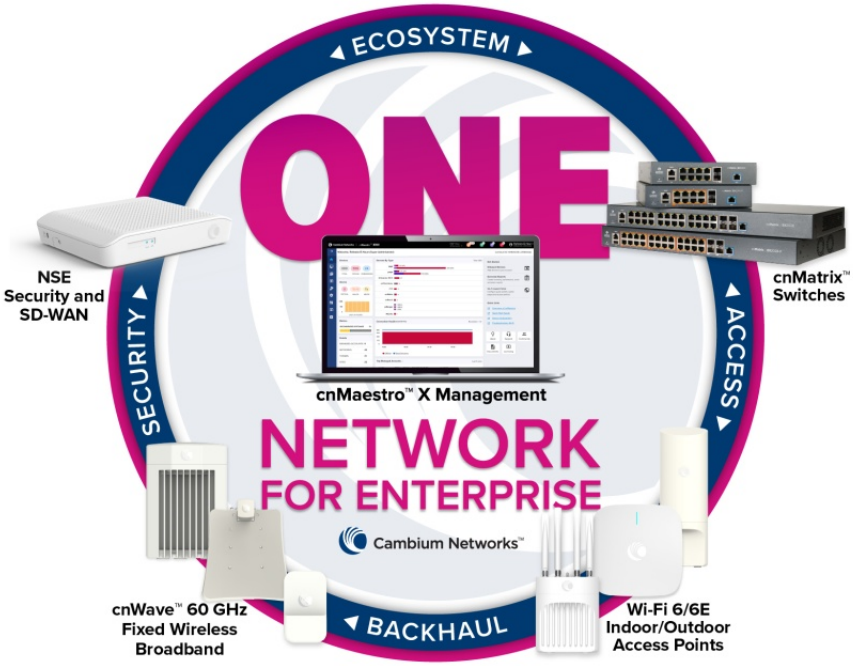
Zentral verwaltete Infrastruktur für Unternehmen aller Größen

Dr. Götz Güttich

Cambium Networks bietet eine Netzwerk-Infrastruktur für Unternehmen an, die sich über ein zentrales Web-Interface verwalten lässt. Zu den dazugehörigen Komponenten gehören unter anderem ein Firewall-Router sowie diverse Switches und Access Points. Wir haben die Lösung bei uns im Testlabor in Betrieb genommen und uns angesehen, wie die tägliche Arbeit damit abläuft.

Das Herzstück der Netzwerklösung von Cambium Networks ist die Management-Software "cnMaestro". Diese lässt sich sowohl in der Cloud als auch on-premises nutzen und ermöglicht die Verwaltung und Überwachung der im Netz aktiven Komponenten von einer zentralen Stelle aus. Darüber hinaus kommt sie auch zum Einsatz, um Geräte über eine Zero-Touch-Provisioning-Funktion (ZTP) automatisch mit einer Konfiguration zu versehen und so direkt in Betrieb zu nehmen.



Es stehen zwei unterschiedliche Versionen von cnMaestro zur Verfügung: "cnMaestro Essentials" ist kostenlos und bietet die Grundfunktionen an, die zum Netzwerkmanagement erforderlich sind. Dazu gehört unter anderem die Möglichkeit, Konfigurationen zu erstellen und automatisch auf den verbundenen Geräten einzuspielen.

Abgesehen davon bietet das System Überwachungsfunktionen für das ganze Netz (inklusive Backhaul- und Point-to-Multipoint-Richtfunk, und WiFi) und dedizierte Dashboards für jedes Gerät mit Konfigurations- und Upgrade-Optionen. Zusätzlich stellt es auch Karten, Tabellen und historische Daten für einzelne Devices oder Gerätegruppen bereit, damit die IT-Verantwortlichen einen umfassenden Überblick über die Vorkommnisse im Netz erhalten.

