IdentiFi™

10 Gründe für IdentiFi Wireless von Extreme Networks

BELL COMPUTER-NETZWERKE

Extreme networks

IdentiFi™

1 – Flexible WLAN Architektur 3

2 – Rollenbasierter Zugriff und Richtlinien-Umsetzung 3

3 – Quality of Service 4

4 – High-Performance für High-Density 4

5 – Energieeffiziente Access Points 5

6 – Zusätzliche Funktionalitäten ohne zusätzliche Kosten 5

7 – Überzeugendes netzwerkübergreifendes Model 5

8 – Die umfassendste WLAN Access Point Garantie der Branche 6

9 – Zentralisiertes Management für Transparenz und Kontrolle (Optional verfügbar durch Netsight) 6

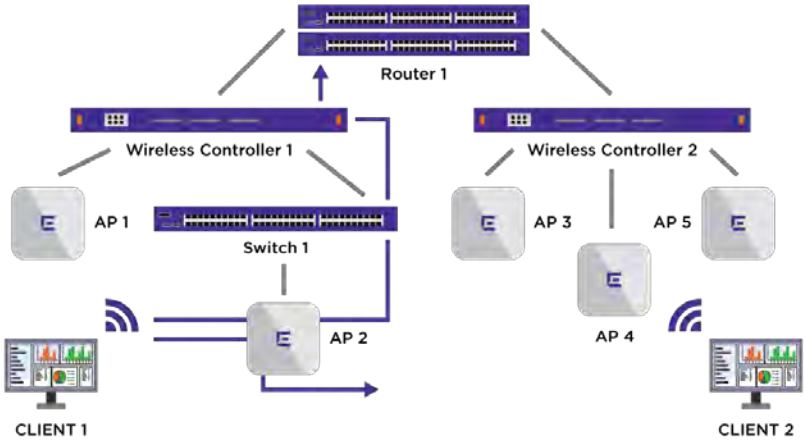
10 – Transparenz und Optimierung von Applikationen (Optional verfügbar durch NetSight und Purview) 7

Die nachfolgenden Punkte zeigen die Hauptmerkmale sowie die fortschrittlichen Funktionalitäten und Features der IdentiFi Wireless Lösung auf.

1. Flexible WLAN Architektur

Die Extreme Networks IdentiFi Wireless Lösung bietet die branchenweit flexibelste Architektur – auf ein und derselben SSID kann der Client-Datenfluss direkt am Access Point oder am Controller erfolgen. Nur Extreme Networks bietet diese einzigartige Möglichkeit, verschiedene Datenpfade innerhalb einer SSID zu unterstützen. Weiterhin können auch unterschiedliche Datenpfade je Client gewählt werden. Die weiteren Merkmale der Lösung beinhalten:

- Versendung des Datenverkehrs und Filterung nach Richtlinien (Policies) direkt am Access Point
- Load Balancing, Band Steering, Band Preferencing und Airtime Fairness werden unabhängig vom Controller und von den Endgeräten am Access Point durchgeführt, was eine optimierte RF-Umgebung sicherstellt, auch wenn der Control-Link nicht aktiv ist
- Unterstützung von RADIUS Authentifizierung, Roaming und Policy-Kontrolle direkt am Access Point und ohne auf den Controller zugreifen zu müssen
- Controller als Hardware oder als virtuelle Appliance verfügbar und somit je nach Kundenanforderungen flexibel gestaltbar



