

2024-
2025



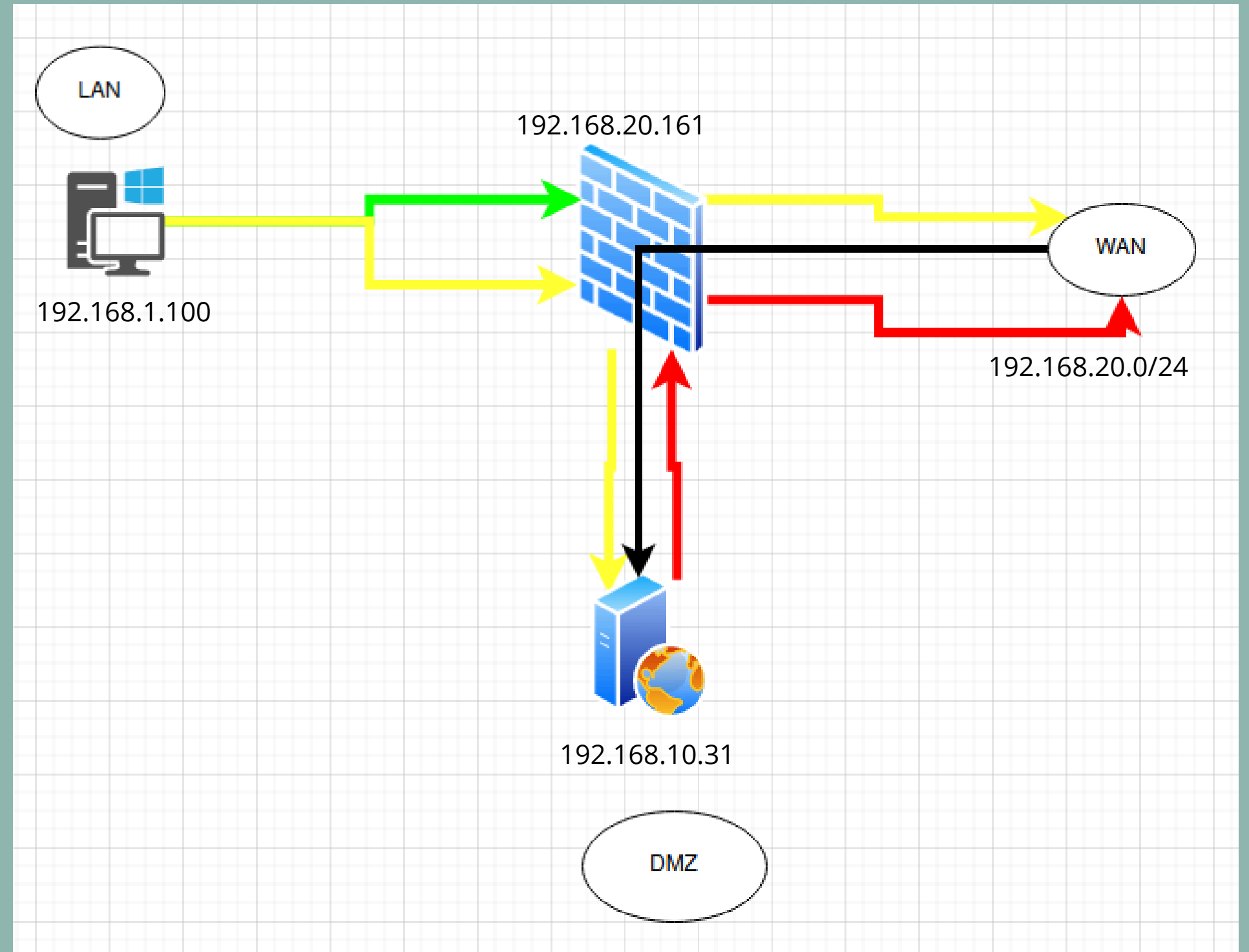
B T S S I O 2

TP-PFSENSE /NTOP/RDP

Nicolas Debut

SHÉMA RÉSEAU

- Redirection WAN vers le site Web
- Accès du LAN vers WAN et DMZ
- Accès à la configuration du pfsense
- Accès de la DMZ vers Internet



Avant de démarrer votre pfSense pour la première fois, veuillez à attribuer 3 interfaces réseau à votre machine.

Pour une VM située sur Proxmox, voici comment procéder :

- **Allez sur Proxmox, puis dans l'onglet Network.**
- **Cliquez ensuite sur Create puis sélectionnez Linux Bridge.**

The screenshot shows the Proxmox VE web interface. On the left, a sidebar lists VMs under 'Datacenter' and 'proxmox3'. The main panel displays the 'Network' configuration page. At the top, there are buttons for 'Create', 'Revert', 'Edit', 'Remove', and 'Apply Configuration'. Below these is a table of network devices.

Name ↑	Type	Active	Autostart	VLAN a...	Ports/Slaves	Bond Mode	CIDR	Gateway	Comment
eno1	Network Device	Yes	No	No					
eno2	Network Device	No	No	No					
eno3	Network Device	No	No	No					
eno4	Network Device	No	No	No					
ens1f0	Network Device	No	No	No					
ens1f1	Network Device	No	No	No					
vmbr0	Linux Bridge	Yes	Yes	No	eno1		192.168.20.203/24	192.168.20.254	
vmbr1	Linux Bridge	Yes	Yes	No					
vmbr2	Linux Bridge	Yes	Yes	No					

Virtual Machine 202 (Pfsense) on node 'proxmox3'

nicolas

Summary

Console

Hardware

Cloud-Init

Options

Task History

Monitor

Backup

Replication

Snapshots

Firewall

Add

Remove

Edit

Disk Action

Revert

Memory	1.00 GiB
Processors	1 (1 sockets, 1 cores) [x86-64-v2-AES]
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI single
CD/DVD Drive (ide2)	local:iso/pfSense-CE-2.7.2-RELEASE-amd64.iso,media=cdrom,size=854172K
Hard Disk (scsi0)	VM:vm-202-disk-0,iouthread=1,size=20G
Network Device (net0)	virtio=BC:24:11:91:9C:E9,bridge=vmbr0,firewall=1
Network Device (net1)	virtio=BC:24:11:50:CF:E4,bridge=vmbr1,firewall=1
Network Device (net2)	virtio=BC:24:11:36:35:46,bridge=vmbr2,firewall=1

Add: Network Device

Bridge:vmbr0

Model:VirtIO (paravirtualized)

VLAN Tag:no VLAN

MAC address:auto

Firewall:☒

Disconnect:☐

Rate limit (MB/s):unlimited

MTU:1500 (1 = bridge MTU)

Multiqueue:

Help

Advanced☒

Add

- **Rendez-vous dans l'onglet de votre pfSense, puis dans la catégorie Hardware.**
- **Cliquez sur Add, puis sur Network Device.**
- **Sélectionnez l'interface réseau que vous souhaitez, puis cliquez sur Add.**
- **Vous devriez ensuite voir l'interface que vous avez ajoutée.**

⇕	Network Device (net0)	virtio=BC:24:11:91:9C:E9,bridge=vmbr0,firewall=1
⇕	Network Device (net1)	virtio=BC:24:11:50:CF:E4,bridge=vmbr1,firewall=1
⇕	Network Device (net2)	virtio=BC:24:11:36:35:46,bridge=vmbr2,firewall=1

```
Should VLANs be set up now [y|n]? n
```

```
If the names of the interfaces are not known, auto-detection can  
be used instead. To use auto-detection, please disconnect all  
interfaces before pressing 'a' to begin the process.
```

```
Enter the WAN interface name or 'a' for auto-detection  
(vtnet0 vtnet1 vtnet2 or a): vtnet0
```

```
Enter the LAN interface name or 'a' for auto-detection  
NOTE: this enables full Firewalling/NAT mode.  
(vtnet1 vtnet2 a or nothing if finished): vtnet1
```

```
Optional interface 1 description found: DMZ  
Enter the Optional 1 interface name or 'a' for auto-detection  
(vtnet2 a or nothing if finished): vtnet2
```

```
The interfaces will be assigned as follows:
```

```
WAN   -> vtnet0  
LAN   -> vtnet1  
OPT1  -> vtnet2
```

```
Do you want to proceed [y|n]? y
```