"cnMaestro X" verfügt über zusätzliche Verwaltungsoptionen, einen Rund-um-die-Uhr-Support sowie einen schnellen Zugriff auf Level-2-Engineers. Außerdem bietet cnMaestroX erweiterte Funktionen wie Mandantenfähigkeit, erweiterte Reports, offene API's und Applikationsvisibilität plus Kontrolle an. Für den Test stellte uns Cambium die cnMaestro-X-Variante zur Verfügung.

Die eingesetzte Hardware

Was die im Test verwendete Hardware angeht, so ist zunächst einmal der Firewall-Router "NSE 3000" (Network Service Edge) zu nennen. Dieses Produkt kann nicht nur Netzwerk- und Sicherheitsdienste bereitstellen, sondern integriert auch SD-WAN-Funktionalitäten.

Mit der Lösung wendet sich Cambium an kleine und mittelgroße Unternehmen. Was das SD-WAN angeht, unterstützt der NSE 3000 Routing, WAN-Load-Balancing und Failover, Bandbreitenkontrolle und WAN QoS (Quality of Service).

Bei den Netzwerkdiensten gehören DHCP und RADIUS zum Leistungsumfang. Im Sicherheitsbereich bietet die Appliance eine Firewall, IDS/IPS (Intrusion Detection/Intrusion Protection), VPNs, IoT Sicherheit und eine LAN-Sicherheitseinschätzung.

Letztere führt periodisch Scans der angeschlossenen Geräte durch, die Common Vulnerabilities and Exposures (CVEs) entdecken und gibt anschließend eine Bewertung und empfohlene Lösungsvorschläge aus. Das lief im Test übrigens problemlos ab. Wir banden ein Notebook unter einem nur teilweise aktualisierten Ubuntu-Linux 18.04.6 LTS in unsere Umgebung ein und kurz darauf erschienen im cnMaestro-Web-Interface Informationen über die CVEs, die für das genannte Gerät relevant waren.

Cambium verfolgt darüber hinaus mit der NSE 3000 das Ziel, blinde Flecken in der IoT-Sicherheit auszumerzen. Deswegen bietet die Lösung, neben der eben angesprochenen Vulnerability-Datenbank auch eine Datenbank an, die dabei hilft, IoT-Geräte im Netz zu identifizieren.

Im Test traten dabei ebenfalls keine Probleme auf und das System erkannte beispielsweise unsere Smarten Glühbirnen von Lifx und diverse Drucker ohne Schwierigkeiten. Es gab allerdings auch ein False Positive: die NSE 3000 vertrat die Meinung, dass ein Apple Notebook ein IoT-Device sei. Alle genannten Datenbanken werden im Betrieb über cnMaestro auf dem aktuellen Stand gehalten.

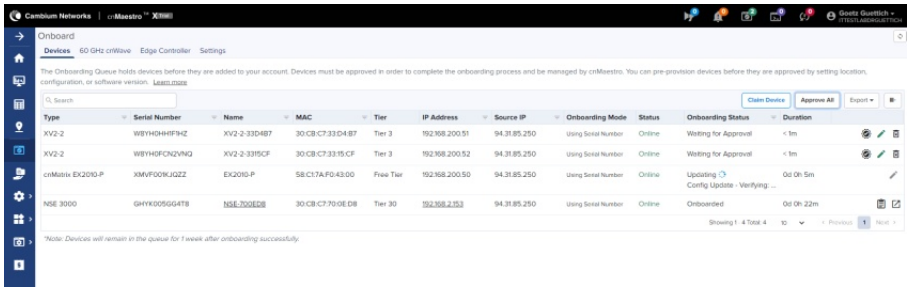
Als Switch stellte uns Cambium den “cnMatrix EX2010-P” zur Verfügung. Dieser verfügt über acht PoE-fähige Ethernet-Anschlüsse sowie zwei SFP-Uplink-Ports und erreicht einen Durchsatz von 20 Gbps. Er unterstützt die Autokonfiguration mit Hilfe von DHCP, verfügt über einen eingebundenen DHCP-Server und lässt sich nicht nur über cnMaestro, sondern auch über eine Kommandozeile administrieren. Darüber hinaus unterstützt er unter anderem 802.1s Multiple Spanning Tree, VLANs und IGMP Snooping V1/V2.

