



Diffusion :

- Libre
- Restreinte
- Interne

LA SOLUTION NETXSERV



Configuration firewall

Cette fiche explique la configuration du firewall intégré à NetXServ

Version	2.0
Auteur	JP
MAJ	DD
Date	28/12/2011
Validation	

Table des matières

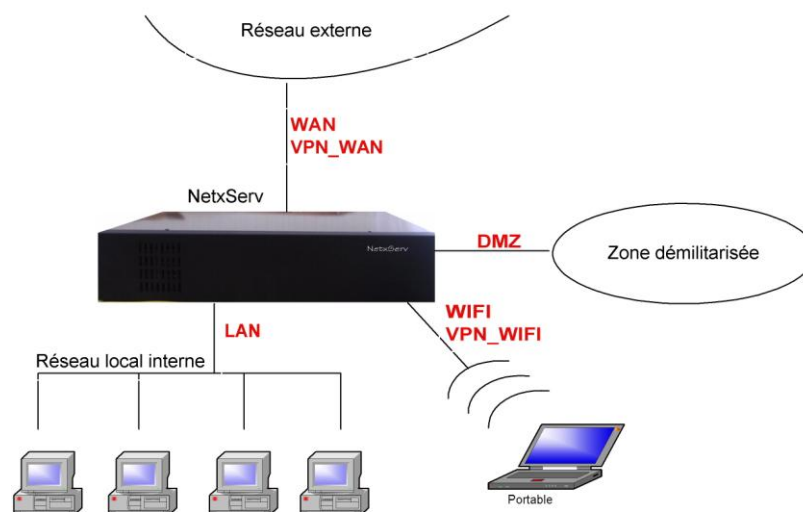
1	Introduction.....	3
2	Comment configurer le firewall du Netxserv?	4
2.1	Gestion des ports	4
2.2	Gestion des macros de filtrage.....	6
2.3	Modification des règles utilisateur.....	9
2.4	Etat des règles	11
2.5	Log des refus.....	12
3	Exemples de configuration firewall.....	13
3.1	Politique de sécurité envisageable.....	13
3.2	Configuration de la règle pour les flux vers l'opérateur SIP.....	14
3.3	Autorisation de flux web sortant.....	14
3.4	Autorisation de flux DNS	15
3.5	Autorisation de flux POP et SMTP	15
3.6	Autorisation des flux VPN SSL pour un nomade.....	16

1 Introduction

Votre IPBX NetxServ peut être équipé d'une ou plusieurs interfaces Ethernet. Afin de simplifier la gestion de ces interfaces, celles-ci sont identifiées par des noms logiques plutôt que par des interfaces physiques. L'association que vous ferez entre les noms physiques (eth0, eth1) et les noms logiques (LAN, WAN, DMZ) définira les règles de protection appliquées à chacune des interfaces Ethernet de votre PABX.

Votre serveur NetXServ gère les interfaces suivantes :

- **LAN** : Votre réseau local
- **WAN** : Sortie Ethernet ou ADSL vers Internet
- **DMZ** : Sortie Ethernet optionnel vers la DMZ
- **WIFI** : Point d'accès sans fil WiFi optionnel



Le Firewall du NetXServ n'est plus activé par défaut, et il n'y a donc plus aucune règles de créer (sauf si vous avez importé une sauvegarde).

Pour activer le service Firewall, il faut aller en mode avancé dans le menu **Administration** → **Services**



Cliquer sur le bouton en forme de crayon pour modifier l'état du service et le mettre à Oui pour l'activer.

L'activation du service nécessite une **Configuration générale avec reboot** (Menu **Actions**)

Il est donc préférable de configurer vos règles et d'activer le service avant de faire cette action, pour ne pas à avoir à le refaire.

2 Comment configurer le firewall du Netxserv?

Le menu principal de la configuration du firewall est accessible en mode avancé dans le menu **Réseau** → **Firewall** :



The screenshot shows a web interface titled "Gestion firewall". It features a grid of menu items for firewall management, organized into two columns. The items are: Etat des règles, Règles utilisateur actives, Etat connexions IP, Profils firewall, Etat des routes, Re-configuration Firewall, Log des refus, Règles utilisateur inactives, Gestion des macros de filtrage, Gestion des ports, Etat des tâches, and Reconfiguration DHCPD.

Gestion firewall	
Etat des règles	Log des refus
Règles utilisateur actives	Règles utilisateur inactives
	Gestion des macros de filtrage
Etat connexions IP	Gestion des ports
Profils firewall	
Etat des routes	Etat des tâches
Re-configuration Firewall	Reconfiguration DHCPD

A partir de cette interface, il est possible de modifier toute la configuration par défaut du firewall.