Démarrez ensuite votre VM afin de procéder à l'installation.
Une fois celle-ci terminée, associez la bonne interface
réseau au bon réseau.

```
(Local Database)
```

```
FreeBSD/amd64 (pfSense.nicolasdebut.com) (ttyv0)
```

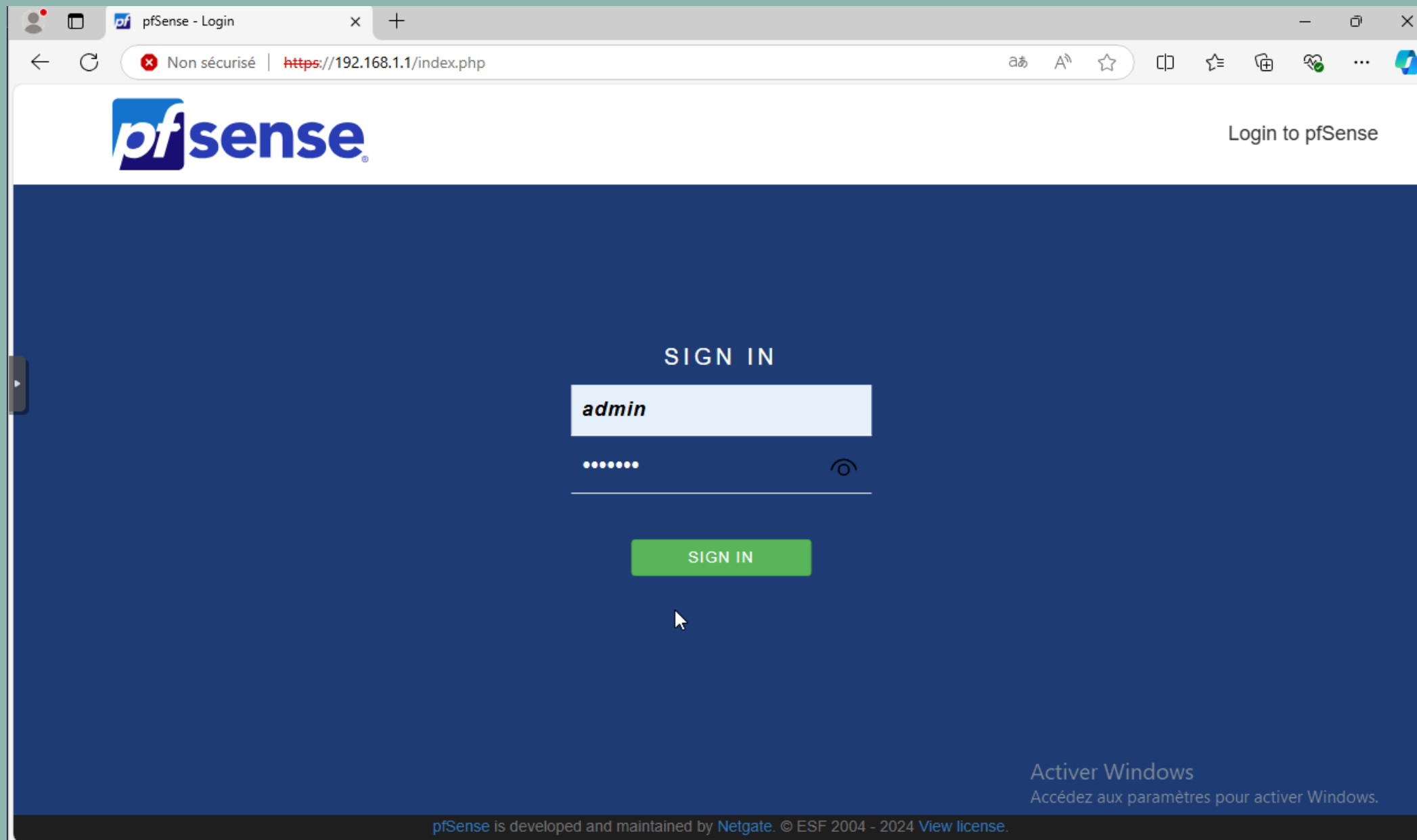
```
KVM Guest - Netgate Device ID: 5f117e33bf87bcfffc63e
```

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
```

```
WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.20.161/24  
LAN (lan)      -> vtnet1      -> v4: 192.168.1.1/24  
DMZ (opt1)     -> vtnet2      -> v4: 192.168.10.1/24
```

```
0) Logout (SSH only)          9) pfTop  
1) Assign Interfaces          10) Filter Logs  
2) Set interface(s) IP address 11) Restart webConfigurator  
3) Reset webConfigurator password 12) PHP shell + pfSense to  
4) Reset to factory defaults    13) Update from console  
5) Reboot system              14) Enable Secure Shell (s  
6) Halt system                15) Restore recent configu  
7) Ping host                  16) Restart PHP-FPM  
8) Shell
```

