

# Test: Raritan's Dominion SX Series

## Serial Console Access over IP

**Dr. Götz Güttich**

*The Dominion SX products from Raritan are 19" 1U appliances providing up to 48 serial consoles over IP networks, depending on the model. For secure access, all IP communications are encoded via SSL. The IAIT test lab put the product's power to the test.*

The Dominion SX enables administrators to control serially configurable network devices over a LAN/WAN, the Internet or a telephone modem. This only requires a connection between the serial port of the managed device (i.e. servers, firewalls, switches, routers, telephone switchboards or other appliances) and the Console Switch, which can then be accessed using any Java-enabled web browser. This dispenses with the need to install software on the target systems and enables management access with excellent security against attacks from the outside. In addition, the product enables the automation of client system management via scripting (which allows e.g. automatic hard disk checks on Unix systems, or database reorganisation), simultaneous access to the same port by a number of users, and chat communications with other users. And that still isn't all: when required, the appliance will send e-mail messages to the administrators and it also logs up to 64 KBytes of recent console activity. Telnet access and SNMP and Syslog support are also features of this Serial Port Switch.

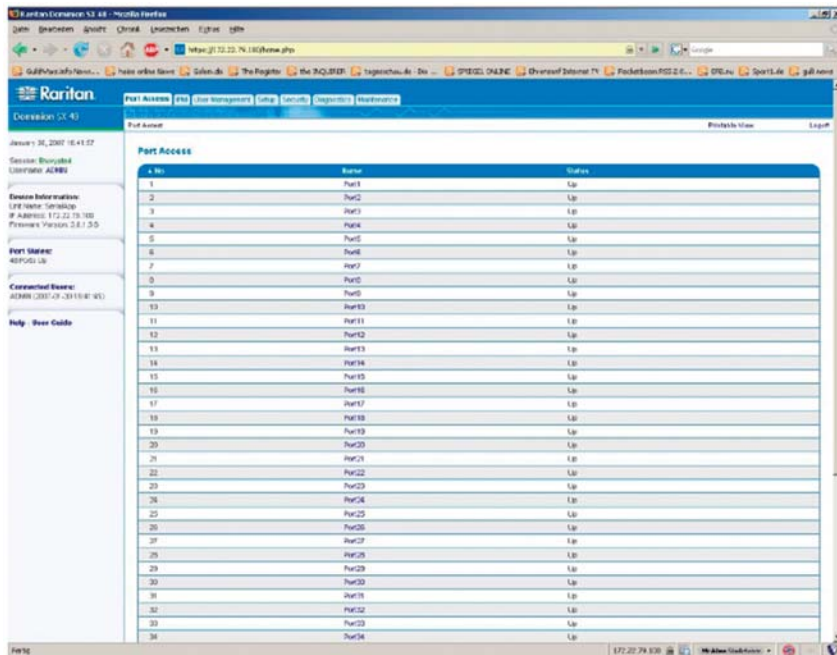


Apart from the SSL encryption mentioned above, the solution's security features include an IP-tables based firewall as well as SSH support and authentication by cooperating with Radius, TACACS+ and LDAP servers. In addition, user-defined and installable Security Certificates provide the safest secure access possible.

### **The Test**

For this test we integrated the Dominion SX into a heterogeneous network running various servers under Debian, Gentoo, Redhat and Suse Linux on a number of hardware platforms from CTT, Dell and Lynx. In addition, we used systems under Windows Server 2003 R2 as well as a managed Linksys SRW2008 switch and a Funkwerk X2300i router.

Going further, we also connected a Funkwerk Elmeg ICT 46 telephone switchboard and a Sun Ultrasparc to the system. This also applies to a Prolific-Chipsatz based Serial-to-USB-Adapter. The latter was intended to test Dominion SX System remote management of newer hardware platforms that no longer have an inbuilt serial port. Unfortunately it was impossible to create a serial connection via this method during the test; however, all other devices functioned. Since serial USB adapters are mainly intended for end users and are rather more rarely deployed in computer centres, this aspect is not all that important to this Console Switch's target group.



