Secure Networks™ for Process Control

Leveraging a Simple Yet Effective Policy Framework to Secure the Modern Process Control Network

An Enterasys Networks White Paper

Introduction

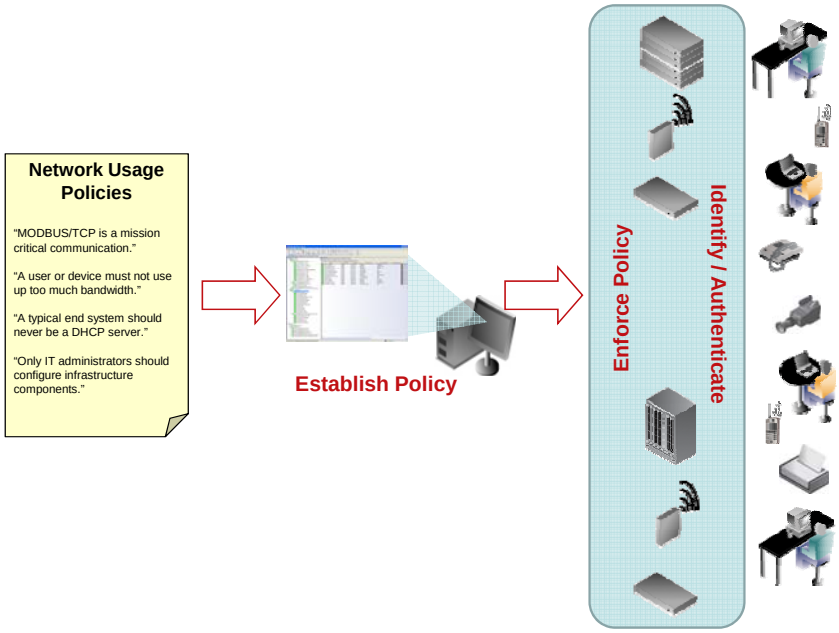
Industrial control systems have evolved significantly over the past several years with an increase in the use of Ethernet data communications networks and IP communications protocol. For example, process control systems now commonly connect historian servers to Ethernet networks to allow users IP-based access to real-time data from the distributed control systems (DCS) and the programmable logic controllers (PLC). More and more critical infrastructure processes are being supported with underlying standards-based network communications technology. While the use of the standards-based Ethernet network has greatly increased the business and process interaction in industrial automation environments, there is also potential for increased security risks to critical infrastructure. It is imperative that clear and concise network security architecture be established as a foundational element to any network communications system involving the plant environment. A Secure Networks™ architecture for process control will provide established standards-based network communications with integration of critical security technologies. The result is a highly manageable, scalable and adaptable network architecture that addresses the critical data communication and security concerns of the control systems environment.

A Secure Networks Policy Framework for Process Control

Leveraging technology to establish and enforce access and usage policies in a network communication environment, a fully integrated approach to networking and security can be realized. A proper architecture for secure data communications in process control should include a network policy framework with the following attributes.

- Centralized administration of network usage policies
- Identification and authentication of all connected devices and users
- Authorization of network usage through policy enforcement

