

Access Policy Tool (APT)

Monitoring tools for field level networks

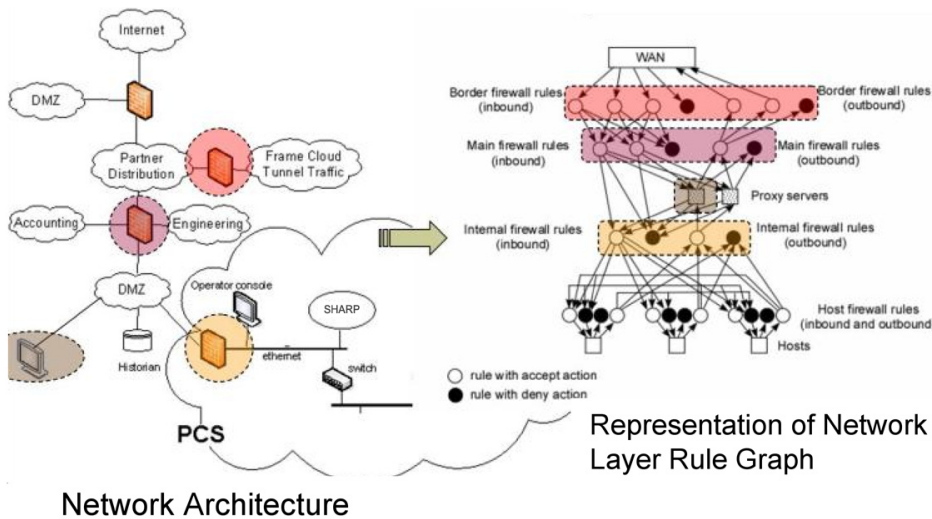
Overview

The Access Policy Tool (APT) developed by the University of Illinois at Urbana-Champaign (UIUC) supports secure operations by assessing whether the system of firewall rule-sets and host policy enforcement mechanisms correctly implements the desired access constraints. APT enforces separation between the Process Control Network and the rest of the system, thereby preventing cyber attacks.

What are firewall rule-sets?

The firewall is a critical asset in the protection of a network. The rule-set of a firewall configures it to provide customized protection based on the network assets. Network firewalls can block various traffic by protocol, such as file transfer and NetBIOS. For example, blocking of NetBIOS prevents users outside the firewall from accessing shared directories on the corporate network, but only if the firewall is configured properly. More complicated rules can separate the network into secure zones that limit user and application access between zones. For example, network traffic between the business network and the process control network can be limited to that which is required and in the required direction of flow.

Most companies configure firewalls to "deny all, permit none" with a few exceptions. The reality is that there are no "generic" rules that "fit all." The specific architecture of the system (e.g., the use of demilitarized zones (DMZ)) will determine which rules should be configured for effective security at a given site.



Key Benefits

APT considers not only firewall rule-sets but also host policies. It uses efficient algorithms to check for compliance with respect to global access constraints. APT provides fast online monitoring of policy implementation to customers.

The product can be used on large-scale process control systems (PCS) and corporate network interface systems.

The product will initially focus on common commercial technologies:

- Ethernet®, TCP/IP, Windows®, Linux, and Cisco firewalls.
- It may be adapted to proprietary technologies as needed.

The tool can be used:

- Before deployment as a system design aid
- In an operational system to find problems with global access compliance and augment online security monitoring

Features

- Can be used to verify correctness of existing policy implementations or to architect new implementations that meet desired global policy constraints
- Able to compare security policy that is actually implemented with security policy that is intended (based on business needs and use)
- In online mode, can detect changes in local policies that lead to global policy violations

About UIUC



UIUC is one of the world's leading universities in computing and information trust. The researchers are active participants in the Information Trust Institute (ITI), which provides national leadership combining research and education with industrial outreach in trustworthy and secure information systems. See www.iti.uiuc.edu

