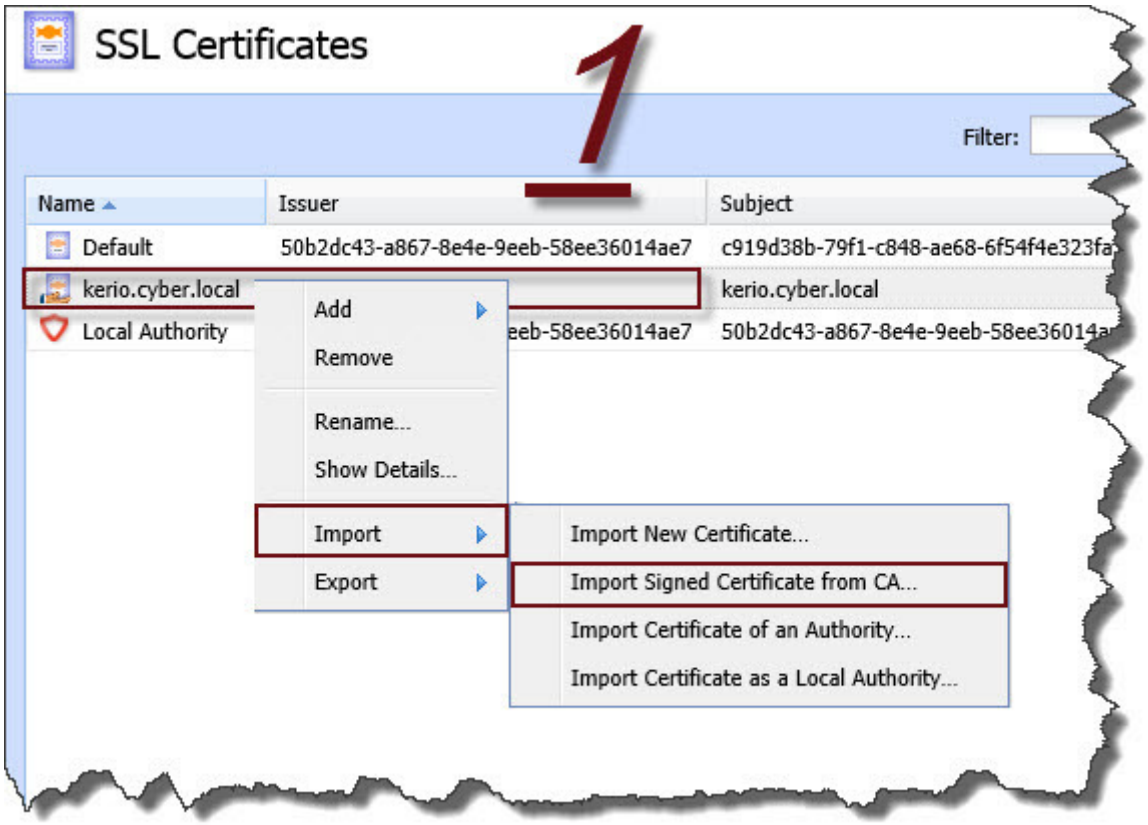
بعد از تهیه درخواست Certificate برای اینکه بتوانیم این درخواست را به سایت CA وارد کنیم به آدرس https://ca.cyber.local/certsrv مراجعه می کنیم و عملیات ثبت و دانلود در خواست را انجام می دهیم.

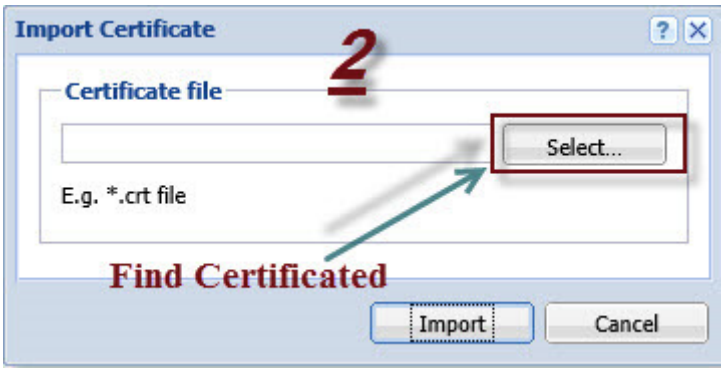


Certificate دانلود شده:

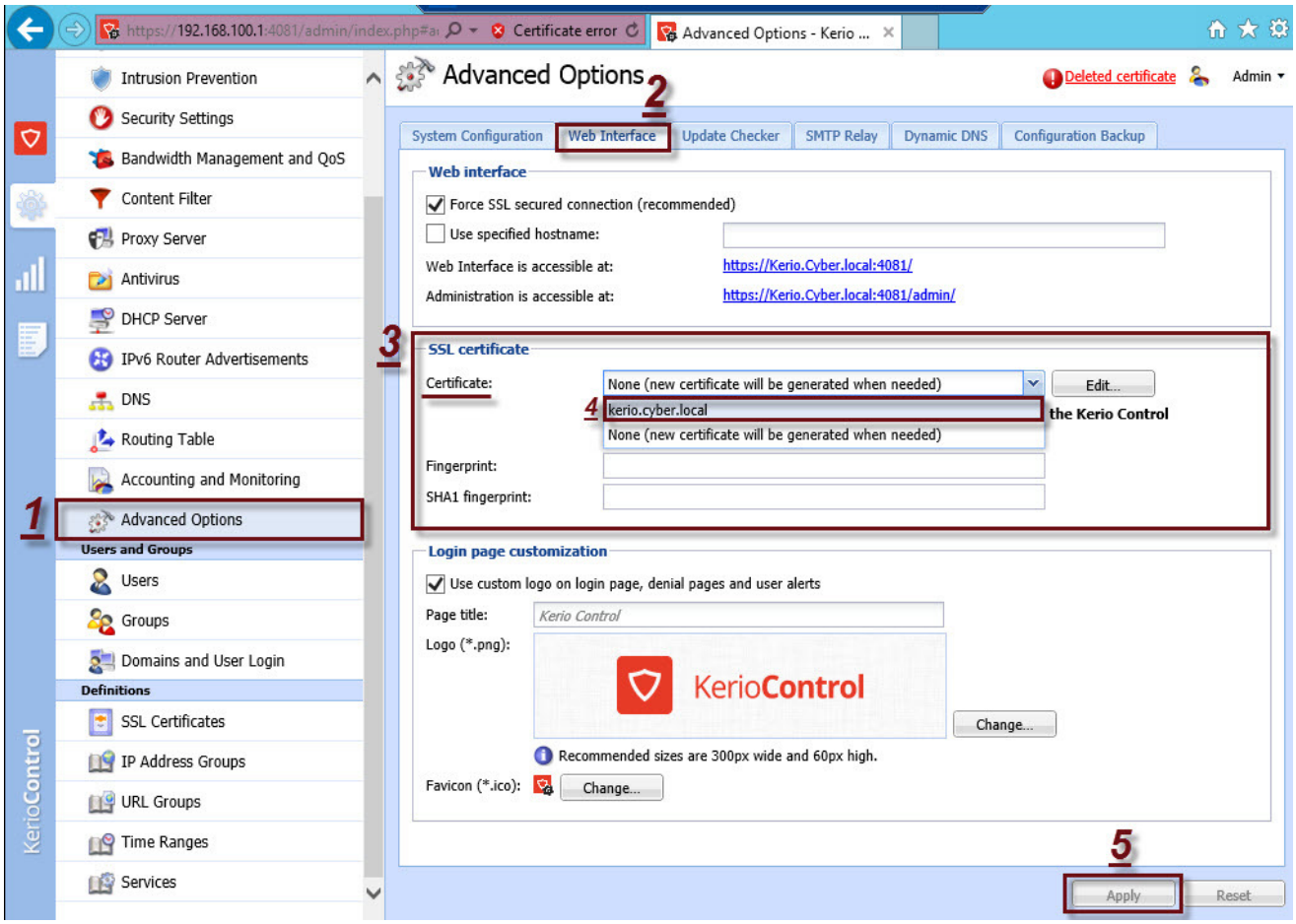


حال برای اینکه Certificate صادر شده از طرف سایت CA به Kerio Control را به این دستگاه اختصاص بدهیم در قسمت SSL Certificate روی درخواست مورد نظر راست کلیک کرده و از قسمت Import گزینه Import Signed Certificate From CA … را انتخاب می کنیم و از آن Certificate ای را که از سایت CA گرفته و در دسکتاپ قرار داده ایم را به داخل سیستم Import می کنیم.





بعد از Import کردن Certificate مورد نظر به داخل سیستم از بخش Advanced Options وارد تب Web Interface می شویم و از قسمت SSL Certificate و Certificate همانا Certificate مورد نظر را انتخاب می کنیم و بعد روی Apply کلیک می کنیم که با این کار Kerio Control یکبار Log out و Log in می شود، هنگام Log in دوباره، بجای استفاده از آدرس https://192.168.100.1:4081/admin از آدرس https://kerio.cyber.local:4081/admin استفاده می کنیم، با انجام این عملیات Kerio Control بصورت رسمی Certificate دار شده و دیگر هیچ Certificate Error ای را مشاهده نخواهیم کرد.



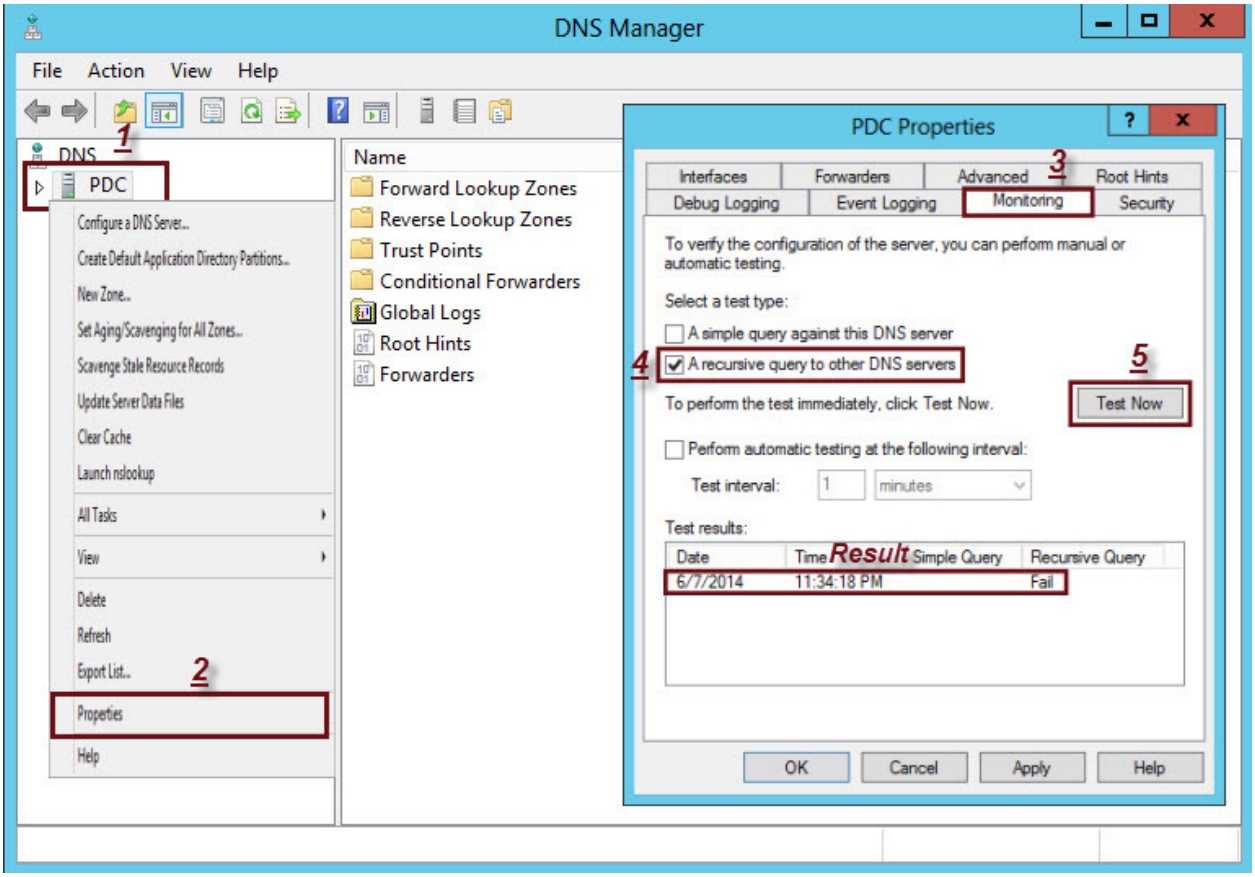
نکته : Kerio Control 8.3.1 یک ویژگی جالبی داره که می توانیم Login Page مربوطه اش را از قسمت Login Page Customization تغییر بدهیم . این قسمت را می توانید در تصویر بالا مشاهده کنید که همان صفحه مربوط به Advanced Options می باشد.

