JUNIPER NETWORKS | Engineering Simplicity

White Paper

THE RISE OF ZERO TRUST

Separating the Reality from the Myths

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Companies are under intense and growing pressure to demonstrate that they're taking proper steps to protect the enterprise from cyber attacks and prevent the compromise of sensitive data. Currently, the most popular—and perhaps most viable—approach to securing the enterprise is the concept of Zero Trust. As an IT or security leader, executive or engineer, it's imperative that you understand why Zero Trust is an essential part of creating a defensible security strategy.

In this white paper, we'll separate the reality of the Zero Trust security architecture from the time-worn myths and misconceptions while demonstrating how Juniper Connected Security not only supports and enables a Zero Trust network architecture, but helps you implement it more quickly and easily.

Introduction: A Model for More Effective Security

As the Zero Trust concept gains momentum, it's upending the way we approach security in general and network architecture in particular. And it's about time; the prevailing assumption that we should inherently trust internal users, networks, and systems is simply no longer valid, as proven by an endless stream of successful data breaches.

While the advantages of a Zero Trust approach are clear and compelling, questions and challenges abound for network and security professionals tasked with implementing the architecture. Will they have to replace the entire network infrastructure? Is microsegmentation a realistic goal? Does the cloud preclude the possibility of a Zero Trust architecture?

In this paper, we'll separate today's reality from the time-worn myths about the Zero Trust security architecture. At the same time, we'll show you how Juniper Connected Security not only supports and enables a Zero Trust network architecture but can help you implement it more quickly and easily.

Wanted: A Better Way to Protect Modern Environments

That was then: Remember when endpoints were owned, managed, and secured by the enterprise? We could assume that any user or device within the perimeter could be trusted. Corporate applications were operated within a secure data center and they could trust each other.

This is now: Today, the network perimeter has evolved as workloads have moved to the cloud while non-managed, mobile devices have become the norm rather than the exception. The location of applications, users, and their devices are no longer static. Data is no longer confined to the corporate data center. Gaps in visibility and protection continue to widen as the attack surface evolves, forcing companies to bolt on multiple, disconnected tools in order to see and secure everything.

Meanwhile, cyber criminals are becoming increasingly adept at circumventing advanced security measures, with more attackers using lateral movement to reach targets for compromise. They're enjoying access to increasingly sophisticated toolkits and explicit explanations describing how to exploit vulnerabilities. And the number of these vulnerabilities continues to grow; in 2018, the National Vulnerability Database published 14,760 known security vulnerabilities—more than twice the number reported in 2016.

The bottom line: Building stronger perimeters is no longer an adequate approach to protecting networks, users, applications, and data.

The Beginnings of Zero Trust

In 2009, Forrester Research introduced the new Zero Trust information security model, which has gained widespread acceptance and adoption. By adopting the concepts and architectural components of Zero Trust, organizations can become more secure while easing compliance burdens and ultimately reducing costs.

Source: "No More Chewy Centers: The Zero Trust Model of Information Security," Forrester research, Inc., March 2016

A New Security Paradigm

Enter Zero Trust, the modern security paradigm that's being widely adopted to provide greater protection against today's threat landscape. The guiding principle for Zero Trust is "never trust; always verify"—in other words, assume that every part of your network is potentially hostile, as if it were directly on the Internet, and treat access requests accordingly.

The Zero Trust approach considers inherent trust a critical vulnerability. Assuming that everything inside an organization's network can be trusted allows threat actors and malicious insiders misusing privileged credentials to move laterally with ease, accessing or exfiltrating data from their target(s).

Instead, by using controls to create microperimeters around critical data, applications, and services, you can make sure that only known, allowed traffic and applications have access to the assets you're protecting. With a Zero Trust architecture, you determine who can transit a microperimeter and set controls close to the assets you are protecting, preventing unauthorized access and exfiltration of sensitive data.

The Growing Importance of Zero Trust

Organizations identified by a recent Forbes Insights survey as "cybersecurity trailblazers" consider initiatives such as Zero Trust as "extremely important" to their security strategies.