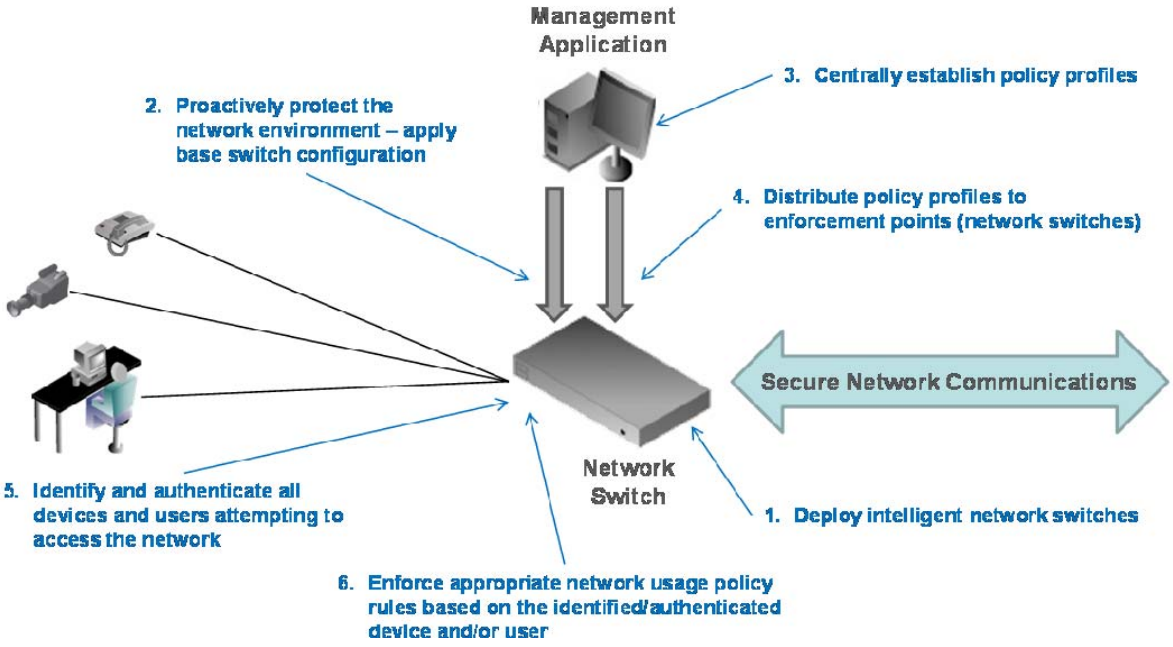
Simply stated, an effective policy framework for securing modern process control networks will include an administrative application to define access and communications policies for all devices and users; intelligent network switches which can identify and authenticate who and what connects to the network; and an ability to enforce the appropriate set of network usage policy rules right at the port where the device and user connects.



Using a well conceived policy framework, an effective security posture can be realized in the modern communications infrastructure of the process control environment. Access to the communications infrastructure, the mission critical applications and services in the process control environment can be controlled and secured; significant proactive measures can be implemented to protect against known threats and dangerous communications behaviors on the process control network; and real-time threats to the process control environment can be automatically isolated and mitigated at the source. The result is a highly available and secure process control network.

Steps for Implementing Secure Networks in the Process Control Environment

Implementing Secure Networks architecture is not difficult. In fact, in most cases, this architectural approach will prove to be easier to implement than solutions where networking and security are not fully integrated. To implement Secure Networks in the process control environment, the following steps should be taken.



1. **Deploy intelligent network infrastructure to support all required communications.**
   Carefully select network switches which have embedded security and policy enforcement capabilities. Capacity and performance are critical elements for network connectivity, but to implement Secure Networks, the switched network infrastructure must also provide advanced features.

2. **Proactively protect the network environment.**
   The network infrastructure must be protected from attack or exposure to threats. Centralized network management software should be leveraged to apply secure base configurations to network switches. This administration of the network should include the ability to disable unnecessary features on a network switch, secure a network switch against service availability attacks, and secure the management and control of a network switch. Important features enabling this secure configuration include:

   - Selectable Device Features (on/off)
   - Secure Host VLAN Configuration
   - Host DoS Prevention Configuration
   - Host Port Access Control Lists
   - Authenticated Host Management
   - RADIUS Configuration
   - Inbound Traffic Rate Limiting
   - Flow Setup Throttling
   - Spanning Tree Protocol Controls and Protection
   - Broadcast Suppression Controls
   - Multicast Controls
   - Secure Management Protocols
   - Secure Logging

3. **Centrally establish role-based acceptable network use policies.**
   In the process control environment, network communications should be strictly controlled so that only the required protocols and application traffic are allowed. Dangerous and unnecessary traffic should be restricted from ever entering the network. Centralized policy administration software should be leveraged to easily construct acceptable use policy profiles for each role of end-systems and/or users in the process control environment. An example of a role-based policy profile would be to filter File Server like services traffic such as

DHCP Server and DNS Server on a network port where an IP phone or IP camera has connected to prevent service spoofing. Another example would be to filter all traffic types but what is specifically required for PLCs updating a Historian thus securing maximum bandwidth and availability for process-related communications.

4. **Distribute policy profiles to Policy Enforcement Points.**
   A highly distributed ability to enforce appropriate policy rules is important to a scalable and affective Secure Networks deployment. Policy should be established centrally, but then distributed to network switches which have appropriate features to function as Policy Enforcement Points.

