Internal Restricted

Designing Network Security

- Port Numbers
- Security Technologies
- Export Controls on Cryptography
- Threats in an Enterprise Network
- Considerations for a Site Security Policy
- Design and Implementation of the Corporate Security Policy
- Incident Handling
- Securing the Corporate Network Infrastructure
- Securing Internet Access
- Securing Dial-In Access
- Sources of Technical Information
- Reporting and Prevention Guidelines: Industrial Espionage and Network Intrusions
- Basic Cryptography

Copyright 1989-2000 © Cisco Systems Inc.

domain	53/udp	Domain Name Server
tacacs-ds	65/tcp	TACACS-Database Service
tacacs-ds	65/udp	TACACS-Database Service
kerberos	88/tcp	Kerberos
kerberos	88/udp	Kerberos
https	443/tcp	HTTP protocol over TLS/SSL
https	443/udp	HTTP protocol over TLS/SSL
smtps	465/tcp	SMTP protocol over TLS/SSL (was ssmtp)
smtps	465/udp	SMTP protocol over TLS/SSL (was ssmtp)
isakmp	500/tcp	ISAKMP protocol
isakmp	500/udp	ISAKMP protocol
nntps	563/tcp	NNTP protocol over TLS/SSL (was snntp)
nntps	563/udp	NNTP protocol over TLS/SSL (was snntp)
sshell	614/tcp	SSL shell
sshell	614/udp	SSL shell
kerberos-adm	749/tcp	Kerberos administration
kerberos-adm	749/udp	Kerberos administration
kerberos-iv	750/udp	Kerberos Version 4
ftps-data	989/tcp	FTP protocol, data, over TLS/SSL
ftps-data	989/udp	FTP protocol, data, over TLS/SSL

ftps	990/tcp	FTP protocol, control, over TLS/SSL
ftps	990/udp	FTP protocol, control, over TLS/SSL
telnets	992/tcp	Telnet protocol over TLS/SSL
telnets	992/udp	Telnet protocol over TLS/SSL
imaps	993/tcp	IMAP4 protocol over TLS/SSL
imaps	993/udp	IMAP4 protocol over TLS/SSL
ircs	994/tcp	IRC protocol over TLS/SSL
ircs	994/udp	IRC protocol over TLS/SSL
pop3s	995/tcp	POP3 protocol over TLS/SSL (was spop3)
pop3s	995/udp	POP3 protocol over TLS/SSL (was spop3)
socks	1080/tcp	SOCKS
socks	1080/udp	SOCKS
pptp	1723/tcp	PPTP
pptp	1723/udp	PPTP
radius	1812/tcp	RADIUS
radius	1812/udp	RADIUS
radius-acct	1813/tcp	RADIUS Accounting
radius-acct	1813/udp	RADIUS Accounting
http-alt	8080/tcp	HTTP Alternate (see port 80)

http-alt	8080/udp	HTTP Alternate (see port 80)

continues

HOME CONTENTS PREVIOUS NEXT GLOSSARY FEEDBACK SEARCH HELP

Posted: Wed Jun 14 11:28:58 PDT 2000
Copyright 1989 - 2000©Cisco Systems Inc.

Media independence	The ISP can leverage any media (Frame Relay, ATM, Point-to-Point, X.25) in the backbone to support the virtual dial-up service.
Dynamic tunnel	Tunnels are initiated and management torn down based on L2TP management. This setup provides a scalable solution because tunnels are initiated only when user traffic is active. Minimizes the NAS resources required to maintain tunnels.
Multiple remote user sessions are multiplexed over a single L2TP tunnel	This is a scalable solution because it minimizes the number of tunnels required to be open at a given time. PVC-based backbone infrastructures such as Frame Relay need only a single PVC between the NAS and the corporate gateway to manage multiple remote user sessions.
Tunnel security maintains random key and sequence numbers	Tunnel establishment involves a NAS (ISP)-to-corporate-gateway authentication process to protect against attacks. In addition, L2TP resists spoofing by using sequence numbers.
No routing protocol dependencies	Neither the ISP nor the corporate customer is required to manage the other's routing domain to provide access and services, freeing both to use whichever routing protocols suits them best.

