Online Training: NP-View Workflow & Remote Network Access Verification

Network Perception
support@network-perception.com
(872) 245-4100

NP-View Training Webinar #2
May 7, 2020

Agenda

- **Reminder on NP-View Resources:** [5min]
  - Portal website and release cycle
  - Knowledge Base, Tech Support, and File Vault
  - Spring 2020 release
- **NP-View Training:** [25min]
  - NP-View Workflow
  - NERC CIP requirements
  - Importing Configurations
  - Reviewing the Topology Map
  - Verifying Network Accesses
  - Demonstration
  - Additional Topics
- **Q&A**

Reminder on NP-View Resources

- **Resources**:
  - Portal: portal.network-perception.com
  - Knowledge Base: kb.network-perception.com
  - Support: support@network-perception.com

- **Solutions:**

NP-View Java	Legacy user interface (Stable)	**Offline desktop application for snapshot audit**
NP-View HTML	New user interface (Beta) New license format	
NP-Live		**On-premise server for continuous config monitoring**

- **Releases:**
  - Quarterly stable release cycle (roadmap)
  - Continuous patch releases (support requests)

- **Config Sanitizer and File Vault**:

Spring 2020 Release

- **Upcoming Versions:**
  - NP-View: 6.1.2
  - NP-Live: 1.7.1

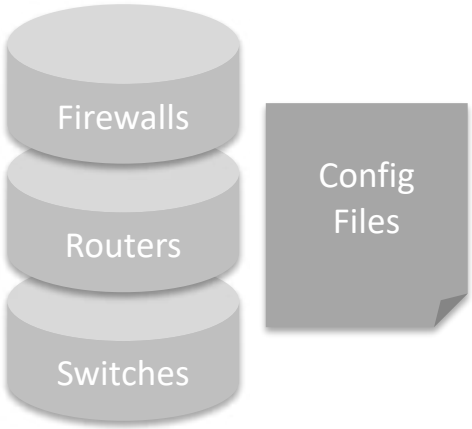
- **Release Notes:**
  - **NP-Connect** – Improved ability to select specific devices for importing into a workspace when connecting to a Network Configuration Manager or a Shared Volume.
  - **New Parsers and Connectors** – New connector and utility script to easily import Check Point R80 and Panorama rulesets.
  - **Policy Manager** – Improved control over your device policies including the ability to add, edit and delete policies / requirements as well as disabling entire policies or specific requirements.
  - **UI/UX Improvements** – User personas have been developed to improve user interface, product navigation and workflows.

Remote Access Verification

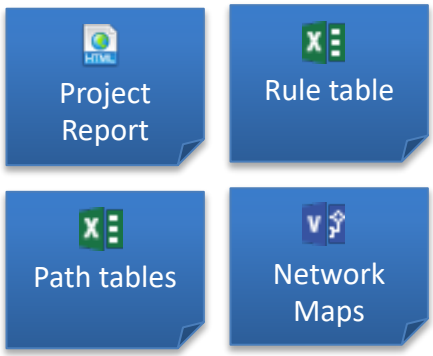
NP-VIEW TRAINING

NP-View Workflow

Input → Process → Output



np-view



Workflow:

1. Import configuration files
2. Review and customize topology map
3. Mark asset criticality and define visual groups
4. Review rules and add justifications
5. Review object groups and mark criticality
6. Run path analysis and verify network accesses
7. Export findings

NERC CIP Requirements

- **Preparation:** Collect and import applicable configuration files from firewalls, routers, and switches into NP-View
- **Topology Map Review:** identify applicable Cyber Assets and Electronic Security Perimeter(s)

  CIP-005 R1.1: All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP

  CIP-005 R1.2: All External Routable Connectivity must be through an identified Electronic Access Point (EAP)

