Customer

Clinton County Schools

Description of Problem

Clinton County Schools uses Extreme Networks Identity Engines(IDE) (End of Sale) solution as RADIUS based network access control. The IDE server provides a central point for authentication for wireless networks, including 802.1x for Microsoft Active Directory(AD) joined machines, as well as MAC-authentication for non-AD machines, and guest/BYOD access. The solution in place provides the ability for IDE to provide the authenticator (generally the access point), the user-name of the connected client. The access point can then forward the user-name upstream via RADIUS accounting to the districts Lightspeed content filter. This provides a single-sign-on(SSO) solution preventing users from constantly re-authentication to a known network.

The IDE server database has become corrupt and is no longer able to provide the user-name information to the access point, thus breaking the solution entirely. Previous efforts include deploying a new instance of IDE, and migrating the configuration via the built in backup/restore methods. This effort proved unsuccessful, as the problem was still exhibited in the new instance.

Proposed Solution

STEP CG proposes deploying a new IDE instance and manually configuring the new instance to avoid inheriting database problems. The steps include, but are not limited to:

- Deploying a new IDE OVA in the existing vmWare environment
- Migrating the licensing from the old IDE instance to the new instance
- Configuring Active Directory integration
- Configuring all required IDE internal user/device groups
- Configuring all required authenticators
- Configuring all RADIUS / User policies
- Configuring all RADIUS / MAC policies
- Creating and configuring all RADIUS outbound values as necessary
- Exporting known device MAC tables for import into new instance
- Importing MAC tables
- Testing database functionality after MAC import
- Testing implementations throughout configuration
- Testing final implementation with customer as on-site resource for verification

Proposed Time-line

Description	Time
Discovery and Data Collection	1 Hour(s)
Initial Deployment & licensing	1 Hour(s)
Advanced configuration	4 Hour(s)
Testing and Verification	2 Hour(s)
Total	**8 Hour(s)**

Cost

Rate	Quantity	Total
$125/hr	8	$1000

Notes

- STEP CG will need cooperation of customer to coordinate licensing through Extreme Networks customer portal
- Customer will need to be available for testing and validation phase at a minimum to ensure full functionality
- Customer may need an active support contract with Extreme Networks in order for license to be transferable.
    - This may be complicated if the customer is not under an existing contract, as support may no longer be available.
- There is the potential that importing known devices introduces the same database problem to the new instance. If this occurs, customer understands that it may be necessary to wipe the guest device database, requiring all users to re-authenticate. There is potential that a corruption of the database occurs with known “district-owned” devices, in which STEP CG can wipe this table as well, and try to import smaller groups to avoid the issue. Unfortunately this cannot be forecasted.