

Ralf Wiegand

50 Hasgate Drive
 Delmar, New York 12054
 Phone: (518) 669-8869
 E-mail: mrsun2001@yahoo.de

SUMMARY:

Network Security Architect/Engineer with over 15 years of Information Technology experience. Extensive experience in providing support in an Internet Service Provider (ISP) and enterprise data center environment, in the areas of security, systems, network administration, network architecture, design, network topologies and documentation. Significant experience providing security assessments and network security design in order to secure client assets and to comply with government regulations (HIPAA) and Payment Card Industries Data Security Standard (PCI DSS) compliance. Expertise working experience in heterogeneous environments, including VMware ESX server, Solaris, Linux and Windows. Current vice president of the Upstate New York UNIX User's Group, Albany, New York. Fluent in English and German Languages.

TECHNICAL SKILLS:

<i>Operating Systems:</i>	Solaris 10, OpenSolaris, Linux (RedHat Enterprise/Fedora, Debian, Windows Vista/ 2008 server, Cygwin)
<i>Networking:</i>	Cisco network equipment (routers/switches), Cisco IOS, multi-layer switching, Cisco Works, Nortel switches and routers, including Nortel 8010, 450 series, Centillion C100 switches, BCN/ARN Routers, protocol analyzers (TCPdump, WireShark, snoop), MRTG, Syslog, LogWatch, LogSurfer, Hping2, Dsniff, Tripwire, LSOF, Honeyd, Samba, Apache2, Opcon/XPS, Send mail/Postfix
<i>Security:</i>	Checkpoint Firewall, Nokia, Cisco PIX ASA 55xx series Firewalls, iptables Firewalls, ipfilter Firewalls, Cisco IOS Firewall Feature Set, ISS RealSecure, Cisco IDS, Snort NIDS, NMAP, Nessus, counter-intelligence honeypots / honeynets, bastion hosts, ntop, NST, Squid, IP Subnetting, IP Routing, TCP/IP traffic analysis, Log analysis, Vulnerability analysis, Penetration testing, Network Forensics, Network programming/scripting and enterprise security systems architecture including Active Directory, McAfee/Norton, Kerberos, PAM, SELinux, baz-arch/CVS/subversion, TrendMicro, ASSP/SPF
<i>Protocols:</i>	TCP/IP, FTP, HTTP, ICMP, IGMP, 802.11 wireless, 802.Q VLAN, SNMP, SMTP, NTP, OSPF, EIGRP, IPSEC, SSH, SSL, DNS, Active Directory Services
<i>Programming/Scripting:</i>	C, CGI, Perl, Unix shells (bash, csh), awk, sed, HTML and PHP, Python
<i>Databases:</i>	MySQL
<i>Hardware:</i>	IBM eServer BladeCenter H20/H21, IBM X3850 series servers, SunFire servers, Enterprise class servers, Enterprise storage
<i>Storage and High Availability:</i>	Enterprise and Network Storage (Sun/EMC), SAN, NAS, RAID storage, VERITAS storage management, Sun Cluster, Sun Volume Manager
<i>Tools/Virtualization:</i>	Microsoft Visio, Adobe Photoshop, Flash 9, Windows Office Suite of Products, OpenOffice, VMware ESX , Xen, Qemu,

CERTIFICATIONS/TRAINING:

- Checkpoint Certified Systems Administrator pending (final exam scheduled)
- Checkpoint Certified Systems Administration NGX I and NGX II Training
- Sun Data Center Specialty Certification
- Sun Storage Tek Elite Certification
- Certified Microsoft Systems Engineer (MCSE)
- Citrix Presentation Server 4.0: Architecture Training
- Citrix Access Suite 4.0: Common Management Platform Administration Training
- Certified Solaris 8 Administrator
- Sun Solaris 10 Advanced System Administration Certifications
- Cisco Certified Networking Associate (in progress)
- Cisco Certified Security Professional (in progress)
- Adobe Photoshop & Flash 8 Certification
- Extensive ISP/DataCenter Administration, using Debian/LAMP environments

PROFESSIONAL EXPERIENCE:

CORESense, Inc

May 2008 – October 2008

Senior IT Hosting Security Engineer

- Open Source Enterprise ISP Environment using Linux Debian Server Operating System.
- Managed over 200 hundred Enterprise clients in a clustered LAMP (Linux, Apache, MySQL and PHP) environment using SaaS (Software as a Service) custom build software.
- Installed and maintained POS (Point of Sales) hosts using Transport Layer Security/Secure Socket Layer authentication in a high security PCI compliant network topology using Internet connectivity
- Maintained and installed SSL Apache Certificates as request from clients
- Updated Coresense internal infrastructure from basic Samba/NIS environment to a Windows Enterprise 2008 Server infrastructure running Active Directory Authentication; added PCI compliant group policies and Norton Anti-Virus to all Laptops
- Replace corporate iptables based Firewall system with a Cisco ASA 5520 IPS/IDS appliance; hardened all customer host based iptables firewall rules.
- Pioneered the deployment of Coresense SaaS client/server installations, using VMware ESX server virtualization; developed long term plan to move to centralized backend storage
- Creation of a PCI three-tier client/server environment to strengthened client productivity and security when conducting client business transactions.
- Planned and implemented new short term backup strategy using Network Attached Storage (NAS) as well as remote sync backup to collocation site.
- Researched, planned and executed installation of IBM eServer BladeCenter HS20/21

severs and IBM X3850 servers, including advanced Cisco router and switch configuration; upgraded existing BladeCenters at co-location high secure site; maintained extensive permission and security plan to prevent security breaches in collocation site and at client networks.

- Installed and maintained MySQL cluster database setups in a SaaS environment.
- Installed LVS/keepalive enterprise server load balancing infrastructure using only Open Source tools.
- Maintained client and corporate email environments using postfix email servers; installed ASSP/SPAM server to reduce email attacks.
- Build high level BladeCenter hardware/software raid server configuration to maintain high availability and disaster recovery in 24/7/365 environment.
- Build from ground up IT Hosting Documentation, including server, client, security and network documentation
- Applied PCI standards to corporate wireless setup and updated Cisco Aironet Wireless network.
- Maintained Wikimedia site; recommended and purchased hardware and software; updated corporate Blog server; installed and maintained jabber messaging server.
- Converted email users from Postfix/Zimbra email server to MS-Exchange server.
- Provided Corporate Server and client infrastructure troubleshooting support; as well 24/7 all night 911 client support.
- Setup and maintained clustered “Nagios” and “hobbit” service monitoring environment for more them 200 hosts and services.
- Supervised junior administrators and conducted training sessions.

UNIVERSAL Technologies, LLC

January 2005 – May 2008

Senior Network Computing Engineer/Security Specialist

Client: New York State Department of Civil Service

- Provided on-site security, network and systems administration consulting services.
- Delivered Proof-of-Concept for Enterprise Virtualization and Consolidation using VMware Virtualization Suite of Products; implemented large VMware computing cluster in existing Enterprise Infrastructure; virtualized printing and scheduling software.
- Web Development using Studio Line H&M Software.
- Setup Data Encryption using PGP and GnuPG.
- Daily System Administration tasks of PeopleSoft and Cold Fusion/Web Logic Servers
- System Monitoring using Hobbit, Nagios and custom shell scripts.
- Responsible for providing network computing inventory services for the purpose of documenting DCS’s enterprise network computing environment.
- Delivered an extensive network computing inventory and a highly customized and detailed network topology diagrams depicting all network computing equipment.
- Provided comprehensive as built documentation in order for the agency personnel to effectively troubleshoot complex network problems, performing capacity planning, risk assessment analysis and reconstructing from a disastrous event.
- Collaborated with Java Developers to ensure the applications are secure, including network analysis and vulnerability testing of java application via Kerberos and PAM.
- Installed Source Code Control (CVS/subversion) on Redhat Linux Enterprise Server using Kerberos, PAM and Samba authentication with Active Directory.

- Implemented Technical Blog (Drupal) and Wikipedia Servers, for daily tracking of Trouble Shooting Tickets and Administration Tasks.
- Interacted with stakeholders of the project to gather a complete understanding of the goals and objectives.
- Application security analysis performed on multiple applications and databases, including Java-based applications and Oracle.
- Collected data, through inventory and personnel interviews, that spans the entire enterprise network computing environment for DCS.
- Data collection and review, including presentation of collected data to IT Executive for clarification, misinterpretation and completeness, review templates for inventory documentation format, review templates for network topology format, review paper drawing sizes for approval by the IT executive for data collection completeness to move forward to the analysis phase.
- Assessed the overall enterprise network computing environment. This includes Security infrastructure assessment, Single points of failure, Operating System assessment, High availability assessment, Reliability assessment, Scalability assessment, Productivity assessment
- Provided detailed documentation for DCS's enterprise network computing environment derived from the data collection, inventory and network topology diagrams.
- Develop a Hands-on User Training Manual for DCS staff member, to continue ongoing documentation updates and to prepare for agency's relocation phase.
- Extended Data collection beyond conventional methods through UNIVERSAL Technologies NST Security Toolkit and other advanced Open Source tools.
- Environment: Solaris 2.9; Checkpoint Firewall Secure Platform; Cisco Pix Firewalls; Cisco Works Enterprise; MS Active Directory; MS Windows; Citrix Farm; Postfix; Cisco IDS Works; Redhat Linux Enterprise 4; Oracle.