تا الان ما تنظیمات مربوط به آماده سازی و ایجاد بستر مناسب برای اینکه Kerio Control وظیفه اصلی خودش را ایفا کند را مهیا ساخته ایم. برای اینکه Kerio Control وظیفه اصلی خودش را بازی کند یک سناریویی را در داخل Kerio Control پیاد می کنیم و آن هم ایجاد محدودیت هایی از حیث دسترسی سرورها و کلاینت های داخل شبکه به اینترنت می باشد، روند کلی کار بدین صورت می باشد که در ابتدا ما می خواهیم سرورها و کلاینت ها به عوض اینکه خودشان به فایلهای آپدیتشان دسترسی داشته باشند به کمک یک سرور که در نقش یک واسط می باشد این کار را انجام دهد چونکه اگر اینکار انجام شود باعث ایجاد ترافیک در شبکه و اشغال پهنای باند اختصاص داده شده می شود، حال برای اینکه این مشکل برطرف شود می توانیم یک سرور مجزا برای اینکار در نظر بگیریم که همان سرور WSUS(Windows Server Update Services) می باشدکه این سرور درخواست های سرورهای دیگر وکلاینت ها را برای دریافت فایلهای آپدیت دریافت می کندو به اینترنت ارجاع می دهد و بعد از دریافت پاسخهای مورد نظر آنها را در سرور WSUS ذخیره می کند تا سرورهای دیگر و کلاینت ها برای دریافت فایلهای آپدیت مورد نظرشان به این سرور مراجعه کنند، همچنین این کار را در مورد DNS سرورها نیز می توانیم انجام بدهیم یعنی سرورها و کلاینت های شبکه داخلی درخواست های DNS ای خود را به یک سروری که در شبکه داخلی DNS در آن پیاده سازی شده انتقال می دهند و فقط این DNS سرور می تواند درخواست ها را به DNS سرورهای شبکه خارجی ارجاع بدهد و جوابهای مورد نظر را دریافت کند.

DNS سرور مورد نظر در شبکه داخلی همان سرور PDC می باشد که روی آن DNS پیاده سازی شده و سایر سرورها و کلاینت ها به آن Join شده اند. برای اینکه بتوانیم این کار را انجام دهیم باید در داخل Kerio Control یک Rule ای ایجاد کنیم که فقط به سرور PDC اجازه دسترسی به DNS سرورهای شبکه خارجی را بدهد.

در مرحله اول برای تست اینکه آیا سرور PDC به DNS سرورهای شبکه خارجی دسترسی دارد یا نه وارد قسمت DNS از سرور PDC می شویم، در سمت چپ صفحه باز شده بر روی آیکون سرور PDC راست کلیک می کنیم و گزینه Properties را انتخاب می کنیم تا صفحه مربوطه باز شود، سپس وارد تب Monitoring می شویم

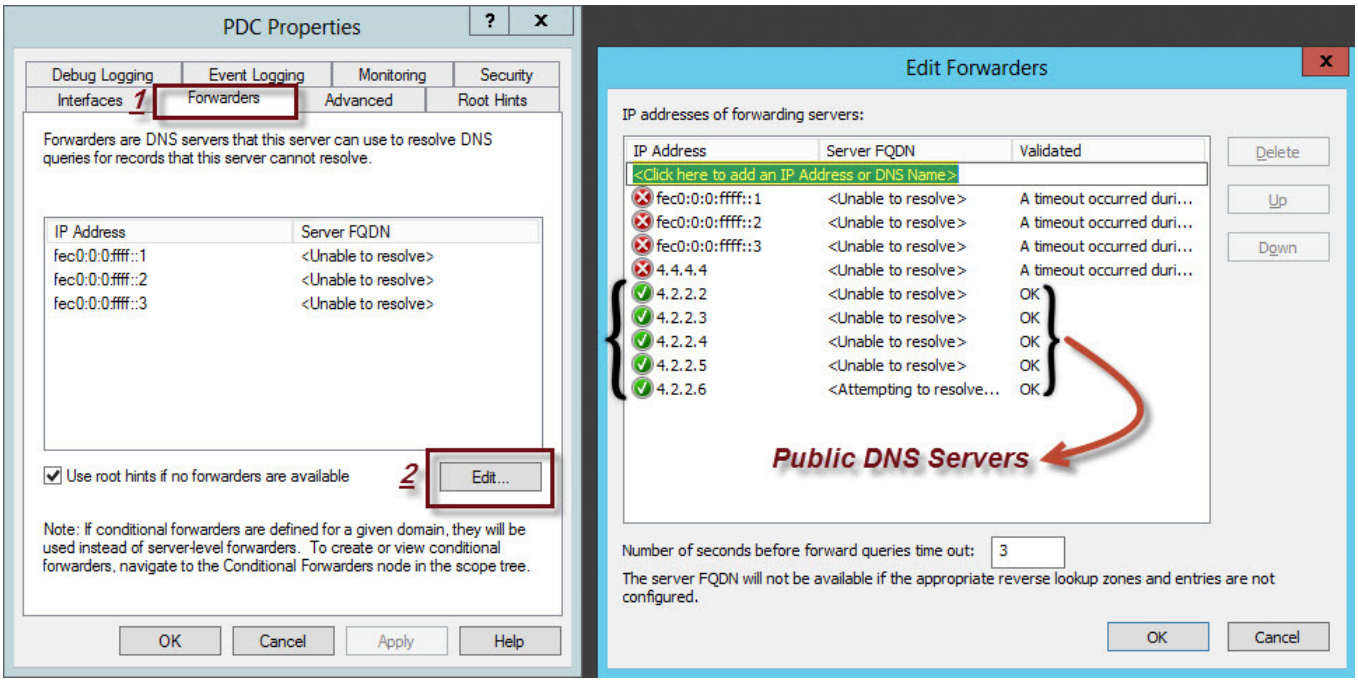
و تیک گزینه A recursive query to other DNS Server را می زنیم وبعد روی Test Now کلیک می کنیم، با این کار مطمئن می شویم که آیا به DNS سرورهای بیرونی دسترسی داریم یا خیر، اگر در کادر پایین صفحه عبارت Fail آمد یعنی به DNS سرورهای خارجی دسترسی نداریم که حالت درست همین هست چونکه Rules مربوطه را ایجاد نکرده ایم و اگر عبارت Pass آمد یعنی به DNS سرورهای خارجی دسترسی داریم که با توجه به اینکه تا اینجا Rules مربوطه ایجاد نشده این حالت نادرست می باشد. در تصویر زیر موارد ذکر شده نشان داده شده است.



بعد از انجام تست اینکه آیا سرورها و کلاینت های شبکه داخلی به DNS سرورهای Public دسترسی دارند یا خیر، نوبت به این رسیده که این عمل را تسهیل کنیم، یعنی با وارد کردن بعضی از آدرسهای DNS سرورهای

Public در قسمت Forwarding و ایجاد Rules ای که بوسیله آن Kerio Control این اجازه را صادر کند که Request DNS ها به Public DNS ها دسترسی داشته باشند.

برای انجام اینکار با توجه به شکل بالا که از PDC، Properties گرفتیم و صفحه PDC Properties بازشد، وارد تب Forwarders می شویم و دکمه Edit را می زنیم و در صفحه مربوطه تعدادی از آدرسهای DNS سرورهای Public را وارد می کنیم.



بعد از وارد کردن Public DNS ها دوباره همانند شکل صفحه قبل وارد تنظیمات DNS می شویم و از تب Monitoring تیک گزینه A recursive query to other DNS Server را می زنیم که این بار باید عبارت Pass ظاهر شود.

حال برای ایجاد Rules مورد نظر برای این کار وارد بخش Traffic Rules از پنل مدیریتی Kerio Control می شویم و یک Rules ای را بدین شرح ایجاد می کنیم:

Name Rules = DNS

Source = 192.168.100.2

Destination = Any

Service = DNS

Action = Allow

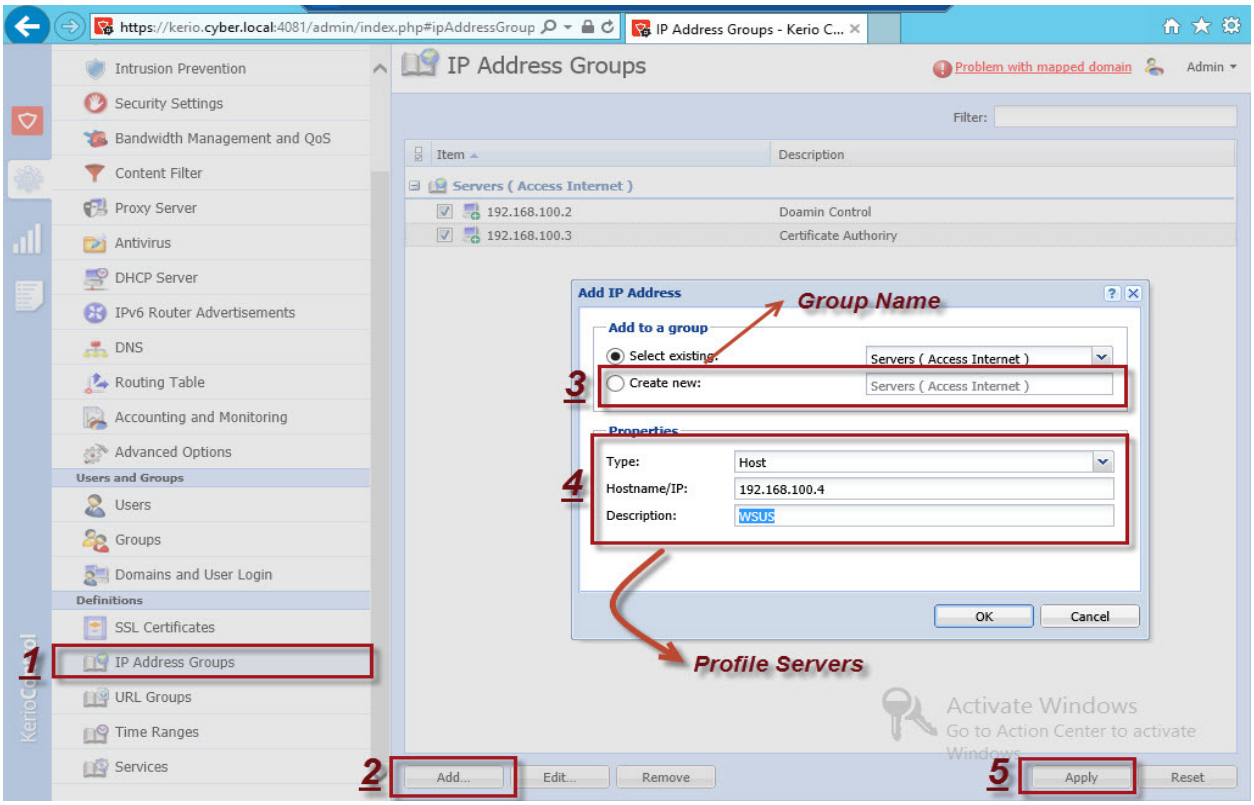
Translation = NAT Balancing per Host

بوسیله این Rules این اجازه را به سرور PDC با IP آدرس 192.168.100.2 می دهیم که فقط با DNS سرورهای Public در ارتباط باشند و نه چیزه دیگر، یعنی به عبارتی سرور PDC این اجازه را خواهد داشت که درخواستهای DNS ای سرورهای داخلی و کلاینت ها را به DNS سرورهای Public فرستاده و جوابهای مورد نظر را دریافت کند.

یک نکته کوچک : اولویت اعمال Rules ها از بالا به پایین می باشد.

در قسمت Traffic Rules همانا Rulesای به نام Internet Access (NAT) وجود دارد ، کار این Rules اینترنت دار کردن تمامی سرورها و کلاینت های شبکه داخلی می باشد. اما ایرادی که این Rules دارد غیر مدیریتی آن می باشد، بنابراین برای اینکه تمامی سرورهای شبکه داخلی را اینترنت دار کنیم یک Rules مجزا برای اینکار در نظر می گیریم. در اول کار یک گروهی ایجاد می کنیم و تمامی سرورها را به داخل این گروه وارد می کنیم، سپس توسط Rules مورد نظر فقط این گروه را اینترنت دار می کنیم که با این عمل باعث می شود که فقط سرورهایی که در داخل این گروه هستند اینترنت دار می شوند.