Source: "Cybersecurity Trailblazers Make Security Intrinsic to Their Business," Forbes Insights, 2019

While this approach doesn't protect organizations from every possible attack, it can:

- Reduce the risk of advanced threats and breaches by preventing unauthorized lateral movement and access
- Accelerate threat detection and response
- Reduce gaps in visibility
- Support compliance requirements such as HIPAA, PCI-DSS, FISMA, and others

A Look at the Pillars of Zero Trust

In the years since the Zero Trust concept was introduced, industry experts and observers such as Forrester analysts have weighed in on this security approach. Forrester calls its latest iteration the Zero Trust eXtended (ZTX) Ecosystem[1].

At its simplest, Zero Trust is a conceptual and architectural model for "how security teams should redesign networks into secure microperimeters, strengthen data security using obfuscation techniques, limit the risks associated with excessive user privileges and access, and dramatically improve security detection and response with analytics and automation."

Taking a complete approach that includes processes and technology, the ZTX Ecosystem encompasses data, workloads, networks, devices, people, visibility and analytics, and automation and orchestration, as illustrated in Figure 1.

Increasingly, companies are embracing the Zero Trust approach; 60 percent of global enterprises are currently working on Zero Trust strategies, meaning they are either formalizing or actively working on executing the plan.[2] These companies have already recognized that the misconceptions that stymied Zero Trust efforts in the past are not reflective of today's reality. Let's look at some of those myths and misconceptions in more detail.

In Support of Zero Trust

"Zero Trust can provide a mature solution today that does not need to add operational complexity or require major architecture changes. In fact, it can simplify operations while increasing security and protecting critical, high value assets."

Source: "Zero Trust Cybersecurity Current Trends," American Council for Technology-Industry Advisory Council (ACT-IAC), April 2019

[1]"The Zero Trust eXtended (ZTX) Ecosystem; Strategic Plan: The Zero Trust Security Playbook," Forrester Research, Inc., July 2019
[2]"The Digital Enterprise Report: How the World's Largest Organizations Are Evolving with Technology," Okta, 2019

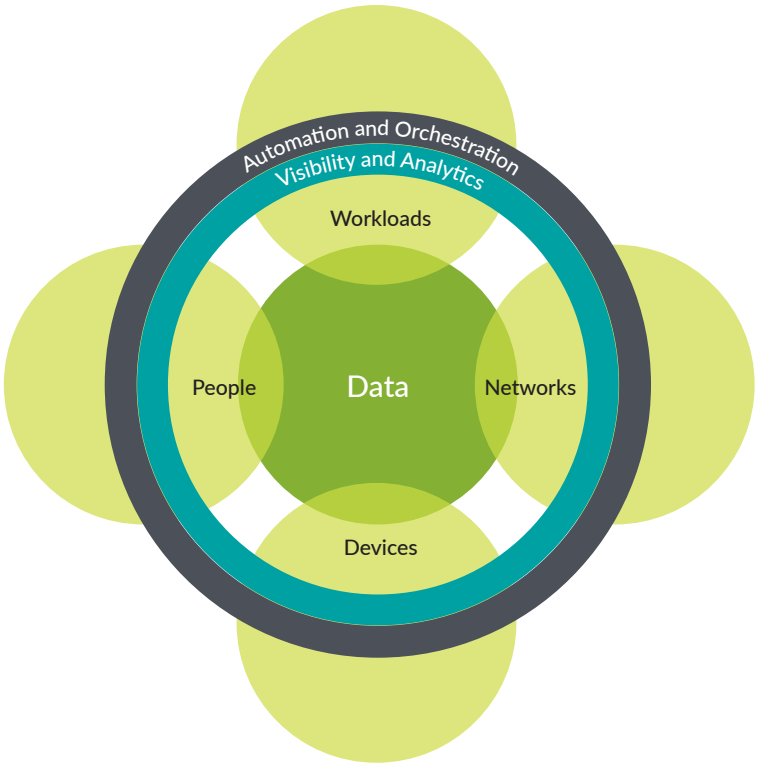

Figure 1: The Zero Trust eXtended (ZTX) Ecosystem, Forrester Research, Inc.

Myth #1: Moving to Zero Trust Is Too Expensive for Most Companies

Many organizations mistakenly assume that implementing a Zero Trust model will be cost-prohibitive for all but the very largest of enterprises. Considering that some of the most well-known examples of Zero Trust in practice include the likes of Google and Coca-Cola, it's understandable that companies without deep pockets might be wary of the cost.

