VNPT Cyber Immunity

DỊCH VỤ CỦA VNPT

DỊCH VỤ VNPT NEXT-GEN FIREWALL

GIỚI THIỆU

Dịch vụ VNPT Next- Gen Firewall là một hệ thống bảo mật mạng tiên tiến được thiết kế để ngăn chặn và giám sát các mối đe dọa mạng hiện đại. Đây là một phần quan trọng trong chiến lược bảo mật của doanh nghiệp hoặc tổ chức để bảo vệ hệ thống và dữ liệu khỏi các cuộc tấn công mạng. Dịch vụ VNPT Next-Gen Firewall không chỉ tập trung vào việc ngăn chặn các đe dọa mạng truyền thống mà còn sử dụng công nghệ tiên tiến để đối phó với các mối đe dọa phức tạp và nguy cơ mạng đang ngày càng tiến triển.

Dịch vụ VNPT Next-Gen Firewall là sự kết hợp giữa công nghệ ảo hóa, dịch vụ vận hành hỗ trợ của VNPT và công nghệ tường lửa thế hệ mới Fortigate của hãng Fortinet mang đến cho khách hàng một giải pháp bảo vệ an toàn, hiệu quả và dịch vụ hỗ trợ vận hành chất lượng.

LỢI ÍCH

01 Chức năng bảo vệ an ninh mạng toàn diện bao gồm: Tường lửa, VPN, phòng chống xâm nhập (IPS), web-filtering anti-virus và chống phần mềm độc hại.

02 Tính linh hoạt và khả năng mở rộng cao: Khách hàng có thể linh hoạt mở rộng, nâng cấp để đáp ứng nhu cầu bảo vệ linh hoạt mà không tốn chi phí thay thế.

03 Triển khai nhanh chóng: Dịch vụ có thể triển khai nhanh chóng trên môi trường ảo hóa, giảm chi phí phần cứng và tăng

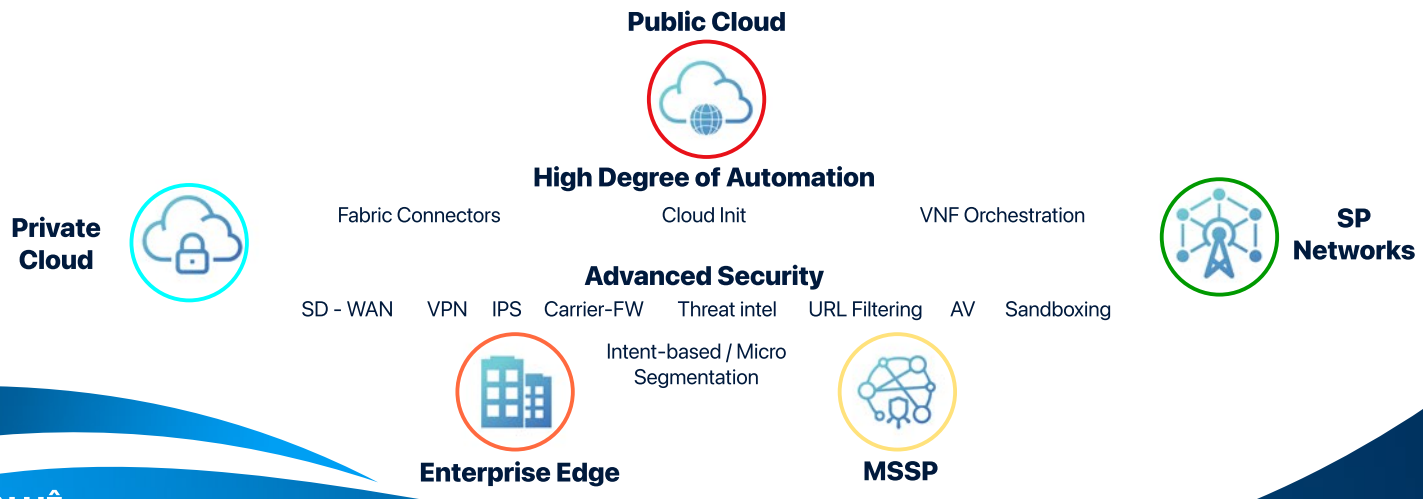
04 Hỗ trợ triển khai theo mô hình HA: Đảm bảo tính sẵn sàng cho hệ thống.

