



Rapport d'audit

Analyse du 26/05/09 au 03/06/09

Rapport édité le 2 juillet 2009

CS One - 42 avenue Montaigne 75008 Paris
*Cabinet de consultants en architectures réseaux,
sécurité et téléphonie IP*

1 Introduction

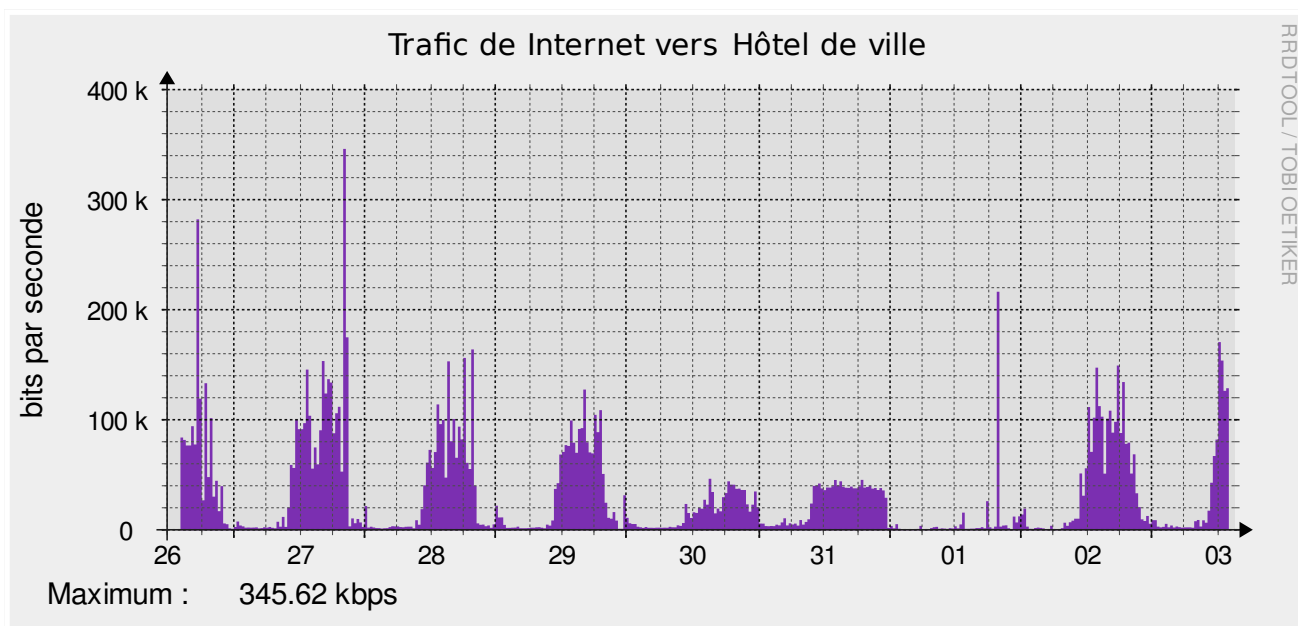
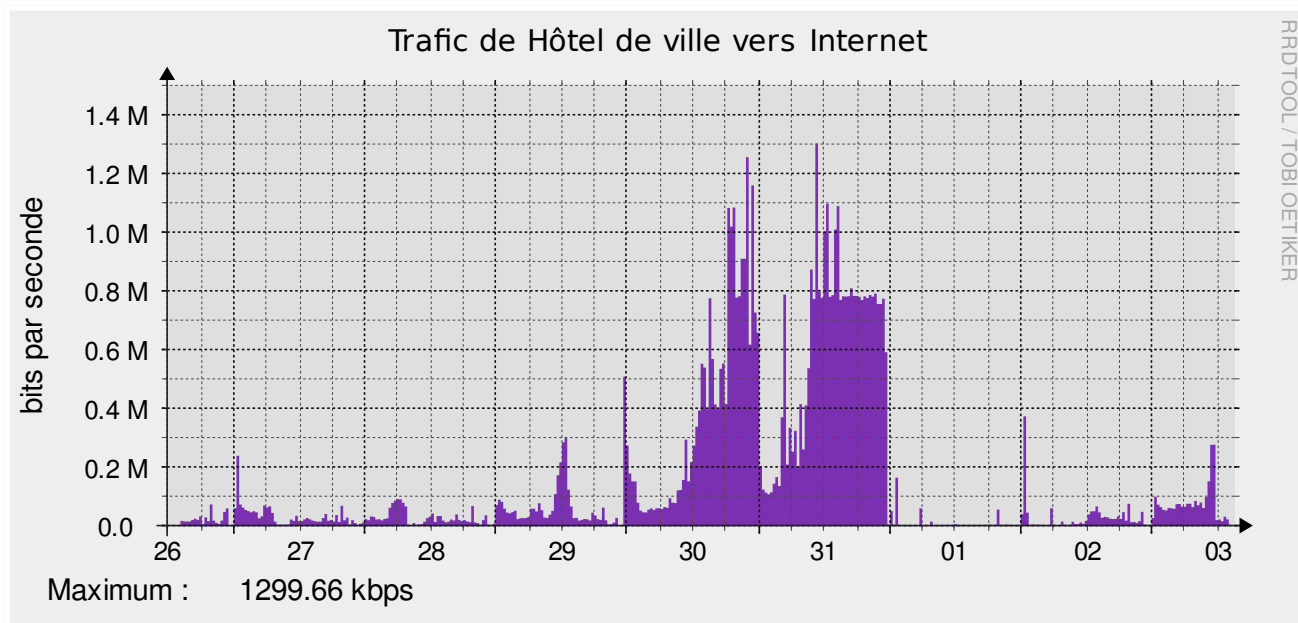
Ce document est un annexe au rapport d'audit.

CE DOCUMENT COMPORTE
INITIALEMENT 460 PAGES POUR
UN MILLIER DE GRAPHIQUES

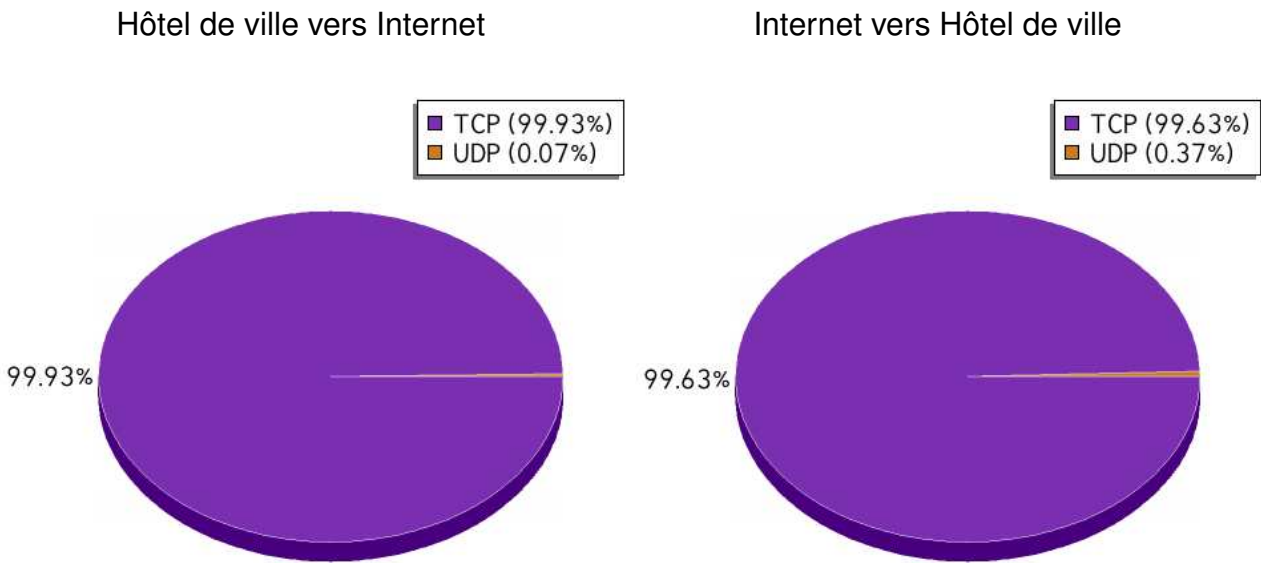
POUR DES RAISONS LEGISLATIVES,
IL A ETE ANONYMISE,
A ETE REDUIT A 22 PAGES,
ET LA TABLE DES MATIERES A ETE RETIREE