2. Rollenbasierter Zugriff und Richtlinien-Umsetzung

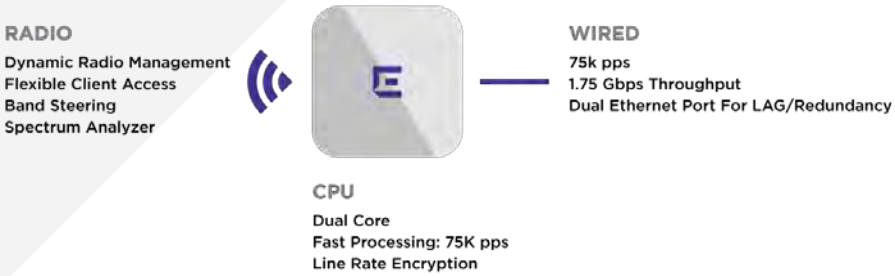
IdentiFi Wireless liefert rollenbasierte Richtlinien (Policies), womit Security, NAC, Mobility und QoS-Priorität auf einer per User-Ebene implementiert werden können. Sobald sich ein User oder Gerät authentifiziert hat, greift eine - zentral definierte - Policy am lokalen Access Point und liefert somit Intelligenz direkt am Edge-Bereich eines Netzwerks. Die Policy sorgt für eine sehr detaillierte Kontrolle über den Zugriffsbereich eines Users oder Gerätes. Die Policy ist außerdem nicht an ein VLAN, sondern an den User oder das Gerät geknüpft und folgt diesem bei seiner Bewegung durch das Netz hinweg. Desweiteren kann sich eine Policy für ein und den selben User dynamisch anpassen, je nach Aufenthaltsort, Gerätetyp und/oder Tageszeit. Dieses Policy-Konzept ist ganzheitlich und homogen auf allen aktuellen Extreme Networks Produkten (wired & wireless) verfügbar.

3. Quality of Service

Dynamische Provisionierung und dynamisches Policy-Management sorgen für einfach umzusetzende Regeln, die wiederum verschiedene Dienste und Zugriffe über die gesamte Infrastruktur hinweg differenzieren und priorisieren. Somit werden Anwendungsverfügbarkeit, Service Level Agreements und die sog. Quality-of-Experience für kritische Daten, Voice und Video-Anwendungen basierend auf Nutzer, Geräte, Orte, Uhrzeiten und Unternehmensanforderungen garantiert.

4. High-Performance für High-Density

Die IdentiFi 802.11ac WLAN Access Points sind so gestaltet, dass sie die beste Performance liefern während zeitgleich mögliche Engpässe aus den drei folgenden Bereichen minimiert werden:



RADIO

Anstelle eines Standard-Chipsatzes wurden bei IdentiFi spezielle Software-Features entwickelt, die für eine zuverlässige Performance in der Luft sorgen:

- Dynamic Radio Management sorgt für eine optimale Kanal- und Leistungsplanung
- Flexible Client Access sorgt für einen optimalen Durchsatz in einer gemischten Client-Umgebung (802.11 a/b/g/n/ac)
- Band Steering steuert die Clients und ermöglicht, dass sich diese bevorzugt im leistungsstärkeren und weniger störungsanfälligen 5GHz Frequenzband einbuchen
- Spectrum Analysis identifiziert RF Störungen und Störquellen

CPU

IdentiFi nutzt einen energieeffizienten und leistungsstarken Dual Core Prozessor, der für eine extrem schnelle Verarbeitung von Datenpaketen sorgt. Zusätzlich dazu gibt es einen dedizierten Netzwerk-Prozessor (NPU), der die Leistung der zu verarbeitenden Datenpakete um bis zu 25% steigert. Ebenso wird eine Hardware-basierte Verschlüsselung unterstützt, um somit die Kapazität der Backplane für eine Ende-zu-Ende Verschlüsselung zu maximieren.

KABELGEBUNDENER TEIL DER ACCESS POINTS

Die Software und Hardware von IdentiFi unterstützt einen Gesamtdurchsatz von 1,75 Gbps bei einer aktuellen Kapazität von 75.000 Paketen (verschiedener Größen) pro Sekunde. Dual Ethernet Ports sorgen via Link Aggregation (LAG) für erhöhte Datenkapazität und Redundanz bei fehlerhaften Kabelverbindungen und somit für eine Aufrechterhaltung des Dienstes.

5. Energieeffiziente Access Points

Die IdentiFi WLAN Access Points leisten die vollen 802.11n oder ac Datenraten über den PoE Standard 802.3af.

