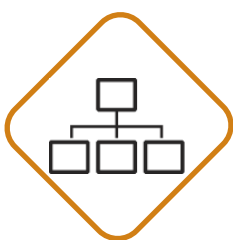


GIẢI PHÁP BẢO VỆ HỆ THỐNG THẾ HỆ MỚI



Trực Quan

Giao diện người dùng hiện đại dễ sử dụng

features



Đầy đủ tính năng

Có mọi thứ bạn cần để bảo vệ hệ thống mạng



Tài liệu sử dụng

Đầy đủ tài liệu trực tuyến với cộng đồng sử dụng rộng lớn



Open Source Initiative

Nguồn mở thực sự

Được cấp phép theo giấy phép do OSI phê duyệt

Mục tiêu của ITServing® trở thành giải pháp bảo vệ hệ thống được sử dụng rộng rãi và hỗ trợ đắc lực cho doanh nghiệp trong việc phòng ngừa, ngăn chặn rủi ro an toàn, an ninh hệ thống.

Chúng tôi mong muốn mang đến cho cá nhân, tổ chức, doanh nghiệp một môi trường an toàn, thân thiện, ổn định và minh bạch.

Nền tảng giải pháp và công nghệ an ninh mạng đến từ Mỹ và châu Âu

Giải pháp và sản phẩm công nghệ **ITServing®** được tinh chỉnh trên nền tảng nguồn mở OPNsense®. Đây là nền tảng định tuyến và tường lửa cao cấp trên nền hệ điều hành nguyên gốc FreeBSD được gia cường an ninh bởi HardenedBSD mà nhiều tổ chức đã và đang sử dụng như: Blue Coat, Check Point, Citrix Systems, Juniper Networks, McAfee, NetApp, Netflix, QNAP, Sophos, Symmetricom...

Khởi đầu từ Middelharnis, Hà Lan vào năm 2015 với một nhóm gồm các chuyên gia công nghệ và những kỹ sư lập trình đam mê mã nguồn mở và là một nhánh phát triển được tách từ pfSense® (© 2004-2014 Electric Sheep Fencing, LLC.), bản thân pfSense® cũng là một nhánh của dự án m0n0wall® (© 2002-2013 Manuel Kasper). Dự án OPNsense® là một dự án cộng đồng mở đang phát triển nhanh chóng và hoạt động mạnh trên toàn cầu.

Sản phẩm **ITServing®** được trang bị hầu hết các tính năng như các tường lửa thương mại cao cấp hiện nay và nhiều tính năng bổ trợ khác cho nhiều tình huống vận hành. Những tính năng phong phú cùng với ưu điểm của nguồn mở có thể kiểm chứng bởi cộng đồng công nghệ đông đảo. **ITServing®** cung cấp các giải pháp an ninh mạng toàn diện dựa trên các công nghệ tiên tiến nhất hiện nay để bảo vệ mạng doanh nghiệp, tổ chức khỏi các mối đe dọa bảo mật đã biết và chưa được biết đến.

Dù là dự án bảo mật non trẻ có tuổi đời chưa được 10 năm nhưng đây là dự án kế thừa kết tinh kỹ thuật, kinh nghiệm vận hành thực tế và có nhiều cải tiến đột phá từ những dự án phần mềm trước đây như: m0n0 từ năm 2002, pfSense năm 2004, OPNsense® năm 2015. Ưu điểm nền tảng được coding lại hoàn toàn nên tương thích tốt với những phần cứng hiện đại vận hành đa luồng (multi-thread) kiến trúc module hóa (microservices architecture) cho khả năng mở rộng và vận hành mạnh mẽ thay vì phần cứng kiến trúc đơn (monolithic architecture) như những nền tảng bảo mật truyền thống khác.

Ưu điểm của nguồn mở

Nghịch lý phần mềm bảo mật nguồn mở, ai cũng có thể xem và tra soát mã nguồn nhưng không có nghĩa phần mềm có nhiều lỗ hổng, sai sót và dễ bị khai thác hoặc tấn công. Thực tế mã nguồn mở luôn được cộng đồng công nghệ đông đảo xem xét, thử nghiệm, kiểm tra, đánh giá, phản hồi và cải tiến liên tục nên những lỗ hổng hoặc khiếm khuyết luôn được mổ xẻ, sửa chữa và cập nhật thường xuyên. Cho nên dù là mã nguồn mở nhưng phần mềm luôn trong trạng thái hoàn chỉnh, an toàn không thua kém so với các phần mềm chính hãng có bản quyền. Và một ưu điểm lớn nhất là hoàn toàn miễn phí bản quyền.

Cuộc chiến chống lừa đảo với kết nối an toàn SSL

Có rất nhiều mối đe dọa mà bạn gặp phải hàng ngày và một trong số đó có thể bạn không hề hay biết. Nổi bật nhất có lẽ là các vấn đề về quyền riêng tư, chẳng hạn như đánh cắp thông tin ngân hàng và gian lận thẻ tín dụng. Các tính năng độc đáo của ITServing® bao gồm hệ thống ngăn chặn xâm nhập nội tuyến có khả năng đưa vào danh sách đen dựa trên dấu vân tay SSL.



Một số điểm nổi bật



Doanh nghiệp

Bảo vệ an toàn mạng doanh nghiệp và bảo mật các kết nối hệ thống (WAN/LAN, Database/File/Web/Mail/App Servers). Tường lửa kiểm tra trạng thái (**stateful firewall**) thế hệ mới đến hệ thống bảo vệ phát hiện và ngăn chặn xâm nhập nội tuyến (**Inline IDS & IPS**), tất cả đều miễn phí với hỗ trợ cộng đồng công nghệ mở rộng lớn. Với công cụ định hình lưu lượng (**traffic shaper**) nâng cao hiệu suất mạng có thể tùy chọn ưu tiên các lưu lượng phục vụ cần thiết. Tự động hóa sao lưu cấu hình lên cloud mà không cần sao lưu thủ công.



Giáo dục

Giới hạn và chia sẻ băng thông khả dụng đồng đều giữa các sinh viên, sử dụng tính năng lọc web dựa trên danh mục để lọc lưu lượng truy cập không mong muốn như nội dung người lớn và các trang web độc hại. Dễ dàng thiết lập mà không cần bổ sung plugin cũng như cài thêm gói nào. Khuyến khích sử dụng tài liệu phát triển nền tảng OPNSense® trong việc đào tạo và nâng cao kiến thức bảo mật cho sinh viên. Khuyến khích Tổ chức giáo dục và sinh viên tham gia cộng đồng cùng phát triển nền tảng OPNSense®



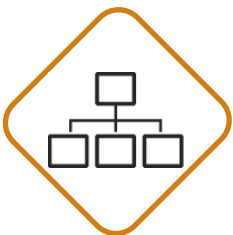
Du lịch & Giải trí

Các khách sạn, resort, khu du lịch, trung tâm thương mại, thường sử dụng cổng xác thực người dùng (**captive portal**) để cho phép khách (trả phí) truy cập internet trong một khoảng thời gian nhất định. Khách có thể đăng nhập bằng voucher tính phí hoặc nhận miễn phí tại quầy lễ tân. ITServing® tích hợp sẵn cổng xác thực người dùng (**captive portal**) với hỗ trợ voucher, dễ dàng tạo voucher một cách nhanh chóng.



Di động

Truy cập hệ thống, kết nối từ xa khi đang di chuyển bất cứ nơi nào. ITServing® là giải pháp tuyệt vời cho doanh nghiệp, cung cấp giải pháp kết nối mã hóa WireGuard, OpenVPN và IPSec VPN về công ty. Dễ dàng xuất khóa mã và cấu hình, giúp việc thiết lập kết nối ứng dụng khách WireGuard, OpenVPN của nhân sự (Windows, MacOS, Android, iOS) với hệ thống mạng công ty (Business LAN) nhanh chóng, tiện lợi, an toàn.



Văn phòng từ xa & SOHO

Sử dụng VPN site to site tích hợp sẵn (IPsec hoặc SSL VPN) tạo kết nối mạng an toàn đến và từ các văn phòng chi nhánh về trụ sở chính.

