

R401

TP N°1 :

METTRE EN ŒUVRE UN RÉSEAU SEGMENTÉ SIMPLE WAN-LAN-DMZ

<u>Module : R401</u>	
Équipe : 6 GRONDIN Angélique (Alternante) HONORINE Kylian GRONDIN Benjamin (Alternant)	Version : 1 Date du document : 07/03/2025

Sommaire

R401.....	1
TP N°1 :	1
METTRE EN ŒUVRE UN RÉSEAU SEGMENTÉ SIMPLE WAN-LAN-DMZ.....	1
Sommaire.....	2
1. Introduction.....	3
1.1 Contexte.....	3
2. Architecture détaillée.....	4
2.1 Principe de déploiement.....	4
2.2 Architecture physique.....	4
2.3 Architecture logique.....	5
2.5 Configuration des équipements Pare-feu.....	5
4. Matrice de flux des pare-feu.....	6
Configuration STORMSHIELD.....	6
Configuration general.....	6
Configuration DHCP.....	7
Configuration interface.....	7
Configuration Apache2.....	8
Filtrage NAT.....	8
Objet Machine / Réseaux.....	9
TP2.....	10
Pre-Tâche 1 : Installer un serveur Web Apache.....	10
Tâche 1 : Accéder au serveur Web depuis le LAN.....	10
Tâche 2 : Finaliser l'accès au serveur web avec NAT de masquage.....	11
Tâche 2 : Publier le serveur Web via routage statique.....	12
Tâche 3 : Publier le serveur Web via NAT (masquage).....	13
TP3.....	15
Tâche 1 : Finaliser l'accès au serveur web avec NAT de masquage.....	15
Tâche 2 : Configurer l'accès DNS.....	16
Tâche 3 : Configurer l'accès Internet du LAN.....	17
5. Tests et validation.....	18
Conclusion.....	18

1. Introduction

1.1 Contexte

Le réseau informatique est au cœur de toute infrastructure informatique moderne. Il est essentiel de segmenter ce réseau afin d'améliorer la sécurité et l'efficacité des communications. Dans ce TP, nous mettrons en place un réseau comportant trois segments :

- **WAN (Wide Area Network)** : Accès à Internet. Cette zone est connectée au réseau externe et constitue l'entrée et la sortie du trafic.
- **LAN (Local Area Network)** : Réseau interne sécurisé utilisé pour les communications entre utilisateurs et serveurs internes.
- **DMZ (Demilitarized Zone)** : Zone intermédiaire où sont placés les serveurs accessibles depuis l'extérieur, tout en limitant l'accès direct aux ressources internes.

L'objectif de cette segmentation est de contrôler le trafic entre ces différentes zones en utilisant des règles de pare-feu adaptées.

Les actions entreprises dans ce TP sont :

- **Configurer un commutateur Cisco avec des VLANs** : La segmentation par VLAN permet d'isoler logiquement les différentes zones du réseau pour renforcer la sécurité et éviter toute communication indésirable entre elles.
- **Mettre en place un pare-feu Stormshield** : Celui-ci servira à filtrer et contrôler le trafic entre le LAN, la DMZ et l'Internet pour empêcher les connexions non autorisées et surveiller les communications.
- **Configurer un serveur DHCP** : L'objectif est de faciliter l'attribution d'adresses IP aux machines du réseau interne (LAN) sans nécessiter de configuration manuelle.
- **Paramétrer une route par défaut** : Cette configuration est essentielle pour permettre aux équipements du LAN et de la DMZ d'accéder à l'Internet via le pare-feu.
- **Appliquer des règles de filtrage** : Elles sont indispensables pour restreindre les accès entre les zones et éviter qu'un attaquant puisse compromettre l'ensemble du réseau.

2. Architecture détaillée

2.1 Principe de déploiement

L'architecture mise en place repose sur un réseau segmenté permettant un contrôle précis du trafic entre les différentes zones. Le pare-feu Stormshield est utilisé comme élément central de la sécurité pour appliquer des règles de filtrage strictes et empêcher les communications non autorisées entre les réseaux.

2.2 Architecture physique

Le schéma physique suivant illustre la connexion entre les équipements :

Équipement	Port Source	Port Destination	Justification
Pare-feu	Port 1 (WAN)	Internet(RT)	Connexion à Internet pour l'accès externe
Pare-feu	Port 2 (LAN)	Switch Gio/1	Communication avec le réseau interne sécurisé
Pare-feu	Port 3 (DMZ)	Switch Gio/6	Hébergement des services accessibles publiquement
PC LAN	NIC	Switch Gio/2	Poste utilisateur interne nécessitant un accès restreint
PC DMZ	NIC	Switch Gio/7	Serveur accessible depuis Internet avec des restrictions

Cette topologie permet d'avoir un point de contrôle unique au niveau du pare-feu pour sécuriser les flux de données et surveiller les communications.

2.3 Architecture logique

L'architecture logique repose sur un plan d'adressage distinct pour chaque réseau segmenté :

Zone	VLAN	Réseau	Masque	Explication
WAN	N/A	192.168.41.0	255.255.254.0 (/23)	Permet la connexion à Internet et la gestion des requêtes sortantes
LAN	206	10.0.96.0	255.255.255.0 (/24)	Zone interne sécurisée pour les utilisateurs et ressources internes
DMZ	406	10.1.96.0	255.255.255.0 (/24)	Permet d'héberger des services accessibles depuis l'extérieur

Le pare-feu permet d'isoler chaque zone et de définir précisément les flux autorisés entre elles.

2.5 Configuration des équipements Pare-feu

Le pare-feu Stormshield est configuré comme suit :

Interface	Nom	Adresse IP	Masque	Rôle
1	WAN	192.168.41.56	255.255.254.0	Permet la communication avec Internet
2	LAN	10.0.96.1	255.255.255.0	Interface dédiée au réseau interne sécurisé
3	DMZ	10.1.96.1	255.255.255.0	Interface dédiée aux services publics contrôlés

Ces configurations permettent de segmenter le réseau tout en assurant un accès contrôlé aux différentes zones et en empêchant les communications non autorisées.

