EVALUATION PROCEDURES

Our standard evaluation installation is 2 days. The evaluation happens either in a test lab or in the production network. If you need to build a test network see the description for a test network. If you will be testing in a Lab, please be sure the lab is fully configured and functional prior to the ENIRA engineer arriving onsite.

1. Before Installation
We will need a list of all network gear (Switches, Routers, Firewalls) involved, as well as network management and security prevention/detection tools that will be integrated into ENIRA during the testing phase (such as IDS, IPS, SIM, Network Management Tools, Antivirus Servers etc.).

2. Day 1 Installation
Work with someone who has network administrative access for the test network to configure them within ENIRA. The goal is to be able to Investigate/Simulate/Quarantine nodes on the test network by the end of day one.

3. Day 1 Integration
Have people capable of configuring the tools to be integrated with available for discussion/testing.

4. Day 2 Further Discussions
Discuss and outline special features and integrations.

5. Day 2 Demonstration
After the installation and integration is completed, all parties that will need to see the system in operations need to be available for the final demonstration. The demonstration will include network topology, node discoveries, and if one or two test hosts are installed, quarantining those during the demonstration.

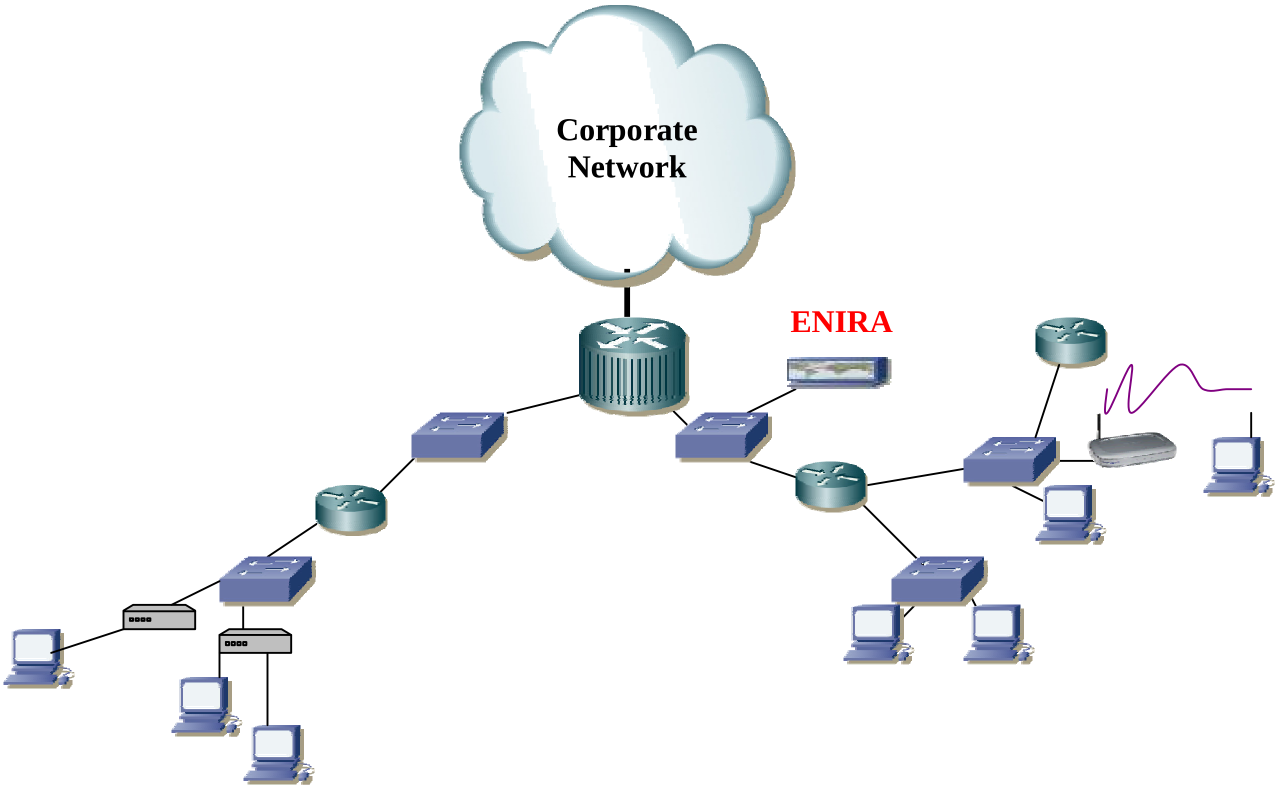
6. Length of the evaluation period
Customer can conduct further tests with the evaluation system during the remaining evaluation time, which is in total up to 2 weeks.

7. Final decision
If, during the evaluation period, the system is installed on the production network, as happens with most of our customers, then the majority of installation and integration has already occurred. If the evaluation confirms the desire to purchase, the customer may decide to take advantage of the installation time already spent by purchasing the existing unit, in place.

