Global Journal of Engineering Science and Research Management

# CONTENT FILTERING AND CLOUD BASED INTRUSION DETECTION SYSTEM

**Dr Sai Manoj Kudaravalli P*, Dr Chiranjeevi Paritala K, Ms Mrudula K**
* Associate Professor Dept. of CSE Amrita Sai Institute of Science and Technology Paritala
Associate Professor Dept. of CSE Amrita Sai Institute of Science and Technology Paritala

**DOI: 10.5281/zenodo.1143971**

**KEYWORDS:** Security Solution Components, Unified Network System, Secure Wireless Architecture.

## ABSTRACT

The prime objective of this proposal is to provide a secure platform for the organizations/ institutions which are involving directly or indirectly with confidential information and having the resources of high usage. This project will complain the needs of the professional institutions in the society offering the e-learning activities like content generation, distribution, training, preparation relating to e-content and its maintenance in both academia and research areas. When it comes to share the user's ideas with experts and software tool providers over internet, security has become the prime concern. The intruders/hackers may be after high speed connection can send malicious viruses and worms to blackening the reputation. In order to ensure security to the resources like software tools, hardware equipment, operating system and e-content the institution has taken necessary precautions. In this context, to overcome the threats, installation of firewalls both hardware and software in nature are of high importance. Though the measures exist, the hackers/intruders are coming up with latest techniques to hijack the networking system. As the users are increasing and mostly depending on internet to extract and use the required information / open source software tools available, to carry out their research and academic projects from the global arena. It is necessary to inspect the incoming and outgoing information, which may cause the damage or loss of digital information, resources and tools. In this context, I propose an intruder detection system against vulnerabilities over internet where the information would be filtered by using a solid hardware firewall with proper configuration and installation of software. This will help the institution to stop intruders from accessing our system. Provider can keep the internet link to the outside world, but it can't share the resources unless the user has granted the privilege. With a firewall in place the users will still have typical email access, but chat and other interactive programs will require the users to take an extra step to grant access before use.

## INTRODUCTION

## OBJECTIVE - SIGNIFICANCE:

The proposal entitled "**Content Filtering: An Intrusion Detection System**" aims at achieving the following goals / objectives, but not limited to

- A Secure Cross – Platform networking model.
- Detection and Prevention of Intrusions from the internet.
- User i.e., Student, Staff and Research Scholar can have an access to the required content / open source tool, preventing unwanted ones.
- Managing Services and Tools efficiently.
- Identification of worms, viruses, masqueradization, Phishing etc.,
- Prevention of data centers from attacks.

The project proposal will be closely associating with department / institutional needs. The institution shall have to maintain the computers, software's and other tools to cater to the needs of the students, faculty and researchers. In order to provide better qualitative knowledge, the institution is facilitating with high end systems, internet connectivity with high speed. To carry out their academic and research activities, everyone is directly or indirectly depending on the internet. In this context, the users of the institution shall have to aware of the viruses, worms and threats which causes to crash the tools like hardware, software, data centers and other resources. Sometimes the entire network system may be crashed. This needs of security like a police to watch/inspect the information coming in and going out of the institution. Hence, there must be a watch on flow of information which may be represented by pictures, text, audio and video formats. Hence, I strongly believe the proposed project is relevant and fulfils the needs of the department and institution in the society. Please refer Annexure I for the proposed system

Global Journal of Engineering Science and Research Management

## LITERATURE SURVEY ON NATIONAL & INTERNATIONAL SCENARIO: PROPOSED SYSTEM

Enterprise businesses are being transformed to meet the evolving challenges of today's global business economy. New innovations and new business models are enabling new kinds of productivity, competitive advantage, revenue growth, and efficiency that drive the top line and the bottom line. Security is fundamental to the ability to leverage, with confidence, these rich services that are critical to business success. The comprehensive and diverse security portfolio enables the complex security challenges faced in this environment to be addressed through an integrated, defence-in-depth approach to security that is embedded in end-to-end solution architectures. In the proposed system, Network Security Integration solution describes how to extend this integrated, defence-in-depth approach to security to encompass the mobility services offered by a LAN. Mobility is a critical service for enterprises, offering employees greater flexibility, and enabling increased productivity, through pervasive access to network resources and applications. However, this service offering must comply with the defined network security policies and integrate with the end-to-end network security strategies in order to be compliant, effective and efficient. Network Security is an ongoing process of defining security policies, implementing proactive security measures to enforce them, monitoring the network to obtain visibility into activity, identifying and correlating anomalies, mitigating threats and reviewing what occurred in order to modify and improve the security posture.

