ANYFI GATEWAY

DATASHEET

KEY BENEFITS

- Unique architecture moves IEEE 802.11 authentication and encryption to the gateway, ensuring end-to-end security even if the Wi-Fi access point cannot be trusted.
- Compatible with any Wi-Fi access point or residential gateway integrating Anyfi.net software.
- Easy to integrate in a 3GPP Trusted WLAN Access Network *(TWAN),* or to operate standalone.
- Wide selection of supported hardware platforms and hypervisors.
- Network Function Virtualization *(NFV)* ready.
- Based on the tried and tested Vyatta Network OS with support for advanced routing, tunneling and security – all from a well-documented and easy to use CLI.

KEY PERFORMANCE METRICS

- Up to 10 Gbps IEEE 802.11 CCMP (AES128 encryption/decryption with integrity check).
- SDWN architecture with just-in-time resource allocation means one Gateway can serve an unlimited number of Wi-Fi access points.

RELATED SOLUTIONS

- Secure mobile offload with SDWN App MOBILE
- Traditional hotspots & homespots with SDWN App HOTSPOT

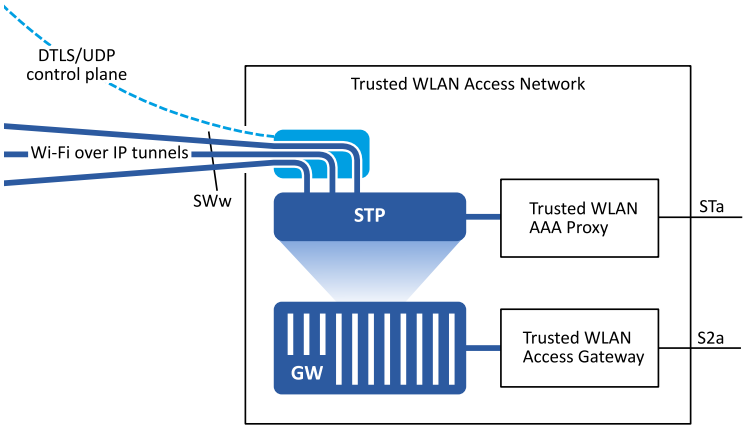
LICENSING OPTIONS

- Free community & evaluation license
- One-time or recurring commercial licenses
- Brocade Vyatta vRouter or Vyatta Core

OVERVIEW

The SDWN architecture partitions the IEEE 802.11 stack into three parts: a low-level radio portion that runs on the access point and handles the real-time aspects of the Wi-Fi protocol, a high-level portion that performs the security processing and a Controller that connects the previous two through an IEEE 802.11 over UDP/IP data plane tunnel.

The Gateway implements that high-level portion of the IEEE 802.11 stack and lets operators terminate tunnels on a massive scale. It can be deployed in the core network or in a data center, on physical hardware or as a virtual machine.



The Gateway integrated in a 3GPP Trusted WLAN Access Network: Authenticating WLAN UE using RADIUS towards the Trusted WLAN AAA Proxy (TWAP) and bridging Ethernet frames between WLAN UE and the Trusted WLAN Access Gateway (TWAG) the Gateway serves a similar role to that of an access point (AP). RADIUS is also used for change of authorization (CoA) and accounting.

FOR MOBILE OPERATORS

3GPP makes a clear distinction between trusted and untrusted WLAN access. Question is, can you really trust access points that may be under the physical control of an attacker? The SDWN architecture lets you answer that question in the negative, while still integrating into them into the network as a trusted non-3GPP access.

How is that possible? By extending the SWw interface *(IEEE Std 802.11)* over the backhaul and terminating it in the Gateway you remove the access point from the security equation: even an attacker with complete control over the access point can only get to the encrypted IEEE 802.11 frames *(SWw)* – which are also available on the air interface.

