▶ **NetAPT** use case: how it works for **Utility leadership and management personnel**

KEY FACTS: HOW NetAPT HELPS UTILITIES MEET CYBER SECURITY AND REGULATORY GOALS

Significantly **reduces time spent by technical and compliance personnel** in review of firewall configurations

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

Verifies all access points to a utility's Electronic Security Perimeter, **reveals all traffic flows within the system**, and **provides easily human-readable, graphical and textual documentation** of a system's compliance with best-practice access policies, as per NERC regulations

How NetAPT can **dramatically streamline utilities' cyber security assessment process** through comprehensive analysis of firewall configurations, thus **avoiding the expense, uncertainty, and extensive labor** involved in manual validation of system security and compliance with industry cyber security regulations

Background

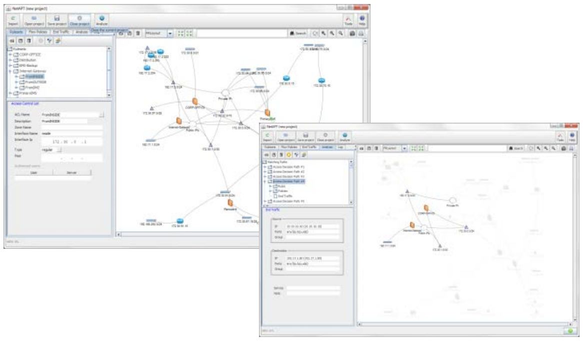
The North American Electric Reliability Corporation (NERC) has issued Critical Infrastructure Protection (CIP) standards that mandate cyber security compliance for the U.S. bulk electric system, with the goal of supporting reliable operation[1]. Utilities that fail to comply may be subject to fines or other sanctions, and may fall victim to cyber attacks that exploit their weak security stance.

Thus, **utilities need a way to verify that their systems deny access to all traffic that isn't necessary for proper operation of critical system functions.** The tool also provides a mechanism for documenting the traffic flows as required in the NERC CIP regulations.

The need for a tool

Most utilities use firewalls as the primary mechanism for establishing access to their critical systems; unfortunately, the firewall configurations may be long and complex, sometimes exceeding thousands of lines. **In the absence of a tool that automates the process, a significant expenditure of person-hours is needed to ascertain the ports and services available in a firewall.**

How NetAPT meets the need

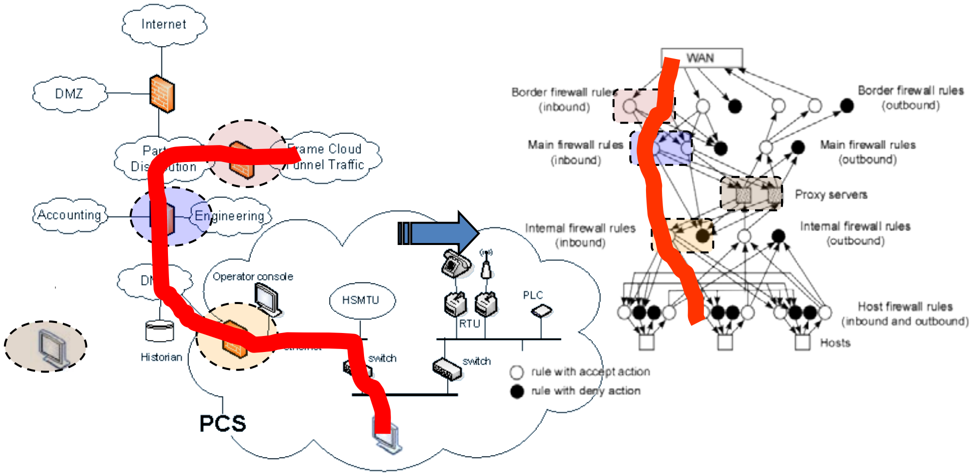


- Designed to work offline, using firewall configuration files generated by a system's firewalls and loaded into NetAPT by the user.
- Provides filterable, customizable graphical connectivity maps generated from information parsed from the firewall configuration files.
- Can discover every path possible between subnetworks (including paths between devices in a specific network of interest) and reports on traffic paths

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

made possible by the rules that are in the firewalls. Analysis will show all network traffic associated with access points.

- Allows users to apply filters that provide views resulting from certain rules or involving certain devices or subnetworks.
- Outputs analysis results in the form of annotatable files that can be manipulated in an external spreadsheet program, such as Microsoft Excel. In addition, NetAPT can generate screenshots of the graphical connectivity map, providing another useful form of documentation.


Internet
DMZ
Part
Dis ution
rame Cloud
unnel Traffic
Accounting
Engineering
DI
Historian
Operator console
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