


“Serveur WEB APACHE”





Apache2 Ubuntu 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 split 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 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  
|-- mods-enabled  
|   |-- *.Load  
|   |-- *.conf
```

Sommaire

Sommaire.....	2
1. Qu'est-ce que Apache2?.....	3
2. Prérequis.....	4
3. Qu'est-ce que.....	4
4. Procédure générale.....	5
5. Installation et configuration "NOM".....	9

1. Qu'est-ce qu'un par-feu?

Un serveur TFTP est un serveur qui utilise le protocole TFTP pour transférer de petits fichiers sur un réseau. Il est simple, rapide, sans sécurité, et sert surtout à charger des configurations, mettre à jour des firmwares ou démarrer un PC via le réseau (PXE).

2. Procédure générale.

RÉSEAU / INTERFACES

Interface	Port	Type	État	Adresse IPv4
WAN	1	Ethernet, 1 Gbit/s		192.168.147.136/24 (DHCP)
LAN	2	Ethernet, 1 Gbit/s		192.168.200.254/24
dmz1	3	Ethernet, 1 Gbit/s		192.168.1.254/24

Interfaces réseaux.

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

FILTRAGE NAT									
Rechercher...									
+ Nouvelle règle X Supprimer ↑ ↓ ✂ Couper 📄 Copier 📄 Coller 🔍 Chercher dans les logs 🔍 Chercher dans la supervision									
	État	Trafic original (avant translation)				Trafic après translation			
		Source	Destination	Port dest.	Source	Port src.	Destination	Port dest.	
1	on	Network_internals	Internet	Any	Firewall_WAN	ephemeral_fw	Any		
2	on	Network_WAN	Firewall	haproxy1	Any		srvhaproxy1	ssh	
3	on	Network_WAN	Firewall	web1	Any		srvweb1	ssh	
4	on	Network_WAN	Firewall	haproxy2	Any		srvhaproxy2	ssh	
5	on	Network_WAN	Firewall	web2	Any		srvweb2	ssh	
6	on	Network_WAN	Firewall	http	Any		ipvirtuelle	http	

Règles de NAT.

3. Connexion de l'AD au Pare-Feu.

PROPRIÉTÉS

Nom de l'objet

Adresse IPv4

Adresse MAC

Résolution

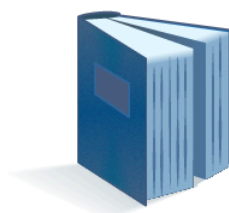
Aucune (IP statique) Automatique

Commentaire

Créer un objet SRV-AD et mettre l'adresse ip du serveur AD.

ASSISTANT DE CRÉATION DE L'ANNUAIRE UTILISATEUR

CHOIX DU TYPE D'ANNUAIRE - (ÉTAPE 1 SUR 3)




- Connexion à un annuaire Microsoft Active Directory
- Connexion à un annuaire LDAP externe
- Connexion à un annuaire LDAP externe de type PosixAccount
- Création d'un annuaire LDAP interne

Accédez au menu Configuration > Gestion des annuaires, puis cliquez sur Ajouter un annuaire. Sélectionnez ensuite l'option Connexion à un annuaire Microsoft Active Directory afin d'initier la liaison avec votre serveur AD.

ASSISTANT DE CRÉATION DE L'ANNUAIRE UTILISATEUR

ACCÈS À L'ANNUAIRE - (ÉTAPE 2 SUR 3)



Nom de domaine: ADTECH.fr

Serveur: SRV-AD

Port: ldap

Domaine racine (Base DN): dc=adtech,dc=fr

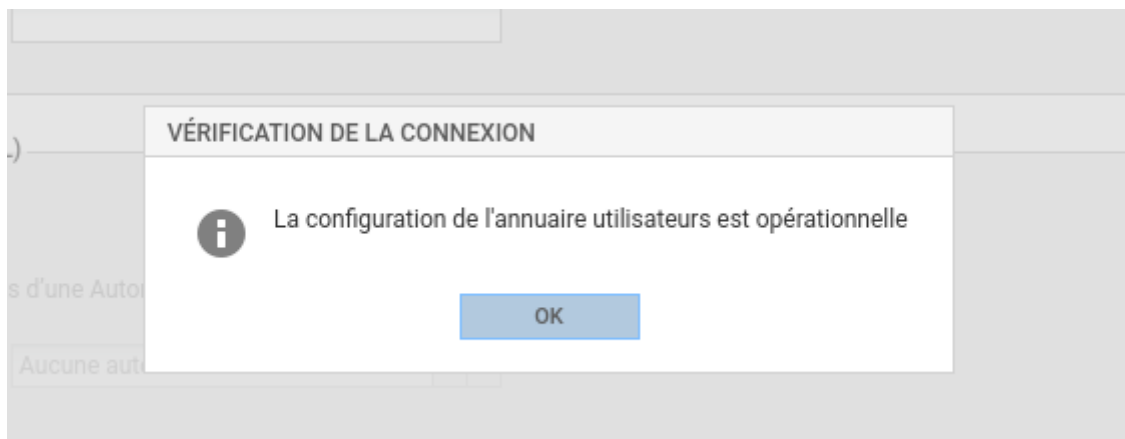
Identifiant (user DN): cn=stormshield,cn=Users

Mot de passe: [masqué]

Hachage des mots de passe: SHA

ANNULER PRÉCÉDENT SUIVANT

Configuration de la connexion entre le pare-feu et l'Active Directory : mise en place du domaine, de la connexion LDAP et du compte autorisé à consulter l'annuaire.



