Using NP-View at Home & Remote Network Access Verification

Network Perception
support@network-perception.com
773-830-4061

NP-View Training Webinar #1
Apr. 2, 2020

Agenda

- **Reminder on NP-View Resources:** [5min]
  - Portal website and release cycle
  - Knowledge Base, support and File Vault
- **Using NP-View at Home:** [10min]
  - Secure workflow
  - Recommendation on data protection
- **Remote Network Access Verification:** [15min]
  - NERC CIP requirements
  - Checking interactive remote access with NP-View
- **Q&A**

Increased Cybersecurity Risk

THE CORONAVIRUS CRISIS

Cybersecurity Lawyer Who Flagged The WHO Hack Warns Of 'Massive' Remote Work Risks

March 30, 2020 · 5:00 AM ET
Heard on Morning Edition

Large numbers of companies are rolling out mandatory work-from-home policies to help limit the risks posed by the coronavirus outbreak. But cybersecurity experts warn that those remote setups invite new hacking risks.

The Federal Bureau of Investigation recently issued warnings of an uptick in fraudulent crimes tied to the coronavirus, particularly by scammers posing as official health agencies.

NPR: https://www.npr.org/sections/coronavirus-live-updates/2020/03/30/822687397/cybersecurity-lawyer-who-flagged-the-who-hack-warns-of-massive-remote-work-risks
FBI: https://www.ic3.gov/media/2020/200320.aspx

Reminder on NP-View Resources

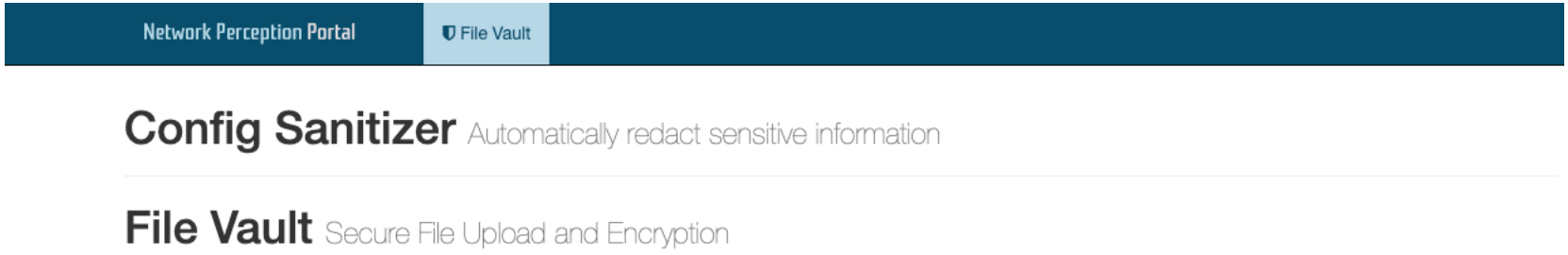
- **Resources**:
  - Portal: portal.network-perception.com
  - Knowledge Base: kb.network-perception.com
  - Support: support@network-perception.com

- **Versions:**

NP-View Java	Legacy user interface (Stable)	**Offline desktop application for snapshot audit**
NP-View HTML	Modern user interface (Beta) New license format	
NP-Live		**On-premise multi-user server for 24/7 monitoring**

