CPA SECURITY CHARACTERISTIC

IPSEC SECURITY GATEWAY

Version 2.3

About this document

This document describes the features, testing and deployment requirements necessary to meet CPA certification for IPsec Security Gateway products. It is intended for vendors, system architects, developers, evaluation and technical staff operating within the security arena.

- Section 1 is suitable for all readers. It outlines the purpose of the security product and defines the scope of the Security Characteristic.
- Section 2 and Section 3 describe the specific mitigations required to prevent or hinder attacks for this product. Some technical knowledge is assumed.
- For more information about CPA certification, refer to The Process for Performing CPA Foundation Grade Evaluations[1].

Document history

The CPA Authority may review, amend, update, replace or issue new Scheme Documents as may be required from time to time. Soft copy location: DiscoverID 27467650

Version	Date	Description
1.1	March 2012	Update for publishing
1.2	August 2012	Added support for a wider range of operating systems
2.0	December 2012	Library related updates
2.1	January 2013	Library related updates
2.2	March 2013	Added Common Criteria Protection Profile Mappings appendix
2.3	April 2013	Updates following external review

This document is derived from the following SC Maps.

SC Map	Map version
VPN Security Gateway	2.1.2
VPN Common	2.0.2
Authentication Libraries	2.0.4
Common Libraries	2.0.4
Crypt Libraries	2.0.4
Network Device Libraries	2.0.4
Physical Protection Libraries	2.0.4

Contact CESG

This document is authorised by: Deputy Technical Director (Assurance), CESG. For queries about this document please contact:

CPA Administration Team
CESG, Hubble Road
Cheltenham
Gloucestershire
GL51 0EX, UK

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

[1] www.cesg.gov.uk/servicecatalogue/CPA

Contents

1.1 Introduction

This document is a CPA Security Characteristic. It describes requirements for assured IPsec Security Gateway products for evaluation and certification under CESG's Commercial Product Assurance (CPA) scheme.

1.2 Product description

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 network connectivity over a less trusted network.

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

1.3 Typical use cases

There are two common use cases for IPsec security gateways: client to gateway and gateway to gateway.

1.3.1 Client to gateway

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.

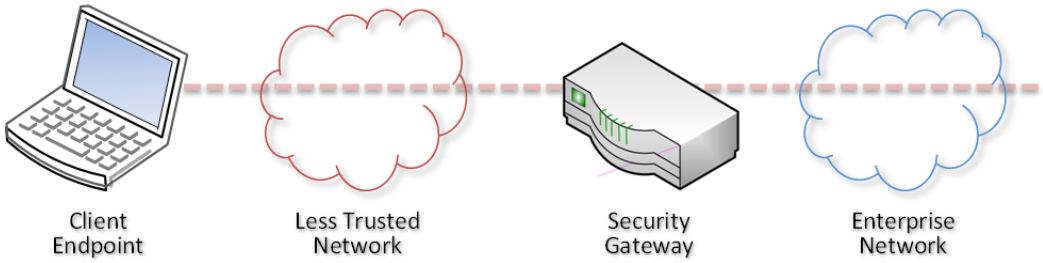

Figure 1: The Client to Security Gateway IPsec model

1.3.2 Gateway to gateway

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

1.4 Expected operating environment

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). The device is additionally expected to be deployed with tamper protection mechanisms.

In the envisaged architecture (see Figure 1 and Figure 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 trusted network.

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.

1.5 Compatibility

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.

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.

No specific requirements are placed on the operating system that hosts a software-based IPsec security gateway (conforming to this Security Characteristic) other than to allow the product to operate correctly whilst meeting the requirements in Section 3. This said, there is a general expectation that the product will be compatible with the latest version of a given operating system.

1.6 Interoperability

This Security Characteristic assumes that the security gateway is deployed as described in RFC 5996 - 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.

To ensure interoperability, this Security Characteristic is designed for products that are compliant with the relevant RFCs for IPsec (primarily RFC 4301 [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.

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)

After a '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.

1.6.1 PSN end-state IPsec profile

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

- PRIME Framework: Base Module, v1.2.0
- PRIME Framework: Suite Definition Module - Suite B.128, v1.2.0
- PRIME Framework: Authentication Module - X.509 via CERTREQ, v1.2.0
- PRIME Framework: IKEv2 NAT Traversal Module, v1.2.0

In the future, the profile summarised in the table below will be updated to track the latest versions of the documents above (currently all at version 1.2.0).

