FCC TAC Cybersecurity Working Group
Securing SDN NFV Sub-Working Group

Security BCP Recommendations for SDN/NFV

December 2016

Table of Contents

Executive Summary

Background

Last year's WP on SDN / NFV Security *(Ref. a)* described, in broad terms, challenges (Security for SDN), opportunities (SDN for Security) and ongoing work carried out by various participants of the industry eco system (e.g. SPs, Operators, Vendors, SDOs and Open Communities). The WP identified several SDN/NFV-related use cases and recommended to develop BCPs (Best Common Practices) for dominant use cases.

FCC Ask

This year, FCC asked WG to identify existing BCPs and develop BCPs to close the gap for securing programmable networks. It also asked for recommendations on lifecycle management process for the BCPs (keeping them current, promote adoption by the industry and assessing their effectiveness).

Use Case

Since BCPs depend on the use case the SWG selected couple of dominant use cases to work on – SD_WAN (representing the Challenge side) and DDoS Mitigation (representing the Opportunity side). Since SD-WAN use case seems to have gained significant traction in the industry by offering solution to address the challenges faced by Enterprises the SWG focused on this use case. Even though SPs and Operators may provide managed SD-WAN services, the ultimate consumer of the service is Enterprise. So, the SWG focused on Enterprise SD-WAN and developed BCPs.

Challenges currently faced by Enterprises in managing their WANs in the light of the evolving dynamic environment (e.g. cost, complexity, bringing branches on board, applications moving to cloud) and business value offered by SD-WAN are described. A generic SD-WAN architecture is presented to provide the context.

Seventeen possible threats were identified for the use case *(Ref. b)*. Based on the consensus in the SWG the following top 5 threats were selected for BCP development. Detailed BCPs are specified for

I. Manipulation of Information
II. Software Firmware Exploits
III. Denial of Service
IV. API Exploitation

V. Unauthorized Activities

Methodology

The SWG based their recommendations on analysis of information from public information sources as well as industry experts. Detailed sessions with industry experts included Versa Networks, OPNFV, Dispersive Networks and VMWare. Additionally, Enterprise SD-WAN vendors, CloudGenix, VeloCloud and Viptela were also consulted.

Recommendations

The SWG recommends

i. FCC to ensure proactive and broad industry support for security as a designed in principle for software defined networks by leveraging industry bodies (CSRIC) and using the content and processes created and piloted by the TAC to promote and drive best common practices across industry architectures and deployments
ii. The work of the SWG be continued in 2017to develop BCPs for:
    Service Provider / Operator SD-WAN
    Other use cases (e.g. DDoS Mitigation)
iii. A pipeline approach leveraging the TAC to develop future additional BCPs and transitioning them to CSRIC for industry promotion and life cycle management

1. Purpose of This Document

To address FCC's questions, this WP identifies potential security threats associated with one of the dominant SDN/NFV-related use cases, Enterprise SD-WAN and specifies detailed BCPs for five high priority threats, out of a list of 17 potential threats. The WP also recommends entities which can sustain these BCPs, promote industry adoption and assess effectiveness.

2. FCC Ask's

1. Identify existing BCPs that focus on securing programmable networks, particularly those that are based on SDN/NFC network architectures
2. Develop BCPs that close the gaps identified.
3. What effective mechanisms should be employed to keep these BCPs current, and relevant to the industry?
4. How should the FCC and the industry, together, promote adoption of these BCPs?
5. How should the FCC and the industry, together, assess the effectiveness of these BCPs?

3. General SDN / NFV Security Challenges and Opportunities

3.1. Opportunities for Better Security Controls from SDN

Introduction: In establishing and evolving BCPs for SD-WAN, the FCC should endeavor to preserve the ability to use the agility properties of Software Defined Networking and the dynamic isolation properties of Virtualized Networks for more efficient, more effective and simpler security.
The use of SDN/NFVs gives rise to new and unique ways to secure systems. Steps are also needed to secure the SDN/NFV components themselves. This document focuses on the latter and selects a common use case for SDN/NFVs and best ways to handle the top threats associated with this use case. Constraints and advantages of some commonly adopted security techniques are enumerated below prior to discussing BCPs.

Potential Issues: Adoption of "full stack lockdown" trust anchor approaches, like TPM/Secure Element hash extension, as an attestation mechanism for stack integrity, create brittle control measurements.

If any layer/component of a measured stack changes (e.g. updates, migration, load balancing, …) the hash extension used for attestation becomes invalid, and must be recomputed and updated to all policy enforcement points. In datacenters with limited workload dynamics, this is not much of a problem. However, as dynamics becomes a normal part of network operation, Hash Extension based attestation must be reconsidered as a primary root of trust strategy, in favor of more dynamic alternatives.
This approach prevents resilient reconfiguration, in response to emergent anomalies. As a result, any extant exploitable vulnerabilities persist much longer than is necessary.
TPMs are still useful for providing tamper resistant unique asset identity, simple secret storage, protecting attestable metadata (geolocation, ownership, classification, etc.). Hash extension may still be useful in establishing provenance and supply chain control for appliance hardware, firmware, operating system and management software. This is generally how TPMs are used by modern cloud operators.

