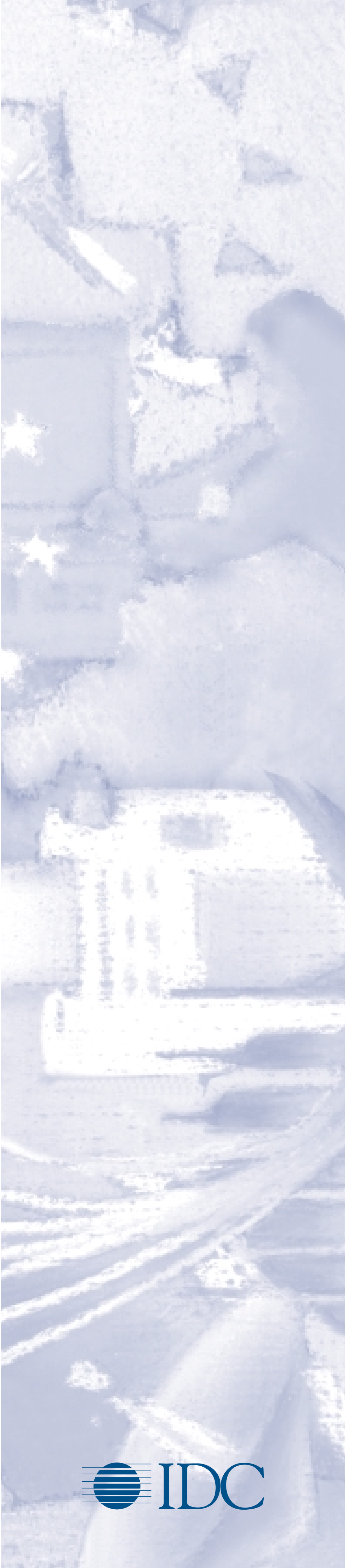


Security: The eBusiness Enabler

An IDC White Paper Sponsored by Tivoli Systems

Analyst: Ken Fraser

IDC

Tivoli

Introduction

"Security" continues to be a source of concern and confusion for enterprise IS management: increasingly, it is receiving the attention of the CEO in addition to that of the CIO.

Security in a networked environment used to be just "keeping the bad guys out" and the standard response to that was, "Put in a firewall." Today, in a world of extended connectivity via extranets and Virtual Private Networks (VPNs), it is just as important to be able to "let the good guys in": customers, partners, suppliers and subcontractors need to be given secure, controlled access to specific resources in order to facilitate business relationships. Next, it is now acknowledged that most network-enabled fraud actually arises from within the enterprise: the traditional firewall is no help here and a new set of security measures is needed.

Managements' attitudes to this changing security environment are conditioned by the historical difficulty and expense of enforcing security consistently across multiple systems on multiple platforms. End-users, also, (whether employees at work or consumers at home) object to working with multiple, intrusive security procedures.

Often, a fundamental issue is the absence of a policy-based approach to security. The fear, uncertainty and doubt surrounding both the commercial threats and the countermeasure technologies are accompanied by a failure to perceive measurable Return On Investment (ROI) and the perception that a full-scale security régime carries a very high Total Cost of Ownership (TCO).

While management understanding of the Risks and Threats (see below) is a necessary precondition for implementing a security régime, these ROI and TCO issues need to be addressed. More recent solutions offered in the security sector seek actively to assist in policy formulation. It is then possible to provide an implementation methodology which draws directly on the rules formulated under that policy. Finally, enterprise-wide security management is enabled through the use of common directory services.

This paper focuses on the goal of cost-effective security implementation. After a brief review of the terminologies, the rationale and business impact of the new security paradigm are examined in the following pages.