```
Enter an option: 
```

Une fois cela fait, créez une VM en veillant à la connecter à l'interface réseau de votre LAN.

Accédez ensuite à votre pfSense en entrant l'IP de votre LAN dans votre navigateur.

Identifiant par défaut : admin

Mot de passe par défaut : pfsense

N'oubliez pas de vérifier votre configuration.

!!! Ne pas oublier de désactiver l'option en bas de la page 4/9 pour permettre d'utiliser un réseau privé comme WAN si nécessaire.

RFC1918 Networks

Block RFC1918 Private Networks

☒ Block private networks from entering via WAN

When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

Vous arriverez ensuite sur la page d'accueil de votre pfSense.

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Status / Dashboard

System Information

Name	pfSense.nicolasdebut.com
User	admin@192.168.1.100 (Local Database)
System	KVM Guest Netgate Device ID: 5f117e33bf87bcffc63e
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 21:10:00 CET 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Wed Sep 25 8:12:36 CEST 2024
CPU Type	QEMU Virtual CPU version 2.5+ AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	00 Hour 47 Minutes 47 Seconds
Current date/time	Wed Sep 25 8:59:01 CEST 2024

Netgate Services And Support

Contract type

Community Support
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the **NETGATE RESOURCE LIBRARY**.

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Netgate Global Support FAQ
- Netgate Professional Services

- Community Support Resources
- Official pfSense Training by Netgate
- Visit Netgate.com

Activer Windows
Accédez aux paramètres pour activer Windows

If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to

**Un message s'affichera pour vous proposer de changer l'option DHCP.
Il est conseillé de passer à la version Kea DHCP, car ISC DHCP n'est plus
d'actualité.**

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit [System > Advanced > Networking](#) to switch DHCP backend.

System / [Advanced](#) / [Networking](#)

[Admin Access](#)

[Firewall & NAT](#)

[Networking](#)

