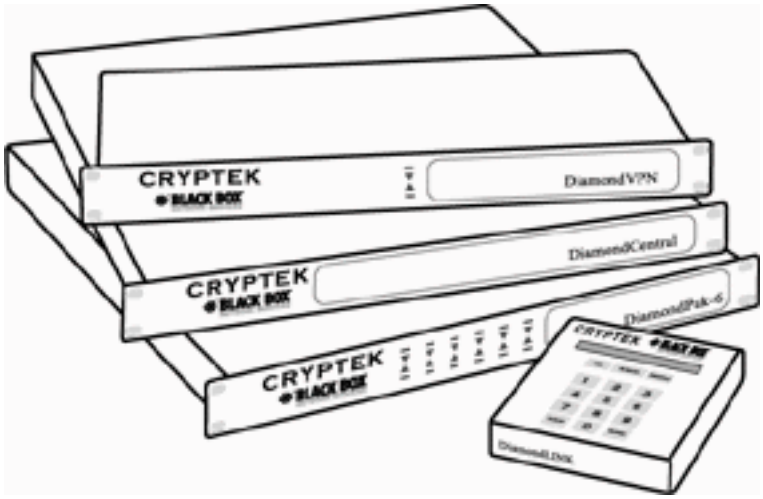
BLACK BOX®
NETWORK SERVICES

Diamond *TEK*

CRYPTEK



Secure Network Solutions Overview

Introduction

DiamondTEK is a powerful network security solution designed for today's open network environments. Unlike other security platforms that are intended strictly for exclusion, the DiamondTEK solution is focused on the "secure inclusion" that today's corporate intranets, extranets, and Internet e-business applications require.

With DiamondTEK, you can create your own Dynamic Secure Virtual Networks (DSVN™) within a single network infrastructure. Featuring a new class of drop-in network security appliance, DiamondTEK protects your sensitive data from both external and internal threats and gives your employees, business partners, and customers the controlled access they need. What's more, DiamondTEK is extremely flexible. DiamondTEK's robust DSVN security can span virtually all network communications paths including end-to-end (LAN and WAN), site-to-site, and remote-to-site networking communications.

DiamondTEK includes several breakthrough features that differentiate us form other solutions and help ensure the safe delivery of information across unprotected networks. Our Data Driven Access Control (DDAC™) labels your sensitive proprietary data and those labels determine where specific data can and cannot go. With DiamondTEK, the network infrastructure and data collaborate to control data transfer and offer the highest level of security available. In addition, DiamondTEK also provides a security processor embedded in our network appliances. This self-protecting security computer is dedicated to enforcing network security policy and includes security functions that prevent subversion by malicious users, network attacks, and operating system flaws.

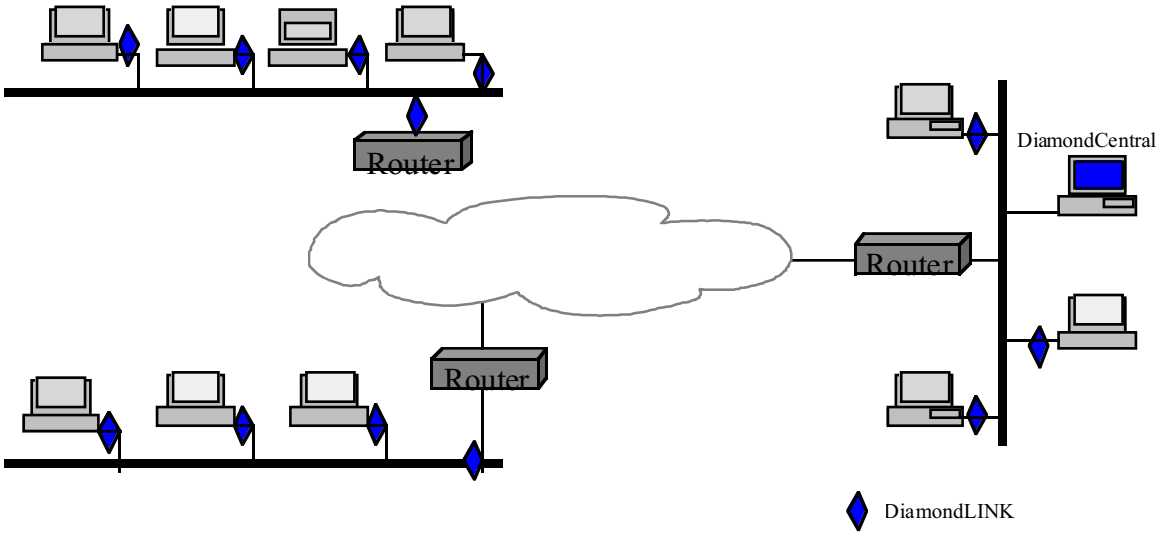
Furthermore, the DiamondTEK DSVN product is a derivative of the only network security product on the NSA's evaluated product list at the B2 level of trust (VSLAN-DiamondLAN). The B2 rating signifies that DiamondTEK has the level of trust required to allow multiple levels of classification to occupy a single network without allowing information from a higher level to seep to a lower one.

Diamond*TEK* System Composition

The DiamondTEK DSVN system is a building block (security tool) for network designers to build secure network systems. The system is governed by a site-defined network security policy and comprised of the following components:

- Diamond*CENTRAL*: the central security controller
- Diamond*TEK* remote network security appliances including:
- Diamond*NIC*: a secure network interface card and authentication card reader
- Diamond*LINK*: an external drop-in network appliance comprised of a built-in DiamondNIC and authentication card reader in a single external device
- Diamond*PAK*: an external drop-in network appliance designed to protect specific servers on the network
- Diamond*VPN*: an external drop-in appliance designed to protect the LAN or WAN network perimeter

These components work together to create the secure network system on which host computers can communicate.



Diamond*TEK* DSVN Basic Network Architecture

Network Security Policy

A network security policy is the set of rules by which communication between host computers (nodes) over a network is defined. The main rules that comprise the network security policy include:

1) Access controls
2) Identification and authentication
3) Communication security
4) Communication integrity
5) Audit

Access controls are defined as a set of rules. Rules that govern access based on the type of information are termed *mandatory access control* and rules that govern based on communication flow are termed *discretionary access control*. *Communication security* rules define the method of securing the data (i.e. encryption) as it passes through the network system. *Communication integrity* rules define how the network system will ensure that modifications to the information during transit will be detected. *Identification and authentication* of network systems is not only concerned with users, but must also include the host systems on which they operate. Lastly, *audit* rules must be definable such that system administrators can investigate events that might be termed security relevant for the site at which the system is deployed.

Network Security Policy Definition

The network security policy definition is performed by individuals at a given site who are tasked with the control and dissemination of the information for the organization. Detailed items that are included in a network security policy include, but are not limited to the following:

1) **How many different types of information require extra security precautions**
2) **On which machines do the different sensitive information types reside**
3) **Which users require access to which type of information**
4) **Which users require access to more that one type of information**
5) **From which workstations should access to the sensitive information be allowed**
6) **What type of encryption is required to prevent wiretappers from accessing the information as it is transferred over the network**
7) **What type of authentication of the user is required; strong or weak**
8) **What type of integrity mechanism should be used to assure proper delivery of the information**
9) **What auditing mechanisms are require to oversee operation and when should they be utilized**

When answers to these questions have been ascertained, the network security administrator can define a security policy using the DiamondCENTRAL portion of the DiamondTEK system.

