Network Intrusion Detection Systems for Critical Infrastructure

by Daniel Paillet, CISSP, CEH

Executive summary

Assaults against critical infrastructure networks are growing in sophistication and are requiring stronger perimeter defenses. Although firewalls offer a good degree of security at the boundary by filtering traffic, these systems can miss advanced attacks coming from inside and outside of the network. Network Intrusion Detection Systems (NIDS), on the other hand, provide an additional layer of depth to a defense strategy. This paper reviews how NIDS defend against cyber attacks.

998-2095-09-15-15AR0

Schneider Electric

Introduction

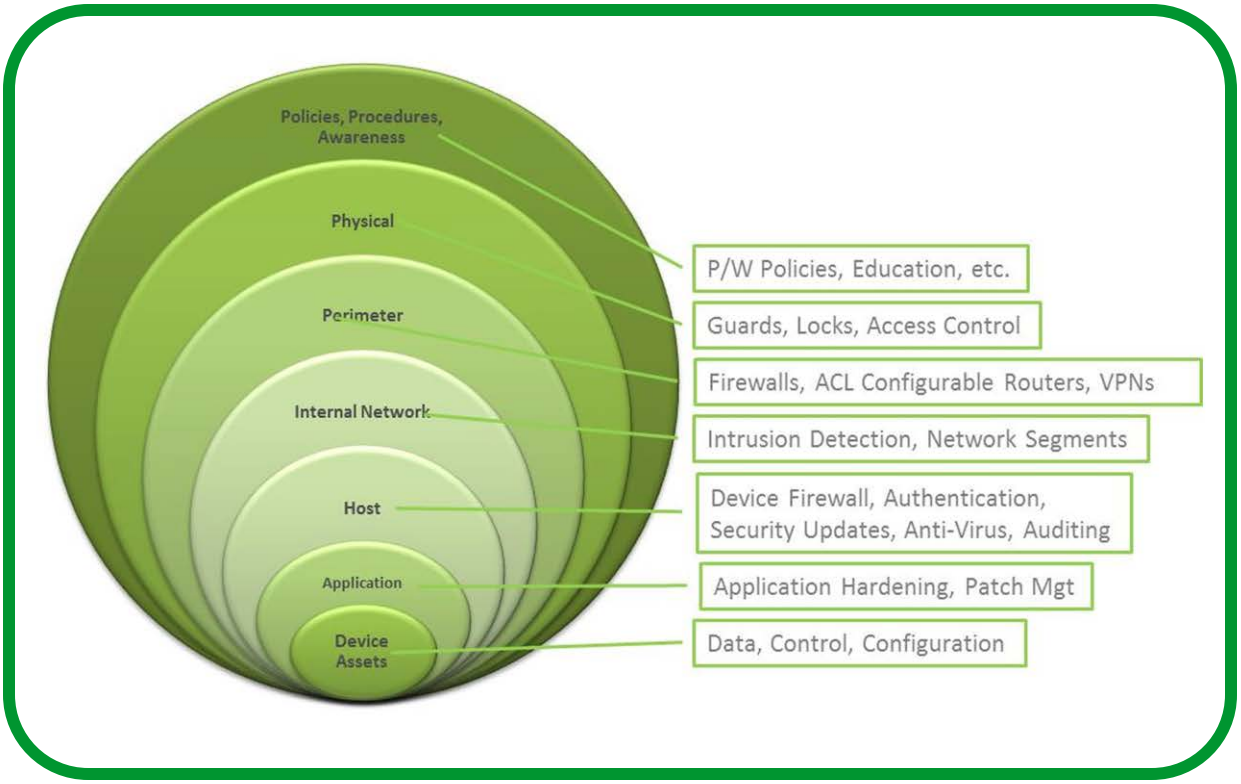
Critical infrastructures (e.g., power grids, water networks, manufacturing SCADA systems) are becoming bigger targets for cyber attacks generated from individuals, rogue groups, and nation states. These attacks are increasing in intensity and sophistication and are capable of changing system settings or destroying systems that are critical to our modern life. Water, power and hospital systems are particularly vulnerable to these types of attacks.

