



Bien configurer le pare-feu de votre routeur par Magicsam

Voici un petit récapitulatif d'un sujet déjà abordé sur le Forum, à savoir optimiser au mieux la configuration du pare-feu de votre routeur.

Ce petit Tutorial prend comme exemple l'interface de configuration française du DG834(G), mais il peut s'appliquer à tous les routeurs Netgear des séries DG, FR, FM, FV, FW.

Seuls les routeurs Netgear des séries RP et WG ne disposent pas d'un paramétrage des règles du pare feu en entrée et sortie.

Seule la 2ème solution de ce Tutorial est applicable pour ces séries à l'aide de la fonction [Block Services](#).

Par défaut, le pare feu SPI de votre routeur bloque toutes les communications entrantes et autorise toutes les communications sortantes.

Pas de problème donc du côté du pare-feu entrant puisqu'il est déjà configuré pour interdire toute tentative d'intrusion.

Vous devrez simplement, si besoin est, autoriser les ports entrants nécessaires à certains applications spécifiques (dans mon exemple de configuration un serveur FTP et BitTorrent pour le PC en 192.168.0.2).

C'est donc du côté du pare-feu sortant que l'on peut optimiser la sécurité.

2 Solutions :

- Privilégier un niveau de sécurité maximum
- Faire un compromis entre la sécurité et la souplesse de configuration

Privilégier un niveau de sécurité maximum

- Règles de base pour autoriser la Navigation Internet et l'envoi/réception d'e-mail (règles 1 à 7)

Créer une règle pour autoriser (**ALLOW always**) les services (déjà pré configurés) DNS, FTP, SMTP, HTTP, HTTPS, NTTP pour les adresses IP des PC qui doivent avoir une connexion Internet (dans mon exemple de configuration seulement les deux PC en 192.168.0.2 et 192.168.0.3).

Créer ensuite un service POP3 en TCP et port 110 (règle 3).

Créer une règle pour autoriser également ce service aux PC disposant d'un accès Internet.

- Règles spécifiques d'autorisation (règles 8 à 11)

Comme pour la règle 3, créer les services dont vous avez besoin et créer ensuite une règle d'autorisation pour les PC concernés.

Dans mon exemple de configuration :

- . BitTorrent en TCP et ports 6881 à 7881 pour le PC en 192.168.0.2
- . Gestion à distance en TCP et port 8080 pour autoriser le PC en 192.168.0.2 à gérer à distance par Internet l'interface de configuration d'un autre routeur
- . LivePass1 et LivePass2 en TCP et respectivement en port 554 et 1755 afin d'autoriser les PC en 192.168.0.2 et 192.168.0.3 à profiter du service LivePass (bouquet de chaînes de télévision) de Club-Internet

- Règle bloquante (règle 12)

Créer une règle bloquant (**BLOCK always**) tous les services (**Any(ALL)**) sur l'intégralité du réseau **Any**, aussi bien en **LAN** (réseau local) qu'en **WAN** (Internet).

- **Attention de bien respecter l'ordre des règles sortantes.**

Les règles d'autorisation doivent toujours être interprétées par le routeur avant la règle bloquante.

- Cette configuration vous procure une sécurité optimale, puisque vous autorisez uniquement les ports sortants nécessaires, tout le reste étant systématiquement bloqué.

Cette configuration est par contre beaucoup plus lourde à mettre en place.

A chaque nouvelle application spécifique (P2P, etc ...) vous devrez déterminer quels sont les ports à ouvrir et créer autant de nouveaux services et de nouvelles règles d'autorisation.

(voir page de configuration ci-après)

- . Sécurité
- . Règles Pare-feu
- . Services sortants

Règles Pare-feu

Services sortants

#	Activer	Nom du service	Action	Utilisateurs LAN	Serveurs WAN	Journal
1		DNS	ALLOW always	192.168.0.2-192.168.0.3	Any	Never
2		FTP	ALLOW always	192.168.0.2-192.168.0.3	Any	Never
3		POP3	ALLOW always	192.168.0.2-192.168.0.3	Any	Never
4		SMTP	ALLOW always	192.168.0.2-192.168.0.3	Any	Never
5		HTTP	ALLOW always	192.168.0.2-192.168.0.3	Any	Never
6		HTTPS	ALLOW always	192.168.0.2-192.168.0.3	Any	Never
7		NNTP	ALLOW always	192.168.0.2-192.168.0.3	Any	Never
8		BitTorrent	ALLOW always	192.168.0.2	Any	Never
9		Gestion à distance	ALLOW always	192.168.0.2	Any	Never
10		LivePass1	ALLOW always	192.168.0.2-192.168.0.3	Any	Never
11		LivePass2	ALLOW always	192.168.0.2-192.168.0.3	Any	Never
12		Any(ALL)	BLOCK always	Any	Any	Never
Par défaut	Oui	Indifférent	Toujours PERMETTRE	Indifférent	Indifférent	Jamais

