Stampede

Technical Datasheet – SNAPguard

Plug-and-play cloud solution for optimum guest Wi-Fi experiences.

Overview

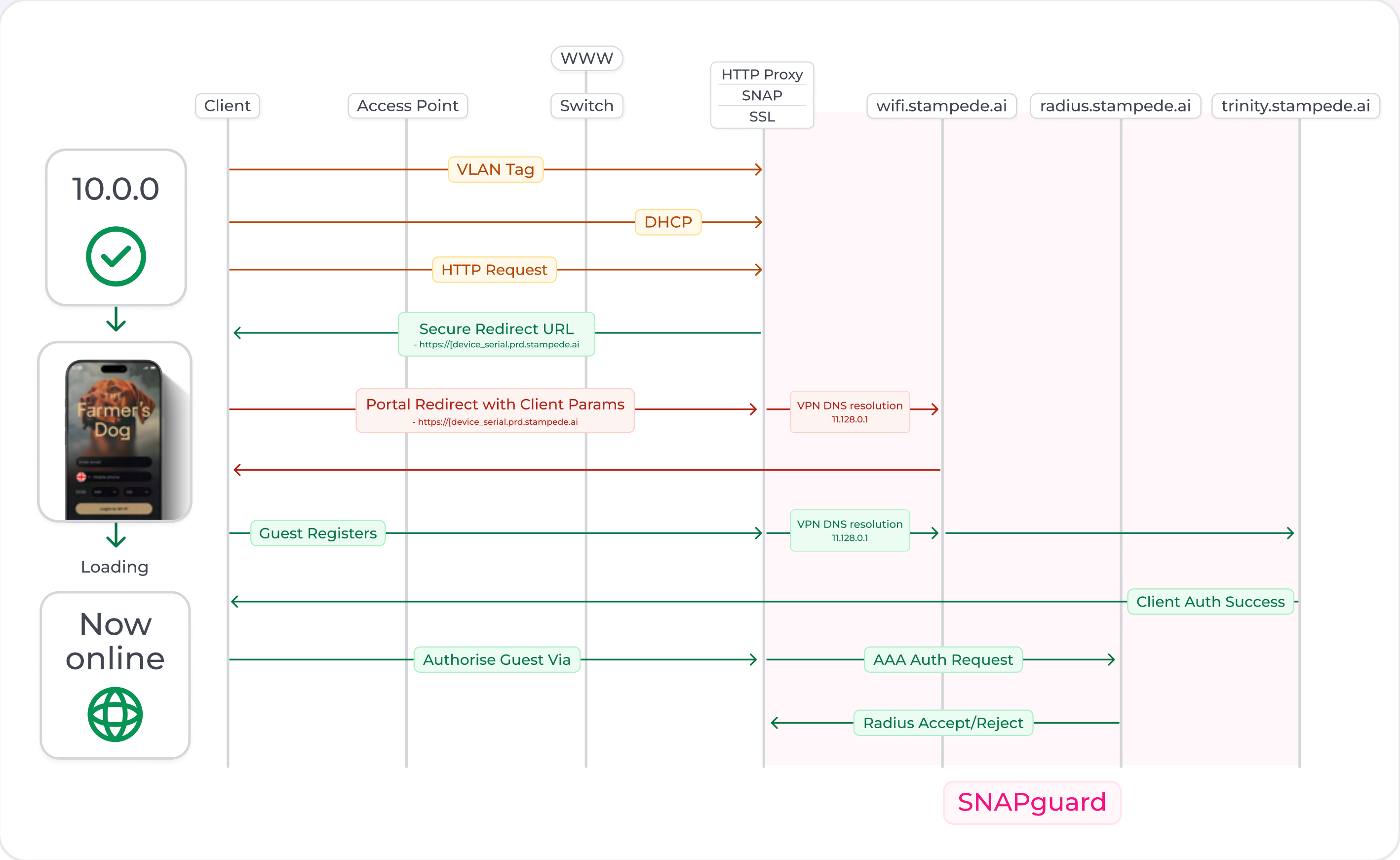
SNAPguard is the secure delivery, control and optimisation layer that underpins Stampede's Guest Wi-Fi. It is purpose-built for the operational realities of hospitality environments where reliability, performance and simplicity matter more than complex enterprise networking.