Module / Algorithm Type	Algorithm Details
ESP	
Encryption	AES-128 in GCM-128
IKEv2	
Encryption	AES-128 in GCM-128 (and optionally CBC*)
Pseudo-random function	HMAC-SHA256-128
Diffie-Hellman group	256bit random ECP (RFC5903), Group 19
Authentication	ECDSA-256 with SHA256 on P-256 curve

Table 1: Non-authoritative summary of Suite B.128

*If supporting CBC for IKEv2 encryption, the integrity algorithm that must be used is HMAC-SHA256-128

1.6.2 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 [p], Encapsulating Security Payload (ESP – RFC 4303 [c]) and the algorithms given in the table below.

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

Table 2: Summary of PSN Interim IPsec profile

1.7 Variants

This Security Characteristic has the following variant type and associated variants:

- Variant Type: Gateway Platform:
  - **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.

1.8 High level functional components

The following diagram illustrates the various high level functional components within this product. All components shown relate to specific mitigations listed in Section 3. These are used to structure the Security Characteristic, and to give context to each mitigation.

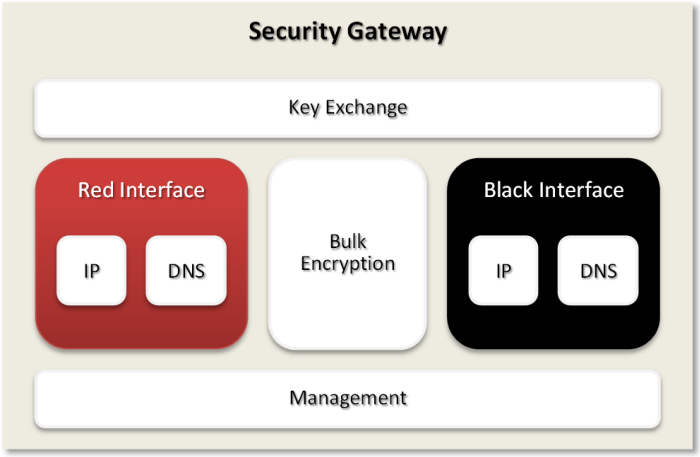

Figure 3: Functional Components of an IPsec Security Gateway

The functional components in Figure 3 are described as follows.

- **Black Interface** - The connection to the less trusted network.
- **Black Interface >> 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.
- **Black Interface >> IP** - Black-side IP interface.
- **Bulk Encryption** - Encrypts or decrypts traffic, depending on its source and destination, according to the requirements in the appropriate IPsec profile.
- **Key Exchange** - Negotiates the traffic encryption keys, according to the requirements in the appropriate IPsec profile.
- **Management** - Provides the functionality to control and configure the security gateway. Management functionality is restricted to authorised administrator use only (i.e. not accessible to standard users) through an authentication mechanism. The exact details of the authentication mechanism are beyond the scope of this document, but could be provided by either the product or host operating system.
- **Red Interface** - The connection to the trusted network which passes all traffic destined for the other endpoint to the bulk encryption.
- **Red Interface >> DNS** - (see notes for Black Interface >> DNS).
- **Red Interface >> IP** - Red-side IP interface.

1.9 Future enhancements

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

A future release will remove the interim IPsec profile and require the use of the PSN end-state IPsec profile [l].

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

2.1 Requirement categories

All CPA Security Characteristics contain a list of mitigations that describe the specific measures required to prevent or hinder attacks. The mitigations are grouped into three requirement categories; design, verification and deployment, and appear in section 3 of this document in that order.

- **Development mitigations** (indicated by the **DEV** prefix) are measures integrated into the development of the product during its implementation. Development mitigations are checked by an evaluation team during a CPA evaluation.
- **Verification mitigations** (indicated by the **VER** prefix) are specific measures that an evaluator must test (or observe) during a CPA evaluation.
- **Deployment mitigations** (indicated by the **DEP** prefix) are specific measures that describe the deployment and operational control of the product. These are used by system administrators and users to ensure the product is securely deployed and used in practice, and form the basis of the Security Operating Procedures which are produced as part of the CPA evaluation.