6. Zusätzliche Funktionalitäten ohne zusätzliche Kosten

Die hochwertigen Wireless-Funktionen wie Hochverfügbarkeit, Mobility und Gastzugang können direkt genutzt werden – keine zusätzlichen Lizenzen sind erforderlich. Durch das vereinfachte „Pay-as-you-grow“ Lizenzmodell kann außerdem auch sehr schnell auf Vergößerungen der WLAN Umgebung eingegangen werden. Beinhaltet sind beispielsweise der Hochverfügbarkeitsmodus, der für eine Redundanz der Controller sorgt – im Falle eines Ausfalls übernimmt der zweite Controller die volle Funktionaliät, ohne das eine spezielle Lizenz erforderlich ist. Zudem können alle Access Points auch unabhängig vom zentralen Controller betrieben werden, was wiederum in WLAN Designs, wo die Wide Area Verbindung ein einschränkender Faktor ist, von Vorteil ist. Der Datenverkehr zwischen dem Access Point und dem Controller kann AES-verschlüsselt sein und somit die Nutzung von ungesicherten WANs wie dem Internet erlauben. IdentiFi unterstützt VoWLAN Umgebungen und ist mit den führenden Voice-over-WLAN Telefonherstellern wie u.a. Unify, Ascom, Polycom und Vocera zertifiziert.

7. Überzeugendes netzwerkübergreifendes Model

Eine standardbasierte Architektur sorgt für den bestmöglichen Einsatz von Netzwerkkomponenten und somit für Senkung der Betriebskosten bei gleichzeitiger Steigerung der Effizienz – ganz gleich ob es sich um eine komplette Extreme Networks Infrastruktur, bestehend aus Data Center, Core, Distribution oder Edge/Access Lösungen, oder aber um eine Netzwerk, bestehend aus Komponenten verschiedener Hersteller handelt. Die Extreme Networks Lösungen senken Anschaffungs- und Betriebskosten durch hohe Sicherheit, Einfachheit, Skalierbarkeit, Flexibilität und volle Kontrolle.

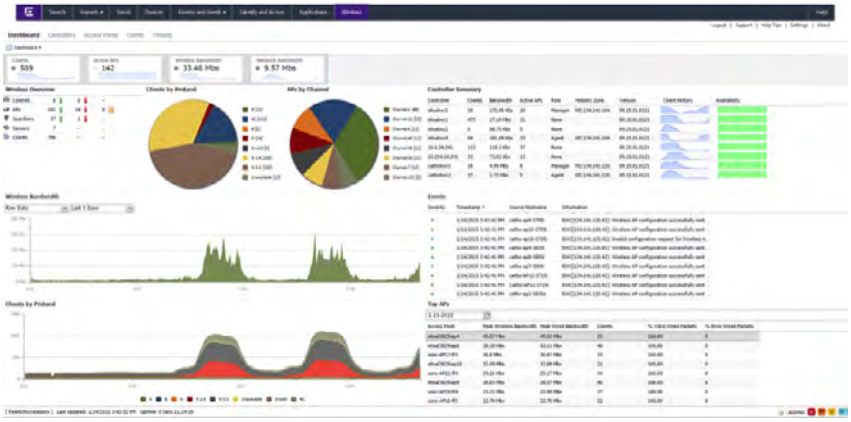
OneFabric™

8. Die umfassendste WLAN Access Point Garantie der Branche

Die Lifetime Warranty für alle Indoor Access Points von Extreme Networks beinhaltet eine Ersatzlieferung am nächsten Tag, ein Jahr lang kostenfreie Firmware Updates und Upgrades (für den Zeitraum danach gibt es Updates über den zugehörigen Controller) und Support während der Geschäftszeiten (8x5) durch das erfahrenste Support-Center der Branche.

