Tổng Quan Về Fortigate Firewall

Tác giả: Nguyễn Quốc Hân

Tổng quan về Fortigate AntiVirus Firewall

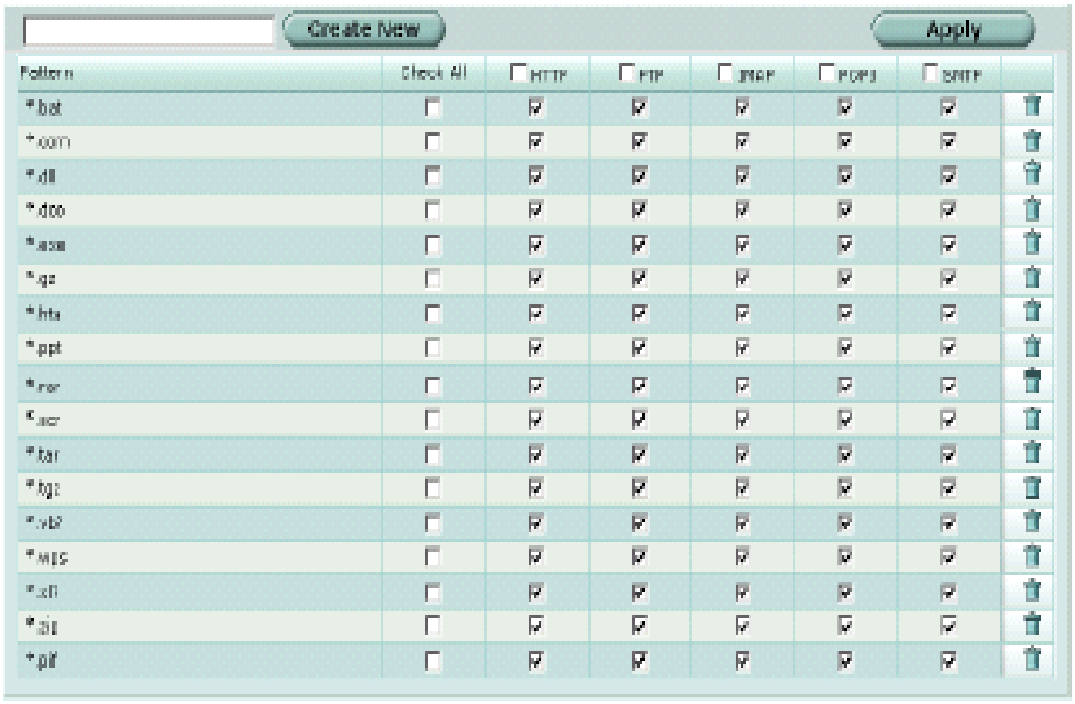
Fortigate AntiVirus Firewall(FGA) là thiết bị security có khả năng kiểm soát traffic của network ở nhiều mức độ khác nhau:

-Mức Application services như chống virus và lọc nội dung

-Mức Network services như firewall, intruction detection, VPN và traffic shaping.

FGA-800 dùng cho doanh nghiệp lớn hỗ trợ Vlan, HA , với 8 port, 4 port kết nối 1000 và 4 port kết nối 100 , support 30.000 current sessions

AntiVirus

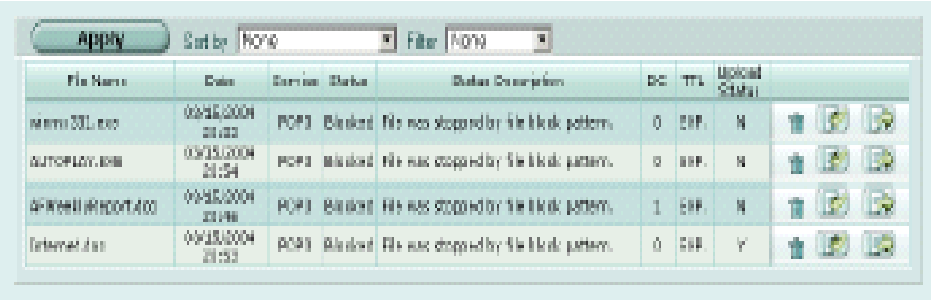


+FGA-800 có khả năng quét virus qua giao thức web (HTTP),FTP,email (SMTP, POP3, IMAP) khi dữ liệu có virus được gởi qua FGA.

