

Title: **Industrial Security Appliances- Safe use of the Internet explained**

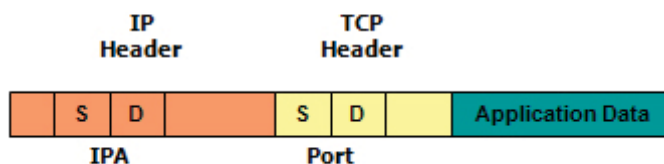
Author: **Barry E. Baker**
CCNA CCSP INFOSEC

The most readily available network access today is a connection to the public Internet. There are very few places one can go and not have easy access to this vast network interconnecting almost every inhabited point on the globe. In a perfect world, the low-cost and ease of implementation of the Internet would make it the best choice for connecting remote sites together into a single logical network or allowing your vendors and customers access to your process control network (PCN). As you may have come to realize, however, we do not live in a perfect world. The essence of the Internet, its openness, was quickly subverted by miscreants and criminals to intercept other people's data. These ne'er-do-wells stole or manipulated the information they intercepted for their own purposes. These attacks became referred to as "Man-in-the-Middle" attacks. Because of security concerns, many companies have avoided the Internet and have maintained expensive private networks to ensure the integrity of their data. Utilizing the advancements in Industrial Security Appliances (ISAs) detailed in this whitepaper, responsible companies can now return to the Internet as a method to interconnect remote sites and allow access to their systems by their suppliers and customers. Advancements in Internet data transmission security utilizing ISA technology can greatly lessen the chance of data theft and network intrusion by unwanted third parties.

Ethernet Background

Before describing the types of ISA technology, it is important to understand exactly what is contained in the Ethernet packet. An Ethernet network is a "packet-switched" network. This means that all of the data transmitted via the Ethernet network is packed into special packages (TCP/IP packets) before it moves out onto the network. The contents of the Ethernet packet are what the various types of network security appliances use to control the data moving from one network to another.

TCP/IP Packet Structure



For the purposes of this whitepaper, the specific data fields within the TCP/IP Packet of interest are the source/destination TCP port found in the TCP header and the source/destination IP address found in the IP packet header. As traffic moves across the network, the source and destination IP addresses identify the original sender and the final recipient(s) for each packet. The source port number identifies the specific application and/or service from which the data originated. The destination port number identifies the specific application to which the data is destined. These are the fields that ISAs use to control data moving from network to network.

ISAs perform two basic functions. The first function, often referred to as "routing," that an ISA performs is the interconnecting of two physically and/or logically separated networks. Networks are considered to be logically separated when each network has a different network-addressing scheme. The second function that ISAs provide is to the control of traffic that is allowed to move between two networks including one or more of the following:

1. Limiting access across the ISA to specific destination nodes.
2. Limiting the type of traffic that can transverse the ISA.
3. Limiting the rate of transfer between the networks.

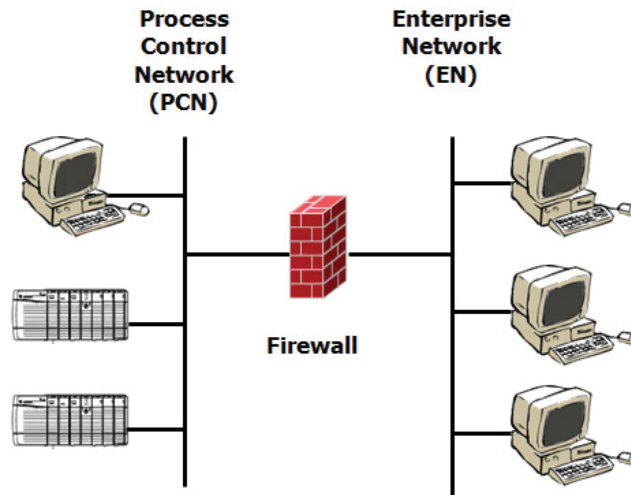


Industrial Networking Solutions

Phone: 800-889-1461 | Fax: 972-248-9533 | Web: www.IndustrialNetworking.com

Broadly speaking, ISAs can perform their two functions using three different methods. The methods are packet-filtering firewalls, stateful-inspection firewalls, and deep-packet inspection firewalls.

