STUDERUS
network technologies

PUNKT.

Das Magazin für
Kompetenz in IT-Sicherheit und
Netzwerk-Technologien

Highlights – auf den Punkt gebracht

WiFi 6E – der nächste Schritt

Internet für die Ferienwohnung

Sicherer Remote-Zugriff auf Firewalls

VPN-Client nur noch im Abo-Modell

Firewall-Management in Nebula

Ausgabe August 2022

WiFi 6E – der nächste Schritt

WiFi 6E ist die nächste Evolutionsstufe drahtloser Netzwerke. Wir zeigen Ihnen, welche Vorteile der neue WLAN-Standard bringt und warum Sie sich schnellstmöglich damit vertraut machen sollten.

Mit WiFi 6E gehen wir den nächsten logischen Schritt und erschliessen zusätzlich zum 5-GHz- auch das 6-GHz-Frequenzspektrum. Somit erweitert sich die bestehende Technologie 802.11ax (WiFi 6) mit dem Standard WiFi 6E um das neue, unlizenzierte 6-GHz-Band.

Die Vorteile von WiFi 6E

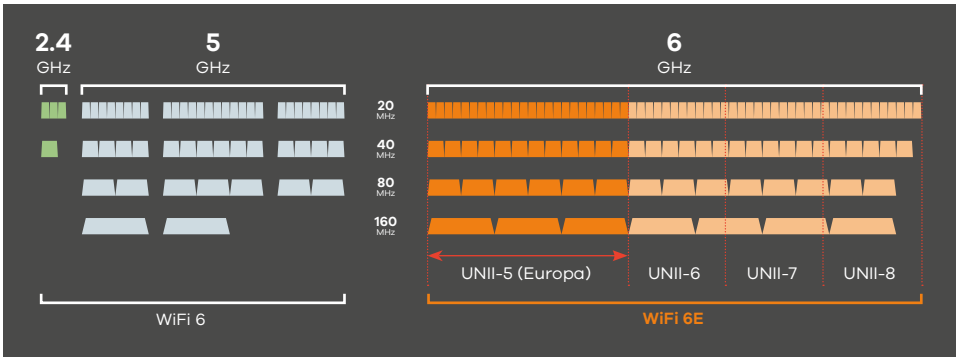
Was bedeutet das nun für den Händler oder Konsumenten, der gerade erst die Vorteile von WiFi 6 kennengelernt hat? Kurz gesagt, WiFi 6E beinhaltet sämtliche Funktionalitäten, welche wir bereits von WiFi 6 kennen, und fügt noch weitere hinzu.
Die Schlüsselvorteile lassen sich wie folgt zusammenfassen:

- 2.5x mehr Kapazität im neuen Frequenzspektrum
- Bis zu 7 superbreite 160-MHz-Kanäle im 6-GHz-Frequenzspektrum für sehr bandbreitenintensive Anwendungen
- Keine Interferenzen durch Mikrowellenstrahlung oder nicht 6E-fähige Geräte
- Verbesserte Geschwindigkeit durch Multi-Gigabit und sehr niedrige Latenzen

6E WiFi 6 Extended

Andere Länder, andere Bereiche

Verschiedene Länder geben davon unterschiedliche Bereiche zur Nutzung frei. Die USA hat beispielsweise sämtliche UNII-Bereiche von 6 GHz zur WiFi-Nutzung freigegeben. Andere Länder wie z. B. Taiwan haben noch keine 6-GHz-Frequenzen freigegeben. In Europa ist es per Stand heute erst im UNII-5 Bereich erlaubt, mit WiFi-6E-Geräten zu senden, was uns den Frequenzbereich von 5'925 MHz (CH1 startet bei 5'955 MHz) bis 6'425 MHz bietet.
Nichtsdestotrotz ergeben sich dadurch auch in der Schweiz bereits 24 zusätzliche WLAN-Kanäle à 20 MHz im 6-GHz-Band, die zur Verfügung stehen. Da die Kanalnummerierung im 6-GHz-Band untypischerweise wieder bei 1 startet, aber jeder Kanal wie im 5-GHz-Band immer noch jeweils 20 MHz umfasst, können wir mit UNII-5 somit die Kanäle 1 bis 93 nutzen.



Übersicht des WiFi-Frequenzspektrums

6-GHz-Band

Um die Vorteile besser einordnen zu können, schauen wir uns das 6-GHz-Band etwas genauer an. Der Faktor der Kapazitätssteigerung vom 6-GHz- verglichen mit dem 5-GHz-Frequenzspektrum ist in etwa so wie der Sprung von 2.4 GHz auf 5 GHz. Das 6-GHz-Frequenzspektrum startet bei 5'925 MHz, endet bei 7'135 MHz und umfasst 233 Kanäle. Dieser Bereich ist unterteilt in vier Partitionen, namentlich UNII-5, UNII-6, UNII-7 und UNII-8.

Neue WiFi-6E-Funktionen:

1. Bevorzugter Sondierungs-Kanal «Preferred Scan Channel (PSC)»

Ungleich dem 5-GHz-Band, in dem man den bevorzugten Primärkanal für die Clients frei definieren kann, ist das bei 6 GHz aufgrund der hohen Anzahl an Kanälen und der dadurch längeren Zeit, welche für die SSID-Sondierung notwendig wäre, nicht mehr möglich. Jeder UNII-Bereich hat spezifisch definierte Primärkanäle, damit der Client nicht jeden Kanal einzeln sondieren muss. Bei UNII-5 sind das die Kanäle 5, 21, 37, 53, 69 und 85.

