

vpn-ssl

MARK RODERICK - VPN SSL

VPN = Virtual Private Network

Buts

- Connexion à distance
- Sécuriser connexion
- Confidentialité
- Authentification

- **IPsec VPN** → protège **tout le trafic réseau**, idéal pour relier deux sites ou donner un accès complet au réseau interne.
- **SSL VPN** → protège **uniquement certaines applications**, facile à utiliser depuis un navigateur, parfait pour les employés en télétravail ou sur des appareils personnels.

*types de vpn

Caractéristique	IPsec VPN	SSL VPN
Couche OSI	Couche réseau (couche 3)	Couche transport (couche 4) via SSL/TLS
Portée du chiffrement	Tout le trafic réseau (IP complet)	Sessions/applications spécifiques
Client requis	Logiciel VPN dédié installé sur l'appareil	Navigateur web (aucun client supplémentaire)
Cas d'usage idéal	Connexion site-à-site, accès complet au réseau	Accès distant aux applications web
Maintenance	Plus complexe, nécessite configuration avancée	Plus simple, déploiement rapide
Performance	Très robuste pour gros volumes de données	Plus léger, adapté aux utilisateurs nomades

VPN sur le sts externe

Thème	Détails et Fonctionnement	Configuration & Prérequis
Modes de VPN	1. Mode Portail : Accès sans client (clientless) aux serveurs Web/HTTP via le portail captif. 2. Mode Tunnel (Complet) : Accès transparent au réseau interne, nécessite un client installé.	Le mode tunnel utilise OpenVPN (gratuit) ou le client Stormshield.
Protocole & Réseau	Encapsulation de paquets IP dans un tunnel TLS (TCP ou UDP). Le réseau VPN est considéré comme "interne" et ne doit pas chevaucher l'existant.	Adressage IP : Le réseau VPN est découpé en sous-réseaux de /30 . Le serveur prend les premières IP, chaque client reçoit un sous-réseau dédié.
Processus de Connexion	1. Authentification utilisateur sur le portail captif. 2. Vérification des droits (Access Privileges). 3. Téléchargement de la config (<code>.ovpn</code> , certificats). 4. Établissement du tunnel TLS.	Le client récupère automatiquement l'archive <code>Openvpn_client.zip</code> contenant la clé PKI et le fichier de configuration.
Prérequis Admin	Le service nécessite une PKI (Autorité de certification) configurée. Un annuaire (LDAP ou interne) doit être actif.	Un profil de portail captif doit être lié à l'interface d'entrée avec une méthode d'authentification valide.

Sécurité & Filtrage	L'accès n'est pas autorisé par défaut. Il faut modifier les Privilèges d'accès (Block → Allow) pour l'utilisateur/groupe.	Des règles de filtrage explicites sont obligatoires pour autoriser le trafic du tunnel (<code>net_ssl_vpn</code>) vers le réseau interne.
Clients Compatibles	PC : Windows, macOS, GNU/Linux. Mobile : Android, iOS.	Le client Stormshield (Windows uniquement) permet la gestion de carnets d'adresses.
Limitations	Le nombre maximum de tunnels simultanés dépend du modèle de l'équipement (ex: 5 pour SN160, 500 pour SNI40).	Limites spécifiques s'appliquent aussi aux appliances virtuelles (V-UTM).

STS eExterne SSL VPN

L'onglet Utilisateurs > Authentification

STB-ext@172.16.10.254 / x 172.16.10.250 Administrat x index

https://172.16.10.254/admin/admin.html#authentication/portal

admin

ÉCRITURE

LOGS : ACCÈS RESTREIN

MONITORING CONFIGURATION EVA1 STB-ext

CONFIGURATION

Rechercher...

roulage multicast

DNS dynamique

DHCP

Proxy cache DNS

OBJETS

Réseau

URL

Certificats et PKI

UTILISATEURS

Utilisateurs

Comptes temporaires

Droits d'accès

Authentification

Enrôlement

Configuration des annuaires

UTILISATEURS / AUTHENTIFICATION

MÉTHODES DISPONIBLES POLITIQUE D'AUTHENTIFICATION PORTAL CAPTIF PROFILS DU PORTAL CAPTIF

Portail captif

CORRESPONDANCE ENTRE PROFIL D'AUTHENTIFICATION ET INTERFACE

+ Ajouter X Supprimer

Interface	Profil	Méthode ou annuaire par défaut
in	Internal	Annuaire LDAP (none)
out	Internal	Annuaire LDAP (none)
sslvpn	Internal	Annuaire LDAP (none)

