BKAV NGFW

STT	Tính năng	Mô tả
1	**Chính sách bảo mật - Security Policy**	Thiết lập được Policy và hỗ trợ các dịch vụ sau đây khi có yêu cầu được phép truy cập:
1.1	Required Services Security Policy	Hỗ trợ chức năng thiết lập chính sách kiểm soát truy cập
1.2	Enforcing the Required Services Security Policy	
1.2.1	Traffic Permitted Inbound	Hỗ trợ các yêu cầu truy cập từ mạng Public tới các dịch vụ bên trong mạng riêng. Đáp ứng cho các dịch vụ sau: 1. FTP (Active and Passive Mode – IPV4 and IPV6) 2. HTTP (IPV4 and IPV6) 3. HTTPS (IPV4 and IPV6) 4. SMTP (IPV4 and IPV6)) 5. DNS and EDNS0 (may be hosted by the firewall – IPV4 and IPV6) 6. POP3 (IPv4 only) 7. IMAP(IPv4 only) 8. SSH (IPv4 only)
1.2.2	Traffic Permitted Outbound	Hỗ trợ các yêu cầu truy cập từ các máy trong mạng riêng đến các dịch vụ ở ngoài mạng Public. Đáp ứng cho các dịch vụ sau: 1. TELNET (IPv4 only) 2. FTP (Active and Passive Mode – IPV4 and IPV6) 3. HTTP (IPV4 and IPV6) 4. HTTPS (IPV4 and IPV6) 5. SMTP (IPV4 and IPV6) 6. DNS and EDNS0 7. POP3 (IPv4 only) 8. IMAP(IPv4 only) 9. SSH (IPV4 and IPV6)
1.2.3	Traffic Permitted for Candidate Firewall Product	- Hỗ trợ các yêu cầu truy cập Quản Trị từ xa, từ các máy mạng private hoặc public. - Từ FW có thể truy cập tới dịch vụ private hoặc public để đồng bộ thời gian.
1.2.4	DROP OR DENY ALL	Tất cả lưu lượng truy cập thông qua FW mặc định bị loại bỏ hoặc từ chối
1.3	No Special Software or Specific Platforms	FW không loại trừ hỗ trợ cụ thể cho bất kỳ lưu lượng từ paltform hoặc hệ điều hành nào, trên các máy chủ, máy khách hoặc dịch vụ private hoặc public
2	**Administration**	
2.1	Administrative Functions	
2.1.1	- Cấu hình thay đổi thời gian hệ thống	Cho phép thay đổi thời gian hệ thống
2.1.2	Cấu hình phương pháp xác thức	Thay đổi các phương pháp xác thực
2.1.3	Cấu hình các thông số quản trị từ xa	Cho phép vào cấu hình từ xa
2.1.4	Cấu hình bật ghi log các sự kiện	Cấu hình ghi log
2.1.5	Xem lại các dữ liệu log	Xem lại log
2.2	Administrative Interface	Có giao diện quản trị (console hoặc web) để có thể truy cập và sử dụng các chức năng quản trị
2.3	Administrative Interface Authentication	Giao diện quản trị phải có cơ chế xác thực khi truy cập
2.4	Authentication Mechanism	Phải sử dụng mật khẩu hợp lệ hoặc một số Cơ chế xác thực mạnh hơn trước khi cấp quyền truy cập vào Chức năng quản trị
2.5	Access Control Rules Administrative Functions	Chức năng quản trị trên hệ thống phải có thể thực hiện các hành động sau:
2.5.1	Tạo các chính sách kiểm soát truy cập	Viết ra các chính sách để kiểm soát truy cập
2.5.1	Xem lại các chính sách kiểm soát truy cập	Xem được các chính sách đã tạo
2.5.3	Thay đổi quy tắc kiểm soát truy cập	Chỉnh sửa chính sách
2.6	Remote Administration	Hỗ trợ quản trị từ xa và lưu lượng phải được mã hóa
2.7	Local Administration	Hỗ trợ quản trị cục bộ thông qua giao **"Administrative Interface"**
2.8	Administrative Accounts	Cho phép cấu hình nhiều tài khoản quản trị với quyền khác nhau
3	**Ghi log - Logging**	
3.1	Required Events	
3.1.1	Tất cả các truy cập inbound (từ mạng internet vào dịch vụ bên trong) đã được định nghĩa trong Policy	
3.1.2	Tất cả các truy cập outbound được phép từ các máy khách hoặc dịch vụ trong mạng privvate ra bên ngoài	
3.1.3	Tất cả các yêu cầu truy cập bị từ chối (drop) từ mạng private hoặc public	
3.1.4	Ghi lại log xác thực thành không hoặc không vào giao diện quản trị	
3.1.5	Ghi lại các phiên truy cập vào giao diện quản trị	
3.1.6	Log khởi động, log cấu hình hệ thống	
3.2	Required Data	Yêu cầu data của mỗi sự kiện log
3.2.1	Date and Time	
3.2.2	Protocol	
3.2.3	Source IP Address	
3.2.4	Destination IP Address	
3.2.5	Source Port (TCP and UDP);	
3.2.6	Destination Port (TCP and UDP);	
3.2.7	Đối với loại sự kiện "Ghi log truy cập vào quản trị" yêu cầu phải có trường đã xác thực thành công hay không?	
