

گروہ آموزشی فیرزان

-0-0-0-



Getting Started Wizard

بعد از نصب Service Pack ها، تنظیمات مربوط به ویزارد TMG را انجام می دهیم. زمانی که ویزارد TMG را اجرا می کنید، پنجره Getting Started Wizard به شما نمایش داده می شود. با استفاده از این ویزارد می توانید تنظیمات پایه، از جمله تنظیمات کارت شبکه، Policy Update ها و وضعیت قرار گیری TMG در شبکه Workgroup یا دامین را مشخص کنید.



گروہ آموزشے فےرزان تنظیمات کارت شبکه متصل شده به شبکه LAN از جمله: IP آدرس، Subnet mask، آدرس DNS سرور.

www.Modir-Shabake.com

تنظیمات کارت شبکه متصل شده به اینترنت اگر از ISP، آدرس IP استاتیک دریافت کرده اید، اطلاعات IP آدرس، Subnet mask و آدرس DNS سرور را نیاز داريد.

تنظیمات هریک از کارت شبکه های اضافه تری که روی کامپیوتر شما قرار دارد، از جمله کارت شبکه سومی که به Perimeter Network شما متصل شده است.

 اطمینان حاصل کنید که نام سرور و نام FQDN را، در صورتی که کامپیوتر شما عضو دامین می باشد در اختیار دارید.

توجه:

گروہ آموزشی فیرزان

Getting Started Wizard، فقط به صورت locally اجرا می شود با استفاده از ریموت قابل اجرا نمی باشد، بعد از اجرای Getting Started Wizard، نباید تغییراتی بر روی کارت شبکه خود ایجاد کنید.

-0-0-0

گروه آموزشیی فیرزان



در انتهای این ویزارد توضیح داده شده است، در صورتی که می خواهید تنظیمات ISA server 2006 را در کنسول TMG، Import کنید، می بایست این عملیات را قبل از اجرای مراحل این ویزارد انجام دهید.

-0-0 www.Modir-Shabake.com گےروہ آموزشے فےرزان کزينه Configure network settings بر روی گزینه Next کلیک کنید Getting Started - Network Setup Wizard X Welcome to the Network Setup Wizard This wizard helps you define basic networking settings for Forefront TMG. This includes network IP settings, network relationships, and routing rules. Advanced network settings can be specified after completing the Getting Started Wizard. To continue, dick Next. Help about the Network Setup Wizard

همانطور که مشاهده می کنید توپولوژیهای پیش فرض قرار گیری TMG در شبکه را می توانید انتخاب کنید. به دلیل اینکه از دو

Next >

Cancel



در این قسمت، کارت شبکه ای را انتخاب می کنیم که به شبکه LAN متصل است. همانطور که مشاهده می کنید تمامی تنظیمات انجام شده بر روی کارت شبکه داخلی نمایش داده می شود.

توجه داشته باشید که: Default gateway را فقط برای کارت شبکه External مشخص کنید، برای سایر کارت شبکه ها وارد نمودن Default gateway لازم نمی باشد. TMG تمامی ترافیکها را به نحو مناسبی، Rout می کند.

در این سناریو از یک DNS Server داخلی استفاده کرده ایم و IP مربوط به DNS Server نیز قابل مشاهده می باشد.

Local Area Network (I	k Setup Wizard LAN) Settings	
Define the settings f	or the network adapter connected to your LAP	
Network adapter connect	ed to the LAN:	
Internal	▼	
(P address:	10 . 1 . 1 . 3	
Subnet mask:	255.0.0.0	
Default gateway:		
ONS server:	10 . 1 . 1 . 1	
Network Destination	Netmask Gateway	Add
		Edit
		Remove

WW

در قسمتSpecify additional network topology routers، شبکه های دیگری را که جزء شبکه Internal ما هستند ولی Subnet های متفاوتی دارند اضافه می کنید.

Local Area Netw Define the se	vork (LAN) Settings ttings for the network adapter	connected to your LAN.	
Network adapter o	connected to the LAN:	T	
IP address: Subnet mask:	Network Topology Route P Specify properties of this net	twork topology route:	
Default gateway	Network Destination:		
DNS server:	Netmask:	255 . 255 . 255 . 255	
Specify additiona	Gateway:		
Network Destin		Count 1	Add
	UK	Cancel	Edit
		-	Nombyo

شکل زیر مثالی از شبکه های دیگری می باشند که بخشی از شبکه داخلی شما محسوب می شوند :



Set the internet settings	based on information from your interne	et service provider (15P).
Network adapter connected to	the Internet:	
External		
C Obtain an IP address auto	matically	
• Use the following IP addre	ss	
IP address:	192 . 168 . 1 . 21	
Subnet mask:	255 . 255 . 255 . 0	
Default gateway:	192 . 168 . 1 . 1	
DNS server:		

W

در این قسمت کارت شبکه ای را که به اینترنت متصل می باشد اضافه میکنیم. نام این کارت شبکه را External در نظر گرفته ایم. همانطور که مشاهده میکنید دو گزینه برای انتخاب وجود دارد، در صورتی که بخواهید آدرس IP را از DHCP مودم دریافت کنید گزینه Obtain an IP

address automatically، را انتخاب کنید. در این حالت کارت شبکه شما تنظیمات IP آدرس، Default gateway و DNS را به صورت اتوماتیک دریافت خواهد کرد و آدرس IP شما ثابت نمی باشد.

در صورتی که بر روی کارت شبکه متصل به اینترنت، تنظیمات را به صورت دستی وارد نموده اید، با انتخاب کارت شبکه متصل به اینترنت، گزینه دوم انتخاب شده و تنظیمات وارد شده را نمایش می دهد.

همانطور که قبلا اشاره شد، بهتر است در قسمت DNS server، IP وارد نکنید و عمل Name Resolution توسط DNS Server ها صورت گیرد.



— 🔘 ——

-0--0

گےروہ آموزشےی فےرزان

تنظیمات مربوط به گزینه Configure network settings، در اینجا به پایان می رسد. تنظیمات گزینه های بعدی را می توانید با استفاده از ویزارد اصلی TMG نیز انجام دهید، که این تنظیمات را در ادامه همین ویزارد کامل می کنیم.

گروہ آموزشی فیرزان

: Configure system settings کزينه



_0_0_0_0_0_0_0_0_0_0_0

بعد از انتخاب این گزینه پنجره زیر به شما نمایش داده می شود.

77777	Welcome to the System Configuration
	Wizard
	This wizard helps you define local system settings for your Forefront TMG computer.
	For successful completion of this wizard, network connectivity should be available.
	To continue, dick Next.
	Help about the System Setup Wizard
	< Back Next > Cancel
	ادامه بر روی next کلیک کنید.