Network Security Policy Enforcement

Enforcement of a defined network security policy by the Diamond*TEK* system begins when the network security administrator enters the security policy into the Diamond*CENTRAL*. The security policy for a particular user is transferred to the Diamond*TEK* device on the user's workstation when the user initializes with the secure network system. The policy is stored in the secure network interface card, which does not allow the host system to modify or influence the enforcement of the security policy. Since the secure network interface card provides its own operating environment, the device will provide the required security checks as defined by the security policy for the host system.

Diamond*TEK* Secure Network interface Appliances

Diamond*TEK*'s secure network interface devices (Diamond*NIC*, Diamond*LINK*, and Diamond*VPN*) replace the existing network interface cards of the host computers. They provides the following functions for the host operating system:

Controlled network access
Identification and Authentication of user
Role based communications channels
Network encryption
Network information integrity
Network auditing

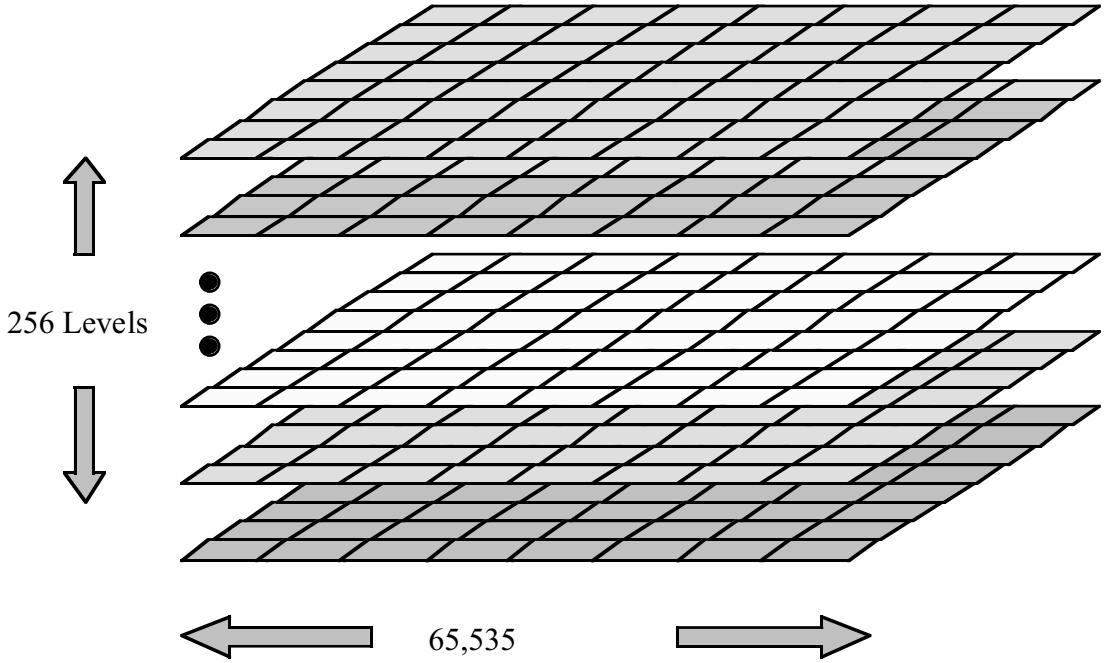
Controlled Network Access

Since Diamond*NIC*, Diamond*LINK*, and Diamond*VPN* are the network interface cards for their host computers, all communications between the host to which they are attached and other hosts on the network must pass through the Diamond*TEK* appliance. This hardware enforcement is essential to ensure that the security mechanisms are being utilized to enforce the defined security policy. The basic access controls supplied by the Diamond*NIC*, Diamond*LINK*, or Diamond*VPN* for network communications include Mandatory Access Control and Discretionary Access Control.

Mandatory Access Control

Mandatory access control provides a means for keeping information of different sensitivities from mingling. Mandatory access controls are implemented by explicitly or implicitly labeling the information in the system. Without labeling the information, there is no means by which computer systems can differentiate between different types of information. This type of access control is essential when information flows are of a high asset value or contain extremely sensitive information.

Examples of mandatory access controls include classification levels (e.g. Secret, Proprietary, Sensitive but Unclassified etc.) and categories of information (e.g. IBM, NOFORN, ARMY, Finance, Engineering, etc.). By utilizing mandatory access controls, communication between host systems can be segregated into like information flows. Each node has its own security window that defines the security capabilities of that node. The Diamond*TEK* system will support 256 levels of classification and 65,535 different categories. Therefore, the security window of a given node can be as small as a single square on a multi-planed matrix or it could include all planes and squares on the matrix.

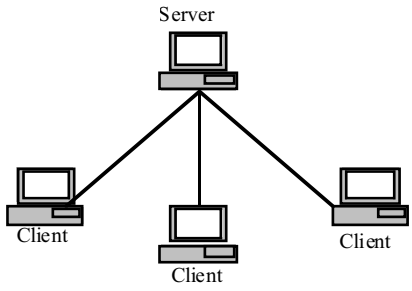


In the Diamond *TEK* system, each datagram will have a label that includes the classification level as well as the category of the information that is contained in the datagram. The format of this label is the Common IP Security Option (CIPSO).

CIPSO Labeling

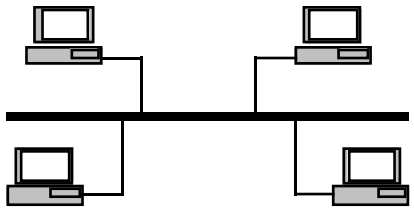
This CIPSO labeling mechanism uses the option field in the IP header to contain the labeling for the datagram. The IP options are a loose collection of add-ins that the IP protocol uses to diagnose network problems, as well as transfer security information. The options field is located immediately following the normal IP header and is null when not used. There are three generally accepted mechanisms for placing the security information in the IP options field. The first is the IP security option (IPSO); second is the revised IP security option (RIPSO); and third is the CIPSO method of labeling datagrams. The CIPSO mechanism provides for a larger number of levels and categories to be represented. For this reason, the Diamond *TEK* system has standardized on the CIPSO labeling format. The CIPSO has two major components that comprise the information that is placed in the IP option field. The main portion of the CIPSO label contains the IP option type (a single octet), a length (a single octet) and the domain of interpretation (four octets) for the label. The second portion of the label is termed the tag. The tag contains the actual level and category values of the information in the datagram. The CIPSO specification defines up to five (5) tag types of which 3 are used by commercial vendors (types 1, 2, and 5). All three of the commercially used tag types represent the classification level in the same manner (a single octet). They differ in the manner in which they represent the category values. Tag type one (1) represents the categories using a bit map string. Tag type two (2) represents the categories by enumeration. Tag type five (5) represents the categories using ordered pairs.

Today's network systems are migrating toward the client/server architecture. This processing paradigm allows for the centralization of the data yet allows the clients to process and make appropriate modifications in a more efficient manner that the old monolithic host based systems. The following diagram depicts a logical view of how communications occur in client/server architectures.



Client/Server Operation Paradigm

Notice that the focal point of the architecture is the server. All information flows through the server and not between the individual client machines. This network architecture works fine with dial-in type connections but current network topologies use communication mechanisms other than dial-in.
Network topologies that are used in today's environments (e.g. Ethernet) cannot enforce the client/server paradigm. Instead, they were designed to support the peer-to-peer paradigm.



Peer-to-peer Operation Paradigm

These network topologies allow host systems to send and receive information from/to any host system on the network. In addition to users sending and receiving information, malicious users can gain access to information as it traverses the network. The overall operational concept is that any device having a connection to the network has the potential to access any information that flows on that network.