However, the reality is that Zero Trust is appropriate and affordable for just about any sized company, from small startups to global corporations. Here's why:

1. It's a journey, not a project. While companies with bottomless coffers and big targets on their backs may be able to justify starting from scratch with a Zero Trust architecture, the vast majority of organizations would be better served taking a more pragmatic, step-by-step approach. An iterative approach means that companies don't need to invest considerable resources and budget up front; rather, they can spread those costs and efforts over a long period of time.
2. Implementing Zero Trust can reduce security costs because it improves operational efficiency and reduces complexity. According to Forrester, "… Zero Trust also reduces expenditures by centralizing security management."[3]

Juniper Connected Security can help you take a step-by-step approach to implementing a Zero Trust architecture, bolstering the security you already have in place while helping you increase visibility and awareness without suffering from "alert overload." For example, Juniper's five-step framework to a more secure network can help you determine where your company is now on its security journey and where it needs to go (see Figure 2).

[3]"The Eight Business and Security Benefits of Zero Trust," Forrester Research, September 2019

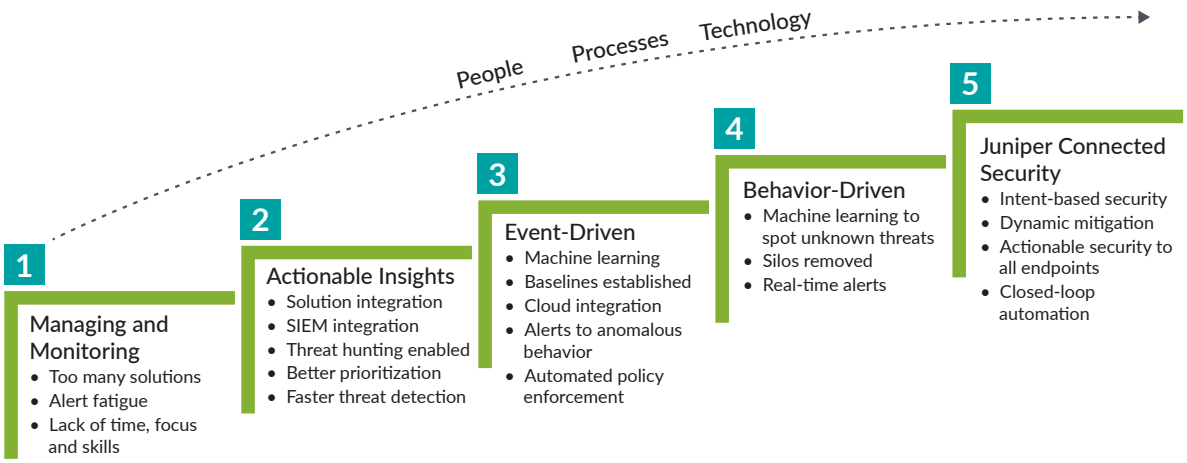

Figure 2: Five-step framework to Juniper Connected Security

Myth #2: Implementing Microsegmentation Is Too Complex to be Realistic

Microsegmentation is a potent tool for securing networks with Zero Trust in mind, breaking down monolithic perimeters into a series of microperimeters that concentrate granular security controls and contain attacks (see Figure 3). So why don't more security and network professionals insist on using this approach?

Early on, microsegmentation was perceived as far too time-consuming and complex to be practical for existing applications and environments. Organizations believed that implementing and maintaining microperimeters simply wasn't feasible, given the large number of applications, application dependencies, services, and users involved. This was potentially true for organizations with disparate security and networking products that did not work together and were subsequently unable to provide end-to-end visibility for the network and environment.

However, technology that embraces Zero Trust and delivers robust support for the architectural components of a Zero Trust network reduces the cost and complexity of creating and maintaining microperimeters. It does this by integrating security functions into devices that can be managed and controlled with centralized security policies.