Complete isolation of solution components can obscure protective and investigative context, unnecessarily complicating security policy management, incident response and investigative efforts.

If the topological relationship between security controls is not always current, accurate and accessible, then incidents will drive security operations into wasteful "re-discovery" of the context of alerts and logs at the worst possible time.

For security controls to "work together" as a system for protection purposes, it is often necessary for the policy expressed in one control, to refer to the state detected by another control.

Example: An OWASP rule in a Web Application Firewall, intended to detect Cross Site Scripting of a management application, can be expensive to evaluate. If an attack is detected, it is therefore useful to allow the policy expressed in an upstream firewall to block the attacking IP Address, to avoid overloading the WAF capacity. Both the relative topology and the detection state need to be communicated between controls for this kind of capability to be automated.

Potential Opportunities: Aggressive isolation of SD-WAN solution layers and components will allow segmentation ("compartmentalization") of the SD-WAN solution, resulting in many security benefits:
Infection of one component, doesn't compromise the entire SD-WAN infrastructure.
Protection (e.g. firewall) can be placed on each compartment boundary *(Ref. c*).
Protection mechanisms can have the simplest possible policy (protection rules), that protects access to only the isolated component.
The protection granularity is nearly ideal, allowing a very tight default deny posture (minimum attack surface).

The visibility of these controls on granular internal isolation boundaries, provide visibility, actionability and context for addressing emergent (unknown) anomalies.
The dynamics enable by network virtualization and software defined topology can provide resilient protection.

Proactive component re-provisioning: This enables proactive re-provisioning (e.g. moving target defense) to prevent "low and slow" infections, hoping to avoid detection. Example: Cluster members may be proactively and regularly re-provisioned from trusted sources, eliminating any latent infections, and forcing persistent attackers to move much more quickly, making them much more detectable.

Dynamic Isolation: Anomalous components can be dynamically routed to investigative capability (e.g. on demand honeypot) allowing both protection of the infrastructure and robust forensic capture and investigation.
Transparent Resilience: When anomalies are detected, alternative infrastructure can be established, and normal workloads shifted, on demand, without affecting overlying configuration.

Conclusion/Transition: In short, establishing BCPs for SD-WAN solutions should not result in, preventing the use of the underlying SD-features for better security. Instead, the BCPs should establish the protection objectives against defined threats, identifying current best and common practice, while preserving the opportunity for transformative improvement in the effectiveness, efficiency and complexity of security operations

4. Use Cases Addressed in this Document

The term SDN/NFV has evolved from something that was rather well defined initially ala separation of control/data plane and moving traditional appliance based functions to cots x86 servers, to a bit of a catch all phrase the next generation of network, cloud and mobile technologies that incorporate some of the original aspects of the term SDN/NFV. As such the first order of business at the beginning of the year was to prioritize and agree on specific use cases that would be covered in the final deliverable for December 2016.

Provided for informational purposes, the list below was the first list of use cases put together by the collective SWG team before any priority or discussion. It was obvious that we would not be able to cover and do justice to the entire list so we quickly shortlisted to **SD WAN** and **DDoS Mitigation with SDN**, the latter being an interesting idea whereby SDN could potentially be used to thwart **DDoS** attacks. The team initially started work on SD WAN and quickly realized there was a great deal of work in that use case alone. Given the size of the team and part time nature of the work it was decided that the focus of this document would be limited to just SD WAN. In the Future Recommend Work section of the document it is recommended that this SWG's charter continue in 2017 to cover other use cases.

5G	**SDN/NFV & IoT**
Network Slicing in context of 5G	**Micro-Segmentation**
Software implementation of "packet cores"	**Routing**
	IMS
SD WAN	
Service function chaining	
Virtualized appliance & cloud "networking"	
Security implications of virtual CPE's	
Central controller programming the network (+ API Security)	
DDoS Mitigation with SDN	
API Security	
Secure the intf to the ctrl plane and the ctrl plane itself	

5. SD WAN Architecture

5.1. Enterprise Network Challenges

Enterprises have traditionally relied upon setting up their own private network or using Service Provider VPNs to get the needed connectivity, performance and security. Branches had always presented challenges to be brought on board and managed. As the business grows and evolves Enterprises may find growing their VPN bandwidth may not be the most optimum option. Efficiently managing WAN costs is another key challenge. With public internet speeds and reliability improving over the years it is becoming a cost-efficient alternative for internet, public-cloud type of traffic. Enterprises may be able to tolerate non time-critical applications using less expensive WAN but still get the best performance using MPLS for predictable QOS for real-time and strategic corporate application, such as VOIP, and for tighter security control. As applications move from in-house to cloud and from client – server to SaaS managing this dynamic environment may present considerable challenges to the Enterprise with the static nature of the current WAN. When appliances from different vendors are involved management becomes complex. Changing this static framework to adapt to evolving business environment (e.g. applications moving to cloud) becomes difficult due to lead times for bandwidth change requests and configuration changes.