- **Rule Audit Review**

  CIP-005 R1.3: Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default

- **Path Analysis and Interactive Remote Access**

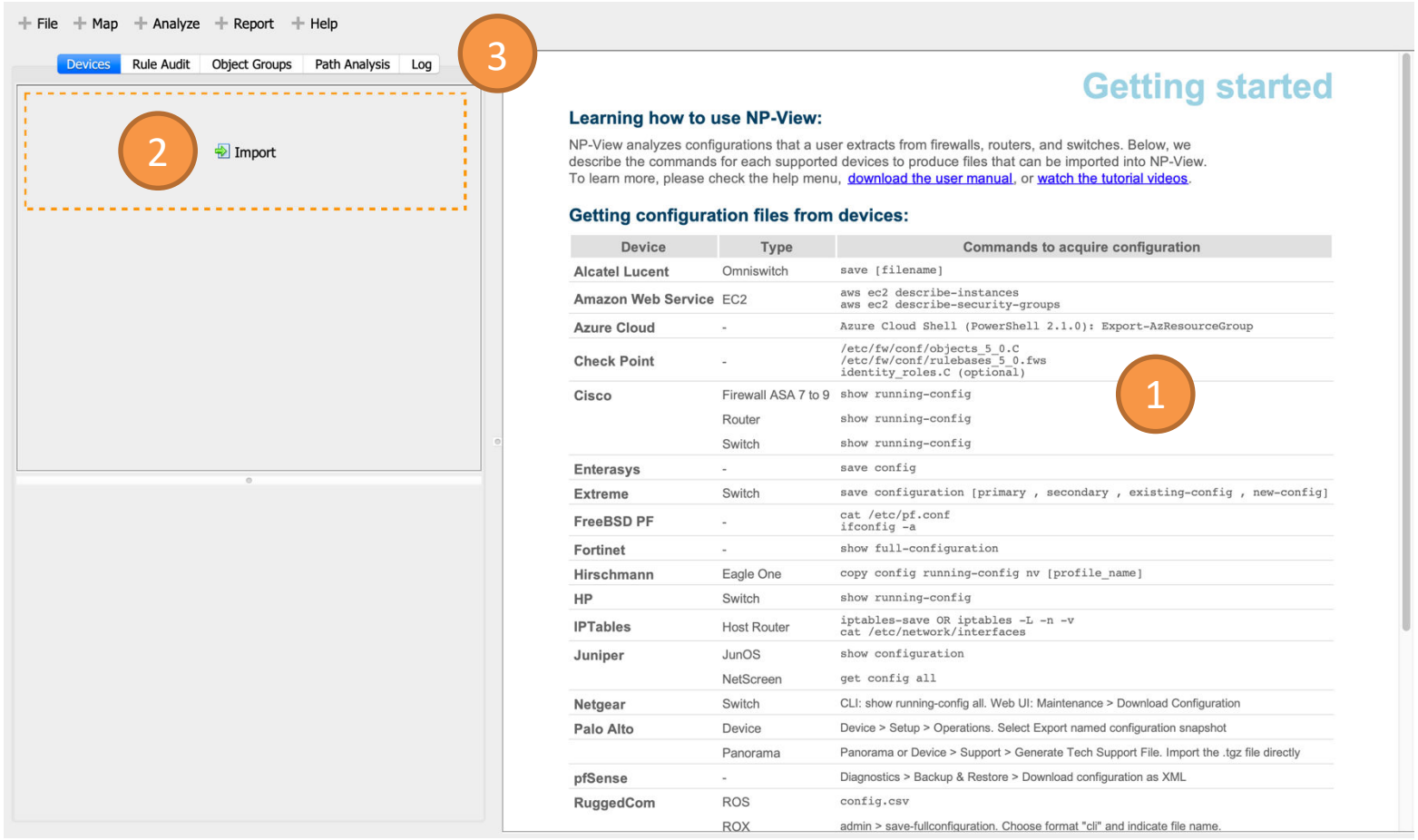
  CIP-005 R2.1: Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset

  CIP-005 R2.2: Interactive Remote Access sessions must be encrypted to the Intermediate System to protect the confidentiality and integrity of the communications