 \bigcirc

Ċ

Ó

0

www.Mo

Getti

Co

Fu

\mathcal{H}
Change
Change
Change,
Change

< Back

Next >

Cancel

در این مرحله Computer name و وضعیت قرار گیری TMG، در شبکه شما نمایش داده شده است. در قسمت Computer name، با انتخاب Change می توانید نام کامپیوتر خود را تغییر دهید. و در قسمت Member of وضعیت TMG که در شبکه Workgroup یا دامین قرار گرفته است مشخص می شود.

گروہ آموزشے فرزان

Primary DNS Suffix نیز تنظیمات DNS Suffix نمایش داده می شود که همان تنظیمات گزینه Change settings در قسمت پراپرتیز Computer می باشد که زمان Join نمودن کامپیوتر به دامین استفاده می کنیم. برای ایجاد تغییر در هر یک از این قسمتها می توانید بر روی گزینه Change، کلیک کنید.

omputer name:	2008R2Ent	Change
Member of		
Windows domain:	farzan.com	Change
O Workgroup:		Change,
Help about <u>domain and wo</u>	rkgroup membership	
Primary DNS Suffix		
DNS suffix:	farzan.com	Change
In a domain, the controller.	primary DNS suffix is provided by the domain	

www.Modir-Shabake.co	گـروه آموزشــی فـرزان om
	برای ادامه بر روی next، کلیک کنید.
Cetting Started - System Co	nofiguration Wizard
	Completing the System Configuration Wizard
	You have successfully completed the System Configuration Wizard. The following settings will be applied:
	Host Identification Membership: Domain Full host name: 2008R2Ent.farzan.com
	< Back Finish Cancel
Configure s، به	تنظیمات مربوط به گزینه ystem settings
	پایان می رسد.
	21

_0_0_0_0_0_0_0_0_0_0_0_0_0_0

Э

-0

C

0-0

 \bigcirc

0-

0

-0

-0

-0-0-0-0

گروہ آموزشی فیرزان

-0-0-0-0-0-0-

 \bigcirc

 \bigcirc

کزینه Define deployment options.



گزینه Define deployment options، را انتخاب می کنیم.

vww.Modir-Shabake.co	گروہ آموزشیی فیرزان om
Getting Started - Deploymer	nt Wizard
EH D	Welcome to the Deployment Wizard
	This wizard helps you deploy Forefront TMG. This includes specifying update settings and joining the Customer Experience Improvement Program.
	To continue, click Next. Help about the Deployment Wizard
	<back next=""> Cancel</back>
	برای ادامه روی next، کلیک کنید.
	23

گےروہ آموزشےی فےرزان



-0-0-0-0-0-0-0-0

در این قسمت مشخص می کنیم که TMG، از Update هایی که مایکروسافت ارائه می دهد استفاده کند یا خیر. دریافت این Update ها به منظور افزایش امنیت TMG می باشد. گزینه اول را به منظور تایید دریافت update ها، انتخاب می کنیم و روی Next کلیک می کنیم.

Forefront TM Use this pa	G Protection Features Settings age to activate licenses required for receiving updates and to enable Forefront
TMG prote	ction mechanisms.
Network Insp	ection System (NIS)
License:	Activate complementary license and enable NIS
What is NIS?	
license:	Activate evaluation license and enable Web Protection
License.	
Key:	Evaluation Expiration date: 4/22/2013
Enable Ma	Iware Inspection
The The	URL Filtering feature queries Microsoft Reputation Service for URL categorization. full URL string is sent to the service, using a secure connection.
Learn about up	dating license agreements

در قسمت NIS و در منوی License، نوع استفاده از لایسنس TMG و فعال بودن قابلیت NIS، که سیستم تشخیص حملات می باشد را مشخص می کنیم. گزینه انتخاب شده فعال سازی لایسنس و قابلیت NIS می باشد. اگرگزینه Disable NIS، را انتخاب کنید این قابلیت غیر فعال خواهد شد.

گروه آموزشی فیرزان

در قسمت Web Protection و در منوی License، سه گزینه برای انتخاب خواهید داشت. گزینه ای که انتخاب شده است، فعال سازی لایسنس به صورت آزمایشی به همراه قابلیت Web protection می باشد. بعد از پایان یافتن اعتبار استفاده از نسخه آزمایشی، نمیتوانید از قابلیت های Web Protection استفاده کنید استفاده از این قابلیت نیاز به لایسنس دارد.

گزینه Activate purchase License and enable web کزینه TMG، وارد نمودن لایسنس TMG و فعال سازی veb protection می باشد. با انتخاب Disable Web protection، قابلیت Web Protection، غیر فعال می شود.

با استفاده از قابلیت Web Protection، و انتخاب گزینه Enable Malware Inspection، کدها و برنامه های مخرب شناسایی شده و از نفوذ آنها جلو گیری می شود. با انتخاب گزینه Enable شده و از نورذ آنها جلو گیری می شود. با انتخاب گزینه URL Filtering، از MRS که پیش از این توضیح داده شد برای تشخیص دسته بندی URL ها، استفاده می شود. در ویزارد اصلی TMG، با تنظیمات پیشرفته تر این گزینه ها آشنا می شوید.

برای ادامه روی Next، کلیک کنید.

	<u></u>
IIS Signature Update Settings Use signatures of known vulnerabilities from the detect and potentially block malicious traffic.	e Microsoft Malware Protection Center to
Signature Set Update Configuration	
Select automatic definition update action:	
Check for and install definitions (recommended)	
Automatic polling frequency:	
Every 15 minutes	
Trigger an alert if no updates are installed after th	is number of days:
	shanber of days.
New Signature Set Configuration	
Select the response policy for new signatures:	
Microsoft default policy (recommended)	
Signatures configured to respond in a way attention on the NIS details pane.	other than the Microsoft default are flagged for
elp about configuring NIS	

در این مرحله تنظیمات update NIS را برای تشخیص آسیب پذیریهای حاصل از کدهای مخرب و مسدود نمودن آنها، مشخص می کنیم.

گـروه آموزشـی فـرزان

در قسمت Select automatic definition update action، گزینه برای انتخاب دارید:

گزینه انتخاب شده بررسی و نصب مشخصه های آسیب پذیریها می باشد و مایکروسافت انتخاب این گزینه را توصیه کرده است.

گزینه Only for check definition، فقط مشخصه های آسیب پذیری را بررسی می کند، گزینه No automatic action، بررسی Update ها و نصب آنها انجام نمی گیرد.

گروہ آموزشے فےرزان

در قسمت Automatic Polling frequency، بازه زمانی را مشخص می کنیم که در چه فواصلی Update ها بررسی شوند.

در قسمت Trigger an alert if no updates are installed after this number of days. مشخص می کنیم که اگر بعد از این بازه زمانی، هیچ update ای نصب نشده باشد یک Alert یا پیغام هشدار به ما نمایش داده شود.

در قسمت New Signature Set Configuration انتخاب روشی برای نحوه واکنش به مشخصه هایی است که هنگام وقوع حملات برای NIS تنظیم کرده ایم. سه گزینه برای انتخاب وجود دارد:

با انتخاب گزینه Microsoft Default Policy، از Policy های پیش فرض، به منظور واکنش و پاسخگویی استفاده می شود. مایکروسافت نیز انتخاب این گزینه را پیشنهاد کرده است.

با انتخاب گزینه Detect only response، فقط واکنش مورد نظر شناسایی می شود، با انتخاب گزینه No response(disable (signature، هیچ واکنشی صورت نمی گیرد.

برای ادامه روی Next کلیک کنید

گےروہ آموزشے فےرزان

گروہ آموزشی فیرزان

-0-0

tting Started - Deployment Wizard	×
Customer Feedback We invite you to join the Customer Experience Improvement Program to help us improve the quality, reliability, and performance of this product.	h
This program collects anonymous information about your hardware configuration and how you use Forefront TMG, without interrupting you. Microsoft uses the information to identify trends and usage patterns.	2
If you choose to participate in the program, Web proxy client access will be enabled on the Forefron TMG Local Host network.	t
You can change your participation choice after closing this wizard. To do this, open the array proper and modify settings on the Customer Feedback tab.	ties
No information will be used to identify or contact you.	
Learn more about the Customer Experience Improvement Program	
 Yes, I am willing to participate anonymously in the Customer Experience Improvement Program (recommended) 	
C No, I don't want to participate	
< Back Next > Can	cel

در این مرحله به صورت اختیاری از کاربران دعوت میشود که در توسعه و بهبود عملکرد این برنامه مشارکت داشته باشند، بدون اینکه اطلاعات فردی اشخاص مورد نیاز باشد.

گروہ آموزشی فیرزان

با انتخاب گزینه Yes، اطلاعاتی در خصوص تنظیمات سخت افزاری و چگونگی استفاده از TMG جمع آوری می شود بدون اینکه در نحوه کارکرد این برنامه وقفه ای حاصل شود. هیچ یک از این اطلاعات به منظور تماس با شما از سوی مایکروسافت استفاده نخواهد شد.

توجه داشته باشید که بعد از تایید یا عدم تایید در این مرحله، میتوانید نام سرور TMG را انتخاب کرده و از منوی Tasks و با استفاده از گزینه Configure Array Properties در تب Customer Feedback نیز، این تنظیمات را تغییر دهید.

برای ادامه روی Next، کلیک کنید.

ing Started - Deployment Wizard	X
Ticrosoft Telemetry Reporting Service Select a participation level for Microsoft telemetry re	eporting.
f you choose to participate in Microsoft telemetry report ttacks on your network is sent to Microsoft. This inform bility to identify attack patterns and mitigate threats. Ir advertently sent, but Microsoft will not use the informa	ting, information regarding malware and other ation helps Microsoft improve Forefront TMG's n some cases, personal information may be ation to identify or contact you.
elect your level of participation:	
Basic	
Basic information about potential threats including the taken, is sent to Microsoft.	eir type and origin, as well as the response
Advanced	
In addition to basic information, information about po samples and full URL strings is sent to Microsoft. This more help in analyzing and mitigating threats.	otential threats in greater detail, including traffic additional information provides Microsoft with
None. No information is sent to Microsoft	
ead our Privacy Statement	

در این مرحله سطح گزارشهای گردآوری شده را مشخص میکنید. اطلاعات malware ها و سایر حملات صورت گرفته به شبکه شما، برای مایکروسافت ارسال می شوند. این اطلاعات به مایکروسافت کمک می کند که توانایی شناسایی الگوهای حملات و کاهش آنها را در TMG بهبود بخشد.

گـروه آموزشـی فـرزان

با انتخاب گزینه Basic: اطلاعات پایه در خصوص حملات بالقوه به شبکه که شامل نوع این حملات و منشأ آنها می باشد، به محض وقوع و واکنش صورت گرفته در مقابل هریک، به مایکروسافت فرستاده می شود.

با انتخاب گزینه Basic د حالت Basic به مایکروسافت ارسال علاوه بر اطلاعاتی که در حالت Basic به مایکروسافت ارسال می شود، جزئیات بیشتری از این تهدیدات بالقوه، که شامل نمونه هایی از این ترافیکها و URL های مربوط به آنها می باشد نیز برای مایکروسافت ارسال می شوند. این اطلاعات به مایکروسافت کمک میکند که آنالیز بهتری بر روی این حملات انجام داده و بروز چنین حملاتی را کاهش دهند.


گروه آموزشـی فـرزان تنظیمات فعال شده است و یک Check Mark، سبز رنگ در کنار هریک نمایش داده می شود.

-0-0-0-0-0-0-0-0



بعد از تکمیل این مراحل با انتخاب Close، به صورت اتوماتیک کنسول Web Access Policy Wizard نمایش داده می شود، که در طی مراحل این ویزارد می توانید Policy کنترل دسترسی

گروه آموزشی فیرزان

به صفحات Web را با اجازه دسترسی یا عدم اجازه دسترسی به دسته بندی خاصی از URL ها، ایجاد کنید و تنظیمات تشخیص malware ها و چگونگی دسترسی به وب سایتهای HTTPS و تنظیمات Web Caching را نیز مشخص نمایید.

برای اینکه ویزارد تنظیمات این Policy نمایش داده نشود، می توانید تیک گزینه Run the web Access wizard را غیر فعال کنید.

می توانید قبل از انجام تنظیمات این ویزارد سیاستهای اعمال Policy سازمان خود را در خصوص دسترسی به وب سایتهای مجاز و دسته بندی کاربران مورد نظر با سطح دسترسی های مجاز و غیر مجاز را به خوبی تحلیل کرده و آنها را در طول انجام

-0-0-0-0-

ویزارد پیاده سازی نمایید. در غیر این صورت می توانید بعد از تکمیل این ویزارد نیز، از طریق کنسول TMG، تغییرات لازم را ایجاد کنید.

	Welcome to the Web Access Policy Wizard
	This wizard helps you define: - Web access for your organization - Blocked URL categories and Web destinations - Malware inspection settings - HTTPS inspection settings - Web caching settings When you complete this wizard, Web access rules will be created.
UKKK	Help about Web access policy

-0

-0-0-0

0-0-0

0-0-0-

- 🌘

برای ادامه روی Next، کلیک کنید.

-0-0-0-0-0

-0-0-0

> > \bigcirc

 \bigcirc

O

 \bigcirc

.

گروہ آموزشی فیرزان

also	create a default blocking rule.	
Do you categori	want the wizard to create a default rule that blocks access to potentially malicious UR ries?	L
 Yes, 	, create a rule blocking the minimum recommended URL categories	
O No,	do not create the rule for me	
1	You can edit the default blocking rule or create your own blocking rule on the next the wizard.	page of
Help abo	out URL categories	

در این مرحله، می توانید یک Rule پیش فرض برای دسترسی کاربران داخلی به اینترنت ایجاد نمایید

گےروہ آموزشے فےرزان

Yes, create a rule blocking the minimum recommended URL categories كزينه

با انتخاب این گزینه یک Access Rule برای بلاک کردن تعدادی از URL ها که در لیست URL Categories ها موجود می باشند، ایجاد خواهد شد. بعد از مشخص نمودن این دسته از URL ها از طریق این ویزارد، با استفاده از کنسول TMG نیز می توانید رولهایی را برای Allow یا Deny کردن دسترسی ها بر روی تعدادی از URL Categories ها ایجاد کنید.

مایکروسافت در طول روز و به صورت منظم، این URL Categories ها را Update می کند و TMG نیز می تواند به گونه ای پیکر بندی شود که Update های این URL Categories ها، را به صورت اتوماتیک دریافت کند.

گروہ آموزشی فیرزان

No, do not create the rule for me كزينه

با انتخاب این گزینه، TMG رول بلاک نمودن Site های پیش فرض را به صورت اتوماتیک ایجاد نخواهد کرد، و شما می بایست به صورت دستی لیست وب سایتهای مورد نظر را برای بلاک شدن، انتخاب نمایید.

گزینه Yes را انتخاب کرده و برای ادامه روی Next کلیک کنید.

گروہ آموزشی فیرزان

Web /	Access Policy Wizard	X Add Destinations
B	A rule "Blocked Web Destinations" will be created. You can define exceptions to the rule on the next page of this wizard.	Destinations: New - Edit Delete
	Anonymizers Anonymizers Botnet Criminal Activities Gambling Hate/Discrimination Illegal Drugs Malicious Obscene/Tasteless To apply URL filtering to rules using URL categories or category sets, Forefront TMG queries the remotely hosted Microsoft Reputation Service. The full URL string is sent to the service, using a secure connection. ead our Privacy Statement	Image: Content servers/Infrastruct Image: Content
	< Back Next > Cancel	Add Close

همانطور که مشاهده می کنید، لیست وب سایتهای پیش فرض به صورت اتوماتیک برای شما انتخاب شده اند. برای اضافه نمودن برخی دیگر از URL ها، گزینه ADD را انتخاب کرده و از URL های مشخص شده در URL Categories، چند نمونه URL دیگر مانند Hacking/Computer Crime ، Chat و Games نیز انتخاب کرده و آنها را به لیست URL های پیش فرض اضافه می کنیم.

TMG queries که یکی از قابلیتهای تعبیه شده در TMG queries می باشد به منظور اعمال URL Filtering بر روی Rule هایی که از URL Categories استفاده می کنند، به صورت ریموت به سرویس MRS متصل شده و تبادل اطلاعات بین TMG و سرویس MRS در خصوص این URL ها با استفاده از یک اتصال امن صورت می گیرد.

گےروہ آموزشے فےرزان

بعد از ورود به کنسول TMG با چگونگی کارکرد TMG با سرویس MRS، و استفاده از این سرویس برای ایجاد انواع دلخواهی از Rule ها که بتواند استفاده از Application های مورد نظر را بلاک کند، آشنا خواهید شد.

گروه آموزشیی فیرزان

برای ادامه روی Next کلیک کنید.

در این مرحله می توانید یک گروه از کاربران را به عنوان موارد استثنا به این قسمت اضافه کنید که دسترسی آنها به URL های مشخص شده، توسط این رول بلاک نشود.

گزینه Add را انتخاب کنید، به صورت پیش فرض دسته ای از کاربران برای شما مشخص شده اند که می توانید با انتخاب New، گروه کاربران مورد نظر را، ایجاد نمایید.

vice
vice
Close

	ِينه New را انتخاب مي کنيم.
New User Set Wizard	×
	Welcome to the New User Set Wizard
	This wizard helps you create a new user set. A user set is a group of users, whether Windows or non-Windows (e.g., RADIUS) users, defined together as a single set.
	When you create Web publishing, protocol, and access policy rules, you can apply the rule to one or more user sets.
	User set name:
UKUKU	Allow Go Anywhere
	To continue, click Next.

ویزارد نمایش داده شده برای ایجاد کاربران یا گروه های مورد نظر شما می باشد. در قسمت User set name، یک نام برای کاربر یا گروهی از کاربران مورد نظر وارد کنید و برای ادامه روی Next کلیک کنید، در این مرحله با انتخاب کلید Add، 4 گزینه به شما نمایش داده می شود:

Namespace Gr	roup	Domain	Add
			Windows users and groups LDAP RADIUS SecurID

-0-0

گروہ آموزشے فرزان

TMG از TMG از Authentication Server هایی که در جدول زیر نمایش داده شده است برای احراز هویت کاربران پشتیبانی می کند:

گـروه آموزشـی فـرزان

 \bigcirc

Q

توضيحات	Authentication Server
(Lightweight Directory Access از پروتکل TMG Directory Service ارائه شده توسط LDAP Protocol) Active Directory Lightweight Directory) AD LDS (Services) سرور می باشد پشتیبانی می کند	LDAP با استفاده از LDAP
Remote Authentication) RADIUS از سرویس TMG Network Policy) NPS که توسط (Dial-In User Service) Server) ارائه شده است پشتیبانی می کند.	RADIUS با استفاده از NPS
TMG از RSA SecureID با دو فاکتور امنیتی احراز هویت پشتیبانی می کند	RSA Authentication Manager

گروہ آموزشی فیرزان

Windows users and groups با انتخاب این گزینه می توانید گروهی از کاربران تعریف شده در Active Directory را انتخاب کنید Active Directory می بایست متعلق به همان Domain یا Forest ای باشد که TMG در آن قرار گرفته است.