### Well-organised: the web-based configuration interface of the Dominion SX

After connecting the products mentioned above to the Console Switch using the adapter and cables supplied by Raritan - Raritan offers Cisco standard compliant cables - and our own CAT-5 Ethernet cables (more on the cabling aspects later in this test report), we connected the solution's network interface to our LAN and booted up the appliance. The device has the default IP address 192.168.0.192, so the responsible staff need to start by setting up a matching route from their configuration client, or immediately moving the client into the corresponding subnet in order to allow access to the configuration interface using the product's default IP address.

As soon as the browser has connected to the address of the Dominion SX, the appliance generates a Certificate and then displays the login window. The initial login is done via the "admin" account with the password "raritan" after which the user is immediately asked to supply a new password for the admin account. This is exemplary behaviour since it prevents any Console Servers to work on the network using default passwords. Only after providing a new password will the user arrive at the solution's web interface. Here the first item, "Port Access," immediately provides access to the individual serial connections. However, at this stages it may be useful to ignore the ports and first complete the basic configuration of the product instead, using the fourth

item, "Set-up". Here, under "Network," a number of obligatory settings can be made to integrate the appliance into the company network, i.e. IP address, name, gateway, domains, and so on. If a modem needs to dial in to enable remote access, this can also be configured in the Setup area. As soon as the new network settings are saved, the appliance will reboot to finish the initial configuration.

### Administration

Once the network setup has been completed, the responsible staff can log in to the Dominion SX and immediately use Port Access to access the serial ports and any devices connected to them, if these devices allow serial communications using the default settings 9600 Baud, No Parity, eight Bits, with Xon/Xoff and Hardware Flow disabled. If so, the product will open a console that branches directly to the serial ports of any connected devices. This console works with the US-ASCII (True VT100), ISO-8859-1 (Latin-1), ISO 8859-15 (Latin-9), and UTF-8 Code Sets as required. The cursor type can be set to Line Cursor or Block Cursor and the administrator has the additional console menu option to activate write access, display a user list for the port in question, or send a Break. It is even possible to copy-and-paste the console contents into the computer's clipboard. In addition, the same location provides the

Logging function mentioned above, which retains the data most recently transported over the serial port. One more attractive function, Chat, concludes the console's features. The functionality of the Dominion SX system is, however, not limited to console access. Other applications can be started after a serial port connection has been established, such as an applet to control Power reports.

In addition to the functions introduced above, the Setup menu also contains a configuration option for Remote Authentication, which can be used by the responsible employee to set the communication parameters for data exchange with Radius, LDAP and TACACS+ servers. In our test network we deployed the console servers together with the Steel Belted Radius Server from

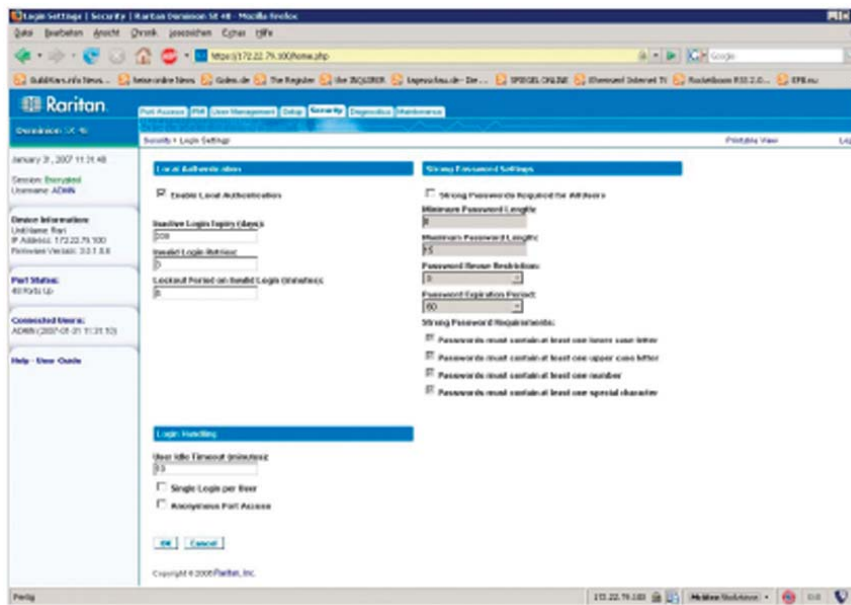
These Keywords can be associated with Events. This allows the appliance to e.g. send an e-mail notification message to IT-responsible staff each time it detects a specific Keyword in the Port's data stream.

