THE SAVVY CIO'S GUIDE TO SOFTWARE-DEFINED NETWORKING

CISCO ACADIA TECHNOLOGY GROUP

TABLE OF CONTENTS

INTRODUCTION

Software-defined networking (SDN) provides growing enterprises with the flexibility necessary to embrace digital transformation in more significant ways. Yet it's a major change from traditional network architecture and often requires firms to have tough conversations around refresh cycles, budgeting, resource allocation, and personnel management.

Enterprises with an eye to the future would do well to develop an even stronger understanding of SDN as well as its drawbacks. In this guide, we take a deep dive into these questions while offering real-world solutions for enterprises looking to grow. There's a great need for network automation for many reasons, not the least of which is security.

With digital transformation comes more data, more IoT-enabled devices, and more ways for potential breaches to occur on your network. Our guide addresses these issues as well while highlighting practical solutions through SDN.

SDN AND PCI DSS COMPLIANCE: CONVERSATIONS WITH THE PCI AUDITOR

Payment Card Industry Data Security Standard (PCI DSS) compliance applies to all types of businesses that process, store, or transmit credit card data. Consistently protecting personal data, credit card information, and customer identities can present a considerable challenge for any organization.

Whenever we engage with a PCI auditor, aka Qualified Security Assessor (QSA), it quickly becomes apparent that many businesses believe becoming compliant is the end goal. In reality, maintaining PCI DSS compliance is an ongoing endeavor.

If your network isn't continuously protected, you run the risk of making headlines like the credit reporting firm Equifax that exposed the data of 143 million US consumers. While some enterprises have enough resources to weather the fallout from such negative publicity, many others just won't make it.

As reported by Verizon, if you're not maintaining PCI DSS standards on an ongoing basis, there's a higher probability you'll be breached.

QSAs are looking for evidence of the following:

- Enhanced network protection
- Consistent maintenance of a secure network
- Cardholder data protection
- Vulnerability management programs
- Deployment of strong control measures
- Regular testing and monitoring of networks
- Consistent maintenance of a robust information security policy and best practices

As technology evolves, IT leaders have to continuously explore how they can maintain PCI DSS compliance. This means that the real challenge comes after obtaining the certificate as you must keep the data safe to maintain your customer's trust. This same security framework can be applied to protect other sensitive data such as Social Security numbers, trade secrets, and financial records.

Cisco's Software Defined Access (SD-Access) presents a viable solution to keep sensitive data safe and address the scaling issues we are experiencing with traditional VLAN network segmentation. It can enable enhanced network protection to maintain security and compliance, while at the same time vastly simplify the administrative burden of provisioning the network and maintaining security.

Restrict Connections from Untrusted Networks

To maintain data security, restrict connections to system components in the cardholder data environment and all untrusted networks.

Sounds simple, right? Historically, this was achieved by building a firewall and configuring routers with lots of complex access lists to restrict access.