[Miscellaneous](#)

[System Tunables](#)

[Notifications](#)

DHCP Options

Server Backend

☒ Kea DHCP

☐ ISC DHCP (Deprecated)

☐ Ignore Deprecation Warning

ISC DHCP has reached end-of-life and will be removed from a future version of pfSense. Kea DHCP is the newer, modern DHCP distribution that includes the most-requested features.

Il est maintenant temps de configurer les règles dans pfSense.
Pour les créer, allez dans Firewall, puis Rules, et cliquez sur Add.
La première règle permettra au LAN d'accéder au web via le WAN (ici, notre réseau de la salle).

Firewall / Rules / Edit

Edit Firewall Rule

Action Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface LAN
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol Any
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match LAN subnets Source Address: /

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

✓ Apply Changes

!!! Après chaque règle sauvegardée, cliquez sur Apply Changes, sinon les règles que vous avez mises en place ne fonctionneront pas.

Destination

Destination ☐ Invert match Any Destination Address: /

Extra Options

Log ☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

Rule Information

Tracking ID	1726648791
Created	9/18/24 10:39:51 by admin@192.168.1.100 (Local Database)
Updated	9/18/24 10:39:51 by admin@192.168.1.100 (Local Database)

[Save](#)

Activer Windows

Firewall / Rules / Edit

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

DMZ

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

DMZ subnets

Source Address: /

Cette règle autorise les flux sortants de la DMZ.

Destination

Destination

☐ Invert match

Any

Destination Address: /

Extra Options

Log

☐ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

Display Advanced

Rule Information

Tracking ID	1726650335
Created	9/18/24 11:05:35 by admin@192.168.1.100 (Local Database)
Updated	9/18/24 11:05:35 by admin@192.168.1.100 (Local Database)

Save

Pour les redirections de port, rendez-vous dans Firewall, puis NAT, et sélectionnez Port Forward. Cliquez ensuite sur Add. Cette redirection fera en sorte que, si le WAN tente de se connecter à votre pfSense, il sera immédiatement redirigé vers votre serveur web.

