ایمن شبکه هوشمند

واحد پشتیبانی فنی

امن‌سازی شبکه با Fortigate Firewall

نگارنده: محمود کریمی

تابستان ۱۴۰۳

Fortigate Firewall

1 Introduction

فایروال فورتی‌نت به عنوان یک محصول پیشرو در حوزه امنیت و با استفاده از راهکارهای جامع خود قابلیت‌های گسترده ای را برای تامین امنیت در شبکه‌ها فراهم کرده است. قابلیت هایی همچون تکنولوژی Virtual SPU [1] و سیستم‌های امنیتی پیشرفته که بهره‌وری بالایی دارند. یکی از محصولاتی که توسط شرکت Fortinet ارائه می‌شود، فایروال‌های FortiGate هستند. فایروال نسل جدید فورتی‌نت ترافیک شبکه را به منظور محافظت سازمان در برابر تهدیدات خارجی فیلتر می‌کند. این فایروال سخت افزاری امکاناتی از جمله کنترل برنامه‌ها، جلوگیری از نفوذ و نظارت پیشرفته در سراسر شبکه را در اختیار سازمان‌ها قرار می‌دهد. از آنجا که تهدیدات هر روزه در حال افزایش و به روز شدن هستند، فایروال‌های قدیمی دیگر کاربرد کاملی ندارند و ضعف‌های موجود در آن‌ها باعث می‌شود تا سازمان شما در معرض خطر قرار گیرد.

- **انواع راه حل های امنیتی شبکه، دستگاه ها و ابزارها**

یکی از اساسی ترین عناصر امنیت شبکه، فایروال سخت افزاری نسل جدید یا NGFW [2] می‌باشد. البته برای محافظت واقعی از شبکه به سایر تکنولوژی‌ها نیز نیاز است. در ضمن می‌توان گفت امنیت موثر شبکه، نیاز به رویکردی جامع و کامل دارد که فایروال را با سایر قابلیت های مهم ادغام نماید. ضرورتا به منظور حفاظت سازمانی به صورت کامل و در سطوح مختلف در برابر حملات، به رویکردی لایه ای به همراه راه حل های امنیتی نیاز است که به صورت یک ساختار امنیتی و یکپارچه بتواند از تمام بخش های شبکه محافظت نماید. فایروال های Fortinet همواره در جهت بهبود پاسخ دهی نیاز های مشتریان خود بوده و با نیازهای امنتیی مشتریان خود آشناست.

- **امنیت سازمانی با فایروال فورتی نت**

در صورتی که سیستم سازمانی شما در معرض تهدیدات مختلف قرار دارد و اگر اطلاعات با اهمیتی در سازمان شما وجود دارد، باید بدانید که استفاده از فایروال فورتی‌گیت برای شما بسیار حائز اهمیت خواهد بود. بدون استفاده از آن شما همواره در خطر از دست دادن و از بین رفتن اطلاعات با اهمیت خود خواهید بود که ممکن است آینده کاری شما و افراد دیگر را تحت تأثیر قرار دهد. قیمت فایروال فورتی نت قطعا نسبت به هزینه‌هایی که شما باید در نتیجه از دست رفتن اطلاعات خود پرداخت کنید بسیار ناچیز است و با توجه به مدل فایروال انتخاب شده و امکانات آن تعیین می‌شود.

[1] Virtual Security Processing
[2] Next Generation Firewall

هنگام خرید فایروال، باید به نکات زیر توجه داشته باشید:

- ویژگی‌های امنیتی مانند انواع ماژول‌ها
- امکانات فیلترینگ وب
- امکانات حفاظت از انواع پروتکل‌هایVOIP
- حفاظت از IPS یا IDS
- پشتیبانی درگاه انتقال (Gateway) از آنتی‌ویروس‌های قدرتمند و شناخته‌شده
- جلوگیری از اسپم
- قابلیت کنترل ترافیک برنامه‌های کاربردی
- قابلیت جلوگیری از از دست رفتن داده‌ها (DLP)
- ارتباط امن از راه دور
- برخورداری از سیستم عاملی قدرتمند که امکانات مورد نیاز شما را داشته باشد
- پشتیبانی از انواع روش‌های احراز هویت

- **انواع فایروال فورتی نت**

Web Application Firewalls

عملکرد فایروال اپلیکیشن های تحت وب (Fortiweb) ، در مقایسه با فایروال شبکه، در سطح متفاوت تری است و ترافیک های ورودی در لایه های ۵ تا ۷ مدل Open System Interconnection (OSI) را مورد بررسی قرار می‌دهد. لایه‌ی پنجم یا لایه‌ی session مکانیزمی را برای آغاز، پایان و مدیریتِ session بین فرایندهای اپلیکیشن‌های کاربران ارائه می‌دهد. لایه ششم نیز مسئولیت تحویل و قالب بندی اطلاعات به لایه‌ی اپلیکیشن را بر عهده دارد. و لایه هفتم به کاربران امکان می‌دهد مستقیما با اپلیکیشن‌ها، تعامل داشته باشند.

فایروال فورتی وب، با بررسی و حصول اطمینان از یکپارچگی کلیه‌ی ترافیک های مبتنی بر وب و اپلیکیشن های مربوطه، یک لایه‌ی امنیتی مازاد ایجاد می‌کند. این دسته از فایروال‌ها، مزایای زیادی در اختیار کاربران خود قرار می‌دهند، زیرا به هنگام بررسی ترافیک، فراتر از آدرس شبکه و تعداد پورت‌ها رفته و به این ترتیب، قادر به شناسایی تهدیدات ناشی از پروتکل اپلیکیشن‌ها مانند HTTP و FTP می‌باشند. مضاف بر این از قابلیت ثبت گزارش نیز برخودار بوده که برای تیم امنیت، ارزش بسیاری دارد.

Unified Threat Management Firewall

فایروال های Fortinet Unified Threat Management (UTM) با ادغام چندین ویژگی ارزشمندِ امنیتی در یک داشبورد واحد، رویکردی مدرن در حوزه ی امنیت ارائه داده اند. آن ها قابلیتِ stateful inspection را با عناصر اصلی امنیتی از جملهantivirus ، intrusion prevention systems، anti-spam، virtual private networks و موارد دیگر، یکپارچه می‌سازند. به طور معمول فایروال های UTM به عنوان یک راهکار امنیتی واحد به کار برده می شوند و قابلیت های متعددی را ارائه می دهند. این فایروال ها با بهره گیری از قابلیت امنیتی layering بر روی شبکه های سازمانی، امنیتی کامل و جامع در برابر تهدیدات سایبری را تضمین می کنند. سازمان های بزرگ که دارای شعب مختلف هستند، با انتخاب فایروال های fortinet UTM می‌توانند امنیتِ همه‌ی بخش‌های شبکه و شعب سازمانی را از یک کنسول واحد اداره و تامین کنند. در این صورت فرایند کاری تیم امنیت و مسئولیت‌های اضافه کاهش پیدا می‌کند. به عبارتی با فایروال UTM، تنها یک تیم امنیت برای کل سازمان و حتی شعب مختلف مورد نیاز می باشد.

Network Address Translation Firewalls

فایروال Network Address Translation (NAT)، ترافیک را از طریق یک درگاه واحد (single gateway) به فضای اینترنت هدایت می‌کند. اساسا این فایروال‌ها، ترافیک را مورد بررسی قرار نمی‌دهند. بلکه شبکه‌ی داخلی را از تجهیزات خارجی پنهان نموده و با استفاده از یک IP addressبرای کانکشن‌های خارجی، سایر آدرس‌های آی‌پی را محفوظ نگه داشته و سپس با استفاده از مجموعه‌ی گسترده ای از آدرس‌های داخلی، ترافیک را مدیریت می‌کنند NAT gateway ها غالبا بر روی روترها به کار گرفته می‌شوند اما گاهی هم برای خدمات VPN از آن ها استفاده می‌شود.

Internal Segmentation Firewalls

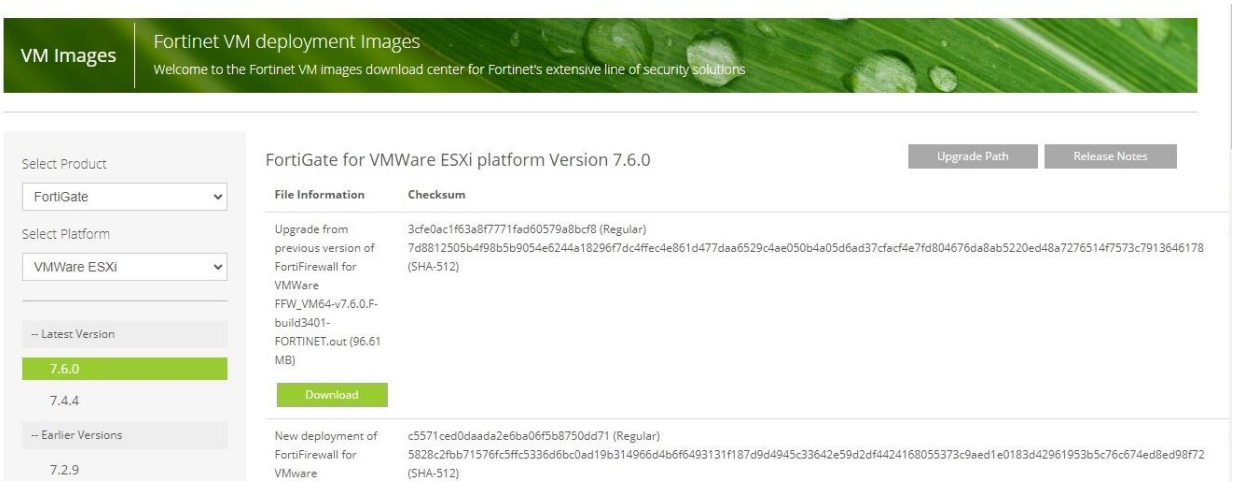
Internal Segmentation یاFortinet ISFW در نقطه ای استراتژیک واقع در شبکه‌ی داخلی، و در کنار سرورهای خاص که حاوی اطلاعات ارزشمند هستند و یا مجموعه ای از تجهیزات یا اپلیکیشن های تحت وب که در فضای کلود هستند، قرار می گیرد. و به این ترتیب نظارت و کنترلی دائمی بر روی ترافیک های ورودی و خروجی به بخش هایی که از پیش تعیین شده به وجود می آید. در ضمن این فایروال‌ها برای ارائه‌ی segmentationو همگام سازی با سایر راهکارها مانند(Network Access Control (NAC طراحی شده اند تا بتوان فرایندهای کاری و تجهیزات جدید را به segment های خاص شبکه و بر اساس معیارهای مختلف اختصاص داد.

Next Generation Firewalls (NGFW)

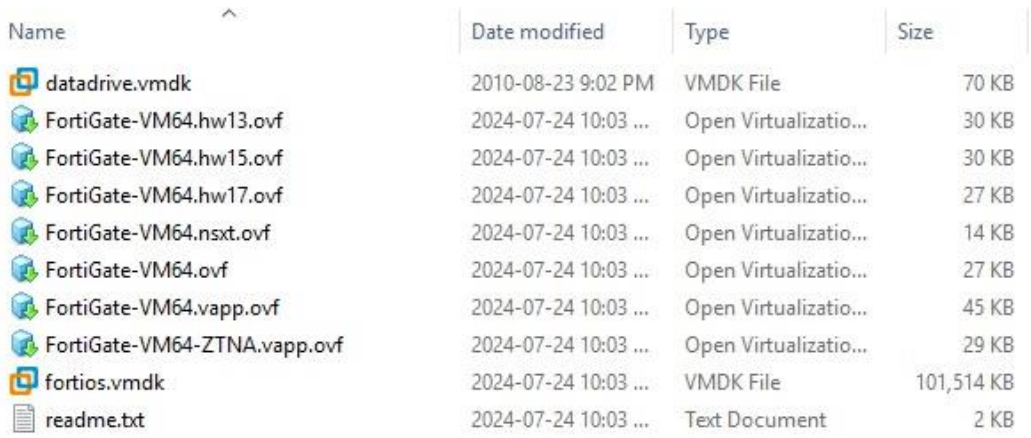
Next Generation (NGFW) از نظر مسدود سازی تهدیدات جدید، شباهت زیادی به فایروال های UTM دارند. آن ها قابلیت‌ها و عملکردهای فایروال های نسل قدیمی تر به عنوان مثال stateful inspection را با تکنیک‌ها و تکنولوژی‌هایی که انواع تهدیدات را مورد بررسی قرار می‌دهند، ادغام می‌سازند. این دسته از فایروال‌ها برای سازمان‌هایی مناسب هستند که در جستجوی امنیتی دقیق و گسترده بوده و تامین امنیت شبکه، برای آنها بسیار حیاتی است. فایروال‌های Fortinet NGFW در تامین امنیت شبکه، فراتر از استانداردهای صنعتی رفته و برای دهمین بار در Magic Quadrantبه عنوان فایروال برتر شبکه، توسط گارتنر شناخته شده است. فایروال‌های نسل جدید فورتی گیت، کلیه‌ی قابلیت‌هایی که در سیر تکامل آن وجود داشته را با هم ادغام نموده و در یک پلتفرم واحد و یکپارچه ارائه داده است. کنسول مدیریت آن، تجربیات مطلوبی را در اختیار کاربران قرار می‌دهد و رویکرد امنیت محور فورتی نت، امنیتی دقیق و گسترده را به تمامی بخش های شبکه اختصاص می‌دهد.

2 Install Fortigate in ESXi

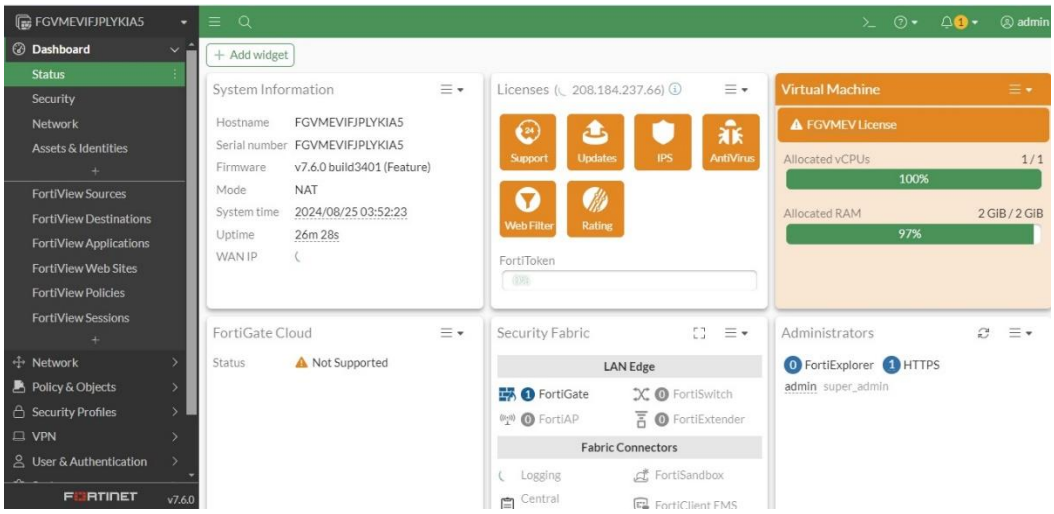
برای اینکه بتوانیم بصورت trial از فورتیگیت استفاده کنیم. باید وارد وب سایت مربوطه شویم و ثبت نام کنیم. سپس ایمیج مورد نیاز را از قسمت Support > VM Image دانلود کنیم. ما اینجا ایمیج مخصوص زیرساخت VM-Ware را دانلود می‌کنیم. در حال حاضر آخرین ورژن آن 7.6.0 می‌باشد.



بعد از دانلود ایمیج مربوطه اگر آن را اکسترکت کنیم. فایل‌هایی شبیه شکل زیر می‌بنیم، که هرکدام از این فایل ها مربوط به یک ورژن خاص از ESXi است. برای اینکه دریابیم کدام یک از فایل‌ها را باید استفاده کنیم. در بخش داکیومنت‌های سایت فورتینت می‌توانیم نکته های آن را ببینیم. در ادامه فایل ovf مربوطه را ایمپورت و سپس ماشین مجازی را روشن می‌کنیم.



بعد از روشن کردن آن، وارد محیط CLI آن می‌شویم و با یوزرنیم admin بدون پسورد وارد می‌شویم و پسورد جدیدی را برای آن در نظر می‌گیریم. و با دستور show system interface یا get system interface physical می‌توانیم آی‌پی ها یا وضعیت اینترفیس‌های تنظیم شده را ببینیم. و به آی‌پی‌های مشخص شده، از طریق وب وصل شویم. با یوزرنیم و پسوردی که در محیط CLI تنظیم کردیم وارد محیط گرافیکی آن می‌شویم.



دستورات ابتدایی در محیط CLI فایروال فورتیگیت:

Get system status

Get system performance status

Get system interface

Get system arp

Get system session list | grep 1.1.1.1

Diagnose sniffer packet any “icmp and host 192.168.10.10”

با دستورات زیر می‌توانیم بصورت CLI روی اینترفیس مورد نظر آی‌پی تنظیم کنیم.

Config system interface

Edit port1

Set mode static

Set ip 192.168.1.1 255.255.255.0

با دستورات زیر می‌توانیم بصورت CLI تظیمات مربوط به DNS را انجام دهیم.

Config system interface

Set primary 8.8.8.8

Set secondary 4.2.2.4

با دستورات زیر می‌توانیم بصورت CLI تظیمات مربوط به Static Route را انجام دهیم.

Config router static

Set status enable

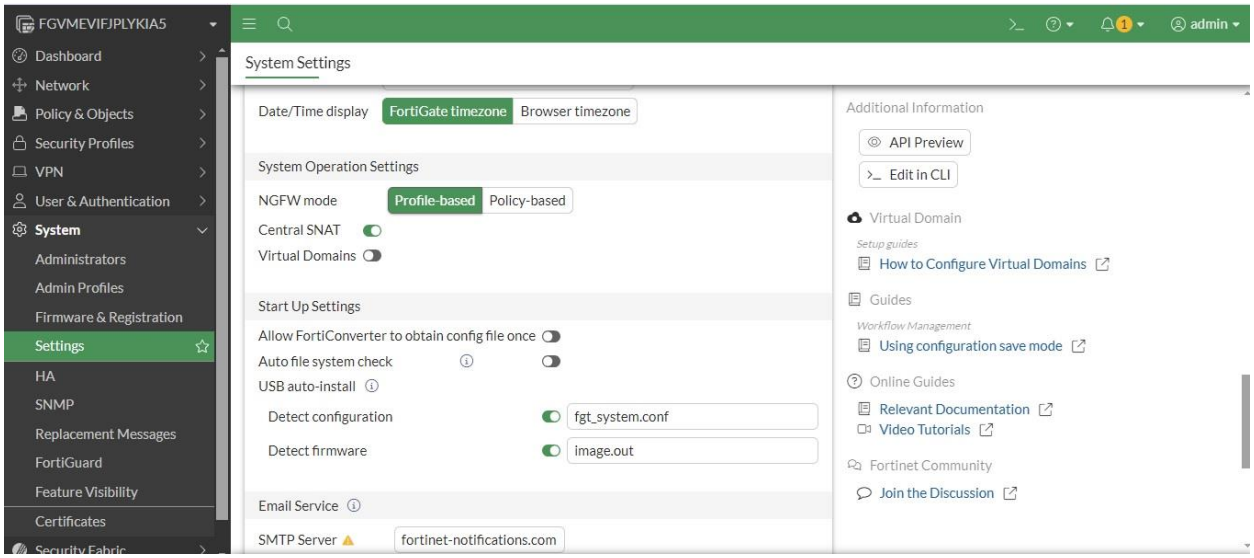
Set gateway 192.168.1.2

Set device port1

3 Firewall Policy (Profile-based vs Policy-based)

نکته مهم اینکه فایروال فورتیگیت بصورت Stateful کار می‌کند، یعنی اگر ترافیکی از داخل به بیرون برود. نیاز به نوشتن پالیسی برگشت و اجازه دادن ترافیک برگشتی نداریم. ترافیک در زمان خروج در جدول Session قرار می‌گیرد سپس برای ورود هم این جدول بررسی می‌شود و اجازه ورود صادر می‌شود. درصورتی که ترافیک از داخل به بیرون رفته باشد اجازه ورود دارد. و یا برعکس. برای ترافیک‌هایی که از بیرون به داخل اجازه ورود دارند هم این قانون صدق می‌کند.

در فایروال فورتیگیت برای ایجاد سطح دسترسی و یا ایجاد محدودیت برای کاربران، پالیسی‌ها را می‌توانیم در دو نوع ایجاد کنیم. این دو نوع بر اساس Profile و Policy هستند. بسیار مهم است که در همان ابتدا مشخص کنیم که فایروال ما بر اساس کدام نوع کار کند. چرا که اگر در ادامه این مورد را تغییر دهیم، تمام پالیسی‌ها و Central NAT های ما حذف خواهند شد. بصورت پیشفرض فایروال روی Profile Based عمل می‌کند. برای تغییر آن وارد مسیر System > Settings > System Operation Settings می‌شویم.

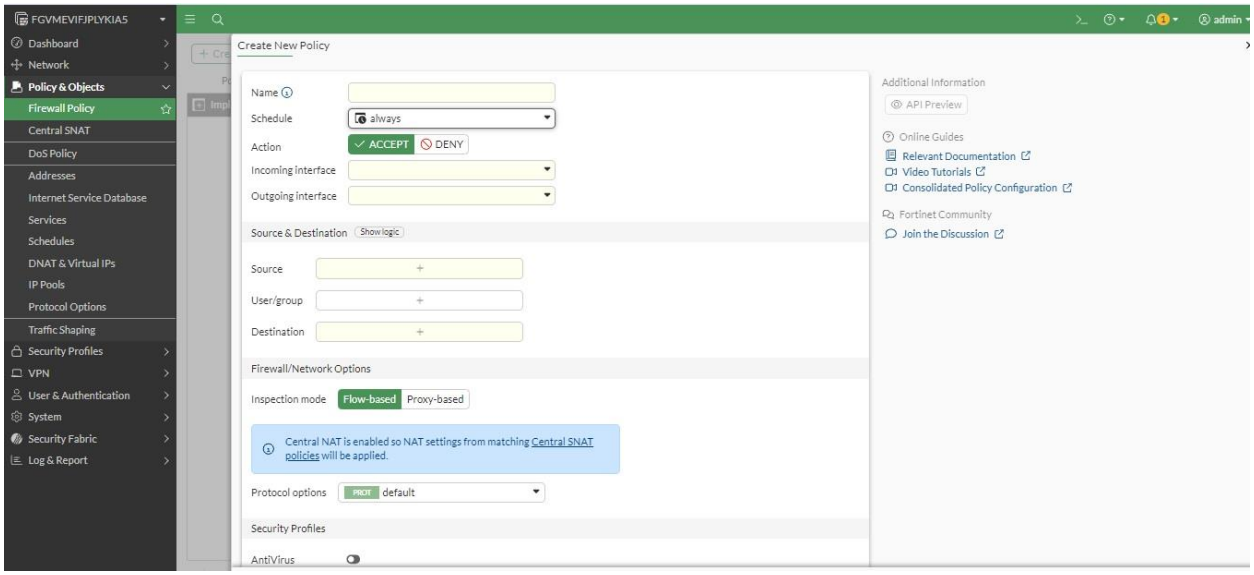


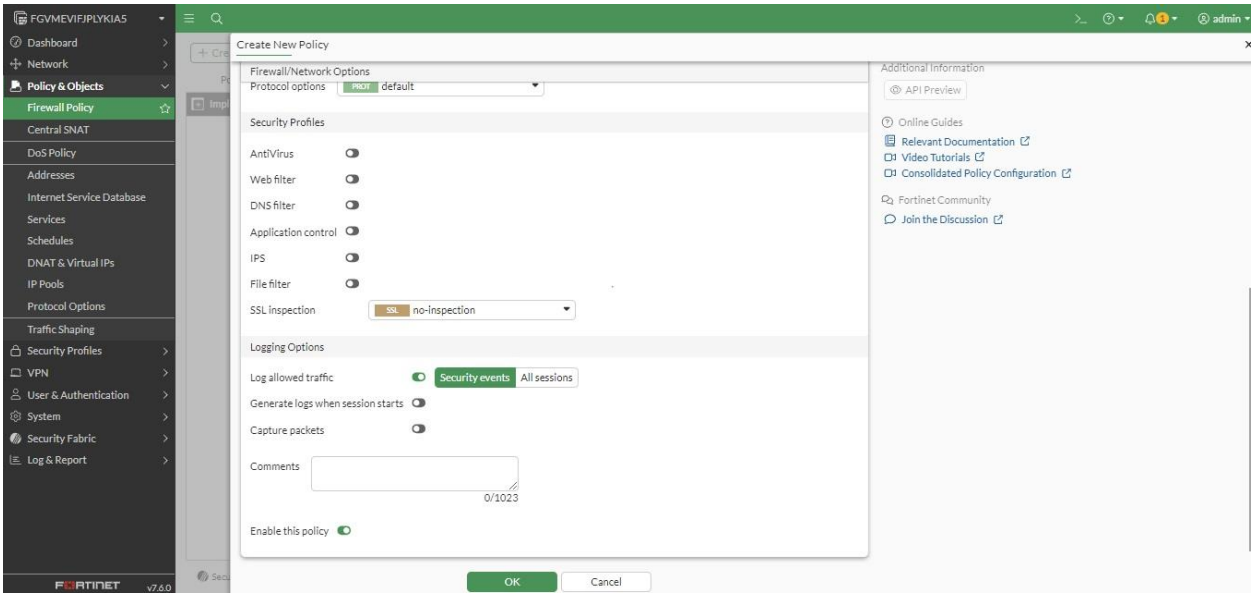
Profile Based: این حالت بدون Central NAT کار می‌کند. یعنی در هر پالیسی باید مکانیزم NAT را اگر بخواهیم، باید برای آن فعال کنیم. البته که میتوانیم Central NAT را برای Policy Based فعال کنیم. Central NAT: محلی که می‌توانیم پالیسی‌های مربوط به NAT را در آن بصورت مرکزی ایجاد و مدیریت کنیم. همچنان قابلیت‌هایی مثل IPS, SSL Inspection, Web Filter و ... را در این حالت بصورت Profile Based داریم. یعنی برای هر کدام از این قابلیت‌ها یک پروفایل مخصوص ایجاد می‌کنیم و در پالیسی خود آن را اعمال می‌کنیم.

Policy Based: این حالت فقط با Central NAT کار می‌کند. در این حالت URL Category و Application Filter به عنوان یکی از گزینه‌های پالیسی هستند و بقیه موارد بصورت Profile Based هستند. در این حالت SSL Inspection and Authentication بصورت یک منوی جدا در زیرشاخه Policy and Objects اضافه می‌شود. این نوع جدیدا اضافه شده است. و فایروال‌های قدیمی بر اساس Profile کار می‌کند.

نکته مهم: پالیسی‌ها به ترتیب اجرا می‌شوند، پس اولویت آن‌ها و ترتیب آن‌ها بسیار مهم است.

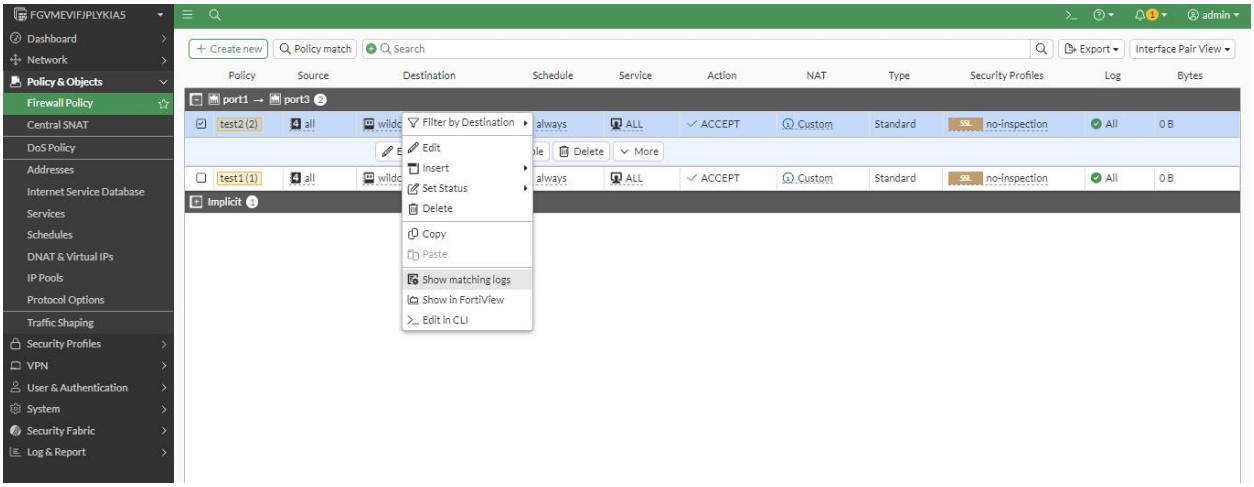
برای ایجاد پالیسی وارد مسیر Policy & Object > Firewall Policy > Create New می‌شویم. و مواردی همچون: مدت زمان فعال بودن این پالیسی، مبدا، مقصد، اینترفیس ورودی و اینترفیس خروجی، فعال یا غیر فعال بودن این پالیسی، Log گرفتن از این پالیسی و فعال کردن انواع Security Profile ها و ... را تنظیم کنیم.



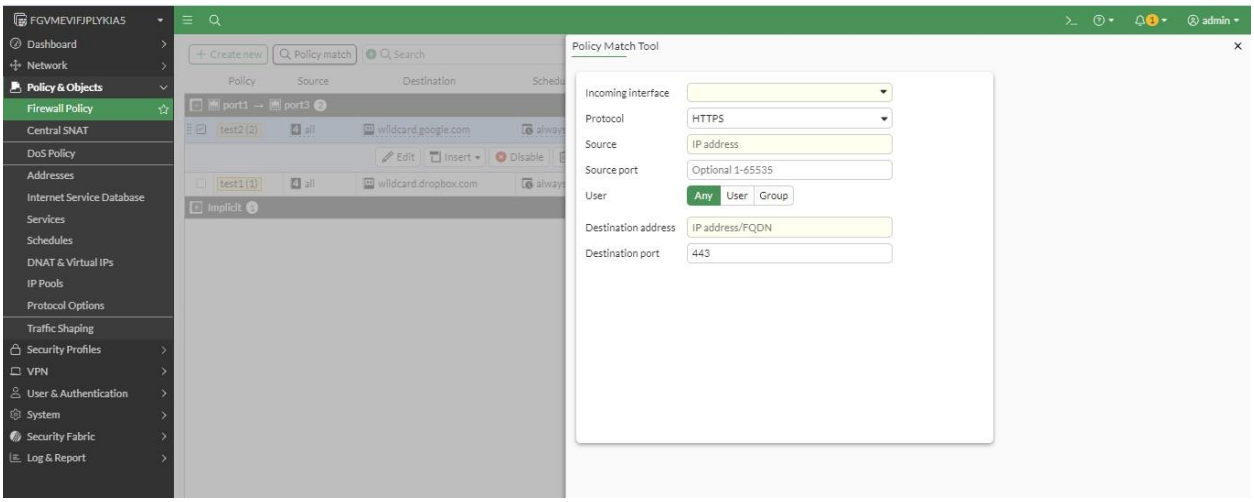


توضیحات بیشتر: در قسمت Source و Destination می‌توانیم به سه طریق، ترافیکی که می‌خواهیم روی آن کنترل داشته باشیم را مشخص کنیم. بر اساس User, IP Address, Internet Service.

نکته مهم: اگر روی پالیسی مورد نظر رایت کلیک کنیم و Show Matching Log را بزنیم. ترافیک‌هایی که با این پالیسی مطابق شده اند را نمایش می‌دهد. دقت کنید که Log ها را کمی با تاخیر نمایش می‌دهد.

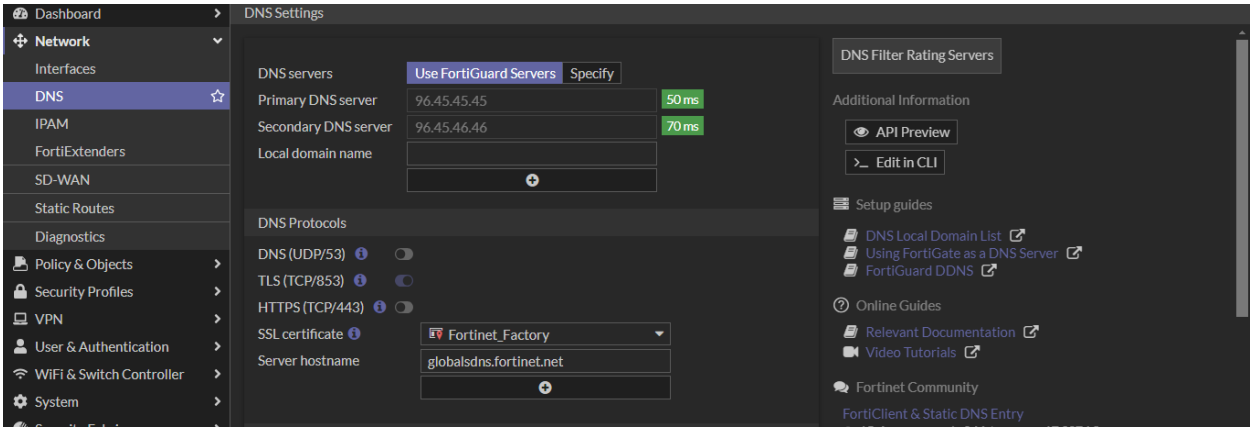


با استفاده از گزینه Policy Match در صفحه Firewall Policy می‌توانیم دریابیم که چه ترافیکی با چه پالیسی مطابق می‌شود.

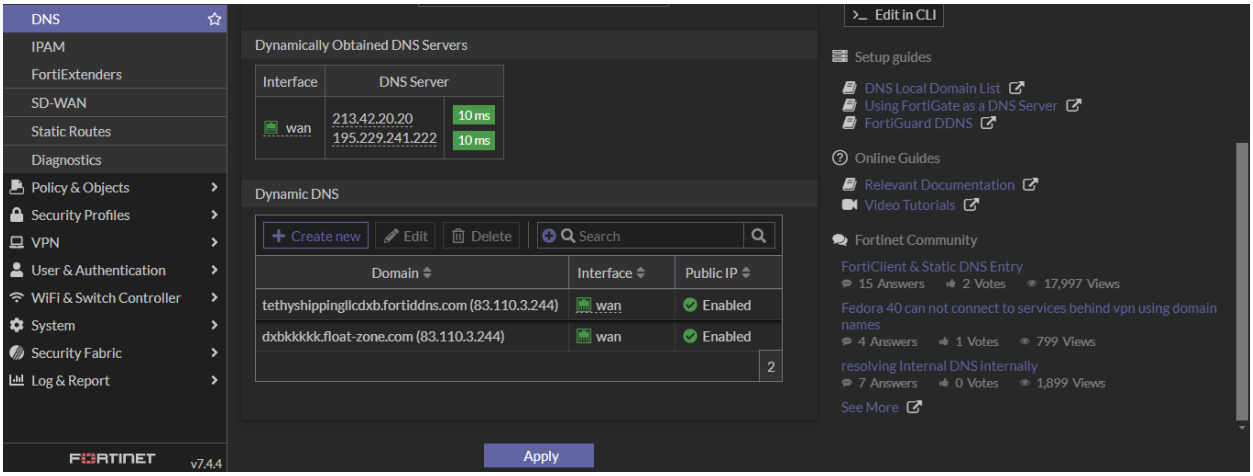


4 Fortigate (DNS, DDNS, DHCP)

یکی از موارد بسیار مهم برای تنظیم در فایروال تنظیم DNS است. که وظیفه تبدیل اسم به آی‌پی و بالعکس را دارد. برای تنظیم این بخش وارد منوی Network > DNS می‌شویم. و در ادامه Public DNS Server هایی که مد نظر است را تعیین می‌کنیم.



در بخش انتهایی می‌توانید از قابلیتی بنام DDNS استفاده کنید. DDNS کاربردهای زیادی دارد. مثلا اگر شما Public IP ندارید. می‌توانید یک نام DDNS انتخاب کنید که Unique باشد. و بصورت اتوماتیک اگر آی‌پی ما تغییر کند. این سرویس متوجه می‌شود و آن را جایگزین می‌کند. و ما می‌توانیم به واسطه این نام به فایروال خود از راه دور متصل شویم.



