Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/ot-network-segmentation-validation/

OPERATIONAL TECHNOLOGY BOUNDARIES

Validating IT and OT Segmentation Across Industrial and Utility Sites

The boundary between your corporate network and your control systems is as strong as every rule and every connection on it, documented or not. Verify every conduit with captures and controlled tests, and close each path on your own schedule. Call (800) 868-8189 at any hour.

Published September 5, 2026 · Updated October 30, 2026

By Joseph Caruso, Founder, CEO and CTO, Global Digital Forensics

Comparing CAD Network Diagrams With Live Plant Floor Traffic

When utility executives or industrial CISOs review their architectural CAD drawings, the boundary between corporate IT and plant floor operational technology always looks clean, segmented and heavily firewalled. Live inspection of multi site industrial environments is where our engineers look for what the drawings leave out: undocumented dual homed data historians bridging both networks, overly permissive any to any firewall rules added during a midnight maintenance emergency years ago, and third party equipment vendors dialing directly into programmable logic controllers via unmanaged cellular modems or TeamViewer installations.

How We Audit Boundary Choke Points Across Every Plant and Substation

Working alongside your plant engineers and corporate security teams, Global Digital Forensics conducts comprehensive multi site OT boundary validation engagements. We reconcile firewall configuration exports against live passive traffic captures at every IT and OT choke point, identifying unauthorized cross zone protocols, cleartext authentication sessions and rogue remote access pathways while production runs normally. We then provide plant specific remediation roadmaps that allow your engineering staff to close hidden backdoors and enforce strict zone conduits aligned with IEC 62443, NIST SP 800-82 and NERC CIP standards.

What Firewall Exports Prove and What Packet Captures Add

A firewall rule base is a statement of intent. Read carefully, it shows which zones were meant to talk, over which ports, in which direction, and the hit counters show which rules are actually carrying traffic and which have sat unused since a project ended. Shadowed rules, disabled logging and broad object groups appear in that review, and they are findings in their own right. Traffic that moves around the firewall is read from a different source. A data historian with an interface in each zone, an engineering laptop that bridges WiFi and the control VLAN, a cellular modem bolted inside a cabinet by a vendor: each of these moves traffic around the boundary, and the examiner looks for them on the wire and in the cabinets rather than in the rule base.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Packet capture at each conduit supplies the other half of the picture. A SPAN session or tap on the switch that carries the zone boundary shows every conversation crossing it, including protocols that have no business there, cleartext credentials in engineering sessions and connections that originate from addresses no diagram accounts for. Comparing the capture to the rule base turns two partial records into one documented account of how the boundary actually behaves. We state the coverage of that account precisely. Capture reads the segments where sensors sit, and serial links and devices powered down during the capture window are checked against the drawings, the asset list and the remote access inventory. The report states the capture points and windows so a reader knows the coverage, and our passive asset discovery guide explains how the inventory beneath the boundary review is built.

The Standards the Boundary Is Judged Against

For bulk electric system operators the governing language is in the NERC CIP standards. CIP-005 requires that applicable cyber systems reside within a defined electronic security perimeter, that all external routable connectivity pass through identified electronic access points, that inbound and outbound access permissions have a documented reason and deny everything else by default, and that interactive remote access pass through an intermediate system with multi factor authentication. Each of those is a testable property, and a segmentation validation is in substance a test of whether the perimeter, the access points and the permissions exist as documented. CIP-010 adds the baseline configuration and change management expectations that make a boundary stable once it is correct.

Outside the electric sector the reference is the zone and conduit model of ISA/IEC 62443, which asks the operator to group assets into zones by shared security requirements, define the conduits that connect them and assign each zone a target security level that its controls must meet. NIST SP 800-82 Revision 3 describes the layered architecture most plants follow, with a demilitarized zone between enterprise and control networks and no direct path between them. Water systems certifying under AWIA and maritime operators meeting Coast Guard requirements both point to the same architecture when asked how the control network is protected. We write findings in those terms so a compliance reviewer sees the standard and the evidence side by side, and our utility OT assurance work extends the same method to the readiness file a utility keeps for regulators.

The Validation Engagement Site by Site

The engagement opens with document collection and a scoping session for each site: network drawings, firewall and switch exports, the asset list, the historian architecture, the vendor remote access inventory and the change records that explain how the current rule base came to be. From that material we identify every conduit between enterprise, DMZ and control zones and select the capture points that will see them. Passive capture then runs long enough to observe normal operations, shift changes and any scheduled vendor activity, because a boundary that looks clean on a quiet afternoon often looks different when the integrator dials in on Tuesday night.

