

NetLOCK

Frequently Asked Questions (FAQs)

1. What is NetLOCK?

NetLOCK is a network-layer security product that protects communications and computer systems from sophisticated attacks originating anywhere in a network:

- (1) Using powerful encryption services, NetLock hides passwords, protocols headers, and user data from eavesdroppers over the entire path this information travels between two networked computers- over both LANs and WANs.
- (2) Using computer-level, authentication and authorization services, NetLOCK tightly controls which networked computers can establish connections to each other, completely blocking unauthorized connections to desktops, servers, and network infrastructure computer systems.

2. Where can NetLOCK be used?

NetLOCK can be used anywhere. It is application independent, media independent and LAN/WAN topology independent. NetLOCK protects all communications between popular PC, Mac, and Unix systems that use TCP/IP. IPX protocols are supported in Version 1.3, available July 1997. NetWare support will be available in August 1997 and AppleTalk will be added by the end of the year.

3. Does NetLOCK work with firewalls? Why do you need NetLOCK if you have a firewall?

Firewalls are an effective defense to restrain Internet users from going beyond a company's dedicated Web server. It is still possible, however, for sophisticated intruders to penetrate a firewall or simply bypass it by dialing directly into the internal network. In a 1996 ASIS [Dana, spell out ASIS] study, 30 percent of the respondents indicated their network has been trespassed by intruders even after they had installed a firewall. NetLOCK can stop all these intrusions by preventing intruders from ever establishing a connection to a targeted computer regardless of their point of entry into the network.

4. Some firewall companies are planning to encrypt communications either between firewalls or between remote users and firewalls. Why is NetLOCK a better solution?

NetLOCK is clearly a more universal and complete solution. NetLock protects all your communications end-to-end regardless of the location of the computers and the type of network used. NetLOCK also works with more types of computer systems and network protocols- and protects the LANs behind the firewall.

5. Can't a software-only solution be subverted easily by either removing the software or copying it to another computer system?

If NetLOCK is removed from a computer it can then communicate only with systems that do not have NetLOCK. Other NetLOCK machines will refuse to communicate with this machine and report every attempt to the NetLOCK Manager.

No security product can protect against all possible types of attacks(even hardware products could be transferred along with their software components to another machine). However, the unauthorized user would still need to know passwords to attack a particular application. And if an installed copy of NetLOCK were transferred to another computer along with its host name and IPaddress, the unauthorized computer would need to be on the same subnet, or routers would not communicate back to it. Finally, if they were on the same subnet both machines could receive responses to the others requests, a tip-off to the legitimate user that something abnormal is happening. NetLock

ensures that a compromised computer cannot compromise data in the net nor network security. Ultimately, physical security is the only way to prevent the stealing of security mechanisms.

6. How much does NetLock increase the size of a data packet? Is any compression used to cut packet size?

Security functions add 14 to 29 bytes to a packet: 14 bytes for the security header, from 0-7 bytes for encryption depending on the user data packet size, and 8 bytes for the data integrity checksum (optional). The variability results from a variable length encryption block pad (0-7 bytes) and the presence or absence of the optional data integrity checksum (8 bytes). Compression is an enhancement planned for NetLOCK later in 1997.

7. Does NL work with all types of firewalls? How can this possibly work?

NetLOCK works with most popular firewalls because they can identify and pass through secure traffic. The firewall filtering is simply configured to pass NetLOCK traffic (which is already protected end-to-end). Since the IP headers of NetLOCK packets are visible to the firewall, the FW can identify a NetLOCK packet (IP protocol number 50) and can still filter packets based on source and destination addresses. When the protected packet reaches the destination computer, NetLOCK provides directional, port-level access controls.

Background:

It's also worth noting that NetLOCK can allow important traffic you might not otherwise permit to pass through a firewall. For example, NFS client-server applications based on X-Windows and remote net management applications both use SNMP and the UDP protocol. Most organizations would normally not allow this traffic through their FW because UDP does not perform any authentication. Use of NetLOCK can allow this traffic because the FW can screen communications on the basis of IP addresses and NL can authenticate the end stations. Working together, NetLock and firewalls provide security that is both stronger and more flexible than a firewall alone.

8. Are security alarms sent to the Manager's screen or only to the Manager's log file?

Security alarms can go to any or all of the following:

(1) the Manager screen, (2) the Manager log, (3) the Agent screen, and (4) the Agent log.

9. How many agents can each manager realistically support?

There are no hard system limits on the number of agents that can be supported by a single manager. The manager is used to create and initialize Agents within its domain and does not directly participate in Agent-to-Agent communications in any way (Note: In Dynamic Addressing environments, the NetLOCK Manager is involved in Host Name and Address resolution). The SCI database is not limited in size. Any natural limit is really defined by the number of computers the security administrator wants to manage from a single location.

10. Can different default security parameters be set within a single manager depending on the subnet of the agent?

The level of granularity for default parameters is the individual node, i.e. an administrator using a single NetLOCK Manager can set the default parameters of each node individually. This capability is used by the auto-setup feature to apply different defaults to different groups of Agents, i.e. any desired group of addresses, not just subnets.

11. What protections are on the NetLOCK Manager to prevent unauthorized access?

The Manager is protected by a password; stronger user authentication is also recommended as well as the physical securing of the management computer system.

12. What kind of network activities generate NetLOCK alarms?

Five different security alarms are generated by the current version of NetLOCK:

- The wrong crypto key has been used for encapsulation
- An invalid checksum has been detected by an Agent
- The IP header was malformed when received by an Agent
- A non-NetLOCK packet was unexpectedly received by an Agent
- A computer with an unauthorized source address has attempted to create a connection with a NetLock'd computer.

13. How long does it take to install Agent software?

Five minutes or less.

14. What happens if a NetLOCK'd computer boots up when the manager is not running? Can the computer communicate?

In a fixed IP address environment, if the manager is unavailable and the agent's certificate has not expired, the agent will use its existing SCI files when it receives no response to its update request. If its certificate has expired — which is highly unlikely, it cannot communicate with other NetLOCK'd computers. Authorized communications with other computers would still be allowed. In a dynamic addressing environment, the computer that receives a new address will not be able to communicate with other NetLOCK'd computers until the manager returns online. All other computers can continue to operate normally.

15. Does NetLock interoperate with IPSEC implementations and if not, are there plans to do so? When?

There are no transport mode netsecurity products that fully implement the IPSEC encapsulation and key management standards. However, NetLock intends to implement the full IPSEC suite of standards, and will test interoperability with other vendors, as soon as this is possible—probably in 1988. Today, NetLOCK implements the full ISO network security standards, but uses the IPSEC encapsulation standard in place of ISO's. It isn't clear yet when the vendor community will be able to do this. (Note: Vendors are now demonstrating interoperable tunnel-mode products in prototype form.)

16. NetLock appears not to be active in the industry's security standards activities. Why would anyone purchase a proprietary solution like NetLOCK™?

NetLOCK is active in the IETF IPSEC working group and committed to open standards. As a general strategy, NetLock intends to support relevant IETF standards in its first major software release after standards have been finalized. Also, it is important to note that current NetLOCK is not a proprietary system. It implements the IPSEC encapsulation protocol, the ISO standards for key management, and uses standard encryption algorithms from NIST and RSA, and SNMPv2 for security management.