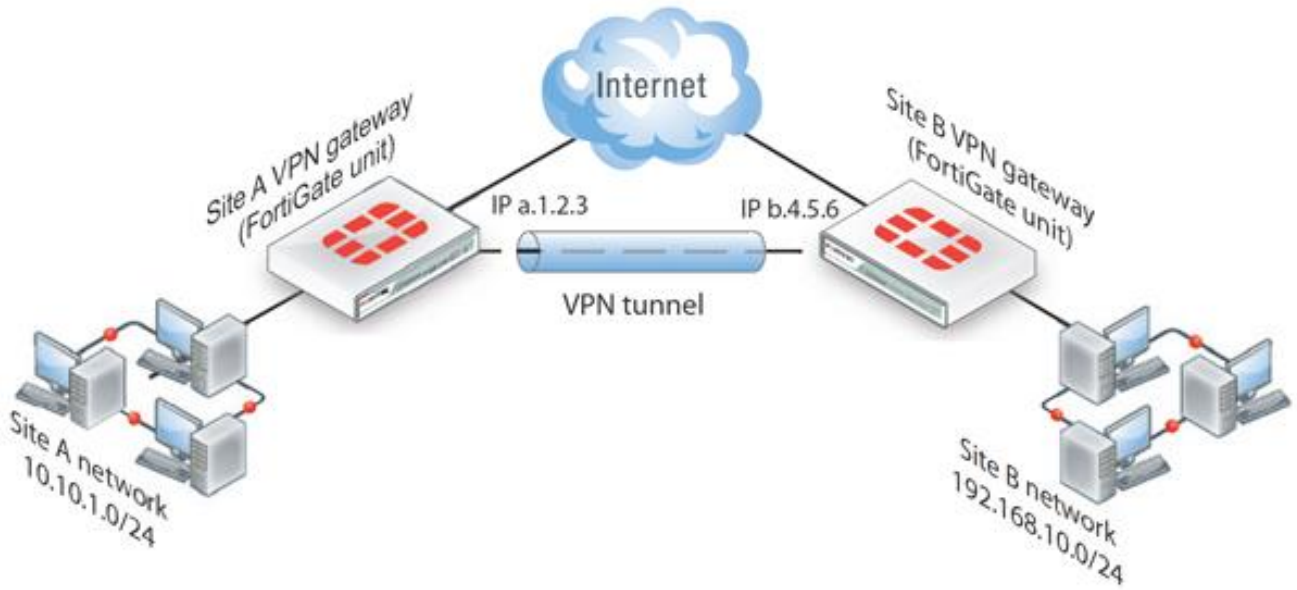


VPN Site-to-Site FortiGate



خلينا مبدأياً نصف انواع ال VPN بشكل مبسط كدا عشان نشوف هنتكلم على ايه النهاردة

اول حاجة عندنا Site-to-site VPN

زي ماشرحت قبل كدا ال Site to site بيتعمل عن طريق بروتوكول IPSec وانا شرحته بالتفصيل فالملف دا ارجع له النهاردة هنتكلم عن الخيارات المتاحة بالنسبة ل FortiGate فالملف دا هنتكلم عن اول نوع وهو

IPSec Site-to-site VPN

بينقسم ل نوعين

1. Policy Based

مش بيحتاج routing بين ال sites بل يعتمد فقط على وجود Policies

ميزته: انه سهل انك تعمله مش محتاج configurations كثير

عيوبه: انه مش مرن مش بيدعم ال Hub & Spoke.

ولا يدعم ال Dynamic Routing Protocol في حالة مثلا رابط فروع الشركة باستخدام Dynamic Routing protocol زي OSPF , EIGRP.

لا يدعم ال Redundancy.

