**Câu 1 :Trong trường hợp nào dùng bridge và transparent mode**

**bridge-mode** để kết nối các thiết bị mạng khác vào một mạng lớn hơn. Trong chế độ bridge mode :

* Tất cả các gói tin sẽ được truyền qua các cổngcủa thiết bị mà không có bất kỳ định tuyến nào diễn ra.

(mạng LAN, đc kết nối trực tiếp)

* **Chế độ transparent mode** (chế độ trong suốt) **cho phép** các **thiết bị** **kết nối đến mạng** của bạn mà **không cần phải cấu hình** lại địa chỉ **IP** hoặc **thông số mạng khác.** 
  + Chế độ này **được sử dụng** k**hi bạn muốn tạo một kết nối mạng không định tuyến giữa các thiết bị mạng**, và **đặc biệt hữu ích** khi bạn **muốn kết nối các thiết bị mạng khác nhau** nhưng chúng **không tương thích với nhau về cấu hình mạng.**

**Thiết bị không tương thích với nhau** về cấu hình mạng là tình trạng khi các thiết bị trong mạng không thể giao tiếp với nhau vì các cấu hình mạng khác nhau, ví dụ như địa chỉ IP, subnet mask, gateway, DNS, v.v.

Tuy nhiên, chế độ transparent mode không phổ biến bằng chế độ bridge mode và được sử dụng trong một số

trường hợp đặc biệt.

**vd:** Khi một công ty muốn giữ nguyên các địa chỉ IP của các thiết bị trong mạng của họ và không muốn thay đổi khi kết nối với mạng của một nhà cung cấp dịch vụ khác.

Khi một doanh nghiệp muốn kết nối hai mạng khác nhau mà không thay đổi bất kỳ thông tin mạng nào của hai mạng đó.

Khi cần triển khai các giải pháp bảo mật để giám sát và kiểm soát các luồng dữ liệu trong mạng.

(

Có nhiều lý do mà một công ty có thể muốn giữ nguyên các địa chỉ IP của các thiết bị trong mạng của họ và không muốn thay đổi khi kết nối với mạng của một nhà cung cấp dịch vụ khác, như sau:

1. **Thuận tiện cho quản lý và triển khai**: Khi **giữ nguyên** các **địa chỉ IP**, công ty có thể **quản lý và triển khai hệ thống mạng của mình dễ dàng hơn**, bởi vì họ **không cần phải thay đổi cấu hình IP** cho các thiết bị khi kết nối với một nhà cung cấp dịch vụ khác.
2. **Giữ cho hệ thống liên lạc nội bộ không bị gián đoạn**: đảm bảo rằng các thiết bị trong hệ thống của họ có thể **liên lạc với nhau một cách liên tục** và **không bị gián đoạn khi kết nối với mạng của một nhà cung cấp dịch vụ khác**.
3. **Bảo vệ khỏi các cuộc tấn công**: Khi sử dụng các địa chỉ **IP tĩnh**, công ty có thể **thiết lập** các **chính sách bảo mật cụ thể** để **bảo vệ** hệ thống mạng của **mình khỏi các cuộc tấn công từ bên ngoài.**
4. **Dễ dàng quản lý bảo trì**: Khi giữ nguyên các địa chỉ IP của các thiết bị trong mạng của mình, công ty có thể **dễ dàng quản lý** và **bảo trì hệ thống mạng** của mình, bởi vì họ **không cần phải thực hiện các thay đổi cấu hình IP** khi kết nối với một nhà cung cấp dịch vụ khác.

)

**đặt gì giữa webserver + appserver và dbserver**

**Giữa webserver + appserver và dbserver**, thường sẽ **đặt một tường lửa (firewall)** để **bảo vệ** các **server** khỏi các **cuộc tấn công mạng bên ngoài**. Tường lửa sẽ **kiểm soát lưu lượng mạng** **vào và ra** của các **server** và cho phép các **lưu lượng truy cập được quy định trước**, từ **các địa chỉ IP được cho phép**, **cổng được sử dụng** và **giao thức được sử dụng**.

Ngoài ra, trong một số trường hợp, còn có thể đặt một **load balancer** **giữa** **webserver + appserver** và **dbserver** để **phân phối tải trọng mạn**g **và đảm bảo sự ổn địn**h và **khả năng mở rộng của hệ thống**.

**Load balancer** sẽ **phân phối** các **yêu cầu từ người dùng** **đến các server khác nhau** theo một số thuật toán nhất định, **nhằm giảm thiểu tải trọng** cho các **server** và **đảm bảo rằng hệ thống luôn hoạt động tốt**.

