



Securing the Process Control Network

The Anatomy of Worm and Virus Threat Management

Securing the Process Control Network

Overview

It is the intention of all network administrators to provide network availability and business continuity while simultaneously ensuring the confidentiality and integrity of the information traversing the network. Since the proliferation of the personal computers as a driving force behind business automation, it has been the goal of network administrators to create an environment where information can be passed and business can be conducted without the constraints of overly restrictive security policies.

Working within the guidelines of a corporate security policy, the Enterasys strategy is to create an environment where a process control network administrator is instantly aware of who or what is connecting to the network while also verifying that a base-level of security has been implemented on the network and end systems. Based on this level of visibility, the Enterasys solution can assign a “business justified communications” configuration on the network that will allow specific end systems to pass traffic to only those systems deemed necessary and additionally limit communications to exactly which TCP and UDP ports are needed – thus reducing exposure of the network to the proliferation of worms and viruses. Enterasys has unique capabilities to proactively prevent and/or mitigate such threats by making it easy to deploy role-based access controls for wired and wireless environments with integrated management, priority, and security that deliver investment protection, operational efficiency, and significantly reduced total cost of ownership.

Through a “what you need is what you get” (WYNIWYG) approach to networking, Enterasys can ensure in real-time throughout the entire network that only the right users/devices can access the right information from the right place at the right time. The following chart provides a quick side-by-side comparison of Enterasys role-based access control policies compared to the VLAN/ACL approaches on firewalls and routers used by our competitors:

Enterasys	The Competition
Business-oriented based on users and applications	Technology-oriented based on ACLs, ports, and VLANs
Easy to administer with point-n-click GUI	Hard to administer through CLI
Embraces user mobility with IP-to-ID mapping and real-time location services	Manual reconfiguration for every move/add/change
Protection & priority within and between VLANs	Protection & priority only between VLANs
Unified policy definition across wired & wireless	Manual reconfiguration for every move/add/change
Automatic policy distribution across the entire network	Manual policy distribution box-by-box
Distributed policy enforcement anywhere and everywhere end-to-end	Centralized policy enforcement
Triggers automated responses	Requires manual responses
Granular visibility and control over individual user, application, and device flows	Restricted to ports and VLANs

The following examples are common threats to a Process Control Network:

Worm / Denial of Service (DoS) Example: Slammer Worm

To envision how a new attack can quickly cripple a network, it is only necessary to understand the success of attacks that have occurred in the past. The Slammer worm, for example, caused a massive DoS attack in enterprise environments. A quick Google search on “Slammer Worm Process Control” provides evidence that Slammer breached “closed secure” networks in the Process Control environment. This resulted in bandwidth saturation and network failure causing critical loss of processing capability and possibly creating safety hazards. It was a simple worm that operated by generating random IP addresses and sending itself out to those addresses. If a selected address happened to belong to a host that was utilizing a vulnerable version of Microsoft SQL Server Resolution Service, that host would immediately become infected and begin spreading more copies of the worm program. The danger was how fast it propagated, which underscores the need for automated response and port-level protection on every interface in the networked infrastructure.

Worms, viruses, and DoS attacks that have the ability to generate the same level of havoc are created every day. These malicious malware programs can enter an enterprise network via the Internet, a mobile device, or even a thumb drive. In an unprotected network, these attacks can cause the failure of critical systems. But these types of attacks can be easily remediated utilizing Enterasys policy-enabled switches configured with the concept of “business justified communications” enforced in real-time through role-based access controls that are easily created and distributed throughout the

entire infrastructure simultaneously. With deterministic communications that only allows specific communications from device-to-device, a worm, such as Slammer, would have been contained to the single device that became infected. Enterasys can also prevent, detect, and respond to more recent threats like “conficker” and “GhostNet/ghOst RAT”.