9. Zentralisiertes Management für Transparenz und Kontrolle (optional verfügbar durch NetSight)

Netsight ist das Herzstück der Extreme Networks Management und Security Produktlinie OneFabric Control Center. Diese Lösung bietet Transparenz und Kontrolle über das gesamte Hardware- und Software-Portfolio hinweg – intuitiv, automatisiert und einfach zu verwalten. Netsight liefert einen Überblick über das gesamte kabellose und kabelgebundene Netzwerk und Dritthersteller – vom Data Center bis hin zum Endgerät – und sorgt somit für eine Vereinfachung des Betriebes, geringeren Aufwand für das Netzwerkmanagement sowie Steigerung der Produktivität der IT und des einzelnen Nutzers.



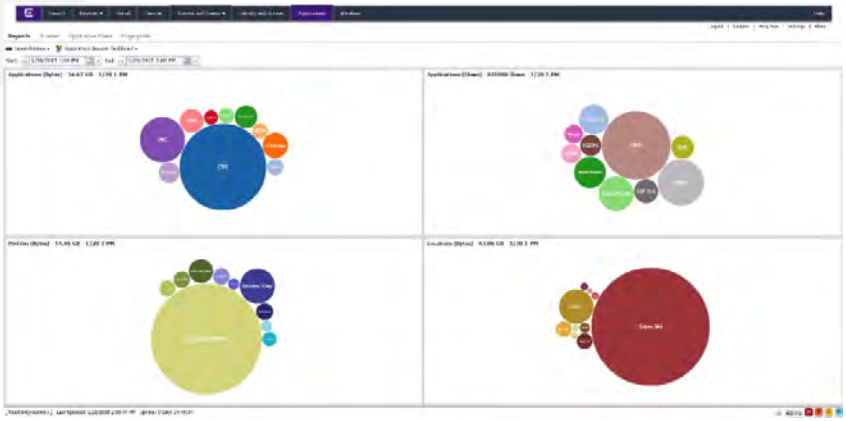
Proaktive Security (optional verfügbar durch die Identity & Access/NAC Lösung)

- Schützt Unternehmensdaten durch proaktive Verhinderung des Netzwerkzugriffs durch nicht-autorisierte Nutzer, geschädigte Zugangspunkte oder andere ungeschützte Systeme
- Proaktive Kontrolle des Security-Status eines jeden Gerätes im Netzwerk, inkl. mitarbeitereigener Geräte (BYOD)

Beobachtung, Limitierung und Sperrung von bestimmten Webseiten oder Anwendungen, basiert auf Nutzer, Gerätetyp, Standort und Uhrzeit.

10. Transparenz und Optimierung von Applikationen (optional verfügbar durch Netsight und Purview)

Purview – als Bestandteil von Netsight – bietet Netzwerkadministratoren eine einzigartige Ansicht über das Nutzerverhalten im WLAN. Dies geschieht durch die Integration einer Appliance, die mehr als 6.000 Applikationen mit mehr als 13.000 Applikationsprofilen („Fingerprints“) identifizieren kann. Diese sind bereits heute standardmäßig inkludiert und können je nach Kundenanforderung bearbeitet und erweitert werden. Purview entdeckt zum einen unerwünschte Applikationen im Netzwerk und analysiert zum anderen die Reaktionszeiten von Applikationen und dem Netzwerk selbst, was speziell für unternehmenskritische Anwendungen von Vorteil ist, da man das Netzwerk somit proaktiv verwalten. Probleme werden entdeckt, bevor sie akut werden und den Nutzer beeinträchtigen. Durch den Einsatz von CoreFlow-Geräten (K- oder S-Serie) von Extreme Networks kann Purview auch auf das kabelgebundene Netzwerk erweitert werden – entweder als Lösung innerhalb des eigenen Netzwerks oder als Overlay zu einem Netzwerk mit Komponenten eines Drittherstellers.



http://www.extremenetworks.com/contact / Phone +1-408-579-2800

©2015 Extreme Networks, Inc. All rights reserved. Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names are the property of their respective owners. For additional information on Extreme Networks Trademarks please see http://www.extremenetworks.com/company/legal/trademarks. Specifications and product availability are subject to change without notice. 9810-0715-08