The Diamond*TEK* network discretionary access controls allow the security administrator to create and enforce a client/server network architecture using today's network topologies. The management of traffic flows via the controls allows for the creation of a more manageable network system and prevents more advanced users from creating their own communications mechanisms within the network system.

Identification and Authentication

Identification and authentication (I&A) in a network system not only requires users to be identified and authenticated, but also requires the host systems on which they may be operating to be identified and authenticated. The Diamond*NIC* supports the Diamond*TEK* identification and authentication (I&A) mechanism by being a trusted entry point for the I&A information. As part of the Diamond*TEK* I&A process, certain unique information about the network interface card is included into the I&A data when the user attempts to initialize a node, thus providing additional hardware-based information that can not be forged by the user.

The Diamond*TEK* system provides the following three methods for users to perform I&A.

1. Authentication Card
2. Authentication Card and PIN
3. ID and Password from the host system

Authentication Card I&A

Diamond*NIC* and Diamond*LINK* provide a card reader into which the user inserts an authentication card. The attachment of the card reader to these devices provides a trusted path between the user and the Diamond*TEK* system for authentication information. In an all trusted computer network, the host systems could relay I&A information from the user to the Diamond*TEK* system. However, there are few, if any, network systems that are composed exclusively of trusted host computers. Since un-trusted computers do not provide for the safe transport of the I&A information from the user to the Diamond*TEK* system, the system itself provides this interface via the Diamond*NIC* and Diamond*LINK* card reader. This direct attachment provides a trusted path for the I&A information even in un-trusted computer systems.

Authentication Card and PIN I&A

The most secure I&A mechanisms employ a concept of "something you have" and "something you know" to create a complete I&A event. The Diamond*TEK* system supports this concept by allowing the security administrator to specify that a particular node or all nodes will require the use of the authentication card (as described above), as well as requiring the user to enter a personal identification number (PIN) number via the host computer's keyboard. Although the PIN number can be copied in un-trusted host systems, it is still perceived that by adding the PIN input to the authentication mechanism, the mechanism itself is strengthened.

ID & Password from Host for I&A

If the user has a system with a trusted operating system, then the network security administrator can configure the Diamond*NIC* and Diamond*LINK* to accept an ID and password from the host system through the each device's shared memory interface. It is left to the operating system to provide the appropriate controls to ensure that the I&A data is provided via a trusted path between the user and the Diamond*TEK* network appliance.

Role-based Communications Channels

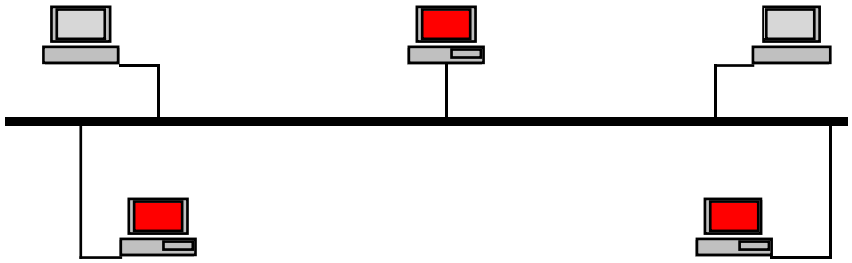
Communication channels are used by host systems to send and receive data over a network. These communication channels are wide open in an Ethernet network system. In an Ethernet network, all hosts on the network have access to all data that passes over the network. To satisfy the need for transmission of sensitive information, the security industry has provided a variety of security products such as firewalls and tunneling encryptors. However, these devices are network protection devices and do not provide host-to-host protection. Today's organizations, with their high-value assets, realize that more is needed to secure communications channels between host systems. This need has brought to the market a category of products called Virtual Private Networks (VPNs). VPNs provide communications security from the sending host to the receiving host system. There are two basic types of VPNs (static and role-based). Static VPNs are little more than a slimmed down (usually software version) of a tunneling encryption product. The newer type of VPN is the role-based VPN. These VPN's allow the user to dynamically reconfigure the security policy of the node based on the role (within a defined security policy) that the user wishes to operate at any given time. The following paragraphs describe these two types of VPNs.

Static VPNs

Static VPNs provide a single communication security policy for a node in the system. The security policy provided is either total encryption (between participating nodes) or selected encryption (which allows encryption to participating nodes and cleartext communication with other nodes). Each of these policies has security and/or operational ramifications.

Total Encryption

Nodes employing the total encryption security policy constrain the user's ability to perform any function other than that within the encrypted realm. The following diagram depicts a typical total encryption policy.

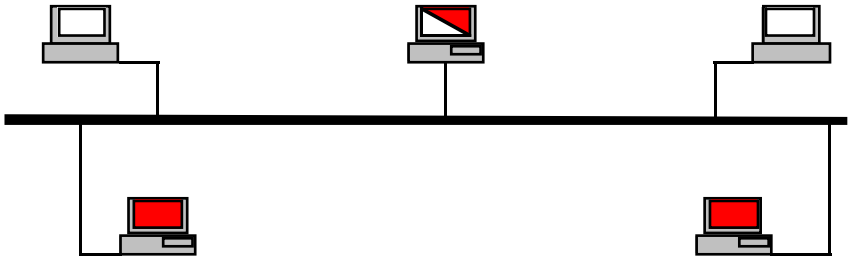


Standard Total Encryption Architecture

In this architecture, the blue hosts will be able to communicate with other blue hosts and red hosts will be able to communicate with other red hosts. However, blue can at no time communicate with red. Therefore, if someone using a blue host needed access to red information, they would have to go to a machine that was providing the red services. This requires the organization to have a larger number of hosts than required or reduces the effectiveness of some users of the system when others are using their machine.

Partial Encryption

The other type of static VPN utilizes a partial encryption security policy. The policy states that between a given node and certain defined IP addresses, communication will be encrypted. To other IP addresses, communication will be in cleartext form. This architecture removes the need for additional equipment but it adds a security risk to the system. A simple example of such a network configuration is shown below:

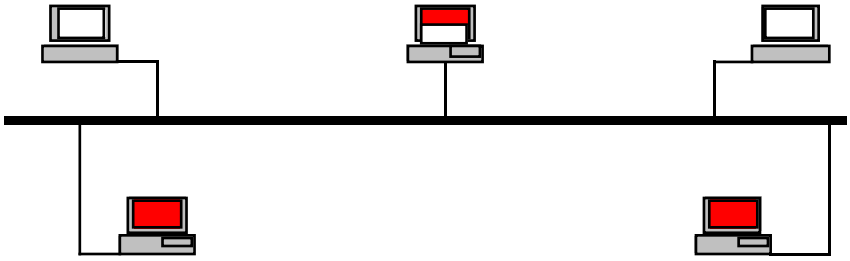


Simple Partial Encryption Architecture

In the diagram, there is one host that is able to see both the white and red networks. A machine configured in this manner poses a tremendous security risk for those organizations that are processing sensitive (government or corporate) information. When operating in the partial encryption mode, the user's workstation can be used as a gateway by attackers on the white logical network to gain access and take information from the red logical network. This gateway function is implemented by the user's workstation running a special application (provided by the attacker) or by the host allowing routing through its own operating system. In ether case, attack groups having good financial backing (re. money) can utilize these capabilities to gain access to the sensitive information.

Role-based VPNs or Dynamic Secure Virtual Networks

Role-based VPNs are the next generation of communication security on network systems. A role-based VPN builds on the capability of static VPNs to create secure communications channels yet provides flexibility to allow the user to select different groups of communications channels. This selection capability is the heart of making a network system that can provide secure communications as well as everyday communications for its users.



