13951018

CPA SECURITY CHARACTERISTIC

IPSEC SECURITY GATEWAY

Version 1.1

Document History

Version	Date	Description
1.0	October 2010	Final Draft
1.1	March 2012	Update for publishing

This Security Characteristic is derived from the following files

File Name	Version
Software VPN Threats - System Profile	1.1
Software VPN Threats – Gateway Profile	1.1
Common Libraries	1.5
Hardware Libraries	1.3
Crypt Libraries	1.4
Generic Network Device	0.2

Soft copy location

DiscoverID 13951018

This document is authorised by:

Deputy Technical Director (Assurance), CESG

This document is issued by CESG

For queries about this document please contact:

CPA Administration Team
CESG
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX
United Kingdom

Tel: +44 (0)1242 221 491
Email: cpa@cesg.gsi.gov.uk

The CPA Authority may review, amend, update, replace or issue new Scheme Documents as may be required from time to time.

CONTENTS

REFERENCES

[a] The Process for Performing Foundation Grade CPA Evaluations, v1.3, August 2011, CESG

[b] RFC4301 Security Architecture for the Internet Protocol, December 2005

[c] RFC4303 IP Encapsulating Security Payload (ESP), December 2005

[d] RFC5996 Internet Key Exchange Protocol Version 2 (IKEv2), September 2010

[e] RFC3602 The AES-CBC Cipher Algorithm and Its Use with IPsec, September 2003

[f] RFC5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile), May 2008

[g] RFC4868 Using HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512 with IPsec, May 2007

[h] RFC2408, Internet Security Association and Key Management Protocol (ISAKMP), November 1998

[i] RFC2409, The Internet Key Exchange, November 1998

[j] CESG Architectural Patterns No. 2, Walled Gardens for Remote Access. Issue 1.0, March 2011 (UNCLASSIFIED). Available from the CESG IA Policy Portfolio.

[k] CESG Technical Specifications No. 5 - PRIME Framework - Suite B.128 Module. Issue 1.1.1, July 2011 (UNCLASSIFIED). Available from the CESG IA Policy Portfolio.

[l] RFC4106 The Use of Galois Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP), June 2005

[m] RFC4304 Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP), December 2005

I. OVERVIEW

1. This document is a CPA Security Characteristic – it describes requirements for a particular type of assured product for evaluation and certification under CESG's Commercial Product Assurance (CPA) scheme.

A. Product Aims

2. An IPsec Security Gateway is an endpoint for an IPsec Virtual Private Network (VPN) tunnel, from either a VPN client or another Security Gateway. The IPsec tunnel provides the end user with secure corporate network connectivity over a less trusted network.

3. "IPsec Security Gateway", as referred to in this Security Characteristic refers to either hardware or software solutions that provide VPN functionality.

B. Typical Use Case(s)

4. There are two common use cases for IPsec security gateways, Client to Gateway and Gateway to Gateway.

- **Client to Gateway**

5. IPsec is used to provide a virtual network between a remote device, on which a client product is installed, and an organisation's Security Gateway at the boundary of its enterprise network. In this scenario, it is assumed that multiple client devices will connect to a single gateway.

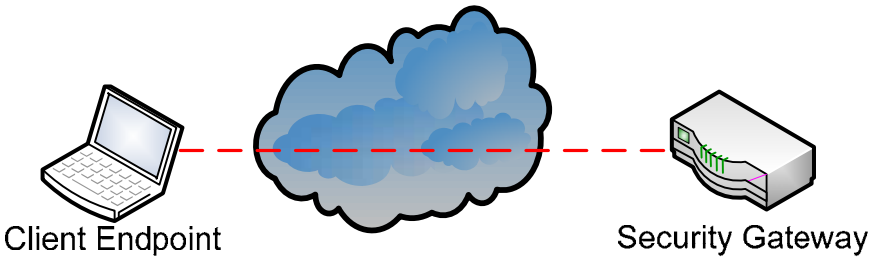

Figure 1 - The Client to Security Gateway IPsec model

- **Gateway to Gateway**

6. A VPN tunnel is formed between a pair of Security Gateways, and is often used to provide a secure overlay on a public network to join multiple fixed networks together.

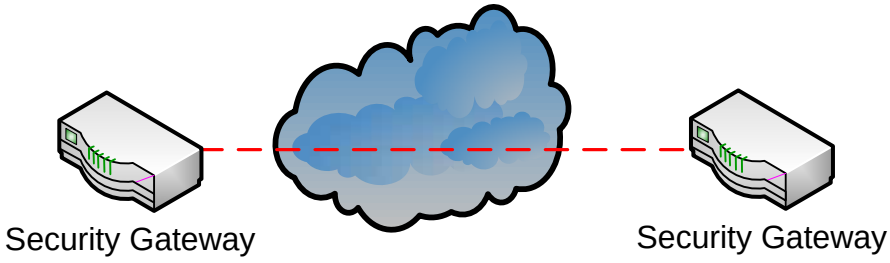

Figure 2 - The Security Gateway to Security Gateway model

C. Expected Operating Environment

7. A Security Gateway is expected to be installed within a physically secure environment and logically sited at the boundary of a security domain, bordering a less trusted network (such as the Internet).