For example, Juniper Connected Security delivers the full functionality necessary to support the key components of a Zero Trust architecture that enable microperimeters:

- **A network segmentation gateway**: Serving as the nucleus of the network, the segmentation gateway integrates traditionally standalone security services and devices into one gateway. Juniper Connected Security provides segmentation gateway functionality that combines next-generation firewall, unified threat management (UTM) services, and full, standards-based IPsec encryption with routing and switching in a single, high-performance, cost-effective platform.
- **Parallel, secure microperimeters**: A switching zone mapped to a high-speed interface creates a secure segment, called a microcore and perimeter (MCAP) by Forrester. MCAPs are multiple, parallel microperimeters that are aggregated into a unified segmentation gateway fabric. Juniper Connected Security delivers microcore segmentation of the network based on defined security attributes and provides visibility into network activity on an application and per-user or role basis for strict access control over each MCAP. Taking this a step further, Juniper extends security to every layer of the network, including switches, routers, and Wi-Fi access points, preventing threats from spreading across the entire network, including both Juniper and third-party switches.
- **Centralized management**: For efficient, scalable, and easy-to-use management, Juniper Connected Security allows IT teams to transparently manage all MCAPs from a single system serving as the network backplane. Security teams can manage a set of holistic policies that maintain the security of each MCAP, regardless of location, reducing the number of policies and rules needed while supporting finer granularity for single segmentation gateway instances.

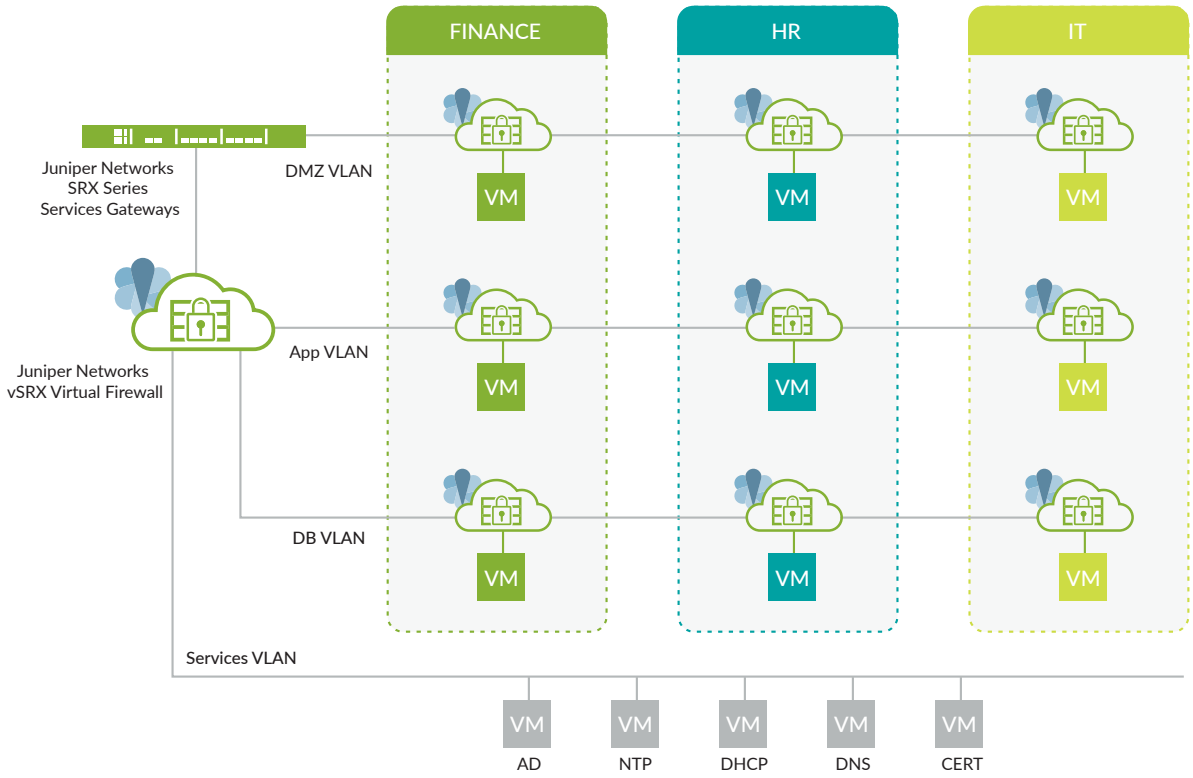

Figure 3: Data center microsegmentation example

Myth #3: It's Only Feasible for Greenfield Implementations

Another broadly disseminated assumption is that Zero Trust is fine only if you have a greenfield implementation. Otherwise, you really need to rip and replace everything and start over with a single platform.

