

# راهنمای استفاده از فورتنی گیت



مترجم: اشکان پزشکی

## مقدمه

فایروال ها یا دیواره های آتش یکی از اصلی ترین عناصر هر شبکه ای می باشند که امروزه اهمیت زیادی پیدا کرده اند. به همین ترتیب استفاده از فایروال های مناسب یکی از الزامات هر شبکه ای بدل گشته است و ادمین ها باید بتوانند بنا به درخواست سازمان های خود فایروال مناسب را پیشنهاد داده و با شناخت کامل اقدام به نصب و پیاده سازی آنها نمایند.

یکی از محبوب ترین UTM های حال حاضر بازار ایران فورتی گیت می باشد. که شرکت های متعدد و کلیدی اقدام به استفاده از این فایروال نموده اند. با تحقیقی مختصر متوجه شدم که هیچ مرجع فارسی جهت ارائه آموزش های مدون و منظم برای این دستگاه محبوب وجود نداشته و تمام منابع، سورس های خارجی می باشند. به همین دلیل تصمیم گرفتم با استفاده از دانش قبلی و کتاب **cookebook** فورتی گیت اقدام به تهیه یک کتاب آموزشی فارسی بنمایم. بعضی از فصول این کتاب نسبت به سورس اصلی ( انگلیسی ) که کمتر مورد استفاده کاربران قرار میگرفت حذف شده است همچنین در بعضی موارد بدلیل گنگ بودن سناریو مترجم اقدام به اضافه کردن توضیحات نموده است. شایان ذکر است کتاب حاضر قطعا دارای عیب و ایراد می باشد و مسلما پیشنهادات و انتقادات شما خواننده گان عزیز سبب بهبود این کتاب آموزشی می شود.

**کپی برداری و نشر مطالب این کتاب کاملا آزاد بوده و هیچ منع قانونی وجود ندارد. امید است سهم کوچکی در ارتقاء سطح علمی هموطنانم داشته باشم.**

جا دارد تقدیر و تشکر کنم ازدوستان عزیزم آقای مهندس علیرضا ترابی و آقای مهندس مرتضی سلیمانی که در تمام زمینه ها بعنوان حامی و راهنما بنده بودند. همچنین تشکر مخصوص از سرکار خانم شیرین بهروش که در تدوین این کتاب کمک شایانی به بنده نمودند. منتظر دریافت پیشنهادات و انتقادات شما هستم.

اشکان پزشکی

شهریورماه ۱۳۹۴

[Ashkanp@live.com](mailto:Ashkanp@live.com)

FortiNet یک کمپانی بزرگ چند ملیتی می باشد که در سال ۲۰۰۰ میلادی توسط دو بردار به نام های Ken و Michael Xie تاسیس شد. شایان ذکر است آقای Ken Xie بنیانگذار و مدیرعامل سابق NetScreen می باشد. تفکرات حاکم در شرکت فورتی نت طوری است که نفرات حاضر در شرکت باید تجربه ی بالایی در زمینه امنیت داشته و از نبوغ و استعداد خاصی برخوردار باشند. دفتر مرکزی این شرکت در حال حاضر در Sunnyvale ایالت کالیفرنیا می باشد. این شرکت یک رهبری جهانی در زمینه امنیت شبکه های کامپیوتری داشته و مبتکر در فلیدهای حفاظتی می باشد. این کمپانی فروشنده محصولات امنیتی بوده و راه حل های جامع و کاملی بر اساس نوع مشتریانش ارائه می دهد. به طوری که تجهیزات امنیتی تولید شده در این کمپانی در دیتاسنترها، مشاغل Enterprise و دفاتر کوچک و ... مورد استفاده قرار می گیرد. سیستم توزیع و پخش محصولات فورتی نت در سرتاسر دنیا گسترده می باشد و محصولات این شرکت توسط ۲۰ هزار پارتنری که وجود دارد به فروش می رسد. فورتی نت در زمینه UTM و امنیت شبکه های کامپیوتری رقابت نزدیکی را با محصولات دیگر شرکت ها از جمله Cisco، Sonic Wall، Check Point دارد. اگر سری به سایت فورتی نت بزنید با این شعار مواجه می شوید: " بزرگ ترین مأموریت ما آن است که نوآورانه ترین و بالاترین پلتفرم های امنیت شبکه را برای زیرساخت های IT فراهم کنیم." به گفته ی مدیران این شرکت آمریکایی محصولات تولیدی تمام سطوح مشاغل را پوشش می دهد از شرکت های کوچک تا دفاتر توزیع شده در سراسر دنیا. آنها اعتقاد دارند رهبری بازار را در اختیار داشته و تنها به تولیدات سخت افزاری فکر نمیکنند بلکه فراهم آوردن مکمل های امنیتی باعث می شود ریسک ها به کمینه مقدار خود برسند.

کمپانی فورتی گیت مدعی است که مشتریان هدف اصلی شرکت بوده و با توجه به توسعه روزافزون این شرکت باز هم رضایتمندی مشتریان از اهم اهداف شرکت می باشد.

محصول اصلی شرکت فورتی نت، Fortigate می باشد که شامل دو مدل فیزیکی و مجازی می باشد. این دستگاه شامل پلتفرم های زیر است:

- *Firewall*
- *Virtual Private Network*
- *Application Control*
- *Anti-malware*
- *Intrusion Prevention*
- *Web Filtering*
- *Vulnerability Management*
- *Anti-Spam*
- *Wireless Controller*
- *Wide Area Network Acceleration*

راه حل های مکمل فورتی گیت:

فورتی نت به شما پیشنهادات و سوسه انگیزی می دهد تا شبکه ای امن و مطمئن داشته باشید این راه حل ها مکمل دستگاه فورتی گیت بوده و این ابزارها در کنار یکدیگر تحفه ای درخور را برای شما به ارمغان می آورد:

- *Advanced Threat Protection (FortiSandbox)*
- *Web Application Firewall (FortiWeb)*
- *Secure Email Gateway (FortiMail)*
- *DDoS Protection (FortiDDoS)*
- *Application Delivery Controllers (FortiADC)*
- *User Identity Management (FortiAuthenticator, FortiToken)*
- *Endpoint Security for desktops, laptops and mobile devices (FortiClient)*
- *Wireless LAN and WAN (FortiWifi, FortiAP, FortiPresence, FortiExtender and more)*
- *Enterprise telephone systems (FortiVoice, FortiFone)*
- *And more....*



## تفاوت های سوئیچ مُد و اینترفیس مُد

این قسمت دربرگیرنده اطلاعاتی است که به شما کمک می نماید تا انتخاب کنید که فورتی گیتی از حالت Switch mode استفاده نماید یا خیر! این تصمیم باید قبل از استفاده از فورتی گیت گرفته شود.

### حالت Internal switch چیست ؟

حالت internal switch تعیین می کند که پورت های فیزیکی فورتی گیت توسط خود دستگاه مدیریت شوند.

دو حالت اصلی شامل Switch mode و Interface mode می باشند.

### Switch mode و Interface mode چه هستند ؟ و چرا مورد استفاده قرار می گیرند؟

در حالت Switch mode همه اینترفیس ها قسمتی از یک Subnet مشابه بوده و همانند یک اینترفیس تک دیده می شوند که به صورت پیش فرض lan یا internal نامیده شده که این نامگذاری بستگی به مدل فورتی گیت دارد. حالت switch mode وقتی مورد استفاده قرار می گیرد که طراحی شبکه ساده و ابتدایی بوده و به عبارتی اغلب کاربران در یک Subnet مشابه قرار دارند.

در حالت Interface، اینترفیس فیزیکی فورتی گیت به صورت کاملاً جدا استفاده می شود و هر اینترفیس IP آدرس خودش را خواهد داشت. تنظیمات اینترفیس ها می تواند بعنوان قسمتی از سخت افزار یا نرم افزار سوئیچ ها ترکیب شده و چندین اینترفیس جزئی از یک اینترفیس تک باشند. این حالت ایده خوبی است برای شبکه هایی که دارای Subnet های متفاوتی می باشند تا ترافیک شبکه قسمت بندی شود.

### کدام حالت بر روی فورتی گیت شما به صورت پیش فرض فعال است ؟

حالت پیش فرضی که بر روی فورتی گیت فعال خواهد بود بستگی به مدل دستگاه شما دارد. تعیین اینکه کدام mode بر روی دستگاه وجود دارد از طریق روش زیر امکان پذیر است :

**System> Network> Interface**

LAN یا Interface خود را تعیین نمایید. اگر اینترفیس موجود در لیست در ستون Type جزو physical interface ها قرار داد پس دستگاه شما در حالت Switch mode است. اگر اینترفیس یک Hardware switch است بنابراین دستگاه شما در حالت Interface قرار دارد.

Name	Type	IP/Netmask	Access	Administrative Status	Link Status
dmz	Physical	10.10.10.1 255.255.255.0	PING, HTTPS, HTTP, FMG-Access, CAPWAP	+	+
TEST	VLAN		PING, HTTPS, HTTP	+	
wan1	Physical		PING, FMG-Access, AUTO-IPSEC	+	1000Mbps/Full Duplex
NEDA_Internet	VLAN		PING, HTTPS, HTTP	+	
SHAHRAD	VLAN		PING, HTTPS, SSH	+	
wan2	Physical		PING, FMG-Access	+	+
internal (LAN)	Physical		PING, HTTPS, SSH, HTTP, TELNET	+	1000Mbps/Full Duplex

### چگونه می توانیم mode فورتی گیت را تغییر دهیم ؟

اگر شما در نظر دارید تا mode فورتی گیت را عوض نمایید ابتدا باید مطمئن شوید که هیچ کدام از پورت های فیزیکی که می خواهید بسازید به جایی در فورتی گیت ارجاع نشده اند ( جایی استفاده نشده اند ) . سپس مراحل زیر را طی نمایید:

#### System >Dashboard >Status

سپس دستورات زیر را در کنسول CLI وارد نمایید:

۱- دستوری که تغییر دهنده ی حالت switch mode فورتی گیت می باشد:

```
config
system global
set internal-switch-mode switch
end
```

۲- دستوری که تغییر دهنده ی حالت interface mode فورتی گیت می باشد:

```
config
system global
set internal-switch-mode interface
end
```

### اتصال یک شبکه داخلی به اینترنت با استفاده از حالت NAT/Route :

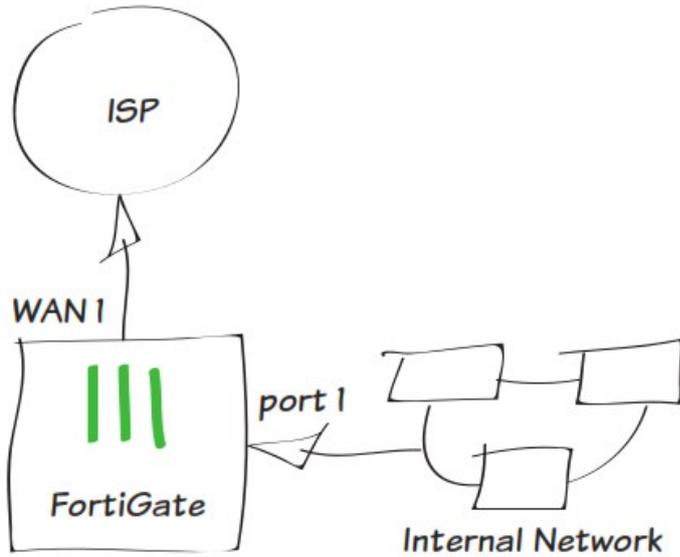
در این مثال، شما یاد می گیرید که چگونه تنظیمات لازم بر روی دستگاه فورتی گیت را انجام دهید تا یک شبکه داخلی را به صورت امن به اینترنت متصل نمایید.

در حالت NAT/Route، دستگاه فورتی گیت همانند یک Gateway یا روتر بین دو شبکه نصب می شود. در بیشتر موارد دستگاه بین یک شبکه داخلی و اینترنت بوده و مورد استفاده قرار می گیرد. این کار به فورتی گیت اجازه می دهد تا IP آدرس های شبکه داخلی را پنهان نموده و از Network Address Translation استفاده نماید.

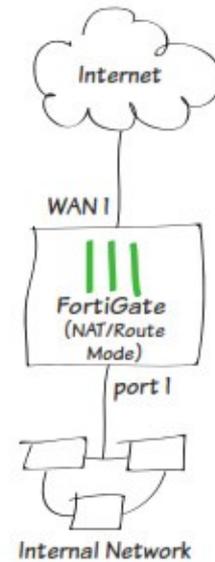
۱- اتصال دستگاه های شبکه به فورتی گیت و لاگین بر روی آن

۲- پیکربندی Configure اینترفیس های فورتی گیت

۳- اضافه کردن default route



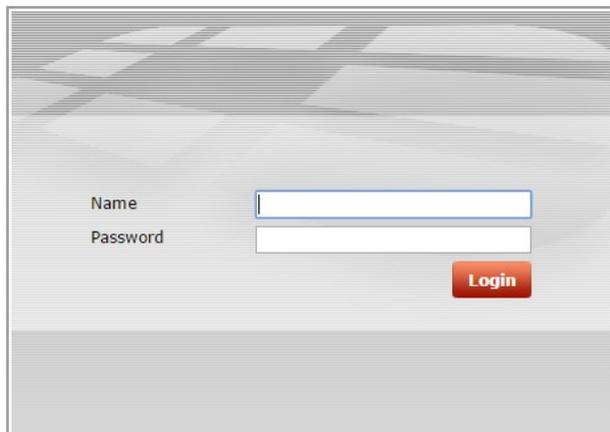
- ۴- انجام تنظیمات مربوط به DNS سرور فورتی گیت
- ۵- ساختن پالسی جهت خروج ترافیک داخلی به اینترنت
- ۶- نتایج



### ۱. اتصال دیوایس های شبکه و لاگین کردن بر روی فورتی گیت:

اینترفیس مربوط به اینترنت را به فورتی گیت متصل می نماییم ( معمولاً WAN1 ) همچنین یک کامپیوتر را به اینترفیس داخلی فورتی گیت متصل می نماییم ( معمولاً Port 1 ). اتصال مربوط را برقرار کرده و اینترنت را به فورتی گیت می دهیم.

از روی کامپیوتری که در شبکه داخلی می باشد با استفاده از یک مرورگر و به صورت وب بیس به فورتی گیت متصل می شویم . برای اتصال از اکانت admin استفاده می نماییم ( به صورت پیش فرض یوزرنیم admin بوده و پسوردی در نظر گرفته نشده است. )



Username=admin

Password=

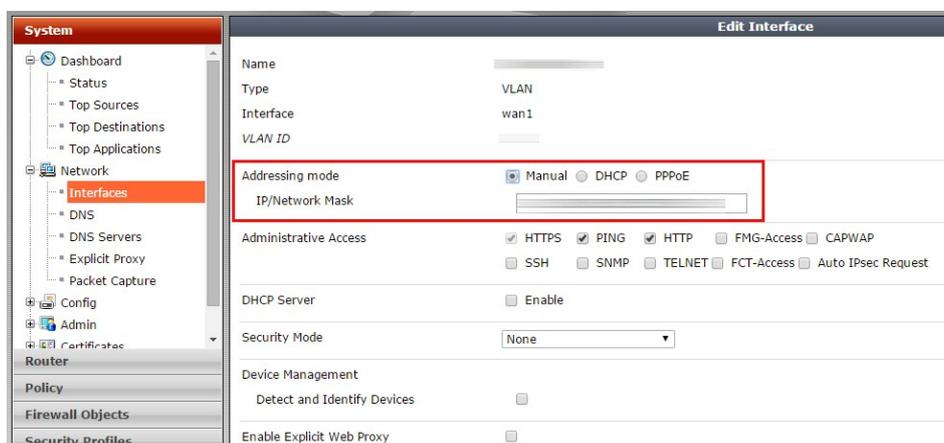
## ۲. تنظیمات مربوط به اینترفیس های فورتی گیت:

مسیر زیر را دنبال کنید :

### System> Network> Interface

اینترفیس مربوط به اینترنت را ویرایش edit نمایید.

در قسمت Addressing Mode گزینه Manual را انتخاب کرده و در فیلد IP/Netmask ، IP آدرس پابلیک خود را وارد نمایید



اینترفیس internal (داخلی) را ویرایش کنید( مثلا به صورت LAN نامگذاری کنید). در قسمت Addressing Mode گزینه Manual را انتخاب کرده و در فیلد IP/Netmask ، IP آدرس شبکه داخلی Private که می خواهید توسط این IP به فورتی گیت دسترسی داشته باشید را وارد نمایید.

## ۳. اضافه کردن Default route

مسیر زیر را جهت اضافه کردن route طی نمایید: ( بستگی به مدل فورتی گیت از مسیرهای زیر اقدام نمایید)

### Router >Static >Static Routers ( System> Network> Routing )

حالا یک route اضافه نمایید.

قسمت Destination IP/Mask به صورت 0.0.0.0/0.0.0.0 وارد نمایید. در قسمت Device اینترفیس مربوط به اینترنت را (WAN) انتخاب نموده و Gateway را بر اساس تنظیمات داده شده ISP وارد نمایید. ( برای وارد کردن Gateway باید IP مربوط به Gateway سرویس دهنده ی اینترنت "ISP" خود را وارد نمایید.) یا می توانید هاب روتر بعدی را بعنوان Gateway انتخاب نمایید. این موضوع کاملا به نوع شبکه شما بستگی دارد.

Destination IP/Mask	<input type="text" value="0.0.0.0/0.0.0.0"/>
Device	<input type="text" value="wan1"/>
Gateway	<input type="text" value="192.168.0.1"/>
Distance	<input type="text" value="10"/> (1-255, Default=10)
Priority	<input type="text" value="0"/> (0-4294967295)
Comments	<input type="text" value="Write a comment..."/> 0/255

**نکته:** یک Default route همیشه به صورت 0.0.0.0/0.0.0.0 می باشد. به صورت معمول شما می توانید تنها یک default route داشته باشید. لیست Static route به صورت پیش فرض شامل یک default route است که شما می توانید آن را edit ، delete و یا add نمایید.

### ۴. وارد کردن DNS سرور برای فورتی گیت ( اختیاری )

به صورت پیش فرض تنظیمات DNS های مربوط به دستگاه فورتی گیت بر روی سرورهای FortiGuard می باشد. این مورد برای اکثر شبکه ها کافی است. اگر شما دوست داشته باشید به راحتی می توانید DNS سرورهای خود را تغییر دهید.

مسیر زیر را طی نمایید:

### System >Network >DNS

و DNS های Primary و Secondary را وارد نمایید.

### DNS Settings

Use FortiGuard Servers  Specify

Primary DNS Server	<input type="text" value="208.91.123.53"/>
Secondary DNS Server	<input type="text" value="208.91.123.52"/>
Local Domain Name	<input type="text"/>

۵. ایجاد یک policy برای خروج ترافیک از LAN به WAN ( اجازه دسترسی منابع داخلی به استفاده از اینترنت )

مسیر زیر را جهت ساخت Policy طی نمایید:

### Policy & Object> Policy> IPv4

حال یک policy مطابق با شرایط زیر می سازیم :

- تنظیم کردن Incoming Interface بر روی اینترفیس internal (LAN) و تنظیم Outgoing interface بر روی اینترفیسی که اینترنت دارد.
- مطمئن شوید که Action بر روی Accept تنظیم شده است.
- NAT در حالت روشن تنظیم شود و اطمینان حاصل کنید که گزینه Use Destination Interface Address انتخاب شده باشد.

Incoming Interface	<input type="text" value="internal"/>	
Source Address	<input type="text" value="all"/>	
Source User(s)	<input type="text" value="Click to add..."/>	
Source Device Type	<input type="text" value="Click to add..."/>	
Outgoing Interface	<input type="text" value="wan1"/>	
Destination Address	<input type="text" value="all"/>	
Schedule	<input type="text" value="always"/>	
Service	<input type="text" value="ALL"/>	
Action	<input type="text" value="ACCEPT"/>	

**Firewall / Network Options**

NAT

Use Destination Interface Address  Fixed Port

Use Dynamic IP Pool

- در انتها گزینه Logging Options را خواهید دید. اگر تمایل دارید لاگ ها را بعدا مشاهده نمایید Log Allowed Traffic را فعال کرده و گزینه All Sessions را انتخاب نمایید.

## ۶-نتایج

بعد از انجام موارد بالا تمام کامپیوترهای داخل شبکه شما که در اینترفیس داخلی فورتی گیت هستند اینترنت خواهند داشت.

شما می توانید تمام اطلاعات در مورد Session ها و ترافیک ها را از طریق مسیر زیر مشاهده بفرمایید :

System> FortiView > All Sessions

همچنین می توانید ترافیک عبوری را همانند زیر فیلتر نمایید :

Src Interface = LAN

Dst nterface=WAN

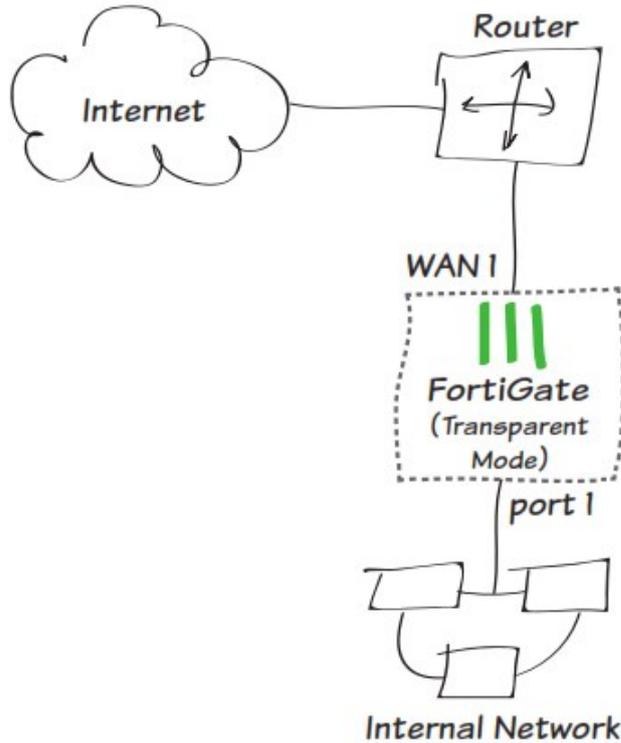
**اضافه کردن فورتی گیت در حالت Transparent بدون ایجاد تغییر در تنظیمات موجود:**

در این مثال شما یاد می گیرید که چگونه به یک دستگاه فورتی گیت متصل شده و تنظیمات را در حالت Transparent انجام دهید. در حالت Transparent فورتی گیت اسکن های امنیتی را بر روی ترافیک ها اعمال می نماید اما باید توجه داشت که route یا NAT صورت نمی گیرد.

**نکته:** تغییر به حالت Transparent باعث میشود تنظیمات صورت گرفته در حالت NAT/Route پاک شود. جهت نگهداری از تنظیمات NAT/Route، تهیه بکاپ از تنظیمات با استفاده از ویجت System Information صورت می گیرد. که می توانید از طریق زیر اقدام نمایید:

System> Dashboard> Status

- ۱- تغییر دادن حالت عملیاتی فورتی گیت
- ۲- تنظیم DNS سرورهای فورتی گیت
- ۳- ساختن Policy جهت عبور ترافیک شبکه داخلی به اینترنت
- ۴- اتصال دستگاه های شبکه



اضافه کردن یک فورتی گیت در حالت Transparent بدون تغییر در تنظیمات موجود در شبکه

۱. تغییر در حالت عملیاتی فورتی گیت:

مسیر زیر را طی نمایید:

**System > Dashboard > Status > System Information widget  
Operation Mode > Change**

The screenshot shows the FortiGate web interface. On the left is a navigation menu with 'System' selected, containing 'Dashboard', 'Status', 'Network', 'Config', 'Admin', 'Certificates', and 'Monitor'. The main area displays a 'System Information' widget. At the top of the widget is a status bar for 'INTERNAL' with ports 1-7 and DMZ, WAN1, WAN2. Below this is a table of system information:

System Information	
Host Name	FortiGate60D [Change]
Serial Number	FGT60D4614068267
Operation Mode	NAT [Change]
HA Status	Standalone [Configure]
System Time	Tue May 12 20:44:18 2015 (192.168.168.2) [Change]
Firmware Version	v5.0,build0292 (GA Patch 9) [Update] [Details]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /1 in Total [Details]
Uptime	7 day(s) 23 hour(s) 30 min(s)

Operation Mode را به حالت Transparent ببرید. IP و Default Gateway که از طریق شبکه داخلی به دستگاه فورتی گیت متصل می شوید را وارد نمایید. حالا می توانید توسط GUI و با وارد کردن IP Management به فورتی گیت خود دسترسی داشته باشید. در این مثال شما می توانید با آدرس <http://172.20.120.122> به دستگاه دسترسی داشته باشید.

Operation Mode	Transparent ▾
Management IP/Netmask	172.20.120.122/255.255.255.0
Default Gateway	172.20.120.2

## ۲. وارد کردن DNS سرورها برای فورتی گیت:

دستگاه های فورتی گیت به صورت پیش فرض تنظیمات مربوط به DNS سرورهای خود را از FortiGuard می گیرند، این مورد در بیشتر شبکه ها صادق می باشد. هرچند، اگر شما بخواهید می توانید DNS سرورهای دلخواه خود را وارد نمایید:

**System> Network> DNS> add Primary Server and Secondary Server**

## ۳. درست کردن یک Policy برای ایجاد دسترسی جهت خروج ترافیک داخلی به بیرون (اینترنت):

مسیر زیر را طی نمایید:

**Policy & Objects> Policy> IPv4**

حال یک Policy جدید مطابق با تنظیمات زیر می سازیم:

Incoming Interface= (LAN) شبکه داخلی می باشد

Outgoing Interface= اینترنتی که بر روی اینترنت قرار دارد

**نکته:** به شما توصیه می کنیم فعلا از Security Profiles ها استفاده ننمایید تا زمانی که فورتی گیت را به

صورت کامل نصب و راه اندازی نمایید. بعد از نصب نهایی می توانید Security profile ها را اعمال کنید.

جهت داشتن لاگ کافی است در قسمت Log Allowed Traffic را فعال نمایید و گزینه All Session را

انتخاب نمایید

## ۴- اتصال دستگاه های شبکه:

مسیر زیر را طی نمایید:

**System> Dashboard> Status> System Resources widget**

اگر گزینه Shutdown را انتخاب نمایید دستگاه فورتی گیت خاموش خواهد شد.

همچنین شما از طریق مسیر زیر وارد محیط CLI شده :

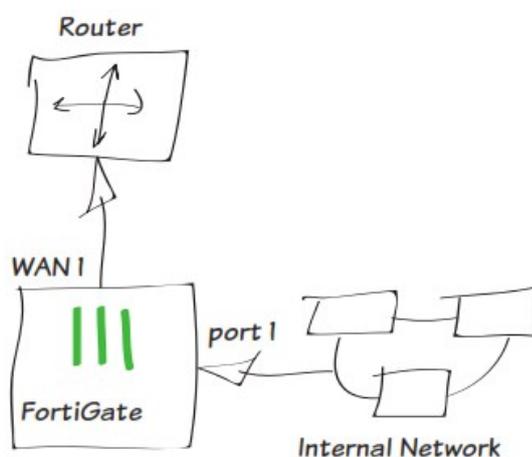
**System> Dashboard> Status> CLI Console**

و با دستور زیر می توانید دستگاه را خاموش نمایید:

## Execute shutdown



تا زمانی که تمام چراغ های روی پنل خاموش شوند ( به جز چراغ پاور ) صبر نمایید. اگر فورتی گیت شما دارای دکمه پاور می باشد جهت خاموش شدن دستگاه از آن استفاده نمایید در غیر این صورت دستگاه را از برق جدا نمایید.



شما می توانید دستگاه فورتی گیت را بین شبکه داخلی و روتر قرار دهید. اینترفیس WAN1 را به روتر داخلی متصل کرده و اینترفیس داخلی را به Port1 متصل نمایید. دستگاه فورتی گیت خود را روشن نمایید.

### ۵- نتیجه گیری:

تمام کامپیوترهایی که در شبکه داخلی به فورتی گیت متصل هستند باید اینترنت داشته باشند. شما می توانید اطلاعات مربوط به ترافیک پروسس شده توسط فورتی گیت و میزان بسته های دریافت و ارسال شده را از مسیر زیر مشاهده نمایید.

System> FortiView> All Sessions

### استفاده از یک لینک WAN برای Redundant اتصال های اینترنت

در این مثال، شما WAN لینکی خواهید ساخت که تامین کننده اینترنت دستگاه فورتی گیت بوده واز دو سرویس دهنده اینترنت تشکیل شده و اینترنت های ورودی را به صورت یک لینک Redundant تحویل می دهد. لینک WAN اینترفیس ها را ترکیب کرده و از دو کانکشن یک اینترفیس تحویل می دهد.

این مثال شامل Weighted Load Balancing است بنابراین بیشتر ترافیک اینترنتی شما توسط یک ISP منتقل میشود.

۱- اتصال ISP ها به فورتی گیت

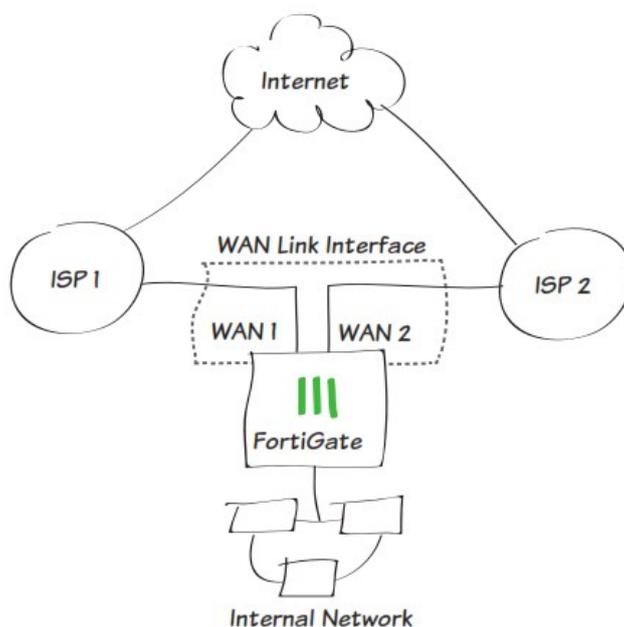
۲- پاک کردن Policy های امنیتی و route هایی که در WAN1 و WAN2 مورد استفاده قرار گرفته است.

۳- ساخت یک اینترفیس لینک WAN

۴- ساختن یک default route برای اینترفیس لینک WAN

۵- Allow کردن ترافیک داخلی جهت خروج از لینک WAN

۶- نتایج



۱. اتصال ISP ها به دستگاه فورتی گیت:

اتصالات مربوط به ISP ها را ایجاد کرده و ارتباطات آنها با فورتی گیت را برقرار نمایید. توجه داشته باشید در مثال ما ترافیک خروجی از WAN1 نسبت به WAN2 بیشتر می باشد.



۲. پاک کردن Security Policy ها و route های مورد استفاده در WAN1 و WAN2 :

اگر تنظیمات کنونی بر روی فورتی گیت مورد استفاده قرار گرفته باشد شما نمی توانید یک WAN لینک اینترفیس اضافه نمایید، بنابراین باید هر Policy و یا route هایی که روی هر دو لینک WAN1 و WAN2

قرار دارند را پاک نمایید. بعضی از مدل های فورتی گیت یک policy پیش فرض جهت دسترسی به اینترنت از طریق WAN1 دارند. این policy نیز باید پاک شود.

