CHƯƠNG I: TỔNG QUAN VỀ IPSEC

1. Khái niệm **về IPSec**

Để có thể bắt tay vào nghiên cứu về IPSec, trước hết chúng ta cần phải hiểu khái niệm, IPSec là gì?

IPSec là một khung kiến trúc cung cấp các dịch vụ bảo mật, mật mã dành cho các gói IP. IPSec là một kỹ thuật bảo mật điểm tới điểm (end-to- end).

Điều đó có nghĩa là chỉ có những trạm biết rõ về sự hiển diện của IPSec, chính là 2 máy tính sử dụng IPSec đang liên lạc với nhau, là biết rõ về cơ chế bảo mật. Các bộ định tuyến giữa đường không thể biết được quan hệ bảo mật của hai trạm trên và chúng chỉ chuyển tiếp các gói IP như là chúng đã làm với tất cả các gói IP khác. Mỗi máy tính sẽ điều khiển chức năng bảo mật tại đầu của nó với giả thiết rằng tất cả các trạm ngang đường đều là không bảo mật. Các máy tính chỉ làm nhiệm vụ định tuyến các gói tin từ nguồn đến đích không cần thiết phải hỗ trợ IPSec. Chỉ có một loại trừ là các bộ lọc gói tin dạng Firewall hay NAT đứng giữa hai máy tính. Với mô hình này IPSec sẽ được triển khai thành công theo kịch bản sau:

* Mạng cục bộ (LAN): mạng cục bộ dạng Chủ - Khách hay mạng ngang hàng.
* Mạng diện rộng (WAN): Mạng WAN giữa các bộ định tuyến (Router-to-Router) hay giữa các cổng (Gateway-to-Gateway)
* Truy cập từ xa: Các máy khách quay số hay truy cập Internet từ các mạng riêng.

Thông thường, cả hai đầu đều yêu cầu cấu hình IPSec, hay còn được gọi là Chính sách IPSec, để đặt các tùy chọn và các thiết lập bảo mật cho phép hai hệ thống thỏa thuận việc sẽ bảo mật các lưu thông giữa chúng như thế nào. Các hệ điều hành Windows Server 2000, Windows XP, và Windows Server 2003 thực thi IPSec dựa trên các chuẩn công nghiệp do nhóm IPSec, của IETF (Internet Engineering Task Force) phát triển.

1. Mục đích của IPSec

Các Header (tiêu đề) của IP, Transmission Control Protocol (TCP- Giao thức Kiểm soát Truyền dẫn), và User Datagram Protocol (UDP-Giao thức gói dữ liệu người dùng) đều chứa một số Kiểm soát (Check sum) được sử dụng để kiểm soát tình toàn vẹn (Integrity) dữ liệu của một gói IP. Nếu dữ liệu bị hỏng, Số Kiểm soát sẽ thông báo cho người nhận biết. Tuy nhiên, do thuật toán Số Kiểm soát này được phổ biến rộng rãi nên kể cả người dùng không có chức năng cũng có thể truy cập vào gói tin một cách dễ dàng thay đổi nội dung của chúng và tính lại số Kiểm soát, sau đó lại chuyển tiếp gói tin này đến tay người nhận mà không một ai, kể cả người gửi lẫn người nhận biết đến sự can thiệp này. Do các hạn chế về chức năng của số kiểm soát như vậy, tại nơi nhận, người dùng không hề biết và cũng không thể phát hiện ra việc gói tin đã bị thay đổi.

Trong quá khứ, các ứng dụng càn bảo mật sẽ tự cung cấp cơ chế bảo mật cho riêng chúng dẫn tới việc có quá nhiều các chuẩn bảo mật khác nhau và không tương thích.

IPSec là một bộ các Giao thức và Thuật toán Mã hóa cung cấp khả năng bảo mật tại lớp Internet (Internet Layre) mà không cần phải quan tâm đến các ứng dụng gửi hay nhận dữ liệu.

Sử dụng IPSec, chỉ cần một chuẩn bảo mật được áp dụng và việc thay đổi ứng dụng không càn thiết.

IPSec có 2 mục đích chính:

* Bảo vệ nội dung của các gói IP.
* Cung cấp việc bảo vệ chống lại các cuộc tấn công mạng thông qua lọc gói tin và việc bắt buộc sử dụng các kết nối tin cậy.

Cả hai mục tiêu trên đều có thể đạt được thông qua việc sử dụng các dịch vụ phòng chống dựa trên cơ chế mã hóa, các giao thức bảo mật và việc quản lý các khóa động. Với các nền tảng như vậy, IPSec cung cấp cả hai tính năng Mạnh vả Uyển chuyển trong việc bảo vệ các cuộc liên lạc giữa các máy tính trong mạng riêng, Miền, Site (bao gồm cả các Site truy cập từ xa), các mạng Intranet, các máy khách truy cập qua đường điện thoại. Thậm chí nó còn được sử dụng để khóa việc nhận hay gửi của một loại lưu thông chuyên biệt nào đó.

Chống lại các cuộc tấn công bảo mật là bảo vệ các gói tin làm cho chúng trở thành quá khó, nếu không nói là không thế, đối với các kẻ xâm nhập để có thể dịch được các dữ liệu mà họ thu giữ được. IPSec có một số các tính năng mà có thể làm giảm đáng kể hay ngăn ngừa được các loại tấn công sau:

* Do thám gói dữ liệu (Packet Sniffing): Packet Sniffer là một ứng dụng thiết bị có thể theo dõi và đọc các gói dữ liệu. Nếu gói dữ liệu không được mã hóa, các Packet Sniffer có thể trình bày đày đủ các nội dung bên trong các gói dữ liệu.
* Thay đổi dữ liệu: Kẻ tấn công có thể thay đổi các thông điệp đang được vận chuyển và gửi đi các dữ liệu giả mạo, nó có thể ngăn cản người nhận nhận được các dữ liệu chính xác, hay có thể cho phép kẻ tấn công lấy được thêm các thông tin bảo mật. IPSec sử dụng các khóa mã hóa, chỉ được chia sẻ giữa người gửi và người nhận, để tạo ra các số Kiểm soát được mã hóa cho mỗi gói IP. Mọi thay đổi đối với gói dữ liệu đều dẫn đến việc thay đổi Số Kiểm soát và sẽ chỉ ra cho người nhận biết rằng gói dữ liệu đã bị thay đổi trên đường truyền.
* Nhận dạng giả mạo : Kẻ tấn công có thể làm giả các mã nhận dạng (Identity Spoofing) bằng cách sử dụng một chương trình đặc biệt để xây dựng các gói IP mà xuất hiện như các gói dữ liệu gốc từ các địa chỉ hợp lệ bên trong mạng được tin cậy. IPSec cho phép trao đổi và xác nhận lại các mã nhận dạng mà không phơi chúng ra cho các kẻ tấn công dịch. Sự xác nhận lẫn nhau (xác thực) được sử dụng để thiết lập tin cậy giữa các hệ thống cũng tham gia liên lạc với các hệ thống khác. Sau khi các mã nhận dạng được thiết lập, IP See sử dụng các khóa mã hóa, được chia sẻ chỉ giữa người gửi và người nhận, để tạo các số kiểm soát được mã hóa cho mỗi gói IP. Các số kiểm soát được mã hóa đảm bảo rằng chỉ các máy tính đã biết rõ về các khóa là có thể gửi được từng gói dữ liệu.
* Tấn công ngang đường (man-in-the-middle attack) trong dạng tấn công này, một người nào đó, đứng giữa hai máy tính đang liên lạc với nhau, sẽ tiến hành theo dõi, thu nhập và điều khiển các dữ liệu một cách trong suốt. IPSec kết hợp việc xác thực lẫn nhau và các được mã hóa để chống lại dạng tấn công này.
* Tấn công từ chối dịch vụ (DoS): Ngăn cản việc vận hành bình thường của các tài nguyên mạng và máy tính. Làm lụt các tài khỏa E-mail bằng các thông điệp không mong muốn là một ví dụ của dạng tấn công này. IPSec sử dụng phương pháp lọc các gói IP (IP packet Filtering) làm cơ sở cho việc xác định mối liên lạc nào là được phép, bảo mật hay phải khóa lại. Việc xác định mối liên lạc nào là được phép, bảo mật hay phải khóa lại. Việc xác định trên dựa vào dẫy địa chỉ IP, Giao thức IP hay thậm chí một số cổng TCP hay ƯDP xác định nào đó.

CHƯƠNG II: TÌM HIỂU VÈ IPSEC

1. Các tính năng bảo mật của IPSec
   1. Các tính năng bảo mật của IPSec

IPSec có rất nhiều tính năng bảo mật được thiết kế để thỏa macn mục tiêu bảo vệ các gói IP va chống lại các cuộc tấn công nhờ vào các bộ lọc và cơ chế kết nối tin cậy. Một vài trong các tính năng bảo mật của IPSec được liệt kê sau:

■ Sự kết họp bảo mật tự động: IPScc sử dụng Internet Security Association (Kết họp bảo mật Internet) và Key Management Protocol

(ISAKMP - Giao thức Quản lý Khóa) để thỏa thuận một cách tích cực về một tập của các yêuc ầu bảo mật cho cả hai phía giữa các máy tính với nhau. Các máy tính không đòi hỏi phải có các chính sách giống hệt nhau, chúng chỉ cần các chính sách đã được cấu hình tùy chọn đã được thỏa thuận đẻ để thiết lập một tập chung các yêu cầu với bảo mật với máy tính kia.

* Lọc gói IP: Quá trình lọc này cho phép hay cấm các liên lạc cần thiết bằng cách chỉ định các khoảng địa chỉ IP, các giao thức, hay thậm chí cả những cổng của giao thức.
* Bảo mật lớp mạng: IPSec nằm tại lớp mạng, cung cấp cơ chế bảo mật một cách tự động, trong suốt cho các ứng dụng.
* Xác thực ngang hàng: IPSec xác nhận lại mã nhận dạng của máy tính đối tác trước khi có bất cứ một gói dữ liệu nào được chuyển. Việc xác thực đối tác IPSec trong Windows Server 2003 được dựa trên các khóa đã chia sẻ, các khóa công khai (ví dụ như các Giấy chứng nhận X509) hoặc Kerberos và Active Directory để được xác thực bằng Kerberos.
* Xác thực dữ liệu gốc: Việc xác thực nguồn dữ liệu gốc ngăn cản người dùng không đúng không can thiệp vào gói tin và khai báo họ là người gửi dữ liệu. Mỗi gói tin dữ liệu được bảo vệ bằng IPSec bao gồm một số số Kiểm Soát bằng mật mã trong định dạng của một giá trị băm có khóa, số Kiểm Soát bằng mật mã còn được biết đến dưới cái tên Intergrity Check Value (ICV - Giá tri kiểm soát tính nguyên vẹn) hay Hash-Based Message Authentication (HMAC - mã xác thực thông điệp được băm nhỏ).
* Tính nguyên vẹn của dữ liệu: Với việc sử dụng số kiểm soát mật mã, IP See bảo vệ dữ liệu đang vận chuyển không bị sửa đổi bởi các người dùng không được xác thực, hay không phát hiện được trong quá trình vận chuyển, đảm bảo chắc chắn rằng các dữ liệu các dữ liệu mà người nhận có được là chính xác các thông tin mà người gửi đã gửi cho mình. Các người sử dụng có ác tâm muốn thay đổi muốn thay đổi nội dung của gói tin phair cập nhật lại một cách chính xác số Kiểm Soát bằng mật mã, một điều gần như là không thể thực hiện được nếu không biềt được các khóa chia sẻ.
* Tính riêng tư của dữ liệu: Các gói dữ liệu khi được gửi là mã hóa bằng các kỹ thuật mã hóa khóa bí mật qui ước. Điều này làm cho dữ liệu trở nên riêng tư. Thậm chí ngay cả khi dữ liệu bị truy nhập và quan sát, kẻ truy nhập cũng chỉ nhìn thấy các dữ liệu đã được mã hóa. Neu không biết các khóa bí mật đã sử dụng thì các dữ liệu gốc vẫn là ẩn. Do khóa bí mật chỉ được chia sẻ giữa nguời gửi và người nhận, tính riêng tư của dữ liệu đảm bảo rằng chỉ người nhận đã định trước của gói tin là có thể giải mã và trình bày được gói tin.
* Tính không lặp: Bằng cách sử dụng số thứ tụ trên trên mỗi gói tin đã được bảo vệ gửi giữa các đối tác có sử dụng IPSec, dữ liệu được trao đổi giữa các đối tác không thể bị lại để thiết lập các quan hệ bảo mật khác hay nhận được sự truy cập không xác thực đến các thông tin hay tài nguyên.
* Quản lý khóa: Việc xác thực nguồn gốc dữ liệu, tính nguyên vẹn, tính riêng tư hoàn toàn phụ thuộc vào các thông tin được chia sẻ của khóa bí mật. Nếu khóa bí mật bị tổn thương, liên lạc sẽ không còn là bảo mật nữa. Để giữ các khóa không bị các người sử dụng có ác tâm phát hiện IPSec cung cấp một phương thức an toàn cho việc trao đổi thông tin khóa để nhận được khóa bảo mật chia sẻ và thay đổi khóa một cách định ký cho các liên lạc càn bảo mật.

