



# امن سازی شبکه با Fortigate Firewall

نگارنده: محمود کریمی

تابستان ۱۴۰۳



# Fortigate Firewall

1	Intro	oduction							
2	Install Fortigate in ESXi								
3	Fire	wall Policy (Profile-based vs Policy-based)9							
4	Fort	igate (DNS, DDNS, DHCP)12							
5	Fire	wall NAT14							
	5.1	Firewall Source NAT							
	5.2	Firewall Destination NAT17							
6	SSL	Inspection							
	6.1	Outbound SSL Inspection							
	6.2	Inbound SSL Inspection							
7	Fire	wall Filtering							
	7.1	Web Filtering							
	7.2	DNS Filter							
	7.3	Application Filtering							
8	User	r Authentication							
9	Anti	virus							
10	IPS/	WAF							
11	Dos	Policy							
12	VPN	V and Cryptography							
	12.1	Site to Site VPN with IPSEC							
	12.2	Remote Access VPN with IPSEC							
	12.3	Remote Access VPN with Web Based SSL							
	12.4	Remote Access VPN with Tunnel Based SSL							
13	Virt	ual Domains (VDOM)							
14	Higl	h Availability (HA)							
15	Trar	1sparent Firewall							



# 1 Introduction

فایروال فورتی نت 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 <sup>(</sup>و سیستمهای امنیتی پیشرفته که بهرهوری بالایی دارند. یکی از محصولاتی که توسط شرکت Fortinet ارائه میشود، فایروالهای FortiGate هستند. فایروال نسل جدید فورتی نت 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 <sup>۲</sup>می باشد. البته برای محافظت واقعی از شبکه به سایر تکنولوژی ها نیز نیاز است. در ضمن می توان گفت امنیت موثر شبکه، نیاز به رویکردی جامع و کامل دارد که فایر وال 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. فایر وال های Fortinet همواره در جهت بهبود پاسخ دهی نیاز های مشتریان خود بوده و با نیازهای امنتی 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 فورتی گیت 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 هزینه هایی 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 می شود.

<sup>&</sup>lt;sup>1</sup> Virtual Security Processing

<sup>&</sup>lt;sup>2</sup> Next Generation Firewall

ایمن<mark>شبکه</mark>هوشمند Secure Intelligent Network

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

- ای ویژگی های امنیتی مانند انواع ماژول ها
  - امكانات فيلترينگ وب
- ۷ΟΙΡ امکانات حفاظت از انواع پروتکل های VOIP
  - حفاظت از IPS یا IDS
- پشتیبانی درگاه انتقال (Gateway) از آنتی و پروس های قدرتمند و شناخته شده
  - ب جلوگیری از اسپم
  - ۵۰ قابلیت کنترل ترافیک برنامه های کاربردی
  - ۵۰ قابلیت جلوگیری از از دست رفتن دادهها (DLP)
    - ارتباط امن از راه دور
- مج برخورداری از سیستم عاملی قدرتمند که امکانات مورد نیاز شما را داشته باشد
  - بشتیبانی از انواع روشهای احراز هویت
    - انواع فايروال فورتى 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 (OSI) Open System Interconnection 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 یکپارچکی 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 پورت ها 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.



**Fortigate Firewall** 

#### **Unified Threat Management Firewall**

فایروال های (UTM) 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 جمله antivirus ، antivirus on antivirus و موارد دیگر، یکپارچه می سازند. به طور معمول فایروال های UTM به UTM به uTM، anti-spam، prevention systems و موارد دیگر، یکپارچه می سازند. 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 هستند، 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 بخش های شبکه و شعب سازمانی را از یک کنسول واحد اداره و تامین کنند. در این صورت فرایند کاری تیم امنیت و مسئولیت های اضافه کاهش پیدا می کند. به عبارتی با فایروال MTW، تنها یک تیم امنیت برای کل سازمان و حتی شعب مختلف مورد نیاز می باشد.

#### **Network Address Translation Firewalls**

فایروال (single gateway) به فضای اینترنت هدایت، Network Address Translation (NAT) میکند. اساسا این فایروال (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 address برای کانکشنهای خارجی، سایر آدرسهای آی پی 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 می شوند اما گاهی هم برای خدمات VPN از آن ها استفاده می شود.

#### **Internal Segmentation Firewalls**

Internal Segmentation یا Fortinet 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 segmentation طراحی شده اند تا بتوان فرایندهای کاری و ایمهیزات جدید را به segment های خاص شبکه و بر اساس معیارهای مختلف اختصاص داد.



# Next Generation Firewalls (NGFW)

(NGFW) از نظر مسدود سازی تهدیدات جدید، شباهت زیادی به فایروال های UTM دارند. آن ها قابلیت ها و معلکردهای فایروال های نسل قدیمی تر به عنوان مثال stateful inspection را با تکنیک ها و تکنولوژی هایی که انواع تهدیدات را مورد بررسی قرار می دهند، ادغام می سازند. این دسته از فایروال ها برای سازمان هایی مناسب هستند که در جستجوی امنیتی دقیق و گسترده بوده و تامین امنیت شبکه، می دهند، ادغام می سازند. این دسته از فایروال های سازمان هایی مناسب هستند که در جستجوی امنیتی دقیق و گسترده بوده و تامین امنیت شبکه، می دهند، ادغام می سازند. این دسته از فایروال ها برای سازمان هایی مناسب هستند که در جستجوی امنیتی دقیق و گسترده بوده و تامین امنیت شبکه، می در برای این این دقیق و گسترده بوده و تامین امنیت شبکه، برای آنها بسیار حیاتی است. فایروال های Fortinet NGFW در تامین امنیت شبکه، فراتر از استانداردهای صنعتی رفته و برای دهمین بار در برای آنها بسیار حیاتی است. فایروال های پروال های Fortinet NGFW در تامین امنیت شبکه، فراتر از استانداردهای صنعتی رفته و برای دهمین بار در برای آنها بسیار حیاتی است. فایروال های Fortinet NGFW در تامین امنیت شبکه، فراتر از استانداردهای صنعتی رفته و برای دهمین بار در برای آنها بسیار حیاتی است. فایروال برتر شبکه، توسط گارتنر شناخته شده است. فایروال های نسل جدید فورتی گیت، کلیهی قابلیت هایی 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 می دهد و رویکرد امنیت محور فورتی نت، امنیتی دقیق و گسترده را به تمامی بخش های شبکه اختصاص می دهد.



# 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.

VM Images	Fortinet VM Welcome to the	1 deployment Ima Fortinet VM images dow	ges nload center for Fortinet's extensive line of security solutions	
Select Product		FortiGate for VN	Ware ESXi platform Version 7.6.0	Upgrade Path Release Notes
FortiGate	~	File Information	Checksum	
Select Platform		Upgrade from previous version of	3cfe0ac1f63a8f7771fad60579a8bcf8 (Regular) 7d8812505b4f98b5b9054e6244a18296f7dc4ffec4e861d477daa6529c4ae0	0b4a05d6ad37cfacf4e7fd804676da8ab5220ed48a7276514f7573c7913646178
VMWare ESXi	~	FortiFirewall for VMWare FFW_VM64-v7.6.0.F-	(SHA-512)	
Latest Version		build3401- FORTINET.out (96.61		
7.6.0		MB)		
7.4.4		Download		
Earlier Versions		New deployment of	c5571ced0daada2e6ba06f5b8750dd71 (Regular)	
7.2.9		FortiFirewall for VMware	5828c2fbb71576fc5ffc5336d6bc0ad19b314966d4b6f6493131f187d9d4945 (SHA-512)	:33642e59d2df4424168055373c9aed1e0183d42961953b5c76c674ed8ed98f72

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

Name	Date modified	Туре	Size
📴 datadrive.vmdk	2010-08-23 9:02 PM	VMDK File	70 KB
😥 FortiGate-VM64.hw13.ovf	2024-07-24 10:03	Open Virtualizatio	30 KB
😥 FortiGate-VM64.hw15.ovf	2024-07-24 10:03	Open Virtualizatio	30 KB
😡 FortiGate-VM64.hw17.ovf	2024-07-24 10:03	Open Virtualizatio	27 KB
😥 FortiGate-VM64.nsxt.ovf	2024-07-24 10:03	Open Virtualizatio	14 KB
😥 FortiGate-VM64.ovf	2024-07-24 10:03	Open Virtualizatio	27 KB
😥 FortiGate-VM64.vapp.ovf	2024-07-24 10:03	Open Virtualizatio	45 KB
😥 FortiGate-VM64-ZTNA.vapp.ovf	2024-07-24 10:03	Open Virtualizatio	29 KB
📴 fortios.vmdk	2024-07-24 10:03	VMDK File	101,514 KB
readme.txt	2024-07-24 10:03	Text Document	2 KB

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 system interface physical میتوانیم آیپی ها یا وضعیت اینترفیس های تنظیم شده را ببینیم. و به آیپی های مشخص شده، از طریق وب وصل شویم. با یوزرنیم و پسوردی که در محیط CLI تنظیم کردیم وارد محیط گرافیکی آن میشویم.



FGVMEVIFJPLYKIA5	•	≡ Q						≻ @• A	1) -
② Dashboard	~ î	+ Add widget	]						
Status	1	[0.1.1.4		-	Learning a reserve		_		
Security		System Infor	mation	= •	Licenses ( 208.18	4.237.66) 🛈	= •	Virtual Machine	= •
Network		Hostname	FGVMEVIFJPLYKIA5					▲ FGVMEV License	
Assets & Identities +	I	Serial number Firmware	FGVMEVIFJPLYKIA5 v7.6.0 build3401 (Feature)		Support Update	s IPS	AntiVirus	Allocated vCPUs	1/1
FortiView Sources		Mode	NAT					8001	
FortiView Destinations		System time	2024/08/25 03:52:23		Web Filter Ratins			Allocated RAM	2 GiB / 2 GiB
FortiView Applications		Uptime	26m 28s					97%	
FortiView Web Sites		WANIP	C		FortiToken				
FortiView Policies									
FortiView Sessions +		FortiGate Cl	oud	≡•	Security Fabric		:3 ≡•	Administrators	2 ≡•
🕂 Network	>	Status	A Not Supported		L	AN Edge		0 FortiExplorer 1 HTTPS	
💄 Policy & Objects	>				FortiGate	X: 0 For	rtiSwitch	admin super_admin	
🔒 Security Profiles	>				(initial) (I) FortiAP	E O For	rtiExtender		
I VPN	>				Eabrie	Connectors			
음 User & Authentication	>				- Lessies	centrectors	and here		
-^					Logging	E Fortisi	andbox		
	7.6.0				Central	E FortiC	lient FMS		

# 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 آی پی تنظیم کنیم.

Config system interface

Edit port1

Set mode static

Set ip 192.168.1.1 255.255.255.0

با دستورات زیر می توانیم 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 می توانیم 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، پالیسی ها 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 پالیسی ها 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 می شویم.

🕞 FGVMEVIFJPLYKIA5 🛛 🗸	≡ Q	>_
② Dashboard > <sup>1</sup>	System Settings	
↔ Network >		
💄 Policy & Objects 💦 >	Date/Time display FortiGate timezone Browser timezone	Additional Information
A Security Profiles		API Preview
□ VPN >	System Operation Settings	>_ Edit in CLI
은 User & Authentication > System	NGFW mode Profile-based Policy-based	Virtual Domain
Administrators	Virtual Domains ①	Setup guides III How to Configure Virtual Domains
Admin Profiles Firmware & Registration	Start Up Settings	Guides
Settings ☆	Allow FortiConverter to obtain config file once	Using configuration save mode
НА	USB auto-install ①	⑦ Online Guides
SNMP	Detect configuration	Relevant Documentation
Replacement Messages		🗅 Video Tutorials 🖸
FortiGuard	Detect firmware C image.out	Pa Fortinet Community
Feature Visibility	Empil Convice	
Certificates	Email Service U	
M Security Fabric > _	SMTP Server A fortinet-notifications.com	-

Profile Based : این حالت بدون Central NAT کار میکند. یعنی در هر پالیسی باید مکانیزم NAT را اگر بخواهیم، باید برای آن فعال کنیم. Tentral Based : این حالت بدون Central NAT کار میکند. یعنی در هر پالیسی باید مکانیزم NAT را اگر بخواهیم، باید برای آن فعال کنیم. IPS, SSL Inspection, Web Filter را برای Policy Based فعال کنیم. Profile Signa محلی که می توانیم پالیسی های مربوط به NAT را در آن بصورت مرکزی ایجاد و مدیریت کنیم. همچنان قابلیت هایی مثل IPS, SSL Inspection, Web Filter و ... را در این حالت بصورت Based Based داریم. یعنی برای هر کدام از این قابلیت ها یک پروفایل مخصوص ایجاد می کنیم و در پالیسی خود آن را اعمال می کنیم.

Policy Based: این حالت فقط با Central NAT کار میکند. در این حالت URL Category و Application Filter به عنوان یکی از گزینه های پالیسی هستند و بقیه موارد بصورت SSL Inspection and Authentication هستند. در این حالت SSL Inspection and Authentication بصورت یک منوی جدا در زیرشاخه Policy and Objects اضافه می شود. این نوع جدیدا اضافه شده است. و فایروال های قدیمی بر اساس Profile کار میکند. نکته مهم: پالیسی ها به ترتیب اجرا می شوند، پس اولویت آن ها و ترتیب آن ها بسیار مهم است.



برای ایجاد پالیسی وارد مسیر Policy & Object > Firewall Policy > Create New می شویم. 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.

🕞 FGVMEVIFJPLYKIA5 🛛 🕶	≡ Q		≻_ ⊙• 4	0 <mark>1</mark> -	(8) admin •
② Dashboard →	(+ cm	Create New Policy			>
+ Network >	( the second				
Policy & Objects 🗸	In Case	Name 🕢	Autoutional Information		
Firewall Policy	Contraction of the local distribution of the	Schedule	NW OF FEISNEW		
Central SNAI	1	Action ACCEPT O DENY	⑦ Online Guides		
Addresses		Incoming interface	Relevant Documentation      D1 Video Tutorials		
Internet Service Database		Outgoing interface	D1 Consolidated Policy Configuration		
Services			Ra Fortinet Community		
Schedules		Source & Destination (Showlogic)	○ Join the Discussion <sup>™</sup>		
DNAT & Virtual IPs		Source +			
IP Pools					
Protocol Options		usengroup +			
Traffic Shaping		Destination +			
Security Profiles		Firewall/Network Options			
S User & Authentication		Incention mode Eleve based Drawy based			
i System >		Hispection mode Providesed Proxy-based			
Security Fabric >		Central NAT is enabled so NAT settings from matching Central SNAT			
E Log & Report →		policies will be applied.			
		Protocol options record default			
		Security Profiles			
		AntiVirus 🔘			
🕞 FGVMEVIFJPLYKIA5 🛛 🕶	≡ Q		>_ @• 4	¢ <b>3</b> ≁	(8) admin +
Ø Dashboard →	+ Cra	Create New Policy			×
** Network >	Pr	Firewall/Network Options	Additional Information		
Eirewall Policy	ime!	Produculophons default T	(1) API Preview		
Central SNAT		Security Profiles	⑦ Online Guides		
DoS Policy		AntiVirus 🗿	Relevant Documentation      Video Tutorials		
Addresses		Web filter	D1 Consolidated Policy Configuration		
Internet Service Database		DNS filter	Q Fortinet Community		
Services		Application control	○ Join the Discussion <sup>™</sup> <sup>™</sup>		
Schedules					
DNAT & Virtual IPs					
IP Pools Protocol Ontions		File niter			1
Traffic Shaning		SSL inspection			
☐ Security Profiles >		Logging Options			
		Log allowed traffic O Security events All sessions			
$\stackrel{\circ}{\simeq}$ User & Authentication $\rightarrow$		Generate loss when session starts			
♦ System >		Contrue prover			
Security Fabric >		Captore pdURCD Captore pdURCD			
E Log & Report →		Comments			
		0/1023			
		Enable this policy 🔍			
	O Ser				
FEIRTINET v760	100 2000	OK Cancel			

توضيحات بيشتر: در قسمت Source و Destination ميتوانيم به سه طريق، ترافيكي كه ميخواهيم روى آن كنترل داشته باشيم را مشخص كنيم. 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.