According to Warwick Ashford of computerweekly.com, “Critical infrastructure organizations are commonly targeted by cyber attacks that are aimed at manipulating equipment or destroying rather than stealing data.”[1]

An Organization of American States (OAS) and security firm Trend Micro survey of over 500 critical infrastructure suppliers reports that 44% have uncovered attempts to delete files. In addition, 60% of the organizations polled said that they had detected attempts to steal data and 53% of the respondents noticed an increase of attacks to their computer systems in 2014. The survey went on to reveal that 76% felt that cyber attacks against infrastructure were getting more sophisticated.[2]

Systems that defend against such attacks come in all shapes and sizes. Levels of security attained vary greatly depending upon the depth of implementation. This paper reviews a defense strategy centered on Network Intrusion Detection Systems (NIDS). **Figure 1** below illustrates a planned, in-depth security architecture and shows where NIDS fit in.

Figure 1
Security architectures incorporate multiple levels



[1] Ashford, Warwick, Computer Weekly April 7, 2015
http://www.computerweekly.com/news/4500243886/Critical-infrastructure-commonly-hit-by-destructive-cyber-attacks-survey-reveals

[2] Ibid

Role of Network Intrusion Detection

Several next generation and unified threat management (UTM) firewalls have intrusion detection and intrusion detection prevention capability. These systems can be effective in protecting the network boundary against bad traffic. However, if an attack were to occur within an internal subnet or internal Virtual Local Area Network (VLAN) the firewall sitting on the external boundary would not be able to detect the attack. This is the reason why NIDS are a valuable and needed system to protect critical infrastructure networks. If next generation or UTM-based firewalls were to miss an attack coming from the outside, NIDS would provide an additional layer of defense support.

NIDS systems perform pre-emptive analysis by searching for anomalies and signatures on the network. Once detected, an alert is forwarded to the analyst for review. Some NIDS also have a defensive capability (prevention) where they can block an anomaly or signature before it can cause damage. **Figure 2** below illustrates an example of the placement of a NIDS device in a network.