Within each of the above categories, the mitigations are further grouped into the functional areas to which they relate (as outlined in the **Error! Reference source not found.** diagram). The functional area for a designated group of mitigations is prefixed by double chevron characters ('>>').

For example, mitigations within a section that begins:

Development>>Management

- concern **Development** mitigations relating to the Management functional area of the product.

Note: Mitigations that apply to the **whole** product (rather than a functional area within it) are listed at the start of each section. These sections do **not** contain double chevron characters.

2.2 Understanding mitigations

Each of the mitigations listed in Section 3 of this document contain the following elements:

- The name of the mitigation. This will include a mitigation prefix (**DEV**, **VER** or **DEP**) and a unique reference number.
- A description of the threat (or threats) that the mitigation is designed to prevent or hinder. Threats are formatted in *italic text*.
- The explicit requirement (or group of requirements) that *must* be carried out. Requirements for foundation grade are formatted in **green text**.

In addition, certain mitigations may also contain additional explanatory text to clarify each of the foundation requirements, as illustrated in the following diagram.

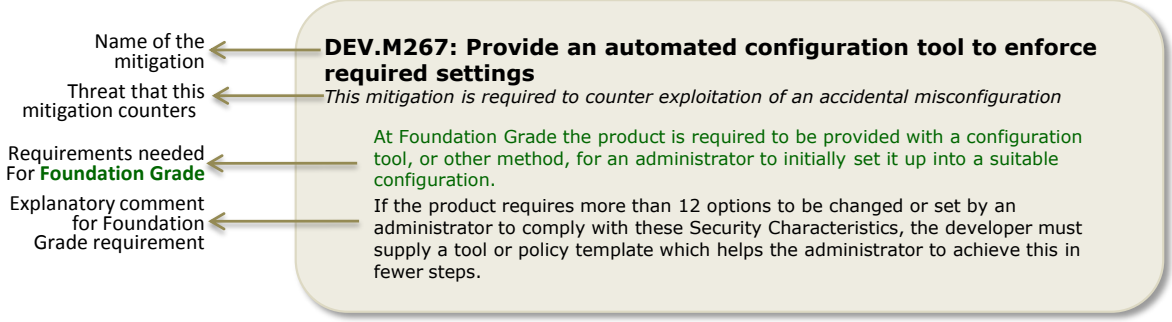

Figure 4 Components of a typical mitigation

Section 3 Requirements

This section lists the Development, Verification and Deployment mitigations for the IPsec Security Gateway Security Characteristic. For a summary of the changed mitigations in this version, please refer to Appendix A.

3.1 Development Mitigations

DEV.M41: (Software Gateway ONLY) Crash reporting

This mitigation is required to counter exploitation of a software implementation/logic 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.M42: (Software Gateway ONLY) Heap hardening

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

At Foundation Grade the product **should** use the memory management provided by the operating system. Products should not implement their own heap.

DEV.M43: Stack protection

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

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

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

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

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

At Foundation Grade the product **should** provide the capability to sanitise all private and symmetric keys during disposal.

DEV.M109: (Hardware Gateway ONLY) Protection of sensitive data lines

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

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.M159: Update product

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

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

DEV.M321: Data Execution Prevention

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

At Foundation Grade the product **is required to** support Data Execution Prevention (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.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** reject connections which do not adhere to the required IPsec profile.

At Foundation Grade the product **is required to** support an IPsec profile defined in the Interoperability section, using both confidentiality and integrity protection.

The implementation must function correctly without custom extensions.

DEV.M340: Address Space Layout Randomisation

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

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

If the product is to be specifically deployed on an operating system that does not support ASLR, there is no requirement for ASLR compatibility.

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

DEV.M349: Sanitise temporary variables

This mitigation is required to counter reading non-sanitised sensitive data from memory

At Foundation Grade the product **is required to** sanitise temporary variables containing sensitive information as soon as no longer required.

A secure erase must consist of at least one complete overwrite.

DEV.M355: Secure software delivery

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

At Foundation Grade the product **should** be distributed via a cryptographically protected mechanism, such that the authenticity of software can be ensured.

