TẠI VIỆT NAM ????

Trung tâm chứng thực chữ ký số quốc gia trực thuộc Cục Ứng dụng công nghệ thông tin – Bộ Thông tin và truyền thông

Trung tâm chứng thực kỹ thuật số - Trung tâm tin học & Nacencomm / Bộ KH & CN. Xây dựng trên cơ sở công nghệ hiện đại, thiết bị chuyên dụng, an toàn và bảo mật mức cao theo tiêu chuẩn hiện hành.

WWW.DIAP.GOV.VN

- Giới thiệu
  - Quá trình phát triển
  - Chức năng nhiệm vụ
  - Cơ cấu tổ chức
  - Tư liệu ảnh
- Tin tức - Sự kiện
- Bài học kinh nghiệm
- Quan hệ hợp tác
- Văn bản pháp lý
- Thông tin nội bộ
- Liên hệ
- Hỏi đáp
- Danh mục Thư điện tử
- Xin ý kiến Dự thảo văn bản

Các đơn vị trực thuộc

Trung tâm Chứng thực chữ ký số quốc gia

Cập nhật : 9:41 - 12/09/2008

Trung tâm Chứng thực chữ ký số quốc gia là đơn vị trực thuộc Cục Ứng dụng công nghệ thông tin có chức năng giúp Cục trưởng Cục Ứng dụng CNTT thực hiện công tác quản lý nhà nước về lĩnh vực chứng thực chữ ký số; quản lý các tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng và chuyên dùng; cấp phát chứng thứ số cho các tổ chức đăng ký cung cấp dịch vụ chứng thư số công cộng; tổ chức các hoạt động thúc đẩy việc sử dụng chữ ký số trong các ứng dụng công nghệ thông tin phục vụ phát triển kinh tế-xã hội trong phạm vi cả nước.

Trung tâm Chứng thực chữ ký số quốc gia là đơn vị sự nghiệp có thu, thuộc Cục Ứng dụng công nghệ thông tin, có tư cách pháp nhân, có con dấu và tài khoản riêng để giao dịch theo quy định của pháp luật, trụ sở chính đặt tại thành phố Hà Nội.

Trung tâm Chứng thực chữ ký số quốc gia có nhiệm vụ, quyền hạn quy định tại Quyết định số 891/QĐ-BTTTT ngày 13/06/2008 của Bộ trưởng Bộ Thông tin và Truyền thông:

1. Hướng dẫn thủ tục, tiếp nhận hồ sơ, tổ chức việc thẩm tra hồ sơ xin cấp phép cung cấp dịch vụ chứng thực chữ ký số công cộng, hồ sơ xin thay đổi nội dung giấy phép cung cấp dịch vụ chứng thực chữ ký số công cộng, hồ sơ xin gia hạn giấy phép;

2. Hướng dẫn thủ tục, tiếp nhận hồ sơ, tổ chức việc thẩm tra hồ sơ đăng ký cung cấp dịch vụ chứng thực chữ ký số chuyên dùng, hồ sơ xin thay đổi nội dung giấy đăng ký cung cấp dịch vụ chứng thực chữ ký số chuyên dùng, hồ sơ xin gia hạn giấy đăng ký cung cấp dịch vụ chứng thực chữ ký số chuyên dùng;

VERISIGN

Cơ quan CA - Certification Authority nổi tiếng và thành lập từ rất lâu

Cung cấp nhiều cấp độ xác nhận

- Class 1 (Lớp thấp nhất)
  - Kết hợp thư điện tử với mã khóa công cộng
- Class 4 (Lớp cao nhất)
  - Apply to servers and their organizations
  - Offers assurance of an individual's identity and relationship to a specified organization

Same Check. New Name. No Hassle.

In April 2012, all VeriSign seals automatically update to the Norton™ Secured Seal.

What it means for you

1 2 3 4

BUY SSL Certificates

BUY VeriSign Trust Seal

BUY Code Signing

TRY Free Trial NEW!

RENEW Renew SSL Certificates

SIGN IN VeriSign Trust Center

Get a VeriSign Seal

Trust from Search to Browse to Buy

Boost your site traffic and conversions with powerful trust features. Free with every SSL Certificate.

Learn more

Protect Your Site. Grow Your Business.

New features from VeriSign SSL make your Web site **easy to trust** and **easy to secure**.

Learn more

VERISIGN

Find WhoIs, Registrar Information, Domain Name Services, Managed DNS, DDoS Protection and iDefense at VerisignInc.com

BẢO VỆ MẠNG

- Firewall
  - Hardware or software
  - Uses security policy to filter packets
  - 3 phương thức:
    - Bộ lọc packet (packet-filtering router)
    - Cổng ứng dụng (application-level gateway hay proxy server)
    - Cổng mạch (circuit - level gateway)
- Proxy servers (proxies)
  - Software servers that handle all communications originating from or being sent to the Internet

FIREWALLS AND PROXY SERVERS

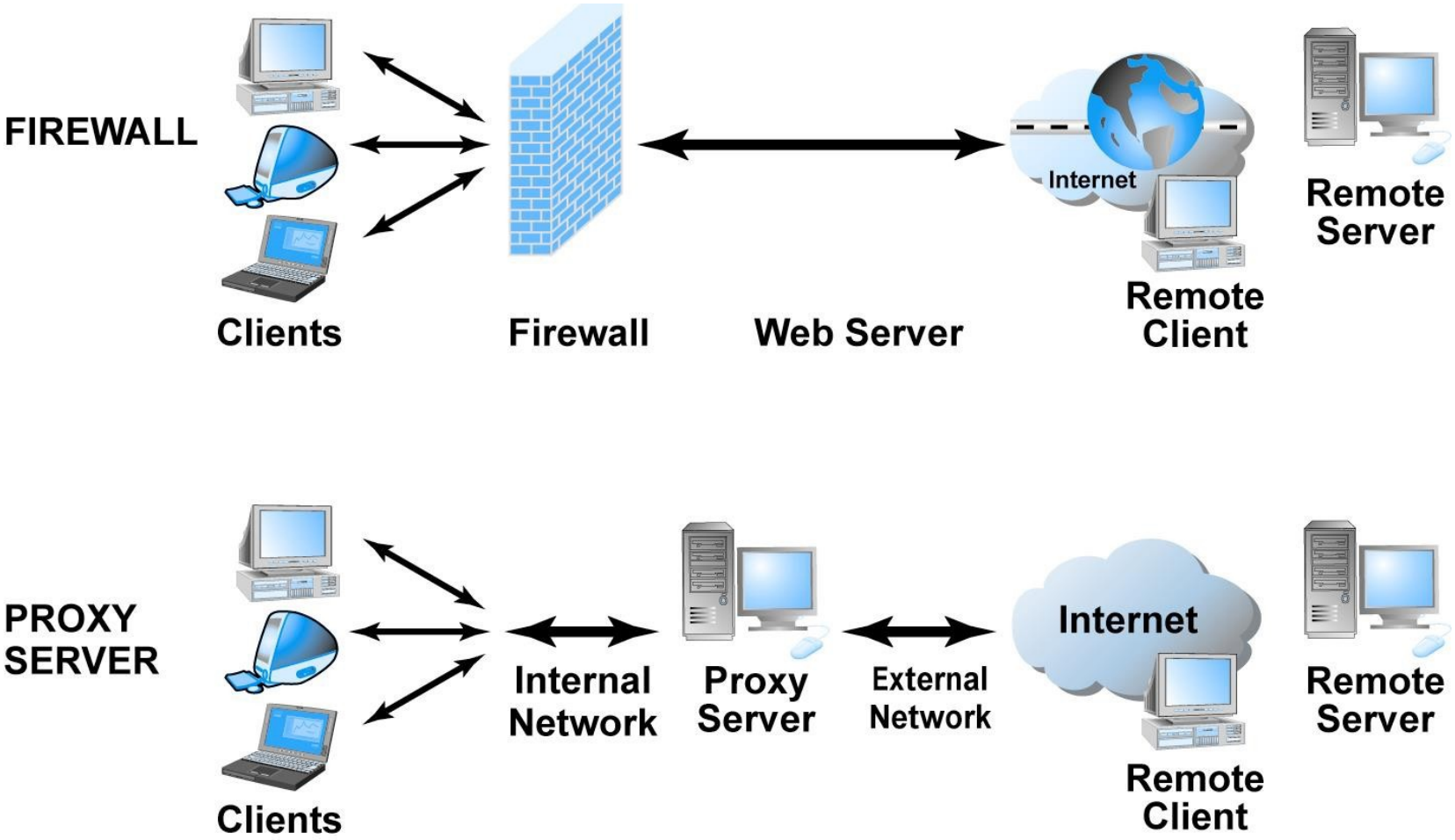


Figure 5.13, Page 301

TƯỜNG LỬA-FIREWALLS

Chức năngchính của Firewall là kiểm soát luồng thông tin từ giữa Intranet và Internet. Thiết lập cơ chế điều khiển dòng thông tin giữa mạng bên trong (Intranet) và mạng Internet

- Cho phép hoặc cấm những dịch vụ truy nhập ra ngoài (từ Intranet ra Internet).
- Cho phép hoặc cấm những dịch vụ phép truy nhập vào trong (từ Internet vào Intranet).
- Theo dõi luồng dữ liệu mạng giữa Internet và Intranet.
- Kiểm soát địa chỉ truy nhập, cấm địa chỉ truy nhập.
- Kiểm soát người sử dụng và việc truy nhập của người sử dụng.
- Kiểm soát nội dung thông tin thông tin lưu chuyển trên mạng

TƯỜNG LỬA-FIREWALLS

- Các chức năng của phần mềm firewall
  - Lọc các gói tin(Packet filters)
    - Kiểm tra tất cả các gói tin đi ngang qua tường lửa
  - Hoạt động như 1 Gateway
    - Lọc gói tin dựa trên yêu cầu các ứng dụng
  - Proxy servers
    - Liên lạc với mạng bên ngoài thay cho mạng cục bộ
    - Vùng đệm cho các trang web

NGUYÊN LÝ BỘ LỌC PACKET

Bộ lọc packet cho phép hay từ chối mỗi packet mà nó nhận được.Nó kiểm tra toàn bộ đoạn dữ liệu để quyết định xem đoạn dữ liệu đó có thoả mãn một trong số các luật lệ của lọc packet hay không.