2 Entre Hôtel de ville et Internet

2.A Bande passante utilisée

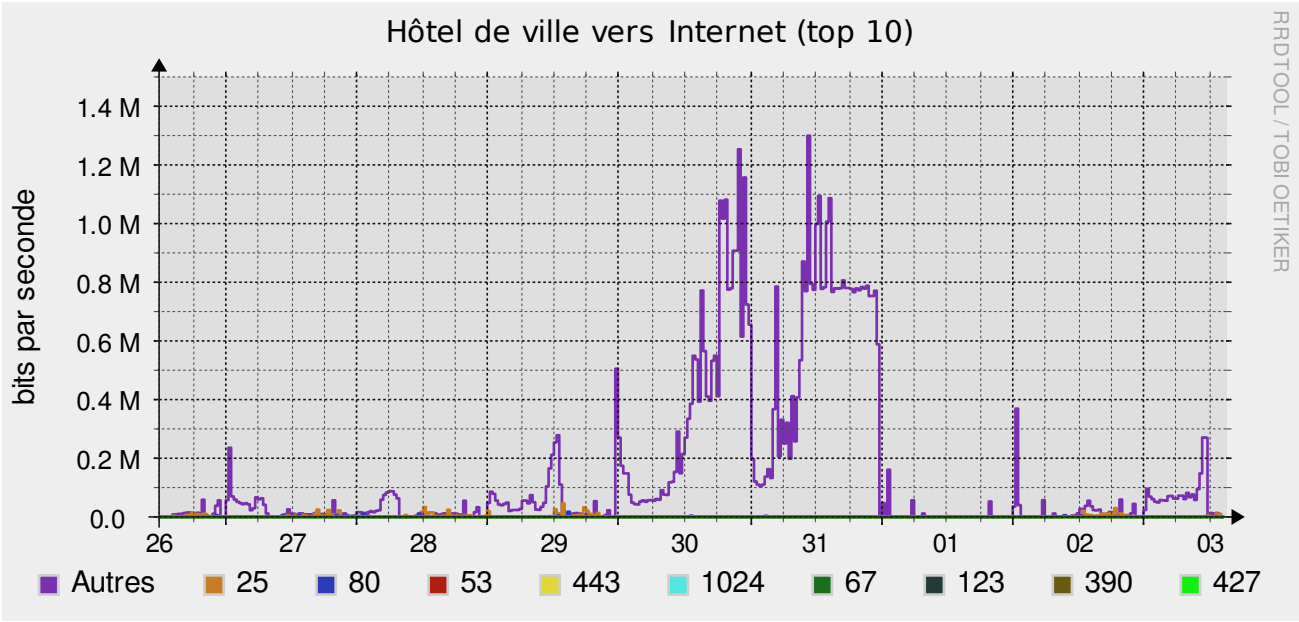


2.B Répartition TCP / UDP

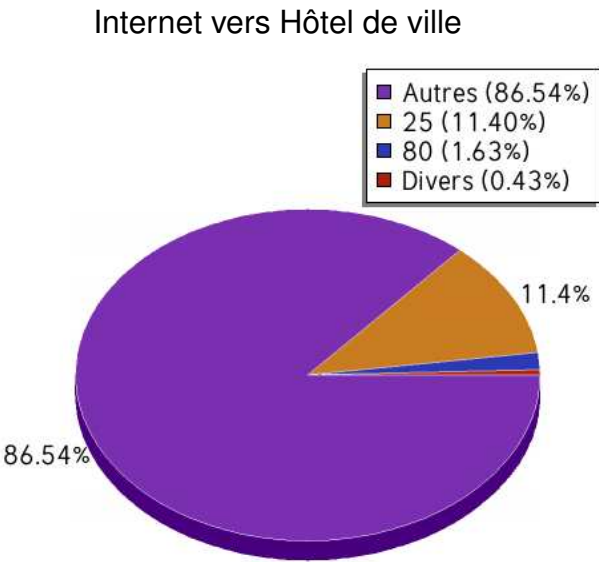
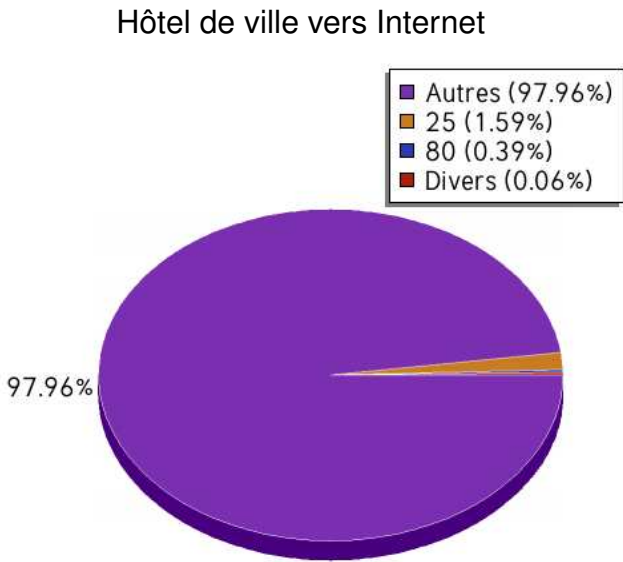
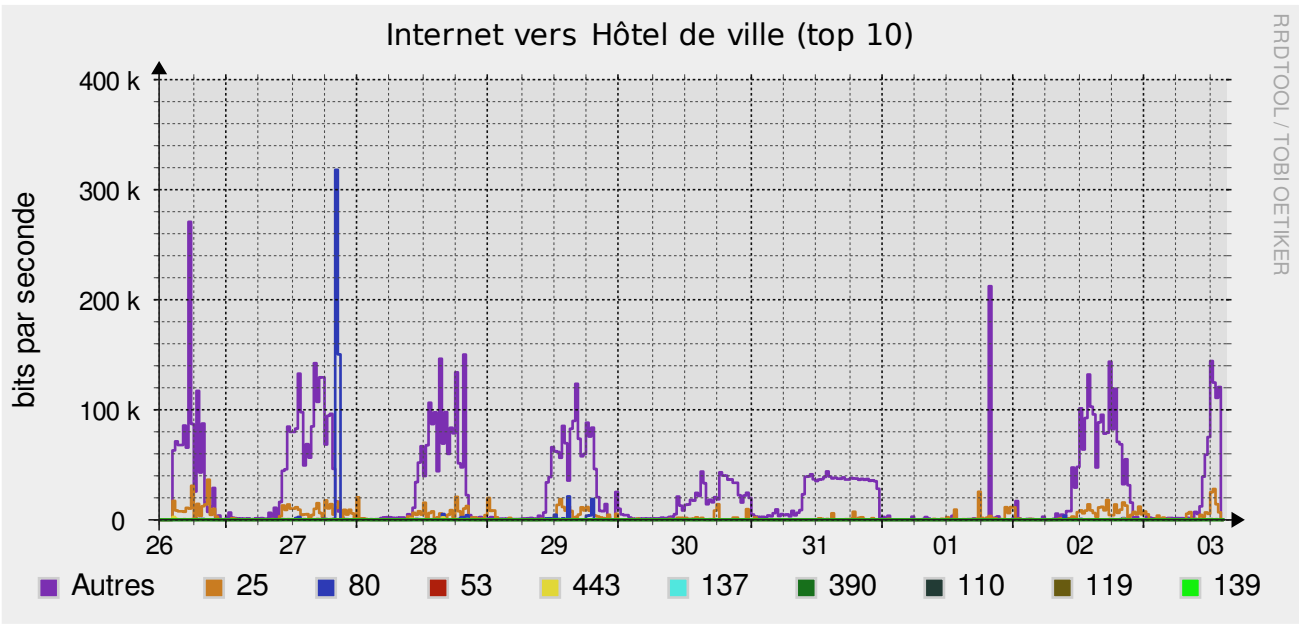


Prot.	Hôtel de ville vers Internet	Internet vers Hôtel de ville
	TCP	TCP
	11.91 Go	2.48 Go
UDP	8.28 Mo	9.54 Mo
Totaux	11.92 Go	2.49 Go

2.C Détails par port



2. ENTRE HÔTEL DE VILLE ET INTERNET



2. ENTRE HÔTEL DE VILLE ET INTERNET

App.	Hôtel de ville vers Internet		Internet vers Hôtel de ville	
	Autres			
		11.68 Go		2.15 Go
	25	194.14 Mo		290.55 Mo
	80	47.76 Mo		41.65 Mo
	53	6.79 Mo		9.84 Mo
	443	516.69 Ko		871.85 Ko
	1024	137.95 Ko		0
	67	113.80 Ko		0
	390	47.18 Ko		10.47 Ko
	123	55.86 Ko		492 octets
	137	4.44 Ko		19.33 Ko
	427	22.98 Ko		0
	162	14.09 Ko		0
	110	8.93 Ko		4.70 Ko
	42	4.60 Ko		0
	119	1.03 Ko		1.08 Ko
	843	1.41 Ko		480 octets
	21	1.16 Ko		480 octets
	139	294 octets		1.01 Ko
	554	744 octets		210 octets
	445	294 octets		225 octets
	161	182.5 octets		0
	402	76.5 octets		0
	Totaux	11.92 Go		2.49 Go

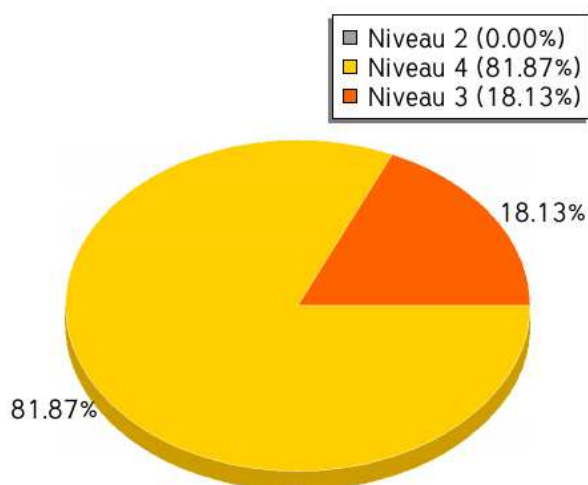
2.D Détails par IP

IP Hôtel de ville	Envoyé à Internet		Reçu de Internet	
	192.168.0.46	11.43 Go		407.28 Mo
	192.168.1.37	235.81 Mo		1.75 Go
	192.168.0.39	235.73 Mo		299.11 Mo
	192.168.0.204	2.94 Mo		32.93 Mo
	192.168.2.44	12.27 Mo		4.13 Mo
	192.168.1.30	3.43 Mo		5.92 Mo
	192.168.1.39	3.70 Mo		245.37 Ko
	192.168.1.31	1.33 Mo		1.90 Mo
	192.168.0.43	0		626.45 Ko
	192.168.0.25	697.05 Ko		0
	Totaux	11.92 Go		2.49 Go

IP Internet	Envoyé à Hôtel de ville		Reçu de Hôtel de ville	
	85.31.145.44	407.28 Mo		11.43 Go
	86.65.152.102	2.04 Go		434.68 Mo
	86.65.152.106	8.81 Mo		45.08 Mo
	156.56.247.193	18.35 Mo		0
	79.141.0.38	4.13 Mo		12.27 Mo
	217.160.7.50	3.83 Mo		0
	229.55.150.208	0		1.47 Mo
	88.191.250.132	1.19 Mo		0
	217.128.119.22	626.44 Ko		375.70 Ko
	217.167.194.69	0		695.65 Ko
	Totaux	2.48 Go		11.92 Go

2.E Analyse des sites internet critiques visités

Répartition des catégories de sites critiques visités



Tops 10 des catégories critiques par niveau d'alerte

Niveau 2	
Malware	15 octets

Niveau 3	
Filehosting	144.94 Ko
Audio-video	945 octets

Niveau 4	
Shopping	352.39 Ko
Cleaning	234.01 Ko
Blog	47.93 Ko
Webmail	22.80 Ko
Publicite	1.57 Ko