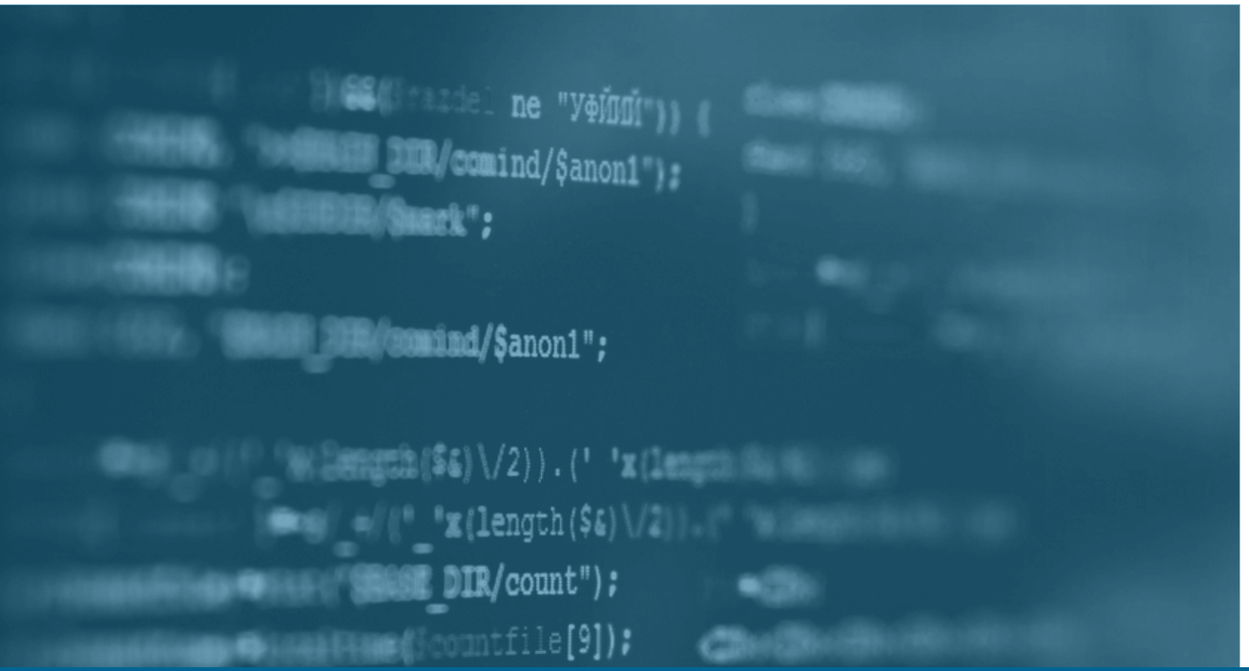
In a PCI scenario, an untrusted network can be described as any network segment that does not carry credit card data. Over time, we have seen a sharp rise in the number of network segments making it increasingly difficult to reduce our attack surface against malware, ransomware, and other viruses. Adding to this difficulty is the rapid rise in the number of devices some firms add to their networks.

Developments such as BYOD and IOT have grown the number of network endpoints faster than we can reduce our segment sizes. Attempting to create more network segments with theoretically fewer endpoints on each has driven up operational complexity. This is because of the need to maintain complex and longer access lists in router and firewall configurations. Long-term, this becomes unwieldy and expensive to manage. Furthermore, as source or destination devices are removed from or changed in the network, corresponding entries in access control lists may or may not be removed/changed potentially leaving the network vulnerable to exploitation.

In these situations, the best approach is to micro-segment these applications and apply firewall-style restrictions between them. This type of zero-trust approach with granular control is only possible with software-defined networks (SDNs).

SDN addresses these issues by placing all network devices and users in groups. Policies (think access-lists) are built using these groups (and not IP addresses) that permit or deny traffic/communications between the groups. Further granularity, or segmentation, can be achieved by permitting or denying traffic/communications between objects in the same group. This policy-based (not IP based) approach allows for greater insight and manageability of the network.

The creation of many isolated network segments isn't required by PCI DSS, but it goes a long way to protect the cardholder data environment. This is because any malicious intrusions that gain a foothold in the network will try to attack sensitive data. So, if the network can be compromised, the risk is greater that the intruder will ultimately get to the more isolated card holder data.



This means you can no longer follow the traditional data center design philosophy that places firewalls on the outside and all the sensitive data inside. Instead, all applications need to be treated just like public cloud providers treat each one of their tenants – isolated and untrusted in their own network segment. Imagine the implications of managing such an environment. SDN can make managing a policy-based environment on an application-by-application basis easy and practical.

Enhanced Cryptography and Security Protocols

When transmitting sensitive data outside of your network, businesses need to employ strong encryption protocols to keep that data safe. Increasingly, this also includes internal networks to reduce risk and further protect data from external or internal threats.

In 2017, we saw a rise in ransomware attacks and this trend is expected to continue in this year. As these threats evolve, the PCI Security Standards Council will also respond to it by updating their data security standards.