Các luật lệ lọc packet này là dựa trên các thông tin ở đầu mỗi packet (packet header), dùng để cho phép truyền các packet đó ở trên mạng:

NGUYÊN LÝ BỘ LỌC PACKET(TT)

Địa chỉ IP nơi xuất phát (IP Source address)

Địa chỉ IP nơi nhận (IP Destination address)

Những thủ tục truyền tin (TCP, UDP, ICMP, IP tunnel)

Cổng TCP/UDP nơi xuất phát (TCP/UDP source port)

Cổng TCP/UDP nơi nhận (TCP/UDP destination port)

Dạng thông báo ICMP (ICMP message type)

Giao diện packet đến (incomming interface of packet)

Giao diện packet đi (outcomming interface of packet)

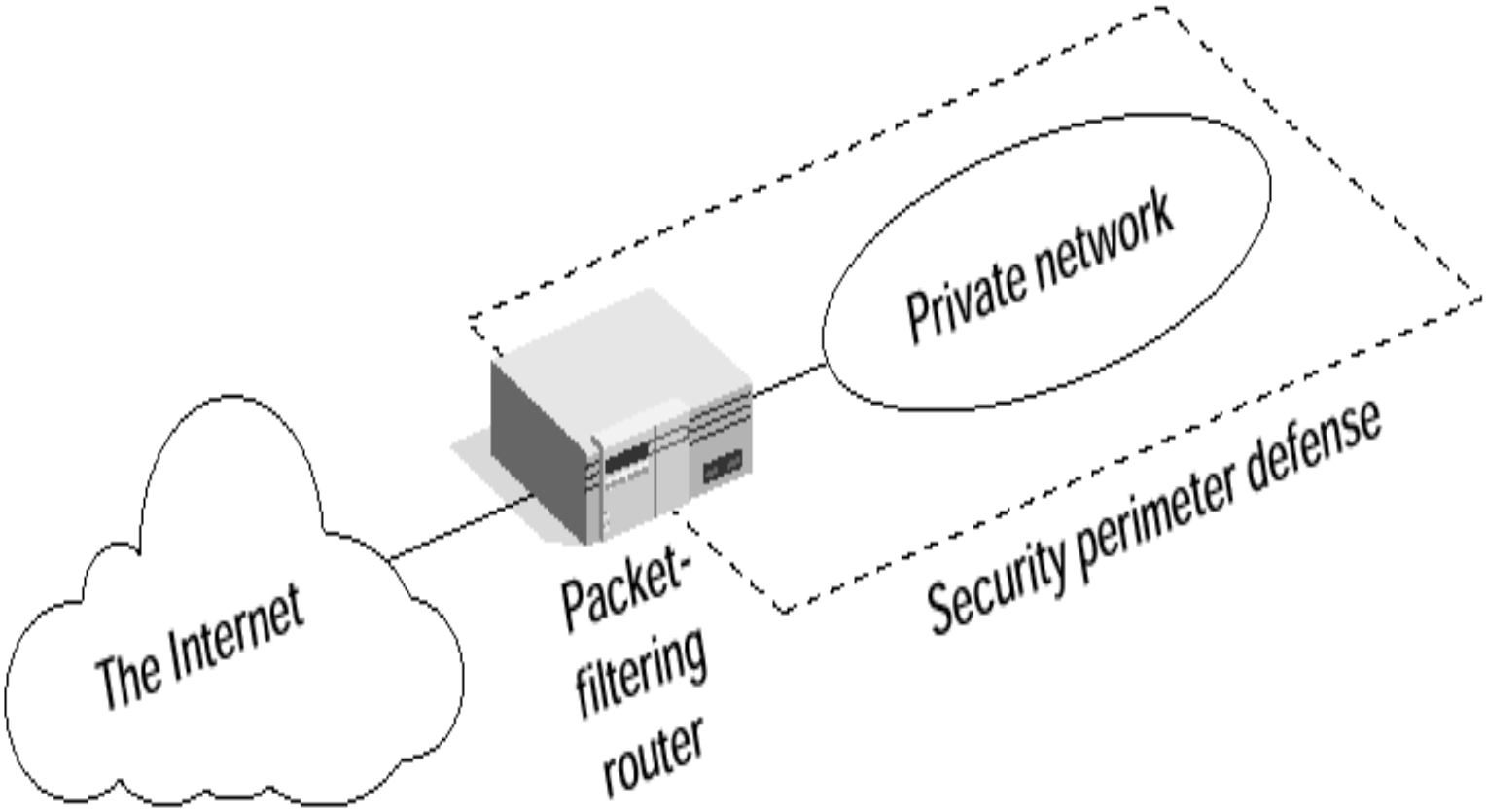
NGUYÊN LÝ BỘ LỌC PACKET(TT)

Nếu luật lệ lọc packet được thoa mãn thì packet được chuyển qua firewall. Nếu không packet sẽ bị bỏ đi.

Nhờ vậy mà Firewall có thể ngăn can được các kết nối vào các máy chủ hoặc mạng nào đó được xác định, hoặc khoá việc truy cập vào hệ thống mạng nội bộ từ những địa chỉ không cho phép.

Việc kiểm soát các cổng làm cho Firewall có kha năng chỉ cho phép một số loại kết nối nhất định vào các loại máy chủ nào đó, hoặc chỉ có những dịch vụ nào đó (Telnet, SMTP, FTP...) được phép mới chạy được trên hệ thống mạng cục bộ

PACKET FILTER



ƯU/KHUYẾT ĐIỂM

Ưu điểm

Đa số các hệ thống firewall đều sử dụng bộ lọc packet.

Chi phí thấp vì cơ chế lọc packet đã được bao gồm trong mỗi phần mềm router.

Bộ lọc packet là trong suốt đối với người sử dụng và các ứng dụng, vì vậy nó không yêu cầu sự huấn luyện đặc biệt nào ca.

Hạn chế

Việc định nghĩa các chế độ lọc package là một việc khá phức tạp

ƯU/KHUYẾT ĐIỂM

Khi đòi hỏi về sự lọc càng lớn, các luật lệ về lọc càng trở nên dài và phức tạp, rất khó để quan lý và điều khiển.

Bộ lọc packet không kiểm soát được nôi dung thông tin của packet. Các packet chuyển qua vẫn có thể mang theo những hành động với ý đồ ăncắp thông tin hay phá hoại của kẻ xấu.

CỔNG ỨNG DỤNG

Nguyên lý

Đây là một loại Firewall được thiết kế để tăngcường chức năng kiểm soát các loại dịch vụ, giao thức được cho phép truy cập vào hệ thống mạng. Cơ chế hoạt động của nó dựa trên cách thức gọi là Proxy service.

Proxy service là các bộ code đặc biệt cài đặt trên gateway cho từng ứng dụng. Nếu người quan trị mạng không cài đặt proxy code cho một ứng dụng nào đó, dịch vụ tương ứng sẽ không được cung cấp và do đó không thể chuyển thông tin qua firewall.

