A Model for Secure Data Sharing Between Different Security Level Networks

Article *in* Computer Engineering & Information Technology · January 2017

DOI: 10.4172/2324-9307.1000163

Mehmet Kara
The Scientific & Technological Research Council of Turkey

Kara, J Comput Eng Inf Technol 2016, 6:1
DOI: 10.4172/2324-9307.1000178

Journal of Computer Engineering & Information Technology

Research Article

A SCITECHNOL JOURNAL

A Model for Secure Data Sharing Between Different Security Level Networks

Mehmet Kara*

Abstract

Most of the data is processed in information systems every day. This leads to easy transmission, share, process, access and save data. Conventional security precautions such as firewall, IDS/IPS, antivirus, VPN are not enough for data sharing between classified networks and internet. Efficient and effective data sharing is very important in different security level networks. A few special solutions are developed for connecting different security level networks but they cannot be applied to all types of network connections. Each different security level network precautions must be diversified according to security level. In this paper a comprehensive model is developed for connecting different security layer networks which describe technical and managerial security requirements and network topology for every secret level network, data information flow scenarios for organizations and security controls for different security level networks.

Keywords

Security; Information security classification; IEG; Data sharing

Introduction

A government organization, military organizations, private companies and personnel data is transferred from paper to information systems. Information systems provide easily transmit, save, access and share for all data. E-government projects are getting increased this lead to more data sharing between organizations. For example ministry of Justice, ministry of health, ministry of finance, gendarme and police departments need to share their data with other organizations. But all of these data is not unclassified and needs high level security. Classified information is shared off line storage medial (CD/DVD, Hard disk etc.). But this method is very slow and it is not sufficient for online connections. Some organizations use leased line or private connections to provide online communications and data sharing. It is required to have one leased line connection for each organization which increases management effort and communications expenses. In addition to technical limitations there are not enough security solutions, comprehensive regulations and laws about online data sharing.

Main purpose of unclassified and classified data sharing is to give an opportunity to produce new economic profit, new information useful for community. There is an increment at government organizations data sharing between and across all levels of government to help other organizations process and build a comprehensive consistent picture of the status, society and the environment. In addition to including a lot of opportunities, data sharing require strict security precautions key to security level. Data privacy, trade secrets, personnel information, government secrets, intellectual properties must be protected. Countries should arrange some laws and regulations for government data sharing but they are not covering all concepts [1].

Information which is processed, transmitted and saved at computer networks needs some precautions according to its security level. However data transfer and information sharing is a real necessity of computer networks. Even if these networks are the same security level they cannot be connected because of they are under control of different organizations. Organizations are requested to have additional technical and managerial security measurements. In this paper different security level networks connection take up consistent and comprehensive approach. Our contribution; define technical and managerial security requirements and network topology for each secret level networks; data information flow scenarios for organizations; defining security controls for different security level networks.

Today different security networks connection requirements can be stated following:

- ➢ Government Networks -> Government Networks
- ➢ Government Networks -> Citizen
- ➢ Government Networks -> Military Organization
- ➢ Government Networks -> Foreign Country Organization
- ➢ Military Organization -> NATO

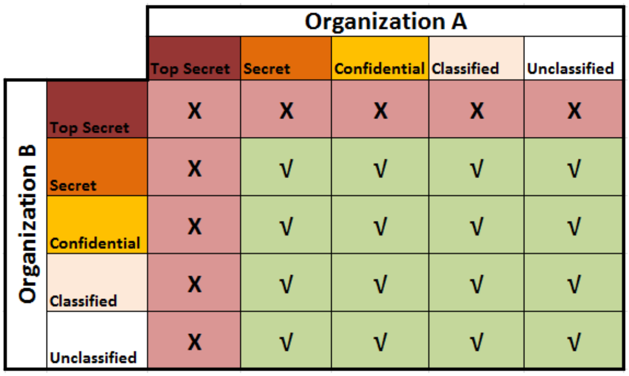
(According to security level different connection combinations are showed at Error! Reference source not found [1] (Figure 1). These connections are addressed up to Secret networks. There is no real solution for Top Secret network connections. So this paper does not include Top Secret network security requirements and connection scenarios. While two different security level networks have been connected, higher security level network requirements must be considered and Information Exchange Gateway (IEG) is the most important part of this connection because other security solutions are used common computer networks. The paper is organized as follows. Section II, provides literature reviews. This chapter focuses on connection of different security level network. In Section III, we gave information about Information Exchange Gateway (IEG) solutions. We dealt with security requirements of different Security Level networks connections Section IV. Information flow and security controls for different security level networks are explained at Section V. Conclusions and future work summarized in Section VI.