🕞 FGVMEVIFJPLYKIA5 🛛 👻	= (	۹										>_ 🛛 -	Q <b>1) •</b> ⊗ admin •
⑦ Dashboard >	(L	Create new	O Ballou match	0.0	arch							B. Event	latarfaca Bair View -
+ Network >	(	createnew	C Policy match	0430	arch						~	Es export +	Internace Fail View +
🛃 Policy & Objects 🛛 🗸 🗸		Policy	Source		Destination	Schedule	Service	Action	NAT	Туре	Security Profiles	Log	Bytes
Firewall Policy 습		m port1 →	🛿 port3 2			-							
Central SNAT		test2(2)	🖪 all	🔛 wildo	$\bigtriangledown$ Filter by Destination $\bullet$	always	ALL	✓ ACCEPT	O Custom	Standard	no-inspection	🛛 All	0 B
DoS Policy				Ø €	P Edit	le 📋 Delete	V More						
Addresses	0	test1(1)	4 all	😐 wildo	T Insert	always	ALL	✓ ACCEPT	Custom	Standard	no-inspection	🖸 All	0.8
Internet Service Database	TEL 1	molicit 🕢	78.00	100.0000	🖉 Set Status 🔸					10.00000000000			
Services					🗊 Delete								
Schedules					(D Copy								
DNAT & Virtual IPs					(D Paste								
IP Pools					🐻 Show matching logs								
Protocol Options					🗠 Show in FortiView	1							
Traffic Shaping					>_ Edit in CLI								
A Security Profiles >													
□ VPN >													
≗ User & Authentication →													
© System →													
Ø Security Fabric >													
Log & Report >													

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

🕞 FGVMEVIFJPLYKIA5 🛛 👻		>_
⑦ Dashboard >	A Craste see O Search Policy Match Tool	×
+ Network		
💄 Policy & Objects 🛛 🗸 🗸	Policy Source Destination Schedu Incoming interface	
Firewall Policy ☆	E B port3 @ Restored HTTDS	
Central SNAT	E 🖸 test2 (2) 🔲 all 🔛 wildcard google.com 🕼 alway	
DoS Policy	Source IP address	
Addresses	Source port Optional 1-65535	
Internet Service Database	User Any User Group	
Services	Destination address IP address/FODN	
Schedules		
DNAT & Virtual IPs	Destination port 443	
IP Pools		
Protocol Options		
Traffic Shaping		
Security Profiles		
□ VPN >		
$\stackrel{{}_\sim}{_\sim}$ User & Authentication $\rightarrow$		
③ System >		
Ø Security Fabric →		
🖻 Log & Report >		

# ایمن شبکه هوشمند Secure Intelligent Network

# 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.

Dashboard	>	DNS Settings			
• Network					DNIC Either Deting Convers
Interfaces		DNS servers	Use FortiGuard Servers Specify		Dis riter kaung servers
DNS	☆	Primary DNS server		50 ms	Additional Information
IPAM		Secondary DNS server		70 ms	API Preview
FortiExtenders		Local domain name			>_ Fdit in CI I
SD-WAN			0		
Static Routes		DNCDestant			🚍 Setup guides
Diagnostics		DNS Protocols			🗿 DNS Local Domain List 🕜
Policy & Objects		DNS (UDP/53) 🚯 🖸			Using FortiGate as a DNS Server C FortiGuard DDNS C
Security Profiles		TLS (TCP/853) 0 C			
🖵 VPN		HTTPS(TCP/443) 🖲 🔾			
User & Authentication		SSL certificate 1	Fortinet_Factory	▼	Video Tutorials 2
		Server hostname	globalsdns.fortinet.net		
System			6		Portinet Community
					FortiClient & Static DNS Entry

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.

DNS	☆				>_ Edit in CLI
IPAM		Dynamically Obtained DNS Servers			🧱 Setun guides
FortiExtenders		Interface DNS Server			
SD-WAN		040 40 00 00 10 ms			$\square$ Using FortiGate as a DNS Server $\square$
Static Routes		wan 195.229.241.222 10 ms			FortiGuard DDNS C
Diagnostics					⑦ Online Guides
📕 Policy & Objects		Dynamic DNS			Relevant Documentation
Security Profiles			-		
□ VPN		+ Create new 🖋 Edit 🔟 Delete 🛛 😌	<b>Q</b> Search	Q	₽ Fortinet Community
User & Authentication		Domain 🗢	Interface 🗘	Public IP 🖨	FortiClient & Static DNS Entry
		tethyshippingllcdxb.fortiddns.com (83.110.3.244)	🔚 wan	Senabled	Fedora 40 can not connect to services behind vpn using domain
🏟 System		dxbkkkkk.float-zone.com (83.110.3.244)	🛗 wan	Enabled	names @ 4 Answers # 1 Votes @ 799 Views
Security Fabric				2	resolving Internal DNS internally
Log & Report					🗭 7 Answers 🗯 0 Votes 🔹 1,899 Views
					See More 🗹
		Analy			
	7.4.4	Арріу			

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.



Dashboard	>	DNSS	Edit DDNS Entry				×
Network	~		Interface		~		
Interfaces			Interface	+			
DNS	☆		Use public IP address				
IPAM				🛱 fleet zene eem	_		
FortiExtenders			Server	@ noat-zone.com			
SD-WAN			Unique location	dxbkkkkk		S Available!	
Static Routes			Domain	dxbkkkkkk.float-zone.com C (83.110.3.244)			
Diagnostics							
Policy & Objects							
Security Profiles							
므 VPN							
User & Authentication							
System							
Ø Security Fabric							
ഥ Log & Report	>						

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

🕞 FGVMEVIFJPLYKIA5 🛛 🗧	Q	VDOM: 🕼 Global 🔹 📐 🗇 🖛 📮 🔕 admin 🔹
② Dashboard >	Edit Interface	x
+ Network 🗸	O DHCP Server	
Interfaces 🏠	DHCP status   Enabled   Disabled	FortiGate
DNS		FGVMEVIFJPLYKIA5
ІРАМ	Address range 0000-0000	Status
Security Profiles	0	O Up
গ্ট System > 💽	] ∄• 8 Netmask 0.0.0.0	
Security Fabric >	Default gateway Same as Interface IP Specify	00:0c:29:f4:73:52
'≡ Log & Report >	DNS server Same as System DNS Same as Interface IP Specify	Additional Information
	Lease time () C (coreco) second(s)	
	004000	© API Preview
	Advanced	% References
		>_ Edit in CLI
	Mode Server Relay	(2) Online Guides
	Type Regular IPsec	Relevant Documentation 12
	NTP server Local Same as System NTP Specify	□ Video Tutorials [2]
	0	On Eastingt Community
		Ioin the Discussion [7]
	Wireless controllers Same as Interface IP Specify	
	0	
	Time zone Same as System Specify	
	Next bootstrap server 0.0.0.0	
	TETP server(s)	
		Ť
🕞 FGVMEVIFJPLYKIA5 🔹 🗏		VDOM: 🚯 Global ▼ >_ ⑦ ▼ 📮 2 ▼ 🛞 admin ▼
② Dashboard >	Edit Interface	×
+ Network v	Additional DHCP Options	A
Interfaces 🏠		
DNS	Create New P coit Delete Search	C POVMEVIDPERIAD
	Code 🗢 Type 🗢 Value 🗢	Status
Security Profiles		O Up
l⊗ System > [-	Be 8 No results	MAC address
Security Fabric		00:0c:29:f4:73:52
Log & Report /	©	Additional Information
	IP Address Assignment Rules	ADI Preview
	+ Crosta New & Edit Delata Coards O III Add from DHCD Client List	9. Defension
		To References
	Type Match Criteria Action IP	>_ Edit in CLI
	Implicit Unknown MAC Addresses Assign IP	⑦ Online Guides
		E Relevant Documentation
		🗆 Video Tutorials 🖸
	<b>0</b>	Ra Fortinet Community



# 5 Firewall NAT

توصیه می شود در طراحی شبکه، سرویس NAT روی فایروال پیاده سازی شود تا روی روتر. به این دلیل که NAT با برخی از سرویس ها مثل ,VPN FTP, Voice, Video به مشکل بر می خورد. چرا که این ترافیک ها نیاز به یک ارتباط پایدار و با تاخیر کم دارند. و در صورت تاخیر، این نوع ترافیکها دچار مشکل می شوند. البته که، فایروال فورتیگیت ترافیک تا لایه اپلیکیشن را می فهمد و می تواند آن را ببیند، لذا می تواند 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 کند. تعداد آدرس های global با تعداد دستگاه های شبکه داخلی که می خواهند از اینترنت استفاده کند 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 یورت و IP ها را ردیابی می کند و براساس آنها جدول NAT را تشکیل می دهد.

وظیفه NAT ترجمه آی پی های Private به آی پی 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، می خواهند به شبکه اینترنت دسترسی داشته باشند. در این حالت ما از این نوع NAT استفاده می کنیم. در فایروال فورتیگیت NAT می تواند به ازای هر پالیسی اجرا شود و هم می تواند بصورت Central NAT ایجاد شود. برای اینکه NAT را به ازای

در فایروال فورنیکیت NAT می نواند به ازای هر پالیسی اجرا شود و هم می نواند بصورت Central NAT ایجاد شود. برای اینکه NAT را به ازای هر پالیسی تنظیم کنیم. وارد منوی پالیسیها می شویم، یکی از پالیسیها را در حالت Edit قرار می دهیم و در قسمت NAT موارد را تنظیم می کنیم. مثلا می توانید برای NAT هم، از آی پی پورت خروجی یا WAN استفاده کنیم و هم از یک رنج IP Pool که بصورت Public هستند استفاده کنیم.

Dashood     Network     Network     Policy & Othes     Firewall Network (Options   Firewall Network (Options   Nat   Dash Dilky   Addresses   Internet Schrice Database   Services   Schedules   Protocol Options   Protocol Options   Tarler Salaning   Security Profiles   Security Security Flank   Security Securi	B FGVMEVIFJPLYKIAS •		>_ ©• Q <b>0</b> • Q <b>0</b> •
Network >   Palicy Addresses Firewall/Network Options   Internet Service Database Pool configuration   Services Preserve source port   Protocol options Preserve source port   Protocol options Protocol options   Traffic Shaping Services   Services Protocol options   Protocol options Mathing   Services Protocol options   Traffic Shaping Services   Services Protocol options   Services Protocol options   Traffic Shaping Services   Services Protocol options   Services Protocol options   Traffic Shaping Services   Services Protocol options   Services Protoc	Dashboard	Edit Policy	
Publicy Collects Insection mode Flow All/Network Options   Services Internet Service Database   Services Pool Configuration   Scrvices Protocol Options   Protocol Options Image: Control Options   Protocol Options Carrent bandwidth   Obs Shire Carrent bandwidth   Dos Shire Carrent bandwidth   Protocol Options Carrent bandwidth   Servicy Profiles Carrent bandwidth   Serviry Profiles Carrent bandwidth   Dis Shire Carrent bandwidth   Dis Shire Carrent bandwidth   Serviry Foldies Serviry Profiles   Serviry Foldies Pist   Serviry Foldies Pist   Dis Shire Serviry Foldies   Serviry Foldies Serviry Foldies   Serviry Foldies Serviry Foldies   Dis Shire Serviry Foldies   Serviry Foldies <td< th=""><th>• Network &gt;</th><th></th><th>Statistics (since last reset)</th></td<>	• Network >		Statistics (since last reset)
Firewall Policy   Dos Policy   Addresses   Internet Service Database   Services   Security Profiles   Additional Information   Security Profiles   Security Profiles   Security Profiles   Security Fabric   Security Fabric </td <td>Policy &amp; Objects 🛛 🗸 🗸</td> <td>Firewall/Network Options</td> <td>ID 2</td>	Policy & Objects 🛛 🗸 🗸	Firewall/Network Options	ID 2
DoS Poloy Addresses   Addresses   Services   Services   Schedules   Vitual IPs   Potocol Options   Security Profiles   Security Profiles   Security Profiles   Security Foldies   System   System   Signed Control   Fiss control   Fiss control   Signed Control   Construction   Construction   Construction   Construction   Signed Control   Construction   Construction   Construction   Signed Control   Construction   Construction <td>Firewall Policy ☆</td> <td>Inspection mode Flow-based Proxy-based</td> <td>Last used N/A</td>	Firewall Policy ☆	Inspection mode Flow-based Proxy-based	Last used N/A
Addresses Internet Services Internet Services Internet Services Se	DoS Policy	NAT O	First used N/A
Ministries work Dubulable   Schrädet   Schrädet   Schrädet   Schrädet   Protocol Options   IP Poole   Protocol Options   Security Profiles   VPN   Dis Sitter   Obs Sitter   Obs Sitter   Security Profiles   VPN   Dis Sitter   Security Profiles   Security Profiles   VPN   Dis Sitter   Dis Sitter   Security Fabric   Log & Report	Addresses	IP pool configuration Use Outgoing Interface Address Use Dynamic IP Pool	Active sessions 0
Schedules   Vartual IPs   IP Pools   Protocol options   Tarffic Shaping   Security Profiles   VPN   VPN   Security Fabric   System   Security Fabric   Log & Report   Security Fabric   Log & Report   Security Fabric   Log & Report     Security Fabric   Log & Report     Security Fabric   Log & Report     Security Fabric   Log & Report     Security Fabric   Log & Report     Security Fabric   Log & Report     Security Fabric   Log & Report     Security Fabric   Log & Report     Security Fabric   Log & Report     Security Fabric   Log & Report     Security Fabric   Log & Report     Security Fabric   Log & Report     Security Fabric   Log & Report     Security Fabric   Log & Report     Security Fabric   Log & Report     Security Fabric   Log & Report     Security Fabric   Log & Report     Security Fabric   Log & Report     Security Fabric   Log & Report     Security Fabric   Log & Report <td>Services</td> <td>Preserve source port</td> <td>Hit count 0</td>	Services	Preserve source port	Hit count 0
Virtual IPs     Security Profiles       IP Pools     Security Profiles       Traffic Shaping     Meb Siter       Security Polies     Meb Siter       VPN     Dis Sitier       Security Fabric     Application control       Security Fabric     Site in control       Log & Report     Stanspection       Log allowed traffic     Security events< All sessions	Schedules	Protocol options	Total bytes 0 B
iP Pools     Protocol Options     Image: Control options     Image: Control options       Trafic: Spaining     AntiVirus     Image: Control options     Additional Information       Very Asuthentication >> Very Asuthentication >> Security Pablics     Application control options     Image: Control options       Very Asuthentication >> Security Fabric     Image: Control options     Image: Control options     Image: Control options       Very Asuthentication >> Security Fabric     Image: Control options     Image: Control options     Image: Control options       In gailowed traffic     Image: Control options     Image: Control options     Image: Control options     Image: Control options       In gailowed traffic     Image: Control options     Image: Control options     Image: Control options     Image: Control options       Image: Control options     Image: Control options     Image: Control options     Image: Control options     Image: Control options       Image: Control options     Image: Control options     Image: Control options     Image: Control options     Image: Control options       Image: Control options     Image: Control options     Image: Control options     Image: Control options     Image: Control options	Virtual IPs		Current bandwidth 0 bps
Protocol Options     AntiVirus:     Image: Constraint of the constr	IP Pools	Security Profiles	Clear Counters
Tardfe Supplie       Meb filter       Additional information         Security Profiles       DNS filter       DNS filter       DNS filter         DNS filter       Application control       Security Fabric       DS filter         Security Fabric       File       File       Online Guides         Inter & Authentication       File filter       Online Guides       DS filter         Security Fabric       SSL Inspection       SSL Inspection       Online Guides         Inter & Guides       SSL Inspection       SSL Inspection       DS fortier         Log & Report       SSL Inspection       SSL Inspection       D solute Guides         Log allowed traffic       Security events       All sessions       D solute Discussion (2)	Protocol Options	AntiVirus	
Security Profiles       Image: Constraint of the constraint of	Traffic Shaping	Web filter	Additional Information
VPN     DkS hiter     DkS hiter     C     Sk     Sk <td< td=""><td>Security Profiles &gt;</td><td></td><td>@ API Preview</td></td<>	Security Profiles >		@ API Preview
User & Authentication >> System >> Security Fabric >> Log & Report       PS       Online Guides       Image: Comparison of the Compari	VPN >	DNS filter	> Edit in CLI
System     IPS     IRelayant Documentation IC       Security Fabric     File filter     Interface       Log & Report     SSL inspection     Interface       Log ing Options     Interface     Jointhe Discussion IC       Log allowed traffic     Security events All sections     Interface	User & Authentication >	Application control	(2) Online Guides
Security Fabric  Log & Report	System >	IPS O	■ Relevant Documentation
Log & Report SSL inspection SSL inspection Capital Consolidated Policy Configuration Capital Consolidated Policy Configuration Capital Consolidated Policy Configuration Capital Consolidated Policy Configuration Capital Cap	Security Fabric >	File filter	🛛 Video Tutorials 🖒
SSL inspection     SSL inspection     Page Forther Community       Logging Options     D Join the Discussion (2)       Log allowed traffic     Security events	Log & Report		CII Consolidated Policy Configuration C
Logging Options O Join the Discussion (2)	cog uneport /	SSL inspection •	Ry Fortinet Community
Log allowed traffic Security events All sections		Logging Options	Ø Join the Discussion ☑
		Log allowed traffic	

همچنان می توانید عمل NAT را به یک IP Pool بدهید. تصویر زیر تنظیمات ایجاد IP Pool را به ما نشان می دهد. گزینه Overload همان PAT همچنان می نشان می دهد. گزینه Overload همان IP ما نشان می دهد.