1. Các tính năng mói của IPSec trong Windows Server 2003

IPSec được tích hợp và có thể sử dụng để bảo mật các cuộc liên lạc mạng trong Windows 2000, Windows XP Professonal, và Windows Server 2003. IPSec hợp lệnh dành cho các máy khách cũng có cho hệ điều hành Microsoft Windows NT 4.0 Microsoft Windows 98, Microsoft Windows Millennium Edition (me). (Bạn có thể tải phần mềm IPSec máy khách từ địa chỉ:

Http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/l2tpclient.asp

Các tính năng mới của IPSec trong Windows Server 2003 bao gồm:

* Snap-in IP Security Monitor (Trình Theo dõi Bảo mật IP) được cải tiến từ công cụ IPSecMon có trong Windows 200 (Snap-in này là mới trong Windows XP Proesional và Windows Serever 2003).
* Khóa chủ mã hóa mạnh hơn, việc trao đổi khóa Diffie-Hellman 2048- bit được sử dụng.
* Công cụ quản lý dạng dòng lệnh Netsh cung cấp tính tiện ích, có thêm nhiều khả năng cấu hình không có tại Snap-in IP Security Policy Management trong phiên bản Windows 2000.
* Việc khởi động các máy tính được bảo mật. Nếu máy tính được cấu hình sử dụng các chế độ kết nối trạng thái bảo (Stateful), các thông tin đi vào mà được gửi để đáp lại các thông tin máy tính gửi ra sẽ được chấp nhận, như các lưu thông chiều vào đáp ứng được các tiêu chí lọc mà chúng ta đã cấu hình, cũng giống như các lưu thông DHCP. Tất cả các thông tin chiều vào khác (bao gồm các gói tin có địa chỉ, quảng bá hay quảng bá có địa chỉ) đều bị loại bỏ. Các thông tin chiều vào ở chế độ kết nối trạng thái cho phép các bộ lọc được hủy bó sau khi dịch vụ IPSec khởi động và thiết lập chính sách IPSec cố định.
* Chính sách IPSec cố định sẽ được áp dụng trong trường hợp chính sách cục bộ hay chính sách Active Directory không được áp dụng.
* Chỉ các thông tin miền IKE là được miễn trừ khỏi các thiết lập của bộ lọc. Sự miễn trừ này là cần thiết trong việc thiết lập mối liên lạc bảo mật.
* Có những hạn chế nhất định sẽ được xác định với những máy tính được phép kết nối dựa trên Miền, trên nguồn gốc Giấy chứng nhận, hay trên nhóm máy tính.
* Tên của Certìicate Authority (CA), sẽ có thể không bao gồm trong các yêu cầu giấy chứng nhận để tránh việc phát hiện các thông tin trong quan hệ tin cậy của máy tính như Miền, CA và công ty.
* Các cách cung cấp địa chỉ IP một cách logic sẽ được áp dụng cho việc cấu hình IP cục bộ - như máy như máy chủ DHCP, Domain Name system (DNS), và Windows Internet Naming Service (Wins).
* IPSec hoạt động trên NAT cho phép các gói ESP đi qua NAT (với các trạm NAT cho phép các lưu thông UDP đi qua).
* Tính năng tích hợp YỚi Network Load Balancing - NBL (Cân bằng tải mạng) được cải thiện, đem lại các lợi ích cho việc cân bằng tải của dịch vụ VPN dựa trên IPSec.
* Sự hỗ trợ đựoc cung cấp cho Snap-in RSoP giúp ta có thể xem được các thiết lập trong chính sách IPSec.

Các giao thức IPSec cung cấp sự bảo mật dựa trên việc sử dụng kết hợp các giao thức, trong đó có giao thức AH và giao thức ESP. Các giao thức này được sử dụng độc lập hay cái trước cái sau còn phụ thuộc vào các yêu cầu của việc giữ tính riêng tư và xác thực.

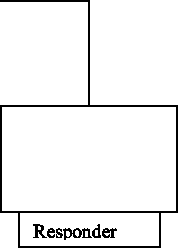
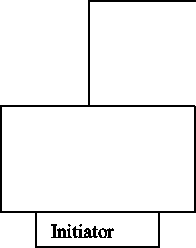
1. Giao thức AH cung cấp tính xác thực, nguyên vẹn và không lặp cho toàn bộ gói tin (gồm cả phần tiêu đề của IP và các giữ liệu được chuyển trong toàn bộ gói tin). Nó không cung cấp tính riêng tư, có nghĩa là nó không mã hóa dữ liệu. Dữ liệu vẫn có thể đọc được, nhưng chúng được bảo vệ chống lại việc thay đổi. Giao thức AH sử dụng các thuật toán Keyed hash để đánh dấu gói dữ liệu nhằm đảm bảo tính toàn vẹn của nó.
2. Giao thức ESP cung cấp tính riêng tư (thêm vào cho tính xác thực, toàn vẹn và không lặp) cho dữ liệu (IP Payload). ESP trong trạng thái vận chuyển sẽ không đánh dấu lại toàn bộ gói tin. Chỉ các thân gói tin IP (IP Payload) - không phải là IP Header - là được bào vệ. ESP có thể được sử dụng độc lập hay kết hợp với AH. Ví dụ, khi sử dụng kết hợp với AH, các gói IP Payload được gửi từ máy tính A đến máy tính B được mã hóa và đánh dấu để đảm bảo tính nguyên vẹn. Khi nhận được, phàn dữ liệu được tmyền sẽ được giải mã sau khi quá trình xác nhận tính xác nhận tính toàn vẹn được thực hiện thành công. Và người nhận có thể biết chắc chắn rằng ai đã gửi gói dữ liệu, dữ liệu không bị thay đổi và không ai khác có thể đọc được chúng.

Il.Các phương thức, dịch yụ, và trình điều khiển IPSec

Il.l.Phương thức

Bạn có thể cấu hình IPSec sử dụng một trong hai phương pháp sau:

II. 1.1.Phương thức Vận chuyển (Transport Mode): Bạn sẽ sử dụng bảo mật điểm-tới-điểm. Cả hai trạm cần hỗ trợ IPSec sử dụng cùng giao thức xác thực, bắt buộc phải sử dụng các bộ lọc IP tương thích và không đi qua một giao tiếp NAT nào. Liên lạc đi qua giao tiếp NAT nào. Liên lạc đi qua giao tiếp NAT sẽ đổi chỉ IP trên phần tiêu đề và làm mất hiệu lực của ICV ( Giá trị Kiểm Soát tính Nguyên vẹn). Hình 6-1 chỉ ra một ví dụ của Transport Mode.

Protected communications

Router

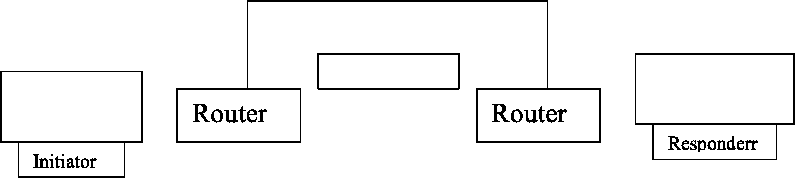
Router

Hình vẽ : Bảo vệ Điểm tới Điểm trong Transport mode

1. Tunel Mode (Phương thức Đường hầm): Bạn sử dụng Tunel Mode

trong trường hợp bạn cần kết nối Site-to-Site thông qua Internet (hay các mạng công cộng khác). Tunel Mode cung cấp sự bảo vệ Gateway-to- Gateway (cửa-đến-cửa). hình 6-2 mô tả một ví dụ của phương thức này.

Protected Communications



Hình vẽ : Bảo vệ Gate-to-gateway trong tunnel mode

II.1.3.Security Associations (Sự Liên kết Bảo mật)

Sự Liên kết Bảo mật (SA) là một tập hợp của các dịch vụ bảo mật, các cơ chế bảo vệ, và các khóa mã đuợc các thông tin càn thiết để xác định các lưu thông sẽ đuợc bảo mật như thế nào (các dịch vụ bảo mật và cơ chế bảo vệ) và với khóa bảo mật nào (Khóa mã hóa). Có hai loại SA sẽ được tạo ra khi các cặp máy tính sử dụng IPSec trao đổi với nhau trong trạng thái bảo mật: SA ISAKMP và SA IPSec.

• SA IASKMP

SA IPSKMP, còn đuợc gọi là SA Phương thức Chính (Main Mode SA) đuợc sử dụng để bảo vệ các thỏa thuận bảo mật IPSec. SA ISAKMP được tạo ra bằng việc thỏa thuận một bộ mật mã (một tập họp các thuật toán mã hóa được sử dụng để mã hóa dữ liệu), mà sẽ được sử dụng để bảo vệ các lưu thông ISPKMP trong tuơng lai, trao đổi chất liệu tạo khóa, sau đó sẽ xác nhận và xác thực từng đối tương IPSec. SA trong vòng CSDL Liên kết Bảo mật ( Security Association Database - SADB). Khi quá trình tạo SA ISAKMP kết

thúc, tất cả các thỏa thuận SA trong tuơng lai cho cả hai loại SA đều đươc bảo vệ. Đó chính là một khi một khía cạnh của việc liên lạc bảo mật được biết đến với tên Thỏa thuận bộ Mã hóa Được bảo vệ (Protected Ciphersuite negotiation). Với cơ chế này, không chỉ các dữ liệu được bảo vệ mà cả xác định các thuật toán bảo mật đã được thỏa thuận giữa các đối tác IPSec cũng được bảo vệ. Để phá vỡ việc bảo vệ IPSec, các người dùng ác ý trước hết phải xác định được bộ mật mã bảo vệ dữ liệu, mà bộ mật mã này lại đưa ra rào cản khác. Đối với IPSec, chỉ có một ngoại lệ để hoàn thành việc thỏa thuận bộ mật mã được bảo vệ là tiến thành thỏa thuận về bộ mật mã với SA ISAKMP ban đẩu, được gửi dưới dạng văn bản tường minh.