Serveur SSL

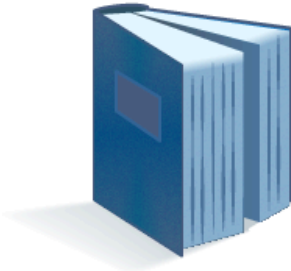
Certificat (clé privée): Sélectionnez un certificat

ds

LDAP

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

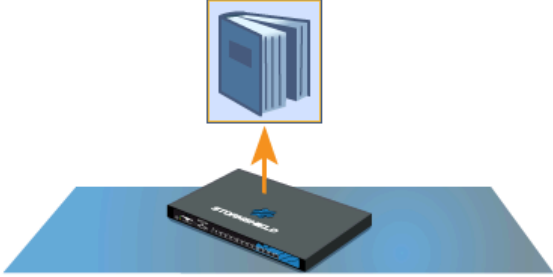
ANNULER PRÉCÉDENT SUIVANT

etape 2

mdp :Azerty123

ASSISTANT DE CRÉATION DE L'ANNUAIRE UTILISATEUR

ACCÈS À L'ANNUAIRE - (ÉTAPE 2 SUR 3)



Organisation: Teststext

Domaine: Teststext.lan

Mot de passe: ●●●●●●●●

Confirmer: ●●●●●●●●

Hachage des mots de passe: SHA


Moyen

ANNULER PRÉCÉDENT SUIVANT

etape 3

ASSISTANT DE CRÉATION DE L'ANNUAIRE UTILISATEUR

AUTHENTIFICATION - (ÉTAPE 3 SUR 3)



L'association entre profils d'authentification et interfaces est déjà réalisée: Choisissez une interfac

- Activer l'enrôlement des utilisateurs via le profil 0 (interne) du portail Web
- Autoriser l'accès à la base LDAP

ANNULER PRÉCÉDENT TERMINER

users

pour y accéder via l'application open vpn

login : usertext
mdp : Azerty123

STORMSHIELD Network Security v4.3.27

MONITORING CONFIGURATION EVA1 STS-ext

admin

ÉCRITURE LOGS: ACC

UTILISATEURS / UTILISATEURS

Rechercher... Tous | + Ajouter un utilisateur + Ajouter un groupe X Supprimer Vérerifier

Cn

Aucun utilisateur ou groupe correspondant

Pour créer un utilisateur, renseignez au moins son identifiant et son nom de famille, vous devez aussi indiquer une adresse E-mail valide.

COMPTE CERTIFICAT MEMBRE DES GROUPES

Créer ou modifier le mot de passe

Identifiant (login): usertext

Nom: usertext

Prénom: usertext

E-mail: usertext@gmail.com

Téléphone: 00000000

Description:

droit access
acces par defaut faut autoriser SSL

ST-Ext@172.16.10.254 x 172.16.10.250 Administr x index x Nouvel onglet x +

https://172.16.10.254/admin/admin.html#useraccesscontrol/default

admin ÉCRITURE LOGS : ACCÈS

MONITORING CONFIGURATION EVA1 STS-ext

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: Interdire

Politique IPsec: Interdire

Politique VPN SSL: Autoriser

Parrainage

Politique de parrainage: Autoriser

PUIS ACCESSEZ détailler

Activités Firefox ESR 18 nov. 15:49

ST-Ext@172.16.10.254 x 172.16.10.250 Administr x index x Nouvel onglet x + v

https://172.16.10.254/admin/admin.html#useraccesscontrol/uac

admin ÉCRITURE LOGS : ACCÈS RESTREINT

MONITORING CONFIGURATION EVA1 STS-ext

UTILISATEURS / DROITS D'ACCÈS

ACCÈS PAR DÉFAUT ACCÈS DÉTAILLÉ SERVEUR PPTP

Rechercher... + Ajouter x Supprimer Monter Descendre

Etat	Utilisateur - groupe d'utilisateurs	VPN SSL Portail	IPSEC	VPN SSL	Parrainage
1 <input checked="" type="checkbox"/> Activé	usertext@testststext.testststext.lan	Interdire	Interdire	Autoriser	Interdire
2 <input checked="" type="checkbox"/> Activé	Any user@testststext.testststext.lan	Interdire	Interdire	Autoriser	Interdire