🕞 FGVMEVIFJPLYKIAS 🔹	ΞQ			>_ ⑦▼ Q <mark>9</mark> ▼ ⊗admin▼
⑦ Dashboard >	+ Cre Edit Poli	New Dynamic IP Pool		×
Photovork     Network	Firesc Proto Securi Antivi	Name       Comments       Type       Overload       External IP Range ()       00.00-00.00       NAT64       0       11       12	0/255	FortiGate FortiGate FortiGate FortiGate Content and Information  Additional Information  Additional Information  Additional Information  Additional Information  Additional Information  Fortige Community  Fortige Community
System     Security Florings     View     V	Web f DNS fi Applic IPS File fil	n n c.		

یا Port Address Translation است. در روترهای سیسکو هم از همین واژه استفاده می شود.

می توانید بصورت CLI هم گزارش هایی در مورد NAT ببینید.

Get system session list



port1 sical port2 port3 ssl.roo <sup>-</sup>	dhcp static static t stat	0.0.0.0 0.0.0 0.0.0 tic 0.	0.0.0.0 .0 0.0.0. .0 0.0.0. .0 0.0.0.0. 0.0.0 0.0	192.16 0 0.0. 0 0.0. 0.0.0	8.11.12 0.0 0.0 0.0 0.0 0.0 0.0	28 255.2 1.0.0 u 1.0.0 u 0.0.0.0	255.25 1 p d 1 p d 1 u p	5.0 up isable isable disable	disable physical physical e tunnel	քիy
FGUMEUI	FJPLYKI	75 # sh	system in	nterface	: Тімеоџ	ıt				
FGVMEVII Password Welcome	FJPLYKII 1: !	75 login	: admin							
FGVMEVI	FJPLYKI	75 # get	system s	session						
FGUMEUI) PROTO T	FJPLYKI EXPIRE	75 # get SOURCE	system s	session SOURCE	list 2-NAT	DES	TINAT	ION	DESTINATIO	N-NA
tcp	3595	192.168	.11.1:248	389 -		1	92.16	8.11.128	:443 -	
udp	172	192.168	. 11. 128:1	1825 -			192.1	68.11.1:	53 -	
tcp	3556	192.168	.11.1:248	348 -		1	.92.16	8.11.128	:443 -	
FGUMEVI	FJPLYKI	<sup>95</sup> # _								

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

🕞 FGVMEVIFJPLYKIA5 🔹		>_
② Dashboard →	Create New Policy	×
+ Network >		
💄 Policy & Objects 🛛 🗸 🗸		Additional Information
Firewall Policy	Incoming Interface +	API Preview
Central SNAT ☆	Outgoing Interface	(2) Online Guider
DoS Policy		E Palement Decumentation 52
Addresses	Source Address	Video Tutorials C
Internet Service Database	Destination Address	
Services		R) Fortinet Community
Schedules	NAT	♀ Join the Discussion
DNAT & Virtual IPs	NAT C NAT	
IP Pools	IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool	
Protocol Options	Protocol Any TCP UDP SCTP Specify 0	
Traffic Shaping	Explicit port mapping	
🖞 Security Profiles 💦 👌		
□ VPN >	Comments Write a comment.	
😤 User & Authentication 💦 >	0.1023	
⊗ System >	Enable this policy C	
Ø Security Fabric		
💷 Log & Report >		



نظر ميگيريم.

## 5.2 Firewall Destination NAT

در حالت Destination NAT در این حالت هم، روی پورتهای مختلف، میتوانیم به سرویسها و سرورهای مختلف از بیرون به داخل شبکه دسترسی آی پی 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 آی پی پابلیک WAN خود را وارد میکنیم. و در قسمت MAP to IPv4 Address در واقع آی پی سروری که از بیرون میخواهیم به آن متصل شویم را وارد میکنیم. در قسمت External Service Port در واقع آی پی میخواهیم وارد کنیم را مشخص میکنیم. و در قسمت Map to IPv4 میشویم در قسمت Map to IPv4 همان پورت مورد نظری که از بیرون میخواهیم وارد کنیم را مشخص میکنیم. و در قسمت Map to IPv4 میشویم در قسمت Service Port همان پورت مورد نظری که از بیرون میخواهیم وارد کنیم را مشخص میکنیم. و در قسمت Map to IPv4 میشویم در قسمت Service Port همان پورت مورد نظری که از بیرون

GVMEVIFJPLYKIA5 -	≡ Q	>_ ⊙ • 4 <mark>0</mark> • ⊗ admin
② Dashboard >	Virtual New DNAT & Virtual IP	
+ Network >		
🛃 Policy & Objects 🛛 🗸 🗸	+ Cra	FortiGate
Firewall Policy	Name	III FGVMEVIFJPLYKIAS
Central SNAT	Comments Write a comment	Statistics (since last reset)
DoS Policy	Color 🖀 Change	ID
Addresses	Status 🜑	Lottured N/A
Internet Service Database		
Services	Network	First used N/A
Schedules	Interface 💌 port1 💌	Hit count 0
DNAT & Virtual IPs 🏠	Type Static NAT FQDN	🗊 Clear Counters
IP Pools	Source interface filter	
Protocol Options	External IP address/range () 10.10.10.10	Additional Information
Traffic Shaping	Map to	API Preview
A Security Profiles >	IPv4 address/range 192.168.1.10	
□ VPN >		O Online Guides
$\stackrel{{}_\sim}{\simeq}$ User & Authentication $\rightarrow$	Optional Filters	Kelevant Documentation     Video Tutorials
© System →	Port Forwarding	
Security Fabric >	Protected TCD LIDD SCTD LIDNO	Ra Fortinet Community
🔳 Log & Report 💦 >		
NEW IN	Port Mapping Type One to one Many to many	
	External service port ① 2323	
	Map to IPv4 port 3389	

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

**E** FGVMEVIEIP Create New Policy Additional Information Policy & Objects Name 🕟 Allow-DNAT @ API Preview Schedule always Central SNAT ⑦ Online Guides ACCEPT O DENY Action 🔲 Relevant Documentation 🗹 -Incoming interface mort1 D1 Video Tutorials 🖒 Addres D1 Consolidated Policy Configuration [7] Outgoing interface 🛛 🕅 port3 -P2 Fortinet Community Source & Destination Showlogic Ø Join the Discussion ∅ Schedules DNAT & Virtual IPs 4 all Source IP Pools User/group Destination S User & Authentication Service 🕸 System Firewall/Network Options A Security Fabric E Log & Report Inspection mode Flow-based Proxy-based Central NAT is enabled so NAT settings from matching <u>Central SNAT</u>
 policies will be applied



# 6 SSL Inspection

امروزه اکثر ترافیک هایی ما که در شبکه ما جا به جا می شوند، 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 می شوند و ترافیک هایی که وارد شبکه می شوند.

در این بحث، مواردی همچون SSL Inspection کاربران هستند، سرتیفیکیت دریافت می کند. و هرترافیکی که از شبکه خارج و یا وارد می شود را با سرتیفیکیت فایروال از یک CA داخلی یا خارجی که Trusted کاربران هستند، سرتیفیکیت دریافت می کند. و هرترافیکی که از شبکه خارج و یا وارد می شود را با سرتیفیکیت خود امضا و موارد رمزنگاری را با کلیدهای Public و Private خود انجام می دهد. تمام ترافیک های رمز شده ابتدا به فایروال داده می شود و فایورال ترافیک را از طرف خود به مقصد مورد نظر می رساند. 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 می کند.



## 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.

lole services	Description
Certification Authority     Certificate Enrollment Policy Web Service     Certificate Enrollment Web Service     Certification Authority Web Enrollment     Network Device Enrollment Service     Online Responder	Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.

۱. سرتيفيكيت CA را از طريق گروپ پاليسي روي تمام سيستم ها بايد نصب و در حالت Trusted قرار دهيم.

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 می شویم. 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.

## **Fortigate Firewall**



FGVMEVIFJPLYKIA5 🔹										Q1-	
⑦ Dashboard →	+ Create/Import *	/ Edit	17 Delete	• View Details	& Download	Search	0				
↔ Network >	Certificate										
Policy & Objects >	Generate CSP			Subject \$		Ą	Comments 🗘	Issuer ≑	Expires 🗘	Status 🕏	Source 4
合 Security Profiles >	Generate Colt	e 🛛							_	_	<u>^</u>
□ VPN >	CA Certificate	C	= US, ST = Calif	ornia, L = Sunnyvale	, O = Fortinet, OU	= Certificat	This is the default CA certificate the SSL Inspection will use when g	Fortinet	2034/08/31 08:07:32	🛛 Valid	Fact
≗ User & Authentication →	Remote Certificate	sted C :	= US, ST = Califo	ornia, L = Sunnyvale	, O = Fortinet, OU	= Certificat	This is the default CA certificate the SSL Inspection will use when g	Fortinet	2034/08/26 03:26:03	<ul> <li>Valid</li> </ul>	Fact/
System ~	CRL	в									
Administrators	Fortinet_Factory	C	= US, ST = Calif	ornia, L = Sunnyvale	, O = Fortinet, OU	= FortiGate	This certificate is the same on every unit (not unique). It has been si	Fortinet	2038/01/18 19:14:07	🛛 Valid	Fact
Admin Profiles	Fortinet_GUI_Serv	er C	= US, ST = Calife	ornia, L = Sunnyvale	, O = Fortinet Ltd.,	OU = Forti	This is the default CA certificate the SSL Inspection will use when g	Fortinet	2026/12/03 07:08:10	🛛 Valid	Fact
Firmware & Registration	Fortinet_SSL	C	= US, ST = Calife	ornia, L = Sunnyvale	, O = Fortinet, OU	= FortiGate	This certificate is embedded in the hardware at the factory and is u	Fortinet	2026/12/03 07:07:32	🛛 Valid	Fact
Settings	Fortinet_SSL_DSA:	1024 C	= US, ST = Calife	ornia, L = Sunnyvale	, O = Fortinet, OU	= FortiGate	This certificate is embedded in the hardware at the factory and is u	Fortinet	2026/12/03 07:07:25	🗢 Valid	Fact/
HA	Fortinet_SSL_DSA:	2048 C	= US, ST = Calife	ornia, L = Sunnyvale	, O = Fortinet, OU	= FortiGate	This certificate is embedded in the hardware at the factory and is u	Fortinet	2026/12/03 07:07:25	🗢 Valid	Fact/
SNMP	Fortinet_SSL_ECD:	SA256 C	= US, ST = Calife	ornia, L = Sunnyvale	, O = Fortinet, OU	= FortiGate	This certificate is embedded in the hardware at the factory and is u	Fortinet	2026/12/03 07:07:25	🛛 Valid	Fact/
Replacement Messages	Fortinet_SSL_ECD:	SA384 C	= US, ST = Califo	ornia, L = Sunnyvale	, O = Fortinet, OU	= FortiGate	This certificate is embedded in the hardware at the factory and is u	Fortinet	2026/12/03 07:07:25	🛛 Valid	Fact/
FortiGuard	Fortinet_SSL_ECD:	SA521 C	= US, ST = Califo	ornia, L = Sunnyvale	, O = Fortinet, OU	= FortiGate	This certificate is embedded in the hardware at the factory and is u	Fortinet	2026/12/03 07:07:25	🛛 Valid	Fact
Feature Visibility	Fortinet_SSL_ED44	48 C =	= US, ST = Califo	ornia, L = Sunnyvale	, O = Fortinet, OU	= FortiGate	This certificate is embedded in the hardware at the factory and is u	Fortinet	2026/12/03 07:07:25	🛛 Valid	Fact/
Certificates 🏠	Fortinet_SSL_ED25	5519 C :	= US, ST = Califo	ornia, L = Sunnyvale	, O = Fortinet, OU	= FortiGate	This certificate is embedded in the hardware at the factory and is u	Fortinet	2026/12/03 07:07:25	🛛 Valid	Fact/
Security Fabric >	Fortinet_SSL_RSA:	1024 C :	= US, ST = Califo	ornia, L = Sunnyvale	, O = Fortinet, OU	= FortiGate	This certificate is embedded in the hardware at the factory and is u	Fortinet	2026/12/03 07:07:25	🛛 Valid	Fact
🖻 Log & Report 💦 🗧 🗧	Fortinet_SSL_RSA2	2048 C	= US, ST = Calif	ornia, L = Sunnyvale	, O = Fortinet, OU	= FortiGate	This certificate is embedded in the hardware at the factory and is u	Fortinet	2026/12/03 07:07:25	🛛 Valid	Fact
	Fortinet_SSL_RSA4	4096 C	= US, ST = Calif	ornia, L = Sunnyvale	, O = Fortinet, OU	= FortiGate	This certificate is embedded in the hardware at the factory and is u	Fortinet	2026/12/03 07:07:25	🛛 Valid	Fact/
	- Remote CA Certifi	icate ③									
	Fortinet_CA	C	= US, ST = Calif	ornia, L = Sunnyvale	, O = Fortinet, OU	= Certificat		Fortinet	2038/01/19 14:34:39	🛛 Valid	Fact
	Fortinet_CA2	C	= US, ST = Calif	ornia, L = Sunnyvale	, O = Fortinet, OU	= Certificat		Fortinet	2056/05/27 13:27:39	🛛 Valid	Fact
	4	-	110 CT - C+114		0.5-2-2-01	C+16+		F	0057/05/07 40:40:00	a vata	*

FGVMEVIFJPLYKIAS	r ≡ Q,	>_ ⑦ ▼     Q <mark>9</mark> ▼     ® admin
Ø Dashboard	Generate Certificate Signing Request	
Network     Policy & Objects     Society & Objects     Ven     Ven     Ven     User & Authentication     System     Administrators	Certificate Name Subject Information ID Type Host IP Domain Name E-Mail Domain Name	FortiGate  FGYMEV/FJPIYKIA5  Additional Information  Additional Information  O API Preview  O Online Guides
Admin Profiles Firmware & Registration Settings HA SNIMP Renlacement Messages	Optional Information Organization Unit Organization Organization Locality(City)	Relevant Documentation Video Tutorials Pa Fortinet Community O Join the Discussion
FortiGuard Feature Visibility Certificates © Security Fabric L2. Log & Report	State / Province Country / Region E-Mail Subject Alternative Name Password for private key Key Type RSA Key Size S12 Bit	
	Enrollment Method File Based Online SCEP	





T SMAL



# 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 می شوند را روی فایروال آپلود می کنیم. در این حالت تمام ترافیکی که از بیرون وارد می شود را فایروال می تواند 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 می شویم و سرتیفیکیت از نوع PKCS را ایمپورت می کنیم.

FGVMEVIFJPLYKIA5 -	= Q						<b>₽1</b> -	🖲 admin =
⑦ Dashboard >	+ 00	Create Certificate						×
$\oplus$ Network $>$	( reie		-	-				
🛃 Policy & Objects 💦 🗧 🗧			O	2				
合 Security Profiles >	E Loca	Choo	ose Method	Certificate Details	Create Certificate	Revie	ew.	
$\Box$ VPN $\rightarrow$	E Loca							
🔗 User & Authentication 💦 >	📄 Rem	A Import Certificate						
System		w						
Administrators		Type Local Certificate	PKCS #12 Certificate Certificate					
Admin Profiles								
Firmware & Registration		Certificate with key file						
Settings			A					
HA								
SNMP			Upload File					
Replacement Messages			Click to select of drop life here					
FortiGuard								
Feature Visibility		Password		Ó				
Certificates 🏠		Confirm password		0				
Security Fabric >								
💷 Log & Report 💦 🔷 🗧								

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 می شود.

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.