2.1 Gestion des ports

Comment créer un port ?

La première étape de la configuration du firewall sera de définir les ports que vous allez utiliser. Un certain nombre de port a déjà été préconfiguré sur votre serveur. Vérifiez si le port que vous souhaitez utiliser n'existe pas déjà. Si c'est le cas, vous pourrez modifier ceux qui existent. Sinon, vous devez créer un nouveau port.

Le menu **Gestion des ports** permet de créer ou de modifier la liste des ports. Après sélection de l'onglet « Gestion des ports », la liste des ports déjà créés apparaît. Ce menu permet de configurer différents ports et aussi d'en créer des nouveaux. Les ports sont définis par un nom et un numéro de port ouvert.

Liste des ports

Créer un nouveau port

Annuler

Nom	Valeur	Description	
5061	5061	GTW patton	
>1023	1024:65535	port non privilégié	
admin_trapeze	8889	Admin Trapeze	
Aucun		Aucun port	
bootpc	68		
bootpc-udp	68		
bootps	67		
bootps-udp	67		
Cluster	694	Port synchronisation cluster	
dns	53		
dns-udp	53		
dns_1026	1026		
dns_135	135		
dns_445	445	Dns dynamique M5	
drbd	7788	Drbd	
ecu-regina	8000	Port de dialogue Ecu vers Regina	

Pour modifier un port existant, cliquez sur le bouton d'édition de la ligne correspondante.

Pour créer un nouveau port, cliquer sur le bouton

Créer un nouveau port

La modification ou la création affiche l'écran suivant :

Modification d'un port

Nom	<input type="text" value="pop3"/>
Valeur	<input type="text" value="110"/>
Description	<input type="text" value="Port pour recuperation mail"/>

Valider

Annuler

Vous devez alors définir le nom que vous souhaitez donner au port ainsi que sa valeur. Rajoutez une description permettant d'avoir une idée plus précise du port.

























2.2 Gestion des macros de filtrage

Comment créer une macro de filtrage ?

Le menu **Gestion des macros de filtrage** permet de créer de nouvelles règles de filtrage.

Après sélection de l'onglet « Gestion des macros de filtrage », la liste des macros déjà créées apparaît. On peut atteindre cette page en passant également par la modification des règles de filtrage en regardant la liste des flux.

Liste des macros de filtrages

Nom	Description		
Saisir le nom	Saisir la description		
Netbios broadcast	exploration Netbios		
netbios entrant	netbios entrant		
ldap sortant	appel serveur ldap		
ldap entrant	ldap entrant		
snmp squid entrant	snmp squid entrant		
snmp squid sortant	snmp squid sortant		
ntp sortant	ntp sortant		
ntp entrant	ntp entrant		
dns sortant	dns sortant		
proxy sortant	proxy sortant		
snmp entrant	snmp entrant		
snmp sortant	snmp sortant		
snmp_trap_entrant	snmp_trap_entrant		

Pour modifier une macro existante, cliquez sur le bouton d'édition de la ligne correspondante. Pour supprimer une macro existante, cliquez sur le bouton de suppression de la ligne correspondante. Enfin, Pour créer une nouvelle entrée, cliquez sur le bouton :

La modification affiche l'écran suivant :



Modification de macro

Nom	<input type="text" value="web sortant"/>
Description	<input type="text" value="web sortant"/>

Liste des règles de filtrages associées

Port interne entrée	Port externe entrée	Port interne sortie	Port externe sortie	Protocole	Options input	Options output	Options ICMP	Type ICMP	Sens ICMP	Description		
>1023	http	>1023	http	tcp	! --syn -m state --state ESTABLISHED,RELATED				o	http		
>1023	https	>1023	https	tcp	! --syn -m state --state ESTABLISHED,RELATED				o	https		

Une macro de filtrage est une règle qui vous permettra de définir un flux prenant en compte :

- les ports utilisés en interne (c'est-à-dire des ports utilisés par les clients de votre réseau),
- les ports externes impliqués dans la communication IP
- le type de port (TCP ou UDP)
- le sens de cette communication (entrant/input ou sortant/output)

On peut aussi ajouter une vérification de la connexion établie (exemple : on reçoit un message alors que l'on a rien envoyé).

