Firewall NAT, DNAT et SNAT

Par défaut le firewall est configuré pour bloquer toutes les communications en dehors du DHCP sur votre réseau interne.
Vous devez définir les règles qui conviennent à vos besoins.

Votre **passerelle Edge** est le dispositif qui réalise la fonctionnalité de filtrage réseau. C'est donc cette passerelle que vous devez créer vos règles DNAT, SNAT et NAT.

Voici une petite explication de leur usage :

Règle	Nom Commun	Description
NAT	Network Address Translation	Nom générique utilisé quand on parle de translation d'adresse sur un réseau au moment de traverser un routeur ou un équipement actif.
DNAT	Destination NAT	Une règle DNAT modifie **l'adresse de destination** du paquet qui traverse le routeur (votre passerelle Edge) . Utilisé principalement pour acheminer un paquet arrivant sur une interface publique pour une certaine une IP publique que l'on souhaite délivrer à une **VM** étant sur un réseau privé. Pour Schématiser, SNAT est utilisé quand une communication est faite **DEPUIS** un réseau Publique **VERS** un réseau Privé
SNAT	Source NAT	Une règle SNAT modifie **l'adresse source** du paquet qui traverse le routeur (votre passerelle Edge) . Utilisé principalement pour acheminer un paquet arrivant sur une interface privée depuis une certaine une IP privé ou un réseau privé souhaitant communiquer avec un réseau externe (Publique). Pour Schématiser, SNAT est utilisé quand une communication est faite **DEPUIS** un réseau privé **VERS** un réseau Publique

Au niveau de votre **VDC**, le firewall n'est pas configuré pour autoriser des communications depuis l'interne vers l'externe . Il n'est pas non plus configuré pour autoriser une communication externe vers l'interne.
Vous devez donc configurer **au moins une règle SNAT pour sortir sur internet** (réseau publique externe) et une règle DNAT si vous souhaitez héberger un service dans votre réseau privé accessible depuis le réseau publique.

Création d'une règle SNAT *(et avoir accès à Internet)*.

Vous souhaitez que votre réseau privé puisse accéder à internet, dans ce cas, vous devez créer une règle **SNAT**

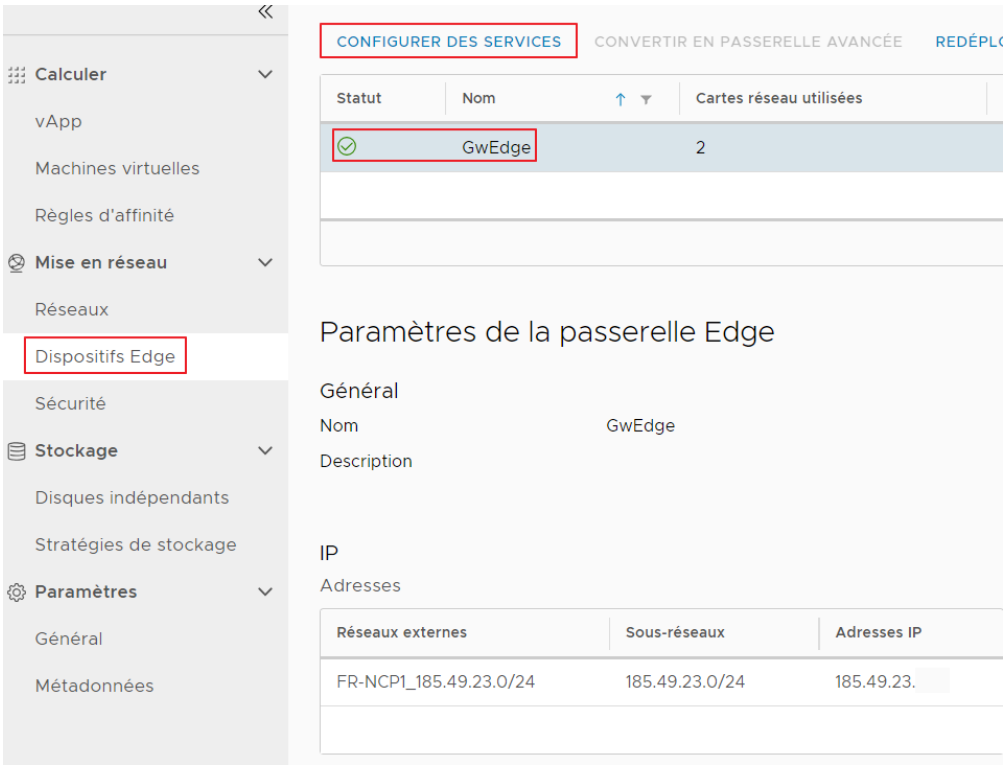
Exemple de mise en place

Dans cet exemple, nous allons configurer :