ANYFI GATEWAY

DATASHEET

NORTHBOUND INTERFACES
- Vyatta CLI
- SNMP v2c
- RADIUS *(RFC2865, RFC2866, RFC2868, RFC2869, RFC3579, RFC4849, RFC5176)*
- SDWN control plane *(DTLS/UDP/IP)*

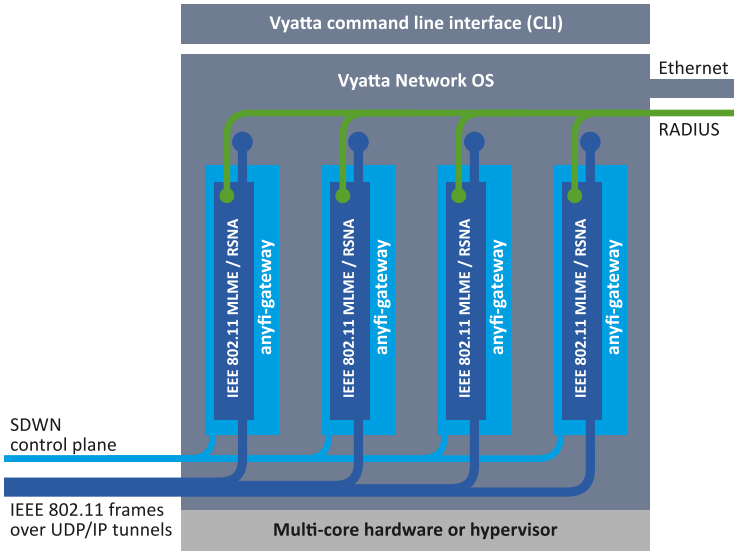
WESTBOUND INTERFACES
- IEEE 802.11 over UDP/IP *(3GPP SWw)*

EASTBOUND INTERFACES
- Ethernet / Dynamic VLAN / L2oGRE / IP

CONFIGURABILITY
- IEEE 802.11 SSID
- IEEE 802.11 Auth Protocol *(WPA/RSN/FT)*
- IEEE 802.11 Auth Mode *(PSK/EAP)*
- IEEE 802.11 Encryption *(CCMP/TKIP)*
- IEEE 802.11 Preauthentication On/Off
- IEEE 802.11 Group Rekey Interval
- IEEE 802.11 Strict Rekey On/Off
- RADIUS authentication server
- RADIUS accounting server
- Vyatta CLI for eastbound processing

KEY FEATURES
- EAP-SIM/AKA/AKA'/TLS/TTLS/PEAP etc.
- PMK key caching *(FT, PMKSA caching, OKC)*
- Load balancing
- Automatic failover

HARDWARE OPTIONS
- VMware, Xen, XenServer and Red Hat KVM hypervisors
- Bare metal x86 hardware



Internal architecture of the Gateway: Incoming IEEE 802.11 over UDP/IP tunnels are terminated on a configurable number of CPU cores, and the resulting Ethernet frames are handed over to Vyatta for further eastbound processing (e.g. bridging, L2oGRE tunneling or IP routing).

FOR FIXED-LINE OPERATORS

The Gateway can also be used to terminate the IEEE 802.11 protocol for an open or EAP protected virtual network, thereby enabling integration of traditional hotspots and homespots into the same unified SDWN architecture.

The power and expressiveness of the Vyatta Network OS command line interface *(CLI)* can be used in this context to implement DHCP, IP gateway and even advanced BGP routing on the Gateway. With detailed RADIUS accounting originating directly from the IEEE 802.11 frame processing you can ensure full traffic traceability and mobility awareness.

By migrating existing homespot and hotspot deployments to a unified SDWN architecture operators can realize all the associated benefits of improved security, quality of service, monitoring and network agility – without changing how users connect to the network and authenticate.

About Anyfi Networks

Anyfi Networks is the company behind the revolutionary Software Defined Wireless Networking (SDWN) architecture. Based on this unique technology we offer broadband operators, fixed as well as mobile, a range of carrier Wi-Fi software solutions: from traditional hotspots and homespots all the way to massively scalable secure mobile Wi-Fi offload. For more information please visit www.anyfinetworks.com or contact sales@anyfinetworks.com.

Anyfi Networks

Carrier Wi-Fi That Just Works