Juniper and Impulse Deliver Cloud-Managed Mobile and IoT Security

Automating device visibility, security, and orchestration for enterprise networks

Challenge

Approximately 37% of data breaches are the result of unauthorized network access[1]. Each unknown device attempting to access your network is a potential source of invasion and compromise.

Solution

Juniper and Impulse offer a joint solution that supports a highly scalable, distributed network environment for all user and IoT devices. This solution enables automated agentless device identification, enterprise wireless data encryption provisioning, and real-time security policy enforcement and compliance.

Benefits

- Cloud-managed deployment and support reduce cost of ownership and business risk
- Simplified, scalable network integration ensures a secure, end-to-end environment while improving the user experience
- Automated assessment, enforcement, and self-remediation orchestration simplifies security policy management
- Third-party intelligence publishing and automated security threat detection reduce attack risks

[1] Source: http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html

The explosion of BYOD and Internet of Things (IoT) devices, coupled with advances in wireless technologies and readily available cloud-based applications, has driven the need for enhanced security to protect business-critical data and address regulatory compliance requirements.

The Challenge

A common challenge for IT managers is enforcing security compliance policies while maintaining a positive user experience and reducing help desk calls in support of BYOD and guest users. Organizations are also faced with the daunting task of correlating mobile device information and user identity over time and across network segments for regulatory compliance, security forensics, and for enabling identity-based next-generation firewall, Web content, security information and event management (SIEM), and bandwidth management policies.

The Juniper-Impulse Solution

Working with Juniper Networks switches and next-generation firewalls, Impulse SafeConnect network access control (NAC) offers a highly simplified and scalable approach to creating a secure networking environment while delivering a superior user experience for managed, BYOD, and guest devices. The Juniper and Impulse SafeConnect integrated solution utilizes key advantages of both architectures: SafeConnect's device-centric network access management approach, coupled with the ability to apply Layer 2/Layer 3 access control policies with Juniper Networks® EX Series Ethernet Switches and third-party wireless partners, provides an end-to-end secure, flexible IT infrastructure.

SafeConnect delivers a consistent multivendor network experience for all client and IoT devices, whether they are wireless, wired, or VPN-connected. It enables automated 802.1X-WPA2 enterprise (wireless data encryption) provisioning and security compliance enforcement before and after admitting devices to the network. Noncompliant devices can be quarantined immediately and offered remediation guidance. Features like agentless device profiling, end-user authentication, real-time device security assessment, and context-aware visibility and reporting enable a superior level of network security. At the same time, the user experience, installation, and ongoing solution management are greatly simplified by an industry exclusive, cloud-managed service.

Juniper Networks, working in concert with Impulse SafeConnect Network Access Management, offers multi-layer security policy enforcement and control at the access and aggregation layers, core, and perimeter, implemented via EX Series and QFX Series switches, MX Series routers, and SRX Series Services Gateways. This multi-layer approach mitigates risk and non-compliance issues while increasing the security profile of the network. Using standard protocols such as 802.1X, Radius, SNMP, and DHCP, Juniper devices share end point information with SafeConnect and enforce policies and enforcement actions based on end-point posture and authentication status provided by SafeConnect.

The SafeConnect Network Access Management offering is certified with EX Series Ethernet Switches and next-generation SRX Series Services Gateways, delivering a unique industry value proposition that addresses the cost, resource burden, and business risk associated with deploying and supporting a secure enterprise network.

Solution Components

Juniper Networks EX Series Ethernet Switches and SRX Series Services Gateways integrate with Impulse's SafeConnect to deliver the industry's most scalable and easiest to deploy network access management solution.

EX Series Ethernet Switches are designed to meet the demands of high-performance businesses, helping companies grow their networks at their own pace while minimizing up-front investments. Based on open standards, the EX Series switches deliver carrier-class reliability, security risk management, virtualization, application control, and lower total cost of ownership (TCO).