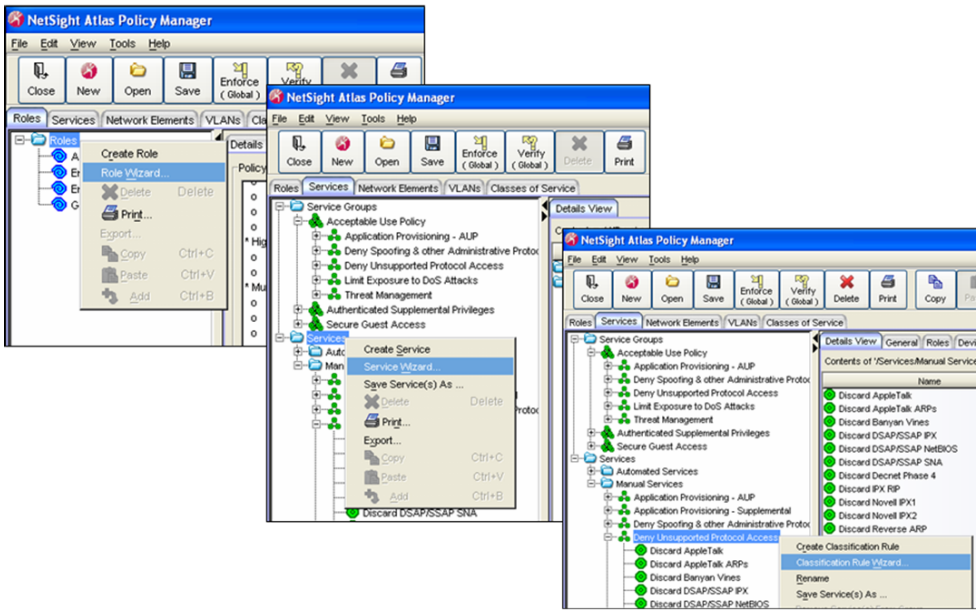
5. **Identify and Authenticate all end systems and users connecting to the network.**
   Identification and authentication of both user-based and non-user-based end systems is important to ensuring the correct policy rules are enforced based on the *role* of the end system device and/or user attempting to access the network. Leveraging technologies in the network switch such as LLDP-MED, 802.1X, Web-Based authentication, MAC-Based authentication, and even protocol snooping, end system types and user roles can be determined so that appropriate policy rules can be enforced. This allows for network usage to be fully aligned with the individual device and/or user accessing the network.

6. **Enforce the acceptable network usage policies.**
   Once the policy profiles have been distributed to the network switch and a connecting end system and/or user has been identified, it is here that the appropriate policy rules should be enforced – right at the switch port where the end system is connected. Policy rules should be used to filter, prioritize and/or rate shape network communications based upon OSI Layer 2, 3 or 4 traffic classifiers. The ability to enforce specific policy rules against individual traffic flows at every switch port in the network allows for very scalable and robust Secure Networks.

Operating Secure Networks in the Process Control Environment

Operating Secure Networks should be simple yet highly effective in order to maximize resources available for administration in a process control environment. Leveraging centralized administrative applications to configure and monitor Secure Networks is key to simple yet effective operation.

Network infrastructure configuration must be easily performed through the use of template-based tools and *one-click* actions. If an administrator wants to configure a secure management VLAN for every switch in a network environment, it should be a global setting rather than having to make a configuration change to each device. From a policy perspective, operation should be through a central application which allows administrators to define complex rules with simple graphical interfaces, and to distribute policy profiles to anywhere in the network (or the entire network) with a single click of the mouse.



Operational tools such as NetFlow should be embedded in the infrastructure switches so that administrators can get a detailed view of what applications are running on the network and how policy rules may need to be configured to better secure and prioritize network communications for mission critical services.

An example of the operational advantage to a well conceived policy framework versus legacy device specific configuration models can be seen below.

Why a Policy Framework is Better than Access Control Lists	
Using ACLs you have to: **1. Telnet to switch** **2. Display ACL configuration file** **3. Highlight ACL text and copy** **4. Paste ACL text into Notepad** **5. Evaluate ACL order and insert new filter rule** **6. Re-order remaining rules** **7. Copy text in Notepad** **8. Paste into switch Telnet session** **9. Repeat – for each switch on network**  Observed time to deploy one change = *1 hour*	Using a Policy Framework you have to: 1. Create packet filter rule in Policy Manager 2. Link rule to appropriate device/user role(s) – *1 click* 3. Enforce to every switch on the network – *1 click*  Observed time to deploy one change = *1 minute*
The bottom line is that leveraging a good policy framework solution can save time and avoid errors!	

