Accès NAT d'un VLAN sur Internet

Sommaire :

1.	Configuration du LAN 1	2
2.	Paramétrage des règles de pare-feu	3

Maintenant que l'on sait comment aller administrer le routeur, nous allons essayer d'obtenir une connexion Internant sur le premier VLAN de celui-ci. Cela nous sera utile pour la communication entre les différents VLAN.

1. Configuration du LAN 1

Premièrement, nous devons ajouter un autre câble RJ-45 sur le port 4 du routeur, que l'on relie à la goulotte de l'îlot.



Avant d'essayer d'obtenir une connexion Internet, il faut que le réseau dans lequel on se trouve soit correctement paramétré. Pour cela, on clique en haut sur l'onglet « Interface », puis sur « LAN ». Si tout est bon, la page suivante devrait s'afficher.

COMMUNITY EDITION	← Interfaces ← Firewall ←	Services - VPN -	Status 🗸	Diagnostics 🕶 Help 🕶	4 2 🕞
WARNING: The 'admin' acco	ount password is set to the default vi	alue. Change the password in th	ie User Manager.		
Interfaces / LAN	(igb1)				莘 🔟 🛛
General Configuratio	n				
Enable	✓ Enable interface				
Description	LAN Enter a description (name) for the	interface here.			
IPv4 Configuration Type	Static IPv4		~		
IPv6 Configuration Type	Track Interface		~		
MAC Address	xxxxxxxxxxxxxx This field can be used to modify (" Enter a MAC address in the follow	spoof") the MAC address of this	s interface. eave blank.		
мти	If this field is blank, the adapter's o	lefault MTU will be used. This is	typically 1500 b	ytes but can vary in some circum	stances.
MSS					
	If a value is entered in this field. th	en MSS clamping for TCP conn	ections to the val	ue entered above minus 40 (TCP	/IP header size) will be in effect.

Ensuite, cocher la case « Enable Interface » si elle n'est pas déjà cochée, descendre en bas de la page et cliquer sur « Save ». Remonter et Appliquer les changements. Il n'y a pas à modifier l'adresse par défaut de ce premier réseau, donc la configuration de celui-ci était assez courte.

2. Paramétrages des règles de Pare-feu

Maintenant que le réseau est bien délimité, il est important d'établir des règles de pare-feu pour établir une connexion Internet. Pour accéder à la page de celles-ci, il faut cliquer sur l'onglet « Firewall », puis « Rules ». On peut ensuite établir des règles pour chaque réseau.

Ici, nous allons nous concentrer sur le WAN et le LAN 1.

Règles à introduire pour le WAN :

Fi	Firewall / Rules / WAN									<u>III</u> 🗐 🕄		
Floating WAN LAN LAN2 LAN3												
Ru	Rules (Drag to Change Order)											
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	×	0 /22 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	0
	×	0 /8 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	0
	~	0 /0 B	IPv4 *	*	*	*	*	*	none			₺₡₢₡
	~	0 /0 B	IPv4 *	*	*	*	*	*	none			≟∥⊡⊘₫

Règles à introduire pour le LAN 1 :

Fi	Firewall / Rules / LAN								± Ш ■ 0			
Flo	oating	WAN	LAN	LAN2	LAN3							
Ru	les ((Drag to Chan	ge Order)								
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	*	3 /16.34 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	٥
	~	10 /902 KiB	IPv4*	LAN net	*	*	*	*	none		Default allow LAN to any rule	≟∥⊡⊘₫

Ces règles sont essentielles pour autoriser le poste à se connecter à Internet.

Si tout cela est bien fait, on devrait obtenir l'accès à Internet. On vérifie cela à l'aide d'une commande Ping (taper « CMD » dans la barre de recherche Windows) suivie d'une adresse internet :