مسیر زیر را طی نمایید:

#### Policy & Objects> Policy> IPv4

حال تمام Policy هایی که مورد استفاده WAN1 و WAN2 می باشند را پاک نمایید.

بعد از اینکه Policy ها را پاک نمودید ترافیکی از سمت WAN1 و WAN2 به سمت فورتی گیت نخواهد آمد.

برای پاک کردن Route ها مسیر زیر را طی نمایید:

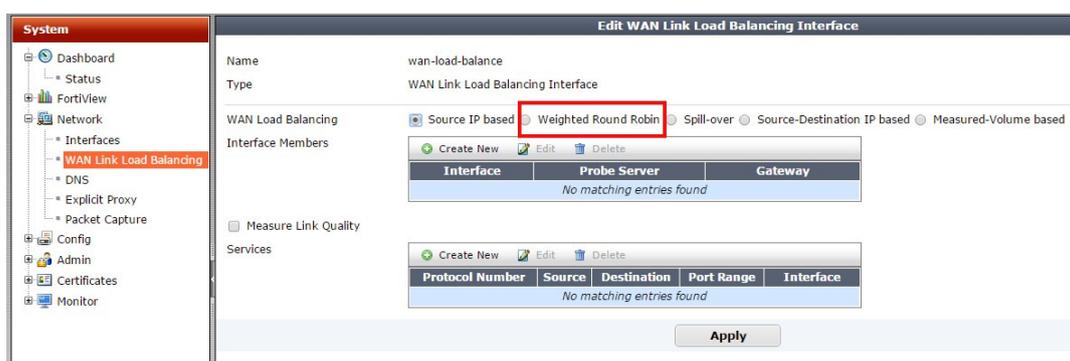
#### Router>Static>Static Routes> delete any route use in WAN1 & WAN2

### ۳. ساختن یک WAN لینک اینترفیس:

مسیر زیر را طی نمایید:

#### System> Network> WAN Link Load Balancing

در قسمت WAN Load Balancing گزینه Weight Round Robin را انتخاب نمایید. این گزینه شما را قادر می سازد تا اولویت WAN1 را بالا برده و باعث شوید ترافیک بیشتری از WAN1 عبور نماید.



WAN1 را به لیست Interface Members اضافه کرده و برای Weight گزینه 3 را وارد نمایید و در قسمت IP Gateway ، IP مربوط به ISP خود را تایپ نمایید. دقیقاً همین مراحل را برای WAN2 طی نمایید. منتهی در قسمت Weight مقدار 1 را وارد کنید.

Interfaces	wan1
Weight	0
Gateway IP	172.20.120.2

تنظیمات وزن دهی باعث میشود که 75 درصد ترافیک مورد استفاده بر روی WAN1 و 25 درصد باقیمانده بر روی WAN2 قرار گیرد.

#### ۴. ساختن Default route برای لینک اینترنت WAN

مسیر زیر را طی نمایید:

**Router> Static> Static Routes>** افه می نمایم Default route

در قسمت Device باید WAN Link Interface را وارد نمایم.

#### ۵. Allow کردن ترافیک شبکه داخلی به بیرون از طریق WAN Link Interface:

مسیر زیر را طی نموده و یک Policy جدید می سازیم:

**Policy & Objects> Policy> IPv4**

در قسمت Incoming Interface دست مربوط به شبکه داخلی ( اینترنتی که شبکه داخلی را میبیند ) را اضافه می کنیم و در قسمت Outgoing Interface دستی که در WAN می باشد را اضافه می کنیم. در آخر گزینه NAT را روشن می نمایم.

Destination IP/Mask	<input type="text" value="0.0.0.0/0.0.0.0"/>
Device	<input type="text" value="wan-load-balance"/>
Distance	<input type="text" value="10"/> (1-255, Default=10)
Priority	<input type="text" value="0"/> (0-4294967295)
Comments	<input type="text" value="Write a comment..."/> 0/255

Incoming Interface	lan
Source Address	all
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	wan-load-balance
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
<b>Firewall / Network Options</b>	
<input checked="" type="checkbox"/> NAT	
<input checked="" type="checkbox"/> Use Destination Interface Address	<input type="checkbox"/> Fixed Port

جهت مشاهده نتایج در آینده و همچنین ثبت وقایع نیاز به لاگ گیری می باشد که با استفاده از روشن کردن گزینه Log Allowed Traffic و انتخاب گزینه All Sessions این امر امکان پذیر می شود.

### ۶. نتایج:

حال شبکه داخلی شما دارای اینترنت می باشد و شما می توانید با باز کردن چند سایت آن را آزمایش نمایید با طی کردن مسیر زیر :

#### System> FortiView> All Sessions

ستون مربوط به Dst Interface در قسمت ترافیک لاگ مشاهده می گردد. اگر این گزینه دیده نمی شود، روی ستون قسمت راست، کلیک کرده و گزینه Dst Interface را از منو مربوطه انتخاب نمایید و سپس دکمه apply را انتخاب نمایید. لاگ ها نشان دهنده آن است که ترافیک از هر دو WAN1 و WAN2 عبور می نماید.

#	Src Interface	Src	Dst Interface	Bytes (Sent/Received)
1	lan	192.168.200.114:54819	wan2	50,909
2	lan	192.168.200.114:54835	wan1	50,839
3	lan	192.168.200.114:54803	wan2	69,529
4	lan	192.168.200.114:54787	wan1	257,587
5	lan	192.168.200.114:54891	wan1	1,971
6	lan	192.168.200.114:54987	wan2	1,436
7	lan	192.168.200.114:54931	wan1	3,086

WAN1 را قطع و امتحان کنید که اینترنت کلاینت ها متصل می باشد یا خیر؟ قطعاً اینترنت وصل بوده و با مشاهده لاگ، شما متوجه می شوید که تمام ترافیک از طریق WAN2 منتقل می گردد.

## راهنمایی های ویژه: T-shoot کردن نصب و راه اندازی :

اگر دستگاه فورتی گیت بعد از نصب و راه اندازی کارایی مورد نظر را ندارد از روش های زیر جهت رفع عیب و ایراد اقدام نمایید.

بیشتر روش های معرفی شده در هر دو حالت Route/NAT و Transparent مورد استفاده قرار می گیرد. هر گونه استثنایی مشخص شده است.

### ۱- اگر با استفاده از Ethernet نمی توانید به دستگاه متصل شوید از FortiExplorer استفاده کنید.

اگر توسط CLI یا GUI نمی توانید به فورتی گیت متصل شوید. ممکن است توسط FortiExplorer بتوانید به دستگاه متصل شوید. برای دریافت اطلاعات بیشتر از QuickStart دستگاه فورتی گیت ( دفترچه راهنما) کمک بگیرید.

### ۲- چک کردن تجهیزات.

بررسی کنید که تمام تجهیزات مرتبط با شبکه روشن و درست در حال کار می باشند. بر اساس راهنمایی های مشخص شده در Quickstart تجهیزات را به فورتی گیت متصل نمایید. همچنین اطلاعاتی در مورد وضعیت چراغ های LED دستگاه بدست بیاورید.

### ۳- چک کردن وضعیت اتصالات فیزیکی شبکه.

کابل های متصل شده را به صورت کامل چک نمایید و مطمئن شوید که کابل های استفاده شده صدمه ( زخمی ) ندیده باشند. اطمینان حاصل نمایید که کابل های ارتباطی با سایر دستگاه ها درست و دقیق ارتباط برقرار کرده باشند. همچنین ویجت عملیاتی را از طریق **System > Dashboard > Status** چک نمایید، مطمئن شوید که ارتباط اینترفیس ها در حالت سبز باشد.

### ۴- بررسی نمایید که از طریق IP آدرس شبکه داخلی می توانید به دستگاه فورتی گیت متصل شوید.

(Route/NAT mode)

از طریق کنسول وب و با IP دستگاه به فورتی گیت متصل شوید. سعی کنید IP دستگاه را PING نمایید. به صورت پیش فرض IP دستگاه 192.168.1.99 می باشد.

اگر نمی توانید به دستگاه متصل شوید، IP مربوط به PC خود را چک نمایید. اگر PING دستگاه را داشته ولی نمی توانید به صورت وب به کنسول مدیریتی فورتی گیت متصل شوید چک نمایید که تنظیمات مربوط به Administrative Access روی اینترفیس درست باشد.

۵- بررسی نمایید که اتصال به Management IP Address دستگاه فورتی گیت در حالت Transparent وجود دارد.

از شبکه داخلی، Ping مربوط به Management ip را بگیرید. اگر Ping را نداشتید تنظیمات مربوط به ip روی PC خود را چک نمایید و وضعیت اتصال کابل ها به سوئیچ ها را بررسی کنید. وقتی می توانید به مرحله بعدی بروید که اتصال به شبکه داخلی را داشته باشید.

۶- بررسی تنظیمات اینترفیس فورتی گیت.

بررسی می کنیم که اینترفیس فورتی گیت به شبکه داخلی متصل و همچنین تنظیمات مربوط به اینترفیس اینترنت درست و اتصالات برقرار باشد. همچنین IP آدرس ها به درستی وارد شده باشد.

۷- تنظیمات مربوط به Security Profile ها را بررسی نمایید.

از مسیر **Policy & Object > Policy > IPv4** بررسی کنید که Policy مربوط به دست داخلی ( اینترفیس شبکه داخلی ) به دست اینترنت ( اینترفیس مربوط به اینترنت ) به درستی اعمال شده باشد. ستون مربوط به Session ها را چک نمایید و مطمئن شوید که ترافیک به درستی پردازش می شود. ( عبور می نماید ) اگر شما از حالت Route/NAT استفاده می نمایید، تنظیمات مربوط به Policy ها را چک نمایید از روشن بود NAT اطمینان حاصل کنید. همچنین تیک گزینه **Use Destination Interface Address** خورده باشد.

۸- بررسی نمایید که دست اینترنتی دستگاه به اینترنت متصل است.

IP آدرس تنظیم شده بر روی دست اینترنتی دستگاه فورتی گیت را Ping کنید. اگر نمی توانید به اینترفیس متصل شوید دستگاه فورتی گیت شما نمی تواند از شبکه داخلی به شبکه خارجی پکت ها را منتقل نماید.

۹- بررسی تنظیمات استاتیک routing:

به مسیر **Router > Static > Static Routes** بروید و مطمئن شوید که Default Route درست است. در بخش Routing Monitor بررسی کنید که default route مشخص شده در لیست همانند یک استاتیک route می باشد. برای هر کدام از دست های فورتی گیت ( هر اینترفیس ) شما می توانید یک connected route ببینید.

۱۰- بررسی نمایید که اتصال با Gateway مربوط به ISP شما برقرار است.

بر روی شبکه داخلی IP آدرس مربوط به Default gateway را Ping نمایید اگر دسترسی به gateway امکان پذیر نیست با ISP خود هماهنگ شوید تا اطلاعات درست را وارد نمایید.

### ۱۱- بررسی نمایید که ارتباط دستگاه فورتی گیت با اینترنت برقرار باشد.

به CLI دستگاه فورتی گیت خود رفته و از دستور `execute ping 8.8.8.8` استفاده نمایید. شما می توانید جهت عیب یابی از وضعیت ارتباطی خود از دستور `execute traceroute 8.8.8.8` نیز استفاده نمایید.

### ۱۲- بررسی تنظیمات DNS دستگاه فورتی گیت و کلاینت ها

بررسی DNS Error ها از آنجا امکان پذیر می شود که شما یک آدرس را Ping می کنید و با جواب `name cannot be resolved` مواجه می شوید. دستگاه فورتی گیت یا PC ها نمی توانند به DNS سرورها متصل شوند و شما باید مطمئن شوید که آدرس DNS ها به درستی تنظیم شده است.

### ۱۳- از وصل بودن دستگاه فورتی گیت به FortiGuard مطمئن باشید.

یک بار که دستگاه رجیستر می شود تمام آپدیت ها از جمله `antivirus` و `application control` و غیره از شبکه FortiGuard گرفته می شود. دستگاه فورتی گیت تا زمانی در شبکه مفید است که بتواند در دسترس پذیری FortiGuard را تایید نماید. (با فورتی گارد در ارتباط باشد)

اولین قسمت، چک نمایید که اطلاعات مربوط به لایسنس دستگاه با فورتی گارد مطابقت دارد. به مسیر `System> Config> FortiGuard` بروید. گزینه `Web Filtering and Email Filtering Options` را باز نمایید و گزینه `Test Availability` را انتخاب نمایید. بعد از چند دقیقه، GUI به شما موفقیت اتصال را نمایش می دهد.

### ۱۴- تغییر دادن MAC Address اینترفیس خارجی (تغییر مک آدرس دست خارجی فورتی گیت):

بعضی از ISP ها بنا بر سیاستی که دارند تمایل دارند که MAC Address دستگاه های آنها به شبکه های کابلی خودشان متصل شوند بنا بر همین سیاست شما باید MAC Address دست اینترنتی دستگاه فورتی گیت خود را عوض نمایید که با استفاده از `Command` زیر در محیط CLI امکان پذیر است:

```
Config system interface
```

```
  Edit <interface>
```

```
    Set macaddr <xx:xx:xx:xx:xx:xx>
```

```
  End
```

```
End
```

## ۱۵- ریست کردن دستگاه فورتی گیت و بازگرداندن آن به حالت تنظیمات کارخانه ای :

اگر همه چیز با مشکل مواجه شده است! دستگاه فورتی گیت را ریست کرده و آن را به تنظیمات کارخانه ای بازگردانید. از طریق محیط CLI و با دستور `execute factoryreset` این اتفاق امکان پذیر می گردد. وقتی این دستور را می زنید باید تایپ کنید Y و اینتر را بزنید.

ریست کردن دستگاه آنرا به حالت Route/NAT باز میگرداند. با مراجعه به سایت [support.fortinet.com](http://support.fortinet.com) اطلاعات بیشتری کسب خواهید کرد.

## ثبت دستگاه فورتی گیت و تنظیمات مربوط به System Setting :

در این مثال شما یاد می گیرید که چگونه دستگاه خود را ریجستر کرده و زمان دستگاه را تنظیم نمایید. همچنین چند یوزر ادمین برای دستگاه ساخته و از دسترسی های غیرمجاز جلوگیری می کنیم.

۱- ثبت فورتی گیت

۲- تنظیم زمان دستگاه

۳- محدود کردن دسترسی ادمین از دستگاه های مجاز

۴- تغییر پسورد default admin

۵- نتایج حاصل

### ۱. دستگاه فورتی گیت خود را ثبت نمایید.

ثبت کردن دستگاه فورتی گیت به شما این امکان را می دهد که بروزرسانی ها را از FortiGuard دریافت نموده و همچنین امکان دریافت آپدیت firmware ها و دسترسی به ساپورت فورتی نت ایجاد می شود.

قبل از ثبت دستگاه فورتی گیت، حتما باید دقت کنید که دستگاه دارای اینترنت باشد.

مسیر زیر را طی نمایید:

**System> Dashboard> Status> License Information Widget**



Register this FortiGate with FortiCare by logging in or creating a new account

Serial Number: FG100D3G12812324

Action:  Login  Create Account

Email: vmartin@fortinet.com

Password: [Redacted]

Country: Canada

Reseller: Other

از یک اکانت ساپورت فورتی نت استفاده کنید یا یک اکانت جدید بسازید. کشور مورد نظر را انتخاب و Reseller را مشخص نمایید.

توصیه می کنیم جهت ثبت از یک اکانت معمول استفاده کنید.

بعد از رجیستر کردن دستگاه قسمت License Information شما باید همانند شکل زیر نمایش داده شود.



## ۲. تنظیمات ساعت دستگاه :

مسیر زیر را طی نمایید:

**System > Dashboard > Status > System Information widget**

گزینه system time را انتخاب کرده و گزینه change را بزنید. حال از قسمت time zone منطقه خود را انتخاب نمایید. توجه نمایید که وارد کردن دستی زمان نیر امکان پذیر می باشد. قابلیت دیگر وارد کردن NTP server می باشد.

System Information	
HA Status	Standalone [Configure]
Host Name	FG100D3G12801361 [Change]
Serial Number	FG100D3G12801361
Operation Mode	NAT [Change]
<b>System Time</b>	<b>Tue Aug 12 14:52:41 2014 [Change]</b>
Firmware Version	v5.2.0,buid595 (Interim) [Update] [Details]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /2 in Total [Details]
Uptime	22 day(s) 1 hour(s) 58 min(s)
Virtual Domain	Disabled [Enable]

۳- محدود کردن دسترسی ادمین از دستگاه های مشخص :

مسیر زیر را طی کنید:

### System> Admin> Administrator

تنظیمات مربوط به Admin را ادیت کنید . تیک گزینه Restrict this Admin Login from Trusted Hosts را بزنیید و آدرس IP دستگاه هایی که با آنها می خواهید به فورتی گیت متصل شوید را بزنیید.

Edit Administrator

Administrator:  Change Password

Type:  Regular  Remote  PKI

Comments:  0/255

---

Contact Info

Email Address

SMS  FortiGuard Messaging Service  Custom

Phone Number:

---

Enable Two-factor Authentication

---

Restrict this Admin Login from Trusted Hosts Only

Trusted Host #1:

Trusted Host #2:

Trusted Host #3:  +

---

Restrict to Provision Guest Accounts

با وارد کردن ساب نت 32/ تنها یک کامپیوتر را در Trusted Host قرار می دهید. اگر ساب نت را در حالت 24/ قرار دهید یک ساب نت را به صورت کامل در حالت Trusted Host قرار می دهید.

۴- تغییر دادن پسورد پیش فرض admin :

مسیر زیر را طی کنید:

## Admin> Administrator System>

تنظیمات مربوط به Admin را ویرایش کنید. گزینه Change Password را بزنید. فیلد Old Password را خالی بگذارید و در فیلد New password پسورد مورد نظر را وارد نمایید. به صورت خودکار بعد از انجام این تغییرات signed out می شوید و باید از پسورد جدید جهت وارد شدن استفاده کنید.

### ۵- نتایج :

سعی کنید با یوزر admin و بدون وارد کردن پسورد لاگین نمایید. مسلماً با جمله معروف Access is denied مواجه خواهید شد. حال با پسورد مرحله قبلی وارد شوید.

مسیر زیر را طی نمایید:

## System> Dashboard> Status

به قسمت Alert Message Console توجه نمایید، نمایانگر تعداد تلاش های ناموفق جهت لاگین به سیستم می باشد.

اگر دسترسی ها به صورت trusted host تعریف شده است، در صورتی که PC در لیست نباشد با پیغام device that is not trusted will be denied مواجه می شوید.

### به روز رسانی فریمور دستگاه فورتی گیت :

در این مثال نسخه ی فریمور فورتی گیت شما بررسی می شود و اگر نیاز باشد به آخرین نسخه ی موجود بروز رسانی می گردد. FortiOS سیستم عامل مورد استفاده در فورتی گیت می باشد. با آپدیت کردن FortiOS شما مطمئن می شوید که تمام ابزارها و امکانات امنیتی موجود بر روی دستگاه فورتی گیت به آخرین نسخه ارتقا پیدا کرده اند.

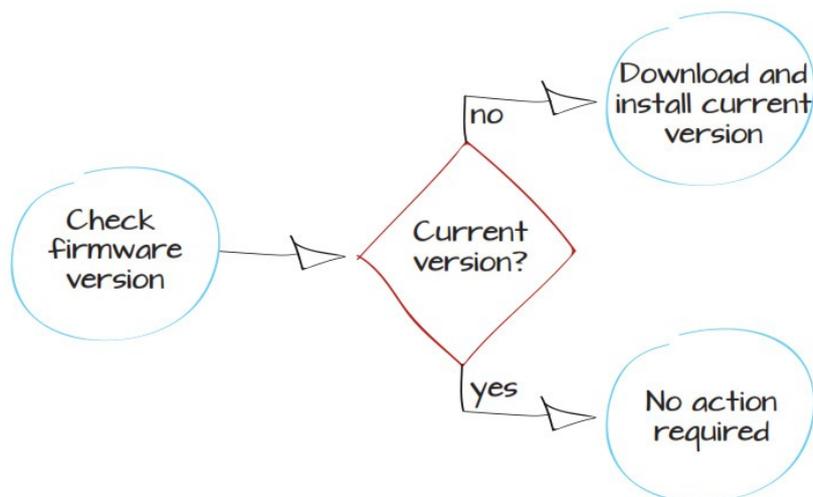
قبل از آپدیت فریمور جدید حتما نوت های مربوطه را مطالعه نمایید. این مستندات را می توانید از سایت فورتی گیت دانلود نمایید.

۱- فریمور FortiOS دستگاه را چک نمایید.

۲- آخرین نسخه مربوطه به FortiOS را دانلود نمایید.

۳- فریمور FortiGate را به آخرین نسخه آپدیت نمایید.

۴- نتایج



### ۱- فریمور حال حاضر دستگاه را چک می نماییم

با وب کنسول به دستگاه لاگین می کنیم و به مسیر زیر می رویم:

#### System> Dashboard> Status

گزینه System Information را بررسی می کنیم. در این قسمت می توانیم نسخه کنونی فریم ویر را مشاهده نماییم.

### ۲- دانلود آخرین نسخه فریمویر FortiOS

جهت دانلود آخرین نسخه فریمویر دستگاه باید به سایت <http://support.fortinet.com> مراجعه نموده و با استفاده از اکانت فورتی نت خود لاگین و آخرین نسخه را دانلود نمایید.

این نکته بسیار حائز اهمیت می باشد که قبل از اینکه شما بتوانید ایمپج مربوطه را دانلود نمایید حتما باید در سایت فورتی نت اکانت داشته باشید.

مسیر زیر را طی نمایید:

#### Download> Firmware Image

مدل فورتی گیت خود را انتخاب و بر اساس فریمویر موجود آنرا دانلود نمایید.

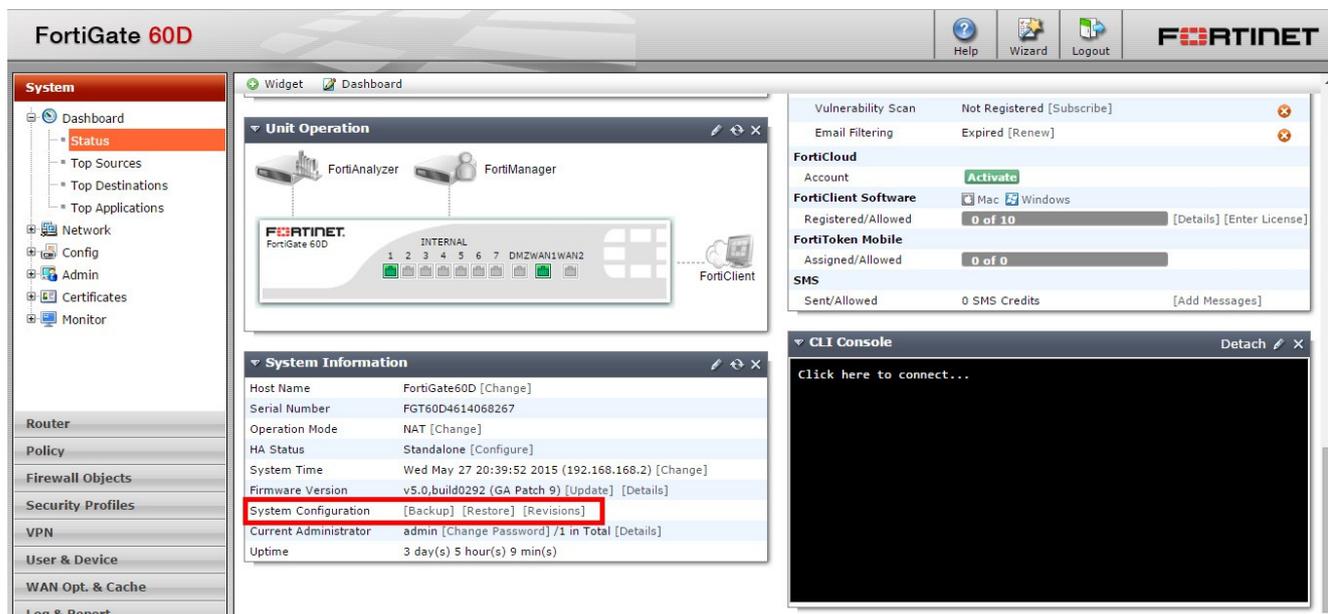
### ۳- آپدیت کردن فورتی گیت به آخرین نسخه ی موجود

#### System> Dashboard> Status

از تنظیمات خود بکاپ تهیه نمایید. این کار را می توانید از مسیر زیر میسر سازید :

#### System Information widget > System Configuration

این نکته را همیشه در ذهن داشته باشید قبل از انجام هر تغییری مخصوصاً آپدیت فریمویر حتماً از دستگاه Backup تهیه نمایید.



بعد از تهیه backup می توانید با خیالی آسوده نسخه فریمویر خود را از مسیر زیر آپدیت نمایید :

### System Information > Firmware Version > Update

بعد از کلیک بر روی update باید ایمجی دانلود شده در مراحل قبل را معرفی نمایید.

#### ۴- نتایج

وقتی فایل ایمجی بر روی فورتی گیت آپلود شد دستگاه ریستارت شده و صفحه لاگین فورتی گیت ظاهر می شود. این پروسه ممکن است چند دقیقه طول کشد.

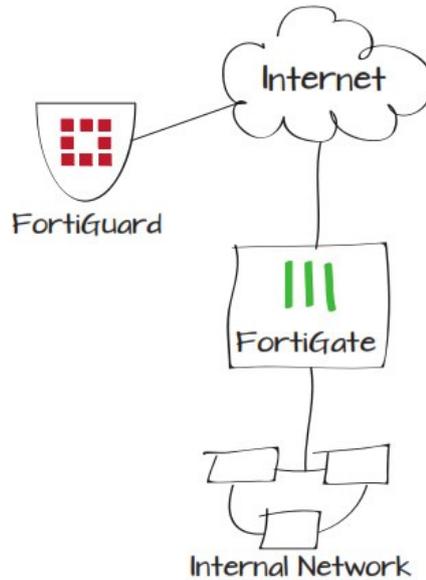
#### راه اندازی سرویس فورتی گارد FortiGuard

اگر سرویس فورتی گارد را خریداری کرده اید و این سرویس را بر روی فورتی گیت خودتان فعال نموده اید، فورتی گیت به صورت کاملاً خودکار به فورتی گارد متصل می شود و اطلاعات مربوط به لایسنس شما و سرویس های فورتی گارد را نمایش می دهد. در این مثال بررسی خواهیم کرد که آیا دستگاه فورتی گیت ارتباط لازم را با شبکه فورتی گارد دارد؟

۱- بررسی ارتباطات

۲- رفع مشکل ایرادات ارتباطاتی

۳- نتایج



## ۱. بررسی ارتباط

مسیر زیر را طی نمایید:

### System> Dashboard> Status > license Information widget

تمام سرویس ها باید دارای تیک سبز رنگ باشند. این نشان می دهد که ارتباطات با موفقیت برقرار شده است. اگر علامت خاکستری ضربدر وجود داشته باشد نشان می دهد که دستگاه فورتی گیت نمی تواند ارتباط درستی با شبکه فورتی گارد برقرار نماید. البته باید توجه داشته باشیم این علامت در صورت عدم ثبت دستگاه هم نمایش داده می شود. اگر دایره ای با رنگ نارنجی و ضربدر مشخص شده باشد نشان دهنده آن است که دستگاه فورتی گیت ارتباط را با فورتی گارد برقرار نموده است اما لایسنس منقضی شده و یا دستگاه اکتیو نشده است.

می توانیم وضعیت ارتباطی فورتی گارد را از مسیر زیر مشاهده نماییم :

### System> Config> FortiGuard

**System** FortiGate 500D FortiGuard Distribution Network

**Support Contract**

Registration	Registered	[Login Now]	✓
Hardware	8 x 5 support (Expires: 2016-04-08)		✓
Firmware	8 x 5 support (Expires: 2016-04-08)		✓
Enhanced Support	8 x 5 support (Expires: 2016-04-08)		✓

**FortiGuard Services**

**Next Generation Firewall**

IPS & Application Control	Licensed (Expires 2016-04-08)		✓ (2015-05-30)
IPS Definitions	6.00649 (Updated 2015-05-29 via Scheduled Update) [Update]		
IPS Engine	3.00073 (Updated 2015-03-27 via Manual Update)		

**ATP Services**

AntiVirus	Licensed (Expires 2016-04-08)		✓ (2015-05-30)
AV Definitions	25.00870 (Updated 2015-05-30 via Scheduled Update) [Update]		
AV Engine	5.00164 (Updated 2015-01-27 via Manual Update)		
Web Filtering	Licensed (Expires 2016-04-09)		✓

**Other Services**

Vulnerability Scan	Licensed (Expires 2016-04-08)		✓ (2015-05-27)
VCM Plugins	1.00380 (Updated 2015-05-27 via Manual Update) [Update]		
Email Filtering	Licensed (Expires 2016-04-09)		✓
Messaging Services	Registered (Expires 2016-04-15)		✓
SMS Messages	4 Allowed (0 Used)		

**FortiClient Information**

FortiGuard Availability	Reachable		✓
FortiClient Version (Mac)	5.2.3 (Updated 2015-05-30)		
FortiClient Version (Windows)	5.2.3 (Updated 2015-05-30)		

**SSL-VPN Package Information**

SSL-VPN Package Version	4.0.2300 (Updated 2015-04-28) [Update]		
-------------------------	--	--	--

**FortiToken Seed Server**

Registration	Unreachable (0 Tokens Registered)		✗
--------------	-----------------------------------	--	---

▶ AV & IPS Download Options  
▶ Web Filtering and Email Filtering Options

**Apply**

۲. رفع ایراد ارتباطت :

مسیر زیر را طی نمایید:

System> Network> DNS

مطمئن شوید که primary و Secondary سرور DNS درست کار می کنند.

#### DNS Settings

Use FortiGuard Servers  Specify

Primary DNS Server

Secondary DNS Server

Local Domain Name

Connected to FortiGuard

Web Filtering Licensed

Enable FortiGuard DDNS

اگر تست شما نشان داد که DNS سرور درست است مسیر زیر را طی کنید :

### System> Dashboard> Status

در محیط CLI دستورات زیر را وارد نمایید:

```
execute ping guard.fortinet.net
```

اگر ارتباط شما برقرار باشد، CLI کنسول باید چیزی شبیه به عکس زیر را به شما نمایش دهد:

```
CLI Console
Connected

FGT60C3G10016011 # execute ping guard.fortinet.net
PING guard.fortinet.net (208.91.112.196): 56 data bytes
64 bytes from 208.91.112.196: icmp_seq=0 ttl=52 time=62.3 ms
64 bytes from 208.91.112.196: icmp_seq=1 ttl=52 time=62.6 ms
64 bytes from 208.91.112.196: icmp_seq=2 ttl=52 time=61.5 ms
64 bytes from 208.91.112.196: icmp_seq=3 ttl=52 time=61.7 ms
64 bytes from 208.91.112.196: icmp_seq=4 ttl=52 time=61.3 ms

--- guard.fortinet.net ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 61.3/61.8/62.6 ms
```

اگر سرویس فورتی گارد در دسترس بود مسیر زیر را طی نمایید:

### Config> FortiGuard> Web filtering and Email Filtering

گزینه Test Availability را انتخاب نمایید. این گزینه به شما نمایش خواهد داد که کدام پورت ها باز هستند.