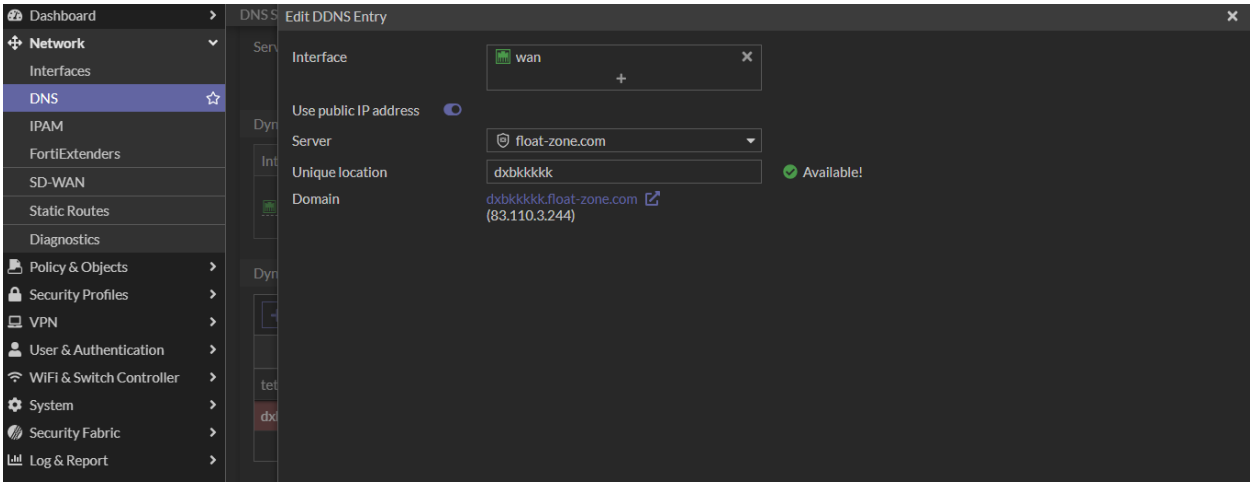
برای تنظیم آن گزینه Create New را می‌زنیم. اینترفیس WAN خود را انتخاب می‌کنیم. یکی از سرورهای شرکت فورتیگیت را انتخاب می‌کنیم. سرورهایی که سرور DDNS را ارائه می‌دهند.

float-zone.com

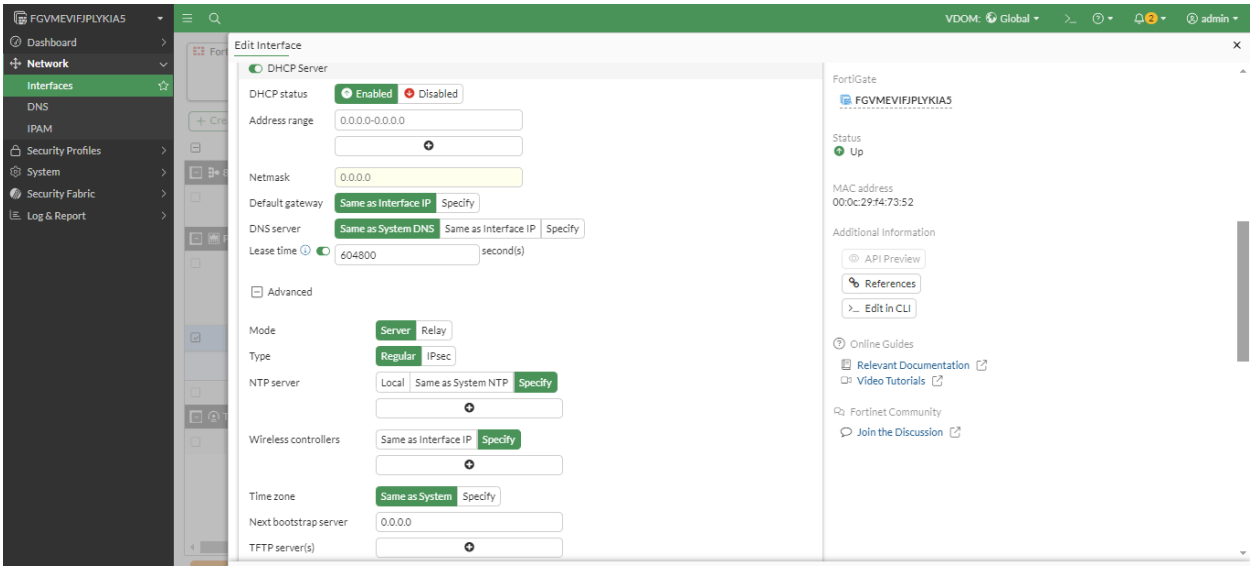
fortidyndns.com

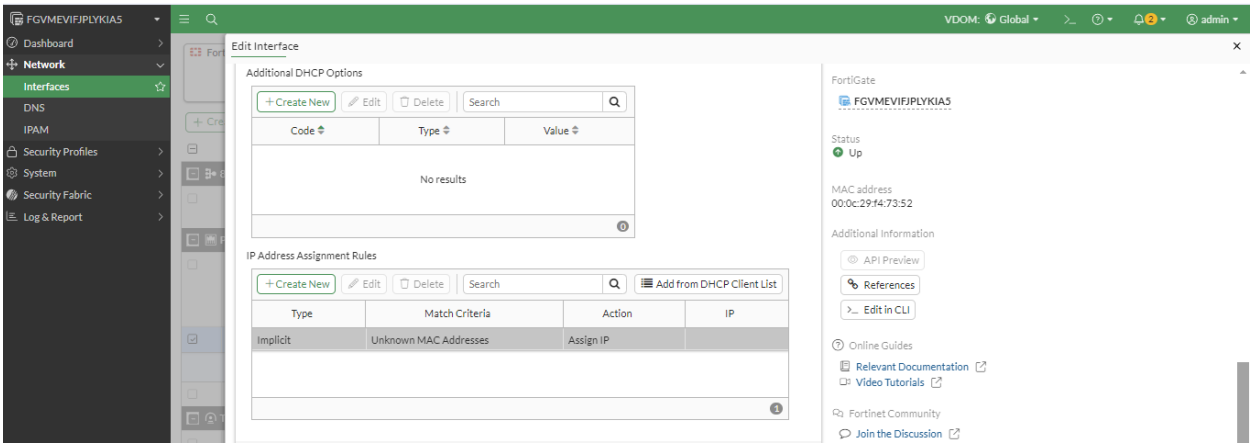
fortiddns.com

و در نهایت یک اسم Unique را وارد می‌کنیم. تا توسط این اسم به واسطه سرویس DDNS به فایروال خود متصل شویم.



برای تنظیم سرویس DHCP روی فایروال فورتیگیت وارد منوی Network > Interface می‌شویم. و گزینه DHCP را فعال می‌کنیم و تنظیمات آن را انجام می‌دهیم. تنظیمات DHCP دو بخش دارد. و ادامه تنظیمات آن در قسمت Advanced است. تنظیماتی همچون DHCP Relay Agent, TFTP, NTP, Additional DHCP, DHCP Binding را هم می‌توانیم انجام دهیم.





5 Firewall NAT

توصیه می‌شود در طراحی شبکه، سرویس NAT روی فایروال پیاده سازی شود تا روی روتر. به این دلیل که NAT با برخی از سرویس‌ها مثل VPN, FTP, Voice, Video به مشکل بر می‌خورد. چرا که این ترافیک ها نیاز به یک ارتباط پایدار و با تاخیر کم دارند. و در صورت تاخیر، این نوع ترافیک‌ها دچار مشکل می‌شوند. البته که، فایروال فورتیگیت ترافیک تا لایه اپلیکیشن را می‌فهمد و می‌تواند آن را ببیند، لذا می‌تواند با قابلیت NAT Traversal به ما به حل این مشکل کمک کند. این قابلیت در روترهای میکروتیک هم وجود دارند. بصورت کلی NAT به سه صورت زیر است:

:Static NAT

در این روش NAT به صورت یک به یک انجام می شود. اگر شما ۱۰۰ کاربر داخلی و ۱۰۰ ادرس global داشته باشید. می توانید از این روش استفاده کنید و برای هر یوزر مشخص کنید از چه آدرس global می تواند استفاده کند. به صورت معمول ما به اندازه کافی آدرس global برای هر کاربر نداریم. استفاده معمول از روش static NAT برای یک سرور در شبکه داخلی یا محیط DMZ است و می خواهیم به کاربران سطح اینترنت دسترسی به این سرور را بدهیم و با استفاده از static NAT می توانیم این دسترسی را فراهم کنیم.

:Dynamic NAT

در این حالت ما یک رنج از آدرس های global داریم و تنها این رنج آدرس ها را به شبکه داخلی اختصاص می دهیم تا زمانیکه هر دستگاه نیاز به استفاده از اینترنت را داشت از آنها استفاده کند. به طور مثال ، یک کاربر می خواهد از اینترنت استفاده کند با شروع به کار او یک آدرس global از این رنج به او اختصاص داده می شود و این کاربر با استفاده از این آدرس global ارتباطش با اینترنت برقرار می شود بعد از یک بازه زمانی کاربر کارش با اینترنت به اتمام می رسد و دیگر نیاز به استفاده از اینترنت را ندارد. در این دستگاهی مثل روتر که عمل NAT را انجام می دهد بعد از یک بازه زمانی مشخص در صورت عدم استفاده آدرس global این آدرس را آزاد خواهد کرد که سایر دستگاه ها بتوانند از آن استفاده کنند. تعداد آدرس های global با تعداد دستگاه های شبکه داخلی که می خواهند از اینترنت استفاده کنند باید برابر باشد.

PAT: Port Address Translation

این روش برای بیشتر کاربرانی که به اینترنت متصل می شوند استفاده می شود. در این روش از مزیت Dynamic NAT که تنها به کاربرانی که نیاز به استفاده از اینترنت دارند آدرس Global اختصاص داده می شود استفاده می کند و در کنار آن با استفاده از شماره پورت های مورد استفاده در ارتباط ، امکان استفاده جندین کاربر را از یک آدرس Global فراهم می کند. در این روش دستگاهی که عمل PAT را انجام می دهد اطلاعات پورت و IP ها را ردیابی می کند و براساس آنها جدول NAT را تشکیل می دهد.

وظیفه NAT ترجمه آی‌پی های Private به آی‌پی های Public و برعکس است. از اصلی ترین انواع NAT بصورت زیر هستند:

Source NAT (Post Routing NAT)

- One to one
- Many to one

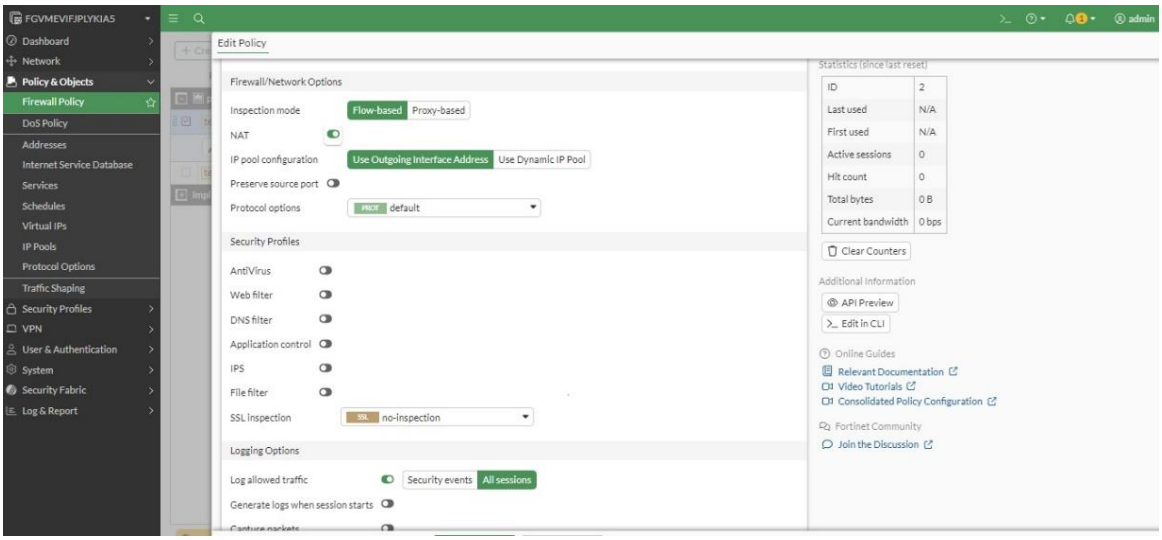
Destination NAT (Pre-Routing NAT)

- One to one
- Many to one

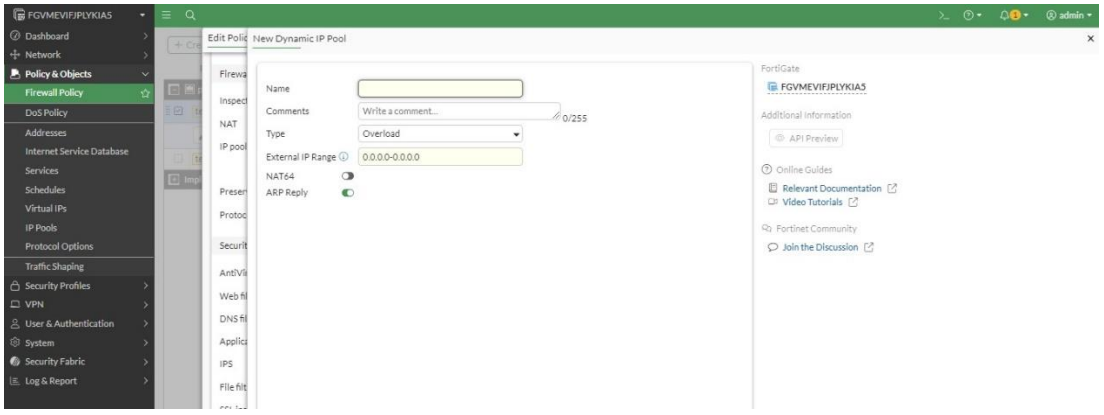
5.1 Firewall Source NAT

در حالت Source NAT مرسوم این است که سیستم‌های داخل شبکه، می‌خواهند به شبکه اینترنت دسترسی داشته باشند. در این حالت ما از این نوع NAT استفاده می‌کنیم.

در فایروال فورتیگیت NAT می‌تواند به ازای هر پالیسی اجرا شود و هم می‌تواند بصورت Central NAT ایجاد شود. برای اینکه NAT را به ازای هر پالیسی تنظیم کنیم. وارد منوی پالیسی‌ها می‌شویم، یکی از پالیسی‌ها را در حالت Edit قرار می‌دهیم و در قسمت NAT موارد را تنظیم می‌کنیم. مثلا می‌توانید برای NAT هم، از آی‌پی پورت خروجی یا WAN استفاده کنیم و هم از یک رنج IP Pool که بصورت Public هستند استفاده کنیم.



همچنان می‌توانید عمل NAT را به یک IP Pool بدهید. تصویر زیر تنظیمات ایجاد IP Pool را به ما نشان می‌دهد. گزینه Overload همان PAT یا Port Address Translation است. در روترهای سیسکو هم از همین واژه استفاده می‌شود.

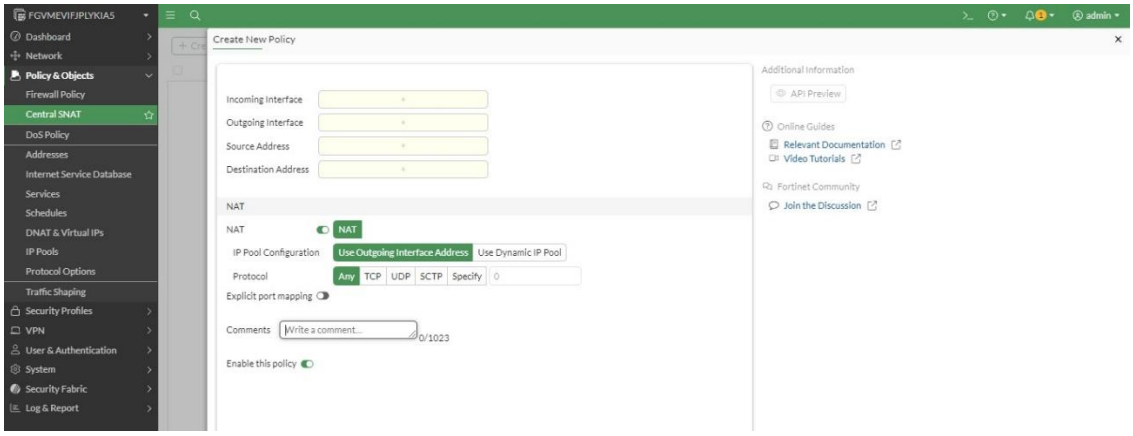


می‌توانید بصورت CLI هم گزارش هایی در مورد NAT ببینید.

Get system session list

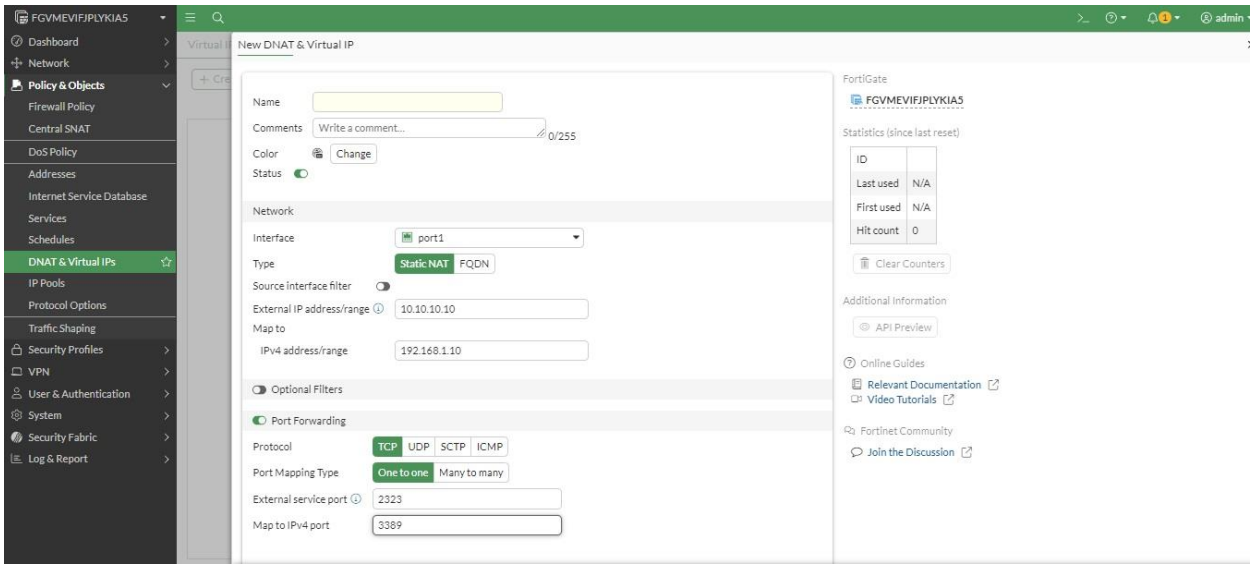
```
port1   dhcp   0.0.0.0 0.0.0.0  192.168.11.128 255.255.255.0  up   disable   phy
sical
port2   static   0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up   disable   physical
port3   static   0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up   disable   physical
ssl.root   static   0.0.0.0 0.0.0.0  0.0.0.0 0.0.0.0  up   disable   tunnel

FGVMEVIFJPLYKIA5 # sh system interface Timeout

FGVMEVIFJPLYKIA5 login: admin
Password:
Welcome!

FGVMEVIFJPLYKIA5 # get system session

FGVMEVIFJPLYKIA5 # get system session list
PROTO   EXPIRE SOURCE          SOURCE-NAT      DESTINATION      DESTINATION-NA
T
tcp     3595   192.168.11.1:24889 -              192.168.11.128:443 -

udp     172    192.168.11.128:1825 -              192.168.11.1:53  -

tcp     3556   192.168.11.1:24848 -              192.168.11.128:443 -


FGVMEVIFJPLYKIA5 # _
```

برای ایجاد Central NAT بصورت زیر عمل می‌کنیم. ابتدا از قسمت Setting باید Central NAT را فعال کنیم. سپس وارد منوی NAT می‌شویم و Create New و در نهایت تنظیمات مورد نظر را همچون تصویر زیر تکمیل می‌کنیم.

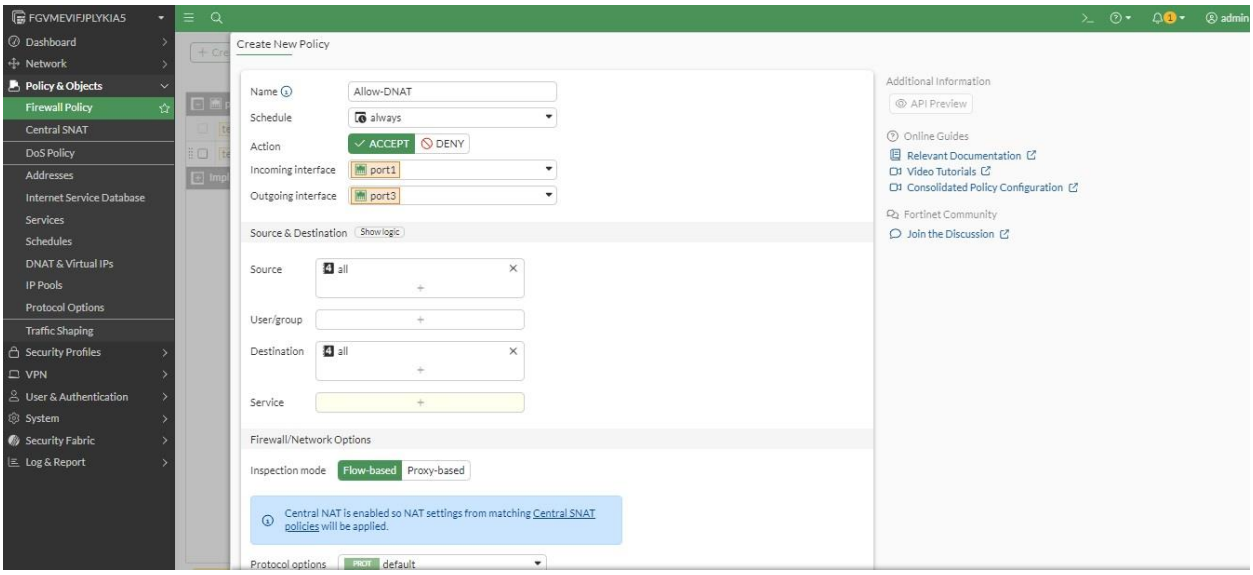


5.2 Firewall Destination NAT

در حالت Destination NAT می‌توانیم از بیرون به سرورهای داخلی خود که رنج آی‌پی Private دارند، دسترسی داشته باشیم. بطور مثال، یک آی‌پی پابلیک داریم. حتی با در این حالت هم، روی پورت‌های مختلف، می‌توانیم به سرویس‌ها و سرورهای مختلف از بیرون به داخل شبکه دسترسی داشته باشیم. برای تنظیم این بخش وارد منوی DNAT & Virtual IP می‌شویم. در قسمت Interface درواقع اینترفیس WAN خود را انتخاب می‌کنیم. در قسمت External IP در واقع آی‌پی پابلیک WAN خود را وارد می‌کنیم. و در قسمت MAP to IPv4 Address در واقع آی‌پی سروری که از بیرون می‌خواهیم به آن متصل شویم را وارد می‌کنیم. در قسمت External Service Port همان پورت مورد نظری که از بیرون می‌خواهیم وارد کنیم را مشخص می‌کنیم. و در قسمت Map to IPv4 Port همان پورت سرویسی که روی سرور می‌خواهیم به آن متصل شویم را وارد می‌کنیم.



در نهایت در قسمت Firewall Policy یک پالیسی ایجاد می‌کنیم و ترافیک بیرون به داخل را روی سرویس، مبدا و مقصد مورد نظر Allow در نظر می‌گیریم.



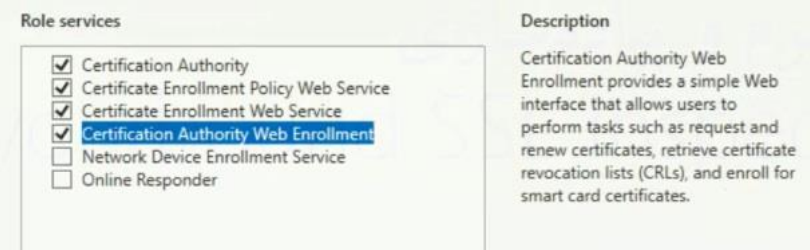
6 SSL Inspection

امروزه اکثر ترافیک هایی ما که در شبکه ما جا به جا می‌شوند، رمز شده هستند. و اگر ما بخواهیم این ترافیک ها را زیر نظر داشته باشیم. باید از قابلیت SSL Inspection فایروال استفاده کنیم تا پکت های رمز شده را باز کنیم و دیتای داخل آن را بررسی کنیم. مثل ترافیک های وب، اپلیکیشن، آنتی ویروس یا IPS. ترافیک های رمز شده در شبکه به دو صورت Inbound و Outbound هستند. یعنی ترافیک هایی که از شبکه خارج می‌شوند و ترافیک هایی که وارد شبکه می‌شوند.

در این بحث، مواردی همچون Certificate Authority, Private Key, Public Key را خواهیم داشت. SSL Inspection به این صورت عمل می‌کند که فایروال از یک CA داخلی یا خارجی که Trusted کاربران هستند، سرتیفیکیت دریافت می‌کند. و هرترافیکی که از شبکه خارج و یا وارد می‌شود را با سرتیفیکیت خود امضا و موارد رمزنگاری را با کلیدهای Public و Private خود انجام می‌دهد. تمام ترافیک های رمز شده ابتدا به فایروال داده می‌شود و فایورال ترافیک را از طرف خود به مقصد مورد نظر می‌رساند. به این صورت فایروال به تمام اطلاعات رمز شده هم دسترسی خواهد داشت. البته که این کار به علت پردازش های زیاد باعث کندی فایروال هم خواهد شد. اصطلاحا در این حالت فایروال بصورت Proxy عمل می‌کند.

6.1 Outbound SSL Inspection

پیاده سازی Outbound SSL Inspection به این صورت است که، ابتدا به یک سرور CA و یک سرور DC نیاز داریم که باید آن را آماده کنیم. سپس قابلیت Certificate Authority با چهار Feature زیر را روی سرور نصب می‌کنیم.



۱. سرتیفیکیت CA را از طریق گروپ پالیسی روی تمام سیستم ها باید نصب و در حالت Trusted قرار دهیم.

۲. یک درخواست سرتیفیکیت در فایروال فورتیگیت خود ایجاد می‌کنیم. وارد مسیر Certificate ها میشویم و گزینه Generate CSR را انتخاب می‌کنیم و موارد خواسته شده را به راحتی تنظیم می‌کنم.

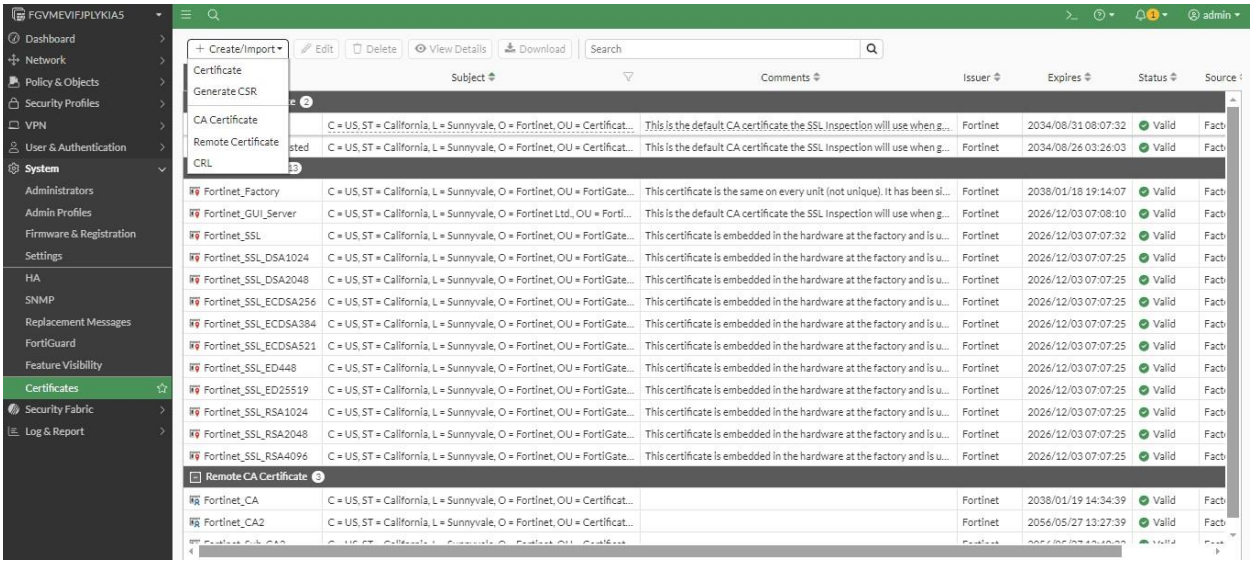
۳. سرتیفیکیت ایجاد شده را دانلود میکنیم و محتویات درون آن را کپی می‌کنیم و در قسمت درخواست های CA وارد می‌کنیم.

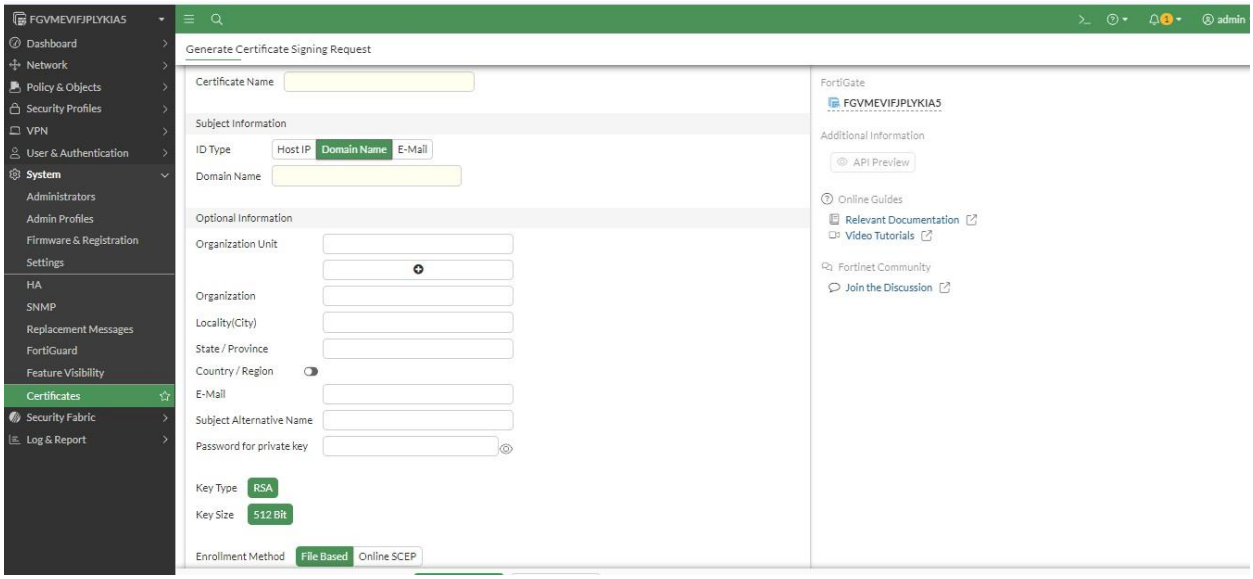
۴. در هنگام وارد کردن Certificate Template را حتما باید Subordinate Certification Authority را باید انتخاب کنیم.

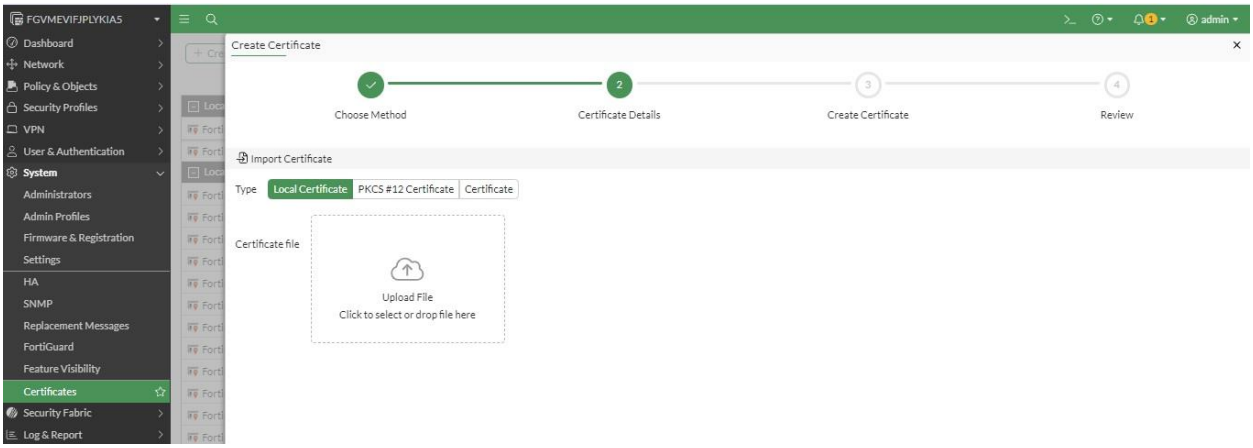
۵. بعد از اینکه از CA سرتیفیکت خود را دریافت کردیم وارد فایروال می‌شویم و در قسمت Certificate گزینه Import Certificate را وارد می‌کنیم و سرتیفیکیتی که از CA گرفتیم را به آن میدهیم. سپس سرتیفیکیت ایجاد شده در فایروال را هم دانلود می‌کنیم و از طریق گروپ پالیسی برای یوزرها Trusted می‌کنیم.

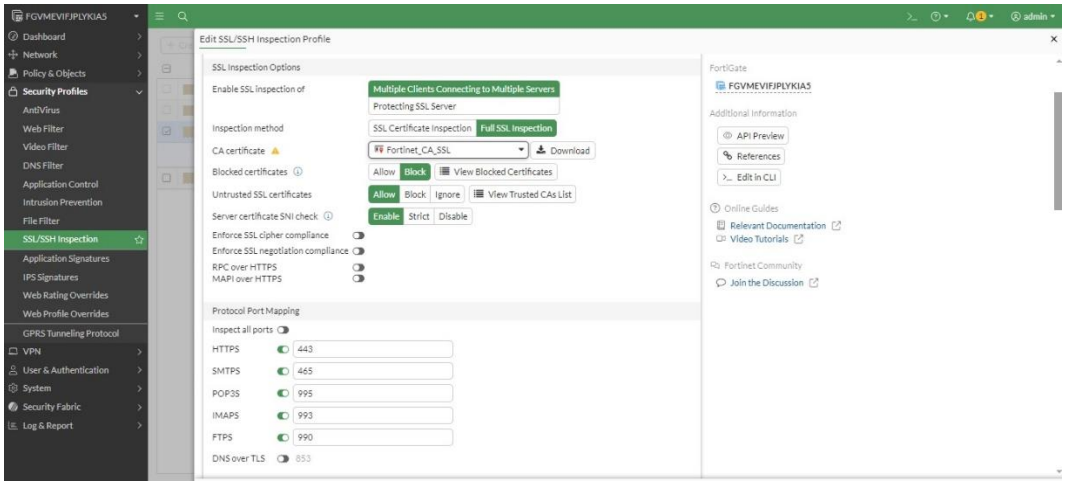
۶. وارد قسمت Security Profile > SSL SSH Inspection > Custom Deep Inspection می‌شویم. و یک Security Profile ایجاد میکنیم تا بتوانیم از آن در قسمت Firewall Policy ها از آن استفاده کنیم. آن را Edit می‌کنیم و تنظیمات خود را اعمال می‌کنیم.

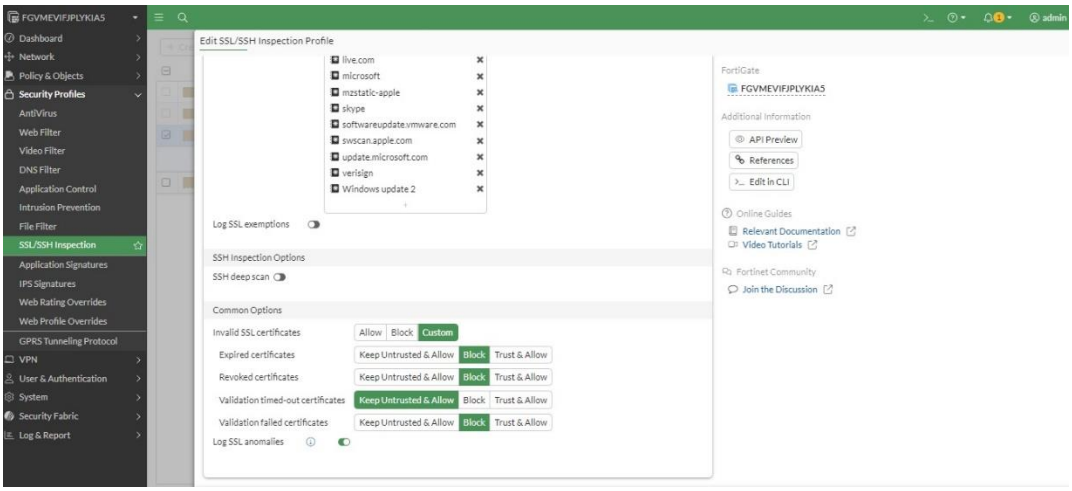
۷. در نهایت در Firewall Policy یکی از پالیسی های خود را انتخاب می‌کنیم و Inspection Mode را در حالت Proxy قرار می‌دهیم. SSL Inspection را همان سرتیفیکیتی که ایجاد کردیم را انتخاب می‌کنیم.