2. Mehrfache BSSID-Informations-Elemente «Multiple SSID IE»

Bei 2.4 / 5 GHz wird pro ausgestrahlter SSID ein Beacon-Signal benötigt. Mit WiFi 6E können im 6-GHz-Band bis zu vier SSID-Informationen mit einem Beacon-Signal transportiert werden. Dadurch bleibt mehr Airtime für die produktive Datenübermittlung zwischen Access-Point und Client.

3. Reduzierung der Informations-Elemente von benachbarten Radios «Reduced Neighbor Reports (RNR) IE»

Die SSID-Informationen für das 6-GHz-Band werden über das 2.4-GHz-/5-GHz-Beacon mitgegeben, wenn der Client einen davon empfängt. Somit muss der Client die Kanäle im 6-GHz-Band nicht mehr sondieren, um die Informationen zu den Primärkanälen zu erhalten. Diese Funktion erhöht ebenfalls die Airtime für die produktive Datenübermittlung zwischen Access-Point und Client.

Clients und Access-Points

Bereits seit Anfang 2022 gibt es erste Clients, welche WiFi 6E unterstützen. Darunter befinden sich Notebooks der neuesten Generation sowie Smartphones, um zwei der verbreitetsten Kategorien zu nennen. Höchste Zeit also, dass die Industrie auch auf Seite der Zugangspunkte mit dem neuesten Standard nachzieht. Mit den Modellen NWA220AX-6E, WAX620D-6E und WAX640S-6E hat Zyxel seine Hausaufgaben bereits gemacht und kündigte im Juni die genannten drei WiFi-6E-Access-Points an. Die ersten Modelle sollen ab Herbst 2022 verfügbar sein und weitere folgen.

Das Flagship-Modell WAX640S-6E wird über einen Triband-Modus verfügen und 2.4 GHz, 5 GHz und 6 GHz simultan unterstützen. Die kleineren Modelle verfügen über Dual-Radios, womit man zwischen 2.4 GHz und 5 GHz simultan oder 2.4 GHz und 6 GHz simultan wählen kann.

Ein kleiner Ausblick

Die nächsten grösseren Neuerungen nach WiFi 6E erwarten wir mit WiFi 7, 802.11be. Dieser Standard wird das 6-GHz-Frequenzspektrum voraussichtlich noch weiter verbessern und maximale Kanalbreiten von bis zu 320 MHz bieten, was eine Verdoppelung verglichen mit WiFi 6E bedeutet. Erste Geräte dazu erwarten wir Stand heute gegen Ende 2023.

Internet für die Ferienwohnung

Auch in den Ferien sind wir auf das Internet angewiesen. Wir zeigen Ihnen, wie einfach und kostengünstig eine flexible Internetzugangslösung für Ihre Zweit-/Ferienwohnung sein kann.

Wer kennt es nicht? Kaum in der Ferienwohnung in Graubünden oder im Tessin angekommen und der Blick aufs Handy offenbart: «Kein Internet, offline».

Lohnt sich das?
Viele sehen es mittlerweile als selbstverständlich an, überall eine einfach zugängliche, stabile und idealerweise auch schnelle Internetverbindung für alle Clients zur Verfügung zu haben. Für viele Ferien-/Zweitwohnungsbesitzer lohnt es sich schlicht nicht, an einem Standort, der nur wenige Wochen im Jahr genutzt wird, einen klassischen Internetzugang über beispielsweise Kupferkabel installieren zu lassen, falls denn diese Option überhaupt verfügbar ist.

Beispiel Kabelanschluss
Rechnen wir ein klassisches Beispiel durch: «blue internet S» mit einem minimalen Kupferkabel-Internetanschluss von Swisscom*, ohne spezielle Vergünstigungen.

Den Router bekommen wir gestellt oder er ist im Abopreis mit der Mindestvertragslaufzeit mit einkalkuliert. Es fallen monatliche Kosten von CHF 64.90 bei einer Geschwindigkeit von 100 Mbps Download/Upload an. Die Mindestvertragslaufzeit beträgt 24 Monate, weshalb wir damit rechnen. Die einmalige Aktivierungsgebühr beträgt CHF 89.–.

Beispiel 5G
Stellen wir dem Ganzen nun ein richtig performantes und flexibles Angebot mit einem 5G-Router und einer SIM-Karte gegenüber: Als Router setzen wir ein Gerät mit 5G/LTE und bis zu 5'000/650 Mbps Download/Upload ein, den Zyxel Nebula NR5101 (CHF 867.–). Er bietet integriertes WiFi 6, AX-WLAN und 2x GbE-Schnittstellen.

Falls Sie bereits über ein bestehendes Mobile-Abo von Swisscom* verfügen, können Sie mit der Option Multi-SIM für CHF 10.–/Monat kostenlos eine zusätzliche SIM-Karte für Ihren 5G-/LTE-Router bestellen. Die zusätzliche SIM-Karte erlaubt dieselbe Internetgeschwindigkeit, welche über das damit verbundene Mobile-Abo verfügbar ist.

5G-Router mit AP und Switch
Um den 5G-/LTE-Router optimal platzieren zu können und in jedem Fall eine gute WLAN-Abdeckung zu gewährleisten, ergänzen wir die Installation noch mit einem zusätzlichen WLAN-Access-Point, dem Zyxel NWA50AX (CHF 128.–). Auch dieser verfügt über WiFi-6-WLAN für die aktuellsten Clients.