Literature Review

National and international information system operations carried out with organizations from different nations and in partnership with organizations in order to achieve the operational objectives. Data sharing between different security level network and organizations

***Corresponding author:** Mehmet Kara, Sistem Bilgisayar, Korfez Mah. S. Rafet Karacan, Sok. No: 2441100, Izmit, Kocaeli, Turkey, E-mail: mehmet29@hotmail.com

Received: October 31, 2016 **Accepted:** December 12, 2016 **Published:** December 21, 2016 *doi: 10.4172/2324-9307.1000178*



		Organization A				
		Top Secret	Secret	Confidential	Classified	Unclassified
Organization B	Top Secret	X	X	X	X	X
	Secret	X	√	√	√	√
	Confidential	X	√	√	√	√
	Classified	X	√	√	√	√
	Unclassified	X	√	√	√	√

Figure 1: Different security level network connection combinations.

is very important requirement. These operations are described as Network Enabled capability (NEC) at NATO systems. So NATO tries to develop secure and reliable data sharing infrastructures and solutions different security level networks [2]. NEXOR developed IEG reference guide for NATO different security level connection which is include IEG concepts NATO connection requirements connections suggestions for NATO systems. Bu this model include NATO requirements and connection scenarios [3].

Boonstra et al. developed a model for different security level network security requirements which is divided the smallest part security solutions such as firewall, IDS, IPS then described security functions of at each point. This model creates minimum security requirements for all networks that lead to minimum device maximum security and easy management. Because there is no accepted properties today security solutions. For example a firewall can be known packet filtering devices but in the real life some firewalls include antivirus system, IDS, IPS, content filtering etc. [4].

Many XML labeling and Meta data based solutions are developed for different security level networks. NATO developed two protection profiles and security device for XML labeling which are Medium Assurance XML Labeling and High Assurance ABACV Guard [5-7]. NEXOR developed a reference model for NATO information exchange between shareholders [1,3]. That model give information about high level overview of NATO Information Exchange Gateway and its usage scenarios. The model consists of four components which are information exchange, IEG management, information management, node protection.

Reference model described five different connection scenarios. The scenarios consider security classifications of connected different domains in addition to security policy, connection types and administrations of those domains. Scenario 1 describes the same security level and the same authority. Scenario 2 describes the same security level but different authority. This scenario includes also connecting different level security but the same authority. Scenario 3 covers NATO missions systems to other systems. Scenario 4 describes NATO system to international organizations. Scenario 5 describes to NATO systems to Internet. Coverage of these scenarios are very wide so it is not easy to cover all scenarios with one IEG device.

In addition to NEXOR IEG capabilities Apiecionek et al. developed a solution which is supports many protocols such as Extensible Messaging and Presence Protocol (XMPP), FTP and HTTP [8]. Serrano et al. examined data sharing difficulties between NATO and shareholders. At this examination they deal with data, sharing protocol, connection devices, sharing scenarios and suggested different solution for different scenarios. They suggested a road map for NATO data sharing [9]. Military and other defense organizations classified networks security and real time data sharing requirements are examined. At the same time basic capabilities of Ezenia InfoWorkSpace and Multi Level Security relation investigated [10].

Dean et al. investigated data sharing without air gap solutions between high security network and low security network. This solution includes format control, network layer control (IP, port, network) and user authorizations techniques. QinetiQ Company worked about two way secure data transfer technologies for United Kingdom Ministry of Defense [11]. James and all worked about secure data sharing on Cloud [12].

Assenco Poland designed Multi Level Security System which provides a secure communication between secret military networks and public networks. This system was designed at Service Oriented Architecture (SOA) model [13,14]. Heath data sharing is very important for government, public organizations and researchers. There are many tools for keeping and sharing health data but none of them provide a complete solution for secure sharing of this data. But secure and flexible architectures are searched using standards. Harris et al. designed a system for secure health data sharing between government organizations, finance organizations, universities and hospitals [15]. Chen et al. worked about network security and perimeter protection design for China industry and governmental organizations that they deal with designing security protection and perimeter protection devices [16]. In addition to security protection and perimeter protection devices this design covers security standards and policies.

Celeseti et al. developed a secure data exchange and service representation model for IaaS cloud services. In this model a cloud request a virtual machine resources another cloud with secure connection using Dataweb and XDI Technologies [17]. Harada et al. described a secure data exchange service using by proxy server. According to this patent client communicate with server over a proxy. Client request service form proxy then proxy establishes a secure connection with server. Digital signature and strong authentication are used in this communication [18].

Liu and Chetal developed a trusted based secret data sharing model and implementation for government agencies. In this model they analyzed cause of information sharing problems, then interest based trust model and protocol; finally they implemented a model and protocol for XML web services. XML provide very useful structure for data sharing between government agencies. Every organization can be define its XML structures and transmit via HTTP or other protocols. This model is completely suitable with Federal Enterprise Architecture (FEA) and integrated to E-Government systems [19]. This paper dealt with comprehensively information sharing between government authorities. Lack of trust is the most important reason for not data sharing between government authorities. Win win policy, legal regulations and common benefit shall be created to build a trust between government organizations.

Federal Enterprise Architecture version 2 was published at 2012 by US government to promote coordination between government, industry, citizen and other parties. This document dealt with a suite of tools to help government organizations implement and align the approaches. FEA includes strategy, business, data, application, infrastructure, security domains. FEA document dealt with conceptual security and general security requirements such as using standards for national or organizational policy, select control at organizational level, enforcing design and control at organization level [20].

IEG systems

Conventional security solutions (Firewall, IDS/IPS, VPN, Antivirus etc.) are not secure enough to connect different security layer network connections. So special solutions are developed for these types of connections. Flow control, air gap, and data diode technologies are used for connecting different security level networks [21].

Flow control technologies control the content of data between communications to system that control applied at application level at computer networks. When flow control system connection is used to connect two different security level networks it checks every bit of data to prevent and detect malwares, DoS attacks and other type attacks. Flow control technology is stated Guard at some paper and reference documents. Flow control looks like firewall, router device ahead of these include application security, malware control, data labeling and classification functions. Flow control system allows only suitable traffics between different security level networks according to organizational policy and rules.

Data diode provides one way physical data communication (send or receive) between two different security level networks. It is possible to send data one way from low level networks to high level networks. According to data transfer direction either transmit or receive line is cut. Some data diodes uses two level communication: First diode receives data coming from outside secondly diode sends the data to external server. This causes some delay at data communication but provide more secure communication. Typical data diode architecture is shown at Figure 2.

Air Gap connects two physically isolated different security level networks. Air Gap system which consist of three part: external site (a secure computer), internal site (a secure computer) and shared disk system. This system provides a secure network traffic flow between two different security level networks in order to realize critical operations fundamentally by preventing transit IP traffic. Security comes from physical, electromagnetic or electrical separation of these networks. Air Gap security could be equal to off line data transfer security such as diskette, CD, USB etc. General Air Gap architecture is shown at Figure 3.

Security requirements of different security level networks connections

There is no conceptual solution for connection different security level networks at literature. Generally focused on special connection like Information Exchange Gateway (IEG), content security solution etc. Connection of different security level is examined both technically and management at this paper.

Network connection vulnerabilities, threats and risks

Vulnerabilities are weak points in computer networks that might be exploited by hackers. Risks are the potential results of unconsidered vulnerabilities. For example unpatched database server includes vulnerability which might be used by threats and causes risks. These risks lead to loss of data, money, prestige and the more important things. So computer network should be checked for vulnerabilities, threats and risks before then connection to other networks. This risks evaluation must be done not only on connection devices but also on all systems. Before then network connection all risks must be decreased to the acceptable level. Threats and risks for network connections are shown at Table 1.

General security requirements for different security level networks

There is no general comprehensive requirement for different security level network connection at literature. Solutions generally focused on special areas of this connection such as Air Gap, Diode, Content Security, Perimeter Protection etc. In this paper a comprehensive model is suggested which includes all technical and manageable subjects.

While protecting classified information confidentiality, integrity and availability at data sharing some technical and management security precautions must be considered. Following technical and managerial security precautions must be taken to provide comprehensive network security (Hata! Başvuru kaynağı bulunamadı.) (Table 2). Security level of network is defined according to importance of processed, saved and transmitted data at network. So different level networks security requirements are different. When two different security level networks are connected firstly risk analysis must be done then technical and management security precautions must be defined.

Network security classifications and security precautions

Information is classified five levels at military and governmental organizations; unclassified, classified, confidential, secret and top secret. At this paper we deal with only unclassified, classified, confidential and secret. Top secret security level requirements are not published by nation so we did not mentioned top secret security requirements.

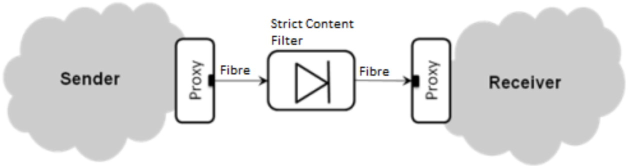


Figure 2: Data diode architecture.

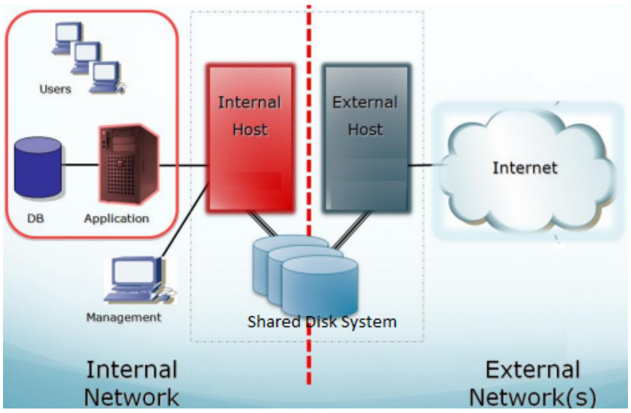


Figure 3: General Air Gap architecture.

Table 1: Threats and risks for network connections.

