JUNIPER NETWORKS | Engineering Simplicity

eGuide

Real-World Guidance from a Leading Practitioner:

How to Develop a **Smart Building with IoT**

Topic 9 of 9

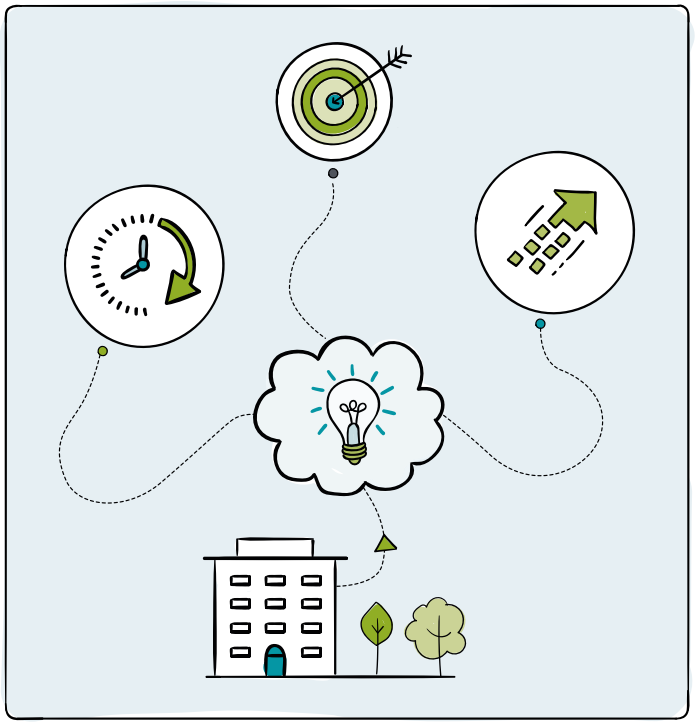
December 2018

Introduction

A smart campus is an intelligent platform. Akin to a miniature smart city full of smart buildings, a smart campus adapts to accelerating change and constantly improves its services.

By leveraging qualities like observability and controlability, tighter feedback loops can drive better outcomes throughout a smart campus. When informed by Internet of Things (IoT) devices and a growing edge compute capability, new and old services alike can be delivered faster and more efficiently.

As a platform for learning and innovation, a smart campus must also ensure it delivers its services in a safe and secure manner. Whether using sensor or "human telemetry", insights by operational and security teams can be realized faster when seeking to detect, mitigate, or contain threats to data integrity or human safety.



About the Author:

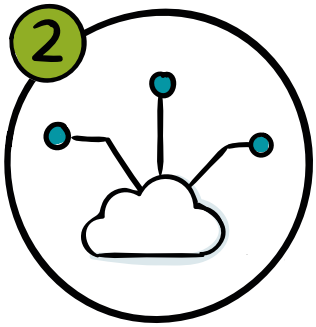
Donal wears many hats and believes we are all network engineers in one form or another. He consults at Defensible, builds engineering testing tools at PanSift, and grows community at iNOG. Donal hails from a mix of engineering and security roles in telco/mobile, enterprise, vendors, and start-ups. He's previously held multiple industry certifications (including a very early CISSP) and comes from a computer science background. These days he gets most satisfaction when growing communities of practice.

– Donal O Duibhir

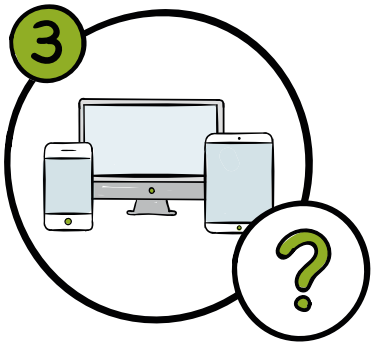
Key Questions

The following questions can help leaders architect and sequence the journey towards a smarter campus:

What is the primary or ultimate goal of a smart campus: smarter citizens and communities, more sustainable practices, or just better use of resources?