- **Document findings**

Importing Configurations

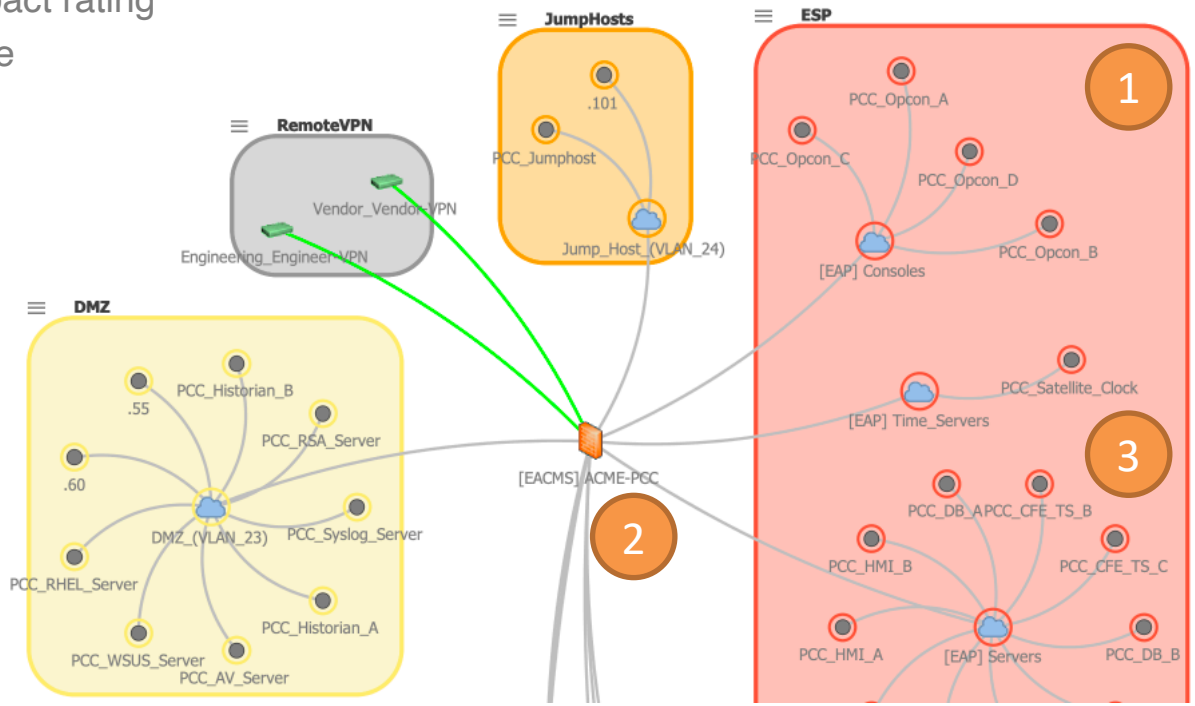
- Step 1: Review instructions to export your device configuration file(s)
- Step 2: Drag-and-drop the files into the import area
- Step 3: Review the log tab and use the “Contact Support” if an error occurs



Device	Type	Commands to acquire configuration
Alcatel Lucent	Omniswitch	save [filename]
Amazon Web Service	EC2	aws ec2 describe-instances aws ec2 describe-security-groups
Azure Cloud	-	Azure Cloud Shell (PowerShell 2.1.0): Export-AzResourceGroup
Check Point	-	/etc/fw/conf/objects_5_0.C /etc/fw/conf/rulebases_5_0.fws identity_roles.C (optional)
Cisco	Firewall ASA 7 to 9	show running-config
	Router	show running-config
	Switch	show running-config
Enterasys	-	save config
Extreme	Switch	save configuration [primary , secondary , existing-config , new-config]
FreeBSD PF	-	cat /etc/pf.conf ifconfig -a
Fortinet	-	show full-configuration
Hirschmann	Eagle One	copy config running-config nv [profile_name]
HP	Switch	show running-config
IPTables	Host Router	iptables-save OR iptables -L -n -v cat /etc/network/interfaces
Juniper	JunOS	show configuration
	NetScreen	get config all
Netgear	Switch	CLI: show running-config all. Web UI: Maintenance > Download Configuration
Palo Alto	Device	Device > Setup > Operations. Select Export named configuration snapshot
	Panorama	Panorama or Device > Support > Generate Tech Support File. Import the .tgz file directly
pfSense	-	Diagnostics > Backup & Restore > Download configuration as XML
RuggedCom	ROS	config.csv
	ROX	admin > save-fullconfiguration. Choose format "cli" and indicate file name.