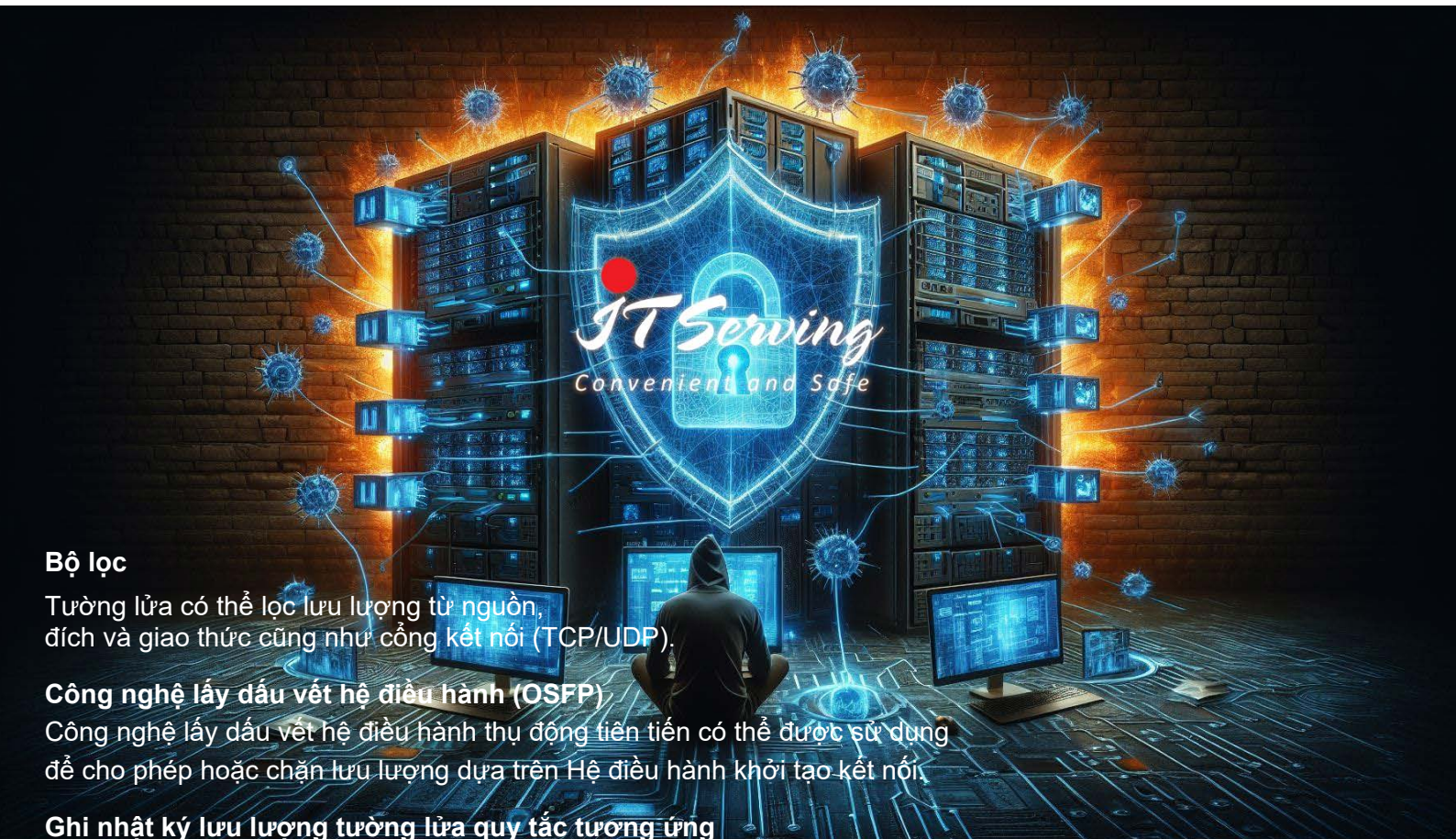
Fully supported

Hỗ trợ toàn diện cho Doanh nghiệp & Tổ chức

Tường lửa trạng thái

(Stateful Inspection Firewall)

“Tường lửa trạng thái theo dõi trạng thái của các kết nối mạng (chẳng hạn như luồng TCP, UDP thông tin liên lạc) đi qua. Tường lửa được lập trình để phân biệt các gói hợp pháp giữa các gói khác nhau và các loại kết nối. Chỉ các gói phù hợp với kết nối đã biết mới được phép vận hành; những kết nối khác sẽ bị từ chối.” - source: en.wikipedia.org



Bộ lọc

Tường lửa có thể lọc lưu lượng từ nguồn, đích và giao thức cũng như cổng kết nối (TCP/UDP).

Công nghệ lấy dấu vết hệ điều hành (OSFP)

Công nghệ lấy dấu vết hệ điều hành thụ động tiên tiến có thể được sử dụng để cho phép hoặc chặn lưu lượng dựa trên Hệ điều hành khởi tạo kết nối.

Ghi nhật ký lưu lượng tường lửa quy tắc tương ứng

Mỗi quy tắc được thiết lập ghi nhật ký trùng khớp, cho phép dễ dàng theo dõi, chặn hoặc cho phép kết nối thông qua module bộ quy tắc tường lửa.

Chính sách dựa trên định tuyến theo qui tắc tùy chọn cổng chính (Gateway)

Với định tuyến dựa trên chính sách, có thể thêm cổng chính (gateway) vào bộ quy tắc và thay đổi hiệu quả định tuyến tiêu chuẩn của lưu lượng truy cập tương ứng.

Hỗ trợ bí danh để gom nhóm và đặt tên IP, mạng (networks) và các cổng (ports)

Bí danh giúp giữ cho bộ quy tắc tường lửa rõ ràng và dễ hiểu, trong môi trường có nhiều địa chỉ IP công cộng và nhiều máy chủ.

Tường lửa lớp 2 trong suốt

Giao diện cầu nối (bridge) và lọc lưu lượng cầu nối, thậm chí cho phép tường lửa không có địa chỉ IP.

Kiểm soát bằng trạng thái chi tiết

Có thể điều chỉnh kích thước bảng trạng thái, khả năng giới hạn lưu lượng trên mỗi quy tắc dựa trên các kết nối đồng thời, trạng thái trên mỗi máy tính & kết nối mới mỗi giây cũng như xác định thời gian chờ trạng thái (state timeout) và kiểu trạng thái (state type).

Vô hiệu hóa lọc gói

Tùy chọn này có thể được sử dụng để chuyển hệ thống thành một bộ định tuyến thuần túy.

Bộ định hình lưu lượng

(Traffic shaper)

Định hình lưu lượng (còn được gọi là "định hình gói") là kiểm soát lưu lượng mạng máy tính nhằm tối ưu hóa hoặc đảm bảo hiệu suất, độ trễ thấp hơn và/hoặc tăng băng thông khả dụng bằng cách trì hoãn các gói đáp ứng các tiêu chí nhất định.

Cụ thể hơn, định hình lưu lượng là bất kỳ hành động nào đối với một tập hợp các gói (thường được gọi là luồng hoặc dòng), áp đặt độ trễ bổ sung cho các gói đó sao cho chúng tuân theo một số ràng buộc được xác định trước (giao kèo hoặc hồ sơ lưu lượng).

Đễ dàng và linh hoạt

Định hình lưu lượng trong IT Serving® rất linh hoạt và được tổ chức xung quanh các đường ống, hàng đợi và các quy tắc tương ứng. Các đường ống xác định bằng thông được phép, các hàng đợi có thể được sử dụng để đặt trọng số trong đường ống và cuối cùng là các quy tắc được sử dụng để áp dụng định hình cho một luồng gói nhất định. Các quy tắc định hình được xử lý độc lập với các quy tắc tường lửa và các cài đặt khác.

Giới hạn băng thông

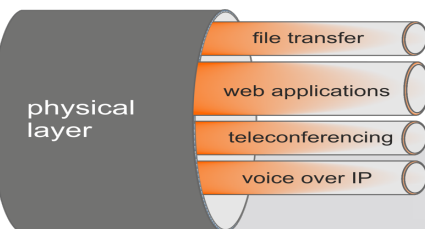
Giới hạn băng thông có thể được xác định dựa trên (các) giao diện, nguồn & đích ip, hướng lưu lượng truy cập (vào/ra) và số cổng (ứng dụng).

Chia sẻ băng thông

Băng thông khả dụng có thể được chia sẻ đồng đều cho tất cả người dùng, điều này cho phép hiệu suất tối ưu mọi lúc.

Ưu tiên

Lưu lượng truy cập có thể được ưu tiên bằng cách thêm hàng đợi và xác định trọng số. Các ứng dụng có trọng số cao hơn có thể tiêu tốn nhiều băng thông hơn các ứng dụng khác khi tổng băng thông khả dụng bị giới hạn.



Traffic shaping with Traffic shaper



Usage without shaping.

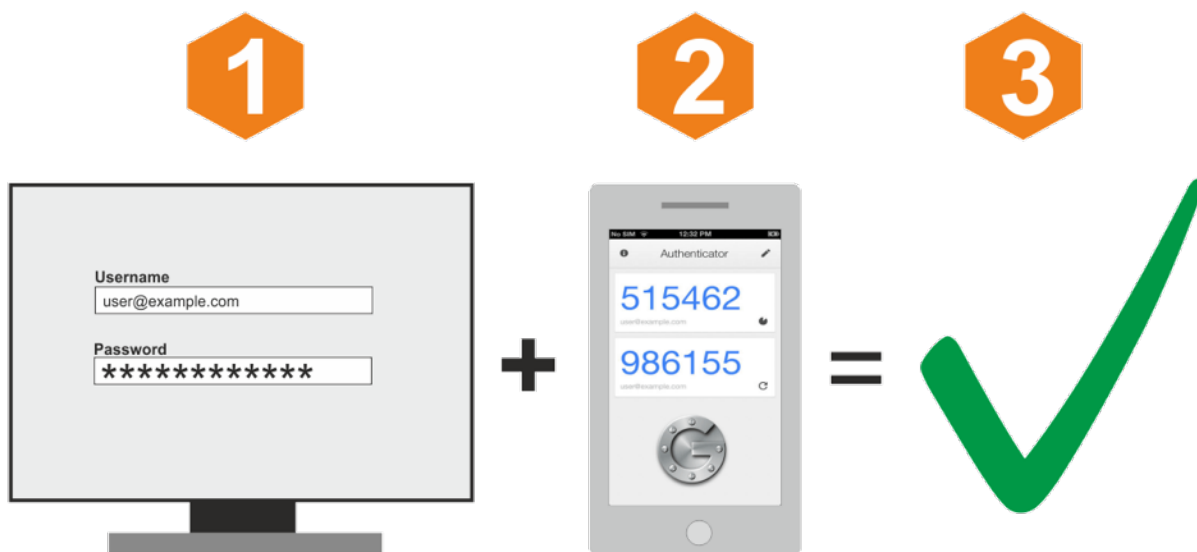


Usage with shaping.

Xác thực 2 nhân tố

(Two-Factor Authentication)

Xác thực hai yếu tố còn được gọi là 2FA hoặc xác minh 2 bước là một phương thức xác thực yêu cầu hai thành phần, chẳng hạn như mã pin/mật khẩu + mã thông báo (TOTP). Chức năng hỗ trợ cho Xác thực hai yếu tố xuyên suốt toàn bộ hệ thống, chỉ với một ngoại lệ là truy cập qua console/ssh.



Mật khẩu dùng một lần đồng bộ giờ (TOTP)

TOTP là một thuật toán (RFC 6238) tính toán mật khẩu một lần từ khóa bí mật dùng chung với thời gian hiện hành. OPNsense có hỗ trợ RFC 6238.

Google xác thực (Google Authenticator)

Hỗ trợ đầy đủ việc sử dụng ứng dụng Google's Authenticator. Ứng dụng này có thể tạo mã trên Hệ điều hành Android, iOS. Ứng dụng hoàn toàn miễn phí và việc thiết lập bằng cực kỳ đơn giản.

Các dịch vụ 2FA được hỗ trợ

Xác thực hai nhân tố (2FA) toàn bộ hệ thống cho các dịch vụ sau:



- ✓ Giao diện người dùng OPNsense
- ✓ Cổng xác thực người dùng (Captive Portal)
- ✓ Mạng riêng ảo (VPN) gồm: OpenVPN & IPsec
- ✓ Bộ đệm Proxy (caching proxy).

Thiết lập dễ dàng

Cấu hình xác thực hai nhân tố (2FA) rất đơn giản bằng Trình xác thực của Google (Google Authenticator).

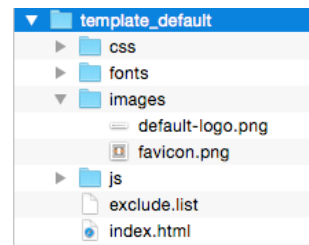
- ✓ Tích hợp trong hệ thống xác thực hợp nhất của OPNsense
- ✓ Xuất mã tự động (Automatic Seed Generation).
- ✓ Kích hoạt mã thông báo bằng mã vạch (barcode).

Cổng xác thực người dùng (Captive portal)

Cổng xác thực người dùng (captive portal) bắt buộc người dùng phải được xác thực hoặc chuyển hướng đến trang chỉ định trước khi được phép truy cập mạng. Xác thực người dùng thường được sử dụng tại các điểm phát sóng (hot spot networks) công cộng nhưng cũng được sử dụng rộng rãi trong cho mạng công ty để có thêm một lớp bảo mật khi kết nối Internet hoặc mạng không dây.

Ứng dụng tiêu biểu

- ✓ Mạng khách
- ✓ Truy cập Wifi khách sạn & công cộng
- ✓ Thiết bị truy cập riêng tư (BYOD)



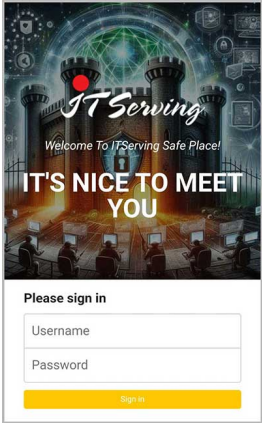
Quản lý mẫu hình

Trình quản lý mẫu độc đáo của IT Serving làm cho việc thiết lập trang đăng nhập của riêng bạn trở thành một nhiệm vụ dễ dàng:

- ✓ Chuyển hướng URL
- ✓ Tùy chọn cho Pop-up của riêng bạn
- ✓ Trang Splash tùy chỉnh

Quản lý vùng (Zone Management)

Các vùng khác nhau có thể được thiết lập trên mỗi giao diện hoặc nhiều giao diện có thể chia sẻ cùng một thiết lập vùng. Mỗi khu vực có thể sử dụng một giao diện xác thực người dùng riêng hoặc chia sẻ với khu vực khác.



Phương thức xác thực

Xác thực an toàn qua HTTPS hoặc chuyển hướng URL đến địa chỉ trang xác thực nhất định với trang nguồn khác nhau, có thể được sử dụng để xác thực người dùng trong một khu vực xác định bằng các phương thức xác thực như:

- ✓ LDAP [Microsoft Active Directory]
- ✓ Radius
- ✓ Quản lý người dùng cục bộ (Local user manager)
- ✓ Vouchers / Tickets
- ✓ Mật khẩu hai nhân tố dùng một lần (2FA)
- ✓ Không xác thực (Chỉ màn hình Splash)
- ✓ Kết hợp (Các phương thức trên)

Quản lý Voucher

Cổng xác thực người dùng (Captive portal) tích hợp tính năng tạo voucher dễ dàng kết xuất voucher sang tập tin csv để linh hoạt sử dụng với bất kỳ ứng dụng nào. Tính năng kết xuất cho phép bạn in voucher bằng cách hợp nhất chúng với MS Word hoặc Open Office và tạo giao diện đẹp mắt với logo và thiết kế theo phong cách của doanh nghiệp.

Đăng xuất & Chào mừng quay trở lại

Tự động ngắt kết nối sau khoảng thời gian người dùng không hoạt động hoặc buộc ngắt kết nối khi thời gian ấn định đã qua ngay cả khi người dùng vẫn còn hoạt động (hết thời gian cho phép). Trong trường hợp người dùng kết nối lại khi thời gian chờ hết hạn và/hoặc hết thời gian qui định, người dùng vẫn có thể tiếp tục hoạt động mà không cần đăng nhập phiên kết nối.