Invite de commandes	_		Х				
::\Users\SISR>ping www.google.com							
Envoi d'une requête 'ping' sur www.google.com [216.58.214.164] avec 32 octets de données : Réponse de 216.58.214.164 : octets=32 temps=12 ms TTL=113 Réponse de 216.58.214.164 : octets=32 temps=12 ms TTL=113 Réponse de 216.58.214.164 : octets=32 temps=12 ms TTL=113 Réponse de 216.58.214.164 : octets=32 temps=12 ms TTL=113							
<pre>Statistiques Ping pour 216.58.214.164: Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%), Durée approximative des boucles en millisecondes : Minimum = 12ms, Maximum = 12ms, Moyenne = 12ms C:\Users\SISR>arp -a</pre>							
Interface : 192.168.1.8 0x6							
Adresse Internet Adresse physique Type 192.168.1.1 40-62-31-07-bc-c7 dynamique Adresse de passerelle LAN 1 192.168.1.255 ff-ff-ff-ff statique Adresse de diffusion	L						
224.0.0.251 01-00-5e-00-00-fb statique 224.0.0.252 01-00-5e-00-00-fb statique 239.255.102.18 01-00-5e-7f-66-12 statique 239.255.250 01-00-5e-7f-ff-fa statique							
C:\Users\SISR>_			v				

Comme nous recevons une réponse de l'adresse internet de Google, on en conclut que nous avons bien réussi à établir une connexion Internet sur le LAN 1.

La requête arp –a permet de savir quelles sont les machines connectées au réseau et quelles sont leurs adresses mac.

es. In	vite de comn	nandes					-	×
Envoi Répon Répon Répon Répon	d'une re ise de 210 ise de 210 ise de 210 ise de 210	equête 'pi 6.58.214.1 6.58.214.1 6.58.214.1 6.58.214.1 6.58.214.1	ing'sur 164 : oct 164 : oct 164 : oct 164 : oct	www.google.com [216.5 ets=32 temps=12 ms TT ets=32 temps=12 ms TT ets=32 temps=12 ms TT ets=32 temps=12 ms TT	8.214.164] avec 32 octet L=113 L=113 L=113 L=113 L=113	s de données :		Â
Stati P Durée M	stiques Paquets : e approxin linimum =	Ping pour envoyés = mative des 12ms, Max	216.58.2 4, reçu 5 boucles 1 mum = 1	14.164: is = 4, perdus = 0 (pe s en millisecondes : .2ms, Moyenne = 12ms e com	rte 0%),			
C:\US	ens/212K	>tracert w	ww.goog1	.e.com				
Déter	mination	de l'itin	néraire v	vers www.google.com [2	16.58.214.164]			
avec	un maxim	um de 30 s	auts :		-		_	
1 2	<1 ms <1 ms	<1 ms <1 ms	<1 ms <1 ms	192.168.1.1 172.16.21.1	}	Adresse de passerelle LAN 1 Adresse de la goulotte		
3	1 ms	1 ms	<1 MS	5.50.84.02				
4	2 ms	1 ms	1 ms	31.33.19.2				
5	*	*	*	Délai d'attente de l	a demande dépassé.			
6	*	*	*	Délai d'attente de l	a demande dépassé.			
	10 mc	10 mc	11 MS	62.34.2.18/	hov fp [313 104 171 06]			
a a	12 m5 *	12 ms	12 ms	62 24 2 E9	DOX.TP [212.194.1/1.96]			
10	12 ms	12 ms	12 ms	72 14 204 68				
11	13 ms	13 ms	13 ms	216.239.40.75				
12	12 ms	12 ms	11 ms	216.239.48.43				
13	12 ms	12 ms	12 ms	par10s42-in-f4.1e100	.net [216.58.214.164]			~

La commande tracert permet de voir le chemin que prennent es paquets lors du ping. Ici, on voit qu'ils passent bien par l'adresse de passerelle du LAN 1.

2 TS SIO

Routage et Filtrage entre les LAN 2 et 3

Sommaire :

1 – Création et configuration des LAN 2 et 3	02
2 – Mise en place des règles de parefeu	06
3 – Test de connectivité entre les LANs 2 et 3	07

1- Création et configuration des LAN



Il faut avant tout brancher les câbles sur les ports suivants :

Notre première étape va être de créer et configurer les deux LAN dans l'interface.

On prend d'abord sur les ordinateurs une configuration réseau conforme en allant dans Paramètres \rightarrow Centre réseau et Partage \rightarrow Ethernet 2 \rightarrow Propriétés \rightarrow Protocole Internet version 4.

