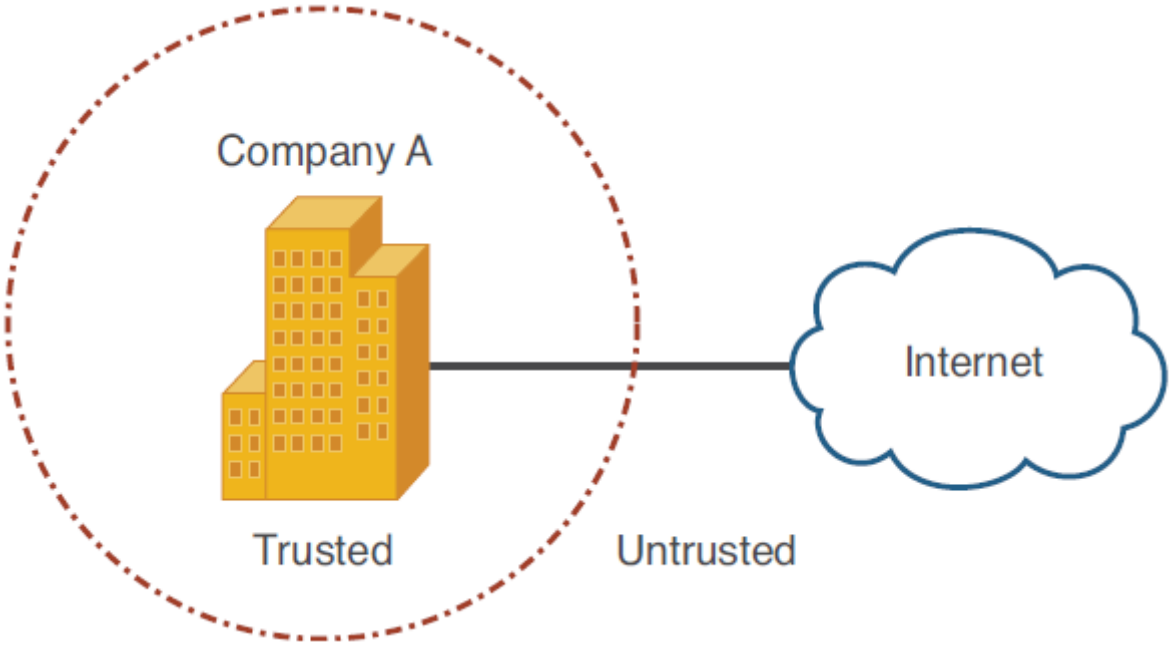
Contents

CHƯƠNG 2 NỘI DUNG THỰC TẬP

2.1 Tìm hiểu Firewall ASA (2 tuần đầu)

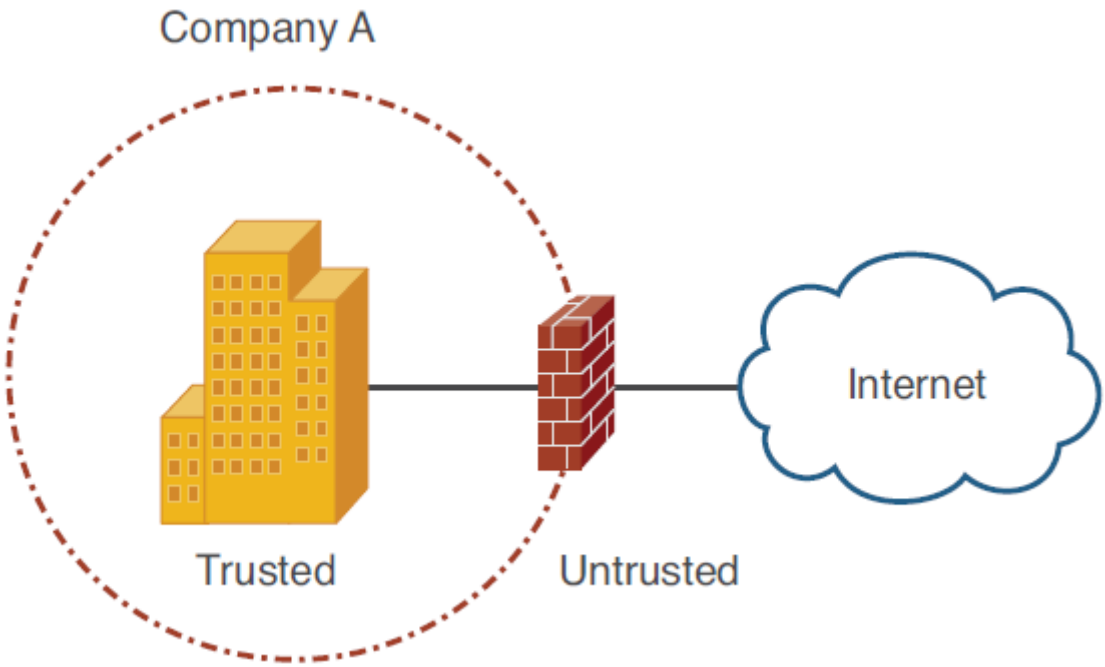
Để bảo mật các tài nguyên trên mạng, hệ thống mạng bằng cách nào đó phải được chia thành 2 vùng, vùng trusted và vùng untrusted. Vùng trusted còn được gọi là vùng security domain, tất cả những gì bên trong vùng security domain sẽ được bảo vệ khỏi những gì ở bên ngoài.

Một ví dụ đơn giản, một công ty A muốn bảo mật thông tin nội bộ khỏi môi trường Internet thì công ty A phải được đặt trong vùng security domain như hình minh họa.



Hình 2. 1 Một vùng security domain đơn lẻ.

Cách hiệu quả nhất để triển khai vùng security domain là đặt firewall ở biên giữa vùng trusted và vùng untrusted như hình minh họa.



Hình 2. 2 Triển khai vùng security domain với một firewall.

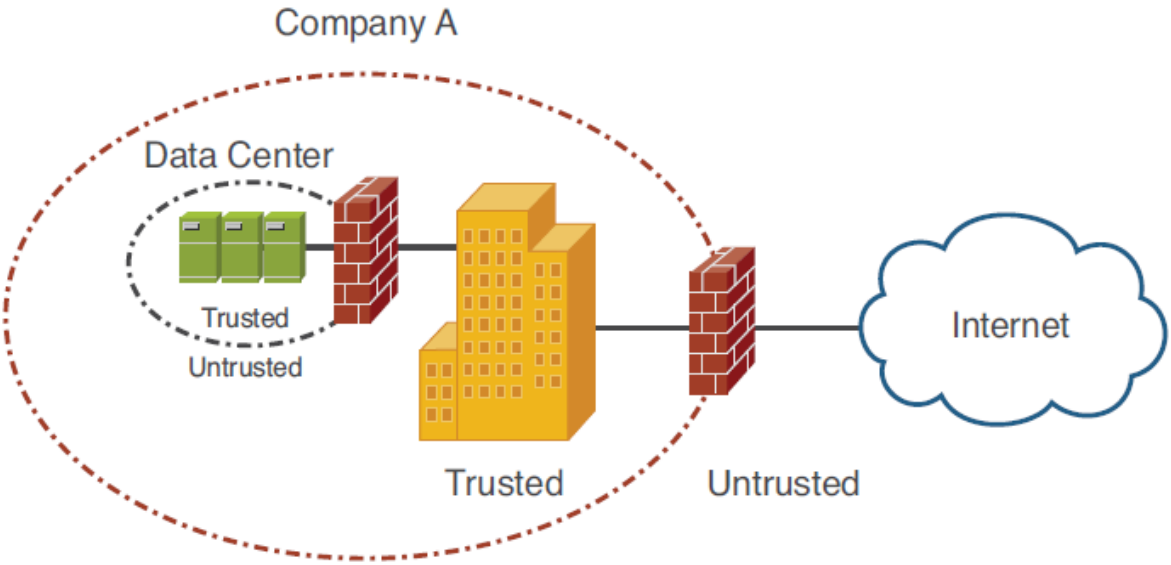
Firewall là thiết bị thực thi các chính sách điều khiển truy cập giữa 2 hay nhiều vùng security domain. Firewall có các cổng interface được kết nối vào mạng để các traffic khi đi qua vùng security domain phải đi qua firewall biên. Nói cách khác, firewall biên là con đường duy nhất để traffic đi qua vùng security domain.

Để bảo mật vùng security domain được an toàn, trước tiên phải đảm bảo 2 điều kiện sau:

Firewall phải là con đường duy nhất để traffic đi qua vùng security domain, không có bất kỳ con đường nào khác ngoài firewall thì mới có thể đảm bảo thực thi chính sách bảo mật đối với các traffic đi qua nó.

Firewall phải được gia cố để ngăn chặn tấn công, nếu không firewall sẽ bị điều khiển và làm thay đổi các chính sách bảo mật từ bên ngoài vùng untrusted.

Đôi khi, một vùng domain security với một firewall là không đủ. Giả sử, công ty muốn mở rộng triển khai data center. Công ty A tin tưởng các nhân viên thực hiện các chức năng công việc của họ, nhưng không muốn để ai khác truy cập vào tài nguyên quan trọng hay làm gián đoạn các dịch vụ trong data center. Cho nên, công ty A quyết định tạo thêm vùng security domain cho data center như hình minh họa.



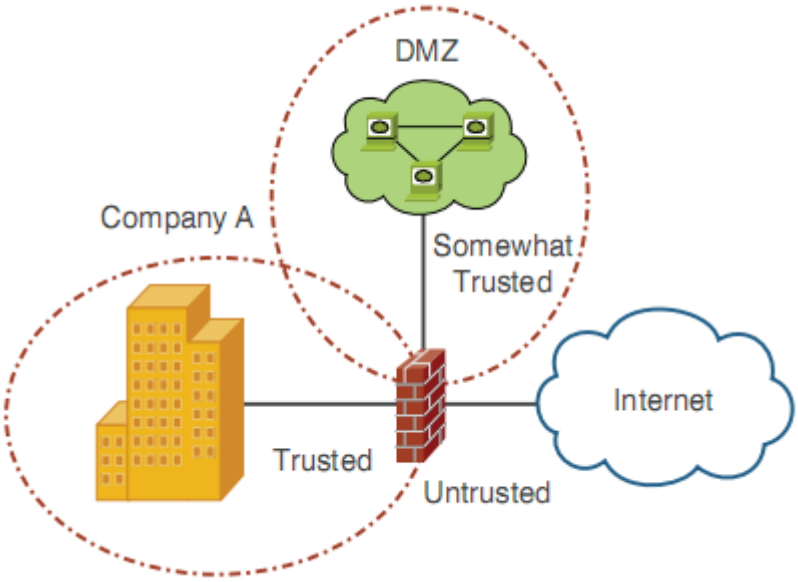
Hình 2. 3 Đa vùng security domain với nhiều firewall

Mỗi vùng security domain được triển khai với 1 firewall biên. Bên trong vùng security domain là các tài nguyên tin cậy, và bên ngoài là những gì không tin cậy. Tuy nhiên, khi xem xét firewall biên của vùng data center, các user bên ngoài vùng data center đều không được tin cậy, nhưng các user này vẫn được tin cậy đối với firewall biên của internet. Mỗi firewall đều có các chính sách bảo mật và khái niệm riêng của firewall biênvề vùng tin cậy.

Công ty A muốn cho phép các user trong công ty truy cập internet ra bên ngoài, trong khi đó công ty A cũng có web server cho phép các user bên ngoài internet truy cập vào bên trong nội bộ với mục đích công việc kinh doanh.

Nếu đặt web server ở một nơi nào đó bên trong vùng security domain, thì các user bên ngoài phải được cấp quyền để truy cập vào web server. Vì web server là tài nguyên tin cậy, nên khi bị tấn công, người dùng bên ngoài sẽ lợi dụng web server này để tấn công các tài nguyên tin cậy khác.

Một giải pháp tối ưu hơn là đặt web server vào giữa vùng trust và vùng untrusted, vùng này còn gọi là vùng DMZ,với giải pháp này, firewall đóng vai trò như biên giới giữa 3 vùng, vùng trust, vùng untrusted và vùng DMZ với 3 cổng interface như hình minh họa sau:

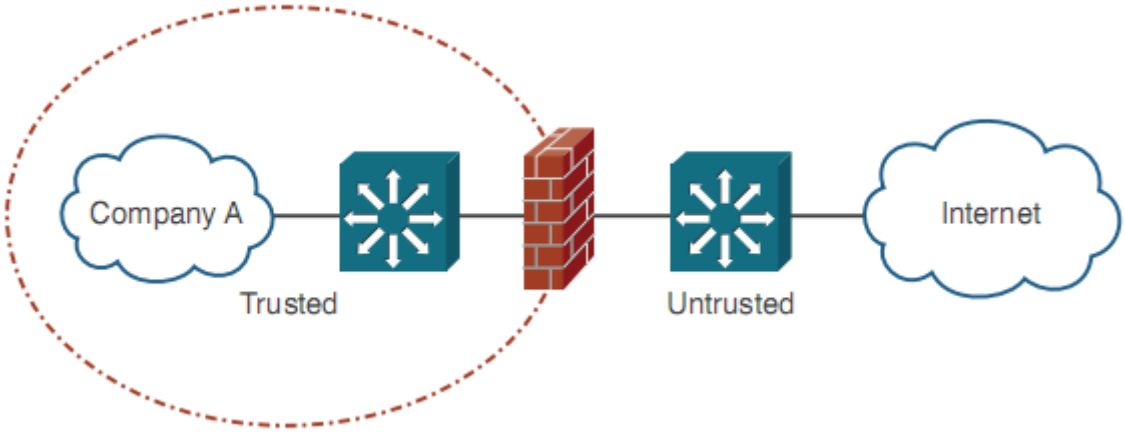


Hình 2. 4 Nhiều vùng security domain với 1 firewall

Có 2 cách chia vùng security domain: cách chia vật lý và cách chia logic.

Cách chia vật lý yêu cầu mỗi cổng interface trên firewall phải được kết nối đến mỗi một hạ tầng mạng riêng biệt, việc này đòi hỏi phải tốn kém thêm phần cứng và chi phí lắp đặt.

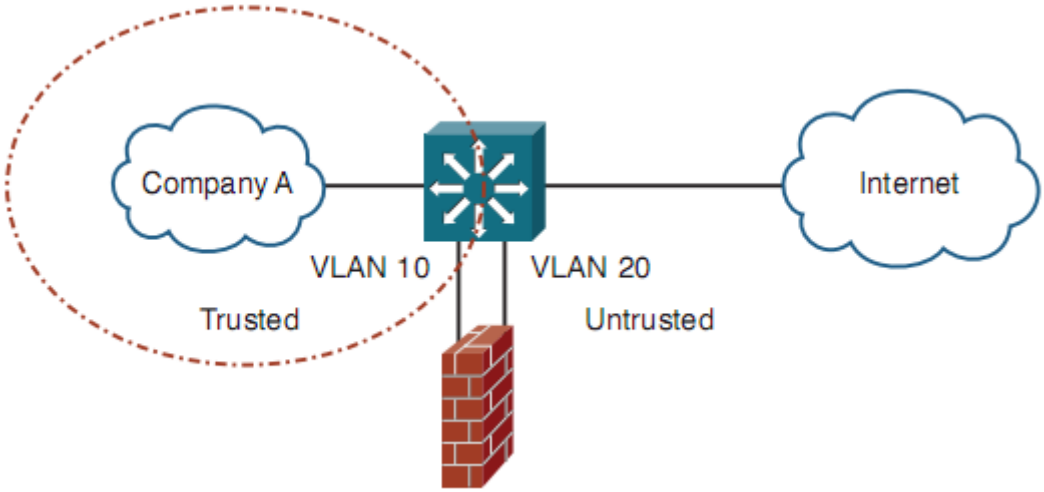
Hình minh họa cho thấy, mỗi cổng interface trên firewall được kết nối vào mỗi một switch khác nhau, cách chia vật lý này có tính bảo mật cao nhất vì traffic sẽ không qua được vùng security domain mà không có sự can thiệp của một số loại thiết bị mạng.



Hình 2. 5 Cách chia vật lý

Cách chia logic cho phép chia security domain trên cùng một hạ tầng mạng và được chia logic thành các VLANs khác nhau, cách chia này tiết kiệm chi phí hơn, nhưng bảo mật kém hơn vì lỗi cấu hình hay lỗi cổng logic.

Hình minh họa cho thấy, firewall chia security domain trên cùng một switch với hai VLANs khác nhau.



Hình 2. 6 Cách chia logic

2.2 Công nghệ của ASA

Về cơ bản, firewall cô lập các cổng interface với nhau để điều khiển các gói tin chuyển tiếp từ cổng này đến cổng khác.

Firewall có thể thực thi việc điều khiển truy cập dựa trên các tầng trong mô hình OSI.

Ví dụ, firewall thực hiện điều khiển truy cập ở tầng network có thể kiểm soát việc truy cập từ tầng 2 đến tầng 4, firewall sẽ thực hiện kiểm tra traffic có thể đi qua hay không, hay các host ở bên này có thể mở kết nối TCP/UDP truy cập tài nguyên ở bên kia hay không.

Trường hợp firewall thực hiện điều khiển truy cập ở tầng application sẽ thực thi chính sách bảo mật từ tầng 5 đến tầng 7, firewall sẽ kiểm soát người dùng ứng dụng mạng trong việc gửi dữ liệu từ nơi này sang nơi khác.Ví dụ, firewall ở tầng này có thể thực thi việc kiểm tra các phiên duyệt web có phù hợp với các chuẩn giao thức hay không, hay kiểm tra người dùng email gửi file có chứa virus hay không, nội dung email có được bảo mật hay không.