Tops 5 des noms de domaine par catégorie

Malware	
amenworld.com	15 octets

Filehosting	
onlinehome.fr	144.94 Ko

2. ENTRE HÔTEL DE VILLE ET INTERNET

	Audio-video
justin.tv	945 octets

	Blog
over-blog.com	47.93 Ko

	Shopping
fnac.com	347.71 Ko
ebay.com	4.35 Ko
shopping.com	336.125 octets

	Cleaning
microsoft.com	199.88 Ko
sourceforge.net	34.13 Ko

	Publicite
doubleclick.net	1.57 Ko

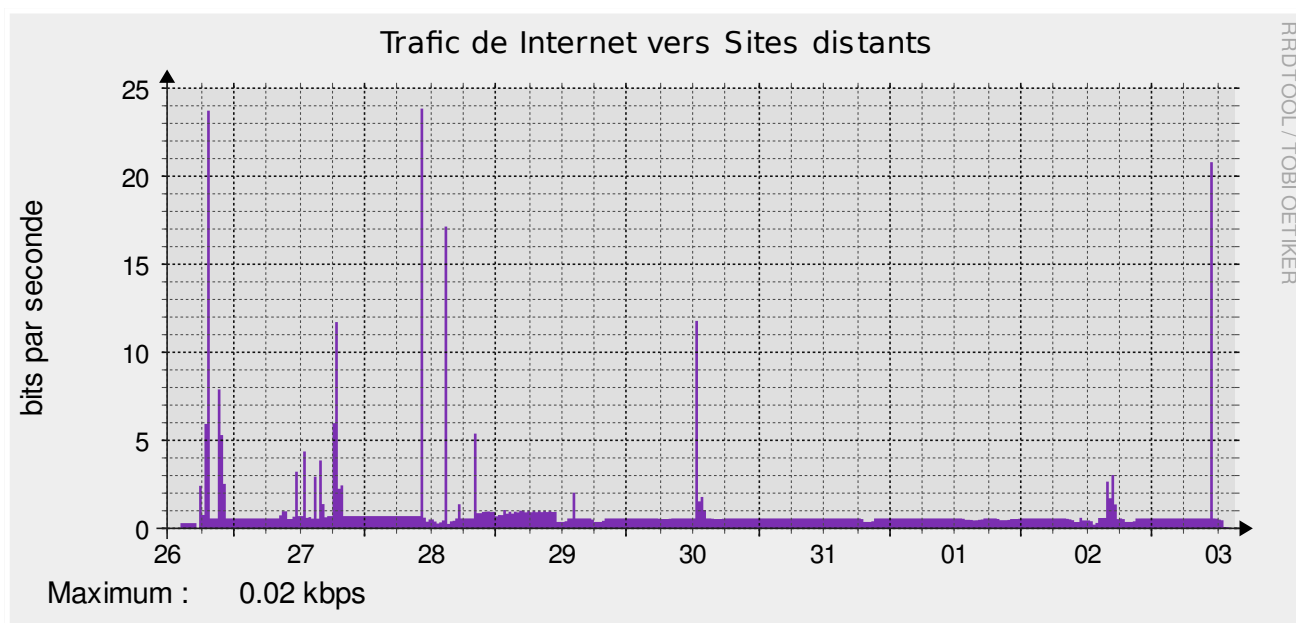
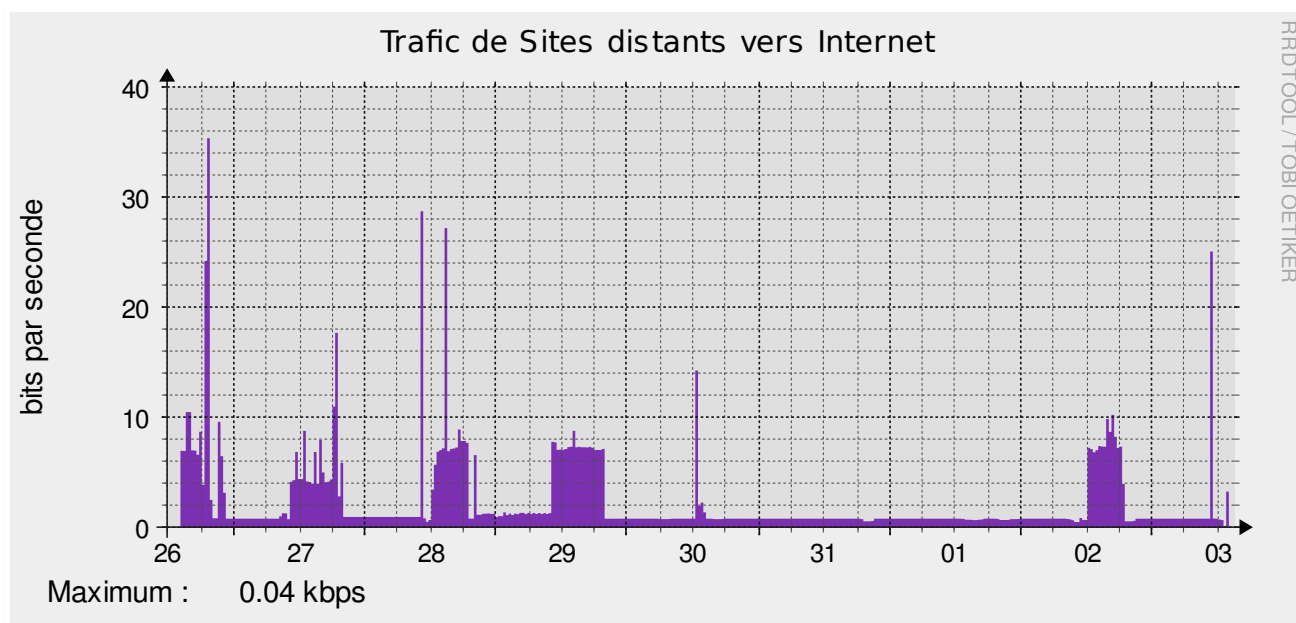
	Webmail
hotmail.com	22.80 Ko

Tops 20 des noms de domaine critiques visités

	Tous niveaux confondus
fnac.com	347.71 Ko
microsoft.com	199.88 Ko
onlinehome.fr	144.94 Ko
over-blog.com	47.93 Ko
sourceforge.net	34.13 Ko
hotmail.com	22.80 Ko
ebay.com	4.35 Ko
doubleclick.net	1.57 Ko
justin.tv	945 octets
shopping.com	336.125 octets
amenworld.com	15 octets