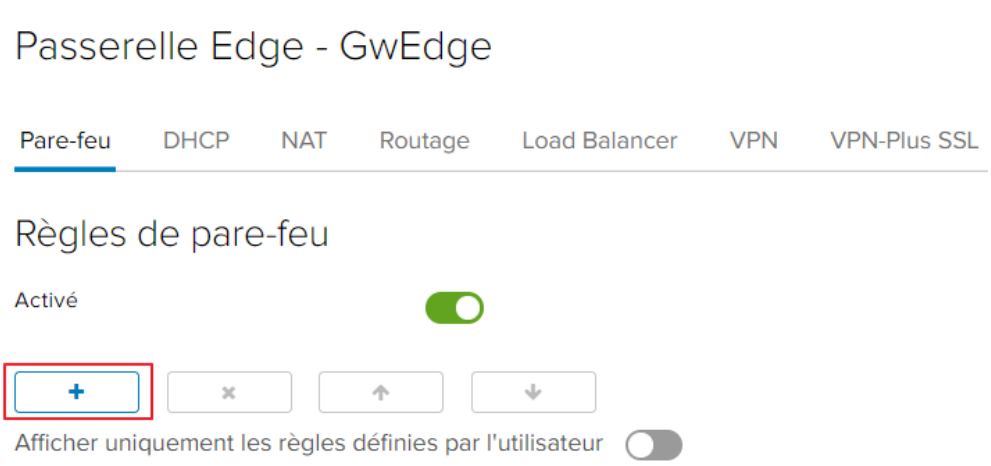
- Le **firewall** pour autoriser **tout** le réseau **local** à sortir sur internet
- Une règle **SNAT** pour que notre adresse IP publique soit utilisé pour la communication externe **pour toutes les machines du réseau local**
- Le **firewall** pour autoriser une communication **provenant de l'externe** vers **une machine et un port interne** sur le réseau local
- Une règle **DNAT** pour que la communication **externe** vers **interne** soit possible avec la translation

Depuis votre interface Vcloud, rendez-vous dans la partie **Mise en réseau, puis cliquer sur Dispositif Edge** .

Sélectionnez votre passerelle Edge et cliquer sur **CONFIGURER DES SERVICES**



Vous êtes par défaut dans l'onget **Pare-feu**



Sélectionnez la dernière ligne dans la liste des règle
Cliquez sur le **+** pour ajouter une nouvelle règle sur le **pare-feu**

Vous pouvez maintenant éditer la règle pour inscrire :

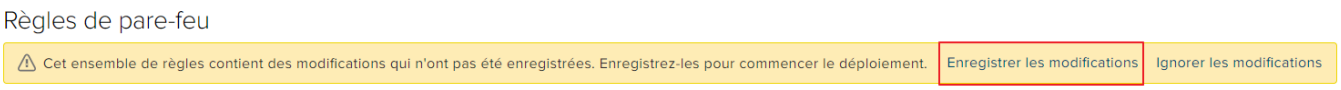
Champ	Valeur
Nom	Trafic sortant (tout autorisé)
Type	Utilisateur

Source	Internal
Destination	Tous
Service	Tous
Action	Accepter
Journalisation	*non coché*

Vous devez avoir quelque chose comme ceci :

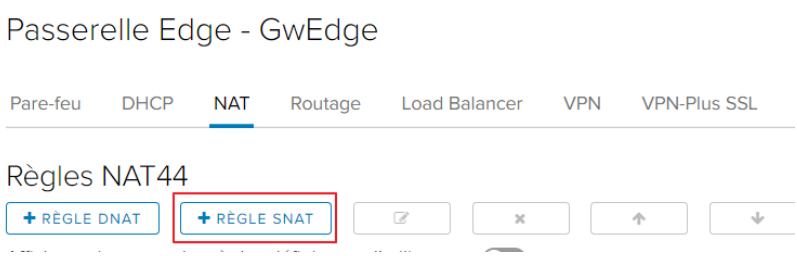
Nom	Type	Source	Destination	Service	Action	Activer la journalisation
Trafic sortant (tout autorisé)	Utilisateur	vnic-1	external	Tous	Accepter	

Pour finir, sauvegardez les modifications :