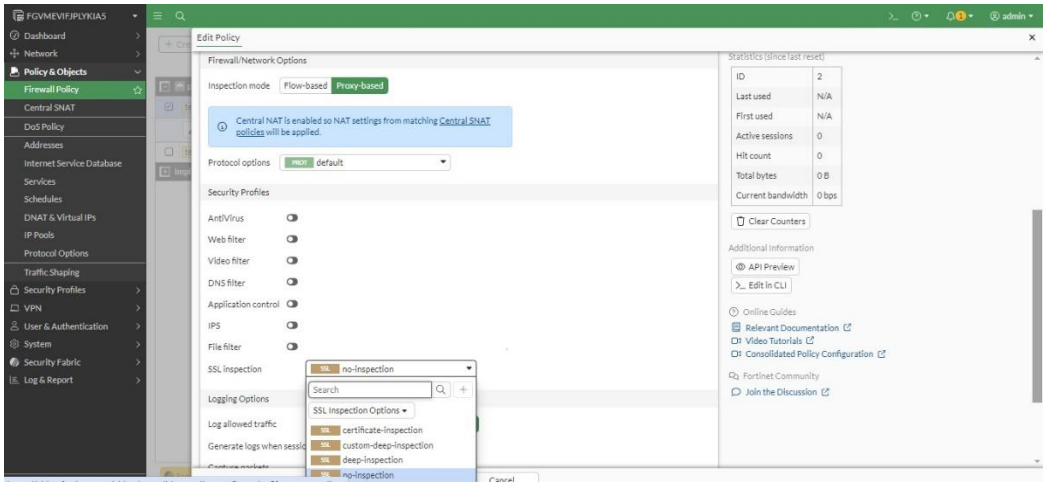

FGVMEVIFJPLYKIA5
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
System
Administrators
Admin Profiles
Firmware & Registration
Settings
HA
SNMP
Replacement Messages
FortiGuard
Feature Visibility
Certificates
Security Fabric
Log & Report
admin
Create/Import
Certificate
Generate CSR
CA Certificate
Remote Certificate
CRL
Edit
Delete
View Details
Download
Search
Subject
Comments
Issuer
Expires
Status
Source
Fortinet_Factory
Fortinet_GUI_Server
Fortinet_SSL
Fortinet_SSL_DSA1024
Fortinet_SSL_DSA2048
Fortinet_SSL_ECDSA256
Fortinet_SSL_ECDSA384
Fortinet_SSL_ECDSA521
Fortinet_SSL_ED448
Fortinet_SSL_ED25519
Fortinet_SSL_RSA1024
Fortinet_SSL_RSA2048
Fortinet_SSL_RSA4096
Remote CA Certificate
Fortinet_CA
Fortinet_CA2


FGVMEVIFJPLYKIA5
Generate Certificate Signing Request
Certificate Name
Subject Information
ID Type
Host IP
Domain Name
E-Mail
Domain Name
Optional Information
Organization Unit
Organization
Locality(City)
State / Province
Country / Region
E-Mail
Subject Alternative Name
Password for private key
Key Type
RSA
Key Size
512 Bit
Enrollment Method
File Based
Online SCEP
FortiGate
FGVMEVIFJPLYKIA5
Additional Information
API Preview
Online Guides
Relevant Documentation
Video Tutorials
Fortinet Community
Join the Discussion


FGVMEVIFJPLYKIA5
Create Certificate
Choose Method
Certificate Details
Create Certificate
Review
Import Certificate
Type
Local Certificate
PKCS #12 Certificate
Certificate
Certificate file
Upload File
Click to select or drop file here


FGVMEVIFJPLYKIA5
Dashboard
Network
Policy & Objects
Security Profiles
AntiVirus
Web Filter
Video Filter
DNS Filter
Application Control
Intrusion Prevention
File Filter
SSL/SSH Inspection
Application Signatures
IPS Signatures
Web Rating Overrides
Web Profile Overrides
GPRS Tunneling Protocol
VPN
User & Authentication
System
Security Fabric
Log & Report
Edit SSL/SSH Inspection Profile
SSL Inspection Options
Enable SSL inspection of
Multiple Clients Connecting to Multiple Servers
Protecting SSL Server
Inspection method
SSL Certificate Inspection
Full SSL Inspection
CA certificate
Fortinet_CA_SSL
Download
Blocked certificates
Allow
Block
View Blocked Certificates
Untrusted SSL certificates
Allow
Block
Ignore
View Trusted CAs List
Server certificate SNI check
Enable
Strict
Disable
Enforce SSL cipher compliance
Enforce SSL negotiation compliance
RPC over HTTPS
MAPI over HTTPS
Protocol Port Mapping
Inspect all ports
HTTPS
443
SMTPS
465
POP3S
995
IMAPS
993
FTPS
990
DNS over TLS
853
FortiGate
FGVMEVIFJPLYKIA5
Additional Information
API Preview
References
Edit in CLI
Online Guides
Relevant Documentation
Video Tutorials
Fortinet Community
Join the Discussion
admin

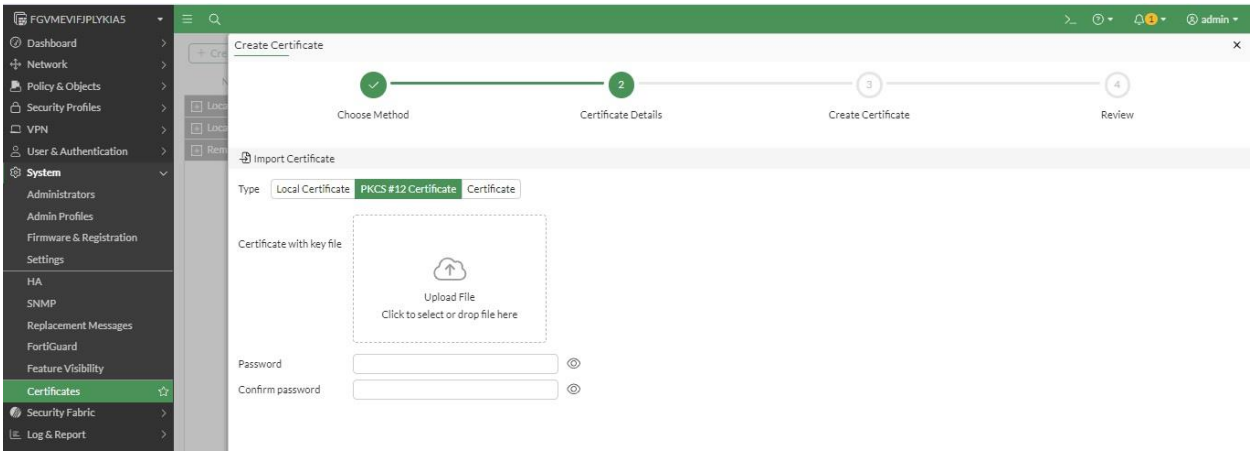

FGVMEVIFJPLYKIA5
Edit SSL/SSH Inspection Profile
live.com
microsoft
mzstatic-apple
skype
softwareupdate.vmware.com
swscan.apple.com
update.microsoft.com
verisign
Windows update 2
Log SSL exemptions
SSH Inspection Options
SSH deep scan
Common Options
Invalid SSL certificates
Allow
Block
Custom
Expired certificates
Revoked certificates
Validation timed-out certificates
Validation failed certificates
Keep Untrusted & Allow
Block
Trust & Allow
Log SSL anomalies
FortiGate
FGVMEVIFJPLYKIA5
Additional Information
API Preview
References
Edit in CLI
Online Guides
Relevant Documentation
Video Tutorials
Fortinet Community
Join the Discussion
admin


FGVMEVIFJPLYKIA5
Edit Policy
Firewall/Network Options
Inspection mode
Flow-based
Proxy-based
Central NAT is enabled so NAT settings from matching Central SNAT policies will be applied.
Protocol options
PROT
default
Security Profiles
AntiVirus
Web filter
Video filter
DNS filter
Application control
IPS
File filter
SSL Inspection
no-inspection
Search
SSL Inspection Options
certificate-inspection
custom-deep-inspection
deep-inspection
no-inspection
Logging Options
Log allowed traffic
Statistics (since last reset)
ID
2
Last used
N/A
First used
N/A
Active sessions
0
Hit count
0
Total bytes
0 B
Current bandwidth
0 bps
Clear Counters
Additional Information
API Preview
Edit in CLI
Online Guides
Relevant Documentation
Video Tutorials
Consolidated Policy Configuration
Fortinet Community
Join the Discussion
admin

6.2 Inbound SSL Inspection

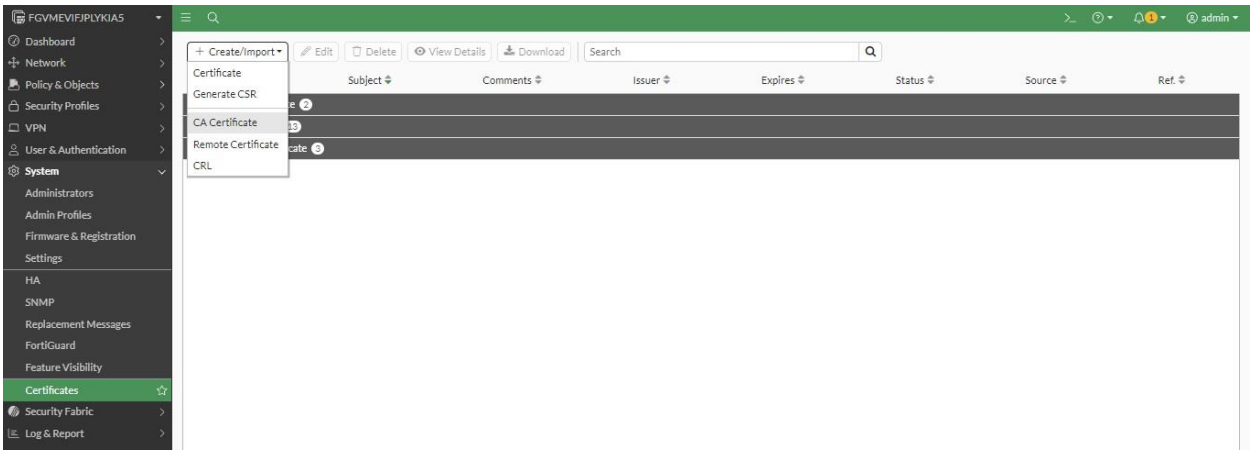
ترافیک های بیرونی که وارد شبکه می‌شوند و به سرورهای ما متصل می‌شوند، ممکن که بصورت رمزشده باشند. با این قابلیت ترافیک های رمز شده را می‌توانیم از این طریق ببینیم و پکت ها را باز کنیم. در غیر این صورت نمی‌توانیم درون پکت ها را ببینیم و آن‌ها ارزیابی کنیم. مراحل کار بصورت زیر است:

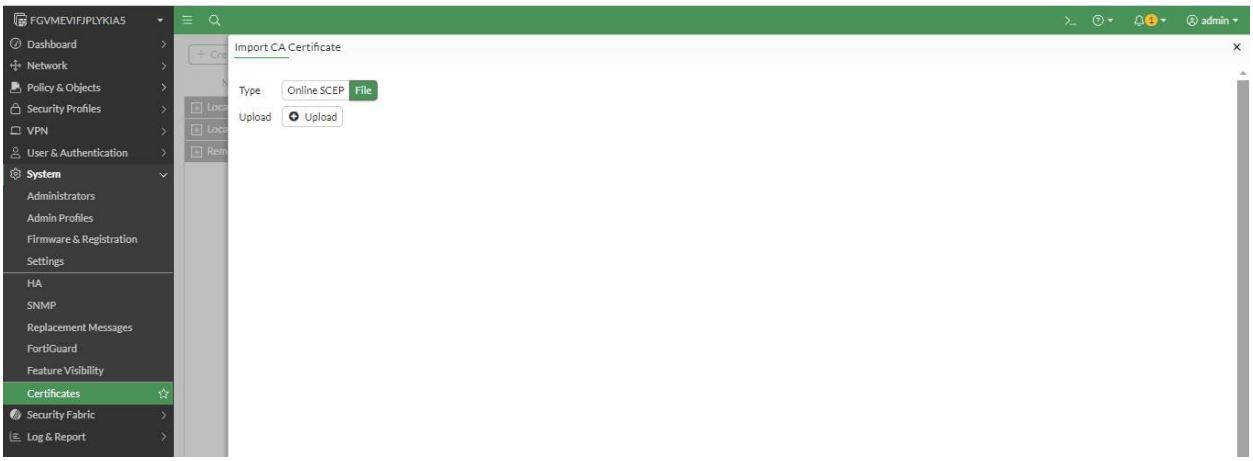
۱. سرتیفیکیت و کلید خصوصی سروری که از بیرون، کاربران به آن متصل می‌شوند را روی فایروال آپلود می‌کنیم. در این حالت تمام ترافیکی که از بیرون وارد می‌شود را فایروال می‌تواند Decrypt کند. چون فایروال کلید خصوصی سرور را دارد. دقت کنید که در هنگام اکسپورت کردن سرتیفیکیت سرور، حتما باید تیک گزینه Private Key را بزنیم تا کلید خصوصی را برای ما اکسپورت بگیرد. در ادامه در فایروال وارد قسمت Import Certificate می‌شویم و سرتیفیکیت از نوع PKCS را ایمپورت می‌کنیم.



۲. روی فایروال یک پالیسی می‌نویسیم که ترافیک از بیرون به داخل، به سرور مورد نظر ما برقرار شود. این کار با Virtual IP و Port Mapping انجام می‌شود.

۳. بهتر است سرتیفیکیت سرور CA را هم برای فایروال و همه کاربران Trusted در نظر بگیریم. برای این کار در فایروال وارد بخش Certificate ها می‌شویم و در قسمت CA Certificate، سرتیفیکیت مربوط به CA خود را آپلود می‌کنیم.

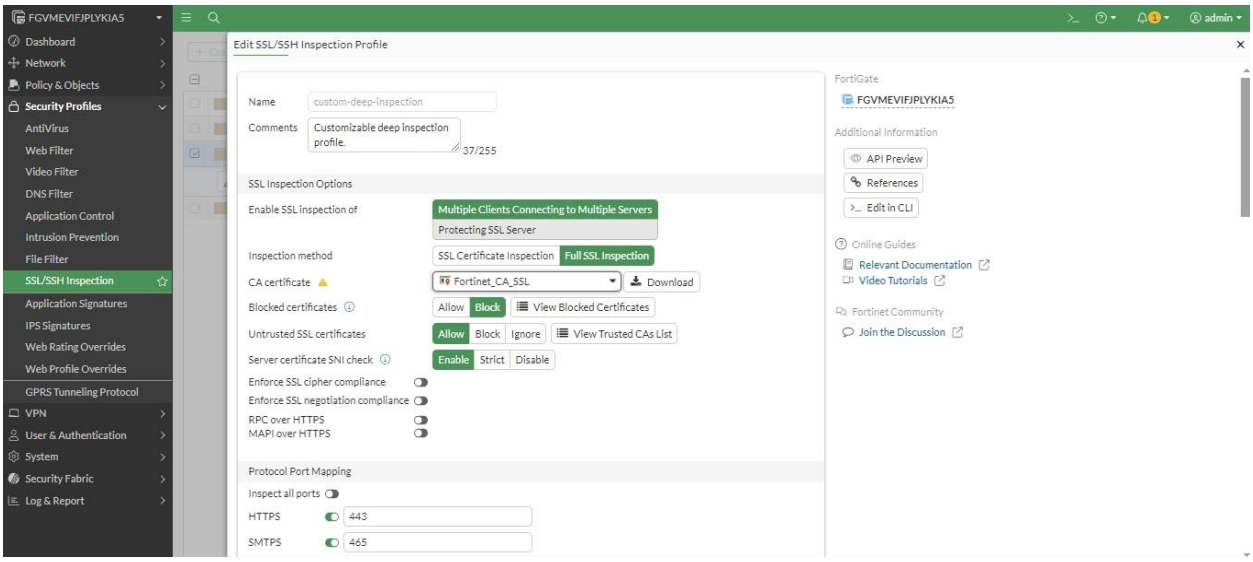




۴. وارد قسمت Security Profile > SSL SSH Inspection > Custom Deep Inspection می‌شویم. و یک Security Profile ایجاد می‌کنیم تا بتوانیم از آن در قسمت Firewall Policy ها از آن استفاده کنیم. آن را Edit می‌کنیم و تنظیمات خود را اعمال می‌کنیم.

۵. در نهایت در Firewall Policy یکی از پالیسی‌های خود را انتخاب و Edit می‌کنیم. البته بهتر است یک پالیسی جدا برای ترافیک های بیرون به داخل شبکه در نظر بگیریم. و SSL Inspection را همان سرتیفیکیتی که ایجاد کردیم را انتخاب می‌کنیم. تا فایروال بتواند این نوع ترافیک ها را باز کند و دسترسی داشته باشد.

نکته مهم: در قسمت Enable Inspection SSL، اگر گزینه اول یعنی Multiple را انتخاب کنیم، یعنی هم ترافیک های Inbound و هم ترافیک های Outbound را Inspect می‌کنیم. و اگر گزینه دوم یا Protecting را انتخاب کنیم یعنی فقط ترافیک های Inbound را Inspect کن.



7 Firewall Filtering

توسط قابلیت های فیلترینگ می‌توانیم دسترسی های بیرون به داخل و برعکس را با جزئیات بیشتری تنظیم کنیم.

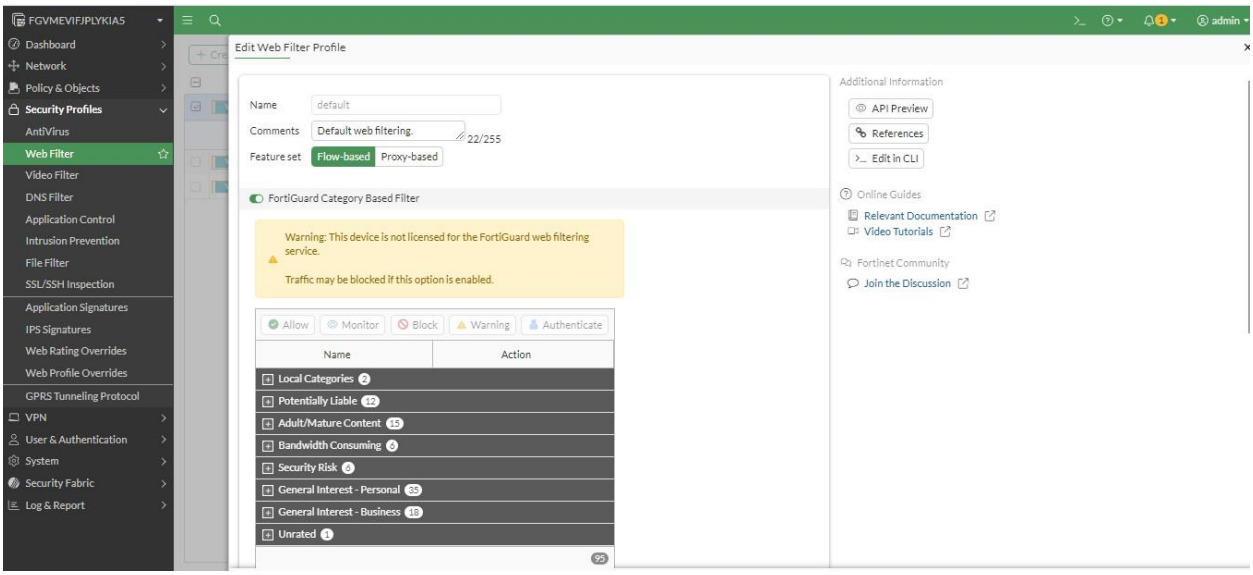
7.1 Web Filtering

با این قابلیت در فایروال فورتیگیت می‌توانیم URL ها را فیلتر کنیم. و اجازه دسترسی بدهیم یا ندهیم. طبق معمول اگر وارد مسیر Security Profiles > Web Filter شویم. می‌توانیم پروفایل مربوطه را ایجاد کنیم و آن را در پالیسی مربوطه اعمال کنیم.

در بخش اول، مشخص می‌کنیم که این پروفایل براساس Flow یا Proxy عمل کند. در حالت Proxy سیستم دقت بیشتری دارد، چرا که Session ها روی فایروال Terminate می‌شوند و دوباره Initiate می‌شوند. و در حالت Flow فایروال دقت کمتری روی ترافیک های دیتا دارد. در حالت Proxy تنظیمات بیشتری را در اختیار ما قرار می‌دهد.

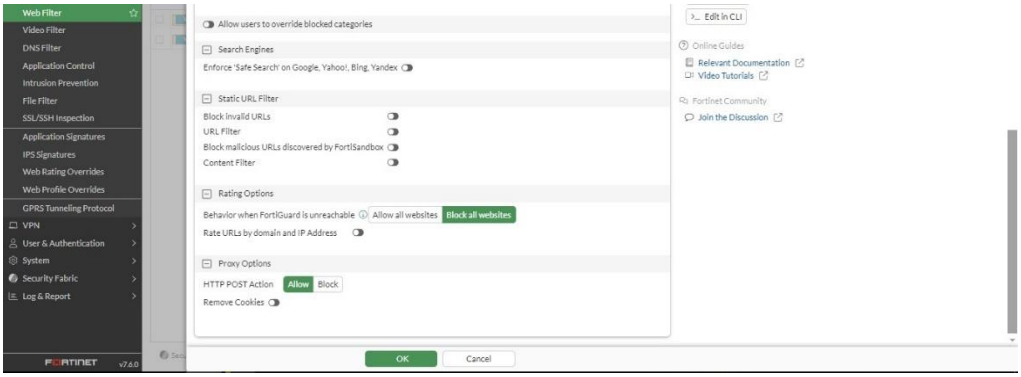
در بخش دوم، یک دسته بندی بصورت پیش‌فرض فایروال انجام داده است. که هر بخش شامل پنج حالت Allow, Monitor, Block, Warning, Authenticate می‌باشد.

در بخش سوم، می‌توانیم مشخص کنیم، یک تعداد از یوزرهای خاص علی رغم اینکه بعضی از دسته بندی ها بلاک شده اند، این یوزرها دسترسی داشته باشند.

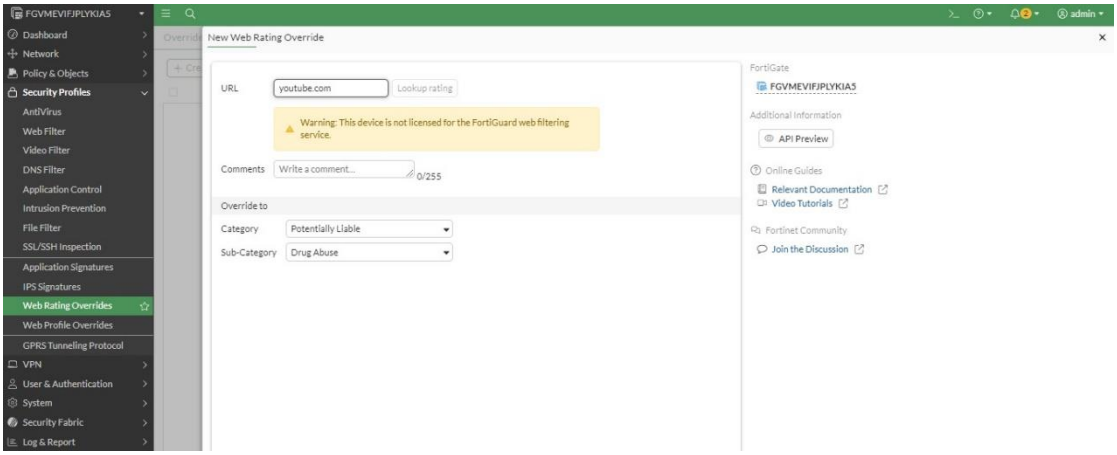


در قسمت بعد می‌توانیم مشخص کنیم که چه URL هایی مد نظر ما است و میخواهیم آن ها را بلاک کنیم. این URL ها را خودمان بصورت استاتیک وارد می‌کنیم.

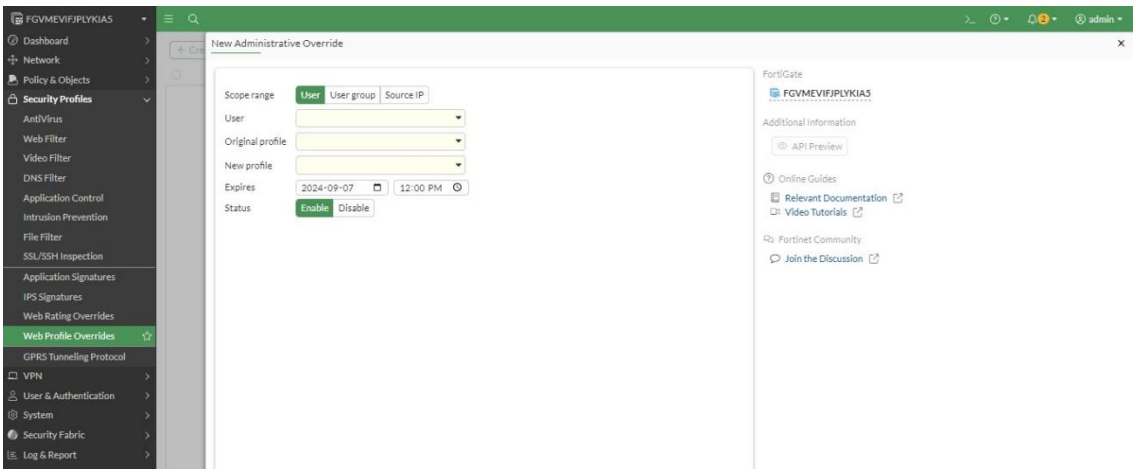
در نهایت می‌توانیم یک سری URL هایی را بر اساس Rating آن ها بلاک کنیم. یا اینکه در حالت Proxy میتوانیم Quota مشخص کنیم. مثلا چه میزان مصرفی برای این URL خاص در نظر بگیریم و یا Block URL ها در یک ساعت خاص در اختیار ما قرار بگیرند.



اگر بخواهیم در Category های خود مثلا Allow یا Deny انجام بدهیم. وارد منوی Web Rating Override می‌شویم. و از قسمت Create New با استفاده از گزینه Looking Rating می‌توانیم URL مورد نظر را ببینیم که در کدام دسته بندی قرار دارد و همان دسته بندی را ببندیم و یا باز بگذاریم. و در قسمت پایین تر آن می‌توانیم اگر دسته بندی فایروال اشتباه بود، دسته بندی آن را تغییر دهیم.



تنظیم دیگری که می‌توانیم روی Web Filter انجام دهیم به این صورت است که، در منوی Web Profile Overrides می‌توانیم برای یک Source یا آی‌پی خاص پروفایل خاصی از Web Filter را در نظر بگیریم.



7.2 DNS Filter

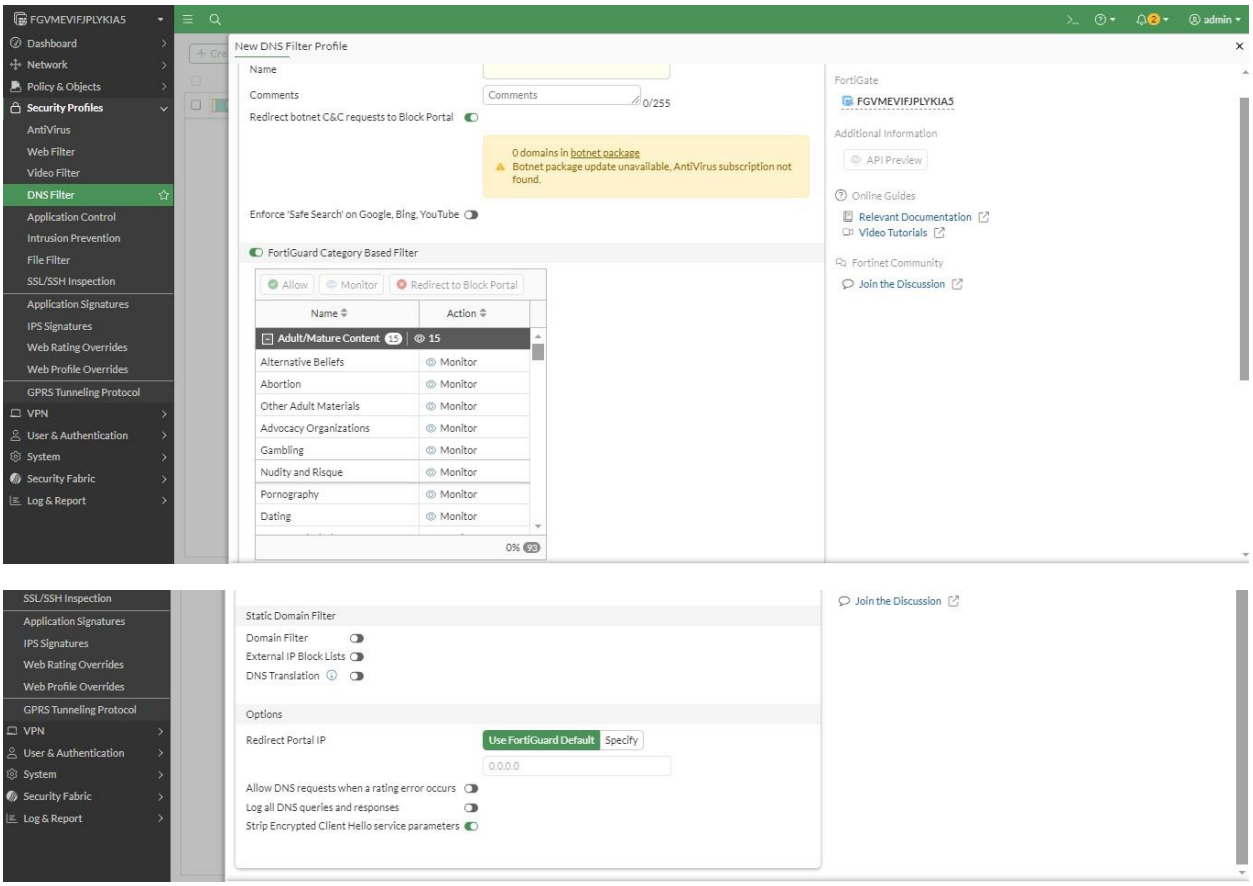
با این قابلیت می‌توانیم پکت‌های DNS Replay را تغییر دهیم و به دلخواه خود برای یک مقصد مشخص آن را تعیین کنیم. رابطه زیادی با Application Filter و Web Filter دارد. مثلا ما می‌توانیم با Web Filter یک URL خاص را فیلتر کنیم، همچنان می‌توانیم، با DNS Filter پکت‌های مربوط به DNS Replay آن را بلاک کنیم.

برای این قابلیت هم می‌توانیم یک Security Profile ایجاد کنیم. و این پروفایل را در یک پالیسی اعمال کنیم. در بخش اول DNS Replay تعداد زیادی Domain که در لیست فایروال فورتیگیت است را بلاک می‌کند.

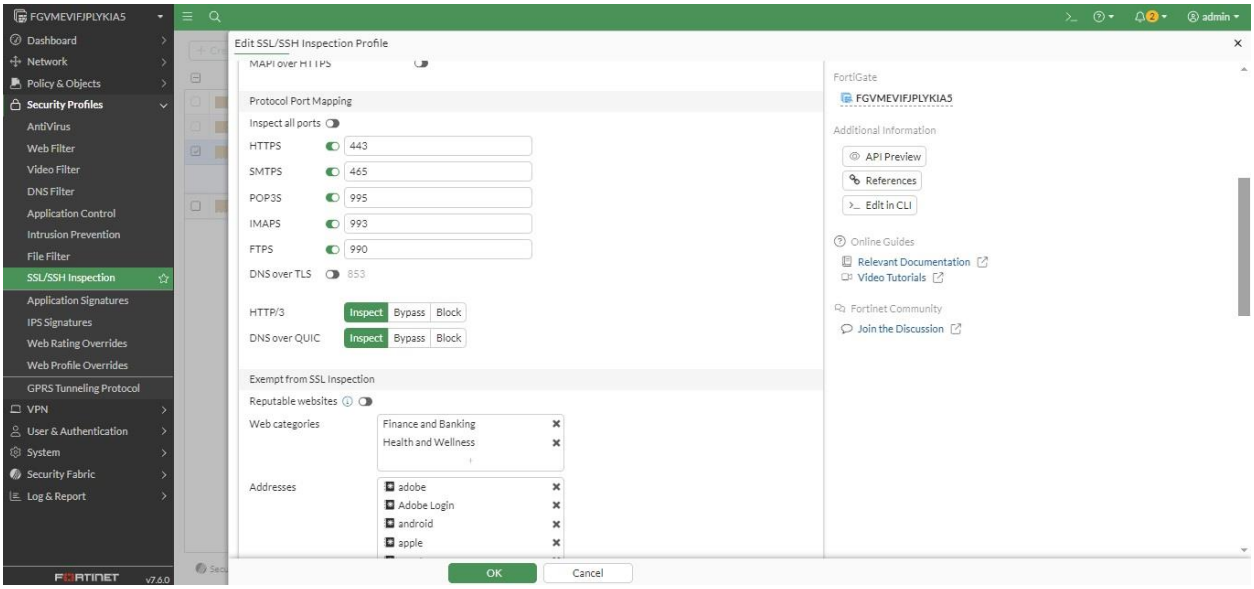
در بخش دوم هم یک سری دسته بندی ها وجود دارد که بر اساس آن هم می‌توانیم پکت های DNS Replay را بلاک کنیم.

در بخش سوم می‌توانیم بصورت استاتیک، Domain Filter را انجام دهیم. و دامین هایی که مد نظر ما است را Deny و یا Allow و یا Redirect کنیم.

در بخش چهارم می‌توانیم یک سری آی‌پی ها را مشخص کنیم تا آن‌ها را بلاک کنیم. در بخش پنجم می‌توانیم مثلا اگر کسی Cisco.com را وارد کرد، وارد google.com شود.



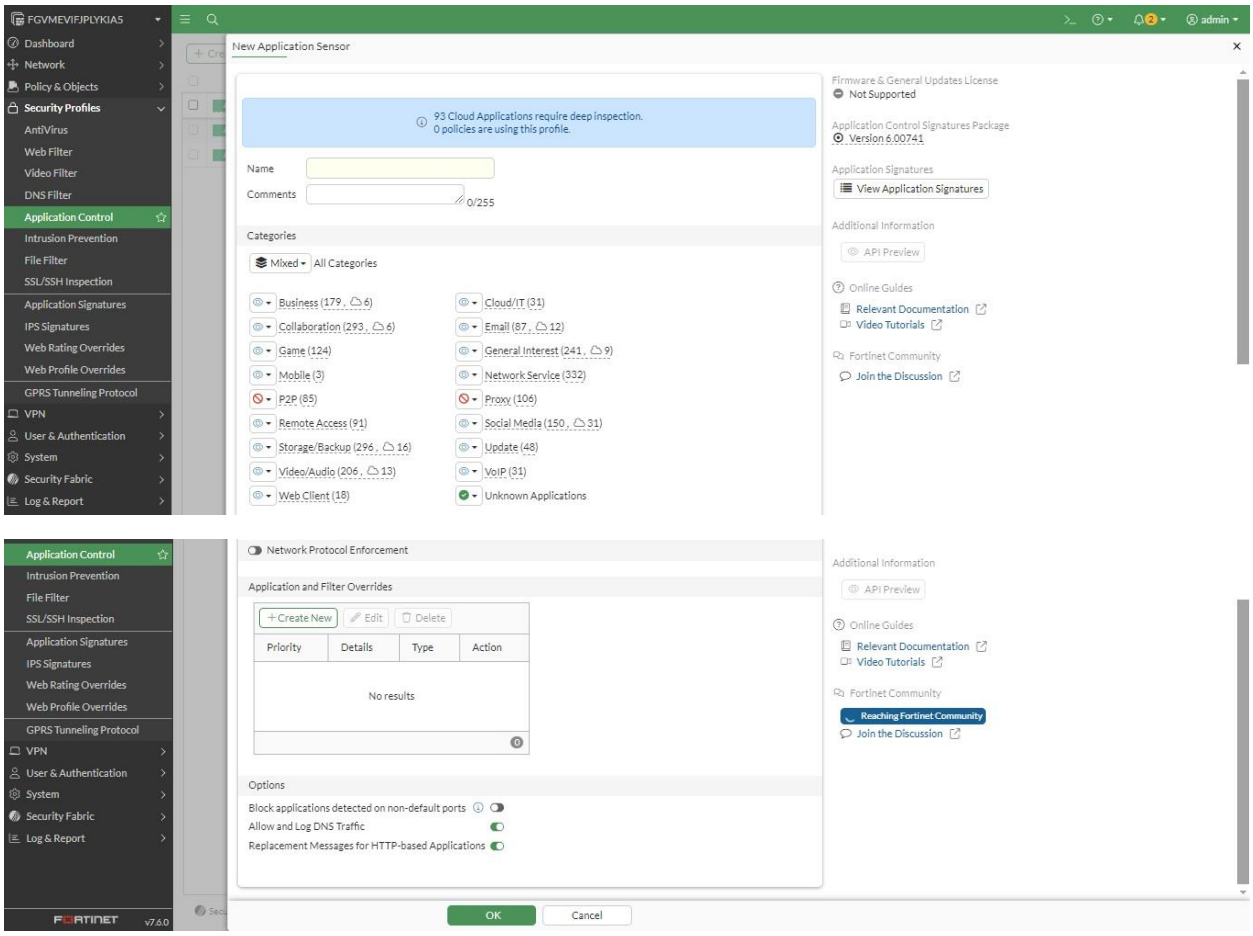
در نهایت ار پکت‌های DNS ما روی یک بستر امن جا به جا شود، یعنی آن‌ها بصورت رمز شده باشند. باید در قسمت SSL Inspection تیک گزینه DNS Over TLS را بزنیم و آن را فعال کنیم تا بتوانیم پکت‌های مربوط به DNS را هم باز کنیم و بخوانیم.



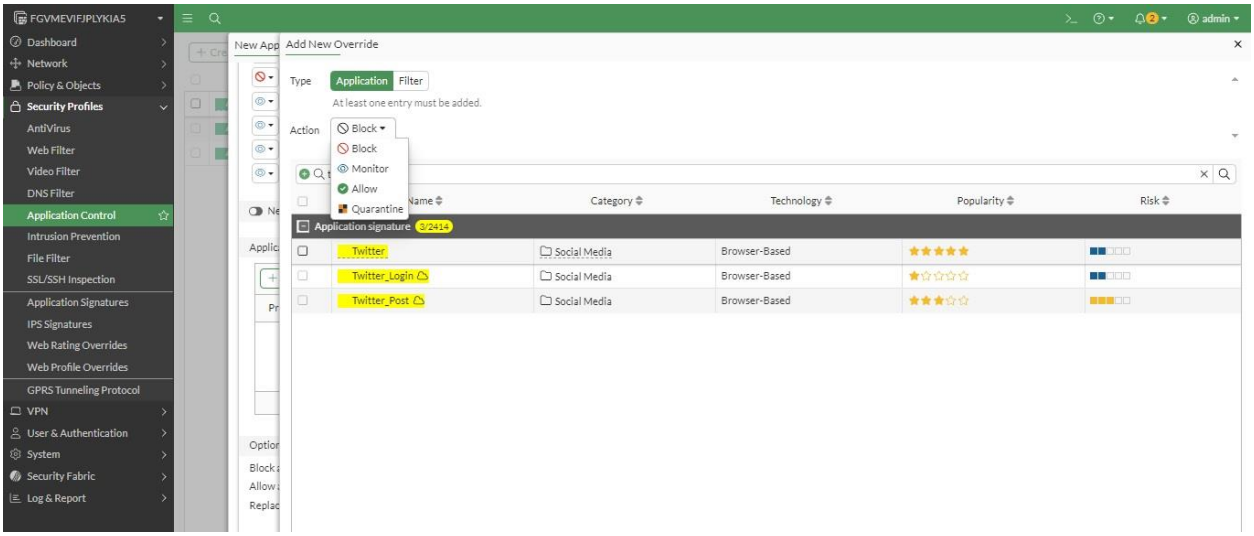
7.3 Application Filtering

با این قابلیت می‌توانیم ترافیک را در لایه اپلیکشین با استفاده از Signature های موجود مدیریت کنیم. مثلا اپلیکیشن هایی مثل توییتر، فیسبوک، تلگرام و یا ... . مهم نیست که ما به این پلیکیش ها از طریق موبایل یا لب‌تاب دسترسی داشته باشیم. دقت کنید که اگر فایروال ما در حالت Profiled-Based باشد ما باید برای Application Control خود یک پروفایل ایجاد کنیم. و آن را به پالیسی خود بدهیم. اما در حالت Policy-Based ما این بخش را در خود پالیسی تنظیم می‌کنیم و جزوی از پالیسی است. دقت کنید که برای کار فعال سازی این قابلیت حتما باید لایسنس داشته باشیم و حتما SSL Inspection را هم فعال کنیم.