Vérification du bon fonctionnement de l'annuaire après son ajout, confirmant que la connexion est opérationnelle.

4. Configuration du VPN SSL.

CRÉER UN OBJET

- Machine
- Nom DNS (FQDN)
- Réseau**
- Plage d'adresses
- Routeur
- Groupe
- Protocole IP

Nom de l'objet

Adresses IPv4

Adresse IP de réseau

Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0

Commentaire

creer objet udp

CRÉER UN OBJET

- Machine
- Nom DNS (FQDN)
- Réseau**
- Plage d'adresses
- Routeur
- Groupe
- Protocole IP

Nom de l'objet

Adresses IPv4

Adresse IP de réseau

Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0

Commentaire

creer objet TCP

VPN / VPN SSL

ON

Activer le VPN SSL

PARAMÈTRES GÉNÉRAUX

VÉRIFICATION DES POSTES CLIENTS (ZTNA) (DÉSACTIVÉ)

Paramètres réseaux

Adresse IP publique (ou FQDN) de l'UTM utilisée	<input type="text" value="192.168.147.164"/>
Réseaux ou machines accessibles	<input type="text" value="Network_LAN"/>
Réseau assigné aux clients (UDP)	<input type="text" value="Net_UDPVPN"/>
Réseau assigné aux clients (TCP)	<input type="text" value="Net_TCPVPN"/>
Maximum de tunnels simultanés autorisés	200

Paramètres DNS envoyés au client

Nom de domaine	<input type="text" value="techuniverse.lan"/>
Serveur DNS primaire	<input type="text" value="dns1.google.com"/>
Serveur DNS secondaire	<input type="text" value="Configuré pour le firewall"/>

▼ Configuration avancée

UTILISATEURS / DROITS D'ACCÈS

ACCÈS PAR DÉFAUT

ACCÈS DÉTAILLÉ

SERVEUR PPTP

Comportement à adopter lorsqu'aucune règle d'accès n'est définie pour l'utilisateur

Accès VPN

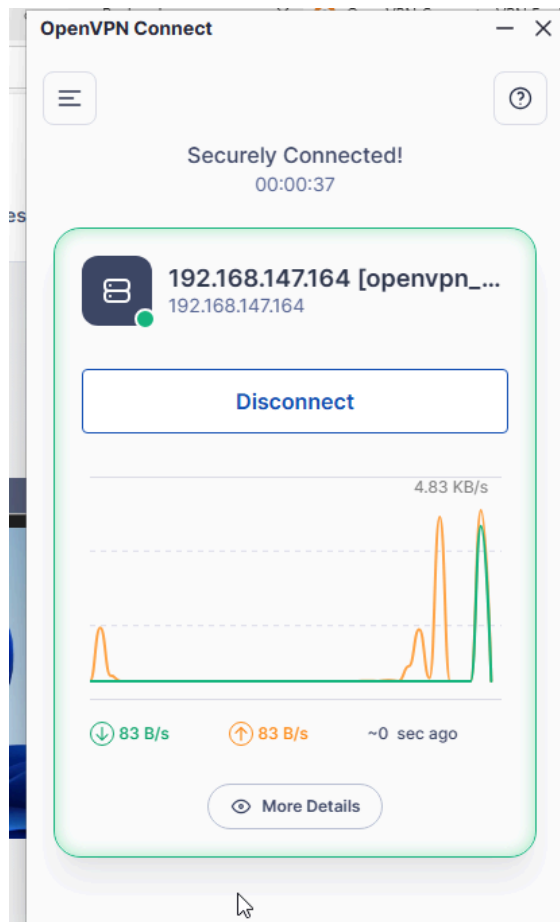
Profil VPN SSL Portail	<input type="text" value="Interdire"/>
Politique IPsec	<input type="text" value="Interdire"/>
Politique VPN SSL	<input type="text" value="Interdire"/>

Parrainage

Politique de parrainage	<input type="text" value="Autoriser"/>
-------------------------	--



exporter le fichier de configuration à mettre dans l'appli openVPN sur l'AD



VPN client AD