Threat Explanation	Risk Explanation
Unauthorized access to protected data by users (Internal and external), systems and malwares	When two different protected networks are connected this connection is increase attack surface each network. Confidentiality, integrity or availability of protected data could be damaged.
Internal and external evil users use software, hardware vulnerabilities that they are used for network connection.	Damage of confidentiality, integrity and availability of source network information. Unauthorized access to the internal information system from vulnerable connection
Unintentionally or intentionally misuse of shared data type or data resources at network connections.	Uncontrolled/unapproved data sharing between connected networks
It is difficult to control contents of data while transferring online	Sharing of inappropriate this is technically suitable for sharing but its content not suitable for unauthorized systems. Garbage or unclassified data sharing.
Reputation of lawful responsibilities or not applied technical and management precautions for shared data	Organizations which produced and provided data could be damaged because of data shared organization mistakes.
Vulnerabilities of network connection devices can be misused by hacker.	Unauthorized access to network connection devices. This effects the availability,
Confidentiality/security level criteria differences. A threat that comes from minimum security precautions applied to networks.	Ignorance of other network technical and operational security requirements which is not understand or deal with correctly.

Table 2: Technical and managerial security precautions.

Security Precaution	Technical	Managerial
Secure Network Architecture	√	
Firewall	√	
Malware Protection	√	
Intrusion Detection and Prevention	√	
Content Security	√	
Router	√	
VPN	√	
Access Control	√	√
Authentication	√	
Secure Configuration	√	√
Security Event Management	√	
Audit logs	√	
Information Exchange Gateways	√	
Security Awareness and Training		√
Physical and Environmental security	√	√
Configuration Management	√	√
Business continuity		√
CERT		√
Maintenance	√	
Portable media security	√	
Personnel Security		√

Unclassified network security requirements

Unclassified networks include public information this means this information can be seen by anybody. Network security architecture is used to provide business continuity access control. In this architecture Demilitarized Zone (DMZ) is used for external data access and there is no direct access internal network. Unclassified network architecture and security requirement is shown at Figure 4.

Classified network architecture and security requirements: Classified information is sensitive and could not be shared with other parties. Classified information should not be disclosed without the permission of the personnel or group. When this information disclosed uncontrolled way organization lost money and prestige. Information security level label is given by owner of data. The owner designate who can be use this information. Internal documents, reports, research and development plans, results and project plans can be evaluated as classified information. Remote user can be access to network resources with VPN solutions. To provide defense in depth classified information (databases) is not accessed directly this servers are accessed throughout to application servers. Classified network architecture and security requirement is shown Figure 5.

Confidential network architecture and security requirements: Confidential information is very important for organizations or personnel. Unauthorized disclosure of this information could adversary effect the organization or personnel. If this information reveals uncontrolled way foreign country or illegal organizations could provide benefit. On the other hand owner of information can lose great amount of image or money. Personnel health information, personnel identity information and organization private information could be evaluated confidential information. To provide security at confidential network architecture many technical and management security precautions applies such as security product evaluation, data encryption, secure communication etc. Confidential network architecture and security requirement is shown Figure 6.

Secret network architecture and security requirements: The unauthorized disclosure of secret information could lead to serious damage to organization or the country. While personnel or organization information have been saving in secret networks, unauthorized personals could not be access, change or delete information. Defense in depth approaches is used in this networks and secure access can be provided to the information internal or external networks via VPN devices or other secure remote access

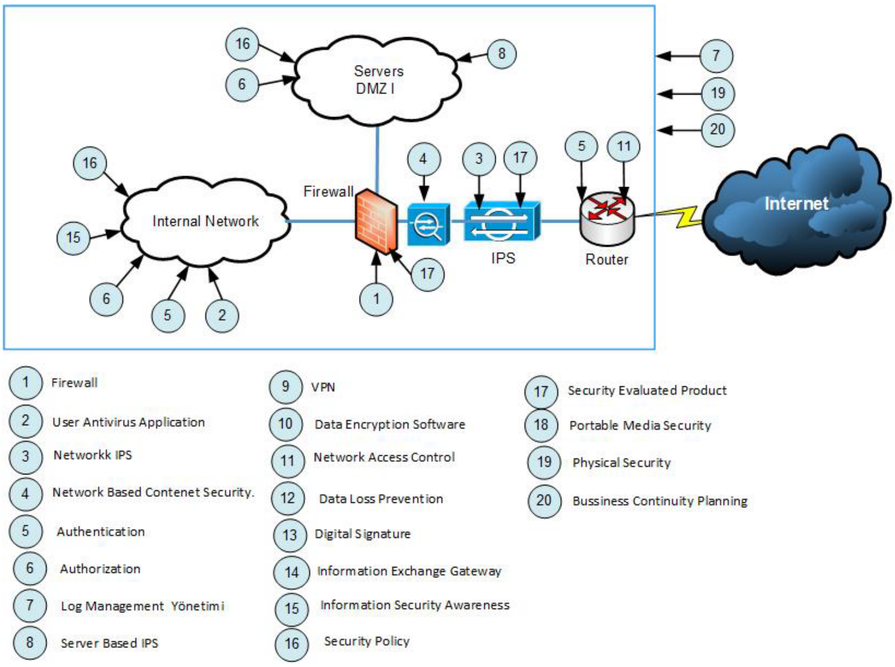

Servers
DMZ I
Internal Network
Firewall
IPS
Router
Internet
1 Firewall
2 User Antivirus Application
3 Networkk IPS
4 Network Based Content Security.
5 Authentication
6 Authorization
7 Log Management Yönetimi
8 Server Based IPS
9 VPN
10 Data Encryption Software
11 Network Access Control
12 Data Loss Prevention
13 Digital Signature
14 Information Exchange Gateway
15 Information Security Awareness
16 Security Policy
17 Security Evaluated Product
18 Portable Media Security
19 Physical Security
20 Bussiness Continuity Planning

Figure 4: Unclassified network architecture and security requirements.

