Are Cloud Computing and Mobility Making You More Vulnerable?

Is your enterprise planning to leverage cloud computing and mobile computing in order to improve business agility, increase employee productivity, and lower capital expenses?

If so, you are no doubt aware that your enterprise is also increasing its attack surface. Cloud-based technologies, smartphones, social media and mobile applications give cybercriminals and hackers more opportunities to find weak points in your defenses and unpatched vulnerabilities on your systems and devices. A single Achilles' heel can result in a loss of confidential information and intellectual property worth millions of dollars.

To keep your data and network safe, and to succeed as what Juniper Networks calls a “Cloud-Enabled Enterprise,” your organization must overcome three security challenges. You need to:

1. Integrate and deploy a comprehensive set of security services to detect and block an expanding array of threats.

2. Close the gap between intelligence and enforcement to cope with zero-day and advanced targeted attacks.

3. Leverage centralized visibility and management to identify and address threats wherever they are detected inside or outside the network perimeter.

This short paper provides an overview of how Juniper Networks helps you address these three challenges and protect data as your organization evolves into a Cloud-Enabled Enterprise.

Integrate and Deploy a Comprehensive Set of Security Services

Today you need to defend against a widening array of attack techniques. Threat actors are devising new types of obfuscated malware for zero-day attacks, new spear phishing and social engineering techniques, and new forms of advanced persistent threats (APTs) that can hide on your network for weeks or months.

To counter these threats, you not only need to deploy a range of diverse security technologies, you must be able to deploy and manage them cost-effectively. In addition, you need to make sure
that your security solutions are integrated, so that an attack detected by one technology can be blocked by another. Yet supporting and integrating multiple point products is very expensive and difficult.

You can count on Juniper Networks to address these issues with its SRX Series Services Gateways and the new Sky Advanced Threat Prevention service.

SRX Series Services Gateways provide a wide variety of critical security services, including:

- Stateful firewall capabilities
- Unified threat management (UTM) technologies such as antivirus, antispam, web filtering and content filtering
- Intrusion prevention system (IPS) capabilities
- Protection against denial of service (DoS) and distributed denial of service (DDoS) attacks
- Application firewall and application quality of service (QoS) features
- SSL encryption and decryption and support for IPSec VPN tunnels

These security services are integrated with core firewall capabilities. For example, attacks detected by the IPS features can be blocked automatically by the firewall.

The breadth of security technologies included in the SRX Series Services Gateways allow you to defend against malware, phishing and social engineering attacks, DDoS attacks, malicious URLs and many other threats with one integrated solution.

Juniper provides an additional critical layer of defense with Sky Advanced Threat Prevention. Sky Advanced Threat Prevention is a cloud-based service that quickly identifies known malware using a cached database, then uses static analysis, dynamic analysis (sandboxing), and unique deception techniques to detect new forms of malware and zero-day threats.

As illustrated in Figure 1, SRX Series Services Gateways and the Sky Advanced Threat Prevention service are integrated with each other and with Juniper’s Spotlight Secure threat intelligence platform (discussed below). As a result, when information on attacks is captured anywhere on your network (or by other Juniper customers) it can be distributed quickly to SRX Gateways throughout the enterprise. That greatly reduces the window during which zero-day attacks can escape detection and blocking.
Close the Gap Between Intelligence and Enforcement

We know that threat intelligence is a critical weapon in the war against cybercriminals and hackers. Threat intelligence allows security defenses to block probes and detect advanced attacks before they can do serious damage. But threat intelligence loses most of its value if it is distributed too slowly, or if it doesn’t reach all of the enterprise’s enforcement points.

Fortunately, you can close the gap between intelligence and enforcement with Spotlight Secure and network security management with Junos Space Security Director from Juniper Networks.

Spotlight Secure

The Spotlight Secure threat intelligence platform gathers a wide range of threat intelligence from Juniper’s own threat intelligence organization, from third party threat feeds, and from the threat detection devices you have already installed on your network.

Spotlight Secure collects signatures and threat intelligence of many types, including:

- **Command and control (C&C) and botnet domains and URLs**, so you can block traffic from servers on the Web that are used to launch phishing and DDoS attacks, manage advanced attacks, and exfiltrate data out of enterprises.
- **GeoIP data**, so you can set policies to monitor or block traffic to and from specific geographical regions.
- **Device fingerprints**, so you can block, restrict or allow traffic from devices that have been uniquely identified based on attributes such as their browser version, add-on apps, IP address, time zone and fonts.

Junos Space Security Director

As shown in Figure 1, Spotlight Secure can push the latest and most relevant security intelligence to firewalls via Junos Space Security Director, an application that is part of the Junos Space Network Management Platform. Junos Space Security Director can update thousands of firewalls simultaneously, without the need for manual changes to firewall policies. That helps you neutralize zero-day attacks and advanced attacks in progress, before they can do serious damage.

Leveraging Centralized Visibility and Management

Today you have to assume that some attackers will be able to penetrate the perimeter and establish beachheads inside. That means your team needs to be able to spot suspicious activities anywhere they occur, even in the far corners of the network. You also need to take immediate action to shut down outbound communication to the attacker’s command and control servers, and to update firewalls across the enterprise so they can stop further penetrations by the attackers.

The Junos Space Security Director gives you centralized visibility and management of essential security services (Figure 2).

Key features of Security Director related to visibility include:

- An easily customized dashboard, with predefined widgets to track key threats and trends and fast drill-down to in-depth security data
- Threat maps, graphs, and other visualization tools to make issues visible at a glance and speed up the analysis of threat patterns.
- Clear, intuitively organized views of security events and policy rules, with features to filter, sort and aggregate key data.
Security Director also allows you to manage all phases of the security policy lifecycle for stateful firewall, UTM, IPS, application firewall, VPN and network address translation. A single web-based interface lets you create firewall, IPS, NAT and UTM rules using wizards and drag-and-drop techniques. An automated rule analysis feature makes recommendations for creating and deploying policies. In addition, with Security Director you can distribute policies to hundreds or thousands of devices with a few clicks. These features help you stay ahead of attackers while ensuring consistency and minimizing management costs.

Summary: Three Ways to Eliminate Your Achilles Heel
Table 1 summarizes how Juniper Networks can help you address the three critical security challenges for Cloud-Enabled Enterprises discussed in this paper.

For more information, please visit www.juniper.net/unite.