HOB Cyber Security

HOBLink VPN 2.1 Gateway

Die VPN-Lösung für mehr Sicherheit und mehr Flexibilität

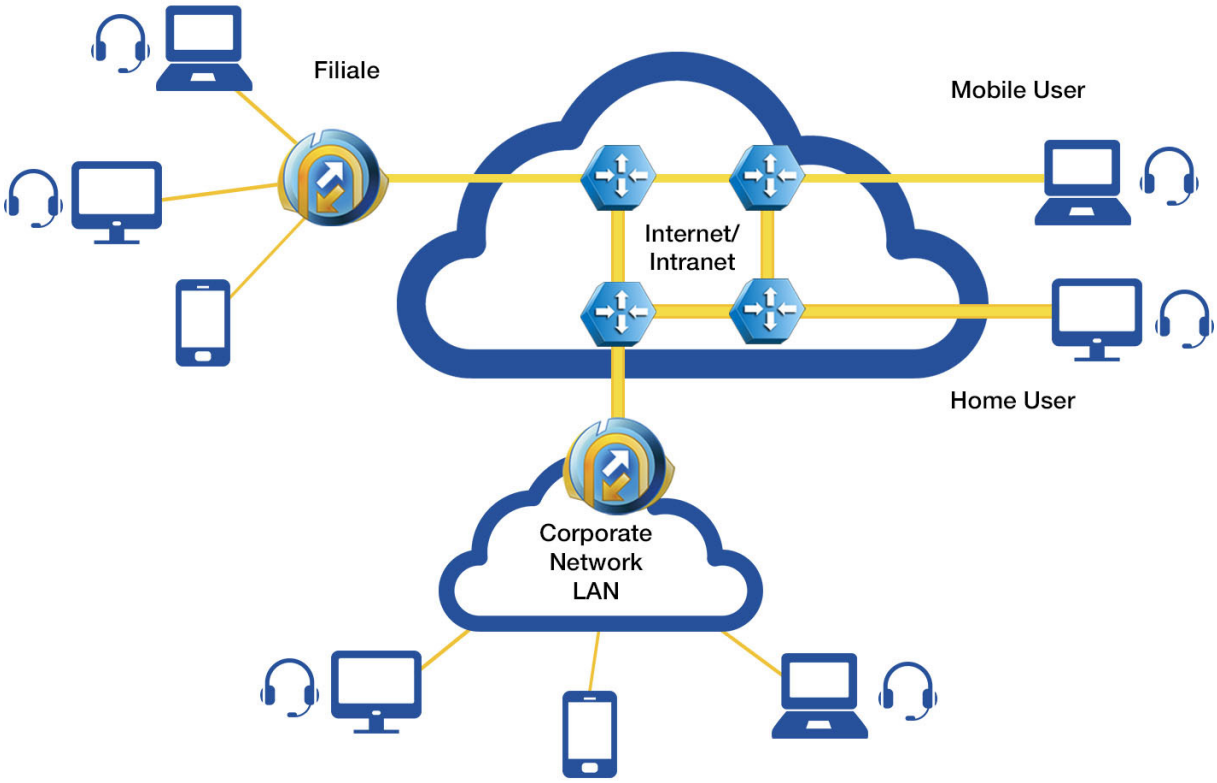
Überblick

Mit HOBLink VPN 2.1 Gateway steigern Unternehmen ihre Kommunikationssicherheit über das Internet und erhöhen ihre Flexibilität erheblich. Basierend auf IPsec VPN und starker Authentifizierung erfolgt eine sichere Anbindung aller Außenstellen und Clients an die zentrale Netzwerkinfrastruktur.

Vorteile auf einen Blick

Mit HOBLink VPN 2.1 Gateway erhalten Sie:

- ein sicheres und flexibles VPN Gateway
- Schutz der gesamten Datenkommunikation im Unternehmen auf Basis der Standards IPsec und IKE/ISAKMP (RFC 2401-ff) mit starker Verschlüsselung und Authentifizierung
- umfassende Unterstützung von Zertifikaten und digitalen Signaturen mit dem integrierten Zertifikat Manager und PKI
- Benutzerauthentisierung mit Radius (z.B. RSA ACE-Server)
- NAT-T (Traversal) / UDP Encapsulation - IPsec über beliebige Router, Firewalls und WLAN Hotspots
- lokale und Browser-basierte Konfiguration und Administration
- eine reine Software-Lösung – ideale Skalierbarkeit



Bespielszenario für den Einsatz von HOBLink VPN Gateway

HOBLink VPN 2.1 Gateway – Spezifikation

Betriebssystem	• Div. Linux, Ubuntu, Red Hat, 32/64 bit
Szenario	• Gateway-Gateway (Peer-to-Peer): nach RFC 2401ff • Client-Gateway: RFC 2401ff • Beispiele: - Apple iOS VPN Client (IPsec) - Android 4 (IPsec) - Windows 7/8 VPN Client (IPsec, IKEv2)
Eingesetzte VPN-Protokolle	• IPsec (AH und ESP im Tunnelmode)
Client Protokolle	• IPsec, L2TP/IPsec (nur mit PAP)
Komprimierung	• IPCOMP/DEFLATE
Benutzer-Authentifizierung	• Lokal • RADIUS • LDAP

Logging	• Syslog
Verschlüsselungen	• AES (128/192/256) • 3DES • RC4 • BLOWFISH • CAST
Authentifizierungen	• HMAC_MD5 • HMAC_SHA1
IPsec Parameter	• Replay-Detection • PFS • SA Lifetime • Dead Peer Detection
IKE Modi Phase 1	• Main Mode • Aggressive Mode • Hybrid Aggressive Mode • XAUTH
IKE Modi Phase 2	• Quick Mode
IKE Verschlüsselung	• AES (128/192/256) • 3DES • BLOWFISH • CAST
IKE Hash-Funktionen	• MD5 • SHA1
IKE Identifikation	• IP-Adresse • FQDN • USER-FQDN
IKE Autthentifizierung	• Symmetrisch: Preshared Secret • DSA-Zertifikate, • RSA-Zertifikate • Asymmetrisch: DSA + User/ Password (hybrid XAUTH) • Benuzerauthentisierung mit RADIUS (z.B. RSA ACE)

IKE Diffie-Hellman-Groups	• 768 - 8192 bit MOD • Elliptic Curve Groups
IKE Parameter	• SA Lifetime • Timeout • Retries
IKE	• IKEv1, IKEv2 • MD5, SHA1 • AES (128, 192, 256), 3DES, BLOWFISH, CAST • PSK, Zertifikate (RSA, DSA) • Main Mode • Aggressive Mode (XAUTH, Hybrid) • IKE Config Mode • Group Identifikation, • FQDN, USER_FQDN, IP-Adresse, • MODP (768 - 8192), Elliptic Curve • NAT detection, NAT-T
IPsec	• AH, ESP, AH/ESP • Tunnel Mode, Transport Mode (L2TP/IPsec) • HMAC_MD5, HMAC_SHA1 • AES(128, 192,256), 3DES, RC4, BLOWFISH, CAST • PFS, Replay Detection, NAT keepalive
Konfiguration	• XML-Datei
NAT (Network Address Translation - Traversal)	• UDP Encapsulation (beliebige VPN Verbindungen über NAT Geräte) • UDP Keepalive

Systemanforderungen

PC Hardware

- Standard PC Server, empf. HP, Dell, IBM
- x86, AMD64
- CD-Laufwerk

Netzwerk-Interface

- LAN/WAN-Adapter

Kompatibilität

- Apple
- Android
- Cisco
- Checkpoint
- Microsoft
- HOB
- und weitere