The theory – threats, risks and countermeasures

The following table illustrates, with a limited sample, the importance of distinguishing between “Threat” and “Risk”:

Table 1: Threats and Risks

Threats	Risks
External (hacker penetration)	
Benign	
“Ethical”	Generally beneficial
“Just for kicks”	Adverse publicity
Malicious	
Data theft/corruption/destruction	From minimal to disastrous
Fraud	Very serious
Internal (improper access)	
Accidental	
Breach of Confidentiality	Potentially serious
Security loophole created	Probably critical
Malicious	
Data theft	Very serious
Data corruption	Very serious
Fraud	Very serious
Data destruction	Potentially disastrous
Denial of Service	Potentially disastrous

Source: IDC, 2000

The risks, categorised by cost, can be further analysed.
For example:

- direct financial loss – e.g. through fraud
- indirect loss – e.g. operational (remedial) costs
- adverse publicity – “image loss”

The threats generally relate to data - destruction, corruption or theft - and are frequently realised through impersonation. “Denial of Service” receives less press coverage but is increasingly critical for enterprises which commit much or all of their business to the online environment.

Countermeasures

It is usual to categorise countermeasure objectives as:

Countermeasure	Objective
Privacy	controlling access to data
Integrity	ensuring that data is neither corrupted nor destroyed
Authenticity	verifying the origin or provenance of the data

Source: IDC, 2000

And to identify two security régimes:

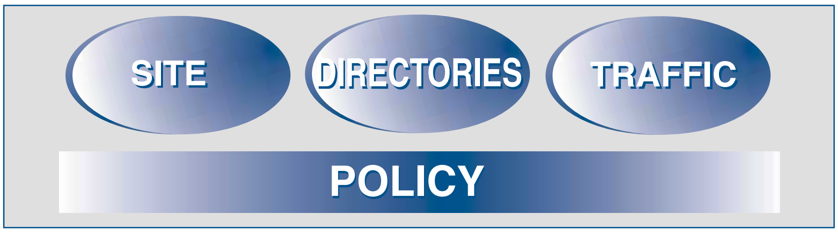
Security	Régime
Site	typified by firewalls, access gateways and intrusion detectors at server level and by anti-virus products at client level.
Traffic	largely achieved through the use of communications encryption techniques

Source: IDC, 2000

Technologies and products

Within the Site and Traffic categories, the specific functions which may be required include firewalls, encryption, antivirus and “3A”. This multiplicity of components has been one of the major impediments to the deployment of good security régimes and modern practice is to adopt a number of inter-function protocols. The side bar, right, identifies some important terms currently in use.

A simplified model of the functionality required is:



Source: IDC, 2000

Some important terms...

Functions

Firewalls

Both software products and “appliances”

Encryption

Including Public Key Infrastructure and Digital Certificates

Antivirus

Including “Mobile Code” and content filters

“3A”

(Authentication, Authorisation and Administration) including Intrusion Detection and Audit, Single-Sign-On and “Two-Factor Authentication” (Tokens, including Smart Card products)

Inter-function Protocols

LDAP

an open protocol which allows applications to both get information from and put data to compliant directories

aznAPI

an open Authorisation Application Programming Interface (API) which uses authenticated user identities (e.g. from a PKI or Kerberos service) to determine user permissions

OPSEC

a proprietary (Checkpoint) protocol which provides interoperation among multiple security products

IPSec, ISAKMP and SKIP

open standards which enable secure Virtual Private Networks to be implemented

PKIX and CDSA

open protocols which aim to permit full interoperability between Certificate Authorities

The operational requirements come first…

Adequate security is an absolute pre-condition for responsibly carrying out business transactions online.

It is certainly the case that any organisation deploying information systems needs to consider security issues. However, if the organisation has any online deployment at all, that consideration is essential and it is not overstating the case to say that adequate security is an absolute pre-condition for responsibly carrying out business transactions online.

What constitutes "adequate" security? Inevitably, "it depends". In fact, it depends on basic system design as well as on the security inherent (or not) in the component applications and any additional security provisions. The system design issue has to do with ensuring that sensitive data and sub-systems are capable of being protected.

To take a naïve case: if a web server carries confidential data in order to handle web user requests (customer credit status, for example), it is inherently more difficult to guard that data than if it is carried on a system which is protected by the site firewall. This requires implementing a dialogue between the external, vulnerable web server and the internal, secure system.

At the other end of the scale, if a web site is totally passive, carrying only "brochure" material, the risks associated with going online may be limited to the "corruption" (e.g. defacing) and "Denial of Service" cases. However these are not trivial matters – for example, obscene material posted on a web site could damage the corporate image, even though it is not in the same league as breaches of the confidentiality of customer account data on a banking system.