• SAIPSec

SA IPSec, còn được gọi là SA Phương thức Nhanh (Quick Mode SA),

Được sử dụng để bảo vệ các dữ liệu đuợc gửi giữa các đối tác IPSec. Việc thỏa thuận bộ mật mã SA IPSec được SA ISAKMP bảo vệ. Không một thông tin nào về lưu thông hay cơ chế bảo vệ được gửi dưới dạng văn bản tường minh. Với mỗi cặp đối tác IPSec, hai kiểu SA IPSec luôn tồn tại cho mỗi giao thức được thỏa thuận cho các lưu thông chiều vào (inbound), một cho các lưu thông chiều ra (Out bound). SA chiều vào của một đối tác IPSec này sẽ là SAchiều ra của đối tác IPSec kía.

II.1.4.Chỉ mục các Thông số Bảo Mật (Sercurity Parameters Index -

SPI)

Với mỗi phiên IPSec, các đối tác IPSec bắt buộc phải làn theo dấu vết việc sử dụng của ba SA khác nhau: SA ISAKMP, SA IPSec chiều vào và SA IPSec chiều ra. Để nhận dạng một SA nhất định, người ta sử dụng một số ngẫu nhiên giả 32 bit, được gọi là Chỉ mục các Thông số Bảo mật (Securyti Parameters Index - SPI). SPI, là một trường trong tiêu đề của IPSec, chỉ ra SA mà đối tác đích sẽ dùng và được gửi cùng với từng gói dữ liệu. Đối tác nhận có trách nhiệm cung cấp một SPI duy nhất cho từng giao thức.

Đối tác khởi tạo một phiên IPSec được gọi là Người khởi tạo (Initiator). Đối tác có trách nhiệm yêu cầu thực hiện việc bảo vệ IPSec được gọi là Người đáp (Responder). Người khởi tạo sẽ chọn SPI của SA ISAKMP, và mỗi đối tác sẽ chọn SPI của SA IPSec dành cho các lưu thông chiểu ra của nó.

II.1.5.Trao đỗi Khóa Internet(Internet Key Exchange - IKE)

IKE là tiêu chuẩn xác định cơ chế thiết lập SA. IKE kết họp ISAKMP và giao thức Oakley Key Determination để tạo ra các chất liệu khóa bảo mật. Ọakley được xây dựng dựa trên thuật toán Trao đổi khóa Diffie - hellman(Diffĩe - Hellmen Key Exchange), cho phép hai đối tác IPSec xác định khóa bảo mật bằng cách trao đổi các giá trị không được mã hóa thông qua mạng công cộng.

Kết quả của quá trình trao đổi khóa Diffie-Hellman bằng cách trao đổi hai số qua mạng công cộng sẽ tạo ra khóa bảo mật mà chỉ riêng hai đối tác tham gia vào quá trinhd trao đổi được biết. Người dùng ác ý khio truy cập vào các gói tin trao đổi khóa có thể xem các số này, nhưng họ sẽ không thực hiện dược cùng một phép tính như các đối tác tham gia thỏa thuận đã thực hiện để nhận được khóa bảo mật chia sẻ.

Quá trình trao đổi khóa Diffie -Heilman không ngăn cản các vụ tấn công ngang đường, trong đó người sử dụng ác ý đứng giữa hai đối tác IPSec sẽ thực hiện hai quá trình trao đổi khóa Diffie-Hellman, mỗi quá trình với một đối tác IPsec. Sau khi đã hoàn thành cả hai quá trình trao đổi khóa nói trên, người dùng ác ý sẽ cá các khóa bảo mật để liên lạc với cả hai đối tác. Để tránh các cuộc tấn công như vậy , IPsec trong Windows Server 2003 thực hiện việc xác thực ngay sau khi quá trình trao đổi khóa kết thúc. Trong trường họp đối tác IPsec không thể thực hiện việc xác thực một cách chính xác, thỏa thuận bảo mật sẽ bị loại bỏ trước khi có bất cứ một dữ liệu nào được gửi đi.

IPSec trong Window Server 2003 cũng hỗ ừợ cơ chế tạo lại khóa tự động (Dynamic Rekeying), sẽ xác định các chất liệu tạo khóa mới thông qua một trao đổi Diffie-Hellman mới. Cơ chế tạo lại khóa tự động dựa trên thời gian

đã trôi qua (mặc định là 480 phút hay 8 giờ ) hoặc dựa trên số các phiên trao đổi dữ liệu với cùng một tập các chất liệu tạo khóa(Mặc định, số này là không giới hạn).

THÔNG TIN THÊM: Quá trình thỏa thuận IKE Để có thêm thông tin về quá trình thỏa thuận IKE, xem RFC 2409 “The Internet Key Exchange (IKE)” tại địa chỉ http ://[www.ietf.or](http://www.ietf.or) g/rfc/rfc2409.txt

1. Dịch vụ IPSec Policy Agent

Mục đích của IPSec Policy Agent (Đại lý Chính sách IPSec) là dùng để phục hồi lại các thông tin chính sách vàchuyền chúng cho các cấu thành IPSec khác có thể yêu cầu các thông tin này để thực hiện các dịch vụ bảo mật.

IPSec Policy Agent là một dịch vụ tồn tại trong máy vi tính chạy hệ điều hành Windows Server 2003, xuất hiện nhưlà một dịch vụ IPSec trong danh sách các dịch vụ hệ thống tại bảng điều khiển Services, IPSec Policy Agent sẽ thực hiện một số chức năng trong hệ điều hành bao gồm:

1. Phục hồi các chính sách IPSec thích hợp (nếu chúng đã được gắn) từ Active Directory (như chỉ ra trong hình 6-3) nếu máy tính là thành viên của Miền, hoặc từ số dăng ký (registry) nếu máy tính không phải là thành viên của Miền.
2. Thu nhập các thay đổi trong việc cấu hình chính sách. Gửi các thông tin chính sách IPSec đến trình điều khiển IPSec.
3. Nếu máy tính là thành viên của miền, quá trình phục hồi chính sách sẽ bắt đầu khi hệ thống khởi động, với khoảng đã xác định trong chính sách IPSec, và tại khoảng thời gian thu thập đăng nhập Windows mặc định. Bạn cũng có thể thu thập các thông tin thay đổi cấu hình chính sách IPSec trong Active Directory một cách thủ công nhờ việc thực hiện lệnh Update/target:tênmáytính.

Sau đây là các khía cạnh khác của hành vi chính sách IPSec dành cho các máy tính thành viên của Miền:

1. Neu các thông tin chính sách IPSec cho các máy tính là thành viên Miền là đuợc cấu hình tập trung, các thông tin chính sách được lưu trong Active Directory và lưu tạm trong Registry cục bộ của máy tính sẽ được áp dụng chính sách.
2. Neu máy tính tạm thời không kết nối tới Miền và chính sách đã lưu tạm, các thông tin chính sách mới dành cho máy tính đó sẽ thay thế cho các thông tin chính sách cũ đang được lưu tạm khi máy tính được kết nối lại tới Miền.
3. Nếu máy tính là máy tính độc lập hay là thành viên của Miền không sử dụng Active Directory để lưu chính sách, Chính sách IP See được lưu trong Registry cục bộ.
4. Nếu không có các chính sách IPSec trong Active Directory hay trong Registry khi IPSec Policy Agent khởi động một cách tự động tại thời điển khởi động, hay IPSec Policy Agent không thể kết nối Active Directory, IPSec Policy Agent sẽ đợi cho đến khi chính sách được gán hay kích hoạt.
5. Trình điều khiển IPSec

Trình điều khiển IPSec nhận danh sách bộ lọc IP tích cực từ IPSec Policy Agent, như chỉ ra trong hình 6-4. Đại lý Chính sách sau đó sẽ kiểm tra sự phù hợp của mỗi gói thông tin chiều ra cũng như chiều vào so với danh sách trong bộ lọc. Bộ lọc IP cho phép quản trị mạng xác định một cách chính xác các lưu thông IP nào là bảo mật. Mỗi danh sách bộ lọc IP bao gồm một hay nhiều bộ lọc, xác định địa chỉ IP và kiểu lưu thông. Một danh sách bộ lọc IP có thể được sử dụng trong nhiều kịch bản liên lạc. Bạn có thể truy cập các bộ lọc IP bằng cách sử dụng Snap-in IP Security Policy management để truy cập các danh sách bộ lọc IP, trong Snap-in IP Security Pocily management, nhấn chuột phải vào điểm IP security Policy, sau đó nhấn Manage IP Filter Lists And Filter Actions.

Khi gói tin phù hợp với bộ lọc, nó sẽ áp dụng các hành vi bộ lọc tương ứng. Khi gói tin không phù hợp bất cứ bộ lọc nào, nó sẽ được chuyển ngược lại cho trình điều khiển TCP/IP để được nhận hay truyền mà không có sự thay đổi nào.

Neu hành động của bộ lọc cho phép truyền, gói tin sẽ được nhận hay truyền mà không bị thay đổi. Neu hành động của bộ lọc là khóa truyền dẫn, gói tin sẽ bị vô hiệu hóa. Nếu hành động của bộ lọc yêu cầu thỏa thuận về bảo mật, SA phương thức chính và phương thức nhanh sẽ được thỏa thuận.

Các khóa và SA phương thức nhanh đã được thỏa thuận được sử dụng với cả các lưu thông chiều ra và chiều vào. Trình điều khiển IPSec lưu thông toàn bộ các SA phương thức nhanhtrong CSDL. Trình điều khiển IPSec sử dụng trường SPI để kiểm tra sự phù hợp của SA với các gói tin.

Khi một gói tin chiều ra thỏa mãn các điều kiện của danh sách bộ lọc IP với hành động thỏa thuận bảo mật, trình điều khiển IPSec sẽ xếp gói tin vào hàng đợi và quá trình IKE bắt đàu tiến hành thỏa thuận bảo mật với địa chỉ IP đích của gói tin.

Sau khi việc thỏa thuận bảo mật được hoàn tất, trình diều khiển IPSec trên máy tính gửi sẽ thực hiện các hành động sau:

1. Trình điều khiển IPSec nhận SA có chứa khóa phiên từ quá trình

IKE.

1. Trình điều khiển IPSec định vị SA chiều ra trong CSDL của nó và chèn SPI lấy từ SA vào tiêu đề (header).
2. Trình điều khiển IPSec ký vào gói tin và mã hóa chúng nếu tính riêng tư được yêu càu.
3. Trình điều khiển IPSec gửi gói tin đến lớp IP để truyền chúng đến máy tính đích.

Trong trường hợp việc thỏa thuận thất bại, trình điều khiển IPSec sẽ triệt tiêu gói tin.

Khi một gói tin được bảo mật IPSec chiều vào thỏa mãn các điều kiện của bộ lọc trong danh sách các bộ lọc IP, trình điều khiển IPSec sẽ thực hiện các hành động sau:

1. Trình điều khiển IPSec nhận khóa phiên, SA, SPI từ quá trình IKE.
2. Trình điều khiển IPSec định vị SA chiều vào trong CSDL bằng cách sử dụng địa chỉ đích và SPI.
3. Trình điều khiển IPSec kiểm tra chữ ký và nếu cần thiết giải mã gói tin.
4. Trình điều khiển IPSec tìm các gói tin IP thõa mãn bộ lọc trong danh sách bộ lọc để chắc chắn rằng không chấp nhận trong quá trình thỏa thuận.
5. Trình điều khiển IPSec gửi gói tin đến trình điều khiển TCP/IP để chuyển cho các ứng dụng nhận.

Khi nhận được một gói tin không được bảo mật, Trình điều khiển IPSec tìm kiếm điều kiện lọc thõa mãn trong danh sách bộ lọc. Nếu việc tìm kiếm là thành công và hành động lọc của bộ lọc đó là yêu càu bảo mật IP hay khóa gói tin, gói tin sẽ bị triệt tiêu.

