Câu hỏi an toàn và bảo mật thông tin

1. vị trí đặt tường lửa trong mạng?

Tường lửa luôn được lắp đặt ở vùng biên giới của hệ thống mạng hay hệ thống máy tính. Tường lửa cá nhân sau khi được cài đặt sẽ chiếm giữ việc quản lý các thông tin đi vào hay đi ra cổng giao tiếp mạng của máy tính. Tường lửa hệ thống sẽ được lắp đặt ngay sau thiết bị kết nối WAN, như Router sử dụng đường kênh thuê riêng (leased-line), hay Router ADSL.

2. Vị trí đặt firewall trước hay sau router vì sao?

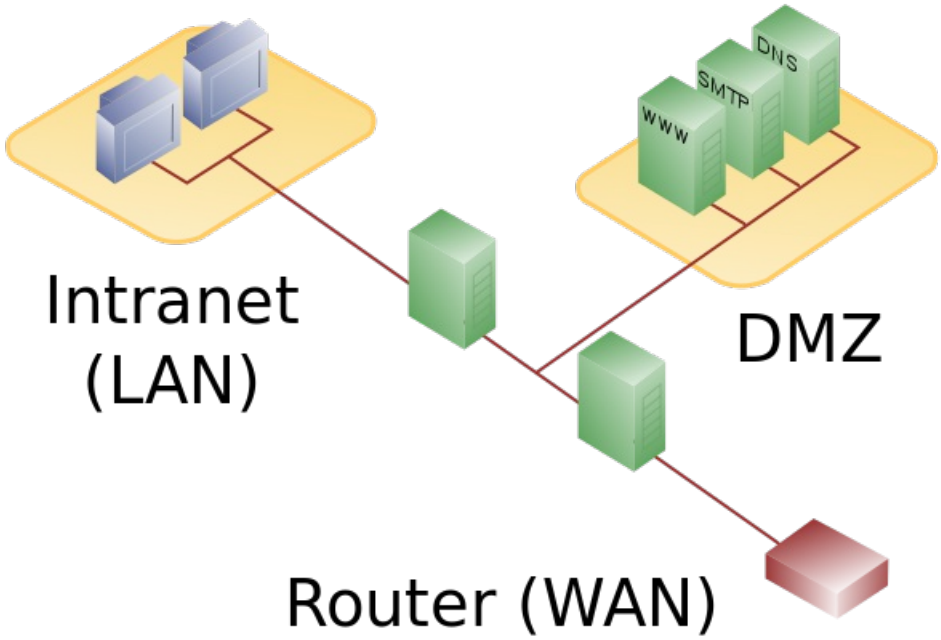
Firewall nên được đặt sau router vì: Router nhanh hơn firewall. Router là một thiết bị mạng đơn giản để chuyển các gói tin từ A đến B. Về mặt chi phí sử dụng router sẽ rẻ hơn so với dùng firewall để phân tích gói tin. d

3. Tại sao firewall cứng lại kém linh hoạt?

- Không thể thêm các chức năng
- Không thể thêm các quy tắc

4. Sử dụng một tường lửa so với 1 tường lửa?

- Khi sử dụng một trường lửa cho cả LAN và WAN. Do sự hạn chế về năng lực tính toán nên một cuộc tấn công từ chối dịch vụ trên tường lửa WAN có thể dẫn tới gián đoạn các dịch vụ trên LAN.
- Khi sử dụng hai tường lửa bạn bảo vệ dịch vụ trong nội bộ mạng LAN khỏi các tấn công từ chối dịch vụ từ perimeter firewall.
-



5. có thể tích hợp đồng thời nhiều mô hình kiến trúc trong firewall không vì sao?