Phương thức điều khiển truy cập của firewall:

Permission Access Control còn được gọi là phương thức điều khiển truy cập phản ứng reactive approach, phương thức này có thể chặn các traffic sau khi các mối đe dọa tiềm tàng được xác định, nếu không tất cả các traffic đều được cho phép đi qua và thường được áp dụng trên IPS, và hệ thống antivirus theo thời gian thực.

Restrictive Access Control còn được gọi là phương thức điều khiển truy cập chủ động proactive approach. Mặc định, tất cả traffic sẽ bị chặn, nếu traffic nào muốn đi qua phải được xác định trước. Phương thức này thường được sử dụng bởi access-list, các quy luật trong access-list được xử lý theo trình tự và luôn kết thúc với quy luật cấm tất cả.

Firewall có thể sử dụng hai phương thức truy cập trên để lọc traffic với những công nghệ lọc gói tin sau đây:

2.2.1 Stateless packet filtering:

Một số firewall kiểm tra traffic chỉ dựa vào giá trị tìm được trong tiêu đề header của gói gói ở tầng 3 hay tầng 4. Việc quyết định chuyển tiếp hay chặn gói tin được thực hiện trên mỗi gói tin một cách độc lập. Vì vậy, firewall không có khái niệm của trạng thái kết nối mà chỉ biết mỗi gói tin có khớp với những chính sách bảo mật hay không.

Stateless packet filtering được thực hiện bằng các tập quy luật được cấu hình tĩnh.

Thậm chí kết nối có liên quan đến thương lượng động hay số port giao thức cũng không nhận thức được.

Các đặc tính của Stateless packet filtering:

Tính năng	Hạn chế
Các quy luật được cấu hình tĩnh, thường theo cách tiếp cận restrictive.	Các quy luật được cấu hình thủ công
Hoạt động hiệu quả ở tầng 3 với địa chỉ IP và tầng 4 với cổng port kết nối.	Không theo dõi các thương lượng động hay thay đổi số cổng port kết nối.
Hiệu quả và tiết kiệm chi phí	Dễ bị tấn công.

2.2.2 Stateful packet filtering:

SPF yêu cầu firewall theo dõi từng phiên hay từng kết nối khi gặp gói tin. Firewall phải duy trì bảng trạng thái cho mỗi kết nối hiện hành để chắc rằng hai host đang theo một hành vi mong đợi khi truyền thông. Tương tự, firewall phải kiểm soát các traffic ở tầng 4 để theo dõi các phiên kết nối mới được thương lượng. Việc theo dõi các phiên thương lượng đòi hỏi một số giao thức ở tầng 7 nhưng rất hạn chế.

Các đặc tính của stateful packet filtering:

Tính năng	Hạn chế
Lọc traffic ở tầng 3 và tầng 4, tiếp cận theo cách restrictive approach.	Không thấy được tầng 5 thông qua tầng 7.
Cấu hình đơn giản.	----
Hiệu suất cao.	Không kiểm tra giao thức.

2.2.3 Stateful packet filtering with application inspection and control:

Cơ chế theo dõi của firewall cho phép tập hợp các phiên kết nối TCP và UDP và quan sát các giao thức ở tầng 7. AIC còn gọi là theo dõi sâu các gói tin DPI, việc theo dõi có thể thực hiện dựa trên tiêu đề và nội dung gói tin ở tầng 7, cho phép quan sát hành vi người dùng rõ ràng hơn. Vì vậy, firewall cần nguồn và bộ nhớ nhiều hơn cho việc xử lý.

Các đặc tính của AIC:

Tính năng	Hạn chế
Lọc traffic ở tầng 3 thông qua tầng 7, tiếp cận theo cách restrictive approach..	Bộ nhớ đệm cho việc phân tích ứng dụng rất hạn chế.
Cấu hình đơn giản	----
Hiệu suất trung bình	Tốn nguồn điện nhiều hơn cho việc xử lý.

2.2.4 Network intrusion prevention system

NIPS kiểm tra, phân tích các traffic và so sanh nó với các hành vi nguy hiểm trong cơ sở dữ liệu. Cơ sở dữ liệu chứa một số lượng lớn các chữ ký hay các mẫu mô tả kiểu tấn công hay khai thác lỗ hỏng bảo mật đã biết. Khi phát hiện kiểu tấn công mới, chữ ký mới sẽ được them vào cơ sở dữ liệu.

Ở một số trường hợp, NIPS có thể phát hiện các hành vi nguy hiểm từ những gói tin đơn. Ở một số trường hợp khác, một nhóm các gói tin phải được tập hợp và kiểm tra. NIPS còn có khả năng phát hiện tấn công dựa trên việc đánh giá các gói tin và các phiên khác với những hành vi thông thường trên mạng như kiểu tấn công DOS, TCP flood.

NIPS tiếp cận theo phương pháp permissive approach, tức là tất cả các traffic đều được cho phép ngoại trừ phát hiện hành vi khả nghi, firewall sẽ tạo ra các quy luật động để chặn hay reset các kết nối hay gói tin có mã độc.

Các đặc tính của NIP:

Tính năng	Hạn chế
Một cơ sở dữ liệu chữ ký phong phú với các mẫu tấn công, bao gồm lớp 3 đến lớp 7.	Bộ nhớ đệm cho việc phân tích ứng dụng rất hạn chế.
Sử dụng phương pháp tiếp cận permissive approach	Thường không phát hiện được các kiểu tấn công mới chưa tồn tại trong cơ sở dữ liệu.
Hiệu suất trung bình	Phải tinh chỉnh thủ công các lỗi phát hiện tấn công do chủ quan hay khách quan.

2.2.5 Network behavior analysis

NBA kiểm tra traffic theo thời gian để xây dựng các mô hình thống kê các hành vi cơ sở, mô hình không đơn giản chỉ là băng thông hay dung lượng bình quân sử dụng mà còn xem xét các traffic volume, traffic rate, connection rate và một số loại giao thức thường dùng. NBA tự động xây dựng và chọn lọc các mô hình mặc dù có sự can thiệp của con người.

Khi các mô hình được xây dựng, NBA có khả năng bắt lỗi các hành vi được xem là bất thường, NBA còn được gọi là IPS dựa trên cơ sở mạng bất thường. NBA có thể phát hiện hành vi nguy hiểm chưa biết trước.

Tính năng	Hạn chế
Kiểm tra traffic hay dữ liệu để thành các mô hình hoạt động bình thường.	Cần sự can thiệp của con người
Có khả năng phát hiện tấn công chưa biết trước.	Tạo ra lỗi chủ quan nếu các traffic có dấu hiệu bất thường
Dùng phương pháp restrictive approach.	----

2.2.6 Application layer gateway

ALG là thiết bị có vai trò gateway giữa client và server. Client gửi request ở tầng 7 đến proxy, proxy giả dạng thành client và chuyển tiếp request đến server. Khi server trả lời request, proxy sẽ đánh giá nội dung và ra quyết định với request đó.

Vì proxy hoạt động ở tầng 7 và lọc traffic dựa vào địa chỉ IP và nội dung được trả về từ server.

Proxy có thể phân tích chi tiết kết nối giữa client và server. Traffic có thể được hợp lệ hóa theo chuẩn các giao thức từ tầng 3 đến tầng 7 và kết quả được chuẩn hóa khi cần.

Tính năng	Hạn chế
Phân tích và chuẩn hóa các giao thức	Không phải tất cả giao thức đều được hỗ trợ.
Phân tích sâu và chi tiết các nội dung.	Phân tích ở thời gian thực tốn thời gian dài.
Kiểm soát truy cập từ tầng 3 đến tầng 7	----

2.3 CÁC TÍNH NĂNG CỦA CISCO ASA

Stateful packet filtering engine: Cơ chế theo dõi trạng thái kết nối, thực hiện chuẩn hóa các giao thức TCP.

Application inspection and control: Phân tích các giao thức ở tầng 7 và theo dõi trạng thái kết nối và đảm bảo việc chuẩn hóa các giao thức.

User-based access control: ASA có thể chứng thực người dùng nội tuyến bởi Cut-through Proxy, và kiểm soát truy cập của người dùng nào đó được phép truy cập. khi người dùng được chứng thực, Cut-through Proxy sẽ đẩy nhanh việc kiểm tra traffic của người dung sau khi được chứng thực.

Session-auditing: Các ghi nhận sẽ được tạo ra dựa trên phiên truy cập của người dùng, cũng như các phiên kết nối ở tầng 7.

Security services modules: Nền tảng ASA hỗ trợ nhiều module tích hợp dịch vụ bảo mật gồm một số thiết bị phần cứng chuyên dùng để giảm tải công việc cho bộ vi xử lý.

Reputation-based Botnet traffic filtering: ASA giúp phát hiện và lọc trafiic có liên quan đến botnet. Cơ sở dữ liệu của botnet traffic filter được Cisco cập nhật liên tục.

Category-based URL filtering: ASA có thể lọc các URL và thực thi các chính sách bảo mật, và điều khiển truy cập các dịch vụ web khác nhau.

Crytographic unified communications proxy: ASA giữ vai trò là proxy. ASA có thể ngắt hay trì hoãn các phiên được bảo vệ mã hóa giữa client và server.

Denial-of-servce prevention: ngăn chặn các kiểu tấn công từ chối dịch vụ.

Traffic correlation: Các chức năng phát hiện mối đe dọa giúp kiểm tra và đối chiếu các traffic từ nhiều phiên và kết nối khác nhau để phát hiện và ngăn chặn sự bất thường từ các cuộc tấn công mạng và các hành vi trinh sát.

Remote access VPNs: Hỗ trợ kết nối VPN từ bên ngoài internet vào bên trong. Các kết nối SSL VPNs và IPSec VPNs đều phải sử dụng phần mềm hỗ trợ.

Site-to-site VPNs: hỗ trợ kết nối VNPs IPSec.có mã hóa cho doanh nghiệp được cấu hình ở firewall biên hay router biên để tạo kết nối Site-to-Site hay Lan-to-Lan VPN.

High availability failover clustering: Hai ASA cùng dòng có thể được cấu hình dung lỗi để đảm bảo tính luôn sẵn sàng.

Redundant interfaces: Nhằm gia tăng tính sẵn sáng, các redundant interface luôn ở trạng thái active.

EtherChannel: ASA có khả năng gom các interface thành một interface logic.

Traffic and policy virtualization: ASA có thể cấu hình thành các cá thể ảo hay còn gọi là security context, mỗi các thể ảo có vai trò như một firewall độc lập và có các logic interface riêng, các chính sách bảo mật riêng.

Rich IP routing functionality: Hỗ trợ định tuyến tĩnh và các giao thức định tuyến động như RIPv1, RIPv2, EIGRP, OSPF

Powerful network address translation: ASA theo dõi và chuyển tiếp gói tin, và có chức năng NAT giúp dịch địa chỉ nguồn sang địa chỉ đích.

Transaparent (bridged) operation: ASA có thể được cấu hình transparent firewall để trở thành cầu nối giữa các cổng interface. ở chế độ transparent mode, firewall có thể chen vào mạng đang tồn tài mà không cần phải đặt lại địa chỉ IP.

Integrated DHCP, DDNS, and PPPoE: ASA có thể cấu hình như một DHCP client nhận địa chỉ IP động hay DHCP server để cấp phát IP động, kết nối PPP qua mội trường Ethernet, và DNS client động giúp ghi nhận lại thông tin phân giải từ tên host thành địa chỉ IP.

IPv6 support: Hỗ trợ IPv6.

IP multicast support: ASA hỗ trợ các giao thức IGMP and PIM trong các traffic hỗ trợ multicast.

Management ocontrol and protocols: ASA hỗ trợ nhiều cách quản lý gồm cổng console, telnet, ssh, https, và snmp.

Simples software management: ASA hỗ trợ các hệ thống file cục bộ và truyền tải file từ xa trong việc nâng cấp phần mềm. việc nâng cấp hần mềm có thể được thực hiện một cách tự động hay thủ công.

Configuration flexibility and scalability: Các chính sách bảo mật và các quy luật có thể tái sử dụng. thông qua Modular Policy Framework, các tính năng bảo mật có thể được cấu hình và áp dụng một cách linh hoạt.

Cisco security management suite: ASA có thể quản lý với nhiều bộ công cụ giao diện đồ họa khác nhau giúp việc quản trị dễ dàng hơn.

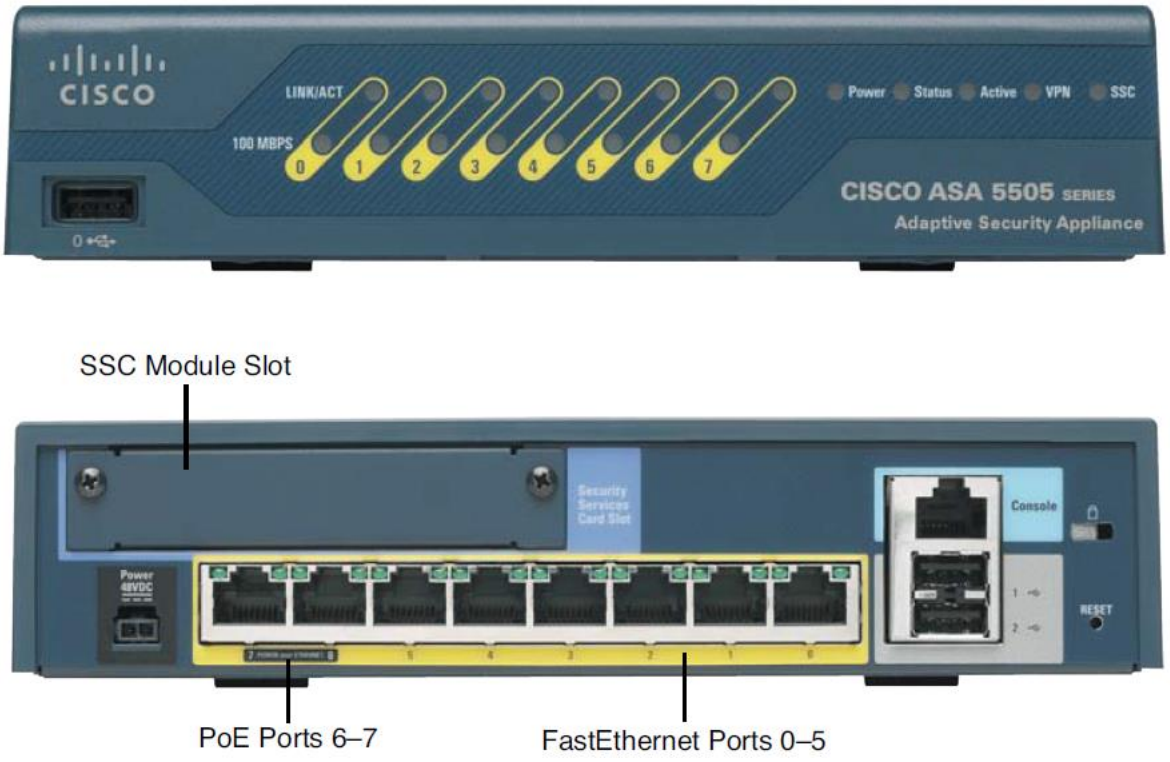
2.4 Các dòng ASA 5500

ASA 5505 là dòng sản phẩm thấp nhất về mặt cấu hình cũng như hiệu suất. Nó được thiết kế dành cho văn phòng nhỏ. Trong doanh nghiệp vừa, nó thường hỗ trợ người dùng truy cập từ xa.

Có 8 cổng FastEthernet dùng để nối vào switch, và 2 cổng PoE, ASA không được cấp nguồn qua PoE. Mặc định, 8 cổng được kết nối với switch cùng 1 VLANs để cho phép các thiết bị có thể giao tiếp trực tiếp với nhau ở tầng 2.

Các cổng có thể được chia thành nhiều VLANs nhằm phân chia văn phòng nhỏ thành các khu vực hay các chức năng khác nhau. ASA kết với với mỗi VLANs thông qua cổng logic riêng biệt. Tất cả các traffic qua VLANs phải đi qua firewall với chính sách bảo mật của nó.

ASA 5505 một khe cắm SSC cho phép cắm AIP-SSC-5 IPS module để có thêm tính năng IPS.



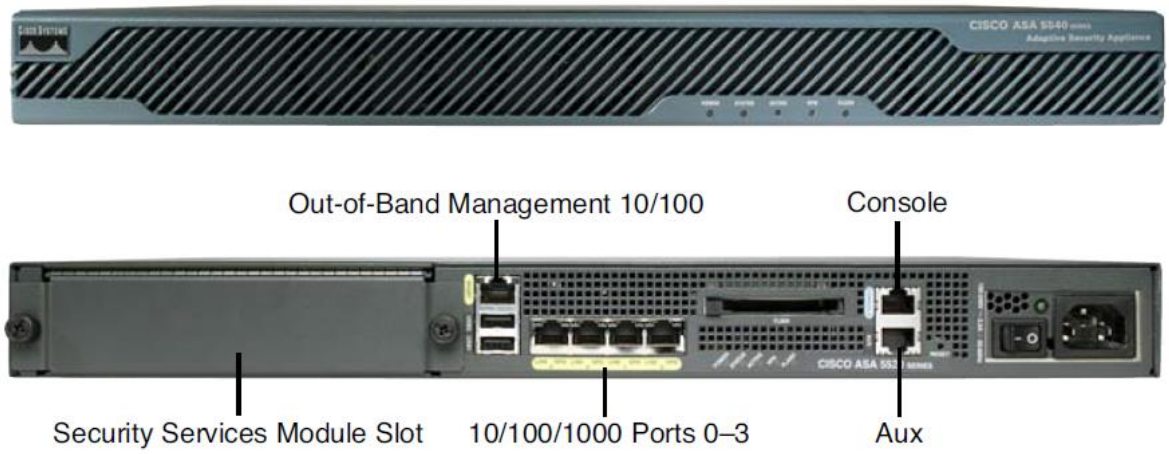
Hình 2. 7 Mặt trước và mặt sau của ASA dòng 5505

ASA 5510, 5520, và 5540 có khung và cổng kết nối giống nhau nhưng có hiệu suất khác nhau.