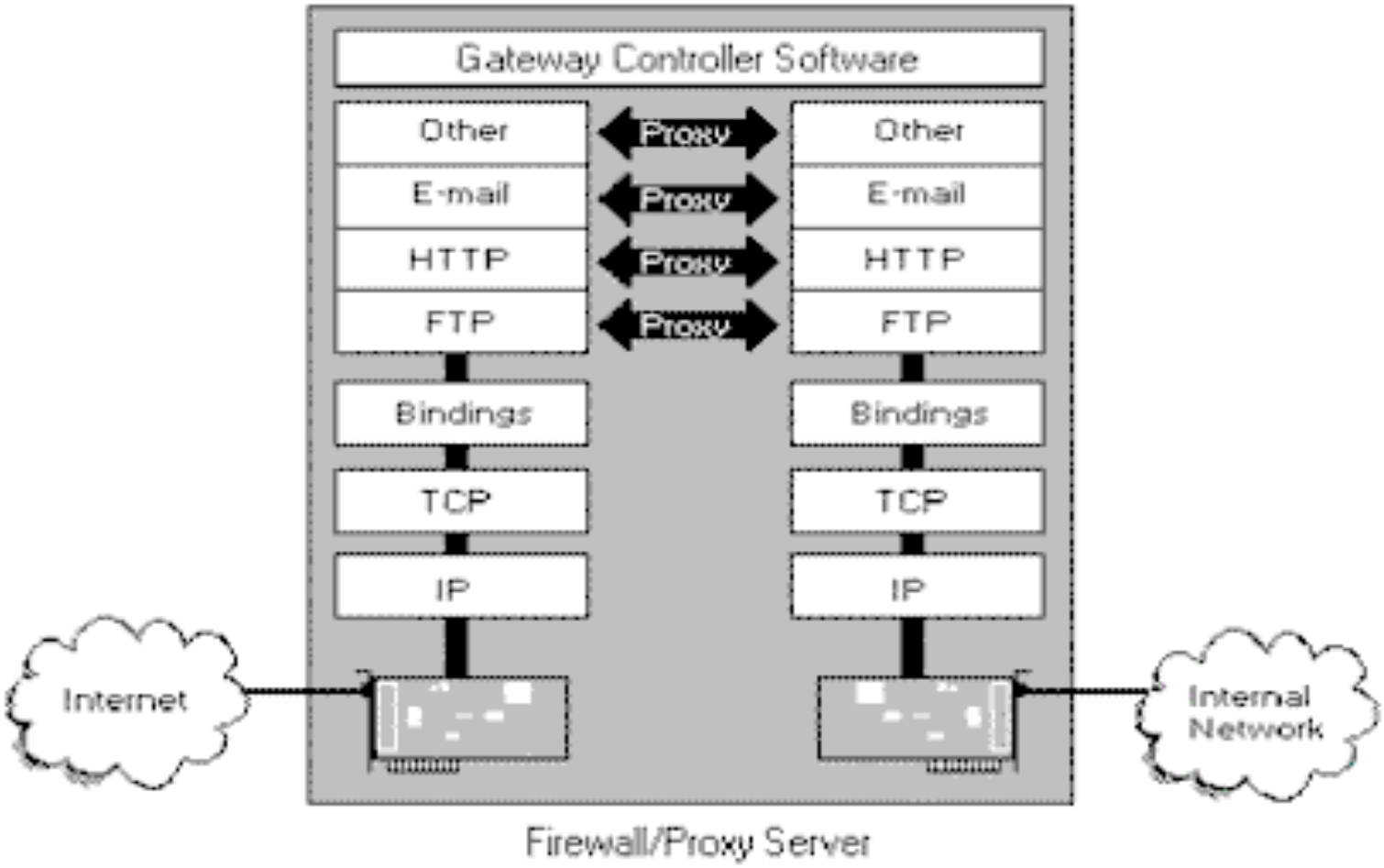
Ngoài ra, proxy code có thể được định cấu hình để hỗ trợ chỉ một số đặc điểm trong ứng dụng mà người quan trị mạng cho là chấp nhận được trong khi từ chối những đặc điểm khác.

CỔNG ỨNG DỤNG

Một cổng ứng dụng thường được coi như là một pháo đài (bastion host), bởi vì nó được thiết kế đặt biệt để chống lại sự tấn công từ bên ngoài. Những biện pháp đam bao an ninh của một bastion host là:

- Luôn chạy các version an toàn (secure version) của các phần mềm hệ thống (Operating system). Các version an toàn này được thiết kế chuyên cho mục đích chống lại sự tấn công vào Operating System, cũng như là đam bao sự tích hợp firewall
- Chỉ những dịch vụ mà người quan trị mạng cho là cần thiết mới được cài đặt trên bastion host, đơn gian chỉ vì nếu một dịch vụ không được cài đặt, nó không thể bị tấn công. Thông thường, chỉ một số giới hạn các ứng dụng cho các dịch vụ Telnet, DNS, FTP, SMTP và xác thực user là được cài đặt trên bastion host.

CỔNG ỨNG DỤNG



CỔNG ỨNG DỤNG

Bastion host có thể yêu cầu nhiều mức độ xác thực khác nhau, ví dụ như user password hay smart card.
Mỗi proxy được đặt cấu hình để cho phép truy nhập chỉ một sồ các máy chủ nhất định. Điều này có nghĩa rằng bộ lệnh và đặc điểm thiết lập cho mỗi proxy chỉ đúng với một số máy chủ trên toàn hệ thống.

Mỗi proxy duy trì một quyển nhật ký ghi chép lại toàn bộ chi tiết của giao thông qua nó, mỗi sự kết nối, khoang thời gian kết nối. Nhật ký này rất có ích trong việc tìm theo dấu vết hay ngăn chặn kẻ phá hoại.

Mỗi proxy đều độc lập với các proxies khác trên bastion host. Điều này cho phép dễ dàng quá trình cài đặt một proxy mới, hay tháo gỡ môt proxy đang có vấn đề.

CỔNG ỨNG DỤNG

Ưu điểm

Cho phép người quan trị mạng hoàn toàn điều khiển được từng dịch vụ trên mạng, bởi vì ứng dụng proxy hạn chế bộ lệnh và quyết định những máy chủ nào có thể truy nhập được bởi các dịch vụ.

Cho phép người quan trị mạng hoàn toàn điều khiển được những dịch vụ nào cho phép, bởi vì sự vắng mặt của các proxy cho các dịch vụ tương ứng có nghĩa là các dịch vụ ấy bị khoá.

Cổng ứng dụng cho phép kiểm tra độ xác thực rất tốt, và nó có nhật ký ghi chép lại thông tin về truy nhập hệ thống.

Luật lệ lọc filltering cho cổng ứng dụng là dễ dàng cấu hình và kiểm tra hơn so với bộ lọc packet.

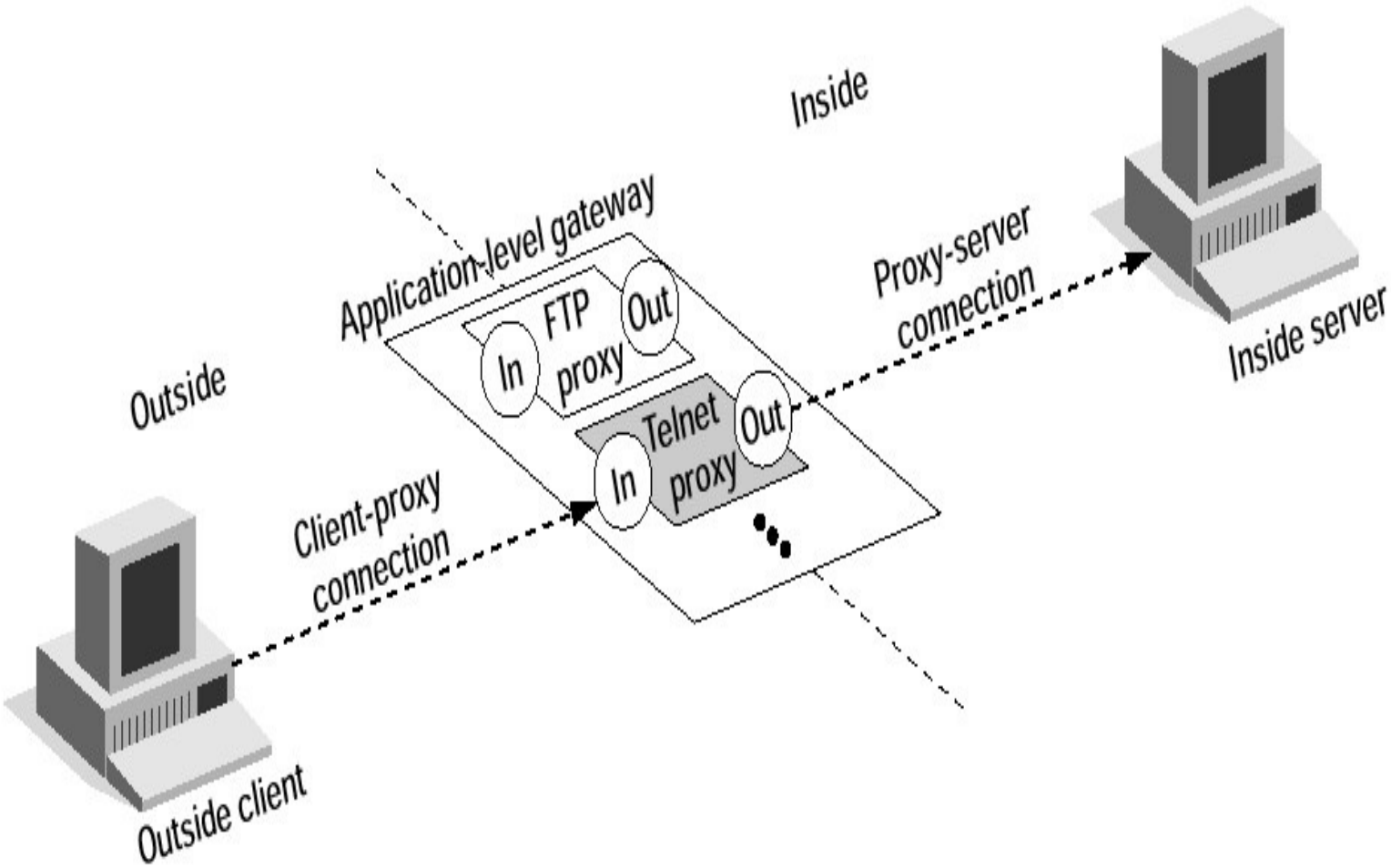
CỔNG ỨNG DỤNG

Hạn chế

Yêu cầu các users thay đổi thao tác, hoặc thay đổi phần mềm đã cài đặt trên máy client cho truy nhập vào các dịch vụ proxy. Chẳng hạn, Telnet truy nhập qua cổng ứng dụng đòi hỏi hai bước để nối với máy chủ chứ không phai là một bước thôi.

