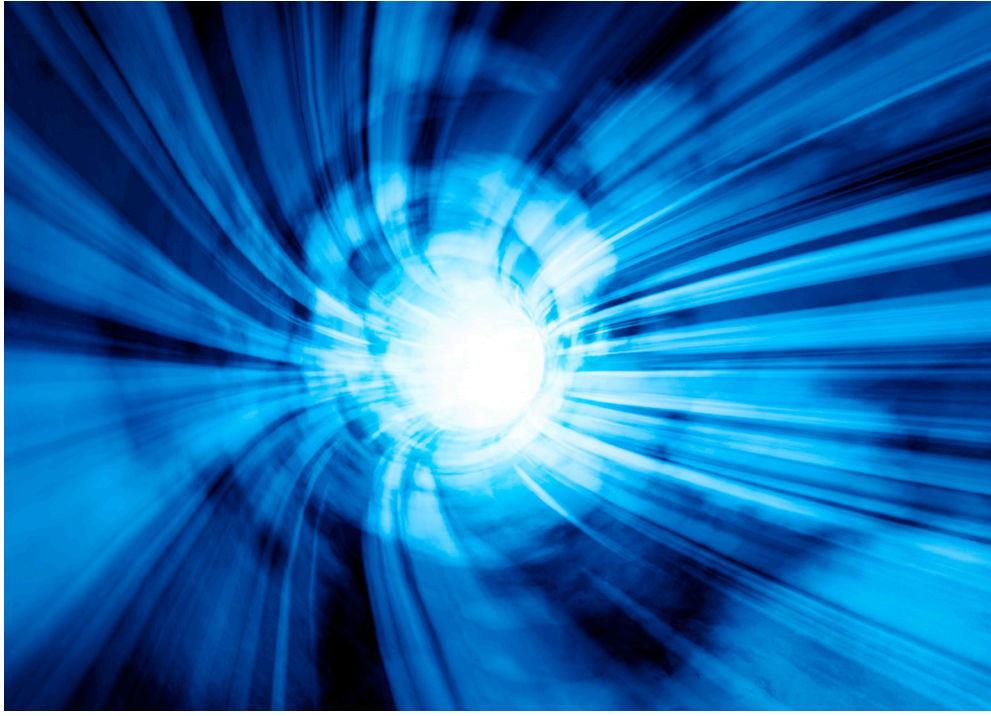
Top 6 Security Measures for the Enterprise Campus Network



As organizations continue to expand their use of mobile networking and social media to stay competitive and on the forefront of business, they are also increasing their reliance on delivering business-critical applications and services through the cloud. The expansion of cloud-enabled models, however, creates critical challenges and risks for builders of enterprise campus networks. These include:

- **Growing security vulnerabilities**—in the cloud-enabled enterprise, threats don't come from a single source and attacks can happen in different forms on any point in the network.
- **Increasing deployment and management complexity** at a time when there is mounting pressure to be faster and more agile in building, scaling and managing the network.
- **Potential performance gaps** that could negatively impact the availability and performance of business-critical applications.

For network builders this not only means ensuring network performance and reduced complexity for a wider volume and variety of devices and locations; it also means adopting a Secure Networks approach that provides a united front against potential attacks. This next-generation network security model moves away from the current tradition of disparate security products and security points. Instead, security is deployed on a network-wide basis in a unified model.

TechTarget® Custom Media
A TECHTARGET IMPACT REPORT

Building, supporting and securing multiple locations in a cloud-enabled enterprise requires that network administrators have full visibility into the entire network from a centralized location. Network builders must also ensure that malware and sophisticated threat detection and intelligence are automatically distributed across firewalls throughout the enterprise.

Beyond that, in building the network you should deploy network management software that lets you enforce policy dynamically and globally, using advanced automation tools that eliminate the risk of human error. For example, you can accelerate deployments and improve security by automating manual tasks such as provisioning new switches and fabrics, or by using profile-based, pre-validated configurations for bulk provisioning.

The concept of a united and integrated Secure Networksd approach for all locations is being driven by the changing needs of the cloud-enabled enterprise. It is also being necessitated by the growing sophistication of security attacks that increasingly exploit vulnerabilities of mobile users, social media and bring-your-own device (BYOD) initiatives.

Building the right solution requires working with a provider that delivers an integrated portfolio that brings together all of the elements required for a comprehensive and strategic approach to network security. In this article we look at six critical factors that will enable you to secure your network at all distributed locations in a cloud-enabled environment. We also describe why a united architecture incorporating and integrating these elements is the best way to protect your enterprise today and for the future

Consideration No 1:
End-to-End Visibility

In order to secure the network you need to have end-to-end visibility so you can understand the network and then be able to program it to defend against any threats or bad actors. As networks become more virtualized and builders increasingly adopt software-defined models, it is important to have visibility and control across both physical and virtual infrastructure.

This type of end-to-end management model is embodied in the Junos Space Network Director from Juniper Networks. Space Network Director provides a highly automated network management platform coupled with sophisticated security management through the Junos Space Security Director, which is described in greater detail below (see Consideration No. 2).

Junos Space Network Director allows network and cloud administrators to visualize, analyze and control their entire enterprise network from end to end through a single pane of glass. This includes data center and campus networks; physical and virtual infrastructure; virtual overlay networks; and wired and wireless networks. It simplifies and automates deployments through features such as fabric automation, Zero Touch Provisioning and bulk provisioning, allowing you to accelerate, simplify and eliminate human error in configuring and deploying new fabrics or switches.