1. Quá trình thỏa thuận bảo mật

Quá trình xử lý IPSec có thể được chia thành hai loại thỏa thuận : Thỏa thuận phương thức chính và thỏa thuận phương thức nhanh.

Ta có thể lấy một ví dụ:

1. Trạm A yêu càu liên lạc bảo mật.
2. Việc thỏa thuận theo phương thức chính được bắt đầu và hoàn tất (Khóa chủ - Master Key - Và SA IKE được thiết lập - xem phần “Thỏa thuận Phương thức Chính”).
3. Việc thỏa thuận phương thức nhanh của cặp SA (chiều vào và chiều ra) cho việc tmyền gói tin ứng dụng hoàn tất.
4. Các gói tin ứng dụng từ trạm A được trình điều khiển TCP/IP chuyển cho trình điều khiển IPSec.
5. trình điều khiển IPSec định dạng và mã hóa gói tin, sau đó sử dụng SA chiều ra để gửi nó cho trạm B.
6. Các gói tin bảo mật được truyền trên mạng.
7. Trình điều khiển IPSec trên trạm B xử lý mật mã các gói tin đến trên SA chiều vào, định dạng chúng như các gói IP thông dụng, sau đó chuyển chúng cho trình điều khiển TCP/IP.
8. Trình đièu khiển TCP/IP chuyển các gói tin cho ứng dụng trên trạm B.

8

|  |  |  |
| --- | --- | --- |
| Host A |  | Host B 8 |
| 1 |  |  |

|  |  |  |
| --- | --- | --- |
|  | 2 |  |
| IKE |  | IKE |
| 3  TRANSPORT |  | TRANSPORT  3 |
| IPSec Driver |  | IPSec Driver |
| 4  NETWORK |  | NETWORK 7 |
| PHYSICAL |  | PHYSICAL |

5

Secured packets 6

Hình vẽ : Quá trình xử lý IPSec

III. 1.Thỏa thuận Phương thức Chính

Việc thỏa thuận phương thức Chính Ọkley được sử dụng để xác định chất liệu khóa mã hóa và phòng chống bảo mật để sử dụng trong các quá trình

bảo vệ các liên lạc phương thức Chính hay phương thức Nhanh. Việc thỏa thuận phương thức Chính có thể chi tiết như sau:

1. Gói tin liên lạc được gửi từ trạm A đến trạm B.
2. Trình điều khiển IPSec trên trạm A kiểm tra các danh sách bộ lọc IP chiều ra của nó và kết luận rằng các gói tin thỏa mãn bộ lọc và hành động của bộ lọc là Negotiate Security (Thỏa thuận bảo mật) - Các gói tin bắt buôvj phải bảo mật.
3. Trình điều khiển IPSec bắt đầu quá trinh thỏa thuận IKE.
4. Trạm A kiểm tra các thiết lập phương thức Chính trong các chính sách của nó để đề xuất với trạm B.
5. Trạm A gửi thông điệp IKE đàu tiên sử dụng ƯDP có địa chỉ cổng nguồn 500 và địa chỉ cổng đích 500.
6. Trạm B nhận thông điệp nói trên và có yêu càu thỏa thuận bảo mật, sau đó sử dụng các dịa chỉ IP nguồn và IP đích của gói tin để tìm kiếm trong bộ lọc IKE của riêng nó. Bộ lọc IKE cung cấp các yêu cầu bảo mật dành cho các liên lạc từ trạm A.
7. Nếu các thiết lập bảo mật do trạm A đề xuất được trạm B chấp nhận, việc thỏa thuận phương thức Chính hay SA IKE bắt đầu.
8. Hai máy tính sẽ thỏa thuận các tùy chọn, trao dổi các mã nhận dạng và xác thực chúng, và sinh ra Khóa chính (Master Key). SA IKE được thiết lập.

Tóm lại, việc thỏa thuận phương thức Chính tạo ra SA ISAKMP. Người khởi tạo và Ngụờỉ đáp trao đỏi hàng loạt thông điẹp ISAKMP để thỏa thuận về bộ mật mã dành cho SA ISAKMP (dưới dạng văn bản tường mình), trao đỏi các vật liệu xác định khóa, nhận dạng và xác thực lẫn nhau.

1. Thỏa thuận Phương thức Nhanh

Khi việc thoả thuận theo phương thức Chính hoàn tất, mỗi đối tác trong cặp IPSec đã hoàn thành việc lựa chọn một tập hợp nhất định các thuật toán mã hóa được dùng cho các thông điệp bảo mật phương thức Chính và phương thức Nhanh, đã trao đổi các thông tin khóa để nhận được khóa bảo mật chia sẻ, và đã thực hiện xong việc xác thực. Trước khi các dữ liệu bảo mật được gửi đi, việc thực hiện phương thức Nhanh nhất thiết phải được thực hiện nhằm xác định kiểu lưu thông sẽ được bảo mật và chúng sẽ được bảo mật như thế nào. Việc thỏa thuận phương thức Nhanh cũng được thực hiện khi SA phương thức Nhanh hết hạn.

Các thông điệp phương thức Nhanh là các thông điệp ISAKMP đã được mã hóa bằng việc sử dụng SA ISAKMP. Kết quả của việc thỏa thuận theo phương thức Nhanh là hai SA IPSec: Một dành cho các thông tin chiều đi và một dành cho các thông tin chiểu đến. Quá trình thỏa thuận được tiến hành như sau:

1. Trạm A thực hiện việc tìm kiếm chính sách của phương thức IKE nhằm xác định toàn bộ các chính sách đã có.
2. Trạm A đưa ra các đề nghị về các lựa chọn của nó (mật mã, cũng như tần suất của việc thay đổi khóa,w...) và về các bộ lọc cho trạm B.
3. Trạm B thực hiện việc tìm kiếm chính sách của phương thức IKE của chính nó, nếu kết quả tìm được là thỏa mãn các đề xuất của trạm A, nó hoàn tất việc thỏa thuận phương thức Nhanh để tạo ra cặp SA IPSec.
4. Một SA sẽ được dành cho chiều đi và một SA sẽ được dành cho chiều đến. Mối SA sẽ được nhận dạng nhờ SPI, và SPI là một phần trong tiêu đề của mỗi gói tin được gửi đi.
5. Trình điều khiển IPSec chuyển các gói tin cho trình điều khiển của Card mạng.
6. Trình điều khiển Card mạng đưa ra các khung dữ liệu lên mạng.
7. Card mạng tại trạm B nhận các gói tin đã mã hóa.
8. Trạm B sử dụng SPI để tìm ra SA tương ứng. (SA này có chứa khóa mã hóa tương ứng cần thiết để giả mã và xử lý gói dữ liệu).
9. Nếu Card mạng được thiết kế đặc biệt để mã hóa - và do đó có thể giải mã các gói tin, nó sẽ thực hiện công việc này. Sau đó, nó chuyển các gói tin cho trình điều khiển IPSec.
10. Trình điều khiển IPSec tại trạm B sử dụng SA chiều đến để phục hồi lại các khóa và xử lý các gói tin nếu cần.

11 .Trình điều khiển IPSec chuyển đổi các gói tin quay trở lại định dạng của các gói tin IP thông thường và chuyển chúng cho trình điều khiển TCP/IP, và đến lượt chúng sẽ chuyển tiếp cho ứng dụng nhận

12.SA IPSec liên tục xử lý các gói tin, SA được làm mới bằng việc thỏa thuận phương thức Nhanh IKE trong suốt thời gian ứng dụng gửi và nhận dữ liệu. Khi SA không lam việc, chúng sẽ được xóa.

IKE phương thức chính không bị xóa khi không làm việc. Tuổi thọ của nó là 8h nhưng con số này là có thể thay đổi được (từ 5 phút tới tối đa là 48h). Trong phạm vi thời gian đã định này, các lưu thông mới sẽ chỉ kích hoạt, việc thỏa thuận phương thức Nhanh. Khi IKE phương thức Chính hết hạn, một phương thức IKE mới sẽ được thỏa thuận khi càn.

1. Tìm hiểu các chính sách bảo mât IPSec

Chính sách là các luật xác định mức độ bảo mật. thuật toán băm, thuật toán mã hóa, và độ dài của khóa được yêu cầu. Các luật này cũng xác định các địa chỉ, giao thức, tên DNS, mạng con mà kiểu kết nối mà các thiết lập bảo mật áp dụng.

Các chính sách IPSec có thể được cấu hình để đáp ứng được các yêu cầu về bảo mật của người dùng, nhóm, ứng dụng, miền, site, hay toàn bộ doanh nghiệp. Windos Server 2003 cung cấp Snap-in IP Security Policy

Management (Quản trị chính sách bảo mật IP) được dùng để tạo và quản trị các chính sách IPSec một cách cục bộ hay thông qua chính sách Nhóm (GP - Group Policy).

Các chính sách đã xác định trước được cung cấp cho cả hai loại cấu hình bảo mật cục bộ và nhóm. Chúng có thể được thay đổi để thỏa mãn các yêu cầu đặc biệt, hày bạn cũng có thể tạo mới hoàn toàn các chính sách. Một khi chính sách đã được xác định, để cho chúng có thể thực sự có tác dụng, bạn phải gán nó cho một đối tượng nào đó. Mặc định không có chính sách nào được gán sẵn.

rv.l. Gán các chính sách IPSec

Như đã thảo luận ở trên, chính sách IPSec được chuyển từ Policy Agent (Đại lý chính sách) sang cho trình điều khiển IPSec và xác định các thủ tục hoàn hảo cho tất cả các khía cạnh của giao thức - từ đâu, khi nào, và làm thế nào để bảo mật dữ liệu YỚi các phương pháp bảo mật được sử dụng, có thể có một vài chính sách được xác định, nhưng trong một thời điểm chỉ có một chính sách được gán cho máy tính mà thôi. Để gán chính sách, bạn có thể nhấn chuột phải vào IPSec Policy trong Local Security Policy hay trong bảng điều khiển Group Policy thích hợp, sau đó nhấn Assign.

Để có thể hiểu rõ hơn về các khả năng của chính sách, bạn bắt buộc phải biết về cấu thành của chính sách. Các cấu thành này bao gồm:

* Thiết lập đường hàm (Tunnel): Địa chỉ IP kết thúc đường hàm (Nếu sử dụng kỹ thuật đường hàm IPSec để bảo vệ các gói tin đến).
* Kiểu mạng: Kiểu kết nối bị chính sách IPSec tác dụng: tất cả các kết nối, LAN, hay truy cập từ xa.

o Bộ lọc IP: tập con của lưu thông mạng dựa trên địa chỉ IP, cổng, và giao thức vận chuyển. Nó thông báo cho trình điều khiển IPSec các lưu thông chiều ra hay chiều vào nào là được bảo mật.

* Danh sách bộ lọc IP: Tập họp của một hay nhiều bộ lọc IP, xác định dãy của các lưu thông mạng.
* Hành động của bộ lọc: Trình điều khiển IPSec sẽ bảo mật lưu thông mạng như thế nào. Các hành động của bộ lọc được xác định trước bao gồm: Permit (cho phép), Request Security (Optional) (đề nghị bảo mật - tùy chọn), và Require Security (yêu cầu bảo mật).
* Phương thức xác thực: Một trong các thuật toán bảo mật và kiểu được sử dụng cho việc xác thực và trao đổi khóa.

o Kerberos

o Certigicates (giấy chứng nhận) o Preshared key (Khóa chia sẻ trước)

Các chính sách bảo mật của IPSec mặc định

Bạn tạo cấu hình các chính sách IPSec cục bộ bằng cách sử dụng tính năng IP Security Policies On Local Computer (các chính sách Bảo mật IP trên máy tính cục bộ), như được chỉ ra trên hình 6-6. (Để truy nhập snap-in này, tham khảo bài tập 6-2, “cấu hình IPSec để sử dụng Giấy chứng nhận”, từ bước 1 đến bước 7).