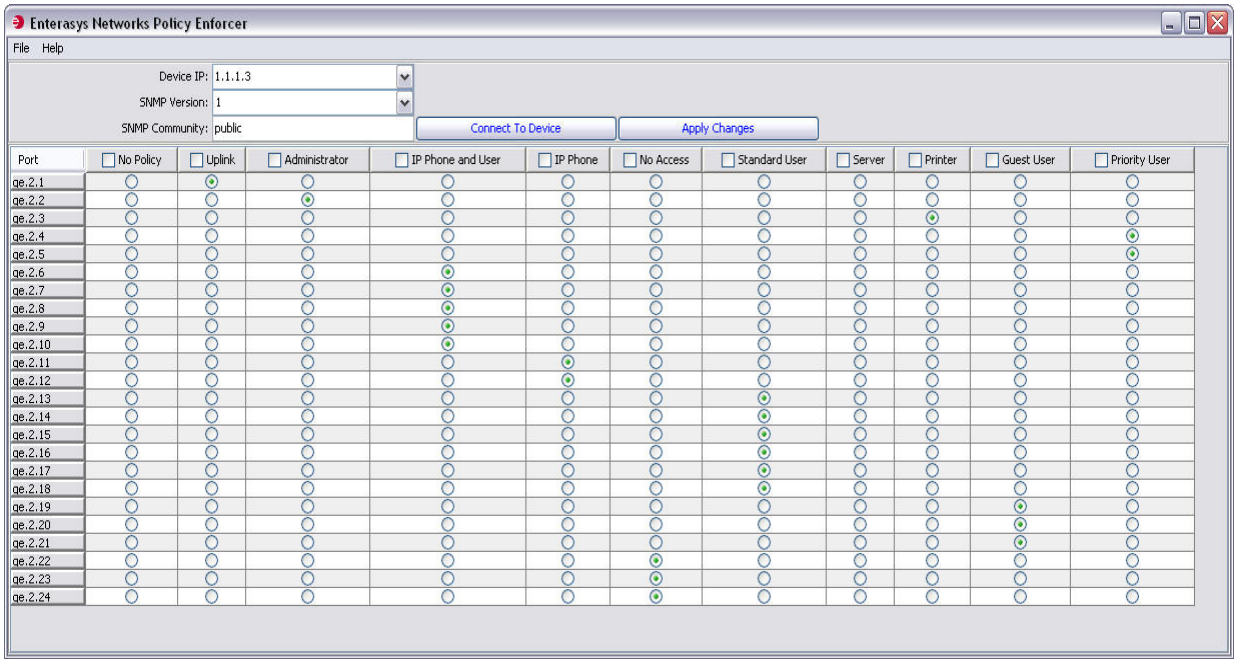
Policy-Based Secure Networks for Process Control: Best Practices

A simple yet effective approach to deploying Secure Networks in a process control network should rely on implementing policy in several key phases. Leveraging purposed-built applications for administering policy in a complex network will significantly expedite all phases of the policy deployment. Applications have been developed that make it easy to implement policy-based Secure Networks. By implementing security policy, the network access-layer can be protected and managed so that only communications important to the business can pass through the network. Using GUI-based policy administration applications, allows the creation of a security policies for users and devices on a process control network. These policies are organized in roles that are based on user or device function and requirements to the business. Policy roles contain specific rules which provide control of how users and devices communicate and what resources they can access.

The first phase to implement and enable network security using policy management would be the creation and enforcement of specific default network usage policies for various user roles and device types. These policy roles would be associated to network edge access ports and would eliminate many security risks. An example would be to deny any ports attempting to run network services that you would normally see from a File Server like DHCP Server, a DNS Server, or an Email/Web Server. It also can deny the use of Telnet, SNMP, SSH, rate limit ICMP protocol and deny or rate limit

HTTP depending on need. This should be able to be implemented to all edge ports of the network by a few clicks of a mouse using a policy management application. Third party consultants or application vendors can assist in the design of a unique default policy profile for all or specific network locations.