Disabled

☐ Disable this rule

No RDR (NOT)

☐ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface

WAN

Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

Display Advanced

Destination

☐ Invert match.

WAN address

Type

Address/mask

Destination port range

HTTP

From port

Custom

HTTP

To port

Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Destination port range

HTTP

From port

Custom

HTTP

To port

Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP

Address or Alias

192.168.10.31

Type

Address

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Redirect target port

HTTP

Port

Custom

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

Description

A description may be entered here for administrative reference (not parsed).

No XMLRPC Sync

☐ Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection

Use system default

Filter rule association

Rule NAT

[View the filter rule](#)

Firewall / NAT / Outbound / Edit

Edit Advanced Outbound NAT Entry

Disabled

☐ Disable this rule

Do not NAT

☐ Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules
In most cases this option is not required.

Interface

DMZ

The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which protocol this rule should match. In most cases "any" is specified.

Source

DMZ subnets

Type

Source network for the outbound NAT mapping.

/ 24

Port or Range

Destination

WAN subnets

Type

Destination network for the outbound NAT mapping.

/ 24

Port or Range

☐ Not

Invert the sense of the destination match.

Ici, vous trouvez la règle permettant à la DMZ d'accéder à Internet via le WAN.

Translation

Address

WAN address

Type

Connections matching this rule will be mapped to the specified address. If specifying a custom network or alias, it must be routed to the firewall.

Port or Range

☐ Static Port

Enter the external source **Port or Range** used for remapping the original source port on connections matching the rule.