Falls der übrige Port am 5G-Router nicht für TV, Notebook usw. ausreicht, ergänzen wir die Installation noch mit einem kleinen Switch, dem Zyxel GS1915-8EP (CHF 185.–) (Swisscom-TV-Multicast über LTE ist nicht möglich, nur «TV air»). Streamingdienst-Anbieter oder die üblichen TV-Anwendungen funktionieren einwandfrei. Mit diesem PoE-Switch ist auch die Stromversorgung des Access-Points über das RJ45-Kabel abgedeckt. Für die Verkabelung greifen wir auf zwei gewöhnliche RJ45-Kabel zurück. Diese schlagen je nach Länge mit rund CHF 20.– zu Buche.

Fazit
Rechnen wir die Swisscom-Variante, ergeben sich 2-Jahres-Kosten von CHF 1'646.60 und zwei Jahre Mindestlaufzeit. Als Pluspunkt sehen wir die Unabhängigkeit von einem guten 5G-/LTE-Signal am Standort.

Rechnen wir die 5G-Router-Variante, summieren sich die 2-Jahres-Kosten auf CHF 1'420.–. Als Pluspunkt sehen wir massiv höhere, mögliche Download-/Upload-Geschwindigkeiten, niedrigere Gesamtkosten und die Hardware ist nicht gemietet, sondern erworben. Alle Komponenten der 5G-Variante können zudem standortunabhängig über die kostenlose Nebula-Cloud-Plattform verwaltet und schnell sowie flexibel an einem anderen Standort eingesetzt werden.

** Die Auswahl von Swisscom als Anbieter dient nur als Beispiel. Es gibt diverse alternative Anbieter mit vergleichbaren Datenflatrate-Abos.*

Mehr Internetzugangslösungen über 5G-Router finden Sie im Studerus-Blog:
blog.studerus.ch/de-ch/internet-ferien

Internetzugangslösung über 5G-Router

SECURITY

ZYXEL nebula

Sicherer Remote-Zugriff auf Firewalls

Sie schützt IT-Systeme vor Angriffen und unbefugten Zugriffen: die Firewall. Damit sie ihre Aufgabe zuverlässig erledigen kann, benötigt sie Aufmerksamkeit und Unterhalt.

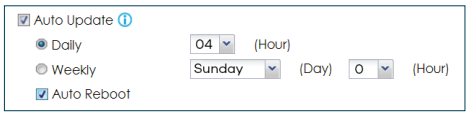
Als Türsteher und Bewacher übernimmt die Firewall eine wichtige Rolle in einem Netzwerk. Sie schützt Ihre Daten, verhindert unberechtigten Zugriff und benachrichtigt Sie, wenn es verdächtige Aktivitäten gibt.
Damit die Firewall ihren Dienst an vorderster Front gewissenhaft leisten kann, braucht sie aber unsere Aufmerksamkeit und muss aktiv betreut werden. Und es muss unbedingt dafür gesorgt werden, dass die Firewall nicht selbst Opfer eines Angriffs wird. Fällt die Firewall, fällt das Netzwerk.
Zum Glück haben wir es aber selbst in der Hand. In diesem Artikel stellen wir einige Möglichkeiten vor, um unser wichtigstes Netzwerkgerät zu schützen.

Patchen! Patchen! Patchen!
Wir alle kennen es: Regelmässig erscheinen Updates für Betriebssystem und Applikationen, weil Sicherheitslücken entdeckt wurden. Aktuellstes Beispiel ist die Log4shell-Zero-Day-Sicherheitslücke. Sehr viel Software und Geräte waren davon betroffen. Dies zwang uns, diverse Patches zu installieren.

Daher gilt für die Firewall genau dasselbe Prinzip wie für die restliche eingesetzte Software: Patchen! Patchen! Patchen!
Dazu veröffentlicht Zyxel regelmässig neue Firmware-Versionen. Oftmals mit neuen Funktionen und Erweiterungen. Aber mindestens genauso wichtig: Aktuelle Sicherheitslücken werden zeitnah gestopft. Und zwar, bevor sie in der Öffentlichkeit bekannt und somit von Angreifern ausgenutzt werden können.

Darum ist es besonders bei Firewalls unerlässlich, immer die neuesten Firmware-Versionen aufzuspielen. Die Frage lautet nun: Wie mache ich das effizient, ohne meine Techniker stundenlang zu beschäftigen? Neben dem Update «von Hand» bietet Zyxel dafür verschiedene andere Optionen:

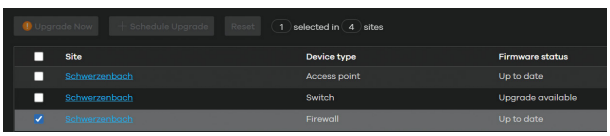
Auto-Update
Die sicherlich einfachste und kostengünstigste Methode ist Auto-Update.



Die Funktion finden Sie unter «Maintenance > File Manager > Firmware Management». Sie können das Update entweder täglich zu einer bestimmten Zeit oder wöchentlich an einem definierten Tag und Zeitpunkt ausführen lassen. Wird Auto-Reboot aktiviert, spielt die Firewall die aktuellste Version auf die Standby-Partition und startet sich neu. Die Firewall startet dann von dieser Standby-Partition. Dadurch entsteht ein Unterbruch, wählen Sie also einen Zeitpunkt ausserhalb der Arbeitszeit.

Der Vorteil dieser Methode ist, dass automatisch immer die aktuellste Firmware-Version eingesetzt wird. Patches gegen bekannte Sicherheits-Schwachstellen werden so schnellstmöglich installiert. Ein kleines Risiko dieses Verfahrens ist, dass die Firewall bei einem Update nicht korrekt neu startet, oder die Konfiguration nicht zu 100 Prozent übernommen wird.