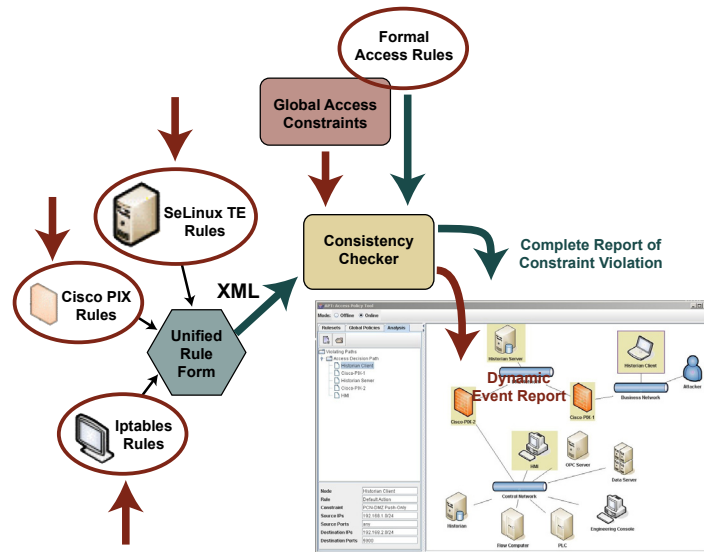
Researcher Contact Information

David Nicol nicol@iti.uiuc.edu William H. Sanders whs@iti.uiuc.edu

Technical Description

Based on the network topology, data flow, host policies, and firewall rule-sets, APT provides:

- A “rule graph” representing the network interconnectivity and data flow among enforcement rules.
- Rule graphs provide two layers:
 - Network layer - Modeling the PCS network topology and firewall rule-sets.
 - Host layer - Modeling the access control mechanisms within the constituent hosts in the PCS network, as well as the host layer graphs linked to host nodes in the network layer.
- Rule graphs are analyzed for global access violations.
 - exhaustive analysis or scalable statistical analysis
 - root cause of violations identified
- Enforcement of access compliance to known rules based on sensitivities; e.g., process control network, personnel information, business/competition sensitive.
- Fast online monitoring of policy implementation.



- **Unified Rule Form** - Rule collection uses secure connections, converts to XML for consistency; format is specified by schema.
- **Consistency Checker** – Checks that the global security policy of the PCS, as implemented via local rule-sets, matches the desired global policy specification.
- **Graphical User Interface** – Supports specification of network topology and provides interface to consistency checker.
- **Reporting** – Report identifies all access constraints that are violated. For each violation it reports all source/destination entities involved in the violation, the implemented rules that permit the violation, and the traffic attributes involved in the violation.

The output “screen” indicates:

- Node name
- Rule
- Constraint
- Source ID (IP address)
- Destination ID (IP address)

Functional Description

Global access constraints specify a subset of the global security policy, e.g.,

- **Traffic-specific** - The policy should specify supported protocols and restrictions by network address range.
- **Role-specific** - The role of the firewall will determine what rules are used; internal, main, and border firewalls should be more restrictive the closer they get to the WAN.
- **Application restrictions** - Roles of servers, process control devices, and user workstations should be standardized in order to provide consistent security.

There are published guidelines (i.e. National Infrastructure Security Co-ordination Centre (NISCC) good practice guide on firewall deployment for SCADA and process control networks) to facilitate development of unique rule-sets for an operating site. For example, a general rule listed in the NISCC’s document reads, “all permit rules should be both IP address and TCP/UDP port specific, and stateful if appropriate.” Subsequently, a knowledgeable network site administrator would determine the enabling and disabling granted on a case-by-case basis.

Summary of Costs

	Low	Medium	High
Component	<\$1,000	\$1,000-\$10,000	>\$10,000
Engineering	Drop-in	Moderate Modification	Complete System Design Lifecycle
Bandwidth/Network Burden	None-Passive Only	Moderate Traffic, Medium Overhead	Heavy Traffic, Large Overhead
Training	No Training Required	Moderate Training	Intensive Training. Additional Staffing May be Required.
Maintenance and Operation	< 1 Hour Per Week	< 5 Hours Per Week	> 5 Hours Per Week

Technology Transfer and Readiness: Bench-tested.

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.



The I3P is managed by Dartmouth College.