Quản lý băng thông

Công cụ định hình lưu lượng mạng (Traffic shaper) tích hợp sẵn có thể dùng:

- ✓ Chia tải băng thông
- ✓ Ưu tiên băng thông cho cổng giao thức (protocols port numbers) và/hoặc các địa chỉ IP cần ưu tiên

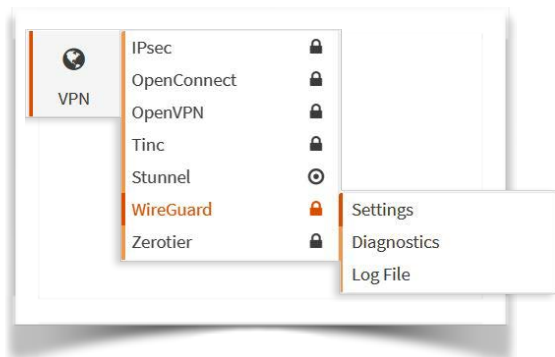
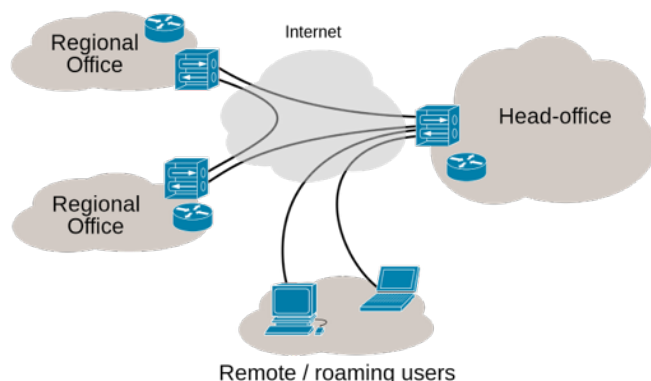
Bỏ qua cổng xác thực

Có thể ấn định địa chỉ MAC và IP thiết bị trong danh sách trắng không cần phải xác thực.

Mạng riêng ảo

(Virtual private network)

Mạng riêng ảo (VPN) mở rộng mạng riêng thông qua mạng công cộng, chẳng hạn như Internet. VPN cho phép máy tính gửi và nhận dữ liệu qua các mạng dùng chung hoặc mạng công cộng hoàn toàn an toàn như đang trong mạng cục bộ (LAN) riêng của tổ chức với đầy đủ các qui tắc chức năng, bảo mật và quản lý của mạng cục bộ (LAN).



Các công nghệ VPN được hỗ trợ

ITServing® hỗ trợ nhiều loại công nghệ VPN khác nhau, từ SSL VPN mới nhất cho đến IPsec phổ biến cũng như các tùy chọn khác.

WireGuard

WireGuard được xây dựng trên cơ sở mã hóa khóa công khai Curve25519, mã hóa Symmetric ChaCha20 và Poly1305 để tạo ra các kết nối an toàn và bảo mật. Giao thức này dễ dàng triển khai trên nhiều nền tảng OS bao gồm: Linux, MacOS, Windows, Android và iOS. Hiện đang được sử dụng phổ biến trong cộng đồng IT vì tính linh hoạt, tiện lợi và bảo mật cao.

IPsec

IPsec cho phép kết nối với bất kỳ thiết bị nào có hỗ trợ IPsec tiêu chuẩn. Ứng dụng phổ biến nhất cho side-to-side kết nối các thiết bị cùng nền tảng, tường lửa nguồn mở khác và hầu hết các giải pháp tường lửa thương mại như Cisco, Juniper...

IPsec cũng có thể được sử dụng để kết nối máy khách di động (road warrior).

OpenVPN

Giải pháp SSL VPN mạnh mẽ hỗ trợ nhiều hệ điều hành máy khách bao gồm cả thiết bị di động (Android/iOS).

Các phần mềm VPN hỗ trợ máy khách kết nối

- ✓ WireGuard for macOS/Windows/Linux
- ✓ WireGuard for Android/iOS
- ✓ Viscosity (Mac OSx & Windows)



Xác thực hai nhân tố (2FA)

- ✓ Hỗ trợ Token TOTP
- ✓ Hỗ trợ tích hợp cho Trình xác thực Google (Google Authenticator)
- ✓ Cài đặt dễ dàng



Trình xác thực Google (Google Authenticator)

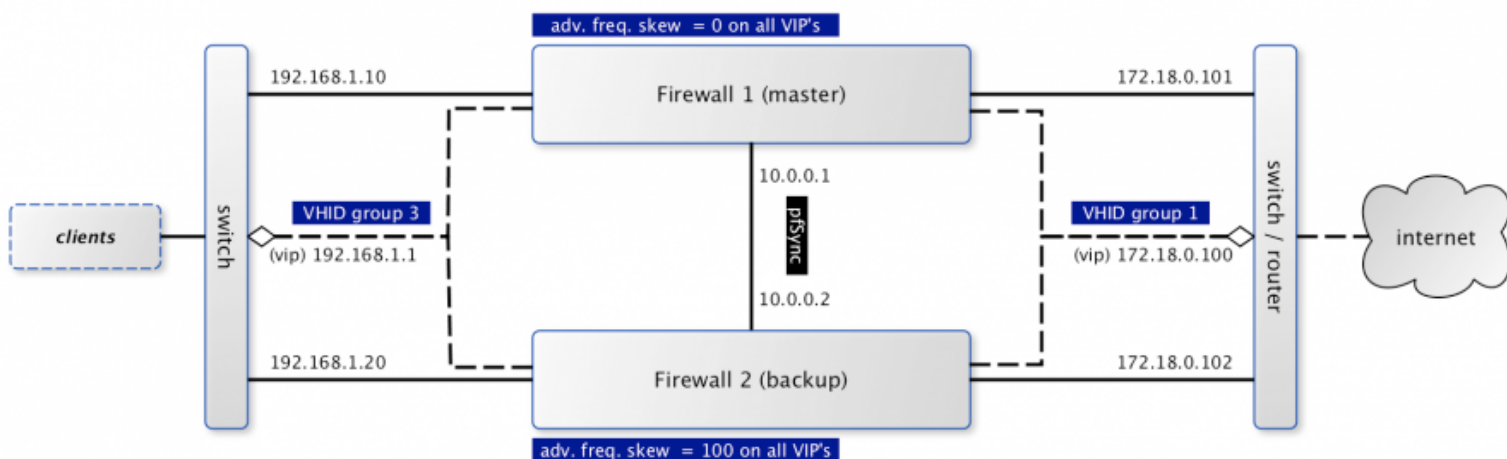
Hỗ trợ tạo mã thông báo miễn phí cho các hệ điều hành sau:

- ✓ Android
- ✓ iOS
- ✓ Blackberry

Tính sẵn sàng/ Chuyển đổi dự phòng

(High Availability / Hardware Failover)

Giao thức dự phòng địa chỉ chung (CARP) cho phép chuyển đổi dự phòng phần cứng. Hai hoặc nhiều tường lửa có thể được cấu hình như một nhóm chuyển đổi dự phòng. Nếu một thiết bị bị lỗi hoặc hoàn toàn ngoại tuyến, thì thiết bị dự phòng sẽ vận hành thay thế. Tính năng này giúp hệ thống vận hành liên tục tránh bị gián đoạn hoạt động khi có thiết bị trong hệ thống bị hỏng hóc.



Tổng quan

ITServing® sử dụng giao thức dự phòng địa chỉ chung (CARP) để chuyển đổi dự phòng phần cứng. Hai hoặc nhiều tường lửa có thể được cấu hình như một nhóm chuyển đổi dự phòng. Nếu một thiết bị bị lỗi hoặc hoàn toàn ngoại tuyến, thì thiết bị dự phòng sẽ vận hành thay thế.

Với tính năng mạnh mẽ này của ITServing®, thiết bị hoàn toàn có khả năng vận hành dự phòng với khả năng chuyển đổi dự phòng tự động, liên tục và liền mạch. Khi thiết bị chuyển sang các kết nối dự phòng, hệ thống sẽ vẫn hoạt động với sự gián đoạn tối thiểu nhất.

Chuyển đổi dự phòng tự động

Nếu tường lửa chính không khả dụng, tường lửa phụ sẽ tiếp quản mà không cần sự can thiệp của người dùng.