Test Network

The testing environment can be an extension of your regular network. Two routers (e.g. Cisco 2500 series) should be connected to a switch (e.g. Cisco 2900 series) in series on one side of the Local Area Network (LAN), and a third should be attached to the other side. Both sides should have clients attached to switches on their subnets. The switch on the single router can be connected to two unintelligent hubs if those are still used in your environment. Client PCs are connected to these hubs. The two routers (and all other subnet devices) can then be moved to any other domains for testing through the firewall. If integration testing is desired then you need to integrate into the test bed the IDS, IPS, Antivirus Software, and other tools you want to test in conjunction with ENIRA. If you don't have IDSs yet, you could also provide a PC and install Snort on it. We will work with this environment.

Sample Test Environment



NRM Functions to Test

1. Test the web interface and remotely configure devices, users, policies and/or rules through administrator role.
2. Network Device Discovery
    a. Creation of Credential Aliases
    b. Discovery of Routers, Switches
3. Execute Network Map creation, and verify that your entire infrastructure is correctly connected. Configuration errors in your infrastructure would appear as isolated router/subnet areas in the 3D map (no connection to the rest of the network).
4. Execute Node Investigate
5. After successful Investigation follow with Quarantine Node Simulate
6. Either quarantine Node from Quarantine Node button after Simulate or from the user menu.
7. Familiarize with the GUI w/ ability to view, create, and edit rules and/or policy.
8. Creation and testing of Response Rules for Denying a User based on IP, MAC, DNS, ENIRA User
9. Creation and testing of Response Rules for Requiring Authorization based on IP, MAC, DNS, ENIRA User
10. Implement policies for desktops, remote clients, collaborative server/desktop, wireless host, Access Point, Exchange, DHCP, DNS, Web, and FTP servers.
11. Test the support for multi-tiered operation where one tier can start the quarantine process and another must approve (or deny) before action is taken. (Authorization process)
12. Test “Block IP Traffic” actions and placement based on network topology
13. Build User Groups with varying levels of user rights to verify GUI menu changes
14. Allow multiple administrators to login and make changes to rules or configurations. Ensure events are logged and attributed to respective administrator for accountability.
15. Test Removal of Quarantine Node and Block IP Traffic Actions (used also for “Rollback” for cases of corrupt or failed policy or action).
16. Create, store, and activate multiple different policies based on current threat and operating environments (Define Threat Levels). Classify policies into groups. Number of groups and names should be configurable.
17. Run Reports on historical quarantine actions

18. Verify Network Device topology changes are detected during a poll and network maps are updated
19. Create Quarantine Zones and verify changes to Simulate
20. Verify View Quarantines output
21. Verify Notification Subscriptions and Message Formats
22. Test integration with an IDS,IPS, SIM tool and setup the report to a trouble ticket tool.

    Example: Setup PC to start an endless ping. Setup an IDS alarm for this type of behavior. On the alarm category configure the ENIRA integration. Setup an expiring blocking time. See the ping trigger the IDS which in turn will quarantine node through ENIRA. After the block expired you can observe that the endless ping started again, which will then trigger the quarantine again.
23. Quarantine hosts based on: Antivirus/Spyware, IDS, Vulnerability Scanner, and SIM alerts.

NCM Functions to Test

1. Verify that the Configuration Library is populated as devices are discovered
2. Verify configuration changes generate Event and create new Configuration Library entry
3. Define Contextual Action and View Filters
4. Define various user groups and associate users with groups
5. Test Full and Contextual configuration compare
6. Verify View Configuration Filters hide sensitive configuration file lines
7. Test Run Device Commands using commands to collect information from a device
8. Test Run Device Commands to make a change to a device
9. Test Push Config File to distribute a partial configuration file
10. Test Push Config File to “rollback” a device’s configuration

Pre-installation Sheet

Evaluation Date:
Start Time:

Company:
Location:

Evaluator:
Phone: Email:

IP addresses, UserIDs, Passwords are known of all equipment to be tested:

YES/NO

Equipment List is filled out and provided to ENIRA (for convenience we have also attached a spreadsheet):

YES/NO

Infrastructure

Brand	Model 1	Qty	Model 2	Qty	Model 3	Qty	Model 4	Qty
Routers								
3Com								
Alcatel								
Cisco								
Enterasys								
Nortel								
Other								
Switches								
3Com								
Alcatel								
Cisco								
Enterasys								
Extreme								
Foundery								
Nortel								
Other								
Firewalls								
Checkpoint								
Cisco								
Netscreen								
Nokia								
Other								

Integration Consideration

Antivirus								
AntiVir								
McAfee								
Symantec								
Trend Micro								
Other								
IDS/IPS								
Cisco								
Intrashield								
McAfee								
Snort								
Symantec								
Other								
SIMS								
Arcsight								
CA								
Cisco								
McAfee								
e-Security								
Symantec								
Other Components								