A wired or wireless network is only one of the attack vectors against a network. While a WLAN network must be secure and able to protect itself from attack, a network-wide security solution that only addresses WLAN-related attacks is dangerously unbalanced. Mobile network clients need to be protected on all interfaces at all locations, enterprise networks need to be protected on all their perimeters, and monitoring and anomaly detection are required regardless of the source of network traffic. Ideally the same sets of tools and interfaces should be used to provide these baseline security functions as it reduces operational costs, reduces the risk of misconfiguration, and avoids the creation of a unbalanced security architecture that can be simply bypassed.

| Security Elements and General Network Security Elements | | |
|---|---|---|
| Proactive Security | WLAN Specific Elements | General Network Security Elements |
| Harden the network infrastructure | Cisco Unified Wireless Network, LWAPP, Management Frame Protection, 802.1X | Infrastructure Hardening |
| Protect the endpoints | Wi-Fi Protected Access/Wi-Fi Protected Access2 | CSA and Cisco Secure Services Client |
| Identify and enforce policy on users | Wi-Fi Protected Access/Wi-Fi Protected Access2, Client | CSA, Cisco Secure Services Client, NAC, and Cisco Firewall |

| | | |
|---|---|---|
| | Exclusion on the Wireless LAN Controller | |
| Secure communication | Wi-Fi Protected Access/Wi-Fi Protected Access2 | |
| Access control | Access Control Lists on Wireless LAN Controller | Cisco Firewall |
| Operational Security | | |
| Monitor the network | Wireless LAN Controller, Wireless Control System, Adaptive wireless IPS | AAA, SNMP, Platform Management, and CS-MARS |
| Detect and correlate anomalies, mitigate threats | Wireless LAN Controller, Wireless Control System, adaptive wireless IPS | CS-MARS, CSA, IPS |

**Security Solution Components**

The Secure Wireless Architecture is built on the core architectures for the branch and campus networks. The Secure Network Architecture describes the integration and collaboration of security solutions with the Unified Networks to provide a common security framework for networks regardless of the client access mechanism. The core components of the Secure Architecture includes Unified Network, Intrusion prevention, Rogue detection and mitigation, Access control, Traffic encryption, User authentication, RF interference and DoS monitoring, Security vulnerability monitoring and auditing, Infrastructure hardening—MFP, infrastructure device authentication, CSA, NAC appliance, Firewalls, IPS, MARS

**Solution Architecture**

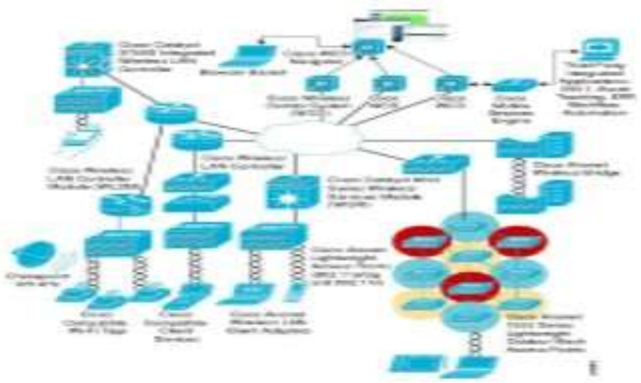
The purpose of the Secure Network Solution Architecture is to provide common security services across the network for wireless and wired users and enable collaboration between wireless and network security infrastructure for layered secure architecture. This architecture is equally applicable in both campus and department deployments. The core components of this architecture are:

- Unified Network Architecture
- Campus Architecture
- Department Architecture

The Unified Network Architecture provides the core mobility services platform securing the wireless environment as well as all the functions required to secure the wireless deployment itself. The underlying campus and department architectures provide a secure high performance, high availability network platform for mobility services. This provides a common wired and wireless platform for the integration of security services, allowing common security architecture to be developed for all network clients and traffic types.

**Unified Network System**

WLANs in the enterprise have emerged as one of the most effective means for connecting to a network. The Network is a unified wired and wireless network solution that addresses the wireless network security, deployment, management, and control aspects of deploying a wireless network. It combines the best elements of wireless and wired networking to deliver secure, scalable networks with a low total cost of ownership. Client devices, Access points, Controllers, network management and mobility services work together to deliver a unified enterprise-class solution.