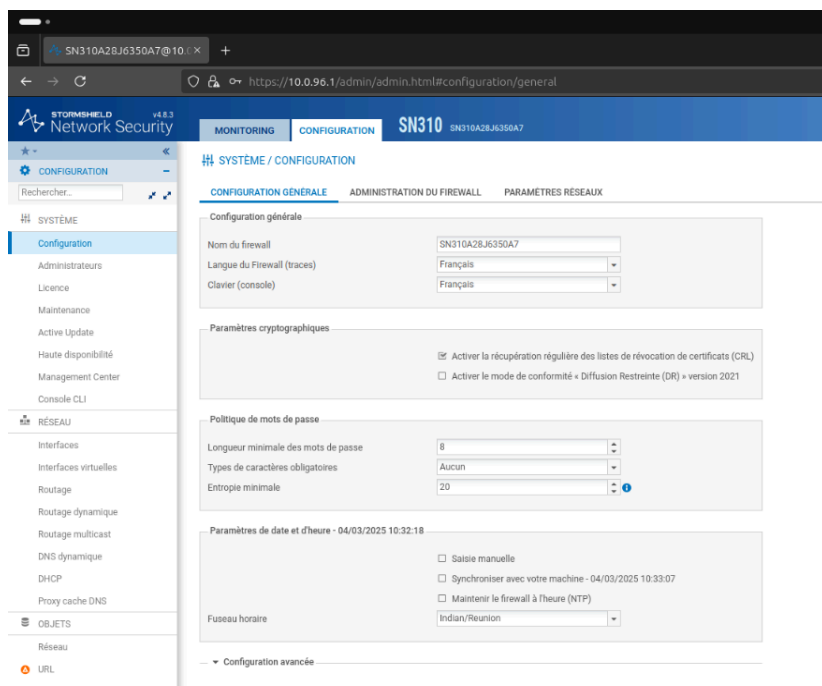
4. Matrice de flux des pare-feu

Source	Destination	Protocole	Action	Justification
N_LAN_10.0.96.0/24	H_PC-DMZ_10.1.96.50	ICMP	Autoriser	Permettre les tests de connectivité et la surveillance
N_LAN_10.0.96.0/24	Internet	HTTP/HTTPS	Autoriser	Autoriser la navigation web sous contrôle du pare-feu

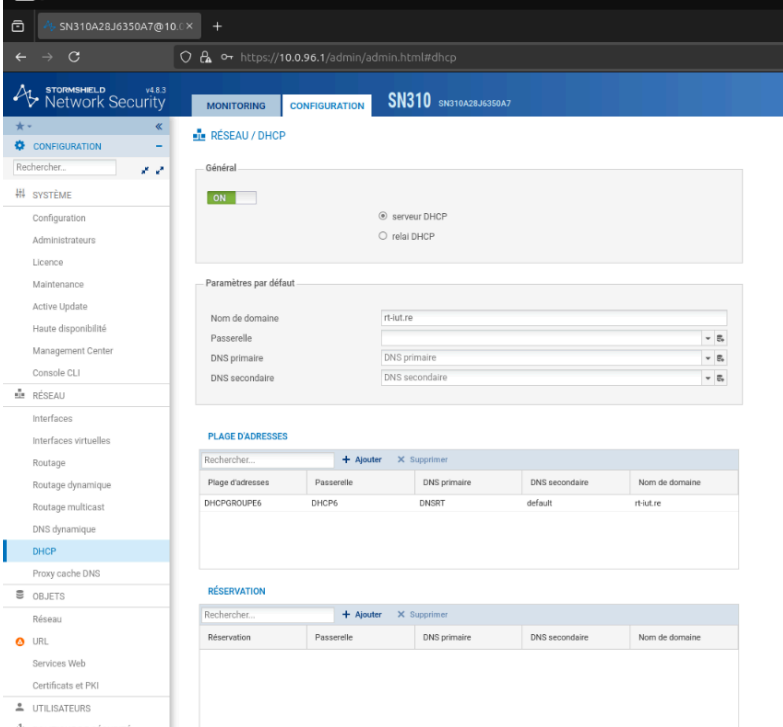
Ce tableau décrit les règles mises en place pour garantir un trafic sécurisé et contrôlé.

Configuration STORMSHIELD

Configuration general

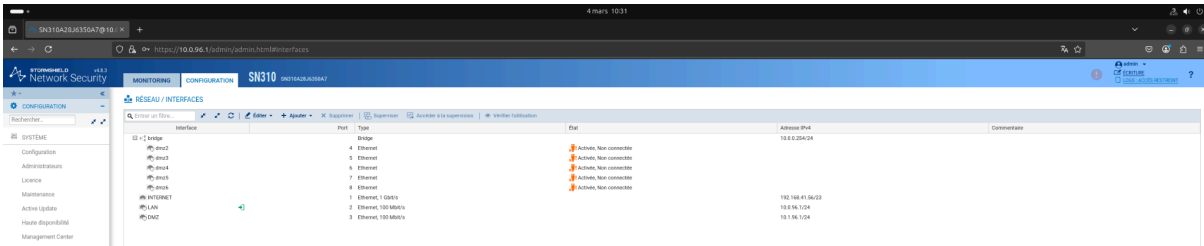


Configuration DHCP



The screenshot shows the Stormshield Network Security configuration interface for the DHCP service. The left sidebar contains a navigation menu with categories like SYSTÈME, RÉSEAU, and UTILISATEURS. The main panel is titled 'RESEAU / DHCP' and includes a 'Général' section with a toggle for 'ON' and radio buttons for 'serveur DHCP' and 'relai DHCP'. Below this is the 'Paramètres par défaut' section with fields for 'Nom de domaine' (rt-lut.re), 'Passerelle', 'DNS primaire', and 'DNS secondaire'. The 'PLAGE D'ADRESSES' section contains a table with columns for 'Plage d'adresses', 'Passerelle', 'DNS primaire', 'DNS secondaire', and 'Nom de domaine'. The 'RÉSERVATION' section also contains a similar table.