+Nếu virus được phát hiện, FGA sẽ loại bỏ virus khỏi luồng dữ liệu đang đi qua và thông báo cho người bị nhiễm vius biết là dữ liệu nhiễm virus đã loại bỏ.N

goài ra để bảo vệ tốt hơn, người dùng có thể cấm định dạng file mà nhiễm virus(.exe,.bat…)

+FGA có khả năng loại bỏ grayware gây nguy hiểm cho hệ thống và quarantine lại trên ổ cứng của FGA và sẽ tự xóa sau một thời gian .FGA sẽ gởi mail cảnh báo đến administrator khi phát hiện có và loại bỏ virus khỏi luồng dữ liệu.



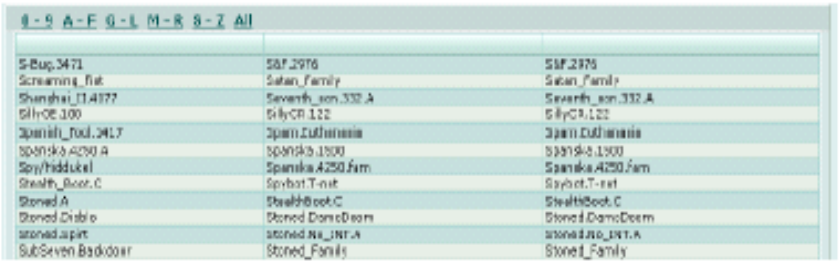
+FGA có thể phát hiện

-100% các loại virus trong WildList(wildlist.org)

-virus trong file nén dùng PKZip

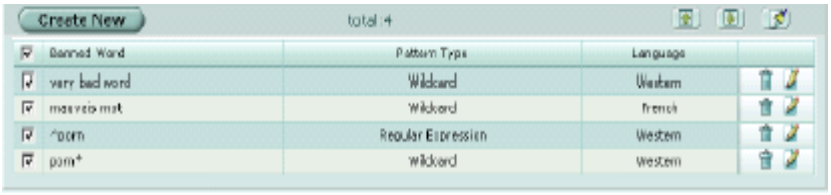
-email được mã hóa bằng uuencode,MINE

- log lại tất cả hoạt động quét.



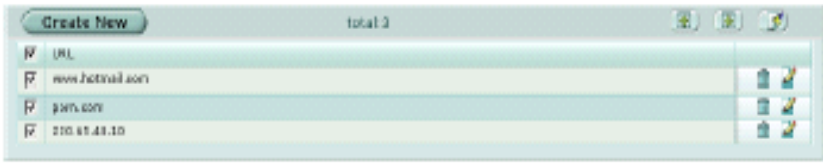
Web Content Filtering

-FGA có thể quét HTTP, các loại URLs, URL patterns và nội dung của web



-Nếu người dùng truy cập trang web trùng với Block list hoặc web chứa 1 từ hoặc 1 cụm từ trong content block list FGA sẽ block trang web đó.Trang web bị blocked sẽ được thay thế bằng trang thống báo blocked

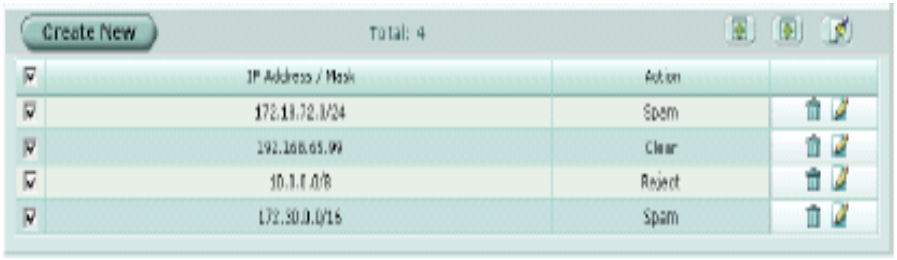
-FGA FortiGuard sẽ block một loại nội dung web nào đó