نحوه وارد کردن سرورها به یک گروه بدین صورت می باشد که اول وارد بخش IP Address Groups از پنل مدیریتی Kerio Control می شویم بعد در صفحه مربوطه اش Add را کلیک می کنیم سپس در بخش پایینی مشخصات و IP سرور مورد نظرمان را وارد می کنیم. مشخصات و IP سرورهای بعدی را نیز به همین منوال وارد گروه می کنیم. مراحل کار در شکل صفحه بعد نمایش داده شده است.



حالا نوبت به ایجاد Rules مورد نظر رسیده که بدین صورت می باشد:

Rules Name = Internet Access For Servers

Source = Servers (Internet Access)

Destination = Any

Service = FTP, HTTP, HTTPS

Action = Allow

Translation = NAT (Balancing per Host)

توسط این Rules این امکان ایجاد می شود که تمامی سرورهای داخل گروه Servers(Internet Access) فقط از حیث پروتکلهای FTP, HTTP, HTTPS اینترنت دار می شوند.

دو Rules ای که تا اینجا ایجاد کرده ایم یعنی Rules ای که بوسیله آن به DNS سرورهای Public دسترسی داریم و Rules دیگری که بوسیله آن تمامی سرورهای داخلی اینترنت دار شده اند می باشند، Rules های مختص Kerio Control نمی باشند بلکه جزء Rules های پیشفرض هر Firewall می باشند و باید اصولا در آنها باشند.

حالا نوبت به اینترنت دار کردن کلاینت ها رسیده، اینترنت دار کردن کلاینت ها یا همان کاربران داخل شبکه به حالت کلی کاری غیره اصولی و غیره مدیریت شده می باشد چرا که اگر این کار انجام پذیرد کاربران قادرند بصورت نامحدود و غیره مدیریت شده از اینترنت استفاده کنند به همین دلیل با انجام تنظیمات مشخص شده و اعمال آنها بوسیله Rules های مورد نظر می توانیم به کاربران یک اینترنت مدیریت شده و کنترل شده بدهیم. در زیر مواردی از تنظیماتی که می خواهیم به کاربران اعمال کنیم را ذکر می کنیم:

1) دسترسی به اینترنت در بازه های زمانی خاص

2) تعیین سرعت دسترسی به اینترنت

3) عدم دسترسی کاربران به URL های خاص

4) عدم دسترسی به Forbidden Words

5) تعیین میزان Upload و Download

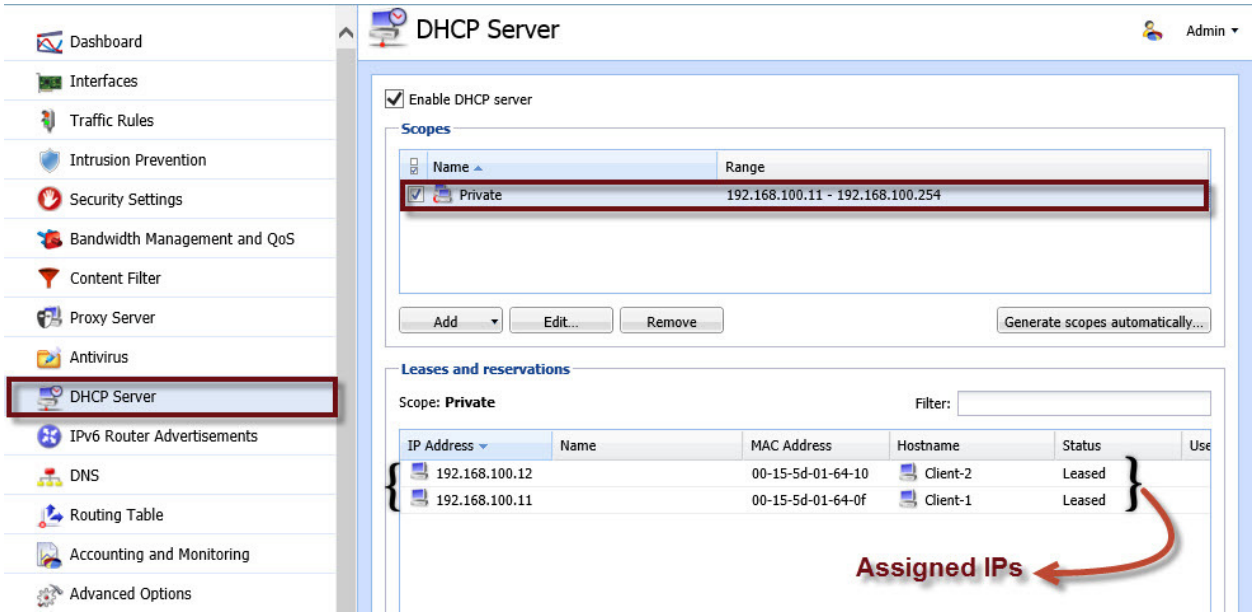
و بسیاری از موارد دیگر ...

که می توان توسط Kerio Control بر روی کلاینت ها یا همان کاربران اعمال نمود، در این مقاله چند مورد از تنظیمات گفته شده را پیاده سازی خواهیم کرد.

قبل از اینکه به کلاینت ها با توجه به تنظیمات در Rules های مورد نظر اینترنت بدهیم یک کاری هست که باید انجام بدهیم، کار مورد نظر دادن IP به کلاینت ها می باشد برای اینکار دو حالت وجود دارد، یکی اینکه در داخل

PDC همانا DHCP Server راه اندازی کنیم و یا اینکه از DHCP Server خود Kerio Control استفاده کنیم که ما حالت دوم را انتخاب می کنیم یعنی از DHCP Server خود Kerio Control استفاده می کنیم.

برای این منظور وارد DHCP Server از پنل مدیریتی Kerio Control می شویم و در صفحه مربوطه اش از قسمت Scope همانا Interface Private خود Kerio Control را مشاهده خواهیم کرد، چونکه تنظیمات TCP/IP کلاینت ها بر روی Automatically می باشد به همین دلیل اگر بر روی Private کلیک کنیم خواهیم دید که Kerio Control بصورت اتوماتیک به کلاینت ها IP داده و IP های اختصاص داده شده در قسمت Leases and Reservations نمایش داده می شود، اگر در داخل کلاینت ها نیز به قسمت TCP/IP وارد بشویم IP های اختصاص داده شده را مشاهده خواهیم کرد.



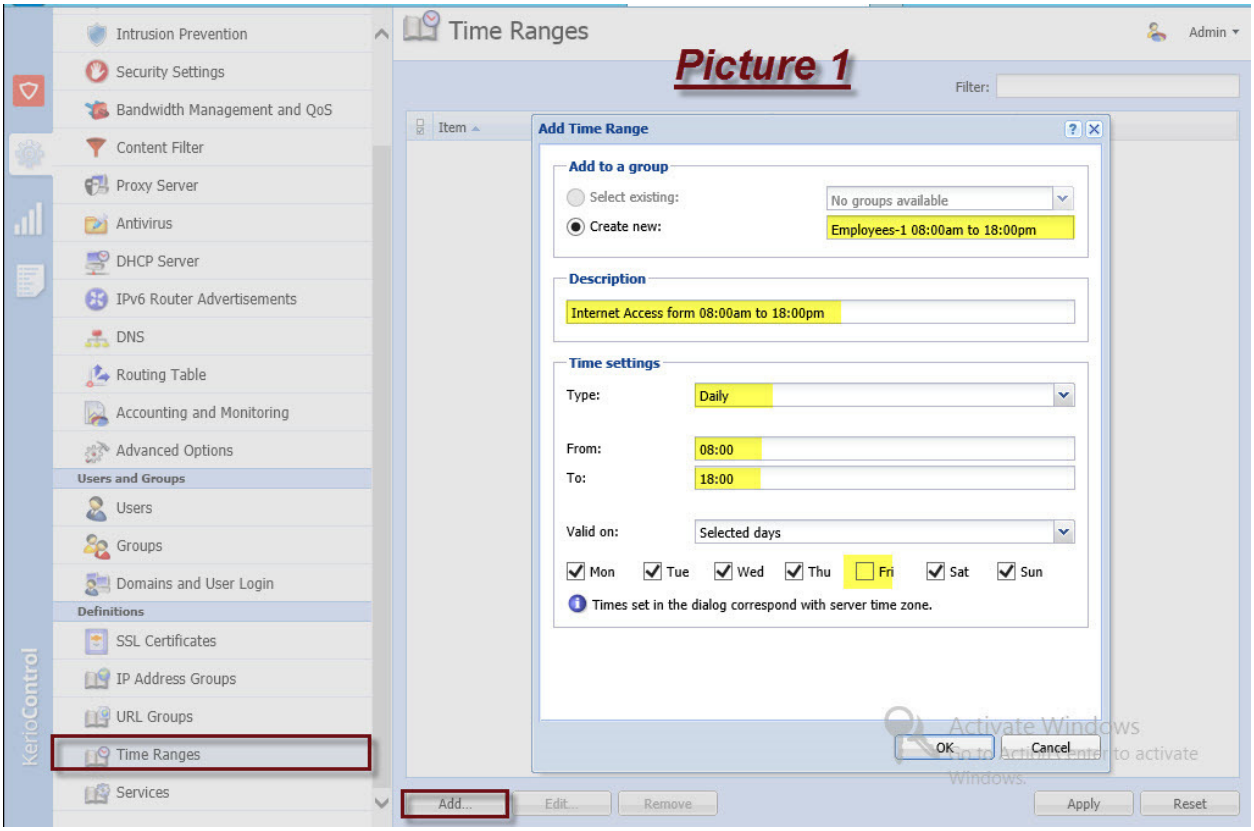
این نکته را باید در نظر داشته باشید که آدرس DNS در Interface Private همانا IP دستگاه PDC یعنی 192.168.100.2 باید باشد که این IP آدرس به کلاینت ها اعمال خواهد شد.

بعد از انجام تنظیمات مربوط به DHCP و گرفتن IP توسط کلاینت ها نوبت به اعمال تنظیمات مربوط جهت اینترنت دار کردن کلاینت ها رسیده، در این سناریو می خواهیم کلاینت ها دربازه های زمانی متفاوت اینترنت دار بشوند مثلاً زمانبندی را اینطوری در نظر می گیریم که یک شرکت دارای دو شیفت کاری صبح و شب می باشد

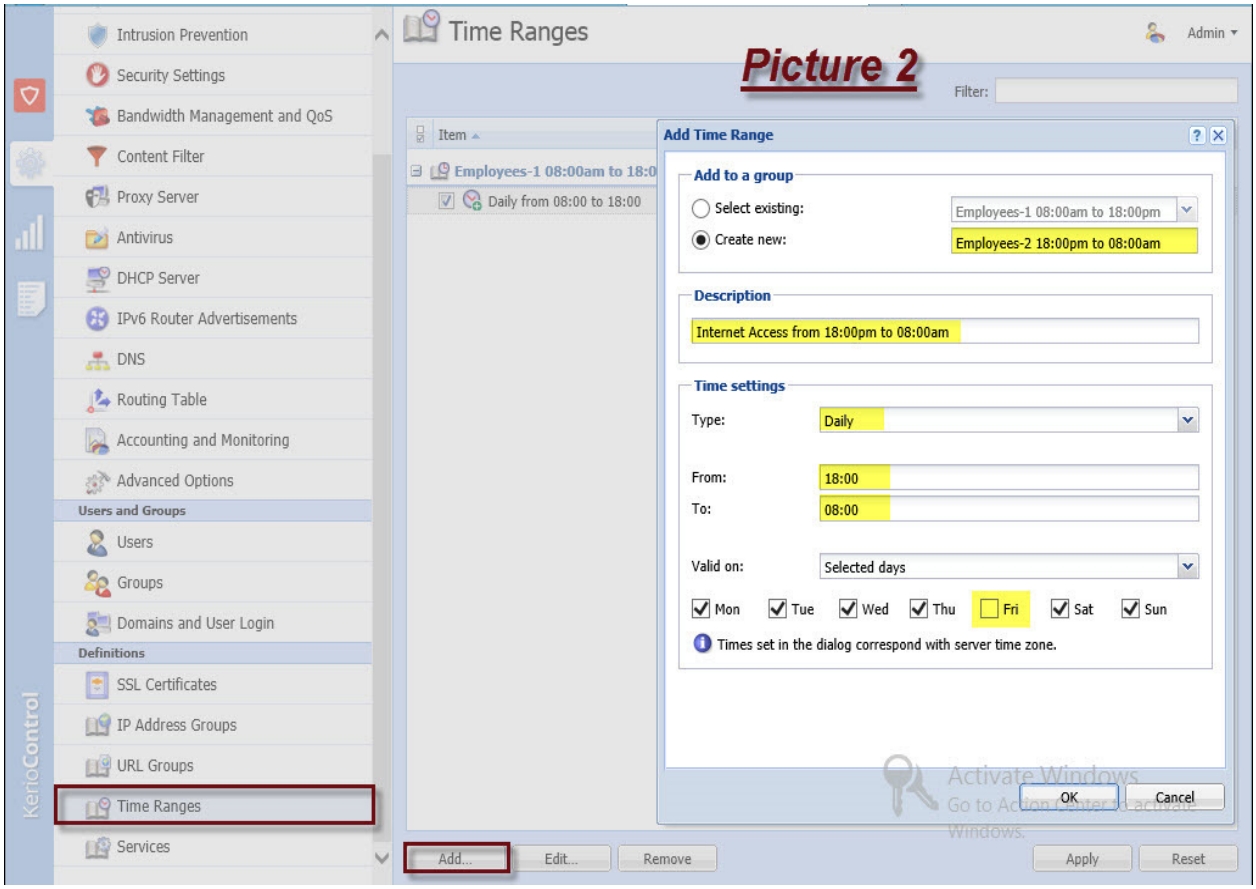
یعنی شیفت صبح از ساعت 08:00 am to 18:00 pm می باشد و شیفت شب از ساعت 18:00 pm to 08:00 am می باشد، در مرحله اول بازه های زمانی ذکر شده را ایجاد می کنیم سپس این بازه ها را در Rules های مربوطه اش بکار می بریم.

