VSU-100/100R/2000 Non-Proprietary Security Policy

Part No. 87-0041-01

Revision 1.0

Change History

Revision	Date	Written/Changed By	Approval	Approval title
1.0	05/06/01	Pete Stefanko		

Table of Contents

Abstract

This document specifies the Non-proprietary Security Policy for VPNos

1.0 Introduction

This document provides the non-proprietary security policy for the VSU-100/100R/2000. The the non-proprietary security policy defines the authorized roles supported by the VSU, the services provided for each role, and the access to security relevant data in the VSU provided to each role by the services. The cryptographic boundary for the non-proprietary security policy is defined to be the physical boundary of the VSU. The VSU is a multi-chip stand-alone module.

2.0 Level

The VSU meets the overall requirements applicable to Level 2 security of FIPS 140-1.

Section	Level
Cryptographic Module	Level 2
Module Interfaces	Level 2
Roles and Services	Level 2
Finite State Machine	Level 2
Physical Security	Level 2
EFP/EFT	Level 2
Software Security	Level 2
Operating System Security	N/A
Key Management	Level 2
Cryptographic Algorithms	Level 2
EMI/EMC	Level 3
Self-Tests	Level 2

The following sections of this document further define the non-proprietary security policy of the VSU in terms of the roles, the services provided to those roles, and their access security relevant data within the VSU.

3.0 Roles and Services

The VPNos supports a Cryptographic Officer Role, User Roles, and a Network Administrator Role. The following sub-sections describe the different roles, how the roles are authenticated, the services provided by VPNos™ and which services are available to each role.

3.1 Roles

3.1.1 Cryptographic Officer Role (VPN Administrator)

The purpose of the VPN administrator is to create IP groups, User Groups, and VPNs, establish user accounts and passwords, and to configure the VSU™. The Cryptographic Officer Role is entered when an authenticated connection is established over a network (LAN/WAN) between the VSU and the management application.

3.1.2 User Role

There are two types of users that are allowed to establish VPNs with the VSU; they are remote clients and remote tunnel end points. The user role is entered when the user successfully negotiates IKE with VPNos. Once the user has successfully negotiated IKE, they are allowed to establish IPSEC tunnels to the VSU and access the network resources behind the VSU.

3.1.3 Network Administrator Role

The purpose of the Network Administrator Role is to initialize the VSU's network configuration when first deploying the VSU. The Network Administrator is also allowed to run tests via the VSU Console to ensure the VSU is working properly. The Network Administrator Role is entered when the VSU Console is successfully logged onto.

3.2 Operator Authentication

3.2.1 Cryptographic Operator (VPN Administrator) Authentication

The VSU uses identity-based authentication to authenticate the Cryptographic Officer. When the Cryptographic Officer uses the VPNmanager™ Console to configure the VSU, the Cryptographic Officer is prompted for their name and password. The VSU can be configured for super-user authentication or LDAP authentication. For super-user authentication, the super-user name and the SHA1 hash of the password are compared against in copies kept in memory. For LDAP

authentication, the cryptographic officer name and password are used to bind to the VPNmanager directory server. If the LDAP bind is successful, then the Cryptographic Officer is authenticated. The Cryptographic Officer authentication can also be configured for super-user/LDAP where the super-user authentication will be attempted first, and if it fails, then the LDAP authentication will be attempted. If the authentication fails, the operator is re-prompted for their user name and password. If several authentication attempts fail in succession, and a retry limit is reached, then the VSU will block further connections from that IP address until a configurable time out period expires.

3.2.2 User Authentication

User authentication uses identity-based authentication based on user name and password or PIN codes. The IKE service uses pre-shared secrets or digital certificates to authenticate the user.

3.2.2.1 User name and Password/PIN authentication

The user name and password/PIN authentication is used to authenticate VPNremote users. The VSU issues a challenge to the VPNremote™ user and the user responds with their user name and password or PIN. The VSU verifies the user name and password against the VSU's local configuration database or with an external authentication server (RADIUS or LDAP).

To verify the user name and password against the local configuration database, the VSU looks up the user name in an internal table, and compares the SHA1 hash of the user's password against the SHA1 hash of the password stored in the local configuration database.

If the VSU is configured to use an external RADIUS server for authentication, then the VSU passes the user name the user's password, to the RADIUS server for authentication. The RADIUS server will return a success or failure response to the VSU.

If the VSU is configured to use an external LDAP server for authentication, then the VSU will attempt to connect to the LDAP server using the user's user name and password. If the connection succeeds then the user is authenticated, otherwise the authentication failed.