اگر پورت پیش فرض فورتی گیت 53 باشد نباید آن بلاک باشد . مسیر زیر را طی نمایید:

### System> Config> FortiGuard

در قسمت Web Filtering and Email Filtering Option گزینه ی Use Alternate Port 8888 را انتخاب نمایید.

### ۳. نتایج

در مسیر :

### System> Dashboard> Status > License Information Widget

به ازاء هر سرویسی که عضو آن هستید باید با تیک سبز رنگ نمایان شود. این نماد نشان می دهد که ارتباط برقرار بوده و لایسنس مورد تایید می باشد.

در مسیر :

### System> Config> FortiGuard

تمام امکانات و سرویس ها باید با تیک سبز رنگ نمایش داده شده باشند. این نماد نشان دهنده ی آن است که ارتباطات به صورت کاملا صحیح و بدون مشکل برقرار می باشد.

### کمک های ویژه: فورتی گارد

این قسمت حاوی نکاتی می باشد که به شما کمک می کند تا در چالش هایی که با فورتی گارد خواهید داشت موفق شوید.

### سرویس های فورتی گارد expired و یا unreachable می شود:

اول از همه بررسی کنید که آیا دستگاه فورتی گیت رجیستر شده است؟ سرویس های فورتی گارد خریداری شده اند؟ و آیا این سرویس ها Expire نشده اند؟!

### سرویس ها فعال هستند اما همچنان با پیغام Expired/Unreachable مواجه میشویم:

بررسی کنید که دستگاه فورتی گیت به اینترنت متصل است ؟ آیا دستگاه اینترنت دارد؟! برای اینکار کافی است در محیط CLI دستور زیر را تایپ نمایید:

```
Execute ping 8.8.8.8
```

دستور زیر هم می تواند در رفع عیب به شما کمک نماید :

```
Execute traceroute 8.8.8.8
```

### فورتی گیت به اینترنت متصل است اما نمی تواند ارتباطی با فورتی گارد برقرار نماید:

بررسی کنید که تنظیمات مرتبط با DNS درست باشد همچنین مطمئن شوید که یک Unblocked پورت برای ترافیک فورتی گیت مورد استفاده قرار گرفته است.

اگر اینترفیس فورتی گیت به اینترنت متصل است و از DHCP آی پی گرفته است به مسیر زیر بروید:

### System> Network> Interface

و دست مربوط به اینترنت ( اینترفیسی که اینترنت دارد ) را ویرایش نمایید. مطمئن شوید که گزینه Override internal DNS انتخاب شده است.

### خطاهای ارتباطی باقی مانده است !

دستگاه فورتی گیت با شبکه فورتی گارد به وسیله ارسال پکت های UDP با سورس پورت های 1027 یا 1031 ارتباط برقرار می نماید و پورت های مقصد 53 یا 8888 می باشند. بسته های بازگشتی دارای پورت های 1027 یا 1031 می باشند. اگر ISP شما پکت های UDP را در این رنج پورت بسته باشد دستگاه فورتی گیت نمی تواند بدرستی با فورتی گارد ارتباط برقرار نماید.

جهت مقابله با پورت بلاکینگ شما می توانید در دستگاه فورتی گیت خود از پورت نامبرهای بالا استفاده نمایید مثل 2048 یا 20000 و ... برای استفاده از این روش دستورات زیر را در محیط CLI وارد نمایید:

```
Config system global
Set ip-scr-port-range 2048-20000
End
```

اگر مشکلات حل نشد با ISP خود هماهنگ کرده و رنج پورتهای که بلاک نمی باشد را در فورتی گیت اضافه نمایید.

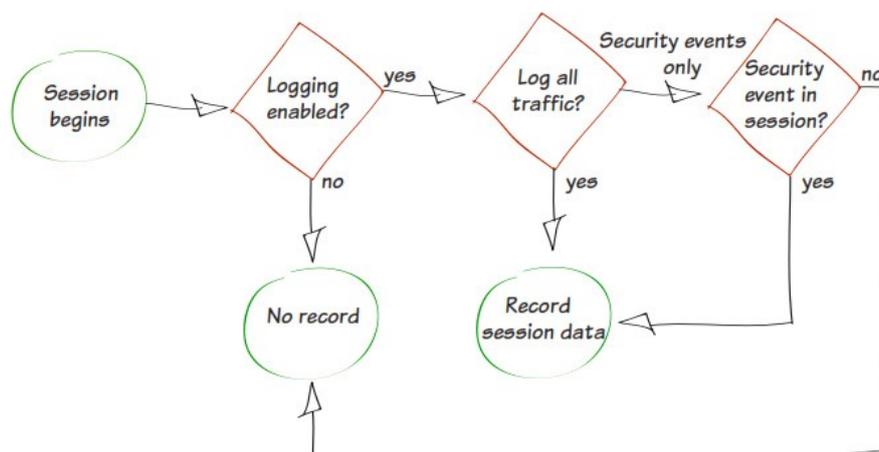
### جمع آوری اطلاعات از وضعیت ترافیک شبکه :

این مثال به شما نشان می دهد که چگونه قابلیت کپچر کردن ترافیک پروسس شده روی دستگاه فورتی گیت را فعال نمایید. کپچر کردن لاگ ها شرایطی را برای شما فراهم می کند که بتوانید در مورد شبکه خود یک دید مناسبی بدست بیاورید.

۱- رکورد کردن لاگ ها و فعال سازی event لاگ ها

۲- فعال سازی لاگ ها در Security policies

۳- نتایج



رکورد کردن لاگ ها و فعال سازی Event log ها

مسیر زیر را طی نمایید:

## Log & Report> Log Config> Log Settings

جایی که قرار است لاگ ها رکورد شود را انتخاب کنید. شما در صورتی می توانید لاگ ها را بر روی دیسک ذخیره نمایید که دستگاه فورتی گیت شما قابلیت ارسال لاگ ها را سمت یک فورتی آنالیزر یا فورتی منیجر داشته باشد. هر کدام از این انتخاب ها به شما اجازه می دهد تا لاگ ها ثبت و بازبینی شود همچنین بر اساس لاگ ثبت شده یک رپورت ایجاد نماید.

در بیشتر موارد، به شما توصیه می شود تا گزینه **Send Logs to FortiCloud** را همانند شکل زیر انتخاب نمایید.

**Log Settings**

**Logging and Archiving**

- Disk
  - Enable Local Reports
- Send Logs to FortiAnalyzer/FortiManager
  - IP Address:
  - Upload Option
    - Store & Upload Logs  at
    - Realtime
    - Encrypt Log Transmission
  - Send Logs to FortiCloud
    - Account:
- Event Logging
  - Enable All
  - Endpoint event
  - Router activity event
  - WiFi activity event
  - VPN activity event
  - System activity event
  - HA event
  - User activity event
  - Explicit web proxy event

**Local Traffic Logging**

- Log Denied Unicast Traffic
- Log Allowed Traffic
- Log Local Out Traffic
- Log Denied Broadcast Traffic

**GUI Preferences**

- Display Logs From:
- Resolve Hostnames (Using reverse DNS lookup)
- Resolve Unknown Applications (Using remote application database)

در مرحله بعدی، گزینه **Event Logging** را فعال نمایید.

شما می توانید با انتخاب گزینه **Enable all** همه نوع لاگ را ثبت نمایید، یا انواع مشخصی از لاگ ها ، همانند **WiFi activity events**، این مورد به نوع نظر شما بستگی دارد.

در قسمت **GUI Preferences** مطمئن شوید که گزینه **Display Logs From** اشاره به مقصدی میکند که لاگ ها در آنجا ثبت می شود.مثلا در **FortiCloud**.

## ۲. فعال سازی لاگ گیری در security policies:

مسیر زیر را طی نمایید: IPv4 Policy > Policy & Objects

ترافیک policy که در نظر دارید تا با لاگ کنترل نمایید مشخص کنید.

در قسمت Logging Options، می توانید یکی از گزینه های Security Events و یا All Sessions را انتخاب نمایید.

در بیشتر موارد، شما باید گزینه Security Events را انتخاب نمایید. گزینه All Sessions جزئیات کاملی از ترافیک را ثبت می نماید که این حالت باعث می شود منابع و فضای ذخیره سازی بیشتری از سیستم گرفته شود.

## ۳. نتایج

جهت نمایش ترافیک لاگ ها کافی است به مسیر زیر بروید:

Log & Report > Traffic Log > Forward Traffic Report > Traffic Log > Forward Traffic

لاگ ها اطلاعات مختلفی از ترافیک را نمایش می دهند، این لاگ ها شامل موارد چون تاریخ/زمان، مبدأ، دیوایس و مقصد می باشند.

جهت تغییر نوع نمایش اطلاعات می توانید روی یکی از ستون ها کلیک راست کرده و گزینه Column Settings را انتخاب نمایید تا بتوانید بعضی از ستون ها را فعال و یا بعضی دیگر را غیرفعال نمایید.

<input type="checkbox"/> OFF Web Filter	default
<input type="checkbox"/> OFF Application Control	default
<input type="checkbox"/> OFF IPS	default
<input type="checkbox"/> OFF Email Filter	default
<input type="checkbox"/> OFF DLP Sensor	default
<input type="checkbox"/> OFF VoIP	default
<input type="checkbox"/> OFF SSL/SSH Inspection	certificate-inspection
<b>Traffic Shaping</b>	
<input type="checkbox"/> OFF Shared Shaper	guarantee-100kbps
<input type="checkbox"/> OFF Reverse Shaper	guarantee-100kbps
<input type="checkbox"/> OFF Per-IP Shaper	client-guest
<b>Logging Options</b>	
<input checked="" type="checkbox"/> ON Log Allowed Traffic	
<input type="radio"/> Security Events	
<input checked="" type="radio"/> All Sessions	
<input type="checkbox"/> Capture Packets	
Comments	Write a comment... 0/1023
<input checked="" type="checkbox"/> ON Enable this policy	

#	Date/Time	Source	Device	Destination	Application Name	Security Action	Security Events	Sent
1	11:35:30	192.168.160.180		10.10.34.34	Browsec	Allowed	1	240 B /
2	11:35:29			54.164.135.208	DNS			74 B / 0
3	11:35:28			92.50.31.200	MS-SQL			1.06 KB
4	11:35:28			10.10.34.34	Browsec	Allowed	APP 1	240 B /
5	11:35:28			125.209.252.16 (legy.g.line-apps.com)	Naver.Line	Allowed	APP 1	906 B /
6	11:35:28			125.209.252.16 (legy.g.line-apps.com)	HTTPS			100 B /
7	11:35:28			23.61.199.131	DNS			85 B / 0
8	11:35:28			205.251.196.159	DNS			85 B / 0
9	11:35:28			60.210.10.52	DNS			77 B / 0
10	11:35:27			205.251.195.16	DNS			77 B / 0
11	11:35:26			54.153.30.23	DNS			77 B / 0
12	11:35:26			217.66.220.132	POP3			132 B /
13	11:35:26			37.77.52.44	DNS			74 B / 0
14	11:35:26			205.251.192.206	DNS			70 B / 2
15	11:35:25			101.227.169.106	DNS			62 B / 3
16	11:35:25			60.210.10.52	DNS			66 B / 0
17	11:35:25			92.50.31.200 (92.50.31.200.user.shahrad.net)	MS-SQL			1.01 KB
18	11:35:25			74.115.14.19 (den-oss-01.solarwinds.com)	DNS			64 B / 8

### ساختن یک Security Policies جهت ایجاد دسترسی به شبکه :

این مثال نشان می دهد که چگونه یک Security Policy ساخته و در Policy table اجرا شود. این Policy ها جهت اعمال سیاست های مختلف در شبکه نوشته و اجرا می شود.

در این مثال، سه پالیسی IPv4 کانفیگ خواهد شد. Policy A یک پالیسی کلی خواهد بود که به شبکه LAN اجازه دسترسی به اینترنت را می دهد. Policy B اجازه دسترسی به اینترنت را می دهد همراه با اعمال web filtering برای یک سری از موبایل دیوایس هایی که از طریق LAN به شبکه ما متصل هستند. Policy C به سیستم ادمین اجازه خواهد داد که فول اکسس دسترسی داشته باشد. (نام سیستم ادمین SysAdmin می باشد)

پالیسی چهارم، پالیسی default یعنی "deny" پالیسی می باشد. این پالیسی هم مورد استفاده قرار خواهد گرفت.

در این مثال، یک وایرلس نتورک هم تنظیم شده است که در یک Subnet مشترک همانند یک شبکه کابلی در LAN می باشد.

۱- تنظیمات Policy A تا به صورت عمومی دسترسی وب داده شود.

۲- ساختن Policy B تا به موبایل ها اجازه دسترسی داده شود.

۳- تعریف SysadminPC

۴- ساختن Policy C برای ایجاد اجازه دسترسی به SysadminPC

۵- ترتیب Policy Table

۶- نتایج

## ۱. تنظیمات Policy A برای دسترسی کلی به وب :

مسیر زیر را طی کنید:

### Policy & Objects> Policy> IPv4

بر اساس تمرینات قبلی پالیسی ایجاد نمایید که دسترسی به اینترنت و سرویس Http باز شود. در این پالیسی می توانید سرویس های Http و Https و DNS را باز نمایید.

مطمئن شوید که حالت NAT را Enable نموده اید.

پایین صفحه و در قسمت Logging Options. گزینه Log Allowed Traffic را ON کرده و All Sessions را انتخاب نمایید.

## ۲. ساخت Policy B و دسترسی دادن به دیوایس های موبایل

مسیر زیر را طی نمایید:

### Policy & Objects> Policy> IPv4

یک پالیسی جدید مطابق با تنظیمات زیر جهت ایجاد دسترسی برای کاربران موبایلی درست میکنیم .

Incoming Interface = LAN

Source Address= All

Source Device Type= Mobile Devices

Outgoing Interface= WAN (دست اینترنتی دستگاه)

Service= Http,Https,DNS

Enable NAT

### Logging Options

Log Allowed Traffic

Security Events

All Sessions

Capture Packets

در قسمت Security Profile گزینه Web Filter را روشن کرده و از پروفایل Default استفاده نمایید. این کار باعث می شود که قابلیت های Proxy Options و SSL Inspection فعال گردد. استفاده

از پروفایل default برای proxy options و SSL inspection اجازه می دهد تا ترافیک HTTPS توسط دستگاه مورد بازبینی قرار گیرد.

نکته: استفاده از قابلیت گروه دستگاه ها (Device Groups) باعث می شود تمام دیوایس های روی اینترفیس LAN به صورت اتوماتیک شناخته شوند.

مثل بقیه تنظیمات در Logging Options قابلیت Log Allowed Traffic را روشن کرده و گزینه All Sessions را انتخاب میکنیم.

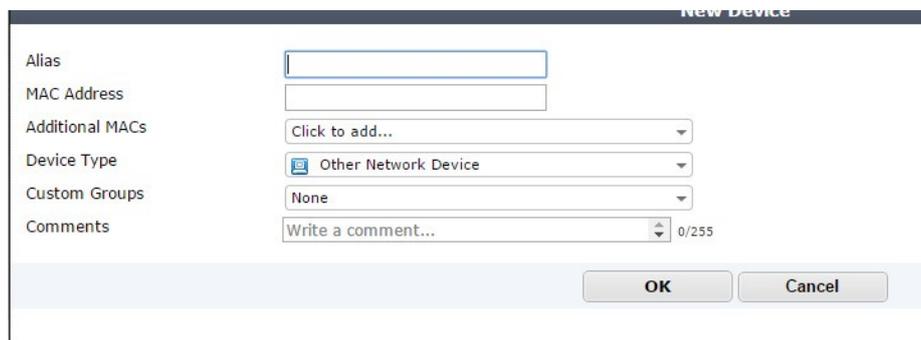
### ۳. تعریف کردن SysadminPC

مسیر زیر را طی نمایید:

#### User & Device> Device Definitaions

حال می توانیم یک PC از سیستم های ادمین ها در این قسمت اضافه نماییم .

گزینه Alias را انتخاب کرده و سپس MAC Address را وارد نمایید و در انتها نوع دستگاه خود را در فیلد Device Type مشخص نمایید.



### ۴. تنظیمات Policy C جهت ایجاد دسترسی برای SysAdminPC ها :

مسیر زیر را طی نمایید:

#### Policy & Objects> Policy> IPv4

یک پالسی جدید با شرایط زیر بسازید:

Incoming Interface= LAN

Source Device Type= SysAdminPC

Outgoing Interface= WAN

Service=All

Enable NAT

## ۵. ترتیب قرارگیری پالیسی ها

مسیر زیر را طی نمایید:

### Policy & Objects> Policy> IPv4

حال می توانید وضعیت جدول پالیسی را مشاهده کنید (Policy Table)

در حال حاضر پالیسی هایی که ساخته شده اند عبارت اند از : Policy A که در بالاترین نقطه قرار دارد. به دنبال آن Policy B قرار دارد و سپس Policy C و در انتها Default Deny Policy قرار دارد. به منظور ایجاد پالیسی های درست رعایت توالی و اولویت بندی آنها بسیار مهم می باشد. این نکته ضروری است که همیشه در نظر داشته باشید پالیسی ها به ترتیب قرارگیری اعمال میشود. بنابراین به خاطر داشته باشید که پالیسی های خاص همیشه در بالا قرار می گیرند.

Seq.#	From	To	Service	Web Filter	Devices
1	lan	wan1	HTTP HTTPS DNS		
2	lan	wan1	HTTP HTTPS DNS	default	Mobile Devices
3	lan	wan1	ALL		SysAdminPC
4	any	any	ALL		

جهت مرتب سازی مجدد پالیسی ها، هر قسمتی از ستون سمت چپ را که می خواهید انتخاب نمایید) در این مثال ما قسمت Seq.# را انتخاب کردیم). Policy B را انتخاب کرده و آن را در لیست بالا می آوریم به همین صورت می توانیم پالیسی ها را جابجا کرده و نتایج را مشاهده نماییم.

## ۶. نتایج

توسط سیستم ادمین و یک سیستم موجود در شبکه و یک موبایل دیوایس در اینترنت چرخی بزنید ( Browse Internet).

به مسیر زیر بروید:

### Log & Report>Traffic Log>Forward Traffic

می توانید ترافیک های عبوری که از پالیسی های مختلف عبور میکنند را مشاهده کنید.

## از پروتکل SNMP جهت مانیتور کردن دستگاه استفاده نمایید

پروتکل Simple Management Protocol (SNMP) جهت مانیتور کردن دستگاه های شبکه مورد استفاده قرار می گیرد. بوسیله انجام تنظیمات بر روی یک برنامه، مثل Fortigate SNMP agent که گزارش های مربوط به وضعیت و اطلاعات سیستم را به SNMP Managers ها ارسال می نماید.

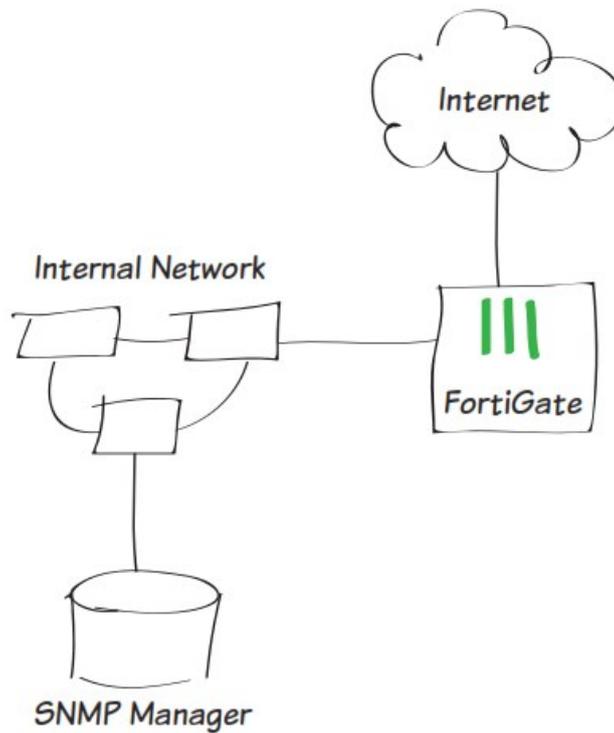
در این مثال، SNMP Agent مربوط به فورتی گیت به SNMP مربوط به Manager اجازه می دهد تا اطلاعات مربوط به سیستم را دریافت نماید.

۱. تنظیمات مرتبط با agent SNMP دستگاه فورتی گیت

۲. فعال سازی SNMP بر روی اینترفیس فورتی گیت

۳. دانلود کردن MIB فایل Fortinet و تنظیمات با یک SNMP Manager

۴. نتایج



۱. تنظیمات مربوط به SNMP agent

مسیر زیر را طی نمایید:

**System> Config> SNMP**

زیر قسمت SNMP v1/v2 گزینه Create New را بزنید تا یک community جدید ایجاد نمایید.

SNMP Agent  Enable

Description

Location

Contact

---

**SNMP v1/v2c**

<input type="checkbox"/>	Community Name	Queries	Traps	Enable
<input type="checkbox"/>	RD	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

---

**SNMP v3**

<input type="checkbox"/>	User Name	Security Level	Notification Host	Queries
<input type="checkbox"/>	RD	Authentication, No Private	<input type="text" value=""/>	<input checked="" type="checkbox"/>

---

**FortiGate SNMP MIB**

[Download FortiGate MIB File](#)

[Download Fortinet Core MIB File](#)

برای قسمت Hosts، آی پی آدرس مربوط به SNMP Manager را وارد نمایید. مثلا در مثال ما 192.168.1.114/32 می باشد. شما به راحتی می توانید چندین و چند SNMP Manager داشته باشید یا برای هر اینترفیس یک SNMP Manager داشته باشید تا با دقت عمل بیشتری شبکه را رصد نمایید.

SNMP Events هایی که نیاز دارید را فعال کنید. در بیشتر موارد تمام قسمت ها فعال می گردد.

**Hosts:**

IP Address/Netmask	Interface	Delete
192.168.1.114/255.255.255.255	ANY	

**Add**

**Queries:**

Protocol	Port	Enable
v1	161	<input checked="" type="checkbox"/>
v2c	161	<input checked="" type="checkbox"/>

**Traps:**

Protocol	Local	Remote	Enable
v1	162	162	<input checked="" type="checkbox"/>
v2c	162	162	<input checked="" type="checkbox"/>

**SNMP Events**

- CPU usage is high
  - Memory is low
  - Log disk space is low
  - Interface IP is changed
  - VPN tunnel up
  - VPN tunnel down
  - WiFi Controller AP up
  - WiFi Controller AP down
- 
- HA cluster status is changed
  - HA heartbeat failure
  - HA member up
  - HA member down
- 
- Virus detected
  - Matched file pattern detected
  - Fragmented email detected
  - Oversized file/email detected
  - Oversized file/email blocked
  - Oversized file/email passed
  - AV bypass happens</

**۲. فعال سازی SNMP بر روی اینترفیس فورتی گیت**

مسیر زیر را پیمایش کنید:

**System> Network> Interfaces**

گزینه Edit یک اینترفیس شبکه را بزنید. توجه داشته باشید که این اینترفیس باید در subnet ( شبکه) همان SNMP Manager باشد. در قسمت Administrative Access تیک گزینه SNMP را بزنید.

**۳. دانلود فایل MIB فورتی نت و تنظیمات یک SNMP Manager**

بر اساس SNMP Managerی که شما استفاده می نمایید، میتوانید MIB فایل مربوط به فورتی نت و فورتی گیت را دانلود و استفاده نمایید.

به مسیر زیر بروید:

**System> Config> SNMP**

MIB فایل های مربوط به فورتنی گیت و فورتنی نت را مانند شکل زیر دانلود نمایید.

SNMP Agent  Enable  
 Description Fortigate  
 Location PardisPars  
 Contact 021-88327832  
 Apply

**SNMP v1/v2c**

Create New Edit Delete

	Community Name	Queries	Traps	Enable
<input type="checkbox"/>	RD	✓	✓	<input checked="" type="checkbox"/>

**SNMP v3**

Create New Edit Delete

	User Name	Security Level	Notification Host	Queries
<input type="checkbox"/>	RD	Authentication, No Private		✓

**FortiGate SNMP MIB**

Download FortiGate MIB File

Download Fortinet Core MIB File

دو نوع از MIB فایل ها برای دستگاه های فورتنی گیت موجود می باشد.

۱. FortiGate MIB

۲. Fortinet MIB

FortiGate MIB فایل حاوی Traps و فیلدها و اطلاعات مخصوصی در مورد دستگاه می باشد.

Fortinet MIB فایلی حاوی Traps و فیلدها و اطلاعاتی که به صورت معمول در تمام محصولات فورتنی نت وجود دارد.

تنظیمات SNMP manager را بر 192.168.1.114 انجام داده تا trapsها را از دستگاه فورتنی گیت دریافت نماید. در صورت نیاز MIB فایل مرتبط با فورتنی گیت و فورتنی نت را نصب نمایید.

#### ۴. نتایج

در این مثال ما از Solarwinds جهت مشاهده SNMP Traps ها استفاده می نماییم. در برنامه Solarwinds در قسمت SNMP> MIB viewer را اجرا نمایید. Select Drive را انتخاب کرده و IP آدرس دستگاه فورتنی گیت را وارد نمایید و Community string مناسب را وارد کنید. در نرم افزار Solarwinds به قسمت SNMP Trap Receiver > Log Management رفته و گزینه Launch را انتخاب نمایید. در دستگاه فورتنی گیت، از طریق System > Event Log > Log & Report می توانید trapهایی که ارسال شده است را مشاهده نمایید.

cfgpath	system.interface	Date/Time	10:49:28 (Fri Mar 8 10:49:28 2013)
Virtual Domain	root	Level	information <span style="color: green;">✔</span>
Timestamp	Fri Mar 8 10:49:28 2013	cfgtid	2949201
logid	44547	Sub Type	system
User Interface	GUI(172.20.120.21)	User	 admin
Action	Edit	cfgobj	dmz
roll	65409	cfgattr	ip[10.10.10.99 255.255.255.0->10.10.10.1 255.255.255.0]
Message	Edit system.interface dmz		

استفاده از Port Forwarding برای ایجاد دسترسی های محدود به سرورهای داخلی :

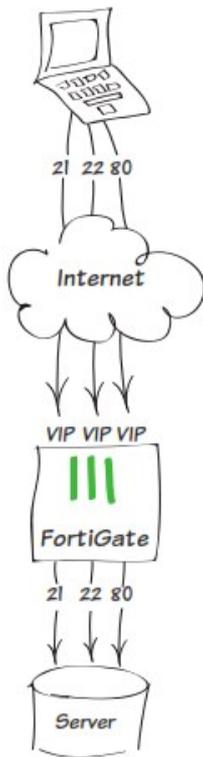
در این مثال ما به شما نشان می دهیم که چطور از Virtual IP برای تنظیمات Port Forwarding بر روی دستگاه فورتی گیت استفاده نمایید. در این مثال پورت 80 TCP و 21 FTP و 22 SSH باز هستند و یوزرهای بیرونی می توانند توسط این پورت ها به سرورهای داخلی ما دسترسی داشته باشند.

۱. ساختن Virtual IP

۲. اضافه کردن Virtual IP به VIP Group

۳. ساختن Security Policy

۴. نتایج



## ۱. ساخت Virtual IP

مسیر زیر را طی نمایید:

**Policy & Objects > Objects > Virtual IPs > Create New > Virtual IP**

Port Forwarding را فعال و برای TCP پورت 80 یک Virtual IP بسازید.

New Virtual IP	
Name	Web server
Comments	Write a comment... 0/255
Interface	WAN
Type	Static NAT
<input type="checkbox"/> Source Address Filter	
External IP Address/Range	0.0 [redacted] - 0.0 [redacted]
Mapped IP Address/Range	192.168.1.1 - 192.168.1.1
<input checked="" type="checkbox"/> Port Forwarding	
Protocol	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> SCTP <input type="radio"/> ICMP
External Service Port	80 - 80
Map to Port	80 - 80
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

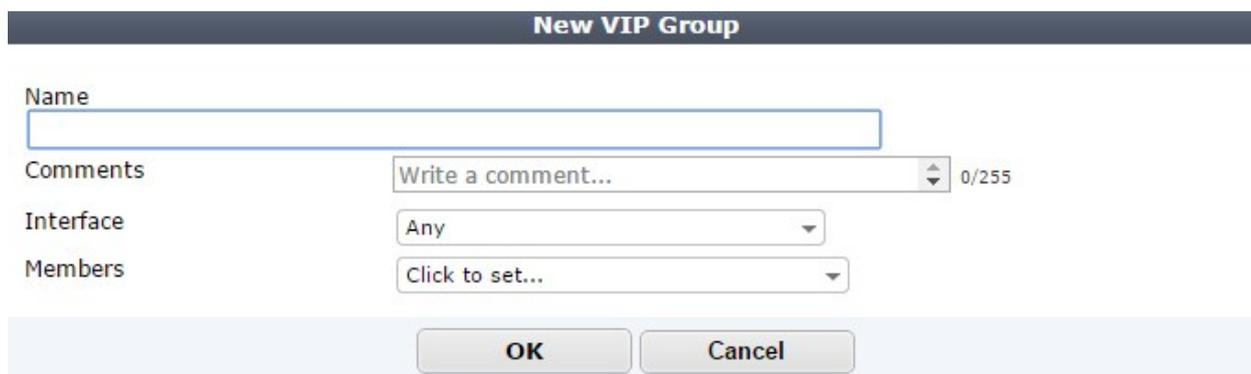
یک Virtual IP ثانویه برای پورت 22 می سازیم. در قسمت label اسم Webserver-SS را انتخاب میکنیم و برای سومی هم پورت 21 را برای FTP در نظر میگیریم.

### ۲. اضافه کردن Virtual IP به VIP group

مسیر زیر را طی نمایید:

Policy & Objects> Objects> Virtual IPs> Create New> Virtual IP Group.

یک VIP Group می سازیم.



The screenshot shows a dialog box titled "New VIP Group". It contains the following fields and controls:

- Name:** A text input field.
- Comments:** A text area with a character count of "0/255".
- Interface:** A dropdown menu currently set to "Any".
- Members:** A dropdown menu currently set to "Click to set...".
- Buttons:** "OK" and "Cancel" buttons at the bottom.

### ۳. ساخت یک Security Policy

مسیر زیر را پیمایش کنید:

Policy & Objects> Policy> IPv4

یک **Security Policy** بسازید که دسترسی به سرورها از پشت فایروال امکان پذیر باشد.

تنظیمات را مطابق با مشخصات زیر اعمال کنید:

**Incoming Interface = WAN** (دست اینترنتی فورتی گیت)

**Outgoing Interface = LAN** (دست داخلی که سرورها از آن ساب نت می باشند)

**Destination = VIP group**

**Service = Allow HTTP, FTP, SSH**

مسئما استفاده از **Security Profile** های مناسب از سرورهای شما محافظت خواهد کرد.

Incoming Interface	wan2	+
Source Address	all	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	internal1	+
Destination Address	Webserver	+
Schedule	always	
Service	HTTP X + FTP X SSH X	
Action	ACCEPT	

**Firewall / Network Options**

NAT  
 Web Cache  
 WAN Optimization

**Security Profiles**

<input checked="" type="checkbox"/> AntiVirus	default	+
<input type="checkbox"/> Web Filter	default	
<input type="checkbox"/> Application Control	default	
<input checked="" type="checkbox"/> IPS	default	+
<input type="checkbox"/> Email Filter	default	
<input type="checkbox"/> DLP Sensor	default	
<input type="checkbox"/> VoIP	default	
<input type="checkbox"/> ICAP	default	
Proxy Options	default	+
<input checked="" type="checkbox"/> SSL Inspection	default	+

#### ۴. نتایج

قبل از هر چیز مطمئن شوید که پورت TCP شماره 80 باز است و می توانید از بیرون فایروال با وب سرور ارتباط برقرار کنید. همچنین از باز بودن پورت های 22 و 21 مطمئن شوید.