Maintaining PCI DSS compliance with SDNs creates innovative opportunities to restrict untrusted networks, enable micro-segmentation, and maintain encryption on all related networks.

Our conversations with PCI assessors consistently reaffirm the potential of SDN to provide a robust network protection strategy. This strategy will not only help firms obtain compliance certification, but it will also lay down a strong foundation that will ensure the protection of sensitive data going forward.

HOW SDN STREAMLINES AND IMPROVES LAW FIRM NETWORK PROTECTION

As cyberattacks on business IT networks grow bolder and more sophisticated, law firms have become a prime target for attackers. How will you protect your firm from attacks?

Recent reports show that more than a third of law firms with 10 to 49 attorneys have experienced a security breach. This can no longer be a problem for just the head of IT, but a problem for the firm's attorneys or corporate legal counsel.

Last year showed ransomware in the legal industry left a great deal of fallout in its wake. As you come to grips with the limitations of your network's security and agility in a demanding climate, software defined networking (SDN) can be a solid option for protecting your firm's network.

Overcoming Roadblocks in Legal Firm Data Security

In the legal sector, data is king. Protecting, moving, and accessing that data, as well as the communication channels that go hand in hand with the legal strategy behind

it, are all vulnerable to wired and wireless networking shortcomings.

Meeting the need for securing the network reveals problems that include:

- Document management relating to preserving and protecting clients' intellectual property, privileged communications and work product
- Lack of granular access management that can be easily tracked and modified in real time
- Secure and high bandwidth remote access for mobile legal personnel
- Unsecure storage environments/device workarounds
- Email and collaborative platform rule policy management for transmission of sensitive information
- Voice, video, and other bandwidth-intensive transmissions across the wired and wireless LAN and WAN
- Unpredictable CAPEX for increasing network hardware needs and OPEX for dedicating IT resources for network configuration, operation, and monitoring

These are complex challenges that only legal Industry SDN can solve by bringing simpler, faster, safer, and more agile/responsive networking.

Building a Better Network with SDN

Since most network configuration changes are manual, your IT team may find it difficult to meet deadlines managing the data and protection needs of a growing law firm. By integrating more responsive and automated security traffic monitoring and responses through SDN, they can deliver agile network configurations in real time.

That means that Cisco's SDN approach for law firms makes it possible to deliver consistent policies and services over wired, wireless, and hybrid networks.

This can all be done while reducing both OPEX and CAPEX.

According to a Cisco Customer Education presentation, 75 percent of OPEX is spent on network visibility. SD-Access provides the deep visibility your network administrator and IT team need through automation that delivers Intent-Based Networking. Intent-based systems let the administrator tell the network what to do and SDA automation makes it happen. This brings legal environments the benefits of:

- Automating simple single-point network operations, along with orchestration and management of network functions
- Granular Identity Access Management that's rule-based with real-time tracking and changes for context for users and devices, including authentication, posture validation, and device profiling
- Hardware savings and reduced CAPEX through agnostic network integration
- Unified cloud resources
- Secure and easily configurable video conferencing, conference calls, Voice over IP and electronic document data transmissions that are secure, simple, and meet QoS requirements, while saving time and cost.
- Automating network printing and scanning security protocol authorization and enforcement

As your IT team faces increasing workloads and growing threats, they must respond with a transparent solution that can adapt to the changing landscape. By automating day-to-day tasks such as configuration, provisioning, monitoring and troubleshooting, your IT team reduces the time and costs of network adaptation and issue resolution while reducing security attack surfaces across the network.

OVERCOMING NETWORK AGILITY ROADBLOCKS WITH SDN FOR MANUFACTURING ENTERPRISES

The movement to creating Smart Factories through manufacturing automation and streamlined data exchange is changing the way things are being made, and software-defined networking is at the forefront of network technologies enabling this transformation.

Industrial IoT (IIoT), machine to machine (M2M), the cloud, wired and wireless networks and the expanding network edge of a global supply chain are now requirements for competitive manufacturing. The IDC Manufacturing Predictions 2018 study says that by 2020, 60 percent of G2000 manufacturers will rely on digital platforms that support 30 percent of overall revenue.