DEV.M759: Control export of long term secrets/keys

This mitigation is required to counter a compromised device exfiltrating keys
This mitigation is required to counter exploitation of unintended information disclosure which leaks keys or secrets
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 the administrator.

Where available, operating system mechanisms, such as user privileges and the certificate store, should be used to ensure that unencrypted private keys and machine certificates cannot be retrieved by a standard user.

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

DEV.M778: Restrict traffic key lifetime

This mitigation is required to counter exploitation of overused traffic key

At Foundation Grade the product **is required to** force renegotiation of a given SA within 24 hours of its establishment or previous renegotiation.

DEV.M802: Export logs

This mitigation is required to counter modification of locally stored logs

At Foundation Grade the product **is required to** provide ability to automatically transfer logs to external device.

This functionality could be provided by a host operating system, where available.

DEV.1 - Development >> Management

DEV.1.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.1.M353: 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 only authenticated administrators are able to change the product's security enforcing settings.

DEV.1.M612: 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 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.

Note: This requirement is only applicable if the product actually incorporates a log viewer.

DEV.1.M615: Inform administrator of account activity

This mitigation is required to counter exploitation of an undetected compromise of administrator authentication

At Foundation Grade the product **should** display recent authentication history.

It is recommended that on login the administrator 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 the administrator is told what to do, preferably on the screen, if the history is not what is expected.

DEV.1.M616: Anti Hammer

This mitigation is required to counter a brute force attack on the authentication interface

At Foundation Grade the product **is required to** limit the number of consecutive failed authentication attempts to fewer than 30 a minute.

This can be achieved by a number of means, such as an exponentially increasing time delay between failed sets of login attempts or purging all key material after a number of failed attempts. The technique employed must ensure that the failed authentication count cannot be reset until a successful authentication occurs.

DEV.1.M618: Passphrases are not displayed on screen in the clear while being entered

This mitigation is required to counter shoulder surfing

At Foundation Grade the product **is required to** ensure the passphrase is never visible in the clear on the screen.

Additionally, passphrases should not be entered in areas where others could see them being entered.

DEV.1.M627: 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** ensure that all log entries 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.

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.

DEV.1.M631: Replaying network traffic will not allow access

This mitigation is required to counter replay attack

At Foundation Grade the product **is required to** ensure that replaying authentication sequences does not grant access.

DEV.1.M796: Local administrator authentication

This mitigation is required to counter weak or non-existent local administrator authentication mechanism

At Foundation Grade the product **is required to** implement local administrator authentication.

If the product can have its configuration locally administered, the administrator must first be required to authenticate (for instance, by entering valid credentials).

Note: For an application-based product, the host operating system may provide the authentication interface.

DEV.1.M798: Prompt administrator to change a default passphrase

This mitigation is required to counter exploitation of a default administrator passphrase

At Foundation Grade the product **is required to** prompt the administrator to change any active default passphrase during the authentication process.

DEV.2 - Development >> Key Exchange

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 validated X.509 certificates to mutually authenticate all connections.

Certificate verification must include full certificate chain verification and processing of the current certificate revocation list(s).

DEV.2.M138: State the Security Strength required for random numbers

This mitigation is required to counter prediction of randomly generated values 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, including any generated keys. 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.2.M140: Smooth output of entropy source with approved PRNG

This mitigation is required to counter prediction of randomly generated values due to a weak PRNG

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 prediction of randomly generated values due to a weak PRNG

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 prediction of randomly generated values 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.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.

Note: Revocation checking does not need to occur immediately after a new CRL is received.

DEV.3 - Development >> Bulk Encryption

DEV.3.M123: Traffic keys are never stored in persistent storage

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

At Foundation Grade the product **should** store traffic keys in non-pageable memory.

DEV.4 - Development >> Black Interface

DEV.4.M85: Resource prioritisation

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

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.

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

DEV.4.M101: Control the attack surface

This mitigation is required to counter exploitation of host via unencrypted 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 in the deployment guide.

DEV.4.M757: Block unauthenticated traffic

This mitigation is required to counter exploitation of host via unencrypted traffic

At Foundation Grade the product **is required to** drop all traffic that is not encrypted and authenticated under an IPsec session.

With the exception of requests for IPsec session establishment and general traffic routing.