جهت ایجاد بازه های زمانی ذکر شده وارد Time Ranges از پنل مدیریتی Kerio Control می شویم سپس روی Add کلیک کرده و مشخصات را وارد می کنیم در Create New اسمی را برای بازه زمانی مورد نظر وارد می کنیم مثلاً با توجه به سناریوی مورد بحث مقدار 08:00 am to 18:00 pm را وارد می کنیم و در قسمت Type مشخص می کنیم که آیا این بازه زمانی روزانه یا هفتگی و یا بصورت مطلق اعمال شود؟ در قسمت From مقدار 08:00 am و در قسمت to مقدار 18:00 pm را می نویسیم و در قسمت Valid on فقط تیک Firday رو برمی داریم چونکه مثلا نمی خواهیم روزهای جمعه اینترنت داشته باشند. برای شیفت بعدی نیز عیناً به همین صورت عمل می کنیم ولی در بازه زمانی 18:00 pm to 08:00 am انجام می گیرد. توضیحات در شکل زیر نشان داده شده هست.

شکل اول مربوطه به بازه زمانی 08:00 am to 18:00 pm می باشد.



شکل دوم مربوط به بازه زمانی 18:00 pm to 08:00 am می باشد.



بازه های زمانی برای دو شیفت کاری صبح ها و شب ها مشخص شد. حال باید Users ها و Groups های مربوطه نیز ایجاد شود یعنی یک گروه برای شیفت صبح و یک گروه نیز برای شیفت شب درست می کنیم و در داخل آنها Users های مربوطه شان را نیز ایجاد می کنیم، هدف از ایجاد این یوزرها و گروهها مشخص کردن اینکه چه کسانی از این بازه های زمانی که مشخص کردیم استفاده کنند.

این تنظیمات در داخل سرور PDC قسمت Active Directory Users and Computers ایجاد می شود، شرح کار بدین صورت می باشد که یک OU ای به نام Employees ایجاد می کنیم و درداخل آن دو OU دیگر به نامهای Computers و Users ایجاد می کنیم سپس در قسمت Users دو یوزر به نامهای User1 و User2 را ایجاد می کنیم. گروههای E1 و E2 را در داخل OU Employees ایجاد کرده و یوزرهای مربوطه شان یعنی User1 و User2 را به داخل این گروهها وارد می کنیم.

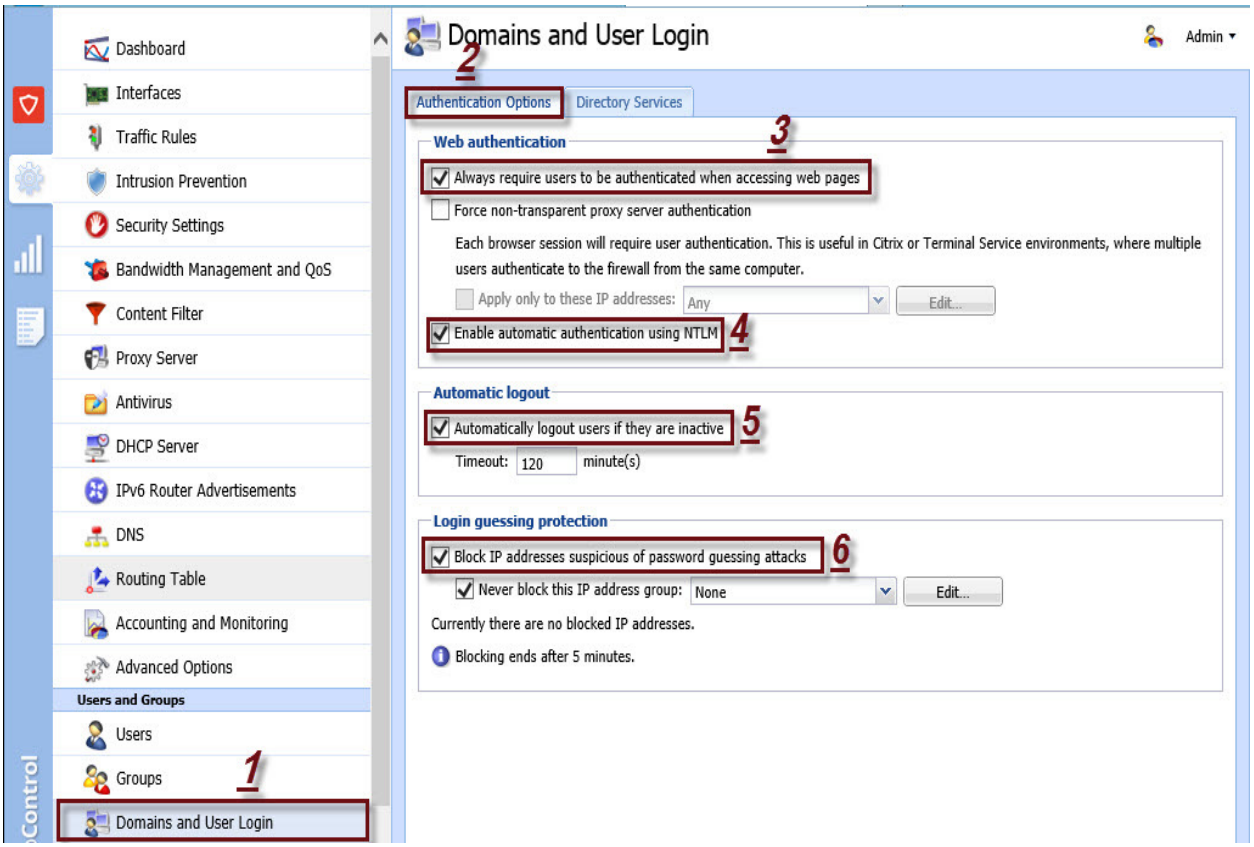
از قسمت Domain and Users Login وارد تب Authentication Options می شویم و در قسمت Web Authentication تیک گزینه Always Require Users to be Authenticated When Accessing Web Page را می زنیم، علت انتخاب این گزینه این هست که سیستم درخواستهای کاربران برای دسترسی به صفحات وب را مجاز دانسته و اجازه دسترسی را به آنها بدهد، یعنی به عبارتی سیستم بعد از شناسایی اجازه دسترسی را به کاربران بدهد. و همچنین تیک گزینه Enable Automatic Authentication Using NTLM را هم می زنیم بدین علت که User هایی مربوط به کاربران در دستگاه Domain ایجاد شده و کاربران در هر بار Login کردن از پشت سیستم شان باید در ارتباطشان با User های مربوط به خودشان در Domain ایجاد شود دستگاه Kerio Control در هر بار ارتباط اینها درخواست Username/Password خواهد کرد، با انتخاب این گزینه دستگاه Kerio Control در هر بار Login کردن کاربران را بصورت اتوماتیک شناسایی کرده و دیگر Username/Password ای درخواست نخواهد کرد، منظور این هست که در ارتباط اول فقط Username/Password را دریافت خواهد کرد ولی در ارتباطهای بعدی شناسایی بصورت اتوماتیک خواهد بود.

در قسمت Automatic Logout مشخص می کنیم که اگر کاربری مثلاً 120 دقیقه غیر فعال بود یعنی هیچ فعالیتی در ارتباطات خودش انجام نداد بصورت اتوماتیک از سیستم Logout شود.

در قسمت Login guessing protection تیک گزینه های:

- Block IP Address Suspicious of Password guessing attacks
- Never Block this IP Address Group

را می زنیم، با انتخاب گزینه اولی باعث می شویم که هر IP آدرسی که در شبکه مشکوک شناخته می شود از حیث عملیات خرابکارانه Block می شود و در گزینه دومی می توانیم گروهی از IP آدرسهایی که نمی خواهیم Block شوند را در این قسمت به سیستم بشناسانیم.



بعد از انجام تنظیمات نوبت به ایجاد Rules های مربوطه اش رسیده یعنی Rules هایی را ایجاد می کنیم که بوسیله آنها اعضای گروههای E1 و E2 اینترنت دار می شوند.

Rules مربوط به اینترنت دار کردن اعضای گروه E1 :

Rules Name = Internet Access for E1

Source = E1@cyber.local

Destination = Internet Interface

Services = HTTP , HTTPS , FTP

Action = Allow

Translation = NAT (Balancing per Host)

Valid Time = Employees-1 (08:00am to 18:00pm)

توسط این Rules اعضای گروه E1 در بازه زمانی 8 صبح تا 6 بعد از ظهر اینترنت دار می شوند.

همانند Rules بالا برای اعضای گروه E2 نیز ایجاد می کنیم:

Rules Name = Internet Access for E2

Source = E2@cyber.local

Destination = Internet Interface

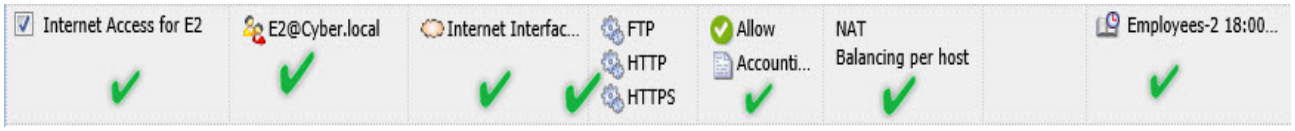
Services = HTTP , HTTPS , FTP

Action = Allow

Translation = NAT (Balancing per Host)

Valid Time = Employees-2 (18:00pm to 08:00am)

توسط این Rules تمامی اعضای گروه E2 در بازه زمانی 6 عصر تا 8 صبح اینترنت دار می شوند.