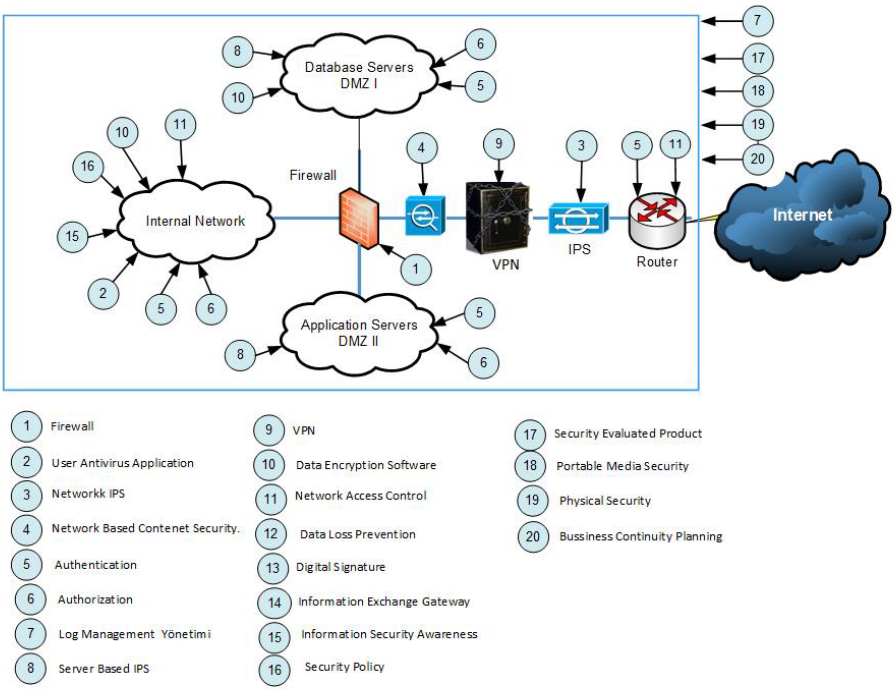

Database Servers
DMZ I
Internal Network
Firewall
VPN
IPS
Router
Internet
Application Servers
DMZ II
1 Firewall
2 User Antivirus Application
3 Networkk IPS
4 Network Based Contenet Security.
5 Authentication
6 Authorization
7 Log Management Yönetimi
8 Server Based IPS
9 VPN
10 Data Encryption Software
11 Network Access Control
12 Data Loss Prevention
13 Digital Signature
14 Information Exchange Gateway
15 Information Security Awareness
16 Security Policy
17 Security Evaluated Product
18 Portable Media Security
19 Physical Security
20 Bussiness Continuity Planning

Figure 5: Classified network architecture and security requirements.

tools. For example access to databases server that information is saved provided by via application servers. In additional to different security precautions there are a lot of DMZ at architecture (Figure 7).

Information flow and security controls for different security level networks

Network security classifications and security precautions: While connecting different security level networks, security precautions are very important such as information leakage, covert channel, network attacks, changing security labels, security policies and directives. When two networks are connected higher security level network security requirements must be implemented. Information Exchange Gateways (IEG) role is very important in this type connections that they are provide main security. Main security levels and connections