🕞 FGVMEVIFJPLYKIA5 🛛 👻								
<pre>② Dashboard &gt;</pre>	+ Create/Import *	R Edit	😡 View Details 🗼 Downlo	Search		0		
+ Network >	Certificate			Jearen		~		
Policy & Objects >	Generate CSR	Subject ♀	Comments 🗢	Issuer 🗘	Expires 🗘	Status ≑	Source 🗢	Ref. ≎
Security Profiles		e 2						
$\Box$ VPN $\rightarrow$	CA Certificate	D						
😤 User & Authentication 💦 >	Remote Certificate	cate ③						
System ~	CRL							
Administrators								
Admin Profiles								
Firmware & Registration								
Settings								
HA								
SNMP								
Replacement Messages								
FortiGuard								
Feature Visibility								
Certificates 😭								
Security Fabric >								
Log & Report >								



🕞 FGVMEVIFJPLYKIA5 🔹	≡ Q				>	⊙-	<b>₽1</b> •	🛞 admin 🕶
$\textcircled{O}$ Dashboard $\rightarrow$	(+ 0	Import C	A Certificate					×
↔ Network >	C. C.C.	-	-					
Policy & Objects >		Туре	Online SCEP	file				
Security Profiles	E Loca	Upload	O Upload					
□ VPN >	E Loca							
${_\sim}$ User & Authentication $\rightarrow$	🔄 Ren							
System ~								
Administrators								
Admin Profiles								
Firmware & Registration								
Settings								
HA								
SNMP								
Replacement Messages								
FortiGuard								
Feature Visibility								
Certificates 🏠								
Security Fabric >								
Log & Report >								

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

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.

US FOUNEVIEURIAS		> • • 4 • • • • • • • • • • • • • •
② Dashboard	Edit SSL/SSH Inspection Profile	×
Hetwork	FortiGate	
A Security Profiles	Name custom-deep-inspection Custom-deep-inspection	
AntiVirus Web Filter	Comments Customizable deep inspection profile 37/255	
DNS Filter	SSL Inspection Options % References	
Application Control	Enable SSL inspection of Multiple Clients Connecting to Multiple Servers 2- Edit in CLI Protecting SSL Server	1
File Filter	Inspection method SSL Certificate Inspection Full SSL Inspection	2
SSL/SSH Inspection	CAcertificate ▲     Fortinet_CA_SSL     SL     Download	j.
Application Signatures	Blocked certificates 🛈 Allow Block 🔳 View Blocked Certificates 🖓 Fortinet Community	
IPS Signatures Web Rating Overrides Web Profile Overrides	Untrusted SSL certificates Allow Block Ignore W Trusted CAs List O Join the Discussion C Server certificate SNI check () Enable Strict Disable	
GPRS Tunneling Protocol	Enforce SSL cipher compliance	
	Enforce SSL negotiation compliance	
S User & Authentication	RPC over HTTPS O MAPI over HTTPS O	
ී System		
Security Fabric	Protocol Port Mapping	
E Log & Report	Inspect all ports         Image: Constraint of the second sec	

# 7 Firewall Filtering

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

#### 7.1 Web Filtering

با این قابلیت در فایروال فورتیگیت می توانیم URL ها را فیلتر کنیم. و اجازه دسترسی بدهیم یا ندهیم. طبق معمول اگر وارد مسیر Security Profiles > Web Filter شویم. می توانیم 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 پیش فرض فایروال انجام داده است. که هر بخش شامل پنج حالت ,Allow, Monitor, Block, Warning می باشد. Authenticate می باشد.

در بخش سوم، می توانیم 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 می توانیم 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.



Web Filter 🏠	11 100		> Edit in CLI
Video Filter	-	Allow users to override blocked categories	
DNSFilter	De De	Search Engines	Online Guides
Application Control Intrusion Prevention		Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex 🍅	Relevant Documentation C U Video Tutorials C
File Filter		Static URL Filter	Ra Fortinet Community
SSL/SSH Inspection		Block invalid URLs	
Application Signatures IPS Signatures Web Rating Overrides		UR, Filter  Block malcous URLs discovered by FortiSandbox  Content Filter	
Web Profile Overrides		Rating Options	
GPRS Tunneling Protocol □ VPN Suser & Authentication		Behavlor when FortiSuard is unreachable ① Allow all websites Block all websites Rate URLs by domain and IP Address ①	
System >		Praxy Options	
Security Fabric >		HTTP POST Action Allow Block	
l≞ Log&Report →		Remove Cookies ()	
	O Saca	OK Cancel	

اگر بخواهیم در Category های خود مثلا Allow یا Deny انجام بدهیم. وارد منوی Web Rating Override میشویم. و از قسمت New 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.

FGVMEVIFJPLYKIAS +	≣ Q,		>_ @	•	<li>2) * (8) admin</li>	
⊘ Dashboard >	Override N	New Web Rating Override				×
Network >     Network >     Policy & Objects >     Security Profiles >	+ Cre	URL youtube.com Lookup rating Gregories (Gregories)				
AntiVirus Web Filter Video Filter		Warning: This device is not licensed for the FortiGuard web filtering Service:  Additional information  Additional information  Additional information  Additional information				
DNS Filter Application Control		Comments Write a comment				
Intrusion Prevention File Filter SSL/SSH Inspection		Overroe to				
Application Signatures IPS Signatures		concretely, (not work				
Web Rating Overrides						
은 VPN > 온 User & Authentication >						
<ul> <li>⊗ System &gt;</li> <li>Ø Security Fabric &gt;</li> <li>E. Log &amp; Report &gt;</li> </ul>						

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.

FGVMEVIFJPLYKIA5 +	≡ Q.	>_ ⊙• Q <mark>2</mark> • ®admin•
② Dashboard >	+ Cre New Administrative Override	×
+ Network >		FartiCate
Policy & Objects		
🖒 Security Profiles 🛛 🗸	Scoperange User group Source IP	
AntiVirus	User	Additional information
Web Filter	Original profile	API Preview
Video Filter	New profile	
DNS Filter	Expires 2024-09-07	Online Guides
Application Control	Status Enable Disable	Relevant Documentation
Intrusion Prevention		La Video lutoriais 🔄
File Filter		R1 Fortinet Community
SSL/SSH Inspection		
Application Signatures		
IPS Signatures		
Web Rating Overrides		
Web Profile Overrides 🎲		
GPRS Tunneling Protocol		
□ VPN >		
System     Sys		
Security Fabric >		
Log & Report >		



# 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 می توانیم 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 می کند.

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 می توانیم بصورت استاتیک، Domain Filter را انجام دهیم. و دامین هایی که مد نظر ما است را Deny و یا Allow و یا کنیم.

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

🕞 FGVMEVIFJPLYKIA5 🛛 👻	≡ Q					(8) admin +
② Dashboard >	1000	New DNS Filter Profile				×
+ Network >	L + cre	Name				
💄 Policy & Objects 💦 >	0	Comments	Comments	FortiGate		
🔒 Security Profiles 🛛 🗸 🗸		Dedirect beteet CSC requests to Plack Partal	Comments 0/255	R FGVMEVIFJPLYKIA5		
AntiVirus		Redirect bothet Calc requests to block Portai		Additional Information		
Web Filter			0 domains in <u>botnet package</u>	(D) ADI Davidaria		
Video Filter			<ul> <li>Botnet package update unavailable, AntiVirus subscription not found</li> </ul>	APTPreview		
DNS Filter 合			iouni.	⑦ Online Guides		
Application Control		Enforce 'Safe Search' on Google, Bing, YouTube		Relevant Documentation		
Intrusion Prevention				🗅 Video Tutorials 🖸		
File Filter		C FortiGuard Category Based Filter		R Fortinet Community		
SSL/SSH Inspection		Allow Monitor Redirect to Bl	ock Portal	🔎 Join the Discussion 🔀		
Application Signatures		Name 🏶 Action	•			
IPS Signatures		Adult/Mature Content 13 0 15				
Web Rating Overrides		Alternative Reliefs				
Web Profile Overrides		Abertian Abertian				
GPRS Tunneling Protocol		Other Adult Materials				
		Adverse Organizations Organizations				
≗ User & Authentication >		Advocacy organizations Oriente				
System >		Gamoing Wonito				
Security Fabric >		Persegraphy O Monito				
E Log & Report >		Pornograpny @ Monito				
		Dating @ Monito				
			0% 😰			-
SSL/SSH Inspection				○ Join the Discussion 17		
Application Signatures		Static Domain Filter				
IPS Signatures		Domain Filter 🕥				
Web Rating Overrides		External IP Block Lists 🕥				
Web Profile Overrides		DNS Translation 🕕 🕥				
GPRS Tunneling Protocol		Ontions				
□ VPN >						
		Kedirect Portai IP	Use Fortiguard Default Specify			
영 System >			0.0.0			
Security Fabric >		Allow DNS requests when a rating error occurs				
I≝ Log & Report >		Log all DNS queries and responses				
		Strip and ypted chemic reno service parameters				
	4 <u>-</u>					Ŧ



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.

🕞 FGVMEVIFJPLYKIA5 🛛 🔫	= Q							🛞 admin 🕶
② Dashboard	1936	Edit SSL/SSH Inspection Pr	ofile					×
+ Network	1.70	MAPLOVER HITPS						
🛃 Policy & Objects					Forti	lGate		
🖞 Security Profiles	. 0	Protocol Port Mapping				FGVMEVIFJPLYKIA5		
AntiVirus	0	Inspect all ports 🕥			Addi	itional Information		
Web Filter	0	HTTPS C 443				API Preview		
Video Filter		SMTPS C 465				Pafarancar		
DNS Filter		POP35 0 995				o References		_
Application Control	0				2	Edit in CLI		
Intrusion Prevention		IMAPS 0 995			3	Online Guides		
File Filter		FTPS 0 990				Relevant Documentation		
SSL/SSH Inspection 🎸	2	DNS over TLS () 853			C <sup>2</sup>	Video Tutorials 🖸		
Application Signatures		HTTD/2	Pupage Plack		Q. F	Fortinet Community		
IPS Signatures		HIINS III	ecc bypass block		0	Join the Discussion 12		
Web Rating Overrides		DNS over QUIC Insp	ect Bypass Block					
Web Profile Overrides								
GPRS Tunneling Protocol		Exempt from SSL Inspectio	'n					
L VPN		Reputable websites 🕕 🖸						
😤 User & Authentication		Web categories	Finance and Banking	×				
③ System			Health and Wellness	×				
Security Fabric			-					
📃 Log & Report		Addresses	adobe	×				
			android	×				
			apple	×				
	0.0						 _	v
	0		ОК	- 4 C - 1	Cancel			

# 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 توینتر، 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 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

برای شروع، وارد منوی Security Profiles > Application Control می شویم 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 ميتوانيم اپليكيشن هاي دلخواه خود را Allow و يا Deny كنيم.



🕞 FGVMEVIFJPLYKIA5 🛛 🔹	≡ Q								>_ @• 4 <mark>2</mark>	🔹 🛞 admin 🕶
② Dashboard >	( de real	New App	Add Nev	v Override						×
+ Network >	( T G B			-						
💄 Policy & Objects 💦 🔷 👌		0.	Туре	Application	Filter					<u>^</u>
🔒 Security Profiles 🛛 🗸		•••		At least one e	ntry must be added.					
AntiVirus	0	•	Action	Slock •	L					÷
Web Filter		•		S Block						
Video Filter		•	Q	Monitor						×Q
DNS Filter				Allow	Name 🖨	Category \$	Technology 🏶	Popularity 🖨	Risk	¢\$
Application Control 🏠			- Ap	plication signa	ture (3/2414)					
Intrusion Prevention		Applic		Twitter		C Social Media	Browser-Based	*****		
File Filter		E	0	Tulanu			Brewere Based			
SSL/SSH Inspection		Ľ		Twitter_i	login CS	C Social Media	browser-based	The set set set		
Application Signatures		Pr		Twitter_I	Post (2)	□ Social Media	Browser-Based	<b>常常常</b> 容容		
IPS Signatures										
Web Rating Overrides										
Web Profile Overrides										
GPRS Tunneling Protocol										
□ VPN →		-								
		Option								
≥ System >		Block								
Security Fabric >		Allowa								
E Log & Report >		Replac								

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 آی پی 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 می شویم. و یک یوزر بصورت لوکال ایجاد می کنیم. یک ویزارد بصورت زیر را باید انجام دهیم. در مرحله اول نوع یوزر را انتخاب می کنیم. که این یوزر از نوع لوکال و یا در اکتیودایرکتوری و یا ... باشد. در مرحله دوم یوزرنیم و پسورد را وارد می کنیم. در مرحله سوم مشخص می کنیم که احراز هویت یوزر در هنگام ورود یک مرحله ای یا دو مرحله ای باشد. این کار برای ایجاد امنیت بیشتر انجام می شود. در مرحله چهارم اگر می خواهیم این یوزر عضو گروهی خاص باشد را مشخص می کنیم. و تعیین می کنیم آیا این یوزر فعال باشد و با غیر فعال.







به همین صورت یوزرها و گروههای مورد نظر خود را ایجاد میکنیم. در نهایت وارد بخش Firewall Policy می شویم 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 می شویم و موارد را بصورت زیر تنظیم میکنیم.

#### **Fortigate Firewall**



🕞 FGVMEVIFJPLYKIA5 🛛 👻	≡ Q.	>_ ⊙ •     Q <b>2</b> •     ® admin •
② Dashboard >	Edit LDAP Server	×
+ Network >		
🛃 Policy & Objects 💦 >	FortiGate	
Security Profiles	Name ITPHP REVERSES	
□ VPN >	Server IP/Name 192.168.1.10 Additional information	
$\stackrel{\scriptstyle >}{\simeq}$ User & Authentication $\qquad \qquad \lor$	Server Port 389 O API Preview	
User Definition	Common Name Identifier cn	
User Groups	Distantished Name and a little designal Proving	
Guest Management	Online Guides     Online Guides	
LDAP Servers ☆	Exchange server  Relevant Documentation  Relevant Documentation	
RADIUS Servers	Bind Type Simple Anonymous Resultar DI Video Tutorials [2]	
Single Sign-On	Username administrator@itphp.loca 🖓 Fortinet Community	
Authentication Settings	Password Q Join the Discussion 12	
FortiTokens	Secure Connection	
System >	Test Connectivity	
Security Fabric >	Test User Credentials	
Log & Report >		

احراز هويت 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 سرویس های این نرم افزار را دارد، وارد میکنیم.

<b>漫</b> — — — — — — — — — — — — — — — — — — —	Fortinet Single Sign On Agent 📃 🗖 🗙
The user account on which Please input the user accou	you want to launch the service Int's name and password. This must be an administrator user.
User name must be in form please enter .\UserName.	DomainName\UserName. If you want to use local user account,
User Name:	.\Administrator
Password:	•••••
	Back Next Cancel



谩	Fortinet Single S	Sign On Agent	: [	- □	x
Install Options					
Fortinet Single Sign Or NTLM authentication re	Agent could be set up to equests from Fortigates.	o monitor user logor Select the proper o	n events and options below	l/or servin	g
Monitor User logo	on events and send the ir	nformation to Fortio	Gate.		
Serve NTLM aut	entication requests comi	ng from FortiGate.			
Please select the acce	ss method of Windows Di	rectory			
• Standard(e.g dor	main \user)				
-Select this option	for easy setup, works for	r most situations			
<ul> <li>Advanced(e.g. C</li> </ul>	N=user,OU=Sales,DC=d	lomain,DC=com)			
-Select this option information from F	if you setup LDAP acces FortiGate	s to Windows AD to	o retrieve use	er/group	
		Back N	lext	Cance	el

حالا بايد وارد مراحل نصب DC Agent شويم، در اينجا اطلاعات DC را ميدهيم.

Fortinet Single Sign On Agent - Install DC Agent 🛛 🗶
Welcome to the DC Agent installation wizard. This wizard will install DC Agent on the Domain Controllers in your domain.
First please confirm the Collector Agent address and listening port.
Collector Agent
Collector Agent IP address: 172.31.0.10
Collector Agent IPv6 address:
Collector Agent listening port: 8002
Note: You need to have administrator access to the domain controller in order to install the DC Agent!
< Back Next > Cancel Help



## **Fortigate Firewall**



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

- 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 ری استارت مجدد دارد.
- در صورت انتخاب Polling Mode شما می توانید از NetAPI و یا Event Log برای ارتباط استفاده کنید که هر دو query ها را هر ۱۰ ثانیه ارسال می کنند، در NetAPI سرعت بیشتر است ولی برخی از log ها ارسال نمی شود ولی در Event log polling تمام Log ها ارسال می شود برای همین کندتر می باشد.

