International Research Journal of Engineering and Management Studies (IRJEMS)
Volume: 03 Issue: 05 | May -2019 ISSN: 1847-9790 || p- ISSN: 2395-0126

Cyber Security Routing for Point to Point Networks

B Ganga Bhavani [1], G L N V S Kumar[2], A S Mallesh[3], R Mohan Kumar[4]

[1]B Ganga Bhavaniirst, Asso, Professor, BVCEC, Odalarevu, E.G.Dt., bhavanicse10@gmail.com.
2G L N V S Kumar, Asso, Professor, Department of MCA, B V C I T S, Amalapuram, E.G.Dt., AP. kumar424@gmail.com
3A S Mallesh, Asso, Professor, Department of CSE, BVCEC, Odalarevu, E.G.Dt., satyamallesh621@gmail.com
4R Mohan Kumar, , Professor, Department of CSE, BVCEC, Odalarevu, E.G.Dt.

Abstract - *Abstract: Cyber security refers to the body of technologies, processes and practices designed to protect networks, devices, programs and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security.viruses and worms can self replicate and damage files or systems ,while spyware and Trojans are often used for surreptitious data collection. Cyber security is defined as the protection of systems, networks and data in cyberspace and is a critical issue for all businesses. we have assessed, designed, and implemented some of the largest and most sophisticated network security infrastructures in the United States, Europe, Asia Pacific Africa, and the Middle East.*

Key Words: ARP, DMZ, CSMA,WPA,SSID, FGRM, LDAP, MAC, TMR, PAN, TSAA, ADSA.

1.INTRODUCTION *(Size 11 , cambria font)*

Cyber security, computer security or IT security is the fortification of computer systems from stealing of or damage to their hardware, software or electronic data, as well as from interference or misdirection of the services they provide.. It describes the functional system configuration requirements for the Cyber Security components of ICS Cyber Security. The scope of work to provide this Functional design specification based on the purchase order and agreement during successive customer meetings. Cyber Security services are delivered to the ICS Components using a Secondary Ethernet. This required two free network interfaces on each computer and more for triple homed computers. Existing Computers that will not be upgraded or replace will be checked for sufficient network interfaces and if required additional network interfaces will be provisioned and installed.

1. Literature Review

Members of the "CLP India, Jhajjar - System Admin" security group are decided administrative human rights to local computer so that they can perform functions that require local administrator constitutional rights, for example, to install software, change network settings and to log on to the domain controllers.

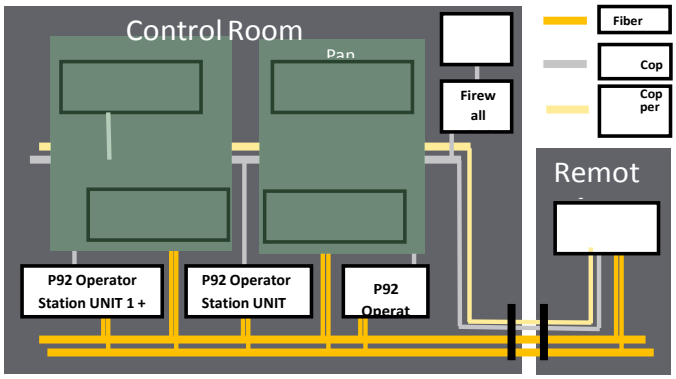
The Domain Controllers host DNS Server for name decision purpose which is one of the major fundamentals of Active Directory. This section gives configuration details for DNS Server security hardening

The offmesh.local domain after automatic creation is ensured that its type set to "Active Directory-Integrated" and "Dynamic updates" is set to "Secure only".

Zone Transfers for the AD incorporated "offmesh.local" domain is set permitted only between Primary and Secondary Domain Controllers Domain Controller hosting DNS Server has GPO applied to define "Audit directory service access" for Success and Failure events. Maximum size of the Log file is set to 128MB and old event will be overwritten as needed.

2 Experimental Setup

Network consists of Network switches and firewalls.



There are North (corporate network facing Firewalls) and South (Plant Network Facing Firewalls). Configuration is done for the security development of the Plant network as well as network device itself.