Services entrants

#	Activer	Nom du service	Action	Adresse IP serveur LAN	Utilisateurs WAN	Journal
1		BiTorrent	ALLOW always	192.168.0.2	Any	Never
2		FTP	ALLOW always	192.168.0.2	Any	Never
Par défaut	Oui	Indifférent	Toujours BLOQUER	Indifférent	Indifférent	Jamais

Faire un compromis entre la sécurité et la souplesse de configuration

Cette approche plus simple à mettre en oeuvre consiste simplement à créer des services associés à autant de règles bloquantes sortantes, toutes correspondant au blocage de ports potentiellement dangereux (utilisés par des vers entre autres).



Comme exemple ici la configuration de notre spécialiste en pare-feu du Forum , **Dwarf** .
Services à créer :

NTP en UDP et port 123
Prts_NetBios en TCP/UDP et ports 135 à 139
Microsoft-DS en TCP/UDP et port 445
MyDoom_bkdr en TCP et ports 3127 à 3198
MyDoom_bkdr2 en TCP et port 6777
Socks en TCP et port 1080
SubSeven en TCP et port 1243
RingZero en TCP et port 3128
NetBus en UDP et port 12345
BioNet en TCP et port 12348
SubSeven_2 en TCP et port 27374
School_Bus en TCP et port 54321
Bagle_Bkdr en TCP et port 2745
Back_Orifice en UDP et port 31337
Korgo_bkdr en TCP et port 113
Korgo_bkdr2 en TCP et port 2041
Korgo_bkdr3 en TCP et port 3067
Sober.G en TCP et port 37
Sasser en TCP et port 5554
Netsky.Y en TCP et port 82
ms-sql-s/m en TCP/UDP et port 1433 à 1434

(voir page de configuration ci-après)

Règles Pare-feu

Services sortants

	#	Activer	Nom du service	Action	Utilisateurs LAN	Serveurs WAN	Journal
	1		NTP	BLOCK always	Any	Any	Match
	2		Prts_NetBios	BLOCK always	Any	Any	Match
	3		Microsoft-DS	BLOCK always	Any	Any	Match
	4		MyDoom_bkdr	BLOCK always	Any	Any	Match
	5		MyDoom_bkdr2	BLOCK always	Any	Any	Match
	6		Socks	BLOCK always	Any	Any	Match
	7		SubSeven	BLOCK always	Any	Any	Match
	8		RingZero	BLOCK always	Any	Any	Match
	9		NetBus	BLOCK always	Any	Any	Match
	10		BioNet	BLOCK always	Any	Any	Match
	11		SubSeven_2	BLOCK always	Any	Any	Match
	12		School_Bus	BLOCK always	Any	Any	Match
	13		Bagle_Bkdr	BLOCK always	Any	Any	Match
	14		Back_Orifice	BLOCK always	Any	Any	Match
	15		Korgo_bkdr	BLOCK always	Any	Any	Match
	16		Korgo_bkdr2	BLOCK always	Any	Any	Match
	17		Korgo_bkdr3	BLOCK always	Any	Any	Match
	18		Sober.G	BLOCK always	Any	Any	Match
	19		Sasser	BLOCK always	Any	Any	Match
	20		Netsky.Y	BLOCK always	Any	Any	Match
	21		ms-sql-s/m	BLOCK always	Any	Any	Match
	Par défaut	Oui	Indifférent	Toujours PERMETTRE	Indifférent	Indifférent	Jamais

Services entrants

	#	Activer	Nom du service	Action	Adresse IP serveur LAN	Utilisateurs WAN	Journal
	1		BiTorrent	ALLOW always	192.168.0.2	Any	Never
	2		FTP	ALLOW always	192.168.0.2	Any	Never
	Par défaut	Oui	Indifférent	Toujours BLOQUER	Indifférent	Indifférent	Jamais