Propriétés de : Protocole Internet version 4 (TCP/IPv4)	×	Propriétés de : Protocole Internet version 4 (TCP/IPv4)
Général		Général
Les paramètres IP peuvent être déterminés automatiquemer réseau le permet. Sinon, vous devez demander les paramètr appropriés à votre administrateur réseau. Obtenir une adresse IP automatiquement Utiliser l'adresse IP suivante : Adresse IP : Masque de sous-réseau : Passerelle par défaut : 10 . 0 . 23 . 10 . 0 . 23 .	t si votre es IP Configuration IP du poste en LAN 2 8 0 54	Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau. Obtenir une adresse IP automatiquement © Utiliser l'adresse IP suivante : Adresse IP : 192.168.3.221 Masque de sous-réseau : 255.255.192 Passerelle par défaut : 192.168.3.254
Obtenir les adresses des serveurs DNS automatiquemer Ottiliser l'adresse de serveur DNS suivante :		Obtenir les adresses des serveurs DNS automatiquement OUtiliser l'adresse de serveur DNS suivante :
Serveur DNS préféré :		Serveur DNS préféré :
Valider les paramètres en quittant	Avancé Configuratio	Nalider les paramètres en quittant Avancé
ОК	Annuler du poste en	LAN 3 OK Annuler

Pour cela, il faut cliquer sur les <u>onglets « Interfaces » \rightarrow « Assignments »</u>, puis en bas à droite dans le tableau des interfaces, cliquer sur « + Add », puis sauvegarder les modifications en appuyant sur « Save ».

	COMMUNITY EDITION	stem -	Interfaces 🕶	Firewall -	Services -	VPN 🗸	Status 🕶	Diagnostics	← Help ←		
	WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.										
	Interfaces / Interface Assignments										
	Interface Assignmen	its In	terface Groups	Wireless	VLANs	QinQs	PPPs GR	Es GIFs	Bridges	LAGG	s
	Interface	Network port									
	WAN	igb0 (40:62:31:07:bc:c6)					*				
	LAN	igb1 (40:62:31:07:bc:c7)						Delete			
	LAN2	igb2 (40:62:31:07:bc:c8)					~	Delete			
	LAN3				igb3 (40:62	2:31:07:bc:c9))			*	Delete
uvegarder	Available network port	igb4 (40:62:31:07:bc:ca)					~	+ Add			
<u> </u>	🖺 Save							Alaut			
dification											A jout
E	insuite, on clio	que su	ir le nom d	de la nou	ivelle in	terface	, puis on	la renom	me en		

fonction du LAN correspondant.

A présent, on configure les LAN correctement. Pour le LAN 2, je donne l'adresse IP **10.0.23.254 /23**. Le LAN 3 quant à lui est assigné en **192.168.3.254 /26**.

LAN 2 :

COMMUNITY EDITION		Firewall 🕇	Services 🕶	VPN -	Statu
WARNING: The 'admin' acc	ount password is set t	o the default valu	<mark>ie.</mark> Change the p	assword in th	e User N
Interfaces / LAN	2 (igb2)				
General Configuratio	n				
Enable	Enable interface	9			
Description	LAN2				
	Enter a description	(name) for the in	terface here.		
IPv4 Configuration Type	Static IPv4				~

Static IPv4 Configura	tion	
IPv4 Address	10.0.23.254	/ 23 🗸
IPv4 Upstream gateway	None Add a new gateway	
	If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the On local area network interfaces the upstream gateway should be "none". Gateways can be managed by click	'Add" button. ng here.
Reserved Networks		
Block private networks and loopback addresses	Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.10 RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless private address space, too.	38/16) and unique loca this network interface
Block bogon networks	Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixe routing table, and so should not appear as the source address in any packets received. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.	s that should never ap;
	E Save	
LAN 3 : DEFSENSE COMMUNITY EDITION WARNING: The 'ad	System ▼ Interfaces ▼ Firewall ▼ Services ▼ VPN ▼ Statu Imin' account password is set to the default value. Change the password in the User N	
Interfaces /	LAN3 (igb3)	
General Config	guration	
	Enable 👩 Enable interface	
Desc	ription LAN3	
ID: 4.0 6 ti-	Enter a description (name) for the interface here.	
Static IPv4 Configuration	ration	
IPv4 Address	192.168.3.254	/ 26 🗸