#### قابلیت های امنیتی :

این فصل در مورد قابلیت های امنیتی دستگاه فورتی گیت شما صحبت می نماید. این قابلیت ها شامل آنتی ویروس، فیلترینگ وب، کنترل برنامه ها، IPS، ایمیل فیلترینگ و DLP می باشد.

هر قابلیت امنیتی یک پروفایل پیش فرض دارد. شما می توانید پروفایل های پیش فرض خود را ساخته و بر اساس ساختار و سیاست شبکه ی خود از آنها استفاده نمایید. پروفایل های ساخته شده قاعدتا عملیاتی می باشند و سیاست های امنیتی شما را پیاده سازی می نمایند همچنین جهت مانیتورینگ شبکه می توان از این

پروفایل ها استفاده نمود. اگر لازم شود ترافیک های داخلی و خارجی که تولید ریسک می کنند توسط این پروفایل ها بلاک می شوند.

این قسمت شامل دستورالعمل های زیر می باشد:

- کنترل کردن برنامه هایی که توانایی دستیابی به منابع شبکه و اینترنت را دارند.
- استفاده نمودن از قابلیت Static URL Filter جهت بستن دسترسی به وب سایت های مشخص
- هنگامی که از SSL Inspection استفاده میکنید اخطارهای امنیتی مربوط به گواهینامه امنیتی برای شما ظاهر نشود.
- استفاده از یک گواهینامه دلخواه برای SSL Inspection

**کنترل برنامه هایی که می توانند به منابع شبکه و اینترنت دسترسی داشته باشند**

در این مثال یاد می گیرید که چگونه از Application Control برای مشاهده ترافیک استفاده نمایید و متوجه شوید اگر برنامه ای نباید از اینترنت استفاده نماید چرا و چگونه در حال استفاده می باشد. هر برنامه ای که متضاد با سیاست های شماست را Block کنید. وظیفه ی خطیر Application Control برای آن است که شما مطمئن شوید برنامه های دلخواه تان نمی توانند به شبکه دسترسی داشته باشند.

۱. فعال سازی Application Control و چندین Security Profiles

۲. استفاده از Application پروفایل های پیش فرض برای مانیتور کردن ترافیک شبکه

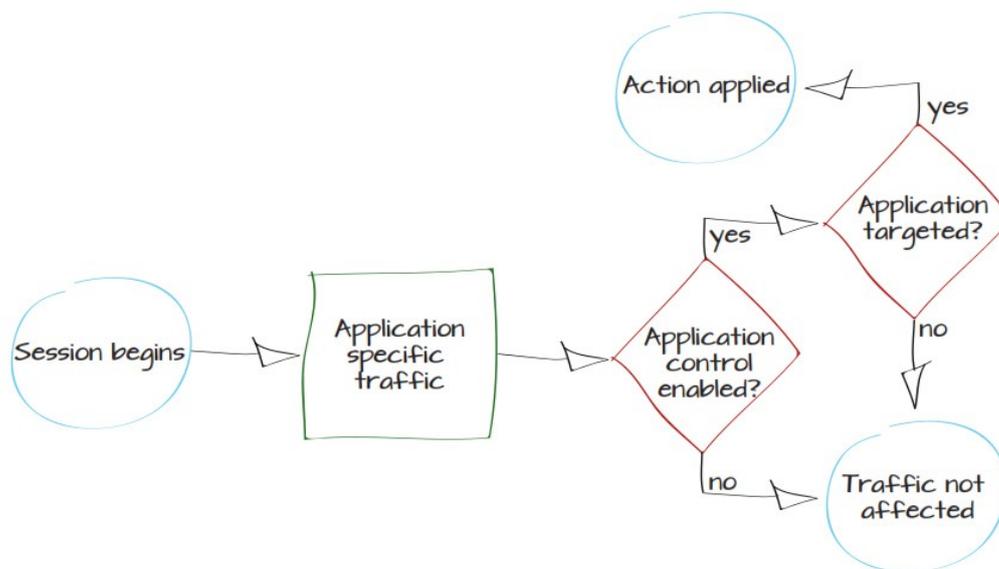
۳. اضافه نمودن Default Profile به یک Security Policy

۴. بررسی نمودن داشبوردهای Fortiview

۵. ساختن یک Application Profile برای لاک کردن برنامه ها

۶. اضافه نمودن Blocking Sensor به یک Security Policy

۷. نتایج

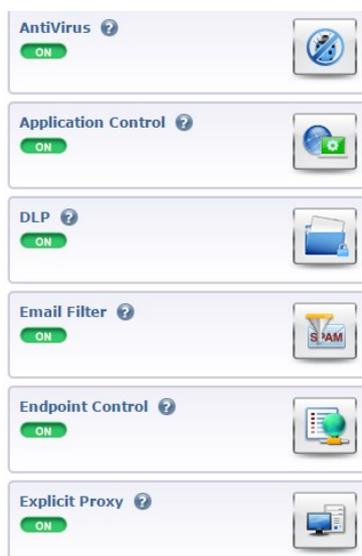


## ۱. فعال سازی Application Control

مسیر زیر را طی نمایید :

**System > Config > Features**

مطمئن شوید که Application Control روشن است .



گزینه Show More انتخاب کنید و Multiple Security Profiles را فعال سازید. تنظیمات اعمال شده را Apply کنید.

## ۲. استفاده از Default application Profile برای مانیتور کردن ترافیک شبکه

مسیر زیر را پیمایش کنید:

## Security Profiles> Application Control

پروفایل پیش فرض موجود را مشاهده می نمایید. یک لیست از برنامه های دسته بندی شده به نمایش گذاشته شده است. به صورت پیش فرض بیشتر دسته بندی انجام شده برای حالت مانیتورینگ تنظیم گردیده است. به منظور نظارت بر تمام اپلیکشن ها ، گزینه All Other Known Application را انتخاب نمایید و آنها را برای حالت مانیتور تنظیم کنید. همین کار را برای All Other Unknown Applications انجام دهید. در پروفایل پیش فرض قابلیت Deep Inspection of Cloud Applications روشن می باشد. این قابلیت به برنامه های تحت وب مثل Video Streaming اجازه می دهد توسط فورتی گیت مانیتور شوند.

### ۳. اضافه نمودن پروفایل پیش فرض به Security Policy

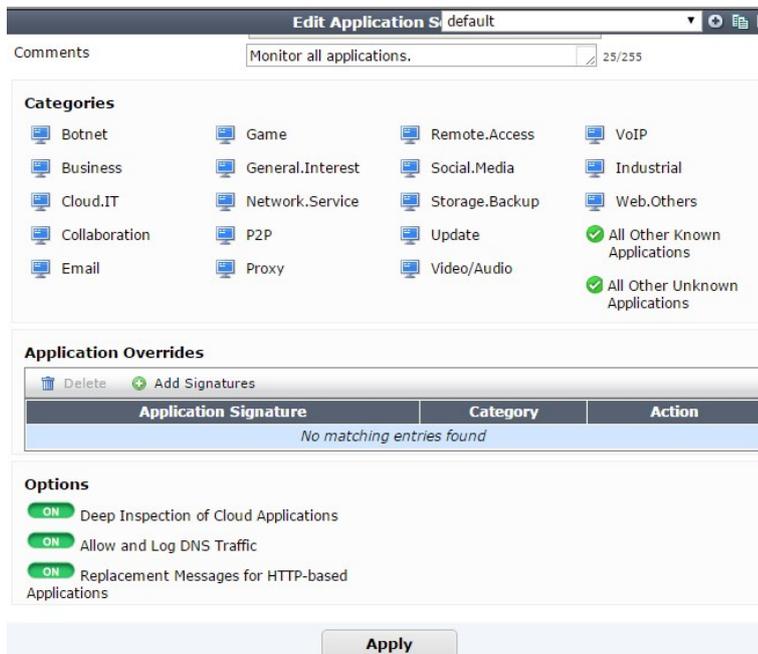
مسیر زیر را طی نمایید:

## Policy & Objects> Policy> IPv4

پالسی مربوط به دسترسی داخلی به اینترنت را ویرایش نمایید . در قسمت Security Profiles، گزینه Application Control را روشن کرده و از پروفایل Default استفاده نمایید. فعال سازی Application Control باعث خواهد شد قابلیت SSL Inspection هم به صورت خودکار فعال گردد. به منظور نظارت بر روی ترافیک Cloud Application ها پروفایل Deep-Inspection باید انتخاب شود.

### ۴. بررسی داشبورد FortiView

مسیر زیر را طی نمایید:



## System> Fortiview> Application

و گزینه Now view را انتخاب نمایید. این داشبورد ترافیکی که در حال حاضر از فورتی گیت عبور میکند را نمایش می دهد (دسته بندی بر اساس برنامه ها می باشد). اگر دوست دارید اطلاعات بیشتری در مورد ترافیک برنامه ها داشته باشید بر روی برنامه نمایش داده شده کلیک نمایید. ترافیک مبدا، ترافیک مقصد و اطلاعات کاملی درباره session ها بدست خواهید آورد.

Application	Category	Risk	Sessions	Bytes (Sent/Received)
Unknown			316	196.70 MB
SSL	Network.Service		6	129.61 KB
HTTPS.BROWSER	Web.Others		1	5.70 KB
QUIC	Network.Service		1	294.11 KB
Apple.iOS.Push.Notification	General.Interest		1	13.30 KB
WebSocket	Network.Service		1	279.63 KB
HTTP.BROWSER_IE	Web.Others		1	889 B
Teredo	Network.Service		1	313.34 KB
HTTP.BROWSER	Web.Others		1	850 B
Skype	Collaboration		1	41.04 KB

برای بدست آوردن اطلاعاتی مشابه از برنامه های **Cloud** می توانید به مسیر زیر رفته

#### System> Fortiview> Cloud Application

و اپلیکشین هایی که مورد استفاده قرار گرفته اند را مشاهده و مانیتور کنید. این قابلیت به شما این امکان را می دهد تا متوجه شوید چه ویدئوهایی دیده شده است البته این در شرایطی است که ترافیک Streaming Video شناخته شده باشد.

#### ۵. ساخت یک Application Profile برای بلاک کردن برنامه ها

در مثال بالا، شما فرض کنید ترافیک BitTorrent شناسایی شده است. حالا وقت آن است که با ساخت یک Application کنترلر که ترافیک P2P را بلاک میکند قدرت فایروال خود را به رخ بکشید.

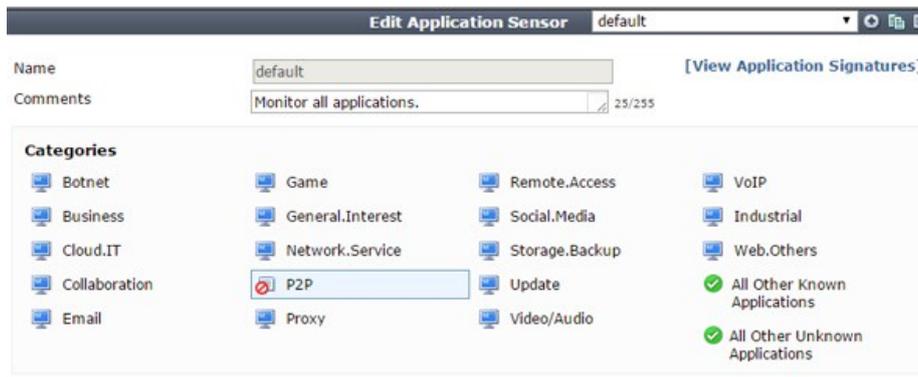
پروفایل جدید تمام برنامه های مرتبط با یوتیوب را هم بلاک خواهد کرد بدون اینکه تاثیر منفی بر روی بقیه ی برنامه های مربوط به Video/Audio بگذارد.

مسیر زیر را طی نمایید:

#### Security Profiles> Application Control

یک پروفایل جدید بسازید.

گروه مربوط به P2P را انتخاب کرده و آنها را Block نمایید.

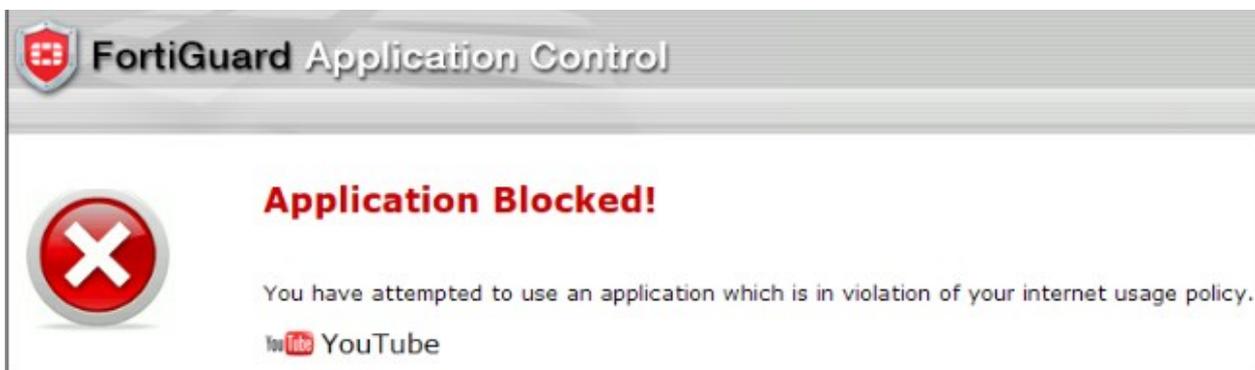


در زیر قسمت Application Overrides قسمت Add Signatures را انتخاب نمایید. کلمه Youtube را سرچ کنید و تمام signatures های مرتبط با آن را انتخاب نمایید. همان طوری که مشاهده میکنید تمام signatures ها به لیست اضافه شدند و به صورت خود کار Block شدند. گزینه Deep Inspection of Cloud Application را فعال نمایید.

در قسمت Security Profile دکمه Application Control را زده تا این قابلیت فعال شود و پروفایل ساخته شده را انتخاب نمایید.

## ۷. نتایج

سعی کنید وارد سایت [www.Youtube.com](http://www.Youtube.com) شوید. یک پیغام هشدار دریافت میکنید که ظاهری مانند عکس زیر دارد و به شما اعلام می کند سایت مورد نظر بلاک شده است.



خیالتان راحت باشد که ترافیک های مربوط به برنامه های بیت تورنت نیز بلاک خواهند شد. جهت کسب اطلاعات بیشتر از برنامه های بلاک شده به مسیر **System > Fortiview > All Session** رفته و حالت 5 minutes را انتخاب نمایید.

استفاده از قابلیت **Static URL filter** جهت جلوگیری از دسترسی به وب سایت های مشخص

وقتی شما اجازه دسترسی به نوع خاصی از محتوا را می دهید مانند دسته بندی Social Network ها، ممکن است فورتی گارد در داخل این دسته بندی سایت هایی باشند که شما دوست دارید آنها را بلاک کرده و اجازه دسترسی را از کاربران بگیرید. در این مثال، شما یاد می گیرید که چگونه فورتی گیت را تنظیم نمایید تا از دسترسی به شبکه های اجتماعی خاص جلوگیری کند. این شامل Sub Domain ها می شود. این به معنی است که یک Static URL Filter می باشد. و بوسیله استفاده از SSL Inspection انجام می شود. شما مطمئن خواهید شد که این وب سایت حتی بوسیله پروتکل SSL هم بلاک خواهد شد.

در این مثال Security Profile برای IPv4 نوشته می شود اما این روش برای IPv6 هم کار خواهد کرد. هر تنظیمی در IPv4 عینا در IPv6 هم کاربردی خواهد بود.

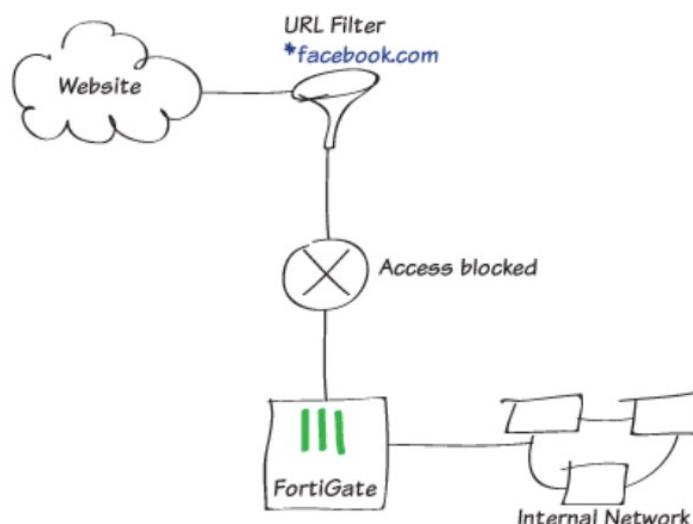
۱- تایید سرویس فورتی گارد ( مطمئن باشیم که سرویس فورتی گارد درست کار میکند)

۲- بخش Web Filter Profile را ویرایش کنید

۳- تایید کردن SSL Inspection Profile

۴- ساخت Security Policy

۵- نتایج



۱. تایید شدن صحت و درستی سرویس های فورتی گارد:

مسیر زیر را طی نمایید:

**System> Dashboard> Status**

در گجت License Information، مطمئن شوید که اشتراک مربوط به Web Filtering فعال است و درست کار میکند. اگر اشتراک را داشته باشید سرویس سبز خواهد بود. ( به شکل زیر دقت کنید)



## ۲. ویرایش Web Filter Profile

مسیر زیر را طی کنید :

### Security Profiles> Web Filter

و Web Filter Profile پیش فرض دستگاه را ویرایش کنید. تنظیم مربوط به Inspection Mode را در حالت Proxy قرار دهید.

FortiGuard Categories را فعال کنید. در قسمت مربوط به Social Network تمام زیرگروه ها را در حالت Allow قرار دهید و مطمئن شوید همه چیز درست تنظیم شده است. جهت ایجاد ممنوعیت برای دیدن یک Social Network سایت از این دسته بندی، به Static URL Filter بروید، تیک قسمت Enable URL Filter را بزنید و بعد Create New را انتخاب کنید:

### Static URL Filter

Enable URL Filter

URL	Type	Action	Status
No matching entries found			

Enable Web Content Filter

برای ساختن وب فیلتر جدید، URL سایتی که می خواهید بلاک کنید را وارد نمایید. اگر در نظر دارید تمام Subdomain های سایت را فیلتر کنید از علامت \* استفاده نمایید. مثلا وارد کنید : \*cloob.com در قسمت Type گزینه Wildcard را انتخاب نمایید و Action را در حالت Block قرار دهید و Status را در حالت Enable قرار دهید.

## ۳. مطمئن شوید که SSL Inspection Profile مورد تایید است

به مسیر زیر بروید:

### Policy & Objects> Policy> SSL Inspection

Certificate-inspection را ویرایش کنید. مطمئن شوید که CA Certificate روی Policy تعریف شده قرار بگیرد.

در قسمت Inspection Method گزینه SSL Certification Inspection را انتخاب نمایید و SSH Deep Scan را روشن کنید.

#### ۴. ساخت یک Security Policy :

مسیر زیر را طی نمایید:

#### Policy & Objects> Policy> IPv4

گزینه Create New را انتخاب کرده و بر اساس توضیحات زیر تنظیمات را انجام دهید:

Incoming Interface= internal Network

Outgoing Interface= Internet Facing (WAN)

Enable NAT

در زیر قسمت Security Profiles قسمت Web Filter را به حالت ON برده و default را انتخاب می کنیم. به صورت خودکار SSL/SSH Inspection فعال می گردد.

بعد از ساخت Policy جدید، مطمئن شوید که این Policy در بالای لیست قرار گرفته است. برای جابجا کردن Policy فقط کافی است آن را به سمت بالا و یا پایین حرکت دهید.

#### ۵. نتایج

سایت های زیر را بازدید کنید تا مطمئن شوید که Website بلاکینگ بدرستی کار میکند:

Cloob.com

Attachment.cloob.com

Upload.cloob.com

صفحه ی Web Page Blocked باید نمایش داده شود!!

اگر شما از پروتکل Https هم برای بازدید از سایت های بلاک شده استفاده کنید مشاهده خواهید کرد که با وجود این پروتکل باز هم این سایت ها بلاک می شوند.

جلوگیری کردن از اعلام اخطار Certificate وقتی که SSL full inspection مورد استفاده قرار می گیرد.

این مثال برای شما شرح خواهد داد که چگونه کاربرانان اخطار Certificate Security می گیرند در حالی که شما حالت SSL Inspection را فعال کرده اید. (deep inspection)

وقتی کاربران پیغام خطا را مشاهده می کنند اولین کاری که به ذهن آنها خطور میکند زدن دکمه Continue می باشد. این عادت بد باعث می شود شما تشویق شوید برای اینکه فراهم آوردن SSL CA فورتی گیت تا روی مرورگرهای کاربران نصب نمایید. خطای مربوط به Certificate تنها زمانی دیده می شود که SSL Inspection در حالت Deep مورد استفاده قرار بگیرد.

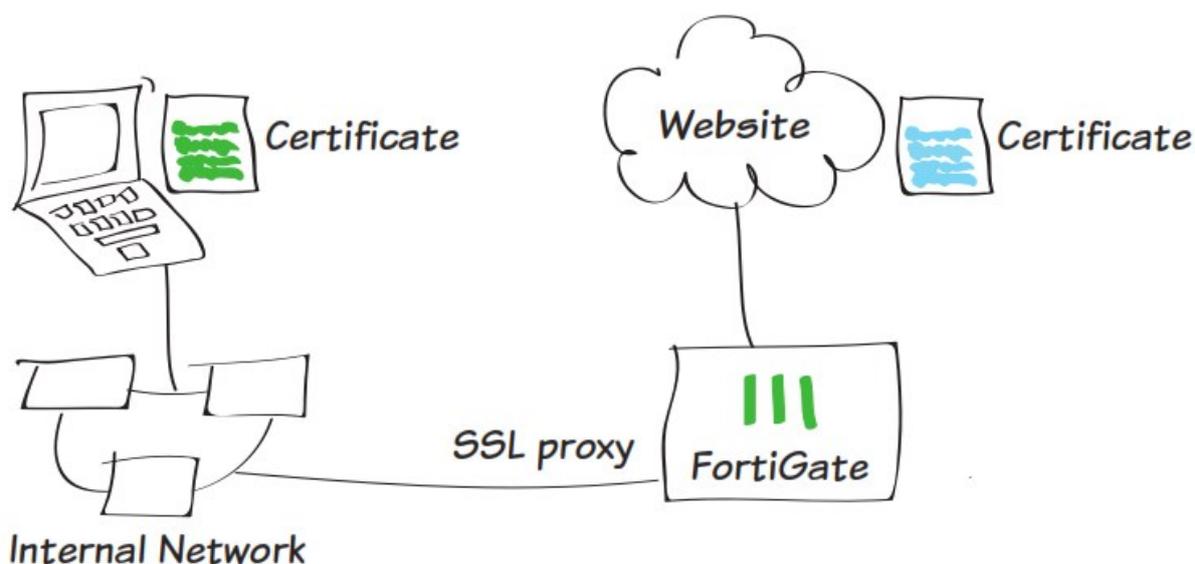
۱. مشاهده کردن وضعیت Deep-inspection SSL Profile

۲. فعال سازی تنظیمات Certificate در قسمت Web-based manager

۳. دانلود گواهینامه Fortinet\_CA\_SSLProxy

۴. وارد کردن CA certificate در داخل مرورگر وب

۵. نتایج

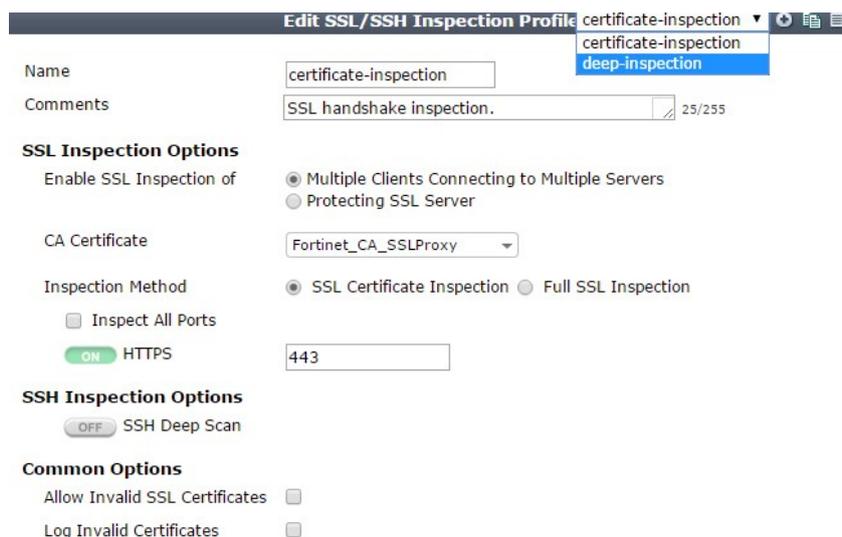


۱. مشاهده ی پروفایل deep-inspection SSL

مسیر زیر را طی نمایید:

**Policy & Objects>SSL/SSH Inspection**

در سمت راست بالاترین قسمت صفحه از منوی مشخص شده در شکل گزینه deep-inspection را انتخاب نمایید.



نکته: پروفایل deep-inspection باعث می شود به صورت دائمی ترافیک کدگذاری شده و SSL inspection اعمال شود.

در این Policy، دسته بندی سایت هایی مانند Health and wellness, Personal Privacy, Finance متمایز شده و این Policy به این گونه از سایت ها اعمال نمی گردد. برنامه هایی مانند itunes و Dropbox که نیازمند certificate ها یکتا (Unique) می باشند نیز از این دسته بندی متمایز می گردند.

## ۲. فعال کردن تنظیمات Certificate در قسمت مدیریتی وب

مسیر زیر را طی نمایید:

### System>Config>Features

بر روی گزینه Show More کلیک نمایید و قسمت Certificate را فعال نمایید. دکمه Apply را بزنید.

## ۳. دانلود نمودن Fortinet\_CA\_SSLProxy certificate

مسیر زیر را طی نمایید:

### System>Certificates>Local Certificates

حال Fortinet\_CA\_SSLProxy certificate را دانلود نمایید.

## ۴. CA certificate را داخل مرورگر وب وارد نمایید.

برای اینترنت اکسپلورر:

مراحل زیر را طی نمایید:

### Tools>Internet Options>Content>Certificates >Trusted Root Certification Authorities

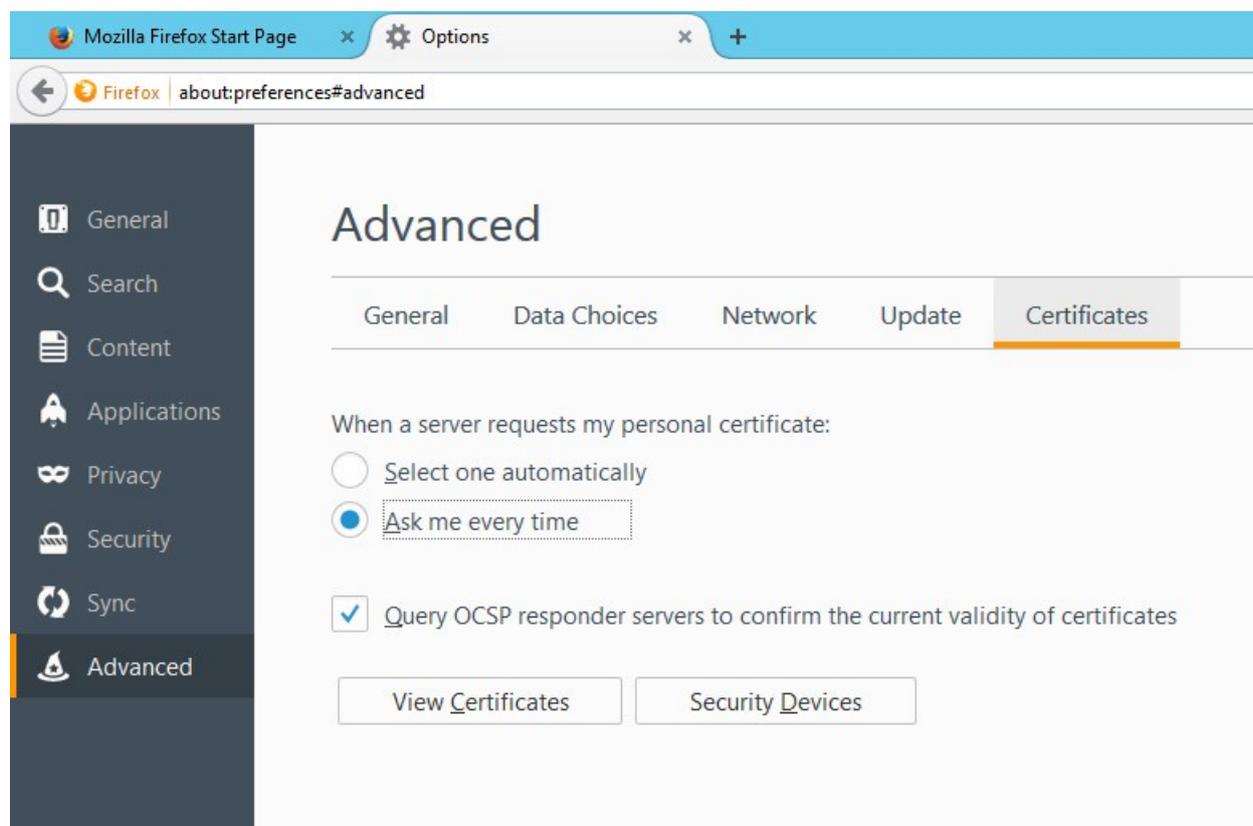
توسط Wizard ظاهر شده certificate را وارد نمایید. مطمئن شوید که Certificate در داخل Trusted Root Certification Authorities وارد شده است.

یک خطاری به شما داده خواهد شد به این خاطر که Certificate صادر شده Self signed می باشد. هیچ مشکلی ایجاد نخواهد شد و شما می توانید با خیالی آسوده certificate را install نمایید.

برای مرورگر فایرفاکس:

مسیر زیر را طی نمایید:

### Menu>Options or Preferences>Advanced >Certificates



می توانید گواهینامه ی صادر شده توسط فورتی گیت را به داخل مرورگر وارد نمایید.

برای مرورگر کروم و سافاری:

وارد محلی شوید که Fortinet\_CA\_SSLProxy را دانلود کردید و سپس گواهینامه را نصب نمایید. مراحل

مربوط به نصب Certificate ظاهر می شود. مطمئن شوید که Certificate در داخل Trusted Root Certification Authorities نصب شود. پس از انجام این کار پیغام خطاری را مشاهده خواهید کرد دلیل

این پیغام Self Signed بودن certificate می باشد. مطمئن باشید این Certificate کاملا امن و بدون مشکل می باشد پس با خیالی آسوده آنرا نصب نمایید.



## ۵. نتایج

در صورت نادیده گرفتن خطاهای مرورگر در مورد Certificate باز هم منو بار بالای صفحه رنگ قرمزی خواهد داشت که بشدت روی اعصاب کاربران است که با نصب Fortigate SSL CA Certification مشکلات حل خواهد شد.