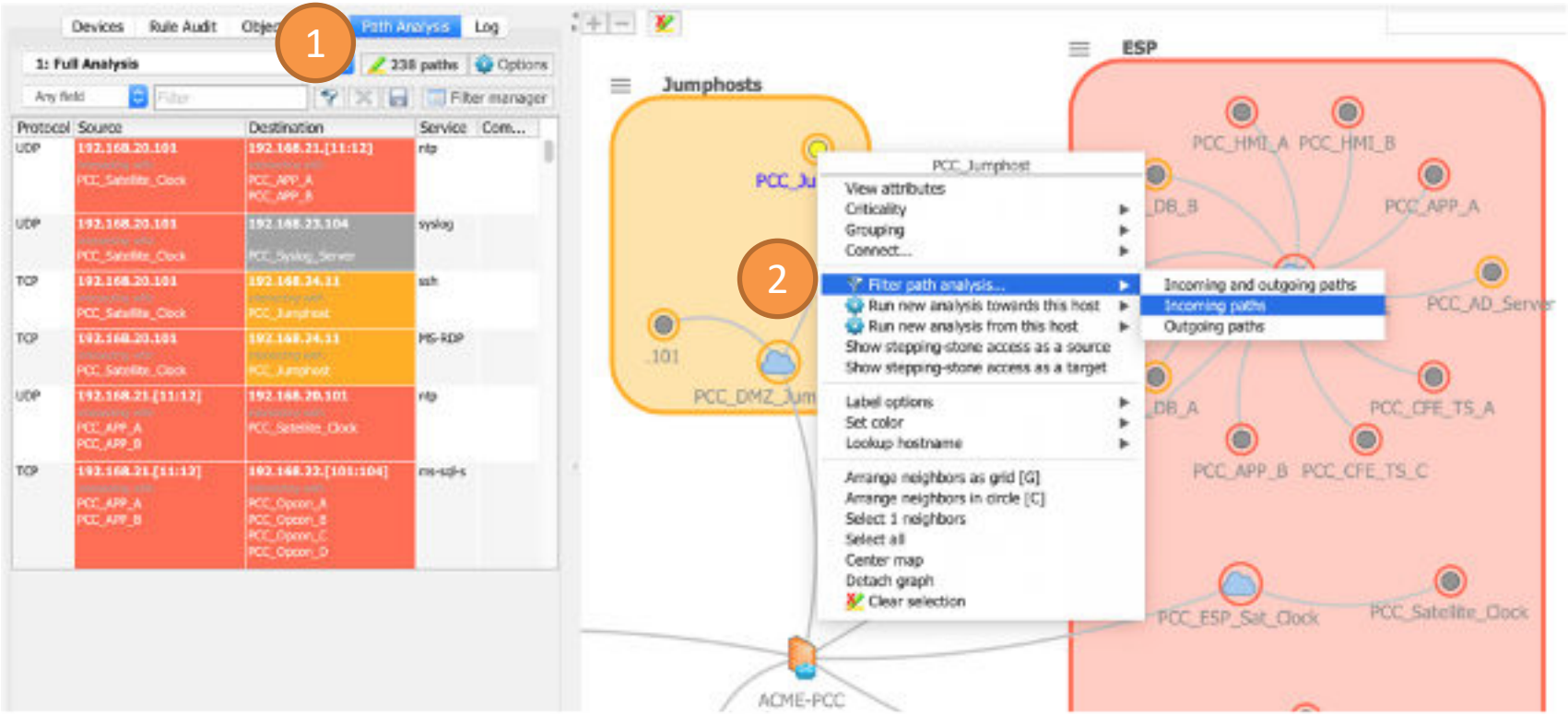
Reviewing the Topology Map

- Step 1: create **visual groups** to identify network zones
- Step 2: identify and **label** the following assets using your asset inventory:
  - EACMS (Electronic Access Control or Monitoring System)
  - EAP (Electronic Access Point)
  - PCA (Protected Cyber Assets)
  - IS (Intermediate Systems) or Jump Hosts
  - Remote cyber assets and VPN end points
- Step 3: assign **criticalities** to groups and assets:
  - High / Medium / Low: impact rating
  - Untrusted: everything else