	192.100.0.204		7 20 +
IPv4 Upstream gateway	None	➤ Add a new gatew	way
	If this interface is an Internet connection, select an ex On local area network interfaces the upstream gatew.	isting Gateway from the list or add a new one ay should be "none". Gateways can be manag	using the "Add" button. ed by clicking here.
Reserved Networks			
Block private networks and loopback addresses	D Blocks traffic from IP addresses that are reserved for RFC 4193 (fc00::/7) as well as loopback addresses (1 private address space, too.	private networks per RFC 1918 (10/8, 172.16, 27/8). This option should generally be turned	/12, 192.168/16) and unique local on, unless this network interface (
Block bogon networks	D Blocks traffic from reserved IP addresses (but not RF routing table, and so should not appear as the source Note: The update frequency can be changed under Sy	C 1918) or not yet assigned by IANA. Bogons address in any packets received. /stem > Advanced, Firewall & NAT settings.	are prefixes that should never app
	🖺 Save		

Quand notre configuration est terminée, on appuie sur le bouton bleu « Save » en fin de page.

2- Mise en place des règles de pare-feu

Une fois les LAN créés, il est important de contrôler les échanges entre les différents réseaux. Pour cela, nous allons créer des règles de pare-feu sur le routeur. Dans l'interface, cliquer sur l'onglet <u>« Firewall » \rightarrow « Rules ».</u>

Par défaut, deux règles sont crées automatiquement lors de la création d'une nouvelle interface.

LAN 2 :

		System -	Interfaces		•	Services -	VPN -	Status 🕶	Diagnosti	cs - Hel	p -	()
WA	RNING	: The 'admin' accoui	nt password is	set to the defau	lt value.	Change the pas	sword in the	User Manager				
Fir	ewa	ll / Rules / L	AN2									‡ III ■ 0
Flo	ating	WAN LAI	N LAN2	LAN3								
Ru	es (D	rag to Change	Order)									
		States	Protocol	Source	Port	Destination	Por	t Gateway	Queue	Schedule	Description	Actions
	~	1 /5.73 MiB	IPv4 *	*	*	LAN2 addres	ss *	*	none			≟∥⊡⊘₫
	•	2 /350.13 MiB	IPv4 *	LAN2 net	*	*	*	*	none			≟∥⊡⊘₫
										1 Add 1	Add 前 Delete	🖺 Save 🕂 Separator

LAN 3 :

Fi	rewal	II / Rules /	LAN3									÷ 🔟 🗖 9
Flo	pating	WAN LA	AN LAN2	LAN3								
Ru	les (D	rag to Change	e Order)									
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	~	States 1 /4.28 MiB	Protocol	*	Port *	Destination LAN3 address	Port *	Gateway	Queue none	Schedule	Description	Actions
	 	States 1 /4.28 MiB 4 /5.89 MiB	Protocol IPv4 * IPv4 *	Source * LAN3 net	Port * *	Destination LAN3 address *	Port * *	Gateway * *	Queue none none	Schedule	Description	Actions ♣ ✔ □ ⊘ ⑪ ♣ ✔ □ ⊘ ⑪

Pour l'instant, cela est suffisant pour notre environnement de travail.

3- Test de connectivité entre les LAN 2 et 3

Maintenant que tout est correctement paramétré sur l'interface, nous devons nous assurer que les deux réseaux peuvent effectivement communiquer entre eux, et qu'ils passent par le bon chemin.

Pour cela, nous allons faire deux types de test différents :

- Un ping suivi d'un tracert pour vérifier que l'on passe bien par le bon chemin, dans un sens puis dans l'autre
- Un ping suivi d'un arp –a pour vérifier que <u>l'ordinateur retiens bien les</u> bonnes adresses, dans un sens puis dans l'autre

LAN 2 vers LAN 3 :



