Contents

[1.Tổng quan 1](#_Toc155291434)

[2.Bộ lọc gói tin (Packet Filter) 2](#_Toc155291435)

[ Khái niệm chung 2](#_Toc155291436)

[ Bộ lọc phi trạng thái 2](#_Toc155291437)

[ Bộ lọc có trạng thái 4](#_Toc155291438)

[3. Cổng mạch (Circuit Gateways) 5](#_Toc155291439)

[ Khái niệm chung 5](#_Toc155291440)

[ Cấu trúc cơ bản 5](#_Toc155291441)

[4. Cổng ứng dụng (Application Gateways) 6](#_Toc155291442)

[ Khái niệm chung 6](#_Toc155291443)

[ Cache Gateways 6](#_Toc155291444)

[5. Bastion Hosts 6](#_Toc155291445)

[6. Cấu hình tường lửa 7](#_Toc155291446)

[ Khái niệm chung 7](#_Toc155291447)

[ Single-Homed Bastion Host System 7](#_Toc155291448)

[ Dual-Homed Bastion Host System 8](#_Toc155291449)

[ Screened Subnets 8](#_Toc155291450)

[ Demilitarized Zones (DMZ) 9](#_Toc155291451)

[ Network Security Topology 9](#_Toc155291452)

[7. Chuyển dịch địa chỉ mạng 9](#_Toc155291453)

[8. TMG – Threat Management Gateway 9](#_Toc155291454)

[1. Yêu cầu cài đặt 10](#_Toc155291455)

[2. Tính năng chính của TMG 10](#_Toc155291456)

[3. Các điểm mới của TMG so với ISA 11](#_Toc155291457)

[4. Các mô hình mạng trong TMG 11](#_Toc155291458)

[5. Cơ chế hoạt động 14](#_Toc155291459)

# 1.Tổng quan

* Các thuật toán mã hoá không hiệu quả khi ngăn chăn các gói tin độc hại đi vào mạng cục bộ.
* Các giải thuật chứng thực có thể được sử dụng để xác định các gói tin đến từ các user tin cậy và giúp ngăn chặn các gói tin độc hại đi vào mạng. Tuy nhiên, các máy tính trong mạng đa số đều không có đủ tài nguyên, phương tiện… để thực hiện các giải thuật chứng thực trong mọi tình huống.

→ Kỹ thuật tường lửa (Firewall)

* Tường lửa là công cụ dùng để hạn chế việc truy cập mạng nhằm bảo mật cho mạng nội bộ.
* Tường lửa ngăn cách giữa vùng không đáng tin cậy là mạng Internet (external network) và vùng có độ tin cậy cao là mạng nội bộ (internal network), ngăn chặn hoặc cho phép các gói tin đi qua giữa hai mạng này dựa trên nguyên tắc quyền tối thiểu.
* Tường lửa có thể là một thiết bị phần cứng, một gói phần mềm hoặc là sự kết hợp của cả hai.
* Tường lửa có thể được nhúng vào các thiết bị mạng phổ biến như router, switch, modem, wireless access point.
* Tường lửa cứng (phần cứng) nhanh nhưng khó cập nhật.
* Tường lửa mềm (phần mềm) linh hoạt hơn vì dễ dàng cập nhật.

Một số tường lửa cứng (phần cứng) thông dụng:

* Cisco Router
* FortiNet
* CheckPoint Safe@Office
* Sonicwall PRO
* WatchGuard Firebox

Một số tường lửa mềm (phần mềm) thông dụng:

* Comodo Firewall
* ESET Smart Security
* ZoneAlarm
* Outpost Firewall Pro
* F-Secure Internet Security

Dựa trên các phương thức đặc trưng riêng, tường lửa có thể được phân thành các loại:

* packet filter: kiểm tra cả IP header lẫn TCP header.
* circuit gateway: kiểm tra giao thức TCP giữa các gói tin (chỉ kiểm tra TCP header)
* application gateway
* dynamic packet filter: là tường lửa lai, kết hợp cả hai loại packet filter và circuit gateway vào trong một hệ thống tường lửa.

