

IPSec Site-to-Site VPN between 2 USG devices

This guide will demonstrate how to configure site-to-site IPSec VPN on USG devices. By doing this, hosts in the LAN sides will be able to reach the other side securely over the Internet.



- 1. Open your web browser and type the IP address of the device into the address bar (defaultLAN IP address : 192.168.1.1)
- 2. Login (default username : admin Password: 1234)
- 3. Create an address object for remote subnet (Configuration > Object > Address) On the site A device, add a subnet for 192.168.20.0/24

92.168.5.217/ext-js/web-pages/index/index.	html#		승 🚥 🚍
	and the second se		Welcome admin 100005 🛛 🤉 Help 🖉 Alcost. 🌩 Site Map 🗐 Okljest Reference 🖵 Console 🕤 CL1
Address Address Group			
Adress Adress Configuration PH4 Address Configuration PH4 Address Configuration Ress Address Configuration Ress Address Physical PhysicaPhysicaPhysicaPhysicaPhysicaPhysicaPhysicaPhysicaPhysica	Type Type INTERFACE SUBNET HOST INTERFACE SUBNET INTERFACE INTE	IPv4 Address dm2-192.168.3.024 192.89.09.1 lse-1-192.168.3.024 ser-1-192.168.5.024 ende_105040 sert_1152 sert_1152	Partemence 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
	Retmaa: 2	IS 255 255 0	
	92.168.5.217/cxt js/web pages /index/index	92.168.5.217/cxt-js/web-pages/index.html#	92.168.5.217/ctr-js/vet-pages/index/index.html#



Products apply USG20/20W/40/40W/60/60W

On the site B device, add a subnet for 192.168.10.0/24

← → C 🔒 https://192.16	8.5.214/ext-js/web-pages/index/index.html#			승 💩 🚍
ZyXEL USG40				Welcome admini I Loopoli 🤇 ? Helo 🕱 Alooci 🗳 Sha Nao 🖾 Oldeci Reference 🖵 Console 🛅 O.1
CONFIGURATION	Address Group			
	IPv4 Address Configuration			
- Web Authentication	# Name *	Тура	IPv4 Address	Reference
	1 DMZ_SUBNET	INTERFACE SUBNET	dmz-192.168.3.0/24	0
	2 IP0to4-Relay	HOST	192.88.99.1	0
- IFAUG VPN - SSL VPN	3 LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.20.0/24	0
	4 LAN2_SUBNET	INTERFACE SUBNET	lan2-192.168.2.0/24	0
- BWM	5 WIZ LAN SUBNET	INTERFACE SUBNET	wan1-192.108.5.0/24	U
Object Zone	14 4 Page 1 of 1 P PI Show 50 ¥ items			Displaying 1 - 5 of 5
- User/Group		📣 Add Address Rule	2. 30	
		Name	Remote 100040	
		Address Tupe:	SUBJET Y	
		Network	102.148.10.0	
		Rielmank	230 230 230 0	
			OK CHKH	

 Create a VPN Gateway on both devices (Configuration > VPN > IPSec VPN > VPN>ateway>Add)

SITE A DEVICE

- Enable
- My address as wan1
- Peer gateway address with a static IP address of the wan 1 on site 2 (192.168.5.214)
- Pre-shared key for authentication

	VPN Connection VPN Gateway Core	entrator Configuration Provisioning		Welcone admin Locat 9 Help - Z About	# Sta Hap 🗍 Original Reference: 🤤 Console 🗇 O.
T Coxesing Locaning Locaning National National South Protoco National South Protoco South Protoco Sout	PH Configuration Configuration Status Nore Nore Nore Nore Nore N	Institute Constant information Constant information	10.000 100000 100000 W0 00jcl + 100000 100000 100000 Wen1 100000 100000 100000 100000 Wen1 100000 100000 100000 100000 100000 Primary 1000000 1000000 1000000000 1000000000000000000000000000000000000	Cancel	IKE Version No data to diselary



Products apply USG20/20W/40/40W/60/60W

Pre-Shared Key	•••••		
unmasked			
Certificate	default	(See My Certificates)	-
User Based PSK		× 1	
hase 1 Settings			
SA Life Time:	86400	(180 - 3000000 Seconds)	
Negotiation Mode:	Main	~	
			OK Cancel

SITE B DEVICE

- Enable
- My address as wan1
- Peer gateway address with a static IP address of the wan 1 on SITE A (192.168.5.217)
- Pre-shared key for authentication

O Add VPN Gateway	1002.0040	unaku Sautura Sauturay	×
🔟 Show Advanced Settings)bject 🗸		
General Settings			
Enable VPN Gateway Name:	115640.2		
IKE Version IKEv1 KEv2	00010_2		
Gateway Settings			
My Address Interface Domain Name / IPv4 	wan1	Static 192.168.5.214/255.255.255.0	
Peer Gateway Address Static Address 	Primary Secondary	192.168.5.217 0.0.0.0	
Fall back to Primary Peer Gate	way when po	ossible	
Fall Back Check Interval:	300	(60-86400 seconds)	
Dynamic Address 1			
Authentication			
		OK Cancel	

Pre-Shared Key	•••••	
📄 unmasked		
Certificate	default	 (See My Certificates)
User Based PSK		· 1
ase 1 Settings		
SA Life Time:	86400	(180 - 3000000 Seconds)
Negotiation Mode:	Main	*