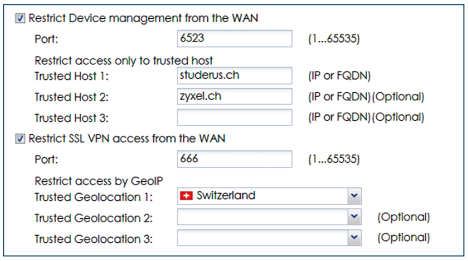
Zentrales Management
Aus unserer Sicht die effizienteste und sicherste Methode ist das Update per Nebula, der zentralen Cloud-Plattform von Zyxel. Dies vereint die Vorteile von «per Hand» und «Auto-Update». Kein langwieriges Heraussuchen der Zugangsdaten, kein VPN-Tunnel ist notwendig. Sie loggen sich einfach mit Ihrem Account ein und können alle Firewalls per Mausklick aktualisieren oder terminieren. Je nach Lizenz kann sehr granular definiert werden, was wann wie aktualisiert wird.



Zyxel-Firewalls lassen sich erst seit ein paar Monaten per Nebula verwalten und konfigurieren. Es werden laufend Firewall-Funktionen hinzugefügt. Anfangs 2023 wird der Funktionsumfang in etwa der On-Premise-Version entsprechen.

Update mit IT-Management-Lösungen
Benutzen Sie eine Netzwerk-Management-Lösung wie Solarwinds oder Barracuda RMM? Hier bieten sich diverse Möglichkeiten, die Firewall per Skript zu aktualisieren, falls die Firewall in das System eingebunden ist. Kommen Sie auf uns zu, falls Sie dieses Vorgehen in Betracht ziehen – wir beraten Sie gerne.
Neben Firmware-Updates gibt es weitere wichtige Punkte, die Sie berücksichtigen sollten:

Nur absolut notwendige Zugänge von aussen
Im besten Fall ist das GUI von aussen nicht über HTTPS (und noch viel weniger über HTTP) erreichbar. Stattdessen sollte ein IPSec-Tunnel verwendet werden. Benutzen Sie auf jeden Fall 2-Faktor-Authentifizierung. Sollte die Firewall aus irgendwelchen Gründen trotzdem per HTTPS erreichbar sein, berücksichtigen Sie folgende Ratschläge:
- Ändern Sie den HTTPS- und SSL-VPN-Port auf etwas anderes als «default».



- Im Normalfall sind Angriffe auf Firewall-Sicherheitslücken automatisiert und berücksichtigen die Standard-Ports. Daher ist das Ändern der entsprechenden Ports eine gute Idee. Trennen Sie auf jeden Fall SSL-VPN und den Admin-Zugang.
- Schränken Sie den Zugang so weit wie möglich ein. Am besten auf eine IP oder mindestens eine IP-Range. Falls das nicht möglich ist, bietet Geoblocking die Möglichkeit, den Zugang wenigstens auf ein Land einzuschränken.
- Verwenden Sie für die Authentifikation zusätzlich Zertifikate.
- Stellen Sie sicher, dass sich nur wirklich benötigte Dienste in der Gruppe «Default_Allow_WAN_To_ZyWALL» befinden.
- Ändern Sie das Admin-Passwort regelmässig.

KB-Artikel und weiterführende Infos im Blog:
blog.studerus.ch/de-ch/remote-access-firewall

SECURITY

ZYXEL

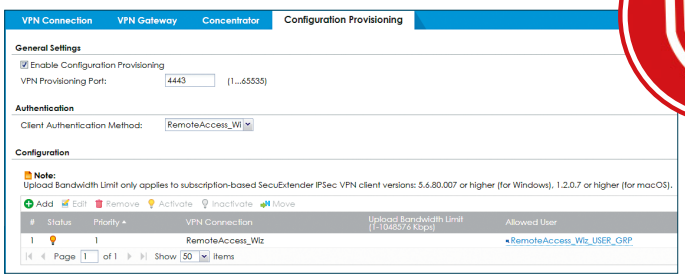
VPN-Client nur noch im Abo-Modell

Der «SecuExtender IPSec VPN Client» für Windows und Mac ist als Abonnement mit einer Laufzeit von einem oder drei Jahren erhältlich.

Bis Ende 2022 werden die letzten unbefristeten Lizenzen des SecuExtender IPSec VPN Client abverkauft sein. Danach ist nur noch die Lizenz mit kostenlosen Updates während einer Laufzeit von einem oder drei Jahren erhältlich. Zyxel folgt somit dem generellen Trend in der Branche, Software nur noch im Abo-Modell anzubieten. Die Abo-Version des SecuExtender ist auf einem neueren Stand als die herkömmliche, einmalige Lizenz. Updates gewährleisten Kompatibilität mit neuen Betriebssystemen und bringen wichtige Sicherheits-Patches. Um den Verwaltungsaufwand mit dem Erneuern der Lizenzen zu reduzieren, wird der Einsatz der 3-Jahres-Lizenzen empfohlen.

Übersicht mit Preis und Artikelnummer der SecuExtender-Abo-Lizenzen

	1 Jahr Artikel / Preis	3 Jahre Artikel / Preis
1 User	2744 / CHF 49.–	2748 / CHF 134.–
5 User	2745 / CHF 235.–	2749 / CHF 650.–
10 User	2746 / CHF 475.–	2750 / CHF 1'323.–
50 User	2747 / CHF 2'370.–	2751 / CHF 6'590.–



Auf der Firewall wird die Provisionierung der Konfiguration aktiviert, aus Sicherheitsgründen wurde der spezielle Port 4443 gewählt.