LDAP احراز هویت کاربران مورد نظر از طریق LDAP Query هایی که به LDAP Server های تعریف شده روی TMG ارسال می شوند، صورت می گیرد. به خاطر داشته باشید که همگی می شوند، صورت می گیرد. به خاطر داشته باشید که همگی می شوند، صورت می گیرد. به خاطر داشته باشید که دامین می شوند، صورت می گیرد. به خاطر داشته باشید که مرک می شوند، صورت می گیرد. به خاطر داشته باشید که مرک مای دامین Directory های دیگری انجام دهد.

RADIUS در صورت وجود RADIUS سرور می توانید برای احراز هویت کاربران این گزینه را انتخاب کنید. توجه داشته باشید زمانی که از RADIUS استفاده می کنید نمی توانید گروهی از کاربران به خصوص تشکیل دهید، بنابراین می بایست کاربران را به صورت جداگانه و تک به تک اضافه کنید.

گروہ آموزشے فےرزان

SecureID، یکی از مکانیزمهای احراز هویت می باشد که از دو فاکتور احراز هویت: PIN کد و Token کد استفاده می کند.

Token کدها با استفاده از PIN pad ها، Standard card ها و یا Software token ها ارائه می شوند.

گےروہ آموزشے فےرزان

با استفاده از یک توکن سخت افزاری (برای مثال Authenticate code) و یا یک توکن نرم افزاری، یک Authenticate code رمانی به کامپیوتر کلاینتها اختصاص داده می شود که در فواصل زمانی ثابت (معمولا هر 60 ثانیه) و با استفاده از Clock داخلی و ثابت (معمولا هر 60 ثانیه) و با استفاده از Clock داخلی و کلید تصادفی می باشد و به نام "Seed" نیز شناخته می شود) تولید می شوند.

گروہ آموزشی فیرزان

SecureID را می توان برای احراز هویت کلاینتهایی استفاده کرد که، از VPN استفاده می کنند و یا کلاینتهایی که می خواهند به وب سرورهای Publish شده داخلی شبکه دسترسی داشته باشند.

كلاينتها مى بايست SecureID ارائه دهند و Token فيزيكى نيز (PIN)، خود را به SecureID ارائه دهند و Token فيزيكى نيز زمان محدودى را براى وارد كردن هر Password توليد مى كند، هم PIN كد و هم Password توليد شده توسط Token براى دسترسى لازم مى باشند.

گروہ آموزشیی فیرزان

در این سناریو که TMG عضو دامین می باشد گزینه Select Select را انتخاب می کنیم، پنجره Select دمت Users or Groups به شما نمایش داده می شود. از قسمت Object Types گزینه مورد نظر را انتخاب کنبد. در اینجا گروهی با نام Allow Go Anywhere، را در AD ایجاد کرده و کاربران مورد نظر را در این گروه قرار داده ایم، بنابراین گزینه Groups را انتخاب می کنیم.

اگر کاربران مورد نظر خود را از Active Directory انتخاب می کنید، بررسی کنید که در قسمت From this location، یک فهرست در زیرعنوان Entire Directory، برای شما نمایش داده شود.

گروہ آموزشے فرزان

در قسمت Enter the object names to select، نام کاربر یا گروه مورد نظر را وارد کرده و روی کلید Check Name کلیک کنید، بعد از شناسایی و تأیید نام وارد شده، روی گزینه OK کلیک نمایید، برای ادامه روی گزینه Next کلیک نمایید.

	05	<u> </u>
Select this object type: Groups		Object Types
From this location:		
farzan.com		Locations
Enter the object names	to select (<u>examples</u>):	
Allow Go Anywhere		Check Names

گروہ آموزشی فیرزان

نام User یا Group اضافه شده در این صفحه به شما نمایش داده می شود. می توانید با استفاده از گزینه ADD، کاربران یا گروه های دیگری را اضافه کنید و بااستفاده از گزینه Remove، آنها را از این لیست، حذف نمایید.

Vamespace	Group	Domain		
Windows	Allow Go Anywhere	FARZAN		Add
				Remove
			-	

/ww.Modir-Shabake.co	وزشــی فــرزان om	ـروه آه
گروه اضافه شده و	عله به اتمام رسیده است، نام کاربر یا آ	بن مرح
شود. برای تکمیل	ار گیری آن به شما نمایش داده می	حل قر
ا كليك نماييد.	راحل انجام شده بر روی گزینه Finish	مودن م
New User Set Wizard	×	
	Completing the New User Set	
	Wizard	
	Wizard You have successfully completed the New User Set Wizard. You created a new user set with the following configuration:	
	Wizard You have successfully completed the New User Set Wizard. You created a new user set with the following configuration: Name: Allow Go Anywhere Users: FARZAN\Allow Go Anywhere	
	Wizard You have successfully completed the New User Set Wizard. You created a new user set with the following configuration: Name: Allow Go Anywhere Users: FARZAN\Allow Go Anywhere Value Contemportation (Contemportation)	

-___

 $\bigcirc - \bigcirc -$

در ادامه ویزارد ایجاد Web Access Rue و در پنجره Blocked Web Destinations Exceptions، مجددا کلید Add را انتخاب کنید. نام کاربر یا گروهی که اضافه نمودید



Web Access Policy Wizard	×	Add Exceptions	×
Blocked Web Destinations Exceptions		Authenticated Access:	
Specify the data in your organization allowed to access the blocked web destinations.	\mathcal{T}	New Edit Delete	
		All Authenticated Users	
Users with unrestricted Web access:		Allow Go Anywhere	
	Add	System and Network Service	
	Edit		
	Remove		
		Add Close	
< Back Next >	Cancel		

نام کاربر یا گروه مورد نظر به این لیست اضافه شده است، برای ادامه روی گزینه Next کلیک نمایید.

Blocked Web Destinations Excepti Specify the users in your organization	ons allowed to access the	blocked Web destinations.	
Users with unrestricted Web access			
Allow Co Apyrehoro			Add
			Add
			Edit
			Remove

در صفحه Malware Inspection Settings، می توانید وضعیت اسکن محتویات درخواستهای HTTP از اینترنت را به منظور تشخیص Malware ها (مانند ویروسها و spyware ها)، مشخص کنید.

گےروہ آموزشے فےرزان

دو گزینه برای انتخاب خواهید داشت:

No, do not inspect Web content requested from the Internet كزينه

اگر این گزینه را انتخاب کنید محتویات در خواستهای Web برای تشخیص malware ها از طریق این Rule، مورد بازرسی قرار نمی گیرند. البته شما می توانید Rule های دیگری را ایجاد کرده و قابلیت Malware Inspection را بر روی آن رولها فعال کنید.

گروہ آموزشے فےرزان

کزینه Yes, inspect Web content requested from the Internet

با انتخاب این گزینه، قابلیت تشخیص malware ها برای محتويات صفحات وب، از طريق اين رول فعال خواهد شد. توجه داشته باشید که فقط محتویات وب که از طریق Web Filter Proxy درخواست می شوند مورد بازرسی قرار می گیرند. محتويات غير وب مانند اتصالات NNTP براي بررسي malware ها، بازرسی نمی شوند. (NNTP یا Network News Transfer Protocol یک Application Protocol است که برای انتقال مقالات اخبار Usnet، مورد استفاده قرار می گیرد. Usnet، یک سیستم توزیع مذاکرات از طریق اینترنت بین News Server ها برای خواندن و ارسال مقالات توسط Client Application ها در سرتاسر جهان می باشد.)

گروہ آموزشے فےرزان

فعال سازي يا عدم فعال سازي چک مارک:

Block encrypted archives...Such files may contain encrypted viruses capable of bypassing antivirus signatures

با فعال سازی چک مارک این گزینه، می توانید مجموعه ای از فایلهای encrypt شده را که ممکن است حاوی ویروس بوده و signature های تعریف شده در دیتابیس antivirus ها را bypass کرده یا دور بزند، توسط TMG بلاک نمایید.

گروہ آموزشی فیرزان

-0-0-0-

ma	Iware, such as viruses and spyware.
Do y	ou want to apply malware inspection to the rules created by the Web Access Policy Wizard?
ON	Io, do not inspect Web content requested from the Internet
€γ	es, inspect Web content requested from the Internet
	⁷ Block encrypted archives (for example, .zip files). Such files may contain encrypted viruses capable of bypassing antivirus signatures.
(To apply malware inspection to other rules, you must enable this feature in the rule properties
telp ab	out malware inspection

در صفحه HTTPS Inspection Settings، چندگزینه برای انتخاب خواهید داشت:

گروہ آموزشے فےرزان

كزينه Allow users to establish HTTPS connections to Web sites

با فعال سازی این گزینه، Access Rule ایجاد شده توسط این ویزارد اجازه برقراری اتصالات از نوع HTTPS را به کاربران می دهد.

گزینه Inspect HTTPS traffic and validate HTTPS site certificates با انتخاب این گزینه اتصال SSL بین کلاینت و سرور، از سمت کارت شبکه کلاینت به TMG شکسته می شود و خود TMG این درخواست را به نیابت از کاربر به وب سرور مقصد می فرستد. علاوه بر آن اعتبار Certificate ارائه شده توسط وب سرور مقصد نیز توسط TMG مورد بررسی قرار می گیرد. اگر certificate ارائه شده از وب سرور مورد نظر توسط GMG مورد تأیید قرار نگیرد، اتصال برقرار شده خاتمه می یابد.

گروہ آموزشی فیرزان

www.Modir-Shabake.com

Do not inspect HTTPS traffic, but validate the HTTPS site كزينه certificateBlock HTTPS traffic if the certificate is not valid

اگر این گزینه را انتخاب کنید ترافیکهای HTTPS بازرسی نمی شوند، اما اعتبار Certificate ارائه شده توسط وب سرور مقصد مورد سنجش قرار می گیرد، اگر Certificate ارائه شده مورد تأیید نباشد، اتصال برقرار نمی شود

کزینه Do not inspect HTTPS traffic and do not validate HTTPS site certificates Allow all HTTPS traffic

با انتخاب این گزینه، هرچند اجازه ورود تمامی ترافیکهای SSL به شبکه شما داده می شود اما TMG به یک فایروال نا امن مبدل خواهد شد. چون ورود malware ها و اتصال به پروکسی های ناشناس به آسانی امکان پذیر بوده و کاربران و مزاحمان را قادر می سازد که با مخفی شدن در تونل SSL، سیاستهای امنیتی شبکه شما را دور زده و شبکه را با خطرات بسیاری روبرو کنند.

گروہ آموزشی فیرزان

-0-0-0

کوینه تمامی درخواستهای خروجی SSL را بلاک می کند، این گزینه تمامی درخواستهای خروجی SSL را بلاک می کند، هرچند امنیت بالایی را فراهم می کند اما اغلب پیاده سازی آن در محیط های عملی ممکن نمی باشد، چون بسیاری از سایتها با فرمت HTTPS hapection Settings Forefrort TMG can scan HTTPS traffic and block content that is not in compliance with policies and filters. Allow users to establish HTTPS connections to Web sites Allow users to establish HTTPS connections to Web sites Allow users to establish HTTPS traffic and validate HTTPS site certificate. Block HTTPS traffic if the certificate is not valid.

-0-0-0-0-0-0-0-0-0

O Do not allow users to establish HTTPS connections



Enabling HTTPS inspection may have legal implications. You should verify if using this protection is in compliance with your corporate policy.

Help about HTTPS inspection

< Back Next >

Cancel

در صفحه HTTPS Inspection Preferences، می توانید گزینه مورد نظر را به منظور اطلاع یا عدم اطلاع کاربران از بازرسی ترافیکهای HTTPS، انتخاب نمایید.

www.Modir-Shabake.com

No, do not notify users of HTTPS inspection كزينه

گروہ آموزشے فےرزان

با انتخاب این گزینه، کاربران شبکه از بازرسی ترافیکهای HTTPS مطلع نمی شوند.

گروہ آموزشی فیرزان

www.Modir-Shabake.com

Yes, notify users. To receive inspection notifications, users must have كزينه Forefront TMG Client installed and enabled on their computers

با انتخاب این گزینه، بازرسی و کنترل درخواستهای HTTPS، به کاربران اطلاع داده می شود. برای دریافت این notification، می بایست نرم افزار TMG Client روی سیستم کاربران نصب و فعال شده باشد. بنابراین زمانی که کاربران به سایتهای SSL یا HTTPS متصل می شوند، یک balloon که حاوی پیغام Inspect شدن ترافیکهای HTTPS است در system tray به کاربران نمایش داده می شود.

گروہ آموزشے فےرزان

گزینه Use a certificate automatically generated by Forefront TMG با انتخاب این گزینه، TMG به صورت اتوماتیک Certificate ایجاد خواهد کرد که در این Certificate به جای آدرس وب سرورهای SSL آدرس خود TMG جایگزین می شود، علاوه بر TMG می تواند جهت اعتماد کلاینتها به این Deploy Active Directory نماید.

گروہ آموزشے فےرزان

گزینه Use a custom certificate ای که خود اگر می خواهید به جای Certificate های SSL ای که خود TMG ایجاد می کند از Certificate هایی که PKI برای شما ایجاد خواهد کرد استفاده کنید، این گزینه را انتخاب نمایید.