SNAPguard transforms guest Wi-Fi from a fragile, inconsistent service into a managed infrastructure that is fast, predictable and secure – even during peak trading periods. It does this by combining a pre-provisioned, on-site gateway with a virtual cloud network, giving Stampede direct control over how guest devices authenticate, connect and behave on the network.

SNAPguard is currently implemented using MikroTik ax2 devices, supplied pre-configured and ready to install. Alternative MikroTik models may be deployed depending on venue size, traffic volumes and performance requirements. The SNAPguard device sits locally within the venue between the guest Wi-Fi VLAN and the Stampede cloud.

By running a full server locally inside the venue, SNAPguard removes reliance on fragile access-point splash pages and third-party redirect logic. This allows Stampede to control captive portal behaviour end-to-end, supporting next-generation standards such as DHCP Option 114 and resolving common Apple and Android auto-login failures that affect traditional guest Wi-Fi deployments.

How SNAPguard Delivers Reliable Guest Wi-Fi



SNAPguard Combines Local Intelligence With Centralised Cloud Control:

- ✓ Runs a full local authentication and captive portal server inside the venue.
- ✓ Supports DHCP Option 114 for modern Apple and Android captive portal behaviour.
- ✓ Caches captive portal assets and Stampede modules locally to reduce latency.
- ✓ Runs local DNS and SSL services, allowing SNAPguard to resolve stampede.ai domains without external cloud lookups.
- ✓ Securely routes all guest traffic through an outbound VPN tunnel to the Stampede cloud.
- ✓ Avoids double NAT and inbound firewall dependencies, simplifying deployment and reducing failure points.

Performance & Reliability

The result is a dramatically smoother and more reliable guest experience. Login screens appear automatically and consistently across modern Apple and Android devices, and most guests are authorised in under one second, even during busy service periods or on low-bandwidth connections.

Local caching, low-latency routing and on-device services reduce reliance on external infrastructure, minimising failures during peak usage. Faster, more reliable access reduces staff intervention, increases successful logins and improves opt-in rates at the moment of connection.

True Plug-And-Play Deployment

Because SNAPguard avoids double NAT and inbound firewall rules, it delivers true plug-and-play deployment. Devices are shipped to venues pre-configured and can be installed quickly with minimal on-site setup, reducing configuration errors and eliminating the need for specialist networking expertise.

At the same time, SNAPguard provides cloud-based access to the local area network, allowing IT teams and managed service providers to see connected devices, traffic behaviour and network health remotely, without requiring physical access to the venue.

A Secure Operational Foundation

Beyond connectivity, SNAPguard provides the operational and security foundation that makes guest Wi-Fi safe, scalable and compliant. It enforces clean separation between guest and operational networks, protects venues from misuse, illegal activity and performance abuse, and supports GDPR and safeguarding requirements.

SNAPguard devices automatically update with security patches and platform enhancements, meaning the system continuously improves over time without manual intervention or site visits.

Operational Controls Designed For Hospitality

Flexible session timeouts: Keep hotel guests authorised for the duration of their stay, or enforce timed re-authentication in cafés and bars to encourage repeat purchases.

Bandwidth fairness & rate controls: Apply session limits and bandwidth policies (e.g. locals vs transient guests) to prevent individual devices from degrading performance for others.

Always improving, always secure: Automatic security patches and feature updates ensure SNAPguard remains protected and evolves over time.

Compliance & Platform Assurance

iOS & Android Captive Portal Compliant

Ensures login screens reliably appear automatically on guest devices.