بعد از نصب FortiGate SSL CA Certificate هیچ گونه اخطار یا پیغام خطایی نباید برای شما نمایش داده شود زیرا بخش SSL Content inspection کار خود را بدرستی انجام می دهد. به طور مثال در حال حاضر iTunes بدون دادن پیغام Certificate اجرا خواهد شد.

### استفاده از یک Certificate دلخواه برای SSL Inspection:

این دستورالعمل به شما آموزش می دهد که چگونه از دستگاه فورتی گیت برای ساختن یک Certificate دلخواه استفاده کنید و این Certificate بوسیله یک CA سرور صادر شود.

این دستورالعمل به شما نشان خواهد داد که چگونه CA Certificate در دستگاه فورتی گیت وارد نمایید و چگونه Certificate را در پروفایل SSL Inspection وارد نمایید.

یک Certificate با CA=True و یا KeyUsage=Certsign یک متا دیتا ایجاد می کند تا در deep inspection مورد استفاده قرار گیرد.

وقتی Certificate پیش فرض فورتی گیت مورد استفاده قرار می گیرد که با وارد کردن یک Certificate دلخواه از یک CA شناخته شده دیگر، یک زنجیره قابل اعتماد ایجاد شود که از قبل وجود نداشته باشد. این شرایط به کاربران شبکه اجازه می دهد تا به دستگاه فورتی گیت همانند یک CA تراست داشته باشند.

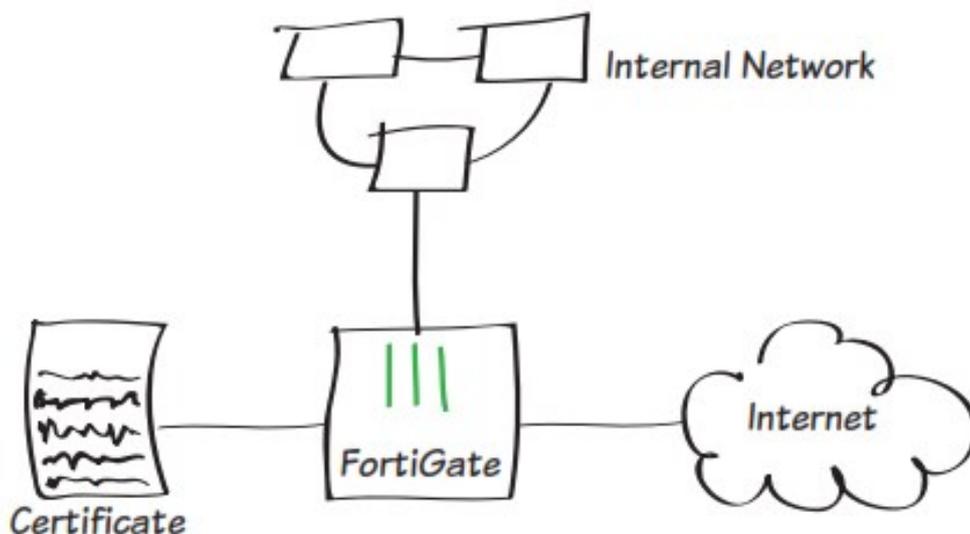
۱. ساخت یک CSR (certificate signing request)

۲. وارد کردن یک signed server certificate از یک روت سرور CA

۳. ساخت یک پروفایل SSL Inspection

۴. تنظیمات یک فایروال پالسی

۵. نتایج



### ۱. درست کردن یک CSR:

مسیر زیر را طی نمایید:

#### System>Certificates>Local Certificates

حال گزینه ی Generate را انتخاب نمایید.

در صفحه ی Generate Certificate Signing Request فیلدهای مربوطه را پر نمایید. شما می توانید حداکثر پنج Organization Unit وارد نمایید.

ممکن است شما Subject Alternative Names را برای Certificateهایی که valid هستند وارد نمایید. جداسازی نام ها با استفاده از کاما صورت می پذیرد.

مسیر زیر را طی نمایید:

#### System>Certificates>Local Certificates

در این قسمت می توانید لیست گواهینامه ها را مشاهده نمایید. وضعیت CSR ساخته شده هم در لیست به صورت Pending قابل مشاهده می باشد. Certificate مورد نظر خود را انتخاب کرده و گزینه Download را بزنید. این CSR باید توسط یک Enterprise root CA ارائه شود تا بتواند مورد استفاده قرار گیرد. وقتی این فایل ارائه شد مطمئن شوید که template برای یک Subordinate Certification Authority مورد استفاده قرار گرفته است.

### ۲. وارد کردن یک signed server certificate از یک enterprise root CA:

اولین باری که یک CSR توسط یک enterprise root CA مورد قبول واقع شد، شما می توانید داخل دستگاه فورتی گیت خود وارد نمایید.

مسیر زیر را طی کنید:

#### **System>Certificates>Local Certificates**

و بر روی گزینه Import کلیک نمایید. در قسمت Type از منوی پایین افتادنی Drop Down Menu گزینه Local Certificate را انتخاب نمایید و بر روی دکمه Choose file کلیک نمایید.

Certificate را که در نظر دارید وارد نمایید locate کرده و آنرا انتخاب نمایید. گواهینامه ی پذیرفته شده توسط CA در قسمت لوکال قابل مشاهده خواهد بود.

#### **۳. ساخت یک SSL Inspection Profile:**

برای استفاده کردن از گواهینامه صادر شده برای شما یک SSL Inspection profile نیاز می باشد

#### **Policy & Objects>Policy>SSL/SSH Inspection**

ساخت یک SSL Inspection Profile در منوی پایین افتادنی CA Certificate گواهینامه ای که Import کردید را انتخاب نمایید. Inspection Method را در حالت Full SSL Inspection قرار داده و تیک گزینه Inspect All Port را بزنید.

ممکن است شما بخواهید دسته بندی وب سایت ها را انتخاب کرده و آدرس هایی که از SSL Inspection معاف هستند را مشخص نمایید.

#### **۴. ویرایش Internet Policy مورد استفاده جهت SSL inspection profile جدید:**

مسیر زیر را طی نمایید:

#### **Policy & Objects >Policy>IPv4**

پالیسی کنترلر مربوط به ترافیک اینترنت را ویرایش نمایید

در قسمت Security Profiles، مطمئن شوید که SSL Inspection و Web Filter روشن می باشند. از منوی پایین افتادنی SSL Inspection پروفایل جدید را انتخاب نمایید. وب فیلتر روی حالت پیش فرض باقی بماند.

#### **۵. نتایج**

وقتی که یک وب سایت HTTPS را به صورت نرمال مشاهده می کنید ممکن است یک پیغام اخطار ظاهر شود البته این اتفاق در شرایطی رخ می دهد که شما از Self-signed certificate استفاده نمایید.

اگر شما از یک گواهینامه توسط یک CA شناخته شده صادر شده باشد استفاده نمایید پیغام اخطار نباید نمایش داده شود.

اگر اطلاعات مرتبط با گواهینامه های صادر شده برای هر وب سایت را مشاهده نمایید اطلاعاتی در مورد وضعیت گواهینامه ها تاریخ صدور و تاریخ انقضا و سایر موارد بدست می آورید.

در حال حاضر یک کاربر معمولی می تواند به صورت دستی گواهینامه ها را import کرده تا trust لازم را بدست آورد اما در شبکه های ویندوزی کاربری که جزو Domain باشد ادمین سیستم می تواند از طریق Group policy گواهینامه ها را فورس نماید.

### اجازه دسترسی به شبکه بر اساس زمانبندی و نوع دستگاه:

در این مثال، یوزر و دیوایس های احراز هویت شده authentication دسترسی متفاوتی نسبت به سایر پرسنل خواهد داشت که این پالسی شامل تمام وقت و یا نیمه وقت بوده و ترافیک برای موبایل ها بسته خواهد شد.

در این اینجا، یک شبکه وایرلس در یک subnet همانند شبکه LAN تنظیم شده است و کاربران در حال استفاده می باشند.

۱. تعریف کردن دو کاربر و دو User Groups

۲. ساخت یک زمانبندی برای کاربران پاره وقت

۳. تعریف کردن یک گروهی که شامل دیوایس ها می باشد که این گروه شامل mobile phone می باشد.

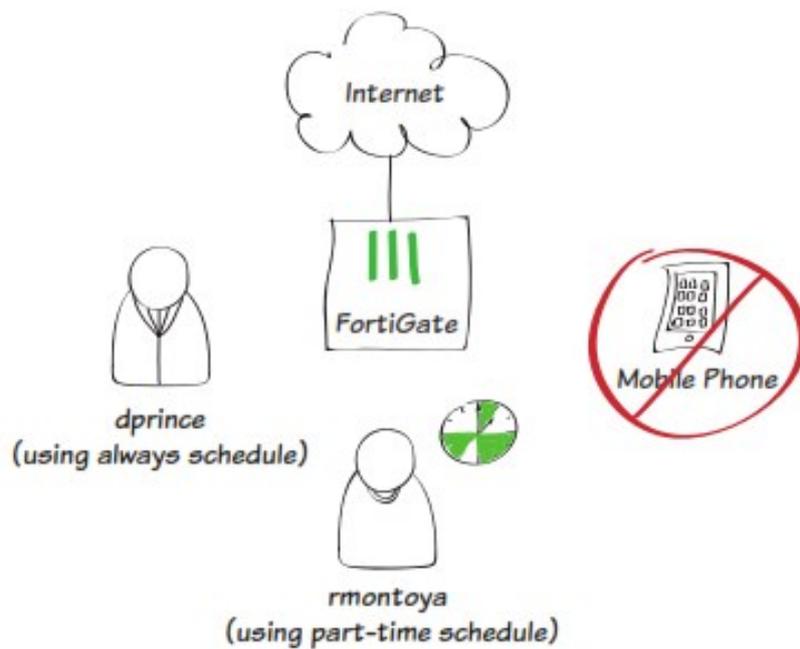
۴. ساخت یک پالسی برای کارکنان تمام وقت

۵. ساخت یک پالسی پاره وقت برای کارکنان و اعمال زمانبندی

۶. ساخت پالسی که ترافیک های مربوط به موبایل را بلاک می کند

۷. نتایج

شماتیکی خلاصه از سناریویی که قصد انجام آن را داریم:



### ۱. تعریف کردن دو یوزر و دو یوزر گروه

مسیر زیر را طی نمایید

User & Device > User > User Definitions

ساخت دو کاربر جدید ( در این مثال ، از نام های داود و رومینا استفاده میکنیم)

هر دو یوزر در لیست یوزرها نمایش داده می شوند.

The screenshots show a multi-step wizard for creating a user:

- Step 1: Choose User Type** - Options: Local User (selected), Remote RADIUS User, Remote TACACS+ User, Remote LDAP User.
- Step 2: Specify Login Credential** - Fields: User Name (davood), Password (masked).
- Step 3: Provide Contact Info** - Field: Email Address (dprince@example.com). There is also an unchecked checkbox for SMS.

به مسیر زیر بروید:

**User & Device > User > User Groups**

یک یوزرگروپ با اسم Full Time بسازید و کاربر داود را به آن اضافه نمایید.  
 یوزرگروپ دوم را ساخته و نام Part-Time را به آن اختصاص دهید و کاربر رومینا را به آن اضافه کنید.

The screenshot shows the configuration for a user group:

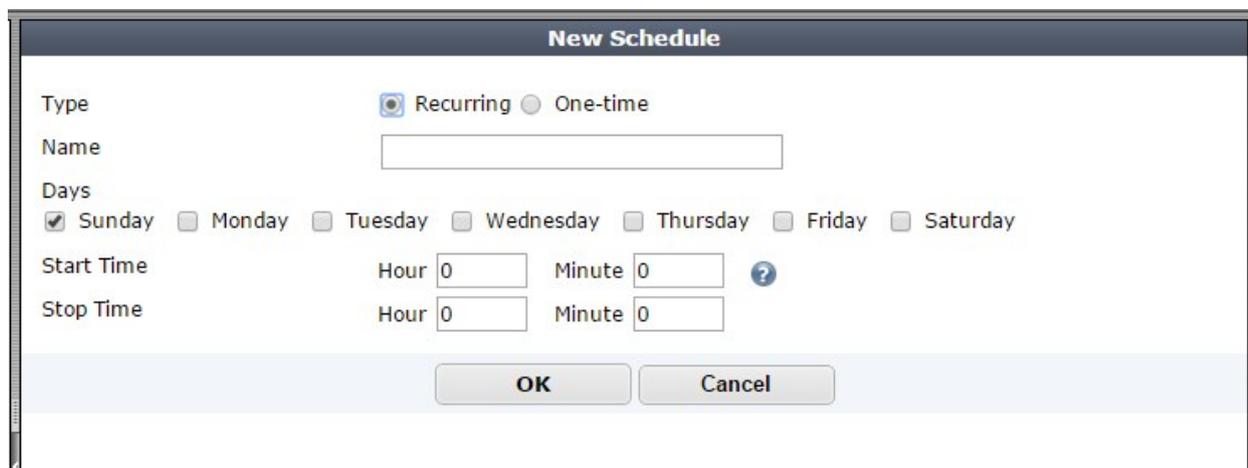
- Name:** part-time
- Type:** Firewall (selected), Fortinet Single Sign-On (FSSO), Guest, RADIUS Single Sign-On (RSSO)
- Members:** romina

۲. ساخت یک زمانبندی برای کاربران نیمه وقت :

مسیر زیر را طی نمایید:

**Policy & Objects > Objects > Schedules**

یک زمانبندی در محدوده ی زمانی مشخص بسازید. تنظیمات را بر اساس زمانبندی مناسب و دلخواه خود انجام دهید.



The screenshot shows a 'New Schedule' dialog box with the following fields and options:

- Type:  Recurring  One-time
- Name: [Empty text box]
- Days:  Sunday  Monday  Tuesday  Wednesday  Thursday  Friday  Saturday
- Start Time: Hour [0] Minute [0] [?]
- Stop Time: Hour [0] Minute [0]
- Buttons: OK, Cancel

۳. تعیین کردن یک گروه از دستگاه ها که شامل موبایل ها می شوند

مسیر زیر را طی نمایید:

**User & Device > Device > Device Groups**

یک گروه جدید بسازید.

مدل های مختلف از موبایل را عضو گروه کنید.

۴. ساخت پالسی برای پرسنل تمام وقت:

مسیر زیر را طی نمایید:

**Policy & Objects > Policy > IPv4**

یک پالسی جدید بسازید...

اینترفیس ورودی خود را شبکه داخلی در نظر گرفته در گزینه Source User(s) گروه full-time را انتخاب نمایید و برای outgoing Interface دست اینترنتی را در نظر گرفته و مطمئن شوید که Schedule روی حالت always قرار دارد. NAT را روشن کنید.

در قسمت logging Options حالت Log Allowed Traffic را روشن کرده و گزینه All Sessions را انتخاب نمایید.

۵. ساخت یک پالسی برای پرسنل یاره وقت

مسیر زیر را طی کنید:

#### Policy & Objects > Policy > IPv4

حال یک پالسی جدید با مشخصات زیر بسازید:

Incoming Interface = Local Network

Source User(S) = Part-time Group

Outgoing Interface = Internet Interface

Schedule = part-time schedule

NAT Turn on

همانند تنظیمات قبلی از بخش Logging Options گزینه Log Allowed Traffic را روشن کرده و گزینه All Sessions را انتخاب نمایید.

به مسیر **System > Dashboard > Status** بروید و دستورات زیر را در محیط CLI وارد نمایید جهت وارد کردن پالسی مربوط به part-time حتما از ID number استفاده نمایید.

این دستور باعث می شود اگر Session های یوزر با سیستم برقرار باشد بعد از اتمام زمان استفاده Session ها بسته شده و ارتباط کاربر قطع شود.

```
config      firewall      policy
            edit      2
            set      schedule-timeout  enable
            end
end
```

#### ۶. ساخت یک پالسی که ترافیک مربوط به موبایل ها را بلاک میکند

به مسیر **Policy & Objects > Policy > IPv4** رفته و یک پالسی جدید مطابق با تنظیمات زیر بسازید.

Incoming Interface = Local Network

Source Device = Mobile Devices

Outgoing Interface = Internet

Action = DENY

Log Violation Traffic = Turned On

این پالسی وقتی مورد استفاده قرار می گیرد که در بالای پالسی های دیگر قرار گیرد. برای بالا بردن اولویت این پالسی کافی است در گوشه ی سمت راست آن کلیک کرده و در حالی که موس را نگه داشته اید آن را به بالا هدایت کنید .

#### ۷. نتایج

جهت استفاده از اینترنت شما صفحه ی مربوط به Authentication را مشاهده خواهید کرد. برای لاگین شدن از اکانت davood استفاده نمایید. این اکانت در تمام ساعات اجازه استفاده را خواهد داشت.



The image shows a Fortinet authentication screen. At the top, the Fortinet logo is displayed in black and red. Below the logo, the text "Authentication Required" is centered. Underneath, a message reads "Please enter your username and password to continue." There are two input fields: "Username:" and "Password:", each followed by a white text box with a small asterisk icon on the right. At the bottom right of the form is a "Continue" button.

از طریق مسیر **User & Device > Monitor > Firewall** کاربر davood را انتخاب کرده و گزینه De-authenticate را بزنید. این بار از طریق یوزر رومینا سعی کنید به اینترنت متصل شوید. بعد از اینکه Authentication اتفاق می افتد شما نمی توانید به اینترنت دسترسی داشته باشید! این نکته را به خاطر بسپارید که تمام دستگاه های موبایل هم اینترنت نخواهد داشت.

اطلاعات در مورد Session های بلاک شده از طریق **System > Fortiview > All Session** قابل دستیابی است.

### IPsec VPN

این قسمت حاوی اطلاعاتی در مورد انجام تنظیمات انواع مختلف IPsec VPN می باشد. همچنین روش های متفاوتی از احراز هویت کاربران در IPsec VPN در این فصل شرح داده خواهد شد.

IPsec VPN از پروتکل امنیتی اینترنت استفاده میکند تا یک Virtual Private Network ساخته و شما با استفاده از بستر اینترنت به شبکه داخلی (خصوصی) خود دسترسی داشته باشید. به منظور اتصال به یک IPsec VPN، کاربران ملزم هستند IPsec VPN کلاینت را بر روی کامپیوترها و یا موبایل های خود نصب و تنظیم نمایند. ( همانند FortiClient ) .

این بخش حاوی دستورالعمل های زیر می باشد:

- پیکربندی یک IPsec VPN برای دستگاه های IOS
- راهنمایی های ویژه برای IPsec VPN
- استفاده از IPsec VPN برای ایجاد ارتباط بین دو شعبه
- پیکربندی IPsec VPN جهت ارتباط بین فورتی گیت و مایکروسافت Azure
- راه اندازی BGP بر روی dynamic IPsec VPN بین دو دستگاه فورتی گیت

### پیکربندی یک IPsec VPN برای دستگاه های iOS:

این دستورالعمل استفاده از ویزارد IPsec VPN جهت دسترسی گروهی از کاربران راه دور به شبکه داخلی شرکت را فراهم می سازد. این نکته قابل ذکر است که این کاربران از سیستم عامل iOS استفاده می کنند.

۱- ساخت یک گروه از کاربرانی که دارای سیستم عامل iOS هستند.

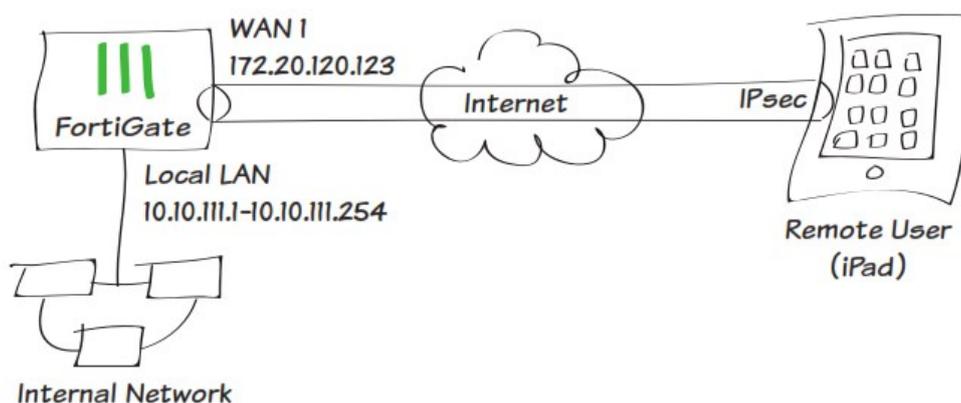
۲- اضافه کردن یک فایروال آدرس برای شبکه محلی

۳- پیکربندی IPsec VPN با استفاده از ویزارد

۴- ساخت یک Security Policy برای دستیابی به اینترنت

۵- پیکربندی VPN بر روی دستگاه iOS

۶- نتایج



۱. ساخت یک گروه از کاربرانی که از iOS استفاده می کنند

به مسیر **User & Device > User > User Definition** بروید.

با استفاده از ویزارد توضیح داده شده در مراحل قبلی یک Local User جدید بسازید. سعی کنید در تمام مراحل اطلاعات را با دقت وارد نمایید.



The screenshot shows the 'User Creation Wizard' interface. It has a progress bar with four steps: 1. Choose User Type, 2. Specify Login Credential, 3. Provide Contact Info, and 4. Provide Extra Info. Under 'Choose User Type', there are four radio button options: Local User (selected), Remote RADIUS User, Remote TACACS+ User, and Remote LDAP User. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

به قسمت **User & Devices > User > User Groups** وارد شوید. یک یوزر گروپ برای کاربران iOS بسازید و کاربر ساخته شده در مرحله قبل را به آن اضافه کنید



The screenshot shows the 'New User Group' dialog box. The 'Name' field contains 'iOS\_groups'. The 'Type' field has four radio button options: Firewall (selected), Fortinet Single Sign-On (FSSO), Guest, and RADIUS Single Sign-On (RSSO). The 'Members' field contains 'morteza'. Below this is a table for 'Remote groups' with columns 'Remote Server' and 'Group Name'. The table is empty with the message 'No matching entries found'. At the bottom are 'OK' and 'Cancel' buttons.

۲. به مسیر **Policy & Objects > Objects > Addresses** بروید. یک فایروال آدرس برای شبکه داخلی اضافه کنید که شامل Subnet و Local Host باشد.



The screenshot shows the configuration for a new address. The 'Category' is 'Address' (selected). The 'Name' is 'Local LAN'. The 'Type' is 'Subnet'. The 'Subnet / IP Range' is '0.0.0.0/0.0.0.0'. The 'Interface' is 'internal (LAN)'. The 'Show in Address List' checkbox is checked. The 'Comments' field is empty. At the bottom are 'OK' and 'Cancel' buttons.

### ۳. پیکربندی IPsec VPN با استفاده از IPsec VPN ویزارد

به مسیر **VPN > IPSec > Wizard** بروید.

یک نام برای VPN connection انتخاب کرده و گزینه **iOS – Dial UP** را انتخاب نمایید.



دست اینترنتی اینترنتی که ترافیک از آن وارد می شود (**Incoming Interface**). **Pre-shared Key** را انتخاب کنید تا Authentication Method انجام شود.

بعد از وارد کردن pre-shared key یوزر گروه مربوط به iOS را انتخاب کرده و Next کنید



LAN را بر روی اینترنتی داخلی تنظیم کنید و در قسمت **Local Address** آدرس شبکه داخلی خود را بدهید. رنج IP مربوط به کاربران VPN را مشخص کنید. شکل زیر کاملاً گویای تمام موارد می باشد.

VPN Setup > Authentication > Policy & Routing

sdsd : Dialup - iOS (Native)

Local Interface: port9

Local Address: client-vlan

Client Address Range: 10.10.10.100-10.10.10.150

Subnet Mask: 255.255.255.255

DNS Server

Use System DNS

Specify

Enable IPv4 Split Tunnel

< Back   Create   Cancel

#### ۴. ساختن Security Profile برای ایجاد دسترسی به اینترنت

به مسیر **Policy & Objects > Policy > IPv4** بروید و یک security policy با توجه به مشخصات زیر بسازید در این پالسی ما به کاربران ریموتی iOS دار اجازه می دهیم از طریق دستگاه فورتی گیت به اینترنت دسترسی داشته باشند.

Incoming Interface: iOSvpn\_Native

Source Address: all

Source User(s): Click to add...

Source Device Type: Click to add...

Outgoing Interface: wan1

Destination Address: all

Schedule: always

Service: ALL

Action: ACCEPT

**Firewall / Network Options**

NAT

Use Destination Interface Address    Fixed Port

#### ۵. پیکربندی VPN بر روی دستگاه های iOS

مسیر زیر را در iPad خود طی کنید:

**Settings > General > VPN > add VPN configuration**

آدرس سرور VPN را وارد نمایید، یوزرنیم و پسورد را در فیلدهای مشخص وارد نمایید در مرحله آخر pre-shared را در فیلد secret وارد کنید.

#### ۶. نتایج

در دستگاه فورتی گیت به قسمت **VPN> Monitor>IPsec Monitor** رفته و وضعیت تانل را مشاهده کنید. همچنین کاربران شبکه داخلی می توانند از دستگاه های iOS خود استفاده کنند.

به مسیر **Log & Report> Traffic Log> Forward Traffic** بروید تا وضعیت ترافیک را مشاهده کنید. با انتخاب یکی از سطرها می توانید جزئیات بیشتری را ببینید.

توجه داشته باشید کاربرانی که توسط دستگاه های iOS خود به شبکه شما متصل شده اند به اینترنت دسترسی دارند البته این دسترسی توسط فورتی گیت داده می شود.

### راهنمایی در مورد IPsec VPN

مطالب گردآوری شده در این بخش کمک خواهد کرد تا IPsec VPN را به راحتی راه اندازی کنید.

### The options to configure policy-based IPsec VPN are unavailable

به مسیر **System > Config > Feature** بروید. گزینه Show more را انتخاب کرده و قابلیت Policy-based IPsec VPN را فعال نمایید.

### The VPN connection attempt fails

اگر در اتصال مشکلاتی دارید موارد زیر را چک کنید:

- مطمئن شوید که هر دو Pre-shared key کاملاً درست است و با یکدیگر مطابقت دارد.
- مطمئن شوید که تنظیمات انتهایی هر دو طرف یکسان و بر اساس تنظیمات پیشنهادی انجام شده است.
- اگر سرویس هایی مثل DHCP/DNS مشکل دارند مطمئن شوید می توانند ترافیک های خود را به بیرون/داخل هدایت کنند.
- چک کنید که استاتیک route ها به درستی پیکربندی شده اند تا ترافیک VPN بتواند route شود.
- مطمئن شوید که دستگاه FortiGate در حالت NAT/ROUTE باشد.
- تنظیمات مربوط به NAT را چک کنید. قابلیت NAT Traversal در فاز ۱ را پیکربندی کنید در حالی که قابلیت NAT در Security Profile غیرفعال می کنید.
- مطمئن شوید که هر دو VPN ها از حالت Main استفاده می کنند، مگر اینکه چندین Dial-up tunnel در حال استفاده می باشد.
- اگر شما از چند IPsec VPN استفاده می کنید مطمئن شوید که هر ID به درستی روی فورتی گیت پیکربندی شده است و Client ها دارای Local ID مشخصی باشند.

- اگر شما از FortiClient استفاده می کنید اطمینان حاصل کنید که نسخه ی آن با فریمویر فورتی گیت همخوانی داشته باشد این کار را می توانید با خواندن دستورات عمل های FortiOS به انجام برسانید.
- مطمئن شوید که Quick Mode Selector به درستی پیکربندی شده است
- مطمئن شوید که تنظیمات دو سر تانل یکسان و شبیه یکدیگر باشد و دستگاه فورتی گیت تنظیماتش برای Enable as Server فعال شده باشد.
- اگر دستگاه فورتی گیت شما پشت NAT است، دستگاهی مثل یک روتر، پورت فورواردینگ را برای UDP پورت های 500 و 4500 فعال کنید.
- تمام پیکربندی هایی که مورد استفاده قرار نگرفته اند و در فازهای ۱ و ۲ قرار دارند را پاک کنید. اگر یک نمونه تکراری از VPN مشخص شد دستگاه را ریست کنید تا تمام ورودی ها پاک شود.
- اگر هنوز هم نمی توانید به VPN Tunnel متصل شوید، دستور مربوط به diagnostic را در CLI بزنید:

```
diag debug application ike -1
diag debug enable
```

- وقتی پروسه diag تمام شد دستور زیر را وارد کنید:

```
diag debug reset
diag debug disable
```

### The VPN tunnel goes down frequently.

- اگر VPN Tunnel شما قطع می شود، فاز ۲ را چک نمایید و Key life را افزایش دهید و یا Autokey Kepp Alive را افزایش دهید.

### استفاده از IPsec VPN جهت برقراری ارتباط بین دو دفتر:

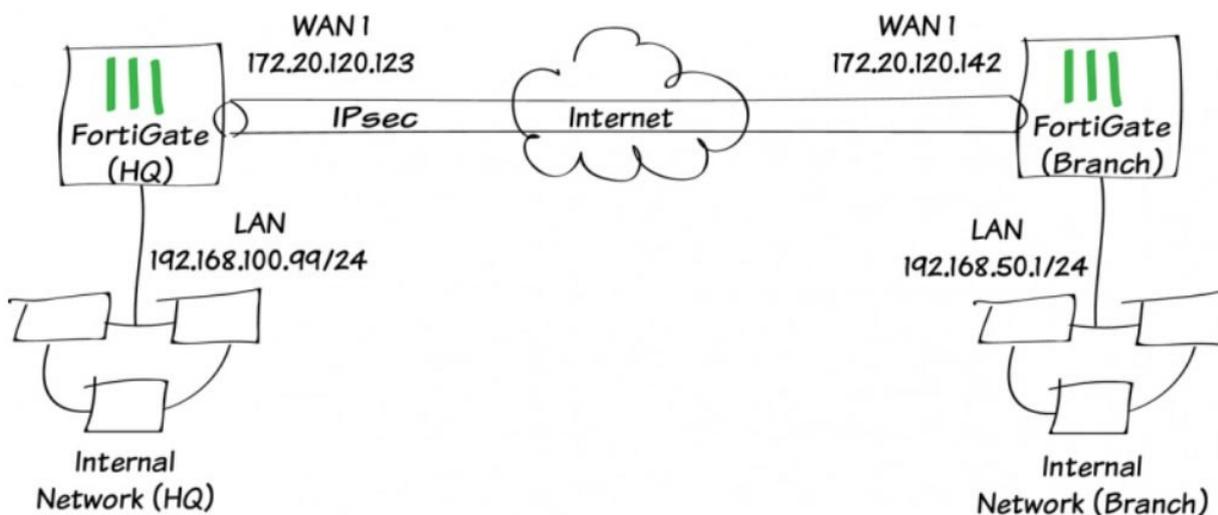
در این مثال، شما اجازه خواهید داد که دو شبکه داخلی که پشت فایروال فورتی گیت هستند و در دو دفتر مجزا قرار دارند با یکدیگر ارتباط برقرار نمایند. شایان ذکر است این ارتباط route-based می باشد.

VPN در هر دو طرف بوسیله Wizard تعریف شده و در دستگاه فورتی گیت ساخته می شود.

در این مثال، یک دفتر مرکزی به اسم HQ و یک شعبه به اسم Branch وجود دارد.