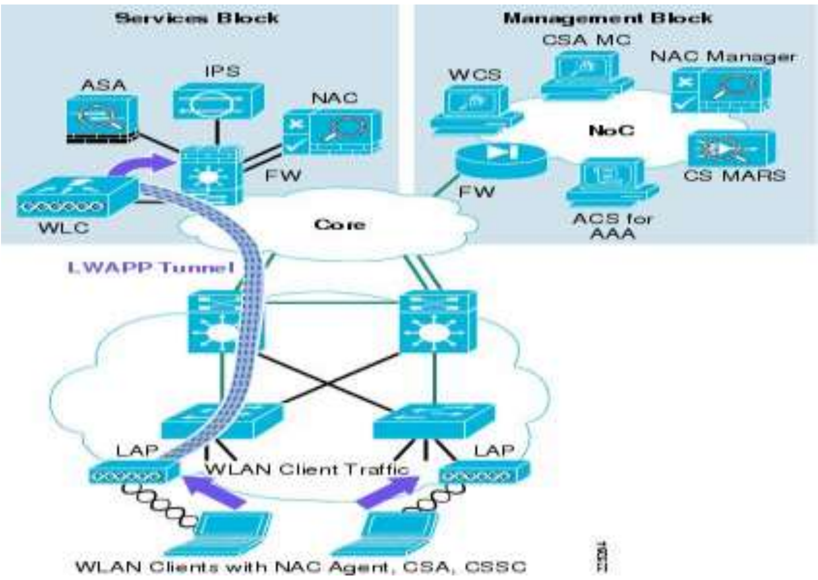
The components required for secure deployment and operations of a wireless network are built into the Cisco Unified Network infrastructure. Leveraging Wireless LAN controllers, access points and wireless management system provide comprehensive wireless security, reducing capital costs while streamlining security operations. Leveraging the features and functions of our proposed network security portfolio delivers a greater degree of control over wired and wireless networks, users, and their traffic. Further, supplementing wireless security with wired network security provides layered defences which deliver more thorough protection, with greater accuracy and operational efficiency for both network operations and security operations teams within the departments. Wireless, due it's over the air transmission, has unique security requirements. The primary security concerns for a network are:

- Rogue access points and clients that can create backdoor access to the network.
- Hacker access points, such as evil twins and honey pots
- Denial of service that disrupts the network.
- Network reconnaissance, eavesdropping, and traffic cracking.
- Controlling the networks users connect to, especially when they are outside of the organization.
- Security for guest users.

Security event management and reporting on all of these functions, complete with physical location tracking of where the security event took place on the network, is key to any robust security solution. All of these concerns are addressed by security technologies built-in to the controllers, access points and CS management system. The same gear that provides connectivity to users also provides security for the entire deployment. A built-in intrusion prevention system detects and mitigates rogue access points and clients, as well as DoS attacks, hacker access points, network reconnaissance, eavesdropping, and attempted authentication and encryption cracking. Further, it can provide wireless IPS monitoring from the same access points that service user traffic, as well as provide full-time dedicated wireless IPS monitoring. Providing both approaches enables site-specific flexibility based on network security policies, which reduces the high infrastructure costs associated with stand-alone wireless intrusion prevention systems. Networks should be self-defending. Providing a hardened network core that is impenetrable to attacks is better than simply detecting an attack after the damage is done. Secure guest access management is also to addressed in the Unified Network infrastructure, providing captive guest user portal, network segmentation, and full guest management functionality. Finally, wrapping all this together is the Security management system.