Configuration interface



The screenshot shows the Stormshield Network Security configuration interface for network interfaces. The left sidebar contains a navigation menu with categories like SYSTÈME, RÉSEAU, and UTILISATEURS. The main panel is titled 'RÉSEAU / INTERFACES' and displays a table of network interfaces. The table has columns for 'Interface', 'Port', 'Type', 'Etat', 'Adresse IP/v4', and 'Commentaire'.

Interface	Port	Type	Etat	Adresse IP/v4	Commentaire
eth0	4	Ethernet	Active, Non connecté	10.0.254.24	
eth1	5	Ethernet	Active, Non connecté		
eth2	6	Ethernet	Active, Non connecté		
eth3	7	Ethernet	Active, Non connecté		
eth4	8	Ethernet	Active, Non connecté		
eth5	9	Ethernet	Active, Non connecté		
eth6	10	Ethernet	Active, Non connecté		
eth7	11	Ethernet	Active, Non connecté		
eth8	12	Ethernet	Active, Non connecté		
eth9	13	Ethernet	Active, Non connecté		
eth10	14	Ethernet	Active, Non connecté		
eth11	15	Ethernet	Active, Non connecté		
eth12	16	Ethernet	Active, Non connecté		
eth13	17	Ethernet	Active, Non connecté		
eth14	18	Ethernet	Active, Non connecté		
eth15	19	Ethernet	Active, Non connecté		
eth16	20	Ethernet	Active, Non connecté		
eth17	21	Ethernet	Active, Non connecté		
eth18	22	Ethernet	Active, Non connecté		
eth19	23	Ethernet	Active, Non connecté		
eth20	24	Ethernet	Active, Non connecté		
eth21	25	Ethernet	Active, Non connecté		
eth22	26	Ethernet	Active, Non connecté		
eth23	27	Ethernet	Active, Non connecté		
eth24	28	Ethernet	Active, Non connecté		
eth25	29	Ethernet	Active, Non connecté		
eth26	30	Ethernet	Active, Non connecté		
eth27	31	Ethernet	Active, Non connecté		
eth28	32	Ethernet	Active, Non connecté		
eth29	33	Ethernet	Active, Non connecté		
eth30	34	Ethernet	Active, Non connecté		
eth31	35	Ethernet	Active, Non connecté		
eth32	36	Ethernet	Active, Non connecté		
eth33	37	Ethernet	Active, Non connecté		
eth34	38	Ethernet	Active, Non connecté		
eth35	39	Ethernet	Active, Non connecté		
eth36	40	Ethernet	Active, Non connecté		
eth37	41	Ethernet	Active, Non connecté		
eth38	42	Ethernet	Active, Non connecté		
eth39	43	Ethernet	Active, Non connecté		
eth40	44	Ethernet	Active, Non connecté		
eth41	45	Ethernet	Active, Non connecté		
eth42	46	Ethernet	Active, Non connecté		
eth43	47	Ethernet	Active, Non connecté		
eth44	48	Ethernet	Active, Non connecté		
eth45	49	Ethernet	Active, Non connecté		
eth46	50	Ethernet	Active, Non connecté		
eth47	51	Ethernet	Active, Non connecté		
eth48	52	Ethernet	Active, Non connecté		
eth49	53	Ethernet	Active, Non connecté		
eth50	54	Ethernet	Active, Non connecté		
eth51	55	Ethernet	Active, Non connecté		
eth52	56	Ethernet	Active, Non connecté		
eth53	57	Ethernet	Active, Non connecté		
eth54	58	Ethernet	Active, Non connecté		
eth55	59	Ethernet	Active, Non connecté		
eth56	60	Ethernet	Active, Non connecté		
eth57	61	Ethernet	Active, Non connecté		
eth58	62	Ethernet	Active, Non connecté		
eth59	63	Ethernet	Active, Non connecté		
eth60	64	Ethernet	Active, Non connecté		
eth61	65	Ethernet	Active, Non connecté		
eth62	66	Ethernet	Active, Non connecté		
eth63	67	Ethernet	Active, Non connecté		
eth64	68	Ethernet	Active, Non connecté		
eth65	69	Ethernet	Active, Non connecté		
eth66	70	Ethernet	Active, Non connecté		
eth67	71	Ethernet	Active, Non connecté		
eth68	72	Ethernet	Active, Non connecté		
eth69	73	Ethernet	Active, Non connecté		
eth70	74	Ethernet	Active, Non connecté		
eth71	75	Ethernet	Active, Non connecté		
eth72	76	Ethernet	Active, Non connecté		
eth73	77	Ethernet	Active, Non connecté		
eth74	78	Ethernet	Active, Non connecté		
eth75	79	Ethernet	Active, Non connecté		
eth76	80	Ethernet	Active, Non connecté		
eth77	81	Ethernet	Active, Non connecté		
eth78	82	Ethernet	Active, Non connecté		
eth79	83	Ethernet	Active, Non connecté		
eth80	84	Ethernet	Active, Non connecté		
eth81	85	Ethernet	Active, Non connecté		
eth82	86	Ethernet	Active, Non connecté		
eth83	87	Ethernet	Active, Non connecté		
eth84	88	Ethernet	Active, Non connecté		
eth85	89	Ethernet	Active, Non connecté		
eth86	90	Ethernet	Active, Non connecté		
eth87	91	Ethernet	Active, Non connecté		
eth88	92	Ethernet	Active, Non connecté		
eth89	93	Ethernet	Active, Non connecté		
eth90	94	Ethernet	Active, Non connecté		
eth91	95	Ethernet	Active, Non connecté		
eth92	96	Ethernet	Active, Non connecté		
eth93	97	Ethernet	Active, Non connecté		
eth94	98	Ethernet	Active, Non connecté		
eth95	99	Ethernet	Active, Non connecté		
eth96	100	Ethernet	Active, Non connecté		
eth97	101	Ethernet	Active, Non connecté		
eth98	102	Ethernet	Active, Non connecté		
eth99	103	Ethernet	Active, Non connecté		
eth100	104	Ethernet	Active, Non connecté		
eth101	105	Ethernet	Active, Non connecté		
eth102	106	Ethernet	Active, Non connecté		
eth103	107	Ethernet	Active, Non connecté		
eth104	108	Ethernet	Active, Non connecté		
eth105	109	Ethernet	Active, Non connecté		
eth106	110	Ethernet	Active, Non connecté		