5.2. Business Value of SD-WAN

SD-WAN approach aims to address these issues by leveraging the NFV / SDN technologies. It provides a logical single access and secure overlay over a collection of underlying different technologies (e.g. Broadband, VPN, Wireless) and dynamically steering application traffic to the optimum WAN facility (e.g. email traffic on broadband while VOIP on MPLS). Bringing up new branches and managing the network are eased by automation from a logically central control function (e.g. Enterprise defining full mesh, partial mesh or hub and spoke WAN topology, local or centralized internet breakout). Increased network-wide visibility to performance makes the network / service management easier and helps in security and compliance. Branch-specific policies can be applied. The agility and flexibility provided by SD-WAN equips Enterprises to be able to adjust to changes quickly. The capability to provide service insertion and chaining through Virtual Network Functions (VNF) makes SD-WAN very attractive to Enterprises.

5.3. Architecture

SD-WAN generally includes the following functions (physical / virtual instantiation may group together some of the following):

- Secure Data Plane functions in the premise; there is a range of deployment models from x86 platform, appliances And appliances with virtualization capabilities
- Scalable and resilient configurations
- Connectivity controller function for managing control plane
- Management functions (e.g. application / branch/ network policies and templates)
- Analytics
- Optional separate orchestration system using NBI (Northbound Interfaces) of the above
- User access function such as portal driving orchestration system
- Optionally, service functions insertion and chaining such as firewall; can be at the premise, at a regional DC / HO or in the central DC / cloud
- A generic Enterprise SD-WAN architecture is shown in **Figure 1**
- A common boot strap and zero touch provisioning process is highlighted in **Figure 2**