	Fortinet Single Sign On Agent - Install DC Agent
Select	domain controllers for monitoring user logon event: Uncheck All
🗹 itp	php\srv.itphp.local
Work	ing Mode
	C Agent Mode (Click Next will start the installation of DC Agent)
	Check Windows Security Event Logs
	Fortinet Single Sign On Agent - Install DC Agent
Select d	omain controllers for monitoring user logon event: Uncheck All
🗹 itp	hp\srv.itphp.local
	installdcagent
2	DC Agent is successfully installed on domain controller:
	You must report the domain controller to monitor user logon event
	Do you want to reboot



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

Monitoring user logon events Support NTLM authentication	Collector Agent Status: RUNNING
Listening ports	Common Tasks
FortiGate: 8000 FortiGate SSL: 8001 DC Agent: 8002	Show Service Status
Enable SSL DCAgent SSL: 8003 Preshared key:	Show Monitored DCs
Logging	
Log level: Warning V Log file size limit(MB): 10 View Log	Show Logon Users
Log logon events in separate logs View Logon Events	Select Domains To Monitor
Authentication	Set Directory Access Information
Hequire authenticated connection from Fortigate     Fassword	Set Group Filters
I imers Workstation verificiaterval (minutes): 5	
Dead extru times ut interval (minutes):	Set Ignore User List
IP address change verify interval (seconds): 60	Sync Configuration With Other Agents
Cache user group lookup result Cache expire in (minutes): 60 Clear Group Cache	Export Configuration

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 سرویس های RDP و RDP به سرور SDC 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 fortinet Single Sign-On و را کلیک می کنیم و Create New می شویم و Create New را کلیک می کنیم و Action Sigle Sign-On می شود. حالا را نتخاب می کنیم.

FortiGate VM64-KVM FW-		Q 🔹 🛌 🚺 🥑 🕘 admin =
CorrtiGate VM64-KVM PW-     Dashboard     Dashboard     Security Fabric     Physical Topology     Logical Topology     Security Rating     Automation     Fabric Connectors     External Connectors     System     Sosystem     Sosystem     Sosystem     Sosystem     Sosystem     Solution     Policy & Objects     Security Profiles     Security Profiles     Solution     User & Authentication     Solution     Log & Report	Edit External Connector Endpoint/Identity  Endpoint/Identity  FSSO Agent on Windows AD  Connector Settings Name  FSSO Trusted SSL certificate  Trusted SSL certificate  Collector Agent Trusted SSL certificate  Frimary FSSO agent  Trusted SSL certificate  For Collector Agent Edit  DAP server  Search filter  Edit  Edit Edit	Q + >       Q + A       E admin-         Status       Image: Consector Setup Guides       Image: Consector Setup Guides         Image: Amazon Web Service of a consector Setup Guides       Image: Consector Setup Guides         Image: Consector Consector Generation       Image: Consector Setup Guides         Image: Consector Consector Generation       Image: Consector Consector Generation         Image: Consector Consector Generation       Image: Consector Consector Generation         Image: Consector Consector Generation       Image: Consector Consector Generation         Image: Consector Consector Consector Generation       Image: Consector Consector Generation         Image: Consector Consec
	F5SO groups will be populated in the background.     Apply & Refresh OK Cance	, v


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 User group source میباشد، 172.31.0.10 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.

FortiGate VM64-KVM					Q >_ [] @- 🔎 🞑 admin-
Dashboard	Edit Policy				
☆ Security Fabric >			Select Entries	¥ ID	^
+ Network >	Name 0	Client-Internet	Address Hose Internet Se	- 1	
System >	Incoming Interface	Inside (port1)	Address Oser Internet Se	Create	
Policy & Objects	Outgoing Interface	ISP1 (port4)	C Search	1 hour(s) ago	
Firewall Policy	Source	🖽 all 🛛 🗙	CN=Domain Controllers,CN=Us	sers,D	
Authentication Rules		E CN=Internet-FSSO,CN=Users,DC ×	CN=Domain Guests,CN=Users,I	DC=ne First used	
ID-4 D=C D=ll=+		+	CN=Domain Osers, CN=Osers, D	nc=nex 1 nour(s) ago	
IPv4 Dos Policy	Destination	🖾 all 🛛 🗙	CN=Enterprise Read-only Doma	ala Cou Hit count	
Addresses		+	CN=Event Log Readers.CN=Buil	20	
Internet Service Database	Schedule	To always	CN=Group Policy Creator Owne	ers,CN	
Services	Service	ALL ×	CN=Guests,CN=Builtin,DC=nex	Active sessions	
Schedules		+	CN=Hyper-V Administrators,CN	N=Buil	
Virtual IPs	Action	✓ ACCEPT Ø DENY	CN=IIS_IUSRS,CN=Builtin,DC=r	nextad 1minutationage now	
IP Pools	and the second s		CN=Incoming Forest Trust Build	ders,Cf	
Directored Options	Inspection Mode	Flow-based Proxy-based	CN=Internet-FSSO,CN=Users,D	OC=ne: Total bytes	
Protocol Options			E CN=Network Configuration Ope	erator	
Traffic Shapers	Firewall / Network C	Options	CN=Performance Log Users,CN	EBuilt Current bandwidth	
Traffic Shaping Policy	NAT	0	CN=Performance Monitor User	s,CN= 0 B/s	
Traffic Shaping Profile	IP Pool Configuration	Use Outgoing Interface Address Use Dynamic IP Pool	CN=Pre-Windows 2000 Compa	itible A	
	Preserve Source Por	t <b>O</b>	CN=Print Operators,CN=Builtin	n,DC=r	
	Protocol Ontions	default 🔹 🥒	CN=Protected Users,CN=Users,	s,DC≠n	
Ilear C Authentication	Trotocor options		CN=RAS and IAS Servers,CN=U	Isers,D ⑦ Documentation	
Oser & Addrendcadori	Security Profiles		CN=RDS Endpoint Servers,CN=	Bulltir 🖉 Online Help 🗹	
Log & Report >	occurry r romes		CN=RDS Management Servers,0	CN=Bt Video Tutoriais C	
	AntiVirus		CN=RDS Remote Access Server	S,CN=	
	Web Filter		CN=Read-only Domain Control	lers,Cr	
	DNS Filter	0	CN=Remote Desktop Users,CN=	=Build	
	Application Control	0	CN=Replicator CN=Ruiltin DC=	sjulin-i	
	IPS			no. V	
	File Filter			,	
			Close		
	SSL Inspection	no-inspection			v

حالا FSSO به اکتیودایرکتوری متصل شده است و می توانیم از آن استفاده کنیم، همانطور که مشخص است یوزر ها و گروه های ما را شناسایی کرده است. در آخر نیز می توانیم 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 فایل های مخرب را دانلود کنند، جلوگیری کند. برای استفاده از این قابلیت هم میتوانیم یک Security Profile ایجاد کنیم و از آن در پالیسی های خود بهرهمند شویم. برای این کار وارد بخش Flow Base میشویم. دو حالت Proxy Base و Proxy Base است که Proxy حالت بهتری است. قابلیت های زیادی دارد که بسیار ساده است.

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

🕞 FGVMEVIFJPLYKIA5 🔹 🔻	≡ Q			>_ ©	-	🛞 admin 🝷
② Dashboard >		Edit AntiVirus Profile				×
$\Leftrightarrow$ Network $>$	(+ cie					
Policy & Objects >		Name default	FortiGate			
🗅 Security Profiles 🛛 🗸		Comments Scan files and block viruses.	B FGVMEVIFJPLYKIA5			
AntiVirus 🏠		AntiVirus scan 🛈 💽 Block Monitor	Additional Information			
Web Filter Video Filter		Feature set Flow-based Proxy-based	API Preview     No References			_
Application Control		Inspected Protocols	>_ Edit in CLI			- 1
Intrusion Prevention File Filter		SMTP C	FortiSandbox			
SSL/SSH Inspection		IMAP C	Understanding Inline Block Feature			- 1
Application Signatures		FTP O	⑦ Online Guides			
IPS Signatures		CIFS OF	Relevant Documentation			
Web Rating Overrides		APT Protection Options	🗅 Video Tutorials 🖸			
Web Profile Overrides		Treat Windows executables	Ra Fortinet Community			
GPRS Tunneling Protocol		In email attachments as viruses	♀ Join the Discussion			
LI VPN >		Include mobile malware protection				
Subser & Authentication		Quarantine (1)				
System						
W Security Fabric >		Virus Outbreak Prevention ()				
Log & Report →		Use FortiGuard outbreak prevention database 🛕 🕥				
		Use external malware block list				
		Use EMS threat feed (i)				Ŧ
	<ul> <li>Secu</li> </ul>	OK Cancel				



#### 10 IPS/WAF

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

FGVMEVIFJPLYKIA5 •	≡ Q					>_ @•	¢ <mark>2</mark> -	🖲 admin 🕶
$\oslash$ Dashboard $>$	+ Cr	Edit IPS Sensor						×
↔ Network >					Section:			
Policy & Objects >			Circle i					
🛆 Security Profiles 🛛 🗸		Name	all_default		IE FGVMEVIFJPLYKIA5			
AntiVirus		Comments	All predefined signatures with		IPS Signatures			
Web Filter			derault setting. // 47/2	255	I View IPS Signatures			
Video Filter		BIOCK Malicious URLS (	)					
DNS Filter		IPS Signatures and Filter	5		Additional Information			
Application Control					API Preview			
Intrusion Prevention 🏠		+Create New	Edit 🗍 Delete		% References			
File Filter		Details Exempt II	Ps Action Packet Logging		>_ Edit in CLI			
SSL/SSH Inspection			③ Default O Disabled					
Application Signatures			•		⑦ Online Guides			
IPS Signatures					Relevant Documentation			
Web Rating Overrides			0					
Web Profile Overrides					Ra Fortinet Community			
GPRS Tunneling Protocol		Detect CCC			Din the Discussion I and a second			
$\Box$ VPN $\rightarrow$		Dotnet C&C						
$\stackrel{{}_\sim}{\simeq}$ User & Authentication $\rightarrow$		Scan Outgoing Connection	ons to Botnet Sites Disable Block	Monitor				
In System →								
Security Fabric >								
E Log & Report >								

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. می توانیم تنظیمات مربوط به این بخش را انجام دهیم. معمولا WAF را برای ترافیکهایی که از بیرون به داخل می آیند، قعال می کنیم. دقت کنید که WAF فقط در حالت Proxy روی فایروال فورتیگیت عمل می کند.

🕞 FGVMEVIFJPLYKIA5 🛛 👻	= Q					
② Dashboard >	+ Cre	New Web Applic	cation Firewall Profile			
↔ Network >						
Policy & Objects >		Nama				
Security Profiles ~		Name				
AntiVirus		Comments	Write a comment	0/1023		
Web Filter		<i></i>				
Video Filter		Signatures				
DNS Filter		🖉 Edit	Search			Q
Application Control		Status	Signature	Action	Severity	
Intrusion Prevention		- 0100010	erossone sentrus (entenses	, ,		
File Filter		Enable	SQL Injection	8 Block		
Web Application Firewall		🔕 Disable	SQL Injection (Extended)	Allow		
SSL/SSH Inspection		🔕 Disable	Generic Attacks	8 Block		
Application Signatures		🔕 Disable	Generic Attacks(Extended)	Allow		
IPS Signatures		🙁 Disable	Trojans	🙁 Block		
Web Rating Overrides		Enable	Information Disclosure	Allow		
Web Profile Overrides		Enable	Known Exploits	8 Block		
GPRS Tunneling Protocol		Enable	Credit Card Detection	8 Block		
□ VPN >		🔇 Disable	Bad Robot	Allow		Ŧ
					100%	11
© System >						
Security Fabric >		Constraints				
E Log & Report >		( rate	Count			0
		e Edit	searcn			Q



### 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 سرویس های طرف مقابل اجرا میشود. برای انجام تنظیمات این بخش وارد منوی Policy & Object > DoS Policy میشویم. و میتوانید یک سری گزینه ها 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.

FGVMEVIFJPLYKIA5 -				🖲 admin 🕶
$\oslash$ Dashboard $>$	Create New Policy			×
↔ Network >				
🖹 Policy & Objects 🛛 🗸		Additional Information		
Firewall Policy	Name 🛈	API Preview		
Central SNAT				
DoS Policy 🟠		(2) Online Guides		
Addresses	Source Address +	Relevant Documentation      Video Tutorials		
Internet Service Database	Destination Address +	🗅 Consolidated Policy Configuration 📝		
Services	Service +	Ph. Fortinet Community		
Schedules		O Join the Discussion 12		
DNAT & Virtual IPs	L3 Anomalies			
IP Pools	Name O Logging Action Dicable Block Monitor Threshold			
Protocol Options				
Traffic Shaping	ip_src_session  Disable Block Monitor 5000			
Security Profiles >				
□ VPN >	ip_dst_session  Disable Block Monitor			
Subser & Authentication >				
In System →	L4 Anomalies			
Security Fabric >	Name O Logging Action Disable Block Monitor Threshold			
E Log & Report >				
	tcp_syn_flood  Disable Block Monitor 2000			
	tcp_port_scan O Disable Block Monitor 1000			
	tcp_src_session			Ŧ
	OK Cancel			

## 12 VPN and Cryptography

VPN مخفف 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.

## VPN Definition (Cont.)

VPNs have the following benefits:

- Cost savings
- Scalability
- Compatibility with broadband technology
- Security



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:

- Favesdropping 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:
  - Teinet, 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 chiffers
  - 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.



## Cisco Modular Network Architecture and VPNs (Cont.)



Cisco Modular Network Architecture

انواع روش های VPN بصورت زیر است:

معمولا بین شعبات مختلف با دفتر مرکزی از روش Site-To-Site استفاده می شود و در روش Remote Access زمانی که یک طرف ارتباطات ما کلاینت ها باشند از این روش استفاده می کنیم. Clientless یعنی بدون نصب نرم افزاری قادر به استفاده از قابلیت VPN است. Full Client یعنی با نصب نرم افزاری می توانیم بصورت کامل از مزایای این قابلیت در VPN بر خوردار 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 يعنى احراز هويت، و ما از اينكه طرف مقابل شخص جعلى نيست مطمين مي شويم.

Encapsulation Method يعنى با چه روش هايي ديتا را سوار بر يک ديتاي امن کنيم و تحويل مقصد دهيم.

Packet Integrity يعنى جلوگيرى از تغيير ديتا در طول مسير.

Key Management يعنى مديريت كليد ها براي رمزنگاري ديتا.

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 می توانند از وظایف VPN هم باشند.

# Secure Communication and Cryptographic Services

- Cryptography provides fundamental components of security for vFNs:
  - Confidentiality
  - Integrity
  - Authentication
  - Nonrepudiation
  - Key management
- Cryptography provides this security by using several types of cryptographic algorithms:
  - Symmetric encryption
  - Asymmetric encryption
  - Hashing
- These technologies can be used in various ways to provide the fundamental components of security.

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 می گیرند.

الگوریتم هایی Cryptography به سه دسته (Symmetric, Asymmetric, Hashing) تقسیم می شوند. 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 می کنند. در Asymmetric Encryption دو طرف ارتباط از کلید غیر مشابه و یا نامتقارن استفاده می کنند.

#### • 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 میباشد. AES میباشد.



## Cryptographic Algorithms

Cryptographic algorithms:

 Symmetric key cryptography also known as secret key or preshared key cryptography



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.

## Confidentiality Using Cryptographic Controls

Confidentiality is provided by encryption.

- Encryption is the process of converting cleartext to ophertext.
- Decryption is the process of converting ciphertext to cleartext.



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.

## Confidentiality Using Cryptographic Controls (Cont.)

Here are some characteristics of symmetric algorithms:

- · Efficient and fast, simple to accelerate in hardware
- Suitable for real-time bulk encryption
- · Key length of several tens to several hundred bits
- Key management can be a problem
- · Examples: DES, 3DES, AES, RC4, SEAL, and Blowfish





#### • 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 می شود. و مکانیزم آن به این صورت است که هر طرف Public خود را در اختیار طرف مقابل قرار می دهد. 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 می باشند.



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

## Confidentiality Using Cryptographic Controls (Cont.)

Here are some characteristics of asymmetric algorithms:

- Very slow compared with symmetric algorithms
- Used for digital signatures or a key exchange
- Typical key lengths in thousands of bits (RSA) or hundreds of bits
- (ECC)
- Simpler key management
- Examples: RSA and ECC



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



## Integrity Using Cryptographic Controls (Cont.)

Digital signatures:

- Asymmetric digital signature algorithms also provide integrity:
  - The sender generates a digital signature over data by using a private (signing) key and appends it to data.
  - The receiver verifies the signature by using a public (verification) key.
- Digital signatures use a combination of a hash algorithm (such as SHA-1) with an asymmetric algorithm (such as RSA).



#### • 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 نمی توانیم 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 می توان MD5, SHA1, SHA2, HMAC را نام برد.