SRX Series Services Gateways are next-generation intelligent security devices that deliver outstanding protection, market-leading performance, six nines reliability and availability, scalability, and services integration. Ideally suited for service provider, large enterprise, and public sector networks, these platforms deliver the highest level of L3-7 protection. They also feature a carrier-grade, next-generation firewall with advanced security services such as application security, Unified Threat Management (UTM), Intrusion Prevention System (IPS), and integrated threat intelligence services.

Impulse SafeConnect delivers a range of capabilities that provide a comprehensive enterprise-wide network access management solution to address the flexibility and security needed to support today's wired, wireless, and VPN environments.

Features and Benefits

Wired and Wireless Support

- SafeConnect's network access control (NAC) architecture leverages RADIUS-Based Enforcement (RBE) Layer 2 access control technology in conjunction with EX Series switches.
- RBE delivers dramatic scalability and granular network access control for 802.1X-WPA2 enterprise/open wireless networks, and EX Series Layer 2 switches are based on contextual intelligence-driven policies.
- SafeConnect can also leverage device access control through EX Series Layer 3 switches, offering the simplest device enforcement alternative based on its Layer 2 independent design, and can be rapidly deployed in support of wireless, wired, and VPN networks.

Remote VPN Support

- SafeConnect delivers consistent identity and device type recognition, security assessment, enforcement, and remediation for SRX Series next-generation firewalls and their remote VPN client feature, in addition to an organization's internal wired and wireless networks.
- Juniper EX Series and QFX Series switches, MX Series routers, and SRX Series firewalls work with Impulse SafeConnect Network Access Management to offer multi-layer security policy enforcement and control at the access, aggregation, core, and perimeter. This multi-layer approach mitigates risk and non-compliance issues, increasing the security profile of the network.

How it Works

Once a new client or IoT device connects to a Juniper Networks switch or wireless access point, it is initially placed in quarantine mode and assessed immediately for policy compliance by Impulse SafeConnect. After examining the device's compliance level based on context-driven policy (identity/role, device type, location, ownership, and security posture), SafeConnect returns a specific RADIUS-based attribute to the wired switch, wireless controller, or wireless access point that authorizes network privileges for the client or IoT device as follows:

- **Full policy-based access** to the trusted network (devices can be granted different access privileges).
- **Limited access rights**, as defined for different user roles (e.g., guests, contractors, and personal devices). Guests and other unknown users will be redirected to a self-registration webpage to receive their access credentials. Each of these user roles can be supported with different policies and associated network privileges. Access rights for each user role can be defined by identity, device type, network location, ownership, access duration, and security policy compliance.
- **Quarantine**, where it is blocked from the trusted network. To reduce help desk calls, user devices are guided through self-remediation options:
  - Windows and Mac OS X devices may be redirected to a remediation webpage with the option to address AUP compliance (e.g., AV software, OS patch policy, encryption software), or provided direction to cease the use of noncompliant applications like P2P, Skype, gaming, etc.
  - Mobile devices may be redirected to install the organization's designated Mobile Device Management (MDM) software. They may also remain in a quarantined state if the device does not fulfill other compliance criteria, like being jail broken, having password or data encryption protection.

Once devices are authorized, they will be assigned applicable network access privileges and monitored continuously in real time to ensure ongoing compliance.