The following are examples of how Enterasys can apply policy to protect a process control network from a threat like Slammer:

1. Policy to block all Server ports like email, Web, DHCP, TFTP, and in this example SQL (UDP Port 1434 and UDP Port 1433) on client-end systems. Blocking these ports will not allow Slammer to move from server-to-server. This role-based access control is applied on all ports throughout the entire network, not just on WAN interfaces or Firewall interfaces.
2. Configure Access Policy to only allow specific communications from system-to-system, thus eliminating risk on normal PCS network traffic. Since only process control related communications is allowed, even if a server were infected through an external source, such as a USB port, viruses and malware cannot spread on the network. The concept of “least-privilege” access control denies all traffic except for specifically allowed business-oriented communications.
3. Policy to rate limit inbound traffic from end systems would limit a DoS attack. Because most Process Control networks require a low bandwidth rate of traffic, rate limiting the traffic between devices will minimize the effect of viruses and malware on other devices in the network. Bandwidth rate limiting allows specific protocols and applications to be given the highest quality of service (QoS) priority, yet protects against unlimited bandwidth usage if the particular protocol or application is somehow compromised.
4. Only allow SQL protocols/sockets to exist on defined “server access interfaces” if SQL is required only on specific systems. This removes the threat of Slammer or some other malware being introduced to the network accidentally by an “authorized user”.

Traffic Emulator Example

The traffic emulation tool pictured below is a free piece of software that can be downloaded from the following Internet web site: <http://3d2f.com/programs/32-559-trafficemulator-download.shtml>. This tool, which can run on any laptop or end system, is used legitimately to test servers, routers, and firewalls by generating massive amounts of ICMP, TCP, or UDP in an effort to simulate a heavy network load. Put in the hands of a malicious or careless user, this tool can be used to launch a Denial of Service (DoS) attack. Because Process Control Systems can easily be taken off-line by sending even small amounts of traffic, this tool (or one like it) can easily disrupt or completely bring down network operations if misused.

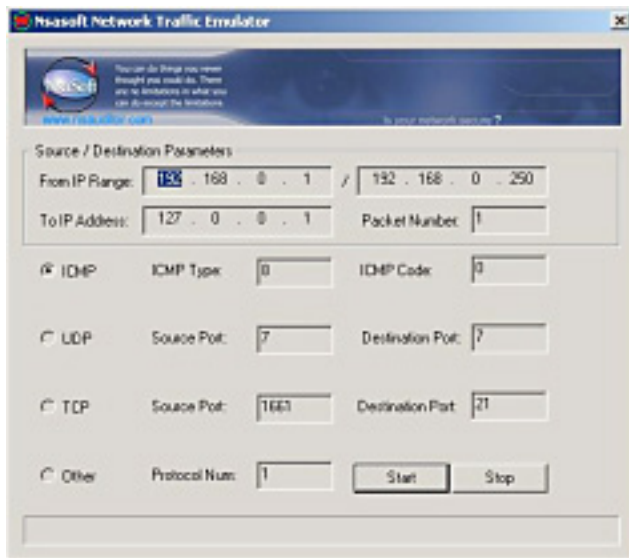


Figure 1

A document created by the Idaho National Laboratory specifically detailing the importance of security practices for Process Control Systems used, as an example, an incident of an attack upon a waste water treatment plant by a contractor working for that plant. It caused millions of liters of raw sewage to escape the plant and contaminated parks, rivers, and a local hotel. Because the network was ill prepared, it took two full months for the plant management to identify and stop the attack.

Typical Process Control Network Implementations

Traditional network switching infrastructure is designed to forward traffic from a source to a destination without considering the concept of “business justified communications”. A typical process control local area network (LAN) which operates at Layer 2 (L2) of the OSI stack, or VLAN layer, cannot restrict traffic between end systems on the network. Utilizing this open access approach to forwarding traffic from source to destination, most switching equipment cannot adequately protect process control networks from attacks. In other words, Enterasys can protect any and all communications within and between VLANs, whereas competitors can only protect communications between VLANs. If a single system is infected with malware, competitors will allow the infection to spread to all other devices within the VLAN at a minimum. Enterasys will prevent the malware from spreading to any other system – period.

Many Process Control System (PCS) environments block threats at the border utilizing routers or firewalls and Access Control Lists (ACLs) between Level 4 (L4) and Level 3 (L3) of the Purdue Reference Model. Sometimes these devices may also segment L3 from L2 and Level 1 (L1) (See Figure 2). Infections that rely on Windows File Sharing can easily reach their targets within each layer even in an environment where these services would not normally need to operate. Many Windows systems are not locked down and may allow network services that could become targets for worm and virus replication. Also, it is not uncommon for a virus or worm to initiate its own SMTP, TFTP, or HTTP services to launch remote control attacks on other end systems. DoS attacks can be launched from malicious users as described above.