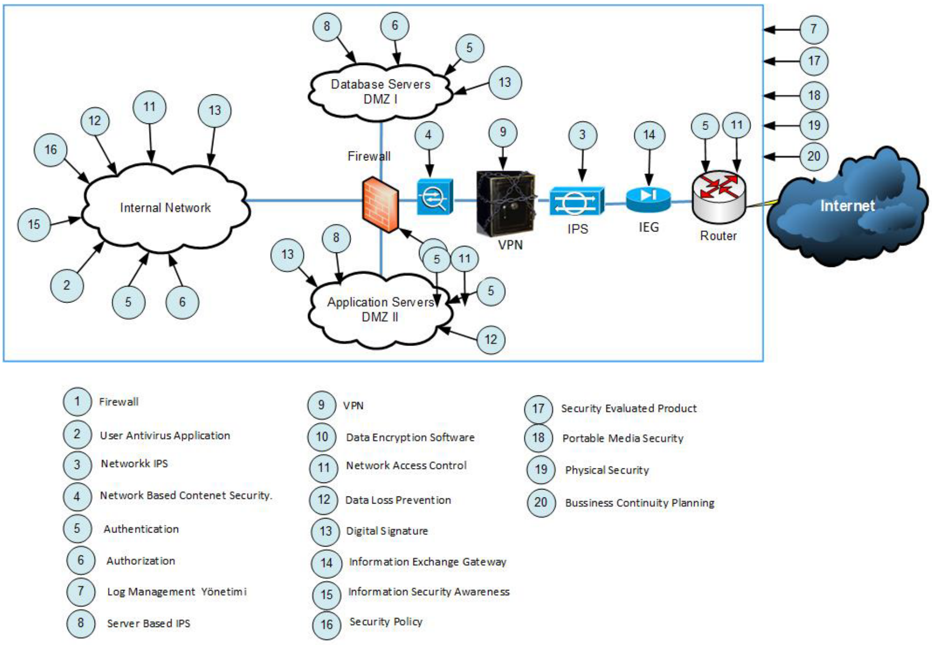

Database Servers DMZ I
Internal Network
Firewall
VPN
IPS
IEG
Router
Internet
Application Servers DMZ II
1 Firewall
2 User Antivirus Application
3 Networkk IPS
4 Network Based Contenet Security.
5 Authentication
6 Authorization
7 Log Management Yönetimi
8 Server Based IPS
9 VPN
10 Data Encryption Software
11 Network Access Control
12 Data Loss Prevention
13 Digital Signature
14 Information Exchange Gateway
15 Information Security Awareness
16 Security Policy
17 Security Evaluated Product
18 Portable Media Security
19 Physical Security
20 Bussiness Continuity Planning

Figure 6: Confidential network architecture and security requirements.

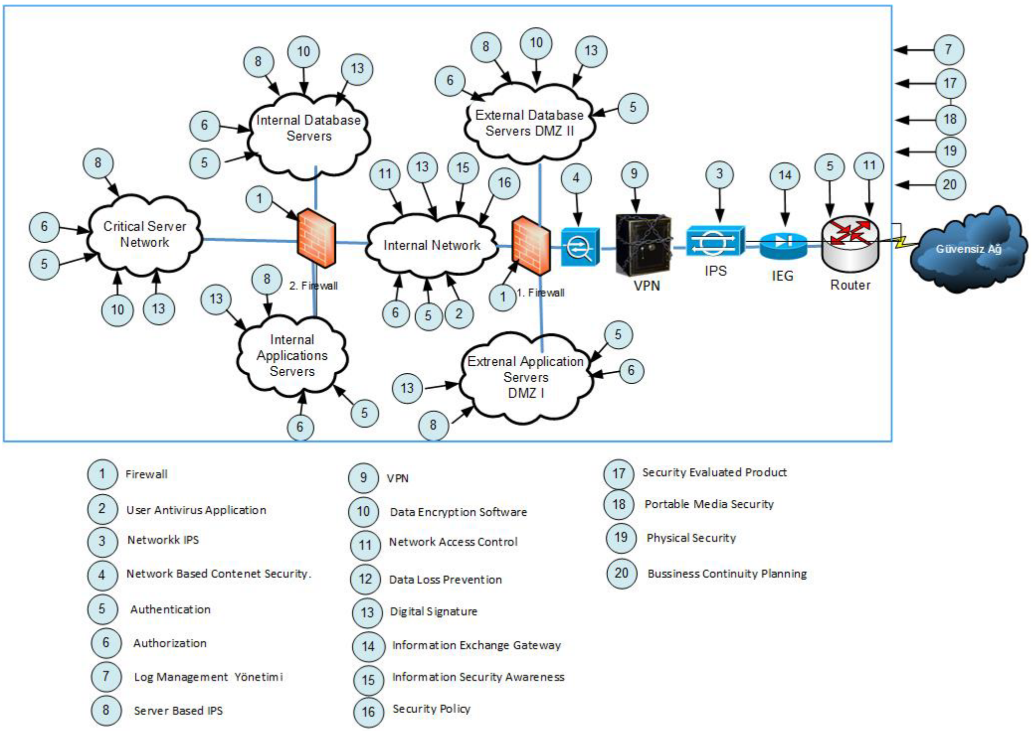

Internal Database Servers
External Database Servers DMZ II
Critical Server Network
Internal Network
2. Firewall
1. Firewall
VPN
IPS
IEG
Router
Güvensiz Ağ
Internal Applications Servers
Extrenal Application Servers DMZ I
1 Firewall
2 User Antivirus Application
3 Networkk IPS
4 Network Based Contenet Security.
5 Authentication
6 Authorization
7 Log Management Yönetimi
8 Server Based IPS
9 VPN
10 Data Encryption Software
11 Network Access Control
12 Data Loss Prevention
13 Digital Signature
14 Information Exchange Gateway
15 Information Security Awareness
16 Security Policy
17 Security Evaluated Product
18 Portable Media Security
19 Physical Security
20 Bussiness Continuity Planning

Figure 7: Secret network architecture and security requirements.

scenarios are showed in Figure 8 which includes six different scenarios described.

Scenario A: The same security level network is connected under the same organization. These networks are operated according to the same policy but they have different physical locations.

Scenario B: The same security level network is connected under the different organization. These organizations security policies and precautions are the same but operated by different authorities. Connection of secret level network at two shareholders can be given an example to scenario B.