There is no avoiding the threat-risk analysis: it is the essential precursor to any consideration of specific countermeasures.

There is no avoiding the threat-risk analysis: it is the essential precursor to any consideration of specific countermeasures. Today's operational requirements, however, include the use of "security" technologies to enable new kinds of networked business. The cryptographic technologies now available can be used to permit secure access to an enterprise's system assets through the rigorous authentication of external as well as of internal system users. Digital Certificates are the means by which these trusted relationships are established: the creation and management of these certificates is now a further demand to be met by system managers.

At all stages – procurement, deployment and operation – it is important that the products and techniques adopted be matched to the specific operational requirements of the organisation: there are absolutely no (honest) “one size fits all” propositions in the IS security shopping mall.

There are absolutely no (honest) “one size fits all” propositions in the IS security shopping mall.

When the analysis has been completed, the cost of building the secure environment can be assessed. The cost of acquisition of the required specialised products is likely to be exceeded by the cost of deployment and this in turn will certainly be exceeded by the ongoing cost of managing those products.

...but the business case is what counts

With almost everything in IT, the ongoing cost of ownership of a technology is likely to have a present value which far exceeds the initial cost of acquisition and deployment.

In the case of a security implementation, existing ongoing costs will typically figure very prominently in any evaluation of achievable Return On Investment.

Most enterprises have already made significant investments in security, ranging from features which are embedded in diverse operating systems and application software suites, through add-in products like virus detection/prevention to discrete, site-wide firewalls and perimeter access controls. Such sub-systems are probably autonomous, resulting in the existence of multiple access control lists, password directories and the like.

In the past, before new sub-systems could come on stream, the IS security manager had first to ensure that the security policy formulated (after performing the threat-risk analysis) was implemented consistently across the diverse operating systems and application suites already referred to. This implementation (and all subsequent maintenance and policy amendment actions) has been all too likely to involve “touching” a large number of devices, from system components like firewalls, routers and servers down to individual workstations and PCs. For example, when an employee leaves, it is necessary to delete their permissions from all directories and Access Control Lists with which they have been involved.

It is the ongoing burden of multi-platform/multi-suite maintenance which, at the least, gives “security” a bad name and which, at worst, invalidates the investment proposal.

Security products are changing to meet the new requirements:

Design and implementation

Once a security policy has been evolved, it should be possible to implement that policy across all system components in a consistent manner, based on clearly articulated rules.

- Once a security policy has been evolved, it should be possible to implement that policy across all system components in a consistent manner, based on clearly articulated rules.
- This capability dramatically reduces the effort required first to implement the policy and subsequently to modify it in the light of changing business requirements.

Operation

In operation, routine changes to user permissions, for example, should be achievable across all systems, devices and processes through a single action.

- In operation, routine changes to user permissions, for example, should be achievable across all systems, devices and processes through a single action.
- Not writing permissions (access control and authentication) into each application but establishing a central point for policy management again results in reduced effort and hence much better ROI.

There is a new security paradigm

The needs identified above have become ever more obvious in recent years and a number of system vendors have addressed one or more aspects, often by the insightful adoption of related standards, whether open or proprietary.

Initiatives in:

- Inter-operation among multiple security components
- Integration of security processes with enterprise directories
- Centralised management of Access Control Lists
- Tackling the inherent insecurity of the operating system itself

have all been the subject of product releases from both security specialists and general system vendors. Most modern security products now interoperate using well-defined standard protocols and this allows "best of breed" products to be integrated. Increasingly, partnering relationships with companies like Finjan (content filtering for malicious code) and Content Technologies (email filtering) are significant for the newer security products.

Now that it is feasible to build aggregated security systems, the industry has developed multi-function perimeter gateways and security suites. Prominent among these are "SecureWay" from Tivoli, "AccessMaster" from Bull and "Border Manager" from Novell.

The industry has developed multi-function perimeter gateways and security suites. Prominent among these are "SecureWay" from Tivoli, "AccessMaster" from Bull and "Border Manager" from Novell.