# 2.Bộ lọc gói tin (Packet Filter)

## Khái niệm chung

* Là kỹ thuật tường lửa cơ bản.
* Kiểm tra các gói tin từ bên ngoài đi vào mạng nội bộ và từ mạng nội bộ đi ra bên ngoài.
* Chỉ kiểm tra IP header và TCP header, không kiểm tra phần payload sinh ra từ lớp ứng dụng.
* Sử dụng một tập các quy tắc để quyết định xem gói tin nào được cho phép hoặc bị từ chối đi vào (ra).
* Gồm hai loại:
* stateless filtering (bộ lọc phi trạng thái)
* stateful filtering (bộ lọc có trạng thái)

## Bộ lọc phi trạng thái

* Là kỹ thuật tường lửa đơn giản nhất và được sử dụng rộng rãi nhất.
* Xử lý mỗi gói tin như một đối tượng độc lập.
* Kiểm tra một gói tin khi nó đến, ra quyết định phù hợp và không lưu lại bất kỳ thông tin nào về gói tin này.
* Cách xử lý của bộ lọc này là sắp xếp và kiểm tra gói để chắc chắn địa chỉ đích là hợp lệ.

Tổng quát, bộ lọc phi trạng thái thường kiểm tra:

* Địa chỉ IP nguồn và đích trong IP header theo một tập quy tắc đã được xác định trước.
* Port nguồn và port đích trong một TCP header hoặc UDP header.
* Tập quy tắc thường được gọi là một Access control list (ACL).

Vì lớp mạng có nhiệm vụ kiểm tra IP header để có thể phân phối các gói tin nên việc hiện thực bộ lọc gói tại lớp mạng không đòi hỏi phải tính toán nhiều.

A screenshot of a computer program

Description automatically generated

Bộ lọc phi trạng thái thường chận những kiểu gói tin:

* Một gói đi vào có địa chỉ IP nội bộ giống như địa chỉ IP nguồn nhằm mục đích che giấu chính nó như là một gói tin hợp pháp trong mạng nội bộ.
* Một gói (vào hoặc ra) có quy định cụ thể bộ định tuyến sẽ được sử dụng nhằm mục đích bỏ qua các tường lửa xác định.
* Một gói có phần payload rất nhỏ với mục đích làm TCP header trong phần payload sẽ bị ngắt thành hai hay nhiều phần. Ví dụ như đóng gói port nguồn và port đích trong những gói IP khác nhau. Đây là cách tấn công TCP fragmentation attack.

Ngoài việc chận những gói tin độc hại đi vào, bộ lọc phi trạng thái còn chận những gói tin nội bộ đi ra mạng ngoài có đặc tính là những gói điều khiển dùng cho việc thực thi truyền thông trong mạng nội bộ:

* Bootp (Bootstrap Protocol)
* DHCP (Dynamic Host Configuration Protocol)
* TFTP (Trial File Transfer Protocol)
* NetBIOS (Network Basic Input / Output System)
* LRP (Line Printer Remote Protocol)
* NFS (Network File System)

Ưu điểm: dễ thực hiện, vì chỉ kiểm tra các IP header và TCP header.

Nhược điểm:

* Không ngăn chặn được các gói tin độc hại khai thác sơ hở của các phần mềm ở tầng ứng dụng.
* Do mỗi gói tin phải được kiểm tra đối với toàn bộ ACL, có thể gây nên một nút cổ chai trên một mạng tốc độ cao, dẫn đến thất thoát gói tin và giảm tốc độ truyền ngoài ý muốn.

### Bộ lọc có trạng thái

* Bộ lọc có trạng thái còn được gọi là bộ lọc trạng thái kết nối (connection-state filtering), giữ lại thông tin về kết nối giữa một host nội bộ và một host bên ngoài.
* Một trạng thái kết nối chỉ ra đó là kết nối TCP hay UDP và kết nối này có được thiết lập hay không.
* Trạng thái kết nối được lưu trong một bảng trạng thái (state table).