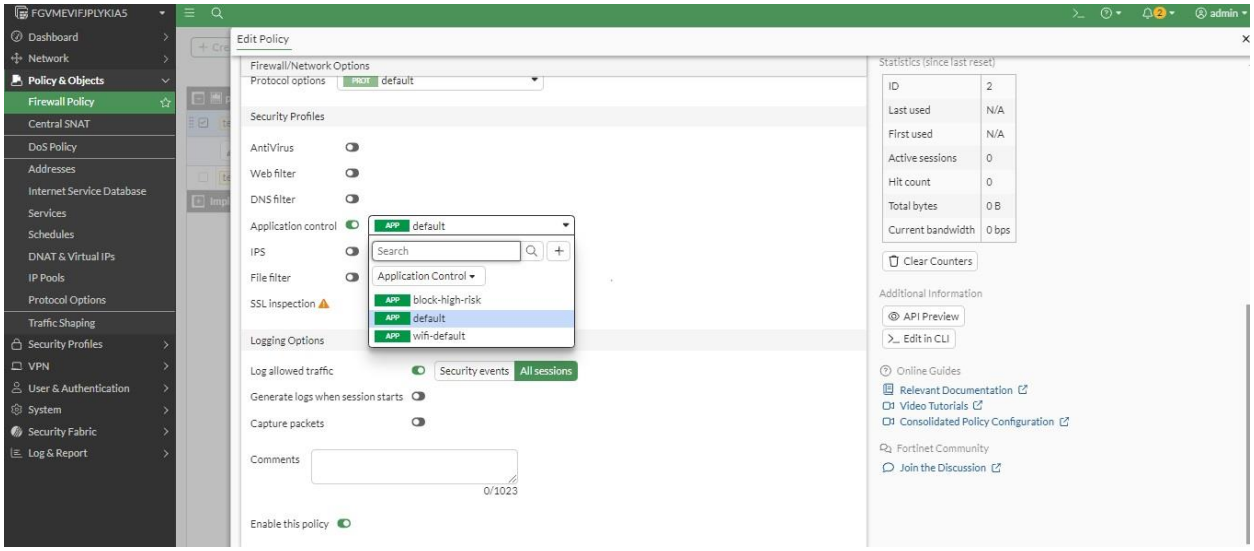
برای شروع، وارد منوی Security Profiles > Application Control می‌شویم و یک پروفایل جدید ایجاد می‌کنیم. در قسمت اول یک سری دسته بندی های اولیه هستند. که دوتای آن در حالت بلاک قراردارند. در قسمت سوم میتوانیم یک سری اپلیکیشن هایی که بصورت پیشفرض فایروال در نظر دارد را مشخص کنیم تا بلاک شوند.



در قسمت Application Filter Overrides میتوانیم اپلیکیشن‌های دلخواه خود را Allow و یا Deny کنیم.



و در نهایت این پروفایل را در یکی از پالیسی های خود اعمال میکنیم.



8 User Authentication

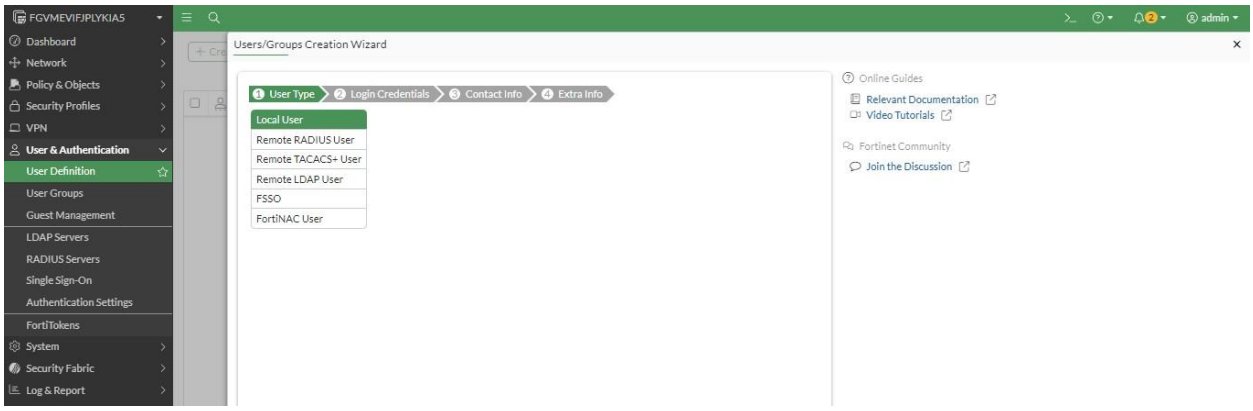
با این قابلیت می‌توانیم پالیسی‌های خود را بر اساس لیست یوزرها انجام دهیم. این کار را با یوزرهای لوکال فایروال می‌توان انجام داد. البته که بهتر است ما بصورت مرکزی یوزرهای خود را مدیریت کنیم. مثلا مدیریت یوزرها توسط اکتیودایرکتوری. در این حالت احراز هویت به دو روش انجام می‌شود، Active Authentication, Passive Authentication.

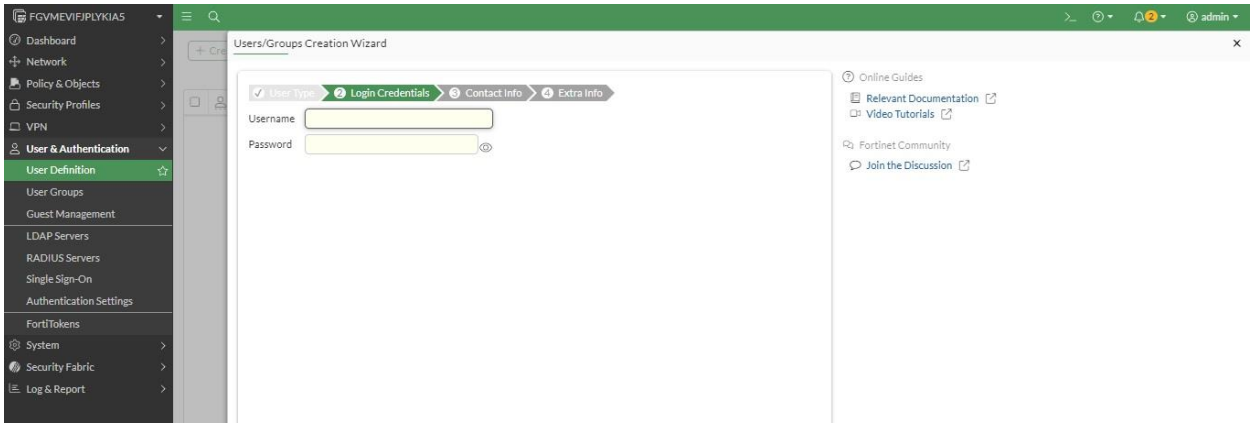
روش اکتیو یعنی ما وقتی می‌خواهیم از شبکه استفاده کنیم، باید یوزرنیم و پسورد خود را وارد کنیم تا دسترسی‌های ما مشخص شود. و بعد از احراز هویت، آی‌پی ما به یوزرنیم ما مطابق می‌شود، این تطابق تا زمانی است که Session ما به پایان برسد. مثلا یک روز یا ۱۰ دقیقه.

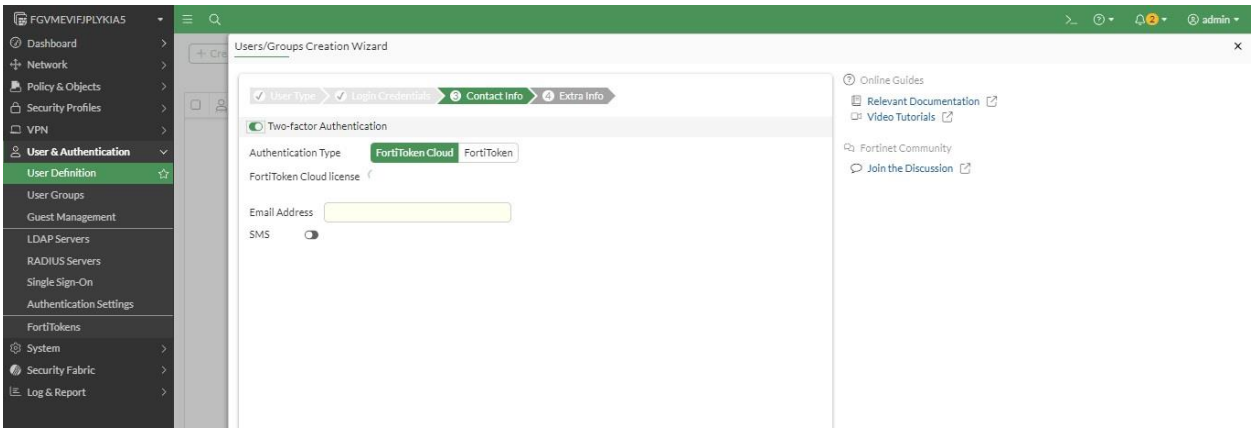
در روش Passive فایروال از قبل با توجه به آی‌پی و یوزرنیم ما، ما را میشناسد و و این احراز هویت نیازی نیست توسط ما دوباره با وارد کردن یوزرنیم و پسورد انجام شود. این کار توسط فایروال انجام می‌شود. که ما باید یک Agent در شبکه خود نصب کنیم. و این Agent از Event های اکتیودایرکتوری اطلاعات را جمع آوری می‌کند.

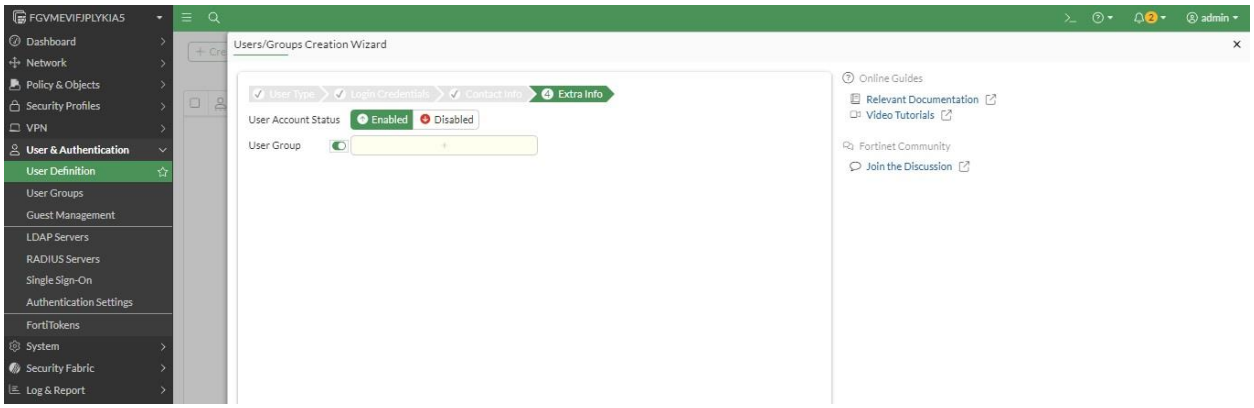
ایجاد یوزر و گروه بصورت لوکال در فایروال:

برای ایجاد یوزر وارد منوی User & Authentication > User Definition می‌شویم. و یک یوزر بصورت لوکال ایجاد می‌کنیم. یک ویزارد بصورت زیر را باید انجام دهیم. در مرحله اول نوع یوزر را انتخاب می‌کنیم. که این یوزر از نوع لوکال و یا در اکتیودایرکتوری و یا ... باشد. در مرحله دوم یوزرنیم و پسورد را وارد می‌کنیم. در مرحله سوم مشخص می‌کنیم که احراز هویت یوزر در هنگام ورود یک مرحله ای یا دو مرحله ای باشد. این کار برای ایجاد امنیت بیشتر انجام می‌شود. در مرحله چهارم اگر می‌خواهیم این یوزر عضو گروهی خاص باشد را مشخص می‌کنیم. و تعیین می‌کنیم آیا این یوزر فعال باشد و یا غیر فعال.





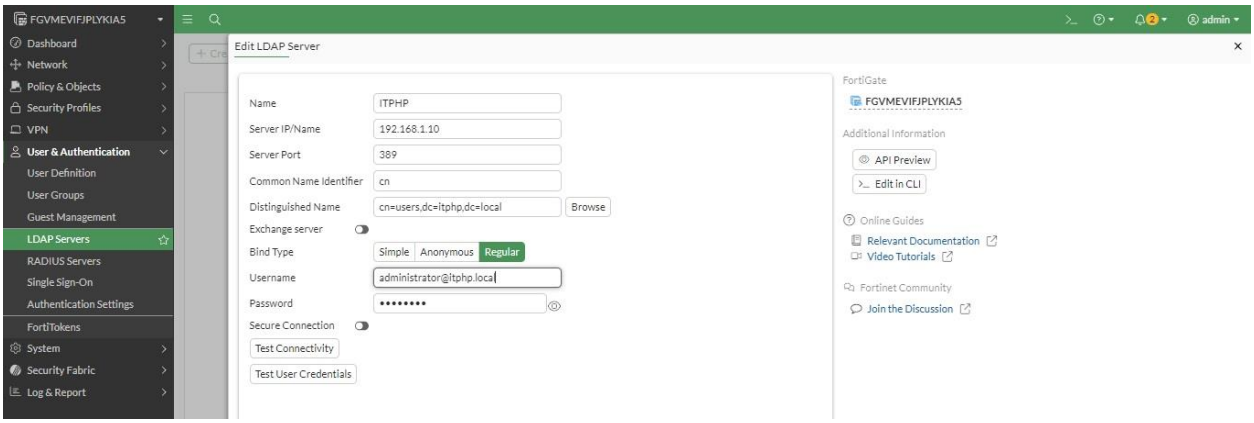




به همین صورت یوزرها و گروه‌های مورد نظر خود را ایجاد می‌کنیم. در نهایت وارد بخش Firewall Policy می‌شویم و مثلا پالیسی که مسئول برقراری ارتباطات به اینترنت است را Edit می‌کنیم و در قسمت User/Groups موارد مورد نظر خود را اضافه می‌کنیم. حال هر یوزری که بخواهد وارد اینترنت شود باید یوزرنیم و پسورد خود را وارد کند تا احراز هویت شود و در ادامه بتواند از دسترسی‌های خود استفاده کند.

فعال سازی یوزرهای اکتیودایرکتوری در فایروال فورتیگیت:

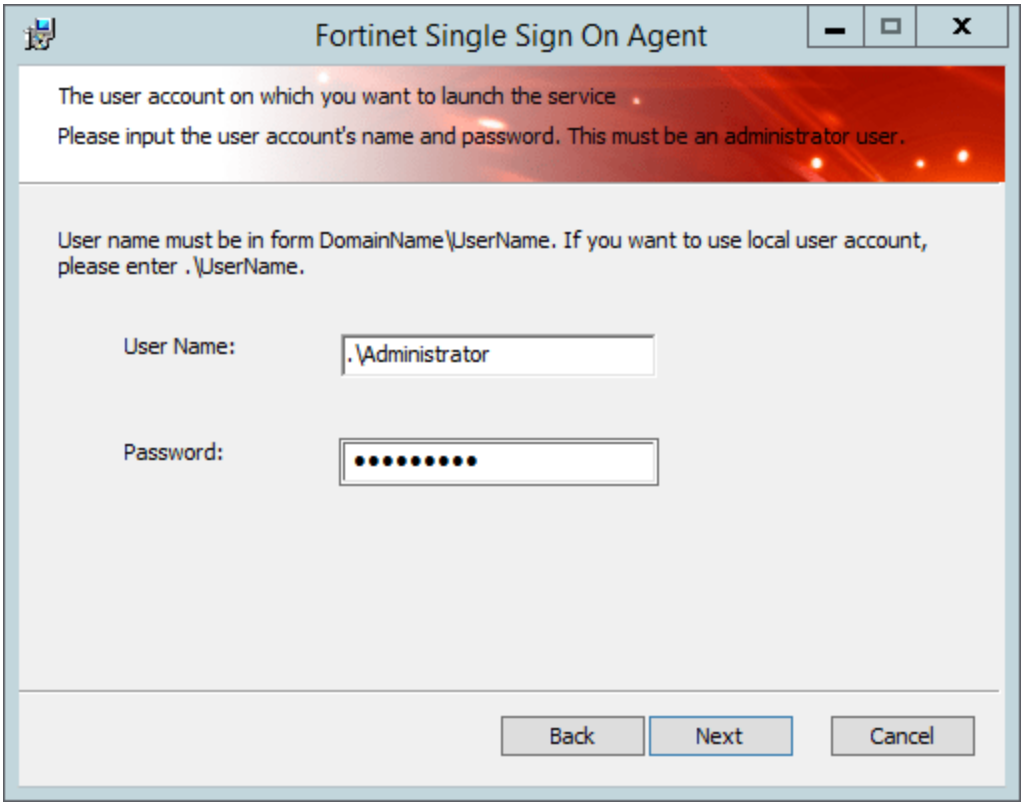
برای اینکه سرور اکتیو دایرکتوری با فایروال فورتیگیت مطابق شود. وارد منوی User & Authentication > LDAP Servers می‌شویم و موارد را بصورت زیر تنظیم می‌کنیم.

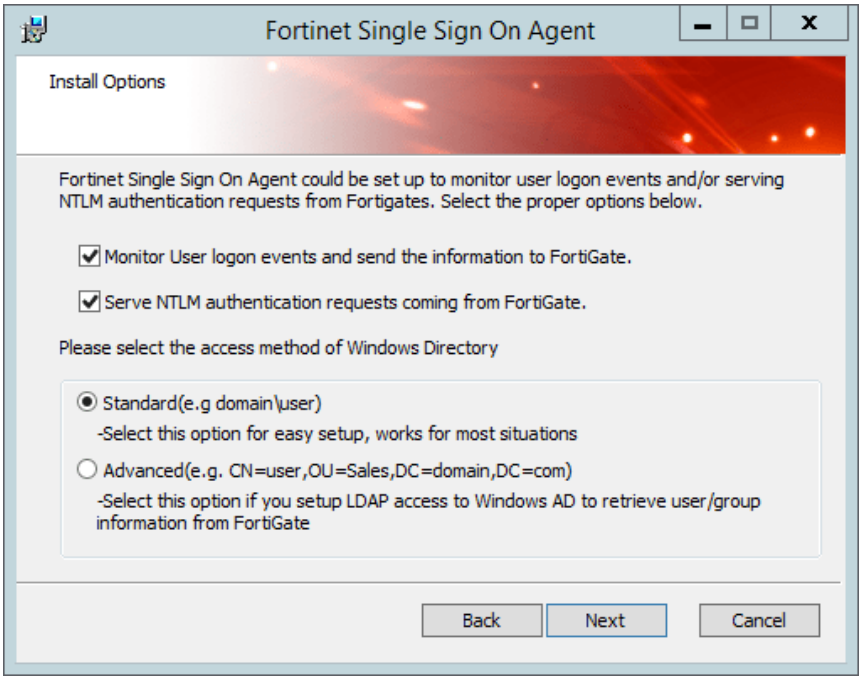


احراز هویت بصورت Passive:

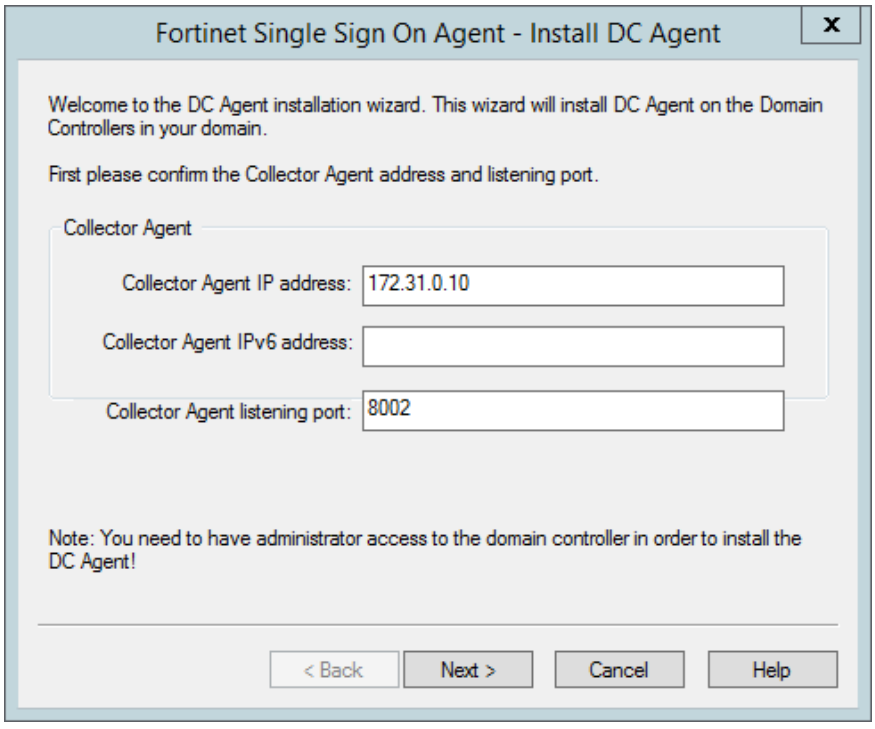
برای اینکه احراز هویت بصورت **Passive** انجام شود. باید Agent مربوط به فایروال را روی یک سرور در شبکه نصب کنید، تا این Agent اطلاعات را از اکتیو دایرکتوری دریافت کند و به فایروال انتقال دهد. نام این Agent برای فایروال FSSO-Setup است. می‌توانید این نرم افزار را مستقیما روی اکتیو دایرکتوری و یا روی یک سرور جدا نصب کنیم. در ادامه مراحل فعال سازی این سرویس را بررسی می‌کنیم.

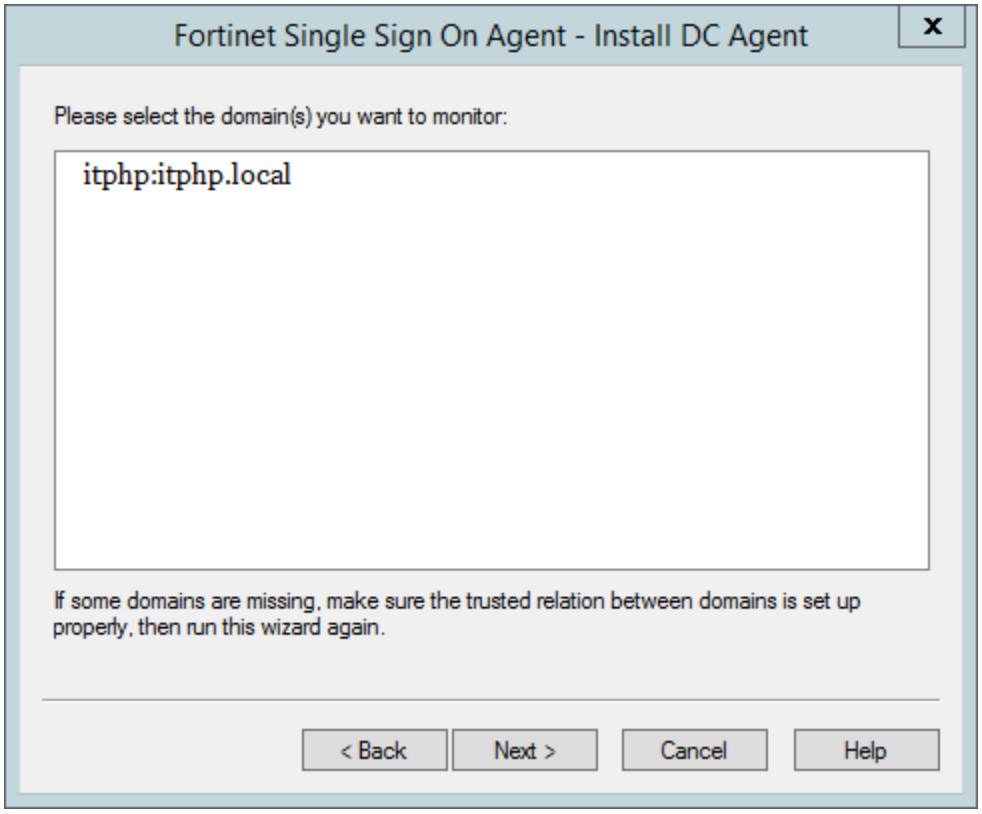
نرم افزار را اجرا می‌کنیم و مراحل اولیه را Next می‌زنیم. در مرحله سوم یوزرنیم و پسورد مربوط به ادمینی که دسترسی به سرویس‌های این نرم افزار را دارد، وارد می‌کنیم.

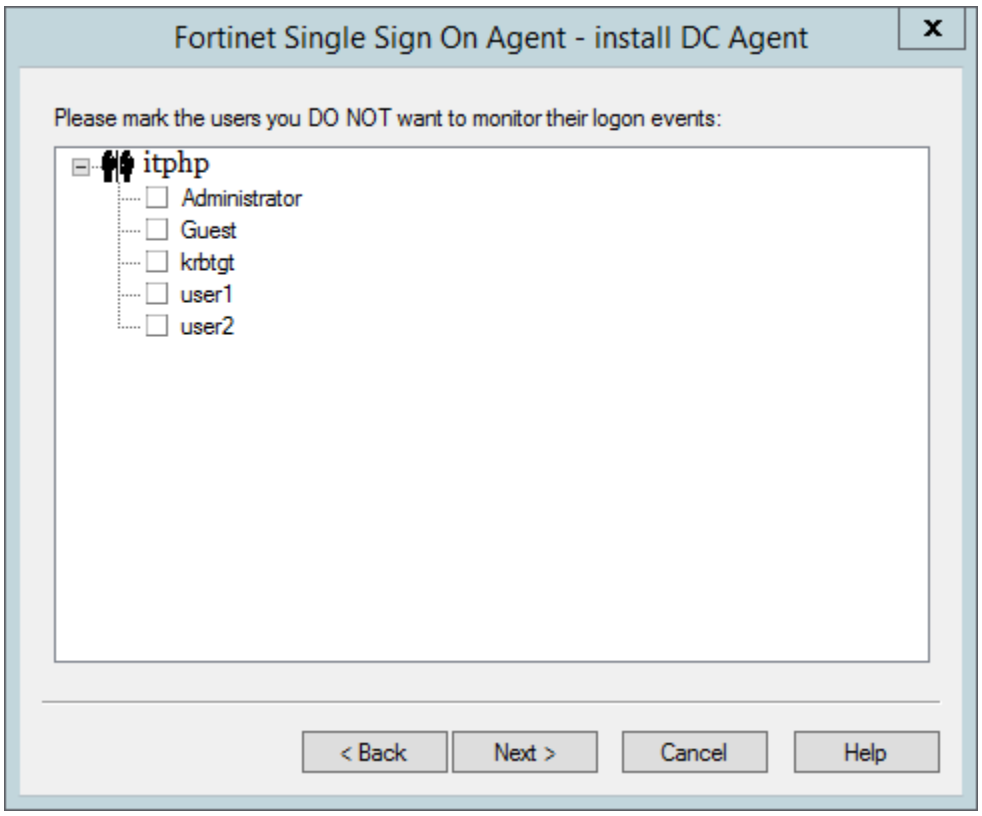




حالا باید وارد مراحل نصب DC Agent شویم، در اینجا اطلاعات DC را می‌دهیم.



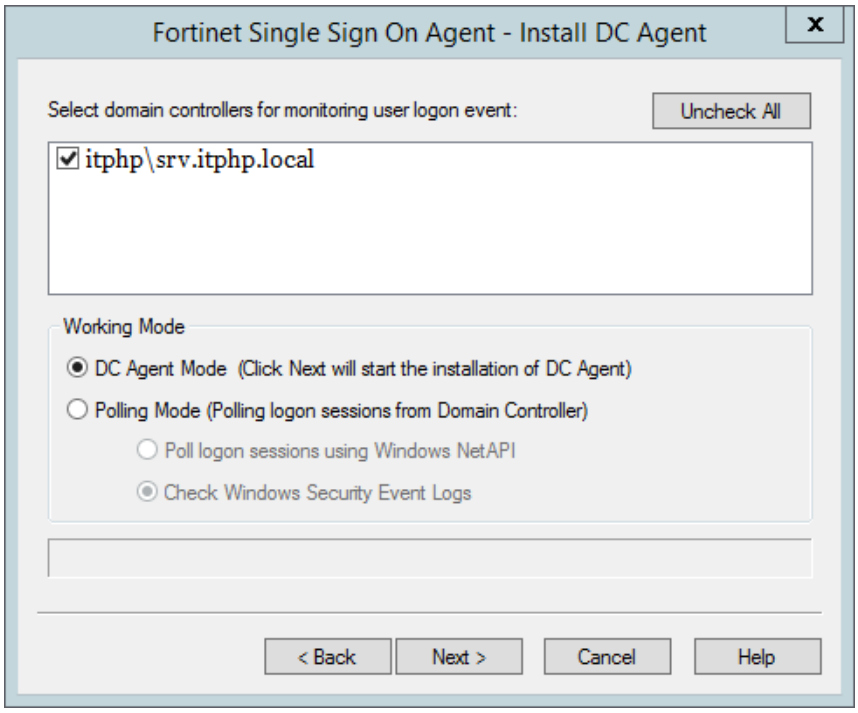

Fortinet Single Sign On Agent - Install DC Agent
Please select the domain(s) you want to monitor:
itphp:itphp.local
If some domains are missing, make sure the trusted relation between domains is set up properly, then run this wizard again.
< Back
Next >
Cancel
Help

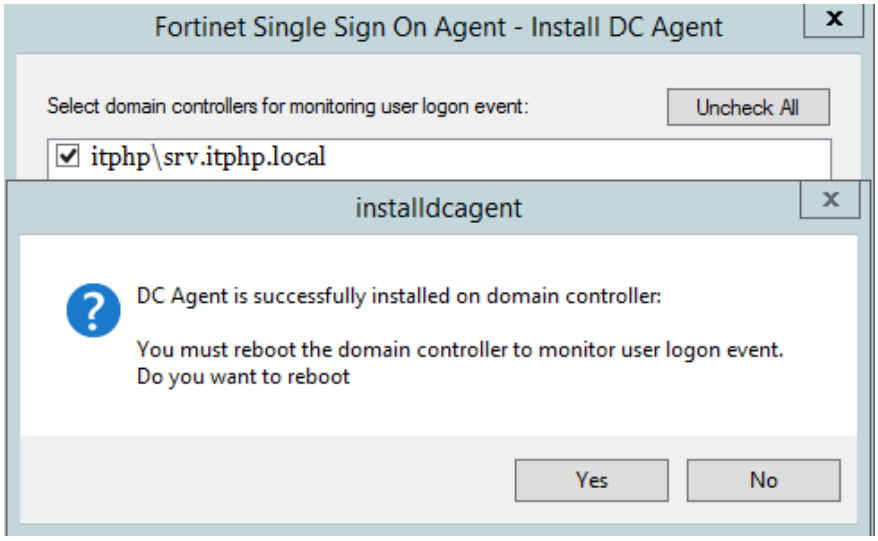

Fortinet Single Sign On Agent - install DC Agent
Please mark the users you DO NOT want to monitor their logon events:
itphp
Administrator
Guest
krbtgt
user1
user2
< Back
Next >
Cancel
Help

در این مرحله باید mode را انتخاب کنید که دوتا حالت کلی داره:

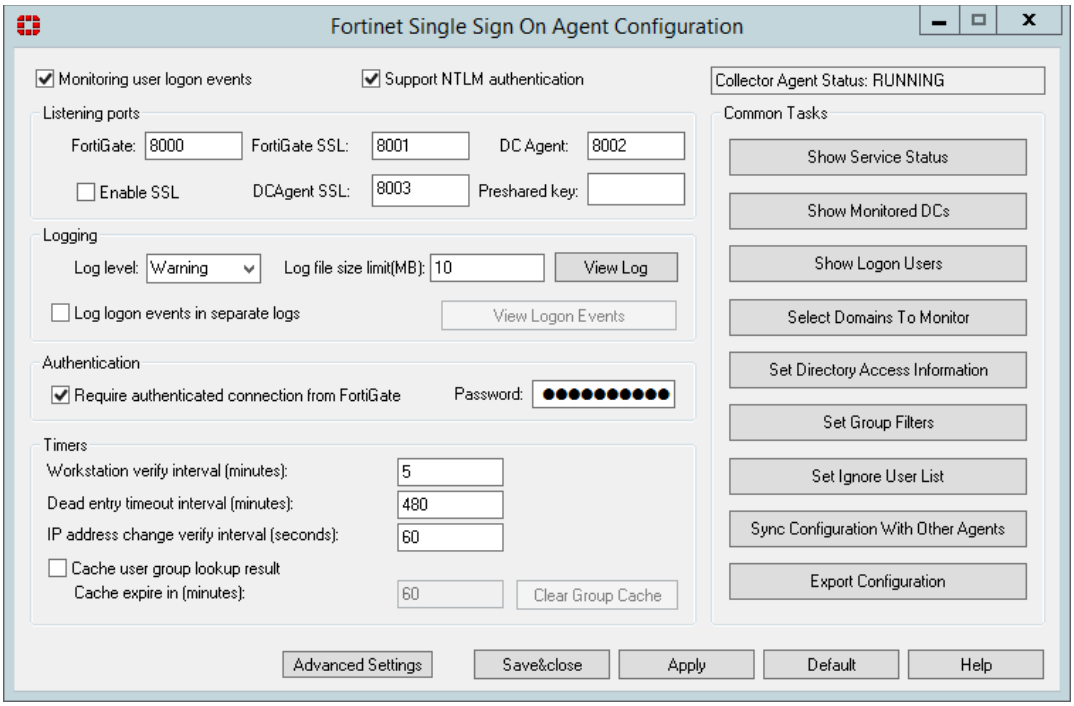
۱. در صورت انتخاب DC-Agent mode یک dcagent.dll در Windows\system32 ایجاد می کند و Agent بر روی DC شما نصب می شود، در این حالت Agent به صورت مستقیم از DC به Forti ارتباط دارد، توجه داشته باشید که در این حالت DC نیاز به ری‌استارت مجدد دارد.

۲. در صورت انتخاب Polling Mode شما می‌توانید از NetAPI و یا Event Log برای ارتباط استفاده کنید که هر دو query ها را هر ۱۰ ثانیه ارسال می‌کنند، در NetAPI سرعت بیشتر است ولی برخی از log ها ارسال نمی‌شود ولی در Event log polling تمام Log ها ارسال می‌شود برای همین کندتر می‌باشد.

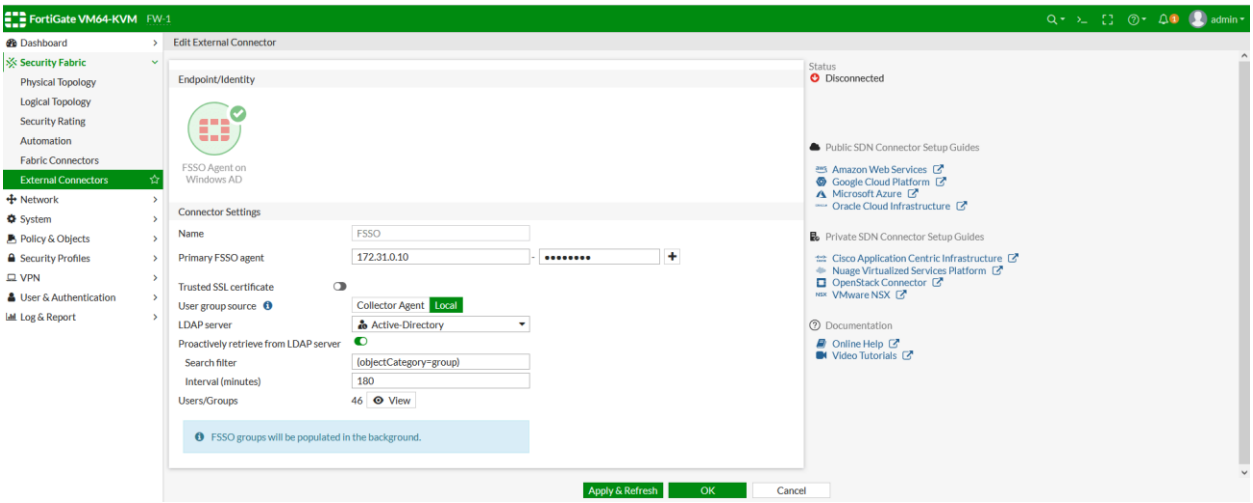




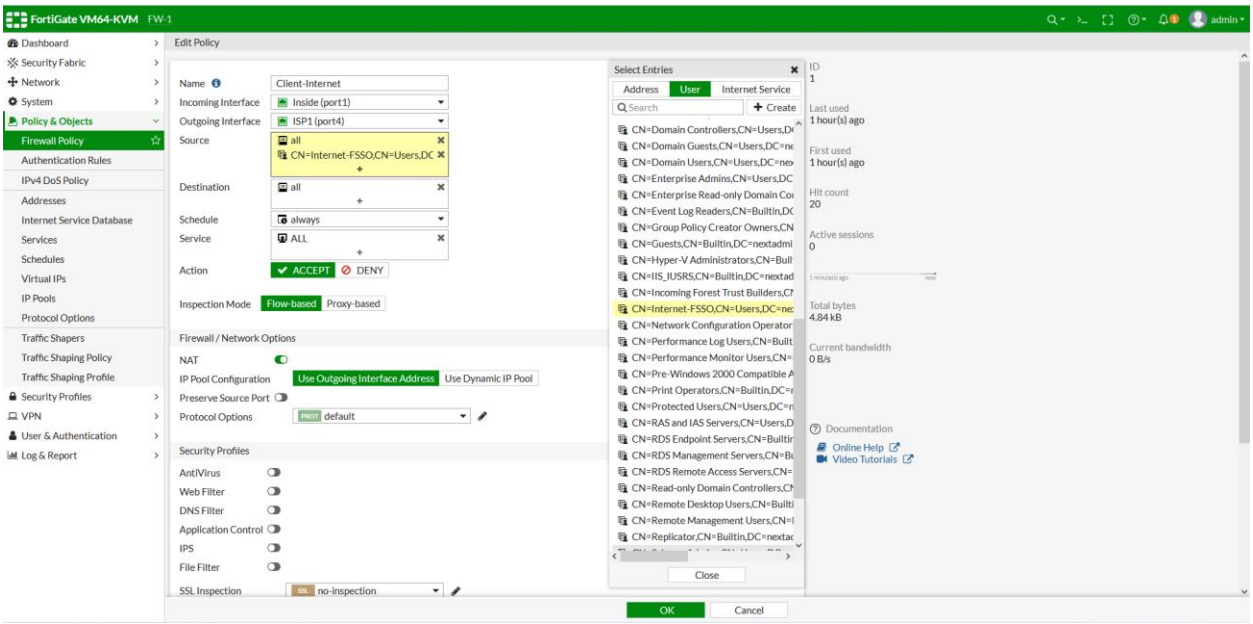
پس از این که سرور DC ما ری‌استارت شد می‌توانید کانفیگ FSSO را باز کنید و مشاهده کنید که سرویس ها RUNNIG می‌باشد یا خیر.



