CẤU HÌNH ISA SERVER 2006 HTTP FILTER

Bài vi

Bài viết này là một cái nhìn tổng quan về ISA Server 2006 HTTP Filter và cách dùng HTTP Filter để bảo vệ mạng nội bộ của bạn.

Trong bài chúng tôi sẽ cung cấp cho bạn ở mức khái quát cao về ISA Server 2006 HTTP Filter. Chúng tôi cũng sẽ hướng dẫn bạn cách dùng HTTP Filter để bảo vệ mạng nội bộ trước một số kiểu tấn công trong môi trường Webserver Publishing, cách ngăn chặn người dùng sử dụng giao thức Universal Firewall Bypass protocol (HTTP) tạo đường vòng cho tường lửa. Kiểu tạo đường vòng này được tiến hành cho lưu lượng mạng như Microsoft Live Messenger, Yahoo Messenger hay thành phần tương tự có khả năng sử dụng HTTP thay vì các giao thức tự nhiên của chúng. Để hiểu một cách đầy đủ về khái niệm và công nghệ của giao thức HTTP, bạn nên tham khảo thêm tại đây.

Còn bây giờ chúng ta hãy bắt đầu với một số vấn đề cơ bản về Webfilter (bộ lọc Web) trong ISA Server 2006.

Webfilter là gì?

Một Webfilter (tức bộ lọc Web) trong ISA Server 2006 là một tập hợp các thư viện liên kết động (DDL) dựa trên nền tảng mô hình Giao diện lập trình ứng dụng Server Internet IIS (IIS ISAPI).

Webfilter trong ISA Server 2006 cũng được load từ Webproxy Filter. Mỗi lần sử dụng Webfilter, tất cả thông tin sẽ được gửi đến Webproxy Filter. Webproxy Filter chịu trách nhiệm xác định xem kiểu sự kiện nào sẽ được giám sát. Mỗi khi các sự kiện này xuất hiện Webproxy Filter sẽ được thông báo.

Bạn sẽ thấy trong ảnh minh họa bên dưới thành phần bổ sung Add-in của HTTP Filter trên ISA Server 2006.

Hình 1: Thành phần bổ sung add-in hỗ trợ bộ lọc HTTP trong ISA Server 2006 HTTP
Chức năng của Webfilter

Webfilter trong ISA Server 2006 chịu trách nhiệm thực hiện các công việc sau:

• Quét và chỉnh sửa các yêu cầu HTTP.

• Phân tích lưu lượng mạng.
• Quét và chỉnh sửa các đáp ứng HTTP.
• Loại bỏ một số đáp ứng HTTP cụ thể.
• Mã hóa và nén dữ liệu.

Ngoài ra còn nhiều chức năng khác nhưng không quan trọng lắm nên chúng tôi không tiện liệt kê ra ở đây.

Quan trọng:
HTTP Filter trong ISA Server 2006 có một số nguyên tắc riêng, trừ thông số thiết lập độ dài tối đa cho Header. Độ dài tối đa cho Header (Maxium Header) tuân theo tất cả nguyên tắc trong tường lửa với các định nghĩa giao thức HTTP như các thành phần khác.

Đáng lưu ý:
HTTP Filter trong ISA Server 2006 cũng có khả năng lọc lưu lượng HTTPS nhưng chỉ trong trường hợp với các Web Server đối chiếu dùng HTTPS Bridging. Nếu bạn muốn kiểm tra HTTPS sắp hết hạn qua bộ lọc ISA Server 2006 HTTP, bạn phải dùng phần mềm được phát triển bởi nhóm thứ ba.

Cấu hình bộ lọc HTTP Filter

Nếu bạn muốn bắt đầu cấu hình bộ lọc HTTP, kích phải chuột lên một quy tắc có chứa định nghĩa giao thức HTTP và chọn Configure HTTP từ menu ngữ cảnh.