Manufacturers working to increase productivity in this new global manufacturing economy are realizing that the goal of fast and agile data throughput and access must be balanced with proactive security and compliance.

In this type of evolving manufacturing landscape, networking is the linchpin for achieving those possibilities. Manufacturers can do this by introducing digital transformation holistically from the factory floor to beyond the network edge.

Software-Defined Network (SDN) is emerging as the ideal solution for meeting the needs of manufacturing. However, SDN for manufacturing enterprises only becomes a clear solution when you understand how it can be applied to address the evolving challenges and pain points across an expanding manufacturing ecosystem.

The Challenges of Transitioning to Smart Factories

According to Cisco, 95 percent of network changes are manual in nature, 70 percent of policy violations are due to human error, and 75 percent of OPEX is spent on network visibility and troubleshooting. Slow and error-prone manual network configuration and fragmented tool offerings are clearly the main challenge to a responsive and agile network in a digital world where:

- Network switch deployments and software upgrades take hours
- Application deployment, access and monitoring are time, resource, and cost-intensive
- Security and policy concerns with proprietary data in transit to and from the cloud as well as within wired and wireless networks leaves evolving points of vulnerability
- The manufacturing environment and broader supply chain are constantly changing and evolving with more users, devices and applications
- Consistent policy between increasing wired and wireless in-network devices and users add complexity and vulnerabilities to credentialing and access configurations
- Finding and troubleshooting network issues becomes more difficult and error-prone
- Bandwidth issues across the network and to the cloud create latency problems that affect network performance

Consequently, it's important to have a way to integrate internal visibility of production processes and networking with external supply chain operations and logistics. The solution must be infinitely agile to enable real-time changes relevant to the manufacturing cycle while eliminating the network silos of IT and operational technology (OT). SDN for manufacturers can deliver the convergence of data-centric computing of IT with OT's event, process, and device monitoring. This enables simplified adjustments in enterprise and industrial operations.

Benefits of SDN in Manufacturing

IIoT and sensor technology are crucial to manufacturing by tying critical operational and control data from shop floor equipment and robotics to product and materials movement, vehicle fleets, and material handling systems. This data is constantly being produced and directed through wired and wireless IT/OT networks and the cloud to beyond the network edge.

Because of the global economy, supply chain management requires agile network provisioning, routing, and monitoring for cost containment and logistical agility. This is the only way to accurately manage the expanding internal systems, applications and devices that produce and run on big data while integrating the many disparate corporate, manufacturing and third-party partners.

SDN solutions help manufacturers manage the global supply chain in real time by seamlessly tying production and operations of the factory floor to:

- Enterprise Resource Planning (ERP), Material Requirements Planning (MRP) and Warehouse Management Systems (WMS) through Integration with machine learning, IIoT, and Robotic Process Automation (RPA)
- Shipping, logistics, channel partners, distributors and retail for making real-time adjustments and forecasting based on need, inventory and scheduling changes
- The ability to make real-time routing and provisioning changes across network access points
- Meet dynamic data bandwidth needs across IT/OT
- Data visibility and actionable use through appropriate architecture, IoT security, advanced network tools and predictive analytics
- Mobility solutions for troubleshooting and reviewing production lines on the go and supporting an increasingly diverse portfolio of applications and users
- Robust, cost-effective and fault tolerant infrastructure
- Overall Equipment Effectiveness (OEE) analysis for improvements in your internal and external supply chains
- Agile and predictive on-demand bandwidth that connects teams and applications across time zones in real-time via glitch and stutter-free video conferences and mobile devices

Application and Security Benefits of SDN

Today, applications and their access determine if manufacturing entities can support given initiatives.

Manufacturers must be able to build such applications, make them agile, deploy them globally and make them securely available to end users. Software-defined networking for manufacturers can meet all of these needs.

