Common Criteria Evaluation and Validation Scheme

National Information Assurance Partnership (NIAP)

Title: Software Defined Network (SDN) Controller Essential Security Requirements

Maintained by: National Information Assurance Partnership (NIAP)

Unique Identifier: 42

Version: 1.0

Status: draft

Date of issue: 29 November 2021

Approved by:

Supersedes:

Background and Purpose

This document describes a core set of high-level fundamental security requirements expected of any Software Defined Networking (SDN) Controller for use in an enterprise. It is intended to provide a minimal, baseline set of requirements which can be built upon by future revisions to provide an overall set of security solutions for an enterprise network.

SDN Controllers are one of many components of an SDN networking architecture. See below diagram.

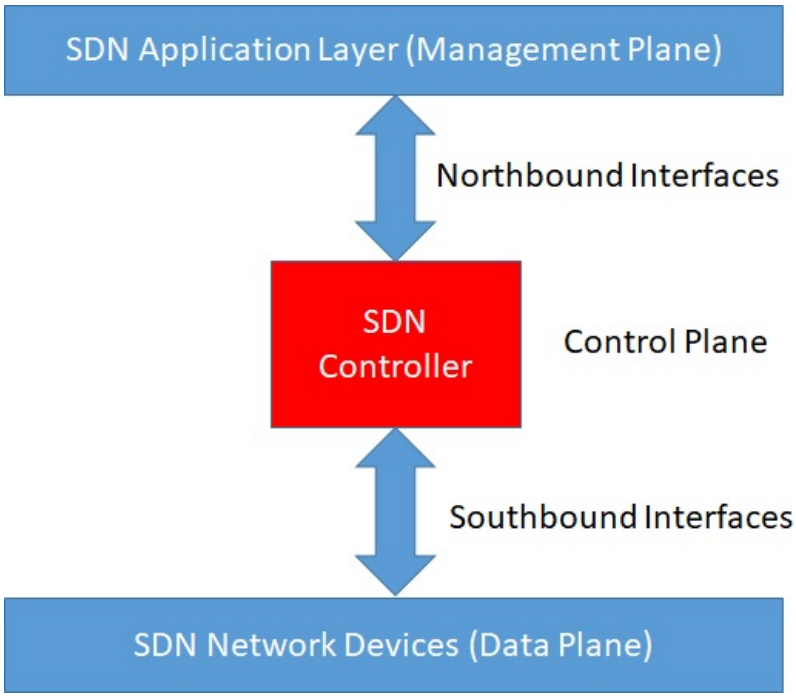

Figure sdn-controller: SDN Controller in relation to the SDN Planes

An SDN Controller is a central and vital component of what constitutes an SDN system and is available as a logical or a physical device. An SDN Controller manages and distributes network policies, collects routing and payload information from the Data Plane, and interfaces with user applications in the Management Plane. Each of the planes in an SDN system is composed of multiple logical or physical components. SDN Controllers logically centralize the network intelligence and state in the Control Plane.

For clarity the following definitions are provided:

- The Control Plane is a logical entity that receives instructions or requirements from the SDN Application layer through its northbound interface and relays them to the Data Plane through its southbound interface. The Controller extracts information about the network from the Data Plane and communicates back to the SDN Application Layer with an abstract view of the network, including statistics and events about what is happening.
- The Data Plane (or SDN Network Devices) controls the forwarding and data processing capabilities for the network. This includes forwarding and processing of the data path.

- The Management Plane (or SDN Applications Layer) is composed of programs that communicate behaviors and needed resources with the SDN Controller via application programming interfaces (APIs). In addition, the applications can build an abstracted view of the network by collecting information from the Controller for decision-making purposes. These applications could include networking management, analytics, or business applications used to run large data centers. For example, an analytics application might be built to recognize suspicious network activity for security purposes. The Management Plane is sometimes also referred to as the Orchestration Layer.

Use Cases

- SDN controller as a standalone physical device.
- SDN controller as a virtual device.
- SDN Controller (standalone or virtual) with management capabilities.
- A cluster of SDN Controllers (standalone or virtual).
- An SDN Controller for hyper-converge consisting of an amalgam of computing resources in a single unit for storage centric, server centric or even hybrid (storage-server) workloads.
- The intent is that an SDN Controller satisfying these requirements will “do no harm” on a network. Rather than providing any explicit security functionality, compliant SDN Controllers simply ensure:
    - They can be remotely managed in a secure manner.
    - Any software/firmware updates are from a trusted source.
    - Any interfaces to applications, VMs, and other devices are trusted (zone of trust).
    - All suspect events are reported.
    - Logical or physical separation of the Control and Data Planes.
    - Logical or physical separation of the Control and Management Planes.
    - Protect data collected and distributed by the Control Plane to the Data Plane such as flow tables and configurations.
    - Protect data collected and distributed by the Control Plane to the Management Plane such as auditable events and traffic/packet statistics.
    - Protect data collected, distributed and shared within the Control Plane such as when multiple SDN controllers exist in the architecture.