Neueste OS unterstützt

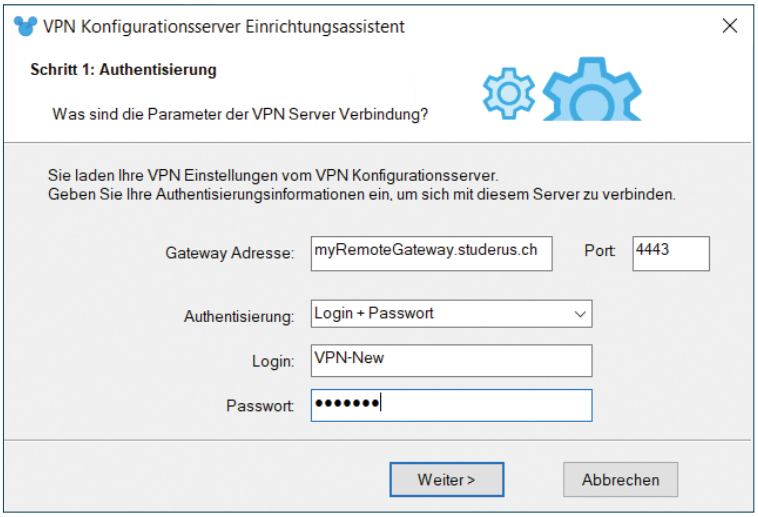
Der Zyxel SecuExtender VPN Client (IPSec VPN/ SSL VPN) unterstützt jetzt auch Windows 11 und macOS 12. Der IPSec VPN-Client hat einen einfachen Konfigurationsassistenten in drei Schritten, sodass mobile Mitarbeiter schneller denn je VPN-Verbindungen erstellen und entfernen können. Er bietet auch eine einfache Skalierbarkeit, indem er eine eindeutige, duplizierbare Datei der Konfiguration und Parameter speichert.

Die VPN-Konfigurationen und Sicherheitselemente, einschliesslich «Pre-shared Key», Zertifikate und IKEv2, lassen sich auf einem USB-Stick speichern. So müssen die Authentifizierungsdaten nicht auf dem Computer gespeichert sein. Benutzer können ihre Remote-Anwendungen und -Daten einfach verwenden, als ob sie im Büro wären.

Einfaches Rollout der Konfiguration

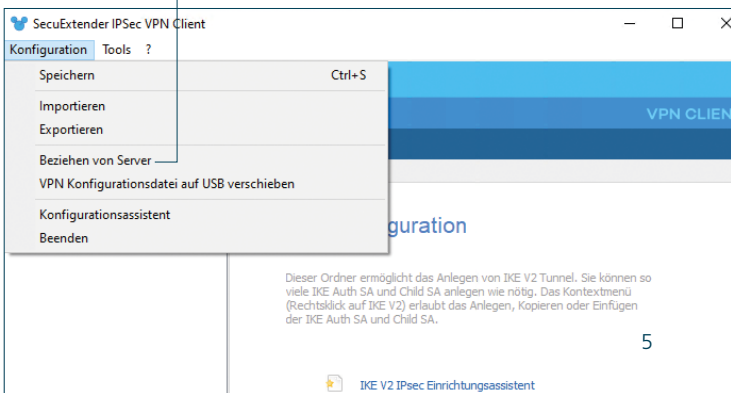
Der Zyxel SecuExtender IPSec VPN Client verfügt über eine Bereitstellungsoption, die es ermöglicht, die vorkonfigurierten VPN-Regeleinstellungen herunterzuladen. So muss der Client nicht manuell konfiguriert werden. Nachdem die Konfiguration heruntergeladen wurde, wird ein VPN-Tunnel zwischen dem PC mit dem VPN-Client und der Firewall eingerichtet.

KB-Eintrag mit Schritt-für-Schritt-Anleitung finden Sie im Zyxel-Support-Portal: **support.zyxel.eu**



Den Zugang zur Firewall mit dem User wählen und schon wird die Konfiguration heruntergeladen, dabei muss derselbe Port 4443 verwendet werden.

Im VPN-Client wird die Konfiguration vom Server/Firewall bezogen.



CLOUD-MANAGEMENT

ZYXEL nebula

Firewall-Management in Nebula

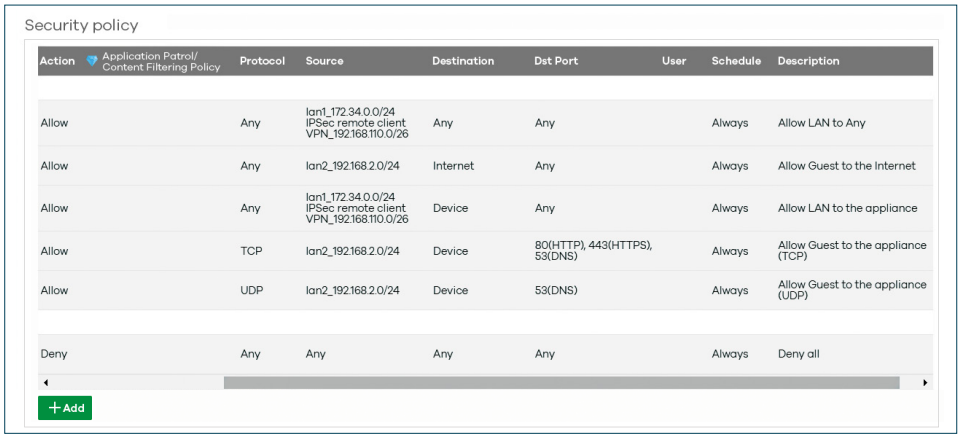
Nebula hat sich als intuitive und übersichtliche Management-Plattform in der Cloud bewährt. Neben WLAN-APs und Switches werden zunehmend auch Firewalls darüber verwaltet.