DEV.5 - Development >> Red Interface

DEV.5.M101: Control the attack surface

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

At Foundation Grade the product **is required to** identify, and enable the securing of red side services introduced by the product.

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).

3.2 Verification Mitigations

VER.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.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.M762: Perform IPsec robustness testing

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

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

At Foundation Grade the evaluator **will** perform testing on the IPsec implementation using commercial fuzzing tools.

VER.1 - Verify >> Management

VER.1.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 that standard user cannot influence any management application, for instance, by modifying registry entries or files, etc.

VER.1.M80: Protocol robustness testing

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

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.2 - Verify >> Key Exchange

VER.2.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.2.M765: Perform IKE robustness testing

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

At Foundation Grade the evaluator **will** perform testing on the IKE implementation and the X.509 certificate parser using commercial fuzzing tools.

VER.3 - Verify >> Bulk Encryption

VER.3.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.4 - Verify >> Black Interface

VER.4.1 - Verify >> Black Interface >> IP

VER.4.1.M80: Protocol robustness testing

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

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.4.2 - Verify >> Black Interface >> DNS

VER.4.2.M80: Protocol robustness testing

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

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.5 - Verify >> Red Interface

VER.5.1 - Verify >> Red Interface >> IP

VER.5.1.M80: Protocol robustness testing

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

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.5.2 - Verify >> Red Interface >> DNS

VER.5.2.M80: Protocol robustness testing

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

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.

3.3 Deployment Mitigations

DEP.M39: Audit log review

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

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

DEP.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.M76: Periodically refresh all issued certificates

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

At Foundation Grade the deployment **should** reissue all client certificates every 2 years and revoke the previous certificates.

DEP.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 certificates and, where possible, keys, prior to disposal.

DEP.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** enable signature verification for applications, services and drivers in the host operating system, where supported and where the product makes use of it.

DEP.M159: Update product

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

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

DEP.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 clients and 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.
Standard users must not be permitted to manage the certificate installation for the VPN product.
When a replacement certificate is provisioned for a gateway, the old certificate must be revoked on the client(s).

DEP.M336: Use with other assured VPN Gateways and Clients

This mitigation is required to counter exploitation of unassured interconnecting client or gateway

At Foundation Grade the deployment **is required to** ensure the product is only used with other VPN Security Gateways and Clients that have been certified to CPA Foundation Grade.

DEP.M340: (Software Gateway ONLY) Address Space Layout Randomisation

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

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

DEP.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 X.509 gateway and client certificates that are chained to a trusted, non-public, certificate authority to enable revocation of the certificates and prevent issue of fraudulent certificates.

DEP.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 update procedure to be used by the administrator must be described within the product's security procedures.

DEP.M776: Use 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 deployment **is required to** configure the device to use an approved IPsec profile defined in the Interoperability section.

DEP.M800: (Software Gateway ONLY) Deploy on Managed Endpoint

This mitigation is required to counter malware on endpoint

At Foundation Grade the deployment **is required to** configure endpoints 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.M801: Physical security controls and tamper evidence

This mitigation is required to counter physical compromise of device

At Foundation Grade the deployment **is required to** implement physical security such that only the administrator can gain local access to the product (e.g. product sited in a locked room).

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.

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.

DEP.1 - Deployment >> Management

DEP.1.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.1.M50: Role based access control

This mitigation is required to counter privilege escalation on management application
This mitigation is required to counter unauthorised use of management privilege

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

DEP.1.M53: Local management authentication

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

At Foundation Grade the deployment **is required to** authenticate any local management interface via username/password, standard users should not be able to reconfigure or disable the product.

DEP.1.M55: Remote management authentication

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

At Foundation Grade the deployment **is required to** authenticate any remote management interface using a secure protocol, such as IPsec, SNMPv3, TLS or SSH with username/password authentication.

DEP.1.M223: 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 privilege escalation on management application
This mitigation is required to counter use of poorly protected management interface

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

Where required, remote management may still be performed via the encrypted tunnel (provided additional access controls restrict such a facility to the administrator).

DEP.1.M606: Control access to device management

This mitigation is required to counter attacking management protocol stack

At Foundation Grade the deployment **is required to** restrict which network interfaces can be used for device management.

If a local console port or dedicated management interface is available, it must be possible to configure the other network interfaces to not have management services accessible on them.