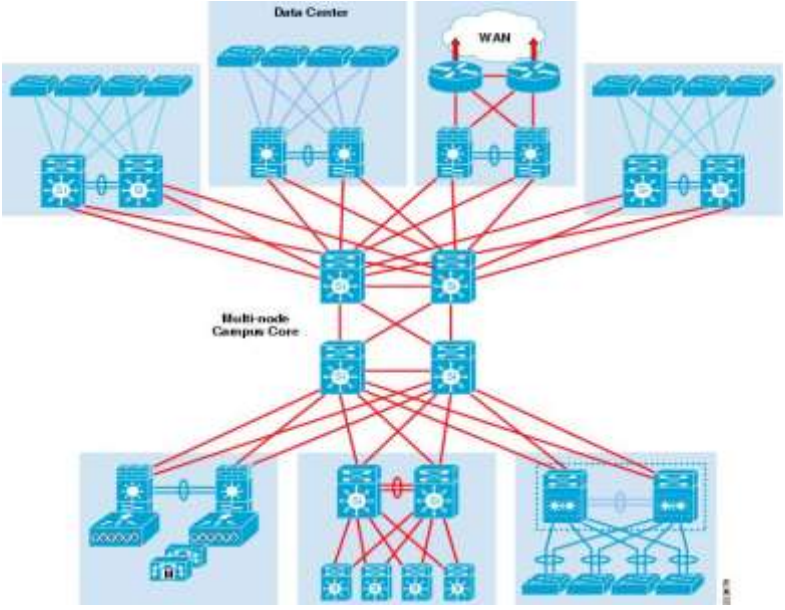
**Secure Wireless Architecture**

The Secure Wireless Solution Architecture consists of a WLAN security component and network security components. The Cisco Unified Wireless Network provides the WLAN security core that integrates with other Cisco network security components to provide a complete solution. The Cisco Unified Wireless Network Architecture provides a mechanism to tunnel client traffic to the wireless LAN controller in a campus service block. The services block provides a centralized location for applying network security services and policies such as NAC, IPS, or firewall. In addition to the components protecting the network in the services block, the Cisco Security Agent provides addition protection network, as well as protecting the mobile client. Wired/wireless collaboration does not just mean putting more boxes in the network. It is the purpose-built linkages that have been built between Cisco's wired and wireless security technologies to deliver a superset of security functionality and protection.



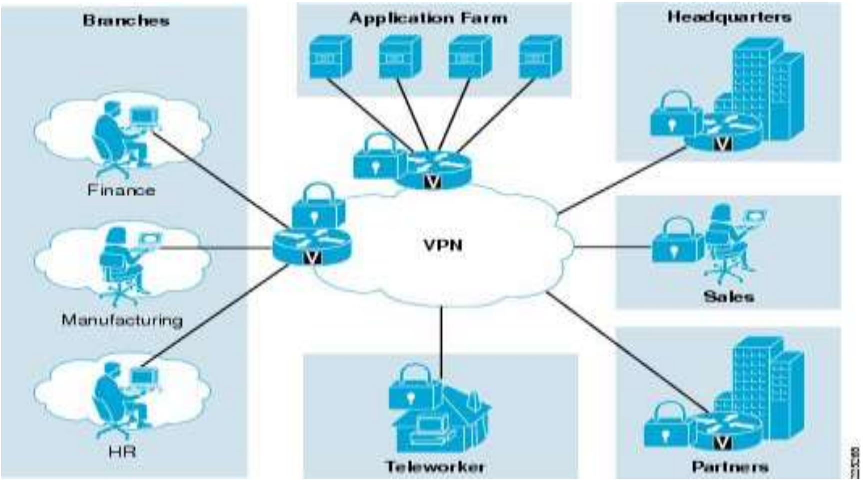
## Campus Architecture

The overall campus architecture is more than the fundamental hierarchical router and switch design. While hierarchies such as access, distribution, and core are fundamental to how to design and build campus networks, they do not address the underlying questions about what a campus network does. The campus network provides services that are used to build the secure wireless solutions. Services such as these provide the foundations for the Secure Solution are High availability, Access services, Application optimization and protection services, Virtualization services, Security services and operational and management services.



## Department Architecture

The full service branch provides the same solutions and services to a branch as are available for the campus. This includes security and wireless, and the Secure Wireless solution is equally applicable for department deployments as it is for the campus. There are a number of LAN/WLAN, firewall, and NAC options for a department, including an H-REAP, WLAN Controller Module (WLCM), 21XX WLC, or larger WLCs, PIX, ASA, or IOS Firewalls, NAC appliances, and IPS appliances.



## REFERENCES

1. Andrew S. Tanenbaum, Computer Network [M]. 4th Edition, USA: Prentice Hall, Sep 2003
2. Chen Bing, "Computer Engineering and Application" Research on Architecture of Network Security *[J]*, Vol38, No7, 2002.
3. Eric Maiwald, Network Security: a beginner's guide. USA: Osborne/McGraw-Hill, 2001.
4. Feng Dengguo, Computer Engineering and Technology *[M]*. 2th Edition, China: Science Press, 2010
5. Hu Daowen, Min Jinhua, Network Security *[M]*. Bei Jing : Qing Hua Press 2004 [6]. Marcus Goncalves, Firewalls complete. USA: McGraw-Hill Companies, 1998
6. Wu Gongyi, Computer Network *[M]*. Bei Jing: Qing Hua Press, 2009.
7. Zhang Shiyong, Network Security Principles and Applications *[M]*. China: May 2003.
8. CISCO Firewall Technology user manual.
9. CISCO Wireless and Network security Integration solution overview