

SINA[®] One Way H

Highly secure, high performance data diode with error-free data transfer



Benefits:

- » The only data diode approved for **SECRET** and **NATO SECRET**
- » Highly secure unidirectional data transfers in encryption networks
- » Data transfer with automatic error correction
- » No media breaks
- » High data transfer of up to **1Gbit/s**
- » Complete compact system

The SINA One Way “black/red” gateway enables data transfer in one direction only: from an open or lower classified “black” source network to a higher classified “red” target network. As an example unclassified data gathered from the Internet can be transferred to a SECRET network.

One Way gateways are inserted as interfaces between networks with ascending information classification. Key features of this network transfer are an exclusively unidirectional data transfer, automated high-performance transfer of large data quantities and low transfer durations. These are requirements that cannot be achieved using so-called “turnstile” interfaces.

A key component of SINA One Way is the hardware-based data diode, which is responsible for the system’s critical feature: The unidirectional data transfer. This definitively precludes the possibility of data leakage from the “red” network back into the “black” one.

With SINA One Way, secunet is addressing the following customer sectors and application areas:

- Federal Armed Forces
- National security authorities
- Companies handling classified information
- Operators of critical infrastructures with automation, process control
- and guidance systems (ICS)

Working principle

In SINA One Way, a data diode and a proxy in both the “black” and the “red” network act as transfer computers. Data is transferred using a protocol that includes automatic error detection and correction, but not reporting. The purely hardware-based data diode thus ensures that no physical reverse channel exists. The data transfer occurs in one direction, exclusively from a “black” to a “red” network. The “red” proxy then receives the transferred data and forwards it to server systems in the “red” network according to protocol specifications.

Using SMTP the “black” proxy will interact with a mailserver and send email messages through the data diode to the “red” network.

With Samba or FTP services, files are dealt with either manually (by an authorised user) or via a service. The transfer to the other side is then initiated by the data diode of SINA One Way and logged. When doing so, appropriate technical and organisational measures are taken in accordance with the level of approval, to ensure that authorised data transfers relating exclusively to the target network are initiated on the “black” proxy.

SINA One Way is easy to administer, via a user-friendly web interface.

Sample usage scenarios

The main use is for the transfer of data from a “black” source network to a “red” target network: this for example enables the transfer of Internet research results, syslog & audit data relevant to monitoring as well as security updates (e.g. new signatures for content security solutions). The forwarding of emails allows users on a “red” network to receive messages from a “black” network.

Another scenario is in the mirroring of high-traffic Internet, FTP and data-base servers in higher classified target networks.

Approvals and sample use matrix

SINA One Way is approved for application environments classified up to and including SECRET and can also be used in equivalently classified NATO networks.

The actual object of evaluation for approval is the data diode as a core component of the SINA One Way. Dimensioning the emission protection for the data diode and peripheral proxies is done using the signal attenuation characteristics of the respective operational environment.

As example operational environments in a national/NATO classification context, the approval-compliant integration options for “black/red” transitions are listed in the following table.

		“Red” target system or network		
		NATO RESTRICTED 	NATO CONFIDENTIAL 	NATO SECRET
		RESTRICTED 	CONFIDENTIAL 	SECRET
“Black” source system or network	NATO CONFIDENTIAL 		—	
	NATO RESTRICTED 	—		
	unclassified 			
	open 			

Technical Data

Proxies

Hardware platform	
Design	19" 1 U, Intel-compatible, RAID
Network interfaces	1000BASE-SX to data diode 1000BASE-SX or 1000BaseT (RJ45) to source/target network
Emission protection	Depending on operational environment: optional SDIP 27A, SDIP 27B
Anti-tamper	Not required
Power supply	2 x 90-250 V, 50-60 Hz, 650 W
Temperature ranges	+5 °C to +55 °C (non-condensing) operation +0 °C to +80 °C (non-condensing) storage and transportation
System and application software	
Operating system	Unix derivative (minimised, hardened)
Supported protocols	Appliance: File Transfer, TCP, FTP/SFTP/FTPS, SMB, CIFS, SCP, SMTP, UDP, NTP and SNMP MS Windows Core or Linux Core: File Transfer, TCP and UDP
Management	Web-based administrator interface

Data diode

Hardware platform	
Design	19" 1 U rack-mountable
Network interfaces	850 nm MM SC/PC
Emission protection	SDIP 27A, SDIP 27B or unzoned
Power supply	90-250 V, 50-60 Hz, 12 W (one network connection with two internal power supplies)
Temperature ranges	+0 °C to +55 °C (non-condensing) in operation +0 °C to +80 °C (non-condensing) during storage and transportation
Weight	1692 g

Complete SINA One Way gateway system

Performance features	
Transfer protocol	Proprietary Automatic error detection and correction
Data transfer rate	1 GBit/s*

* The actual data rate depends on the operating mode and protocol used.

More information:
www.secunet.com/en/sina



secunet Security Networks AG
Essen, Germany
Phone: +49 201 5454-0
Fax: +49 201 5454-1000
E-mail: info@secunet.com
www.secunet.com