Your manufacturing environment also presents an expanding list of cybersecurity threats through machine and device connectivity as well as data and application access in a potentially global ecosystem. As a consequence, the SDN network security impact extends to creating agile:

- Enterprise and Manufacturing Security Policies consisting of:

  - Role Based Access Control
  - Secure Group Tags on all devices
  - Applying consistent security policies across the wired and wireless network

- Demilitarized Zone and Domains of Trust segmentation
- Firewalls to defend the manufacturing edge
- Interior protection and endpoint hardening
- Security Management, Analysis, & Response
- Real-time identity access management, adjustment and policy implementation
- Regulatory compliance, data governance activity and routing systems

Finally, SDN presents real cost-saving opportunities as traditional hardware and network design methodologies in manufacturing networks are unsustainable and incompatible with digital transformations.

Cisco's SDN solution offerings can improve security, reduce operating expenditures, improve compliance and optimize the user experience. An SDN solution allows administrators to design the network, provision networking gear programmatically and enforce group-based policies to secure the network. Using role-based access control, white-listed users and devices can only access applications and resources they are explicitly given permission to access.

Beyond SDN to Intent-Based Networking

Today, SDN continues to evolve in ways that enable even greater network agility through cloud-based platforms that can deliver Intent-Based Networking (IBN). In general, IBN replaces manual configuration of switches, firewalls and other infrastructure components through the command-line interface (CLI) with automation and orchestration.

This new approach to SDN for manufacturers facilitates planning, design and automatic implementation of on-the-fly changes to the network for greater availability, agility, security, and reliability. An IBN solution using Cisco's SDN technologies can enable true IT/OT convergence through segmentation that enables rapid creation, changes, monitoring, and deletion of network services as needed.

Ultimately these next-generation SDN solutions provide smarter end-to-end network control, automation, and service agility so that your manufacturing environment can quickly and easily meet IT and OT needs today and tomorrow. As a skilled and expert Cisco partner, Acadia Technology Group is ideally positioned to provide you with clarity and context for the usage of Cisco's SDN solutions in your network.

11 RULES FOR SOFTWARE-DEFINED NETWORKING INTEGRATION

As CIOs work to improve the network for services delivery in the digital age, software-defined networking for enterprises has seen a steady rise in adoption. For those in the early decision stages, the question of how to integrate SDN into networking architecture through migration is top of mind.

Although the migration process will require network changes that will affect the entire enterprise, having a rule-based approach to integration is the best way to ensure successful outcomes. To start that process, here are 11 rules for software defined networking integration.

#1. Plotting a course based on need rather than technology

Organizations should first think about their reasons for choosing to go the SDN route and what they want to get out of it before looking at platforms. Businesses and IT needs will be different for each organization and sector such as manufacturing and financial institutions, so SDN will be applied in different ways.

Specific needs could be centralizing and improving enterprise network management and security or improving costs. Needs assessment must go beyond words like “agile” to reach the heart of deployment objectives.

These needs determine the technical process and platform. The goal is to determine how the migration, integration and operation of SDN will affect the business across departments, divisions and enterprise wide.

#2. Discovering application connectivity and Improving the network

In this pre-migration stage, organizations will discover and map business application network flows and dependencies, which are crucial to making the changes needed for the SDN migration. Complex networks and data flows can make this difficult, but machine-readable traffic flow records can lessen the challenge. This stage will also require updating of switches and ports to align with a virtualized SDN environment.

#3. Aligning the infrastructure with the right SDN platform

While there are a number of SDN platforms available, most organizations will choose between ACI and NSX. Rather than discuss their differences, it will be sufficient to say that some organizations may be partial to the VMware solution or the Cisco solution based on their current affiliated networking systems.

#4 Looking beyond automation

SDN migration projects require following a highly detailed process for success, so vendors offering automatic conversions should warrant heavy skepticism.

Despite heavy doses of automation, IT teams will still need to discover, model, migrate, and test business applications in digestible chunks. Only with proper planning, testing and management can organizations migrate applications and begin to see SDN benefits.