From IoT Device to Edge: where is the IoT edge and how can edge devices be classified in a security model?



Criteria: what determines which edge devices are IoT and which are not?

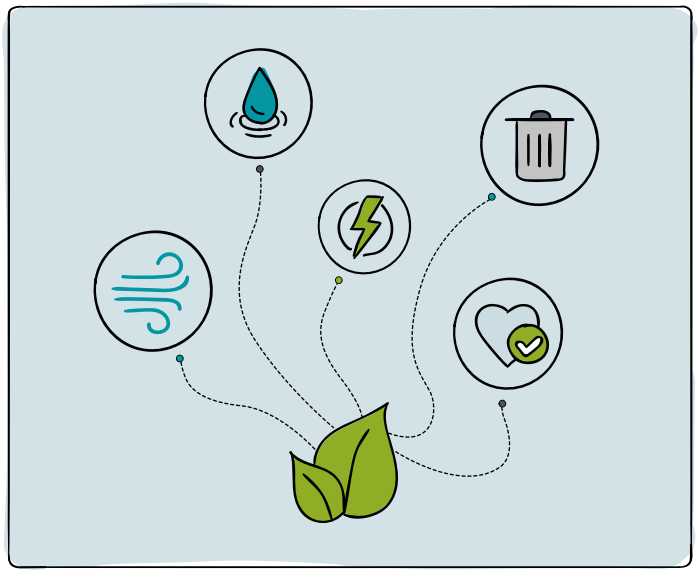
The answers to the above can shape a next-generation platform that leverages automation and is composed of a range of multicloud ecosystems.