8. In the envisaged architecture (see Figures 1 and 2), all traffic that is generated within the local security domain for recipients outside of the domain, will be routed to the gateway. The gateway will then apply confidentiality, integrity and/or authentication cryptographic protection, according to rules determined by the gateway's policy. The resultant traffic will then be sent over the less trusted network to the Client endpoints. This process is reversed for traffic inbound from the Client to the corporate network.

9. Where an IPsec Security Gateway is being used as part of a remote working VPN deployment, the guidance and patterns described in the CESG Walled Garden Architectural Pattern[j] should be followed.

D. Compatibility

10. A Security Gateway product may exist as either a dedicated hardware device or as one or more software modules, deployed on a general purpose platform.

11. In either case, this Security Characteristic does not place any specific hardware requirements upon the product beyond its normal technical requirements. For example, some products may have specific CPU or memory requirements in order to function effectively. This Security Characteristic does not define minimum hardware requirements.

E. Interoperability

12. This Security Characteristic assumes that the security gateway is deployed as described in RFC5996 - Internet Key Exchange Protocol Version 2(IKEv2) [d], in either the endpoint to security gateway model, Figure 1, or in the security gateway to security gateway model as shown in Figure 2. Therefore the security gateway must interoperate with other IPsec devices.

13. To ensure interoperability, this Security Characteristic is designed for products that are compliant with the relevant RFCs for IPsec [b] and have passed testing to ensure that they correctly operate with other IPsec implementations. In addition to ensuring RFC compliance this has the additional benefit of enabling deployments to make use of a range of different IPsec VPN clients or gateways based on their particular business and technology requirements.

14. Products conforming to this Security Characteristic must support at least one of the following IPSec Profiles:

- PSN End-State IPsec Profile (Preferred)
- PSN Interim IPsec Profile (Supported until 2015)
- Manual V Legacy IPsec Profile (Supported until December 2012)

After each ‘supported until’ date has passed, the corresponding IPsec profile will be removed from this Security Characteristic for new certifications. This does not mean that certificates will be invalidated or that deployments will need to replace currently certified products.

- **PSN End-State IPsec Profile**

The PSN end-state IPsec profile is completely specified in the following:

- PRIME Framework: Base Module, v1.1.1
- PRIME Framework: Suite Definition Module - Suite B.128, v1.1.1
- PRIME Framework: Authentication Module – X.509 via CERTREQ, v1.1.1
- PRIME Framework: IKEv2 NAT Traversal Module, v1.1.1

In the future, this profile will be migrated to the latest version of these documents (currently v1.2.0).

Table 1 provides a non-authoritative summary of Suite B.128:

ESP	
Encryption	AES-128 in GCM
IKEv2	
Encryption	AES-128 in GCM
Pseudo-random function	HMAC-SHA256-128
Diffie-Hellman group	256bit random ECP, Group 19
Authentication	ECDSA-256 with SHA256 on P-256 curve

Table 1

- **PSN Interim IPsec Profile**

The PSN Interim IPsec profile consists of an RFC-compliant implementation of IPsec with IKEv1 (RFCs 2408 and 2409 apply) using Extended Sequence Numbers[m] and the algorithms given in Table 2 below.

Encryption	AES128_ CBC
PRF	SHA-1
Diffie-Hellman Group	Group 5 (1536 bits)
Signature	RSA with X.509 certificates

Table 2

- **Manual V Legacy IPsec Profile**

The Manual V legacy IPsec profile consists of an RFC-compliant implementation of IPsec with IKEv1 (RFCs 2408 and 2409 apply) using Extended Sequence Numbers[m] and the algorithms given in Table 3 below.

Encryption	AES128_ CBC
PRF	SHA-1
Diffie-Hellman Group	Group 19
Signature	RSA with X.509 certificates

Table 3

F. Variants

15. This Security Characteristic has two variants, either of which can be selected to implement an IPsec Security Gateway. These variants are:

- **Software Gateway** - The VPN Gateway is software that is deployed onto standard server hardware running a general purpose operating system.
- **Hardware Gateway** - The VPN Gateway is a dedicated appliance, for direct deployment into a network.

G. High Level Functional Components

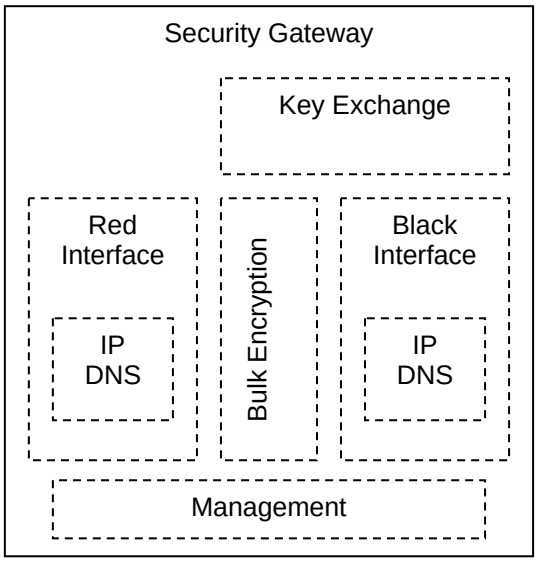

Figure 3 – Functional Components of an IPsec Security Gateway

16. Figure 3 shows the functional components of an IPsec security gateway which are considered for this Security Characteristic. The primary function of the IPsec Security Gateway is to encrypt or decrypt traffic traversing the product.