Analysis reconciles the capture against the rule base and the drawings and produces three lists: traffic that crosses where the design says it should, traffic that crosses where the design says it should not, and paths that bypass the firewall entirely. Within approved maintenance windows and with the plant engineer present, we then perform controlled traversal tests from enterprise hosts toward the DMZ and from DMZ hosts toward designated control zone hosts to confirm that rules deny what they claim to deny. Remote access paths

© 2026 Global Digital Forensics, Inc. All rights reserved.

receive their own test, from the vendor's entry point to the controller it serves. Each site receives a remediation roadmap ordered by the risk a path creates and the effort to close it, and a multi site program receives an enterprise rollup that shows the boundary posture across every plant in a comparable form. A retest after remediation closes the record. Our OT, ICS and SCADA assessment page describes how this fits a broader program.

Reading the deliverable as a compliance lead means following each conduit from the design document to the observed traffic to the test result, and asking whether the three agree. Where they do, the conduit is documented and defensible. Where observed traffic shows a protocol the design does not permit, the finding is a control finding with the evidence attached. Where a controlled test shows a rule allowing what it was written to deny, the finding is an implementation error with a specific fix. The remediation roadmap orders these by the access an attacker would gain and the effort to close the path, so that the network team closes the paths that matter first and the compliance file shows a reasoned sequence rather than a list. A reviewer who can trace that chain for any conduit has good grounds to rely on the rest.

Common Segmentation Findings and How to Prevent Them

The same findings recur across sectors. A permit any rule inserted during an outage years ago and still in place. Management interfaces of firewalls and switches reachable from the enterprise network or from the control network itself. A single Active Directory domain spanning both sides of the boundary, so that one compromised enterprise credential is a control network credential. Historian replication configured to pull directly from controllers across the boundary rather than from a DMZ mirror. Vendor laptops that join the control network with whatever they carried from the last site. Cellular and DSL modems inside cabinets, outside the network team's inventory. Each of these is what the combination of capture and rule analysis looks for, and each is prevented afterward by a documented conduit list with an owner.

Preparation before the first call shortens every phase. The network engineer exports firewall rule bases with hit counts, switch configurations and VLAN assignments for each site. The plant or control engineer marks the drawings with where historians, engineering workstations and vendor connections actually sit, which is often different from where the drawings show them. The security lead compiles the remote access inventory with the vendor, the method and the business owner for each connection, and gathers any prior audit findings on segmentation. With that material, the scoping call can set capture points and windows for the first site immediately. Utilities working through a regulatory review can start with our New York utility audit builder (evestigate.com/tools/ny-utility-audit-builder/) and the power and energy assessment manual, and our utilities and critical infrastructure practice page describes the sector work as a whole.

Schedule a Multi Site OT Boundary Assessment

Call Global Digital Forensics at (800) 868-8189 to validate the boundary that separates your enterprise network from your physical operations. The initial consultation is free, and our guide to passive first OT asset discovery explains the inventory work that gives a boundary review its baseline.

© 2026 Global Digital Forensics, Inc. All rights reserved.

What the Rule Base Proves and What the Capture Adds

The guide explains that a firewall export states intent while a packet capture shows behavior, and that the boundary is documented when the two agree. This table lists the questions a segmentation validation answers, the source that answers each and how the examiner confirms its coverage, so a compliance lead can read a conduit from design to observed traffic to test result. The third column is the reason capture points and windows are stated in the report, with serial links and powered down devices checked against the drawings and the inventories.

Questions in a segmentation validation, the source that answers each and how its coverage is confirmed.

Question	Source that answers it	How coverage is confirmed
Which zones were meant to talk	Firewall rule base and object groups	Hit counters separate active rules from idle ones
Which rules carry traffic	Hit counters on the rule base	Bypass traffic is read from capture at the conduit
What actually crosses the boundary	Packet capture at the conduit	Capture points are listed so coverage is clear
Dual homed and bridged hosts	Capture compared to the drawings	Quiet hosts are checked against the asset list
Rogue remote access	Capture plus the remote access inventory	Powered down modems are checked against the remote access inventory
Whether a rule denies what it claims	Controlled traversal test in a window	A point in time result, repeated at retest
Cleartext credentials crossing	Capture of engineering sessions	Encrypted sessions are recorded by endpoint, port and timing

Build the New York Utility Audit Workbook

New York utilities preparing for a Public Service Commission or Department of Financial Services review can start in the New York utility audit workbook builder (evestigate.com/tools/ny-utility-audit-builder/). Choose the applicable framework sections, enter each boundary between the corporate and control networks, and record the firewall, historian and remote access path that crosses it. Download the workbook set and keep it with the configuration exports you gather, because the review will ask for both. The builder runs in your browser and keeps your entries on your own machine. When a boundary calls for more than configuration to document, call and a passive capture can record what actually crosses it.