Bảng trạng thái được đồng bộ hóa

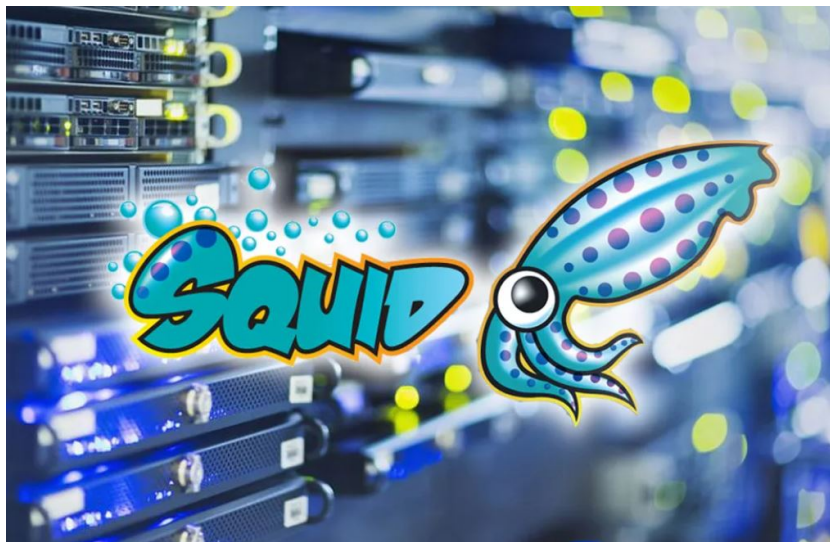
Bảng trạng thái của tường lửa được sao chép cho tất cả các tường lửa được định cấu hình chuyển đổi dự phòng. Có nghĩa là các kết nối hiện có sẽ được duy trì trong trường hợp xảy ra lỗi, điều này rất quan trọng để ngăn chặn sự gián đoạn mạng.

Đồng bộ hóa cấu hình

OPNsense có khả năng đồng bộ hóa tất cả cấu hình. Các thay đổi cấu hình được thực hiện trên hệ thống chính sẽ tự động được đồng bộ hóa với tường lửa phụ.

Trạng thái Dịch vụ & Khởi động lại

Có thể xem và khởi động lại tổng quan về các dịch vụ đang chạy trên thiết bị Dự phòng cho mỗi dịch vụ hoặc tất cả cùng một lúc ngay từ Giao diện Người dùng Chính (Admin).



Bộ Đệm (Caching Proxy)

Squid là proxy bộ nhớ đệm cho Web hỗ trợ HTTP, HTTPS, FTP... Tính năng chính của Squid giúp tiết giảm sử dụng băng thông Internet và cải thiện thời gian phản hồi bằng cách lưu vào bộ nhớ đệm (cache) và dùng lại các trang web được yêu cầu thường xuyên. **Squid** có khả năng kiểm soát truy cập rộng rãi và tạo ra một công cụ tuyệt vời giúp tăng tốc máy chủ.

source - www.squid-cache.org

Đa giao diện

Proxy có thể vận hành với nhiều giao diện khác nhau.

Proxy trong suốt

Proxy có thể được cấu hình là proxy trong suốt.

Trình xác thực

- ✓ LDAP (incl. Microsoft Active Directory)
- ✓ Radius
- ✓ Quản lý người dùng cục bộ (Local user manager)
- ✓ Mật khẩu 2 nhân tố dùng một lần (OTP 2FA)
- ✓ Không cần xác thực

Kiểm soát truy cập

Kiểm soát truy cập chi tiết, bao gồm:

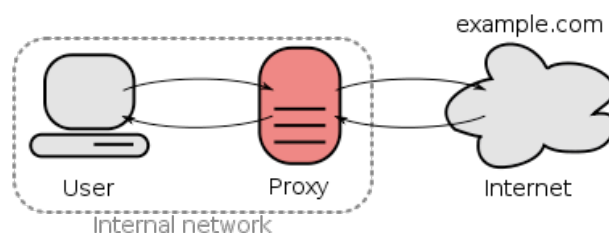
- ✓ Mạng con (Subnets)
- ✓ Cổng kết nối (Ports)
- ✓ Các loại MIME
- ✓ Chặn IP
- ✓ Danh sách trắng
- ✓ Danh sách đen
- ✓ Trình duyệt/Ứng dụng người dùng
- ✓ Các hỗ trợ danh sách đen

FTP proxy

Tích hợp Proxy FTP sử dụng cùng một Danh sách kiểm soát truy cập (ACL).

ICAP

Hỗ trợ làm sạch bên ngoài bằng việc tích hợp công cụ quét virus của bên thứ 3 (như ClamAV).



Quản lý lưu lượng

Proxy có thể được kết hợp với bộ định hình lưu lượng (traffic shaper) và tận dụng tối đa các tính năng định hình. Ngoài ra, còn bao gồm các tùy chọn riêng:

- ✓ Kích cỡ tải về tối đa
- ✓ Kích cỡ tải lên tối đa
- ✓ Điều chỉnh băng thông tổng thể
- ✓ Điều chỉnh băng thông trên mỗi máy (host).

Bộ lọc web dựa trên danh mục phân loại

OPNsense hỗ trợ bộ lọc web dựa trên danh mục tích hợp sẵn. Các tính năng chính bao gồm:

- ✓ Tìm nạp từ một URL từ xa
- ✓ Hỗ trợ danh sách tệp và danh sách nén dựa trên danh mục
- ✓ Tự động chuyển đổi danh sách đen dựa trên danh mục Squid ACL's
- ✓ Luôn cập nhật với lịch trình tích hợp
- ✓ Tương thích với danh sách đen phổ biến nhất



Hệ thống ngăn chặn xâm nhập nội tuyến (*Inline IPS*)

Hệ thống ngăn chặn xâm nhập nội tuyến (The inline IPS system) của ITServing® dựa trên nền tảng an ninh tiên tiến hiện nay Suricata cùng với Netmap giúp nâng cao hiệu suất và giảm thiểu việc sử dụng tài nguyên CPU. Hệ thống kiểm tra chuyên sâu gói tin (deep packet inspection system) này rất mạnh mẽ được sử dụng để giảm thiểu các mối đe dọa bảo mật ở tốc độ cao.

Bộ quy tắc

Tất cả các danh mục quy tắc có sẵn có thể dễ dàng được chọn và áp dụng với cài đặt mặc định hoặc tùy chỉnh theo nhu cầu.

Cảnh báo

Các cảnh báo có thể thấy được trên giao diện người dùng với đầy đủ chi tiết cảnh báo có được hiển thị.

Bộ quy tắc ETOpen về các mối đe dọa mới xuất hiện (>200.000 Rules)

ITServing® tích hợp các quy tắc ET Open (Emerging Threats Open) của Proofpoint. Bộ quy tắc ETOpen là bộ quy tắc cơ bản IDS/IPS chống phần mềm độc hại cho phép tăng cường đáng kể khả năng phát hiện hoạt động của phần mềm độc hại trên nền tảng mạng hiện hữu. Người dùng có thể nâng cấp ETPro để gia cường an ninh.

Abuse.ch

Abuse.ch cung cấp một số danh sách đen để bảo vệ hệ thống chống lại các trang mạng lừa đảo.

ITServing® tích hợp sẵn Danh sách đen SSL (SSLBL) được cập nhật từ Abuse.ch, đây là một dự án được duy trì bởi Abuse.ch. Mục tiêu dự án cung cấp danh sách các chứng chỉ SSL “độc hại” được kiểm tra bởi Abuse.ch có liên quan đến các hoạt động của phần mềm độc hại hoặc mạng botnet.

SSLBL dựa trên dấu vết SHA1 của chứng chỉ SSL độc hại và cung cấp nhiều danh sách đen khác nhau.

Trình theo dõi Feodo

Feodo (còn được gọi là Cridex hoặc Bugat) là một dự án của Abuse.ch với mục tiêu chia sẻ thông tin botnet C&C được liên kết với Dridex, Emotet (hay còn gọi là Heodo), TrickBot, QakBot (hay còn gọi là QuakBot/Qbot) và BazarLoader (hay còn gọi là BazarBackdoor). Feodo cung cấp nhiều danh sách chặn khác nhau, giúp nhà quản trị mạng bảo vệ người dùng hệ thống khỏi nạn lừa đảo và đánh cắp thông tin nhạy cảm (như tài khoản Ngân hàng, thông tin thẻ tín dụng). Người dùng có thể nâng cấp bản cao cấp hơn để gia cường an ninh.

Maxmind GeoLite2 Country

Tích hợp hỗ trợ cơ sở dữ liệu Quốc gia GeoLite2. Cơ sở dữ liệu GeoLite2 là cơ sở dữ liệu định vị vị trí địa lý IP hoàn toàn miễn phí. Cơ sở dữ liệu GeoLite2 được cập nhật vào thứ ba đầu tiên của mỗi tháng.