17. **Red Interface:** The connection to the trusted network which passes all traffic destined for the other endpoint to the bulk encryption.

18. **Bulk Encryption**: Traffic is encrypted or decrypted dependant on its source and destination.

19. **Black Interface**: The connection to the less trusted network.

20. **Red/Black DNS**: When DNS requests are received they are processed as necessary by the bulk encryption and then handled by the DNS proxy, the responses are then passed on to their destination.

21. **Key Exchange:** Negotiates the traffic encryption keys, the requirements for both the key exchange and the bulk encryption are described in the IPsec profile below.

22. **Management:** Provides the functionality to control and configure the security gateway.

H. Future Enhancements

23. CESG welcomes feedback and suggestions on possible enhancements to this Security Characteristic.

24. A future release is likely to remove the interim IPsec profile and require the use of the PRIME B.128 profile[k].

25. A future release is likely to include support for the use of trusted computing technology, such as Trusted Platform Modules.

II. SECURITY CHARACTERISTIC FORMAT

26. All CPA Security Characteristics contain a list of mitigations which are split into three requirement categories: development, verification and deployment requirements. Within each of these sets the mitigations can be grouped based on areas of the product (as illustrated in the High Level Functional Component Diagram above), such as bulk encryption or authentication, or they may be overarching requirements which apply to the whole product. Reference [a] describes how evaluation teams should interpret SECURITY CHARACTERISTIC.

27. The three types of mitigations are denominated as follows:

- **DEV** – These are mitigations that are included by the developer during the design or implementation of the product. These are validated via a review of the product's design or implementation during a CPA evaluation.

- **VER** – Verification mitigations are specific mitigations that the evaluator must test during the assessment of the product.

- **DEP** – Deployment mitigations are points that must be considered by users or administrators during the deployment of the product. These mitigations are incorporated into the security procedures for the product.

28. Each mitigation includes informational text in italics, describing the threat that it is expected to mitigate. It also lists at least one specific mitigation, which describes what must actually be done to achieve that requirement. In some cases there is additional explanatory text which expands upon these requirements.

29. In the requirements listed below, the following terminology can be used:

- 'Must', 'Mandatory' and "Required" are used to express a mitigation that is essential. All mitigations and detailed mitigations are mandatory unless there is an explicit caveat, such as 'if supported by the product'.

- 'Should' and 'Strongly Recommended' are used whenever a requirement is highly desirable, but is not essential. These are likely to become mandatory in future iterations of the SECURITY CHARACTERISTIC.

- 'Could' and 'Recommended' are used to express a non-mandatory requirement that may enhance security or functionality.

30. For example:

DEV.M1: [A mitigation]
This mitigation is required to counter [a threat]
At Foundation the product must [do something].
This can be achieved by [explanatory comment].

III. REQUIREMENTS

A. Design Mitigations

DEV.1 - Design >> Management

DEV.1.1 - Design >> Management >> Logging

DEV.1.M355: Sanitise logged data

This mitigation is required to counter supplying a malicious script through logged data

At Foundation Grade the product is required to ensure logged data is appropriately sanitised prior to display

The method and content of sanitisation will change depending on the content in the logs and where the logs are displayed. For example, output to a HTML viewer for the logs will need to be encoded whereas logging output to a text file may not need to be sanitised.

DEV.1.M358: Inform administrator of account activity

This mitigation is required to counter exploitation of poor management of passphrases by the administrator

This mitigation is required to counter dictionary and exhaustion attacks

At Foundation Grade the product should display recent authentication history

It is recommended that on login the user be notified of the date and time of the last successful login and any failed login attempts since the last successful login.

If recent authentication history is displayed, it is strongly recommended that users are told what to do, preferably on the screen, if the history is not what is expected.

DEV.1.M359: Anti Hammer

This mitigation is required to counter dictionary and exhaustion attacks

At Foundation Grade the product is required to have a mechanism for limiting the rate of login attempts

DEV.1.M374: Protect access to logs

This mitigation is required to counter modification of logging generation

This mitigation is required to counter sanitisation of illegitimate access from logs

At Foundation Grade the product is required to provide ability to automatically push logs to external device

At Foundation Grade the product is required to ensure that only an authenticated administrator can manage logs

At Foundation Grade the product is required to not overwrite logs without alerting the administrator

At Foundation Grade the product is required to ensure that all logs are time stamped

Timestamps must be accurate and the deployment must take measures to ensure this.

Such measures could be NTP synchronisation or a manual process.

DEV.2 - Design >> Key Exchange

DEV.2.M58: RFC compliant implementation

This mitigation is required to counter exploitation of a vulnerability in the key exchange

At Foundation Grade the product should implement RFC5996 compliant IKEv2, if it does not support IKEv2 then it must implement RFC2408/RFC2409 compliant IKEv1.

