# FIPS 140-2 SECURITY POLICY
## NetScreen-5200

Version 4.0.0r7.3 P/N 093-0605-000 Rev. B

## Copyright Notice

# Table of Contents

# A. Scope of Document

The NetScreen-5200 is an Internet security device that integrates firewall, virtual private networking (VPN) and traffic shaping functionalities.

Through the VPN, the NetScreen-5200 provides the following:

- IPSec standard security
- Data Encryption Standard (DES), triple-DES and Advanced Encryption Standard (AES) key management

***Note:*** *Only DES is used for legacy systems.*

- Manual and automated IKE (ISAKMP)
- The use of RSA and DSA certificates

The NetScreen-5200 also provides an interface for users to configure or set policies through the console or network ports.

The general components of the NetScreen-5200 include firmware and hardware. The main hardware components consist of a main processor, memory, flash, ASICs (GigaScreen version 2 and GigaScreen II), 10/100 Mbps ethernet interface, GBIC network interface, console interface, backplane, redundant power supplies and fan tray. The entire case is defined as the cryptographic boundary of the modules. The NetScreen-5200's physical configuration is defined as a multi-chip standalone module.

# B. Security Level

The NetScreen-5200 meets the overall requirements applicable to Level 2 security of FIPS 140-2.

**Table 1: Module Security Level Specification**

| Security Requirements Section | Level |
|---|---|
| Cryptographic Module Specification | 2 |
| Cryptographic Module Ports and Interfaces | 2 |
| Roles, Services, and Authentication | 2 |

**Table 1: Module Security Level Specification (Continued)**

| Security Requirements Section | Level |
|---|---|
| Finite State Model | 2 |
| Physical Security | 2 |
| Operational Environment | N/A |
| Cryptographic Key Management | 2 |
| EMI/EMC | 2 |
| Self-Tests | 2 |
| Design Assurance | 2 |
| Mitigation of Other Attacks | N/A |

## C. Roles and Services

TheNetScreen-5200 supports five distinct roles:

- Cryptographic Officer Role (Root): The module allows one Crypto-Officer. This role is assigned to the first operator who logs on to the module using the default user name and password. Only the Crypto-Officer can create other administrators, and change to FIPS mode.
- User Role (Admin): The Admin user can configure specific security policies. These policies provide the module with information on how to operate (for example, configure access policies and VPN encryption with Triple-DES).
- Read-Only User Role (Admin): This role can only perform a limited set of services to retrieve information or status. This role cannot perform services to configure the box.
- VSYS User Role: This role has the same operations as the User Role above, except that a VSYS user only operates within a particular virtual system. See the *NetScreen Concept and Examples ScreenOS Reference Guide* for more information about virtual systems.
- VSYS Read-Only User Role: This role has the same operations as the Read-Only User Role above, except that a VSYS read-only user only operates within a particular virtual system. See the *NetScreen Concept and Examples ScreenOS Reference Guide* for more information about virtual systems.

The module allows up to 22 concurrent Admin users, either in a User Role or in a Read-Only Role.

The root administrator can create a virtual system (vsys) administrator for each vsys, if the device has multiple virtual systems configured. The vsys administrator can function in either the "user" role or "read-only" role. A virtual system is the architecture that enables the device to respond with a different set of configurations for each vsys administrator. Therefore, a single box can appear to be several logical "virtual systems."

The NetScreen-5200 provides the following services:

- **Clear**: Clear dynamic system info
- **Exec**: Exec system commands
- **Exit**: Exit command console
- **Get**: Get system information
- **Ping**: Ping other host
- **Reset**: Reset system
- **Save**: Save command
- **Set**: Configure system parameters
- **Trace-route**: Trace route
- **Unset**: Unconfigure system parameters

The NetScreen-5200 supports both role-based and identity-based authentication.

- Role-based authentication provides a user name and password, but the actual authentication occurs at a RADIUS server. It is only available for the User Role (Admin).
- All other forms of authentication (local database) are classified as identity based.
- The module supports identity-based authentication for the Crypto-Officer (local database), the User Role (local database), the Read-Only User Role (local database), VSYS User Role, and VSYS Read-Only User Role.