Pour associer une nouvelle règle de filtrage, cliquez sur le bouton :

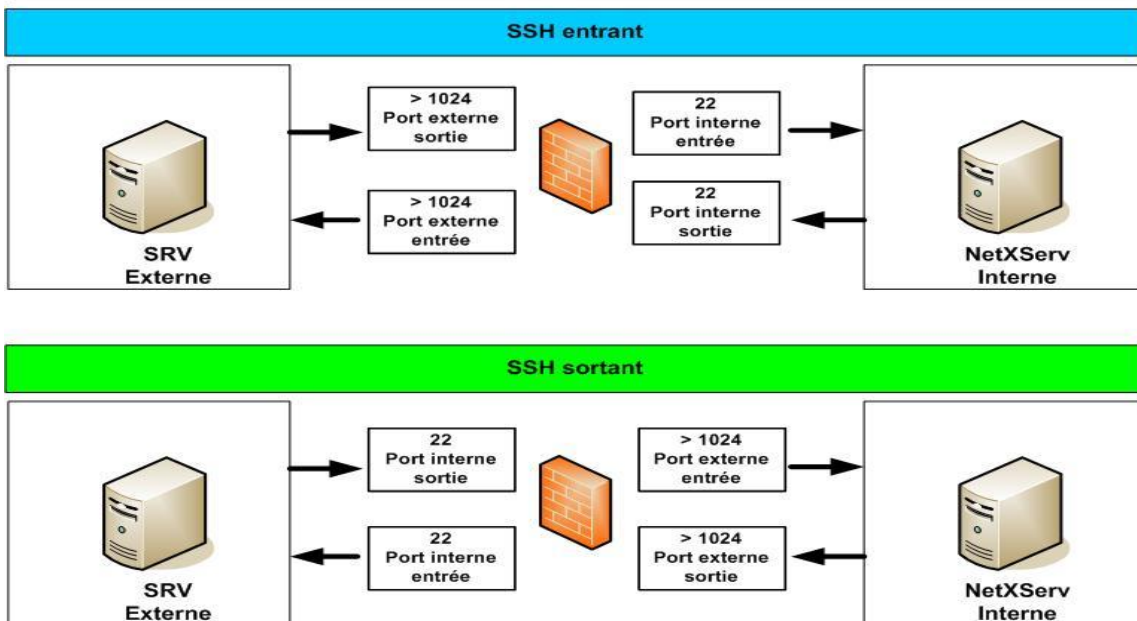
Modification d'une règle de filtrage

Port interne entrée	>1023 (1024:65535)		
Port externe entrée	https (443)		
Port interne sortie	>1023 (1024:65535)		
Port externe sortie	https (443)		
Protocole	tcp		
Type ICMP	(*)		
Sens ICMP	o (output)		
Description	https		
Options input	! --syn -m state --state ESTABLISHED,RELATED		
Options output			
Options ICMP			

La règle ci-dessus, par exemple, définit ainsi un flux dénommé HTTPS qui concerne toute tentative de communication vers l'extérieur du réseau protégé par le firewall qui satisfait les conditions suivantes :

- Le port interne de provenance doit être un port supérieur à 1023
- Le port externe de destination doit être le port 443
- Le port interne de destination doit être un port supérieur à 1023
- Le port externe de provenance doit être le port 443
- La communication doit être initiée à partir du réseau local

Explication de la configuration d'une macro de filtrage sur NetXServ



2.3 Modification des règles utilisateur

Comment mettre en place une règle de filtrage de flux ?
















La dernière étape de configuration des règles de firewall consiste à dire, par rapport à un flux donné, quelles sont les règles à mettre en place. Ceci se fait à travers le lien **Modification des règles utilisateur**.

Après sélection de l'onglet «**Modification des règles utilisateur**», la liste des filtres déjà créés apparaît :

Liste des règles de filtrages

Créer une nouvelle règle de filtrage

Annuler

num	Flux	Actif	IP interne	IP externe	Interface	Vlan	Action	IP NAT	Port NAT	Description	
3093	web sortant	oui	ip wan dynamique	anywhere	wan	0	MASQUERADE	ZZZNULL		Lan Web sortant vers Internet	  
3094	dns sortant	oui	anywhere	dns1	wan	0	ACCEPT	ZZZNULL		DNS sortant vers Internet	  
3095	pop3 sortant	oui	Reseau LAN	anywhere	wan	0	MASQUERADE	ZZZNULL		POP sortant vers Internet	  
3096	smtp sortant	oui	Reseau LAN	anywhere	wan	0	MASQUERADE	ZZZNULL		SMTP sortant vers Internet	  
3102	dns sortant	oui	anywhere	dns2	wan	0	ACCEPT	ZZZNULL		DNS sortant vers Internet	  

Pour modifier une règle existante, cliquez sur le bouton d'édition représenté par le **crayon** de la ligne correspondante.

Pour supprimer une règle existante, cliquez sur le bouton (représenté par la **croix**)

Pour dupliquer une règle, il faut cliquer que le dernier bouton de la ligne correspondante.