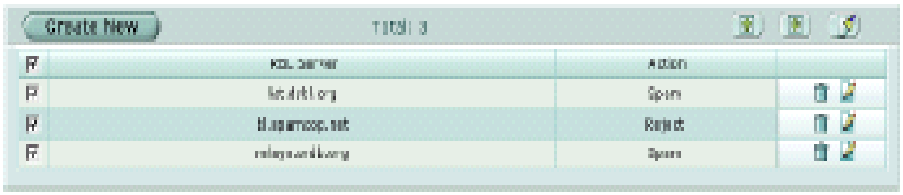
-FGA lọc Java Applet , Cookies và ActiveX…

Spam Filtering

-FGA quét lọc spam qua các giao thức email POP 3, SMTP, IMAP, địa chỉ IP, địa chỉ email, tiêu đề email,nội dung email…



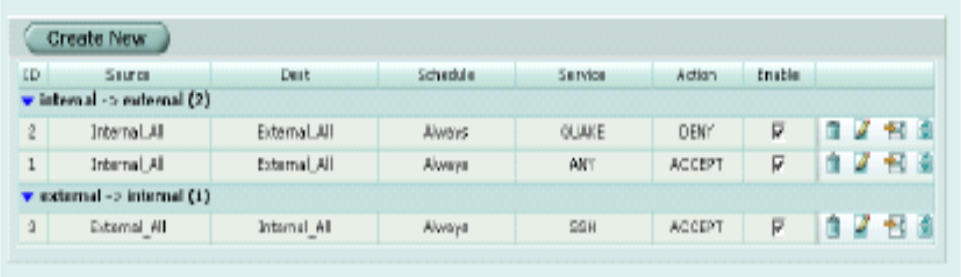
-Chức năng RBL(Realtime Blackhole List)phân loại spam và sắp xếp vào blackhole và ORDBL(Open Relay Database List)chức năng chống gởi mail nặc danh…



-Nếu email được FGA cho là spam thì email sẽ được thêm tab vào subject của email,

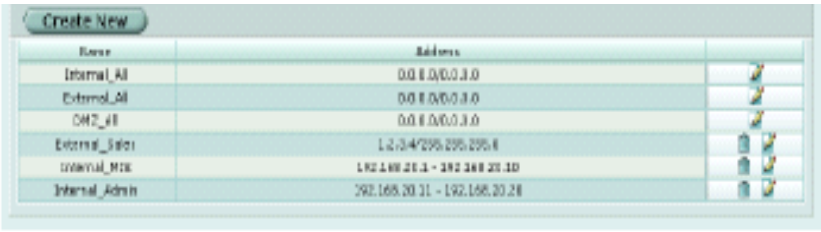
người dùng có thể dùng trình mail client để lọc spam

Firewall



-FGA bảo vệ máy tính trong mạng cục bộ tránh khỏi tấn công từ Internet.

-Sau khi cài đặt sơ bộ FGA có khả năng bảo vệ người dùng trong mạng cục bộ truy suất Internet và blocking các truy suất từ Internet vào mạng cục bộ.



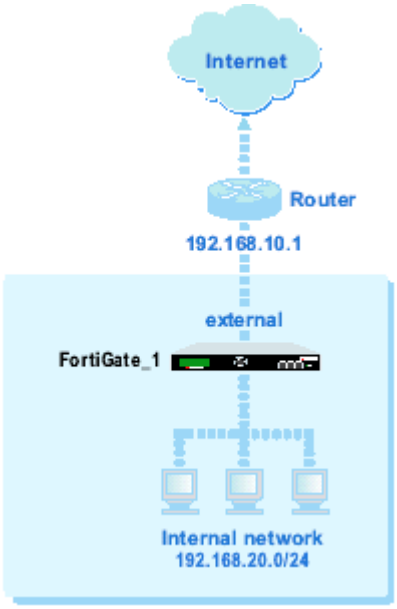
-FGA cho phép cấu hình kiểm soát truy cập từ mạng cục bộ ra ngoài Internet và kiểm

soát truy cập trong mạng nội bộ bao gồm:

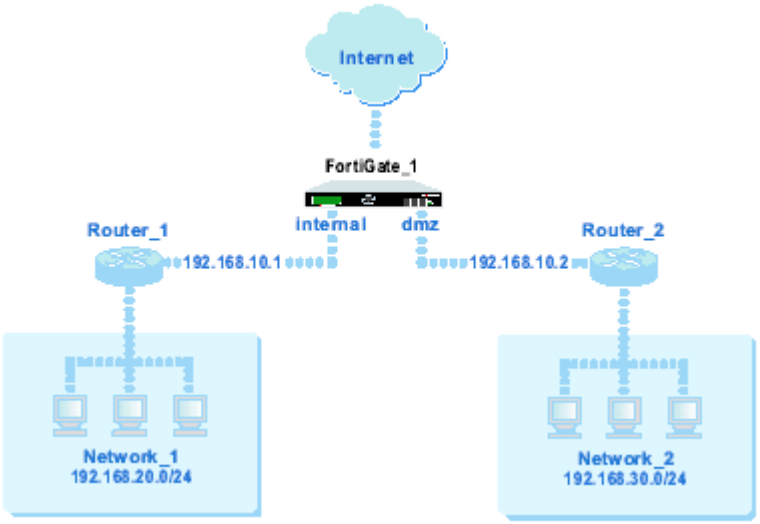
- Kiểm soát tất cả traffic ra vào của mạng
- Kiểm soát mã hóa traffic VPN
- Lọc virus và nội dung web
- Block hoặc cho phép truy cập tất cả policy
- Kiểm soát theo policy
- Chấp nhận hoặc từ chối truy cập từ một địa chỉ
- Kiểm soát người dùng chuẩn và người dùng đặc biệt hoặc nhóm đặc biệt…
- Yêu cầu người dùng chứng thực trước khi truy cập
- Thiết đặt ưu tiên truy cập và bảo đảm hoặc giới hạn băng thông cho từng policy
- Log tất cả kết nối
- NAT/Route Mode Policy
- Mixed NAT và Route Mode policy
- FGA có thể hoạt động NAT/Route mode hoặc Transparent mode

NAT/Route mode

-Ở NAT/Route mode FGA là một thiết Layer 3 , mổi interface có một IP subnet khác nhau và xuất hiện ở thiết bị khác như là một router.



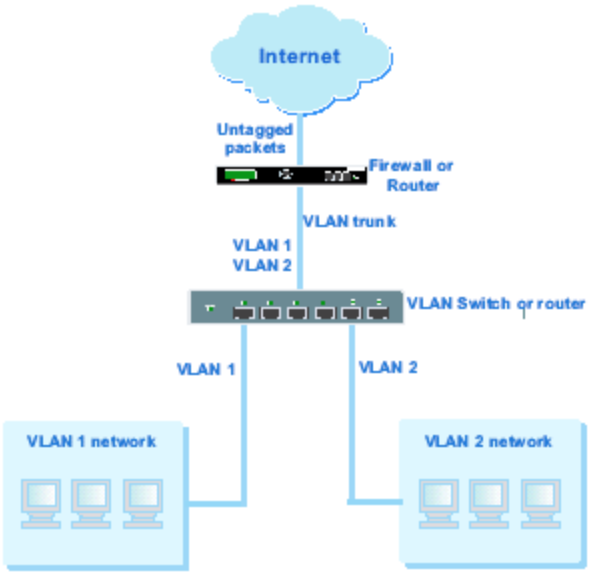
-Đây là nguyên tắc hoạt động của một firewall thông thường.Ở NAT/Route mode, FGA cung cấp NAT mode policies và Route mode policies



-NAT mode policies dùng NAT để giấu địa chỉ giúp gia tăng secure trong mạng kém secure.

-Route mode policies chấp nhận hoặc từ chối kết nối mạng với việc NAT

Transparent mode



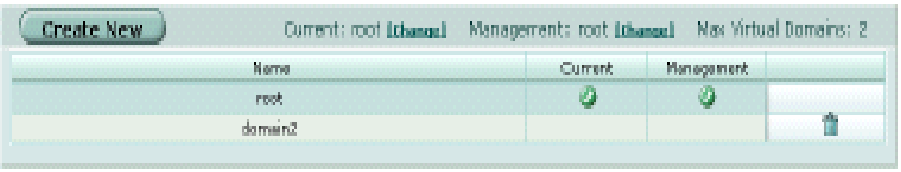
-Transparent mode FGA không làm thay đổi mô hình Layer 3 tức là các interface có cùng 1 IP subnet và xuất hiện như là bridge trong các thiết bị mạng khác.

