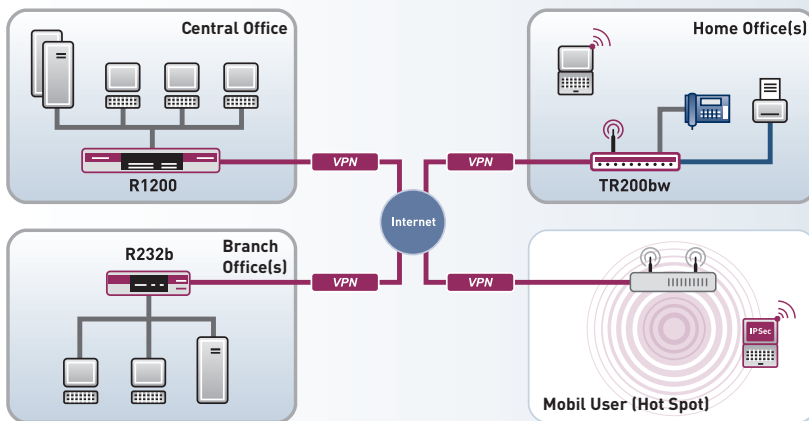


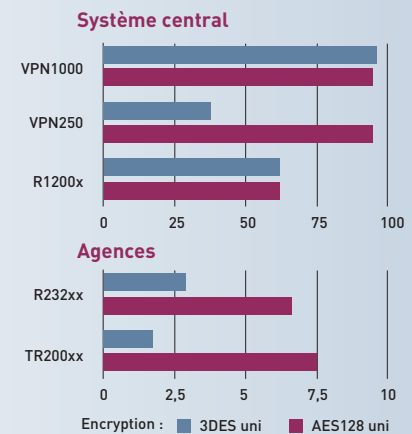
Fiche applicative

Connexion sécurisée des agences et postes de travail à domicile via VPN

Afin que les employés aient un accès centralisé aux données de la société, comme par exemple aux informations clients, au chiffre d'affaire, aux e-mails,... il est nécessaire de travailler en réseau. Dès que les personnes mobiles, télétravailleurs, agences accèdent au serveur de la société en Wi-Fi, les données ne plus sécurisées. La porte est alors ouverte aux pirates. De ce fait, le trafic des données doit donc être protégé, car les données transmises peuvent être lues, manipulées et/ou falsifiées par ces pirates.



Débit des données IPSec en Mbps pour un taille de paquet de 1024 octets



Solution :

Un VPN (Virtual Private Network) est le moyen le plus sécurisé et le plus économique pour protéger les données transmises. Le VPN joue le rôle de tunnel blindé entre récepteur et émetteur. Les intrus n'ont pas accès à ce tunnel. Les données et les e-mails peuvent être échangés en toute sécurité au sein du réseau. De même pour toute conversation téléphonique via Internet - c'est ce que l'on appelle la Voix sur VPN (VoVPN).

Avantages/Points clés :

- ▶ Niveau de sécurité élevé lors du transfert de données via le support de certificats
- ▶ VPN comme technologie de base pour les services avancés, VoIP ou VoVPN
- ▶ Connexion sécurisée des données en Wi-Fi
- ▶ Connexion sécurisée des collaborateurs qui se déplacent au réseau de la société
- ▶ Infrastructure réseau transparente, vue comme réseau unique
- ▶ Secours (backup) RNIS
- ▶ Gestion des certificats

REFERENCES :

ROUTEURS :

LOGICIELS :

COMPOSANTS SUPPLEMENTAIRE :

Fiche applicative Connexion sécurisée des agences et des postes de travail à domicile via VPN

- ▶ Parfumerie Douglas GmbH, Hagen, Allemagne
- ▶ Heinrich Deichmann-Schuhe GmbH & Co. KG, Essen, Allemagne
- ▶ Centrale EDEKA AG & Co. KG, Hamburg, Allemagne
- ▶ Opticiens Krys, Houdan, France
- ▶ Magasins Morgan, Levallois, France
- ▶ Coopératives Système U, Rungis, Mulhouse, France Vendargues, France

bintec série VPN Access

- ▶ Débit de données élevé pour IPSec et PPTP
- ▶ Mémoire interne importante pour gestion de connexions simultanées
- ▶ Matériel redondant avec BRRP
- ▶ Connexion au serveur RADIUS
- ▶ 3x Ethernet pour DMZ
- ▶ Emplacement carte SD

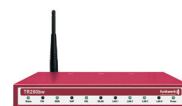
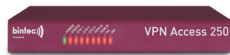
bintec R1200

- ▶ Application diverse avec WAN Ethernet (commutateur 4+1)
- ▶ Accélérateur matériel
- ▶ Equipement pour agence (version de base) ou comme équipement central (+ tunnels par extension de licence)
- ▶ Matériel redondant avec BRRP
- ▶ Connexion au serveur RADIUS
- ▶ Emplacement DSP pour VoIP

bintec R232a(w) / bintec TR200aw

- ▶ Modem ADSL2+, Commutateur 4-ports et Wi-Fi* dans un seul équipement : installation simple
- ▶ Configuration distante pour gestion centralisée
- ▶ 5 tunnels VPN, IPSec, possibilité VoIP
- ▶ Port RNIS (maintenance distante) ou secours DSL
- ▶ TR200aw : intégration RNIS, analogie et téléphonie VoIP (RNIS et analogie interne/externe)

*) excepté pour R232a

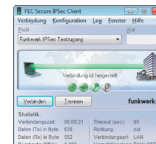


Modèle	bintec VPN250	bintec VPN1000	bintec R1200	bintec R232a(w)	bintec TR200aw
No réf.	22601	22801	24231	24215	501066001
Wi-Fi standard	-	-	(a/b/g)	(b/g)	b/g
Nbre max. de tunnels IPSec	250	1000	110	5	5
VPN avec PPTP	•	•	•	-	-
Equipement "redondant"	•	•	•	-	-
Pre-shared key/certificats	•	•	•	•	•
Conseillé pour	Siège	Siège	Siège/Agence	Agence/Home	Agence/Home



XAdmin

- ▶ Installation sur serveur LAN (Linux)
- ▶ Configuration initiale et mises à jour automatisées/déclenchées par événement
- ▶ Inventaire des routeurs existants et nouveaux
- ▶ Application en environnements RNIS et IP



Client IPSec

- ▶ Logiciel client universel IPSec
- ▶ Niveau de sécurité élevé pour le terminal grâce à la fonction de pare-feu intégrée
- ▶ Connexion sécurisée depuis des points d'accès publics

Logiciel	XAdmin			Client IPSec		
	150 licences	500 licences	illimité	1 licence	5 licences	10 licences
No réf.	80030	80033	80035	80511	80512	80513

Séries packetalarm UTM

Systèmes UTM (Unified Threat Management) pour une protection totale du réseau local. Les équipements packetalarm UTM identifient diverses attaques et menaces en temps réel et effectuent des blocages ciblés.



Funkwerk Enterprise Communications France
6 Allée de la Grande Lande - CS 20102 -
33173 Gradignan

Tél : +33 (0)5 57 35 63 00

Fax : +33 (0)5 56 89 14 05

e-mail : info.france@funkwerk-ec.com

Internet : www.funkwerk-ec.com