Client: New York City Department of Law

- Upgraded Web Proxy Server with a new Open Source Web Proxy server solution. This included the installation of a new ISA Microsoft Proxy server and a Sun/Squid Proxy server for testing by client staff.
- Citrix server documentation and administration.
- Performed Unix system and network administration tasks including the following:
 - Solaris Patch Upgrades to Firewall system.
 - Firewall documentation (rules) and Disaster recovery test (firewall failover test).
 - General System and Network administration tasks.
 - Detailed Network Device documentation.
 - Setup and tuning of a network intrusion detection systems.
 - Setup of system and network monitoring.
- Checkpoint Firewall/Solaris patch install, including review of current patch level on the main Checkpoint firewall.
- Sun server administration and maintenance, including troubleshooting, upgrades and component replacements.
- Firewall failover test and the documentation of all firewall rules.
- Cisco and network documentation, including create network device documentation and integrate this information, including Visio drawings in the existing client system documentation.

- Environment: Solaris 2.9; Checkpoint Firewall-NG; Cisco Pix; Cisco switches and routers; MS Exchange; ISS Real Secure; Sendmail; Postfix; Sun Fire 220R, 440R, 280R; Netscape/I-Planet 4.

TIM Computer Systems, Inc. - Albany, NY
Senior Network and Security Engineer

November 1997 to January 2005

- Provided system and network engineering in the specification, procurement, development, implementation, and test of large-scale corporate network strategies and core Information technology systems.
- Extensive experience in Cisco PIX Firewalls, Virtual Private Networks, network security, TCP/IP, Cisco IOS, multi-layer switching, EIGRP, BGP, VLANs, and IP Subnetting.
- System Administration in heterogeneous environments (including Solaris 2.6 – 2.9, Windows 95/98/NT/2000/2003, Linux).
- Analyze and develop integration process of heterogeneous networks.
- Data Center Management and facility network/operating system support, including setup and management of DNS and LDAP, Apache/SSL web and MySQL servers, as well as Snort IDS and ipfilter firewalls.
- Performed intrusion detection and security responses in web application environments, including Apache, Tomcat, Java-based applications, PHP based applications, Oracle databases and mysql servers.
- Setup and integrated complex storage area networks and remote system administration in a multi operating system environment.
- Sun hardware and software administration, installation and maintenance.
- Performance monitoring, system tuning, capacity planning and report generation using custom programs as well as open source tools and utilities.
- Veritas Volume Manager and Filesystem administration and maintenance
- Setup of corporate e-mail, web and application servers; creation of hot-sync backup model for corporate fail over site. Supported email systems including Exchange and Send mail.
- Management, troubleshooting and research in the area of Wide/Local Area and Metropolitan Area Networks.
- Maintenance of Sendmail/Postfix configuration files
- Integration of UNIX and Windows NT using Samba.
- Integration of Cisco Intrusion Detection Systems and Cisco Works into the Enterprise.
- Wide-ranging experience in analyzing False/Positive network attacks and countermeasure response management.
- Experience in the development and programming of C/Python/Perl/PHP Applications and HTML WebPages.
- Technical writing of white papers, draft RFP's, development of system acquisition, software and system project documentation.
- Interface with customers and corporate management, evaluate the latest applicable technologies, prepare functional specification and test plans.
- Assist customers with implementation and resource management.
- Documented present state of work, including network inventory, network diagrams and system layouts using Visio software.

- Reported available results and predictions in a non-technical level format, using industry standards.
- Developed and conducted training classes to clients in the UNIX and network security areas.

EDUCATION:

- College of Saint Rose, Certification in Computer Science, Albany, New York
- German Federal Government Postal Service (Deutsche Bundespost AG) Degree in Business and Communications
- Federal Republic of Germany Officer Diploma (Beamter)
- Kirchhain High School, Kirchhain, Hessen Germany

REFERENCES:

Available Upon Request