ا زجمله کاربردهایی که Hashing دارد Integrity است. دیتا وارد الگوریتم می شود و یک Hash با مقدار ثابت دریافت میکنیم. و زمانی که دیتا را می خواهید 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 می شود. حال سوال اصلی اینجاس کسی که دیتا را تغییر دهد، حتما می تواند 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 می شود چرا زمانی که گیرنده دوباره دیتا را Hash میکند. همان Hash مورد نظر بدست نمی آید. در این حالت گیرنده به دو مسئله واقف می شود. یکی اینکه متوجه تغییر دیتا در مسیر می شود. 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.

Integrity Using Cryptographic Controls (Cont.)



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

Subject Authentication يعنى مطمين مي شويد، نفر مقابل همان شخص قبل انتظار است. كه معمولا با يوزر نيم و پسورد قابل فهميدن است.

Data Authentication يعنى مطمين شويم ديتا از همان جايي آمده است كه ما انتظار آن را داريم.

### Authentication Using Cryptographic Controls

Cryptographic authentication is used for the following:

- Subject authentication: Authenticate subjects using cryptographic authentication protocols.
- Data authentication: Authenticate data received over an untrusted network. Data authentication is usually performed with the following:
  - Symmetric HMAC algorithms, where high performance is desired without nonrepudiation (for example, SSL/TLS or IPsec)
  - Digital signatures, where performance is not a factor and nonrepudiation is required as well (for example, application layer transactions or XML messages)

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

#### Keys in Cryptography

- Keys are used for all of these three critical VPN functions: Encryption, Packet Integrity Checking, Authentication
- Key management deals with the secure generation, verification, exchange, storage, revocation, and destruction of keys.
- Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/ decrypted.
- The security of a symmetric cryptosystem is a function of two things: the strength of the algorithm and the length of the key.
- Key exchange (also known as "key establishment") is any method in cryptography by which cryptographic keys are exchanged between users, allowing use of a cryptographic algorithm.
- However distributed, keys must be stored securely to maintain communications security.



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 می شود.

Assymetric Encryption در این روش ما معمولا چالش انتقال کلید را نداریم. چرا که از دو کلید Private و Public استفاده می شود که کلید Private برای خودمان میماند و کلید Public را در اختیار بقیه قرار می دهیم. 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 و Private این روش بستری را مهیا می کند 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 می خواهند پابلیک همدیگر را دریافت کنند و می خواهند 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 می شود که هردو طرف کلید پابلیک خود را در اختیار یوزر B قرار می دهند. حال یوزر B پابلیک هرکدام را به همراه اسم هر کدام گرفته و Hash میکند و Hash بدست آمده را به همراه کلید علید Private خود امضا می کند. و بعد آن را تحت عنوان یک Certificate تحویل هرکدام از طرفین می دهد.

## Public Key Infrastructure (Cont.)

- User B can act as a trusted introducer because user B is trusted by both user A and user C.
  - User B signs the public key of user A with the private key of user B and sends it to user C.
  - User B signs the public key of user C with the private key of user B and sends it to user A.
  - Users A and C can verify the signature because they already have the public key of user B.



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



## Public Key Infrastructure (Cont.)

- · Certificate Authorities: PKI extends this concept and makes it scalable:
  - There is only one central trusted introducer (the CA).
  - The CA signs the public key of everyone.
  - Everyone has the public key of the CA.



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.

## Public Key Infrastructure (Cont.)

- Signed public keys (identity certificates) are returned to entities.
- Entities can now exchange their certificates with each other over an untrusted network.



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 = CCMCiuster001
Subject Public Key Information	756EGE0C9ADC7140

## 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- ctainpod, 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	Entitles 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 می گیرند معمولا در بستر MPLS قابل پیاده سازی هستند. در هنگام پیاده سازی VPN ها به سه موضوع Multicast, Redanduncy, QOS دقت زیادی داشته باشید.

## Site-to-Site VPN Technologies

Site-to-site VPNs:

- Connect sites as a replacement for a classic WAN
- Use peer (site) authentication and cryptographic path protection
- Require basic network traffic controls
- Frequently use IPsec for its cryptographic security services
- Often work over controlled networks (MPLS) or Internet backbones
- Often require high availability and performance guarantees (QoS)
- · Can be configured to function in several different ways



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



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 می کنیم. البته که ورژن دو آن مزایای بیشتری دارد. پروتکل IKE از پروتکل های درونی دیگری استفاده می کند. که انواع آن ISAKMP, Oaklay, Skeme می باشد. بعد از مرحله توافقات امنیتی، حال IPSEC مشخص می کند که از کدام پروتکل می خواهد 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 می کند.



· Combines three protocols into a cohesive security framework

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

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 می کنیم.

## Internet Key Exchange v1 and v2 Internet Key Exchange v1:

- Documented in RFC 2408
- Runs over UDP to destination port 500





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

IKE Phase 1 (IKE	ESA)
authentication (pr	re-shared autehntication key, certificate) (secure)
symmetric encryp	ption key exchange (secure)
Security Associat	tion (Authentication, DH, encryption, hashing)
IKE Phase 2 (secu	are) (IPSec SA)
Security Associat	tion (AH:md5, sha1 / ESP:des/3des/aes, md5/sha1)
key exchange (op	ptional): perfect security or PFS
IPSEC (AH/ESP)	
IKE	
IKE Phase 1 (main	n mode or aggressive mode)
IKE Phase 2 (mic	k mode or GDOD
IPSEC	

شکل زیر خصوصیات و ویژگی های IKEv2 را نمایش میدهد.

## Internet Key Exchange v1 and v2 (Cont.)

Internet Key Exchange v2:

- Documented in RFC 4306
- Runs over UDP to destination port 500
- There are two to five messages for basic exchange.
- There are two to five messages for basic exchange.
   IKEv2 creates the child SAs within the same negotiation, instead of using a phased approach.





## 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:

											Au	the	entica	tion	Hea	der	orm	at												
Offsets	Octet <sub>16</sub>				C	)								1							:	2				;	3			
Octet <sub>16</sub>	Bit <sub>10</sub>	0	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														29	30	31											
0	0		Next Header Payload Len Reserved																											
4	32													S	ecur	ity P	aram	eter	s Ind	lex (	SPI)									
8	64															Seq	uend	e Ni	umbe	er										
С	96		Integrity Check Value (ICV)																											

## Header پروتکل ESP با جزئیات بیشتر بصورت زیر است:

										Enc	aps	ulai	ting :	Secu	rity	Payl	oad	form	nat															
Offsets	Octet <sub>16</sub>					0								1								2							;	3				
Octet <sub>16</sub>	Bit <sub>10</sub>	0	1	2	3	4	5	6	7	8	9	10	) 11	12	13	14	15	5 16	17	18	19	20	21	22	2	3 24	25	26	27	28	29	3(	0	31
0	0													S	ecur	ity P	aran	neter	s Ind	dex (	SPI)													
4	32															Seq	uen	nce N	umb	er														
8	64															,	Doule	and a	lata															
				Payload data																														
															Pa	addir	ng (C	0-255	oct	ets)														
																				ŀ	Pad I	Leng	th					Ν	lext I	lea	der			
				Integrity Check Value (ICV)																														



#### 12.1 Site to Site VPN with IPSEC

با این قابلیت می توانید دو سایت مختلف را توسط فایروال فورتیگیت در بستر IPSEC به یکدیگر متصل کنید. برای این کار وارد منوی < VPN VPN Wizard می شویم. در مرحله اول، گزینه Site to Site را انتخاب میکنیم. در ادامه گزینه های دیگر را بررسی میکنیم.

FGVMEVIFJPLYKIA5 +	≡ Q	<b>₽</b> 2 -	🛞 admin 🕶
$\oslash$ Dashboard $>$	VPN Wizard		
↔ Network >			
Policy & Objects >	⑦ Online Guides		Î
☐ Security Profiles >	The IPsec VPN tunnel wizard gets you started with templates for common use cases. If the templates below do not		
L VPN ~	fulfill your needs, fully custom tunnels can be set up. For convenience, it is also possible to start with a template and		
Fabric Overlay Orchestrator	Q Forthet Community ↓ Join the Discussion ♂		
VPN Tunnels			
VPN Wizard 습	Tunnel name Site to Site		
SSL-VPN Portals	Select a template 💿		
SSL-VPN Settings			
SSL-VPN Clients			
VPN Location Map	Remote Site VPN Tunnel Local FortiGate		
△ User & Authentication >			
System >	Site to Site		
Security Fabric >	eache air maintipie, interiorations care stations rectificities connections with each other. Branch officies can also access the main office's intranet.		
E Log & Report >	Supported remote peers: 🗊 🕬		
	Spokes VPN Tunnels Hub		~

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.

🕞 FGVMEVIFJPLYKIA5 🛛 👻			🛞 admin 🔻
$\oslash$ Dashboard $>$	VPN Wizard - Site to Site		
+     Network >			
Policy & Objects >	Online Guides		
合 Security Profiles >	🖪 Relevant Documentation 🖸		
🗆 VPN 🗸			
Fabric Overlay Orchestrator	Internal         Coupoing         Coupoing		
VPN Tunnels			
VPN Wizard 🏠	Remote site		
SSL-VPN Portals			
SSL-VPN Settings	Remote site device type		
SSL-VPN Clients	Remote site device Accessible and static Behind NAT or dynamic		
VPN Location Map	IP/FODN 172 27 11 100		
🖄 User & Authentication 💦 >			
System >	Koute this device's internet trainc through the remote site. ()		
Security Fabric >	Remote site subnets that can access VPN 192.168.1.0/24		
E Log & Report >	+		
	Next Cancel		

در مرحله سوم، مشخص می کنیم 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.



🕞 FGVMEVIFJPLYKIAS 🔹	≡ Q	>_
<pre>② Dashboard &gt;</pre>	VPN Wizard - Site to Site	
Policy & Objects > Security Profiles >		<ul> <li>Online Guides</li> <li>Relevant Documentation 12</li> </ul>
🗆 VPN 🗸		🗅 Video Tutorials 🖒
Fabric Overlay Orchestrator	Remote Site VPN Tunnel Local FortiGate	Q     Fortinet Community       Ø     Join the Discussion
VPN Tunnels		
VPN Wizard ជំ		
SSL-VPN Portals SSL-VPN Settings	VPN tunnel	
SSL-VPN Clients	Authentication method Pre-shared key Signature	
VPN Location Map	Pre-shared key Test@123	
System ≥ 2000 System ≥ 200	IKE Version 2 Version 1	
Ø Security Fabric >	Transport () UDP Auto TCP encapsulation	
E Log & Report >	Use Fortinet encapsulation (3)	
	NAT traversal Enable Disable	
	Keepalive frequency 10	
	Next Cancel	-

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.

FGVMEVIFJPLYKIA5 -	≡ Q	>_
<pre>② Dashboard &gt;</pre>	VPN Wizard - Site to Site	
Policy & Objects > A Security Profiles >		<ul> <li>Online Guides</li> <li>Relevant Documentation 2</li> </ul>
VPN     Fabric Overlay     Orchestrator     VPN Tunnels	Remote Site VPN Tunnel	Ch Video Tutoriala (2) Rg Fortinet Community O Join the Discussion (2)
VPN Wizard 🏠	+ Remote site	
SSL-VPN Portals SSL-VPN Settings	VPN tunnel	
SSL-VPN Clients	Local site	
VPN Location Map       © User & Authentication       >       System       >       Security Fabric       >       Log & Report	Outgoing interface that binds to tunnel          port1        Create and add interface to zone         Local interface          port3         +        Local subnets that can access VPN          192.168.100.0/24	
	Allow remote site's internet traffic through this device ()  Next Cancel	

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 نمی شود.



### 12.2 Remote Access VPN with IPSEC

با این قابلیت کاربران می توانند 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 می شویم و گزینه Remote access را انتخاب می کنیم.

🕞 FGVMEVWPGMJU7R73 🛛 👻			¢ <mark>2</mark> ∙	🙁 admin 🕶
② Dashboard >	VPN Wizard			
↔ Network >	Hub (1) Online Guides	_	 	*
Policy & Objects >	■ Relevant Documentation	ß		
Security Profiles	□a Video Tutorials [2]			
□ VPN ~	🖓 Fortinet Community			
Fabric Overlay Orchestrator	Hub and Spoke with ADVPN O Join the Discussion 12 VPN connections radiate from a central FortiGate unit (the hub) to multiple			
VPN Tunnels	remote peers (the spokes). Traffic can pass between private networks that are each behind a hub or remote peer (spoke). Additionally, spoke to spoke			
VPN Wizard 🖄	traffic is possible via ADVPN tunnels.			
VPN Location Map	Supported remote peers:			
은 User & Authentication >				
钧 System >				
Security Fabric >				
🖻 Log & Report 💦 🗧 🗧				
	Remote VPN Tunnels Local FortiGate			
	Remote Arcess			
	Employees who need to access their company's network from off-site locations or users who want to securely connect to a private network from a public area frequently use this type of VPN.			_
	Supported remote clients: 📧 🕁 📽 🗮			_

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 192.168.100.100-192.168.100.100 با مسک 255.255.255.

FGVMEVWPGMJU7R73 ▼	≡ Q			>_	?▼	¢ <mark>2</mark> -	🙁 admin 🕶
⑦ Dashboard >	VPN Wizard - Test						
Policy & Objects      Security Profiles      VPN      Fabric Overlay      Orchestrator      VPN      VPN	Remote Endpoint	VPN Tunnel	.ocal FortiGate	<ul> <li>⑦ Online Guides</li> <li>☑ Relevant Documentation ☑</li> <li>☑ Video Tutorials ☑</li> <li>☑ Fortinet Community</li> <li>☑ Join the Discussion ☑</li> </ul>			
VPN Wizard 分	Remote endpoint						
VPN Location Map <pre></pre>	VPN client type						
<ul><li>iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii</li></ul>	IP range for connected endpoints Subnet for connected endpoints	0.0.0.0.0.0.0					
i≡ Log & Report >	FortiClient settings						
	Security posture tags	+					
	Auto Connect Always up (keep alive)	0					
		Next Cancel					

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



FGVMEVWPGMJU7R73 🗸	≡ Q	≻_	in <del>-</del>
Dashboard	VPN Wizard - Test		
Policy & Objects	Remote Endpoint VPN Tunnel Incoming Local FortiGate	<ul> <li>Online Guides</li> <li>Relevant Documentation I<sup>2</sup></li> <li>Mideo Extension 62</li> </ul>	*
Security Promes	+ Remote endpoint	Fortinet Community     A list the Dispussion 12	i.
Orchestrator VPN Tunnels	VPN tunnel	Join the Discussion	1
VPN Wizard     C       VPN Location Map        Output        System        Security Fabric	Nutrentication method     Pre-shared key       Pre-shared key     Image: Comparison of the state of the		
E Log & Report	NAT traversal     Enable     Disable       Keepalive frequency     10       User group     •       DNS Server     Use System DNS       Enable IPv4 Split Tunnel ①     •		
	Allow Endpoint Registration		

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.

FGVMEVWPGMJU7R73 -	= Q	≻_
<ul> <li>Ø Dashboard</li> <li>A Network</li> </ul>	VPN Wizard - Test	
Policy & Objects Curity Profiles VPN Fabric Overlay Orchestrator	Remote Endpoint VPN Tunnel	<ul> <li>⑦ Online Guides</li> <li>☑ Relevant Documentation I<sup>A</sup></li> <li>□ Video Tutorials I<sup>A</sup></li> <li>♀ Fortinet Community</li> <li>♀ Join the Discussion I<sup>A</sup></li> </ul>
VPN Tunnels	+ Remote endpoint	
VPN Location Map         ② User & Authentication         ③ System         ⑤ Security Fabric         E       Log & Report	VPN tunnel      Local FortiGate      Incoming interface that binds to tunnel      Create and add interface to zone      Local interface      Local Address      +	
	Next Cancel	]

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 محدودیت هایی دارد و ممکن است برخی از اپلکیشن ها بصورت وب کار نکنند. مثلا پروتکل هایی مثل ,HTTP, HTTPS, FTP, Ping به خوبی با این روش سازگار هستند. اما در روش Tunnel نرم افزاری سمت کلاینت نصب می شود 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:

🕞 FGVMEVIFJPLYKIA5 🛛 🗸		>_
$\oslash$ Dashboard $>$	Edit SSL-VPN Portal	
↔ Network >		A
Policy & Objects >	C Web Mode	FortiGate
Security Profiles >		I FOVMEVIJPETKIAJ
□ VPN ~	<ul> <li>ine regacy SSL-VPN web mode reature is disabled globally, web mode will not be accessible in portals.</li> </ul>	Additional Information
Fabric Overlay Orchestrator		© API Preview
VPN Tunnels	Landing page ① Default Custom	% References
VPN Wizard	Portal Message SSL-VPN Portal	>_ Edit in CLI
SSL-VPN Portals 🖒	Theme Security Fabric 💌	
SSL-VPN Settings	Default protocol HTTP/HTTPS 💌	⑦ Online Guides
SSL-VPN Clients	Show Session Information	Relevant Documentation     Yideo Tutorials     P
VPN Location Map	Show Connection Launcher	
$\stackrel{>}{\simeq}$ User & Authentication $\rightarrow$	Show Login History	R1 Fortinet Community
System >	User Bookmarks	
Security Fabric >	Encus hookmarks	
E Log & Report >	Rewrite Content IP/UI/	
	RDP/VNC clipboard	
	Predefined Bookmarks	
	+Create New & Edit Delete Search Q	
	Name	
	No results	
		· · · · · · · · · · · · · · · · · · ·
FORTIDET V7.6.0	OK Cancel	

اگر روی گزینه Create New را بزنیم می توانیم یک سری موارد را bookmark کنیم، تا زمانی که کاربر وارد پورتال خود می شود، این موارد را ببیند منتر می منتر

و از آن استفاده کند.