Khi một gói tin đến (vào hay ra), bộ lọc sẽ kiểm tra xem gói tin này đã có trong bảng trạng thái hay chưa.

* Nếu có, tường lửa sẽ cho gói tin đi qua và lưu lại thông tin (TCP sequence number…) cho lần sau.
* Nếu gói tin này là gói SYN, tường lửa sẽ tạo một entry mới trong bảng trạng thái.
* Nếu gói tin không thuộc về một kết nối đã có và nó không phải là một gói SYN, tường lửa sẽ huỷ nó.
* Số port là một số dương dùng để nhận diện một chương trình riêng biệt. Bất kỳ một port nào được mở bởi một host nội bộ ngầm định sẽ có số port nhỏ hơn 1024.
* Số port nhỏ hơn 1024 là port chuẩn.
* Ngầm định, host bên ngoài sẽ sử dụng số port giữa 1024 và 65535 để thực thi một kết nối với host nội bộ.
* A table with numbers and a few other numbers

  Description automatically generated with medium confidence Bộ lọc có trạng thái và bộ lọc phi trạng thái thường được sử dụng kết hợp với nhau. Khi gặp khó khăn trong việc xác định chận một gói dựa trên trạng thái kết nối, ACL sẽ được sử dụng để giúp ra quyết định chính xác.
* Việc giữ lại các trạng thái kết nối cần đến các cấu trúc dữ liệu phức tạp và các giải thuật tìm kiếm. Thực hiện những công việc này đòi hỏi không gian lưu trữ lớn, hoạt động nhiều hơn của CPU, giảm lưu lượng mạng.
* Attacker có thể đưa một số lượng lớn các gói tin vào tường lửa mục tiêu sử dụng bộ lọc có trạng thái, có thể làm ngắt các kết nối giữa mạng nội bộ và bên ngoài.
* Do đó, khi sử dụng bộ lọc có trạng thái, cần phải chắc chắn rằng có thể quản lý được sự phức tạp giữa thời gian và không gian. Ví dụ, thay vì giữ lại toàn bộ thông tin lịch sử của một kết nối, chỉ cần giữ lại thông tin của kết nối này trong một khoảng thời gian nào đó.

# 3. Cổng mạch (Circuit Gateways)

## Khái niệm chung

* Cổng mạch (Circuit gateways, còn gọi là Circuit-level gateways), thực thi tại tầng vận chuyển (đôi khi có ngoại lệ).
* Thường kết hợp các bộ lọc gói tin và cổng mạch để tạo ra một bộ lọc gói tin động (Dynamic Packet Filter – DFD).

## Cấu trúc cơ bản

Đối tượng của cổng mạch là chuyển tiếp một kết nối TCP giữa một host nội bộ và một host bên ngoài. Do đó, cổng mạch cũng được xem như là một Transparent Proxy Firewall.