Precautions

شوية احتياطات لازم تاخذ بالك منهم

1. اول حاجة انه مش متفعل by default على FortiGate ولكن لابد

انك تفعله من feature visibility هو ضحك فالأخر ازاي

2. ضع فالحسبان ترتيب ال policy حيث دائما الأكثر تحديدا يكون اولاً

حيث يتم عمل matching من الأعلى للأسفل.

2. ROUTE Based

لابد يكون فيه Routing لكي يحدد المسار اللي هياخده الترافيك
بيكون virtual interfaces تحت ال Wan interface يستخدمها ك VPN
tunnel

دا يخليه مرن اكثر يقدر يعمل Hup & Spoke

(يعني ببساطة فرع رئيسي متصل بيه فروع اخرى فرعية)

وبكدا بيوفر المشاكل اللي ناقصة فالنوع السابق مثل انه بيدعم

- Hup & Spoke
- Dynamic Routing
- Redundancy

في سؤال منطقي جه ف بالك ايه الفائدة اني استخدم Policy-Based
بخلاف انه سهل وبسيط ممكن احتاجه ف ايه ؟

هتحتاجه في حالة كنت مشغل ال firewall في ال Transparent Mode
يعني مفيش اي Routing ودا غالبا بيكون في حالة انه بيأمن
data center

بعد مخلصنا النوعين وامتى بحتاج كل واحد منهم يلا نشوف خطوات
عمل كل نوع

Policy-Based Configuration Steps

1.Enable Policy Based From Feature Visibility

The screenshot displays the Fortinet FortiGate v7.0.3 web interface. The left sidebar contains the navigation menu, and the main area shows the 'Feature Visibility' configuration page. Three steps are highlighted with numbered callouts:

- Step 1:** The 'System' menu item in the left sidebar is highlighted with a red box and a green callout labeled '1'.
- Step 2:** The 'Feature Visibility' menu item in the left sidebar is highlighted with a red box and a green callout labeled '2'.
- Step 3:** The 'Policy-based IPsec VPN' feature toggle in the main configuration area is highlighted with a red box and a green callout labeled '3'.

The 'Feature Visibility' page shows a list of features that can be enabled or disabled. The 'Policy-based IPsec VPN' feature is currently disabled (indicated by a grey toggle switch). The 'Apply' button is visible at the bottom right of the configuration area.

Feature	Status
Endpoint Control	Enabled
Explicit Proxy	Disabled
File Filter	Enabled
Intrusion Prevention	Enabled
Video Filter	Enabled
Web Application Firewall	Disabled
Web Filter	Enabled
Zero Trust Network Access	Disabled
DoS Policy	Enabled
Email Collection	Disabled
FortiExtender	Disabled
ICAP	Disabled
Implicit Firewall Policies	Enabled
Load Balance	Disabled
Local In Policy	Disabled
Local Out Routing	Disabled
Multicast Policy	Disabled
Multiple Interface Policies	Disabled
Policy Advanced Options	Disabled
Policy Disclaimer	Disabled
SD-WAN Interface	Enabled
Policy-based IPsec VPN	Disabled
Replacement Message Groups	Disabled
SSL-VPN Personal Bookmark	Disabled
SSL-VPN Realms	Disabled
Threat Weight Tracking	Enabled
Traffic Shaping	Enabled
VoIP	Disabled

2. Create IPsec Tunnel

1 VPN

2 IPsec Tunnels

VPN-policy-Base

Comments 0/255

Enable IPsec Interface Mode

Network

Remote Gateway Static IP Address

IP Address 192.168.1.15

Interface WAN (port1)

Local Gateway ☒ Primary IP Secondary IP Specify

192.168.1.10

Mode Config ☐

NAT Traversal Enable Disable Forced

Keepalive Frequency 10

Dead Peer Detection Disable On Idle On Demand

DPD retry count 3

DPD retry interval 20 s

Forward Error Correction Egress ☐ Ingress ☐

Advanced...