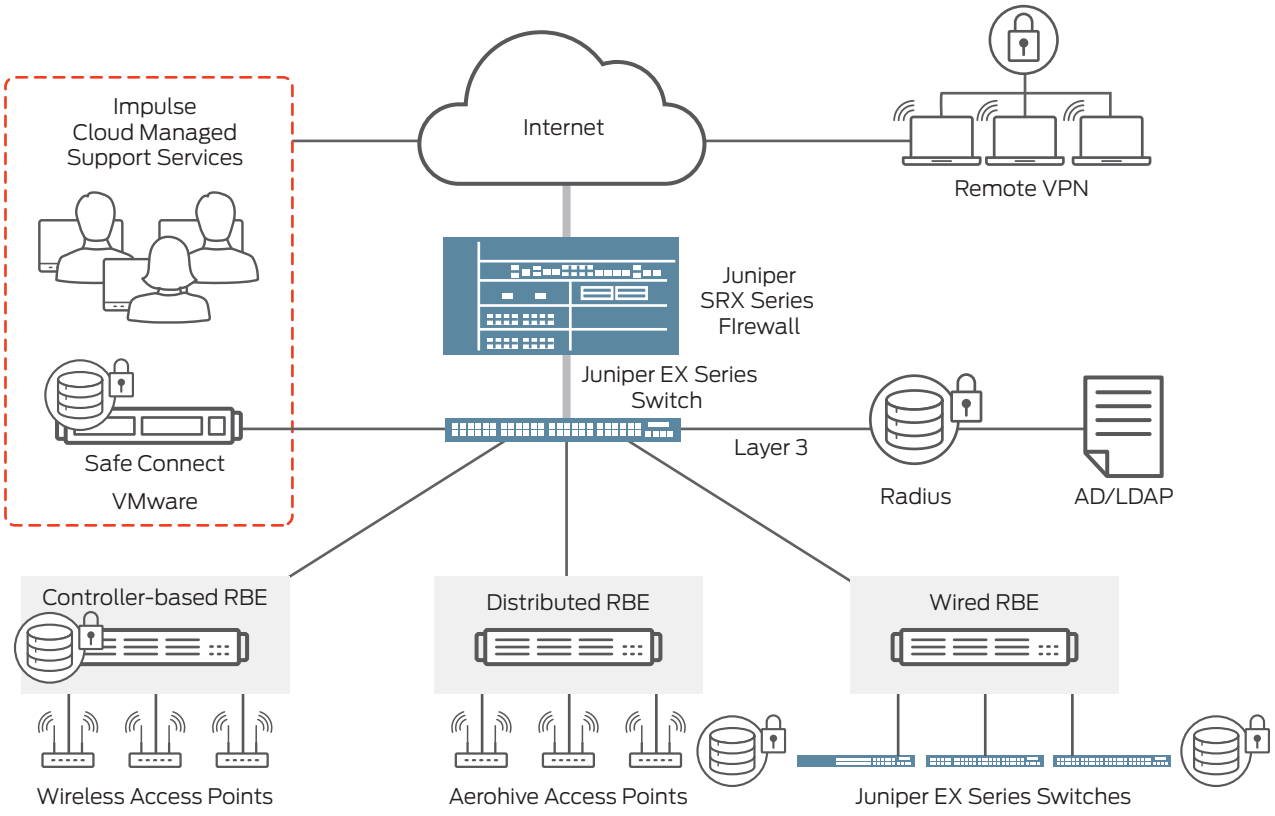

Figure 1: Working in conjunction with EX Series switches, SafeConnect's architecture utilizes L2 RBE or L3 technology to offer the industry's broadest range of device enforcement alternatives.

Employee 802.1X Authentication

The Juniper Networks and Impulse SafeConnect solution offers a uniform wired and wireless experience for employees with company managed devices:

- Devices are automatically configured for 802.1X using SafeConnect Secure BYOD Onboarding.
- They can be onboarded using machine authentication, user authentication, or device certificates.
- Backend authentication is supported with Active Directory/ LDAP.
- Devices can be placed in different VLANs or restricted using firewall filters based on device role.

MAC Authentication Bypass

- Devices like printers and IP phones can use MAC RADIUS to bypass 802.1X authentication.
- SafeConnect can look for known media access control (MAC) addresses and place them in an appropriate VLAN or restrict them.
- If the device is unknown, SafeConnect can send a reject notice or place that device in a restricted VLAN.