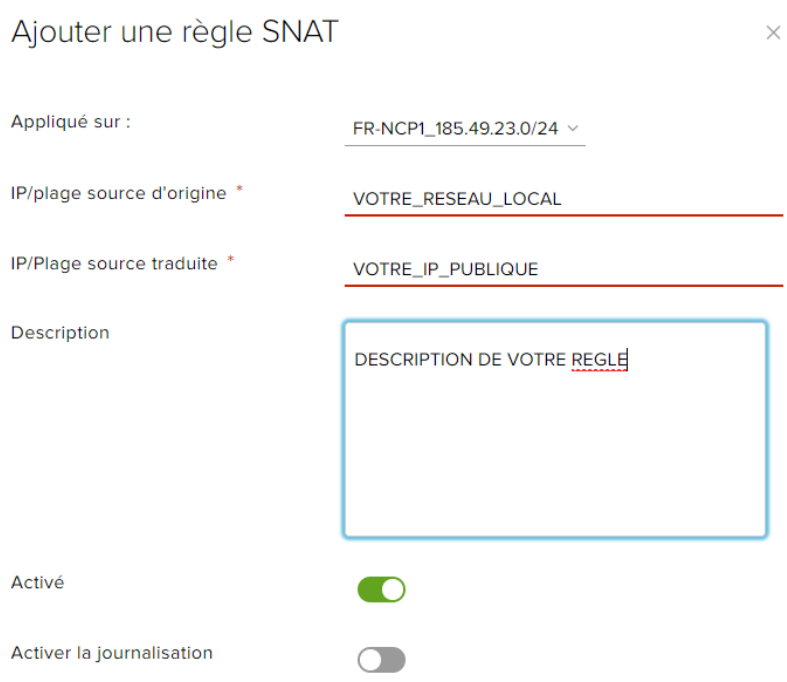


Cliquez maintenant dans l'onglet NAT pour configurer une règle SNAT

Et cliquez sur **+ REGLE SNAT**



Vous pouvez ensuite renseigner la configuration de la règle:



Détail :

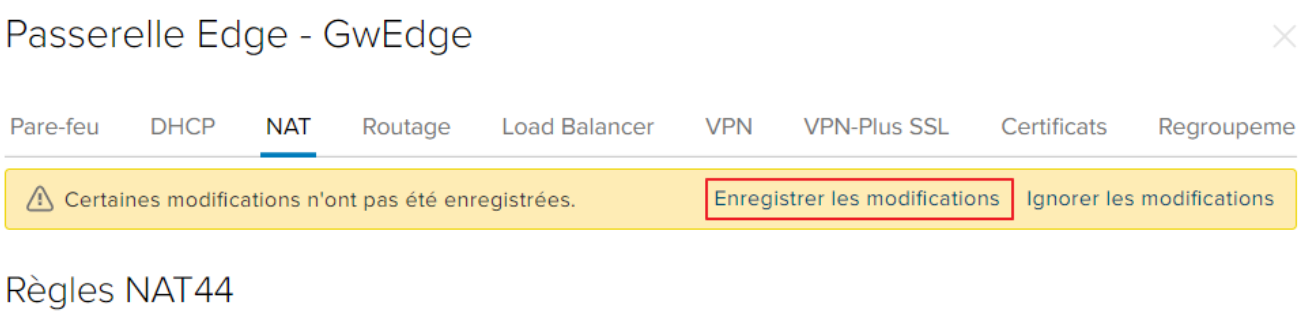
Champ	Valeur	Description
Appliqué sur	FR_NCP1_185.49.23.0/24	Élément publique
IP/plage source d'origine	192.168.50.0/24	Le réseau local couvert
IP/plage source traduite	185.49.23.**X**	Votre IP publique utilisé pour sortir sur internet. Les connexions distantes seront établies via par cette adresse IP
Description	Sortie Local vers Internet	Une description

Pour valider, cliquez sur 

Vous pouvez confirmer que la règle ajoutée correspond bien à ceci :

Type	Action	Appliqué sur	Original		Traduit		Protocole	Activé	Journalisation	Description
			Adresse IP	Port	Adresse IP	Port				
Défini par l'utilisa	SNAT	FR-NCP1_185.49.	192.168.50.0/24	Tous	185.49.23.	Tous	Tous	✔	✖	

Enregistrez les modifications :



Toutes la machines de votre réseau local doivent maintenant avoir accès à Internet

Maintenant, si vous souhaitez exposer un service **de votre réseau local** sur **internet (publiquement)** vous devez ouvrir le **pare-feu** et configurer une règle **DNAT** pour acheminer le trafic vers la bonne machine **locale** sur le bon **port**