Simple Role-based VPN Architecture

In this architecture, the host with the two colors can be attached to either the red or white logical network. When in red mode, the host will only see other red hosts on the network. When the node is initialized in white mode, it will be able to communicate with other white host systems and not with those in the red mode. This simple switching capability allows the workstation and to user to be more productive. Since the host system is only connect to the red or white network but never both simultaneously, there is no danger that the host system ca be used to provide a gateway from one logical network to another.

The role based VPN requires the use of mandatory access controls, discretionary access controls and identification and authentication. Utilizing these three control mechanisms, the network security administrator can create logical networks to allow appropriate users to communicate using defined secure communications channels provided by the defined network security policy. The Diamond*TEK* system provides these role-based communication channels which are selectable by the user (as long as the selection is within a defined security policy). This flexibility allows network administrators to create a more secure network while also giving their users access to services that were not previously accessible. We call this our *Dynamic Secure Virtual Network* or DSVN.

▶ Encryption

Encryption is a process by which recognizable information can be transformed into an unrecognizable form and then back again into the original information. The process of encryption requires two types of information - the data and a cipher key. The encryption process uses the key to transform the data into unrecognizable information that can then be reversed given the appropriate key. There are currently two main forms of encryption - secret key and public key. It is generally accepted that secret key encryption methods are faster than public key encryption methods. However public key encryption mechanisms allow for easier key management strategies. In practice the encryption method used to encrypt data is normally secret key (e.g. DES) while the mechanism used to distribute the cipher keys is usually public key.

Performance & System Characteristics

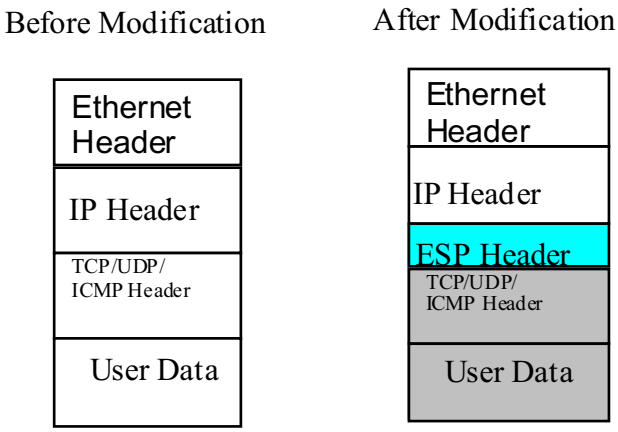
System Component	Managed Nodes	Users	UDP Full duplex sustained (Mbps)	TCP Full duplex sustained (Mbps)	Concurrent 3DES Tunnels	Average Latency (µsec)
System limits:	5000	10'000	n/a	n/a	n/a	n/a
Diamond*Link*	n/a	10'000	140	110	8'000	130
Diamond *VPN*	n/a	n/a	140	110	8'000	130
Diamond *PAK-6*						
- per channel	n/a	n/a	140	110	16'000	130
- aggregate	n/a	n/a	840	660	96'000	130

IPSec Communication

The IPSec RFCs define how encryption communication channels are managed and implemented. Encrypted channels are defined using security associations. These security associations map to a value known as a security parameter index (SPI). The co-operating nodes to uniquely distinguish the communications channel use the SPI. IPSec communication between nodes is defined to be either a transport or tunneling level of operation. The Diamond*TEK* system supports both types of communication.

Transport Level IPSec Communication

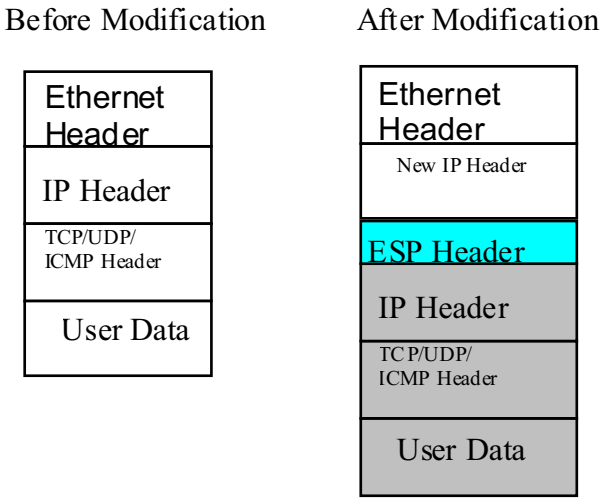
Transport level IPSec communication adds security information headers between the original IP header and the IP data that was contained in the original network datagram. The encryption header involved is the encryption security protocol (ESP) header. This header contains the SPI that signifies the cipher keys and method used to encrypt the datagram. Using SPI, the receiving node will be able to access the appropriate decryption key(s) and decrypt the datagram.



IPSec Transport Communication

Tunneling Level IPSec Communication

Tunneling level IPSec communication encapsulates the original IP datagram in a new IP datagram. This new datagram will contain the appropriate ESP header allowing the receiving node to decrypt the datagram for delivery to the host system. Since the original IP datagram is encapsulated, the original IP address of the datagram is not viewable by the outside world. The only visible addressing is the address of the tunneling device and the address of the destination node (which could also be a tunneling device).



IPSec Tunneling Communication

Encryption Algorithms

An encryption algorithm is the process by which cleartext information is changed into something different and can also be used to convert the modified information back into cleartext form. There are many encryption algorithms available in today's market place including DES, Triple DES, BlowFish, RSA, SkipJack, and others.

DES Algorithm

The DES algorithm was originally developed by IBM in the early 1970's to protect government information that was not classified (unclassified and sensitive-but-unclassified). Since that time, other industries have adopted the use of the algorithm to protect information when it is transferred from one location to another (i.e. banks). DES is currently the only approved (by the National Institute for Standards and Technology) algorithm for the protection sensitive but unclassified information. The Diamond*TEK* system provides the security administrator the ability to select this type of encryption for communication between specified nodes.

Triple DES Algorithm

The Triple DES algorithm is actually the DES algorithm using three keys and performing the algorithm three times on the information. The mechanism of triple DES encryption is as follows:

Encrypt the data block with key A.
Decrypt the data block with key B.
Encrypt the data block with key C.

Note that in some implementations, keys A and C have the same value, which lessens the key storage overhead. The triple DES algorithm has become the defacto standard for encrypting information of a sensitive nature for communication over the Internet because of its heritage in the DES algorithm and its ability to be implemented in hardware which provides for a fast implementation. The DiamondTEK system allows the network security administrator to define communication between specified nodes utilizing triple DES as an option.

Key Distribution

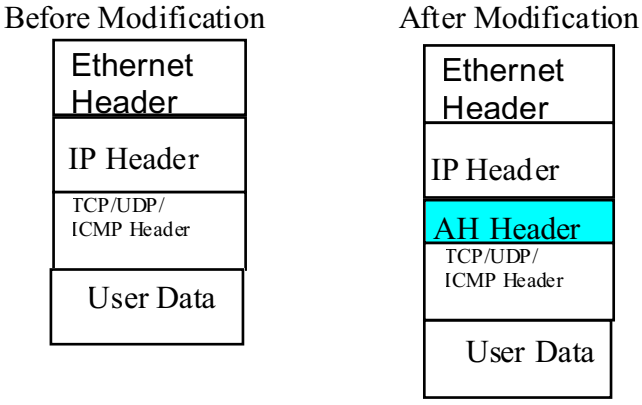
Encryption systems require keys for the encryption process. The mechanism used to deliver keys to the encryption devices is termed key distribution. The IETF is currently working on a standard way of allowing participating nodes to derive keying material for communication. This mechanism is currently defined using the ISAKMP/Oakley protocol. Because of its backing (IETF) and the potential for interoperation with other encryption products, the Diamond*TEK* system will utilize this open architecture mechanism for the distribution of keying material for node-to-node communication.