ASA 5510 dành cho doanh nghiệp vừa và nhỏ, hỗ trợ làm việc từ xa cho doanh nghiệp vừa.

ASA 5520 dành cho doanh nghiệp vừa, ASA 5540 dành cho doanh nghiệp vừa và lớn và các nhà cung cấp dịch vụ mạng.

ASA 5520 và 5540 có 4 cổng FastEthernet 10/100/1000 dùng để kết nối với hạ tầng mạng. Mặc định ASA 5510 có tốc độ 10/100. Nếu mua giấy phép security plus license, sẽ có 2 cổng được kích hoạt thành cổng GigabitEthernet 10/100/1000 và 2 cổng còn lại vẫn là FastEthernet. Cổng management cũng được kích hoạt để sử dụng.



Hình 2. 8 Mặt trước và mặt sau ASA dòng 5510, 5520, và 5540.

ASA 5510, 5520, 5540 có 1 khe SSM có thể cắm 1 trong 3 thiết bị sau:

Four-port Gigabit Ethernet SSM: module này cho phép thêm4 cổng interface có tốc độ 10/100/1000 với chuẩn RJ45 hay cổng SFP.

Advanced Inspection and Prevention (AIP) SSM: module này cho phép thêm tính năng IPS.

Content Security and Control (CSC) SSM: Module này thêm tính năng kiểm soát nội dung và dịch vụ antivus.

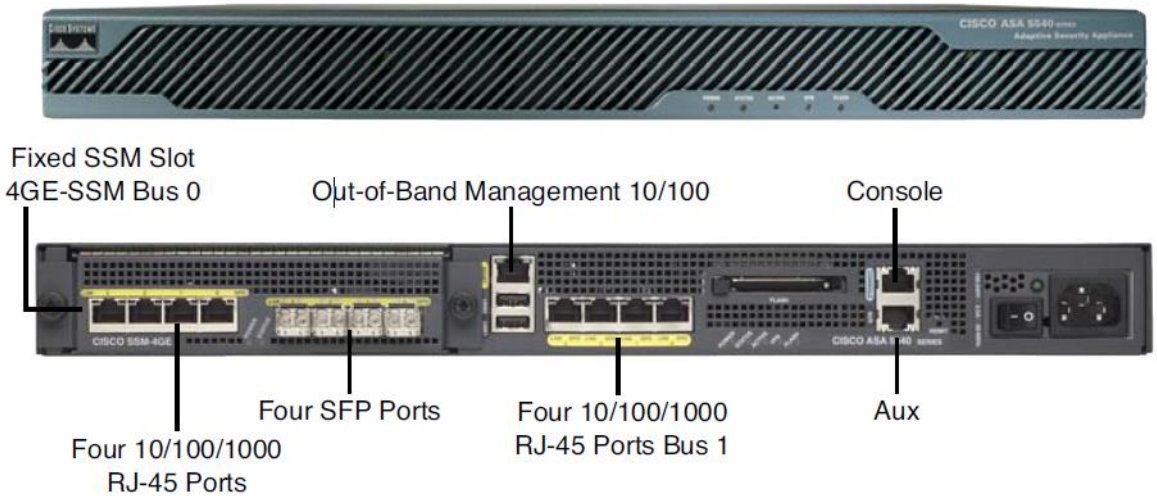
ASA 5510, 5520, 5540 có 1 cổng AUX có thể được dủng như cổng out-of-band management thông qua kết nối serial hay modem. Ngoài ra, có 1 cổng FastEthernet dủng để quản lý nhưng có thể cấu hình.

ASA 5550 dành cho doanh nghiệp lớn và nhà cung cấp dịch vụ mạng. ASA 5550 nhìn giống ASA 5510, 5520, và 5540. Sự khác biệt của ASA 5550 là có thêm module (4GE-SSM) không tháo rời được.

ASA 5550 có các interface vật lý được chia thành 2 nhóm, mỗi nhóm tương ứng với slot 0 và slot 1, mỗi slot tương tứng với bus 0 và bus 1. Slot 0 gồm (4GE-SSM)

Slot 1 gồm (4GE-SSM) và 4 cổng gigabit ethernet SFP mặc dù chỉ có 4 trong 8 cổng có thể dùng được ở bất cứ thời điểm nào.

ASA 5550 có hiêu suất cao, ASA có thể chuyển tiếp traffic hiệu quả hơn từ bus này sang bus khác bằng cách cho traffic đi từ cổng bus 0 đến bus 1.



Hình 2. 9 Mặt trước và mặt sau ASA dòng 5550

ASA 5580 là dòng có hiệu suất cao dành cho doanh nghiệp lớn, data center và các nhà cung cấp dịch vụ quy mô lớn. Nó hỗ trợ đến 24 cổng Gigabit Ehternet, đây là một trong hai dòng có khung lớn hơn các rack tiêu chuẩn.

ASA 5580 có 2 dòng: ASA 5580-20 (thông lượng 5 Gbps) và 5580-40 (thông lượng 10 Gbps) đều được tích hợp 2 cổng interface Gigabit Ethernet có tốc độ 10/100/1000 thường dủng cho việc quản lý, và có 2 bộ nguồn để dự phòng.

ASA 5580 có tổng cộng 9 khe cắm PCI Express. Khe cắm số 1 để dành cắm cryptographic accelerator module hổ trợ kết nối VPNs với hiệu suất cao. Khe cắm số 2 và số 9 để dành, còn lại 6 khe cắm dành cho các card mạng sau:

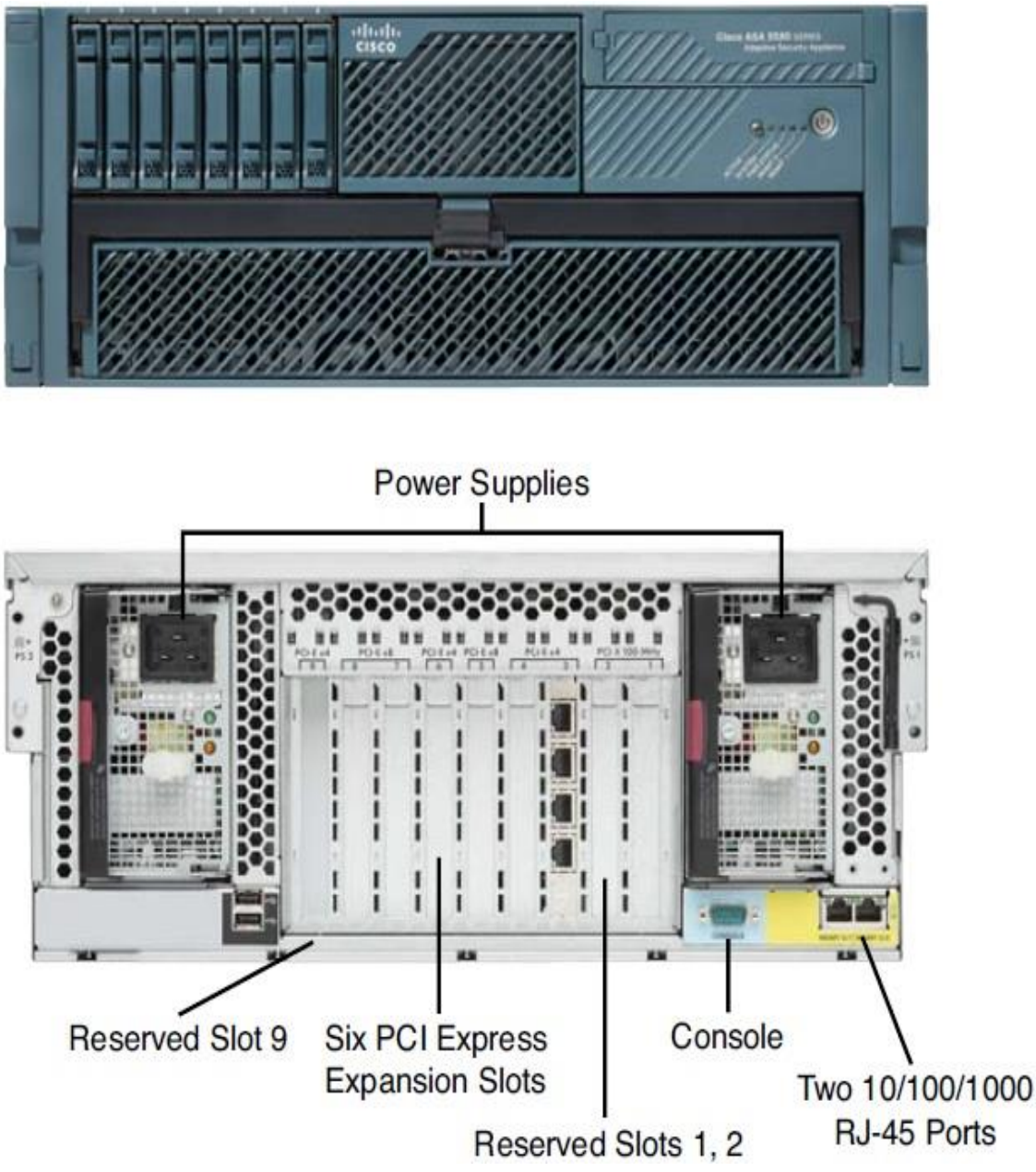
4 cổng gigabit ethernet 10/100/1000 BASE-T dùng cho cáp đồng.

4 cổng gigabit ethernet 1000 BASE-SX dùng cho cáp quang.

2 cổng gigabit ethernet quang 10G BASE-SR

ASA 5580 có 2 I/O bridge cung cấp kết nối cho các khe cắm mở rộng,, khác với ASA 5550, chỉ có 1 I/O bridge. Các cổng của ASA 5580 của khe cắm số 7 và 8 được điều khiển bởi I/O bridge 1 và các cổng ở khe cắm số 3,4,5 và 6 được điều khiển bởi I/O bridge 2.

Các cổng ethernet có tốc độ 10 Gigabit nên được cắm vào khe cắm số 5,7,hoặc 8 vì các khe cắm này hỗ trợ chuẩn cắm PCIe-x8.



Hình 2. 10 Mặt trước và mặt sau dòng ASA 5580.

ASA 5585-X là dòng cao cấp nhật được thiết kế cho các doanh nghiệp lớn và data center. ASA có khung gồm 2 khe cắm rack và 2 nguồn cung dự phòng, mỗi khe cắm hỗ trợ SSP.

ASA 5585-X gồm có 4 dòng, tùy thuộc vào SSP được cài đặt với tính năng VPN-SSP: SSP-10 (thông lượng 3Gbps), the SSP-20 (thông lượng 7Gbps) SSP-40 (thông lượng 12Gbps) và SSP-60 (thông lượng 20 Gbps). Tùy vào mỗi dòng, tính năng VPN SSP có thể cung cấp 10 Gbps kết nối Ethermet trong đó có 6 cổng 10/100/1000 và 2 cổng dùng để quản lý management 10/100/1000.

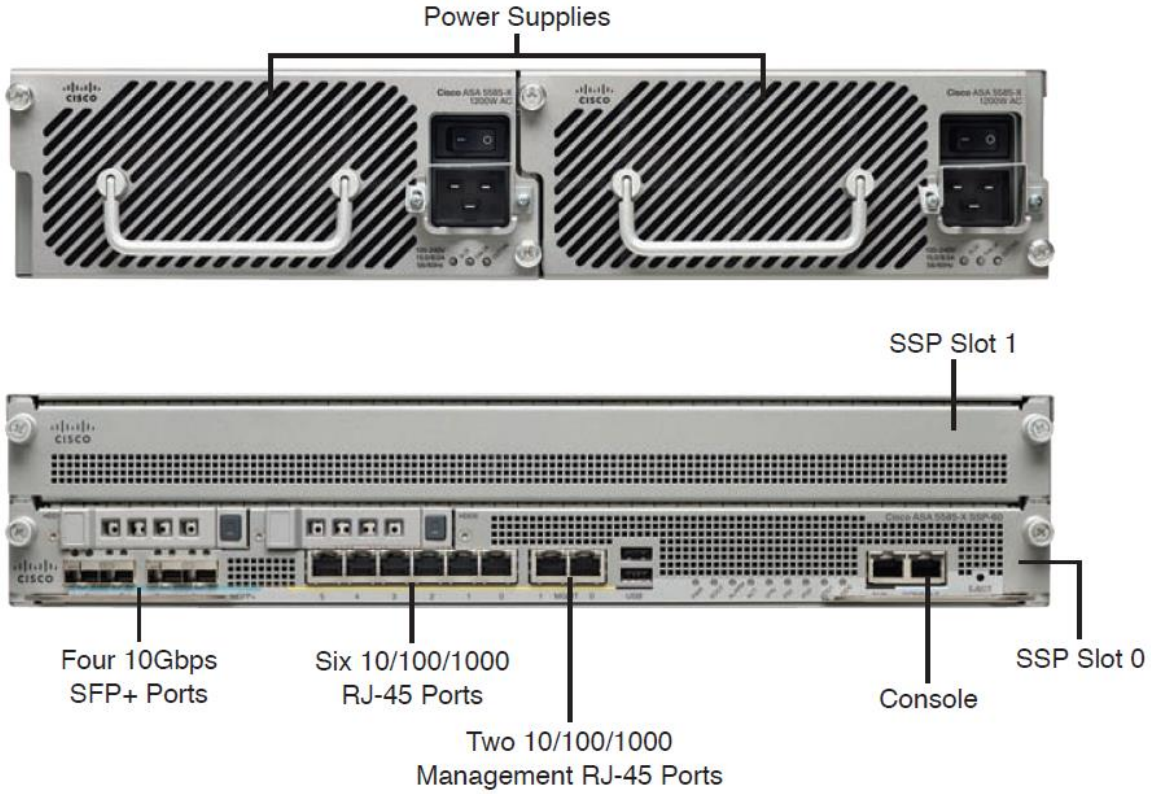
ASA 5585-X còn cung cấp tính năng IPS hiệu suất cao với 4 dòng thông qua khe cắm số 1 với thiết bị mở rộng IPS SSP.

IPS SSP-10 (thông lượng 2 Gbps)

IPS SSP-20 (thông lượng 3 Gbps)

IPS SSP-30 (thông lượng 5 Gbps)

IPS SSP-60 (thông lượng 10 Gbps)



Hình 2. 11 Mặt trước và mặt sau ASA dòng 5585-X

Hình minh họa cho thấy VPN SSP được cắm ở khe cắm số 0 và IPS SSP ở khe cắm số 1. 2 thiết bị nhìn bề ngoài giống nhau nhưng có tính năng khác nhau. Khi IPS SSP được thêm vào, 4 cổng kết nối Ethernet có tốc độ 10 Gbps và 6 cổng với tốc độ 10/100/1000 được điều khiển bởi VPN SSP.

ASA 5585-X yêu cầu Cisco ASA phiên bản 8.2(3) trở lên. Tuy nhiên, nếu cài IPS SSP, ASA phải được nâng cấp lên phiên bản 8.4(2) hay cao hơn và Cisco IPS 7.1(1)E trở lên.

Hình 2. 12 ASA 5585-X được tích hợp module IPS-SSP và VPN-SSP.

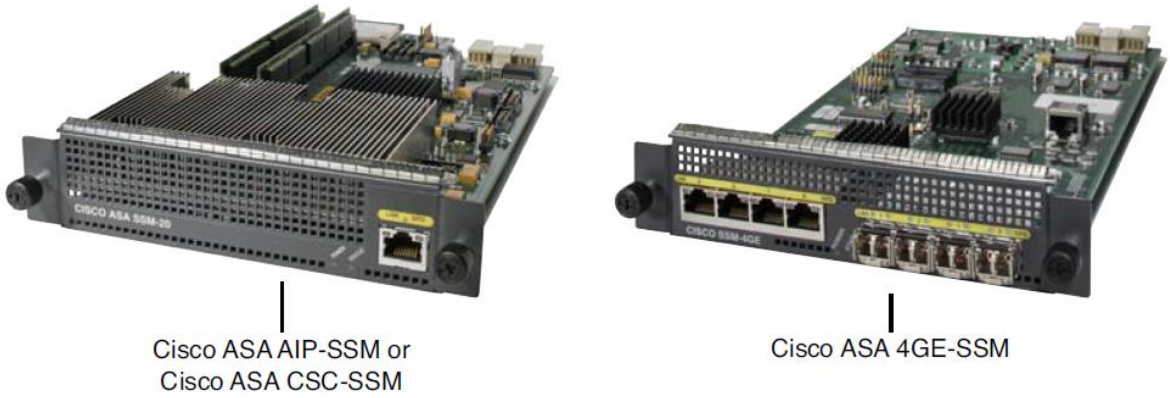
2.5 Các module bảo mật

2.5.1 Security services modules

Các dòng ASA đều hỗ trợ một module SSM. SSM cho phép cắm thêm có phần cứng chuyên dùng giúp giảm tải công việc cho bộ vi xử lý.

Cisco cung cấp module AIP-SSM, CSC-SSM, và 4GE-SSM.

Module AIP-SSM và CSC-SSM có bề ngoài giống nhau nhưng được cài chương trình khác nhau.



Hình 2. 13 Module AIP-SSM, CSC-SSM và 4GE-SSM.

2.5.2 AIP-SSM

AIP-SSM được cài CISCO IPS và thực hiện chức năng phát hiện ngăn chặn xâm nhập. AIP-SSM có thể cấu hình ở inline mode cho phép traffic được chuyển hướng đến module xử lý trước khi gói tin được chuyển đi, AIP-SSM còn được cấu hình ở promiscuous mode cho phép traffic được sao lưu đến module khi chuyển tiếp gói tin.

