

The **Q-NAC**® is an amalgamation of a number of open source software packages, listed below, running on an extremely small form factor, low-power-consumption server. The **Q-NAC** provides Network Access Control (“NAC”) using **PacketFence**. Network Access Control is among the first lines of defense for network security.

**PacketFence** is a fully supported Open Source Network Access Control (NAC) solution. Among its features: flexible VLAN management and Role-Based access control; Guest Access (BYOB); Portal Profiles; Built-in Violation Types to prevent unauthorized access to network resources; Automatic Registration; PKI and EAP-TLS support.

Also includes expiration of credentials management; Device Management; Firewall Integration; Bandwidth Accounting; Floating Network Devices control; Microsoft Active Directory Integration; Routed Networks; Pass Through; High Availability (HA); Standards Based to prevent vendor lock-in; and widely Supported Hardware.

The **Q-NAC** can be used to gradually deploy NAC and is both extensible and easily customized for individual networks.



• **Q-NAC Hardware Specifications:**

- 108 mm x 64 mm x 26 mm – 170 grams  
(4.25" x 2.50" x 1.125" – 6 oz)
- Power consumption under full load:  
12 watts, 120v-240v
- No fan or any moving parts. Must be installed in a well-ventilated space.
- Operates 0°C–70°C (32°F–158°F)

**LED indicators:**

- Power
- Link (physical connection to network)
- Activity (network traffic)
- 1000 mbps (gigabit) NIC connection
- Dual Band WiFi. (2.4 GHz & 5 GHz)

The **Q-NAC** includes:

- **ntop-ng – ntop-ng** (“**ntop next generation**”) is the latest iteration of ntop, which is used to probe all network traffic. Some of its features include showing realtime network traffic and hosts; create long term reports for network throughput, application and application protocols; monitor and report live throughput, network and application latencies, RTT, and full TCP stats.

Additionally it will discover application protocols (e.g. Facebook, BitTorrent, etc.) by leveraging nDPI (ntop Deep Packet Inspection); characterize HTTP traffic using characterization services provided by Google and HPPT Blacklist; provide geolocation mapping of hosts; sort all network traffic via criteria including IP address, port, L7 protocol, throughput, Autonomous Systems (ASs); analyze IP traffic and sort by source and destination; IPv6 support; full Layer 2 support, including ARP stats; and an alerts engine to capture anomalous and suspicious hosts.

- **PacketFence<sup>®</sup> – PacketFence<sup>®</sup>** is the leading open source, enterprise-class, Network Access Control solution. In addition to Network Access Control, **PacketFence** has built-in High Availability (HA). **Q-NAC** appliances can be clustered for failover and load balancing.
- **ModSecurity<sup>®</sup> – ModSecurity<sup>®</sup>** (“**ModSec**”) is the leading open source Web Application Firewall (WAF) for cross-scripting attack protection. We have hardened the **Q-NAC**’s built-in Apache web server to prevent conceivable attacks.
- **ClamAV<sup>®</sup> – ClamAV<sup>®</sup>** is the leading open source anti-virus software package.
- **Tiny Honeypot (THP) - THP** fools attackers by making it appear that the attack is working, while meanwhile logging the attack info. **THP** wastes an attacker’s time, and creates an opportunity to detect the network intrusion by offering to the attacker what appears to be thousands of services.
- **Webmin – Webmin** is the leading open source Web GUI package for server configuration and maintenance. **Webmin** also allows for the linkage of multiple **Q-NAC** appliances for simplified administration.

The **Q-NAC** is completely administered through a Web GUI. All package usage is via Web interfaces, thereby opening up sophisticated intrusion detection, network forensic analysis, and network monitoring to even novice network administrators. No Command Line Interface (CLI) or Linux skill is required.

The **Q-NAC** has both a Gigabit (1000 mbps) NIC and 802.11 Dual Band WiFi. (2.4 GHz and 5 GHz.) Intrusion detection can be set up on either network interface.

The **Q-NAC** is also available as a Virtual Machine (VM).

Using the provided **Webmin** module, two-factor authentication can be added using **Google Authenticator** or **Aauthy**, a commercial service with its own app. **Google Authenticator** runs on Android, IOS, and Blackberry devices, and uses the standard TOTP protocol.

Notifications are provided by e-mail using **SendMail**, which is configured with a module in **Webmin**, and syslog entries. SMS notification is available as an option. The **Q-NAC** can also be integrated with the **Q-Log**® network appliance or any other Syslog or SIEM (Security Information and Event Management) solution, including the **Q-OSSEC**®, as well as monitored via the **Q-BOX**®.

*Q-NAC® and all registered trademarks above are property of their respective owner(s).*