Dấu vết (Finger Printing)

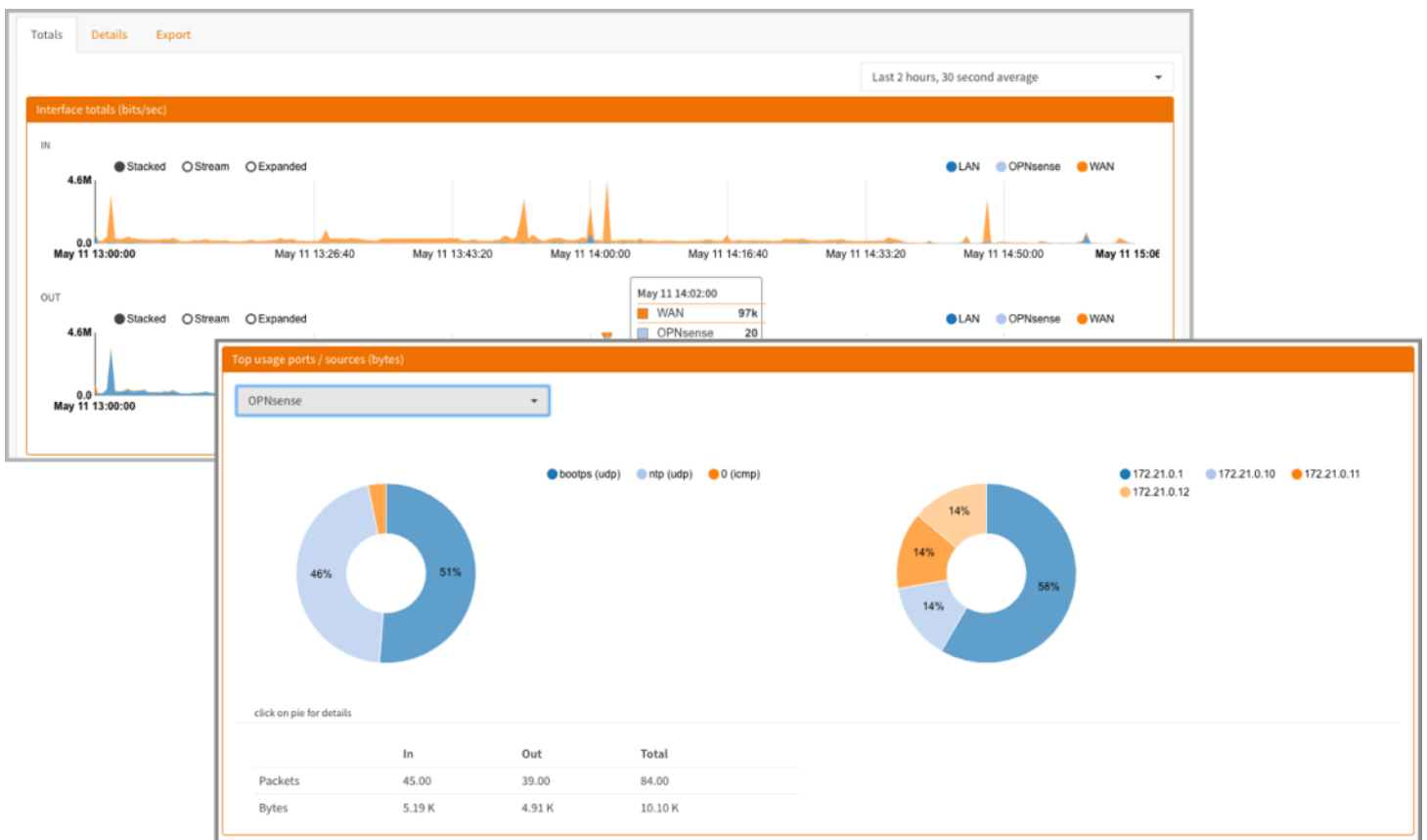
ITServing® được trang bị giải pháp chặn các trang web dựa trên dấu vết SSL.

Phân tích & Kết xuất Netflow

(Netflow Export & Analyses – Insight)

Netflow là một tính năng giám sát do Cisco phát minh, nó được triển khai trong nhân FreeBSD với *ng_netflow* (Netgraph). Vì Netgraph được triển khai từ nhân hệ điều hành nên việc thực thi rất nhanh, vượt trội hơn so với softflowd hoặc pfflowd. Trong khi nhiều giải pháp giám sát như Nagios, Cacti và vnstat chỉ nắm bắt số liệu thống kê lưu lượng truy cập, Netflow nắm bắt các luồng gói hoàn chỉnh bao gồm IP nguồn, IP đích và cổng kết nối. OPNsense cung cấp hỗ trợ đầy đủ để xuất dữ liệu Netflow sang bộ thu thập bên ngoài cũng như Trình phân tích toàn diện có tên gọi Insight (Chi tiết rõ ràng) có thể phân tích tại chỗ và theo dõi trực tiếp.

Đây là giải pháp nguồn mở duy nhất có bộ phân tích Netflow được tích hợp vào Giao diện người dùng.



Kết xuất Netflow

Netflow Exporter hỗ trợ nhiều giao diện, lọc các luồng vào và nhiều luồng đích bao gồm bắt (chụp) các luồng cục bộ để phân tích bằng Insight (OPNsense Netflow Analyser).

Các phiên bản được hỗ trợ

ITServing® hỗ trợ cả Netflow phiên bản 5 (IPv4) và phiên bản 9 (IPv4 & IPv6).

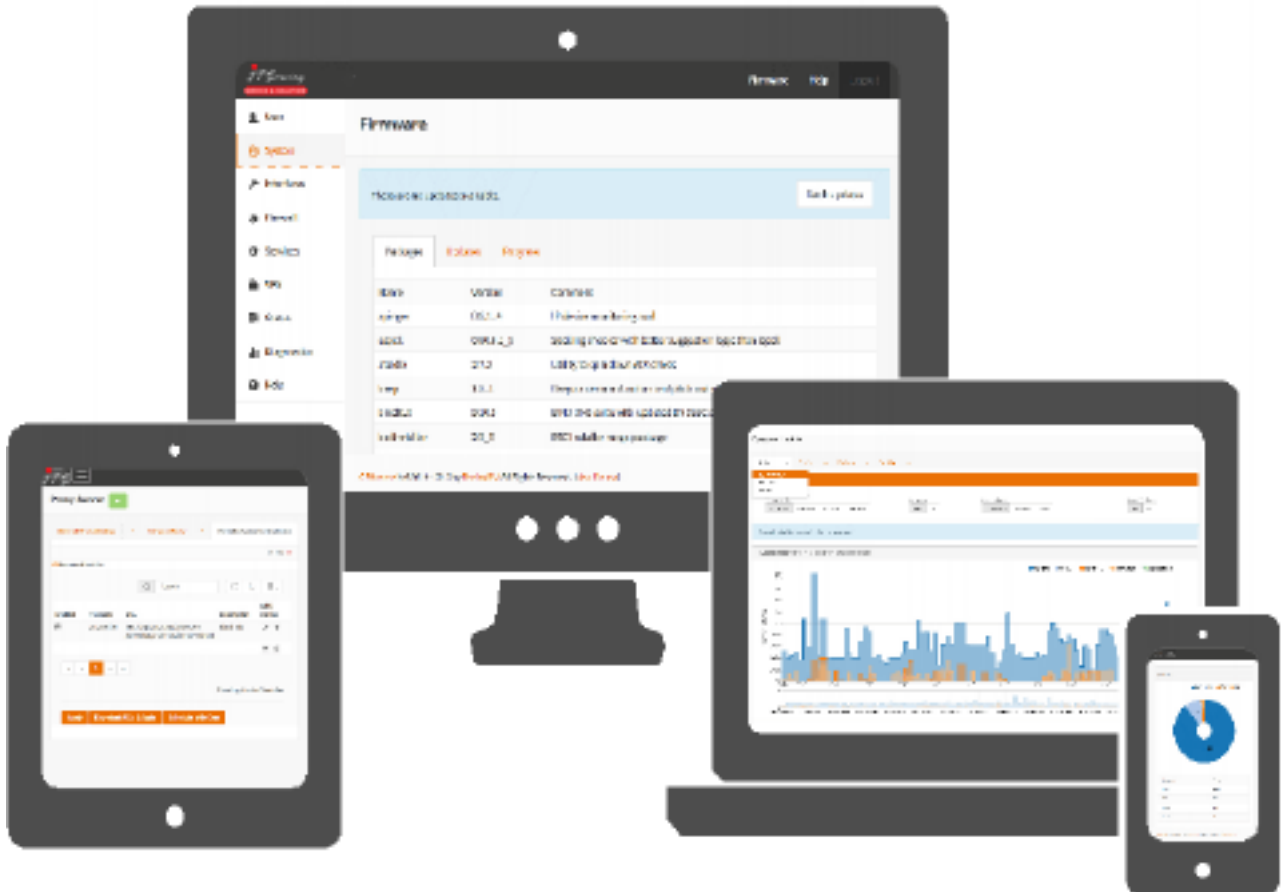
Bộ phân tích Netflow - Chi tiết rõ ràng

Cung cấp Bộ phân tích Netflow đầy đủ với các tính năng:

- ✓ Bắt (chụp) 5 chi tiết cấp độ
- ✓ Biểu diễn đồ họa của các luồng (xếp chồng lên nhau, phát trực tiếp và mở rộng)
- ✓ Mức sử dụng cao nhất trên mỗi giao diện, cả IP và cổng kết nối.
- ✓ Lưu lượng vào/ra đầy đủ theo gói và byte.
- ✓ Chế độ xem chi tiết với lựa chọn ngày, bộ lọc cổng kết nối/ip (tối đa 2 tháng)
- ✓ Xuất dữ liệu sang tập tin CSV để phân tích ngoại tuyến gồm: Lựa chọn mức độ chi tiết, Lựa chọn độ phân giải chi tiết, Lựa chọn theo phạm vi ngày cụ thể. Chức năng này rất hữu ích, có thể phục vụ cho nhiều mục đích khác nhau cho hoạt động quản trị mạng (VD: phục vụ điều tra pháp y quá trình tấn công hệ thống bao gồm: thời gian, phương thức tấn công...).

UI Bootstrap hiện đại

Thiết kế tương tác, dễ sử dụng, có thể truy cập từ máy tính để bàn, máy tính bảng và điện thoại thông minh.



Bao gồm mọi thứ

Tất cả các tính năng do IT Serving® cung cấp đều có thể định cấu hình thông qua giao diện tương tác người dùng.

Đa ngôn ngữ

Giao diện người dùng được hỗ trợ đa ngôn ngữ.

Trợ giúp tích hợp

Nhiều tùy chọn có biểu tượng thông tin với trợ giúp tích hợp sẵn giúp bạn bắt đầu nhanh chóng.

Chế độ nâng cao

Các tính năng phức tạp như proxy, định hình lưu lượng và IDPS có các tùy chọn nâng cao có thể hiển thị hoặc ẩn.

Mặc định sẵn

Nhiều tính năng có các giá trị mặc định có thể sử dụng, cho phép lập cấu hình dễ dàng, nhanh chóng, đơn giản.

Xác thực hai yếu tố (2FA)

Giao diện người dùng của IT Serving® hỗ trợ xác thực thông qua xác thực hai yếu tố bằng Googles Authenticator hoặc các mã thông báo TOTP khác.



Sao lưu & Phục hồi

(Backup & Restore)

Tiện lợi và an toàn, luôn cập nhật bản sao lưu cấu hình hệ thống. Dễ dàng với ITService®.

Lịch sử

Sao lưu tự động các thay đổi cấu hình giúp xem lại lịch sử và khôi phục các cài đặt trước đó.

Sao lưu

Dễ dàng tải xuống bản sao lưu và lưu trữ nơi an toàn.

Mã hóa bản sao lưu bằng mật khẩu mạnh.

Phục hồi

Tải lên tệp sao lưu cấu hình và khôi phục một cách dễ dàng.

Sao lưu dữ liệu lên đám mây

ITService® hỗ trợ mã hóa sao lưu đám mây các cấu hình thiết bị với tùy chọn giữ nhiều bản sao lưu thiết bị từng thời điểm (lịch sử). Google drive được tích hợp sẵn trên giao diện quản trị.

```
Configuration diff from 3/16/16 16:23:56 to 3/23/16 16:39:09
--- /conf/backup/config-1458747549.256.xml 2016-03-23 16:39:09.256742000 +0100
+++ /conf/backup/config-1458747563.3816.xml 2016-03-23 16:39:23.382325000 +0100
@@ -1817,6 +1817,30 @@
</rule>
<rule>
  <type>pass</type>
+ <interface>opt1</interface>
+ <ipprotocol>inet</ipprotocol>
+ <statetype>keep state</statetype>
+ <descr>test</descr>
+ <category>customer a</category>
+ <source>
+ <any1</any>
+ </source>
+ <destination>
+ <any1</any>
+ </destination>
```



Google Drive

Firmware & Plugins

Firmware mạnh mẽ luôn được nâng cấp đối phó với những mối nguy an ninh mới

Packages	Plugins	Updates	Progress
Name	Version	Size	Comment
GeoIP	1.6.9	808KIB	Find the country that any IP address or hostname originates from
apinger	0.6.1_4	86.3KIB	IP device monitoring tool
aspell	0.60.6.1_5	3.68MiB	Spelling checker with better suggestion logic than ispell
ataidle	2.7.2	21.4KIB	Utility to spin down ATA drives
beep	1.0_1	8.28KIB	Beeps a certain duration and pitch out of the PC Speaker
bind910	9.10.3P4	48.8MiB	BIND DNS suite with updated DNSSEC and DNS64
bsdinstaller	2.3_5	1.48MiB	BSD Installer mega-package
bsnmp-regex	0.6_1	63.5KIB	bsnmpd module allowing creation of counters from log files

ITServing® được trang bị cơ chế cập nhật an toàn và đáng tin cậy để cung cấp các bản cập nhật bảo mật.

Cơ chế plugin có thể được sử dụng để cài đặt các gói và tùy chỉnh bổ sung.

Lịch phát hành

Dựa trên nền tảng OPNsense® cung cấp hai bản phát hành chính hàng năm; vào tháng Giêng và tháng Bảy. Các bản cập nhật gia tăng (bảo mật) nhỏ hơn được cung cấp hàng tuần. Các bản cập nhật nhỏ không bắt buộc, nhưng cung cấp thêm một lớp an toàn bằng cách kết hợp các bản sửa lỗi bảo mật nhanh chóng.

Giảm thiểu thời gian chết và luôn cập nhật

Cơ chế nâng cấp đơn giản, dễ sử dụng và đã được chứng minh an toàn. Việc nâng cấp có thể được thực hiện từ bên trong Giao diện người dùng hoặc thông qua bảng điều khiển (CLI). Đối với hầu hết các nâng cấp nhỏ, không cần khởi động lại và các dịch vụ sẽ tiếp tục hoạt động không bị gián đoạn. Trong trường hợp cần khởi động lại, hệ thống sẽ thông báo trước khi nâng cấp thực sự và người dùng có thể chọn hủy quy trình nâng cấp.

Plugins

Tất cả các tính năng đều có trong ITServing® và không yêu cầu bất kỳ phần bổ sung hoặc gói bổ sung nào. Tuy nhiên, hệ thống có khả năng mở rộng cao với các plugin để thêm các tùy chỉnh hoặc tính năng bổ sung. Các plugin tiêu chuẩn bao gồm vmware-tools và Xen-tools để cài đặt ảo hóa.