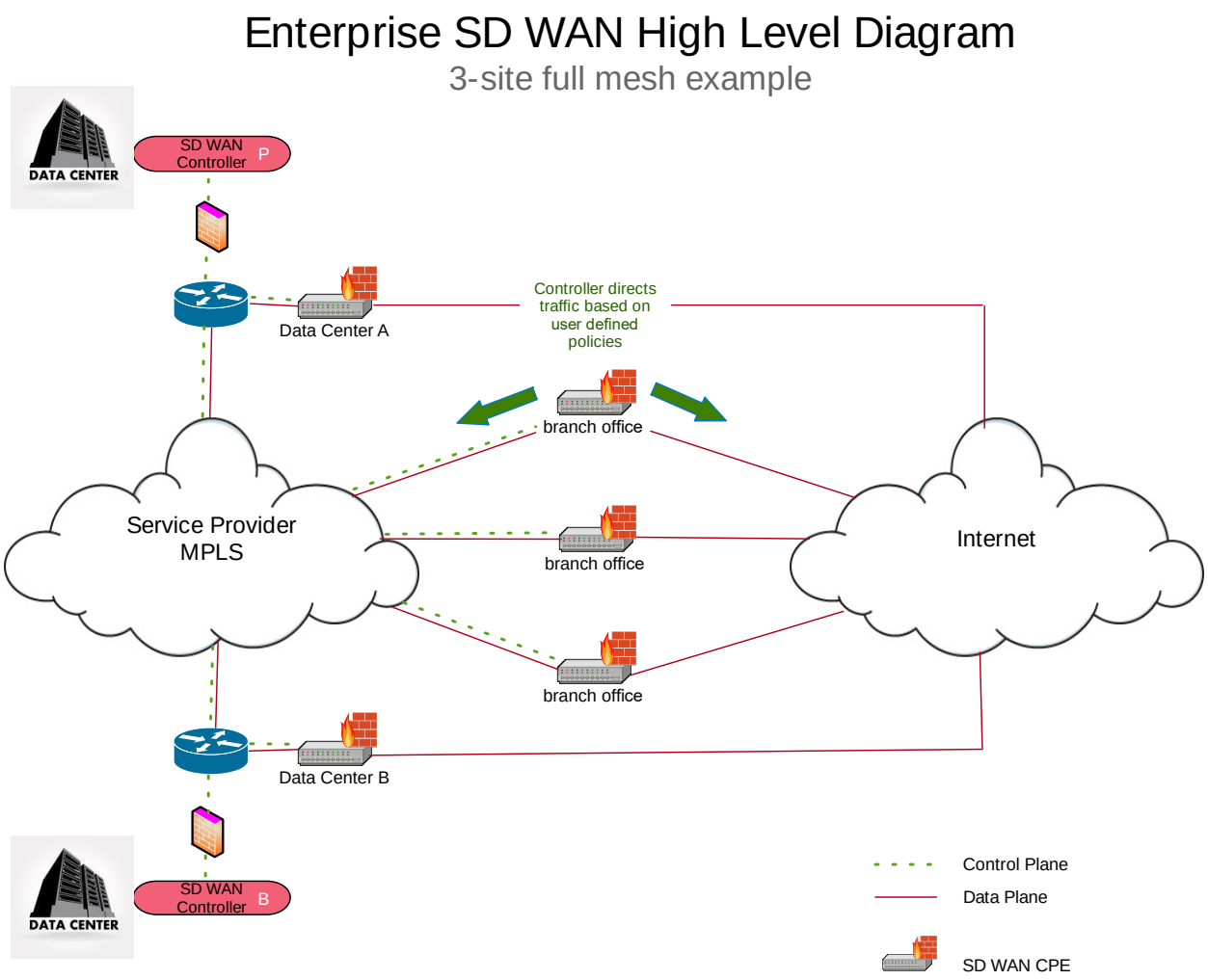


Figure 1: SD-WAN High Level Architecture

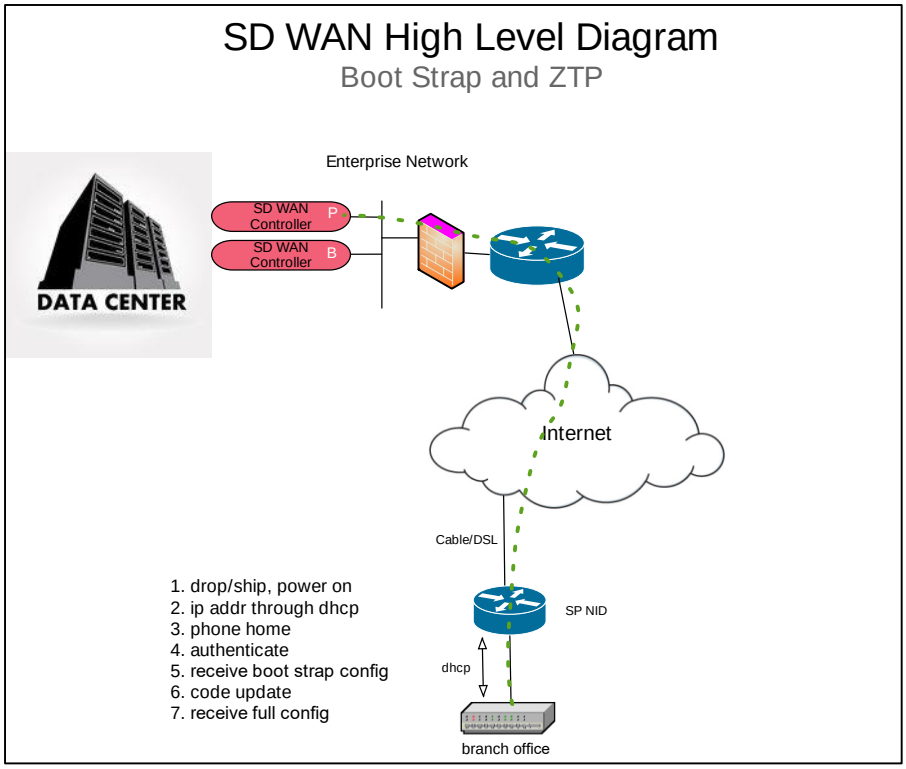


Figure 2: Bootstrap and Zero Touch Provisioning (ZTP) process for bringing up a branch

1. Drop/Ship, power on
2. IP Address through DHCP: The DHCP server can be provisioned to perform DHCP discovery in the network it is deployed on, during initial power on. This enables it to receive IP address and other network information such as DNS server from the local DHCP server.
3. Phone Home
4. Authenticate: The SDN element can be factory-provisioned with an X.509 certificate issued by a Certificate Authority trusted by other components in the SD-WAN network. The certificate chain and trust anchors can also be factory-provisioned. This facilitates the element to mutually authenticate with its home controller after power-on and proceed with the subsequent bootstrapping steps.
5. Receive Bootstrap Configuration
6. Code Update
7. Receive Full Configuration

6. Threats and BCP Recommendations

The threats considered in this section pertain to the SD-WAN use case; which is the focus of this document. Only the top five threats; selected based on likelihood of occurrence and severity of impact, are discussed herein. A comprehensive list of threats for this use case is listed in the Appendix.

6.1. Manipulation of Information

Description: The operation of the SD-WAN depends on routing, naming and configuration information, which consequently must be protected.

- Routing table information controls forwarding behavior.
- Name resolution information (e.g. DNS) determines resilient binding of endpoint names and expressive policy to specific source and destination addresses.
- Configuration information presented from lower level on-premise controllers to the higher level SD-WAN controller, shapes how the SD-WAN allocates resources and behaves operationally.

Threat: Since these information sources directly influence SD-WAN operation, compromise of these information sources could be used to extract valuable/sensitive information, to insert forged information and create SD-WAN denial of service.