If the user authentication fails, the user is re-prompted for their user name and password. If several authentication attempts fail in a row and a retry limit is reached, then the user is blocked by the VSU for a configurable time out period.

3.2.2.2 Pre-shared secret authentication

To use pre-shared secret authentication for IKE, the Cryptographic Officer has to first securely distribute the pre-shared secrets to the users and to the VSU. The user then submits their name and their pre-shared secret to the VSU when negotiating IKE. The IKE service compares the pre-shared secret against the pre-shared secret stored in memory for that user. If the pre-shared secrets match, then the user is authenticated. The user performs similar steps to authenticate the VSU.

3.2.2.3 Digital Certificate authentication

To use digital certificate authentication for users, the Cryptographic Officer must configure the VSU with the certificate of the Certificate Authorities allowed to issue certificates to users. The user submits their certificate to the VSU. The VSU parses the user certificate to determine which Certificate Authority issued the certificate. The VSU retrieves the corresponding Certificate Authority certificate from the VSU's local configuration database. The VSU then uses the public key from the Certificate Authority's certificate to validate the user's certificate. If the user's certificate is valid, then the VSU looks up the user in the VSU's configuration database. If the user exists in the database, the user is authenticated.

3.2.3 Network Administrator Authentication

The Network Administrator Role uses password authentication to authenticate the Network Administrator. The Network Administrator enters their password at the VSU Console. A SHA-1 hash of the password is compared against the SHA-1 hash stored in memory. If the hashes match, the Network Administrator is granted access to the VSU Console Interface. If the hashes don't match, then the VSU re-prompts for password again. The Network Administrator Role requires role based authentication in that everyone that attempts to assume the Network Administrator Role must present the same password to the VSU.

3.3 Services

This section lists the services provided by the VSU and provides a description of each service.

3.3.1 Show Status Service

The Show Status Service allows the Cryptographic Officer or Network Administrator Roles to use the VPNmanager Console, the VSU Console, a Syslog server or an SNMP server to verify the operating status of the VSU. No Security Relevant Data Items are accessed by the Show Status Service.

3.3.1.1 Simple Network Management Protocol (SNMP)

The VSU reports status information to configured SNMP servers via SNMP. The VSU uses standard Management Information Blocks (MIB) to communicate VSU status information such as statistics, VSU configuration, VSU model type, and VPNos version number to the VPNmanager Console. No security relevant data items are accessed by SNMP.

3.3.1.2 Syslog Service

The Syslog Service provides an error logging capability to a designated Syslog server or to an error log in VSU RAM. Events such as the VSU generating a panic and entering the error state are logged to Syslog and to the VSU Console. No security relevant data items are accessed by the Syslog Service.

3.3.2 Self Test Service

The Self-Test Service is a service provided to the Network Administrator to verify the VSU is operating correctly. The Self-Test Service is initiated when the VSU is powered up. The Self-Test Service verifies the VSU is operating correctly. The tests executed by the Self-Test Service verify the integrity of memory, the configuration database, verify the cryptographic algorithms are operating correctly, and exercise critical devices. The self-tests are initiated by cycling power to the VSU. The tests performed by the Self-Test Service are listed in section 5.4 of this document.

3.3.3 Configuration Service

The Configuration service provides a service for the Cryptographic Officer Role to configure the VSU and to set VPN policy for the VSU using VPNmanager. The Configuration Service uses the TLS protocol to secure the communication between the VSU and the VPNmanager Console. The Configuration Service has write access to all security relevant data items in the VSU. The Configuration Service does not allow more than one Cryptographic Officer to configure the VSU at a time. When a Cryptographic Officer accesses the Configuration Service, the Cryptographic Officer locks the Configuration Service until they close their session with the VSU.

3.3.4 Client Configuration Download (CCD) Service

The CCD service provides a service to the User Role for VPNremote users to retrieve their VPN policy configuration. The CCD service authenticates the VPNremote user using the configured authentication server (VSU database in RAM, RADIUS server, Directory server), and if successful returns the user's VPN policy to the user. The CCD service communication between VPNremote and the VSU is secured using TLS.

3.3.5 Secure Authentication Protocol (SAP) Service

The SAP service provides a service to the User Role for VPNremote users to re-authenticate Users when their VPN session has timed out. The SAP service also provides authentication of remote clients that received their vpn policy configuration via a floppy disk. The SAP communication between VPNremote and the VSU is secured using TLS.

3.3.6 Internet Key Exchange (IKE) Service

The IKE service is a service provided by the VSU to the User Role. The IKE service implements the IKE protocol as specified in RFC 2409 published by the Internet Engineering Task Force (IETF). The IKE protocol operates in two phases, Phase 1 and Phase 2.