حالا باید تنظیمات را بر روی فورتی گیت انجام دهیم، فقط برای تست لازم است که PC خود را به DC خود Join کنیم، این نکته را توجه کنید که ما قبلا یک پالیسی ایجاد کرده بودیم که در آن گفته بودیم PC ما فقط اجاده استفاده از سرویس‌های RDP و ICMP به سرور DMZ را دارد که قبل از جوین کردن به سرور باید این پالیسی را تغییر بدید و بر روی ALL قرار دهید تا امکان ارتباط با DNS سرور هم داشته باشه و بتونه جوین دامین شود. حالا وارد Security Fabric > External Connector می‌شویم و Create New + را کلیک می‌کنیم و Fortinet Single Sign-On Agentرا انتخاب می‌کنیم.



حالا یک Name انتخاب می‌کنیم و در Primary FSSO Agent نیز آدرس DC و پسوردی که در DC Agent وارد کردیم را وارد می‌کنیم که 172.31.0.10 می‌باشد، User group source را بر روی Local قرار می‌دهیم و در LDAP server باید اکتیودایرکتوری را انتخاب نماییم که قبلا ایجاد کرده بودیم، در آخر نیز Proactively retrieve from LDAP server را فعال می‌کنیم و OK می‌کنیم.

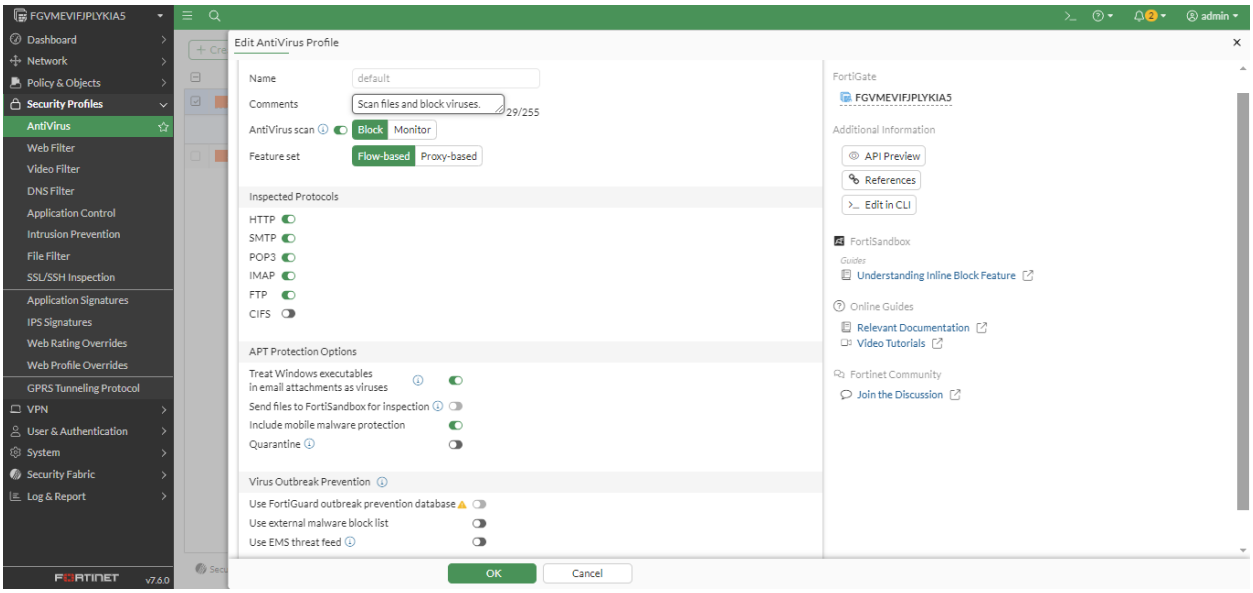


حالا FSSO به اکتیودایرکتوری متصل شده است و می‌توانیم از آن استفاده کنیم، همانطور که مشخص است یوزر ها و گروه های ما را شناسایی کرده است. در آخر نیز می‌توانیم از قسمت پالیسی بر روی پالیسی که برای ارتباط PC خودمان به اینترنت ایجاد کرده بودیم در قسمت Source یوزر یا گروه مورد نظر را وارد کنیم تا از این پس یوزر هایی که ما مشخص کردیم امکان استفاده از اینترنت یا هر پالیسی که ما قرار دادیم را داشته باشند.

9 Antivirus

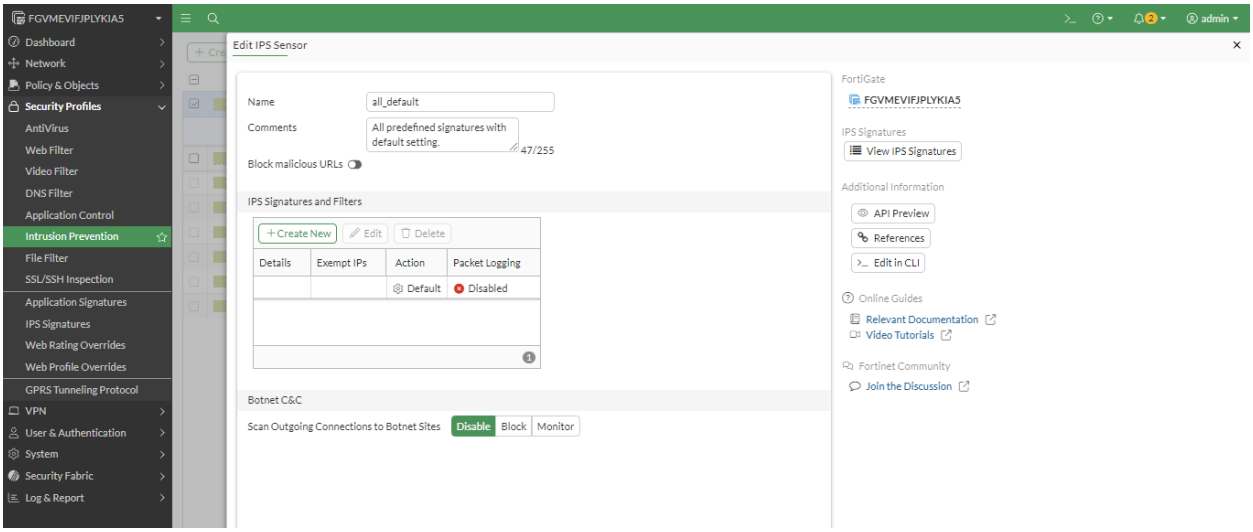
فایروال فورتیگیت آنتی ویروسی را تحت شبکه برای کاربران فعال می‌کند. تا از اینکه کاربران روی لینک‌های مخرب کلیک کنند و یا فایل‌های مخرب را دانلود کنند، جلوگیری کند. برای استفاده از این قابلیت هم می‌توانیم یک Security Profile ایجاد کنیم و از آن در پالیسی‌های خود بهره‌مند شویم. برای این کار وارد بخش Security Profile > Antivirus می‌شویم. دو حالت Proxy Base و Flow Base است که Proxy حالت بهتری است. قابلیت‌های زیادی دارد که بسیار ساده است.

نکته مهم اینکه اگر حتی یکی از پروفایل‌های ما در حالت Proxy باشد. پالیسی‌های ما هم باید در حالت Proxy باشند. با فعال سازی قابلیت Antivirus قابلیت SSL Inspection هم فعال می‌شود. دقت کنید که حتما SSL Inspection باید در حالت Full SSL Inspection باشد. در غیر این صورت عمل خاصی را آنتی ویروس برای ما انجام نمی‌دهد. حال اگر یوزر بخواهد فایل مخربی را دانلود کند، با پیغام Block از طرف فایروال فورتیگیت مواجه می‌شود.

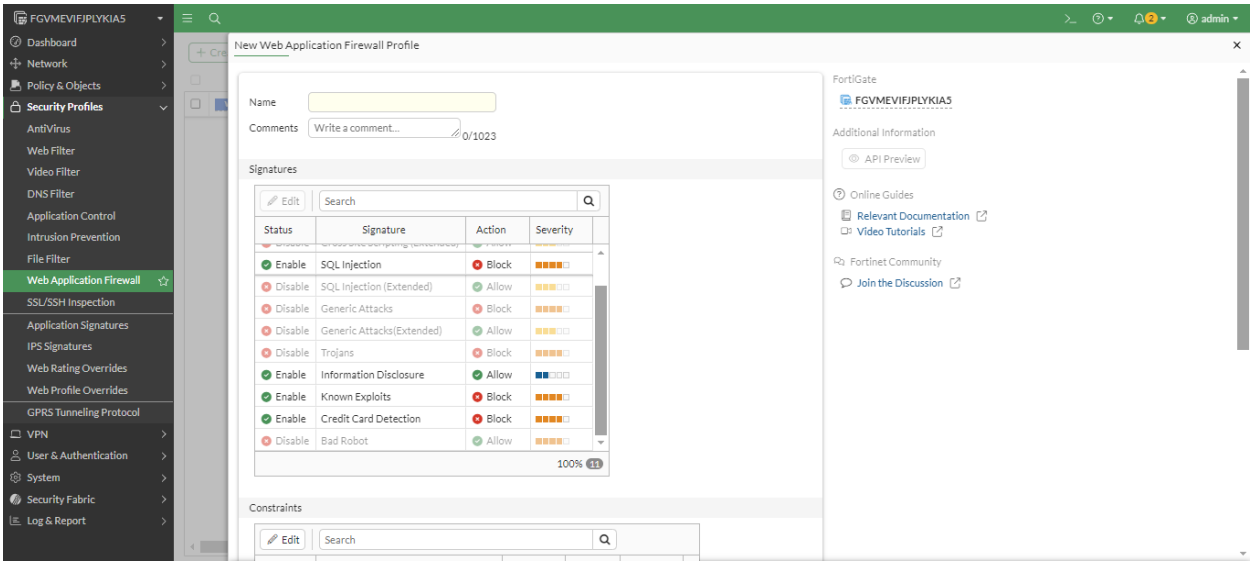


10 IPS/WAF

IPS یا Intrusion Prevention System یکی از قابلیت‌های فایروال فورتیگیت است که ترافیک های مخرب را شناسایی و عملکرد آن‌ها را بلاک می‌کند. ترکیب آنتی ویروس و IPS میتواند خوب باشد، از این جهت که از ورود فایل‌ها و ترافیک‌های مخرب جلوگیری می‌کند. WAF یا Web Application Firewall که حملات تحت وب را کنترل می‌کند. IPS را می‌توانید از قسمت Security Profile > Intrusion Prevention ببینید. و یا حتی یک Signature جدید برای آن ایجاد کنید. و از آن در قسمت پالیسی‌ها استفاده کنید. در منوی Application Signature می‌توانید Signature هایی را ایجاد کنیم. دقت کنید که این بخش را همیشه در حالت آپدیت نگه داریم.



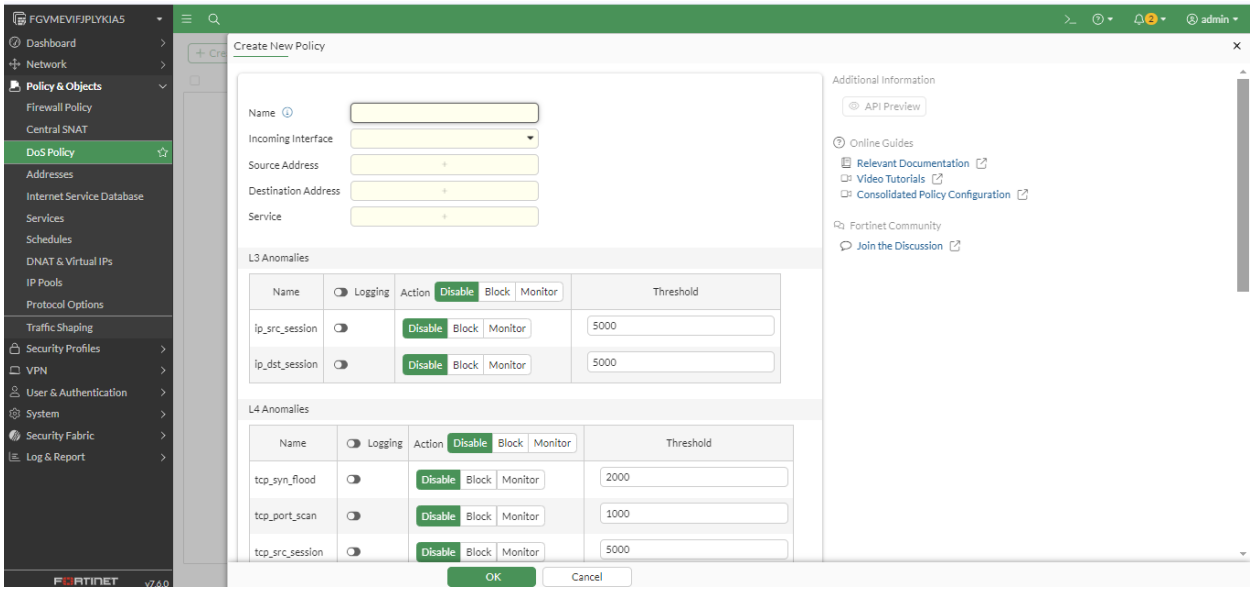
WAF را باید ابتدا از منوی System > Feature Visibility در حالت فعال قرار دهیم تا در منوی Security Profile آن را ببینیم. حال اگر وارد منوی Security Profile > Web Application Firewall شویم. می‌توانیم تنظیمات مربوط به این بخش را انجام دهیم. معمولا WAF را برای ترافیک‌هایی که از بیرون به داخل می‌آیند، فعال می‌کنیم. دقت کنید که WAF فقط در حالت Proxy روی فایروال فورتیگیت عمل می‌کند.



11 Dos Policy

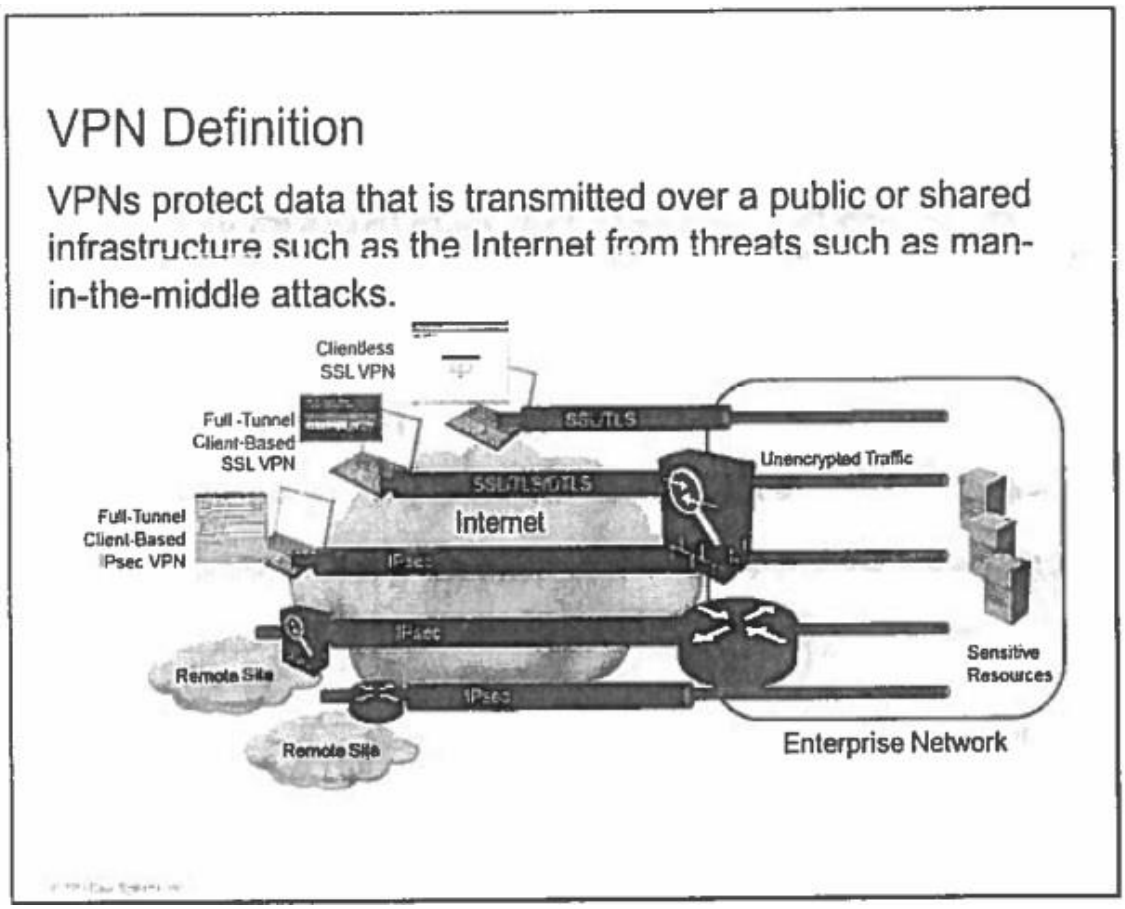
با این قابلیت در فایروال فورتیگیت، می‌توانیم از حملات DoS و DDoS جلوگیری کنیم. این قابلیت بصورت جدا روی فایروال در یک منوی جدا در نظر گرفته شده است. DoS حملاتی هستند که به هدف از کار انداختن سرویس‌های طرف مقابل اجرا می‌شود. برای انجام تنظیمات این بخش وارد منوی Policy & Object > DoS Policy می‌شویم. و می‌توانید یک سری گزینه‌ها که مربوط به جلوگیری حملات از پیش تعریف شده در لیست را فعال کنید. همچنان می‌توانید با توجه به آدرس مبدا و مقصد و سرویس مورد نظر هم برخی از حملات را جلوگیری کنید.

نیازی نیست این پالیسی را در جایی اعمال کنید و به تنهایی قابل استفاده است. نکته این است که قابلیت IPS اکثر این حملات قدیمی و ابتدایی را جلوگیری می‌کند.

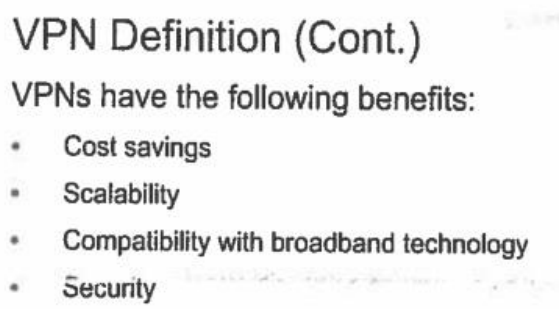


12 VPN and Cryptography

VPNمخفف کلمه Virtual Private Network است. در این بخش نقش VPN در امنیت را بررسی خواهیم کرد. امن سازی دیتایی که روی یک مسیر عمومی انتقال پیدا می‌کند را اصطلاحا VPN می‌گوییم یا بصورتی VPN این مسئولیت را بر عهده دارد. در شکل زیر این تعریف را بهتر درک خواهیم کرد.



مزایای VPN را در شکل زیر مشاهده می‌کنیم. VPN روش بسیار کم هزینه است و براحتی روی بستر اینترنت پیاده سازی می‌شود. مقیاس پذیری زیادی دارد همچنان می‌توانید تا چندین هزار سایت متفاوت را از طریق VPN به هم وصل کنید. با تکنولوژی هایی مثل DSL سازگاری کامل دارد. و می‌توانید روی بستر DSL بحث VPN را پیاده سازی کنید. و در نهایت امنیت خوبی را برای ما فراهم می‌کند.



تهدید هایی که معمولا در محیط های WAN و اتصال بصورت Remote Access وجود دارد، بصورت زیر است. مورد اول به معنای حمله برای شنود، و مورد دوم حمله برای جعل اسناد و مورد سوم حمله به این صورت که مابین دو طرف قرار بگیرد و اطلاعات ارسالی هر دو طرف را داشته باشد که در ادامه توضیحات بیشتری در مورد آن ارائه خواهیم کرد.

Key Threats to WANs and Remote Access

The key threats to data privacy:

- Eavesdropping attacks
- Masquerading attacks
- Man-in-the-middle attacks

روش اول، معمولا از طریق Sniffer ها انجام می‌شود. این نرم افزار ها به راحتی دیتای ما را شنود می‌کنند. و در صورتی که دیتای ما رمز نشده باشند براحتی دیتای ما را می‌خوانند. معمولا توصیه می‌شود از پروتکل هایی با امنیت بالا برای برقراری ارتباط استفاده شود. مثلا بجای استفاده از HTTP از HTTPS استفاده شود.

Key Threats to WANs and Remote Access (Cont.)

Eavesdropping Attacks

- A packet sniffer is a software application that uses a network adapter card in promiscuous mode to capture all network packets.
- Packet sniffers exploit information passed in clear text. Protocols that pass information in the clear include the following:
  - Telnet, FTP, SNMP, POP, HTTP
- Common solutions for companies to protect information are:
  - HTTP with SSL (HTTPS)
  - Implement a VPN with encryption

در روش Eaves Dropping attack حمله کننده آی‌پی خود را جعل می‌کند یا اصطلاحا IP Spoofing انجام می‌دهد. ما باید جلوی هر گونه تغییر روی دیتا را بگیریم. برای جلوگیری می‌توانیم از راه حل Packet Integrity استفاده کنیم.

Key Threats to WANs and Remote Access (Cont.)

Masquerading Attacks

- A masquerading attack is where an individual hides their identity, possibly even assuming someone else's identity, example: IP spoofing.
- IP spoofing occurs when a hacker inside or outside a network impersonates the conversations of a trusted computer.
- Two general techniques are used during IP spoofing:
  - A hacker uses an IP address that is within the range of trusted IP addresses.
  - A hacker uses an authorized external IP address that is trusted.
- The most common solution is to use a packet integrity check system, which is implemented with a hashing function.

در روش Masquerading Attacks شخصی خود را بین دو طرف قرار می‌دهد، بطوری که به تمام دیتای ارسالی از دو طرف دسترسی دارد. و می‌تواند دیتا را جعل و یا شنود کند. معمولا راه حل جلوگیری از این اتفاق، استفاده از فایروال است. فایروال Sequence Number های رندوم ایجاد می‌کند. تا Session های موجود هک نشوند.

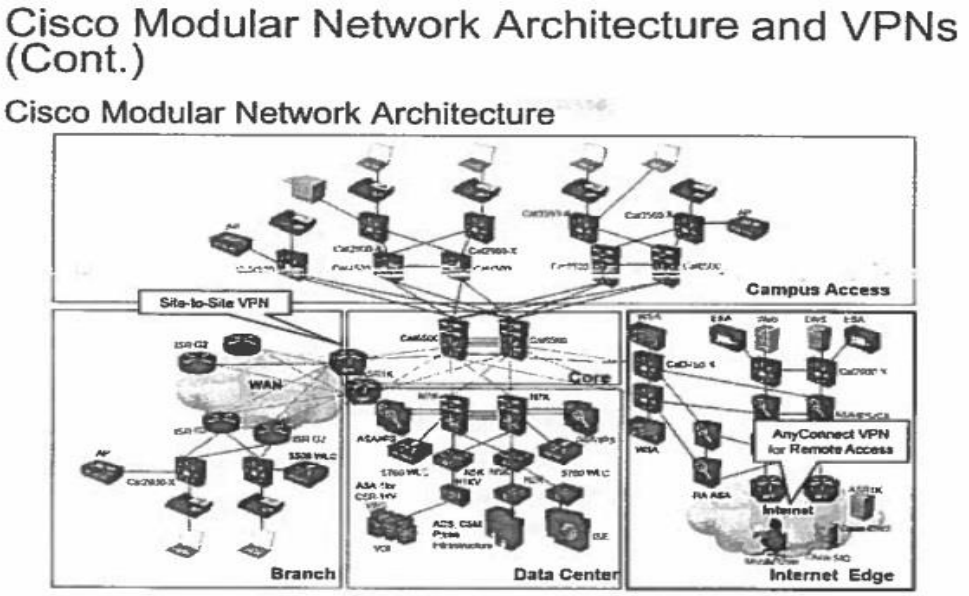
Key Threats to WANs and Remote Access (Cont.)

Man-In-The-Middle

- A man-in-the-middle attack requires that the hacker have access to network packets that come across a network.
- A man-in-the-middle attack is implemented using the following:
  - Network packet sniffers
  - Routing and transport protocols
- Several solutions for man-in-the-middle attacks are:
  - A firewall system randomizes TCP sequence numbers
  - VPNs provide three tools to combat man-in-the-middle attacks: device authentication, packet integrity checking, and encryption

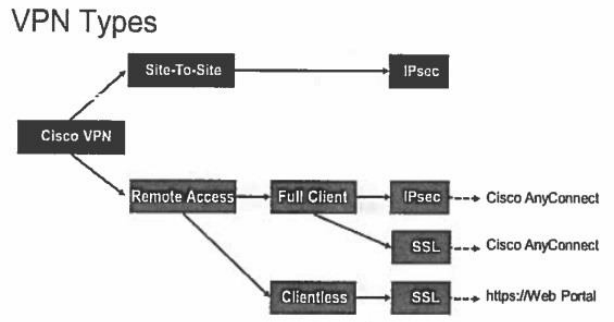
تمام سه مشکل فوق را VPN می‌تواند حل کند.

سیسکو راه حلی برای طراحی امن برای شبکه ها دارد. مثلا راه حل Cisco Safe و یا Cisco CVD یا Cisco Validated Design که مارا جهت یک طراحی امن در شبکه راهنمایی می‌کند. که در شکل زیر معماری کلی یک نتورک را برای ما نمایش می‌دهد. معمولا شبکه‌ها از بخش‌هایی مثل Branch, Data Center, Internet Edge, Campus تشکیل شده اند.

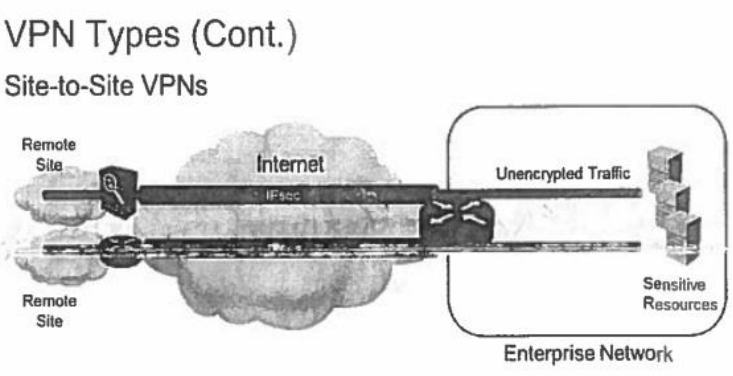


انواع روش های VPN بصورت زیر است:

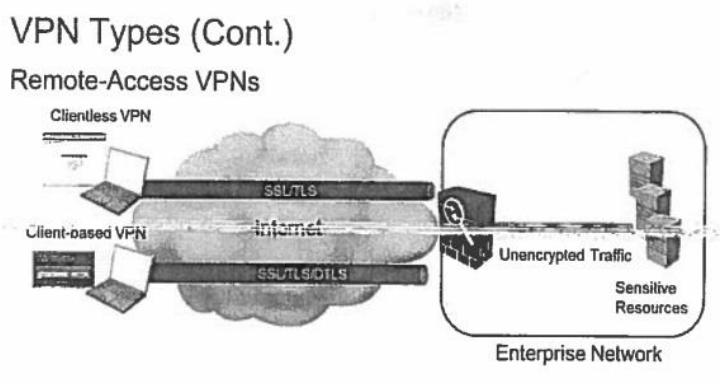
معمولا بین شعبات مختلف با دفتر مرکزی از روش Site-To-Site استفاده می‌شود و در روش Remote Access زمانی که یک طرف ارتباطات ما کلاینت ها باشند از این روش استفاده می‌کنیم. Clientless یعنی بدون نصب نرم افزاری قادر به استفاده از قابلیت VPN است. Full Client یعنی با نصب نرم افزاری می‌توانیم بصورت کامل از مزایای این قابلیت در VPN برخوردار شویم.



تصویر زیر نمونه ای از Site-To-Site VPN است.



در شکل زیر هم نمونه ای از Remote Access VPN را مشاهده می‌کنیم.



اجزا یا قابلیت های VPN به شرح زیر هستند:

Authentication یعنی احراز هویت، و ما از اینکه طرف مقابل شخص جعلی نیست مطمین می‌شویم.

Encapsulation Method یعنی با چه روش هایی دیتا را سوار بر یک دیتای امن کنیم و تحویل مقصد دهیم.

Packet Integrity یعنی جلوگیری از تغییر دیتا در طول مسیر.

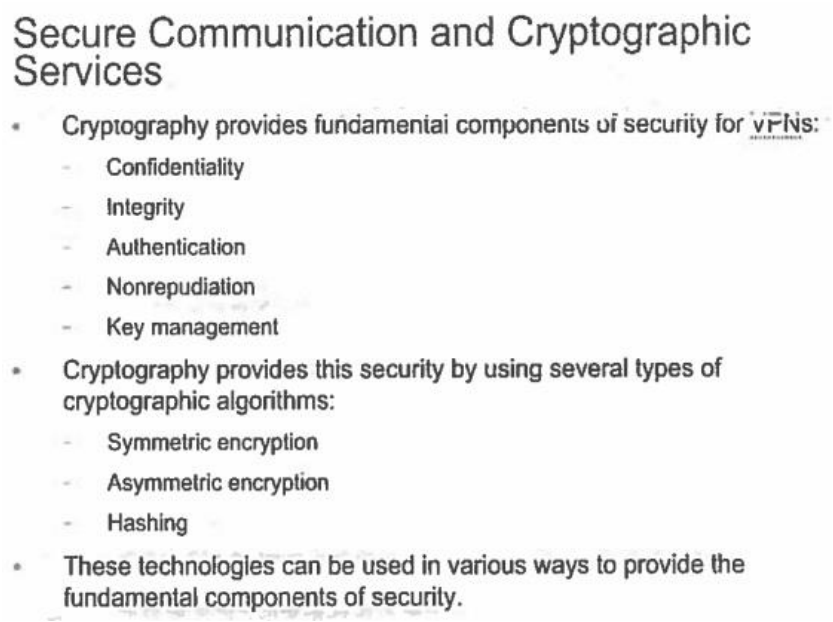
Key Management یعنی مدیریت کلید ها برای رمزنگاری دیتا.

Non-Repudiation جلوگیری از عدم انکار در انجام کاری. یعنی کسی نمی‌تواند انکار کند من این کار را انجام نداده ام در حالی که خودش این کار را انجام داده است. در ادامه این موارد را بصورت جزئی تر بررسی خواهیم کرد.

VPN Components

- Authentication
  - Device
  - User
- Encapsulation Method
- Data Encryption
- Packet Integrity
- Key Management
- Non-Repudiation
- Application and Protocol Support
- Address Management

دو پروتکل برای برقراری امنیت در VPN کاربرد بسیاری دارد. IPSEC و SSL. که هر کدام از آن‌ها از الگوریتم‌های Cryptography استفاده می‌کنند. در این بخش می خواهیم با الگوریتم های Cryptography آشنا شویم. کابردهای Cryptography بصورت زیر هستند که این کاربردها می‌توانند از وظایف VPN هم باشند.

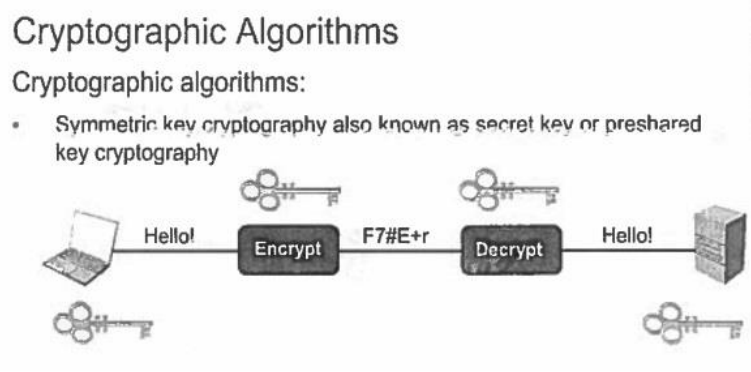


Confidentiality به معنای محرمانگی اطلاعات. یعنی دیتا بصورتی رمز شود تا کسی نتواند آن را شنود کند. **Integrity** به معنای جلوگیری از عدم جعل دیتا در طول مسیر. **Authentication** به معنای احراز هویت تا مطمن شویم شخص مقابل ما همان شخص مورد انتظار ما است. **Nonrepudiation** یعنی کسی نمی‌تواند انکار کند کاری را کرده اما ادعا کند من این کار را نکردم. **Key Management** یعنی مدیریت کلیدهایی که برای ایجاد و پیاده سازی در ارتباطات و امن سازی آن مورد استفاده قرار می‌گیرند.

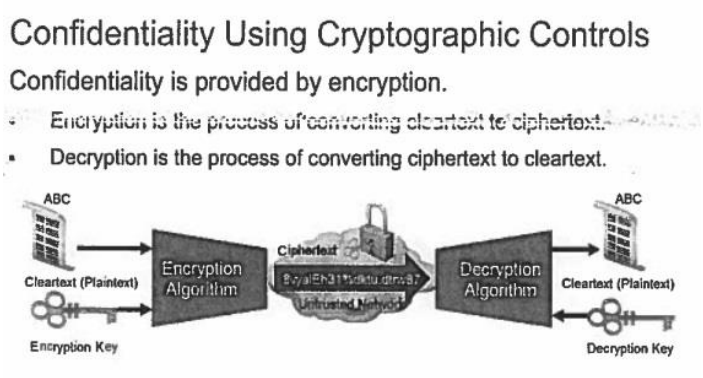
الگوریتم‌هایی Cryptography به سه دسته (Symmetric, Asymmetric, Hashing) تقسیم می‌شوند. تمام کابردهای Cryptography به واسطه سه الگوریتم فوق قابل پیاده سازی است. در روش **Symmetric Encryption** هر دو طرف ارتباط کلید یکسان و مشابه استفاده می‌کنند. در **Asymmetric Encryption** دو طرف ارتباط از کلید غیر مشابه و یا نامتقارن استفاده می‌کنند.

- **Symmetric Encryption**

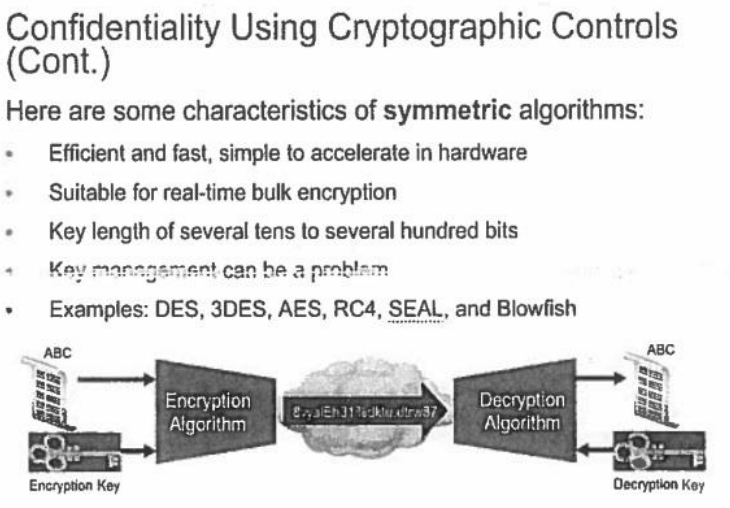
در Symmetric Encryption هر دو طرف ارتباط از کلید یکسان و مشابه استفاده می‌کنند. یعنی فرستنده اطلاعات و گیرنده اطلاعات روی یک کلید مشابه توافق می‌کنند و این کلید برای رمز نگاری و رمزگشایی مورد استفاده قرار می‌گیرد.. سه الگوریتم معروف در این روش DES, 3DES, AES می‌باشد.



مهمترین کاربرد Confidentiality در این الگوریتم می باشد. که فرستنده دیتا را رمز می‌کند و گیرنده دیتا را رمز گشایی می‌کند و هردو طرف با استفاده از یک کلید یکسان این کار را انجام می‌دهند.

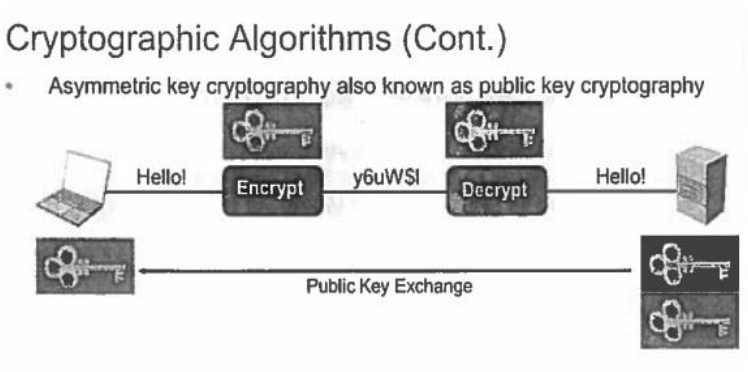


خصوصیاتی که الگوریتم های Symmetric دارند بصورت زیر است. اول اینکه بسیار سریع عمل می‌کنند. برای رمزنگاری دیتاهای حجیم بسیار خوب هستند. طول کلید نقش بسیار مهمی در بالابردن امنیت دارد یعنی هرچه طول کلید بزرگ تر باشد، امنیت آن بالاتر می‌باشد. چالش این روش انتقال این کلید مشابه به هردو طرف ارتباط است.

