

The City of Burbank Improves Network Infrastructure with Juniper Networks

Organization:

City of Burbank

Industry:

Government

Challenge:

Upgrade and modernize city's communication network

Solution:

Juniper Networks NetScreen network security appliances

Benefits:

- Vastly improved network security
- Greater speed and reliability across network
- Secure and assured network system provides internal departments and the general public access to the data that is most relevant to them

Located in the heart of Southern California's entertainment industry, the city of Burbank boasts a population of just over 100,000 people, many of whom work for local entertainment legends such as Walt Disney Studios, Warner Brothers Pictures and NBC Studios. This seventeen-square-mile city boasts 22 parks, 13 ball fields, two municipal pools and a municipal golf course. To keep things running smoothly, the city employs 1,500 people spread across 14 departments.

Two years ago, the city was struggling with an outdated and piecemeal communications network that was proving to be increasingly ill suited to the demands of those who relied on it. Information processing and retrieval was inefficient and time-consuming, requiring data to be transferred manually between departments. Frequent network connection problems were compounded by inadequate backup and failover technologies.

The City of Burbank relies on a Supervisory Control and Data Acquisition (SCADA) system, an OC-3 fiber ring around the city, to monitor the electrical system for the city's power grid. The city's IT staff needed a secure and reliable network solution that would allow connectivity between the City LAN and the SCADA Network

An equally pressing issue facing the staff was the impending debut of the Magnolia Power Project, a \$300M power plant joint effort by six local governments scheduled to go live in mid-2005. Burbank realized it needed to upgrade its network security system so it could share data securely with each of the cities involved in the project.

"The technology behind the Juniper Networks NetScreen network security appliances made it a clear-cut winner in my mind."

Perry Jarvis
Network Operations Manager
City of Burbank, CA

The Solution

With the help of Data Systems Worldwide, Inc., an IT solutions firm that designs, builds and manages enterprise application infrastructure, the city of Burbank selected the Juniper Networks firewall and virtual private network (VPN) solution and intrusion detection and prevention (IDP) solution because of their robust security features, comprehensive network coverage and excellent value for money.

Perry Jarvis, network operations manager for the city of Burbank said, "The technology behind the Juniper Networks security appliances made it a clear-cut winner in my mind. We needed a centralized security solution for the entire city and Juniper was the only vendor that offered us a traditional firewall platform and a true real-time Intrusion and Detection System. The Juniper Networks IDP was a vital component to securing our network."

Juniper Networks NetScreen IDP-100s are deployed throughout the city protecting the corporate network connection to the Internet. NetScreen IDP-100s provide up to 200 Mbps throughput and operate in-line to detect and drop malicious attacks in real-time.

Working in conjunction with Scott Mellon, an electrical engineer at Burbank Water and Power, the City designed a secure solution utilizing both Juniper Networks firewalls and IDP that gave us the ability to safely connect the city LAN to the independent SCADA network, thus safely allowing Internet access and remote data acquisition for the SCADA system, for such activities as load forecasting.

The IT staff replaced an obsolete Symantec firewall connected to a proxy server with the Juniper Networks NetScreen-208 appliance. The NetScreen-208 offers up to 550 Mbps firewall and up to 200 Mbps IPSec VPN throughput.

The city also invested in the Juniper Networks NetScreen-204, which offers up to 400 Mbps of firewall performance and up to 200 3DES IPSec VPN performance with support for up to 128,000 sessions. The firewall is used in conjunction with a Juniper Networks NetScreen IDP-100 appliance to protect the city's library patron network.

Another part of the city's network security infrastructure is a group of Juniper Networks NetScreen-5GTs used to make remote

sites, such as the landfill office, part of the secure VPN deployed at the main office. NetScreen-5GTs offer up to 75 Mbps of firewall throughput and up to 20 Mbps of 3DES IPSec VPN performance. With embedded antivirus protection, the appliances provide a fast, secure and assured connection between the remote sites and the main office.

The Benefits

Since deploying the Juniper Networks security products, the city of Burbank has seen a vast improvement in its network security. With the IDP and firewall/VPN devices installed at critical access points on the network, attacks against the system are detected and repelled automatically twenty-four hours a day, seven days a week. As a result, Denial of Service Attacks, port scans and other popular Internet attacks no longer flood the system and the city's IT staff is able to take a proactive approach to security. Suspicious traffic not immediately blocked by the IDP is flagged and researched.

Burbank city employees also enjoy greater speed and reliability across their network. With the high throughput capacity of the Juniper Networks NetScreen security devices, workers no longer face slow data transfer rates or application time-out errors.

Jennifer Wyatt, Information Technology Director for the city, added "Since securing our network with Juniper Networks city employees haven't been disrupted by networks attacks. We no longer have to waste time and effort dealing with these sorts of issues."

The secure and assured Juniper Networks security system provides city departments and the general public access to the data that is most relevant to them. As Jarvis says, "We're now able to make a wide range of information available to the public. Customers can log in and view their electric and water bills, access the library network and even view Channel 6, our public channel, online via streaming video."

The Magnolia Power Project will go live the summer of 2005 and the Juniper Networks NetScreen security network will serve as a vital link, providing targeted data and auto-generated status reports to each of the cities invested in the project.



**CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS
FOR NORTH AND SOUTH AMERICA**

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888-JUNIPER (888-586-4737)
or 408-745-2000
Fax: 408-745-2100

www.juniper.net

EAST COAST OFFICE

Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978-589-5800
Fax: 978-589-0800

**ASIA PACIFIC REGIONAL
SALES HEADQUARTERS**

Juniper Networks (Hong Kong) Ltd.
Suite 2507-11, Asia Pacific Finance Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

**EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS**

Juniper Networks (UK) Limited
Juniper House
Guildford Road
Leatherhead
Surrey, KT22 9JH, U. K.
Phone: 44(0)-1372-385500
Fax: 44(0)-1372-385501

Copyright 2005, Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

The following are trademarks of Juniper Networks, Inc.: ERX, ESP E-series, Instant Virtual Extranet, Internet Processor, J2300, J4300, J6300, J-Protect, J-series, J-Web, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, NMC-RX, SDX, Stateful Signature, T320, T640, and T-series. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.