* Trước tiên, cổng mạch sẽ xác nhận một phiên TCP (hoặc UDP).
* Kế đó cổng mạch thực thi riêng biệt một kết nối với host nội bộ và một kết nối với host bên ngoài.
* Duy trì một bảng các kết nối hợp lệ và duy trì việc kiểm tra các gói tin đi vào với các thông tin chứa trong bảng.
* Cho phép gói tin đi qua nếu thuộc về một kết nối đã có duy trì trong bảng, ngược lại sẽ bị chận.
* Khi phiên kết thúc, entry tương ứng sẽ bị huỷ khỏi bảng và mạch được đóng lại.
* Trong thực tế, một tổ chức thường phân tách mạng nội bộ của mình với mạng ngoại vi bằng một cổng mạch có một địa chỉ IP public có thể kết nối với ngoại vi, và các host trong mạng nội bộ sử dụng địa chỉ IP private không thể vươn tới được từ Internet.
* Sau khi thực thi một kết nối mạng với host ngoại vi và một kết nối mạng với host nội bộ, cổng mạch sẽ đóng vai trò như là một node chuyển tiếp mà không cần kiểm tra các gói tin đi qua nó. Do đó, một user nội bộ có thể mở một port trên một host nội bộ và chỉ thị cho gateway thực thi kết nối giữa host ngoại vi và host nội bộ.
* Do đó, các gói tin độc hại có thể vào mạng nội bộ qua một kênh đã thiết lập sẵn. Vì vậy, cổng mạch nên được sử dụng cùng với các bộ lọc gói tin.
* Cổng mạch nên sử dụng một tập tin log để ghi nhận lại thông tin của các gói tin (vào, ra) đã xác nhận, bao gồm địa chỉ IP nguồn, port nguồn, địa chỉ IP đích, port đích, và chiều dài của mỗi gói tin. File log này có thể giúp cho việc nhận định các vấn đề phát sinh về sau.

# 4. Cổng ứng dụng (Application Gateways)

## Khái niệm chung

* Còn được gọi là Application-level gateways (ALG) hay Proxy Servers, là các gói phần mềm được cài đặt trên một máy tính được chỉ định.
* Một ALG hoạt động như một proxy cho một host nội bộ, xử lý các dịch vụ được yêu cầu bởi các clients ngoại vi.
* Một ALG thực thi các kiểm tra chi tiết trên mỗi gói IP (vào, ra), bao gồm việc kiểm tra những định dạng chương trình ứng dụng (ví dụ như định dạng MIME, định dạng SQL…) chứa trong gói và xem xét payload của nó có được cho phép hay không.

## Cache Gateways

* Giả sử một tổ chức muốn cài đặt một Web server và cho phép các user hợp pháp trên Internet có thể truy cập đến các trang Web này trên Web server.
* Để bảo vệ Web server khỏi bị tổn hại, một phương án phổ biến là cài đặt một cổng ứng dụng như là một proxy cho Web server này, gọi là Web proxy server.
* Web proxy server nhận các yêu cầu tại cổng 80 từ các client ngoại vi và thực hiện kiểm tra chi tiết phần payload của gói tin.
* Chỉ sau khi phần payload này thoả yêu cầu kiểm tra, Web proxy server sẽ chuyển gói này đến Web server.
* Web proxy server cũng kiểm tra các trang Web do Web server gởi đến các client ngoại vi và lưu chúng trong cache của nó.
* Nếu các client khác cũng yêu cầu những trang Web này, Web proxy server sẽ chuyển trực tiếp các trang này từ cache đến client mày không cần truy cập đến Web server.
* Loại Web proxy server này còn được gọi là cổng ứng dụng (Cache Gateways).
* Một cổng ứng dụng thường sử dụng với một router có khả năng lọc gói tin. Router này được đặt phía sau gateway để bảo vệ các kết nối giữa gateway và các host nội bộ.

# 5. Bastion Hosts

* Một cổng ứng dụng là một máy tính đặt giữa mạng nội bộ và mạng ngoại vi nên dễ bị tấn công bởi attackers từ Internet. Do đó, các máy tính này cần sự bảo vệ nghiêm ngặt để trở thành bastion hosts.
* Bastion hosts là các máy tính với cơ chế phòng thủ mạnh. Chúng thường được dùng làm cổng ứng dụng, cổng mạch, hoặc các kiểu tường lửa khác.
* Một bastion host được cài đặt với một hệ điều hành tin cậy và không chứa những chương trình hoặc chức năng không cần thiết nhằm giảm đi những lỗi không đáng có và dễ dàng kiểm tra tính bảo mật.