Để IPS hoạt động hiều quả, AIP-SSM phải kịp thời được cập nhật chữ ký trong cơ sở dữ liệu, và phải đăng ký dịch vụ IPS mới có thể cập nhật chữ ký qua SIO với hơn 25000 chữ ký trong cơ sở dữ liệu, khi mối đe dọa mới được phát hiện, chữ ký mới sẽ được thêm vào và được tải về cho AIP-SSM.

2.5.3 CSC-SSM

CSC-SSM thực hiện tính năng antivirus, chống spyware, chống phishing, ngăn chặn file, lọc và ngăn chặn URL, lọc nội dung với hợp với ASA. ASA chuyển hướng traffic qua CSC-SSM với chương trình Trend Micro Interscan trên hệ điều hành Cisco CSC-SSM. Vì được tích hợp nhiều tính năng ngăn chặn phần mềm độc hại nên còn được gọi là Anti-X module, các traffic có giao thức HTTP, FTP, SMTP, và POP3 được bảo vệ bởi CSC-SSM.

CSC-SSM phải được cập nhật nội dung thông tin bảo mật mới nhất từ Trend Micro để hoạt động hiệu quả. Việc cập nhật là tự động và yêu cầu phải đăng ký giấy phép sử dụng dịch vụ từ Cisco.

CSC-SSM có 2 dòng, dòng CSC-SSM-10 mặc định hỗ trợ đến 50 người dùng, nhưng có thể mở rộng đến 500 người dùng qua việc mua giấy phép bổ sung. Dòng CSC-SSM hỗ trợ 500 người dùng và có thể mở rộng đến 1000 người dùng với giấy phép bổ sung.

Cà 2 dòng với giấy phép chuẩn có bao gồm tính năng antivirus, antispyware, và chân file. Nếu mua giấy phép bổ sung, CSC-SSM có thêm tính năng antispam, antiphishing, lọc hay ngăn chặn URL và kiểm tra nội dung.

2.5.4 4GE-SSM

4GE-SSM cho phép gia gia 4 cổng gigabit Ethernet trên dòng ASA 5510, 5520, hay 5540, mặc dù được tích hợp sẵn 4 cổng RJ-45 có tốc độ 10/100/1000 và 4 cổng SFP quang nhưng chỉ có 4 cổng được sử dụng ở mọi thời điểm.

2.6 Các tính năng và hiệu suất của các dòng ASA

	5505	5510	5520	5540	5550	5580-20	5580-40
Typical application	Small office, home office, teleworker	Small to medium businesses, remote offices	Medium sized enterprise	Medium to large enterprises	Large enterprise, service provider	Large enterprise, data center, service provider	Large enterprise, data center, service provider
Firewall throughput	150 Mbps	300 Mbps	450 Mbps	500–650 Mbps	1–1.2 Gbps	5–10 Gbps	10–20 Gbps
Connections per second	4000	9000	12,000	25,000	36,000	90,000	150,000
Packets per second (64-byte)	85,000	190,000	320,000	500,000	600,000	2.5 M	4 M
Maximum connections	10,000/25,000[1]	50,000/130,000[1]	280,000	400,000	650,000	1 M	2 M

[1] ASA 5505, 5510: Base license/Security Plus license

Hình 2. 14 Hiệu suất của các dòng ASA tầm trung

	5585-X SSP-10	5585-X SSP-20	5585-X SSP-40	5585-X SSP-60
Typical application	Mission-critical data centers	Mission-critical data centers	Mission-critical data centers	Mission-critical data centers
Firewall throughput	3 Gbps	7 Gbps	12 Gbps	20 Gbps
Connections per second	65,000	140,000	240,000	350,000
Packets per second (64 byte)	1.5 M	3.2 M	6 M	10.5 M
Maximum connections	1 M	2 M	4 M	10 M

Hình 2. 15 Hiệu suất các dòng ASA cao cấp

	5505	5510	5520	5540	5550	5580-20	5580-40
Default interfaces	8 FE switch (2 PoE)	5 FE or 2 GE + 3 FE	4 GE + 1 FE	4 GE + 1 FE	8 GE	2 GE	2 GE
Maximum interfaces	8 FE switch (2 PoE)	4 GE + 5 FE or 6 GE + 3 FE	8 GE + 1 FE	8 GE + 1 FE	8 GE + 1 FE	24 GE or 12 10 GE	24 GE or 12 10 GE
VLANs	3/20[1]	50/100[1]	150	200	250	250	250

[1] ASA 5505, 5510: Base license/Security Plus license

Hình 2. 16 Các cổng interface được hỗ trợ tối đa cho các dòng tầm trung

	5585-X SSP-10	5585-X SSP-20	5585-X SSP-40	5585-X SSP-60
Default interfaces	8 GE + 2 10 GE	8 GE + 2 10 GE	6 GE + 4 10 GE	6 GE + 4 10 GE
Maximum interfaces	16 GE + 4 10 GE	16 GE + 4 10 GE	12 GE + 8 10 GE	12 GE + 8 10 GE
VLANs	1024	1024	1024	1024

Hình 2. 17 Các cổng interface được hỗ trợ tối đa cho các dòng cao cấp

	5505[1]	5510[1]	5520	5540	5550	5580-20	5580-40
Virtual firewalls (security contexts)[2]	0/0	0/5	20	50	50	50	50
High availability[3]	—/State-less A/S	—/A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S

[1] ASA 5505, 5510: Base license/Security Plus license.

[2] All models include two security contexts by default, except the ASA 5505 and ASA 5510 Base, which include none.

[3] A/S = Active/Standby, A/A = Active/Active.

Hình 2. 18 Tính năng virtual firewall và high availability của dòng ASA tầm trung.

	5585-X SSP-10	5585-X SSP-20	5585-X SSP-40	5585-X SSP-60
Virtual firewalls (security contexts)[1]	100	250	250	250
High availability[2]	A/A and A/S	A/A and A/S	A/A and A/S	A/A and A/S

[1] All models include two security contexts by default, except the ASA 5505 and ASA 5510 Base, which include none.

[2] A/S = Active/Standby, A/A = Active/Active.

Hình 2. 19 Tính năng virtual firewall và high availability trên các dòng ASA cao cấp.

	5505	5510	5520	5540	5550	5580-20	5580-40
Max VPN throughput	100 Mbps	170 Mbps	225 Mbps	325 Mbps	425 Mbps	1 Gbps	1 Gbps
Max IPsec VPN sessions	10/25[1]	250	750	5000	5000	10,000	10,000
Max SSL VPN sessions	25	250	750	5000	5000	10,000	10,000

[1] ASA 5505: Base license/Security Plus license.

Hình 2. 20 Khả năng kết nối VPN của dòng ASA tầm trung.

	5585-X SSP-10	5585-X SSP-20	5585-X SSP-40	5585-X SSP-60
Max VPN throughput	1 Gbps	2 Gbps	3 Gbps	5 Gbps
Max IPsec VPN sessions	5000	10,000	10,000	10,000
Max SSL VPN sessions	5000	10,000	10,000	10,000

Hình 2. 21 Khả năng kết nối VPN của dòng ASA cao cấp.

2.7 CÁC LOẠI GIẤY PHÉP

Giấy phép cho phép kích hoạt để dụng các chức năng cao cấp của firewall ASA tùy vào các loại giấy phép.

Base license: cho phép sử dụng các chức năng cơ bản.

Platform-specific license: dòng ASA 5505 và 5510 có thể nâng cấp lên security plus license từ base license để mở khóa thêm một số tính năng bảo mật khác.

Feature licence:các chức năng được kích hoạt một cách riêng biệt.

Feature License	Description
Botnet Traffic Filter	Enables Botnet Traffic Filtering
Strong Encryption	Enables 3DES and AES encryption algorithms for VPN sessions (free license)
GTP/GPRS Inspection	Enables GPRS Tunneling Protocol inspection (ASA 5520 and higher)
Cisco IME	Enables the Intercompany Media Engine functionality
AnyConnect Essentials	Enables the maximum number of AnyConnect SSL VPN clients only
AnyConnect Premium	Enables the maximum number of AnyConnect SSL VPN clients, clientless SSL VPN, and Cisco Secure Desktop features
AnyConnect for Mobile	Enables AnyConnect client access for Windows Mobile touch screen devices (also requires AnyConnect Essentials or Premium license)
Advanced Endpoint Assessment	Enables enhanced host scanning with Cisco Secure Desktop and AnyConnect SSL VPN clients
VPN Shared Licensing	Enables a license with a large number of SSL VPN sessions to be shared among several ASAs
FIPS Validation License	Enables Cisco AnyConnect SSL VPN client version 2.4 users for federal agencies requiring Federal Information Processing Standard (FIPS) 140-2 compliance

Hình 2. 22 Các tính năng có thể kích hoạt khi mua giấy phép feature license.

Virtualization license: mặc định, tất cả dòng ASA chỉ có hai firewall ảo (virtual firewall) hay hai ngữ cảnh bảo mật, giấy phép này cho phép gia tăng bối cảnh bảo mật security context ban đầu là 5,10,20,50 hay 100 hay nâng cấp từ 5 lên 10, từ 10 lên 20, từ 20 lên 50, hay từ 100 lên 250 ngữ cảnh context.

Per-user cryptographic UC proxy license: mặc định ASA cho phép tối đa hai người dùng với chúc năng UC proxy, giấy phép cho phép gia tăng người dùng lên 24, 50, 100, 250, 500, 750,1000,2000,5000 hay 10000 người dùng tùy vào các dòng ASA.

Per-user premium SSL VPN license: giấy phép cho phép gia tăng người dùng từ 2 người lên 10, 25, 50, 100, 250, 500, 750, 1000, 2500, 5000, hay 10000 người dùng tùy vào mỗi dòng ASA.

2.8 Yêu cầu bộ nhớ của các dòng ASA

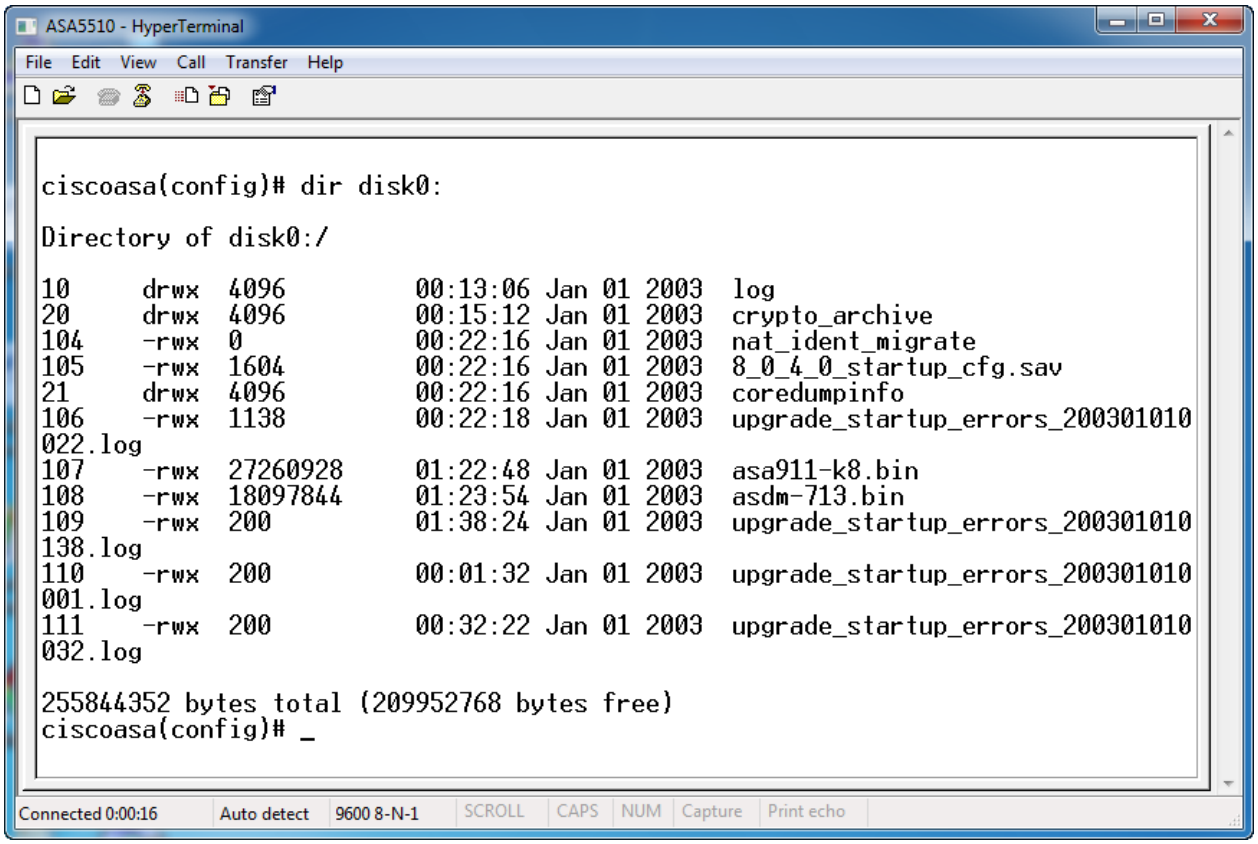
ASA có phiên bản 8.3 có nhiều tính năng bảo mật hơn nên yêu cầu bộ nhớ cao hơn. Cisco cho phép nâng cấp bộ nhớ để chạy các phiên bản từ 8.3 trở lên.

ASA Model	Minimum DRAM Required Prior to 8.3	Minimum DRAM Required 8.3 and Later
5505	256 MB	256 MB
5505 Unlimited User and Security Plus	256 MB	512 MB
5510	256 MB	1 GB
5520	512 MB	2 GB
5540	1 GB	2 GB
5550	4 GB	4GB
5580-20	8 GB	8 GB
5580-40	12 GB	12 GB
5585-X SSP-10	N/A	6 GB
5585-X SSP-20	N/A	12 GB
5585-X SSP-40	N/A	12 GB
5585-X SSP-60	N/A	24 GB

Hình 2. 23 Yêu cầu bộ nhớ cho phiên bản 8.3 trở lên.

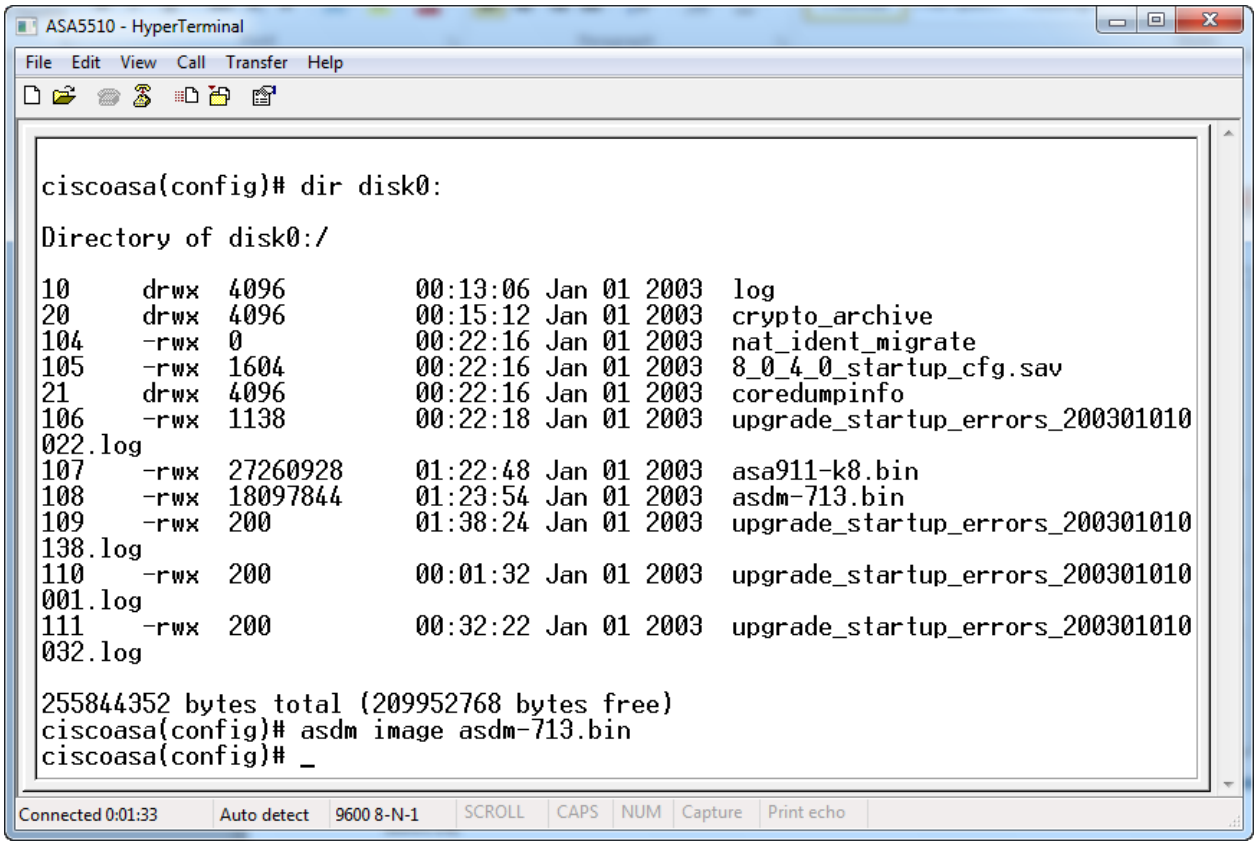
2.9 Cấu hình ASA với ASDM (tuần kế tiếp)

Bước 1: kiểm tra image asdm-713.bin.