كرينه هاى Yes, notify users. To receive inspection كرينه هاى notifications, users must have Forefront TMGClient Use a انتخاب مى their computers و installed and enabled on their computers certificate automatically generated by Forefront را انتخاب مى كنيم و روى Next كليك مى كنيم.

گروہ آموزشی فیرزان

Ó

Q

Web Access Policy Wizard
HTTPS Inspection Preferences Select if you want to notify users that HTTPS traffic is being inspected, and choose how to generate the HTTPS inspection certificate.
Do you want to display inspection notifications to users initiating HTTPS connections?
C No, do not notify users of HTTPS inspection
Yes, notify users. To receive inspection notifications, users must have Forefront TMG Client installed and enabled on their computers.
How do you want to create the certificate used to perform HTTPS inspection?
Use a certificate automatically generated by Forefront TMG
Use a custom certificate This option lets you customize the automatically generated certificate or select an alternate certificate.
Help about HTTPS inspection preferences
< Back Next > Cancel

گروہ آموزشی فیرزان

www.Modir-Shabake.com

در صفحه Certificate Deployment Preferences دو گزینه برای انتخاب وجود دارد:

Automatically deploy the certificate using Active Directory كزينه (recommended)

اگر بخواهید TMG به صورت اتوماتیک Certificate را در Deploy ، Active Directory کرده و آن را در محل مربوط به ذخیره Certificate بر روی کامپیوتر هر کلاینت نصب کند، این گزینه را انتخاب کنید. برای اجرای این عملیات، می بایست اطلاعات نام کاربری و رمز عبور Administrator دامین را به منظور دسترسی این ویزارد به Active Directory و Deploy شدن Certificate در آن، در اختیار داشته باشید. تبادل این تنظیمات جدید با Active Directory هاعت به طول می انجامد.
گروہ آموزشی فیرزان

گزینه: I will manually export and deploy the certificate انتخاب این گزینه توصیه نمی شود ولی در صورتی که نمی خواهید TMG به صورت اتوماتیک Certificate را برای شما Deploy کرده و می خواهید به صورت دستی Certificate ها را export نمایید، این گزینه را انتخاب نمایید.

Select how the HTTPS inspection deployed on client computers.	ces n trusted root certification authority (CA) certificate will be	
 Automatically deploy the certification 	ate using Active Directory (recommended)	
The certificate will be installed au must have domain administrator p Active Directory may take up to 8	itomatically in the certificate store of each client computer. privileges to run this operation. Replication of the new set 8 hours.	. You tings in
Domain administrator username:	administrator@farzan.com	
Domain administrator password:	•••••	
I will manually export and deploy Export the certificate to:	r the certificate	wse
lelp about <u>certificate deployment</u>		
	C Back Next >	Cano

در پنجره Define Cache Drives می توانید مقدار فضایی را که قصد دارید به Cache شدن وب سایتها اختصاص دهید، به MB مشخص کنید. در این قسمت، اطلاعاتی در خصوص میزان فضای موجود در دیسک و مقدار فضای آزاد نمایش داده می شود توجه داشته باشید که درایو مورد نظر می بایست با فرمت NTFS بوده و حداکثر اندازه Cache file ها می بایست MB باشد. (هرچند به طور کلی باید حداکثر فضای فایلهای A0 GB شده را کمتر از 40 GB در نظر بگیرید).

در اینجا MB 10-5 از فضای دیسک را به هر کاربر اختصاص داده ایم، اما ممکن است شما فضای کمتر یا بیشتری را برای این منظور در نظر بگیرید، به صورت پیش فرض مقداری برای Cache اختصاص داده نشده است.

گروہ آموزشیی فیرزان

برای فعال نمودن قابلیت Web Caching و اختصاص فضای لازم به آن، روی کلید Cache Drives button کلیک کرده و در قسمت (MB) مقدار فضای لازم را وارد کرده و روی کلید Set کلیک نمایید تا این مقدار فضا برای Caching اختصاص داده شود.

Web Access Policy Wizard	Define Cache Drives	×
Web Cache Configuration With caching configured, frequently accessed Web content is stored in the cache.	Cache Drives	
Configure cache drives used for Web caching:	Drive Type Disk Space Free Space Cache Si C: NTFS 20377 4530 0	ze
Server Cache Size (all disks) Free Space (all disks) Cache Drives 2008R2ENT 0 MB 4530 MB		
	Maximum cache size (MB): 100 Se	t
The first time you select this option, the wizard creates a Web caching rule enabling the caching of content requested from the Internet. <u>Help about Web caching</u>	Total disk space on NTFS drives (MB): 20377 Current total cache size (MB): 0	20
<pre> < Back Next > Cancel</pre>	OK Cancel	Apply

گروہ آموزشی فیرزان

بعد از مشخص کردن مقدار فضای لازم برای Cache فایلها، توجه داشته باشید که چک مارک گزینه Enable the default Web caching rule فعال شده است. همانطور که مشاهده می کنید مقدار مشخص شده به قسمت Cache Size، اضافه شده است.

برای مشاهده مقدار فضای اختصاص داده شده به Caching و مشاهده تنظیمات Cache، می توانید از طریق کنسول TMG، و با راست کلیک روی Web Access Policy، و انتخاب (Related)، و سپس Web Caching، و تنظیمات انجام شده را مشاهده کنید و یا از سمت راست کنسول TMG و از تب Tasks، گزینه Configure Web Caching، را انتخاب نمایید.

گےروہ آموزشے فےرزان

×

Web Access Policy Wizard

Web Cache Configuration

With caching configured, frequently accessed Web content is stored in the cache.

Enable the default Web caching rule

Configure cache drives used for Web caching:

Server	Cache Size (all disks)	Free Space (all disks)	Cache Drives
2008R2ENT	100 MB	4530 MB	
ne first time you se ontent requested fr elp about Web cach	lect this option, the wizard creation the Internet. Som the Internet.	ates a Web caching rule ena	bling the caching of
		< Back	Next > Cancel

اگر certificate شما با موفقیت Deploy شده باشد پیغام Automatic certificate deployment succeeded به شما نمایش داده می شود. به منظور تکمیل شدن ویزارد Web Access policy روی گزینه Finish، کلیک نمایید.