Hình 2: Các thiết lập chung cho bộ lọc ISA Server 2006 HTTP.
Request Header

Maximum Headers length (bytes): là số byte lớn nhất cho một yêu cầu HTTP trong URL và HTTP Header cho tới khi ISA Server loại bỏ yêu cầu.

Request Payload

Maximum payload length (bytes): Với tùy chọn này bạn có thể giới hạn số byte lớn nhất cho người dùng khi gửi các yêu cầu như HTTP POST trong môi trường Web Server.

URL-Protection

Maximum URL Length (Bytes): độ dài lớn nhất của một URL được phép.

Maximum Query length (Bytes): độ dài lớn nhất của một URL trong yêu cầu HTTP.

Verify normalization

Bạn có thể chọn hộp kiểm này để đặc tả các yêu cầu đường dẫn URL chứa ký tự viết hoa sau ký tự

thường và sẽ được sẽ được thay thế bằng chữ thường. Bình thường hóa là quá trình giải mã các yêu cầu URL được mã hóa. Sau khi giải mã, URL sẽ được bình thường trở lại để chắc chắn rằng chương trình không dùng ký tự % khi mã hóa URL. Nếu HTTP Filter tìm ra điểm khác nhau trong URL sau lần bình thường hóa thứ hai, các yêu cầu sẽ bị loại bỏ.

Block High bit character

Các đường dẫn URL có chứa Ký tự byte kép (DBCS) hay kiểu Latin1 sẽ được loại bỏ nếu thiết lập này được kích hoạt. Một thiết lập kích hoạt thông thường sẽ loại bỏ các ngôn ngữ đòi hỏi hơn 8 bit trong hiển thị ký tự.

Executables

Loại bỏ các đáp ứng chứa nội dung thực thi Windows. Tùy chọn này loại bỏ việc download và thực hiện các nội dung thực thi như file EXE.

Tiếp theo chúng ta sẽ cấu hình các phương thức HTTP được phép hoặc loại bỏ.

Hình 3: Các phương thức HTTP
Trong ví dụ này chúng ta đang loại bỏ lệnh HTTP POST để không ai có thể upload nội dung lên các website bên ngoài.

Hình 4
Loại bỏ các thực thi

Với tùy chọn này bạn có thể loại bỏ hoặc cho phép một số đuôi file mở rộng cụ thể trong quy tắc tường lửa (Firewall).

Hình 5: Dùng ISA Server 2006 để loại bỏ một số đuôi mở rộng của file
Loại bỏ các yêu cầu chứa tên mở rộng mơ hồ

Tùy chọn này chỉ thị cho bộ lọc HTTP loại bỏ tất cả tên file mở rộng ISA Server 2006 không thể xác định được.

Trong ví dụ này chúng ta sẽ loại bỏ quyền truy cập vào tên file mở rộng .EXE.

Hình 6: Loại bỏ tên file mở rộng .EXE
Điều khiển HTTP Header

Khi một Web Client gửi yêu cầu tới Web Server hoặc Web Server trả lời yêu cầu, phần đầu tiên của câu trả lời là một HTTP request hoặc HTTP response. Sau HTTP request hoặc HTTP response, Client hay Server sẽ gửi HTTP Header. Trường Header request cho phép Client gửi thông tin thêm tới Server. HTTP Header chứa thông tin về trình duyệt, hệ điều hành và các chi tiết cấp phép… Header client sử dụng phân phối User-Agent để xác định xem ứng dụng nào chịu trách nhiệm thực

hiện yêu cầu.

Với sự trợ giúp của bộ lọc HTTP Filter, bạn có thể loại bỏ một số HTTP Header nào đó nếu muốn.

Hình 7: Phần Header của bộ lọc HTTP Filter.
Các thiết lập trong trường Server Header cung cấp cho người quản trị khả năng điều khiển loại bỏ các Header HTTP hoặc chỉnh sửa HTTP Header trong phần trả lời và một số thiết lập khác.

