Cambium Networks™

SOLUTION GUIDE

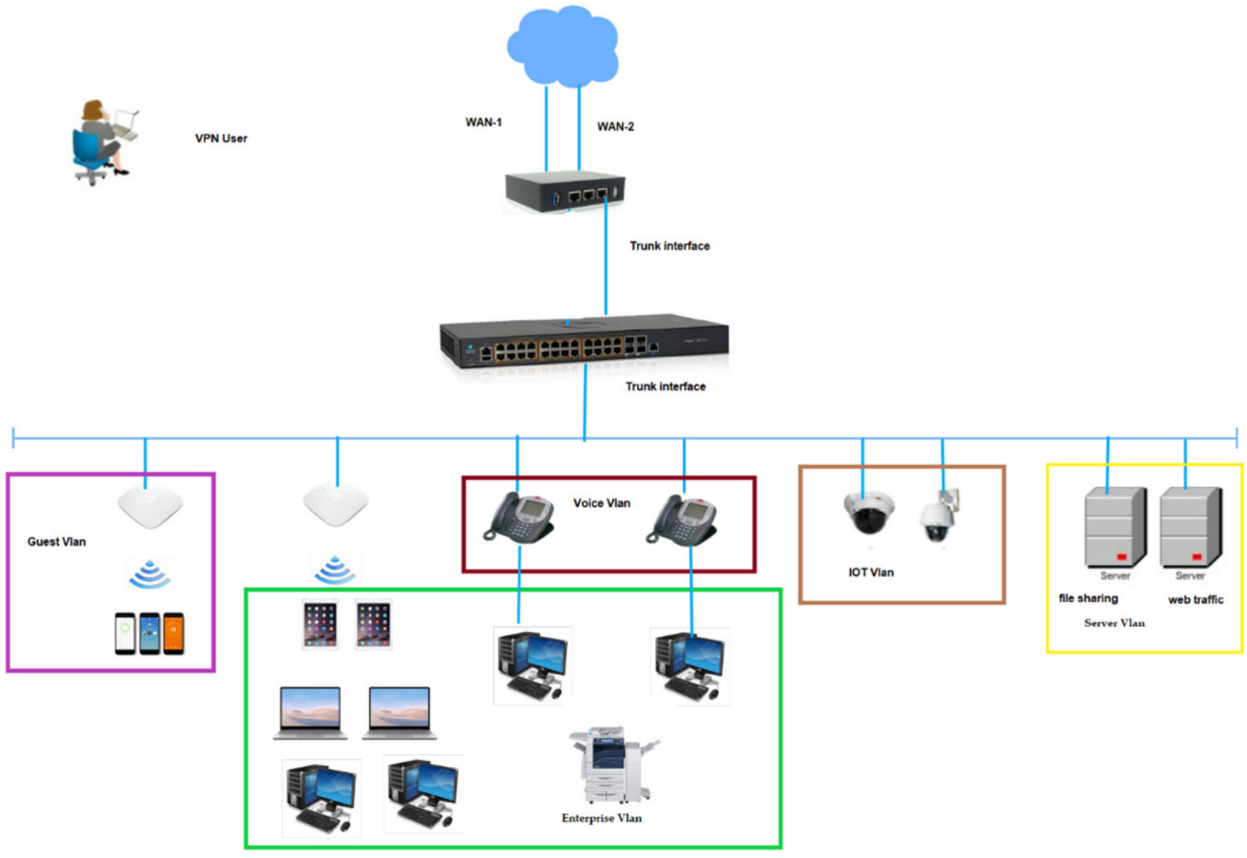
NSE 3000 1.1 Solution Guide

1. Overview

This document describes Cambium Networks' SD-WAN and network security solution for Small and Medium Business (SMB) and small and medium enterprises (SME). An SMB/SME deployment consists of:

- WAN edge connectivity with SD-WAN
- Network security and firewall
- Network services like DHCP, RADIUS and DNS
- PoE/PoE+ switches (1 to 3)
- Up to 10 enterprise Wi-Fi access points
- Applications hosted in the cloud and on-premises

2. Cambium Networks' Solution for SMB/SME



NSE delivers advanced security, routing, and SD-WAN policies for small and medium businesses (SMB) and small and medium enterprises (SME).

