

Le serveur DHCP de votre Livebox attribue automatiquement une adresse IP à chaque équipement de votre réseau local.

Uniquement pour des équipements IPv4.

Paramètres du serveur DHCP

Activer le serveur DHCP

Adresse IP de votre Livebox

Masque de sous-réseau du LAN

Adresse IP de début

Adresse IP de fin

Annuler

Enregistrer

Baux DHCP statiques

Attribuez vous-même une adresse IP à votre équipement.

Ajouter

Équipement	Adresse IP statique	Adresse MAC	
HP-ENVY	10.0.1.41	EC:8E:B5:F7:FE:94	
Équipement	10.0.1.44	00:15:C5:49:FD:E0	
Équipement	10.0.1.35	A4:9A:58:30:61:32	
Équipement	10.0.1.37	A8:FA:D8:D3:3D:34	
Équipement	10.0.1.40	00:0E:7F:38:FB:D5	
Équipement	10.0.1.126	00:13:F6:01:13:A3	
Équipement	10.0.1.51	F8:1E:DF:DF:09:B0	
Équipement	10.0.1.52	34:15:9E:02:91:F0	
LAW10	10.0.1.47	00:1E:C9:37:54:DA	
hp402	10.0.1.49	98:E7:F4:A5:12:6E	
Équipement	10.0.1.53	90:CD:B6:2B:9A:E2	
NAS542	10.0.1.99	D8:EC:E5:44:6F:F6	
Équipement	10.0.1.61	E0:DB:10:6C:15:33	
Équipement	10.0.1.56	A4:4C:C8:18:DC:DE	
Mele-001D63FFFE/57A6E	10.0.1.18	00:1D:63:75:7A:6E	
Équipement	10.0.1.19	14:9F:3C:D9:CE:15	
iphone Monica	10.0.1.20	F6:C1:72:D9:99:C2	
Air-de-Monique	10.0.1.54	C0:95:6D:25:C7:B3	
canalplus-g7	10.0.1.17	84:E0:58:BB:DF:EC	
dLAN #4 BuroYves	10.0.1.101	00:0B:3B:41:C4:C6	
dLAN #6 LB	10.0.1.102	00:0B:3B:41:C6:15	
Équipement	10.0.1.25	6C:3C:7C:FA:A3:17	
E5480	10.0.1.50	10:65:30:F1:1F:56	
Cruiser-5MP Eth	10.0.1.27	A8:31:62:2A:91:AF	
Device-17-inconnu	10.0.1.26	34:98:B5:9F:90:FE	
Imou-IPC-B32	10.0.1.29	A8:31:62:3F:86:95	
Équipement	10.0.1.28	A8:31:62:2A:A1:27	
dLAN #8 Canal+	10.0.1.105	00:0B:3B:49:1F:4C	
Clim Séjour	10.0.1.32	EB:C7:CF:85:2D:01	
Clim Yves	10.0.1.33	58:E4:03:E5:EB:3E	
dLAN #5 SdB	10.0.1.100	00:0B:3B:41:B5:07	
Équipement	10.0.1.103	F4:06:8D:D9:E1:A7	
TV Monique	10.0.1.30	FC:F1:52:BD:05:32	
dLAN #7 MoniqueTV	10.0.1.104	00:0B:3B:49:20:A8	
Clim Monique	10.0.1.36	8C:53:E6:04:DC:FC	

Les règles NAT/PAT sont nécessaires pour autoriser une communication initiée depuis Internet avec un équipement particulier de votre réseau. Utiles pour certaines applications comme des jeux en lignes ou des serveurs de type FTP ... Assurez-vous que cet équipement a une adresse IP statique (paramétrable dans l'onglet DHCP).

Uniquement pour des équipements IPv4.

Vos règles personnalisées

Choisissez des ports qui ne sont pas bloqués par le pare-feu.

Nous vous déconseillons la création d'une règle sur le port 53 (service DNS).