The Purdue Reference Model

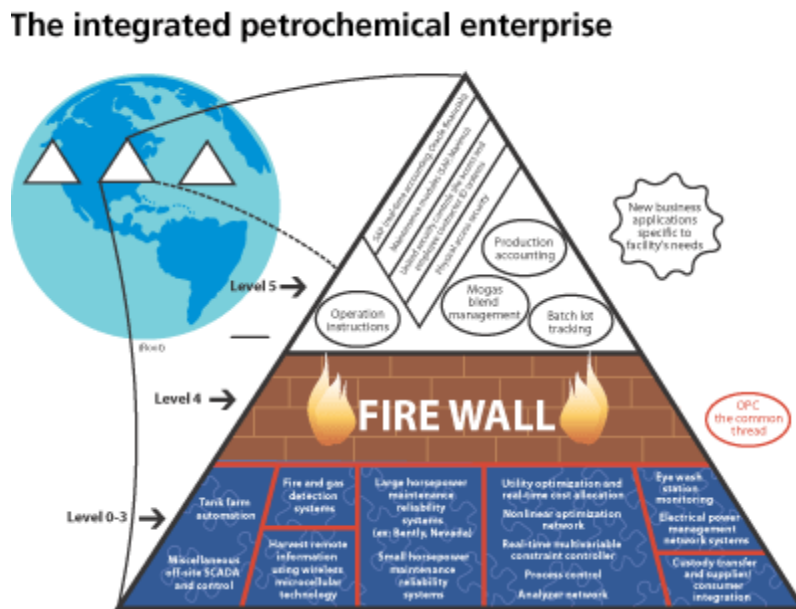


Figure 2

Purdue Model Definitions - Level 4 is the business Level, Level 3 is the Manufacturing Operations & Control Level and Level 2/Level 1 are lower Levels concerning primary data interfaces and measurement.

Enterasys Policy and Network Access Control (NAC) Strategy

Most organizations have a set of rules and acceptable usage guidelines that dictate how the network should be used. Enterasys Acceptable Use Policy provides a foundation for aligning actual network user and application behavior with these business objectives. It is a granular approach to role-based access control policies that includes specific network communications traffic permissions and restrictions based on the authenticated identity of a user or machine. Typically, an Acceptable Use Policy is formulated with input from a number of different business policies. The organization's security policy, for example, may specify network traffic and services that should be eliminated from the network. Other business policies may highlight how specific network services may be used, or which services are critical to the business and require priority access. Enterasys' unique identity-based networking solutions allow the network to provision required business services to users and devices automatically, while preventing undesirable and malicious traffic from entering the infrastructure.

Enterasys provides visibility of “who” or “what” is connecting to the network. Based on a successful authentication, the end system is assigned a “business justified communications” configuration profile that will dictate what resources can be accessed on the network. This is accomplished by enforcing policy capabilities on each port of an Enterasys switch, where rules can be crafted to permit, deny, rate limit, classify, or contain certain types of traffic based on Layer 2 (Source/Destination MAC Address, Ethertypes), Layer 3 (Source/Destination IP Address), or Layer 4 (TCP / UDP Ports) parameters.

Using these advanced policy capabilities Enterasys can deliver firewall-like control on every switch port as to what type of TCP and UDP traffic is allowed to communicate from end system to end system. If an end system, for example, becomes infected with a worm that uses email to infect other systems, a policy rule to deny email traffic applied to the network would stop that attack. Since email traffic should not be allowed on the L2/L1 network (Process Control), this infected system would not infect other end systems and therefore the worm would be contained to a single system.

By taking the same approach as a firewall, Enterasys can configure switching access to “deny all” and then only allow necessary communications between end systems. This will provide very predictable traffic use on the network and eliminate many threats that could appear on a Windows client.

Enterasys Networks also offers a Network Access Control (NAC) solution that can utilize the policy capabilities to provide end system assessment. This will ensure end system compliance to security policies; and that no vulnerabilities are detected on the end system before it can be allowed on the network. By definition, a typical NAC solution should encompass five components: Detection, Authentication, Assessment, Authorization, and Remediation. Enterasys integrates these five components into a closed-loop mechanism, once the end system is on the network. Specifically the Enterasys NAC solution provides the following capabilities:

1. Detection of a system as it connects to the network – the Enterasys NAC Solution provides detection of all networked devices as they connect to the network.
2. Authentication of device by secure guest web portal, MAC Authentication or 802.1X. With the implementation of Authentication, Enterasys can provide detection of all devices and only allow the “authorized access” to trusted devices and users. In the plant environment, a dual authentication method for guests is recommended where a local “trusted” contact would enter his or her credentials in addition to the guest before the guest is granted access and is authorized appropriately.
3. Assessment of end system to ensure proper client compliance – Enterasys can provide both agent-based and agent-less end system assessment to ensure that the end system meets the minimum requirements to be connected to the network. The assessment can check for vulnerabilities on the system, as well as ensure compliance with the security policy. Items that can be checked include but are not limited to: Anti-virus installed, running and up to date, desktop firewall enabled, and Automatic Windows Updates is enabled. It can also check for any unauthorized use of applications like FTP Servers or Peer-to-Peer applications. If the end system does not meet the established requirements to enter the network, the system will be quarantined so that it cannot harm the network.
4. Authorization of end systems and/or users determines what network communications are allowed from this end system – Enterasys switching products provide control of what traffic is allowed from an end system. Setting up this concept of “acceptable use policy” or “business justified communications” on a port of the switch is easy to deploy and manage. This capability can allow a Sensor at L1 to only have network communications with a specific PLC at L2 and allow the PLC to send updates to only a particular Historian at L3 using only the necessary communication protocols and TCP/UDP ports allowed for this transaction. By implementing this control, a large number of threats that can happen in a normal Windows environment can be eliminated.
5. Remediation – proactive quarantine, notification to user. Enterasys switching provides a method to quarantine the end system and provide notification to the user and systems administrator. Through this notification, users will have the necessary information and services to resolve issues (i.e. update anti-virus signatures) and get back on the network.
6. Post connect NAC using [Distributed Intrusion Prevention](#). Enterasys advanced security applications like [Dragon IPS](#) and [Dragon Security Command Console](#) provide capabilities to detect threats that may appear in the network over the necessary traffic protocols using deep packet inspection methods (OSI L7). Once detected through post-connect monitoring and behavioral analysis, these threats and anomalies can be mitigated at the source.

This Enterasys Switching infrastructure alone can be configured and implemented to provide Detection, Authentication, and Authorization (1, 2, & 4 above). With the addition of Dragon advanced security applications, all six items listed above are addressed. The tight integration of these technologies provides a holistic and proactive approach to process control network security.

Summary

With the increasing dependencies of open-standards Ethernet and TCP/IP-based network systems in the process control environment, it is now more critical than ever to address the security vulnerabilities common to these communication infrastructures. Leveraging the pervasive nature of the network infrastructure can provide a valuable asset in the overall approach to securing critical infrastructure. The use of access control, proactive protection, and dynamic response technologies provides the best holistic approach to network security in process control environments.

Leveraging the multitude of advanced technologies embedded in Enterasys products and solutions, a highly secure and effective operational model can be realized. With over 25 years of innovation in network communications technologies, centralized visibility and control solutions, and advanced security applications, Enterasys offers the process control industries a best-in-class architecture built on the foundation of business-oriented, role-based access control policies.

Covering all critical aspects of securing a network with access control, proactive protection, and dynamic response, Enterasys leads the way in securing critical infrastructure.

Appendix – Virus, Worm, Trojan Definitions

Virus - A malicious program that can replicate itself onto an unsuspecting host PC when unknowingly launched from its location on a portable USB drive, network file system, or an email attachment. The result of a virus may be immediate or time delayed and cause damage such as corrupting or deleting a user's files.

Worm - A self-replicating virus that utilizes the network to spread itself onto other networked PCs without a user's intervention or knowledge by exploiting operating system vulnerabilities or weak security components. Once a networked PC is infected, it becomes an additional attacker and further spreads the worm. The most widespread and damaging network worms in recent years have exploited vulnerabilities within Microsoft Windows services (e.g. Windows File Sharing) and may initially go undetected until system or network resources are exhausted.

Trojan - A malicious program deposited on an unsuspecting host PC (possibly by a computer worm or virus) with apparently useful or at least harmless capabilities. When in reality the Trojan has a hidden remote control channel to an attacker which may allow activities such as complete control of the infected host PC, dynamic view of the user's screen, user's keyboard activity, or the theft of files.

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



© 2009 Enterasys Networks, Inc. All rights reserved. Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications. Please visit <http://www.enterasys.com/company/trademarks.aspx> for trademark information.

