

## PCI DSS REQUIREMENTS AND CA PRODUCTS:

# CA NetMaster® Network Management for TCP/IP

CA NetMaster® Network Management for TCP/IP r11.6 provides robust, comprehensive IP network monitoring and diagnostic functions for the z/OS mainframe environment, including low-overhead real-time IP packet tracing and IP traffic analysis.

### PCI Requirement 11.1

*Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts.*

### How CA NetMaster® Network Management for TCP/IP Addresses this Requirement:

The CA NetMaster for TCP/IP Connection List, Traffic Statistics, SmartTrace and other functions can observe activity levels of restricted IP socket applications, and can be used to observe whether or not packet data is encrypted.

### PCI Requirement 11.3.1

*Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:*

*11.3.1 Network-layer penetration tests*

### How CA NetMaster® Network Management for TCP/IP Addresses this Requirement:

The CA NetMaster for TCP/IP SmartTrace function provides real-time tracing and packet viewing of IP packets flowing in and out of network interfaces on all monitored z/OS IP stacks.

SmartTrace can be used to observe network security perimeter testing, including observing test cases that deliberately attempt to breach network perimeter security.

## Additional Considerations

PCI DSS REQUIREMENT NUMBER	PCI DSS REQUIREMENT AREA	SUPPORT BY CA NETMASTER® NETWORK MANAGEMENT FOR TCP/IP
1	Build and Maintain Secure Networks	Inter-NetMaster Communication (INMC) Links that use TCP/IP can utilise INMC IP Proxy support, enabling them to run over VPN tunnels.
2.3	Use technologies such as SSH, VPN, or SSL/TLS	When viewing IP packets, CA NetMaster for TCP/IP SmartTrace can decode GRE protocol (VPN tunnel) packets.
6.2	Subscribe to Alerts	You may subscribe to all alerts at support.ca.com. After logging on, expand the Subscriptions link on the left, and select the Hyper Subscriptions drop-down.

PCI DSS REQUIREMENT NUMBER	PCI DSS REQUIREMENT AREA	SUPPORT BY CA NETMASTER® NETWORK MANAGEMENT FOR TCP/IP
2, 7, 8 10	Common Security Access Concerns	CA NetMaster for TCP/IP integrates with standard external z/OS security packages for both 3270 and Web user validation.
10.3	Maintain Audit Trail	CA NetMaster for TCP/IP can intercept the SMF IP Connection events written by IBM z/OS Communications Server, and write the event details to an activity log, and/or save them in an event history dataset. This event history dataset can be periodically archived to produce an audit trail of all IP Connections to and from all monitored z/OS IP stacks.

CA NetMaster® Network Management for TCP/IP is not itself a firewall, network filter, intrusion detection or network security product and must not be regarded as such. While its visibility of z/OS IP stack traffic positions it well to observe activity of interest to PCI DSS testing, CA NetMaster® Network Management for TCP/IP makes no security-related assessments about any of its observations. Such conclusions are the sole responsibility of staff knowledgeable about the specific network testing environment and the results expected at each point.

### PCI DSS Requirement Number and Area

**1.1.7** Justification and documentation for any risky protocols allowed (for example, file transfer protocol FTP), which includes reason for use of protocol and security features implemented

**1.3.7** Denying all other inbound and outbound traffic not specifically allowed

**2.2.2** Disable all unnecessary and insecure services and protocols (*services and protocols not directly needed to perform the devices' specified function*)

**3.3** Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).  
*Note: This requirement does not apply to employees and other parties with a specific need to see the full PAN; nor does the requirement supersede stricter requirements in place for displays of cardholder data (for example, for point of sale [POS] receipts)*

**4.1** Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks

### Using CA NetMaster® Network Management for TCP/IP to observe activity on monitored z/OS IP stacks

CA NetMaster for TCP/IP can observe and log FTP activity.

CA NetMaster for TCP/IP can list current connections filtered by local/remote port and/or IP address, and can show recent traffic volumes involving any port.

CA NetMaster for TCP/IP can list all protocols used by a z/OS IP stack.

CA NetMaster for TCP/IP SmartTrace can trace and display IP packets for a specified IP socket or connection on output from or input to any monitored z/OS IP stack. The packet content data can be viewed to ascertain whether it contains a full or masked PAN and/or is encrypted as expected at this point.

Further processing such as masking, encryption or decryption may be done at other points that are outside the scope of the CA NetMaster for TCP/IP product, or of the z/OS LPAR itself (i.e. on a non-z/OS platform).

Note that only authorized users are permitted to view packet content data. Other users are restricted to viewing only packet header data or no packet data at all.

## Legal

Copyright © 2008 CA. All rights reserved. DB2 and z/OS are trademarks of International Business Machines Corporation in the United States, other countries, or both. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. THIS DOCUMENT IS FOR YOUR INFORMATIONAL PURPOSES ONLY. TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT WILL CA BE LIABLE FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENT, INCLUDING, WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED OF SUCH DAMAGES. Notwithstanding anything in this publication to the contrary, this publication shall not: (i) constitute product documentation or specifications under any existing or future written license agreement or services agreement relating to any CA software product, or be subject to any warranty set forth in any such written agreement or (ii) serve to affect the rights and/or obligations of CA or its licensees under any existing or future written license agreement or services agreement.

## Source Document

The source for this document is the PCI DSS version 1.2, published in October 2008, as this was the current standard at the time of this writing. A free copy may be obtained at the PCI Security Standards Council ([HTTPS://WWW.PCISECURITYSTANDARDS.ORG/](https://www.pcisecuritystandards.org/)).