



CÔNG TY CỔ PHẦN CÔNG NGHỆ MẠNG LANCS VIỆT NAM

Hotline: +84 868 275 959 | Email: info@lancsnet.com | Website: <https://lancsnet.com/>
Văn phòng: BT35 – TT3, KĐT thành phố Giao Lưu, Đường Phạm Văn Đồng, Phường
Phú Diễn, Hà Nội, Việt Nam.

TÀI LIỆU GIỚI THIỆU

THIẾT BỊ TƯỜNG LỬA THẾ HỆ MỚI ẢO HÓA - vNGFW



SỬA ĐỔI TÀI LIỆU

Lần sửa đổi	Ngày sửa đổi	Nội dung sửa đổi	Người sửa đổi
V00	20/11/2024	Ban hành lần đầu	Nguyễn Văn Vũ

MỤC LỤC

1. Lacs vNGFW là gì?	3
2. Lợi ích & Tính năng chính (Tác dụng).....	3
Bảo mật toàn diện	3
Kết nối an toàn (VPN)	3
Quản lý mạng nâng cao	3
Quản trị và vận hành dễ dàng	4
3. Triển khai & Cài đặt	4
Các định dạng hỗ trợ.....	4
Nền tảng tương thích	4
4. Yêu cầu hệ thống & Hiệu năng.....	5
Cấu hình khuyến nghị.....	5
5. Hướng dẫn Cài đặt ban đầu (Quick Setup)	5
6. Giấy phép & Hỗ trợ (Licensing).....	6
Giấy phép.....	6

1. Lances vNGFW là gì?

Lances vNGFW là một giải pháp firewall ảo (Virtual Firewall Appliance - VFA) mạnh mẽ, linh hoạt và hiệu suất cao. Giải pháp được thiết kế để cung cấp khả năng bảo mật mạng toàn diện, định tuyến nâng cao và kết nối an toàn cho các môi trường ảo hóa và đám mây. Lances vNGFW được đóng gói dưới dạng máy ảo (virtual appliance) và sẵn sàng triển khai ngay lập tức, mang lại sức mạnh của một thiết bị tường lửa chuyên dụng mà không cần phần cứng vật lý.

2. Lợi ích & Tính năng chính (Tác dụng)

Lances vNGFW bảo vệ hạ tầng mạng của bạn bằng cách kiểm soát chặt chẽ lưu lượng truy cập vào và ra, phân vùng các vùng mạng và cung cấp các kết nối từ xa an toàn.

Bảo mật toàn diện

- **Tường lửa trạng thái (Stateful Firewall):** Giám sát và kiểm soát tất cả các kết nối mạng.
- **Network Address Translation (NAT):** Ánh xạ địa chỉ IP public sang private và ngược lại.
- **Stateful Packet Inspection (SPI):** Kiểm tra nội dung gói tin ở cả lớp mạng và lớp ứng dụng để đảm bảo dữ liệu truyền qua tuân thủ các quy tắc bảo mật được thiết lập, phát hiện và ngăn chặn các gói tin bất thường.
- **Phát hiện/Phòng chống xâm nhập (IDS/IPS):** Phát hiện và ngăn chặn hầu hết các cuộc tấn công phổ biến: Packet Anomaly; Port Scan; Ping of Death; Tấn công DoS; Tấn công độc hại/lừa đảo.
- **Threat Protection:** Lướt web an toàn; Chống phần mềm độc hại/Lừa đảo; Chống vi-rút (có kiểm tra TLS/SSL); Lọc tệp, ngăn chặn tấn công DoS, DPI...
- **Domain Filtering:** Kiểm soát truy cập theo tên miền, chặn các trang web không phù hợp, lừa đảo, hoặc chứa mã độc; hỗ trợ chính sách phân quyền truy cập theo nhóm người dùng hoặc thời gian.

Kết nối an toàn (VPN)

- **VXLAN:** Hỗ trợ mở rộng mạng LAN qua hạ tầng Layer 3, tối ưu cho các môi trường ảo hóa và trung tâm dữ liệu phân tán.
- **OpenVPN:** Hỗ trợ kết nối client-to-site và site-to-site linh hoạt.
- **IPsec:** Chuẩn VPN mạnh mẽ sử dụng mã hóa ở lớp mạng; đảm bảo tính bảo mật, toàn vẹn và xác thực dữ liệu giữa các chi nhánh hoặc người dùng từ xa.