The following is a summary of the network and zoning used for the Plant Automation Network (PAN), De-militarized Zone (DMZ), and Corporate Network. This design assets connectivity for other non- Schneider Electric Zones and additional computers within the DMZ.

Network consists of Network switches and firewalls. There are North (corporate network facing Firewalls) and South (Plant Network Facing Firewalls). Configuration is done for the security enhancement of the Plant network as well as network device itself.

The following is a outline of the network and zoning used for the Plant Automation Network (PAN), De-militarized

Zone (DMZ), and Corporate Network. This design reserves connectivity for other non- Schneider Electric Zones and additional computers within the DMZ.

Sample paragraph, The entire document should be in cambria font. Type 3 fonts must not be used. Other font types may be used if needed for special purposes. The entire document should be in cambria font. Type 3 fonts must not be used. Other font types may be used if needed for special purposes.

3. Experimental Results

The following table summarizes the constitutional rights associated with each user and group defined above

Role – Rights and Privileges	Groups	Privileges
Add Workstations to Domain	IA Installer Domain Administrator	Allow Logon Locally Allow Logon through terminal services Back up files and directories Bypass traverse checking Change the system time Create a pagefile Debug programs Enable computer and user accounts to be trusted for delegation Increase scheduling priority Load and unload device drivers Allow log on locally Manage auditing and security log Modify firmware environment values Profile single process Profile system performance Remove computer from docking station Restore files and directories Shut down the system Take ownership of files or other objects Shutdown the system

Privilege Users – Add Trusted Publishers to the Domain

The following table summarizes the privileges associated with each user and group defined above.

Role – Rights and Privileges	Groups	Privileges
Add Trusted Publishers	IA Installer Local Administrator Domain Administrator	Allow Logon Locally Allow Logon through terminal services Back up files and directories Bypass traverse checking Take ownership of files or other objects

Privilege Users – Domain Account Management to the Domain

The following table summarizes the privileges associated with each user and group defined above

Role – Rights and Privileges	Groups	Privileges
Domain Account Management	IA Installer Local Administrator Domain Administrator CS Admins	Allow Logon Locally Allow Logon through terminal services Enable computer and user accounts to be trusted for delegation Manage auditing and security log Restore files and directories Take ownership of files or other objects

Privilege Users – Manage Audit and Security Log

The following table summarizes the privileges associated with each user and group defined above.

Role – Rights and Privileges	Groups	Privileges
Manage Security Audit and Security Log	IA Installer Local Administrator Domain Administrator CS Admins	Manage auditing and security log

Privilege Users – Set Time and Date

The following table summarizes the privileges associated with each user and group defined above.

Role – Rights and Privileges	Groups	Privileges
Set Time and Date	IA Installer Domain Administrator CS Admins	Change System Time

Privilege Users – Take Ownership

The following table summarizes the constitutional rights associated with each user and group defined above.

Role – Rights and Privileges	Groups	Privileges
Take ownership of files or other objects	IA Plant Admins	Take ownership of files or other objects

Domain Auditing

The following are the audit settings for the computers within the plant.

Required properties	CS Computers IA Computers Non-IA Computers	Domain Controllers
Audit account logon events	Success, Failure	No Auditing
Audit account management	Success, Failure	Success, Failure
Audit directory service access	No auditing	Success, Failure
Audit logon events Audit Filtering Platform Connection Auditing Filtering Platform Packet Drop	Success, Failure No auditing No auditing	Success, Failure No auditing No auditing
Audit object access	Failure	No Auditing
Audit policy change	Success, Failure	Success, Failure
Audit privilege use	Success, Failure	No Auditing
Audit process tracking	Failure	Failure
Audit system events	Success, Failure	Success, Failure

DNS Server Security

The Domain which is one of the major fundamentals of Active Directory. This section gives configuration details for DNS Server security hardening Controllers host DNS Server for name resolution purpose

Secure Dynamic Updates

The offmesh.local domain after automatic creation is ensured that its type set to "Active Directory-Integrated" and "Dynamic updates" is set to "Secure only".

