VSU Console

1/14/2004

Table of Contents

1. Introduction

This document will define all VSU console options that are used for configuration and debugging in firmware version 3.2.25.

2. Requirements

VSU
PC with Hyperterminal access or remote telnet access.

3. Main Menu

This is what you will see when vsu first boots up to Main Menu.

Enter VSU console password: ********

VPNet Technologies - VSU 2000 3DES ENCRYPTION - Main Menu

(1) Configuration
(2) Statistics
(3) Utilities
(4) Logout
(5) Quick Setup

4. Configuration

Option 1 from main menu is configuration. Here is a list of those options and their functions.

1) System
- (1) VSU Console Password
  - Security function to password protect console access
- (2) Date
  - Allows you to set date. Incorrect date can affect remote access
- (3) Time
  - Allows you to set your regional time. All messages are time stamped using this value.
- (4) Timezone
  - Allows you to configure the VSUs time for your local timezone.
- (5) Runtime Image
  - Displays what version of firmware is loaded in each flash and gives you the option to switch to non-used flash.
- (6) Unit Identifier
  - Engineering use
- (P) Previous menu
  - Return to previous menu

(2) Ethernet/IP
(1) Ethernet-IP Address
- Public ip address of the vsu.

(2) Secondary Ethernet-IP Address
- Private ip address of the vsu

(3) Default Route
- Default route for all traffic leaving public interface.

(4) VPN Traffic Default Route
- Define route for either encrypted or de-crypted traffic. Used to eliminate static routes or for site to site default route.

(5) Primary DNS Address
- Configure the public DNS server to resolve the vsu's name.

(6) Secondary DNS Address
- Configure the secondary DNS server

(7) SNMP Trap Target Address
- Displays configured servers to receive snmp trap messages.

(8) Static Routes
- Option to manually add static routes for the private network

(9) NAT To Broadcast Addresses

(10) Syslog Targets
- Displays all servers configured to receive syslog messages.

(11) Client Global Config
- Displays Global Client setting
  - Client configuration at startup
  - Inactivity logout value
  - Client security option
    - Purge on exit

(12) Participate in MTU Discovery
- Displays MTU setting and allows you to change setting

(P) Previous menu

(3) Virtual Private Networks
(1) Edit VPNs
- Add,delete,modify vpn and show all vpns

(2) Non-VPN traffic
  (1) Permit all non-VPN traffic
  - Allows both encrypted and clear traffic to pass through VSU.

  (2) Deny IP non-VPN traffic only
  - Allows all non-IP traffic to pass through VSU
  - All non-VPN ip traffic is dropped except ICMP,IGMP,GGP,EGP,IGP,DGP,EIGP ANS OSPF

  (3) Deny all non-VPN traffic
  - All non-VPN traffic is blocked

  (P) Previous menu

(3) Security Control
- Enable and disable VPN security

(4) RADIUS Authentication Messages
- Enable and disable Radius authentication messages

(5) VPN Configuration Mode
- Set **Maintain** or **Force** rebuild of all tunnels

(6) Default Policy

- Show and set Default VPN ID and members

(P) Previous menu

(4) IP Address Mapping
- Displays the Client Mapping timeout value, default is 4 minutes.
- Displays Client Pool Range ex.10.10.10.15 - 10.10.10.20.

(5) IP Filtering
(1) Add a Filter Rule
- Manually configure a filter rule

(2) Delete a Filter Rule
- Manually delete a filter rule

(3) Flush the Filter Table
- Remove all filter rules

(4) Set the Filter Default Rule
- Manually configure default pass,block rule on interface

(5) Set the Filter Log Option
- Enable packet logging on a specified interface

(6) Enable/Disable Access Control Service
- Toggle the ACS on or off

(7) Turn On/Off Advanced Fragment Filter
- Toggle the VSU's ACL advanced fragment filter

(8) Enable/Disable QoS/CoS
- Toggle quality of service on or off

(9) Set QoS-mode (core/boundary)
- Options are core, boundry, and boundrylink

(10) Display Filter Default Rule
- Shows all default queue filter rules, default is "pass" all packets

(11) Display Filter Log Option
- Displays the present log setting for the in and out queue for each interface ethernet0, ethernet1 and tunnel0.

(12) ICSA 3.0a FW Compliance
- Shows if the VSU in running ICSA FW mode

(P) Previous menu

(6) Flush Configuration
- Purges VSU configuration

(7) Toggle Secure SNMP Option
- Enable and Disable secure snmp

(8) Enable/Disable Keypad Input
- Engineering Use only

(9) VPNmanager Authorization
(1) Authorization Provider
- Superuser – user id used for initial configuration
- Superuser/ldap – normal mode, either id authorized to make changes
- LDAP – only LDAP id is authorized to make changes

(2) VSU Superuser Name
- Configure Superuser id

(3) VSU Superuser Password
- Password used with Superuser id to make configuration changes

(4) No Authentication Data Received Timeout
- VSUs maximum time allowed to receive authentication response, default is 10000 miliseconds

(5) No LDAP Authentication Response Timeout
- VSUs maximum time to receive authentication from LDAP, default is 45 seconds

(6) No Configuration Data Received Timeout
- Maximum time for the VSU to receive its configuration from the LDAP, default is 60 seconds

(7) Failed Authentication/Blocked Timeout
- Time authentication is blocked before re-authentication is permitted, default is 3 minutes

(8) Failed Authentication Retry Limit
- Number of attempts before authentication is blocked, default is 15 retries

(9) VPNmanager/VSU SSL Options
- Shows if communications between VSU and VPNmanager is using ssl(636) or non-encrypted(389)

(P) Previous menu

(10) VPNremote Authorization
- Display or change VPNremote message and brand text.