Communication integrity

Communication integrity provides the second component of secured communication. The first requirement (encryption) is useful for keeping others from viewing the information. However, encryption does not prevent others from modifying the information. Communication integrity is the mechanism that provides assurance to the users of the system that the information has not been modified during transmission. Many network transactions will require both the secrecy of keeping the information hidden from view as well as ensuring that the information has not been changed. The IETF has developed standards for integrity as part of the IPSec security protocol.

IPSec Integrity

The IETF has defined a standard by which cooperating nodes can provide a high degree of assurance that information is not modified during transmission. This standard is defined in RFCs 1825 through 1829 and uses an authentication header (AH). The Diamond*TEK* system provides the required integrity process (MD5) as well as provides a hardware based message authentication code generator that enables very high-speed integrity calculation for datagrams.



IPSec Integrity Communication

Audit

Auditing is the mechanism by which administrators can determine what is happening to the network system. The Diamond*TEK* system provides the network administrator with a comprehensive auditing capability. In the Diamond*TEK* system, there are two types of auditing - security relevant and statistical. The administrator has the power to enable and disable auditing of any of these types of audits.

Security Relevant Auditing

The Diamond*TEK* system provides for auditing on attempted security violations. Attempted security violations include:

1) **Attempting to send information to a node that is not in the senders access control list.**
2) **Attempting to receive information from a node that is not in the receivers access control list.**
3) **Attempting to send information that contains a label that a node is not allowed to send.**
4) **Attempting to receive information that contains a label that the node is not allowed to receive.**
5) **The integrity mechanism has detected a modification to a datagram.**
6) **Invalid login attempt by a user of the system (i.e. attempting to initialize using a role not approved for the user, attempting to initialize a node that the user has not been approved).**

These audit types can be enabled or disabled by the security administrator.

Statistical Auditing

In addition to security relevant auditing, the Diamond*TEK* system will provide the network security administrator the ability to determine how his users are utilizing the system. Statistical audit events available to the administrator are as follows:

1) User initialization (time, date, which node, and what role)
2) User role changes (time, date, which node, and what role)
3) TCP connection by user (what other node is the user communicating)
4) TCP connection by node (what other node is the node communicating)
5) Total dropped datagrams
6) Total bytes of information transferred
7) Total bytes of information received

The network security administrator can enable/disable these audits to satisfy an individual site's need to know.

Diamond*CENTRAL* Secure Network Controller

The Diamond*CENTRAL* Secure Network Controller is the security management workstation for the Diamond*TEK* system. It provides the means by which the network security administrator defines and manages the operation of the protected network. The workstation consists of a dedicated Windows NT workstation, one or more special secure network interface cards, and the Diamond*CENTRAL* security application software.

Dedicated Windows NT Workstation

The Diamond*CENTRAL* component utilizes a dedicated Windows NT workstation as the basis of its operation. In order to provide the fully evaluated version of the Diamond*TEK* system the C2 version of Windows NT must be used. The C2 version of Windows NT is version 3.5 with service pack 3 and the C2 extensions. If the customer does not wish to operate the Diamond*CENTRAL* on an operating system that is no longer fully supported by Microsoft, the Diamond*CENTRAL* can be operated on the current version of Windows NT (e.g. 4.x).

Secure Network Interface Card(s)

The Diamond*CENTRAL* system utilizes up to five secure network interface cards for communication to and from the secure network system. One secure network interface is required for each 1000 nodes managed by the system. The Diamond*CENTRAL* secure network interface card provides the mechanism for encryption/decryption, programming of the authentication cards and the transmission/reception of datagrams to the Diamond*NIC*s, Diamond*LINK*s, and Diamond*VPN*s.

Diamond Central Security Software

The Diamond*CENTRAL* security software provides the network security officer with an easy to use intuitive interface to manage the secure network system. The Diamond*TEK* system brings heretofore-unparalleled security for communications and the Diamond*CENTRAL* allows the administrator to configure and manage the network without extensive training.

The functions provided by the Diamond*CENTRAL* application include:

1) Create and manage user certificates
2) Create and manage communication security policy
3) Provide initial keying material for secure communication establishment between nodes of the system
4) Provide audit storage and viewing of attempted security violations and other network events.
5) Provide real time alarms for selected attempted security violations for immediate actions by appropriate personnel

The following paragraphs describe these functions.

Creation and Management of User Certificates

Identification and Authentication of users and nodes to the Diamond*TEK* system is configured and managed by DiamondCENTRAL. Since the Diamond*TEK* supports three methods of I&A (card, card/PIN and ID/Password) the Diamond*CENTRAL* software must provide a means for creating the appropriate information for each of these methods.

The card and card/PIN authentication alternatives require the Diamond*CENTRAL* software to interface to the attached secure network interface card to create a user certificate on a credit card device. The information on the card uniquely identifies the user.

To support the ID/Password and the PIN portion of the card/PIN authentication alternatives, Diamond*CENTRAL* supports the input of the required information via its user interface.

Diamond*CENTRAL* will provide complete management of its authentication data. The administrator will have control of the user certificates by placing a length of time that the certificate is valid as well as being able to immediately revoke a specified certificate.

Creation and management of Communication Security Policy

The main reason to deploy a VPN system is to provide communications security. A communications security policy has three main factors: encryption, integrity, and access control. For the communication of sensitive information over unprotected networks, all of these mechanisms must be available. The Diamond*CENTRAL* security application is tasked to define the network security policy and instruct other Diamond*TEK* secure network devices of their responsibilities.

Communication Security Policy - Encryption

The encryption portion of the security policy managed by the Diamond*CENTRAL* allows the security administrator to specify communications channels between nodes as being encrypted using DES or triple DES. This encryption selection will be available on a node-to-node basis.

Communication Security Policy – Integrity

The integrity mechanisms provided by the Diamond*TEK* include the standard MD5 that is required as part of IPSec security standards. It also includes a high-speed message authentication code calculation that can alternately be used for communication that needs the high-speed capability. The network security administrator will define, on a node-to-node basis, the type of integrity mechanism that is to be used.

Communication Security Policy – Access Control

The access control system of the Diamond*TEK* system includes mandatory access controls (classification and/or categorization of information) as well as discretionary access controls (basic communication channels). Because of its B2 heritage, the Diamond*TEK* system provides for the separation of information by more than just encryption. Separation is also based on a label assigned to each datagram that flows through the system. A transmitting host cannot send nor can a receiving host receive a datagram that is not within the defined security window for the node. This security window is based on the current operationa profile that the user has selected. This ability is the basis of the role-based VPN services provided by the Diamond*TEK* system. Additionally, the Diamond*TEK* system provides a filtering capability for IP addresses. This access control mechanism also provides

port filtering based on TCP and UDP port numbers. These controls allow the network security administrator to close the networking capability of any protected host to only those services necessary.

Key Management Controller

The Diamond*CENTRAL* is the key manager of the Diamond*TEK* system it controls. It provides the initial keying material to the nodes via a predefined secure communications channel over the network. This initial keying material is then utilized by the ISAKMP/Oakley protocols to generate the necessary keys for node-to-node communication. When the PKI structure becomes available, the Diamond*CENTRAL* will be the local authority that will communicate with the remote authorities to acquire the appropriate keying material and certificates for delivery to the individual users and nodes.