Gateways hoạt động trên bastion hosts cần phải thoả những điều kiện:

* Phần mềm Gateway chỉ nên viết theo những module nhỏ để dễ dàng cho việc kiểm tra.
* Một bastion host cần chứng thực các user tại tầng mạng bằng cách xác nhận địa chỉ IP nguồn và đích chứa trong gói IP. Gateways chạy trên bastion host nên chứng thực user độc lập tại một tầng cao hơn.
* Một bastion host chỉ nên kết nối đến một số lượng nhỏ những host nội bộ.
* Bastion hosts nên giữ lại các file log, lưu trạng thái của mỗi phiên TCP để giúp admin xác định được các vấn đề phát sinh.
* Nếu nhiều gateways đang chạy trên một bastion host đơn, những gateways này cần phải được xử lý một cách độc lập. Nếu một gateway bị lỗi, admin có thể shutdown nó mà không ảnh hưởng đến các gateways khác.
* Bastion hosts nên hạn chế ghi dữ liệu lên đĩa cứng của chúng nhằm giảm cơ hội các mã độc hại xâm nhập vào hệ thống.
* Gateways chạy trên một bastion host không nên được dùng quyền admin hệ thống.

# 6. Cấu hình tường lửa

## Khái niệm chung

Gateways chạy trên một bastion host thường được sử dụng với bộ lọc gói tin.

Các cấu hình tường lửa thông dụng:

* Single-Homed Bastion Host System (SHBH)
* Dual-Homed Bastion Host System (DHBH)
* Screened Subnets (SS)
* Demilitarized Zones (DMZ)

## Single-Homed Bastion Host System

* Bao gồm một packet-filtering router và một bastion host, trong đó router kết nối mạng nội bộ với mạng ngoại vi và bastion host nằm trong mạng nội bộ.
* Router sẽ thông báo ra bên ngoài địa chỉ IP và số port của các server nội bộ.
* Router sẽ không chuyển tiếp các gói tin đi vào trực tiếp đến các server mà sẽ kiểm tra các gói tin này, sau đó mới chuyển cho bastion host.
* Bastion host tiếp tục kiểm tra gói tin đi vào, nếu thoả, sẽ xác định server nội bộ nào gói tin muốn được chuyển tới.
* Các gói tin từ mạng nội bộ đi ra bên ngoài cũng phải qua bastion host. Bộ lọc gói tin của tường lửa kiểm tra mỗi gói tin đi ra ngoài và ngăn lại nếu địa chỉ nguồn của nó không phải là địa chỉ IP của bastion host hoặc không thoả các quy tắc lọc.
* Trong một hệ thống SHBH, nếu attacker thoả hiệp được với packet-filtering router thì có thể sửa được các luật trong ACL để bỏ qua bastion host và truyền thông trực tiếp với các host nội bộ. Vấn đề này có thể giải quyết bằng cách sử dụng Dual-Home Bastion Host (DHBH).

## Dual-Homed Bastion Host System

* Một DHBH chia mạng nội bộ vào hai zones: inner zone (private zone) và outer zone.
* Địa chỉ IP của các host trong inner zone không thể vươn tới được từ các mạng ngoại vi.
* Địa chỉ IP của các host trong outer zone có thể vươn tới được trực tiếp từ các mạng ngoại vi.
* Router được đặt giữa mạng ngoại vi và outer zone, giữa mạng ngoại vi và bastion host.
* Inner zone trong DHBH chỉ được kết nối đến bastion host nên được bảo vệ bởi cả bastion host và packet-filtering router.
* Các server trong outer zone được bảo vệ bởi packet-filtering router.
* Tương tự như trong hệ thống SHBH, một DHBH cho phép các máy tính server trong outer zone có thể được truyền thông trực tiếp đến Internet mà không cần phải đi qua bastion host.
* ACL trong router cho phép các gói từ ngoài vào đi qua nó nếu địa chỉ nguồn được cho phép, và địa chỉ IP đích cùng số port thoả với địa chỉ IP của máy server cũng như một port đang mở của server này.
* Trong hệ thống DHBH, attacker nếu thoả hiệp với packet-filtering router cũng vẫn không thể vượt qua được bastion host.