#5. Preparing the organization

At this stage, organizations will begin the skill set assessment and training process to support SDN and infrastructure changes. Key IT personnel will need to be trained to think about the control plane in addition to the data plan. For example, the operations engineers and administrators accustomed to CLI will need to adapt to an SDN dashboard.

#6. Lab testing the platform

Most SDN products are available in a test lab environment due to the portability of software. Software portability makes it possible to conduct this implementation testing using onsite and cloud-based virtual lab environments, which enables:

- SDN controller testing by emulating switches in different topologies
- SDN switch performance testing

#7. Develop a SDN security strategy

Software-defined networking can deliver robust security through its system architecture's design possibilities such as:

- Data packet routing through a single firewall to make IDS and IPS data capture more efficient
- Continuously adaptable data protection measures that can be seen in the case of SDN for PCI compliance across enterprise sectors.
- Segmentation that can harden security and reduce attack surfaces

While these and other SDN security measures can be highly effective, lack of a detailed security strategy can open the network to attacks due to uncontrolled traffic. This strategy requires extremely accurate implementation and programming designs that are based on network security priorities and SDN technology understanding.

#8. Managing the migration process

Since application dependencies are mapped and the current network architecture has been optimized for SDN, the migration and integration process can begin. However, this is not something you can do overnight. The work involved in application migrations can vary depending on the size and complexity of the network, and on what the organization is looking to get out of the project. It's a good idea to take a gradual, step-by-step approach.

All applications can't be migrated at once, so an incremental migration should be built on migration strategy stages that include:

- IP address allocation and server workload assignment to new addresses
- Application software reconfiguration to the new IP addresses
- Application traffic discovery policy writing
- Policy deployment and validation
- Application functionality testing
- Moving the application to production
- Decommissioning the legacy version of the application connectivity

#9. Start small

Reaping the enterprise network management and security benefits of SDN is not an all or nothing proposition in terms of integration. Organizations should consider starting small with automation tools that they can add to the existing network today to gain immediate benefits and improvements. This can be followed by more software that provides application optimization based on policies for traffic routing and performance improvement.

A modular approach can set the organization up for success with a broader SDN integration that can be accomplished faster and more assuredly based on need.

#10. Post-integration management

The next step after application migration to the software-defined network is development and implementation of ongoing security policy management. This requires access to change tracking and auditing as well as risk and compliance reporting. As business applications change over time, administrators will need to modify network policies.

Implementation of a holistic, automated change-request system is the best approach to handling security policy management. Keep in mind that the system must be capable of supporting SDN firewalls and security controls as well as the traditional firewall.

#11. Find an Integration Partner

Software-defined networking for enterprises is continually evolving and does come with a learning curve. This is an important reason to partner with a skilled networking integration partner with a track record in SDN deployments like Acadia Technology Group. Having that experience gives the business constant access to a wealth of knowledge on best practices for integration and management. An approach like this can ensure that the SDN integration successfully meets business needs today and tomorrow.

HOW SDN HELPS ENTERPRISES PREVENT DATA BREACHES

There are many security benefits that come from SDN architecture if designed and implemented properly. Just some of the ways that SDN hardens network security include:

- Prevention of DDoS attacks through its separation of data and control planes
- SDN firewalls that can be programmed with policies that provide granular, agile and immediate control over network traffic for design of sophisticated detection algorithms
- The ability to quickly identify intrusions and limit their reach and impact across the network
- Major reductions in false positives that save time and resources in network security protocols
- The ability to segment parts of the network in near real-time to isolate and quarantine malware, stop breaches, and prevent them from spreading across the network

Besides the centralized control of SDN allowing easy and response driven network programmability, it also sets the stage for the potential introduction of new security vulnerabilities to SDN network architecture.

This is because the SDN controller sits at the heart of the agility and security possibilities of the architecture. The controller becomes a potential single point of failure where major vulnerabilities can be “baked in” without proper network design considerations.