Sử dụng chính sách client (Respond Only) (máy tram - Chỉ Đáp) trên các máy tính thông thường không gửi các dữ liệu được bảo mật. Chính sách này không khởi tạo các liên lạc bảo mật. Neu máy chủ yêu cầu bảo mật, máy hạm sẽ đáp ứng và bảo mật chỉ các lưu thông với cổng và giao thức được yêu cầu với máy chủ đó.

Chính sách Server (Request Security) (máy chủ - đề xuất bảo mật) có thể được sử dụng trên bất cứ máy tính nào - máy trạm hay máy chủ - càn thiết khởi tạo các liên lạc bảo mật. Không giống như chính sách máy trạm, chính sách máy chủ sẽ bảo vệ tất cả các tmyền thông chiều ra. Các truyền thông chiều vào, không bảo mật cũng được chấp nhận. Mặc dù vậy chúng sẽ không được xử lý cho đến khi nhận được các đề xuất bảo mật IPSec từ máy gửi cho tất cả các gói tin đã truyền. Chính sách này yêu cầu sử dụng giao thức bảo mật Kerberos

Chính sách chặt chẽ nhất trong các chính sách bảo mật xác định trước, chính sách Secure Server ( Requừe Security) (Máy chủ Bảo mật - yêu cầu bảo mật) không gửi hay chấp nhận các truyền thông không bảo mật. Các máy trạm muốn liên lạc YỚi máy chủ bảo mật bắt buộc phải sử dụng ít nhất Chính sách Máy chủ xác định trước hay tương đương, Giống như Chính sách Máy chủ, Chính sách Máy chủ Bảo mật sử dụng xác thực Kerberos rv.2. Luật đáp mặc định

Luật đáp mặc định, được kích hoạt một cách mặc định cho tất cả các chính sách, được sử dụng để đảm bảo rằng máy tính sẽ đáp ứng các yêu cầu của các liên lạc bảo mật. Nếu chính sách hiện hành không có luật xác định cho máy tính sẽ đề xuất liên lạc bảo mật, luật Đáp mặc định sẽ được áp dụng và bảo mật sẽ được thỏa thuận. Ví dụ, khi máy tính A liên lạc một cách bảo mật với máy tính B và máy tính B không có bộ lọc thông tin chiều vào dành cho máy tính A, luật Đáp mặc định sẽ được áp dụng.

Các phương thức bảo mật và phương thức xác thực có thể được cấu hình cho Luật Đáp mặc định. Sử dụng Snap-in IP Security Policy Management để thay đổi luật đáp mặc định. (Để tạo bảng điều khiển có chứa Snap-in IP Security Policy Managemen, tham khảo bài tập 6-2, “cấu hình IPSec để sử dụng Giấy chứng nhận”, từ bước 1 đến bước 7).

> Truy nhập và Thay đổi Phương thức Bảo mật của Hành đông Bô loc

1. Mở hay tạo bảng điều khiển có chứa Snap-in IP Security policy Managemen
2. Trên cấu trúc hình cây của bảng điều khiển, nhấn chuột vào vị trí có chứa chính sách bạn muốn thay đổi.
3. Trong khung Chi tiết, nhấn đúp chuột và Chính sách bạn muốn thay đổi.
4. Trong thẻ Rules, tại hộp IP Security Rules chọn luật bạn muốn thay đổi, và nhấn Edit.
5. Trong Filter Action, chọn Hành động Bộ lọc bạn muốn thay đổi, và nhấn Edit.
6. Trong thẻ Security Methods, thêm, thay đổi, ghi lại, hay loại gỏ phương thức bảo mật

Luật đáp mặc định có các đặc tính sau:

* IP Filter List of <Dynamic>: Chỉ ra rằng danh sách bộ lọc là chưa được cấu hình, nhưng các bộ lọc đã được tạo một cách tự động trên cơ sở nhận được các gói thỏa thuận IKE.
* Filter Action of Default Response (Hành động bộ lọc của Luật Đáp mặc định): Bạn có thể xem và thay đổi Hành động của Bộ lọc của sách tương ứng trong Snap-in IP Security Policy Management. Hành động của bộ lọc của Luật đáp mặc định chỉ ra các hành động của bộ lọc của bộ lọc (Permit - Cho phép, Block - Khóa, hay Negotiate Security - Thỏa thuận Bảo mật) là không thể cấu hình được. Negotiate Security sẽ được sử dụng.

Mặc dù vậy bạn vẫn có thể cấu hình các tham số sau:

* Các phương thức bảo mật và thứ tự áp dụng của chúng trong thẻ Security methods.
* Các phương thức xác thực và thứ tự áp dụng của chúng trong thẻ Authentication Methods.

> Thêm thiết lập chính sách

Khi bạn chọn Snap-in IP Security Policy Management để thêm vào bảng điều khiển, bạn sẽ có bốn lựa chọn để quản trị các chính sách bảo mật:

* Local Computer: sử dụng tùy chọn này để quản trị các Chính sách bảo mật IP trên máy tính có chạy bảng điều khiển.
* The Active Directory Domain Of Which This Computer Is A Member (Mien Active Directory mà máy tính này là thành viên): Sử dụng tùy chọn này khi bạn muốn quản trị các chính sách áp dụng cho toàn bộ miền cục bộ.
* Another Active Directory Domain (Use The Full DNS Name Of IP Address) (Mien Active Directory khác - Sử dụng tên DNS đầy đủ hay địa chỉ IP): Sử dụng tùy chọn này khi bạn muốn quản trị các chính sách sẽ áp dụng trên toàn bộ một miền ở xa.
* Another Computer: Sử dụng tùy chọn này để quản trị các chính sách được lưu trữ cục bộ trên máy tính khác.

Để có thể quản trị các chính sách IPSec dựa trên Active Directory, bạn bắt buộc phải là thành viên của nhóm Domain Admin trong Active Directory, hoặc bạn càn có sự ủy quyền thích hợp.

1. Tạo hay mở bảng điều khiển có chứa Snap-in IP Sercurity Policy Management.
2. Trên cấu trúc hình cây của bảng điều khiển, nhấn IP Security Policies tại vị trí bạn muốn quản trị (máy tính cục bộ, miền Active Directory cục bộ hay miền Active Directory ở xa).
3. Trên thực đơn Action, nhấn Create IP Security Policy.
4. Trên trang Welcom to The IP Security Policy Wizard, nhấn Next.
5. Trên trang IP Security Policy Name, nhập tên cho Chính sách bảo mật IP mới. Nếu cần, bạn có thể cung cấp các mô tả sau đó nhấn Next.
6. Đe sử dụng Luật đáp mặc định, trên trang Requests Fỏ Secure Comunication. Kiểm tra xem Activate The Defaul Response Rule đã được lựa chọn và nhấn Next.
7. Trên trang Defaul Response Rule Authentication Method, chọn phương thức xác thực ban đầu cho luật bảo mật, cung cấp các thông tin thêm cho phương thức đã chọn, sau đó nhấn Next.
8. Trên trang Completing The Ip Security Policy Wizard, bỏ lựa chọn hộp Edit Properties, sau đó nhấn Finish.

* Thay đỗi thiết lập chính sách

Để thay đổi một chính sách đang tồn tại, nhấn đúp chuột vào chính sách bạn muốn thay đổi, chọn luật bạn muốn thay đổi và Edit.

* Dỡ bỏ thiết lập chính sách

Để dỡ bỏ thiết lập chính sách, nhấn chuột vào chính sách bạn muốn dỡ bỏ, và trên thực đơn Action, nhấn Delete.

CHƯƠNG IH: TRIỂN KHAI VÀ QUẢN TRỊ IPSEC

I.Triển khai và thưc thi IPSec

•

LI Triển khai các chính sách IPSec

Chính sách IPSEC có thể được triển khai bằng cách sử dụng các chính sách cục bộ, Active Dỉectory, hoặc cả hai. Mỗi phưong pháp đều có các điểm mành và yếu của riêng nó.

1. Triển khai IPSec sử dụng các Chính sách Cục bộ

Chỉ có một Đối tượng Chính sách Nhóm (GPO) cục bộ, thường được biết với tên Local Computer Policy (chính sách Máy tính Cục bộ), được lưu trên máy tính cục bộ. Khi sử dụng GPO cục bộ, bạn có thể lưu các thiết lập Chính sách Nhóm trên từng máy tính riêng mà không cần quan tâm đến việc chúng có phải là thành viên của mien Active Dỉectory hay không.

Trên một mạng không có mien Active Directory (mạng không có Máy chủ Điều khiển Miên Windows 2000 hay Windows Server 2003), các thiết lập GPO cục bộ xác định các hành vi IP Sec do chúng không bị các GPO khác ghi đè. GPO cục bộ có thể bị các GPO đã được gán cho Site, Miền, hay ou ghi đè trong môi trường Active Directory.

Các thiết lập chính sách IPSec cục bộ sẽ được thêm vào các chính sách cố định đã được cấu hình. Trong trường hợp chính sách IPSec dựa trên Active Dừectory đã được gán và máy tính kết nối tới miền Active Directory, các thiết lập của chính sách dựa trên Active Dữectory sẽ được áp dụng thay cho các chính sách IPSec cục bộ.

Bạn nên sử dụng Chính sách Cục bộ trong 2 kịch bản sau:

* Bạn không có sẵn nền tảng Active Directory, hoặc bạn chỉ có một số rất ít các máy tính cần sử dụng IPSec.
* Bạn không muốn tập trung hóa chiến lược IPSec trong cơ quan

1. Các Chính sách cố định (Persistent Policy)

Bạn có cấu hình các chính sách cố định để mở rộng các chính sách IPSec Cục bộ hay IPSec dựa trên Active Directory đã có, ghi đè lên các chính sách này, và tăng cường khả năng bảo mật trong quá trình máy tính khởi động. Các Chính sách cố định tăng cường khả năng bảo mật bằng cách cung cấp khả năng bảo mật trong thời gian quá độ từ khi máy tính khởi động cho đến khi các chính sách IPSec dựa trên Active Directery thực sự có tác dụng. Các Chính sách cố định, nếu được cấu hình, sẽ được lưu trong sổ đăng ký (Registry) cục bộ. Bạn có thể cập nhật Chính sách cố định bất cứ lúc nào, một khi dịch vụ IPSec vẫn chạy. Mặc dù vậy, các thay đổi trong Chính sách Cố định không được kích hoạt tức thời. Bạn cần khởi động lại dịch vụ IPSec để tải các thiết lập mới của Chính sách cố định.

Nếu bạn đã cấu hình các chính sách dựa trên Active Directory, bạn có thể sử dụng Chính sách cố định như là một công cụ để yêu cầu các lưu thông tới Active Dữectory luôn được bảo mật bằng IPSec dựa trên Active Directory. Khi các chính sách cục bộ hay việc dựa trên Avtive Directory được áp dụng, các thiết lập chính sách này sẽ được thêm vào các thiết lập chính sách cố định.

1. Triển khai IPSec sử dụng Active Derectory

Đe triển khai các chính sách IPSec sử dụng Active Directory, cần gán các chính sách IPSec cho GPO đích của Site, miền, hay ou. Việc gán các chính sách này cho GPO sẽ có hiệu quả đối YỚi tất cả các tài khoản máy tính nằm trong phạm vi ảnh hưởng của GPO đó.

Sử dụng bảng điều khiển IP Security Policy Management hay lệnh Netsh để quản trị chính sách dựa trên Active Directory. Bảng điều khiển IP Security Policy Management đã được thảo luận trong quá trình “Thêm Thiết Lập Chính sách”.