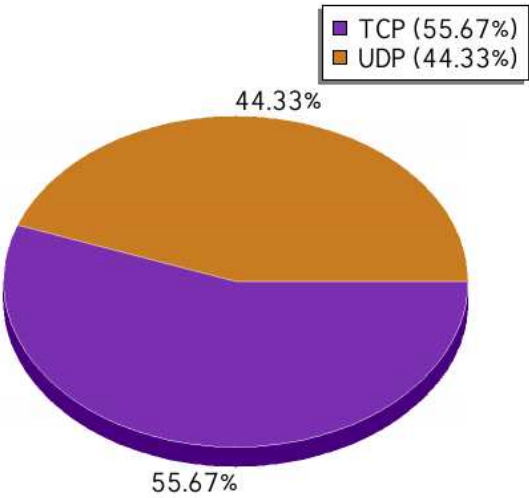
3 Entre Sites distants et Internet

3.A Bande passante utilisée

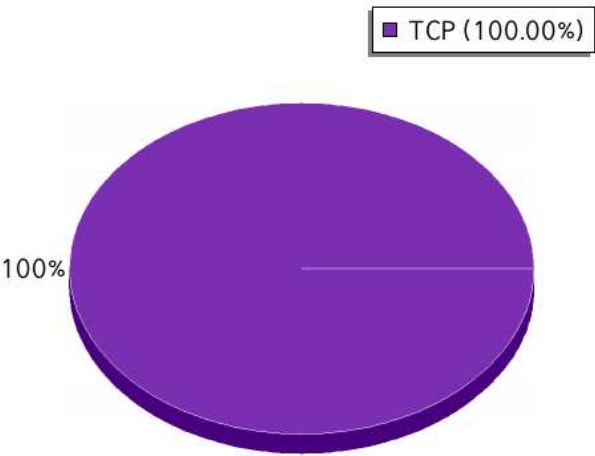


3.B Répartition TCP / UDP

Sites distants vers Internet

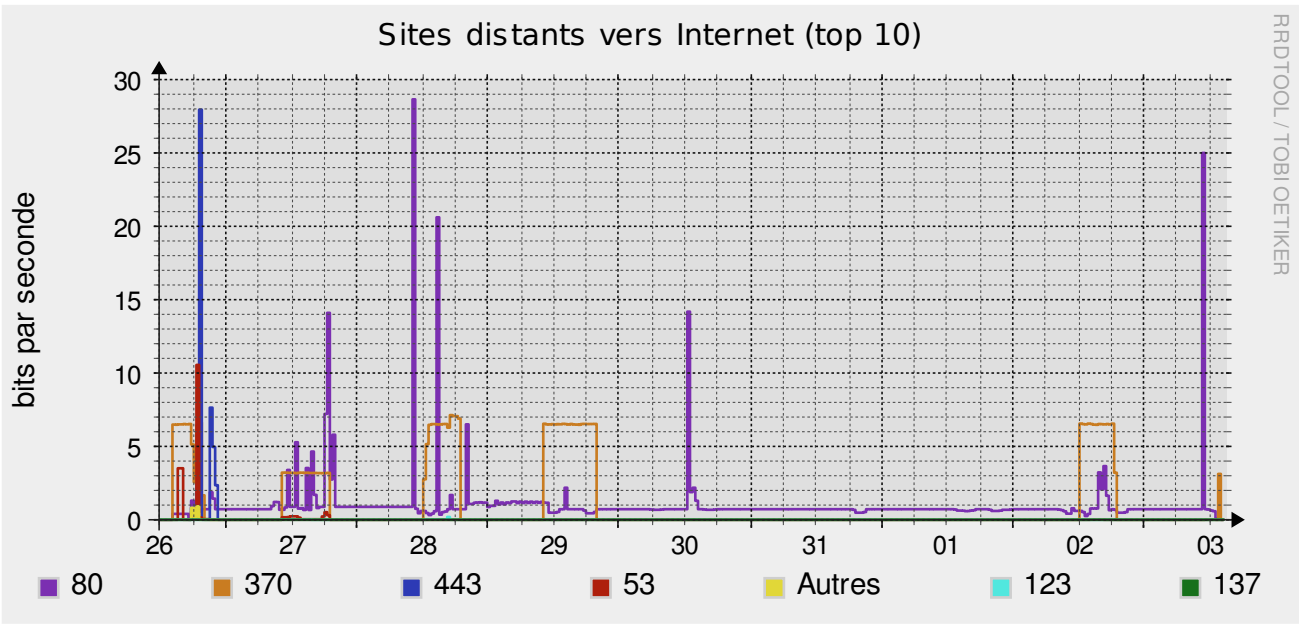


Internet vers Sites distants

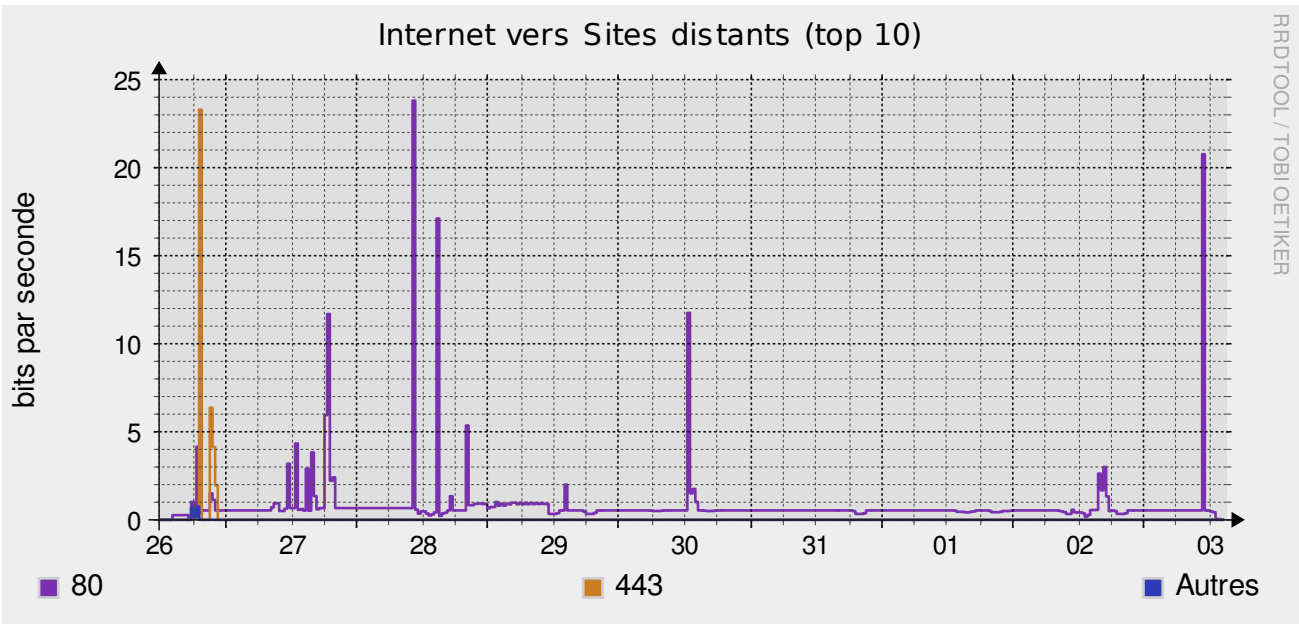


Prot.	Sites distants vers Internet		Internet vers Sites distants	
	TCP	UDP	TCP	UDP
TCP	121.03 Ko		368.49 Ko	
UDP	96.37 Ko		0	
Totaux	217.40 Ko		368.49 Ko	

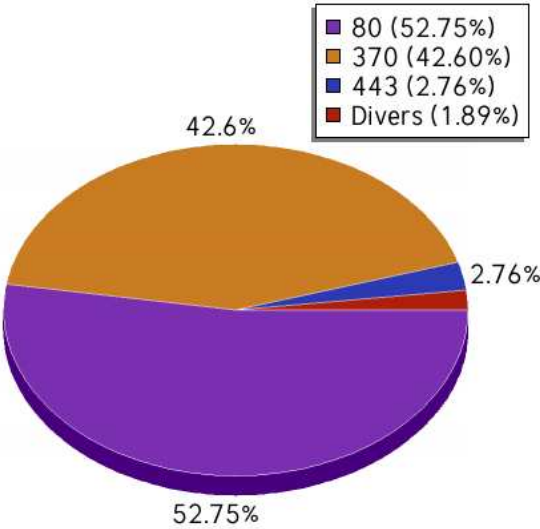
3.C Détails par port



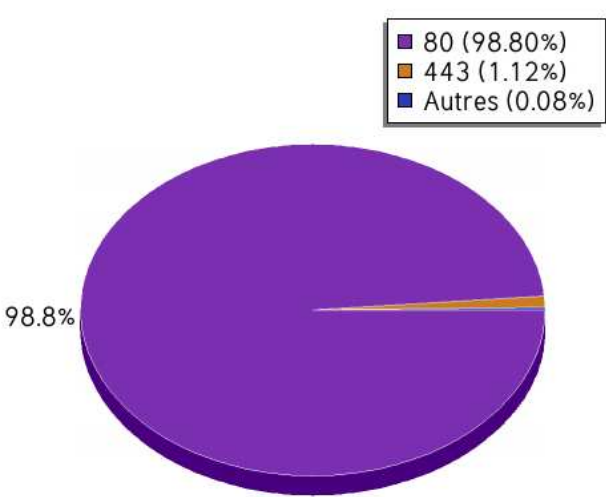
3. ENTRE SITES DISTANTS ET INTERNET



Sites distants vers Internet



Internet vers Sites distants



App.	Sites distants vers Internet		Internet vers Sites distants	
	80	114.68 Ko	80	364.06 Ko
	370	92.62 Ko	370	0
	443	6.00 Ko	443	4.14 Ko
	53	3.23 Ko	53	0
	Autres	604 octets	Autres	300 octets
	123	228 octets	123	0
	137	58.5 octets	137	0
Totaux		217.40 Ko	368.49 Ko	

3. ENTRE SITES DISTANTS ET INTERNET

3.D Détails par IP

IP Sites distants	Envoyé à Internet		Reçu de Internet	
	192.168.17.153	23.25 Ko	272.32 Ko	
	192.168.18.211	92.86 Ko	0	
	192.168.17.151	0	25.98 Ko	
	192.168.22.22	13.36 Ko	11.13 Ko	
	192.168.9.21	13.29 Ko	11.07 Ko	
	192.168.13.21	13.18 Ko	10.99 Ko	
	192.168.11.23	13.15 Ko	10.96 Ko	
	192.168.18.183	4.99 Ko	4.16 Ko	
	192.168.23.23	6.68 Ko	0	
	192.168.22.52	3.23 Ko	2.70 Ko	
Totaux		183.99 Ko	349.31 Ko	

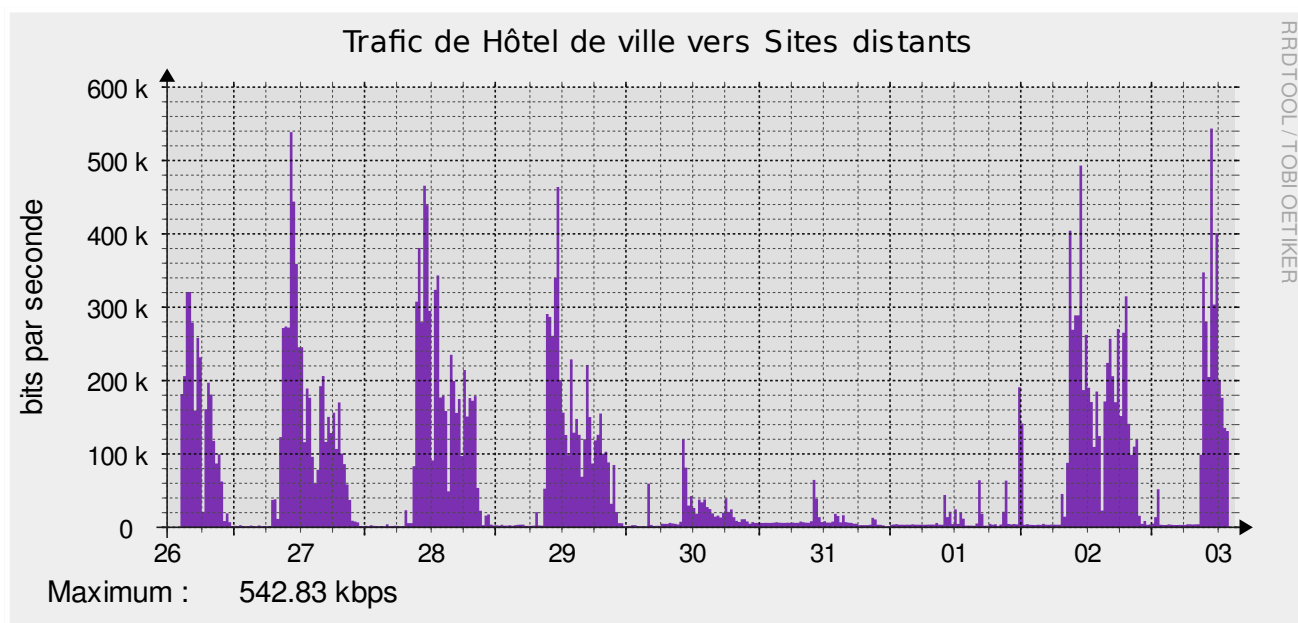
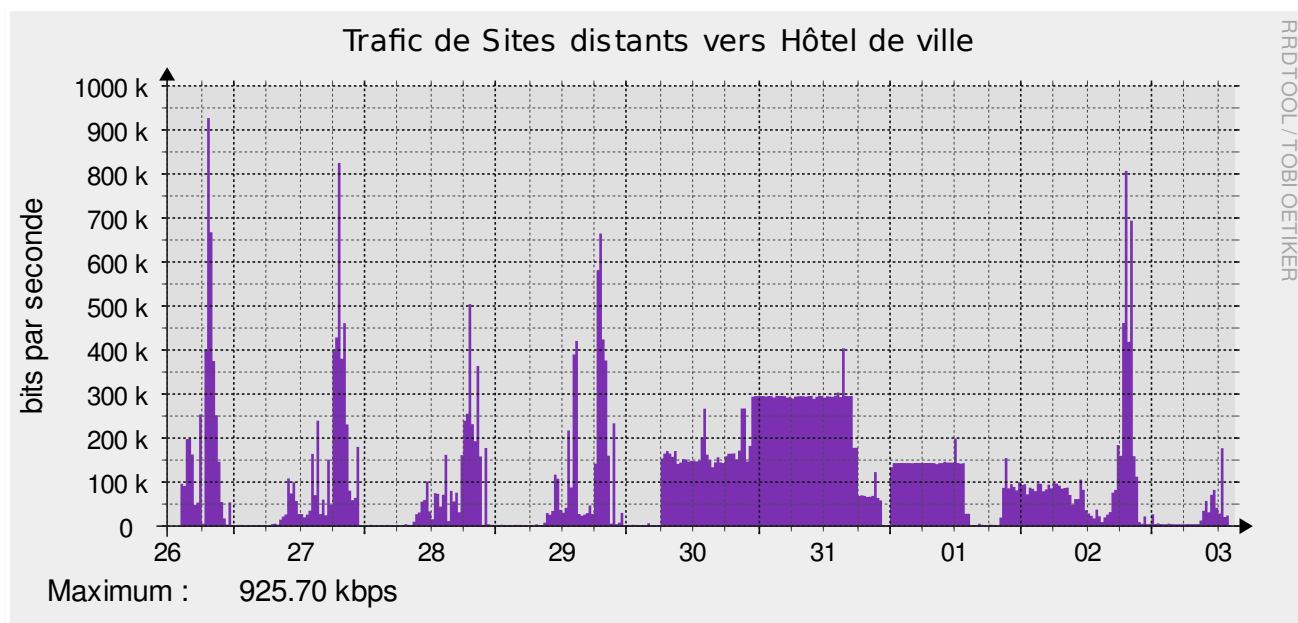
IP Internet	Envoyé à Sites distants		Reçu de Sites distants	
	86.64.17.194	298.30 Ko	25.49 Ko	
	193.51.224.8	21.23 Ko	31.88 Ko	
	193.51.224.14	19.61 Ko	23.54 Ko	
	63.251.254.132	0	26.74 Ko	
	63.251.254.138	0	25.06 Ko	
	63.251.254.133	0	20.87 Ko	
	63.251.254.131	0	19.96 Ko	
	192.18.197.109	5.24 Ko	6.29 Ko	
	213.199.167.251	2.40 Ko	2.88 Ko	
	59.151.130.250	1.52 Ko	0	
Totaux		348.31 Ko	182.71 Ko	