(11) High Availability
- Display HA status and setting
- Enable and Disable HA
- Start and Stop HA
- Enable and Disable HA logging.
- Display and set HA timer setting
-

(P) Previous menu

5. Statistics

This section explains what reporting statistics are available on the VSU console with examples for each statistic.

(2) Statistics

(1) Overview
- Traffic Rates
- Summary of lan frames received
- Summary of errors
- Summary of VPN and non-VPN packets

(2) VPNs
- Summary of all traffic for each VPN configured

(3) Ethernet
- Summary of Ethernet statistics

```
              (1) Frames transmitted and received
              (2) Frames discarded
              (3) Frame, CRC, Underflow and Overflow errors
              (4) Lost carrier, Collisions summary
  (4) IPSec Engine
        • Summary of the IPSEC engin
              (1) Summary of the IPSec sessions
              (2) Commands issued and processed
              (3) Available command buffers
  (5) IP Statistics
        • Summary of the IP traffic
               1. Packets sent and received
               2. Summary of packets fragmented
               3. Unknown protocols received.
  (7) Flush Statistics
        • Clears all VSU statistics
(P) Previous menu
```

6. Utilities

This section explains what utilities that can be ran from the VSU console that are available.

(1) Ping
- Test connectivity with a single icmp ping

(2) Packet Trace
- Engineering packet trace tool

(3) Diagnostics
```
   (1) Display trace
   (2) Display trace triggers
   (3) Empty trace data
   (4) Trace all data
   (5) Trace errors only
   (6) Trace toggle link control
   (7) Trace toggle non IP
   (8) Trace toggle secure IP
   (9) Trace toggle unsecure IP
  (10)Trace toggle non-member blocks
  (11)Trace toggle ACL blocks
```

(3) Diagnostics
- Internal diagnostic tests

(4) Flashware
- Displays what firmware version is loaded in each flash location.

(5) Memory
- Displays total and available memory resources.

(6) Reboot
- Performs complete vsu reboot process to re-initialize vsu.

(7) Show VSU and VPNmanager certificates

- Displays the burned in vsu certificate. Displays all CA certificates being used by the vsu and vpnmnager for communications.

(8) Event Log
- Logs various system messages used for troubleshooting and general vsu processes like "ccd authentications"

(9) Network Tables
(1) Bridge Table
- Displays MAC address

(2) Routing Table
- Dispalys local routing table

(3) IP Bridge Table
- Displays the bridge table if vsu is in bridge mode

(4) Interface Table
- Shows how each interface is configured

(5) Socket Table
- Displays all TCP and UDP ports that are active on the VSU.

(10) Display Dynamic VPNs
- Displays all dynamic VPNs when the LDAP is used for configuration

(11) Radius/VPN Remote Info
- Displays the ccd and sap listening port
- Displays clients inactivity value
- Displays the radius ip address, time out value, authentication re-try value

(12) NAT Utilities
(1) Display NAT Rules
- Shows all configured NAT rules

(2) Display NAT Statistics
- Displays In/Out/dropped statistics.

(13) IP Firewall Utilities
(1) Display IP Filter Rules
- Shows all configured filter rules for the public,private and tunnel interfaces.

(2) Display IP Filter Statistics
- Shows the statistics for each interface
- Packets in and out
- Packets blocks, passed
- Logged failures in and out
- Packet state, kept or lost
- Fragment state, kept or lost

(3) Display State Statistics & Table
- Shows the IP states generated from configured filter rules
- TCP, UDP, Active FTP, Passive FTP, hits, misses, maximum, Active states, expired states, closed states and deleted states.

(4) Display Fragment Statistics & Table
- Shows the IP fragment state

- Shows the number of New, Expired, inuse, deleted and fragments that already exist.

(5) Display IP Filter LOG Info
- Configure the log to be displayed in text or hex format
- Configure log to be sent to Syslog in text or hex format

(6) Display IP State LOG Info
- Displays IP State error log messages

(7) Clear IP Filter Statistics
- Allows you to clear all filter statistics.