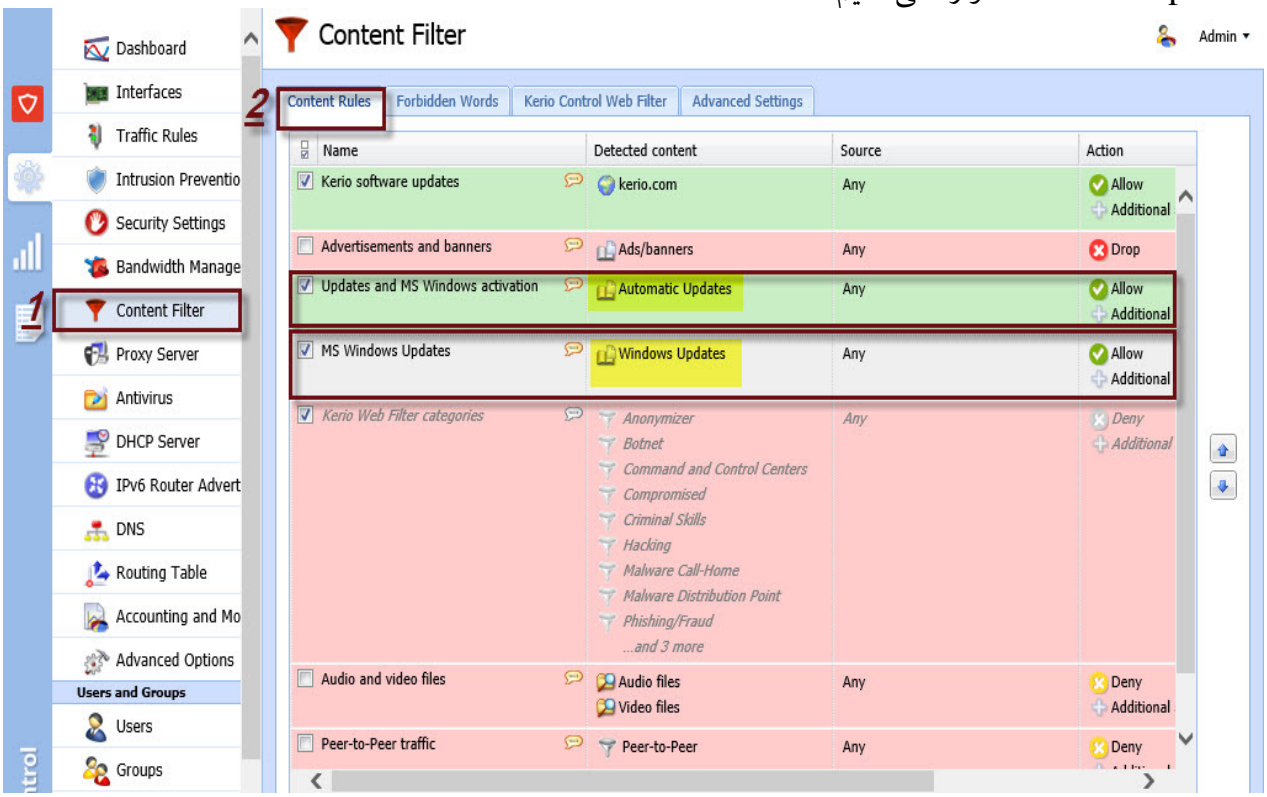
به صورت کلی تمامی ترافیکهایی که در شبکه در حال حرکت هستند توسط فایروال Kerio Control بررسی و شناسایی می شود حال بر حسب نیاز مواردی پیش می آید که با URL هایی مواجه می شویم که نیاز به شناسایی در آن دیده نمی شود به همین دلیل به نوعی باید به Kerio Control بشناسانیم که این URL ها را شناسایی نکند، بطور مثال URL های مربوط به Update که در حالت کلی نیاز نیست که Kerio Control این URL ها را شناسایی کند. تمامی URL های مربوط به Update ویندوزها در دو گروه Automatic Updates و Windows Updates قرار دارند که آنها را می توانید در قسمت URL Groups مشاهده کنید.

برای اینکه به Automatic Updates و Windows Updates امکان عدم شناسایی در Kerio Control را بدهیم بدین صورت عمل می کنیم:

وارد Content Filter و تب Content Rules می شویم در این قسمت باید Rules هایی ایجاد شود که بوسیله آنها موارد ذکر شده قابل شناسایی نباشد. بصورت پیش فرض Rules مربوط به عدم شناسایی Automatic Updates با نام Update and MS Windows Activation هست، بر روی فیلد Action این Rules کلیک کرده تا صفحه مربوطه اش باز شود در صفحه مربوطه حتماً باید تیک گزینه Do not Require Authentication زده شود چونکه در این صورت عملیات عدم شناسایی صورت می گیرد همچنین تیک گزینه های زیر را نیز می زنیم:

- Skip Forbidden Words Filtering
- Skip Antivirus Scanning
- Log the Traffic

عین همین حالتی که برای عدم شناسایی Automatic Updates انجام دادیم Rules ای را نیز برای عدم شناسایی Windows Updates در اینجا ایجاد می کنیم با این تفاوت که در قسمت Detected Content همانا Windows Updates وارد می کنیم.



Content Rules دارای امکانات دیگری نیز می باشد بدین صورت که با ایجاد Rules هایی و انجام تنظیماتی در قسمت Detected Content و Source می توانیم موارد بسیاری از عملیات فیلترینگ را پیاده سازی کنیم، مثلاً می خواهیم تمامی کاربران موجود در شبکه کلاً به سایتهایی که دارای آهنگ و ویدئو هستند دسترسی نداشته باشند برای این کار بصورت پیش فرض Rules ای در این قسمت هست که بدین صورت می باشد:

Name Rules = Audio and Video Files

Detected Content = Audio Files , Video Files

Source = Any

Action = Deny

که توسط این Rules تمامی کاربران شبکه به سایتهایی که محتویا تشان Video و Audio باشد دسترسی نخواهند داشت.

اگر در قسمت Detected Content کلیک کنیم صفحه ای باز می شود که در قسمت Add آن موارد زیر وجود دارد :

- Applications and web Categories
- File Name
- URL and Hostname
- URL Groups

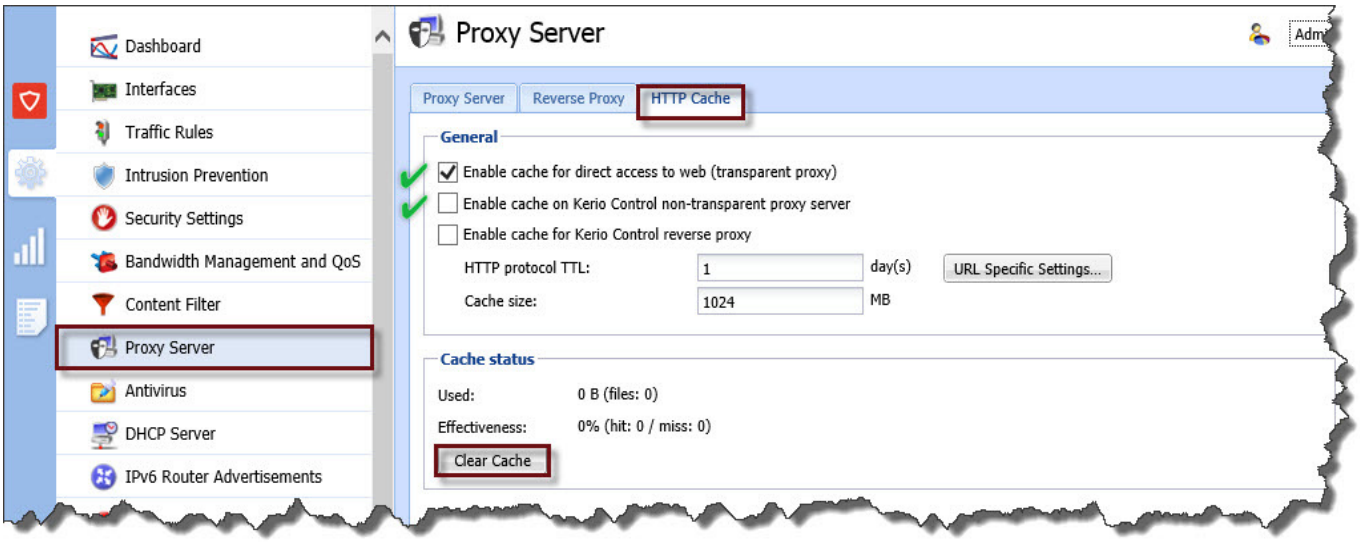
توسط جزئیات موجود در این قسمت می توانیم عملیات فیلترینگ بر حسب نیاز شبکه را پیاده سازی کنیم.

در قسمت Source به سیستم اعلام می کنیم که این عملیات فیلترینگ به چه کسانی اعمال خواهند شد.

بحث Cache در Kerio Control به دو حالت Transparent و non-transparent می باشد، در حالت Transparent از Proxy استفاده نمی کنیم ولی در حالت non-transparent از Proxy استفاده می کنیم ولی چونکه در حالت کلی تنظیمات Proxy در بیشتر مرورگرها متفاوت هست به همین دلیل در فاز اول از حالت Transparent استفاده می کنیم.

نکته : در حالتی که از Proxy استفاده می کنیم آدرس آن با توجه به سناریوی ما https://kerio.cyber.local:3128 خواهد بود.

برای Cache کردن مقدار TTL و Size می توانیم تعریف کنیم همچنین لیستی از URL هایی را که می خواهیم Cache شوند را در قسمت URL Specific Setting وارد می کنیم.

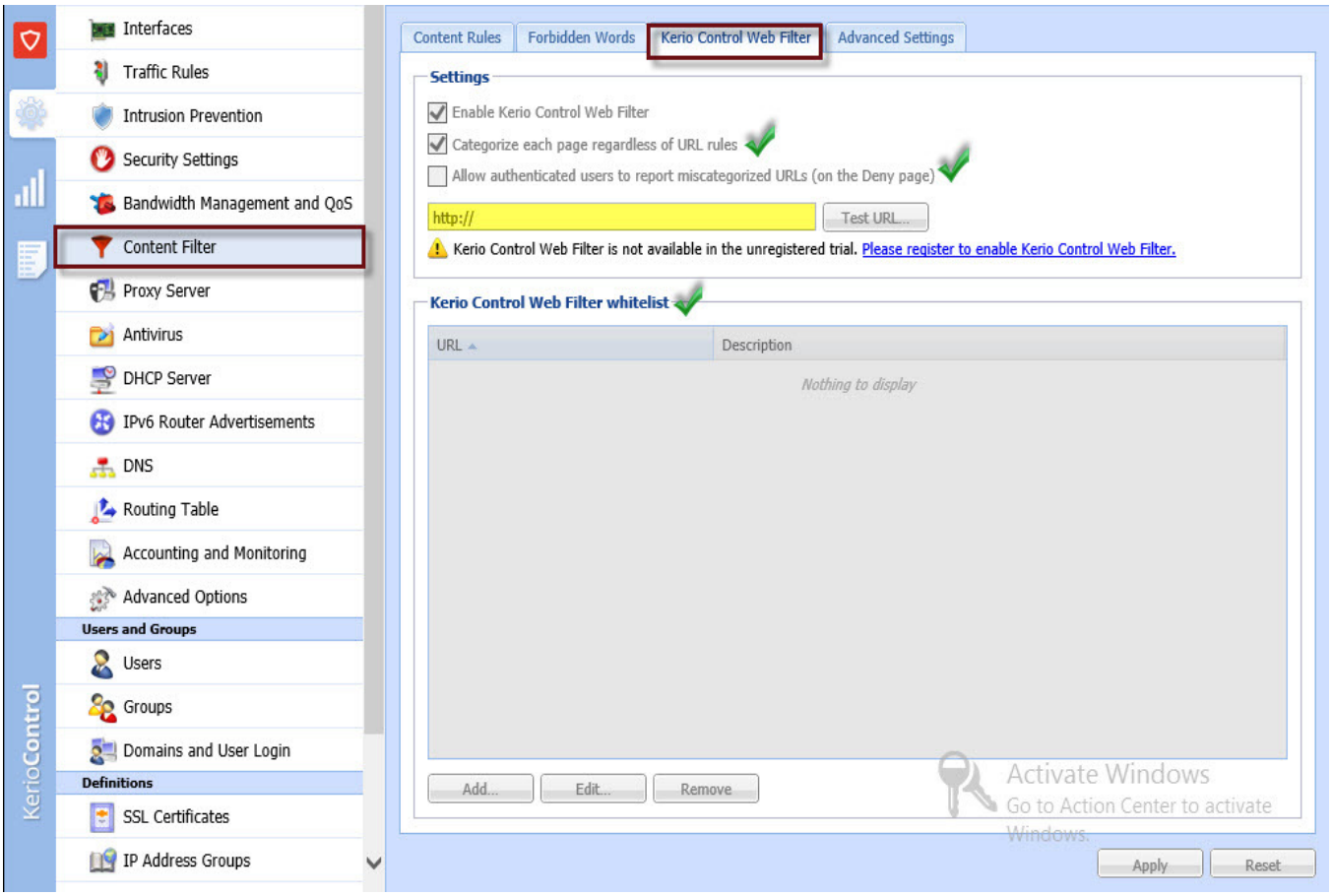


در قسمت Content Filter بخشی به نام Forbidden Word قرار دارد، توسط این قسمت می توانیم آن دسته از لغاتی را که می خواهیم جزء لغات ممنوعه باشند و کاربران نتوانند به نتایج جستجوی حاصل از آنها دست یابند وارد می کنیم، مثلاً: Cracks , Hack , Serial , Warez و ...

در قسمت Setting گزینه Deny Pages if their Weight Reaches قرار دارد که در TextBox مقابلش بصورت پیش فرض مقدارش 70 هست این بدان معنی هست که بر اساس امتیاز هایی که لغات دارند اگر در WebPage ای لغت Serial مثلاً 7 بار تکرار شود و بر این اساس که امتیاز لغت Serial=10 هست پس مجموعش 70 می شود که اگر این مقدار باشد WebPage مربوطه Deny و غیر قابل دسترسی خواهد شد. قابل ذکر هست که مقدار 70 قابل تغییر می باشد.