3.E Analyse des sites internet critiques visités

Aucune donnée

4 Entre Sites distants et Hôtel de ville

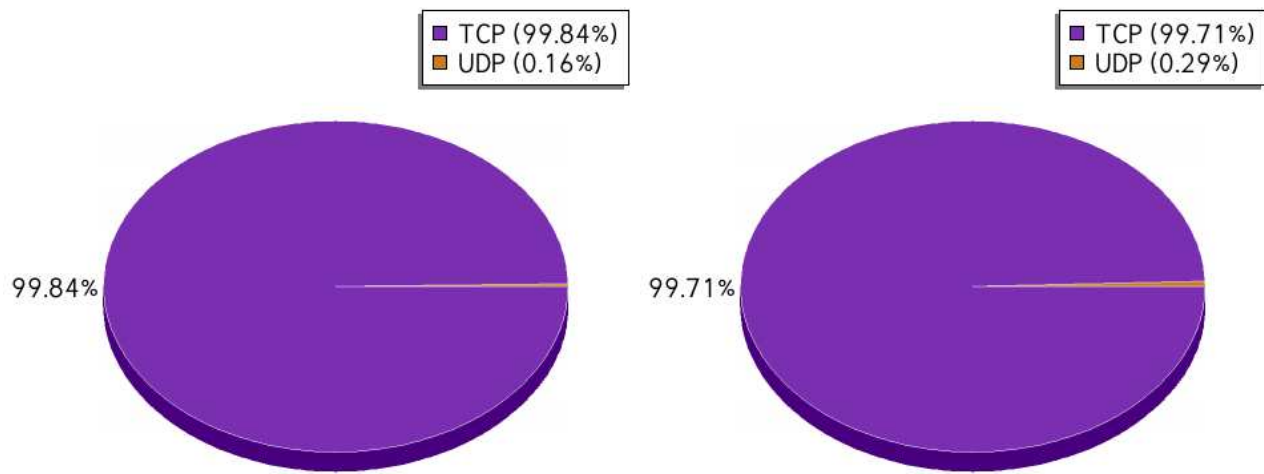
4.A Bande passante utilisée



4.B Répartition TCP / UDP

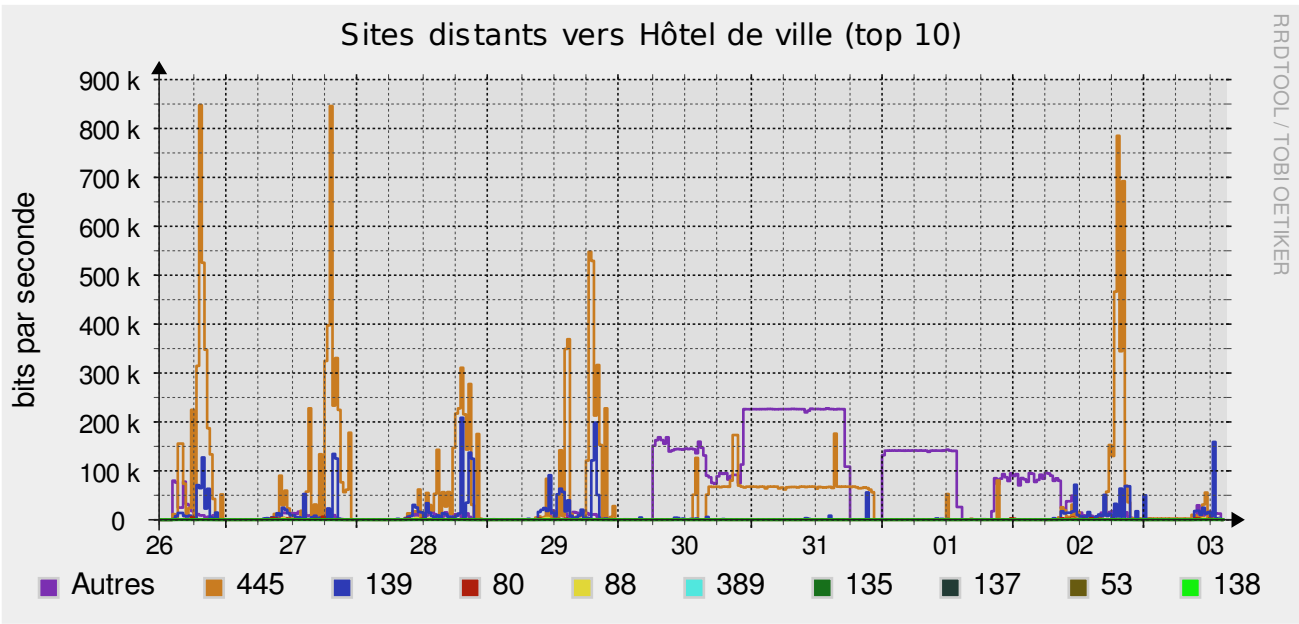
Sites distants vers Hôtel de ville

Hôtel de ville vers Sites distants

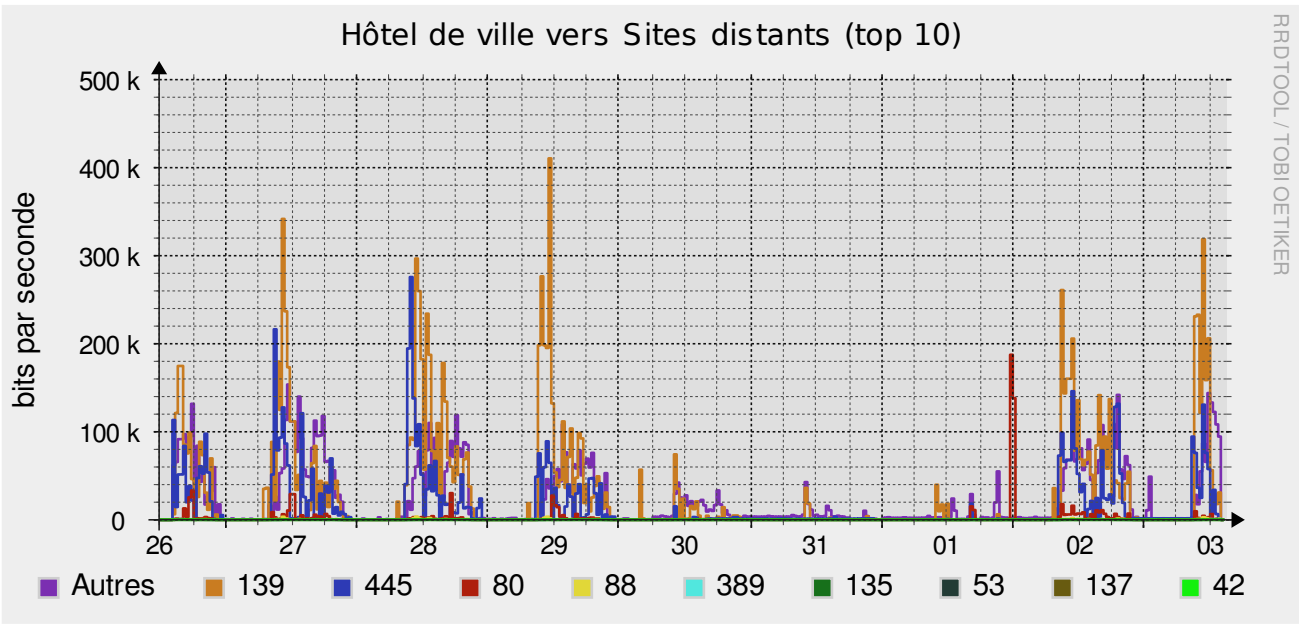


Prot.	Sites distants vers Hôtel de ville		Hôtel de ville vers Sites distants	
	TCP	6.01 Go	UDP	3.86 Go
Totaux	UDP	10.11 Mo	Totaux	11.36 Mo
	Totaux	6.02 Go	Totaux	3.87 Go

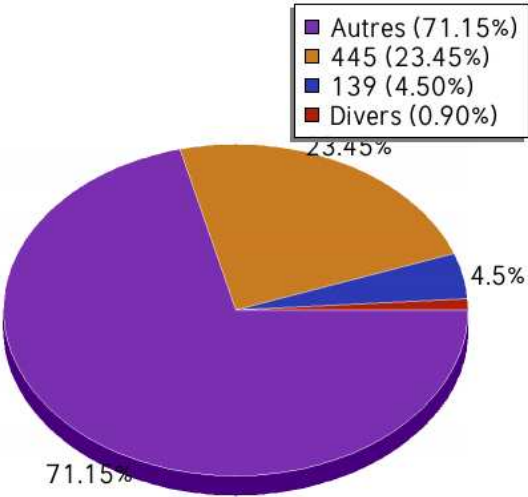
4.C Détails par port



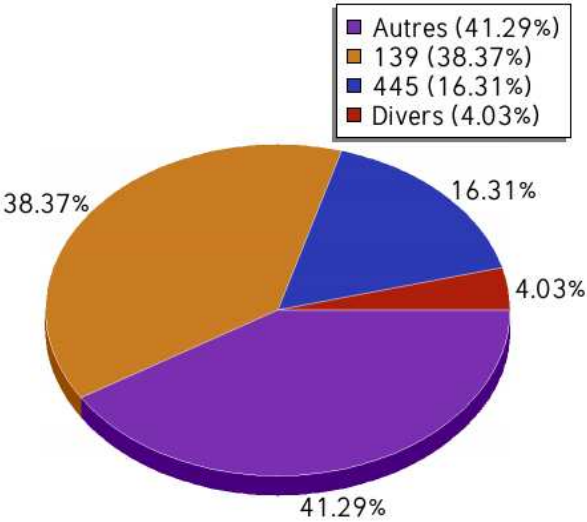
4. ENTRE SITES DISTANTS ET HÔTEL DE VILLE