Whatever the technologies, buzzwords and acronyms involved, a common goal of these new security products is to reduce design and implementation costs, operating cost and operating risk by centralising security management. Once this has been achieved, the mechanisms are available to manage security through explicit policies which, defined and maintained centrally, are propagated out to the set of compliant security sub-systems. In such an environment, a change in policy can be implemented automatically through a single high-level action rather than manually on each component system.

A change in policy can be implemented automatically through a single high-level action rather than manually on each component system.

Bert van Wijk, an IT Project Manager at KLM, who has recently worked with such a product, said:

"Centrally managed access control enables us to administer and, more importantly, revoke access rights across multiple applications from a single point. Previously, administration and revocation of a user's access rights required operations across multiple systems separately... (The) central management allows for reduced TCO while removal of the need to write 'permissions' – identification and access control – into each application by the introduction of a central policy scheme improved the ROI."

Conclusions

While security technologies have progressed rapidly in recent years (especially in the sectors amenable to cryptographic solution), understanding of the relevance and cost-effectiveness of the available solutions has not kept pace.

"Security" actually enables new kinds of business process.

The business pressure to extend online access to partners, customers and others suggests an alternative view in which "security" actually enables new kinds of business process.

This paper distinguished between a situation which is typical in today's enterprise systems – (more or less) secure components – and the more recently developed type of solution: based on a security policy, implemented via explicit rules and operated in conjunction with efficient system-wide directory services – to produce a secure enterprise.

The central goal of modern security design is to use explicit management tools to:

(1) ensure the ongoing integrity of the systems —
so meeting the security objective itself

(2) reduce the costs of both implementation and operation —
so reducing Total Cost of Ownership and generating a better Return On Investment.

We conclude that current, integrated solutions – dealing with both site and traffic issues through a coherent, policy-based structure – warrant close attention by organisations whose existing systems are implemented at the component level.

Tivoli

Tivoli Systems Information Centre
PO BOX 20, B-1070
Anderlecht, Erasmus, Belgium
Tel +32 702 33475 Fax +32 702 33476
www.tivoli.com

IDC

Corporate Headquarters
5 Speen Street
Framingham, MA 01701
508-872-8200

IDC Irvine
2171 Campus Drive, Suite 100
Irvine, CA 92612
714-250-1960

IDC Miami
Latin America Headquarters
5301 Blue Lagoon Drive
Suite 490, Miami, FL. 33126
305-267-2616

IDC New Jersey
120 Wood Ave South, Suite 509
Iselin, NJ 08830
732-632-9222

IDC Texas
100 Congress Ave, Suite 2000
Austin, TX 78701
512-469-6333

IDC West
2131 Landings Drive
Mountain View, CA 94043
650-691-0500

IDC Argentina
Trends Consulting
Lavalle 715 - Piso 7 B
CP 1047 Buenos Aires
Argentina
54-1-322-3159

IDC Asia/Pacific
Suite 2901-02, 29/F
Universal Trade Center
3 Arbuthnot Road, Central
Hong Kong
852-2530-3831

IDC Australia
Level 4, 76 Berry Street
North Sydney, NSW 2060
Australia
61-2-9922-5300

IDC Austria
c/o Loisel, Spiel, Zach Consulting
Mayerhofgasse 6, A-1040
Vienna, Austria
43-1-50-50-900

IDC Beijing
Suite A18, Yintai Office Bldg.
A-137, Xizhimen Wai Dajie
Beijing 100044, PRC
86-10-6833-1179

IDC Benelux
29 Avenue Louis Gribaumont
B-1150,Brussels, Belgium
32-2-779-46-04

IDC Brazil
Alameda Ribeirão Preto,
130 cj 41, 01331-000 São Paulo
SP Brazil
55-11-253-7869

IDC Canada
36 Toronto Street, Suite 950
Toronto, Ontario
Canada M5C2C5
416-369-0033

International Data Corp. Chile
Luis Thayer Ojeda 166 Piso 12
Providencia, Santiago 9
Chile
56-2-231-0111

IDC Colombia
Carrera 90 No. 156-19, Piso 5
Santafe de Bogota, Colombia
571-680-3100

