

RIVIERA HOTEL AND CASINO HITS THE JACKPOT WITH JUNIPER NETWORKS SECURITY INFRASTRUCTURE

Summary

Industry: Gaming and hospitality

Challenge:

- Unreliable, inflexible firewall required constant maintenance.
- Improve operational efficiency by consolidating security appliances.
- Ease burden of PCI and other regulatory requirements.
- Give employees and contractors convenient, secure remote access.

Network Solution: Juniper Networks SSG550M Secure Services Gateway firewall/VPN with unified threat management (UTM), SA Series SSL VPN Appliances, IDP600 Intrusion Detection and Prevention Appliance, and Network and Security Manager.

Results:

- Saving \$280,000 per year on firewall configuration and maintenance.
- Consolidates security infrastructure for comprehensive, coordinated protection and lower operational costs.
- Mitigates the risks of network and application attacks and regulatory non-compliance.
- Meets compliance requirements for comprehensive network security and auditing. Provides easy, secure remote access contractors via any standard Web browser.

Security can't be left to chance when it comes to protecting a casino—especially a Las Vegas icon like the Riviera Hotel and Casino. With a reputation forged in the days of Dean Martin and Liberace, the Riviera is known today for the high customer value it provides and its excellent service. The Riviera has more than 2,000 rooms, 100,000 square feet of casino gaming action, and live stage shows nightly. The casino is among the most active in Las Vegas, with gambling options that range from the exclusive players club and the sports book to video poker and penny slots.

The nature of gaming makes casinos a lucrative target for criminals and scammers. Sensitive customer, corporate, and employee information residing on the corporate network is a literal gold mine. Financial transactions are occurring everywhere—on the casino floor, at restaurants and in the hotel, in entertainment venues and the convention center, and at myriad kiosks across the property. At the same time, casinos must comply with a broad array of state gaming laws, as well as other industry and federal regulations such as Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), and Health Information Portability and Accountability Act (HIPAA).

These are some of the challenges facing Tim Wilbur, executive director of IT, CIO, and David Hugar, associate director of IT, CTO, at the Riviera Hotel and Casino. To make their jobs even more interesting, the Riviera also hosts Defcon, the largest hacker convention in the world.

Selection Criteria

The firewall is the first line of any organization's defense-in-depth strategy, but the Riviera's incumbent firewall/VPN was so difficult to configure and manage that ongoing security operations were labor-intensive and costly. Updating the firewall's signature files to protect against the newest threats consumed many hours of IT staff time each week. Configuring and changing firewall policies were equally laborious because of the incumbent firewall's lack of flexibility. With adult content and gaming traffic permitted on the Riviera's network, security policies can't be set by default, as they might in a different type of corporation. Instead, the IT team must have highly granular control over what type of applications and traffic to permit on the network.

In an attempt to stop the 2 a.m. calls to reboot the firewall and get operating costs under control, the Riviera's IT team deployed the managed version of the same vendor's firewall, but it lost the granular control over policies it so needed to protect its critical business and gaming systems.

"We needed a firewall that was rock solid, but had 100 percent manageability," said Wilbur. After evaluating three leading firewall/VPN with UTM products, the Riviera chose Juniper Networks® SSG550M Secure Services Gateway, which delivers an ideal mix of high performance, security, and LAN/WAN connectivity.

Solution

The SSG550M protects the Riviera's data center server cluster, which is at the heart of the company's business operations. The data center runs casino financials, video poker and slots, hotel property management, business financial systems, email, websites, and many more applications. The data center includes more than 30 Windows and Linux servers and two AS/400 mainframes.

With SSG550M, traffic flowing in and out of the Riviera's server cluster is protected from worms, viruses, spyware, trojans, and malware by a complete set of UTM security features, including stateful firewall, IPsec VPNs, intrusion prevention system (IPS), antivirus, anti-spam and Web Filtering. Stateful firewall performs access control and stops network level attacks. IPS (or Deep Inspection firewall) stops application level attacks. Anti-spam blocks known spammers and phishers. Web filtering blocks access to known malicious download sites or inappropriate Web content. The SSG550M also has denial of service (DoS) mitigation capabilities. Complementing the powerful UTM security is a robust routing engine that allows the SSG550M to function as a firewall and routing device to reduce capital and operational expenses.

"Within 20 minutes of plugging in the SSG550M, we locked down illegitimate traffic that had been passing through undetected with our old firewall," said Hugar. "We thought we knew our environment, but the SSG550M gave us new levels of visibility and better protection."

"We save \$280,000 per year in man-hours and the value of consolidated security with Juniper Networks."