Packet-Filtering ISA



A Packet-Filtering ISA is often implemented by configuring a traditional or industrially-hardened network router to perform the desired packet filtering. This type of traffic filter is called an Access Control List (ACL). An ACL is best understood as a list of rules that precisely defines what traffic will be allowed to traverse the ISA connecting two or more networks together. Similar to ladder logic, the ACL rules are sequentially evaluated. Generally speaking, ISA ACL rules block all traffic other than that originating from one or more designated source IP addresses. The ISA can expose a limited, designated list of destination IP addresses or address range. Further refinement limiting traffic to specific destination or source ports can also be defined. Once defined the rules are processed as follows:

1. An Ethernet packet is received on an interface of the ISA.
2. One or more fields (source/destination port numbers and/or IP addresses) within the received packet are compared to the first rule in the ISA's ACL, and one of the following actions will be taken:
 - a. If the rule specifically allows the packet to be forwarded, the packet is sent to the outgoing interface, and all remaining rules in the ACL are ignored.
 - b. If the rule specifically forbids the packet from being forwarded, the packet is discarded by the ISA, and all remaining rules in the ACL are ignored.
 - c. If the rule neither allows nor forbids the packet, then the next rule defined in the ACL list is considered. This process continues until action 'a' or 'b' above takes place, or until the end of the list is encountered. If the end of the ACL list is encountered without a rule applying to the packet then it is discarded. The only way a packet will ever get through this type of ISA is by encountering a rule within the configured ACL list that specifically allows the forwarding of the packet.

It is important to understand that a thorough knowledge of the allowed or desired traffic is required prior to configuring the necessary ACL rule list. Any change in the desired traffic will require updating the ACL's on one or more ISAs. For a relatively small network with limited and well-defined security needs, maintaining the ACL rules is quite simple, however for a large network with complex security requirements, maintaining the ACL rules can quickly become a full-time job in itself.

A shortcoming of the packet-filter ISA is that it must process each packet one at a time. With a high volume of traffic, the packet-filtering ISA may become a bottleneck for traffic throughput. The longer the ACL list, the longer each filtering decision can take.

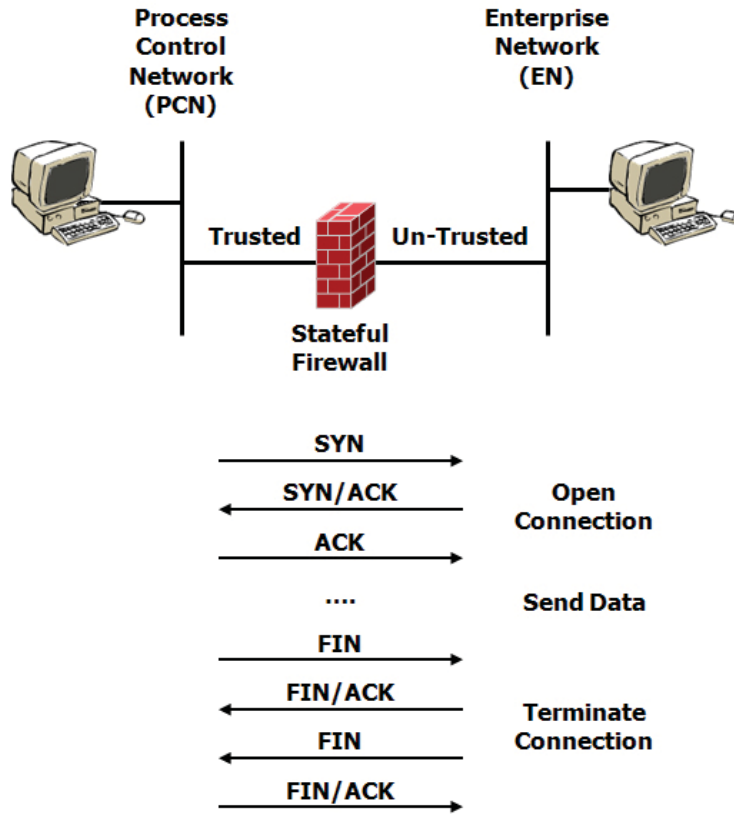


Industrial Networking Solutions

Phone: 800-889-1461 | Fax: 972-248-9533 | Web: www.IndustrialNetworking.com

Stateful-Inspection ISA

Traffic that moves between networks, including industrial Ethernet networks, almost always makes use of the Transmission Control Protocol or TCP. There are a few exceptions to this, but not many. When data is transmitted using TCP, a connection is first established between the source and destination nodes. Data is then transmitted using this established connection. After the nodes end their "conversation," the connection between the two is terminated. A good analogy for this process would be a old-time phone call which involves an telephone operator. Suppose Party "X" wishes to talk to Party "Y." Party "X" picks up the phone and talks to the operator informing him/her that they desire to speak with Party "Y." The operator builds a temporary connection between Parties "X" and "Y" on the switchboard and the conversation then takes place. At the conclusion of the conversation, Party "X" and "Y" hang up their respective phones, and the operator then tears down the temporary connection. This is exactly how a TCP session functions.



A stateful ISA monitors the state of the TCP connection described above. If a connection (conversation) is initiated by a node on the trusted network, the ISA will assume that the conversation is legitimate and will leave the path between the trusted and untrusted nodes open until either node ends the "conversation." Technically, the conversation must be initiated by a synchronization request (SYN) packet sent by the trusted node. Upon passing the SYN packet out the untrusted port, the firewall will remember the destination IP address and port. When the destination node replies, the reply will pass through the firewall to the source node which initiated the "conversation" without any time-consuming packet inspection. The firewall will keep the link open until either of the nodes sends a Finished packet (FIN) notifying the other node that the conversation has ended. At this point the firewall will end the link and all unsolicited packets from the untrusted node will be rejected. This means that it is impossible for an untrusted node to ever initiate data exchange.