Auditing Definition, Storage and Management

Diamond*TEK* provides significant network auditing capabilities for the network security administrator. The security administrator can define an auditing policy that requires the Diamond*NIC*, Diamond*LINK*, and Diamond*VPN* to audit any attempted violation of the security window, integrity failures on received datagrams, invalid login attempts (using the wrong node, attempting to use an inappropriate role, or supplying invalid I&A information), or TCP connection information. The audit information is generated by the Diamond*TEK* remote appliance discovering the event and sent to the Diamond*CENTRAL* for logging and storage. Audit events are sent to the Windows NT event log for easy viewing, manipulation, and archival by the network security administrator. The network security administrator can add third party products for services other than those provided.

Real Time Alarms

Real time alarms are provided by the Diamond*CENTRAL* to alert the network security administrator of improper behavior on the secure network system. Alarm events include attempting to transmit/receive information not within a node's security window, integrity failures of received datagrams and invalid login attempts by users.

Diamond*TEK* Host System

The Diamond*TEK* system provides the security services from within the network interface card (Diamond*NIC*) or through the stand-alone "bump in the wire" Diamond*LINK*. Because it provides its own operating environment it does not steal CPU cycles nor does it rely on the host operating system to protect it from inadvertent or malicious attack from the user or remotely connected system. The requirements for integrating the Diamond*TEK* security mechanism therefore are simply hardware connectivity and driver availability to interface the operating system to the secure network interface card.

The baseline hardware support will include interfaces to PCI, SBUS, and ISA host expansion busses using an Ethernet 10Mb topology. Future releases, targeted for release within the year, will provide network interface speeds of Ethernet 100Mb for the PCI and SBUS versions and the DiamondLINK. Additionally, a 56KB modem device will be available.

Diamond*TEK* System Operation

DiamondTEK system operation can be viewed from the user's perspective and from the internal operational perspective. The following paragraphs describe the system operation from these two viewpoints.

User Perspective

Operational activity from the perspective of the user is simply that the user may need to (if configured as part of policy) engage the Diamond*TEK* identification and authentication mechanism before network access is granted. Otherwise, no changes from the user's perspective should be noticeable as long as the user operates within the defined security policy.

System Perpective

The DiamondTEK system has four basic operational phases - configuration, initialization, key exchange, and secure communication. The following paragraphs briefly describe the events of each of these phases. Additionally, the user is allowed to change roles via a process that will cause the DiamondNIC or DiamondLINK to transition to the initialization state to authenticate the role change.

Configuration Phase

Before a node can be used as part of the Diamond*TEK* network it must be added to the security database that resides on the Diamond*CENTRAL*. Information such as hardware address (e.g. Ethernet address), IP address (unless provided by the Dynamic Host Configuration Protocol), type of authentication to be used, and allowable information type for the node are supplied via the Diamond*CENTRAL* administrator input forms. Once the information is collected, the administrator will generate an administrator configuration card for the node. The node is then installed in its host computer and the configuration card is inserted into a card reader that is directly attached to the device. The node will then complete the initialization sequence by communicating (in a secure manner) with Diamond*CENTRAL* to download any additional pertinent information. Any further control information will be downloaded from the Diamond*CENTRAL* the next time the node is initialized by a user.

Initialization Phase

To initialize a node on the network, users must first be authenticated. This authentication process begins by the network security administrator entering the user's I&A information into the security database that resides on the Diamond*CENTRAL*. Once this information is entered, the security administrator will inform the user of the required information. The following list details the information that is given to the user:

1) **For the card authentication - the administrator programs an authentication card and gives it to the user.**
2) **For card and PIN authentication - the administrator programs an authentication card and selects a PIN value. Both are given to the user.**
3) **For ID/Password authentication - the administrator selects an ID and a password that is to be used by the user. This information is then given to the user.**

Once the user has been given the identification and authentication information, the user can then initialize a node that he has been assigned to use. The initialization process is different for each of the I&A types. The following describes the sequence of events for each of the mechanisms.

Card Authentication

Card authentication for the Diamond*TEK* is performed when the user inserts the authentication card into the Diamond*NIC* or Diamond*LINK* card reader. This provides a trusted path between the user and the system for the input of the I&A information. Once the card has been inserted (and if applicable a role has been selected) the Diamond*NIC* or Diamond*LINK* will send the I&A information (along with other data) to the Diamond*CENTRAL* via an encrypted control communication channel. If the user is allowed to use the node at the desired role, then the security window and other virtual network parameters are downloaded to the Diamond*NIC* or Diamond*LINK*. At that point the host Diamond*TEK* network appliance is available for secure network communication.

Card and PIN Authentication

Card and PIN authentication for the Diamond*TEK* is performed much like the card authentication. The user will follow the same I&A procedures as those associated with card reader I&A. After the card has been inserted into the card reader and the role selected, the Diamond*NIC* or Diamond*LINK* will collect the available I&A information from the card reader and then issue a command to the device driver loaded onto the host system. This command instructs the device driver to prompt the user for a PIN and a selected profile value. This information is then sent to the Diamond*NIC* or Diamond*LINK* as the fulfillment of the I&A information. The Diamond*NIC* or Diamond*LINK* will then create and initialization request message using the supplied information and send it to the Diamond*CENTRAL* for verification via an encrypted control communication channel. If the user is allowed to use the node at the desired role, then the security window and other virtual network parameters are downloaded to the Diamond*NIC* or Diamond*LINK*. At that point the Diamond*NIC* or Diamond*LINK* is available for secure network communication.

ID and Password Authentication

The ID/password I&A mechanism does not require the use of a card reader that is normally attached to the Diamond*NIC* or Diamond*LINK*. However, the host operating must provide a trusted path between the user and its associate ID/password input and the Diamond*NIC* or Diamond*LINK*. Operationally, once the driver has been loaded by the operating system, the Diamond*NIC* or Diamond*LINK* will instruct it to prompt the user for an ID, password, and role values. The user will enter this information and it will be sent to the Diamond*NIC* or Diamond*LINK*. The Diamond*NIC* or Diamond*LINK* will then create an initialization request message using the supplied information and send it to the Diamond*CENTRAL* for verification via an encrypted control communication channel. If the user is allowed to use the node at the desired role, then the security window and other virtual network parameters are downloaded to the Diamond*NIC* or Diamond*LINK*. At that point the Diamond*NIC* or Diamond*LINK* is available for secure network communication.

Key Exchange Phase

When a Diamond*NIC* or Diamond*LINK* wishes to communicate with another Diamond*NIC*, Diamond*LINK*, or other IPSec complaint node, it first checks to determine whether the communication is allowed by the security policy down-loaded to it by the Diamond*CENTRAL*. If the communication is approved, then the traffic and integrity keys must be generated to protect the information as it moves from one host to another. This key determination process is instigated when the Diamond*NIC* or Diamond*LINK* attempts to communicate with another secured node. The keys are determined via the IETF proposed standard ISAKMP/Oakley protocol. The Diamond*CENTRAL* provides the original seed material for this protocol during the initialization phase. The initial seed material is different for each possible classification level that the node is capable of communicating.

Secure Communication Phase

Once the Diamond*NIC* or Diamond*LINK* has been configured, initialized and keying material has been generated for a communication path, the Diamond*NIC* or Diamond*LINK* will begin sending and receiving datagrams to the remote node. The Diamond*NIC* or Diamond*LINK* will format datagrams using the IPSec standard and will accept datagrams so formatted from the remote node. Nodes can be configured to utilize the tunneling or transport encryption mechanism in addition to using MD5 or message authentication codes as the authentication mechanism of the datagrams. When the policy down-loaded to the Diamond*NIC* or Diamond*LINK* includes communication with cleartext nodes, the encryption key determination process is not invoked and the IPSec headers are not applied. The datagram is simply sent to the destination node (assuming the node was in the security policy down-loaded by the Diamond*CENTRAL*). It is important to note that each and every datagram is inspected against the security policy to ensure that the defined policy is enforced.