Authentication

Method Pre-shared Key

Pre-shared Key

IKE

Version 1 2

Mode Aggressive Main (ID protection)

في اول مرحلة دي بنعرف ال FortiGate هيطلع من اي WAN

interface ونضيف ال Remote IP

وبنحدد ال mode , IKE version , Pre-Shared Key

شرحتهم في ملف IPsec VPN

وطبعا يكون static عشان ميعملش مشاكل بعد كذا

لازم تشيل علامة الصح على Enable IPsec Interface Mode لان

دا خاص فال Route-Based

Phase 1

The screenshot shows the 'Phase 1 Proposal' configuration window. On the left is a sidebar with a tree view containing: Network, Policy & Objects, Security Profiles, VPN (expanded), Overlay Controller VPN, IPsec Tunnels (selected), IPsec Concentrator, IPsec Wizard, IPsec Tunnel Template, SSL-VPN Portals, and SSL-VPN Settings. The main area is titled 'Phase 1 Proposal' with an 'Add' button. It contains two rows for 'Encryption' and 'Authentication', both set to 'DES' and 'MD5' respectively. Below these are 'Diffie-Hellman Groups' with a grid of checkboxes; groups 14 and 5 are selected. 'Key Lifetime (seconds)' is set to 86400. 'Local ID' is empty. At the bottom, 'XAUTH' is set to 'Disabled'.

بنددد.له ال Diffie-Hellman Groups Encryption Algorithm ,
ولابد يكون متشابه عن الناحيتين

ولاحظ انه فالنسخة الفري لا يدعم سوى ال. DES , MD5 , SHA1

Phase 2

The screenshot shows the 'Phase 2 Selectors' and 'New Phase 2' configuration windows. The sidebar is the same as in Phase 1. The 'Phase 2 Selectors' table has one entry: 'VPN-policy-Base' with 'Local Address' 0.0.0.0/0.0.0.0 and 'Remote Address' 0.0.0.0/0.0.0.0. The 'New Phase 2' window has a 'Name' field with 'VPN-policy-Base'. 'Comments' is empty. 'Local Address' and 'Remote Address' are both set to 'Subnet' with '0.0.0.0/0.0.0.0'. Under 'Advanced...', 'Phase 2 Proposal' has an 'Add' button. 'Encryption' is 'DES' and 'Authentication' is 'MD5'. 'Enable Replay Detection' and 'Enable Perfect Forward Secrecy (PFS)' are both checked. 'Diffie-Hellman Group' has a grid of checkboxes; groups 14 and 5 are selected. 'Local Port', 'Remote Port', and 'Protocol' are all set to 'All' and checked. 'Auto-negotiate' and 'Autokey Keep Alive' are unchecked. 'Key Lifetime' is set to 'Seconds' with a value of 43200.

بندد ال Encryption Algorithm لل Phase 2 وتقدر تحدد ال
Subnet الال هتروح تكلمها

Enable Relay Detection

دا خيار بيخليه يزود sequence number بشكل عشوائي بحيث يمنع
ال Replay Attack

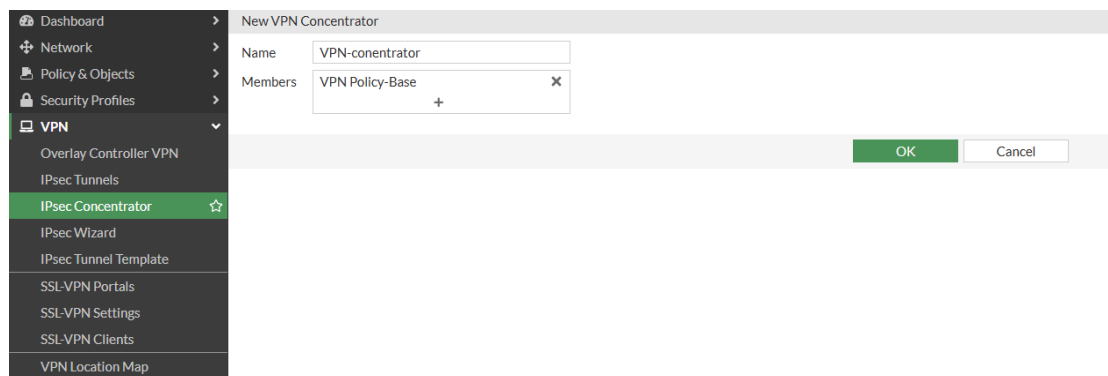
Enable perfect Forward Secrecy PFS

بيغير ال Diffie-Hellman Groups كل اما ينتهي ال life Time

Auto-Negotiate

بيعمل establishment لل connection بشكل automatic

3.Create IPsec Concentrator



The screenshot shows a 'New VPN Concentrator' dialog box. On the left, a sidebar menu is visible with the following items: Dashboard, Network, Policy & Objects, Security Profiles, VPN (expanded), Overlay Controller VPN, IPsec Tunnels, IPsec Concentrator (selected), IPsec Wizard, IPsec Tunnel Template, SSL-VPN Portals, SSL-VPN Settings, SSL-VPN Clients, and VPN Location Map. The main area of the dialog has a 'Name' field containing 'VPN-concentrator' and a 'Members' field containing 'VPN Policy-Base'. There is a plus sign icon next to the 'Members' field. At the bottom right, there are 'OK' and 'Cancel' buttons.

4.create IPsec Policy

The screenshot shows the Fortinet v7.0.3 GUI with the 'Edit Policy' window open. The left sidebar shows the 'Policy & Objects' menu with 'Firewall Policy' selected. The main window displays the configuration for a policy named 'VPN-policy Based'. The 'Incoming Interface' is 'LAN (LAN)', 'Outgoing Interface' is 'WAN (port1)', and 'Source' is 'all'. The 'Destination' is 'all'. The 'Schedule' is 'always' and 'Service' is 'ALL'. The 'Action' is set to 'ACCEPT' and 'IPsec'. The 'VPN Tunnel' is set to 'VPN Policy-Base'. The 'Protocol Options' are set to 'default'. The 'Security Profiles' section shows 'AntiVirus', 'Web Filter', 'DNS Filter', 'Application Control', 'IPS', and 'File Filter' all disabled. The 'Allow traffic to be initiated from the remote site' checkbox is unchecked. The 'OK' and 'Cancel' buttons are at the bottom right.

بعد.كدا.بنعمل ال policyاللي بتوجه الترافيك زي ما موضح.فالصورة
ولكن لابد تاخذ بالك أن ال Action IPsecوتحدد ال VPN Tunnel

Route-Based Configuration Steps

1.Create IPsec Tunnel

2.Create policy for each traffic direction

3.Create Static Route

Dashboard

Network

Policy & Objects

Security Profiles

VPN

Overlay Controller VPN

IPsec Tunnels

IPsec Concentrator

IPsec Wizard

IPsec Tunnel Template

SSL-VPN Portals

SSL-VPN Settings

SSL-VPN Clients

VPN Location Map

User & Authentication

System

Security Fabric

Log & Report

New VPN Tunnel

NameVPN Route-Based

CommentsComments0/255

Enable IPsec Interface Mode

Network

IP VersionIPv4IPv6

Remote GatewayStatic IP Address

IP Address192.168.1.15

InterfaceWAN (port1)

Local Gateway

Mode Config

NAT TraversalEnableDisableForced

Keepalive Frequency10

Dead Peer DetectionDisableOn IdleOn Demand

DPD retry count3

DPD retry interval20s

Forward Error CorrectionEgressIngress

Advanced...