Abgerundet wurde unsere Testumgebung durch zwei Wireless Access Points vom Typ “XV2-2X”. Diese lassen sich sowohl über ein lokales User Interface auf Browser-Basis, als auch über cnMaestro verwalten.

Sie unterstützen WiFi 6 (802.11ax) in den 2,4- und 5-GHz-Bändern und sind abwärtskompatibel zu den Standards 802.11a/b/g/n und ac. Für die Datenübertragungen stehen neben offenen Netzen die Verschlüsselungsstandards WPA PSK (TKIP), WPA 2, WPA 2 Enterprise und WPA 3 zur Verfügung.

Der Test

Im Test legten wir uns zunächst unter https://support.cambium-networks.com/register ein cnMaestro-Konto an, das Cambium anschließend mit der entsprechenden Lizenz versah, damit wir für den Test cnMaestro X nutzen konnten. Danach fügten wir unsere Testgeräte zu dem Account hinzu, nahmen die Komponenten in Betrieb und nutzten sie über den Zeitraum mehrerer Wochen. Dabei sammelten wir Erfahrungen über die Administration der Umgebung und die tägliche Arbeit mit der Lösung. Zum Schluss analysierten wir unsere Ergebnisse.



Nach dem Eingeben der Seriennummer erscheinen die Geräte in einer Liste und können eingerichtet werden

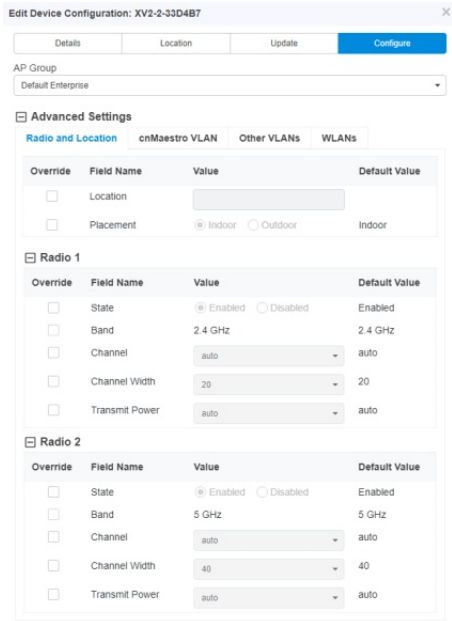
Das Onboarding der Cambium-Geräte

Um die Netzwerkkomponenten von Cambium in die cnMaestro-Umgebung aufzunehmen, stehen zwei unterschiedliche Optionen zur Verfügung: Via Seriennummer oder mit Hilfe der Cambium ID. Im Test wählten wir den Weg über die Seriennummer und wechselten dazu nach “Onboard / Claim Device”.

Danach öffnete sich ein Fenster, in dem wir die Seriennummer eingeben konnten. Das System erkannte daraufhin, um welches

Gerät es sich handelte (also NSE 3000, Switch oder Access Point) und nahm das betroffene Device in eine Liste auf.

Die Cambium ID wird erstellt, wenn ein Anwender ein cnMaestro-Konto anlegt. Sie findet sich unter "Onboarding / Settings" und die Administratoren sind an dieser Stelle auch dazu in der Lage, Benutzerkonten mit "Onboarding Keys" anzulegen, mit denen Anwender die Geräte über die Cambium ID zur Management-Umgebung hinzufügen können.



Im Rahmen des Onboarding-Prozesses besteht die Möglichkeit, den Geräten – wie hier einem Access Point – eine Konfiguration mitzugeben

Die ID und der Key müssen dann im Web-Interface des jeweiligen Geräts eingetragen werden. Dieser Weg ist vor allem für ältere Devices gedacht, die über keine zwölfstellige Seriennummer verfügen, funktioniert aber mit allen Produkten.