## D. Interfaces

The NetScreen-5200 provides a number of interfaces:

- The NetScreen-5200 has eight mini-GBIC interfaces (labelled 1, 2, 3, 4, 5, 6, 7 and 8). These interfaces are the network ports. Each port has 2 link lights (LEDs) to indicate the port status. The top LED indicates the link status. If the LED is on,this means the link is up. If the LED is off, this means the link is down. The bottom LED indicates the link activity. If the LED is on and is blinking, this means the port is active (transmitting/receiving data). If the LED is off, this means the port is inactive.
- Console port: RJ-45.
- Modem port: RJ-45. Disabled in FIPS mode.
- MGT port: 10/100 Mbps ethernet for management traffic. It has 2 link lights (LEDs) to indicate the port status. The right LED indicates the link status. If the LED is on, this means the link is up. If the LED is off, this means the link is down. The left LED indicates the ethernet activity. If the LED is on and is blinking, this means the port is active (transmitting/receiving data). If the LED is off, this means the port is inactive.
- HA1/HA2 port: dual mini-GBIC ports for failover.
- Compact flash interface for a memory flash card.
- Power interface, AC or DC.
- The management module has six types of indicators:
  - CPU utilization: Consists of an array of 5 LEDs that indicate the current level of CPU utilization. Utilization is defined as the amount of traffic detected on the interface at any given time. The CPU utilization LEDs represent the following percentages of utilization: 5%, 10%, 25%, 50%, and 90%. When all LEDs are dark, this indicates CPU utilization is less than 5%.
  - One Power status LED: Illuminates solid green when the power is supplied to the NetScreen-5200.
  - One Module status LED: Illuminates blinking green when the module is operational, or amber when the unit is booting up.
  - System Alarm LED: Illuminates red when a critical alarm occurs, such as a hardware or software failure, or a firewall attack; illuminates amber when a major alarm occurs, such as "low memory;" is dark when there are no alarms.

  - HA LED: Illuminates green if the unit is the master, amber if the unit is the slave, and is dark if HA is not configured.
  - Compact Flash LED: Illuminates green if the compact flash card is installed in the compact flash slot, blinking green if the compact flash card is active, and is dark if the slot is empty.
- The secure port module has two LEDs.
  - One power status LED: Illuminates solid green when the power is supplied to the NetScreen-5200.
  - One module status LED: Illuminates blinking green when the module is operational, or amber when the unit is booting up.
- The fan tray has a status LED: Illuminates solid green when the fan is operational, and is dark when it is not operational.
- Hardware reset button: After the user follows the sequence: insert for 5 seconds, release for 5 seconds, insert for 5 seconds, and release for 5 seconds, the device will erase all configurations and be restored to the default factory settings.

## E.Setting FIPS mode

By default, on the first power-up, the module is in non-FIPS mode.

The commands "get config", or "get system" indicate if the system is in FIPS mode.

The module can be set to FIPS mode only through the CLI. To set the module to FIPS mode, execute "set fips-mode enable" through the CLI.

Special note for firmware upgrade: if a pre-4.0 firmware is upgraded to 4.0 FIPS version and above, even if the box is previously in FIPS mode, please re-enable FIPS mode again by issuing the commands "unset fips-mode enable," "set fips-mode enable," followed by rebooting the box.

This command will perform the following:

- Disable administration via SSL
- Disable the loading and output of the configuration file from the TFTP server
- Disable the Global reporting agent
- Disable administration via SNMP
- Disable the debug service
- Disable the modem port
- Enforce HTTP only through VPN with AES encryption
- Enforce Telnet only through VPN with AES encryption
- Enforce AES for VPN to manual key only, IKE is disabled for AES.
- Enforce SCS to use only 3DES to manage the box
- Disable MD5 algorithm

Execute the "save" command.

Execute the "reset" command.

Please note the following:

- Configure the HA encryption key before using the HA link.
- Telnet and HTTP (WEB UI) are allowed only through a VPN with AES encryption.
- The derivation of keys for ESP-Encryption and ESP-Authentication using a user's password is in non-FIPS mode.