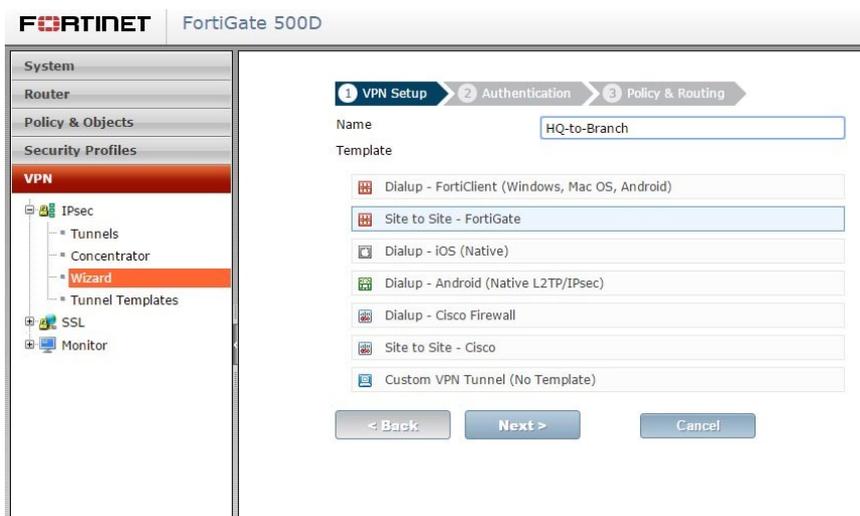
۱. پیکربندی VPN مربوط به HQ

۲. پیکربندی VPN مربوط به Branch

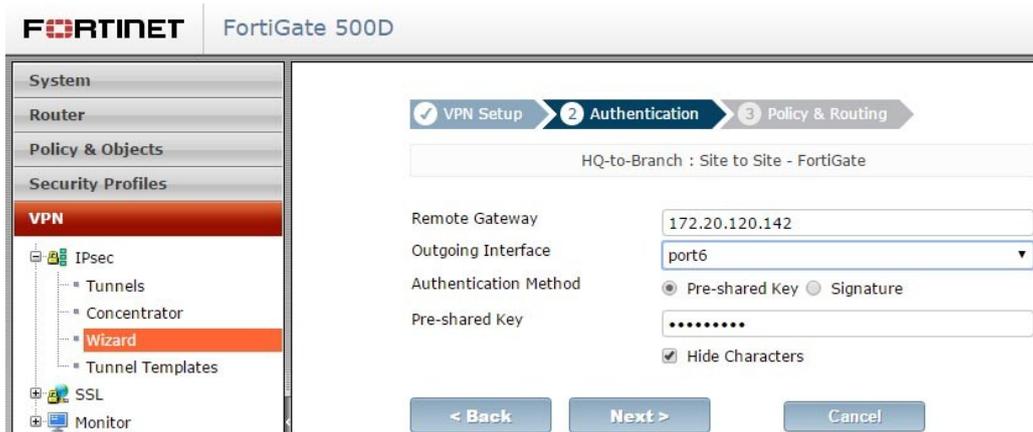


### ۱. پیکربندی IPsec VPN مربوط به HQ

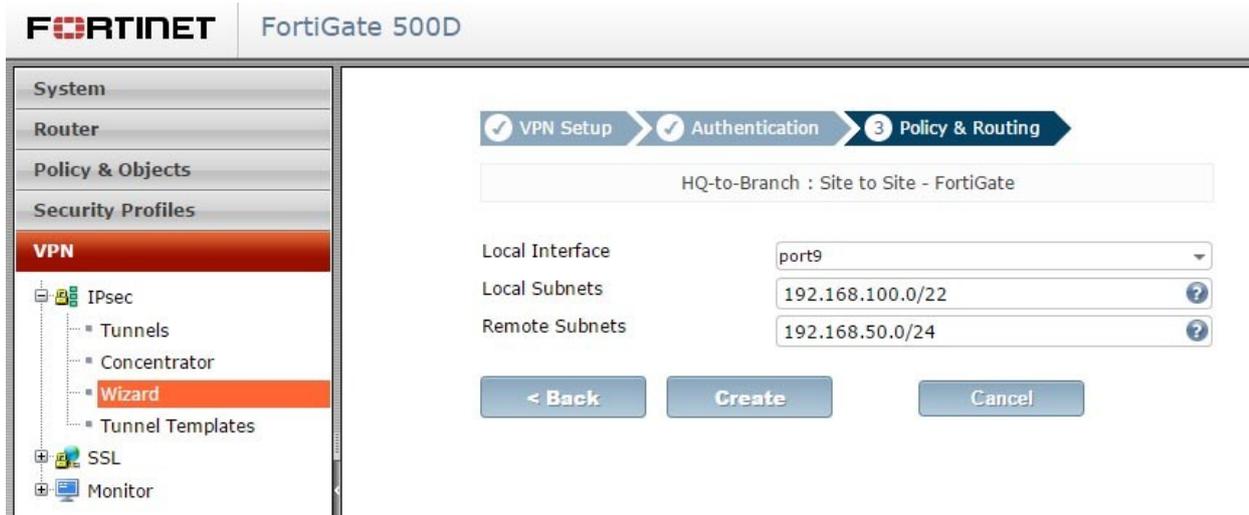
در فورتی گیت دفتر مرکزی HQ به مسیر **VPN > IPsec > Wizard** رفته و گزینه Site to Site – FortiGate را انتخاب نمایید.



در مرحله Authentication، IP آدرس مربوط به شعبه Branch را در قسمت Remote Gateway وارد می کنیم ( Valid IP طرف مقابل را وارد می کنیم). در مرحله بعدی اینترفیسی که در نظر دارید تا با آن پکت ها خارج شوند را مشخص می نمایید. منظور همان Outgoing Interface می باشد. اگر می خواهید از یک Interface مجزا استفاده نمایید می توانید از گزینه Change استفاده نمایید. Pre-shared Key مورد نظر خود را وارد نمایید.



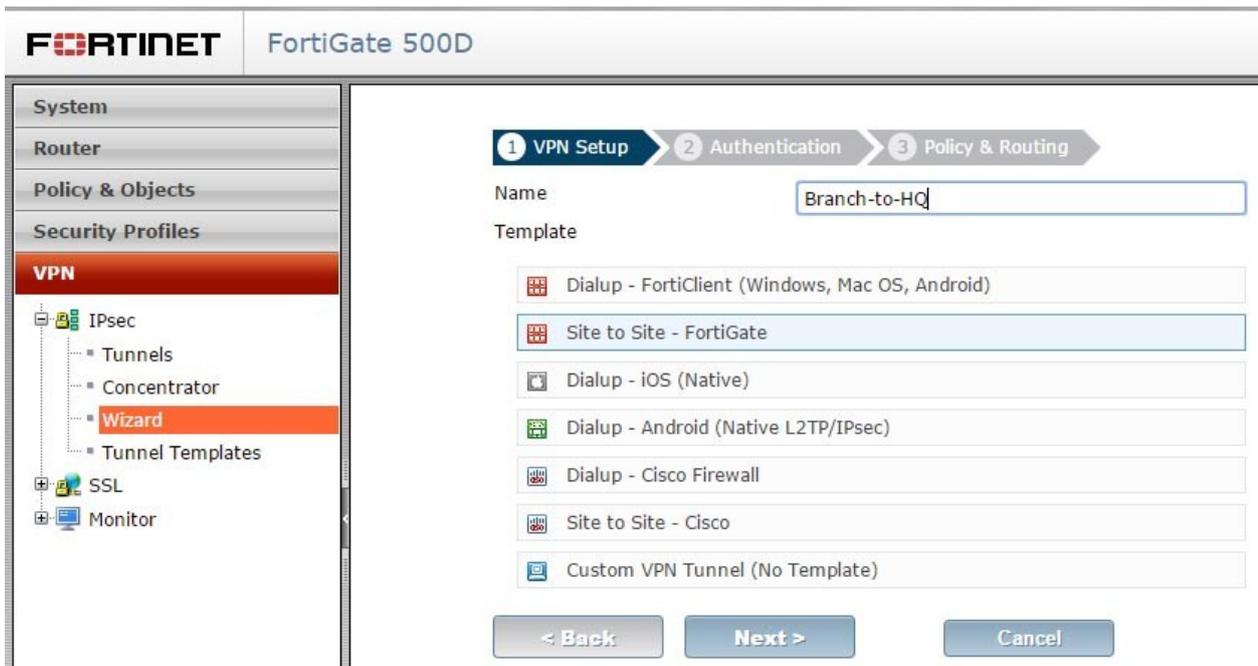
در قسمت Policy & Routing، دست داخلی شبکه خود را مشخص کنید منظور از دست داخلی همان Local Interface می باشد. به صورت خودکار Subnet مربوط به شبکه داخلی مشخص می شود. در قسمت Remote subnet ساب نت Subnet مربوط به شبکه داخلی Branch را مشخص نمایید. ( در این قسمت IP آدرس و Subnet مربوط به شبکه روبرو را وارد می نماییم.) شکل به درستی گویای تمامی مطالب می باشد.



صفحه summary نشان دهنده ی پیکربندی ایجاد شده توسط شما می باشد که حاوی اطلاعاتی از وضعیت ساخت VPN IPsec می باشد.

## ۲. پیکربندی VPN IPsec در Branch:

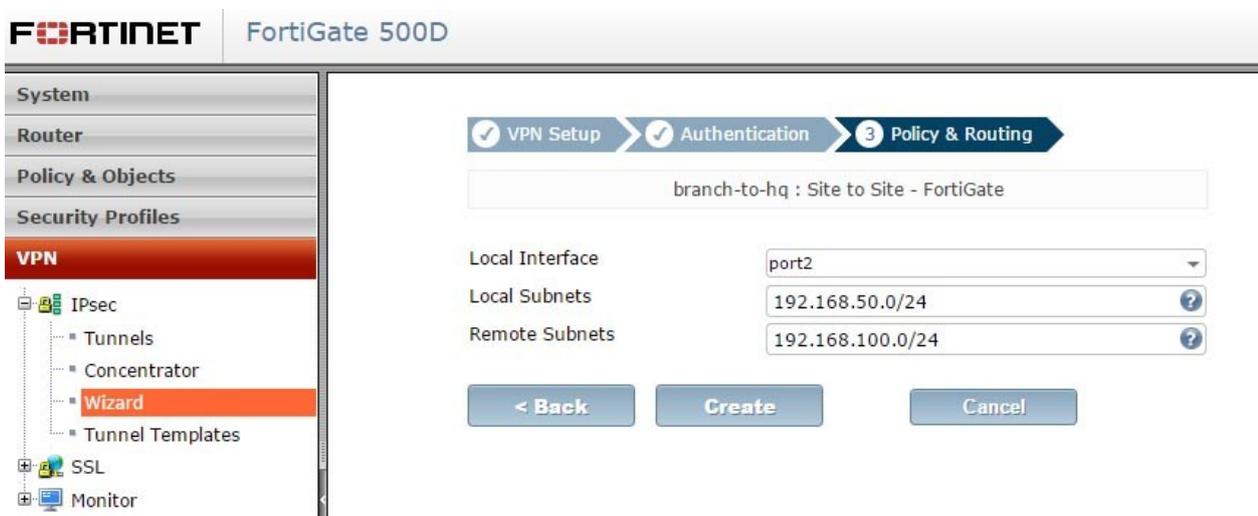
بر روی فورتی گیت مربوط به Branch لاگین کرده و مسیر **VPN > IPsec > Wizard** را طی کنید و گزینه Site to Site – FortiGate را انتخاب کنید.



در مرحله Authentication ، آی پی آدرس مربوط به دستگاه فورتی گیت موجود در HQ را در قسمت Remote Gateway وارد نمایید. بعد از وارد کردن Gateway، Outgoing Interface به صورت خودکار اضافه می شود. اگر تمایل دارید از اینترفیس جداگانه ای استفاده کنید کافی است بر روی لینک Change کلیک نمایید.

Pre-shared Key استفاده شده در HQ را وارد نمایید.

در قسمت Policy and Routing، اینترفیس مربوط به LAN را انتخاب کرده تا Subnet به صورت خودکار اضافه شود. در قسمت Remote Subnets آی پی آدرس و ساب نت *subnet* مربوط به شبکه روبرویی ( در این سناریو منظور شبکه HQ می باشد) وارد نمایید.



همانند قبل یک صفحه مربوط به خلاصه ای از تنظیمات صورت گرفته ظاهر می شود که شما می توانید بازنگری کوتاهی نسبت به تنظیمات داشته باشید.

### ۳. نتایج

به مسیر **VPN> Monitor> IPsec Monitor** بروید تا وضعیت VPN Tunnel خود را مشاهده نمایید. مطمئن شوید **Status** وی پی ان در حالت UP می باشد.

کاربری که در شبکه ی دفتر HQ نشسته است می توانید براحتی به تمام آدرس های شبکه موجود در دفتر Branch دسترسی داشته باشد. برعکس این قضیه هم به روشنی صادق است.

### پیکربندی IPsec VPN بین یک فورتی گیت و مایکروسافت Azure

در تمرینی که مشاهده خواهید کرد برای شما توضیح می دهیم که چگونه یک IPsec VPN را پیکربندی کنید. در این مثال یک طرف دستگاه فورتی گیت قرار داشته و در طرف دیگر یک **host** که روی آن Microsoft Azure قرار گرفته است. برای پیاده سازی شما باید یک پروفایل Microsoft Azure داشته باشید.

مثال به شما نشان می دهد که چطور تانل را بین دو طرف پیکربندی کرده، تا از هر گونه overlapping روی سابنت ها جلوگیری شود. یک تانل امن را می توانیم با ایجاد پروفایل امنیتی مناسب ایجاد کنیم.

۱. پیکربندی Microsoft Azure

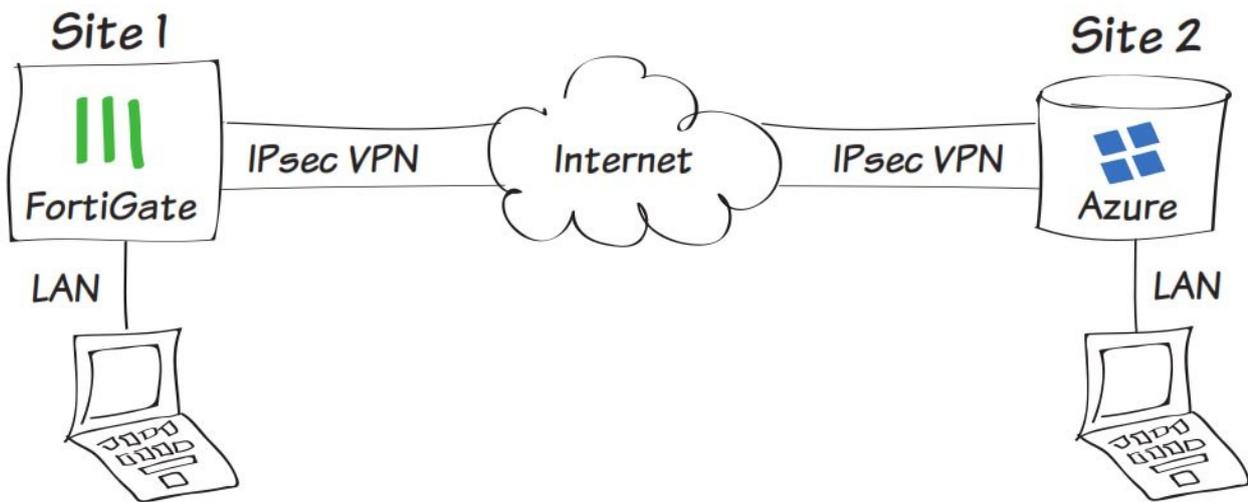
۲. ساخت Virtual network gateway

۳. پیکربندی تانل Fortigate

۴. ساختن آدرس های فایروال فورتی گیت

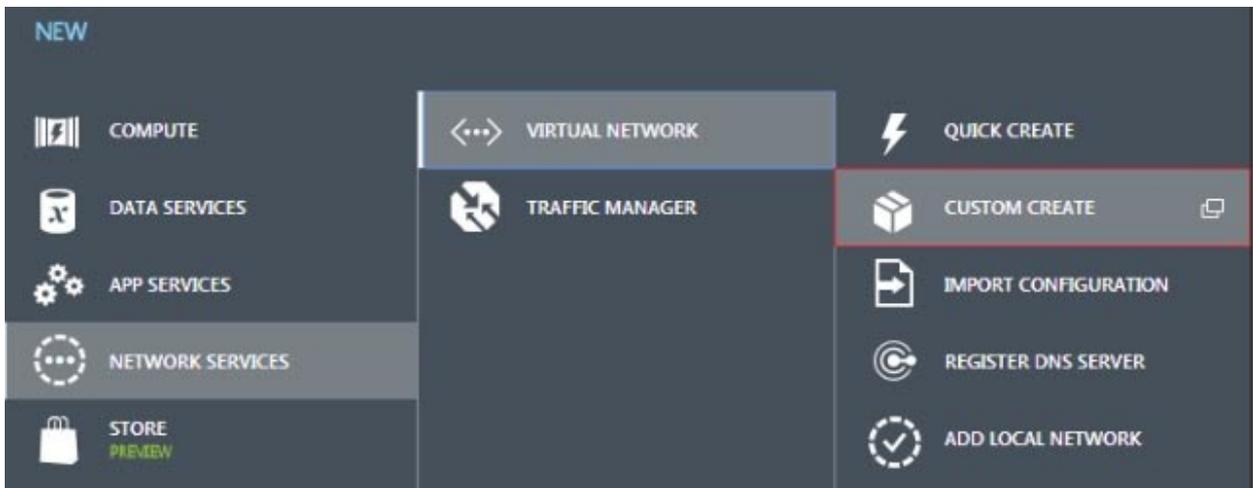
۵. ساختن پالسی فایروال برای فورتی گیت

۶. نتایج



### ۱. پیکربندی شبکه مجازی Microsoft Azure

بر روی Microsoft Azure لاگین کنید و از گوشه ی سمت چپ گزینه New را کلیک کنید تا سرویس جدیدی را اضافه نمایید:



مطابق عکس بالا مسیر را طی نمایید.

#### Network Services > Virtual Network > Custom Create

در زیر گزینه 'Virtual Network Details' و در فیلد Name و Location نام و شهری را انتخاب نمایید.

NAME	LOCATION
Site2SiteVPN	East US

در پایین قسمت 'DNS Servers and VPN Connectivity' تیک گزینه 'Configure a site-to-site VPN' را بزنید و اگر نیاز بود اطلاعات مربوط به DNS Server را وارد نمایید . Next کنید

پایین قسمت 'Site-to-Site Connectivity' یک نام و IP Address مربوط به دستگاه فورتی گیت را وارد نمایید.

قسمت address Space، شامل یک Starting IP و CIDR برای تانل می باشد، این موارد باعث میشود overlapping در سابنت ها ایجاد نشود. با دکمه Next وارد مرحله بعدی شوید.

NAME	ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
Local_Network	192.168.111.0/24	192.168.111.0	/24 (256)	192.168.111.0 - 192.168.111.255

قسمت 'Virtual Network Address Spaces' آدرس های مورد نظر یا تنظیمات دلخواه خودتان را پیکربندی کنید. دکمه add gateway subnet را انتخاب کنید تا تنظیمات مربوط به Gateway را انجام دهید.

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
10.0.0.0/8	10.0.0.0	/8 (16777...)	10.0.0.4 - 10.255.255.254
<b>SUBNETS</b>			
Subnet-1	10.11.12.0	/24 (251)	10.11.12.4 - 10.11.12.254
Gateway	10.11.13.0	/29 (3)	10.11.13.4 - 10.11.13.6

بعد از به پایان رساندن تنظیمات باید کمی صبور باشید تا با اندک زمانی صبر و تحمل تغییرات اعمال شود. مطمئن باشید این زمان طولانی نخواهد بود.

## ۲. ساختن virtual network gateway برای Microsoft Azure

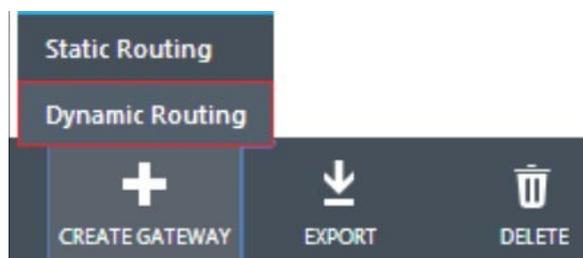
مطابق با شکل بر روی نام virtual network ساخته شده کلیک کنید. در زیر virtual network، به Dashboard بروید. اختاری به شما داده می شود که gateway هنوز ساخته نشده است. در این قسمت gateway خواهید ساخت.

NAME	STATUS
Site2SiteVPN	→ ✓ Created



مسیر زیر را پیمایش کنید:

**Create Gateway> Dynamic Routing> Select YES**



مدت زمان کوتاهی طول می کشد تا gateway virtual network ساخته شده و اجرا گردد. پس از طی کردن مراحل بالا Azure به شما نشان می دهد که gateway ساخته شده است. وقتی کارها به پایان رسید، استاتوس تغییر کرده و به شما یک Gateway IP Address می دهد.

DATA IN: 0B

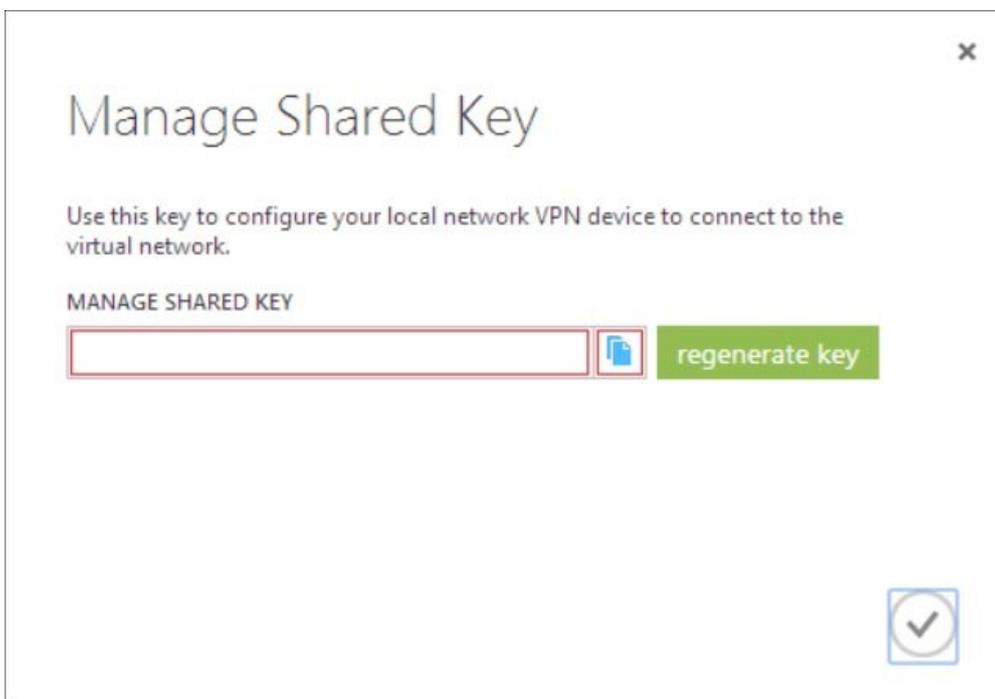
DATA OUT: 0B

GATEWAY IP ADDRESS: 23. . .

دکمه Manage Key را بزنید:



پنجره مربوط به 'Manage Shared Key' نمایان می شود. کلید نمایش داده شده را کپی کنید. برای انتخاب کلید متفاوت می توانید دکمه regenerate key را بزنید. وقتی اطمینان حاصل کردید که کلید کپی شده است دکمه Checkmark را بزنید.



الان وقت آن است که به سراغ فورتنی گیت برویم:

۳. پیکربندی تانل فورتنی گیت:

به مسیر **VPN> IPsec> Wizard** بروید و Custom VPN Tunnel را انتخاب کنید. یک نام برای تانل انتخاب گذاشته و گزینه Next را بزنید:

**1 VPN Setup**

Name

Template

- Dialup - FortiClient (Windows, Mac OS, Android)
- Site to Site - FortiGate
- Dialup - iOS (Native)
- Dialup - Android (Native L2TP/IPsec)
- Dialup - Cisco Firewall
- Site to Site - Cisco
- Custom VPN Tunnel (No Template)

< Back    Next >    Cancel

در قسمت Remote Gateway آی پی مربوط به Microsoft Azure را وارد نمایید. Local Interface را در حالت WAN1 قرار دهید. در قسمت Authentication کلید ساخته شده توسط Microsoft Azure را وارد نمایید .

گزینه NAT Traversal و Dead Peer Detection را غیرفعال کنید.

Name

Comments

Enable IPsec Interface Mode

**Network**

IP Version  IPv4  IPv6

Remote Gateway

IP Address

Local Interface

Mode Config

NAT Traversal

Dead Peer Detection

در قسمت Authentication مطمئن شوید که IKEv2 و در قسمت DH Group گزینه 2 را انتخاب کرده اید. Keylife را در حالت 56600 Sec قرار دهید.

**Authentication**

Method: Pre-shared Key

Pre-shared Key: [.....] Show Key

**IKE**

Version:  1  2

---

**Phase 1 Proposal**

Encryption	Authentication	Remove
AES256	SHA1	Remove
AES256	SHA256	Remove
AES128	SHA1	Remove
AES128	SHA256	Remove

Diffie-Hellman Group:  21  20  19  18  17  16  
 15  14  5  2  1

Key Lifetime (seconds): 56600

Local ID: [.....]

در فاز دوم، فیلد Local Address را با IP Adss مربوط به شبکه داخلی مقابل پر خواهیم کرد (Microsoft Azure) و فیلد مربوط به Remote Address را با IP ثابت شبکه ی مقابل پر میکنیم . Encryption را مطابق با فاز ۱ قرار می دهیم و در این مرحله Keylife را با عدد 7200 Sec تنظیم می کنیم.

#### ۴. ساختن آدرس های فایروال برای فورتنی گیت

به مسیر **Policy & Objects > Objects > Addresses** در فایروال مراجعه کنید و برای شبکه داخلی یک address پیکربندی کنید.

یک آبجکت برای Microsoft Azure بسازید که حاوی اطلاعات زیر باشد:

Name= دلخواه

Subnet/IP Range = 10.11.12.0/255.255.255.0

Interface= any

Visibility= enable

#### ۵. ساختن Firewall Policy در فورتنی گیت:

به مسیر **Policy & Objects > Policy > IPv4** بروید و یک پالسی جدید برای اتصال site-to-site بسازید.

با توجه به آموخته های قبلی Source Address و Destination Address از آبجکت های ساخته شده در مراحل قبلی را مورد استفاده قرار دهید. وقتی کارها انجام شد، یک پالسی جدید برای کانکشن های مشابه که اجازه ورود ترافیک را داشته باشند بسازید. این بار Source Address و Destination Address جابجا می شود.

## ۶. نتایج

به مسیر **VPN> Monitor> IPsec Monitor** بروید. بر روی تانل ساخته شده کلیک راست کرده و گزینه Bring Up را انتخاب نمایید تا تانل فعال شود.

جهت فعال سازی لاگ ها مسیر زیر را طی نمایید:

### Log & Report> Event Log>VPN

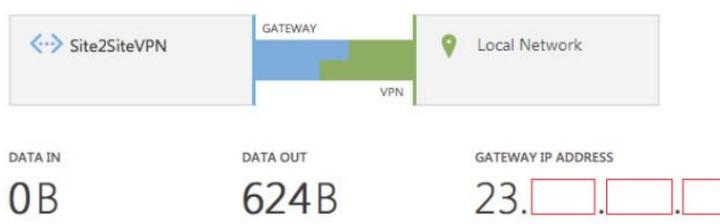
جهت کسب اطلاعات بیشتر کافی است یکی از ورودی ها را انتخاب نمایید.

#	Date/Time	Level	Action	Status	Message	VPN Tunnel
12	15:23:04	notice	phase2-up		IPsec phase 2 status change	Site2Site
13	15:23:04	notice	install_sa		install IPsec SA	Site2Site
14	15:23:04	notice	negotiate	success	negotiate IPsec phase 2	Site2Site
15	15:23:04	notice	negotiate	success	progress IPsec phase 1	Site2Site
16	15:23:04	notice	negotiate	success	negotiate IPsec phase 1	Site2Site

1 / 1582 [ Total: 79053 ]

<b>Action</b>	negotiate	<b>Assigned IP</b>	N/A
<b>Cookies</b>	9de897c069896c80/31b2351571a476b2	<b>Date/Time</b>	15:23:04 (1407770584)
<b>ESP Authentication</b>	HMAC_SHA1	<b>ESP Transform</b>	ESP_AES
<b>Group</b>	N/A	<b>IPsec Local IP</b>	69.171.153.181
<b>IPsec Remote IP</b>	23.100.122.11	<b>Level</b>	notice
<b>Local Port</b>	500	<b>Log Description</b>	negotiate IPsec phase 2
<b>Log ID</b>	37186	<b>Message</b>	negotiate IPsec phase 2
<b>Outgoing Interface</b>	ppp1	<b>Remote Port</b>	500
<b>Role</b>	initiator	<b>Status</b>	success
<b>Sub Type</b>	vpn	<b>Timestamp</b>	8/11/2014, 3:23:04 PM
<b>User</b>	N/A	<b>VPN Tunnel</b>	Site2Site
<b>Virtual Domain</b>	root	<b>XAUTH Group</b>	N/A
<b>XAUTH User</b>	N/A		

به داشبورد Microsoft Azure بازگردید. وضعیت تانل زده شده نمایش داده می شود که نشان می دهد که ارتباط برقرار می باشد یا خیر ؟ Data In و Data Out به نمایانگر این مورد است که چه مقدار ترافیک در حال عبور می باشد.



## راه اندازی BGP بر روی IPsec VPN بین دو فورتی گیت:

این مثال نشان می دهد که چگونه یک تانل IPsec VPN داینامیک بزنیم و اجازه دهیم تا BGP از طریق این تانل متصل شود.

۱. پیکربندی IPsec در فورتی گیت شماره ۱

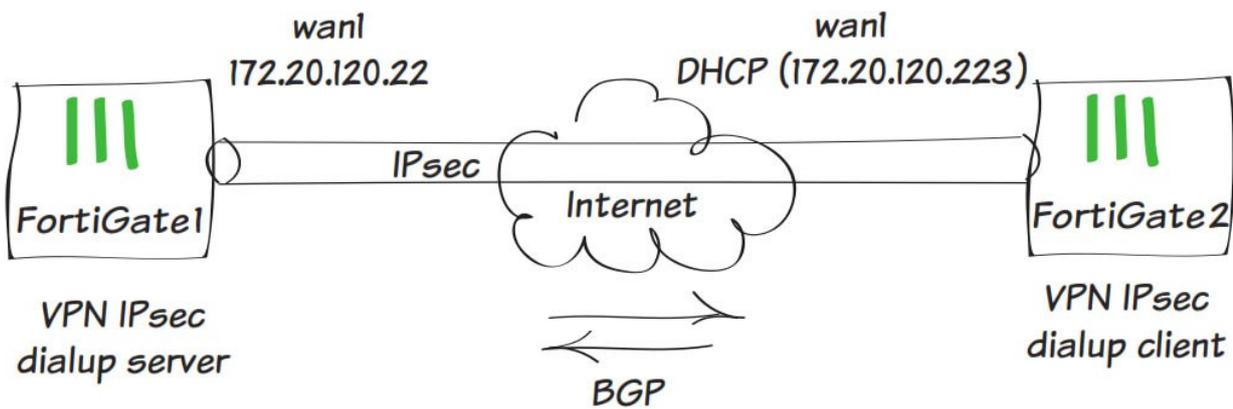
۲. پیکربندی IPsec در فورتی گیت شماره ۲

۳. تایید UP شدن تانل

۴. پیکربندی BGP در فورتی گیت شماره ۱

۵. پیکربندی BGP در فورتی گیت شماره ۲

۶. نتایج



## ۱. پیکربندی IPsec در فورتی گیت ۱

به مسیر **VPN > IPsec > Wizard** رفته و **FortiGate – Site to Site** را انتخاب نمایید. Next کنید

1 VPN Setup 2 Authentication 3 Policy & Routing

Name

Template

- Dialup - FortiClient (Windows, MacOS, Android)
- Site to Site - FortiGate
- Dialup - iOS (Native)
- Dialup - Android (Native L2TP/IPsec)
- Dialup - Cisco Firewall
- Site to Site - Cisco
- Custom VPN Tunnel (No Template)

< Back Next > Cancel

مطابق معمول فیلدهای مربوط به Remote Gateway و Outgoing Interface و Pre-shared key را پر می کنیم و Next را می زنیم.