**non bridge sử dụng khi nào (1%) ?**

**Non-bridge** mode là chế độ mà **một thiết bị mạng** không phải là bridge **sẽ làm việc như một router thông thường**. Chế độ này thường được sử dụng trong các trường hợp sau đây:

1. **Khi** một **thiết bị mạng** đó **cần phải kết nối với Internet** **thông qua** một **router** hoặc **modem** khác và **không thể hoạt động như một bridge.**
2. **Khi** bạn **muốn sử dụng tính năng định tuyến** của **thiết bị mạng** đó **để kết nối các mạng khác nhau,** ví dụ như kết nối mạng LAN và WLAN.
3. **Khi** cấu hình **bridge mode** **không khả dụng** hoặc không thể làm được, ví dụ **như khi một thiết bị không hỗ trợ bridge mode**.

Tuy nhiên, **việc sử dụng non-bridge mode** **phụ thuộc** vào **từng trường hợp cụ thể** và **không phải lúc nào cũng cần thiết**.

**Việc sử dụng non-bridge mode** có thể dẫn đến một số **vấn đề về mạng**, chẳng hạn như **tăng độ trễ và** tốn **nhiều băng thông hơn**. Do đó, cần thận trọng khi sử dụng non-bridge mode và cân nhắc kỹ trước khi thực hiện.

**bridge mode là gì mà khi sử dụng non-bridge mode lại tăng độ trễ và tốn nhiều băng thông hơn**

**Bridge mode** là chế độ mà **một thiết bị mạng** như modem hoặc **router được cấu hình để hoạt động như một bridge**, **cho phép** các gói **dữ liệu truyền qu**a một **cách trực tiếp** từ mạng **nguồn đến** mạng **đích** mà **không được xử lý hay lọc qua thiết bị**.

Bridge mode **thường được sử dụng** khi bạn muốn **sử dụng một thiết bị mạng ngoài như là modem hoặc router,** nhưng **muốn sử dụng một thiết bị mạng khác để xử lý các tính năng mạng như là định tuyến hoặc chia sẻ Internet**.

Khi sử dụng **non-bridge mode**, **thiết bị mạng sẽ xử lý và lọc các gói dữ liệu trước khi chúng được truyền đi,** điều này có thể làm **tăng độ trễ** **và tốn nhiều băng thôn**g hơn.

Khi một thiết bị mạng hoạt động **ở chế độ non-bridge mode**, các **gói dữ liệ**u sẽ đi **qua các lớp phần mềm** của thiết **bị để được xử lý, lọc và định tuyến**, điều này có thể **tốn thời gian và tài nguyên của hệ thống**.

Ngoài ra, khi **sử dụng non-bridge mode**, **thiết bị mạng** **cũng** có thể **tạo ra các gói dữ liệu bổ sung,** chẳng hạn như **các gói đóng gói thêm thông tin địa chỉ mạng**, làm **tăng lượng dữ liệu cần truyền qua lại trên mạng và tiêu tốn thêm băng thông**.

**load balacing ở ngwf và waf khác gì nhau**

**NGFW (Next-Generation Firewall**) và WAF (Web Application Firewall) là **hai loại thiết bị bảo mật mạng**, và cả hai **đều có thể** được sử dụng để **triển khai load balancing trong môi trường mạng.**

Tuy nhiên, có sự khác biệt về cách thức triển khai load balancing giữa NGFW và WAF :

* **NGFW** thường **được triển khai** với m**ột hoặc nhiều thiết bị riêng biệt chuyên dụng** để thực hiện load balancing, trong khi đó **WAF** thường **được tích hợp** với một **giải pháp bảo mật web tập trung** (centralized web security solution) hoặc **ứng dụng cân bằng tải** (application load balancer) để thực hiện **load balancing**.

Một điểm khác biệt khác là **WAF** thường được sử dụng để **bảo vệ ứng dụng web khỏi các cuộc tấn công**, trong khi **NGFW** được sử dụng để **bảo vệ mạng toàn diện**.

Do đó, khi triển khai load balancing bằng **WAF**, các **máy chủ** ứng dụng **web sẽ được cân bằng tải** và **bảo vệ khỏi các cuộc tấn công web như tấn công DDoS** (Distributed Denial of Service) hoặc **SQL injection.**

Tóm lại, **NGFW** và **WAF** đều có thể được sử dụng để triển khai load balancing, tuy nhiên cách thức triển khai khác nhau tùy thuộc vào mục đích sử dụng và yêu cầu bảo mật của mạng và ứng dụng web