



# Industrial Security Appliances

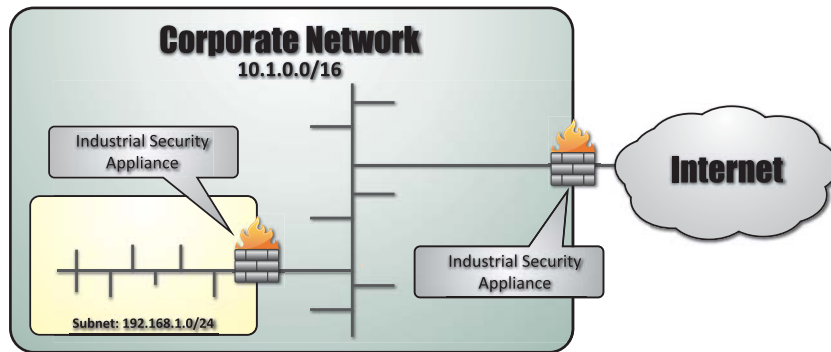
available from

## Industrial Networking Solutions

Industrial Security Appliances (ISA) offer a vast array of features that can be utilized to join, segment, and secure multiple networks. The following illustrates some of the most common and beneficial features of the ISA.

### Routing

When in Router mode, the ISA works as a router between two different networks. You need to configure the internal and external interfaces. The external interface may use static IP settings or receive them from a DHCP server. In Router mode the ISA may act as a DHCP server for the internal and/or external network.

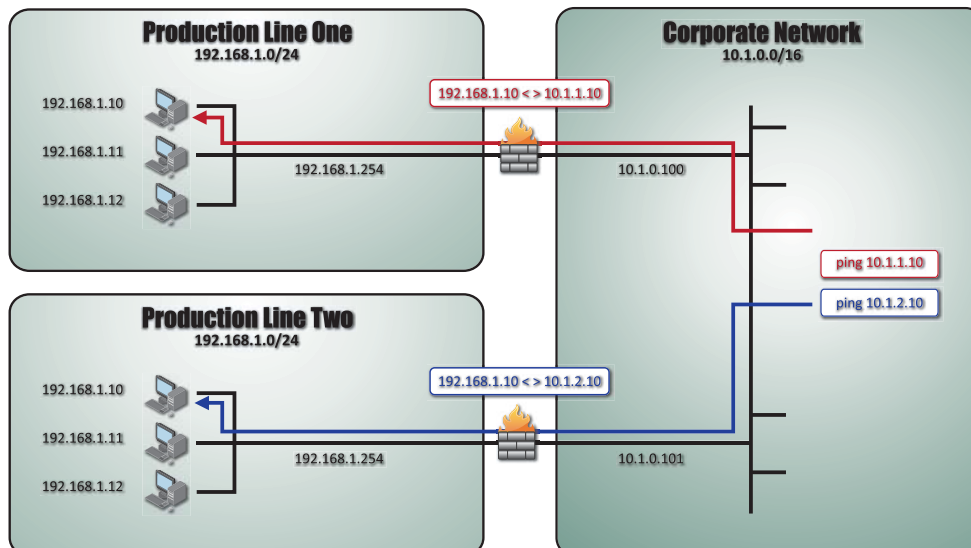


### 1:1 NAT (Network Address Translation)

1:1 NAT can be used for connecting several subnets with the same network addressing scheme to the main network. In the following example two production lines, which use the same network 192.168.1.0/24, shall be connected to the corporate network with the network 10.1.0.0/16.

An ARP daemon on the ISA ensures that routers of the external network know where to send packets directed to the internal network. The systems of the production lines can be reached directly from the corporate network through their mapped IP addresses.

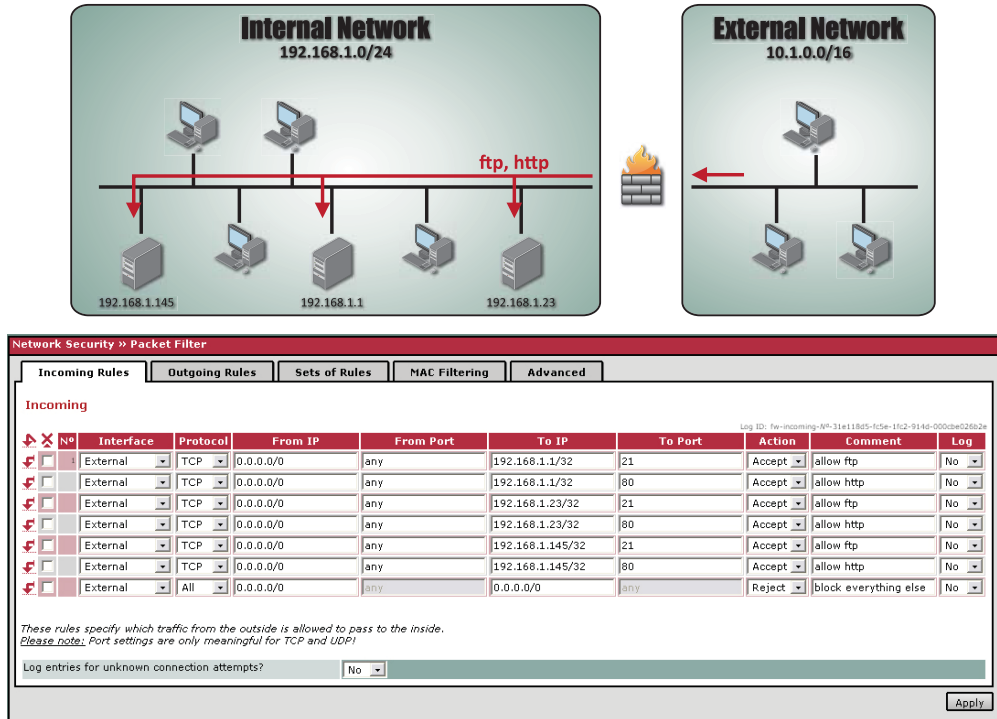
Eliminate concerns about having to re-address entire networks and eliminate the need to maintain uniquely addressed spare parts for each production line.



## Firewall

Integrated Stateful Packet Inspection – The connection data for each active connection is collected in a database (connection tracking). Therefore, it is only necessary to define rules for one direction. Only data from the opposite direction of the connection is allowed through, and none other.

Packet filtering – Packets are analyzed against a set of filters. Packets that make it through the filters are sent to the requesting system and all others are discarded.



## VPN (Virtual Private Network)

A VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as a leased line, a VPN uses “virtual” connections routed through the Internet from the company’s private network to the remote site or employee.

VPNs 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.