Guest Access or BYOD

- All personally owned devices get a consistent wired and wireless experience.
- Users can be redirected to a webpage to provide instructions on how to authenticate/register.
- Users need to agree to an acceptable use policy (AUP) to get a restricted guest access.
- Guest users can login using pre-allocated guest access credentials or can easily self-enroll.
- Employees with noncorporate devices can be required to register their devices and autoconfigure their endpoints for 802.1X using SafeConnect Secure BYOD Onboarding.
- Employee devices can be continuously checked to ensure security policy compliance (i.e., antivirus software is running, data encryption installed, etc.).

Device Type Profiling

- Identifies the type of device connected (e.g., printer, IP phone, Windows, iOS, etc.)
- Network access assignment based on the user identity/role, device type, location, ownership, and security compliance status

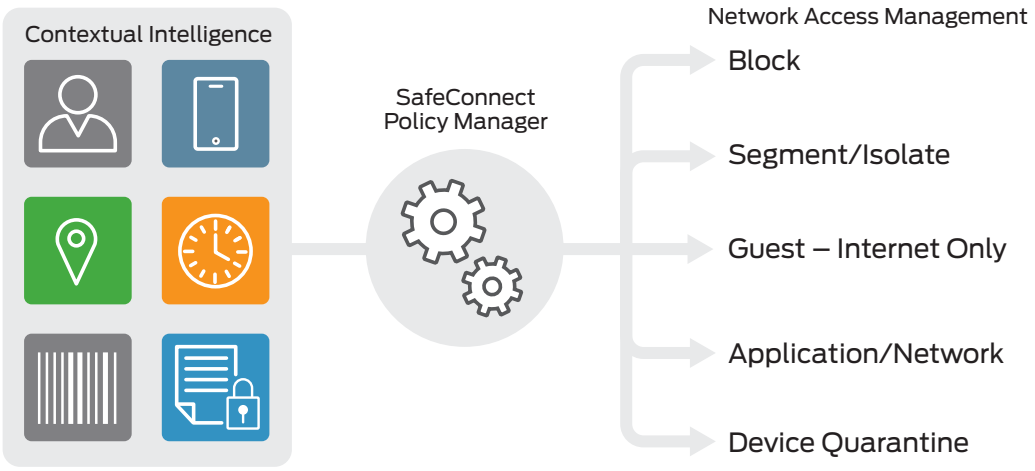

Figure 2: SafeConnect's L2 RBE device enforcement technology assigns network access privileges based on context-aware attributes (identity, device type, location, time, ownership, and security status).

- Eliminates the need for enterprises to manually maintain a list of known device MAC addresses and device type mapping
- Mitigates threats from malicious endpoints that spoof MAC addresses (note: MAC address is not used for device profiling)
- Enables the ability to dynamically provision ports based on type of connected device

Real-Time Network Security Orchestration for SRX Series Services Gateways

- Supports all active directory managed, BYOD, guest, and non-browser-based IoT network devices
- Assigns firewall application access, Web content, and bandwidth policies per device based on contextual, intelligence published attributes (identity/user group, device type, location, or ownership)
- Assigns aggregate data consumption policies per user, including one user with multiple devices
- Provides single sign-on (SSO) for Active Directory Domain Services and RADIUS (802.1X) user environments
- Delivers authentication persistence for devices with no multiple login portal prompts
- Real-time device enforcement and end-user messaging based on SRX Series next-generation firewall threat detection alerts

Cloud-Managed Support Services

In addition to its simplified architecture and enhanced user experience design, a key benefit of this solution is the way it is delivered and supported. SafeConnect solutions are premise-based, but come with a service that keeps the system updated regarding the latest devices, operating systems, and antivirus packages. SafeConnect's Cloud-Managed Support Service includes the following:

- Remote installation, training, and deployment assistance
- 24x7 proactive system monitoring
- Problem determination and resolution ownership
- Daily device type, security updates, and policy configuration data remote backups
- Installation of all maintenance updates and application version upgrades

Summary

Providing high-performance, enterprise-grade networking and security in today's mobile world is key to ensuring productivity for all users, regardless of whether their devices are corporate-issued, personal (BYOD), or IoT. Juniper Networks and Impulse have teamed together to offer a unique and certified industry solution to address the challenges of managing disparate devices in a highly simplified manner that minimizes the technical resources required for deployment and support.