While it's true that some companies are doing this, most organizations are not in a position to take a rip-and-replace approach to Zero Trust. Fortunately, they don't need to—on the contrary, achieving a Zero Trust architecture does not require rebuilding the entire network, and certainly not in one massive effort.

Instead, organizations can develop a roadmap to Zero Trust featuring a step-by-step implementation, increasing their maturity over time. The key to successfully achieving an incremental approach is choosing solutions that can easily support and integrate with what your organization already has, so you can implement new security capabilities to support Zero Trust and extend security across the entire network at the same time.

Rather than try to be all things to all companies, Juniper focuses on open standards and product interoperability. No single vendor can secure a modern enterprise network; Juniper Connected Security provides a consolidated view across security solutions, making it easy to leverage security intelligence, improve detection, and mitigate threats without adding unnecessary complexity.

Myth #4: Zero Trust Is Only for On-Premises Environments

Given that the primary argument for Zero Trust is that organizations can no longer assume trust for everything within their corporate networks, a common myth is that Zero Trust is only applicable within a company's own data centers. While it's true that cyber criminals have exploited the assumption of trust within the corporate environment, their efforts and techniques are not limited to on-premises environments.

Another reason that organizations think implementing Zero Trust applies mainly—or exclusively—to corporate data centers is they tend to believe that the cloud service provider is responsible for security. This is one of the biggest fallacies of cloud computing. In fact, the pervasive model for security in the cloud is the shared responsibility model, where the cloud service provider is responsible for securing the cloud infrastructure and customers are responsible for securing their workloads, data, and users. Not only is Zero Trust applicable to the cloud, but it's critical for extending protection of a company's assets to cloud and multicloud environments.

Juniper Connected Security extends security policy and enforcement into the cloud to support new service delivery models, protecting workloads and data from the endpoint to the edge and every cloud in between. This enables your organization to take your security posture from on-premises to the cloud. With Juniper, you can extend Zero Trust security to containerized workloads as well, extending visibility and enforcement down to the communication between individual microservices within an application.

Myth #5: Zero Trust Requires a Single-Vendor Approach

As the security industry hops on the Zero Trust bandwagon, a good deal of the vendor hype has focused on the need for a single-vendor solution. The argument has been that the only way companies can make sure everything works together in a Zero Trust architecture is to choose one vendor that offers everything needed.

The reality is that no one vendor will ever offer everything required for secure networking within a Zero Trust architecture. Forrester reports that integration of functionality from different security domains is critical, stating that "Usability and command and control of assets across disparate data systems, networks, and infrastructure are critical in Zero Trust."

That's why Juniper Connected Security built a global partner ecosystem dedicated to delivering and implementing networks that drive real business value at all levels of our customers' organizations. These partnerships leverage best-in-class solutions and industry expertise that complement Juniper's own offerings and solve a broader range of customer needs.

Get Started with Zero Trust and Juniper Connected Security

Now that we've separated fact from fiction on Zero Trust architectures, let's look at what uniquely positions Juniper Connected Security to help your organization deploy Zero Trust in the most advantageous way possible.

First and foremost is our leadership in secure, high-performance networks. We help customers build the most advanced networks around the globe, powering the world's largest networks, including 97 of the Fortune Global 100, the world's top five social media properties, and more than 86 percent of U.S. smartphone traffic.

Fueled by a significant investment in research and development, Juniper Networks produces some of the industry's most groundbreaking innovations across every aspect of networking technology: silicon, systems, software, and security. Juniper brings next-generation firewalls, switching, advanced malware defense, intelligent policy, and flexible deployment models together with Juniper Connected Security, effectively positioning Juniper to truly address the Zero Trust needs of organizations around the globe (see Figure 4).