Ở ví dụ dưới chúng ta dùng thành phần HTTP Header trong ISA Server 2006 để loại bỏ Kazaa, thông tin nằm trên Request Header.

Hình 8: Loại bỏ Kazaa
Các ký hiệu trong HTTP Filter

Một ký hiệu HTTP có thể tồn tại trong phần thân HTTP hoặc phần tiêu đề. Bạn có thể dùng các ký hiệu HTTP để từ chối thực thi trên các ứng dụng cụ thể. Muốn tìm một ký hiệu HTTP riêng nào đó, bạn phải biết ký hiệu nào đang dùng cho ứng dụng nào. Một số tài liệu trên Internet có thể giúp bạn tham khảo thêm thông tin về các ký hiệu HTTP, nhưng bạn cũng có thể dùng sniffer mạng để xác định các ký hiệu này. Tôi sẽ chỉ cho bạn cách dùng sniffer mạng ở phần dưới.

Quan trọng:
Việc lọc các ký hiệu HTTP trong ISA Server 2006 chỉ được tiến hành khi các yêu cầu và đáp ứng (request/response) được mã hóa kiểu UTF-8.

Hình 9: Loại bỏ các ký hiệu HTTP
Trong ví dụ dưới chúng ta sẽ loại bỏ quyền truy cập giao thức Windows Live Messenger.

Hình 10: Loại bỏ Windows Live Messenger
Nếu bạn muốn biết nhiều hơn về các ký hiệu ứng dụng, xin mời click vào đây.

Quan trọng:
ISA Server 2006 chỉ kiểm tra 100 byte đầu tiên trong thân yêu cầu và đáp ứng. Bạn có thể tăng thêm số byte lớn nhất nhưng điều này sẽ thể khiến một số thực thi Server bị giảm hiệu quả.

Thông báo lỗi HTTP nếu HTTP Filter loại bỏ nội dung

Hình 11: Thông báo truy cập HTTP Filter
Tìm ra các HTTP Header cụ thể như thế nào

Muốn tìm các ký hiệu HTTP chưa được biết đến, bạn có thể dùng một sniffer mạng như Windows Netmon 3.0 để dò tìm lưu lượng mạng HTTP.

Phần minh họa dưới thể hiện một kiểu dò tìm mạng mẫu trên Microsoft Netmon 2.0, nhưng bạn có thể dùng bất kỳ chương trình giám sát mạng khác như Wireshark (trước đây là Ethereal).

Hình 12: Dò tìm Netmon HTTP
Ví dụ này đưa ra yêu cầu kiểu (GET), yêu cầu HTTP Header (HTTP/1.1) User-Agent (Mozilla/4.0) và ký hiệu (MSIE 6.0).

HTTPFILTERCONFIG.VBS

Bạn có thể dùng HTTPFILTERCONFIG.VBS từ thư mục C:\PROGRAMME\MICROSOFT ISA SERVER 2006 SDK\SDK\SAMPLES\ADMIN trên ISA Server 2006 SDK để nhập và xuất các cấu hình HTTP-Filter.

Hình 13: HTTPFILTERCONFIG.VBS trên ISA 2006 SDK
Kết luận

Trong bài này chúng ta đã tìm hiểu về cách thức hoạt động của bộ lọc HTTP ISA Server 2006. HTTP Filter trong ISA Server 2006 là một công cụ lớn giúp loại bỏ một số nội dung nguy hiểm để bảo vệ chống lại các mã độc hại hoặc Trojan, worm. Bạn cũng có thể dùng HTTP Filter để loại bỏ một số ký hiệu HTTP cụ thể. Loại bỏ các ký hiệu này sẽ giúp người quản trị hạn chế được một số kiểu ứng dụng như Windows Live Messenger. Các kiểu ứng dụng này được tạo ra từ HTTP nếu giao thức thông thường được loại bỏ bởi các phần hạn chế trong tường lửa.