تب دیگری در قسمت Content Filter همانا Kerio Control Web Filter هست در این قسمت می توانیم تمامی صفحات جستجو شده را بر اساس موضوع صفحات بصورت یک دسته بندی منظم درآورده و گزارش دهیم که این عملیات با زدن تیک گزینه Ctegorize each Page Regardless of URL Rules انجام می پذیرد. همچنین اگر می خواهیم بدانیم که سیستم چه Header هایی برای موضوعات در نظر می گیرد کافی هست که URL مورد نظر را در قسمت مربوط به گزینه Allow Authenticated Users to Report miscategorized URLs (on the Deny Page) وارد کنیم و بعد روی Test URL کلیک کنیم تا ببینیم که نتیجه حاصل چه می شود.

در قسمت Kerio Control Web Filter Whitlist اگر به زبان ساده بگوییم می توانیم لیستی از URL هایی که می خواهیم تا سیستم به آنها کاری نداشته باشد را وارد می کنیم.

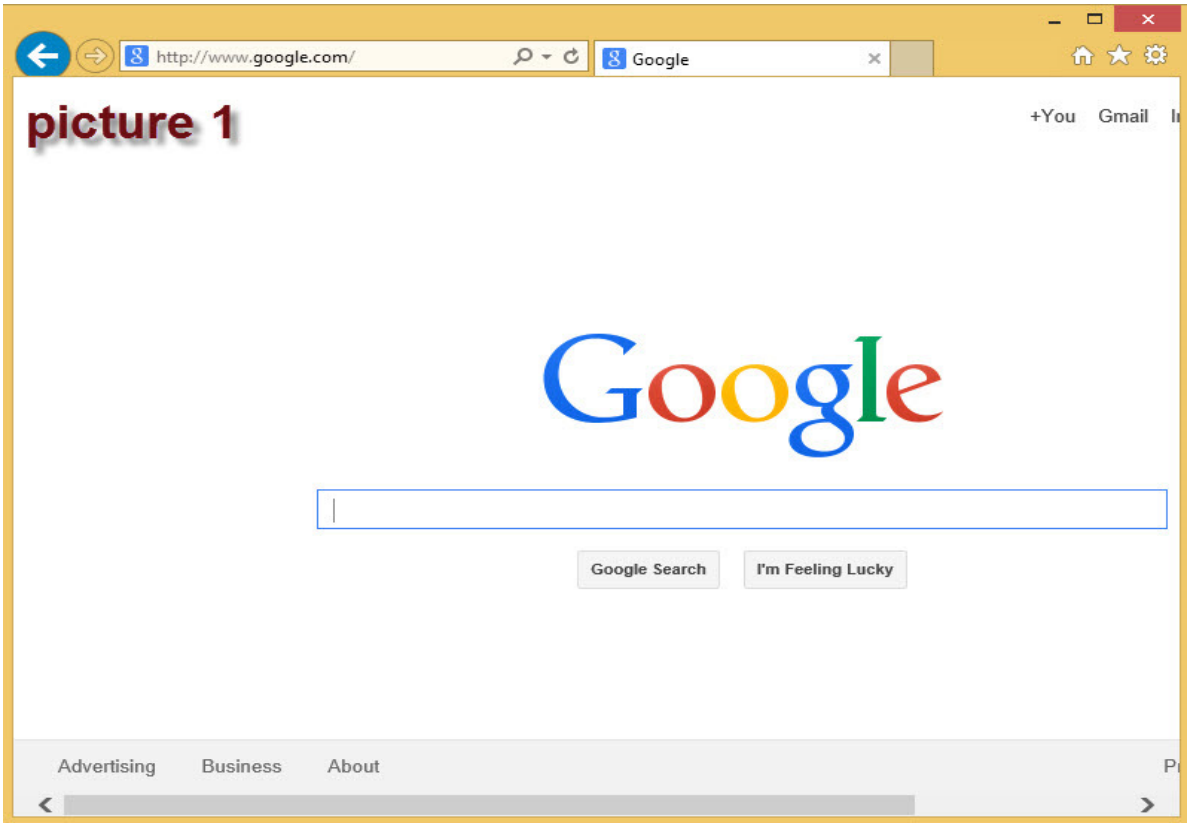


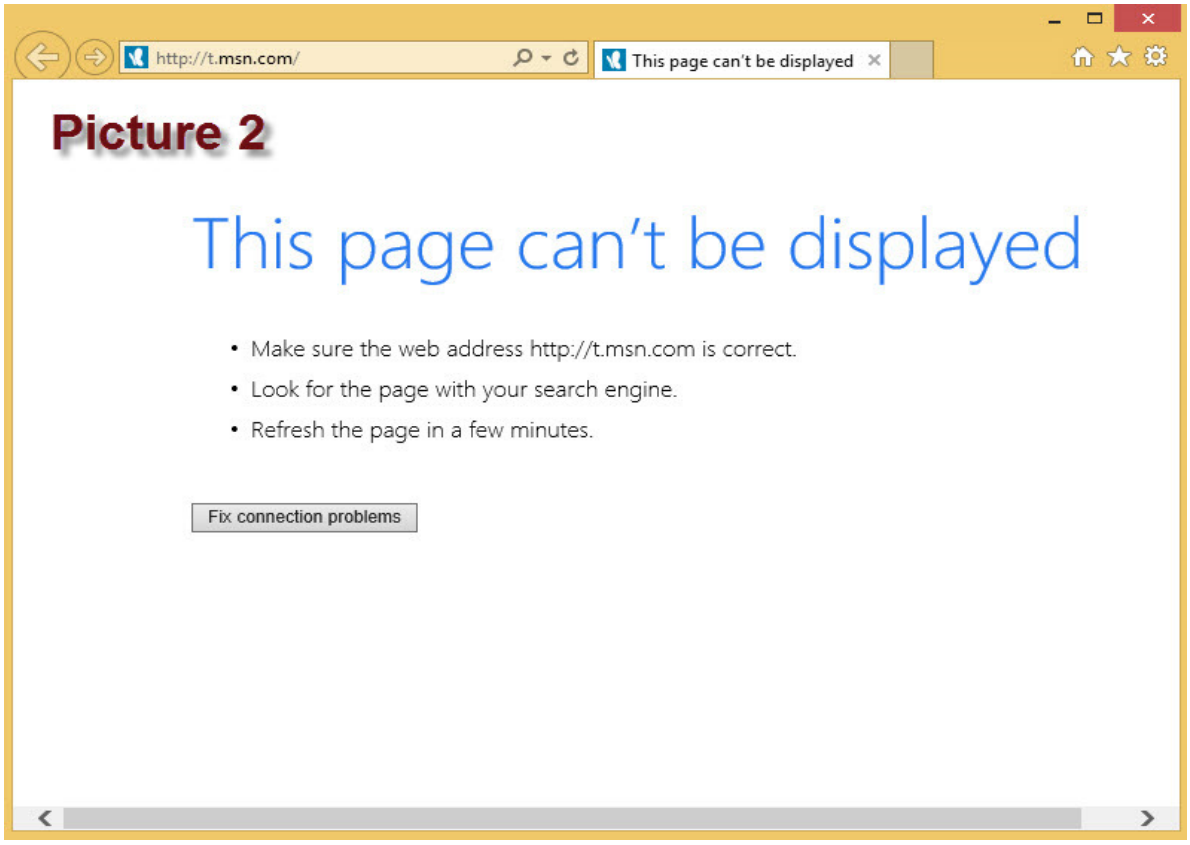
در داخل Domain یوزرهایی را برای کلاینت ها ایجاد کرده ایم و با انجام تنظیماتی هدفمان این هست که اگر کاربری با Domain User ای به سیستم Login کند دارای اینترنت باشد. حال نوبت به انجام این کار رسیده یعنی سیستم ها را Join to Domain می کنیم و با Domain User ها به سیستم ها Login می کنیم تا بصورت عملی مشاهده کنیم که سیستم ها با توجه به بازه های زمانی که در خود Kerio Control ایجاد کرده ایم آیا اینترنت دار می شوند؟

تمامی مشخصات مربوط به IP آدرس ها و DNS ها توسط DHCP Server خود Kerio Control ایجاد و به کلاینت ها اعمال شده است، پس به راحتی عملیات Join را پیش می بریم.

در صفحه بعد شکلهای مربوطه را خواهیم دید یعنی بدین صورت که با user1 پشت سیستمی Login کرده ام که ساعت سیستم اش جزء بازه زمانی 08:00am to 18:00pm می باشد پس سیستم مورد نظر با توجه با بازه زمانی user اش اینترنت دار خواهد بود، ولی زمانی که با user2 به سیستم Login کنم با توجه به اینکه ساعت سیستم جزء بازه زمانی 18:00pm to 08:00am نمی باشد پس user2 روی سیستم ام اینترنت دار نخواهد بود.

شکل 1 مربوط به حالت اول وشکل 2 نیز مربوط به حالت دوم می باشد.





Bandwidth Management (مدیریت پهنای باند) :

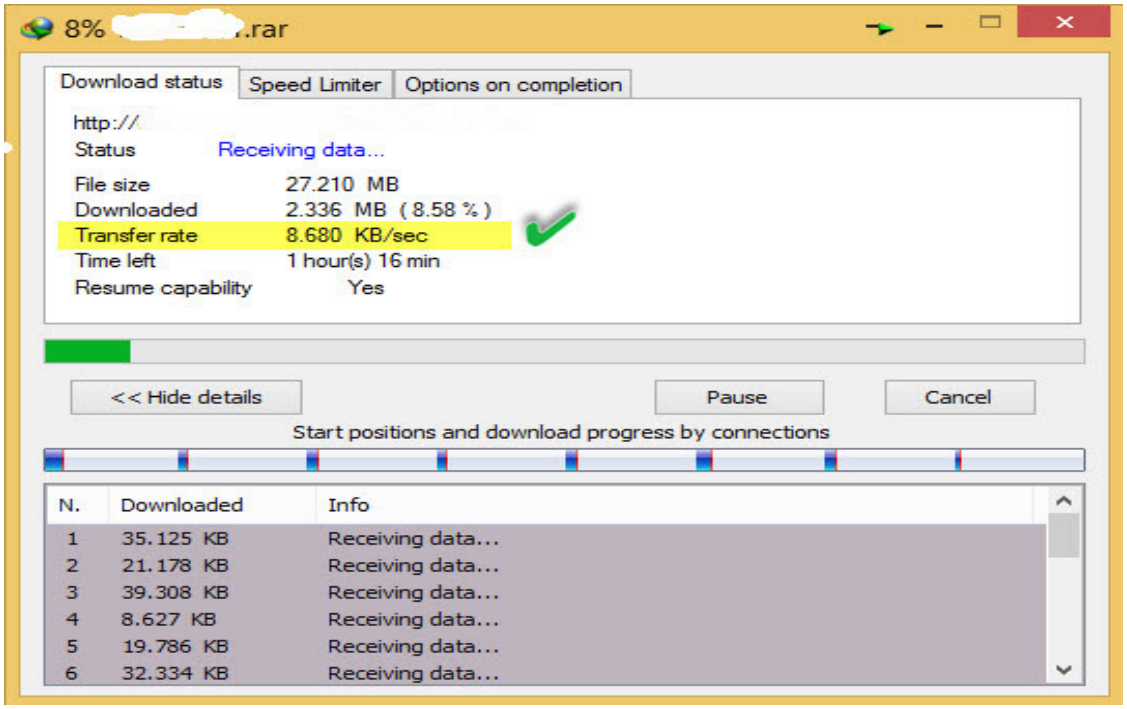
Kerio Control قسمتی دارد که بوسیله آن می توانیم یک مدیریت کلی از حیث میزان Download و Upload داشته باشیم یعنی می توانیم برای کاربران میزان Download و Upload تعیین کنیم.

همه این موارد را با ایجاد Rules هایی در خود Bandwidth Management صورت می گیرد، در بخش ایجاد Rules ها قسمتی به نام Traffic هست که دارای بخشهای مختلفی می باشد که به مرور تمامی این موارد به صورت کامل توضیح داده خواهد شد.