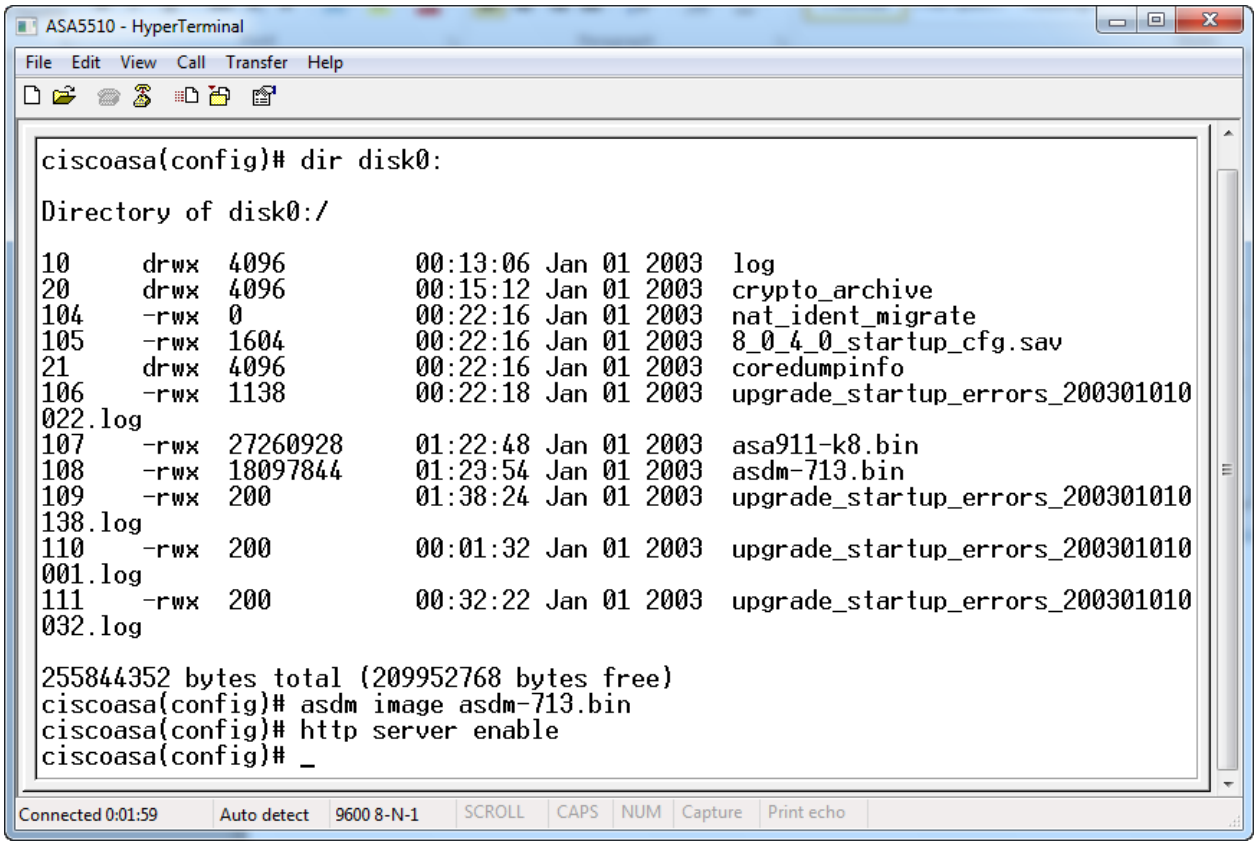
Hình 2. 24 Kiểm tra image ASDM

Bước 2 khai báo image asdm-713.bin.



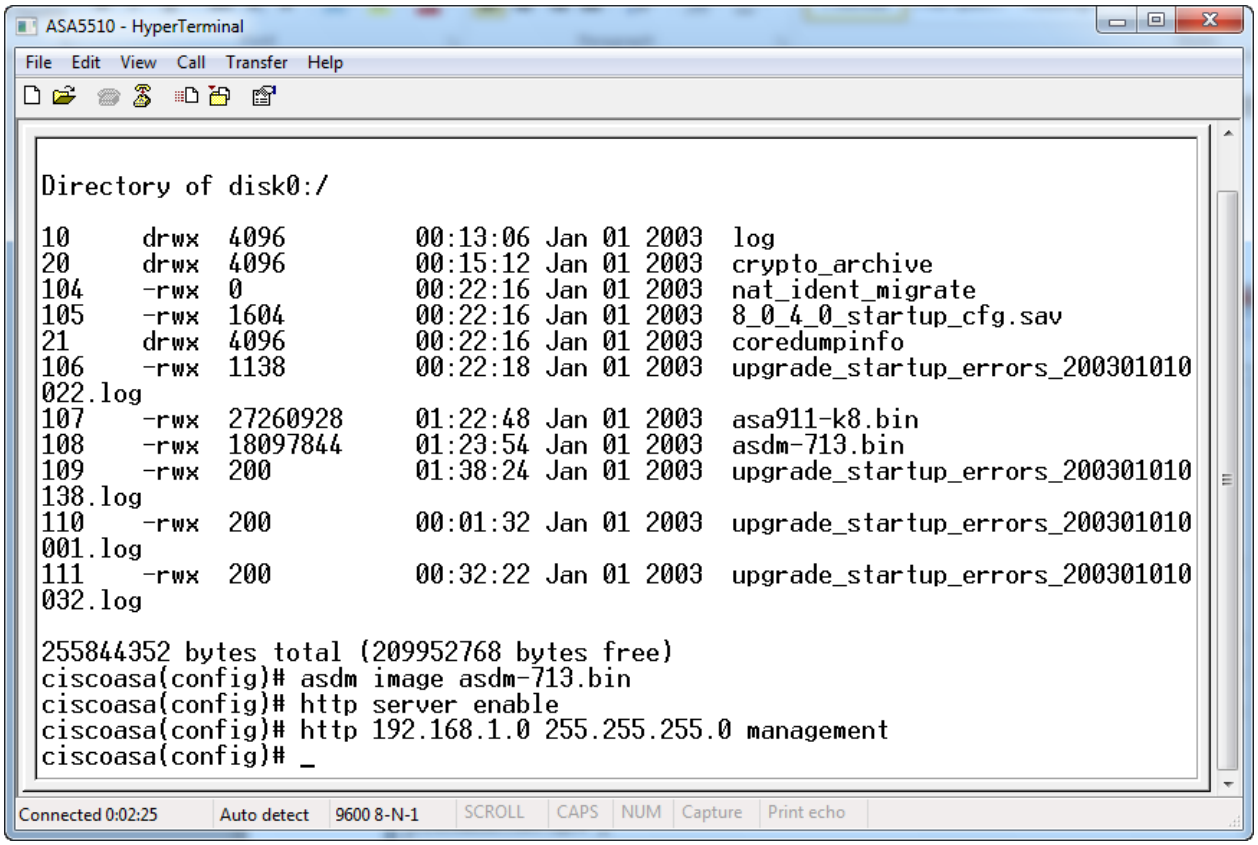
Hình 2. 25 Khai báo image asdm

Bước 3 kích hoạt dịch vụ http



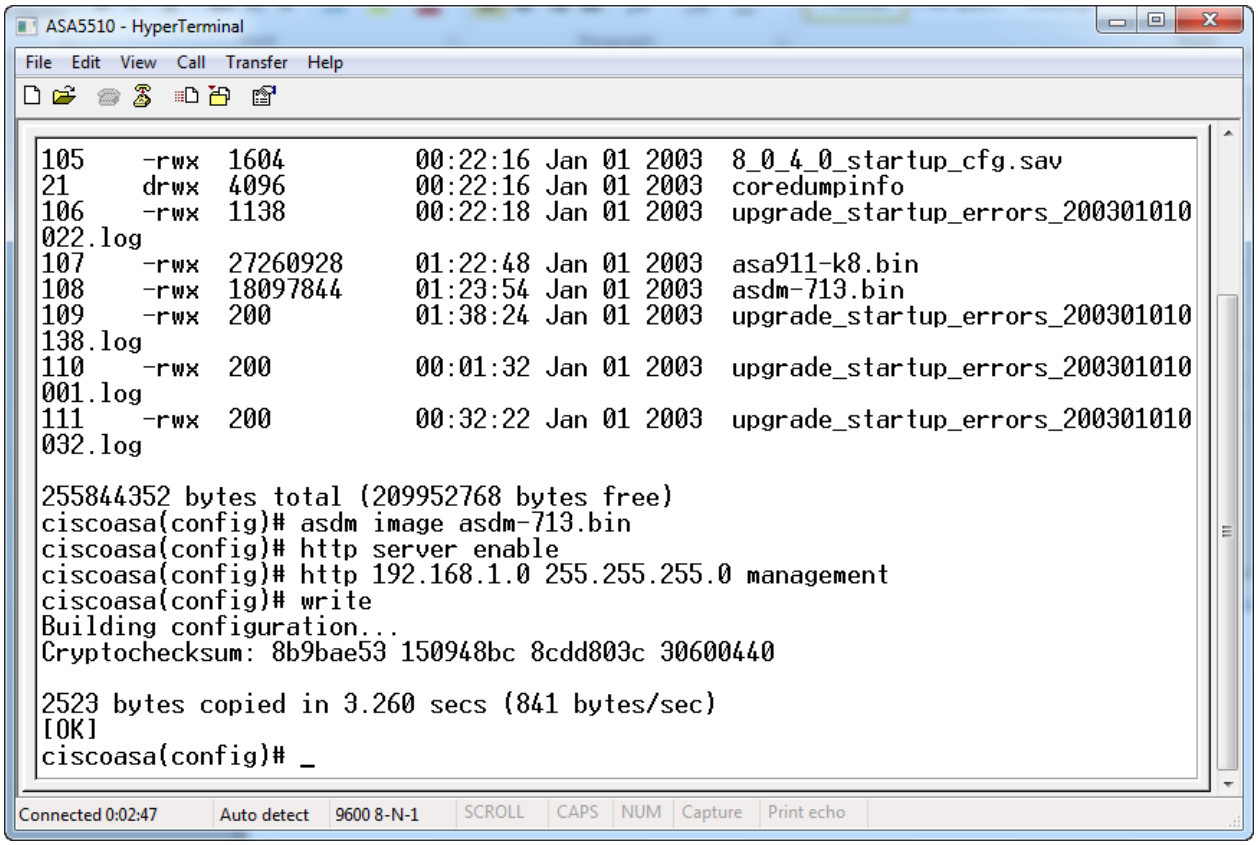
Hình 2. 26 Kích hoạt giao thức http

Bước 4 cho phép lớp mạng 192.168.1.0/24 truy cập ASA qua trình duyệt web.



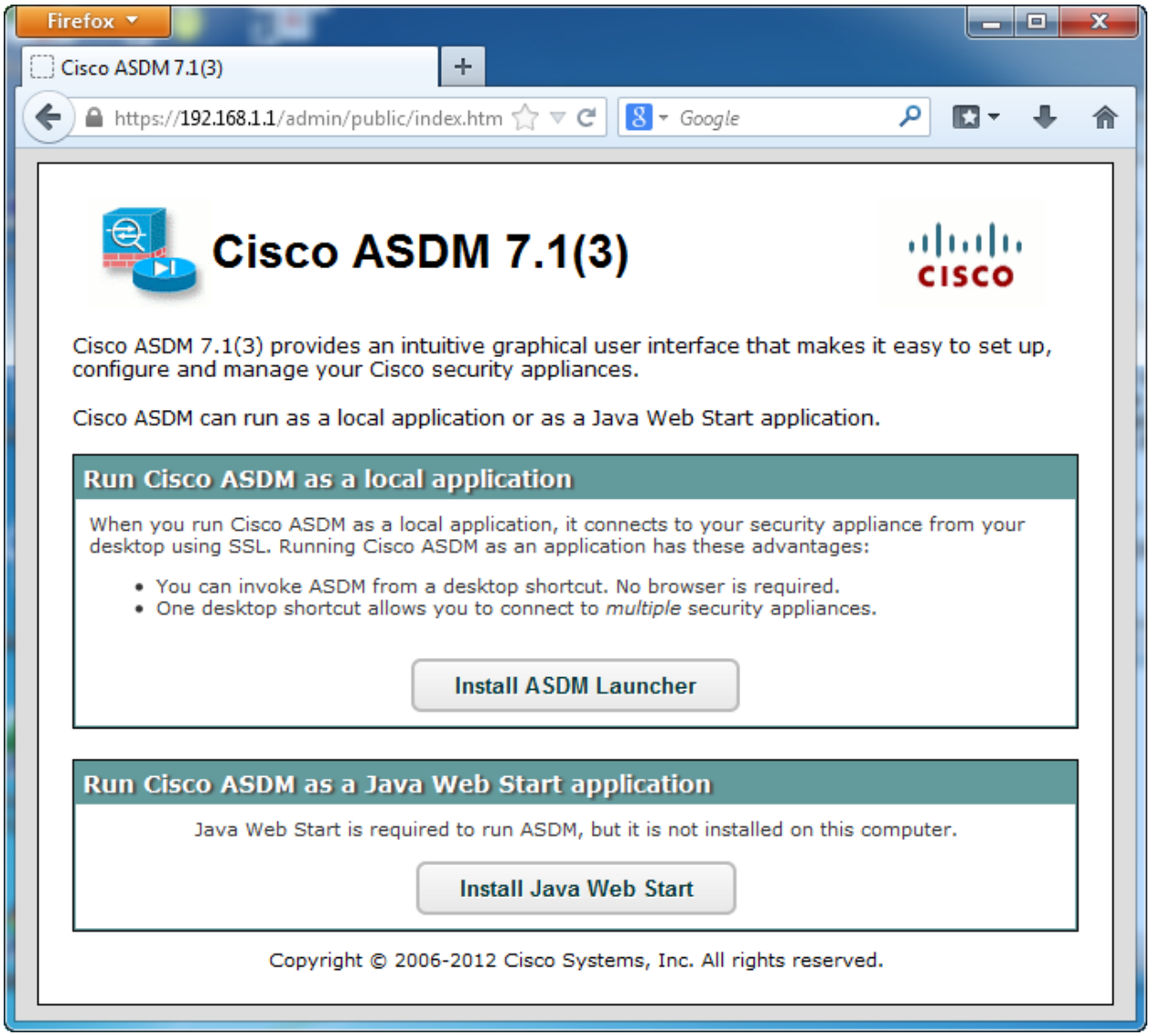
Hình 2. 27 Cho phép địa chỉ IP truy cập ASA qua giao diện web.

Bước 5 lưu cấu hình vào flash để kích hoạt dịch vụ http



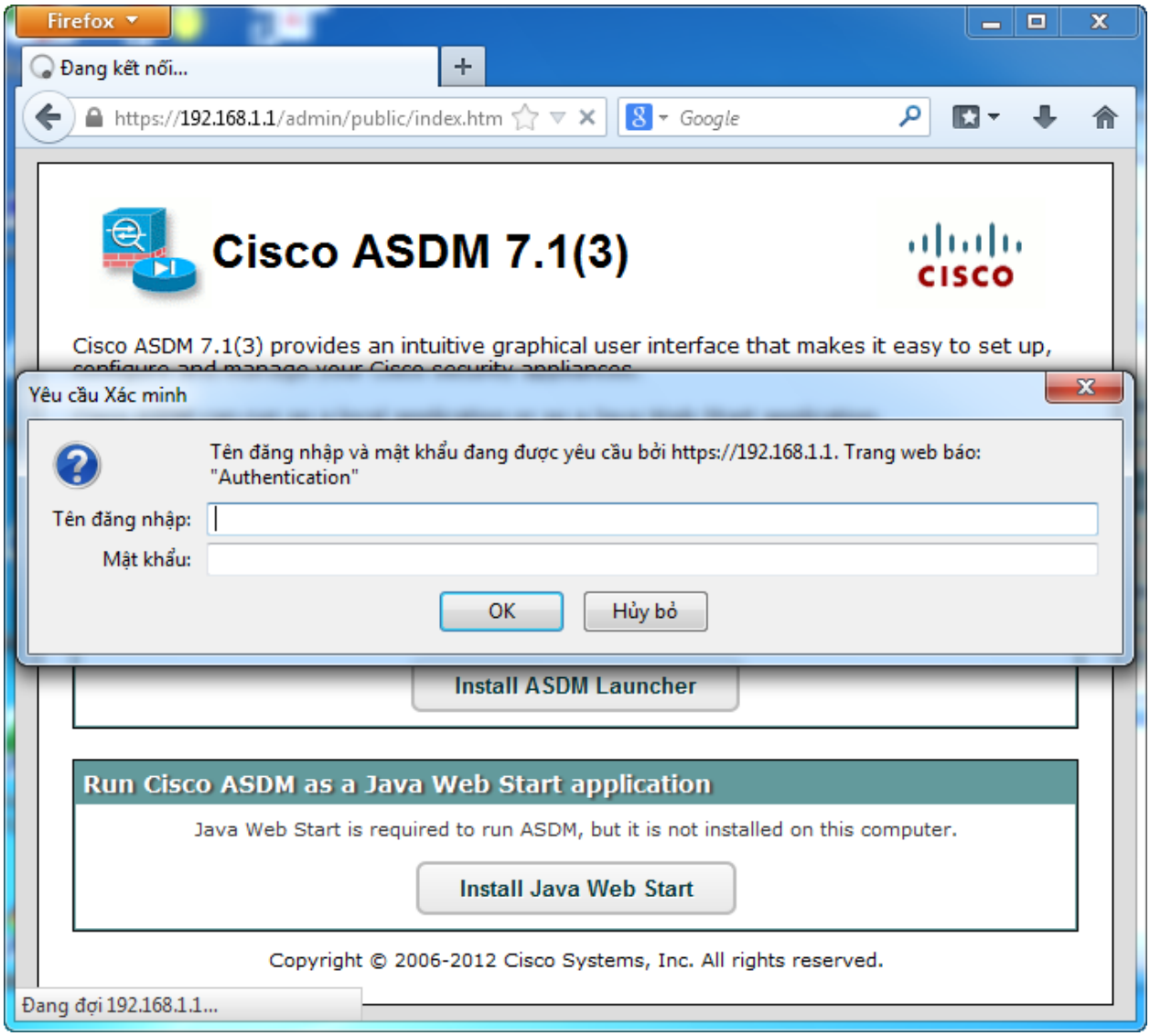
Hình 2. 28 Lưu cấu hình vào flash

Sau đó truy cập https://192.168.1.1 trên trình duyệt web.