The implementation must function correctly without custom extensions. Furthermore, implementations of either IKEv1/2 should be interoperable with other IKE implementations of the same class.

DEV.2.M79: Support mutual authentication

This mitigation is required to counter redirection to a fake gateway via a Man-in-the-Middle attack (on DNS, routing etc)

At Foundation Grade the product is required to use X.509 certificates to mutually authenticate all connections.

Certificate verification must include full certificate chain verification and access to the current certificate revocation list

DEV.2.M140: Smooth output of entropy source with approved PRNG

This mitigation is required to counter predictable key generation due to a weak entropy source

At Foundation Grade the product is required to employ a PRNG of sufficient Security Strength for all random number generation required in the operation of the product

For more details on a suitable PRNG, please see the Process for Performing Foundation Grade Evaluations.

DEV.2.M141: Reseed PRNG as required

This mitigation is required to counter the prediction of randomly generated values due to repeating PRNG output

At Foundation Grade the product is required to follow an approved reseeding methodology

DEV.2.M290: Employ an approved entropy source

This mitigation is required to counter predictable key generation due to a weak entropy source

At Foundation Grade the product is required to generate random bits using an entropy source whose entropy generation capability is understood

The developer must provide a detailed description of the entropy source used, giving evidence that it can generate sufficient entropy for use in the device, including an estimate of entropy per bit.

If a hardware noise source is used, then the manufacturer's name, the part numbers and details of how this source is integrated into the product must be supplied. If a software entropy source is employed, the API calls used must be provided. Where appropriate, details must be given of how the output of multiple entropy sources are combined.

DEV.2.M292: State the Security Strength required for key generation

This mitigation is required to counter predictable key generation due to a weak entropy source

At Foundation Grade the product is required to employ an entropy source of sufficient Security Strength for all random number generation required in the operation of the product

The developer must state the Security Strength required of their entropy source based on analysis of all random numbers used in the product. At this grade, the Security Strength is likely to be 128 bits for products that do not use elliptic curve cryptography. For elliptic curve-based asymmetric mechanisms it is likely to be 256 bits, and for finite field based asymmetric mechanisms it is likely to be 192 bits.

DEV.3 - Design >> Bulk Encryption

DEV.3.M58: RFC compliant implementation

This mitigation is required to counter exploitation of a vulnerability in the bulk algorithm

At Foundation Grade the product is required to implement RFC4301 compliant IPsec.

The implementation must only make use of the requirements for the standard as specified within the RFC.

DEV.3.M337: Support approved IPsec Profile

This mitigation is required to counter exploitation of a weak algorithm
This mitigation is required to counter exploitation of a weakness in a vulnerable cryptographic protocol

At Foundation Grade the product is required to support RFC4303 compliant ESPv3, with the IPsec profile specified above, using both confidentiality and integrity protection

DEV.4 - Design >> Gateway

DEV.4.M22: Update signing

This mitigation is required to counter installing compromised software using the update process

At Foundation Grade the product should use cryptographically signed updates and verify their signatures before installation, if an update mechanism is present.

DEV.4.M28: Code is signed and verified

This mitigation is required to counter installation of malware on host

At Foundation Grade the product is required to ensure all code is cryptographically signed and ensure that the signatures are verifiable against a trusted copy of the manufacturer's public key by the host platform, prior to initial installation and on loading

The digital signature algorithm must be ECDSA-256 or DSA-1536/192 and the hash algorithm must be SHA1 or SHA-256.

If there are additional resources as part of the installation package, such as configuration files, then these must also be signed.

DEV.4.M41: Crash reporting

This mitigation is required to counter exploitation of a software implementation error

At Foundation Grade the product is required to ensure crashes are logged

Where it is possible that sensitive data may end up in the crash data, this must be handled as red data and must only be available to an administrator. Crash data from both the product and the underlying operating system must be considered.

DEV.4.M42: Heap hardening

This mitigation is required to counter exploitation of a software implementation error

At Foundation Grade the product is required to use the memory management provided by the operating system, products should not implement their own heap

DEV.4.M43: Stack protection

This mitigation is required to counter exploitation of a software implementation error

At Foundation Grade the product is required to be compiled with support for stack protection in all libraries, where the tool chain supports it

If more recent versions of the toolchain support it for the target platform then they should be used in preference to a legacy toolchain.

DEV.4.M46: (Software Gateway ONLY) User least privilege

This mitigation is required to counter taking advantage of existing user privilege

At Foundation Grade the product is required to operate correctly from a standard account without elevated privileges

DEV.4.M63: Credentials bound to physical device

This mitigation is required to counter client connecting to a spoofed gateway

At Foundation Grade the product is required to present an X.509 machine certificate to authenticate the identity of the gateway during the key exchange.

