Learn About Network Security Management

This *Learn About* investigates the issues and concerns that network security engineers have with securing their networks. It then suggests several solutions offered by Juniper Networks for easing these network security management concerns and details the technology behind those solutions.

Security Management Challenges

Security teams must support internal and external compliance mandates, enable new services, optimize performance, ensure availability, and support the ability to troubleshoot efficiently on demand – all with no room for error. That's a lot to balance when managing network security.

In addition, an ever expanding matrix of users, devices, locations, and applications makes it difficult for IT staff to ensure that access controls and other security mechanisms are consistently applied to the same user without fail. And mobile workers need *anytime*, *anywhere* access to a broad array of applications, further taxing the security infrastructure.

This exponential growth in network traffic, combined with changes in mobile user behavior and an onslaught of new cloud services and applications, means the avenues available to malicious network attackers are expanding.

The rapid evolution of the threat landscape, in addition to changes in network and security architectures, makes network security management far more challenging and complex than it was just a few years ago. Managing security policy in these complex environments can be prone to error and overly time-consuming, especially if the management solutions employed are slow, unintuitive, or restricted in their level of granularity and control. Poor policy management can also lead to security misconfiguration, making the network vulnerable to sophisticated threats and regulatory noncompliance.

In order to successfully confront these challenges, network administrators will need to learn how to consistently deploy thousands of security policies across their network. To assist them in this task, they will need a new set of tools and technologies that can provide:

- More visibility into network security policies.
- A platform that will enable them to troubleshoot policy issues quickly and efficiently.
- The capacity to do more, with less resources.
- The option to deploy thousands of devices and VPNs in less time.

How to Overcome These Network Security Management Challenges

Security practitioners can no longer resort to CLI or device-level tools to implement next-generation firewall/perimeter security or manage policies. They need consolidated, easy-to-use interfaces that can help them implement security across the entire network. Usability is extremely important; it has become one of the key criteria in deciding between network security equipment vendors.

Data centers are undergoing a dramatic transformation. As Nemertes Research has noted, "workloads in today's data center move dynamically and start and stop based on real-time performance needs." See https://www.nemertes.com/reports/securing-physical-virtual-cloud-continuum. Unfortunately, in many enterprises, the current security architecture looks much the same as it did 15 years ago.

To keep pace with changes, these networks need new security and compliance controls that span physical and virtual environments and dynamically enforce policy regardless of application type or user location. In evaluating next-generation security solutions, administrators must look for the following capabilities, as shown in Figure 1. This applies to all data centers regardless of their size.

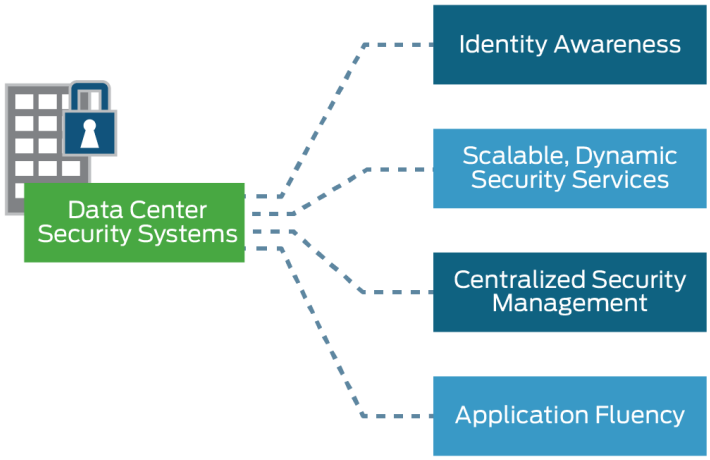


Figure 1 *Security Systems for Data Center Networks*

Network administrators must configure security policies on numerous platforms, both physical and virtual, sift through a flood of logged events to determine which ones require attention, and compile data to demonstrate compliance with government and industry-specific mandates. Today, network administrators must monitor multiple individual management consoles and create and maintain policy scripts for each different security platform – a manual and error-prone process that makes it difficult to apply policy consistently across the network. Similarly, each security system typically generates its own logs, creating silos of event data. Many solutions handle traffic flows and security events separately, which makes it virtually impossible to spot networkwide threats and anomalies.