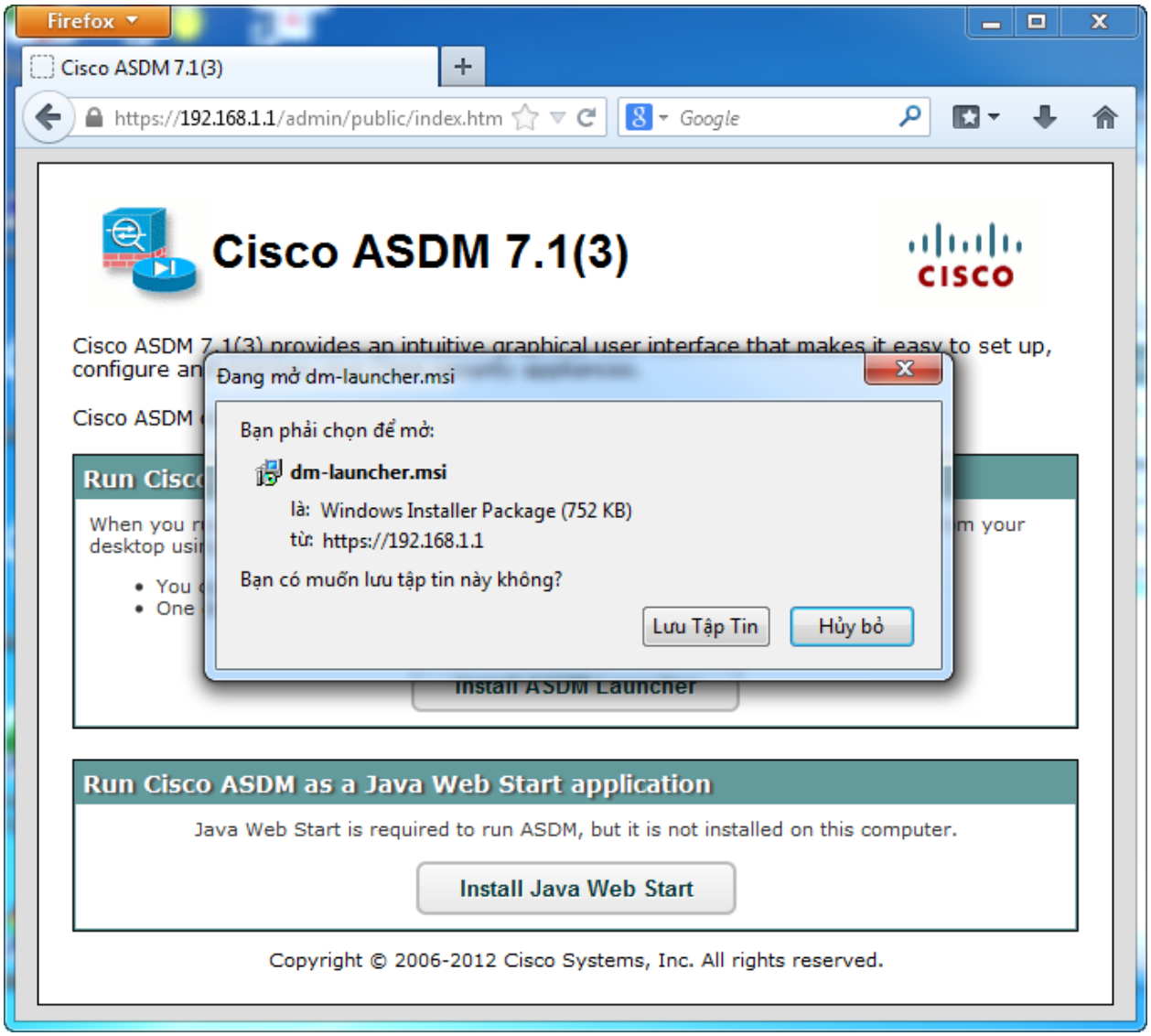
Hình 2. 29 Truy cập ASA qua cổng interface management.

Chọn Install ASDM Launcher và chọn OK



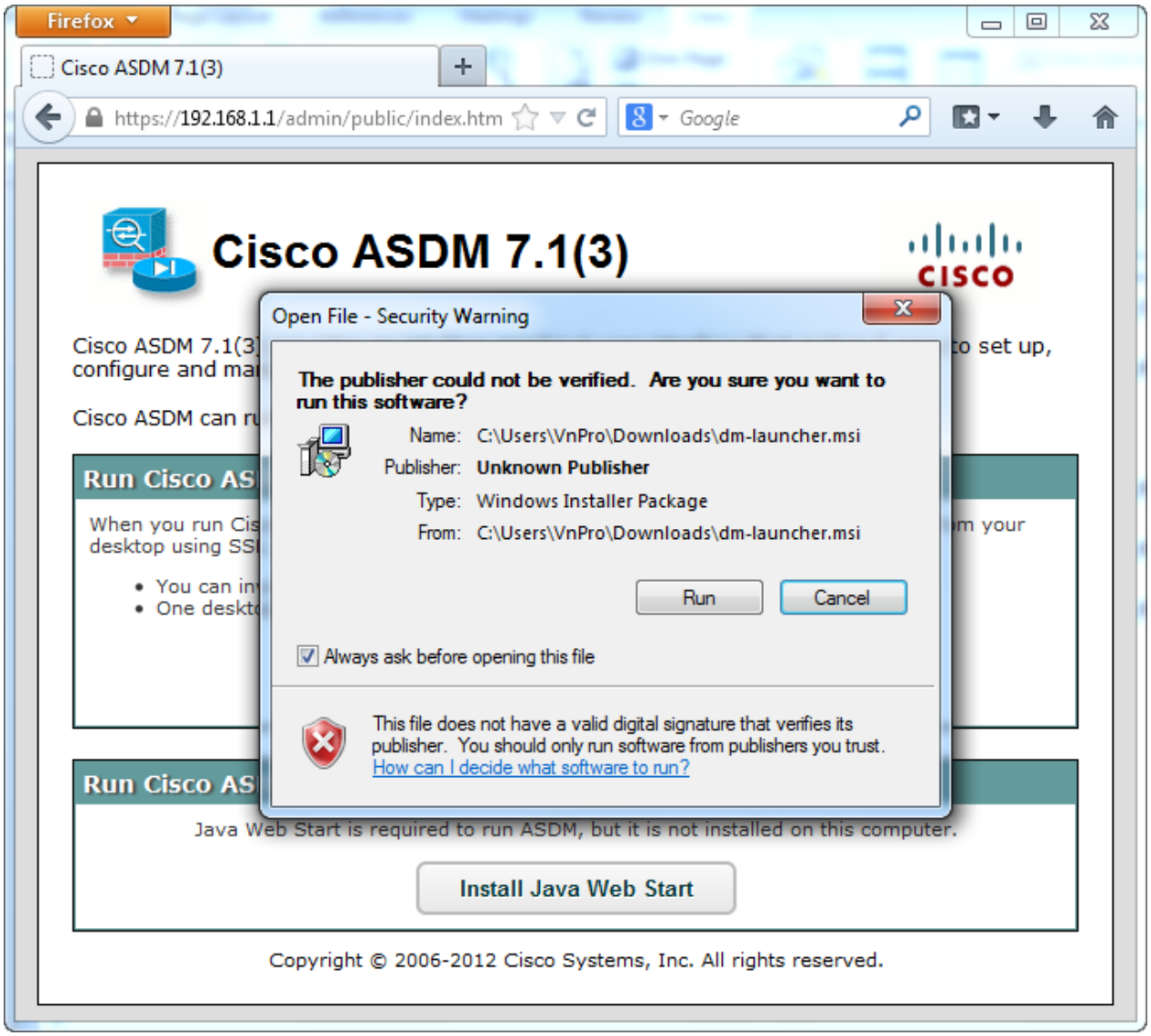
Hình 2. 30 Chọn Install ASDM Laucher

Chọn Lưu Tập Tin để tải về



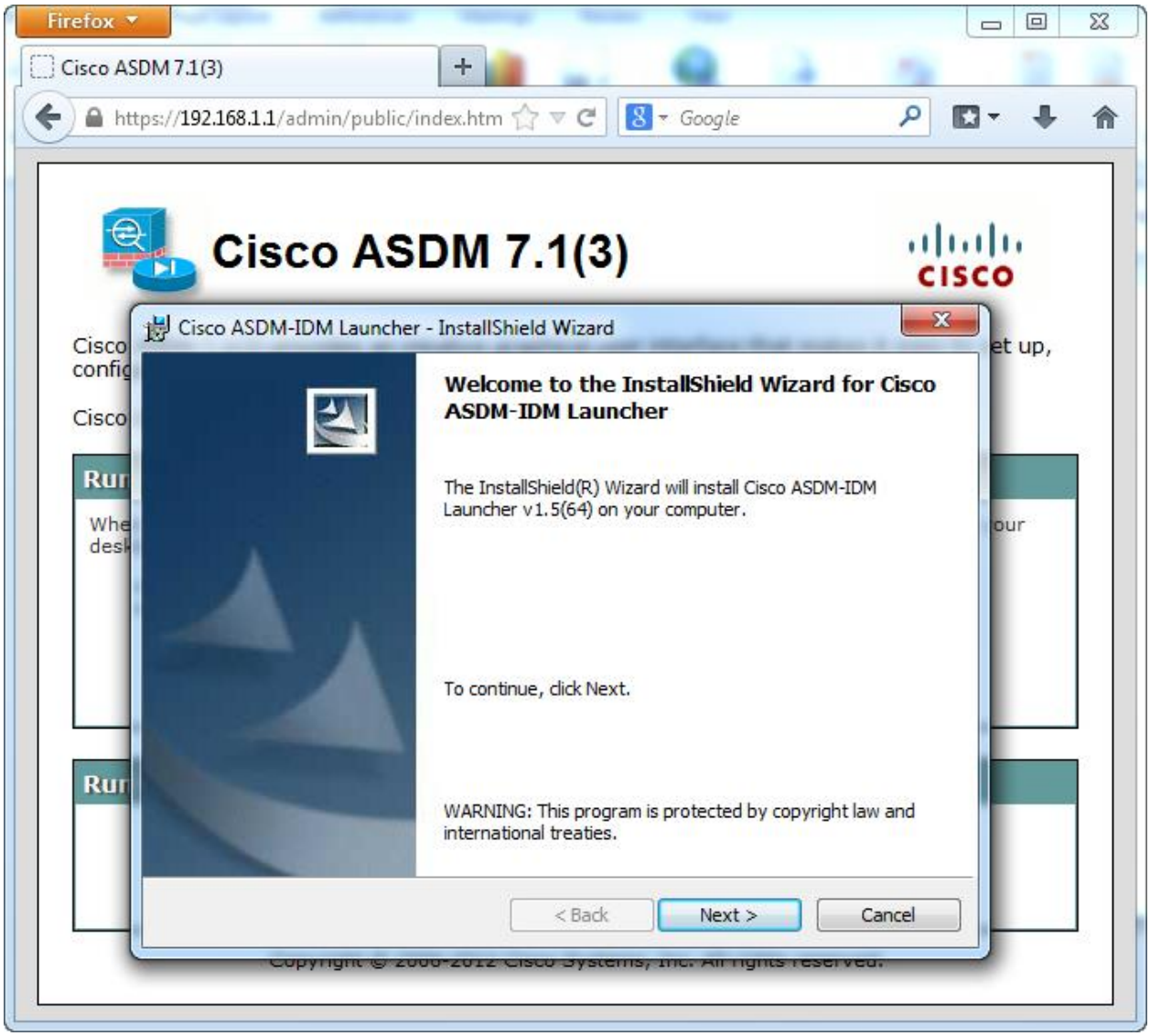
Hình 2. 31 Chọn lưu tập tin dm-laucher.msi

Sau khi cài đặt Java Runtime Environment 1.7.0.45, chọn Run để cài đặtASDM.



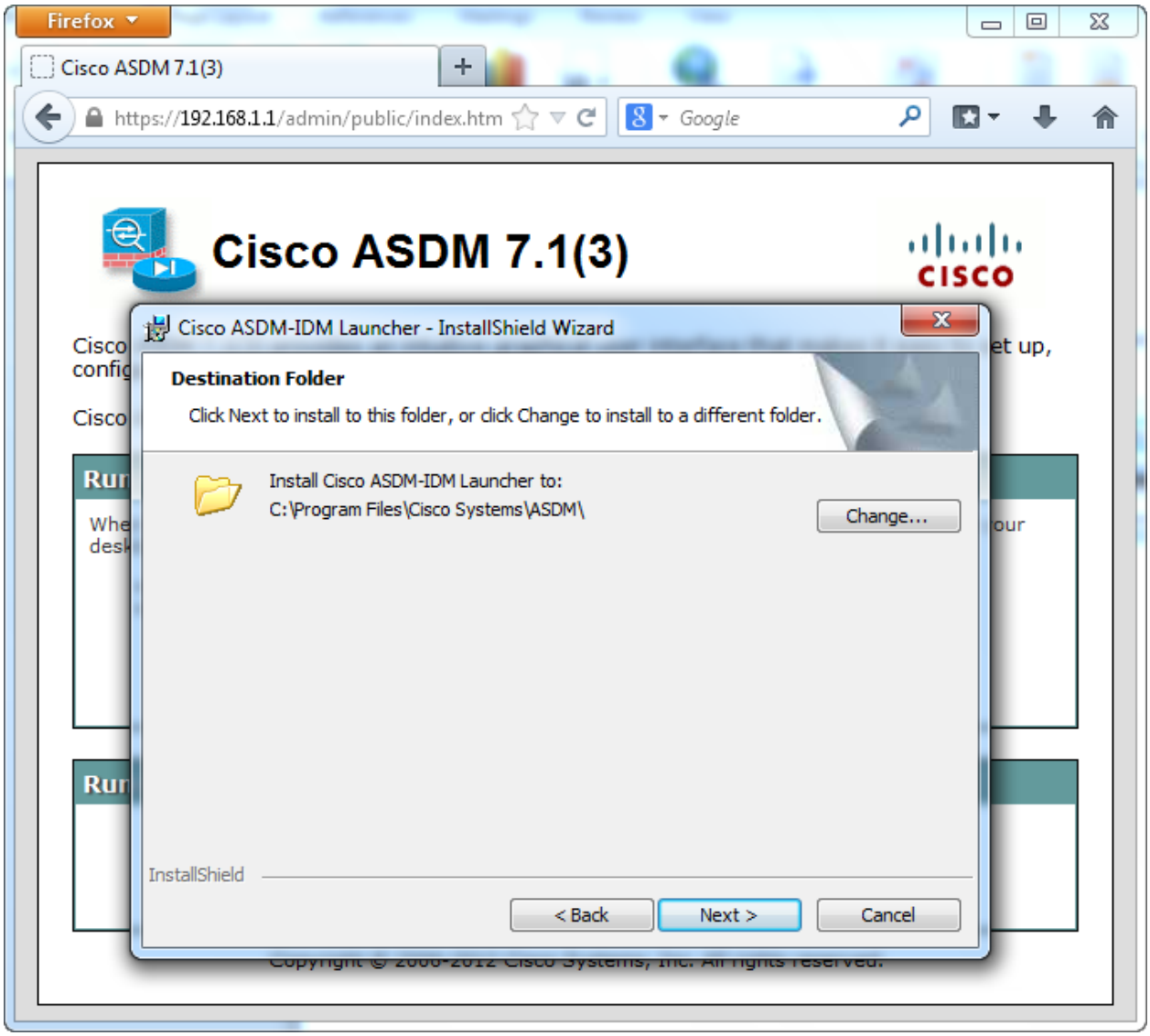
Hình 2. 32 Chọn Run để tiến hành cài đặt