- User names and passwords are case-sensitive. The password consists of at least six alphanumberic characters. Since there are 26 uppercase letters, 26 lowercase letters, and 10 digits, the total number of available characters is 62. The probability of someone guessing a password is $1/(62^{6}) = 1/56,800,235,584$, which is far less than a 1/1,000,000 random success rate. If three login attempts from the console fail consecutively, the console will be disabled for one minute. If three login attempts from Telnet or the WebUI (through VPN with AES encryption) fail consecutively, any login attempts from that source will be dropped for one minute.
- If there are multiple login failure retries within one minute and since the user is locked out after three contiguous login failures, the random success rate for multiple retries is $1/(62^{6}) + 1/ 62^{6}) + 1/(62^{6}) = 3/(62^{6})$, which is far less than 1/100,000.
- DSA-signed firmware image cyrptographic strength analysis: the firmware is signed by a well-protected DSA private key. The generated signature is attached to the firmware. In order for the device to accept an unauthorized image, the image has to have a correct 40-byte (320-bit) signature. The probability of someone guessing a signature correctly is $1/(2^{320})$, which is far less than 1/1,000,000.
- The image download takes at least 23 seconds, so there can be no more than 3 download tries within one minute. Therefore, the random success rate for multiple retries is $1/(2^{320}) + 1/(2^{320}) + 1/(2^{320}) = 3/(2^{320})$, which is far less than 1/100,000.
- In order for authentication data to be protected against disclosure, substitution and modification, the administrator password is not echoed during entry.
- The NetScreen-5200 does not employ a maintenance interface or have a maintenance role.
- When in FIPS mode, the NetScreen-5200 WebUI only displays options that comply with FIPS regulations.
- The output data path is logically disconnected from the circuitry and processes performing key generation or key zeroization.
- The NetScreen-5200 provides a Show Status service via the GET service.
- The NetScreen-5200 cannot be accessed until the initialization process is complete.
- The NetScreen-5200 implements the following power-up self-tests:

Device Specific Self-Tests:

- Boot ROM firmware self-test is via DSA signature
- SDRAM read/write check
- ASIC chip test

Algorithm Self-Tests:

- DES, CBC mode, encrypt/decrypt
- TDES, CBC mode, encrypt/decrypt
- SHA-1
- RSA (encryption and signature)
- DSA Sign/Verify
- Exponentiation
- AES, CBC mode, encrypt/decrypt
- SHA-1-HMAC
- Bypass test

- The NetScreen-5200 implements the following conditional tests:
  - PRNG continuous test
  - Hardware RNG test
  - SCS key agreement test
  - DH key agreement test
  - DSA pair-wise consistency test
  - RSA pair-wise consistency test
  - Bypass test
  - Firmware download DSA signature test

## Other Parameters

Also note that:

- A pair-wise consistency test for DH, DSA and RSA (encryption and signature) key-pairs is employed.
- The firmware can be loaded through the Trivial File Transfer Protocol (TFTP) or the PCMCIA port, where a firmware load test is performed via a DSA signature.
- Keys are generated using a FIPS approved pseudo random number generator per ANSI X9.31, Appendix C.
- For every usage of the module's random number generator, a continuous RNG self-test is performed. Note that this is performed on both the FIPS approved RNG and non-FIPS approved RNG.
- In FIPS mode, only FIPS-approved algorithms are used.
- The NetScreen-5200 enforces both identity based and role based authentication. Based on their identity, the operator assumes the correct role.
- Operators must be authenticated using user names and passwords. Authentication will occur locally. The user can be authenticated via a RADIUS server. The RADIUS server provides an external database for user role administrators. The NetScreen-5200 acts as a RADIUS proxy, forwarding the authentication request to the RADIUS server. The RADIUS server replies with either an accept or reject message. See the log for authenticated logins. The RADIUS shared secret has to be at least 6 characters.
- The operator must enter the user name and password. All logins through a TCP connection disconnect after three consecutive login failures and an alarm is logged.
- A separate session is assigned to each successful administrator login.
- The password is not echoed during the administrator login.
- SCS uses 3DES encryption only.
- The first time an operator logs on to the module, the operator uses the default user name and password, which are both netscreen. This user is assigned the Crypto-Officer role.
- The Crypto-Officer is provided with the same set of services as the user with four additional services: (1) "set admin" and "unset admin". These two services allow the Crypto-Officer to create a new user, change a current user's user name and password, or delete an existing user. (2) "set fips enable" and "unset

fips enable". These two services allow the Crypto-Officer to switch between FIPS mode and default mode.

- HTTP can only come through a VPN with AES encryption. The default page time-out is 10 minutes; this is user configurable. The maximum number of HTTP connections, i.e., the maximum number of concurrent WebUI logins depends on how many TCP sockets are currently available in the system. The maximum number of available TCP sockets is 2048. This number is shared with other TCP connections.
- Telnet can only come through a VPN with AES encryption.
- There are a maximum of 22 sessions shared between Telnet and SCS.
- Upon a Telnet and console login failure, the next prompt will not come up for an estimated 5 seconds.
- The NetScreen-5200's chips are production-grade quality and include standard passivation techniques.
- The NetScreen-5200 is contained within a metal production-grade enclosure.