Given the complexity of today's networks and the rapid evolution of threats from multiple sources, administrators need security management solutions that can:

- Automate security device and service provisioning.
- Abstract and centralize policy definition.
- Provide policy life cycle management.
- Deliver a unified solution for managing traffic flow and security events.
- Provide a single management interface for both physical and virtual systems.
- Correlate data from diverse sources on the network.

Evolving Security Management Solutions

With so many disparate vendor devices and hosts, security teams need a normalized, comprehensive view of their network, including routing rules, access rules, Network Address Translation (NAT), VPN, and more; hosts, including all products (and versions), services, vulnerabilities, and patches; and assets, including asset groupings and classifications. Although administrators need a holistic view of their network in order to see how all the pieces fit together, they must also be able to easily access the information on rules, access policies, and configuration compliance for a particular device.

This information must be provided in a simple, clear, and understandable format. The network components that impact the device come from various vendors, creating data of different vendor languages that must be deciphered, correlated, and optimized to allow administrators to streamline rule sets. For example, network administrators need to be able to block or limit access by application and to view violations of these access policies. Beyond accessing a specific device, network administrators must also be able to drill down to each device level, accessing information on users, applications, vulnerabilities, and more. This provides administrators with a broader network view and enables them to focus on particular devices for management.

Junos Space Security Director Solutions

Juniper Networks Junos Space Security Director is an application that runs on the innovative, intuitive, and intelligent Junos Space Network Management Platform, providing detailed visibility into application and user performances, and reducing risk while enabling users to move quickly from knowing something is wrong, to doing something to fix the problem.

With Security Director, network administrators can provision identity-based and role-based policies across the entire network. It uses an innovative approach that abstracts the network security policy and then applies it to a group – effectively protecting an entire security domain. Security Director has an easy-to-use wizard-driven interface, granular configuration options, and predefined profiles for rapidly deploying devices and security services. Using Security Director, administrators can easily provision complex identity-based policies across their entire network, greatly improving its operational scale and efficiency, and enhancing overall policy consistency and security because of minimal operator error.

As shown in Figure 2, Security Director provides solutions to these problems by:

- Enabling efficient policy management for multiple security devices.
- Providing highly scalable device management to keep up with business growth.
- Allowing comprehensive security policy management for granular protection, including firewall, application security, VPN, and NAT, from a single location.