Similarly, it must also be possible to restrict which network interfaces have management services enabled on them.

DEP.1.M625: Log all relevant actions

This mitigation is required to counter modification of logging generation

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

At Foundation Grade the deployment **is required to** configure the product to log 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.

At Foundation Grade the deployment **should** where available, automatically export logs to management/red side device.

DEP.1.M797: Prevent remote access using a default administrator passphrase

This mitigation is required to counter exploitation of a default administrator passphrase

At Foundation Grade the deployment **is required to** prevent any remote access to the product from potentially untrusted locations whilst a default administrator passphrase is active.

If the product supports remote administration over a network, network connectivity should be avoided until the default passphrase has been changed.
(If the passphrase can only be changed using network-based authentication, the network must be physically restricted to trusted devices only, until the passphrase is changed.).

DEP.2 - Deployment >> Key Exchange

DEP.2.M763: 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 processing of the current certificate revocation list(s).

Appendix A Summary of changes to mitigations

CESG has updated the IPsec Security Gateway Security Characteristic 2.3 (previously published version 2.1) for the following reasons.

- Removal of augmented mitigations

This has resulted in the following changes to mitigations.

A.1 Removed mitigations

The following mitigations have been removed.

- DEV.M44: Data validation on untrusted input
- DEV.M49: Function in a locked-down environment
- DEV.M66: Ephemeral keys protected from high risk processes
- DEV.M74: Deny access to physical data ports
- DEV.M777: Sanitise traffic data buffers
- DEV.2.M142: Perform statistical testing of generated entropy prior to smoothing
- VER.M349: Sanitise temporary variables
- VER.M777: Sanitise traffic data buffers
- VER.M779: Check routing engine robustness
- VER.2.M564: Cryptocheck PRNG implementation
- VER.2.M565: Validate vendor's entropy assertions
- DEP.M124: Plan for recovery from compromise of long term secrets/keys

A.2 Modified mitigations

(No existing mitigations have been modified.)

A.3 Renamed mitigations

(No existing mitigations have been renamed.)

A.4 New mitigations

(No new mitigations have been added.)

Appendix B Common Criteria Protection Profile Mappings

This appendix provides important mappings between this SC document and the Network Device Protection Profile (NDPP) Extended Package (EP) VPN Gateway (reference [q]).

B.1 Protection Profile and Extended Package Selections

There are a number of specific selections which must be made by the author of a Security Target derived from the above Protection Profile and Extended Package to ensure overlap with the Security Characteristic. These are as follows:

Appropriate algorithm selections must be included to match whichever of the cryptographic profile(s) the product claims compliance with (either the PRIME PSN end-state profile or PSN interim profile as detailed in Tables 1 and 2 in the SC). These are summarised below:

PP / EP Requirement	PRIME	PSN Interim
FCS_CKM.1.1(2)	FIPS PUB 186-3, "Digital Signature Standard (DSS)", Appendix B.4 for ECDSA schemes	Either of: • FIPS PUB 186-3, "Digital Signature Standard (DSS)", Appendix B.3 for RSA schemes • ANSI X9.31-1998, Appendix A.2.4 Using AES for RSA schemes
FCS_COP.1.1(2) (in the NDPP)	Elliptic Curve Digital Signature Algorithm (ECDSA)	RSA Digital Signature Algorithm (rDSA)
FCS_COP.1.1(3) (in the NDPP)	SHA-256	SHA-1
FCS_COP.1.1(4) (in the NDPP)	HMAC-SHA-256	HMAC-SHA-1
FCS_IPSEC_EXT.1.4	AES-GCM-128	AES-CBC-128
FCS_IPSEC_EXT.1.5	IKEv2	IKEv1, with RFC 4304 for extended sequence numbers
FCS_IPSEC_EXT.1.6	IKEv2, with AES-GCM-128	IKEv1, with AES-CBC-128
FCS_IPSEC_EXT.1.11	Group 19	Group 5
FCS_IPSEC_EXT.1.12	ECDSA	RSA

Additionally, for FCS_IPSEC_EXT.1.2, the selection must include tunnel mode.

Other selections within the Protection Profile and the Extended Package can be freely made without impact on the Security Characteristic.