Pour créer une nouvelle entrée, cliquez sur le bouton

Créer une nouvelle règle de filtrage

La modification ou la création affiche l'écran suivant :

Modification de règle utilisateur

Actif	<input type="checkbox"/> oui <input checked="" type="checkbox"/>	
Flux	<input type="text" value="smtp sortant"/>	
Adresse interne	<input type="text" value="RESEAU LAN (192.168.200.0/24)"/>	
Adresse externe	<input type="text" value="anywhere (any/0)"/>	
Interface	<input type="text" value="wan (wan)"/>	
Action	<input type="text" value="MASQUERADE (Masquage adresse)"/>	
Adresse NAT	<input type="text" value="ZZZNULL ()"/>	
Port NAT	<input type="text" value="(tous)"/>	
Vlan	<input type="text" value="0"/>	
Mark	<input type="text"/>	
Protocole niveau 7 actif	<input "="" type="checkbox" value="non <input checked="/>	Liste
Protocole niveau 7	<input type="text" value="bittorrent (bittorrent)"/>	
Description	<input type="text" value="SMTP sortant vers Internet"/>	

Il est possible d'avoir la liste des flux en cliquant sur le lien liste (à droite) qui mène vers la gestion des macros de filtrages.

Après avoir choisi le flux concerné par la règle de filtrage, il vous faut définir les adresses IP impliquées dans la communication :

- l'adresse interne qui est celle de votre réseau interne ou l'adresse IP d'un équipement de votre réseau
- l'adresse externe qui est l'adresse hors de votre réseau

Vous devez ensuite indiquer laquelle, des interfaces Ethernet de votre NetXServ, va relayer le flux en question.

Enfin, il vous faut indiquer quelle est la règle qui devra être appliquée :

Action	<input type="text" value="ACCEPT ()"/>	
Adresse NAT	<input type="text" value="ACCEPT ()"/>	
Vlan	<input type="text" value="LOG ()"/>	
Mark	<input type="text" value="MARK (MARK)"/>	

Les options possibles sont :

- **ACCEPT** : accepter la communication
- **DNAT** : faire du NAT sur l'adresse de destination de sorte à forcer une seule destination (utile dans le cas d'un proxy par exemple)
- **DROP** : rejeter la communication
- **SNAT** : faire du NAT de l'adresse source de sorte que le destinataire ne voit que l'adresse IP du NetXServ
- **MARK** : marquer le paquet
- **MASQUERADE** : faire passer tout le trafic comme venant de l'adresse IP du NetXServ

2.4 Etat des règles

Le menu **Etat des règles** permet de visualiser les règles de filtrage du firewall.

Après sélection de l'onglet « **Etat des règles** », la liste des règles de filtrage apparaît :

Liste des regles de filtrage

Mise à jour du 25/08/08 à 14h55

Chain	PREROUTING	(policy	DROP	4253	packets,	382169	bytes)					
pkts	bytes	target	prot	opt	in	out	source	destination				
18502	6668297	ACCEPT	all	--	lo	*	0.0.0.0/0	0.0.0.0/0				
68	9244	ACCEPT	tcp	--	eth0	*	192.168.0.0/16	0.0.0.0/0	tcp	spts:1024:65535	dpt:22	
727	164753	ACCEPT	tcp	--	eth0	*	192.168.0.0/16	0.0.0.0/0	tcp	spts:1024:65535	dpt:8081	
854995	160994189	ACCEPT	all	--	eth0	*	0.0.0.0/0	0.0.0.0/0				
0	0	ACCEPT	tcp	--	eth0	*	192.168.0.0/16	0.0.0.0/0	tcp	spts:1024:65535	dpt:5038	
0	0	ACCEPT	tcp	--	eth0	*	192.168.0.0/16	0.0.0.0/0	tcp	spts:1024:65535	dpt:4445	
362305	33066165	entree_eth0	all	--	*	*	0.0.0.0/0	0.0.0.0/0				
362305	33066165	entree_eth1	all	--	*	*	0.0.0.0/0	0.0.0.0/0				
4249	371081	entree_eth2	all	--	*	*	0.0.0.0/0	0.0.0.0/0				
4249	371081	entree_eth3	all	--	*	*	0.0.0.0/0	0.0.0.0/0				
4249	371081	entree_ath0	all	--	*	*	0.0.0.0/0	0.0.0.0/0				
4249	371081	entree_ath1	all	--	*	*	0.0.0.0/0	0.0.0.0/0				
4249	371081	entree_ath2	all	--	*	*	0.0.0.0/0	0.0.0.0/0				
4249	371081	entree_ppp0	all	--	*	*	0.0.0.0/0	0.0.0.0/0				
4249	371081	entree_vpn_eth1	all	--	*	*	0.0.0.0/0	0.0.0.0/0				
4249	371081	entree_ipsec0	all	--	*	*	0.0.0.0/0	0.0.0.0/0				
4249	371081	entree_vpn_wifi	all	--	*	*	0.0.0.0/0	0.0.0.0/0				