GDPR-Ready by Design

Supports consent-based data capture, audit logging and secure handling of guest data.

Enterprise Security Standards

Aligned to ISO 27001, SOC 2 controls and Cyber Essentials.

Hospitality-Safe Network Separation

Protects POS, staff systems and CCTV while supporting insurer and safeguarding expectations.

SNAPguard – Features & Benefits

Feature	Benefit
Enterprise-Grade Routing & Security Built on MikroTik RouterOS, SNAPguard provides professional-grade routing, firewalling, VPN, VLAN segmentation, traffic shaping and WPA3 support.	Stable, secure network performance suitable for high-traffic hospitality environments.
Simplified Setup (No Double NAT) Eliminates the need for access-point splash pages, walled gardens, RADIUS servers or double NAT configurations, enabling true plug-and-play deployment.	Faster installs, fewer setup errors and reduced IT overhead.
Improved Captive Portal Reliability Gives Stampede full control over captive portal redirects and authentication behaviour, resolving Apple and Android auto-login issues.	Login screens appear reliably, reducing guest frustration and staff intervention.
Performance Gains via Local Caching Captive portal assets and Stampede modules are cached locally on the SNAPguard device.	Faster splash pages, near-instant authorisation and consistent performance during peak periods.
Secure VPN Tunnelling All guest traffic is routed through a secure outbound VPN tunnel to the Stampede cloud.	Encrypted data transfer without inbound firewall exposure.
Virtual Cloud Network (Always On) Each SNAPguard device connects into Stampede's virtual cloud network for persistent control, monitoring and policy enforcement.	Centralised management and consistent behaviour across single venues or multi-site estates.
Mission Control Monitoring Integrates with Stampede Mission Control to monitor network health and connected operational devices such as EPOS, printers and CCTV.	Faster fault detection, proactive alerts and improved operational continuity.
Rogue Device & Misuse Detection Identifies suspicious devices, abnormal behaviour and potential misuse on guest networks.	Improved security posture and protection of venue reputation.
MAC Randomisation Handling Designed to accommodate modern device MAC randomisation behaviour.	More reliable repeat-visit recognition and smoother re-authentication flows.
Multi-SSID & Role-Based Separation Supports multiple SSIDs and VLANs for guest, staff and operational traffic.	Clean network isolation without complex configuration.
Automatic Updates & Continuous Improvement SNAPguard devices automatically receive security patches and platform updates.	A future-proof solution that improves over time without manual intervention.

SNAPguard Device Technical Specification

SPECIFICATIONS

Make and model	MikroTik hAP ax2
Product code	C52iG-5HaxD2HaxD-TC
Architecture	ARM 64bit
CPU	IPQ-6010
CPU core count	4
CPU nominal frequency	864 MHz
CPU Threads count	4
Switch chip model	IPQ-6010
RouterOS license	4
Operating System	RouterOS v7
Size of RAM	1 GB
Storage size	128 MB
Storage type	NAND
MTBF	Approximately 100'000 hours at 25C
Tested ambient temperature	-40°C to 50°C

WIRELESS CAPABILITIES

Wireless 2.4 GHz Max data rate	574 Mbit/s
Wireless 2.4 GHz Number of chains	2
Wireless 2.4 GHz standards	802.11b/g/n/ax
Antenna gain dBi for 2.4 GHz	4
Wireless 2.4 GHz chip model	QCN-5022
Wireless 2.4 GHz generation	Wi-Fi 6
Wireless 5 GHz Max data rate	1200 Mbit/s
Wireless 5 GHz Number of chains	2
Wireless 5 GHz standards	802.11a/n/ac/ax
Antenna gain dBi for 5 GHz	4.5
Wireless 5 GHz chip model	QCN-5052
Wireless 5 GHz generation	Wi-Fi 6
WiFi speed	AX1800

