

Virtual Private Networks (VPN) Security features checklist

Core Security Functionality

Encryption
Bandwidth
Business Continuity
Planning
Denial of Service
Integrity
Data Origin Authentication
Protection against Replay
Attack
Protection against Man-in-
the-Middle Attack
Protection against
Piggyback Attack
Host Security Analysis
VPN Interoperability

Conformance to Protocol Standards

VPN Technology IPsec
VPN Technology TLS
Internet Key Exchange
Transport Layer Security
TLS Certificates

Authentication

Password Management
Password Compatibility
PKI-based Authentication
Multi-factor Authentication

PKI Standards

X.509 Certificates
LDAP Repository
Certificate Revocation
Cryptographic Algorithms

Cryptographic Standards

Encryption Algorithms

Advanced Encryption
Standard (AES)
Triple- Data Encryption
Standard (3DES)

Key Establishment Algorithms

Rivest, Shamir, Adleman
(RSA)
Other algorithms based on
exponentiation of finite
fields
Key Exchange Algorithm
(KEA)
Elliptic Curve algorithms

Digital Signature Algorithms

RSA
Digital Signature Algorithm
(DSA)
Other algorithms based on
exponentiation of finite
fields
Elliptic Curve Digital
Signature Algorithm
(ECDSA)

Hashing Algorithms

SHA-1
SHA-224
SHA-256
SHA-384
SHA-512

Cryptoperiod

Should be appropriate for
the algorithm in use

Assurance Standards

FIPS 140-1
FIPS 140-2
Cryptographic module
Common Criteria (CC)
Evaluation Assurance Level
(EAL) 3 or higher.
Protection Profile or
Security Target

Configurability

Changeable Default Values
Split Tunnelling (IPSec-
based products)
Allow or Disallow
Encryption
Allow or Disallow
Authentication
Logging
Pass-through

Usability

Configuration by Users
Authentication by Users
Maintenance by
Administrators
Reconfiguration by
Administrators

Manageability

Authentication of
Management Traffic
Central Management
Encryption of Management
Traffic

Scalability

Degree of Scalability