Chính sách dựa trên Active Directory luôn ghi đè lên bất cứ chính sách IPS cục bộ nào được gán và thêm vào chính sách IPSec cố định đang được IPSec Policy Agent (Đại lý chính sách IPSec) áp dụng, nếu chính sách cố định đã được cấu hình. Nếu có xung đột giữa chính sách IPSec cố định với hoặc chính sách miền hoặc chính sách cục bộ, các thiết lập chính sách cố định sẽ chiếm ưu thế.

Khi gán chính sách IPSec trong Active Directory, càn cân nhắc các điểm

sau:

* Chúng ta có thể gán danh sách của tất cả các chính sách IPSec tại bất cứ cấp nào trong cấu trúc Active Directory. Mặc dù vậy, chỉ một chính sách IPSec được gán tại một cấp nhất định của Active Directory.
* OƯ sẽ kế thừa chính sách của oư cha trừ trường hợp tính kế thừa bị khóa hay chính sách được gán một cách trực tiếp.
* Không thể gộp các chính sách IPSec từ các OƯ khác nhau.
* Chính sách IPSec được gán cho OƯ trong Active Directory có quyền ưu tiên cao hơn so với chính sách ở các mức miền đối với các thành viên của ou đó.
* Chính sách IPSec được gán cho ou mức thấp nhất trong cấu trúc Active Dữectory sẽ ghi dè lên chính sách IPSec được gán cho ou đó.
* Nên sử dụng việc gán chính sách cho cấp cao nhất có thể trong cấu trúc của Active Directory để giảm thiểu việc cấu hình và công tác quản trị cần thiết. Sử dụng Active Dừectory để triển khai chính sách nếu trong hể thống đáp ứng các tiêu chí:
* Có hạ tầng Active Directory.
* Người quản trị sử dụng một số lượng đáng kể các máy tính cần nhóm lại để gán IPSec.
* Muốn tập trung hóa chiến lược của hệ thống.

1. Triển khai trong môi trường hỗn họp

Bạn có thể triển khai IPSec trong môi trường có máy tính là thành viên của miền và sẽ nhận được chính sách IPSec thông qua chính sách nhóm Active Dỉectory, và các máy tính không phải thành viên của miền và sẽ nhận được chính sách IPSec thông qua Chính sách Nhóm cục bộ. Không phụ thuộc vào việc các máy tính cần liên lạc với nhau vẫn có thể thỏa thuận về các luật xác định trong các chính sách IPSec của chúng.

1. Thực thỉ IPSec sử dụng giấy chứng nhận

IPSec dựa vào sự xác thực lẫn nhau để cung cấp các liên lạc bảo mật. Do IPSec là một chuẩn công nghiệp, việc xác thực này có thể xẩy ra với các hệ thống không chia sẻ kết cấu hạ tầng xác thực thông qua giao thức Kerberos tập trung. Các giấy chứng nhận X.509 cung cấp một khả năng xác thực khác dành cho IPSec đã được chuẩn hóa và có thể sử dụng trong trường hợp có Public Key Infrastructure (PKI- Hạ tầng Khóa Công khai) tin cậy. Phần này mô tả cách bạn có thể sử dụng giấy chúng nhận khóa công khai để xác thực nhằm cung cấp các liên lạc và tin cậy trên mạng.

1. Giấy chứng nhận X.509

* Giấy chứng nhận X509, còn được gọi là chứng nhận số, là một dạng giấy ủy nhiệm điện tử được dùng rộng rãi trong việc xác thực và trao đổi các thông tin bảo mật trên các mạng mở, như Internet, mạng liên nghành (Extranet) hay mạng nội bộ (Intranet).

Giấy chứng nhận kết buộc một cách tin cậy khóa công khai với thực thể nắm giữ khóa riêng tương ứng. Ví dụ, bạn có thể mã hóa dữ liệu dành cho người nhận bằng khóa công khai của người nhận, và hoàn toàn tin chắc rắng chỉ có người nhận có khóa riêng cần thiết cần thiết mới giải mã được dữ liệu.

Người xuất bản giấy chứng nhận (Certifícate issuer), được gọi là Người Chúng nhân (Certifícate Authority -CA), sẽ đặt một dấu hiệu lên giấy chứng nhận. Giấy chứng nhận có thể được cấp cho người dùng, máy tính, hay dịch vụ, ví dụ như IPSec.

Giấy chứng nhận bao gồm các thông tin sau:

* Khóa mã hóa công khai từ cặp khóa riêng và công khai của chủ thể giấy chứng nhận.
* Thông tin về chủ thể yêu cầu giấy chứng nhận.
* Tên phân biệt X.500 của người dùng hay máy tính.
* Địa chỉ E-Mail của người sở hữu giấy chứng nhận.
* Chi tiết về CA.
* Ngày hết hạn .
* Giá trị băm của nội dung giấy chứng nhận nhằm đảm bảo tính xác thực (chữ ký số).

1. Vai Trò của CA

Neu bạn lựa chọn sử dụng giấy chứng nhận để xác thực, bạn cần lựa chọn CA, thường là CA gốc với máy tính chứng nhận đã cài đặt của bạn. Bạn không thể để trường Use Certifícate From This Certification Authority (CA) trống.

> Cấu hình IPSec Sử dụng giấy Chứng nhận.

Để tạo hình IPSec Sử dụng giấy Chứng nhận.

1. Tạo snap-in IP Security Management có chứa các chính sách bảo mật IP, hay mở file bảng điều khiển đã lưu có chứa các chính sách bảo mật IP.
2. Nhấn đúp chuột vào chính sách bạn muốn thay đổi.
3. Trong hộp thoại Edit Rule Propertis (ở đây Policy là tên của chính sách bảo mật IP), nhấn đúp chuột lên luật bảo mật IPSec bạn muốn thay đổi.
4. Trong hộp thoại Edit Rule Properties, trong thẻ Authentication Methods, nhấn Add, hoặc nếu cấu hình lại một phương thức đã có, chọn phương thức xác thực và nhấn Edit.
5. Chọn Use A Certificate From This Certificate Authority (CA), và nhấn Browse.
6. Trong hộp thư thoại Select Certificate, chọn CA thích hợp và nhấn OK.
7. Trong thẻ Authentication Method, nhấn OK.
8. Trong hộp thoại Edit Rule Properties, nhấn OK.
9. Trong hộp thư thoại Policy Properties, nhấn OK.

\* CÔNG CỤ HÕ TRỢ: Sử dụng NAT với IPSec

NAT là một quá trình dịch được sử dụng rộng rãi cho phép một mạng với các địa chỉ IP riêng có thể truy nhập thông tin trên Internet. Một kịch bản thường gặp các công ty chỉ có vài địa chỉ IP công cộng, có thể định tuyển được và phân phối các địa chỉ IP riêng cho các tài nguyên nội bộ của họ.

Việc chuyển đổi các địa chỉ, cổng TCP, hay cổng ƯDP trong NAT để kết nối người dùng với Internet làm mất hiệu lực của dịch vụ bảo mật IPSec. Đặc biệt, địa chỉ vả cổng được dịch sẽ gây ra các vấn đề sau cho các lưu thông IPSec dựa trên EPS.

* Với các gói tin được bảo vệ EPS, các cổng TCP và ƯDP là được mã hóa và do đó chúng không thể được dịch.
* Các thông điệp ISAKMP tính toán giá trị băm và các chữ ký dựa trên các thông tin SA, có chứa địa chỉ IP. Dịch địa chỉ IP sẽ làm mất hiệu lực của các giá trị băm hay chữ ký.

II.Quản trị và theo dõi IPSec

Windows Server 2003 cung cấp một vài công cụ để bạn có thể sử dụng để quản trị và theo dõi IPSec bao gồm: IP Security Monitor, RSoP, Event Viewer, nhật kí Oakley, Netsh, Netdiag.

**n.l.** Sử dụng IP Security Monitor (Trình theo dõi bảo mật IP)

Trong Windows 2000, IP Security Monitor được thực thi dưới dạng chương trình chạy (IPSecmon). Trong Windown Server 2003 và Windown XP, IP Security Monitor được thực thi dưới dạng một bảng điều khiển MMC, và bao gồm các tính năng cao cho phép bạn thực hiện các công việc sau :

* Theo dõi các thông tin IPSec tại máy tính cục bộ cũng như máy tính từ xa.
* Xem chi tiết về các chính sách IPSec đang hoạt động bao gồm tên,mô tả, ngày thay đổi cuối, lưu trữ đường dẫn, OƯ, và tên GPO.
* Xem các bộ lọc chung và riêng của phương thức chính và phương thức nhanh.
* Xem các thống kê về phương thức chính và phương thức nhanh (để nắm thông tin về các thông số thống kê được biểu diễn trên IP Security Monitor, xem các “thống kê phương thức chính và phương thức nhanh trong IP Security Monitor”)
* Xem các SA Phương thức chính và Phương thức Nhanh.
* Xem các chính sách IKE phương thức Chính.
* Xem các chính sách thỏa thuận Phương thức Nhanh.
* Tùy chỉnh tần suất làm mới, và sử dụng sự phân giả tên miền DNS cho bộ lọc và SA chiều ra.
* Tìm kiếm các bộ lọc Phương thức Chính và Phương thức Nhanh nhất định thoả mãn bất kỳ địa chỉ đi hay đến nào, địa chỉ IP đi hay đến trên máy tính cục bộ, hay địa chỉ IP đi hay đến nhất định nào đó.

n.1.1 Sử dụng IP Security Monitor để theo dõi lưu thông IPSec Nếu chính sách IPSec đã được kich hoạt, bạn có thể sử dụng IP Security Monitor để kiểm tra chính sách và các hoạt động của nó. Bạn chỉ có thể theo dõi IPSec chỉ trên các máy tính chạy hệ điều hành Windows XP hay Windows Server 2003. Để theo dõi IPSec trên máy tính chạy Windows 2000,

sử dụng lệnh IPSecmon tại dấu nhắc lệnh. Các thông tin bạn có thể nhận được bao gồm:

* Tên của chính sách IPSec hiện đang kích hoạt.
* Các chi tiết của chính sách đang kích hoạt.
* Các thông số thống kê Chế độ Nhanh.
* Các thông số thống kê Chế độ Chính
* Các thông số về các SA hiện hành.

1. Tìm hiểu các thông số thống kê Chế độ Chính và Chế độ Nhanh trong IP Security Monitor.

Việc xem các thông số thống kê có thể thực hiện rất đơn giản bằng cách mở rộng nút Server, tiếp tục mở rộng nút Main mode hay Quick mode sau đó chọn nút Statistics. Xong việc hiểu rõ ý nghĩa của từng thông số thì lại khó hơn nhiều. Bảng dưới đây mô tả các thông số thông dụng nhất của các thông số thông dụng nhất của các thông số thống kê của Chế độ Chính. Trong bảng, có một vài thông số thống kê có liên quan đến Chế độ Nhanh, mặc dù chúng có liên quan nhưng do chúng được khởi tạo trong quá trình thoả thuận IKE Chế độ Chính, do vậy, chúng được kể vào như là một ohàn của bảng các thông số thống kê Chế độ Chính.