2000 Center Drive Suite A401, Hoffman Estates, Illinois 60192 USA

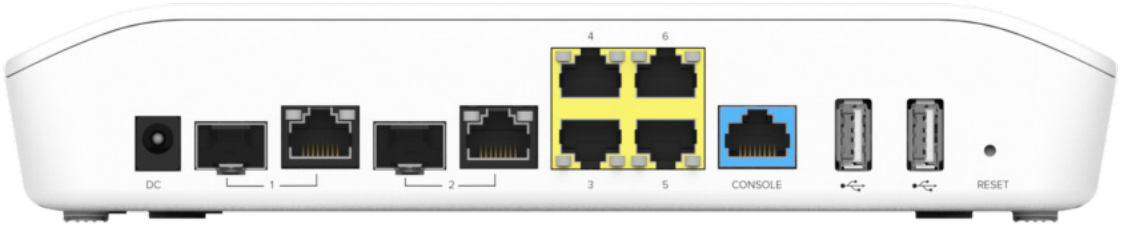
NSE is managed by the easy- to-use, secure and cloud-hosted Cambium Networks cnMaestro™ management system. cnMaestro is a single pane-of-glass management system to operate and manage all Cambium enterprise products.

The SMB/SME solution consists of NSE device(s), cnMatrix™ switches (PoE/PoE+) and access points. The solution provides:

- SD-WAN and Traffic Engineering – Load balance traffic and prioritize business-critical applications
- Security Services – Protects the network access from both the external and internal threats
- Network Services – DHCP, DNS and Radius servers
- Wireless Connectivity – Enable wireless users to connect to the network
- Remote Connectivity – Enable remote workers to log in to network securely from any device with the help of both site-to-site VPN and client VPN
- Analytics – Comprehensive overview and security analysis of all the devices on the network via cloud management platform

3. Introduction to NSE 3000

NSE 3000 is a gigabit device that has 4 LAN ports, 2 WAN ports and 2 USB ports and offers reliable connectivity with WAN throughputs of up to 1 Gbps. It boasts an industry-leading IDS/IPS engine, advanced application and geo-IP firewalls, SD-WAN and cutting-edge application visibility, and control LAN vulnerability assessment and IoT fingerprinting.



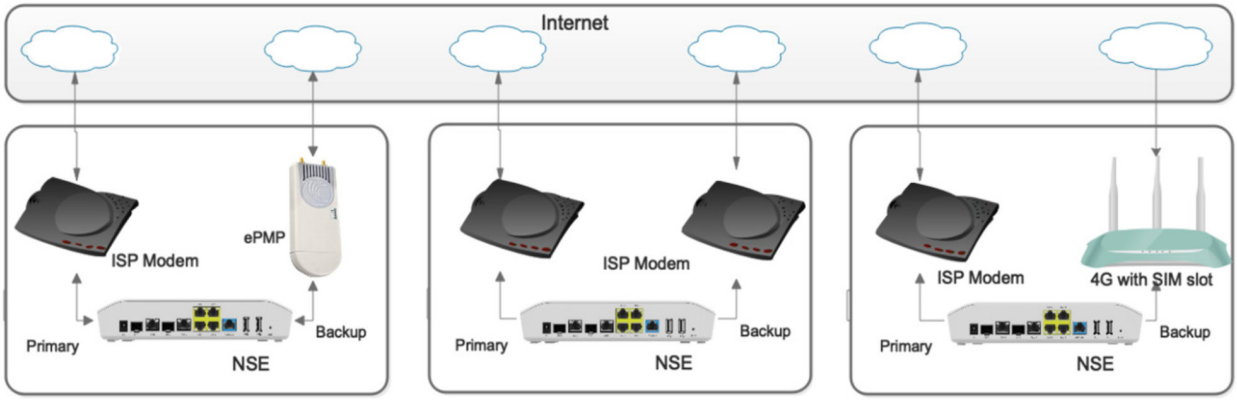
NSE 3000 solution can broadly classified into 3 main pillars:

- SD-WAN
- Security
- Network Services

3.1 SD-WAN

NSE 3000 has two WAN links. The links can be configured either in active-active or in active-backup fashion. NSE can prioritize business critical applications and allows users to reserve bandwidth using the WAN Traffic Shaping feature for time-sensitive voice applications. Specific Layer 3/ Layer 7 traffic can be linked to one WAN interface with the help of flow preference mechanism.

