SmartCS NS-2250 Console Server

Release Notes

Version 1.3

Seiko Solutions Inc.

Table of contents

Version 1.3 (2017/4/14)

Version 1.3 provides the following new features and fixes.

1 Support for IPv6

In this version, IPv6 is added to run the NS-2250 in the IPv6 network.
It supports IPv4/IPv6 dual stack. The functions corresponding to IPv6 are followings.

Category	Function	State
Port access	Port server	○
	Port log sending(SYSLOG/NFS/FTP/Mail)	-
Management	DNS client	○
	Static routing	○
	Telnet/SSH server	○
	Telnet client	○
	FTP/SFTP server	FTP - / SFTP ○
	Bonding	○
	SNTP client	-
	SNMP agent	-
	SYSLOG client	-
	FTP/TFTP client	-
Security	Access control(allowhost)	○
	RADIUS authentication/accounting	-
	TACACS+	-
	Firewall(ipfilter)	-
	IPsec	-

The default value of IPv6 is “disable”, and IPv6 address is not set.
After enable IPv6 by the “create ip6” command, set IPv6 address by the “set ip6addr” command.

2 Change the operating specification when accessing the port server by telnet

In the case of using in the select mode, even if being set to deny the telnet access by not specifying “telnetd/portd telrw/portd telro” in the “create allowhost” command the port select menu is displayed but change the operating specification not to be displayed.

3 Change the specification of sending the mail

Change the specification to insert the DATE/FROM data in the SMTP header when sending the port log by mail.

4 Change the specification of the “traceroute” command

When the DNS server is set in the setting of the NS-2250 the IP address in the output result of the “traceroute” command is displayed to convert to the hostname, but change the specification to be displayed in the form of the IP address.
If there is no response from the DNS server the “traceroute” command becomes not to be kept waiting until the timeout elapsing.

5 Fix for the DoS vulnerability

Fix the following vulnerabilities.

CVE-2017-5970
The vulnerability that the kernel may crash because of receiving the packet whose IP option is modified.

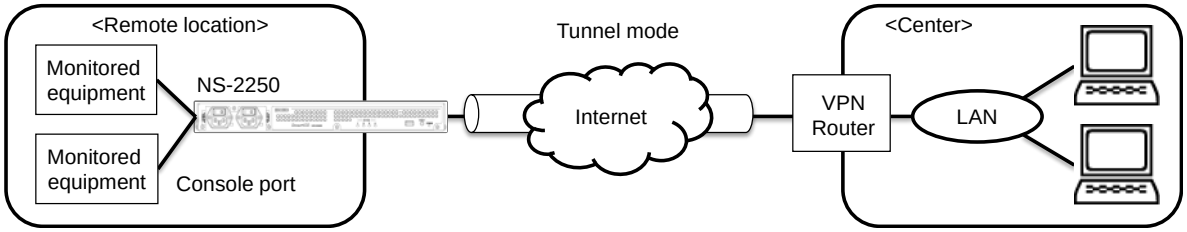
CVE-2017-6214
The vulnerability that an infinite loop may occur because of receiving the TCP packet in which the URG flag is set.

Version 1.2 (2016/10/28)

Version 1.2 provides the following new features and fixes.

1 Support for IPsec encryption

This version added IPsec to encrypt between the NS-2250 and VPN routers. The connection mode supports to both IPsec Initiator and Responder. It supports cryptographic key authentication with pre-shared key (PSK), and the maximum number of connections is 8.



The below table shows the connection mode and the operation mode as well as the number of the available connections.

Item	Description
Connection mode	Cryptographic key authentication by the pre-shared key (PSK)
Operation mode	Tunnel mode
The number of the available connections	Max. 8 connections. The configuration to establish the IPsec connection by the opposite network (subnet) is required.
Monitoring	Detect disconnection of tunnel interface by DPD
Others	NAT traversal (UDP capsuling for ESP)

NS-2250 supports the following IKE ISAKMP-SA (Phase1).

Item	Description
IKE protocol	IKEv1/IKEv2
Encryption algorithm	3DES/AES128/AES128CTR/AES256
Authentication algorithm	MD5/SHA1
DH group	2(1024bit)/5(1536bit)/14(2048bit)
ISAKMP-SA life time	3600～86400 sec. (Default: 10800 sec.)