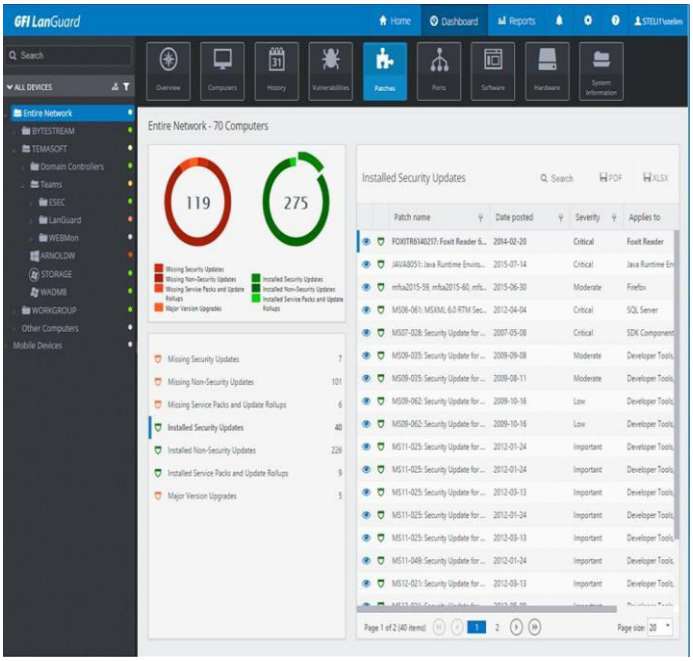
Restricting Zone Transfers

Zone Transfers for the AD incorporated "offmesh.local" domain is set allowed only between Primary and Secondary Domain Controllers.

DNS Audit and Log Settings

Domain Controller hosting DNS Server has GPO applied to define "Audit directory service access" for Success and Failure events. Maximum size of the Log file is set to 128MB and old event will be overwritten as needed.

The Audit Log Configuration will include the audit settings above.



3. CONCLUSIONS

Creating, maintaining, and periodically updating a Corporate Disaster Recovery and Cyber Security plan is critical to any organization wishing to sustain a highly available operating platform. With over 50 years of globally-recognized Control and Safety Systems experience, the Cyber Security Team is an exceptional compliment to an already proven group of technology service providers.

REFERENCES

[1] Bandi, S., M. Gratian, M. Cukier, J. Dykstra, and A. Ginther. 2017 "Correlating Human Traits and Cyber Security Behavior."

[2] Bashir, M., C. Wee, N. Memon, B. Guo. 2017. "Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool," Computers & Security, Volume 65, March 2017, pp. 153-165.

[3] Bhatt, Sh., and T. Santhanam. 2013. "Keystroke dynamics for biometric authentication—A survey." Pattern Recognition, Informatics and Medical Engineering (PRIME), International Conference on, pp. 17-23.

[4] Briggs, P., D. Jeske, and L. Coventry. 2016. "Behavior Change Interventions for Cybersecurity." Behavior Change Research and Theory: Psychological and Technological Perspectives, pp. 115-135.

[5] Dykstra, J. and C. L. Paul. 2015. "Stress and the cyber warrior: cognitive workload in a computer operations center," Journal of Sensitive Cyber Research and Engineering, vol. 3, no. 1, pp. 1-23.

[6] National Science Foundation, "Cyber-Human Systems (CHS)," https://www.nsf.gov/cise/iis/chs_pgm13.jsp. Pfleeger, S.L., and D. D. Caputo. 2012. "Leveraging behavioral science to mitigate cyber security risk," Computers & Security, Volume 31, Issue 4, June 2012, pp. 597-611.

[7] Shi, Weidong, et al. 2011. "Senguard: Passive user identification on smartphones using multiple sensors." Wireless and Mobile Computing, Networking and Communications (WiMob), 2011 IEEE 7th International Conference on. U.K. Government.

[8] "National Cyber Security Strategy 2016 to 2021," November1,2016,https://www.gov.uk/government/publications/national-cyber-security-strategy-2016- to-2021. U.S. Government.

[9] "Federal Cybersecurity Research and Development Strategic Plan," February 2016, https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf. 5 Vieane, A. 2016.