Also interesting is the Logging function. The appliance distinguishes between System Logs, Event Logs, Port Logs and Input Port Logs. If required, the product will use RC4-encryption to encode the Logs.

The Events option, to conclude, serves to configure messaging features whose deployment has other uses that are not Keywords-related. Here it suffices to indicate the SMTP server as well as the target addresses and select the Events to be reported. For the latter, in addition to the Keyword Event, the appliance provides a long list which contains e.g. the following entries:

- "event.amp.notice.restore",
- "event.amp.error",
- "event.amp.notice.config.net work"
- and
- "event.amp.error.outOfMemory".

Two information pages on NFS and SNMP configuration complete the functions available in the Setup menu. For many administrators, the Raritan appliance's IPMI support will be interesting. It can be set up in the menu option of the same name. This allows the responsible staff to use the Intelligent Platform Management Interface functions of remote systems via the Dominion SX.



**The login settings offer many password configuration options to the responsible staff**

If the connected devices have other communication parameters than the ones mentioned above, the responsible user needs to change the port settings first. This is done in the Port Configuration submenu in the Setup menu. Here the responsible staff can, for each individual port, set the required Baud rate (between 1200 and 115,200 Baud), Flow-Control, Parity and Data Bits. In addition, the required Emulation can be defined (VT100, VT220, VT320 or ANSI).

Juniper Networks, which worked without a hitch. The same menu also provides a Service page where services such as HTTP, HTTPS, Telnet and SSH can be enabled or disabled. Here administrators even have the option to automatically forward HTTP traffic to HTTPS, which clearly increases safety levels. Also important: dialogues for the configuration of the Static Routings, the system time (via NTP servers) and the Port Keywords.

Also of central importance: the User Management option for the management of users and groups. Here the responsible user can create user accounts with passwords, and define group membership. The latter determines the ports that can be accessed by user accounts and the rights associated with each account.

Here the Console Switch distinguishes between Administrators, who have all the rights, Observers, who only have Read access, and Operators, who have Read and Write access to the connected devices but are not allowed to change the configuration of the Dominion SX.

The Security configuration - not unexpectedly - is found under the Security menu option. Under Login Settings, the administrators can define how often a user is allowed to log in (once or more than once), whether local logins are allowed, the required password length, and how long they remain valid.

Several other parameters are available, such as obligatory preset capitals and digits in passwords, and the allowed number of failed login attempts. The Security menu also contains Setup dialogues for Kerberos Authentication and Certificate Management (including Certificate Signing Request). The SSH Client Certificates once again provide the most secure SSH access

available, while Security Profiles determine e.g. whether the Telnet access system will be available, strong passwords are obligatory, timeouts are set, and whether the appliance will force HTTPS connections. The Security menu ends with a submenu for the configura-



#### tion of the integrated Firewall. **The Configuration tool of a Funkwerk X2300i router**

The last two items are easily explained. "Diagnostics" contains tools, such as a Process list, Ping and Traceroute, as well as a Netstat command displaying network connection details, and a dialogue field to launch ifconfig, informing the administrator about the status of the network interfaces. Maintenance, in contrast, offers options to view, delete or send the Event Log, create a configuration report, save and restore the configuration, as well as Factory Resets, Reboot and Firmware updates (an update from Firmware version 2.5.7 to Firmware 3.0.1 did not cause any problems during the test and all settings were retained).

