NEXT-GENERATION SECURITY FOR TODAY'S DATA CENTER

Juniper Networks Next-Generation Security Will Prevent Data Breaches with Greater Accuracy, Speed, and Breadth of Protection

Challenge

The uptake of cloud computing and social media combined with the rise and sophistication of botnets, advanced persistent threats (APTs), distributed denial of service (DDoS), and Web application attacks makes the data center more vulnerable to data breaches than ever before.

Solution

Juniper Networks' next-generation security products offer enterprises unparalleled protection against data exfiltration, website outages, and other serious data center threats.

Benefits

- Definitive hacker identification with almost zero false positives
- Global sharing of intelligence on hackers to speed detection and monitoring
- Flexible counterresponse at both the application layer and network firewall
- Cloud scale firewalling and IPS

Today, companies are struggling to keep pace with the increasing volume and sophistication of cyber attacks, particularly those aimed at Web applications and servers, which deal in high value traffic and typically reside in data centers. According to a 2013 Ponemon Institute report commissioned by Juniper Networks, web-based (65 percent) and denial of service (DoS) attacks (60 percent) were cited as the most serious types of attacks experienced by companies. More telling, a majority (60 percent) of security professionals also indicated that current next-generation firewalls and IP reputation feeds only address part of the cybersecurity threat, leaving significant exposure to the most concerning attacks. Protecting against these attacks requires security systems that incorporate real-time, definitive, and actionable intelligence about attackers.

Juniper Networks not only recognizes the need for new and comprehensive next-generation security, but has, for some time, been pioneering the realm of definitive attacker profiling. With Juniper Networks® Junos® WebApp Secure, Juniper offers a Web application protection product that uses intrusion deception to definitively identify hackers with near zero false positives. It then synthesizes a variety of data in order to fingerprint and monitor hackers, and, with a very high degree of accuracy, triggers counterresponses that thwart attacks early in the cycle—before an exploit can even be launched. Now, further advancing this next-generation approach, Juniper will be offering Junos Spotlight Secure—a cloud-based hacker device ID intelligence solution. This new service, which is leveraged by Junos WebApp Secure and Juniper Networks SRX Series Services Gateways, will act as the consolidation point for attacker and threat information, feeding intelligence in real time to Juniper security solutions. It will put non-IP-based attacker profiling at the center of a framework that gathers and distributes attacker fingerprints to a worldwide network of inline security solutions. With a broad security and networking product installed base and this new system for distributing definitive hacker IDs, Juniper is poised to change the speed and accuracy with which security breaches are prevented for its customers. The Junos Spotlight Secure attacker intelligence service will set a new efficacy bar for all security and networking vendors.

The Challenge

Despite significant investment in security technology, organizations are still seeing a gap in security effectiveness. The reason is simple. Traditional defenses rely on signatures and IP addresses. Signatures, used in products like antivirus and intrusion prevention systems (IPS), are effective at detecting known attacks at the time attacks are launched. They are not effective, however, at detecting new attacks or capable of detecting hackers who are still in the reconnaissance phase, probing for weaknesses to attack.

IP reputation databases, meanwhile, rely on the notion that all bad actors can be identified by their IP addresses, and so share this information across systems. Unfortunately, this is as ineffective a methodology as the use of a postal address to identify a person definitively. Like a postal address, an IP address is a singular piece of information, and more data is needed for definitive personal identification. If you consider that many people can reside in a single structure (or at a single IP address), it begins to make sense why traditional Internet defenses are only marginally effective against hackers. For example, jailing a whole apartment building for the actions of one resident is disruptive to the lives of the other non-involved residents. Likewise, blocking an IP address that represents the entirety of a company's employee base is disruptive to that business. To further complicate matters, consider how hackers can easily impersonate legitimate users, or simply change the IP address they are using by pointing to a different anonymous proxy.

Additionally, consider how new platforms, such as virtualization and cloud computing, do not even use IP addresses as identifying marks. In other words, bad actors have many easy ways to dissociate themselves from IP addresses.