DEV.4.M64: All secrets can be purged before disposal

This mitigation is required to counter recovery of secrets from a decommissioned device

At Foundation Grade the product is required to provide the capability to delete or revoke all private and symmetric keys during disposal

DEV.4.M66: (Software Gateway ONLY) Ephemeral keys protected from high risk processes

This mitigation is required to counter a compromised client exfiltrating keys

At Foundation Grade the product is required to use operating system mechanisms (process separation etc) to protect ephemeral secrets

'High Risk' is by default defined as processes which are network facing, run with high privileges or are otherwise directly reachable by an adversary. If a developer has used a different approach to determine whether to enable these defences, this should be recorded in the evaluation report.

DEV.4.M67: Long term keys protected from high risk processes

This mitigation is required to counter exploitation of unintended information disclosure to leak keys/secrets

This mitigation is required to counter a compromised client exfiltrating keys

At Foundation Grade the product is required to use operating system mechanisms, such as user privileges and the OS certificate store, or another protected certificate store, to ensure that unencrypted private keys cannot be retrieved. This must include protecting any APIs or interfaces added by the product which have access to the certificate store.

DEV.4.M68: Sanitisation of buffers

This mitigation is required to counter exploitation of unintended information disclosure to leak keys/secrets

At Foundation Grade the product is required to actively erase memory buffers containing private/symmetric keys after use

DEV.4.M109: Protection of sensitive data lines

This mitigation is required to counter installation of hardware-level malware

At Foundation Grade the product is required to ensure physical access to internal data lines carrying sensitive data requires breaching of the tamper protection

In this context, sensitive data is defined as key material, user data and configuration data.

DEV.4.M123: Traffic keys are never stored in persistent storage

This mitigation is required to counter recovery of secrets from a decommissioned device

This mitigation is required to counter recovery of secrets from a lost/stolen device

At Foundation Grade the product is required to store traffic keys in 'pinned' or otherwise protected memory that is not swapped. Traffic keys must not be stored in persistent storage which is accessible without breaching the tamper protection.

DEV.4.M159: Update product

This mitigation is required to counter exploitation of a software implementation error

This mitigation is required to counter exploitation of a software logic error

At Foundation Grade the product should support the use of software updates

DEV.4.M267: Provide an automated configuration tool to enforce required settings

This mitigation is required to counter exploitation of an accidental misconfiguration

At Foundation Grade the product is required to be provided with a configuration tool, or other method, for an administrator to initially set it up into a suitable configuration

If the product requires more than 12 options to be changed or set by an administrator to comply with these Security Characteristics, the developer must supply a tool or policy template which helps the administrator to achieve this in fewer steps

DEV.4.M321: Data Execution Protection

This mitigation is required to counter exploitation of a software implementation error

At Foundation Grade the product is required to support Data Execution Protection (DEP) when enabled on its hosting platform and must not opt out of DEP

If the product is to be specifically deployed on a platform that does not support either Software DEP or Hardware-enforced DEP, there is no requirement for DEP compatibility.

DEV.4.M340: Address Space Layout Randomisation

This mitigation is required to counter exploitation of a software implementation error

At Foundation Grade the product is required to be compiled with full support for ASLR, including all libraries used

ASLR may be disabled for specific aspects of the product, provided there is justification of why this is required.

DEV.4.M344: Terminate connections with revoked certificates

This mitigation is required to counter an attacker gaining access to credentials on a remote access device

At Foundation Grade the product is required to check certificate revocations at least once per day and terminate any connections where the certificate has been revoked.

DEV.4.M345: Reject connections from tunnel endpoints presenting a revoked certificate

This mitigation is required to counter an attacker gaining access to credentials on a remote access device

At Foundation Grade the product is required to support revocation of endpoint certificates, and reject any connection which attempts to use a revoked certificate to authenticate.

DEV.4.M360: Ensure product security configuration can only be altered by an authenticated system administrator

This mitigation is required to counter unauthorised alteration of product's configuration

At Foundation Grade the product is required to ensure that a change of the products security enforcing settings requires an authenticated administrator

The only security enforcing setting a user should be able to change is their passphrase.

DEV.4.M382: Block unauthenticated traffic

This mitigation is required to counter exploitation of host via un-encrypted traffic

At Foundation Grade the product is required to drop all traffic received via the black interface which is not encrypted

This should be achieved by decrypting and integrity checking all traffic received via the black interface. Traffic which fails the integrity check and any unencrypted traffic must be dropped.

DEV.4.M383: Control export of non-encrypted private keys/machine certificates

This mitigation is required to counter export of secrets through an available API
This mitigation is required to counter recovery of secrets from a lost/stolen device

At Foundation Grade the product is required to control the export of long term secrets, such as private keys or machine certificates, through any available API, unless authenticated as a privileged user.

The product should encrypt long term secrets before allowing them to be exported.

DEV.4.1 - Design >> Gateway >> Black Interface

DEV.4.1.M85: Resource prioritisation

This mitigation is required to counter memory exhaustion through 'half open' attacks
This mitigation is required to counter CPU exhaustion through repeated connect requests

At Foundation Grade the product should limit resources which can be consumed by a single client

At Foundation Grade the product is required to prioritise resources for connections which are already open

This should be done at the expense of new, unauthenticated connections.