Cette liste vous renseigne sur l'ensemble des règles de filtrage actuellement activées sur votre NetXServ. En particulier, cette synthèse vous permet de savoir :

- L'adresse d'origine
- Le port d'origine
- L'adresse de destination
- Le port de destination
- Le type de protocole (tcp ou udp)
- L'interface Ethernet concernée
- La règle applicable : Les différentes règles applicables sont les suivantes : DROP pour rejet, ACCEPT pour accepter, MASQUERADE (pour substituer l'adresse de l'émetteur par celle du NetXServ).

2.5 Log des refus

La log de refus permet de visualiser toutes les tentatives d'intrusions.

Cette log nous fournit des informations comme la date de la tentative d'intrusion mais aussi l'IP source ainsi que l'IP destinataire.

L'interface à droite permet une navigation simple dans le fichier log.

Il est possible de choisir le nombre de lignes à afficher par pages ou bien choisir la ligne de départ de lecture de la log.

A l'aide des flèches de déplacement situées à droite, on peut naviguer dans tout le fichier log pages par pages, aller directement à la fin du fichier ou bien revenir au début.

Une recherche par mot clé est également disponible, aussi bien sur tout le document que par colonne.

Il est possible en cliquant sur le nom d'une colonne de trier cette colonne.

gestion netxserv

user1 (Administrateur avancé) | Déconnexion Mode sin Mode simplifié

Lignes par page: 25 Ligne de départ: 1

Recherche: * Rechercher

Télécharger

num	ligne	date	chaine	in	out	source	dest	DF	proto	spt	dpt	type	code	ttl	seq
1	1	Aug 25 19:08:53	LOG_REFUS_mangle_PREROUTING	IN=eth1	OUT=	MAC=00:19:99:36:8e:c9:00:e0:29:58:e4:02:08:00	SRC=192.168.15.10	.	ID=5898	.	.	PROTO=UDP	SPT=4797	PREC=0x00	LEN=43
2	2	Aug 25 19:08:49	LOG_REFUS_mangle_PREROUTING	IN=eth1	OUT=	MAC=00:19:99:36:8e:c9:00:e0:29:58:e4:02:08:00	SRC=192.168.15.10	.	ID=5896	.	.	PROTO=UDP	SPT=4797	PREC=0x00	LEN=43
3	3	Aug 25 19:08:47	LOG_REFUS_mangle_PREROUTING	IN=eth1	OUT=	MAC=00:19:99:36:8e:c9:00:e0:29:58:e4:02:08:00	SRC=192.168.15.10	.	ID=5895	.	.	PROTO=UDP	SPT=4797	PREC=0x00	LEN=43
4	4	Aug 25 19:08:46	LOG_REFUS_mangle_PREROUTING	IN=eth1	OUT=	MAC=00:19:99:36:8e:c9:00:e0:29:58:e4:02:08:00	SRC=192.168.15.10	.	ID=5895	.	.	PROTO=UDP	SPT=4797	PREC=0x00	LEN=43
5	5	Aug 25 19:08:45	LOG_REFUS_mangle_PREROUTING	IN=eth1	OUT=	MAC=00:19:99:36:8e:c9:00:e0:29:58:e4:02:08:00	SRC=192.168.15.10	.	ID=5894	.	.	PROTO=UDP	SPT=4797	PREC=0x00	LEN=43
6	6	Aug 25 19:08:44	LOG_REFUS_mangle_PREROUTING	IN=eth1	OUT=	MAC=ff:ff:ff:ff:ff:ff:00:e0:29:58:e4:02:08:00	SRC=192.168.15.10	.	ID=5894	.	.	PROTO=UDP	SPT=137	PREC=0x00	LEN=58