As limited as they are, signatures and IP address are the concepts on which the majority of security advancements have been made, including the newer intrusion prevention systems, reputation feeds, and so-called next-generation firewalls.

The game is changing and so, too, must the focus. The focus must be on attackers and not on chasing yesterday's attacks. A new spotlight needs to fall on systems not only capable of uniquely identifying and "fingerprinting" attackers, but also able to share this information across a broader network so that attackers can be monitored and stopped even as they move from target to target.

Juniper Networks Next-Generation Security for Data Centers

Juniper Networks next-generation security protects against today's biggest data center threats. As identified by customers, these threats include disruption of availability and hacking/data breaches of Web applications. Distributed denial of service (DDoS) protection ensures that applications remain online and responsive to legitimate users. Intrusion deception accurately identifies hackers and enables flexible counterresponses both at the application layer and, through tight intelligence integration, at the network firewall. The Juniper security product line provides the most comprehensive data center protection regimen of its kind, comprising and far surpassing the protections possible with next-generation firewalls, reputation feeds, IPS, and Web application firewalls alone.

These next-generation security products are optionally available on dedicated hardware, hypervisors, and SDN-centric data centers. For an enterprise or service provider with physical, virtualized, or hybrid data centers and plans toward software-defined networking (SDN), there is no comparable alternative for data center protection breadth, detection accuracy, and SDN architecture support.

Features and Benefits

- Definitive hacker identification with almost zero false positives
- Global sharing of intelligence on hackers to speed detection and monitoring
- Flexible counterresponse at both the application layer and network firewall
- Protection against volumetric and "slow-and-low" DDoS attacks to maximize availability
- Cloud scale firewalling and IPS
- SDN-centric architecture that enables security to span physical and virtual infrastructures

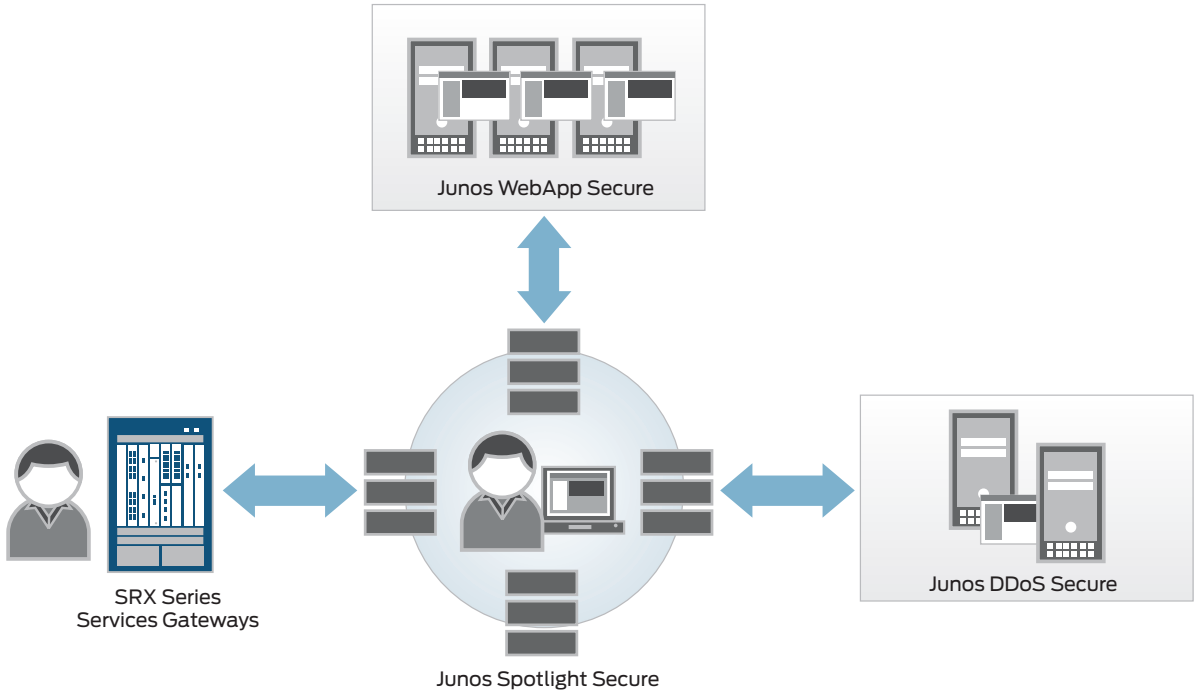

Figure 1: Junos Spotlight Secure in conjunction with Junos WebApp Secure will provide real-time global attacker intelligence sharing.