Tuy nhiên, cũng đã có một số phần mềm client cho phép ứng dụng trên cổng ứng dụng là trong suốt, bằng cách cho phép user chỉ ra máy đích chứ không phai cổng ứng dụng trên lệnh Telnet.

CỔNG ỨNG DỤNG

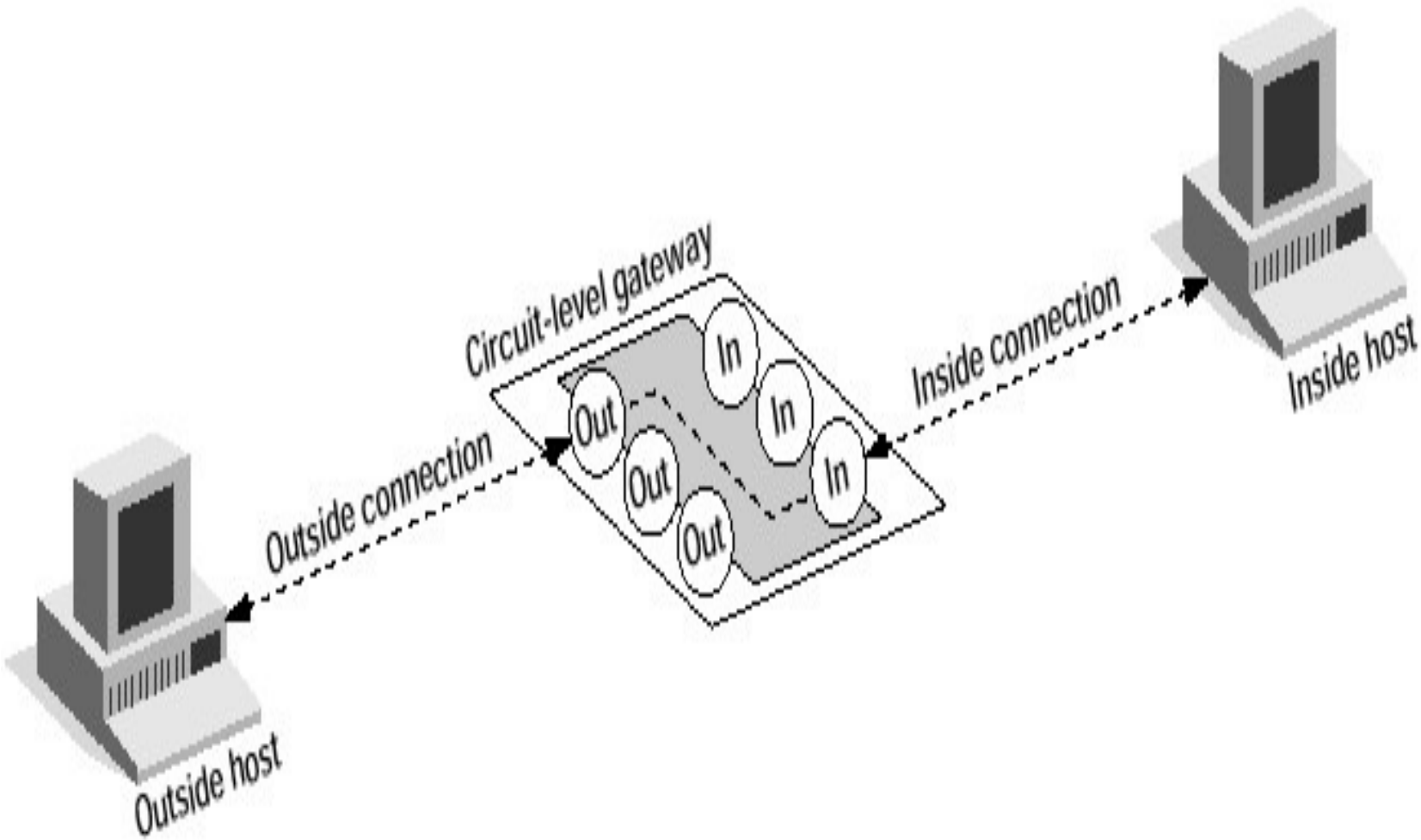


CỔNG VÒNG (CIRCUIT-LEVEL GATEWAY)

Cổng vòng là một chức năng đặc biệt có thể thực hiện được bởi một cổng ứng dụng. Cổng vòng đơn gian chỉ chuyển tiếp (relay) các kết nối TCP mà không thực hiện bất kỳ một hành động xử lý hay lọc packet nào.

Cổng vòng đơn gian chuyển tiếp kết nối telnet qua firewall mà không thực hiện một sự kiểm tra, lọc hay điều khiển các thủ tục Telnet nào.Cổng vòng làm việc như một sợi dây,sao chép các byte giữa kết nối bên trong (inside connection) và các kết nối bên ngoài (outside connection). Tuy nhiên, vì sự kết nối này xuất hiện từ hệ thống firewall, nó che dấu thông tin về mạng nội bộ.

CIRCUIT-LEVEL GATEWAY



CỔNG VÒNG (CIRCUIT-LEVEL GATEWAY)

Cổng vòng thường được sử dụng cho những kết nối ra ngoài, nơi mà các quan trị mạng thật sự tin tưởng những người dùng bên trong. Ưu điểm lớn nhất là một bastion host có thể được cấu hình như là một hỗn hợp cung cấp Cổng ứng dụng cho những kết nối đến, và cổng vòng cho các kết nối đi. Điều này làm cho hệ thống bức tường lửa dễ dàng sử dụng cho những người trong mạng nội bộ muốn trực tiếp truy nhập tới các dịch vụ Internet, trong khi vẫn cung cấp chức năngbức tường lửa để bao vệ mạng nội bộ từ những sự tấn công bên ngoài.

NHỮNG HẠN CHẾ CỦA FIREWALL

Không đủ thông minh như con người để có thể đọc hiểu từng loại thông tin và phân tích nội dung tốt hay xấu của nó.

Chỉ có thể ngănchặn sự xâm nhập của những nguồn thông tin không mong muốn nhưng phai xác định rõ các thông số địa chỉ.

Không thể ngănchặn một cuộc tấn công nếu cuộc tấn công này không "đi qua" nó. Một cách cụ thể, firewall không thể chống lại một cuộc tấn công từ một đường dial-up, hoặc sự dò rỉ thông tin do dữ liệu bị sao chép bất hợp pháp lên đĩa mềm

NHỮNG HẠN CHẾ CỦA FIREWALL

Không thể chống lại các cuộc tấn công bằng dữ liệu (data-drivent attack). Khi có một số chương trình được chuyển theo thư điện tử, vượt qua firewall vào trong mạng được bao vệ và bắt đầu hoạt động ở đây.

Một ví dụ là các virus máy tính. Firewall không thể làm nhiệm vụ rà quét virus trên các dữ liệu được chuyển qua nó, do tốc độ làm việc, sự xuất hiện liên tục của các virus mới và do có rất nhiều cách để mã hóa dữ liệu, thoát khỏi kha năng kiểm soát của firewall.