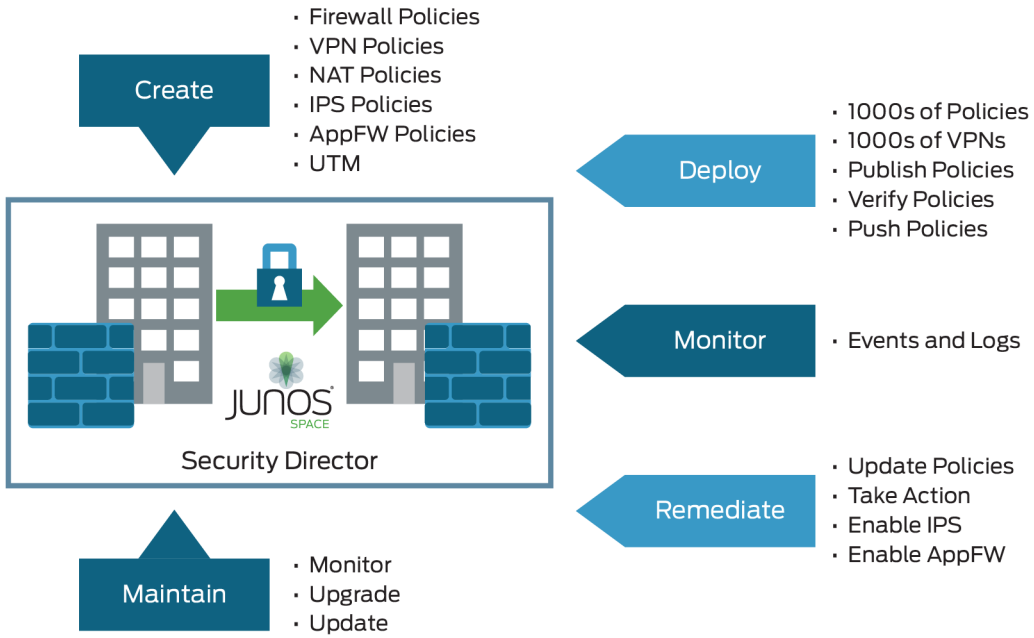


Figure 2 *Junos Space Security Director Components*

Efficient Security Policy Management

Security Director provides efficient security policy management supporting highly scalable policy implementation based on support for the Junos Space Network Management Platform. This efficient security policy management can be achieved by enabling and easing policy management (implementation and validation) across multiple devices, and reducing the chances of errors and misconfigurations in policy enforcement.

A single policy can be applied to multiple Juniper Networks SRX Series devices; you can apply a complex policy with thousands of rules to one or more SRX Series devices, and then scale the number of rules as required.

Highly Scalable Device Management

Security Director supports the management of thousands of devices running Junos OS. It can instantly scale to many devices by simply adding or deleting nodes on the fabric. In addition to managing many devices, Security Director can also increase the number of concurrent administrators.

Comprehensive Security Policy Management

In addition to enabling highly scalable device management, Security Director also enables companies to configure multiple security functions from a single location. Security Director can rapidly manage a comprehensive set of functions, including firewall, VPN, NAT, intrusion prevention system (IPS), and application firewall, from a single management console. It eases policy configuration by providing read-write APIs for firewall policy, objects, and VPNs. A comprehensive and intuitive Google-like search mechanism is built into the main UI, which enables network administrators to quickly locate policy terms or issues, even in the rules, for faster maintenance.

Security Director Dashboard and Web GUI

The Web-based user interface for Security Director includes a dashboard that provides customizable, information-rich widgets offering visually intuitive displays that report security device status at a glance, as shown in Figure 3.

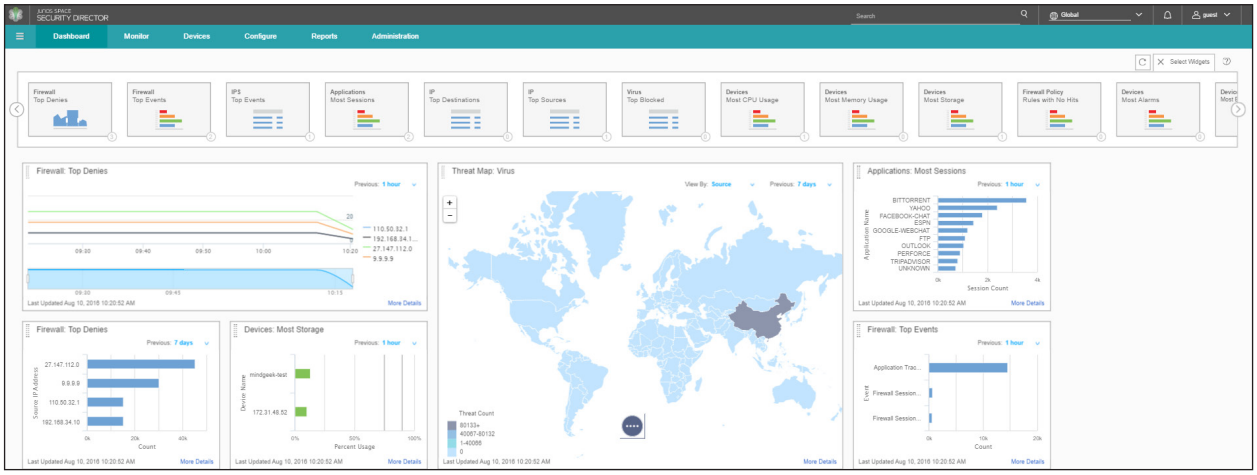


Figure 3 *Security Director Dashboard*

The Security Director Dashboard can display, among other features:

- A palate providing predefined widgets that display firewall, threat, IPS, application throughput, and device-related information.
- A quick view of important statistics for SRX Series devices, such as alarms, consumption for most CPU cycles, or RAM for a specific time period, and more.
- A threat map widget showing the number of IPS events detected per geographic location. The More Details option enables you to drill down to pre-filtered events.

As shown in Figure 4, the Web UI for Application Visibility displays an actionable intelligence feature that eliminates the need to manually create and manage the required firewall rules.

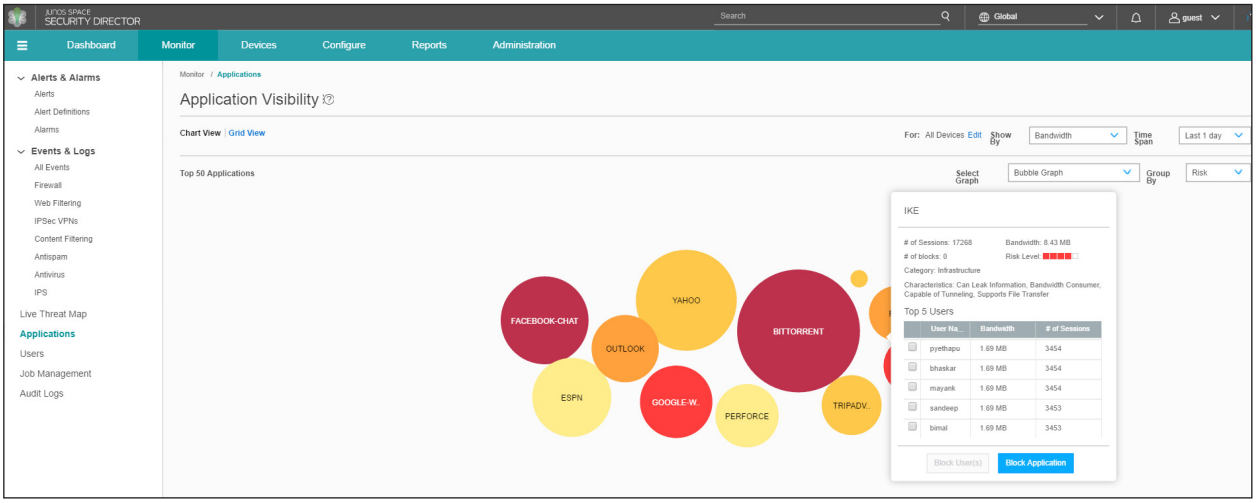


Figure 4 *Security Director Application Visibility*

The Security Director innovative application or user visibility charts display:

- Interactive or graphical summary of applications.
- Visual representation of the types and relative amounts of traffic passing through your network in a graph view. You can block users or applications by selecting the specific application from the graph.

As shown in Figure 5, the Web UI to detect threats shows the attack vectors for currently active IPS and virus attacks.

Figure 5 *Security Director Live Threat Map*

The Security Director live threat map provides:

- Live animation of the threat origin.
- Ability to zoom into a region for filtered threat view details.
- List of threat criteria.
- Insight bar to drill down for more detail.

For a complete list of dashboard features, visit the links at the end of this *Learn About* in the *References and Resources* section.

Security Director Use Case

Let's review a use case for Security Director, and follow the requirements and the solution. This use case concerns a multinational financial services firm with corporate clients around the globe.