TÍNH NĂNG BỔI BẬT

Với thế mạnh của VNPT- Tập đoàn hàng đầu Việt Nam về Viễn thông và Công nghệ thông tin, có vai trò dẫn dắt công cuộc chuyển đổi số Quốc gia; sở hữu hệ sinh thái, chuỗi cung ứng ICT lớn, VNPT Next-Gen Firewall đảm bảo mang đến dịch vụ ATTT hiện đại, hiệu quả, cạnh tranh cho khách hàng.

Tính năng	Chi tiết
VPN	Cung cấp tính năng mạng riêng ảo để đảm bảo kết nối từ internet vào mạng nội bộ
Network and File Security	Cung cấp khả năng bảo vệ chống lại các mối đe dọa dựa trên mạng và dựa trên tệp. Bao gồm tính năng: Phòng chống xâm nhập (IPS) sử dụng mô hình AI/M để thực hiện kiểm tra sâu đối với gói/SSL để phát hiện và ngăn chặn nội dung độc hại cũng như áp dụng bản vá ảo khi có lỗ hổng mới đã phát hiện. Chống phần mềm độc hại để bảo vệ chống lại các tệp dựa trên tệp đã biết và chưa xác định. Sandbox để phân tích tự động mã độc, tệp tin, URL độc hại Kiểm soát ứng dụng tăng cường tuân thủ bảo mật và cung cấp khả năng giám sát ứng dụng theo thời gian thực.
Web and DNS security	Cung cấp khả năng bảo vệ chống lại các mối đe dọa qua web bao gồm các mối đe dọa dựa trên DNS, các mối đe dọa qua URL độc hại (bao gồm cả trong email) và các liên lạc botnet/lệnh và kiểm soát. DNS Filtering cung cấp tính năng lọc, hiển thị đầy đủ về lưu lượng DNS trong khi chặn các miền có rủi ro cao và bảo vệ chống lại đường hầm DNS. URL Filtering tận dụng cơ sở dữ liệu gồm hơn 300 triệu URL để xác định và chặn liên kết đến các trang web độc hại, chống botnet và chặn các cuộc tấn công DDoS từ các nguồn đã biết.
Data leak prevention	Cung cấp khả năng chống thất thoát dữ liệu lớp mạng, giảm nguy cơ lộ lọt hoặc các cuộc tấn công nằm vùng, đánh cắp dữ liệu
Zero-Day Threat Prevention	Cung cấp công nghệ Sandbox hiện đại, để phân tích và chặn các tệp không xác định trong thời gian thực, cung cấp cho NGFW khả năng bảo vệ trước các mối đe dọa zero-day và tinh vi. Tích hợp ma trận MITER ATT&CK® để tăng tốc quá trình điều tra.
Monitor Monitor	Cung cấp giao diện quản trị trực quan để dễ dàng bao quát được tất cả các sự kiện An ninh mạng
Tính năng HA	Active – Active, Active – Passive
Khả năng mở rộng	Linh hoạt, giảm sự ảnh hưởng và gián đoạn dịch vụ trong quá trình mở rộng
Hỗ trợ kỹ thuật	24/7

Dịch vụ có thể được triển khai ở nhiều môi trường ảo hóa khác nhau như: Public cloud, Private cloud, Enterprise Edge, MSSP, SP Networks



LIÊN HỆ

57 Huỳnh Thúc Kháng – Đống Đa – Hà Nội

0243.7265.171

sec.vnpt.vn | security@.vnpt.vn