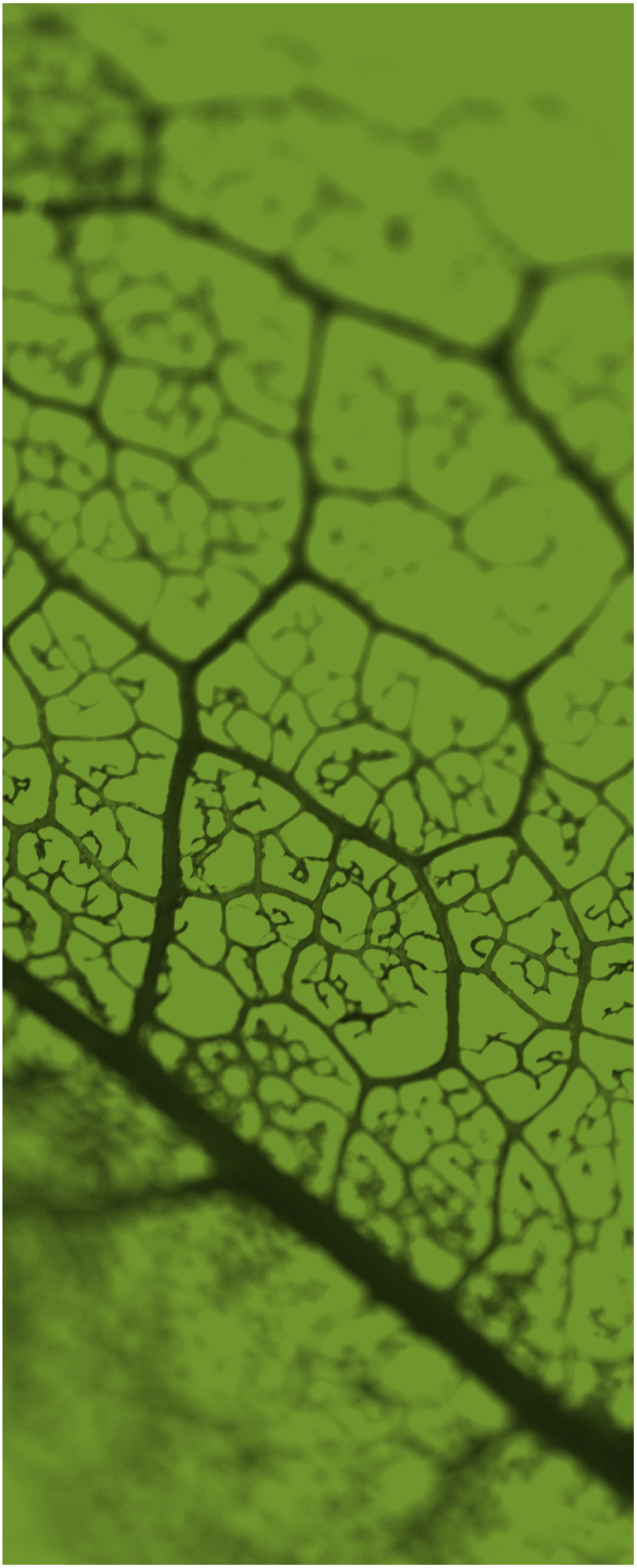
IoT and Our Environment

IoT is an abstract catch-all term for sensors and devices that did not previously provide interconnectivity, IP interfaces or APIs. IoT-enabled devices typically operate independently of human interaction, are mostly wireless, require little power and are often dedicated to a single task rather than more general-purpose compute.

Devices that were standalone or isolated in islands now become part of the campus fabric. When connected, devices such as light bulbs, CCTV systems and thermostats contribute to greater efficiency and more intelligent services. Additionally, air quality is a fundamental consideration: CO_2 and certain VOCs (Volatile Organic Compounds) levels have profound effects on human cognitive performance and general health.

If we focus on optimizing spaces for humans then one fundamental factor is that of air quality. It can have a huge impact on our productivity and learning. Certain CO_2 and VoC (Volatile Organic Compounds) levels have profound effects on cognitive performance and general health. If a campus can become smarter in its management of not just air, but its water, energy, and waste, can it boost the health of its inhabitants and that of surrounding environments?





IoT Security

When grouped together, IoT devices can be thought of as a new cloud or layer which often makes use of the campus access edge. Coupled with an often-weak device security posture, IoT devices are often designated as untrusted (or semi-trusted) and are zoned as such.

Many devices perform their primary function well enough but have not been rigorously security tested, nor built using secure development life cycles. Some expose more of an attack surface than necessarily and are also difficult to upgrade (assuming that firmware upgrades and timely security patches are even available).

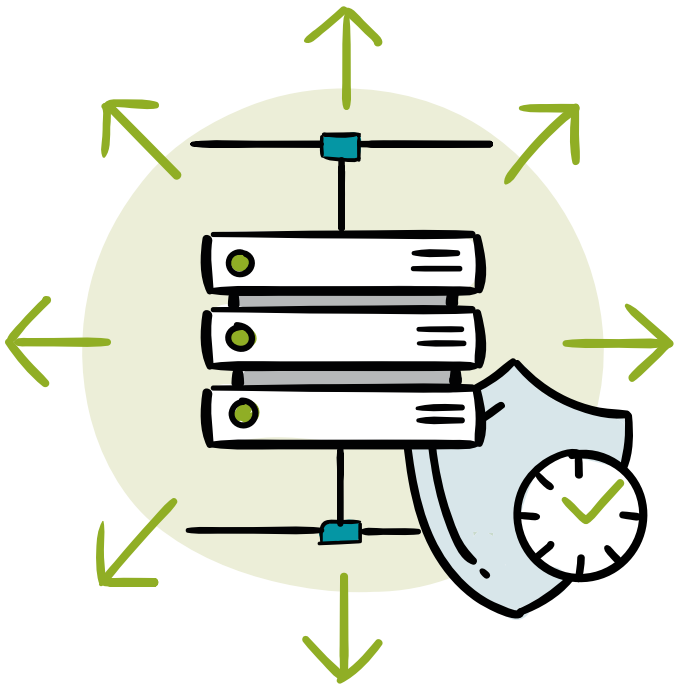
When connecting these devices to a campus fabric, it is advisable to heavily police IoT zones and gateways by enforcing strict policies, including the use of advanced threat protection measures.