The firm wants to accelerate its business transformation and improve its capital position while reducing its Basel III risk and costs. At the same time, it wants to enhance its competitive positioning across its many businesses, so the financial services firm deploys a simple, open, and smart data center based on Juniper Networks MetaFabric architecture. The MetaFabric architecture is delivered through a combination of switching, routing, and security platforms while leveraging network orchestration, software-defined networking (SDN), and open APIs to simplify integration within the technology ecosystem.

The intelligence behind the robust security of the MetaFabric architecture is Security Director, which gives network administrators the power to centrally configure and manage application security, firewalls, IPS, VPNs, and security policies by using a single, intuitive interface.

MetaFabric architecture for this customer includes:

- QFabric System
- SRX Series Services Gateways
- MX Series 3D Universal Edge Routers
- Junos Space Network Management Platform, including Network Director and Security Director
- Junos Space Service Now and Service Insight

By deploying MetaFabric architecture, the financial services firm is able to:

- Improve application performance to better serve clients.
- Cut OpEx by simplifying the turn-up process for new data centers.
- Use automation to reduce IT workload.
- Reduce global data center footprint by more than forty percent.

With a highly intelligent infrastructure in place, this financial services firm has a rock-solid foundation for the future, with the ability to incorporate SDN capabilities when ready.

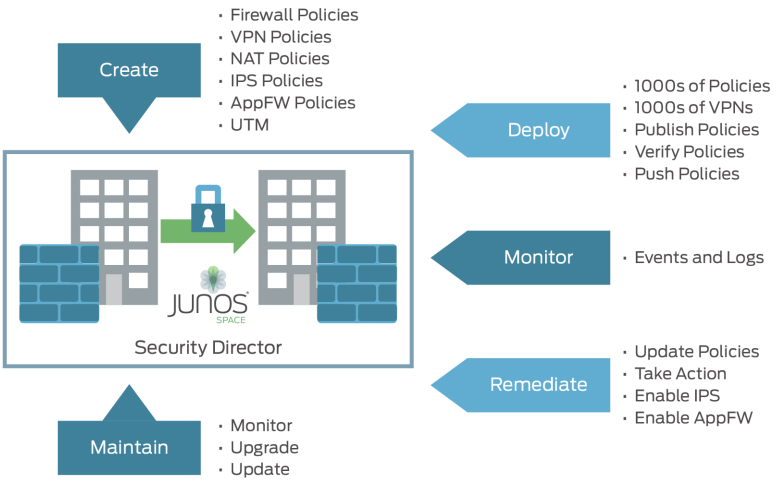
References and Resources

- Start here at the Security Director product page on the Juniper Networks website: http://www.juniper.net/us/en/products-services/security/security-director/
- The datasheet for Security Director provides a great product overview: http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000332-en.pdf
- Security Director is an application that leverages the Junos Space Network Management Platform: http://www.juniper.net/us/en/products-services/network-management/junos-space-platform/
- Security Director Onboarding Guide: http://www.juniper.net/techpubs/en_US/junos-space15.2/topics/task/operational/junos-space-security-director-guide-onboarding.html
- Security Director technical documentation: http://www.juniper.net/techpubs/en_US/release-independent/junos-space-apps/junos-space-security-director.html

Learn About Network Security Management

by Sushma Sethuram

With network security management there is no room for error – the rapid evolution of the threat landscape, in addition to changes in network and security architectures, makes it both challenging and complex. But with Juniper technology, network administrators can provision policies across the entire network – effectively protecting an entire security domain. Learn more about what you can do today to protect your network.



About the Author:
Sushma Sethuram is an Information Development Engineer at Juniper Networks with over 10 years of experience in writing and developing documentation for networking and telecommunications.

Version History: First Edition, September 2016 2 3 4 5 6 7 8 9

For more information go to the TechLibrary at: www.juniper.net/documentation