-FGA hoạt động ở Transparent mode sẽ cung cấp giải pháp antivirus và content filtering đứng đằng sau giải pháp firewall có sẵn.

-Transparent mode cung cấp basic firewall như NAT mode.FGA sẽ block hoặc chấp nhận packets tùy thuộc vào firewall policy.

-FGA có thể gắn vào bất kỳ trong mạng không cần thay đổi cấu trúc và các thành phần của mạng.Tuy nhiên một vài tính năng firewall cao cấp chỉ có ở NAT/Route mode.

VLANs và virtual domains



-FGA support IEEE 802.1Q VLAN tags.

-Dùng VLAN, FGA đơn có khả năng cung cấp security, kiểm soát security kết nối , nhiều security domain gắn vào VLAN IDs thêm vào VLAN packets.

-FGA có thể nhận ra VLAN IDs và apply security policies để secure network và IPSEC VPN giữa security domain.

-FGA có khả năng chứng thực, content filtering và antivirus protection đối với traffic VLAN-tagged network và VPN.

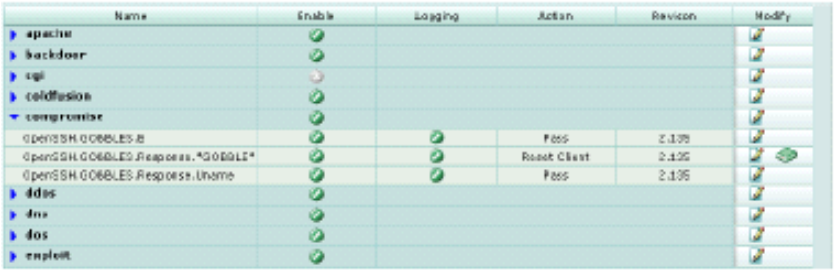
-FGA support VLANs NAT/Route mode và Transparent mode.Ở NAT/Route mode , người dùng nhập vào VLAN subinterfaces để gửi và nhận VLAN packets.

-FGA virtual domains cung cấp nhiều firewall và router logic trên cùng một FGA.

-Khi sử dung virtual domains 1 FGA cung cấp firewall và routing services cho nhiều networks.

-Người dùng có thể tạo và quản lý interfaces, Vlan subinterfaces, zones, firewall policies, routing, và cấu hìnhVPN cho mỗi virtual domains.Mỗi virtual domains là một FGA logic, việc chia ra virtual domains để cấu hình đơn giản, trong cùng một lúc người dùng không thể quản lý nhiều router và firewall.

Intrusion Prevention System(IPS)

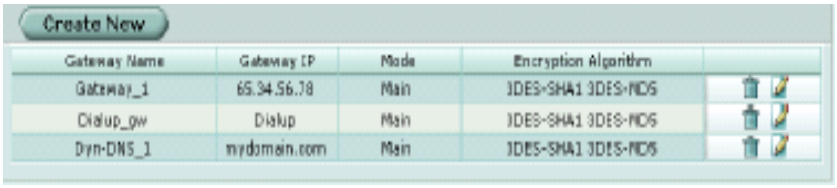


-FGA IPS kết hợp signature và anomaly based intrusion detection and prevention.

-FGA có thể ghi nhận traffic đáng ngờ bằng log, gởi email cảnh báo đến administrator, có thể log, pass,drop,reset hoặc clear packets hoặc session đáng ngờ.

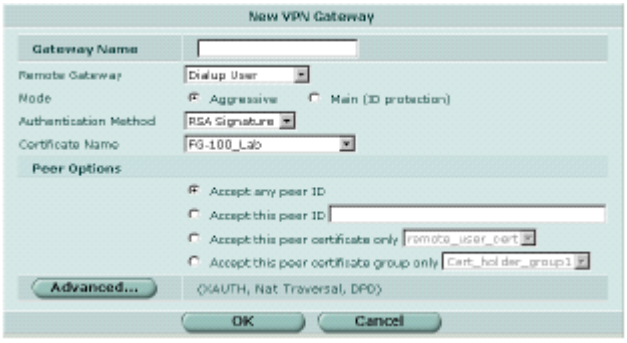
-Cả IPS predefined signatures và IPS engine có thể upgrade thông qua ForiProtect Distribution Network(FDN).Người dùng có thể tạo signatures riêng.