The Edge Compute Evolution

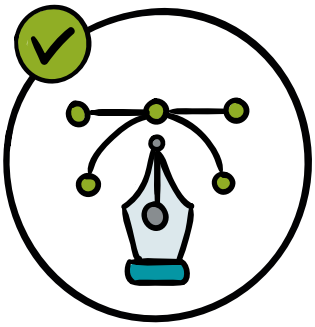
As intelligent and real-time services are made available in even more spaces, increased compute capabilities are moving closer to their data generation sources and points of use.

This enhanced edge is now where even more processing takes place due to the low latency requirements for technologies such as ML (Machine Learning) when applied to machine vision, ICS (Industrial Control Systems) and analytics. Whether the endpoints are fixed or mobile they result in greater demands for localized storage and compute, but conversely in less data transiting the core.

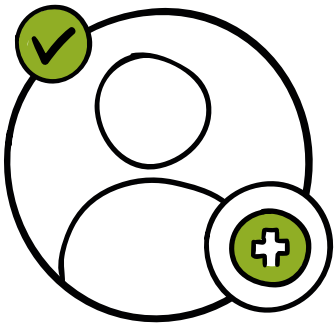
ML training will still primarily take place in public or private clouds while latency sensitive operations will migrate closer to this new compute edge. This also results in greater complexity at the edge which itself demands increased reliability, resiliency and security. This new edge paradigm for storage and compute is one which strengthens the need for unified management and consistent security policy throughout a converged campus fabric.



Checklist:
Developing a Smart Building with IoT

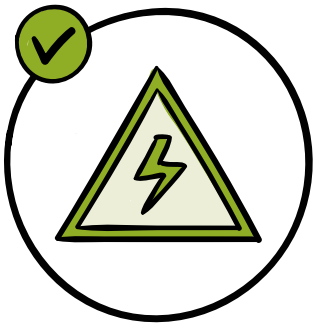


Determine the ultimate goal of the smart campus and keep it in primary focus throughout the design stage.



Consider the likely typical human interactions with the smart campus, and the knock-on effects on resource usage and human health.

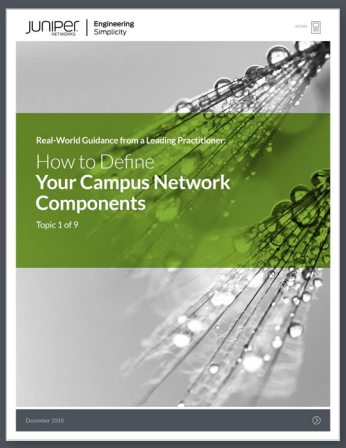
Ensure IoT devices meet the required security levels, especially if they are edge devices involved in processing.



Deploy advanced threat protection to safeguard IoT zones within the campus fabric.

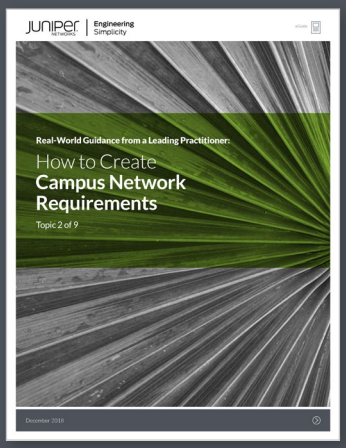
Continue reading the series

Choose from the other topics available in this series to find out more on how to architect your campus network:



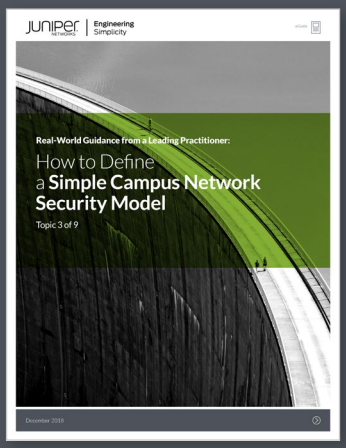
How to Define Your Campus Network Components