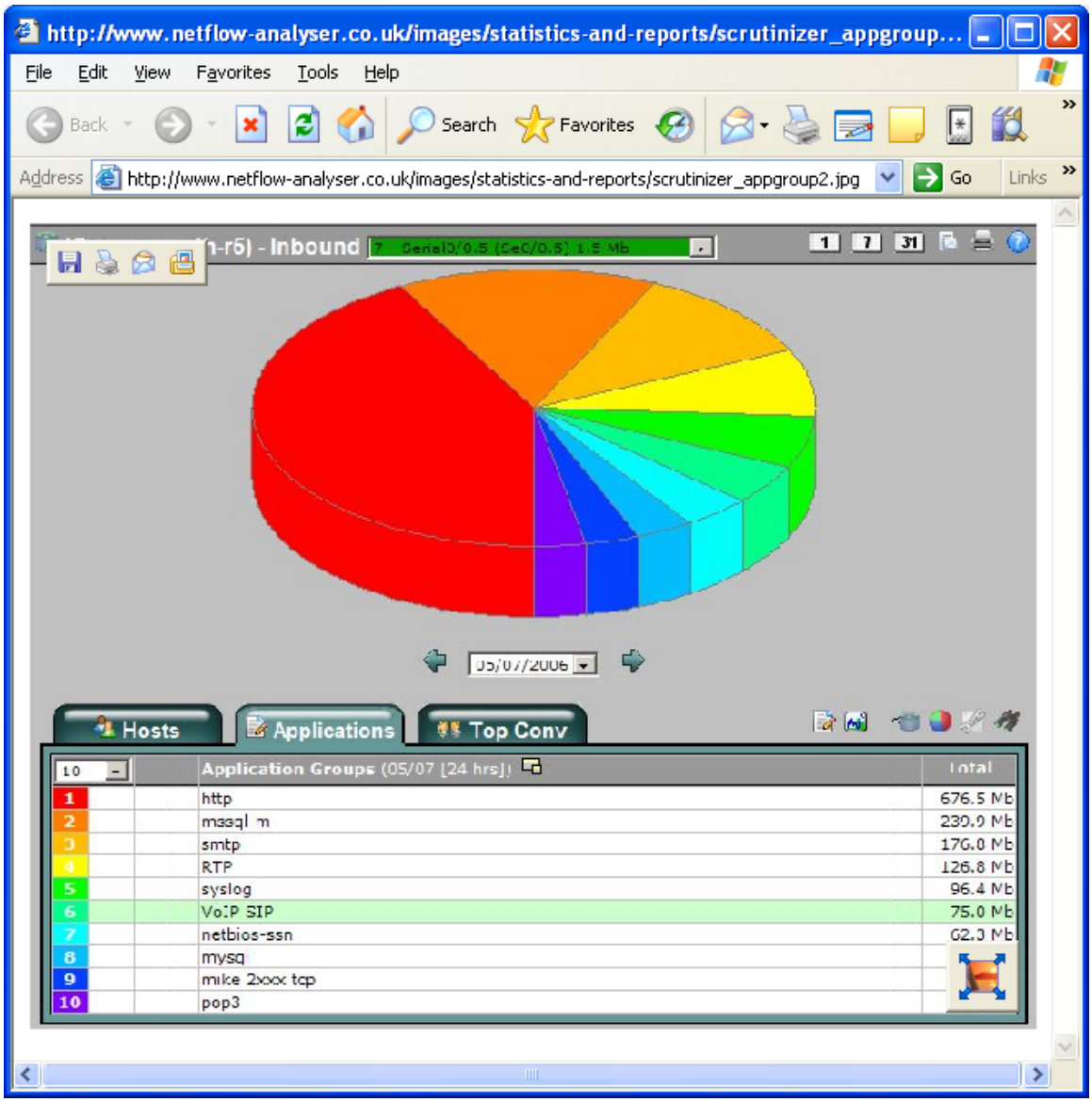
An example of a simple yet effective tool used to implement the first phase of policy deployment can be seen below.



Having an application-based matrix approach allows the network manager to easily match default policies with types of users or devices on a process control network.