Tim Wilbur
IT director,
Riviera Hotel and Casino

SSG550M Secure Services Gateway gave the Riviera's IT team the granular control over security policies that its old firewall couldn't provide. "The SSG550M is so easy to use. The user interface and command line are so easy that I can make policy changes on the fly and know it's going to work," said Hugar.

The Riviera takes advantage of the routing engine in the SSG550M to connect to the company's Black Hawk Casino in the Denver area. Because of the previous firewall's limitations, Riviera's Black Hawk Casino had to be connected to the core network via a gateway. "Inbound traffic went through the firewall to another gateway to a point-to-point connection to another gateway, and then the traffic was managed on the Black Hawk side. There was a lot of overhead," said Wilbur. "Now with the SSG550M, we fire traffic at them."

The Riviera also uses the Juniper Networks IDP600 Intrusion Detection and Protection Appliance inline network IPS to protect its network against a wide range of attacks and help the company meet its PCI compliance and audit requirements. IDP600 provides zero-day protection against worms, trojans, spyware, keyloggers and other malware from penetrating the network or spreading from already infected users. IDP600 also provides information on rogue servers as well as applications and operating systems that may have been unknowingly added to the network. Application signatures enable accurate detection of specific applications, such as peer-to-peer or instant messaging. Not only can administrators control the access of specific applications, but they can ensure that business-critical applications receive a predictable quality of service (QoS) by enforcing bandwidth limitations on nonessential applications.

The Riviera relies on Juniper Networks SA Series SSL VPN Appliances to provide secure remote access to employees working outside the office as well as contractors. The previous firewall included an IPsec VPN client, which demanded that IT perform the time-intensive task of installing and managing software on employees' computers, whether company-issued or employee-owned. The use of SSL, the security protocol found in all standard Web browsers, eliminates the need for client-software deployment, changes to internal servers, and costly ongoing client maintenance and desktop support. In addition, the SA Series provides end-to-end layered security, with endpoint client, device, data, and server security controls. Secure access is identity-driven and specified by user group or role, as well as by network, device, and session attributes.

The Riviera's IT team uses Juniper Networks Network and Security Manager to manage the IPS policies on the SSG550M. NSM is a centralized management solution that handles the network configuration with local and global security policy deployment for Juniper's firewall/VPN, SSL VPN, and other Juniper solutions. NSM provides easy access to extensive logging and fully customizable reporting.

Results

Juniper's integrated security solutions have helped the Riviera improve its information security posture, ease the burdens of regulatory compliance, simplify its security infrastructure, and reap significant hard dollar savings.

The Riviera's network infrastructure might be under constant attack, but it was put to the ultimate test when hackers from around the world attended Defcon. "It was very pleasant for us when we hosted Defcon. We could see the number of attacks rise, but no graffiti showed up and no one got through," said Hugar.

Thanks to the integrated security of the SSG550M Secure Services Gateway, the Riviera consolidated disparate security appliances, including separate products for intrusion prevention and firewall, and now relies exclusively on one box for comprehensive security protection. "In the past, we needed multiple security layers to protect against zero-day issues.

We're very satisfied with the SSG550M, and it's the sole-source firewall/IPS for us," says Wilbur.

The Riviera is ringing up savings of \$280,000 per year by switching to the SSG550M. "Our old firewalls required maintenance 24 hours a day. Policies regularly failed, and we had to reboot them constantly. The firewall was impacted by the installation of any other software, which incurred more man-hours. We had to manage a separate IPS and firewall, and logging was yet another issue," said Wilbur. "Now, one IT person manages the SSG550M Secure Services Gateway, and he can do lots of other projects besides babysit the firewall."

The SSG550M has proven its reputation for robustness at the Riviera. "The SSG550M has been running for almost two years and we've never restarted it," said Wilbur. "The SSG550M is solid. It sits in the rack until I have to put in a policy or add a role."

With application- and network-layer protection against attacks and malware afforded by the IDP Series and SSG550M, the Riviera can more easily meet its PCI and other regulatory requirements. "We use the IDP Series and firewall logs every day for SOX compliance," said Hugar.

When on the road or working from home, employees can easily and securely access their corporate applications from any standard Web browser, thanks to the SA Series. "Our users love the SSL VPN," said Wilbur. "Remote users have access to all the applications and resources they would have if they were in the office. It's as simple as telling people: "Go to your browser, put in this network name and log in."

IT likes it too, since staff no longer has to install and configure IPsec VPN client software for employees or contractors.

Role-based access makes it easy to control which users have access to which resources and from what location.

For More Information

To find out more about Juniper Networks products and solutions, visit www.juniper.net.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters

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

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2009 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. 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.