Chọn Next để tiếp tục cài đặt



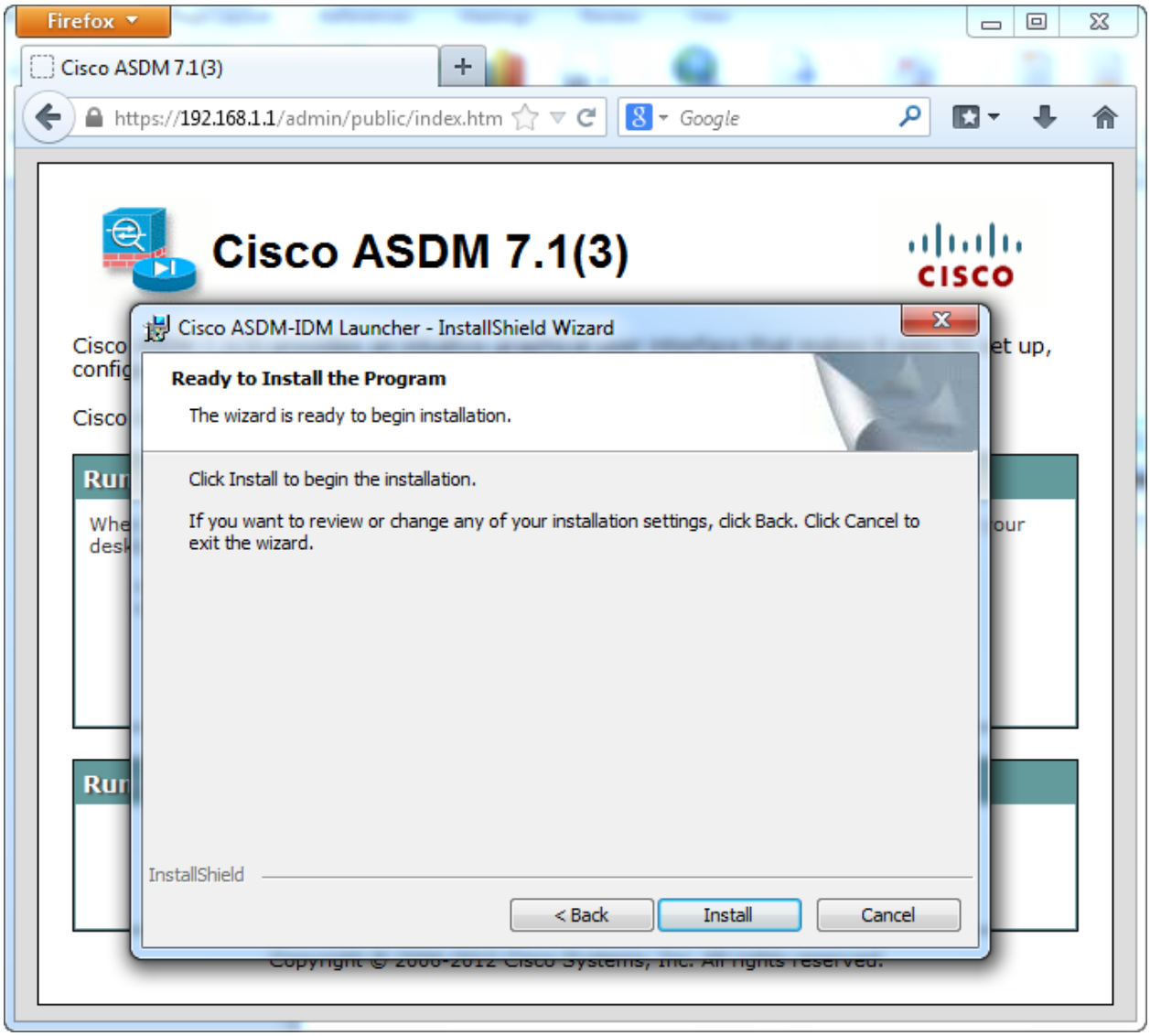
Hình 2. 33 Chọn tiếp để tiếp tục cài đặt

Tiếp tục chọn Next



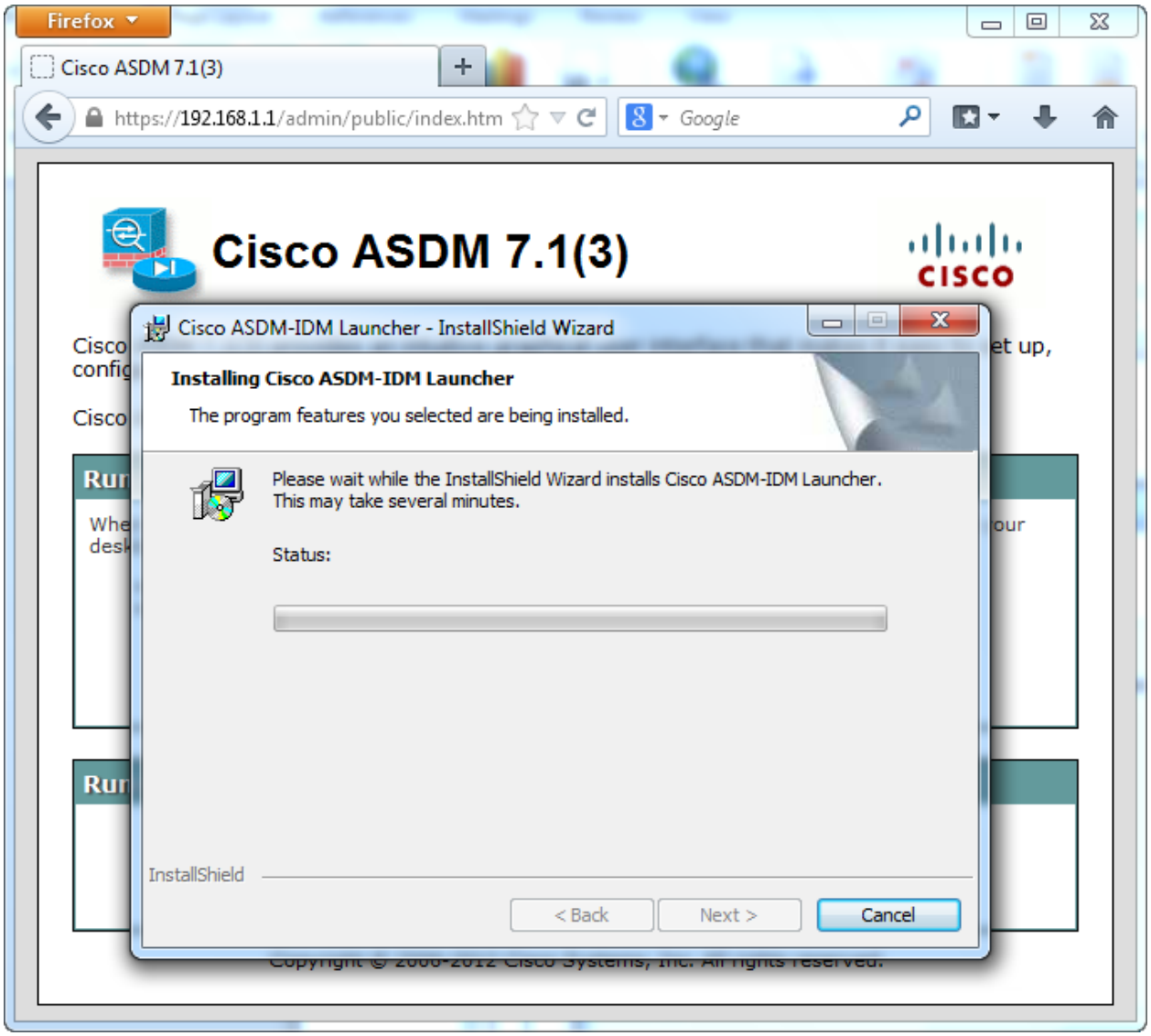
Hình 2. 34 Chọn Next để tiếp tục

Chọn Install để bắt đầu cài đặt



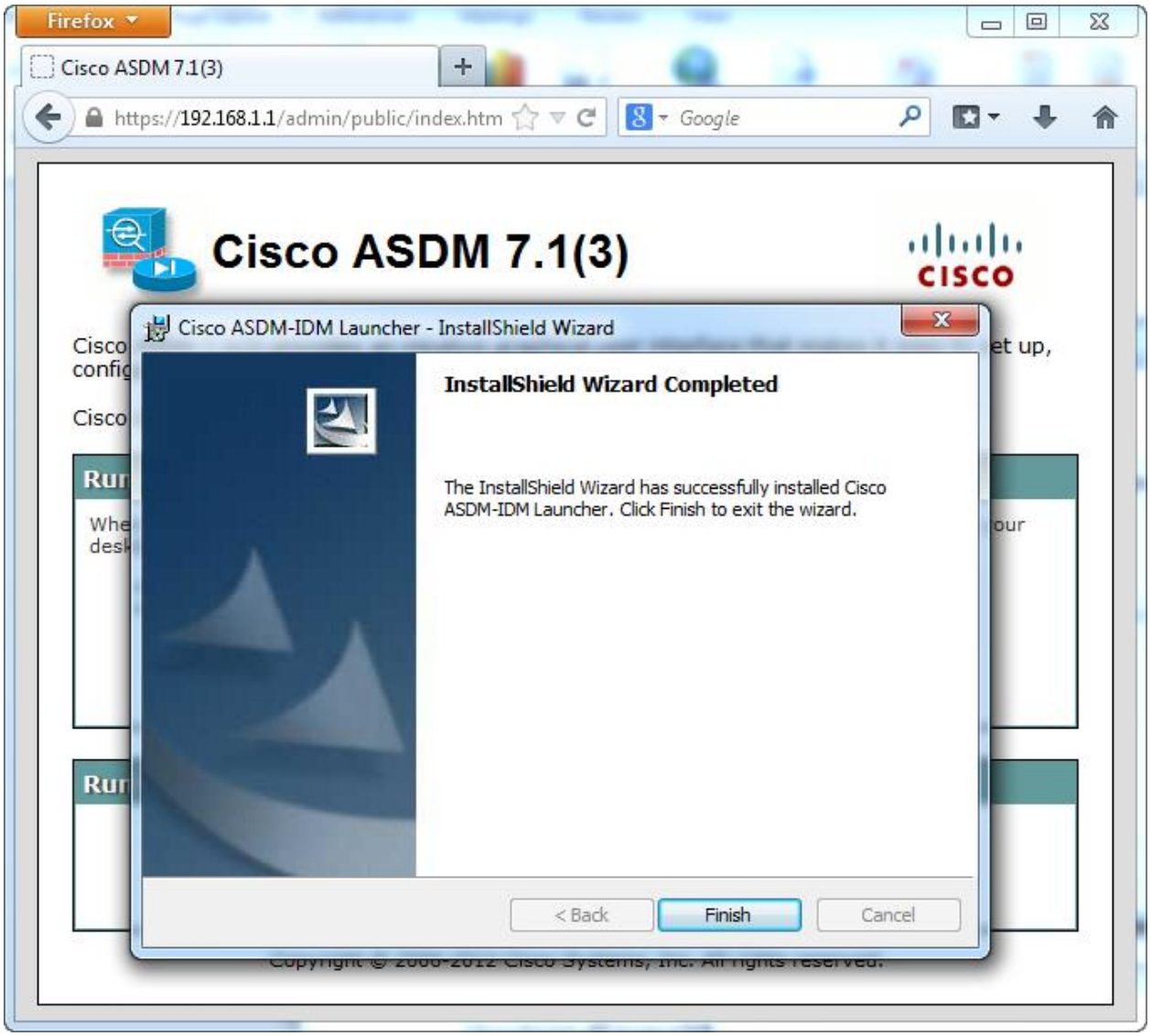
Hình 2. 35 Chọn Install để bắt đầu cài đặt