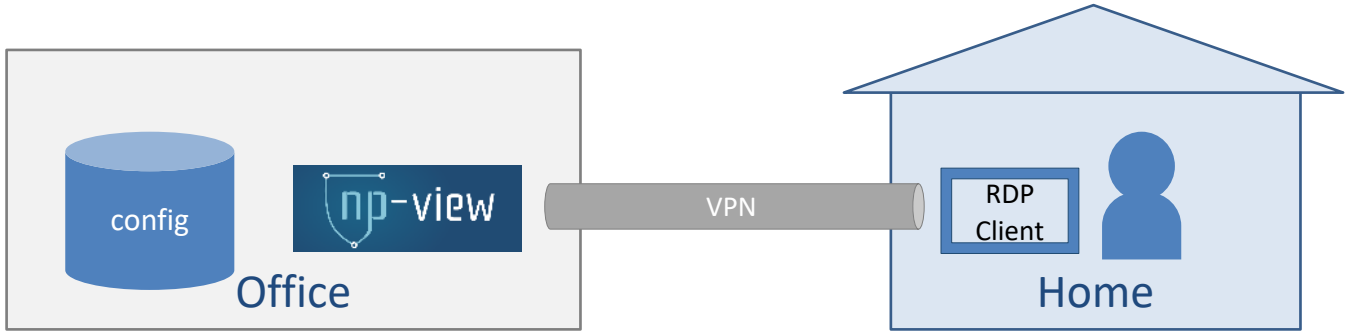
- **Releases:**
  - Quarterly stable release cycle (roadmap)
  - Continuous patch releases (support requests)

- **Config Sanitizer and File Vault**:

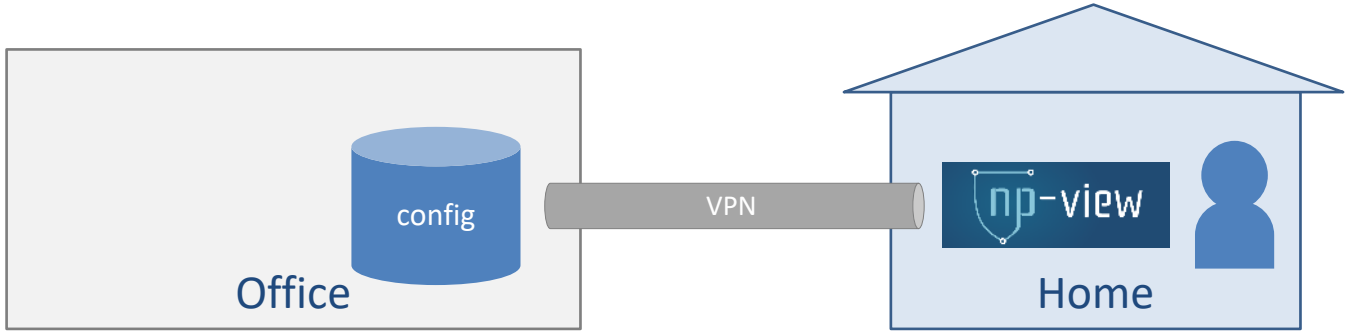


NP-View at Home

- Secure Workflow:
  - **Option 1**: Remote desktop to NP-View workstation

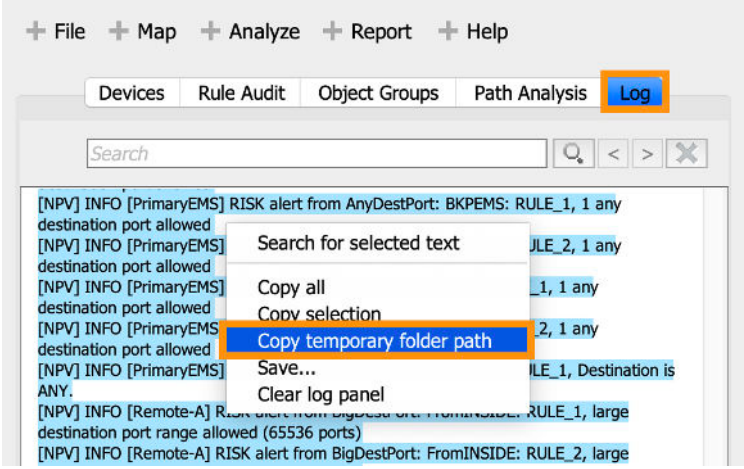


  - **Option 2**: Running NP-View locally with remote access to shared folder



NP-View at Home (cont.)