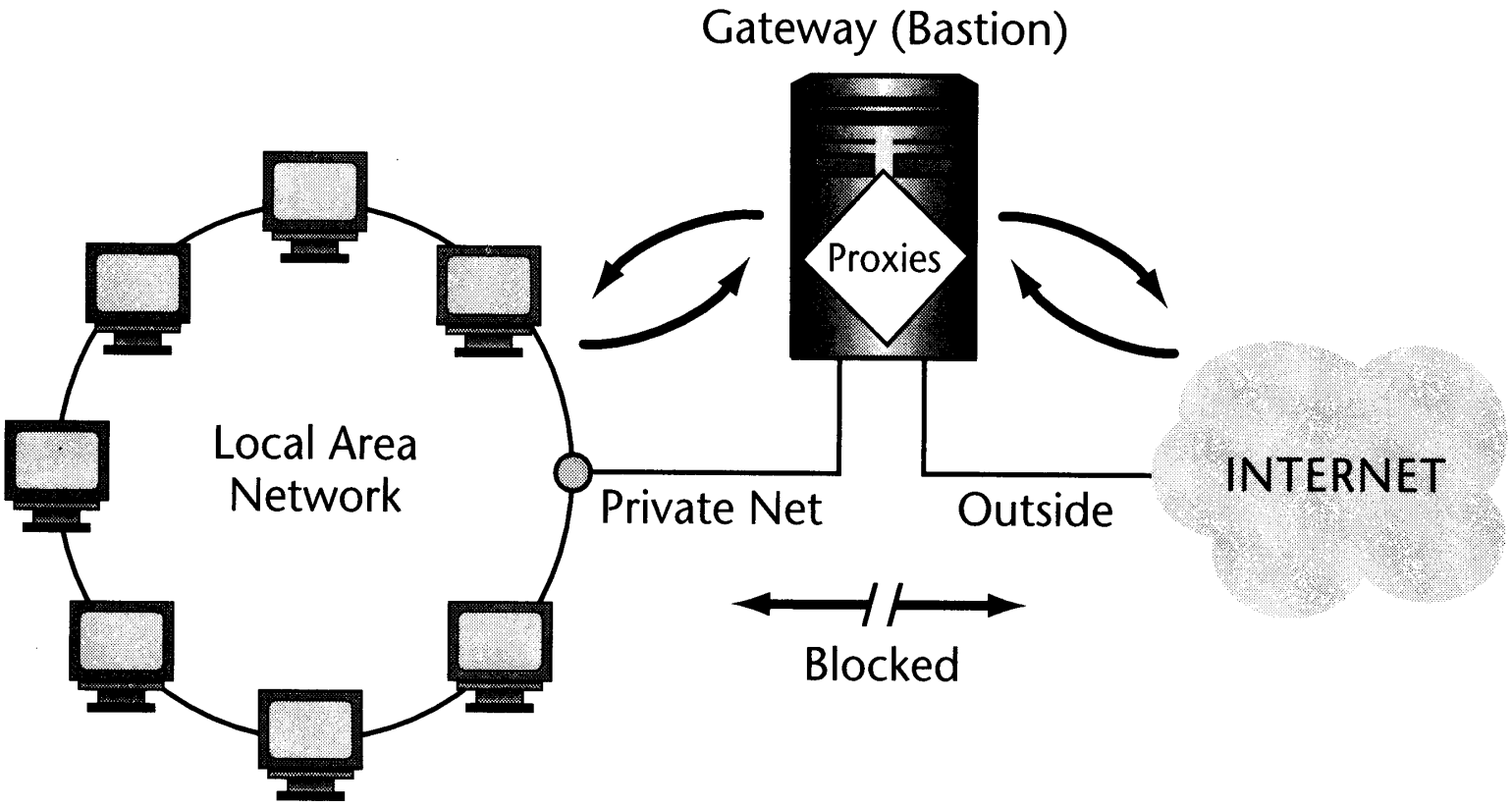
Tuy nhiên, Firewall vẫn là giải pháp hữu hiệu được áp dụng rộng rãi.

CHỌN CẤU HÌNH CHO FIREWALL

- Có nhiều cách thiết lập cấu hình

  - Dạng Bastion host
    - Tập trung triển khai các chế độ bảo vệ
    - Thường ở cấp độ application-level hay circuit level gateway
  - Dạng Dual homed gateway
    - Sử dụng 2 giao tiếp mạng, 1 cho mạng nội bộ và 1 cho mạng ngoài
    - Khả năng lọc packet

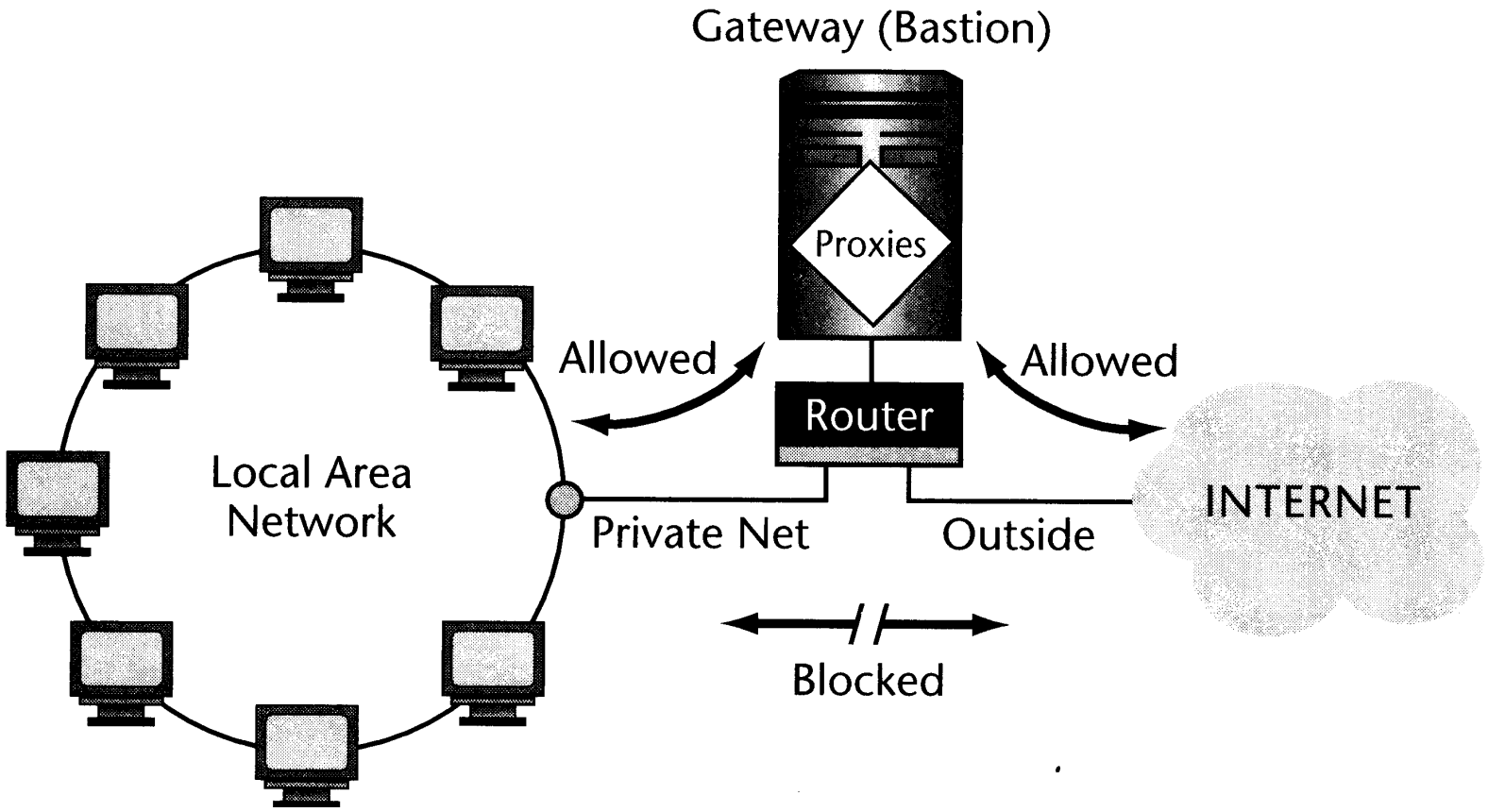
DUAL-HOMED GATEWAY



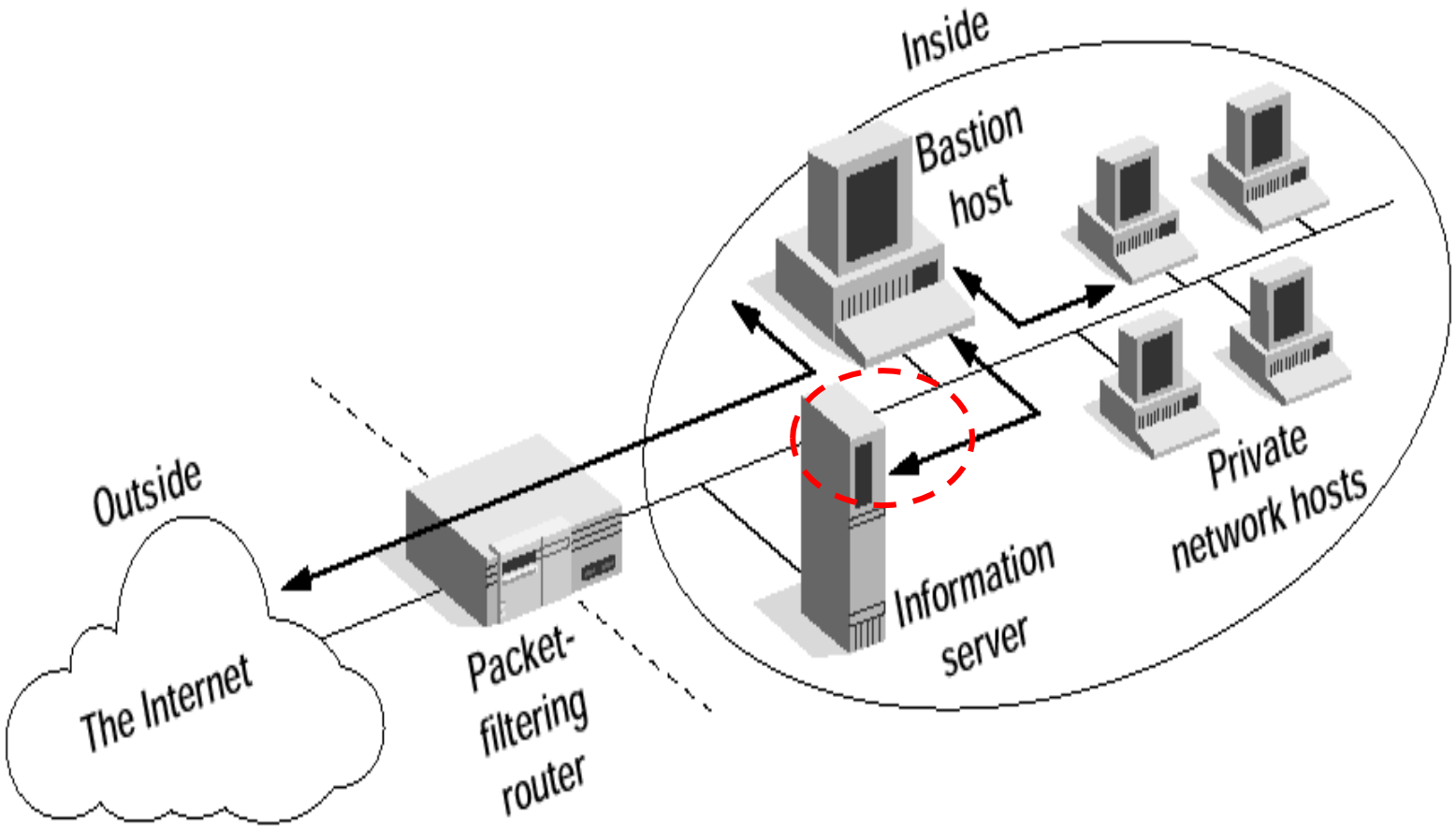
CHỌN CẤU HÌNH CHO FIREWALL (TT)