Mitigations: Best and common practice mitigation Manipulation of Information is generally to ensure that participating nodes/services are legitimate and that the information they provide has not been manipulated. Furthermore, only authenticated and authorized nodes/services can update this information.

BCP 6.1.1 Authentication of All Network Nodes

Authenticating all network nodes prevents rogue devices from inserting themselves into the network and/or from contaminating or manipulating the network topological information on which the SD-WAN relies.

BCP 6.1.2 Establish Network Service Directory with ACLs

Establishing a network service directory, mitigates the risk of rogue network services contaminating the SD-WAN's association between names and addresses. ACLs or white lists

prevent rogue devices from manipulating the information in legitimate network services (e.g. poisoning attacks) consumed by the SD-WAN.

BCP 6.1.3 Enable encryption/integrity protection of south-bound interfaces

Enabling encryption and integrity protection of south bound interfaces, mitigates against rogue devices providing bogus information to the SD-WAN controller directly through south-bound interfaces.

BCP 6.1.4 Validation of flow table entries (detecting out of band change)

Flow table entry information should be checked for consistency and verified, before being consumed by the SD-WAN and used to inform its operations. This can involve periodic comparison of flow table information with authoritative sources, as well as, internal consistency and coherence checks on the flow table information itself.

BCP 6.1.5 Encryption of Persistent Information

SD-WAN sensitive information moved to persistent storage should be encrypted.

6.2. SD-WAN Software/Firmware Exploits

Description: The SD-WAN is a complex system of interacting software components whose function is segregated into control, data and application/policy layers.

Threat: The application layer (layer 7) is a primary vector for attempts to compromise SD-WAN integrity or that of its underlying OS. Exploitation can involve buffer overflows, kernel vulnerabilities, code injection, etc..

Mitigation: Because it is generally impossible to ensure that the SD-WAN OS or components are free of all potentially exploitable vulnerabilities, mutual isolation of SD-WAN functional layers, SD-WAN OS and of SD-WAN applications is a best and common practice.

BCP 6.2.1 Isolation between SD-WAN Layers

The SD-WAN solution should provide isolation between the functional layers. This isolation can be realized using process/name space isolation (operating system), virtualization based isolation (VMs), and physical isolation (hosts/firewalls)

BCP 6.2.2 SD-WAN Applications Isolated from the SD-WAN NOS

vCPE and SD-WAN management applications should be provisioned consistent with a least privilege. vCPE and SD-WAN management applications should be isolated from the SD-WAN NOS core by operating system, virtualization or physical isolation mechanisms

BCP 6.2.3 SD-WAN Exploit Detection and Prevention

Modern antivirus and antimalware techniques are challenged to deal with the large number and rapid evolution of malware attack vectors and payloads, making signature based protection of SD-WAN instances, of limited protective value. Where there is sensitivity to externally based attack vectors, targeted attacks and high levels of risk, these traditional protection techniques should be used in conjunction with more modern behavioral protection technologies, to protect the SD-WAN components.

BCP 6.2.4 TPMs, Secure Elements, UEFI Secure Boot – Roots of Trust

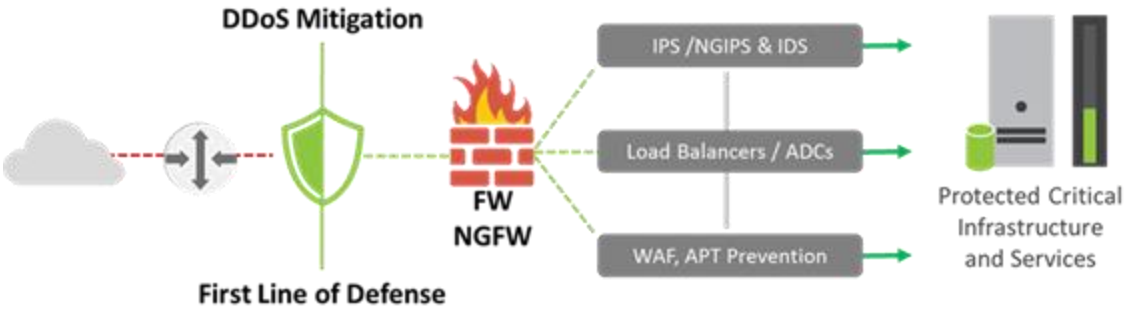
In order to detect and prevent unauthorized modification of underlying hardware, firmware, operating system and application/service images, secure measurement and attestation that the associated software and configuration have not changed, can be supported to varying extents by Trusted Processing Modules (TPMs), Secure Elements, UEFI Trusted Boot and other “Root of Trust” mechanisms. SD-WAN appliance configuration may allow a range of responses when measurement comparisons indicate that the underlying platform state or configuration has changed unexpectedly, including alert generation (detection), boot prevention (launch control) and re-provisioning from trusted sources.