- Recommendations on Data Protection:
  - **How NP-View works**:
    - NP-View uses a temporary folder while a project is opened
    - When a project is closed, NP-View overwrites all files in the temporary folder with zeros before deleting them
    - NP-View has 2 processes: a user interface and a backend engine. The backend engine listens on the localhost interface (127.0.0.1) port TCP/5555 and TCP/5556
  - **Recommendation #1**: reduce your attack surface and have a secure (offline) NP-View workstation if you import sensitive data
  - **Recommendation #2**: check and wipe out NP-View temporary folders in case projects have not been cleanly closed



Remote Network Access Verification

CIP Reliability Standards Addressing Remote Access:

CIP-003-6

Requirement R1: Entities must have cyber security policies governing remote access to BES Cyber Systems. Senior management must approve these policies to help ensure that secure practices are implemented.

CIP-004-6

Requirement R1: Responsible entities must implement a cybersecurity awareness program that, at least once a calendar quarter, reinforces cyber security practices, which may include practices related to remote access.

Requirement R2: All personnel who have remote access capability must periodically receive training that reinforces cyber security practices.

Requirement R4, Part 4.1-4.3: All personnel who have remote access must be explicitly authorized and periodically reviewed to ensure such access is limited and controlled.

Requirement R5, Parts 5.1 and 5.1: To ensure that terminated or transferred personnel do not retain the ability to access BES Cyber Systems remotely, entities must revoke the access rights of terminated or transferred personnel.

CIP-005-5

Requirement R1, Part 1.1: Entities must protect all BES Cyber Systems with routable connectivity by including them in an Electronic Security Perimeter (ESP) to control access. An ESP is defined as the logical border surrounding a network to which BES Cyber Systems are connected using routable protocol.

Requirement R1, Part 1.2: All connections to BES Cyber Systems originating from outside the ESP must be through an identified access point (through a firewall) so that all connections are known and controlled.

Requirement R1, Part 1.3: For all connections to BES Cyber Systems inside the ESP there must be a documented reason for such access, both inbound and outbound, and a denial to all other access.

Requirement R1, Part 1.4: Remote access via dial-up connectivity must be authenticated.

Requirement R1, Part 1.5: All inbound and outbound communications must be examined to detect malicious communication.

Requirement R2, Part 2.1: Interactive Remote Access to BES Cyber Systems must go through an Intermediate System (limiting the entry points to the ESP and controlling the types of access allowed to BES Cyber Systems).

Requirement R2, Part 2.2: Interactive Remote Access sessions must be encrypted to the Intermediate System to protect the confidentiality and integrity of the communications.

Requirement R2, Part 2.3: Interactive Remote Access sessions must have multi-factor authentication to ensure only appropriate personnel have access.

CIP-007-6

Requirement R1, Part 1.1: BES Cyber Systems are further protected from potential remote access attacks by limiting their network exposed ports and services to only those required for operation of the system.

Requirement R4: In the event of unauthorized or suspicious remote access, entities must keep event logs and periodically review them for intervention or after-the-fact analysis.

Requirement R5, Part 5.1: Remote access users of BES Cyber Systems must also authenticate their interactive use access session to the BES Cyber System.

Source: https://www.nerc.com/FilingsOrders/us/NERC%20Filings%20to%20FERC%20DL/Final%20PUBLIC%20Remote%20Access%20Study%20Report%206-30-2017.pdf

NP-View Workflow

- **Preparation:** Collect and import applicable configuration files from firewalls, routers, and switches into NP-View
- **Asset identification process** + **Electronic Security Perimeter**: Customize the topology map: identify applicable Cyber Assets and Electronic Security Perimeter

  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)

