NSE 3000 1.0 Solution Guide

1. Overview

THIS DOCUMENT DESCRIBES Cambium Networks' SD-WAN and network security solution for Small and Medium enterprises (SME). An 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

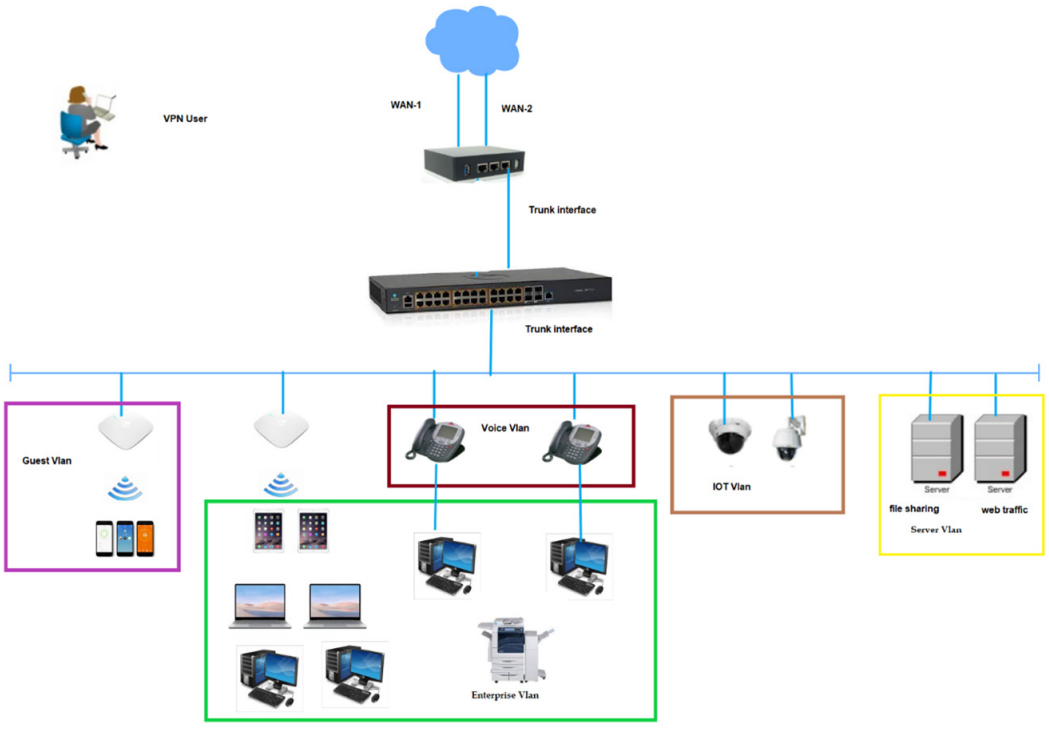
The Network Service Edge (NSE 3000) functions as the SD-WAN, security and network services delivery device. Cambium Networks also offers enterprise Wi-Fi access points and switches that work to provide wired and wireless LAN connectivity to the users.

2. Cambium Networks' Solution for SME

NSE delivers advanced security, routing and SD-WAN policies for small and medium businesses. Model NSE 3000 has two WAN ports and four LAN 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. It boasts an industry-leading IDS?IPS engine, advanced application and Geo-IP filters, SD-WAN, cutting edge application visibility and control, LAN vulnerability assessment and IoT fingerprinting

NSE 3000 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 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
- 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

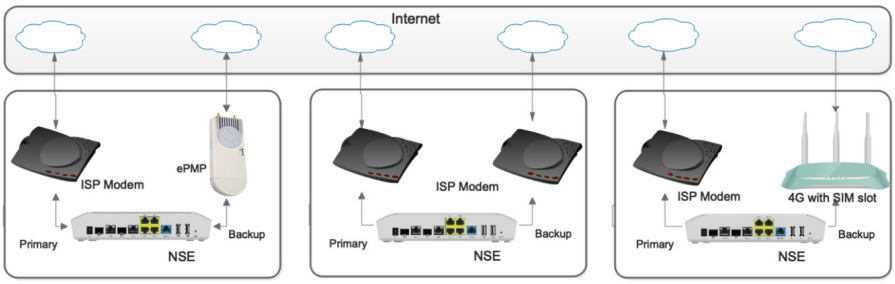
- Analytics – Comprehensive overview and security analysis of all the devices on the network via cloud management platform

2.1 SD-WAN and Traffic Engineering

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 binded to one particular WAN interface with the help of flow preference mechanism.

2.1.1 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.



2.1.2 WAN Load Balancing and Failover

WAN links in active-active mode share traffic on both the WAN links as per the configured traffic share percentage. The amount of traffic that can be transmitted on the WAN link depends on the WAN link capacity.

2.1.2.1 Significance of Traffic Share

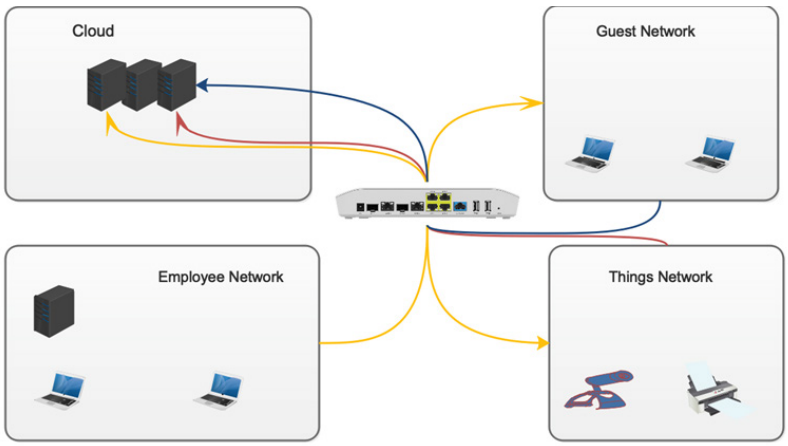
The amount of traffic that can be sent on a WAN link is controlled by the traffic share. WAN links with equal capacity can be configured to carry the same amount of traffic on the WAN links. Traffic share plays a major role when there are WAN links with different capacities. In this case, the WAN link with the higher capacity can be configured to carry a majority of the traffic. For example, a fiber link with 500 Mbps capacity and a cellular link with 50 Mbps capacity can be configured to share traffic in 91:9 ratio.

2.1.2.2 Significance 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.

2.2 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.



2.2.1 Networks

NSE 3000 allows the user to create networks and attach policies against them. Users can create networks for Employees, Guests and Things and attach policies to restrict traffic between these networks or rate limit traffic from a particular network.

For example:

- Allow traffic from Employee network to all other networks and Internet
- Allow Guests to access Things network and Internet
- Allow Things to access only Internet
- Rate limit traffic for all the devices in Things network

2.3 Security Services

NSE 3000 supports various security features.

2.3.1 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.

2.3.1.1 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 detects and generates the alerts, but also prevents the threats.

2.3.1.2 Rule Categories

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

2.3.1.3 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.

2.3.1.4 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.

2.3.2 LAN Vulnerability Assessment

NSE 3000 has an on-box LAN vulnerability assessment 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.

2.3.3 Application-Based Rules

NSE 3000 is application aware and has robust application visibility and control. It has a database of over 2,000 applications spanning across 15+ categories. This database is also constantly updated to include newer applications.

2.3.4 DNS-Based Content Filters

The DNS-based content filtering on the NSE 3000 has three categories: social media, adware and malware sites, and pornography sites. This list is periodically updated.

2.3.5 Geo-IP Filters

The GEO-IP filter supports the creation of policy rules that apply to specified countries. Inbound or outbound network traffic can be blocked or allowed by leveraging the Geo-IP filters.

2.4 Remote Access

VPN Server and Port forwarding are today's remote access solutions. Port forwarding requires opening a port in the firewall and thereby exposes the network to attacks. VPN provides secure remote access to applications. NSE 3000 supports site-to-site VPN, VPN with MFA and

Port forwarding.

2.4.1 VPN Server with MFA

NSE 3000 provides a remote VPN solution with a Multi-Factor Authentication system. The VPN server is L2TP based, and all client devices that can establish an L2TP VPN tunnel can connect to the NSE 3000. The Multi-Factor Authentication is a time-based, one-time password system unique to each user.

2.4.2 Site-to-Site VPN

NSE 3000 offers site-to-site VPN for connecting multiple networks/branches. This configuration expands a network across geographically separated office/branches or connects a group of offices to a data center.

2.4.3 Network Address Translation

NSE 3000 supports various types of Network Address Translation.

2.4.2.1 Port forwarding

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.

2.4.2.2 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.

2.4.2.3 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.

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 deliver connectivity that just works.

cambiumnetworks.com