Immer mehr Systemintegratoren und IT-Verantwortliche setzen auf Cloud-basiertes Netzwerk-Management. Dies zeigt sich als klarer Trend der Hersteller von Netzwerkkomponenten und Firewalls. Der Anteil an über Nebula verwalteten Geräten ist bei den WLAN-Access-Points am höchsten. Da werden normalerweise mehrere APs eingesetzt und diese verwaltet man am einfachsten zentral. Ein Switch gehört bei einem WLAN immer dazu und auch sie werden am einfachsten ebenfalls in Nebula verwaltet. Der Anteil an Firewalls, der über Nebula verwaltet wird, ist noch nicht so hoch, aber tendenziell auch steigend.

Gründe, Firewalls in Nebula zu verwalten:

- **Überwachung 24/7**
  Ist ein Nebula-Device nicht erreichbar, wird in der Nebula-App per Push-Mitteilung gleich ein Alarm ausgelöst. Nebula ist also prädestiniert, um Kunden einen Managed Service mit einer Intervention bei einem Ausfall anzubieten.

- **Einfacher Überblick**
  Auch ein Techniker, der mit einem Netzwerk noch weniger vertraut ist, findet sich dank Nebula schnell zurecht. Der grösste Mehrwert eines Netzwerk-Managements entsteht, wenn möglichst viele Komponenten in dasselbe System integriert werden.



Neue Darstellung der Policies in Nebula

- **VPN per Mausklick**
  Einfache VPN-Verbindungen lassen sich innert Kürze konfigurieren und überwachen.

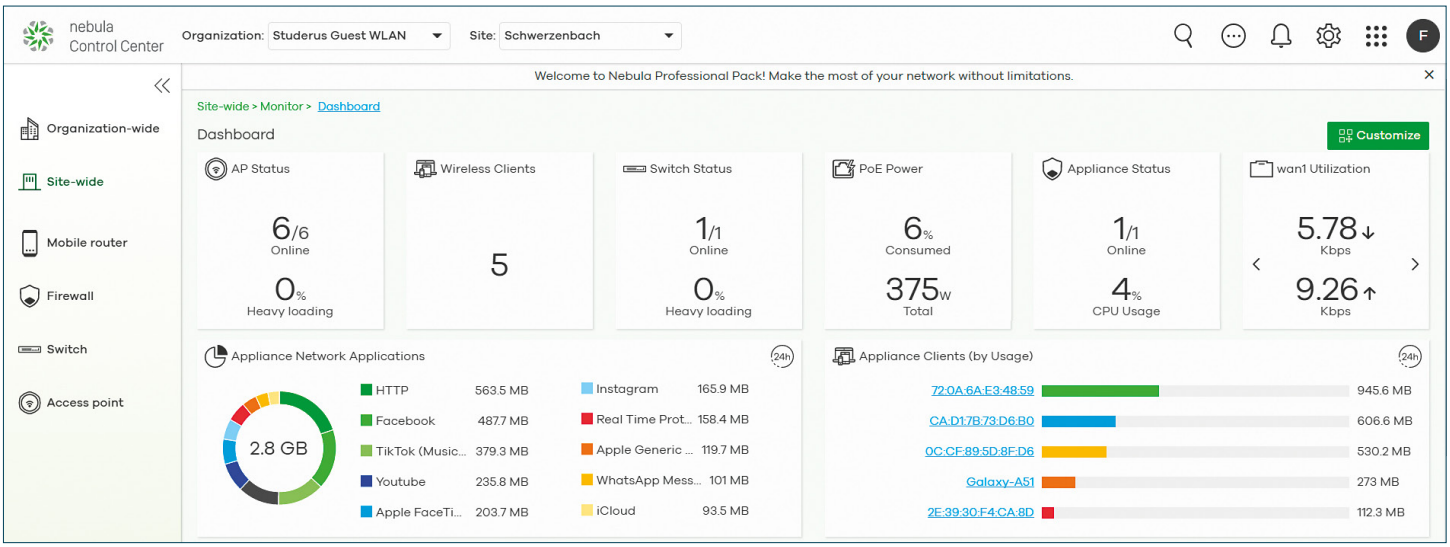
- **Automatisierte Firmware-Updates**
  Patchen ist wichtig. Mit Nebula erfolgt dies automatisiert oder mit minimem Aufwand.

Migration braucht Neukonfiguration

In der Praxis werden Firewalls primär bei Neuinstallationen in Nebula integriert. Um eine bestehende Firewall in Nebula zu migrieren, muss die Konfiguration neu erstellt werden. Jede USG-Flex- oder ATP-Firewall kann Standalone über das Web-GUI oder über Nebula verwaltet werden. Leider ist beides gleichzeitig nicht möglich.

Verknüpfung mit Circle

Die Verwaltung der Lizenzen kann bei einer grösseren Anzahl Geräte mit unterschiedlichen Ablaufdaten schnell unübersichtlich werden. Circle ist eine Plattform für Zyxel-Partner, um Lizenzen einfach zu verlängern. Circle ist mit Nebula verknüpft. Bei autorisierten Partnern erfolgt die Verrechnung im Folgemonat mit einer normalen Rechnung der Studerus AG.