Read Next



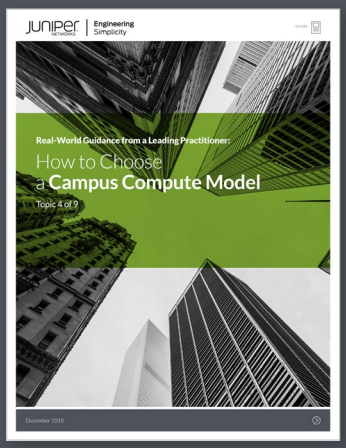
How to Create Campus Network Requirements

Read Next



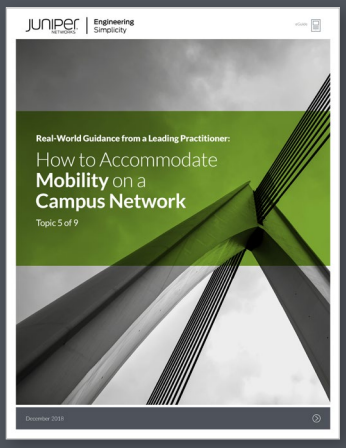
How to Define a Simple Campus Network Security Model

Read Next



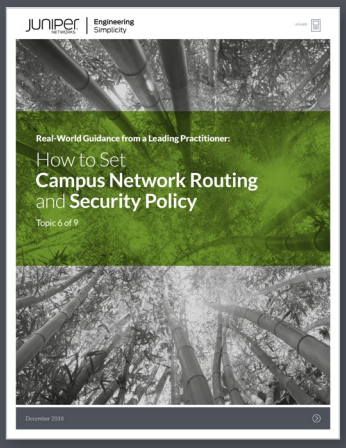
How to Choose a Campus Compute Model

Read Next



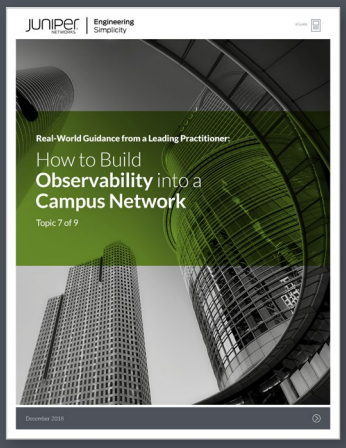
How to Accommodate Mobility on a Campus Network

Read Next



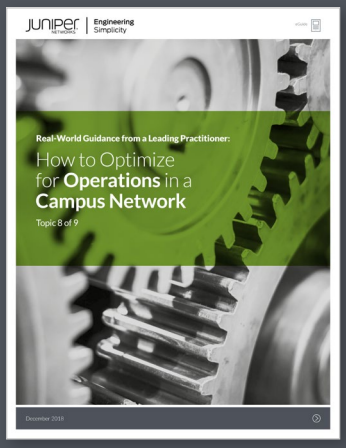
How to Set Campus Network Routing and Security Policy

Read Next



How to Build Observability into a Campus Network

Read Next



How to Optimize for Operations in a Campus Network

Read Next

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

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240
119 PZ Schipol-Rijk
Amsterdam, The Netherlands

Phone: +31.0.207.125.700

Fax: +31.0.207.125.701

Copyright 2018 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. In the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

PN 7400098-001-EN

JUNIPER NETWORKS | **Engineering** Simplicity

Please Note:

This guide contains general information about legal matters. The legal information is not advice, and should not be treated as such.

Any legal information in this guide is provided “as is” without any representations or warranties, express or implied. Juniper Networks makes no representations or warranties in relation to the information in this guide.

You must not rely on the information in this guide as an alternative to legal advice from your attorney or other professional legal services provider. You should never delay seeking legal advice, disregard legal advice, or commence or discontinue any legal action because of information in this guide.

Information correct at time of publication (December 2018).