Solution Components

For unparalleled protection against data exfiltration, website outages, and other serious data center threats, Juniper Networks offers next-generation security products that include the Junos Spotlight Secure attacker database, Junos WebApp Secure, SRX Series Services Gateways, and Junos DDoS Secure.

Junos Spotlight Secure is a new cloud-based threat intelligence solution that will identify individual attackers at the device level (versus the IP address) and track them in a global database. The product will create a persistent fingerprint of attacker devices based on more than 200 unique attributes, delivering precision blocking identification of attackers without the false positives that could impact valid users. Once an attacker is identified and fingerprinted on a subscriber's network using Junos WebApp Secure, the global attacker intelligence solution will immediately share the attacker profile with other subscribers, providing an advanced real-time security solution across multiple networks. When compared with currently available reputation feeds that rely on IP addresses, Junos Spotlight Secure will offer customers more reliable security intelligence about attackers and all but eliminate false positives.

Junos WebApp Secure takes Web application protection to the next level, using the latest intrusion deception technology to definitely identify and mislead attackers while simultaneously profiling and fingerprinting them. Deployed in front of application servers behind the firewall, Junos WebApp Secure is enhanced with the integration of security intelligence from other sources provided by Junos Spotlight Secure. With this integrated intelligence, Juniper will be able to deliver threat mitigation with significantly better accuracy compared to IP-address-only approaches like current next-generation firewalls and reputation feeds, monitoring and identifying hackers as they move from target to target around the world.

Juniper Networks SRX Series Services Gateways integrated with Junos WebApp Secure. The SRX Series is now integrated with Junos WebApp Secure and benefits from intrusion deception technology, as well as the cloud-based Junos Spotlight Secure attacker database. The integration extends the ability of the SRX to block attackers that are identified at the security perimeter, and is particularly effective in blocking high volume automated hacking tools. This capability is new and combines with the SRX Series' existing broad support for visibility to and control of application use as well as its integrated malware detection and intrusion prevention capabilities. The combination of application-level awareness and protections makes the SRX Series one of the most comprehensive next-generation security packages on the market.

Junos DDoS Secure delivers fully automated DDoS protection for websites and Web applications. This solution uses a unique, behavior-based approach to DDoS mitigation that provides protection up to 40 Gbps for high volume attacks, as well as advanced "low-and-slow" application attacks with minimal false positives. Junos DDoS Secure can be deployed as a hardware appliance or as a virtual machine (VM) in private, public, or hybrid cloud environments.

Summary—Next-Generation Security for Broad Data Center Protection Through Detection Accuracy and SDN Architecture Support

Fortified by the Junos Spotlight Secure global attacker intelligence service, Juniper Networks' next-generation security products for the data center will enable customers to benefit from more definitive intelligence about threats and individual attackers across a wide number of networks. Built on automated and actionable intelligence that can be quickly shared and scaled to meet the demands of modern and evolving networks, these products taken together will enable broad defense against attackers and threats targeting data centers from inside and outside the perimeter.

Further, these Juniper security products will be incorporated into security service chains as part of Juniper's Software Defined Networking strategy. This integrated approach will allow additional intelligence to be shared across network layers and facilitate quick deployment of security services as part of the SDN service chains.

Next Steps

For more information about Juniper's next-generation security, please contact your Juniper Networks sales representative or visit **www.juniper.net/security**.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. 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 and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: 31.0.207.125.700
Fax: 31.0.207.125.701

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

3510481-002-EN Apr 2013 Printed on recycled paper