ASDM đang được cài đặt



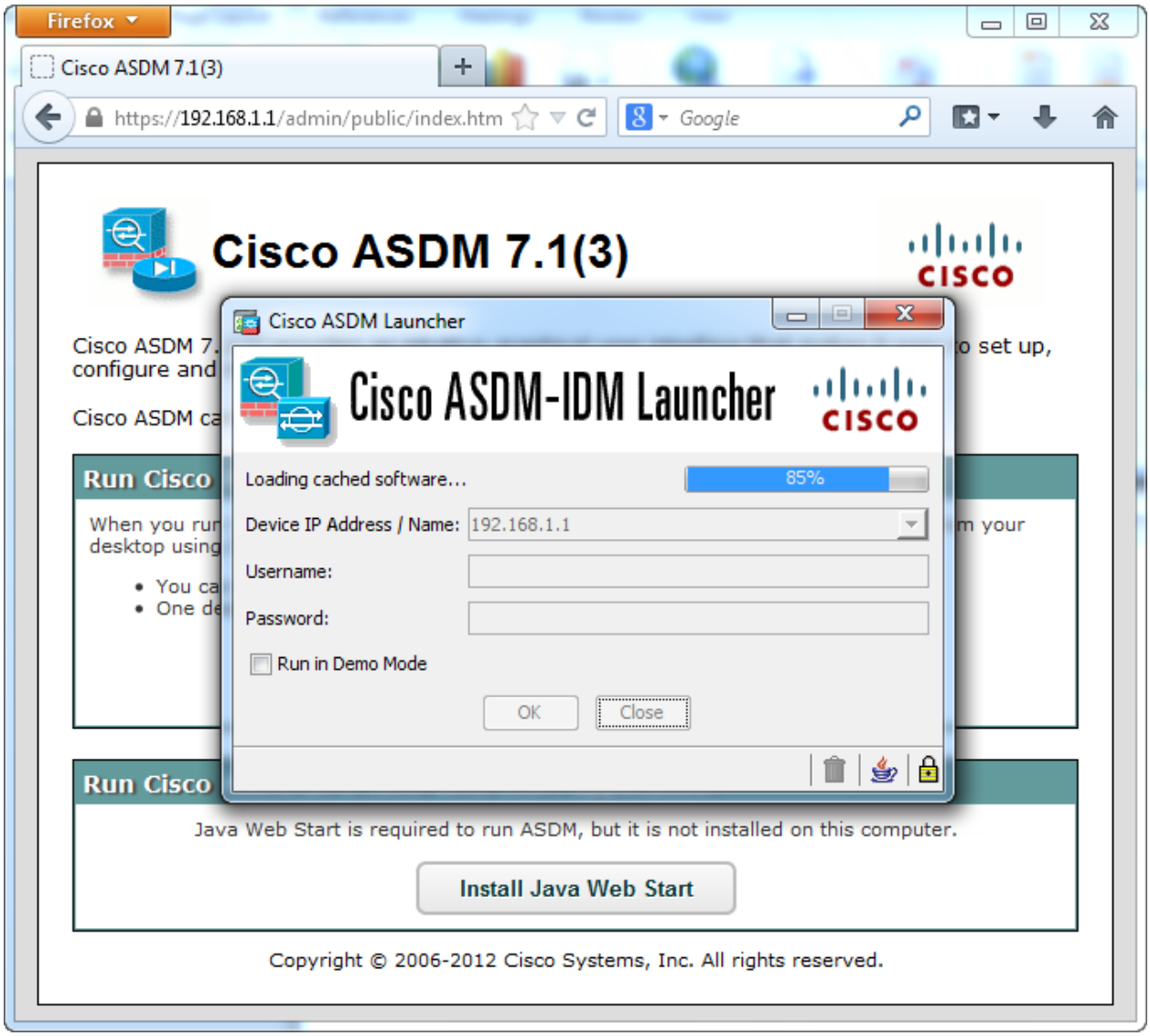
Hình 2. 36 ASDM đang được cài đặt

Chọn Finish để hoàn tất



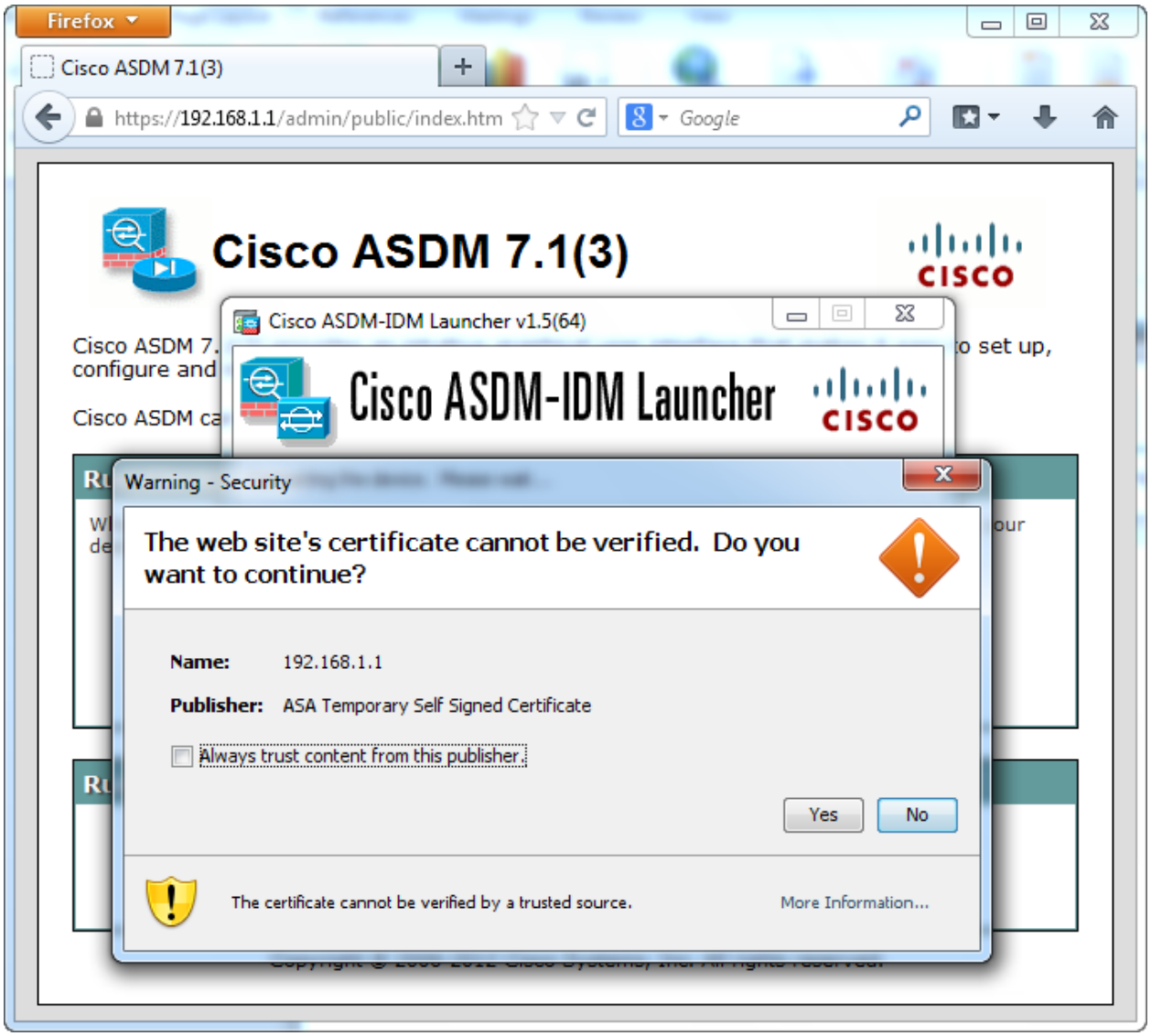
Hình 2. 37 Chọn Finish để hoàn tất

Không có mật khẩu nên chọn OK



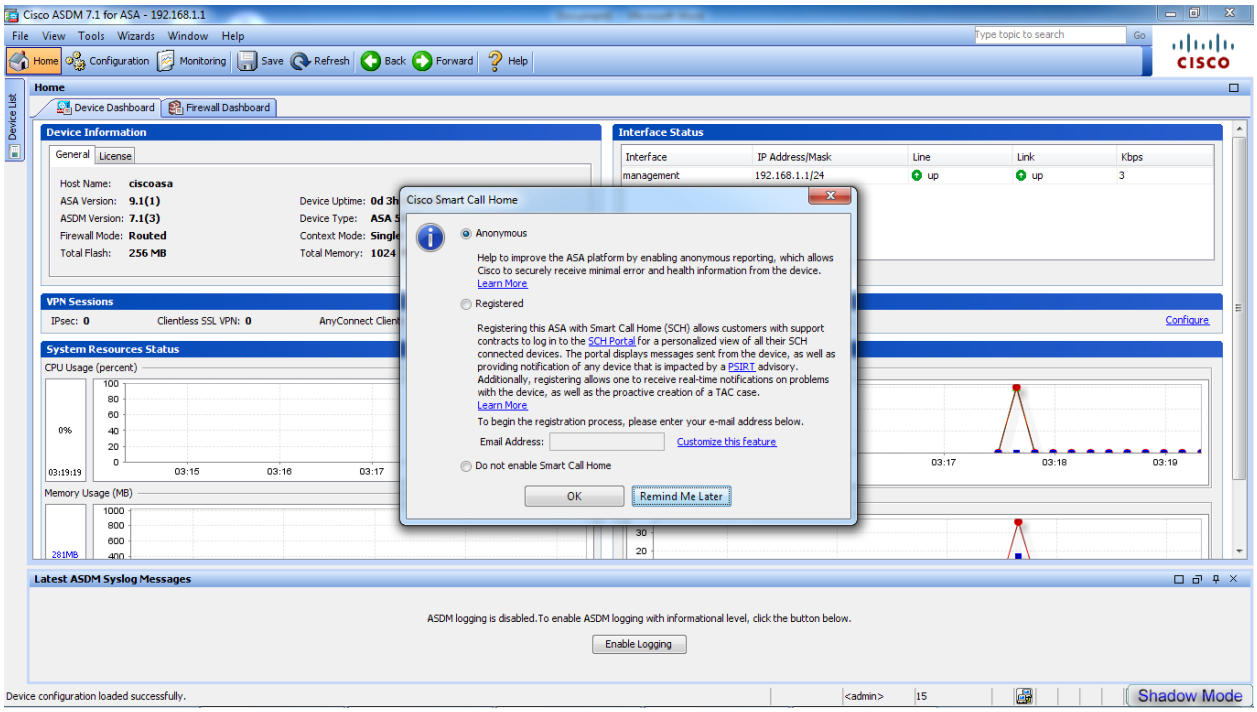
Hình 2. 38 Chọn OK để bắt đầu quản lý ASA

Chọn Yes để tiếp tục



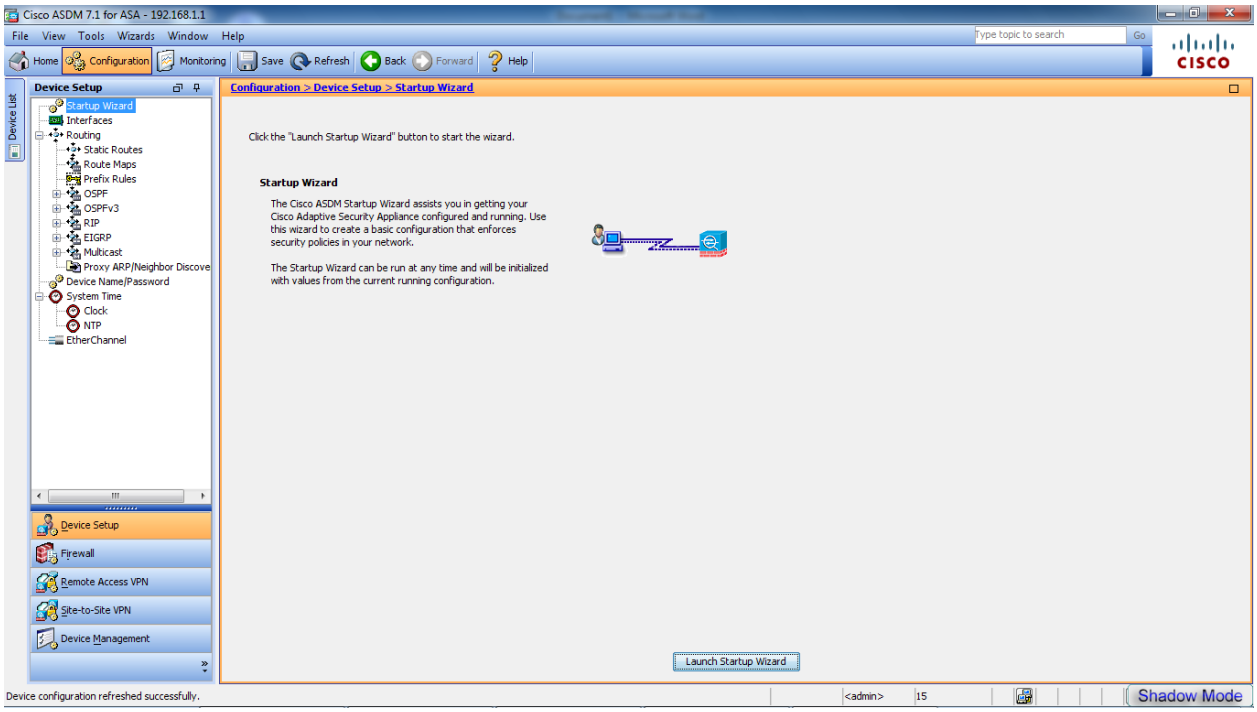
Hình 2. 39 Chọn Yes để tiếp tục

Chọn OK để bắt đầu



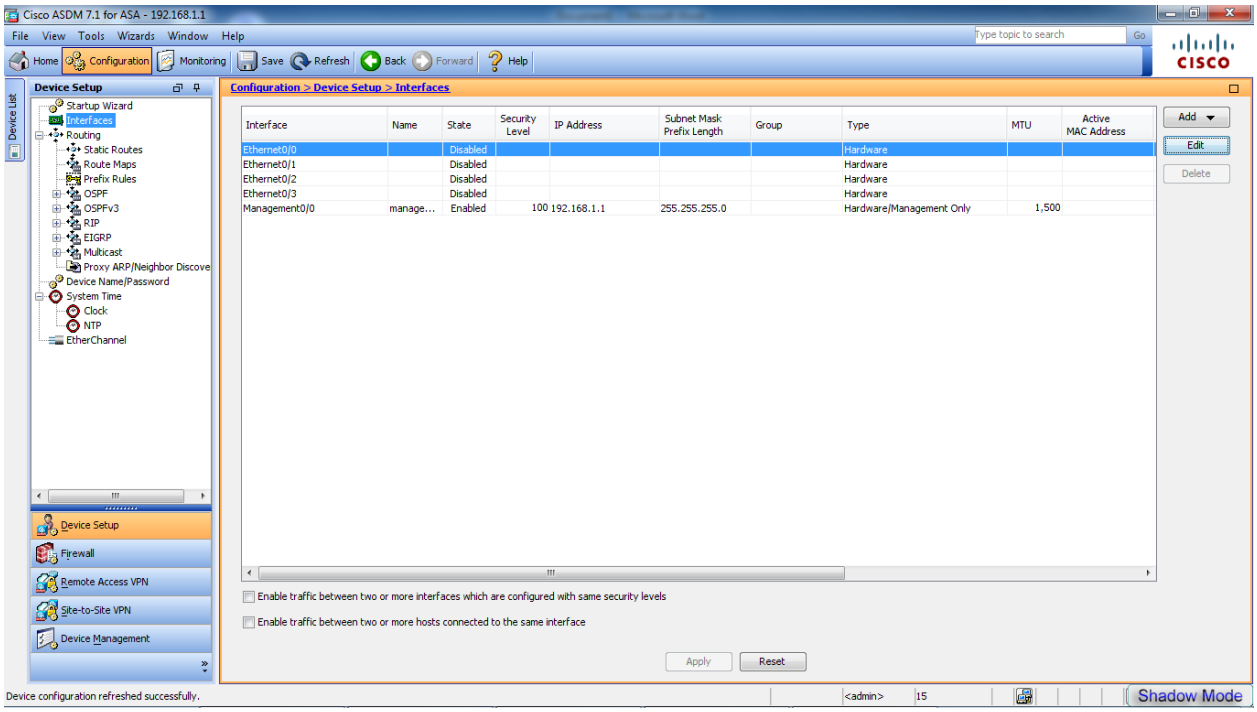
Hình 2. 40 Chọn Ok để vào giao diện quản lý

Giao diện ASDM



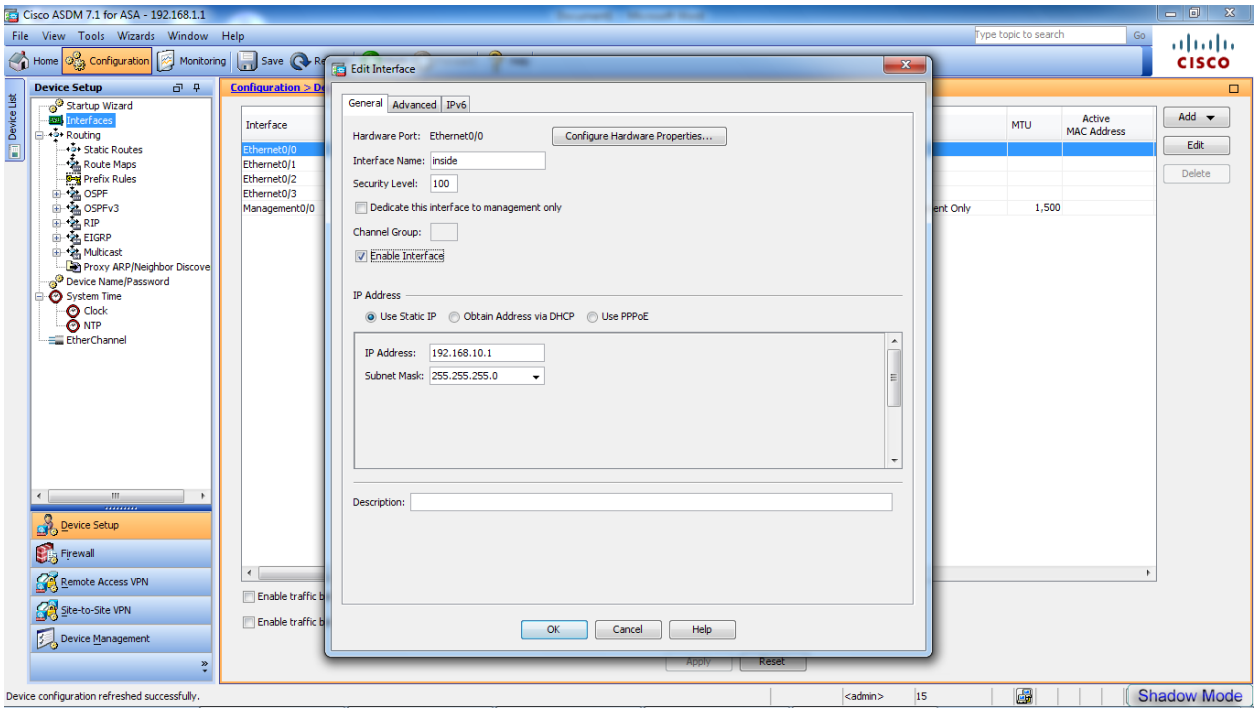
Hình 2. 41 Giao diện chính của ASDM

Cấu hình các cổng interface



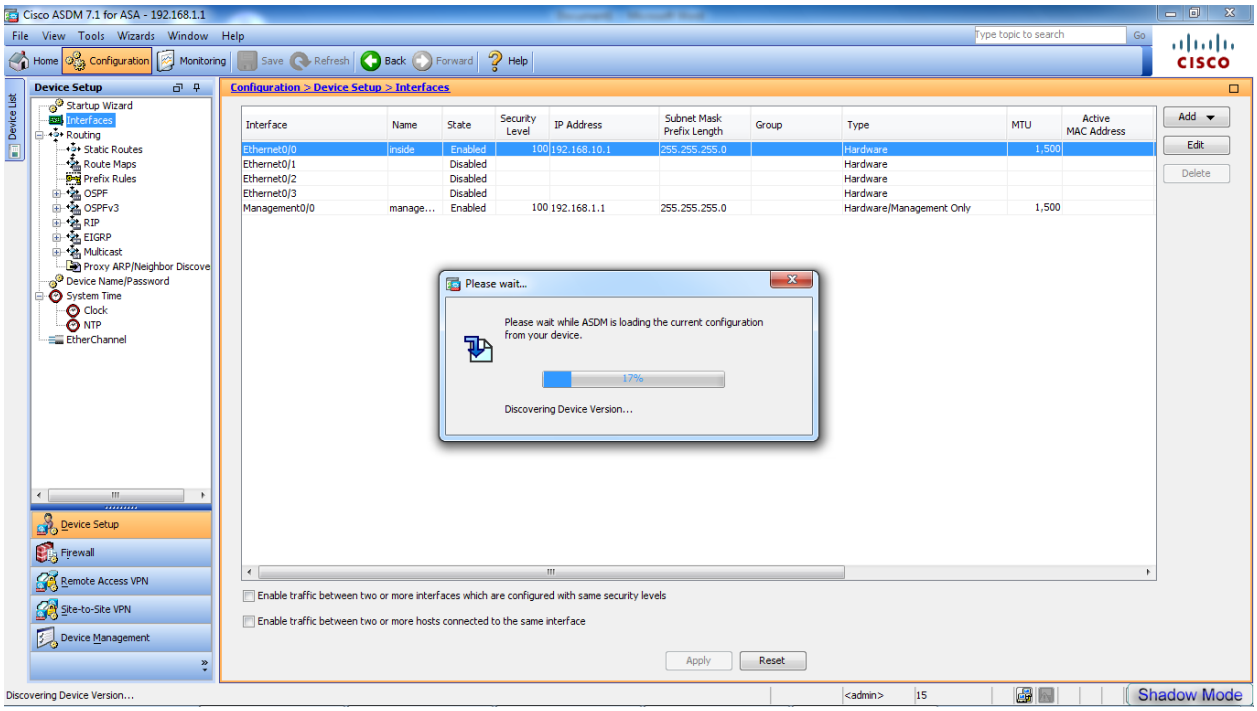
Hình 2. 42 Các cổng interface của ASA 5510

Chọn Edit để cấu hình cổng Ethernet 0/0 inside



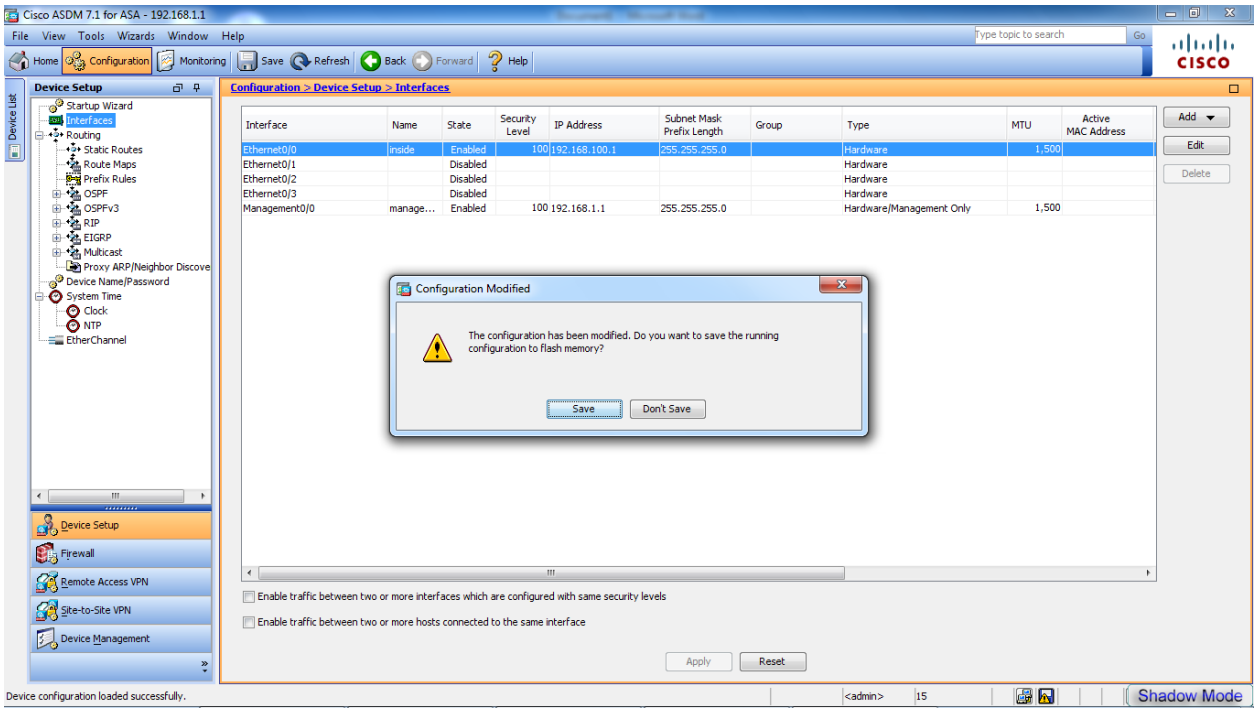
Hình 2. 43 Chọn Edit để nhập địa chỉ IP và đặt tên cho interface

Sau đó chọn Apply để lưu cấu hình



Hình 2. 44 Chọn Apply để lưu lại cấu hình

Khi thoát ASDM, chọn Save để lưu cấu hình vào flash



Hình 2. 45 Chọn Save để lưu cấu hình vào Flash