Quản lý mạng nâng cao

- **Định tuyến (Routing):** Hỗ trợ định tuyến tĩnh và động, cho phép thiết bị kết nối linh hoạt giữa nhiều mạng khác nhau, đảm bảo dữ liệu được truyền tải nhanh chóng và ổn định.
- **LAN Bridge:** Mạng L2 với đầy đủ các tính năng, quản lý thông minh các kết nối nội bộ, giúp hệ thống mạng hoạt động mượt mà và hiệu quả hơn.
- **Hỗ trợ VLAN (802.1q):** Dễ dàng phân chia các mạng con logic.

- **Chất lượng dịch vụ (QoS):** Ưu tiên lưu lượng truy cập quan trọng (ví dụ: Thoại, Video).
- **Load Balancing / Failover:** Sao lưu bằng giao thức dự phòng và tự động đồng bộ hóa cấu hình giữa các Edge.
- **Dịch vụ mạng tích hợp:** Hỗ trợ đầy đủ các dịch vụ mạng cơ bản giúp đảm bảo khả năng hoạt động ổn định và đồng bộ trong hệ thống.
- **Loại kết nối mạng WAN:** Hỗ trợ nhiều kiểu cấu hình kết nối WAN linh hoạt, đáp ứng đa dạng môi trường triển khai.

Quản trị và vận hành dễ dàng

- **Giao diện Web (Web UI):** Giao diện quản trị trực quan, dễ sử dụng.
- **Công nghệ SD-WAN:** Duy trì kết nối an toàn, tin cậy, tiết kiệm và đảm bảo dễ dàng quản trị, vận hành với công nghệ Auto Provisioning.
- **Công nghệ quản lý truy cập (ZTNA) và xác thực không tin cậy (Zero Trust):** Xác thực, kiểm soát và cá nhân hóa truy cập đến từng thiết bị và người dùng, hỗ trợ tăng hiệu quả công việc.
- **Dự phòng hệ thống:** Tự động phát hiện và chuyển đổi khi có sự cố, đảm bảo dịch vụ luôn hoạt động liên tục và không gián đoạn với cơ chế Active-Passive HA.
- **Truyền thông đa phương tiện:** Tích hợp các tính năng truyền thông đa phương tiện vào một thiết bị duy nhất.
- **Quản lý, xử lý sự cố, cập nhật:** Hỗ trợ quản trị qua CLI, Trang web & Trang web LINKSAFE; Lệnh ping; Lệnh theo dõi tuyến đường; Sao lưu & Khôi phục; Nâng cấp WebUI.

3. Triển khai & Cài đặt

Lancs vNGFW được thiết kế để triển khai nhanh chóng trên các nền tảng ảo hóa phổ biến và môi trường đám mây.

Các định dạng hỗ trợ

- **VMDK:** Dành cho VMware vSphere/ESXi, VMware Workstation.
- **IMG:** Định dạng đĩa thô (raw disk image) để chuyển đổi hoặc sử dụng trực tiếp.
- **[QCOW2]:** [Nếu hỗ trợ, cho KVM, Proxmox].
- **[OVA/OVF]:** [Nếu hỗ trợ, đóng gói sẵn cho VMware/VirtualBox].
- **[VHD/VHDX]:** [Nếu hỗ trợ, cho Hyper-V].

Nền tảng tương thích

- **Ảo hóa On-Premise:** VMware ESXi, Proxmox VE, Microsoft Hyper-V, KVM, VirtualBox.
- **Đám mây (Cloud):** AWS (import VM), Azure, Google Cloud, Vultr, Linode.

4. Yêu cầu hệ thống & Hiệu năng

Hiệu năng của Lancs vNGFW phụ thuộc trực tiếp vào tài nguyên (CPU, RAM, I/O) được cấp phát bởi máy chủ ảo hóa.