NS-2250 supports the following IPsec-SA (Phase2)

Item	Description
Encryption algorithm	3DES/AES128/AES128CTR/AES256
Authentication algorithm	HMAC-MD5/HMAC-SHA1
DH group (during PFS)	2(1024bit)/5(1536bit)/14(2048bit)
IPsec-SA life time	3600～86400sec. (Default: 3600 sec.)

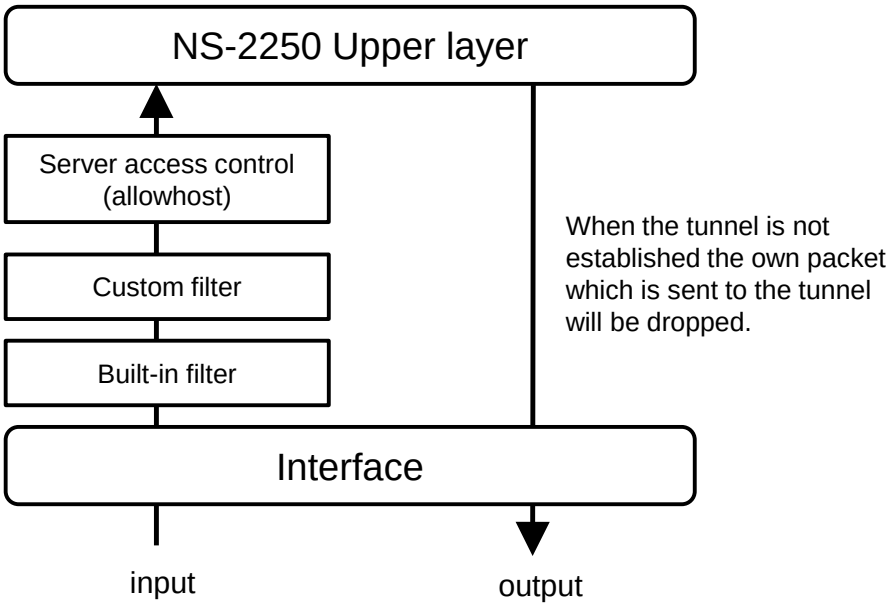
2 Support for Firewall (ipfilter)

Firewall (ipfilter) has been added to enhance security. It supports built-in filters and custom filters on the receiving interface. With the Firewall you can achieve the access control by respective filter conditions such as IP address, protocol type and port number.
The maximum number of registrations is 64 entries for the NS-2250.

Item		Description
Filter Type	Built-infilter (receive)	The built-in filter is a filter which is configured in the system in advance. It accepts the following received packets. (1) Return packet for packet sent by NS-2250 The following packets are also subject to this filter. ・SYN/ACK and ACK packet at 3-way handshake ・FIN, FIN+ACK and RST packet at end of session ・TCP connection request packet (SYN) of FTP-DATA session (passive) when accessing ftpd function ・TCP connection request packet (SYN) of FTP-DATA session (active) when ftp command is executed ・IKE packet after establishing ISAKMP-SA ・ESP packet after establishing IPSEC-SA ・ICMP error message packet (2) Packet sent out from loopback device of NS-2250 Triggered by enabling the Firewall. (Default: disable) Deleting or modifying the built-in filter is not possible.
	Custom filter (receive)	User configurable filter processed at the input of the interface. Processed after the built-in filter. Max. 64 entries can be stored.

Filter condition	Interface	eth1: LAN1 port eth2: LAN2 port bond1: Bonding port
	IP address	SA: Source IP address DA: Destination IP address
	Protocol	ICMP: ICMP type(0-255) TCP: TCP port number(1-65535) UDP: UDP port number(1-65535) ESP: ESP protocol
	Processing	accept: accept the packet drop: drop the packet

When Firewall (ipfilter) become enabled each filter will be evaluated in the order shown below.



3 Enhancement for escape character of Telnet client

In previous version, the escape character of Telnet client was fixed to Ctrl +]. In this version, you can change and disable the escape character. Even if you use Telnet login via jump server many times, you will be able to perform operations such as disconnecting Telnet sessions. This function can be used with "set telnet cmdchar" command.

4 Support for function to change Interface MTU

The function to change the Interface MTU was added. This function can be used with "set ipinterface mtu" command.

5 Fix for Off-Path TCP Exploits vulnerability (CVE-2016-5696)

The TCP protocol is implemented according to RFC 5961 to limit the amount of Challenge ACK transmission in preparation for DOS attacks. This version responded to vulnerabilities that may be subject to attacks of connection disconnection and data injection using the restriction.