Mit der Aufnahme der Geräte in die Onboarding-Liste ist der Prozess allerdings noch nicht abgeschlossen. Es besteht nun die Möglichkeit, über die angesprochene ZTP-Funktion Konfigurationen für die Geräte zu erstellen und diese den Devices vorab zuzuweisen.

Auf diese Weise ist es möglich, die Produkte auch in Umgebungen ans Laufen zu bringen, in denen kein technisches Personal bereitsteht. Die Mitarbeiter müssen die Geräte, die dem Web-Interface von cnMaestro ja bekannt sind, lediglich mit dem Netz und einer Stromversorgung verbinden. Die Devices fahren dann hoch, verbinden sich mit der Management-Umgebung in der Cloud und beziehen von dort ihre Konfiguration. Danach können sie direkt in Betrieb gehen. Das funktioniert immer dann, wenn der Internet-Zugang bereits besteht. Soll eine NSE 3000 die Aufgabe des Internet-Routers übernehmen, so muss der Zugang über DHCP hergestellt werden.

Auf die Konfigurationen gehen wir später noch genauer ein. Im Rahmen des Onboarding-Prozesses sind die Administratoren zusätzlich noch dazu in der Lage, dem Gerät einen Namen zu geben, eine Beschreibung hinzuzufügen sowie zu definieren, an welchem Ort das jeweilige Device zum Einsatz kommen soll und welche Firmware-Version auf ihm verwendet wird. Ist diese Definition abgeschlossen, so reicht es, neben dem betroffenen Geräteeintrag in der Liste auf "Approve" zu klicken.

Danach überträgt das System die Konfigurationsinformationen und – falls gewünscht – die Firmware auf das Gerät und dieses nimmt den Betrieb auf. Im Test ergaben sich dabei an einem Anschluss von "Deutsche Glasfaser" via DHCP keine Probleme.

Die Konfigurationsoptionen für die einzelnen Gerätetypen

Wenden wir uns nun den Konfigurationsoptionen zu, die für die einzelnen Gerätetypen zur Verfügung stehen. Zunächst setzen wir uns mit dem NSE 3000 auseinander. Möchte ein IT-Verantwortlicher für diesen eine Konfiguration erstellen, so muss er nach "Configuration / NSE Groups" wechseln. Dort findet sich eine "Default Configuration", die die Administratoren bearbeiten können, es besteht aber auch die Möglichkeit, neue Konfigurationen zu erstellen oder Konfigurationen zu importieren.

Im Test machten wir uns zu diesem Zeitpunkt daran, die Standardkonfiguration an unsere Bedürfnisse anzupassen. Der NSE 3000 verfügt über eine Firewall-Funktion, die bis hinauf auf Layer-7 arbeitet, das bedeutet, es lassen sich Firewall-Regeln erstellen, die bestimmte Anwendung erlauben oder blockieren. Eine Deep Packet Inspection (DPI) gehört ebenfalls zum Leistungsumfang der Firewall.

Sowohl für ein-, als auch für ausgehenden Verkehr lassen sich Geo-IP-Filter setzen. So ist es beispielsweise möglich, den Datenverkehr nach Brasilien, China oder ein beliebiges anderes Land zu unterbinden, wenn zu diesem keine Geschäftsbeziehungen bestehen. Das funktionierte im Test problemlos.

Über einen DNS-Filter besteht parallel dazu die Option, bestimmte Seiten aus den Bereichen Pornographie, Social Media oder

auch Ad- und Malware zu sperren. Des Weiteren gehört das bereits erwähnte IDS/IPS-System auf Basis von Snort zum Leistungsumfang des NSE 3000. Im Rahmen der Konfigurationsdefinition besteht außerdem die Möglichkeit festzulegen, ob die vorgenommenen Änderungen automatisch auf die verwalteten Geräte synchronisiert werden soll, oder nicht.