Authentication

MethodPre-shared Key

Pre-shared Key

IKE

Version12

ModeAggressiveMain (ID protection)

Phase 1 ProposalAdd

EncryptionDESAuthenticationSHA1

Diffie-Hellman Groups

Key Lifetime (seconds)86400

Local ID

XAUTH

TypeDisabled

Phase 2 Selectors

Name	Local Address	Remote Address
VPN Route-Based	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0

New Phase 2

NameVPN Route-Based

CommentsComments

Local AddressSubnet0.0.0.0/0.0.0.0

Remote AddressSubnet0.0.0.0/0.0.0.0

Advanced...

Phase 2 ProposalAdd

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Diffie-Hellman Group

Local PortAll



Dashboard

Network

Interfaces

DNS

Packet Capture

SD-WAN

Static Routes

Policy Routes

RIP

OSPF

BGP

Routing Objects

Multicast

Policy & Objects

Security Profiles

VPN

User & Authentication

System

Security Fabric

Log & Report

New Static Route

Automatic gateway retrieval

Destination

Subnet Internet Service

10.10.10.0/24

Interface

Blackhole

Administrative Distance

10

VRF ID

0

Comments

Write a comment...

Status

Enabled Disabled

OK Cancel

User & Authentication

System

Security Fabric

Log & Report

Inspection Mode

Flow-based Proxy-based

Firewall / Network Options

NAT

Protocol Options

default

Security Profiles

AntiVirus

Web Filter

DNS Filter

Application Control

IPS

File Filter

OK Cancel

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles

VPN

User & Authentication

System

Security Fabric

Log & Report

New Policy

Name

VPN-route Based Policy

Incoming Interface

VLAN_10

VLAN_20

VLAN_30

Outgoing Interface

VPN Route-Based

Source

all

Negate Source

all

Negate Destination

all

Schedule

always

Service

ALL

Action

ACCEPT DENY IPsec

Inspection Mode

Flow-based Proxy-based

Firewall / Network Options

NAT

Protocol Options

default

Security Profiles

AntiVirus

Web Filter

DNS Filter

Application Control

IPS

File Filter

OK Cancel

VPN Route-Based	VLAN_10	VPN Route-Based	all	all	always	ALL	ACCEPT	Disabled	no-Inspection	UTM	0 B
VPN Route-Based	VLAN_20	VPN Route-Based	all	all	always	ALL	ACCEPT	Disabled	no-Inspection	UTM	0 B
VPN Route-Based	VLAN_30	VPN Route-Based	all	all	always	ALL	ACCEPT	Disabled	no-Inspection	UTM	0 B
VPN Route-Based	VLAN_40	VPN Route-Based	all	all	always	ALL	ACCEPT	Disabled	no-Inspection	UTM	0 B

3.Create Static Route

بنعمل static route وبنضع فيه ال destination Subnet اللي عاوز
اروح له وبنضع فال interface interface vpn tunnel
ويفضل نعمل static route ونضع فيه ال interface Black hole
لو ال tunnel وقع ميطلعش الترافيك ودا افضل من حيث ال Security
ويكون ال Administrative distance 254

The image displays two screenshots of the 'Edit Static Route' configuration window in a network management interface. The left sidebar shows the navigation menu with 'Static Routes' selected. The top screenshot shows a route configured for 'VPN Route-Based' interface with destination '10.10.10.0/255.255.0' and administrative distance '10'. The bottom screenshot shows a route configured for 'Blackhole' interface with destination '10.10.10.0/24' and administrative distance '254'.

Top Screenshot (VPN Route-Based):

- Automatic gateway retrieval: ☐
- Destination: Subnet Internet Service
- Interface: VPN Route-Based
- Administrative Distance: 10
- Comments: Write a comment... 0/255
- Status: ☒ Enabled ☐ Disabled

Bottom Screenshot (Blackhole):

- Automatic gateway retrieval: ☐
- Destination: Subnet Internet Service
- Interface: Blackhole
- Administrative Distance: 10
- VRF ID: 254
- Comments: Write a comment... 0/255
- Status: ☒ Enabled ☐ Disabled