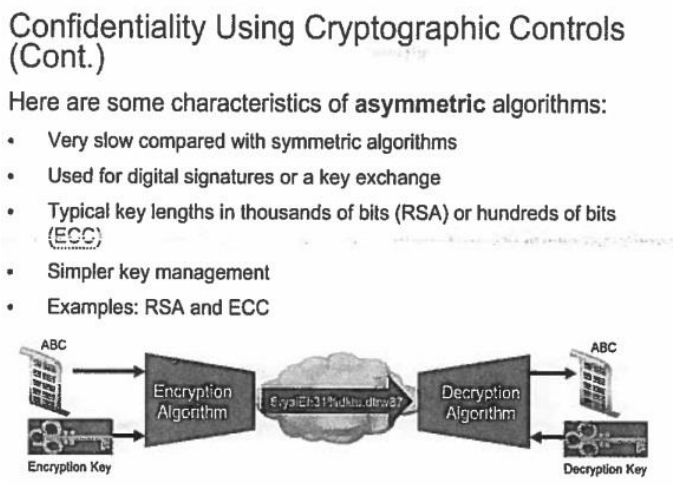


- **Asymmetric Encryption**

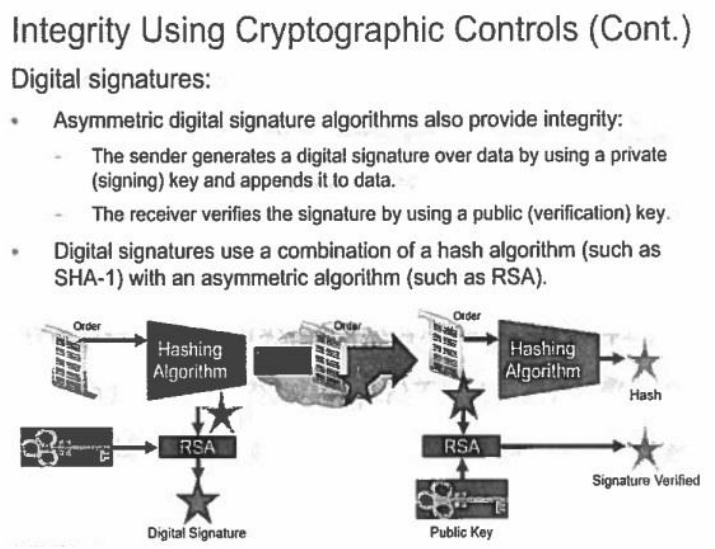
در Asymmetric Encryption دو طرف ارتباط از کلید غیر مشابه استفاده می‌کنند. در این روش هر کاربر دو کلید دارد. یکی Private Key و دیگری Public Key است. هر اطلاعاتی که با Public رمز شود فقط با همان Private باز می‌شود. و مکانیزم آن به این صورت است که هر طرف Public خود را در اختیار طرف مقابل قرار می‌دهد. تا طرف مقابل در صورت ارسال دیتا تمام دیتا را با همین کلید Public رمز کند و برای گیرنده ارسال کند. در این حالت چالش انتقال کلید به طرف مقابل را نداریم. الگوریتم هایی که در این روش کاربرد دارند RSA, DH می‌باشند.



Confidentiality در روش های Asymmetric هم کاربرد دارد. این روش بسیار کند عمل می‌کند.



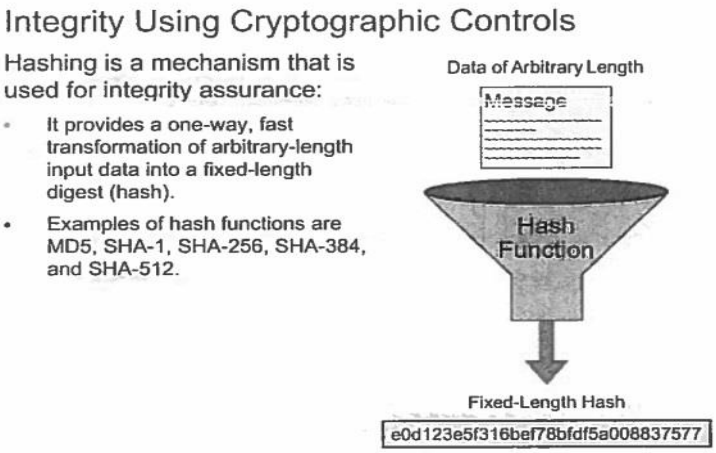
Integrity در روش های Asymmetric هم کاربرد دارد. اصطلاحا به آن امضای دیجیتال گفته می‌شود. به این صورت که دیتا را Hash می‌کنیم و Hash را با Private خودمان رمز می‌کنیم. و گیرنده دیتا را باز میکند و Hash را با Public ما باز می‌کند. و مطمین می‌شود که دیتا در طول مسیر تغییر نکرده، چرا که کلید Private ما را کسی ندارد. این روش Nonrepudiation یا عدم انکار را هم ایجاد می‌کند.



- **Hashing**

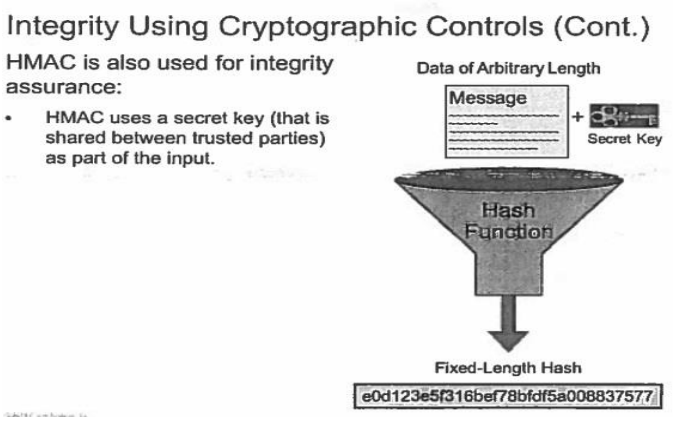
در این الگوریتم دیتا با هر سایزی که به آن داده شود یک خروجی با یک سایز ثابت را دریافت خواهید کرد. این پروسه یک فرآیند یک طرفه است. یعنی ما نمی‌توانیم از یک دیتای Hash شده دوباره به دیتای اصلی برسیم. در این الگوریتم کلیدی وجود ندارد. و دیتا وارد الگوریتمی شده و یک دیتا با سایز ثابت از آن بیرون می آید. از الگوریتم های Hashing می‌توان MD5, SHA1, SHA2, HMAC را نام برد.

ا زجمله کاربردهایی که Hashing دارد Integrity است. دیتا وارد الگوریتم می‌شود و یک Hash با مقدار ثابت دریافت می‌کنیم. و زمانی که دیتا را می‌خواهید ارسال کنید. این دیتا را همراه با Hash آن ارسال می‌کنید. اگر کسی در راه دیتا را تغییر دهد، گیرنده دیتا زمانی که دیتا را دوباره Hash می‌کند و با Hash همراه دیتا مقایسه می‌کند از تغییر دیتا در طول مسیر آگاه می‌شود. حال سوال اصلی اینجاس کسی که دیتا را تغییر دهد، حتما می‌تواند Hash دیتا را هم تغییر دهد. راه حل چیست؟



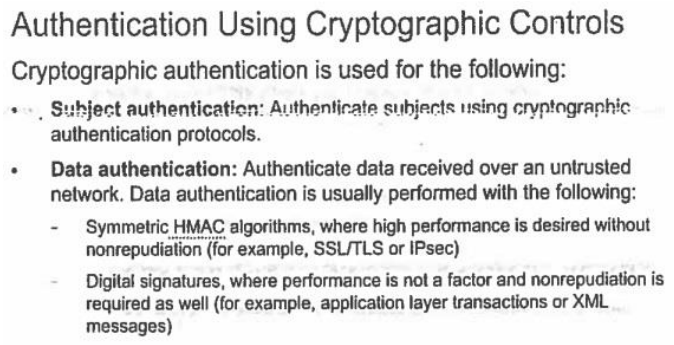
برای اینکه این مشکل حل شود، از راه حل HMAC استفاده می‌کنیم. به این صورت که دیتا را به تنهایی Hash نکنیم. به این صورت که دیتا را همراه با یک کلید Hash کنیم. تا در طول مسیر اگر کسی دیتا با Hash را تغییر داد، گیرنده اطلاعات متوجه می‌شود چرا زمانی که گیرنده دوباره دیتا را Hash می‌کند. همان Hash مورد نظر بدست نمی‌آید. در این حالت گیرنده به دو مسئله واقف می‌شود. یکی اینکه متوجه تغییر دیتا در مسیر می‌شود.

دوم اینکه از اصلی بودن فرستنده اطلاعات بخاطر استفاده از کلید اطمینان حاصل می‌کند. اما مشکل اینجاس که این دو طرف از همدیگر در امان نیستند چرا که کلید هردو طرف یکسان است. این مشکل در روش RSA یا امضای دیجیتال حل شده است.

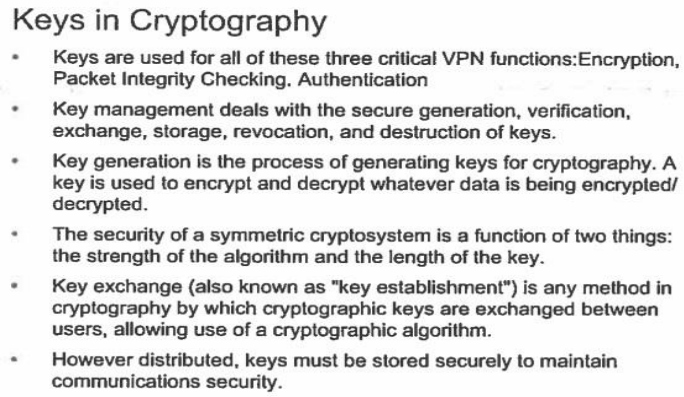


Authentication یا احراز هویت هم دو حالت دارد. که به صورت زیر هستند.

Subject Authentication یعنی مطمین می‌شوید، نفر مقابل همان شخص قبل انتظار است. که معمولا با یوزر نیم و پسورد قابل فهمیدن است.
Data Authentication یعنی مطمین شویم دیتا از همان جایی آمده است که ما انتظار آن را داریم.



یکی از اصلی ترین کارهایی که در Cryptography مطرح می‌شود، بحث مدیریت کلید است. معمولا کلید در تمام الگوریتم ها و روش ها مورد استفاده قرار می‌گیرد. Key Management مجموع فرآیندی است که ضامن امنیت کلید ما است. و سخت ترین مرحله در عملیات Cryptography مدیریت کلید می‌باشد.



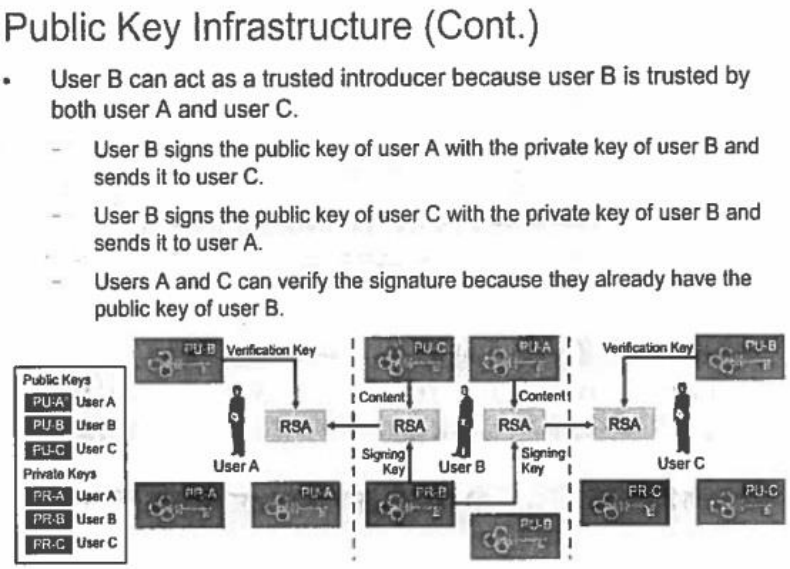
برای انتقال کلید معمولا روش های متفاوتی وجود دارد که به تفصیل زیر هستند.

Manual Key Exchange که این روش بصورت دستی کلید را جا به جا می‌کنیم. که معمولا این روش برای کلاینت های کم کاربرد دارد. و برای شبکه‌های بزرگ روش مناسبی نیست.

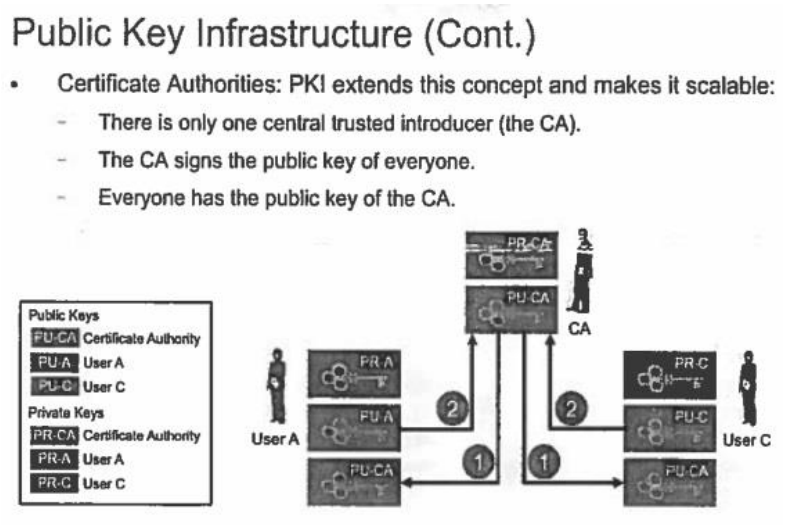
Diffie Hellman این روش معروف ترین روش مدیریت کلید می‌باشد. که یکی از الگوریتم های Asymmetric هم محسوب می‌شود.

Assymetric Encryption در این روش ما معمولا چالش انتقال کلید را نداریم. چرا که از دو کلید Private و Public استفاده می‌شود که کلید Private برای خودمان میماند و کلید Public را در اختیار بقیه قرار می‌دهیم. که این روش چالشی دارد به این صورت که کسی کلید Public خود را به دروغ بنام کس دیگری در اختیار ما قرار دهد. حال ما از کجا مطمین باشیم که این کلید Public همان کلید مورد نظر ما است. با استفاده از روش PKI این معضل حل خواهد شد.

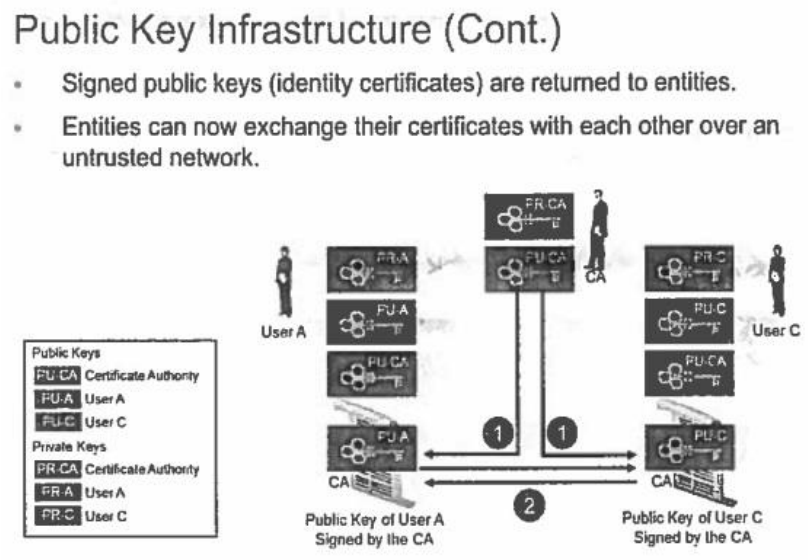
PKI یا Public Key Infrastructure این روش بستری را مهیا می‌کند که ما از دریافت کلید پابلیک مورد نظر اطمینان حاصل کنیم.. در شکل زیر یوزر A و C هرکدام یک کلید Public و Private دارند. و این دو طرف می‌خواهند پابلیک همدیگر را دریافت کنند و می‌خواهند مطمین باشند که پابلیک درست را دریافت کرده‌اند. مابین این دو یوزر B است که مورد اعتماد هردوی اینها است. که این یوزر هم کلید های پابلیک و پرایوت مخصوص خود را دارد. فرآیند به این صورت شروع می‌شود که هردو طرف کلید پابلیک خود را در اختیار یوزر B قرار می‌دهند. حال یوزر B پابلیک هرکدام را به همراه اسم هر کدام گرفته و Hash میکند و Hash بدست آمده را به همراه کلید Private خود امضا می‌کند. و بعد آن را تحت عنوان یک Certificate تحویل هرکدام از طرفین می‌دهد.



تمام کارهای فوق توسط CA یا Certificate Authority انجام می‌شود. که ما CA های معتبری در دنیا داریم که همه به آنها اعتماد دارند.



بعد از اتمام مراحل فوق طرفین ارتباط می توانند سرتیفیکیت به دست آمده را در اختیار یک دیگر قرار دهند و از دریافت کلید پابلیک اصلی هم مطمین شوند.



فیلد هایی که در یک سرتیفیکیت معمول است بصورت زیر است:

Public Key Infrastructure (Cont.)

The table contains examples of the information that is in an identity certificate.

Field	Value
Certificate Format Version	Version 3
Certificate Serial Number	12457801
Signature Algorithm Identifier for CA	RSA with SHA-1
Issuer X.500 Name	C = US O = Cisco CN = CA
Validity Period	Start = 04/01/10 Expire = 04/01/15
Subject X.500 Name	C = US O = Cisco CN = CCMCluster001
Subject Public Key Information	756ECE0C9ADC7140...

Public Key Infrastructure (Cont.)

Field	Value
Extension(s) (v3):	
CRL Distribution Points	URL = http://crl.CA.com/CACRL.crl
CA Signature	2C086C7FE0B6E90DA396AB...

اگر سرتیفیکیتی قبل از زمان اعتبار خود فاش شود و یا تهدید شود آن را Revoke میکنند یعنی از رده خارج می‌کنند. و دیگر مدار اعتبار نمی‌باشد.

ما سه روش خارج کردن سرتیفیکت ها را داریم که بصورت زیر هستند.

Public Key Infrastructure (Cont.)

CRLs	OCSP	AAA Server Certificate Authorization
A list of revoked certificate serial numbers distributed as a time-stamped, CA-signed file	Revocation information is immediately pushed to an online database	Proprietary Cisco technology that is an alternative to OCSP
PKI entities regularly poll the CRL repository to receive the current CRL	Entities can query the OCSP server at any time to check for validity of the received certificate	Entities can query the AAA server at any time to check for validity of the received certificate
A window of opportunity for the attacker while the new CRL is not yet propagated	Not widely deployed	Not integrated with the PKI—requires a separate authorization database

که روش اول بسیار زمان گیر است و روش دوم بسیار سریع تر و بهتر عمل می‌کند. البته روش دوم هنوز مورد استفاده عموم قرار نگرفته است. روش های زیر روش های نسل جدید برای Encryption هستند.

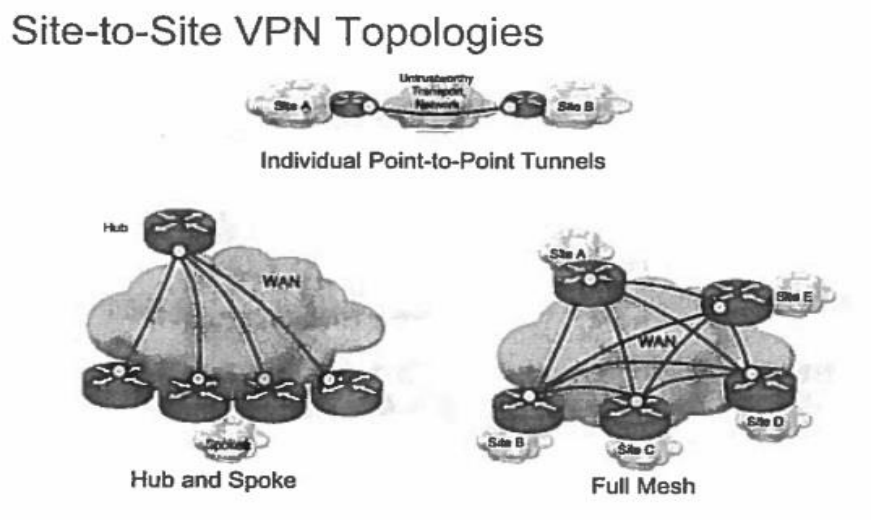
Next-Generation Encryption

- Some older algorithms (and key sizes) do not provide adequate protection from modern threats.
- NGE provides security and scalability requirements for the next two decades (AES-GCM mode, SHA-2, ECDH-384, ECDSA-384).

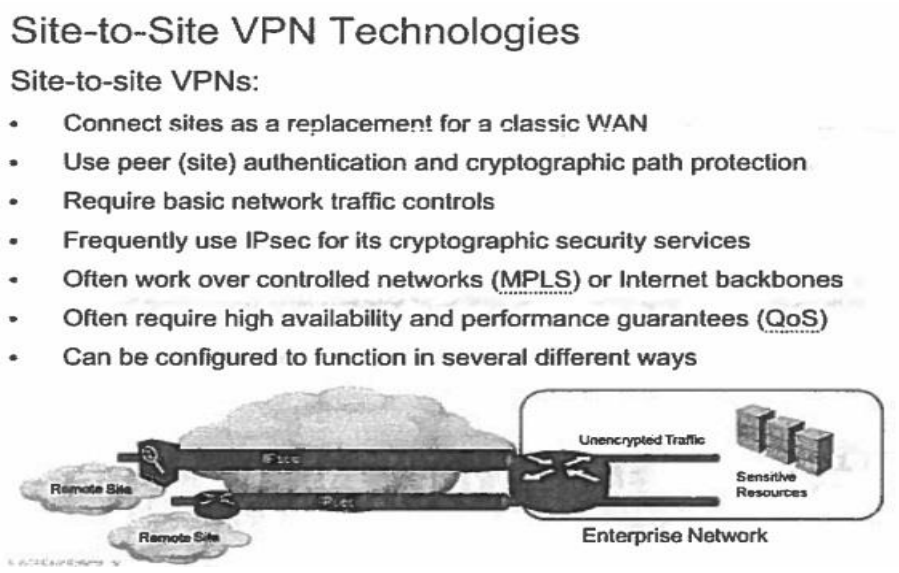
یکی از انواع VPN ها Site-to-Site است. که میتواند دو نقطه را به هم وصل کند. تنها پروتکلی که در این نوع VPN کار می‌کند، IPSEC است. اما به شیوه های مختلفی میتوان این پروتکل را پیاده سازی کرد. مثلا:

IPSEC With Crypto Map, IPSEC With VTI, GRE over IPSEC, Get VPN, DMVPN, Flex VPN

انواع توپولوژی هایی که در Site-to-Site قابل پیاده سازی است بصورت زیر می‌باشد. یکی حالت Hub and Spoke و دیگری حالت Full Mesh است.

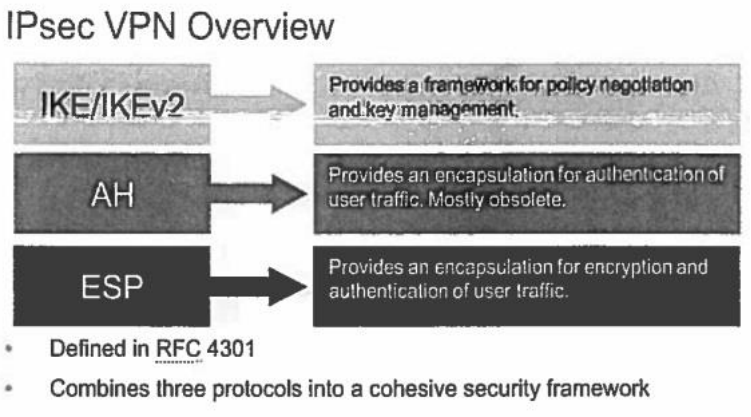


تکنولوژی هایی که در Site-to-Site مورد استفاده قرار می‌گیرند معمولا در بستر MPLS قابل پیاده سازی هستند. در هنگام پیاده سازی VPN ها به سه موضوع Multicast, Redanduncy, QOS دقت زیادی داشته باشید.



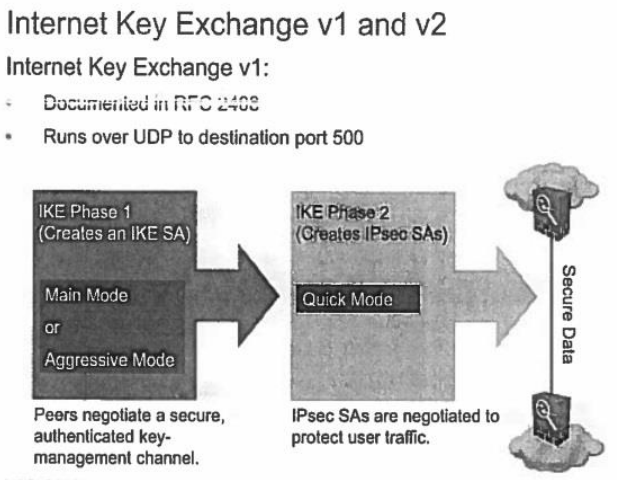
توافقات امنیتی که قبل از برقراری ارتباط ما بین دو طرف برقرار می‌شود توسط IKE یا Internet Key Exchange انجام می‌شود. مثلا دو طرف روی کلید رمزنگاری، روی نوعیت الگوریتم ها و خیلی مسایل دیگر باهم توافق می‌کنند. و پروسه توافقات را اصطلاحا SA یا Security

Association میگویند. از دیگر کارهایی که در پروتکل IKE انجام میشود Key Exchange است. IKE دارای دو ورژن می باشد. که ما معمولا از ورژن یک آن استفاده می‌کنیم. البته که ورژن دو آن مزایای بیشتری دارد. پروتکل IKE از پروتکل های درونی دیگری استفاده می‌کند. که انواع آن ISAKMP, Oaklay, Skeme می‌باشد. بعد از مرحله توافقات امنیتی، حال IPSEC مشخص می‌کند که از کدام پروتکل می‌خواهد استفاده کند. که دو پروتکل را در اختیار دارد. یکی AH و دیگری ESP. تفاوت این دو در این است که AH فقط ارتباط را Authenticate میکند اما ESP علاوه بر آن Encrypt هم می‌کند.



IPSEC برای Encryption دو حالت یا Mode دارد. یکی Transport و دیگری Tunnel. زمانی که ارتباطات شما برقرار است و شما صرفا می‌خواهید ارتباطات خود را امن کنید از حالت Transport استفاده می‌کنید. و زمانی که که هیچ ارتباطی ندارید و می‌خواهید توسط IPSEC هم ارتباط ایجاد کنید و هم ارتباط را امن کنید از حالت Tunnel استفاده می‌کنید.

IKEv1 برای انجام توافقات و برقراری ارتباطات دو فاز دارد. که بصورت زیر است. که فاز اول به دو صورت قابل پیاده سازی است یکی Main Mode و دیگری Aggressive Mode. که حالت Main کار های خود را با شش پکت انجام می‌دهد و حالت Aggressive کارهای خود را با چهار پکت انجام می‌دهد. که حالت Main قوی تر است. و فاز دوم هم دو حالت دارد یکی Quick Mode و دیگری GDOI است. که ما معمولا از حالت Quick Mode استفاده می‌کنیم.



شکل زیر جزئیات بهتری در مورد فرآیند های IKE به مام نمایش می‌دهد.

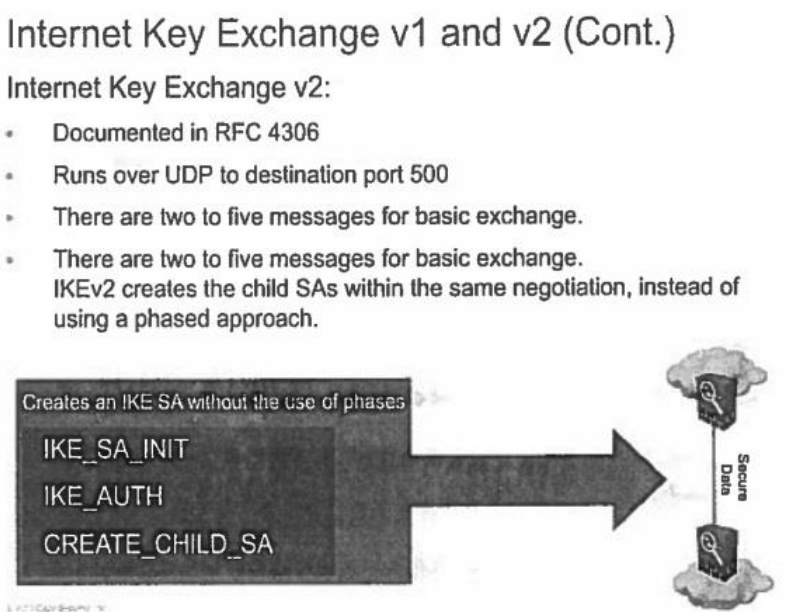
IKE Phase 1 (IKE SA)
authentication (pre-shared autehntication key, certificate) (secure)
symmetric encryption key exchange (secure)
Security Association (Authentication, DH, encryption, hashing)

IKE Phase 2 (secure) (IPSec SA)
Security Association (AH:md5, sha1 / ESP:des/3des/aes, md5/sha1)
key exchange (optional): perfect security or PFS

IPSEC (AH/ESP)

IKE
IKE Phase 1 (main mode or aggressive mode)
IKE Phase 2 (quick mode or GDOI)
IPSEC

شکل زیر خصوصیات و ویژگی های IKEv2 را نمایش می‌دهد.



Internet Key Exchange v1 and v2 (Cont.)

Internet Key Exchange v2 (cont.):

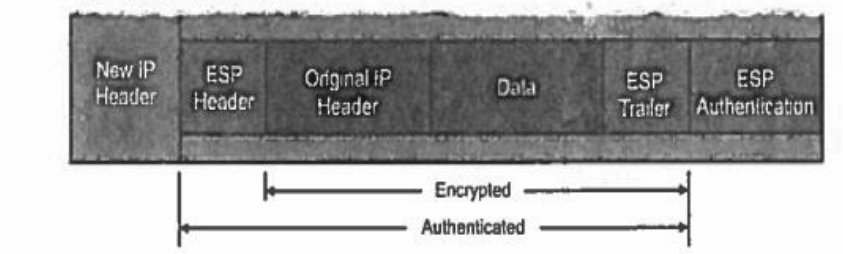
- Is defined in one RFC (RFC 4306)
- Uses a cookie mechanism to prevent DoS attacks from forged source addresses
- Requires fewer round-trip exchanges compared to IKEv1
- Has built-in DPD
- Has built-in configuration payload and user authentication mode (EAP)
- Uses unidirectional authentication methods
- Has built-in NAT traversal
- Provides better rekeying and collision handling

شکل زیر شیوه Encapsulation در پروتکل ESP را نمایش می‌دهد.

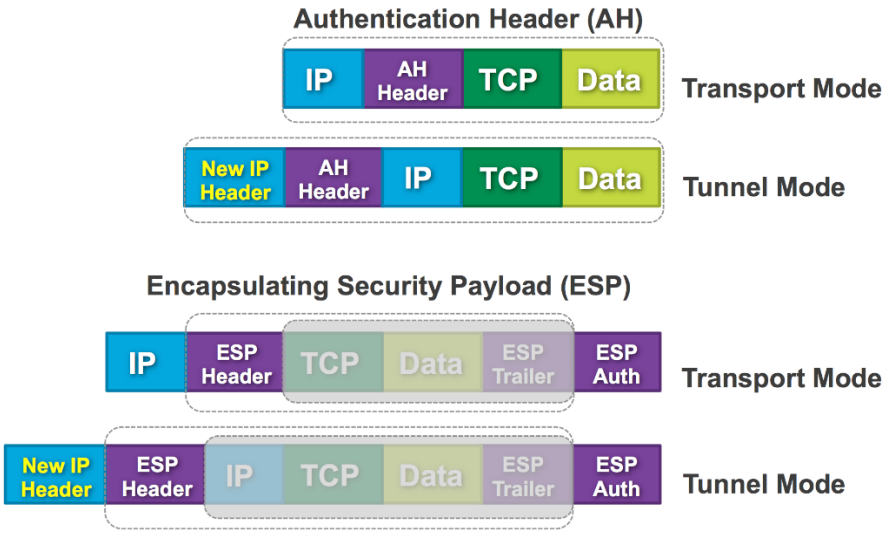
Encapsulating Security Payload

RFC 4303, IP protocol 50

Tunnel Mode ESP



Header پروتکل AH و ESP در حالت Transport Mode و Tunnel Mode بصورت زیر است.



Header پروتکل AH با جزئیات بیشتر بصورت زیر است:

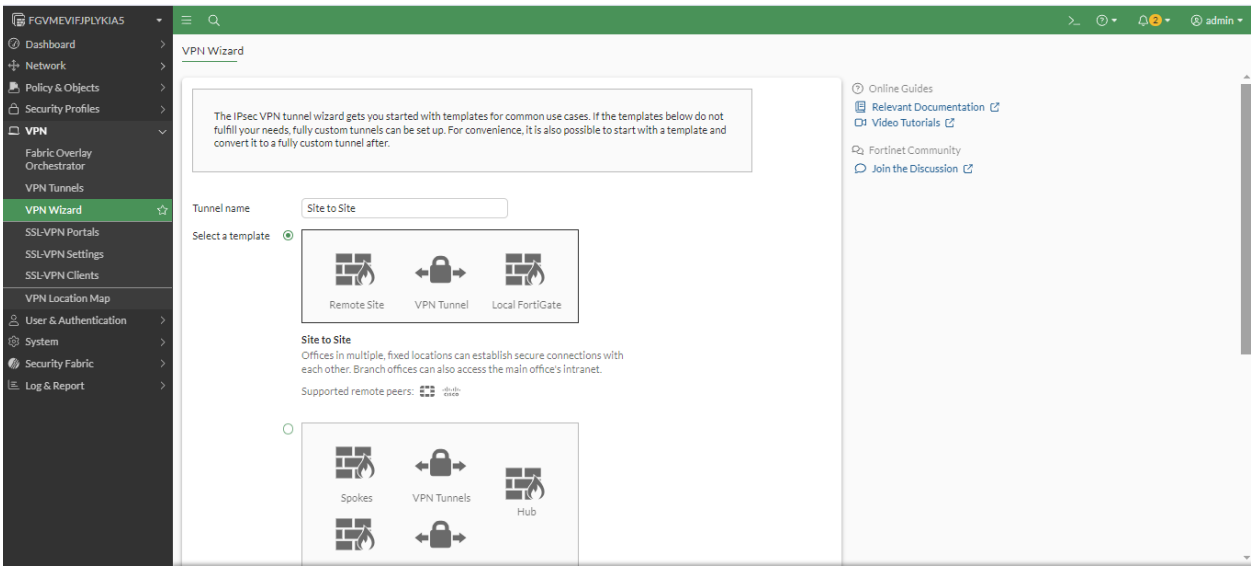
Authentication Header format																															
Offsets	$Octet_{16}$	0								1								2								3					
$Octet_{16}$	Bit_{10}	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Next Header								Payload Len								Reserved															
4	32	Security Parameters Index (SPI)																															
8	64	Sequence Number																															
C	96	Integrity Check Value (ICV)																															
...	...	...																															

Header پروتکل ESP با جزئیات بیشتر بصورت زیر است:

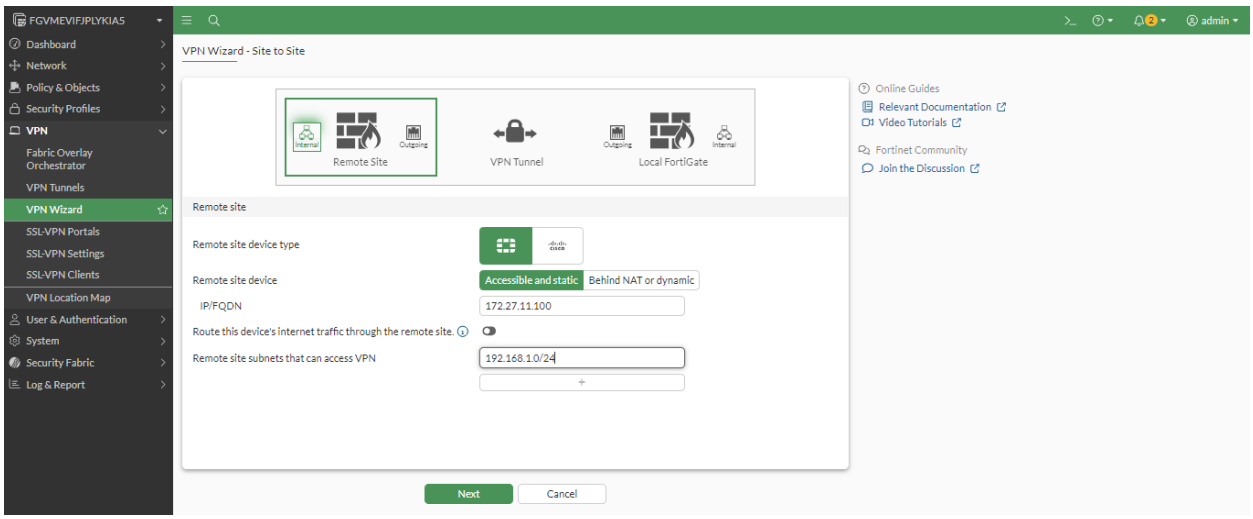
Encapsulating Security Payload format																															
Offsets	$Octet_{16}$	0								1								2								3					
$Octet_{16}$	Bit_{10}	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Security Parameters Index (SPI)																															
4	32	Sequence Number																															
8	64	Payload data																															
...	...																																
...	...									Padding (0-255 octets)																							
...	...																																
...	...																	Pad Length								Next Header						
...	...	Integrity Check Value (ICV)																															
...	...	...																															