Next Steps

Contact your Juniper or Impulse representative for more information. To request a demo, please visit www.impulse.com/product_demo or contact juniper@impulse.com for technical or sales assistance.

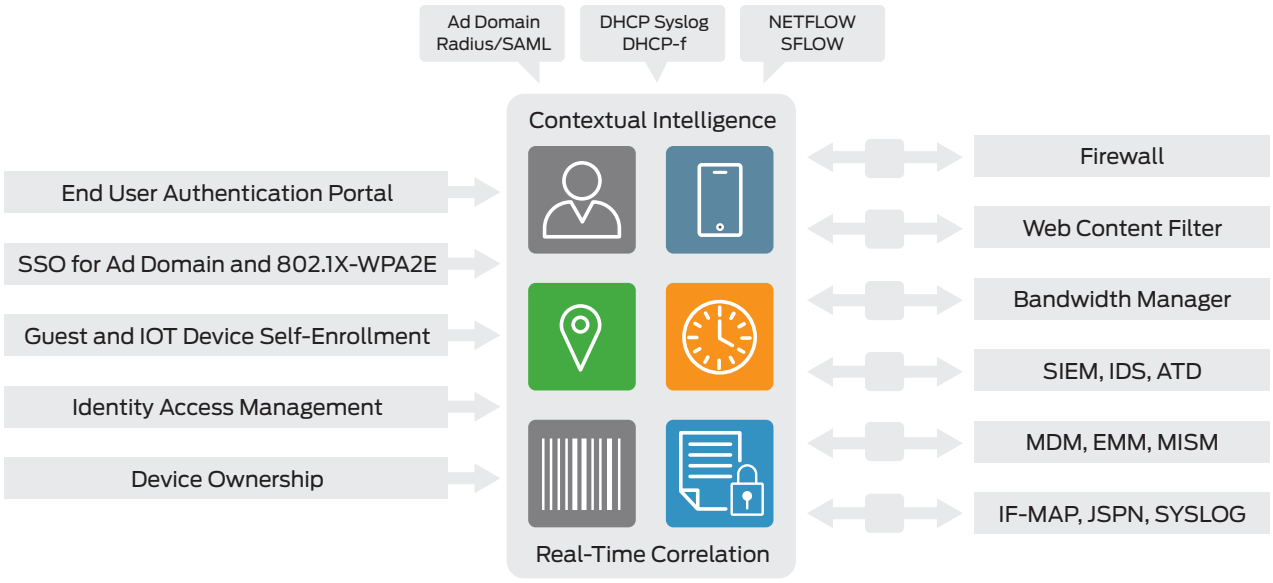

Figure 3: SafeConnect provides real-time contextual intelligence to third-party management and security systems to enable granular identity-based policy assignment, single sign-on, one-time user authentication, and enhanced analytics.

About Impulse

Impulse is the leading provider of Contextual Intelligence and Network Security Orchestration in support of BYOD and IoT enabled enterprises. Impulse securely and efficiently automates BYOD by combining our real-time, context-aware and simplified access control architecture, remote cloud-managed support services, and customer-centric business philosophy to enable customer freedom. Our customers know this as the Impulse Experience. The security of more than six million endpoints is entrusted to Impulse. Visit www.Impulse.com.

About Juniper Networks

Juniper Networks challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks with agility, performance and value. Additional information can be found at Juniper Networks or connect with Juniper on Twitter and Facebook.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
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

3510593-001-EN Sept 2016