> Bảng thông số Thống kê IPSec Chế độ Chính

|  |  |
| --- | --- |
| r  rill /\ A  Thông sô | Môtả |
| Active Acquire | Số lượng các yêu cầu đang chờ thoả thuận IKE cho các SA giữa các cặp IPSec. |
| Active Receive | Số lượng các thông điệp IEK trong hàng đợi xử  lý |
| Acquire  Failures | số lượng các yêu cầu chiều ra để thiết lập SA bị lỗi kể từ khi dịch vụ IPSec khởi động. |

|  |  |
| --- | --- |
| Receive  Failures | Số lượng các lỗi được tìm thấy trong các thông điệp IKE đã nhận kể từ khi dịch vụ IPSec khởi động lần cuối. |
| Send Failures | Số lượng các lỗi xẩy ra khi gửi IKE kể từ khi dịch vụ IPSec khởi động lần cuối. |
| Acquire Heap  Size | Số lượng các yêu cầu chiều ra để thiết lập SA thành công. |
| Receive Heap  Size | Số lượng các thông điệp có trong bộ đệm nhận  IKE |
| Authentication  Failures | Số các lỗi xác thực xẩy ra kể từ khi dịch vụ IPSec khởi động làn cuối. Trong trường hợp bạn không thể thiết lập kết nối IPSec, càn kiểm tra xem các lỗi xác thực có tăng lên trong quá trình kết nối hay không.  Nếu chúng tăng, lối xác thực chính là nguyên nhân của việc không thiết lập được kết nối IPSec . Kiểm tra các thông số bảo mật được chia sẻ là phù họp, các thành viên trong cặp IPSec là cùng một miền, và các giấy chứng nhận là đúng . |
| Negotiation  Failures | Số các thoả thuận Chế độ Chính bị lỗi kể từ khi dịch vụ IPSec khởi động làn cuối. Thực hiện kết nối và quan sát xem số lỗi thỏa thuận có tăng lên không. Nếu chúng tăng, kiểm tra các thông số thiết lập phương thức bảo mật và xác thực để phát hiện các cấu hình sai hoặc không phù họp. |
| Invalid Cookies Received | Tổng số các Cookies không phù họp với SA Chế độ Chính hiện tại kể từ khi dịch vụ IPSec khởi động lần cuối. Cookies là giá trị có chứa trong thông |

|  |  |
| --- | --- |
|  | diep IKE nhan dugc su dung de xac dinh SA che do Chinh phu hop. |
| Total Acquire | Tong so cac yeu cau da dugc chuyen toi cho IKE ke tir khi dich vu IPSec khoi dong lan cuoi nham thiet lap SA. So nay bao gom ca cac ket qua nhan dugc trong SA mem. |
| Total Acquire | Tong so cac yeu cau da dugc chuyen toi cho IKE ke tir khi dich vu khoi dong lan cuoi nham thiet lap SA. So nay bao gom ca cac ket qua nhan dugc trong SA phan mem. |
| Total Get SPI | Tong so cac yeu cau do IKE gui cho trinh dieu khien IKE nham nhan dugc SPI duy nhat ke tir khi dich vu IPSec dugc khoi dong lln culi. SPI phai phu hgp voi cac goi tin chilu din co chua SA. |
| Key Additions | Ting si cac SA Phuong thuc Nhanh chilu ra dugc IKE them vao trinh dilu khiln IPSec kl tir khi dich vu IPSec dugc khoi dong lan cuoi. |
| Key Updates | Ting si cac SA Phuong thuc Nhanh chilu vao dugc IKE them vao trinh dieu khien IPSec ke tir khi dich IPSec dugc khoi dong lln culi. |
| Get SPI Failures | Tong so cac yeu cau da dugc IKE chuyen toi trinh dilu khiln IPSec d! nhan dugc SPI duy nMt bi lli kl tir khi dich vu IPSec dugc khoi dong lln culi. |
| Key Addition Failures | Tong so cac yeu cau phu SA Phuong thuc Nhanh chieu ra do IKE chuyen toi trinh dieu khien IPSec bi loi ke tir khi dich vu IPSec khoi dong lan cuoi. |
| Key Update | Tong so cac yeu cau phu SA Phuong thuc |

|  |  |
| --- | --- |
| Failure | Nhanh chiều vào do IKE chuyển tới trình điều khiển IPSec bị lỗi kể từ khi IPSec khởi động lần cuối. |
| ISADB List  Size | Số lượng các mục vào trạng thái Phương thức Chính. Số này bao gồm các SA Phương thức Chính đã được thoả thuận thành công, các SA Phương thức Chính đang trong quá trình thỏa thuận, và các SA Phương thức Chính có tho ả thuận bị lỗi hay đã hết hạn nhưng chưa bị xoá. |
| Connection List  Size | Số các thỏa thuận Phương thức Nhanh đang trong quá trình thực hiện. |
| IKE Main Mode | Tổng số các SA thành công đã được tạo ra trong quá trình thỏa thuận Phương thức Chính kể từ khi dịch vụ IPSec được khởi động làn cuối. |
| IKE Quick Mode | Tổng số các SA thành công đã được tạo ra trong quá trinh thỏa thuận Phương thức Nhanh kể từ khi dịch vụ IPSec được khởi động làn cuối. |
| Soft  Associations | Tổng số các SA được thiết lập với các máy tính ko đáp ứng được các dự định thỏa thuận SA Phương thức Nhanh kể từ khi dịch vụ IPSec được khởi động lần cuối. Mặc dù các máy tính nói trên không đáp ứng được các dự định thỏa thuận Phương thức Chính nhưng chính sách IPSec vẫn cho phép liên lạc với các máy tính này. SA mềm không được bảo mật như IPSec. |
| Invalid Packets Received | Tổng số các thông điệp IKE không hợp lệ đã nhận được kể từ khi dịch vụ IPSec được khởi động lần cuối. Số này bao gồm các thông điệp IKE có trường Header không hợp lệ, có độ dài thân gói tin |

(Payload) không đúng, các giá trị Cookie đáp sai. Các thông điệp IKE không hợp lệ phần lớn do việc truyền lại các thông điệp IKE, hay do các khoá chia sẻ trước không phù họp giữa các thành viên trong cặp IPSec.

> Bảng các thông số thống kê IPSec Chế độ Nhanh

|  |  |
| --- | --- |
| JTT1 /V Ä  Thông sô | Môtả |
| Active Security Associations | Số lượng các SA Phương thức Nhanh. |
| Offloaded  Security Associations | Số lượng các SA Phương thức Nhanh sử dụng việc mã hoá phần cứng (Hardware Offload). Một số Card mạng có thể tự xử lý các dữ liệu mã hoá nhằm tằng cường hiệu năng chung. |
| Pending Key Operations | Số lượng các hoạt động trao đổi khoá đang được thực hiện. |
| Key Additions | Số lượng các khoá dành cho SA Phương thức Nhanh đã được thêm thành công kể từ khi máy tính khởi động. |
| Key Deletions | Số lượng các khóa dành cho SA Phuơng thức nhanh đã xoá thành công kể từ khi máy tính khởi động. |
| Rekeys | Số lượng các hoạt động làm mới khóa dành cho SA Phương thức Nhanh. |
| Active Tunnels | Số lượng các đường hầm đang hoạt động. |

|  |  |
| --- | --- |
| Bad SPI Packets | Số lượng các gói tin co SPI không dùng kể từ khi may tinh khởi động lần cuối. SPI co the het han hay cac goi tin vira den da qua cu. So nay se tang len neu viec lam mdi khoa la thudng xuyen va co rat nhieu cac SA. No cung co thl la bilu hien cua cac cuoc tin cong lira dao. |
| Packets Not Decrypted | Số lượng cac goi tin khong the giai ma ke tir khi may tinh khdi dong lan cuoi. Goi tin co the khong dugc giai ma nlu viec kilm tra danh gia no khong thanh cong. |
| Packets Not Authenticated | Số lượng cac goi tin ma cac du lieu cua no khong được kiểm chứng (viec kiểm chứng tính toàn vẹn cua goi tin khong thanh cong) kể từ khi may tinh được khởi dong lin cuối. Chi số nay tang co thể hiểu là biểu hiện cua viec tin cong lừa đảo hay thay đổi gói tin, no cung co the la bieu hien cua cac goi tin bi hỏng do các thiết bi mang gay ra. |
| Packets With Replay Detection | Số lượng cac goi tin co chua so thu tu sai ke tir khi may tinh khdi dong lin culi. Chi si nay tang co the la bieu hien cua cac cuoc tan cong lap lai hay cac true trac ve mang. |
| Confidential Bytes Sent | Số lượng cac Byte đã được gửi sử dung giao thuc ESP kể từ khi may tinh được khởi động lần cuối. |
| Confidential Bytes Received | Số lượng cac Byte da nhan dugc sir dung giao thuc ESP (khong tinh cac Byte ESP khong ma hoa) ke tir khi may tinh dugc khdi dong lan cuoi. |
| Authenticated Bytes Sent | So lugng cac Byte da được xac thuc được gửi sử dung giao thuc ESP hoac giao thuc AH ke từ khi may |

|  |  |
| --- | --- |
|  | tính được khởi động lần cuối. |
| Authenticated Bytes Received | Số lượng các Byte nhân được sử dụng phương thức vận chuyển IPSec kể từ khi máy tính được sử dụng lần cuối. |
| Bytes Sent In Tunnels | Số lượng các Byte được gửi sử dụng phương thức đường hầm IPSec kể từ khi máy tính được khổi động lần cuối. |
| Bytes Received In Tunnels | Số lượng các Byte nhận được sử dụng phương thức đường hầm IPSec kể từ khi máy tính được khởi động lần cuối. |
| Offloaded Bytes  Sent | Số lượng các Byte được gửi sử dụng phương thức mã hoá phần cứng kể từ khi máy tính được khởi động lần cuối. |
| Offloaded Bytes Received | Số lượng các Byte nhận được sử dụng phương thức mã hoá phần cứng kể từ khi máy tính được khởi động lần cuối. |

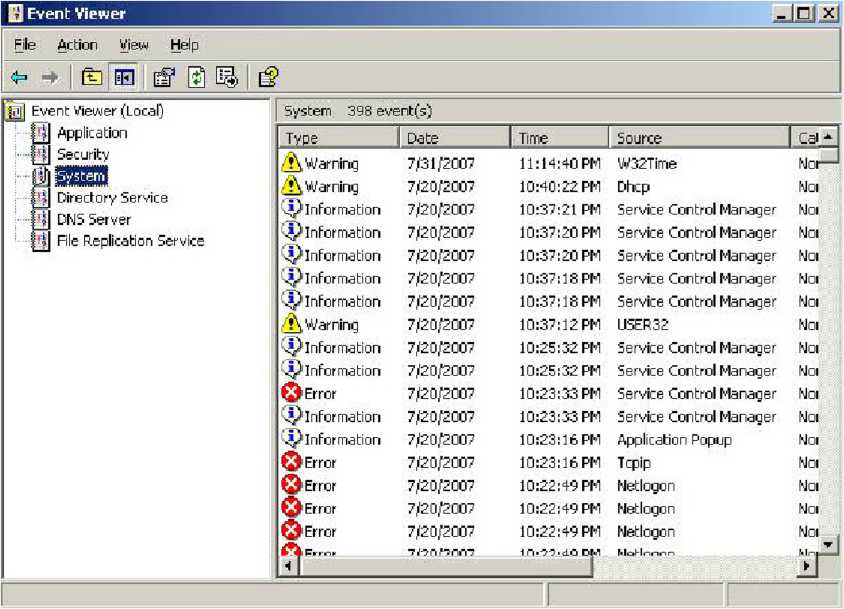
II.2. Sử dụng RSoP

Bền cạnh việc xem các chính sách bằng IP Security Monitor (trình theo dối Bảo mật IP), bạn có thể sử dụng RSoP để xác định các chính sách IP See đã được gán, nhưng chúng không được ứng dụng cho các máy khách IPSec. Snap-in RSoP chỉ hiển thị các thiết lập IPSec chi tiết. Nó hiển thị các luật bộ lọc, các hành động bộ lọc, phương thức xác thực, các đầu dượng hầm, và kiểu kết nối của chính sách đang được áp dụng.