eth107	111	Ethernet	Active, Non connecté		
eth108	112	Ethernet	Active, Non connecté		
eth109	113	Ethernet	Active, Non connecté		
eth110	114	Ethernet	Active, Non connecté		
eth111	115	Ethernet	Active, Non connecté		
eth112	116	Ethernet	Active, Non connecté		
eth113	117	Ethernet	Active, Non connecté		
eth114	118	Ethernet	Active, Non connecté		
eth115	119	Ethernet	Active, Non connecté		
eth116	120	Ethernet	Active, Non connecté		
eth117	121	Ethernet	Active, Non connecté		
eth118	122	Ethernet	Active, Non connecté		
eth119	123	Ethernet	Active, Non connecté		
eth120	124	Ethernet	Active, Non connecté		
eth121	125	Ethernet	Active, Non connecté		
eth122	126	Ethernet	Active, Non connecté		
eth123	127	Ethernet	Active, Non connecté		
eth124	128	Ethernet	Active, Non connecté		
eth125	129	Ethernet	Active, Non connecté		
eth126	130	Ethernet	Active, Non connecté		
eth127	131	Ethernet	Active, Non connecté		
eth128	132	Ethernet	Active, Non connecté		
eth129	133	Ethernet	Active, Non connecté		
eth130	134	Ethernet	Active, Non connecté		
eth131	135	Ethernet	Active, Non connecté		
eth132	136	Ethernet	Active, Non connecté		
eth133	137	Ethernet	Active, Non connecté		
eth134	138	Ethernet	Active, Non connecté		
eth135	139	Ethernet	Active, Non connecté		
eth136	140	Ethernet	Active, Non connecté		
eth137	141	Ethernet	Active, Non connecté		
eth138	142	Ethernet	Active, Non connecté		
eth139	143	Ethernet	Active, Non connecté		
eth140	144	Ethernet	Active, Non connecté		
eth141	145	Ethernet	Active, Non connecté		
eth142	146	Ethernet	Active, Non connecté		
eth143	147	Ethernet	Active, Non connecté		
eth144	148	Ethernet	Active, Non connecté		
eth145	149	Ethernet	Active, Non connecté		
eth146	150	Ethernet	Active, Non connecté		
eth147	151	Ethernet	Active, Non connecté		
eth148	152	Ethernet	Active, Non connecté		
eth149	153	Ethernet	Active, Non connecté		
eth150	154	Ethernet	Active, Non connecté		
eth151	155	Ethernet	Active, Non connecté		
eth152	156	Ethernet	Active, Non connecté		
eth153	157	Ethernet	Active, Non connecté		
eth154	158	Ethernet	Active, Non connecté		
eth155	159	Ethernet	Active, Non connecté		
eth156	160	Ethernet	Active, Non connecté		
eth157	161	Ethernet	Active, Non connecté		
eth158	162	Ethernet	Active, Non connecté		
eth159	163	Ethernet	Active, Non connecté		
eth160	164	Ethernet	Active, Non connecté		
eth161	165	Ethernet	Active, Non connecté		
eth162	166	Ethernet	Active, Non connecté		
eth163	167	Ethernet	Active, Non connecté		
eth164	168	Ethernet	Active, Non connecté		
eth165	169	Ethernet	Active, Non connecté		
eth166	170	Ethernet	Active, Non connecté		
eth167	171	Ethernet	Active, Non connecté		
eth168	172	Ethernet	Active, Non connecté		
eth169	173	Ethernet	Active, Non connecté		
eth170	174	Ethernet	Active, Non connecté		
eth171	175	Ethernet	Active, Non connecté		
eth172	176	Ethernet	Active, Non connecté		
eth173	177	Ethernet	Active, Non connecté		
eth174	178	Ethernet	Active, Non connecté		
eth175	179	Ethernet	Active, Non connecté		
eth176	180	Ethernet	Active, Non connecté		
eth177	181	Ethernet	Active, Non connecté		
eth178	182	Ethernet	Active, Non connecté		
eth179	183	Ethernet	Active, Non connecté		
eth180	184	Ethernet	Active, Non connecté		
eth181	185	Ethernet	Active, Non connecté		
eth182	186	Ethernet	Active, Non connecté		
eth183	187	Ethernet	Active, Non connecté		
eth184	188	Ethernet	Active, Non connecté		
eth185	189	Ethernet	Active, Non connecté		
eth186	190	Ethernet	Active, Non connecté		
eth187	191	Ethernet	Active, Non connecté		
eth188	192	Ethernet	Active, Non connecté		
eth189	193	Ethernet	Active, Non connecté		
eth190	194	Ethernet	Active, Non connecté		
eth191	195	Ethernet	Active, Non connecté		
eth192	196	Ethernet	Active, Non connecté		
eth193	197	Ethernet	Active, Non connecté		
eth194	198	Ethernet	Active, Non connecté		
eth195	199	Ethernet	Active, Non connecté		
eth196	200	Ethernet	Active, Non connecté		
eth197	201	Ethernet	Active, Non connecté		
eth198	202	Ethernet	Active, Non connecté		
eth199	203	Ethernet	Active, Non connecté		
eth200	204	Ethernet	Active, Non connecté		
eth201	205	Ethernet	Active, Non connecté		
eth202	206	Ethernet	Active, Non connecté		
eth203	207	Ethernet	Active, Non connecté		
eth204	208	Ethernet	Active, Non connecté		
eth205	209	Ethernet	Active, Non connecté		
eth206	210	Ethernet	Active, Non connecté		
eth207	211	Ethernet	Active, Non connecté		
eth208	212	Ethernet	Active, Non connecté		
eth209	213	Ethernet	Active, Non connecté		
eth210	214	Ethernet	Active, Non connecté		
eth211	215	Ethernet	Active, Non connecté		
eth212	216	Ethernet	Active, Non connecté		
eth213	217	Ethernet	Active, Non connecté		
eth214	218	Ethernet	Active, Non connecté		
eth215	219	Ethernet	Active, Non connecté		
eth216	220	Ethernet	Active, Non connecté		
eth217	221	Ethernet	Active, Non connecté		
eth218	222	Ethernet	Active, Non connecté		
eth219	223	Ethernet	Active, Non connecté		
eth220	224	Ethernet	Active, Non connecté		

Configuration Apache2



Apache2 Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and splits into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this file for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```

/etc/apache2/
|-- apache2.conf
|-- ports.conf
|-- mod-enabled/
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf

```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mod-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `available/` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2enite`, `a2dissite`, and `a2enconf`, `a2disconf` - see their respective man pages for detailed information.
- The binary is called `apache2` and is managed using `systemd`, so to start/stop the service use `systemctl start apache2` and `systemctl stop apache2`, and use `systemctl status apache2` and `journalctl -u apache2` to check status. `systemd` and `apache2ctl` can also be used for service management if desired. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

Document Roots

By default, Ubuntu does not allow access through the web browser to any file outside of those located in `/var/www`, `public_html` directories (when enabled) and `/usr/share` (for web applications). If your site is using a web document not located elsewhere (such as in `/usr`) you may need to whitelist your document root directory in `/etc/apache2/apache2.conf`.

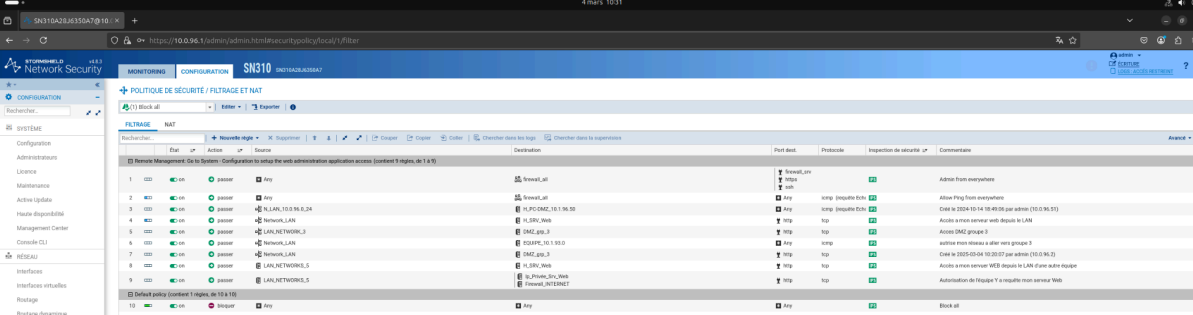
The default Ubuntu document root is `/var/www/html`. You can make your own virtual hosts under `/var/www`.

Reporting Problems

Please use the `ubuntu-bug` tool to report bugs in the Apache2 package with Ubuntu. However, check **existing bug reports** before reporting a new bug.

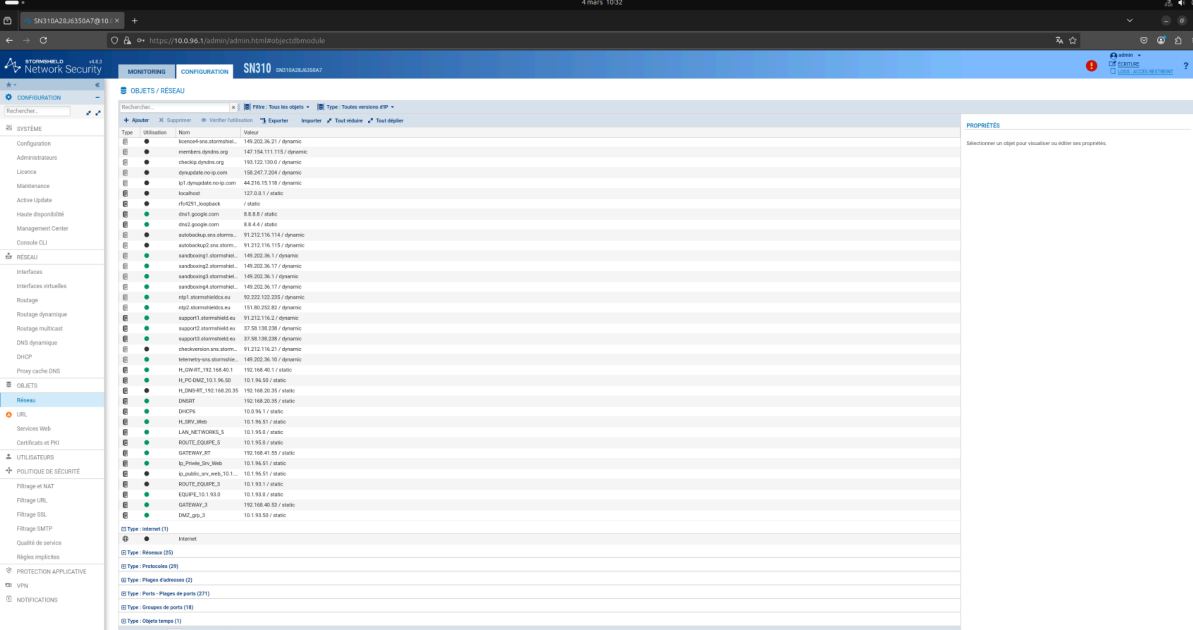
Please report bugs specific to modules (such as PHP and others) to their respective packages, not to the web server itself.

Filtrage NAT



Rule	Chain	Out	Source	Destination	Port dest.	Protocol	Inspection du statut	Commentaire
1	input	passthrough	Any	192.168.1.1	22	tcp	enabled	Accès SSH vers routeur
2	input	passthrough	Any	192.168.1.1	23	tcp	disabled	Accès Telnet vers routeur
3	input	passthrough	192.168.1.0/24	192.168.1.1	80	tcp	enabled	Accès Web vers routeur
4	input	passthrough	192.168.1.0/24	192.168.1.1	443	tcp	enabled	Accès HTTPS vers routeur
5	input	passthrough	192.168.1.0/24	192.168.1.1	8080	tcp	enabled	Accès proxy vers routeur
6	input	passthrough	192.168.1.0/24	192.168.1.1	8081	tcp	enabled	Accès proxy vers routeur
7	input	passthrough	192.168.1.0/24	192.168.1.1	8082	tcp	enabled	Accès proxy vers routeur
8	input	passthrough	192.168.1.0/24	192.168.1.1	8083	tcp	enabled	Accès proxy vers routeur
9	input	passthrough	192.168.1.0/24	192.168.1.1	8084	tcp	enabled	Accès proxy vers routeur
10	input	drop	Any	Any	Any	Any	disabled	Block all

Objet Machine / Réseaux