حال وارد منوی VPN > SSL VPN Settings می شویم و تنظیمات کلی برای SSL را انجام می دهیم. مثلا مشخص می کنیم 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.

🕞 FGVMEVIFJPLYKIA5 🔹	≡ Q	>_
<ul> <li>⊘ Dashboard &gt;</li> <li>↔ Network &gt;</li> </ul>	SSL-VPN Settings	
Policy & Objects  Security Profiles  Number	SSL-VPN status  Chable Additional Information Additional Information Additional Information	Í
Fabric Overlay Orchestrator	▲ For increased security, scalability, and flexibility, use <u>ZTNA</u> or <u>IPsec VPN</u> as an alternative to SSL-VPN tunnel modes.	
VPN Wizard SSL-VPN Portals	▲ SSL-VPN settings are not fully configured       □       SSL-VPN settings are not fully configured         ▲ SSL-VPN settings are not fully configured       □       What is ZTNA?       □         □       What is ZTNA?       □       □       □       □         □       What is ZTNA?       □	
SSL-VPN Settings	Connection Settings  PVPN Setup on FortiClient Usten on Interface(s) Configuring an SSLVPN Connection	n 12
VPN Location Map Suser & Authentication System Security Fabric	Listen on Port 443            443         ③ Online Guides           A Port conflicts with the administrative HTTPS port for this system          Relevant Documentation [2]           Use Tutorials [2]         ☑: Video Tutorials [2]	
LE Log & Report >	Server Certificate     P2: Fortinet Community       Redirect HTTP to SSLVPN     Image: Solution of the Discussion of the Discusicus and the Discussion of	
	Require Client Certificate  Tunnel Mode Client Settings  Apply	

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

FGVMEVIFJPLYKIA5 •	≡ Q		≻_ ®• 4	2.▼ ⑧ admin ▼
<pre>② Dashboard &gt;</pre>	SSL-VPN	New Authentication/Portal Mapping	Select Entries	× + Create
Policy & Objects > A Security Profiles >	Tunnel	Users/Groups +	USER (1)	
□ VPN ~	Addres	Porta	a guest	Ø
Fabric Overlay Orchestrator			USER GROUP (1	L)
VPN Tunnels			🖬 Guest-group	
VPN Wizard	DNISS			
SSL-VPN Portals	Specific			
SSL-VPN Settings	Specify			
SSL-VPN Clients	Authen			
VPN Location Map				
	i			
© System >				
Log & Report >	+0			

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



🕞 FGVMEVIFJPLYKIA5 🛛 🔹			>_
Ø Dashboard >	+ Cre	Create New Policy	×
💄 Policy & Objects 🛛 🗸 🗸	_	Name 🕟 SSL to LAN	Additional Information
Firewall Policy ☆	🖃 🗎 P	Schedule	© API Preview
Central SNAT	ii 🗆 🖿 te		③ Online Guides
DoS Policy	te	Action Acter ODENY	E Relevant Documentation
Addresses	🛨 Impl	Incoming interface (ssl.root)	Di Video Tutorials 🗹
Internet Service Database		Outgoing interface 📕 port2 💌	Chi Consolidated Policy Configuration (2)
Services		Course & Dephilophia (Strender)	Q Fortinet Community
Schedules		Source & Destination (Showing) 😈	O Join the Discussion @
DNAT & Virtual IPs		Source +	
IP Pools			
Protocol Options		User/group +	
Traffic Shaping		One user or group is required	
合 Security Profiles >		Destination +	
□ VPN >			
≗ User & Authentication >		Firewall/Network Options	
© System >		Inspection mode Flow-based Proxy-based	
Ø Security Fabric >			
l≞ Log & Report >		O         Central NAT is enabled so NAT settings from matching <u>Central SNAT</u> golicies will be applied.	
		Protocol options rear default	
		Security Profiles	
	Ø Secu	OK Cancel	



#### 12.4 Remote Access VPN with Tunnel Based SSL

در این روش کاربران محدودیتی به دسترسی به سرویس های داخلی از بیرون ندارند و از همه پروتکل ها 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:

🕞 FGVMEVIFJPLYKIA5 🛛 🛨					🛞 admin 🔻
$\textcircled{O}$ Dashboard $\rightarrow$	Edit SSL-VPN Portal				
↔ Network >					
Policy & Objects >			FortiGate		
合 Security Profiles >	Name full-access		R FGVMEVIFJPLYKIA5		
□ VPN ~	Limit Linear to One CCL V(DN)	Terrentian at a Time (7)	Additional Information		
Fabric Overlay Orchestrator	Limit Users to One SSL-VPN C	connection at a lime 🕜	API Preview		- 1
VPN Tunnels	C Tunnel Mode		% References		
VPN Wizard	Split tunneling	Disabled     All client traffic will be directed over the SSL-VEN turned	>_ Edit in CLI		
SSL-VPN Portals 🏠		An client drame will be directed over the 350 VPN durine.			
SSL-VPN Settings		<ul> <li>Enabled Based on Policy Destination</li> <li>Only client traffic in which the destination matches the destination of the configured firewall</li> </ul>	⑦ Online Guides		
SSL-VPN Clients		policies will be directed over the SSL-VPN tunnel.	Relevant Documentation     Video Tutorials		
VPN Location Map		O Enabled for Trusted Destinations			_
		Only client traffic which does not match explicitly trusted destinations will be directed over the SSL-VPN tunnel.	R Fortinet Community		
In System →					
Security Fabric >	Routing Address Override	+			
E Log & Report >	Source IP Pools	SSLVPN_TUNNEL_ADDR1 X			
	Tunnel Mode Client Options				
	Allow client to save password				
	Allow client to connect auton				
	DNS Solit Tuppeling	ons anve 🕞			
	or opping runnering	3			
	Host Check				Ŧ

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 Settings > SSL VPN می شویم و تنظیمات کلی را برای SSL را انجام می دهیم. مثلا مشخص می کنیم 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 می خواهند وارد پورتال خود شوند باید پورت 4433 را حتما وارد کنند. مثلا 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.

نكات 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 يورتال كاربر مي تواند نرم افزار Forti Client VPN را دانلود و نصب كند.
- 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 می شود.





	= 0		
	- 4		
Ø Dashboard >	+ Cre	Create New Policy	×
↔ Network >			Additional Information
Policy & Objects ~	<b>F N -</b>	Name () SSL to LAN	A ADI Deminu
Firewall Policy 🏠		Schedule	W API Preview
Central SNAT	:: 🗆 🖿 te		⑦ Online Guides
DoS Policy	🗆 te		Relevant Documentation
Addresses	🛨 Impl	Incoming interface	D1 Video Tutorials 🗹 D1 Controlidated Balicy Configuration 57
Internet Service Database		Outgoing interface 🗮 port2 🔹	Consolidated Policy Configuration E
Services		a an di di Mandada 🗛	R Fortinet Community
Schedules		Source & Destination (Snowlogic)	
DNAT & Virtual IPs		Source +	
IP Pools			
Protocol Options		User/group +	
Traffic Shaping		One user or group is required	
合 Security Profiles →		Destination +	
□ VPN >			
		Firewall/Network Options	
© System →		Inspection mode Elow-based Proxy-based	
Security Fabric >			
l≞ Log & Report >		Central NAT is enabled so NAT settings from matching <u>Central SNAT</u> <u>policies</u> will be applied.	
		Protocol options default	
		Security Profiles	*
	Secu	OK Cancel	



#### 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 می شویم و گزینه Virtual Domain را فعال میکنیم.

FGVMEVIFJPLYKIA5 +	≡ Q	≻_
② Dashboard >	System Settings	
Network     Network     Policy & Objects     Segurity Brofiler	Password scope ③ Off Admin   IPsec   Both )	Additional Information
□ security promes >	Workflow Management	>_ Editin CLI
은 User & Authentication >	Configuration save mode () Automatic Manual	Virtual Domain
Administrators	View Settings	Setup guides           Betwee guides           How to Configure Virtual Domains
Admin Prohles Firmware & Registration	Theme Jade	E Guides
Settings 🟠	Date/Time display FortiGate timezone Browser timezone	Workflow Management Using configuration save mode
SNMP	System Operation Settings	Online Guides     Relevant Documentation      C
Replacement Messages FortiGuard	NGFW mode Profile-based Policy-based Central SNAT C	Relevant bocomentation     C     Video Tutorials
Feature Visibility Certificates	Virtual Domains 🔿	Fortinet Community     O Join the Discussion
Security Fabric >	Start Up Settings	
E Log & Report >	Allow FortiConverter to obtain config file once  Auto file system check US8 auto-Install Detect configuration Cfgt_system.conf Detect firmware C Image out	

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

Config system global

Set vdom-mode multi-vdom

End

بعد از وارد كردن دستورات یک بار از فایروال خارج می شوید و دوباره وارد شوید. وقتی وارد می شوید یک VDOM بصورت گلوبال ایجاد می شود که به ما قابلیت مدیریت VDOM ها را می دهد. و یک VDOM به نام root هم ایجاد می شود، که تمام تنظیمات فعلی فایروال، به root VDOM انتقال پیدا می کند.



FGVMEVIFJPLYKIA5 -	≡ Q			VDOM: 🚱 Global 🔹 >_
⑦ Dashboard ~	+ Add widget			🕼 Global
Status :	System Information = •	Licenses () = •	Virtual Machine =	orot     =      =
	Hostname PCVMEVIPIPUXIAS Serial number FCVMEVIPIPUXIAS Firmware v7.6.0 build3401 (Pature) Virtual domail • System time 2024/09/13.04.43.09 Updme 44m.24s WAN IP Unknown	Image: Non-State     Image: Non-State     Image: Non-State       Image: Non-State     Image: Non-State     Image: Non-State	FOVMEV License Allocated VCPUs 100% Allocated RAM 2 GIB/2 97%	Status A Not Supported
	Security Fabric C E = - LAN Edge C O FortiSaitch train O FortiGate C O FortiSaitch train O FortiGate Fabric Connectors O Logging <i>L</i> fortiSandox C Central Management R FortiClient EMS	Administrators $\mathcal{B} \equiv \cdot$ (a) Fortibulore (a) HTTPS admini super_admin (c) Downkoad HTTPSCA certificate ) ×	CPU 1004 805 405 205 0N 43 seconds ago Cu	1 minute = = +
Fairtinet v7.60	Memory 100% 80% 60%	1 minute → Ξ →	Sessions 4 3	1 minute • ≡ •

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.

🕞 FGVMEVIFJPLYKIA5 🛛 👻	≡Q		VDOM: 😡 Global 🔹 📐 💿 🔹 📮 😣 admin 🔹
② Dashboard >		New Virtual Domain	×
↔ Network >	(+ cre		
☐ Security Profiles >	N		Additional Information
🕸 System 🛛 🗸		Virtual Domain	API Preview
VDOM 습		Type () Traffic Admin	>_ Edit in CLI
Global Resources		NGFW mode Profile-based Policy-based	
Administrators		Central SNAT 🕥	(?) Online Guides
Admin Profiles		WiFi country/region United States	Relevant Documentation      ✓     Video Tutorials
Firmware & Registration		Comments	
Settings			Ra Fortinet Community
HA			
SNMP			
Replacement Messages			
FortiGuard			
Feature Visibility			
Certificates			
Security Fabric >			
E Log & Report >			
FGVMEVIFJPLYKIA5 +	≡Q		VDOM: 🚯 Global 🔹 >_ 💿 🔹 🔍 🙎 🔹 🛞 admin 🔹
② Dashboard >		Edit Interface	×
⊕ Network	E Fort		^
Interfaces 🖄			FortiGate
DNS		Name eport2	R FGVMEVIFJPLYKIA5
IPAM	+ Cre	Alias	7. L.
合 Security Profiles >	Ξ	Type Physical Interface	O Down
System >	🖃 📴 8	VRFID () 0	
Ø Security Fabric >		Virtual domain 🗖 root 🔹	MAC address
E Log & Report >		Role () Q Search	10006-6717-7026
	- M F	▲ root	Additional Information
		Dedicated M:	© API Preview
		Address	% References
		Addressing mode Manual IRAM DHCP PPPAF One-Arm Sniffer	> Edit in CLI
		Secondary ID address (	(7) Online Guides
		Securitary in address 🖉	Video Tutorials
		Administrative Access	O Sector Committee
		IPv4 SCIM HTTPS PING	
		FMG-Access SSH SNMP	Sharing the procession (2)
		LI FTM LI RADIUS Accounting Li Security Fabric Connection (3)	
		Speed Test	
		Receive LLDP ④ Use VDOM Setting Enable Disable	
		Transmit LLDP ③ Use VDOM Setting Enable Disable	
	4		· · · · · · · · · · · · · · · · · · ·



نکته مهم دیگری که می توانیم 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 می شویم. 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.

🕞 FGVMEVIFJPLYKIA5 🛛 👻	= Q			VDOM: 😡 Global 🕶	≻_ ⊙•	<b>↓ 2 •</b> ⑧ admin •
Ø Dashboard →		New Administrator				×
↔ Network >	(+ cre					
合 Security Profiles >				Additional Information		
l System v	- Syste	Username		③ API Preview		
VDOM		Туре	Local User	<ul> <li>FortiTaken Cloud</li> </ul>		
Global Resources			Match a user on a remote server group	Factore Cloud Dashboard		
Administrators 🏠			Use public key infrastructure (PKI) group	Le Portrioken Cloud Dashboard		
Admin Profiles		Description of		⑦ Online Guides		
Firmware & Registration		Password		Relevant Documentation     Z     Video Tutorials     Z		
Settings		Confirm Password				
HA		Comments	Write a comment 0/255	R1 Fortinet Community		
Doplacement Messages		Administrator profile	· ·	♀ Join the Discussion		
FortiQuard		Virtual Domains	A root X			
Feature Visibility			+			
Certificates						
Security Fabric >		Iwo-factor Authen	tication			
i≡ Log & Report >		Restrict login to tru	usted hosts			
		Restrict admin to g	uest account provisioning only			
	= 0			VDOM: 🖗 Clobal 🕶	> @•	∩or ®adm
	_ ~	New Admin Profile			<i>i</i> - 0	
Network	+ Cre	New Admin Prome				
合 Security Profiles >	0	Name		Additional Information		
it is system ∽	D pro	Comments		© API Preview		
VDOM	🗆 sup		0/255	> Edit in CLI		
Global Resources		Access Permissions				
Administrators		Accessitermissions		⑦ Online Guides		
Admin Profiles 🏠		Access Control	Permissions Set All •	Relevant Documentation     Video Tutorials     7		
Firmware & Registration		Security Enhric	Nons @ Read & Read Mirite			
Settings		Security Fabric	G Note @ Read p Read/write	R1 Fortinet Community		
HA		FortiView	Sone ◎ Read 🖉 Read/Write	Soin the Discussion		
SNMP		Lines & Davies	Name @ Read & Read Minite			
Replacement Messages		USEI & DEVICE	G Note G Read & Read/Write			
FortiGuard		Firewall	Sone © Read & Read/Write ⊗ Custom			
Feature Visibility						
Certificates		Log & Report	Vione Wield Wield/Write & Custom			
Security Fabric		Network	Sone © Read & Read/Write ⊗ Custom			
🗠 Log & Report 💦 🔿		a star				
		System	Wille W Read / Read/Write & Custom			
		Security Profile	S None ◎ Read 🖉 Read/Write 🕸 Custom			
		VON				
	the second se		MADE AND A REAL AND A			
		VEN	G None W Read & Read/White			

یکی دیگر از مواردی که می توانید برای هر VDOM مشخص کنید، میزان منابع سخت افزاری است که در اختیار هر VDOM می توانیم قرار دهیم. البته این محدودیت را به این صورت می توانیم 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 می توانید از منوی System > VDOM وارد VDOM مربوطه شوید و این مقادیر را مشخص کنید. یا اینکه وارد منوی Syster > Global Resource شوید و تنظیمات کلی را ایجاد کنید تا هر VDOM به همین اندازه در فایروال سهمیه داشته باشد.