DEV.4.1.M381: Minimise presented protocols

This mitigation is required to counter exploitation of host via un-encrypted traffic

At Foundation Grade the product is required to be configurable such that it presents only the protocols required for correct functionality

It is anticipated, but not required, that these protocols may include those necessary to perform IPsec, key exchange, session initiation, routing, DNS, ARP and DHCP.

Any other protocols that the product requires to be exposed on the black interface in order to function must be documented and explained fully.

B. Verification Mitigations

VER.M4: Evaluation/Cryptocheck

This mitigation is required to counter exploitation of a cryptographic algorithm implementation error

At Foundation Grade the evaluator will ensure all cryptographic algorithms employed for security functionality have been validated as per the "Cryptographic Validation" section in the CPA Foundation Process document

VER.1 - Verify >> Bulk Encryption

VER.1.M328: RFC compliant IPsec implementation

This mitigation is required to counter exploitation of a vulnerability in the bulk algorithm

At Foundation Grade the evaluator will ensure that the product has passed an IPsec interoperability test

The product should pass IPsec interoperability testing with an independent implementation of the protocol. This could be done through VPN Consortium testing or other interoperability testing.

VER.1.M387: Perform IPsec robustness testing

This mitigation is required to counter exploitation of a vulnerability in the bulk algorithm

At Foundation Grade the evaluator will demonstrate that the IPsec protocol is robust to fuzz testing, as described in The Process for Performing Foundation Grade CPA Evaluations

VER.2 - Verify >> Key Exchange

VER.2.M389: RFC compliant IKE implementation

This mitigation is required to counter exploitation of a vulnerability in the key exchange

At Foundation Grade the evaluator will ensure that the product has passed an IKE interoperability test

The product should pass IKE interoperability testing with an independent implementation of the protocol.

The test should also include negative testing of invalid, expired and revoked certificates, to ensure that the product correctly uses the certificate revocation list and fails securely in the event of a malformed certificate.

VER.2.M390: Perform IKE robustness testing

This mitigation is required to counter exploitation of a vulnerability in the key exchange

At Foundation Grade the evaluator will demonstrate that the IKE/IKEv2 and the X509 certificate parser are robust to fuzz testing, as described in The Process for Performing Foundation Grade CPA Evaluations

VER.3 - Verify >> Gateway

VER.3.M341: (Software Gateway ONLY) Audit permissions on product install

This mitigation is required to counter exploitation of a privileged local service

At Foundation Grade the evaluator will audit any system permissions and ACLs set or altered by the product during installation to ensure that no changes are made, which would give a standard user the ability to modify any components that run with higher privileges (either product or system provided).

VER.3.M347: Verify update mechanism

This mitigation is required to counter installing compromised software using the update process

At Foundation Grade the evaluator will validate the developer's assertions regarding the suitability and security of their update process

The update process must provide a mechanism by which updates can be authenticated before they are applied.
The process and any configuration required must be documented within the Security Procedures.

VER.3.1 - Verify >> Gateway >> Black Interface

VER.3.1.1 - Verify >> Gateway >> Black Interface >> IP

VER.3.1.1.M80: Protocol robustness testing

This mitigation is required to counter discovery of a vulnerability in the implementation of the protocol

At Foundation Grade the evaluator will perform testing using commercial fuzzing tools

Fuzz testing is described in more detail in the Process for Performing Foundation Grade Evaluations.

VER.3.1.2 - Verify >> Gateway >> Black Interface >> DNS

VER.3.1.2.M80: Protocol robustness testing

This mitigation is required to counter discovery of a vulnerability in the implementation of the protocol

At Foundation Grade the evaluator will perform testing using commercial fuzzing tools

Fuzz testing is described in more detail in the Process for Performing Foundation Grade Evaluations.

VER.3.2 - Verify >> Gateway >> Management

VER.3.2.M52: Management application audited for weak permissions

This mitigation is required to counter privilege escalation on the management application

At Foundation Grade the evaluator will audit the system to ensure the registry or file systems cannot be modified to influence higher privilege processes

VER.3.3 - Verify >> Gateway >> Red Interface

VER.3.3.1 - Verify >> Gateway >> Red Interface >> IP

VER.3.3.1.M80: Protocol robustness testing

This mitigation is required to counter discovery of a vulnerability in the implementation of the protocol

At Foundation Grade the evaluator will perform testing using commercial fuzzing tools

Fuzz testing is described in more detail in the Process for Performing Foundation Grade Evaluations.

VER.3.3.2 - Verify >> Gateway >> Red Interface >> Management

VER.3.3.2.M80: Protocol robustness testing

This mitigation is required to counter discovery of a vulnerability in the implementation of the protocol

At Foundation Grade the evaluator will perform testing using commercial fuzzing tools

Fuzz testing is described in more detail in the Process for Performing Foundation Grade Evaluations.

VER.3.3.3 - Verify >> Gateway >> Red Interface >> DNS

VER.3.3.3.M80: Protocol robustness testing

This mitigation is required to counter discovery of a vulnerability in the implementation of the protocol

At Foundation Grade the evaluator will perform testing using commercial fuzzing tools

Fuzz testing is described in more detail in the Process for Performing Foundation Grade Evaluations.