Mit einer Firewall zeigt die Übersicht in Nebula auf einen Blick, welche Applikationen primär verwendet werden und welche Clients viel Verkehr generieren.

SERVICES

ZYXEL

Erweiterung Support mit Swiss Service Pack

Swiss Service Pack beinhaltet einen Vorabaustausch und eine Anzahl Stunden für einen Online-Konfigurationsservice. Studerus-Fachhändler erhalten den Swiss Service Pack «Next Business Day» (NBD) gratis.

Bei vielen Kunden unserer Fachhändler ist ein umfangreicher technischer Support wichtiger als der tiefste Preis. Mit Swiss Service Pack unterstützen wir Sie und Ihre Kunden mit einem erweiterten Support. Ein Vorabaustausch bei einem Hardware-Defekt sowie ein kostenloser Online-Konfigurationsservice sollen dazu führen, dass Sie Zyxel-Produkte gerne einsetzen.

Was ist Swiss Service Pack?
Swiss Service Pack ist eine Erweiterung der Standard-Support- und Garantieleistungen und in drei unterschiedlichen Varianten erhältlich. Der Service-Pack enthält einen garantierten Vorabaustausch. Zudem wird eine Anzahl Stunden Konfigurationsservice via Telefon und eine Remote-Verbindung angeboten, falls bei der Installation oder Konfiguration eines Zyxel-Produkts Unterstützung benötigt wird.

Service-Bedingungen
Alle Services sind grundsätzlich kostenpflichtig. Studerus-Fachhändler erhalten exklusiv den Swiss Service Pack NBD gratis dazu geliefert, wenn der Produktwert eines Zyxel-Produkts (Händlerpreis) > CHF 200 ist.
Neu sind Verträge für eine Laufzeit von zwei und fünf Jahren erhältlich.

Die drei Varianten von Swiss Service Pack

EXKLUSIV FÜR STUDERUS-HÄNDLER

Swiss Service Pack NBD

(next business day)

Vorabaustausch am Folgetag und Konfigurationsservice

Wird ein Vorabaustausch bis 16.00 Uhr bestellt, wird das Ersatzgerät am nächsten Tag bis 9.00 Uhr per Mond-Express der Post geliefert, auch samstags. Die Dauer des Konfigurationsservices ist vom Produktwert abhängig und beträgt 0.5, 1, 2 oder 3 Stunden.

Swiss Service Pack 4h

Vorabaustausch in 4 Stunden und Konfigurationsservice

Studerus sorgt dafür, dass innert 4 Stunden ein Ersatzgerät bei Ihnen vor Ort steht. Die Zustellung erfolgt über einen Kurierdienst. Die Dauer des Konfigurationsservices ist vom Produktwert abhängig und beträgt 0.5, 1, 2 oder 3 Stunden.

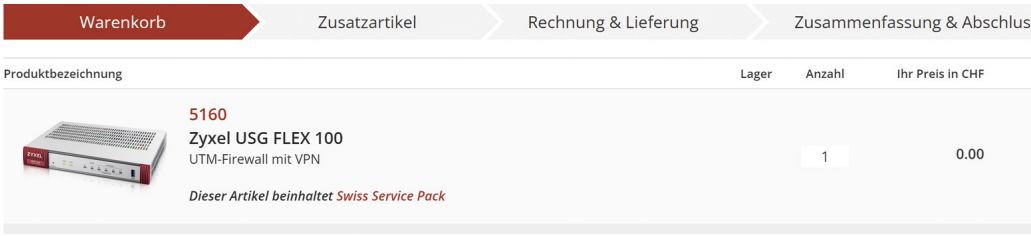
Swiss Service Pack 4h Onsite

Service-Techniker innert 4 Stunden vor Ort und Konfigurationsservice

Studerus organisiert innert 4 Stunden einen Service-Techniker für den Austausch vor Ort. Der Service-Techniker kümmert sich um alles, also auch um die Wiederherstellung der Konfiguration. Die Dauer des Konfigurationsservices ist vom Produktwert abhängig und beträgt 0.5, 1, 2 oder 3 Stunden.

Wie erkenne ich, ob Swiss Service Pack dabei ist?
Achten Sie auf Ihren Dokumenten wie Auftragsbestätigung oder Rechnung bzw. im E-Shop auf den Vermerk «Dieser Artikel beinhaltet Swiss Service Pack»!

Wie profitiere ich vom Service?
Rufen Sie unsere Servicenummer an.
Sie können hier Ihren Vorabaustausch anmelden oder, falls Sie den Konfigurationsservice nutzen möchten, einen Termin für die Konfiguration vereinbaren.



Achten Sie in Ihren Dokumenten darauf, ob Sie von Swiss Service Pack profitieren können.

Servicenummer 044 806 51 01

Alle weiteren Infos über Swiss Service Pack finden Sie unter: **www.studerus.ch/ssp**

SUCCESS-STORY

ZYXEL

nebula

morininet.ch

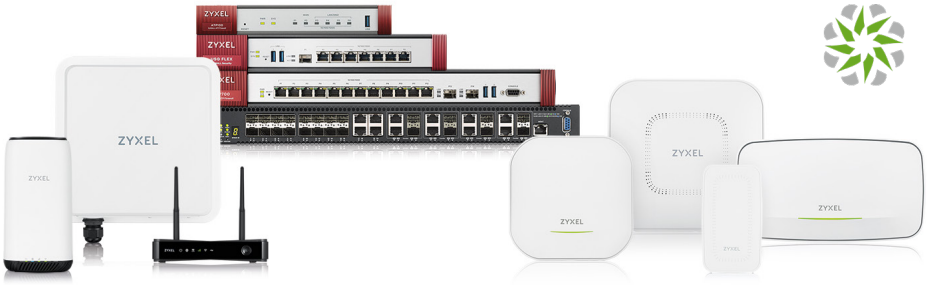
Zyxel Nebula – der Konkurrenz voraus

Viele Hersteller bieten Lösungen für zentrale Netzwerk-Verwaltung an. IT-Dienstleister morininet ag setzt auf die Cloud-Lösung von Zyxel und verrät, welche Vorteile Nebula gegenüber der Konkurrenz hat.