Les équipements doivent être configurés avec une adresse IP statique pour être disponibles.

ex. : 1000

ex. : 1000-2000

IP externes autorisées

CréerUne règle NAT/PAT

Activer	Application/Service	P int	P ext	Proto	Équip	IP externe
	Web_20Server_20_28HTTP_29	80	80	TCP	0.0.0.0	Toutes
x	FTP_20Server	21	21	TCP	NAS542	Toutes
x	FTP_20Data	20	20	TCP	NAS542	Toutes
	Telnet	5001	5001	TCP	0.0.0.0	Toutes
	Secure_20Shell_20Server_20_28SSH_29	443	443	TCP	0.0.0.0	Toutes
	Secure_20Web_20Server_20_28HTTPS_29		5000	5000	TCP	0.0.0.0 Toutes
	ssh	22	22	TCP	0.0.0.0	Toutes
	x-HTTP	8080	8080	TCP	0.0.0.0	Toutes
	x-139	139	139	TCP	0.0.0.0	Toutes
	x-514	514	514	TCP	0.0.0.0	Toutes
	x-548	548	548	TCP	0.0.0.0	Toutes
	x-445	445	445	TCP	0.0.0.0	Toutes
	x-601	601	601	TCP	0.0.0.0	Toutes
	x-873	873	873	TCP	0.0.0.0	Toutes

	x-5002	5002	5002	TCP	0.0.0.0	Toutes
x	rsync	873	873	TCP	NAS542	Toutes
x	HTTP-1	8008	8008	TCP	NAS542	Toutes
	UPnP	5000	5000	TCP	0.0.0.0	Toutes
	y-HTTP	8082	8082	TCP	NAS542	Toutes
	http-y	80	8000	TCP	0.0.0.0	Toutes
	23	23	23	TCP	0.0.0.0	Toutes
	https	443	443	TCP	0.0.0.0	Toutes
x	up-HTTP	8000	8000	TCP	NAS542	Toutes
x	up-HTTPS	8001	8001	TCP	NAS542	Toutes
	appl-HTTP	5000	5000	TCP	NAS542	Toutes
	appl-HTTPS	5001	5001	TCP	0.0.0.0	Toutes
x	appl-TRANS	9091	9091	TCP	NAS542	Toutes
x	appli-5002	5002	5002	TCP	NAS542	Toutes
	http	80	80	TCP	0.0.0.0	Toutes

 Vos règles personnalisées - redirection de protocoles

Choisissez des protocoles qui ne sont pas bloqués par le pare-feu.

Les équipements doivent être configurés avec une adresse IP statique pour être disponibles.

___ aucune règle n'est affichée

Activer	Nom	Protocole	Équipement	IP externe
	Aucune règle à afficher.			

 décochés

entre 2023 et 20240616 avaient été décochés : y-HTTP (8082) et appl-HTTP (5000), on conserve décochés

entre 2023 et 2024 est apparu Secure%20Web%20Server_20 (pas coché)

Suite au ransomware du 11/6/2024 il faudrait tout décocher (tout ne concerne que NAS542) donc : FTP_20Server, FTP_20Data, rsync, HTTP-1, y-HTTP up-HTTP

upHTTPS, appl-TRANS, appli-5002 : FAIT/VERIFIE

NAS542 n'est plus dans la DMZ

Le service DNS permet d'attribuer un nom à chacun de vos équipements pour les retrouver plus facilement en cas de besoin.

Équipements sur votre réseau local

Nom	Nom DNS	Adresse IP
devolo dLAN 200 AVeasy [MT2110]	CPL	10.0.1.100
devolo dLAN 200 AVeasy [MT2110]-1	CPL	10.0.1.101
hp402	IMP-hp402	10.0.1.49
canalplus-g7	TVIP	10.0.1.17
devolo dLAN 200 AVeasy [MT2110]-2	CPL	10.0.1.102
LAW10	PC-yves	10.0.1.47
NAS542	nas542	10.0.1.99
E5480	PC-portable-yves	10.0.1.50
Device-17	inconnu	10.0.1.26
Miele-001D63FFFE757A6E	MàL-Miele	10.0.1.18
HP-ENVY	IMP-Monique	10.0.1.41
smartphone Monica	smartphone Monique	10.0.1.20
Air-de-Monique	AIR-Monique	10.0.1.54
Galaxy-A5-2017	smartphone Yves	10.0.1.19