Port ranges are a low port and high port number separated by ":".
Leave blank when **Static Port** is checked.

Misc

No XMLRPC Sync

☐

Prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

Description

A description may be entered here for administrative reference (not parsed).

Rule Information

Created

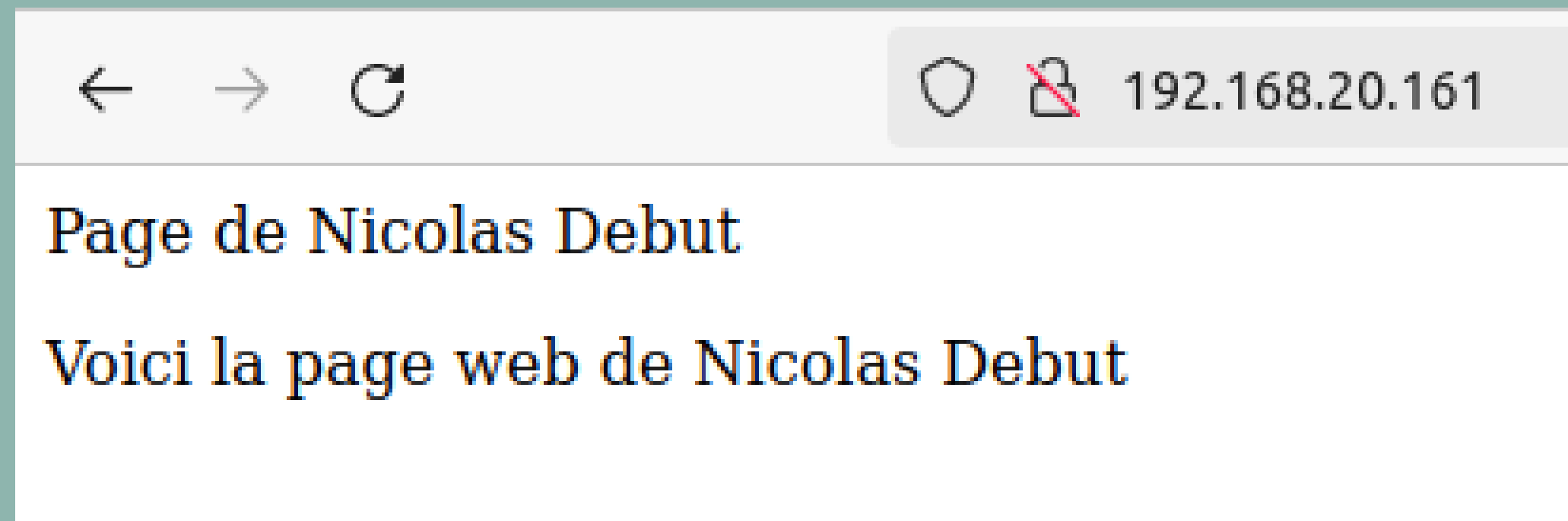
9/18/24 10:57:55 by admin@192.168.1.100 (Local Database)

Updated

9/18/24 10:57:55 by admin@192.168.1.100 (Local Database)

Save

Si, depuis votre WAN, vous entrez l'IP de votre pfSense dans votre navigateur, vous serez redirigé vers votre serveur web situé dans votre DMZ.



NTOP

NTOP est un outil très utile si vous souhaitez superviser l'activité qui se déroule sur votre pfSense, il est inclus dans celui-ci il vous suffit juste de mettre un plugin.

Pour l'installer, vous devrez vous rendre dans l'onglet System, puis Package Manager. Cliquez sur Available Packages, recherchez ntop et installez-le.

System / Package Manager / Available Packages

Installed Packages

Available Packages

Search

Search term

ntop

Both

Search

Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description	
ntopng	0.8.13_10	ntopng (replaces ntop) is a network probe that shows network usage in a way similar to what top does for processes. In interactive mode, it displays the network status on the user's terminal. In Web mode it acts as a Web server, creating an HTML dump of the network status. It sports a NetFlow/sFlow emitter/collector, an HTTP-based client interface for creating ntop-centric monitoring applications, and RRD for persistently storing traffic statistics.	+ Install
Package Dependencies:			
webfonts-0.30_14 ntopng-5.6.d20230920,1 libmaxminddb-1.7.1_1 graphviz-8.1.0_1 redis-7.2.1 gdbm-1.23			

Confirmez l'installation, puis patientez pendant que celle-ci s'effectue.

System / Package Manager / Package Installer

Installed Packages

Available Packages

Package Installer

Confirmation Required to install package pfSense-pkg-ntopng.

✓ Confirm

Please wait while the installation of pfSense-pkg-ntopng completes.