VPN



-Sử dụng FGA VPN, người dùng được cung cấp secure connetion giữa separated office networks hoặc telecomuters hoặc travellers với an office network.

-FGA VPN bao gồm



I

Industry standard and ICSA-certified IPSec VPN

• IPSec VPN in NAT/Route and Transparent mode,

- IPSec, ESP security in tunnel mode,
- DES, 3DES (triple-DES), and AES hardware accelerated encryption,
- HMAC MD5 and HMAC SHA1 authentication and data integrity,
- AutoIKE key based on pre-shared key tunnels,
- IPSec VPN using local or CA certificates,
- Manual Keys tunnels,
- Diffie-Hellman groups 1, 2, and 5,
- Aggressive and Main Mode,
- Replay Detection,
- Perfect Forward Secrecy,
- XAuth authentication,

• Dead peer detection,

• DHCP over IPSec,

• Secure Internet browsing.

• PPTP for easy connectivity with the VPN standard supported by the most popular operating systems.

• L2TP for easy connectivity with a more secure VPN standard, also supported by many popular operating systems.

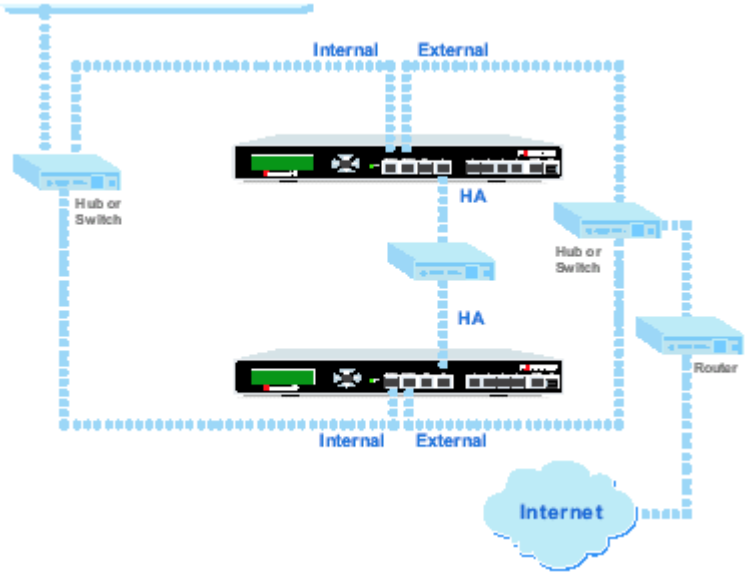
• Firewall policy based control of IPSec VPN traffic.

• IPSec NAT traversal so that remote IPSec VPN gateways or clients behind a NAT can connect to an IPSec VPN tunnel.

• VPN hub and spoke using a VPN concentrator to allow VPN traffic to pass from one tunnel to another through the FortiGate unit.

• IPSec Redundancy to create a redundant AutoIKE key IPSec VPN connection to a remote network.

High availability(HA)



-FGA HA là công nghệ sử dụng nhiều phần cứng FGA và FortiGate

Clustering Protocol (FGCP).

-Mỗi FGA là một HA cluster cùng security policy và cùng cấu hình.Người dùng có thể thêm đến 32 FGA vào HA cluster.

-Mỗi FGA là một HA cluster phải cùng model và cùng chạy FortiOS firmware.FGA HA supports link redudancy và device redundancy.

-FGA có thể hoạt động active-passive(A-P) hoặc active-active(A-A) mode. A-A và A-P cluster có thể chạy ở NAT/Route và Transparent mode

-A-P HA cluster như là hot standby HA bao gồm 1 FGA primary processes traffic và 1 hoặc nhiều FGA subordinate.

-FGA subordinate nối vào network và thành FGA primary nhưng không processes traffic

-A-A HA cluster load balances virus scanning trên tất cả FGA trong cluster.