7	7	Aug 25 19:08:43	LOG_REFUS_mangle_PREROUTING	IN=eth1	OUT=	MAC=ff:ff:ff:ff:ff:ff:00:e0:29:58:e4:02:08:00	SRC=192.168.15.10	.	ID=5893	.	.	PROTO=UDP	SPT=137	PREC=0x00	LEN=58
8	8	Aug 25 19:08:43	LOG_REFUS_mangle_PREROUTING	IN=eth1	OUT=	MAC=ff:ff:ff:ff:ff:ff:00:e0:29:58:e4:02:08:00	SRC=192.168.15.10	.	ID=5893	.	.	PROTO=UDP	SPT=137	PREC=0x00	LEN=58
9	9	Aug 25 19:08:34	LOG_REFUS_mangle_PREROUTING	IN=eth1	OUT=	MAC=00:19:99:36:8e:c9:00:e0:29:58:e4:02:08:00	SRC=192.168.15.10	.	ID=5889	.	.	PROTO=UDP	SPT=4795	PREC=0x00	LEN=43
10	10	Aug 25 19:08:30	LOG_REFUS_mangle_PREROUTING	IN=eth1	OUT=	MAC=00:19:99:36:8e:c9:00:e0:29:58:e4:02:08:00	SRC=192.168.15.10	.	ID=5887	.	.	PROTO=UDP	SPT=4795	PREC=0x00	LEN=43
11	11	Aug 25 19:08:28	LOG_REFUS_mangle_PREROUTING	IN=eth1	OUT=	MAC=00:19:99:36:8e:c9:00:e0:29:58:e4:02:08:00	SRC=192.168.15.10	.	ID=5886	.	.	PROTO=UDP	SPT=4795	PREC=0x00	LEN=43
12	12	Aug 25 19:08:27	LOG_REFUS_mangle_PREROUTING	IN=eth1	OUT=	MAC=00:19:99:36:8e:c9:00:e0:29:58:e4:02:08:00	SRC=192.168.15.10	.	ID=5886	.	.	PROTO=UDP	SPT=4795	PREC=0x00	LEN=43
13	13	Aug 25 19:08:26	LOG_REFUS_mangle_PREROUTING	IN=eth1	OUT=	MAC=00:19:99:36:8e:c9:00:e0:29:58:e4:02:08:00	SRC=192.168.15.10	.	ID=5885	.	.	PROTO=UDP	SPT=4795	PREC=0x00	LEN=43
14	14	Aug 25 19:08:25	LOG_REFUS_mangle_PREROUTING	IN=eth1	OUT=	MAC=ff:ff:ff:ff:ff:ff:00:e0:29:58:e4:02:08:00	SRC=192.168.15.10	.	ID=5884	.	.	PROTO=UDP	SPT=137	PREC=0x00	LEN=58
15	15	Aug 25 19:08:24	LOG_REFUS_mangle_PREROUTING	IN=eth1	OUT=	MAC=ff:ff:ff:ff:ff:ff:00:e0:29:58:e4:02:08:00	SRC=192.168.15.10	.	ID=5884	.	.	PROTO=UDP	SPT=137	PREC=0x00	LEN=58
16	16	Aug 25 19:08:23	LOG_REFUS_mangle_PREROUTING	IN=eth1	OUT=	MAC=ff:ff:ff:ff:ff:ff:00:e0:29:58:e4:02:08:00	SRC=192.168.15.10	.	ID=5883	.	.	PROTO=UDP	SPT=137	PREC=0x00	LEN=58
17	17	Aug 25 19:08:16	LOG_REFUS_mangle_PREROUTING	IN=eth1	OUT=	MAC=00:19:99:36:8e:c9:00:e0:29:58:e4:02:08:00	SRC=192.168.15.10	.	ID=5881	.	.	PROTO=UDP	SPT=4794	PREC=0x00	LEN=98
18	18	Aug 25 19:08:13	LOG_REFUS_mangle_PREROUTING	IN=eth1	OUT=	MAC=ff:ff:ff:ff:ff:ff:00:30:64:04:d5:42:08:00	SRC=192.168.15.5	.	ID=5647	.	.	PROTO=UDP	SPT=138	PREC=0x00	LEN=209

Il est possible, en cliquant sur le bouton télécharger, de charger la log sur son disque en choisissant l'emplacement de téléchargement.

Chaque ligne dans cette log correspond à une tentative d'accès que le firewall du PABX NetXServ a bloqué ou simplement logué (selon les règles que vous avez établies). Il faut, en particulier, prendre en compte dans l'interprétation les champs suivants :