Unter "Management" legt der IT-Verantwortliche das Administrator-Password fest, das zum Zugriff auf das Web-Interface der Appliance selbst genutzt wird. Dieses verfügt nicht über den vollen Funktionsumfang von cnMaestro, kann aber für Upgrades und Ähnliches Verwendung finden. Ebenfalls unter "Management" aktivieren die Administratoren bei Bedarf den SSH-Zugriff auf das Gerät und den DNS-Server und nehmen Einstellungen zur Zeitzone, den NTP-Servern sowie den Syslog-Servern vor. "Network" ermöglicht im Gegensatz dazu die Konfiguration der LAN-Ports (es stehen an dieser Stelle vier Ports zur Verfügung), der VLANs und der statischen Routen.

Bei den VLANs ist es noch erwähnenswert, dass die VLAN-Konfigurationen sich über Policies auf die Geräte verteilen lassen, so dass bei Bedarf beispielsweise NSE-Devices und Access Points automatisch in anderen VLANs landen. Die VLANs können außerdem auch auf Benutzerbasis oder mit Hilfe einer RADIUS-Authentifizierung zugewiesen werden.

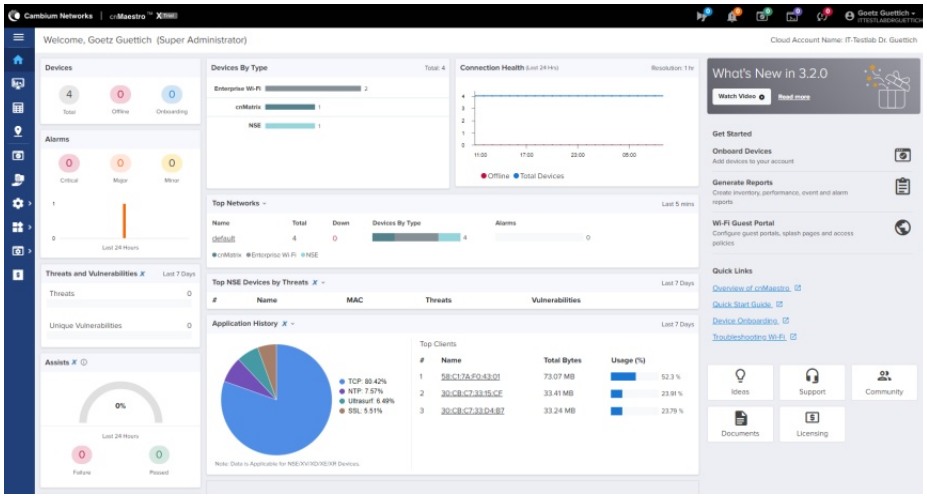
Ebenfalls interessant ist die WAN-Konfiguration, die mit dynamischen Adresszuweisungen, einer statischen IP-Adresse oder PPPoE funktioniert. Da die Appliance über zwei WAN-Ports verfügt, können die Verantwortlichen an dieser Stelle auch eine Load-Balancing-Funktion einrichten, Traffic Shaping aktivieren und die Link-Kapazität beschränken. Zusätzlich lässt sich auch DynDNS konfigurieren.

Über "VPN und RADIUS Server" konfigurieren die Administratoren IPSec-VPNs mit Preshared Key und einer Authentifizierung über den integrierten RADIUS-Server. "User-Defined Overrides" mit Variablen und Makros schließen den Leistungsumfang der NSE-3000-Konfiguration ab. Diese können beispielsweise zum Einsatz kommen, um über Skripting Konfigurationen zu realisieren, die im grafischen Benutzer-Interface des Systems nicht zur Verfügung stehen.

Die Konfiguration des cnMatrix EX2010-P

Bei der Konfiguration für die Switches haben die zuständigen Mitarbeiter zunächst die Wahl anzugeben, ob Konfigurationsänderungen automatisch auf die Geräte synchronisiert werden sollen. Außerdem können sie unter anderem auch die Konfiguration für die PoE-Ports vornehmen.

"Management" ermöglicht wieder das Anschalten des Zugriffs via Telnet, HTTP und SSH, das Setzen der Zeiteinstellungen und die DNS-, SNMP- und Syslog-Konfiguration. Unter "Network" finden sich unter anderem Einstellungen zum IGMP- und DHCP-Snooping, zu den VLANs, den Routen und zum Spanning-Tree-Protokoll.