Products apply USG20/20W/40/40W/60/60W

5. Ensure both are created successfully

YXEL USG40				Welcome eomin 100000 Yhep 2 Accur	🖕 Sie Hep Tigloget Helerence 🖵 Lonso
CONFIGURATION	VPN Connection VPN Gateway Concentrator Configuration Pro	visioning			
T¥ Quick Setup	IPv4 Configuration				
Wireless	🙆 Add 🍞 Edit 🍵 Remove 🤤 Activate 👰 Inactivate 📻 Object Referer	0			
Network Web Authentication	# Status Name	My Address	Secure Gateway	VPN Connection	IKE Version
	1 🤪 USG40_1	-wan1	192.168.5.214		IKEv1
 ■ <u>CRANTRI</u> SSL VPN UTP VPN UTP VPN ■ UTP vPnIa © Object © Object © System ■ Log & Report 	I ⁴ 4 Rape 1 d ² 1 ≥ 2 Story <u>9 v</u> , terms				Disolaying 1 - 1 o
			Arribe Bacat		

- 6. Create VPN connection (Configuration > VPN > IPSec VPN > VPN Connection > Add) Site A device
 - Enable
 - Site-to-Site
 - VPN Gateway as the gateway created on step 5
 - Local policy : LAN_SUBNET 192.168.10.0
 - Remote policy : Address created on step 3 192.168.

Z	YXEL USG40					Welcome admin Count Vitelp Z Alout # Site He	p 😰 Object Reference: 🖵 Conscile 🛄 C
	CONFIGURATION	VPN Connection VIW Ge	ieway Concentrator Configuration Pro	walacing			
	TV Quick Setup	Global Setting					
	Licensing Winkes Winkes Network Wob Authentication Security Policy	Use Policy Route to co I Ignore "Don't Fragment IPv4 Configuration	trol dynamic IPSec rules	7.X			
	- IRSTOWED - SSL VPN	0 Add _2 100 1 10000	General Settings			2.5	
	LETP VPN BWM UTM Profile	P Status	Connection Name:	toRemoteUSG40		*cy	No deta to display
	- Zone		VPN Gateway				
	UserCloup AP Profile Application Admes Schodule Schodule Adhouse Adhouse		Application Scenario Site-to-site Site-to-site Remote Access (Cerver Role) Remote Access (Client Role) VM Gateway: Balance	USG40_1	wan1 192.168.5.214,00.0.0		
	SSL Application System		Local policy:	LAN1 SLIBNET	INTERFACE SUBNET, 192 168 10 0/24		
			Remote policy:	Remote_USG40	SUBNET, 192.168.20.0/24		
			Phase 2 Setting				
			SA Life Time:	86400 (1	80 - 3000000 Seconds)		
					(OK Cancel	



Products apply USG20/20W/40/40W/60/60W

ew Object 🗸		
LANT JODINE	INTERAOL CODITET, TOL. TOU. TO. TO.	
Remote_USG40	SUBNET, 192.168.20.0/24	
86400	(180 - 3000000 Seconds)	
IPSec_VPN	× []	
	×	
5 (5-600 S	ieconds)	
5 (1-10 Se	sconds)	
(1-10)		
	(Domain Name or IP Address)	
Address in the Remote P	Policy	
	W Object + Lens_counct Remote_USG40 86400 IPSec_VPN (5-600 S (1-10 Se (1-10) (1-10) Address in the Remote F	W Object + Interv Hole Object +, Hole Object +, Hole Hole Object +, Hole Obj

On the site 2 device

- Enable
- Site-to-Site
- VPN Gateway as the gateway created on step 5
- Local policy : LAN_SUBNET 192.168.20.0
- Remote policy : Address created on step 3 192.168.10.0

CONFIGURATION	VPN Connection VPN Gat	away Concentrator Configuration Pro	visioning			
	Global Setting					
Wireless Network Web Authentication Research: Dolog	Use Policy Route to con	trol dynamic IPSec rules			7 X	
E VPN	IPv4 Configuration	I Show Advanced Settings I Create new C	bject +			
SSL VPN	Q Add 2 Dill 1 Rends	General Settings			100	
L2TP VPN DWM UTM Profile Object Zone	# Status	Enable Connection Name: VPN Gateway	toRemoteUSG40		akcy	No data to display
UserOfnop AP Profile Acylication Address Schoole Schoole Schoole Address Schoole Address Address Address Address Address Address Method Contribution ISP Account SSL Application		Application Scenario Ste-to-site Ste-to-site with Dynamic Peer Remote Access (Gerver Role) Remote Access (Client Role) VPN Gateway: Policy	usch0,2 ×	wan1 192,168.5.217, 0.0.0.0		
⊜ System ⊕ Log & Report		Local policy: Remote policy: Phase 2 Setting	UN1_SUBNET * Remote_USGH0 *	INTERFACE SUBNET, 192.168.20.0/24 SUBNET, 192.168.10.0/24	_	
		SA Life Time:	86400 (180	3000000 Seconds)		



Products apply USG20/20W/40/40W/60/60W

7. Connect VPN on both devices (Click Connect)



When it's connected the status will change to END