Cấu hình khuyến nghị

Mục đích sử dụng	vCPU (Cores)	RAM (GB)	Dung lượng đĩa (GB)	Thông lượng Firewall (Ước tính)	Thông lượng VPN (Ước tính)
Nhỏ (SOHO/Lab)	2 core CPU	4 GB RAM	100 GB	5 Gbps	400 Mbps
Vừa (Doanh nghiệp)	4 core CPU	8 GB RAM	100 GB	10 Gbps	600 Mbps
Lớn (Enterprise)	8 core CPU	16 GB RAM	100 GB	15 Gbps	1 Gbps

Lưu ý: Hiệu năng thực tế có thể thay đổi tùy thuộc vào cấu hình phần cứng, số lượng rule, và loại lưu lượng truy cập.

5. Hướng dẫn Cài đặt ban đầu (Quick Setup)

- Link download firmware:** https://linksafepub.s3.ap-southeast-1.amazonaws.com/firmware/VIRTUAL_NGFW.img.gz
- Import Máy ảo:** Tải về tệp [Chọn định dạng, ví dụ: VMDK/OVA] và import vào trình quản lý ảo hóa của bạn (vSphere, Proxmox, v.v.).
- Cấu hình Mạng:**
 - Gắn card mạng ảo thứ nhất (NIC 1) vào VMSwitch/Port Group cho mạng **WAN**.
 - Gắn card mạng ảo thứ hai (NIC 2) vào VMSwitch/Port Group cho mạng **LAN**.
- Khởi động:** Bật máy ảo Lances vNGFW.
- Chạy Setup Wizard:** Sau khi máy ảo khởi động xong, ấn Enter để vào màn hình CLI. Ta sẽ tiến hành cấu hình IP mạng WAN (Nối ra internet) và mạng Lan (Nối vào các miền VPC bên trong)

Cấu hình	Câu lệnh
Khởi động cấu hình network	enable network
Vào chế độ cấu hình	config terminal
Cấu hình mạng Lan: Cấu hình dns Bật tính năng DHCP server Cấu hình gateway cho mạng Lan Leasetime	interface logical lan dhcpv4-server dns 8.8.8.8 dhcpv4-server enable dhcpv4-server gateway 192.168.138.1 dhcpv4-server leasetime 12h

Range Cấu hình interface vật lý thuộc mạng Lan IP của mạng Lan Kiểm tra thông tin cấu hình	<pre> dhcpv4-server start 2 limit 200 interface-name set eth1 eth2 eth3 eth4 eth5 ip address 192.168.138.1 subnet 255.255.255.0 exit show ip interface brief </pre>
Cấu hình mạng wan: Cấu hình dns Cấu hình interface vật lý thuộc mạng WAN IP của mạng WAN Range	<pre> interface logical wan interface-name set eth0 ip address 192.168.100.1 subnet 255.255.255.0 gateway 192.168.100.1 exit show ip interface brief </pre>

f. Truy cập Web UI:

- Từ một máy tính trong mạng LAN, mở trình duyệt và truy cập địa chỉ IP mặc định của Lanacs vNGFW:
- **IP đã cấu hình ở bước trên, xem lại bằng lệnh `show ip interface brief`**
- **Tài khoản:** `admin`
- **Mật khẩu:** `lanacs@2024`

*** Giao diện web sẽ yêu cầu license để có thể sử dụng**

- g. Hoàn tất:** Sau khi hoàn tất, bạn có thể bắt đầu cấu hình các quy tắc firewall và tính năng khác.

6. Giấy phép & Hỗ trợ (Licensing)

Giấy phép

Để chạy được Lanacs vNGFW cần 2 license:

- **License 1:** License để OS chạy các tính năng của firewall



Device ID: bee7075a-ac46-4836-80b7-9533e327981d

No valid license found. Please upload a license to access the system.

Check License

Logout

NGFW License

No License or License validation failed.

 Upgrade your license.
Please upload a new license to unlock all features.

Upload License File

Select File:

Thực hiện update license thiết bị:

- Khách hàng cần cung cấp Device ID để công ty tạo và gửi license
- Truy cập lên web local đăng nhập Tài khoản và mật khẩu vào giao diện update license

License 2: License để OS chạy các tính năng nâng cao của firewall: Security Profile