این قسمت را با توجه به سناریوی خودمان پیش می بریم بدین صورت که دو User در دو گروه متفاوت ایجاد کردیم، حال می خواهیم به این دو گروه میزان سرعت از حیث Download و Upload تعیین کنیم . برای این منظور در قسمت Bandwidth Management Rules همانا Rules ای به نام E1 Restrictions ایجاد می کنیم روی فیلد مربوط به Traffic کلیک و از صفحه باز شده روی Add کلیک کرده و گزینه Selected Users / Groups را انتخاب می کنیم، دوباره از صفحه باز شده از قسمت Domain دامین مورد نظر را انتخاب می کنیم تا یوزرها و گروههای مربوطه اش نمایش داده شوند بعد از میان آنها گروه E1 که مد نظر ما می باشد را انتخاب می کنیم (گروه E1 شامل User1 می باشد) و بعد OK را می زنیم و وارد فیلد Download می شویم در این قسمت دو حالت وجود دارد یکی Reserve at Least و دیگری Do not Exceed که اولی میزان حداقلی ذخیره را تعیین می کند و دیگری حدّ مجاز را مشخص می کند که در این حالت ما برای Download قسمت Do not Exceed مقدار 64 Kbit/s را وارد می کنیم و برای Upload نیز برای مقدار 32 Kbit/s وارد می کنیم این مقادیر برای تمامی اعضای گروه E1 می باشد مثلاً اگر اعضای این گروه ده نفر باشد این مقدار بین ده نفر تقسیم می شود.

اگر بخواهیم میزان واقعی سرعت دانلود را محاسبه کنیم مقدار تخصیص یافته را بر 8 تقسیم می کنیم که حاصل 8 می شود یعنی میزان Dawnload rate برای برداشتن یک فایل 8 Kbit/s می باشد.

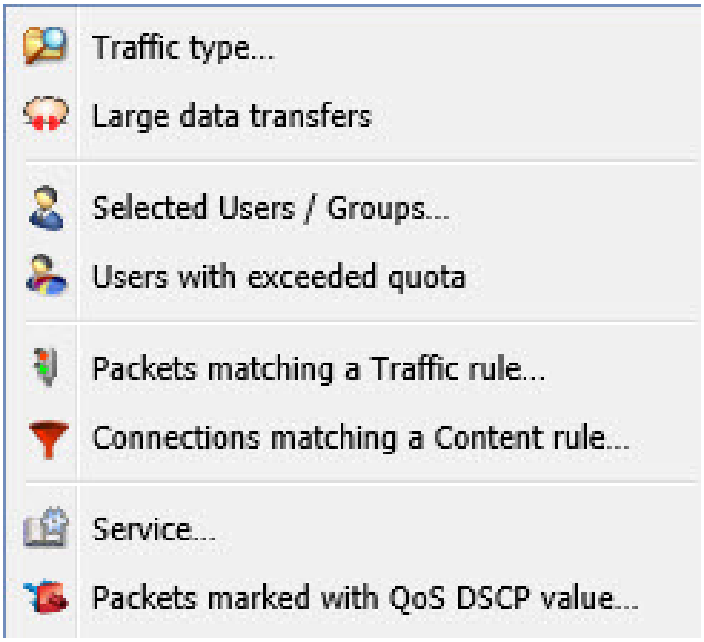
شکل زیر مربوط به تست این حالت می باشد.



بعد از ارائه مباحث مربوط به ایجاد محدودیت دانلود و آپلود برای کاربران نوبت به ارائه جزئیات کلی تر نسبت به موضوع مدیریت پهنای باند رسیده.

توضیح این قسمت با توجه موارد موجود درفیلد Traffic واقع در قسمت Bandwidth Management and QoS می باشد.

اگر در فیلد مربوط کلیک کنیم صفحه ای باز می شود که اگر در آن بر روی Add کلیک کنیم با صفحه ای مواجه می شویم که شامل گزینه های متفاوتی می باشد این گزینه ها امکاناتی برای ما ایجاد می کنند که بوسیله آنها بتوانیم یک محدودیت سلیقه ای و دلخواه درشبکه ایجاد کنیم.



دوستان اگر توجه کرده باشید در اشتراک اینترنتی که استفاده می کنیم یک سری محدودیتهایی وجود دارد، مثلاْ در هنگام دانلود بعضی از فایلها و ویدیوهای خاص با کاهش محسوس سرعت اینترنت مواجه می شویم و یا هنگام دسترسی مان به بعضی از پروتکلها و سایتها نیز سرعت به طرز چشم گیری کاهش می یابد و از همه مهمتر هنگام استفاده از فیلترشکن یا VPN هم سرعت کاهش می یاد و خیلی از جزئیاتی که تقریباْ همه آنها بوسیله موارد موجود در این صفحه ایجاد می شوند. موارد موجود در این صفحه را بطور مختصر تشریح می کنیم.

اگر روی Traffic Type کلیک کنیم صفحه ای باز می شود که در آن می توانیم بر اساس نوع ترافیکهای موجود محدودیتهایی از حیث سرعت دانلود و آپلود ایجاد کنیم، مثلاْ بدین صورت که اگر در داخل شبکه ترافیکهایی از نوع Email ، FTP ، P2P و یا از همه مهمتر VPN مشاهده شد میزان سرعت کاهش یابد.

توسط گزینه Large Data Transfer می توانیم این محدودیت را ایجاد کنیم که اگر کاربری در شبکه بر فرض مثال داده ای که حجمش بیشتر از 1G هست را دانلود کند با کاهش شدید سرعت مواجه شود.

توسط گزینه ... Selected User / Groups می توانیم میزان دانلود یا آپلود برای گروهها و یوزرها ایجاد کنیم.

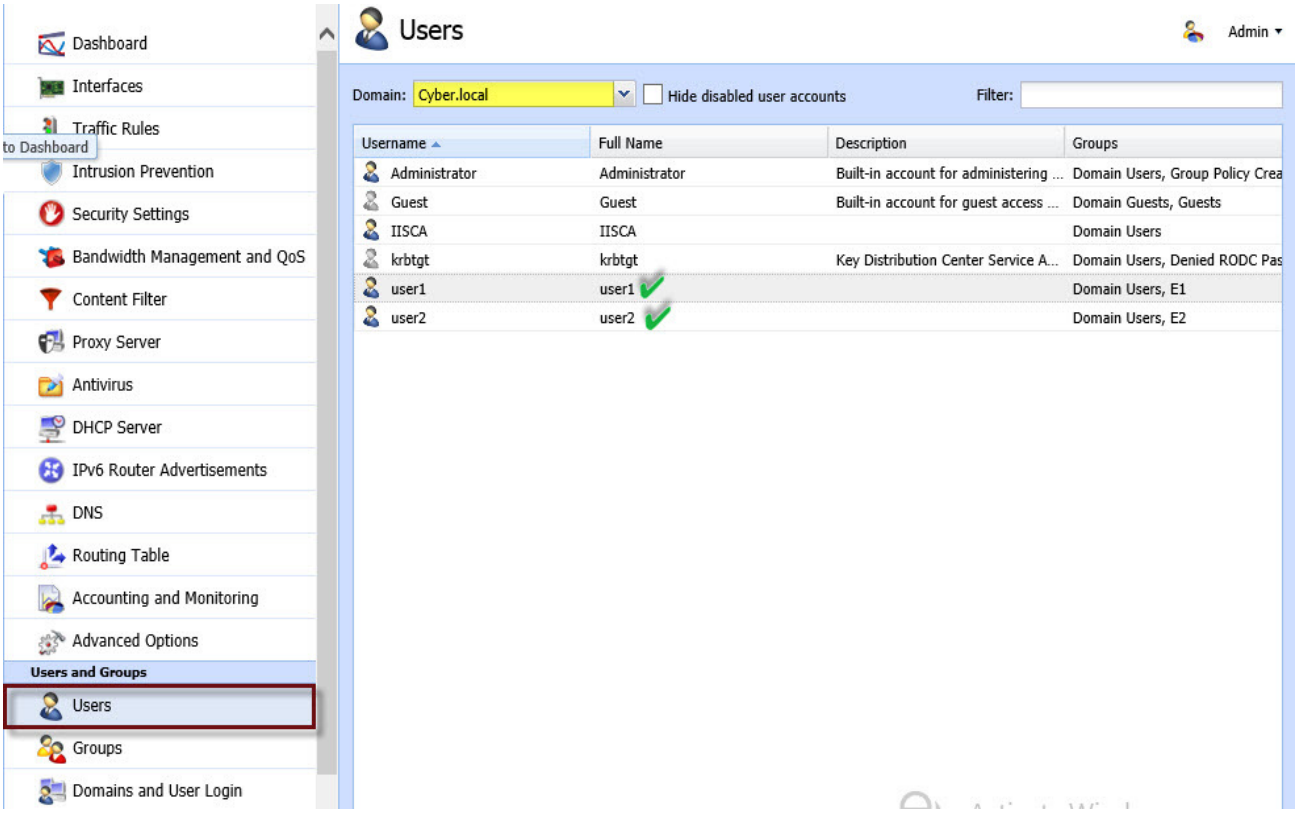
برای هر کاربر میزان سهمیه دانلود و آپلود و میزان ساعات استفاده از اینترنت در طول شبانه روز یا هفته یا ماه در نظر می گیریم، اگر کاربری از این میزان سهمیه خود تجاوز کند می توانیم با کاهش سرعت با آن مقابله کنیم که این عملیات را در قسمت User With Exceeded Qouta انجام می دهیم.

در داخل Traffic Rules از پنل مدیریتی Kerio Control تعدادی ایجاد کرده ایم که توسط آنها کاربرانی بر اساس سیاستهای مورد نظر به اینترنت وصل شده اند، حال در قسمت Packets maching a Traffic Rules می توانیم تنظیماتی را ایجاد کنیم که توسط آن کاربرانی که بوسیله Rules های موجود در Traffic Rules اینترنت دار شده اند با میزان سرعت آپلود و دانلودی که برای آنها در نظر خواهیم گرفت مواجه شوند یعنی به عبارتی یک پهنای باند برای آنها در نظر می گیریم.

اگر به قسمت Connections maching a Content Rules وارد شویم مواردی که بصورت تیتر هستند را مشاهده خواهیم کرد، این موارد دارای جزئیاتی می باشند که اگر در شبکه ترافیکهایی نسبت به این جزئیات مشاهده شد می توانیم بر این اساس میزان سرعت آپلود و دانلود در نظر بگیریم. این جزئیات بدین صورت می باشند که Audio and Video Files شامل سایتهایی می باشند که در آنها Video و Audio هست و Ms windows Update شامل سایتهایی می باشد که بوسیله آنها عملیات Update انجام می گیرد و موارد دیگر نیز به همین ترتیب می باشند.

Quota (سهمیه) :

Quota در حالت کلی یعنی ظرفیت ، سهمیه بندی می باشد و مقداری هست که برای کاربران از حیث میزان دانلود و آپلود در نظر گرفته شده هست. برای دادن Quota به تمامی یوزرهای دامین، Kerio Control یک Template هایی فرآهم آورده که از آنها استفاده می کنیم یعنی اگر تغییراتی در این Template ها ایجاد کنیم به کل دامین اعمال می شود.



وارد قسمت Users از پنل مدیریتی Kerio Control می شویم بعد از صفحه مربوط در قسمت Domain دامین مربوطه را انتخاب می کنیم، در این صورت کل یوزرهای تحت دامین در این صفحه لیست می شوند که با توجه به سناریوی ما دو یوزر User1 و User2 می باشند در پایین صفحه سمت راست گزینه ای به نام Template وجود دارد که با انتخاب آن صفحه مربوط به Template باز می شود این صفحه دارای سه تب , Quota , Rights Preferences می باشد.

توسط تب Rights می توانیم حقوق و مزایایی را نسبت به یوزرها مشخص کنیم که به دو صورت Administration Rights و Additional Rights می باشند.

تب دیگرش Preferences می باشند که دارای دو قسمت Web Content Scanning Options و Language Options می باشد در قسمت اول تعدادی حالات وجود دارد که می توانیم بر حسب نیاز آنها را فیلتر کنیم، مثلاً : Filter out HTML Java applets و یا Filter out HTML Activex objects و مابقیه گزینه ها ... و در قسمت دوم زبان مرورگر مشخص می شود، اگر گزینه Browser Detected را انتخاب کنیم مرورگر هر زبانی را Detected کند با آن کار می کند.

تب آخرش که بیشتر مد نظر ما هست Quota می باشد توسط محتویات این تب می توانیم سهمیه ای برای کاربران از حیث دانلود و آپلود و یا هر دو در بازه های زمانی روزانه ، هفتگی و ماهانه در نظر بگیریم که این عملیات در قسمت Transfer Quota انجام می گیرد.