12.1 Site to Site VPN with IPSEC

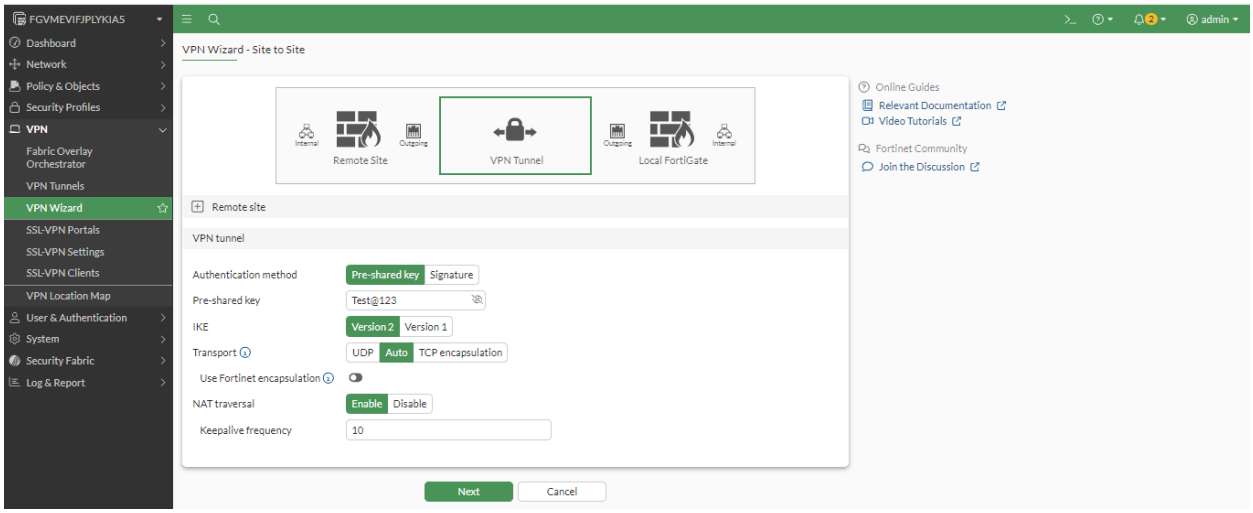
با این قابلیت می‌توانید دو سایت مختلف را توسط فایروال فورتیگیت در بستر IPSEC به یکدیگر متصل کنید. برای این کار وارد منوی VPN > VPN Wizard می‌شویم. در مرحله اول، گزینه Site to Site را انتخاب می‌کنیم. در ادامه گزینه‌های دیگر را بررسی می‌کنیم.



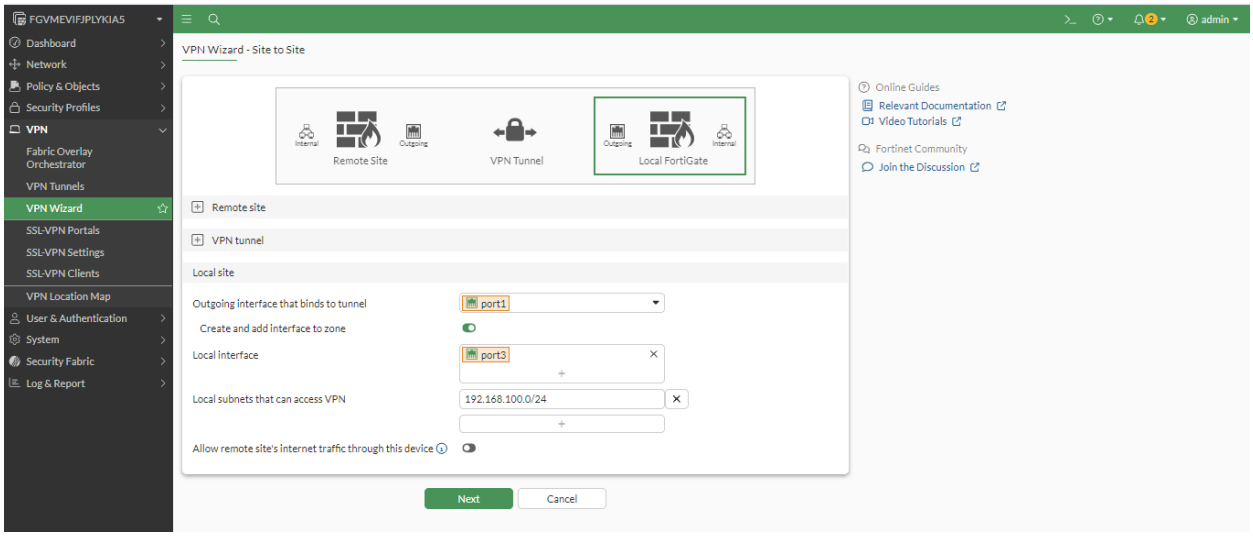
در مرحله دوم، مشخص می‌کنیم که سایت مقابل آی‌پی استاتیک دارد و یا پشت NAT قرار گرفته است. اگر سایت مقابل آی‌پی پابلیک استاتیک داشت، آن را در قسمت IP/FQDN وارد می‌کنیم. در قسمت آخر، رنج شبکه در مقصد که قصد داریم از طریق VPN آن را ببینیم را مشخص می‌کنیم. یعنی رنج شبکه محلی طرف مقابل را وارد می‌کنیم.



در مرحله سوم، مشخص می‌کنیم که روش احراز هویت بر اساس کلید باشد و یا بر اساس امضا. بهتر است قابلیت NAT Traversal را فعال نگه داریم. ورژن IKE بهتر است روی ورژن ۲ باشد.



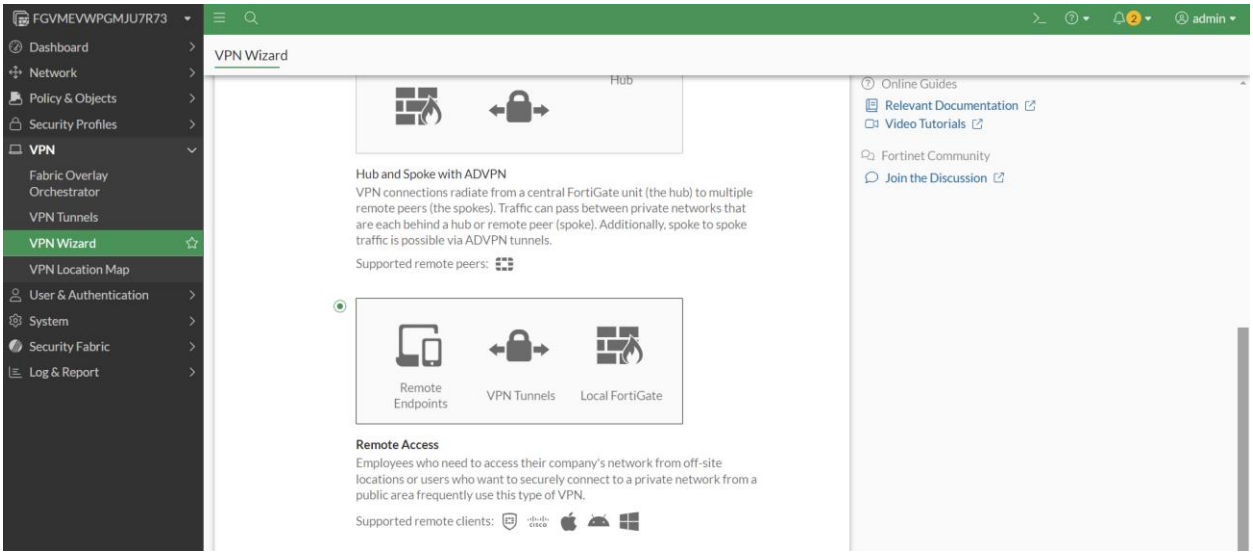
در مرحله چهارم، پورت خروجی یا WAN و پورت ورودی و یا LAN را تعیین می‌کنیم. و در آخر رنج شبکه داخلی مربوط به خودمان را مشخص می‌کنیم تا ترافیک آن‌ها اجازه عبور روی VPN را داشته باشد.



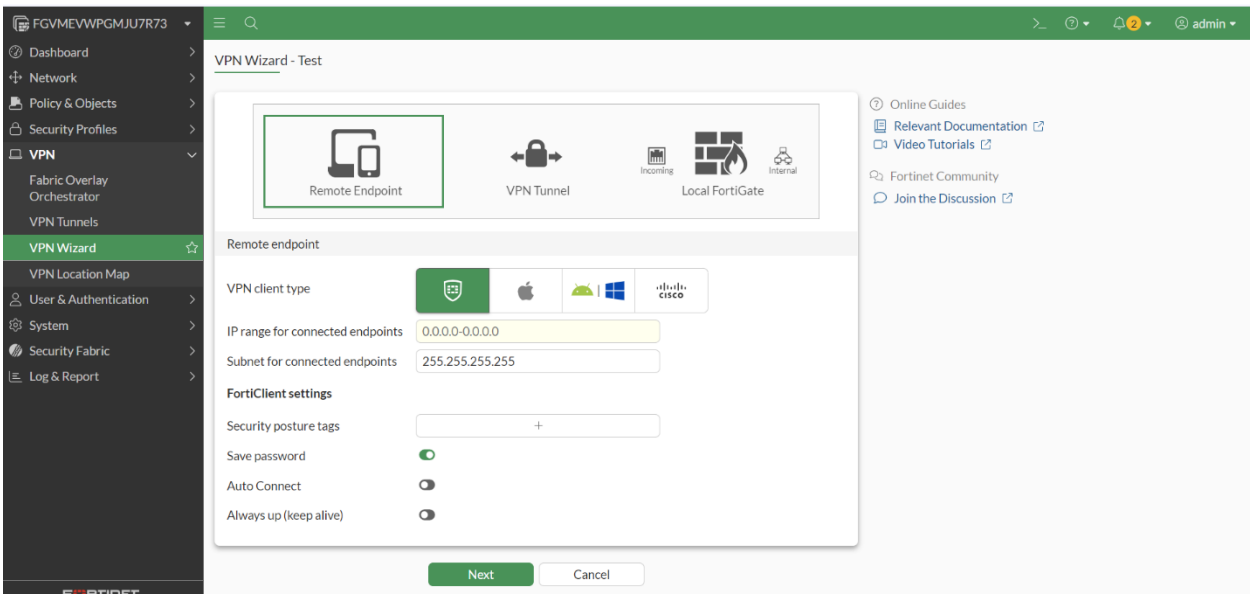
حال اگر وارد بخش Policy ها و Static Route ها شویم. میبینیم که به ازای VPN ما تنظیمات بصورت اتوماتیک ایجاد می‌شود. در نهایت در سایت مقابل، برعکس این تنظیمات را اعمال می‌کنیم. نکته مهم دیگر اینکه تا زمانی که ترافیکی بین دو سایت ارسال و دریافت نشود، تانل فعال نمی‌شود.

12.2 Remote Access VPN with IPSEC

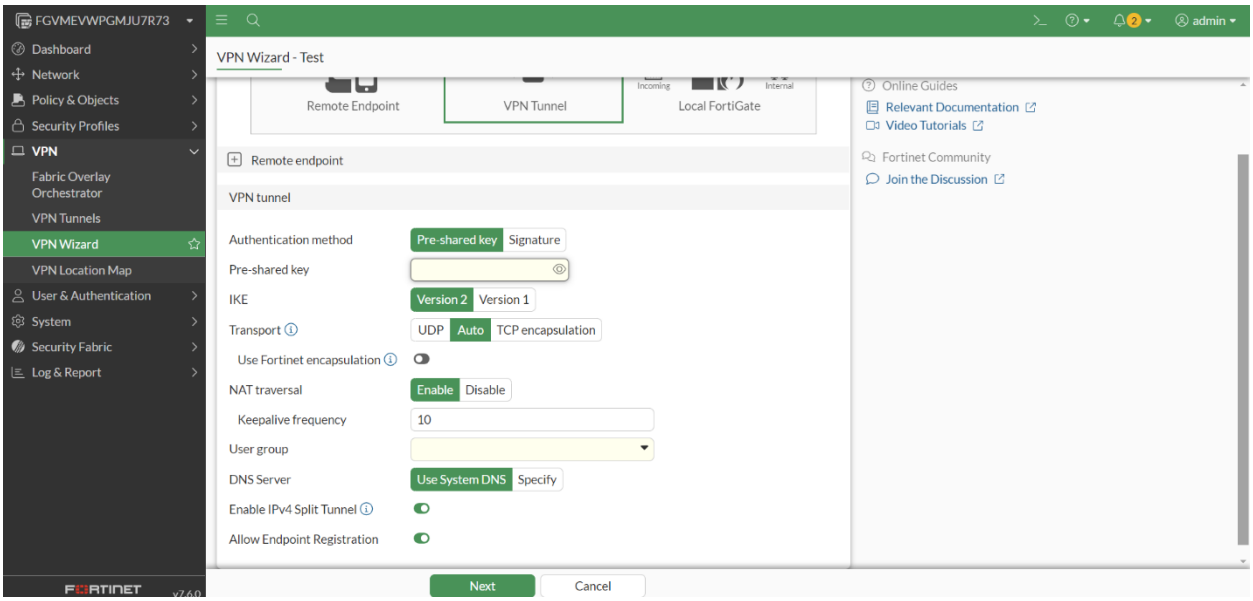
با این قابلیت کاربران می‌توانند به فایروال متصل شوند. و از امکانات شبکه داخلی استفاده کنند. قبل از انجام این سناریو حتما نرم افزار FortiClient را نصب کنید. برای تنظیم روی فایروال، وارد منوی VPN > VPN Wizard می‌شویم و گزینه Remote access را انتخاب می‌کنیم.



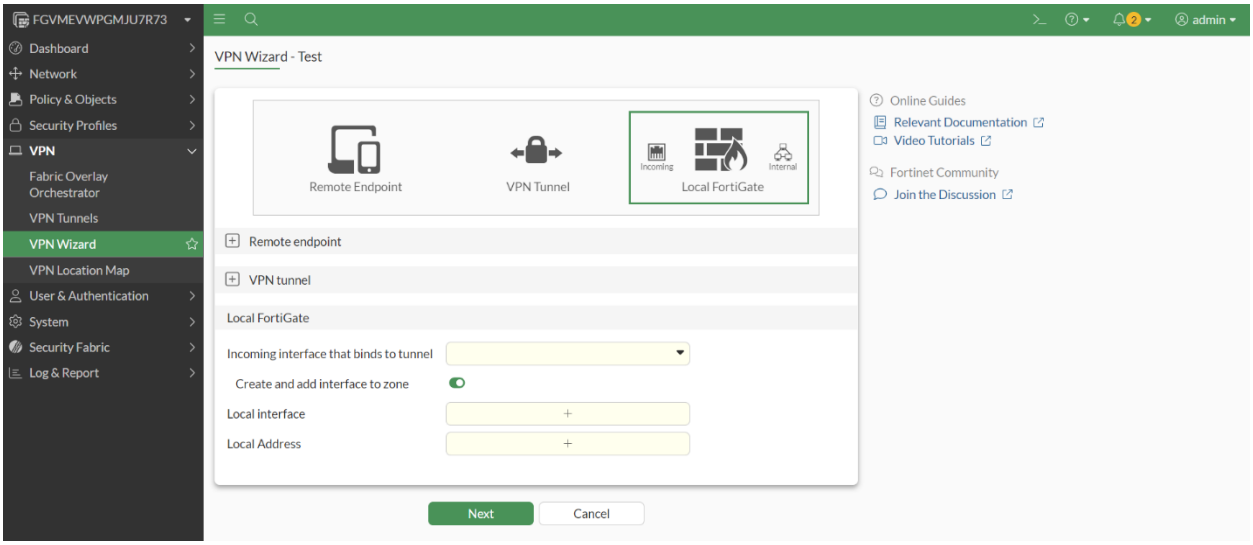
در مرحله دوم، نوع VPN Client را انتخاب می‌کنیم. در قسمت دوم، رنج آی‌پی که به کاربران VPN اختصاص می‌دهید را مشخص می‌کنید. این رنج دلخواه است و بهتر است در رنج شبکه نباشد. مثلا 192.168.100.1-192.168.100.100 با مسک 255.255.255.0 .



در مرحله سوم، مهمترین گزینه‌ها این است که یک کلید تعریف کنید و در ادامه گروهی از کاربران که اجازه وصل شدن با VPN را دارند، مشخص می‌کنیم. بقیه گزینه‌ها بهتر است بصورت پیشفرض باقی بمانند.



در مرحله آخر، اینترفیسی که VPN روی آن وصل می‌شود، یعنی اینترفیس خروجی را انتخاب می‌کنیم. در قسمت بعد اینترفیس داخلی که کاربران قرار است به آن دسترسی داشته باشند را مشخص می‌کنیم. و در نهایت رنج آی‌پی که کاربران قرار است در شبکه داخلی به آن دسترسی داشته باشند را مشخص می‌کنیم. منظور همان اینترفیس و رنج شبکه داخلی است.

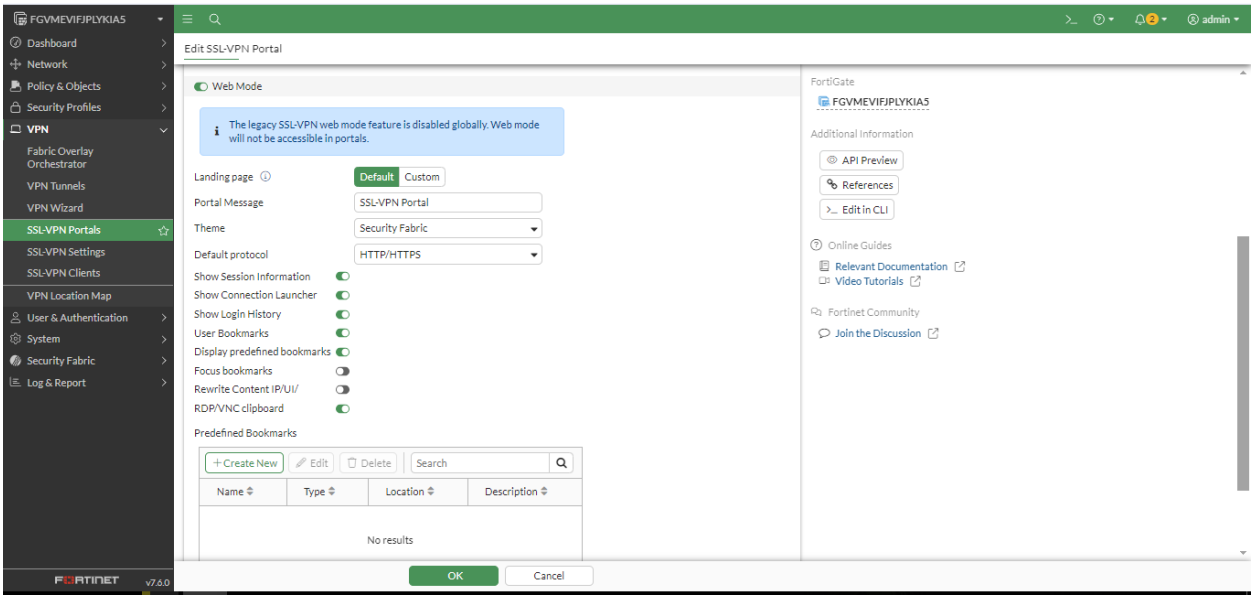


در نهایت خود فایروال Policy های مربوطه و Route های مربوطه را بصورت اتوماتیک ایجاد می‌کند.

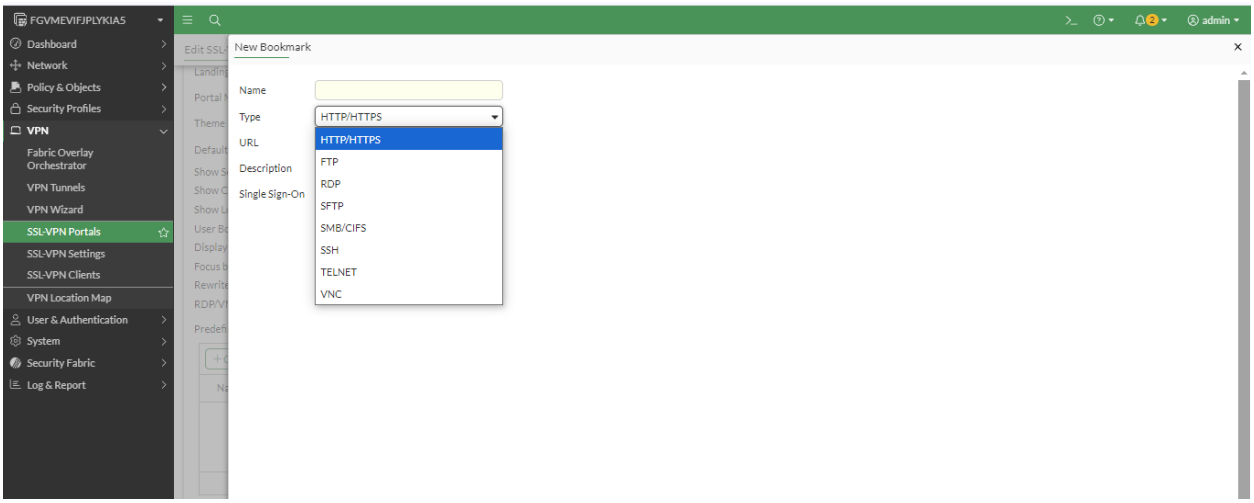
12.3 Remote Access VPN with Web Based SSL

برای استفاده از VPN SSL دو روش Web و Tunnel وجود دارد. که در این بخش روش Web را پیاده سازی می‌کنیم. نکته اینجاست که این روش یک سری محدودیت‌هایی دارد و ممکن است برخی از اپلیکیشن‌ها بصورت وب کار نکنند. مثلا پروتکل‌هایی مثل HTTP, HTTPS, FTP, Ping, به خوبی با این روش سازگار هستند. اما در روش Tunnel نرم افزاری سمت کلاینت نصب می‌شود و هیچ گونه محدودیتی در این روش نداریم.

برای پیاده سازی اگر وارد منوی VPN > SSL VPN Portal شویم. بصورت پیشفرض یک پروفایل Full Access ایجاد شده است. هر پروفایلی که ایجاد می‌کنیم از دو بخش Tunnel mode و Web mode تشکیل شده است. بخش Web شامل تنظیمات زیر است:

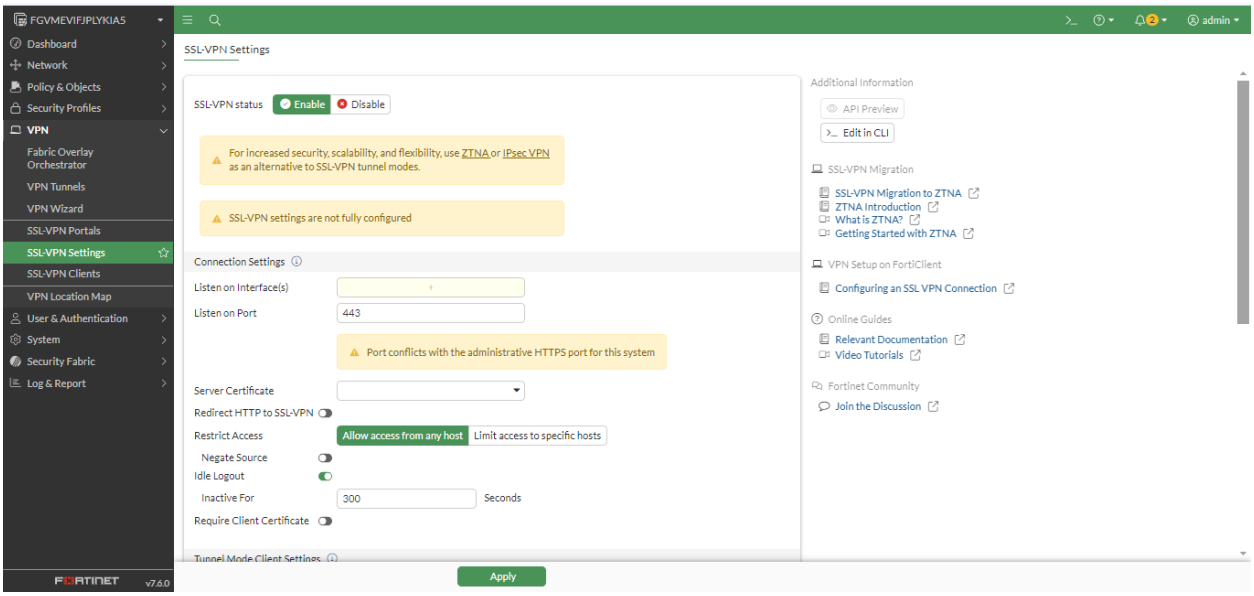


اگر روی گزینه Create New را بزنیم می‌توانیم یک سری موارد را bookmark کنیم، تا زمانی که کاربر وارد پورتال خود می‌شود، این موارد را ببیند و از آن استفاده کند.

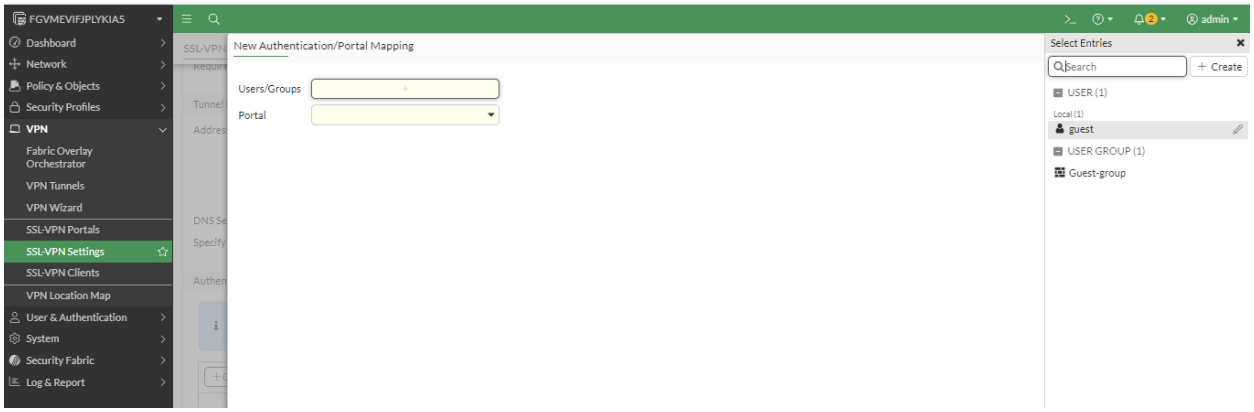


حال وارد منوی VPN > SSL VPN Settings می‌شویم و تنظیمات کلی برای SSL را انجام می‌دهیم. مثلا مشخص می‌کنیم که روی کدام اینترفیس کاربران بتوانند، پورتال را ببینند. که معمولا اینترفیس WAN را باید انتخاب کنیم. تا کاربران از بیرون به پورتال متصل شوند. پورت 443 با خود فایروال conflict دارد و باید یک پورت دیگر را انتخاب کنیم. مثلا پورت 4433.

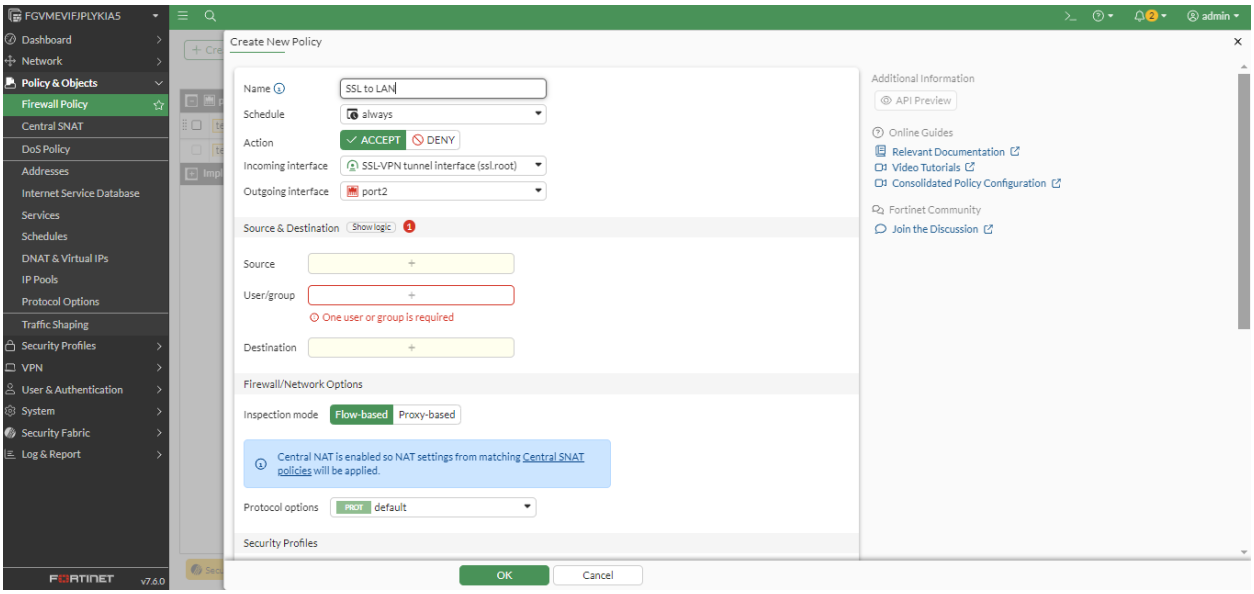
قسمت وسط برای تنظیمات Tunnel mode است.



و در قسمت آخر آن مشخص می‌کنیم که کدام یوزر به کدام پورتال دسترسی داشته باشد.

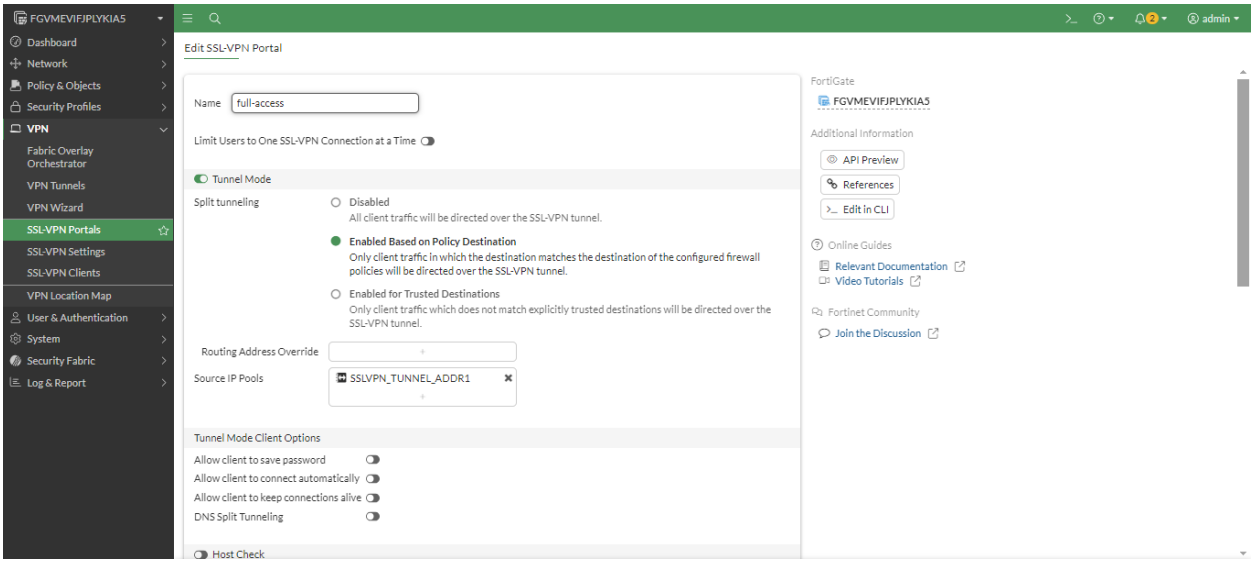


بعد از تنظیم این بخش، حتما باید یک Firewall Policy ایجاد کنیم. و ترافیک اینترفیس SSL VPN را به داخل Accept کنیم.


FGVMEVIFJPLYKIA5
admin
Dashboard
Network
Policy & Objects
Firewall Policy
Central SNAT
DoS Policy
Addresses
Internet Service Database
Services
Schedules
DNAT & Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
System
Security Fabric
Log & Report
FORTINET
v7.6.0
Create New Policy
Name
SSL to LAN
Schedule
always
Action
ACCEPT
DENY
Incoming interface
SSL-VPN tunnel interface (ssl.root)
Outgoing interface
port2
Source & Destination
Show logic
Source
User/group
One user or group is required
Destination
Firewall/Network Options
Inspection mode
Flow-based
Proxy-based
Central NAT is enabled so NAT settings from matching Central SNAT policies will be applied.
Protocol options
PROT
default
Security Profiles
OK
Cancel
Additional Information
API Preview
Online Guides
Relevant Documentation
Video Tutorials
Consolidated Policy Configuration
Fortinet Community
Join the Discussion

12.4 Remote Access VPN with Tunnel Based SSL

در این روش کاربران محدودیتی به دسترسی به سرویس‌های داخلی از بیرون ندارند و از همه پروتکل‌ها می‌توانند استفاده کنند. برای پیاده سازی این بخش اگر وارد منوی VPN > SSL VPN Portal شویم. بصورت پیشفرض یک پروفایل Full Access ایجاد شده است. هر پروفایلی که ایجاد می‌کنیم از دو بخش Tunnel mode و Web mode تشکیل شده است. بخش Tunnel شامل تنظیمات زیر است:



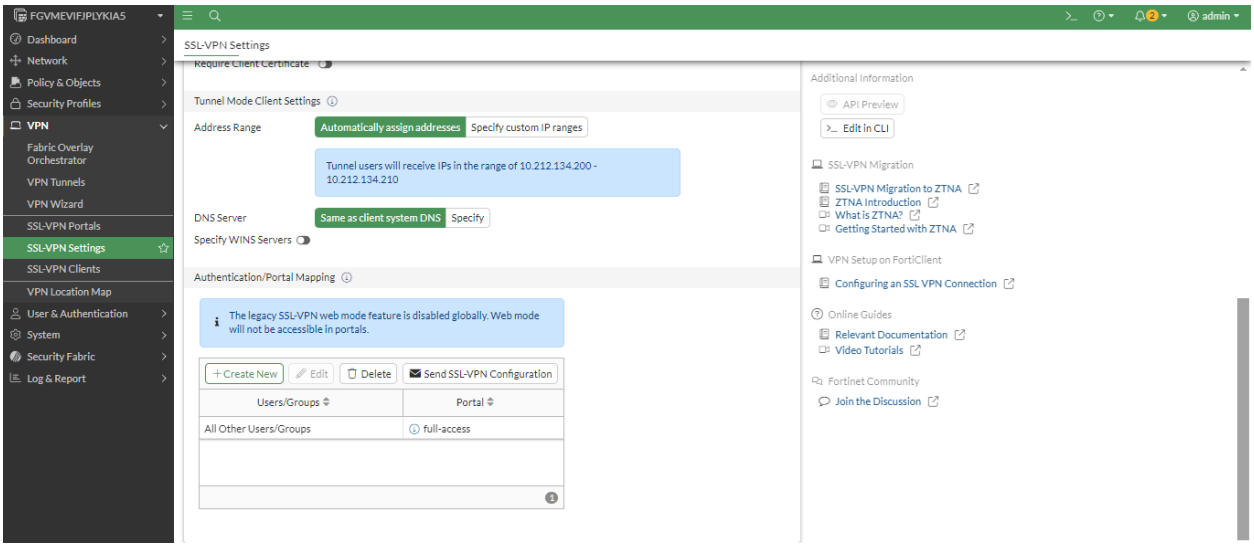
در قسمت اول مشخص می‌کنیم که ترافیک شبکه LAN ما روی VPN قرار بگیرد و اجازه دسترسی به آن داشته باشیم. پس در قسمت Routing Address Overrides رنج شبکه داخلی را مشخص می‌کنیم. چهار گزینه زیر را می‌توانیم Allow کنیم. مثلا می‌توانیم اجازه دهیم تا کاربران هنگام وصل شدن نام کاربری و رمز عبور را ذخیره کنند و یا بصورت اتوماتیک به VPN متصل شوند.

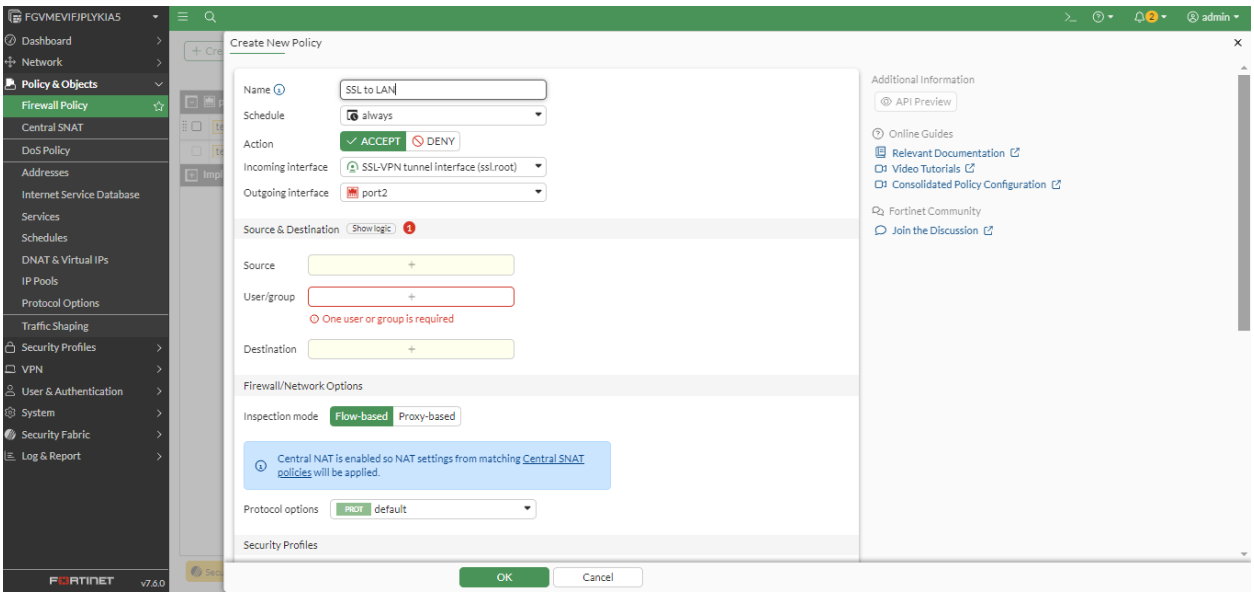
در ادامه وارد منوی VPN > SSL VPN Settings می‌شویم و تنظیمات کلی را برای SSL را انجام می‌دهیم. مثلا مشخص می‌کنیم که روی کدام اینترفیس کاربران بتوانند، پورتال را ببینند. که معمولا اینترفیس WAN را باید انتخاب کنیم. تا کاربران از بیرون به پورتال متصل شوند. در قسمت بعد پورت 443 با خود فایروال conflict دارد و باید یک پورت دیگر را انتخاب کنیم. مثلا پورت 4433. کاربران هروقت می‌خواهند وارد پورتال خود شوند باید پورت 4433 را حتما وارد کنند. مثلا 10.10.10.10:4433 .