- Dạng Screened host firewall system
  - Sử dụng 1 bộ điều hướng mạng (network router) để truyền tai thông tin đi vào mạng nội bộ và ra mạng bên ngoài qua trung gian 1 gateway

SCREENED-HOST GATEWAY



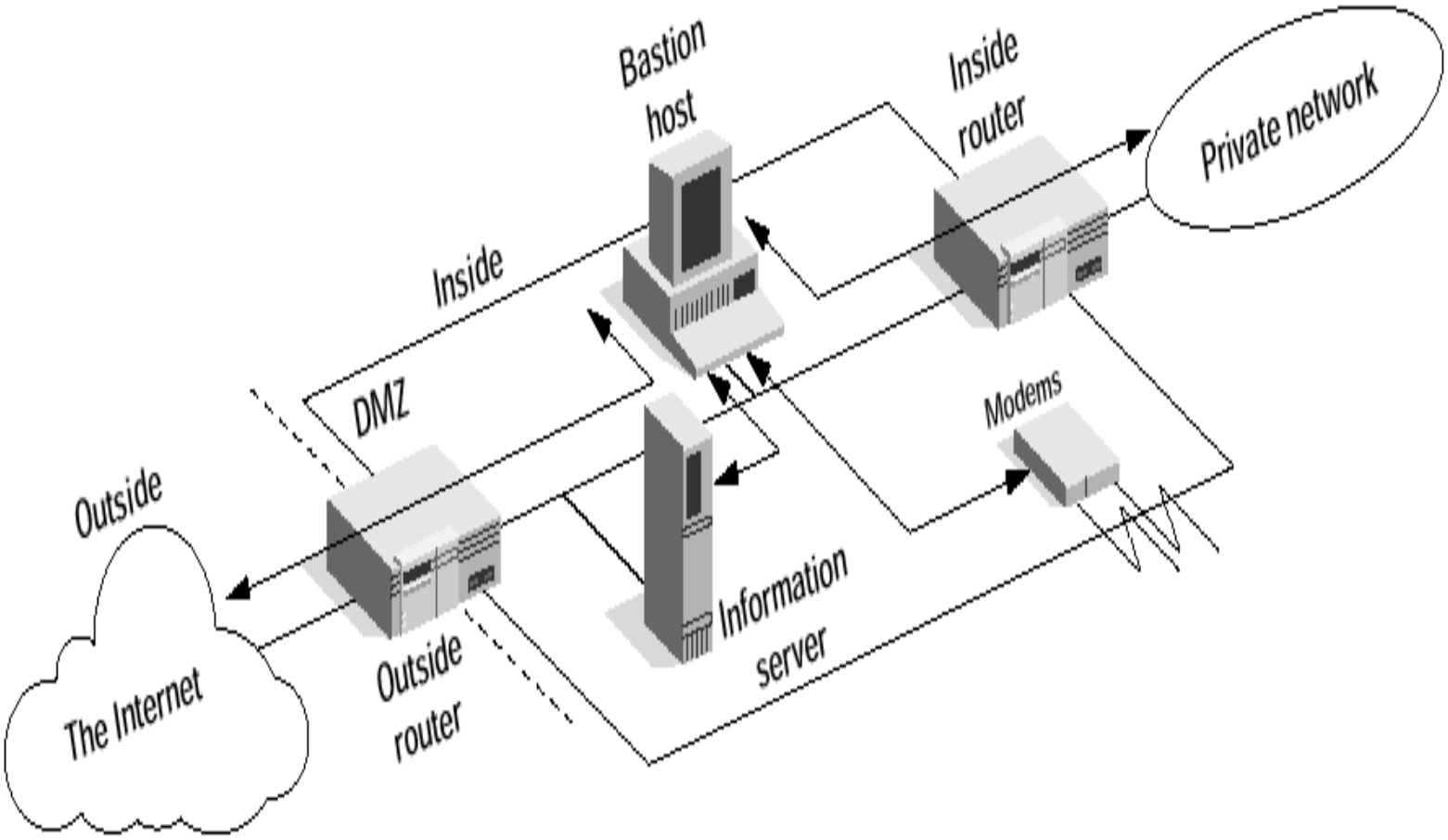
SCREENED HOST FIREWALL



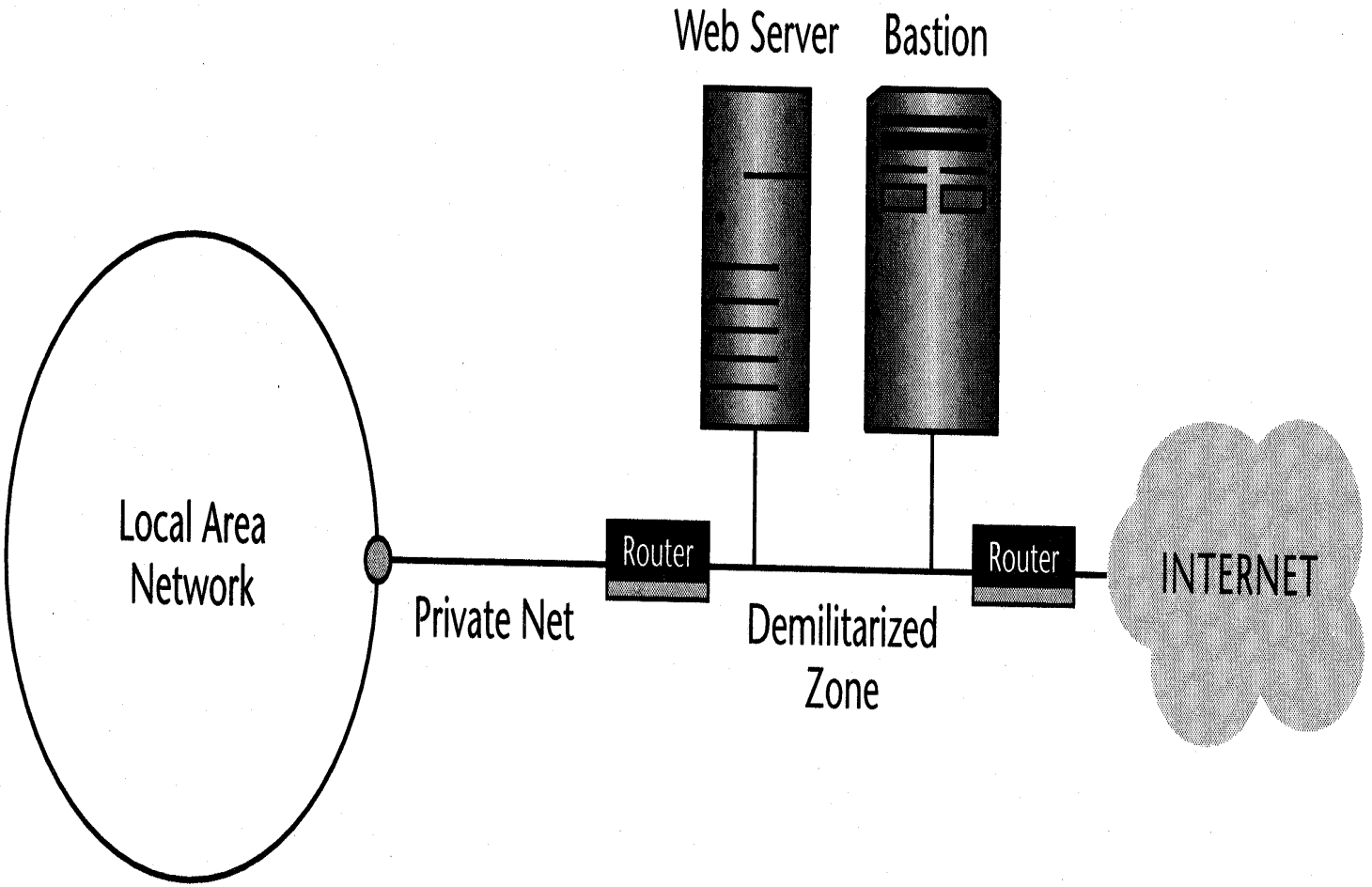
CHỌN CẤU HÌNH CHO FIREWALL (TT)