Consideration No. 2:
An Advanced Network Security Policy and Management Platform

In addition to end-to-end network visibility, network administrators need to set and enforce policy across the entire network to account for emerging and traditional risk vectors. This means network builders should deploy a security management platform that provides extensive scale, granular policy control and policy breadth across the network. The platform should include automated policy enforcement capabilities in order to reduce the risk of human error.

Network builders can extend security and policy control for both physical and virtual firewalls with Juniper's Junos Space Security Director, which is an application on the Junos Space Network Management Platform. Through an intuitive, graphical and centralized Web-based user interface, administrators can quickly manage all phases of the security policy lifecycle for advanced services, including:

- Stateful firewall
- Unified threat management (UTM)
- Intrusion prevention system (IPS)
- Application firewall (NGFW)
- VPN and Network Address Translation (NAT)
- Threat intelligence (Spotlight Secure)

Among the key differentiators of Junos Space Security Director is that it is highly customizable—offering administrators high levels of granularity, control and visibility, along with the ability to access separate policy-level and device-level views.

Consideration No. 3:
Anti-Malware Protection with Advanced Threat Prevention

The threat landscape is an ever-changing place in which those who would do harm to your business are constantly seeking to seize upon new vulnerabilities. Conventional anti-malware products have become less useful as malware grows more sophisticated and bad actors increasingly attempt to leverage command and control (C&C) servers to attack and steal valuable corporate assets. Network builders in cloud-enabled environments therefore need to incorporate new solutions that deliver advanced anti-malware protection against sophisticated zero-day attacks and unknown threats.

One of the industry's innovative solutions is Juniper's Sky Advanced Threat Prevention, which is a cloud-based network sandbox that uses static analysis, dynamic analysis and advanced deception techniques to detect and block new forms of malware and zero-day threats. Sky Advanced Threat Prevention augments sandboxing with unique deception techniques to trick evasive malware into making its presence known. These capabilities deliver higher catch rates and enable Sky Advanced Threat Prevention to identify new malware and prevent attacks as the threat landscape changes.

Consideration No. 4:
Secure Gateways for Campus and Branch Locations

One of the particular challenges of the cloud-enabled enterprise is to provide secure network connectivity for campus and branch locations. These networks provide employees with their on-ramps to the cloud—whether private, public, hybrid or some combination—so securing them must be the highest priority for network builders.

Juniper Networks SRX Series Services Gateways for campus and branch combine next-generation firewall (NGFW) and unified threat management (UTM) services with routing and switching in a single all-in-one high-performance and cost-efficient network device. The SRX Series Service Gateways for the campus and branch provide perimeter security, content security, application visibility, tracking and policy enforcement, user role-based application control and threat intelligence.

Consideration No. 5:
High-Performance Security for Virtual Environments

The cloud-enabled enterprise relies heavily on virtualization to drive efficiencies, reduce costs and enable the business to improve agility through resource sharing. High levels of virtualization, however, can complicate security efforts and security policy management. These challenges can only be met by a new breed of security solutions that have been designed from the ground up for virtualized environments.

The Juniper Networks vSRX Services Gateway is one such solution. The vSRX is a complete virtual firewall solution that includes core firewall, robust networking, advanced security services at Layers 4-7, and automated lifecycle management capabilities. With automated provisioning, network and security administrators can quickly and efficiently provision and scale firewall services to meet the needs of the cloud-enabled enterprise. The vSRX is regarded as the industry's fastest virtual firewall, offering throughput of up to 17 Gbps firewall large packet (1,514 byte) and 4 Gbps IMIX. No other virtual firewall comes close to these performance levels.

Consideration No. 6:
Avoid the Proprietary; Embrace the Open

The underlying framework—and philosophy—of the cloud-enabled enterprise should be based on the support of open standards. Typically, you will be using multiple clouds from different vendors and you want to ensure the highest levels of integration and connectivity. Also, with the move toward software-defined networks, you want to be able to deploy agile and high-capacity networks that serve greater numbers of users, devices and locations—while using fewer resources and delivering improved cost efficiencies.

With technologies evolving so quickly, the last thing you want is to be locked into a proprietary architecture that prevents you from using best-of-breed solutions and new innovations when they become available. Juniper Networks has embraced an open approach through its Open Convergence Framework. Within this framework, Juniper offers not only an open platform, but also an ecosystem of partners to complement its own offerings.

Juniper partners include Aruba Networks, Ruckus Wireless and Aerohive Networks to support secure wired and wireless cloud-based initiatives. These partnerships (and others), along with the Open Convergence Framework, assure that network builders can provide easy access to business resources from any device and any environment—without locking you into a proprietary model.

Putting It All Together

Utilizing the six elements discussed in this article will provide the foundation you need to build secure networks for the cloud-enabled enterprise. But there is one more critical factor: putting it all together. This is another area where Juniper Networks is providing industry-leading innovation through its Unite Architecture. Unite brings together all critical network security elements to provide an integrated, cohesive and comprehensive security framework for the cloud-enabled enterprise.

With this united approach, network builders can deliver the sophisticated threat protection, security management capabilities, visibility, automation and scale necessary to defend the business against threats at any point in the network. Please visit Juniper.net/Unite to learn more about how Juniper can help you build the right network solution to secure your cloud-enabled enterprise.