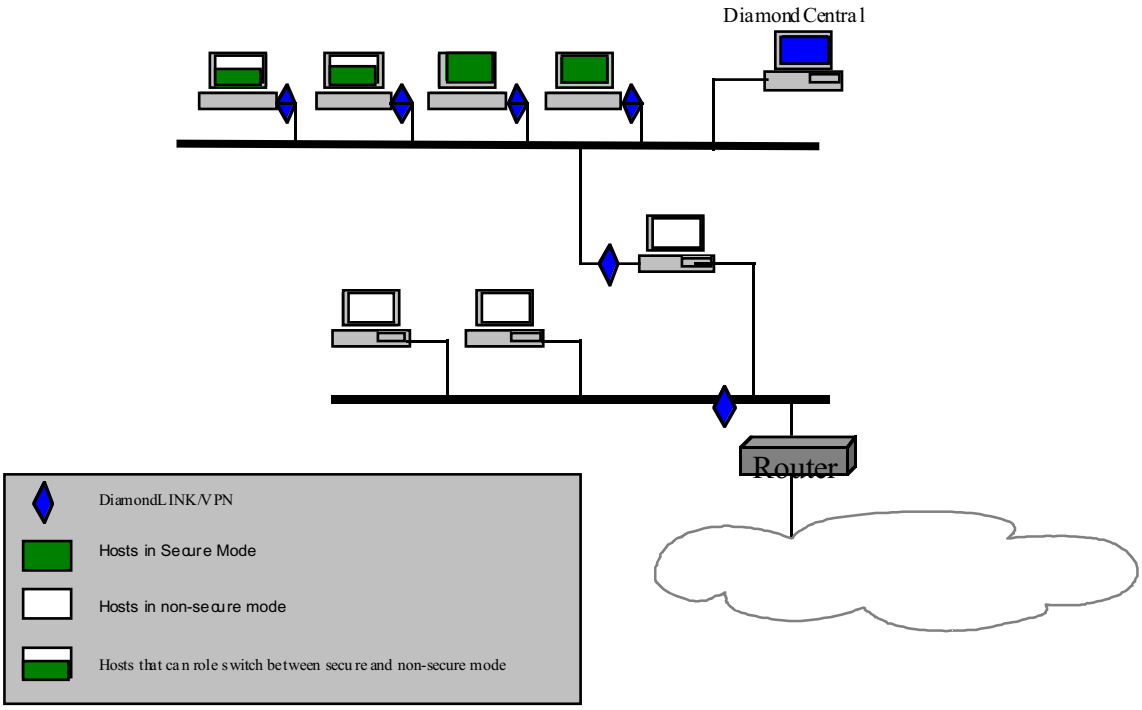
Diamond*TEK* Network Architectures

The DiamondTEK system can be configured (via a security policy) to create many types of network architectures. The following paragraphs describe four of the possible architectures that can be created using the system.

Separated yet Integrated Protection

A common mechanism to protect information as it flows over a network system has been to create physically separate network on which to send the information for each information type. This requires the organization to install and maintain multiple network systems. In addition, users that require access to more than one of these network systems requires access to more than one computer system to perform their duties. This means that either they have more than one computer on their desk or they have to go somewhere else to access the other network. In the first case there is the expense for each of these users for the additional machine and its maintenance costs. In the second case there exists a cost issue with respect to the user having to go somewhere else to perform an action as well as the costs associated with the host and maintenance of the extra group of machines.

One possible solution would be to allow the user to use the machine on their desk to access both networks. Security policy however may not allow the two networks to be simultaneously connected. This is where the Diamond*TEK* system can be used to provide the necessary communication using a single workstation. The following diagram shows the hardware configuration that can be used to fulfil the user's needs without incurring the costs associated with multiple machines.

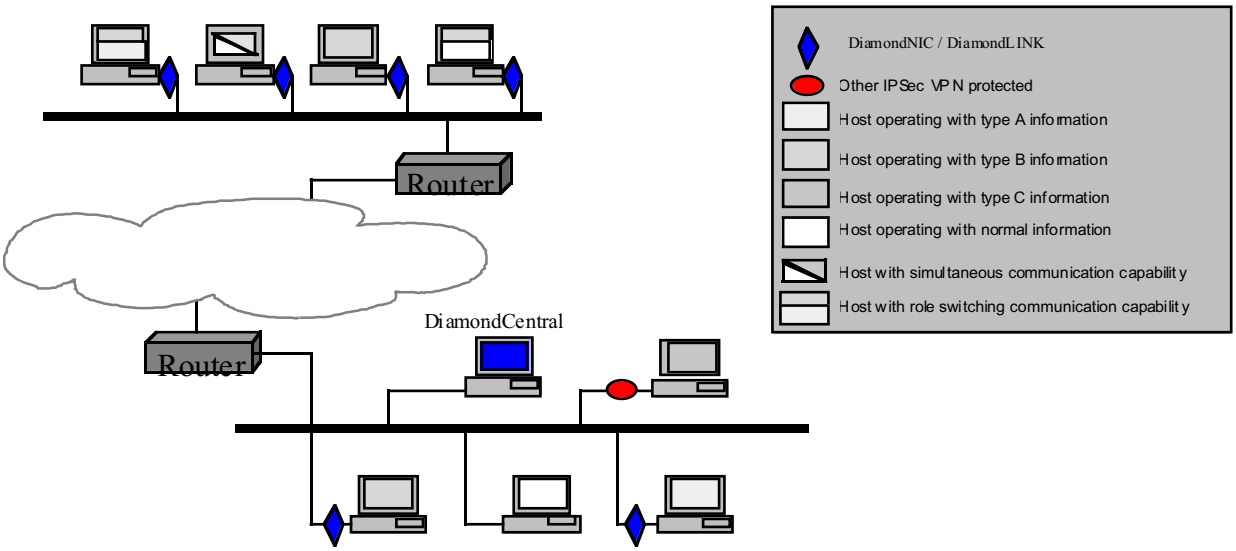


Separate Yet Integrated Network Architecture

In this architecture, the user is either logically connected to the local secure network system or they are allowed communication with the secured router that in turn allows communication to the external network system. The type of connectivity is based on the role the user has selected. The assured separation is provided by the Diamond*TEK* system. Only information of the appropriate labeling is allowed to flow between the two networks. This prevents external users from gaining access to any information that flows on the secured network.

▶ Integrated Host Protection

Many of today's network systems do not have separate cable plants yet need the ability to keep users from accessing unauthorized information. In addition, users who require access to the sensitive information also need access to normal network services. The Diamond*TEK* system can be used to create such a network system using a security policy that defines secured and non-secured communication channels. The security administrator can create a security policy that allows secure and non-secure communication at the same time or a policy can be created that would require the user to perform a role change when a different type of information is to be accessed. This flexibility allows the security administrator to tailor his system to meet the organizations threats and communications needs. The following diagram shows a simple network architecture that provides both secured and non-secured communication.