Screened-subnet firewall system

SCREENED SUBNET FIREWALL



SCREENED SUBNET GATEWAY



BẢO VỆ SERVERS VÀ CLIENTS

Tăngan ninh cho hệ điều hành

Upgrades, patches

Phần mềm Anti-virus:

Cách dễ dàng và ít tốn kém nhất để ngănngừa các hiểm họa đối với hệ thống

Yêu cầu cập nhật hàng ngày

CHÍNH SÁCH QUẢN LÝ, QUI TRÌNH KINH DOANH, VÀ PHÁP LUẬT

Các công ty và tổ chức ở U.S dử dụng 12% ngân sách IT cho an ninh phần cứng, phần mềm và dịch vụ ($120 billion in 2009)

Quan lý rủi ro bao gồm

- Công nghệ
- Hiệu qua của các chính sách quan lý
- Pháp luật

KẾ HOẠCH AN NINH: CÁC CHÍNH SÁCH QUẢN LÝ

- Đánh giá rủi ro
- Chính sách an ninh
- Kế hoạch thực hiện
  - Tổ chức an ninh
  - Kiểm soát truy cập
  - Qui trình xác thực
  - Các chính sách quyền hạn, các hệ thống quan lý quyền hạn
- Kiểm định an ninh

DEVELOPING AN E-COMMERCE SECURITY PLAN

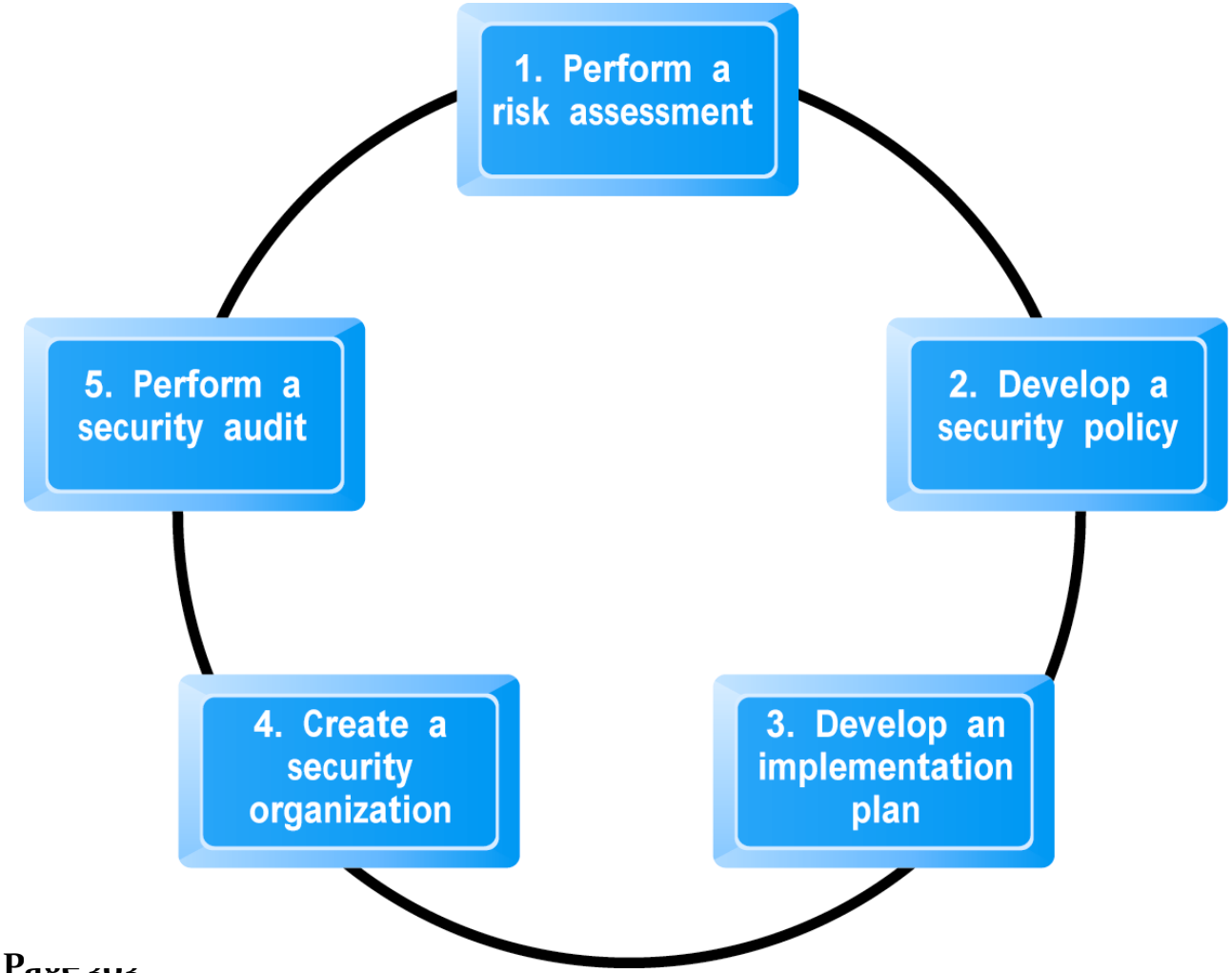


Figure 5.14, Page 303

VAI TRÒ CỦA PHÁP LUẬT VÀ CÁC CHÍNH SÁCH CÔNG

- Năm 2007

✉Nghị định số 63/2007/NĐ-CP quy định xử phạt vi phạm hành

- chính trong lĩnh vực công nghệ thông tin

✉ Nghị định số 27/2007/NĐ-CP quy định chi tiết thi hành Luật Giao dịch điện tử trong hoạt động tài chính

✉Nghị định số 26/2007/NĐ-CP quy định chi tiết thi hành Luật Giao dịch điện tử về Chữ ký số và Dịch vụ chứng thực chữ ký số Năm 2006

✉ Nghị định số 56/2006/NĐ-CP về thương mại điện tử

✉Luật Công nghệ thông tin

- Năm 2005

✉ Luật Giao dịch điện tử

VAI TRÒ CỦA PHÁP LUẬT VÀ CÁC CHÍNH SÁCH CÔNG

- Laws that give authorities tools for identifying, tracing, prosecuting cybercriminals:
  - National Information Infrastructure Protection Act of 1996
  - USA Patriot Act
  - Homeland Security Act
- Private and private-public cooperation
  - CERT Coordination Center
  - US-CERT
- Government policies and controls on encryption software
- OECD guidelines

CÁC HỆ THỐNG THANH TOÁN

Tiền mặt

Hình thức thanh toán phổ biến nhất

Chuyển khoan

Hình thức phổ biến thứ 2 tại U.S.

Thẻ tín dụng

Hiệp hội thẻ tín dụng
Ngân hàng phát hành thẻ
Trung tâm xử lý

Giá trị lưu trữ

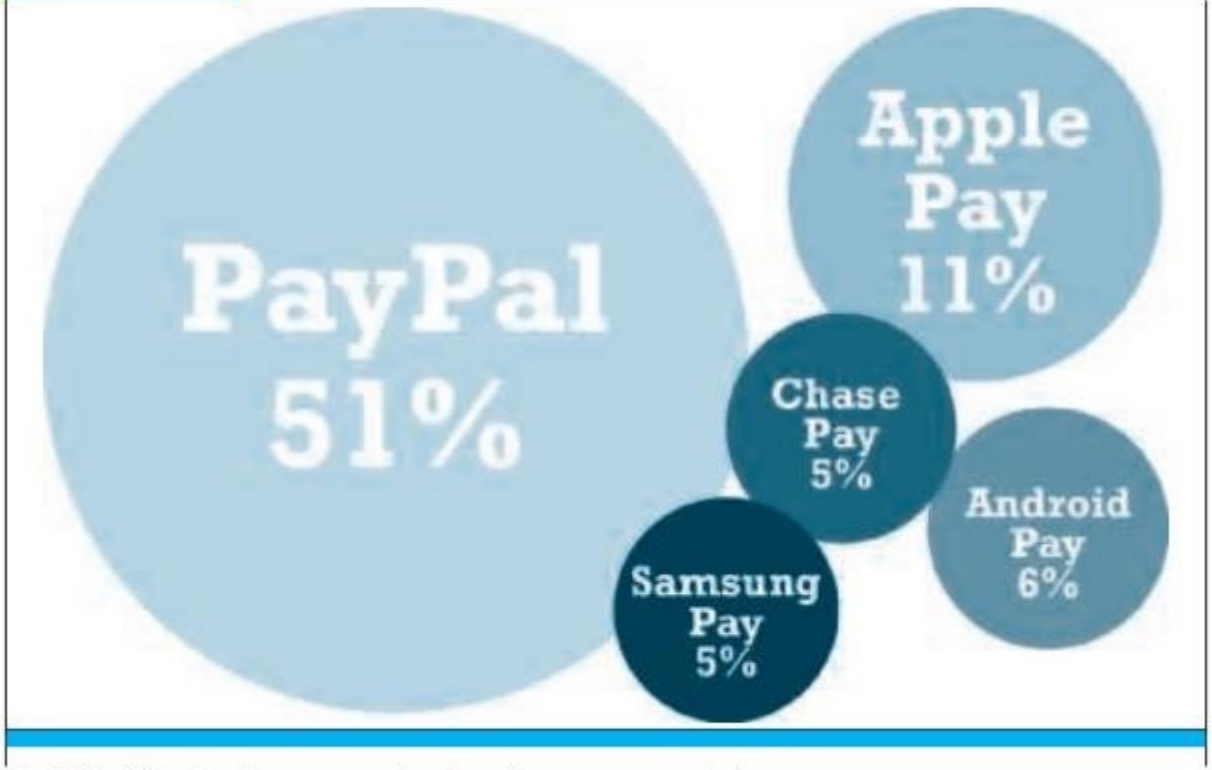
Tiền được gửi trong tài khoan và được rút ra khi cần, vd: thẻ ghi nợ, phiếu quà tặng

Hệ thống thanh toán ngang hàng

TABLE 5.8 MAJOR TRENDS IN E-COMMERCE PAYMENTS 2016–2017

- Payment by credit and/or debit card remains the dominant form of online payment.
- Mobile retail payment volume skyrockets.
- PayPal remains the most popular alternative payment method online.
- Apple, Google, Samsung, and PayPal extend their reach in mobile payment apps.
- Large banks enter the mobile wallet and P2P payments market.
- Square gains further traction with a smartphone app, credit card reader, and credit card processing service that permits anyone to accept credit card payments.
- Google refocuses Google Wallet, which had met with tepid response, solely on sending and receiving money.
- Mobile P2P payment systems such as Venmo take off.