Sites distants vers Hôtel de ville



Hôtel de ville vers Sites distants



4. ENTRE SITES DISTANTS ET HÔTEL DE VILLE

		Sites distants vers Hôtel de ville	Hôtel de ville vers Sites distants
App.	Autres	4.29 Go	1.60 Go
	445	1.41 Go	647.02 Mo
	139	277.69 Mo	1.49 Go
	80	22.57 Mo	124.44 Mo
	88	13.68 Mo	13.61 Mo
	389	10.84 Mo	12.86 Mo
	135	3.04 Mo	3.04 Mo
	53	1.62 Mo	2.95 Mo
	137	2.48 Mo	1.68 Mo
	42	74.40 Ko	667.11 Ko
	138	335.14 Ko	13.83 Ko
	123	172.23 Ko	172.38 Ko
	161	92.82 Ko	143.26 Ko
	21	74.64 Ko	94.65 Ko
	1024	64.98 Ko	52.05 Ko
	25	91.45 Ko	12.36 Ko
	8080	76.82 Ko	10.15 Ko
	20	60.64 Ko	8.47 Ko
	0	0	2.04 Ko
	47	0	562.5 octets
	278	0	187.5 octets
	34	0	187.5 octets
	16	12 octets	0
Totaux		6.02 Go	3.87 Go

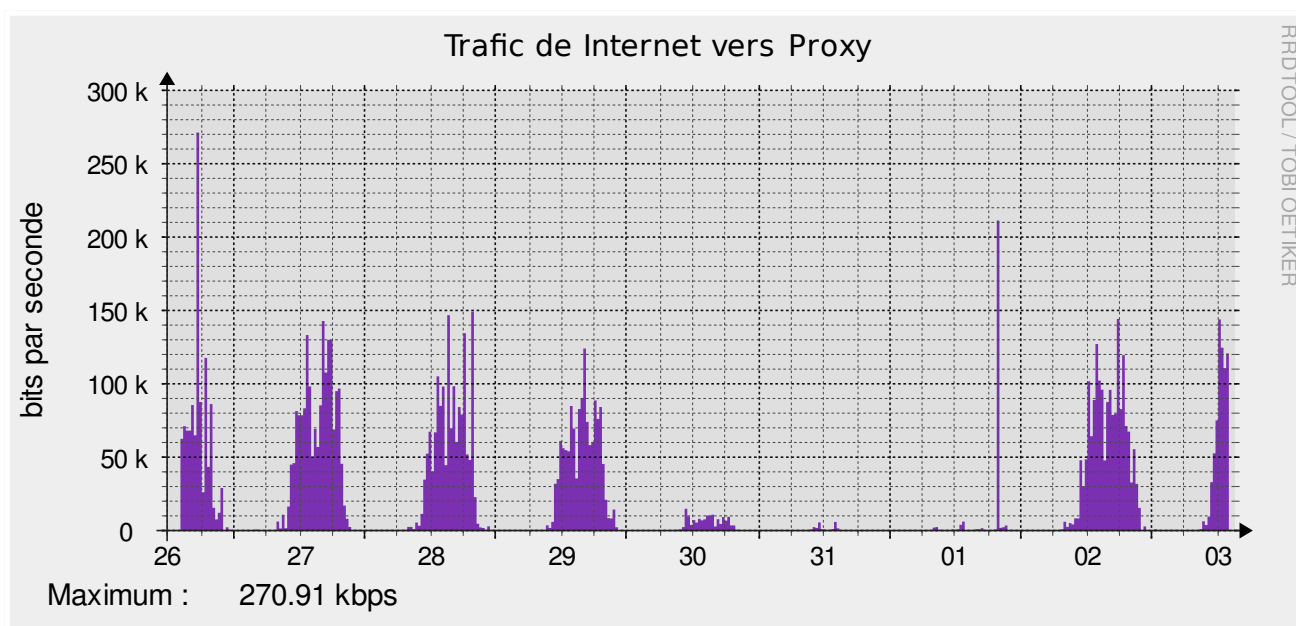
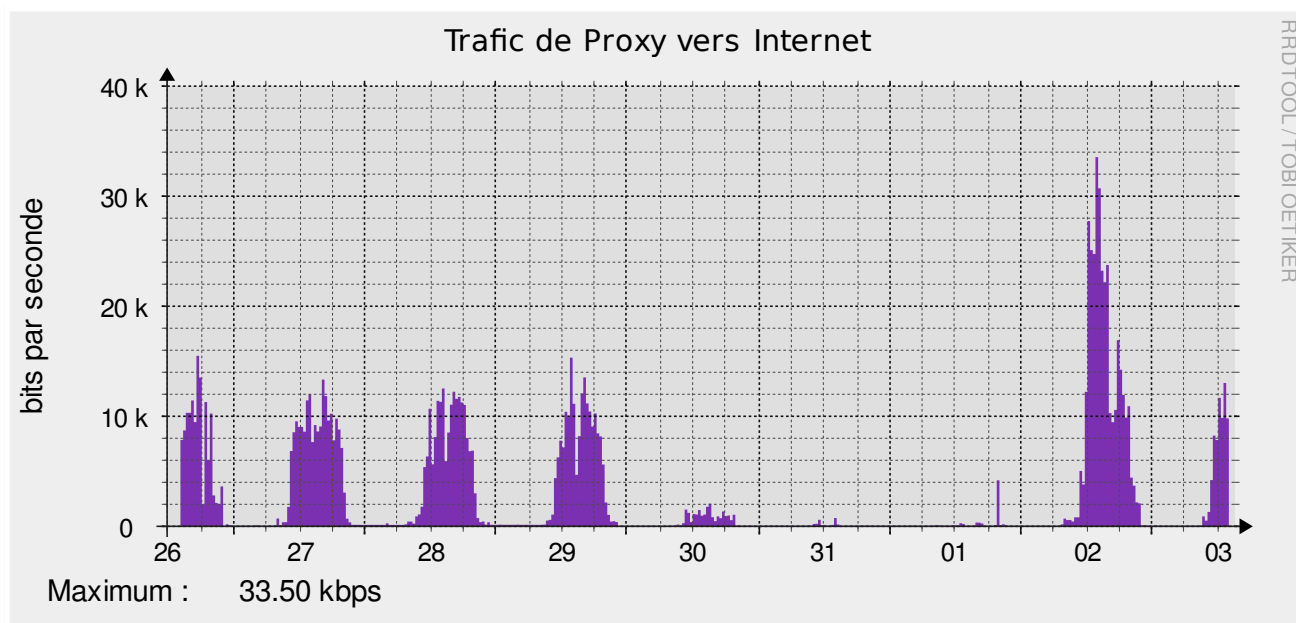
4.D Détails par IP

		Envoyé à Hôtel de ville	Reçu de Hôtel de ville
IP Sites distants	192.168.22.27	1.84 Go	0
	192.168.9.23	924.68 Mo	0
	192.168.15.21	857.83 Mo	0
	192.168.13.22	851.90 Mo	0
	192.168.23.22	254.55 Mo	0
	192.168.11.22	206.16 Mo	0
	192.168.13.121	35.82 Mo	132.28 Mo
	192.168.13.165	0	86.97 Mo
	192.168.22.48	30.21 Mo	79.99 Mo
	192.168.12.125	0	55.23 Mo
	Totaux	4.92 Go	354.47 Mo

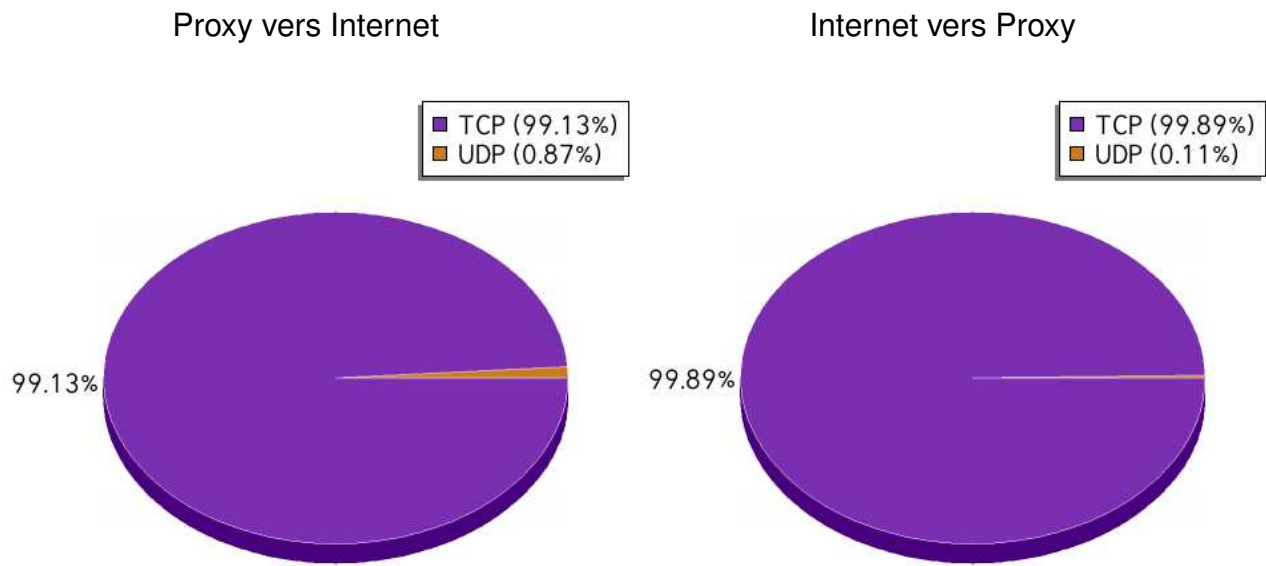
		Envoyé à Sites distants	Reçu de Sites distants
IP Hôtel de ville	192.168.1.40	89.23 Mo	4.85 Go
	192.168.0.24	1.97 Go	186.02 Mo
	192.168.1.37	935.64 Mo	127.88 Mo
	192.168.1.28	33.62 Mo	577.10 Mo
	192.168.0.39	337.32 Mo	67.49 Mo
	192.168.1.45	226.97 Mo	25.13 Mo
	192.168.1.22	82.53 Mo	31.07 Mo
	192.168.1.30	57.83 Mo	47.55 Mo
	192.168.0.36	64.22 Mo	0
	192.168.1.31	23.85 Mo	26.79 Mo
	Totaux	3.78 Go	5.91 Go