Additional Considerations

With any of the VPDN technologies, PPP authentication is used to authenticate users or devices; tunnel endpoints may periodically re-authenticate. However, there is no protection for individual packets (either data or control) that traverse the established tunnel. There is work in progress that proposes using IPsec transport mode to secure the VPDN tunnel traffic. In addition, for individual data packets traveling through the VPDN tunnel, security services including authentication, integrity, replay protection, and confidentiality can be provided by using IPsec in conjunction with L2F, PPTP, or L2TP.

Public Key Infrastructure and Distribution Models

Many security protocols rely on public-key cryptography to provide services such as confidentiality, data integrity, data origin authentication, and non-repudiation. The purpose of a Public Key Infrastructure (PKI) is to provide trusted and efficient key and certificate management to support these protocols.

A PKI is defined by the Internet X.509 Public Key Infrastructure PKIX Roadmap "work in progress"

of approximately 25 members from the exporting community and government agencies.

Additional liberalization of export controls were announced in May 1997. The new policy allowed the export of products without key recovery requirements and an unlimited key length if the products were used solely for financial transactions. This policy was extended in July 1998 to allow the general exportability of products without key recovery mechanisms to financial institutions in 45 countries. (These 45 countries agreed to take steps against money laundering.) These financial institutions would be able to distribute the encryption technology among their international branches (except in terrorist states) after the initial approval was granted.

The export policy was further liberalized in September 1998 to include export of 56-bit DES and equivalent products, without requiring key recovery mechanisms, to approved industries worldwide, including subsidiaries of U.S. firms, insurance companies, health and medical organizations, and online merchants. In all cases however, there is the requirement of a one-time product technical review before the export is allowed.

The changes in U.S. encryption export policy will most likely continue. To get more information on updates on U.S. encryption export regulations, refer to the following Web sites:

- Code of Federal Regulations---International Traffic in Arms Regulations: http://www.epic.org/crypto/export_controls/itar.html
- Current and historical information on US commercial encryption export controls: http://www.bxa.doc.gov/Encryption
- Press release from the Department of Commerce---Bureau of Export Administration (BXA) on Update on Export Controls of Encryption Products (12/30/98): http://www.bxa.doc.gov/PRESS/98/1230Encryption.html

Historical Perspective on International Policy

Internationally, encryption export and import controls are also undergoing vast changes. The Coordinating Committee for Multilateral Export Controls (COCOM) was an international organization that provided common export controls of strategic products and technical data from country members to prescribed destinations. COCOM provided an agreement to control the export and handling of sensitive technologies including supercomputers, fast DSP chips, crypto, lasers, precision CNC milling/machining equipment, and so on. COCOM was, in effect, a generalized effort by the West during the Cold War to prevent the flow of technology into communist countries (not just the USSR). It maintained, among others lists, the International Industrial List and the International Munitions List.

COCOM's 17 members were Australia, Belgium, Canada, Denmark, France, Germany, Greece, Italy, Japan, Luxembourg, the Netherlands, Norway, Portugal, Spain, Turkey, the United Kingdom, and the United States. Cooperating members included Austria, Finland, Hungary, Ireland, New Zealand, Poland, Singapore, Slovakia, South Korea, Sweden, Switzerland, and Taiwan.

One of the goals of the COCOM regulations was to prevent cryptography from being exported to "dangerous" countries---usually, countries thought to maintain friendly ties with terrorist organizations, such as Libya, Iraq, Iran, and North Korea. Exporting to other countries is usually allowed although states often require that a license be granted.

Belgium	Belgium requires a license for exporting cryptography outside of the Benelux	An unclear 1994 law was amended in 1997 to remove any confusion. The new amendment explicitly states that the use of encryption is free. The provision of indicated encryption services to the public is subject to prior notification (four weeks in advance) to the Belgian Institute of Post and Telecommunications.
Brazil	There are no export or import controls.	There are no controls on crypto use.
Burma	None.	Cryptography is restricted through a licensing regime.
Belarus	None.	For manufacture, repair, and operation of cryptography, a license by the State Security Committee is required. Cryptography use by business people is restricted.
Canada	Canada follows the Wassenaar regulations. The export of items from Canada may be subject to restriction if they are included on the Export Control List. No restrictions exist on imports or exports to the United States.	None.
People's Republic of China	China restricts the import and export of voice-encoding devices.	China may be restricting cryptography, but the authorities have not made a statement about encryption. The legal situation is unclear.
Czech Republic	No export/import controls.	None.
Denmark	There are export controls according to the Wassenaar Arrangement.	None.