**Figure 1** Front of the NetScreen-5200 Device

- The enclosures are opaque to visible spectrum radiation.
- The enclosure includes a removable cover and is protected by tamper evident seals. These seals also cover the power block at the back of the unit. The

locations of the tamper evident seals are shown in Figure 2.


**Figure 2** Tamper Evident Mechanisms

Removing the cover damages the tamper evident seals. You should place new seals as follows: Thoroughly clean the areas on which you will place the labels with isopropyl alcohol. Peel off the labels and apply them to the locations shown in Figure 1. Allow the adhesives to cure for 24 hours before they function as tamper evident seals.

- The source code is annotated with detailed comments.
- Ninety-two percent of the software within a cryptographic module is implemented using a high-level language (i.e., C); 5% is written in assembly due to performance issues; and 3% are WEB page files such as HTML, and GIF for the WebUI.
- The Netscreen-5200 does not use third party applications.
- The NetScreen-5200 generates an Initial Vector (IV) using a FIPS approved pseudo random number generator for the beginning of a session. The IV is incremented by one for each packet belonging to this session.
- IKE, Diffie-Hellman (DH), and RSA encryption are employed for public key-based key distribution techniques, which are commercially available public key methods.
- The policy is associated with keys located in the modules. The private/public key pair of the module is located at a certain and exact memory location of the flash.
- All keys are stored in plain text.

- All keys and unprotected security parameters can be zeroized through the Unset and Clear commands, except RNG key.
- The NetScreen-5200 does not perform key archiving.
- The NetScreen-5200 includes the following algorithms:
  - FIPS Approved:

    DSA/SHA1

    TDES (CBC)

    DES (CBC)

    AES (CBC)

    SHA-1-HMAC

    RSA Sign/Verify (PKCS #1)

    RSA Encrypt/Decrypt (used for key wrapping only)
  - Non-FIPS Approved:

    MD5

    DH
- The NetScreen-5200 conforms to FCC part 15, class A.
- Upon the failure of any power-up self-test, the module enters and stays in either the Algorithm Error State or Device specific error state, depending on the self-test failure. The console displays error messages and the status LED flashes red. It is the responsibility of the Crypto-Officer to return the module to NetScreen Technologies, Inc. for further analysis.
- Upon the failure of any conditional test, the module enters and stays in a permanent error state, depending on the type of failure: Bypass test failure, SCS key agreement test failure, DH key agreement test failure, DSA pair-wise test failure, or RSA pair-wise agreement test failure. The console displays error messages and the status LED flashes red. It is the responsibility of the Crypto-Officer to return the module to NetScreen Technologies, Inc. for further analysis.
- On power down, previous authentications are erased from memory and need to be re-authenticated again on power-up.
- Bypass tests are performed at power-up, and as a conditional test. Bypass state occurs when the administrator configures the box with a non- VPN

policy, and traffic matching this policy arrives at the network port. The bypass enabled status can be found by retrieving the entire policy list. Two internal actions must exist in order for bypass to happen: (1) a non- VPN policy is matched for this traffic, and (2) a routing table entry exists for the traffic that matches this non-VPN policy.

- In FIPS mode, SCS can use 3DES only to encrypt/decrypt commands. Also if the command from SCS is to set or get the AES manual key, it will fail and a message will be logged.
- A VPN with AES encryption is manual key only. In other words, IKE is disabled for a VPN using AES.
- HA traffic encryption is 256 bit AES.
- If a VPN uses 3DES Encryption, the key exchange protocol IKE is enforced to use group 5 only.
- SHA-1 algorithm on GigaScreen II has the limitation that it cannot hash more than 8K of data. Other ASIC chips have no such limitation.

## F. FIPS Certificate Verification

In FIPS mode, during the loading of the X509 certificate, if the signing CA certificate cannot be found in the NetScreen-5200, the following message is displayed on the console:

> Please contact your CA's administrator to verify the following finger print (in HEX) of the CA cert...
>
> xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx
>
> Do you want to accept this certificate y/[n]?

Where x is one of (0, 1,2,3,4,5,6,7,8,9,A,B,C,D,E,F).

Based on the result of the CA certificate fingerprint checking, the Crypto-Officer accepts or denies the loaded certificates.