Such capabilities are particularly effective in securing the “supply chain”, when SD-WAN appliance software is hosted on hardware that is acquired independently.

TPMs also generally can support “cryptographic sealing” of SD-WAN software to a particular hardware instance, preventing even an identical copy of SD-WAN software from being run on an untrusted, possibly remote, hardware instance in order to gain access to the SD-WAN by spoofing the software and configuration of an otherwise apparently authorized appliance instance.

Where there is sensitivity to supply chain interference, unauthorized underlying platform modification or appliance instance spoofing, Roots of Trust mechanisms should be configured and monitored, in order to prevent and/or detect such issues.

6.3. Denial of Service



Description:

A DDoS attack occurs when a large number of compromised systems attack a target, such as a website, and overwhelm it with activity that causes the target to become unresponsive and thereby denies legitimate users with access to the system. DDoS attacks are being used not only to disrupt services, but to distract security resources while other attacks are being attempted, e.g., fraudulent transactions. DDoS attacks can target Layer-3/Layer-4 or Layer-7 of the OSI stack. Types of DDoS attacks:

- Volumetric floods (TCP SYN, UDP, and HTTP floods)
- Reflective attacks (NTP, DNS, SSDP/UPnP, Chargen, SNMP); note that these are almost always amplified
- Resource exhaustion (Fragmented and malformed traffic, Low and slow requests)

In SD-WAN scenario, the datacenter or hybrid-cloud hosting the SD-WAN controller will be most prone to DDoS attack since the attackers typically don't target low-value enterprise branch site locations. If access to SD-WAN controller is disrupted, the SD-WAN gateway device will stop receiving policy updates. While this may prevent intelligent traffic routing/balancing across internet/MPLS links, it should not disrupt the overall WAN connectivity from the branch-office site.

Mitigation:

A DDoS mitigation solution must conduct inspections of control traffic (network and application headers), not DPI, determine whether there is a DDoS attack present or not, and instantaneously mitigate an attack at line rates of tens of Gbps. Additionally, it must only drop known “bad” traffic.

While the multi-tier architecture is preferred in high-bandwidth environments, for many customers, building multiple DDoS tiers may be overkill for their low-bandwidth environment. These customers are deploying a DDoS mitigation perimeter device that consolidates application delivery with network and web application firewall services.

BCP 6.3.1 DDoS Mitigation Appliance

By creating a baseline of expected traffic, they can detect and respond to a DDoS attack, scrubbing out false traffic and forwarding only what is left to services. However, since this approach still requires consuming limited internal resources such as bandwidth and processing power -- it’s typically not as scalable in handling the most devastating attacks as a cloud-based solution options.

BCP 6.3.2 Real-time Monitoring & Behavioral Analytics

Early detection and alerting system (Signature-based, Flow-based monitoring)

Understand the types and volumes of traffic on your network. Know where traffic comes in, where it goes out, what it is based on time of day and day of week. Monitor Hosts with a High Number of Failed Flows and/or New Flows, Unwelcome hosts, abnormal spikes in ignored Traffic Class.

Consider Managed security solution offerings from Service Providers or 3rd-party vendors

BCP 6.3.3 Cloud-Proxy for Traffic Scrubbing

This is done by passing network traffic addressed to the target through high-capacity network resources that scrub the data for any malicious characteristics.

BCP 6.3.4 Ensure proper configuration of Firewalls, IPS, DNS, NTP

Reflective and amplification attacks are still common, leveraging misconfigured DNS, NTP, and other network resources with the ability to spoof (forge) source (target) IP addresses

Implement appropriate blocking/shunning rules on the IDS/IPS and firewall

BCP 6.3.5 Internal/External Action Plan for DDoS attack

The average size of a DDoS attack was 7 Gbps in early 2015. Confirm that your infrastructure can still withstand rising attack volumes and new attack vectors as they escalate

If DDoS attack completely saturates an organization's bandwidth, rendering all other controls ineffective. In preparation for such an outcome, organizations need to establish contacts with their ISP. Outline clear communication processes for ISP intervention (block traffic via ACLs, issue new IP addresses, etc.). Make sure you understand the ISP SLAs for response and fix.

6.4. SD-WAN API Exploitation

Description: The SD-WAN solutions may expose key interfaces between the different constituent components. These interfaces may be grouped based on the topological orientation of the interfaces, as follows:

- The *East/West bound APIs* – This group of interfaces is implemented and consumed by the components of the SD-WAN facility and are used to facilitate communications between them.
- The *Southbound API* – This group of interfaces is implemented by the SD-WAN forwarding components in the SD-WAN facility to enable the communication between these forwarding components and underlying network controllers.
- The Northbound API – This group of interfaces is implemented by the certain SD-WAN components and is used to provide the communication between the SD-WAN components and overlying, network and policy management applications.