This may take several minutes. Do not leave or refresh the page!

Installed Packages

Available Packages

Package Installer

Package Installation

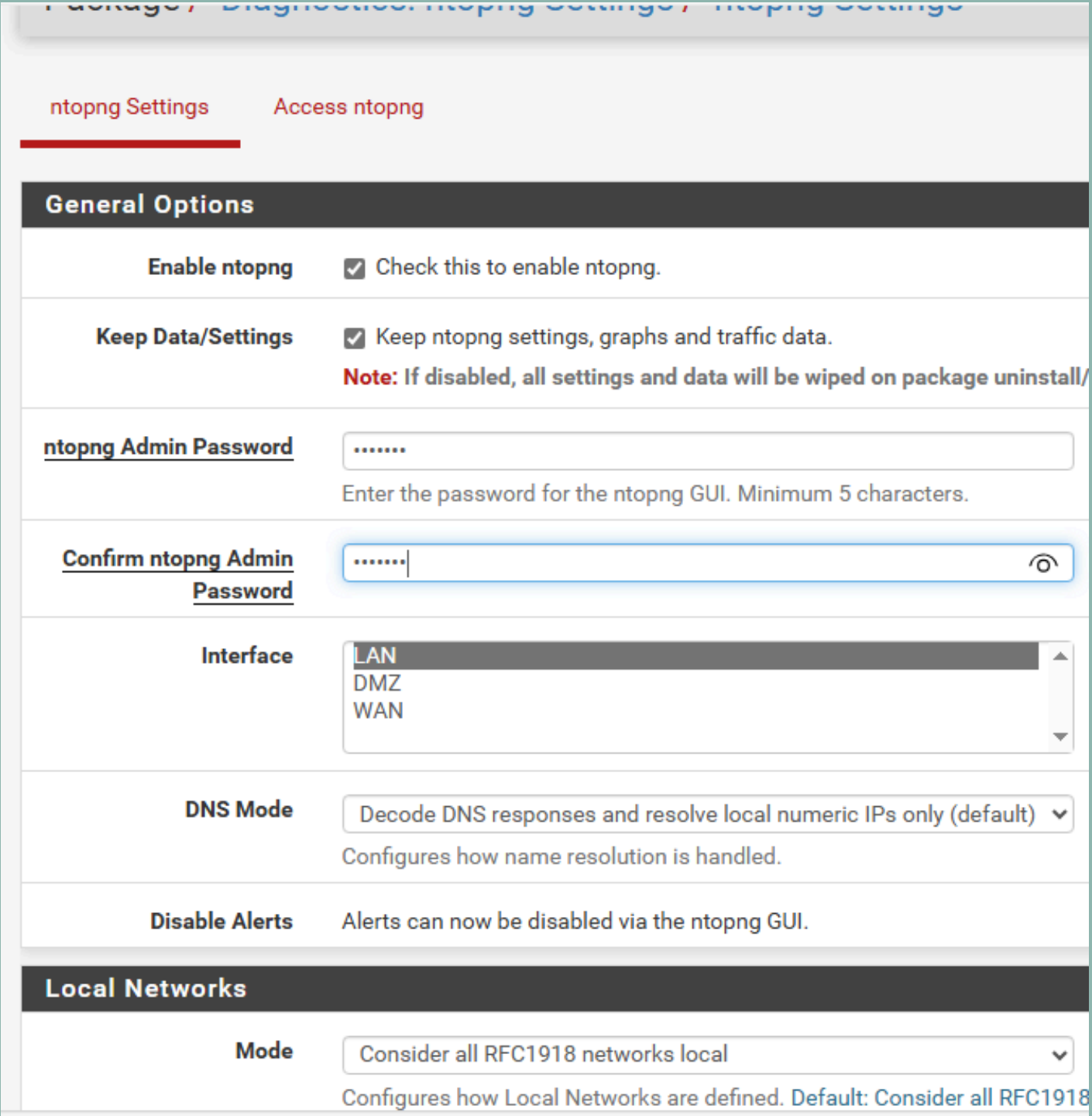
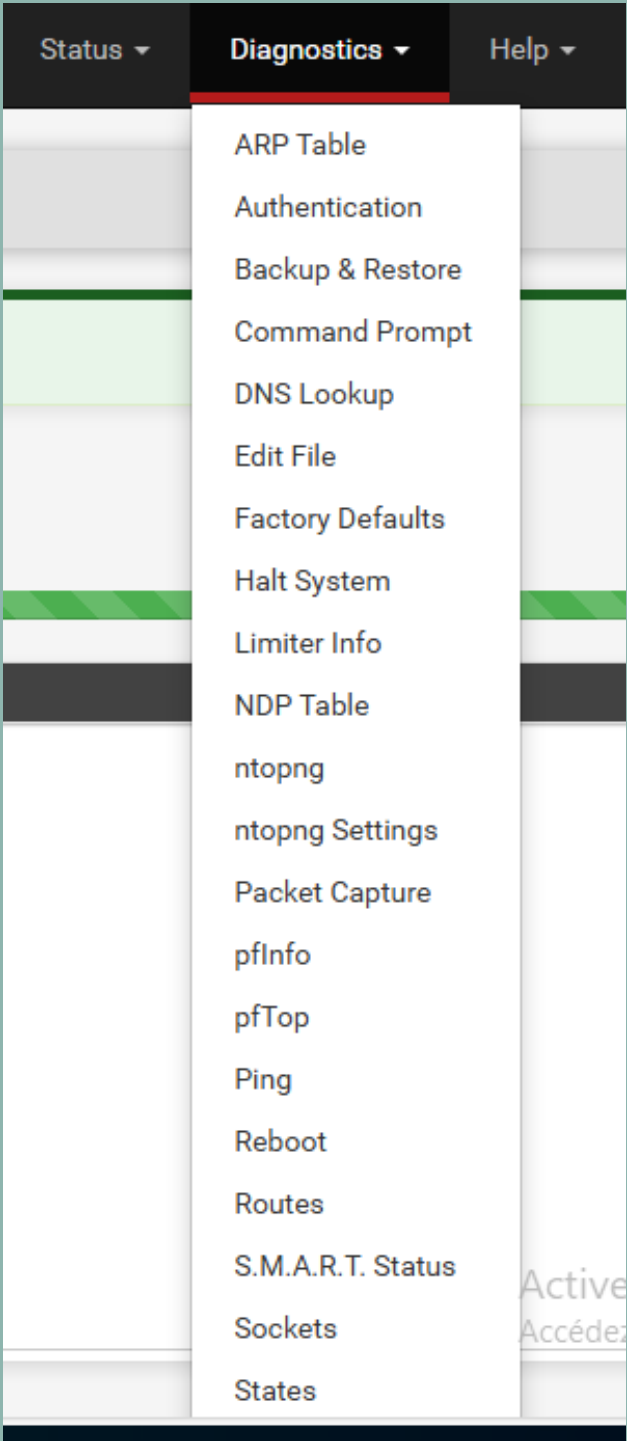
openpgm: 5.2.122_6 [pfSense]
pfSense-pkg-ntopng: 0.8.13_10 [pfSense]
png: 1.6.40 [pfSense]
psutils: 1.17_5 [pfSense]
redis: 7.2.1 [pfSense]
tiff: 4.4.0_2 [pfSense]
uchardet: 0.0.8 [pfSense]
webfonts: 0.30_14 [pfSense]
webp: 1.3.2 [pfSense]

Number of packages to be installed: 38

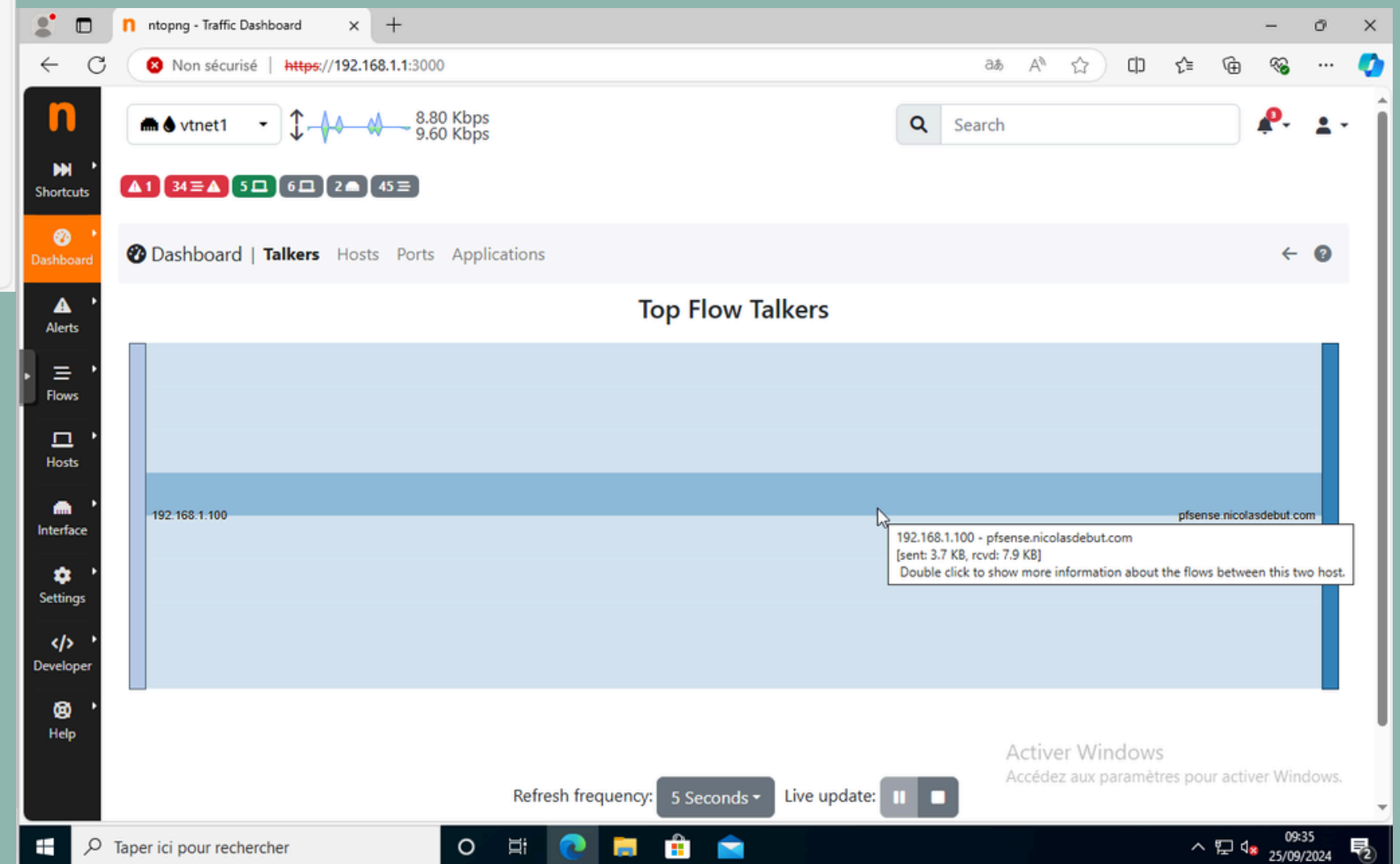
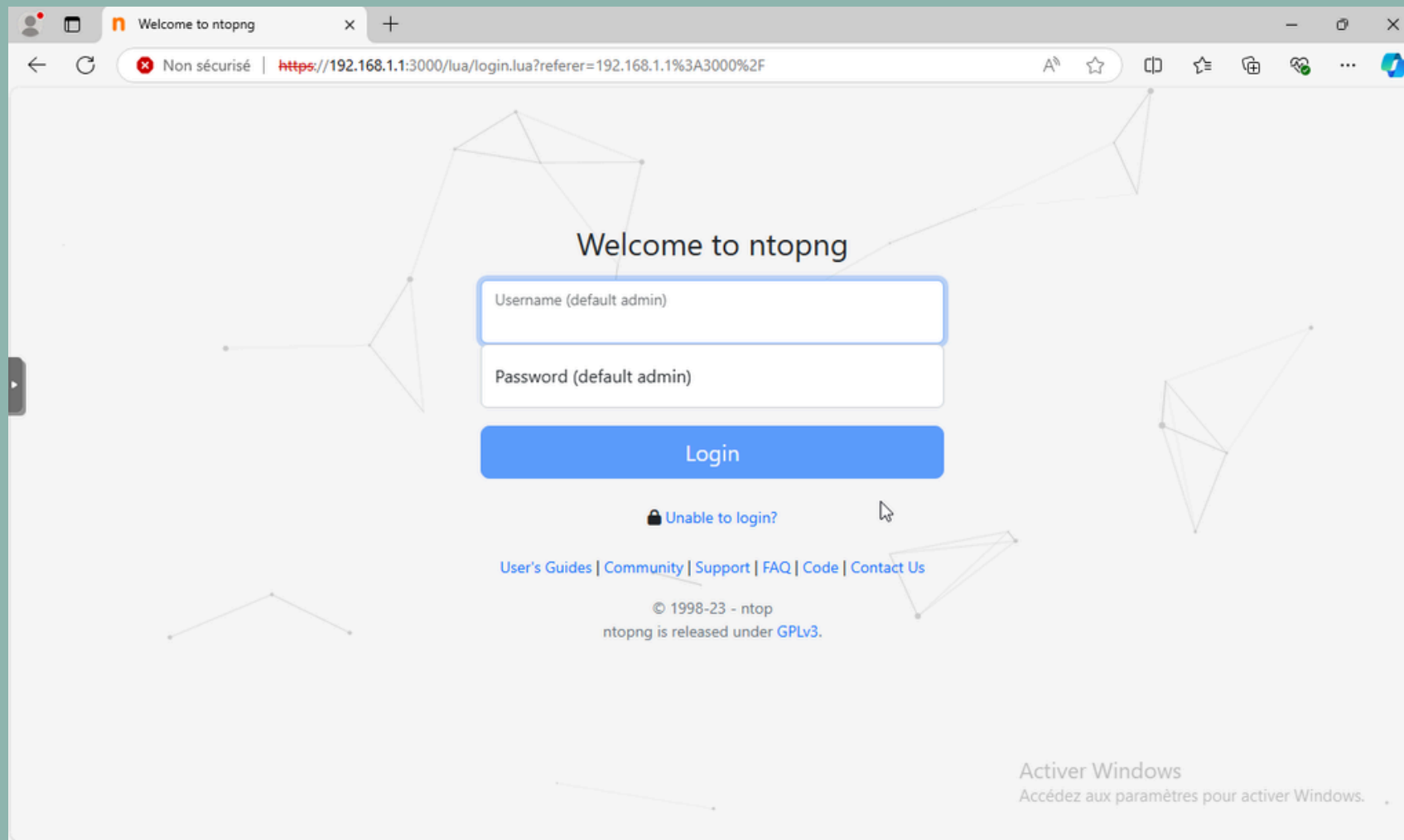
The process will require 212 MiB more space.
26 MiB to be downloaded.
[1/38] Fetching ntopng-5.6.d20230920,1.pkg:

Activer Windows
Accédez aux paramètres pour activer Windows.

Une fois installé, allez dans Diagnostics, puis dans ntopng Settings, activez le service et indiquez l'interface à surveiller.

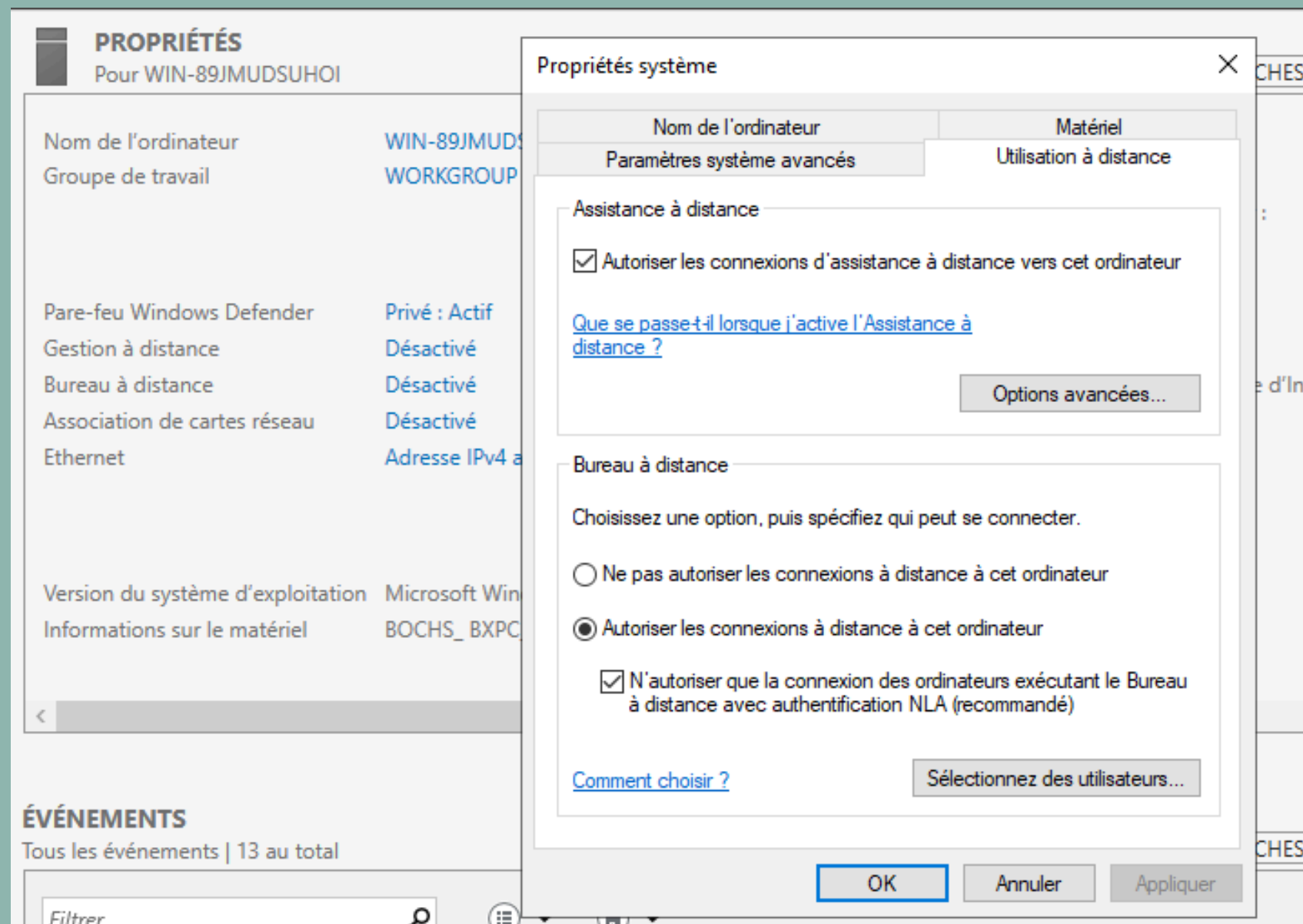


Cliquez ensuite sur Access ntopng pour accéder au service ; indiquez votre identifiant et votre mot de passe, et voilà, votre service est installé.

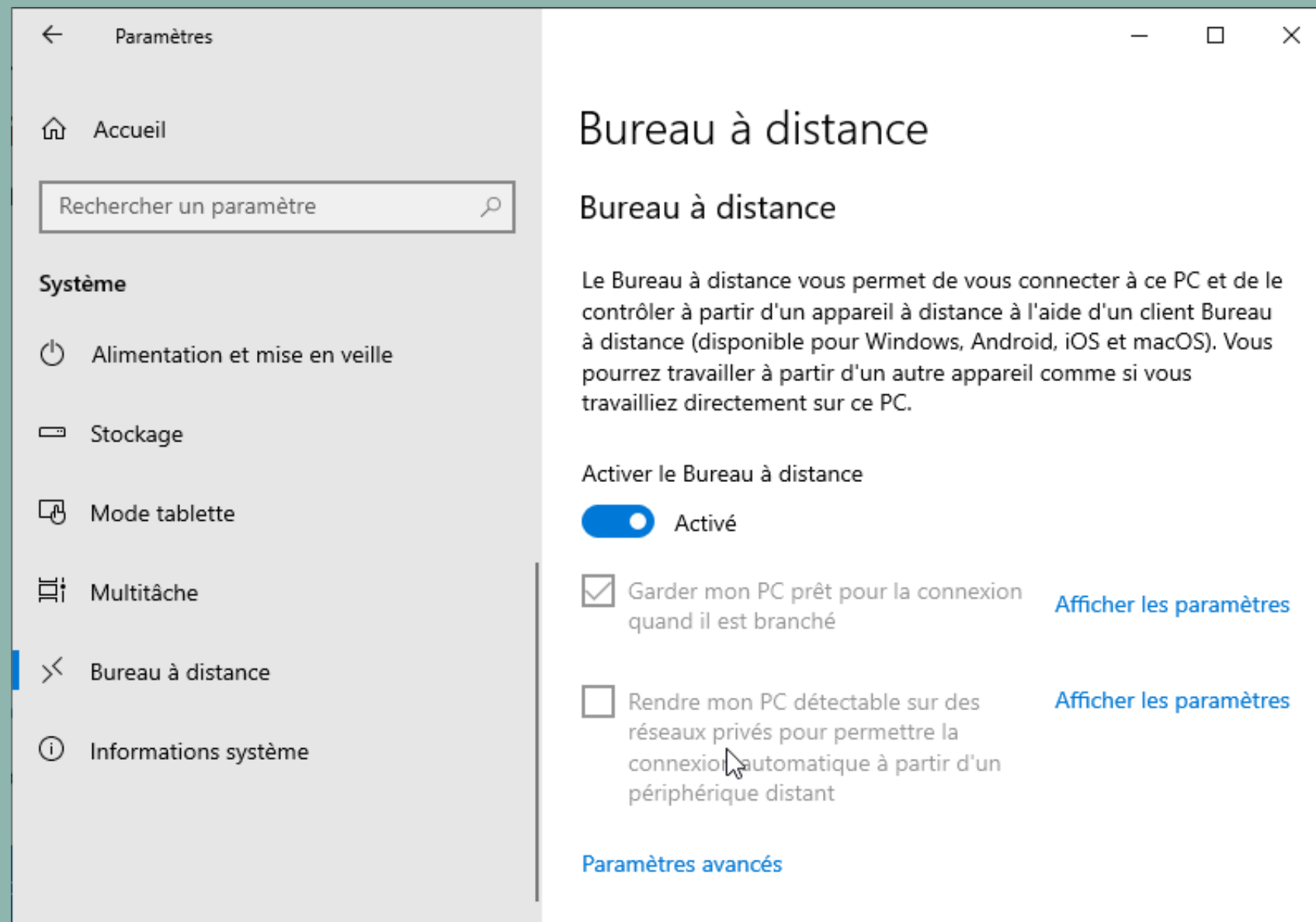


RDP

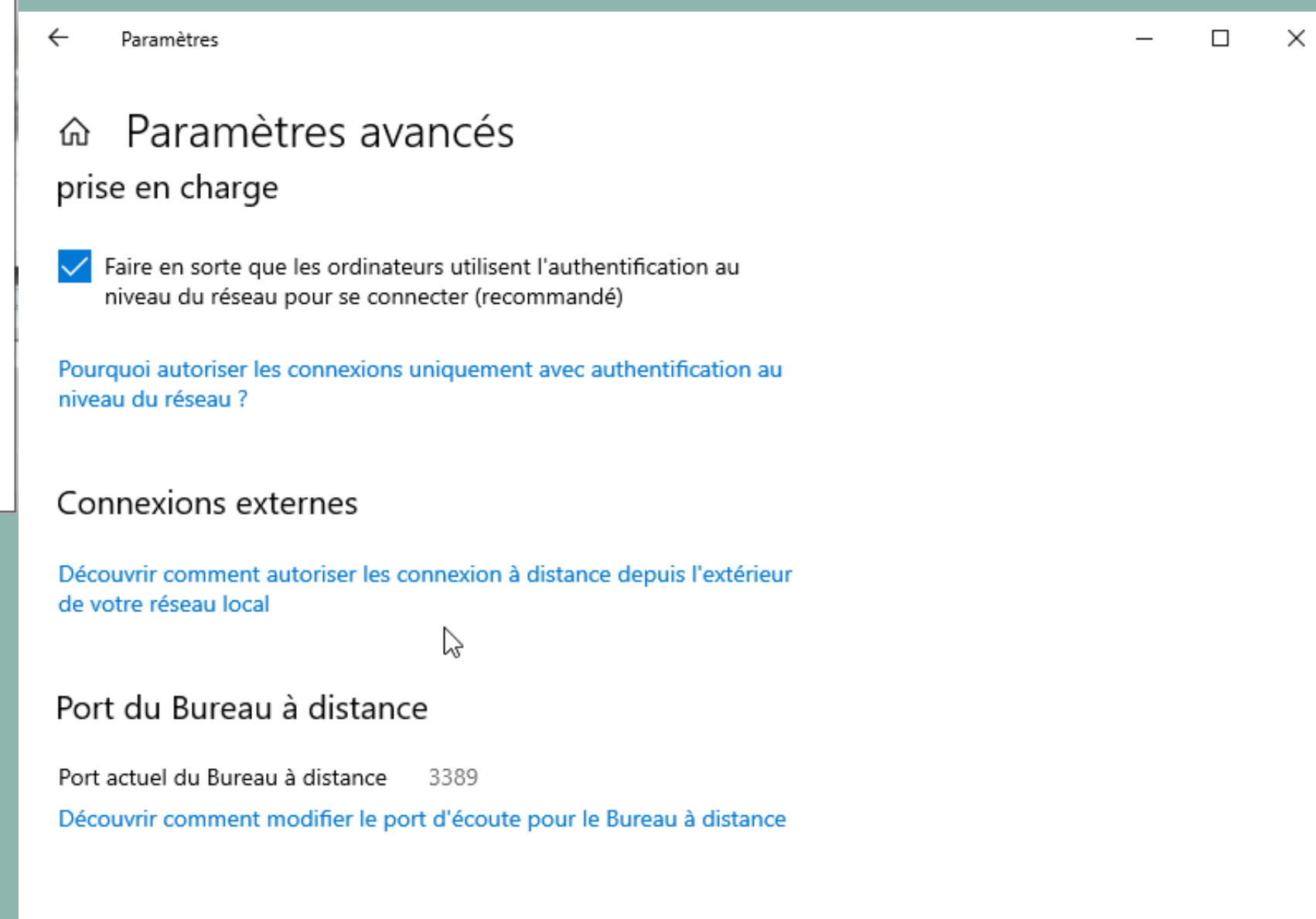
Nous allons maintenant voir comment activer le protocole RDP afin d'accéder à vos appareils à distance. Nous prendrons ici l'exemple d'un Windows Server 2019.



Commencez depuis votre gestionnaire de serveur en activant l'option Bureau à distance.



Allez ensuite dans vos paramètres avancés de Bureau à distance pour vérifier, dans un premier temps, s'il est actif, puis le port qui est utilisé (par défaut, le 3389).



Allez ensuite dans votre pfSense afin de configurer une nouvelle redirection de port pour permettre au WAN d'accéder à distance au Windows Server. Pour des raisons de sécurité, j'ai modifié le port de connexion à 500.

No RDR (NOT)

☐ Disable redirection for traffic matching this rule

This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface

WAN

Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which protocol this rule should match. In most cases "TCP" is specified.