## G. Critical Security Parameter (CSP) Definitions

Below is a list of Critical Security Parameter (CSP) definitions:

- **IPSEC Manual Key**: DES, TDES, and AES for user traffic encryption. It is from user input.
- **IPSEC Session Key**: DES, TDES, and AES for user traffic encryption. It is generated by the IKE key exchange.
- **IKE Pre-Shared Key**:User input data to generate IKE session key and SHA-1-HMAC key.
- **IKE Session Key**: DES, TDES, AES for peer-to-peer IKE message encryption.
- **User Name and Password**: Crypto-Officer and Users' user names and passwords.
- **SCS Server/Host Key**: RSA keypairs used in secure command shell (equivalent to SSH).
- **SCS Session Key**: Encryption key to encrypt telnet commands by using 3DES only.
- **DSA Public Key**: Firmware-download authentication key.
- **HA Key**: AES Encryption key for HA data.
- **IKE DSA Key**: DSA key pair used in IKE identity authentication.
- **IKE RSA Key**: RSA key pair used in IKE identity authentication.
- **PRNG Algorithm Key**: ANSI X9.31 algorithm key required to generate pseudo-random numbers. These items are stored in volatile RAM and in non-volatile flash memory.
- **SHA-1-HMAC Key**: IPSEC authentication key between end users, and IKE authentication between two peers.

## Matrix Creation of Critical Security Parameter (CSP) versus the Services (Roles & Identity)

The following matrixes define the set of services to the CSPs of the module, providing information on generation, destruction and usage. They also correlate the User roles and the Crypto-Officer roles to the set of services to which they have privileges.

The matrices use the following convention:

G: Generate

D: Delete

U: Usage

N/A: Not Available

**Crypto-Officer**

| CSP \ Services | Set | Unset | Clear | Get | Exec | Save | Ping | Reset | Exit | Trace -route |
|---|---|---|---|---|---|---|---|---|---|---|
| IPSEC Manual Key | G | D | N/A | U | N/A | U | N/A | N/A | N/A | N/A |
| IPSEC Session Key | G | D | N/A | U | N/A | N/A | N/A | D | N/A | N/A |
| IKE Pre-shared Key | G | D | N/A | U | G | U | N/A | N/A | N/A | N/A |
| IKE Session Key | N/A | N/A | D | N/A | N/A | N/A | N/A | D | N/A | N/A |
| User Name and Password | G[a] | D[b] | N/A | U | N/A | U | N/A | N/A | N/A | N/A |
| SCS Server/Host Key | G | D | D | U | G | U | N/A | D (Server Key) | N/A | N/A |
| SCS Session Key | N/A | N/A | D | N/A | N/A | N/A | N/A | D | N/A | N/A |
| DSA Public Key | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| HA Key | G | D | N/A | N/A | U | U | N/A | N/A | N/A | N/A |
| IKE DSA Key | N/A | D | N/A | N/A | G,D,U | N/A | N/A | N/A | N/A | N/A |
| IKE RSA Key | N/A | D | N/A | N/A | G,D,U | N/A | N/A | N/A | N/A | N/A |
| PRNG Algorithm Key | N/A | N/A | N/A | N/A | G,U | N/A | N/A | D | N/A | N/A |
| SHA-1-HMAC Key | N/A | N/A | D | N/A | N/A | N/A | N/A | D | N/A | N/A |

a. The Crypto-Officer is authorized to change all authorized operators' user names and passwords, but the user is only allowed to change his/her own user name and password

b. The Crypto-Officer is authorized to remove all authorized operators.

### User and VSYS User

| CSP \ Services | Set | Unset | Clear | Get | Exec | Save | Ping | Reset | Exit | Trace -route |
|---|---|---|---|---|---|---|---|---|---|---|
| IPSEC Manual Key | G | D | N/A | U | N/A | U | N/A | N/A | N/A | N/A |
| IPSEC Session Key | G | D | N/A | U | N/A | N/A | N/A | D | N/A | N/A |
| IKE Pre-shared Key | G | D | N/A | U | G | U | N/A | N/A | N/A | N/A |
| IKE Session Key | N/A | N/A | D | N/A | N/A | N/A | N/A | D | N/A | N/A |
| User Name and Password | G[a] | N/A | N/A | U | N/A | U | N/A | N/A | N/A | N/A |
| SCS Server/Host Key | G | D | D | U | G | U | N/A | D (Server Key) | N/A | N/A |
| SCS Session Key | N/A | N/A | D | N/A | N/A | N/A | N/A | D | N/A | N/A |
| DSA Public Key | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| HA Key | G | D | N/A | N/A | U | U | N/A | N/A | N/A | N/A |
| IKE DSA Key | N/A | D | N/A | N/A | G,D,U | N/A | N/A | N/A | N/A | N/A |
| IKE RSA Key | N/A | D | N/A | N/A | G,D,U | N/A | N/A | N/A | N/A | N/A |
| PRNG Algorithm Key | N/A | N/A | N/A | N/A | G,U | N/A | N/A | D | N/A | N/A |
| SHA-1-HMAC Key | N/A | N/A | D | N/A | N/A | N/A | N/A | D | N/A | N/A |

a. The Crypto-Officer is authorized to change all authorized operators' user names and passwords, but the user is only allowed to change his/her own user name and password.