Resources to be protected

- Any network-facing management interfaces, including traffic to and from the SDN Controller, and any critical data (e.g., audit data).
- SDN Controller software/firmware.
- Data stored locally by the SDN Controller (e.g. Policy, flow control, etc.).
- Configuration and reboot data, including any policy made part of the boot configuration.
- Authentication credentials such as keys and passwords.
- Northbound, Southbound and East/West channels/connections.
- Any stored updates intended for SDN Devices.
- SDN switch configuration and reboot data stored in the SDN Controller.
- Traffic/packet statistics.
- Audit information.

Attacker access

- An attacker can send arbitrary packets to network interfaces.
- An attacker can intercept and arbitrarily modify or drop packets within existing traffic flows.
- An attacker can impersonate the role of the SDN controller in the network. An attacker can impersonate the role of another SDN controller in the network.
- An attacker can leverage the lack of an established standard for communication between the SDN Controller and other components in an SDN network and so taking advantage of interoperability or under-tested protocols
- An attacker can leverage any automation functionality to cause the most damage before being discovered.
- An attacker can intercept and arbitrarily affect communications between an SDN Controller and any northbound applications and/or components.
- An attacker can intercept and arbitrarily affect communications between SDN Controllers, east/west communication.

- An attacker can intercept and arbitrarily affect communications between the SDN Controller and any switches under its control, southbound communication.

Evaluation Boundary

- In the case of a physical standalone SDN Controller device, the hardware, firmware and software of the device define the evaluation boundary.
- In the case of a Virtual SDN Controller, the software of the Virtual Machine (VM) defines the evaluation boundary.
- All of the security functionality is contained and executed within the evaluation boundary of the SDN Controller.

Essential Security Requirements

The following are the essential security requirements that are expected to be implemented by an SDN Controller. Note that these security requirements are conditional on that functionality being present. For example, an SDN Controller that does not include any management functionality is considered to satisfy any security requirements that pertain to the secure use of management features.

Any other conditional requirements that depend on whether or not the product implements a certain capability are listed in the “Optional Extensions” section below.

- The remote administration and audit functions shall use cryptography to protect communications.
- All communications with other SDN components shall be protected and authenticated.
- The SDN Controller shall be capable of auditing administrative actions, including any configuration changes and rebooting of the SDN Controller.
- The SDN Controller shall provide an authentication mechanism for local and remote administrators, as well as the device/VM itself (e.g., the device/VM maintains an authentication credential that can be used to authenticate it to an administrator’s client) .
- The SDN Controller shall provide a cryptographic means to validate the source of updates to be installed on the device/VM.
- The SDN Controller shall require any default passwords / other credentials to be changed upon installation.
- The SDN Controller shall protect keys, key material, and authentication credentials from unauthorized disclosure.
- The SDN Controller shall be robust against malformed network packets, and denial-of-service attacks.
- The SDN Controller shall provide self-tests to ensure the security functions it implements are operating correctly.
- Updates to the SDN Controller shall be authenticated.
- The SDN Controller shall provide a moving target defense mechanism (MTD) that protects the network from attacks by using dynamic network configuration.

Assumptions

- The SDN Controller relies on a trustworthy computing platform for its execution and it is assumed that the platform has not been compromised prior to the installation of the SDN Controller. For example, the effectiveness of non-interference and strict information flow control of an SDN controller will typically depend on the effectiveness of an underlying (embedded) operating system or hypervisor to provide non-interference and controlled information flow.
- The administrator of the underlying platform or SDN Controller is not careless, willfully negligent or hostile, and administers the software within compliance of the approved enterprise security policy.
- Physical security appropriate to the value of the SDN Controller and the data it contains is provided. An SDN Controller is protected from physical attacks by the wider environment.

Optional Extensions

The following requirements may already be realized in some products in this technology class, but the ESR is not mandating these capabilities exist in “baseline” level product:

- Automatic response to certain security events.
- Validation of patches and updates intended for data plane SDN Devices - as an add-on to any validation performed in the switch and not as an alternative.

Objective Requirements

Requirements specified here specify security-relevant behavior that is not expected to be realized currently in SDN Controllers, but capabilities that may be mandated in future versions of the ESR and resulting cPPs.

- The device shall have internal security features to make the device more resilient to security breaches.
- The device shall provide two-factor authentication natively on the device (i.e., does not rely on a separate device to provide this capability).

Outside the TOE's Scope

- Specific security functionality that is not global to all SDN Controllers (e.g. firewall, load balancers) as these will be specified in other ESRs.
- Examination of data plane content (including Virus scanning and email scanning).
- Intrusion detection/prevention capabilities.
- Network Address Translation (NAT) as a security function.
- The hardware or firmware of the underlying platform (virtualized SDN Controller only).
- The host operating system or runtime environment (virtualized SDN Controller only).
- The TOE shall not address other objects belonging in the Data Plane, even if they are delivered as part of the product installation process.