For Phase 1, VPNos supports Main Mode and Aggressive Mode with either Pre-Shared Secret or RSA Digital Signature authentication. VPNos supports Oakley groups 1,2 as specified in rfc 2409 for key generation.

For Phase 2, VPNos supports Basic Quick Mode and PFS.

VPNos does not support New Group Mode or the public key authentication schemes specified in sections 5.2 or 5.3 of the IKE specification .

3.3.7 IPSec Service

The IPSec service is a service provided by the VSU to the User Role. The IPSec Service implements IETF's rfc 2406 the Encapsulating Security Payload (tunnel mode only) and IETF's rfc 2402 the Authentication Header. The IPSec Service guarantees data integrity, data source authentication and confidentiality of IP packets that are transmitted between a user and the VSU.

Data integrity is guaranteed through the use of the SHA1 hash algorithm to generate a message authentication code that is encapsulated with the original data.

Data source authentication is also guaranteed through the use of SHA1 based message authentication codes.

Data confidentiality is guaranteed through the use of the DES or TDES encryption algorithms to encrypt the original packet. The DES or TDES encryption keys are derived session keys that are generated using the Diffie-Hellman key agreement protocol.

3.3.8 Initial Configuration Service

The Initial Configuration Service is provided by the Console interface for the Network Administrator Role. The Initial Configuration Service allows the Network Administrator to set the VSU networking configuration (IP address, network mask), set the SuperUser password, and to enable FIPS mode.

3.3.9 Zeroization Service

The Zeroization service provides the ability to the Cryptographic Officer Role to overwrite all security relevant data items in the VSU with zeros. All digital certificates and their corresponding RSA key pairs are zeroed out, all IKE and IPSec security associations and their session keys are zeroed out, all user passwords are zeroed out. The Zeroize service is accessed by the Cryptographic Officer when the Cryptographic Officer issues a Zeroize command to the VSU.

3.4 Roles vs. Services

Table 2 defines the services that available to each role.

Show Status	Cryptographic Officer, Network Administrator
Self-Test	Network Administrator
Configuration Service	Cryptographic Officer
Client Configuration Download	User
Secure Authentication Protocol	User
Internet Key Exchange	User
IPSec	User
Pre-Initialization Service	Network Administrator

4.0 Security Relevant Data Items

This section lists the security relevant data in VPNos and provides a brief description of their use.

4.1 VPNremote Users passwords

If the VSU is configured to use local authentication and local configuration then the VPN Remote User's name and the SHA-1 hash of their password are stored together in the VSU memory. The user name and SHA-1 hash of the password are used to authenticate the remote user during CCD and SAP.

4.2 VSU LDAP DN and password

If the VSU is configured to use an X.500 directory for authentication or storing configuration data, the VSU requires a Directory Name (DN) and password to use to bind to the directory with. The VSU DN and password are configurable by the Cryptographic Officer. VSU LDAP DN and password are stored in the clear in flash memory.

4.3 Super User name and password

The VSU Super User name and the SHA-1 hash of the Super User password are stored in NVRAM in the VSU. The Super User name and password are set via the VPNmanager Console by the Cryptographic Officer.

4.4 VSU RADIUS password

The VSU RADIUS password is stored as plaintext in NVRAM in the VSU. The RADIUS password is set via the VPN Manager Console by the Cryptographic Officer.

4.5 RSA key pairs

VPNos supports up to nine X509v3 digital certificates for the VSU. The VSU digital certificates include the VSU device certificate installed during the manufacturing process, and up to eight digital certificates for use during IKE or TLS negotiations. Each VSU digital certificate contains a RSA public key and has a corresponding private key stored in the VSU flash. The digital certificate and its associated key pair are used to identify the VSU to peers during IKE or TLS sessions.

4.6 Diffie-Hellman key pairs

The VPNos generates Diffie-Hellman key pairs for exchange during IKE and IPSEC communication sessions. The Diffie-Hellman key pairs are used to generate IKE and IPSEC session keys to secure the IKE and IPSEC tunnels.

4.7 IKE Session keys

The IKE, IPSec and TLS services generate session keys for encrypting/decrypting their data. For IKE and TLS, these session keys are generated for each session. For IPSec, the session keys are generated for each security association. The session keys are deleted when the session terminates or when their key lifetime expires. The key lifetime can be set to the amount of data the keys are used encrypt/decrypt or to a time interval in units of minutes, hours or days.

4.8 IPSEC Session keys

The IPSec service generates session keys for encrypting/decrypting the data that is sent across the VPN. IPSec generates session keys for each security association. The session keys are deleted when the session terminates or when their key lifetime expires. The key lifetime can be set to the amount of data the keys are used encrypt/decrypt or to a time interval in units of minutes, hours or days.

