



Intrusion Prevention System (IPS) Security Features Checklist

Core Security Functionality

- Known Attacks
- New Attacks
- Signature Updates
- Features Upgrades
- Dedicated Hardware
- Software Updates
- Hardened Operating System
- Detection Methods
- Host IPS
- Network IPS
- Network Awareness
- User Awareness
- Vulnerability Assessment
- Performance Under Load
- Remediation

Conformance to Protocol Standards

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Internet Control Message Protocol (ICMP)

Authentication

- Secure Login
- Integrated Sign-on
- Strong Password
- Password Compatibility

PKI Standards

- X.509 Certificates
- LDAP Repository
- Certificate Revocation
- Cryptographic Algorithms

Cryptographic Standards

Encryption Algorithms

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

Assurance Standards

- FIPS 140-1
- FIPS 140-2

Cryptographic Algorithm Validation Program

- Cryptographic module validated

Common Criteria

- Common Criteria (CC) Evaluation Assurance Level (EAL) 3 or higher.
- Protection Profile or Security Target

Configurability

- Changeable Default Values
- Responses to Non-standard Packets
- Logging
- Adaptive Tuning

Usability

- Roles-based Authorization
- Maintenance by administrator
- Reconfiguration by Administrators

Manageability

- Central Management
- Remote Management
- Authentication of Management Traffic
- Encryption of Management Traffic

Scalability

- Degree of Scalability