FIGURE 5.13 **ALTERNATIVE PAYMENT METHODS USED BY U.S. CONSUMERS**



PayPal is still, by far, the most popular alternative payment method.

SOURCE: Based on data from eMarketer, 2016a.

TABLE 5.6 DIMENSIONS OF PAYMENT SYSTEMS

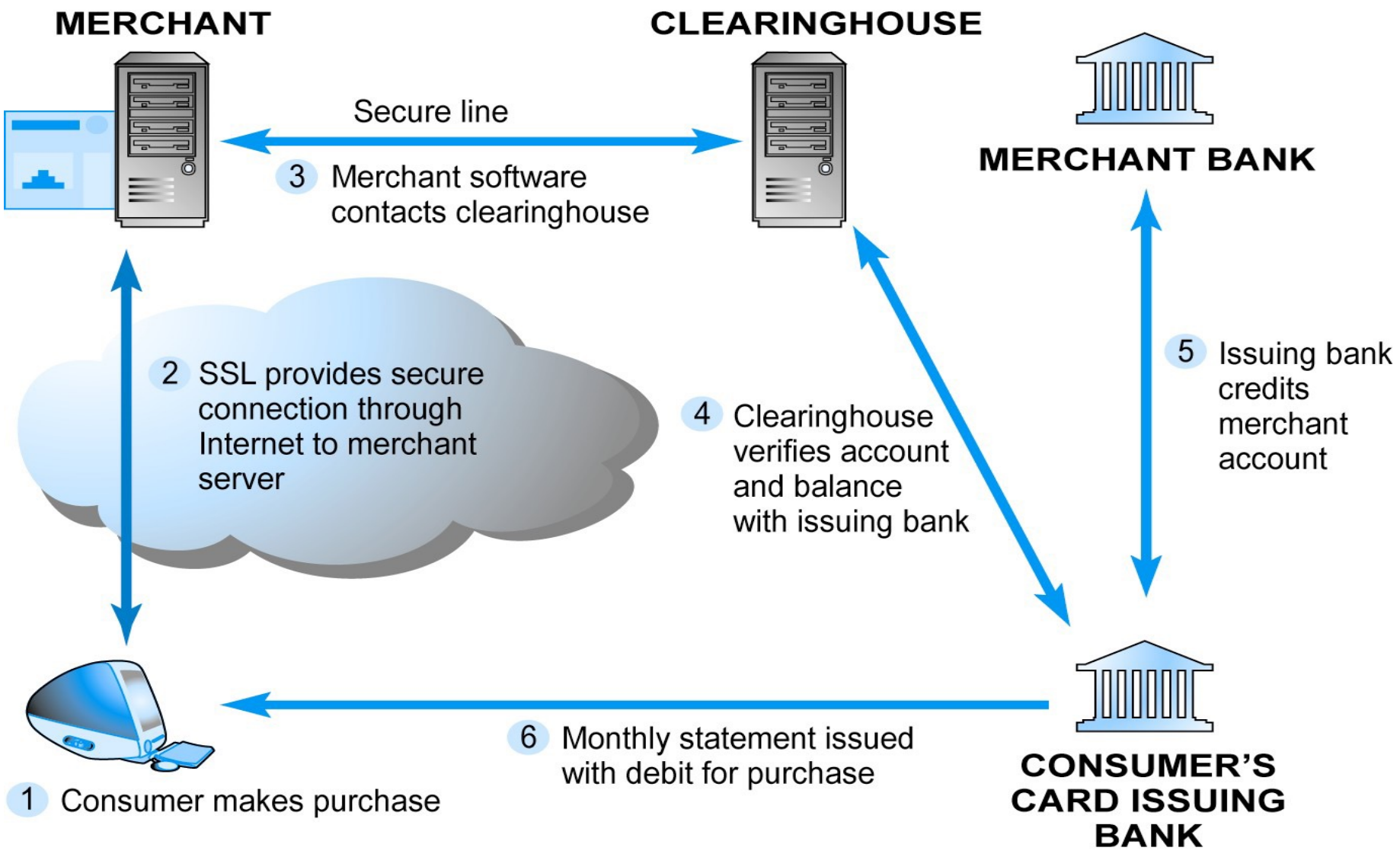
DIMENSION	CASH	PERSONAL CHECK	CREDIT CARD	STORED VALUE (DEBIT CARD)	ACCUMULATING BALANCE
Instantly convertible without intermediation	yes	no	no	no	no
Low transaction cost for small transactions	yes	no	no	no	yes
Low transaction cost for large transactions	no	yes	yes	yes	yes
Low fixed costs for merchant	yes	yes	no	no	no
Refutable (able to be repudiated)	no	yes	yes	no (usually)	yes
Financial risk for consumer	yes	no	up to $50	limited	no
Financial risk for merchant	no	yes	yes	no	yes
Anonymous for consumer	yes	no	no	no	no
Anonymous for merchant	yes	no	no	no	no
Immediately respendable	yes	no	no	no	no
Security against unauthorized use	no	some	some	some	some
Tamper-resistant	yes	no	yes	yes	yes
Requires authentication	no	yes	yes	yes	yes
Special hardware required	no	no	yes—by merchant	yes—by merchant	yes—by merchant
Buyer keeps float	no	yes	yes	no	yes
Account required	no	yes	yes	yes	yes
Has immediate monetary value	yes	no	no	yes	no

CÁ HỆ THỐNG THANH TOÁN TRONG TMĐT

Các hạn chế của hình thức thanh toán trực tuyến bằng thẻ tín dụng

- An ninh
- Chi phí
- Công bằng xã hội

HOW AN ONLINE CREDIT TRANSACTION WORKS



CÁC HỆ THỐNG THANH TOÁN TRONG TMĐT (TT)

Ví số - Digital wallets

Mô phỏng chức năngcủa ví bằng cách chứng thực khách hàng, đam bao việc lưu trữ và chuyển giao giá trị, và an toàn trong việc thanh toán giữa khách hàng và doanh nghiệp

Các nỗ lực phổ biến đều thất bại.

Nỗ lực mới nhất: Google Checkout

Việt Nam: Vcash (vinapay), MegaPayment, Vnmart (Vnpay),...

Tiền số - Digital cash

Lưu trữ giá trị và trao đổi bằng cách sử dụng tokens

Hiện nay không phổ biến do các giao thức và cách thực hiện phức tạp

CÁC HỆ THỐNG THANH TOÁN TMĐT (TT)

Hệ thống lưu trữ giá trị trực tuyến

Dựa trên giá trị lưu trữ trong ngân hàng của khách hàng, kiểm tra, hay tài khoan thẻ tín dụng

PayPal, smart cards

Tài khoan số chi tra tích lũy

Người dùng tích lũy "số dư nợ" (debit balance) mà họ được lập hóa đơn vào cuối tháng

Kiểm soát số - Digital checking:

Mở rộng chức năng của tài khoan hiện có để sử dụng trực tuyến

HỆ THỐNG THANH TOÁN MOBILE

Sử dụng các thiết bị di động cá nhân như là các thiết bị thanh toán, được dùng nhiều ở Europe, Japan, South Korea

Hệ thống thanh toán mobile ở Japan

- E-money (stored value)
- Mobile debit cards
- Mobile credit cards

Không phát triển ở U.S

DIGITAL CASH AND VIRTUAL Currencies

- Digital cash
  - Based on algorithm that generates unique tokens that can be used in "real" world
  - Example: Bitcoin
- Virtual currencies
  - Circulate within internal virtual world
  - Example: Linden Dollars in Second Life, Facebook Credits

Insight on Society: Class Discussion

BITCOIN

- What are some of the benefits of using a digital currency?
- What are the risks involved to the user?
- What are the political and economic repercussions of a digital currency?
- Have you or anyone you know ever used Bitcoin?

ELECTRONIC BILLING PRESENTMENT and Payment (EBPP)

- Online payment systems for monthly bills
- Over 50% of all bill payments
- Two competing EBPP business models:
  - Biller-direct (dominant model)
  - Consolidator
- Both models are supported by EBPP infrastructure providers