Threat: Since these APIs extend SD-WAN control interactions to external facilities and coordinate interaction between SD-WAN components themselves, a clear and present threat is that these APIs will be used or misused by unintended assets to extract sensitive information or insert forged information or to compromise the system.

Mitigations: Best and common practice mitigation of API use or misuse by unintended assets includes the following measures to ensure that only intended assets are allowed to

interact with SD-WAN exposed APIs, and only in authorized ways and to validate all user-supplied data.

BCP 6.4.1 Encryption

All API interaction must be encrypted. By requiring encrypted interaction, anchored to certificates at both ends of intended API interactions, rogue assets are prevented from operating and or offering spoofed bogus SD-WAN APIs. Further, encryption assures that modification and sniffing of API interactions is also mitigated.

By providing authoritative registered certificates at both API interaction endpoints (provider and consumer), man-in-the-middle exploitation of the API interactions is prevented.

Revocation list functionality should be fully implemented as part of the certificate management system used to support SD-WAN API protection.

TLS1.2 is recommended for use with certificates. Also, the TLS implementation should be properly configured following guidelines such as RFC 7525 and NIST SP 800-52r1 and be up-to-date with regards to latest patches.

BCP 6.4.2 Authorization

In addition to requiring registered certificates and encryption, both role based access or attribute based control (RBAC/ABAC) and access control lists (ACL) can provide finer grained authorization that limit which assets and/or processes have access to which APIs and the specific operations that are allowed within the APIs. This can be used establish a “default deny” posture for APIs, wherein assess or processes are allowed access only to the APIs they need to function and no others. Further, such explicit and authoritative authorization policy is useful to security analytics capabilities in helping to clarify if API interactions are “normal” or “anomalous”, and may also be used in scrubbing traffic (see BCP 6.4.4 DoS Protection below)
Use of OAuth tokens containing some or all the attributes required for authorization is also recommended.

BCP 6.4.3 Distributed Firewalls

Evaluating certificates and resolving RBAC policy can be expensive operations. To limit how heavily these computational facilities are loaded, it is often useful to provide firewall functionality at the boundary of SD-WAN component’s north bound, south bound and distributed east/west interfaces, with policies intended to allow only intended assets (VMs,

hosts, services, …) to interact with the protected APIs, and only over allowed protocols. Firewall policy enforcement is extremely efficient and use of distributed firewalls in SD* infrastructures, to efficiently protect constituent components, is an emerging and compelling practice. <ref NIST virtual protection documents>

BCP 6.4.4 DoS Protection

Another abuse of exposed SD-WAN APIs is congestion based Denial of Service (DoS). DoS protection is a common practice for external facing APIs (e.g. internet facing APIs) and would also be appropriate for internally facing APIs, where the potential for rogue assets may exist. Such protection should recognize both volumetric and resource exhaustion DoS behavior and should be sized with enough throttling and analytic capacity to assure that anomalous traffic volumes can be cleaned to allow resilient authorized API interaction to continue despite congestion.

BCP 6.4.5 Parameter and Schema Validation

All parameters within the URL, header and body of the SD-WAN APIs should be properly validated to prevent against injection attacks (e.g. SQL, NoSQL, JSON, etc.). Further, strict JSON or XML schema validation is also recommended to prevent unknown parameters from being exposed to SD-WAN elements.

BCP 6.4.6 White-hat Testing

White-hat testing is also recommended. This helps uncover hidden vulnerabilities and flaws that are not necessarily detected by standard test cases.

6.5. Unauthorized Activities

Description – Unauthorized activities include unauthorized use of APIs and operations, unauthorized access of SD-WAN resources such as binaries and configuration files. The mitigation of unauthorized use of APIs is covered under the previous threat. This section looks into unauthorized access to SD-WAN components and software /firmware resources on these physical elements.

Threat – Unauthorized login to SD-WAN physical resources, unauthorized access to SD_WAN configuration files or binaries.

Mitigations – Best and common practice mitigation of access to hardware and software or firmware resources is to have strong authentication and authorization techniques in place.

BCP 6.5.1 Authentication to Physical SD-WAN Resources

Only restricted administrators should be allowed SSH or other means of login access to servers or VMs that harbor SD-WAN components. Even SSH access should be minimized unless absolutely necessary. Multi-factor authentication of administrator access to physical resources is also recommended.

BCP 6.5.2 Authorization to Software/Firmware on SD-WAN Resources

OS-level ACLs and/ or hardened OS are best common practices to restrict access to specific software/firmware resources on the server/VM executing the SD-WAN functionality.