								🚱 Global 🔹 🛛 📐	ଡ• <mark>-</mark>	🛞 admin 🔻
	+ Cre	dit Virtual Domain Settings								×
↔ Network >	M	Central SNAT					Additional Information			
Security Profiles >		Comments					Additional montacion			
System ~	Sec. 1			10			© API Preview			
VDOM G							% References			
Global Resources		Resource Usage					> Edit in CLI			
Admin Profiles		Reset All					⑦ Online Guides			
Firmware & Registration		Deserves	Current	Clabal Maximum	Our mide Manimum	Currenteed	E Relevant Documentation	3		
Settings		Resource	Usage	Global Maximum	Override Maximum	Guaranteeu	🕫 Video Tutorials 📝			
НА		Active Sessions	(4)	No Limit Set	0		Ra Fortinet Community			
SNMP		Policy & Objects								
Replacement Messages		Firewall Policies	(2)	1032	Э					
Feature Visibility		Firewall Addresses	(24)	11024	0					
Certificates		Convellent data and conv	(4)	5000						
Security Fabric      Security Fabric		Firewall Address Groups	(2)	5000						
E Log & Report >		Firewall Custom Services	(88)	No Limit Set	•					
		Firewall Service Groups	(4)	No Limit Set	0					
		Firewall One-time Schedules	(0)	No Limit Set	•					
		Firewall Decurring Scheduler	(2)	No Limit Set	•					
		Firewall Recurring Schedules	(3)	NO LIMIT SEL	3					
		User & Device	_							
FURTINET V7.6.0					incer					
	= ^						VDOM		Q- 00-	() atain a
G FGVMEVIFJPLYKIA5 •	≡ Q						VDOM	🚱 Global 🔹 >_	⊙• <mark>↓2</mark> •	admin 🕶
FGVMEVIFJPLYKIA5     O Dashboard     Antwork	≡ Q Global Res	ources					VDOM	€ Global + >_	⊙•	⑧ admin <del>•</del>
	⊟ Q Global Res	ources					VDOM	🖗 Global 🔹 🔪	⊙•	⑧ admin ◄
Image: FGVMEVIFJPLYKIA5         ▼           Ø Dashboard         >           Image: Maxwork         >           Image: Security Profiles         >           Image: System         ✓	■ Q Global Res	ources - All	Reso	urce			VDOM Current Usage	Global ▼ >_     Default Maximum	⊙ ▼      Q.2 ▼	⊗ admin +
FOVMEVIEIPLYKIAS     Orbitality     Found     Security Profiles     Security     VDOM	■ Q Global Res	ources All	Reso	urce			VDOM Current Usage	© Global ▼ >_ Default Maximum	⊙ •	© admin +
FOVMEVIPIPLYKIAS     Ozshboard     Dashboard     Network     Scurity Profiles     System     VDOM     Global Resources     Y	E Q Global Res @ Reset Active S	ources All essions	Reso	urce		05	VDOM Current Usage (4)	Global ▼ >     Default Maximum     No Limit Set	Override Max	® admin ▼ dmum
FOVMEVIPIPLYKIAS     Ozshboard     Dzshboard     Source      Network     Security Profiles     System     VDOM     Clobal Resources     Administrators     Administrators	E Q Global Res Reset Active S Policy & O	ources All essions bjects	Reso	urce		05	VDOM Current Usage (4)	Global	Override Max	(€) admin ▼
B FOVMEVIPIPIYKIAS     •       O Dashboard     >       * Network     >       Security Profiles     >       System     >       VDOM     *       Global Resources     *       Administrators     Administrators       Administrators     Firmware & Registration	E Q Global Res © Reset Active S Policy & O Firewall	ources All essions bjects Policies	Reso	urce		05	VDOM Current Usage (4)	Colobal	Override Max       Override Max	(E) admin +
B       FOVMEVIPIPIYKIAS       •         Image: Comparison of the second s	E Q Global Res Reset Active S Policy & O Firewall	ources All essions bjects Policies Addresses	Reso	urce		00	VDOM Current Usage (4) (2) (24)	Colobal	Override Max	limum
B FOVMEVIFIPIYKIAS       •         O Dashboard       >         + Network       >         O Security Profiles       >         Ø System       >         VDOM          Global Resources       \$2         Administrators       Administrators         Administrators       Settings         HA       SNMP	<ul> <li>Q</li> <li>Global Res</li> <li>Global Reset</li> <li>Active S</li> <li>Policy &amp; O</li> <li>Firewall</li> <li>Firewall</li> <li>Firewall</li> </ul>	ources All essions bjects Policies Addresses Address Groups	Reso	urce		05	VDOM Current Usage (4) (2) (24) (24)	Clobal • > Default Maximum No Limit Set 1032 11024 5000	Override Max       Override Max	© admin •
B       FOVMEVIE/PLYKIAS       •         Image: Comparison of the strength of the strenge strength of the strength of the strength	<ul> <li>Q</li> <li>Global Res</li> <li>Global Reset</li> <li>Active S</li> <li>Policy &amp; O</li> <li>Firewall</li> <li>Firewall</li> <li>Firewall</li> <li>Firewall</li> </ul>	ources All All essions bjects Policles Addresses Addresses Custom Services	Reso	urce		03 05 05 05 05	VDOM Current Usage (4) (2) (24) (24) (2) (88)	♥ Global ▼ >_ Default Maximum No Limit Set 1002 11024 5000 No Limit Set	Override Max       Override Max       O	(2) admin •
B       FOVMEVIE/PLYKIAS       -         Image: Comparison of the strength of the strenge strength of the strength of the strength	<ul> <li>Q</li> <li>Global Res</li> <li>Global Reset</li> <li>Active S</li> <li>Policy &amp; O</li> <li>Firewall</li> <li>Firewall</li> <li>Firewall</li> <li>Firewall</li> <li>Firewall</li> <li>Firewall</li> <li>Firewall</li> </ul>	ources All All essions bjects Policies Addresses Addresses Custom Services Service Groups	Reso	urce		05 05 05 05 05	VDOM Current Usage (4) (2) (24) (24) (2) (88) (4)	♥ Global ▼ >_ Default Maximum No Limit Set 1032 11024 5000 No Limit Set No Limit Set	Override Max       Override Max       O       O       O       O       O       O       O       O	(2) admin •
B       FOVMEVIPPLYKIAS       -         Image: Comparison of the second of the se	E Q Global Res Or Reset Active S Policy & O Firewall Firewall Firewall Firewall	ources ources All essions bjects Policies Addresses Addresses Custom Services Service Groups Ource and the schedule of the sch	Reso	urce			VDOM Current Usage (4) (2) (24) (24) (24) (24) (24) (24) (	♥ Global ▼ >_ Default Maximum No Limit Set 1032 11024 5000 No Limit Set No Limit Set No Limit Set	Override Max       Override Max       O       <	() admin +
By FOVMEVIPIPIYKIAS       -         O Dashboard       >         Dashboard       >         Security Profiles       >         Security Profiles       >         VDOM       VDOM         Global Resources       \$2         Administrators       Administrators         Administrators       Administrators         Administrators       Firmware & Registration         Settings       HA         SNMP       Replacement Messages         FortiGuard       FortiGuard         Cartificates       Certificates         Security Fabric       >	E Q Global Res Active S Policy & O Firewall Firewall Firewall Firewall Firewall	ources all all essions bject Policies Addresses Addresses Custom Services Service Groups One-time Schedules	Reso	urce		00 00 00 00 00 00 00 00 00	VDOM Current Usage (4) (2) (24) (24) (24) (2) (28) (4) (4) (0)	€ Global * >_ Default Maximum No Limit Set 1032 11024 5000 No Limit Set No Limit Set No Limit Set	Override Max       Override Max       O       <	S admin +
B       FOVMEVIIPPLYKIAS       -         Image: Comparison of the second of the s	E Q Global Res Reset Active S Policy & O Firewall Firewall Firewall Firewall Firewall	ources ources All essions essions bjects Policies Addresses Addresses Custom Services Service Groups One-time Schedules Recurring Schedules	Reso	urce		00 00 00 00 00 00 00 00 00 00 00	VDOM Current Usage (4) (2) (24) (24) (24) (24) (24) (24) (	€ Global * > Default Maximum No Limit Set 1032 1024 5000 No Limit Set	Override Max	S admin +
B POVMEVILIPIPIYKIAS       -         C Dashboard       >         + Network       >         C Security Profiles       >         Security Profiles       >         VDOM       VDOM         Global Resources       12         Administrators       Administrators         Administrators       Administrators         Administrators       Firmware & Registration         Settings       HA         SNMP       Replacement Messages         FortiGuard       Feature Visibility         Cartificates       >         Security Fabric       >         Log & Report       >	E Q Global Res Active S Policy & O Firewall Firewall Firewall Firewall Firewall Firewall Succession	ources ources All essions essions bjects Policies Addresses Addresses Custom Services Service Groups One-time Schedules Recurring Schedules Vice	Reso	urce		00 00 00 00 00 00 00 00 00 00 00	VDOM Current Usage (4) (2) (24) (24) (24) (24) (24) (24) (	€ Global • > Default Maximum No Limit Set 1032 1024 5000 No Limit Set	Override Max       Override Max       O       <	S admin •
B POVMEVIPIPIYKIAS       -         O Dashboard       >         A Dashboard       >         Security Profiles       >         System       >         VDOM       Clobal Resources       12         Administrators       Administrators         Administrators       Administrators         Administrators       Security Profiles         Firmware & Registration       Security Fabric         SNMP       Replacement Messages         Fortiouard       Feature Visibility         Certificates       >         Security Fabric       >         Log & Report       >	Clobal Res Clobal Res Reset Active S Policy & O Firewall Firewall Firewall Firewall Firewall Firewall Sure & Det User	ources all all all all all all all all all al	Reso	urce		00 00 00 00 00 00 00 00 00 00	VDOM Current Usage (4) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	Global	Override Max	S admin •
B POVMEVIPIPIYKIAS       -         O Dashboard       >         B Dashboard       >         Security Profiles       >         System       >         VDOM       VDOM         Global Resources       12         Administrators       Administrators         Administrators       Administrators         Administrators       Farmare & Registration         Settings       -         HA       SNMP         Replacement Messages       Fortfouard         Feature Visibility       Certificates         © Security Fabric       >         Log & Report       >	Elobal Res Clobal Res Active S Policy & O Firewall Firewall Firewall Firewall Firewall Elevall User & Der User User Gro	ources ou	Reso	urce		00 00 00 00 00 00 00 00 00 00 00 00 00	VDOM Current Usage (4) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	Global ▼      ∑     Calobal ▼      Calobal ▼      ∑     Calobal ▼      ∑     Calobal ▼      Calobal ▼      Calobal ▼      ∑     Calobal ▼      Calobal ▼      Calobal ▼      Calobal ▼     Ca	Override Max	S admin •
B POVMEVIPIPIYKIAS       -         Image: Constraint of the second of the se	Clobal Res Clobal Res Reset Active S Policy & O Firewall Firewall Firewall Firewall Firewall Firewall Firewall User & Det User User Gro	ources ources All essions essions biects Policies Addresses Addresses Custom Services Service Groups One-time Schedules Nee urring Schedules ups ent Explicit Proxy Users	Reso	urce			VDOM Current Usage (4) (2) (24) (24) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	Global ▼	Override Max	S admin •

نکته مهم دیگر اینکه میتوانید در قسمت Security Profile ها، پروفایل هایی 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 می توانید 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 می خواهیم 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 <vom Network > Interface > Create New استفاده کنیم. برای این کار وارد منوی <vom Network این دو این این از این این این کار وارد منوی در این حالت از باط داشته باشد. و این این کار وارد منوی می خواهیم از یک لینک فیزیکی برای اتصال این دو می کنیم که کدام VDOM در این حالت از VDOM Link در این این کار وارد منوی در Network این این ارتباط به چه رنج آی پی انجام شود. مثل این می ماند که دو فایروال را بصورت فیزیکی با یک کابل به یکدیگر متصل کرده باشیم.




## 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 می شود.

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 می شویم و نوع HA خود را که می تواند، Active-Active و Active-Passive باشد را انتخاب می کنیم. بطور مثال ما حالت Active-Passive را انتخاب می کنیم.

SGVMEVIFJPLYKIA5	•	≡ Q		>_	 ¢ <mark>2</mark> -	🖲 admin 🕶
⑦ Dashboard	>	High Ava	ailability			
+‡+ Network	>					
Policy & Objects	>		Additional Information			
Security Profiles	>	Mode	Standalone   API Preview			
C VPN	>		Standalone >_ Edit in CLI			
은 User & Authentication	>		Active-Active			
🔅 System	$\sim$		Active-Passive & High Availability			
Administrators			Guides  Identifying the HA Cluster Units	52		
Admin Profiles			E FGSP (Session-Sync) Peer Setup [2]			
Firmware & Registration			U Troubleshoot an HA Formation C			
Settings			Increasing Device Priority Effect (Override)	2		
НА	ŵ		Cluster Setup			
SNMP			E HAActive-Active Cluster Setup []			
Replacement Messages			🖺 HA Virtual Cluster Setup 🖸			
FortiGuard			⑦ Online Guides			
Feature Visibility			🗉 Relevant Documentation 🖸			
Certificates			🖙 Video Tutorials 🖸			
Ø Security Fabric	>		Pa Fortinet Community			
💷 Log & Report	>		🗘 Join the Discussion 🕜			
			OK Cancel			

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 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 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 حدار انتخاب کنید تا هرکدام از دسترس خارج شد، فایروال دوم فعال شود. اگر این بخش را انتخاب نکنیم، تا را انتخاب نکنیم، تا را استندبای فعال نمی شود. در قسمت Monitor Interface او انتخاب کنید تا هرکدام از دسترس خارج شد، فایروال دوم فعال شود. اگر این بخش را انتخاب نکنیم، تا می مان مانی که فایروال استندبای فعال نمی شود. اگر این بخش ما انتخاب نخیم، تمامی Interface ها روی فایروال دوم فعال شود. اگر این بخش ما را انتخاب نکنیم، تا را انتخاب نکنیم، تا مرکدام از دسترس خارج شد، فایروال دوم فعال شود. اگر این بخش ما انتخاب نکنیم، تا زمانی که فایروال فعلی بصورت کلی از شبکه خارج نشده باشد، فایروال استندبای فعال نمی شود. در قسمت interface میکنیم، ما زمانی که فایروال هلی است را انتخاب میکنیم.

## **Fortigate Firewall**



FGVMEVIFJPLYKIA5 🔹	≡ Q	≻_						
② Dashboard →	High Availability							
↔ Network >		A						
Policy & Objects >		Additional Information						
合 Security Profiles >	Mode Active-Passive -	API Preview     API PrevIPrevII     API Preview     API Preview     API PrevII     API						
□ VPN >	Device priority (1)	>_ Edit in CLI						
Subser & Authentication	Increase priority effect							
System ~		🛧 High Availability						
Administrators Admin Profiles	Cluster Settings	Guider  B Identifying the HA Cluster and Cluster Units  FGSP (Session-Sync) Peer Setup  C						
Firmware & Registration Settings	Group ID U 0 Group name	Troubleshoot an HA Formation [2]     Check HA Sync Status [2]     Increasing Device Priority Effect (Override) [2]						
HA 🏠	Password ••••••• Change	Cluster Setup						
SNMP	Session pickup 🛛 🔘	HA Active-Passive Cluster Setup						
Replacement Messages	Monitor interfaces +	HA Virtual Cluster Setup						
FortiGuard	Heartbeat interfaces +	⑦ Online Guides						
Feature Visibility		🗉 Relevant Documentation 🖸						
Certificates	Management Interface Reservation	🗅 Video Tutorials 🖸						
Security Fabric >	Interface	R₁ Fortinet Community ♀ Join the Discussion [2]						
Log & Report >	Gateway 0.0.0.0							
	Destination subnet 0.0.0.0/0							
	•							
	O Unicast Heartbeat							

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 بايد قبل از دستورات فوق fortilink خود را غير فعال كنيد.

Config system interface
Show
Edit fortilink
Set fortilink disable
End