Source

⚙️ Display Advanced

Destination

☐ Invert match.

WAN address

Type

Address/mask

Destination port range

Other

500

Other

500

From port

Custom

To port

Custom

Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP

Address or Alias

192.168.10.2

Type

Address

Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Redirect target port

MS RDP

Port

Custom

i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Redirect target port

MS RDP

Port

Custom

Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

Description

accès RDP serveur srv-nicolas

A description may be entered here for administrative reference (not parsed).

No XMLRPC Sync

☐ Do not automatically sync to other CARP members

This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection

Use system default

Filter rule association

Rule NAT accès RDP serveur srv-nicolas

[View the filter rule](#)

Rule Information

Created

9/25/24 10:51:13 by admin@192.168.1.100 (Local Database)

Updated

9/25/24 10:51:13 by admin@192.168.1.100 (Local Database)

Save

Voici ce qui devrait s'afficher ensuite.

Attention : n'oubliez pas d'appliquer vos changements.

Firewall / NAT / Port Forward

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor](#) the filter reload progress.

Port Forward

1:1

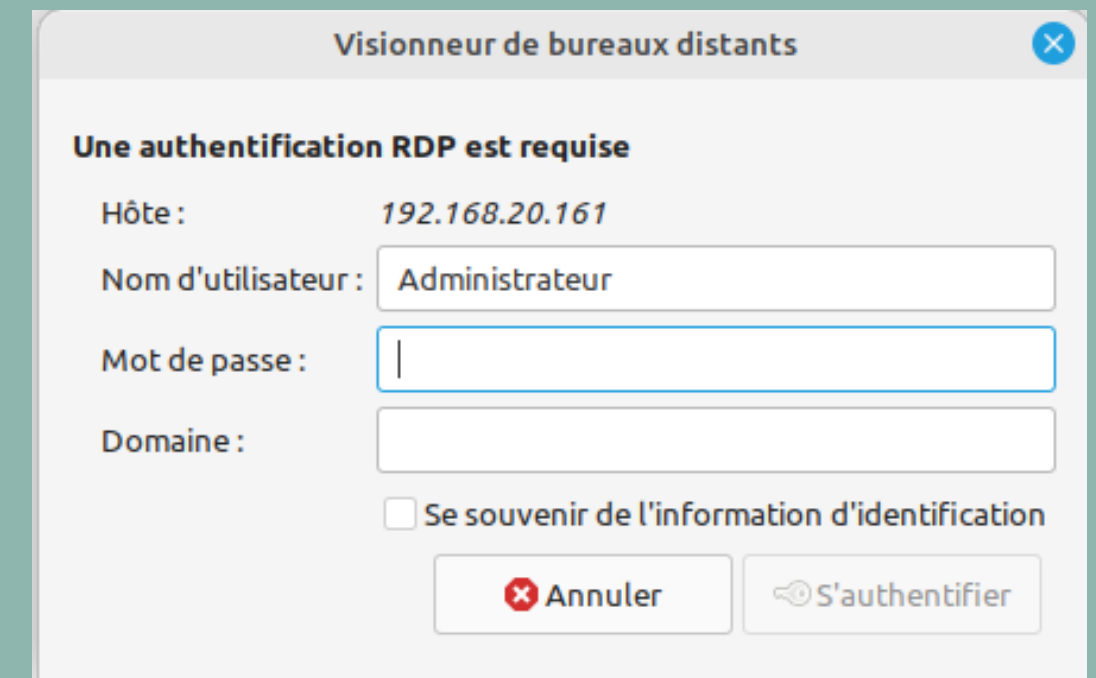
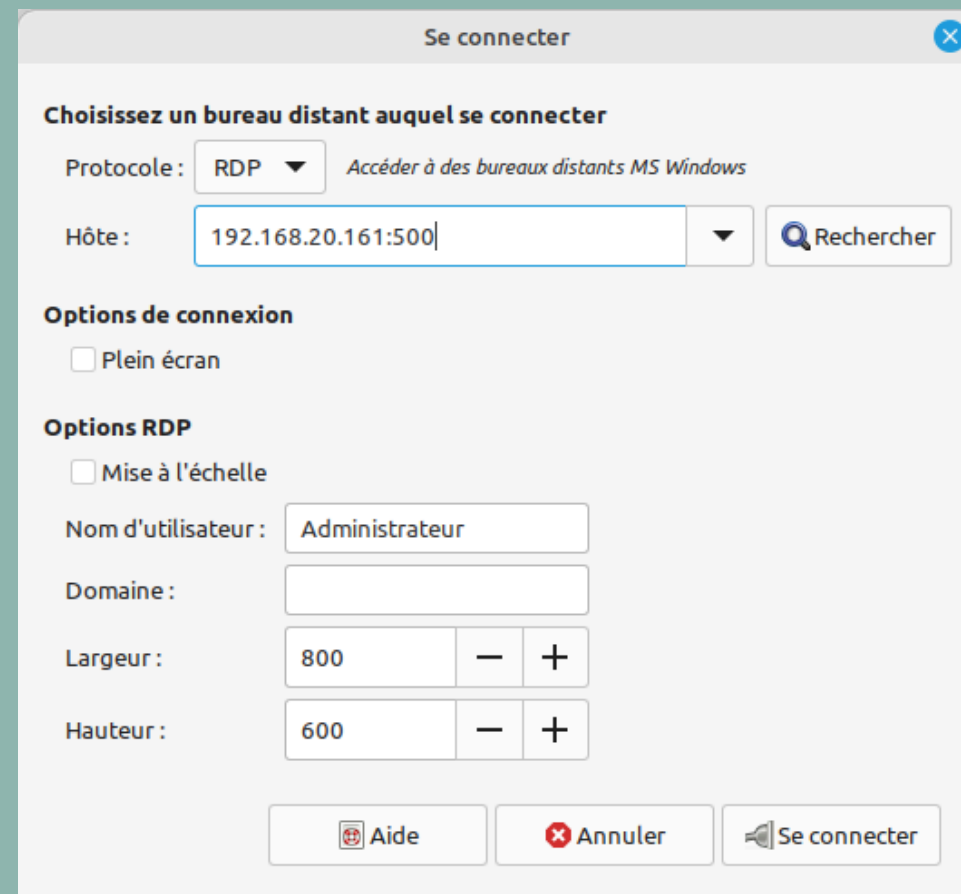
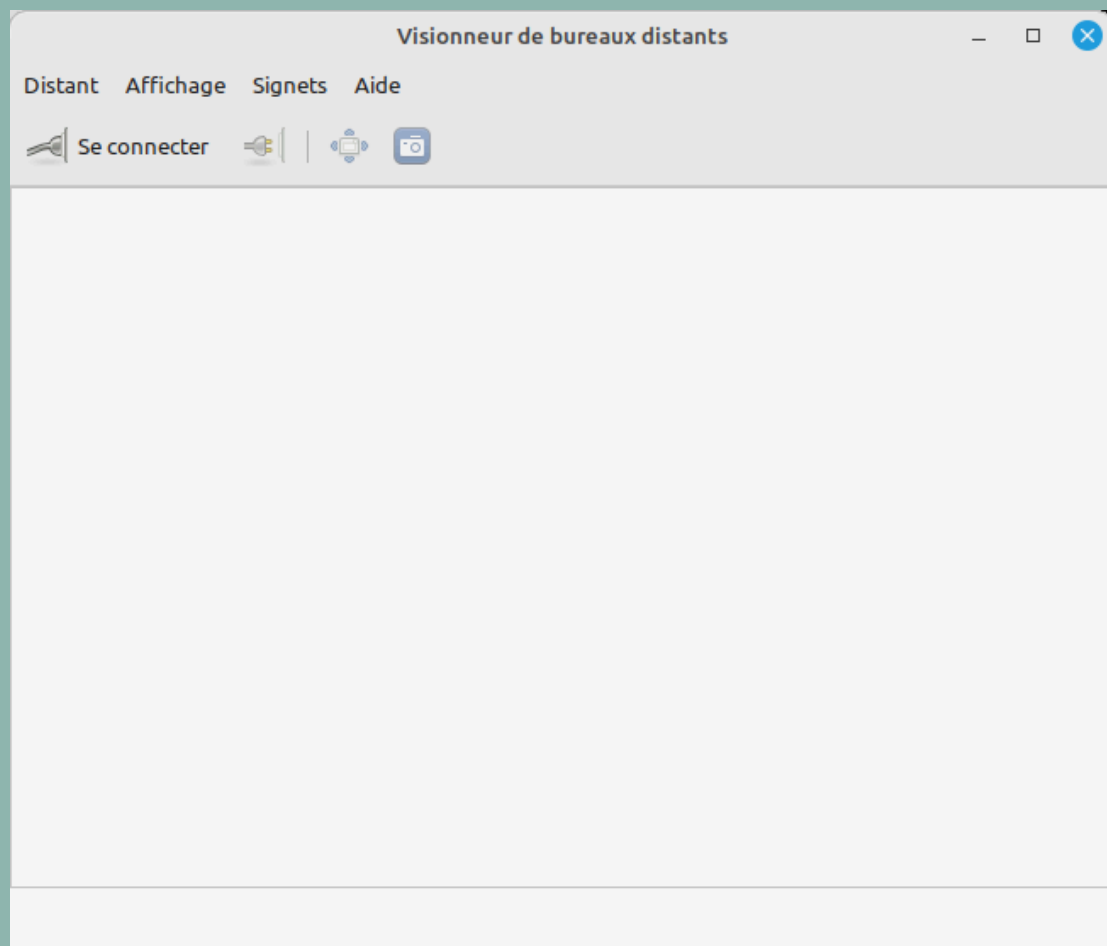
Outbound

NPt

Rules

		Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions	
☐	☒	☒	WAN	TCP	*	*	WAN address	3389 (MS RDP)	192.168.10.2	3389 (MS RDP)	accès RDP serveur srv-nicolas	
☐	☒	☒	WAN	TCP	*	*	WAN address	80 (HTTP)	192.168.10.31	80 (HTTP)		

Essayons maintenant de nous connecter depuis notre WAN (j'utilise personnellement Vinagre, mais tout outil permettant la connexion RDP est utilisable).



Indiquez ensuite l'IP de votre pfSense avec le port que vous avez configuré, puis spécifiez l'utilisateur avec lequel vous souhaitez vous connecter.

Vous êtes maintenant connecté à distance à votre Windows Server.