2000 Center Drive Suite A401, Hoffman Estates, Illinois 60192 USA



3.1.1 WAN Connectivity

WAN links offer throughput of up to 1 Gbps. NSE 3000 offers 3 modes of WAN IP assignment: Static, Dynamic and PPPoE. WAN links can connect directly to ISP networks through ISP-supplied modems, through ePMP/PMP subscriber modules or through 4G/5G routers.

3.1.2 WAN Load-Balancing and Failover

WAN load balancing is a networking technique that distributes network traffic across multiple WAN connections to optimize performance, increase reliability, and utilize available bandwidth efficiently. It involves the allocation of network traffic across multiple links to prevent any single link from becoming overwhelmed and to ensure smooth and balanced traffic flow.

NSE 3000 helps in effective utilization of both the WAN links. When functioning in the shared mode, both the WAN links will be used based on the percentage specified on the WAN links. The amount of traffic that can be sent on a WAN link is controlled by the traffic share. WAN links with equal capacity can be configured to carry the same amount of traffic on the WAN links. Traffic share plays a major role when there are WAN links with different capacities. In this case, the WAN link with the higher capacity can be configured to carry a majority of the traffic.

When functioning in the backup mode, as soon as the active link goes down, the link that specified as backup will become active and forwards all the traffic. The state of the WAN links is identified with the help of monitor hosts.

Monitor hosts play an important role in the health check on WAN links. NSE 3000 constantly monitors the health of the configured monitor hosts. The device sends periodic health messages to the configured monitor hosts. The device declares the link as inactive if there is no response from the monitored host within the health check timeout interval. The device declares the link as active once it starts seeing the responses from the configured monitor host.

2000 Center Drive Suite A401, Hoffman Estates, Illinois 60192 USA

3.1.3 Flow Preference

Flow control mechanism helps to bind traffic with a specific WAN link. This can be configured to determine which uplink a specific flow should utilize. The identification of flows can be performed using either based on IP address or Application.

When load balancing is set up in active/active mode, user traffic can utilize either of the available WAN links.

By configuring flow preferences, you can override the load balancing decision and prioritize a particular flow over a specific wan Link.

As NSE 3000 has two WAN links and when operating in shared load-balancing mode, there may be chances of business-critical application taking a path of lower throughput link. With the help of flow control mechanism, one can bind the business-critical application to a higher throughput and more reliable WAN link. This helps in providing a reliable performance for business-critical application and effective utilization of both the WAN links.

3.1.4 Failover Policy

By using the WAN Failover policy, network administrators can prioritize important traffic during failover situations. The failover policy is applied only when there is one active link available for forwarding the traffic.

In cases where the link is expensive or has limited data usage, allowing unrestricted traffic might lead to significant costs. By implementing failover policy rules for outgoing traffic on a link, the network administrators can enforce restrictions and control the data consumption on the link.

3.1.5 Traffic Shaping

Traffic shaping is a technique used to allocate a specific bandwidth for business-critical applications or servers. This can be configured to use IP address/Subnet, category of application or specific application itself. So, when one uses that IP address/Subnet, category of application, the specified amount of bandwidth will be allocated.

3.2 Security

It boasts an industry-leading IDS/IPS engine, advanced application and geo-IP firewalls, cutting-edge application visibility, and control LAN vulnerability assessment and IoT fingerprinting.

3.2.1 Firewall

NSE 3000 helps to create policies to allow or block traffic based on IP/port/category/application. It also supports various types of Network address translation.

2000 Center Drive Suite A401, Hoffman Estates, Illinois 60192 USA

3.2.1.1 Port Forwarding

Port forwarding is a network configuration technique used to redirect incoming network traffic from one port of a network device to another destination port on a different device within the local network. It allows external users or devices to access specific services hosted on a device behind a router or firewall.

Port forwarding is used to forward traffic destined for the WAN IP of the NSE 3000 on a specific port to any IP address within a local subnet.

3.2.1.2 1:1 NAT

1:1 Network Address Translation is used to map an IP address on the WAN side of the NSE (other than the WAN IP of the NSE 3000 itself) to a local IP address on your network.

3.2.1.3 1:Many NAT

1:Many Network Address Translation is used to map an IP address on the WAN side of the NSE (other than the WAN IP of the NSE 3000 itself) to multiple local IP addresses on your network. 1:Many NAT is more flexible than 1:1 NAT since it allows you to specify one public IP that has multiple forwarding rules for different ports and LAN IPs.

3.2.2 IDS/IPS

NSE 3000 supports an industry-leading IDS/IPS engine. IDP/IPS engine uses a series of rules that help define a malicious network activity. IDP/IPS engine supports rules from Snort and Emerging threats. The solution supports both community and licensed rules. The IDP/IPS engine uses these rules to find packets that match against them and generates alerts for users. The IDP/IPS engine can operate in either detection or prevention mode.

3.2.2.1 Detection vs Prevention Mode

When functioning in detection mode, the threats will be detected and alerts will be generated. When functioning in prevention mode, it will not only detect and generates the alerts, but also prevents the threats.

3.2.2.2 Rule Categories

The IPS engine in NSE 3000 has multiple individual rules grouped into categories; the categories range from Malware to specific exploits.

3.2.2.3 Rule Sets

The IPS engine has three rule sets specifically curated to accommodate the needs of every network. Connectivity, balanced, and security are the different rule sets available. Connectivity has a smaller subset of IPS rules and hence results in better network throughput but at the cost of reduced network security. A balanced rule set provides a balance of network security and network throughput . The security rule set delivers the best network security protection. Note this is only applicable to Snort.

2000 Center Drive Suite A401, Hoffman Estates, Illinois 60192 USA

3.2.2.4 Rule Updates

The IPS rules are auto-updated every 24 hours by default. This enables the NSE 3000 to have the latest rules. The update interval can also be configured every 12 hours.

3.2.3 DNS-Based Content Filtering

This feature allows network administrators to control and manage access to specific websites or categories of websites based on their DNS domain names. It helps organizations to protect users from accessing malicious or inappropriate content.

NSE 3000 provides over 88 different predefined filtering categories such as adult content, social networking, streaming media, gambling, and more. Administrators can choose which categories they want to filter or block for their network. The DNS filtering implementation on NSE3000 complies with policies which are covered as part of CIPA Standards.

3.2.4 Application Visibility and Control

Application visibility and control refers to the ability to monitor, analyze, and manage the usage of applications within a network environment. It involves gaining insights into the applications being used, understanding their characteristics and behaviors, and implementing policies to control their usage.

With the increasing prevalence of cloud services, mobile applications, and sophisticated network threats, application visibility and control have become critical for organizations to ensure network security, optimize performance, and enforce usage policies.

Application visibility and control empower organizations to gain a deeper understanding of application usage within their networks. It allows for effective management of applications, optimization of network resources, mitigation of security risks, and enforcement of usage policies.

With the help of NSE 3000, one can allow or block application access in the network. It can be allowed/blocked with a category of application or can be allowed/blocked based on individual application. This can be enforced for the whole network or subnets or for a specific IP. Multiple policies can be created and enforced on different subnet or IP addresses based on the requirements.

3.2.5 Always-On LAN Vulnerability Scan

LAN vulnerability assessment is a systematic evaluation of potential security weaknesses and risks within a local network infrastructure. It aims to identify vulnerabilities that could be exploited by attackers to compromise the network, systems, or data. Performing regular vulnerability assessments is a crucial part of a comprehensive cybersecurity strategy to proactively address security risks and protect sensitive information.

NSE 3000 has an on-box LAN vulnerability scan feature that scans for vulnerable applications on every connected device in the network. Once this assessment is completed, a list of vulnerable applications is posted on cnMaestro to make the network administrator aware of the vulnerable applications along with the CVE ID to ensure the network administrator can patch the software.

3.2.6 IoT Fingerprinting

IoT (Internet of Things) visibility and security are critical aspects of managing and safeguarding IoT devices and networks. The increasing proliferation of IoT devices has brought significant benefits in various industries, but it has also introduced new security challenges due to the large attack surface and diverse nature of these devices.

IoT device visibility by fingerprinting and checking against the frequently updated device databases. It provides dynamic list of OT and IoT devices in the network. On the IoT device visibility one will be able to see hostname, IP address, MAC address, Manufacturer, Device Type and Device OS.

3.2.7 Geo-IP Filters

Geo-IP filters are security measures that use the geographical location of an IP address to control access to resources, services, or content. These filters allow organizations to enforce policies based on the geographical origin of users or devices, which can be helpful in various scenarios to enhance security, comply with regional regulations, or tailor content delivery.

With NSE 3000 Geo-Ip policies can be set up. Traffic can be allowed or blocked based on the geo location (country).

3.2.8 VPN with MFA

A Client VPN is a secure, encrypted connection that allows individual users or remote devices to connect to a private network, such as a corporate network or a home network, over the internet. Client VPNs provides a secure tunnel for data transmission, enabling users to access resources on the private network as if they were physically connected to it, regardless of their physical location.

NSE 3000 supports L2TP over IPSec and IPSec IKEv2 EAP client.

The Multi-Factor Authentication is a time-based, one-time password system unique to each user.

3.2.9 Site-to-Site VPN

A site-to-site VPN is a secure network connection that connects two or more geographically distant locations or sites over the internet or other untrusted networks. It allows multiple local networks, such as branch offices, data centers, or remote sites, to communicate with each other as if they were part of the same local network, enabling seamless and secure data transmission between the sites.

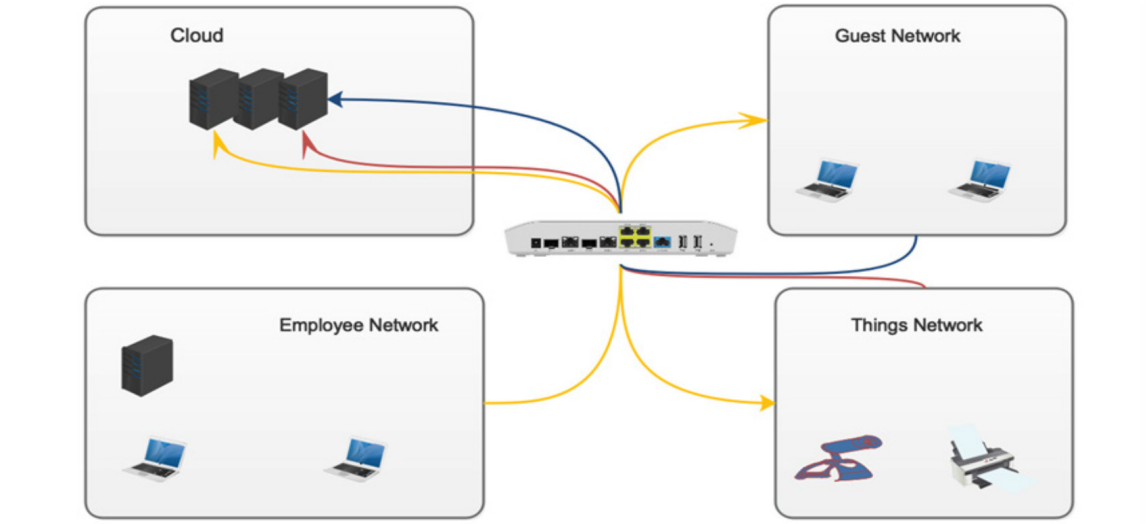
Site-to-Site VPNs are commonly used by organizations with multiple branch offices, remote locations, or data centers. They provide a secure and efficient way to connect and integrate remote sites into a unified network infrastructure.

NSE 3000 supports site-to-site VPN. It also supports Hub and spoke deployment as well as mesh deployment scenarios. NSE 3000 is interoperable with other vendor devices as well.

2000 Center Drive Suite A401, Hoffman Estates, Illinois 60192 USA

3.3 Network Services

NSE 3000 provides network connectivity and authentication services to users. The device provides secure connection to enterprise users and allows access of network to Guest users and Things. The device supports DHCP, DNS and RADIUS servers for network connectivity and authentication services.



With the help of Radius server on the NSE 3000, users can be authenticated who are connecting to wireless or connecting remotely over VPN. NSE 3000 can function as DHCP server as well as relay agent.

About Cambium Networks

Cambium Networks enables service providers, enterprises, industrial organizations, and governments to deliver exceptional digital experiences, and device connectivity, with compelling economics. Our ONE Network platform simplifies management of Cambium Networks' wired and wireless broadband and network edge technologies. Our customers can focus more resources on managing their business rather than the network. We make connectivity that just works.

2000 Center Drive Suite A401, Hoffman Estates, Illinois 60192 USA