The screenshot shows the Mikrotik WinBox interface for configuring network objects. The left sidebar contains the navigation menu with the following items: CONFIGURATION, SYSTEME, RESEAU, and OBJETS. The 'OBJETS' menu is expanded, showing sub-items: Réseau, URL, Services Web, Certificats et PIV, and POLITIQUE DE SÉCURITÉ. The main area displays the 'OBJETS / RESEAU' configuration page. The top bar shows the Mikrotik logo and the text 'WinBox 6.40.1'. The main table lists network objects with columns for Name, Address, and Type. The table contains 20 rows of data, including domains like 'kicooker.org', 'moodle.dicr.fr', 'chakra.dicr.fr', 'dmdicr.org', 'dmdicr.org', 'dmdicr.org', 'dmdicr.org', 'dmdicr.org', 'dmdicr.org', 'dmdicr.org', 'dmdicr.org', 'dmdicr.org', 'dmdicr.org', 'dmdicr.org', 'dmdicr.org', 'dmdicr.org', 'dmdicr.org', 'dmdicr.org', 'dmdicr.org', 'dmdicr.org', and 'dmdicr.org'. The right sidebar shows the 'PROPRIÉTÉS' section for the selected object, which is currently empty.

TP2

Pre-Tâche 1 : Installer un serveur Web Apache

Pourquoi ? L'installation d'un serveur web dans la DMZ permet d'offrir un service accessible aussi bien depuis le LAN que potentiellement depuis l'extérieur. Apache est un serveur web largement utilisé et facile à configurer.

Réalisation :

1. Configurer l'interface réseau du serveur avec l'IP **10.1.96.51**.
2. Désactiver toute autre connectivité (WiFi, pare-feu local) pour assurer que la machine ne communique qu'au travers de la DMZ.
3. Tester l'accès au serveur via un navigateur en tapant <http://10.1.96.51>.



Tâche 1 : Accéder au serveur Web depuis le LAN

Pourquoi ? Les utilisateurs internes doivent pouvoir accéder au serveur web sans restriction pour tester son fonctionnement avant de le publier vers l'extérieur.

Réalisation :

1. **Configurer une ouverture de flux sur le pare-feu**
 - Se connecter à l'interface de gestion du pare-feu.

- Créer une nouvelle règle d'autorisation avec les paramètres suivants :
 - i. **Source** : LAN Networks
 - ii. **Destination** : H_SRV_Web (10.1.9X.51)
 - iii. **Port** : TCP/80 (HTTP)
 - iv. **Action** : Autoriser
- Enregistrer et appliquer la configuration.
- 2. **Vérifier que le serveur web est joignable depuis le LAN**
 - Depuis un poste situé dans le LAN, ouvrir un navigateur web.
 - Saisir l'URL suivante dans la barre d'adresse : <http://10.1.9X.51>.
- 3. **Analyser le résultat attendu**
 - Si la page web s'affiche correctement, cela signifie que l'ouverture de flux est effective et que le serveur est accessible.
 - Si la page ne s'affiche pas :
 - i. Vérifier que le service Apache (ou autre serveur web) est bien actif sur la machine hébergeant le serveur web.
 - ii. Tester l'accessibilité du serveur via la commande [ping 10.1.9X.51](#).
 - iii. Vérifier les logs du pare-feu pour voir si le trafic HTTP est bien autorisé.

test web image

Tâche 2 : Finaliser l'accès au serveur web avec NAT de masquage

Pourquoi ? Dans le TP2, le serveur web était accessible via son IP publique, mais les adresses IP privées des clients LAN étaient visibles dans les logs. Or, sur Internet, les adresses privées ne doivent pas transiter. Le NAT de masquage permet de cacher ces IPs privées en utilisant l'IP publique du pare-feu.

Réalisation :

1. **Ouvrir le trafic entre les réseaux des équipes**
 - Créer une règle de filtrage permettant l'accès au serveur web depuis le LAN d'une autre équipe :
 - **Source** : LAN Networks (autres équipes)
 - **Destination** : H_SRV_Web (10.1.9X.51)
 - **Port** : TCP/80 (HTTP) ou TCP/443 (HTTPS)
 - **Action** : Autoriser
 - Enregistrer et appliquer la configuration.
2. **Tester l'accès depuis un LAN distant**
 - Depuis un poste situé dans le LAN d'une autre équipe, ouvrir un navigateur.
 - Saisir l'URL <http://10.1.9X.51> ou <https://10.1.9X.51>.