قسمت دوم Quota Exceed Actions می باشد که در این قسمت این کار را انجام می دهیم که اگر کاربری خواست از حد میزان دانلود و آپلود خود تجاوز کند با چه رویکرد هایی با آن مقابله کنیم.

در حالت کلی سه روش برای مقابله وجود دارد:

1) Block any Further Traffic
2) Don't Block Further Traffic

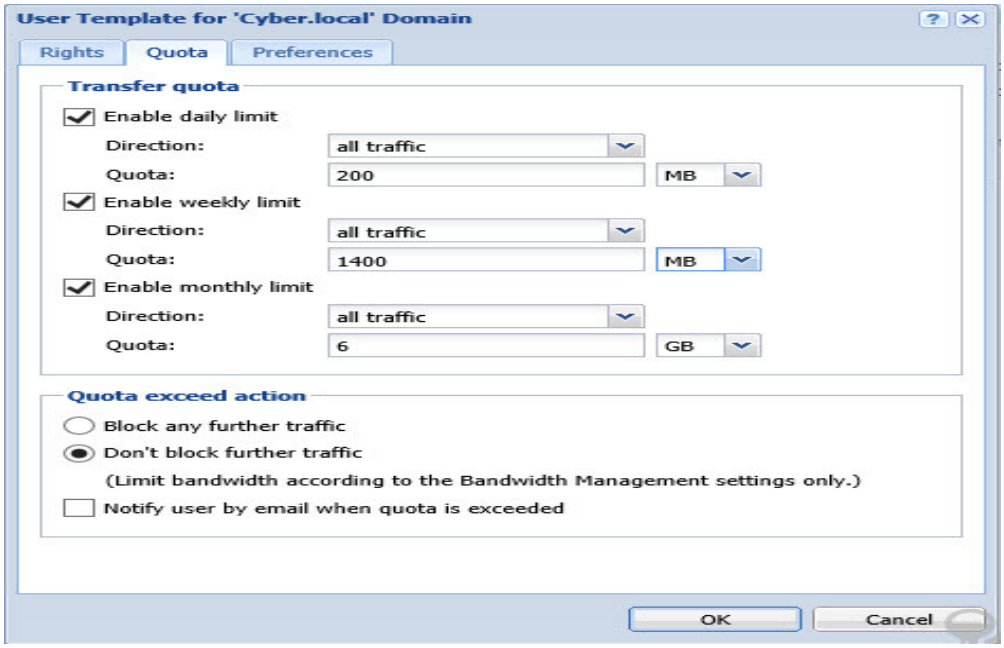
(Limit Bandwidth According to the Bandwidth Management Settings Only.)

3) Notify user by Email quota is Exceeded

توضیح 1) جلوی هر ترافیک بیشتر را بگیر.

توضیح 2) جلوی هر ترافیک بیشتر را نگیر ولی بوسیله قسمت مدیریت پهنای باند آن را محدود کن.

توضیح 3) توسط Email به کاربران اطلاع بدهید که از حدّ خود تجاوز کرده اید.



مقادیره فرضی آپلود و دانلود برای روزانه،هفتگی و ماهانه وارد کرده ایم که در شکل صفحه قبل مشاهده می کنید.

بعد از وارد کردن مقادیر مورد نظر بعنوان Quota روی Ok کلیک می کنیم و وارد قسمت Bandwidth Management می شویم، در این قسمت Rules ای را بدین منظور ایجاد می کنیم که هر وقت کاربری از حدّ میزان آپلود و دانلودی که برایش در نظر گرفته ایم بخواهد بیشتر استفاده کند با کاهش شدید سرعتی که ما برایش در نظر گرفته ایم مواجه شود. مشخصات Rules مورد بحث :

Rules Name = Users Exceeding Quota

Traffic = Exceeded Quota

Download = 64 Kbit/s

Upload = 16 Kbit/s

توسط این Rules تمامی یوزرهای تحت دامین اگر بخواهند که از میزان سهمیه خود تجاوز کنند با کاهش سرعت دانلود و آپلود به اندازه 16 Kbit/s مواجه شوند.

یک امکانی هم که می توانید در اینجا پیاده سازی کنید این هست که Rules ای ایجاد کنید که توسط آن تمامی Admins ها بدون محدودیت از حیث دانلود و آپلود به اینترنت دسترسی داشته باشند. بدین صورت می باشد:

Rules Name = Admins

Traffic = Administrator

Download = No Limit

Upload = No Limit

تا اینجا در مورد Bandwidth Management و چگونگی مدیریت پهنای باند توضیحاتی را خدمتتان ارائه دادیم، حال در نظر داریم سناریوی مورد نظر را جوره دیگه همراه با جزئیات ارائه دهیم بدین صورت که می خواهیم دو گروه متفاوت ایجاد کنیم گروه اول شامل Admins ها و دیگری شامل Users ها یا همان کاربران می باشند که به این دو گروه متفاوت قصد داریم پهنای باند متفاوت ارائه دهیم یعنی دو گروه با پهنای باند متفاوت، به همین دلیل تنظیمات مربوطه را از حیث گروه بندی Users ها و Admins ها در دو OU متفاوت در قسمت Active Directory Users and Computers انجام می دهیم سپس در قسمت Traffic Rules همانا Rules ای را ایجاد می کنیم که بوسیله آن اعضای گروه Domain Admins و گروه Servers که شامل IP تمامی سرورهای شبکه می باشد اینترنت دارمی شوند. مشخصات Rules مورد بحث بصورت زیر می باشد:

Rules Name = Internet Access for Admins & Servers

Source = Servers (Internet Access)

Domain Admins

Destination = Internet Interface

Service = Any

Action = Allow

Translation = NAT

توسط این Rules تمامی اعضای گروه Domain Admins و گروه (Internet Access) Servers که شامل IP تمامی سرورهای شبکه می باشد باید اینترنت دار شوند.

همچنین یک Rules نیز جهت دسترسی کلاینت ها یا همان Users های تحت دامین به اینترنت در نظر می گیریم که بدین شرح می باشد:

Rules Name = Internet Access for Domain Admins

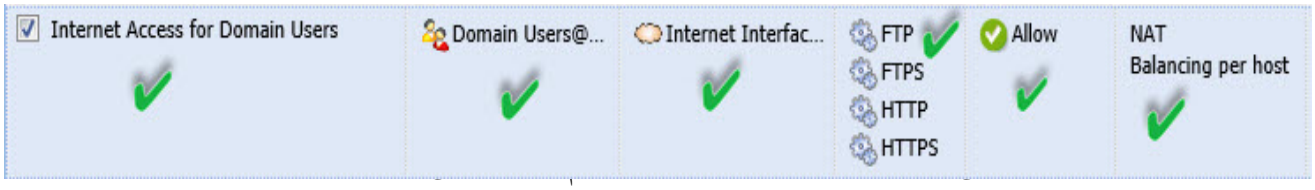
Source = Domain Admins

Destination = Internet Interface

Service = FTP , FTPS , HTTP , HTTPS

Action = Allow

Translation = NAT



معین شده دسترسی خواهند داشت.

حالا بر می گردیم به قسمت Bandwidth Management که در این قسمت دو Rules جهت اختصاص پهنای باند به دو گروه Domain Admins و Domain Users ایجاد می کنیم. Rules ها بدین صورت می باشند :

Rules Name = Bandwidth Management for Domain Admins

Traffic = Internet Access for Domain Admins & Servers

Download = No Limit

Upload = No Limit

توضیح Rules بالا بدین صورت می باشد که اگر Domain Admins ها توسط Rules موجود در Traffic Rules یعنی Internet Access for Domain Admins & Servers اینترنت دار شوند در این صورت پهنای باند آنها از حیث دانلود و آپلود دارای محدودیت نباشد.

برای شناساندن Rules مربوطه در Traffic Rules به Bandwidth Management روی فیلد Traffic دوبار کلیک می کنیم و از قسمت Add صفحه ای باز می شود که در آن گزینه Packet Maching a Traffic Rules را انتخاب می کنیم و سپس Rules مربوطه را از صفحه باز شده بر می گزینیم.

Rules Name = Bandwidth Management for Domain Users

Traffic = Internet Access for Domain Users

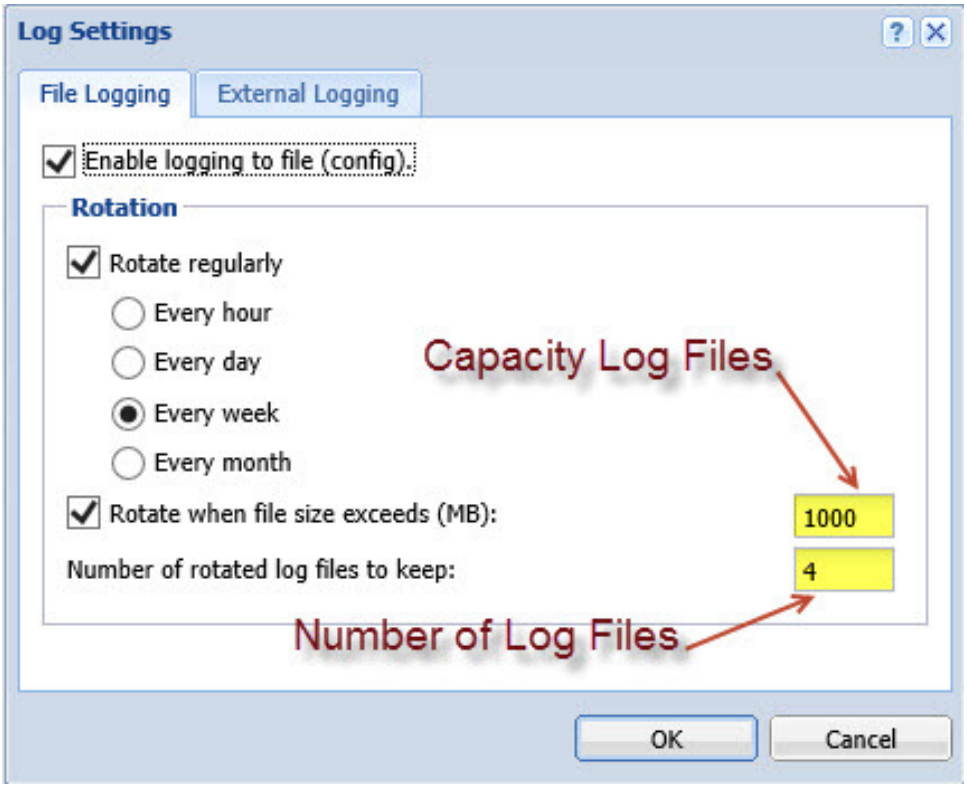
Download = 1 Mbit/s

Upload = 512 Mbit/s

توضیح این Rules هم بدین صورت می باشد که اگر Domain Users ها توسط Rules موجود در Traffic Rules یعنی Internet Access for Domain Users اینترنت دار شوند در اینصورت پهنای باند آنها از حیث Download = 1 Mbit/s و Upload = 512 Mbit/s باشد. برای شناساندن Rules موجود در Traffic Rules به Bandwidth Management عین توضیح Rules قبلی انجام می دهیم.

یک موضوع دیگر هم هست که باید بدان اشاره کنیم نحوه تنظیم Logs های Kerio Control می باشد، برای این موضوع وارد قسمت Logs ها می شویم و در وسط صفحه راست کلیک می کنیم و گزینه Log Settings را انتخاب می کنیم امکاناتی که در صفحه Log Settings هست بدین صورت می باشد که اولاً ما می توانیم Logs ها را بصورتهای ساعتی ، روزانه ، هفتگی و ماهانه ذخیره کنیم حال این Logs ها را می توانیم در فایلهایی که حجم آنها در قسمت Rotate When file size Exceed (MB) مشخص می شود ذخیره کنیم. در قسمت Number of Rotate Log files to Keep نیز می توانیم تعداد Log files ها را بر اساس میزان حجم تعیین شده مشخص کنیم. در قسمت Rotation تیک گزینه Rotate Regularly را می زنیم و عبارت

Every Week را انتخاب می کنیم و در قسمت Rotate When file size Exceed (MB) مقدار 1000 و در قسمت Number of Rotate Log files to Keep نیز مقدار 4 را وارد می کنیم، این تنظیمات بدین معنی می باشد که Kerio Control همانا Logs ها را در 4 فایل با ظرفیت 1000 MB بصورت هفتگی ذخیره می کند و اگر تعداد Log files ها از 4 تا بیشتر شد بصورت FIFO عمل کند یعنی قدیمی ها را از رده خارج کند و Log فایلهای جدیدی را ایجاد کند.



منابع مورد استفاده :

- سایت www.ostadbook.com
- سایت www.kerio.com
- کتاب Kerio Control Administrator’s Guide