6. Các kỹ thuật tấn công firewall?

- Quét cổng
- tấn công từ chối dịch vụ
- Quét mạng
- Quét lỗ hổng

7. Những tiêu chí được sử dụng khi lựa chọn một firewall cho hệ thống mạng cụ thể?

Mỗi loại firewall đều có điểm mạnh và điểm yếu riêng, giải pháp tốt nhất chính là sự kết hợp giữa các loại firewall này một cách hợp lý nhằm mục tiêu thoả mãn các điều kiện an toàn thông tin mà doanh nghiệp đưa ra. Hai điểm sau có thể là tiêu chí để chọn lựa firewall:

- Cấu hình cho firewall là sự áp dụng chính sách an toàn thông tin cho mạng máy tính của bạn. Nếu không có một chính sách an toàn thông tin, bạn sẽ khó lựa chọn firewall tốt cho mình. Bởi vì một biện pháp an toàn sẽ không thể áp dụng cho một nơi không biết phải bảo vệ cái gì, bảo khỏi điều gì và khỏi ai. Chính sách chính là chìa khoá để quản trị firewall, chính sách sẽ đưa ra các hướng dẫn về cái gì được phép làm và cái gì không được phép làm, tài sản nào cần bảo vệ và những ai được phép sử dụng tài sản đó, từ đó nhà quản trị sẽ đưa ra được các luật lọc cho firewall thoả mãn chính sách đã đưa ra.
- Triển khai firewall tuỳ thuộc vào yêu cầu an toàn của tổ chức hay doanh nghiệp và khả năng tài chính của doanh nghiệp đó. Mục tiêu chủ yếu là tạo ra được sự cân bằng giữa chi phí bỏ ra để triển khai firewall và lợi ích mà firewall sẽ đem lại. Mỗi sản phẩm firewall có nhiều tham số để xem xét, ngoài giá cả của nó, điều quan tâm tiếp theo chính là tính năng của nó. Tính năng của một firewall là tham số cho biết nó bảo vệ được hệ thống nào, khả năng ngăn chặn đến đâu, và cả hiệu năng hoạt động của nó, từ đó xem xét xem nó có khả năng thoả mãn yêu cầu an toàn đã đặt ra không. Ngoài ra, tham số quan trọng nữa khi lựa chọn firewall là sự đào tạo và hỗ trợ kỹ thuật của nhà sản xuất firewall. Bởi vì firewall được quản trị bởi chính nội bộ tổ chức hay doanh nghiệp, do đó hiểu biết sâu sắc và quản trị thành thạo sản phẩm firewall sẽ tránh được nhiều lỗi an toàn thông tin.

Cụ thể khi nào chọn loại firewall nào:

- Dễ dàng cài đặt : Software firewall
- Networking: Hardware firewall
- Bảo trì : hardware firewall (hardware firewall không yêu cầu bảo trì)
- Thân thiện với người dùng: Software firewall
- Chi phí: software firewall

8. Với các mạng riêng ảo VPN thì firewall có sử dụng được không?

Có

9. Đánh giá việc sử dụng proxy server với server DMZ?

10. Kết hợp giữa firewall cứng và firewall mềm ntn ?

11. firewall không chống được virus vì sao ?

Vì firewall chỉ kiểm tra phần header của gói tin mà không kiểm tra phần nội dung gói tin nên không thể chống lại virus nằm ở phần nội dung gói tin

12. firewall cứng khác firewall mềm ntn ?

- firewall cứng thường được tích hợp trong router và có các đặc điểm sau
  - Tốc độ
  - Bảo mật: Sử dụng một hệ điều hành riêng
  - Không có giao diện
- firewall mềm thường được cài trên các server riêng và có các đặc điểm sau:
  - Dễ sử dụng: Trong khi so sánh với tường lửa phần cứng, phần mềm tường lửa dễ dàng hơn để cấu hình và thiết lập.
  - Linh hoạt:Thông qua tường lửa mềm, chúng tôi có thể hạn chế một số ứng dụng cụ thể từ Internet. Điều này làm cho bức tường lửa phần mềm linh hoạt hơn
  - Điều khiển hoàn toàn:Tường lửa phần mềm cho phép người dùng kiểm soát hoàn toàn lưu lượng truy cập Internet của họ thông qua một giao diện người dùng thân thiện với người dùng yêu cầu ít hoặc không có kiến thức.

Bonus

- Hardware firewall đắt tiền hơn kém linh hoạt hơn software firewall tại sao vẫn sử dụng?
  - Do tốc độ
  - Ổn định
  - Bảo mật
- Firewall mềm liên quan đến hệ điều hành. Với hardware firewall có hệ điều hành riêng.