گروہ آموزشی فیرزان

Web Access Policy Wizard		×
	Completing the Web Access Policy Wizard	
	You have successfully completed the Web Access Policy wizard. Wh you click Finish, access rules applying this policy will be created and following settings will be applied:	the
	Access Rules Created: Blocked Web Destinations (with exceptions) Allow Web Access for All Users URL Filtering: Enabled Malware Inspection: Enabled HTTPS Inspec	Leway X
	Enabled Web Caching: Enabled Automatic certificate deployment succeeded.	
		ОК
KKH	To apply the configuration and close the wizard, click Finish.	
	< <u>B</u> ack Finish	Cancel

توجه: هر تغییری که در کنسول TMG ایجاد می کنید، دو گزینه Apply و Discard را به شما نمایش می دهد. به منظور اعمال تغییرات صورت گرفته می بایست بر روی گزینه Apply کلیک کنید. و



قبل از Apply کردن تغییرات اعمال شده، با اصطلاحات قسمتهای مختلف کنسول TMG آشنا شوید، از این پس برای اشاره به این قسمتها اصطلاحات مربوط به هریک را به کار خواهیم برد:

www.Modir-Sha	ibake.com	یسروہ آموزشیی فسرزان
Forefront TMG		_ID×
File Action View Help	r×⊛€€€⊒≣⊒®∄∦j∙⊧↓ M	enu and Toolbars
Microsoft Forefront Threat Managem Forefront TMG (TMG 1) Dashboard Monitoring Firewall Policy Web Access Policy	Forefront Notifi Threat Management Gateway 2010 Notifi Apply Discard To save changes and update the configuration	Firewall Policy cation Area Enterprise Ition, click Apply.
 E-Mail Policy Intrusion Prevention System Remote Access Policy (VPN) Networking System Logs & Reports Update Center 	All Firewall Policy Search P Examples A Name Action Protocols From / Listener Web Access Policy Group From / Listener From / Listener From / Listener	To C Users O <u>Content Types</u>
Nodes	nternal 1 Blocked Web Des 🚫 Deny 👯 HTTP 🚽 Internal	Botnet Gambling Gambling Malcous Phishing Pornography
	Constant Con	Computers Computers Computer Sets Computer Sets Computer Sets Computer Sets Computer Sets Computer Sets Computers C
1 1 1	Last Default rule O Deny & All Traffic S. All Networks (🚖 Al Networks (🥂 🕒 🗀 URL Categories
Jone		

قبل از اعمال این تغییرات، سرویس Firewall به راه اندازی مجدد نیاز خواهد داشت. در این ویزارد به شما توضیح داده شده است که فقط بعد از restart شدن سرویس Microsoft Forefront را تغییرات اعمال خواهند شد.

گروہ آموزشی فیرزان

(این سرویس را می توانید با انتخاب نود Monitoring و در تب Services، مشاهده کنید) دو گزینه برای انتخاب وجود دارد:

Save the changes, but don't restart the services كزينه

با انتخاب این گزینه، تغییرات ذخیره می شود اما سرویس فایروال restart، TMG نمی شوند. فقط بعد از اینکه به صورت دستی این سرویس را restart نمایید تغییرات اعمال خواهد شد.

گروہ آموزشے فےرزان

گزینه Save the changes and restart the services با انتخاب این گزینه، تغییرات ذخیره شده و سرویس فایروال restart می شود و این تغییرات بعد از restart شدن این سرویس، اعمال خواهند شد. ممکن است اعمال این تغییرات چند دقیقه به طول بیانجامد. هریک از سرویسهایی که Stop شده اند می بایست به صورت دستی start شوند.

گزینه Save the changes and restart the services را به منظور restart شدن سرویس فایروال و اعمال تغییرات ایجاد شده انتخاب کرده و روی گزینه OK کلیک نمایید.

www.Modir-Shabake.	گروہ آموزشی فیرزان com
Forefro	nt TMG Warning
<u> </u>	Changes will be applied only after the following services are restarted: Microsoft Forefront TMG Firewall
G	Save the changes, but don't restart the services The changes will be applied only after you manually restart the services.
C	Save the changes and restart the services Changes will be applied after the services restart. This may take several minutes. Any stopped services should be manually started.

در این پیغام، توضیح داده شده است که تغییرات اعمال شده توسط شما در Configuration Storage ذخیره خواهد شد و برای بررسی تغییرات به کار گرفته شده برای تمامی اعضای آرایه می توانید وضعیت Configuration Storage را بررسی کنید.

 $\bigcirc -\bigcirc -\bigcirc -\bigcirc -\bigcirc -\bigcirc$

-0-0-0

گروہ آموزشیی فیرزان

لازم به توضیح است زمانی که شما از سرور EMS برای مدیریت متمر کز بر روی آرایه ای از TMG های نسخه Enterprise یا Standalone (به TMG گفته می شود که به صورت مستقل در شبکه عمل می کند) استفاده می کنید، گزینه Configuration فابل مشاهده می باشد که چگونگی پیکربندی EMS و افزودن آرایه ای از TMG ها به آن را توضیح خواهیم داد.

0 - 0 - 0 - 0



گروه آموزشی فرزان

در پیغام فوق، توضیح داده شده است که تغییرات به وجود آمده در Configuration Storage ذخیره خواهند شد

با Configuration Storage و Array Member که مختص به EMS می باشد در فصل های بعدی آشنا خواهید شد، برای تست نمودن رول Web Access Policy، روی سیستم یکی از کلاینت های Workgroup، آدرس URL ایی که دسترسی به آن را Deny کرده ایم (برای مثال Gambling)، در بروزر وارد می کنیم، همانطور که مشاهده می کنید صفحه User name و Vassword نمایش داده شده است و اگر نام کاربری و رمز عبور کلاینتی که اجازه دسترسی به این URL را دارد، نداشته باشید، دسترسی به این URL را دارد، نداشته باشید،

🔗 New Tab - Windows Internet Explore			
http://www.gamblin	j.com/	🔻 🍫 🗙 🔽 Bing	
🚖 Favorites 🛛 🚖 🔊 Suggested Site	s 🔻 🙋 Get more Add-ons 🔻		
🔘 Connecting		🗄 🔻 🗟 👻 🖃	🖶 ▼ Page ▼ Safety ▼ Tools ▼
Reopen closed tabs View tabs that you've closed	Windows Security Connecting to 10.1.1.3.	int to do	about your browsing
Reopen Last Browsing Sessio	User name Password Domain: FARZAN Remember my	/ credentials	ı've copied from a webpage.
		OK Cancel Search with Bing a, Translate with Bing	

Ó

••••••

Ó

 \bigcirc

 \bigcirc

 \bigcirc

 \bigcirc

Ó

Э

 \bigcirc

 \bigcirc

0

--0

-0-0-0-0

گروہ آموزشی فیرزان

این مبحث قسمتی از مطالب مختص به کتاب الکترونیکی آموزش TMG 2010 که توسط گروه آموزشی فرزان تولید شده است، می باشد.

0 - 0 - 0 - 0 - 0 - 0

WWW.Modir-Shabake.com