Hungary	There are export controls according to the Wassenaar Arrangement. There are import controls mirroring the export controls, requiring an import license if an export license would be needed in Hungary. Import and export of mass-market encryption software is exempted.	None.
Iceland	None.	None.
India	India requires an import license for encryptors.	None.
Indonesia	The import/export regulation is unclear.	Use of cryptography is said to be prohibited.
Ireland	None.	None.
Israel	There are export controls, but there is no specific limit on key size. Licenses seem to be granted on a case-by-case basis. The import of cryptography also seems to be regulated. The Ministry of Defense is revising the regulations, creating different classes of encryption with different levels of control; certain cryptography products (such as authentication only) would be released from controls.	Israel imposes restrictions on encryption through the Encryption Order, but their scope is not clear. Use of strong encryption may require a license from the army, to be decided on a case-by-case basis; the license is virtually always granted. However, it is unclear whether and how one is required to request a license. No prosecutions for using unlicensed crypto are known, and strong encryption is widely used in Israel.
Italy	COCOM/EU regulations.	Italy has a law that demands encrypted records to be accessible to the treasury.

Japan	Export regulations are designed to implement the Wassenaar Arrangement. Decisions are made on an individual basis. Japan seems to have tightened its export controls in 1996. Now businesses must acquire approval for a cryptography export order larger than 50,000 yen.	None.
Kazakhstan	For importing or exporting cryptographic products, a license is required from the Licensing Commission of the Committee of National Security. The decisions of this committee are subject to judicial review.	A license from the Committee of National Security is required for the development (including research), manufacture, repair (including technical support), and sale (including use and advertising) of cryptographic products.
Latvia	Export controls are in line with the EU dual-use regulation. Import controls mirror the export controls (that is, an import license is required if export is controlled).	There is no domestic restriction of cryptography.
Malaysia	There are no export or import restrictions.	There is no regulation of crypto use.
Mexico	None.	None.

The Netherlands	Export controls are regulated according to the Wassenaar Arrangement. The export of public-domain and mass-market software generally does not require a validated license. Items capable of file encryption do require a validated license for export.	If encrypted files are found in a computer during a house search, the police cannot order or coerce a suspect to decrypt his own material. They can ask/order someone else, who is not under arrest, to provide what information they can about the encrypted material, or they can ask a specialist in the field to decrypt the material.
New Zealand	A license is required to export cryptography. Export of crypto software by electronic means does not fall under the export regulation.	None.
Norway	Norway abides by the COCOM regulations.	None.
Pakistan	None.	The sale and use of encryption hardware and software require approval by Pakistani telecommunications officials.
Philippines	None.	E-mail encryption is not restricted.
Poland	A license is required for exporting encryption software or hardware, in accordance with the EU dual-use goods regulation. A general authorization or import certificate is required to buy encryption products abroad. The end-user must detail the kind of information to be encrypted and where the cryptography is to be installed.	None.
Portugal	None.	None.
Romania	There are no import controls.	None.

Russia	A license is required for the import of encryption facilities manufactured abroad. The export of cryptography is subject to a tightened state control.	In April 1995, President Boris Yeltsin issued a decree prohibiting unauthorized encryption. State organizations and enterprises need a license to use encryption (for both authentication and secrecy, for storage as well as for transmission). The development, production, implementation, or operation of cryptography without a license is prohibited.
Saudi Arabia	None.	It is reported that Saudi Arabia prohibits the use of encryption but that this prohibition is widely ignored.
Singapore	There are no export restrictions. The Trade Development Board (TDB) imposes an import regulation, which requires people to obtain prior approval for importing cryptography hardware or software. The TDB tends to approve crypto software more than crypto hardware. The unofficial policy seems to readily permit import of crypto for banking and credit card transactions.	There is no legislation on cryptography. However, subscribers have to obtain prior approval from the Telecommunications Authority of Singapore (TAS) to send encrypted messages across the Singapore telecommunications lines. TAS is informed by the TDB of its import permits. The use permit may restrict the address from which the encryption product can be used. Selling of the crypto is prohibited without approval from the TDB/TAS.
South Africa	None.	Use of encryption is free for commercial or private organizations. However, any electronic device connected to a telecommunications line must first be approved by Telkom, the tele-communications regulatory body. This restriction does not apply if the device is connected between a modem or router and the computer. Use or provision of cryptography by government bodies requires approval from the relevant agency; likewise,