Authentification

methodes disponibles faut choisir LDAP

The screenshot shows the EVA1 configuration interface. The main content area is titled 'UTILISATEURS / AUTHENTIFICATION'. Under the 'Méthodes disponibles' tab, there is a list of authentication methods. The 'LDAP' method is highlighted in yellow. Below it, there are options for 'Invités' and 'Parrainage'. The left sidebar contains a navigation menu with 'Authentification' highlighted in blue. The top navigation bar shows 'MONITORING' and 'CONFIGURATION' tabs, with 'EVA1 STS-ext' as the current page.

Politique authentification

The screenshot shows the EVA1 configuration interface for the 'Politique d'authentification' section. A table lists authentication policies. The first policy is 'Activé' and uses 'LDAP' as the default method. The 'Authentification' menu item in the left sidebar is highlighted in blue. The top navigation bar shows 'MONITORING' and 'CONFIGURATION' tabs, with 'EVA1 STS-ext' as the current page.

État	Source	Méthodes (évaluées par ordre)
1 <input checked="" type="checkbox"/> Activé	Any user@testststext.testststext.lan sslvpn	1 LDAP 2 Méthode par défaut

portail captif

UTILISATEURS / AUTHENTIFICATION

MÉTHODES DISPONIBLES POLITIQUE D'AUTHENTIFICATION **PORTAIL CAPTIF** PROFILS DU PORTAIL CAPTIF

Portail captif

CORRESPONDANCE ENTRE PROFIL D'AUTHENTIFICATION ET INTERFACE

+ Ajouter X Supprimer

Interface	Profil	Méthode ou annuaire par défaut
in	Internal	Annuaire LDAP (teststsext.teststsext.lan)
out	Internal	Annuaire LDAP (teststsext.teststsext.lan)
sslvpn	Internal	Annuaire LDAP (teststsext.teststsext.lan)

CONFIGURATION

Rechercher...

- SYSTÈME
- RÉSEAU
- OBJETS
- UTILISATEURS
 - Utilisateurs
 - Comptes temporaires
 - Droits d'accès
 - Authentification**
 - Enrôlement
 - Configuration des annuaires
- POLITIQUE DE SÉCURITÉ

profil portail captif

UTILISATEURS / AUTHENTIFICATION

MÉTHODES DISPONIBLES POLITIQUE D'AUTHENTIFICATION PORTAIL CAPTIF **PROFILS DU PORTAIL CAPTIF**

Internal Renommer ⓘ

Authentification

Méthode ou annuaire par défaut: **Annuaire LDAP (teststsext.teststsext.lan)**

Activer le parrainage

Conditions d'utilisation de l'accès à Internet

Activer l'affichage des conditions d'utilisation d'accès à Internet

Fréquence d'affichage des Conditions: 18 heure(s) 0 minute(s)

Champs personnalisés du portail captif (méthode Invités uniquement)

Champ n°1: Vide

Champ n°2: Vide

Champ n°3: Vide

CONFIGURATION

Rechercher...

- SYSTÈME
- RÉSEAU
- OBJETS
- UTILISATEURS
 - Utilisateurs
 - Comptes temporaires
 - Droits d'accès
 - Authentification**
 - Enrôlement
 - Configuration des annuaires
- POLITIQUE DE SÉCURITÉ
- PROTECTION APPLICATIVE
- VPN