-A-A HA clusters bao gồm 1 FGA primary processes traffic và 1 hoặc nhiều secondary FGA cũng processes traffic.

-Primary FGA sử dụng thuật toán scanning virus phân tán trên tất cả FGA trong HA cluster.

Secure installation, configuration, and management

-Khi bật nguồn FGA lần đầu tiên, FGA được cấu hình với default IP và security policies.

-Kết nối đến FGA thông qua web-based, chỉnh mode hoạt động, dùng Setup wizard để set lại IP và FGA sẵn sàng bảo vệ network.

-Người dùng dùng web để cấu hình tính năng cao cấp của FGA.

-

Người dùng có thể tạo basic configuration cho FGA thông qua LCD nút điều khiển

Web-based manager

-Sử dụng HTTP hoặc HTTPS từ máy tính nào có IE, người dùng có thể connect và quản lý FGA.

-FGA support nhiều ngôn ngữ

-Người dùng cấu hình FGA thông qua HTTP và HTTPS từ bất kỳ interfaces

-Người dùng có thể dùng web để cấu hình hầu hết FGA settings.

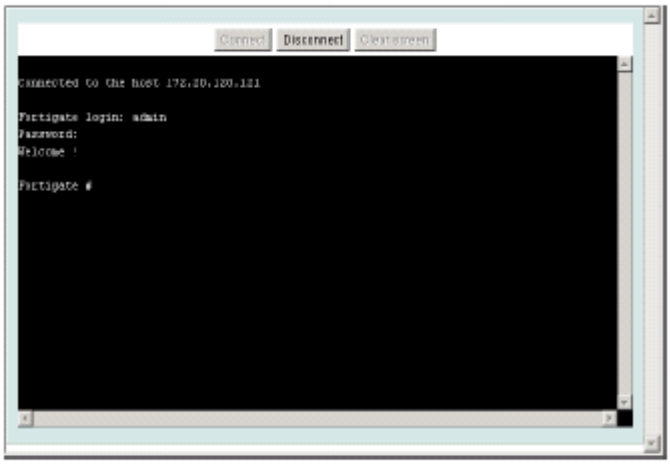
-Người dùng có thể dùng web để quản lý monitor status của FGA

-

-Cấu hình được thay đổi bởi web sẽ có tác dụng tức thì không cần resetting firewall hoặc ngắt dịch vụ.

-Khi đã hài lòng với cấu hình, bạn có thể download về và save lại.Cấu hình sao luu có thể phục hội bất cứ lúc nào.

Command line interface



-Bạn có thể access FGA command line interface (CLI) bằng cách kết nối

cổng serial máy tính đến FGA RS-232 serial console connector.

-Bạn có thể sử dụng Telnet hoặc secure SSH connection để connect đến CLI từ bất kỳ

network nào đã connect đến FGA, kể cả Internet.

-Giao tiếp CLI supports cùng configuration và chức năng monitoring như web-based manager.

-Thêm vào đó, bạn có thể sử dụng CLI cho advanced configuration mà web-based manager không có sẵn.

Logging and reporting

-The FGA supports logging rất nhiều thay đổi về categories của traffic và configuration

-Bạn có thể configure logging to:

• báo cáo traffic connects đến firewall,

• bao cáo network services được sử dụng,

• báo cáo traffic được cho phép trong firewall policies,

• báo cáo traffic bị từ chối trong firewall policies,

• báo cáo sự kiện như configuration thay đổi và events khác, IPSec tunnel negotiation, virus detection, attacks, and web page blocking,

• báo cáo attacks detected bởi IPS,

• gởiemail to system administrators to báo cáo virus ,intrusions, and firewall hoặc VPN events hoặc bị xâm nhập.

-Logs có thể sent đến remote syslog server hoặc 1 WebTrends NetIQ Security Reporting Center and Firewall Suite server sử dụng định dạng WebTrends enhanced log .

-FGA có thể save logs vào hard drive. Nếu hard drive không được installed, bạn có thể

configure FGA ghi log hầu hết events gần và attacks detected by IPS vào system memory.

Người viết: Nguyễn Quốc Hân

VNPro Web Admin