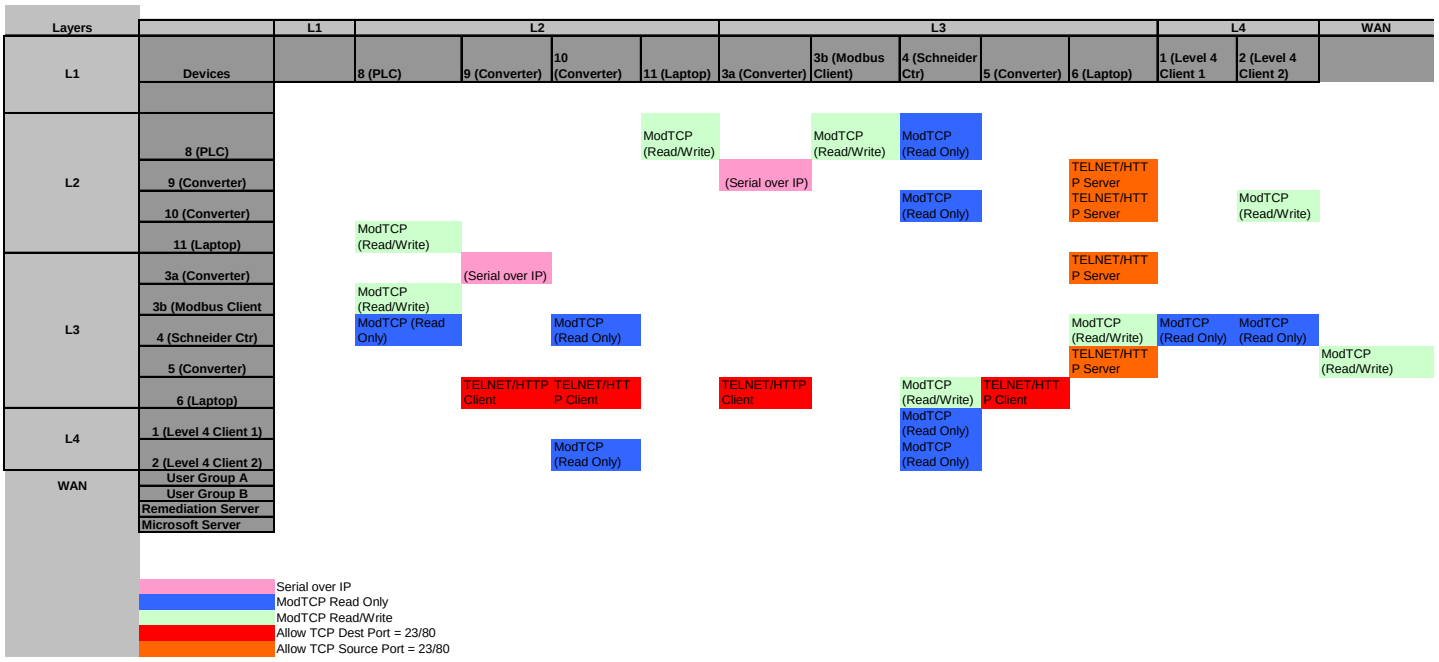
The second phase of implementing and enabling network security would be to add industry or site specific knowledge to further customize the policy profiles by identifying the TCP/UDP ports and protocols that are in use in the network. This will expand control and secure the network to only allow business justified communications over the network. For example, a network device such as an L1 sensor that sends measurements to a PLC at L2 which provides updates to a Historian in L3 uses very specific communications protocols that can be identified with the policy management application. Once identified, policy rules can use this information to construct a policy profile which controls and secures the communication between these specific mission-critical devices.

Using the NetFlow statistics from embedded agents in intelligent network switches, network administrators can view traffic flows and use tools to develop a granular model to provide reporting of the specific TCP/UDP ports and protocols that are in use on the network. This can then be put into a decision matrix that will be used for the creation of specific device roles and specific traffic rules to create a granular communication model that can be replicated throughout the process control network. This can provide deterministic communication control with central administration of device *role of least privilege* which institutes unsurpassed security at the network edge without the complexities of ACL management. An example of NetFlow traffic analysis reporting can be seen below.