Politique de sécurité > Filtrage et Nat

4.3.27 MONITORING CONFIGURATION EVA1 STS-ext admin ÉCRITURE LOGS : ACCÈS RESTREINT

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

(1) Block all Editer Exporter

FILTRAGE NAT

	État	Action	Source	Destination	Port dest.	Protocole	Insp
3	on	passer	sts_interne	Internet	https	https	IPS
4	on	passer	Vlan_srvIT	Internet	http, https, dns	http, https, dns	IPS
5	on	passer	objethote	portfolio	ftp, ssh	ftp, ssh	IPS
6	on	passer	Any interface: out	Firewall_out	http	http	IPS
7	on	passer	Network_internal:	Internet	Any	Any	IPS
8	on	passer	any via Tunnel VPN SSL	Network_internals	Any	Any	IPS
Default policy (contient 1 règles, de 9 à 9)							
9	on	bloquer	Any	Any	Any	Any	IPS

Page 1 sur 1 Page courante 1 - 11 sur 11

VALIDATEUR DE CONFIGURATION

cette regle sur le stormshield
source

27 MONITORING CONFIGURATION EVA1 STS-ext ÉCRITURE LOGS : A

ÉDITION DE LA RÈGLE N° 1

Utilisateur

Source

Méthodes d'authentifi...

UTILISATEUR

Utilisateur ou groupe: Any user@testststext.testststext.lan

VPN SSL

STX-ext@172.16.10.254 x sts-interne@172.16.10.25 x index

https://172.16.10.254/admin/admin.html#vpnsfull

admin

ÉCRITURE

LOGS : ACCÈS RESTREINT

v4.3.27 MONITORING CONFIGURATION EVA1 STS-ext

CONFIGURATION

Rechercher...

SYSTÈME

RÉSEAU

OBJETS

UTILISATEURS

POLITIQUE DE SÉCURITÉ

PROTECTION APPLICATIVE

VPN

VPN IPsec

VPN SSL Portail

VPN SSL

Serveur PPTP

NOTIFICATIONS

VPN / VPN SSL

ON

Paramètres réseaux

Adresse IP publique (ou FQDN) de l'UTM utilisée:

Réseaux ou machines accessibles: Network_internals

Réseau assigné aux clients (UDP):

Réseau assigné aux clients (TCP):

Maximum de tunnels simultanés autorisés: Sélectionnez au moins une plage d'adresses IP ou un réseau pour les clients VPN SSL

Paramètres DNS envoyés au client

Nom de domaine:

Serveur DNS primaire: Configuré pour le fire

Serveur DNS secondaire: Configuré pour le fire

Configuration avancée

STX-ext@172.16.10.25 x 172.16.10.250 Administr x index

https://172.16.10.254/admin/admin.html#vpnsfull

admin

ÉCRITURE

LOGS : ACCÈS RESTREINT

v4.3.27 MONITORING CONFIGURATION EVA1 STS-ext

CONFIGURATION

Rechercher...

Règles implicites

PROTECTION APPLICATIVE

Applications et protections

Protocoles

Profils d'inspection

Management de vulnérabili...

Réputation des machines

Antivirus

Antispam

VPN

VPN IPsec

VPN SSL Portail

VPN SSL

Serveur PPTP

VPN / VPN SSL

ON

Paramètres réseaux

Adresse IP publique (ou FQDN) de l'UTM utilisée: 10.30.5.141

Réseaux ou machines accessibles: Network_internals

Réseau assigné aux clients (UDP): ssl_vpn_udp

Réseau assigné aux clients (TCP): ssl_vpn_tcp

Maximum de tunnels simultanés autorisés: 300

Paramètres DNS envoyés au client

Nom de domaine:

Serveur DNS primaire: dns1.google.com

Serveur DNS secondaire: dns2.google.com

Configuration avancée

10.30.5.141

```
sts_externe_mark sur 9-RA-P2 - Connexion à un ordinateur virtuel
Fichier Action Média Presse-papiers Affichage Aide
[Icons]
NS-BSD/amd64 (VMSNSX00C1212A9) (ttyv0)
login: admin
Password:
Login incorrect
login: admin
Password:
VMSNSX00C1212A9: FW EVA1 (XL / EUROPE)
Firewall software version 4.3.27 VM-RELEASE
System Name: STS-ext
port      name      NS-BSD  state  addressIPv4  addressIPv6
  1        out      hn0     up     10.30.5.141/16
  2        in       hn1     up     172.16.10.254/28
STS-ext-VMSNSX00C1212A9>
```