IDC East Central Europe
Korenskeho 7
150 00 Praha 5
Czech Republic
420-2-544-073

IDC Egypt
39 Iraq Street
Mohandesseen, Cairo, Egypt
20-2-336-9379

IDC Finland
John Stenbergin ranta 2
FIN-00530
Helsinki, Finland
358-9-7016377

IDC France
Immeuble La Fayette
2, Place des Vosges
Cedex 65
92051 Paris la Défense 5 France
33-1-49-04-8000

IDC Germany
Westerbachstr. 23A
61476 Kronberg/Ts.
Germany
49-6173-7098-0

IDC Hungary
Bajcsy-Zsilinszky út. 57
Building 3, Rooms 103-104
H-1065 Budapest, Hungary
36-1-153-0555/ext. 165, 166

IDC India
206, 207, Saraswati House
27, Nehru Place
New Delhi 110 019, India
91-1-6419754

IDC Israel
134 Rothschild Blvd.
Tel Aviv 65272, Israel
972-3-685-8093

IDC Italy
Viale Monza, 14
20127 Milano, Italy
39-02-284571

IDC Japan
10F The Itoyama Tower
3-7-18, Mita Minato-ku
Tokyo 108-0073, Japan
81-3-5440-3400

IDC Korea Ltd
13th Floor, Textile Center
944-31,Daechi-3Dong
Kangnam-Ku, Seoul, Korea
82-2-528-5100

IDC Malaysia
Suite 23.1 23rd Floor
Menara Genesis
33 Jalan Sultan Ismail
50250 Kuala Lumpur, Malaysia
60-3-244-3715

IDC Mexico
Select - IDC
Av. Nuevo Leon No. 54 Desp. 501
Col. Hipodromo, Condesa
C.P. 06100 Mexico, D.F.
525-256-1426

IDC Netherlands
A. Fokkerweg 1
1059 CM Amsterdam
The Netherlands
31-20-669-2721

IDC New Zealand
Level 4
43 High Street
Auckland, New Zealand
64-9-309-8252

IDC Nigeria
House 2, 'C' Close
403 Road, 4th Avenue
New Extension, Festac Town
Lagos, Nigeria
234-1-883585

IDC Poland/ProMarket
Wrobla 43
02-736 Warszawa, Poland
4822-644-4105

IDC Portugal
c/o Ponto de Convergencia S.A.
Rua Leopoldo de Almeida 4A
1750 Lisbon, Portugal
351-1-758 31 26

IDC Russia
c/o PX Post, RDS 186
Ulitsa Zorge 10
Moscow 125525
Russian Federation
7-501-929-9959

IDC Scandinavia
Jagtvej 169B
DK-2100 Copenhagen
Denmark
39-162222

IDC Singapore
72 Bencoolen Street #02-01
Singapore 189643
65-226-0330

IDC South Africa
c/o BMI-TechKnowledge
3rd Floor, 356 Rivonia Blvd.
PO Box 4603
Rivonia, 2128, South Africa
27-11-803-6412

IDC Sweden
Box 1096 Kistagången 21
S-164 25 Kista, Sweden
46-8-751-0415

IDC Taiwan
8F-3, #547
Kuang Fu South Rd
Taipei, Taiwan, R.O.C.
886-2-2729-6040

IDC Thailand
27 Soi Charoen Nakorn 14
Charoen Nakorn Road
Klongtonsai, Klongsan Bangkok
10600, Thailand
662-439-4591-2

IDC Turkey
Tevfik Erdonmez Sok.
2/1 Gul Apt.
Kat 9D; 46 Esentepe
Istanbul, Turkey
90-212-275-0995

IDC U.K.
6 Dukes Gate, Acton Lane
Chiswick, London W4 5DX
United Kingdom
44-181-987-7100

2 Bath Road
Chiswick, London W4 1LN
United Kingdom
44-181-987-7100

IDC Venezuela
Trends Consultores
Av. Francisco de Miranda
Centro Perú, Torre A, Piso 9
Of. 91, Chacao 1060
Caracas, Venezuela
582-261-0352

IDC Government
3110 Fairview Park Drive
Suite 1100
Falls Church, VA 22042
703-876-5055

Version 1.0 February 2000