5 Entre Proxy et Internet

5.A Bande passante utilisée

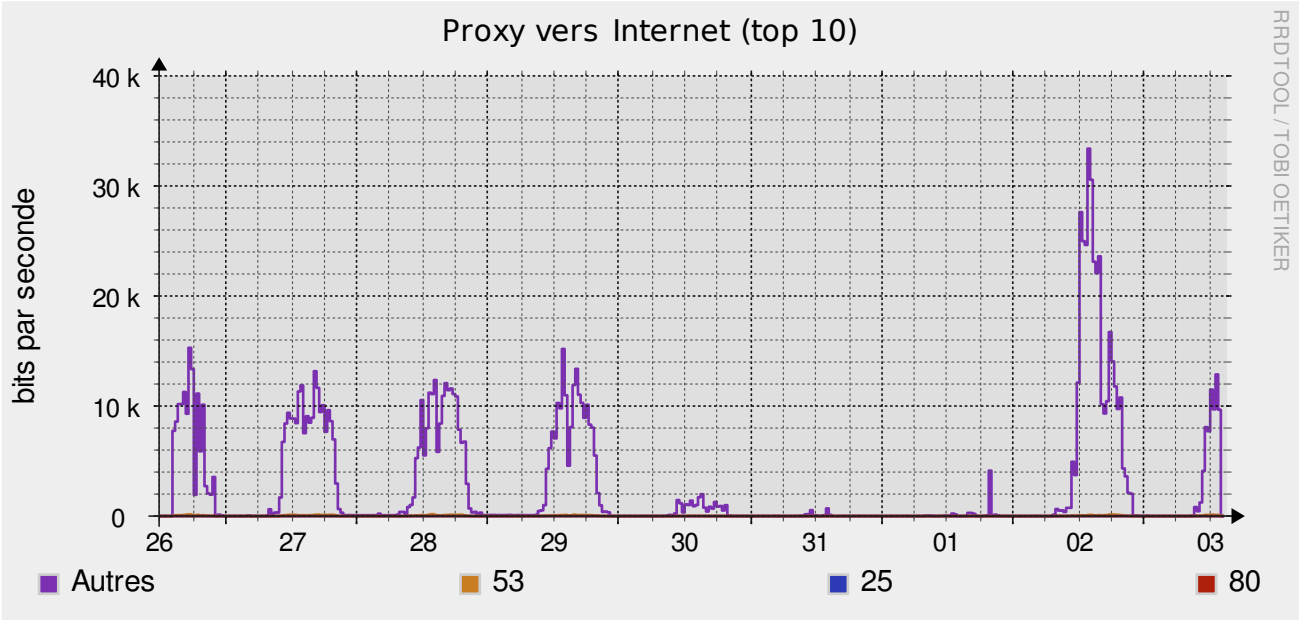


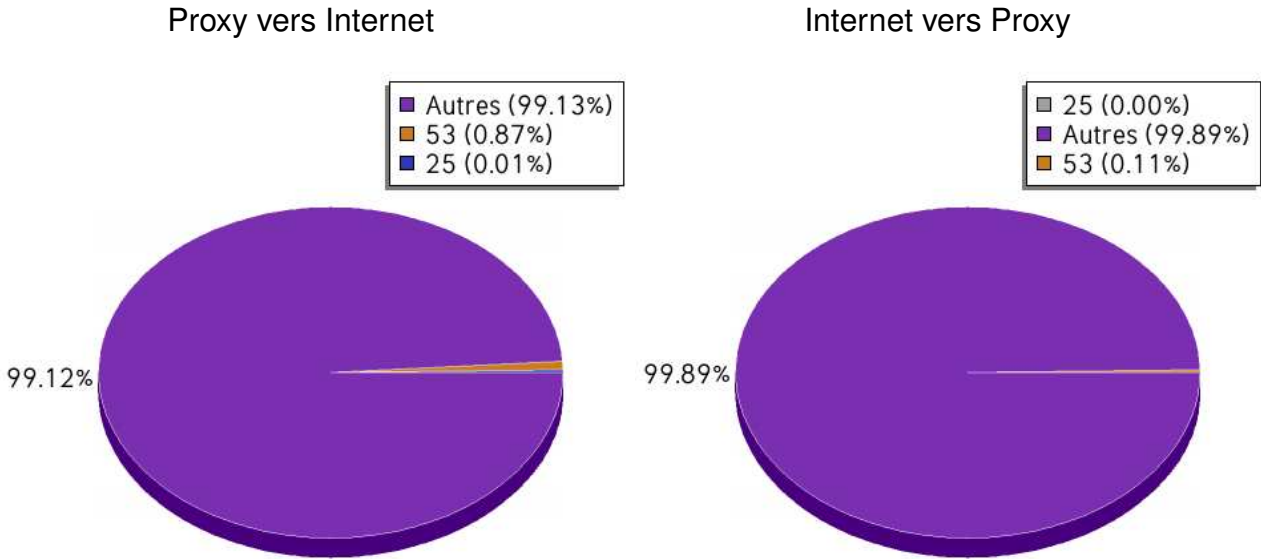
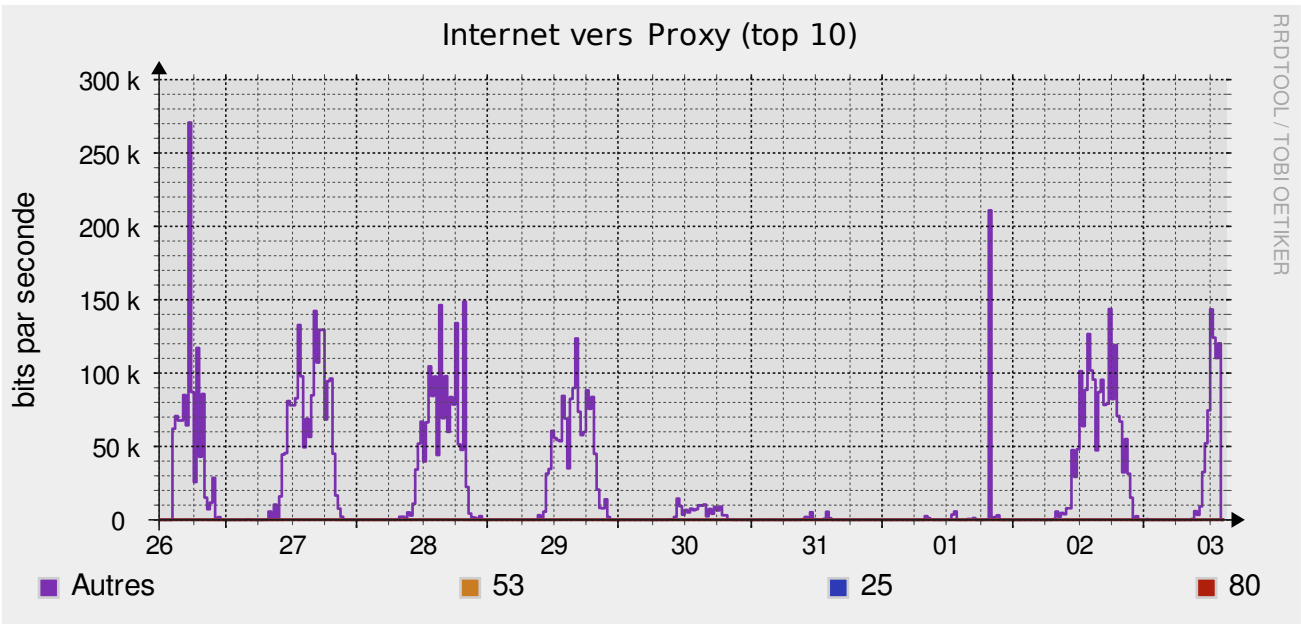
5.B Répartition TCP / UDP



Prot.	Proxy vers Internet		Internet vers Proxy	
	TCP	UDP	TCP	UDP
TCP	233.77 Mo		1.75 Go	
UDP	2.04 Mo		2.01 Mo	
Totaux	235.81 Mo		1.75 Go	

5.C Détails par port





App.	Proxy vers Internet		Internet vers Proxy	
	Autres	233.75 Mo	Autres	1.75 Go
	53	2.04 Mo	53	2.01 Mo
	25	19.75 Ko	25	3.77 Ko
	80	22.5 octets	80	5 octets
	Totaux	235.81 Mo	Totaux	1.75 Go

5.D Détails par IP

IP Proxy	Envoyé à Internet		Reçu de Internet	
	192.168.1.37	235.81 Mo	192.168.1.37	1.75 Go
	Totaux	235.81 Mo	Totaux	1.75 Go

IP Internet

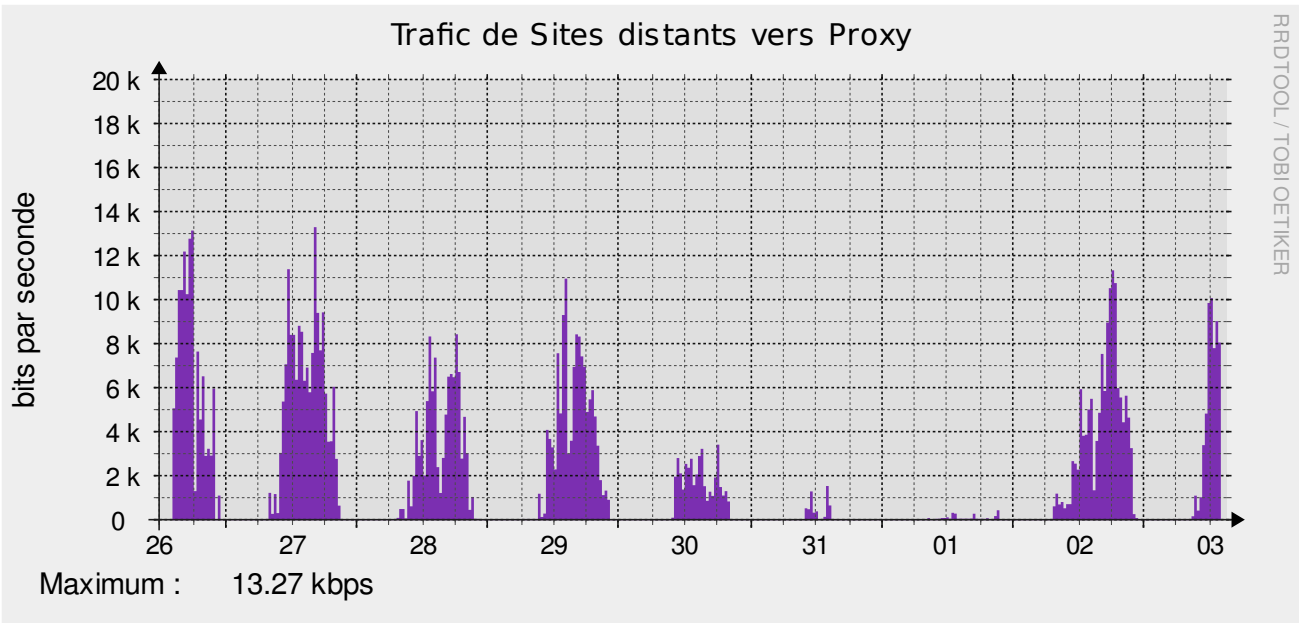
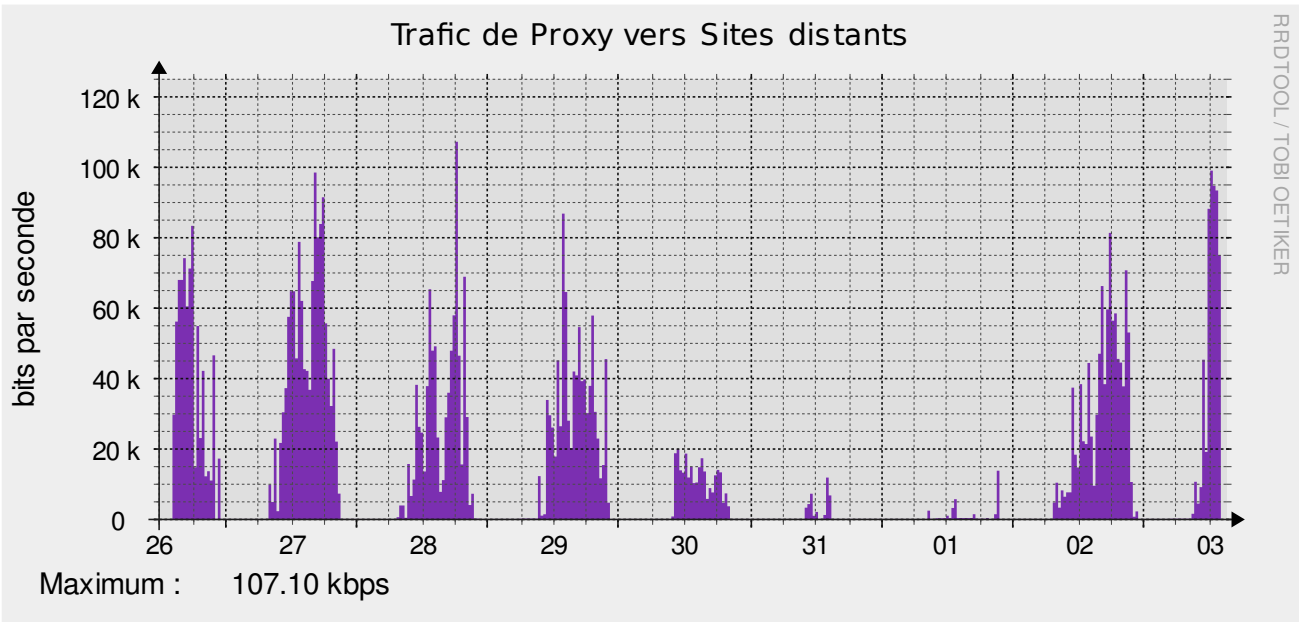
	Envoyé à Proxy	Reçu de Proxy
86.65.152.102	1.75 Go	235.81 Mo
69.16.137.252	5 octets	22.5 octets
Totaux	1.75 Go	235.81 Mo