II.3.Sử dụng Event Viewer

Bạn có thể sử dụng Event Viewer để xem các sự kiện liên quan đến

IPSec:



* Các sự kiện IPSec Policy Agent trong nhật kí kiểm toán.
* Các sự kiện trình điều khiển IPSec trong nhật kỉ hệ thống.
* Các sự kiện IKE ừong nhật kỉ kiểm định.
* Các sự kiện thây đổi chính sách IPSec ừong nhật kí kiểm định.

II.4 Sử dụng nhật kí Oakley

Bạn có thể sử dụng nhật kí Oakley để xem chi tiết của quá trình thiết lập SA. Nhật kí Oakley cổ thể được kích hoạt thông qua Registry, (mặc định chúng không được kích hoạt). Để kích hoạt nhật ký Oakley, bạn đặt giá trị của khóa HKEY\_LOCAL\_MACHEVE\System\CurrentControlSet\Services\ PolỉcyAgent\Oakley\EnableLoggỉng trong Registry bằng 1.

Nhật kí Oakley ghi lại toàn bộ các sự kiện thoả thuận ISAKMP Phương thức Chính và Phương thức Nhanh. Một File nhật kí Oakley mới sẽ được tạo ra mỗi khi IP Sec Policy Agent khởi động, và phiên bản trước của file nhật kí này sẽ được luư dưới dạng Oakley.log.sav.

II.5.SỬ dụng Netsh

Netsh là công cụ dạng dòng lệnh của Windows Server 2003 mà bạn có thể sử dụng để hiển thị hay thay đổi cấu hình mạng của các máy tính chạy Windows Server 2003 cục bộ hay từ xa. Bạn có thể chạy Netsh từ một File bó (batch file) hay tại dấu nhắc lệnh. Bạn có thể sử dụng các lệnh Netsh dành cho IPSec để cấu hình các chính sách IPSec chỉ trên các máy tính chạy các phiên bản của họ Hệ Điều Hành Windows Server 2003.

Để thiết lập ngữ cảnh IPSec của lệnh Netsh, nhập từ static hay Dynamic tại dấu nhắc Netsh IPSec. Ngữ cảnh là một tập xác định của các lệnh được bố trí trong phạm vi của cấu trúc hình cây. Ví dụ, để truy cập các lệnh khi bạn lựa chọn ngữ cảnh, bạn có thể sử dụng các lệnh Netsh để tạo chính sách hay theo dõi các hoạt động IPSec. Lệnh Netsh trong ngữ cảnh IPSec có 2 chế độ

* Chế độ tĩnh (Static mode) cho phép bạn tạo, thay đổi hay gán các chính sách mà không hề ảnh hưởng đến chính sách IPSec đang hoạt động.
* Chế độ động (Dynamic mode) cho phép bạn hiển thị trạng thái hiện thời và thực hiện các thay đổi ngay lập tức đối với chính sách IPSec đang hoạt động. Các lệnh Netsh chế độ động chỉ ảnh hưởng đến dịch vụ IPSec khi nó đang chạy. Trong trường hợp dịch vụ này đang dừng, các thiết lập chính sách chế độ động sẽ bị hủy bỏ.

Bạn có thể sử dụng Netsh để theo dõi phiên làm việc IPSec hiện tại. Việc theo dõi bao gồm việc hiển thị các thông tin chính sách, thực hiện các chẩn đoán và ghi nhật ký các thông tin IPSec. Bất cứ thông tin nào bạn có thể tìm thấy với Snap-in IP Security Monitor, bạn cũng có thể tìm thấy với lệnh Netsh. Để nhận được các thông tin về cú pháp của lệnh Netsh, tại dấu nhắc lệnh, bạn gõ Netsh/?, sau đó nhấn ENTER.

II.5.1.Hiển thị thông tin IPSec

Đe tìm ra chính sách IPSec hiện tại là gì, ta sử dụng lệnh Show. Neu bạn chọn sử dụng lệnh Show all, ta sẽ nhận được rất nhiều thông tin là được hiển thị.

Do có một số lượng lớn các thông tin về cấu hình IPSec, nên sẽ là hiệu quả hơn nếu chúng ta chỉ xem một phần của chúng. Một vài lệnh con của lệnh Show có thể giúp chúng ta thực hiện điều này. Bảng sau trình bày một vài lệnh con trong số đó. Bạn có thể nhập tất cả các lệnh từ ngữ cảnh IPSec của lệnh Netsh trong chế độ tĩnh hay chế độ động, hoặc, với sự thay đổi, từ dấu nhắc lệnh.

Lệnh Netsh IPSec Show Static

|  |  |
| --- | --- |
| Hoạt động | Lệnh |
| Để hiển thị danh sách các bộ lọc nhất định, sử dụng : | Show filterlist name = filterlistname |
| Để hiển thị chính sách đã gán cho GPO, sử dụng : | Show gpoassignedpolicy name= name |
| Để hiển thị một chính sách nhất định, sử dụng : | Show policy name pel icy name |
| Để hiển thị một luật nhất định, sử dụng : | Show rule name = mlename |

II.5.2.Sử dụng Netsh để thu nhận các thông tin chẩn đoán IPSec

Một trong các bước trong quá trình chẩn đoán các sự cố IPSec-hay thiết lập chính sách sẽ làm việc theo đúng những gì bạn dự định-là thu nhập các thông tin về chính sách hiện hành. Các lệnh Show được mô tả trong bảng ( ) Cung cấp cho chúng ta các thông tin như vậy. Thông tin mà mỗi lệnh hiển thị sẽ xác định cho các thiết lập trong chính sách. Ví dụ, lệnh Show Filterlist sẽ liệt kê các thông tin trong danh sách bộ lọc của các chính sách. Một số ví dụ về cú pháp của lệnh Show được trình bày trong bảng ( ). Tại

bảng 6-5, trong các lệnh dấu bang (=) là một phần của lệnh và bạn cần thay từ Value bằng các giá trị xác định.

> Bảng mô tả cú pháp của lệnh Show

|  |  |
| --- | --- |
| Command | Description |
| Show config | Hiển thị cấu hình IPSec và các hành vi trong thời gian khởi động. |
| Show mmsas | Hiển thị các thông tin về IPSec SA Phương thức Chính. Bạn có thể thấy các địa chỉ ngầm và đích. Khi sư dụng từ khóa Resolvedns=yes, tên của máy tính sẽ được hiển thị. |
| Show qmsas | Hiển thị các thông tin về IPSec SA Phương thức Nhanh. |
| Show stats | Hiển thị các thông số thống kê IKE IPSec Phương thức Nhanh, hoặc cả hai. Các thông số thống kê cũng giống như đã mô tả trong bảng 6-2. |

Bên cạnh các lệnh Show, bạn có thể sử dụng các lệnh chẩn đoán Netsh IP See chế độ động để thu các thông tin chẩn đoán, như liệt kê trong bảng 6-5 dưới đây.

> Bảng các lệnh chẩn đoán Netsh IPSec chế độ động

|  |  |
| --- | --- |
| Lệnh | Mô tả |
| Set config property  =ip secdiagno sties value=value | Có thể đặt với giá trị Value từ 0 tới 7, xác định mức độ chi tiết của nhật ký chuẩn đoán IP See. Giá trị mặc định là 0, điều đó có nghĩa là việc ghi nhật ký không được thực hiện, cấp độ 7 sẽ làm cho hệ thống ghi lại toàn bộ các thông tin chuẩn đoán. Máy tính nhất định phải được khởi động lại để việc ghi lại nhật ký được thực hiện. |

|  |  |
| --- | --- |
| Set config | Chỉ định tần xuất (tính theo giây) các sự kiện |
| property | IPSec được gửi tới cho nhật ký sự kiện hệ thống. |
| =ipsecloginterval  value=value | Thông số Value có giá trị nằm trong khoảng từ 60 đến 86.400, mặc định là 3600. |
| Set config | Có thể đặt giá trị Value là 0 hay 1, xác định việc |
| property  =ikelogging | ghi nhật ký IKE (Oekley) có xẩy ra hay không. Lệnh này sẽ sinh ra một file nhật ký với số lượng lớn các |
| value=vahie | thông tin. Bạn phải hiểu rõ các RFC (Requests for Comments) như một chuyên gia để có thể hiểu được các nhật ký Oakley. |
| Set config | Xác định việc kiếm tra danh sách Thu hồi Giấy |
| property | chứng nhận (Certificate Revocation List - CRL) có |
| =strongcrlcheck | được tiến hành hay ko. Nếu Value là 0, chế độ kiểm |
| value=value | tra được tắt. Nếu Value là 1, việc kiểm chứng giấy chứng nhận sẽ bị lỗi chỉ khi giấy chứng nhận đã bị thu hồi. Khi Value là 2, việc kiểm chứng sẽ lỗi khi có bất cứ 1 lỗi nào trong việc kiểm tra CRL. Việc kiểm CRL sẽ là lỗi nếu CRL không thể định vị trên mạng. Bạn có thể thực hiện các chuẩn đoán khác bằng cách thay đổi chính sách hiện tại nhằm giảm mức độ bảo mật. Ví dụ, khi bạn đổi việc xác thực sang Shared Sercret trên cả hai máy tính thay vì sử dụng Kerberos hay Certificate, bạn sẽ loại trừ được khả năng các trục trặc liên quan đến việc xác thực gây ra. |

Il.ó.Sử dụng Netdiag

Netdiag là công cụ dạng dòng lệnh bạn có thể sử dụng để hiển thị các thông tin IP See, thử và xem các cấu hình mạng. Netdiag hiện có trong Windows Server 2003, Windows 2000 và Windows XP. Mặc dù vậy, chúng được cài đặt theo các phương thức khác nhau đối YỚi mỗi hệ điều hành. Đối với Windows Server 2003, Netdiag được cài đặt cùng với Windows Server 2003 Support Tools. Đối với Windows 2000, Netdiag có sẵn trong các công cụ của Windows 2000 Resource Kit mà bạn có thể tải về từ internet. Netdiag cũng có sẵn trong đĩa cài đặt của Windows XP và sẽ được cài đặt nếu bạn chạy Setup trong thư mục Support Tools của đĩa CD cài đặt.

Chúng ta có thể nhận đước các thông tin chẩn đoán tổng quát về mạng (nhưng không có các thông tin IPSec) bằng cách sử dụng lệnh Netdiag. Ví dụ, lệnh netdiag /v /1 sẽ cung cấp các cấu hình IP và cấu hình định tuyến của máy tính, thử việc phân giải tên DNS và WINS, thông báo số phiên bản của hệ điều hành và các bản sửa lỗi nóng đã được cài đặt, và kiểm tra các mối quan hệ tin cậy. Toàn bộ các thông tin này là rất hữu dụng khi càn loại trừ các vấn đề mạng thông thường trước khi tiến hành các việc chẩn đoán IPSec.

KẾT LUẬN

•

Sau khi tiến hành nghiên cứu về Internet Protocol Security (IPSec), chúng ta có thể đi đến kết luận, IPSec là một phương thức chuẩn để cung cấp các dịch vụ bảo mật cho các gói IP. IPSec là nền tảng cho việc phát triển và sử dụng các công cụ bảo mật khác mạnh hơn về sau. Nó giúp ta bảo vệ được dữ liệu người dùng và nguồn tài nguyên trên mạng.

IPSec thực chất là sử dụng các mẫu bảo mật có sẵn nhưng lại có khả năng bảo mật cao và hiệu quả.

Tài liệu tham khảo :

1. Guider to IPSec VPNs
2. A CryptoGraphic Evaluation
3. Tap chi BCVT
4. [www.microsoft.com/technet/network/ipsec/default.mspx](http://www.microsoft.com/technet/network/ipsec/default.mspx)