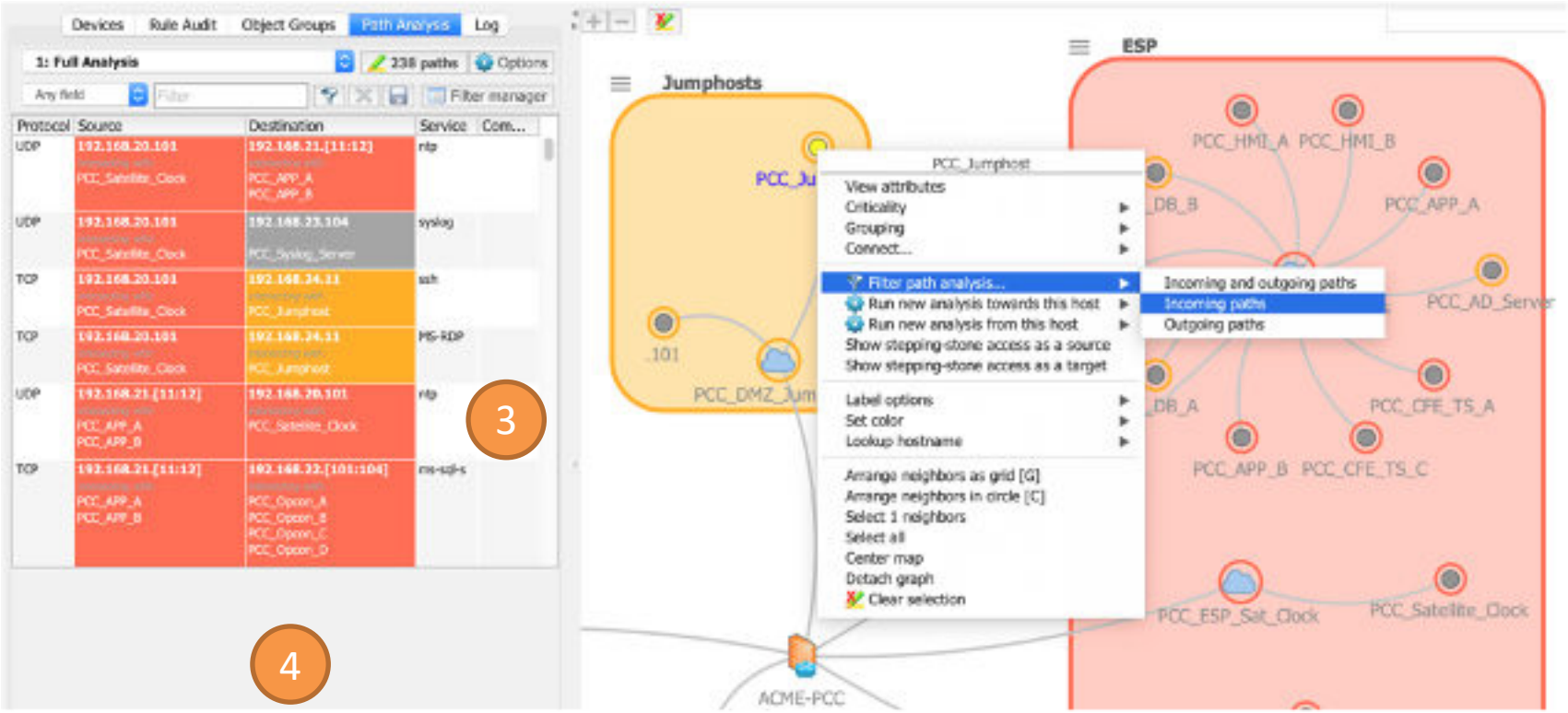
Verifying Network Accesses

- Step 1: run a path analysis
- Step 2: right-click on a cyber asset and filter incoming / outgoing paths



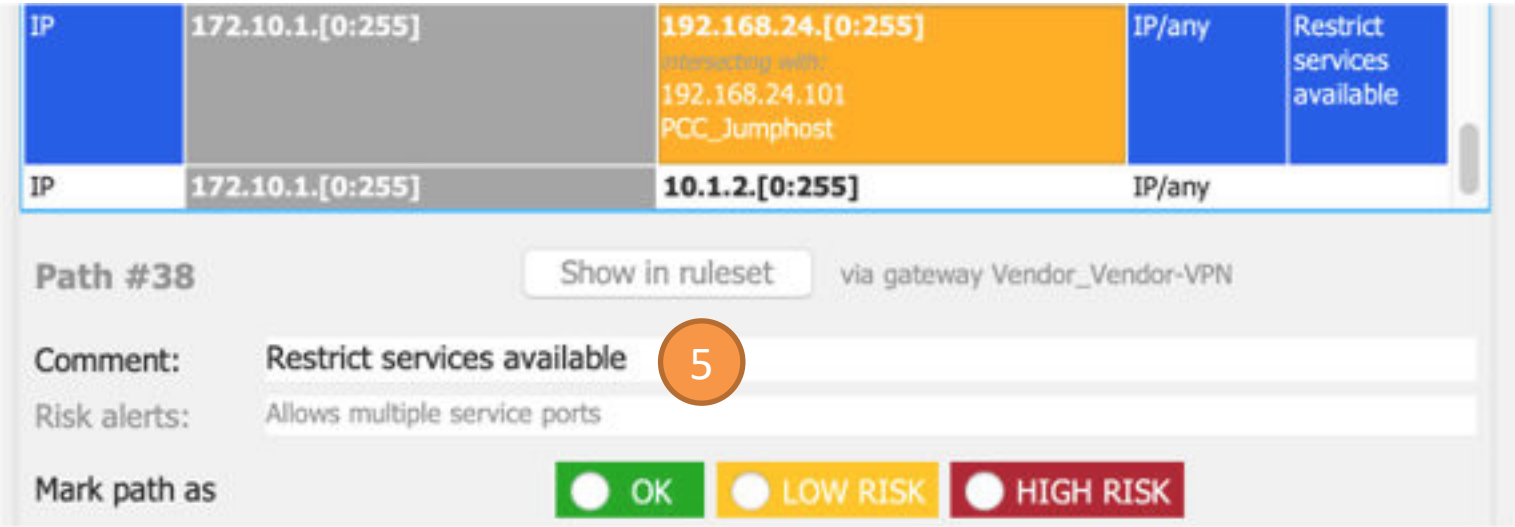
Verifying Network Accesses (cont.)