ETHERNET

10/100/1000 Ethernet ports	5
Number of 1G Ethernet ports with PoE-out	1

POWERING

Number of DC inputs	2 (DC jack, PoE-IN)
DC jack input Voltage	12-28 V
Max power consumption	27 W
Max power consumption without attachments	12 W
PoE in	Passive PoE
Cooling type	Passive
PoE in input Voltage	18-28 V

SNAPguard Device Technical Specification

POE-OUT

PoE-out ports	Ether 1
PoE out	Passive PoE
Low voltage PoE-Out current limit	600 mA
Max total out (A)	0.6 A
Total output current	0.6
Total output power	16.8W

CERTIFICATION & APPROVALS

Certification	CE, FCC, IC, EAC, ROHS
IP	20

OTHER

CPU temperature monitor	Yes
Mode button	Yes

INCLUDED PARTS

hAP case base

K-47 wall mount set

24V 1.2A power supply
(straight plug)

NOTE

The device includes free software updates for the life of the product or a minimum of 5 years starting from date of purchase.

IPsec Test Results

IPG-4010 IPsec throughput		IPG-4010 IPsec throughput					
Mode	**Configuration**	**1600 byte**		**512 byte**		**64 byte**	
		kpps	**Mbps**	**kpps**	**Mbps**	**kpps**	**Mbps**
Single tunnel	AES-128-CBC + SHA1	78.4	878.1	91.9	376.4	93.6	47.9
256 tunnels	AES-128-CBC + SHA1	50.1	561.1	55.5	227.3	58.6	30
256 tunnels	AES-128-CBC + SHA256	50	560	55.4	226.9	58.4	30
256 tunnels	AES-256-CBC + SHA1	49.4	553.3	54.8	226.5	58.4	30
256 tunnels	AES-256-CBC + SHA256	49.4	553.3	55	225.3	58.6	30

1. All tests are done with Xena Networks specialized test equipment (XenaBox), and done according to RFC2544 (Xena2544)
2. Max throughput is determined with 30+ second attempts with 0.1% packet loss tolerance in 64, 512, 1600 byte packet sizes
3. Test results show device maximum performance, and are reached using mentioned hardware and software configuration, different configurations most likely will result in lower results

Wireless Specification

2.4 GHz	Transmit (dBm)	Receive Sensitivity
1MBit/s	27	-108
11MBit/s	27	-94
6MBit/s	27	-94
54MBit/s	25	-80
MCS0	27	-94
MCS7	24	-75
MCS9	22	-70
MCS11	20	-67

5 GHz	Transmit (dBm)	Receive Sensitivity
6MBit/s	26	-94
54MBit/s	23	-80
MCS0	26	-94
MCS7	22	-75
MCS9	20	-70
MCS11	18	-67

Ethernet Test Results

C52iG-5HaxD2HaxD-TC		IPQ-6010 all port test					
Mode	**Configuration**	**1518 byte**		**512 byte**		**64 byte**	
		kpps	**Mbps**	**kpps**	**Mbps**	**kpps**	**Mbps**
Bridging	none (fast path)	216.6	2630.4	591.5	2429.8	1366.2	743.2
Bridging	25 bridge filter rules	216	2622.7	342.5	1402.7	347	188.8
Routing	none (fast path)	216.6	2630.4	590.9	2420.3	1215.6	659.7
Routing	25 simple queues	215.7	2620	327.6	1341.8	350.3	190.6
Routing	25 ip filter rules	216.2	2625.1	222.9	912.9	225.1	122.4

1. All tests are done with Xena Networks specialized test equipment (XenaBox), and done according to RFC2544 (Xena2544)
2. Max throughput is determined with 30+ second attempts with 0.1% packet loss tolerance in 64, 512, 1518 byte packet sizes
3. Test results show device maximum performance, and are reached using mentioned hardware and software configuration, different configurations most likely will result in lower results

Useful Links:

Listing on Mikrotik Website Declaration of Conformity (DoC) Block Diagram User Manual Quick Guide

Stampede

Designed For Hospitality. Built For Growth.