1 VPN Setup 2 Authentication 3 Policy & Routing

ike-bgp-fgt1 : Site to Site - FortiGate

Remote Gateway

Outgoing Interface wan1 ( Detected via routing lookup ) [Change]

Authentication Method  Pre-shared Key  Signature

Pre-shared Key

Hide Characters

< Back Next > Cancel

در قسمت Local interface کارت شبکه داخلی را انتخاب کرده و در قسمت Local Subnet سابنت مربوط به شبکه خودمان را وارد می کنیم. در قسمت Remote Subnet هم سابنت شبکه مقابل را وارد می کنیم.

ike-bgp-fgt1 : Site to Site - FortiGate

Local Interface: lan

Local Subnets: 192.168.1.0/24

Remote Subnets: 10.10.1.0/24

< Back Create Cancel

---

ike-bgp-fgt1 : Site to Site - FortiGate

**✓ The VPN has been set up successfully**

**Summary of Created Objects**

Phase 1 Interface	ike-bgp-fgt1
Phase 2 Interfaces	ike-bgp-fgt1
Static Routes	10.10.1.0/24
Local Address Group	ike-bgp-fgt1_local
Remote Address Group	ike-bgp-fgt1_remote
Local to Remote Policy	5
Remote to Local Policy	7

Add Another Show Tunnel List

طبق آموخته های قبلی فازهای دوم و سوم را طی کرده و ارتباطات را ایجاد می نمایم

## ۲. پیکربندی IPsec در فورتنی گیت ۲

مراحل را مطابق با فورتنی گیت شماره ۱ پیش می بریم تنها در وارد کردن IP Address مربوط به Remote دقت می کنیم چون این تنها فیلدی است که تغییر می کند.

## ۳. مطمئن می شویم که تانل برقرار است

به مسیر **VPN> Monitor> IPsec Monitor** می رویم تا مطمئن شویم که ارتباط UP می باشد.

## ۴. پیکربندی BGP در فورتنی گیت

به مسیر **System> Status** رفته و CLI Console را باز می کنیم و دستورات زیر را وارد می کنیم :

```

config router bgp
  set as 1
  set router-id 172.20.120.22
  config neighbor
    edit "172.20.120.223"
      set remote-as 2
    next
  end
  config redistribute "connected"
    set status enable
  end
  config redistribute "static"
    set status enable
  end
end

```

#### ۵. تنظیمات BGP در فورتی گیت دوم :

همانند فورتی گیت اول مراحل را انجام داده و وارد محیط CLI می شویم و دستورات زیر را میزنیم:

```

config router bgp
  set as 2
  set router-id 172.20.120.223
  config neighbor
    edit "172.20.120.22"
      set remote-as 1
    next
  end
  config redistribute "connected"
    set status enable
  end
  config redistribute "static"
    set status enable
  end
end

```

#### ۶. نتایج

از فورتی گیت ۱ به مسیر **Router> Monitor> Router Monitor** رفته و چک می کنیم که آیا روتر روبرویی به درستی خود را Advertised کرده است و دو روتر شبکه های روبروی خود را می بینند!؟

Type	Network	Gateway	Interface	Up Time
Static	0.0.0.0/0	0.0.0.0	fext-wan1	
Static	0.0.0.0/0	25.52.81.253	fext-wan1	
Static	10.10.1.0/24	0.0.0.0	ike-bgp-fgt1	
BGP	10.10.80.0/24	172.20.120.223	wan1	0 00:31:21
Connected	25.52.81.0/24	0.0.0.0	fext-wan1	
Connected	169.254.1.1/32	0.0.0.0	ssl.root	
Connected	169.254.1.1/32	0.0.0.0	ssl.root	
Connected	172.20.120.0/24	0.0.0.0	wan1	
Connected	192.168.1.0/24	0.0.0.0	lan	
Connected	::1/128	::	root	

از فورتی گیت ۲ به مسیر **Router> Monitor> Routing Monitor** رفته و مطمئن می شویم که Route ها توسط پروتکل BGP از فورتی گیت به درستی و با موفقیت advertised شده اند.

## SSL VPN

در این قسمت اطلاعاتی در مورد پیکربندی انواع SSL VPN بدست خواهید آورد همچنین روش های مختلف احراز هویت کاربران در SSL VPN به شما آموخته می شود.

SSL VPN از Secure Socket Layer جهت ایجاد VPN استفاده می کند که قابلیت دسترسی به شبکه خصوصی تحت بستر اینترنت را به شما می دهد. ارتباط از طریق SSL VPN توسط یک مرورگر صورت می گیرد و هیچ برنامه ی جانبی مورد نیاز نمی باشد.

این بخش شامل دستورالعمل های است:

- ایجاد دسترسی برای کاربران راه دور با استفاده از SSL VPN

### فراهم کردن دسترسی برای کاربران راه دور با استفاده از SSL VPN

در این مثال شما خواهید دید که چگونه قابلیت اتصال به منابع شرکت و استفاده از اینترنت به کاربران راه دور توسط دستگاه فورتی گیت داده می شود. در فاز اتصال، دستگاه فورتی گیت بررسی می کند که آیا آنتی ویروس بر روی سیستم کاربر راه دور نصب می باشد یا خیر؟

۱. ساخت یک پرتال SSL VPN برای کاربران راه دور

۲. ساختن یک کاربر و یک گروه

۳. اضافه کردن یک آدرس برای شبکه داخلی

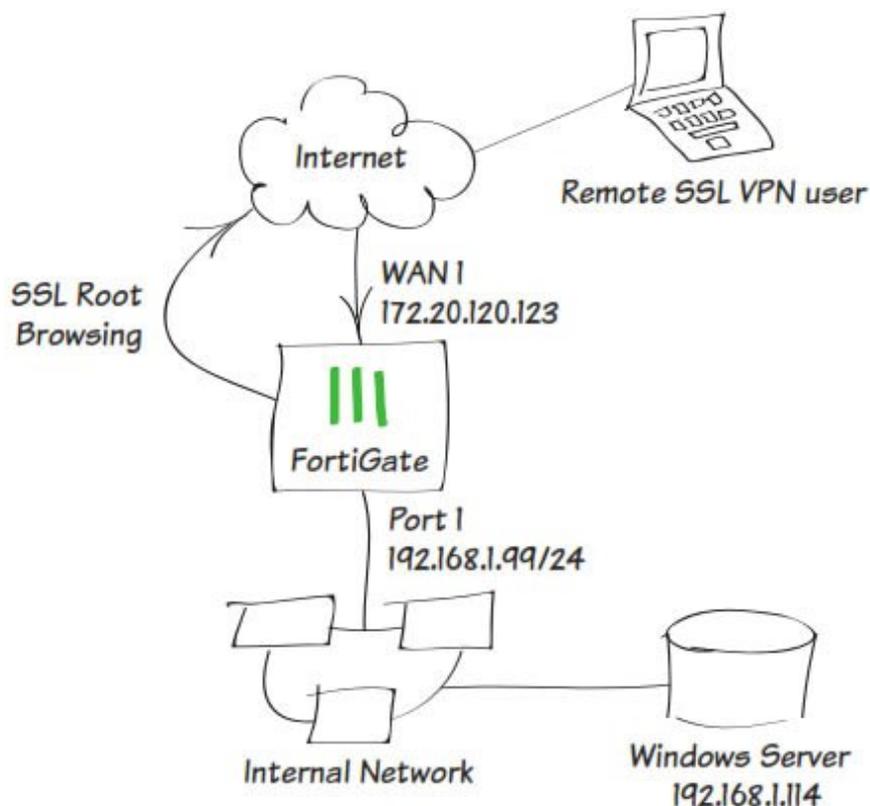
۴. پیکربندی تانل SSL VPN

۵. اضافه کردن Security Policy برای دسترسی به اینترنت و شبکه داخلی

۶. تنظیمات دستگاه فورتی گیت برای بررسی موجود بودن آنتی ویروس بر روی دستگاه کاربران راه

دور

۷. نتایج



#### ۱. ساختن یک پورتال SSL VPN برای کاربران راه دور

به مسیر **VPN > SSL > Portals** بروید. دکمه **Create New** را بزنید و یک اسم برای پورتال خود انتخاب کنید. همچنین می توانید به صورت پیش فرض پورتال **full-access** را ویرایش کنید.

پورتال **full-access** اجازه می دهد که از حالت تانل و یا حالت وب استفاده کنید. در این سناریو ما از هر دو حالت استفاده می نمایم.

**Enable Split Tunneling** فعال نمی باشد بنابراین همه ترافیک اینترنت از طریق فورتی گیت منتقل می شود و این بستگی به سیاست های امنیتی شرکت شما دارد.

در قسمت Predefined Bookmarks گزینه Create New را بزنید تا یک bookmark برای اتصال بسازید. Bookmark ها وقتی مورد استفاده قرار می گیرد که شما در نظر داشته باشید از منابع شبکه داخلی به صورت لینک استفاده نمایید.

یوزرنیم و پسورد باید در قسمت New Bookmark وارد شود. شما باید یوزر را در قسمت بعدی بسازید.

ساختن یک کاربر و یک گروه

به مسیر **User & Device > User > User Definition** بروید. یک کاربر راه دور با استفاده از Wizard اضافه کنید. در این مثال اسم کاربر ما twhite می باشد. توجه داشته باشید که این کاربر باید مشابه همان باشد که در قسمت predefined bookmark ساختید.

به مسیر **User & Devices > User > User Groups** بروید. یوزر 'twhite' به گروه SSL VPN اضافه کنید.

The screenshot shows the configuration for a new user group. The Name is 'sslvpn\_group'. The Type is set to 'Firewall'. The Members list includes 'twhite'. Below this is a table for Remote groups, which is currently empty with the message 'No matching entries found'. There are 'Add', 'Edit', and 'Delete' buttons above the table, and 'OK' and 'Cancel' buttons at the bottom.

### ۳. اضافه کردن آدرس برای شبکه داخلی

به مسیر **Policy & Objects > Objects > Addresses** بروید. آدرس مربوط به شبکه داخلی خود را در قسمت Subnet / IP Range وارد نمایید. همچنین اینترفیس داخلی را هم انتخاب کنید.

### ۴. تنظیمات تانل SSL VPN

به مسیر **VPN > SSL > Setting** مراجعه کنید و از قسمت Listen on Interface(s) اینترفیسی که مربوط به اینترنت شما می باشد را انتخاب کنید در اینجا ما Wan1 را انتخاب می کنیم.

The screenshot shows the configuration for SSL-VPN settings. The Listen on Interface(s) is 'wan1'. The Listen on Port is '443'. The Restrict Access is 'Allow access from any host'. The Idle Logout is 'Logout users when inactive for specified period' with a value of '5000' seconds. The Server Certificate is 'Fortinet\_Factory'. The Require Client Certificate is unchecked. The Tunnel Mode Client Settings section shows 'Specify custom IP ranges' selected with two IP ranges: 'SSLVPN\_TUNNEL\_ADDR1' and 'SSLVPN\_TUNNEL\_IPv6\_ADDR1'.

در قسمت Listen Port پورت 443 و Specify Custome IP Ranges را انتخاب کنید.

در زیر گزینه Authentication portal Mapping قسمت SSL VPN Group را انتخاب کنید.

### ۵. اضافه کردن Security Policies جهت دسترسی به شبکه های داخلی و اینترنت

به مسیر **Policy > IPv4 > Policy > Objects** بروید. یک Security Policy تعریف کنید که اجازه دسترسی به شبکه داخلی با استفاده از ssl.root VPN را داشته باشد.

Incoming Interface را برای ssl.root تنظیم نمایید.

Source Address را برای all انتخاب نمایید و Source User را برای گروه ساخته شده در مرحله دوم انتخاب کنید.

Outgoing Interface را برای شبکه داخلی انتخاب کنید با این کار کاربران راه دور می توانند به شبکه داخلی دسترسی داشته باشند.

Destination Address را در حالت all قرار دهید و NAT را به حالت Enable ببرید و تنظیمات دلخواه خود را برای فایروال و Security Option ها انجام دهید.

یک Security Policy دیگر جهت دسترسی SSL VPN ها به اینترنت ایجاد کنید. برای این پالیسی Incoming Interface را برای ssl.root تنظیم کنید و Outgoing Interface را در حالت wan1 تنظیم کنید.

Incoming Interface	ssl.root (sslvpn tunnel interface)	+
Source Address	all	+
Source User(s)	Click to add...	
Source Device Type	Click to add...	
Outgoing Interface	wan1	+
Destination Address	all	+
Schedule	always	
Service	ALL	+
Action	ACCEPT	

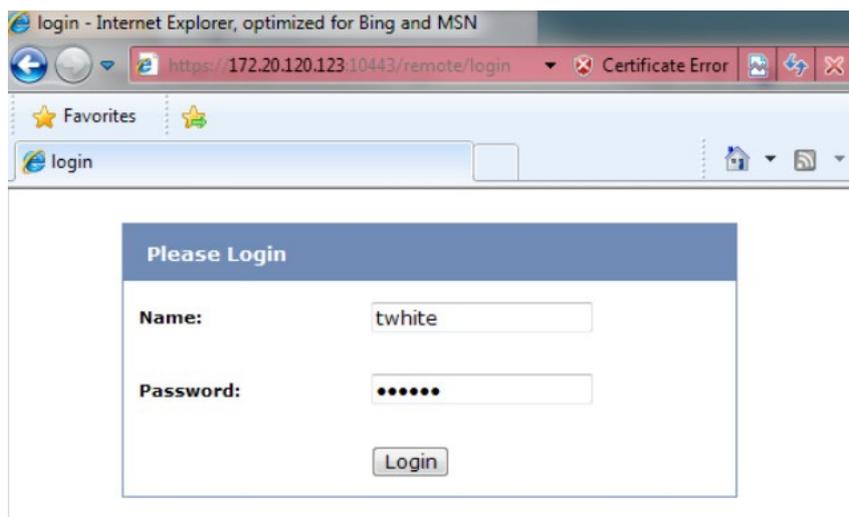
## ۶. تنظیم کردن دستگاه فورتی گیت جهت تشخیص برنامه آنتی ویروس کاربران

به مسیر **Dashboard > status > system** بروید. در CLI کنسول دستورات زیر وارد نمایید. با وارد کردن دستورات زیر باعث می شوید وضعیت آنتی ویروس کاربران راه دور مورد آزمایش قرار بگیرد.

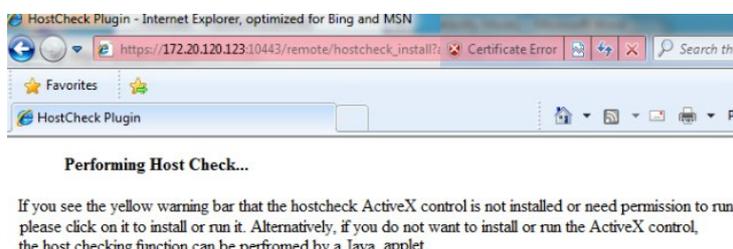
```
# config vpn ssl web portal
(portal) # edit full-access
(full-access) # set host-check av
(full-access) # end
```

## ۷. نتایج

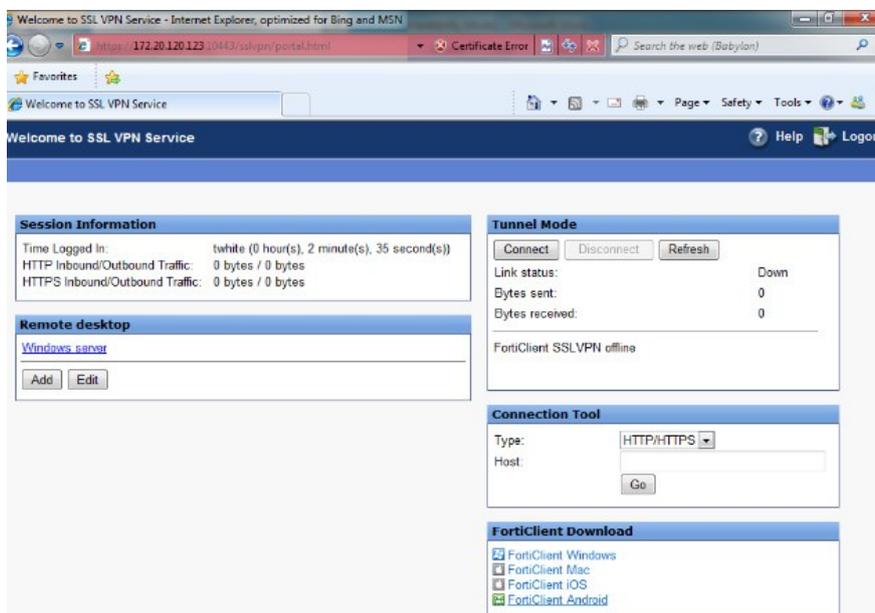
با استفاده از احراز هویت ساخته شده در قسمت دوم به پورتال لاگین کنید.



دستگاه فورتی گیت وضعیت هاست را مورد بررسی قرار می دهد.



بعد از چک شدن شرایط هاست پورتال نمایش داده می شود.



به مسیر **VPN > Monitor > SSL-VPN Monitor** بروید تا لیست کاربران SSL را مشاهده نمایید.

به مسیر **Log & Report > Traffic Log > Forward Traffic** بروید و جزئیات مورد نیاز خود در مورد **SSL** های متصل شده بدست آورید.

به مسیر **Log & Report > Traffic Log > Forward Traffic** بروید. دسترسی به اینترنت از طریق دستگاه فورتی گیت به صورت همزمان صورت می پذیرد. روی هر سطر کلیک نمایید می توانید اطلاعات بیشتری کسب کنید.

<b>Dst</b>	192.168.1.114	<b>Virtual Domain</b>	root
<b>Received</b>	85591	<b>Source Country</b>	Reserved
<b>Sent / Received</b>	8.71 KB / 83.58 KB	<b>Duration</b>	36
<b>Sent</b>	8923	<b>Application Details</b>	
<b>Group</b>	N/A	<b>Service</b>	RDP
<b>Protocol</b>	6	<b>User</b>	twhite
<b>Destination Country</b>	Reserved	<b>Dst Port</b>	3389
<b>roll</b>	65389	<b>Status</b>	✓
<b>Timestamp</b>	Wed Apr 17 14:13:11 2013	<b>Tran Display</b>	noop
<b>Sequence Number</b>	2700	<b>Policy ID</b>	11
<b>Src Interface</b>	wan1	<b>Src</b>	twhite (172.20.120.23)
<b>VPN</b>	sslvpn_web_mode	<b>Sent Packets</b>	71
<b>Level</b>	notice	<b>VPN Type</b>	sslvpn
<b>Src Port</b>	53712	<b>Log ID</b>	13
<b>Sub Type</b>	forward	<b>Threat</b>	
<b>Received Packets</b>	98	<b>Date/Time</b>	14:13:11 (Wed Apr 17 14:13:11 2013)
<b>Dst Interface</b>	port1		

#	Date/Time	Src Interface	Dst Interface	Src	Dst
1	14:26:05	ssl.root	wan1	10.212.134.200	74.125.133.95
2	14:26:04	ssl.root	wan1	10.212.134.200	173.194.77.94
3	14:26:04	ssl.root	wan1	10.212.134.200	173.194.43.79
4	14:26:03	ssl.root	wan1	10.212.134.200	66.171.121.34 (fortinet.co)
5	14:25:57	ssl.root	wan1	10.212.134.200	74.121.50.17 (www.pages)
6	14:25:44	ssl.root	wan1	10.212.134.200	208.91.113.212
7	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30
8	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30
9	14:25:40	ssl.root	wan1	10.212.134.200	192.168.55.30
10	14:24:39	ssl.root	wan1	10.212.134.200	213.199.179.159
11	14:24:37	ssl.root	wan1	10.212.134.200	213.199.179.159
12	14:24:37	ssl.root	wan1	10.212.134.200	132.246.2.6 (www.mefn)

### پیکربندی معماری Redundant جهت استفاده از دو فورتی گیت و سوئیچینگ داخلی

دستورالعمل های زیر برای مشتریانی مفید است که از معماری چند سایت و فایروال های Redundant استفاده می نمایند. این روش ها برای مشتریانی در نظر گرفته شده که کاهش لوازم یک بخش و افزایش امنیت برای آنها در اولویت می باشد و همچنین کاهش هزینه ها برای کارفرما مهم می باشد، بلکه هدف کاملاً ساده است: قابلیت اطمینان و مقرون به صرفه بودن.

FortiOS 5.2 امکانات بسیار زیادی معرفی کرده است که ما درصدد هستیم در این تنظیمات استفاده نماییم، بنابراین بعضی از این تنظیمات بر روی FortiOS 5.0.x یا قبل از آن امکان پذیر نمی باشد. این دستورات در سری FortiGate 1xxD/2xxD قابل اجرا می باشد.

با توجه به دستوراتی که به شما یاد داده می شود، شما می توانید به مشتریان کوچک پیشنهاداتی بدهید که زیرساخت امن و کاملی داشته باشند که بر اساس دیدگاه های UTM تنظیم شده است. در اینجا ما می خواهیم قابلیت های امنیتی زیادی را روی یک دستگاه یا کلاستر ایجاد و متمرکز کنیم.

دستورالعمل ها باعث می شود که به صورت کامل installation انجام شود. این موارد به بخش های زیر تقسیم می شود:

### ۱. سناریو

این قسمت در مورد مشکلاتی که وجود داشته و توسط توپولوژی شبکه جدید حل خواهد شد توضیحاتی می دهد که شامل موارد و مشکلاتی است که توسط توپولوژی ها حل می شود.

### ۲. توپولوژی

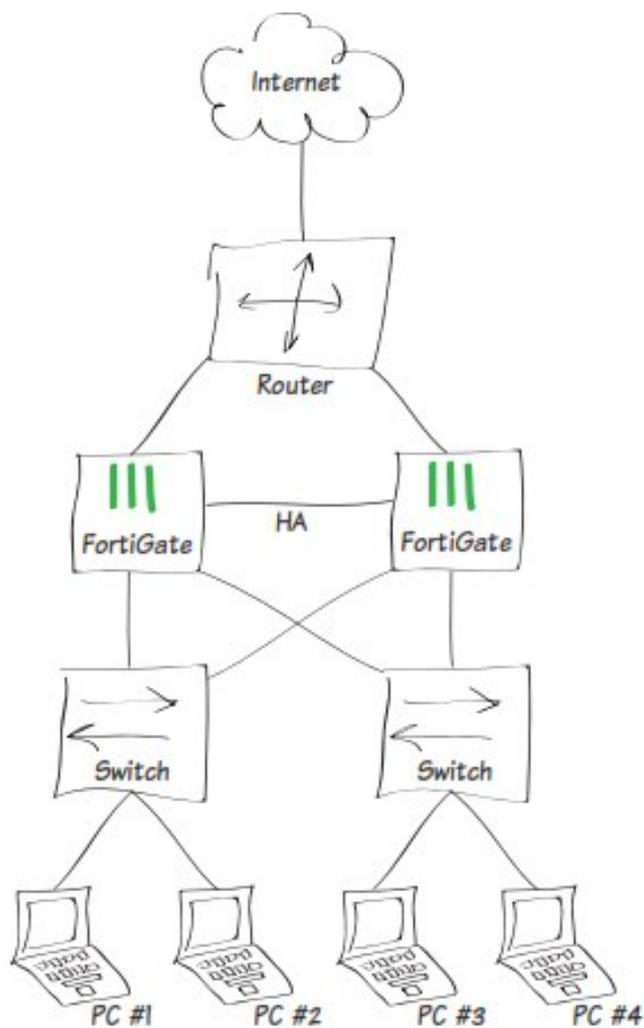
این بخش شامل دیاگرامی از توپولوژی جدید است. همچنین لیستی از ویژگی های کلیدی است. این نوع از معماری ها و توضیحات که مشکلات شناسایی شده در سناریوی قبلی را شناسایی و حل می کند.

### ۳. پیکربندی

این بخش دستورالعملی مرحله به مرحله تهیه کرده و برای پیکربندی فورتی گیت در حالت توپولوژی جدید کاربردی می باشد.

### ۱. سناریو

در سناریو استاندارد، ما فرض توپولوژی زیر را بعنوان نقطه شروع در نظر می گیریم:

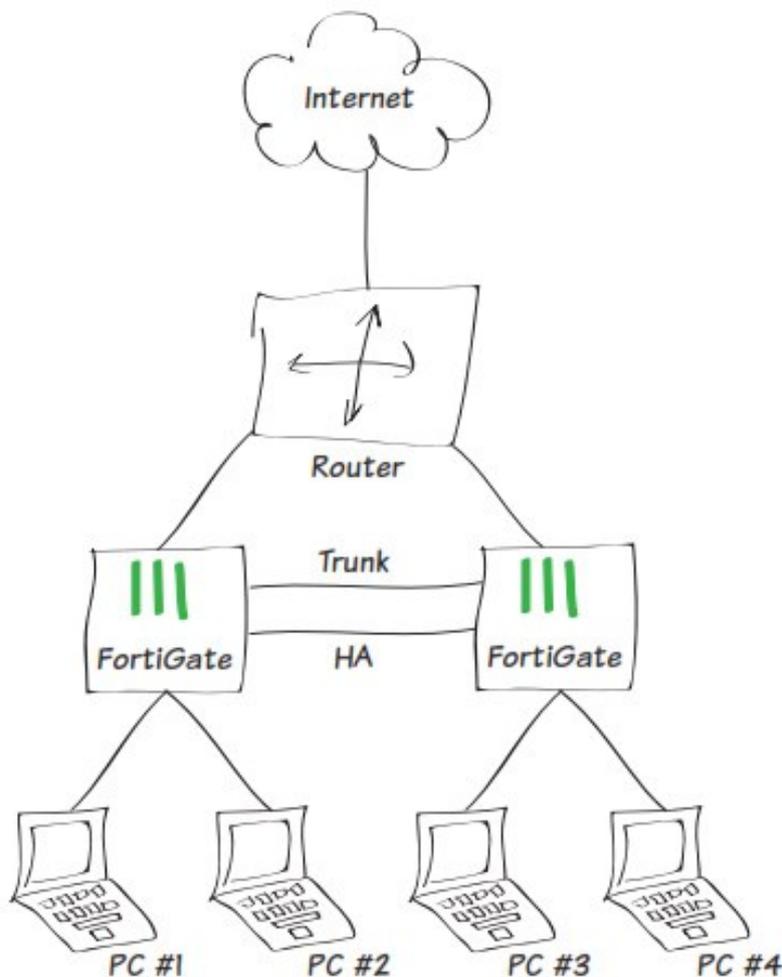


مشتریانی که تمایل دارند از هرگونه قطعی و خرابی اجتناب کنند اغلب از توپولوژی بالا استفاده می نمایند. این مشتریان به دو دستگاه فورتی گیت در حالت Active/Passive نیاز دارند. بنابراین دو عدد سوئیچ در شبکه داخلی جهت تقسیم payload (جابجایی بار) فورتی گیت ها نیاز می باشد.

- چهار دستگاه مورد نیاز می باشد تا بتوانیم نظارت و مدیریت درستی داشته باشیم.
- ادمین ها باید توجه داشته باشند که چگونه با Firewall OS و Switch OS کار کنند.
- اگر یک سوئیچ fail شود. کامپیوترها نمی توانند به اینترنت دسترسی داشته باشند.
- اغلب پورت های فایروال مورد استفاده قرار نمی گیرد.

در این قسمت، نگاهی می‌اندازیم به هدف توپولوژی و سناریوهایی برای failover فورتی گیت. در انتها ما در مورد نقاط قوت صحبت می‌کنیم و بر اساس اهداف توپولوژی تصمیم لازم را اتخاذ خواهیم کرد.

## ۲-۱ هدف توپولوژی

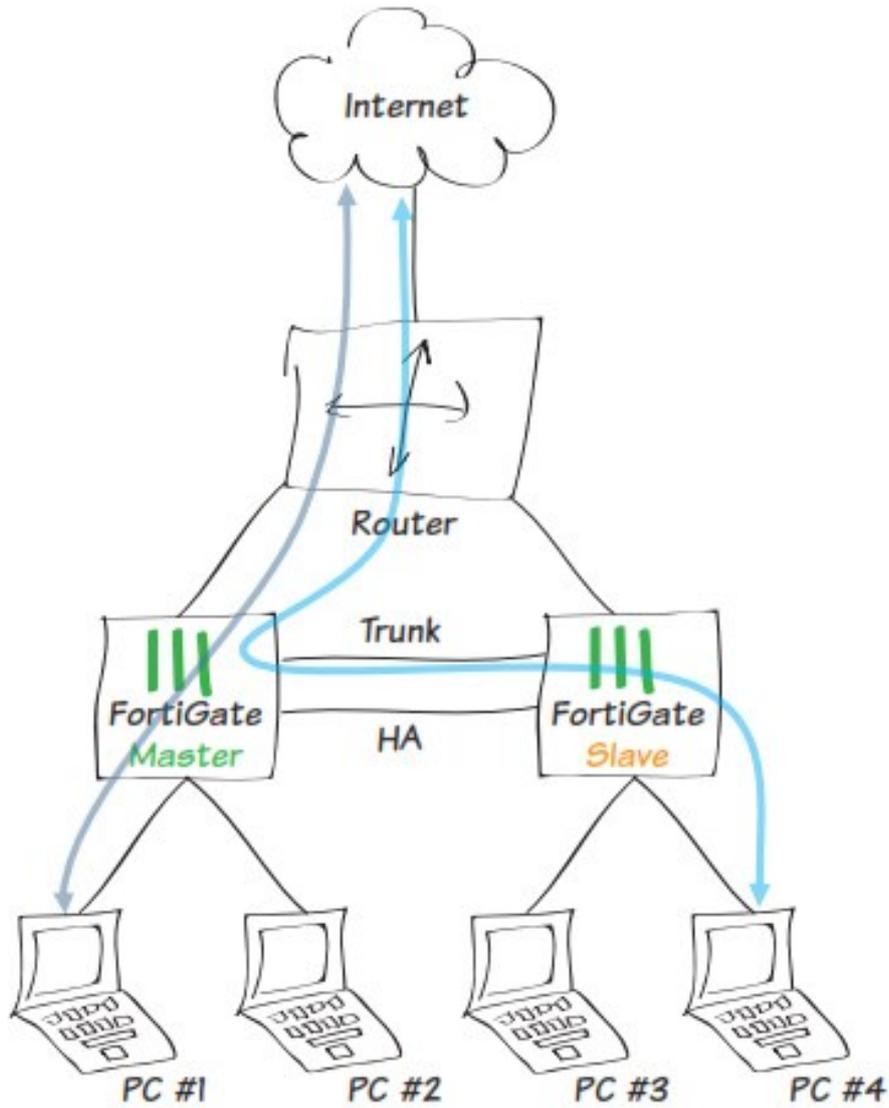


در این توپولوژی، ما نمی‌توانیم از سوئیچ‌های اضافی استفاده نماییم. و به جای آن از راه حل فورتی گیت‌های یکسان شده (ترکیب شده) سوئیچی در هر دو حالت master و slave استفاده می‌نماییم.