- **Ruleset assessment**

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

- **Interactive Remote Access**

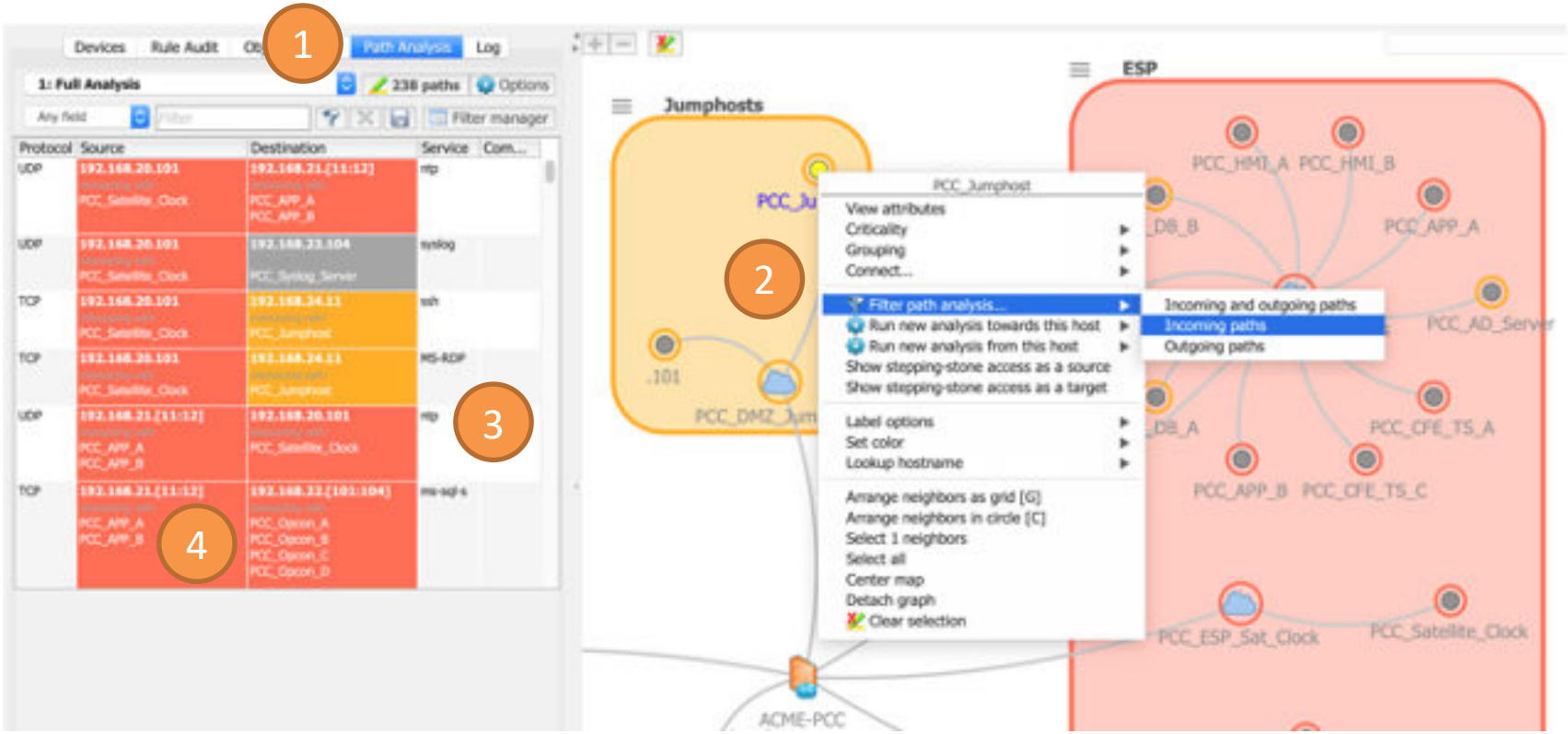
  CIP-005 R2.1: Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset

  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**

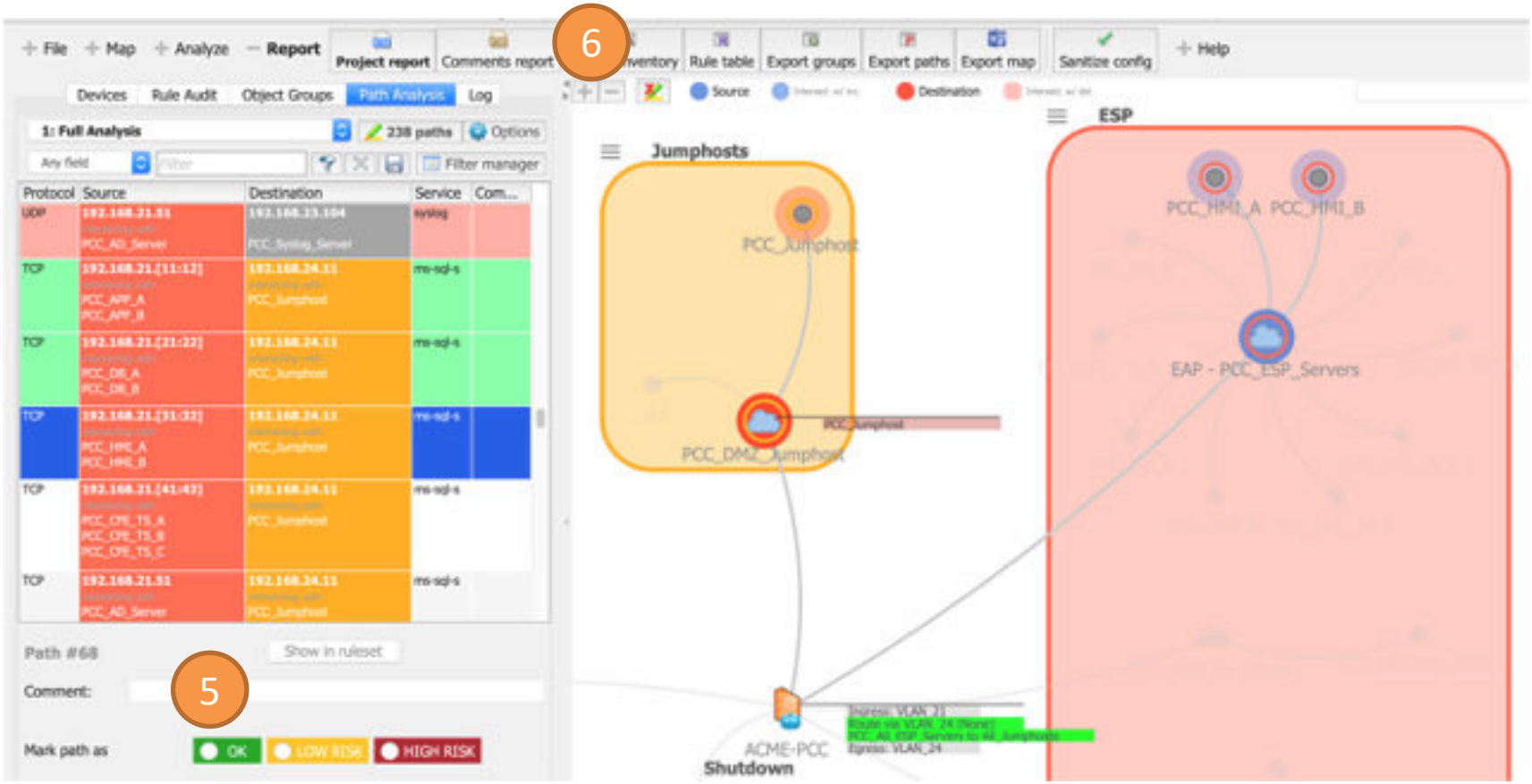
Remote Network Access Verification

- Verifying interactive remote access:
  - Step 1: run a path analysis
  - Step 2: right-click on a cyber asset and filter incoming / outgoing paths
  - Step 3: review accessible ports and services from the path table
  - Step 4: review the use of intermediate system from the path table



Remote Network Access Verification (cont.)

- Verifying interactive remote access (cont.):
  - Step 5: annotate issues in path table
  - Step 6: export the “Comments report” to document findings



Demonstration

- Common interactive remote access ports and services:

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

Q&A

Network Perception

Robin Berthier
rgb@network-perception.com