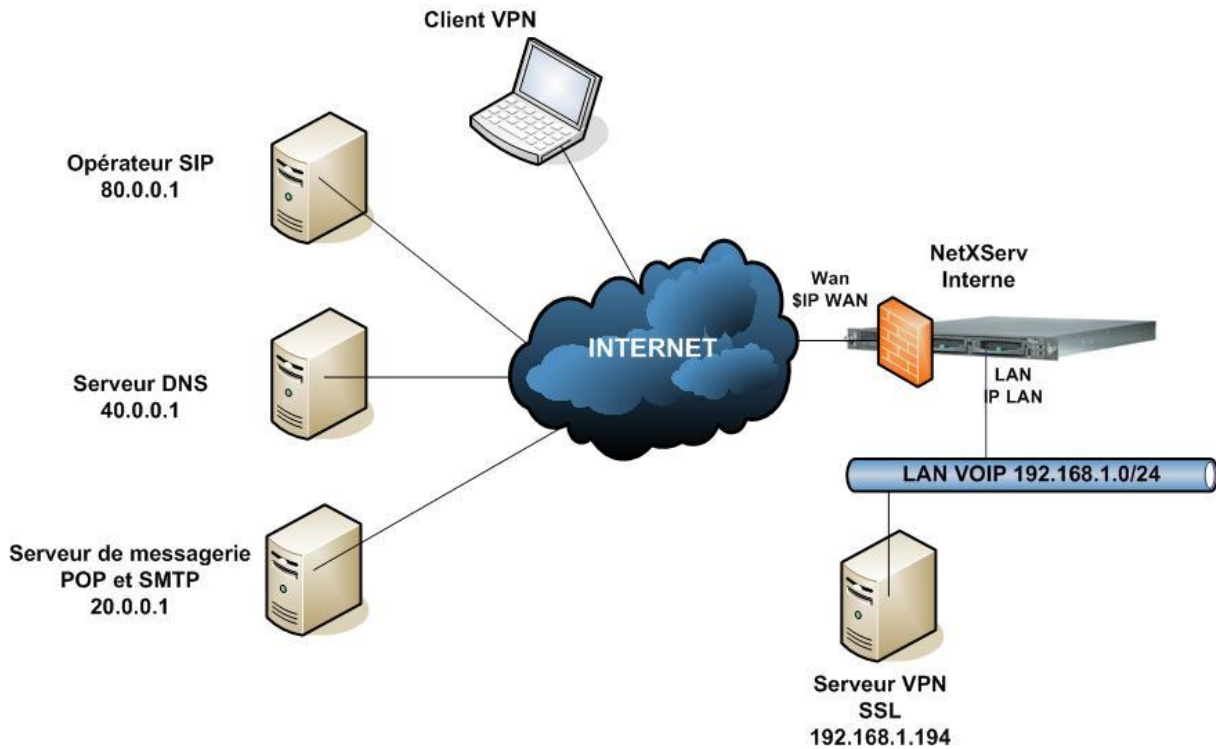
- L'adresse IP source qui est l'adresse de l'émetteur de la demande (src)
- L'adresse IP destination (dest)
- Le port source (spt)
- Le port de destination (dpt)

Ceci vous permettra ainsi d'identifier un paquet, le moment où il a été rejeté et les parties impliquées dans cet échange infructueux.

3 Exemples de configuration firewall

Type d'architecture réseau

Information : les adresses IP sur le schéma ci-dessous sont uniquement à titre d'exemple.



Information : la première chose à faire dans ce type d'architecture, est d'activer le firewall sur votre serveur NetXServ.







3.1 Politique de sécurité envisageable

Flux	IP interne	IP externe	Interface	VLAN	Action
SIP	\$IP WAN	80.0.0.1	wan	0	ACCEPT
DNS sortant	\$IP WAN	40.0.0.1(DNS)	wan	0	ACCEPT
WEB sortant	192.168.1.0/24	Anywhere	wan	0	ACCEPT
POP	192.168.1.0/24	20.0.0.1	wan	0	MASQUERADE
SMTP	192.168.1.0/24	20.0.0.1	wan	0	MASQUERADE
VPN SSL	\$IP WAN	Anywhere	wan	0	DNAT







\$IP WAN : correspond à l'adresse IP publique de votre serveur NetXServ.

3.2 Configuration de la règle pour les flux vers l'opérateur SIP

L'autorisation des flux SIP vers un opérateur SIP doit se faire avec beaucoup de précaution. Cette autorisation doit se faire uniquement vers l'adresse IP publique d'opérateur SIP dont vous avez connaissance.

Actif	<input type="checkbox"/> oui <input checked="" type="checkbox"/> non	
Flux	Sip	
Adresse interne	ip wan dynamique (\$IP_WAN)	
Adresse externe	OPERATEUR SIP 80.0.0.1 (80.0.0.1)	
Interface	wan (wan)	
Action	ACCEPT <input type="checkbox"/>	
Adresse NAT	ZZZNULL <input type="checkbox"/>	
Port NAT	(Aucun)	
Vlan	<input type="text" value="0"/>	
Mark	<input type="text"/>	
Protocole niveau 7 actif	<input type="checkbox"/> non <input checked="" type="checkbox"/> oui	Liste
Protocole niveau 7	bittorrent (bittorrent)	
Description	SIP VERS L'OPERATEUR SIP	

3.3 Autorisation de flux web sortant

Actif	<input type="checkbox"/> oui <input checked="" type="checkbox"/> non	
Flux	web sortant	
Adresse interne	LAN 192.168.1.0/24 (192.168.1.0/24)	
Adresse externe	anywhere (any/0)	
Interface	wan (wan)	
Action	ACCEPT <input type="checkbox"/>	
Adresse NAT	ZZZNULL <input type="checkbox"/>	
Port NAT	(tous)	
Vlan	<input type="text" value="0"/>	
Mark	<input type="text"/>	
Protocole niveau 7 actif	<input type="checkbox"/> non <input checked="" type="checkbox"/> oui	Liste
Protocole niveau 7	bittorrent (bittorrent)	
Description	WEB SORTANT	

3.4 Autorisation de flux DNS

Actif	<input type="checkbox"/> oui <input checked="" type="checkbox"/> non	
Flux	dns sortant	
Adresse interne	ip wan dynamique (\$IP_WAN)	
Adresse externe	DNS 40.0.0.1 (40.0.0.1)	
Interface	wan (wan)	
Action	ACCEPT <input checked="" type="checkbox"/>	
Adresse NAT	ZZZNULL <input checked="" type="checkbox"/>	
Port NAT	(tous)	
Vlan	<input type="text" value="0"/>	
Mark	<input type="text"/>	
Protocole niveau 7 actif	non <input checked="" type="checkbox"/>	Liste
Protocole niveau 7	bittorrent (bittorrent)	
Description	DNS SORTANT	

3.5 Autorisation de flux POP et SMTP

Actif	<input type="checkbox"/> oui <input checked="" type="checkbox"/> non	
Flux	pop3 sortant	
Adresse interne	LAN 192.168.1.0/24 (192.168.1.0/24)	
Adresse externe	POP/SMTP 20.0.0.1 (20.0.0.1)	
Interface	wan (wan)	
Action	MASQUERADE (Masquage adresse)	
Adresse NAT	ZZZNULL <input checked="" type="checkbox"/>	
Port NAT	(tous)	
Vlan	<input type="text" value="0"/>	
Mark	<input type="text"/>	
Protocole niveau 7 actif	non <input checked="" type="checkbox"/>	Liste
Protocole niveau 7	bittorrent (bittorrent)	
Description	POP SORTANT	







Actif	<input type="checkbox"/> oui 0	
Flux	smtp sortant	
Adresse interne	LAN 192.168.1.0/24 (192.168.1.0/24)	
Adresse externe	POP/SMTP 20.0.0.1 (20.0.0.1)	
Interface	wan (wan)	
Action	MASQUERADE (Masquage adresse)	
Adresse NAT	ZZZNULL ()	
Port NAT	(tous)	
Vlan	<input type="text" value="0"/>	
Mark	<input type="text"/>	
Protocole niveau 7 actif	<input type="checkbox"/> non 0	Liste
Protocole niveau 7	bittorrent (bittorrent)	
Description	<input type="text" value="SMTP SORTANT"/>	

3.6 Autorisation des flux VPN SSL pour un nomade

La macro du VPN SSL Sortant

Port interne entrée	openvpn_1194 (1194)		
Port externe entrée	>1023 (1024:65535)		
Port interne sortie	openvpn_1194 (1194)		
Port externe sortie	>1023 (1024:65535)		
Protocole	udp		
Type ICMP	(*)		
Sens ICMP	i (input)		
Description	<input type="text" value="VPN SSL"/>		
Options input	<input type="text"/>		
Options output	<input type="text"/>		
Options ICMP	<input type="text"/>		

La règle filtrage du flux VPN SSL Sortant

Actif	<input type="checkbox"/> oui <input checked="" type="checkbox"/> non	
Flux	VPN SSL SORTANT	
Adresse interne	ip wan dynamique (\$IP_WAN)	
Adresse externe	anywhere (any/0)	
Interface	wan (wan)	
Action	DNAT (nat destination)	
Adresse NAT	SRV VPN 192.168.1.194 (192.168.1.194)	
Port NAT	1194 (openvpn_1194)	
Vlan	<input type="text" value="0"/>	
Mark	<input type="text"/>	
Protocole niveau 7 actif	<input type="checkbox"/> non <input checked="" type="checkbox"/> oui	Liste
Protocole niveau 7	bittorrent (bittorrent)	
Description	<input type="text" value="SSL VERS Serveur VPN"/>	