C:\Users\SISR>ping 192.	168.3.221			
Envoi d'une requête 'Pi Réponse de 192.168.3.22 Réponse de 192.168.3.22 Réponse de 192.168.3.22 Réponse de 192.168.3.22	ng' 192.168.3.221 av 1 : octets=32 temps<1 1 : octets=32 temps<1 1 : octets=32 temps<1 1 : octets=32 temps<1	ec 32 octets ms TTL=127 ms TTL=127 ms TTL=127 ms TTL=127 ms TTL=127	de données :	Le ping a f machines
Statistiques Ping pour Paquets : envoyés = Durée approximative des Minimum = Oms, Maxi	192.168.3.221: 4, reçus = 4, perdus boucles en milliseco mum = 0ms, Moyenne =	= 0 (perte 0 ndes : Oms	%),	
C:\Users\SISR>apr -a 'apr' n'est pas reconnu ou externe, un programm	en tant que commande e exécutable ou un fi	interne chier de comm	andes.	
C:\Users\SISR>arp -a				
Interface : 169.254.217 Adresse Internet 169.254.255.255 224.0.0.22 224.0.0.251 224.0.0.252 239.255.255.250	.22 0x4 Adresse physique ff-ff-ff-ff-ff-ff 01-00-5e-00-00-16 01-00-5e-00-00-fb 01-00-5e-00-00-fc 01-00-5e-7f-ff-fa	Type statique statique statique statique statique		
Interface : 10.0.23.8 -	0x6 Adresse physique	Туре		La command
10.0.23.254 10.0.23.255 224.0.0.22 224.0.0.251	40-62-31-07-bc-c8 ff-ff-ff-ff-ff-ff 01-00-5e-00-00-16 01-00-5e-00-00-fb	dynamique statique statique statique		enregistré la les requêtes
224.0.0.252 239.255.102.18 239.255.255.250	01-00-5e-00-00-fc 01-00-5e-7f-66-12 01-00-5e-7f-ff-fa	statique statique statique		

Le ping a fonctionné : les deux machines communiquent entre elles

La commande montre que l'ordinateur a enregistré la bonne adresse de passerelle pour les requêtes du LAN 2 vers le LAN 3

LAN 3 vers LAN 2 :

C:\Users\SISR>ping 10.0.23.8	
Envoi d'une requête 'Ping' 10.0.23.8 avec 32 octets de données : Réponse de 10.0.23.8 : octets=32 temps<1ms TTL=127 Réponse de 10.0.23.8 : octets=32 temps<1ms TTL=127 Réponse de 10.0.23.8 : octets=32 temps<1ms TTL=127 Réponse de 10.0.23.8 : octets=32 temps<1ms TTL=127	Le ping a fonctionné : les deux machines communiquent entre elles
<pre>Statistiques Ping pour 10.0.23.8: Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%), Durée approximative des boucles en millisecondes : Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms C:\Users\SISR>tracert 10.0.23.8</pre>	
Détermination de l'itinéraire vers 10.0.23.8 avec un maximum de 30 sauts. 1 <1 ms <1 ms <1 ms 192.168.3.254 2 <1 ms <1 ms <1 ms 10.0.23.8	La commande montre que les requêtes passent d'abord par le routeur sur le port LAN 3, puis arrivent à destination
Itineraire determine.	

C:\Users\SISR>ping 10.0.23.8

Envoi d'une requête 'Ping' 10.0.23.8 avec 32 octets de données Réponse de 10.0.23.8 : octets=32 temps<1ms TTL=127 Réponse de 10.0.23.8 : octets=32 temps<1ms TTL=127 Réponse de 10.0.23.8 : octets=32 temps<1ms TTL=127 Réponse de 10.0.23.8 : octets=32 temps<1ms TTL=127

Statistiques Ping pour 10.0.23.8: Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%), Durée approximative des boucles en millisecondes : Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\SISR≻arp -a

Interface : 192.168.3.221 --- 0x5

Adresse Internet	Adresse physique	Туре
192.168.3.254	40-62-31-07-bc-c9	dynamique
192.168.3.255	ff-ff-ff-ff-ff	statique
224.0.0.22	01-00-5e-00-00-16	statique
224.0.0.251	01-00-5e-00-00-fb	statique
224.0.0.252	01-00-5e-00-00-fc	statique
239.255.102.18	01-00-5e-7f-66-12	statique
239.255.255.250	01-00-5e-7f-ff-fa	statique
255.255.255.255	ff-ff-ff-ff-ff	statique

Le ping a fonctionné : les deux machines communiquent entre elles

La commande montre que l'ordinateur a enregistré la bonne adresse de passerelle pour les requêtes du LAN 3 vers le LAN 2

2 TS SIO

Prise en main administrative du PFSense



Dans ce document, nous allons voir comment se connecter pour la première fois à l'interface d'un un routeur PFSense.