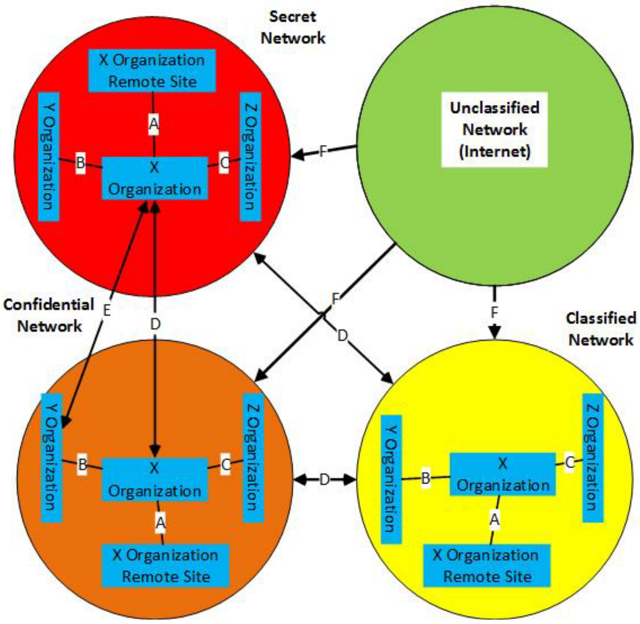


Figure 8: Secure network connection scenarios.

Scenario C: The same security level network is connected under the different organization. These organizations security policies and precautions are different and operated by different authorities. Connection of secret level network at two shareholders can be given an example to scenario c.

Scenario D: Different security level network is connected under the same organization. These organizations security policies and precautions are different and operated by the same authorities. Connection of secret level network at two shareholders can be given an example to scenario D.

Scenario E: Different security level network is connected under the different organization. These organizations security policies and precautions are different and operated by the same authorities. Connection of secret level network at two shareholders can be given an example to scenario E.

Scenario F: Different security level network is connected internet in this scenario. This connection is one way because of preventing data loss from secure network. This connection is used download public information such as meteorology information. Integrity and availability of higher security level networks can be provided controlling accesses from only white list devices which are came from lower security level networks. General security controls such as Viruses scanning, content checking, port control etc. can be provide by external security solutions at information follow system. Confidentiality of information can be providing permitting only tagged messages. After that point we focused on connection of different security level networks which are controlled different authorities.

Information sharing and classification

While sharing information between two organizations, the first issue is to determine the shared data. Depending on the operating situation, the purpose of sharing information should be defined and sharing information should be classified. The common security criteria should be identified between organizations. While defining these criteria risk analysis, common operating procedures, standard and formats, protocols, common networks, certified products, security test policies, accreditation must be considered. These concepts are explained following heading. In many cases the information is automatically collected and shared in specific situations. These sharing could be done manually. Therefore, data collection methods and collection status should be defined explicitly.

Risk analysis

In the security context risk is the possibility multiplies effect of threats. Purpose of risk analysis process to define threats and vulnerabilities to IT assets. It is not at all possible to have 100-percent secure IT systems. Every IT system has vulnerabilities. The skill is in identifying these threats, evaluating the probability of risks actually occurring and the damage they could cause, and then taking the right actions to reduce the overall level of risk in the IT system. The greatest obstacle in front of limitless data sharing is risks at information systems. Each data sharing connection should be assessed under specific conditions and risks should be evaluated. After this risk evaluation one of the risk avoidance, risk acceptance, risk mitigation and risk outsourcing should be applied every risk. There is not a silver bullet for secure data sharing so each case should be evaluated separately and right precautions should be applied the system. Different security analysis methodologies can be used risk analysis.

Common operating procedures

Propose of common procedure is to govern the data exchange rules. These rules cover when information is released, who is the recipients, how to protect and handle information while they transmit and destination, what is the security requirements of destination IT system. The information sharing organization can arrange a protocol or an agreement. A description of the rules governing the exchange of information. Define how and when information is released, what are recipients expected to do with the information and how to handle and protect the information, while in transit or at the final destination. Common procedures are an integral part of information exchange, as they build the trust required to enable the sharing of potential sensitive information.

Standards and formats

Common standards and data formats are crucial for continuous data sharing and interoperability. Incompatible standards are create problems for useful data sharing so if it is possible international or national standards must be used otherwise organizations must be define a data format for data sharing. Content checking at the application layer is very important. For example Incident Object Description Exchange Format (IODEF) format which is used data sharing between Computer Emergency Response Team.

Data sharing systems and infrastructures

In the ahead of common security system, different layer data sharing is requiring special systems and applications. Some special systems use IEG solutions such as Data Diode, Air Gap and Guard etc. Data sharing requirements should analyze at system design phase. If here is a special system for our requirement that system should be preferred. Otherwise a system should be designed which is minimize the security risks. MISP (Malware Information Sharing Platform) could be given an example.

Protocols: Shareholders can receive and transmit data involved in data sharing so that uses common protocols. In addition to common protocols information confidentiality and integrity should be provided for sent and received data. Some protocols support to transmit multilateral data sharing.

Common networks: According to data security level some data can be transmitted on internet some data can be sent private networks. Each network flow must be defined according to data security level.