C. Deployment Mitigations

DEP.1 - Deploy >> Management

DEP.1.M282: Initial passphrase is changed on first use

This mitigation is required to counter use of system default passphrases

At Foundation Grade the deployment is required to ensure passphrase is changed on first logon

The system must force users to use an initial passphrase once only, i.e. forces the passphrase to change on first logon.

It is strongly recommended that initial passphrases have a limited lifetime between generation and first use that is as short as is practicable.

DEP.1.M356: Provide guidance on passphrase management

This mitigation is required to counter a social engineering attack on the administrator

This mitigation is required to counter exploitation of poor management of passphrases by the administrator

This mitigation is required to counter dictionary and exhaustion attacks

This mitigation is required to counter poor passphrase storage

At Foundation Grade the deployment is required to provide training to administrators on passphrase management

Administrators should be provided with guidance regarding the secure handling of passphrases which allow access to sensitive systems.
Administrators must be taught never to disclose passphrases, even to their superiors.
Administrators must also be made aware of the risks of using protectively marked devices in public or untrusted areas. Passphrases should not be entered in areas where others could see them being entered.
An administrator must not use passphrases in more than one system.

At Foundation Grade the deployment is required to ensure any hardcopies of passphrases are stored securely

At Foundation Grade the deployment should educate administrators about social engineering methods used by attackers

DEP.1.M357: Suitable passphrase length and complexity

This mitigation is required to counter exploitation of poor management of passphrases by the administrator

This mitigation is required to counter dictionary and exhaustion attacks

At Foundation Grade the deployment is required to ensure passwords are at least 8 characters long

User generated passphrases are acceptable, but machine generated passphrases should be used where possible.

DEP.1.M372: Log all relevant actions

This mitigation is required to counter modification of logging generation

At Foundation Grade the deployment is required to automatically export logs to management/red side device

At Foundation Grade the deployment is required to configure the product to log capture all actions deemed of interest

Ensure that log data is detailed enough to allow forensic investigation during any incident management.

Sensitive data such as passwords and keys must not be written to the logs.

DEP.1.M373: Monitor logs for unexpected entries

This mitigation is required to counter modification of logging generation

This mitigation is required to counter sanitisation of illegitimate access from logs

At Foundation Grade the deployment is required to assess impact of entries and follow organisational procedures for incident resolution

DEP.2 - Deploy >> Key Exchange

DEP.2.M388: Enable mutual authentication

This mitigation is required to counter redirection to a fake gateway via a Man-in-the-Middle attack (on DNS, routing etc)

At Foundation Grade the deployment is required to configure the device to use X.509 certificates to mutually authenticate all connections.

Certificate verification must include full certificate chain verification and access to the current certificate revocation list

DEP.3 - Deploy >> System

DEP.3.M35: Protect provisioning service

This mitigation is required to counter compromise credential/key provisioning workstation/server

At Foundation Grade the deployment is required to limit access to the VPN provisioning service to authorised users

This includes both physical and network access

DEP.4 - Deploy >> Gateway

DEP.4.M26: Physical tamper evidence

This mitigation is required to counter physical compromise of device

This mitigation is required to counter installation of hardware-level malware

At Foundation Grade the deployment is required to educate users to regularly check that tamper labels are intact

At Foundation Grade the deployment is required to provide administrators with advice on the tamper threat

Advice should include looking for possible damage to tamper evident seals.

In the event of tampering, the event should be reported as soon as possible and the product must be removed from use immediately. Any product that shows evidence of tampering must not be returned to service.

At Foundation Grade the deployment is required to place tamper evident seals over access points on product

Use tamper evidence (e.g. stickers) to make entry to system internals detectable by physical inspection. Tamper stickers should be uniquely identifiable to prevent an attacker successfully replacing it with a new, undamaged sticker.

DEP.4.M30: Detect modification to system

This mitigation is required to counter installation of malware on host

At Foundation Grade the deployment is required to be configured in line with good IT practice as part of a risk-managed accredited system

Typically, this will include the installation and subsequent updating of a commercial antivirus product

DEP.4.M38: Use automated configuration tool

This mitigation is required to counter exploitation of an accidental misconfiguration

At Foundation Grade the deployment is required to be configured using automated tools if provided

DEP.4.M39: Audit log review

This mitigation is required to counter exploitation of a software implementation error

This mitigation is required to counter exploitation of a software logic error

At Foundation Grade the deployment is required to regularly review audit logs for unexpected entries

DEP.4.M46: (Software Gateway ONLY) User least privilege

This mitigation is required to counter taking advantage of existing user privilege

At Foundation Grade the deployment is required to ensure all user accounts have the fewest privileges required to enable business functionality

DEP.4.M75: Protect installed equipment

This mitigation is required to counter export of secrets through physical interfaces

This mitigation is required to counter recovery of secrets from a lost/stolen device

At Foundation Grade the deployment is required to install equipment in a secure facility

The equipment should be deployed in an appropriately accredited data centre for the protective marking of the data that that the device is handling.