1. Initialisation du routeur

Avant de commencer à utiliser le routeur, il faut correctement le brancher et le relier à l'environnement. Nous allons donc brancher un câble RJ-45 sur le port 5 (le port 6 est réservé pour le WAN).



Ensuite, nous allons installer une configuration réseau (adresse IP, masque, interface dans le même réseau que le routeur) compatible avec l'adresse par défaut du PFSense (192.168.1.1). Pour aller modifier cela, il faut se rendre dans les Paramètres -> Réseau et Internet -> Centre Réseau et Partage -> Ethernet 2 -> Propriétés -> Protocole Internet version 4. On rentre ensuite les informations, et quelque on doit obtenir quelque chose de ce style :

ropriétés de : Protocole Internet	version 4 (TCP/IPv4)	\times	
Général			
Les paramètres IP peuvent être d réseau le permet. Sinon, vous dev appropriés à votre administrateur	éterminés automatiquement si votr vez demander les paramètres IP réseau.	e	
Obtenir une adresse IP auto	matiquement		
• Utiliser l'adresse IP suivante			
Adresse IP :	192.168.1.6		Adresse IP du poste
Masque de sous-réseau :	255.255.255.0		
Passerelle par défaut :	192 . 168 . 1 . 1	←	Adresse de l'interface du
Obtenir les adresses des serv	veurs DNS automatiquement		
Utiliser l'adresse de serveur [DNS suivante :		
Serveur DNS préféré :	8.8.8.8		

Pour vérifier que la configuration est bonne, on peut, avant de se connecter au routeur, tenter une commande Ping dans l'invite de commande (taper « CMD » dans la barre de recherche Windows) vers son adresse. On devrait avoir une réponse du routeur :

Microsoft Windows [version 10.0.19044.2 (c) Microsoft Corporation. Tous droits	604] réservés.
C:\Users\SISR>ping 192.168.1.1	Adresse de l'interface du routeur
Envoi d'une requête 'Ping' 192.168.1.1	avec 32 octets de données
Réponse de 192.168.1.1 : octets=32 temp	s<1ms TTL=64
Réponse de 192.168.1.1 : octets=32 temp	s<1ms TTL=64
Réponse de 192.168.1.1 : octets=32 temp	s<1ms TTL=64
Réponse de 192.168.1.1 : octets=32 temp	s<1ms TTL=64

Puis, on va maintenant sur un navigateur et on rentre l'adresse du routeur.

<mark>pf</mark> sense		Login to pfSense
	SIGN IN	
	SIGN IN	

Des identifiants vous sont demandés. Par défaut, ce sont :

User = admin

Password = pfsense

Une fois cela fait, vous devriez accéder à l'interface du PFSense :

Status / L	ashboard	+ 0
System Info	rmation F 🕫 S	Netgate Services And Support 🗢 3
Name	pfSense.localdomain	Contract time Community Support
User	admin@192.168.1.6 (Local Database)	Community Support Only
System	pfSense Netgate Device ID: 561af036cc7fb587a47e	NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES
BIOS	Vendor: American Megatrends Inc. Version: 5.12 Release Date: Fri Nov 23 2018	If you purchased your pfSense gateway firewall appliance from Netgate and elected
Version	2.4.5-RELEASE-p1 (amd64) built on Tue Jun 02 17.51:17 EDT 2020 FreeBSD 11.3-STABLE Obtaining update status •	between you have access to various community support resources. This includes that water, you have access to various community support resources. This includes the NETGATE RESOURCE LIBRARY. You also may upgrade to a Variaged cilosal technical Assistance Center (TAC) Support subscription. We're always on Our team is stated 24x7x355 and exemption du adjunction entering in direct workshale surged at a variable support as the technical exemption.
СРU Туре	Intel(R) Core(TM) I5-6200U CPU @ 2.30GHz Current: 2200 MHz, Max: 2301 MHz 4 CPUs: 1 package(s) x 2 core(s) x 2 hardware threads AES-NI CPU Crypto: Ves (inactive)	Origination of contrasting strategistics, with white support and price point that is more than competitive when compared to others in our space. Upgrade Your Support Community Support Resources Netgate Global Support FAQ Official pfSense Training by Netgate
Kernel PTI	Enabled	Natrata Professional Services Visit Natrate com