- Step 3: review accessible ports and services from the path table
- Step 4: review the rule(s) permitting the selected path(s)



Verifying Network Accesses (cont.)

- Option 1:
  - Step 5: annotate issues in path table
  - Step 6: export the “Comments report” to document findings
- Option 2:
  - Step 5: export the path table to Excel
  - Step 6: document findings within the Excel spreadsheet
    - Add a screenshot of the highlighted path(s) from the topology map to illustrate issues



Demonstration

Common interactive-capable remote access ports:

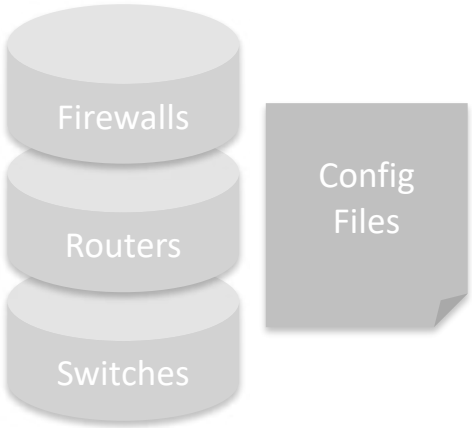
Remote Access Client	Protocol	Well-Known Ports
FTP Client	File Transfer Protocol (FTP)	TCP/20, TCP/21
Free commercial programs	Secure Shell (SSH)	TCP/22
Terminal Emulator	Telnet	TCP/23
Web Browser	HTTP, HTTPS	TCP/80, TCP/443, TCP/8000, TCP/8080
MIB Browser	SNMP	TCP/161, UDP/161
File Explorer, etc.	SMB	TCP/445
Unix r-commands	rlogin, rcp, rsh, etc.	TCP/513
Oracle SQL *Net	Oracle database	TCP/1521-1525
Remote Desktop	Remote desktop protocol	TCP/3389
File Explorer, etc.	NFS	TCP/2049, UDP/2049

Additional Topics

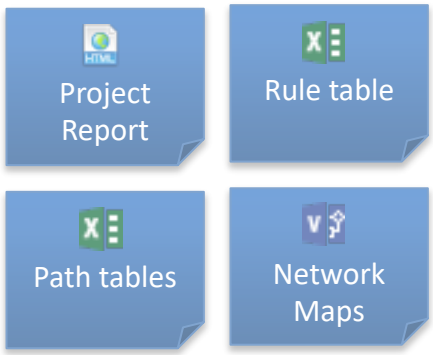
- **Import**:
  1. “Is there best practice guide for troubleshooting guide for importing and/or parsing errors?”
- **Path analysis**:
  1. “Will NP-View correlate paths from multiple firewall configs, like maybe one allows all traffic through a tunnel to another, but another restricts incoming traffic by port/server to trusted host?”
  2. “Is it possible to perform path analysis on the groups drawn on the map, like path analysis from DMZ to ESP”
  3. “Can you show how to combine filter of DMZ to ESP and service of MS-RDP?”
  4. “Identifying interactive remote access (IRA) entering the electronic security perimeter (ESP) without going through an intermediate system (IS)”

Q&A

Input → Process → Output



np-view



Workflow:

1. Import configuration files
2. Review and customize topology map
3. Mark asset criticality and define visual groups
4. Review rules and add justifications
5. Review object groups and mark criticality
6. Run path analysis and verify network accesses
7. Export findings

Network Perception

Robin Berthier
rgb@network-perception.com
(872) 245-4100