Die Begrüßungsseite von cnMaestro, die nach dem Login erscheint gibt einen Überblick über den aktuellen Status

Im "Security"-Bereich richten die Administratoren den RADIUS-Server ein und legen Access Control Lists an. Auch bei den Switches schließen wieder die "User-Defined Overrides" die Konfigurationsoptionen ab. Interessant ist in diesem Zusammenhang, dass sich auch die Switch-Konfigurationen bei Bedarf anhand von Policies automatisiert zuweisen lassen.

Die Verwaltung der Access Points

Gehen wir nun noch kurz auf die Konfiguration der Access Points ein. Hier unterscheidet Cambium bei den Default-Konfigurationen zwischen "Enterprise" und "Ho-

me". Die Home-Konfigurationsoptionen beziehen sich auf einen WLAN-Router für den Home- und Small-Business-Bereich, den Cambium ebenfalls anbietet. Sie spielen für diesen Test keine Rolle.

Bei „Enterprise" geht es wieder mit der Auto-Sync-Konfiguration los, dazu kommen unter anderem Einstellungen zu LLDP-Paketen und den LEDs, die sich bei Bedarf ausschalten lassen. Zusätzlich richten die IT-Verantwortlichen hier auch die von ihnen benötigten WLANs ein beziehungsweise verwalten sie.

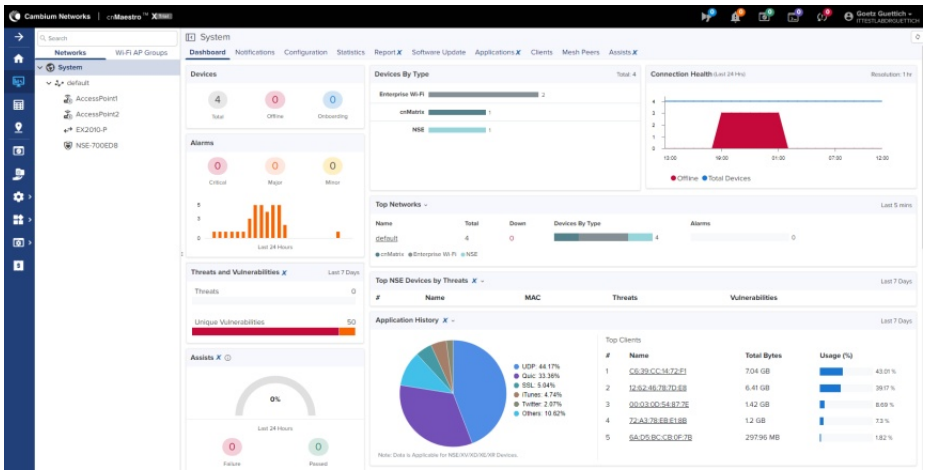
Zu den WLAN-Konfigurationsparametern gehören SSID, VLAN, Verschlüsselungstyp, Band, Einstellung zur Client Isolation, Timeouts und Ähnliches. Außerdem umfassen die Einstellungen Angaben zum Authentifizierungs-Server und Zugriffskontrolloptionen mit MAC-Authentifizierung, ACLs sowie Datenbeschränkungen für Clients und WLANs.

Darüber hinaus richten die Administratoren an dieser Stelle Gastzugriffe ein und konfigurieren ePSKs. Die letztgenannten stellen einzigartige Private-Pre-Shared-Keys dar, mit denen die Benutzer ihren WLAN-Zugriff individuell absichern können.

"Management" umfasst die Zugriffsoptionen wie SSH, HTTP und HTTPS, das Administrator-Passwort, die Konfiguration der Kommunikation mit dem RADIUS-Server sowie Einstellungen zu Syslog, SNMP und Zeit. "Radio" ermöglicht es, für die 2,4-, 5- und bei Hardware, die das unterstützt, auch 6-GHz-Bänder Parameter wie die Übertragungsleistung oder auch die Kanalbreite anzugeben. Außerdem lassen sich hier auch Angaben zum Advanced Roaming und zur dynamischen Auto-RF-Power-Option vornehmen.