The above behavior is the default behavior of most stateful ISA firewall devices. Notice that a stateful ISA examines the relationship between a series of packets instead of evaluating every single packet individually. Generally speaking, this is a far less burdensome process because a complicated explicit list of rules does not have to be maintained. Throughput capacity increases because the firewall does not spend a lot of time inspecting each packet that it handles. Most stateful ISA firewalls can also support the layering of packet filtering over the base stateful inspection functionality.



Industrial Networking Solutions

Phone: 800-889-1461 | Fax: 972-248-9533 | Web: www.IndustrialNetworking.com

Deep-Packet Inspection ISA

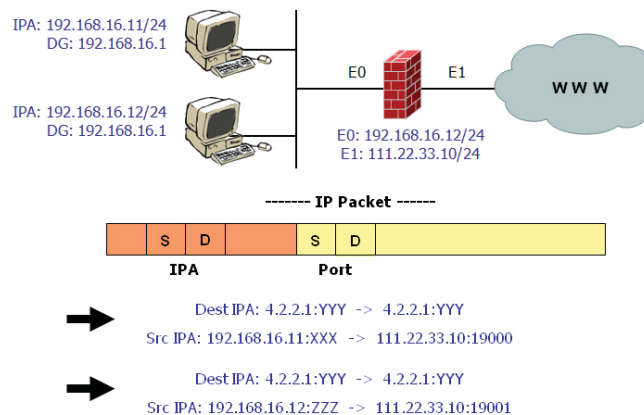
As its name implies, a deep packet inspection ISA goes a step beyond the stateful ISA. The deep-packet inspection examines the application data in the IP packet in addition to the IP address and TCP port numbers. The purpose of this deeper inspection is to determine if one or more packets that are arriving at the untrusted port might possibly be the beginning of some sort of network attack. This determination is made by comparing the arriving packets to “signatures” of known threats like worms and other popular attack techniques that could be contained in traffic from an infected node that would be otherwise trusted. This type of analysis is commonly referred to as Intrusion Detection Service (IDS) and Intrusion Prevention Service (IPS). All packets identified as possibly containing a threat are discarded by the ISA even if the sending node is on an approved device list.

It is important to note that the quality of detection is directly related to the size of the known threat database and the frequency with which the database is updated. The supplier of the deep packet ISA device provides threat database updates periodically, just like virus protection, to adjust for the continuous evolution of threats. These updates can be loaded into the ISA either through an Internet connection or through manual updating for networks that are not connected to the Internet.

Other ISA Services and the Security Appliance

Network Address Translation (NAT), and Virtual Private Network (VPN) gateways are also functions that modern ISA devices provide.

NAT is a useful ISA feature which has many applications, one of which is to obscure a private network-addressing scheme from the public Internet. The basic concept of NAT is that the source IP address within packets which transverse the ISA are replaced with a different address prior to leaving the ISA. The ISA keeps track of the various IP address substitutions. When a reply is sent to the ISA from a device on the secure side of the ISA, the ISA reinserts the original address back into the reply packet prior to sending it back to the initiating node. This process is illustrated below.



An example of NAT that many can relate to is the home broadband router. Even if there are ten computers on your home network, the broadband router usually represents them as a single IP address to the outside world. This reduces the number of IP addresses needed on the Internet.

VPN technologies, which are often available in ISAs, provide a dedicated, encrypted connection between two IP addresses over a public network. By encrypting the data portion of an IP packet, even if the packets are intercepted by a determined thief, the contents are totally obscured, making them unusable to the scoundrel. This in essence allows a secure tunnel to be formed between any two points on the public Internet. At each end of the VPN tunnel, the parties who are communicating with one another have the information necessary to encrypt and decrypt the data inside the Ethernet IP packets they are sending each other. Since the encryption/decryption information is known only to the parties at either end of the tunnel it is now possible to pass information through the easily accessible public internet without fear of discovery.



Industrial Networking Solutions

Phone: 800-889-1461 | Fax: 972-248-9533 | Web: www.IndustrialNetworking.com

Summary

The level of protection provided by ISAs has steadily increased since they were first introduced. Today users can implement sophisticated network protection with a single device rather than multiple devices. It is important to remember that network threats are continuously evolving. What protects the network today may be useless tomorrow. With the right ISA device and vendor, you will be able to keep pace with the evolving threats through updates to your ISA's firmware.



Industrial Networking Solutions

Phone: 800-889-1461 | Fax: 972-248-9533 | Web: www.IndustrialNetworking.com