Finally, there are a good online Help system and - to the left in the browser window - an information area with details on the network configuration, firmware version, port status and logged-in users.

A brief comment regarding the access rights: If a user logs in to the Console Switch who does not have all rights, irrelevant web interface menu options are no longer visible. Once again a commendable approach, since it prevents users from obtaining information about features that are not relevant to their role.

#### **In Practice**

In practice, to set up communications with the devices to be controlled, it is quite important to use the right cable. A basic guideline would be: the special Cisco compatible cables from Raritan are especially suitable for connections with appliances, routers and switches, but also for many Sun systems. Regular Ethernet cabling - in our test we used standard Cat-5 cable for this - are more suitable for communication with standard hardware (i.e. PCs).

When in doubt, it may be helpful - if the device to be accessed does not respond - to simply try the other cable type. For the rest, special measures are by and large unnecessary, since switches, routers, telephone switchboards and appliances

are usually already configured to expose serial configuration access by default and are therefore immediately available to the Dominion SX. Only operating system clients may pose an exception here, as they are not necessarily installed with serial console support, although on many Sun systems disconnecting the keyboard will suffice to activate the serial connection.



### Remote access to a Windows server via SAC

For this reason, we will give examples of Windows Server 2003 (older Windows Server versions do not support communications over serial consoles) and Linux to demonstrate how these systems can be configured to cooperate with the Dominion SX.

Under Windows Server 2003, the Emergency Management Services (EMS) take over the remote administration of the operating system when it can no longer be reached over the network, thus making serial access available.

Since these services are available on all Windows Server 2003 systems, they only need to be activated.

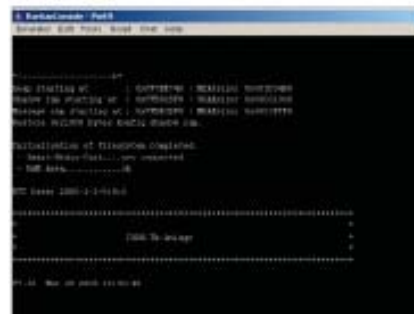
For this, an entry in the boot.ini file will suffice, e.g. the following command:

```
bootcfg.exe /EMS ON /PORT COM1 /BAUD 19200 /ID 1
```

This command is virtually self-explanatory, and the administrators only need to indicate the serial port and the baud rate they require and assign EMS a specific boot-ID. On systems with a single boot menu entry, this ID is always one; with more entries, responsible staff can base the ID on the order of the boot options in the boot.ini file.

Once the above command has been added and the system has been restarted, Windows will direct its output to the first serial port and expose the Special Administration Console (SAC), which provides administrator access to the Windows server.

Under Linux the IT staff first needs to make sure that the used Kernel supports redirection to the serial console. This can be checked in the kernel configuration under "Device Drivers/Character Devices/Serial Drivers/Console on 8250/16550 and compatible Serial Port". If this option is not active, first a new kernel needs to be compiled. Once the new kernel is running, the administrator needs to tell it which serial interface is being used by starting it with the parameter "console".



### Messages from a telephone switchboard over the serial port

If the kernel has to output e.g. to the first serial interface, with 9600 Baud, No Parity and eight Data Bits, the corresponding entry is:

```
console=ttySO,9600n8
```

If this is the only console entry, the computer display is no longer used. If it should remain active, the responsible user needs to add a second entry which additionally sends the output to the local console. This entry looks like this:

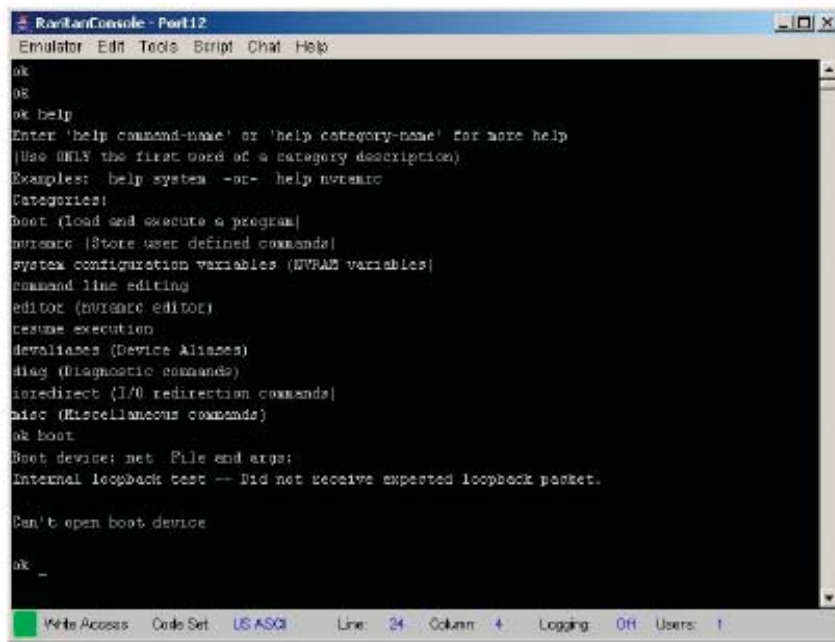
```
console=tty0
```

Sending boot parameters to the kernel is usually done in the boot manager. For example, the kernel section of the Grub boot manager in the "/boot/grub/menu.lst" configuration file on our Debian test system looked as follows:

```
title Debian GNU/Linux
root hd(0,0)
kernel /boot/vmlinuz root=/dev/sda1 ro console=tty0
console=ttySO,9600n8
initrd /boot/initrd.img
savedefault
boot
```

After a reboot, the computer will output all messages to the display connected to the first serial interface. The only thing left to do is to activate a console to accept input from the serial interface. This is done using the entry

```
T0:23:respawn:/sbin/getty -L
ttySO 9600 vt100
```



A failed attempt to start a Sun Ultrasparc over the serial console and the network interface. Here the Console Switch takes advantage of the fact that it does not need a running operating system to access the client computer.

in the "/etc/inittab" file. From now on Linux will cooperate with the Dominion SX just like the other systems.

### Conclusion

Raritan's Dominion SX series offers a powerful Console Server for the professional field with excellent security functions. Administrators who still know how to work using the command line and need to manage the many devices with serial

interfaces will find it a first class alternative to "classical" remote access over the web.

In addition, the serial consoles go the extra mile on most networked systems, since many devices e.g. display messages during system start. For environments with high availability requirements, the appliance is

supplied with two power adaptors. Raritan also offers a redundant installation of the Console Server, so that access to the managed devices is always available. If an appliance with two network connections is available, it can even be configured so that one port is available for open and the other one for private access from the LAN, which neatly separates these network segments from one another.

Administrators who prefer the com-

mand line are also able to configure all functions of the Dominion appliance via a Command Line Interface, which offers the same options as the web console. Functionality like this leaves virtually no wish unfulfilled.

Dr. Götz Güttich leads the Institut zur Analyse von IT-Komponenten (IAIT, Institute for the analysis of IT components) in Korschenbroich, Germany. The institute's web site can be found at <http://www.iait.eu>

### Raritan Dominion SX 3.0.1

Solution for the remote configuration of components with serial access over IP networks.

#### Advantages:

- Simple installation
- Well-organised administration
- Very useful in computer centres
- Good security concept

#### Manufacturer:

### Raritan Deutschland

Lichtstr. 2  
45127 Essen  
0202/74798-0  
[www.raritan.de](http://www.raritan.de)