Unter "Network" besteht die Möglichkeit, die IPv4- und die IPv6-Konfiguration vorzunehmen. Zu den in diesem Zusammenhang relevanten Punkten gehören das Default Gateway, die DNS-Konfiguration, das Routing, das Port-Forwarding und Ähnliches. Außerdem lassen sich hier unter anderem Einstellungen zum DHCP-Pool, den Tunneln, PPPoE und dem VLAN-Pool vornehmen.

Der Punkt "Security" stellt Einstellungen zum DoS-Schutz, zur Wireless Flood Detection und zum WIDS (Wireless Intrusion Detection System) zur Verfügung, das nichts mit dem IDS/IPS des NSE 3000 zu tun hat, aber Angriffe auf den Access Point selbst erkennen kann. "Services" bietet schließlich unter anderem Möglichkeiten zur Konfiguration von LDAP, NAT Logging, Bonjour sowie APIs für Wi-Fi und Bluetooth. Auch hier schließen wieder User-Defined Overrides die Konfigurationsoptionen ab.



Dashboards lassen sich sowohl für einzelne Geräte, als auch für Netzwerke anzeigen

Das Einrichten von Captive Portals

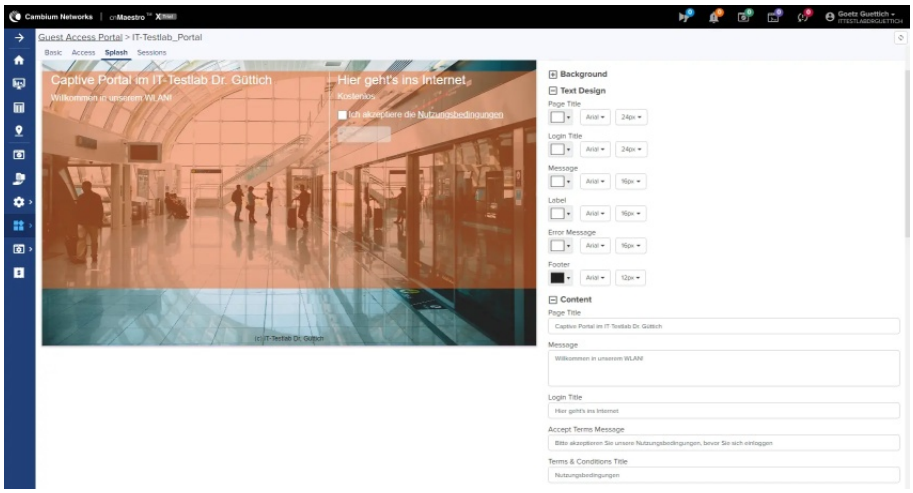
Nachdem wir die Konfiguration unserer Geräte abgeschlossen hatten und alles zu unserer Zufriedenheit funktionierte, machten wir uns daran, ein Captive Portal einzurichten, das den Zugriff auf unser WLAN absichern sollte. Cambium unterstützt in diesem Zusammenhang Captive Portals für kostenlose WLANs, für WLANs, bei denen der Zugriff mit Vouchern ermöglicht wird und für kostenpflichtige WLANs, beispielsweise durch Bezahlungen via Paypal, IPpay oder QuickPay.

Um ein Captive Portal einzurichten, wechseln die Administratoren nach "Network Services / Guest Access Portal" und gehen dort auf "Add Portal". Dann können sie dem Portal einen Namen geben, eine Beschreibung einfügen und das Client-Login-Event-Logging aktivieren.

Ansonsten gibt es noch die Möglichkeit, diverse Parameter wie die Sitzungsdauer, die Down- und Uplink-Raten und die Quota

festzulegen. Darüber hinaus unterstützt das System den Login über Konten Sozialer Netze (Google, Twitter, Facebook und Office 365), die Authentifizierung via SMS und das Anlegen von White Lists.