3.3	Precision of Date and Time	Ngày và giờ được ghi lại trong nhật ký bắt buộc phải phản ánh chính xác thời điểm xảy ra sự kiện
3.4	Data Presentation	Tất cả các sự kiện được trình bày dưới dạng ngôn ngữ con người có thể đọc được
3.5	Log Access Control Rule Change Events	Ghi log khi có sự cấu hình thay đổi về Policy kiểm soát
3.6	Other Requirements	Ghi log được các dịch vụ thêm (VoIP, IPv6) và các tính năng HA
4	**Persistence**	(Khả năng giữ lại cấu hình không thay đổi khi xảy ra restart, mất điện, ...)
4.1	Security Policy	Các chính sách không bị mất hoặc thay đổi
4.2	Logs	Giữ nguyên các log
4.3	Authentication Configuration Data	
4.4	Remote Administration Configuration	Giữ các các cấu hình
4.5	Date and Time Persistence	Đồng bộ được thời gian khi hệ thống khởi động lại
6	**High Availability**	
6.1	HA Configuration	Có khả năng cấu hình để hỗ trợ hoạt động chủ động **hoặc** bị động
6.2	HA Functional	
6.2.1	Established TCP sessions tiếp tục hoạt động sau khi một sự kiện lỗi xảy ra trên một thiết bị	Lỗi: - Mất kết nối mạng - Mất điện
6.2.2	Phải có khả năng duy trì tối thiểu 66,6% số lượng kết nối đồng thời được ghi nhận	
6.3	HA Reaction Time	Sự kiện chuyển đổi dự phòng trong vòng 65s
6.4	HA Event Logging	Ghi log khi chuyển đổi trạng thái Active, Passive
6.5	HA Administration	HA có các chức năng sau: - Phương án xác định được trạng thái hiện tại (đang hoạt động Active hay Passive) - Phương pháp làm cho một thiết bị Active khi có yêu cầu
7	**IPv6**	
7.1	IPv6 Configuration	Hỗ trợ cấu hình ở chế độ Dual stack (IPv4/IPv6)
7.2	IPv6 Administration	Có khả năng chặn tất cả quyền truy cập vào Quản trị với IPv6
7.3	IPv6 Security	
7.3.1	Administrative Access	Có khả năng quản trị thông qua IPv6
7.3.2	Fragmentation Handling	Có khả năng xử lý phân mảnh gói tin
7.3.3	Blocking of Packets	Có khả năng chặn các gói tin Ipv6
7.4	IPv6 Logging	Log phải hiển thị được các thông tin: A. Date and Time B. Indication traffic is IPv6; C. Source IPv6 Address - from the Candidate Firewall Product's perspective; D. Destination IPv6 Address - from the Candidate Firewall Product's perspective; E. Next Header; F. Extension headers; G. Source Port (TCP and UDP); H. Destination Port (TCP and UDP); I. Message Type (ICMPv6); J. Disposition of the Event.
8	**VoIP support**	Hỗ trợ VoIP
9	VPN support	Hỗ trợ các kết nối VPN (Virtual Private Network)
10	Security	NGFW cung cấp các tính năng bảo mật mạnh mẽ để quản lý, giám sát và ngăn chặn các cuộc tấn công mạng
10.1	anti-virus	Phát hiện và chặn các file độc hại
10.2	url filter	lọc url
10.3	SSL inspection	Giải mã lưu lượng HTTPS (mã hóa bằng SSL/TLS) giữa người dùng và máy chủ đích, để kiểm tra nội dung trước khi lưu lượng được chuyển tiếp
11	Application Control	Giúp quản trị viên mạng giám sát và kiểm soát các ứng dụng hoặc dịch vụ chạy trên mạng
13	Multi-WAN	Cho phép một thiết bị sử dụng nhiều kết nối Internet (WAN)
14	WAN Failover	Giúp đảm bảo tính sẵn sàng cao cho kết nối Internet bằng cách tự động chuyển sang một kết nối WAN dự phòng nếu kết nối chính (WAN chính) gặp sự cố
15	WAN Load Balancing	Cho phép phân phối lưu lượng mạng giữa nhiều kết nối WAN
16	Dynamic DNS	Cho phép người dùng duy trì một tên miền mà có thể tự động cập nhật với địa chỉ IP động của một thiết bị

Trụ sở chính: Tòa nhà Bkav, Khu đô thị Yên Hòa, Cầu Giấy, Hà Nội
Điện thoại: (024) 3763 2552 So fax: (024) 3868 4755
Website: security.bkav.com Email: security@bkav.com
Bkav TP. HCM: So 67, Đường số 3, Khu dân cư City Land, P. 7, Q. Gò Vấp, TP HCM
Điện thoai: (028) 6296 6626 So fax: (028) 2253 6103