DNS supprimer	UDP/TCP		53	accepter
IRC supprimer	TCP		6666-6667	refuser
IMAP supprimer	TCP		143	accepter
IMAPS supprimer	TCP		993	accepter
ISAKMP supprimer	UDP		500	accepter
STUN supprimer	UDP		3478	accepter
IPSEC-NAT-T supprimer	UDP		4500	accepter
ESP-ALARM-TOOL supprimer	TCP		30000	accepter
ESP-ALARM supprimer	TCP		30100	accepter
ePower supprimer	TCP	1	8181	accepter
x-HTTP supprimer	TCP		8080	accepter
rsync supprimer	TCP		873	accepter
HTTP-1 supprimer	TCP		8008	accepter
up-HTTP supprimer	TCP		8000	accepter
up-HTTPS supprimer	TCP		8001	accepter
appl-HTTP supprimer	TCP		5000	accepter

appl-HTTPS
supprimer

TCP

5001 accepter

tous

décochés ?

Le réseau local n'habitant pas de serveurs on devrait pouvoir tout décocher, ou plus simplement passer le pare-feu à "Elevé" ou "Moyen" (est-ce que ça supprimé la réponse au ping ?)

on passe à MOYEN (les règles ipV4 sont re-accessibles si "poersonnalisé"

Toutes connexios entrantes bloquées (sauf si NAT ?)

Attention à IPv6

6.1	État DHCPv4	Actif
6.2	Adresse IPv4 de début	10.0.1.17
6.3	Adresse IPv4 de fin	10.0.1.128
6.4	Masque de sous réseau IPv4	255.255.252.0
6.5	Bail DHCPv4	86400
6.6	Passerelle DHCPv4	10.0.1.2
6.7	Adresse MAC	38:B5:C9:D3:57:30
6.8	État DHCPv6	Actif
6.9	Adresse IPv6 GUA	
6.10	Préfixe IPv6	

Port ethernet 1

6.8	État	Actif
6.9	Adresse MAC	38:B5:C9:D3:57:30
6.10	Vitesse maximum	1000
6.11	Vitesse négociée	1000
6.12	Duplex négocié	FULL

Port ethernet 2

6.13	État	Inactif
6.14	Adresse MAC	38:B5:C9:D3:57:30
6.15	Vitesse maximum	1000
6.16	Vitesse négociée	1000
6.17	Duplex négocié	HALF

Port ethernet 3

6.18	État	Inactif
6.19	Adresse MAC	38:B5:C9:D3:57:30
6.20	Vitesse maximum	1000
6.21	Vitesse négociée	1000
6.22	Duplex négocié	HALF

Port ethernet 4

6.23	État	Inactif
6.24	Adresse MAC	38:B5:C9:D3:57:30
6.25	Vitesse maximum	1000
6.26	Vitesse négociée	1000
6.27	Duplex négocié	HALF

- 7.1 État
- 7.2 Numéro téléphonique VoIP
- 7.3 ATM VP/VC ou VLAN
- 7.4 Protocole

disponible
+33146681824
VLAN : 832
sip

Les règles NAT/PAT sont nécessaires pour autoriser une communication initiée depuis Internet avec un équipement particulier de votre réseau. Utiles pour certaines applications comme des jeux en lignes ou des serveurs de type FTP ... Assurez-vous que cet équipement a une adresse IP statique (paramétrable dans l'onglet DHCP).

Uniquement pour des équipements IPv4.

Vos règles personnalisées

Choisissez des ports qui ne sont pas bloqués par le pare-feu.

Nous vous déconseillons la création d'une règle sur le port 53 (service DNS).