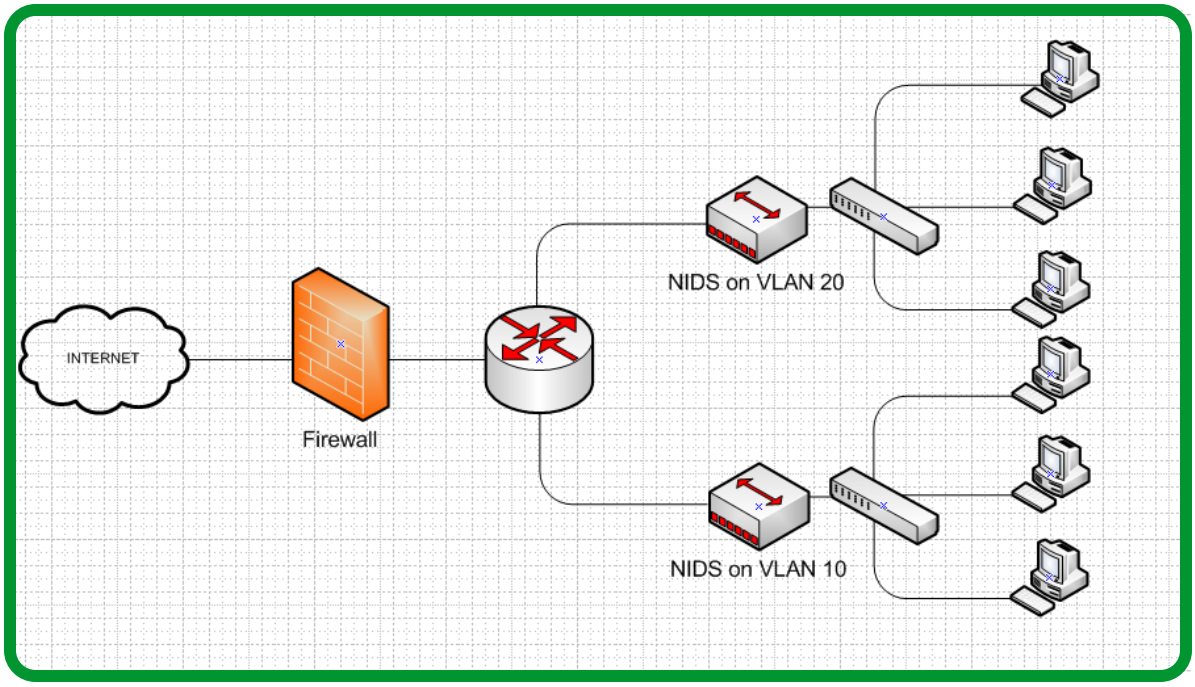


Figure 2
Typical NIDS location within a network

NIDS are deployed at key entry points on a network and report their information to a central server where all alerts appear on a console. These servers tend to run an SQL database where alerting, signatures and reporting are stored. Analysts who are trained in viewing such alerts will be looking at network traffic to determine if the alert and signatures are legitimate attacks. In the event of an attack, appropriate action will be taken by the network defense team to resist the attack according to the organizations internal process and procedures.

Intrusion Detection Systems utilize three different detection methodologies:

- **Signature-Based Detection** - The NIDS detects signatures matching the patterns that correspond to known threats. Detection based signatures are limited in their effectiveness in that they are only as good as the most recent update of signatures that are released by the manufacturer.
- **Anomaly-Based Detection** - In anomaly-based detection, the NIDS compares normal activities against events that are observed and identified to have significant deviations.

Alerts are generated via statistical methods that compare current activity versus previous activity. These can be customized based upon research and observation.

- **Stateful Protocol Analysis** - In this method the NIDS looks at the mechanics of specific protocols to determine if the traffic adheres to the protocol standards. For instance, a repeated “connect” message from a single client within a short timeframe could indicate a Denial of Service (DoS) attack. This can also include Deep Packet Inspection (DPI) to look for any malevolent packets on the network.

Intrusion detection systems are designed to monitor and alert when an unusual pattern or defined signature has been detected. An analyst must investigate and determine if the alert is a false positive or a potential attack against the network. Large organizations have analysts observing traffic from NIDS on a 24x7 hour basis. Some analysts have been trained and have developed the technique of writing custom signatures to capture more detail of network traffic analysis, and to reveal hidden sophisticated attacks launched by outside and inside entities.

Conclusion

Deployment of NIDS within networks varies from organization to organization and from site to site. Budget is an important consideration as is gaining support from senior management for deployment. Other considerations include:

- Identification of the proper vendors with l expertise in the area of physical infrastructure cyber security
- Location and placement of NIDS sensors
- Determination of what types of security policies are in place to address incidents
- Understanding network: traffic direction, and active response mechanisms
- Administration of NIDS: managing installation and maintenance
- Staffing and training of analysts to monitor traffic
- Monitoring of operations and whether 365 x 24 x 7 monitoring is required
- Establishment of an incident response process when an incident is discovered
- Determination of whether outsourcing the management and analysis of NIDS make sense and, if so, how to negotiate the Service Level Agreement

Tuning will also play a large part in the early stages of a NIDS deployment. The analysts’ role is important to determine which alerts are false positives and which alerts are legitimate attacks. This part of the deployment can be very lengthy and intensive. Once the NIDS is tuned (and sometimes tuning is an ongoing process depending on the network), an extra layer of defense will become part of the network architecture.

About the author

Daniel Paillet is currently Cyber Security Lead Architect within the Schneider Electric, Partner Business. His background includes working in the US Department of Defense on various security projects. He has over 15 years of security experience in Information Technology, Operational Technology, Retail, Banking and Point-of-Sale. He holds the CISSP, CEH and other agnostic and vendor specific certifications. His current role is to architect, improve, and develop secure solutions and offerings within Schneider Electric.