BCP 6.5.3 Host-based Security

Host-based security techniques such as intrusion detection or prevention systems and firewalls are also recommended to prevent unauthorized users and clients from gaining unauthorized access to the physical resources of the SD-WAN system

7. BCP Lifecycle Management Recommendations & Future Recommended Work

- Recommendation
  - The TAC recommends that the FCC ensure proactive and broad industry support for security as a designed in principle for software defined networks by leveraging industry bodies (CSRIC) and using the content and processes created and piloted by the TAC to promote and drive best common practices across industry architectures and deployments.
- Background
  - The rapid adoption and application of software defined networks (SDNs) and network functional virtualization (NFV) poses a new and diverse set of cybersecurity considerations. As a follow up to the 2015 TAC recommendations* the FCC requested that the SDN Subcommittee develop best common practices (BCPs) for SDNs and recommend ways to promote and sustain industry initiative around those BCPs.

  - The SDN Subcommittee evaluated a set of SDN applications and created and published a series of best common practice recommendations for SDN with initial focus on SD-WAN. The subcommittee will submit the SD-WAN BCP to CSRIC along with the prioritized list of other SDN applications and deployment architectures as input to future BCP development.
  - The subcommittee recommends that the FCC use CSRIC to promote BCPs across industry
- Additional recommendation
  - The work of the SWG be continued in 2017to develop BCPs for:

    Service Provider / Operator SD-WAN

    Other use cases (e.g. DDoS Mitigation)

  - The subcommittee recommends a pipeline approach leveraging the TAC to develop future additional BCPs and transitioning them to CSRIC for industry promotion and life cycle management

8. Industry Practitioners Consulted

Versa Networks - Sunil Ravi
OPNFV - Luke Hinds, chair of security working group
Dispersive Technologies - Bob Twitchell
CloudGenix - 2665 North First St., #110, San Jose, CA http://www.cloudgenix.com/
Viptela - 1732 North First St, Suite 600, San Jose, CA http://viptela.com/
VeloCloud - 295 N. Bernardo Ave, Ste 200, Mountain View, CA http://www.velocloud.com/
VMWare

9. References & Acknowledgements

a. Queen's University Belfast - "A Survey of Security in Software Defined Networks", Scott-Hayward, S., Natarajan, S., & Sezer, S. (2016)
b. ENSIA (European Union Agency For Network And Information Security) "Threat Landscape and Good Practice Guide for Software Defined Networks/5G – December 2015" https://www.enisa.europa.eu/publications/sdn-threat-landscape
c. IDC Technology Assessment – "Cloud and Drive for WAN Efficiencies Power Move to SD-WAN", Brad Casemore, Rohit Mehra, Nav Chander
d. Gartner Research – "Technology Overview for SD-WAN", July 2015, Andrew Lerner, Neil Rickard

e. https://transition.fcc.gov/bureaus/oet/tac/tacdocs/reports/2016/Securing%20-SDN-NFV%20-SWG-WP-Final.pdf
f. NIST SP 800-125B - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-125B.pdf

10. Appendix

List of Threats Compiled for the SD-WAN use case

The table below enumerates the list of threats compiled for the SD-WAN use case. Of these, the first five threats are the ones for which BCPs have been provided in this document.
As mentioned earlier, the top 5 threats were selected based on probability of occurrence and the severity of impact.

Threat #	Threat
1	Manipulation of information
2	SD-WAN Software/Firmware Exploits
3	Denial of Service
4	SD-WAN API Exploitation
5	Unauthorized Activities
6	Malicious Software
7	Remote SD-WAN Application Exploitation
8	Network Virtualization Bypass
9	Traffic Diversion
10	Side Channel Attacks
11	Identity Spoofing
12	Software/Firmware Exploits
13	Memory Scraping
14	Virtualization Threats (Network Virtualization Bypass)
15	Traffic Sniffing
16	MITM
17	Information Interception

11. Abbreviations and Acronyms

ACL	**Access Control List**
API	**Applications Programming Interface**
BCP	**Best Common Practice**
CPE	**Customer Premise Equipment**
DDOS	**Distributed Denial of Service**
DMZ	De Militarized Zone
DNS	**Domain Name System**
FCC	**Federal Communications Commission**
HTTP	**Hyper-Text Transfer Protocol**
IP	**Internet Protocol**
IPS	**Intrusion Protection System**
MPLS	**Multi-Protocol Label Switching**
NFV	**Network Functions Virtualization**
NTP	**Network Time Protocol**
OS	**Operating System**
OWASP	**Open Web Application Security Project**
QoS	**Quality of Service**
RBAC	**Role Based Access Control**
ROT	**Root of Trust**
SDN	**Software Defined Networking**
SD-WAN	**Software Defined Wide Area Network**
SLA	**Service Level Assurance**
SNMP	**Simple Network Management Protocol**
SWG	**Sub Working Group**
SYN	**Synchronization Packet**
TAC	**Technological Advisory Council**
TCP	**Transmission Control Protocol**
TPM	**Trusted Platform Module**
UEFI	**Unified Extensible Firmware Interface**
vCPE	**virtual Customer Premise Equipment**
VNF	**Virtual Network Function**

VoIP	**Voice over Internet Protocol**
VPN	**Virtual Private Network**
WAN	**Wide Area Network**
WP	**White Paper**