

## Firewalls

### Security Features Checklist

#### Core Security Functionality

Dedicated Corporate Firewall  
 Default 'Deny' access  
 Inbound and Outbound Traffic Filter  
 MAC Address Filtering  
 Packet Filtering  
 Source IP Address Filtering  
 Destination IP Address Filtering  
 Source Port Filtering  
 Destination Port Filtering  
 Known-Attacks Filtering  
 Application Level Firewall  
 Application Proxy  
 Generic proxy  
 Session audit  
 Proper Protocol Format Filtering  
 Appropriate IP addresses / URLs Filtering  
 User authentication  
 Enforce Protocol Restrictions  
 Performance Throughput  
 Demilitarized Zone

#### Conformance to Protocol Standards

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

#### Authentication

Password Management  
 Password Compatibility

#### 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 (EC) Digital Signature Algorithm (ECDSA)

##### *Hashing Algorithms*

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

#### Assurance Standards

FIPS 140-1  
 FIPS 140-2

#### Cryptographic Algorithm Validation Program

Cryptographic module validated

#### Common Criteria

Highest available EAL Protection Profile or Security Target

#### Configurability

Changeable Default Values  
 Responses to Non-standard Packets  
 Logging

#### Usability

Configuration by Users

#### Manageability

Central Management  
 Remote Management  
 Unattended Reboot  
 Authentication of Management Traffic  
 Encryption of Management Traffic

#### Scalability

Degree of Scalability