(8) Clear IP Filter LOG Info
- Allows you to clear all Log info

(9) Clear IP State LOG Info
- Allows you to clear all state log info

(10)Clear Filter Cache Entries
- Clear cached info

(11)Turn On/Off IP State Logging
- Toggles logging on or off

(12) Turn On/Off IP Filter Debug Log Option
- Turns ACL logging on or off to help analyze filter problems

(14) Show ISAKMP/IKE Certificates
- Displays all installed certificates

(15) Delete ISAKMP/IKE Certificates
- Remove all installed certificates

(16) Empty IPSEC Certificate Slot
- Delete selected certificate

(17) Reset Device Certificate
- Engineering use only

(18) Show CRL information
- Engineering use only

(19) IPSEC Utilities

(1) Display ISAKMP SAs
- Shows all ISAKMP SAs and what state they are in
- Alive, dead, larval

(2) Display IPSEC SAs
- Shows all IPSEC SAs and what state they are in

(3) Delete ISAKMP SA
- Delete selected SA by defined tunnel endpoint

(4) Delete IPSEC SAs
- Delete selected SA by its VPN id

(5) ISAKMP Logging
- Enable logging to troubleshoot SAs while they are being built

(6) Enable IPSec padding check (for monotically increasing values)
- Engineering use only

(7) Set Number Of Precomputed Diffie-Hellman Keys
- Engineering use only

(8) Toggle Initial Contact Notify
- Engineering use only

(9) IKE Task Status (partial list below)
- Status of IKE processes
- Total number of Tasks
- Number of free nodes (64 is the maximum available nodes)
- Number of ISAKMP acquire tasks processed
- Number of delete notify tasks processed
-

(10) FIPS HiFn DES Certification Test
- Confirms correct function of the DES encryption process

(11) FIPS HiFn 3-DES Certification Test
- Confirms correct function of the 3-DES encryption process

(12) Flush Sas

(20) Show All VPNs
- Displays all configured VPNs

(21) Flush IP Bridging Table
- Deletes the stored bridging table

(22) RC5-128 test
- Engineering test

(23) Debug

(1) Breakpoints
- Engineering function

(2) Dump memory
- Displays all stored data in memory

(3) Dump Bank Select
- Displays the data stored in a selected memory location

(4) Get IPSec Engine Status
- Displays the status of all IPSec Engines(partial list below)
  - (1) Free IPSec sessions
  - (2) Outbound IPSec sessions
  - (3) Total commands issued
  - (4) Total commands processed
  - (5) Total bytes processed
  - (6) Max IPSec sessions

(5) Trace IPSec Engine Packets
- Display inbound and outbound packets

(6) Process Table
- Displays the state of each running process in the VSU

(7) Force Panic
- Initiates a VSU memory dump.

(8) Watchdog Test
- Confirms the function of the Watchdog timer. When the timer reachs zero, the VSU will initiate a reboot.

(8) Panic on Break
- Force a memory dump using key combination of control-break

(9) Min Phase1 SA Creation Interval
- Engineering Tool

(24) LDAP Configuration
- Displays all configured LDAP servers

(25) Enable/Disable kmalloc tracing
- Enable the memory allocation tracing. This is an engineering debugging tool.

(26) Clear kmalloc trace data
- Resets the trace data for debugging. This is an engineering debug tool

(27) Dump kmalloc trace dump
- Displays all memory allocation traces to the screen for capture
- This is an engineering debug tool

(28) CCD tests
- Tests the CCD processes in the VSU

(29) DCI Auth test
- Tests the authentication between the VSU and the LDAP

(30) Code Trace
- This is an engineering tool

(31) SAP Auth Utility (This is an engineering debug tool)
(1) SAP Auth test
- Display and set authentication source

(2) SAP Show ClientMap Table
- Displays the Client Pool address range

(3) Toggle SAP debug option
- Enable SAP debugging

(32) Resilient Utility
(1) Toggle Drop/Receive Resil Control Packets From Private Port
- Allows private interface to receive control packets

(2) Show Resil Tunnels
- Displays all configured Resilient tunnels

(3) Show Resil Statistics
- Displays information on the Resilient tunnel configuration

(4) Flush Resil Statistics
- Resets all Statistics to zero

(5) Verify Resil Internal Structures
- Engineering debug tool

(33) NAT FTP Utility
(1) Dump Hash Table
- Displays all Hash algorithisms

(2) Dump Timeout Table
- Engineering debug tool

(3) Print NAT FTP Statistics
- Engineering debug tool

(34) SNTP
(1) Show Status
- Displays all SNTP(Simple Network Time Protocol) servers configured. Sets and maintains the VSUs time to GMT.

(2) Add Server
- Configure SNTP servers

(3) Delete Server
- Allows deletion of configured SNTP servers.

(4) Timeouts
- Allows configuration of the number of retries before failing

(5) Debug
- This is an engineering debug tool

(35) Send VSU Info to a File
- Sends critical configuration and the present status of the VSU to a file using the Y-modem protocol for debugging purposes.

7. Lockout

This function will lock the console if you have a console password configured.

8. Quick Setup

This function is normally ran only during initial VSU configuration. The user will be given the option to configure the following items.

- Public IP Address
- Private IP Address
- Default Route
- NON-VPN Traffic mode
  1. Permit all NON-VPN traffic
  2. Permit all IP Traffic
  3. Block all NON-VPN Traffic
- VSU Console password
- FIPS compliant mode
- Date
- Time
- Reboot to complete Quick Setup