B.2 SC requirements additional to Common Criteria

In addition to the Common Criteria testing, there are a small number of additional requirements in the SC which the evaluation team must also ensure the product meets:

SC Requirement	Comment
DEV.M41	The product and the operating environment must ensure that any crashes are logged.

SC Requirement	Comment
DEV.M43	If the developer's tool chain supports it, then the product must be compiled with stack protection enabled.
DEV.M321	The product must support (and not opt-out of) Data Execution Prevention (DEP) when enabled in the operating environment.
DEV.M337	The product must not require custom extensions to IPsec to be used. This requirement extends FCS_IPSEC_EXT.1.5 to note that custom IPsec extensions must not be required for the product to function in the defined cryptographic profile.
DEV.M340	The product, and all of its libraries, must employ ASLR; specific exceptions based on a sound rationale are acceptable.
DEV.M802	The product, or the operating environment, must provide the ability to automatically transfer log information to an external logging service.
DEV.2.M79	Beyond the requirement in FCS_IPSEC_EXT.1.12 test 3, the product must be capable of validating the entire certificate chain, all the way to the root certificate. If there is a limit to the depth of certificate chain that can be validated, this must be clearly noted in the Security Procedures for the product.
DEV.2.M344	In addition to tests in FCS_IPSEC_EXT.1.8, the evaluator should (whilst an SA is established) revoke the certificate associated with the SA. The SA should not be re-established when its lifetime expires.
VER.M762	The evaluator must perform robustness testing of the IPsec implementation.
VER.2.M765	The evaluator must perform robustness testing of the IKE implementation.
VER.4.1.M80 VER.4.2.M80 VER.5.1.M80 VER.5.2.M80	The evaluator must perform robustness testing of any ports or services which the product enables on the black and red side of the client.

Appendix C Glossary

The following definitions are used in this document.

Term	Definition
Black	Data that is not protectively marked or to be protected.
Black Interface	The less trusted interface of the product
CPA	Commercial Product Assurance. A scheme run by CESG providing certificate-based assurance of commercial security products.
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
SC Map	Diagrammatic representation of a Security Characteristic (or part of one).
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.

Appendix D References

This document references the following resources.

Label	Title	Location	Notes
[a]	The Process for Performing Foundation Grade CPA Evaluations	www.cesg.gov.uk/servicecatalogue/CPA	
[b]	RFC4301 Security Architecture for the Internet Protocol	IETF	December 2005
[c]	RFC4303 IP Encapsulating Security Payload (ESP)	IETF	December 2005
[d]	RFC5996 Internet Key Exchange Protocol Version 2 (IKEv2)	IETF	September 2010
[e]	RFC3602 The AES-CBC Cipher Algorithm and Its Use with IPsec	IETF	September 2003
[f]	RFC5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL Profile)	IETF	May 2008
[g]	RFC4868 Using HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512 with IPsec	IETF	May 2007
[h]	RFC2408, Internet Security Association and Key Management Protocol (ISAKMP)	IETF	November 1998
[i]	RFC2409, The Internet Key Exchange	IETF	November 1998
[j]	CESG Architectural Patterns No. 2, Walled Gardens for Remote Access	CESG IA Policy Portfolio	Issue 1.0, March 2011 (Unclassified)
[k]	CESG Technical Specifications No. 2 - PRIME Framework - Base Module	CESG IA Policy Portfolio	Issue 1.2.0, December 2011 (Unclassified)
[l]	CESG Technical Specifications No. 5 - PRIME Framework - Suite B.128 Module	CESG IA Policy Portfolio	Issue 1.2.0, December 2011 (Unclassified)
[m]	CESG Technical Specifications No. 8 - PRIME Framework - X.509 via CERTREQ Module	CESG IA Policy Portfolio	Issue 1.2.0, December 2011 (Unclassified)
[n]	CESG Technical Specifications No. 11 - PRIME Framework - NAT Traversal Module	CESG IA Policy Portfolio	Issue 1.2.0, December 2011 (Unclassified)
[o]	RFC4106 The Use of Galois Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)	IETF	June 2005
[p]	RFC4304 Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)	IETF	December 2005
[q]	Network Device Protection Profile (NDPP) Extended Package (EP) VPN Gateway	www.niap-ccevs.org	Version 1.1, April 2013