Les équipements doivent être configurés avec une adresse IP statique pour être disponibles.

ex. : 1000

ex. : 1000-2000

IP externes autorisées

CréerUne règle NAT/PAT

Activer	Application/Service	P int	P ext	Proto	Équip	IP externe
	Web_20Server_20_28HTTP_29	80	80	TCP	0.0.0.0	Toutes
x	FTP_20Server	21	21	TCP	NAS542	Toutes
x	FTP_20Data	20	20	TCP	NAS542	Toutes
	Telnet	5001	5001	TCP	0.0.0.0	Toutes
	Secure_20Shell_20Server_20_28SSH_29	443	443	TCP	0.0.0.0	Toutes
	Secure_20Web_20Server_20_28HTTPS_29		5000	5000	TCP	0.0.0.0 Toutes
	ssh	22	22	TCP	0.0.0.0	Toutes
	x-HTTP	8080	8080	TCP	0.0.0.0	Toutes
	x-139	139	139	TCP	0.0.0.0	Toutes
	x-514	514	514	TCP	0.0.0.0	Toutes
	x-548	548	548	TCP	0.0.0.0	Toutes
	x-445	445	445	TCP	0.0.0.0	Toutes
	x-601	601	601	TCP	0.0.0.0	Toutes
	x-873	873	873	TCP	0.0.0.0	Toutes

	x-5002	5002	5002	TCP	0.0.0.0	Toutes
x	rsync	873	873	TCP	NAS542	Toutes
x	HTTP-1	8008	8008	TCP	NAS542	Toutes
	UPnP	5000	5000	TCP	0.0.0.0	Toutes
	y-HTTP	8082	8082	TCP	NAS542	Toutes
	http-y	80	8000	TCP	0.0.0.0	Toutes
	23	23	23	TCP	0.0.0.0	Toutes
	https	443	443	TCP	0.0.0.0	Toutes
x	up-HTTP	8000	8000	TCP	NAS542	Toutes
x	up-HTTPS	8001	8001	TCP	NAS542	Toutes
	appl-HTTP	5000	5000	TCP	NAS542	Toutes
	appl-HTTPS	5001	5001	TCP	0.0.0.0	Toutes
x	appl-TRANS	9091	9091	TCP	NAS542	Toutes
x	appli-5002	5002	5002	TCP	NAS542	Toutes
	http	80	80	TCP	0.0.0.0	Toutes

 Vos règles personnalisées - redirection de protocoles

Choisissez des protocoles qui ne sont pas bloqués par le pare-feu.

Les équipements doivent être configurés avec une adresse IP statique pour être disponibles.

___ aucune règle n'est affichée

Activer	Nom	Protocole	Équipement	IP externe
	Aucune règle à afficher.			

 décochés

entre 2023 et 20240616 avaient été décochés : y-HTTP (8082) et appl-HTTP (5000), on conserve décochés

entre 2023 et 2024 est apparu Secure%20Web%20Server_20 (pas coché)

Suite au ransomware du 11/6/2024 il faudrait tout décocher (tout ne concerne que NAS542) donc : FTP_20Server, FTP_20Data, rsync, HTTP-1, y-HTTP up-HTTP

upHTTPS, appl-TRANS, appli-5002 : FAIT/VERIFIE

NAS542 n'est plus dans la DMZ

Le service UPnP IGD permet aux applications (messagerie instantanée, jeux en ligne, etc.) de créer automatiquement des redirections de ports, via des règles NAT/PAT.

Activer le service UPnP IGD (c'est coché)

Application/Service	Adresse IP hôte	Port externe	Port interne	Protocole	Nom/Adresse IP
NAS542-D8_EC_E5_44_6F_F6-WEBDAV_HTTPS	10.0.1.99	5003	5003	tcp	
NAS542-D8_EC_E5_44_6F_F6-WEBPUBLISHING_HTTPS	10.0.1.99	5001	5001	tcp	

ActualiserLa liste

En intégrant un équipement à la DMZ vous rendez cet équipement accessible depuis Internet. Vous devez préalablement associer une adresse IP statique à cet équipement dans l'onglet DHCP.

Vous devez préalablement associer à cet équipement une adresse IP statique dans l'onglet DHCP.

Réservée aux utilisateurs avancés car susceptible de modifier la sécurité de votre réseau.

Intégrer un autre équipement

Équipement

Adresse IP statique

Adresse MAC

la DMZ

a été vidée