4.9 TLS Session keys

The TLS services generate session keys for encrypting/decrypting data. TLS generates session keys for each session. The session keys are deleted when the session terminates or when their key lifetime expires.

4.10 FIPS Switch

The FIPS Switch enables FIPS 140-1 mode of operation for the VSU. The Network Administrator sets the FIPS switch using a VSU console command to put the VSU in FIPS mode. The Cryptographic Officer can clear the FIPS switch from the VPN Manager Console, to disable FIPS operation.

5.0 Security Rules

5.1 Concurrent Users

The VSU supports multiple concurrent users.

5.2 No Bypass Mode

The VSU does not support a crypto-logic bypass mode.

5.3 No Maintenance Role

The VSU does not require maintenance and does not support a maintenance role.

5.4 Self-Tests

Upon application of power or when commanded by the operator, the VSU shall perform the following tests:

- Flash memory CRC test
- Cryptographic Self-Tests

Flash Memory Self Tests
Cryptographic Self Tests
RSA key pair self-test
SHA1 self-test
HMAC SHA-1 self-test
DES self-test
3DES self-test
TLS DES self-test
Big Number, Exponent modules self-test
RSA Key Pair-wise Consistency test
Software Load Test
Continuous Pseudo Random Number Generator Test

6.0 FIPS Approved Cryptographic Algorithms

The VSU uses the following algorithms when operating in FIPS mode.
The algorithms implemented in software are:

- DES operated in CBC mode.
- TDES operated in CBC mode.
- SHA-1.
- RSA (ANSI X9.31)

The algorithms implemented in hardware are:

- DES operated in CBC mode
- TDES operated in CBC mode
- SHA-1

7.0 Non-FIPS compliant operation

The VPNos supports the RC5 encryption algorithm and the MD5 hash algorithm. These algorithms are not FIPS 140-1 approved. These algorithms are not enabled when operating in FIPS 140-1 compliant mode.

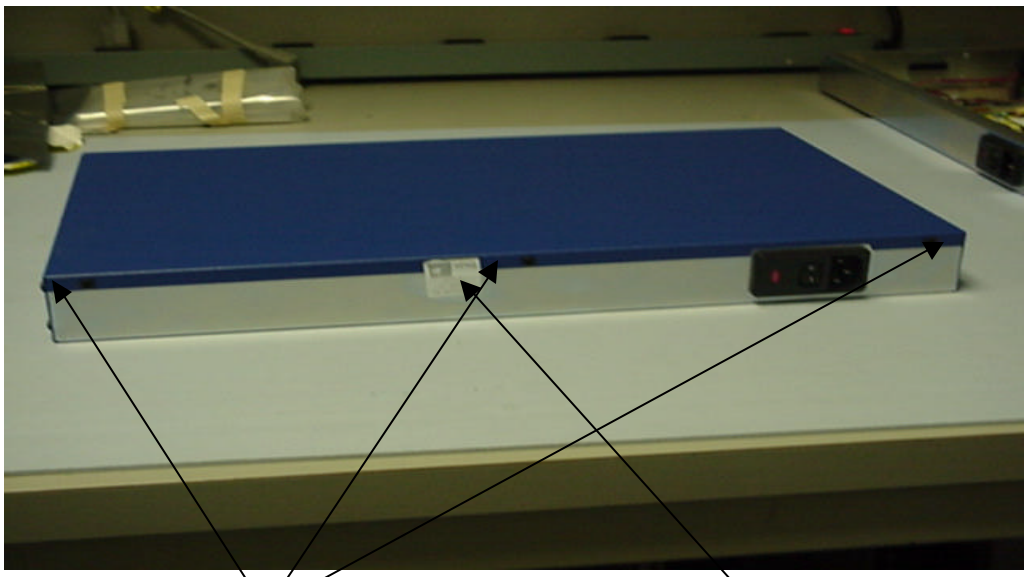
VPNos supports the SKIP key management protocol. The current implementation of SKIP in VPNos only supports the MD5 algorithm. For this reason, SKIP VPNs are not allowed when operating in a FIPS 140-1 compliant mode.

8.0 Physical Security

The physical security of the VSU-100/100R/2000 is guaranteed through the use of tamper evident seals. The following picture shows the placement of the tamper evident seal on the VSU-100/100R.

17) 74-0104 – Tamper evident label

The following picture shows the placement of the tamper evident seal on the VSU-2000.



3 each 79-0039 6-32x3/8" Black pan head screws

Tamper Proof Label P/N 74-0104