Small Business VPN device

Project specification

Copyright Schmied Enterprises LLC 2022 **Have business? hq@schmied.us**

Schmied Enterprises LLC is working on the VPN device below.

Summary

Remote work is a considerable option for many businesses. Commercial VPN products have many limitations for remote workers.

Extensive configuration, expensive software maintenance of kernel based solutions requires expert staff.

Our solution is optimized to do the job but reduce costs, and it does not require extra IT staff to maintain.

Product requirements

- Target audience is non-technical small businesses.
- Low maintenance solution.
- Provides VPN access to a corporate cloud console.
- Hardware only solution.
- No software configuration required.
- Private key encryption distributed on physical media.
- No password or extra PIN is required.
- Forwards only corporate traffic - L3 VPN.
- It is not a replacement for L2 IP masking.
- Primary target base is remote work not cloud browsing.

Business requirements

- Target audience is US small business.
- Target quantity is 10K.
- Target retail price is $100 excluding sales tax.
- R&D limit 10% of project, Marketing & sales limit 20% of project.
- Seeking for offers for hardware & case R&D.
- Seeking for offers for PCB & assembly & case.
- Seeking for EU, US licensing.
- Negotiable IP contracts and regional distribution rights.
- Brand name and logo not included. TBD by OEM.

Technical Details

- L3 packet encryption to a cloud console of HTTP/HTTPS/DESKTOP traffic.
- Pass-through of all other traffic.

- The security limitations require full control of the physical site.
- SD card can be removed temporarily.
- Power Over Standard 24-pin USB type C.
- Input Gigabit Ethernet.
- Output Gigabit Ethernet.
- Standard Microcontroller that has multiple software compatible vendors.
- Low cost preferably microcontroller 32-bit 100MHz.
- Simple bootable IC preferred, no ARM if possible.
- Memory as low as 16MB.
- No flash or nonvolatile memory on board.
- Supplemental SD card only that contains the code & key.
- Software & tests are provided by the OEM.

Security and threat model

The threat model is very simple. It works only if you have full control of the site. However, passwords also require such a setup. Attackers may plant hidden cameras to capture passwords.

The limitation of macro-kernel architectures will be the big software battle of 2020s. Traditional macro- kernel architectures give the biggest attack surface, since they can give access to any device or application in the system. They are also updated frequently due to their size.

End users have almost no ways to ensure the integrity of their operating system kernel, unless they are IT professionals.

Kernel based and built in VPN standards may be prone to key theft through kernel vulnerabilities. An external VPN device makes life easier, and it fixes any issues of hijacked OS devices.

Two-factor authentication can replace local passwords. Device integrity can be resolved by enforcing no on-board storage. The SD card can be removed by the end-user, and they can verify its integrity in a text editor or hash program.

WiFi / Bluetooth are considered less safe and extra risk for now.

Battery power may be required for some users later. An USB attached to a laptop is sufficient.

The most general widespread USB charging helps to penetrate the market.

USB may replace the input in the future but adding a driver is a risk and additional R&D cost.

Future improvements can be WiFi / Bluetooth, battery power, USB type C input instead of Ethernet.