[4]"The Zero Trust eXtended (ZTX) Ecosystem; Strategic Plan: The Zero Trust Security Playbook," Forrester Research, Inc., July 2019

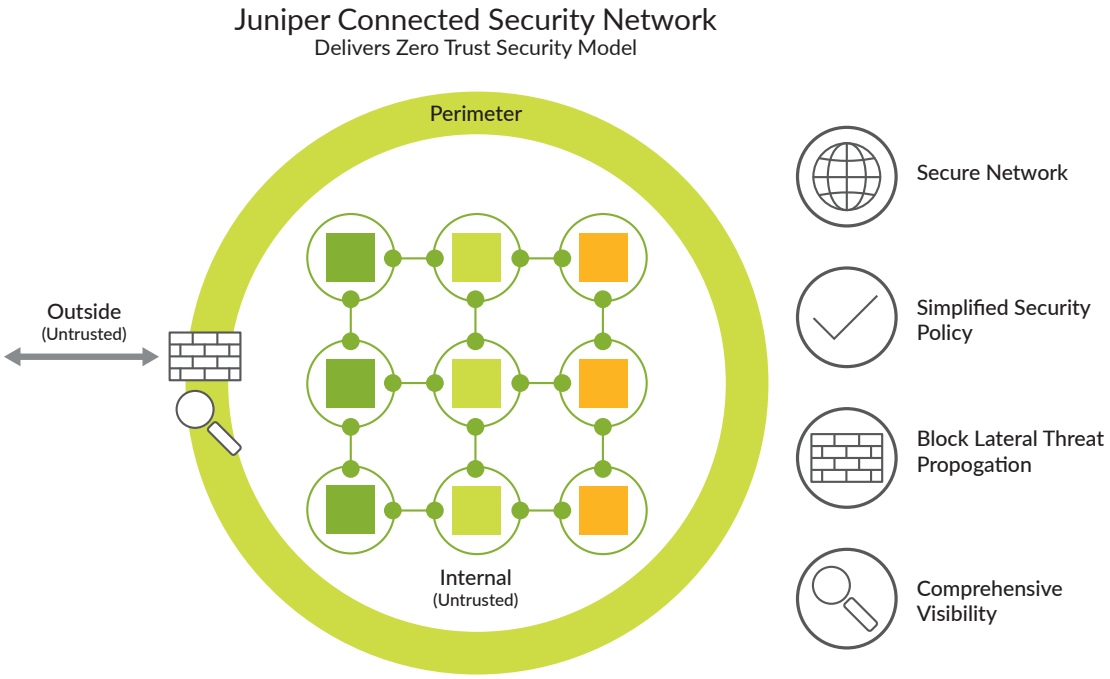

Figure 4. A Zero Trust architecture with Juniper Connected Security

Table 1. Juniper Connected Security Helps Support Each Pillar of the Zero Trust Model

Pillar	Juniper Capabilities
Data	• Provides full, standards-based IPsec encryption for the secure transport of business data across networks • Supports microperimeterization
Networks	• Enables you to see, protect, and automate the network as a single entity • Extends security to all points of the network, including third-party products • Supports microsegmentation with robust segmentation gateway capabilities
Users	• Enables you to govern and enforce user access with a high degree of granular control • Secures and protects user interactions
Devices	• Supports user intent-based policies to allow network devices (switches, routers, firewalls, and other security devices) to share information, resources, and, when threats are detected, remediation actions within the network
Workloads	• Offers advanced defenses deep behind the perimeter, in the public cloud, and anywhere else that modern service delivery models take an organization's workloads • Enables granular policy control
Analytics and Visibility	• Delivers visibility into network traffic, including user and application awareness • Analyzes session information in real time, sending packet captures through a span port to a centralized repository
Automation and Orchestration	• Delivers unified protection powered by automation, machine learning, and real-time threat intelligence • Simplifies management with a platform for creation, deployment, and replication of common security policies to ease the implementation of new applications and services

Conclusion

Given today's threat landscape and modern computing environment, it's time for companies and organizations of all sizes to make Zero Trust a core tenet of their information security strategy. To continue to rely on strengthening perimeter security only is to invite increasingly more successful and frequent cyber attacks on both corporate and cloud environments.

Learn more about the power of Juniper Connected Security at www.juniper.net/us/en/solutions/security/.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions, and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable, and secure networks to move at the speed of business.

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

JUNIPER NETWORKS | Engineering Simplicity