5.E Analyse des sites internet critiques visités

Aucune donnée

6 Entre Proxy et Sites distants

6.A Bande passante utilisée

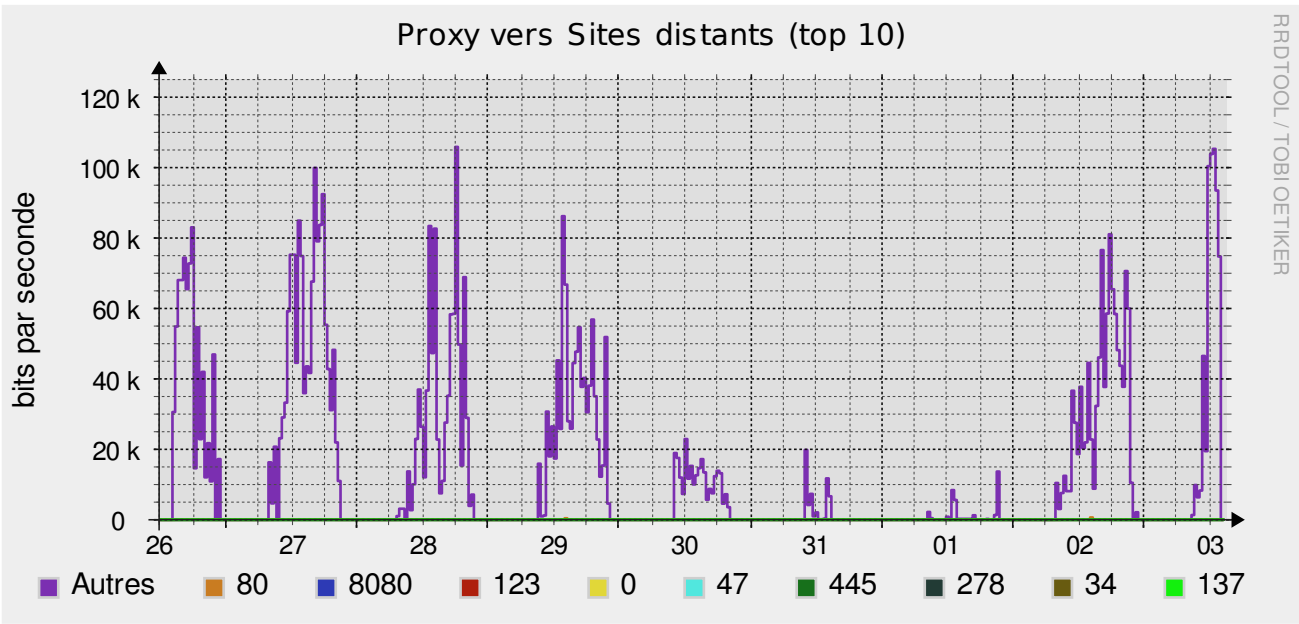


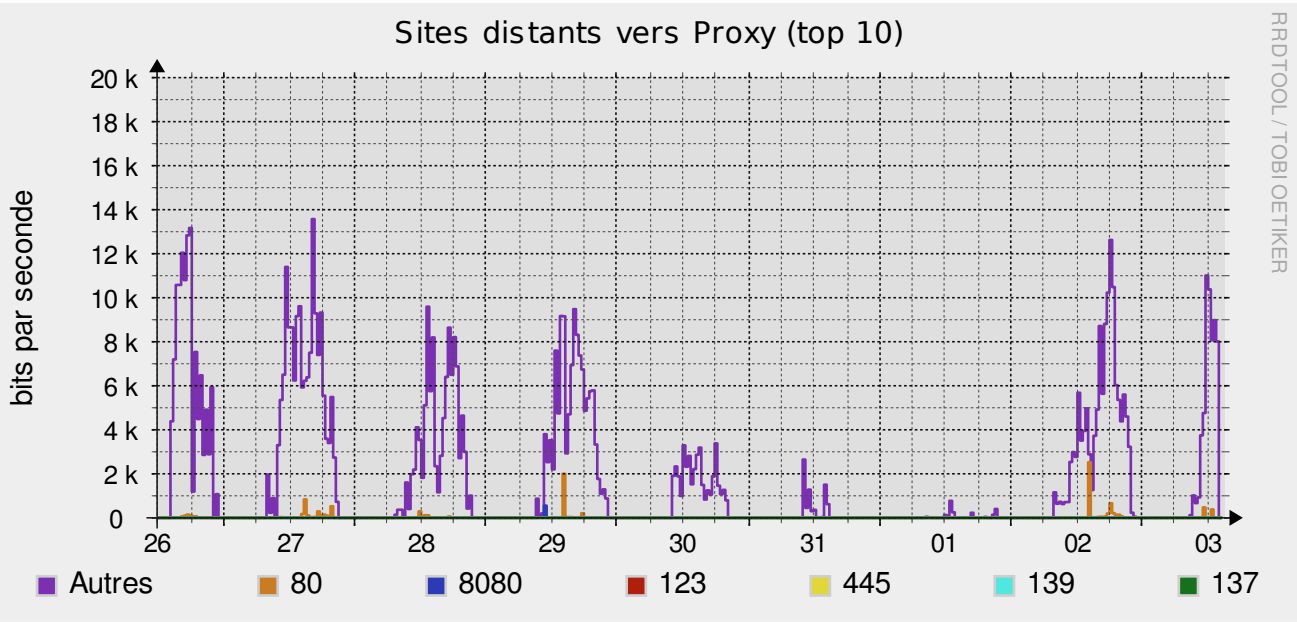
6.B Répartition TCP / UDP



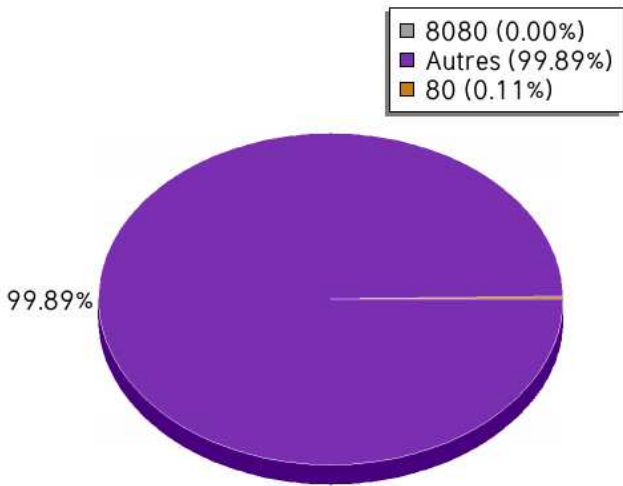
Prot.	Proxy vers Sites distants	Sites distants vers Proxy
	TCP 935.63 Mo	127.88 Mo
UDP	6.26 Ko	6.22 Ko
Totaux	935.64 Mo	127.88 Mo

6.C Détails par port

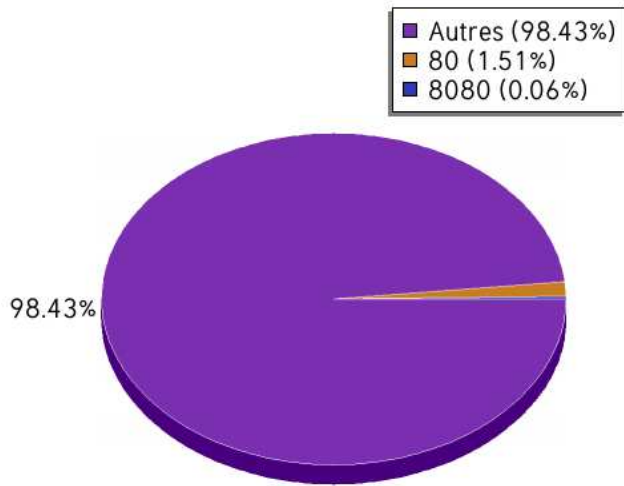




Proxy vers Sites distants



Sites distants vers Proxy



App.	Proxy vers Sites distants		Sites distants vers Proxy	
	Autres	934.62 Mo	Autres	125.87 Mo
	80	1022.38 Ko	80	1.93 Mo
	8080	10.15 Ko	8080	76.82 Ko
	123	6.20 Ko	123	6.20 Ko
	0	1.03 Ko	0	0
	47	562.5 octets	47	0
	445	208.75 octets	445	262.25 octets
	278	187.5 octets	278	0
	34	187.5 octets	34	0
	137	64.25 octets	137	19.5 octets
	139	27.5 octets	139	50 octets
	Totaux	935.64 Mo	Totaux	127.88 Mo