Các tính năng tích hợp

Stateful firewall

- ⊙ Filter by
 - Source
 - Destination
 - Protocol
 - Port
 - OS (OSFP)
- ⊙ Limit simultaneous connections on a per rule base
- ⊙ Log matching traffic on a per rule bases
- ⊙ Policy Based Routing
- ⊙ Packet Normalisation
- ⊙ Option to disable filter for pure router mode

Granular control state table

- ⊙ Adjustable state table size
- ⊙ On a per rule bases
 - Limit simultaneous client connection
 - Limit states per host
 - Limit new connections per second
 - Define state timeout
 - Define state type
- ⊙ State types
 - Keep
 - Sloppy
 - Modulate
 - Synproxy
 - None
- ⊙ Optimisation options
 - Normal
 - High latency
 - Aggressive
 - Conservative

2-Factor Authentication

- ⊙ Supports TOTP
- ⊙ Google Authenticator
- ⊙ Support services:
 - Captive Portal
 - Proxy
 - VPN
 - GUI

802.1Q VLAN support

- ⊙ max 4096 VLAN's

Network Address Translation

- ⊙ Port forwarding
- ⊙ 1:1 of ip's & subnets
- ⊙ Outbound NAT
- ⊙ NAT Reflection

Traffic Shaping

- ⊙ Limit bandwidth
- ⊙ Share bandwidth
- ⊙ Prioritise traffic

- ⊙ Rule based matching
 - Protocol
 - Source
 - Destination
 - Port
 - Direction

IGMP Proxy

- ⊙ For multicast routing

Universal Plug & Play

- ⊙ Fully supported

Dynamic DNS

- ⊙ Selectable form a list
- ⊙ Custom
- ⊙ RFC 2136 support

DNS Forwarder

- ⊙ Host Overrides
- ⊙ Domain Overrides

DNS Server

- ⊙ Host Overrides
 - A records
 - MX records
- ⊙ Access Lists

DNS Filter

- ⊙ Supports OpenDNS

DHCP Server

- ⊙ IPv4 & IPv6
- ⊙ Relay Support
- ⊙ BOOTP options

Multi WAN

- ⊙ Load balancing
- ⊙ Failover
- ⊙ Aliases

Load Balancer

- ⊙ Balance incoming traffic over multiple servers

Network Time Server

- ⊙ Hardware devices
 - GPS
 - Pulse Per Second

Intrusion Detection & Prevention

- ⊙ Inline Prevention
- ⊙ Integrated rulesets
 - SSL Blacklists
 - Feodo Tracker
 - Geolite2 Country IP
 - Emerging Threats ETOpen

- ⊙ SSL Fingerprinting
- ⊙ Auto rule update using configurable cron

Captive Portal

- ⊙ Typical Applications
 - Guest Network
 - Bring Your Own Device (BYOD)
 - Hotel & Camping Wifi Access

- Template Management
- Multiple Zones
- ⊙ Authenticators
 - LDAP
 - Radius
 - Local User Manager
 - Vouchers / Tickets
 - Multiple
 - None (Splash Screen Only)
- ⊙ Voucher Manager
 - Multiple Voucher Databases
 - Export vouchers to CSV
- ⊙ Timeouts & Welcome Back
- ⊙ Bandwidth Management
 - Share evenly
 - Prioritise
 - Protocols
 - Ports
 - IP
- ⊙ Portal bypass
 - MAC and IP whitelisting
- ⊙ Real Time Reporting
 - Live top IP bandwidth usage
 - Active Sessions
 - Time left
 - Rest API

Virtual Private Networks

- ⊙ IPsec
 - Site to Site
 - Road Warrior
- ⊙ OpenVPN
 - Site to Site
 - Road Warrior
 - Easy client configuration exporter

WireGuard

- ⊙ Zerotier

High Availability

- ⊙ Automatic hardware failover
- ⊙ Synchronised state table
- ⊙ Configuration synchronisation

Caching Proxy

- ⊙ Multi interface
- ⊙ Transparent Mode
- ⊙ Access Control Lists
- ⊙ Blacklists
- ⊙ Category Based Web-filter
- ⊙ Traffic Management
- ⊙ Auto sync for remote blacklists
- ⊙ ICAP (supports virus scan engine)

System Health

- ⊙ Round Robin Data
- ⊙ Selection & Zoom
- ⊙ Exportable

Backup & Restore

- ⊙ History & Diff support
- ⊙ File Backup
- ⊙ Cloud Backup

SNMP

- ⊙ Monitor & Traps

Diagnostics

- ⊙ Filter reload status
- ⊙ Firewall Info (pfInfo)
- ⊙ Top Users (pfTop)
- ⊙ Firewall Tables
 - Aliases
 - Bogons
- ⊙ Current Open Sockets
- ⊙ Show All States
- ⊙ State Reset
- ⊙ State Summary
- ⊙ Wake on LAN
- ⊙ ARP Table
- ⊙ DNS Lookup
- ⊙ NDP Table
- ⊙ Ping
- ⊙ Packet Capture
- ⊙ Test Port
- ⊙ Trace route
- ⊙ Traffic Graph

Network Monitoring

- ⊙ Netflow Exporter
- ⊙ Network Flow Analyser
 - Fully Integrated
 - CVS Exporter

Firmware

- ⊙ Easy Upgrade
 - Reboot warning for base upgrades
- ⊙ SSL Flavour selectable
 - OpenSSL
 - LibreSSL
- ⊙ Selectable Package Mirror
- ⊙ Reinstall Single Package
- ⊙ Lock Package (prevents upgrade)
- ⊙ Plugin Support
 - VMware tools
 - Xen tools
 - HAProxy -Load balancer

REST API

- ⊙ ACL support

Online Documentation

- ⊙ Free & Searchable

Fully supported

Hỗ trợ toàn diện cho Doanh nghiệp & Tổ chức

www.it-serving.org



Tầng 3, Tòa Nhà An Phú Plaza, 117-119 Lý Chính Thắng, P.Võ Thị Sáu, Q.3, TP. HCM
Hotline: 0901 33 32 37 - 0901 333 987 (Zalo)
Email: support@it-serving.org

Hỗ trợ Doanh nghiệp & Tổ chức

Tiện lợi và An toàn

- ✓ Tư vấn Giải pháp, Công nghệ & Dịch vụ
- ✓ Hoạch định hệ thống đáp ứng nhu cầu phát triển
- ✓ Thi công, lắp đặt hạ tầng
- ✓ Cấu hình thiết bị theo nhu cầu và mô hình mạng Doanh nghiệp
- ✓ Đào tạo và bàn giao hệ thống
- ✓ Sao lưu, bảo trì & hỗ trợ xử lý sự cố phát sinh
- ✓ Thay thế thiết bị ngay trong vòng 8h

Dịch vụ hỗ trợ tích hợp

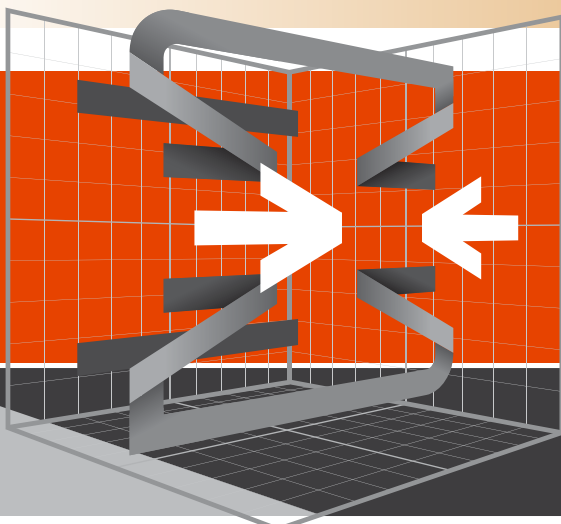
Tư vấn giải pháp công nghệ, đồng hành cùng Doanh nghiệp & Tổ chức trong suốt thời gian cung cấp dịch vụ

- ✓ Tư vấn Giải pháp - Công nghệ phục vụ phát triển hoạt động Doanh nghiệp & Tổ chức
- ✓ Xây dựng giải pháp, lựa chọn thiết bị và công nghệ phù hợp đáp ứng nhu cầu
- ✓ Xây dựng bảng kế hoạch ngân sách theo Giải pháp - Công nghệ đã chọn
- ✓ Tìm kiếm nhà phân phối, đơn vị cung cấp chính thức & cạnh tranh
- ✓ Đại diện giám sát, nhận bàn giao và nghiệm thu công trình

Hỗ trợ Đối tác

Các hỗ trợ đối với Đối tác (IT-ICT partners) của IT Serving

- ✓ Tư vấn Giải pháp - Công nghệ phục vụ công tác Pre-sales & Sales
- ✓ Hỗ trợ xây dựng giải pháp đáp ứng nhu cầu khách hàng
- ✓ Hỗ trợ triển khai và cấu hình hệ thống
- ✓ Hỗ trợ chẩn đoán và xử lý sự cố phát sinh
- ✓ Bảo hành và sửa chữa sản phẩm
- ✓ Chiết khấu tốt nhất cho đối tác



IT Serving
SERVICE & SOLUTION

Powered by OPNsense®

**Your next Generation
open source firewall!**

- Fully featured and easy to use GUI
- Open and transparent for users and developers
- BSD style license