قسمت میانی برای تنظیمات Tunnel mode است. که باید یک رنج آی‌پی، برای کاربرانی که این طریق متصل می‌شوند را مشخص کنیم. همچنان در ادامه باید برای هر یوزر پورتال او را مشخص کنیم یعنی هر یوزر به چه پورتالی اجازه اتصال دارد.

نکات مهم:

- بعد از تنظیم این بخش، حتما باید یک Firewall Policy ایجاد کنیم. و ترافیک اینترفیس SSL VPN را به داخل Accept کنیم.
- بعد از ورود به پورتال کاربر می‌تواند نرم افزار Forti Client VPN را دانلود و نصب کند.
- ممکن است در هنگام اتصال VPN کاربر با پیغام Please Turn off IE Security مواجه شود. کاربر باید در تنظیمات IE روی سیستم‌عامل خود این قابلیت را خاموش کند. در غیر این صورت با خطا مواجه می‌شود.


FGVMEVIFJPLYKIA5
admin
Dashboard
Network
Policy & Objects
Security Profiles
VPN
Fabric Overlay Orchestrator
VPN Tunnels
VPN Wizard
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Clients
VPN Location Map
User & Authentication
System
Security Fabric
Log & Report
SSL-VPN Settings
Require Client Certificate
Tunnel Mode Client Settings
Address Range
Automatically assign addresses
Specify custom IP ranges
Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210
DNS Server
Same as client system DNS
Specify
Specify WINS Servers
Authentication/Portal Mapping
The legacy SSL-VPN web mode feature is disabled globally. Web mode will not be accessible in portals.
Create New
Edit
Delete
Send SSL-VPN Configuration
Users/Groups
Portal
All Other Users/Groups
full-access
Additional Information
API Preview
Edit in CLI
SSL-VPN Migration
SSL-VPN Migration to ZTNA
ZTNA Introduction
What is ZTNA?
Getting Started with ZTNA
VPN Setup on FortiClient
Configuring an SSL VPN Connection
Online Guides
Relevant Documentation
Video Tutorials
Fortinet Community
Join the Discussion

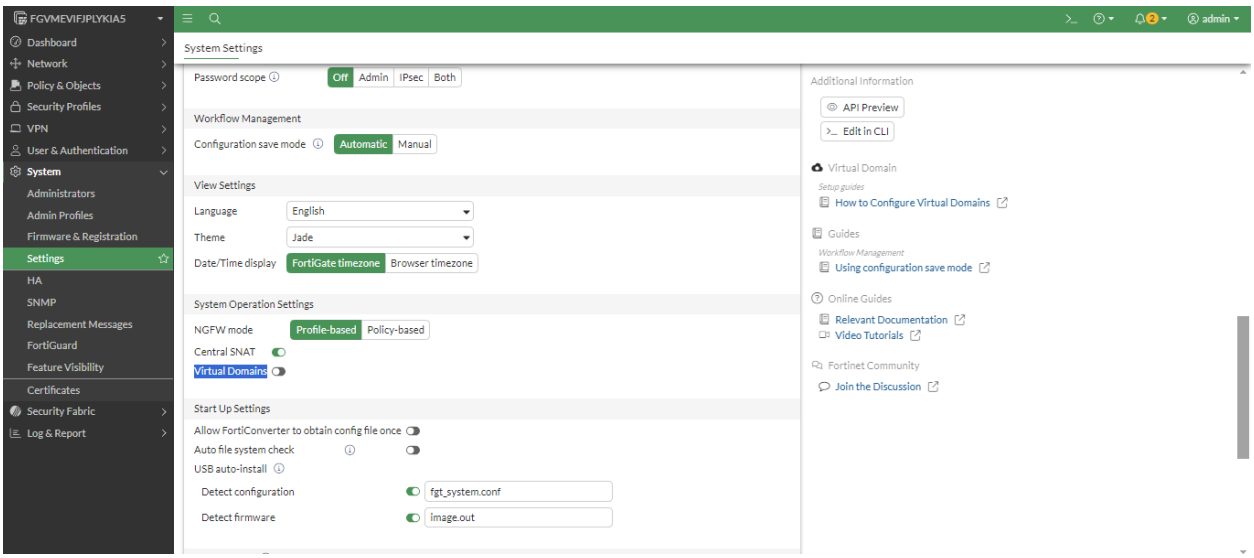

FGVMEVIFJPLYKIA5
admin
Dashboard
Network
Policy & Objects
Firewall Policy
Central SNAT
DoS Policy
Addresses
Internet Service Database
Services
Schedules
DNAT & Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
User & Authentication
System
Security Fabric
Log & Report
FORTINET
v7.6.0
Create New Policy
Name
SSL to LAN
Schedule
always
Action
ACCEPT
DENY
Incoming interface
SSL-VPN tunnel interface (ssl.root)
Outgoing interface
port2
Source & Destination
Show logic
Source
User/group
One user or group is required
Destination
Firewall/Network Options
Inspection mode
Flow-based
Proxy-based
Central NAT is enabled so NAT settings from matching Central SNAT policies will be applied.
Protocol options
PROT
default
Security Profiles
OK
Cancel
Additional Information
API Preview
Online Guides
Relevant Documentation
Video Tutorials
Consolidated Policy Configuration
Fortinet Community
Join the Discussion

13 Virtual Domains (VDOM)

در فورتیگیت، این قابلیت به ما اجازه می‌دهد تا یک فایروال فیزیکی را به چند فایروال Virtual تبدیل کنیم. اما دقت کنید که تعداد فایروال‌های مجازی نباید بصورتی باشد که با محدودیت منابع سخت افزاری در فایروال مواجه شویم. با این قابلیت می‌توانید از این فایروال در چندین قسمت شبکه استفاده کنید. مثلا بین شبکه داخلی و اینترنت. بین شبکه داخلی و دیتاسنتر.

بعد از اینکه این قابلیت را ایجاد کردیم، فایروال یک محیط Global و یک محیط برای فایروال مجازی ما ایجاد خواهد کرد. ما می‌توانیم روی یک فایروال چندین VDOM را داشته باشیم. محیط Global، محلی که بصورت متمرکز می‌توانیم VDOM های مختلف را مدیریت کنیم. یعنی آن‌ها را حذف یا اضافه کنیم و یا اینترفیس‌هایی را به هر VDOM متصل کنیم.

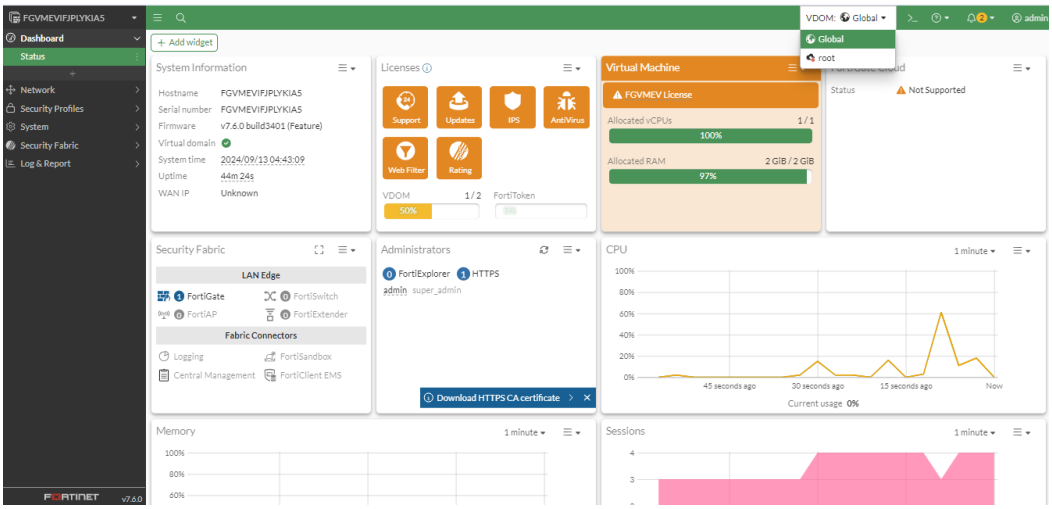
به دو صورت گرافیکی و خط فرمان می‌توانیم VDOM را فعال کنیم. بصورت گرافیکی وارد منوی System > Setting می‌شویم و گزینه Virtual Domain را فعال می‌کنیم.



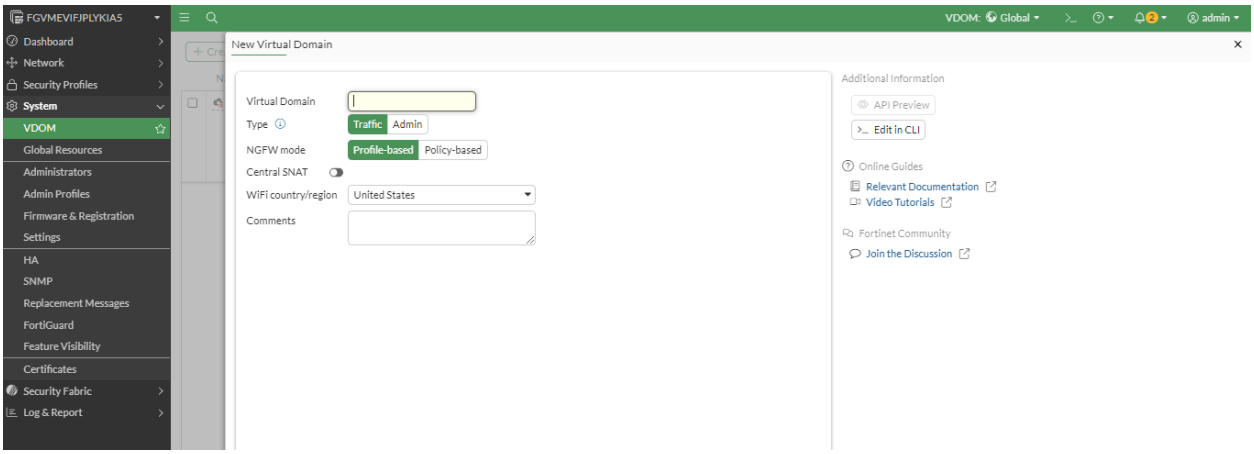
با دستورات زیر در خط فرمان فایروال می‌توانیم VDOM را فعال کنیم.

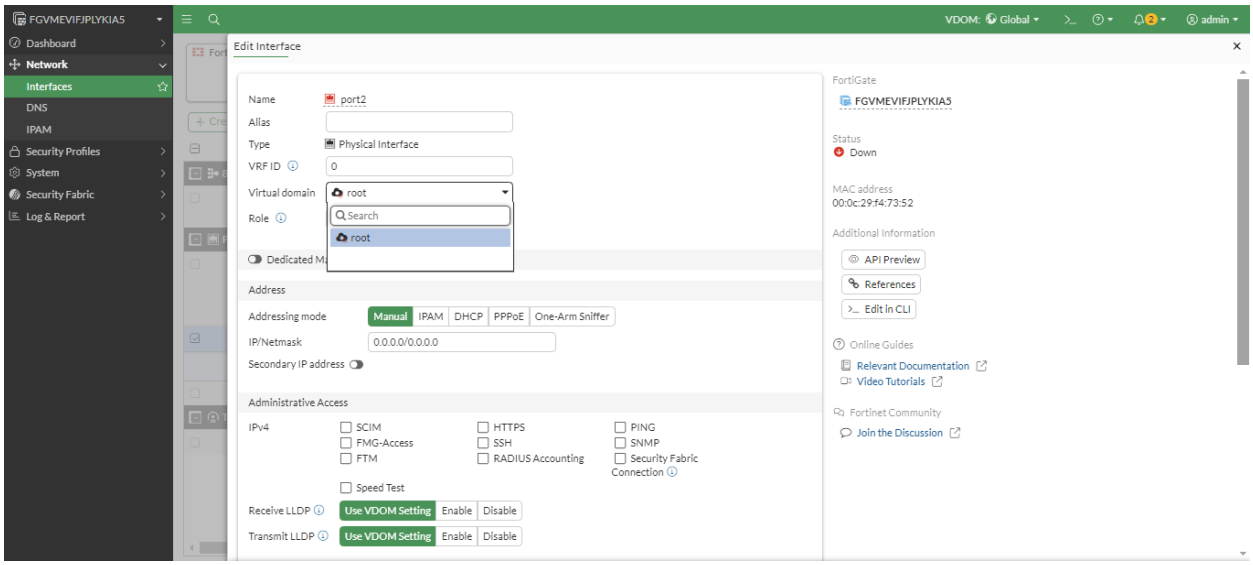
```
Config system global
Set vdom-mode multi-vdom
End
```

بعد از وارد کردن دستورات یک بار از فایروال خارج می‌شوید و دوباره وارد شوید. وقتی وارد می‌شوید یک VDOM بصورت گلوبال ایجاد می‌شود که به ما قابلیت مدیریت VDOM ها را می‌دهد. و یک VDOM به نام root هم ایجاد می‌شود، که تمام تنظیمات فعلی فایروال، به root VDOM انتقال پیدا می‌کند.

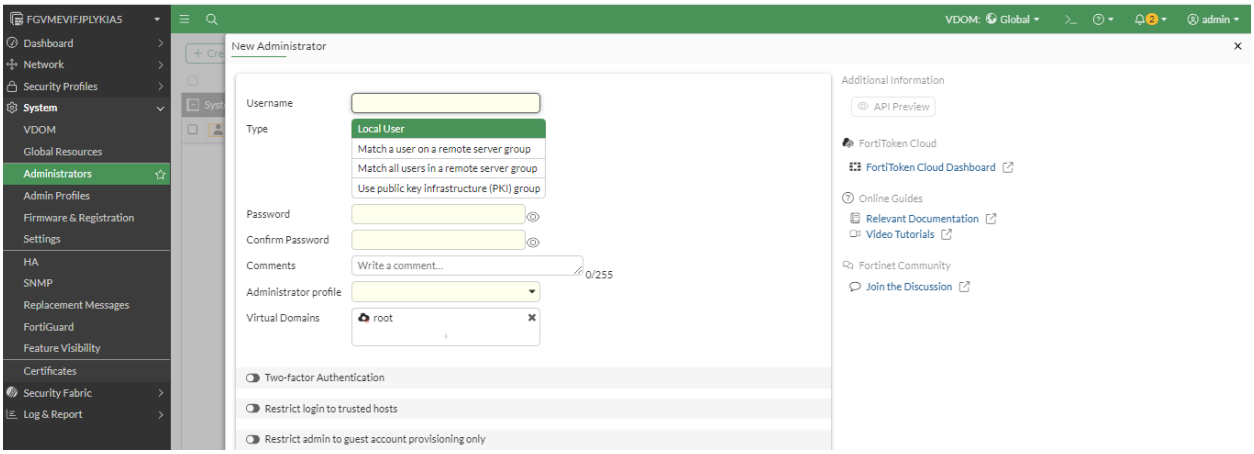


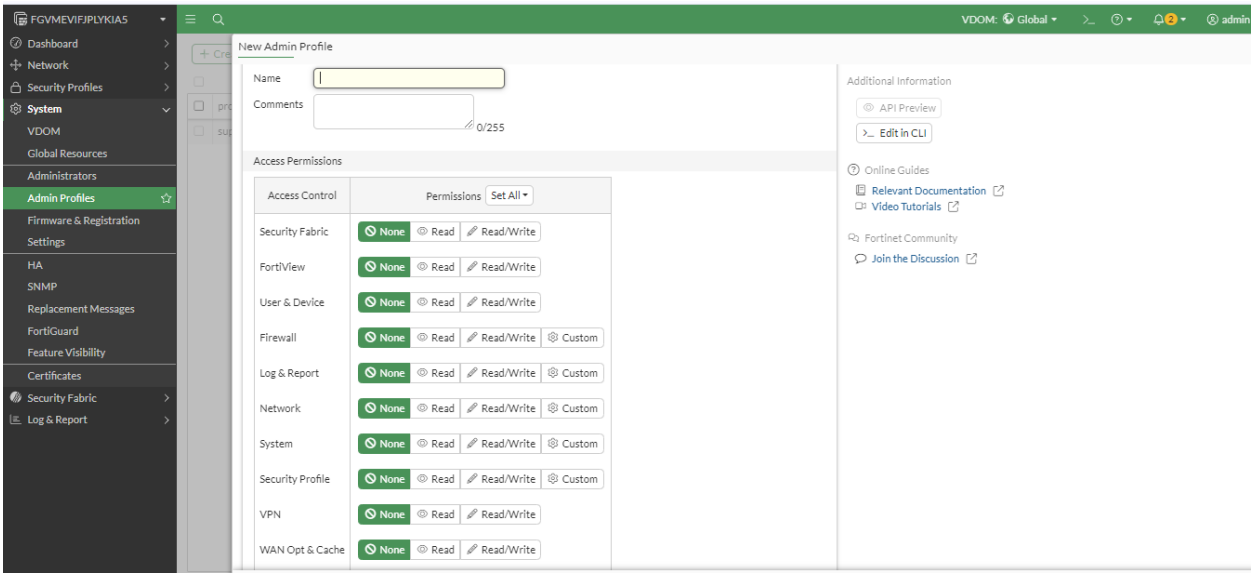
اگر وارد منوی System > VDOM شویم. می‌توانیم یک VDOM جدید بسازیم. در ادامه اگر وارد اینترفیس‌ها شویم، می‌توانیم هر اینترفیس را به یک VDOM مشخص انتصاب دهیم.



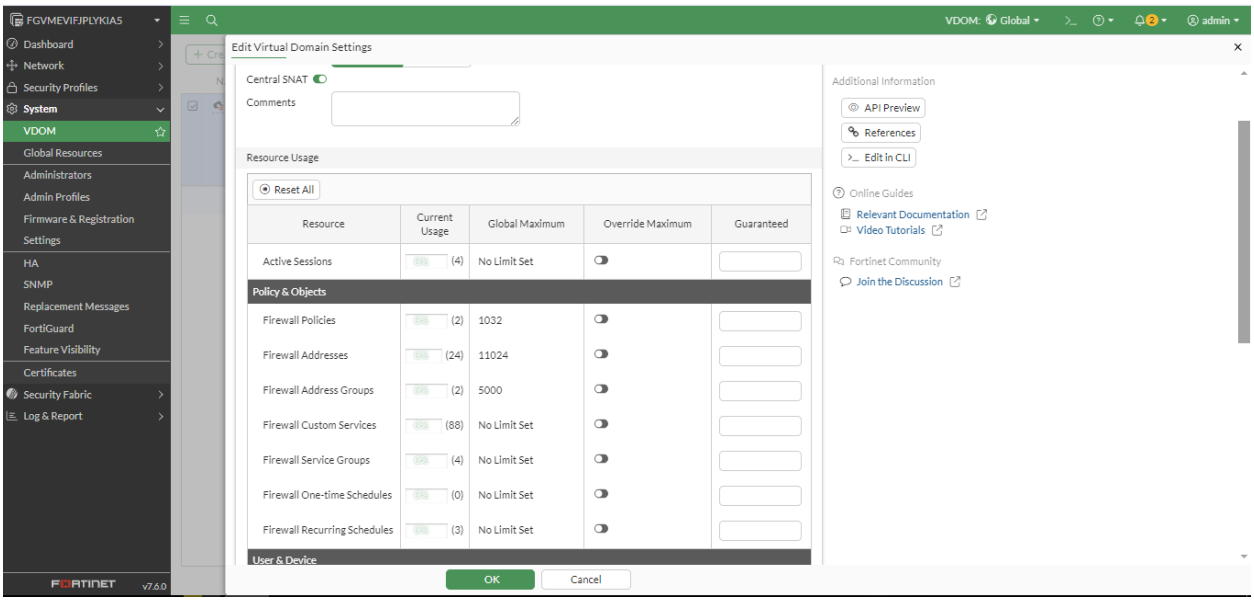


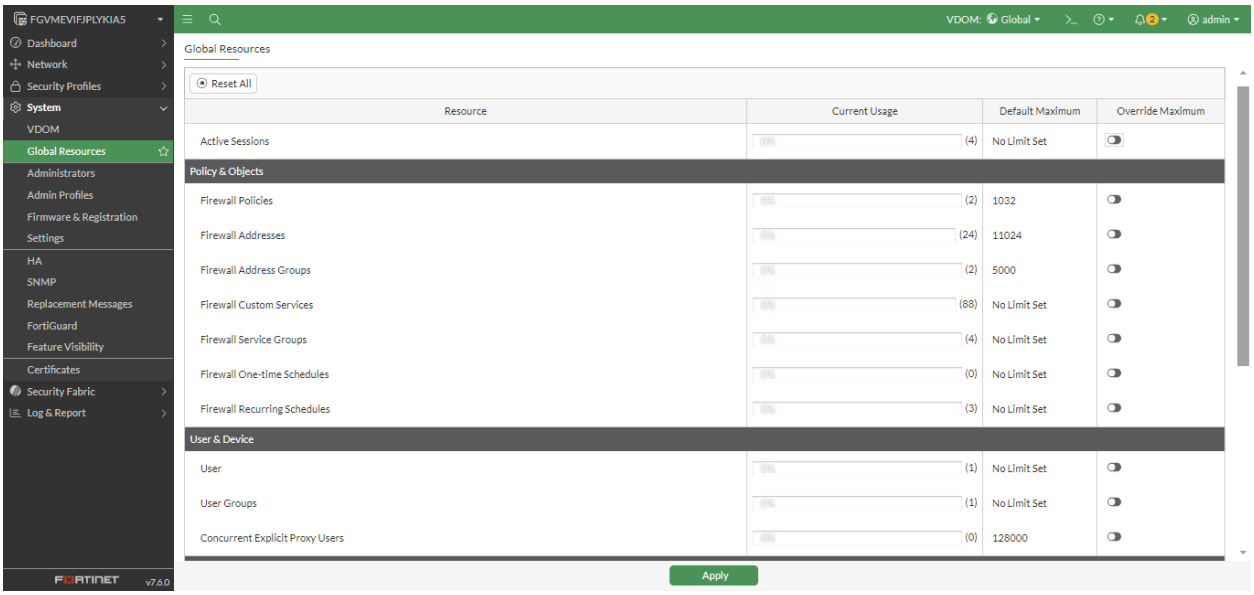
نکته مهم دیگری که می‌توانیم در نظر بگیریم این است که، ممکن است ما بخواهیم مدیریت هر فایروال مجازی ایجاد شده را به شخصی بدهیم. پس دسترسی این افراد به VDOM ها باید متفاوت باشد. برای این کار باید ادمین‌های مختلفی ایجاد کنیم. پس وارد منوی System > Administrator می‌شویم. و یک نام کاربری جدید ایجاد می‌کنیم. در ادامه مشخص می‌کنیم که عضو چه پروفایلی و VDOM ای باشد. دقت کنید که تنظیمات Admin Profiles در این بخش مشخص می‌کند که این یوزر به چه بخش‌هایی دسترسی دارد و یا ندارد.





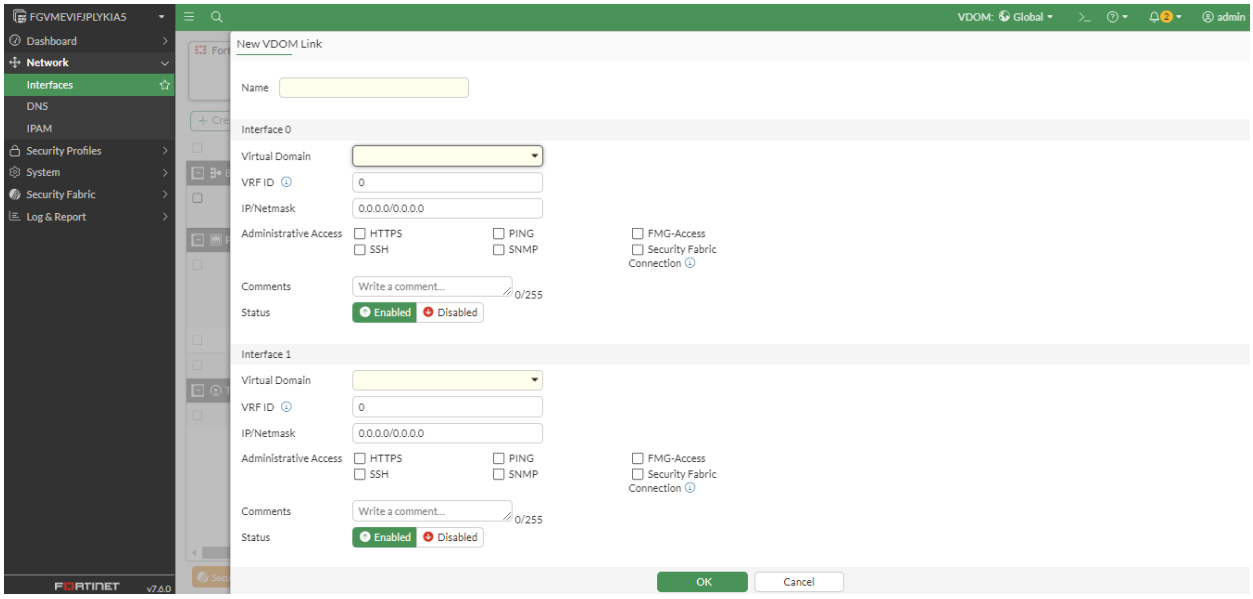
یکی دیگر از مواردی که می‌توانید برای هر VDOM مشخص کنید، میزان منابع سخت افزاری است که در اختیار هر VDOM می‌توانیم قرار دهیم. البته این محدودیت را به این صورت می‌توانیم مشخص کنیم که مثلا، هر VDOM بتواند حداکثر 100 پالیسی را ایجاد کند. یا مثلا حداکثر بتواند 20 یوزر را برای خود ایجاد کند. برای این کار هم می‌توانید از منوی System > VDOM وارد VDOM مربوطه شوید و این مقادیر را مشخص کنید. یا اینکه وارد منوی System > Global Resource شوید و تنظیمات کلی را ایجاد کنید تا هر VDOM به همین اندازه در فایروال سهمیه داشته باشد.





نکته مهم دیگر اینکه می‌توانید در قسمت Security Profile ها، پروفایل‌هایی را ایجاد کنید که بصورت گلوبال، همه VDOM ها بتوانند از آن استفاده کنند. و نیازی نیست هر ادمینی پروفایلی را ایجاد کند و باعث اضافه تر شدن میزان بار روی CPU شود.

یکی از کارهایی که می‌توانید در این حالت انجام دهید استفاده از VDOM Link ها است. مثلا ما یک فایروال فیزیکی را به چند فایروال مجازی تبدیل کرده ایم. حال می‌خواهیم این دو فایروال مجازی با هم ارتباط داشته باشند. بدون اینکه بخواهیم از یک لینک فیزیکی برای اتصال این دو فایروال استفاده کنیم. در این حالت از VDOM Link ها استفاده می‌کنیم. برای این کار وارد منوی Network > Interface > Create New > VDOM Link می‌شویم. و این تنظیمات را انجام می‌دهیم. مشخص می‌کنیم که کدام VDOM با کدام VDOM ارتباط داشته باشد. و این ارتباط به چه رنج آی‌پی انجام شود. مثل این می‌ماند که دو فایروال را بصورت فیزیکی با یک کابل به یکدیگر متصل کرده باشیم.


FGVMEVIFJPLYKIA5
Dashboard
Network
Interfaces
DNS
IPAM
Security Profiles
System
Security Fabric
Log & Report
FORTINET
v7.6.0
VDOM: Global
admin
New VDOM Link
Name
Interface 0
Virtual Domain
VRF ID
0
IP/Netmask
0.0.0.0/0.0.0.0
Administrative Access
HTTPS
PING
FMG-Access
SSH
SNMP
Security Fabric Connection
Comments
Write a comment...
0/255
Status
Enabled
Disabled
Interface 1
Virtual Domain
VRF ID
0
IP/Netmask
0.0.0.0/0.0.0.0
Administrative Access
HTTPS
PING
FMG-Access
SSH
SNMP
Security Fabric Connection
Comments
Write a comment...
0/255
Status
Enabled
Disabled
OK
Cancel

14 High Availability (HA)

در هر شبکه در هر سطحی که هستیم باید مسئله HA را در شبکه خود رعایت کنیم. یکی از موارد بسیار مهمی که حتما باید HA را در آن رعایت کنیم، فایروال‌های شبکه است. تا اگر زمانی یکی از فایروال‌های شبکه از کار افتاد، دسترسی‌ها و اطلاعات ما در خطر نباشند و فایروال دیگری بتواند، وظایف این فایروال را کنترل کند. در ادامه نکات مهم راه اندازی HA در فایروال فورتیگیت را بررسی می‌کنیم.

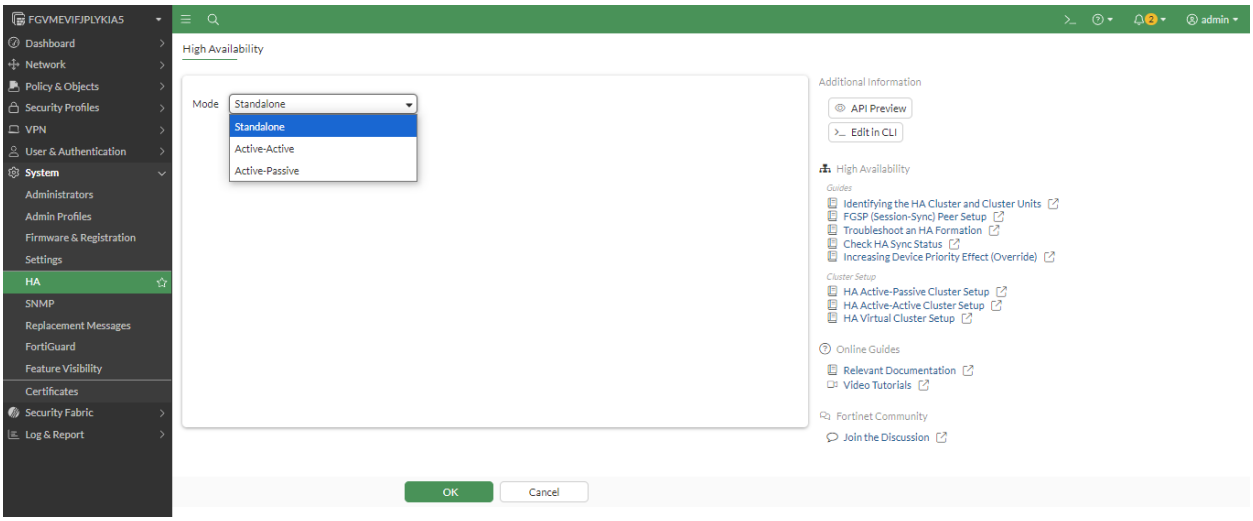
اول: فایروال‌هایی که قرار است به عنوان HA یکدیگر عمل کنند، مشابه یکدیگر باشند. چه از لحاظ سخت افزاری و چه از لحاظ نرم افزاری. حتی نحوه لایسنس آن‌ها هم باید شبیه به هم باشد.

دوم: حداقل دو لینک بین فایروال‌ها به عنوان HA متصل باشد. از این لینک برای Sync کردن تنظیمات، ارسال Session ها به یکدیگر و ارسال پیام Keep a live بین فایروال‌ها استفاده می‌شود.

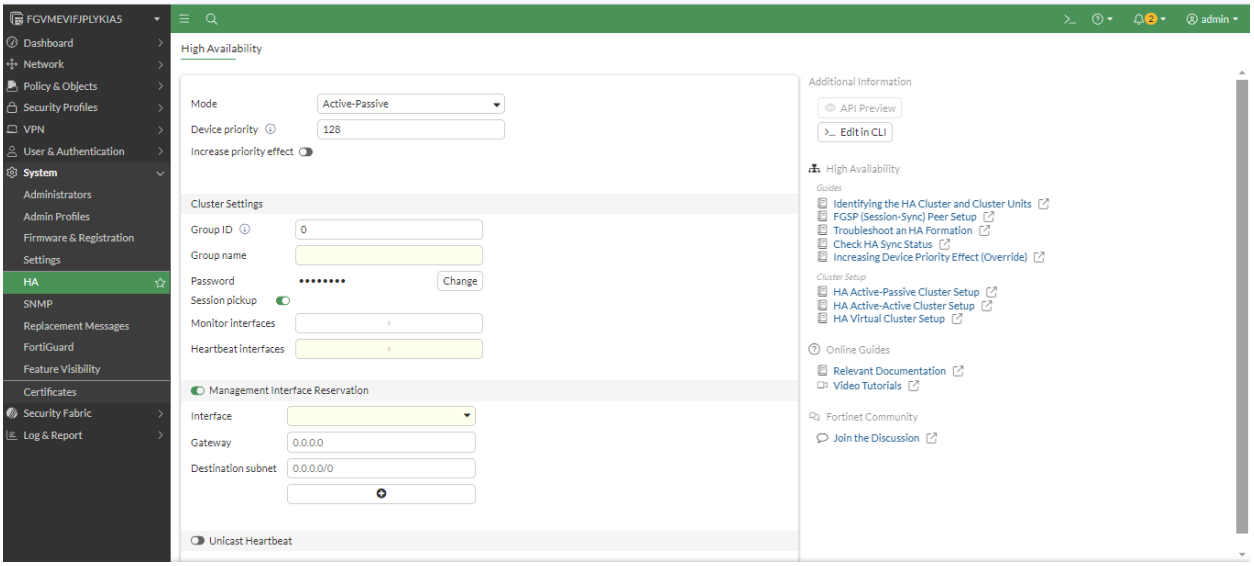
سوم: در HA دو حالت Active-Active و Active-Passive را داریم. در حالتی که هردو اکتیو هستند، یعنی هردو فایروال در شبکه در حال سرویس‌دهی هستند. اما در حالت دیگر یک فایروال در حالت استندبای قرار دارد و زمانی که متوجه شود فایروال دیگر از شبکه خارج شده است، سریعا جای او را پر می‌کند و شروع به سرویس‌دهی می‌کند.

برای تنظیم HA رو هردو فایروال بصورت زیر عمل می‌کنیم:

وارد منوی System > HA می‌شویم و نوع HA خود را که می‌تواند، Active-Active و Active-Passive باشد را انتخاب می‌کنیم. بطور مثال ما حالت Active-Passive را انتخاب می‌کنیم.



در ادامه، Priority فایروال را مشخص می‌کنیم. هرچه این عدد کوچکتر باشد، از اولویت بالاتری برخوردار است. در بخش بعدی در صورتی که از VDOM استفاده می‌کنیم باید یک Group ID مشخص کنیم این ID باید بین 0 تا 7 باشد. یک نام برای این گروه در نظر می‌گیریم. پسوردی که باید بین دو فایروال مشابه باشد. اگر تیک گزینه Session Pickup را بزنیم، تمامی Session ها روی فایروال استندبای انتقال پیدا می‌کند. در قسمت Monitor Interface حتما اینترفیس داخلی و خارجی خود را انتخاب کنید تا هرکدام از دسترس خارج شد، فایروال دوم فعال شود. اگر این بخش را انتخاب نکنیم، تا زمانی که فایروال فعلی بصورت کلی از شبکه خارج نشده باشد، فایروال استندبای فعال نمی‌شود. در قسمت Heartbeat interface همان اینترفیس HA که بین فایروال‌ها است را انتخاب می‌کنیم.



موارد فوق را عینا روی فایروال دوم هم انجام می‌دهیم هردو فایروال یکدیگر را ببینند و با یکدیگر sync شوند.

توسط خط فرمان فایروال هم می‌توانید وضعیت HA را ببینید. با دستور get system ha status. اگر می‌خواهید فایروال را بصورت خط فرمان تنظیم کنید، با دستور زیر می‌توانید این مراحل را انجام دهید. با وارد کردن دستور show تمام دستوراتی که در این بخش می‌توانید وارد کنید را مشاهده می‌کنید.

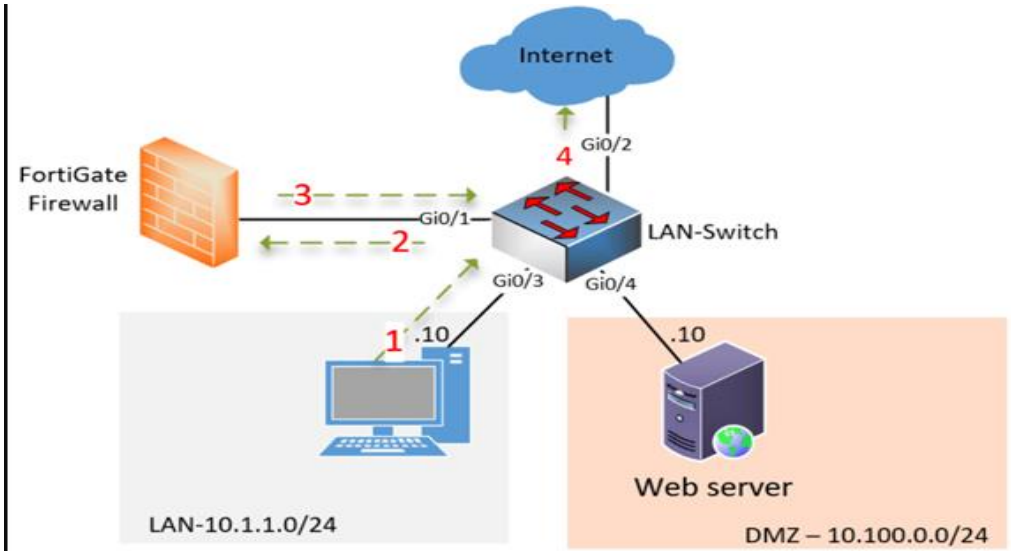
Config ha system

Show

15 Transparent Firewall

معمولا فایروال‌ها در شبکه به حالت Router/NAT قرار می‌گیرند. اما می‌توانیم یک فایروال را در حالت Transparent قرار دهیم. به این صورت که هیچ تغییری در شبکه فیزیکی و کابل‌های خود ایجاد نمی‌کنیم. فقط کافیست فایروال خود را با دو کابل به سوئیچ شبکه متصل کنیم. یک کابل در vLAN کاربران. و یک کابل دیگر در vLAN ای که روتر به آن وصل است. همچون شکل زیر:

دقت کنید که بسیاری از کاربردها را همچون SSL VPN, PPTP, L2TP, DHCP, NAT, از دست می‌دهیم.



با دستورات زیر می‌توانیم این تغییرات را ایجاد کنیم.

Config system settings

Set opmode transparent

Set manageip 192.168.1.10/24

Set gateway 192.168.1.1

End

حتما باید قبل از دستورات فوق fortilink خود را غیر فعال کنید.

Config system interface

Show

Edit fortilink

Set fortilink disable

End