© 2026 Global Digital Forensics, Inc. All rights reserved.

How to Begin and What Happens on the First Call

Our OT Security Readiness: Inventory, Boundaries and Rules Before Testing sets out the items to secure in the order they expire. Have ready the number of sites, their network drawings as they exist, firewall and switch configuration exports if you can obtain them quickly, the remote access inventory with vendors and owners, the historian architecture and any prior audit findings on segmentation. Our OT engineer asks where the enterprise and control boundary sits at each site, which systems have physical safety consequences, which standard or regulator will read the report, when maintenance windows occur and who on the plant floor holds stop authority during any controlled test. You then receive a written scope that names the capture points and conduits for the first site, a timing plan sequenced across sites and a proposal for the validation, the remediation roadmap and the retest. The initial consultation is free, and the hotline at (800) 868-8189 is answered 24/7.

Technical References and Further Reading

Primary sources and provider documentation behind this guide: NIST SP 800-82 Revision 3.

Authorities cited in this guide: NERC CIP standards. Supplies the electronic security perimeter, electronic access point, access permission and interactive remote access requirements in CIP-005 that a boundary validation tests, in the currently effective standards listed by NERC. ISA/IEC 62443 series of standards. Provides the zone, conduit and security level model used to define and evaluate boundaries, as described on the ISA standards page for the series. NIST SP 800-82 Revision 3. Describes the layered OT architecture with a demilitarized zone between enterprise and control networks against which segmentation is evaluated, in the final Revision 3 text.

FREQUENTLY ASKED

Segmentation Proof Without an Outage

Can segmentation be validated without touching the control network?

Most of it can. Passive capture at the boundary switches and offline analysis of firewall and switch configurations produce the majority of findings, including bypass paths and unauthorized cross zone protocols, without sending a packet into the control zone. Confirming that a rule actually denies what it claims is done by a controlled test, which we perform from designated hosts, during approved windows and toward targets the plant engineer selects, with live controllers and safety systems kept off the target list. The report distinguishes passive observations from tested results.

How long does a multi site boundary validation take?

The drivers are the number of sites and conduits, how long passive capture must run at each to observe normal operations and vendor activity, the availability of maintenance windows for controlled testing and the state of the existing documentation. Sites are usually sequenced so lessons from the first refine the rest. A utility with consistent architecture across substations moves faster than a manufacturer whose plants were acquired from different owners with different designs.

© 2026 Global Digital Forensics, Inc. All rights reserved.

What does a segmentation assessment cost?

The initial consultation is free. The proposal reflects the number of sites, the number of conduits to instrument and analyze, whether controlled traversal testing is in scope at each site, the standards the report must map to and the deliverables the engineering, security and compliance functions each need. Operators that prepare the configuration exports and remote access inventory in advance reduce the effort in the first phase.

Our firewall vendor says the rules are correct. Why test?

The vendor's review covers the rule base as written. Validation adds the traffic that moves around the firewall, such as a dual homed historian, a vendor modem or an engineering laptop, and checks that each rule's object groups resolve to what everyone assumes. Capture at the boundary records the traffic that actually crosses, and a controlled test shows whether denial works in practice. The two together are what a regulator or an insurer means when they ask whether segmentation has been validated.

What do we receive at the end?

Each site receives a conduit inventory with owners, a reconciliation of observed traffic against the rule base and design, a list of bypass paths and unauthorized flows with evidence, controlled test results and a remediation roadmap ordered by risk and effort. A multi site program also receives an enterprise rollup comparing boundary posture across plants. Findings are written against the standard that governs you, whether CIP-005, ISA/IEC 62443 or NIST SP 800-82, and a retest after remediation closes the record.

Web Addresses for the Sources Cited

1. NERC CIP standards: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
2. ISA/IEC 62443: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
3. NIST SP 800-82 Revision 3: https://csrc.nist.gov/pubs/sp/800/82/r3/final

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.