Security certified products: Use of secure hardware and software are very important for network connections. Because of test time, budget, know-how requirements customers generally cannot test the security products. So customers prefer certified products. Security certificate guarantees the security properties of products. It means that products are tested and evaluated by accredited laboratories. While connecting two different security level networks importance of requirements is increased.

Security test policies for network connection: Information system security test period and methodology should be defined. Security tests should be planned and applied for perimeter protection devices, servers, active network devices, databases and applications. Security tests could be planned at four levels such as applications, application platforms, operating systems and network

Accreditation of network connection system: Network connection system must be examined by committees which are consisted of each side security experts. After approval of this committee system could be used.

Conclusions and Future Works

Government organizations, military organizations, private companies personnel data are transferred from paper to information systems. Information systems provide easily transmit, save, access and share for all data. The more E-government projects are done the more data sharing is needed between organizations. Conventional security precautions such as firewall, VPN, IDS/IPS are not enough secure to connect different security layer networks. When we try to connect two different security levels network, according to security level of network some extra technical and manageable security precautions are required. Network security requirements are defined as secure network architecture, firewall, malware protection, intrusion detection and prevention, content security, router, VPN, access control, authentication, secure configuration, security event management, audit logs, IEGs, security awareness and training physical and environmental security, configuration management, business continuity, CERT, maintenance, portable media security, personnel security requirements are defined. Security requirements of unclassified, classified, confidential, secret networks are different. While connecting different security level networks information flow scenarios and its security requirements should be dealt with comprehensive perspective.

In addition to security requirements general operating concepts such as common operating procedures, protocols, standards, certified product approach, security testing methodology and accreditation approach are explained. These security requirements can be applied to connection of military, government and public networks. This paper dealt with only connection of different security level networks which are controlled different authorities. In addition to different networks cloud infrastructures (Software as a Service, Platform as a Service, Infrastructure as a Service etc.) are getting popular. These security precautions can be adapted to cloud infrastructures.

References

1. Nexor (2009) Information Exchange Gateways: Reference Architecture.
2. Haakseth R, Nordbotten NA, Jonsson O, Kristiansen B (2015) A high assurance cross-domain guard for use in Service-Oriented Architectures. Military Communications and Information Systems (ICMCIS).
3. Nexor (2015) Secure Information Exchange: Reference Architecture.
4. Boonstra D, Schotanus HS, Verkoelen CAA, Smulders ACM (2011) A Methodology for the Structured Security Analysis of Interconnections. The 2011 Military Communications Conference.
5. Grance T, Hash J, Peck S, Smith J, Korow-Diks K (2002) Security Guide for Interconnecting Information Technology Systems. NIST Special Publication: 800-847
6. Oudkerk S, Bryant I, Eggen A, Haakseth R (2009) A Proposal for an XML Confidentiality Label and Related Binding of Metadata to Data Objects. NATO RTO-MP-IST-091.
7. Wrona K, Oudkerk S, Hallingstad G (2010) Designing Medium Assurance XML-Labeling Guards for NATO. Military Communications Conference.
8. Apiecionek L, Romantowski M, Sliwa J (2011) Safe Exchange of Information for Civil-Military Operations. Military Communication Institute, Poland.
9. Serrano O, Lagadec P, Dandurand L, Jordan F (2013) CIS Security Information Sharing Challenges. NATO NCIA.
10. Ezenia Inc (2007) The Future Evaluation of Multi-Level Security for the Federal Government.
11. Dean T, Wyatt G (2004) Information exchange between resilient and high-threat networks: techniques for threat mitigation. QinetiQ.
12. James JR, Mabry F, Huggins k (2012) Seeing the Real World: Sharing Protected Data In Real Time. 45th Hawaii International Conference on System Sciences.
13. Asseco Poland (2010) Multilevel Security Services. European Defence Agency Project.
14. SSM (2007) “Gizlilik Derecelendirme Kılavuzu” Hazırlama Rehberi.
15. Harris DKhan L, Paul R, Thuraisingham B (2007) Standards for secure data sharing across organizations. Computer Standards & Interfaces archive 29: 86-96.

16. Chen B, Jin B, Zou X (2009) The Security Protection and Control Systems of Network Boundary. The 3rd Research Institute of Ministry of Public Security, China.

17. Celseti A, Tusa F, Villari M, Puliafito A (2012) How The Dataweb Can Support Cloud Federation: Service Representation and Secure Data Exchange. Second Symposium on Network Cloud Computing and applications.

18. Harada LT, Dolecki M, Purdum CS, Hendren CH (2011) Secure Data Exchange Between Data Processing System. US Patent No: US 7,985,446 B2.

19. Liu P, Chetal A (2005) Trusd-Based Secure ınformation Shareng between Federal Government Agencies. Journal of the American Society for Informatıon Science and Technology, 56: 283-298.

20. US Government (2013) Federal Enterprise Architecture Framework V2.

21. Kara M (2014) A Model Different Security Level Network Connections. 7th International Conference on Information Security and Cryptology, Istanbul.

Author Affiliation

Top

Sistem Bilgisayar, Korfez Mah. S. Rafet Karacan, Sok, Izmit, Kocaeli, Turkey