▶ **NetAPT** use case: how it works for **Network administrators at utilities**

KEY FACTS: HOW SYS ADMINS CAN USE NetAPT TO SOLVE SECURITY ISSUES AND SUPPLY COMPLIANCE OFFICERS WITH NEEDED INFORMATION

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

Gives compliance officers auditors a way to **review security controls inside your system based solely on your firewall configuration files, with no need to directly access your system**; 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

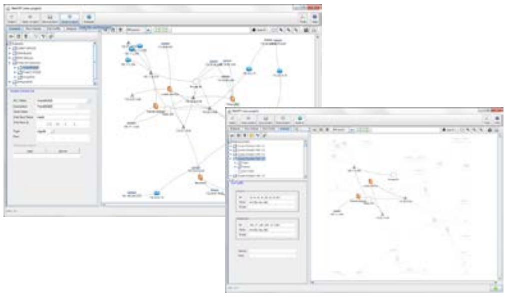
If you're responsible for maintaining the computer networks for a utility, NetAPT's comprehensive security policy analysis of firewall configurations can help you **easily provide compliance officers with the information they need about your system**, and can help you solve practical problems, like **identifying causes of connectivity problems in your system**.

Examples of NetAPT use to support system administration

- If someone puts in a request for access, the system administrator may want to be able to check the firewall rules already in place to see whether the access is already allowed, or to see which rules would need to be adjusted to provide for that access.
- Suppose that a certain host is supposed to be able to get into a network, and something is blocking it. The administrators may want to look at a list of all the rules in place, and try to figure out why a rule that they put in a certain position isn't working. In NetAPT, you can analyze your firewall rules to isolate which rules are causing connectivity issues.
- By revealing the traffic that goes through VPN tunnels, NetAPT can help determine the best places to locate intrusion detection systems (IDSes). It can show where IDSes may not work because traffic is encrypted, and where possibly critical traffic is going to be decrypted—potentially being a good place to put an IDS device to monitor the traffic.
- You can locally edit rule-sets and policies to play "what if" games and then remove problems in accordance with likely root causes suggested by NetAPT.

Background

NetAPT was originally inspired by electric power utilities' need for a user-friendly way to establish and document their compliance with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. However, it is useful far beyond that, supporting other practical decision-making and problem-solving related to firewall configurations.



NERC's CIP standards regulate cyber security compliance for the U.S. Bulk Electric System; utilities must undergo periodic security audits and supply documentation of all flows that can reach critical cyber assets[1]. Firewalls are the primary mechanism utilities use to establish access points to their critical systems. Unfortunately, the traffic flows in a firewall are not easily ascertained; in the absence of an automated analysis method, manual review of long and often complex firewall configurations is time-consuming and error-prone. NetAPT was created to ease that burden.

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

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

How NetAPT works

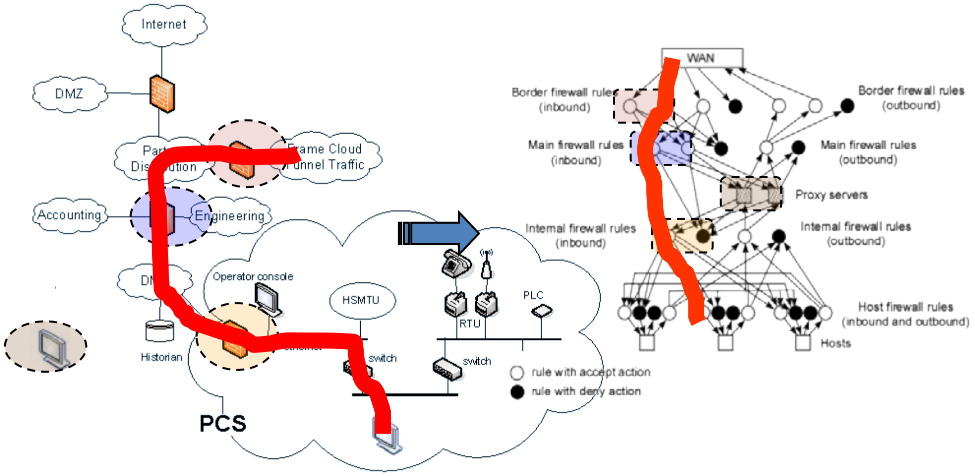
- **Designed to work offline, using firewall configuration files loaded into the tool by the user via the graphical front-end**. NetAPT uses the elements of connectivity information available in the configurations (such as CIDR descriptions of subnetworks facing FW interfaces, route statements, and VPN descriptions) as the basis for "growing" an inferred topology.

- **Provides complete graphical connectivity maps** generated by NetAPT from information parsed from the firewall configuration files. The views are **filterable** (to isolate specific subnetworks or 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. DNS or hosts file reverse-lookup can be used to label nodes appropriately. The connectivity maps may be saved as jpg images.

- **Performs analysis by comparing flow policies entered by the user against the automatically parsed firewall configuration files**. Application of a "report all access" policy will report every path possible between subnetworks (including paths between devices in a specific network of interest). Object groups can be defined in order to focus on specific areas or aspects of the system. Analysis will show all incoming traffic allowed networks defined in the flow policy statement, and will verify the presence of sound security controls.

- Allows users to **apply filters to the rule-sets**. For example, you 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.

- **Outputs analysis results 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 communication within the team and in creation of documentation.


Internet
DMZ
Part Distribution
Frame Cloud Tunnel Traffic
Accounting
Engineering
DM
Operator console
HSMTU
Historian
ethernet
switch
switch
RTU
PLC
PCS
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
○ rule with accept action
● rule with deny action

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.