Bei der Konfiguration des Begrüßungsbildschirms haben die Anwender unter anderem die Möglichkeit, ein Logo und einen Bildschirmhintergrund hochzuladen, die angezeigten Texte und die Schriftart anzupassen und eigene Felder zu definieren. Das funktioniert alles sehr gut, allerdings fragten wir uns im Test, wieso der Hersteller den Editor mit einer verhältnismäßig kleinen Schrift gestaltet hat, die zudem Grau auf Weiß dargestellt wird, was die Arbeit unnötig erschwert. Sobald das Captive Portal fertig konfiguriert wurde, kann es in der WLAN-Konfiguration unter "Guest Access" zugewiesen werden. Danach geht es in Betrieb. Im Test ergaben sich dabei keine Schwierigkeiten.



Die Definition unseres Captive Portals

Das Monitoring und die Problemlösung mit cnMaestro

Ebenfalls von Interesse: Die von cnMaestro bereitgestellten Überwachungs- und Problemlösungsfunktionen. Wechselt beispielsweise ein Administrator unter "Monitor and Manage" auf den Eintrag eines Clients, so erhält er ein Dashboard, das Aufschluss über die Datenübertragungen, die Top-Anwendungen, die Top-Kategorien (wie Datenübertragungen, Messaging und so weiter), die Datenrate, die Signal to Noise Ratio und Ähnliches gibt.

Neben dem Dashboard stellt das System auch noch Reiter zu den verwendeten Applikationen und der Leistung (mit Signalstärke, Signal to Noise Ratio, Datenrate, Nutzung und Anwendungsnutzung) zur Verfügung. Bei beiden Übersichten können die IT-Verantwortlichen mit der Maus über die Graphen fahren und erhalten dann Detailinformationen darüber, welche Datenmengen zu diesem Zeitpunkt von welcher Anwendung übertragen wurden, beziehungsweise welche Datenraten über das Gerät liefen und wie es mit den Signalstärken aussah.

Der letzte Reiter, der in diesem Zusammenhang von Interesse ist, listet die gefundenen Vulnerabilities auf. Auf die dazu gehörende Funktionalität sind wir bereits im Zusammenhang mit unserem Ubuntu-Client-System eingegangen. Die Überwachungsdaten können im Betrieb eine wichtige Hilfe beim Troubleshooting sein. So lassen sich über das Switch-Dashboard beispielsweise einzelne Switch-Ports analysieren, die daran angeschlossenen PoE-Geräte neu starten und Kabeldiagnosen durchführen, die in Metern angeben, in welcher Entfernung der Fehler liegt.

Bei der Fehlerdiagnose für Wireless Clients hilft eine Roaming-History. Diese macht beispielsweise deutlich, wenn es nach dem Wechsel zu einem anderen Access Point zu einem Leistungsabfall kommt. Abgesehen davon besteht auch die Option, in WLANs oder VLANs einen Packet-Capture-Vorgang zu starten, um Probleme ausfindig zu machen. Ein WiFi-Analyzer in den Access Points schafft zudem Klarheit über die Interferenz, den Noise und die Zahl der Access Points, die in bestimmten Kanälen aktiv sind.

Zusammenfassung und Fazit

cnMaestro stellt ein extrem leistungsfähiges Management-Tool dar, das alle Produkte von Cambium verwalten kann. Es ermöglicht nicht nur die Inbetriebnahme und Konfiguration der Komponenten, sondern auch deren Überwachung und das Troubleshooting. Wegen des großen Funktionsumfangs konnten wir im Test nicht auf alle Funktionen der Lösung eingehen. Sie verfügt beispielsweise auch noch über ein RESTful-API und so genannte Webhooks. Damit lassen sich beispielsweise Alarme über Slack ausgeben. Unter dem Strich können wir sagen, dass cnMaestro für Administratoren bei der täglichen Arbeit eine große Hilfe sein kann.