Exemple, ouverture du port 3389 (RDP) vers une machine Windows

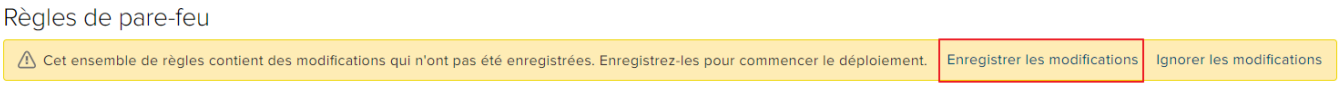
Ouverture du port sur le pare-feu :

Nom	Type	Source	Destination	Service	Action	Activer l...
RDP_IN	Utilisateur	Tous	185.49.23.	tcp:3389:any	Accepter	☐

Champ	Valeur	Description
Nom	RDP_IN	Un nom pour organiser vos règles

Type	Utilisateur	Par défaut
Source	Tous	Ici vous pouvez filter sur des IP distantes spécifiques, **Tous** autorise n'importe quelle source à se connecter sur ce port
Destination	185.49.23.**X**	Une adresse IP publique qui portera le service exposé sur Internet. Cette IP doit faire partie de votre Vcloud
Action	Accepter	Ouvrir le port = Accepter les connexions

Pour finir la configuration de cette règle, sauvegardez les modifications :



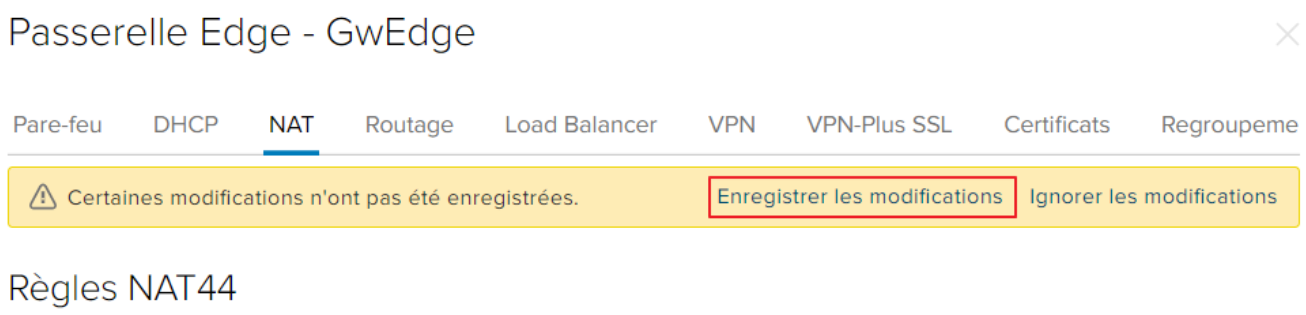
Règle DNAT

La règle DNAT va permetre le trafic **externe, arrivant sur le port 3389** d'être acheminé vers la machine virtuelle Windows (dans cet exemple) **, sur le réseau local, vers le port local 3389**

Type	Action	Appliqué sur	Original		Traduit		Protocole	Activé	Journalisation	Description
			Adresse IP	Port	Adresse IP	Port				
Défini par l'utilisateur	DNAT	FR-NCP1_185.49.23.0	185.49.23 x	3389	192.168.50.124	3389	tcp	✖	✖	

Champ	Valeur	Description
Appliqué sur	FR-NCP1_185.49.23.0	Élément Publique
Original IP	185.49.23.X	Votre IP publique utilisée pour la publication de votre service externe, celle utilisé pour l'ouverture port
Original PORT	33389	Le port exposé sur le réseau publique
Traduit IP	xxx.xxx.xxx.xxx	L'adresse IP de votre machine sur le réseau local (192.168.50.XXX, par défaut)
Traduit PORT	3389	Le port sur lequel écoute le service local, 3389 représente ici l'accès disant RDP
Protocole	TCP	Le protocole utilisé par le service exposé
Activé	coché	Pour activer la règle
Journalisation	non-coché	Pour des besoins de journalisation, laisser non activé par défaut.

Sauvegarder les modification , vous pouvez tester le bon fonctionnement du service .



Toute la configuration est terminée. Vous devez pouvoir :

- vous connecter à Internet depuis une machine de votre réseau local
- communiquer depuis l'externe (Internet) sur le port 3389 de votre IP publique et avoir une réponse du service RDP de votre machine locale écoutant sur le port 3389

Attention :

Vous devez vous assurer que le pare-feu **LOCAL** à votre machine autorise bien les connexions sur le port que vous souhaitez rendre disponible