Integrated Host Network Architecture

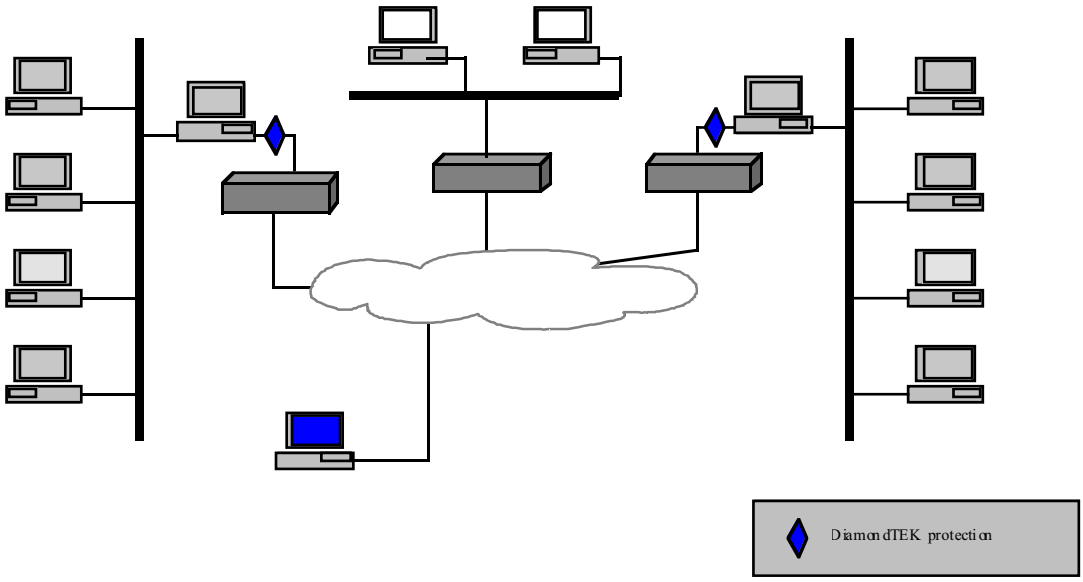
The above architecture supports a system where there are two different types of sensitive information (A and B) and two types of non-sensitive information (C and normal).

For processing sensitive information, the security policy could be to either fix the node at the sensitivity level (as depicted with screens having a one pattern) or configure the node for role switching capability (depicted by screens which have a horizontal split). The security policy for the sensitive machines requires that when accessing one type of information (A, B, C, or normal), other information types (sensitive or non-sensitive) shall not be accessible. This access policy is key when building network systems that do not provide gateway services (known or unknown) between sensitive and non-sensitive networks.

The non-sensitive data on the network does not require the level of security provided for the sensitive information. Because of the level of security is less, additional features of the Diamond*TEK* can be utilized. First, the security window of the node can be configured to allow two types of information at the same time into the node (this is signified by the diagonally split screen). Second, the Diamond*TEK* system can be configured to allow nodes to communicate with other IPSec compliant products (such as software VPNs). The importance to this type of connectivity may become key when communicating with existing systems as well as providing the hardware based encryption and integrity needed for speed on the network.

Site-to-Site Protection

Many of today's communications requirements are a result of organizations attempting to leverage an Internet or other wide area network to transport information that was normally carried by a leased line or special purpose WAN. The cost savings of leveraging an Internet connection or other existing WAN is tremendous when compared to the usage of leased lines. What many security vendors have created are sub-network encryption devices. These devices include firewalls with added encryption as well as separate tunneling encryption devices. The Diamond*TEK* approach to site-to-site encryption is to allow the security administrator to install a board in a host system that is to be used as a router between the local network and the WAN. This host system would perform the required routing from the local network to the WAN and the Diamond*NIC*, Diamond*LINK* or Diamond*VPN* installed in the host would provide the necessary encryption to prevent listeners from viewing the information as it traverses the WAN. The following diagram depicts such a subnetwork-to-subnetwork architecture.

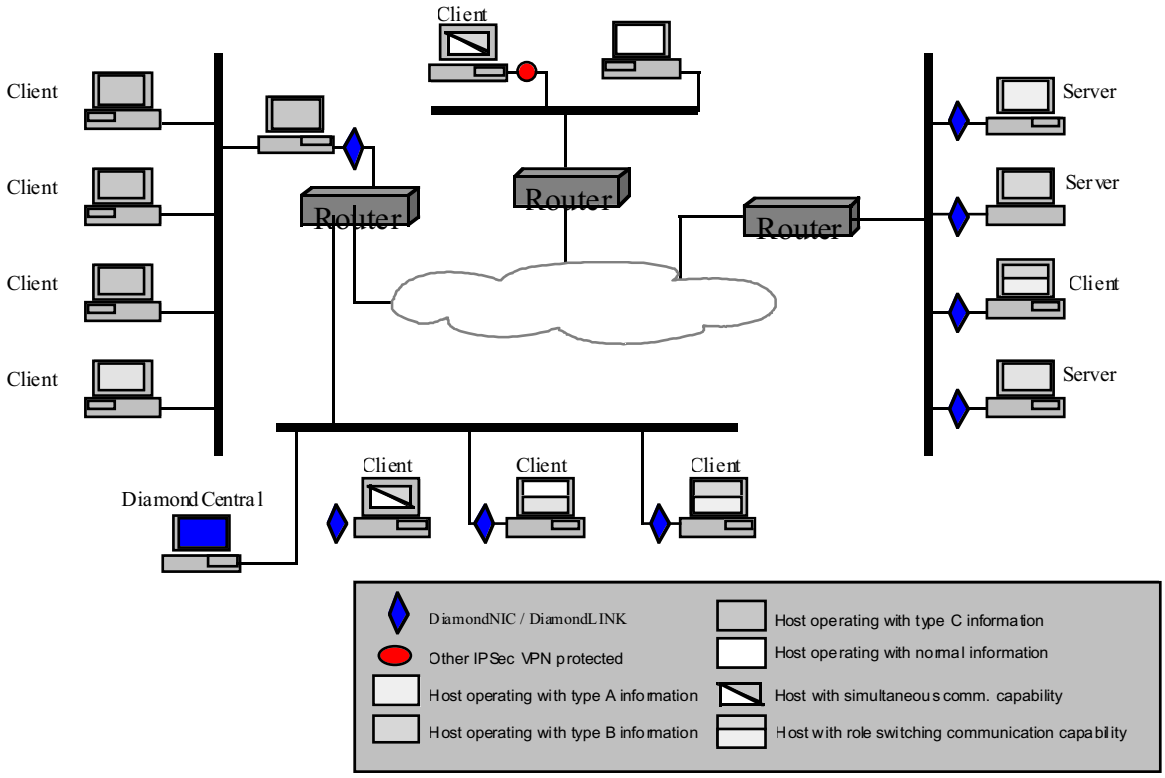


Site to Site Network Architecture

In the site-to-site architecture, the Diamond*TEK* can be used to provide simple encryption between sites as well as an add-on to Firewalls to provide high-speed standards based encryption for these devices. This will ensure that all the subnetworks (independent of the type of Firewall) will be able to communicate.

Site and Host Protection

Network architectures that require a small number of hosts within a remote network to have access to services provided by network systems will become a necessity in the near future. These types of systems are normally data repositories that need to be able to disseminate information to certain users at various sites at remote locations. What is required includes a high level of user authentication and secured communications channels between the site and remote users. The following diagram shows a simple architecture that utilizes the Diamond*TEK* system to provide this communications infrastructure.



Information Dissemination Network Architecture

In this architecture communication between the servers and the Web clients are protected and secured by the Diamond*TEK* system. The Diamond*TEK* ensures that information with the appropriate labeling is all that is seen by the individual Web servers. This information separation allows the data store to provide different levels of information to different levels of users. When information of a sensitive nature is to be provided, the network system can be augmented to include a Diamond*NIC* in the remote workstation to ensure appropriate I&A and that the communication is secured from the data store to the remote node.