- Si la page web ne s'affiche pas, analyser le problème.

Pourquoi le test peut échouer ? Le test peut échouer car il n'existe pas encore de route permettant de joindre les réseaux des autres équipes. Pour que le trafic puisse passer d'une équipe à l'autre, il faut configurer des routes statiques sur les pare-feu.

Mise en place du routage :

1. **Déterminer la passerelle des équipes partenaires**
 - Demander à l'équipe cible son IP publique. Cette adresse servira de passerelle pour router le trafic.
2. **Configurer les routes statiques sur le pare-feu**
 - Aller dans **NETWORK > Routing** sur l'interface du pare-feu.
 - Ajouter les routes statiques suivantes :
 - **Destination** : 10.1.9Y.0/24 (DMZ de l'autre équipe)
 - **Passerelle** : 192.168.41.5Y
 - **Interface** : WAN
 - Appliquer la configuration et tester l'accès.
3. **Tester l'accès avec les nouvelles routes**
 - Depuis un PC du LAN de l'équipe distante, tenter d'accéder à <http://10.1.9X.51>.
 - Si cela fonctionne, la communication inter-équipe est correctement configurée.
 - En cas d'échec, vérifier les logs du pare-feu et tester la connectivité avec [ping](#) et [tracert](#).
 - Depuis un poste du LAN, utiliser [nslookup google.com 192.168.20.35](#) pour vérifier que la résolution fonctionne

Tâche 3 : Publier le serveur Web via routage statique

Pourquoi ? Permettre aux autres équipes d'accéder au serveur en utilisant son IP privée, ce qui correspond à un scénario où les services doivent être accessibles entre différents réseaux internes.

Réalisation :

1. Autoriser l'accès depuis les LANs des autres équipes vers le serveur web :
 - Source : LAN distant
 - Destination : 10.1.9X.51
 - Port : TCP/80 ou TCP/443

2. Configurer les routes statiques sur le pare-feu :
 - Destination : 10.1.9y.o/24 (DMZ de l'autre équipe)
 - Passerelle : 192.168.41.5y
 - Interface : WAN
3. Depuis une machine d'une autre équipe, tester l'accès avec un navigateur : <http://10.1.96.51>.
4. Analyser si l'accès fonctionne et identifier les blocages potentiels.

Réalisation :

1. **Configurer la règle de NAT sur le pare-feu**
 - Accéder à **Security Policy > Filter – NAT**.
 - Créer une règle NAT avec les paramètres suivants :
 - i. **Source originale** : Any
 - ii. **Destination originale** : IP externe du pare-feu (192.168.41.5X)
 - iii. **Port** : TCP/80 (HTTP)
 - iv. **Source tradatée** : Any
 - v. **Destination tradatée** : IP privée du serveur Web (10.1.9X.51)
 - vi. **Port tradaté** : TCP/80 (HTTP)
 - Enregistrer et appliquer la configuration.
2. **Configurer les ouvertures de flux**
 - Ouvrir l'accès entre l'IP publique et le serveur web privé.
 - Enregistrer les modifications.
3. **Tester l'accès au serveur Web**
 - Depuis un PC du LAN d'une autre équipe, tester <http://192.168.41.5X>.
 - Si l'accès fonctionne, la configuration NAT est bien en place.

Nom	Réseaux/Machine	Gateway	VLAN
LAN	10.0.96.0/24	10.0.96.1/24	LAN
DMZ	10.1.96.0/24	10.1.96.1/24	DMZ
Web	10.1.96.51/24	10.1.96.1/24	DMZ
Client	10.0.96.50/24	10.0.96.1/24	LAN
Pare Feu	10.0.96.1/24	X	X

DHCP LAN

Plage d'adressage : 10.0.96.10 - 10.0.96.20

Static device

Web ip : 10.1.96.51

parefeu ip : 10.0.96.1 / 10.0.0.254

VLAN

Plage LAN : fa0/1-5

Plage DMZ : fa0/6-10

Le LAN peut ping la DMZ (la page web)

Carte Ethernet Ethernet :