DEP.4.M130: Purge all secrets before disposal

This mitigation is required to counter recovery of secrets from a decommissioned device

At Foundation Grade the deployment is required to revoke all client certificates and the gateway certificate prior to disposal

DEP.4.M131: (Software Gateway ONLY) Operating system verifies signatures

This mitigation is required to counter installation of a malicious privileged local service

At Foundation Grade the deployment is required to ensure that signature verification is enabled for applications, services and drivers in the host operating system, where available

DEP.4.M159: Update product

This mitigation is required to counter exploitation of a software implementation error

This mitigation is required to counter exploitation of a software logic error

At Foundation Grade the deployment is required to update to the latest version where possible

DEP.4.M332: Secure certificate distribution

This mitigation is required to counter exploitation of the key management process

This mitigation is required to counter inadvertent issue of credentials to the attacker

At Foundation Grade the deployment is required to provision machine certificates to gateways in a secure manner

Configuration of the VPN and installation of the machine certificates must be done by trusted personnel in an appropriately accredited, secure environment. When a replacement certificate is provisioned for a gateway, the compromised certificate must be revoked.

DEP.4.M339: User endpoint is free of malware

This mitigation is required to counter installation of malware on host

At Foundation Grade the deployment is required to use only managed endpoints and, where possible, keep software (including antivirus products) up to date

DEP.4.M340: Address Space Layout Randomisation

This mitigation is required to counter exploitation of a software implementation error

At Foundation Grade the deployment is required to enable ASLR in the host Operating System where available

DEP.4.M342: Use Trusted PKI

This mitigation is required to counter client connecting to a gateway presenting a certificate issued by a compromised CA

This mitigation is required to counter client connecting to a gateway presenting a certificate issued by an untrusted delegated CA

This mitigation is required to counter client connecting to a spoofed gateway

At Foundation Grade the deployment is required to use an X.509 gateway certificate which is chained to a trusted, non-public, certificate authority to enable revocation of the gateway certificate and prevent issue of fraudulent certificates.

DEP.4.M346: Use assured Tunnel Endpoint

This mitigation is required to counter exploitation of unassured client

At Foundation Grade the deployment is required to use a CPA Foundation Grade VPN Client or a CPA Foundation Grade IPsec Security Gateway as the IPsec Tunnel Endpoint

DEP.4.M348: Administrator authorised updates

This mitigation is required to counter installing compromised software using the update process

At Foundation Grade the deployment is required to confirm the source of updates before they are applied to the system

The administrator is required to have authorised the updates before use. If an automatic process is used, the administrator must also configure the product to authenticate updates.

The administrator is required to use the update process described within the Security Procedures.

DEP.4.1 - Deploy >> Gateway >> Black Interface

DEP.4.1.M121: Control access to management interface

This mitigation is required to counter exploitation of a vulnerability in the management protocol

This mitigation is required to counter use of a poorly protected management interface

At Foundation Grade the deployment is required to disable management interfaces on black network

Where required, remote management may still be performed via the encrypted tunnel.

DEP.4.2 - Deploy >> Gateway >> Management

DEP.4.2.M50: Role based access control

This mitigation is required to counter privilege escalation on the management application

At Foundation Grade the deployment is required to enforce separate accounts for device management, account administration and user access

DEP.4.2.M51: Audit

This mitigation is required to counter unauthorised use of management privilege

At Foundation Grade the deployment is required to record audit events, protected from account administrators

DEP.4.2.M53: Local management authentication

This mitigation is required to counter use of a poorly protected management interface

At Foundation Grade the deployment is required to authenticate management activities via username/password

This is intended to include serial console access etc.

DEP.4.2.M55: Remote management authentication

This mitigation is required to counter use of a poorly protected management interface

At Foundation Grade the deployment is required to manage the device using an authenticated secure protocol, such as IPsec, SNMPv3, TLS or SSH with username/password authentication

DEP.4.2.M121: Control access to management interface

This mitigation is required to counter exploitation of a vulnerability in the management protocol

This mitigation is required to counter use of a poorly protected management interface

At Foundation Grade the deployment is required to disable management interfaces on black network

Where required, remote management may still be performed via the encrypted tunnel.

DEP.4.3 - Deploy >> Gateway >> Red Interface

DEP.4.3.M92: Secure red side interface services

This mitigation is required to counter exploitation of red side services that are unavailable from the black network interface

At Foundation Grade the deployment is required to list all red side services in the deployment guide and provide risk management guidance

Services offered on the red side should be described in the deployment guide with an explanation of the risks of using each service and details of how to mitigate them (e.g. how to disable the services).

IV. GLOSSARY

31. The following definitions are used in this document:

Term	Meaning
Black	Data that is not protectively marked or to be protected.
Black Interface	The less trusted interface of the product
CPA	Commercial Product Assurance
Crash	Unexpected event which causes the device to not function as intended
Entropy	A measure of the randomness of a piece of information
IPsec	IP Security
Red	The data that is to be protected
Red Interface	The more trusted interface of the product
Security Characteristic	A standard which describes necessary mitigations which must be present in a completed product, its evaluation or usage, particular to a type of security product.

THIS PAGE IS INTENTIONALLY LEFT BLANK