Once the network has been modeled, a good strategy is to leverage a framework which allows policy to be deployed but not enforced. The policy framework should be able to identify which traffic is being classified by which policy rules without actually enforcing the rules. Network administrators can then use this information to help construct most effective policy profiles. Upon completion of this 2nd phase, a common device list associated with a role name will be mapped to a set of communications rules that will allow specific access over the specified protocols and TCP/UDP ports. These roles can be assigned to unique switch ports by a simple click within Policy Manager to assign the role to the port.

An example of how network analysis information can be used to determine additional policy requirements for securing data patterns between end systems and resources on the L1, L2, L3 network is seen below.



The final phase is the implementation of device authentication. Authentication enables policy roles to be assigned dynamically based on user or device identity and authorization.

Network authentication provides additional security by only allowing the users and devices that have proper trust or access credentials to gain entry to the process control network. To enable authentication, the network administrator should choose what authentication method is desired (802.1X, MAC-Based, Web Based or combinations of all three). Next, using a graphical configuration interface, authentication must be turned-on on the appropriate switch ports. Standards-based authentication will require some sort of AAA server such as a RADIUS Server. Depending on local site requirements and where authentication services are located, RADIUS can be local or remote, and can also be proxy. Local servers can be backed up by remote servers for redundancy.

If using Microsoft Active Directory, intelligent switches should fully support the user credentials that are in place today. Microsoft Server supports Windows IAS which is a RADIUS service. The switch is entered into IAS as a RADIUS client and a standards-based *filter-id* is used to tell the switch what policy role to assign an authenticating user or device. The Windows Server setup can be replicated to many installations and should be very close in its design attributes except actual user credentials.

Additional products like Network Access Control (NAC) can be useful to automate the role assignment of machine centric devices that authenticate using its MAC address. NAC is a solution that when implemented will scan devices to access the security posture and provide the ability to quarantine an offending device if it does not meet a pre-determined security posture. Using a NAC solution to can provide the ability to:

- Detect a device as it attempts to connect to the network.
- Authorize the device based on a pre-determined set of context.
- Assign the right network policy rules to the switch port where the device is connecting
- Track the device and report on its movement throughout the network.

NAC can be implemented in a phased approach as well with the 1st step to just learn and accept all MAC addresses and learn and track user connections. The 2nd step of NAC deployment would be to assign *MAC overrides* that would dynamically assign the already created roles in policy management to ports based on the authenticated device's MAC or user credentials. The 3rd phase of NAC deployment would be the introduction of device compliance which could include scanning end systems to see if they meet the corporate requirements to access the customer network.

The support and operation of the deployed policy framework must be simple yet effective to align with the process control network administration resources. When implementing policy in a process control network, it is of great advantage to have the roles and rules associated with the policy configuration stored in the distributed network environment itself. In the event that a network switch goes off-line and then re-establishes connectivity with the policy management server located either local or remote to the installation, the policy management application can automatically verify the switch's policy configuration. If the configuration is not current, the policy management application should alert the administrator that a role/rule mismatch exists and request that the switch be updated. The policy management application should also gather and track all device configurations and be used to track change management. In addition, the policy management application can push configurations to devices that may need configurations updates due to field replacement or for any other reason.

From a device perspective, there are many switches that have flash memory capabilities which can keep the switch configuration in the event that a field replacement is necessary. Core switches should have the ability to store running configurations on all system modules. In the event that a core switch loses its configuration or a replacement occurs, the configuration can be reloaded from a saved location on another module.

Summary

Designing and implementing Secure Networks for the modern process control environment is critical to ensuring safe and efficient communications and process operations. With the evolution of process control technology including dependencies on traditional Ethernet and IP based networking, an increase in operational effectiveness can be achieved. At the same time, increased security awareness is a must. Securing the process control network environment and the operational communications within is a strategic requirement.

A well conceived policy framework provides a key foundation for Secure Networks. It is the policy framework that enables critical integration of security-enabled infrastructure and centralized visibility and control. The right solution is one which allows customers to efficiently and effectively administer business communication and security policies, and ensure that the policies will be correctly enforced at the right location and time, and for the right person and end system.

Contact Us

For more information, call Enterasys Networks toll free at 1-877-801-7082
or +1-978-684-1000 and visit us on the web at enterasys.com

Thought Leadership
Over 500 global patents

enterasys®
Secure Networks™

Delivering on our promises. On-Time. On-Budget.