```
Suffixe DNS propre à la connexion. . . :  
Adresse IPv6 de liaison locale. . . . : fe80::5963:cead:c2d1:5710%17  
Adresse IPv4. . . . . : 10.0.96.50  
Masque de sous-réseau. . . . . : 255.255.0.0  
Passerelle par défaut. . . . . : 10.0.96.1
```

TP3

Tâche 1 : Finaliser l'accès au serveur web avec NAT de masquage

Pourquoi ? Dans le TP2, le serveur web était accessible via son IP publique, mais les adresses IP privées des clients LAN étaient visibles dans les logs. Or, sur Internet, les adresses privées ne doivent pas transiter. Le NAT de masquage permet de cacher ces IPs privées en utilisant l'IP publique du pare-feu.

Réalisation :

1. Créer une règle NAT de Masquage :

- Aller dans **Security Policy** > **NAT**.
- Ajouter une nouvelle règle NAT (*masquerade* ou *hide*).
- **Source d'origine** : LAN (10.0.9X.0/24).
- **Destination d'origine** : IP publique du serveur Web (192.168.41.5X).
- **Port** : TCP/80.
- **Source transformée** : IP publique du pare-feu (192.168.41.5X).
- **Destination transformée** : Original (ne pas modifier).
- **Appliquer et enregistrer**.

2. Modifier les règles de filtrage pour adapter l'accès au serveur Web :

- Modifier la règle existante qui autorisait les accès HTTP vers l'IP privée.
- **Nouvelle source** : Any (réseau WAN simulé 192.168.40.0/23).
- **Nouvelle destination** : IP publique du serveur Web (192.168.41.5X).
- **Service** : TCP/80.
- **Action** : Autoriser (*Pass*).
- **Appliquer et enregistrer**.

3. Tester et valider :

- Depuis un réseau externe (ex. LAN d'une autre équipe), accéder au serveur Web via son IP publique :
<http://192.168.41.5X>
- Observer dans les logs du pare-feu si l'adresse source est bien masquée.

Tâche 2 : Configurer l'accès DNS

Pourquoi ? L'accès à Internet nécessite un serveur DNS pour résoudre les noms de domaine en adresses IP. Le serveur DNS utilisé est celui du RT (192.168.20.35). Actuellement, les requêtes DNS depuis le LAN n'aboutissent pas car le pare-feu bloque ce trafic.

Réalisation :

1. Créer une règle de filtrage pour autoriser les requêtes DNS :

- Aller dans **Security Policy > Filtrage**.
- Ajouter une nouvelle règle.
- **Source** : Réseau LAN (10.0.9X.0/24).
- **Destination** : Serveur DNS externe (192.168.20.35).
- **Port** : UDP 53 (DNS).
- **Action** : Autoriser (*Pass*).
- **Appliquer et enregistrer**.

2. Créer une règle NAT de Masquage pour les requêtes DNS :

- Aller dans **Security Policy > NAT**.
- Ajouter une nouvelle règle NAT (*masquerade*).
- **Source d'origine** : LAN (10.0.9X.0/24).
- **Destination d'origine** : 192.168.20.35 (serveur DNS).
- **Port** : UDP 53.
- **Source transformée** : IP publique du pare-feu (192.168.41.5X).
- **Destination transformée** : Original.
- **Appliquer et enregistrer**.

3. Tester et valider :

Sur un PC du LAN, exécuter :

nslookup www.google.com 192.168.20.35

-
- Si la requête aboutit et retourne une adresse IP, le DNS fonctionne.
- Vérifier les logs pour voir si le NAT de masquage s'applique bien.

Tâche 3 : Configurer l'accès Internet du LAN

Pourquoi ? Les machines du LAN doivent pouvoir accéder à Internet via HTTP et HTTPS. Pour cela, le pare-feu doit autoriser ces flux et effectuer un NAT de masquage pour que les IPs privées du LAN soient remplacées par l'IP publique du pare-feu.

Réalisation :

1. Créer une règle de filtrage pour autoriser l'accès Internet :

- Aller dans **Security Policy > Filtrage**.
- Ajouter une nouvelle règle.
- **Source** : LAN (10.0.9X.0/24).
- **Destination** : Any (*toutes adresses externes*).
- **Service** : HTTP (80) et HTTPS (443).
- **Action** : Autoriser (*Pass*).
- **Appliquer et enregistrer**.

2. Créer une règle NAT de Masquage pour l'accès Internet :

- Aller dans **Security Policy > NAT**.
- Ajouter une nouvelle règle NAT (*masquerade*).
- **Source d'origine** : LAN (10.0.9X.0/24).
- **Destination d'origine** : Any (*Internet*).
- **Ports** : TCP 80 (HTTP) et TCP 443 (HTTPS).
- **Source transformée** : IP publique du pare-feu (192.168.41.5X).
- **Destination transformée** : Original.
- **Appliquer et enregistrer**.

3. Tester et valider :

- Depuis un PC du LAN :
 - Essayer d'ouvrir <http://www.google.com> et <https://www.google.com>.
 - Vérifier que la page s'affiche normalement.

Exécuter un test ping vers une IP publique, par exemple :

ping 8.8.8.8

-
- Vérifier dans les logs du pare-feu que les connexions HTTP et HTTPS sont bien traduites par le NAT.

5. Tests et validation

Cette section récapitule les vérifications à effectuer pour valider l'ensemble de la configuration du TP3. Chaque fonctionnalité mise en place doit être testée :

- **Accès au serveur Web depuis l'extérieur** : Depuis un réseau externe au vôtre (par exemple le LAN d'une autre équipe ou un PC de l'enseignant simulant un client Internet sur le WAN), accéder à votre serveur Web DMZ via son IP publique. L'URL <http://192.168.41.5X> (avec X votre numéro d'équipe) doit afficher la page web hébergée sur votre serveur DMZ. Vérifiez qu'aucune adresse privée n'apparaît dans la chaîne réseau (par ex., dans les *logs* du serveur web ou du firewall). Désormais, grâce au NAT de masquage (Tâche 4), le trafic entrant devrait sembler provenir d'adresses IP publiques seulement.
- **Résolution DNS depuis le LAN** : Sur un poste du LAN, tester plusieurs résolutions de noms :
 - Exécutez `nslookup nom_de_domaine` (par ex. `nslookup www.google.com`). Le serveur DNS ([192.168.20.35](#)) doit répondre avec une adresse IP correspondante. Le temps de réponse doit être court, signe que le flux DNS sortant est correctement autorisé et la réponse revenue.

Conclusion

Ces TP nous ont permis de mettre en place une infrastructure réseau sécurisée en appliquant des concepts clés comme la segmentation, le filtrage et le NAT. Nous avons appris à configurer un pare-feu, à gérer les accès entre différentes zones et à assurer la connectivité via des règles de routage adaptées. L'implémentation du NAT de masquage et l'accès sécurisé à Internet ont renforcé nos compétences en administration réseau. Enfin, la sauvegarde et la maintenance des configurations nous ont montré l'importance de la gestion à long terme des infrastructures réseau. Ces acquis sont essentiels pour comprendre et sécuriser un environnement informatique moderne.