ادمین لینک بین دو دستگاه فیزیکی فورتی گیت سوئیچ شده را به صورت trunk کانفیگ می‌کند تا کانفیگ مربوط به ساب‌نت‌ها و VLAN‌ها از یکی به دیگری منتقل شود.

در حالت کلاستر از FGCP استفاده می‌شود، در حالت slave فایروال می‌تواند ترافیک را برای بقیه توسط لینک ترانک ارسال نماید.

شکل زیر توصیف‌کننده موارد بالا می‌باشد:

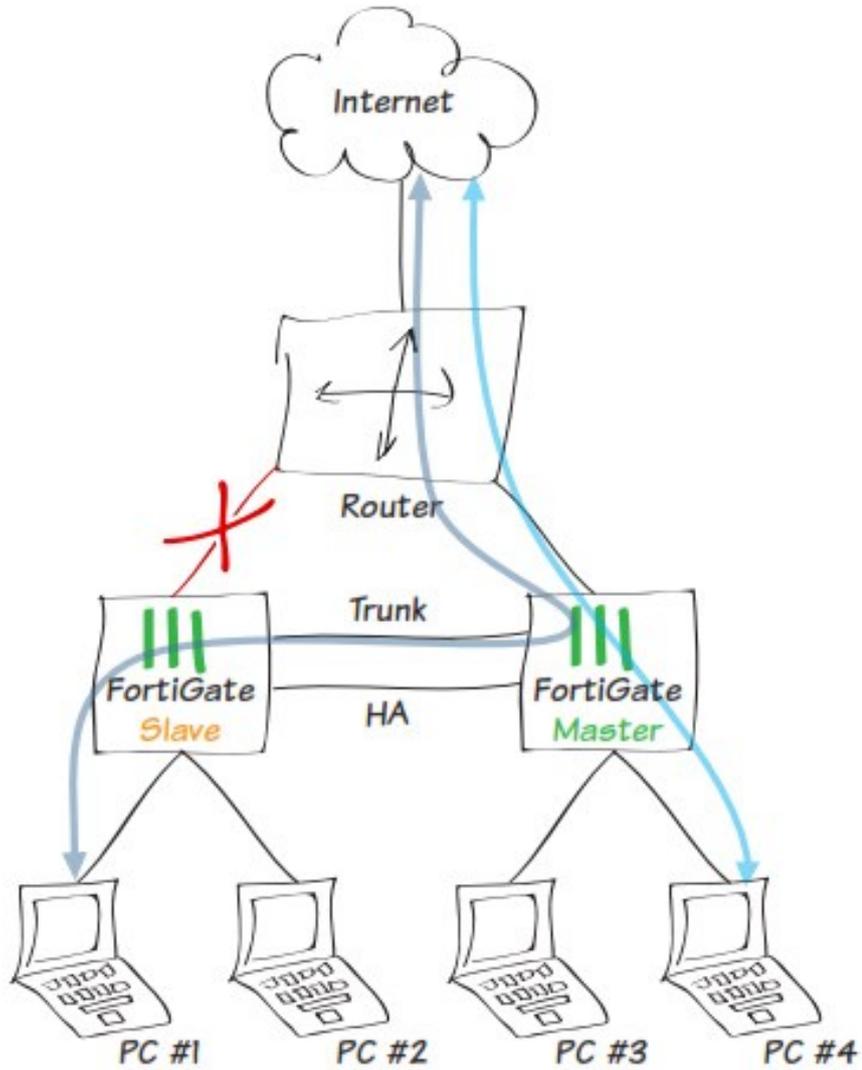


## ۲-۲ Fortigate Failover

مورد اول: Link failure

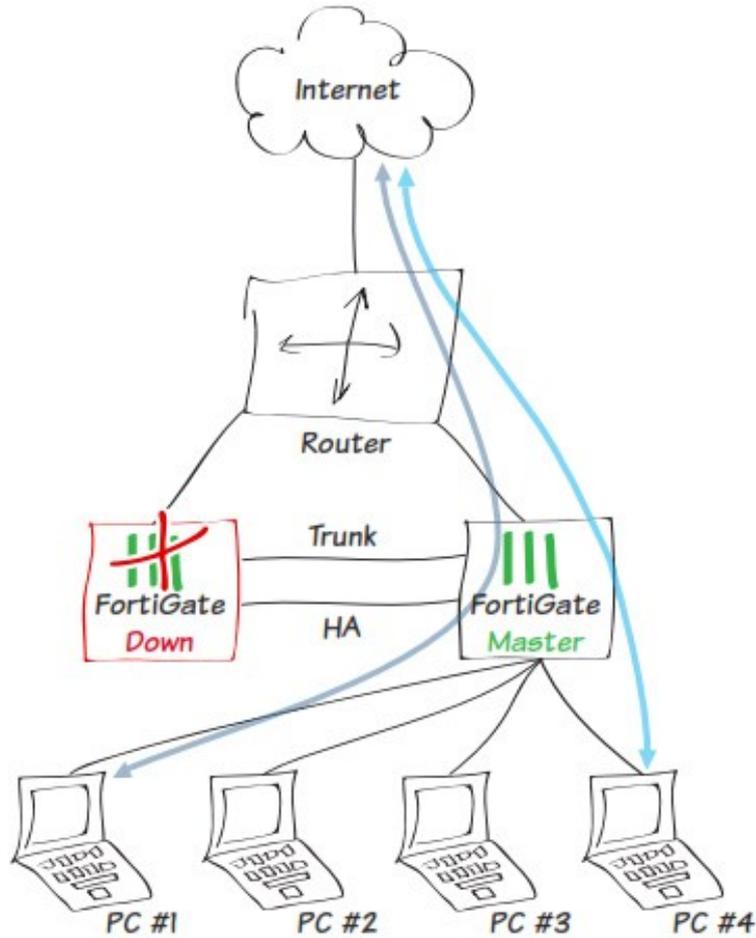
دیگرام زیر نمایش دهنده ی جریان عبوری ترافیک می باشد:

- مانیتور کردن پورت مربوط به اینترنت، در حالتی که فورتنی گیت اصلی از کار بیفتد.
- لینک بین روتر و فورتنی گیت اصلی از کار بیفتد.



مورد دوم: فورتنی گیت اصلی از کار بیفتد:

اگر دستگاه اصلی به صورت کامل از کار بیفتد، ادمین باید به صورت دستی سیگمنت مربوط به LAN را به فایروال سالم متصل کند، در این توپولوژی فقط یک سوئیچ می تواند از کار بیفتند.



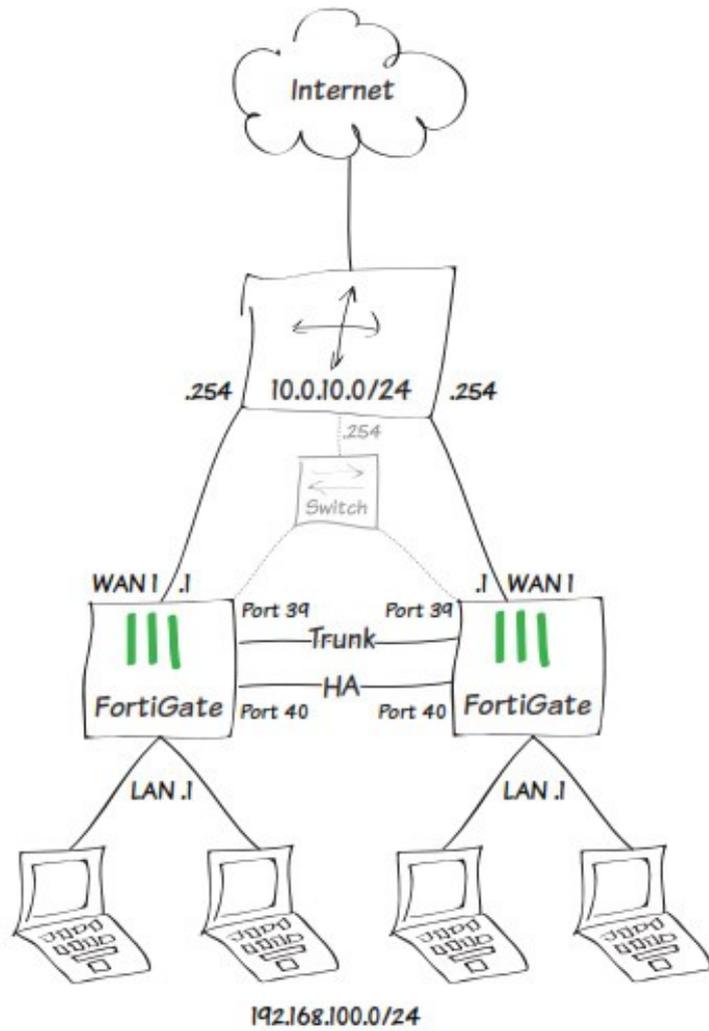
### ۲-۳ مزیت های کلیدی

این توپولوژی نقاط کلیدی را برای شما به ارمغان می آورد:

- فقط دو دستگاه مورد نیاز می باشد، در صورتی که در توپولوژی استاندارد ۴ دستگاه مورد نیاز بود.
- برای ادمین ها مدیریت امنیت و سوئیچینگ روی یک دیوایس بسیار راحت تر است.
- استفاده از FortiManager جهت مدیریت یکپارچه از دستگاه ها
- تنها یک کلاستر جهت نظارت وجود دارد.

### ۳. پیکربندی

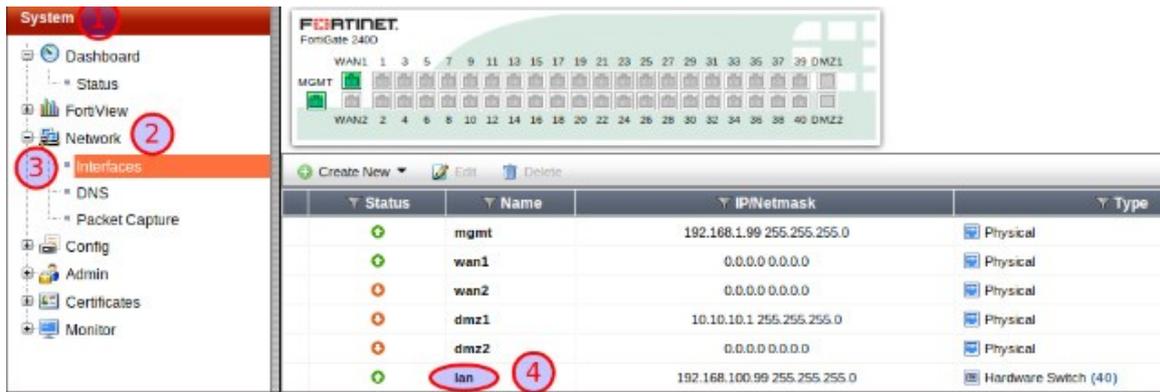
در این قسمت، ما توپولوژی شبکه ای بالا را مجدداً ایجاد خواهیم کرد. توجه داشته باشید که روتر چگونه یک اینترفیس سوئیچ دارد.



### قدم اول: پیکربندی سخت افزاری سوئیچ

به صورت پیش فرض فورتی گیت های سری 1xxD,2xxD ، دستگاه بر روی interface مُد می باشد و تمام پورت های داخلی به سوئیچی به نام LAN متصل می باشند. در این مثال ما به پورت های 39 و 40 برای ترانک شدن و HA نیاز داریم.

اولین قدم پاک کردن پورت های 39 و 40 از LAN سوئیچ می باشد. با ویرایش اینترفیس LAN شروع می کنیم. اگر دستگاه در حالت سوئیچ مُد باشد، باید دوباره تنظیم شده و به مُد Interface برود.



به مسیر **System > Network > Interface** رفته و بر روی LAN دابل کلیک کنید. پورت های 39 و 40 را از لیست پاک نمایید. سپس تنظیمات IP/Network Mask را بر اساس زیر وارد کنید:

IP/Network Mask : 192.168.100.1/255.255.255.0

وقتی کار تمام شد تنظیمات را اعمال نمایید.

حالا وضعیت اینترفیس شما چیزی شبیه عکس زیر باید می باشد:

Status	Name	IP/Netmask	Type
Up	mgmt	192.168.1.99 255.255.255.0	Physical
Up	wan1	0.0.0.0 0.0.0.0	Physical
Down	wan2	0.0.0.0 0.0.0.0	Physical
Down	dmz1	10.10.10.1 255.255.255.0	Physical
Down	dmz2	0.0.0.0 0.0.0.0	Physical
Up	lan	192.168.100.1 255.255.255.0	Hardware Switch (38)
Down	port39	0.0.0.0 0.0.0.0	Physical
Down	port40	0.0.0.0 0.0.0.0	Physical

برای اینکه پورت ترانک بدرستی کار کند ما باید VLAN ID را روی سوئیچ تنظیم کنیم. این فقط در CLI انجام پذیر می باشد.

در اولین قدم ما باید قابلیت globally را فعال نماییم. دستورات در زیر نمایش داده شده است:

```
FGT1 # config system global
FGT1 (global) # set virtual-switch-vlan
```

```

enable
FGT1 (global) # end
FGT1 # show system global
config system global
set fgd-alert-subscription advisory
latest-threat
set hostname "FGT1"
set internal-switch-mode interface
set optimize antivirus
set timezone 04
set virtual-switch-vlan enable
end

```

در مرحله بعدی ویرایش Vswitch و تنظیم VLAN ID صورت میگیرد:

```

FGT1 # config system virtual-switch
FGT1 (virtual-switch) # edit lan
FGT1 (lan) # set vlan 100
FGT1 (lan) # end

```

بعد از زدن دستورات بالا از الان شما باید بتوانید VLAN Switch را در اینترفیس لیست مشاهده نمایید.

Status	Name	IP/Netmask	Type
+	mgmt	192.168.1.99 255.255.255.0	Physical
+	wan1	0.0.0.0 0.0.0.0	Physical
+	wan2	0.0.0.0 0.0.0.0	Physical
+	dmz1	10.10.10.1 255.255.255.0	Physical
+	dmz2	0.0.0.0 0.0.0.0	Physical
+	lan (VLAN ID: 100)	192.168.100.1 255.255.255.0	VLAN Switch (38)
+	port39	0.0.0.0 0.0.0.0	Physical
+	port40	0.0.0.0 0.0.0.0	Physical

مرحله دوم: تنظیم ترانک پورت

مورد استفاده ی پورت ترانک برای عبور ترافیک بین دو virtual Switch هر فورتی گیت می باشد. پیکربندی پورت ترانک فقط با دستورات زیر امکان پذیر می باشد:

```

FGT1 # config system interface
FGT1 (interface) # edit port39
FGT1 (port39) # set trunk enable
FGT1 (port39) # end
FGT1 # show system interface port39
config system interface
edit "port39"
set vdom "root"
set type physical
set trunk enable
set snmp-index 10
next
end

```

در حال حاضر شما باید بتوانید پورت ترانک را در اینترفیس لیست مشاهده کنید.

مرحله سوم: پیکربندی HA

حالا نوبت به High Availability رسیده است. پورت 40 برای heartbeat/Sync جهت ارتباط بین اعضای کلاستر مورد استفاده قرار می گیرد. پورت WAN1 هم برای مانیتور مورد استفاده قرار می گیرد. به مسیر **System > Config > HA** رفته و High Availability را مانند زیر تنظیم نمایید:

### مرحله چهارم: پیکربندی WAN IP routing

به مسیر **System > Network > Interface** بروید و WAN1 را ویرایش کنید دقیقا مانند زیر:

Interface Name: wan1(08:5B:0E:32:5C:E4)  
 Alias: **1** Internet  
 Link Status: Up  
 Type: Physical Interface  
 Addressing mode: **2** Manual (selected), DHCP, PPPoE, Dedicate to Extension Device  
 IP/Network Mask: **3** 10.0.10.1/24  
 Administrative Access:  HTTPS,  PING,  HTTP,  FMG-Access,  CAPWAP,  SSH,  SNMP,  FCT-Access,  Auto IPsec Request  
 DHCP Server:  Enable  
 Security Mode: None  
 Device Management: Detect and Identify Devices   
 Listen for RADIUS Accounting Messages:   
 Secondary IP Address:   
 Comments: Write a comment... 0/255  
 Administrative Status:  Up,  Down  
**4** OK Cancel

به مسیر **Router > Static > Static Routes** بروید و یک route همانند توضیحات زیر بسازید:

Destination IP/Mask: **1** 0.0.0.0/0.0.0.0  
 Device: **2** wan1  
 Gateway: **3** 10.0.10.254  
 Distance: 10 (1-255, Default=10)  
 Priority: 0 (0-4294967295)  
 Comments: Write a comment... 0/255  
**4** OK Cancel

### مرحله پنجم: پیکربندی پالسی های فایروال

به مسیر **Policy & Objects > Policy > IPv4** بروید و پالسی های دلخواه خود را پیکربندی کنید.

### مرحله ششم: تکرار تنظیمات بر روی دستگاه دوم

وقتی برای اولین بار فورتی گیت را تنظیم می کنید، آسان ترین راه برای انجام تنظیمات بر روی دستگاه دوم تهیه یک بکاپ از تنظیمات دستگاه اول و بازیابی بر روی دستگاه دوم می باشد.

به مسیر **System > Dashboard > Status** بروید و از قسمت System Configuration گزینه Backup را انتخاب کنید. با استفاده از همین مسیر و انتخاب گزینه Restore می توانید تنظیمات را بر روی دستگاه دوم بازیابی نمایید.

## واژه نامه :

**BGP**: *Boarder Gateway Protocol* در درجه ی اول جهت استفاده و اتصال شبکه های بزرگ قرار دارد. این پروتکل می تواند چند ISP یا بیشتر را با یکدیگر متصل نماید، یا بین autonomous سیستم ها ارتباط برقرار نماید. اگر شما در این شرایط از فورتی گیت استفاده می کنید کاملاً جوابگوی شما خواهد بود.

**Certificates**: در شبکه، گواهینامه ها شامل کلیدهای عمومی، گواهینامه های دیجیتالی، گواهینامه های شناسایی تامین کننده امضای دیجیتالی می باشد برای وب سایت ها یا سایر ارتباطات الکترونیکی به شما اجازه می دهد که بررسی نمایید آیا یک هویت دیجیتال مشروع و درست می باشد. یک فورتی گیت می تواند از گواهینامه ها برای چیزهای زیادی شامل بازرسی SSL و اعتبارسنجی کاربران استفاده نماید.

**CLI**: *Command Line Interface* بر اساس تکست بوده و جهت پیکربندی دستگاه فورتی گیت در محیط کامند مورد استفاده قرار می گیرد. بیشتر مراحل در این کتاب به صورت گرافیکال دنبال شده است، اما بعضی از تنظیمات تنها در محیط دستوری موجود می باشند.

**DHCP**: *Dynamic Host Configuration Protocol* یک پروتکلی از شبکه می باشد که به دستگاه های شبکه اجازه دریافت بعضی از پارامترها را می دهد. یکی از این پارامترها IP Address می باشد. یک دستگاه فورتی گیت می تواند این وظیفه را برعهده گرفته و همانند یک DHCP سرور عمل نماید تا دستگاه های موجود در شبکه ی شما IP دریافت نمایند.

**DMZ**: *Demilitarized Zone* یک اینترنت فورتی گیت می باشد که به کاربران خارجی با دسترسی امن و حفاظت شده اجازه می دهد به شبکه داخلی دسترسی داشته باشند. این دسترسی بدون دستیابی به سایر قسمت های شبکه صورت می گیرد. این کار اغلب برای subnet هایی شامل وب سرورها انجام می شود. بیشتر مواردی که باید از بیرون به آنها دسترسی وجود داشته باشد. اینترنت DMZ فقط به ترافیکی اجازه عبور می دهد که صریحاً در تنظیمات فورتی گیت وجود داشته باشد. بعضی از مدل های فورتی گیت اینترنت DMZ ندارند البته شما می توانید از سایر اینترنت فیس ها جهت این مورد استفاده نمایید.

**DNS**: *Domain Name System* بوسیله دستگاه هایی که متصل به اینترنت هستند مورد استفاده قرار می گیرد تا وب سایت ها را بوسیله mapping کردن یک اسم دامین به IP آدرس شناسایی نماید. برای مثال DNS سرور نام fortigate.com را به IP آدرس 66.171.121.34 تبدیل می کند. دستگاه فورتی گیت مشخص می نماید که کدام DNS سرور در شبکه مورد استفاده قرار گیرد. فورتی گیت می تواند وظیفه یک DNS سرور را نیز برعهده بگیرد.

**ECMP: Equal Cost Multipath Routing** اجازه می دهد به هاپ های بعدی که پکت های ارسالی را برای یک مقصد ارسال نمایند تا بین چندین مسیر، بهترین انتخاب شود. ECMP توسط فورتی گیت برای اهداف متعددی مورد استفاده قرار می گیرد. یکی از آنها load balancing می باشد.

**Explicit Proxy:** حالتی از پیکربندی می باشد که به کلاینت ها اجازه می دهد تا درخواست هایشان را به یک پروکسی سرور ارسال نمایند. وقتی یک سرور بعنوان واسط مورد استفاده قرار می گیرد برای درخواست هایی که از طرف کلاینت ها ارسال می شود. یک فورتی گیت وقتی از حالت explicit proxy استفاده می کند، کلاینت ها IP آدرس ها و شماره پورت ها را برای پروکسی سرور ارسال می کنند.

**FortiAP:** دستگاه اکسس پوینت می باشد که می تواند توسط یک دستگاه فورتی گیت مدیریت شود. بیشتر وظایف FortiAP می تواند با استفاده از یک دستگاه FortiWiFi انجام شود.

**FortiOS:** سیستم عاملی می باشد که بوسیله Fortigate و FortiWiFi مورد استفاده قرار می گیرد. برای فهم بهتر می توان به یک فریمور تشبیه کرد.

**Gateway:** اگر دستگاهی نتواند آدرس مقصد را در سابلنت خود پیدا کند پکت را به Gateway خود تحویل می دهد.

**GUI: Graphical User Interface.** بیشتر افراد اسم web-based manager می شناسند، یک اینترفیس گرافیکی می باشد جهت انجام تنظیمات مربوط به فورتی گیت به جای استفاده از دستورات خشک و خسته کننده ی CLI

**HTTP: Hypertext Transfer Protocol** پروتکلی می باشد که جهت ارتباطات استفاده می شود و نا امن بوده، شامل اینترنت و دستیابی به وب سایت ها است. فورتی گیت می تواند ترافیک های مربوط به این پروتکل را نیز مدیریت کند.

**HTTPS: Hypertext Transfer Protocol Secure** پروتکل امن HTTP می باشد که ارتباطات را با پروتکل امن امکان پذیر می سازد.

**Interfaces:** نقطه ای می باشد که ارتباطات بین دو بخش متفاوت در این قسمت انجام می شود. این نقاط می تواند فیزیکی باشد، مانند Ethernet پورت ها روی یک فورتی گیت، یا به صورت منطقی همانند یک VPN Portal

**IPsec:** جهت ایجاد امنیت در ارتباطات بکار برده می شود به طوری که هر پکت یک session کدگذاری می شود. فورتی گیت اساسا از این پروتکل جهت ارتباط VPN استفاده میکند.

**LDAP**: *Lightweight Directory Access Protocol* پروتکلی می باشد برای دسترسی و نگهداری از سرویس های توزیع یافته directory information می باشد. سرورهای LDAP به صورت معمول با یک فورتی گیت برای بحث authenticate کاربران مورد استفاده قرار می گیرند.

**MAC address**: *Media Access Control address* یک شناسه خاص و همتا می باشد برای اینترفیس شبکه جهت ارتباطات. یک مک آدرس به یک دیوایس داده می شود این مک آدرس توسط کارخانه سازنده داده می شود و به هیچ عنوان شبیه IP آدرس نمی باشد و به صورت نرمال قابل تغییر نمی باشد. مک آدرس در ۶ قسمت دوتایی از اعداد هگزادسیمال تشکیل شده است که توسط کالون از یکدیگر جدا می شوند. برای مثال 01:23:45:67:89:ab . دستگاه فورتی گیت شما شناسایی خواهد کرد دیوایس هایی که از مک آدرس استفاده می کنند.

**Multicast**: یک مُتد از ارتباط به صورت گروهی می باشد که اطلاعات برای یک گروه ارسال می شود. فورتی گیت می تواند از ترافیک مالتی کست جهت ایجاد ارتباط بین دستگاه های شبکه استفاده نماید.

**NAT**: *Network Address Translation* یک پروسه است که برای تغییرات و یا ترجمه IP آدرس های مبدا یا مقصد مورد استفاده قرار می گیرد. استفاده اصلی از NAT اجازه دادن به چندین دیوایس شبکه بر روی بستر داخلی جهت دسترسی به بیرون با استفاده از یک IP پابلیک وقتی که قصد استفاده از اینترنت را دارند. فورتی گیت از کاربردهای بیشمار NAT پشتیبانی می کند.

**Packet**: یک قسمتی از دیتا می باشد که بین دیوایس های ارتباطی ارسال می شود. یک پکت شامل دو قسمت پیام و اطلاعات کنترلی می باشد، همانند آدرس مبدا ( IP آدرسی دستگاهی که پکت را می فرستد) و آدرس مقصد ( IP آدرس دستگاهی که بسته را ارسال کرده است)

**PING**: یک دستور بسیار سودمند می باشد که با استفاده از این دستور شما می توانید متوجه شوید که یک دستگاه به شبکه متصل می باشد یا خیر؟ همچنین با استفاده از زمان reply متوجه می شوید زمان بازگشت چه مقداری می باشد. پروتکلی که پینگ استفاده میکند ICMP می باشد. اگر ICMP روی مقصد فعال باشد، شما می توانید دستگاه مقصد را پینگ کنید. شما با استفاده از دستور `execute ping` در محیط CLI می توانید از وضعیت دستگاه مقصد آگاه شوید.

**Port Number**: شماره پورت نقاط پایانی ارتباطات است که در ارتباطات شبکه مورد استفاده قرار می گیرد. پورت های مختلف در برنامه های مختلف فرق می کند.

**RADIUS**: مدیریت AAA – Authorization, Authentication, Accounting برای کاربران که از راه دور متصل می شوند و از سرویس های شبکه استفاده می کنند توسط این بخش انجام می شود. Radius سرورها

به صورت معمول با یک فورتنی گیت مورد استفاده قرار می گیرند اینکار برای کاربرانی که در داخل SSO احراز هویت شده اند مورد استفاده قرار می گیرد.

**Session:** یک session دیالوگی هست بین دو یا بیشتر دستگاه های ارتباطی که شامل همه پیام های عبوری بین دستگاه ها است. برای مثال یک session وقتی که یک کاربر از یک سایت بازدید میکند ساخته می شود. session ها برای تمام ارتباطات بین کاربران کامپیوتر و وب سرور ها کاربرد دارد. Session ها بوسیله یک دستگاه فورتنی گیت ردیابی می شوند به شرطی که در قسمت ایجاد لاگ انتخاب شده باشد.

**SIP:** *Session Initiation Protocol* برای کنترل session های ارتباطی مالتی مدیا همانند voice و ویدئو تحت بستر اینترنت استفاده می شود. فورتنی گیت از این پروتکل برای عبور صدا بر روی IP استفاده میکند.

**SNMP:** *Simple Network Management Protocol* پروتکلی است که سخت افزارهای روی شبکه شما را مانیتور می کند. دستگاه فورتنی گیت می تواند از پروتکل SNMP استفاده کند تا وقایعی مانند میزان استفاده از CPU و VPN Tunnel ها و ... را مانیتور نماید.

**SSH:** *Secure Shell* پروتکلی می باشد که برای ایجاد امنیت سرویس ها در شبکه استفاده میشود. شامل دسترسی راه دور از طریق command-line می باشد. SSH می تواند جهت دسترسی به دستگاه فورتنی گیت مورد استفاده قرار بگیرد.

**SSID:** *Service Set Identifier* اسمی می باشد که اکسس پوینت broadcast می کند تا کاربران شبکه وایرلس به آن متصل شوند.

**SSL:** *Secure Socket Layer* پروتکلی برای رمزگذاری اطلاعاتی که در شبکه رد و بدل می شوند. SSL می تواند جهت ارتباطات امن در فورتنی گیت استفاده شود. همچنین برای رمزگذاری ترافیک اینترنت مورد استفاده قرار می گیرد و برای ایجاد دسترسی کاربران راه دور از طریق VPN مورد استفاده قرار می گیرد.

**SSL inspection:** برای استفاده فورتنی گیت می باشد تا ترافیک را اسکن کرده یا session های ارتباطی که از SSL برای رمزگذاری استفاده می کنند بررسی نماید.

**SSO:** قابلیت که به کاربر اجازه می دهد با یکبار لاگین شدن به صورت خودکار یک سری از دسترسی های مشخص را داشته باشد.

**Static route:** اعمال تنظیمات دستی روتینگ که ثابت بوده و قابلیت تغییر ندارد و به صورت دستی اضافه و یا کم می شود.

**Subnet**: یک Subnetwork یا Subnet یک سیگمنتی از شبکه می باشد که به صورت فیزیکی و یا منطقی جدا شده است. جدا کردن شبکه به ساب نت های مختلف باعث ایزوله کردن ترافیک عبوری شده و به کارایی شبکه کمک شایانی می نماید.

**Subnet Mask**: یک قسمتی از آدرس IP می باشد که تعیین می کند اگر دو آدرس در یک ساب نت مشابه هستند بتوانند به یکدیگر دسترسی داشته باشند.

**VLAN**: Virtual Local Area Network به صورت منطقی LAN به قسمت های کوچک تری تقسیم می شود که وظایف و کارایی مستقل تری داشته باشد. دستگاه فورتی گیت می تواند vlan های مختلفی را ایجاد کرده تا کاربران بتوانند با سطوح دسترسی متفاوتی به آنها دسترسی داشته باشند.

**VDOM**: Virtual Domain برای تقسیم یک دستگاه فورتی گیت به دو یا بیشتر فورتی گیت استفاده می شود که همه ی آنها دارای FortiOS بوده و قابلیت های مجزایی دارند و می توانند به صورت مستقل مدیریت بشوند.

**VoIP**: Voice Over Internet پروتکلی که باعث ایجاد ارتباطات صوتی میشود و session های مالتی مدیا را روی پروتکل اینترنت عبور می دهد.

**VPN**: Virtual Private Network دستیابی به شبکه داخلی از طریق بستر اینترنت و ایجاد دسترسی برای کاربران راه دور جهت استفاده از منابع شبکه داخلی می باشد. دو نوع اصلی از وی پی ان که توسط فورتی گیت تنظیم می شود شامل: IPsec VPN و SSL VPN می باشد.

**WAN/WANI**: WAN یا WAN1 پورتهای بر روی Fortigate می باشد که در اغلب موارد جهت اتصال دستگاه به اینترنت استفاده می شود. بعضی از مدل ها، فورتی گیت دارای پورتهای به اسم WAN2 می باشند که جهت لینک Redundant مورد استفاده قرار می گیرد.