How Attackers Could Compromise the Controller

From a security point of view, the separation of control and data planes at the heart of SDN is what provides the programming agility and vast network security improvements. At the same time, the SDN central controller, which is the catalyst for that agility, poses the greatest security vulnerability. This single point of control can be the ideal attack surface that can potentially give a hacker total control of the network.

By compromising the controller, an attacker can:

- Produce false network data and start other attacks on the entire network
- Insert or modify flow rules in the network devices, which would allow packets to be steered through the network to the attacker’s advantage.
- Launch sniffing and man-in-the-middle attacks to intercept, capture, and analyze network communication information by taking advantage of unencrypted communications to intercept traffic from and to a central controller
- Impersonate a controller/application, to gain access to network resources and manipulate the network operation
- Gain control of the communication path to flood the controller with packets requiring a flow rule decision and render it unavailable for legitimate users (DoS attack)

These are some of the primary ways vulnerabilities can be introduced without careful design of the SDN architecture. In the upcoming section on making the most of SDN security possibilities, we provide specific ways that all of these vulnerabilities can be addressed in the SDN architecture design and implementation process. Before discussing the remedies to these challenges, there are other places within the SDN architecture that can be potential vulnerability sources.

Application Manipulation and API Exploitation Vulnerabilities in SDN Architecture

SDN can also be vulnerable to attacks in the application plane that can cause malfunction, disruption of service, or data eavesdropping. A poorly designed application can also introduce vulnerabilities to the system.

APIs within SDN architectures can have vulnerabilities that can give attackers the ability to extract network information or stop network flows. Side channel attacks on the data plane can give attackers the information to redirect traffic flows and allow eavesdropping. The amount of time it takes to establish a new network connection can tell attackers if there are flow rules in place.

All of these vulnerabilities are preventable, but they require a level of knowledge most networking specialists still lack as SDN continues to evolve and grow in adoption. Fortunately, there are numerous ways to avoid the security challenges of SDN while maximizing the security and agility benefits it can bring an organization.

Making the Most of SDN Security Possibilities

New and emerging technologies like SDN are sure to transform networking, but new technologies also bring vulnerabilities. In the case of SDN, those vulnerabilities are a product of a lack of knowledge in proper design and implementation. Consequently, all of the challenges can be avoided to provide all of the benefits that this network architecture can bring.

Based on the security vulnerabilities for the SDN controller and associated systems covered earlier, here are just some of the ways to make the most of SDN security possibilities:

- Roll out redundant controllers and strong encryption on the communication channels to stop controller attacks
- Put proper security mechanisms between every interface, component, and communication channel
- Use secure network elements with strong encryption algorithms to protect against side channel attacks and traffic diversions
- Keep servers updated with the latest patches to protect against application manipulation and API vulnerabilities
- Use rate limiting and packet dropping techniques at the controller plane to avoid DoS attacks

Network security policies and protocols are at the heart of maximizing SDN's security benefits and avoiding its vulnerabilities. By failing to understand how best to implement them or the potential dangers of disabling network designs can introduce the seeds for serious repercussions for the network and the organization.

In an SDN-based network, it will be important for network operators to enforce the implementation of policies such as Transport Layer Security (TLS). Misconfigurations or incorrect use of security features can impact all layers in the architecture.

Success of SDN is Dependent on Proper Design

The benefits of enterprise network security and SDN are growing by the day with most networking professionals understanding that SDN represents the future of network possibilities. But to make the most of SDN, some security challenges must be avoided in the design, implementation, and modification phases within network centralized control and programmability features.

While SDN architectures are the future of secure and agile networking in the digital age, it requires a great deal of knowledge and planning. For example, there are a number of SDN rules that will set the stage for making the most of the architecture. With the support of a partner with expertise in SDN and traditional networking technologies like Acadia Technology Group, enterprises can set the stage for operations capable of meeting all operational needs.

RESOURCES

Threat Matrix 2018 White Paper

Corporate Overview of Acadia Technology Group


Click below to continue the conversation
with Acadia Technology Group.
CONTACT US
CISCO
ACADIA TECHNOLOGY GROUP