## Screened Subnets

* Là cấu hình tường lửa bảo mật nhất.
* Bao gồm một bastion host và hai packet-filtering router (là một mạng SHBH với packet-filtering router thứ hai (inner router) chen vào giữa bastion host và mạng nội bộ.
* Nói cách khác, trong một Screened Subnet, một router đặt giữa Internet và bastion host, một router khác đặt giữa bastion host và mạng nội bộ.
* Hai tường lửa lọc gói sẽ tạo ra một screened subnetwork cô lập ở giữa. Các máy tính server và thiết bị nào không cần bảo mật mạnh thường được đặt trong screened subnetwork này.
* Router ngoài (outer router) sẽ thông báo cho mạng ngoại vi địa chỉ IP và số port của các máy tính server và thiết bị kết nối đến screened subnetwork.
* Router trong (inner router) sẽ thông báo cho mạng nội bộ địa chỉ IP và số port của các máy tính server và thiết bị kết nối đến screened subnetwork.
* Cấu trúc của mạng nội bộ là ẩn với thế giới bên ngoài.
* Có thể di chuyển một số server (database server…) từ screened subnetwork đến mạng nội bộ để cung cấp một sự bảo vệ mạnh hơn.
* Có thể đặt các proxy server tương ứng (chẳng hạn database server) trong screened subnetwork.
* Cấu hình này làm tăng tính bảo mật của hệ thống nhưng cũng làm giảm tốc độ xử lý nên trong mỗi ứng dụng cụ thể, cần tìm kiếm những cấu hình tối ưu phù hợp.

## Demilitarized Zones (DMZ)

* Một subnetwork giữa hai tường lửa trong mạng nội bộ thường được xem như một Demilitarize zone (DMZ).
* Tường lửa bên ngoài bảo vệ vùng DMZ với mạng ngoại vi và tường lửa bên trong bảo vệ mạng nội bộ với vùng DMZ.
* Một DMZ có thể có hoặc không có bastion host. Các server không yêu cầu bảo mật mạnh được đặt trong vùng DMZ.
* Các máy tính cần phải được bảo mật cao nhất được đặt trong subnet kết nối đến tường lửa bên trong.

## Network Security Topology

* Tường lửa có thể sử dụng để chia mạng thành ba vùng phân biệt:
* Vùng không tin cậy: là mạng ngoại vi bên ngoài của tường lửa ngoài.
* Vùng kém tin cậy: là vùng DMZ nằm giữa tường lửa ngoài và tường lửa trong.
* Vùng tin cậy: là mạng nội bộ nằm đằng sau tường lửa trong.

# 7. Chuyển dịch địa chỉ mạng

NAT (Network Address Translation Protocol) chia địa chỉ IP vào hai nhóm.

* Nhóm 1 bao gồm các địa chỉ IP công cộng, có thể vươn tới được từ mạng ngoại vi.
* Nhóm 2 bao gồm các địa chỉ IP riêng và không thể vươn tới được một cách trực tiếp từ mạng ngoại vi.

Xem lại NAT tĩnh, NAT động, PAT, VLAN trong môn Thiết bị mạng.

# 8. TMG – Threat Management Gateway

Forefront Threat Management Gateway 2010 là phiên bản của Microsoft thay thế cho ISA 2006.

## 1. Yêu cầu cài đặt

A blue and white table with text

Description automatically generated with medium confidence

## 2. Tính năng chính của TMG

A close-up of several icons

Description automatically generated

## 3. Các điểm mới của TMG so với ISA

A screenshot of a computer

Description automatically generated

## 4. Các mô hình mạng trong TMG

* Edge Firewall

A diagram of a network connection

Description automatically generated

* 3-Leg Perimeter

A diagram of a network

Description automatically generated

* Front Firewall

A diagram of a network

Description automatically generated

* Back Firewall

A diagram of a network

Description automatically generated

* Single Network Adaptor

A diagram of a network adapter

Description automatically generated

## 5. Cơ chế hoạt động

A table with text on it

Description automatically generated