Sie schiessen aus dem Boden wie Pilze im Frühling: Lösungen für zentrale Netzwerk-Verwaltung. Beinahe jeder Hersteller hat mittlerweile ein entsprechendes Produkt im Portfolio. Zyxel hat das Potenzial schon früh erkannt und bereits 2016 mit Nebula die ersten Schritte in diese neue schöne Welt gewagt.

morininet ag setzt auf Nebula

Der IT-Dienstleister morininet ag aus Buchs im Kanton Aargau ist von Nebula überzeugt. Die Firma von Inhaber Loris Morini hatte lange Zyxel-Produkte im Einsatz, wechselte dann aber zu einem anderen Hersteller. «Bei Ubiquiti nutzten wir ebenfalls eine Cloud-Netzwerkmanagement-Lösung», erzählt Loris Morini. Dann wurden sie auf Nebula aufmerksam – und entschieden sich zu einem Wechsel zurück zu Zyxel.



Das gesamte Netzwerk lässt sich mit Nebula in der Cloud verwalten.

«Der Funktionsumfang ist bei der Konkurrenz ähnlich», hält Loris Morini fest. «Das Hinzufügen von Access-Points ist bei Nebula hingegen deutlich einfacher», lobt er. Auch, dass kein zusätzlicher Controller notwendig ist, sei ein Vorteil von Nebula gegenüber vergleichbaren Lösungen.

«Zudem ist es äusserst sinnvoll, möglichst viele Produkte aus einem Haus zu beziehen», erklärt Loris Morini. Zyxel hat die gesamte Netzwerkpalette im Portfolio – und in jeder Kategorie gibt es Nebula-taugliche Produkte.

Was Nebula kann

Fast alle Zyxel-Business-Produkte lassen sich mit Nebula auf einfache Art und Weise zentral verwalten und konfigurieren. Im Gegensatz zu den meisten Mitbewerbern wird bei der Zyxel-Lösung keine zusätzliche Hardware oder Software benötigt. Das NCC (Nebula Control Center) läuft auf europäischen Amazon-Servern, es braucht vor Ort keine zusätzliche Hardware, weder Server noch eine Appliance. Es sind also auch keine mühsamen Server-Updates und Patches notwendig.
Die IT-Dienstleister können von jedem beliebigen Ort mit einer Internetverbindung auf das Nebula Control Center (NCC) zugreifen. Mit einem einzigen Login behält man alle Netzwerke und Kunden im Blick. Man muss sich weder IP-Adressen noch mehrere Logindaten merken. Mit 2-Faktor-Authentifizierung ist eine hohe Sicherheit gewährleistet. Mit einem Mausklick lässt sich der Kunde wechseln und sofort stehen die wichtigsten Daten in einem Dashboard zur Verfügung.

QR-Codes und App

Geräte hinzuzufügen ist mit Nebula denkbar einfach: Einfach mit der Nebula-App den QR-Code auf der Geräteschachtel scannen oder die Seriennummer und MAC-Adresse von Hand eingeben. Nebula-Geräte finden den Weg in die Cloud ohne manuelles Eingreifen – einstecken und fertig. Es ist auch möglich, alle Konfigurationen vorzunehmen, bevor die eigentliche Hardware in Betrieb genommen wird.

Richtig interessant sind auch die Authentifizierungsmöglichkeiten von Nebula. Neben Radius/AD bietet die Zyxel-Lösung auch eine eigene User-Verwaltung, mit der es ohne grossen Aufwand möglich ist, User anzulegen und mit verschiedenen Rechten auszustatten. Auch für das Onboarding von WLAN-Usern bietet die Zyxel-Cloud verschiedene Möglichkeiten. So zum Beispiel Gutscheine zum Ausdrucken (Vouchers) oder DPPSK (Dynamic Personal Pre Shared Key).

Loris Morini sieht wichtigen Pluspunkt

Einen entscheidenden Vorteil von Nebula gegenüber den Mitbewerbern möchte Loris Morini zum Schluss noch erwähnen: «Im Vergleich zur Konkurrenz funktioniert der Support bei Zyxel/Studerus sehr gut.» Das hören wir gerne.

Loris Morini
Geschäftsleiter

Seit 13 Jahren bietet die morininet ag seinen Kunden Lösungen in den Bereichen Informatik und Telematik. Als klassische IT-Dienstleister installieren sie Netzwerke mit On-Premise, Cloud oder gemischten Lösungen – immer so wie es am besten zum Kunden passt. Im Telematik-Bereich wird eine breite Palette von Dienstleistungen von der Alarmanlage über die Videoüberwachung bis zur Telefonanlage angeboten. Die Firma morininet ag betreut vor allem Kunden aus dem KMU-Segment.

Weitere Infos zum Zyxel-Partner:
www.morininet.ch

PUNKT.

044 806 51 00
www.studerus.ch/contact

myclimate neutral Drucksache
myclimate.org/05-22-880876