### Read-Only User and VSYS Read-Only User

| CSP \ Services | Get | Ping | Exit | Trace-route |
|---|---|---|---|---|
| IPSEC Manual Key | U | N/A | N/A | N/A |
| IPSEC Session Key | U | N/A | N/A | N/A |

### Read-Only User and VSYS Read-Only User

| CSP \ Services | Get | Ping | Exit | Trace-route |
|---|---|---|---|---|
| IKE Pre-shared Key | U | N/A | N/A | N/A |
| IKE Session Key | N/A | N/A | N/A | N/A |
| User Name and Password | U | N/A | N/A | N/A |
| SCS Server/Host Key | U | N/A | N/A | N/A |
| SCS Session Key | N/A | N/A | N/A | N/A |
| DSA Public Key | N/A | N/A | N/A | N/A |
| HA Key | N/A | N/A | N/A | N/A |
| IKE DSA Key | N/A | N/A | N/A | N/A |
| IKE RSA Key | N/A | N/A | N/A | N/A |
| PRNG Algorithm Key | N/A | N/A | N/A | N/A |
| SHA-1-HMAC Key | N/A | N/A | N/A | N/A |

# Glossary

**Authentication Header (AH).** See *ESP/AH*.

**Authentication.** Administrator authentication ensures the user identity by validating user name and password. Data authentication ensures data is from a legitimate source, and its content has not been altered. The algorithms used in data authentication include DSA signature check in the firmware download or IKE exchange, and the keyed hash algorithm SHA-1-HMAC used in IKE exchange or IPSEC data integrity check.

**CLI.** The command line interface.

**DNS.** The Domain Name System maps domain names to IP addresses.

**DHCP**. The Dynamic Host Configuration Protocol used to dynamically assign IP addresses to networked computers.

**ESP/AH.** The IP level security headers, AH and ESP, were originally proposed by the Network Working Group focused on IP security mechanisms, IPSec. The term IPSec is used loosely here to refer to packets, keys, and routes that are associated with these headers. The IP Authentication Header (AH) is used to provide authentication. The IP Encapsulating Security Header (ESP) is used to provide confidentiality to IP datagrams.

**GBIC.** A Gigabit Interface Connector (GBIC) is the kind of interface module card used on the NetScreen-5200 for connecting to a fiber optic network.

**Internet Key Exchange (IKE).** The method for exchanging keys for encryption and authentication over an unsecured medium, such as the Internet.

**Internet Protocol (IP).** An Internet standard protocol that defines a basic unit of data called a datagram. A datagram is used in a connectionless, best-effort, delivery system. The Internet protocol defines how information gets passed between systems across the Internet.

**IP Security (IPSec).** Security standard produced by the Internet Engineering Task Force (IETF). It is a protocol suite that provides everything you need for secure communications—authentication, integrity, and confidentiality—and makes key exchange practical even in larger networks. See also *DES-CBC, ESP/AH*.

**ISAKMP.** The Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for Internet key management and provides the specific protocol support for negotiation of security attributes. By itself, it does not establish session keys, however it can be used with various session key establishment protocols to provide a complete solution to Internet key management.

**MD5**. Message Digest (version) 5, an algorithm that produces a 128-bit message digest (or hash) from a message of arbitrary length. The resulting hash is used, like a “fingerprint” of the input, to verify authenticity.

**RADIUS.** Remote Authentication Dial-In User Service is a service for authenticating and authorizing dialup users.

**SCS.** Secured Command Shell, using SSH to encrypt telnet traffic.

**SHA-1.** Secure Hash Algorithm-1, an algorithm that produces a 160-bit hash from a message of arbitrary length. (It is generally regarded as more secure than MD5 because of the larger hashes it produces.)

**Virtual System.** A feature unique to the NetScreen-5200, a Virtual System is a subdivision of the main system that appears to the user to be a stand-alone entity. Virtual Systems reside separately from each other in the same NetScreen-5200 device. Each one can be managed by its own Virtual System Administrator.

# Index