NetAPT use case: how it works for **Utility auditors and compliance officers**

How the utility sector's auditors and compliance personnel can use NetAPT to **dramatically streamline their audit and vulnerability assessment process** through comprehensive security policy analysis of firewall configurations

KEY FACTS: HOW NetAPT MEETS THE SECURITY COMPLIANCE NEEDS OF THE UTILITY SECTOR

Allows for **complete, fast review of complex firewall configurations, giving users a way to visualize and quickly identify flows that are undesirable**

Verifies all access points to the Electronic Security Perimeter (ESP), as per NERC standards CIP 005 R2 and CIP 005 R4.3

Provides **verification of ESP documentation** as per CIP 005 R1

Provides a **means to review ports and services allowed to cross access points to the ESP**, as per CIP 005 R2 and CIP 005 R4.3

Gives auditors a way to **review security controls inside ESPs without directly accessing the ESPs**; can be run offline and/or whenever a change is made to firewall configurations or flow policies

Significantly reduces time spent in review of firewall configurations

Gives auditors the **ability to generate consistent presentations of sensitive data across multiple utilities** by using a standardizing tool

Background

The North American Electric Reliability Corporation (NERC) has issued Critical Infrastructure Protection (CIP) standards that regulate cyber security compliance for the U.S. Bulk Electric System (BES), with the goal of supporting reliable operation. CIP regulations 002 through 009 provide a best practice approach on a narrow set of assets identified as "Critical Cyber Assets."[1]

In version 3 of the CIP, CIP 005, addressing "Electronic Security Perimeters" (ESPs), presents challenges in both compliance and audit. Requirement R1 calls for the documentation of an ESP and the access points to it. Security controls called for in R2 ask that utilities document organizational processes and technical and procedural mechanisms for control of electronic access; access is to be denied by default, and only ports and services required for operation are to be enabled. The vulnerability assessment requirement of CIP 005 calls for a review of controls to verify that only the required ports and services are enabled. It also calls for the discovery of all access points to the ESP.

The need for a tool

- Many utilities use firewalls as the primary mechanism for establishing access points to their critical systems; unfortunately, the ports and services available in a firewall are not easily ascertained without the use of a tool or the expenditure of significant man hours.
- Many utilities are using a laboriously generated combination of Visio-type diagrams and the configurations of their firewalls to define the ESP and security controls surrounding the ESP.
- In the absence of an automated method to verify the diagram of the ESP, manual review of long and often complex firewall configurations (which sometimes exceed thousands of lines) is time-consuming and error-prone.
- At the same time, audits are typically scheduled to last only a matter of days, and auditors need a method to process the complex data without connecting to the network.

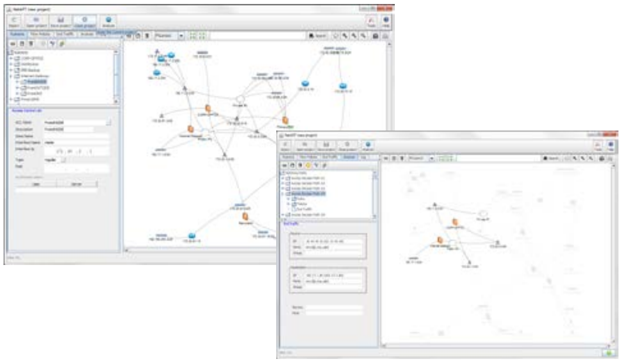
How NetAPT meets the need

- Designed to work offline, using firewall configuration files loaded into the tool by the user.
- Provides graphical connectivity maps generated from information parsed from the firewall configuration files. The views are filterable (to isolate specific subnetworks or

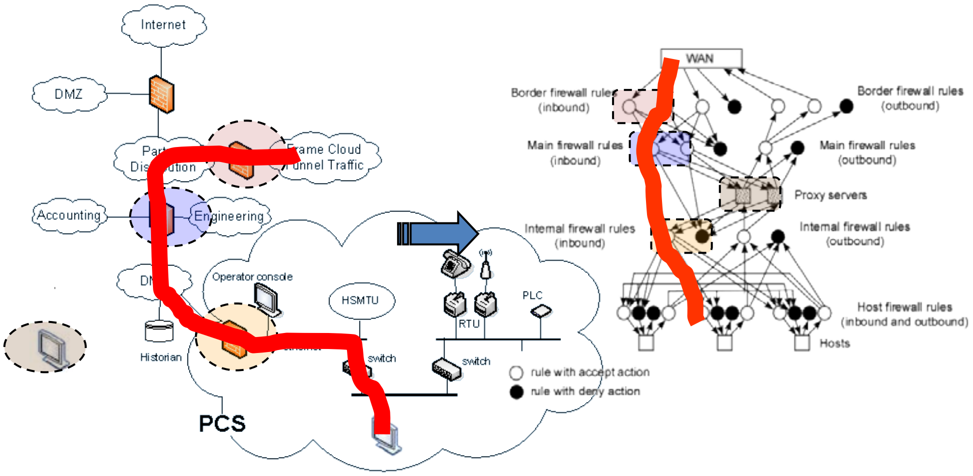
[1] http://www.nerc.com/page.php?cid=2%7C20

traffic flows) and customizable. For example, critical networks can be moved around on the canvas such that they are better highlighted, making later analysis easier. End nodes can be color-coded so that the relative importance of a node can be easily seen. The connectivity maps may be saved as jpg images to provide documentation of ESP layouts.

- Performs analysis by comparing flow policies entered by the user against the automatically parsed firewall configuration files. Can discover every path possible between subnetworks (including paths between devices in a specific network of interest) and reports any traffic flows that match the flow policies. Analysis can show all traffic allowed through any access point into the critical network, and will help to verify that all Critical Cyber Assets are accounted for.
- Allows users to apply filters to the rulesets. For example, one might filter to reveal only the traffic that results from rules with netmasks greater than /24, rules with "any" as the source or destination, rules with publicly routed IP addresses, or "deny by default" rules.



- Supports review of ports and services by either highlighting all incoming traffic, or showing traffic flows for specific ports. Documents flows by filtering traffic based on ports and policy.
- Outputs ports and services listings in a csv- or xml-format results file. All fields from the analysis and annotations are exported to the csv file, which can be further annotated and sorted in an external spreadsheet program, such as Microsoft's Excel. The annotation feature allows operations and technical people to comment on the connectivity allowed at the critical access points, assisting in the creation of documentation.


Internet
DMZ
Part Distribution
Frame Cloud Tunnel Traffic
Accounting
Engineering
Operator console
Historian
HSMTU
RTU
PLC
switch
switch
PCS
○ rule with accept action
● rule with deny action
WAN
Border firewall rules (inbound)
Border firewall rules (outbound)
Main firewall rules (inbound)
Main firewall rules (outbound)
Proxy servers
Internal firewall rules (inbound)
Internal firewall rules (outbound)
Host firewall rules (inbound and outbound)
Hosts

How NetAPT sees a system: a network architecture is on the left; on the right is a network-layer rule graph portraying that network architecture, reflecting how NetAPT might perceive it logically. The red lines show the same path as it appears in both views. Analysis is based on identification of paths in the internal rule graph, where each hop in the path corresponds to a policy implementation.

NetAPT Service Center

(217) 265-6382
netapt-info@iti.illinois.edu

NetAPT website

www.perform.csl.illinois.edu/netapt/

Visit the website to obtain information on licensing NetAPT, to submit a bug report, or to subscribe to the user mailing list.

ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN